Capítulo 6

Inteiros, divisores, e primos

Neste capítulo discutimos propriedades de inteiros. Essa área da matemática é chamada *teoria dos números*, e é um campo verdadeiramente venerável; suas raízes estão lá atrás cerca de 2500 anos, bem no início da matemática grega. Poder-se-ia pensar que após 2500 anos de pesquisa, saber-se-ia essencialmente tudo sobre o assunto. Mas veremos que isso não é o caso: existem questões muito simples e naturais que não podemos responder; e existem outras questões simples e naturais para as quais uma resposta somente foi encontrada nos últimos anos!

6.1 Divisibilidade de inteiros

Começamos com algumas noções muito básicas concernentes a inteiros. Sejam a e b dois inteiros. Dizemos que a *divide* b, ou a *é um divisor de* b, ou b *é um múltiplo de* a (essas frases dizem a mesma coisa), se existe um inteiro m tal que $b = am$. Na notação: $a|b$. Se a não é um divisor de b, então escrevemos $a \nmid b$. Se $a \neq 0$, então isso significa que a proporção b/a é um inteiro.

Se $a \nmid b$, e $a > 0$, então podemos ainda dividir b por a com resto. O resto r da divisão $b : a$ é um inteiro que satisfaz $0 \leq r < a$. Se o quociente da divisão com resto é q, então temos

$$b = aq + r.$$

Essa é uma maneira muito útil de pensar sobre uma divisão com resto.

Você provavelmente viu essas noções antes; os exercícios seguintes devem ajudá-lo(a) a conferir se você se lembra o bastante.

6.1 Verifique (usando a definição) que $1|a$, $-1|a$, $a|a$ e $-a|a$ para todo inteiro a.

6.2 O que significa para a, em termos mais corriqueiros, se (a) $2|a$; (b) $2 \nmid a$; (c) $0|a$.

6.3 Prove que

(a) se $a|b$ e $b|c$ então $a|c$;

(b) se $a|b$ e $a|c$ então $a|b + c$ e $a|b - c$;

(c) se $a, b > 0$ e $a|b$ então $a \leq b$;

(d) se $a|b$ e $b|a$ então $a = b$ ou $a = -b$.

6.4 Seja r o resto da divisão $b : a$. Assuma que $c|a$ e $c|b$. Prove que $c|r$.

6.5 Assuma que $a|b$, e que $a, b > 0$. Seja r o resto da divisão $c : a$, e suponha que s seja o resto da divisão $c : b$. Qual é o resto da divisão $s : a$?

6.6 (a) Prove que para todo inteiro a, $a - 1|a^2 - 1$.

(b) Generalizando, para todo inteiro a e todo inteiro positivo n,

$$a - 1|a^n - 1.$$

6.2 Os primos e sua história

Um inteiro $p > 1$ é chamado um *número primo* se ele não é divisível por qualquer inteiro diferente de $1, -1, p$ e $-p$. Uma outra maneira de dizer isso é que um inteiro $p > 1$ é um primo se ele não pode ser escrito como o produto de dois inteiros positivos menores que ele. Um inteiro $n > 1$ que não é um primo é chamado *composto* (o número 1 é considerado nem primo, nem composto). Por conseguinte, $2, 3, 5, 7, 11$ são primos, mas $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, $9 = 3 \cdot 3$, $10 = 2 \cdot 5$ não são primos. A tabela 6.1 mostra os primos até 500.

Os primos têm fascinado as pessoas desde os tempos antigos. Sua seqüência parece muito irregular, e mesmo assim sob inspeção mais próxima ela parece carregar uma porção de estrutura escondida. Os gregos antigos já sabiam que existe uma quantidade infinita de tais números. (Não apenas eles sabiam isso; eles o provaram!)

Não era fácil provar quaisquer fatos adicionais sobre primos. Sua seqüência é razoavelmente suave, mas ela tem buracos e focos densos (veja a Figura 6.1). Quão grande são tais buracos? Por exemplo, existe um número primo com um número dado qualquer de dígitos? A resposta a essa questão será importante para nós quando discutirmos sobre criptografia. A resposta é na afirmativa, mas esse fato não foi provado até meados do século XIX, e muitas questões semelhantes estão abertas ainda hoje.

Figura 6.1: Um código de barra dos primos até 1000

Uma nova onda de desenvolvimentos na teoria dos números primos veio com a popularização de computadores. Como você decide sobre se um inteiro positivo n

1, ***2***, ***3***, 4, ***5***, 6, ***7***, 8, 9, 10, ***11***, 12, ***13***, 14, 15, 16, ***17***, 18, ***19***, 20, 21, 22, ***23***, 24, 25, 26, 27, 28, ***29***, 30, ***31***, 32, 33, 34, 35, 36, ***37***, 38, 39, 40, ***41***, 42, ***43***, 44, 45, 46, ***47***, 48, 49, 50, 51, 52, ***53***, 54, 55, 56, 57, 58, ***59***, 60, ***61***, 62, 63, 64, 65, 66, ***67***, 68, 69, 70, ***71***, 72, ***73***, 74, 75, 76, 77, 78, ***79***, 80, 81, 82, ***83***, 84, 85, 86, 87, 88, ***89***, 90, 91, 92, 93, 94, 95, 96, ***97***, 98, 99, 100, ***101***, 102, ***103***, 104, 105, 106, ***107***, 108, ***109***, 110, 111, 112, ***113***, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, ***127***, 128, 129, 130, ***131***, 132, 133, 134, 135, 136, ***137***, 138, ***139***, 140, 141, 142, 143, 144, 145, 146, 147, 148, ***149***, 150, ***151***, 152, 153, 154, 155, 156, ***157***, 158, 159, 160, 161, 162, ***163***, 164, 165, 166, 167, 168, 169, 170, 171, 172, ***173***, 174, 175, 176, 177, 178, ***179***, 180, ***181***, 182, 183, 184, 185, 186, 187, 188, 189, 190, ***191***, 192, ***193***, 194, 195, 196, ***197***, 198, ***199***, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, ***211***, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, ***223***, 224, 225, 226, ***227***, 228, ***229***, 230, 231, 232, 233, 234, 235, 236, 237, 238, ***239***, 240, ***241***, 242, 243, 244, 245, 246, 247, 248, 249, 250, ***251***, 252, 253, 254, 255, 256, ***257***, 258, 259, 260, 261, 262, ***263***, 264, 265, 266, 267, 268, ***269***, 270, ***271***, 272, 273, 274, 275, 276, ***277***, 278, 279, 280, ***281***, 282, ***283***, 284, 285, 286, 287, 288, 289, 290, 291, 292, ***293***, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, ***307***, 308, 309, 310, ***311***, 312, ***313***, 314, 315, 316, ***317***, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, ***331***, 332, 333, 334, 335, 336, ***337***, 338, 339, 340, 341, 342, 343, 344, 345, 346, ***347***, 348, ***349***, 350, 351, 352, ***353***, 354, 355, 356, 357, 358, ***359***, 360, 361, 362, 363, 364, 365, 366, ***367***, 368, 369, 370, 371, 372, ***373***, 374, 375, 376, 377, 378, ***379***, 380, 381, 382, ***383***, 384, 385, 386, 387, 388, ***389***, 390, 391, 392, 393, 394, 395, 396, ***397***, 398, 399, 400, ***401***, 402, 403, 404, 405, 406, 407, 408, ***409***, 410, 411, 412, 413, 414, 415, 416, 417, 418, ***419***, 420, ***421***, 422, 423, 424, 425, 426, 427, 428, 429, 430, ***431***, 432, ***433***, 434, 435, 436, 437, 438, ***439***, 440, 441, 442, ***443***, 444, 445, 446, 447, 448, ***449***, 450, 451, 452, 453, 454, 455, 456, ***457***, 458, 459, 460, ***461***, 462, ***463***, 464, 465, 466, ***467***, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, ***479***, 480, 481, 482, 483, 484, 485, 486, ***487***, 488, 489, 490, ***491***, 492, 493, 494, 495, 496, 497, 498, ***499***, 500

Tabela 6.1: Os primos até 500

é primo? Certamente isso é um problema finito (você pode tentar todos os inteiros positivos menores para ver se algum deles é um divisor próprio), mas tais métodos simples ficam impraticáveis tão logo o número de dígitos passe de 20 ou algo assim.

Faz apenas 20 anos desde que algoritmos muito mais eficientes (programas de computador) existem para testar se um dado inteiro é um primo. Daremos uma olhada nesses métodos mais adiante. Usando esses métodos, pode-se agora um tanto facilmente determinar se um número com 1000 dígitos é ou não um primo.

Se um inteiro maior que 1 não é ele próprio um primo, então ele pode ser escrito como um produto de primos: podemos escrevê-lo como um produto de dois inteiros positivos menores que ele; se um desses não é um primo, escrevemo-lo como o produto de dois inteiros menores que ele etc.; mais cedo ou mais tarde temos que termina com somente primos. Os gregos antigos também sabiam (e provaram) um fato mais sutil sobre essa representação: que *ela é única*. O que isso quer dizer é que não existe outra maneira de escrever n como um produto de primos (exceto, é claro, podemos multiplicar os mesmos primos numa ordem diferente). Para provar isso requer alguma sofisticação (como veremos na próxima seção), e reconhecer a necessidade de tal resultado foi uma senhora conquista; mas tudo isso tem mais de 2000 anos!

É realmente surpreendente que, ainda hoje, nenhuma maneira eficiente é conhecida para se *encontrar* tal decomposição. É claro que supercomputadores poderosos e

sistema massivamente paralelos podem ser usados para encontrar decomposições por meio da força bruta para números um tanto grandes; o recorde atual é cerca de 140 dígitos, e a dificuldade cresce muito rapidamente (exponencialmente) com o número de dígitos. Para encontrar a decomposiçàо prima de um dado número com 400 dígitos, por qualquer dos métodos conhecidos, está muito além das possibilidades dos computadores no futuro previsível.

6.3 Fatoração em primos

Vimos que todo inteiro maior que 1 que não é um primo ele próprio pode ser escrito como um produto de primos. Podemos mesmo dizer que *todo* inteiro positivo pode ser escrito como um produto de primos: primos podem ser considerados como "produtos com um fator", e o inteiro 1 pode ser pensado como o "produto vazio". Com isso em mente, podemos enunciar e provar o seguinte teorema, anunciado acima, às vezes chamado de "Teorema Fundamental da Teoria dos Números".

Teorema 6.3.1 *Todo inteiro positivo pode ser escrito como o produto de primos, e essa fatoração é única a menos da ordem dos fatores primos.*

Prova. Provamos esse teorema por meio de uma versão da indução, que é às vezes chamada de argumenteo do "criminoso mínimo". A prova é indireta: Supomos que a asserção é falsa, e usando essa suposição, derivamos uma contradição lógica.

Portanto assumimos que existe um inteiro com duas fatorações diferentes; chame tal inteiro um "criminoso". Pode haver muitos criminosos, mas consideramos o *menor* deles. Sendo um criminoso, esse tem pelo menos duas fatorações diferentes:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_m = q_1 \cdot q_2 \cdot \ldots \cdot q_k \,.$$

Podemos assumir que p_1 é o menor primo ocorrendo nessas fatorações. (De fato, se necessário, podemos trocar o lado esquerdo e o lado direito de modo que o menor primo em qualquer das duas fatorações ocorre na esquerda; e então mudamos a ordem dos fatores no lado esquerdo de modo que o menor fator vem primeiro. Na gíria usual da matemática, dizemos que podemos assumir que p_1 é o menor primo *sem perda de generalidade*.) Vamos produzir um criminoso menor; isso será uma contradição, pois assumimos que n era o menor deles.

O número p_1 não pode ocorrer entre os fatores q_i, caso contrário podemos dividir ambos os lados por p_1 e obter um criminoso menor.

Divida cada q_i por p_1 com resto: $q_i = p_1 a_i + r_i$, onde $0 \leq r_i < p_1$. Sabemos que $r_i \neq 0$, pois um primo não pode ser um divisor de um outro primo.

Faça $n' = r_1 \cdot \ldots \cdot r_k$. Mostramos que n' é um criminoso menor. Trivialmente $r_i < p_1 < q_i$, e portanto $n' = r_1 r_2 \ldots r_k < q_1 q_2 \ldots q_k = n$. Mostramos que n' também tem duas fatorações diferentes em primos. Uma dessas pode ser obtida da definição $n' = r_1 r_2 \ldots r_k$. Aqui os fatores podem não ser primos, mas podemos quebrá-los em produtos de primos, de modo que terminamos com uma decomposição de n'.

Para obter uma outra decomposição, observamos que $p_1|n'$. De fato, podemos escrever a definição de n' na forma

$$n' = (q_1 - a_1p_1)(q_2 - a_2p_1)\ldots(q_k - a_kp_1),$$

e se expandimos, então todo termo será divisível por p_1. (Um dos termos é $q_1 \cdot \ldots \cdot q_k$, que é igual a n e portanto divisível por p_1. Todos os outros termos contêm p_1 como um fator.) Agora dividimos n' por p_1 e então continuamos a fatorar n'/p_1, para obter uma fatoração de n'.

Mas, essas fatorações são diferentes? Sim! O primo p_1 ocorre na segunda, mas ela não pode ocorrer na primeira, onde todo fator primo é menor que p_1.

Por conseguinte encontramos um criminoso menor. Como n era supostamente o menor entre todos os criminosos, isso é uma contradição. A única maneira de resolver essa contradição é concluir que não existem criminosos; nossa "suposição indireta" era falsa, e nenhum inteiro pode ter duas fatorações primas diferentes. □

6.7 Leia cuidadosamente o seguinte argumento do "criminoso mínimo":

> ASSERÇÃO. *Todo inteiro negativo é ímpar.*
>
> PROVA. Suponha, para chegar a uma contradição, que existem inteiros negativos que são pares. Chame esses inteiros de criminosos, e suponha que n seja um criminoso mínimo. Considere o número $2n$. Esse é menor que n (recorde que n é negativo!), portanto ele é um criminoso menor. Mas assumimos que n era o criminoso mínimo, portanto isso é uma contradição.

Essa asserção é obviamente errada. Onde está o erro na prova?

Como uma aplicação do Teorema 6.3.1, provamos um fato que era conhecido dos Pitagoreanos (estudantes de Pitágoras) no século VI a.C.

Teorema 6.3.2 *O número $\sqrt{2}$ é irracional.*

(Um número real é *irracional* se ele não pode ser escrito como a fração de dois inteiros. Para os Pitagoreanos, a questão surgiu da geometria: eles queriam saber se a diagonal de um quadrado é "comensurável" com seu lado, i.e., se existe um segmento qualquer que esteja contido em ambos um número inteiro de vezes. O teorema acima respondeu essa questão na negativa, causando um tumulto substancial em nossas tropas.)

Prova. Damos uma prova indireta novamente: supomos que $\sqrt{2}$ é racional, e derivamos uma contradição. O que a suposição indireta significa é que $\sqrt{2}$ pode ser escrita como o quociente de dois inteiros positivos: $\sqrt{2} = \frac{a}{b}$. Elevando ao quadrado ambos os lados e rearrumando, obtemos $2b^2 = a^2$.

Agora considere a fatoração prima de ambos os lados, e, em particular, o número primo 2 em ambos os lados. Suponha que 2 ocorra m vezes na fatoração prima de a e n vezes na fatoração prima de b. Então ele ocorre $2m$ vezes na fatoração prima de a^2. Por outro lado, ele ocorre $2n$ vezes na fatoração prima de b^2 e por conseguinte ele ocorre $2n + 1$ vezes na fatoração prima de $2b^2$. Como $2b^2 = a^2$, e a fatoração prima é única, temos que ter $2n + 1 = 2m$. Mas isso é impossível pois $2n + 1$ é ímpar mas $2m$ is par. Essa contradição prova que $\sqrt{2}$ tem que ser irracional. □

6.8 Existe algum primo par?

6.9 (a) Prove que se p é um primo, a e b são inteiros, e $p|ab$, então $p|a$ ou $p|b$ (ou ambos).

(b) Suponha que a e b sejam inteiros e $a|b$. Suponha também que p é um primo e $p|b$ mas $p \nmid a$. Prove que p é um divisor da fração b/a.

6.10 Prove que a fatoração prima de um número n contém no máximo $\log_2 n$ fatores.

6.11 Seja p um primo e $1 \leq a \leq p-1$. Considere os números $a, 2a, 3a, \ldots, (p-1)a$. Divida cada um deles por p, para obter restos $r_1, r_2, \ldots, r_{p-1}$. Prove que todo inteiro de 1 a $p-1$ ocorre *exatamente uma vez* entre esses restos.

[Dica: Primeiro prove que nenhum resto pode ocorrer duas vezes.]

6.12 Prove que se p é um primo, então $\sqrt{p}$ é irracional. De maneira mais geral, prove que se n é um inteiro que não é um quadrado, então $\sqrt{n}$ é irracional.

6.13 Tente formular e provar um teorema ainda mais geral sobre a irracionalidade dos números $\sqrt[k]{n}$.

6.4 Sobre o conjunto de primos

O teorema seguinte era conhecido de Euclides no século III a.C.

Teorema 6.4.1 *Existe uma quantidade infinita de primos.*

Prova. O que precisamos fazer é mostrar que para todo inteiro positivo n, existe um número primo maior que n. Para esse fim, considere o número $n! + 1$, e qualquer divisor primo p dele. Mostramos que $p > n$. Novamente, usamos uma prova indireta, supondo que $p \leq n$ e derivando uma contradição. Se $p \leq n$ então $p|n!$, pois ele é um dos inteiros cujo produto é $n!$. Sabemos também que $p|n!+1$, e portanto p é um divisor da diferença $(n!+1) - n! = 1$. Mas isso é impossível, e por conseguinte p tem que ser maior que n. □

Se olharmos para vários gráficos ou tabelas de primos, nossa principal impressão é que existe bastante irregularidade neles. Por exemplo, a Figura 6.1 representa cada primo até 1000 por uma barra. Vemos grandes "lacunas" e então vemos também primos que são muito próximos. Podemos provar que essas lacunas ficam maiores e maiores quando consideramos números maiores e maiores; em algum lugar lá adiante existe uma cadeia de 100 números compostos consecutivos, em algum lugar (ainda mais longe) existe uma cadeia de 1000 números compostos consecutivos, etc. Para enunciar isso em uma forma matemática:

Teorema 6.4.2 *Para todo inteiro positivo k, existem k inteiros compostos consecutivos.*

Prova. Podemos provar esse teorema por um argumento um tanto semelhante à prova do teorema 6.4.1. Seja $n = k + 1$ e considere os números

$$n! + 2,\ n! + 3,\ \ldots,\ n! + n.$$

Algum desses pode ser um primo? A resposta é não: o primeiro número é par, pois $n!$ e 2 são ambos pares. O segundo número é divisível por 3, pois $n!$ e 3 são ambos divisíveis 3 (assumindo que $n > 2$). Em geral $n! + i$ é divisível por i, para todo $i = 2, 3, \ldots, n$. Daí esses números não podem ser primos, e portanto encontramos $n - 1 = k$ números compostos consecutivos. □

Que tal a questão oposta, encontrar primos muito próximos um ao outro? Como todos os primos exceto 2 são ímpares, a diferença dos dois primos tem que ser pelo menos dois, exceto para 2 e 3. Dois primos cuja diferença é 2 são chamados *primos gêmeos*. Por conseguinte $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$ são primos gêmeos. Olhando para a tabela dos primos até 500, encontramos muitos primos gêmeos; cálculo extensivo mostra que existem primos gêmeos com centenas de dígitos. Entretanto, não se sabe se existe uma quantidade infinita de primos gêmeos! (Quase certamente existe, mas nenhuma prova desse fato foi encontrada, apesar dos esforços de muitos matemáticos durante mais de 2000 anos!)

Uma outra maneira de dar uma volta no Teorema 6.4.2: quão grande podem ser essas lacunas, em relação ao ponto onde eles se encontram na reta dos números? Poderia acontecer que não haja de jeito nenhum primos com, digamos, 100 dígitos? Essa é novamente uma questão muito difícil, mas aqui sabemos de fato a resposta. (Não, isso não acontece.)

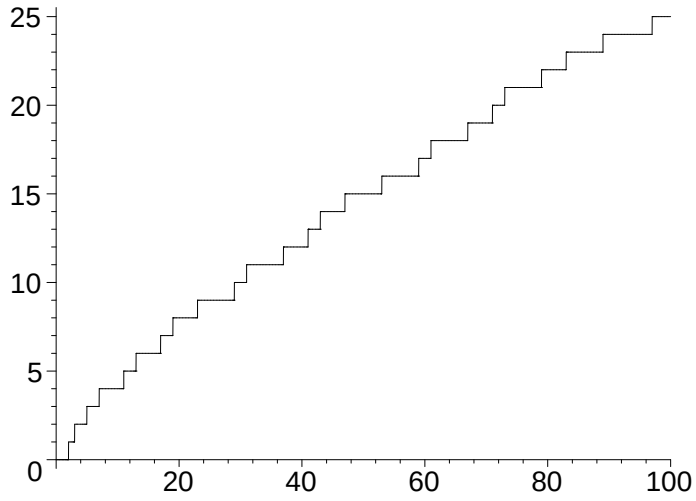

Figura 6.2: O grafo de $\pi(n)$ de 1 a 100

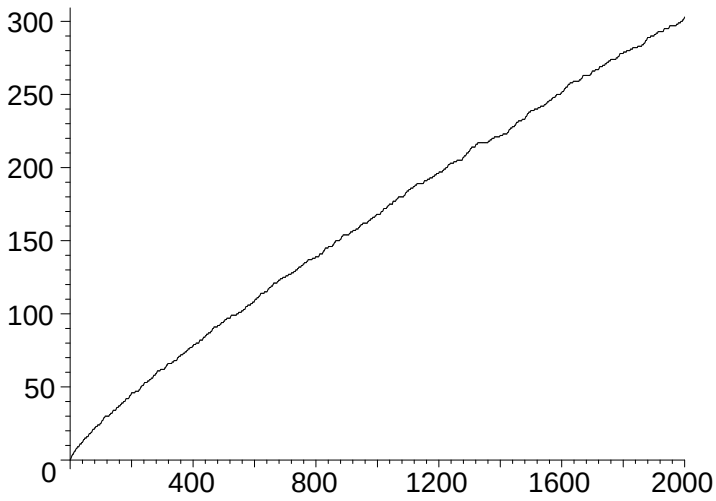

Figura 6.3: O grafo de $\pi(n)$ de 1 a 2000

Uma das questões mais importantes sobre primos é: quantos primos existem até um dado número n? Representamos o número de primos até n por $\pi(n)$. A Figura 6.2 ilustra o grafo dessa função na faixa de 1 a 100, e a Figura 6.3, na faixa de 1 a 2000. Podemos ver que a função cresce razoavelmente suavemente, e que sua inclinação decresce lentamente. Uma fórmula exata para $\pi(n)$ é certamente impossível de obter. Em torno do ano de 1900, um resultado poderoso chamado o Teorema do Número Primo foi provado por dois matemáticos, Hadamard e de la Vallée Poussin.

Teorema 6.4.3 (O Teorema do Número Primo) *Suponha que $\pi(n)$ represente o número de primos entre $1, 2, \ldots, n$. Então*

$$\pi(n) \sim \frac{n}{\ln n}$$

(Aqui $\ln n$ significa "logaritmo natural", i.e., logaritmo na base $e = 2,718281\ldots$. Recordemos também que a notação quer dizer que o quociente

$$\pi(n) \Big/ \frac{n}{\ln n}$$

ficará arbitrariamente próximo a 1 se n for suficientemente grande.)

A prova do teorema do número primo é muito difícil; o fato de que o número de primos até n é cerca de $n/\ln n$ foi observado empiricamente no século XVIII, mas levou mais de 100 anos até que Hadamard e de la Vallée Poussin o provaram em 1896.

Como uma ilustração do uso desse teorema, vamos encontrar a resposta a uma questão que pusemos na introdução: quantos primos com (digamos) 200 dígitos existem? Obtemos a resposta subtraindo o número de primos até 10^{199} do número de

primos até 10^{200}. Pelo Teorema do Número Primo, esse número é cerca de

$$\frac{10^{200}}{200\ln 10} - \frac{10^{199}}{199\ln 10} \approx 1,95 \cdot 10^{197}.$$

Isso é um bocado de primos! Comparando isso com o número total de inteiros positivos com 200 dígitos, que sabemos que é $10^{200} - 10^{199} = 9 \cdot 10^{199}$, obtemos

$$\frac{9 \cdot 10^{199}}{1,95 \cdot 10^{197}} \approx 460.$$

Por conseguinte, entre os inteiros com 200 dígitos, um em cada 460 é um primo.

(Advertência: Esse argumento não é preciso; a principal fonte de preocupação é que no teorema do número primo, apenas enunciamos que $\pi(n)$ é próximo a $n/\ln n$ se n for suficientemente grande. Pode-se dizer mais sobre quão grande n tem que ser para se ter, digamos, um erro menor que 1 por cento, mas isso leva a questões ainda mais difíceis, que ainda hoje não estão completamente resolvidas.)

Há muitas outras observações simples que se pode fazer olhando para as tabelas de primos, mas elas tendem a ser muito difíceis e a maioria delas não estão resolvidas ainda hoje, em alguns casos após 2.500 anos de tentativas. Mencionamos o problema sobre se existe uma quantidade infinita de primos gêmeos.

Um outro famoso problema não-resolvido é a *conjectura de Goldbach*. Ela enuncia que todo inteiro par maior que 2 pode ser escrito como a soma de dois primos. (Goldbach também formulou uma conjectura sobre números ímpares: todo inteiro ímpar maior que 5 pode ser escrito como a soma de três primos. Essa conjectura foi essencialmente provada, usando métodos muito profundos, por Vinogradov nos anos 1930's. Dizemos "essencialmente" pois a prova somente funciona para números que são muito grandes, e a possibilidade de um número finito de exceções permanece aberta.)

P. L. Chebyshev

Suponha que temos um inteiro n e queremos saber quão breve após n podemos ter certeza de encontrar um primo. Por examplo, quão pequeno, ou grande, é o primeiro primo com pelo menos 100 dígitos? Nossa prova da infinitude de primos diz que para todo n, existe um primo entre n e $n! + 1$. Esse é um enunciado muito fraco;

ele diz, por exemplo, que existe um primo entre 10 e $10! + 1 = 3628801$, enquanto que, obviamente, o próximo primo é 11. Chebychev provou no século XIX que existe sempre um primo entre n e $2n$. Está agora provado que existe sempre um primo entre dois cubos consecutivos (digamos, entre $27 = 3^3$ e $64 = 4^3$). Mas é um outro problema famoso e não resolvido se existe sempre um primo entre dois quadrados consecutivos. (Experimente com isso: você encontrará, na realidade, muitos primos. Por exemplo, entre $100 = 10^2$ e $121 = 11^2$ encontramos 101, 103, 107, 109, 113. Entre $100^2 = 10.000$ e $101^2 = 10201$ encontramos 10007, 10009, 10037, 10039, 10061, 10067, 10069, 10079, 10091, 10093, 10099, 10103, 10111, 10133, 10139, 10141, 10151, 10159, 10163, 10169, 10177, 10181, 10193.)

6.14 Mostre que entre os números de k-dígitos, um em cada $2, 3k$ é um primo.

6.5 O "Pequeno" Teorema de Fermat

P. de Fermat

Primos são importantes porque podemos compor todo inteiro a partir deles; mas acontece que eles também têm muitas outras, e frequentemente surpreendentes, propriedades. Uma dessas foi descoberta pelo matemático francês Pierre de Fermat (1601–1655), agora chamado "Pequeno" Teorema de Fermat.

Teorema 6.5.1 *Se p é um primo e a é um inteiro, então $p|a^p - a$.*

Antes de provar esse teorema, observamos que é um tanto frequentemente enunciado na seguinte forma: *se p é um primo e a é um inteiro não divisível por p, então*

$$p|a^{p-1} - 1. \tag{6.1}$$

O fato de que essas duas asserções são equivalentes (no sentido de que se conhecemos a veracidade de uma, é fácil de provar a outra) é deixado ao leitor como Exercício 6.66.

Para provar o Pequeno Teorema de Fermat, precisamos de um lema, que enuncia uma outra propriedade de divisibilidade de primos (mas é mais fácil de provar):

Lema 6.5.2 *Se p é um primo e $0 < k < p$, então $p|\binom{p}{k}$.*

Prova. Sabemos pelo teorema 1.8.1 que

$$\binom{p}{k} = \frac{p(p-1)\cdot\ldots\cdot(p-k+1)}{k(k-1)\cdot\ldots\cdot 1}.$$

Aqui p divide o numerador, mas não o denominador, pois todos os fatores no denominador são menores que p, e sabemos pelo exercício 6.9(a) que se um primo p não divide quaisquer desses fatores, então ele não divide o produto. Daí segue (veja o exercício 6.9(b)) que p é um divisor de $\binom{p}{k}$. □

Prova. [do Teorema 6.5.1] Agora podemos provar o Teorema de Fermat por indução sobre a. A asserção é trivialmente verdadeira se $a = 0$. Suponha que $a > 0$, e faça $a = b + 1$. Então

$$\begin{aligned} a^p - a &= (b+1)^p - (b+1) \\ &= b^p + \binom{p}{1}b^{p-1} + \ldots + \binom{p}{p-1}b + 1 - b - 1 \\ &= (b^p - b) + \binom{p}{1}b^{p-1} + \ldots + \binom{p}{p-1}b. \end{aligned}$$

Aqui a expressão $b^p - b$ nos parênteses é divisível por p pela hipótese da indução, enquanto que os outros termos são divisíveis por p pelo lema 6.5.2. Segue que $a^p - a$ é também divisível por p, o que completa a indução. □

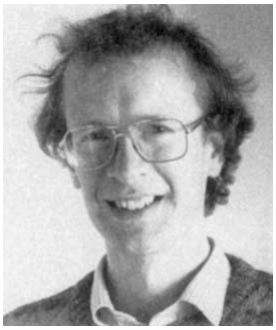

Figura 6.4: A.J. Wiles

Vamos fazer aqui uma observação sobre a história da matemática. Fermat é mais famoso por seu "Último" teorema, que é a seguinte asserção:

Se $n > 2$, então a soma das n-ésimas potências de dois inteiros positivos nunca é a n-ésima potência de um inteiro positivo.

(A suposição de que $n > 2$ é essencial: existem exemplos de dois quadrados cuja soma é um terceiro quadrado: por exemplo, $3^2 + 4^2 = 5^2$, ou $5^2 + 12^2 = 13^2$. Na verdade, existe uma quantidade infinita de tais triplas de quadrados, veja o exercício 6.25.)

Fermat afirmou em uma nota que ele provou isso, mas nunca escreveu a prova. Esse enunciado permaneceu como talvez o mais famoso problema não resolvido em matemática até 1995, quando Andrew Wiles (em uma parte com a ajuda de Robert Taylor) finalmente o provou.

6.15 Mostre por meio de exemplos que nem a assercão no lema 6.5.2 nem o Pequeno Teorema de Fermat permanecem válidos se descartarmos a suposição de que p é um primo.

6.16 Considere um p-ágono regular, e para um k fixo ($1 \leq k \leq p-1$), considere todos os subconjuntos de k-elementos do conjunto de seus vértices. Ponha todos esses k-subconjuntos em um número de caixas: colocamos dois k-subconjuntos na mesma caixa se eles podem ser rotacionados um ao outro. Por exemplo, todos os k-subconjuntos consistindo de k vértices consecutivos pertencerão a uma e à mesma caixa.

(a) Prove que se p é um primo, então cada caixa conterá exatamente p dessas cópias rotacionadas.

(b) Mostre por meio de um exemplo que (a) não permanece verdadeira se descartarmos a suposição de que p é um primo.

(c) Use (a) para dar uma nova prova do Lema 6.5.2.

6.17 Imagine números escritos na base a, com no máximo p dígitos. Ponha dois números na mesma caixa se eles resultam de um deslocamento cíclico um do outro. Quantos estarão em cada classe? Dê uma nova prova do teorema de Fermat dessa maneira.

6.18 Dê uma terceira prova do "Pequeno Teorema" de Fermat baseada no exercício 6.11.
[Dica: considere o produto $a(2a)(3a)\ldots((p-1)a)$.]

6.6 O Algoritmo Euclideano

Até agora, discutimos diversas noções e resultados relativos a inteiros. Agora voltamos nossa atenção para a questão de como fazer cálculos em conexão com esses resultados. Como decidir se um dado número é ou não um primo? Como encontrar a fatoração prima de um número?

Podemos fazer aritmética básica: adição, subtração, multiplicação, divisão com resto eficientemente, e não discutiremos isso aqui.

A chave para uma teoria dos números algorítmica mais avançada é um algoritmo que computa o *máximo divisor comum* de dois inteiros positivos a e b. Isso é definido como o maior inteiro positivo que é um divisor de ambos. (Como 1 é sempre um divisor comum, e nenhum divisor comum é maior que qualquer dos dois inteiros, essa

definição faz sentido.) O máximo divisor comum de a e b é representado por $\mathrm{mdc}(a, b)$. Por conseguinte

$$\mathrm{mdc}(1,6) = 1, \qquad \mathrm{mdc}(2,6) = 2, \qquad \mathrm{mdc}(3,6) = 3, \qquad \mathrm{mdc}(4,6) = 2,$$

$$\mathrm{mdc}(5,6) = 1, \qquad \mathrm{mdc}(6,6) = 6.$$

Dizemos que dois inteiros são *primos entre si* se seu máximo divisor comum é 1. Será mais conveniente definir também $\mathrm{mdc}(a, 0) = a$ para todo $a \geq 0$.

Uma outra noção até certo ponto semelhante é o *mínimo múltiplo comum* de dois inteiros, que é o menor inteiro positivo que é um múltiplo de ambos os inteiros, e representado por $\mathrm{mmc}(a, b)$. Por exemplo,

$$\mathrm{mmc}(1,6) = 6, \qquad \mathrm{mmc}(2,6) = 6, \qquad \mathrm{mmc}(3,6) = 6, \qquad \mathrm{mmc}(4,6) = 12,$$

$$\mathrm{mmc}(5,6) = 30, \qquad \mathrm{mmc}(6,6) = 6$$

O máximo divisor comum de dois inteiros positivos pode ser encontrado um tanto facilmente usando-se as suas fatorações primas: olhe para os fatores primos comuns, eleve-os à menor dos dois expoentes, e tome o produto dessas potências de primos. Por exemplo, $300 = 2^2 \cdot 3 \cdot 5^2$ e $18 = 2 \cdot 3^3$, e portanto $\mathrm{mdc}(300, 18) = 2 \cdot 3 = 6$.

O problema com esse método é que é muito difícil encontrar a fatoração prima de inteiros grandes. O algoritmo a ser discutido nesta seção calculará o máximo divisor comum de dois inteiros de uma maneira muito mais rápida, sem encontrar suas fatorações primas. Esse algoritmo é um importante ingrediente de quase todos os algoritmos envolvendo computação com inteiros. (E, como vemos do seu nome, ele vai lá atrás para o grande matemático grego!)

6.19 Mostre que se a e b são inteiros positivos com $a|b$, então $\mathrm{mdc}(a, b) = a$.

6.20 (a) Prove que $\mathrm{mdc}(a, b) = \mathrm{mdc}(a, b - a)$.

(b) Seja r o resto se dividirmos b por a. Então $\mathrm{mdc}(a, b) = \mathrm{mdc}(a, r)$.

6.21 (a) Se a é par e b é ímpar, então $\mathrm{mdc}(a, b) = \mathrm{mdc}(a/2, b)$.

(b) Se ambos a e b são pares, então $\mathrm{mdc}(a, b) = 2\mathrm{mdc}(a/2, b/2)$.

6.22 Como você pode expressar o mínimo múltiplo comum de dois inteiros, se você conhece a fatoração prima de cada um?

6.23 Suponha que lhe são dados dois inteiros, e que você conheça a fatoração prima de um deles. Descreva uma maneira de computar o máximo divisor comum desses números.

6.24 Prove que para quaisquer dois inteiros a e b,

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

6.25 Três inteiros a, b e c formam uma *tripla pitagórica*, se $a^2+b^2 = c^2$. (a) Escolha quaisquer três inteiros x, y e z, e faça $a = 2xyz$, $b = (x^2-y^2)z$, $c = (x^2+y^2)z$. Verifique que (a, b, c) é uma tripla pitagórica. (b) Prove que todas as triplas pitagóricas surgem dessa maneira: se a, b, c são inteiros tais que $a^2 + b^2 = c^2$, então existem outros inteiros x, y e z de modo que a, b e c possam ser expressos por meio das fórmulas acima.

[Dica: Primeiro, mostre que o problema pode ser reduzido ao caso em que $\mathrm{mdc}(a, b, c) = 1$, a é par, e b, c são ímpares. Segundo, faça $a^2 = (b-c)(b+c)$ e use isso para argumentar que $(b+c)/2$ e $b-c)/2$ são quadrados.]

Agora nos voltamos para o Algoritmo Euclideano. O algoritmo é baseado em dois fatos simples, já familiares como exercícios 6.19 e 6.20.

Suponha que nos são dados dois inteiros positivos a e b, e desejamos achar seu máximo divisor comum. Aqui está o que fazemos:

1. Se $a > b$ então trocamos a por b e vice-versa.

2. Se $a > 0$, dividimos b por a, para obter um resto r. Substituimos b por r e retornamos ao passo 1.

3. Senão (se $a = 0$), retornamos b como o m.d.c. e paramos.

Quando você executa o algoritmo, especialmente à mão, não há razão para trocar as posições de a e b se $a < b$: podemos simplesmente dividir o maior pelo menor (com resto), e substituir o maior pelo resto se o resto não é 0. Vamos fazer alguns exemplos.

$$\begin{aligned}
\mathrm{mdc}(300, 18) &= \mathrm{mdc}(12, 18) = \mathrm{mdc}(12, 6) = 6.\\
\mathrm{mdc}(101, 100) &= \mathrm{mdc}(1, 100) = 1.\\
\mathrm{mdc}(89, 55) &= \mathrm{mdc}(34, 55) = \mathrm{mdc}(34, 21) = \mathrm{mdc}(13, 21) = \mathrm{mdc}(13, 8)\\
&= \mathrm{mdc}(5, 8) = \mathrm{mdc}(5, 3) = \mathrm{mdc}(2, 3) = \mathrm{mdc}(2, 1) = 1.
\end{aligned}$$

Você pode conferir em cada caso (usando uma fatoração prima dos números) que o resultado é de fato o m.d.c.

Se descrevemos um algoritmo, a primeira coisa a se preocupar é se ele termina de alguma forma. Logo, por que o Algoritmo Euclideano é finito? Isso é fácil: os números nunca aumentam, e um deles diminui toda vez que o passo 2 é executado, portanto ele não pode durar infinitamente.

Então obviamente temos que assegurar que nosso algoritmo produz o que precisamos. Isso está claro: o passo 1 (trocar os números de posição) trivialmente não modifica o m.d.c., o passo 3 (substituir o maior pelo resto de uma divisão) não modifica o m.d.c. pelo exercício 6.20(b). E quando paramos no passo 2, o número retornado é de fato o m.d.c. dos dois números correntes pelo exercício 6.19.

Uma terceira, e mais sutil, pergunta que você deveria fazer quando está desenvolvendo um algoritmo: quanto tempo ele leva? Quantos passos ele levará antes que termine? Podemos obter um limitante do argumento que prova terminação finita: como um ou o outro número decresce toda vez que o laço 1-2 é executado, ele certamente vai parar em menos que $a + b$ iterações. Esse não é verdadeiramente um limitante de tempo excelente: se aplicarmos o Algoritmo Euclideano a dois números com 100 dígitos, então ele diz que o algoritmo não levará mais que $2 \cdot 10^{100}$ passos, o que é um número astronômico, e, por conseguinte, inútil. Mas, felizmente esse é apenas um

limitante superior, e um limitante muito pessimista nesse aspecto; os exemplos que consideramos parecem mostrar que o algoritmo termina mais rápido que isso.

Mas os exemplos também sugerem que essa questão é um tanto delicada. Vemos que o Algoritmo Euclideano pode ser um tanto diferente em duração, dependendo dos números em questão. Algumas das observações possíveis feitas a partir desses exemplos estão contidas nos exercícios a seguir.

6.26 Mostre que o Algoritmo Euclideano pode terminar em dois passos para inteiros positivos arbitrariamente grandes, mesmo se seu m.d.c. for 1.

6.27 Descreva o Algoritmo Euclideano aplicado a dois números de Fibonacci consecutivos. Use sua descrição para mostrar que o Algoritmo Euclideano pode levar um número arbitrário de passos.

Então o que *podemos* dizer sobre quanto tempo leva o Algoritmo Euclideano? A chave para a resposta é o seguinte lema:

Lemma 6.6.1 *Durante a execução do Algoritmo Euclideano, o produto dos dois números correntes decresce por um fator de pelo menos 2 em cada iteração.*

Prova. Para ver que isso é o caso, considere o passo no qual o par (a, b) $(a < b)$ é substituído pelo par (r, a), onde r é o resto de b quando dividido por a. Então temos $r < a$ e $a + r \leq b$. Daí $b \geq a + r > 2r$, e portanto $ar < \frac{1}{2}ab$ tal qual afirmado. □

Suponha que apliquemos o Algoritmo Euclideano a dois números a e b e levamos k passos. Segue pelo Lema 6.6.1 que após os k passos, o produto dos dois números correntes será no máximo $ab/2^k$. Como isso é pelo menos 1, obtemos que

$$ab \geq 2^k,$$

e portanto

$$k \leq \log_2(ab) = \log_2 a + \log_2 b.$$

Por conseguinte provamos o seguinte.

Teorema 6.6.1 *O número de passos do Algoritmo Euclideano, aplicado a dois inteiros positivos a e b, é no máximo* $\log_2 a + \log_2 b$.

Substituímos a soma dos números pela soma dos logaritmos dos números no limitante sobre o número de passos, o que é realmente um avanço. Por exemplo, o número de iterações na computação do m.d.c. de dois inteiros de 300-dígitos é menor que $2\log_2 10^{300} = 600\log_2 10 < 2000$. Um tanto menos que $2 * 10^{300}$, que era nossa primeira e ingênua estimativa! Note que $\log_2 a$ é menor que o número de bits de a (quando escrito na base 2), portanto podemos dizer que o Algoritmo Euclideano não leva mais iterações que o número de bits necessários para representar os números na base 2.

O teorema acima dá apenas um limitante superior para o número de passos que o Algoritmo Euclideano leva; podemos ter ainda mais sorte: por exemplo, quando aplicamos o Algoritmo Euclideano a dois inteiros consecutivos, ele leva apenas um

passo. Mas, às vezes, não se pode fazer melhor. Se você fez o exercício 6.27, você viu que quando aplicado a dois números de Fibonacci consecutivos F_k e F_{k+1}, o Algoritmo Euclideano leva $k-1$ passos. Por outro lado, o lema acima dá o limitante

$$\log_2 F_k + \log_2 F_{k+1} \approx \log_2 \left(\frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^k \right) + \log_2 \left(\frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^{k+1} \right)$$

$$= -\log_2 5 + (2k+1) \log_2 \left(\frac{1+\sqrt{5}}{2} \right) \approx 1,388k - 1,628,$$

portanto superestimamos o número de passos apenas por um fator de cerca de 1,388, ou menos que 40%.

Números de Fibonacci não são bons apenas para dar exemplos de números grandes para os quais podemos ver como o Algoritmo Euclideano funciona; eles também são úteis na obtenção de um limitante ainda melhor sobre o número de passos. Enunciamos o resultado como um exercício. Seu conteúdo é que, num certo sentido, o Algoritmo Euclideano é mais demorado sobre dois números de Fibonacci consecutivos.

6.28 Suponha que $a < b$ e que o Algoritmo Euclideano aplicado a a e b leve k passos. Prove que $a \geq F_k$ e $b \geq F_{k+1}$.

6.29 Considere a seguinte versão do Algoritmo Euclideano para computar $\mathrm{mdc}(a, b)$: (1) troque os números de lugar se necessário para ter $a \leq b$; (2) se $a = 0$, então retorne b; (3) se $a \neq 0$, então substitua b por $b - a$ e vá para (1).

(a) Execute esse algoritmo para computar $\mathrm{mdc}(19, 2)$.

(b) Mostre que o Algoritmo Euclideano modificado sempre termina com a resposta certa.

(c) Quanto tempo esse algoritmo leva, no pior caso, quando aplicado a dois inteiros de 100-dígitos?

6.30 Considere a seguinte versão do Algoritmo Euclideano para computar $\mathrm{mdc}(a, b)$. Comece computando a maior potência de 2 que divide ambos a e b. Se essa é 2^r, então divida a e b por 2^r. Após esse "pré-processamento", faça o seguinte:

(1) Troque os números de lugar se necessário para ter $a \leq b$.

(2) Se $a \neq 0$, então verifique as paridades de a e b; se a é par, e b é ímpar, então substitua a por $a/2$; se ambos a e b são ímpares, então substitua b por $b - a$; em cada caso, vá para (1).

(3) se $a = 0$, então retorne $2^r b$ como o m.d.c.

Agora vêm os exercícios:

(a) Execute esse algoritmo para computar $\mathrm{mdc}(19, 2)$.

(b) Parece que no passo (2), ignoramos o caso em que ambos a e b são pares. Mostre que isso nunca ocorre.

(c) Mostre que o Algoritmo Euclideano modificado sempre termina com a resposta certa.

(d) Mostre que esse algoritmo, quando aplicado a dois inteiros de 100-dígitos, não leva mais que 1500 iterações.

O Algoritmo Euclideano dá muito mais que apenas o máximo divisor comum de dois números. A principal observação é que se executarmos o Algoritmo Euclideano para computar o máximo divisor comum de dois inteiros positivos a e b, todos os números que produzimos ao longo da computação podem ser escritos como a soma de um inteiro múltiplo de a e um inteiro múltiplo de b.

Como um exemplo, vamos retomar a computação de $\mathrm{mdc}(300, 18)$:

$$\mathrm{mdc}(300, 18) = \mathrm{mdc}(12, 18) = \mathrm{mdc}(12, 6) = 6.$$

Aqui o número 12 foi obtido como o resto da divisão $300 : 18$; isso significa que, ele foi obtido por meio da subtração de 300 no mais alto múltiplo de 18 que é menor: $12 = 300 - 16 \cdot 18$. Vamos registrá-lo dessa forma:

$$\mathrm{mdc}(300, 18) = \mathrm{mdc}(300 - 16 \cdot 18, 18).$$

A seguir, obtivemos 6 por meio da subtração de 12 em 18, o que podemos fazer de tal maneira que mantemos a forma de (múltiplo de 300)+(múltiplo de 18):

$$\mathrm{mdc}(300 - 16 \cdot 18, 18) = \mathrm{mdc}(300 - 16 \cdot 18, 17 \cdot 18 - 300).$$

Portanto segue que o m.d.c. propriamente dito, a saber 6, é dessa forma:

$$6 = 17 \cdot 18 - 300.$$

Vamos provar formalmente que todos os números produzidos pelo Algoritmo de Euclides para $\mathrm{mdc}(a, b)$ podem ser escritos como a soma de um inteiro múltiplo de a e um inteiro múltiplo de b. Suponha que isso se verifica para dois números consecutivos que computamos, de modo que um é $a' = am + bn$, e o outro é $b' = ak + bl$, onde m, n, k, l são inteiros (não necessariamente positivos). Então no próximo passo que computamos (digamos) o resto de b' módulo a', que é

$$a' - qb' = (am + bn) - q(ak + bl) = a(m - qk) + b(n - ql),$$

que está na forma correta novamente.

Em particular, obtemos o seguinte:

Teorema 6.6.2 *Seja $d = \mathrm{mdc}(a, b)$. Então d pode ser escrito na forma*

$$d = am + bn$$

onde m e n são inteiros.

Como no exemplo trabalhado acima, podemos manter a representação de inteiros na forma $am + bn$ durante a computação. Isso mostra que a expressão para d no teorema não apenas existe, mas ela é facilmente computável.

6.7 Congruências

Notação não é parte da estrutura lógica básica da matemática: poderíamos representar o conjunto dos números reais por $\mathbf{V}$, ou a adição por #, e o significado dos resultados matemáticos seria o mesmo. Mas uma boa notação pode ser maravilhosamente sugestiva, levando a avanços conceituais reais. Um desses passos importantes foi tomado quando Gauss notou que usamos a frase "a dá o mesmo resto que b quando dividido por m" muito frequentemente, e que essa relação se comporta um tanto semelhantemente à igualdade. Ele introduziu uma notação para isso, chamada de *congruência*.

Figura 6.5: Carl Friedrich Gauss (1777-1855).

Se a e b dão o mesmo resto quando divididos por m (onde a, b, m são inteiros e $m > 0$), então escrevemos

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

(leia: a é congruente a b módulo m). Uma maneira equivalente de dizer isso é que m é um divisor de $b - a$. O número m é chamado de *modulus* da relação de congruência.

Essa notação sugere que desejamos considerar essa relação como um análogo da igualdade. E, de fato, muitas das propriedades da igualdade são válidas para congruências, pelo menos se mantivermos o modulus m fixo. Temos a *reflexividade*:

$$a \equiv a \pmod{m},$$

simetria:

$$a \equiv b \pmod{m} \qquad \Longrightarrow \qquad b \equiv a \pmod{m},$$

e *transitividade*:

$$a \equiv b \pmod{m}, \qquad b \equiv c \pmod{m} \qquad \Longrightarrow \qquad a \equiv c \pmod{m}.$$

Essas são triviais se pensarmos na relação de congruência como afirmando a igualdade: a saber, igualdade dos restos quando divididos por m.

Podemos fazer muitos cálculos com congruências tais como com equações. Se temos duas congruências com o mesmo modulus

$$a \equiv b \pmod{m}, \quad \text{and} \quad c \equiv d \pmod{m},$$

então podemos adicioná-las, subtraí-las, e multiplicá-las, para obter

$$a + c \equiv b + d \pmod{m}, \quad a - c \equiv b - d \pmod{m}, \quad ac \equiv bd \pmod{m}$$

(retornaremos à divisão mais adiante). Um caso especial útil da regra da multiplicação é que podemos multiplicar ambos os lados de uma congruência pelo mesmo número: se $a \equiv b \pmod{m}$ então $ka \equiv kb \pmod{m}$ para todo inteiro k.

Essas propriedades precisam ser provadas, no entanto. Pela hipótese, $a - b$ e $c - d$ são divisíveis por m. Para ver que congruências podem ser somadas, temos que verificar que $(a + c) - (b + d)$ é divisível por m. Para esse fim, escrevemo-la na forma $(a - b) + (c - d)$, o que mostra que ela é a soma de dois inteiros divisíveis por m e portanto que ela também é divisível por m.

A prova de que congruências podem ser subtraídas é muito semelhante, mas multiplicação é um pouco mais complicado. Temos que mostrar que $ac - bd$ é divisível por m. Para esse fim, escrevemo-la na forma

$$ac - bd = (a - b)c + b(c - d).$$

Aqui $a - b$ e $c - d$ são divisíveis por m, e portanto também o são $(a - b)c$ e $b(c - d)$, daí sua soma também o é.

A notação de congruência é muito conveniente na formulação de vários enunciados e argumentos sobre divisibilidade. Por exemplo, o "Pequeno" Teorema de Fermat 6.5.1 pode ser enunciado da seguinte maneira: se p é um primo então

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

6.31 Qual é o maior inteiro m para o qual $12345 \equiv 54321 \pmod{m}$?

6.32 Quais das seguintes "regras" são verdadeiras?

(a) $a \equiv b \pmod{c} \;\Rightarrow\; a + x \equiv b + x \pmod{c + x}$;

(b) $a \equiv b \pmod{c} \;\Rightarrow\; ax \equiv bx \pmod{cx}$.

(c) $\left.\begin{array}{l} a \equiv b \pmod{c} \\ x \equiv y \pmod{z} \end{array}\right\} \;\Rightarrow\; a + x \equiv b + y \pmod{c + z}$;

(d) $\left.\begin{array}{l} a \equiv b \pmod{c} \\ x \equiv y \pmod{z} \end{array}\right\} \;\Rightarrow\; ax \equiv by \pmod{cz}$.

6.33 Como você definiria $a \equiv b \pmod{0}$?

6.34 (a) Encontre dois inteiros a e b tais que $2a \equiv 2b \pmod 6$, mas $a \not\equiv b \pmod 6$. (b) Mostre que se $c \neq 0$ e $ac \equiv bc \pmod{mc}$, então $a \equiv b \pmod m$.

6.35 Seja p um primo. Mostre que se x, y, u, v são inteiros tais que $x \equiv y \pmod p$, $u, v > 0$, e $u \equiv y \pmod{p-1}$, então $x^u \equiv y^v \pmod p$.

6.8 Números estranhos

O que é Quinta-Feira+Sexta-Feira?

Se você não entende a pergunta, pergunte a uma criança. Ele/ela lhe dirá que é Terça-Feira. (Pode haver alguma discussão se a semana começa com Segunda-Feira ou Domingo; mas mesmo se acharmos que ela começa com Domingo, ainda assim podemos dizer que o Domingo é o dia 0.)

Agora não deveríamos ter dificuldade de adivinhar que Quarta-Feira·Terça-Feira = Sábado, Quinta-Feira^2=Terça-Feira, Segunda-Feira$-$Sábado=Terça-Feira etc.

Dessa maneira podemos fazer operações aritméticas com os dias da semana: introduzimos um novo sistema numérico. Nesse sistema, existem apenas 7 números, que chamamos Dom, Seg, Ter, Qua, Qui, Sex, Sab, e podemos realizar adição, subtração e multiplicação tal qual com números (poderíamos chamá-los Soneca, Dunga, Feliz, Atchim, Zangado, Mestre e Dengoso; o que é importante é como as operações aritméticas funcionam).

Não apenas podemos definir essas operações; elas funcionam exatamente como as operações com inteiros. Addição e multiplicação são comutativas:

$$\text{Ter} + \text{Sex} = \text{Sex} + \text{Ter}, \qquad \text{Ter} \cdot \text{Sex} = \text{Sex} \cdot \text{Ter},$$

e associativas:

$$(\text{Seg} + \text{Qua}) + \text{Sex} = \text{Seg} + (\text{Qua} + \text{Sex}), \qquad (\text{Seg} \cdot \text{Qua}) \cdot \text{Sex} = \text{Seg} \cdot (\text{Qua} \cdot \text{Sex}),$$

e elas são distributivas:

$$(\text{Seg} + \text{Qua}) \cdot \text{Sex} = (\text{Seg} \cdot \text{Sex}) + (\text{Qua} \cdot \text{Sex}).$$

Subtração é o inverso de adição:

$$(\text{Seg} + \text{Qua}) - \text{Qua} = \text{Seg}.$$

Domingo funciona como 0:

$$\text{Qua} + \text{Dom} = \text{Qua}, \qquad \text{Qua} \cdot \text{Dom} = \text{Dom},$$

e Segunda-Feira funciona como 1:

$$\text{Qua} \cdot \text{Seg} = \text{Qua}.$$

Nada disso é algo novo, se pensarmos em "Segunda-Feira" como 1, "Terça-Feira" como 2, etc., e se nos dermos conta de que como o dia 8 é Segunda-Feira novamente,

temos que substituir o resultado de qualquer operação aritmética pelo seu resto módulo 7. Todas as identidades acima expressam relações de congruência, e são imediatas das propriedades básicas das congruências.

E a divisão? Em alguns casos, ela é óbvia. Por exemplo, o que é Sab/Qua? Traduzindo para inteiros, isso é 6/3, o que dá 2, *i.e.*, Ter. Confira: Ter $\cdot$ Qua $=$ Sab.

Mas o que é Ter/Qua? Em nossos sistemas numéricos mais familiares, isso seria $2/3$, o que não é um inteiro; na verdade, números racionais foram introduzidos precisamente de forma que poderíamos falar sobre o resultado de todas as divisões (exceto divisões por 0). Temos que introduzir "dias da semana fracionários"?

Resulta que esse novo sistema numérico (com apenas 7 "números") é melhor! O que significa Ter/Qua? É um "número" X tal que $X \cdot \text{Qua} = \text{Ter}$. Mas é fácil verificar que Qua $\cdot$ Qua $=$ Ter; portanto temos (ou pelo menos parece fazer sentido dizer que temos) que Ter/Qua=Qua.

Isso dá um exemplo mostrando que somos capazes de realizar divisão sem introduzir novos "números" (ou novos dias da semana), mas sempre podemos realizar a divisão? Para ver como isso funciona, vamos tomar uma outra divisão: Qua/Sex, e vamos tentar *não* adivinhar o resultado; ao contrário, chamemo-lo X e mostremos que um dos dias da semana tem que ser apropriado para X.

Portanto faça $X = \text{Qua}/\text{Sex}$. Isso significa que $X \cdot \text{Sex} = \text{Qua}$. Para cada dia X da semana, o produto $X \cdot$ Sex á algum dia da semana.

A principal afirmação é que *para dias diferentes X, os produtos $X \cdot$ Sex são todos diferentes.* De fato, suponha então que

$$X \cdot \text{Sex} = Y \cdot \text{Sex},$$

então

$$(X - Y) \cdot \text{Sex} = \text{Dom} \tag{6.2}$$

(usamos aqui a lei distributiva e o fato de que Domingo funciona como 0). Agora Domingo é análogo 0 também no sentido de que tal qual o produto de dois números diferentes de zero é diferente de zero, o produto de dois dias diferentes de Domingo é diferente de Domingo. (Confira!) Portanto devemos ter $X - Y = \text{Dom}$, ou $X = Y + \text{Dom} = Y$.

Portanto os dias $X \cdot$ Fr são todos diferentes, e existem sete deles, logo, todo dia da semana tem que ocorrer nessa foram. Em particular, "Qua" ocorrerá.

Esse argumento funciona para qualquer divisão, exceto quando tentamos dividir por Domingo; já sabemos que Domingo funciona como 0, e portanto Domingo multiplicado por qualquer dia é Domingo, logo não podemos dividir qualquer outro dia por Domingo (e o resultado de Domingo/Domingo não está bem definido, poderia ser qualquer dia).

Congruências introduzidas na seção 6.7 provêem uma maneira frequentemente conveniente de manusear esses números estranhos. Por exemplo, podemos escrever (6.2) na seguinte forma:

$$(x - y) \cdot 5 \equiv 0 \pmod{7}$$

(onde x e y são os números correspondentes aos dias X e Y), e portanto 7 é um divisor de $(x - y)5$. Mas 5 não é divisível por 7 nem o é $x - y$ (pois esses são dois inteiros

não-negativos menores que 7 diferentes). Como 7 é um primo, isso é uma contradição. Dessa maneira podemos falar sobre números ordinários ao invés dos dias da semana; o preço que pagamos é que temos que usar congruências ao invés de igualdade.

6.36 Ache Qua/Sex; Ter/Sex; Seg/Ter; Sab/Ter.

Há algo especial a respeito do número 7 aqui? Em uma sociedade onde a semana consiste de 10 ou 13 ou 365 dias, poderíamos definir adição, subtração e multiplicação dos dias da semana de maneira semelhante.

Seja m o número de dias da semana, que em linguagem matemática chamamos de modulus. Seria impraticável introduzir novos nomes para os dias da semana,[1] portanto vamos simplesmente chamá-los $\overline{0}, \overline{1}, \ldots, \overline{m-1}$. A barra superior indica que por exemplo $\overline{2}$ se refere não apenas ao dia 2, mas também ao dia $m+2$, dia $2m+2$ etc.

Adição é definida por $\overline{a}+\overline{b}=\overline{c}$, onde c é o resto de $a+b$ módulo m. Multiplicação e subtração são definidas de uma maneira semelhante. Dessa forma temos um novo sistema numérico: ele consiste apenas de m números, e as operações aritméticas básicas podem ser realizadas. Essas operações obedecerão as leis básicas da computação, que segue tal qual no caso $m=7$ acima. Essa versão da aritmética é chamada de *aritmética modular*.

E a divisão? Se você ler cuidadosamente a prova de que podemos fazer divisão quando $m=7$, você vêque ela usa uma propriedade especial de 7: que ele é um primo! Há de fato uma diferença substancial entre aritmética modular com *moduli*[2] primos e não-primos. No que segue, restringiremos nossa atenção ao caso em que o modulus é um primo, e para enfatizar isso, representá-lo-emos por p. Esse sistema numérico consistindo de $\overline{0}, \overline{1}, \ldots \overline{p-1}$, com as quatro operações definidas como acima, é chamado de *corpo primo*.

O corpo de 2-elementos. O menor número primo é 2, e o corpo primo mais simples tem apenas 2 elementos, $\overline{0}$ e $\overline{1}$. É fácil dar as tábuas de adição e multiplicação:

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

(Há realmente apenas uma operação aqui que não segue das propriedades gerais de 0 e 1, a saber $\overline{1}+\overline{1}=\overline{0}$. Não há necessidade de especificar a tábua de subtração, pois nesse corpo $a+b=a-b$ para todo a e b (confira!), nem a tábua de divisão, pois essa é óbvia: não podemos dividir por $\overline{0}$, e dividir por $\overline{1}$ não muda o dividendo.)

É inconveniente escrever todas essas barras sobre os números, portanto frequentemente as omitimos. Mas então temos que ser cuidadosos, porque temos que saber se $1+1$ significa 2 ou 0; por conseguinte modificamos o sinal de adição, e usamos $\oplus$ para a adição no corpo de 2-elementos. Nessa notação, as tábuas de adição e de multiplicação ficam assim:

[1] Em muitas linguagens, os nomes de alguns dias são derivados de números.
[2] Plural de "modulus" em latim.

$\oplus$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

(não tivemos que introduzir um novo símbolo de multiplicação, porque a tábua de multiplicação para 0 e 1 é a mesma no corpo de 2-elementos que a usada para números ordinários).

Esse corpo é muito pequeno mas muito importante, porque bastante da ciência da computação, teoria da informação e lógica matemática o usa: seus dois elementos podem ser interpretados como "SIM–NÃO", "VERDADEIRO–FALSO", "SINAL–SEM SINAL" etc.

6.37 Suponha que 0 signifique "FALSE" e 1 signifique "TRUE". Sejam A e B dois enunciados (que são verdadeiros ou falsos). Expresse, usando as operações $\oplus$ e $\cdot$, a veracidade de "não A", "A ou B", "A e B".

6.38 Seja 6 o modulus; mostre por meio de um exemplo que divisão por um "número" não-zero nem sempre poder ser realizada. Generalize o exemplo para todo modulus composto.

Divisão em aritmética modular. Nosso argumento de que divisão em aritmética modular pode ser realizada desde que o modulus seja um primo foi razoavelmente simples mas ele não nos disse como realizar a divisão. Para achar o quociente dessa operação seria preciso olhar para todos os números entre 0 e $p-1$, o que era OK para $p = 7$, mas seria um tanto tedioso para um primo como $p = 234527$ (sem falar nos primos realmente enormes usados em criptografia e segurança de computadores, como veremos).

Portanto como dividimos, digamos, $\overline{53}$ por $\overline{2}$ módulo 234527?

Podemos simplificar o problema, e simplesmente perguntar sobre dividir $\overline{1}$ por $\overline{2}$ módulo 234527. Se temos que $\overline{1}/\overline{2} = \overline{a}$, então podemos obter $\overline{53}/\overline{2} = \overline{53} \cdot \overline{a}$, que sabemos como computar.

Nesse ponto a prova pode ser explicada melhor no caso geral, Um modulus primo p e um inteiro a ($1 \leq a \leq p-1$) nos são dados, e desejamos encontrar um inteiro x ($0 \leq x \leq p-1$) tal que $\overline{ax} = \overline{1}$. Usando a notação de congruência da seção 6.7, podemos escrever isso como

$$ax \equiv 1 \pmod{p}.$$

A chave para resolver esse problema é o Algoritmo de Euclides. Vamos computar o máximo divisor comum de a e p. Isso parece bobagem, pois sabemos a resposta imediatamente: p é um primo e $1 \leq a < p$, portanto eles não podem ter qualquer divisor comum maior que 1, e portanto $\mathrm{mdc}(p, a) = 1$. Mas lembre-se que o Algoritmo de Euclides dá mais: ele fornecerá o máximo divisor comum na forma $au + pv$, onde u e v são inteiros. Por conseguinte obtemos

$$au + pv = 1,$$

o que implica que

$$au \equiv 1 \pmod{p}.$$

Estamos quase lá; o único problema é que um inteiro u pode não estar entre 1 e $p-1$. Mas se x for o resto de u módulo p, então multiplicando a congruência $x \equiv u \pmod{p}$ por a (recordemos da Section 6.7 que essa é uma operação legal sobre congruências), obtemos

$$ax \equiv au \equiv 1 \pmod{p},$$

e como $0 \leq x \leq p-1$, isso resolve nosso problema.

Vamos seguir esse algoritmo em cima do nosso exemplo acima, com $a = 2$ e $p = 234527$. O Algoritmo de Euclides funciona de modo realmente simples nesse caso: divida 234527 por 2 com resto, e o resto já chega em 1. Isso dá

$$2 \cdot (-117263) + 234527 \cdot 1 = 1.$$

O resto de -117263 módulo 234527 é 117264, portanto obtemos que

$$\overline{1}/\overline{2} = \overline{117264}.$$

6.39 Compute $\overline{1}/\overline{53}$ módulo 234527.

Uma vez que sabemos como fazer aritmética básica, tarefas mais complicadas como resolver equações lineares podem ser feitas lembrando o que faríamos com números ordinários. Ilustramos isso por meio de alguns exemplos onde usamos a notação de congruência juntamente com suas propriedades básicas da seção 6.7.

Exemplo 1. Considere uma equação linear, digamos

$$\overline{7}X + \overline{3} = \overline{0},$$

onde o modulus é 47 (verifique na tabela que esse é um primo!). Podemos reescrever isso como uma congruência:

$$7x + 3 \equiv 0 \pmod{47}.$$

Essa segunda forma é a mais usual, portanto vamos trabalhar com ela.

Tal qual faríamos com uma equação, transformamos essa em

$$7x \equiv -3 \pmod{47} \tag{6.3}$$

(poderíamos substituir -3 por seu resto 44 módulo 47, se desejássemos manter os números positivos, mas isso é opcional).

A seguir temos que encontrar o inverso de 7 módulo 47. O Algoritmo Euclideano dá

$$\mathrm{mdc}(7, 47) = \mathrm{mdc}(7, 5) = \mathrm{mdc}(2, 5) = \mathrm{mdc}(2, 1) = 1,$$

e seguindo a versão estendida obtemos

$$5 = 47 - 6 \cdot 7, \qquad 2 = 7 - 5 = 7 - (47 - 6 \cdot 7) = 7 \cdot 7 - 47,$$

$$1 = 5 - 2 \cdot 2 = (47 - 6 \cdot 7) - 2 \cdot (7 \cdot 7 - 47) = 3 \cdot 47 - 20 \cdot 7,$$

que mostra que $(-20) \cdot 7 \equiv 1 \pmod{47}$. Portanto o inverso de 7 módulo 47 é -20 (que novamente poderíamos escrever como 27).

Agora dividindo ambos os lados de (6.3) por 7, que é o mesmo que multiplicar ambos os lados por 27, obtemos

$$x \equiv 13 \pmod{47}.$$

(Aqui obtemos 13 ou como o resto de $(-3)(-20)$, ou como o resto de $44 \cdot 27$ módulo 47—o resultado é o mesmo.)

Exemplo 2. A seguir, vamos resolver um sistema de duas equações lineares, com duas variáveis. Tornaremos os números um pouco maior, para ver que podemos lidar com números grandes também. Suponha que o modulus seja $p = 127$, e considere as equações

$$\begin{aligned} \overline{12}X + \overline{31}Y &= \overline{2} \\ \overline{2}X + \overline{89}Y &= \overline{23}. \end{aligned} \tag{6.4}$$

Podemos reescrevê-las como congruências:

$$\begin{aligned} 12x + 31y &\equiv 2 \pmod{127} \\ 2x + 89y &\equiv 23 \pmod{127}. \end{aligned}$$

a. Elimine uma variável. Como resolveríamos esse sistema se essas fossem equações comuns? Poderíamos multiplicar a segunda equação por 6 e subtraí-la da primeira, para eliminar os termos em x. Podemos fazer isso nesse corpo primo também, e obter

$$(31 - 6 \cdot 89)y \equiv 2 - 6 \cdot 23 \pmod{127},$$

ou

$$(-503)y \equiv -136 \pmod{127}.$$

Podemos substituir esses números negativos por seus restos módulo 127, para obter

$$5y \equiv 118 \pmod{127}. \tag{6.5}$$

Divisão. A seguir, desejamos dividir a equação por 5. Isso é o que discutimos acima: temos que usar o Algoritmo de Euclides. A computação do máximo divisor comum é fácil:

$$\mathrm{mdc}(127, 5) = \mathrm{mdc}(2, 5) = \mathrm{mdc}(2, 1) = 1.$$

Isso não traz nada de novo: sabíamos de antemão que esse m.d.c. será 1. Para obter mais, temos que dar prosseguimento a essa computação por meio de uma outra, enquanto que cada número é escrito como um inteiro múltiplo de 127 mais um inteiro múltiplo de 5:

$$\mathrm{mdc}(127, 5) = \mathrm{mdc}(127 - 25 \cdot 5, 5) = \mathrm{mdc}(127 - 25 \cdot 5, (-2) \cdot 127 + 51 \cdot 5) = 1,$$

e isso resulta que

$$(-2) \cdot 127 + 51 \cdot 5 = 1.$$

Por conseguinte $5 \cdot 51 \equiv 1 \pmod{127}$, e portanto encontramos o "inverso" de 5 módulo 127.

Ao invés de dividir a equação (6.4) por cinco, multiplicamos por seu "inverso" 51, para obter

$$y \equiv 51 \cdot 118 \pmod{127}. \tag{6.6}$$

Conclusão. Se calcularmos o lado direito de (6.6) e então computar seu resto módulo 127, obtemos que $y \equiv 49 \pmod{127}$, ou, em outras palavras, $Y = \overline{49}$ é sua solução. Para obter x, temos que substituir esse valor de volta nas equações originais:

$$2x + 89 \cdot 49 \equiv 23 \pmod{127},$$

daí

$$2x \equiv 23 - 89 \cdot 49 \equiv 107 \pmod{127}.$$

Portanto, temos que fazer uma divisão a mais. Similarmente ao que obtivemos acima, obtemos

$$(-63) \cdot 2 + 127 = 1,$$

e portanto

$$64 \cdot 2 \equiv 1 \pmod{127}.$$

Logo, ao invés de dividir por 2, podemos multiplicar por 64, para obter

$$x \equiv 64 \cdot 107 \pmod{127}.$$

Computando o lado direito e seu resto módulo 127, obtemos que $x \equiv 117 \pmod{127}$, ou, em outras palavras, $X = \overline{117}$. Por conseguinte, resolvemos (6.4).

Exemplo 3. Podemos até resolver algumas equações quadráticas; por exemplo,

$$x^2 - 3x + 2 \equiv 0 \pmod{53}.$$

Podemos escrever isso como

$$(x-1)(x-2) \equiv 0 \pmod{53}.$$

Um dos fatores no lado esquerdo tem que ser congruente a 0 módulo 53, daí ou $x \equiv 1 \pmod{53}$ ou $x \equiv 2 \pmod{53}$.

Aqui encontramos uma maneira de escrever o lado esquerdo como um produto somente olhando para ele. O que acontece se temos uma equação com números maiores, digamos $x^2 + 134517x + 105536 \equiv 0 \pmod{234527}$? Duvidamos que alguém possa adivinhar uma decomposição. Nesse caso, podemos tentar seguir o procedimento da escola secundária para resolver equações quadráticas. Isso funciona, mas um passo dele é um tanto difícil: achar raízes quadradas. Isso pode ser feito eficientemente, mas o algoritmo é complicado demais para ser incluído aqui.

6.40 Resolva o sistema de congruências

$$\begin{aligned} 2x + 3y &\equiv 1 \pmod{11} \\ x + 4y &\equiv 4 \pmod{11} \end{aligned}$$

6.41 Resolva as "equações de congruências":

$$\text{(a) } x^2 - 2x \equiv 0 \pmod{11}, \qquad \text{(b) } x^2 \equiv 4 \pmod{23}.$$

6.9 Teoria dos números e combinatória

Muitas das ferramentas combinatórias que introduzimos anteriormente são muito úteis em teoria dos números também. Indução é usada em todos os lugares. Mostramos alguns argumentos elegantes baseados no *Princípio da Casa-de-Pombos* e na *Inclusão-Exclusão*.

São dados n números naturais: $a_1, a_2, ..., a_n$. Mostre que podemos escolher um subconjunto (não-vazio) desses números cuja soma divisível por n.

(É possível que esse subconjunto contenha todos os n números.)

Solução. Considere os seguintes n números:

$$\begin{aligned} b_1 &= a_1 \\ b_2 &= a_1 + a_2 \\ b_3 &= a_1 + a_2 + a_3 \\ &\vdots \\ b_n &= a_1 + a_2 + a_3 + ... + a_n. \end{aligned}$$

Se existe um número entre esses n números que é divisível por n, então encontramos o que desejamos. Se não existe nenhum, então vamos dividir todos os números $b_1, b_2, ..., b_n$ por n com resto. Guarde esses restos. Quais são os números que estamos obtendo? Poderiam ser $1, 2, ...,$ ou $n-1$. Mas temos um total de n números! Portanto pelo Princípio da Casa-de-Pombos, existirão dois números entre $b_1, b_2, ..., b_n$ que dão o mesmo resto quando os dividimos por n. Digamos, esses dois números são b_i e b_j $(i < j)$. Então sua diferença $b_j - b_i$ é divisível por n. Mas

$$b_j - b_i = a_{i+1} + a_{i+2} + ... + a_j.$$

Portanto encontramos um subconjunto especial dos números $a_1, a_2, ..., a_n$, a saber $a_{i+1}, a_{i+2}, ..., a_j$, cuja soma é divisível por n. E isso é o que desejávamos provar.

6.42 São dados n números do conjunto $\{1, 2, \ldots, 2n-1\}$. Prove que podemos sempre encontrar dois números entre esses n números que são primos entre si.

Como uma aplicação muito importante da inclusão–exclusão, vamos responder à seguinte pergunta sobre números: *Quantos números existem até* 1200 *que são primos em relação a* 1200*?*

Como sabemos a fatoração prima de 1200 é: $1200 = 2^4 \cdot 3 \cdot 5^2$, por conseguinte, sabemos que os números divisíveis por quaisquer de 2, 3, ou 5, são precisamente aqueles que têm um divisor comum com 1200. Portanto estamos interessados em contar os inteiros positivos menores que 1200, e que não sejam divisíveis por quaisquer de 2, 3, ou 5.

Pode-se facilmente calcular que até 1200, existem

$\frac{1200}{2}$ números divisíveis por 2

(a cada dois números consecutivos, um deles é par),

$\frac{1200}{3}$ números divisíveis por 3,

$\frac{1200}{5}$ números divisíveis por 5.

Aqueles números divisíveis por ambos 2 e 3 são exatamente aqueles que são divisíveis por 6. Por conseguinte, até 1200 existem

$\frac{1200}{6}$ números divisíveis por 2 e 3,

e, de modo semelhante, existem

$\frac{1200}{10}$ números divisíveis por 2 e 5,

$\frac{1200}{15}$ números divisíveis por 3 e 5.

Finalmente os números divisíveis por todos entre 2, 3, 5 são precisamente aqueles que são divisíveis por 30; portanto existem

$\frac{1200}{30}$ números divisíveis por todos entre 2, 3, 5.

Agora com esses dados, podemos usar a inclusão-exclusão para computar o número que estamos procurando:

$$1200 - \left(\frac{1200}{2} + \frac{1200}{3} + \frac{1200}{5}\right) + \frac{1200}{2\cdot 3} + \frac{1200}{2\cdot 5} + \frac{1200}{3\cdot 5} - \frac{1200}{2\cdot 3\cdot 5} = 320.$$

Se puxarmos 1200 para fora do lado esquerdo da igualdade acima, o que resta pode ser transformado numa bela forma de produto (confira os cálculos!):

$$\begin{aligned} &1200 \cdot \left(1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{2\cdot 3} + \frac{1}{2\cdot 5} + \frac{1}{3\cdot 5} - \frac{1}{2\cdot 3\cdot 5}\right) \\ &\qquad = 1200 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right). \end{aligned}$$

Seja n um número natural. Representamos por $\phi(n)$ o número daqueles números que não são maiores que n, e são primos em relação a n (usamos aqui "não maior", ao invés de "menor", o que tem significância apenas se $n = 1$, pois esse é o único caso em que o número propriamente dito é primo em relação a si próprio; portanto $\phi(1) = 1$). Primos, obviamente, têm o maior número de primos em relação a eles: se p é um primo, então todo inteiro positivo menor é contado em $\phi(p)$, portanto $\phi(p) = p - 1$. Em geral, o número $\phi(n)$ pode ser computado tal qual fizemos no caso concreto acima: *se $p_1, p_2, ..., p_r$ são fatores primos diferentes de n, então*

$$\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot ... \cdot \left(1 - \frac{1}{p_r}\right). \tag{6.7}$$

A prova segue os cálculos acima, e é dada como exercício 6.43.

6.43 Prove (6.7).

6.44 Seja n um número natural. Computamos $\phi(d)$ de todo divisor d de n, e então adicionamos todos esses números. Qual é a soma? (Experimente, formule uma conjectura, e prove-a.)

6.45 Somamos todos os inteiros positivos menores que n e primos em relação a n. Que obtemos?

6.46 Prove a seguinte extensão do Pequeno Teorema de Fermat: se $\mathrm{mdc}(a,b) = 1$, então $a^{\phi(b)} - 1$ é divisível por b.

[Dica: generalize a prova do Pequeno Teorema de Fermat no exercício 6.18.]

6.10 Como testar se um número é primo?

123456 é um primo? É claro que não, pois ele é par. 1234567 é primo? Esse não é fácil de responder, mas se você for pressionado, você pode tentar todos os números $2, 3, 4, 5 \ldots$ para ver se eles são divisores. Se você tiver paciência para ir até 127, então você conseguiu: $1234567 = 127 \cdot 9721$.

Que tal 1234577? Novamente você pode tentar encontrar um divisor tentando $2, 3, 4, 5, \ldots$. Mas dessa vez você não acha um divisor próprio! Mesmo assim, se você é realmente paciente e continuar até chegar à raiz quadrada de 1234577, que é is $1111, 1 \ldots$, você sabe que você não vai encontrar nenhum (por que?).

Que tal o número 1111222233334444555566667777888899967? Se esse é um primo (como o é), então temos que tentar todos os números até a sua raiz quadrada; como o número é maior que 10^{36}, sua raiz quadrada é maior que 10^{18}. Tentar mais 10^{18} números é uma tarefa praticamente impossível mesmo para qualquer computador.

O Teste de Fermat. Daí, como sabemos que esse número é um primo? Bem, nosso computador nos diz, mas como o computador sabe? Uma abordagem é oferecida pelo "Pequeno" Teorema de Fermat. Seu caso não trivial mais simples diz que *se p é um primo, então $p|2^p - 2$*. Se assumimos que p é ímpar (que apenas exclui o caso $p = 2$), então também sabemos que $p|2^{p-1} - 1$.

O que acontece se verificarmos a relação de divisibilidade $n|2^{n-1} - 1$ para números compostos? Ela obviamente falha se n é par (nenhum número par é divisor de um número ímpar), portanto vamos restringir nossa atenção a números ímpares. Aqui vão alguns resultados:

$$9 \nmid 2^8 - 1 = 255, \qquad 15 \nmid 2^{14} - 1 = 16,383, \qquad 21 \nmid 2^{20} - 1 = 1,048,575,$$

$$25 \nmid 2^{24} - 1 = 16,777,215.$$

Isso sugere que talvez poderíamos testar se o número n é ou não um primo verificando se a relação $n|2^{n-1} - 1$ se verifica ou não. Essa é uma ótima idéia, mas ela tem várias limitações sérias.

Como computar potências GRANDES? É fácil escrever a fórmula $2^{n-1} - 1$, mas é uma coisa bem diferente computá-la! Parece que para obter 2^{n-1}, temos que multiplicar 2 $n-2$ vezes por 2. Para um número de 100-dígitos n, isso é cerca de 10^{100} passos, o que nunca seremos capazes de realizar.

Mas, podemos ser espertos quando computamos 2^{n-1}. Vamos ilustrar isso no exemplo de 2^{24}: poderíamos começar com $2^3 = 8$, elevá-lo ao quadrado, para obter $2^6 = 62$, elevá-lo ao quadrado novamente para obter $2^{12} = 4096$, e elevá-lo ao quadrado uma vez mais para obter $2^{24} = 16,777,216$. Ao invés de 23 multiplicações, precisamos de apenas 5.

Parece que esse truque apenas funcionou porque 24 era divisível por potência tão grande de 2, e pudemos computar 2^{24} pela elevação ao quadrado repetida, começando a partir de um número pequeno. Portanto vamos mostrar como fazer um truque semelhante se o expoente é um inteiro menos amigável, digamos 29. Aqui está uma maneira de computar 2^{29}:

$$2^2 = 4, \quad 2^3 = 8, \quad 2^6 = 64, \quad 2^7 = 128, \quad 2^{14} = 16,384,$$

$$2^{28} = 268,435,456, \quad 2^{29} = 536,870,912.$$

É talvez melhor ler essa seqüência de trás para frente: se temos que computar uma potência ímpar de 2, a obtemos multiplicando a potência anterior por 2; se temos que computar uma potência par, a obtemos elevando ao quadrado a potência menor apropriada.

6.47 Mostre que se n tem k bits na base 2, então 2^n pode ser computado usando menos que $2k$ multiplicações.

Como evitar números GRANDES? Mostramos como suplantar a primeira dificuldade; mas as computações acima revelam a segunda: os números ficam grandes demais! Vamos supor que que n tem 100 dígitos; então 2^{n-1} não é apenas astronômico: o número de seus dígitos é astronômico. Nunca poderíamos escrevê-lo, imagine verificar se ele é divisível por n.

A saída é dividir por n assim que obtivermos qualquer número que seja maior que n, e simplesmente trabalhar com o resto da divisão (ou poderíamos dizer que trabalhamos em aritmética modular com modulus n; não teremos que fazer divisões, portanto n não tem que ser um primo). Por exemplo, se desejamos verificar se $25|2^{24} - 1$, então temos que computar 2^{24}. Como acima, começamos computando $2^3 = 8$, então eleve-o ao quadrado para obter $2^6 = 64$. Substituimo-lo imediatamente pelo resto da divisão $64 : 25$, que é 14. Então computamos 2^{12} elevando 2^6 ao quadrado, mas ao invés disso elevamos 14 ao quadrado para obter 196, que substituimos pelo resto da divisão $196 : 25$, que é 21. Finalmente, obtemos 2^{24} elevando 2^{12} ao quadrado, mas ao invés disso elevamos 21 ao quadrado para obter 441, e aí dividimos isso por 25 para obter o resto 16. Como $16 - 1 = 15$ não é divisível por 25, segue que 25 não é um primo.

Isso não parece uma conclusão impressionante, considerando a trivialidade do resultado, mas isso foi apenas uma ilustração. Se n tem k bits na base 2, então como vimos, leva apenas $2k$ multiplicações para computar 2^n, e tudo o que temos que fazer é uma divisão (com resto) em cada passo para manter os números pequenos. Nunca temos que lidar com números maiores que n^2. Se n tem 100 dígitos, então n^2 tem 199 ou 200 — não é muito divertido multiplicar à mão, mas um tanto administrável por computador.

Pseudoprimos. Mas aqui vem a terceira limitação do teste de primalidade baseado no Teorema de Fermat. Suponha que realizamos um teste para um número n. Se ele falha (isto é, n não é um divisor de $2^{n-1}-1$), então é claro que sabemos que n não é um primo. Mas suponha que encontramos que $n|2^{n-1}-1$. Podemos concluir que n é um primo? O Teorema de Fermat certamente não justifica essa conclusão. Existem números compostos n para os quais $n|2^{n-1}-1$? Infelizmente, a resposta é sim. O menor desses números é $341 = 11 \cdot 31$. Esse não é um primo mas satisfaz

$$341|2^{340}-1. \tag{6.8}$$

(Como sabemos que essa relação de divisibilidade se verifica, sem computação extensiva? Podemos usar o Pequeno Teorema de Fermat. É suficiente argumentar que ambos 11 e 31 são divisores de $2^{340}-1$, pois então seu produto também o é, 11 e 31 sendo primos diferentes. Pelo pequeno teorema de Fermat

$$11|2^{10}-1.$$

A seguir invocamos o resultado do exercício 6.6: ele implica que

$$2^{10}-1|2^{340}-1.$$

Logo

$$11|2^{340}-1.$$

Para 31, não precisamos do Teorema de Fermat, mas apenas do exercício (6.6) novamente:

$$31 = 2^5-1|2^{340}-1.$$

Isso prova (6.8).)

Tais números, que não são primos mas se comportam como primos no sentido de que o Pequeno Teorema de Fermat com base 2 se torna verdadeiro para eles, são chamados *pseudoprimos* (primos de mentira). Enquanto que eles são um tanto raros (existem apenas 22 deles entre 1 e 10.000), eles realmente mostram que nosso teste de primalidade pode dar um "falso positivo", e por conseguinte (em um sentido matemático estrito) ele não é um teste de primalidade de forma alguma.

(Se podemos suportar cometer um erro de vez em quando, então podemos viver com o teste simples de Fermat com base 2. Se o pior que pode acontecer quando um número composto que se acredita seja primo é que um jogo de computador caia, podemos arriscar isso; se a segurança de um banco, ou um país, depende de não se usar um primo de mentira, temos que encontrar algo melhor.)

Uma idéia que vem resgatar é que não usamos a força total do Teorema de Fermat: podemos também verificar que $n|3^n-3$, $n|5^n-5$, etc. Esses testes podem ser realizados usando os mesmos truques que os descritos acima. E na verdade já os primeiros desses descartam o "primo de mentira" 341: ele não é um divisor de $3^{340}-1$.

A observação a seguir nos diz que isso sempre funciona, pelo menos se somos suficientemente pacientes:

Um inteiro positivo $n > 1$ é um primo se e somente se ele passa no teste de Fermat

$$n \mid a^{n-1}-1$$

para toda base $a = 1, 2, 3, \ldots, n-1$.

O Teorema de Fermat nos diz que primos realmente passam no teste de Fermat para toda base. Por outro lado, se n é composto, então existem números a, $1 \leq a \leq n-1$, que não são primos em relação a n, e todos os tais a falham no teste de Fermat: de fato, se p é um divisor primo comum de a e n, então p é um divisor de a^{n-1}, portanto ele não pode ser um divisor de $a^{n-1} - 1$, e por conseguinte n não pode ser um divisor de $a^{n-1} - 1$.

Mas esse Teste Geral de Fermat não é suficientemente eficiente. Imagine que nos é dado um número natural n, com algumas centenas de dígitos, e desejamos testar se ele é ou não um primo. Podemos realizar o teste de Fermat com base 2. Suponha que ele passe. Então podemos tentar base 3. Suponha que ele passe novamente, etc. Quanto tempo temos que continuar antes que possamos concluir que n é um primo? Olhando para o argumento acima que justifa o Teste Geral de Fermat, vemos que não temos que continuar além do primeiro número tendo um divisor comum com n. É fácil ver que o menor desses números é o menor divisor primo de n. Por exemplo, se $n = pq$, onde p e q são primos distintos, tendo digamos 100 dígitos cada (portanto n tem 199 ou 200 dígitos), então temos que tentar tudo até o menor de p e q, que é mais que 10^{99} tentativas, o que é desesperadamente grande. (E além do mais, se vamos tão longe, de qualquer forma, podemos fazer um teste simples de divisibilidade, sem necessidade de nada sofisticado como o Teorema de Fermat!)

Ao invés de começar com 2, poderíamos começar verificando se o Teorema de Fermat se verifica com qualquer outra base a; por exemplo, poderíamos escolher um inteiro aleatório a na faixa $1 \leq a \leq n-1$. Sabemos que ele falha se atingimos qualquer a que não é primo em relação a n. Isso nos dá uma boa chance de descobrir se n não é um primo? Isso depende de n, mas certos valores de n são definitivamente ruins. Por exemplo, suponha que $n = pq$ onde p e q são primos diferentes. É fácil listar aqueles números a que não são primos em relação a n: esses são os múltiplos de p ($p, 2p, \ldots, (q-1)p, qp$) e os múltiplos de q ($q, 2q, \ldots, (p-1)q, pq$). O número total de tais números a é $q + p - 1$ (pois $pq = n$ ocorre em ambas as listas). Esse número é maior que $2 \cdot 10^{99}$, mas menor que $2 \cdot 10^{100}$, e portanto a probabilidade de que atinjamos um desses números quando escolhemos um a aleatório é menor que

$$\frac{2 \cdot 10^{100}}{10^{199}} = 2 \cdot 10^{-99},$$

o que mostra que esse evento tem uma probabilidade demasiado pequena de sequer acontecer na prática.

Números de Carmicheal. Nossa próxima esperança é que talvez para um número composto n, o Teste de Fermat falhará muito mais cedo que seu menor divisor primo, ou então, para uma escolha aleatória de a, ele falhará para muitos outros números além daqueles não primos em relação a n. Infelizmente, isso não é sempre o caso. Existem inteiros n, chamados *números de Carmicheal*, que são ainda piores que pseudoprimos: eles passam no teste de Fermat para toda base a prima em relação a n. Em outras palavras, eles satisfazem

$$n | a^{n-1} - 1$$

para todo a tal que $\mathrm{mdc}(n, a) = 1$. O menor desses números é $n = 561$. Embora que tais números sejam muito raros, eles realmente mostram que o teste de Fermat não é completamente satisfatório.

O teste de Miller–Rabin. Mas no final dos anos 1970, M. Rabin e G. Miller encontrarmo uma maneira muito simples de fortalecer o Teorema de Fermat só um pouquinho, e dessa forma suplantar a dificuldade causada pelos números de Carmicheal. Illustramos o método sobre o exemplo de 561. Usamos um pouco de matemática da escola secundária, a saber a identidade $x^2 - 1 = (x - 1)(x + 1)$, para fatorar o número $a^{560} - 1$:

$$\begin{aligned} a^{560} - 1 &= (a^{280} - 1)(a^{280} + 1) \\ &= (a^{140} - 1)(a^{140} + 1)(a^{280} + 1) \\ &= (a^{70} - 1)(a^{70} + 1)(a^{140} + 1)(a^{280} + 1) \\ &= (a^{35} - 1)(a^{35} + 1)(a^{70} + 1)(a^{140} + 1)(a^{280} + 1) \end{aligned}$$

Agora suponha que 561 fosse um primo. Então pelo "Pequeno" Teorema de Fermat, ele tem que dividir $a^{560} - 1$, qualquer que seja a. Se um primo divide um produto, ele divide um dos fatores (exercício 6.9), e portanto pelo menos uma das relações

$$561|a^{35} - 1 \qquad 561|a^{35} + 1 \qquad 561|a^{70} + 1 \qquad 561|a^{140} + 1 \qquad 561|a^{280} + 1$$

tem que se verificar. Mas já para $a = 2$, nenhuma dessas relações se verifica.

O teste de Miller–Rabin teste é uma elaboração dessa idéia. Dado um inteiro ímpar $n > 1$ que desejamos testar para primalidade, escolhemos um inteiro a da faixa $0 \leq a \leq n - 1$ aleatoriamente, e consideramos $a^n - a$. Fatoramo-lo como $a(a^{n-1} - 1)$, e aí continuamos a fatorá-lo, usando a identidade $x^2 - 1 = (x - 1)(x + 1)$, até onde pudermos. Então testamos se um dos fatores tem que ser divisível por n.

Se o teste falha, podemos ter certeza de que n não é um primo. Mas o que acontece se ele é bem sucedido? Infelizmente, isso ainda pode acontecer mesmo se n for composto; mas o ponto crucial é que *esse teste dá um falso positivo com probabilidade menor que* $1/2$ (lembre-se que escolhemos um a aleatório).

Chegando a uma conclusão errada metade das vezes não soa tão bom; mas podemos repetir o experimento várias vezes. Se o repetirmos 10 vezes (com um a novo, aleatoriamente escolhido a cada vez), a probabilidade de um falso positivo é menor que $2^{-10} < 1/1000$ (pois para concluir que n é primo, todas as 10 tentativas têm que dar um falso positivo, independentemente uma da outra). Se repetirmos o experimento 100 vezes, a probabilidade de um falso positivo cai abaixo de $2^{-100} < 10^{-30}$, que é astronomicamente pequena.

Portanto esse algoritmo, quando repetido com freqüência suficiente, testa primalidade com probabilidade de erro que é muito menor que a probabilidade de, digamos, falha de hardware, e por conseguinte ele é um tanto adequado para propósitos práticos. É largamente usado em programas como Maple ou Mathematica e em criptografia.

Suponha que testemos a primalidade de um número n e encontramos que ele é composto. Então gostaríamos de achar sua fatoração prima. É fácil ver que ao invés disso, poderíamos pedir menos: para uma decomposição de n no produto de dois inteiros positivos menores: $n = ab$. Se tivermos um método de encontrar tal decomposição

eficientemente, então podemos continuar e testar a primalidade de a e b. Se eles forem primos, encontramos a fatoração prima de n; se (digamos) a não é um primo, podemos usar nosso método de encontrar uma decomposição de a no produto de dois inteiros menores etc. Como n tem no máximo $\log_2 n$ fatores primos (exercício 6.10), temos que repetir isso no máximo $\log_2 n$ vezes (que é menos que a sua quantidade de bits).

Mas infelizmente (ou felizmente? veja o Capítulo 15 sobre criptografia) não se conhece um método eficiente de se escrever um número composto como um produto de dois inteiros menores. Seria muito importante encontrar um método eficiente de fatoração, ou dar uma prova matemática de que nenhum tal método existe; mas não sabemos qual é a resposta.

6.48 Mostre que 561 é um número de Carmicheal; mais exatamente, mostre que $561|a^{561} - a$, para todo inteiro a. [Dica: como $561 = 3 \cdot 11 \cdot 17$, basta provar que $3|a^{561} - a$, $11|a^{561} - 1$ e $17|a^{561} - a$. Prove essas relações separadamente, usando o método da prova do fato de que $341|2^{340} - 1$.]

Exercícios de Revisão

6.49 Prove que se $c \neq 0$ e $ac|bc$ então $a|b$.

6.50 Prove que se $a|b$ e $a|c$, então $a|b^2 + 3c + 2^b c$.

6.51 Prove que todo primo maior que 3 dá um resto de 1 ou -1 se dividido por 6.

6.52 Suponha que $a > 1$, e $k, n > 0$. Prove que $a^k - 1|a^n - 1$ se e somente se $k|n$.

6.53 Prove que se $a > 3$, então a, $a + 2$ e $a + 4$ não podem ser todos primos. Eles podem ser todos potências de primos?

6.54 Quantos inteiros existem que não são divisíveis por qualquer que seja o primo maior que 20 e não são divisíveis pelo quadrado de qualquer que seja o primo?

6.55 Ache a fatoração prima de (a) $\binom{20}{10}$; (b) $20!$.

6.56 Mostre que um número com 30 dígitos não pode ter mais que 100 fatores primos.

6.57 Mostre que um número com 160 dígitos tem uma potência de primo como divisor que é pelo menos 100. Isso não é verdadeiro se desejamos um divisor primo que seja pelo menos 100.

6.58 Encontre o número de divisores (positivos) de n, para $1 \leq n \leq 20$ (exemplo: 6 tem 4 divisores: 1,2,3,6). Quais desses números têm um número ímpar de divisores? Formule uma conjectura e prove-a.

6.59 Ache o m.d.c. de 100 e 254, usando o Algoritmo Euclideano..

6.60 Encontre pares de inteiros para os quais o Algoritmo Euclideano leva (a) 2 passos; (b) 6 passos.

6.61 Retomando os números de Lucas L_n introduzidos no Exercício 4.14, prove o seguinte:
(a) $\mathrm{mdc}(F_{3k}, L_{3k}) = 2$;
(b) se n não é um múltiplo de 3, então $\mathrm{mdc}(F_n, L_n) = 1$;
(c) $L_{6k} \equiv 2 \pmod 4$.

6.62 Prove que para todo inteiro positivo m existe um número de Fibonacci divisível por m (bem, obviamente, $F_0 = 0$ é divisível por qualquer m—queremos dizer um maior que esse).

6.63 Encontre inteiros x e y tais que $25x + 41y = 1$.

6.64 Encontre inteiros x e y tais que

$$2x + y \equiv 4 \pmod{17}$$

$$5x - 5y \equiv 9 \pmod{17}$$

6.65 Prove que $\sqrt[3]{5}$ é irracional.

6.66 Prove que as duas formas do Teorema de Fermat, Teorema 6.5.1 e (6.1), são equivalentes.

6.67 Mostre que se $p > 2$ é um modulus primo, então

$$\overline{\frac{1}{2}} = \overline{\frac{p+1}{2}}.$$

6.68 Suponha que nos são dados $n+1$ números do conjunto $\{1, 2, \ldots, 2n\}$. Prove que existem dois números entre eles tais que um divide o outro.

6.69 Qual é o número de inteiros positivos não maiores que 210, não divisíveis por 2,3 ou 7?