Criptografia

S. C. Coutinho

Texto já revisado pela nova ortografia.

Antes de Começar

Estas notas tratam de uma aplicação da matemática à criptografia. Embora algumas pessoas ainda associem mensagens codificadas a 007 ou outros agentes igualmente secretos, há mais de uma década que esta não é a aplicação mais importante da criptografia. Isto porque, hoje em dia, uma grande variedade de transações que envolvem dinheiro são feitas de maneira eletrônica, desde compras por cartão de crédito via internet a saques em caixas eletrônicos. A informação referente a estas transações segue por linha telefônica ou redes de alta-velocidade e, em ambos os casos, está facilmente sujeita a escutas.

Se a história acabasse aí, eu seria o primeiro a desejar que os bancos regridissem à era do papel! Felizmente, estas informações não trafegam em aberto pela rede telefônica, elas são codificadas, de modo que só o banco, empresa de cartão de crédito ou loja que você está utilizando consegue ler a informação. Assim, mesmo que alguém intercepte a informação com a intenção de esvaziar sua conta, ele não conseguirá interpretar suas informações, que continuarão seguras.

Os processos pelos quais informações enviadas eletronicamente são codificadas depende, de maneira crucial, do uso da matemática. O

mais curioso é que até os anos 1960, a teoria dos números, que é a parte da matemática mais utilizada nas aplicações à criptografia, era considerada quase que destituída de utilidade prática.

O que os matemáticos entendem como teoria dos números é o estudo das propriedades dos *números inteiros*, e não de quaisquer tipos de números. Por exemplo, questões referentes à fatoração de inteiros, ao cálculo do máximo divisor comum e ao estudo dos números primos, fazem parte desta teoria. Na verdade, juntamente com a geometria, essa é uma das áreas mais antigas da matemática.

Nestas notas desenvolvemos os métodos da teoria dos números necessários às aplicações em um sistema de criptografia específico, o chamado RSA. Há duas razões para isto. A primeira é que os resultados matemáticos utilizados neste sistema são relativamente elementares; a segunda é que se trata do *mais utilizado* dos métodos de criptografia atualmente em uso.

Estas notas se dirigem a um estudante com conhecimento básico sobre a fatoração de inteiros e primos, que tenha certa facilidade no cálculo com fórmulas elementares e que tenha interesse matemático suficiente para apreciar argumentos de demonstrações bastante básicas. Gostaria de agradecer a todas as pessoas que me ajudaram na preparação das notas, especialmente Florêncio Ferreira Guimarães Filho que primeiro sugeriu a ideia destas notas, Suely Druck e Mário Jorge Dias Carneiro que leram todo o texto e deram inúmeras sugestões para melhorá-lo e a Francisca França que leu todo o texto, corrigindo-o, revisando-o e preparando-o para a publicação.

Rio de Janeiro, 13 de maio de 2008 S. C. Coutinho

Sumário

Introdução

O foco deste livro é o método de *criptografia de chave pública* conhecido como RSA.[1] Toda a matemática que vamos estudar estará ligada diretamente a este método. Na introdução apresentaremos a ideia central por trás do funcionamento do RSA.

Criptografia

Em grego, *cryptos* significa secreto, oculto. A *criptografia* estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. É a arte dos "códigos secretos".

O Código de César

Um dos códigos secretos mais simples consiste em substituir uma letra do alfabeto pela seguinte. Por exemplo, a mensagem AMO A

[1] Se sua curiosidade para saber o que as letras significam é irresistível, olhe na página 9

OBMEP seria codificada como

$$BNPBPCNFQ.$$

Um código semelhante a este foi usado, por exemplo, pelo ditador romano Júlio César para comunicar-se com as legiões romanas em combate pela Europa. Este parece ser o primeiro exemplo de um código secreto de que se tem notícia.

Figura 1: Júlio César (100-44 a.C.)

Vejamos como codificar uma mensagem simples. Códigos como o de César padecem de um grande problema: são muito fáceis de "quebrar". Quebrar um código significa ser capaz de *ler* a mensagem, mesmo não sendo seu destinatário legítimo. Na verdade, qualquer código que envolva substituir cada letra sistematicamente por outro símbolo qualquer sofre do mesmo problema. Isto ocorre porque a frequência média com que cada letra aparece em um texto de uma dada *língua* é mais ou menos constante. Por exemplo, a frequência média de cada letra na língua portuguesa é dada na tabela 1.

Letra	%	Letra	%	Letra	%	Letra	%
A	14,64	G	1,30	N	5,05	T	4,34
B	1,04	H	1,28	O	10,73	U	4,64
C	3,88	I	6,18	P	2,52	V	1,70
D	4,10	J	0,40	Q	1,20	X	0,21
E	12,57	L	2,78	R	6,53	Z	0,47
F	1,02	M	4,75	S	7,81		

Tabela 1: Frequência das letras no português

Assim, apenas contando a frequência de cada símbolo no texto, podemos descobrir a que letra correspondem os símbolos mais frequentes. Isto geralmente é suficiente para quebrar o código e ler toda a mensagem. Observe, entretanto, que este método para quebrar o código só funciona bem se a mensagem for longa. É fácil escrever uma mensagem curta cuja contagem de frequência seja totalmente diferente da contagem de frequência média do português. Por exemplo, em "Zuza zoou da Zezé" a letra mais frequente é o Z que aparece 5 vezes em um texto de 14 letras. Como $5/14 = 0,35...$ a porcentagem do Z no texto acima é de cerca de 35%; muito acima dos usuais $0,47\%$. Já o A aparece uma só vez, o que dá uma porcentagem de cerca de 7%; portanto, abaixo dos 14% usuais.

SUMZFI GCSGC SVZFC LZLSJ EZQSL HIFUI JDZQS LTSRF SGCSJ UOZSZ OJTZL ZOEEO LHMSE ESDSL IECLU ILHCD ZTIFE SZMOJ QCZSU IJPSU OTZZL ZOIFH ZFDST IHFIU SEEIH ITSES FZCDI LZDOA ZTIIG CSDIF JZOJB OZBSO EDITI EIEUI TOQIE GCSSJ BIMBS LECVE DODCO UZITS MSDFZ EUILI IGCSS EDZLIE CDOMO AZJTI HZFZU ITORO UZFSE DZLSJ EZQSL JZBSF TZTSZ MQCJE TIEHF OLSOF IEUIL HCDZT

IFSER IFZLU FOZTIE HFSUO EZLSJ DSHZF ZZNCT ZFZGC SVFZFI EUITO QIEES UFSDI ECEZTI EHSMIE ZMSLZSE TCFZJDS ZESQC JTZQC SFFZL CJTOZM SJDFS SEDSE SEDZB ZIUIM IEEICL UILHC DZTIF UIEJD FCOTI JZOJQ MZDSF FZHIF CLZSG COHSM OTSFZ TZHIF ZMZJD CFOJQ CLTIE RCJTZ TIFSE TZUILH CDZUZI UOSJDO ROUZ

Exercício 1. *Será que você notou que o parágrafo acima foi codificado? Use o método de contagem de frequência para quebrar o código e poder decodificar e ler o parágrafo. Para* não *simplificar as coisas, foram eliminados espaços, acentos e pontuação.*

Códigos em Bloco

Por sorte, existe uma maneira simples de tornar inviável a aplicação de uma contagem de frequência. Para isso, subdividimos a mensagem em blocos de várias letras e embaralhamos estes blocos. Por isso este processo de criptografar uma mensagem é conhecido como *código de bloco*. Por exemplo, considere a mensagem AMO A OBMEP. Para codificá-la seguiremos os seguintes passos:

- eliminamos os espaços e completamos a mensagem com um A no final, caso tenha uma quantidade ímpar de letras;
- subdividimos a mensagem em blocos de duas letras;
- refletimos cada bloco;
- permutamos os blocos trocando o primeiro com o último, o terceiro com a antepenúltimo, e assim por diante, mas deixando os outros como estão.

Aplicando isto, passo a passo, à mensagem acima, obtemos primeiro

AMOAOBMEPA

depois

AM-OA-OB-ME-PA

em seguida

MA-AO-BO-EM-AP

e, finalmente,

AP-AO-BO-EM-MA

que nos dá como mensagem codificada

APAOBOEMMA.

Exercício 2. *Discuta as seguintes questões com seus colegas:*

(a) Por que a contagem de frequência não funciona quando usamos códigos em bloco?

(b) Por que escolhemos acrescentar exatamente a letra A quando a mensagem tem quantidade ímpar de letras, em vez de usar, por exemplo, X ou Y?

Apesar de códigos como este serem melhores que o código de César, eles apresentam uma grande desvantagem quando se trata de

aplicações comerciais da criptografia. Por exemplo, digamos que resolvo fazer uma compra via web usando o meu computador, em uma loja em que nunca comprei antes. Para isso entro na página da loja, escolho os produtos que desejo e, quando estou pronto para comprar, escolho "ir para o caixa". O pagamento será feito usando o meu cartão de crédito. Para isso, preciso informar a loja sobre os dados do meu cartão: geralmente o número e a data de vencimento. Mas isto significa que qualquer outra pessoa que tenha estes dados pode fazer compras em meu nome. Para evitar este problema, as informações sobre o meu cartão são codificadas pelo meu computador antes de serem enviadas.

Note, contudo, que meu computador não pode usar um código qualquer para codificar estas informações, porque a loja precisa lê-las e, para isso, tem que saber como decodificar a mensagem. Na prática o que ocorre é que o meu computador comunica-se com o da loja, que lhe informa como deve ser feito o processo de codificação. Isto é, meu computador codifica as informações do cartão de crédito usando um processo de codificação que é enviado pela loja.

Infelizmente os códigos de blocos não se prestam a este tipo de aplicação porque o computador da loja usa a linha telefônica (ou de banda larga) à qual meu computador esta interligado para enviar o processo de codificação a ser utilizado. Como é fácil pôr uma escuta na linha, uma outra pessoa pode facilmente descobrir como meu computador vai codificar as informações sigilosas que serão enviadas à loja. Usando a mesma escuta é fácil interceptar também as mensagens que contêm os dados do cartão. Mas isto basta porque, se sabemos como foi feito o embaralhamento dos blocos, podemos facil-

mente desfazê-lo e ler os dados do cartão!

A única maneira de contornar este problema é ter acesso ao que é conhecido como um *canal seguro*: uma maneira secreta de fazer a informação sobre o processo de codificação chegar até o computador do usuário da loja. Talvez a loja pudesse mandar, pelo correio registrado, um cartão especial com os dados a serem usados para a codificação. O problema é que isto tornaria a transação lenta, já que seria necessário esperar dias pela chegada do cartão – nesse meio tempo eu talvez preferisse escolher uma loja real, mesmo que fosse longe da minha casa. E ainda há outro problema, mais sério. Se o meu computador for invadido por um "hacker", o processo de codificação será descoberto e qualquer mensagem enviada com ele poderá ser lida.

Códigos de Chave Pública

As dificuldades que relacionamos acima parecem condenar de maneira irremediável a possibilidade de fazer transações pela web. Afinal, seja qual for o código utilizado, se sabemos como fazer a codificação, basta desfazê-la e decodificamos a mensagem. Ou não?

De fato, isto é basicamente verdade; mas há um porém. Acontece que podemos imaginar um processo que seja fácil de fazer mas muito difícil de desfazer e, ao utilizá-lo para criptografar uma mensagem, estaríamos garantindo que quem a interceptasse, mesmo sabendo como foi codificada, teria um trabalho enorme em decodificá-la. Abusando um pouco da fantasia, podemos imaginar que o trabalho de desfazer o processo levasse tanto tempo que ninguém conseguisse pô-lo em

prática. É claro que quão difícil será desfazer o procedimento depende dos recursos disponíveis a quem interceptou a mensagem.

Vejamos um exemplo. Você já viu uma dessas armadilhas usadas para pescar lagostas? Elas consistem de uma gaiola com uma porta fechada atrás e uma entrada para a lagosta na frente. O segredo está na entrada, que tem a forma de um funil: larga na parte externa e cada vez menor à medida que a lagosta vai entrando na gaiola. Para uma ilustração da entrada da armadilha veja a figura 2.

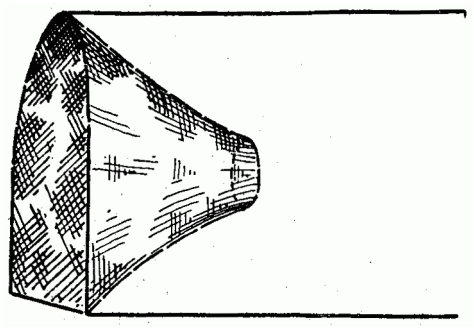


Figura 2: Entrada de armadilha de lagosta

A lagosta fica presa na gaiola porque, para poder sair, teria que encontrar e passar pela parte estreita do funil, que é um problema complicado demais para uma lagosta, cujo cérebro tem o tamanho aproximado de uma ervilha. Não preciso dizer que uma armadilha desse tipo não funcionaria para pegar um macaco, nem mesmo um passarinho.

Muito interessante, mas que problema matemático satisfaz esta condição de ser "fácil de fazer e difícil de desfazer", para que possamos utilizá-lo em criptografia? Isto é o que veremos na próxima seção. Por

enquanto, vamos só observar que tais códigos são conhecidos como de *chave pública*, já que o processo (ou chave) de codificação pode ser conhecido de qualquer um sem comprometer a segurança do código.

Criptografia RSA

O mais conhecido dos métodos de criptografia de chave pública é o RSA. Este código foi inventado em 1977 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T.), uma das melhores universidades americanas. As letras RSA correspondem às iniciais dos inventores do código. Há vários outros códigos de chave pública, mas o RSA continua sendo o mais usado em aplicações comerciais.

O Método RSA

A descrição completa do funcionamento do RSA é justamente o tema desta apostila. Para entender como funciona precisaremos estudar várias ideias e técnicas novas de matemática. Nesta seção explicaremos apenas o suficiente sobre o RSA para que você entenda como é possível um problema ser "fácil de fazer e difícil de desfazer". Isto também nos ajudará a identificar os problemas matemáticos que precisaremos abordar para poder discutir os detalhes do funcionamento do RSA.

Digamos que você vai criar uma implementação do RSA para uma determinada loja, que vai usá-lo na codificação de dados de clientes em compras pela internet. Para começar, você precisa escolher

dois números *primos distintos* e multiplicá-los, obtendo um número inteiro n. A loja manterá secreta a informação sobre quais são os primos escolhidos, porque é isto que é necessário para decodificar as mensagens enviadas usando a versão do RSA que você está construindo. Já n vai ser enviado para o computador de qualquer pessoa que compre nessa loja pela web, porque é dele que o computador do usuário necessita para codificar os dados sobre o do cartão de crédito e enviá-los ao computador da loja. Portanto, no caso do RSA, o problema "fácil de fazer e difícil de desfazer" é simplesmente multiplicar dois primos.

Já consigo imaginar você pensando:

> Só isso? Mas para desfazer o problema basta fatorar o número e achar os primos!

É verdade, mas há um detalhe que esqueci de contar: estes números primos serão muito, muito grandes. Na prática uma chave segura de RSA é gerada a partir de números primos de cerca de 100 algarismos cada, de forma que n, que é o produto destes primos, terá cerca de 200 algarismos. Acontece que, como veremos na página 29, podem ser necessários zilhões de anos para fatorar um número deste tamanho e achar seus fatores primos – mesmo se usarmos os mais poderosos computadores existentes atualmente.

Resumindo:

- para implementar o RSA escolhemos dois primos distintos muito grandes p e q e calculamos o produto $n = p \cdot q$;
- para codificar uma mensagem usamos n;

- para decodificar uma mensagem usamos p e q;
- n pode ser tornado público;
- p e q precisam ser mantidos em segredo;
- quebrar o RSA consiste em fatorar n, que leva muito tempo se n for grande.

Teoria de Números

O que vimos acima sugere que os principais problemas matemáticos relacionados ao RSA são: como achar números primos e como fatorar um número. A área da matemática a que estes problemas pertencem é conhecida como *teoria de números* e tem por objetivo geral o estudo das propriedades dos números inteiros. Entre os problemas que teremos que estudar para podermos descrever completamente o RSA também estão:

- como calcular os restos da divisão de uma potência por um número dado;
- como achar um número que deixa restos especificados quando dividido por uma série de números dados;
- como estabelecer critérios de divisibilidade por números primos.

Há muitos outros problemas que são parte da teoria dos números, mas dos quais não trataremos aqui, entre eles:

1. calcular o máximo divisor comum entre dois números dados;

2. determinar todos os inteiros a, b e c que satisfazem $a^2+b^2=c^2$;

3. mostrar que se três inteiros a, b e c satisfazem $a^n+b^n=c^n$, onde $n>2$ é um inteiro positivo, então a, b ou c têm que ser iguais a zero;

4. provar que $2^{2^n}+1$ é composto se $n>4$;

5. provar que todo número par é soma de dois primos ímpares;

6. determinar todos os inteiros consecutivos que são potências de números inteiros.

Os problemas acima têm grau de dificuldade muito variável. A solução de alguns deles é conhecida desde a antiguidade, como é o caso de (1) e (2). Na verdade, é bem provável que você saiba resolver (1) usando o método descrito por Euclides em seu livro *Elementos* escrito por volta de 300 a.C.; já (2) está relacionado ao Teorema de Pitágoras o que talvez baste para lembrar-lhe de algumas soluções possíveis.

Todas as outras questões são muito mais difíceis. Para começar temos (3), que é muito parecida com (2), exceto pelo fato do expoente n ter que ser pelo menos 3. Este problema tem uma história muito interessante. Em algum momento entre 1621 e 1636 o francês Pierre de Fermat, magistrado da corte de Toulouse, adquiriu uma cópia da recém-publicada tradução latina da *Aritmética* escrita pelo matemático grego Diofanto mais de mil anos antes. Fermat, que era um matemático amador, leu o texto de Diofanto, fazendo várias anotações na margem do texto. Em uma dessas anotações ele afirmou ter uma demonstração do fato enunciado em (3) mas, segundo ele, o

espaço disponível na margem do livro não seria suficiente para conter seu argumento.

É improvável que a demonstração de Fermat estivesse correta, já que o resultado permaneceu sem demonstração até 1995. Como este foi o último resultado enunciado por Fermat a ser demonstrado, tornou-se conhecido como o *Último Teorema de Fermat*. Para complicar, os métodos usados por A. Wiles em sua prova de (3) são extremamente sofisticados e sequer existiam há 50 anos atrás.

A questão (4) é outra que está ligada ao nome de Fermat. Na verdade, o número

$$F(n) = 2^{2^n} + 1$$

é conhecido como o *n-ésimo número de Fermat* porque, em uma de suas cartas a um outro matemático, Fermat propôs que $F(n)$ seria *sempre* primo, qualquer que fosse o valor de n. De fato, calculando $F(n)$ para n de 0 a 4 obtemos os números listados na tabela 2.

n	$F(n)$
0	3
1	5
2	17
3	257
4	65537

Tabela 2: Números de Fermat primos

que são todos primos. Aparentemente, foi nessa tabela que Fermat baseou-se para fazer a sua afirmação. Infelizmente, generalizar a partir de alguns casos é sempre uma prática perigosa em matemática e, neste caso, Fermat deu-se realmente mal. Nenhum número primo da

forma $F(n)$ é conhecido quando $n > 4$, daí o problema enunciado em (4), que ninguém até hoje sabe como resolver.

A questão (5) é conhecida como *Conjectura de Goldbach*, em homenagem a Christian Goldbach, um outro matemático amador, que viveu na mesma época que Euler, com quem trocava frequentes cartas sobre matemática. Embora se saiba que todo número par com menos de 18 algarismos seja mesmo a soma de dois primos ímpares, ninguém até hoje conseguiu provar o enunciado de Goldbach. Apesar disso, alguns resultados parciais são conhecidos. Um dos mais recentes foi a demonstração descoberta em 2002 por Roger Heath-Brown e Jan-Christoph Schlage-Puchta de que todo número par muito grande pode ser escrito como a soma de dois primos ímpares e exatamente 13 potências de 2.

Se você tentar descobrir duas potências de inteiros pequenos, que sejam consecutivas, vai logo dar de cara com 8 e 9, que são iguais a 2^3 e 3^2, respectivamente. Por mais que procure, não encontrará outros exemplos. Em vista disso, o matemático belga Eugène Charles Catalan propôs em 1844 que essas duas potências seriam as únicas soluções do problema (5). Isto é correto, como foi provado pelo matemático romeno Preda Mihăilescu em 2002.

Talvez você tenha percebido que, embora os enunciados das cinco questões acima sejam muito fáceis de entender, resolvê-las pode ser muito difícil: o Último Teorema de Fermat levou mais de 300 anos para ser provado e o problema proposto por Catalan levou 158 anos. Sem falar da conjectura de Goldbach e do problema relativo aos números de Fermat, que até hoje ninguém sabe resolver.

Capítulo 1

Números Inteiros

Neste capítulo estudaremos algumas propriedades básicas dos números inteiros que serão necessárias em nossa descrição do RSA no capítulo 6. Começaremos relembrando algumas definições bastante simples.

1.1 Fatores e Números Primos

Começamos revisando algumas noções básicas relativas à divisibilidade de inteiros.

1.1.1 Divisores e Múltiplos

Um inteiro b *divide* outro inteiro a se existe um terceiro número inteiro c tal que $a = bc$. Neste caso, também dizemos que b é um *divisor* ou *fator* de a, ou ainda que a é *múltiplo* de b. Todas estas

expressões significam a mesma coisa. Quando $1 < b < a$, dizemos que b é um fator ou divisor *próprio* de a. Naturalmente só há dois divisores que não são próprios, 1 e o próprio a. O número c, na definição acima é chamado de *cofator* de b em a. Por exemplo, 5 divide 20 porque $20 = 5 \cdot 4$. Neste exemplo 4 é o cofator de 5 em 20.

Na prática, determinamos que b divide a efetuando a divisão e verificando que o resto é zero. O cofator é o quociente da divisão. Nosso primeiro resultado é uma lista das propriedades dos múltiplos.

Dois inteiros quaisquer sempre têm pelo menos 1 como fator comum; afinal, um divide qualquer inteiro. Se 1 for o único fator comum a dois números, diremos *não têm fator próprio comum* ou que são *primos entre si*. Note que um par de primos distintos não têm fator próprio comum. Mas há muitos números compostos sem fator próprio comum, como é o caso de 6 e 35, por exemplo.

Propriedades dos Múltiplos. *Sejam a, b, c e d quatro números inteiros.*

1. *d divide 0;*
2. *se d divide a e b, então também divide $a + b$;*
3. *se d divide a então divide $a \cdot c$.*

Demonstração. Vamos provar que cada uma destas propriedades é verdadeira. A primeira é mais ou menos óbvia porque

$$0 = 0 \cdot d;$$

de modo que 0 é múltiplo de qualquer número. Para provar a segunda

propriedade, observemos que dizer que d divide a e b significa, pela definição, que existem inteiros a' e b' tais que

$$a = d \cdot a' \text{ e } b = d \cdot b';$$

isto é, estamos chamando de a' e de b' os cofatores de d em a e b, respectivamente. Mas, usando as expressões acima,

$$a + b = (d \cdot a') + (d \cdot b')$$

e pondo d em evidência

$$a + b = d(a' + b')$$

mostrando que d divide $a+b$, tendo $a'+b'$ como cofator. Finalmente, para mostrar (3), apenas multiplicamos $a = d \cdot a'$ por c, o que nos dá,

$$c \cdot a = c \cdot (d \cdot a') = d \cdot (c \cdot a');$$

de forma que d divide $c \cdot a$ com cofator igual a $c \cdot a'$. □

Estas *não* são as únicas propriedades dos múltiplos, embora sejam as mais importantes. Algumas outras propriedades são listadas no próximo exercício.

Exercício 3. *Sejam a, b e d números inteiros. Suponha que d divide a. Mostre que:*

(a) se d também divide b então d divide $a - b$;

(b) se d também divide $a + b$ então d divide b;

(c) se d também divide $a - b$ então d divide b;

(d) a e $a + 1$ não podem ter nenhum fator próprio comum.

O próximo exercício do Banco de Questões da OBMEP-2006 é uma consequência fácil destas propriedades.

Exercício 4. *Da igualdade* $9\,174\,532 \cdot 13 = 119\,268\,916$ *pode-se concluir que um dos números abaixo é divisível por 13. Qual é este número?*

(a) $119\,268\,903$ *(b)* $119\,268\,907$ *(c)* $119\,268\,911$
(d) $119\,268\,913$ *(e)* $119\,268\,923$

1.1.2 Primos e Compostos

Se vamos decompor inteiros em primos, é conveniente começarmos recordando a definição de número primo. Um número inteiro p é *primo* se $p \neq \pm 1$ e os únicos divisores de p são ± 1 e $\pm p$. Portanto 2, 3, 5 e -7 são primos, mas $45 = 5 \cdot 9$ não é primo. Um número inteiro, diferente de ± 1, que não é primo é chamado de *composto*. Logo 45 é composto.

Observe que a definição de primo exclui os números ± 1. Isto é, os números ± 1 *não são primos*; mas também não são compostos! Voltaremos a esta questão ao final do capítulo.

Exercício 5. *Seja $n > 1$ um inteiro. Lembre-se que $n!$ é definido como o produto de todos os números inteiros positivos menores ou iguais a n; isto é*

$$n! = 1 \cdot 2 \cdot \cdots \cdot (n-1) \cdot n.$$

Mostre que os números

$$n! + 2, n! + 3, \ldots, n! + (n - 1)$$

são todos compostos.

Finalmente, uma questão histórica (ou melhor dizendo, etimológica), você já se perguntou porque os números primos têm este nome? O nome é uma herança grega e, naturalmente, não se refere a nenhuma relação de parentesco. Os gregos classificavam os números em *primeiros ou indecomponíveis* e *secundários ou compostos*. Os números compostos são secundários por serem formados a partir dos primos. Os romanos apenas traduziram literalmente a palavra grega para primeiro, que em latim é *primus*. É daí que vêm nossos números primos.

1.2 Fatorando Inteiros

Nesta seção tratamos de maneira sistemática um problema que você já deve ter aprendido a resolver: como fatorar um inteiro; isto é, como encontrar todos os seus fatores primos. Começaremos descrevendo um problema mais simples: como calcular *um* fator (ou divisor) de um número.

1.2.1 Encontrando um Fator

O procedimento mais básico consiste em uma busca sistemática por um fator, começando de 2 e prosseguindo até chegar ao número

que se quer fatorar. Se nenhum fator for encontrado, podemos concluir que o número dado é primo. Por exemplo, se queremos fatorar 91, devemos verificar se é divisível

por 2? não, pois é ímpar;

por 3? como $9+1=10$ não é divisível por 3 então 91 também não é;

por 4? podemos pular 4 já que 91 é ímpar;

por 5? não, já que não acaba em 5 nem em 0;

por 6? outro par que podemos pular;

por 7? dividindo 91 por 7 achamos resto zero e quociente 13;

logo, 7 e 13 são fatores de 91. Note que houve bastante redundância neste processo. De fato, se 2 não divide 91, nenhum número par vai dividi-lo. Com isto poderíamos ter restringido as tentativas aos ímpares.

Exercício 6. *Generalize a afirmação feita no parágrafo acima, mostrando que, se um inteiro k divide outro inteiro m, que por sua vez divide ainda outro inteiro n, então k divide n.*

Vamos parar para pensar um minuto. Este exercício nos diz que o que fizemos para 2 se aplica também a outros números; 3, por exemplo. Então, se 3 não divide 91, nenhum múltiplo de 3 pode

dividi-lo. Isto significa que, tendo verificado que 3 não divide 91 poderíamos pular todos os seus múltiplos se o procedimento acima tivesse continuado. Apesar de parecer uma ideia esperta, essa maneira de proceder acaba sendo pouco útil porque introduz uma complicação extra no nosso método de achar um fator. Afinal, para aplicá-la, teríamos que ser capazes de detectar que um dado número é múltiplo de 3 para poder pulá-lo. Se isto já é complicado de fazer com 3, imagine se tentássemos com 7 ou 13. Apesar disto, veremos na seção 7.2 do capítulo 7 que a mesma ideia pode ser reciclada como um método para achar primos.

Nosso algoritmo para achar fatores tem algumas propriedades importantes que ainda precisamos analisar.

1.2.2 Algoritmo?

Como assim, algoritmo? Os matemáticos chamam de *algoritmo* qualquer método sistemático utilizado para fazer alguma coisa. Meio vago, não? Afinal, uma receita de bolo e um conjunto de instruções sobre como ir de uma cidade à outra são "métodos sistemáticos para fazer alguma coisa", ou não? Claro que são, e nada nos impede de chamá-los de algoritmos (embora talvez não seja uma boa ideia chamá-los assim em público...). Aliás uma receita é um bom lugar para começar, se queremos falar de algoritmos. Vejamos um exemplo.

Pão-de-ló

Ingredientes:

3 xícaras de farinha de trigo;

3 ovos;

3 colheres de sopa de açúcar.

Modo de fazer: Ponha o forno para esquentar, em temperatura média, por 10 minutos. Enquanto isto, separe a clara e a gema dos ovos. Bata as claras em neve. Acrescente as gemas e continue batendo até que a misture fique bem clara. Adicione o açúcar e continue batendo. Acrescente a farinha, uma colher de cada vez, misturando-a bem à massa com uma colher. Asse por mais ou menos vinte minutos.

Uma olhada rápida nesta receita nos mostra que vem em três partes: o título, os ingredientes e o procedimento a ser seguido. O título nos diz o que vai resultar se fizermos a receita; neste caso, um bolo, e não um biscoito ou um mingau. Os ingredientes indicam o que precisamos ter à mão para fazer o bolo. Já o procedimento descreve passo a passo o que devemos fazer para obter um bolo de verdade.

Todos os algoritmos, mesmo os de natureza matemática, têm uma estrutura semelhante à receita acima. Ao título da receita corresponde a *saída* do algoritmo; isto é, o que vai resultar se utilizarmos o algoritmo. Os ingredientes por sua vez, correspondem à entrada do algoritmo. No caso do algoritmo descrito na seção 1.2.1, a entrada é

o número do qual desejamos achar um fator. Finalmente, o procedimento da receita é... Bem, é o procedimento do algoritmo (é difícil dizer isto de outro jeito).

Podemos organizar nosso algoritmo segundo estas etapas. Como geralmente há muitos algoritmos com a mesma entrada e saída, é costume dar um nome ao algoritmo que se descreve. Isto é comum em receitas também, como quando escrevemos *Pão-de-Ló da Vovó* para distinguir uma receita de outra. Na verdade, os algoritmos são frequentemente nomeados em homenagem a quem os criou. Como nosso algoritmo é tão antigo que ninguém lembra quem o inventou, vamos chamá-lo de *Algoritmo acha-fator*.

Algoritmo acha-fator

Entrada: um inteiro positivo n;

Saída: um fator próprio de n ou a conclusão de que n é primo;

Procedimento: tente dividir n por 2. Se for divisível páre, pois descobrimos que 2 é fator de n, se não for, tente dividi-lo por 3. Se for divisível páre, pois descobrimos que 3 é fator de n, se não for, tente dividi-lo por 3. Continue desta maneira até encontrar um número que divida n ou até que o candidato a divisor seja n. Neste último caso, n é primo.

A única coisa que os matemáticos exigem de um algoritmo é que a execução do procedimento que ele descreve sempre chegue ao fim.

É fácil dar exemplos de procedimentos que não param nunca. Que tal este:

> comece com $k = 3$; verifique se k é divisível por 2: se for, páre; se não for, incremente k de 2 (isto é, passe para $k+2$) e tente dividir novamente por 3; continue repetindo isto enquanto um múltiplo de 2 não for encontrado.

Como nenhum número é, simultaneamente, par e ímpar, este procedimento vai se repetir para sempre, de modo que não é um algoritmo.

Observe que não resta a menor dúvida de que *acha-fator* satisfaz esta condição. Afinal de contas, estamos procurando por fatores positivos de um número n que, por serem fatores, têm que ser menores n. Mas, por maior que seja n, a quantidade de inteiros positivos menores que n tem que ser finita. Logo, na pior das hipóteses, visitamos cada um dos inteiros entre 2 e n sem achar fator e paramos porque encontramos n – que, neste caso, será primo.

1.2.3 Algoritmo e Al-Khowarazmi

A origem da palavra algoritmo é muito curiosa. Originalmente a palavra era escrita *algorismo*, que vem da palavra árabe Al-Khowarazmi, "o homem de Khowarazm". Esse era o nome pelo qual o matemático árabe Ibn Musa ficou conhecido. Ele, que viveu no século IX, escreveu um livro chamado *Al-jabr wa'l muqabalah* através do qual o sistema de numeração usado na Índia chegou à Europa Medieval. É por isso que, ainda hoje, falamos em algarismos indo-arábicos. Aliás *algorismo* e *algarismo* são variantes da mesma palavra e significavam, originalmente, os numerais indo-arábicos.

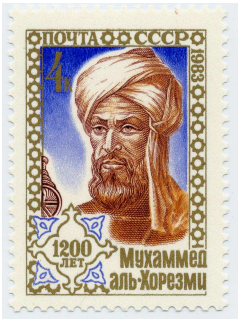


Figura 1.1: Al Khowarazmi

Com o passar do tempo, a palavra algorismo deixou de significar apenas os números e passou a ser usada também para descrever a aritmética e o cálculo com números. A maneira como algorismo ganhou um "t" não é menos curiosa. Outra palavra usada para número na Idade Média era *aritmos* – que é simplesmente número em grego. Alguém, em algum momento, confundiu-se na ortografia e misturou as duas, trocando o *s* de *algorismo* pelo *t* de *aritmos*. Como, naquela época, os livros eram copiados à mão, uns dos outros, o erro acabou se propagando.

O sentido atual da palavra algoritmo, contudo, é bem mais recente. Não é claro como a palavra passou a significar *método sistemático*, mas ela já estava sendo usada mais ou menos neste sentido em 1800. Assim, algoritmo é uma palavra muito antiga, mas que ganhou um significado novo.

Você reparou no nome do livro de Ibn Musa? "Al-jabr" não lhe lembra nada? É daí que vem a palavra *álgebra*. Hoje em dia dizemos que um *algebrista* é um matemático que trabalha em álgebra, mas

este não era, originalmente, o significado da palavra. No passado, um algebrista era um médico que consertava ossos.

Mas chega de conversa mole, voltemos à matemática.

1.2.4 O Algoritmo "acha-fator"

O algoritmo acha-fator trás um bônus grátis: o fator que ele encontra é, necessariamente, um número primo. Para entender o porquê, lembre-se que o algoritmo consiste em fazer uma busca pelo fator de um número n, começando sempre por 2, *que é o menor fator próprio positivo possível para qualquer número*. Por isso, o fator encontrado por este algoritmo é *sempre* o *menor* fator possível p do número n dado. Contudo, se p *não* for primo, então admite um fator $q < p$. Acontece que, segundo o exercício 6, como q divide p, que divide n, devemos ter que q divide n. Mas isto não é possível, uma vez que $q < p$ e já tínhamos concordado que p era o *menor* fator positivo possível de n.

Outro detalhe importante deste algoritmo é que podemos parar nossa busca, e decretar que n é primo, muito antes de chegar a n. A chave para entender isto é, mais uma vez, o fato do algoritmo achar sempre o *menor* fator do número n que se quer fatorar.

Para poder discutir os detalhes, suponhamos que o número inteiro positivo n, que se deseja fatorar, é composto. Neste caso o algoritmo *acha-fator* encontra o *menor* fator p de n. Portanto, podemos escrever

$$n = p \cdot c$$

onde c é o cofator de p como divisor de n. Contudo, c também é um

divisor de n. Levando em conta que p é o menor destes divisores, podemos escrever

$$c \geq p.$$

Combinando esta desigualdade com a equação anterior, obtemos

$$n = p \cdot c \geq p \cdot p.$$

Em outras palavras,

$$n \geq p^2 \quad \text{que é equivalente a} \quad p \leq \sqrt{n}.$$

Resumimos o resultado final em uma proposição para referência futura.

Proposição 1. *Se n for composto, o menor fator próprio de n é menor ou igual à raiz quadrada de n.*

Assim, se n for composto, algum fator deverá ser encontrado antes de nossa busca ultrapassar $\sqrt{n}$. Isto nos permite reformular o algoritmo acha-fator de maneira bem mais eficiente, como segue.

Algoritmo acha-fator

Entrada: um inteiro positivo n;

Saída: um fator próprio de n ou a conclusão de que n é primo;

Procedimento: tente dividir n por 2. Se for divisível páre, pois descobrimos que 2 é fator de n, se não for, tente dividi-lo por 3. Se for divisível páre, pois descobrimos que 3 é fator de n, se não for, tente dividi-lo por 5. Continue desta maneira até encontrar um número que divida n ou até que o candidato a divisor seja maior que $\sqrt{n}$. Neste último caso, n é primo.

Naturalmente, a única diferença entre esta versão e a anterior é que paramos assim que o divisor a ser experimentado ultrapassa a raiz quadrada de n. Com isto, buscamos o divisor entre uma quantidade muito menor de inteiros do que vínhamos fazendo anteriormente.

Finalmente, convém resumir tudo o que aprendemos nesta subseção como uma proposição.

Proposição 2. *O fator de um número inteiro $n > 1$ encontrado pelo algoritmo* acha-fator *acima é sempre um número primo menor ou igual que a raiz quadrada de n.*

Encerraremos este tópico com dois exercícios.

Exercício 7. *Seja n um número inteiro positivo composto e p seu menor fator primo. Sabe-se que:*

1. $p \geq \sqrt{n}$;
2. $p - 4$ *divide* $6n + 7$ *e* $3n + 2$.

Determine todos os possíveis valores de n.

Desafio 1. *Qual o maior número possível de fatores primos de um inteiro n que não tem nenhum fator $\leq n^{1/3}$?*

1.2.5 Custo da Fatoração

Apesar de ser fácil de entender e de utilizar, o algoritmo acha-fator é muito ineficiente, mesmo se usarmos um computador. Isto é facilmente ilustrado se estimarmos o tempo que um computador levaria para achar um fator de um número grande usando este algoritmo.

Lembre-se que, tendo n por entrada, acha-fator executa no máximo $\sqrt{n}$ tentativas de divisão antes de encontrar um fator para n. Na verdade, o pior caso possível ocorre quando precisamos efetuar exatamente $\sqrt{n}$ tentativas de divisão, o que corresponde a dizer que n é primo. É precisamente este o caso cujo tempo de execução vamos estimar.

Para fixar as ideias, consideremos um número *primo* p, de 100 ou mais algarismos. Isto é $p \geq 10^{100}$ e, portanto, $\sqrt{p} \geq 10^{50}$. Assim, precisaremos executar pelo menos 10^{50} divisões para garantir que p é primo pelo algoritmo acha-fator. Para transformar isto em tempo de cálculo, precisamos ter uma ideia de quantas divisões um computador é capaz de efetuar em um segundo. Vamos exagerar e supor que usamos um supercomputador capaz de executar 10^{10} divisões por segundo. Para você ter uma ideia de quão exagerado isto é, o computador no qual estou escrevendo esta apostila não faz mais do que 50 divisões por segundo!

Seja como for, usando nosso suposto supercomputador, precisaríamos de, pelo menos,

$$\frac{10^{50}}{10^{10}} = 10^{40} \text{ segundos}$$

para determinar que n é primo usando acha-fator. Como um ano tem

$$60 \cdot 60 \cdot 24 \cdot 365 = 31\,536\,000 \text{ segundos,}$$

concluímos que 10^{40} segundos corresponde a

$$\frac{10^{40}}{31\,536\,000}$$

que é aproximadamente igual a

$$317\,000\,000\,000\,000\,000\,000\,000\,000\,000 \qquad \text{(são 30 zeros)}$$

anos que é muito mais tempo do que conseguimos imaginar. Afinal de contas, as últimas estimativas da idade do universo indicam que não deve ultrapassar 20 bilhões de anos; ou seja

$$200\,000\,000\,000 \qquad \text{(meros 11 zeros)}$$

anos. Podemos, portanto, concluir, sem qualquer receio, que é impossível confirmar que um número de 100 ou mais algarismos é primo usando este algoritmo.

Isto significa que o algoritmo é inútil? Certamente que não. Se vamos fatorar um inteiro sobre o qual nada sabemos, há sempre a possibilidade que tenha um fator primo pequeno, digamos menor que um milhão. Neste caso, o acha-fator encontrará um tal fator rapidamente.

1.2.6 Fatorando Números Inteiros

Até aqui vimos apenas como encontrar um fator próprio de um número inteiro n, se existir tal fator, ou comprovar que o número é primo. Entretanto, nosso objetivo inicial era bem mais ousado: queríamos escrever n como produto de potências de números primos. Mas, de posse do algoritmo acha-fator, isto é fácil de fazer, basta aplicar acha-fator várias vezes. Vejamos um exemplo.

Considere o inteiro 12 103. Aplicando o algoritmo acha-fator a este número (deixo as contas para você fazer) achamos o fator 7. Como

$$\frac{12\,103}{7} = 1\,729,$$

temos que

$$12\,103 = 7 \cdot 1\,729.$$

Como os fatores encontrados por acha-fator são sempre primos, sabemos que 7 é primo. Portanto, só é necessário aplicar acha-fator novamente ao cofator 1 729 de 7 em 12 103.

Aplicando acha-fator a 1 729, descobrimos que 7 também é fator deste número. Mas,

$$\frac{1\,729}{7} = 247,$$

de modo que

$$12\,103 = 7 \cdot 1\,729 = 7 \cdot (7 \cdot 247) = 7^2 \cdot 247.$$

Novamente, resta-nos aplicar acha-fator ao cofator 247. Desta vez,

o fator encontrado é 13 e

$$\frac{247}{13} = 19,$$

de modo que

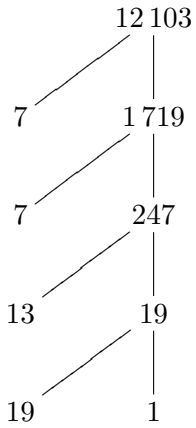
$$12\,103 = 7^2 \cdot 247 = 7^2 \cdot (13 \cdot 19).$$

Contudo, $\sqrt{19} = 4,35...$ e é fácil verificar que 19 não é divisível por 2, nem 3. Isto nos permite concluir, pela proposição 2 que 19 é primo.

Reunindo tudo isto concluímos que a fatoração de 12 103 em potências de primos é

$$12\,103 = 7^2 \cdot 13 \cdot 19.$$

Uma maneira bastante ilustrativa de organizar os cálculos que fizemos acima é dispô-los ao longo de ramos, da seguinte forma:



Quando este algoritmo é efetuado no papel, é costume organizá-lo da seguinte maneira:

12 103	2	... não divisível
12 103	3	... não divisível
12 103	5	... não divisível
12 103	7	... divisível
1 729	7	... divisível
247	9	... não divisível
247	11	... não divisível
247	13	... divisível
19	13	... não divisível
19	15	... não divisível
19	17	... não divisível
19	19	... divisível

A primeira coisa a observar é que, desta maneira, executamos o algoritmo acha-fator algumas vezes sucessivamente de maneira sistemática; sempre sobre o cofator do primo achado na rodada anterior. A segunda coisa tem a ver com a passagem da quarta para a quinta linha. Na quarta linha achamos 7 como fator de 12 103; o cofator encontrado foi 1 729. A partir da quinta linha deveríamos aplicar acha-fator a 1 729 mas, estranhamente, começamos de 7 e não de 2: por quê? A explicação está no próximo exercício.

Exercício 8. *Seja n um inteiro positivo e p o fator encontrado pelo algoritmo acha-fator. Se c é o cofator de p como divisor de n, mostre que o menor fator que c pode ter é p.*

Podemos formular tudo o que fizemos até agora da seguinte maneira:

Teorema da Fatoração. *Dado um inteiro positivo $n \geq 2$ podemos sempre escrevê-lo na forma*

$$n = p_1^{e_1} \dots p_k^{e_k},$$

onde $1 < p_1 < p_2 < p_3 < \cdots < p_k$ são números primos e $e_1, \dots, e_k$ são inteiros positivos.

Os expoentes $e_1, \dots, e_k$ na fatoração acima são chamados de *multiplicidades*. Assim, a multiplicidade de p_1 na fatoração de n é e_1. Observe que n tem k fatores primos *distintos*, mas que a quantidade total de fatores primos (distintos ou não) é a soma da multiplicidades $e_1 + \cdots + e_k$. Por exemplo, na fatoração

$$12\,103 = 7^2 \cdot 13 \cdot 19;$$

o primo 7 tem multiplicidade 2, ao passo que 13 e 19 têm multiplicidade 1 cada.

Figura 1.2: C. F. Gauss

O primeiro a enunciar o resultado acima foi C.F. Gauss no §16 de seu famoso livro *Disquisitiones arithmeticæ*. Isto não significa que este fato não houvesse sido usado *implicitamente* por matemáticos desde a Grécia Antiga. Afinal Euclides já havia provado na Proposição 31 do Livro VII de seus *Elementos* que

todo número composto é divisível por algum primo.

1.2.7 O Teorema da Fatoração Única

Para ser honesto, há mais sobre a fatoração de inteiros do que o enunciado acima leva a crer. De fato cada inteiro maior que 1 admite apenas uma fatoração, desde que, como no enunciado acima, ordenemos os primos em ordem crescente e agrupemos primos iguais em uma única potência. Isto pode parecer óbvio – afinal, quem já viu acontecer de duas pessoas obterem fatorações diferentes de um mesmo número? – mas não é. Discutiremos esta questão com mais detalhes na seção seguinte. O enunciado final do teorema da fatoração, incluindo sua unicidade, é dado a seguir.

Teorema da Fatoração Única. *Dado um inteiro positivo $n \geq 2$ podemos escrevê-lo, de modo único, na forma*

$$n = p_1^{e_1} \dots p_k^{e_k},$$

onde $1 < p_1 < p_2 < p_3 < \cdots < p_k$ são números primos ao passo que $e_1, \dots, e_k$ são inteiros positivos.

Tendo o enunciado preciso deste teorema, podemos explicar porque é necessário excluir ± 1 da definição de número primo. A verdade é

que, se não fizéssemos isto não poderíamos falar da unicidade da fatoração no teorema acima. Por exemplo, se 1 fosse primo, então 2 e $1^2 \cdot 2$ seriam duas fatorações *distintas* do número 2. Usando a mesma ideia de multiplicar o número por uma potência de 1 (ou de -1) teríamos uma infinidade de fatorações distintas para cada inteiro. Para excluir este tipo de fatoração trivial, dizemos que ± 1 não são primos.

Não provaremos a unicidade da fatoração nesta apostila, mas os detalhes podem ser encontrados nas referências [2, capítulo 2], [1] ou [3]. Para que você possa apreciar a importância da unicidade na fatoração, aqui estão dois exercícios que seriam muito difíceis de fazer, não fosse por ela (especialmente o 10). Ao fazer os exercícios procure identificar exatamente onde está utilizando a unicidade da fatoração.

Exercício 9. *Determine se existem inteiros positivos x, y e z que satisfaçam a equação $30^x \cdot 35^y = 21^x \cdot 140 \cdot 5^{2x}$.*

Exercício 10. *Determine se existem inteiros positivos x, y e z que satisfaçam a equação $2^x \cdot 3^4 \cdot 26^y = 39^z$.*

Exercício 11. *Seja n um inteiro positivo e $p > 1$ um número primo que divide n. Mostre que a multiplicidade de p na fatoração de n é o* maior *expoente e tal que p^e divide n.*

O próximo exercício apareceu originalmente no Banco de Questões da OBMEP-2007 (p. 99).

Exercício 12. *Quais números naturais m e n satisfazem a $2^n + 1 = m^2$?*

Capítulo 2

Aritmética Modular

Neste capítulo estudaremos a aritmética dos fenômenos periódicos; isto é, aqueles que se repetem a intervalos regulares. No dia-a-dia nos deparamos constantemente com fenômenos deste tipo: o dia que tem 24 horas, a semana que tem 7 dias, o ano que tem 365 dias, a OBMEP ocorre uma vez a cada ano e o Colóquio Brasileiro de Matemática uma vez a cada dois anos, só para citar alguns.

2.1 Fenômenos Periódicos e Aritmética

Naturalmente, o que caracteriza os fenômenos periódicos é o fato de se repetirem com regularidade. O tempo que decorre entre uma ocorrência e outra destes fenômenos é chamado de *período* do fenômeno. Assim, a Terra leva 24 horas. para dar uma volta em torno de si mesma, de forma que seu período de rotação é de 24 horas. Já o período de revolução da Terra é de 365 dias e um quarto, e corres-

ponde ao menor tempo que leva para dar uma volta em torno do Sol. A Lua, por sua vez, tem período de rotação de 27 dias e período de revolução (em torno da Terra) de 27 dias.

Antes que você ache que encontrou um erro tipográfico ("Ele estava distraído e repetiu o mesmo número do período de translação!") deixa eu esclarecer que não se trata disto. Na verdade, os períodos de revolução da Lua em torno da Terra e de sua rotação em torno de seu próprio eixo são exatamente os mesmos, e é por isso que a Lua sempre tem a mesma face voltada para a Terra. Se você está pensando "mas que incrível coincidência!", então prepare-se para um desapontamento. A verdade é que esta coincidência de períodos foi causada por um efeito de fricção relacionado às marés que a Lua provoca na Terra. Fascinante, não?

2.1.1 Horários Escolares

Quando um fenômeno é quase que perfeitamente periódico, tudo se passa como se a "história" do fenômeno se repetisse cada vez que o período se completa. Em outras palavras, se conhecemos quanto vale o período de um tal fenômeno, tudo que precisamos saber a seu respeito pode ser resumido em uma descrição do que ocorre ao longo da passagem de um período.

Vivemos isto todo dia, por exemplo, nos horários de aula de uma escola. Embora seja necessário descrever os horários de aula de cada matéria ao longo de todo o ano, simplificamos esta tarefa utilizando o fato destes horários se repetirem a cada sete dias. Assim, descrevendo a distribuição de aulas ao longo de uma semana, podemos estendê-la

para todo o ano letivo, simplesmente repetindo o mesmo horário a cada semana.

Por exemplo, imagine que sua mãe lhe pergunta se você terá aula de matemática no dia 23 de setembro. Para responder esta pergunta basta você descobrir em que dia da semana cai 23 de setembro e olhar o seu horário. Como hoje é segunda-feira 10 de setembro e como $23 - 10 = 13$, o dia 23 está a 13 dias desta segunda. Por outro lado, $13 = 7 + 6$. Só que, passado sete dias, estaremos de volta a uma segunda-feira e, a seis dias desta segunda temos um domingo; portanto, a resposta é que não há aula de matemática neste dia – qualquer que seja o seu horário escolar.

Antes de encerrar este exemplo, façamos uma análise matemática mais detalhada do procedimento usado para resolver o problema do parágrafo anterior. Em primeiro lugar, precisamos conhecer a periodicidade do horário, que é de 7 dias, e quanto tempo vai passar entre hoje e o dia no qual queremos saber se vai ou não haver aula de matemática. Se d dias vão se passar, dividimos d por 7 e tomamos nota do quociente q e do resto r desta divisão. Mas, a cada sete dias caímos no mesmo dia da semana que hoje. Portanto, daqui a $d - r = 7 \cdot q$ dias terão passado exatamente q semanas e estaremos de volta a uma segunda-feira, como é o dia de hoje. O dia da semana daqui a d dias pode então ser determinado a partir do resto r conforme mostra a tabela 2.1.

Resto	0	1	2	3	4	5	6
Dia	segunda	terça	quarta	quinta	sexta	sábado	domingo

Tabela 2.1: Dias da semana

A observação crucial é que, do ponto de vista deste problema,

> quaisquer dois dias que diferem por um intervalo de sete dias, representam o mesmo dia da semana.

Uma vez que isto tenha sido observado, o problema se reduz a determinar o resto da divisão de um dado número pelo período do problema, que neste caso é 7.

2.1.2 Um Jogo de Tabuleiro

Embora seja natural começar pensando no período como o intervalo de *tempo* entre duas ocorrências de um dado fenômeno, esta não é sua única aplicação. Para um exemplo que não envolve tempo, considere um jogo de dados cujo tabuleiro é formado por um caminho quadrado na forma ilustrada na tabela 2.2.

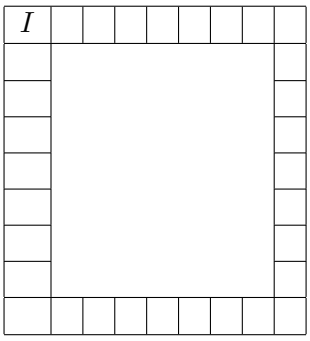


Tabela 2.2: A tabela do jogo

No início do jogo, todos os jogadores devem pôr suas peças na casa inicial marcada com o I. Para sair desta casa, cada jogador deve

atirar o dado duas vezes consecutivas. Se tirar q da primeira vez e r na segunda, deve andar $6q + r$ casas no sentido dos ponteiros do relógio. É claro que tanto r como q só podem ser números entre 1 e 6, já que foram tirados no dado. Por exemplo, se tirei 3 na primeira jogada do dado e 2 na segunda, devo andar

$$6 \cdot 3 + 2 = 20 \quad \text{casas no tabuleiro.}$$

Os jogadores continuam atirando os dados desta maneira e avançando ao longo do tabuleiro. Quem chegar primeiro à casa final, marcada com I, ganha o jogo.

Digamos que, depois de um certo número de jogadas, você se encontra na casa do tabuleiro marcada com • na tabela 2.3.

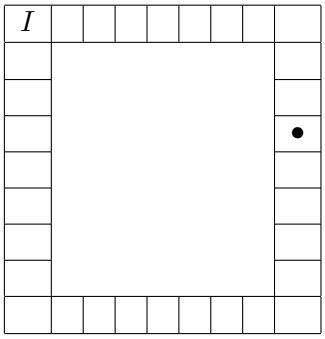


Tabela 2.3: Quanto ganhar para encerrar o jogo?

A pergunta é:

> Quanto você tem que tirar em cada uma das jogadas do dado para ganhar o jogo nesta rodada?

Uma simples contagem mostra que há 21 casas entre a posição que

você está neste momento e a casa inicial. Mas 21 pode ser escrito na forma

$$21 = 6 \cdot 3 + 3,$$

de modo que, para ganhar nesta rodada preciso tirar 3 nas duas jogadas do dado. Note que, mais uma vez, o cálculo matemático requerido para resolver o problema foi uma divisão.

Exercício 13. *Quanto você deve tirar nas duas jogadas do dado para ganhar em uma jogada a partir da posição marcada pelo • no tabuleiro 2.4?*

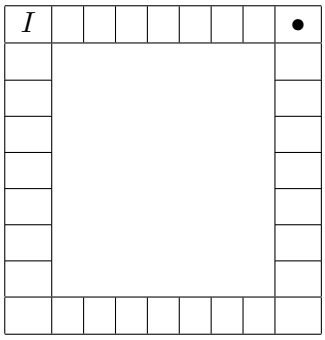


Tabela 2.4: Tabela do Exercício 13

Uma pergunta interessante está formulada no próximo problema.

Exercício 14. *Será que é possível ganhar o jogo já na primeira rodada? Quanto alguém teria que tirar em cada uma dos lances de dados para que isto acontecesse?*

Uma coisa ruim deste jogo é que ele pode nunca terminar.

Exercício 15. *Dê exemplo de uma sucessão infinita de jogadas que faz com que o jogo nunca acabe para um determinado jogador.*

2.1.3 Prova dos Nove

Outra situação em que o período não corresponde a uma variação de tempo ocorre na *prova dos nove* que aprendemos a fazer no ensino fundamental. Por exemplo, são dados dois números que queremos somar; digamos que são 175 e 234. Efetuamos o resultado e obtemos

$$\begin{array}{rr} & 175 \\ + & 234 \\ \hline & 409 \end{array}.$$

Para conferir se fizemos a conta corretamente, somamos os algarismos das duas parcelas, subtraindo nove cada vez que a soma chegue, ou passe, de nove – ou, como é costume dizer, fazendo "noves fora". Aplicando a prova dos nove ao exemplo acima somamos $1 + 7 + 5$ que dá 13, noves fora 4 (isto é, $13 - 9 = 4$). Continuando, somamos os algarismos da segunda parcela: $4 + 2 + 3 = 9$, noves fora zero, de modo que as parcelas dão como resultado $4+0 = 4$. Se a conta estiver correta, devemos obter 4 ao aplicar o mesmo processo ao resultado que calculamos. Mas, 13 noves fora dá 4, que era o valor esperado. Isto indica (mas não garante!) que a conta esteja certa.

Observe que, ao fazer "noves fora", estamos calculando o resto da divisão de um número por 9. Na prática, a prova dos nove consiste em calcular o resto de divisão de uma soma por 9 de duas maneiras diferentes, como veremos na página 66.

Exercício 16. *Dê exemplo onde a prova dos nove falha. Explique o que precisa acontecer para que a prova dos nove não seja capaz de detectar um erro cometido em uma adição.*

Exercício 17. *A prova dos nove também funciona para a multiplicação. Dê exemplo de uma multiplicação errada que a prova dos nove não detecta como tal. Explique o que precisa acontecer para que a prova dos nove não seja capaz de detectar um erro cometido em uma multiplicação.*

2.1.4 Restos de Inteiros

Nos exemplos anteriores, resolvemos os problemas propostos usando divisão de inteiros com resto. Isto sugere que o próprio resto da divisão se comporta de maneira periódica. Por exemplo, os múltiplos de 2 se repetem de dois em dois e, portanto, com período igual a 2. Já os múltiplos de 3 têm período 3 e os de 12, período 12. Mais precisamente,

> os restos dos inteiros sucessivos na divisão por um inteiro positivo qualquer n repetem-se com período n.

Por exemplo, dividindo os números de 0 em diante por 4, obtemos os restos como na tabela 2.5.

Inteiros	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Restos	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2

Tabela 2.5: Alguns restos módulo 4

Em geral, dividindo um inteiro positivo a por outro inteiro positivo n, obtemos

$$a = nq + r \quad \text{e} \quad 0 \leq r < n.$$

Por isto, o mesmo resto na divisão por n se repete a cada n inteiros sucessivos, como vimos, experimentalmente, na tabela 2.5 para o caso $n = 4$.

Em vista disto, podemos dizer que os restos da divisão por n se repetem com período exatamente igual a n. Note que se trata aqui de uma extensão da utilização usual da palavra período que, neste contexto, não se refere a um intervalo de tempo. Para evitar confusão chamaremos estes "períodos generalizados" de *módulos*.

2.2 Definições e Primeiras Propriedades

É hora de sistematizar os cálculos efetuados nos vários exemplos da seção anterior e de considerar algumas aplicações elementares.

2.2.1 Sistematizando

Para começar, temos um inteiro positivo n que representa o *período* ou *módulo* do fenômeno que estamos estudando. Dias, anos, horas e casas na tabela são todos dados por números inteiros e é este o único caso que vamos considerar. Isto é, não vamos tratar de períodos como $365\frac{1}{4}$ que é o número exato de dias que formam um ano. Aliás, é por isso que a cada quatro anos temos um ano *bissexto*, que é aquele no qual fevereiro tem 29 dias.

Analisando cada um dos três exemplos vistos na seção anterior, verificamos que:

no calendário a cada sete dias estamos no mesmo dia da semana.

no jogo a cada 32 movimentos de uma peça, chegamos à mesma casa do tabuleiro;

na prova dos nove cada vez que a soma dá maior ou igual a 9, retemos apenas sua diferença por 9;

nos restos a cada n inteiros obtemos um número que deixa o mesmo resto na divisão por n.

Lembrando que o módulo é, no primeiro caso 7, no segundo 38, no terceiro 9 e no quarto n, vamos fazer a seguinte definição:

> se n é o módulo e a e b são números inteiros, então diremos que a é *congruente* a b *módulo* n se $a - b$ é um múltiplo de n.

Assim:

- o número de dias que se passaram, desde primeiro de janeiro, entre dois sábados de um mesmo ano são congruentes módulo 7;
- o número de movimentos de uma peça, desde o começo do jogo, ao final de duas jogadas diferentes que levam a peça a uma mesma casa do tabuleiro são congruentes módulo 32;
- dois números que são iguais *noves fora*, diferem por um múltiplo de 9;
- dois inteiros com o mesmo resto na divisão por n são congruentes módulo n.

Se dois inteiros a e b são congruentes módulo n, escrevemos

$$a \equiv b \pmod{n};$$

se não são congruentes, escrevemos

$$a \not\equiv b \pmod{n}.$$

Assim,

$$3 \equiv 8 \pmod{5}, \text{ ao passo que } 3 \not\equiv 8 \pmod{7}.$$

Por outro lado,

$$3 \equiv -25 \pmod{7}, \text{ embora } 3 \not\equiv -25 \pmod{5}.$$

2.2.2 Propriedades da Congruência Modular

A congruência modular satisfaz algumas propriedades que a tornam muito semelhante à igualdade usual. As propriedades mais elementares da igualdade são as seguintes:

reflexiva todo número é igual a si próprio;

simétrica se $a = b$ então $b = a$;

transitiva se $a = b$ e $b = c$, então $a = c$.

Na verdade, costumamos usar estas propriedades da igualdade sem ter sequer consciência que o fazemos.

No caso da congruência modular não é assim tão óbvio que estas propriedades são satisfeitas, mas podemos verificá-las sem muito trabalho como faremos adiante. Antes porém, convém perguntarmos para que fazer o esforço de provar que estas propriedades valem para a congruência modular. Será mera curiosidade? A resposta, naturalmente, é que não se trata apenas de curiosidade: precisamos dessas propriedades para poder utilizar de forma correta a congruência modular nas contas que faremos nas próximas seções, incluindo-se a codificação de uma mensagem pelo RSA. É para isto que vamos provar que a congruência modular satisfaz propriedades análogas às enunciadas acima para a igualdade; mais precisamente:

reflexiva todo número é congruente módulo n a si próprio;

simétrica se $a \equiv b \pmod{n}$ então $b \equiv a \pmod{n}$;

transitiva se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$
então $a \equiv c \pmod{n}$;

onde n é um inteiro positivo.

Para mostrar que a congruência módulo n é reflexiva, devemos verificar que

$$a \equiv a \pmod{n}.$$

Mas, pela definição, isto é o mesmo que dizer que $a - a = 0$ é múltiplo de n. Contudo, zero é múltiplo de qualquer inteiro n, uma vez que $0 \cdot n = 0$.

Passemos à simétrica. Pela definição de congruência módulo n, $a \equiv b \pmod{n}$ é o mesmo que dizer que $a - b$ é múltiplo de n. Em

outras palavras, se $a \equiv b \pmod{n}$ então existe algum inteiro k tal que

$$a - b = k \cdot n.$$

Multiplicando esta equação por -1, obtemos

$$b - a = (-k) \cdot n;$$

isto é, $b - a$ é múltiplo de n, ou ainda, $b \equiv a \pmod{n}$.

Para a transitiva, tomamos por hipótese que

$$a \equiv b \pmod{n} \quad \text{e que} \quad b \equiv c \pmod{n}.$$

Mas estas duas congruências se traduzem, por definição, nas igualdades

$$a - b = k \cdot n \quad \text{e} \quad b - c = \ell \cdot n,$$

onde k e ℓ são inteiros escolhidos de maneira adequada. Somando estas duas últimas equações,

$$(a - b) + (b - c) = k \cdot n + \ell \cdot n.$$

Cancelando o b à esquerda e usando a distributividade da direita, obtemos

$$a - c = (k + \ell) \cdot n,$$

que é equivalente à congruência $a \equiv c \pmod{n}$, como requerido pela propriedade transitiva.

2.2.3 Resíduos

Antes de prosseguir, precisamos estudar em mais detalhes a relação entre a congruência módulo n e a divisibilidade de inteiros, já que é isto que torna a congruência tão útil. Para começar, observe que a propriedade reflexiva da congruência módulo n é equivalente à afirmação de que zero é divisível por n. Por sua vez, propriedade simétrica equivale a dizer que se um dado número é divisível por n então, ao multiplicá-lo por -1, obtemos outro múltiplo de n. Finalmente, a transitiva nos diz apenas que a soma de múltiplos de n também é um múltiplo de n. Em outras palavras, as três propriedades que provamos correspondem às propriedades dos múltiplos listadas na proposição em 1.1.1.

Mas podemos ir bem mais longe que isto. Digamos que a é um inteiro positivo. Dividindo a por n temos

$$a = n \cdot q + r \quad \text{e} \quad 0 \leq r < n.$$

Assim,

$$a - r = n \cdot q;$$

que equivale a dizer que

$$a \equiv r \pmod{n}.$$

Verificamos com isto que todo inteiro *positivo* é congruente módulo n ao resto de sua divisão por n, que é um número entre 0 e n.

Em geral, se $a \equiv r \pmod{n}$ e $0 \leq r < n$, dizemos que r é o *resíduo* de a módulo n. Note que usamos o artigo definido ao definir

resíduo: *o resíduo* e não *um resíduo*. Isto porque cada número só pode ter um resíduo módulo n. De fato, se

$$a \equiv r \pmod{n} \text{ com } 0 \leq r \leq n-1;$$
$$a \equiv r' \pmod{n} \text{ com } 0 \leq r' \leq n-1;$$

então, pelas propriedades simétrica e transitiva, temos que $r \equiv r' \pmod{n}$. Digamos que $r \geq r'$. Pela definição da congruência, isto significa que $r - r'$ é um múltiplo de n. Mas tanto r, quanto r' são menores que n, de modo que $0 \leq r - r' < n$. Isto significa que $r - r'$ só pode ser múltiplo de n se o cofator correspondente for zero; o que nos dá $r = r'$, mostrando que os dois resíduos, r e r' têm que ser iguais.

Aparentemente a única coisa que fizemos ao introduzir os resíduos foi inventar um nome novo para o resto, mas não é bem assim. Note que o termo resíduo se aplica a qualquer inteiro, positivo ou negativo, ao passo que o resto geralmente é usado quando dividimos um inteiro positivo por n. O que ocorre, então, se a for negativo?

Para tornar o argumento mais claro, convém começar com um exemplo. Seja $n = 6$ e $a = -55$. Nosso objetivo é calcular o resíduo de -55 módulo 6; em outras palavras, queremos achar um inteiro $0 \leq r < 6$ tal que $-55 \equiv r \pmod{6}$. Poderíamos proceder por tentativa, mas vamos tratar o problema de maneira mais sistemática para podermos lidar mesmo com o caso em que o n for grande. Para isto, dividimos 55 por 6, obtendo quociente 9 e resto 1:

$$55 = 9 \cdot 6 + 1.$$

Multiplicando tudo por -1,

$$-55 = (-9) \cdot 6 - 1,$$

de forma que

$$-55 \equiv -1 \pmod{6}.$$

Observe que -1 não é o resíduo de -55 módulo 6 porque -1 é negativo. Contudo, como $6 = 5 - (-1)$, obtemos

$$-1 \equiv 5 \pmod{6};$$

e a propriedade transitiva da congruência nos permite concluir que

$$-55 \equiv 5 \pmod{6}.$$

Portanto, -55 tem resíduo 5 módulo 6.

Para tratar o caso geral, podemos seguir as etapas do exemplo acima. Primeiramente, como estamos supondo que a é negativo, então $-a$ deve ser positivo. Dividindo-o por n,

$$-a = n \cdot q + r \quad \text{e} \quad 0 \leq r < n,$$

onde q e r são o quociente e o resto da divisão. Multiplicando esta equação por -1, obtemos

$$a = n \cdot (-q) - r \quad \text{e} \quad 0 \leq r < n;$$

isto é

$$a \equiv -r \pmod{n} \quad \text{e} \quad 0 \leq r < n.$$

Se $r = 0$, então $a \equiv 0 \pmod{n}$ e já achamos o resíduo. Se $r \neq 0$, então $(n - r) - (-r) = n$ nos diz que

$$-r \equiv n - r \pmod{n},$$

de modo que a transitividade da congruência nos permite concluir que

$$a \equiv n - r \pmod{n}.$$

Ainda precisamos nos certificar que $n-r$ é um resíduo mas, para isto, basta verificar que está entre 0 e $n - 1$. Como $r \geq 0$ e $r \neq 0$, temos que $r > 0$. Logo $n - r < n$. Entretanto, $r < n$, donde concluímos que $n - r > 0$.

Para poder descrever o que fizemos de maneira sucinta, definimos

$$|a| = \begin{cases} a & \text{se} \quad a \geq 0; \\ -a & \text{se} \quad a < 0; \end{cases}$$

que é chamado de *módulo* de a. Por exemplo,

$$|4| = 4 \quad \text{ao passo que} \quad |-5| = 5.$$

Proposição 3. *Sejam a e $n > 1$ números inteiros e r o resto da divisão de $|a|$ por n, então o resíduo de a módulo n é igual a:*

- 0 *se* $r = 0$*;*
- r *se* $r \neq 0$ *e* $a \geq 0$*;*
- $n - r$ *se* $r \neq 0$ *e* $a < 0$.

Vejamos um exemplo:

> Quais são os resíduos possíveis módulo 6 que um primo $p > 3$ pode ter?

Para começar, os possíveis resíduos módulo 6 são 0, 1, 2, 3, 4 ou 5. Como p é primo, então 0 certamente não é um resíduo possível. Já 1 é possível, afinal 7 é primo e tem resíduo 1 módulo 6. Quanto a 2,

$$p \equiv 2 \pmod 6$$

implica que $p - 2$ é par. Mas isto só é possível se p for par e todo par maior que 2 é composto. Um argumento semelhante mostra que 4 também não pode ser resíduo de um tal primo. Por outro lado,

$$p \equiv 3 \pmod 6$$

equivale a

$$p = 6 \cdot k + 3 \quad \text{para algum inteiro} \quad k \geq 0.$$

Disto segue que

$$p = 3 \cdot (2 \cdot k + 1),$$

que também não é admissível, porque p é primo e é maior que 3. Finalmente, 5 é um resíduo possível; afinal, o próprio 5 é primo. Vamos resumir este resultado para referência futura.

Proposição 4. *Se $p > 3$ é primo, então p só pode ter resíduos iguais a 1 ou a 5 módulo 6.*

Há uma outra maneira de dizer que a deixa resíduo r módulo n que, apesar de às vezes produzir alguma confusão, é usual e muito conveniente. Como $a \equiv r \pmod{n}$ significa que, para algum inteiro k,

$$a = k \cdot n + r,$$

dizemos simplesmente que *a é da forma $kn + r$*. Usando esta terminologia, o enunciado da proposição 4 passaria a ser

todo primo $p > 3$ é da forma $6k + 1$ ou da forma $6k + 5$.

O próximo exercício está enunciado usando esta terminologia.

Exercício 18. *Mostre que todo primo ímpar é da forma $4k+1$ ou da forma $4k + 3$. Dê exemplos de números da forma $4k + 1$ e da forma $4k + 3$ que não são primos.*

O desafio abaixo é uma generalização da proposição 4. Antes de abordá-lo talvez você queira rever o exercício 5, ao qual está relacionado.

Desafio 2. *Seja $n > 3$ um inteiro e $p > n$ um número primo. Quais os resíduos possíveis para $n!$ módulo p?*

2.2.4 Adição, Multiplicação e Congruência

Antes de poder apreciar completamente o poder de fogo da congruência módulo n, precisamos estabelecer a relação entre a congruência e as operações usuais de adição e multiplicação de inteiros.

Há dois fatos importantes que sabemos sobre a congruência módulo n. O primeiro, discutido no artigo anterior, nos diz que a con-

gruência funciona de maneira muito semelhante à igualdade de inteiros. O segundo é consequência da própria definição e nos diz que *números inteiros diferentes podem ser congruentes módulo n*. Para usar uma imagem concreta, a congruência módulo n funciona como uma espécie de filtro: quando olhamos os inteiros através dela, há muitos inteiros que não conseguimos mais distinguir de outros. Não é exatamente isto que acontece quando olhamos através de um filtro colorido? Por exemplo, se olhamos para várias bolas coloridas iguais, exceto pela cor, através de um filtro vermelho, veremos as bolas brancas e vermelhas como se fossem da mesma cor (neste caso, vermelho); e as bolas azuis e pretas como se fossem da mesma cor (neste caso, preto). Da mesma forma, 31, 1 e 51 são diferentes, mas se olhamos para eles através da congruência módulo 5, não conseguimos distingui-los entre si: eles são todos congruentes módulo 5.

Este papo todo tem como única meta introduzir a seguinte pergunta:

> Se $a \equiv a' \pmod{n}$ e $b \equiv b' \pmod{n}$, o que podemos afirmar sobre a relação entre $a+b$ e $a'+b'$?

Usando a imagem da congruência como um filtro é fácil descobrir qual *deveria ser* a resposta a esta pergunta. De fato, se não temos como distinguir entre duas bolas coloridas a e a', nem entre duas bolas coloridas b e b' porque estamos olhando para elas através de um filtro vermelho, como poderemos ser capazes de distinguir entre os conjuntos formados por a e b, de um lado, e a' e b' do outro? É claro que, neste caso, os conjuntos parecerão iguais. Portanto, inspirados na conclusão fornecida por esta imagem, esperamos poder mostrar

que:

se $a \equiv a' \pmod{n}$ e $b \equiv b' \pmod{n}$, então $a + b \equiv a' + b' \pmod{n}$.

O problema é que o filtro colorido é apenas uma imagem para nos guiar, não há como ter certeza de que esta imagem vai ser adequada neste caso. Contudo, uma vez que tenhamos tomado uma decisão sobre *qual deveria ser a resposta*, podemos testá-la em alguns casos simples. Por exemplo,

$$51 \equiv 31 \pmod{5} \quad \text{e} \quad 43 \equiv 103 \pmod{5},$$

ao passo que

$$51 + 43 = 94 \quad \text{e} \quad 31 + 103 = 134;$$

contudo,

$$94 - 134 = 40 = 5 \cdot 8 \quad \text{donde} \quad 94 \equiv 134 \pmod{5}.$$

Embora exemplos como este e quaisquer outros que decidamos inventar aumentem nossa confiança na conclusão, não podemos dá-la como certa a não ser que consigamos prová-lo com rigor matemático.

Como ainda estamos no início de nosso estudo de congruência, pouco sabemos sobre as suas propriedades. Assim, para ter um ponto de partida sólido e já estabelecido no qual nos apoiar, mostraremos que a propriedade desejada é consequência de fatos bem conhecidos dos números inteiros. Nisto vamos apenas repetir a mesma estratégia que já usamos em 2.2.2.

Temos, então, como hipótese que

$$a \equiv a' \pmod{n} \quad \text{e} \quad b \equiv b' \pmod{n}.$$

Mas, usando a definição, podemos traduzir estas congruências na forma das seguintes igualdades de inteiros

$$a - a' = k \cdot n \quad \text{e} \quad b - b' = \ell \cdot n,$$

onde, como em ocasiões anteriores, k e ℓ são os respectivos cofatores. Somando, agora, as duas equações, resulta que

$$(a - a') + (b - b') = k \cdot n + \ell \cdot n.$$

Rearrumando o lado esquerdo e usando a distributividade do lado direito,

$$(a + b) - (a' + b') = (k + \ell) \cdot n;$$

que, traduzido na linguagem de congruências, nos dá

$$(a + b) \equiv (a' + b') \pmod{n};$$

confirmando nossas suspeitas.

Exercício 19. *Mostre que, se* $a \equiv a' \pmod{n}$ *e* $b \equiv b' \pmod{n}$*, então* $a - b \equiv a' - b' \pmod{n}$.

Passando, agora, à pergunta análoga para a multiplicação:

> Se $a \equiv a' \pmod{n}$ e $b \equiv b' \pmod{n}$, o que podemos afirmar sobre a relação entre $a \cdot b$ e $a' \cdot b'$?

Nossa experiência anterior com a adição nos permite afirmar, com uma confiança razoável, que a resposta deve ser que

$$a \cdot b \equiv a' \cdot b' \pmod{n}.$$

Testando nossa conclusão no mesmo exemplo usado no caso da adição, temos de

$$51 \equiv 31 \pmod{5} \quad \text{e} \quad 43 \equiv 103 \pmod{5},$$

que

$$51 \cdot 43 = 2\,193 \quad \text{e} \quad 31 \cdot 103 = 3\,193;$$

cuja diferença é $-1\,000$ e, portanto, um múltiplo de 5, assim

$$51 \cdot 43 \equiv 31 \cdot 103 \pmod{5},$$

como havíamos previsto. Logo, esperamos poder provar que

$$\text{se } a \equiv a' \pmod{n} \text{ e } b \equiv b' \pmod{n}, \text{ então } a \cdot b \equiv a' \cdot b' \pmod{n}.$$

Como no caso da adição, as congruências

$$a \equiv a' \pmod{n} \quad \text{e} \quad b \equiv b' \pmod{n}.$$

se traduzem como as igualdades de inteiros

$$a - a' = k \cdot n \quad \text{e} \quad b - b' = \ell \cdot n$$

onde k e ℓ são inteiros. Copiando o que fizemos no caso da adição, deveríamos multiplicar estas equações; só que, desta vez, é mais con-

veniente reescrever estas equações em outra forma, antes de fazer cálculos com elas. A forma desejada é

$$a = a' + k \cdot n$$

para a primeira, e

$$b = b' + \ell \cdot n,$$

para a segunda. Multiplicando estas duas equações, membro a membro, temos

$$a \cdot b = (a' + k \cdot n)(b' + \ell \cdot n). \tag{2.2.1}$$

Utilizando a distributividade da multiplicação sobre a soma, o lado direito se expande na forma

$$(a' + k \cdot n)(b' + \ell \cdot n) = a' \cdot b' + a' \cdot \ell \cdot n + k \cdot n \cdot b' + k \cdot n \cdot \ell \cdot n.$$

Pondo n em evidência,

$$(a' + k \cdot n)(b' + \ell \cdot n) = a' \cdot b' + n \cdot (a' \cdot \ell + k \cdot b' + k \cdot \ell \cdot n).$$

Comparando esta última equação com (2.2.1), vemos que

$$a \cdot b = a' \cdot b' + n \cdot (a' \cdot \ell + k \cdot b' + k \cdot \ell \cdot n);$$

donde,

$$a \cdot b - a' \cdot b' = n \cdot (a' \cdot \ell + k \cdot b' + k \cdot \ell \cdot n),$$

de modo que a diferença $a \cdot b - a' \cdot b'$ é um múltiplo de n. Mas isto equivale a dizer que $a \cdot b \equiv a' \cdot b' \pmod{n}$, como pretendíamos mostrar. Resumindo, provamos as seguintes fórmulas.

Proposição 5. *Se* $a \equiv a' \pmod{n}$ *e* $b \equiv b' \pmod{n}$*, então:*

- $a + b \equiv a' + b' \pmod{n}$*;*
- $a \cdot b \equiv a' \cdot b' \pmod{n}$.

Em particular,

- $a^k \equiv (a')^k \pmod{n}$*, para qualquer* $k \geq 0$.

Tendo feito o esforço de verificar estas propriedades, resta-nos ver que realmente valeu a pena.

2.3 Critérios de Divisibilidade

Nesta seção utilizaremos o que aprendemos sobre a congruência modular para estabelecer alguns critérios simples de divisibilidade por primos. Como bônus, provaremos também que a prova dos nove funciona corretamente.

Se n for um inteiro positivo, então um *critério de divisibilidade por* n é uma regra que nos permite determinar se um dado inteiro é, ou não divisível por n, *a um custo menor que o de efetuar a divisão.* É claro que a parte crítica desta definição é a última: o custo de aplicar a regra que corresponde ao critério tem que ser menor que dividir o número dado por n, senão o critério simplesmente não vale a pena.

Por exemplo,

> um número inteiro é divisível por 5 se, e somente se, seu algarismo das unidades é 0 ou 5

nos dá o bem conhecido *critério de divisibilidade por* 5. Nossa familiaridade com este critério é mera consequência da observação do comportamento dos múltiplos de 5. Outro critério que também conhecemos bem por pura experiência é o dos múltiplos de 2:

> um número inteiro é divisível por 2 se, e somente se, seu algarismo das unidades é 0, 2, 4, 6 ou 8;

ou, dito em outras palavras,

> um número inteiro é *par* se, e somente se, seu algarismo das unidades é *par*.

Exercício 20. *Prove os critérios de divisibilidade por* 2 *e por* 5 *enunciados acima.*

2.3.1 Divisibilidade por 3

Um outro critério bem conhecido é o de divisibilidade por 3:

> um número inteiro é divisível por 3 se, e somente se, a soma dos seus algarismos é divisível por 3.

Só que, desta vez, o critério não segue imediatamente as regularidades relativas aos múltiplos de 3 que nos são familiares. Usaremos, a seguir, a congruência módulo 3 para provar que este critério é verdadeiro.

Para começar, seja a o número inteiro que queremos saber se é ou não divisível por 3. Para poder aplicar o critério, precisamos conhecer os algarismos de a. Digamos que

$$a_n a_{n-1} \dots a_1 a_0,$$

são estes algarismos, onde a_0 é o algarismo das unidades, a_1 o algarismo das dezenas, e assim por diante. Note que, como $a_0, a_1, \ldots, a_n$ são algarismos, cada um deles é maior ou igual a 0 e menor ou igual a 9, exceto por a_n que não pode ser igual a zero. Dizer que a tem como algarismos decimais $a_n a_{n-1} \ldots a_1 a_0$ é o mesmo que dizer que

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0. \tag{2.3.1}$$

Contudo, $10 \equiv 1 \pmod 3$. Por outro lado,

$$10^2 = 10 \cdot 10,$$

satisfaz

$$10^2 \equiv 10 \cdot 10 \equiv 1 \cdot 1 \equiv 1 \pmod 3.$$

Observe que a congruência da esquerda é óbvia pois dois números iguais são congruentes qualquer que seja o módulo escolhido. Já a segunda congruência é bem mais interessante. Como vimos em 2.2.4,

se $a \equiv a' \pmod n$ e $b \equiv b' \pmod n$, então $a \cdot b \equiv a' \cdot b' \pmod n$.

Tomando, $a = b = 10$ e $a' = b' = 1$, podemos concluir de $10 \equiv 1 \pmod 3$ que

$$10^2 \equiv 1^2 \equiv 1 \pmod 3.$$

Nada nos impede de parar aqui. Assim,

$$10^3 = 10^2 \cdot 10,$$

nos diz que

$$10^3 \equiv 10^2 \cdot 10 \pmod 3.$$

Como já sabemos que $10 \equiv 1 \pmod 3$ e acabamos de verificar que $10^2 \equiv 1 \pmod 3$, podemos concluir da propriedade da multiplicação e da transitividade da congruência que

$$10^3 \equiv 10^2 \cdot 10 \equiv 1 \cdot 1 \equiv 1 \pmod 3.$$

Exercício 21. *Use um argumento semelhante para calcular* 10^4 *módulo* 3. *Você consegue imaginar duas maneiras diferentes de organizar este cálculo?*

É fácil imaginar que este procedimento pode ser continuado indefinidamente e que nos permite verificar que

$10^k \equiv 1 \pmod 3$ qualquer que seja o inteiro $k \geq 0$ escolhido.

O que é que $10^k \equiv 1 \pmod 3$ nos diz sobre a divisibilidade por 3? Voltando um pouco atrás, lembre-se que havíamos chegado à conclusão que

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0.$$

Contudo, pela propriedade reflexiva da congruência, isto implica que

$$a \equiv a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0 \pmod 3.$$

Mas, como acabamos de ver, cada uma das potências de 10 módulo 3 é congruente a 1. Usando isto e as duas propriedades que relacionam

a adição e a multiplicação à congruência, concluímos que

$$a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 3.$$

Logo, pela transitividade,

$$a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 3,$$

que é exatamente o que precisamos para podermos concluir o critério de divisibilidade por 3. De fato, dizer que a é divisível por 3 é o mesmo que dizer que $a \equiv 0 \pmod 3$. Como

$$a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 3,$$

a transitividade nos garante que $a \equiv 0 \pmod 3$ ocorre exatamente quando

$$a_n + a_{n-1} + \cdots + a_1 + a_0 \equiv 0 \pmod 3;$$

que, por sua vez, equivale a dizer que

$$a_n + a_{n-1} + \cdots + a_1 + a_0$$

é divisível por 3. Mas,

$$a_n + a_{n-1} + \cdots + a_1 + a_0$$

é a soma dos algarismos de a; portanto,

> a é divisível por 3 se, e somente se, a soma $a_n + a_{n-1} + \cdots + a_1 + a_0$ dos seus algarismos for divisível por 3,

o que prova que o critério está correto.

Este argumento pode ser copiado para nos dar um critério semelhante, só que desta vez para a divisibilidade por 11. Para obtê-lo, resolva o próximo exercício.

Exercício 22. *Com este exercício procuramos determinar um critério de divisibilidade por* 11. *Procederemos de maneira semelhante ao que foi feito acima. Para isto:*

(a) determine quanto vale 10^k *módulo* 11*;*

(b) escrevendo a na forma da equação (2.3.1)*, calcule a módulo* 11 *usando o resultado obtido em (a).*

2.3.2 Prova dos Nove

Com o que fizemos para provar o critério de divisibilidade por 3 estamos prontos para verificar porque a prova dos nove funciona corretamente. Como vimos na página 43, a principal operação da prova dos nove pode ser definida, sobre um inteiro positivo a, da seguinte maneira

$$\textit{a noves fora} \text{ é igual a } \begin{cases} a & \text{se } \ a < 9; \\ a - 9 & \text{se } \ a \geq 9. \end{cases}$$

Sejam a e a' os dois números inteiros positivos que desejamos somar. Como a prova é aplicada aos algarismos dos números, precisamos listá-los. Mas um número a com $n+1$ algarismos é da forma

$$a_n a_{n-1} \ldots a_1 a_0,$$

onde a_0 é o algarismo das unidades, a_1 o algarismo das dezenas, e assim por diante. Isto equivale a dizer que, se a tem n algarismos, então

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0;$$

donde

$$a \equiv a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0 \pmod 9.$$

Como, $10 \equiv 1 \pmod 9$, temos que qualquer potência de 10 também é congruente a 1 módulo 9, e assim,

$$a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 9;$$

de forma que o resíduo de a módulo 9 é igual ao resíduo módulo 9 da soma dos seus algarismos. Além disso, usando as fórmulas da proposição 5, podemos calcular o resíduo de

$$a_n + a_{n-1} + \cdots + a_1 + a_0$$

passo a passo. Começamos determinando o resíduo r_n de a_n módulo 9. Como a_n é um algarismo e, portanto, está entre 0 e 9, isto pode ser feito usando a operação *noves fora*; o que nos dá

$$r_n = \begin{cases} a_n & \text{se} \quad a_n < 9; \\ 0 & \text{se} \quad a_n = 9. \end{cases}$$

Em seguida, calculamos o resíduo r_{n-1} de

$$r_n + a_{n-1} \equiv a_n + a_{n-1} \pmod 9.$$

Contudo, como $0 \leq r_n < 9$ e $0 \leq a_{n-1} \leq 9$, temos que $0 \leq r_n + a_{n-1} < 18$, de modo que, para achar seu resíduo módulo 9, precisamos, no máximo, subtrair 9 de $r_n + a_{n-1}$. Em outras palavras, basta fazer *noves fora* em $r_n + a_{n-1}$. Em seguida vem o resíduo r_{n-2} de

$$r_{n-1} + a_{n-2} \equiv a_n + a_{n-1} + a_{n-2} \pmod 9$$

que, pelo mesmo argumento, é igual a *noves fora* $r_{n-1} + a_{n-2}$. O processo continua desta maneira até obtermos r_0 que, sendo o resíduo de

$$r_1 + a_0 \equiv a_n + a_{n-1} + a_{n-2} + \cdots + a_0 \pmod 9$$

é igual a *noves fora* $r_1 + a_0$. Moral da história, aplicando *noves fora* à soma progressiva dos algarismos de a, obtemos o resíduo r_0 de a módulo 9.

Evidentemente, ao aplicarmos o mesmo processo a a' e a $a + a'$ obtemos seus resíduos r'_0 e s_0 módulo 9. A prova dos nove segue, então, das fórmulas da proposição 5, segundo as quais

$$r_0 + r'_0 \equiv a + a' \equiv s_0 \pmod 9.$$

Exercício 23. *Mostre que é possível obter, de maneira semelhante, uma* prova dos três.

A *prova dos três* é ainda mais fácil de aplicar que a dos nove, então por que nunca ouvimos falar dela?

Exercício 24. *Mostre que há muitas contas incorretas que a* prova dos nove *detecta que estão erradas, mas que parecem corretas quando aplicamos a* prova dos três.

Como vimos em 2.1.3, a *prova dos nove* não se aplica apenas à adição, um argumento análogo ao que fizemos acima mostra que também pode ser usada para a multiplicação. E mais: apesar de raramente ouvirmos falar da *prova dos nove* para a divisão, ela também pode ser utilizada para esta operação.

Exercício 25. *Formule uma versão da prova dos nove para a divisão e mostre que funciona corretamente.*

2.3.3 Divisibilidade por 7

Em 2.3.1 vimos como enunciar e provar os critérios de divisibilidade por 2, 3 e 5. Além disso, propusemos no exercício 22 um critério para a divisibilidade por 11. Considerando os primos de 2 a 11, o único para o qual ainda não temos um critério é 7. Você conhece algum critério de divisibilidade por 7?

Muito provavelmente sua resposta à pergunta foi "não". Mas nada nos impede de usar a mesma estratégia utilizada na obtenção de um critério por 3 e por 11 para tentar achar um critério para divisibilidade por 7? A resposta, naturalmente, é "nada"! Vejamos o que acontece se fizermos isto. Para começar, sabemos que expressar um inteiro a a partir dos seus algarismos

$$a_n a_{n-1} \cdots a_1 a_0$$

significa que

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} \cdots + a_1 \cdot 10 + a_0.$$

Como isto implica que

$$a \equiv a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} \cdots a_1 \cdot 10 + a_0 \pmod 7,$$

o critério segue por transitividade se pudermos determinar a que são congruentes as várias potências de 10 módulo 7.

Aplicando a mesma estratégia já usada em 2.3.1, temos as seguintes congruências módulo 7:

$$\begin{aligned}
&10^1 \equiv 3 \pmod 7,\\
&10^2 \equiv 3^2 \equiv 2 \pmod 7,\\
&10^3 \equiv 10 \cdot 10^2 \equiv 3 \cdot 2 \equiv 6 \equiv -1 \pmod 7,\\
&10^4 \equiv 10 \cdot 10^3 \equiv (-1) \cdot 3 \equiv 4 \pmod 7,\\
&10^5 \equiv 10 \cdot 10^4 \equiv 3 \cdot 4 \equiv 5 \pmod 7,\\
&10^6 \equiv 10 \cdot 10^5 \equiv 3 \cdot 5 \equiv 1 \pmod 7.
\end{aligned}$$

Para efetuar estes cálculos usamos livremente as várias propriedades da congruência que já conhecemos. Paramos na sexta potência simplesmente porque, daí em diante os restos vão se repetir. De fato,

$$10^7 \equiv 10^6 \cdot 10 \equiv 1 \cdot 3 \equiv 3 \pmod 7,$$

ao passo que

$$10^8 \equiv 10^6 \cdot 10^2 \equiv 1 \cdot 10^2 \equiv 2 \pmod 7,$$

e assim por diante. Mais precisamente, se m é um inteiro qualquer e

q e r seu quociente e resto módulo 6, então

$$10^m \equiv 10^{6q+r} \equiv (10^6)^q \cdot 10^r \pmod 7.$$

Como $10^6 \equiv 1 \pmod 7$, concluímos que

$$(10^6)^q \cdot 10^r \equiv 10^r \pmod 7;$$

e a transitividade nos dá

$$10^m \equiv 10^r \pmod 7.$$

Mas isto é ótimo porque, sendo um resto da divisão por 6, r satisfaz a desigualdade $0 \leq r \leq 5$, de modo que 10^r pode ser determinado facilmente da lista das potências módulo 7 calculada acima. Por exemplo,

$$10^{1\,007} \equiv 10^5 \equiv 5 \pmod 7,$$

porque 1 007 deixa resto 5 na divisão por 6.

Exercício 26. *Calcule o valor das seguintes potências de* 10 *módulo* 7*:*

$$10^{9\,876},\ 10^{6\,543} \ \textit{e}\ \ 10^{1\,247}.$$

Voltando à questão da divisibilidade por 7, devemos aplicar o valor das potências calculadas acima à congruência

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} \cdots + a_1 \cdot 10 + a_0.$$

Fazendo isto, e escrevendo as potências da maior para a menor, temos

$$a \equiv a_0 + a_1 \cdot 3 + a_2 \cdot 2 + a_3 \cdot 6 + a_4 \cdot 4 + a_5 \cdot 5 + a_6 + \\ + a_7 \cdot 3 + \cdots + a_n \cdot 10^r \pmod 7,$$

onde r é o resto da divisão de n por 6. O que você acha? É mais fácil aplicar isto, ou dividir a por 7 e ver se o resto é zero? Como tenho dificuldade em lembrar sequências de números (inclusive, infelizmente, números de telefone...) e como dificilmente vou precisar verificar, na mão, se um número maior que 1 000 000 é divisível por 7, a minha escolha recairia em efetuar a divisão diretamente.

Por sorte, há uma outra maneira de enunciar o critério de divisibilidade por 7 que o torna mais fácil de lembrar. Antes, porém, precisamos de alguma preparação. Digamos que, como antes,

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} \cdots + a_1 \cdot 10 + a_0.$$

Isolando o algarismo das unidades de a podemos escrever

$$a = (a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} \cdots + a_1) \cdot 10 + a_0.$$

Note que pusemos 10 em evidência. Assim, se escrevermos

$$\hat{a} = (a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} \cdots + a_1),$$

teremos

$$a = \hat{a} \cdot 10 + a_0.$$

Um exemplo pode esclarecer o que fizemos. Digamos que

$$a = 12\,346\,998\,654\,343$$

que tem como algarismo das unidades $a_0 = 3$. Assim,

$$a = 1\,234\,699\,865\,434 \cdot 10 + 3,$$

de modo que, neste caso,

$$\hat{a} = 1\,234\,699\,865\,434.$$

Exercício 27. *Determine a_0 e $\hat{a}$ para cada um dos números a indicados abaixo:*

$$a = 87\,645\,564\,348,\ a = 85\,735\,214\,421 \quad e \quad a = 981\,231\,111.$$

Uma vez que tenhamos escrito a na forma

$$a = 10 \cdot \hat{a} + a_0,$$

aplicamos a congruência módulo 7. Como $10 \equiv 3 \pmod 7$, temos que

$$a \equiv 10 \cdot \hat{a} + a_0 \equiv 3 \cdot \hat{a} + a_0 \pmod 7.$$

Portanto, pela transitividade,

$$a \equiv 3 \cdot \hat{a} + a_0 \pmod 7; \tag{2.3.2}$$

isto é,

a é divisível por 7 se, e somente se $3 \cdot \hat{a} + a_0$ também for.

Por exemplo, digamos que desejamos saber se 128 é divisível por 7. Como, se $a = 128$, então $a_0 = 8$ e $\hat{a} = 12$, temos que

$$3 \cdot \hat{a} + a_0 = 12 \cdot 3 + 8 = 44.$$

Como 44 *não é* divisível por 7, o critério acima nos garante que 128 também não pode ser.

Podemos reformular este critério de uma maneira ainda mais agradável. Para isto multiplicamos ambos os membros de (2.3.2) por 2, o que nos dá

$$2 \cdot a \equiv 2 \cdot (3 \cdot \hat{a} + a_0) \equiv 6 \cdot \hat{a} + 2 \cdot a_0 \pmod 7,$$

pela distributividade. Contudo, $6 \equiv -1 \pmod 7$, donde

$$2 \cdot a \equiv -\hat{a} + 2 \cdot a_0 \pmod 7.$$

Claramente, se $a \equiv 0 \pmod 7$, então

$$-\hat{a} + 2 \cdot a_0 \equiv 0 \pmod 7, \tag{2.3.3}$$

pela transitividade da congruência. Por exemplo, sabendo que 875 é múltiplo de 7, podemos concluir que

$$-87 + 2 \cdot 5 = 77$$

também tem que ser. Infelizmente estamos andando na direção errada. Afinal, é difícil imaginar alguém que soubesse que 875 é múltiplo

de 7, mas ignorasse que 77 também é.

O que seria útil é se fôssemos capazes de provar a recíproca; isto é, que se

$$-\hat{a} + 2 \cdot a_0 \equiv 0 \pmod 7, \tag{2.3.4}$$

então $a \equiv 0 \pmod 7$. Para isto precisamos desfazer o que fizemos ao multiplicar a equação toda por 2. Mas isto é fácil de fazer. Como

$$2 \cdot 3 \equiv -1 \pmod 7,$$

temos ao multiplicar ambos os lados de (2.3.4) por 3, que

$$3 \cdot (-\hat{a} + 2 \cdot a_0) \equiv 3 \cdot 0 \pmod 7.$$

Usando a distributividade do lado esquerdo,

$$-3 \cdot \hat{a} + 6 \cdot a_0 \equiv 0 \pmod 7;$$

de modo que $6 \equiv -1 \pmod 7$ nos dá

$$-3 \cdot \hat{a} - a_0 \equiv 0 \pmod 7.$$

Pondo -1 em evidência

$$-(3 \cdot \hat{a} + a_0) \equiv 0 \pmod 7. \tag{2.3.5}$$

Acontece que

$$3 \cdot \hat{a} + a_0 \equiv a \pmod 7$$

de forma que (2.3.5) pode ser reescrita na forma

$$-a \equiv 0 \pmod 7,$$

que é o mesmo que dizer que 7 divide a. Resumindo, mostramos que

se $-\hat{a} + 2 \cdot a_0 \equiv 0 \pmod 7$ então $a \equiv 0 \pmod 7$.

Logo,

para mostrar que 7 divide a, basta testar se 7 divide $-3 \cdot \hat{a} - a_0$, de acordo com a decomposição de a explicada anteriormente.

Voltando ao exemplo anterior, como

$$-87 + 2 \cdot 5 = -77$$

é obviamente divisível por 7, podemos concluir que 875 também é. Partindo para um exemplo mais impressionante, digamos que queremos saber se $a = 10\,794$ é, ou não divisível por 7. Neste caso,

$$a_0 = 4 \text{ e } \hat{a} = 1079,$$

de modo que, pelo critério estabelecido acima, basta descobrir se 7 divide ou não

$$-\hat{a} + 2 \cdot a_0 = -1\,079 + 2 \cdot 4 = -1\,071.$$

Como isto ainda não é fácil de determinar, vamos usar o critério

novamente, só que desta vez para

$$b = 1\,071.$$

Temos que

$$b_0 = 1 \text{ e } \hat{a} = 107,$$

e assim

$$-\hat{b} + 2 \cdot b_0 = -107 + 2 \cdot 1 = -105.$$

Portanto, usando novamente o critério, se 7 divide -105 ou, o que dá no mesmo, se 7 divide -105, então 7 divide b. Como ainda não sei se 7 divide ou não 105, vou aplicar o critério uma última vez, agora a $c = 105$ que tem

$$c_0 = 5 \text{ e } \hat{c} = 10.$$

Como

$$-\hat{c} + 2 \cdot c_0 = -10 + 2 \cdot 5 = 0$$

é claramente divisível por 7, então 7 divide $c = 105$. Mas isto implica, pelo critério, que 7 divide $b = 1\,071$ que, por sua vez, implica que 7 divide $a = 10\,794$, que é o que queríamos saber.

Observe que aplicamos a regra dada pelo critério a números sucessivamente menores, até obter um caso em que sabíamos a resposta sem fazer sequer uma conta. Temos, assim, uma regra *recursiva*, que é o termo utilizado pelos matemáticos para descrever uma regra que reduz um dado problema a um problema análogo mas com dados menores.

Exercício 28. *Use o critério de divisibilidade por* 7 *tantas vezes quantas forem necessárias para determinar se* 35 994 *e se* 36 003 *são di-*

visíveis por 7.

Para encerrar, aqui está um exercício um pouco diferente que pode ser resolvido facilmente usando congruências.

Exercício 29. *Ache um fator primo ímpar de* $5^{25} - 1$.

Capítulo 3

Inversos Modulares

Nesta seção discutiremos um tema que vai ter importância decisiva tanto para o principal teorema desta apostila, quanto para o funcionamento do próprio RSA. Começamos analisando os cálculos que efetuamos para obter o critério de divisibilidade por 7 na seção anterior.

3.1 Motivação e Definições

Você deve ter observado o importante papel que os números 2 e 3 desempenharam no argumento em 2.3.3. Precisávamos mostrar que duas congruências eram equivalentes; mais precisamente, as congruências dadas nas equações (2.3.2) e (2.3.3). Verificamos que, multiplicando (2.3.2) por 2, obtínhamos (2.3.3), ao passo que, multiplicando (2.3.3) por 3, obtínhamos (2.3.2). O segredo para o sucesso desta

conta está na congruência

$$2 \cdot 3 \equiv -1 \pmod 7.$$

Utilizando a linguagem que usaríamos se estivéssemos calculando com números racionais, podemos dizer que -1 "dividido" por 2 é igual a 3. Multiplicando toda a congruência por -1 obtemos

$$2 \cdot (-3) \equiv 1 \pmod 7 \quad \text{e também} \quad (-2) \cdot 3 \equiv 1 \pmod 7.$$

Como

$$-3 \equiv 4 \pmod 7 \quad \text{e} \quad -2 \equiv 5 \pmod 7,$$

podemos concluir que

$$2 \cdot 4 \equiv 1 \pmod 7 \quad \text{e} \quad 5 \cdot 3 \equiv 1 \pmod 7.$$

Neste caso, também podemos dizer que 1 dividido por 2 módulo 7 dá como resultado 5 e 1 dividido por 3 dá 5. Quando isto ocorre, dizemos que 2 e 4 são inversos módulo 7, e o mesmo se dá com 3 e 5.

Sistematizando o conteúdo do parágrafo anterior, diremos que a e a' são *inversos* módulo n se

$$a \cdot a' \equiv 1 \pmod n.$$

Neste caso, também dizemos que a' é o *inverso de a módulo n*, e vice-versa. Na tabela abaixo listamos cada um dos *resíduos* distintos possíveis de inteiros módulo 11, indicando o *resíduo* do seu respectivo inverso. Note que 0 não pode ter inverso módulo n não importa que

valor n assuma, já que

$$0 \cdot b \equiv 0 \pmod{n} \text{ qualquer que seja } b \in \mathbb{Z}.$$

Por isso sequer listamos zero entre os resíduos na tabela. Você pode

Resíduo	Inverso Módulo 11
1	1
2	6
3	4
4	3
5	9
6	2
7	8
8	7
9	5
10	10

estar se perguntando como os inversos nesta tabela foram obtidos. Embora exista uma maneira sistemática de calcular inversos módulo n, ela é trabalhosa demais para valer à pena aplicá-la quando o módulo n é um número pequeno. Por isso, os inversos na tabela foram determinados por tentativa. Em outras palavras, para achar o inverso de 2 módulo 11, multiplicamos 2 pelos inteiros de 2 em diante

até obter a congruência desejada; neste caso,

$$\begin{aligned}
2 \cdot 2 &\equiv 4 \not\equiv 1 \pmod{11} \\
2 \cdot 3 &\equiv 6 \not\equiv 1 \pmod{11} \\
2 \cdot 4 &\equiv 8 \not\equiv 1 \pmod{11} \\
2 \cdot 5 &\equiv 10 \not\equiv 1 \pmod{11} \\
2 \cdot 6 &\equiv 12 \equiv 1 \pmod{11}
\end{aligned}$$

e obtivemos o inverso procurado. Note que isto significa que 6 tem como inverso 2, de modo que acabamos por preencher duas linhas da tabela, a segunda e a sexta.

Na verdade, podemos utilizar um pouco mais que mera tentativa, porque se nos restringimos aos inteiros entre 1 e $n-1$, então cada um destes inteiros tem *exatamente um inverso* neste intervalo. De fato, se a' e a'' são ambos inversos de a módulo n, ambos entre 1 e $n-1$, então

$$a \cdot a' \equiv 1 \pmod{n} \quad \text{e} \quad a \cdot a'' \equiv 1 \pmod{n};$$

donde concluímos que

$$a'' \cdot (a \cdot a') \equiv a'' \cdot 1 \equiv a'' \pmod{n}$$

e também que

$$(a'' \cdot a) \cdot a' \equiv 1 \cdot a' \equiv a' \pmod{n}.$$

Mas tudo o que fizemos foi mudar a posição dos parênteses, e isto não

altera o resultado da conta, logo

$$a' \equiv a'' \pmod{n}.$$

Mas isto significa que a diferença $a' - a''$ é divisível por n. Contudo, a' e a'' são positivos e menores que n, de modo que

$$-n < a' - a'' < n.$$

Logo, a única maneira de $a' - a''$ ser múltiplo de n é se for igual a zero; donde $a' = a''$.

Você pode estar pensando:

> Muito bom, muito bem; mas de que forma isto ajuda na hora de calcular a tabela?

A resposta é que, se já sabemos, por exemplo, que 2 e 6 são inversos um do outro módulo 11, então nem 2 nem 6 podem ser inversos de 3 módulo 11. Assim, procuraremos pelo resíduo do inverso de 3 apenas entre os inteiros $3, 4, 5, 7, 8, 9$ e 10. Por isso, quanto mais inversos determinamos, mais rápido fica determinar os que ainda faltam.

Exercício 30. *Usando as estratégias descritas acima, determine um inverso para cada um dos resíduos distintos módulo* 7 *e para cada um dos resíduos distintos módulo* 13.

Note que existem alguns números que são seus próprios inversos. Na tabela módulo 11, isto vale para 1 e 10. No caso de 1 isto não é nenhuma surpresa, afinal $1 \cdot 1 = 1$; já para 10 o resultado não parece tão óbvio. Contudo, o fato de 10 ser seu próprio inverso módulo 11

não é mera coincidência, como talvez você já tenha desconfiado ao calcular as tabelas correspondentes a 7 e a 13 no exercício 30. No próximo exercício você encontrará a explicação para este fenômeno.

Exercício 31. *Mostre que $n-1$ é sempre seu próprio inverso módulo n.*

Uma questão mais sutil é se pode haver algum número n para o qual existe um inteiro a entre 2 e $n-2$, que é seu próprio inverso módulo n. Em outras palavras, existem inteiros $n > 1$ e a de modo que

$$2 \leq a \leq n-2 \text{ e } \quad a^2 \equiv 1 \pmod{n}?$$

A resposta é sim, mas o desafio de construir tais números fica para você.

Desafio 3. *Construa infinitos números n para os quais existe um inteiro a, entre 2 e $n-2$, que é seu próprio inverso módulo n.*

3.2 Inexistência de Inverso

Vamos calcular uma nova tabela de inversos, desta vez a tabela dos inversos dos resíduos distintos módulo 8. Como 1 é seu próprio

inverso, começaremos com 2; efetuando os cálculos vemos que

$$\begin{aligned}
2 \cdot 2 &\equiv 4 \not\equiv 1 \pmod 8 \\
2 \cdot 3 &\equiv 6 \not\equiv 1 \pmod 8 \\
2 \cdot 4 &\equiv 0 \not\equiv 1 \pmod 8 \\
2 \cdot 5 &\equiv 2 \not\equiv 1 \pmod 8 \\
2 \cdot 6 &\equiv 4 \not\equiv 1 \pmod 8 \\
2 \cdot 7 &\equiv 6 \not\equiv 1 \pmod 8
\end{aligned}$$

e, surpreendentemente, descobrimos que 2 não tem inverso módulo 8. Talvez você ache que teria sido mais preciso dizer "descobrimos que 2 não tem inverso módulo 8 *entre os números inteiros menores que* 8". Lembre-se, contudo, que todo inteiro é congruente módulo 8 ao seu resíduo. Como calcular com um número ou com seu resíduo produzem o mesmo resultado módulo 8, não pode haver *nenhum* inteiro que inverta 2, já que tal inteiro não existe entre os números inteiros de 1 a 8. Como se isto não bastasse, apareceu um resultado muito estranho nos cálculos acima:

> embora 2 e 4 não sejam congruentes a zero módulo 8, o produto deles dois é 8, que é congruente a zero módulo 8.

É como se estivéssemos dizendo que o produto de dois números não nulos deu zero, o que é muito esquisito. A lista completa dos inversos módulo 8 é dada na tabela 3.1

Resíduos	Inverso Módulo 8
1	1
2	*
3	3
4	*
5	5
6	*
7	7

Tabela 3.1: Inversos módulo 8

O asterisco que aparece na coluna dos inversos indica que o elemento correspondente não tem inverso. Neste caso, 2, 4 e 6 não admitem inverso módulo 8. A propósito, você observou que cada um dos elementos que tem inverso módulo 8 é seu próprio inverso?

Será que há uma regularidade clara que nos permita determinar quais são os elementos que têm inverso, e quais os que não têm inverso módulo n, para um dado n? Pelo menos no caso do módulo 8, a regularidade é clara: os ímpares têm inverso, os pares não. Vejamos o que acontece com outros módulos; para isso, calcularemos mais algumas tabelas.

Exercício 32. *Determine um inverso para cada um dos resíduos distintos módulo* 6 *e para cada um dos resíduos distintos módulo* 15.

Tendo calculado as tabelas, você terá verificado que às vezes um ímpar pode não ter inverso, e às vezes um par pode ter inverso, e com isso lá se foi nossa proposta de regularidade. Mas se você está lendo isto de maneira crítica (sem se deixar levar pela minha lábia...), deve estar se perguntando:

> Tem uma coisa esquisita nisso tudo. Eu já tinha feito um exercício assim, só que para 7 e 13, e todos os resíduos tinham inverso; uma maravilha! Agora ele me fala para fazer para 6 e 12 e aparecem vários resíduos sem inverso. Por que só agora? O que é que 7 e 13 têm de bom, que falta a 6 e 15?

A resposta, evidentemente, é que 7 e 13 são primos, ao passo que 6 e 15 são compostos. Então eu pergunto: olhando para as tabelas que você calculou, qual a relação entre os números que não têm inverso e os módulos correspondentes?

Se você pensou com cuidado, terá visto que tanto para o módulo 8, quanto para os módulos 6 e 15, os resíduos que não têm inverso são aqueles que têm um fator primo comum com o módulo. É por isso que os pares não têm inverso módulo 8. Para falar a verdade, é fácil entender porque isto acontece. Mas antes, um exercício. Nossa tentativa frustrada de descobrir o inverso de 2 módulo 8 revelou-nos que

$$2 \cdot 4 \equiv 0 \pmod 8),$$

muito embora, nem 2, nem 4 sejam congruentes a zero módulo 8.

Exercício 33. *Para cada um dos resíduos a que não têm inverso módulo* 6*, determine um resíduo $b \not\equiv 0 \pmod 6$ tal que $a \cdot b \equiv 0 \pmod 6$. Faça o mesmo para os resíduos que não têm inverso módulo* 15*.*

Este exercício parece sugerir que há uma forte ligação entre não ter inverso módulo n e ser anulado módulo n pelo produto com um

resíduo não nulo. Como veremos abaixo, é exatamente isto que acontece.

Digamos que n e $1 < a < n$ são inteiros positivos que têm um fator primo comum $1 < p < n$. Podemos, então, escrever

$$n = p \cdot c \quad \text{e} \quad a = p \cdot e,$$

onde c e e são os cofatores correspondentes. Como $1 < p < n$ então $c = n/p$ também satisfaz $1 < c < n$. Por sua vez, como $1 < a < n$ por hipótese, temos que nem c, nem a são congruentes a zero módulo n. Contudo,

$$c \cdot a \equiv c \cdot p \cdot e \pmod{n}.$$

Ocorre que $n = c \cdot p$, e assim

$$c \cdot p \equiv n \equiv 0 \pmod{n};$$

donde

$$c \cdot a \equiv c \cdot p \cdot e \equiv 0 \pmod{n}. \tag{3.2.1}$$

Bacana, não? Mas, como usar isto para verificar que a não tem inverso módulo n? Bem, de fato estes cálculos mostram que a não pode ter inverso módulo n. Para entender porquê, procederemos por contradição. Suponhamos que a realmente tivesse inverso a' módulo n. Neste caso, deveríamos ter que

$$a \cdot a' \equiv 1 \pmod{n}.$$

Multiplicando ambos os membros da congruência por c (o mesmo cofator c determinado acima), obtemos

$$c \cdot (a \cdot a') \equiv c \pmod{n}.$$

Reagrupando os parêntesis,

$$(c \cdot a) \cdot a' \equiv c \pmod{n}. \tag{3.2.2}$$

Só que, pela equação (3.2.1),

$$c \cdot a \equiv 0 \pmod{n};$$

de modo que

$$(c \cdot a) \cdot a' \equiv 0 \cdot a' \equiv 0 \pmod{n}.$$

Comparando isto com a equação (3.2.2), concluímos que

$$c \equiv 0 \pmod{n};$$

isto é, n divide c. Só que isto não pode ser verdade porque, como vimos acima, $1 < c < n$. Obtivemos, assim, uma conclusão absurda. Isto ocorreu porque fizemos uma hipótese falsa ao supor que a tem inverso módulo n. Portanto, a não pode ter inverso módulo n, como havíamos afirmado antes. Resumindo, mostramos o seguinte resultado.

Teorema 1. *Se existir um fator primo comum entre a e n, então a não tem inverso módulo n.*

3.2.1 Cancelamento

Há uma consequência importante da inexistência do inverso que vai surgir em nossas aplicações posteriores, por isso vamos discuti-la agora.

Se estamos calculando com número inteiros e nos deparamos com uma igualdade do tipo

$$a \cdot c = b \cdot c,$$

pensamos imediatamente em cancelar o c e concluir que $a = b$. Contudo, sabemos que isto só é possível se $c \neq 0$, porque multiplicar por zero iguala o produto a zero. Infelizmente, quando trabalhamos com congruências a situação torna-se bem pior.

Comecemos por um exemplo. Sabemos que

$$2 \not\equiv 0 \pmod 6 \text{ e } 3 \not\equiv 0 \pmod 6$$

ao passo que

$$2 \cdot 3 \equiv 6 \equiv 0 \pmod 6.$$

Assim, apesar da congruência

$$2 \cdot 3 \equiv 2 \cdot 0 \pmod 6$$

ser verdadeira, *não* podemos cancelar o 2 que multiplica os dois lados e concluir que

$$3 \equiv 0 \pmod 6$$

porque isto, como já vimos, é falso. Logo, neste exemplo, o cancelamento não é permitido.

Passando ao caso geral, digamos que $n > 0$ e $1 \leq a \leq n-1$ são inteiros que têm um fator primo comum $1 < p < n$. Escrevendo

$$n = p \cdot c \quad \text{e} \quad a = p \cdot e,$$

onde c e e são os cofatores correspondentes, temos que

$$a \cdot c \equiv a \cdot 0 \pmod{n};$$

embora a e c não possam ser congruentes a zero módulo n, já que são ambos positivos e menores que n. Com isto chegamos à seguinte conclusão:

> se a, b e $n > 1$ são inteiros que têm algum fator primo em comum, então a não pode ser cancelado em congruências do tipo
>
> $$a \cdot b \equiv a \cdot 0 \pmod{n}.$$

Por outro lado, se a admite um inverso módulo n e b e c são inteiros tais que

$$a \cdot b \equiv a \cdot c \pmod{n}, \tag{3.2.3}$$

então o a pode ser cancelado e podemos concluir que $b \equiv c \pmod{n}$. Para provar isto, procedemos como no argumento usado para provar o teorema 1. Seja a' o inverso de a módulo n. Multiplicando a congruência (3.2.3) por a', obtemos

$$(a' \cdot a) \cdot b \equiv (a' \cdot a) \cdot c \pmod{n}.$$

Como

$$a \cdot a' \equiv 1 \pmod{n},$$

resta apenas

$$b \equiv c \pmod{n};$$

mostrando que o cancelamento pode mesmo ser feito neste caso. Resumimos isto em um teorema para referência futura.

Teorema 2. *Suponha que a tem inverso módulo n. Se*

$$a \cdot b \equiv a \cdot c \pmod{n},$$

para $b, c \in \mathbb{Z}$, então

$$b \equiv c \pmod{n}.$$

3.3 Existência de Inverso

Tudo isto pode ser muito interessante, mas não deixa de ser muito negativo. Descobrimos como detectar que certos números não têm inverso módulo n, e provamos que nosso palpite estava correto. Mas, e quanto aqueles que têm inverso? O palpite mais óbvio, claro, é que todos os números que não têm fator próprio comum com n terão inverso módulo n. Sem esquecer, que este palpite é confirmado por todas as tabelas que calculamos anteriormente.

De fato, este resultado é verdadeiro mas, para prová-lo, teremos que trabalhar um pouco. Voltando às definições, sabemos que um

inteiro a tem inverso módulo n se existir um inteiro a' tal que

$$a \cdot a' \equiv 1 \pmod{n}. \tag{3.3.1}$$

Traduzindo isto em termos de divisibilidade de inteiros, temos que

$$n \quad \text{divide a diferença} \quad a \cdot a' - 1.$$

Em outras palavras, existe um inteiro k para o qual

$$a \cdot a' - 1 = n \cdot k. \tag{3.3.2}$$

Como esta última equação é equivalente a (3.3.1), podemos concluir que o que precisamos mostrar é que

> se a e n *não admitem nenhum fator próprio comum*, então existe um inteiro k para o qual $a \cdot a' - 1 = n \cdot k$.

Para provar este resultado, procedemos da seguinte forma. Considere, para começar, o conjunto $V(a, n)$ formado pelos *inteiros positivos* que podem ser escritos na forma

$$x \cdot a + y \cdot n$$

para alguma escolha de inteiros x e y. Note que x ou y podem ser nulos ou negativos, embora estejamos exigindo que $x \cdot a + y \cdot n$ seja positivo. Por exemplo, se $a = 5$ e $n = 12$, então tomando $x = -1$ e $y = 1$, temos que

$$x \cdot a + y \cdot n = (-1) \cdot 5 + 1 \cdot 12 = 7 > 0.$$

Logo, $7 \in V(5, 12)$.

Exercício 34. *Calcule* 5 *elementos em cada um dos seguintes conjuntos* $V(5,12)$, $V(7,15)$ *e* $V(5,10)$.

Uma pergunta razoável é:

Por que introduzimos este estranho conjunto $V(a,n)$?

A resposta é simples. Se fomos capazes de mostrar que $1 \in V(a,n)$ então têm que existir dois inteiros, digamos x_0 e y_0, tais que

$$1 = x_0 \cdot a + y_0 \cdot b.$$

Mas, tomando $a' = x_0$ e $k = y_0$, obtemos

$$1 = a' \cdot a + k \cdot b,$$

que é equivalente à equação desejada (3.3.2). Outro ponto importante a ser notado é que,

se $1 \in V(a,n)$, então ele tem que ser o *menor* elemento de $V(a,n)$,

pois este conjunto só tem elementos positivos.

Voltando ao caso geral, observamos que $V(a,n)$ não pode ser vazio porque tomando $x = 0$ e $y = 1$, vemos que

$$x \cdot a + y \cdot n = 0 \cdot a + 1 \cdot n = n > 0;$$

logo n pertence a $V(a,n)$. Na verdade, isto nos diz mais. Como a quantidade de inteiros entre 1 e n é finita, podemos escolher o menor

destes números que pertence a $V(a,n)$. Mas qualquer inteiro em $V(a,n)$ que esteja fora do intervalo que vai de 1 a n tem que ser maior que n e, portanto, maior que m. Logo,

m é o menor elemento do conjunto $V(a,n)$.

Para podermos concluir nossa demonstração precisamos verificar que $m = 1$. Como a e n são primos entre si, bastaria que fôssemos capazes de mostrar que m divide tanto a como n para que pudéssemos concluir que é igual a 1. Afinal, para um inteiro positivo dividir 1, ele tem que ser igual a 1. Vejamos como mostrar que m divide a e divide n.

Para começar, como $m \in V(a,m)$, então têm que existir inteiros x_1 e y_1 tais que

$$m = x_1 \cdot a + y_1 \cdot n. \tag{3.3.3}$$

Dividindo n por m, temos que

$$n = m \cdot q + r \text{ e } 0 \leq r < m,$$

onde q é o quociente e r o resto da divisão de n por m. Substituindo nesta equação a expressão para m dada em (3.3.3), obtemos

$$n = m \cdot q + r = (x_1 \cdot a + y_1 \cdot n) \cdot q + r,$$

que pode ser rearrumada na forma

$$r = (-x_1) \cdot a + (1 - y_1) \cdot n.$$

Em particular, podemos concluir que $r \in V(a,n)$ por causa da maneira

como conseguimos expressá-lo. Contudo, r é o resto da divisão de n por m, de modo que $r = 0$ ou $r \neq 0$. Só que, neste último caso, $r < m$ (já que m é o divisor), o que bate de frente com o fato de m ter sido escolhido como o menor elemento de $V(a, n)$. Portanto, só resta a primeira possibilidade. Mas se $r = 0$, então m divide n, como queríamos mostrar. Um argumento inteiramente análogo mostra que m divide a.

Exercício 35. *Mostre em detalhes que m divide a.*

Vamos recapitular o que fizemos acima:

- verificamos que $a \cdot a' \equiv 1 \pmod{n}$ é o mesmo que dizer que existe um inteiro k tal que $a \cdot a' + k \cdot n = 1$;
- definimos o conjunto $V(a, n)$ formado pelos inteiros positivos que podem ser escritos na forma

$$x \cdot a + y \cdot n;$$

- se $1 \in V(a, n)$ então existem inteiros x_0 e y_0 para os quais

$$x_0 \cdot a + y_0 \cdot n = 1,$$

e tomando $a' = x_0$ e $k = -y_0$ provamos o resultado desejado.

Portanto, basta mostrar que $1 \in V(a, n)$.

Seja, então, m o menor elemento de $V(a, n)$. Mostraremos que, como a e n são primos entre si, então $m = 1$:

- se r for o resto da divisão de n por m então $r = 0$ ou $r \neq 0$;
- se $r \neq 0$ então mostramos que r pertenceria a $V(a, n)$;
- como o resto é sempre menor que o divisor, teríamos $r < m$;
- mas isto não é possível pela escolha que fizemos para m;
- portanto, $r = 0$ e m divide n.

Um argumento análogo (ver exercício 35) mostra que m divide n. Assim,

- m é um divisor comum de a e de n;
- mas o único divisor comum positivo de a e n é 1;
- logo $m = 1$ e provamos o resultado desejado.

3.4 O Teorema e um Exemplo

É hora de reunir todos os resultados que provamos neste capítulo em um único teorema, que utilizaremos com frequência nesta apostila.

Teorema 3. *Sejam $a < n$ inteiros positivos. O resíduo a tem inverso módulo n se, e somente se, a e n não têm fatores primos em comum.*

Mostramos este resultado em duas partes. No teorema 1 verificamos que se a e n têm fatores primos em comum então *a não* pode ter inverso módulo n. Já a recíproca foi analisada na seção 3.3, onde mostramos que, quando a e n *não* têm fatores primos em comum,

então é possível achar inteiros a' e k tais que $a \cdot a' + k \cdot n = 1$. Como isto implica que $a \cdot a' \equiv 1 \pmod{n}$, podemos concluir que a' é o inverso de a módulo n.

Como consequência deste teorema, temos que se n for primo, então todo resíduo não nulo admite inverso módulo n. Isto explica porque as tabelas de inversos de 7, 11 e 13 podem ser completamente preenchidas. Por outro lado, o teorema também nos diz que, se n for composto, então sua tabela ficará incompleta, pois haverá resíduos sem inverso; o que explica o comportamento das tabelas de 6, 8 e 15.

Outro ponto importante é que nossa demonstração do teorema é o que os matemáticos chamam de *não construtiva*: ela nos garante a existência de um inverso para a quando a e n não têm fator primo comum, mas não nos diz como proceder para calcular este inverso. É importante entender que esta é uma deficiência de nossa demonstração e não do teorema em si. Para uma demonstração construtiva deste mesmo teorema, consulte o capítulo 1 da referência [2].

Combinando o teorema acima com o teorema 2 da página 92, obtemos o seguinte resultado.

Corolário 1. *Sejam $a < n$ inteiros positivos* sem fatores próprios comuns. *Se*

$$a \cdot b \equiv a \cdot c \pmod{n},$$

para $a, b \in \mathbb{Z}$, então

$$b \equiv c \pmod{n}.$$

Corolário? O que é isto? A palavra corolário em português vem do latim *corollarium* que tem uma história (ou etimologia) muito interessante. Originalmente *corolla* em latim era apenas o diminutivo

de *corona*, que quer dizer coroa. Daí a palavra passou a ser usada para significar também uma pequena guirlanda de flores entrelaçadas, por causa de sua semelhança a uma coroa pequena. *Corollarium* começou significando o dinheiro pago para comprar uma *corona*, mas seu sentido acabou se generalizando para cobrir um presente ou qualquer coisa dada de graça. Foi daí que veio o significado moderno: uma consequência quase que imediata (portanto, gratuita) de uma afirmação ou teorema.

3.4.1 Um Exemplo

Encerramos o capítulo considerando um exemplo mais geral de cálculo do inverso, que será muito importante em nossas aplicações do RSA. Suponha que o inteiro positivo n possa ser escrito na forma $n = 6 \cdot k - 2$, onde $k > 0$ é um inteiro. Os primeiros dez números que satisfazem esta propriedade estão listados na próxima tabela juntamente com os valores correspondentes para k:

k	1	2	3	4	5	6	7	8	9	10
$6 \cdot k - 2$	4	10	16	22	28	34	40	46	52	58

Acontece que 3 e $6 \cdot k - 2$ não podem ter nenhum fator primo comum, mas, ao invés de provar isto, vou deixar como exercício.

Exercício 36. *Mostre que* 3 *e* $6 \cdot k - 2$ *não admitem nenhum fator primo em comum.*

Em vista disto, o teorema nos garante que 3 deve ter inverso módulo $n = 6 \cdot k - 2$. Mas será que somos capazes de calcular este

inverso? A resposta é bem fácil. Como $n = 6 \cdot k - 2$, então

$$n - 1 = 6 \cdot k - 3.$$

Pondo 3 em evidência

$$n - 1 = 3(2 \cdot k - 1);$$

isto é,

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

Assim,

$$3(2 \cdot k - 1) + 1 \equiv 0 \pmod{n};$$

donde

$$3(2 \cdot k - 1) \equiv -1 \pmod{n};$$

que pode ser reescrito como

$$3(1 - 2 \cdot k) \equiv 1 \pmod{n}.$$

Logo, $1 - 2 \cdot k$ é o inverso de 3 módulo n. Como $1 - 2 \cdot k$ é negativo, vamos determinar o seu resíduo. Somando $n = 6 \cdot k - 2$, obtemos

$$1 - 2 \cdot k + n = 1 - 2 \cdot k + 6 \cdot k - 2 = 4 \cdot k - 1;$$

que é positivo para todo $k \geq 1$. Além disso, como $4 \cdot k < 6 \cdot k$, também temos que

$$4 \cdot k - 1 < 6 \cdot k - 2;$$

de forma que $4 \cdot k - 1$ é mesmo o resíduo de $1 - 2 \cdot k$ módulo $n = 6 \cdot k - 2$.

Exercício 37. *Calcule os inversos de* 2, 3 *e* 6 *módulo* $6 \cdot k + 1$.

Capítulo 4

Algoritmo Chinês do Resto

Neste capítulo veremos como calcular um inteiro que satisfaz simultaneamente a várias congruências com *módulos distintos*: o chamado *algoritmo chinês do resto*.

4.1 Exemplos

Começamos analisando um exemplo bastante simples.

4.1.1 Restos

Considere o seguinte problema:

> determine o menor inteiro positivo que deixa resto 1 na divisão por 3 e resto 2 na divisão por 5.

Note que este exemplo é simples o suficiente para que possamos resolvê-lo "de cabeça". Contudo, nas aplicações ao RSA, encontraremos sistemas muito maiores, que só conseguiremos resolver procedendo de maneira sistemática, que é outra forma de dizer *usando um algoritmo*. Começaremos descrevendo a aplicação do algoritmo geral ao exemplo acima.

Chamando de n o inteiro que buscamos, podemos escrever as equações correspondentes à divisão de n por 3 e 5 na forma

$$\begin{aligned} n &= 3q_1 + 1, \\ n &= 5q_2 + 2. \end{aligned}$$

Observe que usamos símbolos diferentes (q_1 e q_2) para denotar os quocientes destas divisões. Afinal, não há nenhuma razão para que os quocientes das duas divisões sejam os mesmos, e usar a mesma letra automaticamente implicaria esta igualdade incorreta.

Voltando ao sistema, temos duas equações com três variáveis, a saber n, q_1 e q_2. Como se isto não bastasse, queremos determinar uma solução inteira, o que complica ainda mais o problema. Entretanto, estas equações podem ser reescritas de uma maneira mais simples se usarmos congruências. Fazendo isto, obtemos

$$\begin{aligned} n &\equiv 1 \pmod 3, \\ n &\equiv 2 \pmod 5. \end{aligned}$$

À primeira vista a reformulação foi ótima; afinal, sobrou apenas uma variável: o que podia ser melhor? O problema é como usar as congruências para determinar o inteiro desejado. Geralmente,

quando temos mais de uma equação para resolver, tentamos combiná-las para achar a resposta desejada. Entretanto, estas duas congruências têm módulos *diferentes* e, portanto, não podemos combiná-las diretamente. O que fazer?

A saída é usar uma estratégia *híbrida*: substituiremos $n = 5q_2 + 2$ não na equação $n = 3 \cdot q_1 + 1$, mas sim na primeira congruência, isto é, em $n \equiv 1 \pmod 3$. Efetuando a substituição, obtemos

$$5q_2 + 2 \equiv 1 \pmod 3.$$

Acontece que $5 \equiv 2 \pmod 3$, de forma que a congruência pode ser reescrita na forma

$$2q_2 + 2 \equiv 1 \pmod 3.$$

Subtraindo 2 dos dois lados da congruência, chegamos a

$$2q_2 \equiv -1 \pmod 3;$$

ou ainda a

$$2q_2 \equiv 2 \pmod 3,$$

já que $-1 \equiv 2 \pmod 3$. Como 2 é inversível módulo 3, podemos cancelá-lo na congruência acima pelo teorema 2, o que nos dá

$$q_2 \equiv 1 \pmod 3.$$

Em outras palavras, q_2 deixa resto 1 na divisão por 3, de modo que podemos escrevê-lo como

$$q_2 = 3q_3 + 1,$$

onde q_3 corresponde ao quociente desta divisão.

Voltando ao problema original, temos, além das equações

$$n = 3q_1 + 1,$$
$$n = 5q_2 + 2,$$

originalmente obtidas, uma nova equação

$$q_2 = 3q_3 + 1,$$

que explicita q_2, ainda que seja ao preço de introduzir uma nova variável. Mas isto nos permite substituir o valor de q_2 diretamente na segunda das duas equações originalmente obtidas, o que nos dá

$$n = 5q_2 + 2 = 5(3q_3 + 1) + 2.$$

Fazendo as contas,

$$n = 15q_3 + 7.$$

E daí? Tínhamos duas equações. Fizemos uma peripécia usando congruências. Chegamos a uma nova equação em tudo semelhante às originais. Grande coisa!

Se estes pensamentos lhe passaram pela cabeça, então prepare-se para uma surpresa. O que acontece se dividirmos $15q_3 + 7$ por 3? Para começar, $15 = 3 \cdot 5$, de forma que

$$15q_3 + 7 = 3 \cdot 5q_3 + 7.$$

Se 7 fosse menor que 3, seria o resto desta divisão, como $7 \geq 3$, precisamos escrevê-lo na forma

$$7 = 3 \cdot 2 + 1.$$

Combinando as duas equações e pondo 3 em evidência, obtemos

$$15q_3 + 7 = 3 \cdot (5q_3 + 2) + 1;$$

logo $15q_3+7$ deixa resto 1 na divisão por 3, exatamente o que queríamos que acontecesse com o n a ser determinado em nosso problema. Com uma vantagem: isto acontece qualquer que seja o valor escolhido para q_3!

Passando à divisão por 5, temos que

$$15q_3 + 7 = 5 \cdot 3q_3 + 5 + 2 = 5(3q_3 + 1) + 2;$$

de forma que $15q_3 + 7$ deixa resto 2 na divisão por 5, satisfazendo, mais uma vez, ao que foi pedido no problema. Isto sugere que devemos considerar a solução como sendo $n = 15q_3 + 7$.

Observe, contudo, que o que obtivemos não foi *uma solução*, mas sim *uma família* de soluções. De fato, obteremos uma solução diferente para cada valor inteiro que escolhermos para q_3, como ilustrado na tabela 4.1.

q_3	$15q_3 + 7$
-3	-38
-2	-23
-1	-8
0	7
1	22
2	37
3	52

Tabela 4.1: Tabelando $n = 15q_3 + 7$

Dito isto, fica difícil não perguntar se *todas* as possíveis soluções deste problema podem ser obtidas da fórmula $n = 15q_3 + 7$ simplesmente escolhendo um valor adequado para q_3. A resposta é sim, mas para entender porque você terá que esperar até a seção 4.2.

Relendo o problema, verificamos que ainda há uma condição a ser satisfeita: queremos o *menor n positivo* que satisfaz as duas condições sobre os restos. Entretanto, como mostra a tabela:

- se $q_3 < 0$, então $15q_3 + 7 < 0$;
- se $q_3 > 0$, então $15q_3 + 7 > 7$;

de modo que o valor desejado é mesmo $n = 7$.

Antes de passar a um novo exemplo, vamos refazer a verificação de que $n = 15q_3 + 7$ nos dá uma família de soluções para a equação. Só que desta vez usaremos congruências. Da igualdade $n = 15q_3 + 7$ obtemos a congruência

$$n \equiv 15q_3 + 7 \equiv 1 \equiv 1 \pmod 3;$$

pois $15 \equiv 0 \pmod 3$ e $7 \equiv 1 \pmod 3$. Da forma semelhante,

$$n \equiv 15q_3 + 7 \equiv 2 \equiv 2 \pmod 5.$$

Estas verificações são muito mais diretas e automáticas e, daqui por diante, serão usadas como nossa maneira-padrão de testar a correção de nossas soluções.

Exercício 38. *Na encenação de uma batalha, duas tropas se enfrentam, posicionando-se, atirando com festim, e recarregando seus mosquetes, cada uma a sua vez. Cada lado começa com o mesmo número de cartuchos. Uma tropa tem* 100 *mosquetes e, depois de atirar tantos tiros de festim quanto possíveis, lhe sobram* 13 *cartuchos. A outra tropa tem* 67 *mosquetes, e ao fim da exibição, sobram-lhe* 32 *cartuchos. Supondo que a cada salva de tiros todos os soldados de cada lado atiraram exatamente uma vez, determine o número mínimo de cartuchos com que cada tropa iniciou a exibição.*

4.1.2 Um Exemplo Astronômico

Desta vez o problema trata de tempos e não de restos:

> Três satélites passarão sobre o Rio esta noite. O primeiro à 1 hora da madrugada, o segundo às 4 horas e o terceiro às 8 horas da manhã. Cada satélite tem um período diferente. O primeiro leva 13 horas para completar uma volta em torno da Terra, o segundo 15 horas e o terceiro 19 horas. Determine quantas horas decorrerão, a partir da meia-noite, até que os três satélites passem ao mesmo tempo sobre o Rio.

Podemos formular o problema de maneira muito semelhante à que adotamos na seção anterior, basta lembrar nossa interpretação do módulo como o período de um movimento que se repete a intervalos regulares. Neste caso, o movimento é o dos satélites que giram em torno da Terra.

Chamaremos de x o número de horas, contadas a partir da meia-noite de hoje, quando os três satélites passarão juntos sobre o Rio. O primeiro satélite passa sobre o Rio a cada 13 horas, a contar da 1 da madrugada. Logo precisamos ter que $x = 1 + 13n_1$, para algum inteiro positivo n_1, que representa o número de voltas que o satélite 1 tem que dar em torno da Terra antes que passe junto com os dois outros satélites.

As equações correspondentes aos outros dois satélites são

$$x = 4 + 15n_2 \quad \text{e} \quad x = 8 + 19n_3;$$

onde n_2 e n_3 representam o número de voltas que os satélites 2 e 3 darão antes dos três passarem juntos.

Como fizemos para o problema anterior, podemos reformular estas equações em termos de congruências, o que nos dá

$$\begin{aligned} x &\equiv 1 \pmod{13}, \\ x &\equiv 4 \pmod{15}, \\ x &\equiv 8 \pmod{19}. \end{aligned} \tag{4.1.1}$$

Desta vez temos três equações, ao contrário das duas do problema anterior, mas não vamos nos deixar intimidar. Já que o método

que desenvolvemos só permite resolver duas equações de cada vez, começaremos com as duas últimas. Tomando a última *equação* e substituindo-a na penúltima *congruência*, obtemos

$$8 + 19n_3 \equiv 4 \pmod{15}; \text{ que equivale a } 19n_3 \equiv -4 \pmod{15}.$$

Como $19 \equiv 4 \pmod{15}$, isto nos dá

$$4n_3 \equiv -4 \pmod{15}.$$

Como 4 é inversível módulo 15 pelo teorema 3, podemos cancelá-lo, de modo que

$$n_3 \equiv -1 \equiv 14 \pmod{15}.$$

Assim, $n_3 = 14 + 15n_4$, para algum inteiro positivo n_4. Mas, segundo a terceira equação, $x = 8 + 19n_3$. Combinando estas duas expressões

$$x = 8 + 19(14 + 15n_4) = 274 + 285n_4.$$

O que isto representa? Certamente não a solução do problema, já que sequer usamos as condições impostas pelo primeiro satélite. Entretanto, como é fácil verificar usando congruências,

$$x = 274 + 285n_4$$

nos dá uma solução das duas últimas equações.Isto significa que esta família de soluções deve corresponder aos tempos nos quais os satélites 2 e 3 passam juntos sobre o Rio.

E quanto ao satélite 1? Para incluir na solução a informação referente ao primeiro satélite, basta encontrar as soluções da forma $x = 274 + 285n_4$ (isto é, as soluções comuns aos satélites 2 e 3) que, além disso, satisfazem a congruência $x \equiv 1 \pmod{13}$, relativa ao primeiro satélite. Efetuando a substituição,

$$274 + 285n_4 \equiv 1 \pmod{13};$$

que depois da redução módulo 13 nos dá

$$1 + 12n_4 \equiv 1 \pmod{13}.$$

Logo $12n_4 \equiv 0 \pmod{13}$ e, como 12 é inversível módulo 13, concluímos que $n_4 = 13n_5$. Desta forma, a solução final será

$$x = 274 + 285n_4 = 274 + 285(13n_5) = 274 + 3705n_5,$$

como é fácil verificar substituindo esta fórmula para x nas congruências (4.1.1).

Resta-nos explicitar o que esta solução nos diz sobre os satélites. Em primeiro lugar, como é fácil verificar, 274 é o menor inteiro positivo que satisfaz as congruências (4.1.1). Portanto, os satélites passam juntos sobre o céu do Rio pela primeira vez 274 horas depois da meia-noite de hoje. Isto equivale a 11 dias e 10 horas. Mas isto não é tudo. Afinal, não importa qual seja o valor de n_5, a fórmula $274 + 3\,705n_5$ nos dá uma solução do problema. Portanto, depois de passar juntos uma vez sobre o Rio 274 horas depois da zero hora de hoje, os satélites passarão juntos novamente a cada 3 705 horas; isto é, a cada 154 dias e 9 horas.

Na próxima seção faremos uma análise detalhada do método acima. Observe que nossa estratégia consistiu em dividir a solução do sistema (4.1.1) de 3 equações em duas etapas. Primeiro achamos uma solução comum às duas últimas congruências, que foi $x = 274 + 285n_4$. Em seguida, buscamos as soluções comuns às duas últimas congruências que também satisfazem à primeira. Como $x = 274 + 285n_4$ corresponde à congruência,

$$x \equiv 274 \pmod{285},$$

substituí-la na primeira congruência equivale a resolver o sistema

$$\begin{aligned} x &\equiv 1 \pmod{13}, \\ x &\equiv 274 \pmod{285}. \end{aligned}$$

Uma outra maneira de expressar isto consiste em dizer que a solução de um sistema de muitas equações é obtida através da solução de vários sistemas de duas equações cada. Por isso, na seção 3 é suficiente analisar o algoritmo correspondente à solução de um sistema de duas equações.

Nosso próximo exercício vem do banco de questões da OBMEP-2007 (p. 76).

Exercício 39. *O número 119 tem a seguinte propriedade:*

- *a divisão por 2 deixa resto 1;*
- *a divisão por 3 deixa resto 2;*
- *a divisão por 4 deixa resto 3;*

- *a divisão por 5 deixa resto 4;*
- *a divisão por 6 deixa resto 5.*

Quantos inteiros positivos menores que 2007 satisfazem essa propriedade?

Exercício 40. *Um velho problema chinês:*

> *Três fazendeiros cultivavam juntos todo o seu arroz e o dividiam igualmente entre si no tempo da colheita. Um certo ano cada um deles foi a um mercado diferente vender o seu arroz. Cada um destes mercados só comprava arroz em múltiplos de um peso padrão, que diferia em cada um dos mercados. O primeiro fazendeiro vendeu o seu arroz em um mercado onde o peso padrão era* 87 *kg. Ele vendeu tudo o que podia e voltou para casa com* 18 *kg de arroz. O segundo fazendeiro vendeu todo o arroz que podia em um mercado cujo peso padrão era de* 170 *kg e voltou para casa com* 58 *kg. O terceiro fazendeiro vendeu todo o arroz que podia em um mercado cujo peso padrão era de* 143 *kg e voltou (ao mesmo tempo que os outros dois) com* 40 *kg. Qual a quantidade mínima de arroz que eles podem ter cultivado, no total?*

4.2 O Teorema Chinês do Resto

O procedimento de substituição que utilizamos nas seções anteriores para resolver sistemas de congruências é conhecido como *algoritmo chinês do resto*, porque um dos primeiros lugares em que

aparece é o livro *Manual de aritmética do mestre Sun*, escrito entre 287 d.C. e 473 d.C. Entretanto, o mesmo resultado é mencionado na *Aritmética* de Nicômaco de Gerasa, escrita por volta de 100 d.C. O teorema desta seção apenas sistematiza o resultado final do método utilizado nos problemas das seções anteriores.

Considere o sistema

$$\begin{aligned} x &\equiv a \pmod{m}, \\ x &\equiv b \pmod{n}, \end{aligned} \tag{4.2.1}$$

onde m e n são inteiros positivos distintos e digamos que o número inteiro x_0 é uma solução desta congruência. Isto significa que x_0 satisfaz a ambas as congruências:

$$\begin{aligned} x_0 &\equiv a \pmod{m}, \\ x_0 &\equiv b \pmod{n}. \end{aligned}$$

Como os módulos são diferentes, só podemos combinar as duas congruências se convertermos uma delas em uma igualdade de inteiros. Fazendo isto com a primeira equação, verificamos que

$$x_0 = a + m \cdot k, \text{ onde } k \text{ é um inteiro qualquer,} \tag{4.2.2}$$

de forma que podemos concluir que

$$a + mk \equiv b \pmod{n},$$

ou ainda

$$mk \equiv (b - a) \pmod{n}. \tag{4.2.3}$$

Supondo que m e n sejam primos entre si, concluímos pelo teorema 3 que m é inversível módulo n como vimos no teorema 4.2 da página 113. Digamos que m' é o inverso de m módulo n. Multiplicando (4.2.3) por m', obtemos

$$k \equiv m'(b-a) \pmod{n}.$$

Em outras palavras,

$$k = m'(b-a) + n \cdot t \quad \text{para algum inteiro} \quad \ell.$$

Substituindo esta expressão para k em (4.2.2), vemos que

$$x_0 = a + m(m'(b-a) + n \cdot t).$$

Resumindo, provamos que se x_0 é uma solução de (4.2.1), então

$$x_0 = a + m \cdot (m' \cdot (b-a) + n \cdot t). \tag{4.2.4}$$

Mas é fácil ver que, qualquer que seja o inteiro t, uma expressão da forma $a + m(m'(b-a) + n \cdot t)$ tem que ser solução do sistema (4.2.1). Para começo de conversa, $a+m(m'(b-a)+n\cdot t)$ é claramente congruente a a módulo m. Por outro lado,

$$a + m \cdot (m' \cdot (b-a) + n \cdot t) \equiv a + m \cdot m' \cdot (b-a) \pmod{n}.$$

Como, $mm' \equiv 1 \pmod{n}$ por construção, então

$$a + m \cdot (m' \cdot (b-a) + n \cdot t) \equiv a + 1 \cdot (b-a) \equiv b \pmod{n};$$

comprovando que $a+m\cdot(m'\cdot(b-a)+n\cdot t)$ é mesmo uma solução do sistema (4.2.1). Podemos resumir o que fizemos no seguinte teorema.

Teorema Chinês do Resto. *Sejam m e n inteiros positivos primos entre si. Se a e b são inteiros quaisquer, então o sistema*

$$\begin{aligned} x &\equiv a \pmod{m},\\ x &\equiv b \pmod{n}, \end{aligned}$$

sempre tem solução e qualquer uma de suas soluções pode ser escrita na forma

$$a+m\cdot(m'\cdot(b-a)+n\cdot t),$$

onde t é um inteiro qualquer e m' é o inverso de m módulo n.

Cuidado para não se confundir e achar que $mm'=1$, já que m e m' são inversos um do outro. De fato eles são inversos, mas *somente módulo n*, de modo que a relação correta é $mm'\equiv 1 \pmod{n}$; que não simplifica a fórmula de nenhuma maneira significativa.

4.2.1 Quando os Módulos Não são Primos Entre Si

Apesar de termos obtido uma fórmula exata para a solução de sistemas de duas congruências, isto foi feito ao preço de uma hipótese bastante forte, a de que os módulos são primos entre si. Será que a fórmula continua verdadeira mesmo se esta hipótese não se verifica?

Se você reler o argumento usado para provar a fórmula verá que precisamos que os módulos fossem primos entre si em apenas um ponto: para inverter m na congruência $mk\equiv(b-a) \pmod{n}$ e assim

determinar o valor de k. Isto significa que a estratégia usada acima não funcionaria se m e n não fossem primos entre si. Mas será que não há outra estratégia possível neste caso? A resposta é sim... e não. Vejamos por quê?

Para isto analisaremos dois exemplos muito semelhantes. O primeiro deles é

$$\begin{aligned} x &\equiv 3 \pmod 4, \\ x &\equiv 1 \pmod 6, \end{aligned}$$

e o segundo é

$$\begin{aligned} x &\equiv 2 \pmod 4, \\ x &\equiv 1 \pmod 6. \end{aligned}$$

Note que a única diferença entre eles está no coeficiente à direita da primeira congruência que, no primeiro exemplo é 3 e no segundo é 2. Procederemos exatamente como antes. Portanto, começamos por tirar o valor de x da segunda congruência, que nos dá

$$x = 1 + 6y \quad \text{para algum inteiro} \quad y. \tag{4.2.5}$$

Substituindo isto na primeira, obtemos no primeiro exemplo

$$6y \equiv 2 \pmod 4; \tag{4.2.6}$$

e no segundo

$$6y \equiv 1 \pmod 4. \tag{4.2.7}$$

Chegados a este ponto, não podemos prosseguir, porque 6 e 4 têm 2 como fator comum, de modo que 6 não é inversível módulo 4. Contudo, convertendo (4.2.6) para uma igualdade de inteiros, vemos que

$$6y = 2 + 4z, \quad \text{para algum inteiro} \quad z.$$

Acontece que 2 divide cada uma das parcelas desta equação. Efetuando a divisão, obtemos

$$3y = 1 + 2z.$$

Convertendo esta igualdade em uma congruência, ficamos com

$$3y \equiv 1 \pmod 2;$$

que, como $3 \equiv 1 \pmod 2$, nos dá

$$y \equiv 1 \pmod 2;$$

isto é

$$y = 1 + 2t \quad \text{para algum inteiro} \quad t.$$

Substituindo em (4.2.5),

$$x = 1 + 6(1 + 2t) = 7 + 12t,$$

que é a solução do sistema, como podemos facilmente verificar por substituição.

Passando agora ao outro sistema, precisamos resolver a congruên-

cia (4.2.7). Convertendo-a em uma igualdade de inteiros, temos

$$6y = 1 + 4z, \quad \text{para algum inteiro} \quad z.$$

Contudo, desta vez o divisor comum dos três coeficientes da equação é 1. Rearrumando a equação anterior, obtemos

$$6y - 4z = 1$$

que, como 2 divide 6 e 4, pode ser reescrita na forma

$$2(3y - 2z) = 1. \tag{4.2.8}$$

Entretanto, se existissem números inteiros y e z que satisfizessem esta equação, teríamos que 1 é múltiplo de 2; o que é evidentemente falso. Mas (4.2.8) é consequência de (4.2.7), de modo que esta última também não pode ter solução!

Resumindo, estes exemplos nos mostram que, quando os módulos *não* são primos entre si, o sistema pode ou não ter solução, dependendo dos coeficientes constantes que aparecem nas congruências. Será que podemos prever isto só de olhar para os coeficientes? A resposta é sim e é enunciada abaixo. Provar que está correta fica como desafio para você.

Desafio 4. *Considere o sistema de congruências*

$$\begin{aligned} x &\equiv a \pmod{m}, \\ x &\equiv b \pmod{n}. \end{aligned}$$

Suponha que o máximo divisor comum entre m e n é d. Aplique o

procedimento de substituição do algoritmo chinês a este sistema para mostrar que:

(a) se d divide $b-a$ então o sistema tem solução;

(b) se d "não" *divide $b-a$ então o sistema* "não" *tem solução.*

Capítulo 5

Potências

Neste capítulo veremos como calcular os restos de potências usando aritmética modular. Lembre-se que já fizemos um pouco disto quando calculamos as potências de 10 módulo 3, módulo 7 e módulo 11 ao tratar dos critérios de divisibilidade na seção 2.3 do capítulo 2.

5.1 Restos de Potências

Uma aplicação importante das congruências é ao cálculo de restos da divisão de uma potência por um número qualquer. Começaremos com alguns exemplos simples.

5.1.1 Minhas Primeiras Potências Modulares

Suponhamos que queremos calcular o resto da divisão de 10^{135} por 7. Vimos na página 70 que $10^6 \equiv 1 \pmod 7$. Dividindo 135

por 6 temos $135 = 6 \cdot 22 + 3$. Temos então as seguintes congruências módulo 7:

$$10^{135} \equiv (10^6)^{22} \cdot 10^3 \equiv (1)^{22} \cdot 10^3 \equiv 6 \pmod 7.$$

Logo, $10^{135} \equiv 6 \pmod 7$. Como $0 \leq 6 < 7$, podemos concluir que o resto da divisão de 10^{135} por 7 é 6.

Exercício 41. *Calcule o resto da divisão por* 7 *das potências* 10^{65} *e* 3^{78}.

Outro exemplo, mais exagerado. Qual o resto da divisão de $2^{124\,512}$ por 31? Calculando as potências de 2 módulo 31, vemos que

$$\begin{aligned} 2^2 &\equiv 4 \pmod{31}, \\ 2^3 &\equiv 8 \pmod{31}, \\ 2^4 &\equiv 16 \pmod{31}, \\ 2^5 &\equiv 32 \equiv 1 \pmod{31}. \end{aligned}$$

De modo semelhante ao que ocorreu com as potências de 10 módulo 7, somos capazes de descobrir uma potência de 2 que dá 1 módulo 31. Procederemos como no exemplo anterior, só que desta vez usaremos a congruência $2^5 \equiv 1 \pmod{31}$ para fazer as simplificações. Dividimos 124 512 por 5, obtemos quociente 4 016 e resto 2. Portanto,

$$2^{124\,512} \equiv 2^{24\,902 \cdot 5 + 2} \equiv (2^5)^{24\,902} \cdot 2^2 \pmod{31}.$$

Como $2^5 \equiv 1 \pmod{31}$, temos

$$2^{124\,512} \equiv (1)^{24\,902} \cdot 2^2 \equiv 4 \pmod{31}.$$

Como $0 \leq 4 < 31$, podemos concluir que $2^{124\,512}$ deixa resto 4 na divisão por 31.

Exercício 42. *Calcule o resto da divisão por* 31 *das potências* $2^{6\,556\,423}$ *e* $2^{7\,987\,668}$.

Para falar a verdade, podemos exagerar ainda mais. Por exemplo, qual o resto da divisão de $2^{11^{98\,765}}$ por 31? Lembre-se que para calcular $2^{11^{98\,765}}$ determinamos primeiro $11^{98\,765}$ e depois elevamos 2 a este expoente. O resultado é um número enorme, com mais de 25 mil algarismos. O primeiro problema que esta questão põe é o de como calcular o quociente e o resto da divisão de $11^{98\,765}$ por 5. A bem da verdade, o problema é como calcular o quociente porque, para o resto, podemos usar congruências. De fato, como $11 \equiv 1 \pmod 5$, então

$$11^{98\,765} \equiv 1^{98\,765} \equiv 1 \pmod 5.$$

Logo, ao dividir $11^{98\,765}$ por 5 obtemos resto 1. Quanto ao quociente, não precisamos sequer saber quanto vale. Para se convencer disso, releia os exemplos que acabamos de fazer. Em ambos, é apenas 1 que elevamos ao quociente. Escrevendo, então,

$$11^{98\,765} = 5 \cdot q + 1,$$

onde q é o tal quociente que não conhecemos, obtemos

$$2^{11^{98\,765}} \equiv 2^{5 \cdot q + 1} \equiv (2^5)^q \cdot 2 \pmod{31}.$$

Como $2^5 \equiv 1 \pmod{31}$,

$$2^{11^{98\,765}} \equiv (1)^q \cdot 2 \equiv 2 \pmod{31};$$

e o resto da divisão de $2^{11^{98\,765}}$ por 31 é 2.

Se você prestou muita atenção às contas, talvez tenha pensado:

> Ele está blefando! A conta só ficou fácil porque 11 deixa resto 1 na divisão por 5 e 1 elevado a 98 765 dá 1. Se em vez de 11 fosse 13, seria muiiiiito mais difícil!

Tudo bem, vejamos o que acontece quando tentamos calcular o resto da divisão de $2^{13^{98\,765}}$ por 31. Neste caso, o ponto crucial é calcular o resto da divisão de $13^{98\,765}$ por 5. Usando congruências,

$$13^{98\,765} \equiv 3^{98\,765} \pmod{5},$$

o que parece sugerir que seu comentário se justifica. Porém, calculando as potências de 3 módulo 5, vemos facilmente que

$$3^4 \equiv 81 \equiv 1 \pmod{5}.$$

Portanto, podemos aplicar a $3^{98\,765}$ o já conhecido argumento, e dividir o expoente da potência por 4. Como o resto da divisão de 98 765 por 4 é 1 e o quociente é 24 691, obtemos

$$3^{98\,765} \equiv 3^{4\cdot 24\,691+1} \equiv 3 \pmod{5}.$$

Logo, $13^{98\,765}$ deixa resto 3 na divisão por 5; isto é, $13^{98\,765} = 5 \cdot q' + 3$

e, mais uma vez, o quociente q' não precisa ser calculado. Assim,

$$2^{13^{98\,765}} \equiv (2^5)^{q'} \cdot 2^3 \equiv 2^3 \equiv 8 \pmod{31};$$

e o resto da divisão de $2^{13^{98\,765}}$ por 31 é 8. Mais difícil foi, mas não "muiiiiito mais difícil!"

Exercício 43. *Calcule o resto da divisão por* 31 *das potências* $2^{14^{45\,231}}$, $2^{15^{498\,766\,543\,335\,231}}$ *e* $64^{3^{9\,876}}$.

5.1.2 Ordem de um Inteiro Modular

Os cálculos com potências feitos acima só foram tão fáceis de executar porque, em cada caso, descobrimos um expoente positivo para o qual uma potência da base dava 1 quando tomada em módulo. Assim,

$$10^6 \equiv 3^6 \equiv 1 \pmod{7}, \text{ ao passo que, } 3^4 \equiv 2^5 \equiv 1 \pmod{31}.$$

Será que isto sempre é possível? Isto é,

> será que, dados dois inteiros positivos $b < n$ sempre existe um inteiro *positivo* k tal que $b^k \equiv 1 \pmod{n}$?

Observe que estamos exigindo que k seja *positivo*; sem esta hipótese poderíamos tomar $k = 0$, mas isto em nada nos ajuda em nossos cálculos.

Como dar nome aos conceitos facilita falar sobre eles, vamos introduzir a seguinte terminologia. Se $1 \leq b \leq n-1$ são inteiros, diremos que a *ordem de* b *módulo* n é o menor inteiro positivo k para o qual $b^k \equiv 1 \pmod{n}$. Note que, embora anteriormente apenas falássemos

de uma potência congruente a 1 com expoente positivo, acabamos por introduzir o adjetivo "menor" ao escrever a definição. A razão é que, do contrário, o expoente k não estaria completamente determinado. Por exemplo, já vimos que

$$2^5 \equiv 1 \pmod{31};$$

contudo,

$$2^{10} \equiv (2^5)^2 \equiv 1^2 \equiv 1 \pmod{31},$$

assim como

$$2^{105} \equiv (2^5)^{21} \equiv 1^{21} \equiv 1 \pmod{31}.$$

Na verdade,

$$2^{5k} \equiv (2^5)^k \equiv 1^k \equiv 1 \pmod{31},$$

não importa qual seja o inteiro positivo k. Este exemplo é facilmente generalizável. De fato, se $a^k \equiv 1 \pmod{n}$, então

$$a^{km} \equiv (a^k)^m \equiv 1^m \equiv 1 \pmod{n},$$

para qualquer inteiro $m \geq 1$ que você escolher. Interpretando os cálculos do início da seção usando esta terminologia, podemos dizer que 3 tem ordem 6 módulo 7 e que 2 tem ordem 5 módulo 31. Antes de prosseguir seria bom você fazer alguns exemplos para verificar que entendeu mesmo o conceito de ordem.

Exercício 44. *Calcule a ordem de*

(a) 3 *módulo* 7*;*

(b) 2 *módulo* 11*;*

(c) 5 *módulo* 31*;*

(d) 7 *módulo* 43*.*

Voltando à pergunta, podemos agora reformulá-la da seguinte maneira:

> Será que todo inteiro $1 \leq b \leq n-1$ tem alguma ordem módulo n?

Precisamos experimentar um pouco mais, antes de ensaiar uma conclusão. Revendo os exemplos do início desta seção constatamos que 7 e 31 são primos, mas o que acontece se escolhermos um módulo que não seja primo? Por exemplo, será que existe uma potência de 2 que dá 1 módulo 6? Tentando:

$$\begin{aligned} 2^1 &\equiv 2 \pmod 6, \\ 2^2 &\equiv 4 \pmod 6, \\ 2^3 &\equiv 8 \equiv 2 \pmod 6, \\ 2^4 &\equiv 16 \equiv 4 \pmod 6, \end{aligned}$$

e já deu para ver que os valores das potências de 2 módulo 6 vão se alternar entre 2 e 4. Assim, podemos concluir que nenhuma potência de 2 dá congruente a 1 módulo 6. Aliás, isto é fácil de generalizar, como mostra o próximo exercício.

Exercício 45. *Mostre que se a e n são inteiros positivos pares, então nenhuma potência de a é congruente a* 1 *módulo n.*

Voltando ao exemplo, o que mais *você acha* que podemos concluir dos cálculos acima? Alguém mais ousado talvez ache que isto indica

que potências de inteiros módulo 6 nunca dão 1. Ou, quem sabe, até que potências de inteiros módulo um *número composto* nunca dão 1. A verdade, contudo, é bem mais sutil.

Voltando aos nossos experimentos, porque parar em 2? Por que não tentar também 3? Pois bem, aqui estão as potências de 3 módulo 6:

$$\begin{aligned} 3^1 &\equiv 3 \pmod 6, \\ 3^2 &\equiv 9 \equiv 3 \pmod 6, \\ 3^3 &\equiv 27 \equiv 3 \pmod 6, \\ 3^4 &\equiv 81 \equiv 3 \pmod 6. \end{aligned}$$

Não é que 3 foi ainda pior que 2! Todas as potências positivas de 3 são congruentes a 3. Mas, não desanimemos, tentemos as potências de 4,

$$\begin{aligned} 4^1 &\equiv 4 \pmod 6, \\ 4^2 &\equiv 16 \equiv 4 \pmod 6, \end{aligned}$$

tudo bem, já podemos parar: toda potência de 4 módulo 6 dá 4. Ao que tudo indica, nenhuma potência positiva de um inteiro módulo 6 dá igual a 1 – a não ser que o inteiro seja 1, é claro! Mas, só para tirar a prova, testemos o único inteiro menor que 6 cujas potências ainda não calculamos, o 5. Contudo,

$$5^2 \equiv 25 \equiv 1 \pmod 6,$$

de modo que 5 tem ordem 2 módulo 6.

Surpreso? A bem da verdade, você não devia estar porque este resultado poderia ter sido previsto, desde que você lembrasse do exercício 31. Segundo aquele exercício $n-1$ é seu próprio inverso módulo n. Mas isto significa que

$$(n-1)\cdot(n-1) \equiv 1 \pmod{n},$$

que podemos reescrever como

$$(n-1)^2 \equiv 1 \pmod{n};$$

o que mostra que $n-1$ *sempre* tem ordem *dois* módulo n. E isto vale, não importa qual seja o valor do inteiro $n > 1$. O que vimos no caso $n = 6$ é que os *únicos* inteiros entre 1 e 6 que têm ordem módulo 6 são 1 e $n - 1 = 5$.

O caso do $n - 1$ acena com a possibilidade de haver uma relação entre invertibilidade módulo n e a existência de uma ordem módulo n. Para poder explorar melhor esta relação suponha que b, n e k são inteiros positivos e que

$$b^k \equiv 1 \pmod{n}.$$

Se $k = 1$, então $b \equiv 1 \pmod{n}$ e não há nada a dizer. Por isso podemos supor que $k \geq 2$. Neste caso,

$$b \cdot b^{k-1} \equiv 1 \pmod{n}.$$

Mas isto significa que b^{k-1} funciona como o inverso de b módulo n. Pelo teorema 3 da página 97 isto só é possível se b e n forem primos

entre si. Portanto,

> se $1 \leq b \leq n-1$ tem ordem módulo n então b e n são primos entre si.

Isto explica porque apenas 1 e 5 admitem potências positivas congruentes a um módulo 6 entre todos os inteiros positivos menores que 6, afinal, 2, 3 e 4 têm fatores próprios comuns com 6. Por outro lado, se $p > 1$ é primo então nenhum inteiro $1 \leq b \leq p-1$ tem fator próprio comum com p e, portanto, todos estes inteiros são inversíveis módulo p:

> Será que todos estes números admitem uma ordem módulo p?

A resposta é sim, como veremos na seção 5.2. Por enquanto, vamos determinar a ordem módulo 7 de cada um dos inteiros positivos menores que 7.

Começamos por 2, já que 1 tem obviamente ordem um. Como $2^2 = 4 < 7$, a primeira potência interessante é o cubo, mas

$$2^3 \equiv 8 \equiv 1 \pmod{7};$$

logo, 2 tem ordem 3 módulo 7. Já sabemos que 3 tem ordem 6, por isso passamos ao 4. Porém,

$$4^2 \equiv 16 \equiv 2 \pmod{7}.$$

Como 2 tem ordem 3, vamos precisar elevar 4^2 ao cubo para encontrar 1. Logo,

$$4^6 \equiv 1 \pmod 7.$$

Contudo, isto não impede, em princípio, que uma potência menor de 4 não possa dar igual a 1. Testando as demais potências, vemos que

$$4^3 \equiv 4^2 \cdot 4 \equiv 2 \cdot 4 \equiv 8 \equiv 1 \pmod 7;$$

de modo que a ordem de 4 módulo 7 é 3 e não 6 como o cálculo anterior nos teria feito esperar!

O último número a considerar é 5, porque já vimos que $6 = 7 - 1$ tem que ter ordem 2 módulo 7. Neste caso,

$$\begin{aligned}
5^2 &\equiv 25 \equiv 4 \pmod 7,\\
5^3 &\equiv 5 \cdot 4 \equiv 20 \equiv 6 \pmod 7,\\
5^4 &\equiv 5 \cdot 6 \equiv 30 \equiv 2 \pmod 7,\\
5^5 &\equiv 5 \cdot 2 \equiv 10 \equiv 3 \pmod 7,\\
5^6 &\equiv 5 \cdot 3 \equiv 15 \equiv 1 \pmod 7.
\end{aligned}$$

Portanto, 5 tem ordem 6 módulo 7. Podemos organizar o que descobrimos em uma tabela:

Número	Ordem módulo 7
1	1
2	3
3	6
4	3
5	6
6	2

Exercício 46. *Determine a ordem de cada um dos inteiros* $1 \leq b \leq 10$ *módulo* 11*.*

Exercício 47. *Determine a ordem de cada um dos inteiros* $1 \leq b \leq 11$ *módulo* 12*. Lembre-se que alguns destes inteiros nem sequer admitem uma ordem módulo* 12*. Você pode começar por descobrir quais são e assim nem sequer precisará calcular com eles.*

5.1.3 Mais Exemplos

Já vimos que fica muito fácil calcular potências de um número módulo n quando sua ordem (módulo n) é conhecida. O problema é que nem todo número tem ordem módulo n quando n não é primo. Como proceder neste caso? Por exemplo, como determinar o resto de 6^{35} por 16? Como 6 e 16 têm 2 como fator comum, podemos concluir que 6 não tem ordem módulo 16 e teremos que proceder de alguma outra maneira. Contudo,

$$6^4 \equiv 2^4 \cdot 3^4 \equiv 0 \cdot 3^4 \equiv 0 \pmod{16};$$

de modo que

$$6^{35} \equiv 6^4 \cdot 6^{31} \equiv 0 \pmod{16},$$

e, neste caso, as contas acabaram ficando bastante simples.

Por outro lado, mesmo quando um número tem ordem módulo n, esta pode ser tão grande que fica difícil determiná-la. Este é o caso, por exemplo, da ordem de 3 módulo 31. Já dissemos que, quando p é primo, todo número positivo menor que p tem ordem módulo p: logo 3 tem ordem módulo 31. Mas a ordem é grande e precisamos de muito trabalho para determiná-la. Em casos como este é preferível reduzir o expoente há algo mais fácil de calcular. Digamos, por exemplo, que quiséssemos determinar o resto da divisão de 3^{64} por 31. Calculando os restos das potências de 3 encontramos

$$3^3 \equiv 27 \equiv -4 \pmod{31}.$$

Mas $4 = 2^2$, de modo que

$$3^3 \equiv -2^2 \pmod{31}.$$

É claro que a vantagem de trabalhar com 2 está no fato de já conhecermos a ordem de 2. Usando esta última congruência,

$$3^{64} \equiv (3^3)^{21} \cdot 3 \equiv (-2^2)^{21} \cdot 3 \equiv -(2)^{42} \cdot 3 \pmod{31}.$$

Como $2^5 \equiv 1 \pmod{31}$ e $42 = 8 \cdot 5 + 2$, temos que

$$2^{42} \equiv (2^5)^8 \cdot 2^2 \equiv 4 \pmod{31}.$$

Assim,

$$3^{64} \equiv -(2)^{42} \cdot 3 \equiv -4 \cdot 3 \equiv -12 \pmod{31}.$$

Como $-12 \equiv 19 \pmod{31}$, o resto da divisão de 3^{64} por 31 é 19.

Exercício 48. *Determine a ordem de* 3 *módulo* 31 *e refaça o cálculo do resto de* 3^{64} *por* 31 *usando o resultado obtido. Mas, tenha paciência, a ordem é bem grande.*

Exercício 49. *Calcule o resto da divisão de* $3^{98\,745}$ *por* 43 *procedendo da seguinte maneira:*

(a) calcule a ordem de 6 *módulo* 43*;*

(b) determine uma potência de 3 *que dê congruente a* -6 *módulo* 43*;*

(c) use (a) e (b) para calcular o resto desejado.

5.2 O Teorema de Fermat

Determinar a ordem exata de um dado inteiro módulo n pode ser uma tarefa bastante difícil se n for grande. Felizmente, no caso em que n é primo há um teorema que facilita muito nossa vida.

Teorema de Fermat. *Se p é um primo e a é um inteiro* que não é divisível por p*, então*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Há quem chame este teorema de *Pequeno* Teorema de Fermat. Contudo, levando em conta que este é o resultado mais importante de todo o nosso texto, chamá-lo de *Pequeno* não parece muito apropriado. A demonstração do *Teorema de Fermat* que demos aqui foi descoberta

pelo matemático suíço Leonard Euler no século XVIII e é uma das mais elementares.

Demonstração. Começamos a demonstração do Teorema de Fermat listando os possíveis resíduos módulo p, que são

$$1, 2, 3, \ldots, p-1.$$

Multiplicando cada um destes resíduos por a, temos

$$a \cdot 1, a \cdot 2, a \cdot 3, \ldots, a \cdot (p-1).$$

Digamos que r_1 é o resíduo de $a \cdot 1$, que r_2 é o resíduo de $a \cdot 2$ e assim por diante até r_{p-1}, que será o resíduo de $a \cdot (p-1)$. Vamos calcular o produto

$$r_1 \cdot r_2 \cdots r_{p-1}$$

módulo p de duas maneiras diferentes.

Primeira maneira: levando em conta que

$$\begin{aligned} r_1 &\equiv a \cdot 1 \pmod{p}, \\ r_2 &\equiv a \cdot 2 \pmod{p}, \\ &\vdots \quad \vdots \\ r_{p-1} &\equiv a \cdot (p-1) \pmod{p}; \end{aligned}$$

podemos concluir que

$$r_1 \cdot r_2 \cdot r_3 \cdots r_{p-1} \equiv (a \cdot 1) \cdot (a \cdot 2) \cdot (a \cdot 3) \cdots (a \cdot (p-1)) \pmod{p}.$$

Contudo,

$$(a \cdot 1) \cdot (a \cdot 2) \cdot (a \cdot 3) \cdots (a \cdot (p-1)) = a^{p-1} \cdot (1 \cdot 2 \cdot 3 \cdots (p-1));$$

de forma que

$$r_1 \cdot r_2 \cdot r_3 \cdots r_{p-1} \equiv a^{p-1} \cdot (1 \cdot 2 \cdot 3 \cdots (p-1)) \pmod{p}.$$

Segunda maneira: esta é mais sutil. Começamos observando que não pode haver dois resíduos iguais entre

$$r_1, r_2, r_3, \ldots, r_{p-1}.$$

Para provar isto, suponhamos que $r_k = r_\ell$ para dois inteiros k e ℓ, ambos entre 1 e $p-1$. De acordo com a definição dos resíduos, teríamos que

$$a \cdot k \equiv r_k \equiv r_\ell \equiv a \cdot \ell \pmod{p};$$

isto é,

$$a \cdot k \equiv a \cdot \ell \pmod{p}.$$

Entretanto, como p *não divide* a *e* p *é primo*, estes números não têm fator próprio comum. Mas isto implica que a é inversível módulo p de forma que, pelo teorema 2, podemos cancelá-lo na congruência acima, obtendo

$$k \equiv \ell \pmod{p}.$$

Mas k e ℓ são inteiros positivos menores que p, e só podem ser congruentes se forem iguais. Logo,

$$\text{se } r_k = r_\ell, \text{ então } k = \ell.$$

Isto nos mostra que

$$r_1, r_2, r_3, \ldots, r_{p-1}$$

são $p-1$ resíduos não nulos (pois p não divide a) e diferentes entre si. Acontece que só há $p-1$ resíduos não nulos diferentes módulo p, a saber

$$1, 2, 3, \ldots, p-1;$$

o que nos permite deduzir que a sequência de números

$$r_1, r_2, r_3, \ldots, r_{p-1}$$

é apenas um embaralhamento de

$$1, 2, 3, \ldots, p-1.$$

Em particular,

$$r_1 \cdot r_2 \cdot r_3 \cdots r_{p-1} = 1 \cdot 2 \cdot 3 \cdots (p-1).$$

CONCLUSÃO GERAL: Da primeira maneira de calcular o produto dos resíduos temos que

$$r_1 \cdot r_2 \cdot r_3 \cdots r_{p-1} \equiv a^{p-1} \cdot (1 \cdot 2 \cdot 3 \cdots (p-1)) \pmod{p}$$

e da segunda que

$$r_1 \cdot r_2 \cdot r_3 \cdots r_{p-1} = 1 \cdot 2 \cdot 3 \cdots (p-1).$$

Portanto,

$$a^{p-1} \cdot (1 \cdot 2 \cdot 3 \cdots (p-1)) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}.$$

Contudo, $1 \cdot 2 \cdot 3 \cdots (p-1)$ é produto de inversíveis módulo p logo é, ele próprio, inversível módulo p. Com isto podemos cancelá-lo dos dois lados da congruência, o que nos dá

$$a^{p-1} \equiv 1 \pmod{p};$$

que é o que precisávamos mostrar. □

Pelo Teorema de Fermat, se p é primo, então todo elemento de resíduo não nulo módulo p tem uma potência congruente a 1. Em particular, qualquer um destes elementos admite uma ordem módulo p. Note, contudo, que *não* podemos afirmar que, como

$$b^{p-1} \equiv 1 \pmod{p} \text{ se } b \not\equiv 0 \pmod{p},$$

então b tem ordem $p-1$ módulo p. Para começar, 1 tem ordem 1 módulo p qualquer que seja o p que você escolher. Além disso, como

$$(p-1) \equiv -1 \pmod{p},$$

temos que

$$(p-1)^2 \equiv (-1)^2 \equiv 1 \pmod{p};$$

donde podemos concluir que $p-1$ tem ordem dois qualquer que seja o p. Se estes exemplos ainda não lhe satisfazem, que tal este: de acordo

com o Teorema de Fermat,

$$2^{30} \equiv 1 \pmod{31};$$

contudo, como vimos na seção 5.1, a ordem de 2 módulo 31 é 5, e não 30. Para terminar de uma maneira mais positiva, aqui está um desafio que mostra como a ordem de um inteiro módulo p está relacionada ao expoente $p-1$ do Teorema de Fermat.

Desafio 5. *Seja p um primo positivo e b um inteiro que não é divisível por p. Digamos que k é a ordem de b módulo p.*

(a) Explique porque $k \leq p-1$.

(b) Seja r o resto da divisão de $p-1$ por k. Mostre que, como

$$a^{p-1} \equiv a^k \equiv 1 \pmod{p},$$

então $a^r \equiv 1 \pmod{p}$.

(c) Lembrando que $0 \leq r \leq k-1$, mostre que $r = 0$.

(d) Conclua que a ordem de b é um divisor de $p-1$.

5.3 Potências

Agora que temos o Teorema de Fermat, podemos usá-lo para simplificar o cálculo de restos de potências.

5.3.1 Módulos Primos

Começamos reprisando o cálculo do resto da divisão de 3^{64} por 31, que já fizemos na página 133. Só que, desta vez, usaremos o Teorema de Fermat. Como

$$3^{30} \equiv 1 \pmod{31},$$

pelo Teorema de Fermat e $64 = 2 \cdot 30 + 4$, então

$$3^{64} \equiv (3^{30})^2 \cdot 3^4 \equiv 1 \cdot 81 \equiv 19 \pmod{31},$$

confirmando o resultado de nossos cálculos anteriores de uma maneira bem mais simples.

Exercício 50. *Calcule o resto da divisão de* $3^{98\,745}$ *por* 43 *usando o Teorema de Fermat.*

Vejamos outro exemplo, um pouco mais sutil. Digamos que queremos calcular o resto da divisão de $3^{1\,034^2}$ por 1 033. A primeira coisa a fazer é verificar que 1 033 é primo, pois *só podemos aplicar o Teorema de Fermat quando o módulo é primo.* Como

$$\sqrt{1\,033} = 32,14\ldots$$

só precisamos mostrar que 1 033 não é divisível pelos primos menores que 32 para ter certeza que é primo. Estes primos são,

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31,$$

e é fácil verificar que nenhum deles divide 1 033. Agora que temos

certeza que 1 033 é primo, podemos afirmar que

$$3^{1\,032} \equiv 1 \pmod{1\,033}$$

pelo Teorema de Fermat. Em seguida precisamos dividir $1\,034^2$ por 1 032. Dividir é maneira de dizer, o que precisamos mesmo é do resto da divisão de $1\,034^2$ por 1 032; o quociente não importa porque, por Fermat, vai ser o expoente de 1. Com isso, podemos usar congruências para calcular o resto. Como $1\,034 \equiv 2 \pmod{1\,032}$, temos que

$$1\,034^2 \equiv 2^2 \equiv 4 \pmod{1\,032}.$$

Logo o resto da divisão de $1\,034^2$ por 1 032 é 4. Como não conhecemos o quociente, vamos chamá-lo de q. Mas, seja lá qual for o valor de q, temos que

$$1\,034^2 = 1\,032 \cdot q + 4;$$

donde

$$3^{1\,034^2} \equiv 3^{1\,032 \cdot q + 4} \equiv (3^{1\,032})^q \cdot 3^4 \pmod{1\,033}$$

aplicando o Teorema de Fermat, concluímos que

$$3^{1\,034^2} \equiv 1 \cdot 81 \pmod{1\,033};$$

de forma que $3^{1\,034^2}$ deixa resto 81 na divisão por 1 033.

Exercício 51. *Calcule o resto da divisão de* $2^{41\,048^2}$ *por* 41 047.

Exercício 52. *Calcule o resto da divisão de* $3^{19!}$ *por* 307.

Exercício 53. *Calcule o resto da divisão de*

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \text{ por } p,$$

sabendo-se apenas que $p > 2$ *é* primo.

Desafio 6. *Determine todos os primos positivos* p *para os quais a equação*

$$2x + x^p + x^{p!} \equiv 1 \pmod{p},$$

tem solução $x \not\equiv 0 \pmod{p}$.

5.3.2 Módulos Compostos

Aparentemente a única coisa que teríamos a dizer sobre a aplicação do Teorema de Fermat ao cálculo de potências quando o módulo é composto seria *isto não é possível*! O que faria desta a seção mais curta da apostila. Contudo, podemos combinar o Teorema de Fermat com o Algoritmo Chinês do Resto e, com isso, simplificar drasticamente as contas dos cálculos com potências em alguns casos especiais, mesmo quando o módulo é composto.

Vejamos um exemplo numérico. Digamos que queremos calcular o resto da divisão de $2^{6\,754}$ por 1 155. Fatorando 1 155 vemos que é igual a $3 \cdot 5 \cdot 7 \cdot 11$. Aplicando o Teorema de Fermat a cada um destes primos, obtemos

$$\begin{aligned} 2^2 &\equiv 1 \pmod{3}, \\ 2^4 &\equiv 1 \pmod{5}, \\ 2^6 &\equiv 1 \pmod{7}, \\ 2^{10} &\equiv 1 \pmod{11}. \end{aligned}$$

A seguir dividimos 6 754 por $p-1$, para cada um dos fatores primos p de 1 155,

$$\begin{aligned}
6\,754 &= 2 \cdot 3\,377,\\
6\,754 &= 4 \cdot 1\,688 + 2,\\
6\,754 &= 6 \cdot 1\,125 + 4,\\
6\,754 &= 10 \cdot 675 + 4.
\end{aligned}$$

Substituindo isto nas congruências,

$$\begin{aligned}
2^{6\,754} &\equiv (2^2)^{3\,377} \pmod 3,\\
2^{6\,754} &\equiv (2^4)^{1\,688} \cdot 2^2 \pmod 5,\\
2^{6\,754} &\equiv (2^6)^{1\,125} \cdot 2^4 \pmod 7,\\
2^{6\,754} &\equiv (2^{10})^{675} \cdot 2^4 \pmod{11}.
\end{aligned}$$

Mas aplicando o Teorema de Fermat, estas congruências se reduzem a:

$$\begin{aligned}
2^{6\,754} &\equiv 1 \pmod 3,\\
2^{6\,754} &\equiv 2^2 \equiv 4 \pmod 5,\\
2^{6\,754} &\equiv 2^4 \equiv 2 \pmod 7,\\
2^{6\,754} &\equiv 2^4 \equiv 5 \pmod{11},
\end{aligned}$$

logo,

$$\begin{aligned} 2^{6\,754} &\equiv 1 \pmod 3, \\ 2^{6\,754} &\equiv 4 \pmod 5, \\ 2^{6\,754} &\equiv 2 \pmod 7, \\ 2^{6\,754} &\equiv 5 \pmod{11}. \end{aligned}$$

Precisamos, portanto resolver o sistema

$$\begin{aligned} x &\equiv 1 \pmod 3, \\ x &\equiv 4 \pmod 5, \\ x &\equiv 2 \pmod 7, \\ x &\equiv 5 \pmod{11}. \end{aligned}$$

Usando o algoritmo chinês, que foi descrito na seção 4.2 do Capítulo 4, temos que $x = 1 + 3y$. Substituindo isto na segunda equação, obtemos

$$1 + 3y \equiv 4 \pmod 5, \quad \text{isto é,} \quad y \equiv 1 \pmod 5,$$

já que 3 é inversível módulo 5 e pode ser cancelado nos dois membros da equação. Assim $x = 4+15z$. Substituindo isto na terceira equação e resolvendo-a obtemos $z \equiv 5 \pmod 7$; ou seja $x = 79 + 105t$. Finalmente substituindo isto na última equação, teremos $t \equiv 6 \pmod{11}$, o que dá $x = 709 + 1\,155u$. Concluímos que $2^{6\,754} \equiv 709 \pmod{1\,155}$. Para realmente apreciar as vantagens deste método, experimente refazer os cálculos sem usá-lo.

Exercício 54. *Calcule o resto da divisão de*

(a) 2^{495} *por* $15\,841$*;*

(b) de $2^{41\,045}$ *por* $41\,041$*;*

(c) de 2^{77} *por* $2\,465$.

Capítulo 6

Criptografia RSA

É chegada a hora de reunir tudo o que fizemos anteriormente, na descrição do método RSA. A descrição do RSA propriamente dita consiste em explicitar as receitas usadas para codificação e decodificação de mensagens. Isto é fácil de fazer, uma vez que depende apenas do cálculo dos resíduos de potências, assunto de que já tratamos com detalhes anteriormente. Lembre-se, contudo, que decodificar significa passar da mensagem codificada à mensagem original. Por isso, nossa missão neste capítulo não se resume a descrever as receitas de codificação e decodificação; precisamos também verificar que *se aplicadas nesta ordem* voltamos a obter à mensagem original. Afinal, se isto não fosse verdade, de que serviria este método de criptografia?

6.1 Pré-codificação

Como dissemos acima, o que fazemos para codificar uma mensagem no RSA é calcular sua potência módulo n relativamente a um expoente especialmente escolhido. Entretanto, para que isto seja viável, a mensagem deve ser um número inteiro. Mas não é isto o que ocorre em geral: a maior parte das mensagens é um texto. Por isso, a primeira coisa a fazer, se desejamos usar o método RSA, é inventar uma maneira de converter a mensagem em uma sequência de números.

Suponhamos, para simplificar, que a mensagem original é um texto onde não há números, apenas palavras, e no qual todas as letras são maiúsculas. Portanto, em última análise a mensagem é constituída pelas letras que formam as palavras e pelos espaços entre palavras. Chamaremos esta primeira etapa de *pré-codificação*, para distingui-la do processo de codificação propriamente dito.

Na pré-codificação convertemos as letras em números usando a seguinte tabela de conversão:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

O espaço entre duas palavras será substituído pelo número 99, quando for feita a conversão. Por exemplo, a frase *AMO A OBMEP* é con-

vertida no número

$$1022249910992411221425.$$

Observe que precisamos fazer cada letra corresponder a um número de, pelo menos, *dois* algarismos para evitar ambiguidades. Se fizéssemos A corresponder ao número 1, B ao 2, e assim por diante, não teríamos como saber se 12 representa AB ou L, já que esta última é a décima segunda letra do alfabeto.

Antes de continuar precisamos determinar os parâmetros do sistema RSA que vamos usar. Estes *parâmetros* são dois primos *distintos*, que vamos denotar por p e q, e *cujo resto na divisão por* 6 *tem que ser* 5. A razão para esta estranha condição será explicada na seção 6.3.

Em seguida, ponha $n = pq$. A última fase do processo de pré-codificação consiste em quebrar em blocos o longo número produzido anteriormente. Estes blocos devem ser números *menores* que n. Por exemplo, se escolhermos $p = 17$ e $q = 23$, então $n = 391$. Neste caso, a mensagem, cuja conversão numérica foi feita acima, pode ser quebrada nos seguintes blocos:

$$102 - 224 - 99 - 109 - 92 - 41 - 122 - 142 - 5.$$

A maneira de escolher os blocos não é única e os blocos não precisam sequer ter o mesmo tamanho. Contudo, certos cuidados devem ser tomados. Por exemplo, não é permitido escolher um bloco que comece por 0 porque isto traria problemas na hora de decodificar, já que, por exemplo, não temos como distinguir o bloco 071 do bloco 71.

Observe que os blocos em que quebramos a mensagem *não* correspondem a nenhuma unidade linguística, seja ela palavra, letra ou qualquer outra. Isto é muito bom, porque torna a decodificação por contagem de frequência essencialmente impossível.

6.2 Codificando e Decodificando uma Mensagem

Encerramos assim a pré-codificação, e podemos passar à etapa de *codificação* propriamente dita. Para codificar a mensagem precisamos apenas de n, que é o produto dos primos. Diremos que n é a *chave de codificação* do sistema RSA que estamos usando. *Esta chave pode ser tornada pública; isto é, podemos enviá-la a qualquer um que queira nos mandar uma mensagem, sem preocupação de mantê-la secreta.* Por isso a chave de codificação também é conhecida como *chave pública* do sistema.

Supondo que já submetemos a mensagem à pré-codificação, temos uma sequência de números que, como na seção anterior, chamaremos de *blocos*. Codificaremos cada bloco separadamente. A mensagem codificada será a sequência dos blocos codificados. Isto é muito importante porque depois de codificados os blocos *não podem* mais ser reunidos de modo a formar um longo número. Se isto for feito, será impossível decodificar a mensagem, como ficará claro na seção 6.3, na qual discutimos o funcionamento do RSA.

Exercício 55. *Usando a tabela de primos da página 180, construa uma chave pública para você utilizar na codificação de mensagens RSA para seus colegas.*

6.2.1 Codificação

Digamos, então, que a chave de codificação é n. Como faremos para codificar um bloco b? Lembre-se que b é um inteiro positivo menor que n. Vamos denotar o bloco codificado por $\mathbf{C}(b)$. A receita para calcular $\mathbf{C}(b)$ é a seguinte:

$$\mathbf{C}(b) = \quad \text{resto da divisão de } \ b^3 \ \text{ por } \quad n.$$

Observe que, em termos de aritmética modular, $\mathbf{C}(b)$ é o resíduo de b^3 módulo n. Na verdade, como $b > 0$, o número $\mathbf{C}(b)$ é mesmo o *resto* da divisão de b^3 por n.

Vejamos o que aconteceria no exemplo que estamos considerando. Temos $n = 391$. Assim, o bloco 102 da mensagem anterior deve ser codificado como o resto da divisão de 102^3 por 391. Fazendo as contas, obtemos $\mathbf{C}(102) = 34$. É claro que, para simplificar nosso trabalho, executamos a conta calculando o resíduo de 102^3 módulo 391:

$$102^3 \equiv 102^2 \cdot 102 \equiv 238 \cdot 102 \equiv 24276 \equiv 34 \pmod{391}.$$

Codificando toda a mensagem passo a passo, temos o seguinte:

$$\begin{aligned}
224^3 &\equiv 224^2 \cdot 224 \equiv 128 \cdot 224 \equiv 129 \pmod{391};\\
99^3 &\equiv 99^2 \cdot 99 \equiv 26 \cdot 99 \equiv 228 \pmod{391};\\
109^3 &\equiv 109^2 \cdot 109 \equiv 151 \cdot 109 \equiv 37 \pmod{391};\\
92^3 &\equiv 92^2 \cdot 92 \equiv 253 \cdot 92 \equiv 207 \pmod{391};
\end{aligned}$$

$$41^3 \equiv 41^2 \cdot 41 \equiv 117 \cdot 41 \equiv 105 \pmod{391};$$
$$122^3 \equiv 122^2 \cdot 122 \equiv 26 \cdot 122 \equiv 44 \pmod{391};$$
$$142^3 \equiv 142^2 \cdot 142 \equiv 223 \cdot 142 \equiv 386 \pmod{391};$$
$$5^3 \equiv 5^2 \cdot 5 \equiv 25 \cdot 5 \equiv 125 \pmod{391}.$$

Reunindo todos os blocos, descobrimos que a mensagem codificada é

$$34 - 129 - 228 - 37 - 207 - 105 - 44 - 386 - 125.$$

Exercício 56. *Use a chave pública que você construiu no exercício 55 para codificar seu nome. Escreva a chave e a mensagem em um papel. Os papéis deverão ser reunidos, embaralhados e sorteados entre os alunos para o próximo exercício.*

6.2.2 Decodificação

Vejamos como fazer para decodificar um bloco da mensagem codificada. Em outras palavras, queremos saber qual é a receita que nos permite, de posse de um bloco codificado e da chave pública, reconstruir o bloco original, antes da codificação.

A informação que precisamos para poder decodificar consiste de dois números: n e o inverso $d > 0$ de 3 módulo $(p-1)(q-1)$. Pela definição de inverso isto significa que devemos ter

$$3d \equiv 1 \pmod{(p-1)(q-1)}.$$

A explicação de onde saiu este número misterioso você encontrará na próxima seção. Chamaremos o par (n, d) de *chave de decodificação. Esta chave tem que ser mantida secreta. Quem a descobrir vai poder decodificar qualquer mensagem endereçada a você.*

De posse do par (n, d), como devemos proceder para decodificar uma mensagem? Se a for um bloco codificado, denotaremos por $\mathbf{D}(a)$ o resultado do processo de decodificação do bloco a. A receita para calcular $\mathbf{D}(a)$ é a seguinte:

$$\mathbf{D}(a) = \text{resto da divisão de } \ a^d \ \text{ por } \ n.$$

Em termos de aritmética modular, $\mathbf{D}(a)$ é o resíduo de a^d módulo n. Como no caso da codificação, o bloco a é positivo e este resíduo coincide com o resto da divisão de b^d por n.

Note que, ao chamarmos o processo acima de *decodificação*, estamos assumindo um compromisso importante, que é o de mostrar que ao decodificar um bloco codificado, obtemos o bloco original. Dizendo de outra maneira, se b é um bloco da mensagem original, só será legítimo chamar o processo acima de decodificação se

$$\mathbf{D}(\mathbf{C}(b)) = b.$$

Não é de forma alguma óbvio que isto é verdade: a demonstração de que esta igualdade realmente é válida é dada em detalhes na seção 6.3.

Alguns comentários são necessários antes de fazermos um exemplo. Em primeiro lugar, é muito fácil calcular d. Como estamos supondo

que p e q deixam resto 5 na divisão por 6, temos que

$$p \equiv 5 \pmod 6 \text{ e } q \equiv 5 \pmod 6.$$

Assim,

$$(p-1)(q-1) \equiv 4 \cdot 4 \equiv 16 \equiv 4 \equiv -2 \pmod 6;$$

donde

$$(p-1)(q-1) = 6 \cdot k - 2,$$

para algum inteiro positivo k. Contudo, como já vimos em (3.4.1), o inverso de 3 módulo $6 \cdot k - 2$ é igual a $4 \cdot k - 1$. Logo, podemos tomar

$$d = 4 \cdot k - 1.$$

No exemplo que vimos considerando $p = 17$ e $q = 23$, de forma que

$$(p-1)(q-1) = 16 \cdot 22 = 352 = 6 \cdot 58 + 4$$

que é igual a

$$(p-1)(q-1) = 6 \cdot 59 - 2.$$

Portanto, neste caso, $k = 59$ e

$$d = 4 \cdot 59 - 1 = 235.$$

Aplicando a receita dada anteriormente ao primeiro bloco da mensagem codificada, temos que $\mathbf{D}(34)$ é igual ao resto da divisão de 34^{235} por $n = 391$.

Efetuar esta conta sem um computador seria totalmente impossível, se não tivéssemos o algoritmo chinês do resto e o Teorema de Fermat. Aplicando o método estudado na seção 5.3 do capítulo 5, calculamos 34^{235} módulo 17 e módulo 23, que são os primos em que n se fatora. Para começo de conversa,

$$\begin{aligned} 34 &\equiv 0 \pmod{17}, \\ 34 &\equiv 11 \pmod{23}. \end{aligned}$$

Assim,

$$34^{235} \equiv 0^{235} \equiv 0 \pmod{17}.$$

Aplicando o Teorema de Fermat à outra congruência,

$$11^{235} \equiv (11^{22})^{10} 11^{15} \equiv 11^{15} \pmod{23}.$$

Mas,

$$11 \equiv -12 \equiv -4 \cdot 3 \pmod{23};$$

de forma que

$$11^{235} \equiv 11^{15} \equiv -4^{15} \cdot 3^{15} \pmod{23}.$$

Contudo,

$$\begin{aligned} 4^{11} &\equiv 1 \pmod{23}, \\ 3^{11} &\equiv 1 \pmod{23}, \end{aligned}$$

de modo que

$$4^{15} \equiv 2^{30} \equiv (2^{11})^2 \cdot 2^8 \equiv 2^8 \equiv 3 \pmod{23},$$
$$3^{15} \equiv 3^{11} \cdot 3^4 \equiv 3^4 \equiv 12 \pmod{23}.$$

Donde podemos concluir que

$$11^{235} \equiv -4^{15} \cdot 3^{15} \equiv -3 \cdot 12 \equiv 10 \pmod{23}.$$

Portanto,

$$34^{235} \equiv 0 \pmod{17},$$
$$34^{235} \equiv 10 \pmod{23}.$$

Isto corresponde ao sistema

$$x \equiv 0 \pmod{17},$$
$$x \equiv 10 \pmod{23},$$

que podemos resolver utilizando o algoritmo chinês do resto. Da segunda congruência, obtemos

$$x = 10 + 23y$$

que, ao ser substituído na primeira congruência, nos dá

$$10 + 23y \equiv 0 \pmod{17}.$$

Assim,

$$6y \equiv 7 \pmod{17}.$$

Mas, 6 tem inverso 3 módulo 17, de forma que

$$y \equiv 3 \cdot 7 \equiv 4 \pmod{17}.$$

Portanto,

$$x = 10 + 23y = 10 + 23 \cdot 4 = 102;$$

como seria de esperar, afinal estamos decodificando 34, que corresponde à codificação do bloco 102.

Exercício 57. *Decodifique os demais blocos da mensagem*

$$34 - 129 - 228 - 37 - 105 - 44 - 386 - 125,$$

usando o procedimento acima.

Exercício 58. *Fatore a chave pública que você recebeu quando fez o exercício 56, calcule d e decodifique a mensagem para saber de quem ela veio.*

6.2.3 Segurança

Antes de prosseguir para a explicação de porque o RSA funciona, é conveniente discutir com um pouco mais de detalhes em que se fundamenta a segurança do RSA. Neste contexto, o termo-chave é *quebrar o código*. Digamos que alguém, que vamos chamar de A, põe uma escuta (também conhecida como um "grampo") na linha que uma empresa usa para transmitir mensagens codificadas a um banco. Se

o código utilizado for o RSA, então A vai ter acesso não apenas às mensagens codificadas que a empresa envia ao banco (obtidas pelo grampo), mas também à chave de codificação n usada pela empresa que, afinal de contas, é pública.

Lembre-se que a chave n é igual ao produto de dois números primos p e q que foram escolhidos pela empresa no momento em que sua implementação do RSA foi feita. Em princípio, A não deveria ter nenhuma dificuldade em decodificar a mensagem. De posse de n, precisaria apenas *fatorá-lo*, descobrir p e q e usá-los para calcular d. Uma vez obtido d, a receita de decodificação explicada em 6.2.2 pode ser aplicada para reconstituir a mensagem original.

Embora tudo isto pareça muito simples *em princípio*, na prática é totalmente *inviável*. A razão está em um problema de natureza tecnológica: não existem computadores rápidos o suficiente, nem algoritmos bons o suficiente, que nos permitam fatorar um número inteiro muito grande que não tenha fatores relativamente pequenos. Lembre-se que, na seção 1.2.5 do capítulo 1 mostramos que o tempo necessário para fatorar um número de uns cem algarismos pelo método usual de tentativa é imenso, e excede, em muito, a idade estimada do universo. Entretanto, a afirmação que acabamos de fazer é muito mais forte:

> não existe nenhum algoritmo conhecido capaz de fatorar inteiros grandes de modo realmente eficiente.

Na verdade, não se sabe nem mesmo se é possível que um tal algoritmo exista!

Mas, o que significa a palavra *grande* neste contexto? Mais precisamente, quão *grande* deve ser a chave n usada no RSA para que,

mesmo tendo interceptado a mensagem codificada pela empresa e conhecendo n, o agente A não seja capaz de achar p e q e, assim, decodificar a mensagem? A resposta é que, atualmente, as implementações comerciais do RSA usam chaves públicas com cerca de 200 algarismos, mas algumas destas implementações chegam a permitir chaves públicas com até 2 467 algarismos.

Durante algum tempo, o RSA Laboratory, que pertence à empresa que detém os direitos do sistema de codificação RSA, lançou desafios, que consistiam de uma possível chave pública de RSA que deveria ser fatorada. A última destas chaves a ser fatorada tem 193 algarismos e corresponde ao produto dos primos

$$1634733645809253848443133883865090859841783670033092312181110852389333100104508151212118167511579$$

e

$$1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571.$$

A fatoração foi finalizada em novembro de 2005 por F. Bahr, M. Boehm, J. Franke e T. Kleinjung no Escritório Federal de Segurança de Informação da Alemanha. Os cálculos utilizaram 80 computadores de 2.2 GHz cada um e, mesmo assim, foram necessários 5 meses para completar as contas! A maior das chaves proposta como desafio tem 617 algarismos e, evidentemente, está longe de ser fatorada. Mais detalhes podem ser encontrados no verbete *RSA numbers* da versão em inglês da *Wikipedia*.

Na prática, isto significa que se a empresa está usando uma implementação do RSA com chave pública de uns 200 algarismos, então A não tem a menor chance de ler a mensagem. Outro detalhe prático importante que segue desta argumentação é que a empresa precisa calcular o valor de d a partir dos valores de p e q: se n for calculado e p e q forem esquecidos, já não temos mais como determinar o valor de n, porque ninguém mais será capaz de fatorar n. Portanto, primeiro escolhem-se p e q, que são usados para calcular d; depois multiplicam-se p e q para determinar n. Uma vez de posse do par (n, d) os valores de p e q podem até ser apagados por medida de segurança.

Uma observação final. Quando usamos congruências para efetuar a codificação do bloco 102 na página 150, dissemos que estávamos usando congruências para "facilitar as contas". Isto não é estritamente verdade, porque em uma aplicação comercial do RSA teríamos que calcular potências de números muito grandes, com módulos maiores ainda, e isto não é viável se não utilizarmos aritmética modular. Em outras palavras, não é mera questão de facilitar nada, os cálculos seriam impossíveis sem aritmética modular. Para convencê-lo disto, aqui vai um exemplo. Comecei escolhendo dois primos

$$p = 1000000000000000000000000000000000000000000000000151$$

e

$$q = 1000000000000000000000000000000000000000000001627354656 91$$

Calculei então o quociente

$$\frac{(p-1)(q-1)+2}{6} = 166666666666666666666666666666666$$
$$66666693789244306666666666666666666666666666666666666$$
$$70735053308917$$

que me dá o valor de k; donde

$$d = 4k-1 = 666666666666666666666666666666666666677515697722$$
$$66666666666666666666666666666666666682940213235667.$$

Com isto podemos codificar a mensagem AMO A OBMEP que, neste caso, pode ser tomada como um único bloco

$$m = 1022249910992411221425$$

já que este é um número menor do que $n = pq$. O resíduo de

$$1022249910992411221425^3 \text{ módulo } n$$

é

$$106824592360317689994495293731276889004322696993731601$$
$$3731140625,$$

que corresponde à codificação $\mathbf{C}(m)$ da mensagem m. Se já é difícil imaginar o cálculo do cubo de m módulo n, o que dizer da decodificação de $\mathbf{C}(m)$, que consiste em elevar este número de 63 algarismos

a d, que é um número de 99 algarismos. Na verdade, um computador não consegue escrever todos os algarismos de $\mathbf{C}(m)^d$: há tantos deles que não cabem na memória de nenhum computador. No entanto, usando congruência módulo n o meu computador consegue calcular o resíduo de $\mathbf{C}(m)^d$ módulo n em menos de um centésimo de segundo!

Custa-me crer que, tendo lido este último exemplo, você não esteja perguntando:

Como ele fez para obter este números primos enormes?

Esta é uma ótima pergunta, que fica melhor ainda se você lembrar que:

1. para saber se um número é primo precisamos garantir que não tem fatores próprios e que;
2. não existem meios rápidos para fatorar números tão grandes.

A conclusão aparentemente inevitável de (1) e (2) é que deveria ser impossível determinar com certeza se números muito grandes são primos. Curiosamente, a conclusão é falsa, muito embora tanto (1) quanto (2) sejam verdadeiros. O fato, bastante surpreendente, é que é possível determinar que números muito grandes são primos ou compostos sem que haja necessidade de fatorá-los. Discutiremos isto com um pouco mais de detalhes no próximo capítulo.

6.3 Por que funciona?

Para que o procedimento exposto acima seja realmente útil, é preciso que, ao decodificar uma mensagem, obtenhamos a mensagem

original. Vimos nos exercícios 57 e 58 que, ao menos nestes exemplos, a decodificação reproduziu a mensagem original. Falta, apenas, convencer-nos de que isto *sempre* ocorre.

6.3.1 Explicando o Funcionamento do RSA

Digamos que temos um sistema RSA de parâmetros p e q, com $n = pq$. Então, para a codificação usamos a chave pública n, e para a decodificação o par (n, d), onde

$$(p-1)\cdot(q-1) = 6\cdot k - 2 \quad \text{e} \quad d = 4\cdot k - 1.$$

Usando a notação das seções anteriores, precisamos verificar que, se b é um bloco da mensagem a ser codificada, isto é um inteiro que satisfaz $1 \leq b \leq n-1$, então $\mathbf{DC}(b) = b$. Em outras palavras, queremos mostrar que aplicando o processo de decodifição a um bloco codificado, obtemos de volta o bloco correspondente da mensagem original.

Na verdade, precisamos provar apenas que

$$\mathbf{DC}(b) \equiv b \pmod{n}.$$

Isto é suficiente porque tanto $\mathbf{DC}(b)$ quanto b estão no intervalo que vai de 1 a $n-1$, logo só podem ser congruentes módulo n se forem iguais.

Isto explica porque precisamos escolher b menor que n e porque temos que manter os blocos separados, mesmo depois da codificação. Se não tomássemos estes cuidados, continuaríamos obtendo blocos

congruentes depois da decodificação, mas eles não seriam necessariamente iguais. Em outras palavras, não teríamos de volta a mensagem original o que, convenhamos, não seria muito satisfatório.

Vamos ao argumento. Recapitulando, o que queremos mostrar é a congruência

$$\mathbf{DC}(b) \equiv b \pmod{n}.$$

Mas, pela definição de **D** e de **C** temos que

$$\mathbf{C}(b) \equiv b^3 \pmod{n};$$

e que

$$\mathbf{C}(a) \equiv a^d \pmod{n}.$$

Combinando estas duas congruências, obtemos

$$\mathbf{DC}(b) \equiv \mathbf{D}(b^3) \equiv b^{3d} \pmod{n}. \tag{6.3.1}$$

Queremos, portanto, mostrar que $b^{3d} \equiv b \pmod{n}$. Mas, por definição,

$$3d \equiv 1 \pmod{(p-1)(q-1)},$$

donde

$$3d = 1 + k(p-1)(q-1). \tag{6.3.2}$$

Lembrando que $n = pq$, onde p e q são primos *distintos*, calcularemos os resíduos de b^{3d} módulo p e módulo q e usaremos o teorema chinês do resto para construir, a partir deles, o resíduo módulo n. Como os cálculos dos resíduos são análogos para ambos os primos, basta mostrar como executar um deles. Digamos que queremos achar

o resíduo de b^{3d} módulo p. Levando em conta a expressão para $3d$ obtida em (6.3.2), temos que

$$b^{3d} \equiv b \cdot (b^{p-1})^{k(q-1)} \pmod{p}.$$

Em seguida queremos usar o Teorema de Fermat, mas para isto precisamos saber que p não divide b. Se isto for verdade, então

$$b^{p-1} \equiv 1 \pmod{p}$$

por Fermat, e obtemos

$$b^{3d} \equiv b \cdot (1)^{k(q-1)} \equiv b \pmod{p}$$

mostrando o que queríamos. Por outro lado, se p dividir b, então tanto b quanto b^{3d} são congruentes a zero módulo n. Logo, também neste caso, $b^{3d} \equiv b \pmod{p}$. Resumindo, não importa qual seja o inteiro b, sempre temos que

$$b^{3d} \equiv b \pmod{p}.$$

Fazendo um argumento análogo para o primo q, obtemos o par de congruências

$$\begin{aligned} b^{3d} &\equiv b \pmod{p}, \\ b^{3d} &\equiv b \pmod{q}. \end{aligned} \tag{6.3.3}$$

Observe que b é uma solução de

$$\begin{aligned} x &\equiv b \pmod{p}, \\ x &\equiv b \pmod{q}; \end{aligned}$$

de modo que, pelo teorema chinês do resto, este sistema tem solução geral igual a

$$b + p \cdot q \cdot t,$$

onde $t \in \mathbb{Z}$. Logo b^{3d} que, por (6.3.3) também é solução do mesmo sistema, tem que satisfazer

$$b^{3d} = b + p \cdot q \cdot k,$$

para algum inteiro k. Mas isto é equivalente a

$$b^{3d} \equiv b \pmod{pq};$$

que é a congruência que desejávamos provar.

Exercício 59. *Discuta em grupo os seguintes problemas relativos à segurança do RSA:*

(a) se as chaves públicas de duas pessoas diferentes têm um primo em comum, então é fácil quebrar o RSA destas duas pessoas;

(b) se usamos o RSA, mas codificamos a mensagem partindo-a em blocos que consistem de uma única letra, então é fácil decodificar a mensagem, embora o código não seja quebrado.

Um problema semelhante, porém mais difícil, é proposto no seguinte desafio.

Desafio 7. *Sabemos que se n é a chave pública de uma implementação do RSA, então $n = pq$, onde p e q são primos positivos distintos. Imagine que alguém lhe emprestou um computador (que você não tem a menor ideia de como funciona) que, ao receber a chave pública n calcula o número $m = (p-1)(q-1)$. Mostre que é possível determinar p e q a partir de n e m.*

6.3.2 Comentário

Se você leu o argumento usado para provar que o RSA funciona corretamente em detalhes e com bastante senso crítico, pode estar perguntando:

> Onde usamos o fato dos primos terem que deixar resíduo 5 módulo 6?

A resposta é que isto só é necessário para garantir que 3 é inversível módulo $(p-1)(q-1)$. Como a demonstração toda depende disto, a hipótese parece realmente essencial. Mas não é. O fato é que o RSA pode ser implementado usando quaisquer dois expoentes inteiros positivos, e para codificação e d para decodificação, desde que

$$ed \equiv 1 \pmod{(p-1)(q-1)}.$$

A demonstração de que o sistema se comporta da maneira desejada para tais expoentes é essencialmente a mesma que foi dada acima.

Então, por que estamos nos limitando ao caso em que o expoente de codificação e é igual a 3? A resposta é que, com isto, é fácil determinar d. Para que pudéssemos permitir expoentes mais gerais,

precisaríamos de um outro algoritmo que nos permitisse determinar o inverso de um dado número módulo $(p-1)(q-1)$, quando este inverso existe. Este algoritmo existe e é bem conhecido, trata-se de uma extensão do algoritmo euclidiano que é utilizado para calcular o máximo divisor comum de dois números. Mais detalhes sobre este algoritmo podem ser encontrados no capítulo 1 da referência [2].

Capítulo 7

Encontrando Primos

Neste capítulo veremos como encontrar primos para utilizar no RSA. Como o conhecimento dos fatores primos p e q de n permite a qualquer um descobrir uma mensagem codificada usando n como chave pública, os primos p e q precisam ser muito grandes. Por isto o problema que desejamos resolver neste capítulo pode ser mais precisamente formulado pela pergunta:

> Como achar primos grandes cujo resto na divisão por 6 é 5?

Responderemos a esta pergunta:

1. provando que existem infinitos primos cujo resto na divisão por 6 é 5;
2. descrevendo um procedimento pelo qual podemos encontrar *todos* os primos deste tipo menores que um dado inteiro t.

Na prática a resposta a (2) não é satisfatória, porque não é viável encontrar *todos* os primos que tenham menos dos que 50 algarismos. Há muitos deles, e o tempo necessário para determinar todos seria longo demais. Para achar um primo de 50 algarismos precisamos de um procedimento que nos leve diretamente a ele, sem ter que achar todos os primos intermediários. Isto é possível mas está além das possibilidades desta apostila; para mais detalhes consulte o capítulo 6 da referência [2], por exemplo. Entretanto, para não deixar o problema inteiramente sem resposta analisaremos na seção 7.3 um teste que permite identificar que certos números são compostos sem precisar fatorá-los.

7.1 Infinidade dos Primos

Começaremos discutindo o argumento, dado por Euclides em seus *Elementos*, que mostra que existem infinitos números primos.

7.1.1 Infinitos Primos

Na verdade o que mostraremos é que, dado um conjunto *finito* qualquer $\mathcal{P}$ de primos, tem que existir um primo fora de $\mathcal{P}$.

Digamos que

$$\mathcal{P} = \{p_1, \ldots, p_s\},$$

é um conjunto *finito* formado apenas por números primos e consideremos o número

$$N = p_1 \cdots p_s,$$

que é igual ao produto de *todos* os primos em $\mathcal{P}$. Como N e $N+1$ não podem ter nenhum fator próprio comum (veja Exercício 3), um primo que divide N não pode dividir $N+1$. Mas, *todos* os primos em $\mathcal{P}$ dividem N; logo *nenhum* primo em $\mathcal{P}$ pode dividir $N+1$. Contudo, pelo Teorema da Fatoração Única o número inteiro $N+1$ tem que ter algum fator primo. Como estes fatores não podem dividir N, então são primos que não pertencem a $\mathcal{P}$, provando assim o que queríamos.

O resultado que acabamos de mostrar é importante o suficiente para ser enunciado como um teorema.

Teorema 4. *Se $\mathcal{P}$ é um conjunto* finito *de números primos, então existe um primo que não pertence a $\mathcal{P}$.*

Observe que isto basta para garantir que o conjunto de todos os primos não pode ser *finito*. Afinal, dado um conjunto *finito* qualquer de primos, mostramos que sempre há um primo fora deste conjunto.

Teorema de Euclides. *Existem infinitos números primos.*

Curiosamente, apesar do resultado acima ser frequentemente atribuído a Euclides, o enunciado que aparece nos *Elementos* é mais parecido com o Teorema 4. O que Euclides diz, em uma tradução quase literal do grego é:

> há mais números primos do que qualquer quantidade proposta de primos.

Um erro que muita gente comete ao ler a demonstração do teorema 4 consiste em achar que o argumento mostra que o número $N+1$ é primo. Em outras palavras, multiplicando uma quantidade finita de

primos e somando um obtemos um primo. Isto não é verdade, como você vai verificar no próximo exercício.

Exercício 60. *Se p for um primo, denote por $p^{\#}$ o produto de todos os primos positivos menores ou iguais que p. Por exemplo,*

$$11^{\#} = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11.$$

Chamamos $p^{\#}$ de primorial *de p, porque sua definição parece com a do fatorial. Determine o menor valor de p para o qual $p^{\#} + 1$ é composto.*

Na verdade, há apenas 22 primos p para os quais $p^{\#}+1$ também é primo. O maior deles é 392 113; cujo primorial $392\,113^{\#}$ é o produto de 33 237 primos e dá lugar a um primo $392\,113^{\#} + 1$ de 169 966 algarismos.

Quase tudo o que fizemos acima relativamente a $p^{\#}+1$ também se aplica a $p^{\#}-1$, como você é chamado a mostrar no próximo exercício.

Exercício 61. *Seja p um primo.*

(a) Mostre que $p^{\#}$ e $p^{\#} - 1$ não têm fatores comuns.

(b) Use (a) para mostrar que existem infinitos números primos.

(c) Determine o menor primo ímpar p para o qual $p^{\#} - 1$ é composto.

São conhecidos apenas 18 primos da forma $p^{\#} - 1$, o maior deles é $15\,877^{\#} - 1$ que tem 6 845 algarismos.

7.1.2 Primos da Forma 6k+5

Embora o que acabamos de fazer seja muito interessante, não podemos esquecer que não era bem isto que queríamos provar, mas sim que existem infinitos primos *cujo resto na divisão por* 6 *é* 5. Vejamos se o que já mostramos basta para provar esta afirmação mais restrita.

Em primeiro lugar, qualquer inteiro na divisão por 6 tem que deixar como resto um número entre 0 e 5. Mas, se p for *primo* então as possibilidades de restos são mais restritas. De fato, se o resto for 0, o número é divisível por 6. Por outro lado, se o resto for 2 ou 4, então o número é par, logo divisível por 2; ao passo que se o resto for 3, o número é divisível por 3. Portanto,

> se p for primo só pode deixar resto 1 ou resto 5 quando dividido por 6.

Isto, infelizmente não é bom para o nosso argumento. Embora seja fácil produzir exemplos de primos que deixam resto 5 na divisão por 6 (como 5 e 17), talvez só haja uma quantidade finita destes primos, ao passo que os que deixam resto 1 na divisão por 6 são infinitos. Apesar de não ser verdade, isto é compatível com o fato de existirem infinitos primos.

Isto não esgota nossa caixa de ferramentas, porque ainda podemos pensar em usar o teorema 4 diretamente, em vez de apelar para o Teorema de Euclides, que é apenas uma de suas possíveis consequências. Mais precisamente, queremos mostrar que

> se $\mathcal{P}$ for um conjunto *finito* de primos da forma $6k + 5$

> então existe um primo da mesma forma que *não* pertence a $\mathcal{P}$.

O problema é que o teorema 4 nos diz apenas que existe *algum primo* fora de $\mathcal{P}$ e, como já vimos, há primos que não são da forma $6k+5$.

Em princípio, poderíamos tentar refinar nossa análise repetindo a demonstração do teorema 4 neste caso especial para ver se continua funcionando. Para isso, suponhamos que

$$\mathcal{P} = \{p_1, \ldots, p_s\},$$

é um conjunto *finito* formado apenas por números primos da forma $6k+5$ e consideraremos o número

$$N = p_1 \cdots p_s,$$

que é igual ao produto de *todos* os primos em $\mathcal{P}$. Como antes,

$$N \text{ e } N+1 \text{ não têm fator próprio comum,}$$

só que, como N é um número ímpar, $N+1$ tem que ser par. Portanto, $N+1$ admite 2 como fator e não chegamos a nenhuma contradição porque, por exemplo, isto é compatível com $N+1$ ser uma potência de 2.

Para sair desta enrascada precisaremos de um argumento muito mais delicado. Ao invés de considerar simplesmente $N+1$, escolheremos trabalhar com $6N+5$, porque este último número deixa resto 5 na divisão por 6, como era o caso dos primos com os quais começamos. Infelizmente, 5 pertence ao conjunto $\mathcal{P}$, de modo que é um divisor

comum entre N e $6N+5$, de modo que

$$\text{mdc}(N, 6N+5) \neq 1.$$

Mas isto não é razão para desanimarmos. Depois de pensar um pouco, vemos que esta dificuldade pode ser contornada se excluírmos 5 do produto que define N. Para deixar o argumento mais claro, redefiniremos todos os dados iniciais.

Suponha, então, que

$$\mathcal{P} = \{5, p_1, \ldots, p_s\},$$

seja o conjunto *finito* formado por todos os números primos que deixam resto 5 na divisão por 6. Considere o número

$$N = p_1 \cdots p_s.$$

Observe que deixamos o 5 fora deste produto. Pelo teorema da fatoração única, podemos escrever $6N+5$ na forma

$$6N + 5 = q_1^{e_1} \cdots q_m^{e_m}, \tag{7.1.1}$$

em que os qs são primos positivos e os es são inteiros positivos. Como $6N+5$ é ímpar, todos os seus fatores têm que ser ímpares. Portanto, os q são ímpares e têm que deixar resto 1 ou 5 na divisão por 6. Digamos, por um momento, que todos os qs deixassem resto um na divisão por 6. Neste caso teríamos que

$$q_1^{e_1} \cdots q_m^{e_m} \equiv 1 \pmod 6.$$

Mas isto é impossível, porque pela igualdade (7.1.1),

$$q_1^{e_1} \cdots q_m^{e_m} \equiv 6N + 5 \equiv 5 \pmod 6,$$

e 1 e 5 não são congruentes módulo 6. Isto nos permite concluir que

> $6N + 5$ tem que ter pelo menos um fator primo que deixa resto 5 na divisão por 6.

Acontece que $\mathcal{P}$ é, por hipótese, a lista completa dos primos da forma $6k + 5$. Logo, $6N + 5$ tem que ser divisível por algum elemento de $\mathcal{P}$. Isto é possível?

Vejamos. Para começar, se 5 dividisse $6N + 5$ então teria que dividir

$$(6N + 5) - 5 = 6N = 2 \cdot 3 \cdot p_1 \cdots p_s,$$

o que não é possível, já que 5 não aparece entre os primos nesta fatoração. Por outro lado, se $6N+5$ fosse divisível por um dos primos que dividem N, então

$$(6N + 5) - 6N = 5,$$

teria que ser divisível pelo mesmo primo, o que também não é possível. Isto mostra que $6N + 5$ não pode ser divisível por nenhum elemento de $\mathcal{P}$, e nos dá a contradição desejada. Disto segue imediatamente que há uma quantidade infinita de primos da forma $6k + 5$, como esperávamos mostrar.

Desafio 8. *O objetivo deste desafio é dar uma demonstração de que existem infinitos números primos da forma* $4n + 3$.

(a) Mostre que todo número primo ímpar tem resíduo 1 *ou* 3 *módulo* 4.

(b) Dê exemplos de cinco números primos que têm resíduo 1 *módulo* 4 *e cinco que têm resíduo* 3 *módulo* 4.

(c) Mostre que o produto de dois números inteiros da forma $4n+1$ *é da forma* $4n+1$.

(d) O produto de dois números da forma $4n+3$ *é da forma* $4n+3$*?*

(e) Suponha que $3 < p_1 < \cdots < p_k$ *sejam primos da forma* $4n+3$. *Usando (c), verifique que* $4(p_1 \dots p_k)+3$ *tem que ser divisível por um primo da forma* $4n+3$ *que não pertence ao conjunto* $\{3, p_1, \dots, p_k\}$.

(f) Use (e) para mostrar que existem infinitos números primos da forma $4n+3$.

7.2 Encontrando os Primos

Agora que sabemos que há uma infinidade de primos da forma $6k+5$, só nos resta explicar como se deve proceder para encontrar primos cada vez maiores que são desta forma. Como na seção anterior, começaremos tratando dos primos em geral; só depois veremos o que acontece se nos restringimos apenas aos primos da forma $6k+5$.

7.2.1 O Crivo de Eratóstenes

Descreveremos aqui o mais antigo dos métodos para achar primos, conhecido como *crivo de Eratóstenes*. Como não podia deixar de ser, Eratóstenes foi um matemático grego, e nasceu por volta de 284 a.C. Apesar de sua proficiência em muitos dos ramos de conhecimento, os contemporâneos de Eratóstenes julgavam que não havia chegado à perfeição em nenhum. Por isso era chamado de "Beta" (segunda letra no alfabeto grego) e "Pentatlos". Competitivos, esses gregos, não?

Antes de mais nada, você precisa saber que um *crivo* é uma peneira. Nicômaco em sua *Aritmética*, publicada por volta do ano 100 d.C., introduz o crivo de Eratóstenes da seguinte maneira:

> o método para obtê-los [os números primos] é chamado por Eratóstenes uma peneira, porque tomamos os números ímpares misturados de maneira indiscriminada e, por este método, como se fosse pelo uso de um instrumento ou peneira, separamos os primos ou indecomponíveis dos secundários ou compostos.

Portanto o *crivo* atua como uma peneira que só deixa passar os números primos. Vejamos como funciona.

Em primeiro lugar o crivo determina todos os primos até um certo inteiro positivo n previamente escolhido. Para realizar o crivo com lápis e papel podemos proceder da seguinte maneira. Listamos os ímpares de 3 a n. É claro que só listamos os ímpares porque 2 é o único primo par. Começamos então a operar com o crivo propriamente dito. O primeiro número da nossa lista é 3; riscamos os demais números da lista, de 3 em 3. Assim serão riscados todos os múltiplos de 3 maiores

que ele próprio. Em seguida procuramos o menor elemento da lista, maior que 3, que não tenha sido riscado, que é 5. Riscamos os demais números da lista, de 5 em 5. Assim serão riscados todos os múltiplos de 5 maiores que ele próprio. E assim por diante, até chegar a n.

Por exemplo, se $n = 60$, a lista de números é

	3	5	7	9	11	13	15	17	19
21	23	25	27	29	31	33	35	37	39
41	43	45	47	49	51	53	55	57	59

Ao final da primeira passagem do crivo (de 3 em 3), ficamos com

	~~3~~	5	7	~~9~~	11	13	~~15~~	17	19
~~21~~	23	25	~~27~~	29	31	~~33~~	35	37	~~39~~
41	43	~~45~~	47	49	~~51~~	53	55	~~57~~	59

Ao final da segunda passagem do crivo (de 5 em 5) a lista é

	~~3~~	~~5~~	7	~~9~~	11	13	~~15~~	17	19
~~21~~	23	~~25~~	~~27~~	29	31	~~33~~	~~35~~	37	~~39~~
41	43	~~45~~	47	49	~~51~~	53	~~55~~	~~57~~	59

Ao final da terceira passagem do crivo (de 7 em 7), a lista se torna

	~~3~~	~~5~~	7	~~9~~	11	13	~~15~~	17	19
~~21~~	23	~~25~~	~~27~~	29	31	~~33~~	~~35~~	37	~~39~~
41	43	~~45~~	47	~~49~~	~~51~~	53	~~55~~	~~57~~	59

Ao final da quarta passagem do crivo (de 11 em 11), a lista continua a mesma acima. A quinta passagem seria de 13 em 13, mas novamente nada vai mudar na lista. Na verdade nenhuma passagem

posterior do crivo vai eliminar nenhum número adicional. Logo os primos ímpares positivos menores que 35 são

$$3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 53 \text{ e } 59.$$

Este exemplo nos leva a observar algumas características do crivo. Em primeiro lugar, alguns números são riscados da lista mais de uma vez. É o caso de 15 que já havia sido riscado na primeira passagem (3 em 3), e foi riscado também na segunda (5 em 5). Em segundo lugar, já havíamos riscado da lista todos os números compostos na terceira passagem do crivo. Todas as passagens posteriores foram redundantes.

Consideremos a segunda observação. Ela indica que deve ser possível parar de riscar os números muito antes de chegar a n. De fato, se m é um inteiro da lista, então $m \leq n$. Se m for composto, então terá um fator menor ou igual a $\sqrt{m}$ pela proposição 1. Mas $\sqrt{m} \leq \sqrt{n}$. Isto é, qualquer número composto da lista tem um fator menor ou igual a $\sqrt{n}$. Desta forma não precisamos riscar números de r em r quando $r > [\sqrt{n}]$. No exemplo acima $[\sqrt{60}] = 7$; por isso é suficiente riscar de 3 em 3, de 5 em 5, de 7 em 7 e nada mais.

A outra observação é mais delicada. Infelizmente não é possível evitar completamente o fato de que alguns números serão riscados várias vezes. Mas podemos melhorar um pouco o crivo acima. Digamos que queremos achar os primos até n, e que estamos prestes a riscar os números de p em p para algum primo p. É claro que os múltiplos de p que também são múltiplos de primos menores que p já foram riscados da lista. Portanto, nesta etapa, podemos começar a

riscar de p em p a partir do menor múltiplo de p, *que não é múltiplo de um primo menor que* p. Mas os múltiplos positivos de p são da forma

$$k \cdot p \quad \text{para algum inteiro} \quad k \leq 0,$$

e se $k < p$, o inteiro $k \cdot p$ também é múltiplo do número k que é menor que p. Logo, o menor múltiplo de p, *que não é múltiplo de um primo menor que* p é p^2. Resumindo:

$$\text{podemos riscar de } p \text{ em } p \text{ a começar de } p^2.$$

Isto evita algumas duplicações e torna o crivo um pouco mais econômico.

7.2.2 Primos da Forma 6k + 5

Uma maneira de determinar os primos menores que um inteiro positivo n e que são da forma $6k + 5$ é listar todos os primos até n usando o crivo e testar para ver quais deixam resto 5 quando dividimos por 6. Fazendo isto à lista de primos menores que 60 obtida anteriormente, sobram apenas

$$5,\ 11,\ 17,\ 23,\ 29,\ 41,\ 47,\ 53 \quad \text{e} \quad 59.$$

O problema desta estratégia é que é muito ineficiente. Digamos, por exemplo, que queremos encontrar todos os primos que deixam resto 5 na divisão por 6 e que são menores ou iguais a 1 000. Utilizando o crivo de Eratóstenes na forma apresentada anteriormente, teríamos que gerar uma lista de $1\,000/2 = 500$ números ímpares para riscar. Contudo, somente um em cada seis elementos da lista deixa resto 5

na divisão por 6. Como

$$1\,000 = 6 \cdot 166 + 4;$$

isto significa que bastaria procurar pelos primos que realmente nos interessam entre 166 números: aqueles que deixam resto 5 quando divididos por 6. Mas esta é uma lista muito menor e mais fácil de manipular que a do crivo de Eratóstenes. A questão é:

> Podemos continuar riscando de p em p para determinar se um número é múltiplo de p, *mesmo com a lista reduzida somente aos números da forma* $6k + 5$?

Uma observação, antes de continuarmos, para o caso de você ter pensado:

> Mas para que se preocupar com isto se posso verificar se o número é múltiplo de p simplesmente dividindo-o por p e vendo se o resto é zero?

De fato isto pode ser feito mas, para números mais ou menos grandes, é muito mais trabalhoso do que contar de p em p. E isto continua sendo verdadeiro mesmo se usarmos um computador para fazer o risca-risca.

Para que o crivo possa restringir-se apenas aos números da forma de resíduo 5 módulo 6, precisamos mostrar duas coisas. A primeira é que

(1) todo número composto que tem resíduo 5 módulo 6 admite um fator do mesmo tipo.

Do contrário alguns compostos não seriam riscados já que o risca-risca de p em p está agora limitado aos número que deixam resto 5 na divisão por 6. Que (1) na verdade é consequência de resultados que já vimos antes. De fato, como vimos em 2.2.3, qualquer número *primo* deixa resto 1 ou 5 quando dividido por 6. Porém, se todos os fatores primos de um número n deixarem resto 1 na divisão por 6, teremos $n \equiv 1 \pmod 6$, de modo que n terá necessariamente resto 1 na divisão por 6. Isto nos permite concluir que,

> se um inteiro positivo deixa resto 5 quando dividido por 6 então *pelo menos um dos seus fatores primos* deixa o mesmo resto quando dividido por 6.

A segunda coisa que precisamos mostrar é que

(2) todos os múltiplos de p que aparecem na tabela continuam espaçados de p em p.

Afinal de contas, removemos 5/6 dos números da tabela, o que alterou completamente a posição de cada um deles em relação aos outros, pondo em risco nossa capacidade de detectar múltiplos apenas por manterem um espaçamento constante.

Talvez este último ponto precise ser um pouco melhor elaborado. Considere, por exemplo, a lista dos ímpares até 30:

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29

Nesta tabela os múltiplos de 3 aparecem a cada 3 casas e os múltiplos de 5 a cada 5 casas. Removendo os múltiplos de 3, obtemos a seguinte tabela mais curta:

1	5	7	11	13	17	19	23	25	29

Note que já não é mais verdade que os múltiplos de 5 aparecem a cada 5 casas. A remoção dos múltiplos de 3, alguns dos quais também são múltiplos de 5, alterou a posição dos números uns em relação aos outros e destruiu o fato dos múltiplos de um mesmo número manterem uma distância fixa uns dos outros.

Para mostrar (2), começaremos por tentar identificar qual é a forma de um inteiro que deixa resto 5 na divisão por 6 *e que é divisível por p*. Chamando este inteiro de x, estas condições se traduzem no sistema de congruências

$$\begin{aligned} x &\equiv 5 \pmod 6, \\ x &\equiv 0 \pmod p. \end{aligned}$$

Para resolver o sistema pelo algoritmo chinês do resto, tomamos $x = yp$ da segunda congruência e substituímos na primeira, obtendo

$$yp \equiv 5 \pmod 6. \tag{7.2.1}$$

Como só vamos riscar usando primos cujo resíduo módulo 6 é igual a 5, temos que

$$p \equiv 5 \pmod 6;$$

de forma que (7.2.1) se torna

$$y5 \equiv 5 \pmod 6;$$

donde,

$$y \equiv 1 \pmod 6.$$

Assim, $y = 1 + 6r$ e, portanto,

$$x = p + 6rp.$$

Em outras palavras, mostramos que todos os múltiplos de p em uma tabela que só contém números de resíduo 5 módulo 6 são da forma $p + 6rp$, o que nos permite concluir que

> para irmos de um múltiplo de p que deixa resto 5 na divisão por 6 ao seguinte basta somar $6p$ a este número.

Como os números em nossa tabela já estão espaçados de seis em seis (pois são da forma $6k+5$), se pularmos de um múltiplo de p ao seguinte *na tabela* teremos dois números cuja diferença é $6p$. Pela conclusão enunciada acima estes são precisamente dois múltiplos de p da forma $6k + 5$ *consecutivos*, o que prova (2).

Antes de executarmos o crivo restrito a uma tabela que só contenha os números que deixam resto 5 na divisão por 6, há um detalhe que precisamos considerar. Na versão original do crivo, vimos que

> qualquer número composto admite um fator primo menor ou igual que sua raiz quadrada.

Por outro lado, de acordo com (1),

> se um inteiro positivo que deixa resto 5 quando dividido por 6 então *pelo menos dos seus fatores primos* deixa o mesmo resto quando dividido por 6.

Infelizmente, não podemos combinar estas duas afirmações e deduzir que um inteiro positivo deixa resto 5 quando dividido por 6 tem que ter um fator primo menor ou igual à sua raiz quadrada que satisfaça a mesma propriedade. Só poderíamos chegar a esta conclusão se *todos os fatores primos* de um número cujo resíduo módulo 6 é 5 fossem do mesmo tipo; mas isto é falso. Por exemplo, 161 deixa resto 5 na divisão por 6 e tem dois fatores, 7 e 23, dos quais somente 23 deixa resto 5 na divisão por 6; entretanto,

$$23 > \sqrt{161} = 12,68\ldots$$

de modo que 161 não tem *nenhum* fator menor que sua raiz quadrada que deixe resto 5 na divisão por 6. Do ponto de vista prático isto significa que, ao contrário do que fizemos na versão usual do crivo de Eratóstenes,

> não podemos parar de riscar quando $p > \sqrt{n}$ se restringirmos nossa tabela apenas aos números da forma $6k + 5$.

Passando ao exemplo, usaremos a estratégia desenvolvida acima para determinar os primos da forma $6k + 5$ que são menores que 60. Os números da forma $6k + 5$ menores que 60 são

5	11	17	23	29	35	41	47	53	59

Como 5 é o primeiro número, começamos riscando de cinco em cinco:

5	11	17	23	29	~~35~~	41	47	53	59

Em seguida, riscaríamos de 11 em 11, acontece que a tabela só tem 10 casas: o décimo primeiro número a partir de 11 já está fora da

tabela. É claro que se isto aconteceu com 11, também acontecerá com qualquer outro número maior que 11. Portanto, tendo riscado de 5 em 5, já obtivemos os primos desejados, que são

$$5,\ 11,\ 17,\ 23,\ 29,\ 41,\ 47,\ 53 \quad \text{e} \quad 59.$$

Antes que você fique animado demais talvez seja melhor previni-lo de que as coisas não são assim tão boas quando o limite superior da tabela é um número muito grande.

Exercício 62. *Use esta versão especial do crivo de Eratóstenes para determinar todos os primos da forma* $6k + 5$ *menores que* 500.

7.3 Um Teste de Composição

Como dissemos na introdução deste capítulo, o crivo de Eratóstenes não é uma maneira eficiente de achar primos realmente grandes, como os que apareceram ao final da seção 6.2 do capítulo 6. O problema é que o intervalo ao qual o crivo está sendo aplicado é grande demais, o que o tornará muito lento e fará com que ocupe um enorme espaço na memória do computador, mais até do que teríamos à nossa disposição! Para contornar o problema, os matemáticos criaram os chamados *testes de primalidade*: critérios que permitem determinar com segurança que um dado número é primo. Estes testes procedem de maneira indireta; ao invés de tentar fatorar o número, calculam apenas certas potências modulares, por isso têm execução bastante rápida. O problema é que os testes mais eficientes podem, em alguns casos, ter resultados inconclusivos; isto é, o teste pode não conseguir

decidir se um dado número é ou não primo.

Tudo isto pode estar parecendo um tanto confuso e misterioso, por isso daremos um exemplo de um tal teste, o mais simples de todos. Trata-se de um teste que, ao receber um inteiro $n > 2$, tem uma de duas saídas possíveis: o número n é composto *ou* o teste foi inconclusivo. Note que o teste tem a saída oposta ao que realmente queremos. Desejamos garantir *primalidade*, mas este teste só garante *composição*: se a saída for inconclusiva, o número dado pode ser composto ou não: o teste não é suficiente para garantir qual a resposta correta. Mas lembre-se: vamos apresentar este teste em particular porque é muito simples e dá uma ideia razoável de como testes deste tipo funcionam; só isso.

O teste tem por base o Teorema de Fermat, que enunciamos aqui para lembrá-lo do seu conteúdo exato.

Teorema de Fermat. *Se p é um primo e a é um inteiro* que não é divisível por p, *então*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Portanto, o teorema nos diz que se p é primo então uma certa congruência *tem que ser verdadeira*. Considere, então, o seguinte número de 101 algarismos,

$$R(101) = 11111111111111111111111111111111111111111111111111$$
$$11111111111111111111111111111111111111111111111111.$$

Este número é primo? Calculando o resíduo r de 2^{n-1} módulo n com auxílio de um computador, verificamos que

$$r = 529291418765427305857159888519920259594072875818663971056576050867002198560952050580282534986566941 5.$$

Mas, espera aí: se p *fosse* primo, o resíduo não devia dar 1? Afinal é isso que diz o Teorema de Fermat, não é? Mas se $r \neq 1$ alguma coisa tem que ter saído errado. Ou o cálculo do resíduo está errado (não está, fiz o cálculo no meu computador e testei o resultado), ou 2 divide n (brincadeirinha...), ou o Teorema de Fermat é falso (não é, vimos uma demonstração no capítulo 5) ou nossa impressão de que n fosse primo não se justifica; isto é, na verdade n é composto. O mais interessante é que o algoritmo de fatoração do meu computador *não* consegue calcular nenhum fator para este número, embora o Teorema de Fermat nos garanta que ele é composto!

É fácil generalizar este argumento. Seja n o número inteiro que queremos saber se é composto. Escolhemos um inteiro b qualquer, que não seja divisível por n e calculamos o resíduo r de b^{n-1} módulo n. Se acontecer de $r \neq 1$ então o Teorema de Fermat nos garante que n não pode ser primo. Temos, assim, uma maneira *indireta* de provar que um dado número é composto. Em outras palavras, mesmo não tendo determinado nenhum fator de n podemos ter certeza de que n é composto.

Naturalmente, a pergunta que precisamos fazer é:

> O que podemos afirmar sobre n se o resíduo $r \equiv b^{n-1} \pmod{n}$ *for* igual a 1?

G. W. Leibniz, o famoso matemático alemão do século XVII, acreditava que se $2^{n-1} \equiv 1 \pmod{n}$ então n teria que ser primo. Se isto fosse verdade, teríamos um teste extremamente eficiente para determinar a primalidade de um número inteiro. Infelizmente, a habilidade de Leibniz em matemática não lhe impediu de cometer este erro; de fato,

> pode acontecer que um número ímpar composto satisfaça $b^{n-1} \equiv 1 \pmod{n}$ mesmo quando $b \not\equiv \pm 1 \pmod{n}$.

Um exemplo simples é $n = 25$ quando $b = 7$. Neste caso, precisamos calcular o resíduo de 7^{24} módulo 25. Mas $24 = 8 \cdot 3$ e

$$7^3 \equiv 18 \pmod{25};$$

donde

$$7^{24} \equiv ((7^3)^2)^4 \equiv (18^2)^4 \equiv (24)^4 \equiv (-1)^4 \equiv 1 \pmod{25}.$$

Portanto, o número composto 25 satisfaz a congruência

$$7^{24} \equiv 1 \pmod{25}.$$

Em outras palavras, 25 comporta-se como se fosse um número primo relativamente à congruência do Teorema de Fermat, quando tomamos a base da potência como sendo 7. Tais números são conhecidos como *pseudoprimos*; isto é, *falsos primos* (*pseudo* é um prefixo grego que

significa falso). Mais precisamente, um número inteiro positivo n é um *pseudoprimo* relativamente à base b se n for ímpar, composto e satisfizer a congruência $b^{n-1} \equiv 1 \pmod{n}$. Embora a base b possa ser qualquer inteiro, não há necessidade de considerar bases maiores que $n-1$ ou menores que 1. A razão é que estamos efetuando apenas cálculos módulo n, de forma que qualquer inteiro pode ser substituído por seu resíduo, sem alterar o cálculo da potência.

Por que escolhemos 7 como base no exemplo acima e não, digamos, 2? A razão é que

$$2^{24} \equiv (2^7)^8 \equiv 3^8 \equiv 11 \pmod{25},$$

de modo que o teste detectaria corretamente que 25 é composto se escolhêssemos 2 como base. Isto significa, em particular, que 25 não contradiz a afirmação de Leibniz. O menor inteiro positivo que é composto e satisfaz $2^{n-1} \equiv 1 \pmod{n}$ é 341. Como este número já é bastante grande, efetuaremos os cálculos da potência usando o método do capítulo 5.

Em primeiro lugar, fatoramos 341, obtendo

$$341 = 11 \cdot 31.$$

Portanto, se r é o resíduo de 2^{340} módulo 341, teremos o sistema

$$\begin{aligned} r &\equiv 2^{340} \pmod{11}, \\ r &\equiv 2^{340} \pmod{31}. \end{aligned}$$

Contudo, pelo Teorema de Fermat $2^{10} \equiv 1 \pmod{11}$, ao passo que

um cálculo direto mostra que $2^5 \equiv 1 \pmod{31}$. Logo,

$$2^{340} \equiv (2^{10})^{34} \equiv 1 \pmod{11},$$
$$2^{340} \equiv (2^5)^{68} \equiv 1 \pmod{31}.$$

Com isso, o sistema pode ser reescrito na forma

$$r \equiv 1 \pmod{11},$$
$$r \equiv 1 \pmod{31};$$

e sequer precisamos aplicar o algoritmo chinês do resto porque, evidentemente, $r = 1$ satisfaz ambas as congruências. Logo,

$$b^{340} \equiv 1 \pmod{341};$$

e podemos concluir que 341 é um pseudoprimo para a base 2, contradizendo assim a afirmação do Leibniz.

Feitas estas considerações, podemos formular o teste resultante do Teorema de Fermat da seguinte maneira.

Teste de composição. *Seja $n > 1$ um inteiro ímpar e b um número inteiro* que não é divisível por n. *Calcule o resíduo r de b^{n-1} módulo n. Se*

- $r \neq 1$ *então n é composto;*
- $r = 1$ *então o teste é inconclusivo.*

Naturalmente *inconclusivo* aqui significa que não podemos ter

certeza se n é primo ou composto. Os vilões são os pseudoprimos: números compostos que deixam resíduo 1 na congruência do teste acima. Antes que você ache que fizemos muito esforço por nada, lembre-se do exemplo com o qual começamos esta seção. Usando o teste, descobrimos que $R(101)$ é composto, mas não consigo calcular nenhum fator com o meu computador, porque são grandes demais. Há muitos outros exemplos como este, dos quais o número

$$F(14) = 2^{2^{14}} + 1$$

é um dos mais espetaculares. Este número de 4 933 algarismos é pseudoprimo para a base 2. Contudo, o resíduo de $3^{F(14)-1}$ módulo $F(14)$ é

$$\begin{aligned}
&92663642022947551183021565848142589012803154792904225303 88\\
&60976142997204352101714374329686400063929022247155046201 68\\
&00950017256046301144725895588379405170467294384377481800 83\\
&16450977105160641516447313536213432338694714362586446426 14\\
&34041401943901989617690777880605404239329712486429959945 18\\
&53807528557739238298167136294789598071180430234113290698 43\\
&59183865107351729240586476199922882132105404911410932759 57\\
&03354688221699856311034700754816249389037937973060187076 24\\
&78436873884161743314873233491532724203492915561363828340 77\\
&16796240962068342115743983498143285395647375330642915305 96\\
&57885720009858514806464851816765579755685867642183767044 38
\end{aligned}$$

continua...

060988488130263117212636108323396450557012617640934214933 7
865213995478946419300928509471162806343295463462670858743 6
759446344413962527980242346918773598816980974079801607635 5
875666091573237339335568712643315102368435694879507468144 9
536610247047030838644656773912968340427843724503749537770 0
749112859923685645772643766261153668074028790691118579878 8
784210844455384136810039598705060454181702956752648649358 3
130006604918051658134857228993598437303321832761914237870 6
706698976108412045404884041378064900977622825551192429951 1
054846468206643134371416718777068719587004969381208469051 6
415015669262409418234978959014487754096298232090781813034 5
465163441905858629509738177140043333225318209108751819137 3
996477456135601816013164124537260287503516851065047228245 6
004375730000444814456192339816171537145153561135049460203 4
942162754172012362672641327873567389040693854084923450855 0
929719776008782638247080542421132731524625584030159648530 9
821675471789027162792238277303155766793261809922315576326 2
295705806438792819399873587386590380168100912154956821792 1
627243564399872386714273857683330140616945870777733783564 3
125903518296145349774306713786726816989196031909192518538 7

continua...

676469951069389072312431487988685793475743560951149830363131844823334062273251144043704094931992187308478990052457137262589157129312078042493366031343888921155946218315119689082469166494727207679685314927203177229272338467800148767372894851996110401411699415705634646143314338251012374850282551540449120046780973081044244014767741281300291825405153666245055335308003361813731596202131623827507590046213781468872721337602351383391244036180261460224977840379559838738106235330733724665038646006196783875613152976381049791233951950211880080101092186605955702888504905364923338618684622934578745673012666268102118105170933985522812262409845661532354438296954820814066000994097063264255070300898292412549688259556444711424675142215574007382352712747565179853110280570968457881099763927355501661250045572444417096166004678524716450796935361023345710385526247352937331815633300170022018236152336526309771388106029329476936772612281986907305389765039322880715522866606580278167721829418354292676105433021000072632686528671653305019350583545229716468801760070402873406575426329792220801930214230499203699411451153956920838298291277593375891473822831447578931386987823677

continua...

49601320629399551659698119508264935373988805564270599406760151759614385138660551353702532710344209861260306992151220649119614018260499452781279209835772162809844305894375738189935746058347322426347706658334518704974694110313987606784691748814808710597793230354951146962786688724393282734233676667475539950391592642234581355226600076765073355480225032905869615137201563051827287869692859622561531013520160292789911403225602267534784409091403252749485669809224389864222522872699995571523445109964928482201498844564690687085606873449849327648681891132074343022758313901368744732756102049318851588609633761376006845924402609516283154658749932441120938653606844037085451215604454034043970670096338220614486726966385857698124647867830872097760345083144059745628538838044904201295785245824550483832529686053887853018932684787911122029234580861550866105621059321229813915071683273768500395761254484973375085668822560550701748142603369899198249347826265874560095153249285038574130230205892752609931488450859305614801826302046581881998189351007004932581268587642159064178406363078760126377030539914457648027327963986565069519909277264869794934951743339858296269946169751

continua...

5767722567946729190402238410127417897149773901275188203885
4875445968557341857521192305032447353155620391519830057834
4876043229651234507101232599676867795300534399281154330366
9561543133291104876022846635712773603755805368778662398435
0641126547572149014680068579593366753172005548119021674441
4461318127515595223785701620105649922262886079532365232976
6625056061650120464853768291381463183738603219745698745725
8065949430682912755117725405126442032692160838612266387888
3517903902198194036900560975373472283211077363328017623773
4638563339609601320040017448859818675802421313089099680661
2395196333178133084564313983286325230943963680919341251290
5466765334951445060146002079878932880934085645861962318355
5766170926604159837144983067589856601662702757157733868440
7849723027284737572380283423370935913494095336093788422061 67

que, com certeza, não é igual a 1, provando assim que $F(14)$ é um número composto. Este caso é ainda mais espetacular do que $R(101)$ porque, apesar de meu computador precisar de apenas 13 segundos para determinar que $F(14)$ é composto usando o teste de composição, ninguém ainda foi capaz de determinar fatores para este número!

Você talvez esteja imaginando porque os números $R(101)$ e $F(14)$ ganharam estes nomes, em vez de serem chamados simplesmente de

n ou m. A razão é que estes números pertencem a famílias especiais e bem estudadas. A família $R(n)$ corresponde aos números da forma

$$\underbrace{11111\cdots1111}_{n \text{ números uns}}.$$

O R vem do fato dos números serem obtidos pela **R**epetição da unidade. Já a família $F(n)$ é constituída pelos números da forma

$$F(n) = 2^{2^n} + 1;$$

chamados de *números de Fermat*, e dos quais já falamos um pouco na introdução.

Como vimos na página 13, Fermat acreditava que todos os números da forma $F(n)$ fossem primos, qualquer que fosse o inteiro $n \geq 0$ escolhido. Esta afirmação de Fermat foi trazida ao conhecimento de Euler, e em 1730 ele provou que 641 é fator de $F(5)$, mostrando, assim, que a afirmação de Fermat é falsa. Como estes números vêm sendo estudados há bastante tempo, sabe-se muito sobre eles. Por exemplo, conhecemos a fatoração completa dos números de Fermat correspondentes a $5 \leq n \leq 11$. Já para

$$n = 12, 13, 15, 16, 17, 18, 19, 21 \quad \text{e} \quad 23,$$

conhecemos alguns fatores, *mas não todos.* Também são conhecidos fatores de números de Fermat muito grandes. A mais recente descoberta deve-se a Payam Samidoost que, em agosto de 2008, mostrou que $6\,089 \cdot 279\,223 + 1$ divide $F(79\,221)$. Por outro lado, apesar de sabermos se $n = 14, 20, 22$ e 24, então o os números $F(n)$ corres-

pondentes são compostos, nenhum fator é conhecido para nenhum destes números de Fermat. Isto é inesperado. Como é possível descobrir um fator para um número gigantesco como $F(79\,221)$, mas não para $F(14)$ é uma outra história, muito interessante, mas que não dá para contar aqui. Os detalhes podem ser encontrados no capítulo 9 do livro [2].

Exercício 63. *O objetivo deste exercício é comprovar o resultado de Euler, segundo o qual* 641 *divide* $F(5)$.

(a) Mostre que $641 = 2^7 \cdot 5 + 1$ *e que* $641 = 2^4 + 5^4$.

(b) Use (a) para mostrar que $F(5) \cdot 5 \equiv 0 \pmod{641}$.

(c) Explique porque (b) implica que $F(5) \equiv 0 \pmod{641}$.

Os números da família $R(n)$ têm uma história mais recente: foram estudados a partir do século XIX como parte de uma tentativa de entender melhor os padrões que aparecem em dízimas periódicas. Os únicos valores conhecidos de n para os quais $R(n)$ é primo são

$$2, 19, 23, 317, 1\,031, 49\,081, 86\,453 \quad \text{e} \quad 109\,297.$$

Como estes números são mais fáceis de tratar e têm propriedades mais simples que os números de Fermat, reservaremos o estudo deles para nosso último desafio.

Desafio 9. *Seja n um número inteiro positivo e $R(n)$ o número que consiste em n números uns repetidos.*

(a) Mostre que $R(n) = (10^n - 1)/9$.

(b) Mostre que se k é um fator de n então $R(k)$ divide $R(n)$.

(c) Determine todos os fatores primos de $R(6)$.

(d) Mostre que se $R(n)$ for primo então n tem que ser primo.

(e) Mostre que $R(7)$ é composto usando o teste desta seção.

Você vai precisar de uma calculadora para fazer os itens (c) e (d) deste exercício.

Soluções

Exercícios

1. O texto é o seguinte:

> É claro que quebrar uma mensagem por contagem de frequência é ainda mais simples se temos um computador. Se a língua é conhecida a maior parte do processo pode ser automatizado, o que torna inviáveis todos os códigos que envolvem substituição de letras, como o que estamos utilizando para codificar esta mensagem. Na verdade alguns dos primeiros computadores foram criados precisamente para ajudar a quebrar os códigos secretos usados pelos alemães durante a Segunda Guerra Mundial. Entre estes estava o "Colosso", um computador construído na Inglaterra por uma equipe liderada por Alan Turing, um dos fundadores da computação científica.

2. A contagem não funciona porque a estrutura da frase foi desfeita; acrescentamos o A porque é a letra mais frequente.

3. (d) Se a e $a+1$ tiverem um divisor comum então por (a) este divisor também divide $(a+1)-a=1$; logo o divisor tem que ser ± 1.

4. A.

5. k é fator de $n!+k$ para todo $2 \leq k \leq n-1$. Além disso, o cofator não pode ser um.

6. Se k divide m, então $m = c \cdot k$. Se m divide n, então $n = d \cdot m$. Substituindo a primeira equação na segunda, $n = d \cdot c \cdot k$; donde k divide n.

7. $p = 3$ ou $p = 5$ e $n = p^2$.

8. Se c tivesse um fator menor que p, este é que seria o menor fator de n, e não p.

9. $x = 2$ e $y = 3$.

10. Não há solução.

11. Se $n = p_1^{e_1} \cdots p_t^{e_t}$ e $p_1 < \cdots < p_t$ então a multiplicidade de p_1 na fatoração de n é, por definição, e_1. Contudo,

$$\frac{n}{p_1} = p_2^{e_2} \cdots p_t^{e_t}$$

de modo que $p_1^{e_1}$ divide n. Por outro lado, se $p_1^{e_1+1}$ dividisse n, então poderíamos escrever

$$p_2^{e_1} \cdots p_t^{e_t} = p_1^{e_1+1} \cdot c$$

para algum inteiro positivo c. Cancelando, p^{e_1} dos dois lados da equação, obtemos

$$p_2^{e_2} \cdots p_t^{e_t} = p_1 \cdot c.$$

Como do lado esquerdo todos os primos são distintos e diferentes de p_1, a unicidade da fatoração nos dá uma contradição. Portanto, nenhuma potência de p_1 maior que e_1 divide n e uma afirmação análoga vale para todos os outros primos.

12. Escreva $2^n = (m-1)(m+1)$ e use a unicidade da fatoração. A resposta é $n = 3$.

13. 3 na primeira jogada e 6 na segunda.

14. 5 na primeira jogada e 2 na segunda.

15. Uma possibilidade é tirar 5 na primeira jogada e 3 na segunda e, daí em diante, 5 na primeira jogada e 2 na segunda de cada vez.

16. Basta haver uma diferença de nove unidades entre a soma correta e a soma que foi calculada erradamente.

17. Basta haver uma diferença de nove unidades entre o produto correto e o produto que foi calculado erradamente.

18. Os resíduos possíveis de qualquer número por 4 são 0, 1, 2 e 3. Mas se o resíduo for 0 ou 2 o número é par. Logo um primo ímpar tem resíduo igual a 1 ou 3. Por exemplo, 5 tem resíduo 1 módulo 4, ao passo que 7 tem resíduo 3 módulo 4.

19. Se $a \equiv a' \pmod{n}$ e $b \equiv b' \pmod{n}$, então $a - a' = k \cdot n$ e $b - b' = \ell \cdot n$, onde k e ℓ são os respectivos cofatores. Subtraindo estas duas igualdades, obtemos

$$(a - b) - (a' - b') = k \cdot n - \ell \cdot n = (k - \ell) \cdot n;$$

que equivale a dizer que $a - b \equiv a' - b' \pmod{n}$.

20. Basta notar que o algarismo das unidades de um número é igual a seu resíduo módulo 10 e determinar quais os resíduos possíveis módulo 10 para um número par e para um múltiplo de 5.

21. As duas maneiras diferentes correspondem a escrever 10^4 como $10^3 \cdot 10$ ou $10^2 \cdot 10^2$ e usar os valores já encontrados para estas potências módulo 7.

22. A soma alternada (isto é, com os sinais alternando entre mais e menos) dos algarismos do número é divisível por 11 se, e somente se, o número é divisível por 11.

23. Faça *três fora*, como fizemos no caso dos *noves fora*.

24. Basta haver uma diferença de três unidades entre a soma correta e a soma que foi calculada erradamente.

25. Suponha que, dividindo n por m obtemos quociente q e resto r. Se a conta estiver correta devemos ter que n *noves fora* tem que ser igual a m *noves fora* vezes q *noves fora* mais r *noves fora*.

26. Os restos são, respectivamente, 1, 6 e 5.

27. Os valores são dados na tabela 7.1.

a	a_0	$\hat{a}$
87 645 564 348	8	8 764 556 434
85 735 214 421	1	8 573 521 442
981 231 111	1	98 123 111

Tabela 7.1: Exercício 27

28. Para 35 994 ser divisível por 7 é preciso que $-3\,599+8 = -3\,591$; para 3 591 ser divisível por 7 é preciso que $-359 + 2 = -357$; para 357 ser divisível por 7 é preciso que $-35+14 = -21$. Como 21 é divisível por 7, então 35 994 também é. O outro número não é divisível por 7.

29. Calcule 5^{25} módulo cada um dos primos ímpares até achar resíduo 1. A resposta é 11.

30. Os inversos são dados nas tabelas abaixo.

Resíduo	Inverso
1	1
2	4
3	5
4	2
5	3
6	6

Tabela 7.2: Inversos módulo 7

Resíduo	Inverso
1	1
2	7
3	9
4	10
5	8
6	11
7	2
8	5
9	3
10	4
11	6
12	12

Tabela 7.3: Inversos módulo 13

31. Basta lembrar que $n - 1 \equiv -1 \pmod{n}$.

32. Os inversos são dados nas tabelas abaixo.

Resíduo	Inverso
1	1
2	$\star$
3	$\star$
4	$\star$
5	5

Tabela 7.4: Inversos módulo 6

Resíduo	Inverso
1	1
2	8
3	$\star$
4	4
5	$\star$
6	$\star$
7	13
8	2
9	$\star$
10	$\star$
11	11
12	$\star$
13	7
14	14

Tabela 7.5: Inversos módulo 15

33. Os valores são os seguintes:

Resíduo	Inverso
2	3
3	2
4	3

Tabela 7.6: b tal que $a \cdot b \equiv 0 \pmod 6$

Resíduo	Inverso
3	5
5	3
6	5
9	5
10	3
12	5

Tabela 7.7: b tal que $a \cdot b \equiv 0 \pmod{13}$

34. Alguns exemplos são

$$1, 7, 5, 12, 22 \in V(5, 12)$$
$$1, 7, 15, 29, 50 \in V(7, 15)$$
$$5, 10, 15, 30, 35 \in V(15, 10)$$

mas talvez você escolha outros.

35. Dividindo a por m, temos que

$$a = m \cdot q' + r'.$$

Substituindo isto na equação (3.3.3),

$$a = (x_1 \cdot a + y_1 \cdot n) \cdot q' + r',$$

que equivale a

$$r' = (-x_1) \cdot a + (1 - y_1 \cdot q') \cdot n.$$

Assim, $r' \in V(a, n)$. Contudo, se $r' < M$ fosse positivo teríamos um elemento em $V(a, n)$ ainda menor que m, o que não é possível. Logo $r' = 0$, e m divide a.

36. Se houvesse um fator primo comum, teria que dividir 3. Como 3 é primo o fator teria que ser igual a 3. Mas se 3 dividisse $6 \cdot k - 2$, então também dividiria

$$3 \cdot (2 \cdot k) - (6 \cdot k - 2) = 2,$$

o que não é possível.

37. Como $6k \equiv -1 \pmod{6k+1}$ temos que os inversos são congruentes, respectivamente, a $-3k$, $-2k$ e $-k$.

38. 2 913.

39. 33.

40. A quantidade (mínima) total de arroz é $3 \cdot 105\,288$.

41. 10^{65} deixa resto 5 na divisão por 7 e 3^{78} deixa resto 1 na divisão por 7.

42. Ambos os restos são iguais a 3.

43. Os restos na divisão por 31 são 1 quando o dividendo é $2^{14^{45\,231}}$ e $2^{15^{498\,766\,543\,335\,231}}$ e 2 quando o dividendo é $64^{3^{9\,876}}$.

44. 3 tem ordem 6 módulo 7, 2 tem ordem 10 módulo 11, 5 tem ordem 3 módulo 31 e 7 tem ordem 6 módulo 43.

45. Se $a^k \equiv 1 \pmod{n}$, então $a^k - cn = 1$ para algum inteiro c. Mas se a e n forem pares, o lado esquerdo será um número par; logo não pode ser igual a 1.

46. A tabela com as ordens encontra-se abaixo:

Resíduo módulo 11	Ordem
1	1
2	10
3	5
4	5
5	5
6	10
7	10
8	10
9	5
10	2

Tabela 7.8: Ordens dos resíduos módulo 11

47. Os únicos resíduos que têm ordem módulo 12 são 1, que tem ordem 1 e 5, 7 e 11, que têm ordem 2 cada um.

48. A ordem de 3 módulo 31 é 30.

49. 6 tem ordem 3 módulo 43; $3^7 \equiv 37 \equiv -6 \pmod{43}$ e $3^{98\,745} \equiv 27 \pmod{43}$.

50. Pelo Teorema de Fermat, $3^{42} \equiv 1 \pmod{43}$. Mas,

$$98\,745 = 2\,351 \cdot 42 + 3.$$

Logo,

$$3^{98\,745} \equiv (3^{42})^{2\,351} \cdot 3^3 \equiv 27 \pmod{43}.$$

51. O resto é 16.

52. O resto é 1.

53. O resto é $p - 1$.

54. Os restos são dados pelas congruências

(a) $2^{495} \equiv 1 \pmod{15\,841}$;

(b) de $2^{41\,045} \equiv 32 \pmod{41\,041}$;

(c) de $2^{77} \equiv 1902 \pmod{2\,465}$.

59. Se duas chaves públicas têm um primo em comum então podemos descobri-lo, e com isso fatorar as chaves, calculando o máximo divisor comum das duas chaves públicas.

60. $p = 13$.

61. (a) Como $p^{\#}$ e $p^{\#} - 1$ são números consecutivos, têm que ser primos entre si por ???.

(b) Se houvesse infinitos números primos e o maior deles fosse p, então $p^{\#} - 1$ teria que ter um fator primo maior que p pelo resultado em (a), que é uma contradição.

(c) $p = 7$.

62. Os primos são:

5	11	17	23	29	41	47	53	59	71
83	89	101	107	113	131	137	149	167	173
179	191	197	227	233	239	251	257	263	269
281	293	311	317	347	353	359	383	389	401
419	431	443	449	461	467	479	491		

63. (b) Como $32 = 4 \cdot 7 + 4$, temos que

$$F(5) \cdot 5^4 \equiv (2^7 \cdot 5)^4 \cdot 2^4 + 5^4 \equiv 0 \pmod{641}.$$

(c) Como 5 é inversível módulo 641 podemos concluir de (b) que $F(5) \equiv 0 \pmod{641}$.

Desafios

1. três.

2. Os resíduos possíveis são iguais aos primos entre $n+1$ e $n!$.

3. Por exemplo, se $a > 2$ é um inteiro qualquer, então a tem inverso módulo $n = a^2 - 1$.

4. A primeira congruência nos diz que $x = a + my$ para algum inteiro y. Substituindo na segunda congruência, obtemos

$$my \equiv b - a \pmod{n}.$$

Se m e n não são primos entre si, não podemos simplesmente inverter o m para deixar o y livre. Convertendo esta última congruência em uma expressão de inteiros, temos que

$$my = b - a + nk, \text{ para algum inteiro } k.$$

Em outras palavras,

$$my - nk = b - a.$$

Se d é o máximo divisor comum entre m e n então existem inteiros m' e n' tais que $m = dm'$ e $n = dn'$. Substituindo na última equação, obtemos

$$(m'y - n'k)d = b - a.$$

Portanto, para que haja solução é preciso que d divida $b-a$. Se $b-a=dc$ para algum inteiro c, então

$$m'y - n'k = c,$$

que nos dá $m'y \equiv c \pmod{n'}$. Como cancelamos o máximo divisor comum entre m e n, os inteiros são m' e n' são primos entre si e m' pode ser invertido em $m'y \equiv c \pmod{n'}$, o que nos dá o valor de y. Portanto, quando d divide $b-a$ o sistema tem solução.

5. (a) Pelo Teorema de Fermat, $a^{p-1} \equiv 1 \pmod{p}$.

(b) Dividindo $p-1$ por k obtemos $p-1 = kq+r$, donde

$$a^{p-1} \equiv (a^k)^q \cdot a^r \equiv 1 \cdot a^r \pmod{p},$$

pela definição de k. Como $a^{p-1} \equiv 1 \pmod{p}$, pelo Teorema de Fermat, podemos concluir que $a^r \equiv 1 \pmod{p}$.

(c) Se $r \neq 0$ então teríamos que $0 < r < k$ satisfaz $a^r \equiv 1 \pmod{p}$, o que é impossível pela definição de k como sendo o *menor* inteiro positivo tal que $a^k \equiv 1 \pmod{p}$. Logo, $r = 0$.

(d) Substituindo $r = 0$ em $p-1 = kq+r$, temos que $p-1 = kq$, de modo que k tem que dividir $p-1$.

6. $p = 3$.

7. Temos que

$$m = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q) + 1.$$

Logo,

$$(p+q) = n - m + 1.$$

Para achar p e q quando conhecemos $p+q$ e pq basta resolver uma equação quadrática. Outra solução consiste em notar que

$$(p-q)^2 = (p+q)^2 - 2pq = (n-m+1)^2 - 2n.$$

Com isto temos $p+q$ e $p-q$ em função de n e m e podemos resolver um sistema linear para achar p e q.

8. (a) Qualquer número dividido por 4 tem resto 0, 1, 2 ou 3. Como um primo diferente de 2 é ímpar, os únicos resíduos possíveis módulo 4 neste caso são 1 e 3.

(b) Têm resíduo 1 módulo 4 os primos $5, 13, 17, 29$ e 37 e têm resíduo 3 módulo 4 os primos $3, 7, 11, 19$ e 23.

(c) $(4n+1)(4k+1) = 4(4nk+n+k)+1$ ou use congruência módulo 4. Note que foi preciso escolher letras diferentes k e n, porque os números $4n+1$ e $4k+1$ *podem ser diferentes.*

(d) Não. Por exemplo $3 \cdot 7 = 21 = 4 \cdot 5 + 1$.

(e) Pelo Teorema de Fatoração Única, o número $4(p_1 \ldots p_k)+3$ pode ser escrito como um produto de primos. Estes primos *não* podem pertencer ao conjunto $\{p_1, \ldots, p_k\}$. Só nos resta mostrar que os primos na fatoração de $4(p_1 \ldots p_k) + 3$ não podem ser todos da forma $4n+1$. Mas se fosse este

o caso, o produto destes primos seria da forma $4n+1$ por (c), o que não é verdade pois $4(p_1 \dots p_k)+3$ deixa resto 3 na divisão por 4.

(f) Suponha, por absurdo, que $\{3, p_1, \dots, p_k\}$ é o conjunto de todos os primos da forma $4n+3$ e aplique (e).

9. (a) Mostre que

$$R(n) = (10^n - 1)/9 = \frac{9 \cdots 9}{9} = 1 \cdots 1.$$

(b) Use que

$$\frac{10^{kr}-1}{10^k-1} = 10^{k(r-1)} + 10^{k(r-2)} + \cdots + 10^k + 1.$$

(c) Como $6 = 2 \cdot 3$, temos que $R(2) = 11$ e $R(3) = 111 = 3 \cdot 37$ dividem $R(6)$ por (b). Mas,

$$\frac{R(6)}{3 \cdot 11 \cdot 37} = 91 = 7 \cdot 13.$$

Logo,

$$R(6) = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37.$$

(d) Consequência imediata de (b).

(e) Como $R(7) - 1 = 10 \cdot R(6)$ podemos usar a fatoração de $R(6)$ obtida acima para facilitar o cálculo do resíduo de 2 módulo $R(7)$, que dá 553 891.

Referências Bibliográficas

[1] COELHO, S. P.; POLCINO MILIES, C. *Números: uma Introdução à Matemática*. São Paulo: Editora da Universidade de São Paulo, 2 000.

[2] COUTINHO, S. C. *Números inteiros e criptografia RSA*. Série de Computação e Matemática n. 2, IMPA e SBM, segunda edição (revisada e ampliada), 2 000.

[3] HEFEZ, A. *Elementos de Aritmética*. Sociedade Brasileira de Matemática, 2 005.