Criptografia, Números Primos e Algoritmos

Publicações Matemáticas

Criptografia, Números Primos e Algoritmos

4ª edição

Manoel Lemos
Universidade Federal de Pernambuco

impa

Impresso no Brasil / Printed in Brazil

Capa: Noni Geiger / Sérgio R. Vaz

Publicações Matemáticas

- Introdução à Análise Funcional – César R. de Oliveira
- Introdução à Topologia Diferencial – Elon Lages Lima
- Criptografia, Números Primos e Algoritmos – Manoel Lemos
- Introdução à Economia Dinâmica e Mercados Incompletos – Aloísio Araújo
- Conjuntos de Cantor, Dinâmica e Aritmética – Carlos Gustavo Moreira
- Geometria Hiperbólica – João Lucas Marques Barbosa
- Introdução à Economia Matemática – Aloísio Araújo
- Superfícies Mínimas – Manfredo Perdigão do Carmo
- The Index Formula for Dirac Operators: an Introduction – Levi Lopes de Lima
- Introduction to Symplectic and Hamiltonian Geometry – Ana Cannas da Silva
- Primos de Mersenne (e outros primos muito grandes) – Carlos Gustavo T. A. Moreira e Nicolau Saldanha
- The Contact Process on Graphs – Márcia Salzano
- Canonical Metrics on Compact almost Complex Manifolds – Santiago R. Simanca
- Introduction to Toric Varieties – Jean-Paul Brasselet
- Birational Geometry of Foliations – Marco Brunella
- Introdução à Teoria das Probabilidades – Pedro J. Fernandez
- Teoria dos Corpos – Otto Endler
- Introdução à Dinâmica de Aplicações do Tipo Twist – Clodoaldo G. Ragazzo, Mário J. Dias Carneiro e Salvador Addas Zanata
- Elementos de Estatística Computacional usando Plataformas de Software Livre/Gratuito – Alejandro C. Frery e Francisco Cribari-Neto
- Uma Introdução a Soluções de Viscosidade para Equações de Hamilton-Jacobi – Helena J. Nussenzveig Lopes, Milton C. Lopes Filho
- Elements of Analytic Hypoellipticity – Nicholas Hanges
- Métodos Clássicos em Teoria do Potencial – Augusto Ponce
- Variedades Diferenciáveis – Elon Lages Lima
- O Método do Referencial Móvel – Manfredo do Carmo
- A Student's Guide to Symplectic Spaces, Grassmannians and Maslov Index – Paolo Piccione e Daniel Victor Tausk
- Métodos Topológicos en el Análisis no Lineal – Pablo Amster
- Tópicos em Combinatória Contemporânea – Carlos Gustavo Moreira e Yoshiharu Kohayakawa
- Uma Iniciação aos Sistemas Dinâmicos Estocásticos – Paulo Ruffino
- Compressive Sensing – Adriana Schulz, Eduardo A.B.. da Silva e Luiz Velho
- O Teorema de Poncelet – Marcos Sebastiani
- Cálculo Tensorial – Elon Lages Lima

Distribuição: IMPA E-mail: ddic@impa.br - http://www.impa.br
ISBN: 978-85-244-0043-8

a Adilson e Astréa

Prefácio

No ano de 1989, há precisamente duas décadas, lecionei um curso no 17º Colóquio Brasileiro de Matemática entitulado de **Criptografia, números primos e algoritmos**. As notas de aulas escritas para este curso estão esgotadas. Diante da solicitação feita pelo IMPA para a sua reimpressão, achei interessante as reescrever completamente. Quatro motivos principais me levaram a tormar esta decisão: alguns erros tipográficos presentes nas notas originais; os avanços que ocorreram nestas duas últimas décadas em teoria dos números computacional; a abordagem realizada de forma sucinta na maioria dos tópicos; e a presença de poucos exercícios.

Nos quatro primeiros meses de 1989, as notas de aulas para o curso que lecionei no colóquio em julho do mesmo ano foram escritas. Redigi estas notas em um caderno. Como, naquela época, não utilizava o TEX, não digitei as notas. Quem o fez foi Oscar. Aos erros tipogáficos que cometi ao redigir, Oscar talvez tenha acrescentado mais alguns. Na revisão, não fui capaz de encontrar todos. Para os mais jovens, pode parecer estranho não ter digitado em TEX. Mas a década de 80 foi de transição. Quando fazia o Ensino Fundamental fiz um curso de datilografia. Ganhei dos meus pais uma máquina de escrever Olivetti. Para que a margem esquerda fosse alinhada, necessitava, ao chegar na última palavra, fazer a conta de quantas letras podiam ser digitadas antes do fim da linha para fazer o ajuste. Era um processo muito trabalhoso. A pior parte era jogar fora toda uma página quando um erro era cometido. Símbolos matemáticos nem pensar! Só os disponíveis no teclado. Esta máquina me acompanhou também no Ensino Médio.

Ao ingressar na universidade, não necessitava digitar textos, pois não é comum que trabalhos sejam solicitados nas disciplinas de ciências matemáticas. Não lembro de nenhum. Apenas no mestrado tive de escrever minha dissertação. Digitei a versão preliminar em uma máquina elétrica que podia corrigir os erros. Quando necessário, tive de deixar espaço para escrever à mão as letras gregas e os símbolos matemáticos. A versão final, digitada por Delsa ou Neide, não lembro bem, foi feita em máquina similar. Nestas máquinas, as letras vinham em relevo em uma esfera. Existiam esferas com símbolos matemáticos e letras gregas. Quando era necessário digitar um caracter deste tipo, bastava trocar a esfera. Era muito trabalhoso, mas era um enorme progresso. Na versão final de minha dissertação nada foi escrito a mão. Fui para o doutorado. Ao chegar em Oxford deparei com máquinas de escrever, na sala de café dos estudantes, que possuíam dois teclados: um normal e outro com letras gregas e símbolos matemáticos. Para mudar de teclado, bastava transferir o tambor. Achei que teria dificuldade em redigir meus resultados em uma máquina tão estranha. Logo descobri que o Instituto de Matemática tinha disponibilizado 1 computador pessoal para todos os estudantes de pós-graduação digitarem seus resultados e que estas máquinas tinham sido descartadas. Estávamos no final de 1984. Destaquei o número 1 porque computadores pessoais eram raros nesta época.

Um novo mundo se abriu para mim. Descobri que podia digitar todos os símbolos matemáticos. Bastava escolher em algumas tabelas. A margem esquerda era feita automaticamente. As fórmulas podiam ser centralizadas sem dificuldade. Utilizava o processador de textos conhecido como T3. Ou era T^3? Não lembro bem. Ao chegar de volta no Brasil, passei a utilizar o CHIWRITE. Ambos, quando comparados com o TEX, são bastante rudimentares. Em 1989, ainda não utilizava o TEX. Hoje utilizo uma de suas variantes que é conhecida como LATEX. Estas notas foram digitadas por mim. Qualquer erro tipográfico será de minha inteira responsabilidade. Não terei como terceirizar parte deles.

A maior parte destas notas foi redigida quando lecionava a disciplina Criptografia e Algoritmos aqui na UFPE. Os textos utilizados para ilustrar as aplicações dos diversos sistemas de criptografia abordados tratam de futebol. Quando escritos, o Santa Cruz ainda jogava

na segunda divisão. Neste ano, terminou como lanterna de um dos grupos da quarta. Deixo, como exercício para o leitor, adivinhar em que ano lecionei a disciplina.

Nestas duas últimas décadas, a pesquisa nesta área foi intensa. Destaco dois grandes avanços. O primeiro foi um algoritmo polinomial para fatorar inteiros em um computador quântico. O segundo, a descoberta de um algoritmo polinomial para decidir quando um inteiro é primo. Este algoritmo ficou conhecido como AKS. Portanto, toda a discussão sobre o algoritmo de Lenstra, que foi escrita para o curso do Colóquio, se tornou obsoleta. Abordamos os algoritmos para decidir primalidade no quarto capítulo destas notas. Continuamos apresentando o algoritmo randomizado de Rabin que, apesar de ter mais de 30 anos, ainda é utilizado para encontrar números primos grandes. Discutimos o AKS, mas devido ao espírito destas notas, não o demonstramos. No primeiro e no segundo capítulos abordamos respecitivamente as propriedades dos inteiros e congruências. No quinto e último capítulo fazemos uma pequena discussão sobre livros relacionados.

Por fim faço um pequeno comentário sobre a última reforma em nossa ortografia. A desconsideramos completamente, já que a antiga ainda vale até 2011, isto é, bem depois da próxima Copa. Portanto, palavras como conseqüentemente e seqüência ainda têm o trema nestas notas. Ficaria estranho adotar a nova ortografia sem o novo alfabeto ser utilizado para escrever mensagens. Todos os exemplos foram feitos em um alfabeto sem as letras K, Y e W.

Gostaria de agradecer ao meu colega de departamento, Professor Antonio Carlos Rodrigues Monteiro, por ter lido atentamente estas notas e feito inúmeras sugestões. Por insitência dele, o zero virou um número natural. Na minha abordagem inicial tinha adotado uma possição ambígua, o que pode parecer estranho em matemática. Como alguns autores consideram o zero como natural e outros não, tinha decidido considerar o zero como um natural dependendo da situação. O que, de fato, é estranho. Portanto, descartei esta abordagem informal para esta questão. Gostaria de deixar claro que o Professor Antonio não tem nenhuma resposabilidade sobre qualquer erro que por ventura exista nestas notas. Todos, que imagino formem o conjunto vazio, são de minha inteira responsabilidade. Sobre esta questão, vale a pena aguardar o prefácio da terceira edição destas

notas, caso sejam escritas algum dia.

Em 1989, dediquei as notas de aulas escritas especialmente para o Colóquio ao Professor Adilson Gonçalves e à Professora Astréa Barreto. Ambos foram meus professores na UFPE e, quando estava no doutorado, solicitaram transferência para a UFRJ. A contribuição que deram para a consolidação da matemática brasileira, através de sua atuação profissional consistente ao longos das últimas 4 décadas, foi significativa. Passados 20 anos do Colóquio, entendo que a dedicatória continua muito atual. É pena que não existam tantos professores nas universidades brasileiras com uma atuação tão destacada e positiva quanto a dos dois.

Manoel Lemos
Recife, 20 de setembro de 2009

Conteúdo

Capítulo 1

Inteiros

1.1 Introdução

Neste capítulo, estamos interessados em estudar os seguintes conjuntos de números:

$$\begin{aligned} \mathbb{N} &= \{0, 1, 2, 3, \dots\} \text{ e} \\ \mathbb{Z} &= \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}. \end{aligned}$$

Um número pertencente ao primeiro conjunto é chamado *natural* e ao segundo *inteiro*.

Durante estas notas iremos assumir, como axiomas, algumas propriedades desses conjuntos. Não faremos a construção dos inteiros a partir dos naturais, como é comumente feito em um curso de estruturas algébricas ou lógica. Nem iremos supor apenas um pequeno número de axiomas para os naturais, como os de Peano — a partir destes é possível definir as operações de adição e multiplicação e derivar todas as suas propriedades. Deixamos tal abordagem para um curso de lógica, que se inicia com os axiomas para a teoria dos conjuntos e, a partir destes, definem-se os naturais. Neste caso, o 0 (zero) é um número natural, o que será adotado nestas notas. Como este enfoque para os números naturais e inteiros é bastante demorado, não o consideramos neste curso.

Do parágrafo anterior, destacamos uma passagem: Existem axiomas para a teoria dos conjuntos. Iremos ignorar totalmente este fato. Usaremos livremente as propriedades de conjuntos que nos parecerem naturais. A seguir apresentaremos um paradoxo, proposto por Russell, para ilustrar este ponto. Antes começaremos com um ditado popular: *toda regra possui uma exceção.* Como esta sentença é uma regra, tem de possuir uma exceção, isto é, existe regra sem exceção. Chegamos a uma contradição! Este mesmo fato se manifesta em teoria dos conjuntos. Agora apresentaremos o paradoxo de Russell. Seja S a coleção de todos os conjuntos A tais que $A \notin A$. Portanto, caso S seja um conjunto, $S \in S$ se e somente se $S \notin S$, o que é absurdo! Logo S não pode ser um conjunto. Daí a necessidade de axiomatizar esta teoria.

1.2 Propriedades

Feita estas observações (e advertências) iniciais, passaremos a descrever as propriedades dos números naturais e interios, que serão de dois tipos: aritméticas e de ordem.

1.2.1 Propriedades aritméticas

Seja A um conjunto munido de duas operações binárias: $+$ (adição) e $\cdot$ (multiplicação). Diremos que A é um *anel (comutativo)* quando estas operações possuem as propriedades que descreveremos abaixo.

São comutativas: $a + b = b + a$ e $ab = ba$, para todos $a, b \in A$ (ab é usada, em vez de $a \cdot b$, para denotar o produto de a por b);

São associativas: $a + (b + c) = (a + b) + c$ e $a(bc) = (ab)c$, para todos $a, b, c \in A$;

Possuem elemento neutro: Exixtem elementos 0 (zero) e 1 (um) de A tais que $0 + a = a$ e $1a = a$, para todo $a \in A$.

Existe inverso aditivo: para todo $a \in A$, existe $-a \in A$ tal que $a + (-a) = 0$;

O produto distribui com relação à adição: $a(b + c) = ab + ac$, para todos $a, b, c \in A$.

Por exemplo, podemos mostrar que, em um anel A, o produto de zero por qualquer elemento a de A é igual a zero. De fato, como o zero é o elemento neutro da adição, temos que

$$0 + 0 = 0.$$

Multiplicando esta identidade em ambos os lados por a, obtemos que

$$a(0 + 0) = a0.$$

Como o produto distribui com relação à adição, concluímos que:

$$a0 + a0 = a0.$$

Se adicionarmos o inverso aditivo de a0 a ambos os lados da identidade, temos que:

$$(a0 + a0) + [-(a0)] = a0 + [-(a0)] = 0.$$

Pela associatividade para adição, obtemos que:

$$0 = (a0 + a0) + [-(a0)] = a0 + \{a0 + [-(a0)]\} = a0 + 0$$

e chegamos a conclusão desejada, isto é, $a0 = 0$, pois 0 é o inverso aditivo.

Será que em um anel o zero pode ser igual ao um? Caso isto ocorra, para todo elemento a do anel, temos que

$$a = 1a = 0a = 0.$$

(A primeira igualdade segue porque 1 é o elemento neutro da multiplicação e a última do parágrafo anterior.) Isto é, o anel contém um único elemento que é o zero. Vamos assumir que este não é o caso. Portanto, em qualquer anel, suporemos também que 0 e 1 são distintos. Como exercício, verifique que o inverso aditivo de um elemento é único.

Vamos assumir, ao longo destas notas, que o conjunto dos inteiros, munido das operaçõis habituais de adição e multiplicação, é um anel.

Outros conjuntos possuem operações de adição e multiplicação com estas mesmas propriedades, ou a maioria delas. Por exemplo, as matrizes quadradas de ordem m, com as suas operações de adição e multiplicação usuais, possuem todas estas propriedades exceto comutatividade para o produto, isto quando $m > 1$. Sabemos que existem matrizes X e Y, ambas não nulas, tais que $XY = 0$. Logo iremos assumir que o conjunto dos inteiros possui uma outra propriedade, que é muito importante:

Não existe divisor de zero: se $a, b \in \mathbb{Z}$ e $ab = 0$, então $a = 0$ ou $b = 0$.

Esta propriedade nos permite fazer cancelamento nos inteiros. Suponha que $a, b, c \in \mathbb{Z}$ são tais que $a \neq 0$ e:

$$\begin{aligned} ab &= ac \\ a(b-c) &= 0 \\ b-c &= 0 \\ b &= c. \end{aligned}$$

Observe que a passagem da segunda para a terceira equação se deve a não existência de divisores de zero, pois o produto de a por $b - c$ é igual a 0 e daí $b - c = 0$, pois $a \neq 0$. (Para o leitor, deixamos como exercício listar todas as propriedades que foram utilizadas para obter cada uma destas equações a partir da anterior.)

1.2.2 Propriedades de ordem

Diremos que um anel A é *ordenado* quando existe um subconjunto P de A fechado com realação à soma e ao produto satisfazendo a propriedade da

Tricotomia: para todo $a \in A$, temos que $a = 0$ ou $a \in P$ ou $-a \in P$, sendo estas opções multuamente excludentes.

Diremos que um elemento pertencente ao conjunto P é *positivo* no anel A. Um elemento a de A é dito *negativo* em A quando $-a$ for positivo em em A.

Para a demonstração do próximo lema, necessitamos estabelecer o seguinte:

$$(-1)(-1) = 1. \tag{1.1}$$

Como -1 é o inverso aditivo de 1, por definição, temos que:

$$1 + (-1) = 0.$$

Multiplicando esta identidade em ambos os lados por -1, obtemos que:

$$(-1)[1 + (-1)] = (-1)0.$$

Destibuindo o produto com relação a soma e usando o fato de que o produto de zero por qualquer elemento é zero, concluímos que:

$$(-1)1 + (-1)(-1) = 0.$$

Como um é o elemento neutro da multiplicação, esta identidade equivale a:

$$(-1) + (-1)(-1) = 0.$$

Obtemos (1.1), pois 1 é o inverso aditivo de -1 e o inverso aditivo é único. (Caro leitor, chegue a esta mesma conclusão de outra maneira, isto é, sem usar a unicidade do inverso aditivo.) Agora mostraremos o seguinte:

Lema 1. *Em um anel ordenado A, temos que 1 é positivo.*

Demonstração. Iniciaremos estabelecendo que -1 não é positivo. Argumentaremos por contradição. Suponha que -1 é positivo. Por (1.1), $(-1)(-1) = 1$. Conseqüentemente 1 é positivo, já que o conjunto de elementos positivos é fechado com relação ao produto. Isto é, 1 e -1 são ambos positivos; uma contradição à propriedade da tricotomia. Portanto, -1 não é positivo. Como $1 \neq 0$, temos que 1 ou -1 é positivo. Logo 1 é positivo, pois -1 não é positivo, e o resultado segue. □

Em um anel ordenado A, com conjunto de elementos positivos P, podemos definir uma relação de ordem da seguinte forma: para $a, b \in A$, diremos que $a \geq b$ se somente se $a = b$ ou $a - b \in P$, e que $a > b$ quando $a - b \in P$. Não é difícil verificar que essa relação de ordem tem as propriedades usuais, que deixaremos como exercício para o leitor:

- se $a, b \in A$, então $a > b$ ou $a < b$ ou $a = b$;
- se $a \geq b$ e $b \geq a$, para $a, b \in A$, então $a = b$;
- se $a \geq b$ e $b \geq c$, para $a, b, c \in A$, então $a \geq c$;
- se $a \geq b$, então $a + c \geq b + c$, para $a, b, c \in A$;
- se $a \geq b$ e $c > 0$, então $ac \geq bc$, para $a, b, c \in A$.

(Para as três últimas propriedades, podemos substituir todos os $\geq$ por $>$. Verique também isto.)

Utilizando a propriedade da tricotomia, podemos mostrar que, em um anel ordenado, o produto de um número positivo por um negativo é negativo e que o produto de dois números negativos é positivo. Conclua, a partir desta informação, que este anel não possui divisores de zero. Mostraremos que o produto de dois elementos negativos a e b é positivo. Por definição, $-a$ e $-b$ são positivos. Como o conjunto de números positivos é fechado com relação ao produto, temos que $(-a)(-b)$ é positivo. Contudo:

$$(-a)(-b) = [(-1)a][(-1)b] = [(-1)(-1)]ab = ab.$$

Isto é, o produto de a por b é positivo. (Nesta passagem estamos utilizando um fato que não foi estabelecido e que ficará como exercício: se c é um elemento de um anel, então $-c = (-1)c$.)

Vamos assumir que $\mathbb{Z}$ é um anel ordenado cujo conjunto de elementos positivos é $\mathbb{N} - \{0\}$.

A última propriedade que assumiremos sobre os inteiros é tão importante que será descrita em uma seção própria.

1.2.3 Princípio da indução finita

Como temos agora uma relação de ordem nos inteiros podemos anunciar o último axioma a respeito desses números que iremos assumir.

Axioma da boa ordenação. Todo subconjunto não vazio dos naturais possui um menor elemento.

(Pode-se mostrar que, a menos de isomorfismo, $\mathbb{Z}$ é o único anel ordenado possuindo o axioma da boa ordenação para o conjunto de elementos positivos.) Primeiro encontraremos qual é o menor número inteiro positivo.

Proposição 1. *O menor número inteiro positivo é o 1.*

Demonstração. Pelo axioma da boa ordem, existe um menor número inteiro positivo a. Comparando a com 1, temos uma das três possibilidades:

(i) $a = 1$; ou

(ii) $1 < a$; ou

(iii) $a < 1$.

Será suficiente mostrar que (ii) e (iii) não ocorrem. Claramente (ii) não ocorre, já que 1 é um número inteiro positivo e não pode ser menor que o menor inteiro positivo. Agora assuma que (iii) ocorre. Multiplicando ambos os lados da desigualdade por a, obtemos

$$aa < a1 = a.$$

Como o conjunto dos números inteiros positivos é fechado com relação ao produto, temos que aa é um número inteiro positivo que é menor que a; um absurdo! Concluímos que (iii) também não ocorre. □

Usando esse axioma, podemos estabelecer o princípio da indução finita, que é uma ferramenta importantíssima para demonstrar resultados discretos.

Teorema 1 (Princípio da indução finita — primeira forma)**.** *Seja $P(n)$ uma proposição a respeito de um natural n. Se*

(i) $P(0)$ é verdadeira; e

(ii) assumindo $P(n)$ podemos deduzir $P(n+1)$,

então $P(n)$ é verdadeira para todo natural n.

Demonstração. Seja S o conjunto dos naturais n tais que $P(n)$ não é verdadeira. Queremos mostrar que $S = \emptyset$. Vamos argumentar por contradição: suponha que $S \neq \emptyset$. Pelo princípio da boa ordem, S possui um menor elemento m. Por (i) temos que $m > 0$. Como m é o menor elemento de S, então $m - 1$ é um natural que não pertence a S. Logo $P(m-1)$ é verdadeira. Por (ii) podemos deduzir $P(m)$ a partir de $P(m-1)$, e daí $P(m)$ também é verdadeira. Chegamos a uma contradição e a hipótese de S ser não vazio é falsa. Logo $S = \emptyset$ e $P(n)$ é valida para todo natural n. □

Claro, se desejarmos provar $P(n)$ para $n \geq k$, então basta mostrarmos que $P(k)$ é verdadeiro e que (ii) vale para todo $n \geq k$. Este fato pode ser demostrado de maneira análoga.

Vamos aplicar o resultado que acabamos de demonstrar. Considere a seguinte proposição, que chamaremos de $S(n)$, a respeito de um natural n: a soma dos n primeiros inteiros positivos é igual a metade do produto de n por seu consecutivo, em uma linguagem matemática podemos expressar este fato por:

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

(Mostre que o natural consecutivo ao natural n é $n + 1$, isto é, $n + 1$ é o menor natural maior que n.) Para mostrar que $S(n)$ é verdadeira para todo natural n temos de seguir os passos enunciados no princípio da indução finita:

Passo 1: $S(0)$ é verdadeira pois:

$$0 = \frac{0(0+1)}{2}.$$

Passo 2: Vamos supor que $S(n)$ é verdadeira, isto é que a seguinte relação é válida:

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

Logo temos que:

$$\begin{aligned} 1+2+3+\cdots+n+(n+1) &= (1+2+3+\cdots+n)+(n+1) \\ &= \frac{n(n+1)}{2}+(n+1) \\ &= \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)((n+1)+1)}{2} \end{aligned}$$

e podemos deduzir $S(n+1)$ apartir de $S(n)$.

Logo $S(n)$ é verdadeira para todo natural n, pelo princípio da indução finita.

Esse princípio vai ser tão utilizado que iremos enunciar uma versão mais poderosa dele, sem no entanto prová-la, pois sua demonstração é similar a da primeira versão:

Teorema 2 (Princípio da indução finita — segunda forma)**.** *Seja $P(n)$ uma proposição a respeito de um natural n. Se*

(i) $P(0)$ é verdadeira; e

(ii) quando $n \geq 1$, assumindo $P(k)$, para todo $k < n$, podemos deduzir $P(n)$,

então $P(n)$ é verdadeira para todo natural n.

Demonstração. Exercício. Divirta-se! □

Iremos concluir esta seção fazendo uma aplicação deste resultado. O mesmo comentário feito no parágrafo que segue a demonstração do princípio da indução finita, na primeira forma, também vale neste caso.

A seqüência (f_n) de Fibonacci é famosa. Os dois primeiros termos são: $f_0 = 1$ e $f_1 = 2$. Para cada natural n, com $n \geq 2$, esta seqüência é definida recursivamente como:

$$f_n = f_{n-1} + f_{n-2}. \tag{1.2}$$

Os primeiros termos da seqüência de Fibonacci são:

$$1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

Considere a seguinte proposição, que chamaremos $F(n)$, sobre um número natural n (que pode ser zero):

$$f_n = \left(\frac{5+3\sqrt{5}}{10}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{5-3\sqrt{5}}{10}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n. \quad (1.3)$$

(Vamos assumir as propriedades usuais sobre números reais para mostrar esta identidade. Caso algum leitor não queira assumir tais propriedades, pode ignorar este exemplo.)

Para mostrar que $F(n)$ é verdadeira para todo natural n temos de seguir os passos enunciados no princípio da indução finita:

Passo 1: $F(0)$ é verdadeira pois:

$$\left(\frac{5+3\sqrt{5}}{10}\right)\left(\frac{1+\sqrt{5}}{2}\right)^0 + \left(\frac{5-3\sqrt{5}}{10}\right)\left(\frac{1-\sqrt{5}}{2}\right)^0 = \frac{5+3\sqrt{5}}{10} + \frac{5-3\sqrt{5}}{10} = 1,$$

que é o valor de f_0.

Passo 2: Para $n > 1$, vamos supor que $F(m)$ é verdadeira, para todo $m < n$. Necessitamos estabelecer que $F(n)$ também é válida a partir deste fato. Caso isto ocorra, pelo princípio da indução finita na segunda forma, concluímos que $F(n)$ vale para todo n. Temos dois casos a considerar: quando a recorrência (1.2) pode ser utilizada e quando não pode. A recorrência pode ser utilizada apenas quando $n \geq 2$. Portanto, o caso $n = 1$ tem de ser tratado separadamente. Quando $n = 1$, temos que

$$\left(\frac{5+3\sqrt{5}}{10}\right)\left(\frac{1+\sqrt{5}}{2}\right)^1 + \left(\frac{5-3\sqrt{5}}{10}\right)\left(\frac{1-\sqrt{5}}{2}\right)^1 = \frac{5+2\sqrt{5}}{5} + \frac{5-2\sqrt{5}}{5} = 2,$$

que é o valor de f_1. Portanto, neste caso, $F(n)$ é verificada. Assuma que $n \geq 2$. Neste caso $F(n-2)$ e $F(n-1)$ são verdadeiras, por hipótese de indução. Isto é, podemos substituir n por $n-1$ ou $n-2$ na

identidade (1.3). Para tornar as equações compactas, substituiremos os números envolvidos por letras, a saber:

$$A = \frac{5+3\sqrt{5}}{10}, \alpha = \frac{1+\sqrt{5}}{2}, B = \frac{5-3\sqrt{5}}{10}, \beta = \frac{1-\sqrt{5}}{2}$$

e a equação (1.3) pode ser reescrita como

$$f_n = A\alpha^n + B\beta^n. \tag{1.4}$$

Por (1.2) e (1.4) para $n-1$ e $n-2$, temos que

$$\begin{aligned} f_n &= f_{n-1} + f_{n-2} \\ &= (A\alpha^{n-1} + B\beta^{n-2}) + (A\alpha^{n-2} + B\beta^{n-2}) \\ &= A\alpha^{n-2}(\alpha+1) + B\beta^{n-2}(\beta+1) \\ &= A\alpha^{n-2}(\alpha^2) + B\beta^{n-2}(\beta^2) \\ &= A\alpha^n + B\beta^n \end{aligned}$$

já que α e β são as raízes do polinômio $p(X) = X^2 - X - 1$. Portanto, $F(n)$ também é verificada neste caso.

1.2.4 Exercícios

Terminamos esta secção com uma lista de exercícios complementares (já que vários foram deixados ao longo da seção). Resolva-os utilizando um dos princípios de indução finita vistos na subseção anterior.

1. Mostre que a soma dos ângulos internos de um polígono convexo com n lados, quando medido em radianos, é igual a $\pi(n-2)$.

2. Mostre que a soma dos n primeiros termos de uma progressão geométrica de razão q, $q \neq 1$, e termo inicial a é igual a

$$\frac{a(q^n - 1)}{q - 1}.$$

3. Mostre que dentre quaisquer k números inteiros consecutivos existe um divisível por k.

4. Mostre que a soma dos n primeiros cubos de naturais é igual a

$$\left[\frac{n(n+1)}{2}\right]^2$$

5. Caso existam números racionais a, b e c tais que a soma dos n primeiros quadrados de naturais é igual a $an^3 + bn^2 + cn$, para todo natural n, determine tais números.

6. Mostre que 5 divide $n^5 - n$, para todo natural n.

7. Mostre que o número de subconjuntos com i elementos de um conjunto com n elementos é igual a

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}.$$

8. Para quaisquer números complexos a e b e natural n, mostre que

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

9. Utilizando (1.3), mostre que o n-ésimo termo da seqüência de Fibonacci é dado por:

$$f_n = \left\{ \left(\frac{5+3\sqrt{5}}{10} \right) \left(\frac{1+\sqrt{5}}{2} \right)^n \right\},$$

onde $\{x\}$ denota o inteiro mais próximo do número real x.

10. Seja (a_n) uma seqüência de números complexos definida para todo natural n. Assuma que existam números complexos r e s tais que, para todo natural $n \geq 2$,

$$a_n = ra_{n-1} + sa_{n-2}.$$

Isto é, um termo é definido recursivamente a partir dos dois termos anteriores da seqüência, como no caso da de Fibonacci.

Mostre que, quando α e β são as raízes de $p(X) = X^2 - rX - s$, então, para todo natural n,

$$a_n = \left(\frac{a_1 - \beta a_0}{\alpha - \beta}\right)\alpha^n + \left(\frac{a_1 - \alpha a_0}{\beta - \alpha}\right)\beta^n.$$

11. Um conjunto contendo n retas, sem que quaisquer duas delas seja paralelas, divide o plano em várias regiões. Mostre que:

    (i) Estas regiões podem ser pintadas com duas cores de forma que regiões que possuem um segmento em comum na sua fronteira são pintadas com cores diferentes.

    (ii) O plano fica dividido em pelo menos $2n$ regiões.

    (iii) O mínimo descrito no item anterior é atingido se e somente se estas retas possuem um ponto em comum.

    (iv) O plano fica dividido em no máximo $1 + \frac{n(n+1)}{2}$ regiões.

    (v) O máximo descrito no item anterior é atingido se e somente se estas retas estão em posição geral, isto é, a interceção de quaisquer três delas é vazia.

    O que ocorre em cada um dos itens desta questão quando permitimos que o conjunto possa ter retas em paralelo?

1.3 Números primos

Nessa seção, iniciaremos o estudo dos números primos, e o nosso objetivo, nas seções vindouras, é mostrar que todo inteiro pode ser escrito de maneira única, a menos de ordem dos fatores, como o produto de números primos.

Um natural p maior que 1 é dito *primo* quando é impossível escrever p como o produto de dois naturais a e b com $a > 1$ e $b > 1$. Consequentemente, os únicos divisores de um número primo são a unidade e ele próprio. Como exemplos de primos temos $2, 3, 5, 7, 11, 13, \ldots$

Vamos mostrar agora que qualquer natural não-nulo pode ser escrito como o produto de um número finito de primos. O produto do conjunto vazio dá origem ao 1. O produto do conjunto unitário $\{p\}$ será p. Iremos convencionar isto, para que possamos enunciar esta proposição em toda sua generalidade.

Proposição 2. *Todo natural não-nulo pode ser escrito como o produto de um número finito de primos.*

Demonstração. Para estabelecer este fato, iremos usar o princípio da indução finita em sua segunda forma:

Passo 1: Observe que o resultado vale para $n = 1$, pois 1 é o produto do conjunto vazio (de primos).

Passo 2: Suponha que $n > 1$ e que todo natural $k < n$ possa ser escrito como o produto de números primos. Se n é um número primo, então n é o produto de números primos. Suponha então que n não é um número primo. Nesse caso, existem naturais a e b tais que $a < n$, $b < n$ e $n = ab$. Por hipótese, existem primos p_i e q_j tais que:

$$\begin{aligned} a &= p_1 p_2 \cdots p_r \\ b &= q_1 q_2 \cdots q_s \end{aligned}$$

e conseqüentemente

$$n = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

também é o produto de um número finito de primos. □

Podemos enunciar agora um dos resultados mais antigos conhecidos a respeito dos números primos:

Teorema 3 (Teorema de Euclides)**.** *Existe um número infinito de números primos.*

Demonstração. Argumentaremos por contradição. Suponha que exista apenas um número finito de primos: $p_1, p_2, \ldots, p_k$. Considere o seguinte natural $n = p_1 p_2 \cdots p_k + 1$. Pela proposição anterior, existe um primo p que divide n. Observe que p não pode ser igual a nenhum p_i já que p_i não divide 1. Chegamos a uma contradição e, conseqüentemente, existem infinitos números primos. □

Existem teoremas maravilhosas a respeito da distribuição dos números primos, vamos descrever um deles agora. Considere $\pi(x)$

como sendo o número de primos menores ou iguais a x. Gauss conjecturou o seguinte resultado, que foi provado por Hadamard e Poussin e é conhecido na literatura como o teorema dos números primos:

$$\lim_{x\to\infty} \frac{\pi(x)lnx}{x} = 1.$$

Como sua demonstração não é simples, foge ao propósito dessas notas, e não será apresentada.

1.3.1 Exercícios

1. Um número natural é dito *composto* quando pode ser escrito como o produto de dois números naturais menores. Mostre que todo número natural composto n possui um divisor menor ou igual a $\sqrt{n}$.

2. Fatore os seguintes números como produto de primos: $5^{16} - 1; 7^{12} - 1$ e $2^{15} + 1$.

3. Um número primo da forma $2^n - 1$, para $n \in \mathbb{N}$, é dito de Mersenne. Quando isto ocorre, mostre que n tem de ser primo.

4. A recíproca do exercício anterior vale? Isto é, se n é primo, então $2^n - 1$ é primo?

5. Um número primo da forma $2^n + 1$, para $n \in \mathbb{N}$, é dito de Fermat. Quando isto ocorre, mostre que n tem de ser uma potência de 2.

6. Para $k \in \{1, 3\}$, seja $\mathcal{P}_k$ o conjunto dos números primos que deixam resto k quando divididos por 4. Mostre que:

   (i) O produto, podendo ter repetição, de qualquer número de membros de $\mathcal{P}_1$ deixa resto 1 quando dividido por 4.

   (ii) O produto de um número par de membros de $\mathcal{P}_3$ deixa resto 1 quando dividido por 4.

   (iii) O produto de um número ímpar de membros de $\mathcal{P}_3$ deixa resto 3 quando dividido por 4.

7. Utilizando o exercício anterior e um argumento similar ao utilizado na demonstração do Teorema de Euclides, mostre que existe um número infinito de primos que deixam resto 3 quando dividido por 4.

1.4 Algoritmo da divisão de Euclides

Nessa seção apresentaremos o algoritmo da divisão de Euclides. A fatoração única nos inteiros é decorrência desse algoritmo. Outros conjuntos que possuem duas operações como as dos inteiros gozam da propriedade de fatoração única quando também possuem um algoritmo de divisão similar ao de Euclides.

Teorema 4 (Algoritmo de divisão de Euclides)**.** *Se $a \in \mathbb{Z}$ e $b \in \mathbb{N} - \{0\}$, então existem únicos inteiros q e r tais que $a = qb + r$ e $0 \leq r < b$.*

Demonstração. Seja S o seguinte conjunto:

$$\{a - qb : q \in \mathbb{Z} \text{ e } a - qb \geq 0\}.$$

Obseve que $S \neq \emptyset$ pois $a - qb \in S$, quando $q = -a^2$, já que

$$a - qb = a + a^2 b \geq a + a^2 \geq 0.$$

Pelo axioma da boa ordem, existe um menor elemento $r \in S$. Como $r \in S$, existe $q \in \mathbb{Z}$ tal que $r = a - qb$.

Observe que $r < b$, caso contrário $0 \leq r - b = a - qb - b = a - (q+1)b$ e $r - b \in S$, o que não pode ocorre pois r é o menor elemento de S. Acabamos de demonstrar que a pode ser escrito na forma $qb + r$ com $0 \leq r < b$.

Vamos mostrar que essa decomposição é feita de maneira única. Suponha que

$$a = qb + r = q'b + r', \text{ com } 0 \leq r < b \text{ e } 0 \leq r' < b.$$

Caso $q = q'$ temos que $r = r'$ como queríamos demostrar. Podemos supor que $q \neq q'$, mais ainda, que $q > q'$. Obtemos que

$$(q - q')b = r' - r.$$

Observe que o lado esquerdo dessa igualdade é maior ou igual a b e o direiro menor que b. Chegamos a uma contradição e o resultado segue. □

O algoritmo da divisão, quando b é um inteiro negativo, é uma imediata conseqüência do algoritmo que acabamos de apresentar. Enuncie tal algoritmo e o demonstre.

Dado dois inteiros a e b, um dos quais não é nulo, existe um maior natural que divide simultaneamente a e b. Esse número é dito o *maior divisor comum (MDC)* de a e b e é denotado por (a, b). Antes de descrever o algoritmo de Euclides para encontrar o maior divisor comum entre a e b, observamos que $(a, b) = (b, a)$, $(a, 0) = a$ e $(a, b) = (|a|, |b|)$. Portanto, apresentamos o algoritmo para o calculo do MDC apenas quando os inteiros envolvidos são ambos positivos.

Algoritmo de Euclides para encontrar o MDC. A entrada desse algoritmo são dois inteiros positivos a e b e a saída (a, b).

Passo 1: Faça $i = 1$, $r_0 = max\{a, b\}$ e $r_1 = min\{a, b\}$;

Passo 2: Defina r_{i+1} como o resto da divisão de r_{i-1} por r_i, isto é, $r_{i-1} = q_i r_i + r_{i+1}$ com $0 \leq r_{i+1} < r_i$;

Passo 3: Se $r_{i+1} \neq 0$ incremente i de 1 e volte para o passo 2, senão $(a, b) = r_i$.

Demonstração. Temos de provar que $(a, b) = r_i$. Primeiro, vamos mostrar, por indução em n, que r_i divide r_{i+1-n} para todo $0 \leq n \leq i + 1$. Isso é claramente verdade quando n é igual a 0 e a 1, já que $r_{i+1} = 0$. Suponha que $n > 1$ e que r_i divide r_{i+1-k} para todo $k < n$. Como $r_{i+1-n} = q_{i+1-(n-1)} r_{i+1-(n-1)} + r_{i+1-(n-2)}$, temos que r_i também divide r_{i+1-n} e o resultado segue pelo princípio de indução finita na sua segunda forma. Logo r_i é um divisor comum de a e b.

Seja d um divisor comum de a e b. Vamos mostrar por indução que d divide r_n para todo $0 \leq n \leq i$, em particular divide r_i e consequentemente r_i é o maior divisor comum de a e b. Por hipótese, o resultado vale para k igual a 0 e a 1. Suponha que $n > 1$ e que d divide r_k para todo $k < n$. Como $r_n = r_{n-2} - q_{n-1} r_{n-1}$, então d

também divide r_n e mais uma vez o resultado segue pelo princípio da indução na sua segunda forma. □

No próximo resultado estimamos o número de divisões que são necessárias para calcular o MDC através do algoritmo de Euclides. Para um número real x, denotamos por $\lfloor x \rfloor$ o maior inteiro menor ou igual a x.

Proposição 3. *Se a e b são inteiros tais que $a \geq b > 0$, então o algoritmo de Euclides realiza no máximo $1 + 2\lfloor \log_2 a \rfloor$ divisões para calcular o MDC de a e b.*

Demonstração. Sejam $r_0, r_1, \ldots, r_i, r_{i+1} = 0$ como no algoritmo de Euclides para o cálculo do MDC. Vamos mostrar que

$$r_k > 2r_{k+2}, \tag{1.5}$$

para todo $k < i$. Do algoritmo, sabemos que

$$r_k = q_{k+1} r_{k+1} + r_{k+2}.$$

Como $r_0 \geq r_1 > r_2 > \cdots > r_k > r_{k+1} > r_{k+2} > \cdots > r_i > r_{i+1}$, temos que $q_{k+1} \geq 1$ e daí

$$r_k \geq r_{k+1} + r_{k+2} > r_{k+2} + r_{k+2}.$$

Logo (1.5) segue. Seja m o maior inteiro tal que $2m \leq i$. Por indução em n, mostra-se, a partir de (1.5), que

$$r_0 > 2^n r_{2n}, \tag{1.6}$$

para n satisfazendo $1 \leq n \leq m$. Fazendo $n = m$ e $r_0 = a$ em (1.6) obtemos

$$1 \leq r_i \leq r_{2m} < \frac{a}{2^m}.$$

Conseqüentemente $2^m < a$ e daí

$$m < \log_2 a.$$

O resultado segue pois $i \in \{2m, 2m + 1\}$. □

O algoritmo de Euclides é extremamente eficiente, e é usado até hoje para calcular o maior divisor comum de dois inteiros e escreve-lo como combinação linear destes, com uma pequena otimização, onde permitimos que os restos involvidos possam ser negativos. Isto é, utilizamos a seguinte variante do algoritmo de divisão de Euclides: se a e b são inteiros, com $b \neq 0$, então existem únicos q e r tais que

$$a = qb + r \text{ e } -\frac{|b|}{2} < r \leq \frac{|b|}{2}.$$

(Para garantir a existência e a unicidade do quociente e resto é necessário que o intervalo onde o resto pode variar tenha comprimento $|b|$ e inclua exatamente um dos extremos. Verifique isto.) Com este novo algoritmo de divisão garantimos que o valor do resto cai pela metade em cada etapa e não após duas etapas como no algoritmo que apresentamos.

Vamos fazer um exemplo, calcular $(947, -409)$:

$$\begin{aligned} 947 &= 2 \cdot 409 + 129 \\ 409 &= 3 \cdot 129 + 22 \\ 129 &= 5 \cdot 22 + 19 \\ 22 &= 1 \cdot 19 + 3 \\ 19 &= 6 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

e o maior divisor comum entre 947 e -409 é 1. Usando esse exemplo, vamos escrever o maior divisor comum entre esses números como combinação linear deles:

$$\begin{aligned} 1 &= 19 - 6 \cdot 3 \\ &= 19 - 6 \cdot (22 - 1 \cdot 19) = 7 \cdot 19 - 6 \cdot 22 \\ &= 7 \cdot (129 - 5 \cdot 22) - 6 \cdot 22 = 7 \cdot 129 - 41 \cdot 22 \\ &= 7 \cdot 129 - 41 \cdot (409 - 3 \cdot 129) = 130 \cdot 129 - 41 \cdot 409 \\ &= 130 \cdot (947 - 2 \cdot 409) - 41 \cdot 409 = 130 \cdot 947 - 301 \cdot 409 \end{aligned}$$

e daí $1 = 130 \cdot 947 + 301 \cdot (-409)$. Usando uma raciocínio análogo ao feito acima, podemos mostrar o seguinte resultado:

Proposição 4. *Se a e b são inteiros, um dos quais não é nulo, então existem inteiros α e β tais que $\alpha a + \beta b = (a, b)$.*

Demonstração. Primeiro mostraremos que podemos supor que a e b são não-negativos. Sabemos que $(a, b) = (|a|, |b|)$. Caso

$$(|a|, |b|) = \alpha|a| + \beta|b|,$$

obtemos que

$$(|a|, |b|) = [\mathrm{sg}(a)\alpha]a + [\mathrm{sg}(b)\beta]b,$$

onde $\mathrm{sg}(x)$ é igual a 1, quando x for não-negativo, ou -1, quando x for negativo. Portanto basta mostrar este resultado quando a e b são não-negativos. Se um deles for zero, digamos $b = 0$, então o resultado segue pois

$$(a, b) = a = 1 \cdot a + 0 \cdot b.$$

A partir de agora, vamos assumir que a e b são positivos.

Sejam $r_0, r_1, \ldots, r_i, r_{i+1} = 0$ como no algoritmo de Euclides para o cálculo do MDC. Vamos mostrar por indução, da primeira forma, em n, com n satisfazendo $1 \leq n \leq i-1$, que existem inteiros α_n e β_n tais que

$$r_i = \alpha_n r_{i-n} + \beta_n r_{i-n-1}. \tag{1.7}$$

Como $r_i = -q_{i-1}r_{i-1} + r_{i-2}$, tomamos $\alpha_1 = -q_{i-1}$ e $\beta_1 = 1$. O resultado segue para $n = 1$. Resta mostrar que a partir de (1.7) pode-se obter (1.7) com $n+1$ no lugar de n. Substituindo $r_{i-n} = r_{i-n-2} - q_{i-n-1}r_{i-n-1}$ em (1.7), temos que

$$\begin{aligned} r_i &= \alpha_n(r_{i-n-2} - q_{i-n-1}r_{i-n-1}) + \beta_n r_{i-n-1} \\ &= (\beta_n - q_{i-n-1}\alpha_n)r_{i-n-1} + \alpha_n r_{i-n-2}. \end{aligned}$$

Se definirmos $\alpha_{n+1} = \beta_n - q_{i-n-1}\alpha_n$ e $\beta_{n+1} = \alpha_n$, a última equação pode ser reescrita como

$$r_i = \alpha_{n+1} r_{i-(n+1)} + \beta_{n+1} r_{i-(n+1)-1}$$

que é exatamente (1.7) quando n é substituído por $n+1$. Portanto (1.7) vale por indução da primeira forma. O resultado segue ao fazermos $n = i - 1$ em (1.7). □

Observe que temos um algoritmo para encontrar α e β implícito na demonstração da proposição anterior. Mais ainda, esta proposição será de fundamental importância para mostrar que todo inteiro não nulo decompõe-se como produto de primos de maneira única.

1.4.1 Exercícios

1. Calcule o maior divisor comum dos seguintes pares de números:
   (i) 1385 e 150;
   (ii) 619 e -450;
   (iii) 15018 e 0.
2. Para cada um dos itens da questão anterior, expresse o maior divisor comum de cada par de números como a combinação linear destes números.
3. Suponha que $a, q_1, q_1, \ldots, q_i$ são como no algoritmo de Euclides para o cálculo do MDC. Mostre que
$$|a| \geq q_1 q_2 \cdots q_i = \prod_{k=1}^{i} q_k.$$
4. Seja α_n e β_n como na Proposição 4. Mostre que $|\alpha_n| \leq r_{i-1-n}$ e $|\beta_n| \leq r_{i-n}$.

1.5 Representação de números inteiros

Consideraremos apenas o caso em que o número é inteiro positivo, já que a extensão para os números inteiros é imediata, bastando adicionar um sinal de $-$ (menos) à esquerda da representação quando o número for negativo e o zero é representado como 0.

Proposição 5. *Seja b um número natural tal que $b > 1$. Para cada número inteiro positivo n, existem únicos números naturais $k, b_0, b_1, b_2 \ldots, b_k$ tais que $b_i < b$, para todo $i \in \{0, 1, 2, \ldots, k\}$, $b_k \neq 0$ e*
$$n = \sum_{i=0}^{k} b_i b^i = b_k b^k + \cdots + b_2 b^2 + b_1 b + b_0. \tag{1.8}$$

Demonstração. Inciaremos estabelecendo a existência de k e dos b_i's. Faremos isto por indução do segundo tipo em n. Observe que o resultado vale para todo natural n tal que $n < b$. Neste caso, tome $k = 0$ e $b_0 = b$. Podemos supor que $n \geq b$. Por hipótese de indução, o resultado vale para todo natural menor que n. Pelo algoritmo da divisão, existem inteiros q e r tais que

$$n = qb + r \text{ e } 0 \leq r < b.$$

Como $n \geq b$, temos que $q \geq 1$. Como $q < n$, por hipótese de indução, exitem $k, b_1, b_2, \ldots, b_k$, com $b_i < b$ para todo $i \in \{1, \ldots, k\}$ e $b_k \neq 0$, tais que

$$q = \sum_{i=1}^{k} b_i b^{i-1}$$

Portanto

$$n = \left(\sum_{i=1}^{k} b_i b^{i-1} \right) b + r = \sum_{i=1}^{k} b_i b^i + r.$$

A exsitência da decomposição de n segue por indução bastando tomar $b_0 = r$.

A unicidade segue por indução do segundo tipo em n pois o quociente e o resto da divisão de n por b são respectivamente

$$\sum_{i=1}^{k} b_i b^{i-1} \text{ e } b_0$$

e são únicos. □

Seja b um inteiro tal que $b > 1$. Diremos que $(b_k \cdots b_2 b_1 b_0)_b$ é a *representação de n na base b* quando $n, b, k, b_0, b_1, b_2, \ldots, b_k$ satisfazem as hipóteses e as conclusões da Proposição 5. Note que na demonstração desta proposição está implícito um algoritmo para obter a representação de n na base b. Quando estiver claro com que base estamos trabalhando, a representação de n nesta base será denotada simplesmente por $b_k \cdots b_2 b_1 b_0$. Um inteiro pertencente ao conjunto $\{0, 1, \ldots, b-1\}$ é dito um *dígito* para a base b. Usualmente trabalhamos na base 10. No ocidente, cada dígito para a base 10 possui um símbolo especial para designá-lo que é largamente conhecido:

$0, 1, 2, 3, 4, 5, 6, 7, 8$ e 9 (descritos por ordem crescente de tamanho). Contudo, os computadores trabalham na base 2, com apenas dois que são 0 e 1. O número de dígitos de n na base b é denotado por $\text{dig}_b(n)$ e é igual a $k + 1$. Note que

$$\text{dig}_b(n) = \lfloor \log_b n \rfloor + 1. \tag{1.9}$$

No caso em que $b = 2$, omitimos o índice desta função, isto é, $\text{dig}_2(n)$ é simplesmente denotado por $\text{dig}(n)$.

1.5.1 Exercícios

1. Escreva 10.214 nas seguintes bases: 2, 7 e 26.

2. A representação de um natural na base 2 é 11.010.001.101. Qual é a sua representação na base 10?

3. Faça uma adaptação nos algoritmos conhecidos de soma, comparação, subtração, multiplicação e divisão para números naturais quando escritos em uma base b (que pode ser diferente de 10).

4. Seja n um número natural que possui $k + 1$ dígitos quando escrito na base b. Mostre que $b^k \leq n < b^{k+1}$.

5. Utilizando a questão anterior, demostre a igualdade que foi apresentada na equação (1.9).

1.6 Custo de realizar operações aritméticas

Nesta seção faremos a análise do custo das operações aritméticas nos inteiros, com os algoritmos tradicionais (aqueles que aprendemos na escola há muitos anos atrás). Como os computadores trabalham com números escritos na base 2, consideraremos o custo de realizar as operações nesta base. (A seguir iremos definir como medir tal custo. Não mostraremos aqui, mas o custo independe da base escolhida para representar os inteiros envolvidos na operação.)

Sejam f e g funções que assumem valores reais definidas sobre subconjuntos dos números naturais (ou reais) que contém todo número

natural (ou real) no intervalo $[a, +\infty)$, para algum natural a. Diremos que $f = O(g)$ quando existem um número natural n_0 e um número real positivo C tais que, para todo $n \geq n_0$,

$$|f(n)| \leq C|g(n)|.$$

Por exemplo, quando $f(x)$ é um polinômio de grau k com coeficientes reais, $f(x) = O(x^k)$.

Vamos analisar o custo das operações aritméticas entre dois números naturais a e b que possuem no máximo k dígitos na base 2. Nossas estimativas de custo seriam melhores caso utilizássemos o número de dígitos de a e de b na base 2. Não faremos isto, pois temos apenas o interesse de estabelecer que o custo de tais operações é polinomial em k (observe que k é o tamanho de cada uma das duas entradas do algoritmo — que são os números a e b). Isto é, nosso custo é um polinômio no tamanho da entrada do algoritmo. Um algoritmo com esta característica é conhecido como polinomial. Note que ao restringirmos a análise de custo ao caso em que a entrada do algoritmo são números naturais a e b não perdemos generalidade pois as operações aritméticas entre números inteiros podem ser facilmente reduzidas a operações similares entre números naturais.

Lema 2. *O número de operações elementares realizadas em qualquer operação de comparação ou adição ou subtração entre dois números naturais com até k dígitos na base 2 é $O(k)$, isto é, de tempo linear.*

Para estimar o custo de um algoritmo, calculamos o número de operações elementares que este realiza. Descreveremos o que consideramos como operação elementar na demonstração do lema que virá a seguir.

Demonstração do Lema 2. Sejam a e b os números naturais tendo no máximo k dígitos. Para simplificar nossa argumentação iremos completar estes números com zeros a esquerda de forma que "fiquem com k dígitos" (isto é, vamos operar considerando todas as k posições de memória reservadas para estes números no computador).

Iniciaremos pela comparação. Percorremos os dois números simultaneamente da esquerda para a direita, um dígito de cada vez, e os comparamos. Caso sejam iguais avançamos para o dígito seguinte

e continuamos com o algoritmo (caso não seja possível avançar, estamos no dígito mais a direita de cada um dos números e neste caso $a = b$). Caso sejam diferentes, um dígito será 0 e o outro será 1. O número que possui o dígito 1 será o maior e o algoritmo para retornando esta informação. Consideraremos como operação elementar a comparação dos dois dígitos. Neste algoritmo foram realizadas no máximo k comparações. Portanto seu custo será $O(k)$.

Necessitamos de uma posição de memória extra para o "vai um", que inicialmente recebe o valor 0 (que ao final será o $(k+1)$-ésimo dígito da soma). Percorremos simultaneamente os dois números da direira para a esquerda um dígito de cada vez. Neste momento calcula-se o dígito correspondente da soma dos dois números observando três posições de memória: a do dígito de a, a do dígito de b e a do "vai um". Será 0 se existe um número par de 1's nestas posições e 1 caso contrário. O "vai um" recebe o valor de 0 caso existam no máximo um dígito 1 nestas posições e 1 caso contrário. Esta computação será considerada como uma operação elementar. Ao atingirmos o k-ésimo dígito da soma, colocamos o "vai um" como o $(k+1)$-ésimo dígito da soma. Portanto realizamos k operações elementares e o custo do algoritmo será $O(k)$.

Para calcular $a-b$ necessitamos primeiro realizar uma comparação. Caso $a < b$, calculamos $b-a$ e o resultado será igual a $-(b-a)$. Caso $a = b$, o resultado será 0. Portanto necessitamos apenas de um algoritmo para realizar a subtração $a - b$ no caso em que $a > b$. O custo desta etapa será de uma comparação, logo é $O(k)$. O algoritmo será o mesmo do da adição exceto no cálculo do valor a ser armazenado no "vai um" que será igual a 1 quando o número de dígitos igual a 1 na posição "vai um" e no dígito de b for maior que o número de digitos igual a 1 na posição do dígito de a. Esta segunda etapa tem custo $O(k)$. Conseqüentemente o custo do algoritmo será $O(k)$. □

Lema 3. *O número de operações elementares realizadas em qualquer operação de multiplicação ou divisão entre dois números naturais com até k dígitos na base 2 é $O(k^2)$, isto é, de tempo quadrático.*

Existem algoritmos diferentes dos usuais para realizar as operações de multiplicação e divisão de "números grandes" que são muito mais eficientes. O custo de cada um destes algoritmos é $O(k \log k \log\log k)$.

Não apresentamos tais algoritmos aqui, pois fogem do objetivo deste curso.

Demonstração. Sejam a e b números naturais possuindo no máximo k dígitos quando representados na base 2. Suponha que b possua exatamente l dígitos. O produto de a por b é igual a soma de um conjunto X de números com cardinalidade no máximo l, cada um sendo uma translação de a, obtidos da seguinte forma: enumere as posições dos dígitos de b da direita para esquerda com $0, 1, 2, \ldots, l-1$ e, caso na na posição i o dígito de b for igual a 1, adicione a X um número obtido a partir de a colocando i dígitos iguais a 0 na sua direira (isto é, uma translação de a de i casas para a esquerda). Como a soma de quaisquer dois números em X tem no máximo $2k$ dígitos, o custo de realizar a soma de todos elementos de X será $O(l-1)O(2k) = O(lk) = O(k^2)$. Deixo a análise do algoritmo da divisão por conta do leitor (veja o quinto exercício desta seção). □

Lema 4. *O custo para o cálculo do maior divisor comum de dois números naturais com no máximo k dígitos quando representados na base 2 é $O(k^3)$.*

Demonstração. Seja a o maior destes números. Pela Proposição 3, o número de divisões realizadas pelo algoritmo de Euclides para o cálculo do MDC é limitado superiormente por $2\lfloor \log_2 a \rfloor + 1$. Como $\text{dig}(a) = \lfloor \log_2 a \rfloor + 1$, este limite superior passa a ser $2\text{dig}(a) - 1 \leq 2k - 1 = O(k)$. Pelo Lema 3, o custo de cada uma destas divisões é $O(k^2)$. Portanto, o custo do algoritmo de Euclides para o cálculo do MDC será $O(k^2)O(k) = O(k^3)$. □

1.6.1 Exercícios

1. Para um número real a maior que 1, mostre que $\log_a x = O(\log_2 x)$.

2. Suponha que $f_1, f_2, \ldots, f_k$ são funções tais que $f_i = O(g)$, para todo $i \in \{1, 2, \ldots, k\}$, com k fixo. Mostre que $f_1 + f_2 + \cdots + f_k = O(g)$. (Isto é, a soma de funções $O(g)$ também é uma função $O(g)$.)

3. Mostre que $f_1 f_2 \cdots f_k = O(g_1 g_2 \cdots g_k)$ quando, para cada $i \in \{1, 2, \ldots, k\}$, $f_i = O(g_i)$.

4. Mostre que o custo do algoritmo usual para realizar a multiplicação de dois números naturais a e b é igual a $O(\mathrm{dig}(a)\mathrm{dig}(b))$.

5. Dados números naturais a e b, o algoritmo da divisão garante a existência de números inteiros q e r tais que $a = qb + r$, com $0 \leq r < b$. Mostre que o custo de fazer esta divisão com o algoritmo usual é $O(\mathrm{dig}(q)\mathrm{dig}(b))$.

6. Mostre que o custo de encontrar o MDC de dois números naturais a e b é $O(\mathrm{dig}(a)\mathrm{dig}(b))$ — use o exercício anterior e o exercício 3 da Seção 1.4. (Isto é, podemos obter uma estimativa muito melhor do que a apresentada nesta seção para este custo.)

7. Encontre uma estimativa para o custo de expressar o MDC de dois números naturais como a combinação linear destes números (utilizando o algoritmo implícito na demonstração da Proposição 4).

8. Escreva um algoritmo para encontrar a parte inteira da raiz quadrada de um número natural n cujo custo seja $O(\mathrm{dig}_2(n)^3)$.

1.7 Fatoração única

Nessa seção iremos demonstrar o teorema da fatoração única para os inteiros. O núcleo da demonstração é o lema que provaremos a seguir:

Lema 5. *Sejam a e b inteiros. Se um primo p divide ab, então p divide a ou b.*

Demonstração. Suponha que p não divide a. Nesse caso $(p, a) = 1$, pois os únicos divisores positivos de p são 1 e p. Pela Proposição 4, existem inteiros α e β tais que $\alpha a + \beta p = 1$. Multiplicando esta relação por b obtemos que $\alpha ab + \beta pb = b$. Como p divide ab, temos que p divide b. □

Teorema 5 (Teorema fundamental da aritmética)**.** *Todo número inteiro n não-nulo pode ser escrito de maneira única na forma*

$$n = up_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

onde $u = \pm 1$, $p_1, p_2, \ldots, p_r$ são números primos tais que $p_1 > p_2 > \cdots > p_r$ e $a_1, a_2, \ldots, a_r$ são inteiros positivos.

Demonstração. Observe que basta mostrar o resultado para os naturais. Faremos a demonstração por indução do segundo tipo em n. O resultado é claramente verdadeiro para $n = 1$. Suponha que todo natural $k < n$ pode ser escrito de maneira única como produto de primos e que

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s},$$

com $p_1 > p_2 > \cdots > p_r$ e $q_1 > q_2 > \cdots > q_s$, todos primos. Sem perda de generalidade, podemos supor que $p_1 \geq q_1$. Pelo lema anterior, p_1 divide q_i para algum i. Como $p_1 \geq q_1 > q_2 > \cdots > q_s$, segue que $i = 1$ e $p_1 = q_1$. Consequentemente

$$p_1^{a_1 - 1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{b_1 - 1} q_2^{b_2} \cdots q_s^{b_s}.$$

Por hipótese de indução, todo natural menor que n possui fatoração única e daí $r = s$, $p_i = q_i$ e $a_i = b_i$ para todo i. Logo as fatorações de n acima são idênticas e, por indução, o resultado vale para todo n. □

Observe que foi possível demonstrar fatoração única nos inteiros, pois esse conjunto tem um algoritmo de divisão. Iremos nos deparar com outros conjuntos, que possuem algoritmos de divisão e, de maneira análoga, podemos mostrar que gozam da propriedade da fatoração única. Claro que alguns conjuntos possuem fatoração única, mas não têm um algoritmo de divisão.

1.7.1 Exercícios

1. Encontre o expoente da maior potência de 2 que divide 100! (100 fatorial).

2. Seja p um número primo e n um inteiro positivo. Mostre que o expoente da maior potência de p que divide $n!$ é

$$\sum_{i\geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

1.8 Algumas aplicações da fatoração única

Nessa última seção, iremos fazer algumas aplicações bem simples da fatoração única. Primeiro, iremos mostrar que $\sqrt{2}$ não é um número racional. Argumentaremos por contradição: suponha que $\sqrt{2}$ é um número racional. Logo existem inteiros m e n tais que

$$\sqrt{2} = \frac{m}{n}.$$

Elevando-se essa expressão ao quadrado obtemos

$$2n^2 = m^2.$$

Se 2^a e 2^b são as maiores potências de 2 que dividem m e n, respectivamente, então o expoente de 2 na fatoração de $2n^2$ é $2b+1$ e na de m^2 é $2a$. Chegamos a uma contradição usando o teorema da fatoração única, pois $2n^2 = m^2$. Logo $\sqrt{2}$ não é um racional.

O mais conhecido teorema da matemática, que é o de Pitágoras, garante que em um triângulo retângulo

$$a^2 = b^2 + c^2,$$

onde a é sua hipotenusa e b e c seus catetos. Sabemos que existem vários desses triângulos com todos os lados naturais, por exemplo:

$$\begin{aligned} 3^2 + 4^2 &= 5^2 \\ 5^2 + 12^2 &= 13^2 \\ (501.000)^2 + (1.001)^2 &= (501.001)^2 \ldots \end{aligned}$$

Fazemos a seguinte pergunta: quais são todos esses triângulos? Em outras palavras, quais são todas as soluções nos naturais da equação

$$a^2 = b^2 + c^2.$$

Encontrar todas as soluções inteiras de uma determinada equação, no jargão matemático, é resolver uma equação diofantina (em homenagem ao matemático grego Diofantus).

Observe que $(\lambda a, \lambda b, \lambda c)$ também é uma solução dessa equação quando (a, b, c) é solução, pois

$$(\lambda b)^2 + (\lambda c)^2 = \lambda^2 b^2 + \lambda^2 c^2 = \lambda^2(b^2 + c^2) = \lambda^2 a^2 = (\lambda a)^2.$$

Logo necessitamos encontrar as soluções (a, b, c) tais que $MDC(a, b, c) = 1$, pois as demais são obtidas apartir destas multiplicando-as por um inteiro qualquer. Caso isso ocorra, temos de ter $(a, b) = (a, c) = (b, c) = 1$, caso contrário, $MDC(a, b, c) \neq 1$. (Por exemplo, se um primo p divide b e c, temos que p divide $b^2 + c^2 = a^2$ e daí p divide a.) Podemos fazer uma outra simplificação no problema, procurar soluções apenas nos inteiros positivos, pois (a, b, c) é solução se e somente se $(|a|, |b|, |c|)$ também é, e as únicas soluções que têm uma das coordenadas nula são $(a, \pm a, 0)$ e $(a, 0, \pm a)$.

Seja (a, b, c) uma solução em números inteiros positivos de

$$a^2 = b^2 + c^2$$

tal que $MDC(a, b, c) = 1$. Observe que b ou c é ímpar, caso contrário 2 dividiria $MDC(a, b, c)$ pois a soma de números pares é par. Digamos que b seja ímpar. Como

$$b^2 = a^2 - c^2 = (a - c)(a + c),$$

temos que $MDC(a - c, a + c) = 1$, já que todo número d que divide $a-c$ e $a+c$ também divide $(a-c)+(a+c) = 2a$ e $(a+c)-(a-c) = 2c$ e como $(a, c) = 1$ concluímos que d é igual a 1 ou 2, mas d não pode ser 2 pois divide b, que é ímpar. Se p^a é a maior potência de um primo p que divide b, então $2a$ é o expoente de p na fatoração de b^2 como produto de primos. Em decorrência de $MDC(a-c, a+c) = 1$, temos que p^{2a} ou divide $a - c$ ou divide $a + c$. Consequentemente os expoentes dos primos na fatoração única de $a - c$ e $a + c$ são todos pares e existem naturais ímpares r e s tais que $a-c = r^2$ e $a+c = s^2$, com $(r, s) = 1$. Como $b^2 = (a - c)(a + c) = r^2 s^2$, obtemos que

$$a = \frac{s^2 + r^2}{2}, b = rs, c = \frac{s^2 - r^2}{2}.$$

Logo chegamos ao seguinte resultado:

Teorema 6. *As soluções da equação $a^2 = b^2 + c^2$ nos inteiros positivos são*

$$a = \frac{\lambda(s^2 + r^2)}{2} \text{ e } \{b, c\} = \left\{\lambda rs, \frac{\lambda(s^2 - r^2)}{2}\right\},$$

onde λ é um número inteiro positivo qualquer e r e s são números naturais ímpares, com $s > r$ e $(r, s) = 1$.

Nos parágrafos anteriores, mostramos que toda solução é dessa forma. Para provar que toda tripla dessa forma é solução, observamos que a e c são naturais pois $s^2 - r^2$ e $s^2 + r^2$ são pares. Por fim

$$b^2 + c^2 = \lambda^2 r^2 s^2 + \frac{\lambda^2(s^4 - 2r^2s^2 + r^4)}{4} = \frac{\lambda^2(s^4 + 2r^2s^2 + r^4)}{4} = a^2.$$

Considere agora a seguinte equação

$$a^n = b^n + c^n.$$

Estudamos acima esta equação para $n = 2$. Fermat escreveu nas margens de um livro, há mais de 350 anos atrás, que possuia uma demonstração de que esta equação não tinha solução em inteiros todos não nulos, para $n \geq 3$. Este resultado ficou conhecido como o "Último Teorema de Fermat". Só nesta década, depois de inúmeras tentativas de solução pelos mais renomados matemáticos, este resultado foi demonstrado por Wiles.

Seja

$$\alpha = cos\left(\frac{2\pi}{n}\right) + sen\left(\frac{2\pi}{n}\right) i,$$

que é uma raíz n-ésima da unidade, isto é, $\alpha^n = 1$. Considere o seguinte conjunto de números:

$$S_n = \{p(\alpha) : p(X) \text{ é um polinômio com coeficientes inteiros}\}.$$

Cauchy e Lamé, de maneira independente, nos meados do Século XIX, pensaram que tinham demostrado o "Último Teorema de Fermat", mas suas demonstrações tinham um furo: assumiam que o conjunto de números S_n admitia fatoração única, o que infelizmente

não ocorre para todo n. Kummer observou este erro e foi capaz de demonstrar que para uma infinidade de números primos n o conjunto S_n admite fatoração única em um sentido mais amplo (o número 37 é o primeiro primo n para o qual Kummer não conseguiu estabelecer tal fatoração). Para $n = 4$, este resultado é verdade, e o conjunto S_n é conhecido como inteiros de Gauss (pois este demonstrou a fatoração única nesse conjunto). Obseve que

$$S_4 = \{a + bi : a \text{ e } b \text{ são inteiros}\}.$$

1.8.1 Exercícios

1. Mostre que $\sqrt{5}$, $\sqrt[3]{4}$ e $\sqrt[7]{\frac{9}{13}}$ não são racionais.

2. Para um número racional positivo r e um número natural n, caracterize quando $\sqrt[n]{r}$ é um número racional.

3. Determine todos os triângulos retângulos cujos lados têm comprimentos inteiros tais que a diferença do comprimento de um dos catetos para o da hipotenusa é 1.

4. Mostre que é necessário demonstrar o "Último Teorema de Fermat" apenas quando o expoente n for primo.

5. Sejam a, b e c números naturais tais que $a^2 + 2b^2 = c^2$ e $MDC(a, b, c) = 1$. Mostre que existem números naturais r e s tais que $(r, s) = 1$ e

$$a = |2r^2 - s^2|, b = 2rs, c = 2r^2 + s^2.$$

6. Mostre que $a^4 + b^4 = c^2$ não possui solução inteira com $abc \neq 0$.

7. Encontre um algoritmo da divisão, como o de Euclides, para S_4.

Capítulo 2

Congruências

2.1 Introdução

Neste capítulo apresentaremos o conceito de congruência módulo um natural, noção que foi criada por Gauss, e mostraremos propriedades básicas a seu respeito. Dentre os principais resultados apresentados, destacamos os seguintes:

- **O Pequeno Teorema de Fermat.** Uma pequena variante deste resultado permitiu a Rabin elaborar um algoritmo (randomizado) eficiente para decidir se um número natural é primo ou composto. Este algoritmo, que tem quase três décadas, ainda é utilizado na prática para decidir primalidade. (Encontrar dois números primos "grandes" é essencial para utilizar o sistema de criptografia de chave pública conhecido por RSA.)

- **O Teorema de Euler.** Este resultado generaliza o Pequeno Teorema de Fermat e é fundamental para o funcionamento do RSA. (Em criptografia, poderia ser chamado do Teorema Fundamental do RSA.)

- **O Teorema de Wilson.** Este resultado caracteriza números primos através do cálculo de um fatorial. Seguindo este tópico, faremos considerações sobre a complexidade de realizar exponenciação e calcular o fatorial módulo um natural.

- **O Teorema Chinês dos Restos.** Este resultado é clássico e foi utilizado pelos chineses em aplicações militares (para calcular o número de soldados em seus exércitos).

Sempre discutiremos algoritmos associados com estes resultados, bem como o custo da execução destes procedimentos.

2.2 Definição

Seja n um número natural maior que 1, que manteremos fixo durante toda essa seção. Diremos que dois inteiros a e b são *congruentes módulo* n, e denotamos por

$$a \equiv b \mod n,$$

se e somente se n divide $a - b$. Listaremos abaixo algumas propriedades que essa relação possui:

(C1) $a \equiv a \mod n$;

(C2) se $a \equiv b \mod n$, então $b \equiv a \mod n$;

(C3) se $a \equiv b \mod n$ e $b \equiv c \mod n$, então $a \equiv c \mod n$;

(C4) se $a \equiv b \mod n$ e $a' \equiv b' \mod n$, então $a+a' \equiv b+b' \mod n$;

(C5) se $a \equiv b \mod n$ e $a' \equiv b' \mod n$, então $aa' \equiv bb' \mod n$.

A primeira e segunda propriedade são imediatas. A terceira também: como n divide $a - b$ e $b - c$, então n divide a soma desses números que é $a-c$. Conseqüentemente $a \equiv c \mod n$. Qualquer outra relação que possua as três primeiras propriedades é dita de *equivalência*. Vários resultados que valem para a relação de congruência módulo um natural também são verificados numa relação de equivalência qualquer. A igualdade nos reais e paralelismo em retas no espaço (uma reta é paralela a si mesma) são exemplos de relações de equivalência. Porém, ser maior ou igual não é uma relação de equivalência nos reais.

Agora estabeleceremos a quarta e a quinta propriedades. Como $a \equiv b \mod n$ e $a' \equiv b' \mod n$, temos que n divide $a - a'$ e $b - b'$. Logo também divide

$$a - a' = (a + b) - (a' + b') \text{ e } aa' - bb' = a(a' - b') + (a - b)b'$$

e conseqüentemente

$$a + a' \equiv b + b' \mod n \text{ e } aa' \equiv bb' \mod n,$$

donde seguem a quarta e a quinta propriedades.

Definimos a *classe de congruência* de um inteiro a como

$$\overline{a} = \{b \in \mathbb{Z} : a \equiv b \mod n\}.$$

Observe que $a \in \overline{a}$. Vamos definir operações de adição e multiplicação de classes de congruências e mostrar que essas operações possuem as mesmas propriedades aritméticas que as dos inteiros. Isto é, o conjunto de classes de equivalência módulo um natural, munido com estas operações, é um anel.

Lema 6. *Se $c \in \overline{a}$, então $\overline{c} = \overline{a}$.*

Demonstração. Basta mostrar que $\overline{a} \subseteq \overline{c}$, já que $a \in \overline{c}$ e por esse resultado $\overline{c} \subseteq \overline{a}$, e teremos a igualdade de conjuntos. Se $b \in \overline{a}$, então $a \equiv b \mod n$. Como $c \equiv a \mod n$, pois $c \in \overline{a}$, temos que $c \equiv b \mod n$, por **(C3)**. Logo $b \in \overline{c}$ e conseqüentemente $\overline{a} \subseteq \overline{c}$. □

Lema 7. *Se a e b são inteiros, então $\overline{a} = \overline{b}$ ou $\overline{a} \cap \overline{b} = \emptyset$.*

Demonstração. Suponha que $\overline{a} \cap \overline{b} \neq \emptyset$ e que $c \in \overline{a} \cap \overline{b}$. Pelo Lemma 6, segue-se que $\overline{c} = \overline{a}$ e $\overline{c} = \overline{b}$. Conseqüentemente $\overline{a} = \overline{b}$. □

O seguinte conjunto

$$\mathbb{Z}_n = \{\overline{a} : a \in \mathbb{Z}\},$$

é conhecido como *os inteiros módulo n*. Pelo algoritmo da divisão de Euclides, para cada inteiro a, existem inteiros q e r tais que

$$a = qn + r \text{ com } 0 \leq r < n.$$

Logo $a \equiv r \mod n$ e daí $\overline{a} = \overline{r}$. Isto é, toda classe de congruência tem um representante entre 0 e $n-1$. Conseqüentemente

$$\mathbb{Z}_n = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\right\}.$$

Vamos mostrar que todas as classes listadas acima são diferentes. Suponha que $0 \leq r, r' < n$ e que $\overline{r} = \overline{r'}$. Nesse caso, $r - r' = \lambda n$, para algum inteiro λ, e necessariamente $r = r'$. Logo $|\mathbb{Z}_n| = n$.

Sejam $\overline{a}, \overline{b} \in \mathbb{Z}_n$, definimos a soma e o produto dessas classes de congruências como respectivamente

$$\overline{a} + \overline{b} = \overline{a+b} \text{ e } \overline{a}\overline{b} = \overline{ab}.$$

Como essas operações dependem dos representantes escolhidos, temos que mostrar que estão bem definidas. Caso $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$, segue que $\overline{a+b} = \overline{a'+b'}$ e $\overline{ab} = \overline{a'b'}$, por respectivamente **(C4)** e **(C5)**. Essas operações de $\mathbb{Z}_n$ possuem todas as propriedades das operações dos inteiros: são comutativas, associativas, ambas têm elemento neutro, a adição possui inverso e a multiplicação é distribuitiva com relação a adição. Vamos mostrar a validade da última propriedade, as demais ficam como exercício. Se $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, então

$$\overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{(b+c)} = \overline{a(b+c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{a}\overline{b} + \overline{a}\,\overline{c}.$$

Portanto $\mathbb{Z}_n$ é um anel.

2.2.1 Exercícios

1. Faça as tábuas de adição e multiplicação para $\mathbb{Z}_6$.
2. Encontre o resto da divisão de 7^{256} por 15.
3. Um elemento a de um anel A é dito *nilpotente* quando existe $k \in \mathbb{N}$ tal que $a^k = 0$. Caracterize os naturais n para os quais o anel $\mathbb{Z}_n$ possui um elemento nilpotente diferente de $\overline{0}$?
4. Estabeleça a validade do critério para decidir se um inteiro é divisível por 3 (três) que você aprendeu na quarta série do ensino fundamental.
5. Mostre a validade da "prova dos nove" que foi ensinada na segunda série do ensino fundamental.

6. Considere a seguinte afirmação sobre um natural n: "Um natural é divisível por n se e somente se a soma de seus dígitos, quando representado na base 10, é divisível por n". Para que naturais n esta afirmação é verdadeira?

7. Obtenha um critérito, em termos dos dígitos da representação do número na base 10, para que este seja divisível por 11. Faça o mesmo para 7.

8. Encontre todas as raízes do polinômio $X^2 - \overline{1}$ em $\mathbb{Z}_{2^n}$.

2.3 Inversos multiplicativos em $\mathbb{Z}_n$

Nos inteiros apenas 1 e -1 têm inverso multiplicativo, mas em $\mathbb{Z}_n$ o quadro é completamente diferente. Suponha que a seja um inteiro tal que $(a, n) = 1$. Logo existem inteiros α e β tais que $\alpha a + \beta n = 1$ e daí

$$\overline{1} = \overline{\alpha a + \beta n} = \overline{\alpha a} + \overline{\beta n} = \overline{\alpha}\,\overline{a}.$$

Acabamos de mostrar o seguinte resultado:

Proposição 6. *Se $(a, n) = 1$, então $\overline{a}$ possui inverso multiplicativo em $\mathbb{Z}_n$.*

Em $\mathbb{Z}_{947}$, o inverso de $\overline{409}$ é igual a $\overline{646}$ pois

$$1 = 130 \cdot 947 - 301 \cdot 409,$$

como visto no capítulo anterior. (Para encontrar a combinação linear entre 409 e 947, usa-se o algoritmo de Euclides para o cálculo do maior divisor comum.) Tomando classes de congruências, temos que

$$\begin{aligned}
\overline{1} &= \overline{130 \cdot 947 - 301 \cdot 409} \\
&= \overline{130 \cdot 947} + \overline{(-301 \cdot 409)} \\
&= \overline{130}\,\overline{947} + \overline{(-301)}\,\overline{409} \\
&= \overline{0} + \overline{(-301)}\,\overline{409} \\
&= \overline{646}\,\overline{409}.
\end{aligned}$$

Suponha agora que a seja um inteiro tal que $(a, n) = d \neq 1$ e $\overline{a} \neq \overline{0}$. Observe que

$$a\left(\frac{n}{d}\right) = \left(\frac{a}{d}\right) n.$$

Se $b = \frac{n}{d}$, então $\overline{b} \neq \overline{0}$, pois $0 < b < n$. Logo

$$\overline{a}\,\overline{b} = \overline{0}.$$

Conseqüentemente

Proposição 7. *Se $(a, n) \neq 1$, então $\overline{a}$ é um divisor de zero em $\mathbb{Z}_n$.*

Claro que um divisor de zero não pode ter um inverso mutiplicativo. Suponha que isto possa ocorrer. Seja $\overline{a}$ um elemento de $\mathbb{Z}_n$ que é divisor de zero e tem inverso multiplicativo. Logo existem elementos $\overline{b}$ e $\overline{c}$ de $\mathbb{Z}_n$ tais que $\overline{b} \neq \overline{0}$ e $\overline{a}\overline{b} = \overline{0}$ e $\overline{a}\overline{c} = \overline{1}$. Portanto,

$$\overline{0} = \overline{0}\,\overline{a} = (\overline{b}\,\overline{a})\overline{c} = \overline{b}(\overline{a}\,\overline{c}) = \overline{b}\,\overline{1} = \overline{b};$$

uma contradição.

Estas duas proposições particionam os elementos de $\mathbb{Z}_n$, diferentes de $\overline{0}$, em duas famílias: aqueles que possuem inverso multiplicativo; e aqueles que são divisores de zero. No caso de n ser um número primo, todos os elementos de $\mathbb{Z}_n$, exceto $\overline{0}$, possuem inverso multiplicativo. Denotaremos por $\mathbb{Z}_n^*$ o conjunto de todos os elementos que possuem inverso multiplicativo em $\mathbb{Z}_n$. Note que $\mathbb{Z}_n^*$ é fechado com relação ao produto.

Um anel em que todo elemento diferente de 0 possui inverso multiplicativo é dito um *corpo*. Conseqüentemente $\mathbb{Z}_n$ é um corpo se e somente se n é primo. Não é pouca coisa ser um corpo. Finalizaremos esta seção, estabelecendo que um polinômio de grau k com coeficientes em um corpo tem no máximo k raízes neste corpo (compare este resultado com o último exercício da seção anterior).

O conjunto de todos o polinômios com coeficientes em um anel A e variável X é denotado por $A[X]$. Este conjunto também é um anel quando munido com as operações de adição e multiplicação definidas a seguir. Sejam $f(X)$ e $g(X)$ polinômios com coeficientes em A, digamos

$$f(X) = \sum_{i=0}^{k} f_i X^i \text{ e } g(X) = \sum_{i=0}^{l} g_i X^i.$$

Defina $f_i = 0$, quando $i > k$, e $g_i = 0$, quando $i > l$. A *adição* de f com g é definida por

$$(f+g)(X) = \sum_{i=0}^{\max\{k,l\}} (f_i + g_i)X^i.$$

A *multiplicação* de f por g é definida como

$$(fg)(X) = \sum_{i=0}^{k+l} h_j X^j,$$

onde

$$h_j = \sum_{i=0}^{j} f_i g_{j-i}.$$

Quando $f_k \neq 0$, diremos que o *grau* de f é k. Caso $k = 0$ e $f_0 = 0$, diremos que o *grau* de f é $-\infty$.

Lema 8. *Seja $f(X)$ um polinômio com coeficientes em um anel A. Se $a \in A$, então existe polinômio $q(X)$, com coeficientes em A, tal que*

$$f(X) = (X-a)q(X) + f(a).$$

Demonstração. Será suficiente estabelecer que existe um polinômio $q(X)$ com coeficientes em A e um elemento r de A tais que:

$$f(X) = (X-a)q(X) + r, \tag{2.1}$$

pois, neste caso, $r = f(a)$. Faremos isto por indução no grau k de $f(X)$. Se $f(X)$ é uma constante (isto é, tem grau $-\infty$ ou 0), então tomamos $q(X) = 0$ e $r = f(X)$. Logo (2.1) segue. Suponha que $k \geq 1$ e que o resultado vale para todo polinômio de grau no máximo $k-1$. Seja $f_k X^k$ o termo de maior grau de $f(X)$. Considere

$$g(X) = f(X) - (X-a)f_k X^{k-1}. \tag{2.2}$$

Note que o grau de $g(X)$ é no máximo $k-1$. Por hipótese de indução, existe um polinômio $q'(X)$ com coeficientes em A e um elemento r de A tais que:

$$g(X) = (X-a)q'(X) + r. \tag{2.3}$$

Substituindo (2.2) em (2.16), obtemos que

$$\begin{aligned} f(X) - (X-a)f_k X^{k-1} &= (X-a)q'(X) + r \\ f(X) &= (X-a)[a_f X^{k-1} + q'(X)] + r \end{aligned}$$

e (2.1) segue para $f(X)$. Logo estabelecemos o resultado por indução. □

Proposição 8. *Seja $f(X)$ um polinômio não-nulo com coeficientes em um anel A sem divisores de zero. Se o grau de $f(X)$ é n, então $f(X)$ possui no máximo n raízes em A.*

Demonstração. A demonstração será feita por indução em n. Se $n = 0$, então $f(X)$ é uma constante não-nula e não possui raiz. O resultado segue. Suponha que $n \geq 1$. Se $f(X)$ não possui raízes em A, então o resultado segue. Podemos assumir que $f(X)$ possui uma raiz em A, digamos a. Pelo Lema 8, exsite polinômio $q(X)$ com coeficientes em A tal que:

$$f(X) = (X-a)q(X) + f(a) = (X-a)q(X).$$

Como o grau de $q(X)$ é $n-1$, por hipótese de indução, $q(X)$ possui no máximo $n-1$ raízes em A. Para concluir a prova, será suficiente mostrar que toda raiz b de $f(X)$ diferente de a é raiz de $q(X)$. De fato,

$$0 = f(b) = (b-a)q(b)$$

e daí $q(b) = 0$ porque $b-a$ é diferente de zero e A não possui divizores de zero. □

2.3.1 Exercícios

1. Liste todos os divisores de zero de $\mathbb{Z}_{45}$.

2. Encontre todos os valores inteiros de X que satisfazem cada uma das congruências abaixo:

   (i) $5X \equiv 3 \mod 9$;

   (ii) $6X \equiv 3 \mod 9$;

   (iii) $6X \equiv 4 \mod 9$;

(iv) $2X + 3 \equiv 5X = 9 \mod 13$;

(v) $X^2 \equiv 1 \mod 16$.

3. Suponha que a, b, d e n são números naturais tais que $(a, n) = d$. Quantas soluções, em $\mathbb{Z}_n$, possui a equação

$$\overline{a}X = \overline{b}$$

quando:

(i) d divide b.

(ii) d não divide b.

Descreva quais são as soluções.

4. Para um natural n tal que $n \geq 2$, mostre que o inverso multiplicativo de um elemento de $\mathbb{Z}_n$, quando existe, é único.

5. Para um anel A, mostre que $A[X]$ também é um anel.

6. Sejam $f(X)$ e $g(X)$ polinômios com coeficientes em um anel A. Quando o coeficiente lider de $g(X)$ é igual a 1, mostre que existem polinômios $q(X)$ e $r(X)$ tais que

$$f(X) = q(X)g(X) + r(X),$$

com o grau de $r(X)$ menor que o de $g(X)$.

2.4 O Pequeno Teorema de Fermat

O próximo teorema, que foi demonstrado por Fermat, é uma conseqüência de um resultado bem mais geral obtido por Euler, que será apresentado ao final desta seção. Dada a sua celebridade, o estabeleceremos diretamente.

Teorema 7 (Pequeno Teorema de Fermat)**.** *Se p é primo, então $a^p \equiv a \mod p$, para todo inteiro a.*

Demonstração. Basta mostrar que este resultado vale quando a é natural, pois feito isso, é facilmente estendido aos inteiros. Usaremos indução em a.

O resultado é trivialmente satisfeito para $a = 1$. Suponha que $a \geq 1$ e que $a^p \equiv a \mod p$. Pelo binômio de Newton,

$$\begin{aligned}(a+1)^p &= a^p + \binom{p}{p-1}a^{p-1} + \cdots + \binom{p}{i}a^i + \cdots + \binom{p}{1}a + 1 \\ &\equiv a^p + 1 \mod p \\ &\equiv a + 1 \mod p.\end{aligned}$$

A primeira congruência segue pois

$$\binom{p}{i} \equiv 0 \mod p,$$

para todo $1 \leq i \leq p-1$ e a segunda por indução. Conseqüentemente o resultado vale para a. □

Agora, através de um exemplo, mostraremos que o resultado anterior não caracteriza números primos. O número 1729 é o produto dos seguintes números (primos): $7, 13$ e 19. Pelo resultado acima, temos que $a^{19} \equiv a \mod 19$. Caso $(a, p) = 1$, a possui inverso em $\mathbb{Z}_{19}$, e podemos multiplicar essa congruência pelo inverso de a e obter $a^{18} \equiv 1 \mod 19$. Como 36 divide 1728, então 1728=18b, para algum natural b, e elevando toda essa congruência ao expoente b chegamos a $(a^{18})^b = a^{18b} = a^{1728} \equiv 1 \mod 19$, que é válida para todo a que não é múltiplo de 19. Multiplicando toda a congruência por a temos que

$$a^{1729} \equiv a \mod 19,$$

que é válida para todo inteiro a. Logo 19 divide $a^{1729} - a$. De maneira análoga mostra-se que 7 e 13 também dividem $a^{1729} - a$, o mesmo ocorrendo com o produto desses primos que é 1729. Acabamos de mostrar que

$$a^{1729} \equiv a \mod 1729,$$

vale para todo inteiro a. Em outras palavras, existem expoentes não primos para os quais a conclusão do Pequeno Teorema de Fermat é válida. Um natural desse tipo é dito de Carmichael.

Quando $\gamma(x)$ denota o número de naturais de Carmichael menores ou iguais a x, sabe-se que, para x suficientemente grande, as seguintes desigualdades valem:

$$x^{\frac{2}{7}} < \gamma(x) < x^{1-\frac{\ln\ln\ln x}{\ln\ln x}}.$$

(Em particular, existe um número infinto destes naturais.) Consideraremos estes números mais uma vez quando tratarmos de algoritmos para decidir primalidade.

Seja n um número natural maior que 1. Se $a \in \mathbb{Z}_n^*$, então os seguintes elementos também pertencem a $\mathbb{Z}_n^*$:

$$\overline{1} = a^0, a^1, a^2, a^3, a^4, \ldots, a^m, \ldots$$

(Lembre-se que $\mathbb{Z}_n^*$ é fechado com relação ao produto.) Como $\mathbb{Z}_n^*$ é finito, pelo princípio da casa dos pombos, existem inteiros não-negativos i e j tais que $i \neq j$ e

$$a^i = a^j,$$

digamos $i < j$. Escolha (i, j) tal que j seja o menor possível. Multiplicando i vezes ambos os lados da igualdade anterior pelo inverso multiplicatio de a, que será denotado por a^{-1}, obtemos que

$$a^0 = a^{j-i}.$$

Pela escolha de j, temos que $j - i = j$ e daí $i = 0$. Diremos que j é a *ordem* de a em $\mathbb{Z}_n^*$. Em particular, j será o menor inteiro positivo tal que $a^j = \overline{1}$. A seguir apresentamos o Teorema de Lagrange:

Teorema 8 (Teorema de Lagrange)**.** *Seja a um elemento de $\mathbb{Z}_n^*$ com ordem j, onde n é um natural maior que 1. Se $a^k = \overline{1}$, então j divide k.*

Demonstração. Pelo Teorema 4, existem inteiros q e r tais que

$$k = qj + r \text{ e } 0 \leq r < j.$$

Conseqüentemente

$$\overline{1} = a^k = a^{qj+r} = (a^j)^q a^r = (\overline{1})^q a^r = a^r.$$

Pela definição de ordem, concluímos que $r = 0$ e, portanto, j divide k. □

Vamos utilizar o resultado anterior para determinar a ordem do elemento $\overline{2}$ em $\mathbb{Z}_{97}^*$, que será denotada por j. Como 97 é um número primo, pelo Pequeno Teorema de Fermat, temos que

$$(\overline{2})^{97} = \overline{2}. \tag{2.4}$$

Observe que $\overline{2}$ possui inverso multiplicativo em $\overline{Z}_{97}^*$, pois $(2, 97) = 1$. Multiplicando (2.4) pelo inverso multiplicativo de $\overline{2}$ em ambos os lados, obtemos que:

$$(\overline{2})^{96} = \overline{1}.$$

Pelo Teorema de Lagrange, j divide 96. Logo

$$j \in \{1, 2, 4, 8, 16, 32, 3, 6, 12, 24, 48, 96\}. \tag{2.5}$$

Observe que:

$$(\overline{2})^1 = \overline{2}, (\overline{2})^2 = \overline{4}, (\overline{2})^4 = \overline{16}, (\overline{2})^8 = \overline{62}, (\overline{2})^{16} = \overline{61}, (\overline{2})^{32} = \overline{35}.$$

Podemos calcular as outras potências de $\overline{2}$ da mesma forma. Iniciamos com a menor e depois elevamos ao quadrado sucessivamente.

$$(\overline{2})^3 = \overline{8}, (\overline{2})^6 = \overline{64}, (\overline{2})^{12} = \overline{22}, (\overline{2})^{24} = \overline{96}, (\overline{2})^{48} = \overline{1}, (\overline{2})^{96} = \overline{1}.$$

Por (2.5), temos que $j = 48$. Portanto, no caso em que n é primo, o Pequeno Teorema de Fermat e o Teorema de Lagrange nos permite calcular, através da significativa redução de candidatos, a ordem de qualquer elemento de $\mathbb{Z}_n^*$. A seguir, apresentamos o Teorema de Euler, que juntamente com o Teorema de Lagrange, restringe as possíveis ordens dos elementos de $\mathbb{Z}_n^*$, no caso em que n é um número composto.

A função phi de Euler de um natural n é definda como:

$$\phi(n) = |\{k : 1 \leq k \leq n \text{ e } (k, n) = 1\} = |\mathbb{Z}_n^*|.$$

Observe que:

Lema 9. *Seja p um número primo. Se $r \in \mathbb{N}$ e $r \neq 0$, então $\phi(p^r) = p^{r-1}(p-1)$.*

Demonstração. O conjunto $\{k : 1 \leq k \leq p^r \text{ e } (k, p^r) \neq 1\} = \{kp : 1 \leq k \leq p^{r-1}\}$ tem cardinalidade p^{r-1}. Conseqüentemente, o seu complementar em $\{k : 1 \leq k \leq p^r\}$, que é o valor de $\phi(p^r)$, tem cardinalidade $p^r - p^{r-1}$. □

Teorema 9 (Teorema de Euler)**.** *Seja n um número natural maior que 1. Se $a \in \mathbb{Z}_n^*$, então $a^{\phi(n)} = \overline{1}$.*

Note que o Pequeno Teorema de Fermat é uma conseqüência dos dois resultados anteriores.

Demonstração do Teorema de Euler. Seja $\sigma : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ dada por $\sigma(x) = ax$. Note que σ é injetiva. Como $\mathbb{Z}_n^*$ é finito, temos que σ é também sobrejetiva. Portanto, σ é uma bijeção dos elementos de $\mathbb{Z}_n^*$. Logo

$$\prod_{x \in \mathbb{Z}_n^*} x = \prod_{x \in \mathbb{Z}_n^*} \sigma(x) = \prod_{x \in \mathbb{Z}_n^*} (ax) = a^{\phi(n)} \prod_{x \in \mathbb{Z}_n^*} x.$$

Logo $a^{\phi(n)} = 1$ e o resultado segue. □

2.4.1 Exercícios

1. Mostre que, para todo inteiro n, $n^5 - n$ é divisível por 30.

2. Mostre que um número de Carmichel é livre de quadrados.

3. Calcule a ordem de $\overline{3}$ em $\mathbb{Z}_{97}^*$.

4. Calcule a ordem de $\overline{2}$ em $\mathbb{Z}_{93}^*$.

5. Seja a um elemento de $\mathbb{Z}_{1801}^*$ com ordem 900. Encontre a ordem de a^{125}, a^{30}, a^{97} e a^{614}. (Você é capaz de encontrar tal elemento?)

6. Sejam p e q números primos distintos. Para números naturais r e s, calcule $\phi(p^r q^s)$.

2.5 A exponenciação é rápida

Seja n um número natural excedendo 1 que manteremos fixo. Nesta seção iremos discutir o custo de calcular uma potência de um elemento pertencente ao conjunto $\mathbb{Z}_n$. Mostraremos que este custo é polinomial.

Escolha um elemento a de $\mathbb{Z}_n$. Para um natural m, desejamos calcular a^m. O primeiro passo é escrever m na base 2: existem inteiros não-nagativos $k, d_0, d_1, \ldots, d_k$ tais que $d_i \in \{0,1\}$, para todo $i \in \{0,1,\ldots,k-1\}$, $d_k = 1$ e

$$m = \sum_{i=0}^{k} d_i 2^i = d_0 2^0 + d_1 2^1 + d_2 2^2 + \cdots + d_k 2^k.$$

(Assumiremos que esta passagem não contribui com o custo do algoritmo, já que o computador trabalha com inteiros escritos na base 2.) Conseqüentemente

$$\begin{aligned} a^m &= a^{d_0 2^0 + d_1 2^1 + d_2 2^2 + \cdots + d_k 2^k} \\ &= a^{d_0 2^0} a^{d_1 2^1} a^{d_2 2^2} \cdots a^{d_k 2^k} \\ &= \left(a^{2^0}\right)^{d_0} \left(a^{2^1}\right)^{d_1} \left(a^{2^2}\right)^{d_2} \cdots \left(a^{2^k}\right)^{d_k}. \end{aligned}$$

Desta forma, calcularemos esta potência usando a seguinte relação:

$$a^m = \prod_{i:d_i=1} a^{2^i}. \tag{2.6}$$

Finalizamos o cômputo de a^m da seguinte maneira:

(i) calculando as potências $a^{2^0}, a^{2^1}, a^{2^2}, \ldots, a^{2^k}$; e

(ii) multiplicando as potências encontradas no item anterior que fazem parte do produtório (2.6).

Note que realizamos no máximo k multiplicações em $\mathbb{Z}_n$ para executar o item (ii). Já para o item (i), são necessárias exatamente k multiplicações para calcular todas as potências listadas, pois a seguinte será sempre igual ao quadrado da anterior. Portanto, o

número de multiplicações realizadas em $\mathbb{Z}_n$ para calcular a^m será no máximo $2k = O(\log_2 m)$. Como cada multiplicação em $\mathbb{Z}_n$ envolve uma multiplicação e uma divisão de números naturais com no máximo $2\text{dig}(n)$, o custo de realizar uma multiplicação em $\mathbb{Z}_n$ é igual a $O(\log_2^2 n)$. Portanto, o custo de calcular a m-ésima potência de a em $\mathbb{Z}_n$ é $O(\log_2^2 n \log_2 m)$.

Para ilustrar este algoritmo, vamos calcular $\overline{3}^{48}$ em $\mathbb{Z}_{97}$. Note que $48 = 2^4 + 2^5$. Logo $\overline{3}^{48} = \overline{3}^{2^4}\overline{3}^{2^5}$. Observe que

$$\begin{aligned}
\overline{3}^{2^0} &= \overline{3} \\
\overline{3}^{2^1} &= \left(\overline{3}^{2^0}\right)^2 = \overline{3}^2 = \overline{9} \\
\overline{3}^{2^2} &= \left(\overline{3}^{2^1}\right)^2 = \overline{9}^2 = \overline{81} \\
\overline{3}^{2^3} &= \left(\overline{3}^{2^2}\right)^2 = \overline{81}^2 = \overline{62} \\
\overline{3}^{2^4} &= \left(\overline{3}^{2^3}\right)^2 = \overline{62}^2 = \overline{61} \\
\overline{3}^{2^5} &= \left(\overline{3}^{2^4}\right)^2 = \overline{61}^2 = \overline{35}
\end{aligned}$$

Conseqüentemente $\overline{3}^{48} = \overline{3}^{2^4}\overline{3}^{2^5} = \overline{61}\,\overline{35} = \overline{1}$.

Vimos que o algoritmo apresentado para o cálculo da exponencial em $\mathbb{Z}_n$ é polinomial. Este mesmo algoritmo (e qualquer outro) utilizado para calcular potências de inteiros será exponencial, pois o número de dígitos do resultado será exponencial. Se a e m são naturais, então

$$\text{dig}(a^m) \approx m\text{dig}(a) \approx 2^{\text{dig}(m)}\text{dig}(a).$$

(Para verificar estas aproximações, utilize que $\text{dig}(n) \approx \log_2 n$, para todo natural n.)

2.5.1 Exercícios

1. Caso exista, encontre o menor natural a tal que $a \geq 2$ e a ordem de $\overline{a}$ é igual a 96 em $\mathbb{Z}_{97}$.

2. Qual a maior ordem de um elemento de $\mathbb{Z}_{93}$?

2.6 O Teorema de Wilson

Vimos que o Pequeno Teorema de Fermat não é suficiente para caracterizar números primos. A seguir apresentamos uma caracterização para números primos que, do ponto de vista de aplicações, tem se mostrado de pouca utilidade porque não se conhece um algoritmo eficiente para calcular o fatorial de um número módulo um outro.

Teorema 10 (Teorema de Wilson)**.** *Um número natural n maior que 1 é primo se e somente se* $(n-1)! \equiv -1 \mod n$.

Demonstração. No caso em que n é composto e $n \neq 4$, mostraremos que:

$$(n-1)! \equiv 0 \mod n. \tag{2.7}$$

Por definição, existem naturais a e b tais que $n = ab$ e $1 < a \leq b < n$. Se $a \neq b$, então $(n-1)!$ é múltiplo de n, pois $\{a, b\} \subseteq \{1, 2, \ldots, n-1\}$. Neste caso (2.7) segue. Podemos supor que $a = b$. Se $2b \leq n-1$, então $(n-1)!$ é múltiplo de n, pois $\{a, 2b\} \subseteq \{1, 2, \ldots, n-1\}$. Mais uma vez (2.7) é verificada. Podemos assumir também que $n-1 < 2b$. Portanto

$$2b \geq n = ab = 2b + (a-2)b \geq 2b.$$

Logo temos as igualdades nesta inequação e conseqüentemente $a = b = 2$. Isto é, $n = 4$. Mas $(4-1)! = 6 \equiv 2 \mod 4$.

Agora suponha que n é primo. Neste caso, todo elemento de $\mathbb{Z}_n^* = \{\overline{a} : a \in \{1, 2, \ldots, n-1\}\}$ possui um inverso multiplicativo (que é único). Para cada $a \in \{1, 2, \ldots, n-1\}$, seja a' o único elemento de $\{1, 2, \ldots, n-1\}$ tal que $\overline{a'}$ é o inverso multiplicativo de $\overline{a}$ em $\mathbb{Z}_n$. Note que $\mathcal{X} = \{\{a, a'\} : a \in \{1, 2, \ldots, n-1\}\}$ é uma partição de $\{1, 2, \ldots, n-1\}$. Portanto,

$$(n-1)! = \prod_{A \in \mathcal{X}} \prod_{a \in A} a. \tag{2.8}$$

Se $A \in \mathcal{X}$ e $|A| = 2$, então

$$\prod_{a \in A} a \equiv 1 \mod n. \tag{2.9}$$

Substituindo (2.9), para todo $A \in \mathcal{X}$ tal que $|A| = 2$, em (2.8), temos que:

$$(n-1)! \equiv \prod_{a \in \{1,2,\ldots,n-1\}:\{a\} \in \mathcal{X}} a \mod n. \tag{2.10}$$

Necessitamos obter todos $a \in \{1, 2, \ldots, n-1\}$ tais que $\{a\} \in \mathcal{X}$. Por definição, $a = a'$ e daí

$$a^2 \equiv 1 \mod n.$$

Podemos reescrever esta equivalência como:

$$(a-1)(a+1) = a^2 - 1 \equiv 0 \mod n.$$

Logo n divide $a-1$ ou $a+1$ porque n é primo. Como $a \in \{1, 2, \ldots, n-1\}$, obtemos que $a = 1$ ou $a = n-1$. Por (2.10),

$$(n-1)! \equiv (n-1) \equiv -1 \mod n$$

e o resultado segue. □

Exercícios

1. Seja n um número primo ímpar, digamos $n = 2m + 1$. Para cada $b \in \{1, 2, \ldots, n-1\}$, mostre que:

   (i) $b^m \equiv 1 \mod n$ quando b é um *resíduo quadrático módulo* n (isto é, existe inteiro a tal que $a^2 \equiv b \mod n$).

   (ii) Para cada $a \in \{1, 2, \ldots, n-1\}$, existe um único $a' \in \{1, 2, \ldots, n-1\}$ tal que $aa' \equiv b \mod n$. Mais ainda, $a \neq a'$ quando b não é um resíduo quadrático módulo n.

   (iii) $b^m \equiv -1 \mod n$ quando b não é um resíduo quadrático módulo n.

   (Este critério é devido a Euler e será considerado também na última seção deste capítulo.)

2. Caso existisse um algoritmo eficiente para encontrar o fatorial de um natural módulo um outro, mostre que existiria um algoritmo eficiente para fatorar qualquer natural como produto de primos.

2.7 Teorema Chinês dos Restos

Há mais de mil anos, um general chinês desejava saber exatamente quantos soldados tinha em seu exército. Estimou que este número estava entre 500 e 1000. Para determiná-lo precisamente, utilizou o método descrito a seguir. Ordenou que seus soldados entrassem em uma formação com colunas de 9 soldados e contou o número de soldados que não puderam ser arranjados em uma destas colunas. Foram 3. Repetiu o procedimento com colunas de tamanho 10 e 11 e descobriu que sobraram respectivamente 4 e 10 soldados. Para chegar ao tamanho do seu exército, o general resolveu o problema matemático detalhado no próximo parágrafo. Este fato é verídico exceto pelos números envolvidos.

Encontre o menor natural a cujos restos quando dividido por 9, 10 e 11 são respectivamente 3, 4 e 10. Existe natural q tal que $a = 9q + 3$. Como $a \equiv 4 \mod 10$, temos que $9q \equiv 1 \mod 10$ e daí $q \equiv 9 \mod 10$. Como $a \equiv 10 \mod 11$, temos que $9q \equiv 7 \mod 11$ e daí $q \equiv 2 \mod 11$. Isto é, q deixa resto 9 e 2 quando dividido respectivamente por 10 e 11. Em particular, existe inteiro q' tal que $q = 10q' + 9$. Como $q \equiv 2 \mod 11$, temos que $10q' \equiv 4 \mod 11$ e daí $q' \equiv 7 \mod 11$. Tomando $q' = 7$, temos que $q = 79$ e $a = 714$. O próximo resultado, afirma que os outros inteiros com esta propriedade são da forma $714 + 990b$, para algum inteiro b. Em sua demonstração está implícito o algoritmo que acabamos de utilizar para resolver o problema do general chinês. Portanto, seu exército tinha 714 soldados.

Utilizando indução, reduziremos o problema geral ao caso em que apenas duas divisões são feitas. Analisaremos este caso separadamente. Sejam n_1 e n_2 números naturais não-nulos. Para inteiros r_1 e r_2 tais que $0 \leq r_1 < n_1$ e $0 \leq r_2 < n_2$, existe inteiro a que quando dividido por n_i deixa resto r_i, para $i \in \{1, 2\}$? Como a deixa resto r_1 quando dividido por n_1, existe inteiro não-negativo q tal que

$$a = qn_1 + r_1 \tag{2.11}$$

Quando dividido por n_2, a deixa resto r_2. Logo

$$qn_1 + r_1 \equiv r_2 \mod n_2.$$

Conseqüentemente

$$qn_1 \equiv r_2 - r_1 \mod n_2. \tag{2.12}$$

Note que existe q satisfazendo (2.12) se e somente se (n_1, n_2) divide $r_2 - r_1$. Este será sempre o caso quando $(n_1, n_2) = 1$. (Vamos assumir esta hipótese extra ao enunciar o Teorema Chinês dos Restos.) Podemos escolher q satisfazendo $0 \leq q < n_2$. Por (2.11), obtemos que

$$0 \leq a < n_1 n_2. \tag{2.13}$$

Teorema 11 (Teorema Chinês dos Restos)**.** *Para um natural não-nulo k, suponha que $m_1, m_2, \ldots, m_k$ são naturais não-nulos tais que $(m_i, m_j) = 1$, para todo 2-subconjunto $\{i, j\}$ de $\{1, 2, \ldots, n\}$. Se $r_1, r_2, \ldots, r_k$ são inteiros, então existe um único inteiro X tal que $0 \leq X < m_1 m_2 \cdots m_k$ e*

$$\begin{cases} X \equiv r_1 \mod m_1 \\ X \equiv r_2 \mod m_2 \\ \qquad \cdots \\ X \equiv r_k \mod m_k \end{cases} \tag{2.14}$$

Mais ainda, X' é uma outra solução para (2.14) *se e somente se*

$$X \equiv X' \mod m_1 m_2 \cdots m_k. \tag{2.15}$$

Demonstração. Observe que não perdemos generalidade assumindo que $0 \leq r_i < m_i$, para todo $i \in \{1, 2, \ldots, k\}$. Começaremos estabelecendo a existência de uma solução para (2.14). Faremos a demonstração por indução do primeiro tipo em k. Se $k = 1$, então a solução será $X = r_1$ e o resultado segue. Suponha que exista solução para qualquer sistema com $k - 1$ equações. Em particular, seja $0 \leq r_2' < m_2 \cdots m_k$ uma solução de:

$$\begin{cases} X \equiv r_2 \mod m_2 \\ \qquad \cdots \\ X \equiv r_k \mod m_k \end{cases}$$

Como $(m_1, m_2 \cdots m_k) = 1$, pelo argumento que precede este demonstração, existe solução X para o sistema

$$\begin{cases} X \equiv r_1 \mod m_1 \\ X \equiv r_2' \mod m_2 \cdots m_k \end{cases}$$

tal que $0 \leq X < m_1 m_2 \cdots m_k$. Note que X também é solução de (2.14)

Agora consideraremos a unicidade. Se X e X' são soluções de (2.14), então m_i divide $X - X'$ para todo i. Logo $X - X'$ é divisível por $m_1 m_2 \cdots m_k$. Portanto, existe uma única solução no intervalo $[0, m_1 m_2 \cdots m_k)$. □

Suponha que $m_1, m_2, \ldots, m_k$ são naturais dois a dois relativamente primos. Tome $m = m_1 m_2 \cdots m_k$. O Teorema Chinês dos Restos afima que a seguinte função $\Psi : \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$ definida por $f(\overline{a}) = (\overline{a}, \overline{a}, \ldots, \overline{a})$, para um inteiro a, é uma bijeção. (Esta notação não é muito feliz, pois $\overline{a}$ foi utilizado nesta expressão com $k+1$ significados diferentes: na primeira aparição foi utilizado para denotar a classe de equivalência de a módulo m; na segunda, módulo m_1; na terceira módulo m_2; e na última módulo m_k.) Como Ψ induz uma bijeção entre $\mathbb{Z}_m^*$ e $\mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \cdots \times \mathbb{Z}_{m_k}^*$, temos que

$$\begin{aligned} |\mathbb{Z}_m^*| &= |\mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \cdots \times \mathbb{Z}_{m_k}^*| \\ |\mathbb{Z}_m^*| &= |\mathbb{Z}_{m_1}^*||\mathbb{Z}_{m_2}^*| \cdots |\mathbb{Z}_{m_k}^*| \\ \phi(m) &= \phi(m_1)\phi(m_2) \cdots \phi(m_k). \end{aligned}$$

(Diremos que ϕ é multiplicativa.) Se $m_i = p_i^{u_i}$, para algum primo p_i e natural u_i, então:

$$m = p_1^{u_1} p_2^{u_2} \cdots p_k^{u_k} \text{ e } \phi(m) = p_1^{u_1 - 1}(p_1 - 1) p_2^{u_2 - 1}(p_2 - 1) \cdots p_k^{u_k - 1}(p_k - 1).$$

Para o próximo resultado, utilizaremos a notação $d|n$ com o seguinte significado: d e n são números naturais não-nulos e d divide n.

Lema 10. *Se n é um número natural não-nulo, então*

$$n = \sum_{d|n} \phi(d).$$

Demonstração. Para cada natural d que divide n, considere o conjunto:

$$\mathcal{X}_d = \left\{ m \in \mathbb{N} : 1 \leq m \leq n \text{ e } (m,n) = \frac{n}{d} \right\}.$$

Observe that $a \in \mathcal{X}_d$ se e somente se $a = \frac{n}{d}a'$, para algum natural a' satisfazendo $a' \leq d$ e $(a', d) = 1$. Portanto,

$$|\mathcal{X}_d| = \phi(d). \tag{2.16}$$

O resultado segue de (2.16), pois $\{\mathcal{X}_d : d|n\}$ é uma partição de $\{1, 2, \ldots, n\}$. □

2.7.1 Exercícios

1. Encontre todos os inteiros que quando divididos por
   (i) 5, 7 e 17 deixam respectivamente restos 2, 4 e 12.
   (ii) 4, 9, 11 e 21 deixam respectivamente restos 1, 2, 3 e 4.
   (iii) 15 e 18 deixam respectivamente restos 4 e 7.
   (iv) 12 e 16 deixam respectivamente restos 3 e 13.

2. Mostre que o polinômio $X^2 - \overline{1}$ possui pelo menos 2^k raízes em $\mathbb{Z}_n$, quando n é um natural ímpar divisível por pelo menos k primos distintos e diferentes de 2.

3. Encontre todos os naturais n tais que $\phi(n) \leq 10$.

4. Calcule $\phi(318.322.261.169)$ e $\phi(1.461.660.310.351)$.

5. Encontre o resto da divisão de $11^{56.234.100}$ por 210.

6. Seja $\mathcal{P}$ o conjunto dos primos que dividem um natural n. Mostre que:
$$\frac{\phi(n)}{n} = \prod_{p \in \mathcal{P} : p|n} \left(1 - \frac{1}{p}\right).$$

7. Usando o exercício anterior, mostre que, para todo natural n que é divisível por no máximo 5 primos distintos,
$$\phi(n) \geq \frac{16}{77}n.$$
Para que naturais vale a igualdade?

8. Para um natural m, definimos:

$$N_\phi(m) = |\{n \in \mathbb{N} : \phi(n) = m\}|.$$

Mostre que:

(i) Existem infinitos naturais que são zeros da função N_ϕ. (Considere os números da forma $2 \cdot 7^k$, com $k \geq 1$.)

(ii) Não existe natural m tal que $N_\phi(m) = 1$.

(iii) Não existe natural m tal que $N_\phi(m) = \infty$.

(iv) Para $k \geq 1$, $N_\phi(2 \cdot 3^{6k+1}) = 2$.

9. Sobre a função Ψ definida no último parágrafo desta seção, mostre que:

(i) Está bem definda.

(ii) É injetiva.

(iii) Utilizando os dois itens anteriores, conclua que é bijetiva (obtendo uma demonstração alternativa para o Teorema Chinês dos Restos).

2.8 Existência de geradores

Seja n um natural maior que 1. Um elemento a de $\mathbb{Z}_n^*$ é dito um *gerador* de $\mathbb{Z}_n^*$ quando a ordem de a em $\mathbb{Z}_n^*$ é igual a $\phi(n)$. Neste caso,

$$\mathbb{Z}_n^* = \{a^1, a^2, \ldots, a^{\phi(n)}\} = \{a^i : i \in \mathbb{N}\}.$$

Isto é, os elementos de $\mathbb{Z}_n^*$ são potências do gerador — daí a importância deste. Nesta seção, mostraremos que $\mathbb{Z}_{p^k}$, para p primo e $k \geq 1$, possui um gerador. Este fato é essencial para estimar a probabilidade de erro do segundo algoritmo randomizado para decidir primalidade que discutiremos no Capítulo 4. Iniciaremos determinando a ordem de uma potência de um elemento (como função da ordem do elemento).

Lema 11. *Seja n um natural maior que 1. Se a é um elemento de $\mathbb{Z}_n^*$ com ordem j, então a^i tem ordem $\frac{j}{(i,j)}$.*

Demonstração. Seja k a ordem de a^i. Por definição, k é o menor natural tal que

$$(a^i)^k = a^{ik} = \overline{1}.$$

Pelo Teorema 8, k é o menor natural tal que j divide ik. Portanto, $k = \frac{j}{(i,j)}$. □

Proposição 9. *Seja p um número primo. Se $d|p-1$, então $\mathbb{Z}_p^*$ possui exatamente $\phi(d)$ elementos de ordem d. Em particular, $\mathbb{Z}_p^*$ possui $\phi(p-1) \neq 0$ geradores.*

Demonstração. Para $d|p-1$, denote por $\lambda(d)$ o número de elementos de $\mathbb{Z}_p^*$ de ordem d. Primeiro estabeleceremos que

$$\lambda(d) \in \{0, \phi(d)\}. \tag{2.17}$$

If $\lambda(d) = 0$, então (2.17) segue. Suponha que $\mathbb{Z}_p^*$ tenha elemento de ordem d, digamos a. Seja $f(X) = X^d - \overline{1}$. Para todo $i \in \mathbb{N}$,

$$f(a^i) = (a^i)^d - \overline{1} = (a^d)^i - \overline{1} = (\overline{1})^i - \overline{1} = \overline{0}.$$

Conseqüentemente $a^1, a^2, \ldots, a^d$ são raízes duas a duas distintas de $f(X)$. Pela Proposição 8, estas são todas as raízes de $f(X)$. Logo temos de determinar quais destas tem ordem d, já que todo elemento de ordem d é raiz deste polinômio. Pelo Lema 11, a^i tem ordem d se e somente se $(i,d) = 1$. Portanto, $\phi(d)$ destas raízes tem ordem d e (2.17) segue.

Pelo Pequeno Teorema de Fermat e o Teorema de Lagrange, a ordem de um elemento de $\mathbb{Z}_p^*$ é um divisor de $p-1$. Logo

$$|\mathbb{Z}_p^*| = p - 1 = \sum_{d|p-1} \lambda(d) \leq \sum_{d|p-1} \phi(d) = p - 1,$$

onde a última igualdade segue do Lema 10 e a desigualdade da equação (2.17). Conseqüentemente temos de ter a igualdade acima e daí $\lambda(d) = \phi(d)$, para todo $d|p-1$. A primeira parte do lema segue. A segunda parte é imediata porque $|\mathbb{Z}_p^*| = p-1$ e $\phi(p-1) \neq 0$. □

Proposição 10. *Se p é um primo ímpar e k um natural, então $\mathbb{Z}_{p^k}^*$ possui um gerador.*

Demonstração. Fica como exercício para o leitor. (Sugestão: se $\overline{a}$, para um inteiro a, é um gerador de $\mathbb{Z}_p^*$, então $\overline{a}$ ou $\overline{a+p}$ é um gerador de $\mathbb{Z}_{p^k}^*$.) □

2.8.1 Exercícios

1. Encontre um gerador para $\mathbb{Z}_{31}^*$. Quais são todos os outros geradores de $\mathbb{Z}_{31}^*$?

2. Utilizando geradores, estabeleça o critério de Euler para decidir quais são os resíduos quadráticos módulo um primo ímpar. (Ver o primeiro exercícioda Seção 2.6.)

3. Utilizando os dois exercícios anterios, encontre todos os resíduos quadráticos módulo 31.

Capítulo 3

Criptografia

3.1 Introdução

Neste capítulo iniciaremos nossa discussão sobre criptografia, isto é, a técnica de ocultar de terceiros uma informação compartilhada. Por exemplo, deseja-se encaminhar o número do cartão de crédito em uma transação eletrônica de forma que apenas o dono do cartão e a empresa que está vendendo o produto consigam ter acesso a este dado. Neste caso, quem envia os seus dados pessoais transforma-os de forma que apenas a companhia envolvida na transação pode recuperá-los através de um procedimento que é de seu conhecimento apenas — caso a comunicação seja interceptada por alguém não autorizado, o conteúdo não é legível, pois a informação é acessível apenas para aqueles que possuem o algoritmo para decifrá-la que, no caso, é a firma.

Discutiremos procedimentos para ocultar a informação contida em uma mensagem e como recuperá-la. Necessitamos fixar um alfabeto para escrever estas mensagens. Para simplificar a argumentação, assumiremos que o alfabeto contém 24 letras, que são:

`A B C D E F G H I J L M N O P Q R S T U V X Z b`

onde o `b` denota o espaço em branco. Para transações utilizando a rede mundial de computadores, o alfabeto nas quais as mensagens são escritas possuem como letras todos os símbolos que podem ser

digitados no teclado de computador. Logo tem 106 letras. Mais ainda, iremos assumir que o alfabeto é ordenado, como está escrito acima, isto é, a primeira letra é o `A`, a segunda o `B` e assim por diante. Denotaremos este alfabeto por $\mathcal{A}_{\text{P}}$.

A maneira mais simples de encifrar uma mensagem é através da substituição, em todo o texto, de cada letra por uma outra que é obtida pelo resultado de uma permutação escolhida previamente. Como exemplo, utilizaremos uma permutação das letras que já foi utilizada há mais de dois mil anos para encifrar mensagens, que é a seguinte. A imagem da letra que está na primeira linha, por esta permutação, é a letra que está abaixo desta na segunda linha.

```
A B C D E F G H I J L M N O P Q R S T U V X Z b
D E F G H I J L M N O P Q R S T U V X Z b A B C
```

Mais a frente, explicaremos como esta permutação pode ser descrita matematicamente. Considere o seguinte texto a ser encifrado:

```
FINALMENTE INICIAMOS O ESTUDO DE CRIPTOGRAFIA
```

Devemos sempre substituir: o `F` pelo `I`; o `I` pelo `M`; o `N` pelo `Q`; e assim por diante. No final obtemos o seguinte texto:

```
IMQDOPHQXHCMQMFMDPRVCRCHVXbGRCGHCFUMSXRJUDIMD
```

Ao encifrar a mensagem, cometemos um erro! Você é capaz de descobrir qual letra foi substituída de maneira equivocada? Para decifrar a mensagem, usa-se a permutação inversa. Portanto, para que terceiros não tenham acesso a mensagem original, caso tenham interceptado a mensagem encifrada, a permutação tem de ser matida em segredo pelas partes que trocam a mensagem.

Lembrar uma permutação das letras do alfabeto não é uma tarefa fácil. Por este motivo, sistemas de criptografia utilizados, na vida real, por vários usuários, optaram por um dos seguintes métodos para construir estas permutações, pois não é prudente manter a permutação utilizada registrada em papel na mão de inúmeros usuários — pode ser capturada por terceiros interessados em decifrar as mensagens:

- São dadas por regras matemáticas simples e fáceis de serem lembradas.

- São obtidas a partir de máquinas que podem ser configuradas de várias formas.

A segunda maneira não nos interessa muito. Focaremos nossa atenção na primeira. Contudo apresentamos um exemplo para ilustrar a segunda técnica. Ocorreu na segunda guerra mundial. Os alemães tinham uma máquina chamada de Enigma que podia ser configurada de

$$\frac{3!26^3}{10!}\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}\binom{16}{2}\binom{14}{2}\binom{12}{2}\binom{10}{2}\binom{8}{2}$$

maneiras diferentes. Eeste número na base decimal é gigantesco

$$15.896.255.521.782.636.000$$

Mesmo de posse de uma destas máquinas, os ingleses levaram muito tempo para quebrar o sistema de criptografia alemão, já que ao final de cada dia, eram passadas instruções para a configuração da máquina que seria utilizada no seguinte. A quebra do sistema de cirptografia alemão foi fundamental para a vitória aliada, pois os submarinos alemães estavam afundando uma grande quantidade de navios que iam para o Reino Unido. A participação de Turing foi essencial para a quebra deste sistema porque ajudou a desenvolver um mecanismo eletrônico capaz de rapidamente considerar várias configurações da Enigma até encontrar a que estava sendo utilizada. Podemos considerar este mecanismo como um computador elementar e com um propósito muito bem definido. Depois da guerra, Turing tentou desenvolver o computador eletrônico, mas terminou sendo vencido por von Neumann, já que os Estados Unidos tinham uma quantidade ilimitada de recursos para financiar esta pesquisa.

Voltemos mais de dois mil anos no tempo. Iremos descrever o sistema de criptografia utilizado por Júlio Cesar para comunicar-se com Cícero. Utilizava aquela permutação que vimos anteriormente, mas o alfabeto era um pouco diferente. A descrição deste sistema é muito simples: considerando o alfabelo cíclico, substitua cada letra pela terceira que vem a sua direita. É facílimo de ser lembrado também. Podemos descrever a permutação por trás deste sistema matematicamente. Para cada letra do alfabeto associamos um inteiro pertencente ao intervalo $[0, 24)$. Ao `A` associamos o 0; ao `B` o 1;

ao C o 2; e assim por diante — daí a importância do alfabeto ser ordenado. Isto é, estamos associando à i-ésima letra do alfabeto o i-ésimo inteiro no intervalo $[0, 24)$. Como estes inteiros são precisamente os possíveis restos da divisão por 24, que é o tamanho do alfabeto, podemos associar a cada letra um elemento de $\mathbb{Z}_{24}$, a saber: a classe do inteiro associado a esta letra. Logo a permutação σ dos elementos de $\mathbb{Z}_{24}$ é dada pela expressão:

$$\sigma(X) = X + \overline{3}$$

Obtemos a permutação descrita no início da seção quando substituímos as classes de equivalência por letras.

Inspirado no sistema criado por Júlio Cesar podemos imaginar muitos outros sistemas de criptografia utilizando permutações dos inteiros módulo algum natural. Suponha que L seja o número de letras do alfabeto $\mathcal{A}$ a ser utilizado, que está ordenado. Existe uma bijeção natural entre cada letra do alfabelo e um elemento de $\mathbb{Z}_L$. Associe $\overline{n}$ a $(n+1)$-ésima letra do alfabeto, para todo inteiro n tal que $0 \leq n < L$. Sejam a e b elementos de $\mathbb{Z}_L$ tal que a possui inverso multiplicativo. Observe que $\sigma : \mathbb{Z}_L \to \mathbb{Z}_L$ dada por

$$\sigma(X) = aX + b$$

é uma bijeção de $\mathbb{Z}_L$. De fato, caso $Y = aX + b$, temos que $X = a^{-1}(Y - b)$. Portanto, para cada elemento Y de $\mathbb{Z}_L$, existe um único X em $\mathbb{Z}_L$ tal que $Y = \sigma(X)$. Isto é, σ é uma permutação. Chamamos a e b de *chaves* do sistema. Para referência futura, denotamos este sistema por $\mathrm{scl}_{\mathcal{A}}(a, b)$, onde scl são as iniciais de sistema de criptografia linear. De posse de a e b, podemos encifrar as mensagens e também decifrar, já que é muito fácil encontrar a permutação inversa de σ a partir de a e b. Para decifrar as mensagens usamos o sistema $\mathrm{scl}_{\mathcal{A}}(a^{-1}, -a^{-1}b)$.

Vamos considerar um exemplo. Voltemos ao alfabeto $\mathcal{A}_{\mathrm{P}}$. Sabemos que $\overline{u}$ tem inverso multiplicatio, para um inteiro u, se e somente se $(u, 24) = 1$. Por exemplo, $\overline{13}$. Considere a permutação σ de $\mathbb{Z}_{24}$ dada por

$$\sigma(X) = \overline{13}X + \overline{22}.$$

Observe que σ induz a seguinte permutação no nosso alfabeto:

```
A B C D E F G H I J L M N O P Q R S T U V X Z b
Z M A O C Q E S G U I X L B N b P D R F T H V J
```

Dois valores desta permutação estão errados. Você é capaz de encontrá-los?

Uma abordagem deste tipo é vulnerável por uma análise das letras mais ou menos freqüentes na língua em que o texto foi escrito ou, mais especificamente, sobre o assunto que foi escrito. Por exemplo, um texto sobre futebol em português tem como letras mais freqüentes `b` e `O` respectivamente. Suponha que, ao interceptar um texto encifrado sobre futebol, um terceiro descobre que as letras mais freqüentes são `J` e `b`. Logo saberá que `b` e `O` foram trocados respectivamente por `J` e `b`. Assumindo que quem interceptou a mensagem cifrada conhece o sitema de criptografia utilizado por quem a envia, que foi $\mathrm{scl}_{\mathcal{A}_\mathrm{P}}(a, b)$, exceto as chaves a e b, este pode descobrir as chaves resolvendo o seguinte sistema linear em $\mathbb{Z}_{24}$:

$$\begin{cases} \overline{23}a + b = \overline{9} \\ \overline{13}a + b = \overline{23} \end{cases}$$

A primeira equação informa que o `b` foi substituído pelo `J`. A segunda, que o `O` foi trocado pelo `b`. Subtraíndo da primeira a segunda, obtemos

$$\overline{10}a = \overline{10}.$$

Multiplicando esta equação pelo inverso de $\overline{5}$, encontramos que

$$\overline{2}a = \overline{2}.$$

Conseqüentemente $a = \overline{1}$ ou $a = \overline{13}$. Portanto, $(a, b) \in \{(\overline{1}, \overline{10}), (\overline{13}, \overline{22})\}$. Agora, basta verificar com qual destes dois pares de chaves pode-se decifrar a mensagem.

Na próxima seção explicarmos como é possível contornar esta abordagem para descobrir as chaves através da análise de freqüência de letras.

3.1.1 Exercícios

1. Resolva o sistema de equações lineares em $\mathbb{Z}_{23}$:

$$\begin{cases} \overline{11}X + \overline{14}Y = \overline{5} \\ \overline{13}X + \overline{2}Y = \overline{12} \end{cases}$$

   Faça o mesmo para o sistema:

$$\begin{cases} \overline{1}X + \overline{1}Y + \overline{1}Z = \overline{13} \\ \overline{2}X + \overline{4}Y + \overline{5}Z = \overline{13} \\ \overline{4}X + \overline{16}Y + \overline{1}Z = \overline{3} \end{cases}$$

2. Repita o exercício anterior substituindo $\mathbb{Z}_{23}$ por $\mathbb{Z}_{24}$.

3. Considere o seguinte sistema de equações lineares

$$\begin{cases} \overline{r}X + \overline{1}Y = \overline{u} \\ \overline{s}X + \overline{1}Y = \overline{v} \end{cases}$$

   onde r, s, u e v são inteiros. Para um natural n, com $n \geq 2$, determine quantas soluções em $\mathbb{Z}_n$ este sistema possui. (A resposta depende de n, r, s, u e v.)

4. Sejam f, g e h funções afins de $\mathbb{Z}_{24}$ em $\mathbb{Z}_{24}$ dadas por:

$$f(X) = \overline{6}X + \overline{11}, g(X) = \overline{14}X + \overline{5} \text{ e } h(X) = \overline{7}X + \overline{18}.$$

   Qual destas três funções é uma permutação de $\mathbb{Z}_{24}$? Utilizando esta função e o alfabeto $\mathcal{A}_{\mathrm{P}}$, encifre a seguinte mensagem:

```
O SANTA JOGA NA SEGUNDA DIVISAO DO
CAMPEONATO BRASILEIRO
```

5. A seguinte mensagem encifrada sobre futebol foi interceptada:

```
ZVCFZBJVPZMVLMSDIFHDZVHCJHVDQZVDZVbHQSHBVZVQDRJMSZ
```

   Sobre esta mensagem sabe-se que foi encifrada utilizando o sistema de criptografia $\mathrm{scl}_{\mathcal{A}_{\mathrm{P}}}(a, b)$, para chaves a e b. Utilizando a análise de freqüência, você é capaz de decifrar esta mensagem? Ao encifrar a mensagem, cometemos um erro. Qual a letra foi encifrada errada?

3.2 Trabalhando com blocos

Para evitar um ataque ao sistema de criptografia através de uma análise de freqüência das letras, vamos discutir maneiras de encifrar mensagens substituindo cada bloco com k letras, onde k é um natural fixo, por um outro bloco de k letras. Isto é, utilizaremos uma permutação no conjunto dos blocos com k letras. Na seção anterior, consideramos $k = 1$. Ainda é possível decidir quais são os blocos com 2 letras mais freqüêntes em textos escritos em português. Mas decidir quais blocos com 8 letras são mais freqüêntes aparenta ser muito complexo, se não for impossível. Mesmo que seja possível fazer isto, para utilizar esta técnica em um texto interceptado, o tamanho deste teria de ser muito grande para que uma análise de freqüência pudesse ser tentada. Quanto maior o k mais seguro estaremos. Aumentar o tamanho de k incrementa um pouco o custo de encifrar mensagens, mas não torna o sistema proibitivo.

3.2.1 Considerando o bloco como um elemento

Um bloco com k letras pode ser visto como um natural possuindo até k dígitos quando escrito na base L, onde os L dígitos utilizados para representar um natural nesta base, quando listados em ordem crescente, é o alfabeto $\mathcal{A}$. Lembre-se que L é o número de letras de $\mathcal{A}$. Supondo que o alfabeto utilizado seja $\mathcal{A}_{\mathrm{P}}$, o bloco `GbAT` e `AAAB` correspondem aos seguintes naturais:

$$(\texttt{GbAT})_{24} = 6 \cdot 24^3 + 23 \cdot 24^2 + 0 \cdot 24^1 + 18 \cdot 24^0 = 96.210$$
$$(\texttt{AAAB})_{24} = 0 \cdot 24^3 + 0 \cdot 24^2 + 0 \cdot 24^1 + 1 \cdot 24^0 = 1$$

Observe que qualquer inteiro a tal que $0 \leq a < L^k$ possui no máximo k dígitos, que são as letras do alfabeto ordenado $\mathcal{A}$, quando representado na base L. Adicionando a primeira letra do alfabeto, que representa o zero, à esquerda desta representação, tantas vezes quantas forem necessárias, podemos torná-lo com k letras. Isto é, os blocos com k letras representam os possíveis restos da divisão de um inteiro por L^k. Portanto, cada bloco com k letras do alfabeto L pode ser visto como um elemento de $\mathbb{Z}_{L^k}$. Conseqüentemente, para encifrar mensagens, necessitamos de uma permutação dos elementos de $\mathbb{Z}_{L^k}$.

Mais uma vez, consideramos funções afins. Seja $\sigma : \mathbb{Z}_{L^k} \to \mathbb{Z}_{L^k}$ dada por $\sigma(X) = aX + b$, onde $a \in \mathbb{Z}^*_{L^k}$ e $b \in \mathbb{Z}_{L^k}$. Pela escolha de a, σ é inversível e, portanto, uma permutação de $\mathbb{Z}_{L^k}$, como desejávamos. Diremos que a e b são as *chaves* destes sistema de criptografia, que será denotado por $\mathrm{scl}^k_{\mathcal{A}}(a, b)$. De posse da chave, um terceiro facilmente obtém a inversa de σ e decifra as mensagens. Logo a e b devem ser mantidos em segredo.

Tendo em vista a semelhança com o sistema de criptografia discutido na seção anterior, iremos usá-lo para encifrar uma pequena mensagem apenas, enfatizando as diferenças. Suponha que $k = 2$ e $\mathcal{A} = \mathcal{A}_{\mathrm{P}}$. Desejamos encifrar a palavra `SPORT`. Como o número de letras não é divisível por k, completamos esta palavra com tantos `b` quantos forem necessários para torná-lo divisível por k. Isto é, encifraremos a palavra `SPORTb`. Assumiremos que a permutação de $\mathbb{Z}_{576}$ seja dada pela expressão

$$\sigma(X) = \overline{413}X + \overline{128}.$$

Na tabela seguinte apresentamos:

- Na primeira coluna os blocos da mensagem que devem ser encifrados.
- Na segunda coluna os elementos de $\mathbb{Z}_{576}$ que correspondem a estes blocos.
- Na terceira coluna as imagens, via σ, destes elementos.
- Na quarta coluna os blocos que encifram os blocos que estão na primeira.

`SP`	$\overline{422}$	$\overline{462}$	`UG`
`OR`	$\overline{328}$	$\overline{232}$	`JR`
`Tb`	$\overline{455}$	$\overline{267}$	`MD`

Portanto, a mensagem `SPORTb` foi encifrada em `UGJRMD`.

3.2.2 Considerando o bloco como um vetor

Um bloco com k letras pode ser visto como um vetor (coluna) com k entradas, onde cada entrada é uma letra, ou seja, um elemento de $\mathcal{A}^k$.

Como cada letra de $\mathcal{A}$ está naturalmente associada a um elemento de $\mathbb{Z}_L$, cada bloco com k letras pode ser visto como um elemento de $\mathbb{Z}_L^k$. Transformaremos um bloco de k letras em outro bloco de k letras através de uma função afim de $\mathbb{Z}_L^k$. Mais precisamente, para matrizes A e B de tamanho $k \times k$ e $k \times 1$ respectivamente com entradas em $\mathbb{Z}_L$, seja $\sigma : \mathbb{Z}_L^k \to \mathbb{Z}_L^k$ dada por

$$\sigma(X) = AX + B.$$

Note que $\sigma(X)$ é uma permutação dos elementos de $\mathbb{Z}_L^k$ quando A for uma matriz com inverso multiplicativo. Mais ainda,

$$\sigma^{-1}(X) = A^{-1}(X - B).$$

Denotamos este sistema de criptografia por $\mathrm{SCL}_{\mathcal{A}}^k(A, B)$. Note que o sistema de criptografia $\mathrm{SCL}_{\mathcal{A}}^k(A^{-1}, -A^{-1}B)$ é utilizado para decifrar as mensagens.

O lemma a seguir caracteriza quando uma matriz possui inverso multiplicativo. Em sua demonstração utilizaremos livremente propriedades de determinantes. Está implícito na demonstração uma descrição da matriz inversa. Esta descrição pode ser utilizada para rapidamente encontrar inversas de matrizes pequenas — de tamanho 2 ou 3, por exemplo.

Lema 12. *Uma matriz quadrada X com entradas em um anel A possui inversa multiplicativa se e somente se* $\det(X)$ *possui inverso multiplicativo em A.*

Demonstração. Suponha que X possui inversa multiplicativa. Isto é, existe matriz quadrada Y, com entradas em A, tal que

$$I = XY = YX,$$

onde I denota a matriz identidade. Tomando determinantes, obtemos que:

$$1 = \det(I) = \det(XY) = \det(X)\det(Y).$$

Conseqüentemente $\det(Y)$ é o inverso multiplicativo de $\det(X)$. Logo estabelecemos a ida deste reultado.

Agora mostraremos a volta. Suponha que $\det(X)$ possua inverso multiplicativo. Sejam i e j naturais menores que o tamanho t da

matriz X. Definimos X_{ij} como sendo a matriz $(t-1)\times(t-1)$ obtida de X eliminado-se a i-ésima linha e a j-ésima coluna. Considere a matrix $Y=(y_{ij})$ de tamanho $t\times t$ tal que $y_{ij}=(-1)^{i+j}\det(X_{ji})$. Esta matriz é conhecida como a *de cofatores* de X. Note que

$$XY=\det(X)I.$$

O elemento que está na linha i e na coluna j do produto XY é

$$\sum_{k=1}^{t}x_{ik}y_{kj}=\sum_{k=1}^{t}(-1)^{j+k}x_{ik}\det(X_{jk}),$$

que é igual ao $\det(X)$, quando $i=j$, ou ao determinante da matriz obtida a partir de X substituindo a j-ésima linha pela i-ésima — este determinante é 0, pois esta matriz fica com duas linhas iguais. Conseqüentemente

$$[\det(X)]^{-1}Y$$

é a matriz inversa de X. □

Vamos encotrar todos os valores de a para os quais a matriz A, com entradas em $\mathbb{Z}_{24}$, possui uma inversa, onde

$$A=\begin{pmatrix}\overline{18} & \overline{7} & \overline{22}\\ \overline{13} & \overline{14} & \overline{9}\\ \overline{21} & \overline{19} & a\end{pmatrix}$$

Note que

$$\det(A)=\overline{17}a+\overline{19}.$$

Pelo Lema 12, A é inversível se e somente se $\overline{17}a+\overline{19}$ possui inverso em $\mathbb{Z}_{24}$. Suponha que $a=\overline{r}$, onde r é um inteiro satisfazendo $0\leq r<24$. Logo $\det(A)$ é inversível se e somente se $(17r+19,24)=1$ ou seja 2 e 3 não dividem $17r+19=17(r+1)+2$. Portanto, r é par e $r\not\equiv 1 \mod 3$. Conseqüentemente

$$r\in\{0,2,6,8,12,14,18,20\}.$$

Vamos encifrar a mensagem

```
O AMERICA CAIU
```

utilizando o sistema de criptografia

$$\mathrm{SCL}^2_{\mathcal{A}_\mathrm{P}}\left(\begin{pmatrix}\overline{5} & \overline{14}\\ \overline{18} & \overline{23}\end{pmatrix}, \begin{pmatrix}\overline{4}\\ \overline{10}\end{pmatrix}\right)$$

O determinante da matriz quadrada que é uma das chaves possui inverso em $\mathbb{Z}_{24}$? Quebramos a mensagem a ser encifrada em blocos de tamanho 2. Neste caso obtemos os seguintes blocos:

`Ob`; `AM`; `ER`; `IC`; `Ab`; `CA`; `IU`

Estes blocos correspondem respectivamente aos seguintes vetores de $\mathbb{Z}^2_{24}$:

$$\begin{pmatrix}\overline{13}\\ \overline{23}\end{pmatrix}; \begin{pmatrix}\overline{0}\\ \overline{11}\end{pmatrix}; \begin{pmatrix}\overline{4}\\ \overline{16}\end{pmatrix}; \begin{pmatrix}\overline{8}\\ \overline{2}\end{pmatrix}; \begin{pmatrix}\overline{0}\\ \overline{23}\end{pmatrix}; \begin{pmatrix}\overline{2}\\ \overline{0}\end{pmatrix}; \begin{pmatrix}\overline{8}\\ \overline{19}\end{pmatrix}$$

Encifraremos o primeiro bloco em detalhes:

$$\begin{pmatrix}\overline{5} & \overline{14}\\ \overline{18} & \overline{23}\end{pmatrix}\begin{pmatrix}\overline{13}\\ \overline{23}\end{pmatrix} + \begin{pmatrix}\overline{4}\\ \overline{10}\end{pmatrix} = \begin{pmatrix}\overline{3}\\ \overline{19}\end{pmatrix} + \begin{pmatrix}\overline{4}\\ \overline{10}\end{pmatrix} = \begin{pmatrix}\overline{7}\\ \overline{5}\end{pmatrix}$$

que corresponde ao bloco `HF`. Os demais blocos são encifrados em `Pb`, `IT`, `AI`, `PM`, `EI` e `ZQ` respectivamente. Logo a mensagem foi encifrada em:

`HFPbITAIPMEIZQ`

Um erro foi cometido ao encifrar um destes blocos. Descubra qual decifrando esta mensagem.

Nesta seção, resolvemos um problema que o sistema de criptografia apresentado na primeira seção possuía: ser quebrado através de uma análise de freqüência das letras. Contudo, um outro problema persiste: as chaves para encifrar as mensagens têm de ser mantidas secretas, pois qualquer um que tenha acesso a estas facilmente descobre as chaves para decifrar as mensagens cifradas. Em outras palavras, para este sistema ser utilizado, é necessário que previamente as partes interessadas em trocar informações confidenciais entrem em contato e combinem quais chaves irão utilizar. Este encontro será presencial para garantir a integridade das chaves — breve veremos como isto pode ser feito virtualmente. Esta situação é insatisfatória, pois realizamos muitas transações eletronicamente. Veremos na próxima seção como contornar este problema de uma maneira elegante.

3.2.3 Exercícios

Para todos os exercícios em que um alfabeto faz-se necessário, utilize $\mathcal{A}_{\text{P}}$.

1. Represente cada um dos seguintes naturais como blocos de 5 letras: 5; 12.678; 345.000; 6.118.714

2. Que naturais representam os seguintes blocos: `bbbb`; `DFOI`; `JKDF`; `AAPO`?

3. Com $\text{scl}^2_{\mathcal{A}_{\text{P}}}(\overline{413}, \overline{128})$, encifre a palavra `NAUTICO`. Encontre o sistema de criptografia para decifrar mensagens encifradas com $\text{scl}^2_{\mathcal{A}_{\text{P}}}(\overline{413}, \overline{128})$. Verifique a existência de erros em seus cálculos decifrando a "palavra" obtida.

4. Considere a seguinte mensagem:

   `O SANTA PERDEU TODOS OS JOGOS PARA O VITORIA ESTE ANO`

   Encifre esta mensagem utilizando $\text{SCL}^3_{\mathcal{A}_{\text{P}}}(A, B)$ para

   $$A = \begin{pmatrix} \overline{3} & \overline{2} & \overline{4} \\ \overline{5} & \overline{7} & \overline{9} \\ \overline{1} & \overline{6} & \overline{1} \end{pmatrix} \text{ e } B = \begin{pmatrix} \overline{8} \\ \overline{0} \\ \overline{5} \end{pmatrix}$$

5. Estime o custo de encifrar uma mensagem de n letras, que foi escrita em um alfabeto $\mathcal{A}$ possuindo L letras, utilizando:

   (a) $\text{scl}^k_{\mathcal{A}}(a, b)$.

   (b) $\text{SCL}^k_{\mathcal{A}}(A, B)$.

6. Considere as seguintes matrizes

   $$\begin{pmatrix} \overline{5} & \overline{3} \\ \overline{1} & \overline{7} \end{pmatrix} \text{ e } \begin{pmatrix} \overline{1} & \overline{9} & \overline{36} \\ \overline{1} & \overline{1} & \overline{1} \\ \overline{1} & \overline{3} & \overline{6} \end{pmatrix}$$

   cujas entradas pertencem a $\mathbb{Z}_n$, para algum natural n satisfazendo $n \geq 2$. Para cada uma destas matrizes:

(a) Encontre sua matriz de cofatores.

(b) Calcule seu determinante.

(c) Decida para quais naturais n possui inversa.

(d) Quando existir, encontre a inversa.

7. Seja $A = (a_{ij})$ uma matriz de tamanho $t \times t$ e entradas em $\mathbb{Z}_n$, para um natural n. Se X_{ij} é a matriz obtida a partir de A eliminando-se a i-ésima linha e j-ésima coluna, então, para i fixo,

$$\det(A) = \sum_{j=1}^{t} (-1)^{i+j} a_{ij} \det(X_{ij}).$$

Em termos de t e n, estime o custo de encontrar:

(a) O determinante de A utilizando esta recorrência.

(b) A matriz de cofatores de A.

(c) A matriz inversa de A via matriz de cofatores.

8. Seja A uma matriz de tamanho $t \times t$ com coeficientes em $\mathbb{Z}_n$, onde n é um natural tal que $n \geq 2$. As seguintes operações realizadas nas linhas de A são ditas *elementares*:

- Permutar duas linhas.
- Adicionar a uma linha um múltiplo de uma outra.
- Multiplicar uma linha por um elemento de $\mathbb{Z}_n^*$.

Estas operações são ditas respectivamente do *primeiro, segundo e terceiro tipos*.

(a) Qual o efeito que uma operação elementar tem no determinante da matriz?

(b) Mostre que os seguintes procedimentos são equivalentes:

- Realizar uma operação elementar em A.
- Realizar a mesma operação elementar na matriz identidade I_t de tamanho $t \times t$, obtendo uma matriz E como resultado, e calcular EA.

(c) Mostre que uma operação elementar do terceiro tipo comuta com qualquer outra operação elementar.

(d) No caso em que n é primo considere o seguinte algoritmo para encontrar a inversa de A: escalone a matriz B de tamanho $t \times 2t$, onde as t primeiras colunas são iguais as de A e as t últimas iguais as de I_t. Se, ao final do processo, nas t primeiras colunas temos a identidade, então a inversa de A encontra-se nas t últimas colunas. Senão A não possui inversa.

i. Por que este algoritmo funciona?

ii. Estime seu custo em termos de n e t.

iii. Faça uma adaptação deste algoritmo para calcular $\det(A)$.

9. Encontre a inversa, quando existir, e o determinate da seguinte matriz, cujos coeficientes pertencem a $\mathbb{Z}_n$, para um natural n:

$$\begin{pmatrix} \overline{1} & \overline{1} & \overline{1} & \overline{1} & \overline{1} & \overline{0} & \overline{0} \\ \overline{0} & \overline{1} & \overline{1} & \overline{1} & \overline{1} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} & \overline{1} & \overline{1} & \overline{1} & \overline{1} \\ \overline{1} & \overline{0} & \overline{0} & \overline{1} & \overline{1} & \overline{1} & \overline{1} \\ \overline{1} & \overline{1} & \overline{0} & \overline{0} & \overline{1} & \overline{1} & \overline{1} \\ \overline{1} & \overline{1} & \overline{1} & \overline{0} & \overline{0} & \overline{1} & \overline{1} \\ \overline{1} & \overline{1} & \overline{1} & \overline{1} & \overline{0} & \overline{0} & \overline{1} \end{pmatrix}$$

3.3 Criptografia com chave pública

A idéia de criptografia com chave pública foi inicialmente proposta, de maneira teórica, por Diffie e Hellman em 1976. Cada usuário define um algoritmo E para encifrar as mensagens que lhe são enviadas. Este usuário conhece o algoritmo D para decifrar as mensagens. Em geral, o que difere um algoritmo de um usuário do de um outro é um conjunto de números, como no caso dos sistemas de criptografia clássicos, conhecidos como chaves. A diferença é que o conhecimento de E, isto é, das chaves, não permite, na prática, a descoberta de D — daí o termo chave pública. Claro que é possível imaginar um algoritmo para decifar mensagens que foram encifradas por E: aplique

E a qualquer mensagem que possa originar o texto interceptado, que necessita ser decifrado, até que, para alguma mensagem, este texto seja obtido. O problema com esta abordagem é que muitos textos têm de ser considerados. Suponha que, através de uma análise, descobre-se que a mensagem cifrada, escrita em um alfabeto com 100 letras, foi obtida a partir de um texto com 200. Portanto, esta abordagem teria de considerar até $100^{200} = 10^{400}$ textos para descobrir o que deu origem a mensagem cifrada. Isto é impossível de ser computado! Quantos anos seriam necessários para executar este algoritmo, sabendo que o computador pode processar 10^{10} textos por segunto? Compare o número obtido com a idade do universo. Note que podemos ver E como sendo uma permutação do conjunto de todas as mensagens possuindo como inversa D. Portanto, quando M for um texto, o texto que foi encifrado por E é denotado por $E(M)$.

Será que existem tais algoritmos? A resposta é sim e será explicada na próxima seção. Antes de fazer isto, iremos considerar como quem está enviando a mensagem cifrada pode assiná-la de forma que quem a recebe tenha a certeza do remetente. No nosso exemplo, consideraremos dois usuários: Alice e Bob. Assuma que os algoritmos disponibilizados por Alice e Bob para o público são E_A e E_B respectivamente. Alice e Bob guardam secretamente os correspondentes algoritmos para decifrar D_A e D_B. Alice deseja mandar uma mensagem M para Bob sem que ninguém, a não ser Bob, tenha acesso a seu conteúdo. Mais ainda, Alice quer que Bob tenha certeza que foi ela quem enviou a mensagem. Portanto, Alice mandará para Bob a seguinte mensagem encifrada:

$$N = D_A(E_B(M)). \tag{3.1}$$

Sabendo que a mensagem encifrada N vem de Alice, primeiro Bob aplica E_A, que está disponível ao público, obtendo:

$$E_A(N) = E_A(D_A(E_B(M))) = E_B(M), \tag{3.2}$$

pois E_A é a inversa de D_A. A seguir Bob aplica D_B a este resultado:

$$D_B(E_A(N)) = D_B(E_B(M)) = M. \tag{3.3}$$

Portanto, Bob recupera a mensagem M. Apenas Bob pode obter a mensagem M, pois é o único que conhece D_B e é impossível, na

prática, obter M a partir de $E_B(M)$ sem o conhecimento de D_B. Note que qualquer um pode obter $E_B(M)$. Bob tem certeza que foi Alice que mandou a mensagem M, pois apenas Alice pode calcular $D_A(E_B(M))$, já que ninguem mais tem acesso a D_A. Consqüentemente qualquer usuário pode "assinar" as mensagens enviadas. Este processo é conhecido como assinatura digital.

Bob pode convencer a terceiros que foi Alice quem lhe enviou a mensagem N: aplica E_B a M e E_A a N. Por (3.2), o resultado é o mesmo. Logo N tem de ser $D_A(E_B(M))$ e qualquer outra pessoa ficaria convencida que Alice mandou a mensagem, pois apenas ela teria acesso a D_A.

Em resumo, este sistema possui as seguintes caracteristicas, que são muito importantes para aplicações:

- Confidencialidade (terceiros não têm acesso a informação).
- Autenticidade (quem recebe a informação tem certeza do remetente).
- Integridade (terceiros não podem alterar a informação).
- Incontestabilidade (quem enviou a informação não tem como negar).

3.4 RSA

Em 1978, o primeiro sistema de criptografia com chave pública foi desenvolvido. Seus criadores foram Rivest, Shamir e Adleman. Devido as inciais de seus sobrenomes, este sistema é conhecido como o RSA. Nas três últimas décadas, o RSA vem sendo largamente empregado para garantir segurança em transações eletrônicas. Seu funcionamento é baseado em dois princípios, sendo que o segundo é empírico:

- É fácil encontrar dois números primos grandes. Veremos como fazer isto no próximo capítulo.
- É praticamente impossível fatorar o seu produto. Consideraremos alguns algoritmos para fatoração no último capítulo.

Nesta seção, descreveremos detalhadamente o RSA.

O operador do sistema fixa um alfabeto $\mathcal{A}$ com L letras. As mensagens encaminhadas por qualquer usuário do sistema para qualquer outro serão escritas neste alfabeto. Em geral, este alfabeto consiste de todos os possíveis símbolos que podem ser digitados em um teclado de computador. Dado o seu tamanho não utilizaremos este alfabeto em nossos exemplos. O operador escolhe naturais r e s tais que $r < s$. Para encaminhar uma mensagem a determinado usuário, divide-se a mensagem em blocos de tamanho r e substitui-se cada bloco de tamanho r por um de tamanho s obtido através de um algoritmo que será descrito a seguir. A maneira de encifrar mensagens é bem parecida com a utilizada nos sistemas clássicos discutidos anteriormente.

Um usuário do RSA deve escolher números primos p e q tais que

$$L^r < n < L^s, \text{ onde } n = pq. \tag{3.4}$$

De posse de p e q, o usuário pode calcular

$$\phi(n) = (p-1)(q-1). \tag{3.5}$$

A seguir, o usuário escolhe aleatoriamente um natural e tal que $(e, \phi(n)) = 1$. Isto é, $\overline{e}$ possui inverso em $\mathbb{Z}_{\phi(n)}$. Seja d um natural tal que $\overline{d}$ seja o inverso de $\overline{e}$ em $\mathbb{Z}_{\phi(n)}$. Isto é

$$de \equiv 1 \mod \phi(n). \tag{3.6}$$

Escolha d e e de forma que ambos sejam menores que $\phi(n)$. Neste momento, o usuário destrói p, q e $\phi(n)$. Torna público o par (e, n), que serão suas chaves públicas, e guarda d, que é sua chave privada.

Exitesm algoritmos eficientes para encontrar p e q em algumas situações particulares. A partir destes algoritmos é possível obter algumas condições que p e q devem satisfazer para que a fatoração de n seja inviável na prática. Não abordaremos esta questão nestas notas pois não iremos tratar destes algoritmos de fatoração.

A seguir apresentaremos o resultado de Euler que será fundamental para o funcionamento do RSA. Este resultado é uma pequena variante do Teorema 9.

Teorema 12. *Se $a \in \mathbb{Z}$, então $a^{de} \equiv a \mod n$.*

Demonstração. O resultado segue do seguinte fato: quando $x \in \{p, q\}$,

$$a^{de} \equiv a \mod x. \tag{3.7}$$

Logo p e q dividem $a^{de} - a$ e daí $n = pq$ também o divide. Note que (3.7) é válida quando x divide a. Vamos supor que x não divide a. Pelo Pequeno Teorema de Fermat:

$$a^{x-1} \equiv 1 \mod x.$$

Tomando a $k(y-1)$-ésima potência dos dois membros desta congruência, onde $\{x, y\} = \{p, q\}$ e k é um inteiro, obtemos:

$$a^{k\phi(n)} \equiv 1 \mod x.$$

Por (3.6), existe inteiro k tal que $de = k\phi(n) + 1$. Conseqüentemente

$$a^{de-1} \equiv 1 \mod x.$$

Obtemos (3.7) ao multiplicarmos ambos os lados desta congruência por a. □

Agora apresentaremos o algoritmo para encifrar mensagens. Suponha que iremos enviar uma mensagem para um usuário que publicou as seguintes chaves (n, e). Divide-se a mensagem a ser encifrada em blocos com r letras cada. Talvez seja necessário completar o último bloco com letras sem significado — que podem ser o espaço em branco. Cada bloco B com r letras pode ser visto como sendo a representação de um inteiro não-negativo a na base L. Por (3.4),

$$a < L^r < n. \tag{3.8}$$

Calcule $\overline{a}^e$ em $\mathbb{Z}_n$. Seja a' um inteiro tal que $0 \leq a' < n$ e

$$\overline{a'} = \overline{a}^e \text{ em } \mathbb{Z}_n. \tag{3.9}$$

Por (3.4), temos que

$$a' < n < L^s. \tag{3.10}$$

Portanto, a' possui no máximo s dígitos quando escrito na base L. Logo a' corresponde a um bloco B' com s letras de $\mathcal{A}$. Adiciona-se a

primeira letra de $\mathcal{A}$ tantas vezes quantas forem necessárias à esquerda da representação de a', quando a' tiver menos de s dígitos.

Para decifrar a mensagem, o receptor a divide em blocos com s letras cada. Para cada bloco B' com s, letras, corresponde um número inteiro a', com $0 \leq a' < L^s$. Por contrução, temos que $a' < n$ (veja (3.10)). Em $\mathbb{Z}_n$, utilizando sua chave secreta, o receptor da mensagem calcula:

$$\overline{a'}^d = (\overline{a}^e)^d = \overline{a}^{ed} = \overline{a},$$

onde primeira igualdade segue de (3.9) e a última do Teorema 12. Por (3.8), a é o menor inteiro não-negativo em $\overline{a}$. Portanto, o receptor da mensagem consegue recuperar a e conseqüentemente o bloco B que este representa. Fazendo isto para todo bloco, consegue decifrar a mensagem que lhe foi enviada.

Agora, faremos um exemplo. Para facilitar o entendimento do leitor, iremos escolher números primos "pequenos", do contrário as "contas" seriam imensas. Portanto, nosso exemplo ilustrará apenas o processo. Para trabalhar com segurança, em aplicações, necessitaríamos de primos com pelo menos 100 dígitos na expansão decimal. Seria improdutivo fazer tal exemplo aqui. Utilizaremos o alfabeto $\mathcal{A}_{\text{P}}$. Logo $L = 24$. Vamos supor que $r = 2$ e $s = 3$. Em particular, temos de escolher n entre $L^r = 576$ e $L^s = 13824$. Escolhemos $p = 29$ e $q = 31$. Logo $n = 899$ e $\phi(n) = 840 = 2^3 \cdot 3 \cdot 5 \cdot 7$. Escolha $e = 289$. Vamos encifrar a seguinte mensagem com a chave pública $(n, e) = (899, 289)$:

```
O SPORT GANHOU DUAS VEZES DO TIMAO ESTE ANO
```

Na tabela a seguir, descrevemos como esta mensagem é encifrada. Em cada linha lidamos com um bloco, que está na primiera coluna. Na segunda coluna, apresentamos o elemento a de $\mathbb{Z}_{899}$ que corresponde a este bloco e nas seguintes, nesta ordem, $a^2, a^4, a^8, a^{16}, a^{32}, a^{64}, a^{128}, a^{256}$ e a^{289}, notando que

$$a^{289} = a^{256+32+1} = a^{256}a^{32}a^1.$$

Na última coluna, o bloco encifrado. Eis a tabela:

Ob	335	749	25	625	459	315	335	749	25	459	AUD
SP	405	407	233	439	436	407	233	439	436	202	AIL
OR	328	603	413	658	545	355	165	255	297	847	BMH
Tb	455	255	297	107	661	7	49	603	413	168	AHA
GA	144	59	784	639	175	59	784	639	175	753	BHJ
NH	295	721	219	314	605	132	343	779	16	33	ABJ
OU	331	782	204	262	320	813	204	262	320	447	ATQ
bD	555	567	546	547	741	691	112	857	865	825	BLJ
UA	456	267	268	803	226	732	20	400	877	507	AXD
Sb	431	567	546	547	741	691	112	857	865	422	ASP
VE	484	516	152	629	81	268	803	226	732	400	ARR
ZE	532	738	749	25	625	459	315	335	749	656	BDI
Sb	431	567	546	547	741	691	112	857	865	422	ASP
DO	85	33	190	140	721	219	314	605	132	213	AIX
bT	570	361	865	257	422	82	431	567	546	127	AFH
IM	203	754	348	638	696	754	348	638	696	551	AZb
AO	13	169	692	596	111	634	103	720	576	672	BEA
bE	556	779	16	256	808	190	140	721	219	294	ANG
ST	426	777	500	78	690	529	252	574	442	864	BNA
Eb	119	676	284	645	687	893	36	397	284	398	ARP
AN	12	144	59	784	639	175	59	784	639	592	BAR
Ob	335	749	25	625	459	315	335	749	25	459	AUD

A mensagem é encifrada pela substituição de cada bloco de duas letras que está na coluna da esquerda da tabela pelo bloco de três letras que está à esquerda e na mesma linha. Conseqüentemente a mensagem cifrada é:

AUDAILBMHAHABHJABJATQBLJAXDASPARRBDIASPAIXA
FHAZbBEAANGBNAARPBARAUD

Note que o custo de encifrar ou decifrar um bloco no RSA é respectivamente $O(\log_2 e \log_2^2 n)$ ou $O(\log_2 d \log_2^2 n)$. A estimativa deste custo pode ser melhorada, caso seja utilizado um melhor algoritmo para fazer multiplicações, o que ocorre nas aplicações. Mesmo assim o custo fica bastante elevado, já que e e d são grandes, isto é, $O(\log_2 n)$. Portanto, é bem mais caro para ser utilizado que os sistemas de criptografia clássicos, por exemplo. Quanto maior as chaves

mais lento fica o RSA. A tendência, com o passar dos anos, para garantir segurança, é o aumento no tamanho das chaves, isto é, a escolha de primos p e q maiores, já que novos e melhores algoritmos de fatoração surgem. Por este motivo, alguns dispositivos com pouca memória disponível, como cartões inteligentes, podem optar por outros sistemas de criptografia com chave pública, cujas chaves tenham menor comprimento. Chaves menores implicam em implementações mais rápidas para encifrar e decifrar mensagens, menos memória gasta com armazenamento e processamento, economia de energia (em dispositívos sem fonte externa de alimentação) etc. Tais sistemas existem e usam curvas elípticas. Esta curvas são fascinantes porque pode-se definir uma operação de adição entre seus pontos possuindo as propriedades usuais: associatividade, comutatividade, elemento neutro e inverso aditivo. Não discutiremos tais curvas neste curso pois necessitaríamos de muito tempo para estabelecer todas as suas propriedades.

Hardy, que foi um dos matemáticos mais importantes da primeira metade do século passado, e desenvolvia pesquisa em várias áreas da matemática, dentre as quais teoria dos números, cujo estudo iniciou-se há mais de 2.500 anos, vangloriava-se que esta área da matemática nunca tinha sido aplicada, mantendo-se pura. Mal sabia ele que, passados dois milênios e meio, teoria dos números passaria a ser fundamental nos sistemas de criptografia com chave pública e também em códigos corretores de erros, cujo estudo iniciou-se com Hamming, logo após a segunda guerra mundial, e usa corpos finitos, que são uma extensão de $\mathbb{Z}_p$, quando p é primo.

3.4.1 Exercícios

1. Porque não existe bloco encifrado começando com `C` no exemplo apresentado no texto?

2. Utilizando as informações da primeira linha da tabela, determine a ordem de $\overline{n}$ em $\mathbb{Z}_{899}^*$, para cada $n \in \{5, 25, 335\}$.

3. Utilizando as informações da segunda linha da tabela, determine a ordem de $\overline{407}$ em $\mathbb{Z}_{899}^*$. E de $\overline{405}$?

4. Utilizando as informações das terceira e quarta linhas da tabela,

encontre quatro raízes diferentes para o polinômio $X^2 - \overline{255}$ em $\mathbb{Z}_{899}$.

5. Em uma mesma linha da tabela, em que pares de colunas podemos encontrar o mesmo elemento? Que condição o elemento que ocupa estas posições tem de satisfazer?

6. Encontre o inverso de $\overline{289}$ em $\mathbb{Z}_{840}$.

7. Utilizando o inverso obtido no exercício anterior, decifre a mensagem que foi encifrada nesta seção. Foi cometido algum erro?

8. Suponha que (n, e) seja a chave pública de um usuário do RSA (com parâmetros como definidos nesta seção). Mostre que:

   (i) Um bloco encifrado possui pelo menos

   $$m^* = \max\left\{m : \left\lfloor \frac{L^{s-m}}{n} \right\rfloor \geq 1\right\}.$$

   `A`'s em seu início, onde `A` é a primeira letra do alfabeto.

   (ii) Um bloco encifrado nunca começa com a k-ésima letra do alfabeto, para todo k satisfazendo

   $$k > \left\lceil \frac{n-1}{L^{s-m^*-1}} \right\rceil.$$

3.5 Segurança do RSA

Lenstra, que é um dos maiores especialistas em teoria dos números computacional, afirmou que caso, por engano, jogássemos fora os primos p e q, e mantivermos apenas o seu produto n, as maneiras mais promissoras para recuperar p e q seriam procurar no lixão ou usar técnicas de hipnose, o que parece ser uma derrota da matemática. Em outras palavras, fatorar n é impossível, do ponto de vista prático, desde que p e q sejam grandes. Esta foi a nossa hipótese ao apresentarmos o RSA. Será que a segurança do sistema baseia-se apenas neste fato? Consideraremos várias maneiras de se quebrar o RSA e mostraremos que, caso tenhamos sucesso em alguma delas, teríamos um algoritmo eficiente para fatorar n. Assumimos que tal algoritmos não existe. Cada ataque ao RSA será considerado em uma subseção separada.

3.5.1 É possível descobir $\phi(n)$ a partir de n

A descoberta de $\phi(n)$ nos dá acesso a chave privada d, já que $\overline{d}$ é o inverso de $\overline{e}$ em $\mathbb{Z}_{\phi(n)}$ (que pode ser calculado de maneira eficiente a partir de e e $\phi(n)$). Portanto, um algoritmo eficiente para achar $\phi(n)$ a partir de n, sem encontrar p e q, quebraria o RSA, pois quem o possuísse poderia decifrar as mensagem encaminhadas a qualquer usuário do RSA.

Mostraremos que existe um algoritmo eficiente para fatorar n a partir do conhecimento de $\phi(n)$. Portanto, um algoritmo eficiente para obter $\phi(n)$ a partir de n implica em um algoritmo eficiente para fatorar n. Assumimos que tal algoritmo não existe. Conseqüentemente não poderíamos obter $\phi(n)$ a partir de n rapidamente.

Sabemos que

$$\phi(n) = (p-1)(q-1) = (p-1)\left(\frac{n}{p} - 1\right) = \frac{(p-1)(n-p)}{p}.$$

Esta identidade pode ser reescrita como

$$\begin{aligned} \phi(n)p - (p-1)(n-p) &= 0 \\ p^2 + (\phi(n) - n - 1)p + n &= 0 \end{aligned}$$

Isto é p é raiz do seguinte polinômio com coeficientes inteiros:

$$f(X) = X^2 + (\phi(n) - n - 1)X + n = 0.$$

A outra raiz de $f(X)$ é q. Isto é, p e q são as raízes deste polinômio quadrático, cujos coeficientes dependem apenas de n e $\phi(n)$, e daí iguais a

$$\frac{n + 1 - \phi(n) \pm \sqrt{\Delta}}{2},$$

onde

$$\Delta = (n + 1 - \phi(n))^2 - 4n.$$

Note que $\sqrt{\Delta}$ é um número natural, já que as raízes do polinômio são os naturais p e q. Portanto, necessitamos apenas um algoritmo eficiente para achar $\lfloor\sqrt{m}\rfloor$, para um natural m. Adaptaremos o pior algoritmo que foi apresentado no curso de Cálculo Numérico para fazer esta tarefa, que é o algoritmo da bissecção.

Proposição 11. *Para um natural m, o custo de calcular $\lfloor\sqrt{m}\rfloor$ é $O(\log_2^3 m)$.*

Demonstração. Considere o polinômio $g(X) = X^2 - m$. Desejamos encontrar a parte inteira da raiz positiva de $g(X)$. Utilizaremos o seguinte algoritmo:

1. Faça $a = 0$ e $c = m$.
2. Calcule $b = \lfloor \frac{a+c}{2} \rfloor$.
3. Se $c - a = 1$ ou $g(b) = 0$, então `PARE` porque $\lfloor\sqrt{m}\rfloor = b$.
4. Se $g(b) > 0$, então faça $c := b$ e retorne para o passo 2.
5. Se $g(b) < 0$, então faça $a := b$ e retorne para o passo 2.

Em cada interação deste algoritmo o comprimento do intervalo $[a, c]$ reduz-se pela metade. Portanto, o número de interações deste algoritmo é $O(\log_2 m)$. Como em cada interação, a operação mais cara é um produto de dois naturais, menores que m, então o custo de cada interação é $O(\log_2^2 m)$. Conseqüentemente o custo de descobrir a parte inteira da raiz quadrada é $O(\log_2^3 m)$. □

3.5.2 Pode-se descobir d sem o conhecimento de $\phi(n)$

Para decifrar as mensagens encaminhadas a um usuário do RSA, que possui chaves públicas (n, e), não necessitamos de $\phi(n)$, basta conhecermos a sua chave privada d.

Nesta subseção, mostraremos que existe um algoritmo eficiente para fatorar n caso a chave privada d também seja conhecida. Assumimos que tal algoritmo não existe. Portanto, não é possível existir um algoritmo rápido para calcular d a partir de (n, e).

Note que, caso conheçamos $\phi(n)$, temos um algoritmo eficiente para achar d. Portanto, a análise feita nesta seção engloba a realizada na anterior. Optamos por fazê-la pois:

- É muito mais simples que a apresentada nesta subseção.
- Não envolve algoritmos randomizados.

- E, principalmente, discute um algoritmo polinomial para obtenção da parte inteira da raiz quadrada de um natural.

Seja $m = ed$. Pelo Teorema 12, temos que, para todo natural a tal que $1 \leq a < n$,

$$a^m \equiv a \mod n.$$

Quando $(a, n) = 1$, $\overline{a}$ possui inverso multiplicativo em $\mathbb{Z}_n$ e esta equivalência pode ser reescrita como:

$$a^{m-1} \equiv 1 \mod n. \tag{3.11}$$

Iremos escolher a aleatoriamente no intervalo $[1, n-1]$. Se $(a, n) \neq 1$, então $(a, n) \in \{p, q\}$ e obtemos a fatoração de n.

Para um natural t, definimos os seguintes polinômios com coeficientes em $\mathbb{Z}_n^*$:

$$g_t(X) = X^t - \overline{1} \text{ e } h_t(X) = X^t + \overline{1}.$$

Considere o conjunto de raízes destes polinômios em $\mathbb{Z}_n^*$:

$$G_t = \{a \in \mathbb{Z}_n^* : g_t(a) = \overline{0}\} \text{ e } H_t = \{a \in \mathbb{Z}_n^* : h_t(a) = \overline{0}\}.$$

A equivalência (3.11) informa que $G_{m-1} = \mathbb{Z}_n^*$.

Estabeleceremos alguns resultados preliminares. O primeiro lema será utilizado para decidir, de maneira eficiente, quando

$$G_t = \mathbb{Z}_n^*, \tag{3.12}$$

para um natural t. Sabemos que (3.12) é satisfeita quando $t = m-1$. No algoritmo de fatoração para n, que será descrito nesta subseção, procuramos um t pequeno satisfazendo (3.12).

Lema 13. *Seja t um natural. Se $G_t \neq \mathbb{Z}_n^*$, então a probabilidade de um elemento de $\mathbb{Z}_n^*$, escolhido aleatoriamente, ser raiz de $g_t(X)$ é no máximo $\frac{1}{2}$.*

Demonstração. Sejam $a_1, a_2 \ldots, a_k$ as raízes de $g_t(X)$ em $\mathbb{Z}_n^*$. Observe que $aa_1, aa_2, \ldots, aa_k$ não são raízes de $g_t(X)$ porque

$$g_t(aa_i) = (aa_i)^t - \overline{1} = a^t a_i^t - \overline{1} = a^t - \overline{1} = g_t(a) \neq \overline{0}.$$

O resultado segue, pois $aa_1, aa_2, \ldots, aa_k$ são distintos e pertencem a $\mathbb{Z}_n^*$. □

O próximo lema, cuja demonstração é análoga a do anterior e ficará como exercício, será utilizado ao final desta subseção.

Lema 14. *Seja t um natural. Se $G_t \cup H_t \neq \mathbb{Z}_n^*$, então a probabilidade de um elemento de $\mathbb{Z}_n^*$, escolhido aleatoriamente, ser raiz de $g_t(X)$ ou de $h_t(X)$ é no máximo $\frac{1}{2}$.*

Agora apresentamos um algoritmo randomizado com o objetivo de verificar (3.12), para um natural t tal que $t \leq n^2$. Seja k um natural fixo.

1. Faça $i = 1$.
2. Se $i > k$, então `PARE` e retorne: *a condição* (3.12) *é satisfeita*.
3. Escolha aleatoriamente um natural a tal que $1 \leq a \leq n-1$.
4. Se $(a, n) \neq 1$, então retorne ao passo 3. Logo $(a, n) = p$ ou $(a, n) = q$ e a fatoração de n é obtida. Este algoritmo poderia ser interrompido aqui.
5. Se $\overline{a}$ não é raiz de $g_t(X)$, então `PARE` e retorne: *a condição* (3.12) *não é satisfeita*.
6. Incremente i de 1 e retorne ao passo 2.

Vamos analisar este algoritmo. É possível que ocorra um laço sem fim, caso no passo 4, para todo a escolhido $(a, n) \neq 1$. A probabilidade disto ocorrer para um a fixo é igual a

$$\frac{n-1-\phi(n)}{n} = \frac{pq-1-(p-1)(q-1)}{pq} < \frac{p+q}{pq} = \frac{1}{p} + \frac{1}{q}.$$

Este valor é despresível quando p e q tiverem por volta de 100 dígitos na base 10 e, do ponto de vista prático, podemos supor que é 0. Conseqüentemente, nestas condições e na vida real, nunca retornamos do passo 4 ao passo 3. O custo de realizar o passo 4 e o 5 é respectivamente $O(\log_2^3 n)$ e $O(\log_2 t \log_2^2 n)$. Portanto, o custo de um laço completo, para i fixo, é $O(\log_2^3 n)$, pois $t < n^2$. O custo final do algoritmo é $O(k \log_2^3 n)$. Conseqüentemente é muito rápido, já que k está fixo.

O resultado deste algoritmo é correto? Se o algoritmo para no passo 5, então a condição (3.12) não é satisfeita porque encontramos um elemento de $\mathbb{Z}_n^*$ que não é raiz de $g_t(X)$. Se o algoritmo para no passo 2, então k elementos de $\mathbb{Z}_n^*$, escolhidos de maneira aleatória, são raízes de $g_t(X)$. Caso a condição (3.12) não seja satisfeita, a probabilidade de um elemento de $\mathbb{Z}_n^*$, escolhido de forma aleatória, ser raiz de $g_t(X)$ é no máximo $\frac{1}{2}$, pelo Lema 13. A chance disto ocorrer para todos os k elementos escolhidos é

$$\left(\frac{1}{2}\right)^k = \left(\frac{1}{2^{10}}\right)^{\frac{k}{10}} = \left(\frac{1}{1024}\right)^{\frac{k}{10}} < \left(\frac{1}{1000}\right)^{\frac{k}{10}} = \left(\frac{1}{10^3}\right)^{\frac{k}{10}} = \left(\frac{1}{10}\right)^{\frac{3k}{10}}.$$

Para $k = 100$, a probabilidade do algoritmo cometer um erro é menor que 10^{-30} que, do ponto de vista prático, pode ser considerada como 0.

Algoritmos semelhantes a este serão freqüentes nestas notas.

O próximo lema garante a fatoração rápida de n, desde que consigamos inteiros t e b satisfazendo algumas condições. O objetivo do algoritmo que será apresentado é encontrar tais inteiros de maneira eficiente.

Lema 15. *Seja t um natural tal que $G_{2t} = \mathbb{Z}_n^*$. Se existe inteiro b satisfazendo $(b, n) = 1$,*

$$\overline{b} \notin G_t \text{ e } \overline{b} \notin H_t, \tag{3.13}$$

então $(b^t - 1, n) = p$ ou $(b^t - 1, n) = q$.

Demonstração. Por hipótese, $\overline{b}$ é raiz de $g_{2t}(X)$. Conseqüentemente

$$b^{2t} \equiv 1 \mod n.$$

Esta congruência pode ser reescrita como

$$b^{2t} \equiv 1 \mod p \text{ e } b^{2t} \equiv 1 \mod q.$$

Como $\mathbb{Z}_p$ e $\mathbb{Z}_q$ são corpos, apenas $\overline{-1}$ e $\overline{1}$ são as raízes quadradas de $\overline{1}$. Portanto, existem inteiros u_p e u_q pertencentes ao conjunto $\{-1, 1\}$ tais que:

$$b^t \equiv u_p \mod p \text{ e } b^t \equiv u_q \mod q. \tag{3.14}$$

Se $u_p = u_q$, então p e q dividem $b^t - u_p$. Logo o produto de p por q, que é n, também divide $b^t - u_p$; uma contradição a (3.13). Conseqüentemente $u_p \neq u_q$, digamos $u_p = 1$ e $u_q = -1$. Isto é, p divide $b^t - 1$ e q não divide $b^t - 1$, pois divide $b^t + 1$. Portanto, $(b^t - 1, n) = p$. □

Lema 16. *Seja t um natural tal que $G_{2t} = \mathbb{Z}_n^*$. Se existe inteiro b satisfazendo $(b, n) = 1$ e*

$$\overline{b} \notin G_t, \tag{3.15}$$

então $(a^t - 1, n) = p$ ou $(a^t - 1, n) = q$ para pelo menos a metade dos inteiros a tais que $1 \leq a \leq n$ e $(a, n) = 1$.

Antes da demonstração deste lema, apresentaremos um algoritmo para encontrar um natural t satisfazendo suas hipóteses, isto é,

$$G_{2t} = \mathbb{Z}_n^* \text{ e } G_t \neq \mathbb{Z}_n^*.$$

Lembre-se que $G_{m-1} = \mathbb{Z}_n^*$. Em particular m é ímpar.

1. Faça $t = \frac{m-1}{2}$.
2. Se (3.12) não é satisfeita para t, então `PARE` e retorne t.
3. Senão atribua a t o valor $\frac{t}{2}$ e retorne para o passo 2.

Note que o custo de realizar o passo 2 é $O(\log_2^3 n)$. Provamos isto através do algoritmo anterior. Como o número de etapas deste algoritmo é $O(\log_2 m) = O(\log_2 n)$, segue-se que o custo deste algoritmo é $O(\log_2^4 n)$. Logo rápido.

Demonstração do Lema 16. Observe que $p - 1$ ou $q - 1$ não divide t, do contrário, pelo Pequeno Teorema de Fermat, teríamos que, para todo inteiro a tal que $(a, n) = 1$,

$$a^t \equiv 1 \mod p \text{ e } a^t \equiv 1 \mod q$$

e daí p e q dividem $a^t - 1$ e conseqüentemente o seu produto n também divide $a^t - 1$. Isto não ocorre para b, pela hipótese (3.15). Sem perda de generalidade, podemos assumir que $p - 1$ não divide t.

Seja g um natural tal que $\overline{g}$ é um gerador para $\mathbb{Z}_p^*$. Por hipótese,

$$\overline{g}^{2t} = \overline{1} \text{ em } \mathbb{Z}_n \text{ e daí em } \mathbb{Z}_p.$$

Como $p-1$ não divide t e $\overline{1}$ possui apenas $\overline{-1}$ e $\overline{1}$ como raízes quadradas em $\mathbb{Z}_p$, obtemos que

$$\overline{g}^t = \overline{-1} \text{ em } \mathbb{Z}_p.$$

Pelo Teorema Chinês dos Restos, existe um inteiro u tal que

$$\overline{u} = \overline{g} \text{ em } \mathbb{Z}_p \text{ e } \overline{u} = \overline{1} \text{ em } \mathbb{Z}_q.$$

Conseqüentemente

$$\overline{u}^t = \overline{g}^t = \overline{-1} \text{ em } \mathbb{Z}_p \text{ e } \overline{u}^t = \overline{1} \text{ em } \mathbb{Z}_q.$$

Isto é p divide $u^t + 1$ e q divide $u^t - 1$. Portanto, p e q dividem exatamente um destes números, pois diferem de exatamente 2, e daí

$$\overline{u}^t \neq \overline{1} \text{ e } \overline{u}^t \neq \overline{-1} \text{ em } \mathbb{Z}_n. \tag{3.16}$$

Isto é, $G_t \cup H_t \neq \mathbb{Z}_n^*$. O resultado segue dos Lemas 14 e 15. □

Por fim, apresentamos o algoritmo randomizado para fatorar n. Suponha que t seja um natural satisfazendo as hipóteses do Lema 16. Já apresentamos um algoritmo randomizado, que nunca falha, na prática, para encontrar este natural.

1. Faça $i = 1$.
2. Escolha aleatoriamente um natural a tal que $1 \leq a \leq n-1$.
3. Se $(a, n) \neq 1$, então $(a, n) = p$ ou $(a, n) = q$. Neste caso `PARE` e retorne os naturais (a, n) e $\frac{n}{(a,n)}$.
4. Se $(a^t - 1, n) \notin \{1, n\}$, então $(a^t - 1, n) = p$ ou $(a^t - 1, n) = q$. Neste caso `PARE` e retorne os naturais (a, n) e $\frac{n}{(a,n)}$.
5. Incremente i de 1 e retorne ao passo 2.

Deixamos a análise deste algoritmo, que é similar a do anterior, como exercício (ver a última subseção desta seção).

3.5.3 Extraindo raizes e-ésimas em $\mathbb{Z}_n^*$

Vimos que encontrar $\phi(n)$ ou d é equivalente a fatorar o natural n, tarefa que julgamos ser impossível. Mesmo assim poderíamos quebrar o RSA caso conseguissemos recuperar qualquer elemento a de $\mathbb{Z}_n$ a partir de a^e.

3.5.4 Exercícios

1. Em algoritmos para o cálculo de $\sqrt{x}$, onde x é um número real positivo, encontramos uma seqüência $x_0, x_1, x_2, \ldots, x_n, \ldots$ de números reais cujo limite é igual a $\sqrt{x}$.

   (a) No algoritmo da Subseção 3.5.1, caso tomemos x_n como sendo o $(n+1)$-ésimo valor de b encontrado, mostre que

   $$|x_n - \sqrt{x}| = O\left(\frac{1}{2^n}\right).$$

   (b) Considere, agora, a recorrência obtida através do método de Newton para a extração da raiz quadrada que é:

   $$x_n = \frac{1}{2}\left(x_{n-1} + \frac{x}{x_{n-1}}\right)$$

   para $n \geq 1$, com x_0 sendo qualquer número real positivo. Mostre que, para $x \geq 1$ e $n \geq 1$:

   i. $x_n \geq \sqrt{x}$.
   ii. $x_n \geq x_{n+1}$.
   iii. $\lim_{n\to\infty} x_n = \sqrt{x}$.
   iv. $x_{n+1} - \sqrt{x} \leq \frac{(x_n - \sqrt{x})^2}{2\sqrt{x}}$.
   v. $x_n - \sqrt{x} = O\left(\frac{1}{(2\sqrt{x})^{2^n}}\right) = O\left(\frac{1}{2^{2^n}}\right)$.

   (c) A convergência do algoritmo para extrair raiz quadrada que é considerado no Ensino Fundamental tem convergência comparável com qual destes dois algoritmos?

2. Calcule a probabilidade λ_1 de um apostador acertar a megasena com uma aposta simples. Ache a probabilidade λ_k de um apostador ganhar em k semanas consecutivas a megasena, tendo feito, em cada uma destas semamas, um jogo simples.

(i) Encontre o maior k tal que $\lambda_k > 10^{-30}$.

(ii) Encontre o maior k tal que $\lambda_k > \frac{1}{p} + \frac{1}{q}$, onde p e q são números primos tendo em torno de 100 dígitos na base 10.

3. Neste exercício será feita a análise do último algoritmo apresentado na Subseção 3.5.2. Responda as seguintes perguntas:

(i) Qual o custo de realizar o passo 2? E o passo 3?

(ii) Qual o custo de executar o algoritmo para k diferentes valores de i?

(iii) Qual a probabilidade da fatoração não ter sido encontrada após estes k valores de i terem sido considerados?

(iv) O algoritmo pode nunca parar? Com qual probabilidade?

3.6 Assinatura no RSA

Na seção em que criptografia com chave pública foi introduzida apresentamos uma maneira eficiente de realizar assinaturas digitais, que funciona maravilhosamente na teoria. Na prática, surgem alguns problemas, já que os algoritmos de encifrar e de decifrar podem não se comportar como um par de funções que são uma a inversa da outra no conjunto de todas mensagens. Necessitamos tomar alguns cuidados na hora de assinar as mensagens. Discutiremos como isto pode ser feito no RSA.

Suponha, como antes, que Alice e Bob sejam usuários de nosso sistema. Sejam (n_a, e_a) e (n_b, e_b) as chaves públicas de Alice e Bob respectivamente. Seja d a chave privada de Alice. Alice necessita de sua chave privada para assinar a mensagem que mandará para Bob. Seja a um inteiro tal que $0 \leq a < L^r$ que está associado a um bloco B que será encifrado. No caso em que $n_a > n_b$, Alice faz o seguinte:

1. Calcula o resto b da divisão de a^{e_b} por n_b.

2. Calcula o resto c da divisão de b^d por n_a.

No caso em que $n_b > n_a$, Alice troca a ordem das operações executadas anteriormente:

1. Calcula o resto b da divisão de a^d por n_a.

2. Calcula o resto c da divisão de b^{e_b} por n_b.

Em ambos os casos, c, quando representado na base L, pode ser visto como um bloco B' com s letras. O bloco B' irá substituirá B na mensagem encifrada.

3.6.1 Exercícios

1. O que ocorre caso a ordem das operações seja invertida em qualquer um dos processos para assinatura do RSA?

2. Descreva os passos que Bob tem de ralizar para decifrar uma mensagem, com assinatura digital, que foi encaminhada através do RSA por Alice.

3.7 Chaves públicas × Métodos clássicos

Finalizamos este capítulo apresentando um método desenvolvido por Diffie e Hellman para gerar chaves por dois usuários, digamos Alice e Bob, de maneira virtual. (Estas chaves seriam de conhecimento apenas de Alice e Bob.)

O operador do sistema torna público:

- um grupo multiplicativo finito G; e

- um elemento g em G com ordem muito grande.

Alice escolhe um natural aleatório x_A no intervalo $[1, |G| - 1]$ e manda para Bob o elemento g^{x_A}. Bob escolhe um natural aleatório x_B no intervalo $[1, |G| - 1]$ e manda para Alice o elemento g^{x_B}. Observe que tanto Alice quanto Bob pode calcular

$$(g^{x_B})^{x_A} = g^{x_A x_B} = (g^{x_A})^{x_B}$$

tomando respectivamente a potência de ordem x_A e x_B do elemento que recebeu. Portanto, Alice e Bob podem combinar uma maneira de extrair chaves do elemento $g^{x_A x_B}$ que ambos conhecem. Estas chaves podem ser utilizadas em algum sistema de criptografia cujo tempo

para encifrar mensagens seja baixo como, por exemplo, o DES (Data Encryption Standard).

Caso um terceiro interceptasse a mesagem de Alice para Bob, ou vice-versa, teria o conhecimento de g^{x_A} ou g^{x_B}. Para obter x_A ou x_B teria de resolver o problema do "logaritmo" para G o que, no momento, é intratável em geral.

Capítulo 4

Encontrando primos

4.1 Introdução

Neste capítulo apresentaremos vários algoritmos para decidir primalidade, isto é, determinar quando um número natural é primo.

Seja n um número natural maior que 1. Se n não é primo, então existem inteiros a e b tais que

$$n = ab \text{ e } 1 < a \leq b < n.$$

Observe que $a \leq \sqrt{n}$, do contrário

$$n = ab \geq a^2 > (\sqrt{n})^2 = n.$$

Isto é, um número composto possui um divisor próprio menor ou igual que sua raiz quadrada.

Utilizando o resultado descrito no parágrafo anterior podemos escrever o nosso primeiro algoritmo para decidir a primalidade de um número natural n maior que 1:

1. Faça $d := 2$.
2. Se $d > \sqrt{n}$, então pare e retorne `PRIMO`.
3. Se d divide n, então pare e retorne `COMPOSTO`.

4. Incremente d de 1 e retorne ao passo 2.

Será que este algoritmo é eficiente para decidir a primalidade de um número tendo em torno de 100 dígitos decimais? O número de divisões que este algoritmo realizará, no pior dos casos, é em torno de 10^{50}. Este número é astronômico! Um computador realiza menos de 10^{10} destas divisões por segundo. Como um ano possui

$$60 \cdot 60 \cdot 24 \cdot 365 < 10^2 10^2 10^2 10^3 = 10^{2+2+2+3} < 10^{10}$$

segundos, em um ano, o computador executaria menos que 10^{20} divisões. Portanto, seriam necessários pelo menos 10^{30} anos para concluir o algoritmo. Do ponto de vista prático, este algoritmo não pode ser executado, já que, no caso em que n é primo, necessita de mais anos que o tempo de vida que resta ao Sol.

Este algoritmo é inviável, na prática, pois é exponencial no tamanho da entrada. No caso, a entrada do algoritmo é o natural n, escrito na base 2, que possui aproximadamente $\log_2 n$ dígitos. O número de divisões realizadas, no pior dos casos, será

$$\sqrt{n} - 1 = 2^{\log_2 \sqrt{n}} - 1 = 2^{\frac{1}{2} \log_2 n} - 1 = \sqrt{2}^{\log_2 n} - 1.$$

Podemos reduzir o número de divisões realizadas neste algoritmo significativamente: necessitamos dividir n por d, no terceiro passo, apenas no caso em que d é primo. Portanto, o número de divisões que este algoritmo realiza, no pior dos casos, será $\pi(\sqrt{n})$, onde $\pi(x)$ denota o número de primos menores ou iguais a x. O Teorema dos Números Primos afirma que

$$\pi(x) \sim \frac{x}{\ln x}.$$

Quando n tem em torno de 100 dígitos na base 10, $\sqrt{n}$ possui em torno de 50 dígitos na base 10. Logo $\pi(\sqrt{n})$ não está muito distante de

$$\frac{10^{50}}{\ln 10^{50}} = \frac{10^{50}}{50 \ln 10} > \frac{10^{50}}{100 \cdot 10} = 10^{47}. \tag{4.1}$$

Conseqüentemente a redução no número de divisões, apesar de significativa, é irrelevante para permitir que uma variante deste algoritmo possa ser utilizada na prática.

Omitiremos a demonstração do Teorema dos Números Primos, pois não é simples. Contudo, estabeleceremos o seguinte limite inferior para $\pi(x)$, quando x for um inteiro maior que 1,

$$\pi(x) \geq \left(\frac{\ln 2}{2}\right)\frac{x}{\ln x} = 0,3465735902799\ldots\frac{x}{\ln x} > \left(\frac{1}{3}\right)\frac{x}{\ln x}. \quad (4.2)$$

Note que o limite inferior obtido em (4.1) continua válido ao substituirmos

$$\frac{10^{50}}{\ln 10^{50}} \text{ por } \left(\frac{1}{3}\right)\frac{10^{50}}{\ln 10^{50}}.$$

Agora passamos a demonstrar (4.2). Para um natural m, considere o seguinte natural

$$n = \binom{2m}{m} = \frac{(2m)!}{(m!)^2}.$$

Temos que

$$n = \prod_{i=1}^{m}\left(\frac{m+i}{i}\right) \geq \prod_{i=1}^{m}\left(\frac{i+i}{i}\right) = 2^m. \quad (4.3)$$

Para cada primo p, seja e_p o maior inteiro tal que p^{e_p} divide n. Pelo exercício 2 da Seção 1.7,

$$e_p = \sum_{i\geq 1}\left\lfloor\frac{2m}{p^i}\right\rfloor - 2\sum_{i\geq 1}\left\lfloor\frac{m}{p^i}\right\rfloor = \sum_{i\geq 1}\left(\left\lfloor\frac{2m}{p^i}\right\rfloor - 2\left\lfloor\frac{m}{p^i}\right\rfloor\right)$$

Esta identidade pode ser reescrita como

$$e_p = \sum_{i=1}^{\left\lfloor\frac{\ln(2m)}{\ln p}\right\rfloor}\left(\left\lfloor\frac{2m}{p^i}\right\rfloor - 2\left\lfloor\frac{m}{p^i}\right\rfloor\right),$$

já que $p^i > 2m$ quando $i > \left\lfloor\frac{\ln(2m)}{\ln p}\right\rfloor$. Como, para todo número real y, $\lfloor 2y\rfloor - 2\lfloor y\rfloor \in \{0,1\}$, temos que

$$e_p = \sum_{i=1}^{\left\lfloor\frac{\ln(2m)}{\ln p}\right\rfloor}\left(\left\lfloor\frac{2m}{p^i}\right\rfloor - 2\left\lfloor\frac{m}{p^i}\right\rfloor\right) \leq \sum_{i=1}^{\left\lfloor\frac{\ln(2m)}{\ln p}\right\rfloor} 1 = \left\lfloor\frac{\ln(2m)}{\ln p}\right\rfloor. \quad (4.4)$$

Seja $\mathcal{P}$ o conjunto dos números primos menores ou iguais a $2m$. Temos que

$$n = \prod_{p \in \mathcal{P}} p^{e_p}.$$

Ao tomarmos o logaritmo em ambos os lados desta igualdade, obtemos que

$$\ln n = \sum_{p \in \mathcal{P}} e_p \ln p.$$

Por (4.4), temos que

$$\ln n \leq \sum_{p \in \mathcal{P}} \left\lfloor \frac{\ln(2m)}{\ln p} \right\rfloor \ln p \leq \sum_{p \in \mathcal{P}} \ln(2m) = \pi(2m) \ln(2m).$$

Por (4.3), temos que $\ln n \geq m \ln 2$. Portanto,

$$m \ln 2 \leq \pi(2m) \ln(2m).$$

Podemos reescrever esta desigualdade como

$$\left(\frac{\ln 2}{2}\right) \frac{2m}{\ln(2m)} \leq \pi(2m).$$

Isto é, chegamos a desigualdade (4.2) para $x = 2m$.

No caso de x ser ímpar, digamos $x = 2m - 1$, temos que $\pi(2m) = \pi(2m - 1)$. O resultado segue da desigualdade anterior pois $\frac{x}{\ln x}$ é uma função crescente quando $x > e$.

4.1.1 Exercícios

1. O algoritmo apresentado nesta seção pode ser escrito em paralelo. Supondo que podemos transformar um átomo em um processador, será possível construir um computador para executar este algoritmos em um ano?

2. Mostre que o número de primos menores ou iguais a $\sqrt{n}$, para um natural n, é exponencial em termos do número de dígitos de n na base 2.

3. Para um número real x, $\vartheta(x)$ é definida como a soma de $\ln p$ para todo primo p menor ou igual a x, sendo conhecida como a *função teta de Chebyshev*. Mostre que, para todo $\epsilon > 0$ e x suficientemente grande,

$$\frac{\vartheta(x)}{\ln x} \leq \pi(x) \leq (1+\epsilon)\frac{\vartheta(x)}{\ln x}.$$

4.2 Primalidade de grandes números

Nesta seção apresentaremos um algoritmo randomizado para decidir a primalidade de um natural que possui pelo menos 50 dígitos decimais. Este algoritmo irá utilizar o Pequeno Teorema de Fermat e um limite inferior para o quociente

$$\frac{\gamma(x)}{\pi(x)},$$

onde $\gamma(x)$ denota quantidade de números de Carmichael menores ou iguais ao número real x. Para x grande, isto é, $x \geq 10^{50}$, temos que este quociente é inferior a 10^{-15}. Conseqüentemente, caso saibamos que um natural com pelo menos 50 dígitos decimais é primo ou de Carmichael podemos assumir que este natural é um primo quando for uma de nossas escolhas para o RSA. Cometeremos um erro com probabilidade inferior a 10^{-15}, o que é irrelevante do ponto de vista prático. Contudo, caso este erro tenha sido cometido, não conseguiremos decifrar as mensagens que nos foram encifradas, e saberemos que cometemos um erro. Neste caso, escolhemos dois novos primos utilizando o algoritmo apresentado nesta seção. Para deixar claro que não teremos problemas, observamos que o algoritmo cometerá um erro a cada

1.000.000.000.000.000

tentativas. Temos muito mais chance de ganhar a mega-sena com um jogo simples!

Um natural composto n é dito de Carmichael quando, para todo natural a, n divide $a^n - a$. Isto é, o Pequeno Teorema de Fermat vale para n, mesmo n não sendo primo. A seguir apresentaremos uma caracterização destes números que será utilizada no algoritmo randomizado para decidir primalidade apresentado nesta seção.

Proposição 12. *As seguintes afirmações são equivalentes para um natural composto n:*

(i) n é de Carmichael.

(ii) $a^{n-1} = \overline{1}$, para todo $a \in \mathbb{Z}_n^*$.

Mais ainda, quando n for de Carmichael, temos que:

(iii) n é livre de quadrados.

(iv) $p-1$ divide $n-1$, para todo primo p que divide n.

Demonstração. Claramente (i) implica (ii) pois $a^n = a$ para todo $a \in \mathbb{Z}_n$ e, ao multiplicarmos esta identidade pelo inverso de a, quando este existir, chegamos a igualdade apresentada em (ii). Vamos assumir que (ii) vale. Nosso objetivo será estabelecer (i). Ao fazermos isto, mostraremos que (iii) e (iv) são verificadas para um natural n satisfazendo (ii). Como todo número de Carmichael satisfaz (ii) teremos também que (iii) e (iv) valem para tais números.

Seja p um primo que divide n. Existe inteiro positivo k tal que p^k divide n e p^{k+1} não divide n. Pela Proposição 10, exsite inteiro g tal que $\overline{g}$ é um gerador para $\mathbb{Z}_{p^k}$. Pelo Teorema Chinês dos Restos, existe um natural x tal que

$$x \equiv g \mod p^k \text{ e } x \equiv 1 \mod \left(\frac{n}{p^k}\right). \tag{4.5}$$

Em particular, $\overline{x} \in \mathbb{Z}_n^*$. Substituindo a por $\overline{x}$ em (ii), temos que

$$\overline{x}^{n-1} = \overline{1} \text{ em } \mathbb{Z}_n^*.$$

Como p^k divide n, concluímos que

$$\overline{x}^{n-1} = \overline{1} \text{ em } \mathbb{Z}_{p^k}^*. \tag{4.6}$$

Por (4.5), $\overline{x} = \overline{g}$ em $\mathbb{Z}_{p^k}$. Portanto, por (4.6),

$$\overline{g}^{n-1} = \overline{1} \text{ em } \mathbb{Z}_{p^k}^*.$$

Como $\overline{g}$ é um gerador para $\mathbb{Z}_{p^k}^*$, pelo Teorema de Lagrange, deduzimos que $p^{k-1}(p-1)$ divide $n-1$. Em particular, $p-1$ divide $n-1$.

Portanto, (iv) segue. Resta mostrar (iii). Se (iii) é falsa, então podemos escolher p de forma que $k \geq 2$. Neste caso p também divide $n-1$. Chegamos a uma contradição porque p divide n. Logo n é livre de quadrados. Isto é, verificamos (iii).

Pelo Teorema Fundamental da Aritmética, existem primos $p_1, p_2, \ldots, p_k$ distintos tais que $n = p_1 p_2 \cdots p_k$. Para cada $i \in \{1, 2, \ldots, k\}$, mostraremos que, para todo inteiro a,

$$a^n \equiv a \mod p_i. \tag{4.7}$$

Este é o caso quando p_i divide a. Necessitamos estabelecer (4.7) apenas no caso em que p_i não divide a. Logo $\overline{a} \in \mathbb{Z}_{p_i}^*$ e daí, pelo Pequeno Teorema de Fermat, $\overline{a}^{p_i-1} = \overline{1}$ em $\mathbb{Z}_{p_i}^*$. Por (iv), existe inteiro k tal que $n-1 = k(p_i-1)$. Portanto, em $\mathbb{Z}_{p_i}^*$,

$$\overline{a}^{n-1} = \overline{a}^{k(p_i-1)} = \left(\overline{a}^{p_i-1}\right)^k = \overline{1}^k = \overline{1}.$$

Isto é,

$$a^{n-1} \equiv 1 \mod p_i.$$

Obtemos (4.7) multiplicando esta congruência por a. De (4.7), temos que p_i divide $a^n - a$ para todo n. Conseqüentemente o produto destes números, que é n, divide $a^n - a$. Isto é, n é de Carmichael. □

Para naturais t e n considere o seguinte polinômio com coeficientes em $\mathbb{Z}_n$:

$$g_t(X) = X^t - \overline{1}.$$

Este polinômio foi estudado no capítulo anterior. O conjunto de suas raízes foi definido como:

$$G_t = \{a \in \mathbb{Z}_n : g_t(a) = \overline{0}\}.$$

O Pequeno Teorema de Fermat e a Proposição 12 asseguram que as seguintes afirmações são equivalentes:

(i) n é primo ou de Carmichael.

(ii) $G_{n-1} = \mathbb{Z}_n^*$.

Quando (i) ocorre, para um natural $n > 10^{50}$, a menos de uma probabilidade inferior a 10^{-15}, sabemos que n é primo. Portanto, necessitamos de um algoritmo randomizado para decidir (ii). Isto já foi feito no capítudo anterior. Naquele apresentamos um algoritmo para decidir quando (3.12) é satisfeita que, para $t = n - 1$, nada mais é que (ii).

4.2.1 Exercícios

1. Qual dentre os números $501, 521, 541, 561$ e 581 é de Carmichael?

2. Mostre que todo número de Carmichael é divisível por pelo menos três primos distintos.

3. Encontre todos os números de Carmichael da forma $3pq$, onde p e q são números primos distintos.

4. Para um natural k, suponha que $6k+1, 12k+1$ e $18k+1$ são todos primos. Mostre que $n_k = (6k+1)(12k+1)(18k+1)$ é de Carmichael.

5. Encontre todos os números de Carmichael da forma n_k, para $k \leq 10$.

4.3 Modificando um pouco o algoritmo

Seja n um natural. Será que n é primo? Se n é par, então n não é primo exceto quando for 2. Portanto, podemos supor que n é ímpar. Neste caso, existem naturais r e m, com m ímpar, tais que

$$n - 1 = 2^r m.$$

Para $a \in \mathbb{Z}_n$, $a \neq \overline{0}$, considere a seguinte seqüência:

$$a^m, a^{2m}, a^{4m}, \ldots, a^{2^{i-1}m}, a^{2^i m}, \ldots, a^{2^{r-1}m}, a^{2^r m}. \tag{4.8}$$

Note que esta seqüência pode ser facilmente computada pois cada termo é o quadrado do antecessor.

No caso de n ser primo, o último termo desta seqüência, pelo Pequeno Teorema de Fermat, será igual a $\overline{1}$. Mais ainda, como as raízes quadradas de $\overline{1}$ em $\mathbb{Z}_n$ são $\overline{1}$ e $\overline{-1}$, temos uma das duas alternativas:

(i) $a^m = \overline{1}$; ou

(ii) $a^{2^i m} = \overline{-1}$, para algum inteiro i tal que $0 \leq i < r$.

No caso de n ser composto, diremos que n é *pseudoprimo com respeito ao elemento* a quando (i) ou (ii) ocorre. Nesta seção, mostraremos que n não é pseudoprimo com respeito a pelo menos 75% dos elementos a, quando n é composto. Utilizaremos este fato para construir um algoritmo randomizado para decidir primalidade.

Teorema 13. *Seja n um número ímpar composto. Se $n - 1 = 2^r m$, para naturais r e m, com m ímpar, então n é pseudoprimo com respeito a no máximo 25% dos elementos pertencentes a $\mathbb{Z}_n - \{\overline{0}\}$.*

Demonstração. Nosso objetivo será estabelecer a seguinte desigualdade:

$$P_n = \frac{|\{a \in \mathbb{Z}_n : n \text{ é pseudoprimo com respeito a } a\}|}{n-1} \leq \frac{1}{4}. \quad (4.9)$$

Se n é pseudoprimo com respeito a a, então $a^{n-1} = \overline{1}$ e daí a possui inverso multiplicativo em $\mathbb{Z}_n$. Conseqüentemente (4.9) é equivalente a:

$$P_n = \frac{|\{a \in \mathbb{Z}_n^* : n \text{ é pseudoprimo com respeito a } a\}|}{n-1} \leq \frac{1}{4}. \quad (4.10)$$

Dividiremos a demonstração em dois casos.

Caso 1. *n não é livre de quadrados.*

Pela definição, existe primo p tal que p^2 divide n. Seja t um natural satisfazendo $n = p^2 t$. Pela Proposição 10, existe natural g tal que $0 < g < p^2$ e $\overline{g}$ é um gerador para $\mathbb{Z}_{p^2}^*$. Assuma que n é pseudoprimo com respeito a $\overline{a}$, onde a é um natural tal que

$$0 < a < n. \quad (4.11)$$

Em particular,

$$a^{n-1} \equiv 1 \mod n. \quad (4.12)$$

Vamos obter um limite superior para o número destes inteiros satisfazendo (4.16) e (4.12). De (4.12), temos que

$$a^{n-1} \equiv 1 \mod p^2. \tag{4.13}$$

Existe inteiro i tal que $0 \leq i < \phi(p^2) = p(p-1)$ e

$$a \equiv g^i \mod p^2, \tag{4.14}$$

pois $\overline{g}$ é gerador de $\mathbb{Z}^*_{p_2}$. De (4.13) e (4.14), concluímos que

$$a^{n-1} \equiv g^{i(n-1)} \equiv 1 \mod p^2.$$

Pelo Teorema de Lagrange, a ordem de $\overline{g}$ em $\mathbb{Z}_{p^2}$ divide $i(n-1)$. Isto é, $p(p-1)$ divide $i(p^2t-1)$. Portanto, i tem de ser múltiplo de p. Conseqüentemente $i = pj$ para um inteiro j tal que $0 \leq j < p-1$. De (4.16) e (4.14) obtemos que

$$a = g^{pj} + sp^2, \tag{4.15}$$

onde s é um inteiro satisfazendo $0 \leq s < t$. Logo existem no máximo $(p-1)t$ inteiros a, com $0 < a < n$, satisfazendo (4.15) e conseqüentemente (4.12). Portanto, n é pseudoprimo com respeito a no máximo $(p-1)t$ elementos de $\mathbb{Z}_n$. Logo

$$P_n \leq \frac{(p-1)t}{n-1} = \frac{(p-1)t}{p^2t-1} < \frac{(p-1)t}{(p^2-1)t} = \frac{1}{p+1} \leq \frac{1}{4},$$

pois n e ímpar e daí $p \geq 3$.

Caso 2. *n é livre de quadrados.*

Sejam $p_1, p_2, \ldots, p_k$ distintos tais que $n = p_1 p_2 \cdots p_k$. Para $i \in \{1, 2 \ldots, k\}$, existem naturais r_i e m_i, com m_i ímpar, tais que $p_i = 2^{r_i} m_i$, pois p_i é ímpar. Pela Proposição 9, existe inteiro g_i tal que $0 \leq g_i < p_i$ e $\overline{g_i}$ gera $\mathbb{Z}^*_{p_i}$. Sabemos que a função $\Psi : \mathbb{Z}^*_n \to \mathbb{Z}^*_{p_1} \times \mathbb{Z}^*_{p_2} \times \cdots \times \mathbb{Z}^*_{p_k}$ dada por $\Psi(\overline{a}) = (\overline{a}, \overline{a}, \ldots, \overline{a})$ é uma bijeção, onde a é um inteiro qualquer. Para um natural s, temos que

$$\Psi(\overline{a}^s) = \Psi(\overline{a^s}) = (\overline{a^s}, \overline{a^s}, \ldots, \overline{a^s}) = (\overline{a}^s, \overline{a}^s, \ldots, \overline{a}^s) := \Psi(\overline{a})^s. \tag{4.16}$$

Vamos fixar um inteiro a tal que $0 \leq a < n$ e $(a, n) = 1$. Para cada i, existe a_i, com $0 \leq a_i < p_i - 1$, tal que

$$\Psi(\overline{a}) = (\overline{g_1}^{a_1}, \overline{g_2}^{a_2}, \ldots, \overline{g_k}^{a_k}). \tag{4.17}$$

Agora caracterizaremos os a's tais que $\overline{a}^m = \overline{1}$ em $\mathbb{Z}_n$. Por (4.16) e (4.17), obtemos que

$$(\overline{1}, \overline{1}, \ldots, \overline{1}) = \Psi(\overline{1}) = \Psi(\overline{a}^m) = (\overline{g_1}^{a_1 m}, \overline{g_2}^{a_2 m}, \ldots, \overline{g_k}^{a_k m}).$$

Conseqüentemente esta igualdade será satisfeita se e somente se $p_i - 1 = 2^{r_i} m_i$ divide $a_i m$, para cada $i \in \{1, 2, \ldots, k\}$. O que é equivalente a

$$a_i \text{ ser múltiplo de } 2^{r_i} \frac{m_i}{(m, m_i)}.$$

Como $0 \leq a_i < p_i - 1$, existem (m, m_i) opções para a_i. Portanto, o número de raízes para $X^m - \overline{1}$ em $\mathbb{Z}_n$ é

$$(m, m_1)(m, m_2) \cdots (m, m_k).$$

Para $j \in \{0, 1, \ldots, r-1\}$, necessitamos descrever os a's tais que $\overline{a}^{2^j m} = \overline{-1}$ em $\mathbb{Z}_n$. Por (4.16) e (4.17), obtemos que

$$\begin{aligned}(\overline{-1}, \overline{-1}, \ldots, \overline{-1}) &= \Psi(\overline{-1}) = \Psi(\overline{a}^{2^j m}) \\ &= (\overline{g_1}^{2^j a_1 m}, \overline{g_2}^{2^j a_2 m}, \ldots, \overline{g_k}^{2^j a_k m}).\end{aligned}$$

Conseqüentemente esta igualdade será satisfeita se e somente se

$$p_i - 1 = 2^{r_i} m_i \text{ divide } 2^{j+1} a_i m \text{ e não divide } 2^j a_i m, \tag{4.18}$$

para cada $i \in \{1, 2, \ldots, k\}$. Em particular, $j < \min\{r_1, r_2, \ldots, r_k\}$. Observe que (4.18) é equivalente a

$$a_i \text{ ser múltiplo ímpar de } 2^{r_i - j - 1} \frac{m_i}{(m, m_i)}.$$

Como $0 \leq a_i < p_i - 1$, existem $2^j (m, m_i)$ opções para a_i. Portanto, o número de raízes para $X^{2^j m} + \overline{1}$ em $\mathbb{Z}_n$ é

$$2^{kj} (m, m_1)(m, m_2) \cdots (m, m_k),$$

quando $j < \min\{r_1, r_2, \ldots, r_k\}$, ou 0, caso contrário.

Portanto, n é pseudoprimo com respeito a exatamente

$$(m, m_1)(m, m_2)\cdots(m, m_k) + \sum_{j=0}^{\min\{r_1, r_2, \ldots, r_k, r\}-1} 2^{kj}(m, m_1)(m, m_2)\cdots(m, m_k)$$

elementos de $\mathbb{Z}_n$. Conseqüentemente

$$P_n = \frac{(m, m_1)(m, m_2)\cdots(m, m_k)}{n-1}\left(1 + \sum_{j=0}^{\min\{r_1, r_2, \ldots, r_k, r\}-1} 2^{kj}\right).$$

Substituindo a soma da progressão geomética de razão 2^k pelo seu valor temos que

$$P_n = \frac{(m, m_1)(m, m_2)\cdots(m, m_k)}{p_1 p_2 \cdots p_k - 1}\left(1 + \frac{2^{\min\{r_1, r_2, \ldots, r_k, r\}k} - 1}{2^k - 1}\right).$$

Note que

$$\begin{aligned}\frac{1}{p_1 p_2 \cdots p_k - 1} &< \frac{1}{(p_1 - 1)(p_2 - 1)\cdots(p_k - 1)} \\ &= \frac{1}{2^{r_1 + r_2 + \cdots + r_k} m_1 m_2 \cdots m_k}\end{aligned}$$

e daí

$$P_n < \frac{(m, m_1)(m, m_2)\cdots(m, m_k)}{2^{r_1 + r_2 + \cdots + r_k} m_1 m_2 \cdots m_k}\left(1 + \frac{2^{\min\{r_1, r_2, \ldots, r_k, r\}k} - 1}{2^k - 1}\right).$$

Como

$$1 + \frac{2^{\min\{r_1, r_2, \ldots, r_k, r\}k} - 1}{2^k - 1} \leq \frac{2^{\min\{r_1, r_2, \ldots, r_k, r\}k}}{2^{k-1}},$$

temos que

$$P_n < \left[\frac{2^{\min\{r_1, r_2, \ldots, r_k, r\}k}}{2^{r_1 + r_2 + \cdots + r_k}}\right]\left[\frac{1}{2^{k-1}}\right]\prod_{i=1}^{k}\frac{(m, m_i)}{m_i}.$$

O resultado segue, a menos que

$$k = 2, r_1 = r_2 = r, (m, m_1) = m_1 \text{ e } (m, m_2) = m_2.$$

Neste caso, temos que $n = p_1p_2$ e que $p_1 - 1$ e $p_2 - 1$ dividem $n - 1$. Podemos assumir que $p_1 > p_2$. Mas

$$n - 1 = p_1p_2 - 1 = (p_1 - 1)p_2 + p_2 - 1$$

e daí $n - 1$ deixa resto $p_2 - 1 < p_1 - 1$ quando dividido por $p_1 - 1$; um absurdo e o resultado segue. □

Vamos considerar mais uma vez o seguinte número $n = 1729$. Já mostramos que este número é de Carmichael. Sabemos que $n = 7 \cdot 13 \cdot 19$ e que $n-1 = 2^6 3^3$. Logo $r = 6$ e $m = 27$. Nas colunas da tabela seguinte aparecem respectivamente $a, a^{27}, a^{54}, a^{108}, a^{216}, a^{432}, a^{864}, a^{1728}$, onde a é um elemento de $\mathbb{Z}^*_{1729}$.

$\overline{2}$	$\overline{645}$	$\overline{1065}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$
$\overline{3}$	$\overline{664}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$
$\overline{4}$	$\overline{1065}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$
$\overline{5}$	$\overline{1217}$	$\overline{1065}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$
$\overline{6}$	$\overline{1217}$	$\overline{1065}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$
$\overline{8}$	$\overline{512}$	$\overline{1065}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$
$\overline{9}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$
$\overline{10}$	$\overline{1728}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$

De todas as bases testadas, 1729 é pseudoprimo com respeito apenas a $\overline{9}$ e $\overline{10}$.

Agora apresentamos um algoritmo para decidir a primalidade de um número natural ímpar n diferente de 1.

1. Inicie com o valor de i igual a 1.
2. Se $i > 50$, então pare e retorne n é `PRIMO`.
3. Escolha aleatoriamente um natural a tal que $1 < a < n$.
4. Se $(n, a) \neq 1$, então pare e retorne n é `COMPOSTO`.
5. Se n não é pseudoprimo com respeito a a, então pare e retorne n é `COMPOSTO`.

6. Incremente i de 1 e retorne ao passo 2.

Agora faremos a análise deste algoritmo. No passo 4, caso $(n, a) \neq 1$, temos que (n, a) é um divisor próprio de n. Portanto, n é realmente composto. No passo 5, caso o algoritmo afirme que n é composto, a resposta é correta. Contudo, no passo 2, pode ocorrer de n ser composto e o algoritmo afirmar que é primo. A chance disto ocorrer é mínima, pois n teria de ser pseudoprimo com respeito a 50 elementos de $\mathbb{Z}_n$ escolhidos de maneira aleatória. A probabilidade de n ser pseudoprimo com respeito a um destes elementos é inferior a $\frac{1}{4}$. Portanto, o algoritmo comete um erro com probabilidade inferior a

$$\left(\frac{1}{4}\right)^{50} < 10^{-30}.$$

O quarto passo do algoritmo pode ser eliminado porque $\overline{a}^{n-1} \neq \overline{1}$ em $\mathbb{Z}_n$ quando $(a, n) \neq 1$. Conseqüentemente, no passo 4, ao verificarmos as alternativas (i) e (ii) para a e n, na definição de pseudoprimo, concluímos que nenhuma é satisfeita e daí o algoritmo pararia retornando que n é composto.

Note que o custo de realizar o passo 4 e o 5, que são os de maior custo, é $O(\ln^3 n)$ cada. Isto é, este algoritmo é polinomial, pois realizamos apenas 50 interações.

Se a Hipótese de Riemann Estendida for verdadeira, então, caso n seja um número natural composto, existe um inteiro a tal que $1 < a < 2\ln^2 n$ tal que n não é pseudoprimo com respeito a $\overline{a}$. Portanto, o algoritmo que acabamos de apresentar pode ser transformado em um algoritmo determinístico polinomial, caso esta hipótese seja verificada. Escreva este algoritmo e estime o seu custo.

4.3.1 Exercícios

1. Mostre que 2047 é pseudoprimo com respeito a 2.

2. Na questão anterior, podemos substituir 2047 por um natural menor?

3. Encontre todos os naturais a, que são relativamente primos com 1729, tais que 1729 é pseudoprimo com relação a a.

4. Para um natural a, seja p um primo que não divide $a-1$ e a. Mostre que, quando
$$n = \frac{a^p - 1}{a - 1},$$
   (a) p divide $n-1$; e
   (b) $a^p \equiv 1 \mod n$.

5. Seja n um natural ímpar. Suponha que $n-1 = 2^r m$, para naturais r e m, com m ímpar. Utilizando o exercício anterior, para um natural a maior que 1, mostre que existe uma infinidade destes naturais n tais que $a^m \equiv 1 \mod n$. Escolha pares (a, p) tais que n seja composto. O conjunto de tais pares é infinito?

6. Para um natural a, seja p um primo que não divide $a-1, a$ e $a+1$. Mostre que, quando
$$n = \frac{a^{2p} - 1}{a^2 - 1},$$
   (a) $2p$ divide $n-1$; e
   (b) $a^{2p} \equiv 1 \mod n$.

7. Utilizando o exercício anterior, para um natural a maior que 1, mostre que existe uma infinidade de naturais n tais que $a^{n-1} \equiv 1 \mod n$. Quando n é composto, n é pseudoprimo com respeito a a?

8. Sejam a, k e n naturais tais que n é pseudoprimo com respeito a a. Mostre que n é pseudoprimo com respeito a a^k quando k é ímpar.

9. Encontre todos os naturais a tais que 561 é pseudoprimo com respeito a a.

10. Seja p um número primo. Mostre que $n = 2p + 1$ é primo se e somente se $2^{n-1} \equiv 1 \mod n$.

4.4 AKS

Nesta seção apresentaremos o único algoritmo polinomial conhecido para decidir a primalidade de um natural. Este algoritmo foi desenvolvido por Agrawal, Kayal e Saxena — daí o seu nome. O custo deste algoritmo é muito elevado. Portanto, para usos práticos, o algoritmo randomizado de Rabin, que foi apresentado na seção anterior, continua sendo utilizado. O algoritmo AKS é baseado no seguinte teorema que caracteriza os números primos, como o Teorema de Wilson, mas que, ao contrário deste, dá origem a um algoritmo polinomial para reconhecer primalidade. A sua demonstração será omitida tendo em vista que sua complexidade foge ao espírito destas notas. Ao longo desta seção, para simplificar a notação, $\log x$ denota o logaritmo de x na base 2.

Teorema 14. *Para um natural n diferente de 1, seja r um natural menor que n tal que a ordem de $\overline{n}$ em $\mathbb{Z}_r$ é maior que $\log^2 n$. Então n é primo se e somente se:*

(i) $\sqrt[k]{n}$ *não é inteiro, para todo natural k diferente de 1.*

(ii) Não existe primo menor que $r+1$ que divide n.

(iii) Para cada inteiro a tal que $1 \leq a \leq \sqrt{r}\log n$, $X^r - \overline{1}$ divide

$$(X+\overline{a})^n - (X^n + \overline{a})$$

no anel de polinômios com coeficientes em $\mathbb{Z}_n$.

Vamos analisar o custo de verificar cada um dos três itens da caracterização dos números primos apresentada no último resultado.

Note que $\log^2 n < r$. É possível mostrar que existe r tal que $r < \log^3 n$. Isto é $r = O(\ln^3 n)$. Depois discutiremos como encontrar r.

4.4.1 Verificando (i)

Observe que a raiz k-ésima de n é a solução real positiva do seguinte polinômio

$$f(X) = X^k - n.$$

Podemos adaptar o algoritmo da bisseção, que foi apresentado para a extração da raiz quadrada, para encontrar a raiz de $f(X)$. Seja m o menor inteiro tal que $km > n$. Note que a raiz de $f(X)$ está no interior do intervalo $[0, 10^m]$. Em cada laço do algoritmo, temos de fazer uma k-ésima potência, cujo resultado final é inferior a 10^{km} e, portanto, tem $O(\log n)$ dígitos. Conseqüentemente o custo de computar esta k-ésima potência é $O(\log k \log^2 n)$. O número de etapas que o algoritmo realiza para encontrar $\lfloor \sqrt[k]{n} \rfloor$ é $O(\log n)$. Logo o custo de encontrar $\lfloor \sqrt[k]{n} \rfloor$ é $O(\log k \log^3 n)$. Finalizamos verificando se o resultado encontrado é solução de $f(X)$. Caso seja, então n é a k-ésima potência de um inteiro. Caso contrário, n não é a k-ésima potência de um inteiro. Este processo tem de ser repetido para todo k no intervalo $[2, \lceil \log n \rceil]$. São $O(\log n)$ repetições, cada uma com custo $O(\log \log n \log^3 n)$, pois $k = O(\log n)$. Em resumo, checar (i) tem custo $O(\log^4 n \log \log n)$.

4.4.2 Verificando (ii)

Faremos isto dividindo n por todo natural no intervalo $[2, r]$. São $O(r)$ divisões, cada uma com o custo de $O(\log^2 n)$. O custo desta parte será de $O(r \log^2 n)$.

4.4.3 Multiplicando polinômios

Antes de verificarmos (iii), necessitamos discutir uma maneira rápida de multiplicar dois polinômios cujos coeficientes têm um número limitado de dígitos.

Nesta subseção discutiremos um algoritmo para multiplicar dois polinômios com ceficientes inteiros. Esta multiplicação será reduzida ao produto de dois inteiros convenientes. A análise do custo deste algoritmo que será feita nestas notas não exprime fielmente sua velocidade, pois utilizamos uma estimativa ruim para o custo da multiplicação de inteiros, que foi obtida através do algoritmo usual para ralizar esta operação. O custo deste algoritmo pode ser reduzido significativamente caso seja utilizado um algoritmo rápido para realizar a multiplicação de dois inteiros.

Existem naturais r e N, que dependem do par de polinômios cujo produto desejamos encontrar, que limitam respectivamente o grau e

o valor absoluto dos coeficientes. Portanto, assumiremos que os dois polinômios a serem multiplicados pertencem ao conjuto:

$$P_{N,r} = \left\{ \sum_{i=0}^{r-1} b_i X^i : b_i \in \mathbb{Z} \cap (-N, N], \text{ para todo } i \right\}.$$

Manteremos N e r fixos ao longo desta subseção. Considere a seguinte função:

$$\begin{array}{rccc} \Omega_{N,r}: & P_{N,r} & \to & \frac{\mathbb{Z}_{(2N)^r}}{f(2N)} \\ & f(X) & \mapsto & \end{array}$$

Como o domínio e o contra-domínio de $\Omega_{N,r}$ têm a mesma cardinalidade, para estabelecer que $\Omega_{N,r}$ é uma bijeção, será suficiente mostrar que $\Omega_{N,r}$ é injetiva. Sejam $f(X) = \sum_{i=0}^{r-1} f_i X^i$ e $g(X) = \sum_{i=0}^{r-1} g_i X^i$ polinômios tais que $\Omega_{N,r}(f(X)) = \Omega_{N,r}(g(X))$. Desejamos concluir que $f(X) = g(X)$. Argumentaremos por contradição. Suponha que $f(X) \neq g(X)$ e seja i o menor inteiro tal que $f_i \neq g_i$. Logo

$$\overline{0} = \Omega_{N,r}(f(X)) - \Omega_{N,r}(g(X)) = \sum_{j=i}^{r-1} (f_j - g_j)(2N)^j.$$

Portanto, existe inteiro m tal que

$$(2N)^r m = (f_i - g_i)(2N)^i + \sum_{j=i+1}^{r-1} (f_j - g_j)(2N)^j.$$

Esta identidade pode ser reescrita, após divisão por $(2N)^i$, como

$$f_i - g_i = 2N \left((2N)^{r-i-1} - \sum_{j=i+1}^{r-1} (f_j - g_j)(2N)^{j-i-1} \right).$$

Chegamos a uma contradição, pois $0 \neq |f_i - g_i| < 2N$ e o lado direito da última igualdade é múltiplo de $2N$. Portanto, $f(X) = g(X)$ e daí $\Omega_{N,r}$ é uma bijeção. Isto é, acabamos de associar a cada polinômio pertencente ao conjunto $P_{N,r}$ um dos possíveis restos da divisão por $(2N)^r$.

Lema 17. *Se $f(X) = \sum_{i=0}^{r-1} f_i X^i$ e $g(X) = \sum_{i=0}^{r-1} g_i X^i$ pertencentem a $P_{N,r}$, então $f(X)g(X)$ pertence a $P_{rN^2,2r-1}$.*

Demonstração. O grau de $f(X)g(X)$ é igual a soma dos graus de $f(X)$ e $g(X)$. Portanto, será no máximo $2r-2$. Necessitamos apenas obter o limite para os coeficientes de $f(X)g(X)$ como função de N e r. Se $f(X)g(X) = \sum_{i=0}^{2r-2} c_i X_i$, então

$$c_i = \sum_{j=\max\{0,i-(r-1)\}}^{\min\{r-1,i\}} f_j h_{i-j}.$$

Logo

$$\begin{aligned} |c_i| = \left| \sum_{j=\max\{0,i-(r-1)\}}^{\min\{r-1,i\}} f_j h_{i-j} \right| &\leq \sum_{j=\max\{0,i-(r-1)\}}^{\min\{r-1,i\}} |f_j||h_{i-j}| \\ &\leq \sum_{i=0}^{r-1} N^2 = rN^2. \end{aligned}$$

O resultado segue. □

Sejam $f(X) = \sum_{i=0}^{r-1} f_i X^i$ e $g(X) = \sum_{i=0}^{r-1} g_i X^i$ polinômios em $P_{N,r}$. Pelo Lema 17, $f(X), g(X)$ e $f(X)g(X)$ pertencem a $P_{rN^2,2r-1}$. Portanto, podemos recuperar os coeficientes de $f(X)g(X)$ a partir de $\Omega_{rN^2,2r-1}(f(X)g(X))$ que é igual a $\overline{f(2rN^2)g(2rN^2)}$ em $\mathbb{Z}_{(2rN^2)^{2r-1}}$. Portanto, os coeficientes de $f(X)g(X)$ podem ser obtidos utilizando o seguinte algoritmo:

1. Calcule $f := f(2rN^2)$ e $g := g(2rN^2)$.
2. Calcule $h := fg$.
3. Faça $i := 0$.
4. Seja c_i o inteiro pertencente ao intervalo $(-rN^2, rN^2]$ tal que $h - c_i$ seja divisível por $2rN^2$.
5. Faça $h := \frac{h-c_i}{2rN^2}$.
6. Faça $i := i + 1$.
7. Se $i > 2r - 1$, então pare e retorne $\sum_{i=0}^{2r-2} c_i X^i$. Senão retorne ao passo 4.

A saída deste algoritmo é o produto de $f(X)$ por $g(X)$. Estabelecemos esta fato, de maneira implícita, quando demostramos que $\Omega_{N,r}$ é uma bijeção. Fica como exercício para o leitor a sua verficação. Determinar o custo deste algoritmo, que é $O(r^2 \ln^2 N)$, também fica como exercício. Caso, na estimativa do custo, seja utilizado o algoritmo para realizar multiplicação rápida nos inteiros, que é utilizado nos pacotes que trabalham com aritmética ilimitada, seu custo passa a ser $\widetilde{O}(r(\ln r + \ln N))$, onde $\widetilde{O}(a)$ denota $O(a \ln^{O(1)} a)$.

4.4.4 Verificando (iii)

Vamos considerar o resto da divisão de um polinômio com coeficientes em $\mathbb{Z}_n$ por $X^r - \overline{1}$. Podemos encontrar este resto substituindo toda ocorrência de X^r por $\overline{1}$. Por exemplo, X^{3r+5} é transformado em X^5. Em geral, o resto da divisão do polinômio

$$f(X) = \sum_{i=0}^{m} a_i X^i,$$

onde $a_0, a_1, \ldots, a_m$ pertencem a $\mathbb{Z}_n$, por $X^r - \overline{1}$ é

$$\sum_{i=0}^{r-1} \left(\sum_{j=0}^{\lfloor \frac{m-i}{r} \rfloor} a_{i+jr} \right) X^i.$$

Seja N um natural tal que $n \leq 2N$. Por exemplo, $N = \lceil \frac{n}{2} \rceil$. Para cada elemento a de $\mathbb{Z}_n$, existe inteiro a' no intervalo $(-N, N]$ tal que $a = \overline{a'}$. Quando a' não for único, escolha a' o maior possível. Portanto, um resto da divisão de um polinômio com coeficientes em $\mathbb{Z}_n$ por $X^r - \overline{1}$ é naturalmente identificado com um polinômio com coeficientes inteiros, pertencentes ao intervalo $(-N, N]$, e grau no máximo $r-1$. Isto é, um elemento de $P_{N,r}$. Note que restos diferentes são identificados com polinômios diferentes. Formalmente, o polinômio $\sum_{i=0}^{r-1} a_i X^i$, com coeficientes em $\mathbb{Z}_n$, é identificado com o polinômio $\sum_{i=0}^{r-1} a'_i X^i$.

Utilizaremos o algoritmo de multiplição de polinômios para computar $(X + \overline{a})^n$ no terceiro item do Teorema 14. Esta potência pode

ser calculada, utilizando algoritmo similar ao descrito para computar potências em $\mathbb{Z}_n$, fazendo-se $O(\ln n)$ multiplicações de polinômios pertencentes a $P_{N,r}$. O custo de verificar (iii), para um a fixo, é $O(r^2 \ln^3 n)$. Como (iii) tem de ser verificado para todo a no intervalo $[1, \sqrt{r} \log n]$, o custo de verificar completamente (iii) é $O(r^{\frac{5}{2}} \ln^4 n)$.

4.4.5 Encontrando r

Existe um r tal que $r < \log^3 n$. Note que este limite superior é muito bom, pois $\log^2 n < r$.

Encontraremos tal r da seguinte maneira: para todo inteiro i no intervalo $I := [1, \lceil \log^2 n \rceil]$ e inteiro s satisfazendo $s > \lceil \log^2 n \rceil$, calculamos $n^i \mod s$ até encontrarmos um s tal que a ordem de $\overline{n}$ em $\mathbb{Z}_s$ não pertença ao intervalo I. Tomamos este s para ser o nosso r. Pela estimativa no tamanho de r, temos de considerar no máximo $O(\ln^3 n)$ destes s e para cada s fazer no máximo $O(\ln^2 n)$ pontências, já que podemos parar a computação, para um s fixo, caso a ordem de $\overline{n}$ em $\mathbb{Z}_s$ seja determinada. O total de potências a serem calculadas é $O(\ln^5 n)$. Cada uma com custo de $O(\ln^3 \ln n)$. Este custo é inferior ao da verificação de (iii). Portanto, o custo do AKS é $O(\ln^{11,5} n)$. Uma análise mais cuidadosa, utilizando o custo do algoritmo de multiplicação rápida para inteiros, reduz o custo deste algoritmo para $\widetilde{O}(\ln^{7,5} n)$, o que ainda é muito elevado. Compare com o custo do algoritmo randomizado de Rabin, que é $O(\ln^3 n)$ — esta estimativa foi obtida utilizando o algoritmo clássico para multiplicação.

4.4.6 Exercícios

1. Seja n um natural. Para um primo p que divide n, mostre que p não divide $\binom{n}{p}$.

2. Usando o exercício anterior, mostre que um natural n diferente de 1 é primo se e somente se $(X + \overline{1})^n = X^n + \overline{1}$ no anel de polinômios com coeficientes em $\mathbb{Z}_n$.

3. A caracterização de primos apresentada no exercício anterior dá origem a um algoritmo polinomial para decidir primalidade?

4. No segundo exercício, substitua $\overline{1}$ por $\overline{a}$, onde a é um inteiro qualquer. As implicações ainda funcionam neste caso?

5. O conjunto $P_{N,r}$ é fechado com relação ao produto?

6. Seja $f(X) = \sum_{i=0}^{r-1} a_i X^i$ um polinômio pertencente a $P_{N,r}$. Para um natural a maior que 1, considere o seguinte algoritmo para computar $f(a)$:

   1. Faça $p := a_{r-1}$ e $i := r - 2$.
   2. Se $i < 0$, então pare e retorne p.
   3. Faça $p := pa + a_i$.
   4. Incremente i de 1 e retorne ao passo 2.

   Mostre que:

   (a) O valor de p no passo 3 é limitado por Na^r.

   (b) O custo de realizar um laço deste algoritmo é $O(\ln a \ln N + r \ln^2 a)$ — assuma que o custo de multiplicar naturais x e y é $O(\ln x \ln y)$.

   (c) Quando $a > N$, o custo deste algoritmo é $O(r^2 \ln^2 a)$.

   (d) Estime o custo de realizar o passo 1 do algoritmo de multiplicar polinômios.

7. Estime o custo de multiplicar dois polinômios em $P_{N,r}$.

Capítulo 5

Referências bibliográficas comentadas

5.1 Introdução

Neste capítulo, listamos alguns livros que achamos interessantes visando complementar a matemática que abordamos nestas notas de aulas. A respeito de cada um deles, tecemos alguns poucos comentários.

5.2 Sobre criptografia com chave pública

O livro escrito por Neal Koblitz e publicado pela Springer-Verlag, cujo título é *A course in number theory and cryptography* considera a maior parte do material tratado nestas notas. Além do mais, contém algoritmos para fatoração de números inteiros e aborda curvas elípticas. Tenho a primeira edição que foi publicada em 1987.

Em 1999, Shor publicou um artigo em que conseguia fatorar inteiros em tempo polinomial desde que tivesse um computador quântico possuindo pelo menos tantos qbits quanto o número de bits do inteiro

a ser fatorado. Tal computador está muito longe de ser construído com o atual conhecimento disponível. Caso o seja, o RSA se torna completamente inútil. O livro *Post-quantum cryptography*, editado por Daniel Bernstein, Johannes Buchmann e Erik Dahmen, e publicado pela Springer-Verlag, aborda sistemas de criptografia com chave pública que são seguros mesmo diante de tal computador.

Em português, recomendo o livro de Severino Collier Coutinho, entitulado *Números inteiros e criptografia RSA*, publicado pelo IMPA. Este livro foi escrito para uma disciplina introdutória da mesma forma que estas notas. Infelizmente não disponho mais de minha cópia: foi emprestado para um estudante...

5.3 Sobre curvas elípticas

Curvas elípticas são objetos matemáticos facinantes e altamente sofisticados. Têm inúmeras aplicações nos tópicos considerados nestas notas. São utilizadas nos melhores algoritmos para fatoração de inteiros, em algoritmos randomizados para decidir primalidade e em alguns sistemas de criptografia com chave pública. O livro *Elliptic curves: number theory and cryptography*, escrito por Lawrence Washington e publicado pela Chapman & Hall, é excelente. Aborda curvas elípticas e apresenta as aplicações relacionadas com os tópicos abordados nestas notas de aulas.

5.4 Sobre números primos

Para aqueles que desejam estudar o algoritmo para decidir primalidade, conhecido como AKS, nos mínimos detalhes, existe uma referência em português disponível: o livro *Primalidade em tempo polinomial: uma introdução ao algoritmo AKS*, também escrito por Severino Collier Coutinho e publicado pelo IMPA.

O Livro a respeito dos números primos foi escrito por duas das maiores autoridades na área: Richard Crandall e Carl Pomerance. O título dá uma idéia de sua abrangência *Prime numbers: a computational perspective*. Este livro é excelente e foi publicado pela Springer-Verlag. A leitura não é simples e requer uma certa maturidade matemática. Tenho a primeira edição, que foi publicada em

2001, e ainda não abordava o algorito AKS. Questão rapidamente resolvida na segunda edição.

Para um livro mais elementar recomendo o livro de David Bressoud, também publicado pela Springer-Verlag, e entitulado de *Factorization and primality testing*. Os dois últimos capítulos tratam de curvas elípticas e suas aplicações, em particular, apresenta um algoritmo para fatorar inteiros.

5.5 Sobre algoritmos em teoria dos números

O livro *A computational introduction to number theory and algebra*, escrito por Victor Shoup e publicado pela Cambridge University Press, contém todos os algoritmos abordados nestas notas e muitos outros. É um livro muito bom, mas requer uma certa maturidade matemática para sua leitura.