REGIS PRADO BARBOSA

CONSIDERAÇÕES SOBRE E SOLUÇÕES DOS PROBLEMAS PROPOSTOS DO LIVRO TÓPICOS DE TEORIA DOS NÚMEROS DA COLEÇÃO PROFMAT

São Paulo, 2019

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO PAULO - IFSP

REGIS PRADO BARBOSA

CONSIDERAÇÕES SOBRE E SOLUÇÕES DOS PROBLEMAS PROPOSTOS DO LIVRO TÓPICOS DE TEORIA DOS NÚMEROS DA COLEÇÃO PROFMAT

Orientador: Prof. Me. EMILIANO AUGUSTO CHAGAS

Dissertação de mestrado apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação - Mestrado Profissional em Matemática em Rede Nacional, Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, Câmpus São Paulo.

ESTE EXEMPLAR CORRESPONDE A VERSÃO FINAL DA DISSERTAÇÃO
DEFENDIDA PELO ALUNO REGIS PRADO BARBOSA,
E ORIENTADA PELO PROF. ME. EMILIANO AUGUSTO CHAGAS.

SÃO PAULO, 2019

Catalogação na fonte
Biblioteca Francisco Montojos - IFSP Campus São Paulo
Dados fornecidos pelo(a) autor(a)

B238c Barbosa, Regis Prado
Considerações sobre e soluções dos problemas propostos do livro tópicos de teoria dos números da coleção profmat / Regis Prado Barbosa. São Paulo: [s.n.], 2019.
255 f.

Orientador: Emiliano Augusto Chagas

Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, IFSP, 2019.

1. Teoria dos Números. 2. Aritmética. 3. Olimpíada de Matemática. 4. Resolução de Problemas. I. Instituto Federal de Educação, Ciência e Tecnologia de São Paulo II. Título.

CDD 510

REGIS PRADO BARBOSA

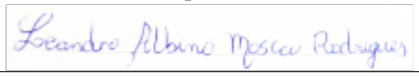
CONSIDERAÇÕES SOBRE E SOLUÇÕES DOS PROBLEMAS PROPOSTOS DO LIVRO TÓPICOS DE TEORIA DOS NÚMEROS DA COLEÇÃO PROFMAT

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação - Mestrado Profissional em Matemática em Rede Nacional, Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, Câmpus São Paulo.

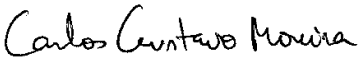
Aprovada em dezembro de 2018.

BANCA EXAMINADORA

Prof. Me. Emiliano Augusto Chagas - Orientador
IFSP - Câmpus São Paulo



Prof. Me. Leandro Albino Mosca Rodrigues
IFSP - Câmpus São Paulo



Prof. Dr. Carlos Gustavo T. de A. Moreira
IMPA

São Paulo - SP
2018

Dedico este trabalho a minha filha Maria Sofia, minha esposa Grazielly, minha mãe Imaculada e meu irmão Armando. Tudo que conquistei até hoje foi graças ao apoio que tive dessas quatro pessoas incríveis.

AGRADECIMENTOS

Agradeço a minha esposa Grazielly com quem sempre pude contar nesses nossos dez anos de relacionamento.

A minha filha Maria Sofia que apenas por existir já me dá mais forças para continuar trabalhando e estudando.

A minha mãe que sempre foi um exemplo para mim e sempre foi meu porto seguro quando a vida trouxe problemas muito grandes.

A meu irmão que mais do que me ajudar a começar nas olimpíadas sempre foi meu parceiro.

A meu amigo e meu eterno professor Edmilson Motta que desde que eu era aluno de olimpíadas até os dias atuais segue me dando conselhos e compartilhando suas experiências de vida comigo.

Ao Professor Emiliano Augusto Chagas, pela orientação deste trabalho e por muitas outras desde que nos conhecemos sendo um amigo que levarei por toda a vida.

Ao Professor Carlos Gustavo T. de A. Moreira, por além de compor a banca examinadora, me ajudar na escolha do tema deste trabalho e me ensinar muitas técnicas para resolução de problemas de matemática.

Ao Professor Leandro Albino Mosca Rodrigues, por aceitar compor a banca examinadora e contribuir com o trabalho.

Ao Instituto Federal de São Paulo, pela oportunidade de realização desse curso de mestrado.

Aos professores e colegas do PROFMAT, do IFSP, que contribuíram não apenas para eu me tornar um professor de matemática mais preparado, mas também uma pessoa melhor.

"Quem diz que não pode ser feito, nunca deve interromper aquele que está fazendo."

(Luffy, *One Piece*)

RESUMO

Este trabalho apresenta as soluções dos problemas propostos do livro Tópicos de Teoria dos Números da Coleção PROFMAT. Há uma breve discussão sobre resolução de problemas matemáticos, especialmente nas teorias de George Polya e Terence Tao que mais contemplam problemas de olimpíada de matemática. De acordo com essas perpesctivas, e a experiência do autor, foram feitas considerações sobre os problemas, incluindo uma categorização dos problemas em de aplicação, olimpíada de matemática iniciante, olimpíada de matemática avançado e problemas teóricos. O ojetivo desta categorização é auxiliar o leitor no estudo destes problemas de acordo com seu perfil, possibilitando para cada indivíduo, desde o professor de matemática até o estudante de olimpíada de matemática, extrair o maior proveito possível dos problemas.

Palavras-chave: Teoria dos Números, Aritmética, Olimpíada de Matemática, Resolução de Problemas, OBM, OBMEP, IMO

ABSTRACT

This work presents the solutions of the proposed problems of the book Topics in Number Theory of Coleção PROFMAT. There is a short discussion about solving mathematical problems, especially in the theories of George Polya and Terence Tao that are more related with math olympiad problems. Considering these perpectives, and the author's experience, considerations were made about the problems, including a categorization of problems in application problems, math olympiad beginner, math olympiad advanced and theoric problems. The goal of this categorization is to help the reader on the study of the problems according its profile, enabling each individual, from the math teacher to the math olympiad student, to extract the best possible benefit from the problems.

Keywords: Number Theory, Artihmetic, Mathematical Olympiad, Problem Solving, OBM, OBMEP, IMO

SUMÁRIO

1

INTRODUÇÃO

Com o crescimento das olimpíadas de matemática, como a OBM e a OBMEP, se torna cada vez mais necessário ter referências confiáveis em português para que alunos e professores possam desenvolver técnicas avançadas em matemática e em argumentação matemática. O autor desta dissertação enquanto aluno de olimpíadas teve certa dificuldade por conta do pouco domínio da língua inglesa. Entre as quatro grandes áreas que compõem praticamente todas as olimpíadas de matemática: Álgebra, Combinatória, Geometria e Teoria dos Números. Como ex-aluno olímpico e treinador de olimpíadas de matemática por muitos anos, vejo que esta útlima é a que mais se afasta do conteúdo regular de sala de aula.

Teoria dos Números é a área da matemática que estuda os números inteiros e suas propriedades, como divisibilidade. É uma área muito importante em pesquisa e com algumas aplicações práticas importantes, como criptografia. Os conteúdos relacionados com essa área se afastam bastante dos temas comuns de ensino médio porque os temas de sala de aula são quase sempre por questões de exames vestibulares.

A proposta da minha dissertação consiste principalmente em produzir e organizar as soluções dos 274 problemas propostos do livro Tópicos de Teoria dos Números da coleção PROFMAT. Os autores desse livro são matemáticos profissionais e possuem uma forte relação com olimpíada de matmática conquistando medalhas na IMO como estudantes e hoje trabalhando na comissão nacional de olimpíadas de matemática. Como os demais livros dessa coleção esse livro existe para auxiliar o ensino da disciplina Teoria dos Números nas turmas do PROFMAT de todo o Brasil. Ele é uma rica referência teórica e conta problemas que vão desde aplicações imediatas das técnicas apresentadas até problemas que fizeram parte da Olimpíada Internacional de Matemática (IMO).

Dessa forma, esse trabalho se diferencia dos anteriores pela profundidade e abrangência dos temas tratados.

A Olimpíada Brasileira de Matemática das Escolas Públicas (Obmep) é um tema bem frequente nos trabalhos do Profmat, no banco de dados das dissertações, o termo "Obmep"aparece 38 vezes e o termo "Olimpíada"ocorre 24 vezes, muito embora existam algumas intersecções nas procuras desses termos.

Trabalhos sobre Olimpíada e Aritmética, ou Teoria dos Números, ocorrem três vezes no repositório de dissertações do Profmat, sendo que em um dos trabalhos (De MORAES, 2018) o enfoque são os erros cometidos pelos alunos da região do autor, os outros dois trabalhos (SOUZA, 2013; PEREIRA, 2016) abordam os problemas da Obmep que envolvem Aritmética. Pereira (2016) inclusive pontua que um dos motivos de escolher essa área foi a falta de material. O autor deste trabalho compartilha dessa opinião. Existem ainda dissertações dedicadas à sequência didática de aulas de olimpíada de matemática, algumas envolvem uma parte bem considerável de Teoria dos Números como De Castro (2013). Badaró (2017) desenvolveu um roteiro de treinamento, com lista de competições que os alunos podem participar, além de livros sugeridos e exercícios de treinamento para os alunos e professores.

A Obmep também foi utilizada como pauta de pesquisa em âmbito de políticas públicas. Como ela é uma competição em larga escala, aplicada em quase todos os municípios brasileiros, é possível encontrar algumas associações relativas aos resultados dos alunos e colégios com avaliações nacionais em larga escala. Biondi, Vasconcellos e Menezes-Filho (2015) encontraram estimativas para encontrar o impacto que alunos premiados na Obmep exerciam no escore da Prova Brasil de seu próprio colégio. O que os pesquisadores encontraram, na avaliação de 2007, foi que

> "A OBMEP tem um efeito positivo e estatisticamente significativo de 2,14 pontos na pontuação média de matemática dos alunos do 9º ano de escolas na Prova Brasil. Esse impacto aumenta à medida que aumenta o número de vezes que a escola participa do programa e é maior nos percentuais de pontuação mais alta do aluno. A análise do retorno econômico também trouxe resultados positivos, mostrando que a OBMEP, ao melhorar a qualidade da educação escolar pública no país, gerará ganhos futuros em termos de

> rendimentos dos participantes."(Biondi, Vasconcellos, Menezes-Filho, 2015, p.14)

Os frutos gerados pelas gerações de competidores olímpicos de diversas áreas do conhecimento podem (e devem) ser quantificados, para que se tenha a dimensão da importância que as olimpíadas possuem e colocá-las na agenda política como uma atividade prioritária de investimento. Um estudo de 2010 conduzido por Campbell e Verna atenta para o fato dessas competições acadêmicas servirem os interesses de Estado.

Nesse estudo, verificou-se a carreira e as produções de 345 ex competidores olímpicos, e as descobertas revelam que 52% desses sujeitos de pesquisa possuíam o título de doutor, e que em conjunto eles produziram mais de 8000 artigos, alguns de bastante impacto. (Campbell, Verna, 2010).

Especificamente em matemática, uma publicação que precedeu esse último trabalho, foi realizada individualmente por Campbell (1997). Dos sujeitos de pesquisa, que são ex alunos olímpicos de matemática, "42% obtiveram doutorado (...) mais um adicional de 13% que estão em conclusão (...). Em termos de produtividade, esses ex olímpicos são responsáveis pela publicação de 15 livros (...), 274 artigos acadêmicos e 15 patentes."(CAMPBELL, 1997).

Além das resoluções dos problemas esse trabalho conta técnicas para resolução de problemas, categorizações dos problemas segundo o autor e algumas sugestões de estudos baseadas nos problemas e nos tipos de leitores segundo o autor. Esperamos que esse trabalho possa auxiliar professores licenciandos em matemática e jovens estudantes a tomarem gosto e se desenvolverem em olimpíadas de matemática, ampliando seus horizontes e contribuindo para uma base sólida na formação de futuros profissionais do país.

2

BASE TEÓRICA EM RESOLUÇÃO DE PROBLEMAS

A base teórica em Teoria dos Números está no livro Tópicos de Teoria dos Números da Coleção do PROFMAT 1ª edição 2012. Neste trabalho trataremos mais profundamente o uso dos resultados desse livro na resolução dos problemas propostos do mesmo. A seguir, serão apresentadas algumas teorias e perspectivas em resolução de problemas em matemática. A primeira de Polya trata resolução de problemas de matemática em geral e a última de Terence Tao se concentra em problemas de olimpíada de matemática.

2.1 RESOLUÇÃO DE PROBLEMAS SEGUNDO POLYA

Em 1945, George Polya publicou o livro "A Arte de Resolver Problemas"(How To Solve It), que rapidamente se tornou sua publicação mais aclamada. Ele vendeu mais de um milhão de cópias e foi traduzido em 17 idiomas. Neste livro, ele identifica quatro princípios básicos de solução de problemas.

Primeiro Princípio de Polya: Entenda o problema

"O que é desconhecido? Quais são os dados? Quais são as condições? É possível satisfazer as condições? A condição é suficiente para determinar o que é pedido? É insuficiente, ou redundante, ou contraditório?"(POLYA, 1956, p.xvi)

Isso parece tão óbvio que muitas vezes nem sequer é mencionado, mas os estudantes são muitas vezes frustrados em seus esforços para resolver problemas simplesmente

porque eles não o compreendem completamente, ou mesmo em parte. Polya ensinou professores a fazer perguntas aos alunos, tais como:

- Você entende todas as palavras usadas para indicar o problema?
- O que é pedido para encontrar ou mostrar?
- Você pode explanar o problema com suas próprias palavras?
- Você consegue pensar em uma figura ou diagrama que possa ajudá-lo a entender problema?
- Existem informações suficientes para que você possa encontrar uma solução?

Segundo Princípio de Polya: Elabore um plano

"Você já viu algo assim antes? Ou você já viu o mesmo problema de um modo ligeiramente diferente? Você conhece um problema relacionado? Existe algum teorema que pode ser útil? (...) É possível reescrever o problema de outro jeito?"(POLYA, 1956, p.xvi)

Polya menciona que existem muitas maneiras razoáveis de resolver problemas. A habilidade de escolher uma estratégia apropriada é melhor aprendida resolvendo-se muitos problemas. Você encontrará uma estratégia cada vez mais fácil. Uma lista parcial de estratégias é a seguinte, também conhecida como a heurística de Polya:

- Adivinhar e verificar
- Procurar um padrão
- Fazer uma lista ordenada
- Desenhar uma imagem
- Eliminar possibilidades
- Resolver um problema mais simples
- Usar simetria
- Usar um modelo
- Considerar casos especiais
- Trabalhar para trás

- Usar raciocínio direto
- Usar uma fórmula
- Resolver uma equação
- Ser engenhoso

Terceiro Princípio de Polya: Concretize o plano

"Carregue o seu plano de solução, conferir cada passo. Você consegue ter clareza que os passos estão certos? Você consegue provar os passos que precisam ser provados?"(POLYA, 1956, p.xvii)

Este passo é geralmente mais fácil do que planejar o plano. Em geral, tudo que você precisa é de cuidado e paciência, dado que você tem as habilidades necessárias. Persista com o plano que você escolheu. Se continuar a não funcionar, descarte-o e escolha outro. Não se engane, é assim que a matemática é feita, até mesmo por profissionais.

Quarto Princípio de Polya: Olhe para trás

"Você consegue conferir o resultado? Você consegue conferir o argumento? Você consegue chegar no resultado de modo diferente? (...) Você consegue usar o resultado, ou o método, em outro problema?"(POLYA, 1956, p.xvii)

Polya menciona que muito pode ser ganho ao refletir e analisar o que você fez, o que funcionou e o que não funcionou. Fazendo isso, você poderá prever qual estratégia usar para resolver problemas futuros.

É relevante mencionar que George Polya nasceu na Hungria e foi um matemático de carreira, trabalhando em diversas áreas como análise combinatória, teoria dos números, análise e probabilidade. A primeira edição do livro "A Arte de Resolver Problemas"data de 1945, quando tinha então 57 anos. Seu trabalho então compartilha a expertise de um profissional em pesquisa matemática sobre a resolução de problemas.

O roteiro de Polya tem a versatilidade de se aplicar a problemas de pesquisa ou de livros didáticos, como por exemplo de cálculo. A primeira olimpíada de matemática que se tem notícia nasceu exatamente no país de origem de Polya, na Hungria, em 1894,

portanto os quatro princípios também podem contemplar olimpíadas de matemática, uma vez que elas já tinham surgido e tiveram um longo tempo para desenvolvimento.

2.2 RESOLUÇÃO DE PROBLEMAS SEGUNDO SCHOENFELD

Uma estrutura mais recente que também versa sobre resolução de problemas foi proposta por Alan Schoenfeld, em 1985, em seu livro "Mathematical Problem Solving", que não possui tradução para o português. O objeto de estudo de Schoenfeld foram alunos do início do curso de matemática e seu desenvolvimento em geometria euclidiana, uma vez que a maioria deles estava há algum tempo sem contato com problemas nessa área do conhecimento.

O panorama desenvolvido por Schoenfeld envolve também quatro categorias, que estão a seguir juntamente com as considerações do autor.

Primeira Categoria: Recursos

"O conhecimento matemático possuído pelo indivíduo que pode ser emprestado para lidar com um problema"(SCHOENFELD, 1985, p.15). Nessa categoria se encontram:

- Intuição e conhecimento informal em relação ao campo
- Fatos
- Procedimentos de algoritmo
- Procedimentos de rotina
- Entendimentos sobre as regras acordadas para trabalhar no domínio

Segunda Categoria: Heurística

"Técnicas e estratégias para se fazer progresso em problemas não familiares e não convencionais; Regras de ouro para resolução efetiva de problemas"(SCHOENFELD, 1985, p.15), na qual se incluem:

- Desenhar figuras e adotar notação adequada
- Explorar problemas relacionados
- Reformular problemas, trabalhar de trás para frente
- Testar e verificar procedimentos

Terceira Categoria: Controle

"Discussões globais com respeito à seleção e implementação de recursos e estratégias"(SCHOENFELD, 1985, p.15). Aqui se envolve

- Planejamento
- Monitoramento e avaliação
- Tomar decisões
- Atitudes conscientes de metacognição

Quarta Categoria: Sistemas de Crença

"O ponto de vista matemático do sujeito, o conjunto de determinantes do comportamento do indivíduo, não necessariamente de modo consciente"(SCHOENFELD, 1985, p.15).

2.3 PROBLEMAS DE OLIMPÍADA DE MATEMÁTICA E TERENCE TAO

Especificamente em olimpíadas de matemática, é possível encontrar alguns trabalhos sobre técnicas de resolução de problemas e considerações sobre tipos de problemas e estratégias. Cheung (1992) utiliza os panoramas de Polya e Schoenfeld na discussão de problemas de olimpíada de matemática que envolvem teoria dos números, combinatória e álgebra, que são os campos não contemplados pela pesquisa de Schoenfeld.

Após a imersão nos problemas e na meta análise sobre o desenvolvimento das resoluções levaram Cheung a concluir que "para problemas em nível olímpico, enquanto a heurística proposta por Polya é útil para analisar problemas e explorar soluções factíveis,

a maioria das estratégias eficazes são as "topic-oriented"(CHEUNG, 1992, p.97), em outras palavras, encontrar algum problema do mesmo tópico que se ajusta em partes, ou possui elementos parecidos, parece surtir mais efeito.

Terence Tao, um dos maiores fenômenos no universo das olimpíadas de matemática, escreveu um livro sobre estratégias de resolução de problemas sob uma perspectiva pessoal. Em "Solving Mathematical Problems", Tao referencia diretamente o trabalho de Polya, além de transcender as técnicas de resolução de problemas, em especial por ser um pesquisador de matemática com um histórico olímpico em matemática, suas perspectivas em problemas possuem o viés de problemas difíceis e competições acirradas. A classificação de Tao (2006) é a seguinte.

Entenda o problema: Que tipo de problema é esse? Há três principais tipos de problemas
Perguntas do tipo "Mostre que ..."ou "Avalie ...", em que uma certa afirmação tem que ser provada verdadeira, ou uma certa expressão tem que ser trabalhada;
"Encontre um ..."ou "Encontre tudo ...", o que requer que alguém encontre algo (ou tudo) que satisfaça certos requisitos;
Perguntas do tipo "Existe um ...", que exigem que você prove uma declaração ou forneça um contra-exemplo (e, portanto, é um dos dois tipos anteriores).

Entenda os dados: O que é dado no problema? Normalmente, uma questão fala sobre vários objetos que satisfazem alguns requisitos especiais. Para entender os dados, é preciso ver como os objetos e requisitos reagem uns aos outros. Isso é importante ao concentrar a atenção nas técnicas e anotações adequadas para lidar com o problema.

Entenda o objetivo: O que nós queremos? Pode ser necessário encontrar um objeto, provar uma declaração, determinar a existência de um objeto com propriedades especiais ou o que for. Como o outro lado dessa estratégia, "entender os dados", conhecer o objetivo ajuda a concentrar a atenção nas melhores armas a serem usadas. Conhecer o objetivo também ajuda na criação de metas táticas que sabemos que nos aproximam da solução da questão.

Selecione uma boa notação: Agora que temos nossos dados e objetivos, devemos representá-los de maneira eficiente, para que os dados e os objetivos sejam representados da maneira mais simples possível. Isso geralmente envolve os pensamentos das duas últimas estratégias.

Anote o que você sabe na notação selecionada; desenhe um diagrama: Colocar tudo no papel ajuda de três maneiras: (a) você tem uma referência fácil mais tarde; (b) o papel é bom para olhar quando você está preso; (c) o ato físico de escrever sobre o que você sabe pode desencadear novas inspirações e conexões.

Modifique o problema ligeiramente: Há muitas maneiras de variar um problema em um que pode ser mais fácil de lidar: (a) Considere um caso especial do problema, como casos extremos ou degenerados. (b) Resolva uma versão simplificada do problema. (c) Formular uma conjectura que implicaria o problema, e tentar provar isso primeiro. (d) Derive algumas conseqüências do problema e tente provar isso primeiro. (e) Reformular o problema (por exemplo, tomar o contrapositivo, provar por contradição, ou tente alguma substituição). (f) Examine soluções de problemas semelhantes. (g) Generalize o problema.

Modifique o problema significativamente: Nesse tipo de estratégia mais agressiva, realizamos grandes modificações em um problema, como remover dados, trocar os dados com o objetivo ou negar o objetivo. (por exemplo, tentar refutar uma declaração em vez de provar isso). Basicamente, tentamos empurrar o problema até que ele quebre e, em seguida, tentar identificar onde a falha ocorreu; isso identifica quais são os principais componentes dos dados e onde estará a principal dificuldade.

Prove os resultados sobre a nossa questão: Os dados estão lá para serem usados, então é preciso pegar os dados e brincar com eles. Pode produzir dados mais significativos? Além disso, provar pequenos resultados poderia ser benéfico mais tarde, ao tentar provar o resultado principal ou encontrar a resposta.

Simplifique, explore dados e alcance metas táticas: Agora, estabelecemos a notação e temos algumas equações. Devemos seriamente considerar atingir nossas metas táticas que estabelecemos. Em problemas simples, geralmente há maneiras padrão de

se fazer isso.Essa parte costuma ser a parte mais longa e mais difícil do problema: no entanto, se alguém se lembra dos teoremas relevantes, os dados e, mais importante, o objetivo, então pode evitar se perder nesse processo.

2.4 COMPARAÇÃO E PERSPECTIVA PESSOAL

A resolução de problemas segundo Polya é muito importante e se aplica de maneira geral para problemas de matemática, sejam de pesquisa ou de olimpíadas. Vale ressaltar que Polya influenciou os demais autores. As categorias de Schoenfeld são muito restritivas. Isso pode ser consequência do contexto de terem sido desenvolvidas baseada em uma turma de curso de matemática e no estudo de geometria euclidiana. Em Teoria dos Números, que é a área principal deste trabalho, essas categorias não pareceram compatíveis com os problemas.

Dentre as bases teóricas apresentadas a que mais gera identificação com o autor é do Terence Tao. Além de ser mais prática que as anteriores, a relação com problemas de olimpíadas de matemática é visível. Qualquer aluno ou professor que consiga utilizar os passos destacados por Tao deve aumentar significativamente a quantidade de problemas que consegue resolver. Esses passos foram muito importantes no desenvolvimento do autor deste trabalho e também para a reunião das soluções aqui contidas.

Podemos destacar principalmente o passo "modifique o problema ligeiramente". Esse passo é extremamente importante na resolução de problemas e não é utilizado pela maioria das pessoas. O motivo disto pode ser que em geral alunos e professores resolvem apenas problemas de exames vestibulares ou voltados para exames vestibulares. Nesses casos espera-se soluções diretas e sem passar por um processo até pelo tempo médio por problema. Porém, acreditamos que qualquer aluno ou professor de matemática pode se beneficiar das ideias de Tao.

3

CATEGORIZAÇÃO DE PROBLEMAS, REUNIÃO DE SOLUÇÕES E GUIA DE ESTUDOS

Os problemas do livro Tópicos de Teoria dos Números da coleção PROFMAT são muito variados. Desde aqueles que são aplicações imediatas dos teoremas e proposições desenvolvidos até problemas originados em pesquisas matemáticas, passando por problemas de olimpíada de matemática que costumam exigir ferramentas próprias de olimpíada de matemática. Visando ajudar os leitores no estudo desses problemas o autor criou uma categorização para os problemas. O autor criou as seguintes quatro categorias e usou as siglas entre parênteses para indicar em cada problema qual a categoria escolhida.

- Aplicação (A) - problema que utiliza diretamente ou quase diretamente as ferramentas desenvolvidas no texto do livro. Grande parte das seções de problemas propostos começa com problemas da categoria aplicação.
- Olimpíada de Matemática Iniciante (OI) - problema de olimpíada de matemática ou com estilo de olimpíada que pode ser abordado por alunos e professores do ensino médio na preparação para competições regionais e nacionais de matemática.
- Olimpíada de Matemática Avançado (OA) - problema de olimpíada de matemática ou com estilo de olimpíada que pode ser usado no treinamento de alunos para competições nacionais e internacionais de matemática. Os principais exemplos são os problemas da IMO.
- Teórico (T) - problema de matemática avançada que aprofunda o domínio e o entendimento de conceitos e estruturas matemática. Muitas vezes são necessárias ferramentas de cursos universitários, como cálculo, para entendimento do problema e resolução. Como exemplo, os problemas da categoria de teórico da

seção de Funções Multiplicativas são fundamentais para o entedimento dessas estruturas.

Essa categorização expressa a opinião do autor sobre os problemas de acordo com sua perspectiva como ex-olímpico e professor de matemática. O leitor pode discrodar dessa categorização, por exemplo alguns problemas de aplicação poderiam muito bem ser classificados como olimpíada iniciante. Outro aspecto que deve ser comentado é que o autor optou por duas categorias de olimpíada. Ele considerou que uma categoria seria insuficiente para o grande espectro de problemas. Usando duas ele poderia direcionar os problemas iniciantes para leitores com pouca experiência e os avançados para alunos e professores que já tiveram contatos com problemas aprofundados.

A metodologia utilizada para reunir as soluções desse trabalho considerou primeiramente que o autor possui grande experiência em olimpíadas de matemática. Como estudante, o autor participou de competições de matemática durante vários anos conquistando três medalhas na IMO, duas de prata e uma bronze. Como professor, ele participa ativamente dos treinamentos para competições de matemática e foi líder do Brasil na IMO 2018. Por tudo isso, a primeira abordagem foi tentar solucionar os problemas sem o uso de outras referências. Essa primeira investida cobriu grande parte dos problemas, principalmente problemas de aplicação (A) e Olimpíada de Matemática Iniciante (OI).
Nos problemas em que a primeira investida não teve sucesso, o autor buscou resoluções ou partes de resoluções em referências conhecidas como o IMO Compendium (Djukic et al, 2011). Mesmo para esses problemas o autor fez mais que uma cópia traduzida, ele reescreveu a resolução com suas próprias palavras tentando torná-la o mais acessível possível dos leitores inexperientes.

Sobre o uso deste material acredito que existam três públicos, o leitor que busca compreender melhor Teoria dos Números, o leitor que busca treinamento básico para olimpídas e leitor que busca treinamento avançado para olimpíadas. Vale ressaltar que nos últimos dois casos podem ser alunos ou professores. A seguir apresento algumas sugestões para esses três públicos. Vale ressaltar que o livro do qual os problemas foram retirados é uma excelente referência e que este trabalho utiliza diversos resultados presentes no livro. Dessa forma, antes de seguir estas sugestões o leitor deve estudar os capítulos do livro para dispor das ferramentas adequadas para tentar resolver os problemas e entender suas resoluções.

- Para quem deseja dominar a área de Teoria dos Números recomenda-se estudar problemas de aplicação (A) e problemas teóricos (T). Não se deve gastar muito tempo tentando resolver esses problemas independentemente, pois a ideia é compreender melhor os resultados. Nos casos dos problemas teóricos (T) recomendo escolher alguns que considerar mais interessante e buscar mais referências. É possível encontrar muitas conexões com outras áreas da matemática.
- Para quem busca treinamento básico de olimpíadas recomenda-se estudar problemas de aplicação (A) e problemas de Olimpíada de Matemática Iniciante (OI). O foco deve ser nos capítulos de Fundamentos e Potências e Congruências. As ideias desses problemas se aplicam a muitos problemas de olimpíada de matemática inclusive problemas de Álgebra e Combinatória.
- Para quem busca treinamento avançado de olimpíadas recomenda-se estudar todos os problemas. Praticamente todos os problemas contribuem para a formação de um aluno que deseja competir em olimpíadas internacionais. Esse grupo foi destacado do anterior porque as técnicas desenvolvidas nos capítulos 2, 3 e 4 do livro Tópicos de Teoria dos Números costumam aparecer em problemas médios ou difícieis da Olimpíada Brasileira de Matemática (OBM) ou de competições internacionais como a IMO.

4

FERRAMENTAS TEÓRICAS DO LIVRO TÓPICOS DE TEORIA DOS NÚMEROS DO PROFMAT

Nesse capítulo temos uma lista de ferramentas desenvolvidas e provas no livro de Teoria dos Números do PROFMAT. As ferramentas vão desde os teoremas mais importantes até definições de estruturas que podem auxiliar o leitor inclusive no entendimento dos enunciados dos problemas propostos.

Teorema 0.20. (Bachet-Bézout) Sejam $a, b \in \mathbb{Z}$. Então existem $x, y \in \mathbb{Z}$ com

$$ax + by = \text{mdc}(a, b).$$

Portanto se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$ então $c \mid \text{mdc}(a, b)$.

Corolário 0.21. Sejam $a, b, c \in \mathbb{Z}$. A equação

$$ax + by = c$$

admite solução inteira em x e y se, e somente se, $\text{mdc}(a, b) \mid c$.

Proposição 0.22. Se $\text{mdc}(a, b) = 1$ e $a \mid bc$, então $a \mid c$.

Corolário 0.23. Seja p um número primo e sejam $a_1, \ldots a_m \in \mathbb{Z}$. Se $p \mid a_1 \cdots a_m$, então $p \mid a_i$ para algum i, $1 \leq i \leq m$.

Lema 0.24. Temos

1. Se p é primo, então $\text{mdc}(a, p)$ é 1 ou p.

2. Se k é um inteiro, então $\text{mdc}(a, b) = \text{mdc}(a - kb, b)$.
3. Se $a \mid c$, então $\text{mdc}(a, b) \mid \text{mdc}(c, b)$.
4. Se $\text{mdc}(a, b) = 1$, então $\text{mdc}(ac, b) = \text{mdc}(c, b)$.

Teorema 0.30. (Teorema Fundamental da Aritmética) Seja $n \geq 2$ um número natural. Podemos escrever n de uma única forma como um produto

$$n = p_1 \cdots p_m$$

onde $m \geq 1$ é um natural e $p_1 \leq \ldots \leq p_m$ são primos.

Proposição 0.38. Para quaisquer $a, b, c, d, n \in \mathbb{Z}$ temos:

1. (Reflexividade) $a \equiv a \pmod{n}$;
2. (Simetria) se $a \equiv b \pmod{n}$, então $b \equiv a \pmod{n}$;
3. (Transitividade) se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a \equiv c \pmod{n}$;
4. (Compatibilidade com a soma e diferença) Podemos somar e subtrair "membro a membro":
$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases} \implies \begin{cases} a + c \equiv b + d \pmod{n} \\ a - c \equiv b - d \pmod{n} \end{cases}$$
Em particular, se $a \equiv b \pmod{n}$, então $ka \equiv kb \pmod{n}$ para todo $k \in \mathbb{Z}$.
5. (Compatibilidade com o produto) Podemos multiplicar "membro a membro":
$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases} \implies ac \equiv bd \pmod{n}$$
Em particular, se $a \equiv b \pmod{n}$, então $a^k \equiv b^k \pmod{n}$ para todo $k \in \mathbb{N}$.
6. (Cancelamento) Se $\text{mdc}(c, n) = 1$, então
$$ac \equiv bc \pmod{n} \iff a \equiv b \pmod{n}.$$

Proposição 0.46. Sejam $a, n \in \mathbb{Z}$, $n > 0$. Então existe $b \in \mathbb{Z}$ com $ab \equiv 1 \pmod{n}$ se, e somente se, $\text{mdc}(a, n) = 1$.

Teorema 0.48. (Wilson) Seja $n > 1$. Então $n \mid (n-1)! + 1$ se, e somente se, n é primo. Mais precisamente,

$$(n-1)! \equiv \begin{cases} -1 \pmod{n} & \text{se } n \text{ é primo} \\ 0 \pmod{n} & \text{se } n \text{ é composto e } n \neq 4. \end{cases}$$

Teorema 0.49. (Wolstenholme) Seja $p > 3$ um número primo. Então o numerador do número

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

é divisível por p^2.

Teorema 0.54. (Euler-Fermat) Sejam a e $m > 0$ são dois inteiros com $\text{mdc}(a, m) = 1$, então

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Teorema 0.55. (Pequeno Teorema de Fermat) Seja a um inteiro positivo e p um primo, então

$$a^p \equiv a \pmod{p}$$

Proposição 0.63. A congruência linear

$$ax \equiv b \pmod{m}$$

admite solução se, e somente se, $\text{mdc}(a, m) \mid b$. Neste caso, há exatamente $\text{mdc}(a, m)$ soluções distintas módulo m.

Teorema 0.64. (Teorema Chinês dos Restos) Se $b_1, b_2, \ldots, b_k$ são inteiros quaisquer e $a_1, a_2, \ldots, a_k$ são primos relativos dois a dois, o sistema de equações

$$\begin{aligned} x &\equiv b_1 \pmod{a_1} \\ x &\equiv b_2 \pmod{a_2} \\ &\vdots \\ x &\equiv b_k \pmod{a_k} \end{aligned}$$

admite solução, que é única módulo $A = a_1 a_2 \ldots a_k$.

O livro traz algumas definições importantes sobre polinômios. Ele define o *grau*

$\deg f(x)$ de um polinômio $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ como sendo o maior i tal que $a_i \neq 0$; o grau do polinômio nulo 0 é definido como sendo $-\infty$. Tal convenção visa a tornar válidas as seguintes identidades para todos os polinômios $f(x), g(x) \in K[x]$:

$$\deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x) \qquad \text{e}$$
$$\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}.$$

O coeficiente do termo de maior grau de um polinômio é chamado de *coeficiente líder*. Um polinômio cujo coeficiente líder é igual a 1 é chamado de *mônico*.

Proposição 1.1. (Algoritmo da divisão) Seja K um corpo. Dados polinômios $f(x), g(x) \in K[x]$, com $g(x) \neq 0$, existem $q(x), r(x) \in K[x]$ (chamados respectivamente de *quociente* e *resto* da divisão de $f(x)$ por $g(x)$), unicamente determinados, tais que

$$f(x) = q(x) \cdot g(x) + r(x) \quad \text{com} \quad \deg r(x) < \deg g(x).$$

Corolário 1.2. Seja K um corpo, $f(x) \in K[x]$ e $a \in K$. Então

$$x - a \mid f(x) \iff f(a) = 0.$$

Proposição 1.4. Seja K um corpo. Um polinômio $f(x) \in K[x]$ não nulo de grau n tem no máximo n raízes em K.

Proposição 1.5. Seja $f(x) = a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$ um polinômio de grau n. Mostre que se p/q é uma raiz racional de $f(x)$, com $p, q \in \mathbb{Z}$ e $\text{mdc}(p, q) = 1$, então $p \mid a_0$ e $q \mid a_n$.

Teorema 1.9. (Bachet-Bézout) Seja $d(x)$ o máximo divisor comum de dois polinômios $f(x)$ e $g(x)$. Então existem dois polinômios $m(x)$ e $n(x)$ tais que $f(x)m(x) + g(x)n(x) = d(x)$.

Definição 1.11. Seja K um corpo. Dizemos que um polinômio não constante $f(x) \in K[x]$ é *irredutível* em $K[x]$ se $f(x)$ não é o produto de dois polinômios em $K[x]$ de graus estritamente menores do que $\deg f(x)$.

Proposição 1.12. Seja K um corpo e sejam $p(x), a_1(x), \ldots a_m(x) \in K[x]$ com $p(x)$ irredutível em $K[x]$. Se $p(x) \mid a_1(x) \cdot \ldots \cdot a_m(x)$, então $p(x) \mid a_i(x)$ para algum i.

Teorema 1.13. (Fatoração única) Seja K um corpo. Todo polinômio não nulo em $K[x]$ pode ser fatorado como um produto de polinômios irredutíveis em $K[x]$. Esta fatoração é única a menos da ordem dos fatores e multiplicação por constantes não nulas.

Teorema 1.14. Seja K um corpo e $f(x)$ um polinômio irredutível em $K[x]$. Então $K[x]/(f(x))$ é um corpo.

Definição 1.16. Um polinômio não nulo $f(x) \in \mathbb{Z}[x]$ é dito *primitivo* se o mdc de seus coeficientes é 1.

Lema 1.17. O produto de dois polinômios primitivos é primitivo.

Teorema 1.18. (Lema de Gauss) Seja $f(x) \in \mathbb{Z}[x]$ um polinômio primitivo não constante. Então $f(x)$ é irredutível em $\mathbb{Q}[x]$ se, e somente se, $f(x)$ é irredutível em $\mathbb{Z}[x]$ (isto é, não podemos escrever $f(x) = g(x)h(x)$ com $g(x), h(x) \in \mathbb{Z}[x]$ não constantes).

Proposição 1.19. (Critério de Eisenstein) Seja $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ um polinômio primitivo não constante. Suponha que exista um número primo p tal que $p \nmid a_n$, $p \mid a_j$ para todo $0 \leq j < n$ e $p^2 \nmid a_0$. Então $f(x)$ é irredutível em $\mathbb{Z}[x]$.

ado $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, definimos a *ordem de* $\overline{a}$, denotado por $\operatorname{ord} \overline{a}$, como o menor inteiro $t > 0$ tal que $\overline{a}^t = \overline{1}$ em $\mathbb{Z}/n\mathbb{Z}$. Se $a, n \in \mathbb{Z}$ com $\operatorname{mdc}(a, n) = 1$, definimos a *ordem de a módulo n*, denotado por $\operatorname{ord}_n a$, como a ordem de $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Note que pelo teorema de Euler-Fermat, temos que $\operatorname{ord}_n a \leq \varphi(n)$. Se $\operatorname{ord}_n a = \varphi(n)$, dizemos que a é *raiz primitiva módulo n*. Por exemplo, 2 é raiz primitiva módulo 5, pois $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, que é a primeira potência de 2 congruente a 1 módulo 5 e $4 = \varphi(5)$.

Proposição 1.22. Temos que $a^t \equiv 1 \pmod{n}$ se, e somente se, $\operatorname{ord}_n a \mid t$.

Corolário 1.23. $\operatorname{ord}_n a \mid \varphi(n)$.

Proposição 1.28. O número a é raiz primitiva módulo n se, e somente se, $\{\overline{a}^t, t \in$

$\mathbb{N}\} = (\mathbb{Z}/n\mathbb{Z})^{\times}$.

Corolário 1.29. Se m divide n e a é raiz primitiva módulo n, então a é raiz primitiva módulo m.

Teorema 1.30. Existe alguma raiz primitiva módulo n se, e somente se, $n = 2$, $n = 4$, $n = p^k$ ou $n = 2p^k$ onde p é primo ímpar.

Proposição 1.43. (Critério de Euler) Seja $p > 2$ um primo e a um inteiro qualquer. Então

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Corolário 1.44. O símbolo de Legendre possui as seguintes propriedades:

1. se $a \equiv b \pmod{p}$ então $(\frac{a}{p}) = (\frac{b}{p})$.
2. $(\frac{a^2}{p}) = 1$ se $p \nmid a$.
3. $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$, ou seja, -1 é resíduo quadrático módulo p se, e somente se, $p \equiv 1 \pmod{4}$.
4. $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.

Lema 1.46. (Gauss) Sejam $p > 2$ um número primo e a um inteiro primo relativo com p. Seja s o número de elementos do conjunto

$$\{a, 2a, 3a, \ldots, \tfrac{p-1}{2} \cdot a\}$$

tais que seu resto módulo p é maior do que $\frac{p-1}{2}$. Então

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Lema 1.47. Seja p um primo ímpar. Então

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{se } p \equiv 1 \pmod{4}, \\ -1 & \text{se } p \equiv 3 \pmod{4}, \end{cases}$$

e

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{se } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{se } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Teorema 1.50. (Reciprocidade Quadrática) Sejam p e q primos ímpares distintos. Então

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Uma classe importante de funções aritméticas é a das chamadas *funções multiplicativas*. Uma função $f : \mathbb{N}^* \to \mathbb{C}$ é dita multiplicativa se $f(mn) = f(m) \cdot f(n)$ para quaisquer m, n primos entre si. No caso em que a propriedade anterior é verdadeira para quaisquer inteiros positivos m e n, dizemos que f é uma *função totalmente multiplicativa*.

Proposição 2.1. Seja $f: \mathbb{N}^* \to \mathbb{R}^*$ uma função totalmente multiplicativa e monótona, então existe $\alpha \in \mathbb{R}$ tal que $f(n) = n^\alpha$.

Teorema 2.2. Se f é uma função multiplicativa então a função

$$F(n) = \sum_{d|n} f(d)$$

é também multiplicativa.

Para todo inteiro positivo n define-se $d(n)$ como o número de divisores positivos de n, $\sigma(n)$ como a soma dos divisores positivos de n e $\sigma_m(n)$ como a soma das m-ésimas potências dos divisores de n. Nesse trecho do livro, os autores relembram também que $\varphi(n)$ denota a quantidade de números naturais menores que n e primos relativos com n.
Todo número inteiro n maior que 1 pode ser escrito como

$$n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s},$$

onde $p_1, \dots, p_s$ são números primos distintos, e $k_1, \dots, k_s$ são inteiros positivos.
Seguindo esta notação temos

$$d(n) = (k_1 + 1)(k_2 + 1) \cdots (k_s + 1)$$

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_s^{k_s+1} - 1}{p_s - 1}$$

$$\sigma_m(n) = \sum_{d|n} d^m = \frac{p_1^{(k_1+1)m} - 1}{p_1^m - 1} \cdot \frac{p_2^{(k_2+1)m} - 1}{p_2^m - 1} \cdots \frac{p_s^{(k_s+1)m} - 1}{p_s^m - 1}.$$

$$\varphi(n) = \prod_{1\le i\le k} \varphi(p_i^{k_i}) = \prod_{1\le i\le k} (p_i^{k_i} - p_i^{k_i-1}) = n \prod_{1\le i\le k} \left(1 - \frac{1}{p_i}\right).$$

Define-se *função de Möbius* $\mu\colon \mathbb{N}_{>0} \to \mathbb{Z}$ por

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } a^2 \mid n \text{ para algum } a > 1 \\ (-1)^k & \text{se } n \text{ é produto de } k \text{ primos distintos.} \end{cases}$$

Lema 2.15. Para todo inteiro positivo n temos

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n > 1. \end{cases}$$

Teorema 2.16. (Fórmula de inversão de Möbius) Seja $f(n)$ uma função sobre os inteiros positivos e $F(n) = \sum_{d|n} f(d)$, então para todo n inteiro positivo,

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Exemplo 2.19. Demonstre que, para todo inteiro $m > 1$,

$$\left| \sum_{k=1}^{m} \frac{\mu(k)}{k} \right| < 1.$$

Para cada x real define-se recursivamente $\alpha_0 = x$, $a_n = \lfloor \alpha_n \rfloor$ e, se $\alpha_n \notin \mathbb{Z}$

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n} \text{ para todo } n \in \mathbb{N}.$$

Se, para algum n, $\alpha_n = a_n$ tem-se

$$x = \alpha_0 = [a_0; a_1, a_2, \ldots, a_n] \overset{\text{def}}{=} a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \; + \cfrac{1}{a_n}}}.$$

Se não denota-se

$$x = [a_0; a_1, a_2, \dots] \stackrel{\text{def}}{=} a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}.$$

Proposição 3.1. Dada uma sequência (finita ou infinita) $t_0, t_1, t_2, \dots \in \mathbb{R}$ tal que $t_k > 0$, para todo $k \geq 1$, definimos sequências (x_m) e (y_m) por $x_0 = t_0$, $y_0 = 1$, $x_1 = t_0 t_1 + 1$, $y_1 = t_1$, $x_{m+2} = t_{m+2} x_{m+1} + x_m$, $y_{m+2} = t_{m+2} y_{m+1} + y_m$, para todo $m \geq 0$. Temos então

$$[t_0; t_1, t_2, \dots, t_n] = t_0 + \cfrac{1}{t_1 + \cfrac{1}{t_2 + \ddots \cfrac{1}{+ \cfrac{1}{t_n}}}} = \frac{x_n}{y_n}, \forall n \geq 0.$$

Além disso, $x_{n+1} y_n - x_n y_{n+1} = (-1)^n$, para todo $n \geq 0$.

Corolário 3.2. As sequências (p_n) e (q_n) satisfazem as recorrências

$$p_{n+2} = a_{n+2} p_{n+1} + p_n \qquad \text{e} \qquad q_{n+2} = a_{n+2} q_{n+1} + q_n$$

para todo $n \geq 0$, com $p_0 = a_0$, $p_1 = a_0 a_1 + 1$, $q_0 = 1$ e $q_1 = a_1$. Além disso,

$$p_{n+1} q_n - p_n q_{n+1} = (-1)^n$$

para todo $n \geq 0$.

Corolário 3.3. Temos, para todo $n \in \mathbb{N}$,

$$x = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}} \qquad \text{e} \qquad \alpha_n = \frac{p_{n-2} - q_{n-2} x}{q_{n-1} x - p_{n-1}}$$

Proposição 3.4. Temos

$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{(\alpha_{n+1} + \beta_{n+1}) q_n^2}$$

onde

$$\beta_{n+1} = \frac{q_{n-1}}{q_n} = [0; a_n, a_{n-1}, a_{n-2}, \dots, a_1].$$

Em particular,

$$\frac{1}{(a_{n+1} + 2) q_n^2} < \left| x - \frac{p_n}{q_n} \right| = \frac{1}{(\alpha_{n+1} + \beta_{n+1}) q_n^2} < \frac{1}{a_{n+1} q_n^2}.$$

Proposição 3.7. Para todo $k \geq 0$, temos

$$\frac{p_{2k}}{q_{2k}} \leq \frac{p_{2k+2}}{q_{2k+2}} \leq x \leq \frac{p_{2k+3}}{q_{2k+3}} \leq \frac{p_{2k+1}}{q_{2k+1}}.$$

Proposição 3.9. Dados inteiros $a_0, a_1, a_2, \ldots$, com $a_k > 0, \forall k \geq 1$, existe um único número real α (que é irracional) cuja representação por frações contínuas é $[a_0; a_1, a_2, \ldots]$.

Teorema 3.11. Temos, para todo $n \in \mathbb{N}$,

$$\left| x - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$$

Além disso,

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{2q_n^2} \qquad \text{ou} \qquad \left| x - \frac{p_{n+1}}{q_{n+1}} \right| < \frac{1}{2q_{n+1}^2}.$$

Teorema 3.15. Para todo $p, q \in \mathbb{Z}$, com $0 < q < q_{n+1}$ temos

$$|q_n x - p_n| \leq |qx - p|.$$

Além disso, se $0 < q < q_n$ a desigualdade acima é estrita.

Corolário 3.16. Para todo $q < q_n$,

$$\left| x - \frac{p_n}{q_n} \right| < \left| x - \frac{p}{q} \right|$$

Corolário 3.17. Se $|qx - p| < |q'x - p'|$, para todo p' e $q' \leq q$ tais que $\frac{p}{q} \neq \frac{p'}{q'}$, então $\frac{p}{q}$ é uma reduzida da fração contínua de x.

Teorema 3.18. Se $\left| x - \frac{p}{q} \right| < \frac{1}{2q^2}$ então $\frac{p}{q}$ é uma reduzida da fração contínua de x.

Teorema 4.1. (Pitágoras) Sejam a, b e c os comprimentos dos lados de um triângulo. O ângulo oposto ao lado c é reto se, e somente se, $a^2 + b^2 = c^2$.

Proposição 4.8. Sejam a e b dois números inteiros tais que $\text{mdc}(a,b) = 1$ e seja p um número primo ímpar tal que p divide $a^2 + b^2$, então p deixa resto 1 quando dividido por 4.

Proposição 4.9. Sejam m e n números que são somas de dois quadrados, então mn também é soma de dois quadrados.

Observação 4.10. Pelo mesmo processo podemos obter que

$$mn = (ac + bd)^2 + (bc - ad)^2 = (ac - bd)^2 + (bc + ad)^2,$$

isto é, se $m, n \neq 2$, então mn tem no mínimo duas representações como soma de dois quadrados.

Lema 4.11. (Lema de Thue) Se m é um número natural e a é um inteiro primo relativo com m, então existem números naturais x e y não nulos menores que $\sqrt{m}$ e tais que algum dos números $ax + y$ ou $ax - y$ é divisível por m.

Teorema 4.12. Todo primo da forma $4k + 1$ pode-se escrever como soma de dois quadrados de inteiros positivos.

Teorema 4.13. Seja n um número primo da forma $4k + 1$. Então n pode ser escrito de forma única como soma de dois quadrados.

Proposição 4.15. Seja $a + b\sqrt{d}$ a solução fundamental da equação de Pell $x^2 - dy^2 = 1$. Se $\{(x_n, y_n)\}_{n\in\mathbb{N}}$ é a sequência de soluções da equação, então

$$\begin{aligned} x_{n+2} &= 2ax_{n+1} - x_n \\ y_{n+2} &= 2ay_{n+1} - y_n, \end{aligned}$$

para todo $n \geq 1$.

Teorema 4.17. Se A tem um divisor primo da forma $4k + 3$, então a equação $x^2 - Ay^2 = -1$ não tem solução inteira positiva.

Teorema 4.18. Seja p um primo da forma $4k + 1$. Então a equação $x^2 - py^2 = -1$ sempre possui solução.

Proposição 4.20. Seja $\alpha = x_1 + y_1\sqrt{A} > 1$ onde (x_1, y_1) é a solução mínima de $x^2 - Ay^2 = 1$. Dado $c \in \mathbb{Z}$ não nulo, se existem $x, y \in \mathbb{N}$ com $x^2 - Ay^2 = c$, então existem $u, v \in \mathbb{N}$ com $u + v\sqrt{A} \leq \sqrt{\alpha|c|}$ e $u^2 - Av^2 = c$ (em particular, para esta solução $0 \leq u \leq \sqrt{\alpha|c|}$ e $0 \leq v \leq \sqrt{\alpha|c|/A}$).

Os *inteiros de Gauß* são os elementos do conjunto

$$\mathbb{Z}[i] \stackrel{\text{def}}{=} \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$

subconjunto dos números complexos (onde $i^2 = -1$). Define-se a *norma* de um inteiro de Gauß como

$$\begin{aligned} N\colon \mathbb{Z}[i] &\to \mathbb{Z} \\ z = a + bi &\mapsto |z|^2 = z\bar{z} = a^2 + b^2. \end{aligned}$$

Lema 4.24. (Divisão Euclidiana) Sejam $\alpha, \beta \in \mathbb{Z}[i]$ com $\beta \neq 0$. Então existem inteiros de Gauß $q, r \in \mathbb{Z}[i]$ tais que

$$\alpha = \beta q + r \qquad \text{com} \qquad N(r) < N(\beta).$$

Definição 4.26. Seja A um domínio, isto é, um anel em que ($ab = 0 \implies a = 0$ ou $b = 0$). Dizemos que um elemento $u \in A$ é uma *unidade* (ou um elemento *invertível*) se ele possui inverso multiplicativo em A, isto é, existe $v \in A$ tal que $uv = 1$. O conjunto de todas as unidades de A com a operação de produto é um grupo multiplicativo, o *grupo de unidades* de A, que denotamos por $A^\times$.

Teorema 4.27. (Bachet-Bézout) Sejam α e β dois elementos em $\mathbb{Z}[i]$ primos entre si, isto é, cujos únicos divisores comuns são unidades. Então existem $x, y \in \mathbb{Z}[i]$ tais que

$$\alpha x + \beta y = 1.$$

Definição 4.30. Dizemos que $\pi \in A \setminus \{0\}$ é *irredutível* se ele não pode ser escrito

como produto de dois elementos em $A \setminus A^\times$. Dois irredutíveis π_1 e π_2 são ditos *associados* se eles diferem por multiplicação por uma unidade: $\pi_1 = u\pi_2$ com $u \in A^\times$.

Lema 4.31.

1. $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Em particular $u \in \mathbb{Z}[i]^\times \iff N(u) = 1$.
2. Se $\pi \in \mathbb{Z}[i]$ é tal que $N(\pi)$ é um número primo, então π é irredutível.
3. Se $p \in \mathbb{Z}$ é um primo $p \equiv 3 \pmod 4$, então p é irredutível em $\mathbb{Z}[i]$.

Lema 4.32. Seja $\pi \in \mathbb{Z}[i]$ um elemento irredutível. Então

$$\pi \mid \alpha\beta \implies \pi \mid \alpha \quad \text{ou} \quad \pi \mid \beta$$

para $\alpha, \beta \in \mathbb{Z}[i]$.

Teorema 4.33. (Fatoração única) Qualquer elemento $\alpha \neq 0$ de $\mathbb{Z}[i]$ admite uma fatoração

$$\alpha = \pi_1 \pi_2 \dots \pi_n$$

em elementos irredutíveis π_i. Tal fatoração é única a menos da ordem dos fatores e de multiplicação por unidades (isto é, a menos de associados).

Exemplo 4.40. Demonstre que a equação $x^4 + y^4 = z^2$ não possui soluções inteiras positivas, isto é, não existem tripas pitagóricas em que os dois catetos sejam quadrados perfeitos.

Exemplo 4.41. Mostre que a equação $x^4 - 2y^2 = 1$ somente possui soluções triviais.

Exemplo 4.43. Mostre que a equação diofantina

$$x^2 + y^2 + z^2 = 3xyz.$$

possui infinitas soluções inteiras positivas, e descrevê-las.

Esta equação é conhecida como equação de Markov.

5

USANDO AS PASSOS DE RESOLUÇÃO DE ALGUNS PROBLEMAS

5.1 INFLUÊNCIA DAS RESOLUÇÕES SOBRE AS CATEGORIAS

Nesse capítulo vamos nos aprofundar nos passos para a resolução de alguns problemas. Os problemas foram separados em seções de acordo com a categoria. Esperamos ressaltar como as resoluções auxiliaram na categorização dos problemas.

Diante dos exemplos que serão apresentados nesse capítulo, observa-se que na resolução dos problemas de Aplicação (A) o passo "modifique o problema ligeiramente"nos leva a ferramentas desenvolvidas no livro. Encontra-se desde problemas semelhantes a exemplos até problemas no qual deve-se utilizar uma sequência de passos, ou seja um algoritmo, na resolução.

Os problemas da categoria olimpíada exigem ferramentas geralmente usadas em competições de matemática e, por isso, conhecidas por professores e alunos que participam delas. Por exemplo, o resto que um inteiro ao quadrado deixa na divisão por 8 e a ideia de somar todos os elementos de dois conjuntos que possuam propriedades similares. A diferenciação entre Olimpíada de Matemática Iniciante (OI) e Olimpíada de Matemática Avançado (OA) é feita através do grau de dificuldade que se evidencia principalmente no passo "simplifique, explore dados e alcance metas táticas". Nos problemas OA esse passo final exige um processo específico desde cotas para variáveis até caraterização de sequências. Já nos problemas OI esse passo pode não ser necessário e mesmo quando se faz necessário quase sempre há uma maneira padrão de concluir a resolução.

Os problemas Teóricos (T) são problemas envolvendo resultados, conceitos e estrutuas matemáticas. Nos três primeiros passos relacionados com o entendimento do problema, dos dados e do objetivo, é possível perceber que são problemas que se afastam mais das ferramentas desenvolvidas no livro texto quando comparado com as outras três categorias. Vale ressaltar também que os resultados dos problemas teóricos se mostram mais úteis em outras áreas da matemática, como, por exemplo, em análise.

5.2 PROBLEMAS DE APLICAÇÃO

Problema 0.1. Demonstrar por indução que para $n \geq 1$ natural

(a) $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

(b) $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$.

(c) $(1^5 + 2^5 + \cdots + n^5) + (1^7 + 2^7 + \cdots + n^7) = 2(1 + 2 + \cdots + n)^4$.

(d) $\operatorname{sen} x + \operatorname{sen} 2x + \cdots + \operatorname{sen} nx = \dfrac{\operatorname{sen} \frac{(n+1)x}{2} \cdot \operatorname{sen} \frac{nx}{2}}{\operatorname{sen} \frac{x}{2}}$.

Entenda o problema - é um problema do tipo "mostre que ...".

Entenda os dados - nesse problema o único dado n é um natural maior do que ou igual a 1.

Entenda o objetivo - dado que esse problema está na seção de indução, então nosso objetivo é provar usando indução cada uma das equações.

Selecione uma boa notação - nesse problema o enunciado já nos fornece uma boa notação que pode ser usada na solução.

Modifique o problema ligeiramente - podemos examinar demonstrações por indução, como, por exemplo, a solução do exemplo 0.1. do livro no qual prova-se que $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Prove os resultados sobre a nossa questão -basta usar indução e concluir a resolução.

Problema 1.12. Seja $K = (\mathbb{Z}/(3))[x]/(f(x))$ onde $f(x) = x^2 + x + 2$. Mostre que $f(x)$ é irredutível em $(\mathbb{Z}/(3))[x]$ e portanto K é um corpo. Construa a tabela de multiplicação do grupo K^* e usando esta tabela determine o menor inteiro positivo n tal que $x^n = 1$ em K.

Entenda o problema - esse problema apresenta duas partes e, por isso, tem tipo "mostre que ..."e "encontre algo...".

Entenda os dados - temos o polinômio $f(x) = x^2 + x + 2$ e conjunto $K = (\mathbb{Z}/(3))[x]/(f(x))$ dos polinômios com coeficiente módulo 3 separados em classes módulo $f(x)$.

Entenda o objetivo - devemos provar que $f(x)$ é irredutível em $(\mathbb{Z}/(3))[x]$. Isso já implica que K é um corpo. Também devemos encontrar a ordem de x em K.

Modifique o problema ligeiramente - podemos consultar o Teorema 1.14., o exemplo após este teorema (não tem referência) e o exemplo 1.15.

Selecione uma boa notação - além das notações usadas no enunciado, usaremos as notações das ferramentas listadas no passo anterior, inclusive para representar a tabela de multiplicação em K.

Prove os resultados sobre a nossa questão - usando as ideias já consultadas podemos construir a tabela e encontrar a ordem de x. Mudando a ordem das tarefas podemos consultar a tabela de multiplicação para verificar que $f(x)$ é irredutível em $(\mathbb{Z}/(3))[x]$.

Esse problema visto fora do contexto do livro poderia ser considerado teórico já que auxilia no entendimento de corpos formados pelas classes de polinômios módulo um polinômio irredutível em certo corpo. Porém, vimos no passo "modifique o problema ligeiramente"que existem ferramentas no livro texto que direcionam a resolução desse

problema. Por isso a categoria desse problema é aplicação.

Problema 2.3. Determine as soluções de $\sigma(n) = 2801$.

Entenda o problema - é um problema do tipo "encontre tudo...".

Entenda os dados - temos a função σ que é a soma dos divisores e o número 2801 que é primo.

Entenda o objetivo - as soluções n são bem limitadas, pois a função σ é multiplicativa e 2801 é primo.

Modifique o problema ligeiramente - podemos consultar o exemplo 2.6. no qual prova-se que $\sigma(n) = 307 \iff n = 17^2$. Usando as mesmas ideias limitamos n a potências de primos.

Prove os resultados sobre a nossa questão - da equação $\sigma(p^k) = 2801$ nos restringimos a $p = 2, 5$ ou 7. Após testar esses valores encontramos a única solução da equação $n = 2401$.

Problema 3.1. Determine a fração contínua de $\sqrt{7}$. Mostre que ela é periódica a partir de um certo ponto, e determine o período.

Entenda o problema - é um problema do tipo "encontre ...". Apesar de falar de uma demonstração ela é consequência da primeira parte.

Entenda os dados - temos o número irracional $\sqrt{7}$.

Entenda o objetivo - encontrar a fração contínua de acordo com o algoritmo fornecido no texto.

Modifique o problema ligeiramente - aqui temos uma pequena separação desse problema em relação aos de aplicação anteriores, pois não conseguimos relacioná-lo diretamente com um exemplo ou outra ferramenta. Porém, basta usar a definição de fração contínua.

Prove os resultados sobre a nossa questão - após realizar os cálculos obtemos $\sqrt{7} = [2; 1, 1, 1, 4, 1, 1, 1, 4, \dots]$. É uma fração contínua de período 4.

5.3 PROBLEMAS DE OLIMPÍADA DE MATEMÁTICA INICIANTE

Problema 0.5. Dado um inteiro positivo n, definimos $T(n, 1) = n$ e, para todo $k \geq 1$, $T(n, k+1) = n^{T(n,k)}$. Prove que existe $c \in \mathbb{N}$ tal que, para todo inteiro $k \geq 1$, $T(2010, k) < T(2, k+c)$. Determine o menor inteiro positivo c com essa propriedade.

Entenda o problema - como o problema possui duas tarefas, ele é do tipo "mostre que ..."e também do tipo "encontre um ...".

Entenda os dados - temos inteiros positivos n e k e a função $T(n, k)$ definida.

Entenda o objetivo - devemos provar que mesmo $2 < 2010$ existe um c tal que $T(2, k+c) > T(2010, k)$.

Selecione uma boa notação - o enunciado já nos fornece uma boa notação.

Modifique o problema ligeiramente - podemos consultar outros problemas que usam desigualdades como o exemplo 0.4. e o problema 0.4. Porém, adaptações desses outros problemas não resolvem diretamente o problema, pois $T(2, k+c) > T(2010, k)$ não é suficiente para que $T(2, k+c+1) > T(2010, k+1)$. Essa necessidade de mais ferramentas deixa claro que não se trata de um problema de aplicação.

Prove os resultados sobre a nossa questão - alguns cálculos provam que $c = 2$ não funciona para $k = 1$ e que $c = 3$ funciona para $k = 1$.

Modifique o problema significativamente - para $n \geq 2$ tentaremos provar por indução que $T(2, n+3) > T(2010, n)^2$.

Simplifique, explore dados e alcance metas táticas - após o uso do PIF podemos concluir o problema, pois $T(2, n+3) > T(2010, n)^2 > T(2010, n)$.

Problema 0.15. Do conjunto $A = \{1, 2, \ldots, 99, 100\}$ escolhemos 51 números. Demonstrar que, entre os 51 números escolhidos, existem dois tais que um é múltiplo do outro.

Entenda o problema - este é um problema tipo "mostre que...".

Entenda os dados - temos o conjunto A dos números inteiros de 1 a 100 e todos os subconjuntos B de A com 51 elementos.

Entenda o objetivo - devemos provar que todo subconjunto B de acordo com os dados possui dois elementos tal que um divide o outro.

Modifique o problema ligeiramente - podemos consultar o exemplo 0.9. no qual prova-se que todo conjunto B nas mesmas condições possui dois elementos consecutivos. Uma consequência importante é que esses dois elementos são primos entre si. A ideia foi usar 50 subconjuntos e o princípio da casa dos pombos.

Selecione uma boa notação - nesse passo usaremos que todo número natural n pode ser escrito como $2^{\alpha} I$ com α e I inteiros não-negativos e I ímpar. Esta é uma ideia importante para problemas de olimpíada de matemática, mas a maioria das pessoas desconhece. Esse é um ponto importante para categorizar esse problema como de olimpíada iniciante.

Prove os resultados sobre a nossa questão - esse passo já permite a conclusão do problema, pois tendo 50 partes ímpares e 51 números temos, pelo PCP, que dois números possuem a mesma parte ímpar e um divide o outro.

Problema 0.80. [OIbM2001] Demonstre que para cada inteiro positivo n existe um inteiro m tal que 2^m tem no mínimo $\frac{2}{3}n - 1$ zeros entre seus últimos n algarismos em notação base 10.

Entenda o problema - este é um problema tipo "mostre que ...".

Entenda os dados - para esse problema só temos um inteiro positivo n.

Entenda o objetivo - precisamos demonstrar que alguma potência de 2 possui muitos zeros entre seus últimos n algarismos.

Selecione uma boa notação - o enunciado do problema já traz uma boa notação.

Modifique o problema ligeiramente - seria possível provar que uma potência de 2 possui os últimos $\frac{2}{3}n - 1$ algarismos iguais a zero? Não, pois teria que ser múltiplo de 10. Podemos procurar outras ideias como o exemplo 0.59. no qual demonstra-se que $2^{2000+\varphi(5^{2000})}$ possui 1333 zeros consecutivos em suas 2000 últimas casas.

Prove os resultados sobre a nossa questão -seguindo do passo anterior, basta fazer algumas contas.

Problema 4.56. Pode um triângulo retângulo com lados inteiros ter área que seja o quadrado de um inteiro?

Entenda o problema - este é um problema tipo "existe um...".

Entenda os dados - o que temos são medidas inteiras positivas que satisfazem o Teorema de Pitágoras.

Entenda o objetivo - a partir dos lados devemos verificar se o produto dos catetos dividido por dois é um quadrado perfeito.

Selecione uma boa notação - desejamos existem (a, b, c, k) inteiros positivos tais que $a^2 + b^2 = c^2$ e $k^2 = ab/2$.

Modifique o problema ligeiramente - sabemos que se $a^2 + b^2 = c^2$, então existem inteiros positivos d, m e n, com m e n primos entre si e de paridades distintas tais que $(a, b, c) = (d2mn, d(m^2 - n^2), d(m^2 + n^2))$.

Prove os resultados sobre a nossa questão - o problema se torna verificar se

$$k^2 = d2mn \cdot d(m^2 - n^2)/2 \Leftrightarrow k^2 = d^2mn(m^2 - n^2)$$

Implica que $d \mid k$ e usando $k_0 = k/d$ temos $k_0^2 = mn(m^2 - n^2)$.
O produto de números primos entre si é um quadrado perfeito se, e somente se, cada um é um quadrado perfeito. Dessa forma, devemos determinar se existem inteiros positivos x, y e z tais que $m = x^2$, $n = y^2$ e

$$m^2 - n^2 = z^2 \Leftrightarrow x^4 - y^4 = z^2$$

Modifique o problema ligeiramente - sabemos que a equação $x^4 + y^4 = z^2$ não possui soluções inteiras positivas (exemplo 4.40. do livro).

Simplifique, explore dados e alcance metas táticas - usando Descenso Infinito de Fermat prova-se que a equação $x^4 = y^4 + z^2$ não possui solução com x, y e z inteiros positivos. No caso deste problema a variação da resolução do exemplo 4.40. exige certo trabalho e a análise de casos. Por isso, esse problema não foi classificado como de aplicação.

Vale ressaltar que esse resultado foi muito importante também na resolução de outros problemas, como 4.58 e 4.63.

5.4 PROBLEMAS DE OLIMPÍADA DE MATEMÁTICA AVANÇADO

Problema 0.20. [IMO2001] Sejam $n_1, n_2, \ldots, n_m$ inteiros com m ímpar. Denotemos por $x = (x_1, \ldots, x_m)$ uma permutação dos inteiros $1, 2, \ldots, m$, e definamos

$f(x) = x_1 n_1 + \cdots + x_m n_m$. Demonstre que existem duas permutações a e b tais que $f(a) - f(b)$ é divisível por $m!$.

Entenda o problema - este é um problema tipo "mostre que ...".

Entenda os dados - temos um ímpar m, os números inteiros $n_1, n_2, \ldots, n_m$, todas as permutações dos números de 1 até m e a função f definida sobre essas permutações.

Entenda o objetivo - desejamos provar que existem duas permutações a e b tais que $m! \mid f(a) - f(b)$ ou de forma equivalente usando ferramentas vistas em seguida no livro que $f(a) \equiv f(b) \pmod{m!}$.

Selecione uma boa notação - o enunciado do problema já traz uma boa notação.

Modifique o problema ligeiramente - supondo que não existam permutações a e b tais que $m! \mid f(a) - f(b)$ implica que para quaisquer duas permutações a e b os números $f(a)$ e $f(b)$ possuem restos distintos na divisão por $m!$.

Modifique o problema significativamente - seguindo do passo anterior. Existem $m!$ restos possíveis na divisão por $m!$ e $m!$ números $f(x)$ com restos distintos. Isso implica que cada resto aparece exatamente uma vez como $f(x)$.

Simplifique, explore dados e alcance metas táticas - apesar de não ser um problema simples, podemos destacar que existe uma forma padrão de explorar os dados obtidos. Se dois conjuntos possuem os mesmos restos na divisão por $m!$ em alguma ordem, então podemos somar todos ou multiplicar todos para obter números com mesmo resto na divisão por $m!$. O que marca esse problema como olimpíada avançado é a dificuldade de trabalhar com a soma de todas as expressões de $f(x)$. Outro ponto importante na conclusão do problema que deve ser ressaltado é o dado de que m é ímpar.

Problema 0.77.[IMO1986] (OA) Seja d um número positivo distinto de 2, 5 e 13. Demonstre que é possível encontrar dois números diferentes a e b que pertençam ao

conjunto $\{2, 5, 13, d\}$ tais que $ab - 1$ não é um quadrado perfeito.

Entenda o problema - este é um problema tipo "mostre que...".

Entenda os dados - temos um inteiro positivo d e um conjunto $\{2, 5, 13, d\}$.

Entenda o objetivo - após notar que $2 \cdot 5 - 1$, $2 \cdot 13 - 1$ e $5 \cdot 13 - 1$ são quadrados perfeitos, precisamos provar que $2d - 1$, $5d - 1$ e $13d - 1$ não podem ser todos quadrados perfeitos.

Modifique o problema ligeiramente - vamos supor o contrário, que esses três números são quadrados perfeitos.

Selecione uma boa notação - uma boa notação para trabalhar nossa suposição é que $2d - 1 = x^2$, $5d - 1 = y^2$ e $13d - 1 = z^2$ onde x, y e z são inteiros positivos.

Prove os resultados sobre a nossa questão - se x é ímpar, então $x^2 \equiv 1 \pmod 8$. Esse fato é muito conhecido e útil em competições de matemática, embora não poucas pessoas conheçam em geral. Esse seria o passo essencial que cotegoriza esse problema como de olimpíada. Esse resultado nos permite concluir que $d \equiv 1 \pmod 4$. Com isso, y e z são pares.

Selecione uma boa notação - podemos usar $y = 2y_1$ e $z = 2z_1$, onde y_1 e z_1 são inteiros. Dessa forma, podemos inserir esses dados sobre paridade nas equações.

Simplifique, explore dados e alcance metas táticas - agora só precisamos trabalhar as equações para encontrar uma contradição. De fato, $8d = (13d - 1) - (5d - 1)$ que é equivalente a $2d = (z_1 - y_1)(z_1 + y_1)$. Estudando as paridades temos $2d$ ímpar ou múltiplo de 4 que entram em contradição com o fato de d ser ímpar.

Problema 1.35.[IMO2000] Existe um inteiro N divisível por exatamente 2000 primos diferentes e tal que N divide $2^N + 1$?

Entenda o problema - este é um problema tipo "existe um... ?".

Entenda os dados - a princípio só temos a quantidade de fatores primos: 2000.

Entenda o objetivo - a partir da experiência de vários problemas podemos conjecturar que o 2000 não é importante e podemos trocar por um k qualquer.

Modifique o problema ligeiramente - seguindo do passo anterior, vamos tentar generalizar o problema. Pra cada k inteiro positivo provaremos que existe um inteiro N_k com k divisores primos e tal que $N_k \mid 2^{N_k}+1$. Para isso precisamos de alguma manipulação que adicione fatores primos. Um dos fatos conhecidos em competições de matemática é que para $a \geq 8$ que a^3+1 possui um fator primo p com $p > 3$ e $p \nmid a+1$.

Simplifique, explore dados e alcance metas táticas - uma forma padrão de concluir é usar indução partindo de $N_1 = 3$ e $N_{k+1} = 3 \cdot N_k \cdot p_{k+1}$ onde p_{k+1} é um divisor de $2^{2N_k} - 2^{N_k} + 1$ que não divide $2^{N_k}+1$.

Problema 1.55.[IMO2008] Prove que existe um número infinito de inteiros positivos n tais que n^2+1 tem um divisor primo maior do que $2n+\sqrt{2n}$.

Entenda o problema - este é um problema tipo "mostre que...".

Entenda os dados - temos números da forma n^2+1.

Entenda o objetivo - devemos provar que para infinitos inteiros positivos n o número n^2+1 possui um divisor primo relativamente grande.

Modifique o problema ligeiramente - ao invés de considerar os números n^2+1, vamos considerar os primos p da forma $4k+1$, pois de $(\frac{-1}{p}) = 1$ exite x com $x < \frac{p}{2}$ tal que $p \mid x^2+1$. Vale ressaltar que mais uma vez temos um fato muito conhecido no universo de competições internacionais de matemática.

Simplifique, explore dados e alcance metas táticas - para concluir usamos algumas cotas, como $p > 13$ implicando $2x < p - 4$ e $x = \frac{p-t}{2} \iff p = 2x + t > 2x + \sqrt{2x}$.

5.5 PROBLEMAS TEÓRICOS

Problema 0.16. Dado um número irracional u, demonstrar que sempre é possível encontrar infinitos números racionais $\frac{p}{q}$, $p, q \in \mathbb{Z}$, de tal forma que

$$\left| u - \frac{p}{q} \right| < \frac{1}{q^2}.$$

Entenda o problema - este é um problema tipo "mostre que...".

Entenda os dados - temos um número irracional u.

Entenda o objetivo - devemos provar que existem infinitos racionais $\frac{p}{q}$ tais que a distância até u é menor que $\frac{1}{q^2}$.

Selecione uma boa notação - o enunciado já nos deu uma notação adequada até aqui.

Modifique o problema ligeiramente - podemos consultar o exemplo 0.12. no qual prova-se que para todo α real existem inteiros k e m tais que $|k\alpha - m| < \frac{1}{n}$.

Modifique o problema significativamente - podemos considerar que u pode ser racional, mas nesse caso podemos aproximar u por racionais de modo que $\left| u - \frac{p}{q} \right| = 0$. Nesse problema, isso não será útil para a resolução, mas deixa claro que esse dado é essencial.

Prove os resultados sobre a nossa questão - a partir das ideias do passo anterior prova-se que $\left| u - \frac{m}{k} \right| < \frac{1}{kn} < \frac{1}{k^2}$.

Simplifique, explore dados e alcance metas táticas - para concluir o problema devemos passar de existe um racional $\frac{m}{k}$ com a propriedade para existem infinitos racionais $\frac{m_i}{k_i}$. O passo essencial vem do fato de podermos escolher n_{j+1} de modo que $\frac{1}{n_{j+1}} < \left|u - \frac{m_j}{k_j}\right|$.

É importante ressaltar que além de ser um problema interessante, ele também apresenta um resultado muito útil na compreensão de números irracionais. Por exemplo, desse resultado fica claro que todo irracional u é limite de uma sequência de números racionais $\frac{m_i}{k_i}$.

Problema 1.50. Demonstre que, para $p = 1093$,

$$2^{\frac{p-1}{2}} \equiv -1 \pmod{p^2}$$

Entenda o problema - este é um problema tipo "mostre que...".

Entenda os dados - temos um primo $p = 1093$ grande.

Entenda o objetivo - pensando como um problema de olimpíada pode-se conjecturar que é uma propriedade que vale para todo primo, mas essa conjectura é falsa. Inclusive podemos encontrar contraexemplos.

Selecione uma boa notação - além da notação do problema usamos as ferramentas desse capítulo com ênfase no símbolo de Legendre.

Modifique o problema ligeiramente - esse passo não se mostrou útil nesse problema.

Prove os resultados sobre a nossa questão - a ideia é realmente fazer contas com congruências de potências de 2 módulo 1093.

Simplifique, explore dados e alcance metas táticas - após provar que $2^{p-1} \equiv 1 \pmod{p^2}$ basta usar a proposição 1.43. e o lema 1.47. para concluir o problema.

Observe que esse problema traz um resultado interessante de Teoria dos Números, mas ao modificá-lo ligeiramente não temos ferramentas desenvolvidas no livro texto nem resultados conhecidos de competições de matemática. Porém, a pergunta se existe algum primo com a propriedade mencionada faz sentido no contexto de pesquisa matemática.

Problema 2.33. Dados dois números reais α e β tais que $0 \leq \alpha < \beta \leq 1$, demonstre que existe um número natural m tal que

$$\alpha < \frac{\varphi(m)}{m} < \beta.$$

Entenda o problema - este é um problema tipo "mostre que...".

Entenda os dados - temos a razão $\frac{\varphi(m)}{m}$ que é o produto de fatores $\frac{p-1}{p}$ para p primo e um intervalo aberto (α, β) que pode ter coprimento $\beta - \alpha$ muito pequeno.

Entenda o objetivo - queremos provar que com a escolha adequada de primos o produto de fatores $\frac{p-1}{p}$ estará no intervalo (α, β) com extremos entre 0 e 1.

Observe que até para entender bem esse objetivo o leitor precisa de alguma experiência com problemas de ensino superior.

Modifique o problema ligeiramente - ao considerar $\prod_{p \text{ primo}} \frac{p-1}{p}$ conseguimos relacionar o problema como a série hamônica H_n. É conhecido que H_n tende para o infinito e isso implica que $\prod_{p \text{ primo}} \frac{p-1}{p} \to 0$.

Simplifique, explore dados e alcance metas táticas - para concluir o problema consideramos uma sequência $x_k = \prod_{i=0}^{k} \frac{p_{N+i}-1}{p_{N+i}}$ que começa próximo de 1 e vai decaindo lentamente tendendo para 0. O número N é grande o suficiente para que algum termo dessa sequência esteja necessariamente no intervalo (α, β).

Em outras palavras, nesse problema mostramos que o conjunto dos números $\frac{\varphi(m)}{m}$ com m inteiro positivo é denso em $[0, 1]$.

Problema 3.8. Prove que, para qualquer $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, e quaisquer $s, t \in \mathbb{R}$ com $s < t$, existem inteiros m, n com $n > 0$ tais que $s < n\alpha + m < t$.

Entenda o problema - este é mais um problema tipo "mostre que...".

Entenda os dados - temos um α irracional e um intervalo real (s, t).

Entenda o objetivo - queremos provar que qualquer intervalo real (s, t) possui um número da forma $n\alpha + m$. Em outras palavras, desejamos provar que o conjunto dos números $n\alpha + m$ é denso em $\mathbb{R}$.

Modifique o problema ligeiramente - sabemos que podemos aproximar α muito bem através das reduzidas da sua fração contínua. Além disso, no capítulo 0 vimos como aproximar $k\alpha$ para inteiros mais próximos. Adaptando esta ideia conseguimos provar essencialmente que $n\alpha$ é denso em $(0, 1)$.

Simplifique, explore dados e alcance metas táticas - para concluir basta tomar n tal que $s < n\alpha < s + t - s$ e $m = -\rfloor kq\alpha \lfloor + \rfloor s \lfloor$.

6

FUNDAMENTOS

0.1 PRINCÍPIO DA INDUÇÃO FINITA

Problema 0.1. *(A) Demonstrar por indução que para $n \geq 1$ natural*

(a) $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

(b) $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$.

(c) $(1^5 + 2^5 + \cdots + n^5) + (1^7 + 2^7 + \cdots + n^7) = 2(1 + 2 + \cdots + n)^4$.

(d) $\operatorname{sen} x + \operatorname{sen} 2x + \cdots + \operatorname{sen} nx = \dfrac{\operatorname{sen} \frac{(n+1)x}{2} \cdot \operatorname{sen} \frac{nx}{2}}{\operatorname{sen} \frac{x}{2}}$.

Solução

(a) Notemos que $1^2 = \frac{1(1+1)(2\cdot 1+1)}{6}$ donde a propriedade vale para $n = 1$ (base de indução). Suponha que a igualdade vale para $n = k$ (hipótese de indução):

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$$

Somando $(k+1)^2$ dos dois lados

$$\begin{aligned}1^2+2^2+\cdots+k^2+(k+1)^2 &= \frac{k(k+1)(2k+1)}{6}+(k+1)^2\\ &= (k+1)\left(\frac{2k^2+k}{6}+(k+1)\right)\\ &= (k+1)\left(\frac{2k^2+k+6k+6}{6}\right)\\ &= (k+1)\left(\frac{2k^2+7k+6}{6}\right)\\ &= \frac{(k+1)(k+2)(2k+3)}{6}\end{aligned}$$

Isso implica que a igualdade também vale para $n = k+1$. Pelo PIF, a igualdade vale para todo número natural $n \geq 1$.

(b) Primeiro, lembremos que $1+2+\cdots+n = \frac{n(n+1)}{2}$ para todo natural $n \geq 1$ e o problema é equivalente a provar que

$$1^3+2^3+\cdots+n^3 = \frac{n^2(n+1)^2}{4}$$

Veja que a propriedade é verdadeira para $n = 1$, pois $1^3 = \frac{1^2(1+1)^2}{4}$ (base de indução). Suponha que a propriedade é verdadeira para $n = k$ (hipótese de indução):

$$1^3+2^3+\cdots+k^3 = \frac{k^2(k+1)^2}{4}$$

Somando $(k+1)^3$ dos dois lados

$$\begin{aligned}1^3+2^3+\cdots+k^3+(k+1)^3 &= \frac{k^2(k+1)^2}{4}+(k+1)^3\\ &= (k+1)^2\left(\frac{k^2}{4}+(k+1)\right)\\ &= (k+1)^2\left(\frac{k^2+4k+4}{4}\right)\\ &= \frac{(k+1)^2(k+2)^2}{4}\end{aligned}$$

Isso implica que a igualdade também vale para $n = k+1$. Pelo PIF, a igualdade vale para todo número natural $n \geq 1$.

(c) Novamente, lembremos que $1+2+\cdots+n = \frac{n(n+1)}{2}$ para todo natural $n \geq 1$. Assim, o problema passa a ser provar que

$$(1^5+2^5+\cdots+n^5)+(1^7+2^7+\cdots+n^7) = 2\left(\frac{n(n+1)}{2}\right)^4 = \frac{n^4(n+1)^4}{8}$$

. A propriedade é verdadeira para $n = 1$, pois $1^5 + 1^7 = \frac{1^4(1+1)^4}{8}$ (base de indução). Suponha que vale para $n = k$ (hipótese de indução):

$$(1^5 + 2^5 + \cdots + k^5) + (1^7 + 2^7 + \cdots + k^7) = \frac{k^4(k+1)^4}{8}$$

Somando $(k+1)^5 + (k+1)^7$ dos dois lados

$$(1^5 + \cdots + (k+1)^5) + (1^7 + \cdots + (k+1)^7) = \frac{k^4(k+1)^4}{8} + (k+1)^5 + (k+1)^7$$

Desenvolvendo o lado direito:

$$\begin{aligned}
\frac{k^4(k+1)^4}{8} + (k+1)^5 + (k+1)^7 &= (k+1)^4\left(\frac{k^4}{8} + (k+1) + (k+1)^3\right) \\
&= (k+1)^4\left(\frac{k^4 + 8k + 8 + 8(k+1)^3}{8}\right) \\
&= (k+1)^4\left(\frac{k^4 + 8k + 8 + 8k^3 + 24k^2 + 24k + 8}{8}\right) \\
&= (k+1)^4\left(\frac{k^4 + 8k^3 + 24k^2 + 32k + 16}{8}\right) \\
&= (k+1)^4\left(\frac{k^4 + 4\cdot k^3\cdot 2 + 6\cdot k^2\cdot 2^2 + 4\cdot k\cdot 2^3 + 2^4}{8}\right) \\
&= \frac{(k+1)^4(k+2)^4}{8}
\end{aligned}$$

Isso implica que a igualdade também vale para $n = k+1$. Pelo PIF, a igualdade vale para todo número natural $n \geq 1$.

(d) A propriedade é verdadeira para $n = 1$, pois $\operatorname{sen} x = \frac{\operatorname{sen}\frac{(1+1)x}{2}\cdot\operatorname{sen}\frac{1\cdot x}{2}}{\operatorname{sen}\frac{x}{2}}$ (base de indução). Suponha que essa propriedade seja verdadeira para $n = k$ (hipótese de indução):

$$\operatorname{sen} x + \operatorname{sen} 2x + \cdots + \operatorname{sen} kx = \frac{\operatorname{sen}\frac{(k+1)x}{2}\cdot\operatorname{sen}\frac{kx}{2}}{\operatorname{sen}\frac{x}{2}}$$

Somando $\operatorname{sen}(k+1)x$ dos dois lados

$$\begin{aligned}
\operatorname{sen} x + \cdots + \operatorname{sen}(k+1)x &= \frac{\operatorname{sen}\frac{(k+1)x}{2}\cdot\operatorname{sen}\frac{kx}{2}}{\operatorname{sen}\frac{x}{2}} + \operatorname{sen}(k+1)x \\
&= \frac{\operatorname{sen}\frac{(k+1)x}{2}\cdot\operatorname{sen}\frac{kx}{2} + \operatorname{sen}(k+1)x\cdot\operatorname{sen}\frac{x}{2}}{\operatorname{sen}\frac{x}{2}} \\
&= \frac{cos(\frac{x}{2}) - cos(\frac{(2k+1)x}{2}) + cos(\frac{(2k+1)x}{2}) - cos(\frac{(2k+3)x}{2})}{2\operatorname{sen}\frac{x}{2}} \\
&= \frac{cos(\frac{x}{2}) - cos(\frac{(2k+3)x}{2})}{2\operatorname{sen}\frac{x}{2}} \\
&= \frac{\operatorname{sen}(\frac{(k+2)x}{2})\cdot\operatorname{sen}(\frac{(k+1)x}{2})}{\operatorname{sen}\frac{x}{2}}
\end{aligned}$$

Isso implica que a igualdade também vale para $n = k+1$. Pelo PIF, a igualdade vale para todo número natural $n \geq 1$.

No desenvolvimento das equações usamos a seguinte identidade trigonométrica

$$\operatorname{sen} a \cdot \operatorname{sen} b = \frac{cos(a-b) - cos(a+b)}{2}$$

Problema 0.2. *(A) Seja F_n o n-ésimo termo da sequência de Fibonacci. Demonstrar que para todo natural $n \geq 1$ temos*

(a) $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.

(b) $F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n$.

(c) $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$.

(d) $\binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \binom{n-3}{3} + \cdots = F_{n+1}$, *onde na soma interpretamos* $\binom{m}{k} = 0$ *se* $k > m$.

Solução

(a) A propriedade é verdadeira para $n = 1$, pois $F_1 = F_3 - 1$ (base de indução). Suponha que é verdadeira para $n = k$ (hipótese de indução):

$$F_1 + F_2 + \cdots + F_k = F_{k+2} - 1$$

Somando F_{k+1} dos dois lados e lembrando que $F_{k+1} + F_{k+2} = F_{k+3}$ temos

$$F_1 + F_2 + \cdots + F_k + F_{k+1} = F_{k+2} - 1 + F_{k+1} = F_{k+3} - 1$$

Isso implica que a igualdade também vale para $n = k+1$. Pelo PIF, a igualdade vale para todo número natural $n \geq 1$.

(b) Observemos que $F_2 \cdot F_0 - F_1^2 = 1 \cdot 0 - 1^2 = -1 = (-1)^1$ e a propriedade vale para $n = 1$. Suponha que a propriedade é verdadeira para $n = k$:

$$F_{k+1} \cdot F_{k-1} - F_k^2 = (-1)^k$$

Vamos desenvolver a expressão para $n = k+1$ lembrando que $F_{k+2} = F_{k+1} + F_k$ e $F_k = F_{k+1} - F_{k-1}$.

$$\begin{aligned} F_{k+2} \cdot F_k - F_{k+1}^2 &= (F_{k+1} + F_k)F_k - F_{k+1}^2 \\ &= F_{k+1}F_k + F_k^2 - F_{k+1}^2 \\ &= F_{k+1}(F_{k+1} - F_{k-1}) + F_k^2 - F_{k+1}^2 \\ &= F_{k+1}^2 - F_{k+1} \cdot F_{k-1} + F_k^2 - F_{k+1}^2 \\ &= -(F_{k+1} \cdot F_{k-1} - F_k^2) \\ &= -(-1)^k \\ &= (-1)^{k+1} \end{aligned}$$

Isso implica que a igualdade também vale para $n = k+1$. Pelo PIF, a igualdade vale para todo número natural $n \geq 1$.

(c) A propriedade vale para $n = 1$, pois $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^1 = \begin{pmatrix} F_2 & F_1 \\ F_1 & F_0 \end{pmatrix}$ (base de indução). Suponha que a igualdade vale para $n = k$ (hipótese de indução)

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix}$$

Para $n = k+1$ sabemos que para qualquer matriz A temos $A^{k+1} = A \cdot A^k$ e usando a hipótese de indução:

$$\begin{aligned} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{k+1} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} F_{k+1} + F_k & F_{k+1} \\ F_k + F_{k-1} & F_k \end{pmatrix} \\ &= \begin{pmatrix} F_{k+2} & F_{k+1} \\ F_{k+1} & F_k \end{pmatrix} \end{aligned}$$

Isso implica que a igualdade também vale para $n = k+1$. Pelo PIF, a igualdade vale para todo número natural $n \geq 1$.

(d) Para esse problema a base de indução deve ser formada por dois casos, pois usaremos dois valores no passo indutivo.
Para $n = 1$ temos $\binom{1}{0} = 1 = F_2$ e para $n = 2$ temos $\binom{2}{0} + \binom{1}{1} = 2 = F_3$. Então nossa

base com dois valores está provada.

Suponha que a propriedade é verdadeira para $n = k-1$ e para $n = k$, ou seja,

$$\binom{k-1}{0} + \binom{k-2}{1} + \binom{k-3}{2} + \binom{k-4}{3} + \cdots = F_k$$

e

$$\binom{k}{0} + \binom{k-1}{1} + \binom{k-2}{2} + \binom{k-3}{3} + \cdots = F_{k+1}$$

Somando os termos da sequência de Fibonacci, $F_k + F_{k+1} = F_{k+2}$. Somaremos os dois somatórios lembrando que $\binom{k}{0} = 1 = \binom{k+1}{0}$ e agrupando as parcelas que possuem o mesmo número na parte de cima do binomial. Isso nos permite usar a seguinte identidade de binomiais

$$\binom{n-1}{m} + \binom{n-1}{m-1} = \binom{n}{m}$$

Assim, temos

$$\begin{aligned} F_{k+2} &= \binom{k-1}{0} + \binom{k-2}{1} + \cdots + \binom{k}{0} + \binom{k-1}{1} + \binom{k-2}{2} + \cdots \\ &= \binom{k}{0} + \left(\binom{k-1}{0} + \binom{k-1}{1}\right) + \left(\binom{k-2}{1} + \binom{k-2}{2}\right) + \cdots \\ &= \binom{k+1}{0} + \binom{k}{1} + \binom{k-1}{2} + \cdots \end{aligned}$$

Isso implica que a igualdade também vale para $n = k+1$. Pelo PIF, a igualdade vale para todo número natural $n \geq 1$.

Comentário: existem outras formas de demonstração essa igualdade. Por exemplo, pode-se argumentar que para $n \geq 2$ os dois lados da igualdade contam o número de subconjuntos do conjunto $\{1, 2, \cdots, n-1\}$ sem números consecutivos.

Problema 0.3. *(A) Demonstrar que*

(a) $n^3 - n$ *é um múltiplo de* 6 *para todo natural* n.

(b) $5^n - 1$ *é múltiplo de* 24 *para todo número natural* n *par.*

(c) $2^n + 1$ *é múltiplo de* 3 *para todo natural ímpar* n.

Solução

(a) Observemos que para $n = 0$ temos $0^3 - 0 = 0$ que é múltiplo de 6. Suponha que $k^3 - k$ é múltiplo de 6. Vamos desenvolver a expressão para $k+1$:

$$(k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - k - 1 = k^3 - k + 3k(k+1)$$

Por hipótese, $k^3 - k$ é múltiplo de 6. Um dos números k ou $k+1$ é par, então $k(k+1)$ é múltiplo de 2 e, portanto, $3k(k+1)$ é múltiplo de 6. A soma de dois múltiplos de 6 é também múltiplo de 6. Assim, pelo PIF concluímos que $n^3 - n$ é múltiplo de 6 para todo natural n.

(b) Como a propriedade vale apenas para n par, podemos fazer indução de k para $k+2$ ou podemos considerar $n = 2m$ e fazer indução no m. Aqui usaremos a segunda opção. Para $m = 0$ temos $5^{2\cdot 0} - 1 = 0$ que é múltiplo de 24. Supoha que vale para $m = k$, ou seja, que $5^{2k} - 1$ é divisível por 24. Para $m = k+1$ temos

$$5^{2(k+1)} - 1 = 5^{2k+2} - 1 = 5^{2k} \cdot 5^2 - 1 = 24 \cdot 5^{2k} + 5^{2k} - 1$$

O número da primeira parcela é múltiplo de 24, pois é 24 vezes um inteiro, e o número que resta é múltiplo de 24 por hipótese. Logo o resultado é um múltiplo de 24.

Assim, para todo natural m o número $5^{2m} - 1$ é múltiplo de 24. Em outras palavras, para todo natural n par temos que $5^n - 1$ é múltiplo de 24.

(c) Como no item anterior podemos adotar duas abordagens: indução de k para $k+2$ ou escrever $n = 2m+1$ e fazer indução em m. Dessa vez usaremos a primeira abordadem.

Para $n = 1$ temos $2^1 + 1 = 3$ que é múltiplo de 3. Suponha que o número $2^k + 1$ é múltiplo de 3 para k ímpar. O próximo número ímpar é $k+2$ e temos

$$2^{k+2} + 1 = 2^k \cdot 2^2 + 1 = 3 \cdot 2^k + 2^k + 1$$

O número $3 \cdot 2^k$ é múltiplo de 3, pois tem o fator 3, e o número $2^k + 1$ é múltiplo de 3 por hipótese. Concluímos que $2^n + 1$ é múltiplo de 3 para todo natural n ímpar.

Comentário: nesse tipo de problema é muito importante observar a base de indução, pois o passo indutivo funcionaria também para k par, já que vai de k para $k+2$, porém é impossível encontrar algum número n_0 par tal que $2^{n_0} + 1$ seja múltiplo de 3.

Problema 0.4. *(A) Mostre que para todo natural $n \geq 4$*

(a) $2^n < n!$.

(b) $2n^3 > 3n^2 + 3n + 1$.

Solução

(a) A inequação é verdadeira para $n = 4$, pois $2^4 = 16 < 4! = 24$ (base de indução). Suponha que vale para $n = k$, ou seja, $2^k < k!$ para algum $k \geq 4$. Para $n = k+1 \geq 5$ temos

$$2^{k+1} = 2^k \cdot 2 < k! \cdot 5 \leq k! \cdot (k+1) = (k+1)!$$

Logo, por PIF, temos $2^n < n!$ para todo natural $n \geq 4$.

(b) Dividindo os dois lados por n^3 temos

$$2n^3 > 3n^2 + 3n + 1 \Leftrightarrow 2 > \frac{3}{n} + \frac{3}{n^2} + \frac{1}{n^3}$$

Provaremos esta última inequação por indução. Para $n = 4$ temos

$$\frac{3}{4} + \frac{3}{4^2} + \frac{1}{4^3} = \frac{3 \cdot 4^2 + 3 \cdot 4 + 1}{4^3} = \frac{61}{64} < 2$$

Suponha que a inequação é verdadeira para $n = k$, ou seja,

$$2 > \frac{3}{k} + \frac{3}{k^2} + \frac{1}{k^3}.$$

Para $n = k+1$ sabemos que $\frac{1}{k} > \frac{1}{k+1}$, $\frac{1}{k^2} > \frac{1}{(k+1)^2}$ e $\frac{1}{k^3} > \frac{1}{(k+1)^3}$ que implica

$$2 > \frac{3}{k} + \frac{3}{k^2} + \frac{1}{k^3} > \frac{3}{k+1} + \frac{3}{(k+1)^2} + \frac{1}{(k+1)^3}$$

Logo a desigualdade vale para todo natural $n \geq 4$ por PIF.

Problema 0.5. *(OI) Dado um inteiro positivo n, definimos $T(n,1) = n$ e, para todo $k \geq 1$, $T(n,k+1) = n^{T(n,k)}$. Prove que existe $c \in \mathbb{N}$ tal que, para todo inteiro $k \geq 1$, $T(2010,k) < T(2,k+c)$. Determine o menor inteiro positivo c com essa propriedade.*

Solução

Começamos vendo que $c = 2$ não funciona para $k = 1$:

$$T(2010,1) = 2010 > T(2,3) = 2^{2^2} = 2^4 = 16$$

Vamos provar que o menor inteiro é $c = 3$. Para $k = 1$ temos

$$T(2010,1) = 2010 < T(2,4) = 2^{T(2,3)} = 2^{16} = 65536$$

Para $n \geq 2$ provaremos por indução que $T(2,n+3) > T(2010,n)^2$. Para $n = 2$ temos

$$T(2010,2)^2 = 2010^{2 \cdot 2010} < (2^{11})^{2 \cdot 2010} = 2^{22 \cdot 2010} = 2^{44220}$$

e

$$T(2,5) = 2^{T(2,4)} = 2^{65536} > 2^{44220} > T(2010,2)^2$$

Suponha que vale para $n = k$, ou seja, que $T(2, k+3) > T(2010, k)^2$. Para $n = k+1$ temos

$$T(2010, k+1)^2 = 2010^{2 \cdot T(2010,k)} < 2^{22 \cdot T(2010,k)} < 2^{T(2010,k)^2} < 2^{T(2,k+3)} = T(2, k+4)$$

Nas passagens usamos que $2010 < 2^{11} = 2048$ e que $22 < T(2010, k)$ já que $T(2010, k)$ é no mínimo 2010.
Logo, por PIF, para todo natural $n \geq 2$ temos $T(2, n+3) > T(2010, n)^2 > T(2010, n)$.

Comentário: neste problema foi necessário provar um resultado mais forte para que a indução funcionasse, pois $T(2010, k) < T(2, k+3)$ não é suficiente para provar que $T(2010, k+1) < T(2, k+4)$.

Problema 0.6. *(A) Mostre que para quaisquer n e k inteiros positivos temos*

$$\binom{n}{n} + \binom{n+1}{n} + \binom{n+2}{n} + \cdots + \binom{n+k}{n} = \binom{n+k+1}{n+1}.$$

Solução

Provaremos por indução que para todo natural k vale essa igualdade para todo inteiro positivo n. A igualdade vale para $k = 0$, pois $\binom{n}{n} = 1 = \binom{n+1}{n+1}$ (base de indução). Suponha que vale para $k = m$ (hipótese de indução), ou seja,

$$\binom{n}{n} + \binom{n+1}{n} + \binom{n+2}{n} + \cdots + \binom{n+m}{n} = \binom{n+m+1}{n+1}.$$

Somando $\binom{n+m+1}{n}$ dos dois lados temos

$$\binom{n}{n} + \cdots + \binom{n+m+1}{n} = \binom{n+m+1}{n+1} + \binom{n+m+1}{n} = \binom{n+m+2}{n+1}$$

Veja que na última passagem usamos a igualdade de binomiais $\binom{x-1}{y} + \binom{x-1}{y-1} = \binom{x}{y}$ para quaisquer x e y inteiros positivos. Logo, pelo PIF, a igualdade vale para quaisquer n e k inteiros positivos.

Problema 0.7. *(A) Demonstre a fórmula do* binômio de Newton *para n natural:*

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n.$$

Solução

Para $n = 0$ temos $(x+y)^0 = 1 = \binom{0}{0}x^0y^0$. Suponha que o binômio de Newton é verdadeiro para $n = k$, ou seja,

$$(x+y)^k = \binom{k}{0}x^k + \binom{k}{1}x^{k-1}y + \cdots + \binom{k}{k-1}xy^{k-1} + \binom{k}{k}y^k$$

Multiplicando os dois lados por $x+y$ temos

$$(x+y)^{k+1} = (x+y)\left(\binom{k}{0}x^k + \binom{k}{1}x^{k-1}y + \cdots + \binom{k}{k-1}xy^{k-1} + \binom{k}{k}y^k\right)$$

Haverá apenas uma parcela com x^{k+1}: $x\binom{k}{0}x^k = \binom{k+1}{0}x^{k+1}$. E o mesmo acontece para y^{k+1}. As demais parcelas $x^t y^{k+1-t}$ aparecem em pares que somados

$$x\binom{k}{t-1}x^{t-1}y^{k+1-t} + y\binom{k}{t}x^t y^{k-t}$$

$$= \left(\binom{k}{t-1} + \binom{k}{t}\right)x^t y^{k+1-t} = \binom{k+1}{t}x^t y^{k+1-t}$$

Dessa forma, temos

$$(x+y)^{k+1} = \binom{k+1}{0}x^{k+1} + \binom{k+1}{1}x^k y^1 + \cdots + \binom{k+1}{k}x^1 y^k + \binom{k+1}{k+1}y^{k+1}$$

e o binômio de Newton vale para todo n natural.

Problema 0.8. *(A) Encontrar com demonstração uma expressão para o multinômio*

$$(x_1 + x_2 + \cdots + x_k)^n$$

em termos dos coeficientes multinomiais

$$\binom{n}{i_1, \ldots, i_k} \stackrel{\text{def}}{=} \frac{n!}{i_1! \cdots i_k!}$$

onde $i_1 + \cdots + i_k = n$.

Solução

Provaremos por indução em n que

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{i_1+i_2+\cdots+i_k=n} \binom{n}{i_1, i_2, \ldots, i_k} x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k}$$

Primeiro faremos a base de indução. Para $n = 0$ temos $(x_1 + x_2 + \cdots + x_k)^0 = 1 = \binom{0}{0,\ldots,0}x_1^0 \cdots x_k^0$. Suponha que é verdade para $n = m$, ou seja,

$$(x_1 + x_2 + \cdots + x_k)^m = \sum_{i_1+i_2+\cdots+i_k=m} \binom{m}{i_1, i_2, \ldots, i_k} x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k}$$

Podemos multiplicar os dois lados dessa equação por $(x_1 + x_2 + \cdots + x_k)$. De um lado teremos $(x_1 + x_2 + \cdots + x_k)^{m+1}$. Do outro teremos cada x_i multiplicando termos cuja soma dos expoentes era m. Podemos concluir as somas dos expoentes dos resultados serão todas $m+1$. Para certa soma $i_1 + i_2 + \cdots + i_k = m+1$ vejamos o coeficiente de $x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k}$.

Essas parcelas vem de $x_t x_1^{i_1} \cdots x_t^{i_t-1} \cdots x_k^{i_k}$ que contribuem com $\binom{m}{i_1,\ldots,i_t-1,\ldots,i_k}$. Portanto o coeficiente de $x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k}$ é

$$\binom{m}{i_1-1, i_2 \ldots, i_k} + \binom{m}{i_1, i_2-1 \ldots, i_k} + \ldots + \binom{m}{i_1, i_2 \ldots, i_k-1}$$

Multiplicando o numerador e o denominador da primeira parcela por i_1, os da segunda parcela por i_2 e assim por diante até o da última parcela por i_k teremos

$$\frac{m!\, i_1 + m!\, i_2 + \cdots + m!\, i_k}{i_1! \cdots i_k!} = \frac{((m+1)!\,)}{i_1! \cdots i_k!} = \binom{m+1}{i_1, \ldots, i_k}$$

Então, por PIF, concluímos que a igualdade vale para todo natural n.

Problema 0.9. *(OI) Considere n retas em posição geral em um plano, isto é, sem que haja duas retas paralelas ou três retas concorrentes em um mesmo ponto.*

(a) Determine (em função de n) o número de regiões em que as retas dividem o plano.

(b) Demonstre que é possível colorir essas regiões com duas cores sem que duas regiões vizinhas tenham a mesma cor (duas regiões são vizinhas se elas possuem um segmento de reta em comum).

Solução

(a) Chamaremos de r_n o número de regiões formadas por n retas. Podemos verificar os valores iniciais de r_n: $r_1 = 2$, $r_2 = 4$ e $r_3 = 7$. Provaremos por indução que $r_n = 1 + \frac{n(n+1)}{2}$.

A base da indução já está feito nos valores iniciais. Suponha que quaisquer k retas em posição geral dividem o plano em $r_k = 1 + \frac{k(k+1)}{2}$ regiões. Considere um conjunto de $k+1$ retas. Escolha uma das retas s e ignore essa reta por enquanto. Então as outras k retas dividem o plano em r_k regiões. Agora vamos analisar a influência da reta s. Como as retas estão em posição geral a reta s intersecta cada uma das k outras retas em k pontos distintos dois a dois. Esses pontos formam 2 semirretas e $k-1$ segmentos de reta. Então existem $2+k-1 = k+1$ regiões formadas pelas k retas que são particionadas pela reta s em duas regiões. Isso resulta em um saldo de mais $k+1$ regiões. Portanto, o número de regiões formadas pelas $k+1$ retas é

$$r_{k+1} = r_k + k + 1 = 1 + \frac{k(k+1)}{2} + \frac{2(k+1)}{2} = 1 + \frac{(k+1)(k+2)}{2}$$

Isso conclui nossa demonstração por indução.

(b) Vamos usar as cores preto e branco. Para $n = 1$ temos duas regiões e colorimos uma de preto e a outra de branco. Suponha que para qualquer conjunto de k retas é possível colorir as regiões de modo que regiões vizinhas tenham cores distintas. Considere um conjunto qualquer de $k+1$ retas. Escolha uma das retas s e a ignore por enquanto. As regiões formadas pelas outras k retas podem ser coloridas por hipótese de indução. Agora volte a considerar a reta s. A reta s divide o plano em dois semiplanos. Em todas as regiões de um semiplano mantenha a coloração usada para k retas e em todas as regiões do outro semiplano inverta as cores, ou seja, se a região estava colorida de preto troque para branco e vice-versa. Assim, as regiões vizinhas que tem lado comum sobre s terão cores distintas, uma foi mantida e a outra invertida, e as regiões vizinhas que tem lado comum sobre outras retas possuem cores distintas por hipótese de indução. Dessa forma, é possível colorir todas as regiões com duas cores sem que duas regiões vizinhas tenham a mesma cor.

Problema 0.10. *(OI) Demonstrar que para cada número natural n existe um número natural M satisfazendo simultaneamente as seguintes duas condições:*

(i) M possui n dígitos pertencentes ao conjunto $\{1,2\}$.

(ii) M é divisível por 2^n.

Solução

Para cada $n \geq 1$ mostraremos que existe um número M_n com as propriedades listadas. Para $n = 1$ tomamos $M_1 = 2$ (base de indução). Suponha que para $n = k$ temos um M_k formado por k dígitos do conjunto $\{1,2\}$ que seja divisível por 2^k. Considere os seguintes dois números com $k+1$ dígitos $A = 10^k + M_k$ e $B = 2 \cdot 10^k + M_k$. Já que M_k é divisível por 2^k sabemos que $M_k = 2^k \cdot t$ para algum inteiro t. Se t for ímpar tome $M_{k+1} = A = 2^k(5^k + t)$ que é divísvel por 2^{k+1}, pois $5^k + t$ é par. Por outro lado, se t for par tome $M_{k+1} = B = 2^k(2 \cdot 5^k + t)$ que é divísvel por 2^{k+1}, pois $2 \cdot 5^k + t$ é par. Portanto, a partir de M_k sempre podemos construir o M_{k+1} com $k+1$ dígitos do conjunto $\{1,2\}$ que seja divisível por 2^{k+1}. Por PIF, fica provado que existe M_n para todo natural $n \geq 1$.

Problema 0.11 (IMO1987)**.** *(OA) Mostre que não existe uma função $f\colon \mathbb{N} \to \mathbb{N}$ tal que $f(f(n)) = n + 1987$ para todo $n \in \mathbb{N}$.*

Solução

Vamos resolver esse problema por contradição. Suponha que existe uma função que satisfaz essa condição. Veja que

$$f(f(f(n))) = f(n+1987) = f(n) + 1987$$

Então, por indução podemos provar que para quaisquer naturais n e m vale a equação $f(n+1987m) = f(n) + 1987m$. A base já está feita e para o passo de indução

$$f(n+1987(k+1)) = f(n+1987k+1987) = f(n+1987k) + 1987 = f(n) + 1987k + 1987$$

Dessa forma, para determinar o $f(n)$ para todo n basta determinar $f(r)$ para $r \in \{0, 1, \cdots, 1986\}$. Tome $f(r) = 1987k + s$ onde k e s são inteiros tais que $k \geq 0$ e $0 \leq s < 1987$. Temos

$$f(f(r)) = r + 1987 = f(1987k + s) = f(s) + 1987k$$

Veja que $1987k \leq f(s) + 1987k = 1987 + r < 1987 \cdot 2$ implicando $k = 0$ ou $k = 1$. Se $k = 0$ então $f(r) = s$ e $f(s) = r + 1987$. Se $k = 1$ então $f(r) = s + 1987$ e $f(s) = r$. Nos dois casos podemos concluir que $r \neq s$, pois caso fossem iguais teríamos $r = r + 1987$ que é uma contradição. Assim, o conjunto $R = \{0, 1, \cdots, 1986\}$ dos restos na divisão por 1987 é particionado em pares $\{x, y\}$ tais que

$$f(x) = y \text{ e } f(y) = x + 1987$$

Porém, $|R| = 1987$ é ímpar e é impossível particionar o conjunto em pares de elementos. Como chegamos em uma contradição, podemos concluir que a suposição inicial é falsa e que não existe uma função f satisfazendo essa condição.

0.2 PRINCÍPIO DA CASA DOS POMBOS

Problema 0.12. *(A) Escolhem-se 7 pontos no interior de um retângulo de dimensões* 2×3*. Demonstrar que sempre é possível encontrar dois pontos tal que sua distância é menor ou igual a* $\sqrt{2}$*.*

Solução

Divida o retângulo em 6 quadrados 1×1. Essas serão nossas "gavetas". Como escolhemos 7 pontos, pelo PCP existem dois pontos no mesmo quadrado 1×1. A distância entre esses dois pontos é menor ou igual a diagonal desse quadrado que mede $\sqrt{2}$.

Vamos provar esse fato sobre o quadrado. Considere dos pontos X e Y no interior ou no bordo de um quadrado $ABCD$ de lado 1. Suponha que a reta XY intersecta os lados do quadrado nos pontos Z e W. Temos $XY \leq ZW$. Se Z e W estão em lados consecutivos do quadrado, por exemplo AB e BC, temos $ZW = \sqrt{BZ^2 + BW^2} \leq \sqrt{BA^2 + BC^2} = \sqrt{2}$. Se Z e W estão em lados opostos do quadrado trace a perpendicular ZT por Z ao lado que contém W. Temos $ZW = \sqrt{ZT^2 + TW^2} \leq \sqrt{1^2 + 1^2} = \sqrt{2}$.

Problema 0.13. *(A) Escolhem-se 9 pontos no interior de um quadrado de lado* 1*. Demonstrar que é possível escolher 3 deles de tal forma que a área do triângulo que formam é menor ou igual a* $\frac{1}{8}$.

Solução

Divida o quadrado em 4 quadrados menores de lado $\frac{1}{2}$. Como são $9 = 4 \times 2 + 1$ pontos podemos afirmar que há 3 pontos em um desses quadrados. Provaremos que a maior área possível que esse triângulo pode ter é $\frac{1}{8}$.

Sejam X, Y e Z três pontos no interior do quadrado de lado $\frac{1}{2}$. A reta YZ intersecta o quadrado nos pontos R e S. Temos $[XYZ] \leq [XRS]$. Suponha que a reta XR intersecta o quadrado novamente no ponto $T \neq R$. Temos $[XYZ] \leq [XRS] \leq [TRS]$ e os vértices desse triângulo estão no bordo do quadrado. Temos dois casos para tratar.

(i) Se dois vértices estão sobre um mesmo lado do quadrado. Suponha que sejam R e S sobre um lado e que h_T é a altura de T relativa a esse lado. Temos $[TRS] = \frac{RS \cdot h_T}{2} \leq \frac{1/2 \cdot 1/2}{2} = \frac{1}{8}$.

(ii) Se não há dois vértices sobre um mesmo lado do quadrado. Seja $ABCD$ o quadrado de lado $\frac{1}{2}$. Suponha sem perda de generalidade que T, R e S estão sobre os lados AB, BC e CD, respectivamente. Trace por R uma reta paralela à reta TS. Ela corta o lado AB ou o lado CD num ponto R'. Pode cortar ambos se a reta TS for paralela ao lado BC, mas nesse caso R' pode ser qualquer dos pontos de interseção. Veja que $[TRS] = [TR'S]$, pois podemos calculá-las usando a mesma base TS e a mesma altura relativa a essa base já que a reta RR' é paralela à reta TS. Mas o triângulo $TR'S$ se encaixa no caso anterior e já provamos que sua área é no máximo $\frac{1}{8}$.

Problema 0.14. *(A) Dadas 6 pessoas numa festa, demonstrar que necessariamente existem 3 pessoas que se conhecem mutuamente ou 3 pessoas que não se conhecem mutuamente. Suponha que a relação de conhecer é simétrica. Este é um caso particular do teorema de Ramsey, veja por exemplo [17].*

Solução

Considere uma pessoa A entre as 6 pessoas. Essa pessoa tem $5 = 2 \times 2 + 1$ relações com as outras pessoas. Pelo PCP pelo menos três dessas relações são conhece ou pelo menos três são de não conhece. Suponha sem perda de generalidade que A conhece três ou mais pessoas. Separemos um conjunto de três pessoas entre as pessoas que A conhece $\{B, C, D\}$. Se duas pessoas desse conjunto se conhecem, então junto com A formam um conjunto de três pessoas que se conhecem mutuamente. Por exemplo, B conhece C então A, B e C são 3 pessoas que se conhecem mutuamente. Por outro lado, se não existirem duas pessoas desse conjunto que se conhecem, então B, C e D são 3 pessoas que não se conhecem mutuamente.

Vale notar que com 5 pessoas é possível que não existam 3 que conhecem mutuamente nem 3 que não se conhecem mutuamente. Para provarmos basta dar um contraexemplo. Imagine 5 pessoas ao redor de uma mesa redonda em que cada pessoa conhece seus 2 vizinhos da esquerda e da direita e não conhece as outras 2 pessoas. Assim, para quaisquer 3 pessoas dessas 5 haverá duas que se conhecem e duas que não se conhecem.

Problema 0.15. *(OI) Do conjunto $A = \{1, 2, \ldots, 99, 100\}$ escolhemos 51 números. Demonstrar que, entre os 51 números escolhidos, existem dois tais que um é múltiplo do outro.*

Solução

Cada número inteiro positivo n pode ser escrito de maneira única como $2^{\alpha} \cdot I$ com α e I inteiros não-negativos e I ímpar. Chamaremos I de parte ímpar de n.

Para provar isto basta dividir n por 2 até obter um resultado ímpar. Nesse caso I será esse resultado e α será o número de divisões. Por exemplo, $13 = 2^0 \cdot 13$ e $20 = 2^2 \cdot 5$. Vejamos a unicidade. Suponha que $2^{\alpha_1} \cdot I_1 = 2^{\alpha_2} \cdot I_2$. Se $\alpha_1 > \alpha_2$ teríamos $2^{\alpha_1 - \alpha_2} \cdot I_1 = I_2$ implicando I_2 par que é uma contradição. Analogamente não podemos ter $\alpha_1 < \alpha_2$. Portanto, $\alpha_1 = \alpha_2$ e após cancelar as potências de 2 temos $I_1 = I_2$.

Podemos particionar os números do conjunto A de acordo com suas partes ímpares. Essas serão nossas "gavetas". Como existem 50 partes ímpares possíveis (ímpares de 1 até 99) e escolhemos 51 números, pelo PCP dois números $a > b$ possuem a mesma parte ímpar. Nesse caso, $\frac{a}{b} = 2^{x-y}$ é inteiro e a é múltiplo de b.

Veja que se escolhermos apenas 50 números, então é possível que não existam dois tal que um é múltiplo de outro. Tome por exemplo $\{51, 52, ..., 100\}$. Para quaisquer dois números a e b desse conjunto com $a > b$ temos $\frac{a}{b}$ não pode ser inteiro, pois $1 < \frac{a}{b} \leq \frac{100}{51} < 2$.

Problema 0.16. *(T) Dado um número irracional u, demonstrar que sempre é possível encontrar infinitos números racionais $\frac{p}{q}$, $p, q \in \mathbb{Z}$, de tal forma que*

$$\left| u - \frac{p}{q} \right| < \frac{1}{q^2}.$$

Solução

Nesse problema usaremos a mesma ideia usada no exemplo 0.12. Assim provaremos que existem inteiros n, k e m tais que $0 < k < n$ e $|ku - m| < \frac{1}{n}$. Seja n um inteiro com $n \geq 2$. Considere os números $\{ku\}$ para $k = 1, 2, \ldots, n$. Particione o intervalo $[0, 1)$ em n partes de tamanho $\frac{1}{n}$:

$$[0,1) = \left[0, \frac{1}{n}\right) \cup \left[\frac{1}{n}, \frac{2}{n}\right) \cup \left[\frac{2}{n}, \frac{3}{n}\right) \cup \cdots \left[\frac{n-1}{n}, 1\right)$$

Se $\{ku\} \in [0, \frac{1}{n})$ ou $\{ku\} \in [\frac{n-1}{n}, 1)$ para algum $k = 1, \ldots, n-1$, então temos os inteiros procurados. Caso contrário, pelo PCP haverá duas partes fracionárias $\{ju\}$ e $\{ku\}$ com $1 \leq j < k \leq n-1$ pertencentes a um mesmo intervalinho dentre os $n-2$ restantes. Sendo $x = (k-j)u$, teremos

$$\{x\} = \begin{cases} \{ku\} - \{ju\} & \text{se } \{ku\} \geq \{ju\} \\ 1 + \{ku\} - \{ju\} & \text{se } \{ku\} < \{ju\} \end{cases}$$

e portanto $\{x\} \in [0, \frac{1}{n})$ ou $\{x\} \in [\frac{n-1}{n}, 1)$, assim $k - j$ satisfaz as condições desejadas. Nesse caso também provamos que os inteiros n, k e m existem.

Veja agora que

$$|ku - m| < \frac{1}{n} \Rightarrow \left| u - \frac{m}{k} \right| < \frac{1}{kn} < \frac{1}{k^2}$$

Isso prova que existe um racional. Para provar que existem infinitos usaremos uma sequência. Para $n_1 = 2$ podemos encontram k_1 e m_1 tal que

$$\left| u - \frac{m_1}{k_1} \right| < \frac{1}{k_1 n_1} < \frac{1}{k_1^2}$$

Tome n_2 tal que $\frac{1}{n_2} < \left| u - \frac{m_1}{k_1} \right|$. Usando a estratégia acima encontraremos k_2 e m_2 de modo que

$$\left| u - \frac{m_2}{k_2} \right| < \frac{1}{k_2 n_2} < \frac{1}{k_2^2}$$

E temos

$$\left| u - \frac{m_2}{k_2} \right| < \frac{1}{k_2 n_2} \leq \frac{1}{n_2} < \left| u - \frac{m_1}{k_1} \right|$$

Nossa construção gera racionais cada vez mais próximos de u e, portanto, distintos dois a dois.

Problema 0.17 (IMO1985). *(OA) Dado um conjunto M com 1985 inteiros positivos distintos, nenhum dos quais tem divisores primos maiores do que 23, mostre que há 4 elementos em M cujo produto é uma quarta potência.*

Solução

De 1 até 23 existem 9 fatores primos. Então cada um dos inteiros positivos pode ser escrito como $p_1^{x_1} p_2^{x_2} \cdots p_9^{x_9}$ com x_i inteiro não-negativo. Considerando que cada x_i é par ou ímpar temos $2^9 = 512$ possibilidades de paridades para os expoentes. Se considerarmos 513 entre os 1985 números, então pelo PCP existem dois números a e b com exatamente as mesmas paridades nos primos. Daí o produto $a \cdot b$ terá expoente par em todos os primos, ou seja, podemos escrever $a \cdot b = p_1^{2y_1} p_2^{2y_2} \cdots p_9^{2y_9}$.
Podemos separar a e b e repetir o processo com os $1983 > 513$ números restantes. Assim, podemos formar $\frac{1983-513}{2} = 736$ pares de números e ainda um a mais com os 513 números que sobraram. Como temos $736 + 1 = 737$ pares e $737 > 512$ podemos usar o PCP para afirmar que existem dois pares com mesma paridades do y_i. Suponha que os pares $\{a, b\}$ e $\{c, d\}$ possuem essa propriedade, ou seja, $a \cdot b = p_1^{2y_1} p_2^{2y_2} \cdots p_9^{2y_9}$, $c \cdot d = p_1^{2z_1} p_2^{2z_2} \cdots p_9^{2z_9}$ e $y_i + z_i$ é par para cada p_i. Concluímos que o produto dos quatro números do conjunto $\{a, b, c, d\}$ é uma quarta potência, pois

$$abcd = p_1^{2(y_1+z_1)} p_2^{2(y_2+z_2)} \cdots p_9^{2(y_9+z_9)}.$$

Problema 0.18 (OIbM1998). *(OA) Determinar o mínimo valor de n para o qual, de todo subconjunto de $\{1, 2, \ldots, 999\}$ com n elementos, é possível selecionar quatro inteiros diferentes a, b, c, d tais que $a + 2b + 3c = d$.*

Solução

A resposta é 835. Lembrando que este tipo de problema possui duas partes: um exemplo com 834 elementos no qual não é possível selecionar os quatro inteiros e provar que em qualquer subconjunto com 835 elementos é possível selecionar os quatro inteiros.
Para a primeira parte tome o conjunto $\{166, 167, 168, \ldots, 999\}$ com $999 - 166 + 1 = 834$ elementos. Veja que $a + 2b + 3c \geq 168 + 2 \cdot 167 + 3 \cdot 166 = 1000 > 999 \geq d$ e não é possível selecionar quatro inteiros tais que $a + 2b + 3c = d$.
Para a segunda parte considere um conjunto qualquer com 835 elementos $1 \leq a_1 < a_2 < a_3 < \cdots < a_{835} \leq 999$. Veja que $a_1 \leq 165$, pois de 166 até 999 há apenas 834 elementos. Analogamente, $a_2 \leq 166$. Defina $D = 2a_2 + 3a_1$. Veja que $D \leq 827 \Rightarrow 999 - D \geq 172$. Faremos casos em relação aos possíveis valores de D. Agora considere os seguintes números formados usando a_1: $3a_1 + a_3$, $3a_1 + a_4$, $\ldots$, $3a_1 + a_{835}$. E considere os seguintes números formados usando a_2: $a_3 - 2a_2$, $a_4 - 2a_2$, $\ldots$ e $a_{835} - 2a_2$. O maior valor

possível para esses números é $3a_1 + a_{835} \leq 3 \cdot 165 + 999 = 1494$ e o menor valor possível é $a_3 - 2a_2 \geq a_2 + 1 - 2a_2 = 1 - a_2 \geq -165$. Então temos $2 \cdot 833 = 1666$ números, esses serão nossos pombos, que vão de -165 até 1494, essas serão as casas de pombos. São $1494 - (-165) + 1 = 1660$ valores distintos então pelo princípio da casa dos pombos algum valor será repetido. Os números formados usando a_1 são distintos entre si e o mesmo acontece com os números formados usando a_2. Assim, existem a_i e a_j tal que $3a_1 + a_i = a_j - 2a_2$. Note que $i \neq j$, pois $3a_1 > 0 > -2a_2$. Então encontramos uma solução $a_j = a_i + 2a_2 + 3a_1$.

Problema 0.19. *(OI) Demonstre que de qualquer conjunto de $2^{n+1} - 1$ números inteiros positivos é possível escolher 2^n elementos de tal forma que sua soma é divisível por 2^n.*

Solução

Vamos fazer por indução em n. Para $n = 0$ em um conjunto com $2^{0+1} - 1 = 1$ número podemos achar $2^0 = 1$ número que seja divisível por 1. Para o passo de indução suponha que a propriedade é verdadeira para $n = k$, ou seja, para qualquer conjunto de $2^{k+1} - 1$ temos 2^k elementos cuja soma é divisível por 2^k. Para $n = k + 1$ considere um conjunto qualquer com $2^{k+2} - 1$ elementos. Tome $2^{k+1} - 1$ elementos e, pela hipótese de indução, existem 2^k cuja soma é divisível por 2^k. Separe esses 2^k números num conjunto A. Restam $2^{k+2} - 1 - 2^k > 2^{k+1} - 1$ números. Podemos usar a hipótese novamente e encontrar outros 2^k números cuja soma é divisível por 2^k. Separemos esses 2^k números num segundo conjunto B. Restam ainda $2^{k+2} - 1 - 2 \cdot 2^k = 2^{k+1} - 1$ e podemos usar a hipótese pela terceira vez e encontrar o conjunto C com 2^k elementos e soma dos elementos divisível por 2^k. Sejam $2^k \cdot a$, $2^k \cdot b$ e $2^k \cdot c$ as somas dos elementos dos conjuntos A, B e C, respectivamente. Pelo PCP dois dos números do conjunto $\{a, b, c\}$ possuem mesma paridade. Suponha sem perda de generalidade que são a e b. Então temos $a + b$ par, $2^k(a + b)$ é divisível por 2^{k+1} e o conjunto $A \cup B$ possui $2^k + 2^k = 2^{k+1}$ elementos cuja soma é divisível por 2^{k+1}.

Problema 0.20 (IMO2001)**.** *(OA) Sejam $n_1, n_2, \ldots, n_m$ inteiros com m ímpar. Denotemos por $x = (x_1, \ldots, x_m)$ uma permutação dos inteiros $1, 2, \ldots, m$, e definamos $f(x) = x_1 n_1 + \cdots + x_m n_m$. Demonstre que existem duas permutações a e b tais que $f(a) - f(b)$ é divisível por $m!$.*

Solução

Existem $m!$ permutações e, portanto, $m!$ valores de $f(x)$. Existem $m!$ restos possíveis na divisão de $f(x)$ por $m!$. Se algum dos restos não aparece entre os $f(x)$, então temos $m!$ números e $m! - 1$ restos. Pelo PCP duas permutações a e b deixariam o mesmo resto por

$m!$ e $f(a) - f(b)$ seria divisível por $m!$. Então devemos analisar a outra possibilidade, ou seja, se $f(x)$ cobre todos os restos na divisão por $m!$. Como as quantidades de $f(x)$ e de restos são iguais, cada resto aparece exatamente uma vez. Nesse caso, vamos somar $f(x)$ sobre todas as permutações de duas formas. A primeira forma observando os restos.

$$\sum_x f(x) = m!\,a_0 + 0 + m!\,a_1 + 1 + \ldots + m!\,a_{m!-1} + (m! - 1) = m!\,k + \frac{(m! - 1)m!}{2}$$

Como m é ímpar, podemos concluir que esse valor não é múltiplo de $m!$.
Mas também podemos calcular usando a fórmula de $f(x)$. Veja que $x_1 = 1$ para $(m-1)!$ permutações, $x_1 = 2$ para $(m-1)!$ permutações e assim por diante. Chamando $N = n_1 + n_2 + \ldots + n_m$ podemos desenvolver o somatório

$$\sum_x f(x) = n_1(1 + 2 + \cdots + m)(m-1)! + \ldots + n_m(1 + 2 + \cdots + m)(m-1)!$$

$$= N \cdot \frac{m(m+1)}{2}(m-1)! = m! \cdot N \cdot \frac{m+1}{2}$$

Nesse caso, o mesmo valor visto anteriormente é múltiplo $m!$. Isso implica uma contradição. Então é impossível que todos restos na divisão por $m!$ apareceram entre os $f(x)$.

Problema 0.21 (IMO1991)**.** *(OA) Seja $S = \{1, 2, \ldots, 280\}$. Encontre o menor inteiro n para o qual todo subconjunto de S com n elementos contém cinco números que são dois a dois primos entre si.*

Solução

Provaremos que $n = 217$. Primeiro vamos mostrar um exemplo com 216 tais que qualquer conjunto de cinco números tem dois que não são primos entre si. Para isso considere todos os números que são múltiplos de 2, 3, 5 ou 7. Podemos contar essa quantidade usando o princípio da Inclusão-Exclusão

$$|M_2 \cup M_3 \cup M_5 \cup M_7| = |M_2| + |M_3| + |M_5| + |M_7|$$

$$- |M_6| - |M_{10}| - |M_{14}| - |M_{15}| - |M_{21}| - |M_{35}|$$

$$+ |M_{30}| + |M_{42}| + |M_{70}| + |M_{105}| - |M_{210}|$$

$$= 140 + 93 + 56 + 40 - 46 - 28 - 20 - 18 - 13 - 8$$

$$+9 + 6 + 4 + 2 - 1 = 216$$

Tomando quaisquer cinco números dessa união pelo menos dois estarão no mesmo conjunto M_2, M_3, M_5 ou M_7, pelo PCP, e estes dois terão um fator primo em comum.

Agora provaremos que para qualquer subconjunto A de S com 217 números existem 5 que são dois a dois primos entre si. Veja que o conjunto das uniões dos múltiplos de 2, 3, 5 e 7 possui 4 números primos e 212 compostos. Fora dele existem 8 números compostos em S: 11^2, $11 \cdot 13$, $11 \cdot 17$, $11 \cdot 19$, $11 \cdot 23$, 13^2, $13 \cdot 17$, $13 \cdot 19$. Se usarmos apenas primos maiores ou iguais a 17 o menor número composto é $17^2 = 289 > 280$. Assim, S é composto por 220 números compostos, um número 1 e 59 primos. Se dos 60 últimos números tomarmos 5 números então temos 5 números primos entre si dois a dois. Então resta analisar quando A tem no máximo 4 elementos entre esses e pelo menos 213 números compostos. No total S possui 220 números compostos e no máximo 7 números compostos de S não estão em A. Tome os seguintes 8 conjuntos de 5 números compostos de S.

$$X_1 = \{2 \cdot 2, 3 \cdot 3, 5 \cdot 5, 7 \cdot 7, 13 \cdot 13\}$$
$$X_2 = \{2 \cdot 23, 3 \cdot 19, 5 \cdot 17, 7 \cdot 13, 11 \cdot 11\}$$
$$X_3 = \{2 \cdot 29, 3 \cdot 23, 5 \cdot 19, 7 \cdot 17, 11 \cdot 13\}$$
$$X_4 = \{2 \cdot 31, 3 \cdot 29, 5 \cdot 23, 7 \cdot 19, 11 \cdot 17\}$$
$$X_5 = \{2 \cdot 37, 3 \cdot 31, 5 \cdot 29, 7 \cdot 23, 11 \cdot 19\}$$
$$X_6 = \{2 \cdot 41, 3 \cdot 37, 5 \cdot 31, 7 \cdot 29, 11 \cdot 23\}$$
$$X_7 = \{2 \cdot 43, 3 \cdot 41, 5 \cdot 37, 7 \cdot 31, 13 \cdot 17\}$$
$$X_8 = \{2 \cdot 47, 3 \cdot 43, 5 \cdot 41, 7 \cdot 37, 13 \cdot 19\}$$

Como existem no máximo 7 números compostos que não estão em A temos $X_i \subset A$ para algum i entre 1 e 8 e esse conjuntos é formado por 5 números dois a dois primos entre si.
Os conjuntos usados na segunda parte da solução foram consultados em [14].
Concluímos que para qualquer conjunto com 217 elementos de S possui cinco números dois a dois primos entre si.

Problema 0.22 (Erdős)**.** *(OA) Mostre que toda a sequência com $n^2 + 1$ números reais contém ou uma subsequência crescente com $n + 1$ termos ou uma subsequência decrescente com $n + 1$ termos.*

Solução

Sejam $x_1, x_2, \ldots, x_{n^2+1}$ os temos da sequência. Para cada x_i definimos y_i como o número máximo de termos de uma subsequência crescente começando com x_i. Se existe $y_i \geq n + 1$ então conseguimos uma subsequência crescente com $n + 1$ termos. Suponha

que não existe, ou seja, para todo i temos $1 \leq y_i \leq n$. Como são n^2+1 termos podemos afirmar que algum dos valores de 1 até n aparece pelo menos $\left\lceil \frac{n^2+1}{n} \right\rceil = n+1$ vezes. Considere os $n+1$ termos x_i que possuem os mesmos y_i em ordem crescente de índices $x_{a_1}, x_{a_2}, \ldots, x_{a_{n+1}}$ com $y_{a_1} = y_{a_2} = \cdots = y_{a_{n+1}}$. Note que $x_{a_k} > x_{a_{k+1}}$, pois caso contrário poderíamos construir uma subsequência começada por x_{a_k} que incluísse $x_{a_{k+1}}$ e, consequentemente, y_{a_k} teria que ser maior que $y_{a_{k+1}}$ mas nessa subsequência os y_i são iguais. Logo $x_{a_1} > x_{a_2} > \cdots > x_{a_{n+1}}$ formando uma subsequência decrescente com $n+1$ termos.

Problema 0.23. *(OI) Pintamos todos os pontos do plano de azul, verde ou preto. Mostre que existe no plano um retângulo cujos vértices têm todos a mesma cor.*

Solução

Considere quatro pontos em uma mesma reta vertical. Pelo PCP existem dois deles pintados da mesma cor. Agora considere $3^4 + 1 = 82$ colunas de quatro pontos tais que os primeiros pontos de cada linha estão numa mesma reta horizontal, os segundos estão numa horizontal, assim como os terceiros e os quartos. Por exemplo, no plano cartesiano podemos tomar os pontos (x, y) tais que $0 \leq x \leq 81$ e $0 \leq y \leq 3$. Existem $3^4 = 81$ maneiras de pintar cada quatro pontos em coluna. Tendo 82 colunas temos duas colunas com a mesma coloração pelo PCP. Mas como vimos antes essas colunas possuem dois pontos da mesma cor. Então tomando os dois pontos da mesma cor na primeira coluna e os correspondentes dois pontos da mesma cor na segunda coluna temos um retângulo com todos os vértices da mesma cor.

0.3 DIVISIBILIDADE

0.4 MDC, MMC E ALGORITMO DE EUCLIDES

0.5 O TEOREMA FUNDAMENTAL DA ARITMÉTICA

Problema 0.24 (IMO1959)**.** *(A) Mostre que a fração $\frac{21n+4}{14n+3}$ é irredutível para todo n natural.*

Solução

Basta calcular o *mdc* do numerador e do denominador. Temos

$$\begin{aligned}\text{mdc}(21n+4, 14n+3) &= \text{mdc}((21n+4)-(14n+3), 14n+3)\\ &= \text{mdc}(7n+1, 14n+3)\\ &= \text{mdc}(7n+1, 14n+3-2(7n+1))\\ &= \text{mdc}(7n+1, 1)\\ &= 1.\end{aligned}$$

Problema 0.25. *(A) Encontre todos os inteiros positivos tais que*

(a) $n+1 \mid n^3-1$

(b) $2n-1 \mid n^3+1$

(c) $\frac{1}{n}+\frac{1}{m}=\frac{1}{143}$

(d) $2n^3+5 \mid n^4+n+1$

Solução

(a) Para todo inteiro n temos $n+1 \mid n^3+1=(n+1)(n^2-n+1)$. Logo $n+1 \mid n^3-1 = n^3+1-2 \iff n+1 \mid 2$ e o único inteiro positivo que satisfaz essa equação é $n=1$.

(b) Para todo inteiro n temos $2n-1 \mid 8n^3-1=(2n)^3-1^3=(2n-1)((2n)^2+2n+1)$. Assim $2n-1 \mid n^3+1 \implies 2n-1 \mid 8n^3+8=8n^3-1+9 \implies 2n-1 \mid 9$. Temos $2n-1=1$, 3 ou 9 e $n=1$, 2 ou 5. Testando esses valores vemos que os três são soluções. É importante testar, pois um ou mais passos foi implicação ($\implies$) que não era equivalência ($\iff$). Isso limita as possibilidades, mas não é equivalente à propriedade original. Em outras palavras, todos os valores da condição inicial aparecem na condição final, mas para saber quais realmente funcionam precisamos testas.

(c) A equação dada é equivalente a $\frac{m+n}{mn}=\frac{1}{143} \iff 143m+143n=mn \iff mn-143m-143n+143^2=143^2 \iff (m-143)(n-143)=143^2$. Considerando a fatoração em primos $143^2=11^2\cdot 13^2$ e que $n-143>-143$ temos

$$n-143=-11^2,-13,-11,-1,1,11,13,11^2,11\cdot 13,13^2,11^2\cdot 13,11\cdot 13^2 \text{ ou } 11^2\cdot 13^2.$$

E o conjunto solução de n nos inteiros positivos é

$$\{22,130,312,142,144,154,156,264,286,312,1716,2002,20592\}$$

(d) Temos que $2n^3+5 \mid 2n^4+5n$ e $2n^3+5 \mid n^4+n+1 \implies 2n^3+5 \mid 2n^4+2n+2 = 2n^4+5n-3n+2$. Isso implica $2n^3+5 \mid 3n-2$. Podemos usar a limitação $|2n^3+5| \leq |3n-2|$. Como n é inteiro positivo temos $n \geq 1$, $3n-2 \geq 1$ e $2n^3+5 \geq 7$. Logo $2n^3+5 \leq 3n-2 \iff 2n^3-3n+7 \leq 0 \iff n(2n^2-3)+7 \leq 0$. Para $n \geq 2$ temos $2n^2-3 > 0$ e $n(2n^2-3)+7 > 0$. Para $n = 1$ temos $2 \cdot 1^3 - 3 \cdot 1 + 7 = 6 > 0$. Portanto, nenhum inteiro positivo satisfaz essa divisibilidade.

Problema 0.26. *(A) Demonstre:*

(a) se $m \mid a-b$, então $m \mid a^k - b^k$ para todo natural k.

(b) se $f(x)$ é um polinômio com coeficientes inteiros e a e b são inteiros quaisquer, então $a-b \mid f(a)-f(b)$.

(c) se k é um natural ímpar, então $a+b \mid a^k+b^k$.

Solução

(a) Primeiro, veja que para $k = 0$ temos $m \mid a^0 - b^0 = 1 - 1 = 0$. Para $k \geq 1$ provaremos por indução em k que

$$a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + b^{k-1})$$

Para $k = 1$ temos $a^1 - b^1 = (a-b)(a^0b^0)$. Suponha que a equação é verdadeira para $k = k_0$. Veja que

$$\begin{aligned} a^{k_0+1} - b^{k_0+1} &= a^{k_0+1} - ab^{k_0} + ab^{k_0} - b^{k_0+1} \\ &= a(a_0^k - b^{k_0}) + b^{k_0}(a-b) \\ &= (a-b)(a^{k_0-1} + a^{k_0-2}b + a^{k_0-3}b^2 + \cdots + b^{k_0-1} + b^{k_0}) \end{aligned}$$

A partir disso é imediato que $a-b \mid a^k - b^k$ para todo natural k e se $m \mid a-b$ então $m \mid a^k - b^k$.

(b) Como $f(x)$ é um polinômio com coeficientes inteiros existem inteiros c_0, c_1, $\ldots$, c_{n-1} e c_n tais que

$$f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0.$$

Com isso, $f(a) - f(b) = c_n(a^n - b^n) + \cdots + c_1(a-b)$. Pela resolução do item anterior temos $a-b \mid c_i(a^i - b^i)$ para todo $i = 1, 2, \ldots, n$ e pela propriedade "d divide" concluímos que $a-b$ divide a soma dessas parcelas, ou seja, $a-b \mid f(a)-f(b)$.

(c) Veja que $a-b \mid a^k - b^k$ para quaisquer inteiros a e b e qualquer natural k. Tomando $a = A$, $b = -B$ e k ímpar temos $A-(-B) \mid A^k - (-B)^k \implies A+B \mid A^k + B^k$, pois para k ímpar $(-B)^k = -B^k$.

Problema 0.27. *(A) Mostre que*

(a) $2^{15}-1$ *e* $2^{10}+1$ *são primos entre si.*

(b) $2^{32}+1$ *e* 2^4+1 *são primos entre si.*

Solução

(a) Seja $d = \text{mdc}(2^{15}-1, 2^{10}+1)$. Veja que $d \mid 2^{15}-1 \implies d \mid 2^{30}-1 = (2^{15}-1)(2^{15}+1)$ e $d \mid 2^{10}+1 \implies d \mid 2^{30}+1 = (2^{10}+1)(2^{20}-2^{10}+1)$. Com isso $d \mid (2^{30}+1)-(2^{30}-1) = 2 \implies d = 1$ ou $d = 2$. Como $2^{10}+1$ é ímpar $d \neq 2$ e concluímos que $d = 1$. Logo, $2^{15}-1$ e $2^{10}+1$ são primos entre si.

(b) Seja $d = \text{mdc}(2^{32}+1, 2^4+1)$. Veja que $d \mid 2^4+1 \implies d \mid 2^{32}-1 = (2^{16}+1)(2^8+1)(2^4+1)(2^4-1)$. Adicionando a isto que $d \mid 2^{32}+1$ temos que d divide a diferença que é 2. Novamente, 2^4+1 é ímpar implicando $d \neq 2$. Logo, $\text{mdc}(2^{32}+1, 2^4+1) = 1$ e eles são primos entre si.

Problema 0.28. *(OI) Demonstre que* $(n-1)^2 \mid n^k - 1$ *se, e somente se,* $n-1 \mid k$.

Solução

Primeiro note que

$$\frac{n^k-1}{(n-1)^2} = \frac{n^{k-1}+n^{k-2}+\cdots+n+1}{n-1}$$

Assim,

$$(n-1)^2 \mid n^k-1 \iff n-1 \mid n^{k-1}+n^{k-2}+\cdots+n+1 = (n^{k-1}-1)+(n^{k-2}-1)+\ldots(n-1)+(1-1)+k.$$

Porém, sabemos que $n-1 | n^t - 1^t$ para todo t natural e com isso,

$$n-1 \mid (n^{k-1}-1)+(n^{k-2}-1)+\ldots(n-1)+(1-1)+k \iff n-1 \mid k.$$

Na maioria dos problemas com "se, e somente se," recomenda-se fazer dois passos: supondo a primeira condição para provar a segunda e supondo a segunda para provar a primeira. Isso pode ser feito nesse problema também, mas não foi necessário nessa solução, porque conseguimos conectar as duas condições com equivalências ($\iff$).

Problema 0.29 (IMO1992). *(OA) Encontre todos os inteiros a, b, c com $1 < a < b < c$ tais que $(a-1)(b-1)(c-1)$ é divisor de $abc - 1$.*

Mostre primeiro que $a \leq 4$ e considerar os possíveis casos.

Solução

Sejam $x = a - 1$, $y = b - 1$ e $z = c - 1$. Como $1 < a < b < c$ temos $0 < x < y < z$. A divisibilidade que temos que resolver é

$$xyz \mid (x+1)(y+1)(z+1) - 1 = xyz + xy + yz + zx + x + y + z.$$

Lembrando que $xyz \mid xyz$ temos $xyz \mid xy + yz + zx + x + y + z$. Se $x \geq 3$ então $xyz \geq 3yz = yz + yz + yz \geq yz + (x+1)z + (x+1)(y+1) = yz + xz + xy + x + y + z + 1$ que contraria a propriedade da limitação na divisibilidade anterior. Logo $x = 1$ ou $x = 2$. Faremos os casos

(i) Se $x = 1$ então $yz \mid yz + 2y + 2z + 1 \iff yz \mid 2y + 2z + 1$. Se $y \geq 4$ temos $yz \geq 4z = 2z + 2z \geq 2z + 2(y+1) = 2z + 2y + 2 > 2y + 2z + 1$ que contraria a propriedade da limitação. Então $y \leq 3 \implies y = 2$ ou $y = 3$. Se $y = 2$ a divisibilidade é $2z \mid 2z + 5 \implies 2z \mid 5$ que é falso. Se $y = 3$ a divisibilidade é $3z \mid 2z + 7 \implies z \mid 7 \implies z = 7$, pois $z > y > x$, e chegamos na solução $(x, y, z) = (1, 3, 7) \implies (a, b, c) = (2, 4, 8)$.

(ii) Se $x = 2$ então $2yz \mid yz + 3y + 3z + 2 \implies yz \mid 3y + 3z + 2$. Da mesma forma que fizemos no caso anterior, se $y \geq 6$ temos $yz \geq 6z \geq 3z + 3y + 3$. Logo $3 \leq y \leq 5 \implies y = 3, 4$ ou 5.
Se $y = 3$ temos $6z \mid 6z + 11 \implies 2 \mid 11$ que é falso.
Se $y = 4$ temos $8z \mid 7z + 14 \implies z \mid 14$ e temos $z = 7$ ou $z = 14$, pois $z > y = 4$.
Se $z = 7$ teremos que $8 \cdot 7 \mid 7 \cdot 7 + 14 \implies 56 \mid 63$ que é falso. Se $z = 14$ temos a solução $(x, y, z) = (2, 4, 14) \implies (a, b, c) = (3, 5, 15)$.
Se $y = 5$ então $10z \mid 8z + 17 \implies 2 \mid 17$ que é falso.

Concluímos que as únicas soluções possíveis são $(a, b, c) = (2, 4, 8)$ ou $(a, b, c) = (3, 5, 15)$. Essas duas soluções funcionam na divisibilidade, pois $1 \cdot 3 \cdot 7 = 21 \mid 2 \cdot 4 \cdot 8 - 1 = 63$ e $2 \cdot 4 \cdot 14 = 112 \mid 3 \cdot 5 \cdot 15 - 1 = 224$.
Novamente, devemos lembrar de testar na divisibilidade original, pois em alguns passos usamos $\implies$ e não apenas $\iff$.

Problema 0.30 (IMO1998). *(OA) Determine todos os pares de inteiros positivos (a, b) tais que $ab^2 + b + 7$ divide $a^2b + a + b$.*

Mostre que $ab^2+b+7 \mid 7a-b^2$ e considerar três casos: $7a-b^2$ maior, menor ou igual a zero.

Solução

Veja que $ab^2+b+7 \mid (a^2b+a+b)b = a^2b^2+ab+b^2$ e $ab^2+b+7 \mid (ab^2+b+7)a = a^2b^2+ab+7a$. Fazendo a diferença temos $ab^2+b+7 \mid 7a-b^2 \implies |ab^2+b+7| \leq |7a-b^2|$. Faremos três casos em relação ao sinal de $7a-b^2$.

(i) Se $7a-b^2=0$ então $7 \mid b \implies b=7k$ e $a=7k^2$ para qualquer inteiro positivo k. Testando $ab^2+b+7 = 7^3k^4+7k+7$ teria que ser um divisor de $a^2b+a+b = 7^3k^5+7k^2+7k = k(7^3k^4+7k+7)$. Então temos essa família de soluções $(a,b)=(7k^2,7k)$ para todo inteiro positivo k.

(ii) Se $7a-b^2<0$ então $|7a-b^2| = b^2-7a$ e $ab^2+b+7 \leq b^2-7a < ab^2$ que é falso. Então não temos solução nesse caso.

(iii) Se $7a-b^2>0$ então $|7a-b^2| = 7a-b^2$ e $ab^2+b+7 \leq 7a-b^2 < 7a \implies b^2 < 7 \implies b=1$ ou $b=2$.
Se $b=1$ então $a+8 \mid a^2+a+1 \iff a+8 \mid a^2-8^2+a+8+8^2-8+1 \iff a+8 \mid 57$. Os únicos divisores de 57 maiores que 8 são $a+8=19 \iff a=11$ e $a+8=57 \iff a=49$. Temos as soluções $(a,b)=(11,1)$ ou $(a,b)=(49,1)$. Observe que essas soluções já foram geradas por equivalência da divisibilidade original.
Se $b=2$ teremos $4a+9 \mid 2a^2+a+2 \implies 4a+9 \mid 4a^2+2a+4$. Como $4a+9 \mid 4a^2+9a$ temos $4a+9 \mid 7a-4$. Veja que $4a+9 \mid 7(4a+9)-4(7a-4)=79$ que não possui solução, pois 79 é primo e $4a+9$ não pode ser 1 nem 79.

Concluímos que as soluções são $(a,b)=(11,1)$, $(49,1)$ ou $(7k^2,7k)$ para um inteiro positivo k qualquer.

Problema 0.31. *(A) Mostre que, se $n>1$, então*

$$\sum_{k=1}^{n} \frac{1}{k} = 1+\frac{1}{2}+\cdots+\frac{1}{n}$$

não é um número inteiro.

Solução

Suponha que $H_n = 1+\frac{1}{2}+\cdots+\frac{1}{n}$ seja inteiro. Seja t o inteiro tal que $2^t \leq n < 2^{t+1}$ e M o mínimo múltiplo comum dos números de 1 até n. Para $n>1$ temos $t \geq 1$. Note que $2^t \mid M$ e $2^{t+1} \nmid M$, pois como M é o mmc ele tem a menor quantidade de fatores 2

possível que seja maior que ou igual à quantidade de fatores 2 de cada número de 1 a n. Multiplicando a equação de H_n por M temos

$$M \cdot H_n = M + \frac{M}{2} + \cdots + \frac{M}{2^t} + \cdots + \frac{M}{n}$$

Veja que se H_n é inteiro então $M \cdot H_n$ é par. No outro lado da equação temos a soma de n inteiros sendo $\frac{M}{2^t}$ ímpar e os demais pares já que M tem exatamente t fatores 2 e o único número de 1 a n com t fatores 2 é 2^t. Isso implica um número par igual a um número ímpar que é uma contradição.
Concluímos que a suposição inicial estava falsa e H_n não é inteiro.

Problema 0.32 (OBM1997). *(OA) Sejam $c \in \mathbb{Q}$, $f(x) = x^2 + c$. Definimos*

$$f^0(x) = x, \quad f^{n+1}(x) = f(f^n(x)), \forall n \in \mathbb{N}.$$

Dizemos que $x \in \mathbb{R}$ é pré-periódico se $\{f^n(x), n \in \mathbb{N}\}$ é finito. Mostre que o conjunto $\{x \in \mathbb{Q} |\, x$ é pré-periódico$\}$ é finito.

Solução
Se $|x| > |c|+1$ então

$$x^2 = |x|^2 > |x|(|c|+1) = |x||c|+|x| > (|c|+1)|c|+|x| = c^2+|c|+|x| \implies x^2+c > |x|+c^2+(|c|+c) > |x|.$$

Isso implica $|f(x)| > |x| > |c|+1$. Daí $|f^n(x)| > |f^{n-1}(x)| > \cdots > |f(x)| > |x|$ e x não é pré-periódico. Concluímos que se r é pré-periódico então $-(|c|+1) \leq r \leq |c|+1$.
Agora usaremos que os números são racionais. Veja que se x e c são racionais então $f(x)$ também é. Podemos escrever $c = \frac{a}{b}$, $x = \frac{p}{q}$ e $f(x) = \frac{u}{v}$ sendo as frações irredutíveis com denominadores positivos. Se alguma das frações for negativa o sinal vai para o numerador. Temos

$$\frac{u}{v} = \left(\frac{p}{q}\right)^2 + \frac{a}{b} \iff uq^2b = vp^2b + vq^2a \iff q^2(ub - va) = p^2vb$$

Logo $q^2 \mid p^2vb$ e $mdc(p,q) = 1$ implicando $q^2 \mid vb \implies q^2 \leq vb$.
Se $q > b$ então $vb \geq q^2 > qb \implies v > q > b$. Então se o denominador de x é maior que o denominador de c então o denominador de $f(x)$ é maior que o denominador de x e segue sendo maior que c. Como os denominadores crescem a cada aplicação de f temos que x não é pré-periódico. Com isso, os racionais pré periódicos estão no intervalo $[-|c|-1, |c|+1]$ e possuem denominador menor que ou igual ao denominador de c. Como os racioanis que satisfazem essas duas condições são finitos podemos concluir que $\{x \in \mathbb{Q} |\, x$ é pré-periódico$\}$ é finito.

Problema 0.33. *(A) Demonstre que se* $\text{mdc}(a, 2^{n+1}) = 2^n$ *e* $\text{mdc}(b, 2^{n+1}) = 2^n$*, então* $\text{mdc}(a+b, 2^{n+1}) = 2^{n+1}$.

Solução

A partir de $\text{mdc}(a, 2^{n+1}) = 2^n$ e $\text{mdc}(b, 2^{n+1}) = 2^n$ podemos concluir que existem inteiros ímpares a_0 e b_0 tais que $a = 2^n a_0$ e $b = 2^n b_0$. Dessa forma, $a + b = 2^n(a_0 + b_0)$. Os números a_0 e b_0 são ímpares implicando $2 \mid a_0 + b_0 \implies 2^{n+1} \mid 2^n(a_0 + b_0) = a + b \implies \text{mdc}(a+b, 2^{n+1}) = 2^{n+1}$.

Problema 0.34. *(A) Demonstre que se a, b, c, d, m e n são inteiros tais que* $ad - bc = 1$ *e* $mn \neq 0$*, então*

$$\text{mdc}(am + bn, cm + dn) = \text{mdc}(m, n).$$

Solução

Seja $d_1 = mdc(m, n)$ e $d_2 = \text{mdc}(am + bn, cm + dn)$. Basta provar que $d_1 \mid d_2$ e que $d_2 \mid d_1$, pois $d_1, d_2 \geq 1$ e pela propriedade da limitação $d_1 \leq d_2 \leq d_1 \implies d_1 = d_2$.

A primeira parte é direta, pois $d_1 \mid m$ e $d_1 \mid n$ implica que $d_1 \mid am + bn$ e também que $d_1 \mid cm + dn$. Com isso d_1 divide qualquer combinação linear desses números incluindo d_2. Concluímos que $d_1 \mid d_2$.

Para a segunda parte, temos $d_2 \mid am + bn \implies d_2 \mid adm + bdn$ e também temos $d_2 \mid cm + dn \implies d_2 \mid bcm + bdn$. Fazendo a diferença $d_2 \mid (ad - bc)m + (bd - bd)n = m$. Com isso, $d_2 \mid am \implies d_2 \mid bn$ e, analogamente, $d_2 \mid dn$. Multiplicando a primeira por c, a segunda por a e tomando a diferença desta menos aquela temos $d_2 \mid (ad - bc)n = n$. Das divisibilidades $d_2 \mid m$ e $d_2 \mid n$ temos $d_2 \mid d_1$.

Problema 0.35. *(A) Seja* F_n *o n-ésimo termo da sequência de Fibonacci.*

(a) Encontre dois números inteiros a e b tais que $233a + 144b = 1$ *(observe que* 233 *e* 144 *são termos consecutivos da sequência de Fibonacci).*

(b) Mostre que $\text{mdc}(F_n, F_{n+1}) = 1$ *para todo* $n \geq 0$.

(c) Determine x_n *e* y_n *tais que* $F_n \cdot x_n + F_{n+1} \cdot y_n = 1$.

Solução

(a) Usando as divisões sucessivas do algoritmo de Euclides

$$\begin{aligned}
233 &= 144 \cdot 1 + 89 \\
144 &= 89 \cdot 1 + 55 \\
89 &= 55 \cdot 1 + 34 \\
55 &= 34 \cdot 1 + 21 \\
34 &= 21 \cdot 1 + 13 \\
21 &= 13 \cdot 1 + 8 \\
13 &= 8 \cdot 1 + 5 \\
8 &= 5 \cdot 1 + 3 \\
5 &= 3 \cdot 1 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 1 \cdot 2 + 0
\end{aligned}$$

Concluímos que $\text{mdc}(233, 144) = 1$ e temos

$$\begin{aligned}
1 &= 3 \cdot 1 + 2 \cdot (-1) = 3 \cdot 1 + (5 - 3) \cdot (-1) \\
&= 5 \cdot (-1) + 3 \cdot 2 = 5 \cdot (-1) + (8 - 5) \cdot 2 \\
&= 8 \cdot 2 + 5 \cdot (-3) = 8 \cdot 2 + (13 - 8) \cdot (-3) \\
&= 13 \cdot (-3) + 8 \cdot 5 = 13 \cdot (-3) + (21 - 13) \cdot 5 \\
&= 21 \cdot 5 + 13 \cdot (-8) = 21 \cdot 5 + (34 - 21) \cdot (-8) \\
&= 34 \cdot (-8) + 21 \cdot 13 = 34 \cdot (-8) + (55 - 34) \cdot 13 \\
&= 55 \cdot 13 + 34 \cdot (-21) = 55 \cdot 13 + (89 - 55) \cdot (-21) \\
&= 89 \cdot (-21) + 55 \cdot 34 = 89 \cdot (-21) + (144 - 89) \cdot 34 \\
&= 144 \cdot 34 + 89 \cdot (-55) = 144 \cdot 34 + (233 - 144) \cdot (-55) \\
&= 233 \cdot (-55) + 144 \cdot 89
\end{aligned}$$

(b) Para os casos iniciais $\text{mdc}(F_1, F_0) = \text{mdc}(1, 0) = 1$, $\text{mdc}(F_2, F_1) = \text{mdc}(1, 1) = 1$ e $\text{mdc}(F_3, F_2) = \text{mdc}(2, 1) = 1$. Agora analisemos para $n > 3$. Veja que ao dividir F_{n+1} por F_n temos

$$F_{n+1} = F_n \cdot 1 + F_{n-1}$$

Com quociente 1 e resto F_{n-1}, pois $0 \leq F_{n-1} < F_n$. Pelo Algoritmo de Euclides sabemos que $\text{mdc}(a, b) = \text{mdc}(b, r)$ e aplicando na sequência de Fibonacci temos $\text{mdc}(F_{n+1}, F_n) = \text{mdc}(F_n, F_{n-1})$. Repetindo esse passo $n - 2$ vezes

temos $\text{mdc}(F_{n+1}, F_n) = \text{mdc}(F_n, F_{n-1}) = \text{mdc}(F_{n-1}, F_{n-2}) = \cdots = \text{mdc}(F_3, F_2) = \text{mdc}(2, 1) = 1$.

(c) Pelas equações obtidos no primeiro item conjectura-se que

$$F_n(-1)^n F_{n-1} + F_{n+1}(-1)^{n+1} F_{n-2} = 1.$$

Podemos provar que essa equação é válida para todo inteiro $n \geq 2$ usando a fórmula fechada da sequência de Fibonacci apresentada na seção de indução.

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

na qual $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2}$. Nos próximos passos usaremos que $\alpha + \beta = 1$, $\alpha - \beta = \sqrt{5}$, $\alpha \cdot \beta = -1$ e

$$\alpha^3 = \alpha \cdot \alpha^2 = \alpha(\alpha + 1) = \alpha^2 + \alpha = (\alpha + 1)\alpha \iff \alpha^3 = 2\alpha + 1.$$

Analogamente, também podemos usar que $\beta^3 = 2\beta + 1$. Desenvolvendo um dos lados da equação que queremos demonstrar

$$\begin{aligned}
&F_n(-1)^n F_{n-1} + F_{n+1}(-1)^{n+1} F_{n-2} = \\
&= \frac{(\alpha^n - \beta^n)(-1)^n(\alpha^{n-1} - \beta^{n-1}) + (\alpha^{n+1} - \beta^{n+1})(-1)^{n+1}(\alpha^{n-2} - \beta^{n-2})}{(\alpha - \beta)^2} \\
&= \frac{(-1)^n(\alpha^{2n-1} - \alpha^n\beta^{n-1} - \alpha^{n-1}\beta^n + \beta^{2n-1}) + (-1)^{n+1}(\alpha^{2n-1} - \alpha^{n+1}\beta^{n-2} - \alpha^{n-2}\beta^{n+1} + \beta^{2n-1})}{(\alpha - \beta)^2} \\
&= (-1)^n \frac{-\alpha^n\beta^{n-1} - \alpha^{n-1}\beta^n + \alpha^{n+1}\beta^{n-2} + \alpha^{n-2}\beta^{n+1}}{(\alpha - \beta)^2} \\
&= (-1)^n \frac{-\alpha(-1)^{n-1} - \beta(-1)^{n-1} + \alpha^3(-1)^{n-2} + \beta^3(-1)^{n-2}}{(\alpha - \beta)^2} \\
&= (-1)^{2n-2} \frac{-\alpha(-1) - \beta(-1) + \alpha^3 + \beta^3}{(\alpha - \beta)^2} \\
&= \frac{3\alpha + 3\beta + 2}{(\alpha - \beta)^2} \\
&= \frac{5}{5} \\
&= 1
\end{aligned}$$

Assim, podemos usar os seguintes valores $x_n = (-1)^n F_{n-1}$ e $y_n = (-1)^{n+1} F_{n-2}$.
Vale lembrar que essa é apenas uma opção para x_n e y_n. De maneira geral poderíamos usar $x_n = (-1)^n F_{n-1} + kF_{n+1}$ e $y_n = (-1)^{n+1} F_{n-2} - kF_n$ para qualquer inteiro k.

Problema 0.36. *(A) Sejam a e b dois inteiros positivos e d seu máximo divisor comum. Demonstre que existem dois inteiros positivos x e y tais que $ax - by = d$.*

Solução

Pelo Teorema de Bachet-Bézout sabemos que existem inteiros X e Y tais que

$$aX + bY = d$$

Porém, somando e subtraindo abk para um inteiro k qualquer temos

$$a(X + bk) + b(Y - ak) = d$$

Sendo a e b inteiros positivos podemos tomar k suficientemente grande de modo que $X + bk > 0$ e $Y - ak < 0$. Por exemplo, $k = X + Y$ já seria suficiente nesse caso. Logo existem inteiros positivos $x = X + bk$ e $y = -(Y - ak)$ tais que $ax - by = d$.

Problema 0.37. *(OI) Definimos a* sequência de frações de Farey *de ordem n como o conjunto de frações reduzidas $\frac{a}{b}$ tais que $0 \leq \frac{a}{b} \leq 1$, $1 \leq b \leq n$. Por exemplo a sequência de Farey de ordem 3 é $\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$.*

(a) Demonstre que se $\frac{a}{b}$ e $\frac{c}{d}$ são dois termos consecutivos de uma sequência de Farey, então $cb - ad = 1$.

(b) Demonstre que se $\frac{a_1}{b_1}$, $\frac{a_2}{b_2}$, $\frac{a_3}{b_3}$ são três termos consecutivos de uma sequência de Farey, então $\frac{a_2}{b_2} = \frac{a_1+a_3}{b_1+b_3}$.

Solução

Provaremos por indução os dois itens. Para $n = 1$, a sequência de Farey é $\frac{0}{1}, \frac{1}{1}$ que satisfaz as condições. Suponha que a sequência de Farey de ordem n satisfaz as condições. Tomemos agora a sequência de frações de Farey de ordem $n+1$. Seja $\frac{x}{n+1}$ uma fração irredutível entre 0 e 1. Os dois termos vizinhos tem denominador menor que $n+1$. Tome o inteiro positivo k tal que $\frac{k}{n} \leq \frac{x}{n+1} < \frac{k+1}{n} \Leftrightarrow k(n+1) \leq xn < (k+1)(n+1)$. Se houvesse a igualdade $(n+1) \mid xn$ e $\text{mdc}(n+1, n) = 1$ implicando $n+1 \mid x \Rightarrow n+1 \leq n \Rightarrow \frac{x}{n} > 1$. Essas duas frações como frações irredutíveis terão denominadores menores que ou iguais a n. Assim,

$$\frac{a}{b} < \frac{x}{n+1} < \frac{c}{d}$$

com $b, d \leq n$. As distâncias para os vizinhos são

$$\frac{x}{n+1} - \frac{a}{b} = \frac{bx - a(n+1)}{b(n+1)} = \frac{y}{b(n+1)}$$

e

$$\frac{c}{d} - \frac{x}{n+1} = \frac{c(n+1) - dx}{d(n+1)} = \frac{z}{d(n+1)}$$

Na sequência de Farey de ordem n as frações $\frac{a}{b}$ e $\frac{c}{d}$ são consecutivas e, por hipótese de indução, temos $\frac{c}{d} - \frac{a}{b} = \frac{cb-ad}{bd} = \frac{1}{bd}$. Implicando

$$\frac{y}{b(n+1)} + \frac{z}{d(n+1)} = \frac{1}{bd} \Rightarrow \frac{dy+bz}{bd(n+1)} = \frac{1}{bd} \Rightarrow dy + bz = n+1 \geq b+d \Rightarrow y = z = 1.$$

Com isso, temos ainda $b + d = n + 1$.

Isso conclui a primeira parte do passo indutivo, pois $\frac{a}{b} < \frac{x}{n+1} < \frac{c}{d}$ e $bx - a(n+1) = c(n+1) - dx = 1$.

Para a segunda parte, $\frac{a}{b} < \frac{a+c}{b+d} = \frac{a+c}{n+1} < \frac{c}{d}$. Mas a única fração com denominador $n+1$ entre essas duas frações é por construção $\frac{x}{n+1}$. Concluímos, finalmente, que $\frac{a+c}{b+d} = \frac{x}{n+1}$.

Problema 0.38. *(A) Utilize indução em* $\min\{a, b\}$ *e o algoritmo de Euclides para mostrar que* $ax + by = \text{mdc}(a, b)$ *admite solução com* $x, y \in \mathbb{Z}$*, obtendo uma nova demonstração do teorema de Bachet-Bézout.*

Solução

Suponha sem perda de generalidade que $a \geq b$. Faremos indução em b. A base é $b = 1$. Veja que $\text{mdc}(a, 1) = 1$ e $a \cdot 0 + 1 \cdot 1 = 1 = \text{mdc}(a, 1)$.

Passando à hipótese de indução, suponha que para todo número b menor que ou igual a n e qualquer $a \geq b$ existem x e y inteiros tais que $\text{mdc}(a, b) = ax + by$.

Tome $b = n + 1$ e $a \geq b$. Pela divisão euclidiana existem inteiros q e r tais que

$$a = (n+1)q + r, 0 \leq r < n+1$$

Se $r = 0$, então $n + 1 \mid a$ e $\text{mdc}(a, n+1) = n+1 = a \cdot 0 + (n+1) \cdot 1$. Caso contrário, $1 \leq r \leq n$ e vale a hipótese para $\text{mdc}(n+1, r)$, ou seja, existe inteiros x e y tais que

$$\text{mdc}(n+1, r) = (n+1)x + ry$$

Mas pelo algoritmo de Euclides $\text{mdc}(n+1, r) = \text{mdc}(a, n+1)$. Substituindo r usando a equação da divisão, temos

$$\text{mdc}(a, n+1) = (n+1)x + (a - (n+1)q)y = ay + (n+1)(x - qy)$$

Para qualquer $a \geq n + 1$.

Assim, por indução, para quaisquer a e b inteiros positivos existem inteiros x e y tais que

$$\text{mdc}(a, b) = ax + by.$$

Problema 0.39. *(T) Sejam a e b números inteiros positivos. Considere o conjunto*

$$C = \{ax + by \mid x, y \in \mathbb{N}\}$$

Lembre-se de que já mostramos num dos exemplos que se $\text{mdc}(a, b) = 1$ *todo número maior que $ab - a - b$ pertence a C.*

(a) Demonstre que o número $ab - a - b$ não pertence a C.

(b) Achar a quantidade de números inteiros positivos que não pertencem a C.

Solução

(a) Suponha que existem inteiros não negativos x e y tais que $ax + by = ab - a - b \Rightarrow a(x+1) + b(y+1) = ab$. Temos $a \mid b(y+1)$ e $\text{mdc}(a, b) = 1$ implicando $a \mid y + 1 \Rightarrow a \leq y + 1$. Analogamente, $b \leq x + 1$. Logo

$$ab = a(x+1) + b(y+1) \geq ab + ba = 2ab > ab$$

Que é uma contradição. Portanto, não existem inteiros não negativos x e y.

(b) Considere os números $a \cdot 0$, $a \cdot 1$, ..., $a(b-1)$. Veja que não há dois deles com o mesmo resto na divisão por b. Caso contrário, se ax e ay distintos deixam o mesmo resto, então $b \mid a(x-y) \Rightarrow b \mid x - y$ já que $\text{mdc}(a, b) = 1$ e assim $x - y = 0 \Leftrightarrow ax = ay$ ou $b \leq |x - y| \leq b - 1$. Temos b números com b restos distintos, então temos todos os restos e cada resto aparecendo exatamente uma vez. Seja r_x o resto de ax na divisão por b. Note que os números que deixam resto r_x na divisão por b que não podem ser escritos como $am + bn$ para m e n inteiros não negativos são $ax - b, ax - 2b, \ldots, ax - t_x b$ onde $t_x = \left\lfloor \frac{ax}{b} \right\rfloor = \frac{ax - r_x}{b}$. Somando sobre todos os restos, a quantidade de números que não podem ser escritos com $am + bn$ é

$$\sum_{x=0}^{b-1} t_x = \sum_{x=0}^{b-1} \frac{ax - r_x}{b} = \frac{a(0 + 1 + \cdots + b - 1) - (0 + 1 + \cdots + b - 1)}{b}$$

$$= \frac{a\frac{(b-1)b}{2} - \frac{(b-1)b}{2}}{b} = \frac{(a-1)(b-1)}{2}$$

Vale observar que a ideia de tomar os números da forma $ax - b$, $ax - 2b$, ... para cada x de 0 a $b - 1$ também prova que todo número maior que $ab - a - b = a(b-1) - b$ pode ser representado como $am + bn$ para inteiros não negativos m e n. Observe que esse número tem o mesmo resto que $a(b-1)$ na divisão por b e é justamente o último número com esse resto que não pode ser representado.

Problema 0.40 (IMO1984). *(OA) Dados os inteiros positivos a, b e c, dois a dois primos entre si, demonstre que* $2abc - ab - bc - ca$ *é o maior número inteiro que não pode expressar-se na forma* $xbc + yca + zab$ *com* x, y *e* z *inteiros não negativos.*

Solução

Suponha que existem inteiros não negativos x, y e z tais que $2abc - ab - bc - ca = xbc + yca + zab$. Como a divide quase todos os termos temos $a \mid (x+1)bc$. Como $\text{mdc}(a, bc) = 1$ temos $a \mid x+1 \Rightarrow x \geq a-1$. Da mesma forma, $y \geq b-1$ e $z \geq c-1$. Logo $xbc + yca + zab \geq (a-1)bc + (b-1)ca + (c-1)ab = 3abc - ab - bc - ca > 2abc - ab - bc - ca$.

Agora mostraremos que é possível encontrar inteiros não negativos x, y e z para qualquer $k > 2abc - ab - bc - ca$ inteiro. Sabemos que $1 = \text{mdc}(bc, a) = \text{mdc}(bc, \text{mdc}(ca, ab))$. Pelo Teorema de Bachet-Bézout existem inteiros u, v e w tais que $k = ubc + vca + wab$. Veja que $k = (u - ta)bc + (v - sb)ca + (w + (t+s)c)ab$ para quaisquer inteiros t e s inteiros. Podemos escolher esses parâmetros de modo que $0 \leq x = u - ta \leq a-1$ e $0 \leq z = v - sb \leq b-1$. Isso nos leva a $xbc + yca \leq (a-1)bc + (b-1)ca = 2abc - bc - ca$. Veja que $(w + (t+s)c)ab = k - xbc - yca \geq k - (2abc - bc - ca) > -ab \Rightarrow (w + (t+s)c) > -1 \Rightarrow z = w + (t+s)c \geq 0$.

Problema 0.41 (IMO1977). *(OI) Sejam* a, b *inteiros positivos. Quando dividimos* $a^2 + b^2$ *por* $a + b$*, o quociente é* q *e o resto é* r*. Encontre todos os* a, b *tais que* $q^2 + r = 1977$.

Solução

Temos $q^2 \leq 1977 < 45^2 \Rightarrow q \leq 44$. Assim, $a^2 + b^2 = q(a+b) + r < (q+1)(a+b) \leq 45(a+b)$. Sabemos que $(a-b)^2 \geq 0 \Rightarrow a^2 + b^2 \geq 2ab$ e, portanto, $(a+b)^2 \leq 2(a^2+b^2) < 90(a+b) \Rightarrow a + b < 90$. Com isso, $r < 90$ e $q^2 = 1977 - r > 1977 - 90 = 1887 > 43^2 \Rightarrow q > 43$. Podemos concluir que $q = 44$ e $r = 1977 - 44^2 = 41$. Então o problema passa a ser

$$a^2 + b^2 = 44(a+b) + 41 = (a-22)^2 + (b-22)^2 = 22^2 + 22^2 + 41 = 1009$$

Como 1009 é um primo que deixa resto 1 na dvisião por 4 existem apenas duas soluções inteiras positivas para (A, B) tal que $A^2 + B^2 = 1009$ que são $(A, B) = (15, 28)$ e $(A, B) = (28, 15)$. Logo as soluções são $a - 22 = \pm 15$ e $b - 22 = \pm 28$ e os mesmos pares com a ordem trocada. Lembrando que $b - 22 = -28 \Leftrightarrow b = -6 < 0$ que não satisfaz as condições, as soluções são

$$(a, b) \in \{(37, 50), (7, 50), (50, 7), (50, 37)\}.$$

Problema 0.42. *(OI) Demonstre que* $\text{mdc}(2^a - 1, 2^b - 1) = 2^{\text{mdc}(a,b)} - 1$ *para todo* $a, b \in \mathbb{N}$.

Solução

Veja que para $a = b$ é imediato que $\text{mdc}(2^a - 1, 2^a - 1) = 2^a - 1 = 2^{\text{mdc}(a,a)} - 1$.
Para $a > b$ vamos provar que $\text{mdc}(2^a - 1, 2^b - 1) = \text{mdc}(2^{a-b} - 1, 2^b - 1)$. Tome $D = \text{mdc}(2^a - 1, 2^b - 1)$ e $d = \text{mdc}(2^{a-b} - 1, 2^b - 1)$. Veja que

$$D \mid (2^a - 1) - (2^b - 1) = 2^b(2^{a-b} - 1) \Rightarrow D \mid 2^{a-b} - 1$$

Nesse último passo usamos que D é ímpar já que divide números ímpares e $\text{mdc}(D, 2) = 1$. Note que D é um divisor comum de $2^b - 1$ e $2^{a-b} - 1$ e, portanto, é um divisor do mdc deles, ou seja, $D \mid d$.
Analogamente, temos

$$d \mid 2^b \cdot (2^{a-b} - 1) - (2^b - 1) = 2^a - 1 \Rightarrow d \mid D.$$

Dois números inteiros positivos tais que um divide o outro são iguais. Assim, $D = d \Leftrightarrow \text{mdc}(2^a - 1, 2^b - 1) = \text{mdc}(2^{a-b} - 1, 2^b - 1)$. Pelo algoritmo de Euclides aplicado aos expoentes, basta mostrar que $\text{mdc}(2^{bq+r} - 1, 2^b - 1) = \text{mdc}(2^b - 1, 2^r - 1)$. Do fato que demonstramos segue esse resultado, pois podemos repetir q vezes a subtração de b no expoente mantendo o mesmo mdc.

Problema 0.43. *(A) Encontre todas as funções $f : \mathbb{N}^* \times \mathbb{N}^* \longrightarrow \mathbb{Z}$ satisfazendo simultaneamente as seguintes propriedades*

(i) $f(a, a) = a$.

(ii) $f(a, b) = f(b, a)$.

(iii) Se $a > b$, então $f(a, b) = \frac{a}{a-b} f(a - b, b)$.

O domínio da função foi trocado de $\mathbb{Z} \times \mathbb{Z}$ para $\mathbb{N}^* \times \mathbb{N}^*$, pois a solução nos inteiros positivos usa técnicas desenvolvidas neste capítulo e no conjunto dos inteiros essas três propriedades não permitem calcular certos valores de f, como, por exemplo, $f(1, 0)$.

Solução

Provaremos por indução em $\min\{a, b\}$ que $f(a, b) = \text{mmc}(a, b)$ para a e b inteiros positivos. Veja que para $a = b$ temos $f(a, a) = a = \text{mmc}(a, a)$. Pela segunda propriedade não importa a ordem dos números, então podemos supor sem perda de generalidade que $a \geq b$. Quando o menor dos números igual a 1 temos

$$f(n, 1) = \frac{n}{n-1} f(n - 1, 1) = \frac{n}{n-1} \cdot \frac{n-1}{n-2} f(n - 2, 1) = \ldots$$

$$= \frac{n}{n-1} \frac{n-1}{n-2} \ldots f(2, 1) f(1, 1) = n = \text{mmc}(n, 1).$$

Suponha que para $b \leq m$ a função f para um par de números é igual ao mmc desses números.

Para $a > b = m+1$, podemos fazer a divisão euclidiana temos $a = bq + r$ com $0 \leq r < b$. Se $r = 0$, então $b \mid a$ e $\text{mmc}(a,b) = a$. Podemos aplicar a terceira propriedade $q-1$ vezes e obter

$$f(a,b) = \frac{a}{a-b}\frac{a-b}{a-2b}\cdots\frac{a-b(q-2)}{a-b(q-1)}f(b,b) = \frac{a}{b}b = a = \text{mmc}(a,b)$$

Se $r > 0$ podemos aplicar a terceira propriedade q vezes e obter

$$f(a,b) = \frac{a}{a-b}\frac{a-b}{a-2b}\cdots\frac{a-b(q-1)}{a-bq}f(r,b) = \frac{a}{r}\,\text{mmc}(b,r)$$

Sabemos que $\text{mmc}(x,y) = \frac{xy}{\text{mdc}(x,y)}$ e que, pelo Algoritmo de Euclides, $\text{mdc}(a,b) = \text{mdc}(b,r)$. Usando esses fatos:

$$f(a,b) = \frac{a}{r}\frac{br}{\text{mdc}(b,r)} = \frac{a\cdot b}{\text{mdc}(a,b)} = \text{mmc}(a,b)$$

Problema 0.44. *(A) Mostre que se n é um número natural composto, então n é divisível por um primo p com $p \leq \lfloor\sqrt{n}\rfloor$.*

Solução

Seja p o menor fator primo de n. Podemos escrever n como produto $p\cdot q$. Veja que $q \geq 2$, pois para $q = 1$ o número n seria primo. Então q possui um ou mais fatores de n e $q \geq p$. Logo $n = p\cdot q \geq p\cdot p = p^2 \Rightarrow \sqrt{n} \geq p \Rightarrow \lfloor\sqrt{n}\rfloor \geq p$.

Problema 0.45 (IMO1989)**.** *(OI) Prove que, para todo inteiro positivo n, existem n inteiros positivos consecutivos, nenhum dos quais é potência de primo.*

Solução

Seja $N = (n+1)!^2+1$ e considere os números $N+1, N+2, \ldots, N+n$. Afirmamos que nenhum desses n números é potência de primo.

Suponha o contrário, ou seja, que existe um i com $1 \leq i \leq n$ e um primo p tal que $N+i = p^k$. Daí, $p^k = N+i = (n+1)!^2+(1+i) \Rightarrow i+1 \mid p^k \Rightarrow i+1 = p^t$ para algum expoente t com $1 \leq t < k$. Veja que $i+1$ aparece em $(n+1)!$ implicando que $p^{t+1} \mid (n+1)!^2$. De $k > t$ temos $p^{t+1} \mid N+i$. Dessas duas últimos divisibilidades $p^{t+1} \mid i+1 = p^t$ que é um absurdo.

Problema 0.46 (China1998)**.** *(OI) Encontre todos os naturais $n > 3$ para os quais $1 + \binom{n}{1} + \binom{n}{2} + \binom{n}{3}$ divide 2^{2000}.*

Solução

Seja $N = 1 + \binom{n}{1} + \binom{n}{2} + \binom{n}{3}$. Expadindo os binomiais

$$N = 1 + n + \frac{n(n-1)}{2} + \frac{n(n-1)(n-2)}{6} = n + 1 + \frac{3n(n-1) + n(n-1)(n-2)}{6}$$
$$= \frac{6(n+1) + n(n-1)(n+1)}{6} = \frac{(n+1)(n^2 - n + 6)}{6}.$$

Note que $N \mid 2^{2000}$ se, e somente se, $n+1 = 2^a$ e $n^2 - n + 6 = 2^b \cdot 3$ ou $n+1 = 2^a \cdot 3$ e $n^2 - n + 6 = 2^b$.

No primeiro caso, $n = 2^a - 1$ e

$$n^2 - n + 6 = 2^{2a} - 2^{a+1} + 1 - 2^a + 1 + 6 = 2^b \cdot 3$$

$$2^{2a} - 3 \cdot 2^a + 8 = 2^b \cdot 3$$

Para $a \geq 4$ temos $2^3(2^{2a-3} - 3 \cdot 2^{a-3} + 1)$. O segundo fator é ímpar e contém todos os fatores ímpares desse número. Veja que $2^{2a-3} - 3 \cdot 2^{a-3} + 1 \geq 2^5 - 3 \cdot 2^1 + 1 = 27 > 3$ e não temos solução. Veja que apesar da subtração estamos analisando $n(n-3)$ que é crescente para $n > 3$. Como $n > 3$ sabemos que $a \geq 3$. Resta testar $a = 3$. Temos solução, pois:

$$2^{2a} - 3 \cdot 2^a + 8 = 64 - 24 + 8 = 48 = 2^4 \cdot 3$$

Logo, $n = 2^3 - 1 = 7$ é solução.

No segundo caso, $n = 3 \cdot 2^a - 1$

$$n^2 - n + 6 = 9 \cdot 2^{2a} - 3 \cdot 2^{a+1} + 1 - 3a \cdot 2^a + 1 + 6 = 2^b$$

$$9 \cdot 2^{2a} - 9 \cdot 2^a + 8 = 2^b$$

Novamente, para $a \geq 4$ temos $9 \cdot 2^{2a} - 9 \cdot 2^a + 8 = 2^3(9 \cdot 2^{2a-3} - 9 \cdot 2^{a-3} + 1)$ e $9 \cdot 2^{2a-3} - 9 \cdot 2^{a-3} + 1 > 9 \cdot 32 - 9 \cdot 2 + 1 = 271 > 1$. Não temos solução com $a \geq 4$. Como $n > 3$ temos $a \geq 1$. Resta testar $a = 1$, 2 ou 3.

Para $a = 1$

$$9 \cdot 2^{2a} - 9 \cdot 2^a + 8 = 9 \cdot 4 - 9 \cdot 2 + 8 = 26 \neq 2^b$$

Para $a = 2$

$$9 \cdot 2^{2a} - 9 \cdot 2^a + 8 = 9 \cdot 16 - 9 \cdot 4 + 8 = 116 \neq 2^b$$

Para $a = 3$

$$9 \cdot 2^{2a} - 9 \cdot 2^a + 8 = 9 \cdot 64 - 9 \cdot 8 + 8 = 512 = 2^9$$

Dessa forma, encontramos a segunda solução $n = 3 \cdot 2^3 - 1 = 23$.

Os inteiros n que satisfazem a divisibilidade são 7 e 23.

Problema 0.47 (IMO2002). *(OA) Sejam $d_1 < d_2 < \cdots < d_k$ os divisores positivos de um inteiro $n > 1$. Seja $d = d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k$. Mostre que $d < n^2$ e encontre todos os n para os quais $d \mid n^2$.*

Solução

Temos $d = \frac{n^2}{d_kd_{k-1}} + \frac{n^2}{d_{k-1}d_{k-2}} + \cdots + \frac{n^2}{d_2d_1} < n^2 \cdot (\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots) = n^2 \cdot (\frac{1}{1} - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \frac{1}{3} - \frac{1}{4} + \cdots) = n^2$.

Por outro lado, se p é o menor primo que divide n^2, temos que $d \geq d_{k-1}d_k = \frac{n^2}{p}$. Como $\frac{n^2}{p}$ é o maior divisor de n^2 menor que n^2 e $d > d_{k-1}d_k$ se $k > 2$, temos que $d \mid n^2$ se, e somente se, $n = p$ é primo.

Problema 0.48 (IMO1997). *(OA) Encontre todos os pares (x, y) de inteiros positivos tais que $x^{y^2} = y^x$.*

Solução

Sejam $x = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ e $y = p_1^{\beta_1} \dots p_n^{\beta_n}$ as fatorações de x e y em primos. Os primos p_i são a união dos primos que dividem esses números, então alguns expoentes α_i e β_i podem ser nulos, mas não os dois expoentes para o mesmo p_i.
De $x^{y^2} = y^x$ temos $y^2\alpha_i = x\beta_i$ implicando $\frac{\alpha_i}{\beta_i} = \frac{x}{y^2} = \frac{p}{q}$ para p e q primos entre si. Assim, podemos considerar o número $a = p_1^{\frac{\alpha_1}{p}} \dots p_n^{\frac{\alpha_n}{p}}$ escrever $x = a^p$ e $y = a^q$. Se $a = 1$ temos a solução $(x, y) = (1, 1)$. Se $a > 1$, então $a^{pa^{2q}} = a^{qa^p} \Rightarrow pa^{2q} = qa^p$. Dessa expressão podemos concluir que $p \neq q$ e nos resta dois casos

(i) Se $p < q$.
Temos $\frac{q}{p} = a^{2q-p}$. Usando uma variável auxiliar $d = 2q - p \geq 0$ temos $q = a^dp$ e $a^d = a^{(2a^d-1)p} \Rightarrow d = (2a^d - 1)p$. Porém, $2a^d - 1 > d$ para $a \geq 2$ e $d \geq 1$. Então não há soluções com $p < q$.

(ii) Se $p > q$.
Temos $a^{2q} < a^p \Rightarrow 2q < p$. Logo $p = a^{p-2q}q \Rightarrow q \mid p$ e $\text{mdc}(q, p) = 1 \Rightarrow q = 1$. Chegamos em $p = a^{p-2}$. Considere $d = p - 2 \geq 1$. Temos $d + 2 \geq a^d > d + 2$ para $d \geq 3$. Basta testar $d = 1$ e $d = 2$. Para $d = 1$ temos $q = 1$, $a = p = 3$ e temos o par $(x, y) = (27, 3)$ que é solução. Para $d = 2$ temos $q = 1$, $a = 2$, $p = 4$ e o par $(x, y) = (16, 2)$ que também é solução.

As soluções para (x, y) são $(1, 1)$, $(27, 3)$ e $(16, 2)$.

Problema 0.49. *(OA) Generalizar o resultado anterior para $x^{y^n} = y^x$, onde x e y são inteiros positivos.*

Solução

Seguiremos grande parte dos passos do problema anterior. Comecemos novamente com as fatorações em primos $x = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ e $y = p_1^{\beta_1} \dots p_k^{\beta_k}$.
De $x^{y^n} = y^x$ temos $y^n \alpha_i = x\beta_i$ implicando $\frac{\alpha_i}{\beta_i} = \frac{x}{y^n} = \frac{p}{q}$ para p e q primos entre si. Novamente, podemos considerar o número $a = p_1^{\frac{\alpha_1}{p}} \dots p_k^{\frac{\alpha_k}{p}}$ escrever $x = a^p$ e $y = a^q$. Se $a = 1$ temos as soluções $(x, y, n) = (1, 1, m)$ em que m pode ser qualquer inteiro positivo. Para $a > 1$ temos $a^{py^n} = a^{qx} \Rightarrow py^n = qx \Rightarrow pa^{nq} = qa^p$. Agora vamos analisar três casos $p = q$, $p < q$ ou $p > q$.

(i) Se $p = q$.
Então $a^{nq} = a^p \Rightarrow nq = p \Rightarrow n = 1$ e temos as soluções $(x, y, n) = (m, m, 1)$ para qualquer inteiro positivo m. De fato, se $n = 1$ temos $x = y = m$, então a partir de agora consideraremos $n \geq 2$.

(ii) Se $p < q$.
Então $a^{nq} > a^p \Rightarrow nq > p$ e tomamos o inteiro positivo $d = nq - p$. Temos $pa^{nq} = qa^p \Rightarrow pa^d = q$. Isso implica que $p \mid q$ e $\text{mdc}(p, q) = 1$. Concluímos que $p = 1$ e $q = a^d$. Mas $d = nq - p \Rightarrow d = na^d - 1 > 2 \cdot 2^d - 1 > d$ para $d \geq 1$. Concluímso que esse caso não tem soluções.

(iii) Se $p > q$.
Então $a^{nq} < a^p \Rightarrow nq < p$ e tomamos o inteiro positivo $d = p - nq$. Temos $pa^{nq} = qa^p \Rightarrow p = qa^d \Rightarrow q \mid p$ e $\text{mdc}(q, p) = 1 \Rightarrow q = 1$ e $p = a^d$. Com isso, $d = a^d - n \Rightarrow n = a^d - d$. Observe que $x = a^p = a^{a^d}$ e $y = a^q = a$ e temos as soluções $(x, y, n) = (a^{a^d}, a, a^d - d)$ que satisfazem a equação, pois

$$x^{y^n} = y^x \Leftrightarrow a^{a^d \cdot a^n} = a^{a^{a^d}} \Leftrightarrow a^d \cdot a^{a^d - d} = a^{a^d} \Leftrightarrow d + (a^d - d) = a^d.$$

Concluímos que as soluções são $(x, y, n) = (1, 1, m)$, $(x, y, n) = (m, m, 1)$ ou $(x, y, n) = (a^{a^d}, a, a^d - d)$ para quaisquer m, a e d inteiros positivos com $a \geq 2$.

Veja que as soluções para $n = 2$ são $(x, y, n) = (1, 1, 2)$ e $a^d - d = 2$. O segundo caso nos dá $(a, d) = (2, 2) \Rightarrow (x, y, n) = (16, 2, 2)$ ou $(a, d) = (3, 1) \Rightarrow (x, y, n) = (27, 3, 2)$, pois para $a \geq 4$ temos $a^d - d > 2$.

Problema 0.50 (IMO1984)**.** *(OA) Sejam a, b, c, d inteiros ímpares tais que $0 < a < b < c < d$ e $ad = bc$. Demonstre que se $a + d = 2^k$ e $b + c = 2^m$ para inteiros k e m, então $a = 1$.*

Solução

Esta solução foi consultada em [14].

Observe que

$$(d+a)^2-(d-a)^2 = 4ad = 4bc = (c+b)^2-(c-b)^2$$

Sabendo que $d-a > b-c$ temos $d+a > b+c \Rightarrow 2^k > 2^m \Rightarrow k > m$. Veja que $d = 2^k - a$ e $c = 2^m - b$. Com isso,

$$ad = bc \Rightarrow a(2^k-a) = b(2^m-b) \Rightarrow (b-a)(b+a) = 2^m(b-2^{k-m}a)$$

Como $k-m \geq 1$, temos $2^{k-m}a$ par e $b-2^{k-m}a$ ímpar. Logo, existem inteiros positivos m_1, m_2, p e q tais que $b-a = 2^{m_1}p$ e $b+a = 2^{m_2}q$ com p e q ímpares e $m_1+m_2 = m$. Daí, $b = 2^{m_1-1}p + 2^{m_2-1}q$ é ímpar. Se $m_1, m_2 \geq 2$ ou $m_1 = m_2 = 1$ teríamos b par que contradiz as condições do problema. Logo $m_1 = 1$ ou $m_2 = 1$. Se $m_1 = 1$ teríamos $b-a = 2^{m_2}q \geq 2^{m-1} = \frac{b+c}{2} > b$ que é uma contradição. Portanto, $m_2 = 1$ e $m_1 = m-1$. Note que $b+a = 2^{m-1}q < b+c = 2^m \Rightarrow q < 2 \Rightarrow q = 1$. Dessa forma, $b = 2^{m-1} - a$ e.

$$a(2^k-a) = b(2^m-b) \Rightarrow a(2^k-a) = (2^{m-1}-a)(2^m-2^{m-1}+a) = (2^{m-1}-a)(2^{m-1}+a)$$

$$\Rightarrow a2^k - a^2 = 2^{2(m-1)} - a^2$$

Logo $a = 2^{2(m-1)-k}$ é uma potência de 2 ímpar e só pode ser 1.

Além de provar que $a = 1$ podemos concluir que todas as soluções (a,b,c,d) são da forma $(1, 2^{m-1}-1, 2^{m-1}+1, 2^{2(m-1)}-1)$ para qualquer inteiro positivo $m \geq 3$, pois $b = 2^{m-1}-1$, $c = 2^m - b = 2^{m-1}+1$ e $d = \frac{bc}{a} = 2^{2(m-1)}-1$.

0.6 CONGRUÊNCIAS

0.7 BASES

0.8 O ANEL DE INTEIROS MÓDULO n

0.9 A FUNÇÃO DE EULER E O TEOREMA DE EULER-FERMAT

Problema 0.51. *(A) Demonstre que*

(a) $61 \mid 20^{15} - 1$.

(b) $13 \mid 2^{70} + 3^{70}$.

Solução

(a) Veja que $20 = 2^2 \cdot 5 \Rightarrow 20^{15} = 2^{30} \cdot 5^{15}$. Temos $2^6 \equiv 3 \pmod{61} \Rightarrow 2^{30} \equiv 3^5 \equiv 243 \equiv -1 \pmod{61}$. Para o 5 temos $5^3 \equiv 3 \pmod{61} \Rightarrow 5^15 \equiv 3^5 \equiv -1 \pmod{61}$. Concluímos que $20^{15} \equiv (-1)^2 \equiv 1 \pmod{61} \Rightarrow 61 \mid 20^{15} - 1$.

(b) Vamos calcular as congruências de cada potência. Para 2 temos $2^6 \equiv -1 \pmod{13}$. Daí, $2^{66} \equiv (-1)^{11} \equiv -1 \pmod{13} \Rightarrow 2^{70} \equiv 2^4 \cdot (-1) \equiv -3 \pmod{13}$. Para 3 temos $3^3 \equiv 1 \pmod{13} \Rightarrow 3^{69} \equiv 1 \pmod{13} \Rightarrow 3^{70} \equiv 3 \pmod{13}$. Logo $2^{70} + 3^{70} \equiv -3 + 3 \equiv 0 \pmod{13} \Rightarrow 13 \mid 2^{70} + 3^{70}$.

Problema 0.52. *(A) Encontre os últimos 3 dígitos de* 3^{2009} *em notação decimal.*

Solução

Os três últimos dígitos são o resto na divisão por 1000. Observe que $\varphi(1000) = 1000(1 - \frac{1}{2})(1 - \frac{1}{5}) = 400$. Como $\text{mdc}(1000, 3) = 1$ podemos usar o Teorema de Euler-Fermat para concluir que $3^{\varphi(1000)} \equiv 3^{400} \equiv 1 \pmod{1000} \Rightarrow 3^{2000} \equiv 1 \pmod{1000}$. Para concluir basta calcular $3^9 = 19683$ e substituindo $3^{2009} \equiv 3^{2000} \cdot 3^9 \equiv 683 \pmod{1000}$. O três últimos dígitos de 3^{2009} são 683 nesta ordem.

Problema 0.53. *(A) Verificar se* 987654321 *é divisível por* 9, 11, 13, 17 *ou* 19.

Solução

Como $10 \equiv 1 \pmod{9}$ temos $987654321 \equiv 9 + 8 + 7 + 6 + 5 + 4 + 3 + 2 + 1 \equiv 45 \equiv 0 \pmod{9}$ e $9 \mid 987654321$.

Para a divisbilidade por 11 partimos de $10 \equiv -1 \pmod{11}$ e obtemos $987654321 \equiv 9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1 \equiv 5 \pmod{11}$. Então 987654321 não é divisível por 11.

Para 13 usaremos $10^3 \equiv -1 \pmod{13}$ e $987654321 \equiv 987 \cdot 10^6 + 654 \cdot 10^3 + 321 \equiv 987 - 654 + 321 \equiv 654 \equiv 4 \pmod{13}$. O número não é divisível por 13.

Para 17 temos $10^2 \equiv -2 \pmod{17}$ e $987654321 \equiv 9 \cdot (-2)^4 + 87 \cdot (-2)^3 + 65 \cdot (-2)^2 + 43 \cdot (-2) + 21 \equiv -357 \equiv 0 \pmod{17}$. O número 987654321 é divisível por 17.

Finalmente, para 19 temos $10^2 \equiv 5 \pmod{19}$, $10^4 \equiv 5^2 \equiv 6 \pmod{19}$, $10^6 \equiv 5 \cdot 6 \equiv 11 \pmod{19}$ e $10^8 \equiv 11 \cdot 5 \equiv -2 \pmod{19}$. Esses valores facilitam as contas para 987654321:

$$987654321 \equiv 9 \cdot (-2) + 87 \cdot 11 + 65 \cdot 6 + 43 \cdot 5 + 21 \pmod{19}$$

$$987654321 \equiv 9 \cdot (-2) + 11 \cdot 11 + 8 \cdot 6 + 5 \cdot 5 + 2 \equiv 178 \equiv 7 \pmod{19}$$

Então 19 não divide 987654321.

Dos números fornecidos apenas 9 e 17 são divisores de 987654321.

Problema 0.54. *(A) Demonstre que todo número palíndromo com um número par de dígitos é divisível por* 11. *O que acontece com os números palíndromos com um número ímpar de dígitos?*

Solução

Seja $N = a_1a_2 \ldots a_na_n \ldots a_2a_1$ um palíndromo com $2n$ dígitos. Veja que podemos escrever N usando a representação na base decimal e as potências de 10

$$N = \sum_{i=1}^{n} a_i(10^{i-1} + 10^{2n-i}).$$

Sabemos que $10 \equiv -1 \pmod{11}$ e que a soma $i - 1 + 2n - i = 2n - 1$ ímpar implica que um desses números é par e o outro ímpar. Assim,

$$10^{i-1} + 10^{2n-i} \equiv -1 + 1 \equiv 0 \pmod{11}$$

e N é uma soma de múltiplos e, portanto, é divisível por 11.
Se a quantidade de dígitos for ímpar o número poderá ser divisível por 11, como $121 = 11^2$, ou não, como 131 que deixa resto 10 na divisão por 11.

Problema 0.55. *(OI) Encontre todos os números N de três dígitos em representação decimal, tais que N é divisível por* 11 *e além disso $N/11$ é igual à soma dos quadrados dos dígitos de N.*

Solução

Se chamarmos de c, d e u os dígitos das centenas, dezenas e unidades, respectivamente, de N temos que satisfazer

$$100c + 10d + u = 11(c^2 + d^2 + u^2)$$

Como $10 \equiv -1 \pmod{11}$ temos $100c + 10d + u \equiv c - d + u \pmod{11}$. Como $-9 \leq c + u - d \leq 18$ só temos dois múltiplos de 11 possíveis: 0 e 11.
Se $c + u - d = 0$, então $d = c + u$ e nossa igualdade se torna

$$100c + 10(c + u) + u = 11(c^2 + (c + u)^2 + u^2) \Leftrightarrow 10c + u = 2c^2 + 2cu + 2u^2$$

Veja que u é par e podemos testar os 5 valores. Se $u = 0 \Rightarrow 10c = 2c^2 \Rightarrow c = 5$ e temos a solução $550 = 11(5^2 + 5^2 + 0^2)$.
Se $u = 2 \Rightarrow 10c + 2 = 2c^2 + 4c + 8 \Rightarrow c^2 - 3c + 3 = 0$ e não existe c.
Se $u = 4 \Rightarrow 10c + 2 = 2c^2 + 8c + 32 \geq 2c + 8c + 32 > 10c + 2$.

Para $u \geq 5$ temos $2cu \geq 10c$ e o lado direito é maior que o esquerdo.
Se $c+u-d = 11$, então $d = c+u-11$ e nossa igualdade se torna

$$100c+10(c+u-11)+u = 11(c^2+(c+u-11)^2+u^2) \Leftrightarrow 10c+u-10 = 2c^2+2cu+2u^2-22c-22u+121$$

$$\Leftrightarrow 32c+23u = 2c^2+2cu+2u^2+131$$

Veja que u é ímpar, que por congruência módulo c temos que c é um divisor de $2u^2+131-23u$ e que $c+u = 11+d \geq 11$. Faremos os casos.
Se $u = 1$ teríamos $c \geq 11-u = 10$ que não tem solução.
Se $u = 3$ teríamos $c \geq 11-u = 8$ e $c \mid 80$. A única possibilidade é $c = 8$. Temos a solução $803 = 11(8^2+0^2+3^2)$.
Se $u = 5$ teríamos $c \geq 11-u = 6$ e $c \mid 66$. A única possibilidade é $c = 6$. Mas o número 605 não funciona.
Se $u = 7$ teríamos $c \geq 11-u = 4$ e $c \mid 68$. A única possibilidade é $c = 4$. Mas o número 407 não funciona.
Se $u = 9$ teríamos $c \geq 11-u = 2$ e $c \mid 86$. A única possibilidade é $c = 2$. Mas o número 209 não funciona.
As únicas soluções são 550 e 803.

Problema 0.56. *(OI) Mostre que o dígito das dezenas de qualquer potência de 3 é um número par (por exemplo, o dígito das dezenas de $3^6 = 729$ é 2).*

Solução
Veja que $3^1 = 3$, $3^2 = 9$, $3^3 = 27$ e $3^4 = 81$ satisfazem as condições, pois os dígitos das dezenas são 0, 0, 2 e 8, respectivamente. Os dígitos das unidades das potências de 3 se repetem a cada quatro potências, pois $3^4 \equiv 1 \pmod{10} \Rightarrow 3^{N+4} \equiv 3^N \pmod{10}$.
Agora veja que módulo 100 temos

$$3^k \equiv 10a+3 \pmod{100} \Rightarrow 3^{k+1} \equiv 10(3a)+9 \pmod{100}$$

$$3^k \equiv 10b+9 \pmod{100} \Rightarrow 3^{k+1} \equiv 10(3b+2)+7 \pmod{100}$$

$$3^k \equiv 10c+7 \pmod{100} \Rightarrow 3^{k+1} \equiv 10(3c+8)+1 \pmod{100}$$

$$3^k \equiv 10d+1 \pmod{100} \Rightarrow 3^{k+1} \equiv 10(3d)+3 \pmod{100}$$

Se a, b, c e d são pares, então $3a$, $3b+2$, $3c+8$ e $3d$ também são pares.
Por indução, segue que o dígito das dezenas de qualquer potência de 3 é par.

Problema 0.57. *(A) Mostre que, para todo $n \geq 0$, vale que $13 \mid 7^{2n+1}+6^{2n+1}$.*

Solução

Veja que $7 \equiv -6 \pmod{13}$, pois $13 \mid 7-(-6)$. Elvando os dois lados a $2n+1$ temos $7^{2n+1} \equiv (-6)^{2n+1} \equiv -6^{2n+1} \pmod{13}$. Note que o sinal negativo pode sair da potência porque o expoente é ímpar. Dessa forma, $13 \mid 7^{2n+1} - (-6^{2n+1}) = 7^{2n+1} + 6^{2n+1}$.

Problema 0.58. *(A) Encontre todas as soluções da congruência* $x^2 \equiv 1 \pmod{30}$. *Conclua que existem valores de* x *tais que* 30 *não divide* $x+1$ *nem* $x-1$ *mas divide* x^2-1. *Generalize esse resultado.*

Solução

Veja que $x^2 \equiv 1 \pmod{30} \Leftrightarrow 30 \mid x^2-1 = (x-1)(x+1)$. Temos as possibilidades de separar os fatores primos de $30 = 2 \cdot 3 \cdot 5$ nesses dois termos. Podemos escrever $x = 30q + r$ com $0 \leq r < 30$ e analisar os possíveis valores de r. Observe que $2 \mid x-1 \Leftrightarrow 2 \mid x+1$, então podemos resumir as possibilidades do fator 2 por r ímpar. Para os demais fatores temos os casos.

(i) Se $x-1$ tem os fatores 3 e 5, então $r = 3k+1$ e $r = 5t+1$. O único valor possível é $r = 1$.

(ii) Se $x-1$ tem o fator 3 e $x+1$ tem o fator 5, então $r = 3k+1$ e $r = 5t+4$. O único valor possível é $r = 19$.

(iii) Se $x-1$ tem o fator 5 e $x+1$ tem o fator 3, então $r = 3k+2$ e $r = 5t+1$. O único valor possível é $r = 11$.

(iv) Se $x+1$ tem os fatores 3 e 5, então $r = 3k+2$ e $r = 5t+4$. O único valor possível é $r = 29$.

As soluções são $x = 30q+1$, $x = 30q+11$, $x = 30q+19$ ou $x = 30q+29$, para qualquer inteiro q.

Em geral, $x^2 \equiv 1 \pmod{m}$ só implica que $m \mid x-1$ ou $m \mid x+1$ se m é um primo maior que 2 ou é potência de um primo maior que 2.

Problema 0.59. *(A) Encontre um número positivo* $k < 50$ *tal que* $a^k \equiv 1 \pmod{99}$ *para todo inteiro a primo relativo com* 99.

Solução

Pelo Teorema de Euler-Fermat poderíamos usar $\varphi(99) = \varphi(9)\varphi(11) = 6 \cdot 10 = 60$ como expoente. Porém $60 > 50$ e não satisfaz a condição $k < 50$.

Porém, veja que $k = 30$ já satisfaz a propriedade desejada. Já que $\text{mdc}(a, 99) = 1 \Rightarrow \text{mdc}(a, 9) = 1$ e $\text{mdc}(a, 11) = 1$. Pelo Teorema de Euler-Fermat com 9 e 11 temos

$$a^6 \equiv 1 \pmod 9 \Rightarrow a^{30} \equiv 1 \pmod 9$$

$$a^{10} \equiv 1 \pmod{11} \Rightarrow a^{30} \equiv 1 \pmod{11}$$

Assim, se $\text{mdc}(a, 99) = 1$ então $a^{30} \equiv 1 \pmod{99}$.

Problema 0.60. *(T) Mostre que para todo inteiro a temos que $a^{561} \equiv a \pmod{561}$ e $a^{1105} \equiv a \pmod{1105}$, mas 561 e 1105 não são primos, o que mostra que o recíproco do pequeno teorema de Fermat é falso.*

Solução

Veja que se p primo satisfaz $p - 1 \mid n - 1$ temos $a^n \equiv a \pmod p$. Se p divide a então os dois lados são congruentes a zero. Se p não divide a então $\text{mdc}(p, a) = 1$, e pelo Teorema de Euler-Fermat $a^{p-1} \equiv 1 \pmod p \Rightarrow a^{n-1} \equiv 1^{\frac{n-1}{p-1}} \equiv 1 \pmod p \Rightarrow a^n \equiv a \pmod p$.

Fatorando em primos, temos $561 = 3 \cdot 11 \cdot 17$. Veja que $3 - 1 = 2$, $11 - 1 = 10$ e $17 - 1 = 16$ são todos divisores de $561 - 1 = 560$. Pelo fato demonstrado anteriormente, $a^{561} \equiv a \pmod 3$, $a^{561} \equiv a \pmod{11}$ e $a^{561} \equiv a \pmod{17}$. Concluímos que $a^{561} \equiv a \pmod{561}$.

Analogamente, fatoramos $1105 = 5 \cdot 13 \cdot 17$ e observamos que $5 - 1 = 4$, $13 - 1 = 12$ e $17 - 1 = 16$ são todos divisores de $1105 - 1 = 1104$. Usando o fato demonstrado, $a^{1105} - a$ possui fatores 5, 13 e 17 implicando $a^{1105} \equiv a \pmod{1105}$.

Problema 0.61. *(A) Mostre que*

$$a^{12} \equiv b^{12} \pmod{91} \iff \text{mdc}(a, 91) = \text{mdc}(b, 91).$$

Solução

Fatorando $91 = 7 \cdot 13$. Sabemos que $\text{mdc}(a, 91) = 1, 7, 13$ ou 91 dependendo dos fatores que 7 ou 13 que a possui.

Veja que se $7 \mid a$, então $a^{12} \equiv 0 \pmod 7$ e caso contrário pelo Teorema de Euler-Fermat $a^6 \equiv 1 \pmod 7 \Rightarrow a^{12} \equiv 1 \pmod 7$. Em outras palavras, $a^{12} \equiv 0 \pmod 7 \iff \text{mdc}(a, 7) = 7$ e $a^{12} \equiv 1 \pmod 7 \iff \text{mdc}(a, 7) = 1$.

Analogamente, $a^{12} \equiv 0 \pmod{13} \iff \text{mdc}(a, 13) = 13$ e $a^{12} \equiv 1 \pmod{13} \iff \text{mdc}(a, 13) = 1$.

Temos $a^{12} \equiv b^{12} \pmod{91} \iff a^{12} \equiv b^{12} \pmod 7$ e $a^{12} \equiv b^{12} \pmod{13} \iff \text{mdc}(a, 7) = \text{mdc}(b, 7)$ e $\text{mdc}(a, 13) = \text{mdc}(b, 13)$. Mas $\text{mdc}(a, 7)$ e $\text{mdc}(a, 13)$ indicam

os fatores 91 que a possui e concluímos que $\text{mdc}(a,7) = \text{mdc}(b,7)$ e $\text{mdc}(a,13) = \text{mdc}(b,13) \iff \text{mdc}(a,91) = \text{mdc}(b,91)$.

Problema 0.62. *(P. Sabini) (OI) Mostre que entre os números da forma*

$$14, \quad 144, \quad 1444, \quad 14444, \quad 144\cdots44, \ldots$$

os únicos quadrados perfeitos são $144 = 12^2$ *e* $1444 = 38^2$.

Solução

Primeiro note que o quadrado de um número é par se, e somente se, o número é par. Em seguida, veja que um número par deixa resto 0 ou 2 na divisão por 4. Quando elevamos números com esses restos por 4 ao quadrado temos números da forma $(4k)^2 = 16k^2$ ou da forma $(4k+2)^2 = 16k^2 + 16k + 4$. Então todo quadrado perfeito par deixa resto 0 ou 4 na divisão por 16.

Veja que se um número é 1 seguido de $n \geq 4$ algarismos 4 então ele é da forma $144\ldots4 \cdot 10^4 + 4444$. Veja que $10^4 = 2^4 \cdot 5^4$ é múltiplo de 16 e esse número $144\ldots4 \cdot 10^4 + 4444 \equiv 12 \pmod{16}$. Pelo que vimos anteriormente nenhum quadrado perfeito deixa resto 12 na divisão por 16 e podemos concluir que 1 seguido de $n \geq 4$ algarismos 4 não é um quadrado perfeito.

Problema 0.63. *(OI) Seja* $f : \mathbb{N}_{>0} \to \mathbb{N}$ *uma função definida do conjunto dos inteiros positivos no conjunto dos números naturais tal que*

(a) $f(1) = 0$*;*

(b) $f(2n) = 2f(n) + 1$*;*

(c) $f(2n+1) = 2f(n)$.

Utilize a representação em base 2 *de* n *para encontrar uma fórmula não recursiva para* $f(n)$.

Solução

Seja n um inteiro positivo e k um inteiro tal que $2^k \leq n < 2^{k+1}$. Provaremos por indução em k que $f(n) = 2^{k+1} - 1 - n$.

Para $k = 0$ temos $f(1) = 0 = 2 - 1 - 1$. Para $k = 1$ temos $f(2) = 2f(1) + 1 = 1 = 4 - 1 - 2$ e $f(3) = 2f(1) = 0 = 4 - 1 - 3$. Suponha que a fórmula de $f(n)$ funcione para $n < 2^{k+1}$. Tome n tal que $2^{k+1} \leq n < 2^{k+2}$. Se n é par, então $n = 2m$ com $2^k \leq m < 2^{k+1}$. Nesse caso, $f(n) = 2f(m) + 1 = 2(2^{k+1} - 1 - m) + 1 = 2^{k+2} - 1 - n$. Se n é ímpar, então $n = 2m + 1$ com $2^k \leq< m < 2^{k+1}$ e $f(n) = 2f(m) = 2(2^{k+1} - 1 - m) = 2^{k+2} - 2 - 2m =$

$2^{k+2} - 1 - n$. Isso conclui a indução.
Observe que isso nos dá uma forma não recursiva, pois $k = \lfloor log_2 n \rfloor$ e $f(n) = 2^{k+1} - 1 - n$. Porém, podemos ver o que isso significa na base 2. Temos um número n com $k+1$ dígitos e subtraímos ele de um números com $k+1$ dígitos 1. Na base 2 isso tranforma cada 1 em 0 e cada 0 em 1. Então $f(n)$ é o número obtido a partir de n trocando todos os dígitos na base 2.

Problema 0.64. *(OI) Mostre que todo número racional positivo pode ser escrito de maneira única na forma*

$$\frac{a_1}{1!} + \frac{a_2}{2!} + \cdots + \frac{a_k}{k!}$$

onde:

$$0 \leq a_1, \quad 0 \leq a_2 < 2, \quad 0 \leq a_3 < 3, \quad \ldots, \quad 0 < a_k < k.$$

Solução

Primeiro provaremos que existe uma representação e depois provaremos que é única. Seja $\frac{p}{q}$ um racional. Seja m o menor inteiro positivo tal que $q \mid m!$. Tal inteiro existe, pois $q \mid q!$. Existe um inteiro t tal que $\frac{p}{q} = \frac{pt}{m!}$. Fazemos a divisão euclidiana de pt por m encontramos quociente q_m e resto a_m tais que $pt = mq_m + a_m$ e $0 \leq a_m < m$. Daí $\frac{p}{q} = \frac{mq_m + a_m}{m!} = \frac{q_m}{(m-1)!} + \frac{a_m}{m!}$. Podemos repetir o processo mais $m-1$ vezes e obter $\frac{p}{q} = \frac{a_1}{1!} + \frac{a_2}{2!} + \cdots + \frac{a_m}{m!}$ com $a_1 \geq 0$ e $i > a_i \geq 0$ para $i = 2, \ldots, m$.
Para provar a unicidade suponha que existem duas representações distintas para $\frac{p}{q}$ e seja k o maior índice que aparece nessas representações. Podemos completar com zero para termos a mesma quantidade de termos nas duas representações.

$$\frac{a_1}{1!} + \frac{a_2}{2!} + \cdots + \frac{a_k}{k!} = \frac{b_1}{1!} + \frac{b_2}{2!} + \cdots + \frac{b_k}{k!}$$

Seja i o menor índice tal que $a_i \neq b_i$. Suponha sem perda de generalidade que $a_i > b_i$. Temos assim

$$\frac{1}{i!} \leq \frac{a_i - b_i}{i!} = \frac{b_{i+1} - a_{i+1}}{(i+1)!} + \frac{b_{i+2} - a_{i+2}}{(i+2)!} + \cdots + \frac{b_m - a_m}{m!} \leq \frac{i}{(i+1)!} + \frac{i+1}{(i+2)!} + \cdots + \frac{m-1}{m!}$$

Pela identidade $\frac{1}{(x-1)!} - \frac{1}{x!} = \frac{x-1}{x!}$ podemos calcular essa soma e obter

$$\frac{1}{i!} \leq \frac{1}{i!} - \frac{1}{m!} < \frac{1}{i!}$$

Que é uma contradição.
Concluímos que para todo racional positivo existe exatamente uma representação satisfazendo as condições.

Problema 0.65 (OBM1991)**.** *(OI) Demonstre que existem infinitos múltiplos de* 1991 *que são da forma* 19999 . . . 99991.

Solução

Observe que o número 19999 . . . 99991 formado por n algarismos pode ser escrito como

$$19999\ldots99991 = 2\cdot 10^{n+1} - 9$$

Queremos infinitos x tal que $2\cdot 10^x \equiv 9 \pmod{1991}$. Sabemos que para $x = 3$ essa congruência é verdadeira e que pelo Teorema de Euler-Fermat se $\text{mdc}(1991, 10) = 1$ então $10^{\varphi(1991)} \equiv 1 \pmod{1991}$. Logo, podemos tomar $x = 3 + \varphi(1991)k$ para qualquer k inteiro não negativo, pois

$$2\cdot 10^{3+\varphi(1991)k} - 9 \equiv 2\cdot 10^3 \cdot (10^{\varphi(1991)})^k - 9 \equiv 2\cdot 10^3 - 9 \equiv 0 \pmod{1991}.$$

Problema 0.66 (IMO1983)**.** *(OA) É possível escolher 1983 inteiros positivos distintos, todos menores que* 10^5*, tal que não existam três que sejam termos consecutivos de uma progressão aritmética?*

Usar base 3*.*

Solução

Tomaremos inteiros positivos n menores que 10^5 que possuem apenas 0 e 1 na representação na base 3. Como $10^5 = (12002011201)_3$. Podemos escolher cada um dos 11 algarismos para ser 0 ou 1, pois o número formado por 11 algarismos 1 na base 3 é menor que 10^5. Excluindo o 0 em que todas as escolhas são 0 temos $2^11 - 1 = 2047$ números. Isso já é maior que 1983, então basta excluir o excesso.
Veja que três números x, y e z estão em progressão aritmética se, e somente se, $x + z = 2y$. Se três dos nossos 2047 números estão em progressão aritmética então $2y$ possui apenas 0 e 2 na base 3. Veja que cada posição na representação de $x + z$ na base 3 é 0 quando ambos tem 0 nessa posição, 1 quando um deles tem 0 e o outro 1 e 2 quando ambos tem 1. Dessa forma, $x + z = 2y$ para esses números implica que eles possuem os mesmos dígitos em cada posição na base 3 e $x = y = z$. Logo, entre nossos 2047 números não existem três que sejam termos consecutivos de uma progressão aritmética.

Problema 0.67. *(OI) Seja* $S(n)$ *a soma dos dígitos de* n*. Encontre* $S(S(S(2^{2^5} + 1)))$.

Solução

Por congruência módulo 9, sabemos que $S(n) \equiv n \pmod 9$. Então o número desejado satisfaz a congurência a seguir.

$$S(S(S(2^{2^5} + 1))) \equiv 2^{32} + 1 \equiv (2^3)^{10}\cdot 2^2 + 1 \equiv (-1)^{10}\cdot 4 + 1 \equiv 5 \pmod 9$$

Além disso, veja que $2^{32} < (2^3)^{11} < 10^{11}$ tem no máximo 11 algarismos e $S(2^{2^5}+1) \leq 9 \cdot 11 = 99$. Agora podemos seguir limitando as somas dos dígitos $S(S(2^{2^5}+1)) \leq 9+9 = 18$ e $S(S(S(2^{2^5}+1))) \leq 1+8 = 9$. O único inteiro positivo menor que ou igual a 9 que é congruente a 5 módulo 9 é o próprio 5. Concluímos que $S(S(S(2^{2^5}+1))) = 5$.

Problema 0.68 (China2003). *(OI) Encontre todas as ternas (d,m,n) de inteiros positivos tais que d^m+1 divide d^n+203.*

Solução

Vamos representar as soluções por triplas (d,m,n).

Se $d = 1$ a divisibilidade é verdadeira para quaisquer inteiros positivos m e n. Temos soluções $(1,m,n)$. Se $m = 1$ então $d^n+203 \equiv (-1)^n+203 \pmod{d+1}$. Se n par, então $d+1 \mid 204$ e temos $d = 1,2,3,5,11,16,33,50,67,101$ ou 203. Para cada um deles temos solução $(d,1,2k)$. Se n ímpar, então $d+1 \mid 202$ e temos $d = 1,100$ ou 201. Temos duas soluções $(100,1,2k+1)$ e $(201,1,2k+1)$.

De agora em diante consideraremos $d \geq 2$ e $m \geq 2$. Faremos três casos.

(i) Se $n < m$, então

$$d^n+203 \geq d^m+1 \geq d^{n+1}+1 \Rightarrow 202 \geq d^n(d-1).$$

Temos os seguintes casos:
Se $d = 2$ então $1 \leq n \leq 7$.
Se $d = 3$ então $1 \leq n \leq 4$.
Se $d = 4$ então $1 \leq n \leq 3$.
Se $d = 5$ então $1 \leq n \leq 2$.
Se $d = 6$ então $1 \leq n \leq 2$.
Se $7 \leq n \leq 14$ então $n = 1$.
Para $n \geq 15$, então $d^n(d-1) \geq 15 \cdot 14 = 210 > 202$ e não temos soluções.
Testando os casos temos soluções $(2,2,1)$, $(2,3,2)$ e $(5,2,1)$.

(ii) Se $n = m$, então $d^m+1 \mid 202$ e temos soluções $d^m = 1,100$ ou 201 que só tem a solução $(10,2,2)$ com $d \geq 2$ e $m \geq 2$.

(iii) Se $n > m$, então $d^n \equiv d^{n-m} \cdot d^m \equiv -d^{n-m} \pmod{d^m+1}$ e temos $d^m+1 \mid d^{n-m}-203$.

(a) Se $d^{n-m} < 203$, então considere $n-m = s \geq 1$ e $d^m+1 \mid 203-a^s$. Veja que $203-a^s \geq a^m+1 \Rightarrow 202 \geq d^m+d^s \geq d^s(d+1)$.
Como vimos antes podemos limitar as possibilidades para $d \leq 14$ e testar. As triplas (d,m,s) que satisfazem a divisibilidade são $(2,2,3)$, $(2,6,3)$, $(2,4,4)$,

$(2,3,5)$, $(2,2,7)$, $(3,2,1)$, $(4,2,2)$, $(5,2,3)$ e $(8,2,1)$.
E isso nos dá as seguintes soluções (d,m,n): $(2,2,5)$, $(2,6,9)$, $(2,4,8)$, $(2,3,8)$, $(2,2,9)$, $(3,2,3)$, $(4,2,4)$, $(5,2,5)$ e $(8,2,3)$.

(b) Se $d^{n-m} = 203$, então $d = 203$, $n-m = 1$ e temos a solução $(203, m, m+1)$ com $m \geq 2$.

(c) Se $d^{n-m} > 203$, então $d^m + 1 \mid d^{n-m} - 203 \Rightarrow d^m < d^{n-m} \Rightarrow n \geq 2m$. Usando novamente que $d^m \equiv -1 \pmod{d^m+1}$ temos $d^m + 1 \mid d^{n-2m} + 203$. Nesse caso (d,m,n) é solução se, e somente se, $(d,m,n-2m)$ também é solução.

Concluímos que as soluções com $d \geq 2$ e $m \geq 2$ são $(2,2,4k+1)$, $(2,3,6k+2)$, $(2,4,8k+8)$, $(2,6,12k+9)$, $(3,2,4k+3)$, $(4,2,4k+4)$, $(5,2,4k+1)$, $(8,2,4k+3)$, $(10,2,4k+2)$ e $(203,m,(2k+1)m+1)$, onde k é um inteiro não negativo qualquer e $m \geq 2$ um inteiro.

Problema 0.69. *(A) Seja $p > 2$ um número primo. Demonstre que*

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

Solução

Pelo Teorema de Wilson sabemos que $(p-1)! \equiv -1 \pmod{p}$. Para $k > \frac{p-1}{2}$ podemos trocar k por $-(p-k) \equiv k \pmod{p}$ com $p-k < \frac{p+1}{2}$. Sendo $\frac{p-1}{2}$ fatores -1 temos.

$$-1 \equiv (p-1)! \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 (-1)^{(p-1)/2} \pmod{p}$$

$$\Rightarrow \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

Problema 0.70 (Austrian-Polish1996)**.** *(OA) Mostre que não existem inteiros não negativos m, n tais que $m! + 48 = 48(m+1)^n$.*

Solução

Esta solução foi consultada em [1].
Suponha que existem m e n. Veja que $48 \mid m! \Rightarrow m \geq 6$. Sabe-se que $\frac{6!}{48} = 15$. Para $m = 6$ e $m = 7$ as equações são

$$\frac{6!}{48} + \frac{48}{48} = 7^n \Leftrightarrow 15 + 1 = 7^n$$

$$\frac{7!}{48} + \frac{48}{48} = 8^n \Leftrightarrow 105 + 1 = 8^n$$

Para ambas não existe solução n. Para $m \geq 8$ o número $\frac{m!}{48}$ possui todos os fatores primos menores que ou iguais a m. Se $m+1$ não é primo, então ele tem um divisor

primo p que divide $\frac{m!}{48}$ e não pode dividir $\frac{m!}{48}+1$. Se $m+1$ é primo, então pelo Teorema de Wilson sabemos que $m+1 \mid m!+1$ e pela equação fornecida $m+1 \mid m!+48$ implicando que $m+1 \mid 47 \Rightarrow m+1=47 \Rightarrow m=46$. Resta mostrar que $\frac{46!}{48}+1$ não é uma potência de 47.

Para isso usaremos módulo 53. Pelo Teorema de Wilson $52! \equiv -1 \pmod{53}$ e sabemos que os inversos módulo 53 de 6, 5, 4, 3 e 2 são 9, 32, 40, 18 e 27, respectivamente. Daí,

$$52! \equiv 46! \cdot (-6) \cdot (-5) \cdot (-4) \cdot (-3) \cdot (-2) \cdot (-1) \pmod{53}$$

$$\Rightarrow 46! \equiv 9 \cdot 32 \cdot 40 \cdot 18 \cdot 27 \cdot (-1) \pmod{53}.$$

Veja que $9 \cdot 18 \equiv 3 \cdot 54 \equiv 3 \pmod{53}$, $32 \cdot 40 \equiv 160 \cdot 8 \equiv 8 \pmod{53}$ e $27 \cdot (-1) \equiv 26 \pmod{53}$. Isso nos leva a

$$\frac{46!}{48}+1 \equiv \frac{3 \cdot 8 \cdot 26}{48}+1 \equiv 14 \pmod{53}.$$

Observe as congruências das potências de $47 \equiv -6 \pmod{53}$ módulo 53.

$$(47^1, 47^2, 47^3, 47^4, 47^5, 47^6, 47^7, 47^8, 47^9, 47^{10}, 47^{11}, 47^{12}, 47^{13}) \equiv$$

$$\equiv (47, 36, 49, 24, 15, 16, 10, 46, 42, 13, 28, 44, 1) \pmod{53}$$

Temos $47^{13} \equiv 1 \pmod{53}$ e $47^n \equiv 47^{13q+r} \equiv 47^r \pmod{53}$ e esses são todas congruências possíveis módulo 53.

Como 14 não está entre os possíveis valores podemos concluir que $\frac{46!}{48}+1$ não é uma potência de 47.

Problema 0.71. *(OA) Seja p um número primo. Demonstre que $(p-1)!+1$ é uma potência de p se, e somente se, $p = 2$, 3 ou 5.*

Solução

Suponha para $p > 5$ que $(p-1)!+1 = p^k$ para um inteiro positivo k. Temos

$$(p-1)! = p^k - 1 = (p-1)(p^{k-1} + p^{k-2} + \cdots + p + 1)$$

$$\Rightarrow (p-2)! = p^{k-1} + p^{k-2} + \cdots + p + 1$$

Note que para $p > 5$ temos $p-2 > \frac{p-1}{2} > 2 > 1$ e $p-1 \mid (p-2)!$. Então módulo $p-1$ temos

$$0 \equiv p^{k-1} + p^{k-2} + \cdots + p + 1 \equiv 1^{k-1} + 1^{k-2} + \cdots + 1 + 1 \equiv k \pmod{p-1} \Rightarrow p-1 \mid k$$

A partir disso, temos as desigualdades a seguir.

$$p^k \geq p^{p-1} > (p-1+1)(p-2)(p-3)\ldots 2 \cdot 1 > (p-1)!+1$$

Portanto, para p primo com $p > 5$ o número $(p-1)!+1$ não é potência de p.

Problema 0.72. *(OA) Demonstre que para todo número primo $p > 3$, o número $\binom{np}{p} - n$ é divisível por p^{3+r} onde p^r é a maior potência de p que divide n.*

Solução

Veja que $\binom{np}{p} - n = \frac{np}{p}\binom{np-1}{p-1} - n = n\left(\binom{np-1}{p-1} - 1\right)$. Então provar que $\binom{np}{p} - n$ é divisível por p^{r+3} é equivalente a provar que $\binom{np-1}{p-1} - 1$ é divisível por p^3. Veja que

$$\binom{np-1}{p-1} - 1 = \frac{(np-1)(np-2)\cdots(np-(p-1)) - (p-1)!}{(p-1)!}$$

O denominador não possui fatores p e o problema passa a ser provar que o numerador possui 3 ou mais fatores p. Veja que

$$(np-1)(np-2)\cdots(np-(p-1)) - (p-1)! \equiv$$

$$\equiv n^2p^2(-1)^{p-3}S_{p-3} + np(-1)^{p-2}S_{p-2} + (-1)^{p-1}S_{p-1} - (p-1)! \pmod{p^3}$$

Onde cada S_i é a soma dos produtos de i números de 1 até $p-1$. Como $S_{p-1} = (p-1)!$ e $(-1)^{p-1} = 1$, pois p é ímpar, os dois últimos termos se cancelam. Observe que $S_{p-2} = (p-1)!\left(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{p-1}\right)$. Pelo Teorema de Wolstenholme, se $\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{p-1} = \frac{N}{D}$, então $p^2 \mid N$. Com isso, $np(-1)^{p-2}S_{p-2} \equiv 0 \pmod{p^3}$. Cada parcela de S_{p-3} é o produto de todos os números de 1 até $p-1$ com exceção de dois fatores i e j. Denotaremos por r_i e r_j os inversos multiplicativos módulo p de i e j de 1 até $p-1$, ou seja, $ir_i \equiv jr_j \equiv 1 \pmod{p}$. Então multiplicando por $ir_ijr_j \equiv 1 \pmod{p}$ cada parcela é congruente módulo p a $(p-1)!\,r_ir_j \equiv -r_ir_j \pmod{p}$. Observe que todos os números de 1 até $p-1$ aparecem exatamente uma vez entre os r_i e temos $\sum_{i=1}^{p-1} r_i = 1 + 2 + \cdots + p - 1 = \frac{p(p-1)}{2} \equiv 0 \pmod{p}$. Temos

$$2S_{p-3} \equiv \sum_{1\le i<j\le p-1} -2r_ir_j \equiv \sum_{i=1}^{p-1} -r_i(\sum_{j=1}^{p-1}(r_j) - r_i) \equiv \sum_{i=1}^{p-1} r_i^2 \pmod{p}$$

Temos $\sum_{i=1}^{p-1} r_i^2 = \sum_{i=1}^{p-1} i^2 = \frac{(p-1)p(2p-1)}{6} \equiv 0 \pmod{p} \Rightarrow p \mid S_{p-3}$ para $p > 3$. Logo, $n^2p^2(-1)^{p-3}S_{p-3} \equiv 0 \pmod{p^3}$. Portanto, temos

$$p^3 \mid (np-1)(np-2)\cdots(np-(p-1)) - (p-1)! \Rightarrow p^3 \mid \binom{np-1}{p-1} - 1 \Rightarrow p^{r+3} \mid \binom{np}{p} - n.$$

Problema 0.73. *(A) Demonstre que*

$$\sum_{1\le k\le n, \mathrm{mdc}(n,k)=1} k = \frac{n\varphi(n)}{2}.$$

Solução

Para $n = 1$ a igualdade não é verdadeira, pois o lado esquerdo é 1 e o direito é $\frac{1}{2}$. Vamos provar que vale para $n \geq 2$. Para $n = 2$ a igualdade é verdadeira, pois $1 = \frac{2 \cdot 1}{2}$. Para $n > 2$ temos $\text{mdc}(n, k) = 1 \Leftrightarrow \text{mdc}(n, n-k) = 1$, pois para cada fator primo p de n se $p \mid k$ então $p \mid n - k$ e vice-versa. Além disso, os números são distintos $k = n - k \Leftrightarrow k = \frac{n}{2}$ e para $n > 2$ temos $\text{mdc}(n, \frac{n}{2}) = \frac{n}{2} > 1$. Portanto, para $n > 2$ o número $\varphi(n)$ é par e podemos formar $\frac{\varphi(n)}{2}$ pares de números $(k, n-k)$ que somam n. Concluímos que a soma dos números menores que n primos com n é $\frac{\varphi(n)}{2} \cdot n = \frac{n\varphi(n)}{2}$.

Problema 0.74. *(OI) Demonstre que se* $\text{mdc}(a, b) = 1$*, então todos os divisores primos de* $a^2 + b^2$ *são da forma* $4k + 1$.

Utilize o teorema de Euler-Fermat.

Solução

Seja p um divisor primo de $a^2 + b^2$. Se $p \mid a$ então $p \mid a^2 \Rightarrow p \mid b^2 \Rightarrow p \mid b$ e a e b não seriam primos entre si. Logo p não divide a e p não divide b. Se $p = 2$ então $p \mid 1^2 + 1^2$ e temos uma exceção. Para p ímpar o número $\frac{p-1}{2}$ é inteiro e podemos manipular a congruência a seguir.

$$p \mid a^2 + b^2 \Rightarrow a^2 \equiv -b^2 \pmod{p} \Rightarrow (a^2)^{\frac{p-1}{2}} \equiv (-b^2)^{\frac{p-1}{2}} \pmod{p}$$

Se $p \equiv 3 \pmod 4$ então $\frac{p-1}{2}$ é um inteiro positivo ímpar e pelo Teorema de Euler-Fermat:

$$1 \equiv a^{p-1} \equiv -b^{p-1} \equiv -1 \pmod{p} \Rightarrow p \mid 2.$$

Como isso é uma contradição, não há nenhum primo p com $p \equiv 3 \pmod 4$ tal que $p \mid a^2 + b^2$ e esse número só tem fatores primos $4k + 1$ e o 2 que é exceção.
Outra forma de usar esse resultado é: se p é um primo, $p \equiv 3 \pmod 4$ e $p \mid a^2 + b^2$ então $p \mid a$ e $p \mid b$.

Problema 0.75. *(OI) Demonstre que existem infinitos primos da forma* $4k + 1$.

Solução

Suponha que existe uma quantidade finita de primos $4k + 1$. Se a quantidade é finita, então podemos listar todos os primos $4k + 1$: $p_1, p_2, \ldots, p_n$. Considere o número $N = (2p_1p_2 \ldots p_n)^2 + 1^2$. Pelo Teorema Fundamental da Aritmética N pode ser fatorado em primos. Pelo problema anterior do fato de N ser ímpar e a soma dos quadrados de dois números primos entre si sabemos que ele só possui fatores primos $4k + 1$. Porém, para cada p_m sabemos que $p_m \mid N - 1$ implicando que $p_m \nmid N$. Então N possui um fator

primo $4k+1$ que não está listado gerando uma contradição. Portanto, existem infinitos primos da forma $4k+1$.

Problema 0.76. *(OI) Sejam m, n inteiros positivos. Demonstre que $4mn-m-n$ nunca pode ser o quadrado de um número inteiro.*

Solução

Suponha que $4mn-m-n$ seja o quadrado de um número inteiro x. Temos

$$4mn-m-n=x^2 \Leftrightarrow 16mn-4m-4n+1=4x^2+1 \Leftrightarrow (4m-1)(4n-1)=(2x)^2+1^2$$

Veja que $4m-1 \equiv 3 \pmod 4$ é ímpar e não pode ter apenas fatores primos da forma $4k+1$, pois o produto de números $4k+1$ é congruente a 1 módulo 4. Existe um primo p da forma $4k+3$ tal que $p \mid 4m-1$. Isso implica que $p \mid (2x)^2+1^2$ que é a soma dos quadrados de dois números primos entre si implicando que $p \mid 2x$ e $p \mid 1$ que é uma contradição. Portanto, não existem m e n inteiros positivos tais que $4mn-m-n$ seja um quadrado perfeito.

Problema 0.77 (IMO1986)**.** *(OA) Seja d um número positivo distinto de 2, 5 e 13. Demonstre que é possível encontrar dois números diferentes a e b que pertençam ao conjunto $\{2,5,13,d\}$ tais que $ab-1$ não é um quadrado perfeito.*

Solução

Veja que $2\cdot 5-1=3^2$, $2\cdot 13-1=5^2$ e $5\cdot 13-1=8^2$. Então provaremos que um dos números $ab-1$ usando o d não é quadrado perfeito. Suponha que existem inteiros positivos x, y e z tais que $2d-1=x^2$, $5d-1=y^2$ e $13d-1=z^2$. Como $2d-1$ é ímpar, então x é ímpar e $2d-1 \equiv x^2 \equiv 1 \pmod 8 \Rightarrow d \equiv 1 \pmod 4$. Com isso, os números $5d-1$ e $13d-1$ são pares e, portanto, y e z são pares. Existem inteiros positivos y_1 e z_1 tais que $y=2y_1$ e $z=2z_1$. Note que $z^2-y^2=(13d-1)-(5d-1)=8d \Rightarrow 4z_1^2-4y_1^2=8d \Rightarrow (z_1-y_1)(z_1+y_1)=2d$. Se z_1 e y_1 possuem paridades distintas temos z_1-y_1 e z_1+y_1 seriam ambos ímpares e $2d$ teria que ser ímpar, que é impossível. Se z_1 e y_1 possuem a mesma paridade, então z_1-y_1 e z_1+y_1 seriam ambos pares e $2d$ teria que ser múltiplo de 4, mas isso é ímpossível já que d é ímpar. Concluímos que um dos três números $2d-1$, $5d-1$ ou $13d-1$ não é um quadrado perfeito.

Problema 0.78. *(OI) Demonstre que se $p \mid (a^p-b^p)$, então $p^2 \mid (a^p-b^p)$.*

Solução

Vamos resolver o problema supondo que p é primo, pois existem contraexemplos

quando p não é primo. Por exemplo, $3^8 - 1^8$ é divisível por 8, mas não por 8^2.
Pelo Teorema de Euler-Fermat, $a \equiv a^p \equiv b^p \equiv b \pmod{p} \Rightarrow a \equiv b \pmod{p} \Rightarrow a = pt + b$ para algum inteiro t. Podemos expandir $a^p - b^p$ pelo Binômio e Newton

$$a^p - b^p = (pt)^p + \cdots + \binom{p}{2}(pt)^2 b^{p-2} + \binom{p}{1}(pt)^1 b^{p-1} + b^p - b^p =$$

$$= (pt)^p + \cdots + \binom{p}{2}(pt)^2 b^{p-2} + p^2 t b^{p-1} \equiv 0 \pmod{p^2}$$

Usamos que $\binom{p}{1} = p$ e que para $k \geq 2$ temos $p^2 \mid \binom{p}{k}(pt)^k b^{p-k}$ já que esse número tem pelo menos k fatores p.

Problema 0.79 (IMO1984). *(OA) Encontre um par de inteiros positivos a, b tais que $ab(a+b)$ não é divisível por 7, mas $(a+b)^7 - a^7 - b^7$ é divisível por 7^7.*

Solução
Pelo Binômio de Newton temos

$$(a+b)^7 - a^7 - b^7 = 7a^6 b + 21a^5 b^2 + 35a^4 b^3 + 35a^3 b^4 + 21a^2 b^5 + 7ab^6 =$$

$$= 7ab(a^5 + b^5 + 3ab(a^3 + b^3) + 5a^2 b^2(a+b))$$

Podemos fatorar $a^5 + b^5$ e $a^3 + b^3$ por $a + b$ e obter

$$(a+b)^7 - a^7 - b^7 = 7ab(a+b)(a^4 - a^3 b + a^2 b^2 - ab^3 + b^4 + 3a^3 b - 3a^2 b^2 + 3ab^3 + 5a^2 b^2) =$$

$$= 7ab(a+b)(a^2 + ab + b^2)^2.$$

A partir dessa fatoração, para que $7^7 \mid (a+b)^7 - a^7 - b^7$ basta que $7^3 \mid a^2 + ab + b^2$.
Observe que $18^2 + 18 \cdot 1 + 1^2 = 343 = 7^3$ e temos a solução $(a, b) = (18, 1)$.

Problema 0.80 (OIbM2001). *(OI) Demonstre que para cada inteiro positivo n existe um inteiro m tal que 2^m tem no mínimo $\frac{2}{3}n - 1$ zeros entre seus últimos n algarismos em notação base 10.*

Solução
Pelo Teorema de Euler-Fermat,

$$2^{\varphi(5^n)} \equiv 1 \pmod{5^n} \Rightarrow 2^{\varphi(5^n)+n} \equiv 2^n \pmod{10^n}$$

Tomando $m = \varphi(5^n) + n = 4 \cdot 5^{n-1} + n$ temos que os últimos n algarismos de 2^m são formados por zeros e pelos algarimos de 2^n.
Se n é múltiplo de 3 temos $2^n = 8^{\frac{n}{3}} < 10^{\frac{n}{3}}$ que possui $\frac{n}{3} + 1$ algarismos. Nesse caso, 2^m

possui no mínimo $n-(\frac{n}{3}+1)=\frac{2n}{3}-1$ zeros entre seus últimos n algarismos.
Se n não é múltiplo de 3, para $x=1$ ou 2 temos $n+x$ múltiplo de 3 e $2^n < 2^{n+x} = 8^{\frac{n+x}{3}} < 10^{\frac{n+x}{3}}$ que é o menor número com $\frac{n+x}{3}+1$ algarimos. Daí, 2^n no máximo $\frac{n+x}{3}$ algarismos e 2^m possui no mínimo $n-\frac{n+x}{3}=\frac{2n}{3}-\frac{x}{3}>\frac{2n}{3}-1$ zeros entre seus últimos n algarismos.

Problema 0.81 (IMO2003)**.** *(OA) Seja p um número primo ímpar. Demonstre que existe um primo q tal que para todo n, o número n^p-p não é divisível por q.*

Solução

Seja q um fator primo de $N=\frac{p^p-1}{p-1}=p^{p-1}+\cdots+p^2+p+1$. Podemos tomar q de modo que $q\not\equiv 1 \pmod{p^2}$, pois se todos os fatores primos de N fossem congruentes a 1 módulo p^2 o produto das potências deles seria congruente a 1 módulo p^2, mas $N\equiv p+1 \pmod{p^2}$. Note que se $q\mid p-1$ então $p\equiv 1 \pmod q \Rightarrow 0\equiv p^{p-1}+\cdots+p^2+p+1\equiv p \pmod q \Rightarrow q\mid p \Rightarrow q=p$. Porém, isso é uma contradição, pois $N\equiv 1 \pmod p$ e $N\equiv 0 \pmod q$.
Pelo Teorema de Euler-Fermat, sabemos que $p^{q-1}\equiv 1 \pmod q$ e $q\mid p^{q-1}-1$. Daí, temos que $q\mid \operatorname{mdc}(p^p-1,p^{q-1}-1)=p^{\operatorname{mdc}(p,q-1)}-1$. O primo p só tem dois divisores 1 e p. Já vimos que 1 não serve, pois $q\nmid p-1$, então tem que ser p e $\operatorname{mdc}(p,q-1)=p \Rightarrow p\mid q-1$. Existe um inteiro positivo x tal que $q-1=px$.
Suponha que existe um inteiro n tal que $q\mid n^p-p$. Se $q\mid n$ então $q\mid p \Rightarrow q=p$ e já vimos que isso não é possível nesse problema. Se $q\nmid n$ então $p\equiv n^p \pmod q \Rightarrow p^x\equiv n^{px}\equiv n^{q-1}\equiv 1 \pmod q$. Mas isso implica $q\mid p^x-1$ e $q\mid \operatorname{mdc} p^p-1,p^x-1=p^{\operatorname{mdc}(p,x)}-1=p-1$ ou p^p-1. Novamente, lembramos que $q\nmid p-1$ e ficamos com $\operatorname{mdc}(p,x)=p \Rightarrow p\mid x$. Ora, mas isso nos leva a $q-1\equiv 0 \pmod{p^2} \Rightarrow q\equiv 1 \pmod{p^2}$. Mas por construção $q\not\equiv 1 \pmod{p^2}$ gerando uma contradição. Então o contrário da suposição é verdadeiro, ou seja, não existe n inteiro tal que n^p-p seja divisível por q.

Problema 0.82 (IMO1979)**.** *(OI) Sejam m e n inteiros positivos tais que*

$$\frac{m}{n}=1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots-\frac{1}{1318}+\frac{1}{1319}.$$

Mostre que m é divisível por 1979.

Solução

Manipulando o somatório temos

$$\frac{m}{n}=1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots+\frac{1}{1318}+\frac{1}{1319}-2\left(\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{1318}\right)$$

Cada fração $\frac{1}{2k}$ multiplicada por 2 cancela com $\frac{1}{k}$. Isso ocorre para $k = 1, 2, \cdots, 659$. Então,

$$\frac{m}{n} = \frac{1}{660} + \frac{1}{661} + \cdots + \frac{1}{1318} + \frac{1}{1319}.$$

Somando as frações nos extremos $\frac{1}{x} + \frac{1}{1979-x} = \frac{1979}{x(1979-x)}$. Temos

$$\frac{m}{n} = 1979 \left(\sum_{x=660}^{989} \frac{1}{x(1979-x)} \right)$$

A soma das frações do somatório é $\frac{N}{D}$ em que D é um divisor do produto dos núemros de 660 até 1319. O fator 1979 não se cancela com D, pois 1979 é primo e, portanto, relativamente primo com cada número menor que ele. Então m é igual a $1979N$ e é divisível por 1979.

Problema 0.83. *(OA) Seja p um número primo ímpar e sejam a e b inteiros não divisíveis por p tais que $p \mid a - b$. Mostre que $p^k \mid a^n - b^n \iff p^k \mid n(a-b)$.*

Solução

Suponha que $a - b$ possua $\alpha \geq 1$ fatores p e que n possua $\beta \geq 0$ fatores p. Veja que $n(a-b)$ possui exatamente $\alpha + \beta$ fatores p. Então basta provar que $a^n - b^n$ possui essa mesma quantidade de fatores p.

Podemos escrever a como $p^\alpha \cdot t + b$ com $p \nmid t$. Dessa forma,

$$a^n - b^n = (p^\alpha t + b)^n - b^n = (p^\alpha t)^n + \cdots + \binom{n}{2}(p^\alpha t)^2 b^{n-2} + \binom{n}{1}(p^\alpha t) b^{n-1}$$

O último termo é $np^\alpha t b^{n-1}$ e possui exatamente $\alpha + \beta$ fatores p. Se provarmos que todos os outros possuem pelo menos $\alpha + \beta + 1$ fatores p, então $a^n - b^n = p^{\alpha+\beta+1}x + p^{\alpha+\beta}y = p^{\alpha+\beta}(px + y)$ onde p não divide y.

Cada termo é da forma

$$\binom{n}{k}(p^\alpha t)^k b^{n-k} = \frac{n}{k}\binom{n-1}{k-1}(p^\alpha t)^k b^{n-k}$$

Se k não possui fatores p temos pelo menos $\beta + \alpha \cdot k \geq \alpha + \beta + 1$ para $k \geq 2$. Se k possui alguns fatores p. Seja r a quantidade de fatores p de k. Podemos escrever $k = p^r k_0$ tal que p não divide k_0. Nesse caso, a quantidade de fatores p é $\beta + \alpha \cdot k - r \geq \beta + \alpha \cdot p^r - r$. Mas para $p \geq 3$ e $r \geq 1$ sabemos que $p^r > r + 1$ e a quantidade de fatores p será maior que $\beta + \alpha(r+1) - r = \alpha + \beta + \alpha \cdot r - r = \alpha + \beta$. Então, de fato, para $k \geq 2$ cada termo tem pelo menos $\alpha + \beta + 1$ fatores p.

Portanto, $n(a-b)$ e $a^n - b^n$ possuem a mesma quantidade de fatores p e

$$p^k \mid a^n - b^n \iff p^k \mid n(a-b).$$

Problema 0.84. *(A) Sem usar computador (mas podendo usar calculadora) e sabendo que os fatores de n estão perto um do outro, use o método de Fermat para determinar os fatores de*

(a) $n = 62236177$.

(b) $n = 6218583803$.

Solução

(a) Pelo método de Fermat começamos testando $x_0 = \lfloor\sqrt{62236177}\rfloor + 1 = 7889$. Veja que $x_0^2 - 62236177 = 144 = 12^2$ e podemos fatorar o número

$$n = 62236177 = 7889^2 - 12^2 = (7889 - 12)(7889 + 12) = 7877 \cdot 7901.$$

(b) Novamente, começaremos pelo método de Fermat $x_0 = \lfloor\sqrt{6218583803}\rfloor + 1 = 78858$. Como $x_0^2 - 6218583803 = 361 = 19^3$ temos a fatoração

$$n = 6218583803 = 78858^2 - 19^2 = (78858 - 19)(78858 + 19) = 78839 \cdot 78877.$$

Problema 0.85. *(A) Fatore (sem usar computador)* 801621073 *sabendo que tem três fatores primos: um muito pequeno e os outros dois muito próximos.*

Solução

Primeiro testamos os menores primos possíveis. Veja que

$$801621073 \equiv +8 - 0 + 1 - 6 + 2 - 1 + 0 - 7 + 3 \equiv 0 \pmod{11}$$

Dividindo por 11 obtemos $801621073 = 11 \cdot 72874643$. Agora usaremos o método de Fermat para terminar de fatorar. Temos $x_0 = \lfloor\sqrt{72874643}\rfloor + 1 = 8537$. Temos $x_0^2 - 72874643 = 5276$ que não é um quadrado perfeito. Vamos para $x_1 = 8538$. Veja que $x_1^2 - 72874643 = 22801 = 151^2$. Daí,

$$72874643 = 8538^2 - 151^2 = (8538 - 151)(8538 + 151) = 8387 \cdot 8689.$$

A fatoração do número inicial em primos é

$$801621073 = 11 \cdot 8387 \cdot 8689.$$

Problema 0.86. *(A) Encontre os fatores de* 521827 *sabendo que é produto de dois primos e* $\varphi(521827) = 520056$.

Solução

Queremos encontrar dois primos p e q tais que $pq = 521827$ e $\varphi(521827) = 520056 \Rightarrow (p-1)(q-1) = pq - p - q + 1 = 520056 \Rightarrow p + q = 1772$. Usando a equação do segundo grau temos $(x-p)(x-q) = x^2 - (p+q)x + pq = x^2 - 1772x + 521827 = 0$. Temos $\Delta = (-1772)^2 - 4 \cdot 1 \cdot 521827 = 1052676 = 1026^2$ e $x = \frac{1772 \pm 1026}{2}$. Suponha sem perda de generalidade que $p > q$. As soluções são $p = \frac{1772+1026}{2} = 1399$ e $q = \frac{1772-1026}{2} = 373$. Portanto, a fatoração de 521827 em primos é $1399 \cdot 373$.

Problema 0.87. *(A) Sabendo que a chave pública de criptografia RSA são os números $N = 26549$ e $s = 101$, determine a chave privada.*

Solução

Comecemos fatorando $N = 26549$ através do método de Fermat. Temos $x_0 = \lfloor \sqrt{26549} \rfloor + 1 = 163$ e testamos os possíveis valores na tabela a seguir.

x_i	$\sqrt{x_i^2 - 26549}$
163	$\sqrt{20}$
164	$\sqrt{347}$
165	26

,

Assim, $N = 26549 = 165^2 - 26^2 = 139 \cdot 181$ e $\varphi(N) = (139-1)(181-1) = 24840$. A chave privada é a solução da congruência $101x \equiv 1 \pmod{24840}$. Podemos encontrá-la usando o Algoritmo de Euclides.

$$24840 = 101 \cdot 245 + 95$$

$$101 = 95 \cdot 1 + 6$$

$$95 = 6 \cdot 15 + 5$$

$$6 = 5 \cdot 1 + 1$$

$$5 = 1 \cdot 5 + 0$$

Temos que $\text{mdc}(24840, 101) = 1$ e podemos encontrar inteiros x e y tais que $101x + 24840y = 1$.

$$1 = 6 \cdot 1 + 5 \cdot (-1)$$

$$1 = 6 \cdot 1 + (95 + 6(-15)) \cdot (-1) = 6 \cdot 16 + 95 \cdot (-1)$$

$$1 = (101 \cdot 1 + 95 \cdot (-1)) \cdot 16 + 95 \cdot (-1) = 101 \cdot 16 + 95 \cdot (-17)$$

$$1 = 101 \cdot 16 + (24840 \cdot 1 + 101 \cdot (-245)) \cdot (-17) = 101 \cdot 4181 + 24840 \cdot (-17)$$

Logo $1 = 101 \cdot 4181 + 24840 \cdot (-17) \Rightarrow 101 \cdot 4181 \equiv 1 \pmod{24840}$ e a chave privada é $r = 4181$.

0.10 EQUAÇÕES LINEARES MÓDULO m

Problema 0.88. *(A) Determine a menor solução inteira positiva do sistema*

$$\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 5 \pmod 9 \\ x \equiv 2 \pmod 8. \end{cases}$$

Solução

As soluções da primeira congruência são da forma $x = 7x_1 + 3$ para algum inteiro x_1. Resolvendo na segunda congruência $7x_1 + 3 \equiv 5 \pmod 9 \Leftrightarrow 7x_1 \equiv 2 \pmod 9$ como $\text{mdc}(7,9) = 1$ podemos multiplicar os dois lados pelo inverso de 7 modulo 9 que é 4. Daí, $28x_1 \equiv x_1 \equiv 8 \pmod 9$. Temos que $x_1 = 9x_2 + 8$ e as soluções das duas primeiras congruências são da forma $x = 7(9x_2 + 8) + 3 = 63x_2 + 59$. Finalmente, usamos essa forma na terceira congruência $63x_2 + 59 \equiv 2 \pmod 8 \Leftrightarrow 63x_2 + 3 \equiv 2 \pmod 8 \Leftrightarrow 63x_2 \equiv -1 \pmod 8$. Veja que $\text{mdc}(63,8) = 1$ e 63 possui inverso módulo 8. Multiplicando os dois lados por -1 temos $x_2 \equiv 1 \pmod 8$ e $x_2 = 8x_3 + 1$. Concluímos que as soluções desse sistema de congruências é da forma

$$x = 63(8x_3 + 1) + 59 = 504x_3 + 122$$

para qualquer inteiro x_3.

A menor solução inteira positiva do sistema é $x_{min} = 504 \cdot 0 + 122 = 122$.

Problema 0.89. *(A) Determine todas as soluções do sistema*

$$\begin{cases} x \equiv 1 \pmod 6 \\ x \equiv 7 \pmod{10} \\ x \equiv 4 \pmod{33}. \end{cases}$$

Observe que o sistema não satisfaz as condições do teorema Chinês dos restos.

Solução

As soluções da primeira congruência são da forma $x = 6x_1 + 1$ para todo inteiro x_1. Substituindo na segunda $6x_1 + 1 \equiv 7 \pmod{10} \Leftrightarrow 6x_1 \equiv 6 \pmod{10}$. Como $\text{mdc}(6,10) = 2 > 1$ não podemos cancelar 6 na multiplicação, que matematicamente seria multiplicar pelo inverso de 6 e este não existe. Mas veja que $6x_1 \equiv 6 \pmod{10} \Leftrightarrow 6x_1 \equiv 6 \pmod 2$ e $6x_1 \equiv 6 \pmod 5$. Veja que $6x_1 \equiv 0 \equiv 6 \pmod 2$ para qualquer x_1.

Então resta analisar $6x_1 \equiv 6 \pmod 5 \Leftrightarrow x_1 \equiv 1 \pmod 5$, pois $\text{mdc}(6,5) = 1$ e 6 possui inverso multiplicativo em $\mathbb{Z}/(5)$. Logo, as soluções das duas primeiras congruências são da forma $x = 6(5x_2+1)+1 = 30x_2+7$. Seguimos para a terceira e última congruência do sistema $30x_2+7 \equiv 4 \pmod{33} \Leftrightarrow 30x_2+7 \equiv 4 \pmod 3$ e $30x_2+7 \equiv 4 \pmod{11}$. Veja que $30x_2+7 \equiv 0x_2+1 \equiv 1 \equiv 4 \pmod 4$ é verdadeira para todo x_2 inteiro. Já a outra congruência $30x_2+7 \equiv 4 \pmod{11} \Leftrightarrow -3x_2 \equiv -3 \pmod{11} \Leftrightarrow x_2 \equiv 1 \pmod{11}$. Vale lembrar que podemos cancelar o -3, pois $\text{mdc}(-3,11) = 1$. Portanto, as soluções desse sistema de congruências são os números da forma

$$x = 30(11x_3+1)+7 = 330x_3+37$$

para qualquer inteiro x_3.

Problema 0.90. *(A) Determine todas as soluções de* $x^2+x+18 \equiv 0 \pmod{42}$.

Solução

Fatorando $42 = 2\cdot 3\cdot 7$ temos $x^2+x+18 \equiv 0 \pmod{42} \Leftrightarrow x^2+x+18 \equiv 0 \pmod 2$, $x^2+x+18 \equiv 0 \pmod 3$ e $x^2+x+18 \equiv 0 \pmod 7$. Veja que módulo 2 a congruência é verdadeira para todo x, pois x ou $x+1$ é par e $x^2+x+18 \equiv x(x+1)+0 \equiv 0 \pmod 2$. Analisando módulo 3 temos $x^2+x+18 \equiv 0 \pmod 3 \Leftrightarrow x(x+1) \equiv 0 \pmod 3 \Leftrightarrow x \equiv 0 \pmod 3$ ou $x \equiv 2 \pmod 3$. No último passo usamos o fato de 3 ser primo e que um primo divide um produto se, e somente se, ele divide um dos fatores. Para o módulo 7 veja que $x^2+x+18 \equiv 0 \pmod 7 \Leftrightarrow x^2+x \equiv 3 \pmod 7$. Vamos multiplicar por 4 e somar 1 para montar o quadrado perfeito. Veja que isso conserva a equivalência das congruências, pois $\text{mdc}(4,7) = 1$. Daí, $(2x+1)^2 \equiv 4\cdot 3+1 \equiv 6 \pmod 7$. Por outro lado, veja que as possibilidades são $n \equiv 0,1,2,3,-3,-2,-1 \pmod 7 \Rightarrow n^2 \equiv 0,1,4,2,2,4,1 \pmod 7$. Então não há solução para esta congruência.
O conjunto solução dessa congruência é o conjunto vazio.

Problema 0.91. *(A) Quantos elementos tem* $(\mathbb{Z}/(210))^*$*? Quantos deles têm ordem* 24*?*

Solução

Por definição, o número de elementos de $(\mathbb{Z}/(210))^\times$ é $\varphi(210)$. Lembrando que se $\text{mdc}(m,n) = 1$ então $\varphi(mn) = \varphi(m)\varphi(n)$ temos

$$\varphi(210) = \varphi(2)\varphi(3)\varphi(5)\varphi(7) = 1\cdot 2\cdot 4\cdot 6 = 48.$$

Um elemento $a \in (\mathbb{Z}/(210))^\times$ tem ordem 24 quando $a^24 \equiv 1 \pmod{210}$ e $a^t \not\equiv 1 \pmod{210}$ para $1 \leq t < 24$. Em outras palavras a ordem é o menor expoente t tal que

a^t deixa resto 1 na divisão por 210.
Veja que mmc($\varphi(2), \varphi(3), \varphi(5), \varphi(7)$) = mmc$(1,2,4,6) = 12$. Se tomarmos um inteiro a tal que mdc$(a, 210) = 1$ podemos usar o Teorema de Euler-Fermat para provar que

$$a^1 \equiv 1 \pmod 2 \Rightarrow a^{12} \equiv 1 \pmod 2$$

$$a^2 \equiv 1 \pmod 3 \Rightarrow a^{12} \equiv 1 \pmod 3$$

$$a^4 \equiv 1 \pmod 5 \Rightarrow a^{12} \equiv 1 \pmod 5$$

$$a^6 \equiv 1 \pmod 7 \Rightarrow a^{12} \equiv 1 \pmod 7$$

então $a^{12} \equiv 1 \pmod{210}$. Concluímos que nenhum elemento tem ordem 24.
No capítulo 1 do livro há mais informações e resultados sobre ordem.

Problema 0.92. *(A) Resolver as equações lineares*

(a) $7x \equiv 12 \pmod{127}$

(b) $12x \equiv 5 \pmod{122}$

(c) $40x \equiv 64 \pmod{256}$

Solução

(a) Como mdc$(7, 127) = 1$ temos que 7 possui inverso módulo 127. Podemos determiná-lo pelo Algoritmo de Euclides

$$127 = 7 \cdot 18 + 1$$

Temos $7 \cdot 18 \equiv -1 \pmod{127} \Rightarrow 7 \cdot (-18) \equiv 1 \pmod{127}$. Multiplicando a congruência fornecida por (-18) a congruência é equivalente a

$$x \equiv 5 \cdot (-18) \equiv -90 \equiv 37 \pmod{127}.$$

As soluções são $x = 127k + 37$ para todo inteiro k.

(b) Não admite solução inteira, pois mdc$(12, 122) = 2 \nmid 5$.

(c) Veja que mdc$(40, 256) = 8$ e podemos dividir todos os números por 8.

$$40x \equiv 64 \pmod{256} \Leftrightarrow 5x \equiv 8 \pmod{32}.$$

Vale ressaltar que isso só possível porque $8 \mid 64$. Caso contrário não teríamos solução como aconteceu no item anterior.

Temos $\text{mdc}(5, 32) = 1$ e existe o inverso multiplicativo de 5 em $\mathbb{Z}/(32)$. Como $5 \cdot 13 \equiv 65 \equiv 1 \pmod{32}$ podemos multiplicar a congruência por 13 e obter

$$x \equiv 8 \cdot 13 \equiv 8 \pmod{32}.$$

Então as soluções são $x = 32k + 8$ para todo k inteiro.
Observe que esses números representam 8 congruências módulo $256 = 32 \cdot 8$, uma para cada resto de k na divisão por 8. Por exemplo, se k deixa resto 3 na divisão por 8 temos $k = 8q + 3$ e $x = 32(8q + 3) + 8 = 256q + 104$.

Problema 0.93. *(A) Resolver o sistema de congruências lineares*

$$\begin{aligned} x &\equiv 0 \pmod{7} \\ x &\equiv 1 \pmod{12} \\ x &\equiv -5 \pmod{17} \end{aligned}$$

Solução

As soluções da primeira congruência são da forma $x = 7x_1$. Substituindo essa forma na segunda e lembrando que se $\text{mdc}(7, 12) = 1$ então 7 possui inverso multiplicativo em $\mathbb{Z}/(7)$ temos $7x_1 \equiv -1 \pmod{12} \Leftrightarrow 49x_1 \equiv -7 \pmod{12} \Leftrightarrow x_1 \equiv -7 \equiv 5 \pmod{12}$. Assim, $x_1 = 12x_2 + 5$ e as soluções das duas primeiras congruências são da forma $x = 7(12x_2 + 5) = 84x_2 + 35$. Substituindo essa forma na terceira e, novamente, lembrando que se $\text{mdc}(84, 17) = 1$ então 84 possui inverso multiplicativo em $\mathbb{Z}/(17)$ temos $84x_2 + 35 \equiv -5 \pmod{17} \Leftrightarrow 84x_2 \equiv -40 \equiv -6 \pmod{17} \Leftrightarrow x_2 \equiv 6 \pmod{17}$, pois $84 \equiv -1 \pmod{17}$. Concluímos que as soluções do sistema de congruências são da forma

$$x = 84(17x_3 + 6) + 35 = 1428x_3 + 539.$$

para qualquer inteiro x_3.

Problema 0.94. *(OI) Um inteiro positivo n é chamado de* auto-replicante *se os últimos dígitos de n^2 formam o número n. Por exemplo, 25 é auto-replicante pois $25^2 = 625$. Determine todos os números auto-replicantes com exatamente 4 dígitos.*

Solução

Observe que n é auto-replicante de 4 dígitos se, e somente se, n possui 4 dígitos e satisfaz $x^2 \equiv x \pmod{10^4}$, pois os 4 últimos dígitos formam o resto na divisão por 10^4. Usando a fatoração em primos temos $x^2 \equiv x \pmod{10^4}$ se, e somente se, é solução do sistema

$$x^2 \equiv x \pmod{2^4}$$

$$x^2 \equiv x \pmod{5^4}$$

Veja que $x^2 - x = x(x-1)$ então cada uma das congruências módulo potência de primo se torna x congruente a 0 ou 1. Faremos as quatro combinações possiveis

(i) $x \equiv 0 \pmod{16}$ e $x \equiv 0 \pmod{625} \Leftrightarrow x \equiv 0 \pmod{10000} \Leftrightarrow x = 10000q$ e não temos solução de 4 dígitos.

(ii) $x \equiv 0 \pmod{16}$ e $x \equiv 1 \pmod{625}$. Da segunda congruência $x = 625k + 1$ e testando na primeira $625k + 1 \equiv 0 \pmod{16} \Leftrightarrow k \equiv 15 \pmod{16}$. As soluções são da forma $x = 625(16q + 15) + 1 = 10000q + 9376$. Temos uma solução auto-replicante de 4 dígitos $n = 9376$.

(iii) $x \equiv 1 \pmod{16}$ e $x \equiv 0 \pmod{625}$. Da segunda congurência $x = 625k$ e testando na primeira $625k \equiv 1 \pmod{16} \Leftrightarrow k \equiv 1 \pmod{16}$. As soluções são da forma $x = 625(16q + 1) = 10000q + 625$. Não temos solução de 4 dígitos.

(iv) $x \equiv 1 \pmod{16}$ e $x \equiv 1 \pmod{625} \Leftrightarrow x \equiv 1 \pmod{10000} \Leftrightarrow x = 10000q + 1$ e não temos solução de 4 dígitos.

O único número auto-replicante de 4 dígitos é 9376.

Problema 0.95. *(OI) Sejam $a, n \in \mathbb{N}_{>0}$ e considere a sequência (x_k) definida por $x_1 = a$, $x_{k+1} = a^{x_k}$ para todo $k \in \mathbb{N}$. Demonstre que existe $N \in \mathbb{N}$ tal que $x_{k+1} \equiv x_k \pmod{n}$ para todo $k \geq N$.*

Solução

Vamos provar por indução em n. Para $n = 1$ o resultado é imediato. Para $n = 2$, se a é par, os termos da sequência são todos 0 módulo 2 e, se a é ímpar, são todos 1 módulo 2. Suponha que o resultado é verdadeiro para todo inteiro positivo n com $n < m$. Em outras palavras, para todo inteiro positivo a existe N tal que $k \geq N \Rightarrow x_{k+1} \equiv x_k \pmod{n}$.

Faremos o passo indutivo com $n = m$. Se m possui dois ou mais fatores primos distintos, então podemos escrever $m = rs$ com $1 < r < s < m$ e $\text{mdc}(r, s) = 1$. Dado um inteiro positivo a sabemos por hipótese que existem inteiros positivos N_r e N_s tais que $k \geq N_r \Rightarrow x_{k+1} \equiv x_k \pmod{r}$ e $k \geq N_r \Rightarrow x_{k+1} \equiv x_k \pmod{s}$. Tomemos $N = \max\{N_r, N_s\}$ e teremos $k \geq N \Rightarrow k \geq N_r$ e $k \geq N_s$ implicando $x_{k+1} \equiv x_k \pmod{r}$ e $x_{k+1} \equiv x_k \pmod{s} \Rightarrow x_{k+1} \equiv x_k \pmod{m}$. Resta analisar o caso em que m é uma potência de primo. Seja $m = p^t$. Considere um inteiro positivo a. Se $p \mid a$, então para N suficientemente grande $k \geq N \Rightarrow m \mid x_k$, pois a cada termo possui mais fatores p que seu antecessor. Portanto, temos $k \geq N \Rightarrow x_{k+1} \equiv 0 \equiv x_k \pmod{m}$. Se $p \nmid a$,

então $\text{mdc}(a, m) = 1$ e $a^{\varphi(m)} \equiv 1 \mod m \Rightarrow a^{\varphi(m)j} \equiv 1^j \equiv 1 \pmod{m}$. Por hipótese, a sequência se torna eventualmente constante módulo $\varphi(m) < m$, ou seja, existe $N_{\varphi(m)}$ tal que $k \geq N_{\varphi(m)} \Rightarrow x_{k+1} \equiv x_k \pmod{\varphi(m)} \Rightarrow \varphi(m) \mid x_{k+1} - x_k$. Considerando $N = N_{\varphi(m)} + 1$ temos $k \geq N \Rightarrow x_{k+1} - x_k = a^{x_k} - a^{x_{k-1}} = a^{x_{k-1}}(a^{x_k - x_{k-1}} - 1)$. Mas $k \geq N \Rightarrow k - 1 \geq N_{\varphi(m)} \Rightarrow \varphi(m) \mid x_k - x_{k-1} \Rightarrow a^{x_k - x_{k-1}} \equiv 1 \pmod{m}$ implicando que $m \mid a^{x_{k-1}}(a^{x_k - x_{k-1}} - 1) \Rightarrow x_{k+1} \equiv x_k \pmod{m}$.

Problema 0.96. *(T) Demonstre que o sistema de equações*

$$\begin{aligned} x &\equiv b_1 \pmod{a_1} \\ x &\equiv b_2 \pmod{a_2} \\ &\vdots \\ x &\equiv b_k \pmod{a_k} \end{aligned}$$

tem solução se, e somente se, para todo i e j, $\text{mdc}(a_i, a_j) \mid (b_i - b_j)$*. (No caso particular em que* $\text{mdc}(a_i, a_j) = 1$*, o problema se reduz ao teorema chinês dos restos).*

Solução

Seja $d = \text{mdc}(a_i, a_j)$. Se existe solução, então temos $x \equiv b_i \pmod{a_i} \Rightarrow x \equiv b_i \pmod{d}$ e $x \equiv b_j \pmod{a_j} \Rightarrow x \equiv b_j \pmod{d}$. Juntando as duas $b_i \equiv x \equiv b_j \pmod{d} \Rightarrow d \mid b_i - b_j$. Então essa condição é necessária. Resta provar que também é suficiente.

Para cada fator primo p_j que divide algum dos a_i considere o a_i que possui a maior quantidade de fatores p_j. Em caso de empate, considere qualquer dos a_i com essa quantidade máxima. Suponha que a_i possui k_j fatores p_j. Tome a solução X do sistema de congruências $x \equiv b_i \pmod{p_j^{k_j}}$ tomando todos os primos. Essa solução existe pelo Teorema Chinês dos Restos já que $p_r \neq p_s \Rightarrow \text{mdc}(p_r^{k_r}, p_s^{k_s}) = 1$.

Considere a fatoração em primos de $a_i = p_1^{x_1} p_2^{x_2} \dots p_m^{x_m}$. Para cada p_j se a_i determinou o b correspondente, então $X \equiv b_i \pmod{p_j^{x_j}}$ e um outro a_h determinou o b do p_j então $X \equiv b_h \pmod{p_j^{k_j}} \Rightarrow X \equiv b_h \pmod{p_j^{x_j}}$, pois $k_j \geq x_j$ já que era o maior expoente possível. Temos também que $p_j^{x_j} \mid \text{mdc}(a_i, a_h)$ e $\text{mdc}(a_i, a_h) \mid b_i - b_h \Rightarrow p_j^{x_j} \mid b_i - b_h \Rightarrow b_i \equiv b_h \equiv X \pmod{p_j^{x_j}}$. Logo, $X \equiv b_i \pmod{p_j^{x_j}}$ para cada potência $p_j^{x_j}$ do a_i implicando $X \equiv a_i \pmod{b_i}$.

Aplicando esse resultado para todos os a_i concluímos que X é solução do sistema de congruências $x \equiv b_i \pmod{a_i}$ com $1 \leq i \leq k$.

Problema 0.97. *(A) Demonstre que, para k e n números naturais, é possível encontrar k números consecutivos, cada um dos quais tem ao menos n divisores primos diferentes.*

Solução

O conjunto dos números primos é infinito. Podemos considerar kn primos distintos p_1, $p_2, \ldots, p_k n$. Considere o seguinte sistema de congruências.

$$\begin{aligned} x &\equiv -1 \pmod{p_1 p_2 \ldots p_n} \\ x &\equiv -2 \pmod{p_{n+1} p_{n+2} \ldots p_{2n}} \\ &\vdots \\ x &\equiv -k \pmod{p_{(k-1)n+1} p_{(k-1)n+2} \ldots p_{kn}} \end{aligned}$$

Pelo Teorema Chinês dos Restos esse sistema possui solução X.
Por construção, cada um dos k números consecutivos $N+1$, $N+2$, $\ldots$, $N+k$ possui pelo menos n fatores primos distintos.

Problema 0.98. *(OI) Demonstre que se a, b e c são três inteiros diferentes, então existem infinitos valores de n para os quais $a+n$, $b+n$ e $c+n$ são primos relativos dois a dois.*

Solução

Seja p um primo tal que $p \mid a+n$ e $p \mid b+n$. Veja que $p \mid (a+n)-(b+n) = a-b$. Então para qualquer inteiro positivo n os primos que podem dividir dois dos números $a+n$, $b+n$ e $c+n$ são divisores de $A = a-b$, $B = b-c$ ou $C = c-a$. Vale lembrar que esses números não são zero, pois a, b e c são três inteiros diferentes.
Considere o sistema de congruências $x \equiv -a+1 \pmod{p}$ para cada p primo tal que $p \mid A$, $x \equiv -b+1 \pmod{q}$ para cada q primo tal que $q \mid B$ e $q \nmid A$ e $x \equiv -c+1 \pmod{r}$ para cada r primo tal que $r \mid C$, $r \nmid A$ e $r \nmid B$. Os módulos usados são primos distintos e, portanto, primos entre si dois a dois. Pelo Teorema Chinês dos Restos esse sistema de equações possui solução única módulo o produto desses primos. Isso nos dá infinitas soluções inteiras positivas, pois basta somar quantas vezes desejarmos o produto dos números a uma solução.
Vale observar que $a \equiv b \pmod{A}$, $b \equiv c \pmod{B}$ e $c \equiv a \pmod{C}$. Isso significa que um p primo é tal que $p \mid B$ e $p \mid A$ então $x \equiv -a+1 \pmod{p} \Leftrightarrow x \equiv -b+1 \pmod{p}$. Analogamente, para todo divisor primo r de C temos $x \equiv -c+1 \pmod{C}$.
Tomando n como uma dessas infinitas soluções do sistema de congruências implica $\text{mdc}(a+n, b+n) = \text{mdc}(a+n, a-b) = 1$, pois para cada p primo tal que $p \mid a-b = A$ temos $n \equiv -a+1 \pmod{p} \Rightarrow a+n \equiv 1 \pmod{p}$ e $p \nmid a+n$. Analogamente, $\text{mdc}(b+n, c+n) = \text{mdc}(b+n, b-c) = 1$, pois se $q \mid b-c = B$ então $n \equiv -b+1 \pmod{q} \Rightarrow b+n \equiv 1 \pmod{q}$ e $q \nmid b+n$. E podemos fazer o mesmo para o úlitmo par $\text{mdc}(c+n, a+n) = \text{mdc}(c+n, C) = 1$.

Concluímos que existem infinitos inteiros n tais que $a+n$, $b+n$ e $c+n$ são primos relativos dois a dois.

Problema 0.99. *(OI) Demonstre que para todo inteiro positivo m e todo número par $2k$, este último pode ser escrito como a diferença de dois inteiros positivos, cada um dos quais é primo relativo com m.*

Solução

Sejam $p_1, p_2, \ldots, p_r$ os divisores primos de m. Veja que $p_i \mid x$ ou $p_i \mid x+2k$ se, e somente se, $x \equiv 0 \pmod{p_i}$ ou $x \equiv -2k \pmod{p_i}$. Vamos provar que podemos escolher uma congruência a_i tal que $a_i \not\equiv 0 \pmod{p_i}$ e $a_i \not\equiv -2k \pmod{p_i}$. Se $p_i = 2$, então essas duas congruências são equivalentes a $x \equiv 0 \pmod 2$ e basta tomar $a_i = 1$. Se $p_i \geq 3$, então há pelo menos um valor de a_i, pois estamos descartando no máximo duas classes de congruência e $p_i - 2 \geq 1$.

Considere o sistema de congruências $x \equiv a_i \pmod{p_i}$ para $i = 1, 2, \ldots, r$. Pelo Teorema Chinês dos Restos esse sistema possui solução única módulo $P = p_1 p_2 \ldots p_r$. Seja $x = X + Ps$ onde X é uma solução e s é um inteiro qualquer. Temos $(x+2k) - x = 2k$ e $\text{mdc}(x, m) = \text{mdc}(x+2k, m) = 1$, pois por construção nenhum primo que divide m divide x ou $x+2k$. Variando s obtemos infinitos valores de x.

Problema 0.100. *(OI) Demonstre que existem progressões aritméticas de comprimento arbitrário formadas por inteiros positivos tais que cada termo é a potência de um inteiro positivo com expoente maior do que* 1.

Solução

Vamos provar por indução que podemos montar n números em progressão arimética com n potências de expoentes maiores que 1. Para $n = 1$ tome uma potência $2^2 = 4$. Para $n = 2$ tome $5^2 = 25$ e $3^3 = 27$. Agora mostaremos como construir um exemplo para $n = 3$. O próximo termo da progressão para $n = 2$ seria 29 que não é uma potência. Porém podemos multiplicar os termos por uma potência de 29 conveniente que torne todos potências. Teríamos $(25 \cdot 29^k, 27 \cdot 29^k, 29^{k+1})$. Basta pegar um múltiplo comum de cada um dos expoentes do caso anterior. No nosso exemplo, os expoentes eram 2 e 3 e podemos tomar $k = 6$ e obter $((5 \cdot 29^3)^2, (3 \cdot 29^2)^3, 29^7)$.

Vamos generalizar essa ideia. Suponha que temos $(a_1, a_2, \ldots, a_n)$ números em progressão aritmética de razão r tal que a_i é uma potência de expoente $b_i > 1$. Seja $B = b_1 b_2 \ldots b_n$. Tome os $n+1$ números $(a_1(a_n+r)^B, a_2(a_n+r)^B, \ldots, a_n(a_n+r)^B, (a_n+r)^{B+1})$. A diferença entre termos consecutivos é sempre a mesma $a_{k+1}(a_n+r)^B - a_k(a_n+r)^B = r(a_n+r)^B$ e os números estão em progressão aritmética. Cada $a_i(a_n+r)^B$ segue sendo

uma potência de expoente $b_i > 1$ para $i = 1, 2, \ldots, n$ e $(a_n + r)(a_n + r)^B = (a_n + r)^{B+1}$ é uma potência de expoente $B + 1 > 1$.

Então sempre podemos aumentar o tamanho da progressão e montar progressões aritméticas de comprimento arbitrário formadas por inteiros positivos tais que cada termo é a potência de um inteiro positivo com expoente maior do que 1.

7

POTÊNCIAS E CONGRUÊNCIAS

1.1 POLINÔMIOS

Problema 1.1. *(A) Sejam* $f(x) = x^5 - 4x^3 - 5x + 1$ *e* $g(x) = x^2 + x + 1$ *polinômios em* $\mathbb{Q}[x]$. *Determine* $mdc(f(x), g(x))$ *e ache dois polinômios* $m(x), n(x) \in \mathbb{Q}[x]$ *tais que*

$$f(x)m(x) + g(x)n(x) = mdc(f(x), g(x)).$$

Solução

Usaremos o Algoritmo de Euclides. Na primeira divisão temos

$$f(x) = g(x)(x^3 - x^2 - 4x + 5) + (-6x - 4).$$

E na segunda divisão temos

$$g(x) = (-6x - 4)(-\frac{1}{6}x - \frac{1}{18}) + \frac{7}{9}.$$

Concluímos que $\text{mdc}(f(x), g(x)) = 1$ e podemos calcular os coeficientes pedidos voltando nas divisões.

$$14 = 18g(x) + (-6x - 4)(3x + 1)$$

$$\Rightarrow 14 = 18g(x) + (f(x) - g(x)(x^3 - x^2 - 4x + 5))(3x + 1)$$

$$\Rightarrow 14 = f(x)(3x + 1) + g(x)(-3x^4 + 2x^3 + 13x^2 - 11x + 13)$$

$$\Rightarrow 1 = f(x)(\frac{3}{14}x + \frac{1}{14}) + g(x)(-\frac{3}{14}x^4 + \frac{1}{7}x^3 + \frac{13}{14}x^2 - \frac{11}{14}x + \frac{13}{14}).$$

Problema 1.2. *(A) Sejam* $f(x) = x^4 + x^2 + 1$ *e* $g(x) = x^3 + 1$ *polinômios em* $(\mathbb{Z}/(2))[x]$. *Determine* $\text{mdc}(f(x), g(x))$ *e ache dois polinômios mônicos (com coeficientes em* $\mathbb{Z}/(2)$*)* $m(x)$ *e* $n(x)$ *tais que*

$$f(x)m(x) + g(x)n(x) = \text{mdc}(f(x), g(x)).$$

Solução

Usaremos o Algoritmo de Euclides com as divisões em $(\mathbb{Z}/(2))[x]$. Vale lembrar que $1 \equiv -1 \pmod 2$ e podemos trocar o sinal dos coeficientes em $\mathbb{Z}/(2)$.

$$f(x) = g(x)(x) + (x^2 + x + 1)$$

$$g(x) = (x^2 + x + 1)(x + 1)$$

Concluímos que $\text{mdc}(f(x), g(x)) = x^2 + x + 1$ e notamos que pela primeira divisão $m(x) = 1$ e $n(x) = x$ são soluções da equação dada.

Problema 1.3. *(A) Seja $f(x) \in \mathbb{C}[x]$ um polinômio que deixa restos 10 e 1 quando dividido por $x - 1$ e $x - 10$ respectivamente. Encontre o resto de $f(x)$ na divisão por $(x - 1)(x - 10)$.*

Solução

Sabemos que o resto da divisão por um polinômio de grau 1 tem grau menor que 1, ou seja, uma constante. Temos $f(x) = (x - 1)q_1(x) + 10$. Essa é uma equação polinomial, então interpretando como função polinomial é uma equação que vale para todo x complexo. Usando $x = 1$ temos $f(1) = 10$. Analogamente, $f(10) = 1$.
Sabemos que o resto da divisão por um polinômio de grau 2 tem grau menor que 2 e podemos escrever como $r(x) = ax + b$. Assim,

$$f(x) = (x - 1)(x - 10)q(x) + (ax + b)$$

Novamente, usamos valores complexos em x e obtemos $f(1) = a \cdot 1 + b = 10$ e $f(10) = a \cdot 10 + b = 1$. Resolvendo o sistema $a = -1$ e $b = 10$. Portanto, o resto da divisão é $-x + 11$.

Problema 1.4. *(A) Determine o resto da divisão de $f(x) = x^{100}$ por $g(x) = x^3 + 2x^2 - x - 2$.*

Dica: Fatore $g(x)$.

Solução

Comecemos fatorando o divisor $g(x) = x^3 + 2x^2 - x - 2 = (x + 2)(x^2 - 1) = (x + 2)(x + 1)(x - 1)$. Sabemos que o resto da divisão é um polinômio de grau menor que 3 e podemos escrever como $ax^2 + bx + c$. Assim,

$$f(x) = (x + 2)(x + 1)(x - 1)q(x) + (ax^2 + bx + c)$$

Usando as funções polinomiais com os mesmos coeficientes e $x = -2$, $x = -1$ e $x = 1$ temos $4a - 2b + c = (-2)^{100} = 2^{100}$, $a - b + c = (-1)^{100} = 1$ e $a + b + c = 1^{100} = 1$. Resolvendo o sistema, $a = \frac{2^{100}-1}{3}$, $b = 0$ e $c = \frac{4-2^{100}}{3}$.

Problema 1.5. *(A) Determine o resto da divisão de $f(x) = x^{100}$ por $g(x) = x^3 + 2x^2 + x + 2$.*

Solução

Fatorando $g(x)$ em $\mathbb{C}[x]$ temos $g(x) = (x+2)(x^2+1) = (x+2)(x-i)(x+i)$. O resto da divisão tem grau menor que 3 e pode ser escrito como $ax^2 + bx + c$. Usando os valores -2, i e $-i$ obtemos $4a - 2b + c = (-2)^{100}$, $-a + bi + c = i^{100} = 1$ e $-a - bi + c = (-i)^{100} = 1$. Resolvendo o sistema $a = \frac{2^{100}-1}{5}$, $b = 0$ e $c = \frac{2^{100}+4}{5}$.

A resposta é a mesma se a divisão for em $\mathbb{R}[x]$, pois o inverso de número real é número real e como os polinômios dados possuem coeficientes reais realizar essa divisão euclidiana em $\mathbb{C}$ ou em $\mathbb{R}$ tem os mesmos quociente e resto.

Problema 1.6. *(A) Mostre que o polinômio $f(x) = x^4 - 4x^3 + 6x^2 - x + 1$ é irredutível em $\mathbb{Q}[x]$.*

Dica: substituir x por $x + a$ com a adequado e usar o critério de Einsentein.

Solução

Pelo Lema de Gauss, basta provar que $f(x)$ é irredutível em $\mathbb{Z}[x]$. Considere o polinômio $f(x+1) = (x+1)^4 - 4(x+1)^3 + 6(x+1)^2 - (x+1) + 1 = x^4 + 3x + 3$. Todos os coeficiente são múltiplos de 3 menos o coeficiente líder e o coeficiente independente não é múltiplo de 3^2. Pelo Critério de Eisenstein para $p = 3$ temos que $f(x+1)$ é irredutível em $\mathbb{Z}[x]$. Veja que se $f(x)$ fosse redutível em $\mathbb{Z}[x]$ então $f(x) = g(x)h(x) \Rightarrow f(x+1) = g(x+1)h(x+1)$ e $f(x+1)$ também seria. Logo, se $f(x+1)$ é irredutível então $f(x)$ também é.

Problema 1.7. *(A) Mostre que o polinômio $f(x) = x^4 - 20x^2 + 16$ é irredutível em $\mathbb{Q}[x]$.*

Solução

Primeiro trabalhemos em $\mathbb{R}[x]$. Temos

$$f(x) = x^4 - 20x^2 + 16 = (x^2 - 10)^2 - 84 = (x^2 - 10 - \sqrt{84})((x^2 - 10 + \sqrt{84}))$$

$$\Rightarrow f(x) = (x - \sqrt{10 + \sqrt{84}})(x + \sqrt{10 + \sqrt{84}})(x - \sqrt{10 - \sqrt{84}})(x + \sqrt{10 - \sqrt{84}}).$$

Sabemos que essa fatoração em polinômios é única em $\mathbb{R}[x]$. Agora voltando para $\mathbb{Q}[x]$. Suponha que $f(x)$ seja redutível em $\mathbb{Q}[x]$ então $f(x) = g(x)h(x)$ com graus entre 1 e 3. Note que $g(x)$ e $f(x)$ são compostos pelos fatores irredutíveis em $\mathbb{R}[x]$.

Se $\deg g(x) = 1$ então seria $x - r$ multiplicado por racional para uma das raízes acima. Porém, isso não é possível, pois todas as raízes são irracionais. Se $\deg h(x) = 1$ temos o mesmo problema. Resta apenas $\deg g(x) = \deg h(x) = 2$. Nesse caso $g(x)$ seria de $(x-r)(x-s) = x^2 - (r+s)x + rs$ multiplicado por racional. Porém, pelo menos um

dos coeficientes $r+s$ ou rs é irracional. Portanto, essa fatoração é impossível e $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Problema 1.8. *(A) Fatore o polinômio $x^8 - x \in (\mathbb{Z}/(2))[x]$ em fatores irredutíveis.*

Solução

Veja que $x^8 - x = x(x^7 - 1) = x(x-1)(x^6 + x^5 + \cdots + x + 1)$ em $(\mathbb{Z}/(2))[x]$. Veja que $1 \equiv -1 \equiv 3 \pmod 2$ e em $\mathbb{Z}/(2)$ temos $1 = -1 = 3$. Logo, $x - 1 = x + 1$ e $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = x^6 + x^5 + x^4 + 3x^3 + x^2 + x + 1 = (x^3 + x^2 + 1)(x^3 + x + 1)$. Note que esses dois últimos são irredutíveis, pois caso fossem redutíveis seriam o produto de polinômio de grau 1 e um de grau 2 implicando que teriam raízes, mas $x = 0$ e $x = 1$ não são raízes. Concluímos que em $(\mathbb{Z}/(2))[x]$ a fatoração de $x^8 - x$ em polinômios irredutíveis é $x(x+1)(x^3 + x^2 + 1)(x^3 + x + 1)$.

Problema 1.9. *(A) Fatore o polinômio $x^{25} - x \in (\mathbb{Z}/(5))[x]$ em fatores irredutíveis.*

Solução

Comecemos por $x^{25} - x = x(x^{24} - 1) = x(x^{12} - 1)(x^{12} + 1)$. Podemos usar diferença de quadrados no segundo fator: $x^{12} - 1 = (x^6 - 1)(x^6 + 1)$. E também podemos fazer na terceira. Dado que $1 \equiv -4 \equiv -2^2 \pmod 5$ temos $x^{12} + 1 = x^{12} - 2^2 = (x^6 - 2)(x^6 + 2)$ em $\mathbb{Z}/(5)$. Agora usaremos somas e diferenças de cubos $x^6 - 1 = (x^2 - 1)(x^4 + x^2 + 1)$, $x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1)$, $x^6 - 2 = x^6 - 3^3 = (x^2 - 3)(x^4 + 3x^2 + 9)$ e $x^6 + 2 = x^6 + 3^3 = (x^2 + 3)(x^4 - 3x^2 + 9)$, pois $2 \equiv 3^3 \pmod 5$. Veja que $x^2 - 1 = (x-1)(x+1) = (x-1)(x-4)$ e $x^4 + x^2 + 1 = x^4 + 2x^2 + 1 - x^2 = (x^2 + 1)^2 - x^2 = (x^2 - x + 1)(x^2 + x + 1)$. No produto seguinte, $x^2 + 1 = x^2 - 2^2 = (x-2)(x+2) = (x-2)(x-3)$. e $x^4 - x^2 + 1 = x^4 - 2x^2 + 1 - 4x^2 = (x^2 - 1)^2 - (2x)^2 = (x^2 - 2x - 1)(x^2 + 2x - 1)$. Note que $x^2 + 3$ e $x^2 - 3$ já são irredutíveis, pois para fatorá-los teriam que ter raízes em $\mathbb{Z}/(5)$, mas não existe x tal que $x^2 \equiv -3 \pmod 5$ nem $x^2 \equiv 3 \pmod 5$. Já para os outros fatores temos $x^4 + 3x^2 + 9 = x^4 + 4x^2 + 4 - x^2 = (x^2 + 2)^2 - x^2 = (x^2 - x + 2)(x^2 + x + 2)$ e $x^4 - 3x^2 + 9 = x^4 - 4x^2 + 4 - 4x^2 = (x^2 - 2)^2 - (2x)^2 = (x^2 - 2x - 2)(x^2 + 2x - 2)$. Usando o mesmo argumento do $x^2 - 3$ podemos concluir que esses polinômios de grau 2 são irredutível em $\mathbb{Z}/(5)$.

Logo, a fatoração em polinômios irredutíveis de $\mathbb{Z}/(5)[x]$ é $x^25 - x = x(x-1)(x-4)(x^2 - x + 1)(x^2 + x + 1)(x-2)(x-3)(x^2 - 2x - 1)(x^2 + 2x - 1)(x^2 - 3)(x^2 - x + 2)(x^2 + x + 2)(x^2 + 3)(x^2 - 2x - 2)(x^2 + 2x - 2)$.

Problema 1.10. *(OI) Encontre um valor de $a \in \mathbb{N}$ tal que o polinômio $f(x) = x^{100} + ax^{98} + 11$ não tenha raízes racionais, mas não seja irredutível em $\mathbb{Q}[x]$.*

Dica: Calcule um a tal que $f(x)$ seja divisível por um polinômio irredutível de grau 2.

Solução

Considere o polinômio $g(x) = x^2 + 1$ que não possui raízes racionais. Veja que $g(x) \mid f(x) \iff f(i) = 0$ onde i é unidade imaginária. Daí, temos $f(i) = 0 \iff i^{100} + ai^{98} + 11 = (-1)^{50} + a(-1)^{49} + 11 = 0 \iff 1 - a + 11 = 0 \iff a = 12$. Assim, temos que $x^2 + 1 \mid x^{100} + 12x^{98} + 11$ e $x^{100} + 12x^{98} + 11$ é redutível. Por outro lado, pelo teste da raiz racional se $\frac{p}{q}$ é raiz de $f(x)$ então $p \mid 11$ e $q \mid 1$. As únicas raízes racionais possíveis são 1, -1, 11 e -11. Mas $f(1) = f(-1) = 1 + 12 + 11 = 24 > 0$ e $f(11) = f(-11) = 11^{100} + 12 \cdot 11^{98} + 11 > 0$. De maneira mais geral, $f(x)$ não possui raiz real, pois se r real então $r^2 \geq 0$ e $f(r) \geq 11 > 0$.

Problema 1.11. *(OI) Seja α uma raiz de $X^3 - 3X + 1 = 0$. Mostre que $\alpha^2 - 2$ também é uma raiz deste polinômio.*

Solução

Sejam $f(x) = x^3 - 3x + 1$ e $g(x) = x^2 - 2$. Note que $f(g(x)) = (x^2 - 2)^3 - 3(x^2 - 2) + 1 = x^6 - 6x^4 + 12x^2 - 8 - 3x^2 + 6 + 1 \Leftrightarrow f(g(x)) = x^6 - 6x^4 + 9x^2 - 1$. Fazendo a divisão de $x^6 - 6x^4 + 9x^2 - 1$ por $f(x) = x^3 - 3x + 1$ obtemos

$$f(g(x)) = x^6 - 6x^4 + 9x^2 - 1 = (x^3 - 3x + 1)(x^3 - 3x - 1) = f(x)(x^3 - 3x - 1)$$

Então para toda raiz α de $x^3 - 3x + 1$ temos $f(\alpha) = 0 \Rightarrow f(g(\alpha)) = 0 \Rightarrow f(\alpha^2 - 2) = 0$ e $\alpha^2 - 2$ também é raiz desse polinômio.

Problema 1.12. *(A) Seja $K = (\mathbb{Z}/(3))[x]/(f(x))$ onde $f(x) = x^2 + x + 2$. Mostre que $f(x)$ é irredutível em $(\mathbb{Z}/(3))[x]$ e portanto K é um corpo. Construa a tabela de multiplicação do grupo K^* e usando esta tabela determine o menor inteiro positivo n tal que $x^n = 1$ em K.*

Solução

O resto na divisão por $x^2 + x + 2$ tem grau menor que 2. Os coeficientes de x^1 e x^0 são elementos de $\mathbb{Z}/(3)$ e temos $3 \cdot 3 = 9$ elementos. Montamos a tabela a seguir lembrando que os coeficientes são elementos de $\mathbb{Z}/(3)$, que $x^2 \equiv -x - 2 \equiv 2x + 1 \pmod{x^2 + x + 2}$ e que $2x^2 \equiv 4x + 2 \equiv x + 2 \pmod{x^2 + x + 2}$.

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$	$\overline{2x}$	$\overline{2x+2}$	$\overline{2x+1}$	$\overline{x}$	$\overline{x+2}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{1}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x+2}$	$\overline{2}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2}$	$\overline{x}$	$\overline{2x+1}$
$\overline{x+2}$	$\overline{0}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{x+1}$	$\overline{2x}$	$\overline{2}$	$\overline{2x+2}$	$\overline{1}$	$\overline{x}$
$\overline{2x}$	$\overline{0}$	$\overline{2x}$	$\overline{x}$	$\overline{x+2}$	$\overline{2}$	$\overline{2x+2}$	$\overline{2x+1}$	$\overline{x+1}$	$\overline{1}$
$\overline{2x+1}$	$\overline{0}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{2x+2}$	$\overline{x}$	$\overline{1}$	$\overline{x+1}$	$\overline{2}$	$\overline{2x}$
$\overline{2x+2}$	$\overline{0}$	$\overline{2x+2}$	$\overline{x+1}$	$\overline{2}$	$\overline{2x+1}$	$\overline{x}$	$\overline{1}$	$\overline{2x}$	$\overline{x+2}$

Veja que K^* possui $9-1=8$ elementos invertíveis e $ord_K x$ é um divisor de 8 e só pode ser 1, 2, 4 ou 8. Pela tabela, temos

$$x^1 \equiv x \pmod{x^2+x+2}$$

$$x^2 \equiv 2x+1 \pmod{x^2+x+2}$$

$$x^4 \equiv 2 \pmod{x^2+x+2}$$

$$x^8 \equiv 1 \pmod{x^2+x+2}$$

Concluímos que $ord_K x = 8$.
Vale notar que na tabela estudamos todos os polinômios em $(\mathbb{Z}/(3))[x]$ de grau menor que ou igual a 1 e nenhum deles é um divisor de $f(x)$. Portanto, $f(x)$ é irredutível em $(\mathbb{Z}/(3))[x]$.

Problema 1.13. *(A) Seja $\theta \in \mathbb{R}$ e n um inteiro positivo. Calcule o resto da divisão do polinômio $(\cos\theta + x\sin\theta)^n \in \mathbb{R}[x]$ por x^2+1.*

Solução

Fazendo a divisão euclidiana dos polinômios

$$(\cos\theta + x\sin\theta)^n = (x^2+1)q(x) + r(x), \deg(r(x)) \leq 1$$

Podemos escrever $r(x)$ como $ax+b$ para a e b reais. Como a igualdade acima é polinomial podemos usar qualquer valor complexo para obter igualdades. Usando $x = i$ a unidade imaginária e a fórmula de Moivre, temos

$$(\cos\theta + i\sin\theta)^n = (i^2+1)q(i) + r(i) \Rightarrow \cos(n\theta) + i(\sin n\theta) = ai + b.$$

Se dois números complexos são iguais, então eles possuem mesma parte real e mesma parte imaginária. Assim, $r(x) = (\sin n\theta)x + (\cos n\theta)$.

Problema 1.14 (IMO1993). *(OA) Seja $f(x) = x^n + 5x^{n-1} + 3$ onde $n > 1$. Demonstre que $f(x)$ não pode se expressar como produto de dois polinômios não constantes com coeficientes inteiros.*

Solução

Suponha que $f(x)$ é redutível em $\mathbb{Z}[x]$ e podemos escrever $f(x) = g(x)h(x)$.
Se $\deg g(x) = 1$ ou $\deg h(x) = 1$, então um deles seria da forma $ax + b$ com a e b inteiros e $f(x)$ teria raiz racional $-\frac{b}{a}$. Pelo teste da raiz racional em $f(x)$, se $\frac{p}{q}$ é uma raiz racional, então $p \mid 3$ e $q \mid 1$ e as possibilidades são 1, -1, 3 e -3. Provaremos que nenhum desses números é raiz de $f(x)$. Para $x = 1$ temos $f(1) = 1^n + 5 \cdot 1^{n-1} + 3 = 9 > 0$. Para $x = -1$ temos $f(-1) = (-1)^n + 5 \cdot (-1)^{n-1} + 3$ que pode ser $-1 + 5 + 3 = 7$ se n ímpar ou $1 - 5 + 3 = -1$ se n par. Para $x = 3$ temos $f(3) = 3^n + 5 \cdot 3^{n-1} + 3 > 0$. Finalmente, para $x = -3$ temos $f(-3) = (-3)^n + 5 \cdot (-3)^{n-1} + 3$. Para $n \geq 3$ se $f(-3) = 0$ então $(-3)^2 = 9 \mid 3$ que é falso. Para $n = 2$ temos $f(-3) = (-3)^2 + 5(-3) + 3 = 9 - 15 + 3 = -3 \neq 0$. Portanto, $f(x)$ não tem raiz racional e não tem divisores de grau 1.
Agora trataremos o caso em que $\deg g(x) \geq 2$ e $\deg h(x) \geq 2$. Considere a igualdade em $\mathbb{Z}/(3)[x]$ e $f(x) = x^n + 5x^{n-1} = x^{n-1}(x + 5)$. Pela fatoração única em $\mathbb{Z}/(3)[x]$ os polinômios $g(x)$ e $h(x)$ são produto desses fatores em $\mathbb{Z}/(3)[x]$. Como eles possuem grau pelo menos 2 temos $x \mid g(x)$ e $x \mid h(x)$ implicando que $3 \mid g_0$ e $3 \mid h_0$ onde g_0 e h_0 são os coeficientes de x^0 em $g(x)$ e $h(x)$ respectivamente. Porém, isso implica que $3^2 \mid g_0 \cdot h_0$. Por outro lado, $g_0 \cdot h_0 = 3$, pois é o coficiente de x^0 em $f(x)$. Como, $9 \nmid 3$ concluímos que é impossível fazer tal fatoração.
Nos dois casos temos contradições. Podemos concluir que a suposição inicial é falsa e $f(x)$ é irredutível em $\mathbb{Z}[x]$.

Problema 1.15. *(OI) Encontre todos os pares $(c, P(x))$ onde c é um real e $P(x)$ é um polinômio não nulo tal que*

$$P(x^4 + x^2 + x) = (x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)P(cx).$$

Solução

Seja $\deg P(x) = n$. Se $c = 0$ temos $4n = 6 + 0 \iff n = \frac{3}{2}$ que é impossível, pois n é inteiro positivo já que $P(x)$ é um polinômio não nulo. Podemos tratar agora $c \neq 0$ e $4n + 6 + n \iff 3n = 6 \iff n = 2$. Seja $P(x) = a_2x^2 + a_1x + a_0$. Aplicando $P(x)$ em $x^4 + x^2 + x$ temos

$$P(x^4 + x^2 + x) = a_2x^8 + 2a_2x^6 + 2a_2x^5 + (a_1 + a_2)x^4 + 2a_2x^3 + (a_1 + a_2)x^2 + a_1x + a_0$$

E desenvolvendo o outro lado chamando de A a expressão $a_2c^2 + a_1c + a_0$ temos

$$a_2c^2x^8 + (a_2c^2 + a_1c)x^7 + Ax^6 + Ax^5 + Ax^4 + Ax^3 + Ax^2 + (a_1c + a_0)x + a_0$$

Comparando os coeficientes temos as equações $a_2 = a_2c^2$, $0 = a_2c^2 + a_1c$, $2a_2 = A$, $2a_2 = A$, $a_1 + a_2 = A$, $2a_2 = A$, $a_1 = a_1c + a_0$ e $a_0 = a_0$. Temos $a_1 + a_2 = A = 2a_2 \Rightarrow a_1 = a_2$ e $0 = a_2c^2 + a_1c = a_2 + a_2c \Rightarrow a_2(1 + c) = 0$. Como o grau de $P(x)$ é 2 temos $a_2 \neq 0$ e $1 + c = 0 \Rightarrow c = -1$. Com isso, podemos determinar a_0 da equação $a_1 = a_1c + a_0 \Rightarrow a_2 = -a_2 + a_0 \Rightarrow a_0 = 2a_2$. Concluímos que os únicos valores possíveis são $c = -1$ e $P(x) = a_2x^2 + a_2x + 2a_2 = k(x^2 + x + 2)$ onde k é um número qualquer não nulo no conjunto dos coeficientes, reais ou complexos.
Note que, de fato $(c, P(x)) = (-1, k(x^2 + x + 2))$ satisfazem a equação para todo k não nulo.

Problema 1.16 (Austrian-Polish1998)**.** *(OI) Encontre todos os inteiros positivos n e m tais que todas as soluções de $x^3 - 17x^2 + mx - n^2 = 0$ são inteiras.*

Solução

Seja $p(x) = x^3 - 17x^2 + mx - n^2$. Veja que se $\alpha \leq 0$ então $p(\alpha) < 0$, pois cada parcela é negativa. Portanto, as soluções devem ser inteiras positivas. Seja r, s e t as raízes inteiras positivas não necessariamente distintas. Podemos fatorar o polinômio $p(x) = (x - r)(x - s)(x - t) = x^3 - (r + s + t)x^2 + (rs + rt + st)x - rst$ e obter $r + s + t = 17$, $rs + rt + st = m$ e $rst = n^2$. Vamos usar a soma deles para listas as possibilidades e testar se o produto é um quadrado perfeito na terceira equação. Suponha sem perda de generalidade que $r \leq s \leq t$.
Se $r = 1$ então pela soma temos os casos $(r, s, t) = (1, 1, 15)$, $(1, 2, 14)$, $(1, 3, 13)$, $(1, 4, 12)$, $(1, 5, 11)$, $(1, 6, 10)$, $(1, 7, 9)$ ou $(1, 8, 8)$. A única tripla que dá solução é $(r, s, t) = (1, 8, 8)$ implicando $m = 8 + 8 + 64 = 80$ e $n = \sqrt{1 \cdot 8 \cdot 8} = 8$.
Se $r = 2$ então os casos são $(r, s, t) = (2, 2, 13)$, $(2, 3, 12)$, $(2, 4, 11)$, $(2, 5, 10)$, $(2, 6, 9)$ ou $(2, 7, 8)$. Existe apenas uma tripla que nos fornece solução: $(r, s, t) = (2, 5, 10)$ implicando $m = 10 + 20 + 50 = 80$ e $n\sqrt{2 \cdot 5 \cdot 10} = 10$.
Se $r = 3$ então $(r, s, t) = (3, 3, 11)$, $(3, 4, 10)$, $(3, 5, 9)$, $(3, 6, 8)$ ou $(3, 7, 7)$. A única tripla que dá solução é $(r, s, t) = (3, 6, 8)$ implicando $m = 18 + 24 + 48 = 90$ e $n = \sqrt{3 \cdot 6 \cdot 8} = 12$.
Se $r = 4$ então $(r, s, t) = (4, 4, 9)$, $(4, 5, 8)$ ou $(4, 6, 7)$. Uma tripla nos fornece solução: $(r, s, t) = (4, 4, 9)$ implicando $m = 16 + 36 + 36 = 88$ e $n = \sqrt{4 \cdot 4 \cdot 9} = 12$.
Se $r = 5$ então $(r, s, t) = (5, 5, 7)$ ou $(5, 6, 6)$. Nenhuma tripla nos fornece solução.
Se $r \geq 6$ então $r + s + t \geq 6 + 6 + 6 = 18 > 17$ e não precisamos mais testar.
Concluímos que as soluções (m, n) são $(80, 8)$, $(80, 10)$, $(90, 12)$ e $(88, 12)$.

Problema 1.17. *(OI) Dados $x, y \in \mathbb{N}$, defina $a := x(y+1) - (y!+1)$. Mostre que imagem da função $f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por*

$$f(x,y) = \frac{y-1}{2}\left(|a^2-1| - (a^2-1)\right) + 2$$

é exatamente o conjunto dos números primos.

Solução

Faremos dois casos. Se $a^2 \geq 1$, então $|a^2-1| = a^2-1$ e $f(x,y) = \frac{y-1}{2} \cdot 0 + 2 = 2$ que é primo. Se $a^2 < 1$ então $a = 0$, pois $a \in \mathbb{Z}$ e $|a| < 1$. Isso implica $f(x,y) = \frac{y-1}{2} \cdot 2 + 2 = y+1$. Ora, mas $a = 0 \Leftrightarrow x(y+1) = y!+1$ implicando que $y+1 \mid y!+1$. Se $y+1 = p$ primo, então essa divisibilidade é verdadeira pelo Teorema de Wilson. E de fato podemos fazer $a = 0$ usando $y = p-1$ e $x = \frac{(p-1)!+1}{p}$ que nos leva a $f(\frac{(p-1)!+1}{p}, p-1) = p$. Se $y+1$ não é primo então $y+1 = a \cdot b$ com $2 \leq a \leq b \leq y$ implicando que $a \mid y!$, $a \mid y+1 \Rightarrow a \mid y!+1$ e, fazendo a diferença, $a \mid 1$ que é uma contradição. Então quando $y+1$ não é primo temos $f(x,y) = 2$. Concluímos a imagem da função é exatamente o conjunto dos números primos.

Problema 1.18. *(A) Prove a seguinte modificação do Critério de Eisenstein: considere $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ um polinômio primitivo não constante e sem raízes racionais. Suponha que exista um número primo p tal que $p \nmid a_n$, $p \mid a_j$ para todo $0 \leq j < n$ e $p^2 \nmid a_1$. Então $f(x)$ é irredutível em $\mathbb{Z}[x]$.*

Solução

Suponha que $f(x)$ satisfaz as condições e é redutível em $\mathbb{Z}[x]$. Tomemos $f(x) = g(x)h(x)$. Veja que $\deg g(x) > 1$ e $\deg h(x) > 1$, pois se algum deles tivesse grau 1 seria da forma $ax+b$ e $f(x)$ teria raiz racional $-\frac{b}{a}$. Usando os polinômios em $\mathbb{Z}/(T)[x]$ temos $g(x)h(x) = a_n x^n$ e pela fatoração única temos $g(x) = g_k x^k$ e $h(x) = h_{n-k} x^{n-k}$ em $\mathbb{Z}/(T)[x]$ com $k \geq 2$ e $n-k \geq 2$. Isso implica que $g_1 \equiv g_0 \equiv h_1 \equiv h_0 \equiv 0 \pmod{p}$ onde g_1, g_0, h_1 e h_0 são os coeficientes de x^1 e x^0 em $g(x)$ e $h(x)$. Com esse resultado, podemos voltar para $\mathbb{Z}[x]$ e comparar os coeficiente de x^1 nos dois lados da equação $f(x) = g(x)h(x)$ implicando $a_1 = g_1 h_0 + g_0 h_1 \Rightarrow p^2 \mid a_1$ que contradiz as condições do enunciado. Logo, se $f(x)$ satisfaz as condições do enunciado, então $f(x)$ é irredutível em $\mathbb{Z}[x]$.

Problema 1.19. *(Zagier) (OA) Dado um número primo, associe a ele um polinômio cujos coeficientes são os dígitos decimais desse primo (por exemplo, $9x^3 + 4x^2 + 3$ para o primo 9403). Mostre que este polinômio é sempre irredutível em $\mathbb{Z}[x]$.*

Solução

Solução consultada em [22].

Suponha que $f(x) = a_n x^n + \cdots + a_1 x + a_0$ é o polinômio associado ao primo p seja redutível em $\mathbb{Z}[x]$ e considere $f(x) = g(x)h(x)$ uma fatoração em polinômios de grau maior ou igual a 1. Veja que $p = f(10) = g(10)h(10)$ implicando que um desses últimos é 1 e o outro p. Veja que caso fossem -1 e $-p$ poderíamos trocá-los por $-g(x)$ e $-f(x)$. Suponha sem perda de generalidade que $g(10) = 1$. Pelo Teorema Fundamental da Álgebra, podemos fatorar $g(x)$ em $\mathbb{C}[x]$ como $g(x) = c(x - r_1)\ldots(x - r_d)$ onde c é inteiro e $d = \deg g(x) \geq 1$.
Suponha que alguma das raízes r_i possui parte real positiva e módulo maior que ou igual a 4. Veja que $Re(r_i^{-1})$ também é positiva e $g(r_i) = 0 \Rightarrow f(r_i) = 0 \Rightarrow a_n r_i^n + \cdots + a_1 r_i + a_0 = 0 \Rightarrow a_n + \cdots + a_1 r_i^{-n+1} + a_0 r_i^{-n} = 0 \Rightarrow 1 \leq a_n \leq Re(a_n + a_{n-1} r_i^{-1}) = Re(-a_{n-2}b^{-2} - \cdots - a_0 b^{-n}) \leq |-a_{n-2}b^{-2} - \cdots - a_0 b^{-n}| \leq \frac{9|b|^{-2}}{1-|b|^{-1}} = \frac{9}{|b|(|b|-1)} \leq \frac{9}{12}$.
Assim, r_i possui parte real negativa ou módulo menor que ou igual a 4. Isso implica que $|10 - r_i| \geq 6$ e $1 = |g(10)| = |c||10 - r_1|\ldots|10 - r_d| \geq 6^d$ gerando absurdo. Portanto, $f(x)$ é irredutível.

Problema 1.20. *(OI) Encontre todos os valores de k para os quais o polinômio $x^{2k+1} + x + 1$ é divisível por $x^k + x + 1$.*

Solução

Para $k = 0$ temos que $2x + 1$ não é divisível por $x + 2$, pois -2 não é raiz de $2x + 1$. Para $k = 1$ temos $x^3 + x + 1$ não é divisível por $2x + 1$, pois $-\frac{1}{2}$ não é raiz de $x^3 + x + 1$.
Agora vamos considerar $k \geq 2$. Veja que $x^k + x + 1 \mid x(x^k + x + 1)(x^k - x - 1) = x(x^{2k} - (x+1)^2) = x^{2k+1} - x(x+1)^2$. Logo $x^k + x + 1 \mid x^{2k+1} + x + 1 \iff x^k + x + 1 \mid x(x+1)^2 + (x+1) = (x+1)(x^2 + x + 1)$. Observe que $\text{mdc}(x^k + x + 1, x + 1) = \text{mdc}(x^k, x + 1) = 1$ e podemos retirar o $x + 1$ da divisibilidade que continua sendo verdadeira. Assim, $x^k + x + 1 \mid x^{2k+1} + x + 1 \iff x^k + x + 1 \mid x^2 + x + 1 \iff k = 2$.

Problema 1.21 (IMO2002)**.** *(OA) Encontre todos os pares de inteiros $m, n > 2$ tais que existam infinitos valores de k para os quais*

$$\frac{k^m + k - 1}{k^n + k^2 - 1}$$

é inteiro.

Solução

Considere os polinômios $f(x) = x^m + x - 1$ e $g(x) = x^n + x^2 - 1$. Suponha que na divisão euclidiana de $f(x)$ por $g(x)$ obtivemos quociente $q(x)$ e resto $r(x)$ de grau menor que grau de $g(x)$. Note que como o coeficiente líder de $g(x)$ é 1 os polinômios $q(x)$ e $r(x)$ tem coeficientes inteiros. Veja que $\frac{k^m+k-1}{k^n+k^2-1} \in \mathbb{Z} \Leftrightarrow q(k) + \frac{r(k)}{g(k)} \in \mathbb{Z}$. Se essa expressão é

um inteiro para infinitos valores de k então é inteiro para um k suficientemente grande tal que $|r(k)| < |g(k)|$. Se $r(x)$ não for o polinômio nulo então para k suficientemente grande $0 < \frac{|r(k)|}{|g(k)|} < 1$ e a fração não será um inteiro. Portanto, $r(x)$ é o polinômio nulo e $f(x) = g(x)q(x)$. Também sabemos que se a fração é um número inteiro para infinitos valores de k então é inteira para todos os valores inteiros de k. Veja que $g(0) = -1 < 0 < 1 = g(1)$ implicando por continuidade que $g(x)$ possui uma raiz α entre 0 e 1. Note que $g(\alpha) = 0 \Rightarrow f(\alpha) = 0$ e

$$\alpha^m + \alpha = \alpha^n + \alpha^2 = 1$$

Se $m \geq 2n$ então $1 - \alpha = \alpha^m \leq (\alpha^n)^2 = (1-\alpha^2)^2$ que nos leva a $1 \leq (1-\alpha)(1+\alpha)^2 \Rightarrow 1 \leq 1 + 2\alpha + \alpha^2 - \alpha - 2\alpha^2 - \alpha^3 \Rightarrow 0 \leq \alpha(1 - \alpha - \alpha^2) \Rightarrow 0 \leq 1 - \alpha - \alpha^2 \Rightarrow \alpha^2 \leq 1 - \alpha = \alpha^m < \alpha^2$. Então $m < 2n$.
Veja que $\frac{f(x)}{g(x)} = x^{m-n} - \frac{x^{m-n+2} - x^{m-n} - x + 1}{g(x)}$ então $g(x) \mid x^{m-n+2} - x^{m-n} - x + 1$ e $m - n + 2 \leq 2n - 1 - n + 2 = n + 1$. Concluímos que $g(x) = x^{m-n+2} - x^{m-n} - x + 1$ ou $x^{m-n+2} - x^{m-n} - x + 1 = (x - z)g(x)$ para um inteiro z. Veja que $1^{m-n+2} - 1^{m-n} - 1 + 1 = 0$ e $g(1) = 1$. Isso implica o primeiro caso é impossível e que no segundo z tem que ser 1, pois é uma raiz do resultado que $g(x)$ não possui. Assim,

$$x^{m-n+2} - x^{m-n} - x + 1 = (x-1)(x^n + x^2 - 1)$$

$$\iff x^{m-n+2} - x^{m-n} - x + 1 = x^{n+1} - x^n + x^3 - x^2 - x + 1$$

$$\iff x^{m-n+2} - x^{m-n} = x^{n+1} - x^n + x^3 - x^2$$

Comparando os graus $m - n + 2 = n + 1 \iff m - n = n - 1 \iff m = 2n - 1$. Portanto, $x^{m-n} = x^2$ e $x^n = x^3$ que nos leva a $m = 5$ e $n = 3$. Veja que de fato para todo inteiro k temos $k^5 + k - 1 = (k^3 + k^2 - 1)(k^2 - k + 1)$.

1.2 ORDEM E RAÍZES PRIMITIVAS

Problema 1.22. *(A) Determine a ordem de* 3 *módulo* 200.

Solução

Primeiro fatoramos 200 em potências de primos distintos $200 = 2^3 \cdot 5^2$. Calculando a ordem de 3 módulo cada potência temos $\text{ord}_8 3 = 2$ e $\text{ord}_{25} 3 = 20$, sabemos que $\text{ord}_5 3 = 4$ e basta verificar que $3^4 \not\equiv 1 \pmod{25}$. Concluímos que $\text{ord}_{200} 3 = \text{mmc}(2, 20) = 20$.

Problema 1.23. *(A) Encontre uma raiz primitiva módulo* 71.

Solução

O número $\varphi(71) = 70 = 2 \cdot 5 \cdot 7$ possui 8 divisores 1, 2, 5, 7, 10, 14, 35 e 70. Vamos testar se 2 é raiz primitiva. Sabemos que $\text{ord}_{71} 2 \mid 70$ e temos $2^1 \equiv 2 \pmod{71}$, $2^2 \equiv 4 \pmod{71}$, $2^5 \equiv 32 \pmod{71}$, $2^7 \equiv 57 \pmod{71}$, $2^{10} \equiv 30 \pmod{71}$, $2^{14} \equiv 54 \pmod{71}$ e $2^{35} \equiv 1 \pmod{71}$. Logo $\text{ord}_{71} 2 = 35$ e 2 não é raiz primitiva módulo 71. Porém, a partir dos resultados obtidos podemos provar que $69 \equiv -2 \pmod{71}$ é raiz primitiva. Veja que as potências de 69 com expoentes 1, 2, 5, 7, 10, 14 e 35 são congruentes a -2, 4, -32, -57, 30, 54 e -1 módulo 71. Portanto, $\text{ord}_{71} 69 = 70 = \varphi(71)$ e 69 é raiz primitiva de 71.

Vale notar que existem $\varphi(71-1) = 24$ raízes primitivas incongruentes módulo 71 e é possível listar todas elas com o auxílio de um computador: 7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68 e 69.

Problema 1.24. *(A) Sabendo que* $\text{ord}_{13^2} a = 4$*,* $\text{ord}_{11^2} a = 55$ *e* $\text{ord}_{7^2} a = 21$*, determine* $\text{ord}_{1001^2} a$*.*

Solução

Veja que $1001^2 = 7^2 \cdot 11^2 \cdot 13^2$ e temos $\text{ord}_{1001^2} a = \text{mmc}(\text{ord}_{7^2} a, \text{ord}_{11^2} a, \text{ord}_{13^2} a) = \text{mmc}(21, 55, 4) = 21 \cdot 55 \cdot 4 = 4620$.

Problema 1.25. *(OI) Prove que existem infinitos inteiros positivos* n *tais que* $n | 2^{2n} + 1$*.*

Solução

Vamos provar que a divisibilidade é verdadeira para $n = 5^k$ para qualquer k inteiro positivo. Veja que 2 é raiz primitiva de 5, pois $\varphi(5) = 4$, $2^1 \equiv 2 \pmod 5$ e $2^2 \equiv -1 \pmod 5$ não são congruentes a 1 módulo 5. Além disso, $2^4 \equiv 16 \not\equiv 1 \pmod{5^2}$ implicando que 2 é raiz primitiva módulo 5^2 e, consequentemente, módulo 5^k para todo k inteiro positivo. Com isso, $\text{ord}_{5^k} 2 = \varphi(5^k) = 5^k - 5^{k-1} = 4 \cdot 5^{k-1}$ implicando que $5^k \mid 2^{4 \cdot 5^{k-1}} - 1 = (2^{2 \cdot 5^{k-1}} - 1)(2^{2 \cdot 5^{k-1}} + 1)$. Mas veja que $2^{2 \cdot 5^{k-1}} \equiv (-1)^{5^{k-1}} \equiv -1 \pmod 5$ implicando que todos os fatores 5 estão em $2^{2 \cdot 5^{k-1}} + 1$. Temos $2^{2 \cdot 5^{k-1}} \equiv -1 \pmod{5^k} \Rightarrow 2^{2 \cdot 5^k} \equiv (-1)^5 \equiv -1 \pmod{5^k} \Rightarrow 5^k \mid 2^{2 \cdot 5^k} + 1$ para todo inteiro positivo k.

Problema 1.26. *(A) Determine uma raiz primitiva módulo* 7^3*.*

Solução

Veja que 3 é raiz primitiva módulo 7, pois $\varphi(7) = 6$ e $3^1 \equiv 3 \pmod 7$, $3^2 \equiv 2 \pmod 7$ e $3^3 \equiv -1 \pmod 7$ não são congruentes a 1 módulo 7. Como $3^6 \equiv 43 \not\equiv 1 \pmod{7^2}$ temos que 3 é raiz primitiva módulo 7^2 e, consequentemente, módulo 7^k para todo inteiro positivo k. Portanto, 3 é raiz primitiva de 7^3.

Problema 1.27. *(A) Encontre as ordens de* 2 *e* 5 *módulo* 101. *Encontre também todos os elementos de ordem* 20 *em* $(\mathbb{Z}/101\mathbb{Z})^\times$.

Solução

Observe que $\varphi(101) = 100$ e $\text{ord}_{101}\, a \mid 100$.

Para 2 temos $2^{10} \equiv 1024 \equiv 14 \pmod{101}$, $2^{20} \equiv 14^2 \equiv -6 \pmod{101}$ e $2^{50} \equiv 2^{20} \cdot 2^{20} \cdot 2^{10} \equiv (-6)^2 \cdot 14 \equiv -1 \pmod{101}$. Logo, a ordem de 2 não divide 20 nem 50. Como 100 só tem fatores 2 e 5 concluímos que $\text{ord}_{101}\, 2 = 100$. Note que 2 é raiz primitiva módulo 100.

Para 5 veja que $5^5 \equiv 3125 \equiv -6 \pmod{101}$ e $5^{25} \equiv (-6)^3(-6)^2 \equiv (-14) \cdot 36 \equiv 1 \pmod{101}$. Então $ord_{101}5$ divide 25 e não divide 5. Podemos concluir que $\text{ord}_{101}\, 5 = 25$. Usando o fato de 2 ser raiz primitiva de 101 vemos que $\text{ord}_{101}\, a = 20$ se, e somente se, $a \equiv 2^{5k} \pmod{101}$ em que $1 \leq 5k \leq 100 \Leftrightarrow 1 \leq k \leq 20$ e k não possui fatores 2 ou 5. Sabemos que todas as classes de congruências são potências da raiz primitiva e usando ordem

$$(2^{5k})^t \equiv 1 \pmod{101} \Leftrightarrow 100 = \text{ord}_{101}\, 2 \mid 5kt \Leftrightarrow 20 \mid t.$$

Temos as oito potências de 2.

$$2^5 \equiv 32 \pmod{101}$$

$$2^{15} \equiv 2^{10} \cdot 2^5 \equiv 14 \cdot 32 \equiv 44 \pmod{101}$$

$$2^{35} \equiv 2^{20} \cdot 2^{15} \equiv (-6) \cdot 44 \equiv 39 \pmod{101}$$

$$2^{45} \equiv 2^{10} \cdot 2^{35} \equiv 14 \cdot 39 \equiv 41 \pmod{101}$$

$$2^{55} \equiv 2^{10} \cdot 2^{45} \equiv 14 \cdot 41 \equiv 69 \pmod{101}$$

$$2^{65} \equiv 2^{10} \cdot 2^{55} \equiv 14 \cdot 69 \equiv 57 \pmod{101}$$

$$2^{85} \equiv 2^{20} \cdot 2^{65} \equiv (-6) \cdot 57 \equiv 62 \pmod{101}$$

$$2^{95} \equiv 2^{10} \cdot 2^{85} \equiv 14 \cdot 62 \equiv 60 \pmod{101}$$

Os elementos de $(\mathbb{Z}/101\mathbb{Z})^\times$ com ordem 20 são 32, 44, 39, 41, 69, 57, 62 e 60.

Problema 1.28. *(OI) Demonstre que* $2n \mid \varphi(a^n + 1)$ *para todo inteiro positivo* a.

Solução

Vamos calcular $\text{ord}_{a^n+1}\, a$. Veja que $a^n \equiv -1 \pmod{a^n+1} \Rightarrow a^{2n} \equiv 1 \pmod{a^n+1}$. Sabemos que $\text{ord}_{a^n+1}\, a \mid 2n$ e se $\text{ord}_{a^n+1}\, a < 2n$, então $\text{ord}_{a^n+1}\, a \leq \frac{2n}{2} = n$ que é o maior divisor próprio de $2n$, mas para $k \leq n$ sabemos que $a^k - 1 \leq a^n - 1 < a^n + 1$ e $\text{ord}_{a^n+1}\, a > n$. Concluímos que $\text{ord}_{a^n+1}\, a = 2n$ e $2n \mid \varphi(a^n + 1)$.

Problema 1.29 (IMO1978)**.** *(OI) Sejam m e n inteiros positivos com $m < n$. Se os três últimos algarismos de 1978^m são os mesmos que os três últimos algarismos de 1978^n, encontre m e n tais que $m+n$ assume o menor valor possível.*

Solução

Os três últimos dígitos são os mesmos quando $1978^n \equiv 1978^m \pmod{1000} \Leftrightarrow 1978^n \equiv 1978^m \pmod{2^3}$ e $1978^n \equiv 1978^m \pmod{5^3}$. A primeira congruência é verdadeira se, e somente se, $n > m \geq 3$, pois 1978 possui um fator 2 e $1978^n - 1978^m$ tem exatamente m fatores 2. Já a segunda congruência é equivalente a $1978^{n-m} \equiv 1 \pmod{5^3}$. O valor mínimo de $n-m$ é $k = \mathrm{ord}_{5^3} 1978$. Note que $1978 \equiv 3 \pmod{5^2}$. Veja que 3 é raiz primitiva de 5, pois $\varphi(5) = 4$, $3^1 \equiv 3 \pmod 5$ e $3^2 \equiv -1 \pmod 5$. Adicionando que $3^4 \equiv 6 \not\equiv 1 \pmod{5^2}$ podemos concluir que 3 é raiz primitiva módulo 5^t para todo inteiro positivo t. Veja que $1978^k \equiv 1 \pmod{5^3} \Rightarrow 1978^k \equiv 3^k \equiv 1 \pmod{5^2} \Rightarrow 20 \mid k$. E como k é ordem temos $k \mid \varphi(5^3) = 5^3 - 5^2 = 100$. Logo, $k = 20$ ou $k = 100$. Basta estudar 1978^{20} módulo 5^3:

$$1978^{20} = (25\cdot 79+3)^{20} = \cdots + \binom{20}{2} 25^2 \cdot 79^2 \cdot 3^{18} + \binom{20}{1} 25\cdot 79 \cdot 3^{19} + 3^{20} \equiv 3^{20} \not\equiv 1 \pmod{5^3},$$

pois para todo $m \geq 2$ o número 25^m possui $2m > 3$ fatores 5, $125 \mid \binom{20}{1}25 = 20\cdot 25$ e na última passagem usamos o fato de 3 ser raiz primitiva módulo 5^3. Portanto, $k = 100$. Portanto, $m+n$ assume o valor mínimo quando $m = 3$ e $n = 100 + m = 103$.

Problema 1.30. *(A) Sejam d e n números naturais tais que $d \mid 2^{2^n}+1$. Demonstre que existe um inteiro k tal que $d = k.2^{n+1}+1$.*

Solução

Seja p um fator primo de d. Temos que $d \mid 2^{2^n}+1$ implica que $p \mid 2^{2^n}+1$. Observe que $2^{2^n} \equiv -1 \pmod p \Rightarrow 2^{2^{n+1}} \equiv (-1)^2 \equiv 1 \pmod p$. Logo, $\mathrm{ord}_p 2 \mid 2^{n+1}$ e $\mathrm{ord}_p 2 \nmid 2^n$ implicando que $\mathrm{ord}_p 2 = 2^{n+1}$. Como a ordem sempre divide o φ temos $\mathrm{ord}_p 2 = 2^{n+1} \mid \varphi(T) = p-1 \Rightarrow p \equiv 1 \pmod{2^{n+1}}$. Veja que isso vale para qualquer fator primo p de d, então se fatorarmos d em primos temos a congruência $d \equiv p_1^{\theta_1} p_2^{\theta_2} \ldots p_m^{\theta_m} \equiv 1^{\theta_1} 1^{\theta_2} \ldots 1^{\theta_m} \equiv 1 \pmod{2^{n+1}} \Rightarrow d = k\cdot 2^{n+1}+1$ para algum inteiro k.

Problema 1.31. *(OI) Seja $k \geq 2$ e $n_1, n_2, \ldots, n_k \geq 1$ números naturais que tem a propriedade*

$$n_2 \mid (2^{n_1}-1), \quad n_3 \mid (2^{n_2}-1), \ldots, n_k \mid (2^{n_{k-1}}-1) \text{ e } n_1 \mid (2^{n_k}-1)$$

Demonstre que $n_1 = n_2 = \cdots = n_k = 1$.

Solução

Seja $M = \text{mmc}(n_1, n_2, \ldots, n_k)$. Se $M = 1$, então $n_1 = n_2 = \cdots = n_k = 1$. Suponha que $M \geq 2$. Veja que M possui divisores primos e que para cada primo p que divide M se M possui θ fatores p então $p^\theta \mid n_x$ para algum x implicando que $p^\theta \mid 2^{n_y} - 1$ e de $n_y \mid M$ temos $2^{n_y} - 1 \mid 2^M - 1 \Rightarrow p^\theta \mid 2^M - 1$. Fazendo isso para todas as potências de primo que dividem M podemos concluir que $M \mid 2^M - 1$. Seja q o menor primo que divide M. Temos $\text{mdc}(q-1, M) = 1$ e de $q \mid 2^M - 1$ e $q \mid 2^{q-1} - 1$ implica $q \mid 2^{\text{mdc}(M,q-1)} - 1 = 2^1 - 1 = 1$. Isso é uma contradição. Portanto, é impossível que M seja maior que 1.

Problema 1.32. *(A) Mostre que $x^3 - x + \overline{1}$ é irredutível em $\mathbb{Z}/3\mathbb{Z}[x]$. Encontre todas as raízes primitivas do corpo finito $\frac{\mathbb{Z}/3\mathbb{Z}[x]}{(x^3-x+\overline{1})}$.*

Solução

Seja $p(x) = x^3 - x + 1$. Se $p(x)$ é redutível, então $p(x) = g(x)h(x)$ onde $g(x)$ e $h(x)$ tem grau pelo menos 1, então um deles tem grau 1 implicando que $p(x)$ teria pelo menos uma raiz em $\mathbb{Z}/3\mathbb{Z}$. Mas isso não é verdade, pois $0^3 - 0 + 1 \equiv 1^3 - 1 + 1 \equiv 2^3 - 2 + 1 \equiv 1 \pmod 3$. Portanto, $p(x) = x^3 - x + 1$ é irredutível em $\mathbb{Z}/3\mathbb{Z}[x]$.
O corpo finito $\frac{\mathbb{Z}/3\mathbb{Z}[x]}{(x^3-x+1)}$ pode ser representado por polinômios de grau menor que ou igual a 2 com coeficientes 0, 1 ou 2. São 3 possibilidades para os coeficientes de x^2, de x^1 e de x^0 que nos dá $3^3 - 1 = 26$ termos não nulos. Com isso, para cada a nesse corpo temos $\text{ord}_{p(x)}\, a \mid 26$ e $\text{ord}_{p(x)}\, a = 1, 2, 13$ ou 26. Vamos testar se x é raiz primitiva módulo $f(x)$ em $\mathbb{Z}/3\mathbb{Z}[x]$. Veja que x e x^2 não são congruentes a 1. Temos

$$x^3 \equiv x - 1 \equiv x + 2 \pmod{f(x)}$$

$$\Rightarrow x^9 \equiv x^3 - 3x^2 + 3x - 1 \equiv x^3 - 1 \equiv x - 2 \equiv x + 1 \pmod{f(x)}$$

$$\Rightarrow x^{12} \equiv x^9 \cdot x^3 \equiv (x+1)(x+2) \equiv x^2 + 2 \pmod{f(x)}$$

$$\Rightarrow x^{13} \equiv x^{12} \cdot x \equiv (x^2+2)x \equiv x^3 + 2x \equiv 2 \equiv -1 \pmod{f(x)}$$

E concluímos que x é raiz primitiva módulo $f(x)$. Todas as classes de congruência são potências de x^t com $0 \leq t \leq 25$. Observe que $\text{ord}_{f(x)}\, x^t = 26 \iff \text{mdc}(t, 26) = 1$. Se o mdc = 1 então $(x^t)^k \equiv 1 \pmod{f(x)} \iff 26 \mid tk \iff 26 \mid k$ e $\text{ord}_{f(x)}\, x^t = 26$. E se mdc = $d > 1$ então $(x^t)^{26/d} \equiv (x^{26})^{t/d} \equiv 1 \pmod{f(x)}$ e $\text{ord}_{f(x)}\, x^t < 26$. As doze raízes primitivas são x^t com $0 \leq t \leq 25$ e $\text{mdc}(t, 26) = 1$ que podem são calculadas a seguir. Para fazer as contas usamos que $x^3 \equiv x + 2 \pmod{f(x)}$, $2x^3 \equiv 2x + 1 \pmod{f(x)}$, $x^4 \equiv x^2 + 2x \pmod{f(x)}$ e $2x^4 \equiv 2x^2 + x \pmod{f(x)}$ considerando os coeficientes módulo 3.

$$x^1 \equiv x \pmod{f(x)}$$

$$x^3 \equiv x+2 \pmod{f(x)}$$

$$x^5 \equiv x^3+2x^2 \equiv 2x^2+x+2 \pmod{f(x)}$$

$$x^7 \equiv 2x^4+x^3+2x^2 \equiv 2x^2+x+x+2+2x^2 \equiv x^2+2x+2 \pmod{f(x)}$$

$$x^9 \equiv (x^3)^3 \equiv x+1 \pmod{f(x)}$$

$$x^{11} \equiv x^3+x^2 \equiv x^2+x+2 \pmod{f(x)}$$

$$x^{15} \equiv x^{13}\cdot x^2 \equiv 2x^2 \pmod{f(x)}$$

$$x^{17} \equiv x^{13}\cdot x^4 \equiv 2x^4 \equiv 2x^2+x \pmod{f(x)}$$

$$x^{19} \equiv 2x^4+x^3 \equiv 2x^2+x+x+2 \equiv 2x^2+2x+2 \pmod{f(x)}$$

$$x^{21} \equiv 2x^4+2x^3+2x^2 \equiv 2x^2+x+2x+1+2x^2 \equiv x^2+1 \pmod{f(x)}$$

$$x^{23} \equiv x^4+x^2 \equiv x^2+2x+x^2 \equiv 2x^2+2x \pmod{f(x)}$$

$$x^{25} \equiv x^{13}\cdot x^{12} \equiv 2x^2+1 \pmod{f(x)}$$

Problema 1.33 (APMO1997)**.** *(OI) Encontre um n no conjunto $\{100, 101, \ldots 1997\}$ tal que n divide 2^n+2.*

Solução

O problema pede um número com tal propriedade. Então podemos tentar alguns formatos. Veja que $n = p$ ou $n = 2p$ para um $p > 3$ primo não funcionam, pois podemos usar o Teorema de Euler-Fermat e concluir que $2^p+2 \equiv 2+2 \equiv 4 \not\equiv 0 \pmod{p}$ e $2^{2p}+2 \equiv 2^2+2 \equiv 6 \not\equiv 0 \pmod{p}$. Agora tentaremos o formato $n = 2pq$ com p e q primos. Temos que $2pq \mid 2^{2pq}+2$ se, e somente se, $2 \mid 2^{2pq}+2$, $p \mid 2^{2pq}+2$ e $q \mid 2^{2pq}+2$. A primeira congruência é sempre verdadeira. A segunda é equivalente a $(2^p)^{2q} \equiv 2^{2q} \equiv -2 \pmod{p} \Leftrightarrow 2^{2q-1} \equiv -1 \pmod{p} \Rightarrow 2^{4q-2} \equiv 1 \pmod{p}$. Se conseguirmos primos p e q tais que $4q-2 = p-1 \Leftrightarrow p = 4q-1$ e $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ segunda divisibilidade é verdadeira. Na terceira teremos $q \mid 2^{2pq}+2 \Leftrightarrow q \mid (2^q)^{2p}+2 \Leftrightarrow q \mid 2^{2p}+2 = 2^{8q-2}+2 \Leftrightarrow q \mid (2^q)^8+2^3 \Leftrightarrow q \mid 2^8+2^3 = 8\cdot 33$. Temos dois casos $q = 3$ ou $q = 11$. Se $q = 3$ então $p = 4\cdot 3-1 = 11$ é primo e temos $2^5 \equiv -1 \pmod{11}$, mas $n = 2\cdot 3\cdot 11 = 66$ não está no intervalo pedido. Se $q = 11$ temos $p = 4\cdot 11-1 = 43$ é primo e $2^{21} \equiv (2^7)^3 \equiv (-1)^3 \equiv -1 \pmod{43}$. Observe que $n = 2\cdot 11\cdot 43 = 946$ está no intervalo e satisfaz as condições.

Problema 1.34. *(A) Definimos a* função de Carmichael $\lambda\colon \mathbb{N} \to \mathbb{N}$ *como o menor inteiro positivo tal que $a^{\lambda(n)} \equiv 1 \pmod{n}$ para todo a primo com n. Observe que, pelo teorema da Raiz Primitiva, $\lambda(p^l) = p^{l-1}(p-1)$ para todo p primo ímpar. Mostre que*

(a) $\lambda(2) = 1$, $\lambda(4) = 2$ *e* $\lambda(2^l) = 2^{l-2}$ *para todo* $l \geq 3$.

(b) Se $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ *é a fatoração em primos de* n, *então*

$$\lambda(n) = \text{mmc}\{\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_k^{\alpha_k})\}.$$

Solução

(a) Veja que $\text{mdc}(a, 2^n) = 1$ para $n \geq 1$ se, e somente se, a é ímpar. Assim, $a = 2k+1$ para algum k inteiro. Temos $a^1 \equiv 1 \pmod 2$. Logo, $\lambda(2) = 1$. Veja que a ímpar temos a congruente a 1 ou 3 módulo 4, mas $a^2 \equiv (2k+1)^2 \equiv 4k^2 + 4k + 1 \equiv 1 \pmod 4$. Portanto, $\lambda(4) = 2$. Para $n = 3$ e a ímpar temos $a^2 - 1 = (a-1)(a+1)$. Se $a \equiv 1 \pmod 4$ então $2^2 \mid a-1$ e $2^1 \mid a+1$ e se $a \equiv 3 \pmod 4$ então $2^1 \mid a-1$ e $2^2 \mid a+1$. Logo, $2^3 \mid a^2 - 1$ para qualque a ímpar. Para $a = 3$ temos $2^3 \nmid a - 1$. Podemos concluir que $\lambda(2^3) = 2$. Observe também que $2^4 \nmid a^2 - 1$ para $a = 3$ provando que $a^2 - 1$ pode ter exatamente 3 fatores 2. Para $n \geq 4$ vamos calcular a quantidade de fatores 2 no número $a^{2^{n-2}} - 1$ usando a fatoração da diferença de quadrados.

$$a^{2^{n-2}} - 1 = (a^{2^{n-3}} + 1)(a^{2^{n-3}} - 1) = (a^{2^{n-3}} + 1) \ldots (a+1)(a-1)$$

Temos que $(a+1)(a-1)$ possui exatamente 3 fatores 2 ou mais que 3 fatores e que $a^{2^t} + 1$ possui exatamente um fator 2, pois $a^{2^t} + 1 \equiv (a^2)^{2^{t-1}} + 1 \equiv 2 \pmod 4$. Logo $a^{2^{n-2}} - 1$ possui exatamente $(n-3) + 3 = n$ fatores 2 ou mais. Concluímos que $\lambda(2^n) = 2^{n-2}$, pois $a^{2^{n-2}} - 1$ tem n fatores 2 e $a^{2^{n-3}} - 1$ pode ter exatamente $n-1$ fatores 2.

(b) Seja $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Veja que $a^{\lambda(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}} \Rightarrow a^{\lambda(k \cdot p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}$. Então se m é múltiplo de cada $\lambda(p_i^{\alpha_i})$, então $a^m \equiv 1 \pmod{p_i^{\alpha_i}}$ para todo i e $a^m \equiv 1 \pmod n$.
Por outro lado, $n \mid a^{\lambda(n)} - 1$ para todo a primo com n. Temos $n \mid a^{\lambda(n)} - 1 \Rightarrow p_i^{\alpha_i} \mid a^{\lambda(n)} - 1 \Rightarrow \text{ord}_{p_i^{\alpha_i}} a \mid \lambda(n)$. Seja g uma raiz primitiva módulo $p_i^{\alpha_i}$. Tome a uma solução das congruências $a \equiv g \pmod{p_i^{\alpha_i}}$ e $a \equiv 1 \pmod{p_j^{\alpha_j}}$ para $j \neq i$. Tal a existe pelo Teorema Chinês dos Restos. Para esse a temos $\text{ord}_{p_i^{\alpha_i}} a = \varphi(p_i^{\alpha_i}) = \lambda(p_i^{\alpha_i})$ e $\lambda(p_i^{\alpha_i}) \mid \lambda(n)$. Essa divisibilidade é verdadeira para todo i.
Assim, $\lambda(n)$ tem que ser múltiplo dos $\lambda(p_i^{\alpha_i})$ e se esse expoente é múltiplo de todos os $\lambda(p_i^{\alpha_i})$ então $m \mid a^{\lambda(n)} - 1$. Concluímos que

$$\lambda(n) = \text{mmc}\{\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_k^{\alpha_k})\}.$$

Problema 1.35 (IMO2000). *(OA) Existe um inteiro N divisível por exatamente* 2000 *primos diferentes e tal que N divide $2^N + 1$?*

Dica: Tente construir indutivamente inteiros N_k divisíveis por exatamente k primos distintos e tais que $N_k \mid 2^{N_k} + 1$.

Solução

Vamos provar primeiro que para $a \geq 8$ que $a^3 + 1$ possui um fator primo p com $p > 3$ e $p \nmid a + 1$. Veja que $a^3 + 1 = (a+1)(a^2 - a + 1)$ e usando $\text{mdc}(a+1, a^2 - a + 1) = d$ temos $a \equiv -1 \pmod{d}$. Daí, $0 \equiv a^2 - a + 1 \equiv (-1)^2 - (-1) + 1 \equiv 3 \pmod{d} \Rightarrow d \mid 3 \Rightarrow d = 1$ ou $d = 3$. Se $3 \nmid a + 1$ então $d = 1$ e qualquer fator primo de $a^2 - a + 1 \geq 8^2 - 8 + 1 = 57$ já serve. Se $3 \mid a + 1$ então $a = 3k - 1$ e $a^2 - a + 1 = (3k-1)^2 - (3k-1) + 1 = 9k^2 - 6k + 1 - 3k + 1 + 1 = 9k^2 - 9k + 3$ só tem um fator 3 e é maior que 3. Assim, $a^2 - a + 1$ tem um fator $p > 3$ que não divide $a + 1$.

Agora vamos construir indutivamente os N_k. Tome $N_1 = 3$, pois $3 \mid 2^3 + 1$. A partir de N_k tomemos

$$2^{3N_k} + 1 = (2^{N_k})^3 + 1 = (2^{N_k} + 1)(2^{2N_k} - 2^{N_k} + 1)$$

Pelo resultado que vimos anteriormente, podemos tomar um fator primo p_{k+1} de $2^{2N_k} - 2^{N_k} + 1$ que não divide $2^{N_k} + 1$ e construir o número $N_{k+1} = 3 \cdot N_k \cdot p_{k+1}$ que possui exatamente $k + 1$ fatores primos distintos. De $N_{k+1} \mid 2^{3N_k} + 1$ e $3N_k \mid N_{k+1}$ temos $N_{k+1} \mid 2^{N_{k+1}} + 1$.

A partir dessa construção, o N_{2000} possui exatamente 2000 fatores primos distintos e $N_{2000} \mid 2^{N_{2000}} + 1$.

Problema 1.36 (IMO1990). *(OA) Encontre todos os números naturais n tais que $n^2 \mid 2^n + 1$.*

Solução

Se $n = 1$ a divisbilidade é verdadeira. Se $n > 1$ então podemos tomar p como o menor fator primo de n. Veja que $p > 2$, pois $n^2 \mid 2^n + 1$ que é ímpar. Temos que $p \mid 2^n + 1 \Rightarrow p \mid 2^{2n} - 1$ e $p \mid 2^{p-1} - 1$. Veja que $\text{mdc}(n, p-1) = 1 \Rightarrow \text{mdc}(2n, p-1) = 2$ e $p \mid 2^2 - 1 = 3 \Rightarrow p = 3$. Suponha que $n = 3^k n_0$ em que $3 \nmid n_0$ e $k \geq 1$. Jogando isso na divisibilidade

$$3^{2k} n_0^2 \mid 2^{2n} - 1$$

Porém, 2 é raiz primitiva módulo 3^{2k}, pois $2^2 \equiv 4 \pmod{9}$ e $2^3 \equiv -1 \pmod{9}$ implicando que 2 é raiz primitiva módulo 3^2. Temos que $\text{ord}_{3^{2k}} 2 = \varphi(3^{2k}) = 2 \cdot 3^{2k-1}$. Então teríamos que $2 \cdot 3^{2k-1} \mid 2n \iff 2k - 1 \leq k \iff k = 1$.

Se $d = 1$ então $n = 3$ que é solução, pois $3^2 \mid 2^3 + 1$.
Se $d > 1$ tome o menor primo q que divide d. Temos $q \geq 5$ e $\text{mdc}(q-1, d) = 1 \Rightarrow \text{mdc}(q-1, 2n) = \text{mdc}(q-1, 6d) = \text{mdc}(q-1, 6) \mid 6$. Usando esse primo q temos $q \mid 2^{q-1} - 1$ e $q \mid 2^{2n} - 1$ implicam que $q \mid 2^{\text{mdc}(q-1,2n)} - 1 \Rightarrow q \mid 2^6 - 1 = 63 \Rightarrow q = 7$, pois $q \neq 3$. Mas veja que $7 \nmid 2^n + 1$, pois $\text{ord}_7 2 = 3$ e as únicas congruências possíveis de potências de 2 módulo 7 são $2^1 \equiv 2 \pmod 7$, $2^2 \equiv 4 \pmod 7$ e $2^3 \equiv 1 \pmod 7$.
Portanto, as únicas soluções de $n^2 \mid 2^n + 1$ são 1 e 3.

Problema 1.37 (IMO1999). *(OA) Encontre todos os pares (n, p) de inteiros positivos tais que p é primo, $n \leq 2p$ e $(p-1)^n + 1$ é divisível por n^{p-1}.*

Solução

Se $n = 1$ temos solução $(1, p)$ para qualquer primo p. Daqui para frente $n \geq 2$.
Se $p = 2$ temos $n \mid (2-1)^n + 1 = 2 \iff n = 2$ e nos dá a nova solução $(2, 2)$. A partir desse ponto trataremos $p \geq 3$.
Se $p \geq 3$ então p é ímpar, $(p-1)^n + 1$ é ímpar e n ímpar, pois é divisor de um número ímpar. Seja q o menor divisor primo de n. Veja que $q \mid n$ e $n \mid (p-1)^n + 1 \Rightarrow (p-1)^n \equiv -1 \pmod q$. Observe que $\text{mdc}(p-1, q) = 1$ e sabemos também que $(p-1)^{q-1} \equiv 1 \pmod p$ pelo Teorema de Euler-Fermat. Pelo Teorema de Bachet-Bézout existem inteiros positivos α e β tais que $n\alpha = (q-1)\beta + 1$. Como q é ímpar o número $(q-1)\beta + 1$ é ímpar e, consequentemente, α é ímpar. Logo, $-1 = (-1)^\alpha \equiv (p-1)^{n\alpha} \equiv (p-1)^{(q-1)\beta+1} \equiv ((p-1)^{q-1})^\beta (p-1) \equiv p-1 \pmod q \Rightarrow q \mid p \Rightarrow q = p$. Das condições $p \mid n$, n ímpar e $n \leq 2p$ podemos concluir que $n = p$. A divisibilidade passa a ser $p^{p-1} \mid (p-1)^p + 1 = p^p - \binom{p}{p-1} p^{p-1} + \cdots - \binom{p}{2} p^2 + \binom{p}{1} p - 1 + 1 = p^p - \cdots - \frac{p(p-1)}{2} p^2 + p^2 = p^2(pt+1)$ que é verdadeira para $p - 1 \leq 2 \iff p = 3$. Encontramos a solução $(3, 3)$.
As soluções (n, p) são $(1, p)$, onde p é um primo qualquer, $(2, 2)$ e $(3, 3)$.

Problema 1.38 (Banco-IMO2000). *(OA) Determine todas as triplas (a, m, n) de inteiros positivos tais que $a^m + 1 \mid (a+1)^n$.*

Solução

Observe que $(a, 1, n)$ e $(1, m, n)$ são soluções. Agora vamos ver as soluções com $a > 1$ e $m > 1$.
Se m é par, então $a^m + 1 \equiv (-1)^m + 1 \equiv 2 \pmod{a+1}$. Temos $\text{mdc}(a^m + 1, a + 1) = \text{mdc}(2, a+1) = 1$ ou 2. Isso implica que $a^m + 1 \mid 2^n$ e $a^m + 1 = 2^k$. Veja que $2 < a^m + 1 = (a^2)^{m/2} + 1 \equiv 2 \pmod 4$ e não temos solução.
Se m é ímpar, então podemos tomar $m = p \cdot m_1$. Nesse caso, $(a+1)^n \mid (a^{m_1} + 1)^n$ e de

$a^m+1 \mid (a+1)^n$ temos $(a^{m_1})^p+1 \mid (a^{m_1}+1)^n$. Mudando a variável para $b=a^{m_1}$ temos $b^p+1 \mid (b+1)^n$. Por outro lado, veja que

$$\frac{b^p+1}{b+1} = b^{p-1}-b^{p-2}+\cdots-b+1 \mid (b+1)^n$$

Lembrando que $b \equiv -1 \pmod{b+1}$ temos

$$b^{p-1}-b^{p-2}+\cdots-b+1 \equiv 1-(-1)+\cdots-(-1)+1 \equiv p \pmod{b+1}$$

Isso implica que $\text{mdc}(b^{p-1}-b^{p-2}+\cdots-b+1, b+1) = 1$ ou p. Se for 1 temos $b^{p-1}-b^{p-2}+\cdots-b+1 \mid 1 \Rightarrow b^{p-1}-b^{p-2}+\cdots-b+1=1 \Rightarrow b^p+1=b+1 \Rightarrow p=1$ que é falso. Se for p então $b^{p-1}-b^{p-2}+\cdots-b+1=p^k$ e $p \mid b+1 \Rightarrow b=tp-1$. Com isso,

$$\frac{b^p+1}{b+1} = \frac{(tp)^p-\cdots-\binom{p}{2}(tp)^2+\binom{p}{1}(tp)-1+1}{tp}$$

$$= (tp)^{p-1}-\ldots\frac{p(p-1)}{2}(tp)+p \equiv p \pmod{p^2}$$

Nessa última passagem, veja que todos os termos exceto o último p possuem dois ou mais fatores p. Logo, $p^k = b^{p-1}-b^{p-2}+\cdots-b+1 = p(p\alpha+1) \Rightarrow k=1$. Mas $\frac{b^p+1}{b+1}=p \iff b^p+1=p(b+1)$. Se $b=2$ temos $2^p+1=3p$ que vale $p=3$ e para $p \geq 5$ tem-se $2^p+1>3p$.

Se $b \geq 3$ temos $b^3+1>3(b+1)$ e se $b^k>k(b+1)-1$ então $b^{k+1}>kb(b+1)-b \geq 3k(b+1)-b>(k+1)(b+1)-1$. Não há soluções para $b>2$.

Assim, $b=2$ e $p=3$. Temos $a^{m_1}=2 \iff a=2$ e $m_1=1$. E isso nos diz que as soluções só podem ser $(a,m,n)=(2,3,n)$. Essas triplas funcionam se, e somente se, $2^3+1=9 \mid 3^n \iff n \geq 2$.

As soluções são $(a,1,n)$, para quaisquer inteiros positivos a e n, $(1,m,n)$, para quaisquer inteiros positivos m e n, e $(2,3,n)$, para n inteiro positivo com $n \geq 2$.

1.3 RESÍDUOS QUADRÁTICOS E SÍMBOLO DE LEGENDRE

Problema 1.39. *(A) Calcule* $\left(\frac{2}{7}\right)$, $\left(\frac{3}{11}\right)$ *e* $\left(\frac{5}{13}\right)$.

Solução

Usando os resultados demonstrados

$$\left(\frac{2}{7}\right) = (-1)^{\frac{7^2-1}{8}} = 1.$$

$$\left(\frac{3}{11}\right) \equiv 3^{\frac{11-1}{2}} \equiv 3^5 \equiv 1 \pmod{11} \Rightarrow \left(\frac{3}{11}\right) = 1.$$

$$\left(\frac{5}{13}\right) \equiv 5^{\frac{13-1}{2}} \equiv 5^6 \equiv (5^2)^3 \equiv (-1)^3 \equiv -1 \pmod{13} \Rightarrow \left(\frac{5}{13}\right) = -1.$$

Problema 1.40. *(A) Quantos pontos de coordenadas inteiras existem no interior do triângulo de vértices* $(0,0)$, $(3/2,0)$ *e* $(3/2,2012)$ *?*

Solução

A reta por $(0,0)$ e $(3/2,2012)$ é da forma $y = mx$ e para determinar m temos $2012 = m \cdot 3/2 \iff m = 1341 + 1/3$. O único x inteiro com $0 < x < 3/2$ é $x = 1$. Então são 1341 pontos de coordenadas inteiras, a saber $(1,1)$, $(1,2)$, $\ldots$, $(1,1341)$.

Problema 1.41. *(A) Seja* $p > 3$ *primo. Quantos pontos de coordenadas inteiras existem no interior do triângulo de vértices* $(0,0)$, $(p/2,0)$ *e* $(p/2,3)$ *?*

Para quais primos p *o polinômio* $x^2 - 3$ *é redutível módulo* p *?*

Solução

A reta definida por $(0,0)$ e $(p/2,3)$ tem equação $y = mx$ com $3 = mp/2 \iff m = 6/p$. Para cada $k = 1, 2, \ldots, \frac{p-1}{2}$ contaremos os pontos N_k em que a primeira coordenada é k. Os pontos vão de 1 até $\left\lfloor \frac{6k}{p} \right\rfloor$. Sabemos que para $p > 3$ temos $p = 6a+1$ ou $p = 6a+5$. Se $p = 6a+1$, então $\frac{p-1}{2} = 3a$ e $\left\lfloor \frac{6k}{p} \right\rfloor = 0$ para $1 \leq k \leq a$, $\left\lfloor \frac{6k}{p} \right\rfloor = 1$ para $a+1 \leq k \leq 2a$ e $\left\lfloor \frac{6k}{p} \right\rfloor = 2$ para $2a+1 \leq k \leq 3a$. Portanto, $N = a \cdot 0 + (2a-a) \cdot 1 + (3a-2a) \cdot 2 = 3a = \frac{p-1}{2}$. Se $p = 6a+5$, então $\frac{p-1}{2} = 3a+2$ e $\left\lfloor \frac{6k}{p} \right\rfloor = 0$ para $1 \leq k \leq a$, $\left\lfloor \frac{6k}{p} \right\rfloor = 1$ para $a+1 \leq k \leq 2a+1$ e $\left\lfloor \frac{6k}{p} \right\rfloor = 2$ para $2a+2 \leq k \leq 3a+2$. Portanto, $N = a \cdot 0 + ((2a+1)-a) \cdot 1 + ((3a+2)-(2a+1)) \cdot 2 = 3a+3 = \frac{p-1}{2} + 1$.
Sabemos que $(\frac{3}{p}) = (-1)^N$, que é um resultado conhecido de reciprocidade quadrática, e esse resultado depende da paridade de a em cada caso. O que nos leva à congruência de p módulo 12.

(i) Se $p = 12m+1$ então $p = 6a+1$, a par e $(\frac{3}{p}) = (-1)^{3a} = 1$.

(ii) Se $p = 12m+5$ então $p = 6a+5$, a par e $(\frac{3}{p}) = (-1)^{3a+3} = -1$.

(iii) Se $p = 12m+7$ então $p = 6a+1$, a ímpar e $(\frac{3}{p}) = (-1)^{3a} = -1$.

(iv) Se $p = 12m+11$ então $p = 6a+5$, a ímpar e $(\frac{3}{p}) = (-1)^{3a+3} = 1$.

Concluímos que $x^2 - 3$ é redutível módulo p quando $p \equiv \pm 1 \pmod{12}$.

Problema 1.42. *(T) a) (Euler) Seja* $F_n = 2^{2^n} + 1$ *o n-ésimo número de Fermat. Prove que todo fator primo de* F_n *é da forma* $k \cdot 2^{n+1} + 1$.

b)(Lucas) Prove que, se $n \geq 2$, então todo fator primo de F_n é da forma $k \cdot 2^{n+2} + 1$.

c) Mostre que $2^{2^5} + 1$ é composto.

Solução

a) Se $p \mid 2^{2^n} + 1$ então $p \mid 2^{2^{n+1}} - 1$ e podemos determinar a ordem. Veja que $\text{ord}_p 2 \mid 2^{n+1}$ e $\text{ord}_p 2 \nmid 2^n$ implicando $\text{ord}_p 2 = 2^{n+1}$. Para p primo sabemos que $\text{ord}_p 2 \mid p-1 \iff 2^{n+1} \mid p-1 \Rightarrow p = 2^{n+1}k + 1$.

b) Para $n \geq 2$ temos $p = 2^{n+1}k + 1 \equiv 1 \pmod 8$ que $(\frac{2}{p}) = 1$ e existe x inteiro tal que $x^2 \equiv 2 \pmod p$. Pelo resultado do item anterior $p \mid 2^{2^n} + 1 \Rightarrow p \mid x^{2^{n+1}} + 1 \Rightarrow p \mid x^{2^{n+2}} + 1$. Temos $\text{ord}_p x = 2^{n+2} \mid p - 1$ e $p = 2^{n+2}k + 1$.

c) Pelo item anterior, se $p \mid 2^{2^5} + 1$ então $p = 2^7 k + 1$. Testando os valores de k percebemos que para $k = 5$ temos que $p = 641$ é primo, que $641 = 625 + 16 = 5^4 + 2^4$ e que

$$2^{32} \equiv (2^4)^7 \cdot 2^4 \equiv (2^4)^7 \cdot (-5^4) \equiv -(2^7 \cdot 5)^4 \equiv -1 \pmod{641} \Rightarrow 641 \mid 2^{32} + 1.$$

Então $2^{2^5} + 1$ é composto, pois é múltiplo de 641 e maior 641.

1.4 LEI DE RECIPROCIDADE QUADRÁTICA

Problema 1.43. *(A) Calcular $(\frac{44}{103})$, $(\frac{-60}{1019})$ e $(\frac{2010}{1019})$.*

Solução

Temos $(\frac{44}{103}) = (\frac{4}{103}) \cdot (\frac{11}{103}) = (\frac{11}{103})$. Veja que $(\frac{103}{11}) = (\frac{4}{11}) = 1$ e pela Lei da Reciprocidade Quadrática

$$\left(\frac{11}{103}\right) \cdot \left(\frac{103}{11}\right) = (-1)^{\frac{11-1}{2}\frac{103-1}{2}} = -1 \Rightarrow \left(\frac{11}{103}\right) = -1 \Rightarrow \left(\frac{44}{103}\right) = -1.$$

Temos $(\frac{-60}{1019}) = (\frac{-1}{1019}) \cdot (\frac{4}{1019}) \cdot (\frac{3}{1019}) \cdot (\frac{5}{1019})$. Veja que $1019 \equiv 3 \pmod 4 \Rightarrow (\frac{-1}{1019}) = -1$, $(\frac{4}{1019}) = 1$, $1019 \equiv 11 \pmod{12} \Rightarrow (\frac{3}{1019}) = 1$ e $2^{10} = 1024 \equiv 5 \pmod{1019} \Rightarrow (\frac{5}{1019}) = 1$. Logo,

$$\left(\frac{-60}{1019}\right) = (-1) \cdot 1 \cdot 1 \cdot 1 = -1$$

Para o terceiro valor, temos $(\frac{2010}{1019}) = (\frac{2}{1019}) \cdot (\frac{3}{1019}) \cdot (\frac{5}{1019}) \cdot (\frac{67}{1019})$. Sabemos que $1019 \equiv 3 \pmod 8 \Rightarrow (\frac{2}{1019}) = -1$, $1019 \equiv 11 \pmod{12} \Rightarrow (\frac{3}{1019}) = 1$ e $2^{10} = 1024 \equiv 5 \pmod{1019} \Rightarrow (\frac{5}{1019}) = 1$. Para $(\frac{67}{1019})$ usaremos a Lei da Reciprocidade Quadrática e que $(\frac{1019}{67}) = (\frac{14}{67}) = (\frac{9^2}{67}) = 1$ temos

$$\left(\frac{67}{1019}\right) \cdot \left(\frac{1019}{67}\right) = (-1)^{\frac{67-1}{2}\frac{1019-1}{2}} = -1 \Rightarrow \left(\frac{67}{1019}\right) = -1.$$

Com isso,

$$\left(\frac{2010}{1019}\right) = (-1)\cdot 1\cdot 1\cdot(-1) = 1.$$

Problema 1.44. *(A) Prove que o polinômio $x^4 - 16x^2 + 4$ é irredutível em $\mathbb{Z}[x]$ mas não é irredutível em $(\mathbb{Z}/(T))[x]$ para nenhum primo p.*

Solução

Fazendo uma mudança de variável $y = x^2$ podemos resolver $y^2 - 16y + 4 = 0$. O discriminante $\Delta = (-16)^2 - 4\cdot 1\cdot 4 = 240$ não é um quadrado perfeito. Logo, os quadrados das raízes são irracionais e o polinômio não tem raízes racionais. Se esse polinômio fosse redutível, então teria que ser o produto de dois polinômios de grau 2. Mas $x^4 - 16x^2 + 4 = (x^2 + ax + c)(x^2 + bx + d)$ implica no coeficiente de x^3 a igualdade $0 = a + b \iff b = -a$, no coeficiente de x^2 a igualdade $c + d + ab = -16 \iff c + d - a^2 = -16 \iff a^2 = c + d + 16$, no coeficiente de x a igualdade $ad + bc = 0$ e no coeficiente de x^0 a igualdade $cd = 4$. Fazendo as possibilidades do produto ser 4 temos $c + d = -5, -4, 4$ ou 5 e $a^2 = 11, 12, 20$ ou 20. Então a não pode ser inteiro e concluímos que $x^4 - 16x^2 + 4$ é irredutível em $(\mathbb{Z}/(T))[x]$.
Para fatorar em $(\mathbb{Z}/(T))[x]$ faremos três casos.

1. Se $(\frac{20}{p}) = 1$, então $a^2 \equiv 20 \pmod{p}$ e podemos fatorar o polinômio

$$x^4 - 16x^2 + 4 = x^4 + 4x^2 + 4 - 20x^2 = (x^2 + 2)^2 - (ax)^2 = (x^2 + 2 - ax)(x^2 + 2 + ax).$$

2. Se $(\frac{12}{p}) = 1$, então $b^2 \equiv 12 \pmod{p}$ e podemos fatorar o polinômio

$$x^4 - 16x^2 + 4 = x^4 - 4x^2 + 4 - 12x^2 = (x^2 - 2)^2 - (bx)^2 = (x^2 - 2 - bx)(x^2 - 2 + bx).$$

3. Se $(\frac{60}{p}) = 1$, então $c^2 \equiv 60 \pmod{p}$ e podemos fatorar o polinômio

$$x^4 - 16x^2 + 4 = x^4 - 16x^2 + 64 - 60 = (x^2 - 8)^2 - c^2 = (x^2 - 8 - c)(x^2 - 8 + c).$$

Veja que um desses casos sempre acontece, pois se $(\frac{20}{p}) = -1$ e $(\frac{12}{p}) = -1$, então $(\frac{20\cdot 12}{p}) = (\frac{4\cdot 60}{p}) = (-1)(-1) = 1 \Rightarrow (\frac{60}{p}) = 1$.

Problema 1.45. *(OI) Sejam p um primo ímpar e c um inteiro que não é múltiplo de p. Prove que*

$$\sum_{a=0}^{p-1}\left(\frac{a(a+c)}{p}\right) = -1.$$

Solução

Se $a = 0$ então $(\frac{a(a+c)}{p}) = 0$ e não influencia a soma. Se $a \not\equiv 0 \pmod{p}$ então existe um inteiro a' tal que $a \cdot a' = 1$ e podemos escrever

$$\left(\frac{a(a+c)}{p}\right) = \left(\frac{a(a+aa'c)}{p}\right) = \left(\frac{a^2)}{p}\right)\left(\frac{a'c+1}{p}\right) = \left(\frac{a'c+1}{p}\right)$$

Quando variamos a de 1 a $p-1$ obtemos os $p-1$ resíduos não nulos distintos em $a'c$. Logo, a soma pedida é

$$\sum_{a=0}^{p-1}\left(\frac{a(a+c)}{p}\right) = \sum_{b=1}^{p-1}\left(\frac{b+1}{p}\right) = \sum_{c=2}^{p}\left(\frac{c}{p}\right).$$

Sabemos que $x^2 \equiv y^2 \pmod{p} \iff x \equiv \pm y \pmod{p}$ e existem exatamente $\frac{p-1}{2}$ resíduos quadráticos não nulos módulo p, a saber $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$. Então a soma tem $\frac{p-1}{2} - 1$ parcelas 1 (veja que 1 não aparece no $b+1$), $\frac{p-1}{2}$ parcelas -1 e mias uma parcela 0 (justamente quando $a'c \equiv -1 \pmod{p} \iff c \equiv -a \pmod{p}$). Concluímos que $\sum_{a=0}^{p-1}(\frac{a(a+c)}{p}) = -1$.

Problema 1.46. *(OI) Existem inteiros m e n tais que*

$$5m^2 - 6mn + 7n^2 = 1985\,?$$

Solução

Multiplicando os dois lados da equação por 5 podemos montar um quadrado perfeito do lado esquerdo

$$25m^2 - 30mn + 35n^2 = 9925 \iff (5m - 3n)^2 + 26n^2 = 9925$$

Usando módulo 13 se essa equação possui solução então $(\frac{9925}{13}) = 1 \iff (\frac{6}{13}) = 1 \iff (\frac{2}{13}) \cdot (\frac{3}{13}) = 1$. Mas $13 \equiv 5 \pmod{8} \Rightarrow (\frac{2}{13}) = -1$ e $13 \equiv 1 \pmod{12} \Rightarrow (\frac{3}{13}) = 1$. Logo, $(\frac{6}{13}) = -1$, 9925 não é resíduo quadrático módulo 13 e a equação não possui solução.

Problema 1.47. *(A) Demonstre que a congruência $6x^2 + 5x + 1 \equiv 0 \pmod{m}$ tem solução para todo valor natural de m.*

Solução

Veja que

$$6x^2 + 5x + 1 = \frac{144x^2 + 120x + 24}{24} = \frac{(12x+5)^2 - 1}{24}.$$

Podemos fatorar m como $m = 2^a \cdot 3^b \cdot m_0$ em que m_0 não possui fatores 2 nem 3. Observe que $x^2 \equiv 1 \pmod{t} \iff x \equiv 1 \pmod{t}$ ou $x \equiv -1 \pmod{t}$. Para m_0 podemos

encontrar $x_1 \pmod{m_0}$ tal que $12x_1 + 5 \equiv 1 \pmod{m_0}$, pois $\text{mdc}(12, m_0) = 1$. Para 2^a veja que podemos encontrar x_2 tal que $12x_2 + 5 \equiv 1 \pmod{2^{a+3}} \iff 4(3x_2 + 1) \equiv 0 \pmod{2^{a+3}} \iff 3x_2 + 1 \equiv 0 \pmod{2^{a+1}}$, pois 3 é primo com 2^{a+1}. Para 3^b podemos encontrar x_3 tal que $12x_3 + 5 \equiv -1 \pmod{3^{b+1}} \iff 3(4x_3 + 2) \equiv 0 \pmod{3^{b+1}} \iff 4x_3 + 2 \equiv 0 \pmod{3b}$, pois 4 é primo com 3^b. Pelo Teorema Chinês dos Restos podemos encontrar um inteiro positivo x tal que $x \equiv x_1 \pmod{m_0}$, $x \equiv x_2 \pmod{2^{a+1}}$ e $x \equiv x_3 \pmod{3^b}$. Para esse inteiro positivo $24m \mid 6x^2 + 5x + 1 \iff m \mid \frac{(12x+5)^2-1}{24}$.

Problema 1.48. *(OI) Demonstre que existem infinitos primos da forma $3k+1$ e $3k-1$.*

Solução

Suponha que existe uma quantidade finita de primos da forma $3k-1$. Dessa suposição podemos listar todos os primos dessa forma $P_1, P_2, \ldots, P_{t-1}$ e P_t. Considere o número $N = 3P_1P_2 \ldots P_t - 1$. Se todos os primos que dividem N fossem $3k+1$ então $N \equiv 1 \pmod 3$. Porém, $N \equiv -1 \pmod 3$ e algum primo q divide N e é congruente a 2 módulo 3. Veja que $P_i \mid N+1 \Rightarrow P_i \nmid N$ e esse primo q não estava na lista de todos os primos $3k-1$. Temos uma contradição e a quantidade de primos da forma $3k-1$ é infinita.
Agora, para primos da forma $3k+1$. Novamente, suponha que a quantidade é finita e que $P_1, P_2, \ldots, P_{t-1}$ e P_t são todos os primos dessa forma. Considere o número $N = (2P_1P_2 \ldots P_t)^2 + 3$. Por construção, vemos que $2 \nmid N$ e $3 \nmid N$. Seja q um fator primo de N. Sabemos que $q > 3$ e que $q \neq P_i$, pois cada P_i divide $N - 3$. Veja que $(\frac{-3}{q}) = 1 \iff ((\frac{3}{q})((\frac{-1}{q})) = 1 \iff (\frac{3}{q}) = (\frac{-1}{q})$. Sabemos que $(\frac{-1}{q}) = 1$ se $q \equiv 1 \pmod 4 \iff q \equiv 1, 5 \text{ ou } 9 \pmod{12}$ e $(\frac{-1}{q}) = -1$ se $q \equiv 3 \pmod 4 \iff q \equiv 3, 7 \text{ ou } 11 \pmod{12}$. Sabemos também que $(\frac{3}{q}) = 1$ se $q \equiv 1 \text{ ou } 11 \pmod{12}$ e $(\frac{3}{q}) = -1$ se $q \equiv 5 \text{ ou } 7 \pmod{12}$. Assim, $(\frac{-3}{q}) = 1 \iff q \equiv 1 \text{ou } 7 \pmod{12}$ que implica $q \equiv 1 \pmod 3$ e q da forma $3k+1$. Novamente, temos um novo primo da forma $3k+1$ gerando uma contradição e podemos concluir que existem infinitos primos da forma $3k+1$.
Outra forma, de provar que existem infinitos primos da forma $3k+1$ é tomar os divisores primos de números $N = (3x+1)^2 - (3x+1) + 1 = 9x^2 + 3x + 1$. Seja q um fator primo de N. Temos $q \neq 2$ e $q \neq 3$, pois N não é divisível por 2 nem 3. Veja que $q \mid (3x+1)^3 - 1$ e $q \nmid (3x+1) - 1 = 3x$ implicando $\text{ord}_q\, 3x+1 = 3 \mid q-1 \Rightarrow q = 3k+1$. Os números N só possuem fatores $3k+1$. Mas poderiam ser sempre os mesmos primos. Para resolver isso considere que temos t primos $3k+1$ a saber $q_1, q_2, \ldots, q_t$. Tome $x = q_1q_2 \ldots q_t$ e para q_i temos $q_i \mid N-1$ e $q_i \nmid N \Rightarrow q \neq q_i$ para todo i. Conseguimos gerar infinitos primos $3k+1$.

Problema 1.49. *(OI) Demonstre que se* $\text{mdc}(a,b) = 1$ *o número $a^2 + b^2$ não pode ter fatores primos da forma $4k-1$ e se além disso* $\text{mdc}(a,3) = 1$ *então o número $a^2 + 3b^2$ não*

pode ter fatores ímpares da forma $3k-1$. Que podemos dizer sobre os fatores primos de a^2+pb^2 onde p é um primo?

Solução

Seja p um divisor primo de a^2+b^2. Veja que se $p \mid a$ então $p \mid a^2 \Rightarrow p \mid b^2 \Rightarrow p \mid b \Rightarrow p \mid \text{mdc}(a,b) = 1$ que é falso. Então $p \nmid a$ e $p \nmid b$. Veja que existe b' tal que $b \cdot b' = 1$ e $a^2 \equiv -b^2 \pmod{p} \iff (ab')^2 \equiv -1 \pmod{p}$. Se $p \equiv -1 \pmod 4$ temos $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = -1$ e a última congruência não teria solução. Concluímos que a^2+b^2 com $\text{mdc}(a,b) = 1$ não possui fatores $4k-1$. Inclusive, esse fato gera uma forma de provar que existem infinitos primos da forma $4k+1$. Basta supor que existe uma quantidade finita $p_1, \ldots, p_t$ e toma $N = (2p_1 \ldots p_t)^2 + 1$ que não é divisível por algum p_i e por ser soma de quadrados não fatores $4k-1$.
Como fizemos anteriormente $p \nmid a$, $p \nmid b$ e $a^2 \equiv -3b^2 \pmod{p} \iff (ab')^2 \equiv -3 \pmod{p}$. Os fatores primos ímpares da forma $3k-1$ são os primos $6t+5$. Temos dois casos.

1. Se $p = 12k+5$ então $(\frac{-3}{p}) = (\frac{-1}{p}) \cdot (\frac{3}{p}) = 1 \cdot (-1) = -1$, pois $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$ e $(\frac{3}{p}) = 1 \iff p \equiv \pm 1 \pmod{12}$.
2. Se $p = 12k+11$ então $(\frac{-3}{p}) = (\frac{-1}{p}) \cdot (\frac{3}{p}) = (-1) \cdot 1 = -1$. A justificativa é análoga à do caso anterior.

Então a última congruência não teria solução e a^2+3b^2 não possui fatores $6k+5$.
Seja q um fator primo de a^2+pb^2. Se $q \mid a$ então $q \mid b$ e $q \mid \text{mdc}(a,b) = 1$. Então q não divide a nem b. Usando o inverso de b módulo q temos $a^2 \equiv -pb^2 \pmod{q} \iff (ab')^2 \equiv -p \pmod{q}$ e só existe solução para essa última congruência quando $(\frac{-q}{p}) = 1$.

Problema 1.50. *(T) Demonstre que, para $p = 1093$,*

$$2^{\frac{p-1}{2}} \equiv -1 \pmod{p^2}$$

Solução

Esta solução foi retirada de [26].
Temos

$$2^{10} \equiv 1024 \equiv p - 69 \pmod{p^2}$$

$$\Rightarrow 2^{14} \equiv 16p - 1104 \equiv 15p - 11 \equiv -1078p - 11 \equiv -11(1+98p) \pmod{p^2}$$

Como $11^3 = 1331 = p + 238$ temos

$$11^4 \equiv 11p + 2618 \equiv 13p + 432 \equiv 432 - 1080p \equiv 2^3 \cdot 3^3(2-5p) \pmod{p^2}$$

Veja também que

$$3^7 \equiv 2187 \equiv 2p+1 \pmod{p^2}$$

Por Binômio de Newton, para quaisquer a e b inteiros, temos

$$(a+bp)^n \equiv \binom{n}{1} a^{n-1}bp + a^n \equiv na^{n-1}bp + a^n \pmod{p^2}$$

Juntando todos esses fatos obtemos

$$2^{392} \equiv (2^{14})^{28} \equiv 11^{28}(1+98p)^{28} \equiv \left(2^3 \cdot 3^3 \cdot (2-5p)\right)^7 (1+2744p) \pmod{p^2}$$

$$\Rightarrow 2^{392} \equiv 2^{21} \cdot 3^{21} \cdot (2^7 - 2^6 \cdot 5 \cdot 7 \cdot p)(1+558p) \pmod{p^2}$$

$$\Rightarrow 2^{392} \equiv 2^{27} \cdot (2p+1)^3 \cdot (2-35p)(1+558p) \pmod{p^2}$$

$$\Rightarrow 2^{392} \equiv 2^{27}(1+6p)(2-12p) \equiv 2^{28} \pmod{p^2}$$

Assim, $2^{1092} \equiv 2^{3(392-28)} \equiv 1 \pmod{p^2}$. Dessa forma, $2^{\frac{p-1}{2}} = 2^{546}$ é congruente a 1 ou a -1 módulo $p^2 = 1093^2$. Porém, $p \equiv -3 \pmod 8$ e, pela proposição 1.43. juntamente como o lema 1.47., $2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \equiv -1 \pmod p$.
Concluímos que para $p = 1093$ temos $2^{\frac{p-1}{2}} \equiv -1 \pmod{p^2}$.

Problema 1.51 (IMO1996). *(OA) Sejam a, b inteiros positivos tais que $15a+16b$ e $16a-15b$ sejam quadrados perfeitos não nulos. Encontre o menor valor que pode tomar o menor destes quadrados.*

Solução

Considere $15a+16b = x^2$ e $16a-15b = y^2$ com x e y inteiros positivos. Temos $15x^2 + 16y^2 = 481a^2$. Fatorando 481 em primos temos $481 = 13 \cdot 37$.
Vejamos módulo 13. Se $13 \nmid x$ então $13 \nmid y$ e podemos escrever

$$15x^2 \equiv -16y^2 \pmod{13} \iff 2x^2 \equiv -3y^2 \pmod{13} \iff (2xy^{-1})^2 \equiv -6 \pmod{13}$$

Mas veja que $\left(\frac{-6}{13}\right) = \left(\frac{-1}{13}\right) \cdot \left(\frac{2}{13}\right) \cdot \left(\frac{3}{13}\right) = 1 \cdot (-1) \cdot 1 = -1$, pois $13 \equiv 1 \pmod 4$, $13 \equiv 5 \pmod 8$ e $13 \equiv 1 \pmod{12}$. Portanto, é necessário que $13 \mid x$ e $13 \mid y$.
De maneira similar, módulo 37 se $37 \nmid x$ então $37 \nmid y$ e

$$15x^2 \equiv -16y^2 \pmod{37} \iff (15xy^{-1})^2 \equiv -15 \cdot 16 \equiv 19 \pmod{37}$$

Mas veja que $(\frac{19}{37})$ pode ser calculado de $(\frac{37}{19}) = (\frac{-1}{19}) = -1$, pois $19 \equiv 3 \pmod 4$, e da Lei da Reciprocidade Quadrática

$$\left(\frac{19}{37}\right) \cdot \left(\frac{37}{19}\right) = (-1)^{\frac{19-1}{2}\frac{37-1}{2}} = 1 \Rightarrow \left(\frac{19}{37}\right) = -1$$

Com isso a congruência anterior não tem solução e podemos concluir que $37 \mid x$ e $37 \mid y$. Temos que $841 \mid x$ e $841 \mid y$ implicando que eles são pelo menos 481. De fato, tomando $(a, b) = (31 \cdot 481, 481)$ obtemos $x = y = 481$. Então o menor valor do menor desses quadrados é $481^2 = 231361$.

Problema 1.52. *(T) Seja p um número primo ímpar. Mostre que o menor não resto quadrático positivo de p é menor que $\sqrt{p}+1$.*

Solução

Seja a o menor resíduo não quadrático módulo p. Considere o menor inteiro positivo b tal que $a \cdot b \geq p$. Como p é primo e $a > 1$, pois 1 é sempre resíduo quadrático, podemos concluir que $a \cdot b > p$. Temos $a \cdot b = p + r$ com $r < a$, pois $r \geq a$ implicaria que $p \leq p + r - a = a(b-1)$ e b não seria mínimo. Temos $ab \equiv r \pmod p$ e $(\frac{r}{p}) = (\frac{ab}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p})$. Como a é um resíduo não quadrático $(\frac{a}{p}) = -1$. Se $(\frac{b}{p}) = 1$ então $(\frac{r}{p}) = -1$ e temos uma contradição por a ser mínimo. Se $(\frac{b}{p}) = -1$ então b também é um resíduo não quadrático. Isso implica $b \geq a$ e por b ser mínimo temos $p > a(b-1) > (a-1)^2 \Rightarrow \sqrt{p}+1 > a$.

Problema 1.53. *(T) Sejam M um número inteiro e p um número primo maior do que 25. Mostre que a sequência $M, M+1, \cdots, M+3\lfloor\sqrt{p}\rfloor - 1$ contém um resto não quadrático módulo p.*

Solução

Esta solução foi retirada de [34].

Dado um inteiro Q, com $1 < Q < p$. Definimos

$$S_x = \sum_{z=0}^{Q-1} \left(\frac{x+z}{p}\right)$$

e

$$S = \sum_{x=0}^{p-1} S_x^2$$

Note que podemos reagrupar as parcelas de S como

$$S = \sum_{x=0}^{p-1} \sum_{z_1=0}^{Q-1} \sum_{z=0}^{Q-1} \left(\frac{(x+z_1)(x+z)}{p}\right)$$

Para $z = z_1$ e cada x não congruente a $-z$ temos parcela 1 e para $x \equiv -z \pmod{p}$ temos 0. São Q valores para $z = z_1$ e $p-1$ valores de x. A soma dessas parcelas é $(p-1)Q$.
Já para $z \neq z_1$ temos que $\sum_{a=0}^{p-1} (\frac{a(a+c)}{p}) = -1$ com $a = x + z_1$ e $c = z - z_1$ módulo p. São Q valores para z_1 e $Q-1$ diferentes para z implicando $(-1)Q(Q-1)$. E chegamos em $S = (p-1)Q - Q(Q-1) = (p-Q)Q$.
Faremos $\lfloor \sqrt{p} \rfloor = Q$ para usar o resultado provado. Note que $Q \leq \sqrt{p} < Q+1 \Rightarrow p < (Q+1)^2$.
Supondo que não há resíduos não quadráticos em M, $M+1$, ... $M+3Q-1$. Nesse caso $|S_x| \geq Q-1$ para $x = M, M+1, \ldots, M+2Q-1$ e como S_x^2 é sempre maior que ou igual a 0 temos

$$2Q(Q-1)^2 \leq (p-Q)Q \Rightarrow 2(Q-1)^2 < (Q+1)^2 - Q \Rightarrow Q^2 - 5Q < 0 \Rightarrow 0 < Q < 5$$

Porém, para $p > 25$ temos $\sqrt{p} > 5$ e $Q = \lfloor \sqrt{p} \rfloor \geq 5$

Problema 1.54 (Putnam 1991). *(OA) Seja p um primo ímpar. Quantos elementos tem o conjunto*

$$\{x^2 \mid x \in \mathbb{Z}/p\mathbb{Z}\} \cap \{y^2 + 1 \mid y \in \mathbb{Z}/p\mathbb{Z}\}?$$

Solução

Nos elementos na interseção $x^2 \equiv y^2 + 1 \pmod{p} \iff (x+y)(x-y) \equiv 1 \pmod{p}$. Mas isso é equivalente a $x-y$ ser o inverso de $x+y$ módulo p. Qualquer resíduo não nulo possui inverso módulo p. Por outro lado, para qualquer k com $1 \leq k \leq p-1$ podemos tomar $x + y = k$ e $x - y = k^{-1}$. Existem $p-1$ pares de soluções (x, y) da forma $(\frac{k+k^{-1}}{2}, \frac{k-k^{-1}}{2})$ para $k = 1, 2, \ldots, p-1$.
Porém, o que queremos contar é $h \equiv x^2 \equiv y^2 + 1 \pmod{p}$ e alguns pares (x, y) geram o mesmo h. Sabemos que $z^2 \equiv s \pmod{p}$ tem duas soluções quando s é resíduo quadrático, zero soluções quando s não é resíduo e uma solução quando s é 0. Desta forma, em geral há 4 pares de soluções $(\pm x_0, \pm y_0)$ correspondem ao mesmo h. A exceção que sempre acontece tem duas soluções é $(\pm 1, 0)$ correspondendo a $h = 1$. Se -1 é resíduo quadrático temos mais uma exceção $(0, \pm y_0)$ que corresponde a $h = 0$. Se -1 não é resíduo quadrático então só tem a exceção em $h = 1$.
Logo, se $p \equiv 1 \pmod{4}$ temos $(\frac{-1}{p}) = 1$ e, considerando as duas exceções, são $\frac{p-1-4}{4} + 2 = \frac{p+3}{4}$ elementos h na interseção. Se $p \equiv 3 \pmod{4}$ temos $(\frac{-1}{p}) = -1$ e, considerando apenas uma exceção, são $\frac{p-1-2}{4} + 1 = \frac{p+1}{4}$ soluções. Uma resposta que junta os dois casos é $\lfloor \frac{p}{4} \rfloor + 1$.

Problema 1.55 (IMO2008). *(OA) Prove que existe um número infinito de inteiros positivos n tais que n^2+1 tem um divisor primo maior do que $2n+\sqrt{2n}$.*

Solução

Uma ideia muito interessante para resolver esse problema é considerar os primos ao invés dos números n no enunciado. Tome um dos infinitos primos p da forma $4k+1$ para algum inteiro k. Sabemos que $(\frac{-1}{p}) = 1 \Rightarrow$ existe x tal que $x^2 \equiv -1 \pmod{p}$. Sabemos que todos os resíduos módulo p aparecem em $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$, então existe x com $1 \leq x \leq \frac{p-1}{2}$ tal que $p \mid x^2+1$. Seja $x = \frac{p-t}{2}$. Temos $p \mid x^2+1 = \frac{p^2-2pt+t^2+4}{4} \iff p \mid t^2+4$. Mas isso implica $t^2+4 > p \iff t > \sqrt{p-4}$. Veja que $x \leq \frac{p-1}{2} \iff 2x \leq p-1$. Lembrando que $2x$ é par, os maiores valores possíveis são $p-1$ e $p-3$. Mas $2x = p-1 \Rightarrow 4x^2+4 = (p-1)^2+4 = p^2-2p+5$ que só é múltiplo de p para $p = 5$ e $2x = p-3 \iff 4x^2+4 = (p-3)^2+4 = p^2-6p+13$ que só múltiplo de p para $p = 13$. Tomando $p > 13$ temos $2x < p-4$ e $\sqrt{2x} < \sqrt{p-4} < t$.
Dessa forma, x^2+1 possui um divisor primo p tal que $x = \frac{p-t}{2} \iff 2x = p-t \iff p = 2x+t > 2x+\sqrt{2x}$. Tomando infinitos p da forma $4k+1$ com $p > 13$ teremos infinitos x tal que x^2+1 tem um divisor primo maior que $2x+\sqrt{2x}$.

8

FUNÇÕES MULTIPLICATIVAS E AS FÓRMULAS DE INVERSÃO DE MÖBIUS

Problema 2.1. *(A) Calcule* $\varphi(1001)$ *e* $\sigma(1001)$.

Solução

Fatorando o número em potências de primos $1001 = 7 \cdot 11 \cdot 13$. Podemos usar a fórmula para φ.

$$\varphi(1001) = 1001\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{13}\right) = 6 \cdot 10 \cdot 12 = 720$$

Para σ podemos usar o fato de ser multiplicativa e que $\sigma(T) = p+1$.

$$\sigma(1001) = (7+1)(11+1)(13+1) = 1344$$

Problema 2.2. *(A) Determine o número de divisores de* 2008*,* 2009*,* 2010 *e* 2011.

Solução

Basta considerar as fatorações dos números n e a fórmula para $d(n)$.

$$d(2008) = d(2^3 \cdot 251) = (3+1)(1+1) = 8$$

$$d(2009) = d(7^2 \cdot 41) = (2+1)(1+1) = 6$$

$$d(2010) = d(2 \cdot 3 \cdot 5 \cdot 67) = (1+1)(1+1)(1+1)(1+1) = 16$$

$$d(2011) = d(2011) = (1+1) = 2$$

Problema 2.3. *(A) Determine as soluções de* $\sigma(n) = 2801$.

Solução

Como σ é uma função multiplicativa, se n tiver dois ou mais fatores primos distintos

então $\sigma(n)$ é composto. Como 2801 é primo podemos concluir que n tem que ser potência de primo. Seja $n = p^k$. Temos $2801 = \sigma(p^k) \iff 2801 = \frac{p^{k+1}-1}{p-1} \iff 2801p - 2801 = p^{k+1} - 1 \iff p(2801 - p^k) = 2800$. Então p tem que ser um fator primo de 2800. São 3 casos

(i) Se $p = 2$ então $2801 - 2^k = 1400 \iff 1401 = 2^k$ que não tem solução.

(ii) Se $p = 5$ então $2801 - 5^k = 560 \iff 2241 = 5^k$ que não tem solução.

(iii) Se $p = 7$ então $2801 - 7^k = 400 \iff 2401 = 7^k \iff k = 4$ e temos a solução $n = 7^4$.

Concluímos que a única solução da equação $\sigma(n) = 2801$ é $n = 7^4 = 2401$.

Problema 2.4. *(A) Mostre que as funções σ_m são multiplicativas para todo $m \neq 0$. Observe que para todo $n > 1$ se tem que $\lim_{m\to 0} \sigma_m(n) = d(n)$.*

Solução

Sabemos que $f(n) = n^m$ é multiplicativa (e até totalmente multiplicativa) e isso é suficiente para que σ_m é multiplicativa.

Com mais detalhes considere a e b inteiros tais que $\text{mdc}(a, b) = 1$ então os fatores primos de ab estão em a ou em b, mas não nos dois. Cada divisor d do produto ab pode ser separado em d_1 e d_2 sendo os fatores primos de a e os de b, respectivamente. Temos

$$\begin{aligned}\sigma_m(ab) &= \sum_{d|ab} d^m = \sum_{d_1|a, d_2|b} (d_1 d_2)^m = \sum_{d_1|a, d_2|b} d_1^m d_2^m \\ &= \sum_{d_1|a} \sum_{d_2|b} d_1^m d_2^m = \sum_{d_1|a} d_1^m \sum_{d_2|b} d_2^m \\ &= \sigma_m(a)\sigma_m(b).\end{aligned}$$

E concluímos que σ_m é multiplicativa.

Com isso, temos a fórmula para σ_m.

$$\sigma_m(n) = \sum_{d|n} d^m = \frac{p_1^{(k_1+1)m} - 1}{p_1^m - 1} \cdot \frac{p_2^{(k_2+1)m} - 1}{p_2^m - 1} \cdots \frac{p_s^{(k_s+1)m} - 1}{p_s^m - 1}.$$

Cada fração pode ser fatorada usando $p_i^{(k_i+1)m} - 1 = \left(p_i^m\right)^{k_i+1}$

$$\frac{p_i^{(k_i+1)m} - 1}{p_i^m - 1} = p_i^{mk_i} + p_i^{m(k_i-1)} + \cdots + p_i^{2m} + p_i^m + 1$$

Quando $m \to 0$ temos $p_i^m \to 1$ e $\frac{p_i^{(k_i+1)m}-1}{p_i^m-1} \to 1+1+\cdots+1+1 = k_i+1$. Com isso, $\lim_{m\to 0} \sigma_m(n) = (k_1+1)(k_2+1)\ldots(k_s+1) = d(n)$.

Problema 2.5. *(OI) Determine as soluções do sistema* $\begin{cases} \sigma(n) = 8784 \\ d(n) = 12. \end{cases}$

Solução

Fatorando os números em primo $8784 = 2^4 \cdot 3^2 \cdot 61$ e $12 = 2^2 \cdot 3$. A partir de $d(n)$ os possíveis formatos de n são p^{11}, pq^5, p^2q^3 ou pqr^2.

(i) Se $\sigma(p^{11}) = 8784$ então $1+p+\cdots+p^{11} = 8784 \iff p(1+p+\cdots+p^{10}) = 8783$ e essa última equação não tem solução, pois 8783 é primo.

(ii) Se $\sigma(pq^5) = 8784$ então $(1+p)(1+q+\cdots+q^5) = 8784$. Veja que $1+p \geq 3$ e $1+q+\cdots+q^5 \leq \frac{8784}{3} \Rightarrow 1+q+\cdots+q^5 \leq 2928$. Se $q \geq 5$ então $1+q+\cdots+q^5 > 5^5 = 3125$ e não temos solução. Resta testar $q \leq 3$. Se $q = 2$ então $1+p = \frac{8784}{63}$ que não é inteiro. Se $q = 3$ então $1+p = \frac{8784}{364}$ que não também não é inteiro. Então nesse caso não temos solução.

(iii) Se $\sigma(p^2q^3) = 8784$ então $(1+p+p^2)(1+q+q^2+q^3) = 8784$. Veja que $1+p+p^2 \geq 1+2+4 = 7$ e $1+q+q^2+q^3 \leq \frac{8784}{7} < 1255$. Se $q \geq 11$ então $q^3 = 1331 > 1255$. Resta testar $q \leq 7$. Veja que para $q = 2, 3, 5$ ou 7 temos $1+q+q^2+q^3 = 15, 40, 156$ ou 400. Mas nenhum deles divide 8784. Logo, não temos soluções.

(iv) Se $\sigma(pqr^2) = 8784$ então $(1+p)(1+q)(1+r+r^2) = 8784$. Novamente, podemos limitar $(1+p)(1+q) \geq 3 \cdot 4 = 12$ e $1+r+r^2 \leq \frac{8784}{12} = 732$. Como essa cota ainda está muito alta para testar, podemos usar mais informações. Por exemplo, 8784 possui um fator 61. Se esse fator aparece em $1+p$ ou $1+q$ então $1+r+r^2 \mid \frac{8784}{61} = 144 \Rightarrow r < 12$. Podemos testar $r = 2, 3, 5, 7$ ou 11 e obter $1+r+r^2 = 7, 13, 31, 57$ ou 132, mas nenhum deles divide 8784. Logo $61 \mid 1+r+r^2$. Então $1+r+r^2 = 61k \leq 732 = 61 \cdot 12$ implicando $k \leq 12$. Veja também que $1+r+r^2 = 1+r(r+1)$ é ímpar então só precisamos testar k ímpar $1+r+r^2 = 61, 61 \cdot 3, 61 \cdot 5, 61 \cdot 7, 61 \cdot 9$ ou $61 \cdot 11$. Não precisamos fazer conta dos que possuem fatores 5, 7 ou 11, pois eles não aparecem no 8784. Resta, testar $r(1+r) = 60, 182$ ou 548. A única possibilidade é $r(1+r) = 182 \Leftrightarrow r = 13$. Fica faltando completar $(1+p)(1+q) = \frac{8784}{1+13+13^2} = 48$. Suponha sem perda $p < q$ e temos $(1+p)^2 < (1+p)(1+q) = 48 < 7^2 \Rightarrow p < 6$. Se $p = 5$ temos $q = 7$ e chegamos na solução $n = 5 \cdot 7 \cdot 13^2 = 5915$. Se $p = 3$ temos $q = 11$ e temos a solução $n = 3 \cdot 11 \cdot 13^2 = 5577$. Se $p = 2$ temos $1+q = \frac{48}{3} = 16 \Leftrightarrow q = 15$ que não é

primo.

Portanto, as únicas soluções são 5915 e 5577.

Problema 2.6. *(A) Seja f uma função multiplicativa tal que para todo número primo p,*

$$f(p^k) = \begin{cases} 1 & \text{se } k = 2^s \text{ para algum } s \in \mathbb{N} \\ 0 & \text{caso contrário.} \end{cases}$$

Mostre que f é uma função tal que $f(n^2) = f(n)^2$ para todo $n \in \mathbb{N}$, mas não é totalmente multiplicativa.

Solução

Para $n = 1$ temos $f(1) = 1$ que satisfaz as condições. Para $n \geq 2$ seja $n = p_1^{k_1} \dots p_s^{k_s}$ a fatoração de n em potências de primos. Como f é multiplicativa $f(n) = f(p_1^{k_1}) \dots f(p_s^{k_s})$. Veja que $f(n) = 1$ se todos os expoentes são potência de 2 e $f(n) = 0$ caso contrário. A fatoração de n^2 é $p_1^{2k_1} \dots p_s^{2k_s}$ e sabemso que k_i é potência de 2 se, e somente se, $2k_i$ é potência de 2. Então $f(n) = 1 \iff f(n^2) = 1$. Dessa forma, se $f(n) = 1$ temos $f(n^2) = 1 = 1^2 = f(n)^2$ e se $f(n) = 0$ temos $f(n^2) = 0 = 0^2 = f(n)^2$.
A função não é totalmente multiplicativa, pois $0 = f(3^2 \cdot 3^4) \neq f(3^2)f(3^4) = 1 \cdot 1 = 1$.

Problema 2.7. *(A) Construa um exemplo de uma função multiplicativa f, que não seja totalmente multiplicativa, tal que $f(n^k) = f(n)^k$ para todo $k \leq 10$ e todo $n \in \mathbb{N}$. Generalize o resultado anterior para $k \leq N$ (em lugar de $k \leq 10$), com N inteiro fixo.*

Solução

Considere a função f definida por $f(n) = 1$, se $n = 1$, se na fatoração em primos todos os expoentes são 1 ou são números que só possuem fatores primos menores que 11 e $f(n) = 0$ para os demais casos, ou seja, se n tem algum expoente de primo na fatoração tem fator primo maior que ou igual a 11.
Por exemplo, $f(2^{13}) = 0$, pois o expoente tem fator 13 maior que 11, e $f(2^{20} \cdot 3^{15} \cdot 5) = 1$, pois 20, 15 e 1 não possuem algum fator primo maior ou igual a 11.
A função f é multiplicativa, pois se a e b são primos entre si, então os conjuntos de fatores primos deles são disjuntos. Temos $f(ab) = 1$ se, e somente se, ab não tem expoentes com fatores primos maiores ou iguais a 11 que é equivalente a a e b não terem expoentes com fatores primos maiores ou iguais a 11 sendo, portanto, $f(a) = f(b) = 1$.
Fica provado também que $f(a) = 0$ ou $f(b) = 0$ é equivalente a $f(ab) = 0$, pois o expoente de primo com fator primo maior que 10 que aparece em a ou em b aparece em ab.

Para $n = 1$ é claro que $f(1^k) = f(1)^k = 1$. Para $n > 1$ seja $n = p_1^{k_1} \dots p_s^{k_s}$ a fatoração de n em potências de primos. Veja que $n^k = p_1^{kk_1} \dots p_s^{kk_s}$. O número k não possui fatores primos maiores que 11 e kk_i não possui fatores primos maiores ou iguais a 11 se, e somente se, k_i não possui fatores primos maiores ou iguais a 11.
Essa função não é totalmente multiplicativa, pois $0 = f(3^{11}) \neq f(3^10)f(3^1) = 1 \cdot 1 = 1$.
Para generalizar, basta considerar a função g dada por $g(n) = 1$, se $n = 1$ ou se na fatoração em primos todos os expoentes são 1 ou números que só possuem fatores primos menores ou iguais a N e $g(n) = 0$ caso contrário, ou seja, se n tem algum expoente de primo na fatoração tem fator primo maior que N.
Os passos da demonstração de que g é multiplicativa, que $g(n^k) = g(n)^k$ para $k \leq N$ e que g não é totalmente multiplicativa são análogos.

Problema 2.8. *(T) Mostrar que existe um inteiro positivo n_0 tal que, para todo inteiro $n \geq n_0$, temos que*

$$n \geq \frac{d(n)^2}{4} + \varphi(n),$$

e vale a igualdade para um inteiro $n \geq n_0$ se e somente se n é primo.

Solução

Vamos fazer em dois casos.
Se n é potência de um primo. Podemos escrever que $n = p^k$, $d(n) = k+1$ e $\varphi(n) = p^k - p^{k-1}$. Daí,

$$n \geq \frac{d(n)^2}{4} + \varphi(n) \iff p^{k-1} \geq \frac{(k+1)^2}{4}$$

Se $k = 1$, ou seja, para n primo, temos a igualdade. Se $k = 2$ a expressão é equivalente $p \geq \frac{9}{4}$ que é verdade para $p \geq 3$. Se $k \geq 3$ temos $p^{k-1} \geq 2^{k-1} \geq \frac{(k+1)^2}{4}$. Essa última inequação é equivalente a $2^{k+1} \geq (k+1)^2$ que por indução é verdade para $k+1 \geq 4$ e ocorre igualdade apenas em $k+1 = 4$. Então para potências de $p \geq 3$ temos a inequação e para $p = 2^k$ temos inequação para $k \geq 4$. Então para $n \geq n_0$ grande a inequação é verdadeira.

Se n possui dois ou mais fatores primos. Podemos escrever $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, $d(n) = (k_1+1)(k_2+1)\dots(k_s+1)$ e $\varphi(n) = n(1-\frac{1}{p_1})\dots(1-\frac{1}{p_s})$.

$$n > \frac{d(n)^2}{4} + \varphi(n) \iff 1 > \frac{1}{4}\frac{(k_1+1)^2}{p_1^{k_1}} \dots \frac{(k_s+1)^2}{p_s^{k_s}} + (1-\frac{1}{p_1})\dots(1-\frac{1}{p_s})$$

Para $p_i \geq 3$ temos $\frac{(k_i+1)^2}{p_i^{k_i}} \leq \frac{4}{p_i}$ e para $p_i = 2$ temos $\frac{(k_i+1)^2}{4 \cdot p_i^{k_i}} \leq \frac{4}{p_i}$. Com isso,

$$\frac{1}{4}\frac{(k_1+1)^2}{p_1^{k_1}} \dots \frac{(k_s+1)^2}{p_s^{k_s}} \leq \frac{4^s}{p_1 p_2 \dots p_s}$$

E para concluir basta provar que

$$\frac{4^s}{p_1 p_2 \dots p_s} + (1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_s}) = \frac{4^s + (p_1 - 1)(p_2 - 1) \dots (p_s - 1)}{p_1 p_2 \dots p_s} < 1$$

Note que

$$(p_1 - 1)(p_2 - 1) \dots (p_s - 1) = (p_1 - 1)(p_2 - 1) \dots (p_{s-1} - 1)p_s - (p_1 - 1)(p_2 - 1) \dots (p_{s-1} - 1)$$

$$< p_1 p_2 \dots p_s - (p_1 - 1)(p_2 - 1) \dots (p_{s-1} - 1)$$

Então é suficiente provar que

$$(p_1 - 1)(p_2 - 1) \dots (p_{s-1} - 1) > 4^s$$

Note que separamos um p_s qualquer e podemos usá-lo como o menor dos primos. Então se entre os primos p_i existir um primo muito grande, $p_i > 4^s + 1$, essa desigualdade é verdadeira.

Note também que podemos reescrever a inequação como $\frac{(p_1-1)}{4} \frac{(p_2-1)}{4} \dots \frac{(p_{s-1}-1)}{4} > 4$ e a desigualdade é verdadeira para $s > s_0$, pois $\frac{p_x-1}{4} \geq \frac{7}{4} > 1$ a partir de certo x e o lado esquerdo cresce com o s.

Resta analisar o caso em que a quantidade de primos é limitada $s \leq s_0$ e os primos utilizados são limitados $p_i \leq 4^s + 1 \leq 4^{s_0} + 1$. Se tomarmos $n \geq n_0$ suficientemente grande, teremos alguma das potências de primo suficientemente grande $p_i^{k_i} \geq n_0^{\frac{1}{s_0}}$. Para $k_i = 1$ podemos fazer com que p_i seja maior que $4^{s_0} + 1$ com a escolha de n_0. Se $k_i \geq 2$ podemos fazer com que $\frac{(k_i+1)^2}{p_i^{k_i-1}} < 4\epsilon$ com a escolha do n_0. Isso nos levaria a

$$\frac{1}{4} \frac{(k_1 + 1)^2}{p_1^{k_1}} \dots \frac{(k_s + 1)^2}{p_s^{k_s}} \leq \frac{4^s \epsilon}{p_1 p_2 \dots p_s}$$

E, repetindo os passos anteriores, bastaria provar que

$$(p_1 - 1)(p_2 - 1) \dots (p_{s-1} - 1) > 4^s \epsilon$$

Fazendo $\epsilon < \frac{1}{4^{s_0}}$ temos $4^s \epsilon < 4^{s_0} \frac{1}{4^{s_0}} = 1 \leq (p_1 - 1)(p_2 - 1) \dots (p_{s-1} - 1)$. Então para $s \geq 2$ e n_0 grande o suficiente $n \geq n_0$ implica que n possui muitos fatores primos, n

possui um fator primo muito grande ou n possui uma potência de primo muito grande em sua fatoração. E em cada um desses casos vale a inequação.

Dessa forma, para n_0 suficientemente grande se $n \geq n_0$ vale a inequação $n \geq \frac{d(n)^2}{4} + \varphi(n)$ com igualdade se, e somente se, n é primo.

Problema 2.9. *(A) Quantos números com* 35 *divisores existem, tais que todos seus fatores primos sejam menores que* 20 *? Qual é o maior e o menor de tais números?*

Solução

Existem 8 fatores primos menores que 20: 2, 3, 5, 7, 11, 13, 17 e 19. Um número com 35 divisores pode ser da forma p^{34} ou p^4q^6. No primeiro caso são 8 formas de escolher p e no segundo caso são 8 formas de escolher p e 7 formas de escolher q. Portanto, são $8 + 8 \cdot 7 = 64$ números.
O menor número é $2^6 \cdot 3^4$. Veja que se tivermos um fator primo $p^{34} \geq 2^{34} > 2^{14} = 2^6 \cdot 4^4 > 2^6 \cdot 3^4$ e se tivermos dois fatores primos $p^6 \cdot q^4 \geq 2^4 \cdot 3^6 > 2^6 \cdot 3^4$. O maior é 19^{34}, pois é o maior entre os números com um fator primo e $19^{34} > 19^6 \cdot 19^4 > 19^6 \cdot 17^4$ que é o maior número com dois fatores primos.

Problema 2.10. *(A) Seja n um número composto. Mostre que* $2^n - 1$ *também é composto.*

Solução

Se n é composto, então $n = ab$ com $1 < a \leq b < n$. Daí $2^{ab} - 1 = (2^a)^b - 1^b = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$ e $2^n - 1$ possui um divisor $2^a - 1$ com $1 < 2^2 - 1 \leq 2^a - 1 < 2^n - 1$ e é composto.

Problema 2.11. *(A) Mostre que um número n tem um número ímpar de divisores se, e somente se, n é um quadrado perfeito.*

Solução

Considere a fatoração de n em primos $n = p_1^{k_1} \ldots p_s^{k_s}$. A quantidade de divisores é dada por $d(n) = (k_1 + 1) \ldots (k_s + 1)$. Observe que $d(n)$ é ímpar se, e somente se, os $k_i + 1$ são todos primos que equivale a todos os k_i serem pares e n ser um quadrado perfeito.

Problema 2.12. *(OI) Determine a menor solução da equação* $2d(n^2) = 17d(n)$.

Solução

Observe que $n = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$ satisfaz a equação, pois $d(n) = (8+1)(4+1)(2+1)(1+1) = 9 \cdot 5 \cdot 3 \cdot 2$ e $d(n^2) = (2 \cdot 8 + 1)(2 \cdot 4 + 1)(2 \cdot 2 + 1)(2 \cdot 1 + 1) = 17 \cdot 9 \cdot 5 \cdot 3$. Assim, $\frac{d(n^2)}{d(n)} = \frac{17}{2}$.

Provaremos que essa é a menor solução.
Veja que se os expoentes de n na fatoração em primos são k_i, então a equação é equivalente a

$$2(2k_1+1)(2k_2+1)\dots(2k_s+1) = 17(k_1+1)(k_2+1)\dots(k_s+1)$$

Vale ressaltar que para minimizar o número colocamos o maior expoente no 2, o segundo maior no 3 e assim por diante. Se não usarmos essa ordem qualquer número gerado será maior que o número gerado dessa forma.
O fator 17 aparece em $d(n)^2$ e podemos supor sem perda de generalidade $17 \mid 2k_1+1$. O segundo menor valor ímpar possível é $2k_1+1 = 3\cdot 17 = 51$. Mas nesse caso já teríamos $n \geq 2^{25} > 2^8\cdot 2^8\cdot 2^5\cdot 2^3 > 2^8\cdot 3^4\cdot 5^2\cdot 7$ e todas as soluções, se existirem, seriam maiores que nossa menor solução. Se $2k_1+1 = 17 \iff k_1 = 8$. A equação passa a ser

$$2(2k_2+1)\dots(2k_s+1) = 9(k_2+1)\dots(k_s+1)$$

Se $9 \mid 2k_i+1$, então podemos sem perda que $i = 2$. Se $2k_2+1 > 9$ então $2k_2+1 \geq 27 \iff k_2 \geq 13$ e teríamos $n \geq 2^{13}\cdot 3^8 = 2^8\cdot 2^5\cdot 3^4\cdot 3^4 > 2^8\cdot 3^4\cdot 5^2\cdot 7$ e seriam soluções maiores que nossa menor. Se $2k_2+1 = 9 \iff \iff k_2+1 = 5$ e devemos resolver

$$2(2k_3+1)\dots(2k_s+1) = 5(k_3+1)\dots(k_s+1)$$

Suponha se perda de genralidade que $5 \mid 2k_3+1$ então $2k_3+1 = 5 \iff k_3 = 2$ ou $2k_3+1 \geq 15 \iff k_3 \geq 7$. Nessa segunda possibilidade, já teríamos um número pelo menos $2^8\cdot 3^7\cdot 5^4$ que é maior que nossa cota para o menor. Se $2k_3+1 = 5$ então ficaríamos com

$$2(2k_4+1)\dots(2k_s+1) = 3(k_4+1)\dots(k_s+1)$$

Temos pelo menos mais um fator primo e obtemos um número que é pelo menos nossa cota de menor solução. De fato, nossa solução aparece se $k_4 = 1$, $s = 4$ e usar os expoentes em ordem decrescente nos primos em ordem crescente.

Resta fazer o caso em $9 \nmid 2k_i+1$. Então dois números devem contribuir com fatores 3. Porém, se $2k_1+1 = 3 \iff k_1+1 = 2$ e $2k_2+1 = 3 \iff k_2+1 = 2$ então o lado direito possui dois ou mais fatores 2 e do outro lado haveria apenas um 2 que geraria contradição. Se um desses números é maior que 3, então, lembrando que é ímpar e não múltiplo de 9, o menor seria 15. Veja que $2k_i+1 = 15 \iff k_i = 7 \iff k_i+1 = 8$ teria 3 fatores 2 enquanto o outro lado da equação só teria 1 gerando contradição. O seguinte seria $2k_i+1 \geq 21 \iff k_i \geq 10$ e o número seria no mínimo $2^10\cdot 3^8\cdot 5^1$ que é

maior que nossa cota, pois $2^2 \cdot 3^4 > 5 \cdot 7$.

Portanto, a menor solução $n = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 = 3628800$.

Problema 2.13. *(OI) Encontre infinitos valores de n para os quais $d(n)$ é um divisor de n.*

Solução

Vamos tentar soluções potências de primo $n = p^k$. Demos $d(n) \mid n \iff k+1 \mid p^k$. Podemos tomar $k = p - 1$. Então $n = p^{p-1}$ para todo primo p nos dá uma solução de $d(n) = p \mid n = p^{p-1}$.

Problema 2.14. *(A) Denotemos por $f(n)$ a soma dos divisores de n que são quadrados perfeitos. Mostre que f é uma função multiplicativa, e determine uma fórmula fechada para esta função.*

Solução

Considere a função $q : \mathbb{Z}_+^* \to \mathbb{Z}_+^*$ dada por

$$q(n) = \begin{cases} n & \text{se } n \text{ é um quadrado perfeito} \\ 0 & \text{caso contrário.} \end{cases}$$

Essa função $q(n)$ é multiplicativa, pois $\text{mdc}(a, b) = 1$ temos ab é quadrado perfeito se, e somente se, a e b são quadrados perfeitos já que eles não compartilham fatores prioms. Isso nos leva a $q(ab) = ab = q(a)q(b)$ se ambos são quadrados perfeitos e $q(ab) = 0 = q(a)q(b)$ se algum deles não é quadrado.
Com isso, $f(n) = \sum_{d|n} q(d)$ é multiplicativa também.
Para calcular a fórmula basta calcular $f(p^k)$ para p primo, pois $n = p_1^{k_1} \dots p_s^{k_s} \Rightarrow f(n) = f(p_1^{k_1}) \dots f(p_s^{k_s})$. Se o expoente em p^k for par então $k = 2m$ e $f(p^k) = 1 + p^2 + \cdots + p^{2m} = \frac{p^{2m+2}}{p^2-1} = \frac{p^{2\left\lfloor \frac{k}{2} \right\rfloor + 2}}{p^2-1}$ e se for ímpar $k = 2m+1$ e $f(p^k) = 1 + p^2 + \cdots + p^{2m} = \frac{p^{2m+2}-1}{p^2-1} == \frac{p^{2\left\lfloor \frac{k}{2} \right\rfloor + 2}}{p^2-1}$.
Dessa forma, a fórmula para $n = p_1^{k_1} \dots p_s^{k_s}$ é

$$f(n) = \frac{p_1^{2\left\lfloor \frac{k_1}{2} \right\rfloor + 2}}{p_1^2 - 1} \cdots \frac{p_s^{2\left\lfloor \frac{k_s}{2} \right\rfloor + 2}}{p_s^2 - 1}$$

Problema 2.15. *(A) Determine todas as soluções de $\varphi(n) = 24$.*

Solução

Veja que se $n = 2 \cdot n_0$ com n_0 ímpar, então $\varphi(n) = \varphi(2) \cdot \varphi(n_0) = \varphi(n_0)$. Então podemos considerar que n não tem fator 2 ou tem 2 ou mais fatores 2. Se n possui 4 ou mais

fatores primos distintos, então $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ então $\varphi(n) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \dots \varphi(p_s^{k_s})$ e cada um dos $s \geq 4$ fatores tem um fator 2 implicando $2^4 \mid \varphi(n) \Rightarrow \varphi(n)$ não pode ser 24 que só tem 3 fatores 2.

Agora resta fazer os três casos $s = 1, 2$ ou 3.

Veja também que para cada primo $p \mid n$ temos $p - 1 \mid \varphi(p^k)$ e $\varphi(p^k) \mid 24$ implicando $p - 1 \mid 24$ e $p = 2, 3, 5, 7$ ou 13. Note que 5, 7 e 13 não são divisores de 24, então se são divisores de n possuem expoente 1 na fatoração.

Se n é potência de primo. Então $n = p^k$ e $\varphi(n) = p^k - p^{k-1} = 24$. Se $k = 1$, então $p = 25$ que não é primo. Se $k \geq 2$, então $p^{k-1}(p-1) = 24 \Rightarrow p \mid 24 \Rightarrow p = 2$ ou $p = 3$. Para $p = 2$ teríamos $2^{k-1} = 24$ que não tem solução e para $p = 3$ teríamos $3^{k-1} = 12$ que também não tem solução.

Se n possui dois fatores primos. Então $n = p^k q^t$, $\varphi(n) = p^{k-1}q^{t-1}(p-1)(q-1) = 24$ e podemos supor sem perda que $p < q$. Se $q = 13$ então $p^{k-1}(p-1)12 = 24 \iff p^{k-1}(p-1) = 2$. Isso implica $p - 1 \mid 2$ e $p = 2$ ou 3. Nos dá as soluções $n = 3 \cdot 13 = 39$ e $n = 2^2 \cdot 13 = 52$. Lembre-se que para os n ímpares podemos tomar também $2n$ com o mesmo φ e nesse caso temos também a solução $n = 2 \cdot 3 \cdot 13 = 78$. Se $q = 7$ então $p^{k-1}(p-1)6 = 24 \iff p^{k-1}(p-1) = 4$. Isso implica $p - 1 \mid 4$ e $p = 2, 3$ ou 5. Testando, encontramos soluções $n = 2^3 \cdot 7 = 56$, $n = 5 \cdot 7 = 35$ e $n = 2 \cdot 5 \cdot 7 = 70$. Se $q = 5$ então $p^{k-1}(p-1)4 = 24 \iff p^{k-1}(p-1) = 6$. Como $p < q = 5$ só temos $p = 2$ ou 3. As soluções desse caso são $n = 3^2 \cdot 5 = 45$ e $n = 2 \cdot 3^2 \cdot 5 = 90$. Resta apenas o caso $q = 3$ e $p = 2$. O único fator 3 do 24 só pode vir de $\varphi(3^t)$ então $t = 2$ e temos $\varphi(2^k) = 4 \iff k = 3$ o que nos dá a solução $n = 2^3 \cdot 3^2 = 72$.

Se n possui três fatores primos. Então $n = p^k q^t r^l$, $\varphi(n) = p^{k-1}q^{t-1}r^{l-1}(p-1)(q-1)(r-1) = 24$ e podemos supor sem perda que $p < q < r$. Repetindo o processo do último caso. Se $r = 13$ então $p^{k-1}q^{t-1}(p-1)(q-1)12 = 24 \iff p^{k-1}q^{t-1}(p-1)(q-1) = 2$, mas cada um desses φ é par e não pode ser 2. Se $r = 7$ então $p^{k-1}q^{t-1}(p-1)(q-1)6 = 24 \iff p^{k-1}q^{t-1}(p-1)(q-1) = 4$. A única solução é se cada φ for 2 que ocorre com $p^k = 2^2$ e $q^t = 3$. Assim, $n = 2^2 \cdot 3 \cdot 7 = 84$. Se $r = 5$ então $p = 2$ e $q = 3$ e devemos resolver $2^{k-1}3^{t-1}(2-1)(3-1)4 = 24 \iff 2^{k-1}3^{t-1} = 3$ que não é possível já que para o expoente do 2 o expoente deve ser maior que 1. Portanto, as soluções de $\varphi(n) = 24$ são 35, 39, 45, 52, 56, 70, 72, 78, 84 e 90.

Problema 2.16. *(T) Denotemos por n# o produto de todos os primos menores ou iguais a n. Mostre que $\varphi(n\#)$ divide $n!$ e usando este resultado mostre que a equação $\varphi(x) = n!$ sempre possui solução $x \in \mathbb{N}$.*

Solução

Se $n\# = p_1 p_2 \dots p_k$ então $\varphi(n\#) = (p_1 - 1)(p_2 - 1)\dots(p_k - 1)$ que é o produto de k números distintos dois a dois menores que n. Como $n!$ é o produto de todos os números menores que ou iguais a n então esses k números aparecem nesse produto e temos $\varphi(n\#) \mid n!$. Além disso, o número inteiro $m = \frac{n!}{\varphi(n\#)}$ só possui fatores primos menores que ou iguais a n. Para cada primo que aparece na fatoração de m com expoente k deve ser usado com expoente $k+1$ para montar o número M. Assim, $\varphi(M)$ é o produto de $\varphi(p^{k+1}) = p^k(p-1)$. Montando a equação

$$\varphi(M) = m\varphi(n\#) = n!$$

Problema 2.17. *(T) Determine todos os valores de $k \in \mathbb{N}$ tais que $n = k\varphi(n)$ possui solução.*

Solução

Para $n = 1$ temos $1 = k\varphi(1) \iff k = 1$. Para $n = 2$ temos $2 = k\varphi(2) \iff k = 2$. Para $n > 2$ temos $\varphi(n)$ é par, pois tem dois ou mais fatores 2 ou um fator primo ímpar p tal que $p - 1$ é par. Então, $\varphi(n) \mid n \Rightarrow 2 \mid n$. Suponha que $n = 2^{a_1} \cdot p_2^{a_2} \dots p_s^{a_s}$. Se $s \geq 3$ então $\varphi(p_2^{a_2})$ e $\varphi(p_3^{a_3})$ possuem fatores 2 e $2^{a_1 - 1} \mid \varphi(2^{a_1})$. Nesse caso, $\varphi(n) = \varphi(2^{a_1})\varphi(p_2^{a_2})\varphi(p_3^{a_3})\dots$ é múltiplo de 2^{a_1+1} e não poderia dividir n. Se $s = 1$ então $n = 2^{a_1}$ e temos $2^{a_1} = k \cdot 2^{a_1 - 1} \iff k = 2$. Se $s = 2$ então $n = 2^{a_1} \cdot p_2^{a_2}$ e temos $2^{a_1} \cdot p_2^{a_2} = k \cdot 2^{a_1 - 1} \cdot p_2^{a_2 - 1}(p_2 - 1) \iff 2p_2 = k(p_2 - 1)$. Veja que $p_2 - 1 \mid 2p_2$ e $\text{mdc}(p_2 - 1, p_2) = 1$ implicando $p_2 - 1 \mid 2 \Rightarrow p_2 = 3$, pois $p_2 > 2$. Dessa forma, $2 \cdot 3 = k \cdot (3 - 1) \iff k = 3$.

Concluímos que $\varphi(n) \mid n \iff n = 2^a \cdot 3^b$, com $a \geq 1$ e $b \geq 0$, ou $n = 1$. E que os únicos inteiros k tais que $n = k\varphi(n)$ são 2 e 3.

Problema 2.18. *(A) Mostre que para todo n existe um k tal que $\varphi(x) = kn$ possui solução.*

Solução

Já provamos que $\varphi(M) = n!$ possui solução. Então tomando $k = (n-1)!$ sempre podemos encontrar x tal que $\varphi(x) = (n-1)! \cdot n = n!$.

Problema 2.19. *(A) Determinar todas as soluções da equação $\varphi(n) = 2d(n)$.*

Solução

Veja que para $p \geq 5$ temos $\varphi(p^k) = p^{k-1}(p-1) \geq 5^{k-1} \cdot 4 \geq 2(k+1) = 2d(p^k)$. Com igualdade se, e somente se, $p = 5$ e $k = 1$. A demonstração é por indução. Para $k = 1$ temos $5^0(5-1) \geq 2(1+1)$. Para $k = 2$ temos $5 \cdot 4 > 2(2+1)$. O passo indutivo é

$$5^{k+1-1}(5-1) = 5^k(5-1) = 5 \cdot 5^{k-1}(5-1) > 5 \cdot 2(k+1) = 2(5k+5) > 2(2k+3)$$

Com isso, $n = 5$ é solução e não temos outras soluções em que n só possui fatores primos maiores que 3.

Veja que para as potências de 2 temos $\frac{\varphi(2^1)}{1+1} = \frac{1}{2}$, $\frac{\varphi(2^2)}{2+1} = \frac{2}{3}$, $\frac{\varphi(2^3)}{3+1} = 1$, $\frac{\varphi(2^4)}{4+1} = \frac{8}{5}$ e para $t \geq 5$ temos $\frac{\varphi(2^t)}{t+1} > 2$. A demonstração dessa última desigualdade é análoga à outra anterior.

Para as potências de 3 temos $\frac{\varphi(3^1)}{1+1} = 1$, $\frac{\varphi(3^2)}{2+1} = 2$ e para $t \geq 3$ temos $\frac{\varphi(3^t)}{t+1} \geq \frac{9 \cdot 2}{4} > 4$.

Se $2 \nmid n$. Então n ímpar. Se n é potência de 3, então temos a solução $n = 3^2 = 9$. Se n for potência de 3 multiplicada por potências de primos maiores o resultado a razão $\frac{\varphi(n)}{d(n)}$ será no mínimo $1 \cdot 2 = 2$. Essa igualdade ocorre se, e somente se, a potência de 3 for 3^1 e os demais primos forem apenas 5^1. Isso nos dá a solução $n = 3^1 \cdot 5^1 = 15$.

Se n tem um fator 2. Então $n = 2n_0$ com n_0 ímpar e $\frac{\varphi(2n_0)}{d(2n_0)} = \frac{1}{2}\frac{\varphi(n_0)}{d(n_0)}$. Então precisamos resolver a equação $\frac{\varphi(n_0)}{d(n_0)} = 4$ para n_0 ímpar. Não há soluções para n_0 potência de 3. Se usarmos potência de 3 teria que ser 3^1 ou 3^2. Se for 3^1 então $n_0 = 3^1 \cdot n_1$ e a equação passa a ser $\frac{\varphi(n_1)}{d(n_1)} = 4$. Se n_1 tem 2 ou mais fatores primos distintos $\frac{\varphi(n_1)}{d(n_1)} > 2 \cdot 2 = 4$. Se n_1 for uma potência de primo com expoente maior que ou igual a 2 então $\frac{\varphi(n_1)}{d(n_1)} \geq \frac{5^1(5-1)}{3} > 4$. Podemos testar 5^1 e 7^1 que não funcionam. A partir de 11 já temos razão maior que $\frac{10}{2} = 5$. Se for 3^2 então $n_0 = 3^2 \cdot n_1$ e a equação passa a ser $\frac{\varphi(n_1)}{d(n_1)} = 2$ e a única solução é $n_1 = 5^1$. Logo, a única solução desse caso é $n = 2^1 \cdot 3^2 \cdot 5^1 = 90$.

Se n tem dois fatores 2. Então $n = 4n_0$ com n_0 ímpar e $\frac{\varphi(4n_0)}{d(4n_0)} = \frac{2}{3}\frac{\varphi(n_0)}{d(n_0)}$. Precisamos resolver $\frac{\varphi(n_0)}{d(n_0)} = 3$ para n_0 ímpar. Não há solução com n_0 potência de 3. Se usarmos 3^2 ou maior com outras potências o produto será pelo menos 4. Se usarmos 3^1 ou não usarmos potência de 3 precisamos resolver $\frac{\varphi(n_1)}{d(n_1)} = 3$. Testando 5^1 e 7^1 obtemos as soluções $n = 2^2 \cdot 7^1 = 28$ e $n = 2^2 \cdot 3^1 \cdot 7^1 = 84$. Para $n_1 > 7^1$ temos $\frac{\varphi(n_1)}{d(n_1)} > 3$ e não temos outras soluções.

Se n possui três fatores 2. Então $n = 8n_0$ com n_0 ímpar e $\frac{\varphi(8n_0)}{d(8n_0)} = \frac{\varphi(n_0)}{d(n_0)}$. Temos que resolver $\frac{\varphi(n_0)}{d(n_0)} = 2$. Se n_0 tem dois fatores 3 temos a solução $n = 2^3 \cdot 3^2 = 72$. Se n_0 tem mais que dois fatores 2 então $\frac{\varphi(n_0)}{d(n_0)} > 2$. Se n_0 possui 0 ou 1 fator 3 precisamos resolver $\frac{\varphi(n_1)}{d(n_1)} = 2$ com n_1 possuindo fatores primos maiores que 5. A única solução é $n_1 = 5$. Portanto, temos soluções $n = 2^3 \cdot 5 = 40$ e $n = 2^3 \cdot 3^1 \cdot 5 = 120$.

Se n possui quatro fatores 2. Então $n = 16n_0$ com n_0 ímpar e $\frac{\varphi(16n_0)}{d(16n_0)} > 2\frac{\varphi(n_0)}{d(n_0)} > 2$. Não temos solução nesse caso.

Se n possui cinco ou mais fatores 2, então $n = 2^t n_0$ com n_0 ímpar e $\frac{\varphi(2^t n_0)}{d(2^t n_0)} > 2\frac{\varphi(n_0)}{d(n_0)} \geq 2$. Não temos mais soluções.

Portanto, as soluções são 5, 9, 15, 28, 40, 72, 84, 90 e 120.

Problema 2.20. *(A) Determinar todos os números inteiros positivos n tais que $n = d(n)^2$.*

Solução

Sabemos que $n = 1$ é solução. Buscaremos as soluções com $n > 1$. Veja que n é um quadrado perfeito e sua fatoração em primos só tem expoentes pares. Podemos escrever $n = p_1^{2k_1} \dots p_s^{2k_s}$. A equação $n = d(n)^2$ é equivalente a

$$p_1^{2k_1} \dots p_s^{2k_s} = (2k_1+1)^2 \dots (2k_s+1)^2 \iff p_1^{k_1} \dots p_s^{k_s} = (2k_1+1) \dots (2k_s+1)$$

Como o produdo de ímpares é ímpar e só tem fatores primos ímpares temos $p_i \geq 3$. Notemos que $3^k \geq 2k+1$ com igualdade se, e somente se, $k = 1$. A demonstração é por indução. Para $k = 1$ temos $3^1 = 2 \cdot 1 + 1$ e para $k = 2$ temos $3^2 = 9 > 2 \cdot 2 + 1 = 5$. O passo indutivo para $m \geq 2$.

$$3^{m+1} = 3 \cdot 3^m > 3(2m+1) = 6m + 3 > 2m + 3$$

Para p primo $p > 3$ temos $p^k > 3^k \geq 2k+1$ para todo k inteiro positivo. Logo, $p_1^{k_1} \dots p_s^{k_s} \geq (2k_1+1) \dots (2k_s+1)$ com igualdade se, e somente se, o produto só tem um fator primo que é 3 com expoente 1.
A única solução de $n = d(n)^2$ é $n = 3^2 = 9$.

Problema 2.21. *(A) Dois números a e b são* amigos *se $\sigma(a) - a = b$ e $\sigma(b) - b = a$. Por exemplo* 1184 *e* 1210 *são amigos (verificar!). Encontrar outra dupla de números amigos.*

Solução

Fatorando em primos $1184 = 2^5 \cdot 37$ e $1210 = 2 \cdot 5 \cdot 11^2$. Calculando as somas dos divisores $\sigma(1184) = \frac{2^6-1}{2-1}\frac{37^2-1}{37-1} = 2394$ e $\sigma(1210) = \frac{2^2-1}{2-1}\frac{5^2-1}{5-1}\frac{11^3-1}{11-1} = 2394$ e de fato vale $\sigma(1184) - 1184 = 1210$ e $\sigma(1210) - 1210 = 1184$.

Outra dupla de números amigos é $220 = 2^2 \cdot 5 \cdot 11$ e $284 = 2^2 \cdot 71$. Para verificar essa propriedade, temos $\sigma(220) = \frac{2^3-1}{2-1}\frac{5^2-1}{5-1}\frac{11^2-1}{11-1} = 504$ e $\sigma(284) = \frac{2^3-1}{2-1}\frac{71^2-1}{71-1} = 504$. Assim, $\sigma(220) - 220 = 284$ e $\sigma(284) - 284 = 284$.

Problema 2.22. *(T) Determine todas as soluções de* $\varphi(\varphi(n)) = 2^{13}3^25^4$.

Solução

Primeiro provaremos que $\sqrt{\frac{n}{2}} \leq \varphi(n) < n$. A última desigualdade é imediata da definição de $\varphi(n)$. Para a primeira considere

$$\frac{\varphi(n)^2}{n} = \prod_{p_i|n} \frac{(p_i^{k_i-1}(p_i-1))^2}{p_i^{k_i}} = \prod_{p_i|n} p_i^{k_i-2}(p_i-1)^2 \geq \prod_{p_i|n} \frac{(p_i-1)^2}{p_i}$$

Note que para $p_i = 2$ a fração é $\frac{1}{2}$ e para $p_i \geq 3$ implica $(p_i-1)^2 - p_i = p_i(p_i-3)+1 \geq 0$. Logo

$$\frac{\varphi(n)^2}{n} \geq \frac{1}{2} \iff \varphi(n) \geq \sqrt{\frac{n}{2}}$$

Com isso, para qualquer inteiro positivo N temos $\varphi(x) = N \Rightarrow \sqrt{\frac{x}{2}} \leq N \leq x$ que é equivalente a $N \leq x \leq 2N^2$. E aplicando novamente $\varphi(\varphi(x)) = M$ implica $M \leq \varphi(x) \leq 2M^2$ e usando as estimativas feitas $M \leq \varphi(x) \leq x \Rightarrow M \leq x$ e $\frac{x}{2} \leq \varphi(x) \leq 2M^2 \Rightarrow x \leq 8M^4$. Logo, $\varphi(\varphi(x)) = M \Rightarrow M \leq x \leq 8M^4$ e o número de soluções da equação é finita para todo M inteiro positivo.

Veja que podemos encontrar uma solução da forma $n = 2^a \cdot 3^b \cdot 5^c$ com $a, b, c \geq 2$. Nesse caso $\varphi(\varphi(n)) = \varphi(2^{a-1} \cdot 3^{b-1} \cdot 2 \cdot 5^{c-1} \cdot 4) = \varphi(2^{a+2} \cdot 3^{b-1} \cdot 5^{c-1}) = 2^{a+1} \cdot 3^{b-2} \cdot 2 \cdot 5^{c-2} \cdot 4 = 2^{a+4} \cdot 3^{b-2} \cdot 5^{c-2}$. Pelas igualdades $a+4 = 13 \iff a = 9$, $b-2 = 2 \iff b = 4$ e $c-2 = 4 \iff c = 6$. Temos assim a solução $n = 2^9 \cdot 3^4 \cdot 5^6$.

Determinar mesmo todas as soluções é impraticável mesmo com o auxílio de um computador razoável, pois apesar de finitas são muitas soluções já que podemos usar vários fatores primos em n completando com alguns fatores 2, 3 e 5. Por exemplo, se $n = 2^a \cdot 3^b \cdot 5^c \cdot 2017$ com $a, b, c \geq 1$ temos

$$\varphi(n) = \varphi(2^a \cdot 3^b \cdot 5^c \cdot 2017) = 2^{a-1} \cdot 3^{b-1} \cdot 2 \cdot 5^{c-1} \cdot 4 \cdot 2016 = 2^{a+7} \cdot 3^{b+1} \cdot 5^{c-1} \cdot 7$$

E aplicando a função mais uma vez

$$\varphi(\varphi(n)) = \varphi(2^{a+7} \cdot 3^{b+1} \cdot 5^{c-1} \cdot 7) = 2^{a+6} \cdot 3^b \cdot 2 \cdot 5^{c-2} \cdot 4 \cdot 6 = 2^{a+10} \cdot 3^{b+1} \cdot 5^{c-2}$$

Usando $a = 3$, $b = 1$ e $c = 6$ temos a solução $n = 2^3 \cdot 3^1 \cdot 5^6 \cdot 2017^1$.

Problema 2.23. *(A) Mostre que para todo m e n inteiros vale a identidade*

$$\varphi(mn) \cdot \varphi(\text{mdc}(m,n)) = \text{mdc}(m,n) \cdot \varphi(n) \cdot \varphi(m).$$

Solução

Veja que dividindo por mn e manipulando os fatores temos:

$$\frac{\varphi(mn)}{mn} = \frac{\frac{\varphi(m)}{m}\frac{\varphi(n)}{n}}{\frac{\varphi(\text{mdc}(m,n))}{\text{mdc}(m,n)}}$$

Observe que para todo a inteiro positivo temos $\frac{\varphi(a)}{a} = \prod_{p|a}\left(1-\frac{1}{p}\right)$ em que esse produtório percorre os primos que dividem a. Temos:

$$\frac{\varphi(mn)}{mn} = \prod_{p|mn}\left(1-\frac{1}{p}\right) = \frac{\prod_{p|m}\left(1-\frac{1}{p}\right)\prod_{p|n}\left(1-\frac{1}{p}\right)}{\prod_{p|m,p|n}\left(1-\frac{1}{p}\right)} = \frac{\frac{\varphi(m)}{m}\frac{\varphi(n)}{n}}{\frac{\varphi(\text{mdc}(m,n))}{\text{mdc}(m,n)}}$$

Vale ressaltar que $p \mid m$ e $p \mid n \iff p \mid \text{mdc}(m,n)$.

Problema 2.24. *(T) Mostre que 945 é o menor número abundante ímpar.*

Solução

Note que $\sigma(n) > 2n \iff \frac{\sigma(n)}{n} > 2$. A função $\frac{\sigma(n)}{n}$ é multiplicativa e para $n = p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$ temos

$$\frac{\sigma(n)}{n} = \frac{\sigma(p_1^{k_1})}{p_1^{k_1}}\cdots\frac{\sigma(p_s^{k_s})}{p_s^{k_s}} = \frac{p_1^{k_1+1}-1}{p_1^{k_1+1}-p_1^{k_1}}\cdots\frac{p_s^{k_s+1}-1}{p_s^{k_s+1}-p_s^{k_s}}$$

Observe que para $n = 945$ temos fatoração $945 = 3^3\cdot 5\cdot 7$ e $\frac{\sigma(n)}{n} = \frac{3^4-1}{3^4-3^3}\frac{5^2-1}{5^2-5}\frac{7^2-1}{7^2-7} = \frac{40}{27}\cdot\frac{6}{5}\cdot\frac{8}{7} = \frac{1920}{945} > 2$. Portanto, 945 é de fato abundante.

Se um n ímpar tem 4 ou mais fatores primos, então o valor mínimo é $3\cdot 5\cdot 7\cdot 11 = 1155 > 945$ e já é maior que nossa cota. Veja que podemos cotar superiormente $\frac{p_i^{k_i+1}-1}{p_i^{k_i+1}-p_i^{k_i}} < \frac{p_i^{k_i+1}}{p_i^{k_i+1}-p_i^{k_i}} = \frac{p_i}{p_i-1}$ e

$$\frac{\sigma(n)}{n} < \frac{p_1}{p_1-1}\frac{p_2}{p_2-1}\cdots\frac{p_s}{p_s-1}$$

É importante ressaltar que $\frac{n}{n-1} = 1+\frac{1}{n-1}$ é decrescente em n.

Para $s \le 2$ temos $\frac{\sigma(n)}{n} < \frac{3}{2}\cdot\frac{5}{4} = \frac{15}{8} < 2$. Resta estudar $s = 3$.

Suponha que n ímpar tem 3 fatores primos. Se n não possui fator 3 então $\frac{\sigma(n)}{n} \le$

$\frac{5}{4}\cdot\frac{7}{6}\cdot\frac{11}{10}=\frac{385}{240}<2$ e não pode ser abundante. Se n não possui fator 5 então $\frac{\sigma(n)}{n}\leq\frac{3}{2}\cdot\frac{7}{6}\cdot\frac{11}{10}=\frac{231}{120}<2$ e não pode ser abundante. Se além dos primos 2 e 3 o terceiro primo p for maior que ou igual a 17, então $\frac{\sigma(n)}{n}\leq\frac{3}{2}\cdot\frac{5}{4}=\frac{17}{16}=\frac{255}{128}<2$. Resta analisar os números ímpares menores que 945 com exatamente três divisores primos que podem ser $\{3,5,7\}$, $\{3,5,11\}$ ou $\{3,5,13\}$.

(i) Se os três primos são $\{3,5,7\}$. O número n é da forma $3\cdot5\cdot7\cdot k=105k$ para k ímpar.
Se $k=1$, então $n=105$ e $\frac{\sigma(n)}{n}=\frac{3^2-1}{3^2-3}\frac{5^2-1}{5^2-5}\frac{7^2-1}{7^2-7}=\frac{8}{6}\frac{24}{20}\frac{48}{42}=\frac{4}{3}\frac{6}{5}\frac{8}{7}=\frac{192}{105}<2$.
Se $k=3$, então $n=315$ e $\frac{\sigma(n)}{n}=\frac{3^3-1}{3^3-3^2}\frac{5^2-1}{5^2-5}\frac{7^2-1}{7^2-7}=\frac{26}{18}\frac{24}{20}\frac{48}{42}=\frac{13}{9}\frac{6}{5}\frac{8}{7}=\frac{624}{315}<2$.
Se $k=5$, então $n=525$ e $\frac{\sigma(n)}{n}=\frac{3^2-1}{3^2-3}\frac{5^3-1}{5^3-5^2}\frac{7^2-1}{7^2-7}=\frac{8}{6}\frac{124}{100}\frac{48}{42}=\frac{4}{3}\frac{31}{25}\frac{8}{7}=\frac{992}{525}<2$.
Se $k=7$, então $n=735$ e $\frac{\sigma(n)}{n}=\frac{3^2-1}{3^2-3}\frac{5^2-1}{5^2-5}\frac{7^3-1}{7^3-7^2}=\frac{8}{6}\frac{24}{20}\frac{342}{294}=\frac{4}{3}\frac{6}{5}\frac{57}{49}=\frac{1368}{735}<2$.
Para $k\geq9$ já chegamos em 945 e a partir dele obtemos resultados cada vez maiores.

(ii) Se os três primos são $\{3,5,11\}$. O número n é da forma $3\cdot5\cdot11\cdot k=165k$ para k ímpar.
Se $k=1$, então $n=165$ e $\frac{\sigma(n)}{n}=\frac{3^2-1}{3^2-3}\frac{5^2-1}{5^2-5}\frac{11^2-1}{11^2-11}=\frac{8}{6}\frac{24}{20}\frac{120}{110}=\frac{4}{3}\frac{6}{5}\frac{12}{11}=\frac{288}{165}<2$.

Se $k=3$, então $n=495$ e $\frac{\sigma(n)}{n}=\frac{3^3-1}{3^3-3^2}\frac{5^2-1}{5^2-5}\frac{11^2-1}{11^2-11}=\frac{26}{18}\frac{24}{20}\frac{120}{110}=\frac{13}{9}\frac{6}{5}\frac{12}{11}=\frac{936}{495}<2$.

Se $k=5$, então $n=825$ e $\frac{\sigma(n)}{n}=\frac{3^2-1}{3^2-3}\frac{5^3-1}{5^3-5^2}\frac{11^2-1}{11^2-11}=\frac{8}{6}\frac{124}{100}\frac{120}{110}=\frac{4}{3}\frac{31}{25}\frac{12}{11}=\frac{1488}{825}<2$.
Se $k\geq7$, então $n>945$ e não precisamos testar se é abundante.

(iii) Se os três primos são $\{3,5,13\}$. O número n é da forma $3\cdot5\cdot13\cdot k=195k$ para k ímpar.

Se $k=1$, então $n=195$ e $\frac{\sigma(n)}{n}=\frac{3^2-1}{3^2-3}\frac{5^2-1}{5^2-5}\frac{13^2-1}{13^2-13}=\frac{8}{6}\frac{24}{20}\frac{14}{13}=\frac{4}{3}\frac{6}{5}\frac{14}{13}=\frac{336}{195}<2$.

Se $k=3$, então $n=585$ e $\frac{\sigma(n)}{n}=\frac{3^3-1}{3^3-3^2}\frac{5^2-1}{5^2-5}\frac{13^2-1}{13^2-13}=\frac{26}{18}\frac{24}{20}\frac{14}{13}=\frac{13}{9}\frac{6}{5}\frac{14}{13}=\frac{84}{45}<2$.

Se $k\geq5$, então $n\geq975>945$ e não precisamos testar se é abundante.

Portanto, o menor número ímpar abundante é 945.

Problema 2.25. *(A) Mostre que todo múltiplo de um número abundante é abundante.*

Solução

Sabemos que um número é abundante quando $\sigma(n) > 2n$. Podemos escrever $\sigma(n)$ como soma de $\frac{n}{d_i}$ sobre os divisores de n. Assim, $2n < \sigma(n) = \sum_{d|n} \frac{n}{d} \iff 2 < \sum_{d|n} \frac{1}{d}$. Se m é múltiplo de n abundante então todos os divisores de n são divisores de m e temos

$$\sum_{d|m} \frac{1}{d} \geq \sum_{d|n} \frac{1}{d} > 2.$$

Problema 2.26. *(T) Determine qual é o número mínimo de divisores primos que um número deve ter se ele é*

- *abundante ou perfeito,*
- *não divisível por* 2*, nem por* 3*.*

Solução

Como fizemos no problema 2.24, podemos considerar a função multiplicativa $\frac{\sigma(n)}{n}$ e a cota superior

$$\frac{\sigma(n)}{n} < \frac{p_1}{p_1 - 1} \frac{p_2}{p_2 - 1} \cdots \frac{p_s}{p_s - 1}$$

Ressaltamos que $\frac{n}{n-1} = 1 + \frac{1}{n-1}$ é decrescente em n.
Queremos que $\frac{\sigma(n)}{n} \geq 2$ para que o número seja abundante ou perfeito. Se $s \leq 14$ então

$$\frac{\sigma(n)}{n} \leq \frac{7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59}{6 \cdot 10 \cdot 12 \cdot 16 \cdot 18 \cdot 22 \cdot 28 \cdot 30 \cdot 36 \cdot 40 \cdot 42 \cdot 46 \cdot 52 \cdot 58} < 2$$

E um número com 14 ou menos fatores primos diferentes de 2 e de 3 não pode ser abundante ou perfeito. Para $s = 15$ temos para os menores primos

$$\frac{7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61}{6 \cdot 10 \cdot 12 \cdot 16 \cdot 18 \cdot 22 \cdot 28 \cdot 30 \cdot 36 \cdot 40 \cdot 42 \cdot 46 \cdot 52 \cdot 58 \cdot 60} > 2$$

Essas contas foram feitas com auxílio de computador.

Veja que na fórmula de $\frac{\sigma(n)}{n}$ se jogarmos k_i para infinito

$$\frac{\sigma(n)}{n} = \frac{\sigma(p_1^{k_1})}{p_1^{k_1}} \cdots \frac{\sigma(p_s^{k_s})}{p_s^{k_s}} = \frac{p_1^{k_1+1} - 1}{p_1^{k_1+1} - p_1^{k_1}} \cdots \frac{p_s^{k_s+1} - 1}{p_s^{k_s+1} - p_s^{k_s}} \to \frac{p_1}{p_1 - 1} \frac{p_2}{p_2 - 1} \cdots \frac{p_s}{p_s - 1}$$

E, de fato, existem números abundantes não divisíveis por 2 nem por 3 com 15 fatores primos.

Problema 2.27. *(T) Seja $f : \mathbb{N}^+ \to \mathbb{R}^+$ uma função multiplicativa e crescente.*

(a) Prove que, para todo inteiro $M > 1$ e todo inteiro positivo n,

$$f(M^{n+1} - 1) \geq f(M^n - 1)f(M) \text{ e } f(M^{n+1} + 1) \leq f(M^n + 1)f(M).$$

Conclua que

$$\lim_{n\to\infty} \sqrt[n]{f(M^n)} = f(M).$$

(b) Utilize o item anterior para M potência de primo para concluir que $f(p^k) = f(T)^k$ para todo primo p.

(c) Conclua que f é totalmente multiplicativa, e portanto existe $\alpha > 0$ tal que $f(n) = n^\alpha$ para todo inteiro positivo n.

Solução

(a) Veja que $\text{mdc}(M^n - 1, M) = \text{mdc}(M^n + 1, M) = 1$ e podemos fazer

$$f(M^n - 1)f(M) = f(M^{n+1} - M) < f(M^{n+1} - 1) < f(M^{n+1})$$

e

$$f(M^{n+1}) < f(M^{n+1} + 1) < f(M^{n+1} + M) = f(M^n + 1)f(M)$$

Usando esse fato $n - 1$ vez em $f(M^n)$ e tirando a raiz n-ésima obtemos

$$f(M) \cdot \sqrt[n]{\frac{f(M-1)}{f(M)}} < \sqrt[n]{f(M^n)} < f(M) \cdot \sqrt[n]{\frac{f(M+1)}{f(M)}}$$

Fazendo o limite quando $n \to \infty$ $\sqrt[n]{\frac{f(M-1)}{f(M)}} \to 0$ e $\sqrt[n]{\frac{f(M+1)}{f(M)}} \to 0$ e concluímos que

$$\lim_{n\to\infty} \sqrt[n]{f(M^n)} = f(M).$$

(b) Usaremos um lema auxiliar.
Lema: Se $L = \inf_{p\nmid x} \frac{f(x+p)}{f(x)}$ então $L = 1$.
Demonstração: Pela definição de L para qualquer x tal que $p \nmid x$ temos $f(x + p) \geq Lf(x)$ e aplicando k vezes $f(x + kp) \geq L^k f(x)$ para todo $k \geq 0$. Veja que sempre podemos encontrar $x > kp$ tal que $2 \nmid x$ e $p \nmid x$. Para esse valor temos

$$f(2)f(x) = f(2x) \geq f(x + kp) \geq L^k f(x)$$

Isso implica que $L^k \leq f(2)$ para todo k e $L \leq 1$. Veja que $\frac{f(x+p)}{f(x)} \geq 1$ para todo x implicando $L \geq 1$. Concluímos que $L = 1$. Em outras palavras sempre podemos tomar x de modo que $\frac{f(x+p)}{f(x)}$ seja tão próximo de 1 quanto se queira.

Seja p um primo e x um inteiro não divisível por p. Vamos definir a sequência $y_n = f(p^n)$. Pelo que vimos no item anterior do fato de $px-1$, x e $px+1$ serem primos com p temos

$$(px-1)p^n < xp^{n+1} < (px+1)p^n \Rightarrow f(px-1)y_n \leq f(x)y_{n+1} \leq f(px+1)y_n$$

Assim,

$$\frac{y_{n+1}}{y_n} \leq \inf \frac{f(px+1)}{f(x)} \leq \inf \frac{f(px+p)}{f(x)} \leq f(T) \inf \frac{f(x+p)}{f(x)} = f(T) \cdot L = f(T)$$

Por outro lado, podemos provar também que

$$\frac{y_{n+1}}{y_n} \geq f(T)U$$

Onde

$$U = \sup \frac{f(x-p)}{f(x)} = \sup \frac{f(x)}{f(x+p)} = \frac{1}{L} = 1$$

Portanto, $\frac{y_{n+1}}{y_n} = f(T)$ para cada n e podemos concluir que $f(p^n) = f(T)^n$.

(c) Assim, para $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ temos $f(n) = f(p_1)^{k_1} f(p_2)^{k_2} \dots f(p_s)^{k_s}$. Veja que f é totalmente multiplicativa, pois se $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ e $m = p_1^{t_1} p_2^{t_2} \dots p_s^{t_s}$ com k_i ou t_i possivelmente nulos.

$$f(mn) = f(p_1)^{k_1+t_1} f(p_2)^{k_2+t_2} \dots f(p_s)^{k_s+t_s}$$

$$= f(p_1)^{k_1} f(p_2)^{k_2} \dots f(p_s)^{k_s} f(p_1)^{t_1} f(p_2)^{t_2} \dots f(p_s)^{t_s} = f(m)f(n)$$

A conclusão segue do resultado provado no texto do livro.
Seja $\alpha = \log_2 f(2)$. Vejamos que $f(n) = n^\alpha$. Para isto observemos que, aplicando f, para todo $m \in \mathbb{N}^*$ temos

$$2^{\lfloor m \log_2 n \rfloor} \leq n^m < 2^{\lfloor m \log_2 n \rfloor + 1}$$

$$\Longrightarrow 2^{\alpha \lfloor m \log_2 n \rfloor} \leq (f(n))^m < 2^{\alpha(\lfloor m \log_2 n \rfloor + 1)}$$

Assim,

$$2^{\frac{\alpha \lfloor m \log_2 n \rfloor}{m}} \leq f(n) < 2^{\frac{\alpha(\lfloor m \log_2 n \rfloor + 1)}{m}} \quad \text{para todo } m \in \mathbb{N}^*.$$

Mas

$$\lim_{m\to\infty} \frac{\alpha \lfloor m \log_2 n \rfloor}{m} = \lim_{m\to\infty} \frac{\alpha(\lfloor m \log_2 n \rfloor + 1)}{m} = \alpha \log_2 n,$$

donde concluímos que $f(n) = 2^{\alpha \log_2 n} = n^\alpha$.

2.1 FUNÇÃO DE MÖBIUS E FÓRMULA DE INVERSÃO

Problema 2.28. *(A) Encontre fórmulas fechadas para as somas*

- $\sum_{r|n} \mu(r)d(n/r)$
- $\sum_{d|n} \mu(d)\sigma(n/d)$
- $\sum_{d|n} \mu(d)\sigma_m(n/d)$

Solução

Já vimos que se $F(n) = \sum_{d|n} f(d)$ então $f(n) = \sum_{d|n} \mu(d)f(n/d)$. Assim, podemos achar as seguintes fórmulas fechadas

- $d(n) = \sum_{d|n} 1 \Rightarrow 1 = \sum_{d|n} \mu(d)d(n/d)$.
- $\sigma(n) = \sum_{d|n} d \Rightarrow n = \sum_{d|n} \mu(d)\sigma(n/d)$.
- $\sigma_m(n) = \sum_{d|n} d^m \Rightarrow n^m = \sum_{d|n} \mu(d)\sigma_m(n/d)$.

Problema 2.29. *(A) Seja f uma função multiplicativa e não identicamente nula e $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Mostre que*

$$\sum_{d|n} \mu(d)f(d) = \prod_{j=1}^{k}(1 - f(p_j)).$$

Solução

Veja que a função $g(n) = \mu(n)f(n)$ é multiplicativa, pois μ e f são multiplicativas, e, consequentemente, $G(n) = \sum_{d|n} \mu(d)f(d)$ também é multiplicativa. Assim,

$$G(n) = G(p_1^{\alpha_1}) \cdots G(p_k^{\alpha_k}) = (1 + (-1)^1 f(p_1) + 0 + \dots) \cdots ((1 + (-1)^1 f(p_k) + 0 + \dots))$$

Pois se $\mu(p_i^k) = 0$ para $k \geq 2$. Concluímos que

$$\sum_{d|n} \mu(d)f(d) = G(n) = \prod_{j=1}^{k}(1 - f(p_j)).$$

Problema 2.30. *(A) Encontre fórmulas fechadas para as somas*

- $\sum_{r|n} \mu(r)d(r)$
- $\sum_{d|n} \mu(d)\sigma(d)$
- $\sum_{d|n} \mu(d)\varphi(d)$

- $\sum_{d|n} \frac{\mu(d)}{d}$.

Solução

Para cada um dos itens usaremos que $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ e o resultado do problema anterior.

- $\sum_{r|n} \mu(r)d(r) = \prod_{j=1}^{k}(1 - d(p_j)) = (-1)^k$.
- $\sum_{d|n} \mu(d)\sigma(d) = \prod_{j=1}^{k}(1 - \sigma(p_j)) = (-1)^k p_1 \cdots p_k$.
- $\sum_{d|n} \mu(d)\varphi(d) = \prod_{j=1}^{k}(1 - \varphi(p_j)) = \prod_{j=1}^{k}(2 - p_j)$.
- $\sum_{d|n} \frac{\mu(d)}{d} = \prod_{j=1}^{k}(1 - \frac{1}{p_j}) = \frac{\varphi(n)}{n}$.

Observe que para $n = 1$ temos $k = 0$ e as fórmulas anteriores também são verdadeiras.

Problema 2.31. *(A) Seja r o número de fatores primos diferentes de n. Demonstre que*

$$\sum_{d|n} |\mu(d)| = 2^r.$$

Solução

Sejam $\{p_1, p_2, \ldots, p_r\}$ o conjunto dos divisores primos de n. Sabemos que $|\mu(d)| = 1$ se, e somente se, d é livre de quadrados, ou seja, é o produto dos primos de algum subconjunto do conjunto de primos. Veja que isso inclui o vazio, pois $\mu(1) = 1$. Como o conjunto tem 2^r subconjuntos (para cada primo há duas possibilidades ele divide d ou não) concluímos que essa a quantidade de parcelas 1 e as demais são zero. Portanto, $\sum_{d|n} |\mu(d)| = 2^r$.

Problema 2.32. *(A) Seja n um inteiro positivo que não é primo e tal que $\varphi(n) \mid n - 1$. Demonstre que n possui ao menos quatro fatores primos distintos.*

Solução

Primeiro veja que n é livre de quadrados. Suponha que não, então p^k é a maior potência de p que divide n com $k \geq 2$. Veja que $\varphi(p^k) = p^{k-1}(p-1)$ é múltiplo de p e $\varphi(n) = \varphi(p^k) \cdot \varphi(n/p^k) \Rightarrow p \mid \varphi(n)$. Com isso, $p \mid n$ e $p \mid n - 1$ implicando $p \mid 1$ que é uma contradição. Portanto, n é o produto de primos distintos $n = p_1 p_2 \ldots p_s$.
Veja que $s > 1$, pois n não é primo. Se $s = 2$, então $n = pq$ e $\varphi(n) \mid n - 1 \iff (p-1)(q-1) \mid pq - 1$. Sabemos que $(p-1)(q-1) = pq - p - q + 1 \mid pq - p - q + 1$. Fazendo a diferença $(p-1)(q-1) \mid p + q - 2 = (p-1) + (q-1)$. Suponha sem perda de generalidade que $p > q$. Se $q = 2$ temos $p - 1 \mid p$ que é falso para todo p primo maior que 2. Se $q \geq 3$ então $(p-1)(q-1) \geq 2(p-1) = (p-1) + (p-1) > (p-1) + (q-1)$ e $(p-1)(q-1) \nmid (p-1) + (q-1)$. Se $s = 3$ temos $n = pqr$ e $\varphi(n) \mid n - 1 \iff$

$(p-1)(q-1)(r-1) \mid pqr-1$. Suponha sem perda de generalidade que $p > q > r \geq 2$. Esse é exatamente o problema 0.29 deste livro e as únicas soluções dessa divisibilidade são $(p,q,r) = (2,4,8)$ e $(p,q,r) = (3,5,15)$. Nas duas soluções não temos três valores primos e também não temos solução para $s = 3$.
Concluímos que se houver solução, então $s \geq 4$.

Se $\varphi(n) = n-1$ então n é primo, pois todos os números menores que n são primos com n. Como no nosso problema n não é primo, então $\varphi(n) \mid n-1 \Rightarrow \varphi(n) \leq \frac{n-1}{2}$, pois esse é o maior valor possível para um divisor de $n-1$ menor que $n-1$. Nesse caso, temos

$$\frac{\varphi(n)}{n} = \prod_{p|n}\left(1-\frac{1}{p}\right) \leq \frac{n-1}{2n}$$

Problema 2.33. *(T) Dados dois números reais α e β tais que $0 \leq \alpha < \beta \leq 1$, demonstre que existe um número natural m tal que*

$$\alpha < \frac{\varphi(m)}{m} < \beta.$$

Solução

Primeiro veja que $\prod_{p\ primo} \frac{p-1}{p} \to 0$.
Uma forma de provar isto é usar que para $2^a \leq n < 2^{a+1}$ então $H_n = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n} \geq \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{2^a}$ e essa última pode ser cotada usando que $\frac{1}{3} + \frac{1}{4} > \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$, $\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} > \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} = \frac{1}{2}$ e assim por diante. Temos $H_n > 1 + \frac{a}{2}$ e para $a \to \infty$ temos $H_n \to \infty$. Além disso, temos que cada $\frac{1}{n}$ pode ser ser quebrado como produto de $\frac{1}{p^k}$. Por exemplo, $\frac{1}{12} = \frac{1}{2^2} \cdot \frac{1}{3}$. Veja também que para cada primo a soma dos inversos das potências é $\frac{1}{1} + \frac{1}{p} + \frac{1}{p^2} + \cdots = \frac{1}{1-\frac{1}{p}} = \frac{p}{p-1}$. Logo

$$H_n < \left(1 + \frac{1}{2} + \frac{1}{2^2} + \ldots\right)\left(1 + \frac{1}{3} + \frac{1}{3^2} + \ldots\right)\cdots = \prod_{p\ primo} \frac{p}{p-1}$$

Se $\prod_{p\ primo} \frac{p}{p-1} \to \infty$ então $\prod_{p\ primo} \frac{p-1}{p} \to 0$.
Veja também que para p suficientemente grande temos $\frac{p-1}{p} = 1 - \frac{1}{p}$ é tão próximo de 1 quando se queira.
Dados α e β com $0 \leq \alpha < \beta \leq 1$ tome o natural M tal que $\frac{1}{M} < \beta - \alpha$. Ele existe, pois $\frac{1}{M} \to 0$ para M tendendo a infinito. Tome N tal que o primo N-ésimo p_N seja maior que M. Assim, $\frac{p_N - 1}{p_N} = 1 - \frac{1}{p_N} > 1 - \frac{1}{M}$.
Considere a sequência $x_k = \prod_{i=0}^{k} \frac{p_{N+i}-1}{p_{N+i}}$ em que esses são os primos em ordem crescente a partir do p_N. Temos a sequência x_n é decrescente, pois cada fator é menor que

1, $x_0 > \frac{M-1}{M}$ e $x_n \to 0$ quando n vai para infinito, já que $\prod_{p\ primo} \frac{p-1}{p} \to 0$. Mas a sequência não pode "saltar"intervalos grandes

$$x_k - x_{k+1} = x_k(1 - \frac{p_{N+k+1} - 1}{p_{N+k+1}}) = \frac{x_k}{p_{N+k+1}} < \frac{1}{M}$$

Como a sequência vai para zero existe um x_r com r mínimo tal que $x_r < \beta$. Como r é mínimo, então $x_{r-1} \geq \beta$. Se Tivermos $x_r \leq \alpha$ então

$$\frac{1}{M} < \beta - \alpha < x_{r-1} - x_r < \frac{1}{M}$$

que é absurdo. Logo $\alpha < x_r < \beta$ e temos $x_r = \prod_{i=0}^{r} \frac{p_{N+i}-1}{p_{N+i}} = \prod_{i=0}^{r} \frac{\varphi(p_{N+i})}{p_{N+i}} = \frac{\varphi(p_N p_{N+1} \cdots p_{N+r})}{p_N p_{N+1} \cdots p_{N+r}}$ que é forma $\frac{\varphi(A)}{A}$.

Problema 2.34. *(OI) Seja m um inteiro positivo. Dizemos que um inteiro $m \geq 1$ é "superabundante" se*

$$\forall k \in \{1, 2, \ldots, m-1\} \qquad \frac{\sigma(m)}{m} > \frac{\sigma(k)}{k}.$$

Demonstre que existe um número infinito de números superabundantes.

Solução

Pelos resultados provados nos problemas 2.33 e 2.38 sabemos que $\frac{\sigma(n!)}{n!} \geq H_n$, onde H_n é a soma dos inversos dos inteiros positivos e tende para infinito quando n cresce indefinidamente. Isso nos diz que $\frac{\sigma(m)}{m}$ pode se tornar tão grande quando se queira.
Suponha por absurdo que a partir de certo N não temos mais inteiros $m > 1$ superabudantes. Seja k_{max} o valor de $\{1, 2, \ldots, N\}$ tal que $\frac{\sigma(k_{max})}{k}_{max}$ seja máximo. Se existe $t > N$ temos $\frac{\sigma(A)}{t} > \frac{\sigma(k_{max})}{k}_{max}$, então o menor t com essa propriedade é superabundante já que é o primeiro valor em que a função passa de $\frac{\sigma(k_{max})}{k}_{max}$ que era o máximo até então. Se tal t não existe, então $\frac{\sigma(m)}{m}$ seria limitada e já provamos que isto é falso. Logo, não existe um N tal que não existem mais números superabundantes após N. Concluímos que existem infinitos números superabundantes.

Problema 2.35. *(OI) Demonstre que*

$$\frac{\sigma(n)}{d(n)} \geq \sqrt{n}.$$

Solução

Para cada divisor d de n temos também o divisor $\frac{n}{d}$. Pela desigualdade das médias

$$\frac{d + \frac{n}{d}}{2} \geq \sqrt{d \cdot \frac{n}{d}} = \sqrt{n} \iff d + \frac{n}{d} \geq 2\sqrt{n}$$

Logo

$$2\sigma(n) = \sum_{d|n}(d + \frac{n}{d}) \geq \sum_{d|n} 2\sqrt{n} = 2d(n)\sqrt{n} \Rightarrow \frac{\sigma(n)}{d(n)} \geq \sqrt{n}.$$

Problema 2.36. *(A) Encontre todos os valores de n para os quais $\varphi(n) \mid n$.*

Solução

Usando o resultado do problema 2.17 temos $n = 1$ ou $n = 2^a \cdot 3^b$ com $a \geq 1$ e $b \geq 0$.

Problema 2.37. *(T) Demonstrar que $m \mid \sigma(mn-1)$ para todo n se, e só se, $m = 3$, 4, 6, 8, 12 ou 24.*

Obs.: *Você pode usar na solução o teorema de Dirichlet, segundo o qual se a e b são inteiros positivos com* $\text{mdc}(a,b) = 1$ *então existem infinitos primos* $p \equiv a \pmod{b}$.

Solução

Seja $m = p_1^{k_1} \dots p_s^{k_s}$. Se tivermos algum $p_i \geq 3$ veja que podemos tomar x e y primos tais que $x \equiv 2 \pmod{p_i^{k_i}}$ e $x \equiv -1 \pmod{p_j^{k_j}}$, para $j \neq i$, e $y \equiv \frac{p_i^{k_i}-1}{2} \pmod{p_i^{k_i}}$ e $y \equiv 1 \pmod{p_j^{k_j}}$, para $j \neq i$. Pelo Teorema Chinês dos restos existem soluções x_0 e y_0 que são únicas módulo m. Veja que $\text{mdc}(x_0, m) = \text{mdc}(y_0, m) = 1$, pois para cada primo que divide m sabemos pelas congruências que ele não divide x_0 nem y_0. Agora pelo Teorema de Dirchlet podemos tomar x e y primos. Note que $x \cdot y \equiv -1 \pmod{m}$, pois $x \cdot y \equiv -1 \pmod{p_j^{k_j}}$ para todo j incluindo i, e existe n tal que $xy = mn - 1$. Por outro lado, veja que

$$m \mid \sigma(xy) \Rightarrow p_i^{k_i} \mid (x+1)(y+1) = xy + x + y + 1$$

$$\Rightarrow p_i^{k_i} \mid x + y = 2 + \frac{p_i^{k_i} - 1}{2} = 2 + \frac{p_i^{k_i} - 1}{2}$$

$$\Rightarrow p_i^{k_i} \mid \frac{p_i^{k_i} + 3}{2} \Rightarrow p_i^{k_i} \mid 3$$

Que só é verdade para $p_i = 3$ e $k_i = 1$.

Logo, só precisamos estudar $n = 2^k$ e $n = 2^k \cdot 3$.

Mas para esses n como no caso anterior podemos encontrar x e y primos tais que $x \equiv 5 \pmod{n}$ e $y \equiv (n-1) \cdot 5^{-1} \pmod{n}$ onde 5^{-1} é o inverso multiplicativo de 5 módulo n que existe pois $\text{mdc}(n, 5) = 1$. Temos $xy \equiv -1 \pmod{n}$ e $n \mid (x+1)(y+1) = xy + x + y + 1 \Rightarrow n \mid x + y$. Veja que $n \mid 5(x+y)$ e $5(x+y) \equiv 5^2 + (n-1) \equiv 24 \pmod{n}$. Concluímos que $n \mid 24$.

Para provar que os divisores de 24 maiores que 2 realmente possuem a propriedade.

Podemos ver rapidamente que $m = 2$ não funciona, pois $9 \equiv -1 \pmod{2}$ e $2 \nmid \sigma(9) = 9 + 3 + 1 = 13$.

Para $m > 2$, considere a fatoração de $mn-1$ em primos $mn-1 = p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$. Veja que $\sigma(mn-1) = \sigma(p_1^{k_1})\sigma(p_2^{k_2})\cdots\sigma(p_s^{k_s})$ e $\sigma(p_i^{k_i}) \mid \sigma(mn-1)$ para cada i.
Se $3 \mid m$ então $mn-1 = 3k-1$. Temos $p_i \neq 3$ e se cada potência $p_i^{k_i}$ fosse congruente a 1 módulo 3 então $-1 \equiv 3k-1 \equiv 1^s \equiv 1 \pmod 3$ que é falso. Existe algum índice j tal que $p_i^{k_i} \equiv 2 \equiv -1 \pmod 3$. Isso significa que $p_i \equiv 2 \pmod 3$ e k_i é ímpar. Logo, $\sigma(p_i^{k_i}) = \frac{p_i^{k_i+1}-1}{p_i-1}$. Como k_i+1 é par $3 \mid p_i^{k_i+1}-1$ e $3 \nmid p_i - 1 \Rightarrow 3 \mid \sigma(p_i^{k_i}) \Rightarrow 3 \mid \sigma(3k-1)$.
Se $4 \mid m$ o mesmo raciocíno acima funciona. Temos $mn-1 \equiv 4k-1$, $p_i \neq 2$ e se cada potência $p_i^{k_i}$ fosse congruente a 1 módulo 4, então $4k-1$ seria congruente a 1 módulo 4 que é falso. Então tem alguma potência $p_i^{k_i}$ com congruência $3 \equiv -1 \pmod 4$ e k_i ímpar. Novamente, $\sigma(p_i^{k_i}) = \frac{p_i^{k_i+1}-1}{p_i-1}$. Como k_i+1 é par $8 \mid p_i^{k_i+1}-1$ ($x^2 \equiv 1 \pmod 8$ para todo x ímpar) e $4 \nmid p_i - 1 \Rightarrow 4 \mid \sigma(p_i^{k_i}) \Rightarrow 4 \mid \sigma(4k-1)$.
Se $6 \mid m$ a situação é análoga aos casos 3 e 4, pois cada primo $p \geq 5$ é congruente a 1 ou $5 \equiv -1 \pmod 6$. Os outros restos possíveis não podem ser primos $6k = 2\cdot 3\cdot k$, $6k+2 = 2\cdot(3k+1)$, $6k+3 = 3\cdot(2k+1)$ e $6k+4 = 2\cdot(3k+2)$. Como nos casos anteriores há $p_i \equiv -1 \pmod 6$ com expoente k_i ímpar implicando $6 \mid \sigma(p_i^{k_i})$.
Se $8 \mid m$ as potências de primos de $8k-1$ são congruentes a 1, 3, -3 ou -1. Como $8k-1 \equiv -1$ não podemos ter todas congruentes a 1. Então pelo menos uma apresenta outra congruência.
(i) Se alguma possui a congruência -1 então $p_i \equiv -1 \pmod 8$, k_i ímpar, $16 \mid p^{k_i+1}-1 = (8t-1)^2 - 1 = 8^2t^2 - 16t$, $4 \nmid p_i - 1$ e podemos concluir que $8 \mid \sigma(p_i^{k_i})$ e $8 \mid \sigma(8k-1)$.
(ii) Se temos duas ou mais potências com congruência 3 módulo 8. Pelo que vimos no caso 4 teríamos os σ de dois ou mais valores múltiplos de 4 e o nosso resultado seria múltiplo de 16. Temos $8 \mid \sigma(8k-1)$.
(iii) Falta cobrir o caso em que não há congruência -1 e há no máximo uma congruência 3. Se não há congruência 3, então o -1 da congruência de $8k-1$ viria apenas do -3, mas isso é possível, pois seria o produto de potência 1 módulo 4 resultando em -1. Resta o caso em que há exatamente uma potência congruente a 3 e (como 3 não é equivalente a -1) pelo menos uma potência congruente a -3. Nesse caso, novamente, usamos que $p_i^{k_i} \equiv 3 \pmod 8 \Rightarrow p_i \equiv 3 \pmod 8$, k_i ímpar e $4 \mid \sigma(p_i^{k_i}) = \frac{p_i^{k_i+1}-1}{p_i-1}$ (8 divide o numerador e 4 não divide o denominador) e $p_j^{k_j} \equiv -3 \pmod 8 \Rightarrow p_j \equiv -3 \pmod 8$, k_i ímpar e $2 \mid \sigma(p_i^{k_i}) = \frac{p_i^{k_i+1}-1}{p_i-1}$ (8 divide o numerador e 8 não divide o denominador).
Isso conclui a solução, pois $12 = 3\cdot 4$ é consequência de $3 \mid m$ e $4 \mid m$ e $24 = 3\cdot 8$ é consequência de $3 \mid m$ e $8 \mid m$.
Portanto, se $m \mid \sigma(mn-1), \forall n \iff m = 3, 4, 6, 8, 12$ ou 24.

Problema 2.38. *(A) Demonstre que*

$$\frac{\sigma(n!)}{n!} > 1 + \frac{1}{2} + \cdots + \frac{1}{n}.$$

Solução

Sabemos que $\frac{\sigma(m)}{m} = \sum_{d|m} \frac{d}{m} = \sum_{d|m} \frac{1}{d}$, já que para cada divisor d temos um outro $\frac{m}{d}$. Dessa forma, $\frac{\sigma(n!)}{n!}$ é a soma dos inversos dos divisores de $n!$. Observe que para cada $1 \leq x \leq n$ temos $x \mid n!$. Concluímos que a soma dos inversos dos números de 1 a n é a soma dos inversos de alguns divisores de $n!$ que é menor que a soma dos inversos de todos os divisores de $n!$ do outro lado.

Problema 2.39. *(T) Demonstre que existem infinitos números naturais n para os quais $\sigma(x) = n$ não tem solução.*

Solução

Comecemos observando que $\sigma(6) = \sigma(11) = 12$ e que para qualquer p primo com $p > 3$ temos $\sigma(6p) = \sigma(6) \cdot \sigma(T) = 12(p+1) = \sigma(11p)$. Considere a sequência p_i dos primos maiores que ou iguais a 5, ou seja, $p_1 = 5$, $p_2 = 7$ e assim por diante. Para cada n considere o conjunto $A_n = \{1, 2, \ldots, 11p_n\}$.

Se $a > 11p_n$ então $\sigma(a) \geq a + 1 > 11p_n$. Dessa forma, cada $a \in A_n$ só pode ser imagem por σ de outro elemento de A_n. Seja B_n o conjunto formado pelos elementos b de A_n tais que existe a em A_n que satisfaz a equação $\sigma(a) = b$. Note que para pelo menos n elementos $b = 12(p_i + 1)$ de A_n podemos encontrar dois elementos distintos $a_1 = 6p_i$ e $a_2 = 11p_i$ tais que $\sigma(a_1) = \sigma(a_2) = b$. É como se a_2 não adicionasse elementos à imagem de σ. Assim, podemos concluir que $|B_n| \leq |A_n| - n$ já que não há termos suficientes para cobrir mais elementos que isso. Em outras palavras, pelo menos n elemento de $a \in A_n$ tais que a equação $\sigma(x) = a$ não possui solução.
Então o conjunto dos inteiros a tais que $\sigma(x) = a$ não tem solução não pode ser limitado, pois podemos pegar n suficientemente grande. Concluímos que tal conjunto é infinito.

Problema 2.40. *(T) Demonstre que para todo $m > 1$*

$$\left| \sum_{k=1}^{m} \frac{\mu(k)}{k} \right| < \frac{2}{3}.$$

Solução

Na parte teórica do livro foi provado que

$$\left| \sum_{k=1}^{m} \frac{\mu(k)}{k} \right| < 1.$$

Vamos melhorar essa cota. A chave para isso é que $\mu(x) = 0$ quando x possui algum divisor quadrado perfeito. Observe que de 1 a m temos $\lfloor \frac{m}{4} \rfloor$ múltiplos de 4, $\lfloor \frac{m}{9} \rfloor$ múltiplos de 9 e $\lfloor \frac{m}{36} \rfloor$ múltiplos de 36. Pelo Princípio da Inclusão-Exclusão sabemos que $\mu(x) = 0$ para pelo menos

$$\left\lfloor \frac{m}{4} \right\rfloor + \left\lfloor \frac{m}{9} \right\rfloor - \left\lfloor \frac{m}{36} \right\rfloor > \frac{m}{4} - 1 + \frac{m}{9} - 1 - \frac{m}{36} = \frac{m(9+4-1)}{36} - 2 = \frac{m}{3} - 2$$

valores k com $1 \leq k \leq m$.

Por conta dessa parcela -2 podemos observar fazer separadamente os casos $m = 1$, $m = 2$, $m = 3$, $m = 4$ e $m = 5$ que resultam em 1, $1 - \frac{1}{2} = \frac{1}{2}$, $1 - \frac{1}{2} - \frac{1}{3} = \frac{1}{6}$, $\frac{1}{6}$ (pois $\mu(4) = 0$) e $1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} = \frac{-1}{30}$. Usaremos de agora em diante que $-1 < \frac{\mu(1)}{1} + \frac{\mu(2)}{2} + \frac{\mu(3)}{3} + \frac{\mu(4)}{4} + \frac{\mu(5)}{5} < 1$.

Para $k \geq 6$ temos $-1 < \mu(k)\left(\lfloor \frac{m}{k} \rfloor - \frac{m}{k}\right) < 1$, se k não é divisível por 4 ou 9, e 0, se $4 \mid k$ ou $9 \mid k$. Assim,

$$\left| \sum_{k=1}^{m} \mu(k) \left\lfloor \frac{m}{k} \right\rfloor - m \sum_{k=1}^{m} \frac{\mu(k)}{k} \right| < 1 + (m-5) - (\frac{m}{3} - 2) = \frac{2m}{3} - 2$$

Lembrando que $\sum_{k=1}^{m} \mu(k) \lfloor \frac{m}{k} \rfloor = 1$ temos

$$\left| m \sum_{k=1}^{m} \frac{\mu(k)}{k} \right| < \frac{2m}{3} \Rightarrow \left| \sum_{k=1}^{m} \frac{\mu(k)}{k} \right| < \frac{2}{3}.$$

Problema 2.41. *(A) Encontre todos os inteiros positivos n tais que*

$$n = d_6^2 + d_7^2 - 1,$$

onde $1 = d_1 < d_2 < \cdots < d_k = n$ são todos os divisores positivos do número n.

Solução

Sabemos que $d_7 \mid n$ e $d_7 \mid d_7^2$ então $d_7 \mid d_6^2 - 1 = (d_6 - 1)(d_6 + 1)$. Analogamente, temos também $d_6 \mid d_7^2 - 1$ e podemos concluir que $\text{mdc}(d_6, d_7) = 1$. Sendo divisores de n primos entre si podemos concluir que $d_6 d_7 \mid n$ e podemos escrever $n = Q d_6 d_7$ para algum inteiro positivo Q. Veja que os divisores de d_6 e d_7 também são divisores de n. Faremos alguns casos.

(i) Se $d_6 = m$ e $d_7 = m + 1$ então $n = m^2 + (m+1)^2 - 1 = 2m^2 + 2m = 2m(m+1)$. Observe que $2 \mid m(m+1)$Como $m = d_6$ temos $m \geq 6$.
- Se $m = 6$ então $n = 2 \cdot 6 \cdot 7 = 84$ e 6 não é o sexto divisor.
- Se $m = 7$ então $n = 2 \cdot 7 \cdot 8 = 112$ e 7 não é o sexto divisor.

- Se $m = 8$ então $n = 2 \cdot 8 \cdot 9 = 144$ e, nesse caso, temos que 144 é solução, pois os sete menores divisores de 144 são 1, 2, 3, 4, 6, 8 e 9 satisfazendo as condições.
- Se $m = 9$ então $n = 2 \cdot 9 \cdot 10 = 180$ e 9 não é o sexto divisor.
- Se $m = 10$ então $n = 2 \cdot 10 \cdot 11 = 220$ e 10 não é o sexto divisor.
- Se $m = 11$ então $n = 2 \cdot 11 \cdot 12 = 180$ e 11 não é o sexto divisor.
- Se $m = 12$ então $n = 2 \cdot 12 \cdot 13 = 312$ e 12 não é o sexto divisor.

Para $m \geq 13$, se $3 \mid 2m(m+1)$ então os números do conjunto $\{1, 2, 3, 4, 6, 12\}$ são divisores de n menores que m. Se m é uma potência de 2, então $m = 2^k$ e $n = 2^{k+1}(2^k + 1)$. Mas n possui $k - 1$ divisores 2^a menores que m e se $k \geq 6$ então 2^k não poderá ser o sexto divisor. Se $k = 5$ então $3 \mid 2^5 + 1 = 33$ e já vimos que não funciona. Se $m + 1$ é uma potência de 2, então $m + 1 = 2^k$ e $n = 2^{k+1}(2^k - 1)$. Como vimos anteriormente n possui $k - 1$ divisores 2^a menores que n e se $k \geq 6$ não pode haver solução. Se $k = 5$ então temos a solução $n = 2 \cdot 31 \cdot 32 = 1984$, pois seus sete menores divisores são 1, 2, 4, 8, 16, 31 e 32. Se os dois não são potências de primos. Existem primos ímpares p e q tais que $p \mid m$ e $q \mid m + 1$. Os números $\{1, 2, 4, p, 2p, q, 2q\}$ são sete divisores de n e $d_6 < d_7$ que é menor que ou igual ao maior elemento desse conjunto.

- Se $p > q$ então o maior elemento é $2p$. Temos $d_6 < d_7 \leq 2p \Rightarrow d_6 = p$ e $d_7 = p + 1$. Se $d_7 = p + 1 = 2q$ então p seria o quinto divisor de n e não iria satisfazer as condições. Se $p + 1 = 4q$ então 8 divide n e os números 1, 2, 4, 8, q e $2q$ são seis divisores de n menores que p. Se $q > 4p$ então 1, 2, 4, q, $2q$ e $4q$ são divisores de n menores que p. Em todos os casos, não seria possível $d_6 = p$.
- Se $p < q$ então o maior elemento é $2q$. Temos $d_7 \leq 2q \Rightarrow d_7 = 2q$ ou $d_7 = q$. Se $d_7 = 2q$ então $d_6 = 2q - 1$ é um múltiplo ímpar de p. Se for $3p$ então $3 \mid n$ e já vimos que não há solução. Se $d_6 \geq 5p$ então não pode ser o sexto divisor, pois 1, 2, 4, p, $2p$ e $4p$ são seis divisores menores que esse candidato a d_6. Se $d_7 = q$ então $d_6 = q - 1$ é um múltiplo par de p. Se $d_6 = q - 1 = 2p$ então seria apenas o quinto divisor de n, após 1, 2, 4 e p. Se for $4p$ então o número é múltiplo de 8 e d_6 seria pelo menos o sétimo divisor após os já listados com 8 e $2p$. Para $d_6 = q - 1 \geq 6p$ os divisores 1, 2, 4, p, $2p$ e $4p$ nos garantem que esse não pode ser o sexto divisor de n.

Portanto, as únicas soluções nesse caso são 144 e 1984.

(ii) Se d_7 é potência de um primo maior que 2. Podemos escrever $d_7 = p^k$. Daí, $p \mid (d_6 - 1)(d_6 + 1) \Rightarrow p \mid d_6 - 1$ ou $p \mid d_6 + 1$, mas não ambos, pois $\text{mdc}(d_6 - 1, d_6 + 1) \mid 2 < p$. Logo, $d_7 = p^k \mid d_6 - 1$ ou $d_7 = p^k \mid d_6 + 1$. O primeiro caso não

pode ser verdade, pois implicaria $d_7 \leq d_6 - 1 < d_7$ que é absurdo. O segundo caso $d_7 \leq d_6 + 1 \leq d_7 \Rightarrow d_7 = d_6 + 1$. Recai no caso (i) que já resolvemos.

(iii) Se d_7 é uma potência de 2. Temos $d_7 = 2^k$ e $2^k \mid (d_6 - 1)(d_6 + 1)$. Temos $d_7 \geq 7 \Rightarrow k \geq 3$. Como o mdc dos fatores divide 2 temos que $2^{k-1} \mid d_6 - 1$ ou $2^{k-1} \mid d_6 + 1$. - Se $2^{k-1} \mid d_6 - 1$ temos $d_6 - 1 = 2^{k-1} \cdot t < 2^k \Rightarrow t = 1$. Veja que $k \leq 6$, pois $k \geq 7$ implica que 2^k não pode ser o sétimo divisor de n. Se $k = 3, 4, 5$ ou 6 temos os possíveis pares (d_6, d_7) são $(5, 8)$, $(9, 16)$, $(17, 32)$ e $(33, 64)$, respectivamente. O primeiro caso não serve pois $d_6 \geq 6$. O segundo não serve, porque 9 já é pelo menos sétimo divisor de um múltiplo de 9 e 16. No terceiro caso vemos que $17 \nmid 32^2 - 1$. E no quarto e último caso 33 é pelo menos o sétimo divisor do número.
- Se $2^{k-1} \mid d_6 + 1$ temos $d_6 + 1 = 2^{k-1} \cdot t \leq d_7 = 2^k \Rightarrow t \leq 2$. Se $t = 2$, então $d_6 + 1 = d_7$ e recaímos no caso (i). Se $d_6 + 1 = 2^{k-1}$. Novamente, $k \leq 6$ e para $k = 3, 4, 5$ ou 6 temos os possíveis pares (d_6, d_7) são $(3, 8)$, $(7, 16)$, $(15, 32)$ e $(31, 64)$, respectivamente.o primeiro caso não pode, pois $d_6 \geq 6$. Nos demais casos $d_6 \nmid d_7^2 - 1$.

De agora em diante sabemos que d_7 possui dois ou mais divisores primos.

(iv) Veja que se d_7 possui três fatores primos distintos então teria pelo menos $2 \cdot 2 \cdot 2 - 1 = 7$ divisores menores que ele e não poderia ser o sétimo divisor de n. O mesmo ocorre se d_7 tem dois divisores primos com um expoente maior que ou igual a 3. Se d_7 tem dois fatores primos cada um com expoente 2 então tem $3 \cdot 3 - 1 = 8$ divisores menores que ele e novamente não poderia ser o sétimo divisor. Isso nos deixa apenas dois casos $d_7 = p^2 q$ e $d_7 = pq$ para p e q primos.

(v) Se d_6 é uma potência de 2. Então $d_6 \geq 6$ implicando $d_6 = 2^k$ com $k \geq 3$. Temos os sete divisores 1, 2, 2^2, 2^3, p, q e $2p$ menores que d_7 e não temos solução.

(vi) Se d_6 é uma potência de primo p ímpar. Temos $d_6 = p^k$ implica $p \mid d_7 - 1$ ou $p \mid d_7 + 1$, mas não ambos pois o mdc deles é 1 ou 2. Então um dos fatores leva todos os fatores e $d_6 \mid d_7 - 1$ ou $d_6 \mid d_7 + 1$.
- Se $d_6 \mid d_7 - 1$ então $d_7 = kd_6 + 1$. Temos

$$Qd_6(kd_6 + 1) = d_6^2 + kd_6(kd_6 + 2) \Rightarrow Q(kd_6 + 1) = d_6 + k(kd_6 + 1) + k$$

$$\Rightarrow kd_6 + 1 \mid k + d_6$$

Mas isso nos leva a $kd_6 + 1 \leq k + d_6 \iff (k-1)(d_6 - 1) \leq 0$. Se $k = 1$ temos então $d_6 = d_7 - 1$ e mais uma vez cairíamos no caso (i). Se $k \geq 2$ a desigualdade é falsa.

- Se $d_6 \mid d_7 + 1$ então $d_7 = kd_6 - 1$. Temos

$$Qd_6(kd_6 - 1) = d_6^2 + kd_6(kd_6 - 2) \Rightarrow Q(kd_6 - 1) = d_6 + k(kd_6 - 1) - k$$

$$\Rightarrow kd_6 - 1 \mid -k + d_6$$

Se $k = d_6$ então $d_7 = d_6^2 - 1$ com d_6 ímpar e temos que $2^3 \mid d_7$. Vimos no caso (iv) que não dá solução.

Se $k \neq d_6$ temos $|kd_6 - 1| \leq |-k + d_6|$ que é equivalente a

$$kd_6 - 1 \leq -k + d_6 \iff (k-1)(d_6 + 1) \leq 0$$

ou

$$kd_6 - 1 \leq k - d_6 \iff (k+1)(d_6 - 1) \leq 0$$

Como $d_7 > d_6$ sabemos que $k \geq 2$ e as duas possibilidades são falsas.

Concluímos que nesse caso d_6 não temos solução. Daqui para frente podemos supor que d_6 tem pelo menos dois divisores primos distintos.

(vii) Se $d_7 = p^2q$ então 1, p, p^2, q e qp são 5 divisores de d_7 menores que d_7. Resta apenas uma possibilidade para d_6 que é primo com d_7. Ele precisa ser um primo r, pois se tiver mais algum divisor menor que ele o $d_7 = p^2q$ não poderia ser o sétimo divisor. Os casos (v) e (vi) garantem que não temos solução.

(viii) Se $d_7 = pq$ então 1, p e q são três divisores de n menores que d_7. Além disso, d_6 possui pelo menos dois fatores primos r e s. Isso no mínimo resulta em 3 outros divisores r, s e rs menores que d_7. Dessa forma, pq só poderá ser o sétimo divisor se $d_6 = rs$ e os únicos divisores de n menores que pq são 1, p, q, r, s e rs. Se $r < p$, então rq seria mais um divisor de n menor que pq e não teríamos solução. Logo, para poder ter solução $r > p$. Analogamente, devemos ter $s > q$ para não termos o divisor $ps < pq$. Porém, essas duas desigualdades nos levam a $d_6 = rs > pq = d_7 > d_6$. Portanto, não temos solução.

Concluímos que as únicas soluções são 144 e 1984 provenientes do caso (i).

Problema 2.42 (IMO1998). *(OA) Para cada inteiro positivo n, $d(n)$ denota o número de divisores de n. Determine todos os inteiros positivos k tais que $d(n^2) = kd(n)$ para algum n.*

Solução

Seja $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. Temos

$$k = \frac{d(n^2)}{d(n)} = \frac{(2\alpha_1+1)(2\alpha_2+1)\dots(2\alpha_s+1)}{(\alpha_1+1)(\alpha_2+1)\dots(\alpha_s+1)}$$

Então os k que satisfazem a equação se, e somente se, possuem representação como

$$k = \frac{2k_1-1}{k_1}\frac{2k_2-1}{k_2}\dots\frac{2k_s-1}{k_s}$$

Para inteiros positivos k_i. Veja que $k \mid (2k_1-1)(2k_2-1)\dots(2k_s-1)$ e k é obrigatoriamente ímpar. Vamos provar por indução que todo k ímpar podemos encontrar solução. Para $k = 1$ temos $1 = \frac{2\cdot 1-1}{1}$ e, de fato, para $n = 1$ temos $k = 1$. Se $k = 2t-1$ com t ímpar podemos usar $k = \frac{2t-1}{t} \cdot t$ e usar a representação de t que existe por hipótese de indução. Se $k = 4t-1$ com t ímpar. Tome

$$k = \frac{12t-3}{6t-1} \cdot \frac{6t-1}{3t} \cdot t$$

e usar a representaçãode t.

Para os valores iniciais temos para $k = 3$ a representação $3 = \frac{9}{5} \cdot \frac{5}{3}$ (nesse caso $t = 1$ e pode ser omitido) e para $k = 5$ temos a representação $\frac{5}{3} \cdot 3 = \frac{5}{3} \cdot \frac{12t-3}{6t-1} \cdot \frac{6t-1}{3t}$. Veja que não há problema em usar um mesmo valor de k_i várias vezes, pois podemos tomar primos diferentes com mesmo expoente.

De maneira geral, se $m = 2^r \cdot t - 1$ com t ímpar. Podemos usar o seguinte padrão para resolver por indução.

$$k = \frac{2^r(2^r-1)t-(2^r-1)}{2^{r-1}(2^r-1)t-(2^{r-1}-1)} \dots \frac{4(2^r-1)t-3}{2(2^r-1)t-1} \cdot \frac{2(2^r-1)t-1}{(2^r-1)t} \cdot t$$

Assim, para todo k ímpar podemos representá-lo usando a representação de um número t ímpar menor e, por indução, todo inteiro positivo ímpar pode ser representado na forma apresentada.

Concluímos que $k = \frac{d(n^2)}{d(n)} \iff k$ é ímpar.

Problema 2.43. *(A) Se n é composto, mostre que $\varphi(n) \leq n - \sqrt{n}$.*

Solução

Seja p o menor divisor primo de n. Como p é o menor divisor primo de n temos $p < n/p$ e $n = p \cdot n/p \geq p \cdot p = p^2 \Rightarrow \sqrt{n} \geq p$. Uma consequência que será útil é

$\sqrt{n} = \frac{n}{\sqrt{n}} \leq \frac{n}{p} \Rightarrow -\sqrt{n} \geq -\frac{n}{p}$.
Agora veja que $1 - \frac{1}{q} < 1$ para todo primo.

$$\varphi(n) = n \prod_{q|n} \left(1 - \frac{1}{q}\right) \leq n \left(1 - \frac{1}{p}\right) = n - \frac{n}{p} \leq n - \sqrt{n}.$$

Problema 2.44. *(A) Mostre que $\varphi(n) + \sigma(n) \geq 2n$ para todo inteiro positivo n.*

Solução

Temos

$$\varphi(n) + \sigma(n) \geq 2n \iff \frac{\varphi(n)}{n} + \frac{\sigma(n)}{n} \geq 2$$

Lembrando que $\sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}$, que $\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}$ e $\mu(x) \in \{-1, 0, 1\}$ temos

$$\frac{\varphi(n)}{n} + \frac{\sigma(n)}{n} = \sum_{d|n} \frac{1 + \mu(d)}{d} \geq \frac{1 + \mu(1)}{1} = 2$$

Pois para $d > 1$ temos $\frac{1+\mu(d)}{d} \geq 0$.

Problema 2.45. *(T) Seja $f : (0, +\infty) \to \mathbb{R}$ tal que $f(x) = 0$ se $x \in (0, 1)$ e $f(x) = x \sum_{k \leq x} \frac{\mu(k)}{k}, \forall x \geq 1$. Prove que $\sum_{k \geq 1} f(x/k) = x, \forall x \geq 1$.*

Solução

Veja que $\sum_{k \geq 1} f(x/k) = \sum_{k=1}^{x} f(x/k)$, pois para $k > x$ temos $0 < x/k < 1$ e $f(x/k) = 0$.
Agora vamos desenvolver o somatório

$$\sum_{k=1}^{x} f(x/k) = \sum_{k=1}^{x} \left(\sum_{k_1 \leq x/k} \frac{x\mu(k_1)}{kk_1} \right)$$

Veja que para cada y com $1 \leq y \leq x$ ele aparece no denominador quando cada um de seus divisores é k_1 e $k = \frac{y}{k_1}$. Esse somatório se torna

$$\sum_{y=1}^{x} \frac{x}{y} \left(\sum_{d|y} \mu(d) \right) = x.$$

Na última passagem usamos o fato da soma de $\mu(d)$ sobre os divisores de n ser 1 para $n = 1$ e 0 para os demais valores de n.

Problema 2.46. *(T) Dadas duas funções $f, g : \mathbb{N}_{>0} \to \mathbb{C}$, definimos o produto de Dirichlet (ou convolução de Dirichlet) $f * g : \mathbb{N}_{>0} \to \mathbb{C}$ de f e g por*

$$f * g(n) \stackrel{\text{def}}{=} \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} f(d_1) g(d_2).$$

(a) Prove que, se $s \in \mathbb{R}$ (ou $s \in \mathbb{C}$) e as séries $\sum_{n\geq 1} \frac{f(n)}{n^s}$ e $\sum_{n\geq 1} \frac{g(n)}{n^s}$ convergem absolutamente então

$$\sum_{n\geq 1} \frac{f(n)}{n^s} \cdot \sum_{n\geq 1} \frac{g(n)}{n^s} = \sum_{n\geq 1} \frac{f*g(n)}{n^s}.$$

(b) Prove que, para quaisquer funções $f, g, h : \mathbb{N}_{>0} \to \mathbb{C}$, temos $f*g = g*f$ e $f*(g*h) = (f*g)*h$ (isto é, o produto de Dirichlet é comutativo e associativo), e que a função $I : \mathbb{N}_{>0} \to \mathbb{C}$ dada por $I(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n > 1 \end{cases}$ é o elemento neutro do produto $*$, i.e., $I*f = f*I = f$, $\forall f : \mathbb{N}_{>0} \to \mathbb{C}$.

(c) Prove que se f e g são multiplicativas então $f*g$ é multiplicativa.

(d) Prove que, se $f : \mathbb{N}_{>0} \to \mathbb{C}$ é tal que $f(1) \neq 0$, então existe uma única função $f^{(-1)} : \mathbb{N}_{>0} \to \mathbb{C}$ tal que $f*f^{(-1)} = f^{(-1)}*f = I$, a qual é dada recursivamente por $f^{(-1)}(1) = 1/f(1)$ e, para $n > 1$,

$$f^{(-1)}(n) = -\frac{1}{f(1)} \sum_{d|n, d<n} f\left(\frac{n}{d}\right) f^{(-1)}(d).$$

(e) Prove que, se f é multiplicativa, então a função $f^{(-1)}$ definida no item anterior também é multiplicativa.

Solução

(a) Antes de fazer as manipulações algébricas devemos lembrar que se o somatório converge absolutamente, então podemos mudar a ordem das parcelas e a série continua sendo congergente.

Para cada $N \geq 1$ podemos agrupar todos os pares m e n tais que $m \cdot n = N$. Passando por todos os n possíveis passaremos por todos os divisores de N. Assim, podemos concluir que

$$\sum_{n\geq 1} \frac{f(n)}{n^s} \cdot \sum_{n\geq 1} \frac{g(n)}{n^s} = \sum_{n\geq 1} \frac{f*g(n)}{n^s} = \sum_{N\geq 1} \left(\sum_{nm=N} \frac{f(n)}{n^s} \cdot \sum_{n\geq 1} \frac{g(m)}{m^s} \right)$$

$$= \sum_{N\geq 1} \frac{1}{N^s} \left(\sum_{nm=N} f(n)g(m) \right) = \sum_{N\geq 1} \frac{(f*g)(N)}{N^s}.$$

(b) Veja que podemos escrever a operação como

$$(f*g)(n) = \sum_{a\cdot b=n} f(a)g(b).$$

Com a percorrendo todos os divisores de n. Mas nesse caso b percorre também todos os divisores na ordem contrária e fica claro que $f * g = g * f$.
Temos $A = (g * k)$, $f * (g * k) = f * A$ e

$$(f * (g * k))(n) = (f * A)(n) = \sum_{a \cdot d = n} f(a)A(d) = \sum_{a \cdot d = n} f(a) \left(\sum_{b \cdot c = d} g(b)k(c) \right)$$

$$= \sum_{a \cdot b \cdot c = n} f(a)g(b)k(c)$$

Se tomarmos $B = (f * g)$ podemos desenvolver $(B * k)(n)$ da mesma forma que fizemos com $f * A$ e obter o mesmo resultado. Logo,

$$f * A = B * k \Rightarrow f * (g * k) = (f * g) * k.$$

Sobre $I(n)$, veja que

$$(f * I)(n) = \sum_{d|n} f(d)I(\frac{n}{d}) = f(n),$$

pois $f(d)I(\frac{n}{d}) = 0$ para $d \neq n$ e $f(d)I(\frac{n}{d}) = 1$ para $d = n$.
Como já vimos que a operação é comutativa temos

$$f * I = I * f = f.$$

(c) Seja $h = f * g$ e considere m e n inteiros positivos primos entre si. Temos

$$h(mn) = \sum_{c|mn} f(c)g(\frac{mn}{c})$$

Sabemos que cada divisor c de mn pode ser escrito de maneira única como ab em que $a \mid m$, $b \mid n$, $\text{mdc}(a, b) = 1$ e $\text{mdc}(\frac{m}{a}, \frac{n}{b}) = 1$. Então o somatório pode ser considerado como

$$h(mn) = \sum_{a|m, b|n} f(ab)g(\frac{m}{a}\frac{n}{b})$$

$$h(mn) = \sum_{a|m, b|n} f(a)f(b)g(\frac{m}{a})g(\frac{n}{b})$$

$$h(mn) = \left(\sum_{a|m} f(a)g(\frac{m}{a}) \right) \left(\sum_{b|n} f(b)g(\frac{n}{b}) \right) = h(m)h(n).$$

(d) Para $n = 1$ temos $(f * f^{-1})(1) = I(1) \iff f(1)f^{-1}(1) = 1 \iff f^{-1}(1) = \frac{1}{f(1)}$.
Suponha que já determinamos os valores de f^{-1} para $k < n$. Queremos resolver a equação $(f * f^{-1})(n) = I(n)$ que é equivalente a

$$\sum d \mid n f(\frac{n}{d})f^{-1}(d) = 0$$

Separando a parcela que queremos calcular

$$f(1)f^{-1}(n) + \sum d \mid n, d < n f(\frac{n}{d})f^{-1}(d) = 0$$

Se os valores para $d < n$ já estão determinados e $f(1) \neq 0$ podemos isolar $f^{-1}(n)$ na equação

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{d|n, d<n} f(\frac{n}{d})f^{-1}(d).$$

Isso determina f^{-1} para cada n.
Já que a função foi determinada para cada valor podemos concluir que ela existe e é única.

(e) Vamos provar um resultado primeiro, se ambos g e $f * g$ são multiplicativas, então f também é multiplicativa. Suponha que f não é multiplicativa e vamos provar que $f * g$ não poderia ser. Se f não é multiplicativa, então existem m e n inteiros positivos com $\text{mdc}(m, n) = 1$ tal que

$$f(mn) \neq f(m)f(n)$$

Vamos considerar o par com o menor produto possível em que vale essa propriedade. Caso exista mais de um par, podemos tomar o que tenha o menor m.
Se $mn = 1$ então $f(1) \neq f(1)f(1)$ então $f(1) \neq 1$. Como $h(1) = f(1)g(1) = f(1) \neq 1$ e h não poderia ser multiplicativa.
Se $mn > 1$, então $f(ab) = f(a)f(b)$ para todos os a e b primos entre si com $ab < mn$. Agora, nós podemos usar as ideias do item b deste problema. Exceto no caso $a = m$ e $b = n$ que separamos.

$$h(mn) = \sum_{a|m, b|n, ab<mn} f(ab)g(\frac{mn}{ab}) + f(mn)g(1)$$

$$h(mn) = \left(\sum_{a|m} f(a)g(\frac{m}{a})\right)\left(\sum_{b|n} f(b)g(\frac{n}{b})\right) - f(m)f(n) + f(mn)$$

$$h(mn) = h(m)h(n) - f(m)f(n) + f(mn)$$

Mas se $f(mn) \neq f(m)f(n)$, então $h(mn) \neq h(m)h(n)$ e h não poderia ser multiplicativa.

A partir disso, se f e $f * f^{-1} = I$ são multiplicativas, então f^{-1} é multiplicativa.

9

FRAÇÕES CONTÍNUAS

Problema 3.1. *(A) Determine a fração contínua de $\sqrt{7}$. Mostre que ela é periódica a partir de um certo ponto, e determine o período.*

Solução

Temos $\alpha_0 = \sqrt{7}$ e $a_0 = \left\lfloor \sqrt{7} \right\rfloor = 2$. No termo seguinte $\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{\sqrt{7}+2}{3}$ que está entre 1 e 2. Isso nos leva a $a_1 = \lfloor \alpha_1 \rfloor = 1$.

Daí, $\alpha_2 = \frac{1}{\frac{\sqrt{7}+2}{3} - 1} = \frac{3}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{2}$. Novamente, o valor está entre 1 e 2 e temos $a_2 = 1$ além de $\alpha_3 = \frac{1}{\frac{\sqrt{7}+1}{2} - 1} = \frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3}$.

Como $1 < \alpha_3 < 2$ temos $a_3 = 1$ e podemos passar para o 4 onde $\alpha_4 = \frac{1}{\frac{\sqrt{7}+1}{3} - 1} = \frac{3}{\sqrt{7}-2} = \frac{3(\sqrt{7}+2)}{3} = \sqrt{7}+2$ está entre 4 e 5. Logo $a_4 = 4$ e $\alpha_5 = \frac{1}{\sqrt{7}-2} = \alpha_1$.
Portanto, $\sqrt{7} = [2; 1, 1, 1, 4, 1, 1, 1, 4, \ldots]$.

Problema 3.2. *(A) Escreva na forma $r + \sqrt{s}$, com $r, s \in \mathbb{Q}$, $s \geq 0$, os números reais cujas representações em frações contínuas são as seguintes:*

(a) $[0; 3, 6, 3, 6, 3, 6, \ldots]$.

(b) $[0; k, k, k, \ldots]$, *onde k é um inteiro positivo dado.*

(c) $[0; 1, 1, 2, 2, 1, 1, 2, 2, 1, 1, 2, 2, \ldots]$.

Solução

(a) Seja $x = [0; 3, 6, 3, 6, 3, 6, \dots]$. Veja que

$$x = \frac{1}{3 + \frac{1}{6 + \frac{1}{3 + \dots}}} = \frac{1}{3 + \frac{1}{6+x}}$$

Que nos leva a

$$x = \frac{6+x}{18+3x+1} \iff x^2 + 6x - 2 = 0$$

As raízes são $x = \frac{-6 \pm \sqrt{44}}{2} = -3 \pm \sqrt{11}$. Como o piso de x deve ser 0 a solução que dejamos é a positiva. Logo, $x = -3 + \sqrt{11}$.

(b) Seja $x = [0; k, k, k, \dots]$. Veja que $x = \frac{1}{k+x}$ e nos leva a $x^2 + kx - 1 = 0$. Tem uma solução negativa que não é nossa resposta e a outra positiva $x = \frac{-k+\sqrt{k^2+4}}{2} = \frac{-k}{2} + \sqrt{\frac{k^2+4}{4}}$.

(c) Novamente, seja $x = [0; 1, 1, 2, 2, 1, 1, 2, 2, 1, 1, 2, 2, \dots]$. Nossa equação é

$$x = \frac{1}{1 + \frac{1}{2 + \frac{1}{2+x}}}$$

Fazendo de baixo para cima, $2 + \frac{1}{2+x} = \frac{5+2x}{2+x}$, $1 + \frac{2+x}{5+2x} = \frac{7+3x}{5+2x}$, $1 + \frac{5+2x}{7+3x} = \frac{12+5x}{7+3x}$ e $x = \frac{7+3x}{12+5x}$. Essa última nos fornece a equação do segundo grau

$$12x + 5x^2 = 7 + 3x \iff 5x^2 + 9x - 7 = 0.$$

Como $x \geq 0$, temos $x = \frac{-9+\sqrt{221}}{10} = \frac{-9}{10} + \sqrt{\frac{221}{100}}$.

Problema 3.3. *(A)*

(a) Sabendo que $3,14 < x < 3,15$, determine o maior natural n e inteiros $a_0, a_1, \dots, a_n$ para os quais é possível garantir que a representação em frações contínuas de x começa por $[a_0; a_1, \dots, a_n]$.

(b) Sabendo que $3,141592 < x < 3,141593$, determine o maior natural n e inteiros $a_0, a_1, \dots, a_n$ para os quais é possível garantir que a representação em frações contínuas de x começa por $[a_0; a_1, \dots, a_n]$.

(c) Sabendo que $3,1415926 < x < 3,1415927$, determine o maior natural n e inteiros $a_0, a_1, \dots, a_n$ para os quais é possível garantir que a representação em frações contínuas de x começa por $[a_0; a_1, \dots, a_n]$.

Solução

(a) Começando por $3,14 < x < 3,15$ temos $a_0 = 3$. Daí, $0,14 < x-3 < 0,15 \iff \frac{100}{14} > \alpha_1 = \frac{1}{x-3} > \frac{100}{15}$. Mas nesse intervalo a parte inteira muda de 6 em $\frac{100}{15}$ para 7 em $\frac{100}{14}$ e a_1 tem dois valores possíveis. Logo, o maior n que podemos garantir é $n = 0$.

(b) Novamente, temos $a_0 = 3$ e $0,141592 < x-3 < 0,141593 \iff 7,06254590655 > \alpha_1 = \frac{1}{x-3} > 7,06249602735$. Nesse caso os extremos tem o mesmo piso, então $a_1 = 7$ e podemos seguir para o próximo passo usando $\alpha_1 = \frac{1}{x-3}$ e $0,06254590655 > \alpha_1 - 7 > 0,06249602735 \iff 15.9882565488 < \alpha_2 = \frac{1}{\alpha_1 - 7} < 16.001017063$. De fato, a fração contínua do extremo inferior começa com $[3;7,15,\dots]$ e o superior começa com $[3;7,16,\dots]$. Concluímos que a_2 poderia ser 15 ou 16 e o maior n que podemos garantir que as representações começam com os mesmos valores é $n = 1$.

(c) Mais uma vez, temos $a_0 = 3$ e $0,1415926 < x-3 < 0,1415927$ implicando $7,06251597894 > \alpha_1 = \frac{1}{x-3} > 7,06251099103$ e $a_1 = 7$. No próximo passo $0,06251597894 > \alpha_1 - 7 > 0,06251099103$ implicando $15,9959104369 < \alpha_2 = \frac{1}{\alpha_1 - 7} < 15.997186791$ e $a_2 = 15$. Vamos para os termos α_3 e a_3, $0,9959104369 < \alpha_2 - 15 < 0.997186791$ implicando $1,0041063563 > \alpha_3 = \frac{1}{\alpha_2 - 15} > 1,00282114547$ que nos dá $a_3 = 1$. Teremos $0,0041063563 > \alpha_3 - 1 > 0,00282114547$ nos levando a $243,524898217 < \alpha_4 = \frac{1}{\alpha_3 - 1} < 354,46594677$. Portanto, temos vários valores possíveis para o a_4. Portanto, o valor de n que podemos garantir os primeiros n valores na representação como fração contínua é $n = 3$.

Problema 3.4. *(OI)*

(a) Determine as primeiros 6 reduzidas da fração continua de $\sqrt{5}$.

(b) Definimos a sequência $a_n = n\sqrt{5} - \lfloor n\sqrt{5} \rfloor$. *Determine os valores de* $n \leq 2011$ *tais que* a_n *seja respectivamente máximo e mínimo.*

Solução

(a) Pelo item a do problema 3.5 com $a = 2$ temos $\sqrt{5} = [2;\overline{4}]$ e as seis primeiras reduzidas são $\frac{p_0}{q_0} = \frac{2}{1}$, $\frac{p_1}{q_1} = \frac{2\cdot 4+1}{4} = \frac{9}{4}$, $\frac{p_2}{q_2} = \frac{9\cdot 4+2}{4\cdot 4+1} = \frac{38}{17}$, $\frac{p_3}{q_3} = \frac{38\cdot 4+9}{17\cdot 4+4} = \frac{161}{72}$, $\frac{p_4}{q_4} = \frac{161\cdot 4+38}{72\cdot 4+17} = \frac{682}{305}$ e $\frac{p_5}{q_5} = \frac{682\cdot 4+161}{305\cdot 4+72} = \frac{2889}{1292}$.

(b) Provaremos que $n\sqrt{5} - \lfloor n\sqrt{5} \rfloor$ é mínimo para $n = 1597$ e máximo para $n = 1292$. Seguindo os passos do item anterior temos $\frac{p_6}{q_6} = \frac{12238}{5473}$. Usando as frações contínuas sabemos que $\frac{682}{305} < \sqrt{5} < \frac{2889}{1292}$. O candidato a mínimo ocorre em $n = 305$ onde temos $305\sqrt{5} - \left\lfloor 305\sqrt{5} \right\rfloor = 305\sqrt{5} - 682 < \frac{1}{305}$. Já o candidato a máximo é com

$n = 1292$ implicando $1292\sqrt{5} - \left\lfloor 1292\sqrt{5} \right\rfloor = 1292\sqrt{5} - 2888 > 1 - \frac{1}{1292}$.
Pelo Teorema 3.15 do livro texto sabemos que $0 < q < q_6 = 5473$ vale

$$|1292\sqrt{5} - 2889| = |q_5\sqrt{5} - p_5| \leq |q\sqrt{5} - p|$$

na verdade é menor, pois $\sqrt{5}$ é irracional. Então o valor máximo está provado.
Para a cota inferior, para $0 < q < q_5 = 1292$ vale

$$|305\sqrt{5} - 682| = |q_4\sqrt{5} - p_4| \leq |q\sqrt{5} - p|$$

Isso não seria suficiente para analisar até 2011. Para $1293 < q \leq 2011$ veja que

$$q\sqrt{5} - p < 305\sqrt{5} - 682 \iff (q - 305)\sqrt{5} < p - 682 \iff \sqrt{5} < \frac{p - 682}{q - 305}$$

Mas $\sqrt{5} > \frac{12238}{5473}$ e isso implica

$$\frac{p - 682}{q - 305} > \frac{12238}{5473} \iff 5473p - 682 \cdot 5473 > 12238q - 305 \cdot 12238 \iff 4 > 12238q - 5473p$$

Teria que ser 1, 2 ou 3. Note que igual a 0 daria $5473 \mid q$ e $q > 2011$.
Podemos verificar as congruências de q módulo 5473. Veja que $12238 \cdot 1292 - 5473 \cdot 2889 = -1$ implicando $12238q \equiv 1 \pmod{5473} \iff q \equiv -1292 \equiv 4181 \pmod{5473}$. Logo 1, 2 ou 3 nos dão congruências $q \equiv 4181, 2889$ ou $1597 \pmod{5473}$. Como nosso limitante é 2011, só precisamos testar $q = 1597$. Mas nesse caso, temos $12238 \cdot 1597 - 5473p = 3 \iff p = 3571$.

$$1597\sqrt{5} - 3571 = \frac{5 \cdot 1597^2 - 3571^2}{1597\sqrt{5} + 3571} = \frac{4}{1597\sqrt{5} + 3571}$$

e

$$305\sqrt{5} - 682 = \frac{5 \cdot 305^2 - 682^2}{305\sqrt{5} + 682} = \frac{1}{305\sqrt{5} + 682} = \frac{4}{1220\sqrt{5} + 2728}$$

Concluímos que $1597\sqrt{5} - 3571 < 305\sqrt{5} - 682$. Pelo que foi demonstrado $n\sqrt{5} - \lfloor n\sqrt{5} \rfloor$ é maior que ou igual a $305\sqrt{5} - 682$ para $n \neq 1597$ e menor que isso em $n = 1597$. Então o mínimo ocorre em $n = 1597$.

Problema 3.5. *(A) Demonstre que, para todo inteiro positivo a, temos as seguintes expansões em frações contínuas periódicas:*

(a) $\sqrt{a^2 + 1} = [a, \overline{2a}]$.

(b) $\sqrt{a^2 - 1} = [a - 1, \overline{1, 2a - 2}]$.

(c) $\sqrt{a^2 - 2} = [a - 1, \overline{1, a - 2, 1, 2a - 2}]$.

(d) $\sqrt{a^2-a} = [a-1, \overline{2, 2a-2}]$.

Solução

(a) Temos $\alpha_0 = \sqrt{a^2+1}$ e $a_0 = \left\lfloor \sqrt{a^2+1} \right\rfloor = a$. Daí, $\alpha_1 = \frac{1}{\sqrt{a^2+1}-a} = \sqrt{a^2+1}+a$ e $a_1 = \lfloor \alpha_1 \rfloor = 2a$. Dessa forma, $\alpha_2 = \frac{1}{\sqrt{a^2+1}+a-2a} = \frac{1}{\sqrt{a^2+1}-a} = \sqrt{a^2+1}+a = \alpha_1$. Podemos concluir α_i são todos iguais e $a_i = 2a$ para todo i positivo.

(b) Temos $\alpha_0 = \sqrt{a^2-1}$ e $a_0 = \left\lfloor \sqrt{a^2-1} \right\rfloor = a-1$. Daí, $\alpha_1 = \frac{1}{\sqrt{a^2-1}-(a-1)} = \frac{\sqrt{a^2-1}+(a-1)}{2a-2}$ e $a_1 = \lfloor \alpha_1 \rfloor = 1$. No passo seguinte, $\alpha_2 = \frac{1}{\frac{\sqrt{a^2-1}+(a-1)}{2a-2}-1} = \frac{2a-2}{\sqrt{a^2-1}-a+1} = \frac{(2a-2)(\sqrt{a^2-1}+a-1)}{2a-2} = \sqrt{a^2-1}+a-1$. Isso nos leva a $a_2 = \lfloor \alpha_2 \rfloor = 2a-2$. Observe que $\alpha_3 = \frac{1}{\sqrt{a^2-1}+a-1-(2a-2)} = \frac{1}{\sqrt{a^2-1}-(a-1)} = \alpha_1$. Então os α_i entraram em um período de tamanho 2 e podemos concluir que $a_{2k-1} = 1$ e $a_{2k} = 2a-2$ para todo k inteiro positivo.

(c) Começamos a representação por $\alpha_0 = \sqrt{a^2-2}$ e $a_0 = \left\lfloor \sqrt{a^2-2} \right\rfloor = a-1$. Daí, $\alpha_1 = \frac{1}{\sqrt{a^2-2}-(a-1)} = \frac{\sqrt{a^2-2}+(a-1)}{2a-3}$ e $a_1 = \lfloor \alpha_1 \rfloor = 1$. No passo seguinte, $\alpha_2 = \frac{1}{\frac{\sqrt{a^2-2}+(a-1)}{2a-3}-1} = \frac{2a-3}{\sqrt{a^2-2}-a+2} = \frac{(2a-3)(\sqrt{a^2-2}+a-2)}{4a-6} = \frac{\sqrt{a^2-2}+a-2}{2}$. Veja que $a-1 < \sqrt{a^2-2} < a$ implicando $\frac{2a-3}{2} < \alpha_2 < \frac{2a-2}{2} = a-1$ e $a_2 = \lfloor \alpha_2 \rfloor = a-2$. Com isso, $\alpha_3 = \frac{1}{\frac{\sqrt{a^2-2}+a-2}{2}-(a-2)} = \frac{2}{\sqrt{a^2-2}-a+2} = \frac{2(\sqrt{a^2-2}+a-2)}{4a-6} = \frac{\sqrt{a^2-2}+a-2}{2a-3}$. Pela estimativa que fizemos em α_2 temos $\frac{2a-3}{2a-3} < \alpha_3 < \frac{2a-2}{2a-3}$ e $a_3 = 1$. Para o próximo passo, $\alpha_4 = \frac{1}{\frac{\sqrt{a^2-2}+a-2}{2a-3}-1} = \frac{2a-3}{\sqrt{a^2-2}-a+1} = \frac{(2a-3)(\sqrt{a^2-2}+a-1)}{2a-3} = \sqrt{a^2-2}+a-1$. Assim, $a_4 = \lfloor \alpha_4 \rfloor = 2a-2$. Finalmente, no passo 5 teremos $\alpha_5 = \frac{1}{\sqrt{a^2-2}+a-1-(2a-2)} = \frac{1}{\sqrt{a^2-2}-(a-1)} = \alpha_1$. Temos que a sequência α_i forma um período de tamanho 4 e $a_{4k-3} = a-1$, $a_{4k-2} = a-2$, $a_{4k-1} = 1$ e $a_{4k} = 2a-2$ para todo k inteiro positivo.

(d) Novamente, começamos calculando α_i até encontrar um período. Temos $\alpha_0 = \sqrt{a^2-a}$. Veja que $a_0 = a-1$, pois $(a-1)^2 < a^2-a < a^2$. Daí, $\alpha_1 = \frac{1}{\sqrt{a^2-a}-(a-1)} = \frac{\sqrt{a^2-a}+a-1}{a-1}$. Pela estimativa feita anteriormente, $2 = \frac{a-1+a-1}{a-1} < \alpha_2 < \frac{a+a-1}{a-1} = 2+\frac{1}{a-1}$ e $a_1 = 2$. Seguindo, $\alpha_3 = \frac{1}{\frac{\sqrt{a^2-a}+a-1}{a-1}-2} = \frac{a-1}{\sqrt{a^2-a}-a+1} = \frac{(a-1)(\sqrt{a^2-a}+a-1)}{a-1} = \sqrt{a^2-a}+a-1$. Com isso, $a_2 = 2a-2$ e temos $\alpha_3 = \frac{1}{\sqrt{a^2-a}+a-1-(2a-2)} = \frac{1}{\sqrt{a^2-a}-a+1} = \alpha_1$. O período da sequência α_i é 2 e podemos concluir que $a_{2k-1} = 2$ e $a_{2k} = 2a-2$ para todo inteiro positvo k.

Problema 3.6. *(A) Encontre as frações contínuas de* $\sqrt{a^2+4}$ *e* $\sqrt{a^2-4}$.

Solução

Se $a = 1$ temos $\sqrt{1^2+4} = \sqrt{5} = [2; \overline{4}]$ e $\sqrt{1^2-4}$ não é real. Se $a = 2$ temos $\sqrt{2^2+4} =$

$\sqrt{8} = \sqrt{3^2-1} = [2;\overline{1,4}]$ e $\sqrt{2^2-4} = 0$ que é inteiro. Agora vamos considerar $a \geq 3$ e precisaremos considerar dois casos a par e a ímpar.

(i) Se a é par.

Para $\sqrt{a^2+4}$ começamos com $\alpha_0 = \sqrt{a^2+4}$ e $a_0 = \left\lfloor \sqrt{a^2+4} \right\rfloor = a$. Seguimos para os próximos termos $\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{\sqrt{a^2+4}-a} = \frac{\sqrt{a^2+4}+a}{4}$. Veja que $a_1 = \lfloor \alpha_1 \rfloor = \frac{a}{2}$ que é inteiro, pois nesse caso a é par. Daí, $\alpha_2 = \frac{1}{\frac{\sqrt{a^2+4}+a}{4} - \frac{a}{2}} = \frac{4}{\sqrt{a^2+4}-a} = \sqrt{a^2+4}+a$ e $a_2 = 2a$. Com isso, $\alpha_3 = \frac{1}{\sqrt{a^2+4}+a-2a} = \frac{1}{\sqrt{a^2+4}-a} = \alpha_1$. Então a sequência α_n tem período 2 a fração contínua é $\sqrt{a^2+4} = [a;\overline{a/2, 2a}]$.

Seguimos para $\sqrt{a^2-4}$. Se $a = 4$ temos uma exceção que pelo último item do problema anterior temos $\sqrt{4^2-4} = \sqrt{12} = [3;\overline{2,6}]$. Para $a \geq 6$. Temos $\alpha_0 = \sqrt{a^2-4}$ e $a_0 = a-1$. Segue que $\alpha_1 = \frac{1}{\sqrt{a^2-4}-a+1} = \frac{\sqrt{a^2-4}+a-1}{2a-5}$. Temos $2a-2 < \sqrt{a^2-4}+a-1 < 2a-1$ e $a_1 = 1$. Daí, $\alpha_2 = \frac{1}{\frac{\sqrt{a^2-4}+a-1}{2a-5}-1} = \frac{2a-5}{\sqrt{a^2-4}-a+4} = \frac{(2a-5)(\sqrt{a^2-4}+a-4)}{8a-20} = \frac{\sqrt{a^2-4}+a-4}{4}$. Obeserve que $\frac{2a-5}{4} < \frac{\sqrt{a^2-4}+a-4}{4} < \frac{2a-4}{4}$ e sendo a par temos $a_2 = \frac{a}{2} - 2$. No próximo passo, $\alpha_3 = \frac{1}{\frac{\sqrt{a^2-4}+a-4}{4} - (\frac{a}{2}-2)} = \frac{4}{\sqrt{a^2-4}-a+4} = \frac{4(\sqrt{a^2-4}+a-4)}{4(2a-5)} = \frac{\sqrt{a^2-4}+a-4}{2a-5}$. Pela cota já feita temos $a_3 = 1$. E no passo seguinte $\alpha_4 = \frac{1}{\frac{\sqrt{a^2-4}+a-4}{2a-5}-1} = \frac{2a-5}{\sqrt{a^2-4}-a+1} = \sqrt{a^2-4}+a-1$ e, consequentemente, $a_4 = 2a-2$. Daí, $\alpha_5 = \frac{1}{\sqrt{a^2-4}+a-1-(2a-2)} = \frac{\sqrt{a^2-4}+a-1}{2a-5}\alpha_1$. Segue que α_n tem período 4 e $\sqrt{a^2-4} = [a-1;\overline{1, \frac{a}{2}-2, 1, 2a-2}]$.

(ii) Se a é ímpar.

Para $\sqrt{a^2+4}$ começamos com $\alpha_0 = \sqrt{a^2+4}$ e $a_0 = \left\lfloor \sqrt{a^2+4} \right\rfloor = a$. Seguimos para os próximos termos $\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{\sqrt{a^2+4}-a} = \frac{\sqrt{a^2+4}+a}{4}$. Veja que $a_1 = \lfloor \alpha_1 \rfloor = \frac{a-1}{2}$ que é inteiro, pois nesse caso a é par. Daí, $\alpha_2 = \frac{1}{\frac{\sqrt{a^2+4}+a}{4} - \frac{a-1}{2}} = \frac{4}{\sqrt{a^2+4}-a+2} = \frac{4(\sqrt{a^2+4}+a-2)}{4a} = \frac{\sqrt{a^2+4}+a-2}{a}$. Note que $2a-2 < \sqrt{a^2+4}+a-2 < 2a-1$ e $a_2 = 1$. Seguindo para o próximo passo, $\alpha_3 = \frac{1}{\frac{\sqrt{a^2+4}+a-2}{a}-1} = \frac{a}{\sqrt{a^2+4}-2} = \frac{a(\sqrt{a^2+4}+2)}{a^2} = \frac{\sqrt{a^2+4}+2}{a}$. Segue que $a_3 = 1$ e podemos calcular o próximo termo $\alpha_4 = \frac{1}{\frac{\sqrt{a^2+4}+2}{a}-1} = \frac{a}{\sqrt{a^2+4}-a+2} = \frac{\sqrt{a^2+4}+a-2}{4}$. Novamente, podemos usar o fato de a ser ímpar para calcular $a_4 = \frac{a-1}{2}$. No passo seguinte, $\alpha_5 = \frac{1}{\frac{\sqrt{a^2+4}+a-2}{4} - \frac{a-1}{2}} = \frac{4}{\sqrt{a^2+4}-a} = \sqrt{a^2+4}+a$. Segue que $a_5 = 2a$ e $\alpha_6 = \frac{1}{\sqrt{a^2+4}+a-2a} = \frac{1}{\sqrt{a^2+4}-a} = \alpha_1$. Concluímos que α_n tem período 5 e $\sqrt{a^2+4} = [a;\overline{\frac{a-1}{2}, 1, 1, \frac{a-1}{2}, 2a}]$.

Para $\sqrt{a^2-4}$ se $a = 3$ temos $\sqrt{3^2-4} = \sqrt{5} = [2;\overline{4}]$ que é exceção. Para $a \geq 5$ podemos calcular os termos da fração contínua até encontrar o período. Temos

$\alpha_0 = \sqrt{a^2-4}$ e $a_0 = a-1$. Segue que $\alpha_1 = \frac{1}{\sqrt{a^2-4}-a+1} = \frac{\sqrt{a^2-4}+a-1}{2a-5}$. Temos $2a-2 < \sqrt{a^2-4}+a-1 < 2a-1$ e $a_1 = 1$. Daí, $\alpha_2 = \frac{1}{\frac{\sqrt{a^2-4}+a-1}{2a-5}-1} = \frac{2a-5}{\sqrt{a^2-4}-a+4} = \frac{(2a-5)(\sqrt{a^2-4}+a-4)}{8a-20} = \frac{\sqrt{a^2-4}+a-4}{4}$. Obeserve que $\frac{2a-5}{4} < \frac{\sqrt{a^2-4}+a-4}{4} < \frac{2a-4}{4}$ e, nesse caso, a ímpar temos $a_2 = \frac{a-3}{2}$. Seguindo o processo, $\alpha_3 = \frac{1}{\frac{\sqrt{a^2-4}+a-4}{4}-\frac{a-3}{2}} = \frac{4}{\sqrt{a^2-4}-a+2} = \frac{4(\sqrt{a^2-4}+a-2)}{4a-8} = \frac{\sqrt{a^2-4}+a-2}{a-2}$ e $a_3 = 2$. Daí, $\alpha_4 = \frac{1}{\frac{\sqrt{a^2-4}+a-2}{a-2}-2} = \frac{a-2}{\sqrt{a^2-4}-a+2} = \frac{(a-2)(\sqrt{a^2-4}+a-2)}{4a-8} = \frac{\sqrt{a^2-4}+a-2}{4}$ e $a_4 = \frac{a-3}{2}$. Seguindo para o quinto passo, $\alpha_5 = \frac{1}{\frac{\sqrt{a^2-4}+a-2}{4}-\frac{a-3}{2}} = \frac{4}{\sqrt{a^2-4}-a+4} = \frac{\sqrt{a^2-4}+a-4}{2a-5}$ e $a_5 = 1$. Fazendo mais um passo, $\alpha_6 = \frac{1}{\frac{\sqrt{a^2-4}+a-4}{2a-5}-1} = \frac{2a-5}{\sqrt{a^2-4}-a+1} = \sqrt{a^2-4}+a-1$ e $a_6 = 2a-2$. E no sétimo passo, finalmente, chegamos em $\alpha_7 = \frac{1}{\sqrt{a^2-4}+a-1-(2a-2)} = \frac{1}{\sqrt{a^2-4}-a+1} = \alpha_1$. Portanto, o período da sequência α_n é 6 e podemos escrever $\sqrt{a^2-4} = [a-1; \overline{1, \frac{a-3}{2}, 2, \frac{a-3}{2}, 1, 2a-2}]$.

Problema 3.7. *(A) Prove que, para quaisquer inteiros p, q com $q > 0$, temos $\left|\sqrt{2} - \frac{p}{q}\right| > \frac{1}{3q^2}$. Determine todos os pares de inteiros (p, q) com $q > 0$ tais que $\left|\sqrt{2} - \frac{p}{q}\right| < \frac{1}{q^3}$.*

Solução

Se $q = 1$ temos uma exceção, pois $|\sqrt{2}-1| < 1$. Para $q \geq 2$ vamos fazer dois casos. Se $\sqrt{2} + p/q > 3 > 2\sqrt{2}$ então $|\sqrt{2} - \frac{p}{q}| = \frac{p}{q} - \sqrt{2} > 3 - 2\sqrt{2} = \frac{1}{3+2\sqrt{2}} > \frac{1}{12} \geq \frac{1}{3q^2}$ para $q \geq 2$. Observe que $\sqrt{2} + p/q \neq 3$, pois $\sqrt{2}$ é irracional. Se $\sqrt{2} + p/q < 3$ veja que $|2q^2 - p^2| \geq 1$, pois é inteiro e não pode ser 0 já que $\sqrt{2}$ é irracional. Temos $|2 - \frac{p^2}{q^2}| \geq \frac{1}{q^2} \iff |\sqrt{2} - \frac{p}{q}| \cdot |\sqrt{2} + \frac{p}{q}| \geq \frac{1}{q^2} \iff |\sqrt{2} - \frac{p}{q}| \geq \frac{1}{(\sqrt{2}+p/q)q^2} > \frac{1}{3q^2}$.
Para $q = 1$ podemos tomar $\frac{1}{1}$ e $\frac{2}{1}$ tais que a diferença para $\sqrt{2}$ é menor que $\frac{1}{1^3} = 1$. Para $q \geq 2$ temos $\frac{1}{q^3} > |\sqrt{2} - \frac{p}{q}| > \frac{1}{3q^2} \Rightarrow 3q^2 > q^3 \Rightarrow 3 > q$. Então só precisamos testar $q = 2$. A distância de $\sqrt{2}$ até $\frac{2}{2}$ e $\frac{4}{2}$ são maiores que $0,2 = \frac{1}{5} > \frac{1}{2^3}$. Então só precisamos estudar a distância de $\sqrt{2}$ até $\frac{3}{2}$. Temos $\frac{3}{2} - \sqrt{2} = \frac{3-2\sqrt{2}}{2} = \frac{1}{2(3+2\sqrt{2})} < \frac{1}{8}$.
Os pares são $(1,1)$, $(2,1)$ e $(3,2)$.

Problema 3.8. *(T) Prove que, para qualquer $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, e quaisquer $s, t \in \mathbb{R}$ com $s < t$, existem inteiros m, n com $n > 0$ tais que $s < n\alpha + m < t$.*

Solução

Considere a aproximação de α com frações contínuas $\frac{p}{q}$ com $|\alpha - \frac{p}{q}| < \frac{1}{q^2} \iff \frac{p}{q} - \frac{1}{q^2} < \alpha < \frac{p}{q} + \frac{1}{q^2} \iff p - \frac{1}{q} < q\alpha < p + \frac{1}{q}$. Dessa forma, $q\alpha = p + \epsilon$ ou $q\alpha = p - \epsilon$.

Veja que se $q\alpha = p + \epsilon$ então os números $kq\alpha$ estarão em todos os intervalos de tamanho maior que $\frac{1}{q}$, pois $kq\alpha = kp + k\epsilon$ implica $kq\alpha = k\epsilon$, então $k\epsilon < 1$. Analogamente, se $q\alpha = p + \epsilon$ os números $kq\alpha$ também terão representantes em todos os intervalos de tamanho maior que $\frac{1}{q}$.

Voltando ao problema, $s < n\alpha + m < t \iff 0 < n\alpha + m - s < t - s$. Podemos fazer $n = kq$ para q suficientemente grande de modo que $s < kq\alpha < s + \frac{1}{q}$ e $\frac{1}{q} < t - s$. Já m seria $-\rfloor kq\alpha \lfloor + \rfloor s \lfloor$. Assim,

$$0 < n\alpha + m - s < \frac{1}{q} < t - s.$$

Problema 3.9. *(OI) Seja*

$$\frac{p_n}{q_n} = \cfrac{1}{1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{\ddots\, 2 + \cfrac{(2n-3)^2}{2}}}}}$$

a n-ésima convergente da fração contínua

$$\cfrac{1}{1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{\ddots}}}}}$$

Demonstre que $\frac{p_n}{q_n} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots + (-1)^{n-1}\frac{1}{2n-1}$.

Solução

Considere duas sequências de números reais a_n e b_n. Defina as sequências x_n e y_n recursivamente por $x_1 = 1$, $y_1 = a_1$, $x_2 = a_2$, $y_2 = a_1a_2 + b_1$ e $x_{n+1} = a_{n+1}x_n + b_nx_{n-1}$ e $y_{n+1} = a_{n+1}y_n + b_ny_{n-1}$. Provaremos por indução que

$$\cfrac{1}{a_1 + \cfrac{b_1}{a_2 + \ddots \cfrac{}{a_{n-1} + \cfrac{b_{n-1}}{a_n}}}} = \frac{x_n}{y_n}, \forall n \geq 1.$$

Para $n = 1$ e $n = 2$ temos $\frac{x_1}{y_1} = \frac{1}{a_1}$ e $\frac{x_2}{y_2} = \frac{1}{a_1+\frac{b_1}{a_2}} = \frac{a_2}{a_1a_2+b_1}$. Suponha que o resultado é verdade para todo inteiro positivo menor que ou igual a n com $n \geq 2$. Observe que na sequência de frações trocamos a_n por $a_n + \frac{b_n}{a_{n+1}}$ e usando o resultado para n temos

$$\frac{1}{a_1 + \dfrac{b_1}{a_2 + \ddots \\ a_n + \dfrac{b_n}{a_{n+1}}}} = \frac{(a_n + \frac{b_n}{a_{n+1}})x_{n-1} + b_{n-1}x_{n-2}}{(a_n + \frac{b_n}{a_{n+1}})y_{n-1} + b_{n-1}y_{n-2}}$$

Desenvolvendo

$$\frac{(a_n + \frac{b_n}{a_{n+1}})x_{n-1} + b_{n-1}x_{n-2}}{(a_n + \frac{b_n}{a_{n+1}})y_{n-1} + b_{n-1}y_{n-2}} = \frac{(a_nx_{n-1} + b_{n-1}x_{n-2}) + \frac{b_nx_{n-1}}{a_{n+1}}}{(a_ny_{n-1} + b_{n-1}y_{n-2}) + \frac{b_ny_{n-1}}{a_{n+1}}} = \frac{a_{n+1}x_n + b_nx_{x-1}}{a_{n+1}y_n + b_ny_{x-1}}\frac{x_{n+1}}{y_{n+1}}$$

Antes de continuar vale a pena observar que não tornamos as frações irredutíveis e dependendo das sequências a_n e b_n os números x_n e y_n podem ter fatores em comum. Podemos usar esse resultado no problema com $b_n = (2n-1)^2$ para todo inteiro positivo n, $a_1 = 1$ e $a_n = 2$ para $n \geq 2$. Provaremos por indução que $\frac{p_n}{q_n} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots + (-1)^{n-1}\frac{1}{2n-1}$. Para $n = 1$ e $n = 2$ temos $\frac{p_1}{q_1} = \frac{1}{1} = 1$ e $\frac{p_2}{q_2} = \frac{2}{3} = 1 - \frac{1}{3}$. Suponha que para todo inteiro positivo menor que ou igual a n com $n \geq 2$ temos

$$\frac{p_n}{q_n} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots + (-1)^{n-1}\frac{1}{2n-1}$$

Isso implica

$$\frac{p_n}{q_n} = \frac{p_{n-1}}{q_{n-1}} + \frac{(-1)^{n-1}}{(2n-1)}$$

Que nos leva a $q_n = (2n-1)q_{n-1}$ e $p_n = (2n-1)p_{n-1} + (-1)^{n-1}q_{n-1} \iff (2n-1)p_{n-1} = p_n + (-1)^nq_{n-1} \iff (2n-1)p_{n-1} = p_n + \frac{(-1)^nq_n}{2n-1}$.
Pelo resultado provado no começo da solução

$$\frac{p_{n+1}}{q_{n+1}} = \frac{2p_n + (2n-1)^2p_{n-1}}{2q_n + (2n-1)^2q_{n-1}} = \frac{2p_n + (2n-1)(p_n + \frac{(-1)^nq_n}{2n-1})}{2q_n + (2n-1)q_n}$$

$$\frac{p_{n+1}}{q_{n+1}} = \frac{(2n+1)p_n + (-1)^nq_n}{(2n+1)q_n} = \frac{p_n}{q_n} + \frac{(-1)^n}{2n+1}$$

Concluímos que

$$\frac{p_{n+1}}{q_{n+1}} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots + (-1)^{n-1}\frac{1}{2n-1} + (-1)^n\frac{1}{2n+1}.$$

Por indução, segue que $\frac{p_n}{q_n}$ é igual ao somatório alternado dos inversos dos n primeiros ímpares para todo n inteiro positivo.

Problema 3.10. *(T) Dizemos que dois números irracionais α e β são $GL_2(\mathbb{Z})$-equivalentes se existem inteiros a, b, c, d com $|ad - bc| = 1$ tais que $\beta = \dfrac{a\alpha + b}{c\alpha + d}$.*

Mostre que, se as frações contínuas de α e β são $\alpha = [a_0; a_1, a_2, \dots]$ e $\beta = [b_0; b_1, b_2, \dots]$ então α e β são $GL_2(\mathbb{Z})$-equivalentes se, e somente se, existem $r \in \mathbb{Z}$ e $n_0 \in \mathbb{N}$ tais que $b_n = a_{n+r}, \forall n \geq n_0$.

Solução

Suponha que existem $r \in \mathbb{Z}$ e $n_0 \in \mathbb{N}$ tais que $b_n = a_{n+r}, \forall n \geq n_0$. Então podemos escrever $\alpha = [a_0; a_1, a_2, \dots, \alpha_{n_0+r}]$ e $\beta = [b_0; b_1, b_2, \dots, \beta_{n_0}]$ e $\alpha_{n_0+r} = \beta_{n_0}$. Pela Teoria de Frações Contínuas temos

$$\alpha = \frac{\alpha_{n_0+r} p_{n_0+r-1} + p_{n_0+r-2}}{\alpha_{n_0+r} q_{n_0+r-1} + q_{n_0+r-2}} \iff \alpha_{n_0+r-2} = \frac{p_{n_0+r-2} - q_{n_0+r-2}\alpha}{q_{n_0+r-1}\alpha - p_{n_0+r-1}}$$

E, analogamente, temos

$$\beta_{n_0} = \frac{r_{n_0-2} - s_{n_0-2}\beta}{s_{n_0-1}\beta - r_{n_0-1}}$$

Temos $\alpha_{n_0+r} = \beta_{n_0}$ implicando

$$\frac{p_{n_0+r-2} - q_{n_0+r-2}\alpha}{q_{n_0+r-1}\alpha - p_{n_0+r-1}} = \frac{r_{n_0-2} - s_{n_0-2}\beta}{s_{n_0-1}\beta - r_{n_0-1}}$$

Por simplicidade, podemos escrever

$$\frac{A - B\alpha}{C\alpha - D} = \frac{E - F\beta}{G\beta - H} \iff AG\beta - BG\alpha\beta - AH + BH\alpha = CE\alpha - CF\alpha\beta - DE + DF\beta$$

E separando todas as parcelas com β temos

$$\beta(AG - DF) + \beta\alpha(CF - BG) = \alpha(CE - BH) + (AH - DE) \iff \beta = \frac{\alpha(CE - BH) + (AH - DE)}{\alpha(CF - BG) + (AG - DF)}$$

Resta verificar se $|ad - bc| = 1$ que nesse caso seria

$$|(CE - BH)(AG - DF) - (AH - DE)(CF - BG)| =$$

$$|CEAG - CEDF - BHAG + BHDF - (AHCF - AHBG - DECF + DEBG)|$$

$$= |AC - BD| \cdot |EG - HF| = 1$$

No último passo usamos que $|p_{n_0+r-2} q_{n_0+r-1} - p_{n_0+r-1} q_{n_0+r-2}| = 1$ e $|r_{n_0-2} s_{n_0-1} - r_{n_0-1} s_{n_0-2}| = 1$ pelas recorrências que geram as frações contínuas.

Para a volta, suponha que

$$\beta = \frac{a\alpha + b}{c\alpha + d}, ad - bc = \pm 1$$

Suponha de generalidade que $c\alpha + d > 0$. Podemos fazer isso, pois caso seja negativo podemos multiplicar numerador e denominador por -1. Se

$$\alpha = [a_0; a_1, \ldots, a_{k-1}, \alpha_k] = \frac{p_{k-1}\alpha_k + p_{k-2}}{q_{k-1}\alpha_k + q_{k-2}}$$

Podemos substituir essa expressão de α na equação do β e obter

$$\beta = \frac{P\alpha_k + R}{Q\alpha_k + S}$$

Onde $P = ap_{k-1} + bq_{k-1}$, $Q = ap_{k-2} + bq_{k-2}$, $R = cp_{k-1} + dq_{k-1}$ e $S = cp_{k-2} + dq_{k-2}$. Observe que

$$PS - QR = (ad - bc)(p_{k-1}q_{k-2} - p_{k-2}q_{k-1}) = \pm 1$$

Veja que podemos tomar índices k o suficientemente grande temos

$$\left|\alpha - \frac{p_{k-1}}{q_{k-1}}\right| < \frac{1}{q_{k-1}^2}, \left|\alpha - \frac{p_{k-2}}{q_{k-2}}\right| < \frac{1}{q_{k-2}^2}$$

Existem ϵ e ϵ' tais que $p_{k-1} = q_{k-1}\alpha + \frac{\epsilon}{q_{k-1}}$, $p_{k-2} = q_{k-2}\alpha + \frac{\epsilon'}{q_{k-2}}$, $|\epsilon| < 1$ e $|\epsilon'| < 1$. Isso nos leva a

$$Q = (c\alpha + d)q_{k-1} + \frac{c\epsilon}{q_{k-1}}$$

$$S = (c\alpha + d)q_{k-2} + \frac{c\epsilon'}{q_{k-2}}$$

Sabendo que $c\alpha + d > 0$, $q_{k-1} > q_{k-2}$ e $q_n \to \infty$ quando $n \to \infty$, podemos tomar k suficientemente grande de modo que $Q > S > 0$. Para esse k teremos $\beta = \frac{P\alpha_k + R}{Q\alpha_k + S}$, $PS - QR = \pm 1$ e $Q > S > 0$.

Provaremos que isso é suficiente para $\frac{R}{S}$ e $\frac{P}{Q}$ são reduzidas consecutivas de β. Veja que

$$\left|\beta - \frac{P}{Q}\right| = \left|\frac{P\alpha_k + R}{Q\alpha_k + S} - \frac{P}{Q}\right| = \left|\frac{PQ\alpha_k + QR - PQ\alpha_k - PS}{Q(Q\alpha_k + S)}\right| = \frac{1}{Q^2\alpha_k + QS}$$

Se para algum α_k suficientemente grande tivermos $\alpha_k \geq 2$ então $\left|\beta - \frac{P}{Q}\right| < \frac{1}{2Q^2}$ e pelo Teorema 3.18 temos que $\frac{P}{Q}$ é uma reduzida de β. Seja $\frac{r_w}{s_w}$ essa reduzida. Isto nos diz que $P = r_w$ e $Q = s_w$, pois as duas frações tem o mesmo valor e são irredutíveis.
Caso contrário, teremos $1 \leq \alpha_k < 2$ para todo k grande. Mas isso isso implica $\alpha_k = \frac{1+\sqrt{5}}{2}$, pois $a_n = 1$ para todo $n \geq n_0$. Veja que os denominadores das frações contínuas seguem

a recorrência $q_{m+2} = q_{m+1} + q_m$. Nesse caso, podemos resolver a recorrência e obter que $\frac{q_{k-1}}{q_{k-2}} \to \frac{1+\sqrt{5}}{2}$. Veja que

$$\frac{Q}{S} = \frac{(c\alpha + d)q_{k-1} + \frac{c\epsilon}{q_{k-1}}}{(c\alpha + d)q_{k-2} + \frac{c\epsilon'}{q_{k-2}}}$$

que para q_{k-1} e q_{k-2} suficientemente grandes é muito próximo de $\frac{1+\sqrt{5}}{2}$. Podemos aproximar S por $\frac{Q}{\frac{1+\sqrt{5}}{2}}$. Com isso, $Q^2\alpha_k + QS$ pode ser tão próximo de $Q^2(\alpha_k + \frac{1}{\alpha_k})$ quanto necessário e $\alpha_k + \frac{1}{\alpha_k} = \frac{1+\sqrt{5}}{2} + \frac{\sqrt{5}-1}{2} = \frac{2\sqrt{5}}{2} = \sqrt{5} > 2$. Então, como no caso anterior, também podemos encontrar

$$\left|\beta - \frac{P}{Q}\right| = \frac{1}{Q^2\alpha_k + QS} < \frac{1}{2Q^2}$$

Novamente, concluímos que $P = r_w$ e $Q = s_w$.
Temos mais dois casos. Se a equação está com mesmo sinal.

$$PS - QR = r_w s_{w-1} - r_{w-1}s_w \iff r_w(S - s_{w-1}) = s_w(R - r_{w-1})$$

Mas $Q = s_w \mid r_w(S - s_{w-1})$. Porém, $\text{mdc}(s_w, r_w) = 1$, $Q = s_w > S > 0$ e $s_w > s_{w-1}$ implicando $S = s_{w-1}$ e, com isso, $R = r_{w-1}$.

Vamos provar que se as expressões possuem sinais opostos chegamos em uma contradição.

$$PS - QR = -r_w s_{w-1} + r_{w-1}s_w \iff r_w(S + s_{w-1}) = s_w(R + r_{w-1})$$

Nesse caso, $s_w \mid S + s_{w-1}$ e $0 < S + s_{w-1} < 2s_w \Rightarrow S = s_w - s_{w-1}$ e $R = r_w - r_{w-1}$. Além dessa equação podemos comparar as duas expressões para β.

$$\frac{r_w\alpha_k + R}{s_w\alpha_k + S} = \frac{r_w\beta_{w+1} + r_{w-1}}{s_w\beta_{w+1} + s_{w-1}}$$

Multiplicando cruzado

$$r_w s_w \alpha_k \beta_{w+1} + r_w s_{w-1}\alpha_k + R s_w \beta_{w+1} + R s_{w-1} = r_w s_w \alpha_k \beta_{w+1} + r_{w-1} s_w \alpha_k + r_w S \beta_{w+1} + r_{w-1} S$$

$$\iff (r_w s_{w-1} - r_{w-1}s_w)\alpha_k + (Rs_w - r_w S)\beta w + 1 + (Rs_{w-1} - r_{w-1}S) = 0$$

Usando $S = s_w - s_{w-1}$ e $R = r_w - r_{w-1}$ temos

$$Rs_w - r_w S = (r_w - r_{w-1})s_w - r_w(s_w - s_{w-1}) = r_w s_{w-1} - r_{w-1}s_w$$

$$Rs_{w-1} - r_{w-1}S = (r_w - r_{w-1})s_{w-1} - r_{w-1}(s_w - s_{w-1}) = r_w s_{w-1} - r_{w-1}s_w$$

Ora, mas se todos os coeficientes são iguais e são $(-1)^m \neq 0$, então $\alpha_k + \beta_{w+1} + 1 = 0$. Note que isso é impossível, pois por construção $\alpha_k > 1$ e $\beta_{w+1} > 1$.

Concluímos que $P = r_w$, $R = r_{w-1}$, $Q = s_w$, $S = s_{w-1}$ e

$$\frac{r_w\alpha_k + r_{w-1}}{s_w\alpha_k + s_{w-1}} = \frac{r_w\beta_{w+1} + r_{w-1}}{s_w\beta_{w+1} + s_{w-1}}$$

que fazendo o produto cruzado e os cancelamentos implicam

$$(r_w s_{w-1} - r_{w-1}s_w)\alpha_k + (r_{w-1}s_w - r_w s_{w-1})\beta w + 1 = 0 \iff \alpha_k = \beta_{w+1}.$$

Portanto, as frações contínuas de α e β coincidem a partir de algum termo.

10

EQUAÇÕES DIOFANTINAS NÃO LINEARES

4.1 TEOREMA DE PITÁGORAS E TRIPLAS PITAGÓRICAS

Problema 4.1. *(A) Determine todos os triângulos retângulos com lados inteiros e um de seus catetos com comprimento igual a*

a) 60

b) 825

Solução

a) Temos que encontrar inteiros positivos b e c tais que

$$60^2 + b^2 = c^2 \iff 3600 = 2^4 \cdot 3^2 \cdot 5^2 = (c-b)(c+b)$$

Os dois números possuem a mesma paridade e precisam ser pares já que o produto é par. Temos $\frac{c-b}{2} \cdot \frac{c+b}{2} = 900$ e $c - b < c + b$. Como $d(900) = (2+1)(2+1)(2+1) = 27$ então teremos os 13 casos e soluções a seguir.
$c - b = 2$ e $c + b = 1800 \Rightarrow b = 899$ e $c = 901$
$c - b = 4$ e $c + b = 900 \Rightarrow b = 448$ e $c = 452$
$c - b = 6$ e $c + b = 600 \Rightarrow b = 297$ e $c = 303$
$c - b = 8$ e $c + b = 450 \Rightarrow b = 221$ e $c = 229$
$c - b = 10$ e $c + b = 360 \Rightarrow b = 175$ e $c = 185$
$c - b = 12$ e $c + b = 300 \Rightarrow b = 144$ e $c = 156$
$c - b = 18$ e $c + b = 200 \Rightarrow b = 91$ e $c = 109$
$c - b = 20$ e $c + b = 180 \Rightarrow b = 80$ e $c = 100$
$c - b = 24$ e $c + b = 150 \Rightarrow b = 63$ e $c = 87$

$c-b=30$ e $c+b=120 \Rightarrow b=45$ e $c=75$
$c-b=36$ e $c+b=100 \Rightarrow b=32$ e $c=68$
$c-b=40$ e $c+b=90 \Rightarrow b=25$ e $c=65$
$c-b=50$ e $c+b=72 \Rightarrow b=11$ e $c=61$

b) Temos que encontrar inteiros positivos b e c tais que

$$825^2+b^2=c^2 \iff 680625=3^2\cdot 5^4\cdot 11^2=(c-b)(c-b)$$

Os dois números possuem a mesma paridade e precisam ser ímpares já que o produto é ímpar. Como $c-b<c+b$ e $d(825^2)=(2+1)(4+1)(2+1)=45$ teremos os seguintes 22 casos e soluções.
$c-b=1$ e $c+b=680625 \Rightarrow b=340312$ e $c=340313$
$c-b=3$ e $c+b=226875 \Rightarrow b=113436$ e $c=113439$
$c-b=5$ e $c+b=136125 \Rightarrow b=68060$ e $c=68065$
$c-b=9$ e $c+b=75625 \Rightarrow b=37808$ e $c=37817$
$c-b=11$ e $c+b=61875 \Rightarrow b=30932$ e $c=30943$
$c-b=15$ e $c+b=45375 \Rightarrow b=22680$ e $c=22695$
$c-b=25$ e $c+b=27225 \Rightarrow b=13600$ e $c=13625$
$c-b=33$ e $c+b=20625 \Rightarrow b=10296$ e $c=10329$
$c-b=45$ e $c+b=15125 \Rightarrow b=7540$ e $c=7585$
$c-b=55$ e $c+b=12375 \Rightarrow b=6160$ e $c=6215$
$c-b=75$ e $c+b=9075 \Rightarrow b=4500$ e $c=4575$
$c-b=99$ e $c+b=6875 \Rightarrow b=3388$ e $c=3487$
$c-b=121$ e $c+b=5625 \Rightarrow b=2752$ e $c=2873$
$c-b=125$ e $c+b=5445 \Rightarrow b=2660$ e $c=2785$
$c-b=165$ e $c+b=4125 \Rightarrow b=1980$ e $c=2145$
$c-b=225$ e $c+b=3025 \Rightarrow b=1400$ e $c=1625$
$c-b=275$ e $c+b=2475 \Rightarrow b=1100$ e $c=1375$
$c-b=363$ e $c+b=1875 \Rightarrow b=756$ e $c=1119$
$c-b=375$ e $c+b=1815 \Rightarrow b=720$ e $c=1095$
$c-b=495$ e $c+b=1375 \Rightarrow b=440$ e $c=935$
$c-b=605$ e $c+b=1125 \Rightarrow b=260$ e $c=865$
$c-b=625$ e $c+b=1089 \Rightarrow b=232$ e $c=857$

Problema 4.2. *(A) Determine todos os triângulos retângulos com lados inteiros e hipotenusa de comprimento* 105.

Solução

Suponha que a e b são os catetos com $a < b$. Então $a^2 + b^2 = 105^2$ implicando $b^2 < 105^2 < 2b^2$ e $75 \leq b \leq 104$. Após limitar devemos testar para quais desse valores de b o número $105^2 - b^2$ é quadrado perfeito. Temos apenas uma solução $105^2 - 84^2 = 63^2 \Rightarrow (63, 84, 105)$.

Outra forma de resolver seria usar que $105 = 3 \cdot 5 \cdot 7$ como 3 e 7 são primos da forma $4k+3$ temos $3 \mid a^2 + b^2 \Rightarrow 3 \mid a$ e $3 \mid b$ e analogamente para 7. Isso permite concluir que $21 \mid a$ e $21 \mid b$ e $a^2 + b^2 = 105^2 \iff (\frac{a}{21})^2 + (\frac{b}{21})^2 = 5^2$ e é bem fácil testar que a única solução com hipotenusa 5 é com catetos 3 e 4. Considerando $a < b$ a única solução é $a = 21 \cdot 3 = 63$ e $b = 21 \cdot 4 = 84$.

Problema 4.3. *(OI)*

a) Mostre que o quadrado de um número ímpar sempre deixa resto 1 *quando dividido por* 8.

b) Existe algum triângulo retângulo com lados inteiros e catetos ímpares?

Solução

a) Seja $n = 2k+1$ um número ímpar qualquer. Veja que

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$$

Como k e $k+1$ são números consecutivos um deles é par e $2 \mid k(k+1) \Rightarrow 8 \mid 4k(k+1) \Rightarrow (2k+1)^2$ deixa restos 1 na divisão por 8.

b) Não. Suponha que exista um triângulo retângulo com catetos a e b ímpares e hipotenusa de comprimento c inteiro. Como a^2 e b^2 são ímpares c^2 é par e c tem que ser par. Se $c = 2m$ então $c^2 = 4m^2 \equiv 0$ ou $4 \pmod 8$. Por outro lado, usando o resultado do item anterior

$$c^2 = a^2 + b^2 \equiv 1 + 1 \equiv 2 \pmod 8$$

Como não existe c inteiro tal que $c^2 \equiv 2 \pmod 8$ concluímos que tal triângulo não existe.

Problema 4.4. *(OI) Observem que usando o triângulo retângulo* $(1, 1, \sqrt{2})$*, é possível construir* $\sqrt{2}$ *com régua e compasso. Mostre que para todo inteiro positivo n, o número* $\sqrt{n}$ *é construtível com régua e compasso.*

Solução

Provaremos por indução. No enunciado já temos $\sqrt{1} = 1$ e $\sqrt{2}$. Suponha que existe uma forma de construir $\sqrt{n}$. Seja AB o segmento de comprimento $\sqrt{n}$. Trace por B uma perpendicular ao segmento AB e marque C de modo que BC tenha comprimento 1. Pelo Teorema de Pitágoras no triângulo ABC temos

$$AC^2 = AB^2 + BC^2 = (\sqrt{n})^2 + 1^2 = n + 1 \Rightarrow AC = \sqrt{n+1}.$$

Detalhando essa construção com régua e compasso considerando que temos segmento de comprimento 1 como referência. Prolongue AB e com o compasso marque ponts E e F na reta AB tais que $BE = BF$. Em seguida, com o compasso trace circunferência de centros E e F e mesmo raio que é maior que BE. Ligando os dois pontos de interseção dessas circunferências temos a mediatriz de EF que é perpendicular a AB e passa em B, pois B é o ponto médio de EF. Para concluir usamos a abertura do compasso no segmento de 1 para transferir essa medida para o ponto B e um ponto dessa perpendicular chegando assim ao ponto C.

Problema 4.5. *(OI) Existe algum triângulo retângulo com lados inteiros e perímetro igual a uma potência de 2?*

Solução

Não. Vamos provar por contradição. Suponha que existe algum triângulo com tal propriedade e tome aquele com menor perímetro e em caso de empate o que possua a menor hipotenusa e o menor cateto. Seja $a < b < c$ os lados e $a + b + c = 2^k$. Veja que a e b não podem ser ambos pares, pois nesse caso c seria par e $(\frac{a}{2}, \frac{b}{2}, \frac{c}{2})$ também seriam lados inteiros de um triângulo retângulo com perímetro $2^{k-1} < 2^k$. Já vimos também no problema 4.3 que a e b não podem ser ambos ímpares, então podemos concluir que um deles é par, o outro ímpar e c ímpar. Veja que $a^2 + b^2 = c^2$ e

$$a+b = 2^k - c \iff (a+b)^2 = (2^k - c)^2 \iff a^2 + 2ab + b^2 = 2^{2k} - 2^{k+1}c + c^2 \iff 2ab = 2^{k+1}(2^{k-1} - c)$$

Isso implica que $2^{k+1} \mid 2ab \iff 2^k \mid ab \Rightarrow 2^k \mid a$ ou $2^k \mid b$, pois um deles é ímpar. Mas isso implica $2^k < a + b + c = 2^k$ que é uma contradição.

4.2 TRIÂNGULOS RETÂNGULOS DE PITÁGORAS E PLATÃO

Problema 4.6. *(A) Existem triplas pitagóricas primitivas, tais que a diferença entre a hipotenusa e um cateto seja 3, 4, 5, 6, 7 ou 8? Caso haja em algum dos casos, determine a fórmula geral delas.*

Solução

De acordo com o resultado que será provado no problema 4.7 sabemos que se r não é quadrado perfeito ímpar ou duas vezes um quadrado perfeito então não existe tripla pitagórica primitiva tal que a diferença entre a hipotenusa e um dos catetos seja r. Resta resolver apenas o caso $r = 8$. As triplas teriam que ser $(a, b, b+8)$. Vale lembrar que não sabemos qual dos catetos é maior a ou b. Temos

$$a^2 = (b+8)^2 - b^2 = 16b + 64 \Rightarrow 16 \mid a^2 \Rightarrow 4 \mid a$$

então existe um k inteiro positivo tal que $a = 4k$ e temos

$$16k^2 = 16b + 64 \iff b = k^2 - 4$$

Temos $c = b + 8 = k^2 + 4$ e k ímpar, pois a é par e $\text{mdc}(a, b) = 1$. Podemos escrever as triplas pitagóricas primitivas na forma $(a, b, c) = (4k, k^2 - 4, k^2 + 4)$ com k inteiro positivo ímpar e $k \geq 3$.

Problema 4.7. *(A) Dado r natural, encontre a família de todas as triplas pitagóricas primitivas tais que a diferença entre a hipotenusa e um cateto seja r.*

Solução

Considere a tripla $(a, b, b+r)$. Veja que essa tripla é pitagórica se, e somente se,

$$a^2 = (b+r)^2 - b^2 \iff a^2 = r(2b+r)$$

Se existe um primo p ímpar tal que seu expoente na fatoração de r é ímpar, ou seja, $p^{2k-1} \mid r$ e $p^{2k} \nmid r$. Então $p^{2k-1} \mid a^2 \Rightarrow p \mid a$. Seja α o expoente de p na fatoração de a. Temos $p^{2k-1} \mid a^2 \Rightarrow 2k - 1 \leq 2\alpha \Rightarrow k \leq \alpha$. Concluímos que $p^k \mid a$ e $p^{2k} \mid a^2 = r(2b+r) \Rightarrow p \mid 2b + r \Rightarrow p \mid b$. Porém, só nos interessa triplas pitagóricas primitivas e, nesse caso, já obtemos que a e b teriam o fator b em comum.
Se $2 \mid r$ e o expoente de 2 na fatoração de r é par. Então $2^{2k} \mid r$ com $k \geq 1$ e $2^{2k+1} \nmid r$. Podemos escrever $r = 2^{2k} r_0$ com r_0 ímpar e $a^2 = r(2b+r) = 2^{2k+1} r_0(b + 2^{2k-1} r_0) \Rightarrow 2^{2k+1} \mid a^2$ então expoente de 2 na fatoração de a^2 é pelo menos $2k+1$ e é par. Concluímos que $2^{2k+2} \mid a^2 \Rightarrow 2 \mid r_0(b + 2^{2k-1} r_0) \Rightarrow 2 \mid b$, pois r_0 ímpar e $2^{2k-1} r_0$ é par. Veja que mais uma vez chegamos que a e b não são primos entre si e não temos triplas pitagóricas primeitivas $(a, b, b+r)$.
Para os demais casos temos triplas pitágoricas primitivas.
Se r é quadrado ímpar, então $r = m^2$ e temos

$$a^2 = m^2(2b + m^2) \iff (\frac{a}{m})^2 = 2b + m^2$$

Então $2b+m^2$ tem que ser um quadrado n^2. Temos soluções $(a,b,c) = (mn, \frac{n^2-m^2}{2}, \frac{n^2+m^2}{2})$ com m e n ímpares primos entre si.
Se r é duas vezes um quadrado, então $r = 2m^2$ e temos

$$a^2 = 2m^2(2b+2m^2) \iff (\frac{a}{2m})^2 = b+m^2$$

Então $b+m^2$ tem que ser um quadrado n^2. Temos soluções $(a,b,c) = (2mn, n^2-m^2, n^2+m^2)$ com $n > m$ e m e n com paridades distintas e primos entre si.
Vale a pena é observar que nos dois casos são as mesmas triplas mudando apenas a ordem. Na primeira forma seja $M = \frac{n-m}{2}$ e $N = \frac{n+m}{2}$. Temos $mn = (N+M)(N-M) = N^2-M^2$, $\frac{n^2-m^2}{2} = 2NM$ e $\frac{n^2+m^2}{2} = N^2+M^2$. A condição de n e m ímpares primos entre si se torna N e M inteiros positivos primos entre si com paridades distintas, pois $N+M = n$ e $N-M = m$ são ímpares que não possuem fatores em comum.

Problema 4.8. *(A) Encontre todas as triplas pitagóricas tais que os lados estão em progressão aritmética.*

Solução

Suponha que (a,b,c) é uma tripla pitagórica em progressão aritmética. Temos $a+c = 2b$ e pelo Teorema de Pitágoras.

$$b^2 = c^2-a^2 = (c+a)(c-a) \iff b = 2(c-a) \iff \frac{a+c}{2} = 2(c-a) \iff a+c = 4c-4a \iff 5a = 3c$$

Como $5 \mid 3c$ e $\text{mdc}(5,3) = 1$ temos $5 \mid c$ e $c = 5k$ para algum inteiro positivo k. Substituindo nas equações anteriores $a = 3k$ e $b = \frac{3k+5k}{2} = 4k$. As triplas pitagóricas em progressão geométrica são $(a,b,c) = (3k, 4k, 5k)$ para algum inteiro positivo k.

4.3 TRIPLAS PITAGÓRICAS PRIMITIVAS

Problema 4.9. *(A) Determine todas as soluções inteiras da equação $2x^2+y^2 = z^2$.*

Solução

Faremos o caso em que $\text{mdc}(y,z) = 1$. Veja que se y e z possuem um divisor primo ímpar em comum então $p \mid 2x^2 \Rightarrow p \mid x$ e $(\frac{x}{p}, \frac{y}{p}, \frac{z}{p})$ também seria solução. Se $2 \mid y$ e $2 \mid z$ então $2^2 \mid z^2-y^2 = 2x^2 \Rightarrow 2 \mid x$ e $(\frac{x}{2}, \frac{y}{2}, \frac{z}{2})$ também seria solução da equação.
Se x é ímpar $y^2+2 \equiv z^2 \pmod 8$, mas $y^2 \equiv 0, 1$ ou $4 \pmod 8$ implica $y^2+2 \equiv 2, 3$ ou $6 \pmod 8$ e nenhum é quadrado. Logo x é par e como y e z são primos entre si com y^2-z^2

par podemos afirmar que são ímpares. Temos $x = 2x_0$ e $2x^2 = z^2 - y^2 \iff 8x_0^2 = (z-y)(z+y)$. Temos $2x_0^2 = \frac{z-y}{2} \cdot \frac{z+y}{2}$. De $\frac{z-y}{2} + \frac{z+y}{2} = z$, $\frac{z+y}{2} - \frac{z-y}{2} = y$ e $\text{mdc}(y,z) = 1$ podemos concluir que $\frac{z-y}{2}$ e $\frac{z+y}{2}$ são dois números primos entre si de paridades distintas. Se $\frac{z-y}{2}$ é par, então $x_0^2 = \frac{z-y}{4} \cdot \frac{z+y}{2}$ e podemos conluir que existem quandos perfeitos primos entre m^2 e n^2 tais que $\frac{z-y}{4} = m^2$ e $\frac{z+y}{2} = n^2$. Que nos dá o conjunto de soluções $(x,y,z) = (2mn, n^2 - 2m^2, n^2 + 2m^2)$ com $n^2 > 2m^2$.
Se $\frac{z+y}{2}$ é par, então, seguindo a mesma ideia do caso anterior, $x_0^2 = \frac{z-y}{2} \cdot \frac{z+y}{4}$ e podemos conluir que existem quandos perfeitos primos entre m^2 e n^2 tais que $\frac{z-y}{2} = m^2$ e $\frac{z+y}{4} = n^2$. Que nos dá o conjunto de soluções $(x,y,z) = (2mn, 2n^2 - m^2, 2n^2 + m^2)$ com $2n^2 > m^2$.

Problema 4.10. *(OI) Existe algum triângulo retângulo com lados inteiros e perímetro $2p^k$ com p um número primo e k inteiro?*

Solução

Não. Provaremos por contradição. Suponha que existe um triângulo retângulo com lados inteiros e perímetro $2p^k$. Usando a fórmula para triplas pitagóricas $(a,b,c) = (d(2uv), d(u^2 - v^2), d(u^2 + v^2))$, com $u > v > 0$ e d inteiro positivo. Se o perímetro é $2p^k$ então $a + b + c = 2p^k \iff 2duv + 2du^2 = 2p^k \iff du(u+v) = p^k$. Como p é primo, temos $d = p^x$, $u = p^y$ e $u + v = p^z$ para inteiros não negativos x, y e z tais que $x + y + z = k$. Veja que $u + v > u \iff p^z > p^y \iff z > y \iff z - y > 0$. Mas isso implica que $v \geq p^y(2-1) = p^y = u$ e $u^2 - v^2 \leq 0$. Isso gera contradição, pois cada lado teria que ser inteiro positivo.

Problema 4.11. *(A) Determine todos os triângulos retângulos com lados inteiros e perímetro* 120.

Solução

Usando a fórmula para triplas pitagóricas $(a,b,c) = (d(2uv), d(u^2 - v^2), d(u^2 + v^2))$, com $u > v > 0$, d inteiro positivo e a tripla $(2uv, u^2 - v^2, u^2 + v^2)$ é uma tripla pitagórica primitiva. Pelo perímetro

$$a + b + c = 120 \iff 2du(u+v) = 120 \iff du(u+v) = 60 \Rightarrow u(u+v) \mid 60$$

Então precisamos de dois divisores de 60 para ser u e $u + v$ lembrando que $u < u + v < 2u$. Veja que $u^2 < du(u+v) = 60 \Rightarrow u < 8$. Os divisores de 60 até 7 são 1, 2, 3, 4, 5 e 6. Se $u = 1$ não tem outro divisor menor que $2 \cdot 1 = 2$. Se $u = 2$ temos $2 < u + v < 4 \Rightarrow u + v = 3$. Com $u = 2$ e $v = 1$ temos a tripla $(4,3,5)$ que com $d = 10$ nos dá a solução $(40,30,50)$. Se $u = 3$, então $u + v = 4 \iff v = 1$ ou $u + v = 5 \iff v = 2$.

Se $v = 1$ então a tripla com u e v não é primitiva já que todos os termos seriam pares. Se $v = 2$ temos a tripla $(12, 5, 13)$ que com $d = 4$ fornece a solução $(48, 20, 52)$. Se $u = 4$ temos $u + v = 5 \iff v = 1$ ou $u + v = 6 \iff v = 2$. Se $v = 1$ temos a tripla $(15, 8, 17)$ que juntamente com $d = 3$ gera a solução $(45, 24, 51)$. Se $v = 2$ os três números são pares e a tripla não com u e v é primitiva. Se $u = 5$, então $u + v = 6$, pois é o único divisor de $\frac{60}{5} = 12$ menor que 10. Mas com $u = 5$ e $v = 1$ a tripla com u e v não é primitiva. Se $u = 6$ então $u + v = 10$ é o único divisor de $\frac{60}{6} = 10$ menor que 12. Mas, mais uma vez, com $u = 6$ e $v = 4$ a tripla com u e v não é primitiva.
Concluímos que os triângulos retângulos de perímetro 120 possuem lados $(40, 30, 50)$, $(48, 20, 52)$ ou $(45, 24, 51)$.

4.4 TRIÂNGULOS PITAGÓRICOS E O MÉTODO GEOMÉTRICO

Problema 4.12. *(A) Determine todas as soluções inteiras da equação* $a^2 + 3b^2 = 13c^2$.

Solução

Dividindo por c^2 temos $\left(\frac{a}{c}\right)^2 + 3\left(\frac{b}{c}\right)^2 = 13$ e queremos soluções racionais da equação de elipse $x^2 + 3y^2 = 13$. Podemos usar a solução $(-1, -2)$ para achar as outras soluções. Seja $\frac{m}{n}$ a inclinação da reta que passa por $\left(\frac{a}{c}, \frac{b}{c}\right)$ e $(-1, -2)$. A reta é $y - (-2) = \frac{m}{n}(x - (-1)) \iff y = \frac{m}{n}x + \frac{m-2n}{n}$. Temos que resolver o sistema

$$\begin{cases} x^2 + 3y^2 = 13 \\ y = \frac{m}{n}x + \frac{m-2n}{n}, \end{cases}$$

Substituindo

$$13 = x^2 + 3\left(\frac{m}{n}x + \frac{m-2n}{n}\right)^2$$

$$\iff 0 = \left(\frac{n^2+3m^2}{n^2}\right)x^2 + 6\left(\frac{m(m-2n)}{n^2}\right)x + \left(\frac{3m^2-12mn-n^2}{n^2}\right)$$

$$\iff x^2 + 6\left(\frac{m(m-2n)}{n^2+3m^2}\right)x + \left(\frac{3m^2-12mn-n^2}{n^2+3m^2}\right) = 0$$

Como um dos pontos é $(-1, -2)$ temos uma solução $x_1 = -1$ e a outra pode ser encontrada por soma e produto das raízes

$$\frac{a}{c} = x_2 = \frac{n^2 + 12mn - 3m^2}{n^2 + 3m^2}$$

E com isso podemos achar o $y = \frac{b}{c}$ correspondente

$$\frac{b}{c} = \frac{m}{n}\left(\frac{n^2+12mn-3m^2}{n^2+3m^2}\right) + \frac{m-2n}{n} = \frac{6m^2+2mn-2n^2}{n^2+3m^2}$$

Podemos concluir que as soluções são da forma

$$a = \frac{k}{d}(n^2 + 12mn - 3m^2), \quad b = \frac{k}{d}(6m^2 + 2mn - 2n^2) \quad \text{e} \quad c = \frac{k}{d}(n^2 + 3m^2)$$

Onde $d = \text{mdc}(n^2 + 12mn - 3m^2, 6m^2 + 2mn - 2n^2, n^2 + 3m^2)$.

Problema 4.13. *(OI) Mostre que a equação $x^2 + y^2 = 6z^2$ não possui soluções inteiras positivas.*

Dica: Mostre que o quadrado de todo ímpar deixa resto 1 quando dividido por 8, assim os quadrados quando divididos por 8 somente podem deixar resto 0, 1 ou 4.

Solução

Provaremos por contradição. Suponha que a equação possui solução e considere a solução (x, y, z) que possui o menor z possível. Casa exista mais de uma tripla com esse z mínimo tome qualquer uma delas.

Veja que qualquer inteiro n é congruente a 0, 1 ou 2 módulo 3 e $n^2 \equiv 0^2, 1^2$ ou $2^2 \pmod 3$ implicando $n^2 \equiv 0$ ou $1 \pmod 3$. Logo, se $x^2 + y^2 = 6z^2$ então $3 \mid x^2 + y^2 \Rightarrow 3 \mid x$ e $3 \mid y$ e existem x_0 e y_0 tais que $x = 3x_0$ e $y = 3y_0$. Porém, $x^2 + y^2 = 6z^2 \iff 9x_0^2 + 9y_0^2 = 6z^2 \iff 3(x_0^2 + y_0^2) = 2z^2 \Rightarrow 3 \mid 2z^2 \Rightarrow 3 \mid z$ e existe um inteiro positivo z_0 tal que $z = 3z_0$, mas com isso

$$x^2 + y^2 = 6z^2 \Rightarrow x_0^2 + y_0^2 = 6z_0^2$$

Porém, essa solução (x_0, y_0, z_0) possui um z menor que o mínimo possível e isso gera contradição.

Portanto não existem soluções inteiras positivas.

Problema 4.14. *(OI) Demonstre que a equação $x^2 + y^2 = 3z^2$ não tem soluções inteiras positivas.*

Solução

Como no problema anterior podemos supor que tem solução e tomar a solução com o menor z possível (x, y, z). Isso implicaria que $(x_0, y_0, z_0) = (\frac{x}{3}, \frac{y}{3}, \frac{z}{3})$ também seria solução com $z_0 = \frac{z}{3} < z$ gerando contradição.

Concluímos que não tem soluções inteiras positivas.

Problema 4.15. *(A) Encontre todas as soluções inteiras da equação $x^2 + y^2 = 5z^2$.*

Solução

Pelo método geométrico temos

$$x^2 + y^2 = 5z^2 \iff \left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 5$$

Queremos pontos racionais na circunferência $x^2 + y^2 = 5$. Temos o ponto $(-1, -2)$ e podemos tomar a reta de inclinação $\frac{m}{n}$ que passa por $(-1, -2)$ e $(\frac{x}{z}, \frac{y}{z})$. Temos $y - (-2) = \frac{m}{n}(x - (-1)) \iff y = \frac{m}{n}x + \frac{m-2n}{n}$.
Precisamos resolver o seguinte sistema de equações

$$\begin{cases} x^2 + y^2 = 5 \\ y = \frac{m}{n}x + \frac{m-2n}{n}, \end{cases}$$

Substituindo o y temos

$$x^2 + \left(\frac{m}{n}x + \frac{m-2n}{n}\right)^2 = 5$$

$$\iff \left(\frac{m^2+n^2}{n^2}\right)x^2 + \left(\frac{2m(m-2n)}{n^2}\right)x + \frac{m^2-4mn-n^2}{n^2} = 0$$

$$\iff x^2 + \left(\frac{2m(m-2n)}{m^2+n^2}\right)x + \frac{m^2-4mn-n^2}{m^2+n^2} = 0$$

Uma das soluções é $x_1 = -1$ e a outra pode ser encontrada por soma e produto das raízes.

$$\frac{x}{z} = x_2 = \frac{n^2+4mn-m^2}{m^2+n^2}$$

Substituindo na equação da reta podemos encontrar $y_2 = \frac{y}{z}$ correspondente.

$$\frac{y}{z} = y_2 = \frac{m}{n}\left(\frac{n^2+4mn-m^2}{m^2+n^2}\right) + \frac{m-2n}{n}$$

$$\frac{y}{z} = \frac{2m^2+2mn-2n^2}{m^2+n^2}$$

As soluções são

$$x = \frac{k}{d}(n^2+4mn-m^2), \quad y = \frac{k}{d}(2m^2+2mn-2n^2) \quad \text{e} \quad z = \frac{k}{d}(m^2+n^2)$$

Onde $d = \text{mdc}(n^2+4mn-m^2, 2m^2+2mn-2n^2, m^2+n^2)$.

Problema 4.16. *(A) Um bloco retangular é chamado Bloco de Euler se o comprimento de seus lados é inteiro e o comprimento das diagonais em cada face é inteira. Um bloco de Euler é chamado primitivo se o mdc dos comprimentos dos lados é 1. Mostre que um bloco com medidas* 44*,* 117 *e* 240 *é um bloco de Euler.*

Solução

Seja a, b e c os comprimentos das arestas do bloco. Pelo Teorema de Pitágoras em cada face as diagonais medem $\sqrt{a^2+b^2}$, $\sqrt{b^2+c^2}$ e $\sqrt{a^2+c^2}$. É um Bloco de Euler se, e somente se, esses três valores são inteiros positivos.
Para $(a,b,c) = (44,117,240)$ temos

$$\sqrt{44^2+117^2} = 125, \quad \sqrt{117^2+240^2} = 267 \quad \text{e} \quad \sqrt{44^2+240^2} = 244.$$

Portanto, esse um bloco com essas medidas é um Bloco de Euler.

Problema 4.17. *(A) Mostre que se um bloco com medidas a, b e c é de Euler, então um bloco com medidas* (bc, ab, ac) *é de Euler.*

Solução

Veja que

$$\sqrt{(bc)^2+(ab)^2} = b\sqrt{c^2+a^2},$$
$$\sqrt{(ab)^2+(ac)^2} = a\sqrt{b^2+c^2},$$
$$\sqrt{(bc)^2+(ac)^2} = c\sqrt{b^2+a^2}.$$

Se (a,b,c) é um Bloco de Euler, então $\sqrt{c^2+a^2}$, $\sqrt{b^2+c^2}$ e $\sqrt{b^2+a^2}$ são inteiros positivos. Se esses três valores são inteiros positivos, então os três valores calculados acima também são e o bloco retangular com medidas (bc, ab, ca) também é um Bloco de Euler.

Problema 4.18. *(A) Encontre um bloco de Euler cuja aresta de menor comprimento é* 85*.*

Solução

Considere as arestas com medidas 85, 132 e 720. Veja que

$$\sqrt{85^2+132^2} = 157, \quad \sqrt{132^2+720^2} = 732 \quad \text{e} \quad \sqrt{85^2+720^2} = 725.$$

Como todas as diagonais do bloco de arestas $(85,132,720)$ são inteiros podemos concluir que esse é um Bloco de Euler.

Problema 4.19. *(A) Mostre que existem infinitos blocos de Euler primitivos .*

Obs.: É um problema aberto a existência de um bloco de Euler com diagonal inteira.

Solução

Uma forma de gerar infinitos Blocos de Euler é a partir de uma tripla pitagórica primitiva (x, y, z), com $x^2 + y^2 = z^2$, gerar a tripla (a, b, c) com

$$a = x|4y^2 - z^2|, \quad b = y|4x^2 - z^2| \quad \text{e} \quad c = 4xyz.$$

Veja que

$$a^2 + b^2 = x^2(16y^4 - 8y^2z^2 + z^4) + y^2(16x^4 - 8x^2z^2 + z^4) = z^6 = (z^3)^2,$$

$$a^2 + c^2 = x^2(16y^4 - 8y^2z^2 + z^4) + 16x^2y^2z^2 = x^2(16y^4 + 8y^2z^2 + z^4) = (x(4y + z))^2,$$

$$b^2 + c^2 = y^2(16x^4 - 8x^2z^2 + z^4) + 16x^2y^2z^2 = y^2(16x^4 + 8x^2z^2 + z^4) = (y(4x + z))^2.$$

Vamos provar que esse bloco é primitivo. Suponha que existe um fator primo p que divide a, b e c. Como $p \mid c$ temos $p \mid 4$, $p \mid x$, $p \mid y$ ou $p \mid z$.

Se $p \mid 4$ então $p = 2$. Porém na tripla pitagórica primitiva dois termos são ímpares e um é par. Suponha sem perda de generalidade que x é par e y e z são ímpares. Daí $b = y|4x^2 - z^2|$ é ímpar e $2 \nmid b$. Veja que de modo geral fica provado que 2 não divide pelo menos um dos termos.

Se $p \mid x$ então de $p \mid 4yx^2$ e $p \mid b$ temos $p \mid yz^2 \Rightarrow p \mid y$ ou $p \mid z$. Mas isso é uma contradição, pois $\text{mdc}(x, y) = \text{mdc}(x, z) = 1$.

Se $p \mid y$ é análogo ao caso anterior.

Se $p \mid z$ então de $p \mid xz^2$ e $p \mid a$ temos $p \mid 4xy^2$. Já vimos que 2 não divide os três termos. Resta $p \mid xy^2$ implicando $p \mid x$ ou $p \mid y$. Isso novamente é uma contradição, pois $\text{mdc}(z, x) = \text{mdc}(z, y) = 1$.

Logo não existe fator primo comum aos três números e $\text{mdc}(a, b, c) = 1$. Como existem infinitas triplas pitagóricas primitivas, existem infinitos Blocos de Euler primitivos.

4.5 TRIÂNGULOS COM LADOS INTEIROS E ÂNGULOS EM PROGRESSÃO ARITMÉTICA

Problema 4.20. *(A) Mostre que não existem triângulos com lados inteiros de tal forma que um de seus ângulos seja* $30°$*,* $45°$ *ou* $72°$.

Solução

Veja que se θ é um ângulo de um triângulo com coordenadas inteiras então $\cos\theta$ é racional, pois se os lados são a, b e c com c oposto a θ por Lei dos Cossenos temos

$$\cos\theta = \frac{a^2 + b^2 - c^2}{2ab}$$

Sabe-se que $\cos 30^\circ = \frac{\sqrt{3}}{2}$, $\cos 45^\circ = \frac{\sqrt{2}}{2}$ e $\cos 72^\circ = \frac{\sqrt{5}-1}{4}$ são todos irracionais e, portanto, não existem triângulos com lados inteiros formando algum desses ângulos.

Problema 4.21. *(A) Encontre todos os triângulos com lados inteiros e com um ângulo α tal que* $\cos\alpha = \frac{2}{5}$.

Solução

Desejamos encontrar triplas de inteiros positivos (a,b,c) que satisfazem

$$c^2 = a^2 + b^2 - 2ab\cos\alpha = a^2 + b^2 - \frac{4ab}{5}$$

Veja que dessa igualdade já vale a desigualdade triangular, pois $c^2 = a^2 + b^2 - \frac{4ab}{5}$ implica $(a-b)^2 < c^2 < (a+b)^2 \iff |a-b| < c < a+b$.
Sendo $(x,y) = \left(\frac{a}{c}, \frac{b}{c}\right)$ desejamos encontrar as soluções racionais de

$$1 = x^2 + y^2 - \frac{4xy}{5}$$

Usando o método geométrico de resolução podemos tomar a reta de inclinação que passa pelo ponto $(0,-1)$ e possui inclinação $\frac{m}{n}$. Podemos substituir a equação da reta $y = \frac{m}{n}x - 1$ na equação de grau 2.

$$\begin{aligned} 1 &= x^2 + \left(\frac{m}{n}x - 1\right)^2 - \frac{4x(\frac{m}{n}x-1)}{5} \\ \iff 0 &= \left(1 + \frac{m^2}{n^2} - \frac{4m}{5n}\right)x^2 + \left(\frac{-2m}{n} + \frac{4}{5}\right)x \\ \iff 0 &= (5n^2 + 5m^2 - 4mn)x^2 + (n(-10m+4n))x \end{aligned}$$

Estamos interessados na solução $x \neq 0$ que é a razão $\frac{a}{c}$ procurada

$$x = \frac{a}{c} = \frac{10mn - 4n^2}{5n^2 + 5m^2 - 4mn}$$

E substituindo na equação da reta

$$y = \frac{b}{c} = \frac{10m^2 - 4mn}{5n^2 + 5m^2 - 4mn} - 1 = \frac{5(m^2 - n^2)}{5n^2 + 5m^2 - 4mn}$$

Concluímos que os lados de triângulos com lados inteiros e ângulo α são

$$a = 2kn(5m - 2n), \quad b = 5k(m^2 - n^2) \quad \text{e} \quad c = k(5n^2 + 5m^2 - 4mn),$$

com k inteiro positivo e $m > n$, ou

$$a = 2kn(2n - 5m), \quad b = 5k(n^2 - m^2) \quad \text{e} \quad c = k(5n^2 + 5m^2 - 4mn),$$

com k inteiro positivo e $n > \frac{5m}{2}$.

Problema 4.22. *(OI) Seja $0 < \alpha < 180^\circ$, tal que $\cos\alpha$ é um número racional. Mostre que existem infinitos triângulos não semelhantes e com lados inteiros tais que um de seus ângulos mede α.*

Solução

Seja $\cos\alpha = \frac{p}{q}$ com $q > 0$, p inteiro e $\text{mdc}(p,q) = 1$. Temos que resolver a equação diofantina

$$c^2 = a^2 + b^2 - \frac{2pab}{q}$$

Veja que a desigualdade triangular segue dessa equação, pois $-1 < \cos\alpha = \frac{p}{q} < 1$ e temos $(a-b)^2 < c^2 < (a+b)^2 \iff |a-b| < c < a+b$.

Usando o método geométrico de resolução podemos considerar a reta com inclinação $\frac{m}{n}$ que corta a curva de equação $1 = x^2 + y^2 - \frac{2pxy}{q}$ nos pontos $(0,-1)$ e $\left(\frac{a}{c}, \frac{b}{c}\right)$. Podemos escrever a reta como $y = \frac{m}{n}x - 1$ e substituir na equação da curva

$$1 = x^2 + (\frac{m}{n}x - 1)^2 - \frac{2px(\frac{m}{n}x - 1)}{q}$$

$$\iff 0 = (1 + \frac{m^2}{n^2} + \frac{2pm}{qn})x^2 + (\frac{-2m}{n} + \frac{2p}{q})x$$

$$\iff 0 = (\frac{qn^2 + qm^2 - 2pmn}{qn^2})x^2 + (\frac{n(-2qm + 2pn)}{qn^2})x$$

Queremos a solução $x = \frac{a}{c} \neq 0$ e temos

$$x = \frac{a}{c} = \frac{n(2qm - 2pn)}{qn^2 + qm^2 - 2pmn}$$

E podemos determinar o y correspondente usando a equação da reta

$$y = \frac{m}{n}\frac{n(2qm - 2pn)}{qn^2 + qm^2 - 2pmn} - 1 = \frac{q(m^2 - n^2)}{qn^2 + qm^2 - 2pmn}$$

Então podemos gerar infinitas soluções (a,b,c) para lados de triângulos não semelhantes com

$$a = n(2qm - 2pn),$$

$$b = q(m^2 - n^2),$$

e

$$c = qn^2 + qm^2 - 2pmn,$$

com $m > n$.

Para provar que existem infinitos não semelhantes entre si podemos observar todos gerados por $n = 1$. Veja que

$$\frac{a}{b} = \frac{a'}{b'} \iff \frac{qm - p}{m^2 - 1} = \frac{qm' - p}{(m')^2 - 1}$$

Multiplicando cruzado é equivalente a

$$qm(m')^2 - qm - p(m')^2 = qm^2m' - qm' - pm^2 \iff (m-m')(qmm' + q - p(m+m')) = 0$$

Para m e m' suficientemente grandes $qmm' + q - p(m+m') > 0$ e $m = m'$.

4.6 OUTRA RELAÇÃO DE ÂNGULOS

Problema 4.23. *(A) Determine todos os triângulos $\triangle ABC$ com lados inteiros, $\angle A = 2\angle B$ e $c = 40$.*

Solução

Pelo resultado do problema 4.24 a seguir o número de triplas é

$$\frac{d((\frac{40}{4})^2) - 1}{2} = \frac{d(100) - 1}{2} = \frac{(2+1)(2+1) - 1}{2} = 4$$

Elas vem de considerar $s \mid 40$ com s livre de quadrados. Os possíveis s são $s = 1$, 2, 5 ou 10. Faremos os casos.

1. Se $s = 1$ então $\frac{40}{s} = 40$ e temos $(t-k, t+k) = (2, 20)$ ou $(4, 10)$ que implica $(t, k) = (11, 9)$ ou $(7, 3)$.
2. Se $s = 2$ então $\frac{40}{s} = 20$ e temos $(t-k, t+k) = (2, 10)$ que implica $(t, k) = (6, 4)$.
3. Se $s = 5$ então $\frac{40}{s} = 8$ e temos $(t-k, t+k) = (2, 4)$ que implica $(t, k) = (3, 1)$.
4. Se $s = 10$ então $\frac{40}{s} = 4$ sendo os dois pares seriam $(t-k, t+k) = (2, 2)$ que dá $k = 0$ e não gera triângulo.

As triplas são $(a, b, c) = (skt, k^2s, (t^2 - k^2)s)$ e substituindo as triplas são

$$(99, 81, 40), (21, 9, 40), (48, 32, 40) \text{ e } (15, 5, 40).$$

Pela desigualdade triangular, apenas $(99, 81, 40)$ e $(48, 32, 40)$ são lados possíveis de um triângulo.

Problema 4.24. *(A) Encontre uma fórmula para o número de triângulos $\triangle ABC$ com lados inteiros, $\angle A = 2\angle B$ e lado c um inteiro dado (esta fórmula deve depender do número de divisores de c).*

Solução

Traçamos a bissetriz AD do ângulo $\angle BAC$ com D sobre BC. Temos $\frac{\angle A}{2} = \angle DAB = \angle DBA = \angle B$. Isso implica que $DA = DB$ e $\angle CDA = \angle DAB + \angle DBA = 2\angle B$. Esta última nos leva à semelhança de triângulos entre ΔCDA e ΔCAB. Se $AD = DB = x$ temos $CD = a - x$ e $\frac{x}{c} = \frac{b}{a} = \frac{a-x}{b}$. Temos $x = \frac{bc}{a}$ e $\frac{b}{a} = \frac{a-\frac{bc}{a}}{b} \iff b^2 = a^2 - bc \iff a^2 = b(b+c)$.

Veja que para qualquer número inteiro positivo podemos escrever n de maneira única como $k^2 s$ com s livre de quadrados. Para $n = 1$ temos $1 = 1^2 \cdot 1$ e para $n \geq 2$ o número s é produtos dos fatores primos de n com expoente ímpar. Qualquer outro s implicaria que s não é livre de quadrados ou que $\frac{n}{s}$ não é quadrado perfeito. Assim, podemos escrever $b = k^2 s$ e $b + c = t^2 s$, pois caso contrário $b(b+c)$ não seria quadrado perfeito. Daí temos que resolver $c = s(t^2 - k^2) = s(t-k)(t+k)$.

Faremos dois casos

(i) Se c é ímpar. Considere a fatoração em primos $c = p_1^{x_1} p_2^{x_2} \dots p_m^{x_m}$. Como s é o produto de alguns primos de c existem 2^m valores possíveis para s. Vamos olhar para formas de fatorar $\frac{c}{s}$ como produto de números $t - k < t + k$ de mesma paridade. Se $\frac{c}{s}$ não quadrado isso é $\frac{d(\frac{c}{s})}{2}$, pois é possível fazer parzinhos ordenados de números ímpares com todos os divisores de $\frac{c}{s}$ com produto $\frac{c}{s}$. O número $\frac{c}{s}$ é um quadrado para um valor de s, exatamente o produto dos fatores primos com expoente ímpar na fatoração de c, e nesse caso temos $\frac{d(\frac{c}{s})-1}{2}$. Portanto, o número de soluções é $-1 + \sum_{s|c, k^2 \nmid s} \frac{d(\frac{c}{s})}{2}$. Se $p_1 \mid s$ a contribuição de x_1 nos somatórios será $x_1 - 1 + 1 = x_1$ e se $p_1 \nmid s$ então será $x_1 + 1$. Variando sobre todas as somas teremos $x_1 S_1 + (x_1 + 1) S_1 = (2x_1 + 1) S_1$. O número de soluções é $\frac{(2x_1+1)(2x_2+1)\dots(2x_m+1)-1}{2} = \frac{d(c^2)-1}{2}$.

(ii) Se c é par. O processo é muito similar, mas devemos adicionar o fato de $t - k$ e $t + k$ terem a mesma paridade. Isso significa que ou ambos d e $\frac{c/s}{d}$ possuem fator 2 ou nenhum deles. Se $c = 2c_0$ com c_0 ímpar, então obrigatoriamente $2 \mid s$ e temos a solução para c_0: $\frac{d(c_0^2)-1}{2} = \frac{d((\frac{c}{2})^2)-1}{2}$. Se $c = 2^2 c_0$ então s não pode tomar os dois fatores 2 então precisamos colocá-los em $t - k$ e $t + k$ e novamente o número de solução é o mesmo da parte ímpar c_0: $\frac{d(c_0^2)-1}{2}$. Se $c = 2^k c_0$ com c_0 ímpar e $k \geq 3$. Quando $2 \nmid s$ temos $k - 1$ maneiras de escolher os fatores 2 a saber α fatores 2 no d com $\alpha = 1, 2, \dots, k-1$. Se $2 \mid s$ então temos $k - 2$ maneiras de escolher os fatores 2. Então nesse caso a contribuição de 2^k será $k - 1$ ou $k - 2$ e no somatório $2k - 1$. Tomando a fatoração em primos $c = 2^k p_1^{x_1} p_2^{x_2} \dots p_m^{x_m}$ o número de soluções é $\frac{(2k-3)(2x_1+1)\dots(2x_m+1)-1}{2}$. De maneira geral para $k \geq 2$ temos $\frac{d((\frac{c}{4})^2)-1}{2}$.

Vale ressaltar que essa é a quantidade de triplas de inteiros positivos $(a,b,c) = (skt, k^2s, (t^2-k^2)s)$, mas elas devem ser testadas na desigualdade triângular para determinar se realmente formam triângulo.

4.7 CONTANDO TRIÂNGULOS PITAGÓRICOS COM UM CATETO DADO

Problema 4.25. *(A) Determine o número de triângulos pitagóricos com um cateto de comprimento 60. Observe que existem exatamente* 4 *triplas pitagóricas primitivas em que um dos catetos vale 60.*

Solução

Conforme fizemos no problema 4.1 são 13 triângulos.

Problema 4.26. *(A) Quantos triângulos pitagóricos têm* 2×3^k *como um de seus catetos?*

Solução

Pelo Teorema de Pitágoras, a tripla $(2 \cdot 3^k, b, c)$ de inteiros são os lados de um triângulo retângulo se, e somente se,

$$(2 \cdot 3^k)^2 = c^2 - b^2 = (c-b)(c+b) \iff 3^{2k} = \left(\frac{c-b}{2}\right)\left(\frac{c+b}{2}\right).$$

Vale ressaltar que $c-b$ e $c+b$ possuem a mesma paridade e como o resultado é par os dois precisam ser pares. Sendo 3 primo, o produto de números só pode ser potência de 3 quando cada um é potência de 3. Lembrando que $\frac{c-b}{2} < \frac{c+b}{2}$ temos $\frac{c-b}{2} = 3^x$ e $\frac{c+b}{2} = 3^y$ com $x+y = 2k$ e $x < y$. Existem exatamente k soluções $\left(\frac{c-b}{2}, \frac{c+b}{2}\right) = (3^x, 3^{2k-x})$ com $x = 0, 1, \ldots, k-1$.

Portanto, existem k triângulos pitagóricos com um dos catetos igual a 2×3^k.

Problema 4.27. *(A) Quantos triângulos pitagóricos têm* 3^k5^l *como um de seus catetos?*

Solução

Novamente, pelo Teorema de Pitágoras, a tripla $(3^k5^l, b, c)$ de inteiros são os lados de um triângulo retângulo se, e somente se,

$$(3^k \cdot 5^l)^2 = c^2 - b^2 = (c-b)(c+b) \iff 3^{2k} \cdot 5^{2l} = (c-b)(c+b).$$

Como o resultado é ímpar os números $c-b$ e $c+b$ são ambos ímpares e não nos preocupamos com paridade.

Veja que $d(3^{2k} \cdot 5^{2l}) = (2k+1)(2l+1)$ e esses divisores podem ser pareados (d_1, d_2) com produto $d_1 d_2 = 3^{2k}5^{2l}$ e satisfazendo $d_1 < d_2$. São $\frac{(2k+1)(2l+1)-1}{2} = 2kl + k + l$ parzinhos. Isso é exatamente o número de triângulos, pois cada triângulo satisfaz $c - b = d_1$ e $c + b = d_2$ que é equivalente a $c = \frac{d_1+d_2}{2}$ e $b = \frac{d_2-d_1}{2}$.
Concluímos que são $2kl + k + l$ triângulos pitagóricos.

4.8 NÚMEROS QUE SÃO SOMAS DE DOIS QUADRADOS

Problema 4.28. *(A) Escrever 73, 89 e 97 como somas de dois quadrados.*

Solução

Esse números são primos da forma $4k+1$ então sabemos que é possível. Para encontrar as somas de dois quadrados basta testar. Obtemos $73 = 8^2 + 3^2$, $89 = 8^2 + 5^2$ e $97 = 9^2 + 4^2$.

Problema 4.29. *(A) Escrever 145 e 187 como somas de dois quadrados de duas formas distintas.*

Solução

Veja que $145 = 5 \cdot 29 = (2^2 + 1^2)(5^2 + 2^2)$ e usando as duas fatorações possíveis, $ad + bc$ e $ad - bc$, temos $145 = (2 \cdot 5 + 1 \cdot 2)^2 + (1 \cdot 5 - 2 \cdot 2)^2 = 12^2 + 1^2$ e $145 = (2 \cdot 5 - 1 \cdot 2)^2 + (1 \cdot 5 + 2 \cdot 2)^2 = 8^2 + 9^2$.
É impossível escrever 187 como soma de quadrados, pois $187 = 11 \cdot 17$ e $11 \equiv 3 \pmod 4$. Se existissem a e b inteiros tais $187 = a^2 + b^2$ então $11 \mid a^2 + b^2 \Rightarrow 11 \mid a$ e $11 \mid b \Rightarrow 11^2 \mid a^2 + b^2 = 187$ que é uma contradição.

Problema 4.30. *(A) De quantas formas distintas pode-se escrever 1001^2 como soma de dois quadrados?*

Solução

Veja que $1001^2 = 7^2 \cdot 11^2 \cdot 13^2$ e os primos 7 e 11 são $4k+3$. Sabemos do problema 0.74 que se p primo, $p \equiv 3 \pmod 4$ e $p \mid a^2 + b^2$ então $p \mid a$ e $p \mid b$. Logo $1001^2 = a^2 + b^2 \iff 13^2 = \left(\frac{a}{77}\right)^2 + \left(\frac{b}{77}\right)^2$. Podemos as possíveis somas de dois quadrados e obter $\{\frac{a}{77}, \frac{b}{77}\} = \{13, 0\}$ ou $\{12, 5\}$ e existem duas maneiras de escrever 1001^2 como soma de quadrados $(13 \cdot 77)^2 + (0 \cdot 77)^2$ e $(12 \cdot 77)^2 + (5 \cdot 77)^2$.
Se for soluções em que apenas troca-se a ordem devem ser consideradas diferentes, então teríamos quatro soluções.

Problema 4.31. *(OI) Seja p um número primo tal que a congruência $c^2 \equiv -2 \mod p$ possui solução. Mostre que existem inteiros a e b tais que $p = a^2 + 2b^2$.*

Solução

Considere os números $cx + y$ para x e y menores que $\sqrt{p}$, ou seja, $0 \leq x, y \leq \lfloor \sqrt{p} \rfloor$. São $(\lfloor p \rfloor + 1)^2 > p$ números e pelo PCP existem dois parzinhos distintos com mesma congruência módulo p. Sejam (x_1, y_1) e (x_2, y_2) essas soluções. Veja que $x_1 = x_2 \iff y_1 = y_2$ então podemos tomar $x_1 \neq x_2$ e $y_1 \neq y_2$. Veja que

$$cx_1 + y_1 \equiv cx_2 + y_2 \pmod{p} \Rightarrow c(x_1 - x_2) \equiv y_2 - y_1 \pmod{p}$$

Tomando $x = |x_1 - x_2|$ e $y = |y_2 - y_1|$ temos $0 < x, y < \sqrt{p}$ e

$$y^2 \equiv c^2 x^2 \equiv -2x^2 \pmod{p}$$

Logo, $p \mid y^2 + 2x^2$ e $0 < y^2 + 2x^2 < p + 2p = 3p$. Só poderia ser p ou $2p$. Mas $y^2 + 2x^2 = 2p \Rightarrow 2 \mid y$ e $y = 2z$ para algum inteiro positivo z implicando $4z^2 + 2x^2 = 2p \iff x^2 + 2z^2 = p$.

Portanto, se $c^2 \equiv -2 \pmod{p}$, então existem inteiros positivos a e b tais que $p = a^2 + 2b^2$.

Problema 4.32. *(OI) Demonstre que todo primo da forma $6k + 1$ pode se expressar de forma única como $x^2 + 3y^2$, com x e y inteiros positivos.*

Solução

Se $p = 6k + 1$, então pelo resultado provado no problema 1.41 temos $(\frac{-3}{p}) = (\frac{-1}{p}) \cdot (\frac{3}{p})$ que é $1 \cdot 1 = 1$, se $p = 12t + 1$, ou $(-1)(-1) = 1$, se $p = 12t + 7$. Logo, existe c inteiro tal que $c^2 \equiv -3 \pmod{p}$.

Usando os mesmos passos do problema anterior provamos que existem x e y com $0 < x, y < \sqrt{p}$ tais que $p \mid x^2 + 3y^2 < p + 3p = 4p$. Logo, $x^2 + 3y^2 = p$, $2p$ ou $3p$. Se der p está resolvido. Se der $2p$ veja que x e y são pares ou ambos ímpares e $x^2 + 3y^2 \equiv 0 + 3 \cdot 0$ ou $1 + 3 \cdot 1 \pmod{4}$ implicando que $2p = x^2 + 3y^2 \Rightarrow 4 \mid 2p \Rightarrow 2 \mid p$ que é falso, pois $p = 6k + 1$. Se for $3p$ temos $3 \mid x^2 + 3y^2 \Rightarrow 3 \mid x^2 \Rightarrow 3 \mid x$. Podemos substiuir $x = 3z$ com z inteiro positivo e obter

$$3p = (3z)^2 + 3y^2 = 9z^2 + 3y^2 \Rightarrow p = y^2 + 3z^2$$

.

Em todos os casos conseguimos escrever $p = a^2 + 3b^2$ com a e b inteiros positivos.

Suponha que existem duas representações $a^2+3b^2 = c^2+3d^2$ com $0 < a,b,c,d < \sqrt{p}$. Temos $a^2 \equiv -3b^2 \pmod{p}$ e $c^2 \equiv -3d^2 \pmod{p}$. Multiplicando cruzado podemos cancelar o -3 que é primo com p e obter $(ad)^2 \equiv (bc)^2 \pmod{p}$ e $p \mid ad-bc$ ou $p \mid ad+bc$. Se $p \mid ad-bc$ e $|ad-bc| < p$ então $ad-bc = 0 \iff \frac{a}{b} = \frac{c}{d}$. Como são frações irredutível $a = c$ e $b = d$.

Se $p \mid ad+bc$. Temos $0 < ad+bc < p+p = 2p$ e $ad+bc = p$. Tome o produto

$$p^2 = (a^2+3b^2)(c^2+3d^2) = (ac)^2+9(bd)^2+3((ad)^2+(bc)^2)$$

Completando os quadrados temos duas formas de representar p^2

$$p^2 = (ac+3bd)^2+3(ad-bc)^2$$

e

$$p^2 = (ac-3bd)^2+3(ad+bc)^2$$

Usando esta última possibilidade, $p^2 = (ac-3bd)^2+3p^2 \Rightarrow 0 = (ac-3bd)^2+2p^2 > 0$. Chegamos numa contradição e podemos afirmar que $p \nmid ad+bc$.

Dos passos feitos, se $p = 6k+1$ é um primo, então existem a e b inteiros positivos tais que $p = a^2+3b^2$.

Problema 4.33. *(A) Mostre que os números da forma $4^k(8n+7)$ não podem ser escritos como soma de três quadrados.*

Solução

Suponha que $4^k(8n+7) = x^2+y^2+z^2$. Se $k > 0$, então $4 \mid x^2+y^2+z^2 \equiv 0+0+0, 0+0+1, 0+1+1$ ou $1+1+1 \pmod 4$, pois se m é ímpar então $m^2 \equiv 1 \pmod 8$ e se m é par $m^2 \equiv 0$ ou $4 \pmod 8$ que são múltiplos de 4. Mas a soma só dá zero quando são todos zeros, ou seja, todos os números pares. Daí, podemos traformar a equação em $4^{k-1}(8n+7) = \left(\frac{x}{2}\right)^2+\left(\frac{y}{2}\right)^2+\left(\frac{z}{2}\right)^2$. Podemos repetir esse processo até chegar em $8n+7 = x_0^2+y_0^2+z_0^2$. Mas $x_0^2+y_0^2+z_0^2 \equiv 0+0+0, 0+0+1, 0+0+4, 1+1+0, 1+1+1, 1+1+4, 4+4+0, 4+4+1, 4+4+4$ ou $0+1+4 \pmod 8 \Rightarrow x_0^2+y_0^2+z_0^2 \equiv 0,1,4,2,3,6,0,1,4$ ou $5 \pmod 8$. Como nenhum é congruente 7 módulo 8 a equação $x_0^2+y_0^2+z_0^2 = 8n+7$ não tem solução e fica provado que $4^k(8n+7)$ não pode ser escrito como soma de três quadrados.

Problema 4.34 (Scholz)**.** *(T) Prove a seguinte generalização do lema de Thue: Sejam n um número natural positivo e r e s números naturais tais que $rs > n$ com $1 < r,s < n$.*

Então, para todo a com $(a,n) = 1$*, a congruência* $ay \equiv \pm x \pmod{n}$ *tem solução inteira com* $0 < x < r$ *e* $0 < y < s$*.*

Solução

Considere todos os possíveis $ax + y$ com $0 \leq x \leq r-1$ e $0 \leq y \leq s-1$. São rs números e existem apenas n classes de congruência módulo n. Pelo PCP, se $rs > n$, então dois pares (x_1, y_1) e (x_2, y_2) satisfazem $ax_1 + y_1 \equiv ax_2 + y_2 \pmod{n}$. Se $x_1 = x_2$, então $y_1 \equiv y_2 \pmod{n} \Rightarrow y_1 = y_2$. E se $y_1 = y_2$, então $ax_1 \equiv ax_2 \pmod{n} \Rightarrow x_1 \equiv x_2 \pmod{n} \Rightarrow x_1 = x_2$. Portanto, temos $x_1 \neq x_2$ e $y_1 \neq y_2$. Suponha sem perda de generalidade que $x_1 > x_2$. Podemos concluir que $a(x_1 - x_2) \equiv y_2 - y_1 \pmod{n}$, $0 < x = x_1 - x_2 < r$ e $0 < y = |y_2 - y_1| < s$. Assim, podemos concluir que $ax \equiv \pm y \pmod{n}$.

Problema 4.35. *(T) Demonstre que todas as soluções inteiras de* $x^2 + y^2 + z^2 = t^2$*, estão dadas pelas equações*

$$x = d(m^2 - n^2 - p^2 + q^2),\ y = d(2mn - 2pq),$$

$$z = d(2mp + 2nq),\ t = d(m^2 + n^2 + p^2 + q^2),$$

com d, m, n, p, q *inteiros.*

Solução

Usaremos os seguintes lemas.

Lema 1: Se um número pode ser escrito como soma de quadrados de inteiros $\alpha^2 + \beta^2$ e o quociente $\frac{\alpha^2+\beta^2}{a^2+b^2}$ é um inteiro m, com a e b inteiros e $a^2 + b^2$ um primo, então m também é a soma de quadrados.

Demonstração: Temos

$$m = \frac{\alpha^2 + \beta^2}{a^2 + b^2} = \frac{(\alpha^2 + \beta^2)(a^2 + b^2)}{(a^2 + b^2)^2} = \left(\frac{\alpha a \pm \beta b}{a^2 + b^2}\right)^2 + \left(\frac{\alpha m \mp \beta a}{a^2 + b^2}\right)^2.$$

É suficiente provar que $\alpha a + \beta b$ ou $\alpha a - \beta b$ é múltiplo de $a^2 + b^2$, pois isso já implicaria que a outra parcela é inteira. Por congruência, $a^2 \equiv -b^2 \pmod{a^2 + b^2}$ e $\alpha^2 \equiv -\beta^2 \pmod{a^2 + b^2}$. Multiplicando, $a^2 + b^2 \mid (\alpha a)^2 - (\beta b)^2 = (\alpha a - \beta b)(\alpha a + \beta b)$ e do fato de $a^2 + b^2$ ser primo segue que um dos fatores é múltiplo de $a^2 + b^2$.

Lema 2: Se p é um primo $4k+1$ tal que $p = a^2 + b^2$ com a e b inteiros. Seja m um inteiro tal que $pm = \alpha^2 + \beta^2$, com α e β inteiros. Então existe uma representação de m como soma de dois quadrados,

$$m = \left(\frac{\alpha a \pm \beta b}{a^2+b^2}\right)^2 + \left(\frac{\alpha m \mp \beta a}{a^2+b^2}\right)^2$$

tal que a representação $\alpha^2 + \beta^2$ de pm é obtida das representações de p e m por meio da multiplicação e da identidade

$$(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2.$$

Demonstração: pelo lema 1 sabemos que tal representação existe e fazendo manipulações algébricas vemos que, de fato, qualquer representação de pm é originada da representação de p multiplicada por uma representação de m.

Comecemos supondo que $\text{mdc}(x,y,z,t) = 1$, pois caso seja $d > 1$ podemos considerar a quádrupla $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}, \frac{t}{d}\right)$. Veja também que pelo menos dois dos números x, y e z precisam ser pares, pois caso contrário $t^2 \equiv 2$ ou $3 \pmod 4$ que é impossível. Suponha que y e z são pares. Pelo mdc ser 1 sabemos que x é ímpar e t é ímpar.

$$x^2 + y^2 + z^2 = t^2 \iff y^2 + z^2 = (t-x)(t+x)$$

Se existe um primo r com $r \equiv 3 \pmod 4$ tal $r \mid t-x$ e $r \mid t+x$ então $r \mid (t-x)+(t+x) \Rightarrow r \mid 2t \Rightarrow r \mid t$ e analogamente $r \mid x$. Além disso, $r \mid y^2+z^2$ e $r \equiv 3 \pmod 4 \Rightarrow r \mid y$ e $r \mid z$. Isso é impossível, pois $\text{mdc}(x,y,z,t) = 1$.
Assim, se r primo, $r \equiv 3 \pmod 4$ e $r \mid y^2+z^2$ implica que o expoente de r na fatoração de y^2+z^2 é par e no outro lado esses fatores não são separados. Se $r \mid t-x$ então $t-x$ em todos esses fatores r e essa quantidade é par. Concluímos que $t-x$ e $t+x$ podem ser escritos como somas de dois quadrados. Adicionamos a isso o fato de eles serem pares e podemos afirmar que existem m, n, p e q tais que $t-x = 2(m^2+q^2)$ e $t+x = 2(n^2+p^2)$. Isso nos leva a $x = n^2+p^2-m^2-q^2$ e $t = n^2+p^2+m^2+q^2$. Pelo lema 2 encontramos também que $y = 2mp+2nq$ e $z = 2mn-2pq$.
Concluímos que todas as soluções são da forma

$$x = d(m^2-n^2-p^2+q^2),\ y = d(2mn-2pq),$$
$$z = d(2mp+2nq),\ t = d(m^2+n^2+p^2+q^2),$$

para alguns inteiros d, m, n, p e q.

4.9 TRIÂNGULOS PITAGÓRICOS COM CATETOS CONSECUTIVOS E A EQUAÇÃO DE PELL

Problema 4.36. *(A) Observe que* $8^3 - 7^3 = 13^2$. *Mostre que existem infinitos pares de cubos consecutivos tais que sua diferença é um quadrado perfeito.*

Solução

Queremos mostrar que a equação $(x+1)^3 - x^3 = y^2$ possui infinitas soluções inteiras. Veja que

$$(x+1)^3 - x^3 = y^2 \iff 3x^2 + 3x + 1 = y^2 \iff 3(4x^2 + 4x + 1) + 1 = (2y)^2$$

$$\iff (2y)^2 - 3(2x+1)^2 = 1$$

Precisamos de infinitas soluções da equação $A^2 - 3B^2 = 1$ com A par. Veja que B ímpar é consequência. Podemos usar a solução dada como exeplo $2y = 2 \cdot 13 = 26$ e $2x + 1 = 2 \cdot 7 + 1 = 15$. De fato, $26^2 - 3 \cdot 15^2 = 1$. Tomamos as soluções $A_k + B_k\sqrt{3} = (26 + 15\sqrt{3})^{2k+1}$. Veja que A_k é par pois é a soma de termos $\binom{2k+1}{t} 26^{2k+1-t}(B_k\sqrt{3})^t$ com t par. Cada parcela é par, pois $2k + 1 - t$ é ímpar e o expoente de 26 é positivo.

Problema 4.37. *(OI) Mostre que a soma de três quadrados consecutivos não pode ser igual a um quadrado. Pode a soma de cinco quadrados consecutivos ser igual a um quadrado?*

Solução

Podemos escrever a soma de três quadrados consecutivos como $(x-1)^2 + x^2 + (x+1)^2 = 3x^2 + 2 \equiv 2 \pmod 3$. Isso não pode ser um quadrado, pois todo quadrado perfeito é congruente 0 ou 1 módulo 3.

A soma de cinco quadrados consecutivos pode ser escrita como $(x-2)^2 + (x-1)^2 + x^2 + (x+1)^2 + (x+2)^2 = 5x^2 + 10 = 5(x^2+2)$. Se isso for um quadrado então tem uma quantidade par de fatores 5 implicando que $5^2 \mid 5(x^2+2) \Rightarrow 5 \mid x^2 + 2$. Porém, $x^2 \equiv 0, 1$ ou $4 \pmod 5$. Portanto, a soma de 5 quadrados consecutivos não pode ser um quadrado perfeito.

4.10 SOLUÇÃO FUNDAMENTAL DA EQUAÇÃO DE PELL

Problema 4.38. *(A) Calcule a solução fundamental da equação de Pell* $x^2 - dy^2 = 1$, *onde* $d = a^2 - 2$ *e* $d = a^2 - a$ *para a inteiro arbitrário.*

Solução

No capítulo 3 determinamos as frações contínuas de $\sqrt{a^2-2}$ e $\sqrt{a^2-a}$. Como $\sqrt{a^2-2} = [a-1;\overline{1, a-2, 1, 2a-2}]$ a fração contínua de $\sqrt{a^2-2} + \left\lfloor \sqrt{a^2-2} \right\rfloor$ tem período 4 e basta encontrar a quarta reduzida.

$$\frac{p}{q} = a - 1 + \frac{1}{1 + \frac{1}{a-2+\frac{1}{1}}} = \frac{a^2-1}{a}$$

A solução fundamental é $(x, y) = (a^2-1, a)$.

Como $\sqrt{a^2-a} = [a-1;\overline{2, 2a-2}]$ a fração contínua de $\sqrt{a^2-a} + \left\lfloor \sqrt{a^2-a} \right\rfloor$ tem período 2 e basta encontrar a segunda reduzida.

$$\frac{p}{q} = a - 1 + \frac{1}{2} = \frac{2a-1}{2}$$

A solução fundamental é $(x, y) = (2a-1, 2)$.

Problema 4.39. *(A) Determine a fração contínua de $\sqrt{a^2+2}$, e determine para que valores de a, a equação $x^2 - (a^2+2)y^2 = -1$ tem solução.*

Solução

Primeiro vamos determinar a fração contínua. Temos $\alpha_0 = a^2+2$ e $a_0 = \lfloor \alpha_0 \rfloor = a$. Temos $\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{\sqrt{a^2+2}-a} = \frac{\sqrt{a^2+2}+a}{2}$. Segue que $a_1 = a$ e $\alpha_2 = \frac{1}{\alpha - 1 - a_1} = \frac{1}{\frac{\sqrt{a^2+2}+a}{2} - a} = \sqrt{a^2+2} + a$. Veja que $a_2 = 2a$ e $\alpha_3 = \frac{1}{\sqrt{a^2+2}+a-2a} = \frac{1}{\sqrt{a^2+2}-a} = \alpha_1$. Logo $\sqrt{a^2+2} = [a;\overline{a, 2a}]$. Podemos observar que a fração contínua de $\sqrt{a^2+2} + \left\lfloor \sqrt{a^2+2} \right\rfloor$ tem período 2 que é par. Assim, a equação $x^2 - (a^2+2)y^2 = -1$ não possui soluções inteiras.

Problema 4.40. *(A) Determine a solução fundamental da equação $x^2 - 31y^2 = 1$.*

Solução

Em fração contínua, temos

$$\sqrt{31} = [5;\overline{1, 1, 3, 5, 3, 1, 1, 10}]$$

O período da fração contínua de $\sqrt{31} + \left\lfloor \sqrt{31} \right\rfloor$ é oito. Usando a oitava reduzida $[5; 1, 1, 3, 5, 3, 1, 1] = \frac{1520}{273}$. A solução fundamental é $(x, y) = (1520, 273)$.

Problema 4.41. *(A) Determine a solução fundamental da equação $x^2 - 41y^2 = -1$.*

Solução

Em fração contínua, temos

$$\sqrt{41} = [6;\overline{2, 2, 12}]$$

O período da fração contínua de $\sqrt{41} + \left\lfloor \sqrt{41} \right\rfloor$ é três. Como o período é ímpar $x^2 - 41y^2 = -1$ possui solução. A terceira reduzida $\frac{p}{q} = [6;2,2] = \frac{32}{5}$ e a solução fundamental é $(x,y) = (32,5)$.

4.11 OUTRAS EQUAÇÕES DO TIPO $x^2 - Ay^2 = c$

Problema 4.42. *(A) Determine se a equação $x^2 - 19y^2 = 21$ possui solução inteira.*

Solução

Começamos pela fração contínua $\sqrt{19} = [4;\overline{2,1,3,1,2,8}]$. O período é 6, então tomamos a sexta reduzida $[4;2,1,3,1,2] = \frac{170}{39}$. A solução fundamental de $x^2 - 19y^2 = 1$ é $(x,y) = (170,39)$.

Temos $84 < \sqrt{21(170+39\sqrt{19})} < 85$ e $19 < \sqrt{\frac{21(170+39\sqrt{19})}{19}} < 20$. Pela proposição 4.20 e de $x^2 > 21$ se existe solução então uma solução satisfaz $5 \leq x \leq 85$ e $y \leq 20$. Para cada $1 \leq y \leq 20$ podemos testar se $19y^2 + 21$ é um quadrado. Os valores de $19y^2 + 21$ são $40, 97, 192, 325, 496, 705, 952, 1237, 1560, 1921, 2320, 2757, 3232, 3745, 4296, 4885, 5512, 6177, 6880$ e 7621. Nenhum deles é um quadrado. Concluímos que a equação $x^2 - 19y^2 = 21$ não tem solução inteira.

Observe que poderíamos concluir esse resultado usando reciprocidade quadrática, pois se houvesse solução teríamos $x^2 \equiv x^2 - 19y^2 \equiv 21 \equiv 2 \pmod{19}$, mas $(\frac{2}{19}) = -1$ pois $19 \equiv 3 \pmod 8$.

Problema 4.43. *(A) Determine todos os $|c| < 10$ tais que $x^2 - 17y^2 = c$ possui solução inteira.*

Solução

Primeiro veja que se tem solução, então $x^2 \equiv x^2 - 17y^2 \equiv c \pmod{17} \Rightarrow (\frac{c}{17}) = 1$. Vejamos os resíduos quadráticos módulo 17 a partir de $0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2$ e 8^2 que nos dão, respectivamente, $0, 1, 4, 9, -1, 8, 2, -2$ e -4. Os c que não são congruentes a números dessa lista não possuem solução. Os valores de c tais que a equação pode ter solução são $-9, -8, -4, -2, -1, 0, 1, 2, 4, 8$ e 9.

Veja que 0 não é possível, pois $x^2 - 17y^2 = 0 \iff \sqrt{17} = \frac{x}{y}$ e $\sqrt{17}$ é irracional.

Com exceção de -2 e 2 podemos encontrar soluções testando. Obtemos assim,

$$12^2 - 17 \cdot 3^2 = -9$$

$$3^2 - 17 \cdot 1^2 = -8$$

$$8^2 - 17 \cdot 2^2 = -4$$

$$4^2 - 17 \cdot 1^2 = -1$$

$$33^2 - 17 \cdot 8^2 = 1$$

$$66^2 - 17 \cdot 16^2 = 4$$

$$5^2 - 17 \cdot 1^2 = 8$$

$$99^2 - 17 \cdot 24^2 = 9$$

Provaremos que 2 e -2 não possuem soluções. Em frações contínuas $\sqrt{17} = [4;\overline{8}]$. O período é 1 que é ímpar, então a solução fundamental é $x + y\sqrt{17} = (4+\sqrt{17})^2 = 33 + 8\sqrt{17}$. Para testar soluções de $x^2 - 17y^2 = c$ com $|c| \leq 9$ basta testar $x < \sqrt{9(33+8\sqrt{17})} < 25$ e $y < \sqrt{\frac{9(33+8\sqrt{17})}{17}} < 6$. Particularmente, para 4 e 9 podemos usar soluções $(x,y) = (2,0)$ e $(x,y) = (3,0)$, respectivamente. Basta testar $0 \leq y \leq 6$ se $17y^2 \pm 2$ é um quadrado perfeito. Os valores de $17y^2$ são $0, 17, 68, 153, 272, 425$ e 612 e adicionando ou subtraindo 2 não temos quadrados perfeitos.
Portanto, os valores de c com $|c| < 10$ tal que $x^2 - 17y^2 = c$ possui solução inteira são $\{-9, -8, -4, -1, 1, 4, 8, 9\}$.

Problema 4.44. *(A) Usando o fato de que a equação* $x^2 - 91y^2 = 1$ *tem como solução fundamental o par* $(1574, 165)$*, mostre que a equação* $7x^2 - 13y^2 = 1$ *não possui soluções inteiras.*

Solução

Se a equação $7x^2 - 13y^2 = 1$ possui solução, então $(7x)^2 - 91y^2 = 7$ tem solução. Se $A^2 - 91B^2 = 7$ tem solução, então possui solução com $A < \sqrt{7(1574 + 165\sqrt{91})} < 149$ e $B < \sqrt{\frac{7(1574+165\sqrt{91})}{91}} < 16$. Só precisamos testar para $0 \leq B \leq 15$ se $91B^2 + 7$ é um quadrado perfeito.

$$910^2 + 7 = 7$$

$$911^2 + 7 = 98$$

$$912^2 + 7 = 371$$

$$913^2 + 7 = 826$$

$$914^2 + 7 = 1463$$

$$915^2 + 7 = 2282$$

$$916^2 + 7 = 3283$$

$$917^2 + 7 = 4466$$

$$918^2 + 7 = 5831$$

$$919^2 + 7 = 7378$$

$$9110^2 + 7 = 9107$$

$$9111^2 + 7 = 11018$$

$$9112^2 + 7 = 13111$$

$$9113^2 + 7 = 15386$$

$$9114^2 + 7 = 17843$$

$$9115^2 + 7 = 20482$$

Nenhum dos números é um quadrado perfeito e podemos concluir que $7x^2 - 13y^2 = 1$ não possui soluções inteiras.
Por reciprocidade quadrática, se $A^2 - 91B^2 = 7$ tivesse solução, então $A^2 \equiv 7 \pmod{13}$, mas $(\frac{7}{13}) = -1$ e não existe A que satisfaça a congruência. Portanto, $A^2 - 91B^2 = 7$ não tem solução inteira.

4.12 CONTANDO TRIÂNGULOS PITAGÓRICOS COM HIPOTENUSA FIXADA: INTEIROS DE GAUSS

Problema 4.45. *(A) Calcule um resto da divisão de* $38 + 65i$ *por* $7 - 5i$.

Solução

Veja que

$$\frac{38 + 65i}{7 - 5i} = \frac{(38 + 65i)(7 + 5i)}{(7 - 5i)(7 + 5i)} = \frac{-59 + 645i}{74} = \frac{-59}{74} + \frac{645}{74}i$$

Tomamos como quociente os $q = a + bi$ com a e b inteiros mais próximos de $\frac{-59}{74}$ e $\frac{645}{74}$, respectivamente. Temos $q = -1 + 9i$ e o resto da divisão é

$$r = (38 + 65i) - (7 - 5i)(-1 + 9i) = (38 + 65i) - (38 + 68i) = -3i.$$

Problema 4.46. *(A) Determine* $\text{mdc}(232 + 156i, 371 + 223i)$.

Solução

Podemos usar os passos do Algoritmo Estendido da Divisão

$$371 + 223i = (232 + 156i) \times 1 + (139 + 67i)$$

$$232 + 156i = (139 + 67i) \times 2 + (-46 + 22i)$$

$$139 + 67i = (-46 + 22i) \times (-2 - 2i) + (3 + 19i)$$

$$-46 + 22i = (3 + 19i) \times (1 + 3i) + (8 - 6i)$$

$$3 + 19i = (8 - 6i) \times (-1 + 2i) + (-1 - 3i)$$

$$8 - 6i = (-1 - 3i) \times (1 + 3i)$$

Concluímos que $\text{mdc}(232 + 156i, 371 + 223i) = 1 + 3i$ que é equivalente a $-1 - 3i$ a menos de multiplicação por unidade.

Problema 4.47. *(A) Use o algarismo estendido da divisão para determinar as soluções* $x, y \in \mathbb{Z}[i]$ *de* $(13 + 10i)x + (7 + 20i)y = 1$.

Solução

Novamente, usaremos os passos do Algoritmo Estendido da Divisão

$$7 + 20i = (13 + 10i) \times (1 + i) + (4 - 3i)$$

$$13 + 10i = (4 - 3i) \times (1 + 3i) + i$$

Observe que i é unidade, então $\text{mdc}(7 + 20i, 13 + 10i) = 1$ e usando as equações

$$i = (13 + 10i) - (4 - 3i)(1 + 3i)$$

$$i = (13 + 10i) - ((7 + 20i) - (13 + 10i)(1 + i))(1 + 3i)$$

$$i = (7 + 20i)(-1 - 3i) + (13 + 10i)(-1 + 4i)$$

Para obter 1 basta multiplicar i e os coeficientes por $-i$. Assim, os x e y desejados seguem na equação

$$1 = (7 + 20i)(-3 + i) + (13 + 10i)(4 + i).$$

Problema 4.48. *(OA) Determine todas as soluções inteiras da equação* $x^2 + y^2 = 2z^3$.

Solução

Comecemos observando que $z = 0$ implica os demais 0. E $x = 0$ implica $(x, y, z) = (0, 2^2k^3, 2k^2)$. Analogamente, $y = 0$ implica $(x, y, z) = (2^2k^3, 0, 2k^2)$. Podemos agora supor que todos são não nulos.

Suponha que existe um primo p primo com $p \equiv 3 \pmod 4$ tal que $p \mid z$. Seja c o expoente de p na fatoração de z. Temos p^{3c} a maior potência de p que divide $2z^3$. Veja

que $p \mid x^2+y^2 \Rightarrow p \mid x$ e $p \mid y \Rightarrow p^2 \mid x^2+y^2$. Podemos escrever $(\frac{x}{p})^2+(\frac{y}{p})^2$ com dois fatores p a menos. Se c for ímpar, então após repetir esse processo várias vezes sobrará que $p \mid (x')^2+(y')^2$ e $p^2 \nmid (x')^2+(y')^2$ que é absurdo. Então c tem que ser par e podemos escrever $c = 2k$ e afirmar que p^{3k} divide x e y.

Se $2 \mid z$, então podemos supor que z possui c fatores 2 com $c \geq 1$. Assim, $2^{3c+1} \mid 2z^3$. Sabemos que se n é ímpar, então $n^2 \equiv 1 \pmod 4$. Usando módulo 4 se $2^2 \mid x^2+y^2$ então $2 \mid x$ e $2 \mid y$ implicando $2 \mid x$ e $2 \mid y$ e podemos considerar o número $(\frac{x}{2})^2+(\frac{y}{2})^2$ que possui 2 fatores 2 a menos. Após fazer isso várias vezes temos dois casos. Se c é ímpar, acabamos com todos os fatores 2 e o que sobra é $(x')^2+(y')^2 = (z')^3$ com z' ímpar. Se c é par, então sobra exatamente um fator 2 e $(x')^2+(z')^2 \equiv 2 \pmod 4$ implicando x' e y' ímpares.

Se z não possuir mais fatores, então a única solução possível seria $(x,y,z) = (2^{3k}I^3, 2^{3k}I^3, 2^{2k}I^2)$. No outro caso, $z' = 1$ implicaria $(x')^2+(y')^2 = 1$ que daria um deles igual a 0.

Se z possui fatores primos p com $p \equiv 1 \pmod 4$. Veja que $x^2+y^2 = 2z^3 \iff (x+yi)(x-yi) = 2z^3$. Suponha que z possui c fatores p e que a e b são inteiros tais que $p = a^2+b^2$. Em $\mathbb{Z}[i]$ temos $p = (a+bi)(a-bi)$ e em $2z^3$ são $3c$ fatores irredutíveis $a+bi$ e $3c$ fatores irredutíveis $a-bi$. Veja que $a+bi \mid x+yi \iff a-bi \mid x-yi$ por conjugado complexo. Logo, esses $3c$ fatores são pareados para $x+yi$ e $x-yi$. Existem inteiros não negativos m e n tais que $(a+bi)^m(a-bi)^n \mid x+yi$, $(a-bi)^m(a+bi)^n \mid x+yi$ e $m+n = 3c$.
Portanto, todas as soluções são descritas por

(i) Se z tem uma quantidade par de fatores 2.

$$z = 2^{2k}I^2p_1^{k_1}\dots p_s^{k_s}$$

$$x+yi = 2^{3k}I^3\prod(a_j+b_ji)^{m_j}(a_j-b_ji)^{3k_j-m_j}$$

Onde cada p_j é um primo congruente a 1 módulo 4 e $a_j^2+b_j^2 = p_j$.

(ii) Se z tem uma quantidade impar de fatores 2.

$$z = 2^{2k+1}I^2p_1^{k_1}\dots p_s^{k_s}$$

$$x+yi = 2^{3k+2}I^3\prod(a_j+b_ji)^{m_j}(a_j-b_ji)^{3k_j-m_j}$$

Onde cada p_j é um primo congruente a 1 módulo 4 e $a_j^2+b_j^2 = p_j$.

Problema 4.49. *(OI) Mostre que se p um primo da forma $4k+1$ então $x^2+y^2 = pz^4$ possui infinitas soluções com* $\text{mdc}(x,y) = 1$.

Solução

Considere os números da forma $z = p^k$. Assim, $x^2+y^2 = pz^4$ pode ser reescrito como

$$(x+yi)(x-yi) = p^{4k+1}$$

Como $p \equiv 1 \pmod 4$ existem inteiros positivos a e b tais que $p = a^2+b^2 = (a+bi)(a-bi)$. Podemos tomar como solução

$$x+yi = (a+bi)^{4k+1}$$

Usando o conjugado complexo temos $x-yi = (a-bi)^{4k+1}$ e segue que x e y são solução da equação.

Resta estudar o mdc de x e y. Mas se $\text{mdc}(x,y) = d$ temos $d \mid x+yi$ e $d \mid x-yi$ em $\mathbb{Z}[i]$. Mas cada um desses números é o produto de termos irredutíveis distintos em $\mathbb{Z}[i]$ e, portanto, $\text{mdc}(x+yi, x-yi) = 1 \Rightarrow d = 1$.

Problema 4.50. *(OI) Mostre que a equação $25x^2+14xy+2y^2 = z^5$ possui infinitas soluções com* $\text{mdc}(x,y) = 1$.

Solução

Considere a equação $2y^2+14xy+25x^2-z^5 = 0$ como equação do 2º grau em y. O discriminante é $\Delta = (14x)^2 - 4\cdot 2\cdot(25x^2-z^5) = 196x^2-200x^2+8z^5 = -4x^2+8z^5 = 4(-x^2+2z^5)$. As soluções são

$$y = \frac{-14x \pm 2\sqrt{-x^2+2z^5}}{2\cdot 2} = \frac{-7x \pm \sqrt{-x^2+2z^5}}{2}$$

Queremos que a equação $-x^2+2z^5 = w^2 \iff 2z^5 = x^2+w^2$. Tome $z = p$ com p primo e $p \equiv 1 \pmod 4$. Como $p = 4k+1$ existem a e b ínteiros positivos tais que $p = a^2+b^2 = (a+bi)(a-bi)$. Tome $x+wi = (1+i)(a+bi)^5$. Por conjugado complexo, $x-wi = (1-i)(a-bi)^5$ e sabemos que $2p^5 = x^2+w^2$. Note que $y = \frac{-7x+w}{2}$ é inteiro, pois se x^2+w^2 é par os dois números possuem a mesma paridade.

Resta apenas provar que $\text{mdc}(x,y) = 1$. Se existe um primo q tal que $q \mid x$ e $q \mid y$ então $q^2 \mid 2y^2+14xy+25x^2 = p^5 \Rightarrow q \mid p \Rightarrow q = p$. Dessa forma, $p \mid 2y+7x = w$. Mas em $\mathbb{Z}[i]$ teremos $p \mid x+wi$ e $p \mid x-wi$. Esses dois números são produtos de inteiros de Gauss irredutíveis diferentes e $\text{mdc}(x+wi, x-wi) = 1$ gerando contradição.

Problema 4.51. *(A) Encontre todos os triângulos retângulos com hipotenusa* 330.

Solução

Fatoramos 330 em primos $330 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 11^1$. Só importa o expoente do 5 que é 1. Pelo Teorema 4.37 há $T_2(330) = \frac{1}{2}(2 \cdot 1 + 1) - \frac{1}{2} = 1$ triângulo.

De fato, o único triângulo possui lados $(198, 264, 330)$. Isso pode ser visto também do fato $330^2 = x^2 + y^2$ implica $2^2 \mid x^2 + y^2 \Rightarrow 2 \mid x$ e $2 \mid y$. E para p primo $4k+3$, nesse caso 3 e 11, se $p \mid x^2 + y^2$ então $p \mid x$ e $p \mid y$. Resta apenas o 5 que pode ser escrito como $a^2 + b^2$ de maneira única.

Problema 4.52. *(A) Quantos triplas pitagóricas têm hipotenusa igual a* 5525*?*

Solução

Fatorando 5525 em primos obtemos $5525 = 5^2 \cdot 13 \cdot 17$. Pelo Teorema 4.37 usaremos todos os expoentes já que são todos primos $4k+1$ e há $T_2(5525) = \frac{1}{2}(2 \cdot 2 + 1)(2 \cdot 1 + 1)(2 \cdot 1 + 1) - \frac{1}{2} = 22$ triângulos pitagóricos de hipotenusa 5525.

A seguir temos as 22 soluções listadas com o auxílio de um computador.

$$235^2 + 5520^2 = 5525^2 \Rightarrow (235, 5520, 5525)$$

$$525^2 + 5500^2 = 5525^2 \Rightarrow (525, 5500, 5525)$$

$$612^2 + 5491^2 = 5525^2 \Rightarrow (612, 5491, 5525)$$

$$845^2 + 5460^2 = 5525^2 \Rightarrow (845, 5460, 5525)$$

$$1036^2 + 5427^2 = 5525^2 \Rightarrow (1036, 5427, 5525)$$

$$1131^2 + 5408^2 = 5525^2 \Rightarrow (1131, 5408, 5525)$$

$$1320^2 + 5365^2 = 5525^2 \Rightarrow (1320, 5365, 5525)$$

$$1360^2 + 5355^2 = 5525^2 \Rightarrow (1360, 5355, 5525)$$

$$1547^2 + 5304^2 = 5525^2 \Rightarrow (1547, 5304, 5525)$$

$$2044^2 + 5133^2 = 5525^2 \Rightarrow (2044, 5133, 5525)$$

$$2125^2 + 5100^2 = 5525^2 \Rightarrow (2125, 5100, 5525)$$

$$2163^2 + 5084^2 = 5525^2 \Rightarrow (2163, 5084, 5525)$$

$$2340^2 + 5005^2 = 5525^2 \Rightarrow (2340, 5005, 5525)$$

$$2600^2 + 4875^2 = 5525^2 \Rightarrow (2600, 4875, 5525)$$

$$2805^2 + 4760^2 = 5525^2 \Rightarrow (2805, 4760, 5525)$$

$$2880^2 + 4715^2 = 5525^2 \Rightarrow (2880, 4715, 5525)$$

$$3124^2 + 4557^2 = 5525^2 \Rightarrow (3124, 4557, 5525)$$

$$3315^2 + 4420^2 = 5525^2 \Rightarrow (3315, 4420, 5525)$$

$$3468^2 + 4301^2 = 5525^2 \Rightarrow (3468, 4301, 5525)$$

$$3500^2 + 4275^2 = 5525^2 \Rightarrow (3500, 4275, 5525)$$

$$3720^2 + 4085^2 = 5525^2 \Rightarrow (3720, 4085, 5525)$$

$$3861^2 + 3952^2 = 5525^2 \Rightarrow (3861, 3952, 5525)$$

Problema 4.53. *(A) Encontre o menor valor para c de tal forma que existam exatamente* 28 *triângulos com hipotenusa igual a c.*

Solução

Usando a fórmula do Teorema 4.37 temos que resolver $T_2(c) = 28 \iff (2\alpha_1 + 1)\ldots(2\alpha_k + 1) = 55$ onde α_i são expoentes dos primos $4k+1$. Se estamos interessados no menor número, então não usaremos 2 ou primos $4k+3$ já que só tornam o número maior sem alterar $T_2(c)$. Além disso, devemos colocar o maior expoente no 5 que é menor primo $4k+1$, o segundo menor expoente no 13 que é o segundo menor primo possível e assim por diante. Só temos dois casos. O primeiro é $2\alpha_1 + 1 = 55 \iff \alpha_1 = 27$ e o menor número nesse caso é 5^{27}. O segundo é $2\alpha_1 + 1 = 11$ e $2\alpha_2 + 1 = 5$ que nos dá $\alpha_1 = 5$ e $\alpha_2 = 2$ implicando o menor número possível $5^5 \cdot 13^2$. Veja que $5^5 \cdot 13^2 < 5^5 \cdot (5^2)^2 = 5^9 < 5^{27}$ e o menor número possível vem do segundo caso.
Concluímos que o menor número c que é hipotenusa de exatamente 28 triângulos retângulos é $c = 5^5 \cdot 13^2 = 528125$.

4.13 DESCENSO INFINITO DE FERMAT

Problema 4.54. *(OI) Seja p um número primo e n um inteiro maior do que* 1. *Usar o método do descenso infinito para mostrar que* $\sqrt[n]{p}$ *é um número irracional.*

Solução

Suponha que $\sqrt[n]{p}$ seja racional. Então existe uma representação $\sqrt[n]{p}$ como fração irredutível $\frac{a}{b}$. Sendo irredutível temos $\text{mdc}(a, b) = 1$ e essa é a representação com o menor numerador possível.
Porém, de $\sqrt[n]{p} = \frac{a}{b}$ temos $pb^n = a^n \Rightarrow p \mid a^n \Rightarrow p \mid a$, pois p é primo. Então $a = pa_0$ e $pb^n = p^n a_0^n \Rightarrow b^n = p^{n-1}a_0^n \Rightarrow p \mid b$ e podemos escrever $b = p \cdot b_0$. Isso gera uma

contradição, pois $\frac{a}{b} = \frac{pa_0}{pb_0} = \frac{a_0}{b_0}$, a fração $\frac{a}{b}$ é redutível e $\sqrt[n]{p}$ possui uma representação com o denominador menor que a.
Concluímos que $\sqrt[n]{p}$ é irracional.

Problema 4.55. *(OI) Seja p um número primo. Mostre que não existem inteiros positivos a, b e c tais que $a^3 + pb^3 + p^2c^3 = 0$.*

Solução

Suponha que existem inteiros positivos (a, b, c) que satisfazem a equação e considere a solução com $a + b + c$ mínimo. Se houver mais de um tripla com soma mínimo tome qualquer um delas.
Veja que $p \mid 0 = a^3 + pb^3 + p^2c^3 \Rightarrow p \mid a^3 \Rightarrow p \mid a$, pois p é primo. Podemos escrever $a = pa_0$ e substituindo na equação $p^3a_0^3 + pb^3 + p^2c^3 = 0 \Rightarrow b^3 + pc^3 + p^2a_0^3 = 0$. Isso gera contradição, pois a tripla (b, c, a_0) também satisfaz a equação e $b + c + a_0 = b + c + \frac{a}{p} < a + b + c$ contradiz a minimilidade da solução.
Portanto, não existem inteiros positivos a, b e c tais que $a^3 + pb^3 + p^2c^3 = 0$.

Problema 4.56. *(OI) Pode um triângulo retângulo com lados inteiros ter área que seja o quadrado de um inteiro?*

Solução

Não existe e provaremos por contradição usando o seguinte lema.
Lema: a equação $x^4 = y^4 + z^2$ não possui solução com x, y e z inteiros positivos. Em outras palavras, como os expoentes são pares se $x^4 = y^4 + z^2$ para inteiros x, y e z então $xyz = 0$.
Demonstração: Provaremos usando Descenso Infinito de Fermat. Suponha que a equação tem solução positiva e tome uma das soluções com o menor x possível. Se $d = \text{mdc}(x, y) > 1$ então $(x', y', z') = (\frac{x}{d}, \frac{y}{d}, \frac{z}{d^2})$ também seria solução e com $x' < x$. Então $d = 1$ e a tripla pitagórica (x^2, y^2, z) é primitiva. Temos dois casos y par e z ímpar ou y ímpar e z par.

(i) Se y par. Existem inteiros positivos u e v primos entre si e de paridades distintas tais que $y^2 = 2uv$, $z = u^2 - v^2$ e $x^2 = u^2 + v^2$. Da segunda equação sabemos que existem r e s tais que $2u = 4r^2 \iff u = 2r^2$ e $v = s^2$. Mas $x^2 = u^2 + v^2$ também satisfaz as condições de uma tripla pitagórica primitiva e existem t e w primos entre e de paridades distintas tais que $u = 2tw$, $v = t^2 - w^2$ e $x = t^2 + w^2$. Veja que por u temos $tw = r^2 \Rightarrow t = (t')^2$ e $w = (w')^2$. Com isso $v = t^2 - w^2$ se torna $s^2 + (w')^4 = (t')^4$. Veja que $t' < t < x$ gerando contradição na minimplidade da

solução com x.

(ii) Se y ímpar. Novamente, existem u e v inteiros positivos primos entre si de paridades distintas para a tripla pitagórica, mas dessa vez $y^2 = u^2 - v^2$, $z = 2uv$ e $x^2 = u^2 + v^2$. Mas isso nos leva a $(xy)^2 = (u^2 + v^2)(u^2 - v^2) = u^4 - v^4 \iff u^4 = v^4 + (xy)^2$. Veja que $u^2 < u^2 + v^2 = x^2 \Rightarrow u < x$ e novamente chegamos numa solução menor que a mínima.

Após os dois casos, concluímos que a equação $x^4 = y^4 + z^2$ não tem solução positiva.

Voltando ao problema. Suponha que existe um triângulo retângulo com lados inteiros cuja área é um quadrado perfeito. Por triplas pitagóricas os lados desse triângulo são $(a, b, c) = (d2mn, d(m^2 - n^2), d(m^2 + n^2))$ com $c^2 = a^2 + b^2$ e $\text{mdc}(m, n) = 1$. Se a área é um quadrado perfeito podemos escrevê-la como k^2 e calcular esse mesmo valor usando os catetos.

$$k^2 = \frac{d2mn \cdot d(m^2 - n^2)}{2} \iff k^2 = d^2mn(m^2 - n^2)$$

Temos $d^2 \mid k^2 \Rightarrow d \mid k$. Temos $k = dk_0$ para algum inteiro positivo k_0 e

$$k_0^2 = mn(m^2 - n^2)$$

Veja que $\text{mdc}(m, n) = 1 \Rightarrow \text{mdc}(m^2 - n^2, m) = \text{mdc}(m^2 - n^2, n) = 1$. Se esse produto de três fatores dois a dois primos entre si é um quadrado perfeito então existem inteiros positivos x, y e z tais que

$$m = x^2, n = y^2 \text{ e } m^2 - n^2 = z^2$$

Substituindo chegamos em $x^4 = y^4 + z^2$. Pelo lema, essa equação não possui solução inteira positiva. Dessa forma, a suposição estava errada e esse triângulo não existe.

Problema 4.57. *(OI) Mostre que a equação $x^2 + y^2 + z^2 = x^2y^2$ não possui soluções inteiras positivas.*

Solução

Manipulando a equação temos

$$z^2 + 1 = x^2y^2 - x^2 - y^2 + 1 = (x^2 - 1)(y^2 - 1)$$

Se $x = 1$ ou $y = 1$, então $z^2 + 1 = 0$ que não tem solução. Suponha daqui para frente que $x, y \geq 2$.

Se x é par, então $x^2 - 1 \equiv 3 \pmod 4$ e existem um primo p da forma $4k+3$ que divide z^2+1. Isso é um absurdo, pois se p primo com $p \equiv 3 \pmod 4$ divide a soma de quadrados então tem que dividir cada quadrado implicando que p dividiria 1.
Se x ímpar, então $x^2 - 1 \equiv 0 \pmod 4$ implicando $4 \mid z^2+1$ e $z^2 \equiv 3 \pmod 4$. Isso é impossível, pois todo quadrado perfeito é congruente a 0 ou 1 módulo 4.
Por meio desses dois casos podemos concluir que a equação $x^2+y^2+z^2 = x^2y^2$ não possui soluções inteiras positivas.

Problema 4.58. *(OI) Mostre que não existem inteiros não nulos x, y, z, w tais que cumprem o sistema de equações* $\begin{cases} x^2+y^2=z^2 \\ x^2-y^2=w^2 \end{cases}$.

Solução

Suponha que esses inteiros existem. Como as equações usam expoentes pares podemos supor $x, y, z, w > 0$. Multiplicando as duas equações $z^2w^2 = (x^2+y^2)(x^2-y^2) \iff x^4 = y^4 + (zw)^2$. Isso implica que (x, y, zw) é solução da equação diofantina $A^4 = B^4 + C^2$. Pelo lema provado na resolução do problema 4.56, essa equação não possui solução positiva. Então o sistema de equações não possui solução com x, y, z e w inteiros não nulos.

Problema 4.59. *(A) Mostre usando o método do descenso infinito que a equação $x^4+y^4 = 2z^2$ não tem soluções não triviais.*

Solução

Suponha que a equação possui solução. Usando manipulações algébricas adequadas

$$z^4 = \left(\frac{x^4+y^4}{2}\right)^2 = \frac{x^8+2x^4y^4+y^8}{4} = \frac{x^8-2x^4y^4+y^8+4x^4y^4}{4}$$

$$\iff z^4 - (xy)^4 = \left(\frac{x^4-y^4}{2}\right)^2$$

Já usamos o Descenso Infinito de Fermat para provar no problema 4.56 que a equação $A^4 = B^4 + C^2$ só admite solução com $ABC = 0$. Pode ser $z = 0$ que implica $x = y = 0$. Pode ser $xy = 0$ que implica um deles igual a zero. Supondo que seja y, temos $x^4 = 2z^2$ que só tem solução com $x = z = 0$, pois $\frac{x^2}{z} = \sqrt{2}$ e este último é irracional. Se $\frac{x^4-y^4}{2} = 0$ então $x = \pm y$ e $2x^4 = 2z^2$ implicando $z = \pm x^2$.
Concluímos que as únicas soluções são as triviais $(x, y, z) = (0, 0, 0)$ e $(x, y, z) = (k, \pm k, \pm k^2)$ para todo k inteiro.

Problema 4.60. *(A) Sejam a e b inteiros positivos tais que ab divide a^2+b^2+2. Mostre que $\frac{a^2+b^2+2}{ab} = 4$.*

Solução

Se ab divide a^2+b^2+2, então existe um inteiro positivo k tal que $a^2+b^2+2 = kab \iff a^2-(kb)a+(b^2+2) = 0$. Esta é uma equação do segundo grau em a. Suponha que temos uma solução (a,b) com $a > b$. Isso significa que a equação $x^2-(kb)x+(b^2+2) = 0$ possui uma solução a inteira. Chamando de a' a outra solução temos $a+a' = kb \iff a' = kb-a$, o número a' é inteiro, e $a \cdot a' = b^2+2 \iff a' = \frac{b^2+2}{a} < b+\frac{2}{b}$. Veja que $b^2+2 > 0$ e $a > 0$ implicam a' positivo.

Assim, para $b > 2$ podemos reduzir uma solução (a,b) para outra (b,a') com $a' < b$. De qualquer solução podemos encontrar uma solução com $b \leq 2$ e o mesmo k.

Para $b = 1$ temos $k = \frac{a^2+3}{a}$ implicando $a \mid 3$ e $a = 1$ ou $a = 3$. Então as possibilidades são $k = \frac{1+3}{1} = 4$ ou $k = \frac{3^2+3}{3} = 4$.

Para $b = 2$ temos $k = \frac{a^2+6}{2a}$ temos $2 \mid a$ e $a \mid 6$ implicando $a = 2$ ou $a = 6$. As possibilidades são $\frac{2^2+6}{2\cdot 2} = \frac{5}{2}$ e $\frac{6^2+6}{2\cdot 6} = \frac{7}{2}$. Esses números não são inteiros e podemos concluir que nenhuma solução é reduzida para $b = 2$.

Logo, se $ab \mid a^2+b^2+2$, então $\frac{a^2+b^2+2}{ab}$ podemos reduzir (a,b) até uma solução com um dos termos igual a 2 mantendo o mesmo k. Assim, podemos concluir que $k = 4$.

Problema 4.61 (IMO1988). *(OA) Sejam a e b inteiros positivos tais que $ab+1$ divide a^2+b^2. Mostre que o número $\dfrac{a^2+b^2}{ab+1}$ é um quadrado perfeito.*

Solução

Suponha que existem a e b inteiros positivos tais que o número $\dfrac{a^2+b^2}{ab+1}$ é um inteiro $k \geq 2$ que não é um quadrado perfeito. Se $a = b$ então $a^2+1 \mid 2a^2$ e $\text{mdc}(a^2+1, a^2) = 1$. Dessa forma, $a^2+1 \mid 2$, $a = 1$ e $k = \frac{1^2+1^2}{1\cdot 1+1} = 1$ que é um quadrado perfeito. De agora em diante consideramos os casos em que são distintos e suponhamos sem perda de generalidade que $a > b$.

Tome a solução (a,b) tal que o máximo dos dois números é o menor possível. Considere a equação do segundo grau

$$x^2-(kb)x+(b^2-k) = 0$$

Uma das raízes é o a da solução. A outra é a'. Sabemos que a' é inteiro, pois $a' = kb-a$. O produto das raízes é b^2-k. Se $a' < 0$ então $kb < a$ e $b^2-k = aa' \leq -a$. Resulta que $k \geq a+b^2 > a > kb$. Mas isso é uma contradição. Se $a' = 0$ então $b^2-k = 0$ e k seria quadrado perfeito. Resta o caso $a' > 0$. Daí, $a' = \frac{b^2-k}{a} \leq \frac{b^2-1}{b+1} = b-1$. Dessa forma,

de uma solução (a, b) podemos gerar outra (b, a') menor. Isso gera uma contradição na hipótese de que há soluções k não quadrados.
Concluímos que se $k = \frac{a^2+b^2}{ab+1}$ é inteiro então é um quadrado perfeito.

Problema 4.62. *(OA) Seja k um número inteiro distinto de 1 e 3. Mostre que a equação $x^2 + y^2 + z^2 = kxyz$ não possui soluções inteiras positivas.*

Solução

Comecemos fazendo o caso $k > 3$. Se $x = y$ então $2x^2 + z^2 = kx^2z$ implica $x^2(kz - 2) = z^2$ e $x^2 \mid z^2 \Rightarrow x \mid z$. Existe z_0 tal que $z = xz_0$ então $2 + z_0^2 = kxz_0 \Rightarrow z_0 \mid 2$. Se $z_0 = 1$ então $3 = kx$ e $k = 1$ ou 3. Se $z_0 = 2$ então $6 = 2kx \iff kx = 3$ e $k = 1$ ou 3. Daqui para frente os números são distintos dois a dois.
Considere a solução positiva (a, b, c) tal que o máximo dos três é mínimo. Suponha sem perda de generalidade $a > b > c \geq 1$. Veja que $a^2 + b^2 + c^2 = kabc \iff a^2 - (kbc)a + (b^2 + c^2) = 0$. Isto quer dizer que a equação do segundo grau $x^2 - (kbc)x + b^2 + c^2 = 0$ tem a como uma de suas raízes. Seja a' a outra raiz. Veja que $a' = kbc - a$ é inteiro e $a' = \frac{b^2+c^2}{a}$ é positivo. A tripla (a', b, c) também é solução da equação. Considere a função do segundo grau $f(x) = x^2 - (kbc)x + b^2 + c^2$. Veja que de $c < b$ e $k \geq 4$ temos

$$f(b) = b^2 - kb^2c + b^2 + c^2 = 3b^2 - kb^2c = (3 - kc)b^2 < 0$$

Implicando que b está entre as duas raízes. Logo $a' < b < a$ e obtivemos uma tripla (a', b, c) em que o máximo dos três menor que o menor máximo dos três possível. Isso gera contradição, então podemos afirmar que não tem solução para $k > 3$.
Se $k = 2$. Suponha que a equação $x^2 + y^2 + z^2 = 2xyz$ tem solução positiva. Se os três forem ímpares temos $x^2 + y^2 + z^2$ ímpar e não há solução. Suponha sem perda de generalidade que x é par, então $x = 2x_0$ implica $4x_0^2 + y^2 + z^2 = 4x_0yz$. Temos $4 \mid y^2 + z^2$ e, por congruência módulo 4, $2 \mid y$ e $2 \mid z$. Mas fazendo $y = 2y_0$ e $z = 2z_0$ teremos $x^2 + y^2 + z^2 = 2xyz \iff x_0^2 + y_0^2 + z_0^2 = 4x_0y_0z_0$. Mas essa seria uma equação com $k > 3$ que já resolvemos.
Podemos conluir que a equação $x^2 + y^2 + z^2 = kxyz$ não tem solução para $k \neq 1$ e $k \neq 3$.

Problema 4.63. *(A) Determine todas as soluções inteiras de $x^4 - 2y^2 = -1$.*

Solução

Seja (x, y) uma solução da equação. Isolando y^2 e elevando ao quadrado

$$y^4 = \left(\frac{x^4 + 1}{2}\right)^2 = \frac{x^8 - 2x^4 + 1 + 4x^4}{4}$$

$$y^4 = \left(\frac{x^4-1}{2}\right)^2 + x^4$$

Então $(A, B, C) = (x, y, \frac{x^4-1}{2})$ é solução da equação $A^4 = B^4 + C^2$. Pelo lema provado na resolução do problema 4.56 que as soluções dessa equação satisfazem $ABC = 0$. Se $x = 0$ então a equação se torna $-2y^2 = -1$ que não tem solução. Se $y = 0$ então a equação se torna $x^4 = -1$ que também não tem solução. Se $\frac{x^4-1}{2} = 0$ então $x = 1$ e temos as únicas soluções $(x, y) = (\pm 1, \pm 1)$.

11

CONSIDERAÇÕES FINAIS

Sobre o livro Tópicos de Teoria dos Números da coleção do PROFMAT, ele é uma boa referência em português na área de Teoria dos Números, uma vez que possui muitos problemas em nível de olimpíada e nível de pesquisa. Embora existam alguns erros no texto e nos problemas propostos, isso não diminui a importância desse livro para o aprendizado deste assunto tão desafiador. Esperamos que este trabalho possa auxiliar nesse aprendizado.

Reunir e escrever essas soluções e classificar os problemas foi um processo longo e difícil, mas também enriquecedor e gratificante. Havia muitos problemas conhecidos, mas havia também muitos que o autor desconhecia e que o fizeram crescer como professor de matemática. Por isso, esperamos que este trabalho mesmo estudado a parte do livro Tópicos de Teoria dos Números também contribua positivamente na formação de alunos e professores.

Se torna claro que um material como este pode ajudar muitos leitores a se desenvolverem em Teoria dos Números e como resolvedores de problemas de matemática. Nesse sentido, existem várias possibilidades para trabalhos futuros. Seguindo em Teoria dos Números, poderiam ser feitas outras coletâneas de problemas considerando problemas mais recentes das olimpíadas nacionais e internacionais de matemática. Inclusive é possível relacionar muitos problemas recentes com problemas deste trabalho. Saindo de Teoria dos Números, poderiam ser feitas coletâneas de Álgebra, Combinatória ou Geometria. Embora existam mais materiais dessas áreas por conta de vestibulares, ainda há muito espaço para materiais voltados para resolução de problemas de olimpíada de matemática.

BIBLIOGRAFIA

[1] ANDREESCU, T.; KEDLAYA K. Mathematical Contests 1996-1997: Olympiad Problems and Solutions from around the World - American Mathematics Competitions, 1998

[2] BADARÓ, R. L., Do Zero ás Medalhas: Orientações aos Professores de Cursos Preparatórios para Olimpíadas de Matemática

[3] BIONDI, R. L.; VASCONCELLOS, L.; MENEZES-FILHO, N. A. Evaluating the impact of participation in the Brazilian Public School Mathematical Olympiad on math scores in students standardized tests. JOURNAL OF LACEA ECONOMIA (2012).

[4] BROCHERO MARTINEZ, F. E. et al. Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro - Projeto Euclides, IMPA, 2010.

[5] CAMINHA A. Equações diofantinas, Revista Eureka! No. 7, pp. 39-48.

[6] CAMPBELL, J. R.; VERNA, M. A. Academic Competitions Serve the US National Interests. Online Submission (2010).

[7] CAMPBELL, J. R. Early identification of mathematics talent has long-term positive consequences for career contributions. International Journal of Educational Research25.6 (1996): 497-522.

[8] CASTRO, F. Z., Uma Proposta de Sequência Didática para Treinamento Olímpico em Matemática

[9] CHEUNG, P. H. Problem-Solving Strategies: Research Findings from Mathematics Olympiads. Mathematical Medley, Vol 20 (2). Singapura, 1992.

[10] CUSICK, T. W.; FLAHIVE, M. E. *The Markoff and Lagrange spectra*, Math. Surveys and Monographs, no. 30, A.M.S. (1989).

[11] COUTINHO, S. C. *Números inteiros e criptografia RSA*, Coleção Computação e Matemática, SBM e IMPA (2000).

[12] CRAMÉR, H. *On the order of magnitude of the difference between consecutive prime numbers*, Acta Arithmetica 2: 23–46 (1936).

[13] DÍAZ, L. J.; REZENDE JORGE D. *Uma introdução aos Sistemas Dinâmicos via Frações Contínuas*, 26º Colóquio Brasileiro de Matemática, IMPA (2007).

[14] DJUKIC, D. et al. The IMO Compendium (A collection of Problems sugested for the International Mathematical Olympiads 1959-2009) , Springer 2011.

[15] HEFEZ, A. Elementos de Aritmética, 2a. edição. Textos Universitários, SBM (2005).

[16] MORAES, M. M. ANÁLISE DE ERROS EM PROBLEMAS DE ARITMÉTICA: UMA ABORDAGEM NA 2ª FASE DA OBMEP NO OESTE DO PARÁ

[17] MOREIRA, C. G. *O teorema de Ramsey*, Revista Eureka! 6, 23–29.

[18] MOREIRA, C. G. *Geometric properties of the Markov and Lagrange spectra*. Preprint-IMPA-2009.

[19] MOREIRA, C. G.; BROCHERO MARTINEZ, F. E.; SALDANHA N. C. Tópicos de Teoria dos Números - Coleção PROFMAT, SBM, 2012.

[20] PEREIRA, M, M. A RESOLUÇÃO DE QUESTÕES DAS OLIMPÍADAS DE MATEMÁTICA COM TEOREMAS DA ARITMÉTICA

[21] POLYA, G. A Arte de Resolver Problemas: um novo aspecto do método matemático. 2a edição, 1956. Princeton University Press, Princeton.

[22] POLYA, G., SZEGO, G., Problems and Theorems in Analysis II, Springer, Reprint of the 1976 Edition.

[23] D. H. J. Polymath, *Deterministic methods to find primes*, preprint, http://polymathprojects.files.wordpress.com/2010/07/polymath.pdf; veja também http://polymathprojects.org/2009/08/09/research-thread-ii-deterministic-way-to-find-primes/ e http://michaelnielsen.org/polymath1/index.php?title=Finding_primes

[24] POLITI, A.; MATTHEWS, J. C. F.; O'BRIEN, J. L. *Shor's Quantum Factoring Algorithm on a Photonic Chip*, Science 4 September 2009: Vol. 325. no. 5945, p. 1221.

[25] RIBENBOIM, P. *Selling primes*, Math. Mag. 68 (1995), 175–182. Traduzido como *Vendendo primos*, Rev. Mat. Univ. 22/23 (1997), 1–13.

[26] ROBERTS, J. Elementary Number Theory - a problem oriented approach, the MIT press, Cambridge, Massachusetts - London, England, 1977.

[27] SANTOS, J. P. O. Introdução à Teoria dos Números, 3a. edição. Coleção Matemática Universitária, IMPA (2010).

[28] SERRE, J. P. *On a theorem of Jordan*, Bull. Amer. Math. Soc. (N.S.) 40 (2003), no. 4, 429–440.

[29] SHEN, A.; VERESHCHAGIN, N. K. *Basic Set Theory*, AMS, 2002.

[30] SCHOENFELD, A. H., Mathematical Problem Solving. Academic Press, San Diego. 1985.

[31] SHOR, P. W., *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Comput. 26 (5), 1484-1509 (1997). Também em `arXiv:quant-ph/9508027v2`.

[32] SOUZA, G. L. RESOLUÇÃO DE PROBLEMAS SOBRE ARITMÉTICA PARA A OLIMPÍADA BRASILEIRA DE MATEMÁTICA DAS ESCOLAS PÚBLICAS OBMEP.

[33] TAO, T. Solving Mathematical Problems: a personal perspective. OUP, Oxford. 2006

[34] VINOGRADOV, I. M., Elements of Number Theory, Dover Publications, 2003.