Centro Federal de Educação Tecnológica de Minas Gerais
PROFMAT - Mestrado Profissional em Matemática em Rede Nacional

Thiago de Mattos Serafim

Criptografia RSA: da aritmética modular à sala de aula

Belo Horizonte
2022

Thiago de Mattos Serafim

Criptografia RSA: da aritmética modular à sala de aula

Dissertação apresentada ao Centro Federal de Educação Tecnológica de Minas Gerais como parte das exigências do Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional, para obter o título de Mestre.

Orientador
Éden Santana Campos Amorim

Banca Examinadora
Alexandre Alvarenga Rocha
Fernanda Aparecida Ferreira
Ricardo Saldanha de Morais

Belo Horizonte
2022

Serafim, Thiago de Mattos
S481c Criptografia RSA: da aritmética modular à sala de aula / Thiago de Mattos Serafim. – 2022.
84 f.

Dissertação de mestrado apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional.
Orientador: Éden Santana Campos Amorim.
Dissertação (mestrado) – Centro Federal de Educação Tecnológica de Minas Gerais.

1. Aritmética modular – Teses. 2. Criptografia de dados – Teses. 3. Proteção de dados – Teses. 4. Base Nacional Comum Curricular – Teses. I. Amorim, Èden Santana Campos. II. Centro Federal de Educação Tecnológica de Minas Gerais. III. Título.

CDD 005.82

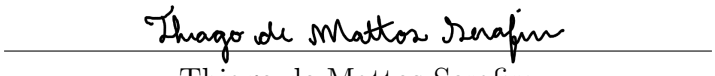
Elaboração da ficha catalográfica pela bibliotecária Jane Marangon Duarte, CRB 6º 1592 / Cefet/MG

Thiago de Mattos Serafim

CRIPTOGRAFIA RSA: DA ARITMÉTICA MODULAR À SALA DE AULA

Dissertação apresentada ao Centro Federal de Educação Tecnológica de Minas Gerais como parte das exigências do Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional, para obter o título de Mestre.

Aprovada: 27 de janeiro de 2022.



Thiago de Mattos Serafim
(Autor)

Éden Santana Campos Amorim
(Orientador)

Belo Horizonte
2022

Dedico esse trabalho à minha mãe, que foi sempre uma incentivadora aos meus estudos, mesmo que ela própria não teve tantas oportunidades para estudos formais. Dedico também ao meu saudoso pai, que estaria orgulhoso tanto de mim quanto do Galo, que vem fazendo uma bela campanha em 2021. Obrigado mãe e pai, obrigado Tina e Ciro!

Agradecimentos

Durante minha passagem por este curso, o PROFMAT, não há dúvidas de que ele cumpriu seu papel na formação continuada desse professor de matemática, tal como norteado pelo seu regimento. E cumprir o seu papel não significa somente que a minha trajetória na busca pelo título de mestre vem sendo bem sucedida. Significa também que os docentes, os colegas, a coordenação e todas as pessoas que participam de forma direta ou indireta na formação dessa turma de mestres - da qual tenho imenso orgulho de fazer parte - estão colaborando de forma relevante - seja nos processos de ensino e aprendizagem em si, seja nas diversas conversas necessárias à distância, por conta da pandemia - para que as coisas aconteçam bem. Portanto, sou grato a muitos.

Porque como base de uma conquista pessoal, em particular uma relacionada ao intelecto, além de uma necessária dedicação individual há também um feito, uma construção e uma vitória coletivos.

Fica, então, um abraço especial aos meus colegas de turma, que temo em citar nomes com medo de esquecer injustamente de algum. E não tenham dúvidas de que todos que trocaram uma resolução de exercício, uma conversa boa e até mesmo (ou especialmente) compartilharam uma cerveja, têm espaço reservado na minha vida.

Não posso deixar de agradecer também aos solícitos professores que me ajudaram nesta trilha. E, olha, ajuda não me faltou! Destaco, ainda com medo de cometer injustiças, três: a professora Érica Pagani, que foi praticamente uma coorientadora não oficial, me deu muitos direcionamentos, especialmente sobre a composição das atividades para a Educação Básica; a professora Fernanda Ferreira, que compartilhou comigo a autoria de meu primeiro artigo publicado, além de ter ministrado de maneira magistral a disciplina TCC; e claro, o meu orientador Éden Amorim, que pacientemente me conduziu nas pesquisas, nos estudos e nas escritas que culminaram nesta dissertação.

Aonde quer que nossas vidas nos levem, espero revê-los todos!

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

Resumo

Tendo como pano de fundo a Criptografia RSA, apresentamos em linhas gerais a teoria matemática que embasa este modelo de encriptação, assim como sua contextualização como parte do modo de vida atual e sua segurança, para depois propor um produto destinado ao Ensino Básico (EB). Para isso, apresentamos a ótica da Base Nacional Comum Curricular (BNCC) sobre o uso de tecnologias no ensino de matemática, além de possibilidades para o uso de calculadoras em turmas do Ensino Fundamental (EF). Antes, contudo, elementos básicos da Aritmética Modular são apresentados, construindo-se o modelo matemático que sustenta a Criptografia RSA - além da Função totiente, como um tópico adicional. Assim, guiando-nos pelo questionamento "É possível trazer a temática Criptografia RSA para o contexto de sala de aula da Educação Básica? " nosso objetivo é o de criarmos atividades em que, a partir do uso de tecnologias, conceitos de Aritmética modular sejam abordados, levando os estudantes a compreenderem o método de Criptografia RSA. Como resultado, apresentamos o produto final, direcionado à EB, composto por uma proposta de sequência didática para o 6^o ano do EF, que tem por finalidade introduzir o conceito de primalidade lançando-se mão de calculadoras, e de duas propostas de aulas para o Ensino Médio (EM), abordando-se o cálculo de restos de potências através da Aritmética Modular, ora com cálculos manuais, ora com planilhas eletrônicas. Também há sugestões de como pode se dar a abordagem das atividades propostas no EM. Por fim, conclui-se que este trabalho pode ser uma diretriz de estudos, pesquisas e práticas futuras, de forma que sua elaboração e conclusão foram exitosos no sentido de dar continuidade à formação de um professor que ensina matemática na EB.

Palavras-chave: Aritmética Modular, Criptografia RSA, BNCC.

Abstract

With RSA Cryptography as background, we present, generally speaking, the mathematical theory that underlies that encryption model, as well as its contextualization as part of the modern way of life and its security, and then proposes a product for Basic Education (BE). For this, we show the Brazilian National Common Core Curriculum (BNCC) view about the use of technologies in the mathematics teaching in addition to possibilities for the use of calculators in Elementary School (ES) classes. Before, however, basic elements of Modular Arithmetic are presented, building the mathematical model that supports RSA Cryptography - in addition to the totient function, as an additional topic. Thus, guided by the question "Is it possible to bring the RSA Cryptography theme to the Basic Education classroom?" our goal is to createactivities in which, from the use of technologies, modular arithmetic concepts are addressed, leading students to understand the RSA Encryption method. As a result, we present the final product, aimed at Basic Education, consisting of a proposal for didactic sequence for the 6th year of Elementary School, which aims to introduce the concept of primality using calculators, and two proposals for classes for the High School, approaching the calculation of residual powers through Modular Arithmetic, sometimes with manual calculations, sometimes with electronic spreadsheets. There are also suggestions on how can be approached the activities proposed in the High School. Finally, it is concluded that this work can be a guideline for future studies, research and practices, so that its elaboration and conclusion were successful in the sense of giving continuity to the formation of a teacher who teaches mathematics in Basic Education.

Keywords: Modular Aritmetics, RSA encryption, BNCC.

Lista de Figuras

Lista de Tabelas

Sumário

1 Introdução

É perceptível o vínculo estreito entre as tecnologias de informação e comunicação e a vida moderna. Enviar e receber mensagens de texto, fotos, vídeos e outros tipos de arquivos; fazer pagamentos sem mais ir a bancos ou agências lotéricas, dispondo apenas de um *smartphone*; a obsolescência dos catálogos telefônicos, com seus mapas estáticos e listas de telefones, tudo agora mais dinâmico e disponível a poucos cliques de distância; e muitas outras atividades que se tornaram mais práticas, rápidas e até mais fáceis compõem parte essencial do nosso cotidiano. Vale-se ponderar que a praticidade, rapidez e facilidade são relativas, visto que dependem em grande parte de acesso à internet e outros recursos essenciais, tais como o próprio acesso a tecnologias.

Essa relatividade também se dá porque nem todos sabem usar os recursos tecnológicos disponíveis, mesmo possuindo acesso. Nem mesmo os "nativos digitais", termo definido em [1] como as pessoas que nasceram em um mundo já globalizado e recheado de tecnologias da informação e comunicação, ou seja, os estudantes da atualidade. É fato que crianças e adolescentes adquirem rápida familiaridade com computadores, *smartphones*, *tablets* etc. e com seus aplicativos e *softwares*, entretanto qual uso fazem desses objetos é uma indagação pertinente. Assim, consideramos que também é pertinente nos indagarmos qual uso o professor faz e pode fazer desses mesmos recursos. Nesse sentido, acreditamos que a Criptografia, que de um breve modo é a ciência que trata dos assuntos ligados a codificar e decodificar informações com o intuito de proteger dados sensíveis, cumpre um papel importante. Isso se dá, pois, ao mesmo tempo que a Criptografia está muito presente no modo de vida atual, ela também é de certa forma "invisível" a muitos. Mesmo presente em várias tarefas rotineiras, ela é potencialmente desconhecida, tanto seu significado quanto sua função.

Portanto, por meio do estudo de um modelo de Criptografia, o modelo RSA, suas bases matemáticas, e considerando a importância destacada anteriormente dessa ciência e sua presença massiva nos nossos cotidianos, pretendemos através deste trabalho propor

atividades para a Educação Básica (EB) que, a partir do uso de tecnologias, abordem conceitos relacionados à Aritmética Modular, ramo da matemática que dá forma ao modelo RSA, de modo a levar à sala de aula esse método de encriptação. Como diretriz do produto criado, procuramos responder à pergunta "É possível trazer a temática Criptografia RSA para o contexto da sala de aula do Ensino Fundamental (EF) e Ensino Médio (EM)?" e as atividades foram divididas em uma sequência didática para o EF e atividades de cálculo de restos de potência para o EM, onde propomos também o uso de tecnologias, a saber, calculadoras e planilhas.

Antes das questões relacionadas ao ensino e aprendizagem matemáticos, abordamos a teoria matemática que sustenta o sistema de Criptografia RSA. Os conceitos da Aritmética Básica são relembrados no capítulo 2, como a divisão euclidiana e números primos. Em seguida, é vez da Aritmética Modular, no capítulo 3, e as Classes de Congruência Modular, no capítulo 4. Nesse último, incluímos resultados chave para a construção do RSA, como o teorema de Euler. Finalmente, no capítulo 5, apresentamos o funcionamento da Criptografia RSA e discutimos sobre sua segurança, teórica e computacional. De forma complementar, trazemos no capítulo 6 outros conceitos matemáticos inerentes ao uso do RSA, como a função totiente.

Após isso, retomamos a reflexão sobre o uso de tecnologias digitais como recurso didático e sobre a Criptografia e sua importância nos tempos atuais. O núcleo desta dissertação se encontra no capítulo 7, onde apresentamos o produto final desse trabalho: uma proposta de sequência didática baseada na criptografia RSA, sugerida para o 6º ano do Ensino Fundamental. As atividades dessa sequência utilizam as noções de primalidade e fatoração, codificação e decodificação, criptografia e segurança, através de uma versão simplificada da criptografia RSA. Um aprofundamento da discussão e os respectivos fundamentos teóricos são apresentados na primeira seção do capítulo.

De forma adicional, no Capítulo 8 exploramos ainda mais, teórica e computacionalmente, a base dos cálculos no RSA: cálculo do resto de potências. Em seguida, no capítulo 9, trazemos outro conjunto de atividades, sugeridas agora para o Ensino Médio, ensinando como utilizar planilhas para automatizar cálculos correlacionados aos sistemas criptográficos.

Nas próximas seções do presente capítulo, introduzimos os conceitos, termos e usos da Criptografia e, em particular, do modelo RSA, contextualizando sua origem.

1.1 Breve contextualização histórica do RSA

A necessidade de governantes e de seus representantes em se comunicarem confidencialmente existe há séculos. Para isso lançaram mão de artifícios para encobrir ou disfarçar o sentido original das mensagens, afinal acesso à informação sempre foi uma forma de poder. Uma estratégia de guerra, por exemplo, não poderia cair em mãos inimigas, senão todo o plano seria comprometido.

Os modelos antigos para se fazer a proteção das mensagens baseavam-se em artifícios como troca de letras do texto original por outras letras pré-determinadas, ou por permutações das letras originais ou ainda pelo uso de símbolos com certos significados. As mensagens eram entregadas fisicamente e portanto seu conteúdo era altamente vulnerável. Importante, até então, é perceber que a **Criptografia**, ou seja, os processos que envolvem a codificação da informação, é um antigo objetos de estudo da humanidade.

A Criptografia possui como etapas básicas a codificação, a decodificação, a pré-codificação e também o deciframento. Decifrar e decodificar parecem sinônimos, a princípio, entretanto atribuiremos ao ato de o destinatário efetivo ler uma mensagem codificada como decodificar, enquanto o ato de uma terceira parte intrusa, que assim não se trata nem do emissor nem do destinatário, de lê-la será chamado de decifrar. Organizaremos um pequeno glossário com definições e termos técnicos na seção seguinte deste capítulo.

Conforme as tecnologias de informação avançavam, especialmente com o advento dos computadores e da internet no século XX, processos de criptografia mais eficientes tornaram-se necessários e também viáveis. Assim como nos modelos antigos, a ideia inicial era de se garantir a segurança da informação, ou seja, garantir apenas que o destinatário pré-determinado fosse capaz de compreender a mensagem, uma vez que se considera a possibilidade de a mensagem ser interceptada deliberadamente ou não por terceiros.

Em meados da década de 70, com a popularização dos computadores, surgiu a possibilidade de facilitar transações entre pessoas físicas e jurídicas, por exemplo, entre bancos e seus clientes, e que demandavam, além da proteção de informações contra terceiros mal intencionados, uma validação jurídica que de fato caracterizasse consentimento das partes - uma espécie de assinatura, que fosse de baixo custo e computacionalmente viável para distribuição em larga escala. É neste contexto e visando tais demandas que surge o modelo RSA [2], desenvolvido em conjunto pelo matemático e criptologista estadunidense Ron Rivest, pelo criptógrafo de Israel Adi Shamir e pelo informático e biólogo molecular,

também estadunidense, Leonard Max Adleman.

A proposta desses cientistas para um modelo de encriptação foi baseada pela publicação do artigo "A method for obtaining digital signatures and public-key cryptosystems" [3], de autoria do criptógrafo e matemático Whitfield Diffie e do criptógrafo Martin Hellman, ambos estadunidenses. Nesse artigo eles descrevem um modelo de criptografia baseado na ideia de logaritmo discreto. A principal característica comum entre esse modelo e o RSA é que ambos propuseram a chamada criptografia de chave pública. Em poucas palavras, isso significa que tanto o texto codificado quanto uma das chaves necessárias para codificá-lo (e também decodificá-lo) podem ser enviados via algum canal não seguro, porque apenas seu conhecimento não possibilita que o texto seja decifrado.

Até aquela época as formas mais usadas de criptografia precisavam de um canal seguro para ao menos transmitir as chaves, pois seu conhecimento desencadearia na possibilidade de decifrar a informação protegida, canal que comumente era o correio físico. Assim, além da pouca eficiência pelo tempo gasto, havia um alto custo que impossibilitava a utilização da criptografia em maiores escalas, uma vez que havia a necessidade de as chaves serem privadas.

Como veremos, o RSA tem como base quatro naturais x, y, p e r, onde p e r são primos muito grandes[1] e não divulgados, ou seja, privados, que determinam o inteiro $m = p \cdot r$, enquanto x e y possuem a propriedade de satisfazer para algum inteiro k, a equação $x \cdot y = k \cdot (p-1)(r-1) + 1$. O par (x,m) é a chave pública, pois é compartilhado com o destinatário sem maiores preocupações sobre sua segurança e posteriormente usada pelo emissor para codificar a mensagem e assim transformá-la em um texto ilegível que, por sua vez, precisa do número y para ser decodificado.

O ponto é que para se obter a mensagem através do texto cifrado é necessário determinar p e q, de forma que os "ataques" que têm por intenção "quebrar" o código que protege o texto no modelo RSA se resumem a fatorar m, como bem apontam [3] e [4], e trata-se até hoje de um problema computacionalmente inviável para boas escolhas dos parâmetros x, y, p e r, de forma que este modelo de encriptação é ainda bem eficiente e bastante utilizado.

[1] Com duzentos dígitos cada, no sistema decimal, já se garante uma segurança considerável.

1.2 Onde se usa Criptografia?

Onde há troca de mensagens ou necessidade de comprovação de identidade no meio eletrônico, há o uso de algum modelo de criptografia. Sem usá-lo, os dados ficariam expostos ou propensos a fraudes. Em sites de bancos, de universidades, sites de compras e aplicativos de troca de mensagens, só para citar alguns exemplos, são canais onde trafegam imensa quantidade de dados, sejam números de cartão de crédito, números de cadastros, como o CPF, endereço e variadas informações pessoais e usam a criptografia como ferramenta de proteção. Ademais, em variados processos desses canais necessita-se de identificação, tornando novamente importante o uso da criptografia.

Em particular, a criptografia é amplamente utilizada em aplicativos de mensagem, como **Whatsapp**, **Viber**, **Threema**, **Sigmal**, **Riot**, **Messenger**, que utilizam logarítmo discreto na encriptação e **iMessage**, **Skype**, **Telegram**, que por sua vez utilizam o modelo RSA para dar segurança aos seus usuários.[2].

Outro ponto que merece destaque é que durante a pandemia de COVID-19 a demanda por fechamentos de contratos de forma eletrônica aumentou, com as recomendações sanitárias em evitar deslocamentos desnecessários, de modo que a Corregedoria Nacional de Justiça instituiu e regulamentou o sistema de atos notoriais eletrônicos, com o objetivo de resguardar a segurança de contratos imobiliários.

Entre as definições do ato [3], editado em maio de 2020, está a assinatura digital, como se segue.

> Art. 2º. Para fins deste provimento, considera-se:
> III – assinatura digital: resumo matemático computacionalmente calculado a partir do uso de chave privada e que pode ser verificado com o uso de chave pública, cujo certificado seja conforme a Medida Provisória n. 2.200-2/2001 ou qualquer outra tecnologia autorizada pela lei; [5]

A Medida Provisória 2.200-2/2001 por sua vez instituiu a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, como forma de garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica e de aplicações que usem certificados digitais, visando garantir a segurança na realização de transações eletrônicas. [4].

[2]Disponível em https://www.securemessagingapps.com/, acesso em 25 de novembro de 2021.

[3]Disponível em https://www.cnj.jus.br/wp-content/uploads/2020/05/DJ156_2020-ASSINADO.pdf, acesso em 25 de novembro de 2021

[4]Disponível em http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm#:~:text=2200%2D2&text=MEDIDA%20PROVIS%C3%93RIA%20No%202.200,que%20lhe%20confere%20o%20art, acessado em 25 de novembro de 2021

1.3 Glossário de termos

As definições aqui presentes baseiam-se nas encontradas na literatura de uma maneira geral, especialmente em [6]. Alguns termos foram acrescentados por terem designações específicas no presente contexto, apesar de não estarem explicitamente definidos nos materiais consultados. Convém também dizer que todos os termos deste glossário podem ter outros ou mais amplos sentidos e significados que os aqui definidos mesmo em contextos similares, como as chaves pública e privada. Ademais, a ordem não alfabética é proposital.

CRIPTOGRAFIA é a ciência que transforma dados em um texto inelegível ou incompreensível para as partes que não conhecem o modo apropriado de traduzi-lo.

PARTES* são pessoas físicas, jurídicas ou ainda criminosos ou organizações criminosas relacionados de alguma forma a certos dados, direta ou indiretamente. Assim, pertencem às partes o emissor, receptor e algum interceptor não autorizado.

TRADUZIR é o ato de decifrar ou decodificar algum dado.

DECODIFICAR é o ato de o destinatário dos dados recebê-los e transformá-los na informação original que o emissor concebeu.

CODIFICAR é a ação do emissor que consiste em transformar a informação original em um texto sem significado para outra parte que não seja o receptor pré-determinado.

DECIFRAR é similar a decodificar, entretanto é executado por algum interceptor, ou seja, um destinatário não autorizado.

DADOS* podem ser alguma mensagem ou informação em seu amplo sentido.

MENSAGEM* são dados ou informações que se deseja enviar.

CIFRAR é o uso da criptografia para esconder o real significado de um conjunto de dados para protegê-los ou ainda para autenticá-los, como é o caso da assinatura digital.

ASSINATURA DIGITAL é o mecanismo digital utilizado para se fornecer garantias sobre as autenticidades do remetente e da própria mensagem.

ENCRIPTAR é o mesmo que cifrar.

CHAVE é um código que se usa para cifrar ou traduzir mensagens.

CHAVE PÚBLICA é uma chave que pode ser enviada em meio não protegido.

CHAVE PRIVADA é uma chave mantida sob conhecimento de apenas de uma das partes.

ATAQUES são tentativas de se decodificar alguma mensagem encriptada.

QUEBRAR uma mensagem ou algum dado é o mesmo que decodificar.

2 Elementos básicos

Nosso objetivo é entender a matemática da **criptografia RSA**. Para isso, usamos basicamente a **Divisão Euclidiana** e a **Aritmética Modular**. Como exemplo motivador, a fim de se iniciar os estudos sobre aritmética modular, vamos considerar um problema relativamente simples e muito usado no cotidiano e que pode ser especialmente explorado na Educação Básica.

Uma situação comum que muitos de nós já passamos é o controle de horários de uma medicação. Suponha que você precise tomar um antibiótico três vezes ao dia a cada 8 horas e pretenda iniciar a medicação às dez horas da manhã. 8 horas passadas a partir das 10 da manhã será 18 horas. Afinal, $10 + 8 = 18$. Agora, 8 horas a partir das dezoito, será duas da manhã. Ou seja, "$18 + 8 = 2$"!

Podemos concluir que se você inciar o uso dos antibióticos às dez da manhã e for responsável, então você terá que acordar de madrugada. Podemos concluir também, se você registrar as operações, que há algo de incomum com o que seria registrado, baseado nos registros usuais para a operação soma de números reais.

O raciocínio anterior não é nada complexo, talvez o mais estranho seja o registro e entendimento da operação "$18 + 8 = 2$", que faz completo sentido no contexto apresentado. Note que, na adição usual, $18 + 8 = 26$, e $26 = 1 \cdot 24 + 2$, ou seja, 26 pode ser representado como um múltiplo de 24 acrescido de 2. Veremos então que os inteiros 2 e 26 guardam uma propriedade em relação ao inteiro 24, a qual iremos formalizar, e que constitui a ideia base da aritmética modular.

Assim, neste capítulo vamos definir seus elementos básicos, chegando até o Teorema da divisão euclidiana e propriedades gerais dos números primos.

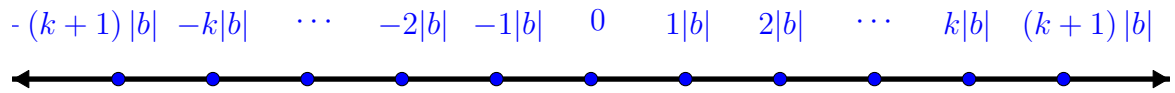
Consideramos, neste trabalho, a estruturação de $\mathbb{Z}$, o conjunto dos números inteiros, como um anel, ou seja, com a adição e multiplicação de seus elementos bem definida, bem como consideramos sua **boa ordenação**, o que nos permite fazer o uso, dentre outras coisas, do princípio de indução matemática.

2.1 Divisão Euclidiana

Dados dois inteiros a e b, se existir outro inteiro q tal que $a = b \cdot q$, dizemos que **a é múltiplo de b** ou que **b divide a**, ou ainda, que **b é um divisor de a**. Considerando a comutatividade da multiplicação nos inteiros, segue que a é múltiplo de q ou que q é divisor de a. Caso não exista q que satisfaça tal condição, então b não divide a, ou a não é múltiplo de b.

O que desejamos argumentar nesta seção é o fato de que para quaisquer a e b inteiros, com b não nulo, existem **únicos** q e r também inteiros, tais que $a = b \cdot q + r$, com $0 \leq r < |b|$. No caso em que a é um múltiplo de b, temos $r = 0$.

Considere a reta dos números inteiros, ou seja, a reta real somente com os elementos $x \in \mathbb{Z}$. Nela vamos destacar alguns dos múltiplos do inteiro b, como se segue:



É geometricamente intuitivo que, se a é um múltiplo de b, então a estará sobre um, e apenas um dos pontos destacados na figura, pois, se $a = k|b|$ e $a = k'|b|$ então $k|b| = k'|b|$ e portanto $k = k'$. Segue que, se $r = 0$, já temos garantido que $a = b \cdot q$, onde q é único. Vamos analisar o caso em que $r \neq 0$, ou seja, quando a não é múltiplo de b

Assim, novamente apelando à representação geométrica, é razoável afirmar que a está exatamente entre dois e apenas dois múltiplos consecutivos de b. De fato, supondo $k|b| < a < (k+1)\,|b|$ e $k'|b| < a < (k'+1)\,|b|$, com $k < k'$, temos $k'|b| < a < (k+1)\,|b|$. E podemos fazer $k' = k + m$, com $m > 0$, já que $k < k'$.

Portanto, $(k+m)\,|b| < a < (k+1)\,|b|$, o que implica em $m|b| < |b|$, o que é um absurdo! Como tal contradição foi gerada supondo que a está entre mais de dois múltiplos consecutivos de b, conclui-se que isso não pode ocorrer, ou seja, nossa intuição geométrica é válida nesse contexto e $k|b| < a < (k+1)\,|b|$, onde k é único.

Assim, existe r positivo tal que $a = k|b| + r$. Logo, $k|b| < k|b| + r < (k+1)\,|b|$ se, e somente se, $0 < r < |b|$, o que era esperado. Além do mais, se $a = k|b| + r'$, teríamos $k|b| + r = k|b| + r'$ e portanto $r = r'$. Assim, garantimos a unicidade de k e r, nas condições dadas. O que fizemos foi provar o seguinte importante teorema:

Teorema 2.1 (Teorema da Divisão Euclidiana): Dados a e $b \in \mathbb{Z}$, com b não nulo, existem e são únicos q e $r \in \mathbb{Z}$ tais que $a = q \cdot b + r$, com $0 \leq r < |b|$.

Note que, se $b > 0$, então $q = k$, e se $b < 0$, então $q = -k$. O inteiro q é o **quociente da divisão de a por b** e r será dito o **resto da divisão de a por b**, ou simplesmente, quociente e resto.

2.2 MDC e números primos

Antes de iniciar as definições desta seção vamos estabelecer uma notação mais compacta para lidar com divisibilidade. Iremos indicar o fato de um inteiro q dividir outro inteiro a como $q|a$, ou seja, isso significa que existe $b \in \mathbb{Z}$ tal que $a = q \cdot b$. No caso em que q não dividir a, escreveremos $q \nmid a$.

Definição 2.2 (Máximo Divisor Comum): O máximo divisor comum entre dois inteiros a e b, que denotaremos como $mdc\,(a,b)$ é um número inteiro $d > 0$ tal que:

1. $d|a$ e $d|b$;
2. se $c|a$ e $c|b$, então $c|d$

É natural nos perguntarmos se $mdc\,(a,b)$ é único, ou ainda, se existe. Em primeiro lugar, perceba que, se d existe, ele faz jus ao nome, ou seja, é o maior dos divisores comuns entre dois números inteiros dados pela segunda condição da definição. Para provar a sua unicidade, considere os conjuntos D_a e D_b, respectivamente, dos divisores positivos de a e b.

D_a é finito, pois se $x > a$ segue que $x \notin D_a$, e D_b também é finito pelo mesmo motivo. Note que $1 \in D_a \cap D_b$, e essa intersecção também é um conjunto finito. Portanto, temos que o conjunto dos divisores comuns de dois inteiros a,b dados é não vazio e limitado. Assim, $D_a \cap D_b$ possui maior elemento d, ficando garantidas a existência e a unicidade do $mdc\,(a,b)$. Para iniciar aplicações interessantes do mdc, vamos definir números primos.

Fatorar um número no conjunto dos inteiros é escrevê-lo como produto de outros diferentes da unidade. Neste contexto estamos interessados na fatoração em números primos, ou seja, em expressar um inteiro qualquer como produto apenas de números primos, sendo essa fatoração um ponto essencial do sistema de criptografia RSA. Para isso definamos um número primo.

Definição 2.3 (Números Primos): Um número $p \in \mathbb{N}$ e $p > 1$ é primo se seus únicos divisores positivos forem 1 e p.

Um número natural que não é primo e é maior que um é chamado **composto**. Se um natural a é composto então ele possui pelo menos dois divisores b e q, com $1 < b < a$, $1 < q < a$ e $a = b \cdot q$, senão ele seria primo.

É fácil perceber a existência de números primos listando, digamos, os dez primeiros naturais. Por exemplo, 7 só possui como divisores positivos o próprio 7 e 1. Mais do que isso, veremos que na verdade existem infinitos primos. Antes, vamos garantir que todo número composto pode ser escrito com fatores primos, ou seja, fatorado como o produto de apenas números primos.

Por inspeção os números compostos dentre os dez primeiros naturais podem ser expressos de tal forma, a saber, $8 = 2 \cdot 2 \cdot 2$, $6 = 2 \cdot 3$ e $4 = 2 \cdot 2$. Isso nos permite tomar um número composto a, e os conjuntos $P = \{p \in \mathbb{N},\ p\ primo, p < a\}$ e $D = \{d \in \mathbb{N},\ tal\ que\ d\ divide\ a\}$, respectivamente o conjunto dos primos menores que a e dos divisores de a.

Suponha então que a não tenha divisor primo. Assim $P \cap D = \emptyset$ e portanto todo elemento de D é composto. Pela Boa Ordenação dos inteiros, D possui menor elemento d_0. Daí podemos inferir duas coisas: primeiro, como d_0 é divisor de a, pois pertence a D, existe um $t \in \mathbb{N}$ tal que $a = d_0 \cdot t$; segundo, que, pelo fato de ser composto, existem m,$n \in \mathbb{N}$ tais que $d_0 = m \cdot n$, e $1 < m < d_0$, $1 < n < d_0$.

Assim, de $a = d_0 \cdot t$ temos $a = m \cdot n \cdot t$. Portanto m é divisor de a, daí pertence a D. Mas temos que $m < d_0$. Absurdo, pois contradiz o fato de d_0 ser o menor elemento de D. Assim um composto qualquer possui pelo menos um fator primo.

Ainda queremos garantir mais propriedades sobre a fatoração de um composto a. Para isso, vamos usar um resultado preliminar.

Lema 2.4: Seja a um natural composto. Então existe $m \in \mathbb{N}$ tal que $2^m \leq a < 2^{m+1}$.

Demonstração. Como a é composto, $a > 2$. Seja X o conjunto de todas as potências de 2 menores ou iguais a a. X não é vazio pois $2^1 \in X$. Como $a + 1$ é um limite superior para este conjunto, então X é limitado e assim possui maior elemento 2^m. Portanto 2^{m+1} não pertence ao conjunto e assim $a < 2^{m+1}$, provando que $2^m \leq a < 2^{m+1}$. □

Usando o lema 2.4 temos uma forma de mostrar que um número natural $a > 1$ quando escrito como produto de outros naturais maiores que 1 tem finitos fatores. Isso porque se m é tal como no referido lema, $a < 2^{m+1}$. Caso alguma fatoração de a possuísse $m+1$ fatores ou mais, então $a \geq 2^{m+1}$, contradizendo o resultado do lema. Agora vamos garantir que qualquer natural $a > 1$ pode ser expresso como fatores de números primos.

Se a for primo, não há o que demosntrar. Agora, quando a é composto, já sabemos que existe p_1 primo tal que $a = p_1 \cdot b_1$. Se b_1 for também primo, então a foi expresso com fatores primos. Caso b_1 não seja primo, sabemos que ele pode ser expresso por ao menos um fator primo também. Assim, $b_1 = p_2 \cdot b_2$ e $a = p_1 \cdot p_2 \cdot b_2$. Novamente, caso b_2 não seja primo, ele pode ser da forma $b_2 = p_3 \cdot b_3$ e $a = p_1 \cdot p_2 \cdot p_3 \cdot b_3$. Suponha então que $a = p_1 \cdot p_2 \cdots p_n \cdot b_n$ para algum n natural. Ora, sabemos também que não pode haver mais que $m+1$ fatores, ou seja, $n+1 < m+1 \Rightarrow n < m$.

Então podemos supor, sem perda de generalidade, que a possui no máximo $n+1$ fatores. Assim, afirmamos que b_n é primo, pois se fosse composto teríamos $b_n = p_{n+1} \cdot b_{n+1}$ e a teria $n+2$ fatores, o que seria absurdo. Portanto um natural maior que 1 pode ser escrito como produto de apenas números primos.

Precisamos garantir a unicidade dessa representação, ou seja, podem haver $p_i's$ e $q_j's$ todos primos, com $1 \leq i,j \leq k,n$ tais que $a = p_1 \cdot p_2 \cdots p_n$ e $a = q_1 \cdot q_2 \cdots q_k$? Para argumentar que isso não pode ocorrer, vamos mostrar alguns resultados que nos ajudarão nesta e em outras tarefas.

Lema 2.5: Seja $a \in \mathbb{Z}$ não nulo. Se a divide $b+c$ e a divide b, então a divide c.

Demonstração. Temos, usando as hipóteses, que $b + c = a \cdot q$ e $b = a \cdot q'$, onde q e q' são inteiros. Portanto, $b + c = a \cdot q' + c = a \cdot q$. Segue que $c = a\,(q - q')$ o que prova a afirmação.

□

Teorema 2.6: Se p é primo e $a \in \mathbb{Z}$, então $mdc\,(p,a) = p$ ou $mdc\,(p,a) = 1$.

Demonstração. Seja $d = mdc\,(p,a)$. Então $d|a$ e $d|p$. Ora, como p é primo, então $d = p$ ou $d = 1$. □

Teorema 2.7: Seja p primo e $A = \{1,2,3,\cdots,p-1\}$. Sejam $r_1 \leq r_2 \in A$. Então p não divide $r' \cdot r''$.

Precisamos de uma definição antes do próximo resultado. Vamos dizer que se $mdc\,(a,b) = 1$, então a e b são **coprimos** ou são **primos entre si**.

Demonstração. Note inicialmente que p e $r^{'}$ são coprimos, assim como p e $r^{''}$. Suponha por absurdo que $p|r^{'} \cdot r^{''}$. Então existe k, tal que $r^{'} \cdot r^{''} = p \cdot k$. Agora seja $mdc(r^{'},k) = d^{'}$ e $mdc(r^{''},k) = d^{''}$. Assim $d^{'} \cdot d^{''}|r^{'} \cdot r^{''} \Rightarrow d^{'} \cdot d^{''}|p \cdot k$. Nem $d^{'}$ nem $d^{''}$ dividem p, pois caso contrário contradiria o fato de p e $r^{'}$ serem coprimos, assim como p e $r^{''}$. Portanto $d^{'} \cdot d^{''}|k$.

Sejam $\frac{r^{'}}{d^{'}} = r_1^{'}$, $\frac{r^{''}}{d^{''}} = r_1^{''}$ e $\frac{k}{d^{'} \cdot d^{''}} = k_1$ Assim, temos

$$r_1^{'} \cdot r_1^{''} = p \cdot k_1.$$

Podemos dividir o lado esquerdo da última equação pelos mdc's de $r_1^{'}$ e $r_1^{''}$ e, pela mesma argumentação do parágrafo anterior, podemos dividir k_1 pelo produto destes mdc's.

Repetindo este processo por um número finito de vezes, obteremos

$$r_n^{'} \cdot r_n^{''} = p \cdot k_n$$

onde $r_n^{'}$ e k_n são coprimos, tal como $r_n^{''}$ e k_n.

Ora, mas o lado esquerdo da equação é divisível por $r_n^{'}$ mas nem p nem k_n o são, chegando-se em um absurdo. A conclusão é que, nas hipóteses dadas, p não divide $r_1 \cdot r_2$.

□

Teorema 2.8: Seja p primo tal que p divide $a \cdot b$. Então p divide a ou p divide b.

O que queremos mostrar é que se p é primo e $p|a \cdot b$, então $p|a$ ou $p|b$. Perceba que caso p não fosse primo esse fato nem sempre seria verdade. Por exemplo, $12|4 \cdot 9$ mas 12 não divide nem 4 nem 9. Vamos à demonstração dessa outra propriedade dos primos.

Demonstração. Suponha que p não divida a, pois se assim não fosse não haveria nada a provar. Logo $a = p \cdot q_1 + r_1$, com $0 < r_1 < p$. E seja $b = p \cdot q_2 + r_2$, $0 \leq r_2 < p$. Por hipótese, $a \cdot b = p \cdot q$, para algum inteiro q, e fazendo $(p \cdot q_1 + r_1) \cdot (p \cdot q_2 + r_2)$ obtemos $a \cdot b = p \cdot q' + r_1 \cdot r_2$, com $q' \in \mathbb{Z}$.

Pela propriedade 2.7, se $r_2 \neq 0$, $r_1 \cdot r_2$ não seria múltiplo de p, o que seria absurdo de acordo com o lema 2.5. Então temos $r_2 = 0$ e assim $b = p \cdot q_2$, ou seja, p divide b.

□

Teorema 2.9: Se p_1 e q_1 são primos e $p_1|q_1$, então $p_1 = q_1$.

Demonstração. De fato, de acordo com as hipóteses, $mdc\,(p_1,q_1) = p_1$. Ora, como q_1 é primo, $mdc\,(p_1,q_1) = q_1$, o que nos leva a concluir, devido à unicidade do mdc, que $p_1 = q_1$. □

Voltando à fatoração em primos de a, suponha que $a = p_1 \cdot p_2 \cdots p_n$ e $a = q_1 \cdot q_2 \cdots q_k$, com $p_i's$ e $q_j's$ todos primos, $1 \leq i,j \leq k,n$.

Note que, se isso acontecer, como p_1 divide a, temos que p_1 divide $q_1 \cdot q_2 \cdots q_k$, de modo que podemos usar o teorema 2.8 e afirmar que p_1 divide um dos $q_j's$. Sem perda de generalidade, podemos supor que $p_i|q_i$.

Agora, de acordo com o teorema 2.9 temos $p_1 = q_1, p_2 = q_2, \cdots p_n = q_n$, de modo que n deve ser igual a k e demonstramos a unicidade e existência da fatoração em primos de um natural composto, o que nos garante o seguinte importante resultado.

Teorema 2.10 (Teorema Fundamental da Aritmética): Seja $a \in \mathbb{Z}$. Ou a é primo ou a pode ser representado de forma única, a menos da ordem dos fatores, em um produto de números primos.

Teorema 2.11 (Infinitude dos números primos): Existem infinitos números primos.

Demonstração. Suponha que apenas exista uma quantidade finita de números primos $p_1, p_2, \cdots, p_k$ e seja $a = p_1 \cdot p_2 \cdots p_k + 1$. Então $a > p_k$ e portanto, composto. Assim, algum primo $p_i|a$ e então $p_i|p_1 \cdot p_2 \cdots p_k + 1$. Ora, mas $p_i|p_1 \cdot p_2 \cdots p_k$ e pelo lema 2.5, $p_i|1$, o que é absurdo.

Concluímos que não pode haver uma quantidade finita de números primos, já que o absurdo foi gerado por supormos exatamente isso. □

2.3 Alguns testes de primalidade

Seria natural tentarmos verificar agora, após as definições e teoremas iniciais, se um número natural a dado é primo ou composto, ou seja, qual é a sua **primalidade**.

Podemos iniciar com um teste que segue direto da definição 2.3, ou seja, verificar se a é divisível por algum natural entre 2 e $a-1$.

Corolário 2.12 (Teste de primalidade 1): Seja $n \in \mathbb{N}$ e $X = \{2,3,\cdots,n-1\}$. Se $x \nmid n$, $\forall\ x \in X$, então n é primo.

Como já dito, o resultado desse corolário segue diretamente da definição de números primos, pois no caso n só teria como divisores naturais o número 1 e o próprio n. Apesar de simples, note que não é um teste muito eficiente de se fazer, pois no caso em que n é primo faríamos $n-2$ divisões. Por exemplo, tomemos $n = 4001$. Após 3999 iterações concluiríamos que n é primo.

Podemos refinar um pouco o teste de primalidade. Para isso definiremos o **piso** de um número real, especialmente para usarmos a parte inteira da raiz quadrada de um natural.

Antes, precisamos garantir que qualquer $x \in \mathbb{R}$ pode ser escrito de forma única como $x = a + \alpha$, onde $a \in \mathbb{Z}$ e $\alpha \in \mathbb{R}$ tal que $0 \leq \alpha < 1$. Se não fossem únicos, teríamos $x = a + \alpha$ e $x = a' + \alpha'$ com a e a' inteiros e $0 \leq \alpha < 1$ e $0 \leq \alpha' < 1$. Podemos considerar, sem perda de generalidade, $\alpha' > \alpha$, de modo que $0 < \alpha' - \alpha < 1$ e portanto

$$a + \alpha = a' + \alpha' \Rightarrow a - a' = \alpha' - \alpha \Rightarrow 0 < a - a' < 1$$

o que é um absurdo, uma vez que a e a' são inteiros.

Definição 2.13 (Piso de um número real): Seja $x = a + \alpha$ tal que $a \in \mathbb{Z}$, $\alpha \in \mathbb{R}$ e $0 \leq \alpha < 1$. Então a **é o piso de x**, que denotaremos por $\lfloor x \rfloor$.

Note que $\lfloor x \rfloor \in \mathbb{Z}$ e $\lfloor x \rfloor$ é a parte inteira do real x. Como exemplos, temos que $\lfloor \frac{5}{4} \rfloor = 1$, $\lfloor -8{,}36 \rfloor = -9$ e $\lfloor \sqrt{101} \rfloor = 10$. Seguimos assim com o segundo teste de primalidade.

Teorema 2.14 (Teste de primalidade 2): Seja $n \in \mathbb{N}$ e $Y = \{2,3,\cdots,\lfloor \sqrt{n} \rfloor\}$. Se $y \nmid n\ \forall\ y \in Y$, então n é primo.

Antes de demonstrarmos o teorema precisamos garantir que se $m \in \mathbb{Z}$ é tal que $m > \lfloor x \rfloor$, então $m > x$. Usando a representação $x = a + \alpha$, temos que $x < a + 1$. Por outro lado, como $m > \lfloor x \rfloor$, ou seja, como $m > a$, temos $m \geq a + 1$, pois $m \in \mathbb{Z}$ e daí segue

o resultado.

Demonstração. Suponha por absurdo que nenhum elemento de Y divida n e que n seja composto. Assim, existem $m > \lfloor\sqrt{n}\rfloor$ e $p > \lfloor\sqrt{n}\rfloor$ tais que $n = m \cdot p$. Mas, pelo exposto no parágrafo anterior com $\sqrt{n} = x$, temos que $m > \sqrt{n}$ e $p > \sqrt{n}$, o que implica em $m \cdot p > \sqrt{n} \cdot \sqrt{n}$, ou $m \cdot p > n$, o que é absurdo.

Portanto n tem que ser primo.

□

Tomando novamente $n = 4001$, temos $\lfloor\sqrt{4001}\rfloor = 63$. Assim, enquanto o teste 2.12 demanda 3999 divisões, o teste 2.14 demanda apenas 61. Apesar dessa enorme economia de iterações, um n na ordem dos bilhões ainda demandaria mais de 1000 operações. Tomando n cada vez maior, mais tempo se gasta para determinar sua primalidade de forma que se torna impossível fazê-lo na prática usando esses testes.

Os testes de primalidade acima são algoritmos determinísticos que empregam a estratégia de força bruta, gerando um grande custo de tempo e recursos computacionais. Podemos especificar esse custo através do conceito de *complexidade computacional*, como será brevemente delineado na seção 5.4. Nesses termos, sem entrar em cálculos explícitos de suas complexidades computacionais, podemos dizer que os testes de primalidade acima citados têm alta complexidade computacional, de ordem de crescimento exponencial.

Coutinho [4] apresenta outros testes mais eficientes, como complexidades computacionais mais baixas, de ordem de crescimento polinomial. Um exemplo é o teste de Miller, um algoritmo não-determinístico, o qual não exploraremos aqui. Além do mais, no epílogo do referido livro o autor chama a atenção para a existência de outros testes de primalidade mais modernos e eficientes, como o *crivo quadrático* e os baseados em *curvas elípticas*, que dependem de métodos matemáticos que fogem dos aqui abordados. Por fim, o teste de primalidade mais eficiente, determinístico e de complexidade polinomial, é o algoritmo AKS, também apresentado por Coutinho em [7]

3 Aritmética Modular

Voltando ao texto introdutório do Capítulo 2, afirmamos que 26 e 2 guardam uma propriedade com o número 24. Usando a divisão euclidiana podemos escrever $26 = 1 \cdot 24 + 2$ e $2 = 0 \cdot 24 + 2$, ou seja, os restos desses números na divisão por 24 são iguais a 2 e é basicamente essa propriedade que iremos formalizar e explorar. Observe que qualquer inteiro na forma $24q + 2$, com q também inteiro, deixa resto 2 quando dividido por 24, de maneira que há infinitos inteiros que satisfazem essa condição e ainda que a diferença entre dois desses números é sempre um múltiplo de 24.

Portanto, neste capítulo faremos um esforço para caracterizar, classificar e estudar as propriedades de elementos inteiros a e b que deixam o mesmo resto r na divisão euclidiana por um determinado natural m.

3.1 Congruência módulo m

Começaremos com uma notação que designa elementos com mesmo resto na divisão por um mesmo natural.

Definição 3.1: Seja $m \in \mathbb{N}$, a,$b \in \mathbb{Z}$. Se $a = mq_1 + r$ e $b = mq_2 + r$, com $0 \leq r < m$, então diremos que **a e b são congruentes entre si módulo m**, ou, se o contexto deixar m claro, simplesmente congruentes. Denotaremos, quando isso ocorrer, por

$$a \equiv b \; mod\,(m)\,.$$

Perceba que nesse caso, quando os restos na divisão por m são iguais, temos

$$a - b = mq_1 + r - mq_2 - r = m\,(q_1 - q_2)\,.$$

Ou seja, a diferença entre elementos congruentes módulo m é um múltiplo de m. E, supondo dois inteiros $a = mq_1 + r_1$ e $b = mq_2 + r_2$ cuja diferença é um múltiplo de m,

teremos

$$a - b = mk \Rightarrow m\,(q_1 - q_2) + (r_1 - r_2) = mk.$$

Mas $0 \leq r_1 - r_2 < m$[1] e, pelo lema 2.5, $m|r_1 - r_2$, o que implica em $r_1 - r_2 = 0$ e portanto $r_1 = r_2$.

Acabamos de provar a primeira propriedade dessa relação entre inteiros, que pode ser enunciada como se segue.

Lema 3.2: $a \equiv b \mod (m) \Leftrightarrow m|(a - b)$.

Usando este lema, temos que:

1. $a \equiv a\ mod\,(m)$ pois $a - a = 0$ e $m|0$;
2. $a \equiv b\ mod\,(m)$ implica em $b \equiv a\ mod\,(m)$, pois se $m|a - b$ então $m| - (a - b)$, ou seja, $m|b - a$;
3. e se $a \equiv b\ mod\,(m)$ e $b \equiv c\ mod\,(m)$, então $a \equiv c\ mod\,(m)$, pois $m|a - b$ e $m|b - c$, logo $m|\,(a - b) + (b - c)$, ou seja, $m|\,(a - c)$.

Em outras palavras, as três propriedades listadas acima mostram que congruência módulo m é respectivamente reflexiva, simétrica e transitiva, ou seja, é uma **relação de equivalência**.

3.2 Inverso multiplicativo

Vamos trabalhar com a relação de congruência da mesma forma como trabalhamos com uma equação, especialmente quando multiplicamos ambos os lados por elementos convenientes. Entretanto, como no exemplo do parágrafo que segue, há propriedades das equações entre inteiros que podem não ser válidas na congruência módulo m. Então nos preocuparemos em estabelecer critérios para tal.

Inicialmente olhemos para um caso particular. Temos que $78 \equiv 42\ mod\,(4)$, pois $78 - 42 = 36$, é um múltiplo de 4. Como 2 é divisor tanto de 78 quanto de 42, poderíamos inferir que $39 \equiv 21\ mod\,(4)$, o que é **falso**, pois $39 - 21 = 18$, que não é um múltiplo de 4. Entretanto, usando raciocínio análogo agora com 3, que também divide 78 e 42, podemos inferir que $26 \equiv 14\ mod\,(4)$, e de fato $26 - 14 = 12$, que é um múltiplo de 4.

[1] Se $r_2 \geq r_1$ a argumentação é análoga.

Portanto temos uma motivação para verificar quando podemos ou não inferir uma relação dessas. Na verdade verificaremos quando a divisão pode ser definida, ou, equivalentemente, quando o **inverso multiplicativo de um elemento** existe. A multiplicação é sempre garantida, pois se $a \equiv b \mod (m)$ então $m|(a-b)$ e portanto $m|\,(a-b)\,c$. Então $ac - bc$ é um múltiplo de m, ou seja $ac \equiv bc \mod (m)$.

Definição 3.3 (Inverso multiplicativo): Diremos que $x \in \mathbb{Z}$ é inverso multiplicativo de a módulo m, ou simplesmente inverso quando o contexto permitir, se

$$a \cdot x \equiv 1 \mod (m).$$

Note que $a \cdot x \equiv 1 \mod (m)$ significa que para algum $k \in \mathbb{Z}$ temos $ax - mk = 1$. Se algum $d \in \mathbb{N}$ é tal que $d|a$ e $d|m$, então pelo lema 2.5 $d|1$. Logo $d = 1$ e a e m são coprimos. De modo análogo, x e m também são coprimos, o que era de se esperar, portanto, devido à comutatividade da multiplicação nos inteiros, podemos afirmar também que a é o inverso de x módulo m.

Provamos que caso x, o inverso multiplicativo de a módulo m, exista, então $mdc\,(a,m) = mdc\,(x,m) = 1$. É razoável verificar se a recíproca dessa afirmação é válida, ou seja, dados a e m coprimos, verificar se existe x com a propriedade de o produto ax deixar resto 1 na divisão euclidiana por m. Veremos que sim, que o fato de a e m serem primos entre si garantirá a existência do inverso de a.

Já podemos garantir a unicidade de x supondo x' tal que $a \cdot x' \equiv 1 \mod (m)$. Pela transitividade da congruência teremos que $a \cdot x \equiv a \cdot x' \mod (m)$, ou seja, para algum $t \in \mathbb{Z}$ seguirá que

$$ax - ax' = tm \Rightarrow a\,(x - x') = tm \Rightarrow m|a\,(x - x')\,.$$

Mas a e m são coprimos, de modo que $m|x - x'$ e portanto $x \equiv x' \mod (m)$. Por outro lado se $y \equiv x \mod (m)$, podemos fazer $ay \equiv ax \mod (m)$ e argumentar de forma análoga para garantir que $x \equiv y \mod (m)$.

O que provamos foi o fato de que se o produto ax deixar resto 1 na divisão por m e o produto ax' também o fizer, então x e x' deixam o mesmo resto na divisão por m e vice-versa. Assim o inverso multiplicativo módulo m não é único em $\mathbb{Z}$, **ele é único**

na relação de congruência módulo m. De fato, tomando $x' = x + mk$, onde $k \in \mathbb{Z}$, $ax' = ax + amk$, que é sempre congruente a 1 módulo m, pois a parcela ax deixa resto 1 enquanto a parcela amk deixa resto 0 na divisão por m. Como exemplo veja que $5 \cdot 2 \equiv 1 \mod (3)$ assim como $5 \cdot 8 \equiv 1 \mod (3)$ e $5 \cdot 11 \equiv 1 \mod (3)$, e tanto 2 quanto 8 e 11 deixam o mesmo resto na divisão por 3, ou seja, $2 \equiv 8 \equiv 11 \mod (3)$.

Antes de continuar vamos listar propriedades da congruência que foram e serão úteis e derivam diretamente da definição.

Teorema 3.4 (Propriedades gerais da congruência): Sejam inteiros a e b tais que $a \equiv b \mod (m)$, e c,$t \in \mathbb{Z}$. Então:

1. $ac \equiv bc \mod (m)$;
2. $a + c \equiv b + c \mod (m)$;
3. $a + mk \equiv b \mod (m)$.

A primeira dessas propriedades já foi provada. A segunda é fácil de se provar pois $(a + c) - (b + c) = a - b$, que é um múltiplo de m por hipótese. Para a terceira propriedade, note que $mk \equiv 0 \mod (m)$.

Para se provar a existência do inverso multiplicativo e inclusive uma forma de construí-lo, vamos demonstrar um lema e depois o **algoritmo de Euclides estendido**.

Lema 3.5: Seja $a = mq + r$, com $0 \leq r < |m|$. Então $mdc\,(a,m) = mdc\,(r,m)$.

Demonstração. Seja $d = mdc\,(a,m)$, então $d|a$ e $d|m$. Assim $d|a - mq$, ou seja, $d|r$. Suponha d' tal que $d'|r$ e $d'|m$. Assim $d'|mq + r$, ou seja, d' divide a e m. Pela definição de mdc e por $d = mdc\,(a,m)$ temos que $d'|d$. Portanto $d = mdc\,(r,m)$ □

Perceba que quando conveniente podemos estender o lema para $r = ax + my$ com x e y inteiros, além de que a hipótese sobre r ser desnecessária. O ponto é que iremos aplicá-lo especialmente nesse contexto.

Considere assim a divisão euclidiana de a por m, onde $a = mq_0 + r_0$ com $0 \leq r_0 < |m|$. Aplicando a divisão e o lema anterior sucessivas vezes teremos os resultados conforme registrados na tabela 3.1 a seguir onde r_n é o último resto não nulo.

Perceba que existe o último resto não nulo r_n, pois a sequência de restos r_i é estritamente decrescente até 0. Ademais, como resultado do lema 3.5, temos que

Tabela 3.1: Tabela de divisões euclidianas sucessivas.

Divisão euclidiana	Pelo lema 3.5	Restos
$a = mq_0 + r_0$	$mdc\,(a,m) = mdc\,(m,r_0)$	$0 \leq r_0 < \lvert m\rvert$
$m = r_0q_1 + r_1$	$mdc\,(m,r_0) = mdc\,(r_0,r_1)$	$0 \leq r_1 < r_0$
$r_0 = r_1q_2 + r_2$	$mdc\,(r_0,r_1) = mdc\,(r_1,r_2)$	$0 \leq r_2 < r_1$
$r_1 = r_2q_3 + r_3$	$mdc\,(r_1,r_2) = mdc\,(r_2,r_3)$	$0 \leq r_3 < r_2$
$r_2 = r_3q_4 + r_4$	$mdc\,(r_2,r_3) = mdc\,(r_3,r_4)$	$0 \leq r_4 < r_3$
$\cdots$	$\cdots$	$\cdots$
$r_{n-2} = r_{n-1}q_n + r_n$	$mdc\,(r_{n-2},r_{n-1}) = mdc\,(r_{n-1},r_n)$	$0 \leq r_n < r_{n-1}$

Fonte: criada pelos autores.

$mdc\,(a,m) = mdc\,(r_{n-1},r_n)$, e $r_{n-1} = r_nq_{n+1}$, pois o próximo resto, r_{n+1}, deve ser nulo, de modo que $mdc\,(r_{n-1},r_n) = r_n$ e $mdc\,(a,m) = r_n$.

Além disso r_0 é uma combinação linear de a e m, pois $r_0 = a - mq$. E substituindo-se r_0 na segunda equação temos que r_1 também é uma combinação linear de a e m. Substituindo-se os restos sucessivamente, concluímos que $r_n = ax + my$ para algum x e algum y. Vamos resumir o que foi provado em um teorema.

Teorema 3.6 (Algoritmo de Euclides Estendido): Sejam a e $b \in \mathbb{Z}$ e $d = mdc\,(a,b)$. Então existem inteiros x e y tais que

$$d = a \cdot x + b \cdot y.$$

Isso nos dá o necessário para provar a existência do inverso multiplicativo módulo m quando $mdc\,(a,m) = 1$, pois pelo teorema 3.6 existem x e y tais que $ax + my = 1$ e assim $ax = -my + 1$, ou seja, $ax \equiv 1 \mod (m)$. Isso nos dá o resultado que se segue.

Teorema 3.7 (Existência do inverso multiplicativo módulo m): Existe $x \in \mathbb{Z}$ tal que $a \cdot x \equiv 1 \mod (m)$ se, e somente se, $mdc\,(a,m) = 1$.

4 Classes de congruência módulo m

Neste capítulo, iremos organizar os elementos de $\mathbb{Z}$ em subconjuntos de acordo com a congruência definida no capítulo anterior. Podemos afirmar, como exemplo, que os inteiros 2, 26, 50 e -22 estão num mesmo conjunto (que denominamos classe) novamente em relação ao natural 24, pois deixam o mesmo resto na divisão euclidiana. Existirão, claro, outros conjuntos que correspondem aos outros possíveis restos, tomando como base o mesmo natural. E, por fim, chegaremos em um resultado que se aplica diretamente na construção do modelo RSA.

4.1 O conjunto $\mathbb{Z}_m$

Sabemos que qualquer elemento $x \in \mathbb{Z}$ pode ser representado como $x = mq + r$, em relação a um natural m, com $0 \leq r < m$. Logo, considerando o conjunto $M = \{0,1,\cdots m-1\}$, podemos afirmar que todos os restos possíveis na divisão euclidiana de qualquer inteiro por m pertencem a M. Além do mais, dados dois elementos $r_1 \geq r_2$ de M, temos que se $r_2 \equiv r_1 \ mod(m)$ então $r_1 - r_2 = mk$, para algum inteiro k. Mas $r_1 - r_2 < m$ de modo que a única possibilidade é $k = 0$ e daí segue que $r_1 = r_2$.

O que a argumentação anterior prova é que o conjunto M além de possuir todos os restos possíveis na divisão por m, não os repete, pois como mostrado dois elementos de M só deixam o mesmo resto se forem iguais. Em outras palavras, dado $x \in \mathbb{Z}$ existe único $r \in M$ tal que $x \equiv r \mod (m)$.

Assim o conjunto M pode representar todo o conjunto $\mathbb{Z}$ na congruência módulo m, pois, grosso modo, o que interessa neste contexto são apenas os restos. Entretanto note que M não é o único com esta propriedade. Por exemplo, somando-se um múltiplo de m a cada resto possível obtemos outro conjunto com as mesma características, ou seja, capaz de representar todos os restos em relação a m. Convém, portanto, definir conjuntos de elementos que deixam o mesmo resto.

Definição 4.1 (Classes Residuais): A classe residual do inteiro a em relação a m ou classe residual de a módulo m é o conjunto $\overline{a}$ tal que $\overline{a} = \{x \in \mathbb{Z}\ tal\ que\ a \equiv x\ mod(m)\}$.

Segue diretamente da definição que, se $a = qm + r$, então $r \in \overline{a}$. Mais que isso, qualquer elemento de $\overline{a}$ pertence a $\overline{r}$ pela transitividade da congruência módulo m e vice-versa, qualquer elemento de $\overline{r}$ pertence a $\overline{a}$. Portanto $\overline{r} = \overline{a}$. A conclusão é que podemos nos referir a todas as classes usando os elementos de M, e de fato, dado qualquer x inteiro, x pertence a uma e somente uma das classes $\overline{0}$,$\overline{1}, \cdots \overline{m-1}$. Motiva-se então, outra definição.

Definição 4.2 (O conjunto $\mathbb{Z}_m$): $\mathbb{Z}_m = \{\overline{0},\overline{1}, \cdots \overline{m-1}\}$.

Portanto $\mathbb{Z}_m$ é conjunto de todas as classes residuais módulo m e perceba que o número de elementos de $\mathbb{Z}_m$ é m, ou $\#\mathbb{Z}_m = m$. Note também que $\mathbb{Z}_m$ é um conjunto formado por subconjuntos de $\mathbb{Z}$ cuja união de seus elementos é o próprio $\mathbb{Z}$.

Exemplificando as definições e propriedades temos que $\mathbb{Z}_4 = \{\overline{0},\overline{1},\overline{2},\overline{3}\}$ pois qualquer inteiro dado deixa restos 0, 1, 2 ou 3 na divisão por 4. Mas podemos usar outros representantes de cada classes para representar esse conjunto, por exemplo $\mathbb{Z}_4 = \{\overline{-16},\overline{21},\overline{14},\overline{43}\}$.

Definindo a adição de elementos $\overline{r_1}$ e $\overline{r_2}$ de $\mathbb{Z}_m$ como $\overline{r_1} + \overline{r_2} = \overline{r_1 + r_2}$ e a multiplicação como $\overline{r_1} \cdot \overline{r_2} = \overline{r_1 \cdot r_2}$ temos que $\mathbb{Z}_m$ é um anel comutativo com unidade, conforme propriedades que listaremos.

Teorema 4.3 ($\mathbb{Z}_m$ é um anel): Sejam $\overline{a}$, $\overline{b}$ e $\overline{c}$ elementos de $\mathbb{Z}_m$. Então as seguintes propriedades são válidas.

1. **Associatividade da adição:** $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$
2. **Comutatividade da adição:** $\overline{a} + \overline{b} = \overline{b} + \overline{a}$
3. **Elemento neutro da adição:** $\overline{a} + \overline{0} = \overline{a}$
4. **Elemento neutro da adição:** $\overline{a} + \overline{-a} = \overline{0}$
5. **Associatividade da multiplicação:** $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$
6. **Comutatividade da multiplicação:** $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$
7. **Elemento neutro da multiplicação:** $\overline{a} \cdot \overline{1} = \overline{a}$

8. **Distributividade:** $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$

O teorema acima segue basicamente porque, conforme definido, a soma de classes é a classe da soma de inteiros e o produto de classes é a classe do produto de inteiros, ou seja, herdam propriedades do anel $\mathbb{Z}$.

4.2 O conjunto $\mathbb{Z}_p$

Caso $\mathbb{Z}_m$ também goze da existência de inverso multiplicativo para todo elemento diferente de $\overline{0}$, então $\mathbb{Z}_m$ é um corpo. Argumentaremos nesta seção que $\mathbb{Z}_m$ é um corpo se, e somente se, m é primo. Daí usaremos $\mathbb{Z}_p$ para designar tal conjunto nesse caso particular.

Sendo assim, para um $\overline{x} \in \mathbb{Z}_m$ não nulo devemos investigar quando existe $\overline{y}$ tal que $\overline{x} \cdot \overline{y} = \overline{1}$. Podemos considerar, conforme a seção anterior, x e y entre 0 e $m-1$. Como um elemento típico da classe $\overline{x}$ é da forma $mq + x$ e um elemento típico da classe $\overline{y}$ é da forma $mq' + y$, exigir que $\overline{x} \cdot \overline{y} = \overline{1}$ é o mesmo que fazer $(mq + x)(mq' + y) = mk + 1$. Desenvolvendo o produto da esquerda, teremos para algum b inteiro que $mb + xy = mk + 1$, ou seja, que $xy \equiv 1 \mod (m)$.

Já sabemos que existe y que satisfaz $xy \equiv 1 \mod (m)$ se, e só se, $mdc(x,m) = 1$, concluindo o resultado que segue.

Teorema 4.4: O inverso multiplicativo da classe x módulo m existe se e somente se $mdc(x,m) = 1$.

Vale notar que para todo $a = mq + x$ temos $mdc(a,m) = mdc(x,m)$ pelo lema 3.5, de forma que a escolha do elemento da classe é indiferente. E tanto se tratando de elementos inteiros quanto de classes diremos inverso multiplicativo módulo m, de forma que o contexto deixará claro se estamos nos referindo a um elemento de $\mathbb{Z}$ ou de $\mathbb{Z}_m$.

Tome agora um primo p e seja $P = \{0,1,\cdots,p-1\}$. Com exceção do 0 todo elemento de P é coprimo com p e $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \cdots, \overline{p-1}\}$. Portanto, pelo teorema 4.4 concluímos que $\mathbb{Z}_p$ é um corpo.

Vamos verificar que a volta dessa conclusão é também verdadeira. Suponha assim que $\mathbb{Z}_m$ seja um corpo. Em particular todos elementos do conjunto $\{2,3,\cdots,m-1\}$ são coprimos com m e portanto não dividem m. Aplicando o teste 2.12 concluímos que m é primo e temos mais um resultado.

Teorema 4.5 (Caracterização de $\mathbb{Z}_p$): $\mathbb{Z}_p$ é um **corpo** se e somente se p é primo.

Importante afirmar que para m composto podem haver elementos que admitem inversos. Por exemplo, em $\mathbb{Z}_6$, além do $\overline{1}$, temos que $\overline{5}$ também possui inverso pois $\overline{5} \cdot \overline{5} = \overline{25} = \overline{1}$, e segue que esse elemento é seu próprio inverso. Enquanto, por verificação, nenhum outro elemento de $\mathbb{Z}_6$ possui inverso.

4.3 Teoremas de Euler e Fermat

Considere, em $\mathbb{Z}_m$, dois elementos $\overline{x_1}$ e $\overline{x_2}$ tais que possuam inversos $\overline{y_1}$ e $\overline{y_2}$ respectivamente. Assim $\overline{x_1} \cdot \overline{y_1} = 1$ e $\overline{x_2} \cdot \overline{y_2} = 1$. Portanto

$$\overline{x_1} \cdot \overline{y_1} \cdot \overline{x_2} \cdot \overline{y_2} = \overline{x_1 \cdot x_2} \cdot \overline{y_1 \cdot y_2} = 1$$

Portanto o elemento $\overline{x_1 \cdot x_2}$ também possui inverso multiplicativo, a saber, $\overline{y_1 \cdot y_2}$. Note que se tivéssemos um produto de k elementos invertíveis em $\mathbb{Z}_m$ ao invés de apenas dois, como foi o caso, concluiríamos de modo análogo que $\overline{x_1} \cdot \overline{x_2} \cdots \overline{x_k}$ também possuiria inverso multiplicativo neste anel, o que nos assegura que tal produto é um inteiro coprimo com m. Logo, **um produto de elementos invertíveis é um elemento invertível em um anel**, em particular em $\mathbb{Z}_p$.

Agora seja $mdc(a,p) = 1$ e considere o conjunto $\{\overline{0},\overline{a \cdot 1}, \cdots, \overline{a(p-1)}\}$ formado através da multiplicação de cada elemento de $\mathbb{Z}_p$ por $\overline{a}$. Se $\overline{a} \cdot \overline{r_1} = \overline{a} \cdot \overline{r_2}$ onde $\overline{r_1}$ e $\overline{r_2}$ são elementos distintos de $\mathbb{Z}_p$, temos, sendo $\overline{b}$ o inverso multiplicativo de $\overline{a}$, que

$$\overline{b} \cdot \overline{a} \cdot \overline{r_1} = \overline{b} \cdot \overline{a} \cdot \overline{r_2} \Rightarrow \overline{r_1} = \overline{r_2}$$

Mas sabemos que isso é impossível, pois cada elemento de $\mathbb{Z}_p$ é uma classe diferente. Logo $\mathbb{Z}_p = \{\overline{0},\overline{a \cdot 1}, \cdots, \overline{a(p-1)}\}$, pois além desse conjunto possuir p elementos, são todos classes distintas.

Assim é fato que existe uma bijeção entre os elementos de $\{\overline{a \cdot 1},\overline{a \cdot 2}, \cdots, \overline{a(p-1)}\}$ e de $\{\overline{1},\overline{2}, \cdots, \overline{p-1}\}$ que garante uma igualdade dois a dois destes. Não necessariamente $\overline{a \cdot i} = \overline{i}$, mas existe um único inteiro r_j com $1 \leq r_j \leq p-1$ tal que $\overline{a \cdot i} = \overline{r_j}$ onde $1 \leq i,j \leq p-1$. Então podemos fazer, sem perda de generalidade, $\overline{a \cdot i} = \overline{r_i}$ de forma que

$$\overline{a \cdot 1} \cdot \overline{a \cdot 2} \cdots \overline{a(p-1)} = \overline{r_1} \cdot \overline{r_2} \cdots \overline{r_{p-1}} \Rightarrow \overline{a^{p-1}} \cdot \overline{(p-1)!} = \overline{r_1} \cdot \overline{r_2} \cdots \overline{r_{p-1}}.$$

Logo, se $\overline{x}$ é o inverso multiplicativo de $\overline{(p-1)!}$ e como $\overline{r_1} \cdot \overline{r_2} \cdots \overline{r_{p-1}}$ é igual a $\overline{1} \cdot \overline{2} \cdots \overline{p-1}$ e que, por sua vez, pode ser escrito como $\overline{(p-1)!}$, temos que

$$\overline{a^{p-1}} \cdot \overline{(p-1)!} = \overline{(p-1)!} \Rightarrow \overline{a^{p-1}} \cdot \overline{(p-1)!} \cdot \overline{x} = \overline{(p-1)!} \cdot \overline{x} \Rightarrow \overline{a^{p-1}} = \overline{1}.$$

Note que $\overline{(p-1)!}$ nada mais é que um produto de elementos invertíveis em $\mathbb{Z}_p$, assegurando a existência de $\overline{x}$, seu inverso multiplicativo. Podemos escrever o resultado anterior com a linguagem de congruências.

Teorema 4.6 (Pequeno Teorema de Fermat): Se p é primo e $mdc(a,p) = 1$, então

$$a^{p-1} \equiv 1 \; mod(p).$$

O próximo corolário segue diretamente do Pequeno Teorema de Fermat.

Corolário 4.7: Se p é primo e $k \in \mathbb{N}$, então $a^{k(p-1)+1} \equiv a \; mod(p)$

Demonstração. Perceba que como consequência do teorema de Fermat teremos

$$\underbrace{a^{p-1} \cdots a^{p-1}}_{k \; vezes} \equiv \underbrace{1 \cdots 1}_{k \; vezes} mod(p)$$

e assim $a^{k(p-1)} \equiv 1 \; mod(p)$. E multiplicando cada lado desta congruência por a temos a prova completa.

□

Um fato importante é que os resultados desta seção seguem do fato de que há $p-1$ naturais coprimos com p e menores que p. No capítulo 6 há detalhes da **função fi de Euler**, que determina quantos coprimos há com n menores que n, para qualquer natural n, não somente primos.

4.4 Uma generalização do teorema de Euler

Nesta seção chegaremos a um resultado que de certa forma resume a teoria de congruências módulo m para a aplicação na criptografia RSA e que deriva dos resultados da seção anterior, entretanto com menos restrições. Basicamente queremos construir uma ferramenta para ser usada em $\mathbb{Z}_m$, onde m é o produto de dois primos.

Para isso reescrevamos o teorema de Euler, 4.7, como $\overline{a^{k(p-1)+1}} = \overline{a}$, em $\mathbb{Z}_p$, lembrando que tal resultado foi construído com as hipóteses de a ser coprimo com p e de p ser primo. Entretanto, supondo que a e p não sejam primos entre si teríamos que p divide a, pois p é primo, e assim a diferença entre potências de a seria um múltiplo de p, em particular p dividiria $a^{k(p-1)+1} - a$, ou seja, $\overline{a^{k(p-1)+1}} = \overline{a}$, de forma que o teorema de Euler vale para qualquer $a \in \mathbb{Z}$.

Importante destacar que o fato de não necessitarmos de muitas restrições sobre o inteiro a é essencial para o RSA, uma vez que esse número será a informação ou o texto cuja segurança queremos garantir, como veremos em capítulos posteriores.

Seja agora $r \neq p$ também primo. Para qualquer natural n é verdade que tanto em $\mathbb{Z}_p$ quanto em $\mathbb{Z}_r$ vale a igualdade $\overline{a^{n(p-1)(r-1)+1}} = \overline{a}$. Para prová-la basta tomar $k = n(r-1)$ e aplicar o teorema 4.7 em $\mathbb{Z}_p$ e depois proceder de maneira análoga em $\mathbb{Z}_r$, tomando $k' = n(p-1)$. Considere então o natural m formado pelo produto desses primos, $m = pr$. Vamos mostrar que tal igualdade de classes também é válida em $\mathbb{Z}_m$, fato que advém imediatamente do resultado que se segue.

Lema 4.8: Sejam p e r primos distintos tais que $p|b$ e $r|b$. Então $pr|b$.

Demonstração. Como $p|b$ temos $b = pq$ para algum inteiro q. Usando os teoremas 2.8 e 2.9 e a hipótese, temos que $r|q$. Daí $q = rq'$ e assim $b = prq'$. Portanto $pr|b$.

□

Teorema 4.9 (Teorema de Euler para o RSA): Sejam p e r primos distintos e $m = pr$. Então $a^{n(p-1)(r-1)+1} \equiv a \ mod(m)$ para quaisquer $n \in \mathbb{N}$ e $a \in \mathbb{Z}$.

Demonstração. De acordo com o teorema 4.7, $\overline{a^{n(p-1)(r-1)+1}} = \overline{a}$ em $\mathbb{Z}_p$ e em $\mathbb{Z}_r$, o que pode ser escrito respectivamente como

$$a^{n(p-1)(r-1)+1} \equiv a \ mod(p) \quad e \quad a^{n(p-1)(r-1)+1} \equiv a \ mod(r).$$

Daí segue que p e r dividem $a^{n(p-1)(r-1)+1} - a$ e de acordo com o lema 4.8, tem-se que $m = pr$ também divide essa diferença, tomando $b = a^{n(p-1)(r-1)+1} - a$ e colecionamos outro resultado, este com aplicação direta na criptografia RSA.

□

Temos basicamente o último resultado de que precisamos para entender o funcionamento da criptografia RSA. Portanto cabe-nos agora estudar as fases de encriptação e aplicar o Teorema.

5 O RSA

Neste capítulo vamos compreender como funciona a matemática da Criptografia RSA, aplicando o Teorema de Euler para RSA, além de investigar a dificuldade em se quebrar o código protegido por esse modelo de encriptação.

5.1 Pré-codificação

Foi dito na última seção do capítulo anterior que o número a no teorema 4.9 seria a informação ou o texto a ser protegido, que chamaremos agora de "mensagem original". Na primeira etapa da criptografia, a pré-codificação, precisamos converter os caracteres que formam tal mensagem em números para que o computador possa entendê-la. Basicamente significa trocar cada número, letra, sinal etc. que compõem a mensagem original por um número em uma tabela pré-definida, que na maioria dos casos por motivos de padronização é a Tabela *ASCII*.

A Figura 5.1 mostra a Tabela *ASCII*. Há várias colunas, mas vamos destacar apenas as que nos interessam aqui. Na base decimal, os caracteres de texto são numerados de 0 a 127, de modo que, por exemplo, a letra "M" é representada pelo número 77. Há diferenciação entre letras maiúsculas e minúsculas, e a letra "m" é convertida para o número 109 após a pré-codificação. O espaço entre palavras, pelo número 32.

Então o texto, após esse primeiro processo, em geral forma um número natural muito grande. O próximo passo é escolher dois primos distintos p e q, definindo m, que é o produto desses primos. Depois, o natural ao qual a mensagem original foi convertida é "separado" em números $a_i's$ menores que m, formando uma sequência de números que denominaremos blocos. Muitas vezes nos referiremos à mensagem como sendo um número, o que faz sentido no presente contexto.

Ao longo do capítulo iremos lançar mão de um exemplo para melhor ilustrar o funcionamento da encriptação através do modelo RSA. Iniciaremos com a pré codificação, a seguir.

Exemplo 5.1.1: Usando a tabela ASCII o texto

A criptografia RSA utiliza chave pública

se torna, após a transcrição[1] na base decimal, em

$a = 653299114105112116111103114971021059732828365321171161051081051229732$
$991049711810132112250981081059997 46$

Para fazermos a pré-codificação, tomemos como exemplo $m = 1457$ o produto dos primos 47 e 31. Separamos agora, de maneira aleatória, a em 34 blocos de números menores que 1457. Veja que assim escolhemos p e q pequenos, apenas com propósito de exemplificar o processo, pois na prática é recomendável que tenham em torno de 200 dígitos cada um, na base decimal. Assim obteremos os blocos que seguem.

$a_1 = 653$,$a_2 = 299$, $a_3 = 114$, $a_4 = 1051$, $a_5 = 1211$, $a_6 = 611$, $a_7 = 1103$, $a_8 = 1149$, $a_9 = 710$, $a_{10} = 210$, $a_{11} = 597$, $a_{12} = 328$, $a_{13} = 283$, $a_{14} = 653$, $a_{15} = 211$, $a_{16} = 711$, $a_{17} = 610$, $a_{18} = 510$, $a_{19} = 810$, $a_{20} = 512$, $a_{21} = 297$, $a_{22} = 329$, $a_{23} = 910$, $a_{24} = 497$, $a_{25} = 118$, $a_{26} = 1013$, $a_{27} = 211$, $a_{28} = 22$, $a_{29} = 509$, $a_{30} = 810$, $a_{31} = 810$, $a_{32} = 599$, $a_{33} = 974$ e $a_{34} = 6$.

Portanto a pré-codificação da nossa pequena mensagem está pronta.

5.2 Codificação e decodificação

Uma vez pré-codificada, a mensagem está quase pronta para ser enviada. Tratando-se de mensagens que contenham informações confidenciais, como o número do cartão de crédito, ou de cunho pessoal, como conversas que possam revelar indesejadamente vulnerabilidades caso em posse de pessoas mal intencionadas, é extremamente necessário protegê-las.

A escolha do natural m já inicia o processo de codificação, ou, mais precisamente, a escolha de p e r tais que $pr = m$ o inicia. Assim podemos separar a mensagem a em blocos $a_i's$, todos naturais menores que m. Isso é importante porque nos garante que cada bloco é igual a um resto na divisão por m, de outra forma, cada a_i se associa a apenas um elemento do conjunto $\{1,2,\cdots m-1\}$. O inverso não é necessariamente verdadeiro, ou seja, um elemento do conjunto dos restos pode se associar a mais de um bloco ou até a

[1] Feito com auxílio do site http://www.numaboa.com.br/escolinha/garranchos/146-informatizados/351-ascii, acesso em 25 de novembro de 2021

Figura 5.1: Tabela ASCII

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DE

Fonte: disponível em http://www.lookuptables.com/, acesso em 25 de novembro de 2021

nenhum bloco.

O passo seguinte é determinar x e y tais que, em $\mathbb{Z}_{(p-1)(r-1)}$, $\overline{x} \cdot \overline{y} = \overline{1}$, ou seja, determinar um inteiro invertível e seu inverso no anel em questão. Note que dessa forma existe $k \in \mathbb{N}$ tal que $xy = k(p-1)(r-1)+1$. Depois calcula-se t_i tal que $t_i \equiv a_i^x \mod (m)$ para cada i, ou seja, para cada bloco da mensagem. Os blocos $t_i's$ representam a **mensagem codificada**. Perceba que de posse da mensagem a precisamos apenas de x e m para codificá-la.

Usando o exemplo 5.1.1, temos $p = 47$ e $r = 31$. Logo devemos procurar em $\mathbb{Z}_{(47-1)(31-1)}$, ou seja, em $\mathbb{Z}_{1380}$, x invertível e seu inverso. Podemos, para posteriormente escolher x, analisar os primos que não estão na fatoração nem de 46 e nem de 30, como por exemplo 7 e 11. Logo 7 e 11 também não aparecem na fatoração de 1380, sendo coprimos com este, tal como seu produto, 77, que é portanto invertível em $\mathbb{Z}_{1380}$. Portanto podemos tomar $x = 77$.

Exemplo 5.2.1: Elevando cada bloco a 77 e tomando seu respectivo resto na divisão euclidiana por 1457 e concatenando-os obtemos o natural

$t = 139980310784747171128144096513313468391409141110891307306892971116382934231367127210902101307125232711631163906107121 2$

que é justamente a mensagem protegida, que denotaremos **mensagem codificada**.

Para determinar y precisamos resolver $77y \equiv 1 \mod (1380)$, o que equivale a encontrar y e c na equação $77y + 1380c = 1$. Podemos determiná-los usando o método descrito para se provar o algoritmo de Euclides estendido, 3.6, obtendo $77 \cdot 233 + 1380 \cdot (-13) = 1$ e assim $y = 233$.

Em geral, para decodificar a mensagem, ou seja, a partir dos blocos $t_i's$ recuperar a mensagem original, determinamos $b_i's$ menores que m tais que $t_i^y \equiv b_i \mod (m)$, para cada i. Então chamaremos de **mensagem decodificada** a concatenação dos blocos $b_i's$ na mesma ordem que os respectivos $t_i's$. Argumentaremos então que a mensagem decodificada coincide com a mensagem original.

Em outras palavras, mostratremos que $b_i = a_i$ para todo i, de modo que obtemos a mensagem inicial após os dois últimos passos, que consistiram, respectivamente, em elevar cada bloco encriptado a y e depois a determinar a qual resto na divisão euclidiana por m cada um é congruente.

De uma maneira mais detalhada temos que $t_i^y = a_i^{xy}$ e, por sua vez, $a_i^{xy} = a_i^{k(p-1)(r-1)+1}$, pois x e y foram escolhidos para satisfazerem essa condição para algum k natural. Assim, aplicando o Teorema de Euler para RSA, 4.9, em $\mathbb{Z}_m$

$$\overline{a_i^{k(p-1)(r-1)+1}} = \overline{a}_i$$

A princípio isso só garante uma igualdade de classes, pois, como uma interpretação do resultado anterior, o resto da divisão por m do bloco encriptado elevado a y é o mesmo resto na divisão por m de cada bloco original, ou seja, não encriptado. Entretanto a condição de cada bloco a_i ser um natural menor que m garante, como já dito, que eles pertençam ao conjunto $M = \{0,1,\cdots m-1\}$, ou seja, que eles sejam o próprio resto, de modo que, de posse dos $b_i's$ - os blocos encriptados elevados a y - os restos destes na divisão por m serão, pela congruência das classes, os próprios $a_i's$.

5.3 Uma ilustração

Vamos organizar o raciocínio estabelecido na seção anterior e exemplificar o funcionamento do RSA supondo um aplicativo de mensagens chamado "CEFET MESSENGER" e dois usuários do aplicativo, THIAGO e ÉDEN. Digamos que THIAGO queira enviar uma mensagem para ÉDEN usando esse aplicativo. Os passos que envolvem a proteção da mensagem desde sua concepção pelo remetente até a leitura pelo destinatário serão listados a seguir.

1 ÉDEN determina m,x e calcula y tal que seja invertível em $\mathbb{Z}_{(p-1)(r-1)}$;

2 ÉDEN envia m e x para THIAGO;

3 THIAGO escreve a mensagem original e a pré-codifica no natural a;

4 THIAGO "separa" o natural a em números $a_i's$ menores que m;

5 THIAGO calcula, para cada i, $t_i = a_i^x$;

6 THIAGO envia os $t_i's$ para ÉDEN;

7 ÉDEN calcula, para cada i, t_i^y;

8 ÉDEN obtém a mensagem original.

Cabem algumas observações. Primeiramente há um abuso de linguagem, pois nenhum dos usuários faria qualquer coisa a não ser escrever e ler a mensagem. Assim, quando falamos que ÉDEN determina m e x por exemplo, deixamos implícito que o CEFET MESSENGER o faz no dispositivo em que é usado, um *smartphone* por exemplo.

No segundo passo, quando ÉDEN envia o par de números (m,x) a THIAGO, ele o faz através de uma transmissão de dados insegura, de forma que esses números se tornam vulneráveis, ou seja, acessíveis a qualquer um. De fato, eles são o que denomina *chave pública*, acessíveis a qualquer um que queira enviar informações a ÉDEN ou eventuais intrusos, tanto que podemos falar em compartilhá-la e não necessariamente em enviá-la, dispondo-a em alguma pasta pública.

De maneira semelhante, no sexto passo THIAGO envia os blocos da mensagem encriptados a ÉDEN deixando-os de certa forma expostos a receptores indesejáveis, como

por exemplo *hackers* interessados em fazer mal uso de dados muitas vezes particulares que possam compor a mensagem original. Daí a necessidade de transmiti-la de forma codificada.

Sem posse do natural y, inverso multiplicativo de x em $\mathbb{Z}_{(p-1)(r-1)}$, e dos fatores primos de m, é praticamente impossível decifrar a mensagem, pois o custo computacional para se fazê-lo é muito alto. E é justamente nesse ponto que reside a segurança do método RSA, na impossibilidade prática de se determinar p, r ou y, que determinam a *chave privada*, conhecendo-se apenas a chave pública, mesmo que teoricamente seja possível.

5.4 A segurança do RSA

De acordo com o primeiro capítulo do livro [8], algoritmos são sequências de procedimentos computacionais bem definidos que transformam um conjunto de valores que toma como **entrada** em outro conjunto de valores que formam a **saída**, com um objetivo claro de resolver algum problema computacional. Tais problemas são extremamente variados e muito possivelmente inúmeros deles determinam ou no mínimo influenciam nosso cotidiano, mesmo que não percebamos. Seguem alguns exemplos.

Organizar listas de números em ordem crescente. Neste caso uma lista com n números reais em ordem aleatória forma a entrada, enquanto uma lista com estes mesmos n reais agora em ordem crescente forma a saída.

Otimizar a rota de uma entrega. Uma entrada podem ser os variados caminhos e a saída um caminho considerado ótimo, em relação ao tempo e à distância percorrida.

Uma busca na internet. O texto da busca em algum site de pesquisa como o *Google* pode ser a entrada e as páginas de internet que aparecem como resultados podem ser as saídas.

Determinar a primalidade de um número natural. A entrada é um número natural e a saída é a afirmação ou negação de sua primalidade.

Fatorar um número natural. A entrada é um natural e a saída são seus fatores primos.

Os dois últimos exemplos da lista são de nosso particular interesse para argumentar sobre a segurança dos modelos de encriptação que usam o RSA.

Como já citado em 2.3, é importante compreender a **complexidade computacional** de um algoritmo, a medida do número de operações computacionais realizadas para aplicar o algoritmo em função do tamanho de sua entrada. Em geral, são consideradas as representações binárias das entradas e operações computacionais. No caso dos testes de primalidade e algoritmos de fatoração, considera-se o número de dígitos na representação binária do inteiro.

Mais importante do que determinar o número exato de operações, é identificar a ordem de crescimento da complexidade computacional. Assim, dizer que a complexidade computacional de um algoritmo tem ordem de crescimento exponencial - ou simplesmente que o algoritmo tem complexidade exponencial - é dizer que o número de operações realizadas é proporcional a uma função exponencial do tamanho da entrada. Assim, para entradas muito grandes, o número de operações cresce significativamente. Já um algoritmo com complexidade polinomial teria um custo computacional bem reduzido em relação ao anterior, uma vez que a ordem de crescimento de uma função polinomial é bem menor que a de uma função exponencial. Vale ressaltar que a ordem de crescimento está diretamente relacionada ao tempo de execução do algoritmo.

Algoritmos de teste de primalidade mais ingênuos como os apresentados na seção 3 do capítulo 2 têm complexidade computacional com ordem de grandeza exponencial. Apesar disso, existem outros testes mais eficientes e atuais, como o algoritmo AKS, determinístico e de complexidade polinomial. A eficiência dos algoritmos de teste de primalidade é demandada para a escolha do par de primos p e r da criptografia RSA.

Porém, para os algoritmos de fatoração de um natural em primos, não é conhecido algoritmo determinístico com complexidade computacional polinomial - em computação clássica![2] O que pode parecer uma característica "defectiva" dos algoritmos de fatoração é o que garante a segurança do RSA.

Em outras palavras, pode-se descobrir facilmente a primalidade de um número natural sem fatorá-lo mas pode ser muito difícil fatorar um número natural composto dado. Em particular, existe certa praticidade em se determinar p e r e certa dificuldade em se fatorar n.

Assim, para a construção do RSA estamos interessados em verificar a primalidade de números naturais muito grandes para produzir números compostos muito grandes. No

[2] É sabido pelo algoritmo de Schor que é possível executar a fatoração de um inteiro em tempo polinomial, em um computador quântico.

contexto da encriptação pelo modelo RSA, precisa-se de números primos com duzentos dígitos ou mais no sistema decimal para se definir p e r de modo a garantir alguma segurança.

E, como dito, é essencial para a segurança do RSA que seja assim, tanto para a construção do modelo quanto para sua proteção, visto que fatorar n significa saber p e r, e assim, de posse também de x ficaria relativamente simples determinar y e ter acesso à mensagem codificada.

6 Usando a Função Totiente para o cálculo de chaves do RSA

Entre os variados questionamentos pertinentes após teorizarmos o modelo RSA, podemos nos perguntar quantas chaves distintas e não triviais x e y pode-se obter tais que $xy \equiv 1 \mod (p-1)(r-1)$, lembrando que p e r são primos. Não triviais porque gostaríamos que tanto x quanto y fossem diferentes de 1 ou, de uma maneira mais geral, não pertencessem à classe $\overline{1}$ em $\mathbb{Z}_{(p-1)(r-1)}$, senão não haveria encriptação.

De fato, se a é um bloco da mensagem original e se $x \in \overline{1}$ no dito anel, então

$$x = k(p-1)(r-1) + 1,$$

para algum k natural, de modo que basta aplicar 4.9 para se obter a mensagem original sem a necessidade da chave y, pois teríamos $a^x \equiv a \mod (m)$.

Veremos que mesmo após estabelecida uma fórmula que de certa maneira calcula a quantidade de diferentes chaves, sua aplicação não é tão simples.

6.1 Função phi de Euler

Podemos aperfeiçoar um pouco a pergunta: na verdade precisamos saber quantas classes possuem elementos coprimos com $(p-1)(r-1)$ em $\mathbb{Z}_{(p-1)(r-1)}$. Isso porque cada classe nos dará infinitos elementos em $\mathbb{Z}$ com tal propriedade. Assim podemos olhar apenas para o conjunto de naturais entre 1 e $(p-1)(r-1)-1$ e contar quantos são os coprimos com $(p-1)(r-1)$.

Para isso definimos a função *totiente*, também conhecida como *phi de Euler*, que basicamente conta, dado um natural n qualquer, quantos coprimos com n existem entre 1 e $n-1$.

Definição 6.1 (A função Totiente): Seja $n \in \mathbb{N}$. Então $\phi(n)$ é a quantidade de

números i pertencentes ao conjunto $\{1,2,\cdots,n-1\}$ tais que $mdc(n,i) = 1$.

Por exemplo, para se calcular $\phi(6)$ deve-se analisar quantos elementos em $\{1,2,3,4,5\}$ são coprimos com 6. Como apenas 1 e 5 são coprimos com 6 nesse conjunto, temos $\phi(6) = 2$.

Agora note que $\phi(2) = 1$, $\phi(3) = 2$, $\phi(5) = 4$, $\phi(7) = 6$, $\phi(11) = 10$, etc, de modo a levantarmos a conjectura de que se p é primo, então $\phi(p) = p - 1$, o que é fato, pois p ser primo implica em $mdc(p,i) = 1$ para todo i entre 1 e $p - 1$. E note que a volta também é verificada, ou seja, se $\phi(p) = p - 1$, então p é primo, pois se fosse composto existiria ao menos um $i \in \{1,2,\cdots,p-1\}$ tal que $mdc(p,i) \neq 1$ e assim $\phi(p) < p - 1$. Segue o resultado.

Teorema 6.2: Seja $p \in \mathbb{N}$. Então $\phi(p) = p - 1$ se, e somente se p é primo.

Também podemos calcular $\phi(p^n)$, ou seja, dado uma potência de um número primo podemos determinar quantos coprimos menores a essa potência existem. Notemos primeiro que $mdc(p^n,i) = 1$ se, e somente se i não é múltiplo de p, pois p é primo. Portanto, para se determinar $\phi(p^n)$ basta retirarmos da quantidade total de naturais até p^n os múltiplos de p.

Mas os múltiplos de p são $1p, 2p, \cdots, p^{n-1}p$, de modo que há p^{n-1} múltiplos de p até sua enésima potência, e portanto

$$\phi(p^n) = p^n - p^{n-1} \Rightarrow \phi(p^n) = p^{n-1}(p-1).$$

Teorema 6.3: Seja p um natural primo e $n \in \mathbb{N}$. Então $\phi(p^n) = p^{n-1}(p-1)$.

Agora nossa tarefa é a de determinar $\phi(a \cdot b)$, onde a e b são coprimos. Mostraremos que, com essa hipótese, $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$. Feito isso, estaremos aptos a calcular $\phi(n)$ para qualquer $n \in \mathbb{N}$. No entanto, precisamos de alguns resultados preliminares.

O primeiro deles é o fato de que, dados a e b que são coprimos e outro natural i, se a e i são coprimos assim como b e i o são, temos ab e i coprimos, e vice versa, se ab e i são coprimos, então $mdc(a,i) = mdc(b,i) = 1$.

Para provarmos a ida temos como hipóteses $mdc(a,b) = mdc(a,i) = mdc(b,i) = 1$. Então suponha que $mdc(ab,i) \neq 1$, ou equivalentemente, suponha que exista um primo p tal que $p|i$ e $p|ab$. Como a e b são coprimos, p deve dividir a ou b, mas isso implicaria que

$mdc(a,i) = p$ ou $mdc(b,i) = p$, o que contradiz a hipótese. Então

$$mdc(a,b) = mdc(a,i) = mdc(b,i) = 1 \Rightarrow mdc(ab,i) = 1.$$

Agora, para a volta, temos como hipótese $mdc(a,b) = mdc(ab,i) = 1$, e chegamos imediatamente no resultado, pois se algum d divisor de i é tal que $d|a$ ou $d|b$, teríamos que $d|ab$, acarretando em uma contradição. Assim concluímos

$$mdc(a,b) = mdc(a,i) = mdc(b,i) = 1 \Leftrightarrow mdc(a,b) = mdc(ab,i) = 1.$$

Os outros dois resultados preliminares dizem respeito ao anel comutativo com unidade, $\mathbb{Z}_m$. Para fins didáticos, trataremos de um resultado em $\mathbb{Z}_a$ e outro em $\mathbb{Z}_b$.

Já temos conhecimento que cada elemento do conjunto $A = \{1,2,\cdots,a\}$ pertence a uma classe distinta, e somente uma, de $\mathbb{Z}_a$, que por sua vez é completamente representável por A, de modo que $\mathbb{Z}_a = \{\overline{a},\overline{1},\overline{2},\cdots,\overline{a-1}\}$. Somando um múltiplo de a a cada elemento $\alpha \in A$, teremos $\alpha + ak$, e assim, em $\mathbb{Z}_a$:

$$\overline{\alpha + ak} = \overline{\alpha} + \overline{ak} = \overline{\alpha} + \overline{0} = \overline{\alpha}.$$

Em palavras, os naturais de 1 a a representam todo $\mathbb{Z}_a$ e somando qualquer múltiplo de a a esses naturais obtemos também uma representação de todas classes de $\mathbb{Z}_a$, e na mesma ordem. Poderíamos também ter usado o terceiro item de 3.4 para tê-lo provado, mas o uso de propriedades de classes torna o trabalho mais conciso.

Para exemplificar, considere $\mathbb{Z}_6 = \left\{\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6}\right\}$. Qualquer um dos conjuntos $\{7,8,9,10,11,12\}$, $\{13,14,15,16,17,18\}$, $\{19,20,21,22,23,24\}$, $\{25,26,27,28,29,30\}$ ou $\{-5,-4,-3,-2,-1,0\}$ pode ser usado para representar $\mathbb{Z}_6$.

Na seção 4.3 mostramos que multiplicar cada elemento de $\mathbb{Z}_b$ por a nos dará outra representação de $\mathbb{Z}_b$, mesmo que não mantendo a ordem, pois $mdc(a,b) = 1$. Ou seja

$$\mathbb{Z}_b = \left\{\overline{0 \cdot a},\overline{1 \cdot a},\overline{2 \cdot a},\cdots,\overline{(b-1) \cdot a}\right\}.$$

Mais ainda, somando um inteiro k a cada elemento desse anel, ainda teremos outra maneira

de representá-lo, ou seja

$$\mathbb{Z}_b = \left\{\overline{0 \cdot a + k}, \overline{1 \cdot a + k}, \overline{2 \cdot a + k}, \cdots, \overline{(b-1) \cdot a + k}\right\}.$$

Isso ocorre porque se $\overline{n_1 \cdot a + k} = \overline{n_2 \cdot a + k}$, com $0 \leq n_1 \leq b-1$, $0 \leq n_2 \leq b-1$ e $n_1 \neq n_2$ então

$$\overline{n_1 \cdot a + k} = \overline{n_2 \cdot a + k} \Leftrightarrow \overline{n_1 \cdot a} + \overline{k} = \overline{n_2 \cdot a} + \overline{k} \Leftrightarrow \overline{n_1 \cdot a} = \overline{n_2 \cdot a}$$

o que contradiz a hipótese, já que devem ser classes distintas em $\mathbb{Z}_b$.

Por exemplo, $\{\overline{1}, \overline{7}, \overline{13}, \overline{19}, \overline{25}\}$, $\{\overline{2}, \overline{8}, \overline{14}, \overline{20}, \overline{26}\}$, $\{\overline{3}, \overline{9}, \overline{15}, \overline{21}, \overline{27}\}$ e $\{\overline{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}\}$ são representações de $\mathbb{Z}_5$ usando representantes distintos para suas classes.

Já temos o que precisamos para calcular $\phi(a \cdot b)$. Para isso vamos organizar os números de 1 a $a \cdot b$ na tabela 6.1 e usar as propriedades provadas.

Tabela 6.1: Tabela de elementos de $\mathbb{Z}_{ab}$.

$0 \cdot a + 1$	$0 \cdot a + 2$	$\cdots$	$0 \cdot a + a = 1a$
$1 \cdot a + 1$	$1 \cdot a + 2$	$\cdots$	$1 \cdot a + a = 2a$
$2 \cdot a + 1$	$2 \cdot a + 2$	$\cdots$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
$(b-1) \cdot a + 1$	$(b-1) \cdot a + 2$	$\cdots$	$(b-1) \cdot a + a = ab$

Fonte: criada pelos autores.

Note que cada linha desta tabela tem exatamente a elementos e é uma representação de $\mathbb{Z}_a$ e que cada coluna tem exatamente b elementos e é uma representação de $\mathbb{Z}_b$, conforme os argumentos desta seção. Portanto cada linha tem $\phi(a)$ coprimos com a e cada coluna tem $\phi(b)$ coprimos com b. E mais, se um elemento de uma linha for coprimo com a, todos elementos da coluna a que ele pertence são, pois são da forma *múltiplo do natural a mais um inteiro fixo*.

Como também provado aqui, se um número desta tabela é coprimo com ab, ele deve ser coprimo com a e b simultaneamente. Então considere as colunas de coprimos com a. Há $\phi(a)$ colunas desta. Cada uma delas, como dito, é uma representação de $\mathbb{Z}_b$, de maneira que há $\phi(b)$ coprimos com b em cada. Então há $\phi(a) \cdot \phi(b)$ coprimos com ab de 1 a ab. Assim, concluímos a demonstração do teorema principal desta seção.

Teorema 6.4: Sejam a e b naturais tais que $mdc(a,b) = 1$. Então $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

Vamos calcular $\phi(5 \cdot 6) = \phi(30)$. Antes do cálculo, note as propriedades aqui descritas na tabela 6.2, similar à 6.1, para exemplificação, onde a terceira coluna e a quarta linha foram escritas de forma a se verificar uma possível construção de $\mathbb{Z}_5$ e $\mathbb{Z}_6$, respectivamente.

Tabela 6.2: Tabela de elementos de $\mathbb{Z}_{30}$.

1	2	$0 \cdot 6 + 3$	4	5	6
7	8	$1 \cdot 6 + 3$	10	11	12
13	14	$2 \cdot 6 + 3$	16	17	18
$3 \cdot 6 + 1$	$3 \cdot 6 + 2$	$3 \cdot 6 + 3$	$3 \cdot 6 + 4$	$3 \cdot 6 + 5$	$3 \cdot 6 + 6$
25	26	$4 \cdot 6 + 3$	28	29	30

Fonte: criada pelos autores.

Usando o teorema, temos que $\phi(30) = \phi(5) \cdot \phi(6) = 4 \cdot 2 = 8$.

Pensando em estender o teorema 6.4, considere $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$, onde cada p_i é um primo distinto, k é um natural e cada e_i é natural ou nulo, ou seja, trata-se da fatoração em primos de n. Então $mdc(p_i^{e_i}, p_j^{e_j}) = 1$ se $i \neq j$, de modo que podemos usar os teoremas 6.4 e 6.3 e obter uma generalização, que encerra esta seção.

Teorema 6.5: Seja $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$ a fatoração em primos de n. Então

$$\phi(n) = \phi(p_1^{e_1}) \cdot \phi(p_2^{e_2}) \cdots \phi(p_k^{e_k}) = p_1^{e_1-1}(p_1 - 1) \cdot p_2^{e_2-1}(p_2 - 1) \cdots p_k^{e_k-1}(p_k - 1).$$

6.2 Consequências e reflexões

Agora já temos um algoritmo para calcular quantas "classes coprimas" há em $\mathbb{Z}_m$ para qualquer m, ou seja, conseguimos calcular quantos coprimos menores que um certo m há. Potencialmente, porque para se efetuar o cálculo dependemos da fatoração de m.

Em particular, para $m = pr$ com p e r primos distintos,

$$\phi(m) = \phi(p) \cdot \phi(r) = (p - 1)(r - 1).$$

Assim, o teorema 4.9 pode agora ser reescrito como se segue.

Teorema 6.6 (Teorema de Euler para o RSA - segunda versão): Sejam p e r primos distintos e $m = pr$. Então $\overline{a^{n\phi(m)+1}} = \overline{a}$ em $\mathbb{Z}_m$, com $n \in \mathbb{N}$ e $a \in \mathbb{Z}$.

Recordando, o problema proposto no início neste capítulo é o de se verificar quantas chaves distintas x e y não triviais podemos obter para a encriptação RSA, ou seja, $xy \equiv 1$ mod $\phi(m)$. Para contá-las podemos fazer $\phi((p-1)(r-1))$ ou $\phi(\phi(m))$, o que nem sempre é simples, pois depende de determinarmos os fatores primos de $\phi(m)$.

Os fatores $p-1$ e $r-1$ são pares, logo não são primos, além de não serem coprimos entre si, não podendo aplicar diretamente o teorema 6.5.

Tomemos o exemplo do capítulo 5, onde $p = 47$ e $r = 31$. Temos que

$$\phi(47 \cdot 31) = 46 \cdot 30 = 1380.$$

E como $1380 = 2^2 \cdot 3 \cdot 5 \cdot 23$, o que foi feito usando o algoritmo clássico ensinado na educação básica, temos

$$\phi(1380) = 2^{2-1}(2-1)3^{1-1}(3-1)5^{1-1}(5-1)23^{1-1}(23-1) = 352.$$

7 Uma proposta de sequência didática para o 6° ano do Ensino Fundamental

7.1 Diretrizes da proposta

Nas três próximas seções apresentamos uma proposta de sequência didática para alunos do 6° ano do EF que são organizadas de acordo com as diretrizes de plano de aulas sugerido por [9], que envolvem apresentar o objetivo, os recursos, a metodologia e o público alvo. Apenas a sistemática de avaliação não foi proposta, deixando mais amplo o contexto de atuação para o docente que se utilizar das atividades. Convém destacar que neste texto entendemos como sequência didática uma proposta de atividades destinadas a um grupo pré-definido de estudantes e em que há conexão e progressão de ideias. Também se faz importante afirmar que acreditamos que um plano de aula não pode ser desconexo do contexto escolar onde ele se insere, e sim, sob nossas perspectivas e das autoras de [9], é parte integrante deste. Assim, sob essa ótica, apesar de parecerem fragmentadas neste texto, as atividades foram pensadas em um contexto particular mas escritas para que sejam mais abrangentes. Isso se dá tanto por conta de deliberadamente deixar a proposta mais ampla, e também porque não foi possível aplicá-las devido aos efeitos da pandemia de COVID-19 no ano letivo de 2021, o que poderia gerar discussões mais particulares.

Com um total de quatro aulas, o objetivo principal da sequência é o de se introduzir os conceitos de primalidade através de um sistema simplificado de Criptografia RSA, o uso de calculadoras e de jogos. Na primeira aula proposta retoma-se as ideias de múltiplo e divisor através de um jogo; na segunda, introduz-se brevemente o conceito de primalidade e pede-se para os estudantes que, usando calculadoras, criem uma forma de se verificar quando um dado número é primo ou não além de testarem a primalidade de alguns números em uma lista; já na terceira aula, introduz-se a ideia de criptografia através de pesquisas

em aplicativos de compra e de troca de mensagens e constrói-se chaves para um modelo simplificado de encriptação; e, por fim, na quarta aula proposta os estudantes simulam uma "quebra de código" através desse modelo simplificado de encriptação, estimulando o desenvolvimento de habilidades relacionadas à fatorar e decidir se um número é primo ou não, através de um jogo e usando calculadoras. Possibilita também criar-se um espaço para contextualizar a criptografia nos cotidianos dos estudantes.

Cabe aqui uma observação importante. Apesar de os atuais discentes serem nativos digitais, ou seja, além de familiarizados com as tecnologias digitais fazem uso delas com bastante regularidade, como apontado em [1][1] não se pode inferir que utilizam tais ferramentas de maneira consciente, no sentido do trecho a seguir, extraído da BNCC, ao tratar das complexidades que envolvem o Ensino Fundamental.

> Há que se considerar, ainda, que a cultura digital tem promovido mudanças sociais significativas nas sociedades contemporâneas. Em decorrência do avanço e da multiplicação das tecnologias de informação e comunicação e do crescente acesso a elas pela maior disponibilidade de computadores, telefones celulares, tablets e afins, os estudantes estão dinamicamente inseridos nessa cultura, não somente como consumidores. Os jovens têm se engajado cada vez mais como protagonistas da cultura digital, envolvendo-se diretamente em novas formas de interação multimidiática e multimodal e de atuação social em rede, que se realizam de modo cada vez mais ágil.
>
> Por sua vez, essa cultura também apresenta forte apelo emocional e induz ao imediatismo de respostas e à efemeridade das informações, privilegiando análises superficiais e o uso de imagens e formas de expressão mais sintéticas, diferentes dos modos de dizer e argumentar característicos da vida escolar. Todo esse quadro impõe à escola desafios ao cumprimento do seu papel em relação à formação das novas gerações. É importante que a instituição escolar preserve seu compromisso de estimular a reflexão e a análise aprofundada e contribua para o desenvolvimento, no estudante, de uma atitude crítica em relação ao conteúdo e à multiplicidade de ofertas midiáticas e digitais. Contudo, também é imprescindível que a escola compreenda e incorpore mais as novas linguagens e seus modos de funcionamento, desvendando possibilidades de comunicação (e também de manipulação), e que eduque para usos mais democráticos das tecnologias e para uma participação mais consciente na cultura digital. Ao aproveitar o potencial de comunicação do universo digital, a escola pode instituir novos modos de promover a aprendizagem, a interação e o compartilhamento de significados entre professores e estudantes. ([10], pg. 61)

A própria criptografia, que possui uma importância inquestionável no mundo

[1] Apesar de a análise da autora se basear no público português, um cenário muito parecido pode ser observado no Brasil, especialmente analisando-se os resultados da PNAD Contínua TIC 2018, mostrando a presença progressiva que as tecnologias digitais de informação obtêm no nosso cotidiano.

contemporâneo visto que possibilitou trocas de mensagens e serviços de compra em massa moldando mesmo que indiretamente nosso modo de viver, pode ser desconhecida por muitos discentes. Logo a sequência didática permite criar um espaço enriquecedor para se tratar desse tema e corroborar a formação de cidadãos ativos. Além do mais não há dúvidas de que os empregos do futuro certamente exigirão a capacidade de manipular e compreender variados *softwares* em variados níveis de habilidade, de modo que a inclusão e ascensão social também dependerão (já dependem, em certo nível) de quão capacitado estará o sujeito para lidar com essas ferramentas. Ademais, a própria rotina, independentemente do trabalho, já é cercada por tecnologias digitais. Portanto, acreditamos que as escolas já devem se orientar e se organizar no sentido de levar em conta tais tecnologias no seu projeto político pedagógico.

> Essa constante transformação ocasionada pelas tecnologias, bem como sua repercussão na forma como as pessoas se comunicam, impacta diretamente no funcionamento da sociedade e, portanto, no mundo do trabalho. A dinamicidade e a fluidez das relações sociais – seja em nível interpessoal, seja em nível planetário – têm impactos na formação das novas gerações. É preciso garantir aos jovens aprendizagens para atuar em uma sociedade em constante mudança, prepará-los para profissões que ainda não existem, para usar tecnologias que ainda não foram inventadas e para resolver problemas que ainda não conhecemos. Certamente, grande parte das futuras profissões envolverá, direta ou indiretamente, computação e tecnologias digitais. ([10], pg. 473)

Caminhando nesse sentido, a BNCC [10] além de sugerir o uso de planilhas, calculadoras e outras tecnologias da informação no currículo de matemática, também se preocupa com os impactos de tecnologias disruptivas. Sugere assim que o ensino de matemática deve se preocupar em desenvolver habilidades que considerem o pensamento computacional, a importância de codificar, armazenar e proteger a informação, assim como considerar e refletir sobre os impactos da revolução digital na sociedade. Nessa direção, considera-se o uso de calculadoras na sequência didática tanto como forma de se usar recursos tecnológicos, indo ao encontro do que propõe a BNCC e também o artigo "Concepções de futuros professores sobre o uso de calculadoras nos anos iniciais do Ensino Fundamental" [11], enquanto como forma de dar mais dinamismo às aulas.

Apesar de se referir aos anos iniciais do EF, acredita-se que as considerações e observações feitas neste estudo [11] são úteis também para estudantes do 6° ano dessa etapa. Especialmente porque "Para que uma calculadora encontre o resultado correto é

necessário ser manipulada pelo ser humano havendo um raciocínio antecipado ([11], 2017, pg. 2).” Ou seja, o raciocínio não é desconsiderado quando se usa a calculadora de maneira planejada e orientada, pelo contrário. Convergindo ao que propõem Gitriana et al [12], o uso dessa ferramenta pode potencializar o ensino e aprendizagem de matemática.

> Sabemos que com o uso da máquina de calcular, diminui-se o volume de cálculos rotineiros e vagarosos que os alunos precisam realizar, liberando desta forma mais tempo para raciocinar. ([12], pg. 2)

Portanto, como a sequência didática é uma proposta para se introduzir e desenvolver a noção de primalidade, pode ser vantajoso destinar menos tempo para operações e mais tempo para se pensar nas propriedades e estratégias envolvidas.

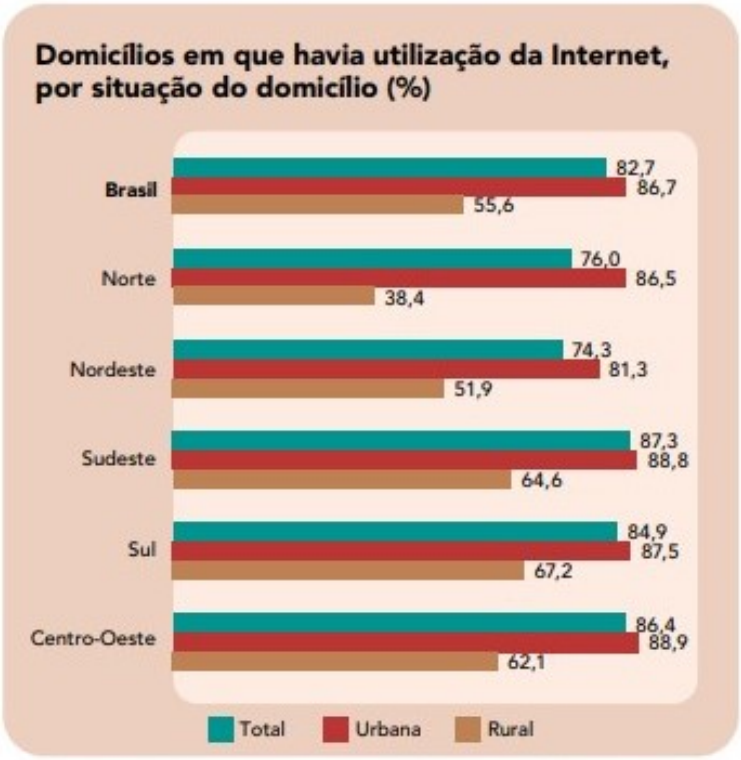
Por fim, reiteramos que ao nosso ver, apesar de indicarmos o 6° do EF como público-alvo da sequência e destacarmos habilidades que podem ser trabalhadas de acordo com a BNCC, isso não impede de o assunto ser tratado em anos distintos e de serem exploradas outras habilidades. Como sempre, preparar, modificar ou até mesmo retomar alguma atividade depende das percepções do docente e outros fatores que julgar relevantes dentro do seu contexto de atuação.

7.2 Contextualizando

Objetivando servir como fonte para composição de aulas que contextualizem a Criptografia, compomos esta seção na qual vamos exemplificar, através de duas situações muito comuns no cotidiano da maioria das pessoas, como e onde podemos encontrar a criptografia. Inicialmente, percebamos através da Figura 7.1 o considerável volume de brasileiros que possuíam internet em seus domicílios no ano de 2021, e que potencialmente, mesmo que de modo indireto e à primeira vista imperceptível, utilizam a Criptografia no seu cotidiano, o que pode ser uma justificativa razoável para sua abordagem na Educação Básica.

Agora, vamos a dois contextos possivelmente próximos a muitos estudantes onde a Criptografia age, mesmo que possivelmente imperceptível a maioria, como afirmamos. O primeiro são as compras de modo remoto. Comprar sem sair de casa tornou-se mais comum nos últimos anos, intensificado pela pandemia de COVID-19. Boa parte dessas compras acontecem através de sites de *e-commerce*, ou seja, sites que possibilitam a compra de variados produtos sem a necessidade de ir a uma loja física. Há, para isso,

Figura 7.1: Uso e acesso à internet no Brasil em 2021.



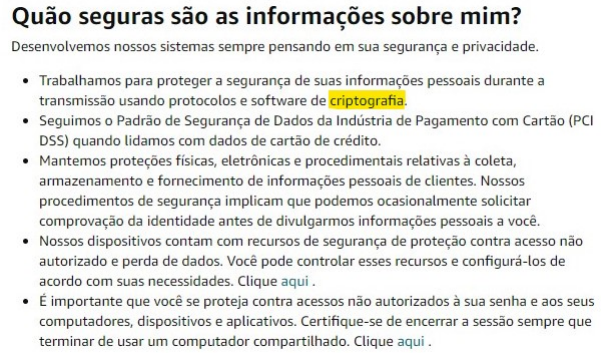
Fonte: IBGE. Disponível em https://biblioteca.ibge.gov.br/visualizacao/livros/liv101794_informativo.pdf, acessado em 25 de novembro de 2021.

coleta de variadas informações de seus clientes, desde CPF, número de telefone e endereço, até número do cartão de crédito, e portanto precisam dificultar que terceiros tenham acesso a esses dados. E é neste monto onde a Criptografia faz seu papel, protegendo essas informações. A Figura 7.2 extrai um trecho de perguntas e respostas de um famoso site de compras sobre como se dá a proteção de informações de seus clientes.

Um segundo contexto, talvez mais tangível ao dia-a-dia de jovens, é o uso de aplicativos de mensagem, tão popularizados nos últimos anos por todo o mundo. Todo tipo de conversa trafega por estes canais, tanto conversas pessoais quanto comerciais, e assim também carecem de proteção, a fim de se assegurar a privacidade dos usuários desses aplicativos. E, novamente, tal proteção é feita também usando-se variados modelos de criptografia, como o RSA. As figuras 7.3 e 7.4 foram retiradas de seções de informações aos usuários de dois aplicativos de mensagens muito utilizados por todo o mundo sobre como a proteção de mensagens é feita.

Percebamos assim, com os dois exemplos anteriormente descritos, que mesmo em ações ordinárias cotidianas a Criptografia se faz presente. As informações que as empresas

Figura 7.2: Empresas de *e-commerce* utilizam criptografia para ajudar na proteção dos dados dos clientes.



Quão seguras são as informações sobre mim?

Desenvolvemos nossos sistemas sempre pensando em sua segurança e privacidade.

- Trabalhamos para proteger a segurança de suas informações pessoais durante a transmissão usando protocolos e software de criptografia.
- Seguimos o Padrão de Segurança de Dados da Indústria de Pagamento com Cartão (PCI DSS) quando lidamos com dados de cartão de crédito.
- Mantemos proteções físicas, eletrônicas e procedimentais relativas à coleta, armazenamento e fornecimento de informações pessoais de clientes. Nossos procedimentos de segurança implicam que podemos ocasionalmente solicitar comprovação da identidade antes de divulgarmos informações pessoais a você.
- Nossos dispositivos contam com recursos de segurança de proteção contra acesso não autorizado e perda de dados. Você pode controlar esses recursos e configurá-los de acordo com suas necessidades. Clique aqui .
- É importante que você se proteja contra acessos não autorizados à sua senha e aos seus computadores, dispositivos e aplicativos. Certifique-se de encerrar a sessão sempre que terminar de usar um computador compartilhado. Clique aqui .

Fonte: Amazon. Disponível em https://www.amazon.com.br/gp/help/customer/display.html?nodeId=201909010, acessado em 25 de novembro de 2021

Figura 7.3: A criptografia presente também no *Whatsapp*.

WhatsApp WHATSAPP WEB RECURSOS DOWNLOAD SEGURANÇA CENTRAL DE AJUDA PT (BR)

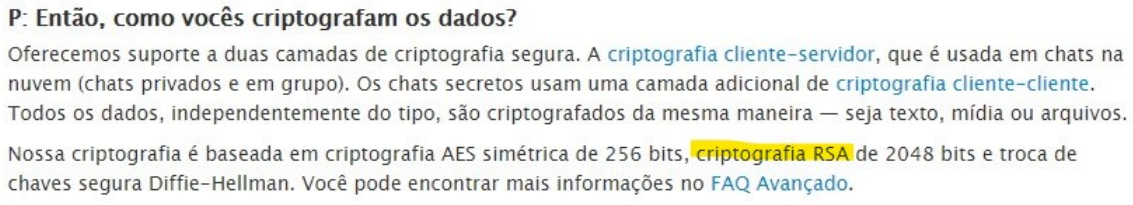
Conversas pessoais

A criptografia de ponta a ponta do WhatsApp protege suas mensagens e chamadas no WhatsApp Messenger, garantindo que elas fiquem somente entre você e a pessoa com quem você está conversando. Ninguém mais pode ler ou ouvi-las, nem mesmo o WhatsApp. Essas mensagens são protegidas com um cadeado exclusivo, e somente você e seus destinatários têm acesso à chave especial para destrancá-lo e ler as mensagens. Todo esse processo acontece automaticamente: não é necessário ativar configurações ou criar conversas secretas especiais para garantir a segurança de suas mensagens.

Fonte: Whatsapp. Disponível em https://www.whatsapp.com/security, acessado em 25 de novembro de 2021

fornecem aos sues clientes sobre como a proteção é feita, presentes nas imagens desta seção, nos dão a pista da importância da Criptografia e podem ser um ponto de partida para que o professor dialogue com seus estudantes, conectando a matemática ao dia-a-dia.

Figura 7.4: O aplicativo de mensagens *Telegram* utiliza o RSA como uma de suas formas de encriptação.



P: Então, como vocês criptografam os dados?

Oferecemos suporte a duas camadas de criptografia segura. A criptografia cliente-servidor, que é usada em chats na nuvem (chats privados e em grupo). Os chats secretos usam uma camada adicional de criptografia cliente-cliente. Todos os dados, independentemente do tipo, são criptografados da mesma maneira — seja texto, mídia ou arquivos.

Nossa criptografia é baseada em criptografia AES simétrica de 256 bits, criptografia RSA de 2048 bits e troca de chaves segura Diffie-Hellman. Você pode encontrar mais informações no FAQ Avançado.

Fonte: Telegram. Disponível em https://telegram.org/faq#p-entao-como-voces-criptografam-os-dados

7.3 Aula Jogo dos Divisores

Pré-requisito: Esta aula tem o objetivo de retomar conceitos de múltiplos e divisores estudados nos anos iniciais do Ensino Fundamental. Apesar disso, o professor pode explicar brevemente tais conceitos antes de os alunos iniciarem o jogo proposto, caso julgue necessário.

Público alvo: 6° ano do Ensino Fundamental.

Recursos: Dados comuns, quadro, pincel e impressões.

Tempo: Uma aula de 50 minutos

Habilidades:

(EF06MA03) Resolver e elaborar problemas que envolvam cálculos (mentais ou escritos, exatos ou aproximados) com números naturais, por meio de estratégias variadas, com compreensão dos processos neles envolvidos com e sem uso de calculadora.

(EF06MA05) Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10, 100 e 1000. (EF06MA06) Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor.

Roteiro:

Orientações aos professores. Esta aula tem como objetivos principais retomar conceitos de múltiplos e divisores através de um jogo. As regras, que serão listadas mais abaixo podem ser alteradas pelo professor para adaptar às suas turmas

- As regras podem ser lidas pelo professor ou distribuídas para os alunos.

- A pontuação pode ser marcada com tampinhas, por exemplo.
- Após finalizar todas as rodadas de um jogo, a ideia é que se repita, pois assim os alunos podem se apropriar melhor das regras e das estratégias.
- O jogo pode ser jogado com dupla contra dupla.
- Regras do jogo
    1. Cada dupla joga o dado duas vezes com o intuito de se formar um número.
    2. O primeiro resultado será a unidade do número a ser formado e o segundo resultado do lançamento do dado será a dezena desse número.
    3. A dupla deverá anotar o número formado e um divisor desse número. Caso acertar ele ganha um ponto, caso errar ou não souber, ele perde.
    4. Então será a vez de outro aluno do grupo, que jogará o dado duas vezes a fim de se formar outro número.
    5. Caso se encontre o mesmo número, os divisores não podem se repetir. Se todos os divisores do número encontrado já tiverem sido listados, a dupla perde a vez.
    6. Ganha quem fizer mais pontos em cinco rodadas.

Orientações aos estudantes .

1. Forme grupos de dois a quatro estudantes.
2. Prepare uma folha comum para o grupo.
3. Tire com seu professor dúvidas sobre as regras.
4. Defina quem vai começar o jogo arremessando o dado. O maior número começa e assim sucessivamente.

Exemplo

A Dupla A vai iniciar o jogo, enfrentando a Dupla B

A primeira jogada tem como resultado o número 4, e a segunda, o número 3, formando-se o número 34.

A Dupla A anota o número 34 e anota também um divisor desse número, por exemplo o número 2

A Dupla B verifica que 34 é divisível por 2, pontuando a Dupla A

Agora tudo se repete, invertendo-se os papéis das duplas

Caso o natural 34 se repita durante as jogadas, não serão aceitos os mesmos divisores dele como resposta. Caso já estejam esgotados, a dupla em questão deve arremessar novamente o dado. Este pode ser um momento oportuno para a intervenção do professor, ajudando os alunos a verificarem quando todos os divisores de um dado número estão realmente listados.

7.4 Usando Calculadora para Determinar Primalidade

Pré-requisito: Compreender os conceitos de múltiplos e divisores e operações básicas.

Público alvo: 6º ano do Ensino Fundamental

Recursos: Aula expositiva, atividade escrita, calculadoras ou computadores

Tempo: Uma aula de 50 minutos

Habilidades: (EF06MA04) Construir algoritmo em linguagem natural e representá-lo por fluxograma que indique a resolução de um problema simples (por exemplo, se um número natural qualquer é par).

(EF06MA03) Resolver e elaborar problemas que envolvam cálculos (mentais ou escritos, exatos ou aproximados) com números naturais, por meio de estratégias variadas, com compreensão dos processos neles envolvidos com e sem uso de calculadora.

Roteiro:

Orientação aos professores. Esta aula tem como objetivo trabalhar a primalidade com os estudantes. Para isto, divididos em grupos os alunos devem montar estratégias para definir se um número n é primo ou composto.

- Preparar antecipadamente calculadoras, que podem ser dos *smartphones* dos estudantes.
- Explicar de forma breve o que significa um número ser primo com a definição e exemplos.

- Orientá-los a descrever os passos para facilitar o procedimento. Por exemplo, o Grupo A listado acima pode descrever o procedimento da seguinte forma:
  1. Anotar o número n.
  2. Dividi-lo por todos os números menores que ele, começando por 2 até obter uma divisão exata ou até chegar em seu antecessor.
  3. Informar se n é primo ou não.

Orientação aos alunos. Em grupos, vamos elaborar uma maneira de se verificar quando um número é primo!

- Formem grupos de 2 a 4 alunos.
- Cada grupo deverá montar uma estratégia para verificar se um dado número é primo ou composto.
- Vocês podem usar calculadora!
- Depois de montada a estratégia, divida-a em passos.
- Verifique se cada um dos seguintes naturais é primo ou não através da estratégia criada usando o passo-a-passo.

a 97	**e** 667	**i** 2297
b 117	**f** 673	**j** 3047
c 133	**g** 887	**k** 3307
d 323	**h** 1799	**l** 3803

Exemplo

O Grupo A define como estratégia inicial dividir n por cada natural menor ou igual a n

O grupo, então, vai verificar se o natural 97 é ou não primo

Supondo que o grupo é composto por 4 integrantes e que cada um dispõe de calculadora, o professor pode sugerir que gerenciem a tarefa de fazer as divisões da seguinte forma: o Integrante 1 verifica os números de 1 a 24; o Integrante 2, de 25 a 48; o Integrante 3, de 49 a 72; e o Integrante 4, de 73 a 97

O professor pode instigá-los a pensar se é a estratégia pode ser melhorada, perguntando, por exemplo, se é necessário dividir por 1 ou 97

O Grupo B define como estratégia listar até o primeiro número primo maior ou igual ao natural que se deseja verificar a primalidade

7.5 Um modelo simplificado de encriptação

Pré-requisito: Conceitos de múltiplo e divisores, operações básicas e conceitos de primalidade.

Público alvo: 6º ano do Ensino Fundamental

Recursos: Calculadoras, *smartphones* e internet .

Tempo: Duas aulas de 50 minutos cada

Habilidades:

(EF06MA03) Resolver e elaborar problemas que envolvam cálculos (mentais ou escritos, exatos ou aproximados) com números naturais, por meio de estratégias variadas, com compreensão dos processos neles envolvidos com e sem uso de calculadora. (EF06MA04) Construir algoritmo em linguagem natural e representá-lo por fluxograma que indique a resolução de um problema simples (por exemplo, se um número natural qualquer é par). (EF06MA05) Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10, 100 e 1000. (EF06MA06) Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor

Roteiro:

Orientação aos professores. Esta dinâmica de grupos propõe um ambiente competitivo e saudável para que os estudantes ao mesmo tempo reforcem os conceitos de divisor e primalidade e relacionem essas noções básicas com a criptografia.

Depois os alunos construirão suas chaves, como descrito a seguir, já sabendo da dinâmica porvir.

Ainda na primeira aula, o professor deve introduzir o Modelo Simplificado de Encriptação, que será descrito a seguir.

A segunda aula é destinada à dinâmica.

- Num primeiro momento o professor pede aos alunos, já em grupos, para que verifiquem como aplicativos de compra e de conversa como o *Whatsapp* protegem os dados dos usuários. A ideia é que o termo "criptografia" apareça naturalmente nas pesquisas, vide figuras 7.2, 7.3 e 7.4. Entretanto, caso não apareçam, o professor deve estar preparado para ou instruir os alunos ou mostrar em slides figuras semelhantes.
- O professor deve, depois do tempo destinado à pesquisa, introduzir o modelo simplificado de criptografia.
- O modelo simplificado de encriptação consiste no seguinte: cada grupo de alunos protege suas chaves privadas, que são números primos, através de um número m formado pelo produto de dois primos. Se alguém descobrir quais são os dois primos, ou seja, se alguém fatorar m, então o código foi quebrado. Quem quebra o código ganha pontos
- Os alunos serão divididos em grupos de modo que utilizem da estratégia para verificação da primalidade montada na aula anterior em um modelo de encriptação simplificado. Então pode ser mais interessante manter os mesmos grupos.
- Para isso, cada grupo de estudantes terá de escolher quatro números primos e a partir deles fazer até seis produtos possíveis que formarão suas chaves públicas.
- Os grupos receberão, na aula seguinte, uma lista com as chaves públicas dos outros grupos com o objetivo de fatorá-las através da estratégia montada.
- Pode ser interessante que o professor mostre um exemplo para a construção de chaves.

Orientação aos estudantes. Aula 1.

1. Pesquise em aplicativos de compra e de mensagem como eles protegem os dados de seus usuários.
2. Vamos usar a estratégia da aula passada para descobrir quatro números primos. Cada número primo escolhido será sua CHAVE PRIVADA. NUNCA mostre estes números aos integrantes dos outros grupos!

3. Duas CHAVES PRIVADAS formam uma CHAVE PÚBLICA! Basta multiplicar! Para explicar melhor, as CHAVES PÚBLICAS serão feitas da seguinte forma: separe os quatro números primos em pares e multiplique cada par. Essas serão suas CHAVES PÚBLICAS. Quantas chaves vocês montaram?

Tabela 7.1: Exemplo de chaves.

CHAVE PRIVADA	CHAVE PRIVADA	CHAVE PÚBLICA	
2	3	2×3	6
2	5	2×5	10
2	7	2×7	14
3	5	3×5	15
3	7	3×7	21
5	7	5×7	35

Fonte: criada pelos autores.

4. Escreva as CHAVES PÚBLICAS em uma folha. Não se esqueçam de escrever o nome do grupo e de seus integrantes.

Orientação aos estudantes. Aula 2.

1. Cada um dos grupos montou suas CHAVES PÚBLICAS através da multiplicação de duas CHAVES PRIVADAS, certo? Na aula de hoje o objetivo é descobrir o máximo de CHAVES PRIVADAS DOS OUTROS GRUPOS.
2. Para isso cada grupo receberá uma lista com todas as chaves públicas de todos os outros grupos.
3. Usando **calculadora** e a **estratégia** elaborada pelo grupo na aula 7.4, vocês devem tentar descobrir quais são as CHAVES PRIVADAS de cada grupo. Quanto mais chaves descobrir, maior a pontuação!
4. Boa sorte, espiões!

8 Uma proposta para a construção de atividades para o EM

Neste capítulo, propomos planos de aulas que têm como foco desenvolver habilidades matemáticas correlacionadas à teoria de encriptação que aqui exploramos, o RSA, voltadas para a última etapa do Ensino Básico. As atividades surgiram como uma proposta de se extrapolar a aritmética básica ensinada e aprendida até o terceiro ano do Ensino Médio. Ou seja, trata-se de abordagens extras, destinadas especialmente a discentes que visam ampliar os conhecimentos matemáticos. Convergindo ao que se propõe no capítulo 7, lança-se mão de planilhas como ferramentas tecnológicas para ensinar e aprender matemática.

As duas primeiras aulas propostas formam uma sequência com o objetivo de explorar propriedades da aritmética modular sem, num primeiro momento, se ater a formalismos. Na Aula 8.1 objetiva-se explorar as propriedades de potências que deixam o mesmo resto na divisão euclidiana por outro inteiro e na aula seguinte, 8.2, continuar explorando tais propriedades porém através de planilhas e de seus recursos.

Adaptações de acordo com as especifidades de cada turma são encorajadas, e isso dá ao nosso planejamento mais um caráter de guia do que o de um plano de aulas: tratam-se mais de ideias que podem ser adotadas para o planejamento docente do que planos de aulas acabados.

8.1 Simplificando Restos de Potências

Pré-requisito: Propriedades básicas de potenciação e da divisão euclidiana

Público alvo: Alunos do Ensino Médio.

Recursos: Exposição e conteúdo no quadro e resolução de atividades no caderno

Tempo: Uma aula de 50 minutos

Roteiro:

Orientações ao professor: Esta aula é destinada a extrapolar as propriedades básicas

de álgebra usualmente estudadas no Ensino Básico.

- Divida a turma em grupos.
- Os exercícios têm o propósito de sugerir aos estudantes a percepção de um padrão nos restos das potências.

Orientação aos alunos: Façam as seguintes atividades em duplas.

1. Calcule os restos das divisões abaixo, exibindo as operações envolvidas.
   (a) O resto da divisão de 7 por 6
   (b) O resto da divisão de 7^2 por 6;
   (c) O resto da divisão de 7^3 por 6;
   (d) O resto da divisão de 7^4 por 6;
   (e) O resto da divisão de 7^5 por 6;
   (f) O resto da divisão de 5 por 3;
   (g) O resto da divisão de 5^2 por 3;
   (h) O resto da divisão de 5^3 por 3;
   (i) O resto da divisão de 5^4 por 3;
   (j) O resto da divisão de 5^5 por 3;
   (k) O resto da divisão de 9 por 7;
   (l) O resto da divisão de 9^2 por 7;
   (m) O resto da divisão de 9^3 por 7;
   (n) O resto da divisão de 9^4 por 7;
   (o) O resto da divisão de 9^5 por 7;
2. Calcule os restos das divisões abaixo também justificando a resposta.
   (a) O resto da divisão de 7^{900} por 6;
   (b) O resto da divisão de $7^{5.000}$ por 6;
   (c) O resto da divisão de $7^{10.051}$ por 6;
   (d) O resto da divisão de 5^8 por 5;
   (e) O resto da divisão de 5^{201} por 5;
   (f) O resto da divisão de 5^{400} por 5;

(g) O resto da divisão de $5^{2.201}$ por 5;

(h) O resto da divisão de 9^{50} por 7;

(i) O resto da divisão de 9^{100} por 7;

(j) O resto da divisão de 9^{501} por 7;

3. **DESAFIOS** Você conseguiu notar algum padrão nas respostas anteriores? Tente notar esse padrão e perceba o quanto ele pode ser útil para se fazer os seguintes cálculos.

(a) O resto da divisão de 13^{50} por 10;

(b) O resto da divisão de 23^{35} por 6;

(c) O resto da divisão de $76^{10.000}$ por 5;

(d) O resto da divisão de $19^{20.000}$ por 17;

Observações:

Entre os conceitos desta aula está o fato de que, para se calcular o resto r da divisão de a^n por m pode-se primeiramente calcular os restos r_1, r_2, $\cdots$, r_k respectivamente das potências menores a^{n_1}, a^{n_2}, $\cdots$, a^{n_k} na divisão por m, onde cada n_i é natural e $n_1 + n_2 + \cdots + n_k = n$, e depois calcular o resto de $r_1 \cdot r_2 \cdot \cdots \cdot r_k$ na divisão por m. Isso decorre do teorema 9.1, exibido no capítulo 9.

Entretanto, uma forma de demonstrar o teorema ou dar indicações de como fazê-lo, com uma linguagem mais simplificada e mais acessível a estudantes do Ensino Médio pode se dar como se segue.

Teorema 8.1: Se a e b são naturais e $a = bq + r$ a divisão euclidiana de a por b, então o resto de a^2 da divisão por b é o resto de r^2 na divisão por b.

Demonstração. De $a^2 = (bq + r)^2$ temos

$$a^2 = \underbrace{b(q^2 + 2qr)}_{\text{Múltiplo de b}} + r^2$$

e assim para se determinar o resto de a^2 por b basta verificar o resto de r^2 por b. □

O teorema anterior mostra apenas um caso particular. Uma generalização usando binômio de Newton pode ser como se segue.

Teorema 8.2: Se a e b são naturais e $a = bq + r$ a divisão euclidiana de a por b, então o resto de a^n por b é o resto de r^n na divisão euclidiana por b.

Demonstração. Aplicamndo o binômio de Newton para $a^n = (bq + r)^n$ temos que

$$a^n = \sum_{i=0}^{n} \binom{n}{i} (bq)^{n-i} r^i = t_0 + t_1 + \cdots + t_n$$

onde em todas as parcelas t_i há um múltiplo de b exceto em t_n que é igual a r^n. Portanto, para algum $T \in \mathbb{N}$,

$$a^n = Tb + r^n$$

e assim determinar o resto de a^n por b é equivalente a determinar o resto de r^n por b. □

Importante notar que, caso a potência seja muito alta, e muito alta aqui pode ser relativo[1], o último teorema pode ser usado várias vezes através de um rearranjo do expoente. Vejamos um exemplo, calculando o item d dos desafios, ou seja, o resto da divisão de $19^{20.000}$ por 17.

Primeiro notemos que $19 = 1 \times 17 + 2$, assim o resto procurado será o mesmo de $2^{20.000}$ por 17 segundo o teorema 8.2. Considerando que a potência é muito alta, podemos fazer

$$2^{20.000} = (2^{10})^{2.000} = 1.024^{2.000}.$$

Como $1.024 = 60 \times 17 + 4$ podemos aplicar novamente o teorema para concluir que o resto procurado é o mesmo de $4^{2.000}$ por 17. Ainda é uma potência alta! Rearranjando, aplicando o teorema de novo e usando que $4^5 = 1.024$, concluímos que as potências $4^{2.000}$, 4^{400}, 4^{80}, 4^{16} e $4^4 = 256$ deixam o mesmo resto na divisão euclidiana por 17. O resto desta última pode ser facilmente calculado, pois $256 = 15 \times 17 + 1$. Então o resto de $19^{20.000}$ na divisão euclidiana por 17 é 1.

Há várias escolhas possíveis para se fazer a iteração mostrada acima, e nossa escolha foi longe de ser ideal. Caso usássemos que os restos de 19^8 e 2^8 na divisão em questão são iguais, foi notado que

$$2^8 = 256 = 15 \times 17 + 1$$

[1]Para mais detalhes sobre quantidade de algarismos de uma potência veja o capítulo 9

o que facilitaria muito os cálculos.

Os teoremas 8.2 e 8.1 mostram possibilidades de se ensaiar uma generalização ou de fato de se generalizar a propriedade em questão, ou seja o cálculo facilitado do resto na divisão euclidiana onde o dividendo é uma potência, com habilidades matemáticas exploráveis na educação básica. Claro que, a depender da turma e das percepções de cada professor, a formalização pode não ser viável ou tampouco necessária. O que pode ser de fato interessante e talvez necessário como uma sequência da aula 8.1 é considerar um ambiente onde haja socialização das respostas e dúvidas dos estudantes, compartilhando ideias.

8.2 Planilhas e Restos de Potências

Pré-requisito: Pode ser uma continuação da aula 8.1. **Público alvo**: Estudantes do Ensino Médio

Recursos: Atividade escrita e computadores

Tempo: Uma aula de 50 minutos

Roteiro para o professor :

- Divida a turma em duplas de modo que cada dupla use um computador.
- Disponibilize folhas de rascunho para cada dupla.
- Distribua a atividade:

Atividade:

1. Exercício 1: calcule as potências a seguir usando ora o operador circunflexo ora a função POTÊNCIA.

a	5^7	b	12^{13}	c	81^4	d	96^4	e	77^5
f	101^4	g	2^{14}	h	22^7	i	6^{19}	j	69^7

2. Exercício 2: calcule os restos das divisões a seguir usando a função MOD.

a	$16.685 \div 140$	b	$206.111 \div 63$
c	$999.999.999 \div 9.999$	d	$999.999.999 \div 999$
e	$1.111.693 \div 77$	f	$169.895.696.666 \div 4.598$
g	$66.593.654.001 \div 15.986.696$	h	$966.593.654.991 \div 8.888$
i	$777.999.888.666 \div 222$	j	$99.652.099.000 \div 222$

3. Exercício 3: calcule os restos das divisões a seguir usando a função MOD sem necessariamente calcular as potências antes. Ou seja, você pode usar o operador circunflexo em um dos argumentos da função MOD.

   a $2^{16} \div 36$ b $11^{10} \div 60$ c $16^5 \div 31 \div 9.999$
   d $99^7 \div 50.698$ e $1.069^4 \div 77$ f $136^6 \div 8.888$

4. Exercício 4: calcule os restos das divisões a seguir usando a função MOD usando propriedades de potência.

   a $2^{101} \div 36$ b $11^{50} \div 60$ c $16^{37} \div 31 \div 9.999$
   d $99^{20} \div 50.698$ e $1.069^{10} \div 77$ f $136^{15} \div 8.888$

Observações:

Esta aula pode ser uma sequência dos estudos iniciados na aula 8.1, de modo a usar outras mídias para os cálculos além do lápis e papel. Escolhemos planilhas eletrônicas, mas o professor que julgar conveniente lançar mão de outros *softwares*, especialmente de cálculo algébrico, pode notar que em linhas gerais o raciocínio e a estratégia usados são os mesmos.

Isso porque há interesse aqui em explorar a memória dessas ferramentas, ou seja, a capacidade de armazenar informação enquanto se efetua outros cálculos. Entretanto há também a possibilidade de se explorar os limites que elas possuem, estimulando os estudantes a notarem que há um limite de precisão para se exibir um número em algum *software*, como nas planilhas, de modo que o teorema 9.1 se torna bem útil.

Pode ser mais produtivo se os discentes já tiverem um contato ao menos breve com planilhas, mas basicamente exploramos as operações potenciação e a função MOD.

Para se usar a potenciação, sugerimos o uso do operador circunflexo. Por exemplo, efetuar 5^2 inserimos em uma célula da planilha =5 ^ 2 ou +5 ^ 2. Já a função MOD fornece o resto da divisão euclidiana de um dado divisor a por um dado dividendo d. Assim, para se usá-la, digite em uma célula =MOD(a;b). Por exemplo, digitando-se =MOD(17;5) o resultado é 2. Perceba que o caractere ";" separa os argumentos da função MOD, no caso o dividendo e o divisor. Em geral, esse caractere tem a função de separar argumentos das variadas funções que uma planilha oferece.

Outras informações úteis podem ser encontradas no capítulo 9, o qual mostra em sua primeira seção uma maneira de se verificar quantos dígitos tem uma dada potência

na base decimal, o que pode ser um facilitador no planejamento de atividades, e na seção 9.4, exemplos de dois dos exercícios sugeridos nesta aula, feitos na planilha de cálculo. Há, neste mesmo capítulo, sugestões e resultados que podem ser interessantes para se compor atividades para esta aula e a aula 8.1.

9 Tópicos sobre as atividades do Ensino Médio

No presente capítulo mostraremos resultados interessantes e que podem ser particularmente úteis na composição das atividades apresentadas no Capítulo 8, quase todos derivados das propriedades do anel comutativo Z_m.

Apresentamos primeiro um resultado que facilita o cálculo de restos de potência sem precisar calcular diretamente as potenciações, sendo especialmente útil com potências muito grandes. Dando continuidade, é importante saber qual a precisão do *software* que o professor pode usar ou usa em suas aulas para saber se o resultado de uma operação está aproximado ou exato, o que pode ser feito através de testes. Assim, exibimos um modo de se calcular quantos dígitos tem uma potência na base decimal.

Também é apresentada uma maneira de se compor as atividades apresentadas no capítulo 8, ou seja, de determinação de restos de potências, discutindo-se sobre possíveis limitações e sobre quando o roteiro sugerido funciona.

Por fim, algumas atividades são resolvidas utilizando-se as técnicas discutidas.

9.1 Simplificando potências

Sem muitos detalhes técnicos e de uma maneira direta e simples, há sempre um limite para o maior número natural que se pode usar para executar cálculos e demais manipulações em planilhas eletrônicas e outros programas sem aproximações que causam erros. Em planilhas de cálculo de computadores pessoais é comum termos uma precisão de dezesseis dígitos na base decimal.

Por exemplo, na planilha utilizada para os cálculos e aulas aqui feitos, temos 9.007.199.254.740.990 como resultado de 2^{53}, o que é apenas uma aproximação, já que $2^{53} = 9.007.199.254.740.992$. Claro que para certas aplicações pode ser uma excelente aproximação, entretanto, para a criptografia RSA não o é, pois a imprecisão desconfiguraria

a mensagem ou alteraria a assinatura, supondo que 2 pudesse ser um caractere do texto codificado e 53 alguma chave privada, comprometendo o completamente o processo.

Entretanto, fazendo-se o uso de uma propriedade relativamente simples de congruências modulares, exibida no seguinte teorema, é possível resolver este problema.

Teorema 9.1: Seja $a = a_1 \times a_2 \times \cdots \times a_k$, com $k \in \mathbb{N}$ e $a \equiv r \mod (m)$, onde $r \in \mathbb{Z}$ é tal que $0 \leq r < m$. Se $a_i \equiv r_i \mod (m)$ com $0 \leq r_i < m$ para cada i de 1 a k, então $r_1 \times r_2 \times \cdots \times r_k \equiv r \mod (m)$.

Demonstração. Perceba que em $\mathbb{Z}_m$ temos $\overline{a} = \overline{r}$ e portanto

$$\overline{a_1 \times a_2 \times \cdots \times a_k} = \overline{r} \Rightarrow \overline{a_1} \times \overline{a_2} \times \cdots \times \overline{a_k} = \overline{r} \Rightarrow \overline{r_1} \times \overline{r_2} \times \cdots \times \overline{r_k} = \overline{r},$$

o que equivale a $r_1 \times r_2 \times \cdots \times r_k \equiv r \mod (m)$, em linguagem de aritmética modular.

□

A facilidade em certos cálculos no contexto da aritmética modular, e portanto do RSA, é que nos interessamos apenas pelo resto da divisão de potências muito grandes por certos naturais, e não no resultado da potência em si.

Então, como um exemplo, suponha que queiramos determinar o resto r da divisão de 2^{53} por, digamos, $m = 282.151$. O cálculo direto pode ser inviável, dependendo dos recursos que se tem,ou dependendo da precisão dos recursos computacionais disponíveis.

Já que $2^{53} = 2^{45} \times 2^8$, podemos determinar através de algum software os restos de 2^{45} e 2^8 na divisão por m, a saber 184.728 e 256 respectivamente, e aplicar 9.1, obtendo:

$$2^{45} \times 2^8 \equiv r \mod (282.151) \Rightarrow 184.728 \times 256 \equiv r \mod (282.151).$$

Esse cálculo é computacionalmente mais fácil que o inicial[1] para certos *softwares*. Assim, temos que o resto de 184.728×256 na divisão por $m = 282.151$ é 171.151 que é o resto r procurado.

[1]Convidamos o leitor a fazê-los usando, por exemplo, a função MOD em planilhas de cálculo, que determina o resto de uma divisão euclidiana dados o divisor e o dividendo.

Para resumir, o que o resultado desta seção garante é que para qualquer fatoração de um inteiro a o resto de a na divisão euclidiana por um natural m é o produto dos restos dos fatores de a por m, de modo que a escolha dos fatores pode ser feita de modo conveniente a cada caso e ainda pode-se aplicar o teorema várias vezes .

9.2 Determinando a quantidade de algarismos na base decimal

Pensando-se em propor atividades para a educação básica e ajudar na construção de atividades para o EM como feito no Capítulo 8, e também em aplicar o teorema da seção anterior, uma indagação que pode surgir é a de se determinar quantos dígitos na base decimal uma potência a^n possui. Seja então $x_k x_{k-1} \cdots x_1 x_0$ a representação de a^n na base decimal.

Note que assim a^n possui $k+1$ dígitos em tal base e

$$a^n = 10^k x_k + 10^{k-1} x_{k-1} + \cdots + 10^1 x_1 + 10^0 x_0$$

de modo que $10^k < a^n < 10^{k+1}$, quando a^n não é uma potência de 10, e portanto

$$\log_{10} 10^k < \log_{10} a^n < \log_{10} 10^{k+1} \Rightarrow k < n \log_{10} a < k+1.$$

Vamos determinar quantos algarismos na base decimal $95^{1.698}$ possui, ou seja, vamos determinar $k+1$. Temos, pelo exposto anteriormente, que $k < 1.698 \log_{10} 95 < k+1$. Usando um software de computação algébrica, calculadora científica ou mesmo alguma planilha, temos com aproximação de quatro casas decimais, $k < 3358{,}1747 < k+1$, e como k é natural, temos $k+1 = 3.359$, ou seja, tal potência possui 3.359 dígitos no sistema decimal de numeração! Ter esta informação pode ser muito importante antes de manipular tais números no nosso contexto, por exemplo, e até em planejar atividades.

Caso a^n fosse uma potência de 10, então $x_i = 0$ para todo i de 0 até $k-1$, $x_k = 1$ e $n = k$, de modo que a^n possuiria $n+1$ algarismos.

9.3 Compondo exercícios

As aulas 8.1 e 8.2 demandam um acervo de potências do tipo $X^k \equiv y \mod (m)$ e assim podemos pensar em maneiras diferentes de compô-las. Vale frisar que buscamos y natural ou nulo e menor que m, pois estamos interessados no resto da divisão euclidiana de X^k por m.

Um modo simples de fazê-lo pode ser tomando X com um ou dois algarismos e m com três algarismos, de modo que X^k seja maior que m, para que o problema fique mais interessante. Por exemplo, tomando $X = 17$, $k = 6$ e $m = 483$ temos que $17^6 \equiv 127 \mod (483)$.

Agora, usando planilhas, verificamos que 22 deixa resto 1 na divisão por 483, ou seja, $22^6 \equiv 1 \mod (483)$, e considere o resultado que se segue.

Teorema 9.2: Sejam inteiros a, b, c, d e m tais que $a \equiv b \mod (m)$ e $c \equiv d \mod (m)$. Então $ac \equiv bd \mod (m)$.

Demonstração. De acordo com a primeira propriedade do teorema 3.4 temos que

$$a \equiv b \mod (m) \Rightarrow ac \equiv bc \mod (m)$$

e também que

$$c \equiv d \mod (m) \Rightarrow cb \equiv db \mod (m).$$

Assim, pela reflexão e transitividade da congruência módulo m, temos que

$$ac \equiv bd \mod (m).$$

□

Combinando $17^6 \equiv 127 \mod (483)$ e $22^6 \equiv 1 \mod (483)$ através do teorema 9.2, obtemos facilmente mais um resultado, $374^6 \equiv 127 \mod (483)$. Ou seja, elaboramos três exercícios, dispostos a seguir, de modo que o terceiro foi construído a partir dos dois primeiros e é de certa forma mais complexo.

1. Determine o resto de $17^6 \div 483$. Resposta: 127.

2. Determine o resto de $22^6 \div 483$. Resposta: 1.

3. Determine o resto de $374^6 \div 483$. Resposta: 127.

Usando o exemplo anterior como gatilho, vamos sugerir uma maneira de se compor essas potências e abordar problemas interessantes relacionados. Enfatizamos antes que esta composição muito depende de cálculos e testes, de modo a não se tratar na maioria das vezes de problema muito simples, mesmo com o auxílio de ferramentas tais como algum software de computação numérica.

Entretanto, descobrindo-se quando possível uma potência k de X tal que $X^k \equiv 1 \mod (m)$ temos mais possibilidades de elaborar essas atividades. Dizemos quando possível não só pelo dificuldade numérica que potencialmente encontraremos mas também pelo fato de só existir X^k com essa propriedade se X for invertível em $\mathbb{Z}_m$, como mostraremos no teorema mais abaixo.

Os passos para tal composição são apresentadas a seguir, onde consideramos m tal como referido no processo de encriptação RSA, ou seja, como o produto de dois primos distintos, apenas para contextualização.

1. Escolha dois primos distintos p e r e faça $m = p \cdot r$.

2. Escolha dois primos distintos p_1 e p_2 tais que

$$mdc(p_1,m) = mdc(p_2,m) = 1.$$

3. Determine dois expoentes k_1 e k_2 diferentes de 1 tais que

$$p_1^{k_1} \equiv p_2^{k_2} \equiv 1 \mod (m).$$

4. Determine k, múltiplo comum de k_1 e k_2.

5. Calcule y tal que dado um $x \in \mathbb{Z}$ tenhamos

$$x^k \equiv y \mod (m).$$

6. Então teremos que

$$(p_1 \cdot p_2 \cdot x)^k \equiv y \mod (m).$$

O passo 1 trata apenas da escolha de m e no segundo passo, basta que os primos p_1 e p_2 sejam diferentes de p e r para que sejam coprimos com m. É no terceiro passo que há uma interessante questão: quando existirão potências de um natural não trivial iguais a classe $\overline{1}$ em um certo anel comutativo? O teorema a 9.3 dá as condições para a existência dessa propriedade.

Teorema 9.3: Dados m e x inteiros, existe $t \in \mathbb{N}$ tal que $x^t \equiv 1 \mod (m)$ se, e somente se, $mdc(x,m) = 1$.

Demonstração. Vamos iniciar a demonstração considerando como hipóteses que, dados $x \in \mathbb{Z}$ e $m \in \mathbb{Z}$, existe t natural que satisfaz

$$x^t \equiv 1 \mod (m)$$

e concluiremos que x e m são coprimos. Isso é quase imediato, pois podemos escrever a congruência como

$$x \cdot x^{t-1} \equiv 1 \mod (m),$$

seguindo que x e x^{t-1} são inversos em $\mathbb{Z}_m$, e daí segue que $mdc(x,m) = 1$, em concordância com o resultado 3.7.

Agora, suponha que $mdc(x,m) = 1$. Vamos denotar por Φ_m o subconjunto de $\mathbb{Z}_m$ tal que todos elementos de Φ_m são coprimos com m. Então $\#\Phi_m = \phi(m)$, ou seja, Φ_m tem $\phi(m)$ elementos, de acordo com a definição 6.1.

Como já discutido na seção 4.3, o produto de elementos invertíveis é um elemento invertível em uma classe, logo, como x possui inverso em $\mathbb{Z}_m$, x^i também possui, $\forall i \in \mathbb{N}$, de modo que $\overline{x^i} \in \Phi_m$.

Seja $\overline{X}$ o conjunto de classes $\{\overline{x^0}, \overline{x^1}, \overline{x^2}, \cdots\}$, que são, de acordo com a discussão anterior, classes invertíveis em $\mathbb{Z}_m$, ou seja, $\overline{X} \subset \Phi_m$. Então $\overline{X}$ é finito, pois Φ_m o é, de modo que podemos escrever $\overline{X} = \{\overline{x^0}, \overline{x^1}, \overline{x^2}, \cdots, \overline{x^k}\}$ para algum k, onde esses elementos não se repetem.

Isso significa que se tomarmos um natural n tal que $n > k$, temos, para algum i inteiro, $0 \leq i \leq k$, que $\overline{x^n} = \overline{x^i}$. Se $\overline{b}$ é o inverso de $\overline{x}$ no anel em questão,

temos

$$\overline{x^i} \cdot \overline{b^i} = \overline{1}$$

e como consequência, e usando o fato de que $\overline{x^n} = \overline{x^i}$, temos

$$\overline{x^{n-i}} \cdot \overline{x^i} = \overline{x^i} \Rightarrow \overline{x^{n-i}} \cdot \overline{x^i} \cdot \overline{b^i} = \overline{x^i} \cdot \overline{b^i} \Rightarrow \overline{x^{n-i}} = \overline{1}.$$

Fazendo $t = n - i$, $t \in \mathbb{N}$ e escrevendo em linguagem de congruências modulares, obtemos

$$x^t \equiv 1 \mod (m)$$

e concluímos a demonstração.

□

Como consequência qualquer número da forma at, com $a \in \mathbb{N}$ satisfaz

$$x^{at} \equiv 1 \mod (m).$$

Há uma outra maneira de garantir um resultado parecido usando as restrições sobre m.

Teorema 9.4: Seja $m = pr$ onde p e r são primos distintos e seja $x \in \mathbb{Z}$ tal que $mdc(x,m) = 1$. Então $x^{\phi(m)} \equiv 1 \mod (m)$.

Demonstração. Por Fermat, 4.6, temos que $x^{\phi(p)} \equiv 1 \mod (p)$, já que p é primo e assim $\phi(p) = p - 1$ pelo resultado 6.2. Analogamente temos $x^{\phi(r)} \equiv 1 \mod (r)$.

Agora, por 6.4 temos $\phi(m) = \phi(p)\phi(r)$ o que implica em

$$x^{\phi(m)} \equiv 1 \mod (p) \text{ e } x^{\phi(m)} \equiv 1 \mod (r).$$

Então existem c e k inteiros tais que $x^{\phi(m)} = cp+1$ e $x^{\phi(m)} = kr+1$, seguindo que $cp = kr$. Como p e r são coprimos, $p|k$ e podemos escrever

$$x^{\phi(m)} = k'pr + 1 \Rightarrow x^{\phi(m)} = k'm + 1 \Rightarrow x^{\phi(m)} \equiv 1 \mod (m).$$

□

9.4 Algumas sugestões para a resolução de atividades

Vamos propor uma forma de se resolver a letra a da atividade 3 e a letra a da atividade 4, ambas da aula 8.2 além de fazermos observações que podem ser úteis.

Primeiro, note que calculando-se 2^{16} obtemos o valor exato dessa potência enquanto calculando-se 2^{101} na planilha só obteremos uma aproximação, justificando a necessidade de se usar o teorema 9.1.

Assim, sabendo-se que a função MOD calcula o resto da divisão de um dividendo e um divisor dados nesta ordem, podemos primeiro calcular a potência $2^{16} = 65.536$ e fazer em alguma célula da planilha $MOD(65.536; 36)$ ou $MOD(2^{16}; 36)$, obtendo 16, o resto procurado.

Agora, para se determinar o resto de 2^{101} na divisão por 36, podemos usar o resultado anterior e o teorema 9.1 fazendo $2^{101} = (2^{16})^6 \times 2^5$, de modo que os restos das potências menores fornecem $16^6 \times 32$. Podemos aplicar novamente o teorema e calcular $MOD(16^6; 36)$, obtendo 28. Então devemos calcular o resto de $28 \times 32 = 896$ na divisão por 36, logo $MOD(896; 36) = 32$.

É interessante que os discentes percebam a grande utilidade do teorema 9.1, que transforma o trabalho de se calcular o resto de 2^{101}, uma potência que nem uma calculadora comum e nem uma planilha determinam com exatidão, na divisão por 36 pelo cálculo do resto de 896 também na divisão por 36.

Convém destacarmos os passos da atividade $4a$. Vamos escrever $r(a \div b)$ para designar o resto da divisão euclidiana de a por b, de modo a não nos prendermos apenas na aplicação em planilhas.

1. Escrever a potência como produto de potências menores:

$$2^{101} = (2^{16})^6 \times 2^5.$$

2. Estabelecer o resultado do exercício $3a$:

$$r(2^{16} \div 36) = 16.$$

3. Usar o teorema 9.1, notando que

$$r(2^{101} \div 36) = r((2^{16})^6 \times 2^5 \div 36) = r(16^6 \times 32 \div 36).$$

4. Perceber a inconveniência[2] de se calcular com exatidão

$$16^6 \times 32.$$

5. Calcular

$$r(16^6 \div 36) = 28.$$

6. Usar novamente 9.1:

$$r(16^6 \times 32 \div 36) = r(28 \times 32 \div 36) = r(896 \div 36) = 32.$$

7. Concluir, por transitividade, que

$$r(2^{101} \div 36) = 32.$$

[2]Quando se opta em fazê-la manualmente, a operação pode ser muito demorada. Caso se escolha um programa diferente de uma planilha que possa possuir uma precisão menor na representação decimal, por exemplo o caso do *Scilab*, pode-se novamente encontrar um obstáculo. Caso conveniente, pode-se aplicar diretamente 9.1, finalizando a atividade.

10 Conclusão

Como já afirmado em mais de uma ocasião neste texto, os modelos de criptografia, inclusive a Criptografia RSA, desempenham importante papel no nosso moderno modo de viver. Entretanto, mesmo tão presente em tarefas diárias, é possível que a criptografia, sua função e seus processos sejam desconhecidos para muitos, como também já destacamos. Assim, acreditamos que este trabalho cumpre um tímido papel em um complexo filme de muitos personagens: apresenta em linhas gerais a teoria matemática que modela o RSA e propõe abordagens possíveis para professores que ensinam matemática na EB, através de atividades baseadas na matemática que envolve este modelo de encriptação.

Outro importante papel também foi cumprido através deste trabalho na carreira de um professor: estudar matemática aplicada e conseguir contextualizá-la na sua prática docente. Mesmo que ainda não propriamente aplicadas, o processo de criação das atividades no contexto da Criptografia RSA desencadeou diversas reflexões e exigiu variadas leituras e discussões, especialmente sobre ensino e aprendizagem de Matemática na EB. Convém destacar que a não aplicação das atividades criadas se deu majoritariamente como consequência da pandemia de COVID-19, cujos primeiros casos no Brasil foram registrados em fevereiro de 2020, afetando diretamente as práticas escolares neste ano e no ano seguinte. Além de as escolas serem por muitos meses fechadas, mesmo quando as aulas foram retomadas de forma remota não se pôde, em muitos casos, obter um pleno retorno, especialmente porque muitos estudantes careciam de estrutura básica, como computador e internet, para que os processos de ensino e aprendizagem ocorressem.

Assim, além da construção de ideias e de aprendizados na trajetória que culminou neste produto, há também de se considerá-lo com o potencial de direcionar práticas futuras. Pois abre-se caminho para estudos e pesquisas de diversos temas relacionados direta ou indiretamente a este trabalho. Por exemplo, questões mais amplas que já possuem clara preocupação na área de Ensino de Matemática, como os benefícios de se lançar mão de tecnologias nas aulas de matemática, e ainda mais, como se pode fazê-lo almejando uma

aprendizagem que seja significativa. Inclusive já tangenciamos essa questão no Capítulo 7, quando fizemos apontamentos sobre como a BNCC aborda e sugere o uso de recursos tecnológicos e também quando falamos sobre possibilidades do uso de calculadoras.

Considerando novamente a escassez de recursos para que diversos estudantes especialmente da rede pública de ensino obtivessem acesso às aulas de forma remota, outras questões que extrapolam os processos de ensino e aprendizagem em si ganham mais relevo para estudos: qual a importância de um acesso significativo e democrático às tecnologias para a formação cidadã e quais os impactos de sua escassez, em particular para estudantes da rede pública de ensino? Claro que, devido à pandemia de COVID-19, o planejamento pedagógico foi drasticamente afetado, com impactos no calendário escolar, mas a falta de recursos tecnológicos foi sem dúvidas o fator que mais impactos negativos trouxe. Também há de se considerar que mesmo com tais recursos disponíveis, a falta de conhecimento sobre como usá-los pode também comprometer os processos de ensino e aprendizagem. É possível que dados oriundos de pesquisas estatísticas em breve nos mostrem direcionamentos para abordar tais questões.

Somando-se a essas possibilidades, há também um propício cenário para se colocar em prática as aulas aqui propostas. Algumas delas podem justamente compor pesquisas relacionadas ao ensino de matemática através de tecnologias, tais como as aulas 7.4 e 8.2, e a contextualizar uma aplicação matemática com impacto direto nas vidas dos estudantes, através de modelos simplificados do RSA, como é o caso da da aula 7.5, ou de partes dos processos de codificação e decodificação, além de abrirem espaço para discussões sobre tecnologias disruptivas.

Enfim, mais do que ser uma síntese de um processo de aprendizagem que marcou o percurso neste programa de mestrado, esta dissertação criou, através dos diversos processos envolvidos em sua produção, diversas possibilidades futuras para sua continuidade, seja para estudos e pesquisas, seja para a prática pedagógica em sala de aula em si.

Referências

1 CARREIRA, S. Matemática e tecnologias—ao encontro dos "nativos digitais" com os "manipulativos virtuais". *Quadrante*, v. 18, n. 1&2, p. 53–86, 2009.

2 RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, ACM New York, NY, USA, v. 21, n. 2, p. 120–126, 1978.

3 DIFFIE, W.; HELLMAN, M. New directions in cryptography. *IEEE transactions on Information Theory*, IEEE, v. 22, n. 6, p. 644–654, 1976.

4 COUTINHO, S. C. Números inteiros e criptografia rsa. IMPA, 1997.

5 CONSELHO NACIONAL DE JUSTIÇA. Provimento n° 100, DE 26 DE MAIO DE 2020. 2022–02–03. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2020/05-/DJ156_2020-ASSINADO.pdf>. Acesso em: 04 de março de 2022.

6 VOLPI, M. M. Assinatura digital aspectos técnicos, práticos e legais. Axcel Books do Brasil Editora, 2001.

7 COUTINHO, S. C. Primalidade em tempo polinomial: uma introdução ao algoritmo aks. SBM, 2004.

8 CORMEN, T. H. et al. Introduction to algorithms. MIT press, 2009.

9 FARIAS, I. M. S. d. Didática e docência: aprendendo a profissão. Liber livro, 2008.

10 BRASIL. Ministério da Educação. Base nacional comum curricular (bncc). Disponível em: <http://basenacionalcomum.mec.gov.br/a-base>. Acesso em: 04 de março de 2022.

11 CONTI, K. C.; VILELA, M. L.; PINTO, N. K. D. Concepções de futuros professores sobre o uso de calculadoras nos anos iniciais do ensino fundamental. 2017.

12 SANTOS, M. R. dos; ANDRADE, V. L. V. X. d.; GITIRANA, V. A concepção dos licenciandos de matemática sobre o uso de calculadora no ensino fundamental: um estudo exploratório. *VII Encontro Nacional de Educação Matemática - UFPE*, 2004.