UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO

CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA

PROFMAT – Mestrado Profissional em Matemática em Rede Nacional

Aspectos Interessantes de Teoria dos Números para o Ensino Básico

Manuel Simão Pilar Santamarinha

RIO DE JANEIRO

2016

Manuel Simão Pilar Santamarinha

Aspectos Interessantes de Teoria dos Números para o Ensino Básico

Trabalho de Conclusão de Curso apresentado ao Programa de Pós-graduação em Matemática PROFMAT da UNIRIO, como requisito para a obtenção do grau de MESTRE em Matemática.

Orientador: Silas Fantin
Doutor em Matemática – UNIRIO

Rio de Janeiro
2016

Santamarinha, Manuel Simão Pilar

Aspectos Interessantes de Teoria dos Números no Ensino Básico.
/ Manuel Simão Pilar Santamarinha – 2016

83. p.

1.Matemática 2. Álgebra. I. Título

CDU 536.21

Manuel Simão Pilar Santamarinha

ASPECTOS INTERESSANTES DE TEORIA DOS NUMEROS
PARA O ENSINO BASICO

Trabalho Final de Curso apresentado a Coordenação de Pós-Graduação *Stricto-sensu* da Universidade Federal do Estado do rio de Janeiro, como requisito parcial para a obtenção do titulo de Mestre em Matemática pelo Programa PROFMAT.

Aprovada em 01 de agosto de 2016.

BANCA EXAMINADORA

Dr. Silas Fantin – UNIRIO – Orientador

Dr. Fabio Xavier Penna - UNIRIO

Dr. Francisco Roberto Pinto Mattos – UERJ

Dedicatória

À minha amada esposa Vânia que me apoiou em todos os momentos e foi imprescindível para a conclusão deste curso. Aos meus filhos Daniel e Débora, que foram o meu maior estímulo nessa jornada superando e compreendendo minha ausência por várias vezes e ao meu neto, Davi, que me traz muita alegria.

Resumo

Neste trabalho de conclusão de curso do programa de Pós-Graduação em matemática PROFMAT da UNIRIO, apresentamos alguns aspectos de Teoria dos Números por considerarmos que este assunto permeia situações interessantes e desafiadoras para o aluno do Ensino Fundamental e Médio.

Os conceitos foram introduzidos de forma lúdica usando como recursos, por exemplo: jogos, dinâmicas, contos de Malba Tahan, com o objetivo de despertar o interesse dos alunos pelo tópico a ser estudado.

Entre os muitos tópicos dessa Teoria destacamos: Divisibilidade, Aritmética dos Restos, Cálculo de Potências, Equações Diofantinas Lineares, Teorema Chinês dos Restos e Números Primos.

Procuramos colocar os pontos mais interessantes de cada assunto numa linguagem mais adequada ao alunado que gostaríamos de atingir.

Palavras–chaves: Divisibilidade, Aritmética dos Restos, Equações Diofantinas, Teorema Chinês dos Restos e Números Primos.

Abstract

In this conclusion's work of Pos-Graduate course in mathematics PROFMAT UNIRIO program, we present some aspects of Number Theory because we consider that this matter goes through interesting and challenging situations for elementary and high school students.

He concepts were introduced in ludica form using resources such as games, dynamics, Malba Tahan tales, in order to arouse the interest of students by topic being studied.

Among the many topics of this Theory we include: Divisibility, Remains' Arithmetic, Exponent Calculation, Linear Diophantine Equations, Chinese Remainder Theorem and Prime Numbers.

We try to develop the most interesting topics of each subject in a more appropriate language for the students that we would like to achieve.

Keywords: Divisibility, Remains' Arithmetic, Diophantine Equations, Chinese Remainder Theorem and Prime Numbers.

Agradecimentos

Gostaria de agradecer a Deus pelo privilégio de conseguir chegar aonde cheguei dando-me saúde e perseverança para vencer as dificuldades apresentadas pela vida durante essa jornada e também a todos que de um modo ou de outro contribuíram para que esse trabalho se concretizasse. Gostaria de destacar alguns deles.

À minha esposa pelo apoio, pela força nos momentos mais difíceis que enfrentei durante o curso, pelo suporte emocional e principalmente por saber lidar com a minha ausência em muitos finais de semana.

Aos meus queridos filhos, Débora e Daniel, que sempre tiveram presentes na minha vida e me encantam todos os dias.

Ao meu neto Davi que mesmo sem ter a consciência necessária para lidar com a minha ausência, mostrava sempre o seu carinho por mim nas horas que mais precisava.

Aos meus amigos de curso Newton e Fábio que me ajudaram muito diante das minhas dificuldades apresentadas durante as aulas.

Ao professor e orientador Silas Fantin por quem tenho uma dívida impagável pelos seus ensinamentos, paciência e dicas durante a elaboração desse trabalho.

Aos professores da UNIRIO que receberam a nossa turma com muita dedicação.

A CAPES, pelo suporte financeiro, que permitiu a realização deste trabalho.

SUMÁRIO

INTRODUÇÃO

Mesmo a matemática tendo um enorme desenvolvimento nos últimos tempos, esse fato não impediu que crescessem as dificuldades em ensinar os conceitos matemáticos.

Entre os números inteiros há muitas propriedades e relações e a ciência cujo objetivo é estudá-las é a Teoria dos Números. Essa ciência serve de ferramenta em diversas áreas da matemática, tais como: Probabilidade, Álgebra, Sistemas dinâmicos, etc.. onde obtemos resultados significativos.

Com o objetivo de estudar alguns aspectos básicos da Teoria dos Números, analisando o processo de ensino e aprendizagem de tópicos importantes que devem ser desenvolvidos no Ensino Básico, foram investigados os seguintes itens: Divisibilidade, Aritmética dos Restos, Cálculo de Potências grandes, Teorema Chinês dos Restos, Equações Diofantinas Lineares e Números Primos.

Mesmo diante das dificuldades em ensinar os conceitos matemáticos por diversos motivos que não cabe nesse momento uma colocação a respeito, o objetivo deste trabalho é servir como um material de pesquisa para estudantes que estejam interessados em desvendar os prazeres de algumas descobertas da teoria dos números, pois a matemática se faz interessante para muitas pessoas pelas oportunidades que oferece para as descobertas assim como pela sua utilidade.

A seguir, faremos uma descrição sucinta do que será abordado em cada capítulo:

No Capítulo 1, abordaremos um conceito fundamental em teoria dos números que é o conceito de divisibilidade apresentado por Euclides de Alexandria. Iremos apresentar um jogo de origem da china antiga para dois jogadores. Foi o primeiro jogo a ser estudado matematicamente onde é possível obter uma estratégia vencedora utilizando o algoritmo da divisão euclidiana caso satisfaça algumas condições iniciais. Iremos apresentar também uma atividade denominada "mágica das moedas" que mostra uma aplicação da divisibilidade por dois.

No segundo capítulo, abordaremos o conceito de números primos; veremos que são em quantidade infinita e que são os alicerces da teoria dos números através do Teorema Fundamental da Aritmética, devido a Euclides.

Dando continuidade, no capítulo 3, veremos também uma das noções mais férteis da aritmética que permite identificar dois números inteiros sempre que a diferença entre eles for um múltiplo de um inteiro $m \geq 2$, e esta propriedade foi amplamente desenvolvida e explorada por Carl Friedrich Gauss (1777-1855). Veremos também como aplicação dessa aritmética, o cálculo efetivo de potências grandes.

Em seguida, no Capítulo 4 veremos se a equação de uma reta com coeficientes inteiros possui solução com coordenadas inteiras. Diofanto de Alexandria, que viveu no século III, foi um dos primeiros a se interessar por este tipo de problema, analisando se existe alguma solução, se o numero de soluções é em número finito ou infinito, e como determiná-las, e devido a isto, tais equações foram denominadas Equações Diofantinas em sua homenagem.

No capítulo 5 veremos como resolver sistemas de Equações Diofantinas, que podem modelar vários problemas interessantes, e aprender, como podemos resolvê-los através de um resultado clássico da literatura, conhecido como o Teorema Chinês dos Restos.

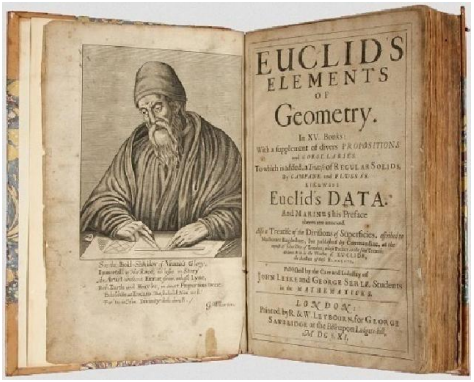
Finalmente, no capítulo 6, apresentaremos atividades e suas soluções, envolvendo aplicações de teoria dos números que podem ser aplicadas em sala de aula para alunos do Ensino Fundamental e Médio.

CAPÍTULO 1 – PRÉ-REQUISITOS

O presente capítulo destina-se a apresentar os pré-requisitos que serão necessários para a compreensão deste trabalho.

O berço da teoria dos números foi à Grécia. Nossa principal fonte de informações a respeito dos primeiros passos da matemática grega é o chamado Sumário Eudemiano de Proclo.

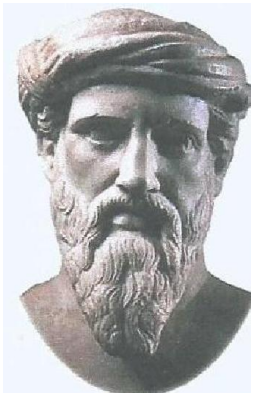
Esse Sumário consiste nas páginas de abertura do comentário sobre Euclides, Livro I, de Proclo e é um breve resumo do desenvolvimento da geometria grega desde os seus primeiros tempos até Euclides.


EUCLIDS
ELEMENTS
OF
Geometry.

A história dos trezentos (300) primeiros anos da matemática grega foi obscurecida pela grandeza dos "Elementos de Euclides", escritos por volta de 300 a.C. De fato, essa obra eclipsou tanto os trabalhos matemáticos gregos anteriores que eles acabaram sendo descartados e por fim se perderam para nós.

É difícil avaliar o débito da matemática grega primitiva para com a matemática oriental, tampouco está satisfatoriamente elucidado o caminho de transmissão de uma para outra, mas há evidências de uma conexão com o Oriente.

O próximo matemático ilustre a ser mencionado no Sumário Eudemiano é Pitágoras, envolto numa névoa tal de misticismo por seus seguidores que pouco se sabe sobre ele com algum grau de certeza. È possível que Pitágoras tenha sido discípulo de Tales, pois era cinquenta (50) anos mais novo do que este e morava perto de Mileto, onde viveu Tales.



As ideias do matemático e filósofo grego Pitágoras contribuíram para o desenvolvimento da Matemática moderna e da Filosofia ocidental. Seu objetivo era explicar todos os fenômenos naturais em termos matemáticos. Ele ficou conhecido sobretudo por sua fórmula sobre as proporções dos lados do triângulo retângulo; entretanto, muitos outros conceitos (como as progressões aritméticas e geométricas e os números quadrados), fundamentais na moderna Matemática, baseiam-se em ideias de Pitágoras. Com seus seguidores elaborara a matemática das **harmônicas,** ciência dos sons musicais, base da música ocidental contemporânea.

Parece que residiu algum tempo no Egito e ao retornar a Samos encontrou-a sob o domínio persa com o tirano Polícrates levando-o a emigrar para o porto marítimo de Crotona, uma colônia grega situada no sul da Itália onde fundou a escola Pitagórica.

Essa escola além de ser um centro de estudos de Filosofia, Matemática e Ciências Naturais, era também uma irmandade estreitamente unida por ritos secretos e cerimônias. Com o tempo, a influência e as tendências aristocráticas da irmandade tornaram-se tão grandes que forças democráticas do sul da Itália destruíram os prédios da escola fazendo com que a confraria se dispersasse.

Segundo um relato, Pitágoras fugiu para Metaponto onde morreu talvez assassinado, com uma idade avançada entre setenta e cinco e oitenta anos de idade. A irmandade, embora dispersa, continuou a existir por pelo menos mais dois séculos.

A filosofia Pitagórica baseava-se na suposição de que a causa última de várias características do homem e da matéria são os números inteiros.

Isso levava a uma exaltação e ao estudo das propriedades dos números e da aritmética, no sentido de teoria dos números, junto com a geometria, a música e a astronomia que constituíam as artes liberais básicas do programa de estudo Pitagórico.

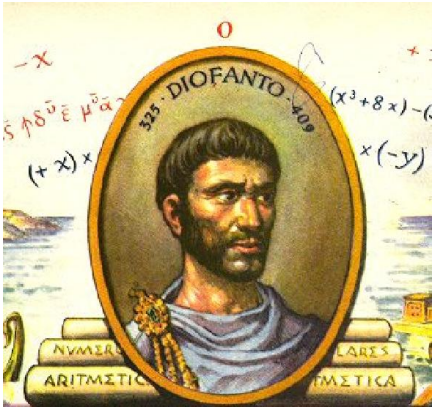
Como os ensinamentos da escola eram inteiramente orais e como era costume da irmandade atribuir todas as descobertas ao reverenciado fundador é difícil agora saber

exatamente que descobertas matemáticas se devem ao próprio Pitágoras e quais se devem a outros membros da confraria.

Os Pitagóricos estudaram as relações entre números do ponto de vista do que hoje denominamos Teoria dos Números.

Entre os principais estudiosos dessa teoria podemos citar Euclides de Alexandria (330 – 275 a. C), que organizou a obra monumental "Os Elementos" composta de 13 livros onde os livros VII, VIII e IX estão dedicados à Teoria dos Números.

Vários outros matemáticos gregos estudaram problemas da Teoria dos Números. Desses o mais importante foi sem dúvida Diofanto.



Diofanto de Alexandria teve uma importância enorme para o desenvolvimento da Álgebra e uma grande influência sobre os europeus que posteriormente se dedicaram à Teoria dos Números.

Diofanto escreveu três trabalhos: Aritmética, o mais importante do qual remanesceram seis dos treze livros que estavam na biblioteca de Alexandria no ano de 642 d. C. devido aos ataques dos cristãos; sobre Números Poligonais do qual restou apenas um fragmento e Porismas, que se perdeu. O trabalho "Aritmética" é uma abordagem analítica da teoria algébrica dos números que eleva o autor à condição de gênio em seu campo. Sua aritmética trata principalmente da solução de equações indeterminadas com coeficientes inteiros.

Diofanto tinha o gosto para questões que exigiam números inteiros a tal ponto de hoje tais problemas serem conhecidos como Equações Diofantinas. Gostava de inventar novos problemas além de debruçar também em problemas bem conhecidos.

De acordo com a memória de um resolvedor de problemas, o único detalhe sobre a vida de Diofanto que restou foi um enigma, que dizem ter sido gravado na lápide de seu túmulo:

> *"Deus lhe concedeu a graça de ser um menino pela sexta parte de sua vida. Depois por um doze avo, ele cobriu seu rosto com a barba. A luz do casamento iluminou o após a sétima parte e cinco anos depois do casamento. Ele concedeu-lhe um filho. Ah! Criança tardia e má, depois de viver metade da vida de seu pai o destino frio o levou. Após consolar sua mágoa em sua ciência dos números, por quatro anos,. Diofanto terminou sua vida."*

O desafio é calcular quanto tempo Diofanto viveu.

1.1 - DIVISIBILIDADE

Como a divisão de um número inteiro positivo por outro nem sempre é possível, se expressa esta possibilidade através da relação de divisibilidade.

Quando não existir uma relação de divisibilidade entre dois números, veremos que, ainda assim, será possível efetuar uma "divisão com resto pequeno", chamada de divisão euclidiana. O fato de sempre ser possível efetuar tal divisão é responsável por inúmeras propriedades que exploraremos agora.

Dados dois números naturais a e b com $a \neq 0$, diremos que a divide b, escrevendo $a|b$, quando existir $c \in \mathbb{N}$ tal que $b = a \cdot c$. Neste caso, diremos também que a é um divisor ou um fator de b ou, ainda, que b é um múltiplo de a.

Observe que a notação $a|b$ não representa nenhuma operação em $\mathbb{N}$, nem representa uma fração. Trata-se de uma sentença que diz ser verdade que existe c tal que $b = a \cdot c$. A negação dessa sentença é representada por $a \nmid b$, significando que não existe nenhum número natural c tal que $b = a \cdot c$.

Como exemplo, se quisermos dividir seis goiabas inteiras em partes iguais para duas pessoas, não teremos problemas, pois basta dar três goiabas para cada pessoa, pois $2|6$, visto que podemos escrever $6 = 2 . 3$.

Nem todos os problemas podem ser resolvidos dessa maneira Um exemplo seria tentar dividirmos vinte e uma calças para quatro pessoas. Não teríamos a opção de dividir uma calça em quatro pedaços. Como nem sempre é possível dividirmos um número natural por outro devemos expressá-la por uma relação de divisibilidade, pois podemos efetuar essa divisão com um resto "pequeno", chamada de divisão euclidiana. Neste caso poderíamos escrever que $21 = 5 \cdot 4 + 1$ onde 1 seria esse resto "pequeno" e portanto $4 \nmid 21$.

Percebemos que podemos descobrir o total de calças no começo se soubermos:

- Quantas pessoas receberão calças: 4
- Quantas calças recebeu cada pessoa: 5
- Quantas calças sobraram: 1

Fazendo as contas teremos que $4 \cdot 5 + 1 = 20 + 1 = 21$.

Se tivéssemos vinte calças para essas mesmas quatro pessoas daríamos cinco calças para cada uma delas, pois $20 = 4 .5$.

Agora, podemos entender o que é a divisão euclidiana entre números naturais:

- Um número que queremos dividir chamado de **dividendo** que representamos pela letra maiúscula $\boldsymbol{D}$**.**
- Um número que vai dividir o dividendo chamado de **divisor** que representamos pela letra minúscula **d**, onde $\boldsymbol{d}$ é sempre diferente de zero.
- O maior número de vezes que conseguimos colocar o divisor dentro do dividendo chamado de **quociente** ou resultado que representamos pela letra minúscula $\boldsymbol{q}$.
- O número de unidades que resta chamado de **resto** e que representamos pela letra minúscula $\boldsymbol{r}$ e que deve ser sempre menor que o divisor.

Dessa maneira podemos escrever que:

$$D = d \cdot q + r, \quad 0 \leq r < d$$

Exemplo 1.1.1: Se tivermos sessenta e cinco bombons para dividirmos entre sete pessoas, quantos bombons receberá cada pessoa? Quantos bombons sobrarão? Escreva a situação usando a equação de Euclides, ou seja, a divisão euclidiana, permite escrever $65 = 7 \cdot 9 + 2$**.** Desta forma, cada pessoa receberá 9 bombons e sobrarão 2 bombons.

Vamos usar a notação $a|b$ para indicar que o número a é divisor de b ,ou seja, a divide b e caso contrário $a \nmid b$ para indicar que a não é divisor de b ou seja, a não divide b. Assim, $7|63$ e $7 \nmid 65$. Pelo visto acima, podemos dizer que $7|63$, pois existe um número que multiplicado por 7 é igual a 63 e $7 \nmid 65$ pois não existe um número natural que multiplicado por 7 é igual a 65.

Nas aulas de matemática da Educação básica, quase sempre os alunos são estimulados a procurarem as respostas "certas" e "únicas" dos problemas que lhe são propostos. Não é muito comum eles serem confrontados com situações onde o problema apresenta inúmeras soluções ou mesmo não apresenta solução alguma. **Como exemplo, vamos ver o problema dos 3 marinheiros retirado do livro "O homem que calculava" de Malba Tahan** que, se não fosse uma informação adicional colocada no texto, apresentaria inúmeras soluções. **Malba Tahan** apresentou a resposta do problema, mas não fez um estudo detalhado sobre como chegarmos até ela. Ele fazia isso com frequência, com o intuito de forçar o leitor a pensar e refletir sobre a questão proposta. Trata-se de uma questão muito interessante e que pode ser usada com grande sucesso nas aulas do Ensino Fundamental.

Problema 1.1.2**:** *" Um navio que voltava de Serendibe, trazendo grande partida de especiarias, foi assaltado por violenta tempestade. A embarcação teria sido destruída pela fúria das ondas se não fosse a bravura e o esforço de três marinheiros que, no meio da tormenta, manejaram as velas com extrema perícia.*

O Comandante, querendo recompensar os denodados marujos, deu-lhes certo número de moedas. Esse número, superior a duzentos, não chegava a trezentos. As moedas foram colocadas numa caixa para que no dia seguinte, por ocasião do desembarque, o almoxarife as repartisse entre os três corajosos marinheiros.

Aconteceu, porém, que, durante a noite, um dos marinheiros acordou e lembrou-se das moedas e pensou: __ "Será melhor que eu tire a minha parte. Assim não terei ocasião de discutir ou brigar com os meus amigos". E, sem nada a dizer aos companheiros, foi, pé ante pé, até onde se achava guardado o dinheiro, dividiu-o em três partes iguais, mas notou que a divisão não era exata e que sobrava uma moeda. O melhor é jogá-la fora, pensou. Assim foi feito.

O 2° e o 3° marinheiros tiveram a mesma ideia e coincidentemente ocorreram as mesmas coisas que ocorreu com o 1° marinheiro.

Quando no dia seguinte, houve a divisão das moedas, sobrou também uma moeda que o almoxarife guardou como paga de seu trabalho. Nenhum dos marinheiros reclamou.

Quantas eram as moedas e quanto recebeu cada um dos marujos?"

Solução: Malba Tahan, ao final do livro, nos comentários sobre os problemas, diz que para essa questão usou a fórmula $M = 81k - 2$, onde M representa o número de moedas e k é um parâmetro natural não nulo, ou seja, que pode assumir os valores $1, 2, 3, 4, \ldots$. No livro, com o intuito de deixar o problema com uma única solução possível, foi dada a informação de que o número de moedas deveria estar entre $200\ e\ 300$. Nesse caso, basta substituirmos k por 3 para obtermos as 241 moedas da solução.

Investigando sobre a expressão proposta pelo ilustre matemático, que não é uma questão muito óbvia, nos deparamos com um excelente exercício de álgebra. Vejamos:

Sejam:

- M = total de moedas na caixa
- a = parte do 1° marinheiro
- b = parte do 2º marinheiro
- c = parte do 3° marinheiro
- r = restante final, que fora subdividido pelo almoxarife.

Sabemos que M foi dividido, pelo marinheiro, em três partes iguais, e que uma moeda foi lançada fora. Logo, $a = \frac{M-1}{3}$ ou $M = 3a + 1$.

Como o 1° marinheiro retirou a parte dele, (a), ficaram ainda duas partes iguais àquela $(2a)$. Como o segundo marinheiro voltou a dividir essa parte restante por três, jogando uma moeda fora, temos que a parte que ficou para esse marinheiro pode ser expressa por $b = \frac{2a-1}{3}$ ou ainda que $2a = 3b + 1$. Seguindo analogamente esse raciocínio até a divisão final, formaremos o seguinte sistema linear:

$$\begin{cases} M = 3a + 1 \\ 2a = 3b + 1 \\ 2b = 3c + 1 \\ 2c = 3r + 1 \end{cases}$$

Escrevendo $a, b\ e\ c$ em função de r, e, finalmente, M em função de r, após algumas contas termos obtido:

$$M = \frac{81r+65}{8}.$$

Trabalhando mais um pouco a expressão obtida, mesmo não sabendo o valor de r, teremos:

$$M = \frac{1}{8}(81r + 65)$$

$$M = \frac{1}{8}(80r + r + 64 + 1)$$

$$M = 10r + \frac{r}{8} + 8 + \frac{1}{8}$$

$$\boxed{M = 10r + 8 + \frac{1}{8}(r+1)} \rightarrow \boxed{A\ expressão\ obtida\ vai\ acarretar\ que\ r+1\ deve\ ser\ múltiplo\ de\ 8, ou\ seja, r+1 = 8k (k\ natural\ não\ nulo)}$$

Fazendo, agora, $r = 8k - 1$, e substituindo na expressão obtida, teremos:

$$M = 10.r + 8 + \frac{1}{8}(r+1)$$

$$M = 10 \cdot (8k - 1) + 8 + \frac{1}{8}(8k)$$

$$M = 80k - 10 + 8 + k$$

$$M = 81k - 2.$$

Verifique que obtivemos exatamente a expressão apresentada por **Malba Tahan** em seu livro. É claro que diversas outras respostas atenderiam ao problema caso não existisse a condição de que o número de moedas deveria estar entre $200\ e\ 300$.

O problema seria considerado, então, indeterminado. Por exemplo, se fizermos $k = 10$, termos a resposta $M = 81.10 - 2 = 808$ moedas. Verifique, acompanhando a história dos marinheiros, que tal resposta também atenderia ao interessantíssimo problema.

Vejamos outro problema retirado do livro "O homem que calculava" de Malba Tahan

Problema 1.1.3: *"Um Rajá deixou às suas filhas certo número de pérolas e determinou que a divisão se fizesse do seguinte modo:*

- *A filha mais velha tiraria uma pérola e um sétimo do que restasse;*
- *Viria, depois, a segunda e tomaria para si 2 pérolas e um sétimo do restante;*
- *A seguir a terceira jovem receberia 3 pérolas e um sétimo do que restasse.*

E assim sucessivamente.

As filhas mais moças apresentaram queixa a um juiz, alegando que por esse sistema complicado de partilha, elas seriam fatalmente prejudicadas.

O juiz que __ reza a tradição __ era hábil na resolução de problemas, respondeu prontamente que as reclamantes estavam enganadas e que a divisão proposta pelo velho rajá era justa e perfeita. E tinha razão. Feita a partilha, cada uma das herdeiras recebeu o mesmo número de pérolas."

Pergunta-se:

- *Qual é o número de pérolas?*
- *Quantas são as filhas do Rajá?*

Solução: Seja:

- x o número de pérolas do Rajá.
- As filhas do Rajá $F_1, F_2, F_3, \cdots$

Segundo o enunciado do problema, a filha mais velha F_1 retirou uma pérola e $\frac{1}{7}$ do restante. Então, como existiam x pérolas, ao retirar uma, ficariam $(x-1)$ pérolas.

Desse restante, pela regra estabelecida pelo Rajá, ela retirou $\frac{1}{7}$ delas, ou seja, $\frac{1}{7}(x-1)$.

Chamando de $n(F_1)$ o número de pérolas retiradas pela filha F_1, é óbvio que:

$$n(F_1) = 1 + \frac{1}{7}(x-1) = 1 + \frac{x-1}{7} = \frac{7+x-1}{7} = \frac{x+6}{7}.$$

Ora, restaram $x - n(F_1) = x - \left(\frac{x+6}{7}\right) = \frac{7x-x-6}{7} = \frac{6x-6}{7}$.

Agora, a filha F_2 vem e retira duas pérolas, conforme o enunciado. Resta então, a seguinte quantidade de pérolas:

$$\frac{6x-6}{7} - 2 = \frac{6x-6-14}{7} = \frac{6x-20}{7}.$$

Destas, ela retira $\frac{1}{7}$, ou seja, $\frac{1}{7}\left(\frac{6x-20}{7}\right) = \frac{6x-20}{49}$.

Portanto, o número de pérolas da filha F_2 será igual a:

$$n(F_2) = 2 + \frac{6x - 20}{49} = \frac{98 + 6x - 20}{49} = \frac{6x + 78}{49}.$$

Poderíamos agora, achar a expressão que define o número de pérolas da terceira filha F_3.

Mas, não precisa, porque o problema diz que "a divisão proposta pelo Rajá era justa e perfeita, o que significa que todas as filhas receberam quantidades iguais de pérolas.

Portanto, $n(F_1) = n(F_2) = n(F_3) = \cdots$

Então, como $n(F_1) = n(F_2)$, usando os resultados obtidos anteriormente, vem:

$$\frac{x + 6}{7} = \frac{6x + 78}{49}.$$

Efetuando e multiplicando, temos:

$$7x + 42 = 6x + 78 \Longrightarrow 7x + 42 - 6x - 78 = 0 \Longrightarrow x - 36 = 0 \Longrightarrow x = 36.$$

Portanto, são 36 pérolas.

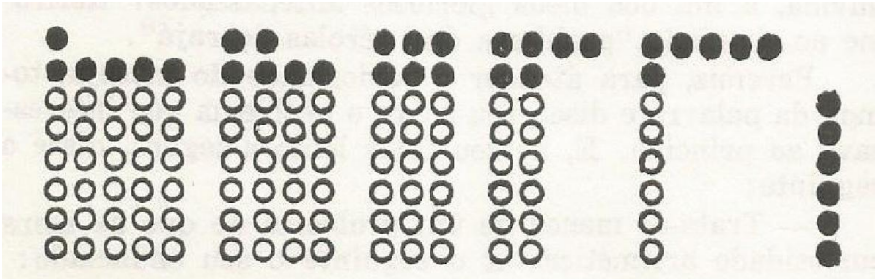
Vejamos então a distribuição das pérolas, conforme os dados do problema:

A filha mais velha F_1 retira 1 pérola e ficam $36 - 1 = 35$ pérolas. Destas, ela retira $\frac{1}{7}$ ou seja, $\frac{1}{7} \cdot 35 = 5$. Logo, a filha F_1 retirou $1 + 5 = 6$ pérolas.

Como é dito que todas as filhas recebem o mesmo número de pérolas, já que "a divisão proposta pelo Rajá era justa e perfeita", e como restaram $36 - 6 = 30$ pérolas, é claro que as 30 pérolas foram distribuídas com $\frac{30}{6} = 5$ filhas.

Portanto, o número total de filhas é igual a $1 + 5 = 6$.

Podemos visualizar essa divisão pela figura abaixo.



Não poderíamos deixar de colocar um problema de **Malba Tahan** envolvendo raciocínio lógico.

Problema 1.1.4: *"Tenho cinco lindas escravas; comprei-as há poucos meses, de um príncipe mongol. Dessas cinco encantadoras meninas, duas têm os olhos negros, as três restantes têm olhos azuis.*

- *As duas escravas de olhos negros, quando interrogadas, dizem sempre a verdade;*
- *as escravas de olhos azuis, ao contrário, são mentirosas, isto é, nunca dizem a verdade.*

Dentro de alguns minutos, essas cinco jovens serão conduzidas a este salão: todas elas terão o rosto inteiramente oculto por espesso véu.

O haic que as envolve torna impossível, em qualquer delas, o menor traço fisionômico.

Terás que descobrir e indicar, sem a menor possibilidade de erro, quais as raparigas de olhos negros e quais as de olhos azuis.

"Poderás interrogar três das cinco escravas, não sendo permitido, em caso algum, fazer mais de uma pergunta à mesma jovem."

As perguntas feitas e as respostas das escravas foram as seguintes:

- **Pergunta para a 1ª escrava: De que cor são os teus olhos?**

Resposta: A escrava respondeu em dialeto chinês, totalmente desconhecido pelos muçulmanos presentes.

Ficou combinado que as outras duas perguntas deveriam ser respondidas em árabe puro para que todos entendessem.

- **Pergunta para a 2ª escrava: Qual foi a resposta que a sua companheira acabou de proferir?**

Resposta: __ As palavras dela foram: "Os meus olhos são azuis".

- **Pergunta para a 3ª escrava: De que cor são os olhos dessas duas jovens que acabo de interrogar?**

Resposta: __ A primeira tem os olhos negros e a segunda olhos azuis!

Solução: Como a resposta da 1ª escrava só poderia ser " os meus olhos são negros" pois se tivesse olhos negros diria a verdade e se tivesse olhos azuis mentiria dizendo negros, concluímos que a 2ª escrava têm olhos azuis porque mentiu na sua resposta.

Pela resposta da 3ª escrava, "a primeira têm olhos negros e a segunda olhos azuis", percebemos que ela falou a verdade e portanto ela e a 1ª escrava têm olhos pretos e, consequentemente, as duas últimas escravas têm olhos azuis.

Proposição 1.1.5: Sejam $a, b \in \mathbb{N}^*$ e $c \in \mathbb{N}$. Tem-se que:

i) $1|c,\ \ a|a\ ,\ \ e\ \ a|0\ .$

ii) $se\ a|b\ \ e\ \ b|c,$ então $a|c.$

Prova: (i) Isto ocorre das igualdades $c = 1 \cdot c,\ \ a = a \cdot 1,\ \ e\ \ a \cdot 0 = 0.$

$(ii)\ a|b\ \ e\ \ b|c$ implica que existem $f, g \in \mathbb{N}$, tais que $b = a \cdot f\ \ e\ \ c = b \cdot g.$ Substituindo o valor de b da primeira equação na outra, obtemos $c = b \cdot g = (a \cdot f) \cdot g = a \cdot (f \cdot g)$, o que nos mostra que $a|c.$ ■

O item (i) da proposição acima nos diz que todo número natural não nulo é divisível por 1 e por si mesmo.

Proposição 1.1.6: Se $a, b, c, d \in \mathbb{N}$, com $a \neq 0\ \ e\ \ c \neq 0$, então $a|b\ \ e\ \ c|d \Longrightarrow a \cdot c|b \cdot d.$

Prova: Se $a|b\ \ e\ \ c|d,$ então $\exists\ f, g \in \mathbb{N}, b = a \cdot f\ \ e\ \ d = c \cdot g.$ Portanto, $b \cdot d = (a \cdot c)(f.g)$, logo, $a \cdot c \mid b \cdot d.$ ■

Proposição 1.1.7: Sejam $a, b, c \in \mathbb{N}$, com $a \neq 0$, tais que $a|(b+c)$. Então $a|b \Leftrightarrow a|c$.

Prova: Como $a|(b+c)$, existe $f \in \mathbb{N}$ tal que $b+c = f \cdot a$. Agora, se $a|b$, temos que existe $g \in \mathbb{N}$ tal que $b = a \cdot g$. Juntando as duas igualdades acima, temos $a \cdot g + c = f \cdot a = a \cdot f$, donde se segue que $a \cdot f > a \cdot g$, e, consequentemente, $f > g$. Portanto, da igualdade acima e do fato que $c \cdot (b-a) = c \cdot b - c \cdot a$, obtemos $c = a \cdot f - a \cdot g = a \cdot (f-g)$, o que implica que $a|c$, já que $f - g \in \mathbb{N}$.
A prova da outra implicação é totalmente análoga. ■

Proposição 1.1.8: Sejam $a, b, c \in \mathbb{N}$, com $a \neq 0$, e $b \geq c$, tais que $a|(b-c)$. Então $a|b \Leftrightarrow a|c$.
Prova: Como $a|(b-c)$ implica que existe $f \in \mathbb{N}$ tal que $(b-c) = a \cdot f$. Como $a|b$ implica que existe $g \in \mathbb{N}$ tal que $b = a \cdot g$. Assim, podemos afirmar que $a \cdot g - c = a \cdot f$, ou seja, $c = a \cdot (g-f)$ e consequentemente $a|c$, pois, nas condições dadas $(g-f) \in \mathbb{N}$. ■

Proposição 1.1.9: Se $a, b, c \in \mathbb{N}$, com $a \neq 0, e\ x, y \in \mathbb{N}$ são tais que $a|b$ e $a|c$, então $a|(xb + yc)$; e se $xb \geq yc$, então $a|(xb - yc)$.

Prova: Como $a|b$ e $a|c$ implicam que existem $f, g \in \mathbb{N}$ tais que $b = af$ e $c = ag$. Logo, $xb \pm yc = x(af) \pm y(ag) = a(xf \pm yg)$, o que prova o resultado, pois, nas condições dadas, $xf \pm yg \in \mathbb{N}$. ■
Proposição 1.1.10: Dados $a, b \in \mathbb{N}^*$, temos que $a|b \Longrightarrow a \leq b$.

Prova: De fato, se $a|b$, existe $c \in \mathbb{N}^*$ tal que $b = ac$. Como não existe nenhum número natural *n* tal que $0 < n < 1$ e como $c \geq 1$, segue-se que $a \leq ac = b$. ■

1.2 – DIVISÃO EUCLIDIANA

Mesmo quando um número natural a não divide o número natural b, Euclides, nos seus Elementos, utiliza, sem enunciá-lo explicitamente, o fato de que é sempre possível efetuar a divisão de b por a, com resto.

Este resultado, cuja demonstração segue abaixo, não só é um importante instrumento na obra de Euclides, como também é um resultado central da teoria.

Antes de começarmos a mostrar a existência dos números q e r precisamos esclarecer que: Considerando um subconjunto S de $\mathbb{N}$, dizemos que um número natural a é um menor elemento de S se possui as seguintes propriedades: $i)\ a \in S\ \ e\ \ ii)\ \forall n \in S, a \leq n.$

A Propriedade da Boa Ordem afirma " Todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento."

Teorema 1.2.1 (Divisão Euclidiana): Sejam a e b dois números naturais com $0 < a < b$. Existem dois únicos números naturais q e r tais que $b = a \cdot q + r,\ com\ r < a.$

Prova: Suponha que $b > a$ e considere, enquanto fizer sentido, os números $b, b-a, b-2a, \ldots, b - n \cdot a, \ldots$

Pela propriedade da Boa Ordem, o conjunto S formado pelos elementos acima tem um menor elemento $r = b - q \cdot a$. Vamos provar que r tem a propriedade requerida, ou seja, que $r < a$.

Se $a|b$, então $r = 0$ e nada mais temos a provar. Se, por outro lado, $a \nmid b$, então $r \neq a$, e, portanto, basta mostrar que não pode ocorrer $r > a$.

De fato, se isto ocorresse, existiria um número natural $c < r$ tal que $r = c + a$.

Consequentemente, sendo $r = c + a = b - q \cdot a$, teríamos $c = b - (q+1) \cdot a \in S, com\ c < r$, o que é uma contradição pelo fato de r ser o menor elemento de S. Portanto, temos que $b = a \cdot q + r\ \ com\ \ r < a$, o que prova a existência de q e r.

Agora, vamos provar a unicidade.

Note que, dados dois elementos distintos de S, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a, é pelo menos a. Logo, se $r = b - a \cdot q\ \ e\ \ r' = b - a \cdot q'$,

$com\ r < r' < a$, teríamos $r' - r \geq a$, (basta fazer $(b - a \cdot q') - (b - a \cdot q)$) o que acarretaria $r' \geq r + a \geq a$, o que é um absurdo.

Portanto $r = r'$. Daí segue-se que $b - a \cdot q = b - a \cdot q'$, o que implica que $a \cdot q = a \cdot q'$ e, portanto, $q = q'$. ■

Nas condições do teorema acima, os números $q\ e\ r$ são chamados, respectivamente, de quociente e de resto da divisão de b por a. Note que o resto da divisão de b por a é zero se, e somente se, a divide b.

Note que a demonstração do teorema fornece um algoritmo (um procedimento) para calcular o quociente e o resto da divisão de um número por outro, por subtrações sucessivas.

Corolário 1.2.2: Dados dois números naturais a e b com $1 < a \leq b$, existe um número natural n tal que $na \leq b \leq (n + 1)a$.

Prova: Pela divisão euclidiana, temos que existem $q, r \in \mathbb{N}$ com $r < a$, univocamente determinados, tais que $b = a \cdot q + r$. Basta agora tomar $n = q$. ■

Existem alguns problemas interessantes sobre divisibilidade que veremos a seguir. O **primeiro deles é o jogo de Nim.**

Trata-se de um antigo jogo chinês de palitos jogado por duas pessoas ou equipes. Este jogo foi objeto, em 1901, de um artigo científico na prestigiosa revista Annals of Mathematics, de autoria de C. L. Bouton, mostrando que há uma estratégia que se adotada pelo jogador que inicia o jogo, ele sempre ganhará.

Há várias versões deste jogo, cada uma com uma estratégia própria. Vamos adaptar esse jogo de Nim para o jogo das correntes retirado do livro "Jogos e Resolução de Problemas: Uma estratégia para as aulas de Matemática" – Júlia Borin

Material: um tabuleiro para duas equipes oponentes e lápis para marcar as jogadas.

Meta: não marcar o último elo.

Regras:

O jogo, disputado por dois jogadores, é estabelecido da seguinte forma:

I. A quantidade de elos deve ser um número natural N .
II. O jogador 1 marca um X e o jogador 2 marca um Y, para qualquer quantidade de elos entre 1 e n com $n > 1$ arbitrário.

III. Supõe-se, ainda, que nem N nem $N-1$ sejam múltiplos de $(n+1)$.

IV. O vencedor será aquele que não marcar o último elo da corrente.

Pergunta natural: Existe alguma estratégia vencedora para o jogador 1. Em caso afirmativo, exiba uma estratégia vencedora.

Resposta: Sim. Segue uma estratégia vencedora:

Seja q o quociente e r o resto da divisão euclidiana de N por $n+1$. Isto é,

$$N = q.(n+1) + r$$

Da condição III das regras, segue que $r > 0$ e $r > 1$, logo $(r-1) > 0$. Desta forma, obtemos q grupos de $(n+1)$ elos, e como $r-1>0$ podemos escrever

$$r = (r-1) + 1,$$

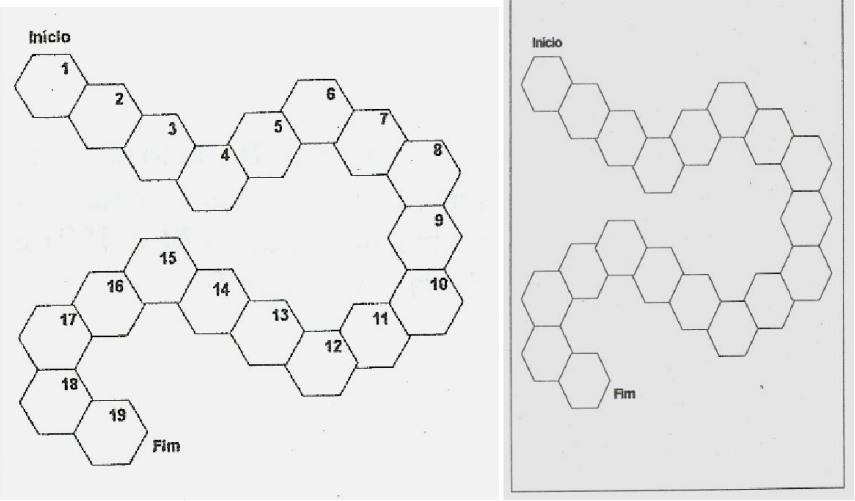
logo podemos reescrever N da seguinte forma:

$$N = q(n+1) + (r-1) + 1$$

O jogador 1 marca X nesse grupo de $(r-1)$ elos, ficando $q(n+1)+1$ elos sem marcação.

O jogador 2 ao marcar Y numa quantidade de $1\,a\,n$ elos, o jogador 1 irá marcar o complementar de $(n+1)$ em função da marcação do Jogador 2, fazendo que, no final, sobre 1 elo na vez do jogador 2, provocando a sua derrota.

Vejamos um exemplo. Considere uma corrente com $N = 19$ elos, onde cada jogador poderá assinalar de 1 a 4 elos em cada jogada.



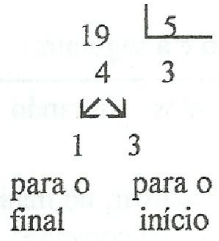
Qual a estratégia vencedora a ser usada caso a sua equipe seja a primeira a jogar?

Como podemos perceber temos dezenove elos e cada equipe pode marcar de um a quatro elos.

Assim é possível para qualquer equipe sempre fechar cinco elos (um mais quatro) da corrente, ou seja, se a outra equipe marcar dois elos ela marca três elos, pois $2 + 3 = 5$.

Se a outra equipe marcar um elo ela marca quatro elos, pois $1 + 4 = 5$. Assim vão ser formados alguns grupos de cinco elos e sobrarão alguns elos. Quantos? Basta fazer a divisão euclidiana de 19 por 5. Assim $19 = 3 \cdot 5 + 4$.

Podemos perceber que a estratégia vencedora passa pelo resto, pois nesse resto estará o elo final que não deve ser marcado e os outros $4 - 1 = 3$ elos que devem ser marcados no início do jogo.



Então a sequência vencedora seria $3 \rightarrow 8 \rightarrow 13 \rightarrow 18$.
Assim é o resto 4 que é importante.

Questões para serem refletidas em aula:

- Será que, para vencer, é necessário ser o primeiro jogador, independente do número de elos que a corrente tenha?
- O número de elos, permitido para marcar a jogada, influencia no resultado?
- E se quem marcar o último elo ganhar o jogo, a estratégia vencedora mudaria?

Agora vamos voltar ao jogo de Nim original.
Nesta versão, este jogo consiste em colocarmos sobre uma mesa três fileiras com quantidades diferentes de palitos. Este jogo é para dois participantes, sendo assim, perde o que retirar o último palito. É necessário seguir as seguintes regras:
- Cada jogador, em cada jogada, deverá escolher uma fileira para retirar os palitos, sem restrição de quantidade (no mínimo um e no máximo toda fileira).

- Os jogadores alternam suas jogadas.

Exemplo:

Fileira 1: $|||||||||$ $(9\ palitos)$

Fileira 2: $||||||$ $(6\ palitos)$

Fileira 3: $||||$ $(4\ palitos)$

Estratégia para vencer o jogo:

- No exemplo citado acima, converteremos as quantidades de palitos em cada fileira por sua representação em binário:

Fileira 1: 1 0 0 1 $(9\ em\ binário)$

Fileira 2: 1 1 0 $(6\ em\ binário)$

Fileira 3: + 1 0 0 $(4\ em\ binário)$

1 2 1 1

Somando- se as colunas teremos um resultado com dígitos entre 0 e três, no caso, obtivemos "1 2 1 1".

Chamaremos de combinação segura, aquela que obtiver como resultado das somas das colunas apenas os dígitos "2" e "0".

Para vencer o jogo, basta o jogador transformar este resultado (1 2 1 1) numa combinação segura, retirando palitos.

Observe que, como não se podem adicionar palitos, teremos que retirar palitos da fileira 1, de modo que tenhamos uma combinação segura.

XXX

1 1 0

1 0 0

2 2 0

Logo, na fileira 1 devemos ter "0 1 0", que representa 2 palitos (verifique que esta é a única solução possível). Para isso, basta retirarmos 7 palitos da fileira 1.

Após conseguir uma combinação segura, o próximo jogador não poderá fazer uma nova combinação segura.

Não é difícil observar isso, pense que em binário, para diminuir um número somente podemos mudar de "0" para "1" e vice- versa, logo, pelo menos um "1" se tornaria "0", e esta coluna, que antes tinha soma "2" passa a ter soma "1" que não é um dígito de combinação segura.

Até agora conseguimos observar que se um jogador fizer uma combinação segura, poderá mantê- la, e por que então ele ganhará o jogo?

Adicionaremos algumas exceções de combinação segura: se a soma der 3, isto é , linha1: 1 palito, linha 2: 1 palito e linha 3: 1 palito será uma combinação segura, e a menor combinação segura será a de apenas um palito no total.

Também, como exceção, se a soma das linhas derem 2, não será uma combinação segura.

Vamos analisar o que ocorrerá: seja P uma combinação segura e I uma não segura, A o jogador que deixa na mesa uma combinação segura e B o outro jogador, teremos o seguinte:
P⟶ I⟶ P⟶ I ... como os palitos estão diminuindo, poderemos chegar as seguintes combinações finais que garantirão o desfecho do jogo:

a) Se uma das linhas for eliminada pelo jogador B, como ele não consegue deixar uma combinação segura, significa que nas linhas restantes existe um número diferente de palitos, logo, basta o jogador A igualá-los, fazendo assim, uma nova configuração segura (salvo a única exceção já citada).
b) Se o jogador A eliminar uma fila, significa que temos a configuração final do item anterior, ou seja, ficamos com 2 filas com a quantidade igual de palitos.

Analisando os casos a) e b), a sequência vai convergir para os seguintes resultados:

- O jogador A compõe a menor configuração segura do tipo soma = "dois" e "zero" , que é deixar dois palitos em cada fileira, nesta condição, o jogador B executará mais uma jogada e permitirá ao jogador A compor a última e menor combinação segura que é a de apenas um palito na mesa, e ganhará o jogo.

- O jogador B elimina uma fileira inteira, assim, restando palitos apenas numa fileira, basta o jogador A deixar somente um palito nesta, e vencerá.

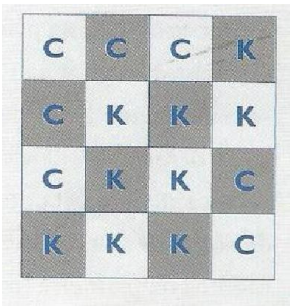
c) Se nenhuma fileira for eliminada, a menor configuração segura do tipo soma= ″0″ *ou* "2", será: as linhas com $1, 2\ e\ 3$ palitos, respectivamente, nesta situação, o jogador B, se retirar uma linha inteira, recorre no caso a) e perderá o jogo, se retirar um palito da linha que tem 3, deixará duas linhas com 2 palitos, levando o jogador A ao procedimento do item b) ;

Finalizando, se o jogador B retirar ou dois palitos da linha que tem três, ou um palito da linha que tem dois, permitirá ao jogador A realizar a configuração segura de soma= ″3″ (ou seja, um palito em cada linha), e vencerá o jogo em mais uma jogada.

Conhecendo esta estratégia, basta conhecer os representantes "binários", fazer algumas continhas de cabeça e vencer o jogo.

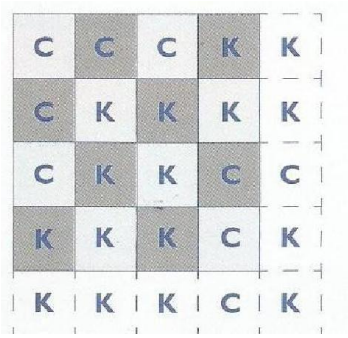
Mágica com moedas

Sou o adivinho e você o meu ajudante. Disponha 16 moedas aleatoriamente em um tabuleiro 4 × 4. Suponha que fique como na figura abaixo, sendo K = cara e C = coroa.



A seguir, escolha uma moeda e troque a sua face no tabuleiro, sem que eu saiba. Meu objetivo é tentar "adivinhar" a moeda que você virou no tabuleiro.

Antes, porém, de você escolher em segredo a moeda a ser virada, vou pegar mais moedas e acrescentar uma linha abaixo e uma coluna à direita para "tornar as coisas mais difíceis".

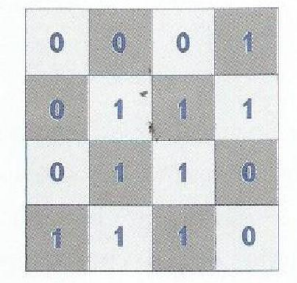


Finjo que esse acréscimo tenha se dado de forma aleatória. Agora sim, viro de costas e peço que você escolha e vire uma dessas moedas, podendo ser inclusive a das que eu inclui.

Pronto, olho para o tabuleiro e descubro qual moeda foi virada. Como?

Explicando a magia.

Em primeiro lugar, eu troco mentalmente C por 0 e K por 1.



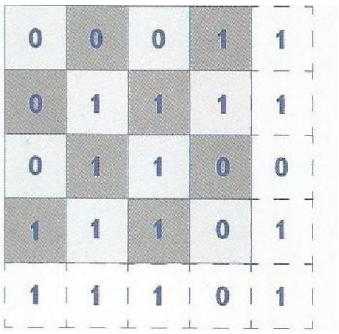
Em seguida, abaixo de cada coluna, acrescento o resto da divisão da soma dos seus elementos por 2.

Por exemplo, na primeira coluna, a soma de seus elementos é igual a 1, e o resto da divisão por 2 será também 1.

Já na quarta coluna, a soma vale 2, e o resto é 0. Faço o mesmo para cada linha: acrescento à direita de cada linha o resto da divisão da soma de seus elementos por 2.

A soma dos elementos da primeira linha é 1, cujo resto da divisão por 2 é igual a 1.

A soma dos elementos da 4ª linha é 3, tendo como resto 1. A matriz fica assim:



Obviamente esses números estão apenas na minha cabeça, pois, de fato, o tabuleiro é constituído de moedas, de modo que vou acrescentar caras onde seriam os números 1(K) e coroas onde seriam os números 0(C).

E quanto ao elemento do canto inferior direito? Esse seguirá o mesmo princípio: se a linha que foi acrescentada à sua esquerda somar um número par, acrescento o 0(coroa C), se somar um número ímpar acrescento o 1(cara K).

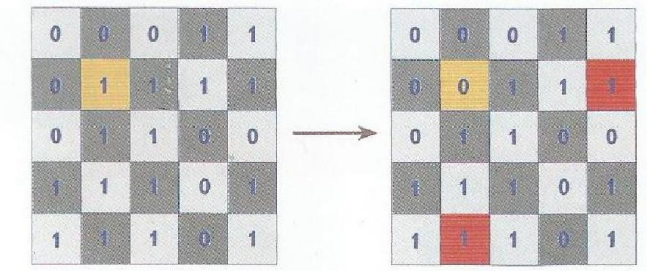
A surpresa é que vale o mesmo resultado para a coluna acima desse elemento do canto inferior direito: se a soma dos seus elementos for par será par também a soma dos elementos da linha, o mesmo se dando se der ímpar.

No mesmo caso, a soma dos elementos da linha e, portanto da coluna também, é ímpar; logo, deixa resto 1 na divisão por 2, e por isso devo acrescentar, no canto inferior direito, o número 1 (em verdade uma cara).

Antes, suponha que você tenha invertido, por exemplo, o elemento da 2ª linha e 2ª coluna, de 1 para 0, em amarelo na figura a seguir (de fato, de cara para coroa).

O meu trabalho será conferir em qual linha e em qual coluna o resto da divisão da soma dos elementos não bate.

Trocando o 1 por 0 na segunda linha e segunda coluna, os elementos que acrescento abaixo dessa coluna e à direita dessa linha, que eram os restos da divisão das respectivas somas por 2, em vermelho na matriz a seguir, ficam errados, acusando qual moeda você escolheu.



Análise inteiramente análoga é feita se é escolhida qualquer das moedas que foi acrescentada.

Vejamos agora a demonstração matemática da coincidência do elemento do canto inferior direito.

Seja m um inteiro fixado, $m > 2$. Suponha que a matriz inicial escolhida pelo ajudante seja de ordem $(m-1) \times (m-1)$.

Considere que a soma dos elementos da coluna j, $\sum_{i=1}^{m-1} a_{ij}$, deixe resto a_{mj}, para cada j de 1 até $m-1$, na divisão por 2.

Em notação de congruências, temos:

$$\sum_{i=1}^{m-1} a_{ij} \equiv a_{mj}(mod2).$$

Então, esses elementos $a_{mj}\ e\ a_{im},\ i\ e\ j\ de\ 1\ até\ m-1$, é que são acrescentadas abaixo das colunas j, e à direita das linhas i, respectivamente.

A questão é saber qual será o elemento do canto inferior direito a_{mn}.

Ora, observe a propriedade:

Propriedade P: Se dois números $A\ e\ B$ deixam restos $r\ e\ s$ na divisão por Q, respectivamente, então a soma $A + B$ deixa o mesmo resto que a soma $r + s$ na divisão por Q.

Vamos verificar a propriedade:

Sejam $A = tQ + r,\ B = uQ + s,\ r + s = wQ + z,\ sendo\ r, s\ e\ z$ os restos das divisões de $A\ por\ Q,\ B\ por\ Q\ e\ r + s\ por\ Q$, respectivamente; logo,

$$A + B = (t + u)Q + (r + s) = (t + u + w)Q + z.$$

Por indução, vale para a soma de mais termos.

Em notação de congruências, a propriedade P pode ser reescrita assim:

Se $A \equiv r(modQ)\ e\ B \equiv s(modQ), então$:

$$(A + B) \equiv (r + s)(modQ).$$

Podemos agora provar a afirmação: a soma dos elementos da linha que foi acrescentada, $\sum_{j=1}^{m-1} a_{mj}$, deixa o mesmo resto na divisão por 2 que a soma dos elementos que foi acrescentada, $\sum_{i=1}^{m-1} a_{im}$.

Denotemos por $C_1, C_2, \cdots, C_{m-1}$ a soma dos elementos das colunas $1, 2, \cdots, m-1$, respectivamente; denotemos por $L_1, L_2, \cdots, L_{m-1}$ a soma dos elementos das linhas $1, 2, \cdots, m-1$, respectivamente. Se S é a soma de todos os elementos da matriz inicial, é claro que

$$S = C_1 + C_2 + \cdots + C_{m-1} = L_1 + L_2 + \cdots + L_{m-1}.$$

Pela propriedade P, temos

$$S = (C_1 + C_2 + \cdots + C_{m-1}) \equiv \sum_{j=1}^{m-1} a_{mj} (mod 2)$$

$$S = (L_1 + L_2 + \cdots + L_{m-1}) \equiv \sum_{i=1}^{m-1} a_{im} (mod 2)$$

Então ,

$\sum_{j=1}^{m-1} a_{mj} \equiv \sum_{i=1}^{m-1} a_{im} (mod 2)$, o que prova a afirmação acima e define o elemento a_{mn}.

Observação: Numa aula no ensino médio, as congruências utilizadas podem ser substituídas por: "deixa o mesmo resto que."

CAPÍTULO 2 - NÚMEROS PRIMOS

Nos livros didáticos e nas salas de aula, os números primos eram abordados diretamente pela definição (números com dois, e apenas dois divisores distintos).

Dessa maneira, não se percebia sua importância, não se compreendia o propósito de estudá-los e até o nome primo soava estranho aos alunos.

As pesquisas históricas indicam que os pensadores gregos de 2 500 anos atrás foram os primeiros a estudar esses números pelo simples prazer de conhecê-los, mas dificilmente algum outro tipo de número encerrará tanta atratividade e mistério em torno de si.

Vamos abordar alguns pontos, deixando outros por não fazer parte do interesse do nosso trabalho.

Mas o que é um número primo?

É um número natural maior do que um (1) cujos únicos fatores (divisores) são um (1) e o próprio número. Determinaremos alguns números primos usando o Crivo de Erastotenes e apresentaremos os conceitos de Máximo Divisor Comum (MDC) e Mínimo Múltiplo Comum (MMC) relacionado com a noção de números primos.

Lembre-se que se a e b dois são dois números naturais com $0 < a < b$, então existem dois únicos números naturais q e r tais que $b = a \cdot q + r,\ com\ r < a,$ onde os números $q\ e\ r$ são chamados, respectivamente, de quociente e de resto da divisão de $b\ por\ a$. Note que o resto da divisão de $b\ por\ a$ é zero se, e somente se, $a\ divide\ b$.

2.1 - Máximo Divisor Comum

Dados dois inteiros positivos $a\ e\ b$, eles certamente têm um divisor comum que é o 1. Como todos os divisores comuns de $a\ e\ b$ são menores ou iguais a a e/ou a b, então, existe o maior divisor comum de $a\ e\ b$. Este número é designado por $mdc(a, b)$.

Dados dois números naturais $a\ e\ b$, não simultaneamente nulos, diremos que o número natural $d \in \mathbb{N}^*$ é um divisor comum de $a\ e\ b$ se *d/a* e *d/b.*

Como exemplo, os números $1, 2, 3\ e\ 6$ são divisores comuns de $12\ e\ 18$.

A definição que se segue é exatamente a definição dada por Euclides nos Elementos e se constitui em um dos pilares da sua aritmética.

Definição 2.1.1 (Máximo divisor comum): Diremos que d é um máximo divisor comum (mdc) $de\ a\ e\ b$ se possuir as seguintes propriedades:

a) d é um divisor comum de a e de b, e,

b) se c é um divisor comum de $a\ e\ b, então\ c|d$.

Portanto, se $d = mdc\ (a, b)$ e c é um divisor comum desses números, então $c \leq d$. Isto nos mostra que o máximo divisor comum de dois números é efetivamente o maior dentre todos os divisores comuns desses números.

Em particular, isto nos mostra que, se $d\ e\ d'$ são dois mdc de um mesmo par de números, então $d \leq d'\ e\ \ d' \leq d$, e, consequentemente, $d = d'$. Ou seja, o mdc de dois números, quando existe, é único. ■

Exercício 2.1.2: Como aplicação, podemos ver o seguinte problema:

- Dividindo-se 7040 $por\ n$, obtem-se resto 20.
- Dividindo-se 12384 também por n, obtem-se resto 9.

Determine o valor de n.

Solução: Aplicando o teorema da divisão temos que:

- $7040 = nq_1 + 20 \implies nq_1 = 7020 \quad (n > 20)$
- $12384 = nq_2 + 9 \implies nq_2 = 12375 \ \ (n > 9)$

Como n é divisor comum de $7020\ \ e\ 12375$, n é divisor do mdc desses números. Como

$$mdc\ (7020, 12375) = 45$$

e sendo n divisor de 45 e $n > 20$, temos que $n = 45$.

O Maximo divisor comum de $a\ e\ b$, será denotado por $mdc(a, b)$. Como o $mdc\ (a, b)$ não depende da ordem em que $a\ e\ b$ são tomados, temos que $mdc(a, b) = mdc(b, a)$.

Em alguns casos particulares, é fácil verificar a existência do mdc. Por exemplo, se $a\ e\ b$ são números naturais, tem-se claramente que $mdc(0,a) = a,\ mdc(1,a) = 1$ e que $mdc\ (a,a) = a$. Mais ainda, temos que $\frac{a}{b} \Leftrightarrow mdc(a,b) = a$.

De fato, se $a|b$, temos que a é um divisor comum de $a\ e\ b$, e, se c é um divisor comum de $a\ e\ b$, então c divide a, o que mostra que $a = mdc(a,b)$.

Reciprocamente, se $(a,b) = a$, segue-se que $a|b$.

Para provar a existência do máximo divisor comum, Euclides utiliza, essencialmente, o resultado abaixo.

Lema de Euclides 2.1.3: *Sejam* $a, b, n \in \mathbb{Z}$. *Então*

$$mdc\ (a,b) = mdc(a, b - na).$$

Prova: Seja $c = mdc\ (a,b)\ \ e\ d = mdc(a, b - na)$. Como:

$d = mdc(a, b - na) \Rightarrow d \mid a\ e\ d \mid (b - na)$

$\Rightarrow\ d \mid b\ \ pois\ b = (b - na) + na$

$\Rightarrow\ d \mid a\ \ e\ \ d \mid b$

$\Rightarrow\ d \mid c$

Por outro lado, como:

$c = mdc\ (a,b) \quad \Rightarrow\ c \mid a\ \ e\ \ c \mid b$

$\Rightarrow\ c \mid a\ \ e\ \ c \mid (b - na)$

$\Rightarrow\ c \mid d$

Como c e d são ambos positivos, segue que $c = d$. ■

Exercício 2.1.4: Mostre que, para todo $n \in \mathbb{N}$, a fração $\frac{21n+4}{14n+3}$. é irredutível .

(Retirado de MA14-2012/2° semestre)

Solução: Temos que mostrar $mdc\ (21n + 4,14n + 3) = 1$. Assim

$mdc\ (21n + 4, 14n + 3) = mdc\ (14n + 3, 21n + 4 - 14n - 3)$

$= mdc(14n + 3,7n + 1)$

$= mdc\ (7n + 1, 14n + 3 - 2(7n + 1))$

$= mdc\ (7n + 1,1) = 1$ ■

Em virtude do algoritmo da divisão euclidiana e do Lema de Euclides, podemos obter o Algoritmo de Euclides que é um primor do ponto de vista computacional e pouco se conseguiu aperfeiçoá-lo em mais de dois milênios para o cálculo do máximo divisor comum procedendo da seguinte maneira:

Dados $a, b \in \mathbb{Z}$, segue da divisão euclidiana que existem $q_1, r_1 \in \mathbb{Z}$ tal que $b = aq_1 + r_1$. Assim

$$mdc(a,b) = mdc(a, a.q_1 + r_1) \underbrace{=}_{Lema\ Euclides} mdc\ (a, r_1)$$

Da mesma forma, para os inteiros $a, r_1 \in \mathbb{Z}$ segue da divisão euclidiana que existem $q_2, r_2 \in \mathbb{Z}$ tal que $a = r_1 q_2 + r_2$. Assim

$$mdc\ (r_1, a) = mdc\ (r_1, r_1 q_2 + r_2) \underbrace{=}_{Lema\ Euclides} mdc\ (r_1, r_2)$$

Portanto, podemos concluir que

$$mdc\ (a,b) = mdc\ (a, r_1) = mdc\ (r_1, r_2)$$

Procedendo desta forma, de maneira recursivamente, o $mdc\ (a,b)$ será o ultimo resto não nulo.

No exemplo para $a = 86$ e $b = 30$, temos que

$$mdc\ (86{,}30) = mdc(30{,}26) = mdc(26{,}4) = mdc(4{,}2) = 2$$

O algoritmo acima pode ser sintetizado e realizado na prática da seguinte forma: Inicialmente, efetuamos a divisão $b = aq_1 + r_1$ e colocamos os números envolvidos no seguinte diagrama:

		q_1
	b	a
	r_1	

A seguir, continuamos efetuando a divisão $a = r_1 q_2 + r_2$ e colocamos os números envolvidos no diagrama

		q_1	q_2
	b	a	r_1
	r_1	r_2	

Prosseguindo, enquanto for possível, teremos:

	q_1	q_2	q_3	...	q_{n-1}	q_n	q_{n+1}
b	a	r_1	r_2	...	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	...	r_n		

2.2 Mínimo Múltiplo Comum

Diremos que um número é um múltiplo comum de dois números naturais dados se ele é simultaneamente múltiplo de ambos os números.

Em qualquer caso, o número $a \cdot b$ é sempre um múltiplo comum de $a\ e\ b$.

Definição 2.2.1: (Mínimo Múltiplo Comum) Diremos que um número inteiro positivo m é um mínimo múltiplo comum (mmc) dos números a e b se possuir as seguintes propriedades:

a) m é um múltiplo comum de $a\ e\ b$, e

b) se c é um múltiplo comum de $a\ e\ b, então\ m|c$.

Por exemplo, 12 é um múltiplo comum de $2\ e\ 3$, mas não é um mmc destes números. O número 6 é um $mmc\ de\ 2\ e\ 3$.

Se c é um múltiplo comum de $a\ e\ b$, então, do item b) da definição acima, temos que m divide c , e, portanto, $m \leq c$, o que nos diz que o mínimo múltiplo comum, se existe, é único e é o menor dos múltiplos comuns de $a\ e\ b$.

O mínimo múltiplo comum de $a\ e\ b$, se existe, é denotado por $[a, b]$.

Dados dois números positivos, digamos $10\ e\ 18$, eles têm um múltiplo comum que é $10 \cdot 18$.

Portanto, dentre todos os múltiplos comuns, deve existir um menor de todos, que é chamado o mínimo múltiplo comum de $10\ e\ 18$ e é denotada por $mmc(10,18)$.

Para calculá-lo, escrevemos a lista de múltiplos de 10, a lista de múltiplos de 18 e determinamos qual o menor número presente em ambas as listas.

- Múltiplos de $18 = \{ 18, 36, 54, 72, 90, 108, ... \}$

- Múltiplos de $10 = \{10, 20, 30, 40, 50, 60, 70, 80, 90, 100, \ldots\}$

Logo, 90 é o mínimo múltiplo comum de $10\ e\ 18$. A abreviação é $mmc(10,18) = 90$.

Proposição 2.2.2 : *Dados dois números inteiros $a\ e\ b$, temos que*

$$mdc(a,b)\ .\ mmc(a,b) = ab.$$

Prova: Seja $m = \frac{ab}{mdc(a,b)}$. Como

$$m = a\ \frac{b}{mdc(a,b)} = b\frac{a}{mdc(a,b)} \quad \Rightarrow \quad a|m \ \ e\ \ b|m.$$

Seja c um múltiplo comum de $a\ e\ b$; logo

$$c = na = k\ b \underbrace{\Rightarrow}_{divide\ por\ mdc\ (a,b)} n\ \frac{a}{mdc\ (a,b)} = k\ \frac{b}{mdc\ (a,b)}.$$

Como $\frac{a}{mdc\ (a,b)}\ \ e\ \ \frac{b}{mdc(a,b)}$ são primos entre si, segue que

$$k = \frac{a}{mdc(a,b)}d\ \ para\ algum\ d\ \ \Rightarrow\ m = b\frac{a}{mdc(a,b)}\ \ |\ b\ k = b\ \frac{a}{mdc(a,b)}\ d = c \quad \blacksquare$$

Corolário 2.2.3: Se $a\ e\ b$ são números naturais primos entre si, então $mmc[a,b] = ab$.

Um número natural maior do que 1 divisível apenas por 1 e por si próprio é chamado de número primo. Dados dois números primos $p\ e\ q$ e um número natural a qualquer, decorrem da definição acima os seguintes fatos:

i) Se $p|q$, então $p = q$.

De fato, como $p|q$ e sendo q primo, temos que $p = 1\ \ ou\ \ p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$.

ii) Se $p \nmid a$, então $mdc(p,a) = 1$.

De fato, se $mdc(p,a) = d,$ temos que $d|p\ \ e\ \ d|a$. Portanto, $d = p\ \ ou\ \ d = 1$. Mas $d \neq p$, pois $p \nmid a$ e, consequentemente, $d = 1$.

Um número maior do que 1 e que não é primo será chamado *composto*. Portanto, se um número n é composto, existirá um divisor $n_1 \ de \ n \ tal \ que \ n_1 \neq 1 \ e \ n_1 \neq n$. Logo, existirá um número natural n_2 tal que $n = n_1 \cdot n_2, \ com \ 1 < n_1 < n \ e, \ 1 < n_2 < n$.

Por exemplo, $2, 3, 5, 7, 11 \ e \ 13$ são números primos, enquanto que $4, 6, 8, 10 \ e \ 12$ são compostos.

Do ponto de vista da estrutura multiplicativa dos naturais, os números primos são os mais simples e ao mesmo tempo são suficientes para gerar todos os números naturais, conforme veremos agora no Teorema Fundamental da Aritmética.

Teorema 2.2.4 (Teorema Fundamental da Aritmética): *Todo número natural maior do que* 1 *ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos*.

Prova : Usaremos a segunda forma do Princípio de Indução. Se $n = 2$, o resultado é obviamente verificado.

Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar.

Suponhamos, então, que n seja composto. Logo, existem números naturais $n_1 \ e \ n_2 \ \ tais \ que$

$$n = n_1 \cdot n_2, \text{ com } 1 < n_1 < n \ e \ 1 < n_2 < n.$$

Pela hipótese de indução, temos que existem números primos

$$p_1, \dots, p_r \ e \ q_1, \dots, q_s \ \ tais \ que \ n_1 = p_1 \dots p_r \ e \ n_2 = q_1 \dots q_s.$$

Portanto,

$$n = n_1 \, n_2 = p_1 \dots p_r q_1 \dots q_s.$$

Vamos, agora, provar a unicidade. Suponhamos, agora, que

$$n = p_1 \dots p_r = q_1 \dots q_s,$$

onde os $p_i \ e \ os \ q_j$ são números primos. Como $p_1 / q_1 \dots q_s$, temos que $p_i = q_j$ para algum j, que, após reordenamento de $q_1, \dots, q_s$, podemos supor que seja q_1. Portanto,

$$p_2 \dots p_r = q_2 \dots q_s.$$

Como $p_2 \dots p_r < n$, a hipótese de indução acarreta que $r = s \ e \ os \ p_i \ e \ q_j$ são iguais aos pares. ■

Agrupando, nesse teorema, os fatores primos repetidos, se necessário, e ordenando os primos em ordem crescente, temos o seguinte enunciado: *"Dado um número natural* $n > 1$, *existem primos* $p_1 < \cdots < p_r \ e \ \alpha_1, \ldots, \alpha_r \in \mathbb{N}^*$, *univocamente determinados, tais que* $n = {p_1}^{\alpha_1} \ldots {p_r}^{\alpha_r}$."

Observe que um número natural $n > 1$, escrito na forma $n = {p_1}^{\alpha_1} \ldots {p_r}^{\alpha_r}$, como no teorema acima, é um quadrado perfeito se, e somente se, cada expoente α_i é par.

A fatoração única é muito importante.

Caso considerássemos o número 1 como um número primo, algumas propriedades baseadas na fatoração única não seriam válidas, pois neste caso, temos que $12 = 2^2 \cdot 3 = 1^3 \cdot 2^2 \cdot 3 = 1^5 \cdot 2^2 \cdot 3$ e neste caso não teríamos fatoração única.

Exemplo 2.2.5: Determine $m \in \mathbb{N}$ de modo que o número $20 \cdot 21^m$ tenha exatamente 96 divisores positivos.(Retirado de MA13-AVF-2014)

Solução: Denotando por $D(n)$ o número de divisores positivos do número natural $n, se\ n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ é a decomposição de n em fatores primos distintos, sabemos que

$$D(n) = (\alpha_1 + 1) \cdots (\alpha_r + 1).$$

Como

$$20 \cdot 21^m = 2^2 \cdot 5(3 \cdot 7)^m = 2^2 \cdot 3^m \cdot 5^1 \cdot 7^m$$

Por hipótese, temos que $D(20 \cdot 21^m) = 96$. Logo:

$$(2 + 1)(m + 1)(1 + 1)(m + 1) = 96 \Leftrightarrow (m + 1)^2 = 16,$$

Assim

$$m^2 + 2m + 1 - 16 = (m + 5)(m - 3) = 0$$

Portanto, como m é natural, a resposta é $m = 3$.

Exemplo 2.2.6: Em um corredor há 900 armários, numerados de 1 a 900, inicialmente todos fechados e 900 pessoas, numeradas de 1 a 900, atravessam o corredor.

A pessoa de número k reverte o estado de todos os armários cujos números são múltiplos de k.

Por exemplo, a pessoa de número 4 mexe nos armários de números $\{4, 8, 12, \cdots\}$, abrindo os que encontram fechados e fechando os que encontram abertos.

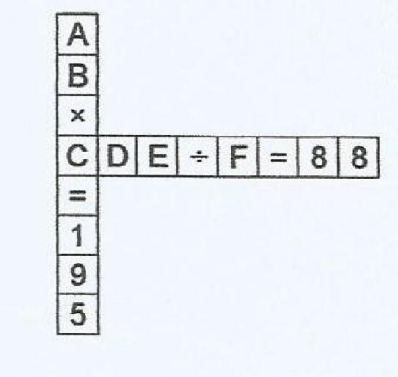
Ao final, quais armários ficarão abertos? (A Matemática do Ensino Médio-V.2 - SBM)

Solução: O armário de número k é mexido pelas pessoas cujos números são divisores de k. Um armário ficará aberto se for mexido um número ímpar de vezes. Devemos lembrar também que o número de divisores positivos de $2^{\alpha} \cdot 3^{\beta} \cdot 5^{\gamma} \cdot \cdots$ é igual a $(\alpha+1)(\beta+1)(\gamma+1)\cdots$.

Isso ocorre com os números cujos expoentes são todos pares na decomposição em fatores primos, ou seja, são quadrados perfeitos. Assim, permanecerão abertos os armários cujos números são quadrados perfeitos, ou seja, os números $1^2, 2^2, \cdots, 30^2$.

Exemplo 2.2.7: As contas $AB \cdot C = 195 \ e \ CDE \div F = 88$ estão corretas, sendo $A, B, C, D, E \ e \ F$ algarismos diferentes. O número AB é formado pelos algarismos $A \ e \ B$, e o número CDE é formado pelos algarismos $C, D \ e \ E$.

Qual é o algarismo representado pela letra F? (OBMEP-2016)



Solução: Devemos saber a decomposição em fatores primos do número 195. Assim temos que $195 = 3 \cdot 5 \cdot 13$.

Então temos algumas possibilidades de escrever o número 195 como um produto de dois números. Vejamos:

1ª Possibilidade: $195 = 65 \cdot 3$

Dessa possibilidade temos que $A = 6, B = 5 \ e \ C = 3$.

Como CDE é um múltiplo de 88 e nesse caso, está entre $300 \ e \ 400$ temos que $CDE = 88 \cdot 4 = 352$.

Dessa forma vamos ter $C = 3, D = 5, E = 2 \ e \ F = 4$, mas esses valores não atendem o enunciado que afirma que os valores precisam ser diferentes e temos $B = D$.

2ª Possibilidade: $195 = 39 \cdot 5$

Dessa possibilidade temos que $A = 3, B = 9 \ e \ C = 5$.

Como CDE é um múltiplo de 88 e nesse caso, está entre $500 \ e \ 600$ temos que $CDE = 88 \cdot 6 = 528$.

Dessa forma vamos ter $C = 5, D = 2, E = 8 \ e \ F = 6$ e como todos os algarismos são diferentes, temos que $F = 6$.

Exemplo 2.2.8: Descubra o menor número natural da forma $n! = n(n-1) \cdots 2.1$, múltiplo de 1000.

Solução: Como $1000 = 2^3 \cdot 5^3$, o número de fatores iguais a 2 e a 5 precisam ser no mínimo iguais a 3. Basta que procuremos o número que tenha 3 fatores iguais a 5 na sua composição pois o fator 2 aparecerá com maior frequência.

Dessa forma o número procurado é 15! pois o fator 5 aparece 3 vezes, a saber: no próprio 5, no $10 = 2.5$ e no $15 = 3.5$.

Exemplo 2.2.9: Considere o número

$$a = \ 467775 = 3^5 \cdot 5^2 \cdot 7 \cdot 11 \quad e \quad b = \ 2592 = 2^5 \cdot 3^4.$$

Calcule o $mdc(a, b)$ e o $mmc(a, b)$.

Solução: Vamos denotar por $d = mdc(a, b)$. Um número primo p é um fator de d exatamente quando ele dividir simultaneamente $a = 467775$ e $b = 2592$. Observando a fatoração de a e b, segue que apenas o fator 3 é passível de tal propriedade. A maior potência de 3 que divide ambos é 3^4, logo, $d = mdc(2592,467775) = 3^4 = 81$.

Então, a regra para encontrar $d = mdc(a, b)$ pode ser assim descrita:

I. Encontre as fatorações de $a \ e \ b$ como produto de primos.

II. Tome os primos p comuns a ambas as fatorações.

III. Agora tome p^e para cada fator primo comum, onde e é o menor dos expoentes de p nas duas fatorações.

IV. Então, d será o produto de todas as potências p^e.

E quanto ao menor múltiplo comum? Como encontramos $l = mmc(2592,467775)$?

Olhando para as fatorações, vemos imediatamente que $l = 2^5 \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11$. Tome todas as potências p^e, onde p divide $a\ ou\ b$, e e é o maior dos expoentes.

Deve ficar bem entendido que se p não divide a, então, tome p com o expoente no qual ele aparece em b, e de maneira análoga se p não divide b. O que precisamos realmente saber são as fatorações dos números como potências de números primos e já sabemos que isso pode ser um processo muito longo e trabalhoso.

Na verdade é possível evitar essas fatorações através do seguinte procedimento:

Para quaisquer dois números $a\ e\ b$ maiores que zero devemos fazer o seguinte processo:

I. Fazemos o produto *ab*.

II. Encontramos $d = mdc(a, b)$ por sucessivas divisões euclidianas não sendo necessário fazer fatorações.

III. Finalmente fazemos $l = mmc(a, b) = \frac{ab}{d}$, onde fatorações também não são necessárias.

Sobre a distribuição dos números primos

Quantos serão os números primos? Essa pergunta foi respondida por Euclides no Livro IX dos Elementos. Utilizaremos a mesma prova dada por Euclides, onde pela primeira vez se registra o uso de uma demonstração por redução ao absurdo em matemática. Essa prova é considerada uma das pérolas da matemática.

Teorema 2.2.10: *Existem infinitos números primos.*

Prova: Suponhamos que a sucessão $p_1 = 2, p_2 = 3, \ldots, p_r$ dos r números primos seja finita. Façamos $P = p_1 p_2 \ldots p_r + 1$ e seja p um numero primo p que divide P. Esse número p não pode ser igual a qualquer um dos números $p_1, p_2, \ldots, p_r$ porque então ele dividiria a diferença $P - p_1 p_2 \ldots p_r = 1$ o que é impossivel. Assim p é um numero primo que não pertence à sucessão e, por conseqüência, $p_1, p_2, \ldots, p_r$ não podem formar o conjunto de todos os números primos. ■

Relembrando o Crivo de Erastótenes

Como descobrir um número primo é uma questão que até os dias de hoje ainda não foi resolvida totalmente. Existe um método bastante simples sem ter que fazer divisões que indica os números primos. Para números "pequenos" ele funciona satisfatoriamente. O Crivo de Erastótenes que consiste em escrever, os números ímpares em linhas e seguir algumas recomendações. Como exemplo vamos achar os números primos até 100.

Como sabemos que 2 é o único número par que é primo.

1º) Colocamos os números ímpares em linhas com 5 números ímpares em cada uma.

1 3 5 7 9

11 13 15 17 19 ...

2°) Elimine o número 1.

3°) Não elimine o 3, salte três números; elimine o 9 e salte três números; elimine o 15, e continue desta forma.

4º) O menor número que ainda não foi eliminado é o 5 – não o elimine, mas salte 5 números.

O próximo número é o 15 que já foi eliminado anteriormente.

Salte cinco números e elimine o 25; repita esse processo.

5°) O menor número que ainda não foi eliminado é o 7 – não o elimine.

Salte então, sete números e chegue ao 21, que já foi eliminado anteriormente.

Salte mais sete números e chegue ao 35, que já foi eliminado.

Salte, então, mais sete números e elimine o 49. Repita esse processo.

6°) Pare! Os números eliminados são múltiplos de números menores (diferentes de 1), e portanto não são primos.

Pelo mesmo motivo, números que não foram eliminados são primos. Não precisamos verificar mais, pois, depois do 7, deveríamos manter o 11, e saltar 11 números onde chegaríamos a $11 \times 11 = 121$, que é maior que 100.

Resumindo, os números primos menores que 100 são:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 \; e \; 97.$$

O Crivo de Erastótenes tem um custo computacional muito elevado tornando-se por isto um método inviável na prática. Até o momento continuamos sem métodos eficazes para elaborar tabelas de números primos. Outras duas questões que ainda não foram resolvidas satisfatoriamente do ponto de vista computacional são: a verificação se um dado inteiro é primo (chamado de teste de primalidade) e a decomposição em números primos para números inteiros grandes (fatoração em irredutíveis).

Lema 2.2.11: *Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leq n$, então n é primo.*

Prova: Suponhamos, por absurdo, que n não seja primo. Seja p o menor número primo que divide n; então $n = pn_1$, com $p \leq n_1$. Segue daí que $p^2 \leq pn_1 = n$ o que gera uma contradição da hipótese. ■

Um aspecto interessante nos números primos é que ao observarmos os primeiros números primos temos a impressão que eles aparecem a toda hora na sequência dos números naturais. Até o número 50 temos os seguintes primos $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 \; e \; 47\}$. De 50 até o 100 temos os primos $\{ 53, 59, 61, 67, 71, 73, 79, 83, 89 \; e \; 97 \}$.

É possível termos um conjunto de números naturais consecutivos onde haja apenas um número primo e o restante dos números seja todo formado por números compostos?

A resposta é sim. Vejamos:

Começamos verificando para 5 números naturais consecutivos onde haja apenas um número primo. No exemplo acima temos $53, 54, 55, 56 \; e \; 57$ onde apenas o número 53 é um número primo.

Será que existem 10 números consecutivos onde haja apenas um número primo. Se observarmos o Crivo de Erastótenes verificaremos que: $\{113, 114, 115, 116, 117, 118, 119, 120, 121, 122\}$ é uma sequência de 10 números naturais consecutivos onde apenas o número 113 é primo.

Mas se quiséssemos construir uma sequência com 100 números naturais consecutivos onde apenas um deles seja primo, pelo crivo de Erastótenes essa verificação ficaria muito demorada e trabalhosa.

Assim se faz necessário mostrar de outra maneira.

Vamos considerar o número $100! = 1 \cdot 2 \cdot 3 \cdots 100$. Agora, a sequência $100! + 2$, $100! + 3$, $100! + 4, \ldots, 100! + 100$ é uma sequência de 99 números todos compostos pois, $100! + k = k\left(\frac{100!}{k} + 1\right), 2 \leq k \leq 100, k \in \mathbb{Z}$ é um número composto pois $\frac{100!}{k}$ é um número inteiro nas condições estabelecidas acima.

Desse modo vimos que temos 99 números inteiros consecutivos. Logo, sendo $p \leq 100! + 1$ esse primo, dessa maneira teremos $p + 1, p + 2, \ldots, p + 99$ todos compostos pois

$$p + 99 \leq 100! + 100.$$

Portanto temos uma sequência $p, p + 1, p + 2, \ldots, p + 99$ com apenas um número primo.

Esse raciocínio nos leva a conjecturar que podemos construir uma sequência de números naturais consecutivos com qualquer quantidade de números naturais com apenas um número primo.

Prova: Seja o número $x! = 1 \cdot 2 \cdot 3 \cdot \cdots x$. Consideremos os números naturais consecutivos $x! + 2$, $x! + 3$, $x! + 4$, $\cdots, x! + x$, que são claramente números compostos, pois

$$x! + k = k\left(\frac{x!}{k} + 1\right), \qquad 2 \leq k \leq x, \qquad k \in \mathbb{Z}.$$

Assim temos uma sequência com $(x - 1)$ números naturais consecutivos compostos. Temos que achar o maior número primo menor que $x! + 2$. Assim seja p o maior numero primo que satisfaz $p \leq x! + 1$. Portanto, a sequência

$$p, p + 1, p + 2, \cdots, p + (x - 1)$$

é a sequência procurada, pois $p + (x - 1) \leq x! + x$ atende o enunciado. ■

No dia 23/06/1993, Andrew Wiles, após três séculos desde a apresentação do Último Teorema de Fermat (UTF) faz, numa de suas palestras, o anúncio da descoberta da demonstração desse teorema, para a surpresa de todos os presentes. Infelizmente havia uma pequena falha na sua demonstração que Wiles, após um ano, apresenta a demonstração reformulada, que foi finalmente aceita.

Wiles conheceu o problema de sua vida, ainda criança, com 10 anos, quando certo dia, voltava para casa e decidiu passar na biblioteca da Rua Milton, uma pequena biblioteca, mas que tinha uma boa coleção de livros sobre enigmas, e foi atraído por um livro que tinha apenas um problema, mas sem solução.

O livro era "O Último Problema", de Eric Temple Bell, onde apresentava a história de um problema matemático de origem grega, mas só atingiria sua maturidade no século XVII, quando Fermat o colocara como desafio, e que durante trezentos anos nenhum matemático tinha conseguido a solução. Além do problema, o livro continha a tentativa de vários matemáticos em solucioná-lo. A partir daí, Wiles trilhou sua infância e sua vida acadêmica na tentativa de descoberta de uma solução para esse desafio, o que acabou conseguindo.

Agora conhecido como o Último Teorema de Fermat ou Teorema de Fermat-Wiles, ele afirma o seguinte:

"Não existe nenhum conjunto de inteiros positivos x, y, z e n com n maior que 2 que satisfaça a equação $x^n + y^n = z^n$."

Existem, na matemática, problemas intrigantes e outros bastante simples, mas que não foram resolvidos até os dias de hoje. Colocaremos alguns desses problemas, pois são desafiadores e estimulantes que, a exemplo de Andrew wiles, possa ser encontrado por alguém que assuma o propósito de solucioná-los.

Problema 1: Na matemática, os números primos sempre foram objeto de especial atenção. Em 1742, na correspondência entre o matemático prussiano Cristian Goldbach e o famoso suíço Leonard Euler, foi formulada a seguinte questão, conhecida por **"Conjectura de Goldbach",** que afirma o seguinte:

"Todo inteiro par maior que 2 pode ser escrito como a soma de dois números primos."

Euler afirmou a Goldbach que estava absolutamente certo sobre isso, porém não era capaz de provar.

Esta suposição tornou-se um dos problemas mais intrigantes da matemática e não foi resolvido até os dias de hoje.

Problema 2: Um par de números primos é chamado de **primos gêmeos** se eles são dois números primos p, q tais que $q = p + 2$. Como exemplo temos (3,5), (5,7), (11,13), (17,19),etc...

A conjectura dos primos gêmeos diz que **"existem infinitos números primos gêmeos",** porém até hoje não se pôde provar nem refutar tal afirmação.

Ficam aqui essas duas conjecturas desafiadoras.

CAPÍTULO 3 - ARITMÉTICA DOS RESTOS

Uma das noções mais férteis da Aritmética foi introduzida por Gauss no seu livro Disquisitiones Arithmeticae de 1801. Trata-se da realização de uma aritmética com os restos da divisão euclidiana por um número fixado. É a aritmética dos fenômenos periódicos, isto é, aqueles que se repetem a intervalos regulares. Isto sugere que o próprio resto de uma divisão se comporta de maneira periódica.

Mais precisamente os restos dos inteiros sucessivos na divisão por um inteiro positivo qualquer n repetem-se com período n. Por exemplo, os múltiplos de 4 se repetem de 4 em 4 e, portanto com período igual a 4, assim, dividindo os números inteiros por 4, obtemos os restos como na tabela:

Inteiros	...	-4	-3	-2	-1	0	1	2	3	4	5	6	7	...
Restos	...	0	1	2	3	0	1	2	3	0	1	2	3	...

$\underbrace{\textbf{período igual a 4}}$

Definição 3.1: Seja m um número inteiro diferente de zero. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de suas divisões euclidianas por m são iguais. Quando isso acontece, ou seja, quando os inteiros a e b são congruentes módulo m, escreve-se

$$a \equiv b \; mod \; m.$$

Quando a relação $a \equiv b \; mod \; m$ for falsa, diremos que a e b não são congruentes módulo m, e nesse caso, escrevemos que $a \not\equiv b \; mod \; m$.

Veja que $5 \equiv 9 \; mod \; 4$ e $5 \not\equiv 7 \; mod \; 4$. No primeiro caso tanto 5 quanto 9 deixam restos iguais a 1 quando divididos por 4 enquanto que no segundo caso 5 e 7 têm restos diferentes quando divididos por 4.

Como o resto da divisão de um número inteiro qualquer por 1 é sempre nulo, temos que $a \equiv b \; mod \; 1$, quaisquer que sejam $a, b \in N$. Isto torna desinteressante a aritmética dos restos módulo 1. Portanto, consideraremos sempre $m > 1$.

Para verificar se dois números são congruentes módulo m, não é necessário efetuar a divisão euclidiana de ambos por m para depois comparar os seus restos. É suficiente aplicar o seguinte resultado.

Proposição 3.2: *Suponha que* $a, b \in N$ *são tais que* $a \geq b$. *Tem-se que* $a \equiv b \, mod \, m$ *se, e somente se* $m|(a-b)$.

Prova: Seja $a = q_1 \cdot m + r \;\; e \;\; b = q_2 \cdot m + r, \; a \geq b \; e \; a, b \in \mathbb{N} \;\; e \; r < m.$ Assim, $a - b = (q_1 - q_2) \cdot m$ e, dessa forma $(a-b)$ é um múltiplo de m. ■

Um exemplo numérico, pode ser dado por $31 = 6 \cdot 5 + 1 \;\; e \;\; 16 = 3 \cdot 5 + 1$ então $(31 - 16) = 15 = 3 \cdot 5$.

A relação de congruência satisfaz algumas propriedades satisfeitas pela relação de igualdade usual. As propriedades mais elementares da igualdade são as seguintes:

Reflexiva: todo número é igual a si próprio.
Simétrica: se $a = b$ então $b = a$.
Transitiva: se $a = b$ e $b = c$, então $a = c$.

No caso da relação de congruência não é assim tão óbvio que estas propriedades são satisfeitas, mas podemos verificá-las sem muito trabalho.

Reflexiva: Todo número é congruente módulo m a si próprio.
Prova: Devemos verificar que $a \equiv a \, mod \, m$. Mas, pela definição, isto é o mesmo que dizer que $a - a = 0$ é múltiplo de m. Contudo, zero é múltiplo de qualquer inteiro m, uma vez que $0 \, . \, m = 0$. ■

Simétrica: se $a \equiv b \, mod \, m$ então $b \equiv a \, mod \, m$.
Prova: Pela definição de congruência módulo m, $a \equiv b \, mod \, m$ é o mesmo que dizer que $(a-b)$ é múltiplo de m. Em outras palavras, se $a \equiv b \, mod \, m$ então existe algum inteiro k tal que $a - b = k.m$. Multiplicando esta equação por -1, obtemos $b - a = (-k).m$, isto é, $b - a$ é múltiplo de m, ou ainda, $b \equiv a \, mod \, m$. ■

Transitiva: se $a \equiv b \, mod \, m$ e $b \equiv c \, mod \, m$, então $a \equiv c \, mod \, m$.

Prova: Tomemos por hipótese que $a \equiv b \, mod \, m$ e que $b \equiv c \, mod \, m$. Mas estas duas congruências se traduzem, por definição, nas igualdades $a - b = k.m$ e $b - c = l.m$, onde k e l são inteiros escolhidos de maneira adequada. Somando estas duas últimas equações, temos $(a - b) + (b - c) = k.m + l.m$. Cancelando o termo b à esquerda e usando a distributividade da direita obtemos $a - c = (k + l).m$, que é equivalente à congruência $a \equiv c \, mod \, m$, como requerido pela propriedade transitiva. ■

A relação entre congruência módulo m e a divisibilidade de inteiros vista com mais detalhes permite-nos perceber algumas de suas utilidades. Para começar a **propriedade reflexiva** da congruência módulo m é equivalente à afirmação de que **zero é divisível por m**.

Por sua vez, a **propriedade simétrica** equivale a dizer que se um dado número a é divisível por m então, ao multiplicá-lo por -1, obtemos outro múltiplo de m.

Finalmente, a **propriedade transitiva** nos diz que a soma de múltiplos de m também é um múltiplo de m.

Vejamos uma outra situação: Um farsante resolveu levar a vida como um prestidigitador, fingindo adivinhar ou ler a mente de pessoas em um público desconhecido. Descobriu que poderia ganhar dinheiro com truques matemáticos que podiam ser confundidos com adivinhações.

- Em um de seus shows ele escreveu algo num pequeno bilhete, dobrou-o e entregou-o a um espectador qualquer.
- Escolheu aleatoriamente outro espectador da platéia e solicitou que este espectador falasse 7 números entre $1 \, e \, 1000$.

Independente de quais tenham sido as escolhas do segundo espectador, quando o primeiro espectador desdobrou e leu o bilhete, verificou o que estava escrito, estava correto. Desta forma o farsante concluiu seu show como um grande adivinho.

Admitindo que a resposta do bilhete seja afirmativa em qualquer situação respondida pelo segundo espectador, qual pode ter sido o texto escrito pelo falso mago no bilhete? (CM-2016)

a) Entre os números escolhidos estaria um número par.

b) Entre os números escolhidos estaria um múltiplo de sete.
c) Entre os números escolhidos estaria um múltiplo de sete ou a diferença entre dois dos números escolhidos seria um múltiplo de sete.
d) Dois dos números escolhidos teriam o mesmo resto pela divisão por dez.
e) Qualquer formulação que o mago quisesse, pois uma adivinhação desta forma, só seria possível se ele escolhesse uma pessoa combinada da platéia.

Solução: Como são escolhidos sete números, escrevendo esses números na forma

$$N = 7k + r, \;\; 0 \leq r \leq 6,$$

temos duas possibilidades:

- **1ª possibilidade:** Todos os setes números têm restos diferentes quando divididos por sete. Dessa maneira, teríamos o número $N = 7k + 0$ e, portanto, N seria um múltiplo de sete.
- **2ª possibilidade:** Pelo menos dois números teriam o mesmo resto quando divididos por sete e, portanto a diferença entre eles seria um múltiplo de sete pois

$$7k + r - 7k' - r = 7(k - k') = 7k^*.$$

Assim, o texto apresentado na letra C seria sempre correto. ■

O que torna útil e poderosa essa noção **é o fato de ser uma relação de equivalência** compatível com as operações de adição e multiplicação nos inteiros, conforme veremos na proposição a seguir.

$$\text{Se } \; a \equiv b \; mod \; m \;\; e \;\; c \;\equiv d \; mod \; m \quad \text{então} \quad \begin{cases} a + c \equiv b + d \; mod \; m \\ a.c \equiv b.d \quad mod \; m \end{cases}$$

Proposição 3.3 : Sejam $a, b, c, d, m \in \mathbb{N}$, com $m > 1$.

i) Se $(b - a)$ e $(d - c)$ são múltiplos de m, então $(b + d) - (a + c)$ também é um múltiplo de m.
ii) Se $(b - a)$ e $(d - c)$ são múltiplos de m, então $b \cdot d - a \cdot c$ também é um múltiplo de m.

Prova: Por hipótese, temos que $(b-a) = k_1 m \;\; e \;\; (d-c) = k_2 m$, para $k_1, k_2 \in \mathbb{Z}$.

(i) Somando $(b+d)-(a+c) = (b-a)+(d-c) = m(k_1+k_2)$.

(ii) Segue que $(b-a)d = \underbrace{bd-ad} = k_1 m\, d$ e $a(d-c) = \underbrace{ad-ac} = ak_2 m$. Somando, ambos os lados, temos $bd - ac = bd \underbrace{-ad + ad} - ac = k_1 md + ak_2 m = m(k_1 d + ak_2)$ ■

Vejamos isso com exemplos numéricos:

(i) Vamos dividir $17 \; e \; 19 \; separadamente \; por \; 5$. Depois vamos dividir $(17+19) \; por \; 5$. Temos que $17 = 3 \cdot 5 + \mathbf{2} \; e \; 19 = 3 \cdot 5 + \mathbf{4}$. Assim, $17 + 19 = 36 = 7 \cdot 5 + 1$ e podemos notar que $\mathbf{2} + \mathbf{4} = 6 = 1 \cdot 5 + 1$.

(ii)Vamos dividir $17 \; e \; 19 \; separadamente \; por \; 5$. Depois vamos dividir $(17 \cdot 19) \; por \; 5$. Como $17 = 3 \cdot 5 + \mathbf{2} \; e \; 19 = 3 \cdot 5 + \mathbf{4}$, Temos que $17 \cdot 19 = 323 = 64 \cdot 5 + \mathbf{3}$. Podemos notar que $\mathbf{2} \cdot \mathbf{4} = 8 = 1 \cdot 5 + \mathbf{3}$.

Exemplo 3.4: Ache o resto da divisão de $1998 + 1999 \; por \; 7$.

Solução: Como $1998 = 285 \cdot 7 + 3$, temos que $1999 = 285 \cdot 7 + 4$ e, portanto $1998 + 1999$ é múltiplo de $7 \; pois \; 3 + 4 = 7$ e $7 = 1 \cdot 7 + 0$.

Exemplo 3.5: Calcule o resto da divisão de $(2006^{2006} + 2004^{2004})^{2005} \; por \; 5$. (Retirado do Livro "Problemas selecionados de Matemática IME-ITA-Olimpíadas de Marcílio Miranda)

Solução: Na divisão por 5, temos que

$$\begin{cases} 2006 \; deixa \; resto \; 1 \\ 2004 \; deixa \; resto \; 4 \end{cases}$$

Via relação de congruência, a classe do 4 é igual a classe do (-1), portanto podemos escrever a expressão acima, trocando os elementos por um representante da classe dos restos. Logo,

$$[(1)^{2006} + (-1)^{2004}]^{2005}$$

que terá o mesmo resto da expressão original na divisão por 5. Assim, queremos calcular o resto da divisão $(1+1)^{2005} \; por \; 5$ ou seja $2^{2005} \; por \; 5$. Como $2^4 = 16 = 3.5 + 1$,16 deixa resto 1 na divisão por 5. Por outro lado

$$2^{2005} = (2^4)^{501} \cdot 2$$

Trocando (2^4) por seu represente na classe dos restos na divisão por 5, temos que

$$2^{2005} = (2^4)^{501} \cdot 2 = (1)^{501}.2 = 2 \ \ mod \ \ 5$$

portanto, o resto da divisão de $(2006^{2006} + 2004^{2004})^{2005} \ \ por \ \ 5$ é igual a 2.

Exemplo 3.6: Calcule o resto da divisão de $5^{131} + 7^{131} + 11^{131} + 13^{131} \ \ por \ \ 9$. (Retirado do Livro "Problemas selecionados de Matemática IME-ITA-Olimpíadas de Marcílio Miranda)

Solução: Na divisão por 9, temos respectivamente que $5, 7, 11, 13$ deixam resto $5, 7, 2, 4$. Via relação de congruência, as classes respectivamente de $5 \ e \ 7$ podem ser trocadas pelas classes de $-4, -2$ e portanto podemos escrever a expressão acima, trocando os elementos por um representante da classe dos restos, Assim

$$(-4)^{131} + (-2)^{131} + (2)^{131} + (4)^{131}$$

terá o mesmo resto que a expressão original. Como esses valores são simétricos temos que o resto da divisão de $5^{131} + 7^{131} + 11^{131} + 13^{131}$ por 9 é 0 (zero).

Exemplo 3.7: Podemos afirmar também que $1998 \cdot 1999$ dividido por 7 deixa resto 5.

Solução: Como $1998 = 285.7 + 3$ e $1999 = 285.7 + 4$, segue que, o produto dos restos

$$3 \cdot 4 = 12 = 1 \cdot 7 + 5.$$

E assim, concluímos que $1998 \cdot 1999$ dividido por 7 deixa resto 5.

De maneira análoga, do fato que $1998 = 285.7 + 3$ podemos concluir que 1998^3 quando dividido por 7 deixa resto 6

De fato, basta verificar que $3^3 = 3 \cdot 3 \cdot 3 = 27 = 3 \cdot 7 + 6$.

Fica um desafio: Determine o resto da divisão de $3^{201} \ por \ 8$?

Sugestão: Use que 3^2 deixa resto 1 quando dividido por 8. Faça uso também das propriedades das potências e use a aritmética dos restos.

3.1 CÁLCULO DE POTÊNCIAS "GRANDES"

Um assunto importante e bastante interessante para os alunos do ensino básico é o cálculo do resto de divisões de potências "grandes" de um número qualquer por outro número também "grande".

Veremos como calcular potências grandes de um número a módulo m, onde m pode ter centenas de dígitos. ***O modo natural de calcular a^n é por repetidas multiplicações por a.*** Vejamos isso através de uma tabela:

$a_1 \equiv a \ mod \ m$	$a_2 \equiv a.a_1 \ mod \ m$	$a_3 \equiv a.a_2 \ mod \ m$
$a_4 \equiv a.a_3 \ mod \ m$	$a_5 \equiv a.a_4 \ mod \ m$	$a_6 \equiv a.a_5 \ mod \ m$
	...	

Fica claro que $a_k \equiv a^k \ mod \ m$, mas se k é muito grande o algoritmo não faz sentido em ser aplicado. Uma boa ideia é usar a expansão binária para o expoente k, ou seja, escrever

$$k = b_0 + \ b_1.2^1 + b_2.2^2 + \ b_3.2^3 + \cdots + \ b_r.2^r, \ \text{ com } \ b_j \in \{0,1\},$$

onde podemos assumir que $b_r = 1$.

Vale lembrar que para obtermos os valores de cada um dos b_j podemos fazer divisões sucessivas por 2, começando pelo número k, até obtermos um quociente zero. Deste modo, os b_j serão os restos obtidos como divisões. Observe o exemplo:

Vamos escrever a expansão binária do número 57.

Divisões	**Quociente**	**Resto**	b_j
57: 2	28	1	$b_0 = 1$
28:2	14	0	$b_1 = 0$
14:2	7	0	$b_2 = 0$
7:2	3	1	$b_3 = 1$
3:2	1	1	$b_4 = 1$
1:2	0	1	$b_5 = 1$

Assim, de acordo com a tabela podemos escrever que:

$$57 = b_0 + b_1.2^1 + b_2.2^2 + b_3.2^3 + b_4.2^4 + b_5.2^5$$
$$= 1 + 0.2^1 + 0.2^2 + 1.2^3 + 1.2^4 + 1.2^5$$
$$= 1 + 2^3 + 2^4 + 2^5$$

Nesse caso é também usada a aritmética dos restos, pois iremos aplicar as propriedades da adição e multiplicação dos restos nesse cálculo. Por exemplo, queremos saber o resto da divisão de 5^{320} por 950, em outras palavras, $5^{320} \equiv a \; mod \; 950$.

O primeiro passo desse processo é escrever o expoente 320 como uma soma de potências de 2. Assim, $320 = 2^6 + 2^8$. Podemos então colocar que

$$320 = 2^6 + 2^8 \Longrightarrow 5^{320} = 5^{2^6+2^8} = 5^{2^6} \cdot 5^{2^8}$$

Observe que a sequencia abaixo, é relativamente fácil de calcular, visto que cada número é o quadrado do anterior:

$$5^{2^0} = 5 \; ; \quad 5^{2^1} = 5^2 = 5.5 \; ; \quad 5^{2^2} = 5^4 = 5^2.5^2 \; ; \quad 5^{2^3} = 5^8 = 5^4.5^4 \; ; \quad \text{etc...}$$

Além disso, como só precisaremos destes valores módulo 950, nunca precisaremos armazenar mais do que 3 dígitos. A seguir construiremos uma tabela com todas as potências de 5 módulo 950 até 5^{2^8}e indicaremos na 2ª linha os respectivos restos da divisão de 5^{2^i} por 950 fazendo uso da aritmética dos restos. Assim,

i	0	1	2	3	4	5	6	7	8
$5^{2^i} mod \; 950$	5	25	625	175	225	275	575	25	625

A criação da tabela acima permite que façamos apenas 8 multiplicações e acoberta o fato de que o número $5^{2^8} = 5^{256}$ tem um expoente muito grande porque cada entrada sucessiva na tabela é igual ao quadrado da entrada anterior. Portanto, segue da tabela que:

$$5^{320} = 5^{2^6}.\; 5^{2^8} \equiv 575 \,.625 \; mod \; 950 \equiv 275 \; mod \; 950$$

Assim, podemos afirmar que o resto da divisão de 5^{320} por 950 é 275. Percebemos, dessa forma, que o cálculo reduziu em muito essa divisão não necessitando lidar com números muito grandes.

CAPÍTULO 4 - EQUAÇÕES DIOFANTINAS LINEARES (EDL)

Essas equações são chamadas dessa maneira em homenagem a Diofanto de Alexandria, matemático grego que viveu nos meados do século II. Ele baseou seus estudos usando símbolos que facilitaram a escrita e os cálculos matemáticos. Dessa maneira, as expressões que eram escritas totalmente com palavras puderam ser representadas com abreviações.

A nossa primeira intenção é descobrir, por tentativa e erro, uma solução inteira de uma equação do tipo $ax + by = c$. Desse modo, qual seria uma solução inteira para a equação $5x + 3y = 1$? Pelos coeficientes de x e y podemos notar que x e y terão sinais diferentes. Assim, podemos perceber que $x = -1 \ \ e \ \ y = 2$ é uma solução.

Exemplo 4.1: Determine uma solução inteira da equação $17x + 5y = 4$.

Da mesma forma que o exercício anterior, $x \ \ e \ \ y$ deverão ter sinais contrários. Assim, verificamos que $x = -3 \ \ e \ \ y = 11$ ou que $x = 7 \ \ e \ y = -23$ são soluções.

Agora, vamos pensar um pouco: Por que a equação $3x + 6y = 4$ não possui soluções inteiras? Sugestão: pense nos termos da equação. O que $3x + 6y \ \ e \ \ 4$ devem ter em comum?

Como $3x \ \ e \ \ 6y$ são múltiplos de 3, o termo da direita também tem que ser múltiplo de 3. Como isso não acontece, a equação não tem solução.

Seguindo esse raciocínio, verifique se $119x + 35y = 6$ têm solução inteira?

O que teríamos que verificar? Obviamente que $119x \ \ e \ \ 35y$ precisam ser múltiplos de um número que o termo da direita também o seja. Como fazer isso?O $mdc(119,35)$ aqui é importante? Claro que sim. Como $mdc(119,35) = 7$, logo o termo da direita tem que ser múltiplo de 7, o que não acontece. Assim, a equação não tem soluções inteiras.

Podemos agora responder a seguinte pergunta que surge de modo natural: Quando uma equação do tipo $ax + by = c$, tem solução inteira?

Como $ax + by$ será sempre múltiplo do $mdc(a, b)$, o termo c também deve ser. Caso contrário, a equação não tem solução.

Proposição 4.2: *Sejam* $a, b \in \mathbb{N}^*$ e $c \in \mathbb{N}$, *a equação* $aX + bY = c$ *admite solução em números naturais se, e somente se,* $mdc(a,b)|c$.

Prova: Se $a\ e\ b$ são primos entre si, a prova é imediata, pois $mdc(a,b) = 1$ e $1|c$.

No caso de $a\ e\ b$ não serem primos entre si temos o seguinte:

Seja $d = mdc(a,b)$. Assim $d|a\ \ e\ \ d|b$. Mas isso significa que $d|aX\ \ e\ \ d|bY$. Assim

$$d|aX\ \ e\ \ d|bY \Leftrightarrow d|(aX + bY) = c \Leftrightarrow\ \ mdc(a,b)|c. \quad \blacksquare$$

Proposição 4.3: Seja x_0, y_0 a solução minimal da equação $aX - bY = c,\ onde\ mdc(a,b) = 1$. Então, as soluções $x, y\ \ em\ \ \mathbb{N}$ da equação são

$$\begin{cases} x = x_0 + tb\ \ para\ t \in \mathbb{N} \\ y = y_0 + ta\ \ para\ t \in \mathbb{N} \end{cases}$$

Prova: Seja x, y uma solução de $aX - bY = c$, logo, $ax_0 - by_0 = ax - by = c$. Consequentemente, $a(x - x_0) = b(y - y_0)\ (*)$. Como $mdc(a,b) = 1$, segue-se que $b|(x - x_0)$. Logo, $x - x_0 = tb, t \in \mathbb{N}$. Substituindo a expressão de $x - x_0\ acima\ (*)$, segue-se que $y - y_0 = ta$, o que prova que as soluções são do tipo exibido. $\blacksquare$

Assim, $5x + 3y = 1$ tem solução pois $mdc(5,3) = 1$ e 1 divide 1. Já $3x + 6y = 4$ não tem solução pois $mdc(3,6) = 3$ e 3 não divide 4. Como até aqui verificamos a solução de uma equação diofantina por tentativa e erro, agora temos condições de verificar se uma equação tem ou não solução.

Dessa maneira, surge uma outra pergunta: **Se a equação tiver solução como encontrá-la?** Vamos encontrar uma solução para a equação $5x + 3y = 1$ pelo processo e não por tentativa.

1º passo: Começamos fazendo o algoritmo de Euclides

Quociente		1	1	
	5	3	2	1
Resto	2	1	0	

$mdc(5,3) = 1$

Como $mdc(5,3) = 1$ e 1 divide 1, a equação tem solução. Vejamos as etapas que foram feitas:

$$5 = 1 \cdot 3 + 2 \Longrightarrow 2 = 5 - 1 \cdot 3$$

$$3 = 1 \cdot 2 + 1 \Longrightarrow 1 = 3 - 1 \cdot 2$$

Agora, vamos refazer o $mdc(5,3)$, ou seja, de trás para frente. Assim,

$$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (5 - 1 \cdot 3) = 5.(-1) + 3.(2)$$

Podemos observar que escrevemos $1 = 5 \cdot (-1) + 3 \cdot (2)$ ou seja, $x = -1 \ \ e \ y = 2$ como havíamos verificado. Até aqui encontramos uma solução para uma Equação Diofantina Linear (EDL); ***agora, como encontrar todas as soluções inteiras de uma EDL?*** Vamos calcular todas as soluções inteiras da equação $5x + 3y = 1$.

Como já vimos anteriormente, uma solução dessa equação é $x = -1 \ \ e \ \ y = 2$. Assim, podemos somar e subtrair o mesmo valor ao primeiro termo que a equação será equivalente. Mas que número escolheremos? Escolheremos exatamente o $mmc(5,3) = 15$ pois nos ajudará na fatoração. Então $5x + 3y + 15 - 15 = 1$. Arrumando temos que $5x + 15 + 3y - 15 = 1 \Longrightarrow 5(x + 3) + 3(y - 5) = 1$. ***O que isso quer dizer?***

Significa que ao somarmos três unidades ao valor de x, devemos subtrair cinco unidades ao valor de y para que a equação continue verdadeira, ou seja, acharíamos outras soluções. Assim, x' e y' dadas por

$$\begin{cases} x' = x_0 + 3 = -1 + 3 = 2 \\ y' = y_0 - 5 = \ \ 2 - 5 = -3 \end{cases}$$

também é uma solução da equação $5x + 3y = 1$. Portanto, a solução geral, ou seja, todas as soluções da equação $5x + 3y = 1$ são dadas para $t \in \mathrm{Z}$ por

$$\begin{cases} x = -1 + 3t \\ y = 2 - 5t \end{cases}$$

Obtivemos assim uma maneira de encontrarmos todas as soluções inteiras de uma EDL $ax + by = c$. Mas se quiséssemos encontrar apenas soluções naturais? Como procederíamos?

Quando $ax - by = c$ o processo é idêntico à verificação das soluções inteiras. Assim, o que nos interessa é verificar as soluções naturais na equação $ax + by = c$.

Vamos examinar, por exemplo, a equação $3x + 4y = 2$. Por tentativa, concluímos que a equação não tem solução nos números naturais, pois $3x + 4y$ será sempre maior que 2.

Então como verificar se uma equação $ax + by = c$ tem solução nos números naturais?Algumas perguntas precisam ser respondidas, tais como:

- O $mdc(a, b)$ é importante nessa verificação?
- O que mais precisaríamos para acharmos uma solução?

O processo é idêntico sendo que teríamos que verificar quais soluções são naturais. Seria uma quantidade limitada de soluções, pois as soluções dependeriam do parâmetro t. Vejamos um exemplo.

Exemplo 4.4: Vamos achar as soluções naturais de $3x + 4y = 20$. Podemos notar claramente que $(0,5)$ é uma solução natural. Assim,

$$3x + 12 + 4y - 12 = 20 \Longrightarrow 3(x + 4) + 4(y - 3) = 20$$

Portanto temos que: $x = 4t \ \ e \ \ y = 5 - 3t$. Como:

$$\begin{cases} x = 4t \geq 0 \Leftrightarrow t \geq 0 \\ y = 5 - 3t \geq 0 \Leftrightarrow t \leq \frac{5}{3}. \end{cases}$$

Assim, os valores possíveis para t são $0 \leq t \leq 1$ e portanto temos 2 soluções naturais:

- Caso: $t = 0 \Longrightarrow x = 0 \ \ e \ \ y = 5$
- Caso: $t = 1 \Longrightarrow x = 4 \ \ e \ \ y = 2$.

Logo temos que $(0,5) \ \ e \ \ (4,2)$ são as únicas soluções naturais da equação.

Seria interessante mostrar a equação diofantina contextualizada. Assim poderíamos colocar problemas como o seguinte:

Problema 4.5: João foi ao banco retirar $R\$\,50{,}00$ para seu gasto semanal com condução. Chegando ao banco havia disponível no caixa eletrônico notas de 2 reais e notas de 10 reais. De quantas e quais maneiras diferentes ele poderia retirar esse dinheiro?

Solução: Vamos considerar que temos uma quantidade x de notas de 2 reais e uma quantidade y de notas de 10 reais. Assim a equação $2x + 10y = 50$ é equivalente a equação $x + 5y = 25$.

Podemos notar que $(25,0)$ é uma solução natural da equação. Portanto podemos escrever que $x + 5 + 5y - 5 = 25 \Longrightarrow 1(x + 5) + 5(y - 1) = 25.$

Isso quer dizer que

$$\begin{cases} x = 25 + 5t \\ y = -t \end{cases}$$

e como as soluções precisam ser números naturais temos que

$$\begin{cases} 25 + 5t \geq 0 \Leftrightarrow\ t \geq -5 \\ -t \geq 0 \quad \Leftrightarrow\ t \leq 0 \end{cases}$$

e para satisfazer as duas condições $-5 \leq t \leq 0$. A seguir temos uma tabela com as soluções desejadas.

$\boldsymbol{t}$	$\underbrace{\boldsymbol{x = 25 + 5t}}_{\textbf{notas de 2 reais}}$	$\underbrace{\boldsymbol{y = -t}}_{\textbf{notas de 10 reais}}$	**Solução** $\boldsymbol{(x, y)}$
$\mathbf{0}$	$\mathbf{25}$	$\mathbf{0}$	$\mathbf{(25, 0)}$
$\mathbf{-1}$	$\mathbf{20}$	$\mathbf{1}$	$\mathbf{(20, 1)}$
$\mathbf{-2}$	$\mathbf{15}$	$\mathbf{2}$	$\mathbf{(15, 2)}$
$\mathbf{-3}$	$\mathbf{10}$	$\mathbf{3}$	$\mathbf{(10, 3)}$
$\mathbf{-4}$	$\mathbf{5}$	$\mathbf{4}$	$\mathbf{(5, 4)}$
$\mathbf{-5}$	$\mathbf{0}$	$\mathbf{5}$	$\mathbf{(0, 5)}$

Vejamos outra situação.

Exemplo 4.6: Ache as quatro menores soluções naturais da equação da reta

$$r: y = \frac{3}{2}x + 7.$$

Multiplicando toda a equação por 2, temos que:

$$3x - 2y = -14 \Longrightarrow 3x + 6 - 2y - 6 = -14 \Longrightarrow 3(x + 2) - 2(y + 3) = -14.$$

Como $(-2,4)$ é uma solução dessa equação, podemos escrever que:

$$\begin{cases} x = -2 + 2t \\ y = 4 + 3t \end{cases}$$

Como x e y precisam ser não negativos temos que

$$\begin{cases} -2 + 2t \geq 0 \Longrightarrow t \geq 1 \\ 4 + 3t \geq 0 \Longrightarrow 3t \geq -4 \Longrightarrow t \geq -\frac{4}{3} \end{cases}$$

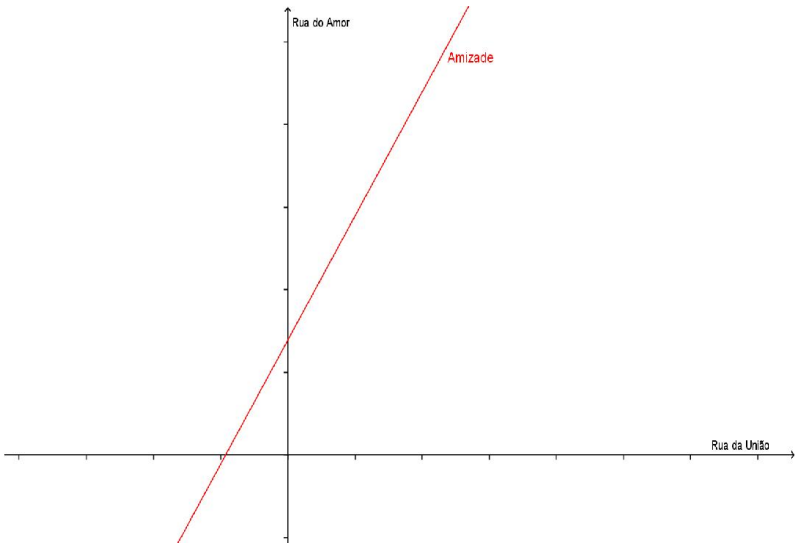
Para satisfazer as duas condições temos que $t \geq 1$. A seguir temos uma tabela com as soluções desejadas.

t	$\underbrace{x = -2 + 2t}_{\text{abscissa do ponto}}$	$\underbrace{y = 4 + 3t}_{\text{ordenada do ponto}}$	$\boldsymbol{solu}$ção (x, y)
1	**0**	**7**	$(0, 7)$
2	**2**	**10**	$(2, 10)$
3	**4**	**13**	$(4, 13)$
4	**6**	**16**	$(6, 16)$

Vejamos a mesma situação contextualizada :

"Arnaldo, Bernaldo, Cernaldo e Dernaldo são quadrigêmeos de Florisnaldo e Macabéa. Eram tão unidos que quando casaram foram morar na mesma rua: a Rua da Amizade. Essa rua é transversal às ruas perpendiculares chamadas União e Amor."

Veja o esboço das ruas.

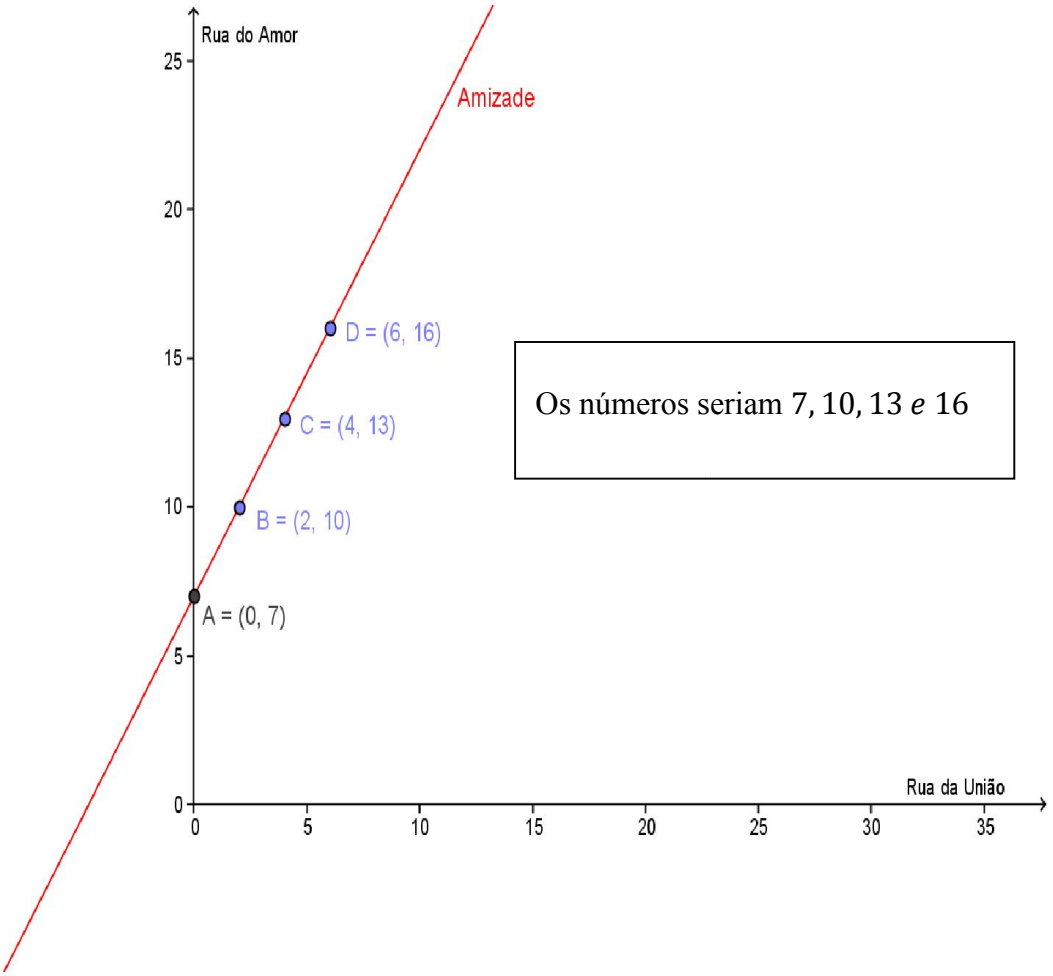


Determine os números das casas dos quatro irmãos sabendo que:

- *A rua da Amizade em relação as outras duas ruas pode ser representada como a equação da reta* $r: y = \frac{3}{2}x + 7$.

- *Os números de suas casas são formados pelas ordenadas inteiras dos pares ordenados pertencentes a esta reta.*
- *Os números de suas casas são os quatro menores números formados nessas condições.*
- *Lembre que não existe número de casa negativo.*

Fazendo os cálculos já vistos anteriormente teríamos os números $7,10,13\ e\ 16$.



Os números seriam $7, 10, 13\ e\ 16$

Se tivéssemos 3 variáveis, teríamos a equação de um plano. E como resolveríamos? Usaríamos o mesmo processo sendo que em duas etapas.

Exemplo 4.7: Ache as soluções inteiras da equação do plano $10x + 9y + 5z = 2$.

Como o $\text{mdc}(10, 9, 5) = 1$ *e* 1 divide 2, temos que a equação do plano tem solução inteira.Vamos denotar

$$10x + 9y = w.$$

Assim podemos escrever que $10x + 9y = w$ e que uma solução (x_0, y_0) dessa equação é $(w, -w)$. Então somando e subtraindo o $mmc(10,9) = 90$ segue que

$$10x + 90 + 9y - 90 = w \Longrightarrow 10(x + 9) + 9(y - 10) = w.$$

Podemos afirmar então que:

$$(I) \quad \begin{cases} x = w + 9t \\ y = -w - 10t \end{cases}$$

Podemos escrever também da equação original $\underbrace{10x + 9y}_{} + 5z = 2$ a equação $w + 5z = 2$ e uma solução particular (w_0, z_0) dada por $w_0 = 12 \ e \ z_0 = -2$. Assim,

$$w + 5 + 5z - 5 = 2 \Longrightarrow 1(w + 5) + 5(z - 1) = 2.$$

Desse modo temos que:

$$(II) \quad \begin{cases} w = 12 + 5t \\ z = -2 - t \end{cases}$$

Substituindo (II) em (I) temos:

$$\begin{cases} x = 12 + 14t \\ y = -12 - 15t \\ z = -2 - t \end{cases}$$

Portanto, essas são as soluções inteiras da equação do plano $10x + 9y + 5z = 2$.

CAPÍTULO 5 - TEOREMA CHINÊS DOS RESTOS

Na verdade vamos resolver sistemas de Equações Diofantinas, que podem modelar vários problemas interessantes, e aprender, como podemos resolvê-los através de um resultado clássico da literatura, conhecido como o Teorema Chinês dos Restos.

Dizem que o Teorema chinês dos restos surgiu com os antigos generais chineses, pois esses costumavam contar suas tropas perdidas após a guerra da seguinte forma: Ordenavam que as tropas formassem várias colunas com um determinado tamanho e depois contavam quantas sobravam e faziam isto para vários tamanhos diferentes.
Um exemplo que trata dessa questão é esse.

Problema 5.1: Digamos que um general chinês possuía 1200 tropas antes da guerra. Após a guerra, ele alinhou as tropas de 5 em 5 de forma que sobraram 3 tropas. Quando alinhou de 6 em 6 também sobraram 3 tropas; quando alinhou de 7 em 7 sobrou 1 tropa e quando alinhou de 11 em 11 não sobrou nenhuma tropa. Quantas tropas o general tinha?

Solução: Para resolver este problema, é necessário saber lidar com congruências. Além disso, vamos utilizar uma poderosa arma em teoria dos números chamada de Teorema Chinês dos Restos. Basta então um pequeno esforço para interpretar o problema.

Quando o general alinha suas tropas formando colunas de tamanho n, ele está realizando uma divisão do número de tropas por n, e depois verificando seu resto. Observe que na prática contar o resto é muito mais fácil que contar o número total ou o quociente. Aliás, quem conhece um pouco de Teoria dos números, sabe que raramente estamos interessados no quociente, o resto é o que importa.

Teorema Chinês do Resto: Sejam $n_1, n_2, \dots, n_k$ inteiros, relativamente primos dois a dois (isto é, tais que $i \neq j$, então $mdc(n_i, n_j) = 1$), e sejam $c_1, c_2, \dots, c_k$ inteiros arbitrários. Então, o sistema de congruências lineares abaixo admite uma solução, que é única módulo $n = n_1 n_2 \dots n_k$

$$\begin{cases} a_1 X \equiv c_1 (mod\ n_1) \\ a_2 X \equiv c_2 (mod\ n_2) \\ \vdots \\ a_k X \equiv c_k (mod\ n_k) \end{cases}$$

Prova: Consideremos o número $n = n_1 n_2 \dots n_k$. Para cada índice i definimos então

$$N_i = \frac{n}{n_i}.$$

Como N_i é o produto de todos os inteiros $n_1, \dots, n_k$e eles são relativamente primos com n_i, segue que $mdc(N_i, n_i) = 1$. Podemos determinar então inteiros r_i, s_i tais que

$$r_i N_i + s_i n_i = 1, 1 \leq i \leq k. \qquad (I).$$

Mostraremos, então, que o número x_0 a seguir é uma solução do sistema dado.

$$x_0 = c_1 r_1 N_1 + c_2 r_2 N_2 + \cdots + c_k r_k N_k$$

De fato, observamos inicialmente que se $j \neq i$, então $N_j \equiv 0 (mod\ n_i)$, pois n_i é um dos fatores de N_j, logo, $c_j r_j N_j \equiv 0 (mod\ n_i)$, donde segue que

$$x_0 = c_1 r_1 N_1 + c_2 r_2 N_2 + \cdots + c_k r_k N_k \equiv c_i r_i N_i (mod\ n_i).$$

Ainda, de (I), vem que $r_i N_i \equiv 1 (mod\ n_i)$, logo,

$$x_0 \equiv c_i r_i N_i \equiv c_i (mod\ n_i),$$

isto é, x_0 é solução da equação $X \equiv c_i (mod\ n_i)$, para cada i, consequentemente, é uma solução do sistema. Resta unicamente mostrar que toda outra solução é congruente a x_0 *módulo* n. Se x é outra solução, temos que

$$x_0 \equiv c_i (mod\ n_i) \quad 1 \leq i \leq k.$$

Como também $x_0 \equiv c_i (mod\ n_i)$, da transitividade da relação de congruência vem que

$$x \equiv x_0 (mod\ n_i),$$

isto é, $n_i | (x - x_0)$, para cada $i, 1 \leq i \leq k$. Ainda, como os inteiros n_i são relativamente primos, temos que

$$n_1 n_2 \dots n_k | (x - x_0),$$

logo, $x \equiv x_0 (mod\ n)$. ■

A nossa intenção é transmitir esse teorema numa linguagem que o aluno do 8º ano do ensino fundamental entenda e consiga aplicá-lo.Vejamos o problema das tropas do general chinês.

O problema diz que juntando as tropas de 5 em 5 sobram 3 tropas. Assim podemos colocar que o número de tropas procuradas é da forma $5k + 3$. Ajuntando as tropas de 6 em 6 também sobram 3 tropas e dessa forma afirmar que o número de tropas procuradas é da forma $6k + 3$. Ajuntando as tropas de 7 em 7 sobra apenas uma tropa. Portanto o número de tropas procuradas é da forma $7k + 1$. E por fim ficamos cientes que o número de tropas procuradas é um múltiplo de 11 ,ou seja, é da forma $11k$. Então podemos afirmar que x pode ser escrito das seguintes formas:

$$\begin{cases} 5k + 3 \\ 6k + 3 \\ 7k + 1 \\ 11k \end{cases}$$

Podemos aplicar o teorema chinês dos restos, pois $5, 6, 7\ e\ 11$ são primos entre si.

Vamos colocar $5 \cdot 6 \cdot n$ sendo da forma $7k + 1$ ou seja

$$5 \cdot 6 \cdot n = 7k + 1 \Longrightarrow 30n = 7k + 1$$

que pela aritmética dos restos implica que

$$28n + 2n = 7k + 1 \Longrightarrow 2n = 7k + 1, k \in \mathbb{N}.$$

Isso é verdadeiro, pois $28n$ é da forma $7k, k, n \in \mathbb{N}$. Assim, temos que $n = 4$ e, portanto $5.6.4 = 120$. ***O que significa isso?*** Significa que 120 é múltiplo de 5, é múltiplo de 6 e é da forma $7k + 1$.

Agora vamos fazer $5.7.n$ sendo da forma $6k + 1, k \in \mathbb{N}$ ou seja,

$$5 \cdot 7 \cdot n = 6k + 1 \Longrightarrow 35n \equiv 6k + 1 \Longrightarrow 30n + 5n = 6k + 1 \Longrightarrow 5n = 6k + 1, k \in \mathbb{N}.$$

Isso é verdadeiro, pois $30n$ é da forma $6k, k, n \in \mathbb{N}$. Assim, temos que $n = 5$ e, portanto $5 \cdot 7 \cdot 5 = 175$. ***O que significa isso?*** Significa que 175 é múltiplo de 5, é múltiplo de 7 e é da forma $6k + 1$. Como queremos que o número seja da forma $6k + 3$, pela aritmética dos restos basta multiplicar $175 \cdot 3 = 525$.

Portanto 525 é da forma $6k + 3$.

Por fim precisamos descobrir um número natural que seja múltiplo de 6, múltiplo de 7 mas que seja da forma $5k+1, k \in \mathbb{N}$ e depois aplicar a aritmética dos restos para acharmos um número da forma $5k+3$. Assim, temos que

$$6 \cdot 7 \cdot n = 5k+1 \Longrightarrow 42n = 5k+1 \Longrightarrow 40n + 2n = 5k+1.$$

Como $40n = 5k_2$, para algum $k_2, n \in \mathbb{N}$, temos que $2n = 5k_3 + 1$, também para algum $k_3, n \in \mathbb{N}$. Nesse caso, temos que para $k_3 = 1 \Longrightarrow n = 3$. Então o menor número natural nas condições dadas é $6 \cdot 7 \cdot 3 = 126$. Isso significa que 126 é múltiplo de 6, múltiplo de 7 e é da forma $5k+1, k \in \mathbb{N}$. Como queremos que o número seja da forma $5k+3$, pela aritmética dos restos basta multiplicarmos $126 \cdot 3 = 378$. Assim 378 é da forma $5k+3$. Então temos que:

120 é múltiplo de 5, múltiplo de 6 e é da forma $7k+1$.

525 é múltiplo de 5, múltiplo de 7 e é da forma $6k+3$.

378 é múltiplo de 6, múltiplo de 7 e é da forma $5k+3$.

Aplicando a aritmética dos restos quanto à adição temos que:

$$120 + 525 + 378 = 1023 = \begin{cases} 7k+1 \\ 6k+3 \\ 5k+3 \end{cases}, k \in \mathbb{N}.$$

Como 1023 é menor do que 1200 e ao mesmo tempo é múltiplo de 11, logo 1023 é da forma $11k, k \in \mathbb{N}$, temos que a quantidade de tropas do general após a guerra é 1023.

Problema 5.2: Este problema é da prova MA14 – AV3 – 2011.

> *" Quando um macaco sobe uma escada de dois em dois degraus, sobra um degrau, quando sobe de três em três degraus, sobram dois degraus e quando sobe de cinco em cinco degraus sobram três degraus. Quantos degraus possui a escada, sabendo que o úmero de degraus está entre* 150 *e* 200*."*

Solução: Queremos encontrar um número que seja simultaneamente, das formas:

$$\begin{cases} n = 2k+1 \\ n = 3k+2 \\ n = 5k+3 \end{cases}, \quad k \in \mathbb{Z},\ 150 < n < 200$$

Assim, precisamos achar um número que seja:

1) Múltiplo de 2, múltiplo de 3 e múltiplo de 5 somado a 3;
2) Múltiplo de 3, múltiplo de 5 e múltiplo de 2 somado a 1;
3) Múltiplo de 2, múltiplo de 5 e múltiplo de 3 somado a 2;

De fato:

1) Vejamos um número que tenha a primeira condição. Para isso vamos achar um número que seja das formas $2k, 3k \; e \; 5k + 1$ e depois aplicarmos a aritmética dos restos. Assim,

$$2 \cdot 3 \cdot n = 5k + 1 \Longrightarrow 6n = 5k + 1 \Longrightarrow \; 5n + n = 5k + 1.$$

Como $5n$ é da forma $5k$, temos que n é da forma $5k + 1$. Para $k = 1$, temos que $n = 6$. Assim, o número $2.3.6 = 36$ é da forma $5k + 1$.

Portanto o número que queremos é $\mathbf{36 \cdot 3 = 108}$ que será da forma $\mathbf{5k + 3}$.

2) Vejamos um número que tenha a segunda condição. Para isso vamos achar um número que seja das formas $3k, 5k \; e \; 2k + 1$. Assim,

$$3 \cdot 5 \cdot n = 2k + 1 \Longrightarrow 15n = 2k + 1 \Longrightarrow 14n + n = 2k + 1.$$

Como $14n = 2(7n)$ é da forma $2k$ temos que n é da forma $2k + 1$. Para $k = 1$, temos que $n = 3$.

Assim, o número $\mathbf{3 \cdot 5 \cdot 3 = 45}$ será da forma $\mathbf{2k + 1}$ como queremos.

3) Vejamos um número que tenha a terceira condição. Para isso vamos achar um número que seja das formas $2k, 5k \; e \; 3k + 2$. Assim,

$$2 \cdot 5 \cdot n = 3k + 1 \Longrightarrow 10n = 3k + 1 \Longrightarrow 9n + n = 3k + 1.$$

Como $9n = 3(3n)$ é da forma $3k$, temos que n é da forma $3k + 1$. Para $k = 1$, temos que $n = 4$. Assim, o número $2 \cdot 5 \cdot 4 = 40$ é da forma $3k + 1$.

Portanto o número que queremos é $\mathbf{40 \cdot 2 = 8\ 0}$que será da forma $\mathbf{3k + 2}$.

Dessa forma temos que $108 + 80 + 45 = 233$ é da forma

$$\begin{cases} 2k + 1 \\ 3k + 2 \\ 5k + 3 \end{cases}$$

Então o número que queremos é $n = 233 + \underbrace{30}_{mmc(2,3,5)} t \quad e \quad 150 < 233 + 30t < 200$, temos que $t = -2$ e consequentemente, o número de degraus é 173.

Problema 5.3: Esse problema está adaptado da questão que caiu no ENQ-2012.

Descubra o número, menor do que 1000, que dividido por 9 deixa resto 7, dividido por 10 deixa resto 8 e dividido por 11 deixa resto 9.

Solução: Do enunciado temos que esse número é um múltiplo de 9 somado a 7, um múltiplo de 10 somado a 8 e um múltiplo de 11 somado a 9. O número n procurado pode ser escrito como:

$$\begin{cases} n = 9k + 7 \\ n = 10k + 8 \\ n = 11k + 9 \end{cases}$$

Primeiramente vamos achar um número que seja múltiplo de 10, múltiplo de 11 e seja da forma $9k + 1$. Depois, aplicaremos a aritmética dos restos e acharemos o número da forma $9k + 7$. Assim, $10 \cdot 11 \cdot n = 9k + 1, k, n \in \mathbb{N}$. Temos que

$$110n = 9k + 1 \implies 108n + 2n = 9k + 1.$$

Como $108n$ é da forma $9k$ para algum $k, n \in \mathbb{N}$, temos que $2n$ é da forma $9k + 1$ e dessa forma temos que se $k = 1 \implies n = 5$. Assim, $10 \cdot 11 \cdot 5 = 550$ é da forma $9k + 1$. Aplicando a aritmética dos restos temos que

$$550 \cdot 7 = 3850 = 9k + 7, k \in \mathbb{N}$$

ou seja,3850 é múltiplo de 10, é múltiplo de 11 e será da forma $9k + 7$.

De maneira semelhante, temos que achar um número que seja múltiplo de 9, múltiplo de 11 mas que seja da forma $10k + 1$. Aplicaremos depois a aritmética dos restos e acharemos o número da forma $10k + 8$. Assim, $9 \cdot 11 \cdot n = 10k + 1, k, n \in \mathbb{N}$. Então

$$99n = 10k + 1 \implies 90n + 9n = 10k + 1.$$

Como $90n$ é da forma $10k$, para algum $k, n \in \mathbb{N}$, termos que $9n$ é da forma $10k + 1$. Percebemos facilmente que se $k = 8 \implies n = 9$. Dessa maneira,

$$9 \cdot 11 \cdot 9 = 891 = 10k + 1, k \in \mathbb{N}.$$

Aplicando a aritmética dos restos, temos que

$$891 \cdot 8 = 7128 = 10k + 8, \quad k \in \mathbb{N},$$

ou seja,7128 é múltiplo de 9, múltiplo de 11 e é da forma $10k + 8$.

Finalmente, temos que achar um número que seja ao mesmo tempo múltiplo de 9, múltiplo de 10 e seja da forma $11k + 1$ para depois aplicarmos a aritmética dos restos e acharmos o número procurado da forma $11k + 9$. Então temos $9 \cdot 10 \cdot n = 11k + 1, k, n \in \mathbb{N}$. Assim,

$$90n = 11k + 1 \Longrightarrow \ 88n + 2n = 11k + 1.$$

Como $88n$ é da forma $11k$, para algum $k, n \in \mathbb{N}$, temos que $2n$ é da forma $11k + 1$. Percebemos facilmente que se $k = 1 \Longrightarrow n = 6$. Assim, $9 \cdot 10 \cdot 6 = 540 = 11k + 1, k \in \mathbb{N}$. Aplicando a aritmética dos restos, temos que

$$540 \cdot 9 = 4860 = 11k + 9, \ \ k \in \mathbb{N}.$$

Aplicando novamente a aritmética dos restos percebemos que:

$$3850 + 7128 + 4860 = 15838$$

pode ser escrito como $9k + 7, 10k + 8 \ \ ou \ \ 11k + 9, k \in \mathbb{N}$. Mas também podemos escrever

$$15838 = \underbrace{(9 \cdot 10 \cdot 11)t + R}_{teorema} \quad \Rightarrow \ \ 15838 = 990 \cdot 15 + 988$$

Portanto, o número procurado é 988.

CAPÍTULO 6 - ATIVIDADES EM SALA DE AULA

Nesse capítulo propusemos alguns exercícios para os alunos do 9° ano do Colégio Santamarinha onde trabalhamos esses conceitos em 5 (cinco) encontros de $3h$ cada um.

O objetivo dessas atividades é propiciar a esse aluno o desafio de tentar resolvê-los com o que aprenderam sobre os pontos de teoria dos números exposto nesse trabalho. Ao final dos exercícios propostos temos as soluções dos mesmos.

1ª aula: Divisão Euclidiana e Aplicação do Lema de Euclides

1) Quando o inteiro x é dividido pelo inteiro y, o quociente é q e o resto é r. Qual é o resto da divisão de $x + 2qy\ por\ y$? $Resp: r$

2) O resto da divisão do inteiro N por 20 é 8. Qual é o resto da divisão de N por 5? Resp: 3

3) Calcule o $MDC[1960,1050]$. $Resp: 70$

4) Expresse o $MDC[-180,252]$ na forma $x(-180) + y(252)$

$$Resp: 36 = (-3) \cdot (-180) + (-2) \cdot (252)$$

5) Mostre que, para todo $n \in \mathbb{N}$, a fração $\frac{21n+4}{14n+3}$ é irredutível.

2ª aula: Aritmética dos restos e Fatoração

6) Determine o resto da divisão de $14543^{567}\ \ por\ \ 3$. $Resp: 2$

7) Seja N um número natural; prove que a divisão de N^2 por 6 nunca deixa resto 2.
Sugestão: use $N = 6k + r, 0 \leq r < 6$.

8) Mostre, para todo $a \in N$, que:
a) $2|a^2 - a$ b) $3|a^3 - a$ c) $5|a^5 - a$ Sugestão: use a fatoração

9) Determine o menor natural N para o qual $1260.N = x^3, sendo\ x\ um\ inteiro.$ $Resp: 7350$

10) Descubra o menor número natural da forma $n! = n(n-1)\cdots\cdots\cdot 1$, múltiplo de 1000.

3ª aula: Equações Diofantinas e Diversos

11) Ache as soluções inteiras da equação $2x + 5y = 1$ $Resp: x = 5t - 2\ \ e\ \ y = 1 - 2t, t \in \mathrm{Z}$

12) Ache as soluções inteiras da equação $29x + 21y = 6$ $Resp: x = 6 + 21t\ \ e\ \ y = -8 - 29t,\ \ t \in \mathrm{Z}$

13) Subindo uma escada de dois em dois degraus sobra um degrau. Subindo a mesma escada de três em três degraus sobram dois degraus. Determine quantos degraus possui a escada sabendo que o seu número é um múltiplo de 7 e está compreendido entre $40\ e\ 100$. Resp: 77

14) Qual é o menor número primo que deixa restos $2, 3\ e\ 2$ quando dividido respectivamente por $3, 5\ e\ 7$? Resp: 23

15) De quantas maneiras pode-se comprar selos de 3 reais e de 5 reais de modo que se gaste 50 reais? R: 4 maneiras

16) Joaquim disse para sua professora que tinha inventado um novo tipo de número: os primos em segundo grau. São números que tem apenas três divisores, disse ele. Assim, continuou Joaquim, o número 4 é um primo em segundo grau pois os divisores de 4 são $1, 2\ e\ 4$.

a) Que outro número entre $1\ e\ 10$ é um primo em segundo grau?

b) Descubra os primos em segundo grau que estão entre $850\ e\ 1000$.

c) Há uma relação entre os números primos, os números quadrados e os números primos em segundo grau. Descubra essa relação e explique-a.

Resp: a) 9 b) $900\ e\ 961$ c) Os números primos em segundo grau são os quadrados dos números primos.

17) “Deus lhe concedeu a graça de ser um menino pela sexta parte de sua vida. Depois por um doze avos, ele cobriu seu rosto com a barba. A luz do casamento iluminou o após a sétima parte e cinco anos depois do casamento. Ele concedeu-lhe um filho. Ah! Criança tardia e má, depois de viver metade da vida de seu pai o destino frio o levou. Após consolar sua mágoa em sua ciência dos números, por quatro anos,. Diofanto terminou sua vida.” Quanto tempo viveu Diofanto? Resp: $84\ anos$

Solução das Atividades:

1) Como $x = qy + r \Longrightarrow x + 2qy = 3qy + r \ \ e \ \ (3qy + r) \div y = (3qy) \div y + r \div y$ e portanto o resto é r pois $r < y$.

2) $n = 20q + 8 \Longrightarrow n = 4 \cdot 5q + 8$ e, portanto o resto será igual a $8 = 1 \cdot 5 + 3$. Então temos que $n = 5q + 3$ e, portanto o resto é igual a 3.

3) $(1960,1050) = (1050,1960 - 1 \cdot 1050) = (1050,910) = (910,1050 - 1 \cdot 910) =$
$= (910,140) = (140,910 - 6 \cdot 140) = (140,70) = 70.$

4) $\text{mdc}(-180,252) = 36$ e $252 = 1 \cdot 180 + 72 \, ; 180 = 2 \cdot 72 + 36 \, ; 36 = 180 - 2 \cdot 72$
temos que: $36 = 180 - 2(252 - 180) \Longrightarrow 36 = 3 \cdot 180 - 2 \cdot 252$. Assim, temos que
$$36 = (-3) \cdot (-180) + (-2) \cdot (252).$$

5) Temos que mostrar $(21n + 4,14n + 3) = 1$.
Assim, $(21n + 4, 14n + 3) = (21n + 4 - 14n - 3, 14n + 3) = (7n + 1,14n + 3) =$
$(7n + 1, 14n + 3 - 14n - 2) = (73 + 1, 1) = 1.$

6) Como $14543 = 3k + 2, k \in \mathbb{Z}$, aplicando a aritmética dos restos temos que:
$14543^2 = 14543 \cdot 14543 = (3k + 2) \cdot (3k + 2) = 3k' + 1$.
Assim, $(14543)^{567} = (14543^2)^{283} \cdot 14543$
Aplicando a aritmética dos restos teremos que o resto de $(14543)^{567}$ por 3 será igual a:
$(1)^{283} \cdot 2 = 2.$

7) $N = 6k + r, \ 0 \leq r < 6$

$$N = 6k \Longrightarrow N^2 = 6k' \Longrightarrow r = 0,$$
$$N = 6k + 1 \Longrightarrow N^2 = 6k' + 1 \Longrightarrow r = 1$$
$$N = 6k + 2 \Longrightarrow N^2 = 6k' + 4 \Longrightarrow r = 4$$
$$N = 6k + 3 \Longrightarrow N^2 = 6k' + 3 \Longrightarrow r = 3$$
$$N = 6k + 4 \Longrightarrow N^2 = 6k' + 4 \Longrightarrow r = 4$$
$$N = 6k + 5 \Longrightarrow N^2 = 6k' + 1 \Longrightarrow r = 1$$

8) a) $a^2 - a = a(a-1)$ e, portanto um dos dois é par, pois são consecutivos.

b) $a^3 - a = a(a^2-1) = (a-1)(a)(a+1)$ e, portanto um dos três é múltiplo de três.

se $a = 3k$, ok

se $a = 3k+1 \Longrightarrow a - 1 = 3k$, ok

se $a = 3k+2 \Longrightarrow a + 1 = 3k$, ok

c) $a^5 - a = a(a^4-1) = a(a^2+1)(a^2-1) = (a-1)(a)(a+1)(a^2+1)$ e um deles é múltiplo de 5.

se $a = 5k$, ok

se $a = 5k+1 \Longrightarrow a - 1 = 5k$, ok

se $a = 5k+2 \Longrightarrow a^2 + 1 = 5k' + 5$, ok

se $a = 5k+3 \Longrightarrow a^2 + 1 = 5k' + 10$, ok

se $a = 5k+4 \Longrightarrow a + 1 = 5k + 5$, ok

9) Como x^3 é da forma ${\alpha_1}^3, {\alpha_2}^3, \cdots, {\alpha_n}^3, \alpha_i$ primo temos que $1260 \cdot N$ também será. Assim, como $1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$ vamos ter que $N = 2 \cdot 3 \cdot 5^2 \cdot 7^2 = 7350$.

10) Como $1000 = 2^3 \cdot 5^3$, o número de fatores iguais a 2 e a 5 precisam ser ,no mínimo, iguais a 3.

Basta que procuremos o número que tenha 3 fatores iguais a 5 na sua composição pois o fator 2 aparecerá com maior frequência.

Dessa forma o número procurado é $15!$ pois o fator 5 aparece 3 vezes; no próprio 5, no $10 = 2 \cdot 5$ e no $15 = 3 \cdot 5$.

11) $2x + 5y = 1$ têm uma solução $(x, y) = (3, -1)$.

Então $2x + 5y + 10 - 10 = 1 \Longrightarrow 2(x+5) + 5(y-2) = 1$.

Assim, $x = 3 + 5t \quad e \quad y = -1 - 2t$.

12) $29x + 21y = 6$ têm uma solução $(x, y) = (6, -8)$.

Então $29x + 21y + 609 - 609 = 6 \Longrightarrow 29(x+21) + 21(y-29) = 6$.

Assim, $x = 6 + 21t \quad e \quad y = -8 - 29t$.

13) Seja $2.3.n = 7k \Longrightarrow 6n = 7k$ e para $k = 6 \Longrightarrow n = 7$. Assim, $2.3.7 = 42$ é da forma $7k$.
Do mesmo modo, $3.7.n = 2k + 1 \Longrightarrow 21n = 2k + 1$ e para $k = 10 \Longrightarrow n = 1$. Assim, 21 é da forma $2k + 1$.
Semelhantemente, $2.7.n = 3k + 2 \Longrightarrow 14n = 3k + 2$ e para $k = 4 \Longrightarrow n = 11$. Assim,14 é da forma $3k + 2$.
Aplicando a Aritmética dos restos temos que:
$42 + 21 + 14 = 77$ pode ser escrito nas formas $\begin{cases} 7k \\ 2k + 1 \\ 3k + 2 \end{cases}$ e como $40 < 77 < 100$, o número de degraus é 77.

14) $N = 3k + 2 = 5k' + 3 = 7k" + 2$

Assim, $3 \cdot 5 \cdot n = 7k + 1 \Longrightarrow 15n = 7k + 1 \Longrightarrow 14n + n = 7k + 1$. Como $14n = 2n \cdot 7$, temos que n é da forma $7k + 1$. Para $k = 1 \Longrightarrow n = 8$. Assim, $3 \cdot 5 \cdot 8 = 120$ é da forma $7k + 1$ e <u>240 é da forma $7k + 2$.</u>

$3 \cdot 7 \cdot n = 5k + 1 \Longrightarrow 21n = 5k + 1 \Longrightarrow 20n + n = 5k + 1$. Como $20n = 4n \cdot 5$, temos que n é da forma $5k + 1$. Para $k = 1 \Longrightarrow n = 6$. Assim, $3 \cdot 7 \cdot 6 = 126$ é da forma $5k + 1$ e <u>378 é da forma $5k + 3$.</u>

$5 \cdot 7 \cdot n = 3k + 1 \Longrightarrow 35n = 3k + 1 \Longrightarrow 33n + 2n = 3k + 1$. Como $33n = 11n \cdot 3$, temos que $2n$ é da forma $3k + 1$. Para $k = 1 \Longrightarrow n = 2$. Assim, $5 \cdot 7 \cdot 2 = 70$ é da forma $3k + 1$ e <u>140 é da forma $3k + 2$.</u>

Então temos que $240 + 378 + 140 = 758$ pode ser escrito nas formas :
$7k + 2\,, 5k + 3\ e\ 3k + 2$ e assim $N = 758 + 3 \cdot 5 \cdot 7t$ ou seja, $N = 758 + 105t, t \in \mathbb{Z}$.
Por inspeção, temos que se $t = -7$, teremos $N = 23$.

15) x selos de 3 reais e y selos de 5 reais.

$3x + 5y = 50$ e uma solução é $(10,4)$.

Assim, $3x + 15 + 5y - 15 = 50 \Longrightarrow 3(x + 5) + 5(y - 3) = 50$.

Portanto, temos $x = 10 + 5t\ \ e\ \ y = 4 - 3t\ \ ,\ \ t \geq -2$.

$t = -2 \Longrightarrow x = 0 \ \ e \ \ y = 10$
$t = -1 \Longrightarrow x = 5 \ \ e \ \ y = 7$
$t = 0 \Longrightarrow x = 10 \ \ e \ \ y = 4$
$t = 1 \Longrightarrow x = 15 \ \ e \ \ y = 1$

16) a) Por inspeção, temos o 9 pois $D(9) = \{1,3,9\}$.

b) Como $4 = 2^2 \ \ e \ \ 9 = 3^2$, temos que $30^2 = 900 \ \ e \ \ 31^2 = 961$ são os números procurados.

c) Os números primos em segundo grau são os quadrados dos números primos.

17) Seja x a idade de Diofanto. Assim,

Assim, $x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4$. Como o $mmc(6,12,7,2) = 84$, temos que:

$84x = 75x + 756 \Longrightarrow x = 84$. Portanto, Diofanto viveu 84 $anos$.

CONCLUSÃO

Durante a elaboração deste trabalho nossa preocupação foi evidenciar as ligações que há entre conteúdos distintos da Teoria Elementar dos Números.

Explorando essas ligações percebemos o significado e funcionalidade nos conceitos trabalhados acarretando consequentemente com a assimilação desses conteúdos.

No desenvolvimento dos conteúdos abordados como também na aplicação dos mesmos foi nossa intenção colocá-los dentro de um nível de compreensão e maturidade de um aluno do Ensino Fundamental e Médio.

Na troca de ideias com professores sobre o nosso assunto, as respostas obtidas foram muito importantes. O que fizemos em termos de pesquisa e consulta a amigos para a realização desse trabalho nos possibilitou aprender muito a respeito não só do tema em estudo, mas também do ensino da Matemática em geral.

Confesso que cresci pessoal e profissionalmente com esse trabalho tendo dessa forma ampliado meus horizontes para estudos na busca de melhoria do ensino da Matemática a partir dos anos finais do Ensino Fundamental.

Por fim, esperamos que esse trabalho possa contribuir como estímulo e ao mesmo tempo servir de fonte de consulta por parte de professores e alunos que estejam interessados neste tipo de assunto buscando ampliar seus conhecimentos com a finalidade de minimizar as dificuldades encontradas no trato dessa matéria.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] – Hefez, Abramo. Elementos de Aritmética – Coleção PROFMAT – 2ª Ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2011.

[2] – Milies, Francisco César Polcino. Números: Uma Introdução à Matemática – 3ª Ed. 1 . reimpr. São Paulo: Editora da Universidade de São Paulo, 2003.

[3] – Oliveira, Krerley Irraciel Martins. Iniciação à Matemática: um curso com problemas e soluções – Rio de Janeiro: Sociedade Brasileira de Matemática, 2010.

[4] – Muniz Neto, Antônio Caminha. Tópicos de Matemática Elementar: teoria dos números – 2ª Ed. – Rio de Janeiro: Sociedade Brasileira de Matemática, 2012.

[5] – Ribenboin, Paulo. Números primos, amigos que causam problemas – Rio de Janeiro: Sociedade Brasileira de Matemática, 2015.

[6] – Morgado, Augusto César, Eduardo Wagner e Miguel Jorge. Álgebra I – Rio de Janeiro: F. Alves,1974.

[7] – Borin, Julia. Jogos e Resolução de problemas: Uma estratégia para as aulas de Matemática – 5ª Ed. – São Paulo: Instituto de Matemática e Estatística da USP, 2004.

[8] – Jurkiewicz, Samuel. Divisibilidade e Números Inteiros Introdução à Aritmética Modular – Rio de Janeiro: Programa de Iniciação científica da OBMEP, 2007.

[9] – Coutinho, S. C.. Criptografia – Rio de Janeiro: Programa de Iniciação Científica da OBMEP,2007.

[10] – Eves, Howard. Introdução à História da Matemática – Campinas, SP: Editora da UNICAMP, 2004.

[11] – Tahan, Malba. O Homem que Calculava – 25ª Ed. – Rio de Janeiro: Editora Conquista, 1975.

[12] – RPM: Revista do Professor de Matemática nº 5, 85

[13] – Indeterminação Matemática:Trabalho do Prof. Ilydio Pereira de Sá.

[14] – Apostilas do PIC: Programa de Iniciação Científica do IMPA.