Primos de Mersenne

(e outros primos muito grandes)

Carlos Gustavo T. A. Moreira, Nicolau C. Saldanha

Introdução

Nosso objetivo neste livro é descrever o processo utilizado para encontrar os maiores números primos conhecidos. Em março de 2008, os seis maiores primos conhecidos são da forma $M_p = 2^p - 1$ para $p = 32582657, 30402457, 25964951, 24036583, 20996011, 13466917$. Estes são os únicos primos conhecidos com mais de 4000000 de algarismos.

Primos da forma $2^p - 1$, com p primo, têm sido estudados há séculos e são conhecidos como *primos de Mersenne*; não é difícil demonstrar que $2^p - 1$ só pode ser primo quando p é primo. Parte do interesse em primos de Mersenne deve-se à sua estreita ligação com números perfeitos. Um número perfeito é um inteiro positivo que é igual à soma de seus divisores próprios (como $6 = 1+2+3$ e $28 = 1+2+4+7+14$); os números perfeitos pares são precisamente os números da forma $2^{p-1}(2^p - 1)$ onde $2^p - 1$ é primo (um primo de Mersenne).

Talvez o primeiro resultado não trivial sobre primos de Mersenne seja devido a Hudalricus Regius que em 1536 mostrou que $2^p - 1$ não precisa ser primo sempre que p for primo: $2^{11} - 1 = 2047 = 23 \cdot 89$. Em 1603, Pietro Cataldi tinha corretamente verificado a primalidade de $2^{17} - 1$ e $2^{19} - 1$ e afirmou (incorretamente) que $2^p - 1$ também era primo para $p = 23$, 29, 31 e 37. Em 1640, Fermat mostrou que $2^{23} - 1$ e $2^{37} - 1$ são compostos. Em 1644, o monge Marin Mersenne (1588-1648) afirmou por sua vez (também incorretamente) que $2^p - 1$ era primo para

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 \text{ e } 257$$

e composto para os demais valores de $p \leq 257$. Esta afirmação demoraria séculos para ser completamente corrigida.

Em 1738, Euler mostrou que $2^{29} - 1$ é composto e em 1750, verificou que $2^{31} - 1$ é primo. Lucas desenvolveu um algoritmo para testar a primalidade de

números de Mersenne e em 1876 verificou que $2^{127}-1$ é primo; este número permaneceria por muito tempo como o maior primo conhecido (ver [**Lucas**]). Só em 1947 a lista dos primos até 257 foi varrida: os valores de p nesta faixa para os quais 2^p-1 é primo são

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 \text{ e } 127.$$

O algoritmo de Lucas foi posteriormente melhorado por Lehmer para dar o seguinte critério: sejam $S_0 = 4$, $S_1 = 4^2 - 2 = 14$, ..., $S_{k+1} = S_k^2 - 2$; dado $p > 2$, $2^p - 1$ é primo se e somente se S_{p-2} é múltiplo de $2^p - 1$. Esta seqüência cresce muito rápido, mas basta fazer as contas módulo $2^p - 1$: temos assim o chamado critério de Lucas-Lehmer (ver [**Lehmer**]).

Em 1951, computadores eletrônicos começaram a ser usados para procurar grandes números primos. Desde então foram encontrados os seguintes valores de p para os quais M_p é primo: 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457 e 32582657. Em todos os casos foi usado o critério de Lucas-Lehmer. Os últimos dez foram encontrados com a ajuda de computadores pessoais: se você tem um computador você também pode participar da busca do próximo número de Mersenne (veja as instruções em `www.mersenne.org`).

Note que um número de Mersenne M_p é escrito na base 2 como $111\ldots111$, com p algarismos. Uma generalização natural seriam os números escritos como $111\ldots111$ em outra base, isto é, números da forma $(B^p - 1)/(B - 1)$, onde B é a base. É fácil ver que um tal número só pode ser primo se p for primo. No caso $B = 10$ estes números são conhecidos como *repunits*. Não se conhece um critério análogo ao de Lucas-Lehmer para testar a primalidade de números deste tipo quando $B > 2$. O maior primo conhecido desta forma é $(28839^{8317} - 1)/28838$, que tem 37090 algarismos. Os únicos repunits (comprovadamente) primos conhecidos são para $p = 2, 19, 23, 317, 1031$. Recentemente (entre 1999 e 2007), foram descobertos os seguintes valores de p para os quais os repunits correspondentes são *provavelmente* primos, i.e., passam por diversos testes probabilísticos de primalidade (veja o Capítulo 3 para uma discussão sobre testes determinísticos e probabilísticos de primalidade): 49081, 86453, 109297 e 270343. De acordo com os testes já realizados, qualquer outro repunit primo deve ter mais de 400000 dígitos.

No primeiro capítulo veremos algumas idéias básicas de teoria dos números. Inicialmente apresentaremos a definição e as propriedades mais importantes do

mdc e demonstraremos o teorema fundamental da aritmética. Depois apresentaremos a linguagem de congruências, o teorema chinês dos restos e os teoremas de Fermat, Euler e Wilson. Estudaremos a função φ de Euler, fórmula de inversão de Möbius e bases de numeração. Veremos o teorema dos números primos (com demonstração de uma versão fraca) e comentaremos vários resultados e problemas em aberto famosos sobre primos.

O segundo capítulo, um pouco mais avançado que o primeiro, começa com um pouco de álgebra: falamos sobre corpos e polinômios. Estaremos especialmente interessados em corpos finitos e demonstraremos que em todo corpo finito existe uma raiz primitiva. Depois discutiremos a existência de soluções para a congruência $X^2 \equiv a \pmod{n}$ e reciprocidade quadrática.

O terceiro capítulo é de certa forma o mais importante do livro: nele discutiremos como gerar grandes primos ou testar a primalidade de grandes inteiros. Faremos inicialmente algumas considerações gerais e depois discutiremos testes de primalidade para n quando é conhecida uma fatoração de $n-1$ ou de $n+1$. Primos de Mersenne são um caso muito particular desta segunda situação. Daremos neste capítulo duas demonstrações para o critério de Lucas-Lehmer.

No quarto capítulo discutiremos aspectos computacionais de implementações de testes de primalidade, especialmente do teste de Lucas-Lehmer. Uma questão importantíssima para garantir a rapidez de uma implementação é a multiplicação rápida de inteiros grandes; discutiremos brevemente dois algoritmos: o de Karatsuba e FFT (fast Fourier transform).

Duas referências que foram muito usadas neste livro são o excelente livro de Paulo Ribenboim, *Nombres premiers, mystères et records* e a também excelente home page sobre primos de Chris Caldwell [1] onde, entre outras coisas, podem ser sempre encontradas as listas atualizadas dos maiores primos conhecidos.

Carlos Gustavo T. de A. Moreira
IMPA, Estr. D. Castorina 110
Rio de Janeiro, RJ 22460-320
gugu@impa.br, http://www.impa.br/~gugu

Nicolau C. Saldanha
Depto. de Matemática, PUC-Rio
R. Mq. de S. Vicente 225
Rio de Janeiro, RJ 22453-900
nicolau@mat.puc-rio.br, http://www.mat.puc-rio.br/~nicolau

[1] http://www.utm.edu/research/primes

Capítulo 1

Divisibilidade e congruências

Neste primeiro capítulo veremos os tópicos básicos de teoria dos números, como divisibilidade, congruências e aritmética módulo n.

1.1 Divisão euclidiana e o teorema fundamental da aritmética

A divisão euclidiana, ou divisão com resto, é uma das quatro operações que toda criança aprende na escola. Sua formulação precisa é: dados $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$ existem $q, r \in \mathbb{Z}$ com $0 \leq r < |b|$ e $a = bq + r$. Tais q e r estão unicamente determinados e são chamados o *quociente* e *resto* da divisão de a por b. Se $b > 0$ podemos definir $q = \lfloor a/b \rfloor$ e se $b < 0$, $q = \lceil a/b \rceil$; em qualquer caso, $r = a - bq$. O resto r é às vezes denotado por $a \bmod b$; definimos $a \bmod 0 = a$. Lembramos que $\lfloor x \rfloor$ denota o único inteiro k tal que $k \leq x < k + 1$ e $\lceil x \rceil$ o único inteiro k tal que $k - 1 < x \leq k$.

Dados dois inteiros a e b (em geral com $b \neq 0$) dizemos que b *divide* a, ou que a é um *múltiplo* de b, e escrevemos $b|a$, se existir $q \in \mathbb{Z}$ com $a = qb$. Se $a \neq 0$, também dizemos que b é um *divisor* de a. Assim, $b|a$ se e somente se $a \bmod b = 0$.

Proposição 1.1: Dados $a, b \in \mathbb{Z}$ existe um único $d \in \mathbb{N}$ tal que $d|a$, $d|b$ e, para todo $c \in \mathbb{N}$, se $c|a$ e $c|b$ então $c|d$. Além disso existem $x, y \in \mathbb{Z}$ com $d = ax + by$.

Esse natural d é chamado o *máximo divisor comum*, ou mdc, entre a e b. Escrevemos $d = \text{mdc}(a, b)$ ou (se não houver possibilidade de confusão) $d = (a, b)$.

Dem: O caso $a = b = 0$ é trivial (temos $d = 0$). Nos outros casos, seja $I(a, b) = \{ax + by; x, y \in \mathbb{Z}\}$ e seja $d = ax_0 + by_0$ o menor elemento positivo de $I(a, b)$. Como $d \in \mathbb{N}^*$, existem $q, r \in \mathbb{Z}$ com $a = dq + r$ e $0 \leq r < d$. Temos $r = a - dq = a(1 - qx_0) + b(-qy_0) \in I(a, b)$; como $r < d$ e d é o menor elemento positivo de $I(a, b)$, $r = 0$ e $d|a$. Analogamente, $d|b$. Suponha agora que $c|a$ e $c|b$; temos $c|ax + by$ para quaisquer valores de x e y donde, em particular, $c|d$. ■

O *algoritmo de Euclides* para calcular o mdc baseia-se nas seguintes observações simples. Se $a = bq + r$, $0 \leq r < b$, temos (com a notação da demonstração acima) $I(a, b) = I(b, r)$, donde $(a, b) = (b, r)$. Definindo $a_0 = a$, $a_1 = b$ e $a_n = a_{n+1}q_{n+2} + a_{n+2}$, $0 \leq a_{n+2} < a_{n+1}$ (ou seja, a_{n+2} é o resto da divisão de a_n por a_{n+1}) temos $(a, b) = (a_0, a_1) = (a_1, a_2) = (a_2, a_3) = \cdots = (a_n, a_{n+1})$ para qualquer valor de n. Seja N o menor natural para o qual $a_{N+1} = 0$: temos $(a, b) = (a_N, 0) = a_N$.

Lema 1.2: *Se* $(a, b) = 1$ *e* $a|bc$ *então* $a|c$.

Dem: Como $(a, b) = 1$, existem $x, y \in \mathbb{Z}$ com $ax + by = 1$, logo $a|c = acx + bcy$. ■

Quando $(a, b) = 1$ dizemos que a e b são *primos entre si*. Um natural $p > 1$ é chamado *primo* se os únicos divisores positivos de p são 1 e p. Um natural $n > 1$ é chamado *composto* se admite outros divisores além de 1 e n.

Claramente, se p é primo e $p \nmid a$ temos $(p, a) = 1$. Usando o lema anterior e indução temos o seguinte resultado:

Corolário 1.3: *Sejam* p *um número primo e sejam* $a_1, \ldots a_m \in \mathbb{Z}$. *Se* $p|a_1 \cdots a_m$ *então* $p|a_i$ *para algum* i, $1 \leq i \leq n$.

Estamos agora prontos para enunciar e provar o teorema que diz que todo inteiro admite fatoração única como produto de primos.

Teorema 1.4: (Teorema fundamental da aritmética) Seja $n \geq 2$ um número natural. Podemos escrever n de uma única forma como um produto

$$n = p_1 \cdots p_m$$

onde $m \geq 1$ é um natural e $p_1 \leq \ldots \leq p_m$ são primos.

Dem: Mostramos a existencia da fatoração por indução. Se n é primo não há o que provar (escrevemos $m = 1$, $p_1 = n$). Se n é composto podemos escrever $n = ab$, $a, b \in \mathbb{N}$, $1 < a < n$, $1 < b < n$. Por hipótese de indução, a e b se decompõem como produto de primos. Juntando as fatorações de a e b (e reordenando os fatores) obtemos uma fatoração de n.

Vamos agora mostrar a unicidade, também por indução. Suponha que

$$n = p_1 \cdots p_m = q_1 \cdots q_{m'},$$

com $p_1 \leq \ldots \leq p_m$, $q_1 \leq \ldots \leq q_{m'}$. Como $p_1 | q_1 \cdots q_{m'}$ temos $p_1 | q_i$ para algum valor de i, donde, como q_i é primo, $p_1 = q_i$ e $p_1 \geq q_1$. Analogamente temos $q_1 \leq p_1$, donde $p_1 = q_1$. Mas por hipótese de indução

$$n/p_1 = p_2 \cdots p_m = q_2 \cdots q_{m'}$$

admite uma única fatoração, donde $m = m'$ e $p_i = q_i$ para todo i. ■

Outra forma de escrever a fatoração é

$$n = p_1^{e_1} \cdots p_m^{e_m},$$

com $p_1 < \cdots < p_m$, $e_i > 0$. Ainda outra formulação é escrever

$$n = 2^{e_2} 3^{e_3} 5^{e_5} \cdots p^{e_p} \cdots$$

onde o produto é tomado sobre *todos* os primos mas apenas um número finito de expoentes é maior do que zero.

Segue deste teorema o outro algoritmo comum para calcular o mdc de dois números: fatoramos os dois números e tomamos os fatores comuns com os menores expoentes. Este algoritmo é bem menos eficiente do que o de Euclides para inteiros grandes (que em geral não sabemos fatorar) mas é instrutivo saber que os dois algoritmos dão o mesmo resultado.

Corolário 1.5: *Se* $(a, n) = (b, n) = 1$ *então* $(ab, n) = 1$.

Dem: Evidente a partir do algoritmo descrito acima. ■

Teorema 1.6: (Euclides) *Existem infinitos números primos.*

Dem: Suponha por absurdo que $p_1, p_2, ..., p_m$ fossem *todos* os primos. O número $N = p_1 \cdot p_2 \cdots p_m + 1 > 1$ não seria divisível por nenhum primo, o que contradiz o teorema fundamental da aritmética. ■

Observe que *não* provamos que $p_1 \cdot p_2 \cdots p_m + 1$ é primo para algum conjunto finito de primos (por exemplo, os m primeiros primos). Aliás, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$, $2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209 = 11 \cdot 19$, $4! + 1 = 25 = 5^2$ e $8! - 1 = 40319 = 23 \cdot 1753$ não são primos. Não existe nenhuma fórmula simples conhecida que gere sempre números primos. Veja a seção 3.1.

1.2 Congruências

Sejam $a, b, n \in \mathbb{Z}$. Dizemos que a *é congruente* a b *módulo* n, e escrevemos $a \equiv b \pmod{n}$, se $n | b - a$. Como a congruência módulo 0 é a igualdade e quaisquer inteiros são côngruos módulo 1, em geral estamos interessados em $n > 1$.

Proposição 1.7: *Para quaisquer* $a, a', b, b', c, n \in \mathbb{Z}$ *temos:*

(a) $a \equiv a \pmod{n}$;

(b) *se* $a \equiv b \pmod{n}$ *então* $b \equiv a \pmod{n}$;

(c) *se* $a \equiv b \pmod{n}$ *e* $b \equiv c \pmod{n}$ *então* $a \equiv c \pmod{n}$;

(d) *se* $a \equiv a' \pmod{n}$ *e* $b \equiv b' \pmod{n}$ *então* $a + b \equiv a' + b' \pmod{n}$;

(e) *se* $a \equiv a' \pmod{n}$ *então* $-a \equiv -a' \pmod{n}$;

(f) *se* $a \equiv a' \pmod{n}$ *e* $b \equiv b' \pmod{n}$ *então* $a \cdot b \equiv a' \cdot b' \pmod{n}$.

Dem: Para o item (a) basta observar que $n | a - a = 0$. Em (b), se $n | b - a$ então $n | a - b = -(b - a)$. Em (c), se $n | b - a$ e $n | c - b$ então $n | c - a = (c - b) + (b - a)$. Em (d), se $n | a' - a$ e $n | b' - b$ então $n | (a' + b') - (a + b) = (a' - a) + (b' - b)$. Em (e), se $n | a' - a$ então $n | (-a') - (-a) = -(a' - a)$. Em (f), se $n | a' - a$ e $n | b' - b$ então $n | a'b' - ab = a'(b' - b) + b(a' - a)$. ■

Os itens (a), (b) e (c) da proposição acima dizem, nesta ordem, que a relação $\equiv \pmod{n}$ ("ser côngruo módulo n") é uma relação reflexiva, simétrica e transitiva. Relações satisfazendo estas três propriedades são chamadas *relações de equivalência*. Dada uma relação de equivalência $\sim$ sobre um conjunto X e um elemento $x \in X$ definimos a *classe de equivalência* $\overline{x}$ de x como

$$\overline{x} = \{y \in X | y \sim x\};$$

observe que $x \sim y$ se e somente se $\overline{x} = \overline{y}$. As classes de equivalência formam uma partição de X, i.e., uma coleção de subconjuntos não vazios e disjuntos de X cuja união é X. O conjunto $\{\overline{x} | x \in X\}$ das classes de equivalência é chamado o *quociente* de X pela relação de equivalência $\sim$ e é denotado por $X/\sim$.

Aplicando esta construção geral ao nosso caso, definimos o quociente $\mathbb{Z}/(\equiv \pmod{n})$, chamado por simplicidade de notação de $\mathbb{Z}/(n)$, $\mathbb{Z}/n\mathbb{Z}$ ou às vezes $\mathbb{Z}_n$. Dado $a \in \mathbb{Z}$, a definição de $\overline{a}$ como um subconjunto de $\mathbb{Z}$ raramente será importante: o importante é sabermos que $\overline{a} = \overline{a'}$ se e somente se $a \equiv a' \pmod{n}$. Se $n > 0$, a divisão euclidiana diz que todo inteiro a é côngruo a um único inteiro a' com $0 \leq a' < n$; podemos reescrever este fato na nosso nova linguagem como

$$\mathbb{Z}/(n) = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Quando não houver possibilidade de confusão omitiremos as barras e chamaremos os elementos de $\mathbb{Z}/(n)$ simplesmente de $0, 1, \ldots, n-1$.

Os itens (d), (e) e (f) da proposição dizem que as operações de soma, diferença e produto são compatíveis com a relação de congruência. É esta propriedade que torna congruências tão úteis, nos possibilitando fazer contas módulo n. Podemos por exemplo escrever

$$\begin{aligned} 196883 &= 1 \cdot 10^5 + 9 \cdot 10^4 + 6 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10^1 + 3 \cdot 10^0 \\ &\equiv 1 \cdot 1^5 + 9 \cdot 1^4 + 6 \cdot 1^3 + 8 \cdot 1^2 + 8 \cdot 1^1 + 3 \cdot 1^0 \\ &= 1 + 9 + 6 + 8 + 8 + 3 \\ &= 35 \\ &\equiv 8 \pmod{9}, \end{aligned}$$

já que $10 \equiv 1 \pmod{9}$ (mostrando assim porque funciona o conhecido critério de divisibilidade por 9). Uma formulação mais abstrata da mesma idéia é dizer que as operações $+$ e $\cdot$ *passam ao quociente*, i.e., que podemos definir

$$+ : \mathbb{Z}/(n) \times \mathbb{Z}/(n) \to \mathbb{Z}/(n), \qquad \cdot : \mathbb{Z}/(n) \times \mathbb{Z}/(n) \to \mathbb{Z}/(n)$$

por $\overline{a}+\overline{b}=\overline{a+b}$ e $\overline{a}\cdot\overline{b}=\overline{a\cdot b}$. A dúvida à primeira vista seria se a escolha de a e b não afeta a resposta: afinal existem infinitos inteiros a' e b' com $\overline{a}=\overline{a'}$ e $\overline{b}=\overline{b'}$. Os itens (d) e (f) da proposição são exatamente o que precisamos: eles nos dizem que nestas condições $\overline{a+b}=\overline{a'+b'}$ e $\overline{a\cdot b}=\overline{a'\cdot b'}$.

Proposição 1.8: *Sejam* $a, n \in \mathbb{Z}$, $n>0$. *Então existe* $b \in \mathbb{Z}$ *com* $ab \equiv 1 \pmod{n}$ *se e somente se* $(a,n)=1$.

Dem: Se $ab \equiv 1 \pmod{n}$ temos $nk = 1-ab$ para algum k, donde $(a,n)|ab+nk=1$ e $(a,n)=1$. Se $(a,n)=1$ temos $ax+ny=1$ para certos inteiros x e y, donde $ax \equiv 1 \pmod{n}$. ■

Dizemos portanto que a é *invertível* [1] módulo n quando $(a,n)=1$ e chamamos b com $ab \equiv 1 \pmod{n}$ de *inverso* de a módulo n. O inverso é sempre único módulo n: se $ab \equiv ab' \equiv 1 \pmod{n}$ temos $b \equiv ab^2 \equiv abb' \equiv b' \pmod{n}$.

Corolário 1.9: *Se* $(a,n)=1$ *e* $ab \equiv ab' \pmod{n}$ *então* $b \equiv b' \pmod{n}$.

Dem: Basta escrever $b \equiv abc \equiv ab'c \equiv b' \pmod{n}$ onde c é o inverso de a módulo n. ■

Definimos $(\mathbb{Z}/(n))^* \subset \mathbb{Z}/(n)$ por

$$(\mathbb{Z}/(n))^* = \{\overline{a}; (a,n)=1\}.$$

Observe que o produto de elementos de $(\mathbb{Z}/(n))^*$ é sempre um elemento de $(\mathbb{Z}/(n))^*$ (corolário 1.5).

Teorema 1.10: (Teorema Chinês dos restos) *Se* $(m,n)=1$ *então*

$$f : \mathbb{Z}/(mn) \to \mathbb{Z}/(m) \times \mathbb{Z}/(n)$$
$$\overline{a} \mapsto (\overline{a},\overline{a})$$

é uma bijeção. Além disso, a imagem por f *de* $(\mathbb{Z}/(mn))^*$ *é* $(\mathbb{Z}/(m))^* \times (\mathbb{Z}/(n))^*$.

Note que cada $\overline{a}$ na definição de f é tomado em relação a um módulo diferente. A função está bem definida pois $a \bmod mn$ determina $a \bmod m$ e $a \bmod n$.

Dem: Como $\mathbb{Z}/(mn)$ e $\mathbb{Z}/(m)\times\mathbb{Z}/(n)$ têm mn elementos cada, para provar que f é bijetiva basta verificar que f é injetiva. E, de fato, se $a \equiv a' \pmod{m}$

[1] Alguns autores preferem escrever *inversível*. Os interessados em discutir esta questão ortográfica devem escrever para o Prof. Zoroastro Azambuja, IMPA, Estr. D. Castorina 110, Rio de Janeiro, RJ

e $a \equiv a' \pmod{n}$ então $m|(a-a')$ e $n|(a-a')$, donde $mn|(a-a')$ e $a \equiv a' \pmod{mn}$. A imagem de $(\mathbb{Z}/(mn))^*$ é $(\mathbb{Z}/(m))^* \times (\mathbb{Z}/(n))^*$ pois $(a, mn) = 1$ se e somente se $(a, m) = (a, n) = 1$. ■

Dados inteiros $m_1, m_2, \ldots, m_r$, dizemos que estes inteiros são *primos entre si* se $(m_i, m_j) = 1$ para quaiquer $i \neq j$.

Corolário 1.11: *Se $m_1, m_2, \ldots, m_r$ são inteiros primos entre si. Então*

$$f : \mathbb{Z}/(m_1 m_2 \cdots m_r) \to \mathbb{Z}/(m_1) \times \mathbb{Z}/(m_2) \cdots \mathbb{Z}/(m_r)$$
$$\overline{a} \mapsto (\overline{a}, \overline{a}, \ldots, \overline{a})$$

é uma bijeção.

Dem: Basta aplicar o teorema anterior r vezes. ■

A aplicação mais comum deste teorema é para garantir que existe a com $a \equiv a_i \pmod{m_i}$ onde a_i são inteiros dados quaisquer.

1.3 A função de Euler e o pequeno teorema de Fermat

Definimos $\varphi(n) = |(\mathbb{Z}/(n))^*|$ (onde $|X|$ denota o número de elementos de X). A função φ é conhecida como a *função de Euler*. Temos $\varphi(1) = \varphi(2) = 1$, e, para $n > 2$, $1 < \varphi(n) < n$. Se p é primo, $\varphi(p) = p - 1$; mais geralmente $\varphi(p^k) = p^k - p^{k-1}$ pois $(a, p^k) = 1$ se e somente se a não é múltiplo de p e há p^{k-1} múltiplos de p no intervalo $0 \leq a < p^k$.

Dizemos que os n números inteiros $a_1, a_2, \ldots, a_n$ formam um *sistema completo de resíduos* (ou s.c.r.) módulo n se $\{\overline{a_1}, \overline{a_2}, \ldots \overline{a_n}\} = \mathbb{Z}/(n)$, isto é, se os a_i representam todas as classes de congruência módulo n. Por exemplo, 0, 1, 2, $\ldots n-1$ formam um s.c.r. módulo n. Equivalentemente, podemos dizer que $a_1, a_2, \ldots, a_n$ formam um s.c.r. módulo n se e somente se $a_i \equiv a_j \pmod{n}$ implicar $i = j$. Os $\varphi(n)$ números inteiros $b_1, b_2, \ldots, b_{\varphi(n)}$ formam um *sistema completo de invertíveis* (s.c.i.) módulo n se

$$\{\overline{b_1}, \overline{b_2}, \ldots \overline{b_{\varphi(n)}}\} = (\mathbb{Z}/(n))^*,$$

isto é, se os b_i representam todas as classes de congruências invertíveis módulo n. Também equivalentemente, $b_1, b_2, \ldots, b_{\varphi(n)}$ formam um s.c.i. módulo n se e somente se $(b_i, n) = 1$ para todo i e $a_i \equiv a_j \pmod{n}$ implicar $i = j$.

Proposição 1.12: *Sejam* $q, r, n \in \mathbb{Z}$, $n > 0$, q *invertível módulo* n, a_1, $a_2, \ldots, a_n$ *um s.c.r. módulo* n e $b_1, b_2, \ldots, b_{\varphi(n)}$ *um s.c.i. módulo* n. *Então* $qa_1 + r, qa_2 + r, \ldots, qa_n + r$ *formam um s.c.r. módulo* n e $qb_1, qb_2, ...qb_{\varphi(n)}$ *formam um s.c.i. módulo n.*

Dem: Se $qa_i + r \equiv qa_j + r \pmod{n}$ então $n|q(a_i - a_j)$ e $a_i \equiv a_j \pmod{n}$, donde $i = j$; com isto provamos que $qa_1 + r, qa_2 + r, \ldots, qa_n + r$ formam um s.c.r..

Como $(q, n) = (b_i, n) = 1$, temos $(qb_i, n) = 1$. Por outro lado, se $qb_i \equiv qb_j \pmod{n}$ temos $b_i \equiv b_j \pmod{n}$ (como no parágrafo anterior) e $i = j$. Isto conclui a demonstração. ■

Teorema 1.13: (Euler) *Sejam* $a, n \in \mathbb{Z}$, $n > 0$, *tais que* $(a, n) = 1$. *Então* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dem: Seja

$$b_1, b_2, \ldots . b_{\varphi(n)}$$

um s.c.i. módulo n. Pela proposição anterior,

$$ab_1, ab_2, \ldots ab_{\varphi(n)}$$

também formam um s.c.i. módulo n. Assim,

$$b_1 \cdot b_2 \cdots b_{\varphi(n)} \equiv ab_1 \cdot ab_2 \cdots ab_{\varphi(n)} \pmod{n}$$

pois módulo n os dois lados têm os mesmos fatores a menos de permutação. Mas isto pode ser reescrito como

$$a^{\varphi(n)}(b_1 \cdot b_2 \cdots b_{\varphi(n)}) \equiv 1 \cdot (b_1 \cdot b_2 \cdots b_{\varphi(n)}) \pmod{n}$$

e pelo corolário 1.9 isto implica $a^{\varphi(n)} \equiv 1 \pmod{n}$. ■

Corolário 1.14: (Pequeno Teorema de Fermat) *Se* p *é primo então, para todo inteiro* a, $a^p \equiv a \pmod{p}$.

Dem: Se $p|a$, então $a^p \equiv a \equiv 0 \pmod{p}$. Caso contrário, $\varphi(p) = p - 1$, $a^{p-1} \equiv 1 \pmod{p}$ e novamente $a^p \equiv a \pmod{p}$. ■

Outra demonstração do pequeno teorema de Fermat é por indução em a usando o binômio de Newton e algumas propriedades de números binomiais. Se $0 < i < p$ temos

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \equiv 0 \pmod{p}$$

pois há um fator p no numerador que não pode ser cancelado com nada que apareça no denominador. Os casos $a = 0$ e $a = 1$ do teorema são triviais. Supondo válido o teorema para a, temos

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

e a indução está completa.

Corolário 1.15: *Se* $(m,n) = 1$ *então* $\varphi(mn) = \varphi(m)\varphi(n)$.

Dem: Construimos uma bijeção entre $(\mathbb{Z}/(mn))^*$ e $(\mathbb{Z}/(m))^* \times (\mathbb{Z}/(n))^*$, o que garante que estes conjuntos têm o mesmo número de elementos. ■

Corolário 1.16: *Se*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$$

com $p_1 < p_2 < \ldots < p_m$ *e* $e_i > 0$ *para todo* i *então*

$$\begin{aligned}\varphi(n) &= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_m^{e_m} - p_m^{e_m-1}) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right).\end{aligned}$$

Dem: Isto segue da fórmula que já vimos para $\varphi(p^e)$ e do corolário anterior. ■

Em particular, se $n > 2$ então $\varphi(n)$ é par.

Mais adiante estudaremos equações do segundo grau em $\mathbb{Z}/(p)$; vejamos desde já um pequeno resultado deste tipo que garante que os únicos a que são seus próprios inversos módulo p são 1 e -1.

Lema 1.17: *Se* p *é primo então as únicas soluções de* $x^2 = 1$ *em* $\mathbb{Z}/(p)$ *são 1 e* -1. *Em particular,se* $x \in (\mathbb{Z}/(p))^* - \{1,-1\}$ *então* $x^{-1} \neq x$ *em* $\mathbb{Z}/(p)$.

Dem: Podemos reescrever a equação como $(x-1)(x+1) = 0$, o que torna o resultado trivial. ■

Teorema 1.18: (Wilson) *Seja* $n > 4$. *Então* $(n-1)! \equiv -1 \pmod{n}$ *se* n *é primo e* $(n-1)! \equiv 0 \pmod{n}$ *se* n *é composto.*

Dem: Se n é composto mas não é o quadrado de um primo podemos escrever $n = ab$ com $1 < a < b < n$: neste caso tanto a quanto b aparecem em $(n-1)!$ e $(n-1)! \equiv 0 \pmod{n}$. Se $n = p^2$, $p > 2$, então p e $2p$ aparecem em $(n-1)!$ e novamente $(n-1)! \equiv 0 \pmod{n}$; isto demonstra que para todo n composto, $n > 4$, temos $(n-1)! \equiv 0 \pmod{n}$.

Se n é primo podemos escrever $(n-1)! \equiv -(2 \cdot 3 \cdots n-2) \pmod{n}$; mas pelo lema anterior podemos juntar os inversos aos pares no produto do lado direito, donde $(n-1)! \equiv -1 \pmod{n}$. ■

1.4 A função de Möbius

Vejamos inicialmente uma propriedade da função φ.

Teorema 1.19: *Para todo natural* n,

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

Este teorema segue facilmente da fórmula que provamos para $\varphi(n)$ na seção anterior. Daremos entretanto uma demonstração *bijetiva*.

Dem: Considere as n frações

$$\frac{0}{n}, \frac{1}{n}, \ldots, \frac{n-1}{n}$$

e simplifique cada uma delas: obtemos assim, para cada $d|n$, $\varphi(d)$ frações com denominador d, donde segue a identidade do enunciado.

Mais formalmente, dado $\overline{a} \in \mathbb{Z}/(n)$, sejam $d = n/(n,a)$ e $a' = a/(n,a)$. Claramente $\overline{a'} \in (\mathbb{Z}/(d))^*$ e definimos assim uma função de $\mathbb{Z}/(n)$ para a união disjunta dos conjuntos $(\mathbb{Z}/(d))^*$, onde d varia sobre os divisores de n. A inversa desta função leva $\overline{a'} \in (\mathbb{Z}/(d))^*$ em $\overline{a}$, $a = na'/d$, donde a função é uma bijeção. ■

O processo de construir g a partir de f como

$$g(n) = \sum_{d|n} f(d)$$

é bastante comum em teoria dos números. Seria interessante poder inverter esta identidade para escrever f a partir de g. O teorema anterior nos mostra que se fazemos $f = \varphi$ na equação acima temos $g(n) = n$; invertendo esta identidade teríamos uma fórmula para φ. O objetivo desta seção é mostrar como fazer este tipo de inversão.

Definimos a *função de Möbius* $\mu : \mathbb{N}^* \to \mathbb{Z}$ por

$$\mu(n) = \begin{cases} (-1)^m, & \text{se } n = p_1 p_2 \cdots p_m, \text{ com } p_1, p_2, \cdots, p_m \text{ primos distintos,} \\ 0, & \text{se } n \text{ tem algum fator primo repetido em sua fatoração.} \end{cases}$$

Assim, $\mu(1) = \mu(6) = \mu(10) = 1$, $\mu(2) = \mu(3) = \mu(5) = \mu(7) = -1$ e $\mu(4) = \mu(8) = \mu(9) = 0$.

Lema 1.20: *Para todo inteiro positivo n temos*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{se } n = 1, \\ 0, & \text{se } n > 1. \end{cases}$$

Dem: O caso $n = 1$ é trivial. Se $n > 1$, seja p um divisor primo de n e seja $n = p^e n'$ com $p \nmid n'$. Temos

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{d|n, p\nmid d} \mu(d) + \sum_{d|n, p|d, p^2\nmid d} \mu(d) + \sum_{d|n, p^2|d} \mu(d) \\ &= \sum_{d|n'} \mu(d) + \sum_{d'|n'} \mu(pd') + 0 \\ &= \sum_{d|n'} \mu(d) - \sum_{d'|n'} \mu(d') \\ &= 0. \end{aligned}$$

■

Teorema 1.21: (Fórmula de inversão de Möbius) *Se para todo* $n > 0$ *temos*

$$g(n) = \sum_{d|n} f(d)$$

então

$$f(n) = \sum_{d|n} \mu(n/d) g(d).$$

Observe que a fórmula do corolário 1.16 para $\varphi(n)$ segue facilmente dos dois teoremas acima.

Dem: Basta provar que

$$f(n) = \sum_{d|n} \mu(n/d) \left(\sum_{d'|d} f(d') \right).$$

Mas, escrevendo $d'' = n/d$ e $m = n/d'$ temos

$$\sum_{d|n} \mu(n/d) \left(\sum_{d'|d} f(d') \right) = \sum_{m|n} \left(\sum_{d''|m} \mu(d'') \right) f(n/m) = f(n).$$

■

Teorema 1.22: (Segunda fórmula de inversão de Möbius) *Sejam* f *e* g *funções reais com domínio* $(0, +\infty)$ *tais que* $f(t) = g(t) = 0$ *para todo* $t < 1$. *Se*

$$g(x) = \sum_{k=1}^{\infty} f\left(\frac{x}{k}\right) = \sum_{1=k}^{\lfloor x \rfloor} f\left(\frac{x}{k}\right)$$

para todo x *então então*

$$f(x) = \sum_{k=1}^{\infty} \mu(k) g\left(\frac{x}{k}\right) = \sum_{1=k} \lfloor x \rfloor \mu(k) g\left(\frac{x}{k}\right).$$

Dem: Basta provar que

$$f(x) = \sum_{k=1}^{\infty} \mu(k) \left(\sum_{r=1}^{\infty} f\left(\frac{x}{kr}\right) \right),$$

mas, tomando $m = kr$ a última soma é igual a

$$\sum_{m=1}^{\infty} \left(\left(\sum_{k|m} \mu(k) \right) f\left(\frac{x}{m}\right) \right)$$

que pelo lema é igual a $f(x)$. ■

Apesar de não estar relacionada com o resto da nossa discussão, não podemos deixar de mencionar a seguinte conjectura.

Conjectura 1.23: (Hipótese de Riemann) *Se $\alpha > 1/2$ então*

$$\lim_{n\to\infty} \frac{1}{n^{\alpha}} \sum_{1\le m}^{n} \mu(m) = 0.$$

Esta é uma das formulações da famosa hipótese de Riemann, um dos problemas em aberto mais importantes da matemática.

Podemos reenunciar esta conjectura assim: seja $f : (0, +\infty) \to \mathbb{R}$ definida por $f(t) = 0$ se $t < 1$ e

$$\sum_{k=1}^{\infty} f(t/k) = 1, \quad \text{se } t \ge 1$$

então, para todo $\alpha > 1/2$,

$$\lim_{t\to\infty} \frac{f(t)}{t^{\alpha}} = 0.$$

De fato, pela segunda fórmula de inversão de Möbius temos

$$f(t) = \sum_{m=1}^{\lfloor t \rfloor} \mu(m).$$

1.5 Bases

A notação usual para naturais é a chamada base 10, com algarismos $0, \ldots, 9$. Isto significa, por exemplo, que

$$196883 = 1 \cdot 10^5 + 9 \cdot 10^4 + 6 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10^1 + 3 \cdot 10^0.$$

O teorema abaixo mostra como escrever qualquer natural em qualquer base d.

Teorema 1.24: *Seja $n \geq 0$ e $d > 1$. Então existe uma única seqüência $a_0, \ldots, a_k, \ldots$ com as seguintes propriedades:*

(a) *para todo k, $0 \leq a_k < d$,*

(b) *existe m tal que se $k \geq m$ então $a_k = 0$,*

(c) $n = \sum_k a_k d^k$.

Dem: Escrevemos $n = n_0 = n_1 d + a_0$, $0 \leq a_0 < d$, $n_1 = n_2 d + a_1$, $0 \leq a_1 < d$, e em geral $n_k = n_{k+1} d + a_k$, $0 \leq a_k < d$. Nossa primeira afirmação é que $n_k = 0$ para algum valor de k. De fato, se $n_0 < d^m$ então $n_1 < d^{m-1}$ e mais geralmente, por indução, $n_k < d^{m-k}$; fazendo $k \geq m$ temos $n_k < 1$ donde $n_k = 0$. Segue daí que $a_k = 0$ para $k \geq m$. A identidade do item (c) é facilmente demonstrada por indução.

Para a unicidade, suponha $\sum_k a_k d^k = \sum_k b_k d^k$. Se as seqüências a_k e b_k são distintas existe um menor índice, digamos j, para o qual $a_j \neq b_j$. Podemos escrever $a_j + \sum_{k>j} a_k d^{k-j} = b_j + \sum_{k>j} b_k d^{k-j}$ donde $a_j \equiv b_j \pmod{d}$, o que é uma contradição. ■

Às vezes é interessante considerar expansões não apenas em outras bases mas com outros conjuntos de algarismos (veremos um exemplo disso no último capítulo). Por exemplo, podemos preferir algarismos negativos pequenos a algarismos positivos grandes e assim um bom conjunto de algarismos na base 10 seria

$$-4, -3, -2, -1, 0, 1, 2, 3, 4, 5.$$

Desta forma, escrevemos $13 = 1 \cdot 10 + 3$ mas escrevemos $9 = 1 \cdot 10 - 1$ e $64 = 1 \cdot 10^2 - 4 \cdot 10 + 4$. Generalizando, os algarismos na base d seriam os inteiros a com $-d/2 < a \leq d/2$, ou seja,

$$a = -\lfloor (d-1)/2 \rfloor, -\lfloor (d-1)/2 \rfloor + 1, \ldots, -1, 0, 1, \ldots, \lfloor d/2 \rfloor - 1, \lfloor d/2 \rfloor.$$

Este conjunto de algarismos nos permite enunciar um teorema análogo ao anterior, com a diferença que agora números negativos não precisam ser tratados em separado.

Teorema 1.25: *Seja $n \in \mathbb{Z}$ e $d > 2$. Então existe uma única seqüência $a_0, \ldots, a_k, \ldots$ com as seguintes propriedades:*

(a) *para todo k, $-d/2 < a_k \leq d/2$,*

(b) *existe* m *tal que se* $k \geq m$ *então* $a_k = 0$,

(c) $n = \sum_k a_k d^k$.

Dem: Escrevemos $n = n_0 = n_1 d + a_0$, $-d/2 < a_0 \leq d/2$, $n_1 = n_2 d + a_1$, $-d/2 < a_1 \leq d/2$, e em geral $n_k = n_{k+1} d + a_k$, $-d/2 < a_k \leq d/2$. Novamente, nossa primeira afirmação é que $n_k = 0$ para algum valor de k. De fato, se

$$-d^m/2 < n_0 \leq d^m/2$$

então, por indução,

$$-d^{m-k}/2 < n_k \leq d^{m-k}/2;$$

fazendo $k \geq m$ temos $n_k = 0$. Segue daí que $a_k = 0$ para $k \geq m$. A identidade do item (c) e a unicidade são demonstradas como no teorema anterior. ■

Pode-se estudar representações na base d com outros conjuntos X de algarismos. Algumas condições mínimas para que X seja um conjunto de algarismos interessante são que $0 \in X$, que X seja um sistema completo de resíduos e que o mdc dos elementos de X seja 1.

1.6 Sobre a distribuição dos números primos

Já vimos que existem infinitos primos; o teorema dos números primos dá uma estimativa de quantos primos existem até um inteiro x, ou seja, descreve a distribuição dos primos. Defina $\pi(x)$ como sendo o número de primos p com $2 \leq p \leq x$.

Teorema 1.26: (Teorema dos números primos)

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

Observe que aqui e em todo o livro log denota o logaritmo natural. Este resultado foi conjecturado por vários matemáticos, inclusive por Legendre e Gauss, mas a demonstração completa só foi encontrada em 1896, por de la Vallée Poussin e Hadamard (independentemante). Não demonstraremos este teorema: as demonstrações elementares conhecidas são todas bastante difíceis (lembramos que uma demonstração é dita *elementar* quando não usa ferramentas avançadas: muitas demonstrações elementares são longas e sofisticadas).

Daremos uma demonstração da seguinte proposição (devida a Tchebycheff) que é claramente uma versão fraca do teorema dos números primos.

Proposição 1.27: *Existem constantes positivas* $c < C$ *tais que*

$$c\frac{x}{\log x} < \pi(x) < C\frac{x}{\log x}$$

para todo $x \geq 2$.

Dem: Observemos inicialmente que $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ é múltiplo de todos os primos p que satisfazem $n < p \leq 2n$. Como

$$\binom{2n}{n} < \sum_{0\leq k\leq 2n} \binom{2n}{k} = 2^{2n},$$

segue que o produto dos primos entre n e $2n$ é menor do que 2^{2n}. Como há $\pi(2n) - \pi(n)$ primos como esses segue que $n^{\pi(2n)-\pi(n)} < 2^{2n}$ (pois todos esses primos são maiores que n), donde $(\pi(2n) - \pi(n)) \log n < 2n \log 2$ e

$$\pi(2n) - \pi(n) < \frac{2n \log 2}{\log n}.$$

Isso implica facilmente, por indução, que

$$\pi(2^{k+1}) \leq \frac{5 \cdot 2^k}{k}$$

(começando com $k = 5$; até $k = 5$ segue de $\pi(n) \leq n/2$). Daí segue que se $2^k < x \leq 2^{k+1}$ então

$$\pi(x) \leq \frac{5 \cdot 2^k}{k} \leq \frac{5x \log 2}{\log x}$$

pois $f(x) = x \log 2/\log x$ é uma função crescente para $x \geq 3$.

Vamos agora provar a outra desigualdade. O expoente do primo p na fatoração de $n!$ é

$$\begin{aligned} w_p(n) &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots \\ &= \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \end{aligned}$$

(esta é uma soma finita pois se $k > \log_p n = \log n/\log p$ então $\lfloor \frac{n}{p^k} \rfloor = 0$). De fato, $\lfloor \frac{n+1}{p^j} \rfloor - \lfloor \frac{n}{p^k} \rfloor$ é sempre 0 ou 1, e é igual a 1 se e só se p^j divide $n+1$. Assim, $w_p(n+1) - w_p(n)$ é igual ao expoente de p na fatoração de $n+1$, o que fornece uma prova por indução do fato acima.

Assim, o expoente de p em $\binom{2n}{n} = (2n)!/n!^2$ é

$$\sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right).$$

Temos agora que $\lfloor \frac{2n}{p^k} \rfloor - 2\lfloor \frac{n}{p^k} \rfloor$ é sempre 0 ou 1 (pois $0 \le x - \lfloor x \rfloor < 1$ para todo x), donde o expoente de p em $\binom{2p}{p}$ é no máximor $\log_p n = \log n/\log p$ para todo primo p. Por outro lado, se $n < p \le 2n$, o expoente de p em $\binom{2p}{p}$ é 1. Assim, se $\binom{2n}{n} = \prod_{p<2n} p^{\alpha_p}$ é a fatoração de $\binom{2n}{n}$ então

$$\begin{aligned}
\log \binom{2n}{n} &= \sum_{p<2n} \alpha_p \log p \\
&= \sum_{p\le n} \alpha_p \log p + \sum_{n<p\le 2n} \log p \\
&\le \pi(n)\log n + (\pi(2n) - \pi(n))\log(2n) \\
&\le \pi(2n)\log(2n)
\end{aligned}$$

donde

$$\pi(2n) \ge \log \binom{2n}{n} / \log(2n) \ge n \log 2/\log(2n)$$

pois

$$\binom{2n}{n} = \frac{2n}{n} \cdot \frac{2n-1}{n-1} \cdots \frac{n+1}{1} \ge 2^n,$$

donde

$$\pi(x) \ge \frac{x \log 2}{\log x}$$

para todo x par, o que implica na mesma estimativa para todo x inteiro, pois $\pi(2k-1) = \pi(2k)$. ■

Corolário 1.28: *Seja $f : \mathbb{N} \to [0, +\infty)$ uma função decrescente. A série*

$$\sum_{p \text{ primo}} f(p)$$

converge se e somente se a série

$$\sum_{n=2}^{\infty} \frac{f(n)}{\log n}$$

converge. Em particular,

$$\sum_{p \text{ primo}} \frac{1}{p} = +\infty.$$

Deixamos a demonstração deste corolário como exercício.

Uma aproximação mais precisa para $\pi(x)$ é dada por

$$\mathrm{Li}(x) = \int_0^x \frac{dt}{\log t},$$

onde tomamos o valor principal desta integral, ou seja,

$$\mathrm{Li}(x) = \lim_{\varepsilon \to 0} \int_{\varepsilon}^{1-\varepsilon} \frac{dt}{\log t} + \int_{1+\varepsilon}^{x} \frac{dt}{\log t};$$

claramente

$$\lim_{x \to \infty} \frac{\mathrm{Li}(x)}{\log(x)/x} = 1.$$

Sabe-se entretanto que

$$|\pi(x) - \mathrm{Li}(x)| \leq Cxe^{-a(\log x)^{3/5}(\log\log x)^{-1/5}}$$

para algum valor das constantes a e C (independente de x). Em particular, para qualquer $k > 0$ existe $C > 0$ tal que,para todo x,

$$|\pi(x) - \mathrm{Li}(x)| \leq C\frac{x}{(\log x)^k},$$

o que mostra que $\mathrm{Li}(x)$ (e mesmo $x/(\log x - 1)$) é uma aproximação de $\pi(x)$ bem melhor do que $x/\log x$.

A hipótese de Riemann, já mencionada, equivale a dizer que para todo $\varepsilon > 0$ existe C com

$$|\pi(x) - \mathrm{Li}(x)| \leq Cx^{1/2+\varepsilon};$$

ninguém sabe demonstrar que esta estimativa seja correta sequer para algum valor de $\varepsilon < 1/2$. A hipótese de Riemann também implica que existe C com

$$|\pi(x) - \mathrm{Li}(x)| \leq Cx^{1/2} \log x,$$

o que daria uma estimativa para o tamanho deste erro muito melhor de que as que se sabe demonstrar. Por outro lado, sabe-se demonstrar que não pode existir nenhuma estimativa muito melhor do que esta para $|\pi(x) - \mathrm{Li}(x)|$: existe uma constante $C > 0$ e inteiros x_1 e x_2 arbitrariamente grandes com

$$\pi(x_1) - \mathrm{Li}(x_1) < -C\frac{\sqrt{x_1}\log\log\log x_1}{\log x_1},$$
$$\pi(x_2) - \mathrm{Li}(x_2) > C\frac{\sqrt{x_2}\log\log\log x_2}{\log x_2}.$$

1.7 Outros resultados e conjecturas sobre primos

Nesta seção veremos o enunciado de alguns resultados clássicos sobre números primos. Também veremos vários problemas em aberto famosos.

Teorema 1.29: (Dirichlet) *Dados naturais* a, d *com* $\mathrm{mdc}(a, d) = 1$, *existem infinitos primos da forma* $a + dn$ *(com* n *natural).*

A demonstração usual deste teorema usa variáveis complexas. Muitos casos particulares admitem demonstrações elementares mais ou menos simples. O leitor não deve ter dificuldade em demonstrar, por exemplo, que existem infinitos primos da forma $4n + 3$ ou $6n + 5$.

Existem vários refinamentos conhecidos do teorema de Dirichlet. Definimos $\pi_{d,a}(x)$ como sendo o número de primos da forma $a + dn$ no intervalo $[2, x]$. De la Vallée Poussin provou que

$$\lim_{x\to+\infty} \frac{\pi_{d,a}(x)}{\pi(x)} = \frac{1}{\varphi(d)},$$

isto é, todas as possíveis classes módulo d têm aproximadamente a mesma proporção de primos.

Por outro lado, Tchebycheff observou que para valores pequenos de x $\pi_{3,2}(x) - \pi_{3,1}(x)$ e $\pi_{4,3}(x) - \pi_{4,1}(x)$ são positivos. Um teorema de Littlewood, entretanto, demonstra que estas funções mudam de sinal infinitas vezes. Em 1957, Leech demonstrou que o menor valor de x para o qual $\pi_{4,3}(x) - \pi_{4,1}(x) = -1$ é 26861 e em 1978 Bays e Hudson demonstraram que o menor valor de x para o qual $\pi_{3,2}(x) - \pi_{3,1}(x) = -1$ é 608981813029.

Seja $p(d, a)$ o menor primo da forma $a + dn$, n inteiro e

$$p(d) = \max\{p(d, a) \mid 0 < a < d, \mathrm{mdc}(a, d) = 1\}.$$

Linnik (1944) provou que existe $L > 1$ com $p(d) < d^L$ para todo d suficientemente grande. A melhor estimativa conhecida para L é $L \leq 5,5$, devida a Heath-Brown (1992), que também conjecturou que

$$p(d) \leq Cd(\log d)^2.$$

Por outro lado, não se sabe demonstrar que existam infinitos primos da forma $n^2 + 1$; aliás, não existe nenhum polinômio P em uma variável e de grau maior que 1 para o qual se saiba demonstrar que existem infinitos primos da forma $P(n)$, $n \in \mathbb{Z}$. Por outro lado, existem muitos polinômios em mais de uma variável que assumem infinitos valores primos: por exemplo, prova-se facilmente que todo primo da forma $4n + 1$ pode ser escrito também na forma $a^2 + b^2$, $a, b \in \mathbb{Z}$. Por outro lado, Friedlander e Iwaniec provaram recentemente um resultado muito mais difícil: que existem infinitos primos da forma $a^2 + b^4$.

Um dos problemas em aberto mais famosos da matemática é a conjectura de Goldbach: todo número par maior ou igual a 4 é a soma de dois primos. Chen demonstrou que todo número par suficientemente grande é a soma de um primo com um número com no máximo dois fatores primos. Vinogradov demonstrou que todo ímpar suficientemente grande (por exemplo, maior do que $3^{3^{15}}$) é uma soma de três primos.

Quando p e $p + 2$ são ambos primos, dizemos que eles são *primos gêmeos*. Conjectura-se, mas não se sabe demonstrar, que existem infinitos primos gêmeos. Brun, por outro lado, provou que primos gêmeos são escassos no seguinte sentido: se $\pi_2(x)$ é o número de pares de primos gêmeos até x então

$$\pi_2(x) < \frac{100x}{(\log x)^2}$$

para x sufientemente grande. Em particular,

$$\sum_{p \text{ primo gêmeo}} \frac{1}{p} < +\infty.$$

Acredita-se que $\pi_2(x)$ seja assintótico a $Cx/(\log x)^2$ para alguma constante positiva C. Deixamos como exercício provar a seguinte caracterização de primos gêmeos devida a Clement. Seja $n \geq 2$; os inteiros n e $n+2$ são ambos primos se e somente se

$$4((n-1)! + 1) + n \equiv 0 \pmod{n(n+2)}.$$

Seja p_n o n-ésimo número primo. O teorema dos números primos equivale a dizer que

$$\lim_{n\to\infty} \frac{p_n}{n \log n} = 1.$$

Por outro lado, sabe-se muito pouco sobre o comportamento da função $d_n = p_{n+1} - p_n$. Por exemplo, a conjectura de que existem infinitos primos gêmeos equivale a dizer que $\liminf d_n = 2$. Não se sabe provar nem que $\liminf d_n < \infty$. Seja

$$L = \liminf \frac{d_n}{\log p_n};$$

Erdös provou que $L < 1$ e Maier que $L \leq 0,248$. Apenas em 2005, D. A. Goldston, J. Pintz e C. Y. Yıldırım provaram que $L = 0$ (ver [GPY1]). De fato eles provaram bem mais (ver [GPY2]): por exemplo, temos

$$\liminf \frac{d_n}{\sqrt{\log p_n}(\log\log p_n)^2} < \infty.$$

Erdös também provou que o conjunto dos pontos de acumulação de $d_n/\log p_n$ tem medida positiva. Por outro lado, é um teorema clássico, conhecido como postulado de Bertrand, que sempre existe pelo menos um primo entre m e $2m$, ou seja, $d_n < p_n$. Em 1931, Westzynthius provou que

$$\limsup \frac{d_n}{\log p_n} = \infty,$$

e em 1963 Rankin, completando um trabalho de Erdös, mostrou que

$$\limsup \frac{d_n(\log\log\log p_n)^2}{\log p_n \log\log p_n \log\log\log\log p_n} \geq e^{\gamma} \approx 1,78107$$

onde γ é a constante de Euler-Mascheroni,

$$\gamma = \lim_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\log n\right) \approx 0,5772156649;$$

este resultado foi melhorado posteriormente por Pomerance e Pintz, que provou que o lado esquerdo é maior ou igual a $2e^{\gamma}$ ([**Pintz**]). Conjectura-se que

$$\limsup \frac{d_n}{(\log p_n)^2} = C$$

para alguma constante positiva C. Outra conjectura famosa é que sempre há pelo menos um primo entre n^2 e $(n+1)^2$. Observamos que a primeira vez que $d_n > 1000$ ocorre para $p_n = 1693182318746371$, quando $d_n = 1132$, o que foi descoberto recentemente por T. Nicely e D. Nyman.

Ben Green e Terence Tao provaram recentemente em [GT] que existem progressões aritméticas arbitrariamente grandes formadas exclusivamente por números primos (veja [AMM] para um texto expositório sobre este teorema e outros resultados relacionados). A maior progressão aritmética conhecida formada exclusivamente por números primos é $468395662504823+205619\cdot 23\#\cdot k = 468395662504823 + 45872132836530 \cdot k, 0 \leq k \leq 23$, que tem 24 termos e foi descoberta em 2007 por Jaroslav Wroblewski.

Sierpinski provou que existem infinitos números naturais ímpares k (os chamados *números de Sierpinski*) tais que $k\cdot 2^n+1$ é composto para todo inteiro positivo n e Riesel provou que existem infinitos números naturais ímpares k (os chamados *números de Riesel*) tais que $k\cdot 2^n - 1$ é composto para todo inteiro positivo n. Conjectura-se que os menores valores de k com as propriedades acima são respectivamente 78557 e 509203. Há um projeto cooperativo, que consiste em procurar primos grandes, para demonstrar estas conjecturas (veja `http://vamri.xray.ufl.edu/proths/`).

Também existem infinitos naturais ímpares k que são simultaneamente números de Sierpinski e de Riesel, os chamados *números de Brier*. O menor número de Brier conhecido é 878503122374924101526292469. Veja `http://www.research.att.com/~njas/sequences/A076335` e as páginas e referências lá mencionadas para mais informações.

O leitor interessado em aprender mais sobre problemas em aberto em teoria dos números pode consultar [**Guy**].

Nota: Durante a revisão para a terceira edição, em fevereiro de 2008, verificamos que a página `http://vamri.xray.ufl.edu/proths/` mencionada acima

parece inativa. Um sumário de vários projetos cooperativos para encontrar primos grandes pode ser encontrado em `http://www.prothsearch.net/`. Projetos ativos que pretendem provar que 78557 e 509203 são os menores números de Sierpinski e Riesel podem ser encontrados respectivamente em `http://www.seventeenorbust.com/` e `http://www.rieselsieve.com/`.

O projeto Seventeen or Bust tem obtido resultados particularmente bons nos últimos anos. O fato de que 78557 é um número de Sierpinski foi provado em 1962 por John Selfridge (veja o exercício abaixo). Quando o projeto começou, em 2002, havia 17 números menores que 78557 sobre os quais não se sabia se eram números de Sierpinski ou não: 4847, 5359, 10223, 19249, 21181, 22699, 24737, 27653, 28433, 33661, 44131, 46157, 54767, 55459, 65567, 67607 e 69109.

Desde então, os participantes do projeto encontraram os seguintes primos (informamos após cada primo o nome ou a equipe de seu descobridor): $46157 \cdot 2^{698207} + 1$ (S. Gibson), $65567 \cdot 2^{1013803} + 1$ (J. Burt), $44131 \cdot 2^{995972} + 1$ (equipe *deviced*), $69109 \cdot 2^{1157446} + 1$ (S. DiMichele) e $54767 \cdot 2^{1337287} + 1$ (P. Coels) em 2002, $5359 \cdot 2^{5054502} + 1$ (R. Sundquist) em 2003, $28433 \cdot 2^{7830457} + 1$ (equipe *TeamPrimeRib*), $27653 \cdot 2^{9167433} + 1$ (D. Gordon) e $4847 \cdot 2^{3321063} + 1$ (R. Hassler) em 2005, $19249 \cdot 2^{13018586} + 1$ (K. Agafonov) e $33661 \cdot 2^{7031232} + 1$ (S. Sunde) em 2007. Sobraram portanto os 6 números 10223, 21181, 22699, 24737, 55459 e 67607. Veja `http://www.seventeenorbust.com/` para mais informações (em particular sobre como participar do projeto).

Exercício: Prove que 78557 é um número de Sierpinski, e que existem infinitos números de Sierpinski a partir das congruências

$$78557 \cdot 2^0 + 1 \equiv 0 \pmod 3$$

$$78557 \cdot 2^1 + 1 \equiv 0 \pmod 5$$

$$78557 \cdot 2^7 + 1 \equiv 0 \pmod 7$$

$$78557 \cdot 2^{11} + 1 \equiv 0 \pmod{13}$$

$$78557 \cdot 2^3 + 1 \equiv 78557 \cdot 2^{39} + 1 \equiv 0 \pmod{73}$$

$$78557 \cdot 2^{15} + 1 \equiv 0 \pmod{19}$$

$$78557 \cdot 2^{27} + 1 \equiv 0 \pmod{37}.$$

Capítulo 2

Corpos finitos e reciprocidade quadrática

Veremos neste capítulo alguns resultados de álgebra e teoria dos números um pouco mais abstratos e avançados do que no capítulo 1. O leitor que conhecer um pouco de álgebra terá mais facilidade em acompanhar mas tentamos ser auto-contidos, pelo menos para o que é necessário para acompanhar o resto do livro.

2.1 Corpos e polinômios

Um *grupo* é um conjunto G munido de uma operação $* : G \times G \to G$ e um elemento $e \in G$ com as seguintes propriedades:

- para quaisquer $a, b, c \in G$, $a * (b * c) = (a * b) * c$.
- para qualquer $a \in G$, $a * e = e * a = a$,
- para qualquer $a \in G$ existe $b \in G$ com $a * b = b * a = e$.

Se além disso tivermos $a * b = b * a$ para quaisquer $a, b \in G$ dizemos que o grupo é *comutativo* ou *abeliano*. Quando a operação $*$ se chama $+$ dizemos que G é um grupo aditivo e chamamos o elemento neutro e de 0. Se a operação se

chama $\cdot$ chamamos G de grupo multiplicativo e denotamos o elemento neutro e por 1. Assim, $\mathbb{Z}/(n)$ é um grupo abeliano aditivo e $(\mathbb{Z}/(n))^*$ é um grupo abeliano multiplicativo.

Um *anel comutativo com unidade* é um grupo abeliano aditivo A munido de uma segunda operação $\cdot : A \times A \to A$ satisfazendo $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$, $a \cdot b = b \cdot a$ para quaisquer $a, b, c \in A$ e um elemento $1 \in A$ com $1 \cdot a = a$ para todo $a \in A$. Assim, $\mathbb{Z}/(n)$ é um anel comutativo com unidade.

Um *corpo* é um anel comutativo com unidade onde para todo $a \in K$ com $a \neq 0$ existe $b \in K$ com $a \cdot b = 1$. Repetindo então, K é munido de duas operações $+ : K \times K \to K$ e $\cdot : K \times K \to K$, de uma função $- : K \to K$ e dois elementos especiais distintos chamados 0 e 1 satisfazendo as seguintes propriedades:

$$\begin{aligned} a + (b + c) &= (a + b) + c \\ a + 0 &= a \\ a + (-a) &= 0 \\ a + b &= b + a \\ a(b + c) &= ab + ac \\ a(bc) &= (ab)c \\ a1 &= a \\ ab &= ba \end{aligned}$$

e onde para todo $a \in K$, $a \neq 0$ existe $b \in K$ com

$$ab = 1.$$

Os exemplos mais conhecidos de corpos são $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$. Vimos no capítulo anterior que $\mathbb{Z}/(p)$ também é um corpo se p é primo; veremos a seguir outros exemplos de corpos finitos.

Dado um corpo K, definimos o anel comutativo com unidade $K[x]$ como sendo o conjunto das expressões da forma $P = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, chamados de *polinômios* com coeficientes em K. Observe que x é um símbolo formal e não um elemento de K; apesar disso, cada polinômio define uma *função polinomial*

$$\begin{aligned} P : K &\to K \\ c &\mapsto P(c) = a_0 + a_1 c + a_2 c^2 + \cdots + a_n c^n \end{aligned}$$

também chamada de P. A distinção entre um polinômio e uma função polinomial é bem ilustrada pelo polinômio $P = x^p - x \in (\mathbb{Z}/(p))[x]$: este polinômio é não nulo pois seus coeficientes são não nulos mas para todo $x \in \mathbb{Z}/(p)$ temos $P(x) = 0$ pelo pequeno teorema de Fermat.

Se $P = \sum a_i x^i$ e $Q = \sum b_i x^i$ são polinômios definimos $P + Q = \sum (a_i + b_i)x^i$ e $PQ = \sum c_i x^i$ onde $c_k = \sum_{i+j=k} a_i b_j$. Definimos o *grau* $\deg P$ de um polinômio $P = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ como sendo n se $a_n \neq 0$ mas $a_m = 0$ para $m > n$; definimos ainda o grau do polinômio 0 como sendo $-\infty$.

Lema 2.1: *Para quaisquer polinômios* P *e* Q *temos* $\deg(PQ) = \deg(P) + \deg(Q)$ *e* $\deg(P + Q) \leq \max\{\deg(P), \deg(Q)\}$.

Dem: Fácil. ■

Observe que definimos $-\infty < n$ e $(-\infty) + (-\infty) = -\infty + n = -\infty$ para todo n. Temos uma forma de divisão com resto em $K[x]$.

Teorema 2.2: *Sejam* $A, B \in K[x]$, $B \neq 0$. *Então existem únicos polinômios* $Q, R \in K[x]$ *com* $A = QB + R$ *e* $\deg R < \deg B$.

Dem: A demonstração é feita por indução no grau de A. Se $\deg(A) < \deg(B)$, tomamos $Q = 0$, $R = A$. Caso contrário, sejam n e m os graus de A e B e sejam a e b os coeficientes de mais alto grau destes polinômios. Podemos escrever $A = (a/b)x^{n-m}B + A_1$, com $\deg(A_1) < \deg(A)$. Pela hipótese de indução, temos $A_1 = Q_1 B + R$, com $\deg(R) < \deg(B)$. Fazendo $Q = (a/b) + x^{n-m} + Q_1$ temos $A = QB + R$. A unicidade segue facilmente do lema anterior. ■

A demonstração acima nada mais é do que o algoritmo usual de divisão usual. Um polinômio P tem *raiz* a (i.e., $P(a) = 0$) se e somente se $(x - a)|P$. Mais geralmente, $P(a)$ é o resto da divisão de P por $x - a$.

Proposição 2.3: *Um polinômio* P *não nulo de grau* n *tem no máximo* n *raízes.*

Dem: A demonstração é feita por indução em $n = \deg(P)$; os casos $n = 0$ e $n = 1$ são triviais. Se P tivesse $n + 1$ raízes distintas $a_1, \ldots, a_{n+1}$ então P seria múltiplo de $(x - a_{n+1})$; $P/(x - a_{n+1})$ teria grau $n - 1$ e raízes $a_1, \ldots, a_n$, contradizendo a hipótese de indução. ■

A partir da divisão com resto podemos repetir muitas das construções feitas para $\mathbb{Z}$ no capítulo anterior; dizemos que $K[x]$ (assim como $\mathbb{Z}$) é um *domínio euclidiano*. Daremos um esboço desta teoria; estes resultados não serão necessários para acompanhar o resto do livro.

Definimos $A|B$ se existe C com $AC = B$ e dizemos que um polinômio P de grau maior que $n > 0$ é *irredutível* se seus divisores todos têm grau 0 ou n (assim generalizando o conceito de número primo). O conceito de mdc também se generaliza, como indicado na proposição abaixo.

Proposição 2.4: *Dados polinômios não nulos $A, B \in K[x]$ existe um único $D \in K[x]$ (a menos de multiplicação por constante) tal que $D|A$, $D|B$ e, para todo $C \in K[x]$, se $C|A$ e $C|B$ então $C|D$. Além disso existem $E, F \in \mathbb{Z}$ com $D = AE + BF$.*

Dem: Definimos $I(A, B) = \{AE + BF; E, F \in K[x]\}$ e tomamos D de grau mínimo dentre os elementos não nulos de $I(A, B)$; o resto da demonstração é análoga à da proposição 1.1. ■

Polinômios irredutíveis são como números primos: um produto de polinômios só é múltiplo de um polinômio irredutível se um dos fatores o for.

Proposição 2.5: *Sejam P um polinômio irredutível e sejam $A_1, \ldots A_m \in K[x]$. Se $P|(A_1 \cdots A_m)$ então $P|A_i$ para algum i, $1 \leq i \leq n$.*

Dem: Análoga à do corolário 1.3. ■

Temos também um teorema de fatoração única.

Teorema 2.6: *Todo polinômio pode ser fatorado como um produto de polinômios irredutíveis; esta fatoração é única a menos da ordem dos fatores.*

Dem: Análoga à do teorema fundamental da aritmética, usando a proposição acima e fazendo indução no grau do polinômio. ■

Os exemplos mais evidentes de polinômios irredutíveis são os da forma $x-a$, $a \in K$. Quando estes são os *únicos* polinômios irredutíveis dizemos que o corpo é *algebricamente fechado*. Polinômios de grau 2 e 3 são irredutíveis se e somente se não têm raízes.

O pequeno teorema de Fermat também admite uma formulação em termos de polinômios.

Teorema 2.7: *Seja p primo; em $(\mathbb{Z}/(p))[x]$ temos*

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1)).$$

Dem: Os dois polinômios dos dois lados da equação têm grau p e o coeficiente de x^p é 1 nos dois casos. Assim, a diferença tem grau menor do que p mas se anula em p pontos: $0, 1, \ldots p-1$. Pelo corolário anterior, esta diferença deve ser o polinômio zero. ■

A partir do teorema acima temos uma nova prova do teorema de Wilson: $x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1))$ em $(\mathbb{Z}/(p))[x]$, mas o coeficiente independente é -1 do lado esquerdo e $(p-1)!$ do lado direito.

Podemos definir congruências em $K[x]$:

$$A \equiv B \pmod{P} \iff P|(B-A).$$

As propriedades básicas de congruências podem ser traduzidas para este novo contexto e podemos definir um quociente $K[x]/(P)$ da mesma forma como definimos $\mathbb{Z}/(n)$; demonstra-se que $K[x]/(P)$ é um corpo exatamente quando P é irredutível.

Prometemos que veríamos outros exemplos de corpos finitos além de $\mathbb{Z}/(p)$: o parágrafo acima ensina que podemos construir tais corpos como $(\mathbb{Z}/(p))[x]/(P)$ onde $P \in (\mathbb{Z}/(p))[x]$ é irredutível. Por exemplo, o polinômio $x^2 + x + 1$ é irredutível em $(\mathbb{Z}/(2))[x]$ o que nos permite construir um corpo de 4 elementos: 0, 1, x e $x+1$. As operações em $\mathbb{Z}/(2)$ e a relação $x^2 = x+1$ definem as operações neste corpo (denotamos $x+1$ por x'):

+	0	1	X	X'
0	0	1	X	X'
1	1	0	X'	X
X	X	X'	0	1
X'	X'	X	1	0

*	0	1	X	X'
0	0	0	0	0
1	0	1	X	X'
X	0	X	X'	1
X'	0	X'	1	X

De fato existem em $(\mathbb{Z}/(p))[x]$ polinômios irredutíveis de qualquer grau e todo corpo finito pode ser construido desta forma. Enunciaremos sem demonstração um teorema que classifica os corpos finitos.

Teorema 2.8: *Existe um corpo finito com q elementos se e somente se q é da forma p^n para algum primo p e algum inteiro positivo n. Além disso, dados dois corpos finitos K_1 e K_2 com o mesmo número de elementos existe*

uma única bijeção $f : K_1 \to K_2$ *com* $f(a+b) = f(a) + f(b)$ *e* $f(ab) = f(a)f(b)$ *para quaisquer* $a, b \in K_1$.

Uma bijeção como a descrita acima é chamada de *isomorfismo* e dois corpos são ditos *isomorfos* se existe entre eles um isomorfismo; a idéia é que corpos isomorfos são iguais a menos dos nomes dos elementos. Veremos mais tarde outras formas mais concretas de construir corpos finitos.

2.2 Ordens e raízes primitivas

Dados $n, a \in \mathbb{Z}$ com $n > 0$ e $(a, n) = 1$, definimos a *ordem de* a *módulo* n, denotada por $\mathrm{ord}_n a$, como sendo o menor inteiro positivo t com $a^t \equiv 1 \pmod{n}$. Analogamente, se K for um corpo finito e $a \in K$, $a \neq 0$, definimos a *ordem de* a *em* K, denotada por $\mathrm{ord}_K a$, como sendo o menor inteiro positivo t com $a^t = 1 \in K$; temos $\mathrm{ord}_p a = \mathrm{ord}_{\mathbb{Z}/(p)} a$.

Claramente $a^e \equiv a^{e'} \pmod{n}$ se e somente se $e \equiv e' \pmod{\mathrm{ord}_n a}$; pelo teorema de Euler, $\mathrm{ord}_n a | \varphi(n)$.

Dizemos que a é uma *raiz primitiva módulo* n se $\mathrm{ord}_n a = \varphi(n)$. Analogamente, dizemos que a é uma *raiz primitiva em* K se $\mathrm{ord}_K a = q-1$, onde $q = |K|$ é o número de elementos de K. Por exemplo, 2 é raiz primitiva módulo 5 mas 2 não é raiz primitiva módulo 7 ($2^3 \equiv 1 \pmod{7}$). Também é fácil verificar que não existe raiz primitiva módulo 8 pois se x é ímpar então $x^2 \equiv 1 \pmod{8}$. Podemos também dizer que a é raiz primitiva se a função

$$\begin{aligned} \mathbb{Z}/(\varphi(n)) &\to (\mathbb{Z}/(n))^* \\ r &\mapsto a^r \end{aligned}$$

ou

$$\begin{aligned} \mathbb{Z}/(q-1) &\to K^* \\ r &\mapsto a^r \end{aligned}$$

é injetora. Como o domínio e contradomínio são conjuntos finitos com o mesmo número de elementos, a função é injetora se e somente se ela é sobrejetora. Podemos assim dizer que a é uma raiz primitiva módulo n se e somente se para todo $b \in (\mathbb{Z}/(n))^*$ (ou para todo $b \in K^*$) existe r com $a^r = b$.

Um corolário desta caracterização de raízes primitivas é que se a é raiz primitiva módulo n e $m|n$ então a é raiz primitiva módulo m. O objetivo

da próxima seção é caracterizar os valores de n para os quais existe uma raiz primitiva módulo n. Nesta seção mostraremos que todo corpo finito admite raiz primitiva; em particular existe raiz primitiva módulo p para qualquer primo p.

Precisamos primeiro de uma versão do pequeno teorema de Fermat para corpos finitos:

Teorema 2.9: *Se K é um corpo finito e $q = |K|$ então $a^q - a = 0$ para todo $a \in K$.*

Dem: Se $a = 0$ o teorema vale; vamos supor a partir de agora $a \neq 0$. Sejam $b_1, \ldots b_{q-1}$ os elementos não nulos de K. Os elementos $ab_1, \ldots ab_{q-1}$ são todos não nulos e distintos, logo são os *próprios* $b_1, \ldots b_{q-1}$, apenas permutados. Assim

$$\begin{aligned} b_1 \cdot b_2 \cdots b_{q-1} &= (ab_1)(ab_2)\cdots(ab_{q-1}) \\ &= a^{q-1}(b_1 \cdot b_2 \cdots b_{q-1}) \end{aligned}$$

e $a^{q-1} = 1$. ■

Segue deste teorema que $\mathrm{ord}_K\, a | q-1$, analogamente ao que já sabiamos para $\mathbb{Z}/(n)$. A partir do que vimos sobre polinômios temos também que

$$x^q - x = x(x - b_1)\cdots(x - b_{q-1})$$

em $K[x]$.

Teorema 2.10: *Se K é um corpo finito então existe raiz primitiva em K.*

Dem: Seja d um divisor de $q-1$: definimos $N(d)$ como o número de elementos de K^* de ordem d. Claramente $\sum_{d|q-1} N(d) = q - 1$.

Se $N(d) > 0$, seja a_d um elemento de K com $\mathrm{ord}_K\, a_d = d$: os elementos $1, a_d, a_d^2, \ldots a_d^{d-1}$ são raízes do polinômio $x^d - 1 = 0$. Como este polinômio tem no máximo d raízes, estas são todas as raízes. Assim, os elementos de K de ordem d são precisamente a_d^r, $r \in (\mathbb{Z}/(d))^*$. Assim os únicos valores possíveis para $N(d)$ são 0 e $\varphi(d)$. Mas como $\sum_{d|q-1} N(d) = \sum_{d|q-1} \varphi(d) = q - 1$, temos $N(d) = \varphi(d)$ para todo $d|q-1$. Em particular $N(q-1) > 0$ e existem raízes primitivas. ■

Apesar de existirem raízes primitivas módulo p para todo primo p não existe uma fórmula simples para obter uma raiz primitiva. Por outro lado, conjectura-se que todo inteiro que não é um quadrado é raiz primitiva para infinitos valores de p (conjectura de Artin).

Corolário 2.11: *Dados $x \in K^*$ e um inteiro positivo k existe $y \in K^*$ com $y^k = x$ se e somente se $x^{(q-1)/\mathrm{mdc}(k,q-1)} = 1$, onde $q = |K|$.*

Dem: Se $x = y^k$ então $x^{(q-1)/\mathrm{mdc}(k,q-1)} = (y^{q-1})^{k/\mathrm{mdc}(k,q-1)} = 1$ pois $y^{q-1} = 1$. Suponha agora que $x^{(q-1)/\mathrm{mdc}(k,q-1)} = 1$. Sejam a uma raiz primitiva de K e $r \in \mathbb{Z}$ com $x = a^r$. Temos $(a^r)^{(q-1)/\mathrm{mdc}(k,q-1)} = 1$ donde $\mathrm{mdc}(k, q-1) \mid r$ e portanto existem inteiros u, v com $ku + (q-1)v = r$. Assim $x = a^r = a^{ku+(q-1)v} = (a^u)^k \cdot (a^{q-1})^v = y^k$ onde $y = a^u$. ■

2.3 Raízes primitivas em $\mathbb{Z}/(n)$

Nesta seção caracterizaremos os inteiros n para os quais existe raiz primitiva módulo n.

Lema 2.12: *Sejam p um número primo e $a \in \mathbb{Z}$ uma raiz primitiva módulo p. Então a ou $a' = a + p$ é raiz primitiva módulo p^2.*

Dem: Pelo binômio de Newton, $a'^p = (a+p)^p \equiv a^p \pmod{p^2}$. Sem perda de generalidade, podemos supor $a^p \not\equiv a \pmod{p^2}$ ou $a^{p-1} \not\equiv 1 \pmod{p^2}$, donde $\mathrm{ord}_{p^2} a \neq p-1$. Como $p-1 = \mathrm{ord}_p a \mid \mathrm{ord}_{p^2} a \mid \varphi(p^2) = p(p-1)$ isto implica em $\mathrm{ord}_{p^2} a = p(p-1)$. ■

Lema 2.13: *Se p é um número primo ímpar e a é raiz primitiva módulo p^2 então a é raiz primitiva módulo p^k para todo $k > 2$, $k \in \mathbb{Z}$.*

Dem: Temos $a^{p-1} \equiv 1 \pmod{p}$, mas $a^{p-1} \not\equiv 1 \pmod{p^2}$, donde $a^{p-1} = 1 + b_0 p$ com $b_0 \not\equiv 0 \pmod{p}$. Vamos mostrar por indução que $a^{p^j(p-1)} =$

$1 + b_j p^{j+1}$ com $b_j \equiv b_0 \pmod{p}$. Podemos escrever

$$\begin{aligned} a^{p^{j+1}(p-1)} &= (a^{p^j(p-1)})^p \\ &= (1 + b_j p^{j+1})^p \\ &= 1 + p b_j p^{j+1} + \binom{p}{2} b_j^2 p^{2j+2} + \cdots + b_j^p p^{pj+p} \\ &= 1 + b_j (1 + \binom{p}{2} b_j p^j + \cdots b_j^{p-1} p^{(p-1)j+p-2}) p^{j+2} \\ &= 1 + b_{j+1} p^{j+2} \end{aligned}$$

com $b_{j+1} \equiv b_j \pmod{p}$ pois o parêntesis na penúltima linha é da forma $1+$ um múltiplo de p. Esta última afirmação segue da positividade dos expoentes de p *exceto* no caso $j = 0$; neste caso o expoente do primeiro termo não trivial é zero mas temos $\binom{p}{2} \equiv 0 \pmod{p}$ pois $p > 2$ (é neste ponto que precisamos da hipótese de p ser ímpar). O lema segue de $a^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k}$ por indução, pois teremos $(p-1)p^{k-2} = \mathrm{ord}_{p^{k-1}} a \mid \mathrm{ord}_{p^k} a \mid \varphi(p^k) = (p-1)p^{k-1}$, donde $\mathrm{ord}_{p^k} a = (p-1)p^{k-1}$. ■

Lema 2.14: *Seja $n > 1$. O número de soluções para a congruência $x^2 \equiv 1 \pmod{n}$ é:*

(a) *1 se $n = 2$,*

(b) *2 se $n = 4$,*

(c) *4 se $n = 2^k$, $k > 2$,*

(d) *2 se $n = p^k$, p um primo ímpar,*

(e) *2^{m+i} se $n = 2^k p_1^{e_1} \cdots p_m^{e_m}$, onde $i = 0$ se $k \leq 1$, $i = 1$ se $k = 2$ e $i = 2$ se $k > 2$.*

Dem: Os itens (a) e (b) são verificáveis diretamente. As quatro soluções no item (c) são 1, $2^{k-1} - 1$, $2^{k-1} + 1$ e $2^k - 1$. De fato, é fácil verificar que estes quatro valores são soluções da congruência. Por outro lado, para que a seja solução da congruência devemos ter $2^k | (a+1)(a-1) = a^2 - 1$; portanto a deve ser ímpar. Um dentre $a - 1$ e $a + 1$ deve ser da forma $2b$, b ímpar. Assim o outro deve ser múltiplo de 2^{k-1}, o que diz que a deve ter um dos quatro valores acima. Analogamente para o item (d), apenas um dentre $a - 1$ e $a + 1$ é múltiplo de p, o que só permite as soluções 1 e $n - 1$.

Para o item (e) usamos os itens anteriores e o teorema chinês dos restos: a é solução da congruência acima se e somente se a satisfaz $a^2 \equiv 1 \pmod{2^k}$ e $a^2 \equiv 1 \pmod{p_i^{e_i}}$ para cada i. Assim, o número de soluções módulo n é o produto do número de soluções módulo 2^k, $p_1^{e_1}$, ..., $p_m^{e_m}$, o que nos dá a fórmula do item (e). ■

Teorema 2.15: *Um inteiro $n > 1$ admite raiz primitiva se e somente se $n = 2$, $n = 4$ ou n é da forma p^k ou $2p^k$, onde p é um primo ímpar, admite raiz primitiva.*

Dem: Os casos $n = 2$ e $n = 4$ podem ser verificados diretamente. A existência de uma raiz primitiva módulo p^k (p um primo ímpar) segue dos dois primeiros lemas desta seção. Para o caso $2p^k$, seja a uma raiz primitiva módulo p^k: a ou $a + p^k$, aquele que for ímpar, será uma raiz primitiva módulo $2p^k$ pois $\varphi(2p^k) = \varphi(p^k)$.

Se n não for de uma destas formas, o lema anterior garante que a congruência $x^2 \equiv 1 \pmod{n}$ admite mais de duas soluções. Por outro lado, a existência de uma raiz primitiva a módulo n garante que a congruência $x^2 \equiv 1 \pmod{n}$ só tem as soluções 1 e $n-1$. De fato, qualquer solução pode ser escrita da forma a^k para algum k e nossa congruência torna-se $a^{2k} \equiv 1 \pmod{n}$ ou $2k \equiv 0 \pmod{\varphi(n)}$, que só tem as soluções $k = 0$ ($a^k = 1$) e $k = (\varphi(n))/2$ ($a^k \equiv n - 1 \pmod{n}$).

Outra demonstração, sem usar o lema anterior, consiste em observar que se n não for de uma destas duas formas então $n = n_1 n_2$, com $n_1, n_2 \geq 3$ e $\mathrm{mdc}(n_1, n_2) = 1$. Temos então $a^{\varphi(n)/2} \equiv 1 \pmod{n}$ para todo a inteiro com $\mathrm{mdc}(a, n) = 1$, pois $\varphi(n_1) \mid \varphi(n)/2$ e $\varphi(n_2) \mid \varphi(n)/2$. ■

2.4 A lei da reciprocidade quadrática

A lei de Gauss de reciprocidade quadrática afirma que se p e q são primos há uma relação direta entre p ser quadrado módulo q e q ser quadrado módulo p. Este teorema fornece um rápido algoritmo para determinar se a é quadrado módulo p onde a é um inteiro e p um número primo.

Definição 2.16: *Seja* p *um primo e* a *um inteiro. Definimos o símbolo de Lagrange* $(\frac{a}{p})$ *por*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } p \text{ divide } a \\ -1 & \text{se } a \text{ não é quadrado módulo } p \\ 1 & \text{se } p \nmid a \text{ e } a \text{ é quadrado módulo } p. \end{cases}$$

Proposição 2.17: *Seja* p *um primo ímpar e* $a \in \mathbb{Z}$ *tal que* $p \nmid a$. *Então* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Dem: Sabemos que se $p \nmid a$ então $a^{p-1} \equiv 1 \pmod{p}$, ou seja, $X^{p-1} - 1$ tem como raízes $1, 2, \ldots, p-1$ em $\mathbb{Z}/(p)$. Por outro lado, $X^{p-1} - 1 = (X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1)$. Se existe $b \in \mathbb{Z}$ tal que $a \equiv b^2 \pmod{p}$ então $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$; ou seja, $\left(\frac{a}{p}\right) = 1 \equiv a^{\frac{p-1}{2}} \pmod{p}$. Como $X^2 \equiv Y^2 \pmod{p} \Leftrightarrow X \equiv \pm Y \pmod{p}$, há pelo menos $\frac{p-1}{2}$ quadrados em $(\mathbb{Z}/(p))^*$, logo os quadrados são exatamente as raízes de $X^{\frac{p-1}{2}} - 1$ em $\mathbb{Z}/(p)$, donde os não quadrados são exatamente as raízes de $X^{\frac{p-1}{2}} + 1$, ou seja, se $(\frac{b}{p}) = -1$ então $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. ■

Corolário 2.18: *Se* p *é primo ímpar então* $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.

Vamos agora reinterpretar a Proposição 1. Seja $a \in (\mathbb{Z}/(p))^*$. Para cada $j = 1, 2, \ldots, \frac{p-1}{2}$ escrevemos $a \cdot j$ como $\varepsilon_j m_j$ com $\varepsilon_j \in \{-1, 1\}$ e $m_j \in \{1, 2, \ldots, \frac{p-1}{2}\}$. Se $m_i \neq m_j$ temos $a \cdot i = a \cdot j$ ou $a \cdot i = -a \cdot j$; a primeira possibilidade implica $i = j$ e a segunda é impossível. Assim, se $i \neq j$ temos $m_i \neq m_j$ donde $\{m_1, m_2, \ldots, m_{\frac{p-1}{2}}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$. Assim

$$\begin{aligned} \left(\frac{a}{p}\right) &\equiv a^{\frac{p-1}{2}} \\ &= \frac{(a \cdot 1)(a \cdot 2) \cdots (a \cdot \frac{p-1}{2})}{1 \cdot 2 \cdots \frac{p-1}{2}} \\ &\equiv \frac{\varepsilon_1 \varepsilon_2 \cdots \varepsilon_{\frac{p-1}{2}}\, m_1, m_2, \ldots, m_{\frac{p-1}{2}}}{1 \cdot 2 \cdots \frac{p-1}{2}} \\ &= \varepsilon_1 \varepsilon_2 \cdots \varepsilon_{\frac{p-1}{2}} \pmod{p} \end{aligned} \tag{2.1}$$

donde $(\frac{a}{p}) = \varepsilon_1\varepsilon_2\ldots\varepsilon_{\frac{p-1}{2}}$, pois ambos pertencem a $\{-1,1\}$. Assim, $(\frac{a}{p}) = (-1)^m$ onde m é o número de elementos j de $\{1,2,\ldots,\frac{p-1}{2}\}$ tais que $\varepsilon_j = -1$. Como primeira conseqüência deste fato temos o seguinte resultado.

Proposição 2.19: *Se p é um primo ímpar então*

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{se } p \equiv \pm 1 \pmod 8, \\ -1, & \text{se } p \equiv \pm 3 \pmod 8. \end{cases}$$

Dem: Se $p \equiv 1 \pmod 4$, digamos $p = 4k+1$, temos $\frac{p-1}{2} = 2k$. Como $1 \le 2j \le \frac{p-1}{2}$ para $j \le k$ e $\frac{p-1}{2} < 2j \le p-1$ para $k+1 \le j \le 2k$, temos

$$(\frac{a}{p}) = (-1)^k = \begin{cases} 1, & \text{se } p \equiv 1 \pmod 8, \\ -1, & \text{se } p \equiv 5 \pmod 8. \end{cases}$$

Se $p \equiv 3 \pmod 4$, digamos $p = 4k+3$, temos $\frac{p-1}{2} = 2k+1$. Para $1 \le j \le k$ temos $1 \le 2j \le \frac{p-1}{2}$ e para $k+1 \le j \le 2k+1$ temos $\frac{p-1}{2} < 2j \le p-1$, donde

$$(\frac{a}{p}) = (-1)^{k+1} = \begin{cases} -1, & \text{se } p \equiv 3 \pmod 8, \\ 1, & \text{se } p \equiv 7 \pmod 8. \end{cases}$$

■

Teorema 2.20: (Lei de reciprocidade quadrática) *Sejam p e q primos ímpares. Então $(\frac{p}{q}) = (-1)^{(p-1)(q-1)/4}(\frac{q}{p})$.*

Dem: Na notação acima, com $a = q$, para cada $j \in P$, onde

$$P = \{1,2,\ldots,(p-1)/2\},$$

temos que $\varepsilon_j = -1$ se e só se existe $y \in \mathbb{Z}$ tal que $-(p-1)/2 \le qj - py < 0$. Tal y deve pertencer a Q, onde

$$Q = \{1,2,\ldots,(q-1)/2\}.$$

Assim, temos que $(\frac{q}{p}) = (-1)^m$ onde $m = |X|$ e

$$X = \{(x,y) \in P \times Q \mid -(p-1)/2 \le qx - py < 0\};$$

note que $qx - py$ nunca assume o valor 0. Analogamente, $(\frac{p}{q}) = (-1)^n$, onde $n = |Y|$ e

$$Y = \{(x, y) \in P \times Q \mid 0 < qx - py \leq (q-1)/2\}.$$

Daí segue que $(\frac{p}{q})(\frac{q}{p}) = (-1)^k$ onde $k = m + n = |Z|$ onde

$$Z = \{(x, y) \in P \times Q \mid -(p-1)/2 \leq qx - py \leq (q-1)/2\}$$

pois $qx - py$ nunca assume o valor 0. Temos $k = |C| - |A| - |B|$ onde $C = P \times Q$,

$$A = \{(x, y) \in C \mid qx - py < -(p-1)/2\},$$
$$B = \{(x, y) \in C \mid qx - py > (q-1)/2\}.$$

Como $|C| = (p-1)(q-1)/4$, basta mostrar que $|A| = |B|$. Mas $f : C \to C$ definida por $f(x, y) = (((p+1)/2) - x, ((q+1)/2) - y)$ define uma bijeção entre A e B. ■

2.5 Extensões quadráticas de corpos finitos

Sejam p primo e d um inteiro que não seja quadrado perfeito. O anel $(\mathbb{Z}/(p))[\sqrt{d}]$ é o conjunto

$$\{a + b\sqrt{d},\ a, b \in \mathbb{Z}/(p)\}$$

onde

$$(a + b\sqrt{d}) + (\tilde{a} + \tilde{b}\sqrt{d}) = (a + \tilde{a}) + (b + \tilde{b})\sqrt{d}$$
$$(a + b\sqrt{d})(\tilde{a} + \tilde{b}\sqrt{d}) = (a\tilde{a} + db\tilde{b}) + (a\tilde{b} + \tilde{a}b)\sqrt{d}.$$

Por definição,

$$a + b\sqrt{d} = \tilde{a} + \tilde{b}\sqrt{d} \Leftrightarrow a = \tilde{a}, b = \tilde{b}.$$

Como grupo aditivo, $(\mathbb{Z}/(p))[\sqrt{d}] = \mathbb{Z}/(p) \times \mathbb{Z}/(p)$. Vamos investigar a estrutura multiplicativa de $(\mathbb{Z}/(p))[\sqrt{d}]$. Observemos inicialmente que, se d é um quadrado módulo p então $(\mathbb{Z}/(p))[\sqrt{d}]$ não pode ser um corpo, pois se $a^2 = d$ em $\mathbb{Z}/(p)$ então $(a + \sqrt{d})(a - \sqrt{d}) = 0$ em $(\mathbb{Z}/(p))[\sqrt{d}]$. A próxima proposição é uma recíproca deste fato:

Proposição 2.21: *Se $(\frac{d}{p}) = -1$ então $(\mathbb{Z}/(p))[\sqrt{d}]$ é um corpo.*

Dem: De fato, se $(a, b) \neq (0, 0)$, $(a + b\sqrt{d})^{-1} = (a - b\sqrt{d})/(a^2 - db^2)$. Temos que $a^2 - db^2 \in (\mathbb{Z}/(p))^*$, pois d não é quadrado mod p, logo, se $b \neq 0$, $a^2 - db^2 = 0$, que equivale a $d = (a/b)^2$ seria uma contradição e, se $b = 0$, $a^2 - db^2 = a^2 \neq 0$ pois $(a, b) \neq (0, 0) \Rightarrow a \neq 0 \Rightarrow a^2 \neq 0$. ■

Capítulo 3

Primos de Mersenne e testes de primalidade

Várias fórmulas já foram propostas para gerar números primos arbitrariamente grandes: Fermat, por exemplo, conjecturou que todo número da forma $2^{2^n}+1$ fosse primo, o que foi desmentido por Euler ($2^{2^5}+1$ é composto). Apesar dos esforços, não se conhece nenhuma fórmula simples para gerar primos arbitrariamente grandes, e a maioria dos matemáticos acredita que não existe uma fórmula deste tipo.

Existem entretanto algumas fórmulas que geram *famílias* interessantes de primos. A fórmula deste tipo que mais nos interessa é $M_p = 2^p - 1$, os chamados *números de Mersenne*. Quando M_p é primo, dizemos que M_p é um *primo de Mersenne*. Parte da razão pela qual números desta forma são interessantes é que apesar de M_p nem sempre ser primo é relativamente fácil *testar* para um dado expoente p, mesmo bastante grande, se M_p é primo ou composto. Em grande parte por este motivo os seis maiores primos conhecidos hoje são primos de Mersenne e ao longo da história o maior primo conhecido quase sempre foi um primo de Mersenne(ver tabelas).

A Seção 3.1 é profundamente afetada pela descoberta do algoritmo de Agrawal-Kayal-Saxena. Optamos por manter a forma original da seção (inclusive com algumas frases que se tornaram obsoletas) e acrescentamos a ela um breve apêndice tratando destes resultados recentes.

3.1 Fórmulas para primos e testes de primalidade

Mencionamos na introdução deste capítulo que não se conhece nenhuma fórmula simples para gerar primos arbitrariamente grandes. Uma palavra imprecisa mas importante nesta frase é "simples". Existem fórmulas que geram números primos, mas que são tão complicadas que não ajudam muito nem a gerar números primos explicitamente nem a responder perguntas teóricas sobre a distribuição dos primos. Um exemplo de fórmula para p_n, o n-ésimo primo, é

$$p_n = \left\lfloor 1 - \frac{1}{\log 2} \log \left(-\frac{1}{2} + \sum_{d | P_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right\rfloor,$$

onde $P_{n-1} = p_1 p_2 \cdots p_{n-1}$; deixamos a demonstração a cargo do leitor. Outra fórmula é

$$p_n = \lfloor 10^{2^n} c \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} c \rfloor,$$

onde

$$c = \sum_{n=1}^{\infty} \frac{p_n}{10^{2^n}} = 0.0203000500000007\ldots.$$

A inutilidade desta última fórmula vem do fato que para calcular c devemos encontrar todos os primos; a fórmula se tornaria mais interessante se existisse outra interpretação para o número real c, o que parece muito improvável. Por outro lado, exite um número real $a > 1$ tal que $\lfloor a^{3^n} \rfloor$ é sempre primo.

Um tipo de fórmula para primos, de certa forma mais intrigante, são polinômios de coeficientes inteiros em S variáveis com a seguinte propriedade quase mágica: a interseção da imagem de $\mathbb{N}^S$ com $\mathbb{N}$ é exatamente o conjunto dos números primos. Note que se tomarmos um ponto de $\mathbb{N}^S$ "ao acaso", o valor do polinômio neste ponto quase certamente será negativo; assim, é difícil usar o polinômio para gerar primos. A título de curiosidade, vejamos um exemplo de polinômio com estas propriedades; aqui $N = 26$, o valor do polinômio é P,

as variáveis chamam-se $a, b, \ldots, z$ e $A, B, \ldots, N$ são expressões auxiliares:

$$
\begin{aligned}
P &= (k+2)(1 - A^2 - B^2 - C^2 - \cdots - N^2),\\
A &= wz + h + j - q,\\
B &= (gk + 2g + k + 1)(h + j) + h - z,\\
C &= 16(k+1)^3(k+2)(n+1)^2 + 1 - f^2,\\
D &= 2n + p + q + z - e,\\
E &= e^3(e+2)(a+1)^2 + 1 - o^2,\\
F &= (a^2 - 1)y^2 + 1 - x^2,\\
G &= 16r^2y^4(a^2 - 1) + 1 - u^2,\\
H &= ((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2,\\
I &= (a^2 - 1)l^2 + 1 - m^2,\\
J &= ai + k + 1 - l - i,\\
K &= n + l + v - y,\\
L &= p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m,\\
M &= q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x,\\
N &= z + pl(a - p) + t(2ap - p^2 - 1) - pm.
\end{aligned}
$$

Algumas observações simples: a única forma de P ser positivo é se $A = B = \cdots = N = 0$; neste caso seu valor será $k + 2$. Vemos assim que para produzir um número primo P com este polinômio devemos antes de mais nada tomar $k = P - 2$. As expressões auxiliares viram equações: como $A = 0$ temos $q = wz + h + j$. Assim, dado k para o qual $k + 2$ é primo, precisamos procurar valores para as outras letras que satisfaçam estas equações. Estes valores de certa forma *encodificam* uma demonstração de que $P = k + 2$ é primo.

Uma questão relacionada com a de *gerar* números primos é a de *testar* se um determinado número é primo. Existe um algoritmo bastante simples para testar se qualquer inteiro positivo n é primo: calcule o resto da divisão de n por cada inteiro m com $2 \leq m \leq \sqrt{n}$. Se o resto for 0 em algum caso então n é composto e encontramos um divisor; se isto nunca ocorrer, n é primo. O inconveniente deste algoritmo é que ele é muito lento: mesmo para um inteiro de 200 algarismos, teríamos que fazer aproximadamente 10^{100} divisões o que não só está fora do alcance da tecnologia atual mas fora do alcance de qualquer tecnologia plausível de acordo com o que se conhece de física [1].

[1] Bem, esta frase parecia verdadeira há uns dez anos atrás mas hoje suspeita-se que alguns

Alguns teoremas de teoria dos números podem ser usados para testar a primalidade de um inteiro positivo n. Pelo teorema de Wilson, por exemplo, podemos testar a primalidade de n calculando $(n-1)! \bmod n$; infelizmente, esta conta parece ser tão difícil de efetuar quanto a busca de divisores pelo algoritmo anterior. Observe que dizemos apenas que a conta *parece* difícil: não está excluída a possibilidade de alguém inventar um algoritmo rápido para calcular $(n-1)! \bmod n$.

Uma idéia mais bem sucedida é a de usar o pequeno teorema de Fermat: tomamos a, $1 < a < n$, e calculamos $a^{n-1} \bmod n$. Se n for primo teremos $a^{n-1} \equiv 1 \pmod n$; qualquer outro resultado indica que n é composto mesmo sem termos encontrado um fator de n. Observe que para calcular $a^{n-1} \bmod n$ não precisamos calcular $a \cdot a \cdots a$, $n-1$ vezes. Podemos fazer esta conta com menos de $4 \log_2 n$ operações envolvendo inteiros menores do que n^2: se $n-1 = \sum_{0 \le i < N} b_i 2^i$, $N = \lfloor \log_2(n-1) \rfloor$, então definimos

$$p_k = a^{\sum_{0 \le i < k} b_{N-k+i} 2^i} \bmod n$$

e temos $p_0 = 1$, $p_N = a^{n-1} \bmod n$, e podemos calcular p_{k+1} a partir de p_k com uma operação de elevar ao quadrado, tomar o resto da divisão por n, possivelmente multiplicar por a e novamente tomar o resto da divisão por n.

Se $a^{n-1} \equiv 1 \pmod n$, por outro lado, não demonstramos que n é primo; se n for composto satisfazendo $a^{n-1} \equiv 1 \pmod n$ dizemos que n é um *pseudoprimo* na base a. Pseudoprimos existem mas são raros (ver **(Cipolla)**): o menor pseudoprimo na base 2 é $341 = 11 \cdot 31$ e existem apenas 21.853 pseudoprimos na base 2 menores do que $2,5 \cdot 10^{10}$ (contra 1.091.987.405 primos). Pomerance (melhorando um resultado anterior de Erdös) provou que se $P\pi_a(x)$ é o número de pseudoprimos até x na base a temos

$$P\pi_a(x) \le x \cdot e^{-\frac{\log x \log\log\log x}{2 \log\log x}}$$

aspectos da física quântica possam ser explorados para colocar um computador especial em um estado de superposição em que ele faz várias contas diferentes em paralelo. Desta forma seria possível não apenas testar primalidade rapidamente mas até fatorar rapidamente inteiros muito grandes. Alguns *computadores quânticos* (é assim que são chamadas estas máquinas) extremamente rudimentares (com uns poucos q-bits de memória) já foram construidos mas não se sabe com certeza se é realmente possível construir computadores quânticos capazes, por exemplo, de fatorar rapidamente inteiros grandes; se isto for possível, o impacto científico e tecnológico será imenso. Por outro lado, não se sabe exatamente quais tarefas seriam rápidas para um computador quântico; suspeita-se que alguns problemas, como o de verificar se um grafo pode ser pintado com três cores de modo que não haja vértices adjacentes de mesma cor, seriam difíceis mesmo para este novo tipo de equipamento.

para x suficientemente grande. A proposição abaixo exibe uma família infinita de pseudoprimos na base a (para qualquer $a > 1$ dado); assim a simples verificação $a^{n-1} \equiv 1 \pmod{n}$ não *demonstra* a primalidade de n.

Proposição 3.1: *Seja $a > 1$ e p primo, $p > 2$. Então*

$$n = \frac{a^{2p}-1}{a^2-1} = \frac{a^p-1}{a-1} \cdot \frac{a^p+1}{a+1}$$

é um pseudoprimo na base a.

Dem: Pelo pequeno Teorema de Fermat,

$$\frac{a^p-1}{a-1} \equiv \frac{a^p+1}{a+1} \equiv 1 \pmod{p}$$

e verifica-se facilmente que estes números são ímpares, donde $n \equiv 1 \pmod{2p}$, ou $n = 2kp+1$ para k inteiro. Assim, como $a^{2p} \equiv 1 \pmod{n}$ temos $a^n = a^{2kp+1} = (a^{2p})^k \cdot a \equiv a \pmod{n}$. ■

Uma idéia natural é a de testar vários valores de a. Claramente, se $(a,n) > 1$, teremos $a^{n-1} \not\equiv 1 \pmod{n}$; entretanto, se n for um produto de uns poucos primos grandes os valores de a para os quais $(a,n) > 1$ são raros e se formos obrigados a encontrar um tal valor de a teremos feito muito pouco progresso em relação aos primeiros algoritmos. Aliás, uma vez encontrado a com $(a,n) > 1$ é fácil encontrar (a,n) pelo algoritmo de Euclides, o que nos dá uma fatoração (parcial) de n. É um fato interessante que existam alguns raros números compostos n, chamados *números de Carmichael*, com a propriedade que se $0 < a < n$ e $(a,n) = 1$ então $a^{n-1} \equiv 1 \pmod{n}$. Foi até demonstrado recentemente por Alford, Granville e Pomerance que se $CN(x)$ é o número de números de Carmichael menores do que x então

$$CN(x) \geq x^{2/7}$$

para x suficientemente grande, o que implica na existência de infinitos números de Carmichael. Há apenas 2163 números de Carmichael menores do que $2,5 \cdot 10^{10}$ e os primeiros são 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973 e 75361 [2].

Podemos refinar o conceito de pseudoprimo para definir *pseudoprimos fortes* na base a. Para definir quando n é um pseudoprimo forte na base a inicialmente

[2] Veja `ftp://ftp.dpmms.cam.ac.uk/pub/Carmichael` para a lista dos números de Carmichael menores do que 10^{16}.

escrevemos $n-1 = 2^k \cdot b$, com b ímpar. Se $n > 2$ é primo deve existir um menor valor de j para o qual $(a^b)^{2^j} \equiv 1 \pmod{n}$ (observe que por Fermat $(a^b)^{2^k} \equiv 1 \pmod{n}$). Se $j = 0$ isto significa que $a^b \equiv 1 \pmod{n}$; caso contrário temos $(a^b)^{2^{j-1}} \equiv -1 \pmod{n}$ já que -1 é o único valor de x diferente de 1 (módulo n) para o qual $x^2 \equiv 1 \pmod{p}$. Assim, dizemos que n composto ímpar é um pseudoprimo forte na base a se *ou* $a^b \equiv 1 \pmod{n}$ *ou* existe $j' < k$ com $(a^b)^{2^{j'}} \equiv -1 \pmod{n}$. Claramente todo pseudoprimo forte na base a é um pseudoprimo na base a mas pseudoprimos fortes são mais raros do que pseudoprimos.

Observe que se n for pseudoprimo base a mas não pseudoprimo forte base a, então o teste acima não apenas demonstra que n é composto mas produz uma fatoração parcial de n. De fato, seja $c = (a^b)^{2^{j-1}}$; temos $c - 1 \not\equiv 0 \pmod{n}$, $c + 1 \not\equiv 0 \pmod{n}$ mas $(c-1)(c+1) = c^2 - 1 \equiv 0 \pmod{n}$. Assim, $n = (n, c-1)(n, c+1)$.

Existem infinitos pseudoprimos fortes em qualquer base $a > 1$: Pomerance provou que, se $SP\pi_a(x)$ é o número de pseudoprimos fortes na base a menores ou iguais a x então

$$SP\pi_a(x) \geq e^{(\log x)^{5/4}}$$

para todo x suficientemente grande (ver [**Pomerance**]). Não existem "números de Carmichael fortes": para todo número composto ímpar n existe $0 < a < n$ com $(a, n) = 1$ e tal que n *não* é um pseudoprimo forte na base a. Melhor ainda, os valores de a que servem de testemunha para a não-primalidade de n são sempre relativamente freqüentes, como vemos na proposição abaixo.

Proposição 3.2: *Seja $n > 1$, n composto ímpar. Então o número de inteiros a, $0 < a < n$, para os quais n é um pseudoprimo na base a é menor do que $n/2$.*

Dem: Seja $n = p_1^{e_1} \dots p_m^{e_m}$ a fatoração completa de n. Pelo Teorema chinês dos restos e pela existência de raízes primitivas módulo $p_i^{e_i}$, podemos escrever $G = (\mathbb{Z}/(n))^* = \mathbb{Z}/\varphi(p_1^{e_1}) \oplus \dots \oplus \mathbb{Z}/\varphi(p_m^{e_m})$. Se escrevamos $\varphi(p_i^{e_i}) = 2^{k_i} \cdot b_i$, com b_i ímpar, podemos também escrever $G = G_2 \oplus G_o$, onde $G_2 = \mathbb{Z}/(2^{k_1}) \oplus \dots \oplus \mathbb{Z}/(2^{k_m})$ e G_o tem ordem ímpar. Não é difícil ver que n é um pseudoprimo forte na base a se e somente se a ordem das componentes de a^b em cada componente $\mathbb{Z}/(2^{k_i})$ é a mesma (onde $n - 1 = 2^k \cdot b$ com b ímpar). Mas dada uma ordem (digamos, a ordem de a^b em $\mathbb{Z}/(2^{k_1})$) o número de elementos de $\mathbb{Z}/(2^{k_2})$ com aquela ordem prescrita é no máximo a metade da ordem do grupo. ■

Na verdade pode-se demonstrar um resultado mais forte (quase certamente o melhor possível):

Teorema 3.3: *Seja $n > 1$, n composto ímpar. Então o número de inteiros a, $0 < a < n$, para os quais n é um pseudoprimo na base a é menor do que $n/4$.*

A demonstração deste teorema será omitida; o leitor pode considerar isto como um exercício. O caso em que n tem três ou mais fatores primos distintos pode ser tratado como na demonstração da proposição.

O teorema acima serve de base para os testes de primalidade *probabilísticos*. Dado n, tomamos N valores de a ao acaso no intervalo $1 < a < n$ e verificamos para cada a se n passa no teste de primalidade na base a. Se n for ímpar composto, a probabilidade de que um dado a acuse a não-primalidade de a é maior do que $3/4$ (pelo teorema); assim, a probabilidade de que n escape a N testes é menor do que 4^{-N}. Mesmo para valores moderados de N podemos dizer, se n passar no teste, que n é *provavelmente* primo. Este tipo de teste é extremamente útil em aplicações (como em criptografia) onde é importante criar primos relativamente grandes mas não existe a preocupação com demonstrações ou com perfeição absoluta. Nosso ponto de vista neste livro, entretanto, é o de um matemático: queremos não apenas um teste probabilístico mas uma demonstração da primalidade de n. Para isto nosso teste não parece tão bom: para demonstrarmos que n é primo ainda somos obrigados a testar aproximadamente $n/4$ valores de a, o que é lento demais.

Existe uma variação do conceito de pseudoprimalidade forte. Suponhamos que $n - 1 = p^k \cdot b$, $p \nmid b$. Seja a um inteiro, $0 < a < n$. O pequeno teorema de Fermat diz que se n é primo devemos ter $(a^b)^{p^k} \equiv 1 \pmod{n}$. Suponhamos que isto ocorra: nosso teste refinado consiste em considerar o último termo não côngruo a 1 módulo n da seqüência $a^b, (a^b)^p, (a^b)^{p^2}, \ldots, (a^b)^{p^k}$: chamemos este termo de c (se ocorrer $a^b \equiv 1 \pmod{n}$ não podemos aplicar o teste). Temos claramente $c^p - 1 = (c^{p-1} + \cdots + c + 1)(c - 1) \equiv 0 \pmod{n}$ e $c - 1 \not\equiv 0 \pmod{n}$; se n for primo devemos obrigatoriamente ter $c^{p-1} + \cdots + c + 1 \equiv 0 \pmod{n}$. Em outras palavras, se $c^{p-1} + \cdots + c + 1 \not\equiv 0 \pmod{n}$ sabemos que n é composto. Assim como no caso de pseudoprimos fortes, se n for pseudoprimo na base a mas falhar este teste para algum primo p acabamos de obter uma fatoração para n: $n = (n, c - 1)(n, c^{p-1} + \cdots + c + 1)$.

Já enunciamos a hipótese de Riemann no capítulo 1. Existe uma generalização importante da hipótese de Riemann, chamada hipótese de Riemann generalizada. Uma descrição precisa do enunciado da hipótese de Riemann

generalizada está fora dos nossos objetivos mas ela tem conseqüências muito importantes para testes de primalidade.

Teorema 3.4: (Teste de Miller) *Se a hipótese de Riemann generalizada é verdadeira então para todo* n *ímpar composto existe* $a < 2(\log n)^2$ *tal que* n *não é um pseudoprimo forte na base* a.

Não daremos a demonstração do teorema acima; o leitor interessado deve consultar [**Bach**].

Uma demonstração da hipótese de Riemann generalizada implicaria assim na existência de um teste de primalidade rápido e geral: não é difícil verificar que o tempo necessário para verificar primalidade de n pelo teste de Miller é limitado superiormente por um polinômio em $\log n$. Existe um outro algoritmo, bem mais sofisticado, devido a Adleman, Pomerance e Rumely, que demonstra (sem a necessidade de invocar conjecturas como a hipótese de Riemann) a primalidade de um primo n em um tempo limitado por $(\log n)^{c \log\log\log n}$ para uma certa constante positiva c.

Existem muitos valores de n para os quais é possível demonstrar primalidade em um tempo muito menor do que pelo teste de Miller. Veremos duas grandes classes de testes especiais: quando conhecemos uma fatoração (pelo menos parcial) para $n-1$ e quando conhecemos uma fatoração (também pelo menos parcial) para $n+1$.

Apêndice: O algoritmo de Agrawal-Kayal-Saxena:

Em agosto de 2002 os matemáticos indianos Manindra Agrawal, Neeraj Kayal e Nitin Saxena surpreenderam a comunidade matemática ao anunciar um algoritmo polinomial e determinístico muito simples para testar a primalidade de um número arbitrário.

O algoritmo é o seguinte:

Entrada: um inteiro $n > 1$.
1. Se ($n = a^b$ para $a, b \in \mathbb{N}$ e $b > 1$), retorna COMPOSTO.
2. Encontre o menor r tal que $\mathrm{ord}_r n > 4\log^2 n$.
3. Se $1 < \mathrm{mdc}(a, n) < n$ para algum $a \leq r$, retorna COMPOSTO.
4. Se $n \leq r$, retorna PRIMO.
5. Para $a = 1$ até $\lfloor 2\sqrt{\varphi(r)}\log n \rfloor$ faça
   se $((X+a)^n \not\equiv X^n + a \pmod{X^r - 1, n})$, retorna COMPOSTO;
6. Retorna PRIMO;

O artigo dos autores ([AKS]), já incorporando alguns melhoramentos sugeridos por outros especialistas na área, apresenta uma demonstração elementar de que o algoritmo funciona (e gasta um tempo total limitado por um polinômio em $\log n$). Não repetiremos essa prova aqui, limitando-nos a apresentar um importante resultado relacionado, que motiva o algoritmo. Veja também [Co] para uma exposição sobre o assunto.

Proposição: *Sejam a, n inteiros positivos com $n > 1$ e $\mathrm{mdc}(a, n) = 1$. Então $(X + a)^n \equiv X^n + a \pmod{n}$ se e somente se n é primo.*

Observe que no enunciado acima (e no algoritmo) a congruência é entre polinômios.

Dem: Se n é primo, $(X + a)^n \equiv X^n + a$ segue do pequeno teorema de Fermat e do fato de que $\binom{n}{m}$ é múltiplo de n para todo m com $0 < m < n$, quando n é primo (veja a Proposição 3.17). Por outro lado, se n é composto e q é um primo que divide n, então o coeficiente de X^q no desenvolvimento de $(X + a)^n$ é $\binom{n}{q} \cdot a^{n-q}$, que não é múltiplo de n: de fato, se q^k é a maior potência de q que divide n então a maior potência de q que divide $\binom{n}{q}$ é q^{k-1}. ■

Essa proposição fornece um algoritmo para testar primalidade, o qual entretanto é muito ineficiente, pois o grau de $(X + a)^n$ é muito alto. O que o algoritmo de [AKS] faz é testar a congruência da proposição módulo $X^r - 1$ para um certo valor de r (determinado pelo algoritmo) e para uma certa quantidade de valores de a. A validade dessas congruências já é suficiente para garantir que n é primo.

3.2 Testes baseados em fatorações de $n-1$

Proposição 3.5: *Seja $n > 1$. Se para cada fator primo q de $n-1$ existe um inteiro a_q tal que $a_q^{n-1} \equiv 1 \pmod n$ e $a_q^{(n-1)/q} \not\equiv 1 \pmod n$ então n é primo.*

Dem: Seja q^{k_q} a maior potência de q que divide $n-1$. A ordem de a_q em $(\mathbb{Z}/(n))^*$ é um múltiplo de q^{k_q}, donde $\varphi(n)$ é um múltiplo de q^{k_q}. Como isto vale para todo fator primo q de $n-1$, $\varphi(n)$ é um múltiplo de $n-1$ e n é primo. ■

Proposição 3.6: (Pocklington) *Se $n-1 = q^k R$ onde q é primo e existe um inteiro a tal que $a^{n-1} \equiv 1 \pmod n$ e $\mathrm{mdc}(a^{(n-1)/q} - 1, n) = 1$ então qualquer fator primo de n é congruo a 1 módulo q^k.*

Dem: Se p é um fator primo de n então $a^{n-1} \equiv 1 \pmod p$ e p não divide $a^{(n-1)/q} - 1$, donde $\mathrm{ord}_p\, a$, a ordem de a módulo p, divide $n-1$ mas não divide $(n-1)/q$. Assim, $q^k | \mathrm{ord}_p\, a | p-1$, donde $p \equiv 1 \pmod{q^k}$. ■

Corolário 3.7: *Se $n-1 = FR$, com $F > R$ e para todo fator primo q de F existe $a > 1$ tal que $a^{n-1} \equiv 1 \pmod n$ e $\mathrm{mdc}(a^{(n-1)/q} - 1, n) = 1$ então n é primo.*

Dem: Seja q um fator primo de F e q^k a maior potência de q que divide F; pela proposição anterior, todo fator primo de n deve ser côngruo a 1 módulo q^k. Como isto vale para qualquer fator primo de F, segue que qualquer fator primo de n deve ser côngruo a 1 módulo F. Como $F > \sqrt{n}$, isto implica que n é primo. ■

De fato, basta conhecer um conjunto de fatores primos cujo produto seja maior do que $(n-1)^{1/3}$ para, usando o resultado de Pocklington, tentar demonstrar a primalidade de n (o que deixamos como exercício). Os seguintes critérios clássicos são conseqüências diretas das proposições acima.

Fermat conjecturou que todo número da forma $F_n = 2^{2^n} + 1$ fosse primo e verificou a conjectura para $n \leq 4$. Observe que $2^n + 1$ (e em geral $a^n + 1$ com $a \geq 2$) *não* é primo se n não é uma potência de 2: se p é um fator primo ímpar de n, podemos escrever $a^n + 1 = b^p + 1 = (b+1)(b^{p-1} - b^{p-2} + \cdots + b^2 - b + 1)$ onde $b = a^{n/p}$. Euler mostraria mais tarde que F_5 não é primo (temos $F_5 = 4294967297 = 641 \cdot 6700417$) e já se demonstrou que F_n é composto para vários outros valores de n; nenhum outro primo da forma $F_n = 2^{2^n} + 1$ é conhecido, mas se conhecem muitos primos (alguns bastante grandes) da forma $a^{2^n} + 1$,

que são conhecidos como primos de Fermat generalizados. O teste a seguir mostra como testar eficientemente a primalidade de F_n.

Corolário 3.8: (Teste de Pépin) *Seja* $F_n = 2^{2^n}+1$; F_n *é primo se e somente se* $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

Dem: Se $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ então a primalidade de F_n segue da Proposição 3.5. Por outro lado, se F_n é primo então $3^{(F_n-1)/2} \equiv (\frac{3}{F_n}) = (\frac{F_n}{3}) = (\frac{2}{3}) = -1 \pmod{F_n}$. ■

Corolário 3.9: (Teorema de Proth; 1878) *Seja* $n = h \cdot 2^k + 1$ *com* $2^k > h$. *Então* n *é primo se e somente se existe um inteiro* a *com* $a^{(n-1)/2} \equiv -1 \pmod{n}$.

Dem: Se n é primo, podemos tomar a qualquer com $(\frac{a}{n}) = -1$; ou seja, metade dos inteiros entre 1 e $n-1$ serve como a. A recíproca segue da Proposição 3.7 com $F = 2^k$. ■

Corolário 3.10: *Se* $n = h \cdot q^k + 1$ *com* q *primo e* $q^k > h$. *Então* n *é primo se e somente se existe um inteiro* a *com* $a^{n-1} \equiv 1 \pmod{n}$ *e* $\mathrm{mdc}(a^{(n-1)/q} - 1, n) = 1$.

Dem: Se n é primo, podemos tomar a qualquer que não seja da forma x^q módulo n; ou seja, uma proporção de $(q-1)/q$ dentre inteiros entre 1 e $n-1$ serve como a. A recíproca segue da Proposição 3.7 com $F = q^k$. ■

Uma expressiva maioria entre os 100 maiores primos conhecidos estão nas condições do teorema de Proth (ver tabelas). Isto se deve ao fato de primos desta forma serem freqüentes (mais freqüentes do que, por exemplo, primos de Mersenne) e que sua primalidade é facilmente demonstrada usando este resultado.

3.3 Primos de Mersenne

Lembramos que um número de Mersenne é um número da forma $M_p = 2^p - 1$. Vejamos primeiramente que $2^p - 1$ só tem chance de ser primo quando p é primo.

Proposição 3.11: *Se* $2^n - 1$ *é primo então* n *é primo.*

Dem: Se $n = ab$ com $a, b \geq 2$ então $1 < 2^a - 1 < 2^n - 1$ e $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 \equiv 1^b - 1 = 0 \pmod{2^a - 1}$ e $2^n - 1$ é composto. ■

Por outro lado, não se sabe demonstrar nem que existam infinitos *primos de Mersenne* nem que existem infinitos primos p para os quais M_p é composto. Conjectura-se, entretanto, que existam infinitos primos p para os quais M_p é primo e que, se p_n é o n-ésimo primo deste tipo, temos

$$0 < A < \frac{\log p_n}{n} < B < +\infty$$

para constantes A e B. Existem algumas conjecturas mais precisas quanto ao valor de

$$\lim_{n\to\infty} \sqrt[n]{p_n};$$

Eberhart conjectura que este limite exista e seja igual a $3/2$; Wagstaff por outro lado conjectura que o limite seja

$$2^{e^{-\gamma}} \approx 1{,}4757613971$$

onde γ é a já mencionada constante de Euler-Mascheroni.

Primos de Mersenne são interessantes também por causa de *números perfeitos*. Dado $n \in \mathbb{N}^*$, definimos

$$\sigma(n) = \sum_{d|n} d,$$

a soma dos divisores (positivos) de n. Pelo teorema fundamental da aritmética demonstramos facilmente que se

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m},$$

com $p_1 < p_2 < \cdots < p_m$ então

$$\begin{aligned}\sigma(n) &= (1 + p_1 + \cdots + p_1^{e_1}) \cdots (1 + p_m + \cdots + p_m^{e_m}) \\ &= \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdots \frac{p_m^{e_m+1} - 1}{p_m - 1}.\end{aligned}$$

Em particular, se $(a, b) = 1$ então $\sigma(ab) = \sigma(a)\sigma(b)$. Um inteiro positivo n é dito *perfeito* se $\sigma(n) = 2n$; os primeiros números perfeitos são 6, 28 e 496. Nosso próximo resultado caracteriza os números perfeitos pares.

Proposição 3.12: *Se M_p é um primo de Mersenne então $2^{p-1}M_p$ é perfeito. Além disso, todo número perfeito par é da forma $2^{p-1}M_p$ para algum primo p, sendo M_p um primo de Mersenne.*

Dem: Se M_p é primo então

$$\sigma(2^{p-1}M_p) = (2^p - 1)(M_p + 1) = 2 \cdot 2^{p-1}M_p.$$

Por outro lado seja $n = 2^k b$, com $k > 0$ e b ímpar, um número perfeito par. Temos $\sigma(n) = 2n = \sigma(2^k)\sigma(b)$ donde $2^{k+1}b = (2^{k+1} - 1)\sigma(b)$. Como $(2^{k+1} - 1)|2^{k+1}b$ e $(2^{k+1} - 1, 2^{k+1}) = 1$, temos $(2^{k+1} - 1)|b$, donde $b = (2^{k+1} - 1) \cdot I$, para um certo número ímpar I. Caso $I > 1$, teremos

$$\sigma(n) = (2^{k+1} - 1)\sigma(b) \geq (2^{k+1} - 1) \cdot (1 + I + b) =$$

$$= 2^{k+1}b + (2^{k+1} - 1)I - b + 2^{k+1} - 1 = 2^{k+1}b + 2^{k+1} - 1 > 2^{k+1}b = 2n,$$

absurdo. Assim $b = 2^{k+1} - 1$ e $(2^{k+1} - 1)\sigma(b) = \sigma(n) = 2n = 2^{k+1}b = (2^{k+1} - 1)(b + 1)$, donde $\sigma(b) = (b + 1)$, e portanto b é primo. Pela proposição 3.9, $p = k + 1$ é primo, $b = M_p$ e $n = 2^{p-1}M_p$. ■

Por outro lado, um dos problemas em aberto mais antigos da matemática é o da existência de números perfeitos ímpares. Sabe-se apenas que um número perfeito ímpar, se existir, deve ser muito grande (mais de 300 algarismos) e satisfazer simultaneamente várias condições complicadas.

Conjectura 3.13: *Não existe nenhum número perfeito ímpar.*

Nosso próximo resultado é o critério de Lucas-Lehmer, a base dos algoritmos que testam para grandes valores de p se $2^p - 1$ é ou não primo:

Teorema 3.14: *Seja S a seqüência definida por $S_0 = 4$, $S_{k+1} = S_k^2 - 2$ para todo natural k. Seja $n > 2$; $M_n = 2^n - 1$ é primo se e somente se S_{n-2} é múltiplo de M_n.*

Dem: Observemos inicialmente que

$$S_n = (2 + \sqrt{3})^{2^n} + (2 - \sqrt{3})^{2^n}$$

para todo natural n. A demonstração por indução é simples: claramente $S_0 = 4 = (2 + \sqrt{3})^{2^0} + (2 - \sqrt{3})^{2^0}$ e

$$\begin{aligned} S_{k+1} &= S_k^2 - 2 \\ &= ((2 + \sqrt{3})^{2^k} + (2 - \sqrt{3})^{2^k})^2 - 2 \\ &= ((2 + \sqrt{3})^{2^k})^2 + 2 \cdot (2 + \sqrt{3})^{2^k} \cdot (2 - \sqrt{3})^{2^k} + ((2 - \sqrt{3})^{2^k})^2 - 2 \\ &= (2 + \sqrt{3})^{2^{k+1}} + (2 - \sqrt{3})^{2^{k+1}}. \end{aligned}$$

Suponha por absurdo que $M_n|(2+\sqrt{3})^{2^{n-2}}+(2-\sqrt{3})^{2^{n-2}}$ e que M_n seja composto, com um fator primo q com $q^2 < M_n$. Teremos $(2+\sqrt{3})^{2^{n-2}} + (2-\sqrt{3})^{2^{n-2}} \equiv 0 \pmod{q}$ donde, no grupo multiplicativo $G = (\mathbb{Z}/(q)[\sqrt{3}])^*$, temos $(2+\sqrt{3})^{2^{n-2}} = -(2-\sqrt{3})^{2^{n-2}}$. Como $2-\sqrt{3} = (2+\sqrt{3})^{-1}$, esta equação pode ser reescrita como $(2+\sqrt{3})^{2^{n-1}} = -1$ (ainda em G), o que significa que a ordem de $2+\sqrt{3}$ em G é exatamente 2^n. Isto é um absurdo, pois o número de elementos de G é no máximo $q^2-1 < 2^n$. Fica portanto demonstrado que se S_{n-2} é múltiplo de M_n então M_n é primo.

Suponha agora M_n primo, $n > 2$. Lembramos que n é um primo ímpar. Por reciprocidade quadrática temos $(\frac{3}{M_n}) = -(\frac{M_n}{3}) = -1$, pois $3 \equiv M_n \equiv -1 \pmod 4$ e $M_n \equiv 1 \pmod 3$. Assim, 3 não é um quadrado em $\mathbb{Z}/(M_p)$ e $K = \mathbb{Z}/(M_p)[\sqrt{3}]$ é um corpo de ordem M_n^2. Queremos provar que $(2+\sqrt{3})^{2^{n-2}} + (2-\sqrt{3})^{2^{n-2}} \equiv 0 \pmod{M)_p}$, ou seja, que é igual a 0 em K. Isto equivale a demonstrarmos que temos $(2+\sqrt{3})^{2^{n-2}} = -(2-\sqrt{3})^{2^{n-2}}$ em K, o que pode ser reescrito como $(2+\sqrt{3})^{2^{n-1}} = -1$; devemos portanto provar que a ordem de $2+\sqrt{3}$ é exatamente 2^n. Note que $2^n = M_n + 1$ donde $(2+\sqrt{3})^{2^n} = (2+\sqrt{3})^{M_n}(2+\sqrt{3}) = (2^{M_n} + \sqrt{3}^{M_n})(2+\sqrt{3}) = (2+3^{\frac{M_n-1}{2}}\sqrt{3})(2+\sqrt{3}) = (2+(\frac{3}{M_n})\sqrt{3})(2-\sqrt{3}) = (2-\sqrt{3})(2+\sqrt{3}) = 1$; assim é claro que a ordem de $2+\sqrt{3}$ é um divisor de 2^n.

Como K^* tem $M_n^2 - 1 = 2^{n+1}(2^{n-1}-1)$ elementos, devemos provar que $2+\sqrt{3}$ não é uma quarta potência em K. Note que $(2+\sqrt{3})^{2^n} = 1$ demonstra que $2+\sqrt{3}$ é um quadrado, o que aliás pode ser visto mais diretamente: $2+\sqrt{3} = (1+\sqrt{3})^2/2$ e $2 = 2^{n+1} = 2^{(n+1)^2}$ é uma quarta potência em K. Resta-nos assim demonstrar que $\pm(1+\sqrt{3})$ não são quadrados em K. Suponha por absurdo que $\epsilon(1+\sqrt{3}) = (a+b\sqrt{3})^2$, com $\epsilon = \pm 1$; temos $\epsilon(1-\sqrt{3}) = (a-b\sqrt{3})^2$ e, multiplicando, $-2 = (a^2-3b^2)^2$, o que significa que -2 é um quadrado módulo M_n (pois a e b são inteiros). Isto, entretanto, é claramente falso: $(\frac{-2}{M_n}) = (\frac{-1}{M_n})(\frac{2}{M_n}) = -1 \cdot 1 = -1$, pois $M_n \equiv 3 \pmod 4$ e já vimos que 2 é um quadrado módulo M_p. Isto conclui a demonstração. ■

Mesmo quando M_p não é primo, podemos garantir que seus fatores primos serão de certas formas especiais. Isto é muito útil quando procuramos primos de Mersenne pois podemos eliminar alguns expoentes encontrando fatores primos de M_p. Isto também pode ser útil para conjecturarmos quanto à "probabilidade" de M_p ser primo, ou, mais precisamente, quanto à distribuição dos primos de Mersenne.

Proposição 3.15: *Sejam* $p > 2$ *e* q *primos com* q *um divisor de* M_p. *Então* $q \equiv 1 \pmod{p}$ *e* $q \equiv \pm 1 \pmod{8}$.

Dem: Se q divide M_p então $2^p \equiv 1 \pmod{q}$, o que significa que a ordem de 2 módulo q é p (pois p é primo). Isto significa que p é um divisor de $q-1$, ou seja, que $q \equiv 1 \pmod{p}$. Por outro lado, $2 \equiv 2^{p+1} = (2^{(p+1)/2})^2 \pmod{q}$, donde $(\frac{2}{q}) = 1$, o que significa que $q \equiv \pm 1 \pmod{8}$. ■

Os vários valores de p para os quais a primalidade de M_p foi testada sugerem que para a ampla maioria dos valores de p, M_p *não* é primo. Isto é apenas uma conjectura: não se sabe demonstrar sequer que existem infinitos primos p para os quais M_p seja composto. Vamos agora ver uma proposição que serve para garantir que para certos valores especiais de p, alguns muito grandes, M_p *não* é primo.

Proposição 3.16: *Seja* p *primo,* $p \equiv 3 \pmod{4}$. *Então* $2p+1$ *é primo se e somente se* $2p+1$ *divide* M_p.

Dem: Se q é primo então $M_p = 2^p - 1 = 2^{(q-1)/2} - 1 \equiv (\frac{2}{q}) - 1 \pmod{q}$. Mas $p \equiv 3 \pmod{4}$ significa que $q \equiv 7 \pmod{8}$, donde $(\frac{2}{q}) = 1$. Assim, $M_p \equiv 0 \pmod{q}$, o que demonstra uma das implicações da proposição.

Por outro lado, se $2p+1$ não é primo tem fatores primos r com $r \not\equiv 1 \pmod{p}$ (pois $r < p$). Se $2p+1$ dividisse M_p, r seria um fator primo de M_p, contrariando a proposição anterior. ■

Os primos p para os quais $2p+1$ é primo são chamados de *primos de Sophie Germain*. Alguns primos de Sophie Germain bastante grandes são conhecidos, como $p_0 = 48047305725 \cdot 2^{172403} - 1$; assim, pela proposição anterior, M_{p_0} é composto. Sabe-se também que se $\pi_{SG}(x)$ denota o número de primos de Sophie Germain menores do que x então existe C tal que para todo x

$$\pi_{SG}(x) < C\frac{x}{(\log x)^2}.$$

Acredita-se que $\pi_{SG}(x)$ seja assintótico a $cx/(\log x)^2$ para algum $c > 0$ mas não se sabe demonstrar sequer que existem infinitos primos de Sophie Germain.

3.4 Testes baseados em fatorações de $n+1$

Suponha dados inteiros $n > 1$, P e Q tais que $D = P^2 - 4Q$ não é um quadrado módulo n. Seja

$$\alpha = \frac{P + \sqrt{D}}{2},$$

raiz da equação $X^2 - PX + Q = 0$. É fácil provar por indução que

$$\alpha^m = \frac{V_m + U_m\sqrt{d}}{2}$$

para todo natural m onde U_m e V_m são definidos recursivamente por

$$\begin{array}{lll} U_0 = 0, & U_1 = 1, & U_{m+2} = PU_{m+1} - QU_m, \\ V_0 = 2, & V_1 = P, & V_{m+2} = PV_{m+1} - QV_m. \end{array}$$

Se

$$\overline{\alpha} = \frac{P - \sqrt{D}}{2}$$

é a segunda raiz da equação $X^2 - PX + Q = 0$, podemos também escrever

$$U_m = \frac{\alpha^m - \overline{\alpha}^m}{\sqrt{D}}, \qquad V_m = \alpha^m + \overline{\alpha}^m,$$

como se demonstra facilmente por indução. Segue destas fórmulas que

$$U_{n+1} = \frac{PU_n + V_n}{2}, \qquad V_{n+1} = \frac{DU_n + PV_n}{2}$$

e

$$U_{2m} = U_m V_m, \qquad V_{2m} = V_m^2 - 2Q^m.$$

Estas fórmulas nos permitem calcular U_m e V_m módulo n em $C \log m$ operações (para alguma constante positiva C): escrevemos $m = \sum_{0 \le i < M} a_i 2^i$, definimos

$$m_k = \sum_{0 \le i < k} a_{i+N-k} 2^i$$

e calculamos sucessivamente U_{m_1}, V_{m_1}, ..., U_{m_k}, V_{m_k}, ..., $U_{m_M} = U_m$, $V_{m_M} = V_m$.

Lembramos que vimos no capítulo anterior que se $p > 2$ é primo e d não é um quadrado módulo p então $K = (\mathbb{Z}/(p))[\sqrt{d}]$ é um corpo com p^2 elementos.

Proposição 3.17: *Se n é primo e D não é um quadrado módulo n então $\alpha^n = \overline{\alpha}$ em $K = (\mathbb{Z}/(n))[\sqrt{D}]$.*

Dem: Suponhamos que n seja primo. Em K temos a identidade $(X+Y)^n = X^n + Y^n$: ela segue do binômio de Newton e do fato que

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

é múltiplo de n se $0 < m < n$. Aplicando esta identidade a α temos

$$\alpha^n = \frac{P^n + D^{(n-1)/2}\sqrt{D}}{2^n} = \frac{P - \sqrt{D}}{2} = \overline{\alpha},$$

pois $P^n \equiv P \pmod{n}$, $2^n \equiv 2 \pmod{n}$ e $D^{(n-1)/2} \equiv -1 \pmod{n}$. ■

Analogamente, se n é primo, temos $\overline{\alpha}^n = \alpha$ em K. Assim, ainda em K, $\alpha^{n+1} = \overline{\alpha}^{n+1} = \alpha\overline{\alpha}$. Segue da fórmula para U_m que $U_{n+1} \equiv 0 \pmod{n}$. Proclamamos este resultado como uma proposição:

Proposição 3.18: *Se n é primo ímpar, $(\frac{D}{n}) = -1$ e as seqüências U_m e V_m são definidas pelas recorrências*

$$\begin{aligned} U_0 &= 0, & U_1 &= 1, & U_{m+2} &= PU_{m+1} - QU_m, \\ V_0 &= 2, & V_1 &= P, & V_{m+2} &= PV_{m+1} - QV_m. \end{aligned}$$

então $U_{n+1} \equiv 0 \pmod{n}$.

Dem: Acima. ■

Esta proposição nos dá mais um algoritmo para testar a primalidade de n.

Proposição 3.19: *Se $n \neq 2$ é primo, $n \nmid Q$, $n \nmid D$ e D é quadrado módulo n então $U_{n-1} \equiv 0 \pmod{n}$.*

Dem: No anel $K = \mathbb{Z}/(n)[\sqrt{D}]$, 2 é invertível, assim como D e $\sqrt{D}$. Em K temos, portanto,

$$\alpha^n = \frac{P^n + D^{\frac{n-1}{2}}\sqrt{D}}{2^n} = \frac{P + \sqrt{D}}{2} = \alpha$$

donde $\alpha^{n-1} = 1$ em K (pois α é invertível em K: de fato, $\alpha\overline{\alpha} = Q$, que é invertível em K). Do mesmo modo, $\overline{\alpha}^{n-1} = 1$ em K e portanto temos, em K,

$$U_{n-1} = \frac{1}{\sqrt{D}}(\alpha^{n-1} - \overline{\alpha}^{n-1}) = 0,$$

ou seja, $U_{n-1} \equiv 0 \pmod{n}$. ■

Em suma, se $n \neq 2$ é primo, $n \nmid Q$, $n \nmid D$ então $U_{n-(\frac{D}{n})}$ é múltiplo de n, o que se deve ao fato de α^m ser igual a $\overline{\alpha}^m$ se $m = n - (\frac{D}{n})$ no anel $K = \mathbb{Z}/(n)[\sqrt{D}]$. Observemos agora que se $\alpha^m = \overline{\alpha}^m$ em K então existe um inteiro r tal que

$$\alpha^m = \overline{\alpha}^n + nr\sqrt{D}$$

pois $\frac{\alpha^m - \overline{\alpha}^m}{\sqrt{D}} \in \mathbb{Z}$. Vamos usar este fato para mostrar por indução o seguinte resultado.

Proposição 3.20: *Se $n \neq 2$ é primo, $n \nmid Q$ e $n \nmid D$ então, para todo natural $k \geq 1$, $U_{m \cdot n^{k-1}}$ é múltiplo de n^k, onde $m = n - (\frac{D}{n})$.*

Dem: Vamos supor, por hipótese de indução, que $\alpha^{m \cdot n^{k-1}} = \overline{\alpha}^{m \cdot n^{k-1}} + n^k r_k \sqrt{D}$, $r_k \in \mathbb{Z}$. Elevando os dois lados da equação à n-ésima potência temos

$$\alpha^{m \cdot n^k} = (\overline{\alpha}^{m \cdot n^{k-1}} + n^k r_k \sqrt{D})^n = \overline{\alpha}^{m \cdot n^k} + n^{k+1} r_{k+1} \sqrt{D}$$

onde r_{k+1} pertence a $\mathbb{Z}[\sqrt{D}]$ por um lado, e por outro $n^{k+1} r_{k+1} = U_{m \cdot n^k}$ é um inteiro, o que implica que $r_{k+1} \in \mathbb{Q} \cap \mathbb{Z}[\sqrt{D}]$, e portanto é inteiro, o que conclui a prova da afirmação, que equivale ao enunciado. ■

Proposição 3.21: *Sejam $r \geq 1$ com $\mathrm{mdc}(r, Q) = 1$, e (U_k) uma seqüência de Lucas (com $U_0 = 0$, $U_1 = 1$ e $U_{k+2} = PU_{k+1} - QU_k$). Se $A_r = \{k \in \mathbb{N}^* \mid U_k$ é múltiplo de $r\}$ é não vazio então existe $a \in \mathbb{N}^*$ tal que $r \mid U_k$ se e somente se $a \mid k$. Tal a será denotado por $\mathrm{ord}_r U$.*

Dem: Observemos inicialmente que para todo $m, n \in \mathbb{N}$, $n \neq 0$ temos $U_{m+n} = U_m U_{n+1} - QU_{m-1}U_n$. De fato, considerando m fixo e n variável, os dois lados da igualdade satisfazem a mesma recorrência de segunda ordem $X_{k+2} = PX_{k+1} - QX_k$, $\forall k \in \mathbb{N}$, e temos, para $n = 0$, $U_{m+0} = U_m \cdot U_1 - QU_{m-1} \cdot U_0$ (pois $U_1 = 1$ e $U_0 = 0$), e, para $m = 1$, $U_{m+1} = U_m \cdot U_2 - QU_{m-1} \cdot U_1$ (pois $U_2 = P$, $U_1 = 1$ e $U_{m+1} = PU_m - QU_{n-1}$), o que implica a igualdade para todo $n \in \mathbb{N}$.

Como conseqüência, se $r \mid U_\ell$ e $r \mid U_n$ então $r \mid U_{m+n}$. Por outro lado, se $r \mid U_\ell$ e $r \mid U_s$, com $\ell < s$ então, como (fazendo $m = \ell$, $n = s - \ell$) $U_s = U_\ell U_{s-\ell+1} - QU_{\ell-1}U_{s-\ell}$ temos que r divide $QU_{\ell-1}U_{s-\ell}$, mas $\mathrm{mdc}(Q, r) = 1$ e $\mathrm{mdc}(U_{\ell-1}, U_\ell)$ divide $Q^{\ell-1}$ (o que pode ser facilmente provado por indução a partir de $U_{\ell+1} = PU_\ell - QU_{\ell-1}$), donde $\mathrm{mdc}(r, U_{\ell-1})$ também é igual a 1, logo $r \mid U_{s-\ell}$. Assim, $m, n \in A_r \Rightarrow m + n \in A_r$, $\ell, s \in A_r$, $\ell < s \Rightarrow s - \ell \in A_r$, o que implica que A_r é da forma descrita, com $a = \min A_r$ (de fato, se existe $k \in A_r$ que não seja múltiplo de a, existiriam b e c naturais com $k = ab + c$,

$0 < c < a$, mas $k \in A_r$ e, como $a \in A_r$, $ab \in A_r$, logo $c = k - ab$ pertenceria a A_r , contradizendo a definição de a. ■

Teorema 3.22: *Seja $n > 1$ um inteiro ímpar. Se existe um inteiro d primo com n tal que para todo fator primo r de $n+1$ existem $P^{(r)}$, $Q^{(r)}$ e $m^{(r)}$ inteiros com* $\mathrm{mdc}(m^{(r)}, n) = 1$ *e* $D^{(r)} = (P^{(r)})^2 - 4Q^{(r)} \equiv d(m^{(r)})^2 \pmod n$ *tais que a seqüência de Lucas associada* $(U_k^{(r)})$ *satisfaz* $U_{n+1}^{(r)} \equiv 0 \pmod n$ *e* $U_{\frac{n+1}{r}}^{(r)} \not\equiv 0 \pmod n$ *então n é primo.*

Dem: Seja $n+1 = r_1^{\alpha_1} r_2^{\alpha_2} \dots r_k^{\alpha_k}$ a fatoração prima de $n+1$. As hipóteses implicam que $r_i^{\alpha_i}$ divide $\mathrm{ord}_n U^{(r_i)}$ para $i = 1, 2, \dots, k$. Por outro lado, se $n = \ell_1^{\beta_1} \ell_2^{\beta_2} \dots \ell_s^{\beta_s}$ é a fatoração prima de n, segue da Proposição 3.20 que $\mathrm{ord}_{\ell_j^{\beta_j}} U^{(r_i)}$ divide $\ell_j^{\beta_j - 1}(\ell_j - (\frac{d}{\ell_j}))$ (A hipótese $\ell_j \nmid Q^{(r_i)}$ é satisfeita. De fato, como $\mathrm{mdc}(n, d) = 1$, ℓ_j não divide $D^{(r_i)}$, e, se ℓ_j dividisse $Q^{(r_i)}$, ℓ_j não dividiria $P^{(r_i)}$, e teríamos $U_k^{(r_i)} \equiv (P^{(r_i)})^{k-1} \pmod{\ell_j}$ para todo $k \geq 1$, e ℓ_j não dividiria $U_k^{(r_i)}$ para nenhum $k \geq 1$, contradizendo o fato de n dividir $U_{n+1}^{(r_i)}$). Assim, se $M = \mathrm{mmc}\{\ell_j^{\beta_j - 1}(\ell_j - (\frac{d}{\ell_j})),\ 1 \leq j \leq d\}$ temos que $\ell_j^{\beta_j}$ divide $U_M^{(r_i)}$, para $1 \leq j \leq d$, $1 \leq i \leq k$. Isso implica que $n = \ell_1^{\beta_1} \dots \ell_s^{\beta_s}$ divide $U_M^{(r_i)}$ para $1 \leq i \leq k$, e portanto $r_i^{\alpha_i} | \mathrm{ord}_n U^{(r_i)} | M$ para $1 \leq i \leq k$, donde $n+1$ divide M. Temos agora duas possibilidades:

(i) $s = 1$. Nesse caso temos que $n+1$ divide $M = \ell_1^{\beta_1}(\ell_1 - (\frac{d}{\ell_1}))$ o que é absurdo se $(\frac{d}{\ell_1}) = 1$, pois teríamos $M < \ell_1^{\beta_1} = n$, e se $(\frac{d}{\ell_1}) = -1$ temos que $\ell_1^{\beta_1} + 1$ divide $\ell_1^{\beta_1 - 1}(\ell_1 + 1)$, o que implica $\beta_1 = 1$, ou seja, n é primo.

(ii) $s \geq 2$. Nesse caso

$$\begin{aligned} M &= \mathrm{mmc}\{\ell_j^{\beta_j - 1}(\ell_j - (d/\ell_j))\} \\ &= 2\,\mathrm{mmc}\{\ell_j^{\beta_j - 1}(\ell_j - (d/\ell_j))/2, \quad 1 \leq j \leq s\} \\ &\leq 2\prod_{j=1}^{s}(\ell_j^{\beta_j - 1}(\ell_j - (d/\ell_j))/2) \\ &\leq 2n\prod_{j=1}^{s}\frac{\ell_j + 1}{2\ell_j}, \end{aligned}$$

que é sempre menor que n (pois $2 \cdot \frac{4}{6} \cdot \frac{6}{10} < 1$) e portanto é um absurdo que $n+1$ divida M. ■

A seguinte proposição, devida a Morrison, é análoga ao resultado de Pocklington:

Proposição 3.23: *Seja* $N > 1$ *um inteiro ímpar e* $N + 1 = FR$. *Se existe um inteiro* d *primo com* N *tal que para todo fator primo* r *de* F *existe uma seqüência de Lucas* $U_n^{(r)}$ *associada a inteiros* $P^{(r)}, Q^{(r)}$ *e um inteiro* $m^{(r)}$ *primo com* N *e* $D^{(r)} = (P^{(r)})^2 - 4Q^{(r)} \equiv d(m^{(r)})^2 \pmod N$ *tal que* $N \mid U_{N+1}^{(r)}$ *e* $\mathrm{mdc}(U_{\frac{N+1}{r}}^{(r)}, N) = 1$ *então cada fator primo* ℓ *de* N *satisfaz* $\ell \equiv (\frac{d}{\ell}) \pmod F$.

Dem: Se $F = r_1^{\alpha_1} r_2^{\alpha_2} \dots r_k^{\alpha_k}$ é a fatoração prima de F então $\mathrm{ord}_N\, U^{(r_i)} \mid N+1$ para $1 \le i \le k$. Se ℓ é um fator primo de N, também temos $\mathrm{ord}_\ell\, U^{(r_i)} \mid N+1$. Como $\mathrm{mdc}(N, U_{\frac{N+1}{r_i}}^{(r_i)}) = 1$ segue que $\ell \nmid U_{\frac{N+1}{r_i}}^{(r_i)}$, donde $\mathrm{ord}_\ell\, U^{(r_i)} \nmid \frac{M+1}{r_i}$, e portanto $r_i^{\alpha_i}$ divide $\mathrm{ord}_\ell\, U^{(r_i)}$ para $1 \le i \le k$. Por outro lado, $\mathrm{ord}_\ell\, U^{(r_i)}$ divide $\ell - (\frac{d}{\ell})$, donde $r_i^{\alpha_i}$ divide $\ell - (\frac{d}{\ell})$ para $1 \le i \le k \Rightarrow F$ divide $\ell - (\frac{d}{\ell}) \implies \ell \equiv (\frac{d}{\ell}) \pmod F$. ■

Corolário 3.24: *Nas condições da proposição, se* $F > R$ *então* N *é primo.*

Dem: Qualquer fator primo de N deve ser congruente a 1 ou a -1 módulo F, mas, se N é composto, deve ter um fator primo menor ou igual à sua raiz quadrada, que deve, pois, ser igual a $F - 1$. Como $F > \sqrt{N+1}$, $F^2 - 1 > N$, logo $\frac{N}{F-1} < F + 1$, donde o outro fator primo de N também deve ser igual a $F - 1$, e teríamos $N = (F-1)^2 \Rightarrow N + 1 = F^2 - 2F + 2$, que só seria múltiplo de F se F fosse igual a 2, e $F - 1$ igual a 1, absurdo. ■

Proposição 3.25: *Seja* $n > 1$ *um inteiro ímpar. Se para todo fator primo* r *de* $n + 1$ *existem* $P^{(r)}, Q^{(r)}$ *inteiros com* $\mathrm{mdc}(D^{(r)}, n) = 1$ *onde* $D^{(r)} = (P^{(r)})^2 - 4Q^{(r)}$ *tais que a seqüência de Lucas associada* $(U_k^{(r)})$ *satisfaz* $U_{n+1}^{(r)} \equiv 0 \pmod n$ *e* $\mathrm{mdc}(U_{\frac{n+1}{r}}^{(r)}, n) = 1$ *então* n *é primo.*

Dem: Seja ℓ um fator primo de n. Para cada fator primo r de $n+1$ temos que $U_{n+1}^{(r)} \equiv 0 \pmod \ell$ e $U_{\frac{n+1}{r}}^{(r)} \not\equiv 0 \pmod \ell$. Assim, se r^{α_r} é a maior potência de r que divide $n+1$, então r^{α_r} divide $\ell - (\frac{D^{(r)}}{\ell})$, como acima. Em particular, r^{α_r} divide $\ell^2 - 1 = (\ell-1)(\ell+1)$, donde $n+1$ divide $\ell^2 - 1$. Assim, $\ell^2 - 1 \ge n+1$ donde $\ell > \sqrt{n}$, o que implica na primalidade de n pois n não tem nenhum fator primo menor ou igual à sua raiz quadrada. ■

Vamos agora dar outra prova do critério de Lucas-Lehmer usando os resultados anteriores.

Dem: A seqüência de Lucas associada a $P = 2$, $Q = -2$, é dada pela fórmula $U_k = \frac{1}{2\sqrt{3}}((1+\sqrt{3})^k - (1-\sqrt{3})^k)$. Temos $(1+\sqrt{3})^k = \frac{V_k}{2} + U_k\sqrt{3}$, onde $V_k = (1+\sqrt{3})^k + (1-\sqrt{3})^k$. Além disso, $U_{2k} = U_k V_k$ para todo $k \in \mathbb{N}$.

Para $r \geq 1$ temos

$$\begin{aligned} V_{2^r} &= (1+\sqrt{3})^{2^r} + (1-\sqrt{3})^{2^r} = (4+2\sqrt{3})^{2^{r-1}} + (4-2\sqrt{3})^{2^{r-1}} \\ &= 2^{2^{r-1}}((2+\sqrt{3})^{2^{r-1}} + (2-\sqrt{3})^{2^{r-1}}) = 2^{2^{r-1}} S_{r-1} \end{aligned}$$

(onde $S_0 = 4$, $S_{m+1} = S_m^2 - 2$, $\forall m \in \mathbb{N}$). Se $n > 2$ e $M_n = 2^n - 1$ divide S_{n-2} então M_n divide $V_{2^{n-1}}$, logo também divide $U_{M_n+1} = U_{2^n} = U_{2^{n-1}} V_{2^{n-1}}$, e, como $U_{\frac{M_n+1}{2}} = U_{2^{n-1}}$, e $V_k^2 - 12U_k^2 = 4(-2)^k$, segue que $V_{2^{n-1}}^2 - 12U_{2^{n-1}}^2 = 2^{2^{n-1}+2}$, e, se M_n dividisse $U_{\frac{M_n+1}{2}}$, dividiria também $2^{2^{n-1}+2}$, absurdo. Assim, pelo Teorema 3.22, M_n é primo.

Por outro lado, se M_n é primo, como $D = 12$, $(\frac{12}{M_n}) = (\frac{3}{M_n}) = -(\frac{M_n}{3}) = 1$, logo M_n divide $U_{M_n+1} = U_{2^n}$, e, como

$$\begin{aligned} V_{2^{n-1}}^2 &= V_{2^n} + 2(-2)^{2^{n-1}} = V_{2^n} + 2 \cdot 2^{\frac{M_n+1}{2}} \\ &= V_{2^n} + 4 \cdot 2^{\frac{M_n-1}{2}} = V_{2^n} + 4(\frac{2}{M_n}) \equiv V_{2^n} + 4 \pmod{M_n}, \end{aligned}$$

pois $2 \equiv 2^{n+1} \equiv (2^{\frac{n+1}{2}})^2 \pmod{M_n}$ (já sabemos que n deve ser um primo ímpar). Temos $V_{2^n} = (1+\sqrt{3})^{2^n} + (1-\sqrt{3})^{2^n} = (1+\sqrt{3})^{M_n+1} + (1-\sqrt{3})^{M_n+1}$, que é igual a $(1-\sqrt{3})(1+\sqrt{3}) + (1+\sqrt{3})(1-\sqrt{3}) = -4$ em $K = \mathbb{Z}/(M_n)[\sqrt{3}]$ (pois $(\frac{3}{M_n}) = -1$) donde $V_{2^{n-1}}^2 = V_{2^n} + 4 \equiv 0 \pmod{M_n}$ e portanto $M_n \mid V_{2^{n-1}} = 2^{2^{n-2}} S_{n-2}$. Assim, M_n divide S_{n-2}, o que conclui nossa nova demonstração do critério de Lucas-Lehmer. ■

Se N é um primo ímpar e d não é quadrado módulo N, então $K = \mathbb{Z}/(N)[\sqrt{d}]$ é um corpo finito com N^2 elementos e portanto existem inteiros a e b tais que $x = a + b\sqrt{d}$ é uma raiz primitiva de K. Sejam $\overline{x} = a - b\sqrt{d}$ e, para $m \in \mathbb{N}$, $U_m = (x^m - \overline{x}^m)/2b\sqrt{d}$. Temos $U_0 = 0$, $U_1 = 1$ e $U_{m+2} = 2aU_{m+1} - (a^2 - db^2)U_m$ para todo $m \in \mathbb{N}$. Temos ainda $b \neq 0$ em K, senão x pertenceria a $\mathbb{Z}/(M) \subset K$ e $\mathrm{ord}_K\, x$ dividiria $N - 1$. Assim, b e $\sqrt{d}$ são invertíveis em K e, se $P = 2a$, $Q = a^2 - db^2$ então $D = P^2 - 4Q = 4db^2$ satisfaz $(\frac{D}{N}) = -1$. Pela proposição 3.18, $U_{n+1} \equiv 0 \pmod{N}$. Por outro lado, se m é menor que

$N+1$, caso N divida U_m teríamos $x^m = \overline{x}^m$ em K, donde teríamos em K, $(\overline{x}/x)^m = 1$. Pela proposição 3.17, $\overline{x} = x^N$, logo $x^{(N-1)m} = 1$, absurdo, pois $\mathrm{ord}_K\, x = N^2 - 1 = (N-1)(N+1) > (N-1)m$. Isto fornece recíprocas para os resultados desta seção.

Capítulo 4

Aspectos computacionais

No capítulo anterior demonstramos vários critérios de primalidade, Neste capítulo faremos várias considerações quanto ao valor prático deste critério, sendo nosso objetivo dar uma idéia geral do funcionamento dos programas que encontraram os maiores números primos conhecidos. Ao invés de tentarmos acompanhar as fontes da última versão do programa, optaremos inicialmente por nos colocarmos na posição de um programador ou matemático um pouco ingênuo que acaba de aprender que existe este critério e resolveu colocá-lo em prática; veremos assim programas simples que de fato implementam o teste mas nas nossas primeiras tentativas teremos um sucesso bastante relativo. Ao chegarmos ao final do capítulo, entretanto, esperamos ter discutido os principais aspectos matemáticos de uma boa implementação do teste. Veremos que uma das nossas principais preocupações será a de saber multiplicar inteiros rapidamente e os melhores algoritmos para esta tarefa estão baseados na transformada de Fourier discreta. A parte deste capítulo referente a este tema está fortemente baseada no livro de M. Clausen e U. Baum, *Fast Fourier Transforms* ([**CB**]).

Nossos programas são escritos em C e foram testados em um Pentium-Linux, com o compilador `gcc`. Os programas que apresentaremos são pedagógicos e ilustrativos, muito aquém do ideal principalmente em termos de velocidade. Todos os programas podem ser obtidos pela rede; os de nossa autoria estão em `http://www.mat.puc-rio.br/~nicolau/publ/papers/mersenne.tar.gz`.

4.1 Primeiras tentativas

Uma primeira tentativa poderia ser:

Ao tentarmos executar o programa, vimos que ele corretamente disse que $M_2 = 3$, $M_3 = 7$ e $M_5 = 31$ são primos mas incorretamente disse que $M_7 = 127$ é composto! O que aconteceu? Ao mandarmos o programa imprimir os valores de S_n, vimos $4, 14, 194, 37634, 1416317954, -264425470, -1443577854, \ldots$ e fica evidente que algo está muito errado. De fato, o que os computadores chamam de `int` é um elemento de $\mathbb{Z}/(2^N)$ para algum valor de N; no nosso caso, $N = 32$. Como S_n cresce muito rápido, em poucos passos ultrapassamos o limite de 2^N e os valores de s calculados passam a estar errados.

A solução para o problema é fazer todas as contas modulo M_p, já que só precisamos saber no final se S_{p-2} é ou não múltiplo de M_p. Uma versão levemente melhorada do nosso programa seria `ll2.c`; esta versão do programa agora verifica corretamente que $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$ são primos, que $M_{11} = 2047 = 23 \cdot 89$ é composto e que $M_{13} = 8191$ é primo mas afirma incorretamente que $M_{17} = 131071$ é composto. O que ocorre é que apesar de M_{17} ainda ser bem menor do que 2^{32}, o limite de tamanho de `int`s, em contas intermediárias elevamos números na faixa de 0 a 131070 ao quadrado, e isto nos joga fora da margem de bom funcionamento de `int`s.

4.2 Alguns programas usando a biblioteca `gmp`

Isto deve convencer ao leitor que nunca iremos muito longe enquanto não nos livrarmos de limites tão baixos sobre tamanhos de inteiros. Uma idéia seria usar uma biblioteca para inteiros de precisão arbitrária, como `gmp` (GNU MultiPrecision, cujas fontes podem ser obtidas em `www.gnu.org`) ou `giantint` (fontes em `http://www.perfsci.com/free/giantint`). Uma explicação de como funcionam estas bibliotecas está fora dos nossos objetivos; o leitor interessado deve consultar sua documentação. Basta-nos notar que elas permitem usar um tipo de variável novo, chamado `mpz_t` no `gmp` e `giant` no `giantint`, que funciona como um inteiro (e não um elemento de $\mathbb{Z}/(N)$ para algum valor fixo de N) sem limitações de tamanho exceto as impostas pela memória do computador. Note que para testar se M_p é primo pelo critério de Lucas-Lehmer, teremos que fazer comtas modulo M_p; um número módulo M_p ocupa p bits de memória e, levando em conta que talvez precisemos guardar alguns resultados

intermediários, podemos estimar que a memória necessária se p é aproximadamente igual a 10 milhões deve ser de uns 10 MBytes, o que não é muito para os padrões atuais. Note por outro lado que se tentássemos calcular S_{p-2} (e não S_{p-2} modulo M_p) isto excederia em muito a memória de qualquer computador.

Vejamos um programa simples que implementa o teste de Lucas-Lehmer usando a biblioteca `gmp`:

Bem, este programa finalmente funciona! Ele verifica corretamente se M_p é primo ou composto mesmo para valores altos de p. Por exemplo, testamos com ele a primalidade de M_{11213} usando um Pentium 166-Linux, e a resposta certa veio após pouco menos de 6 minutos. Mas se é verdade que este programa está correto, ele pode ser tornado bem mais rápido. As contas no computador são feitas na base 2 mas a redução módulo M_p é feita sem levar em conta o fato de que M_p tem uma expansão na base 2 tão simples. O programa `ll4.c` é uma pequena modificação do anterior que explora estes fatos. Aproveitamos a ocasião para modificar o programa de tal forma que ele teste não apenas a primalidade de *um* número de Mersenne e sim de todos os números de Mersenne em uma faixa dada.

A principal diferença está na parte em que reduzimos módulo M_p: é muito fácil fazer uma divisão com resto de um inteiro n por 2^p, pois o resto n_1 corresponde aos últimos p algarismos na base 2 enquanto o quociente n_2 corresponde aos demais algarismos. Como $2^p \equiv 1 \pmod{M}_p$, podemos trocar $n = 2^p \cdot n_1 + n_2$ por $n_1 + n_2$ sem alterar seu valor módulo M_p e sem sequer calcular o próprio M_p. Esta nova versão do programa demorou aproximadamente 1 minuto e 40 segundos para verificar a primalidade de M_{11213}, 1 hora para verificar a primalidade de M_{44497} e 7 horas para testar todos os expoentes primos até 12000.

Um pequeno programa capaz de encontrar números primos relativamente grandes é nosso exemplo `proth1.c`, que usa o critério de Proth (Corolário 3.9) para procurar primos da forma $h \cdot 2^k + 1$; o programa encontra primos com centenas de algarismos em poucos segundos. Yves Gallot escreveu um programa sério para encontrar primos muito grandes deste tipo[1].

Chegamos no ponto onde já temos programas que funcionam e devemos discutir como torná-los mais rápidos. Voltando ao exemplo do teste de Lucas-Lehmer, a parte que fica fora do `for` é claramente bem simples. Tudo o que vem dentro do `for`, por outro lado, é executado p vezes e portanto é com esta parte que devemos nos preocupar: uma multiplicação (ou um quadrado),

[1] ver `http://perso.wanadoo.fr/yves.gallot/`

algumas adições, subtrações e divisões por 2^p. Já vimos que as divisões por 2^p são simples; adições e subtrações são também rápidas, mesmo usando o método ensinado na escola. Resta a multiplicação, e é aí que nosso programa gasta quase todo seu tempo. Discutiremos no restante deste capítulo como multiplicar rapidamente inteiros com muitos algarismos.

4.3 O algoritmo de multiplicação de Karatsuba

A forma de multiplicar inteiros ensinada na escola é simples e conveniente para inteiros relativamente pequenos, mas vejamos seu custo. Para multiplicar dois inteiros de n algarismos na base d procedemos basicamente a partir da fórmula:

$$(\sum_i a_i d^i)(\sum_j b_j d^j) = \sum_{i,j} a_i b_j d^{i+j} :$$

calculamos (ou olhamos na tabuada) todos os produtos de um algarismo de um dos inteiros com um algarismo do outro, multiplicamos pela potência de d apropriada (o que equivale a acrescentar zeros à direita) e somamos as n^2 parcelas obtidas. Efetuamos no processo n^2 multiplicações e um número comparável de somas; assim, o tempo gasto com este algoritmo é aproximadamente An^2 para alguma constante positiva A. Se isto fosse o melhor que pudéssemos fazer, o tempo para checar a primalidade de M_p seria aproximadamente Ap^3. Existem entretanto outros algoritmos de multiplicação: examinemos primeiro um algoritmo relativamente simples, o algoritmo de Karatsuba, usado pela biblioteca `gmp` (e portanto por nossos programas acima).

Sejam A e B dois inteiros com n algarismos cada um. Se $m = \lceil n/2 \rceil$, podemos escrever $A = A_1 d^m + A_0$, $B = B_1 d^m + B_0$ e $AB = A_1 B_1 d^{2m} + (A_1 B_0 + A_0 B_1) d^m + A_0 B_0$. Pelo algoritmo anterior, calcularíamos os quatro produtos de inteiros com m algarismos. Entretanto, os produtos $A_1 B_0$ e $A_0 B_1$ não são necessários individualmente, e podemos calcular sua soma da seguinte forma:

$$A_1 B_0 + A_0 B_1 = (A_1 - A_0)(B_0 - B_1) + A_1 B_1 + A_0 B_0.$$

Em outras palavras, podemos escrever

$$AB = A_1 B_1 (d^{2m} + d^m) + (A_1 - A_0)(B_0 - B_1) d^m + A_0 B_0 (d^m + 1).$$

Assim, podemos calcular os três coeficientes com apenas três multiplicações (ao invés de quatro) e algumas somas. Mesmo que o número de somas aumente, já

sabemos que somas são rápidas e portanto podemos esperar que este algoritmo represente uma melhora substancial em relação ao anterior.

Mais precisamente, repetimos este processo para diminuirmos o tamanho dos inteiros. Assim, se denotarmos por $f(n)$ o tempo necessário para multiplicar inteiros de n algarismos temos $f(n) \approx 3f(\lceil n/2 \rceil) + An$ e provamos facilmente que

$$f(n) \approx An^{\alpha},$$

onde $\alpha = (\log 3)/(\log 2)$.

4.4 Multiplicação de polinômios usando FFT

Suponha que queiramos multiplicar dois polinômios $P, Q \in \mathbb{C}[x]$, de grau menor do que n, representados pelos seus coeficientes:

$$P(x) = \sum_{0 \le j < n} a_j x^j \qquad = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1},$$
$$Q(x) = \sum_{0 \le j < n} b_j x^j \qquad = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}.$$

O método aprendido na escola exige n^2 multiplicações; o métode de Karatsuba pode ser adaptado para este problema e exige aproximadamente n^{α} multiplicações, com $\alpha = (\log 3)/(\log 2)$. Veremos agora como efetuar esta multiplicação com um número muito menor de operações.

Uma idéia é a de considerar os polinômios como representados não pelos seus coeficientes e sim pelos seus valores em n pontos distintos $\xi_0, \ldots, \xi_{n-1}$. Temos evidentemente $(P \cdot Q)(\xi_j) = P(\xi_j) \cdot Q(\xi_j)$: se o produto PQ tem grau menor do que n então PQ é o único polinômio que assume estes n valores. A dificuldade em usar este método está em calcular os valores de P e Q nos n pontos $\xi_0, \ldots, \xi_{n-1}$ e em recuperar PQ a partir de seu valor nestes mesmos pontos. Se os valores ξ_j forem escolhidos sem critério este método pode acabar sendo mais lento do que os outros que já apresentamos. Veremos que certas escolhas de n e ξ_j tornam o algoritmo rápido: uma das mais simples é tomar n uma potência de 2 e $\xi_j = \omega^j$, onde $\omega = e^{2\pi i/n}$ é uma raiz da unidade de ordem n.

Suponha que $\xi_k = -\xi_j \neq 0$ então as potências pares de ξ_j e ξ_k coincidem, enquanto as potências ímpares diferem pelo sinal. Isto nos permite economizar

multiplicações quando calculamos $P(\xi_j)$ e $P(\xi_k) = P(-\xi_j)$ simultaneamente. Se n é par, podemos escrever

$$P(\xi_j) = P_+(\xi_j^2) + \xi_j P_-(\xi_j^2),$$
$$P(-\xi_j) = P_+(\xi_j^2) - \xi_j P_-(\xi_j^2),$$

onde

$$P_+(x) = \sum_{0 \le j < n/2} a_{2j} x^j,$$
$$P_-(x) = \sum_{0 \le j < n/2} a_{2j+1} x^j,.$$

Ou seja, reduzimos o problema de calcular um polinômio de grau n em dois pontos ao problemas de calcular dois polinômios de grau $n/2$ em um mesmo ponto, seguido de uma multiplicação, uma soma e uma subtração. Se os ξ_j sempre ocorrerem aos pares, com por exemplo $\xi_{j+(n/2)} = -\xi_j$, o cálculo de $P(\xi_0), \ldots, P(\xi_n)$ reduz-se ao cálculo de $P_+(\xi_0^2), \ldots, P_+(\xi_{(n/2)-1}^2)$, $P_-(\xi_0^2), \ldots, P_-(\xi_{(n/2)-1}^2)$ seguido de $3n/2$ operações.

O ideal é que pudéssemos repetir o processo acima, ou seja, que n seja múltiplo de 4 e que também no conjunto $\xi_0^2, \ldots, \xi_{(n/2)-1}^2$ os números ocorressem em pares diferindo apenas por sinal. Reordenando os termos, podemos reformular esta condição como $\xi_{j+(n/4)}^2 = -\xi_j^2$, ou, sem perda de generalidade, como $\xi_{j+(n/4)} = i\xi_j$. Para podermos repetir este processo um número máximo de vezes, devemos tomar n como uma potência de 2 e $\xi_{j+k} = \omega^k \xi_j$, onde $\omega = e^{2\pi i/n}$. Devemos assim tomar $\xi_j = \omega^j \xi_0$ e a escolha $\xi_0 = 1$ parece particularmente simples.

Façamos agora uma estimativa de $T(n)$, o número de operações usadas neste algoritmo para calcular $P(\xi_0), \ldots, P(\xi_n)$. Já vimos que $T(n) = 2T(n/2) + 3n/2$; claramente $T(1) = 0$. Daí temos $T(2) = 3$, $T(4) = 12$ e, por uma indução simples, $T(2^k) = 3k \cdot 2^{k-1}$. Assim, é possível calcular $P(1), \ldots, P(\omega^{n-1})$ muito rápidamente.

Reformulemos este problema na linguagem de álgebra linear. Temos

$$\begin{pmatrix} P(1) \\ P(\omega) \\ P(\omega^2) \\ \vdots \\ P(\omega^{n-1}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega & \omega^2 & \ldots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \ldots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \ldots & \omega^{(n-1)^2} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{pmatrix};$$

a matriz de ordem n e coeficientes ω^{ij}, $0 \leq i,j < n$, é chamada de DFT_n, a *transformada de Fourier discreta*. O que aprendemos nos parágrafos acima foi a multiplicar DFT_n por um vetor rapidamente (pelo menos quando n é uma potência de 2). Em termos algébricos, aprendemos a escrever DFT_n como um produto de $\log_2 n$ matrizes esparsas cujos coeficientes não nulos são potências de ω; cada matriz esparsa correspondendo a uma etapa do algoritmo FFT.

Falta aprender a recuperar os coeficientes de um polinômio P a partir de

$$P(1), \ldots, P(\omega^{n-1}),$$

ou seja, a multiplicar $(\mathsf{DFT}_n)^{-1}$ por um vetor. Mas para isto basta observar que

$$(\mathsf{DFT}_n)^2 = n \cdot \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \end{pmatrix},$$

pois o coeficiente (i,k) de $(\mathsf{DFT}_n)^2$ é

$$\sum_j \omega^{ij}\omega^{jk} = \sum_j \omega^{(i+k)j}$$

que é igual a n se $i + k \equiv 0 \pmod{n}$ e 0 caso contrário pois

$$\omega^{\ell n} - 1 = (\omega^\ell - 1)\sum_j \omega^{\ell j}.$$

Assim, o coeficiente (i,j) de $(\mathsf{DFT}_n)^{-1}$ é $(1/n)\omega^{-ij}$ e este processo de FFT inversa (ou interpolação) é tão fácil e rápido quanto FFT (ou evaluação). Temos portanto um algoritmo para multiplicar polinômios de grau n fazendo aproximadamente $Cn\log n$ operações (onde C é uma constante positiva).

Reproduzimos abaixo o pseudo-código de [**CB**] para este algoritmo:

Input: O comprimento n (uma potência de 2); uma raiz primitiva da unidade ω de ordem n; um vetor $(a_0, \ldots, a_{n-1})$ de coeficientes complexos.

Output: O vetor $(A_0, \ldots, A_{n-1})^t = (\mathsf{DFT}_n)(a_0, \ldots, a_{n-1})^t$.

```
procedure FFT(n, ω, a_0, a_1, ..., a_{n-1}; A_0, A_1, ..., A_{n-1});
begin
```

```
    if n = 1 then
      A_0 = a_0;
    else
      FFT(n/2, ω^2, a_0, a_2, ..., a_{n-2}; E_0, ..., E_{n/2-1});
      FFT(n/2, ω^2, a_1, a_3, ..., a_{n-1}; O_0, ..., O_{n/2-1});
      for k = 0 to n/2 - 1 do
        A_k = E_k + ω^k O_k;
        A_{k+n/2} = E_k - ω^k O_k;
end
```

Até agora consideramos polinômios com coeficientes em $\mathbb{C}$ mas o leitor atento já deve ter percebido que podemos usar o mesmo algoritmo para multiplicar polinômios sobre qualquer corpo K desde que exista em K um elemento ω que seja uma raiz da unidade de ordem n. Um exemplo de corpo onde existe um tal ω é $\mathbb{Z}/(p)$ se $p \equiv 1 \pmod{n}$. Na verdade não é sequer necessário que os coeficientes estejam em um corpo: podemos trabalhar sobre qualquer anel A onde exista ω com as seguintes propriedades:

1. $\omega^n = 1$,
2. n é inversível em A,
3. se $0 < \ell < n$ então $\omega^\ell - 1$ é inversível em A.

Na próxima seção veremos uma situação onde será interessante trabalhar com $A = \mathbb{Z}/(2^K + 1)$.

Lembramos que este algoritmo calcula corretamente o produto dos polinômios P e Q desde que este produto tenha grau menor do que n. Mais geralmente, estaremos encontrando o único polinômio de grau menor que n que coincide com PQ em $\xi_0, \xi_1, \ldots, \xi_{n-1}$. Como estamos tomando sempre $\xi_j = \omega^j \xi_0$ temos

$$(x - \xi_0)(x - \xi_1) \cdots (x - \xi_{n-1}) = x^n - \xi_0^n$$

e nosso algoritmo calcula $PQ \bmod (x^n - \xi_0^n)$.

4.5 Multiplicação de inteiros usando FFT

Quando escrevemos um inteiro a na base d,

$$a = \sum_k a_k d_k,$$

podemos pensar que estamos escrevendo

$$a = P(d), \quad P(x) = \sum_k a_k x^k.$$

Se desejarmos calcular ab onde

$$b = Q(d), \quad Q(x) = \sum_k b_k x^k$$

podemos usar o algoritmo da seção anterior para calcular os coeficientes c_k do produto

$$(PQ)(x) = \sum_k c_k x^k, \quad c_k = \sum_j a_j b_{k-j}$$

e temos $ab = (PQ)(d)$. Os c_k em geral não serão algarismos aceitáveis para uma expansão na base d do inteiro ab mas isto pode facilmente ser corrigido: escrevemos $c'_0 = c_0 + de_0$, $c'_1 = c_1 - e_0 + de_1$, ..., $c'_k = c_k - e_{k-1} + de_k$, ..., onde a cada passo tomamos c'_k como sendo um algarismo aceitável. Ao final, teremos

$$ab = \sum_k c'_k d_k,$$

a expansão de ab na base d.

A dificuldade maior reside no fato que as contas descritas na seção anterior envolvem números complexos, e as partes real e imaginária destes números complexos são irracionais. Uma alternativa é fazer as contas usando variáveis do tipo double; teremos inevitavelmente erros de truncamento mas o fato de sabermos que a resposta final é um inteiro nos dá uma oportunidade de corrigir estes erros. É claro que precisamos ter o cuidado de evitar que os erros de truncamento somem mais do que $0,5$: neste caso acabaríamos arredondando a resposta final para o inteiro errado. Esta possibilidade desastrosa pode ser evitada tomando d pequeno (e portanto grau grande, o que implica em uma transformada de Fourier de comprimento maior); também ajuda muito tomar o conjunto dos algarismos aceitáveis simétrico em relação ao zero, pois assim os produtos $a_j b_{k-j}$ serão menores e terão sinais diferentes, o que evita que os coeficientes c_k sejam grandes demais. Mesmo para inteiros bem maiores do que o maior primo conhecido existem valores de d que garantem o bom funcionamento deste método, um dos mais rápidos para multiplicar inteiros grandes (em parte porque a maioria dos computadores é capaz de multiplicar doubles com grande rapidez). Por isso, ele é usado pelo programa mprime-prime95, que encontrou os últimos 4 primos de Mersenne. Escrevemos um

pequeno programa que usa o critério de Lucas-Lehmer para testar a primalidade de M_p e que multiplica usando FFT: as funções FFT estão em `fft.c` e o programa principal em `fftest2.c`.

Uma segunda alternativa é escolher um primo p e fazer a multiplicação de polinômios considerando os coeficientes como elementos de $\mathbb{Z}/(p)$. Para recuperarmos os verdadeiros coeficientes do produto (que são inteiros), precisamos ter o cuidado de garantir que $|c_k| < p/2$ onde $c_k = \sum a_j b_{k-j}$. Um primo usado em alguns programas [2] é $p = 2^{64} - 2^{32} + 1$, que tem aliás várias propriedades especiais que o tornam particularmente apropriado para nossa tarefa. Com este valor de p, como $2^{32}|p-1$, podemos fazer FFTs de comprimento 2^{32} com $d = 2^{16}$, o que permite (em princípio) multiplicar inteiros de módulo menor do que $2^{16\cdot 2^{32}-1}$, ou seja, inteiros com alguns *bilhões* de algarismos; o simples armazenamento de um tal inteiro exige memória maior do que a que tem a maioria dos computadores atuais.

Mas estas alternativas, apesar de computacionalmente atraentes, não satisfazem ao matemático puro pois funcionam para inteiros menores do que um certo tamanho fixo (apesar de muito grande). A segunda alternativa apresentada acima pode ser levada adiante tomando primos cada vez maiores, mas não será fácil provar que existem sempre primos com as propriedades desejadas. Veremos agora como multiplicar inteiros de tamanho arbitrário em tempo baixo fazendo as contas não em $\mathbb{Z}/(p)$, mas em $\mathbb{Z}/(2^K+1)$ (mesmo 2^K+1 não sendo primo) e assim evitaremos esta dificuldade. Uma outra vantagem deste método é que será muito fácil multiplicar por potências de ω (assim tornando rápidas as FFTs).

Mais precisamente, mostraremos como multiplicar inteiros (dados por suas expansões binárias) módulo 2^N+1; esta é a versão simplificada de Schönhage de um algoritmo devido a Schönhage e Strassen. Se N for tomado suficientemente grande este algoritmo multiplica inteiros. Consideraremos apenas valores de $N \geq 320$ da forma

$$N = \nu \cdot 2^n, \quad n-1 \leq \nu \leq 2n, \quad n \geq 4;$$

estes valores de N serão chamados de *aceitáveis*. Supomos que já sabemos multiplicar módulo 2^K+1, onde $K = \kappa \cdot 2^k < N$ também é um valor aceitável (a ser escolhido).

[2] Em particular no StrongARM, veja **http://www.axis.demon.co.uk/armprime/**

Para usar a multiplicação de polinômios, escrevemos os inteiros a e b a serem multiplicados na base d, i.e.,

$$a = \sum_{0 \le i < 2^m - 1} a_i d^i, \quad b = \sum_{0 \le j < 2^m - 1} b_j d^j, \quad 0 \le a_i, b_j < d,$$

onde $m = \lfloor n/2 \rfloor + 1$ e $d = 2^{N/2^m}$. Temos $d^{2^m} = 2^N \equiv -1 \pmod{2^N + 1}$. Assim, podemos escrever $c \equiv ab \pmod{2^N + 1}$ com

$$c = \sum_{0 \le \mu < 2^m - 1} b_\mu d^\mu, \quad c_\mu = \sum_{i+j=\mu} a_i b_j - \sum_{i+j=\mu+2^m} a_i b_j.$$

Pela seção anterior e por indução, sabemos efetuar estas contas módulo $2^K + 1$ mas novamente precisamos do valor de cada c_μ como inteiro, ou seja, precisamos escolher K de tal forma que possamos garantir que $|c_\mu| \le 2^{K-1}$. É fácil verificar que podemos escolher $\kappa = \lceil (\nu + 1)/2 \rceil$ e $k = \lceil n/2 \rceil + 1$; observe que $K = \kappa \cdot 2^k$ é de fato aceitável.

Sejam $\tilde{\omega} = 2^{K/2^m}$ e $\omega = \tilde{\omega}^2$. Como $\omega^{2^{m-1}} \equiv -1 \pmod{2^K + 1}$ temos que ω é uma raiz da unidade em $\mathbb{Z}/(2^K + 1)$ de ordem 2^m: este valor de ω pode ser usado para fazer FFT como na seção anterior; temos

$$c_\mu \equiv \tilde{\omega}^{-\mu} \sum_{i+j \equiv \mu \pmod{2^m}} (\tilde{\omega}^i a_i)(\tilde{\omega}^j b_j) \pmod{2^K + 1}.$$

Note que podemos efetuar tanto FFT quanto FFT inversa pois 2^m e $\omega^i - 1$ são inversíveis módulo $2^K + 1$ (o que deixamos como exercício).

Falta apenas estimar o número de operações gasto por este algoritmo; note que por operação aqui queremos dizer uma operação sobre bits. Em todo o algoritmo, efetuamos duas FFTs de comprimento 2^m sobre $\mathbb{Z}/(2^K + 1)$, 2^m multiplicações ponto a ponto (também sobre $\mathbb{Z}/(2^K + 1)$) e uma FFT inversa de comprimento 2^m. Observe que como ω é uma potência de 2, as multiplicações por potências de ω que ocorrem nas FFTs são rápidas pois são apenas translações dos algarismos; mais precisamente, exigem no máximo CK operações cada uma (para alguma constante positiva C). Assim, cada FFT exige no máximo $Cm \cdot 2^m K$ operações. O número total $T(N)$ de operações satisfaz assim a recorrência

$$T(N) \le 2^m T(K) + Cm \cdot 2^m K$$

donde podemos demonstrar que, para alguma constante positiva C,

$$T(n) \le CN \log N \log\log N.$$

4.6 A complexidade das operações aritméticas

Vimos na seção anterior que o número de operações (e portanto o tempo) necessário para multiplicar inteiros de N algarismos é aproximadamente (a menos de um fator constante) $N \log N \log\log N$ se utilizarmos um dos algoritmos descritos. Não se conhece nenhum algoritmo que seja assintóticamente mais rápido mas também não se sabe demonstrar que não existe um tal algoritmo. Mostraremos nesta seção que o tempo necessário para realizar qualquer uma das operações abaixo é assintoticamente o mesmo (isto é, difere por uma constante multiplicativa). Note que adições e subtrações são mais rápidas e desprezaremos o tempo exigido por essas operações.

1. Multiplicar inteiros de N algarismos.
2. Elevar ao quadrado um inteiro de N algarismos.
3. Inverter, ou seja, encontrar os primeiros $2N$ algarismos depois da vírgula de $1/n$, onde n tem N algarismos, ou ainda, calcular $\lfloor Q^{2N}/n \rfloor$ (se trabalharmos na base Q).
4. Fazer a divisão com resto de dois inteiros de N algarismos, i.e., dados n e m encontrar q e r com $n = qm + r$, $0 \leq r < m$.

Estas operações podem ser reduzidas uma às outras com a mesma ordem de grandeza de tempo, i.e., multiplicando o tempo necessário por uma constante. Faremos isto da seguinte forma:

(a) Quem sabe multiplicar sabe elevar ao quadrado.

(b) Quem sabe elevar ao quadrado sabe multiplicar.

(c) Quem sabe multiplicar sabe inverter.

(d) Quem sabe inverter sabe elevar ao quadrado.

(e) Quem sabe multiplicar e inverter sabe dividir com resto.

(f) Quem sabe dividir com resto sabe inverter.

Os itens (a), (e) e (f) são triviais. O item (b) segue de $mn = ((m+n)^2 - (m-n)^2)/4$. O item (d) segue de $x^2 = (x^{-1}-(x+1)^{-1})^{-1}-x$. O item (c) segue do fato que se $x = n/Q^N \in (1/Q, 1]$ (x um número real dado com uma certa precisão) e se $y \in [1, Q)$ é uma aproximação para $1/x$ com k casas de precisão então $y' = y(2 - xy)$ é uma aproximação para $1/x$ com aproximadamente $2k$ casas de precisão. De fato temos $y' - 1/x = -x(y - 1/x)^2$ donde $|y' - 1/x| \leq |y - 1/x|^2$. Este algoritmo pode ser visto como uma aplicação do método de Newton para a função $f(t) = -x + 1/t$. Note que as primeiras aproximações para $1/x$ podem ser calculadas com poucos algarismos de precisão, donde as primeiras multiplicações podem ser feitas com poucos algarismos; isto garante que o tempo total para obter N algarismos de $1/x$ é comparável ao tempo de uma multiplicação de inteiros com N algarismos.

4.7 Tabelas

Nesta última seção apresentaremos algumas tabelas indicando os maiores primos conhecidos em março de 2008.

Os dez maiores primos de Mersenne conhecidos

Primo	Nº de dígitos	Descobridores	Data
$2^{32582657}-1$	9808358	Cooper, Boone, GIMPS et al.	2006
$2^{30402457}-1$	9152052	Cooper, Boone, GIMPS et al.	2005
$2^{25964951}-1$	7816230	Nowak, GIMPS et. al.	2005
$2^{24036583}-1$	7235733	Findley, GIMPS et al.	2004
$2^{20996011}-1$	6320430	Shafer, GIMPS et al.	2003
$2^{13466917}-1$	4053946	Cameron, Woltman, Kurowski (GIMPS)	2001
$2^{6972593}-1$	2098960	Hajratwala, Woltman, Kurowski (GIMPS)	1999
$2^{3021377}-1$	909526	Clarkson, Woltman, Kurowski (GIMPS)	1998
$2^{2976221}-1$	895932	Spence, Woltman (GIMPS)	1997
$2^{1398269}-1$	420921	Armengaud, Woltman (GIMPS)	1996

Lembramos que quando p e $p+2$ são ambos primos, dizemos que eles são *primos gêmeos*.

Os dez maiores pares de primos gêmeos conhecidos

Primo	Dígitos	Descobridores	Data
$2003663613 \cdot 2^{195000} \pm 1$	58711	Vautier, McKibbon, Gribenko, NewPGen, PrimeGrid, TPS, LLR	2007
$194772106074315 \cdot 2^{171960} \pm 1$	51780	Jarai_Z, Farkas, Csajbok, Kasza, Jarai	2007
$100314512544015 \cdot 2^{171960} \pm 1$	51780	Jarai_Z, Farkas, Csajbok, Kasza, Jarai	2006
$16869987339975 \cdot 2^{171960} \pm 1$	51779	Jarai_Z, Farkas, Csajbok, Kasza, Jarai	2005
$33218925 \cdot 2^{169690} \pm 1$	51090	Papp, Proth.exe	2002
$60194061 \cdot 2^{114689} \pm 1$	34533	Underbakke, TwinGen, PRP, Proth.exe	2002
$1765199373 \cdot 2^{107520} \pm 1$	32376	McElhatton, Proth.exe	2002
$318032361 \cdot 2^{107001} \pm 1$	32220	Underbakke, Carmody, PrimeForm	2001
$1046619117 \cdot 2^{100000} \pm 1$	30113	Barnes, NewPGen, LLR	2007
$1807318575 \cdot 2^{98305} \pm 1$	29603	Underbakke, Carmody, Gallot	2001

Seja $n\#$, chamado o *primorial* de n, o produto de todos os números primos menores ou iguais a n. Usamos também a notação $n!_k = n!!\ldots!!$, com k pontos de exclamação, para o produto $n(n-k)(n-2k)\ldots$ dos inteiros positivos menores ou iguais a n e côngruos a n módulo k. Um primo da forma $n\# \pm 1$ é chamado *primorial* e um primo da forma $n!!\ldots!! \pm 1$ é chamado *multifatorial*.

Os dez maiores primos multifatoriais e primoriais conhecidos

Primo	Nº de dígitos	Descobridores	Data
$392113\# + 1$	169966	HEUER, PrimeForm	2001
$366439\# + 1$	158936	HEUER, PrimeForm	2001
$95493!_3 + 1$	144697	Harvey, MultiSieve, MultiF, OpenPFGW	2006
$34790! - 1$	142891	Marchal, Carmody, Kuosa, PrimeForm	2002
$80069!_3 + 1$	119284	Harvey, MultiSieve, MultiF, OpenPFGW	2006
$52608!_2 + 1$	112762	DavisK, MultiSieve, MultiF, OpenPFGW	2003
$242893!_{11} - 1$	109330	DavisK, MultiSieve, MultiF, OpenPFGW	2004
$26951! + 1$	107707	DavisK, Kuosa, PrimeForm	2002
$225562!_{11} + 1$	100870	Harvey, MultiSieve, MultiF, OpenPFGW	2006
$21480! - 1$	83727	DavisK, Kuosa, PrimeForm	2001

Lembramos que p é dito um primo de Sophie Germain se $2p + 1$ também é primo e que M_p é composto para estes valores de p se $p \equiv 3 \pmod 4$. Este nome é usado porque Sophie Germain provou o primeiro caso do último teorema de Fermat (recentemente demonstrado completamente por Wiles) para primos p desta forma.

Os dez maiores primos de Sophie Germain conhecidos

Primo	Dígitos	Descobridores	Data
$48047305725 \cdot 2^{172403} - 1$	51910	Underbakke, TwinGen, LLR	2007
$137211941292195 \cdot 2^{171960} - 1$	51780	Jarai_Z, Farkas, Csajbok, Kasza, Jarai	2006
$7068555 \cdot 2^{121301} - 1$	36523	Minovic, TwinGen, LLR	2005
$2540041185 \cdot 2^{114729} - 1$	34547	Underbakke, TwinGen, PRP, Proth.exe	2003
$1124044292325 \cdot 2^{107999} - 1$	32523	Underbakke, TwinGen, LLR	2006
$112886032245 \cdot 2^{108000} - 1$	32523	Underbakke, TwinGen, LLR	2006
$18912879 \cdot 2^{98395} - 1$	29628	Angel, Jobling, Augustin, NewPGen, OpenPFGW	2002
$10495740081 \cdot 2^{83125} - 1$	25034	Underbakke, TwinGen, LLR	2006
$61078155 \cdot 2^{82002} - 1$	24693	Underbakke, TwinGen, LLR	2006
$1213822389 \cdot 2^{81131} - 1$	24432	Angel, Jobling, Augustin, NewPGen, Proth.exe	2002

O maior primo conhecido ao longo da história

Primo	Nº de dígitos	Data	Descobridores
$2^{17}-1$	6	1588	Cataldi
$2^{19}-1$	6	1588	Cataldi
$2^{31}-1$	10	1772	Euler
999999000001	12	1851	Loof
$(2^{59}-1)/179951$	13	1867	Landry
$(2^{53}+1)/(3\cdot 107)$	14	1867	Landry
$2^{127}-1$	39	1876	Lucas
$(2^{148}+1)/17$	44	1951	Ferrier
$180(2^{127}-1)^2+1$	79	1951	Miller & Wheeler
$2^{521}-1$	157	1952	Robinson
$2^{607}-1$	183	1952	Robinson
$2^{1279}-1$	386	1952	Robinson
$2^{2203}-1$	664	1952	Robinson
$2^{2281}-1$	687	1952	Robinson
$2^{3217}-1$	969	1957	Riesel
$2^{4423}-1$	1332	1961	Hurwitz
$2^{9689}-1$	2917	1963	Gillies
$2^{9941}-1$	2993	1963	Gillies
$2^{11213}-1$	3376	1963	Gillies
$2^{19937}-1$	6002	1971	Tuckerman
$2^{21701}-1$	6533	1978	Noll & Nickel
$2^{23209}-1$	6987	1979	Noll
$2^{44497}-1$	13395	1979	Nelson & Slowinski
$2^{86243}-1$	25962	1982	Slowinski
$2^{132049}-1$	39751	1983	Slowinski
$2^{216091}-1$	65050	1985	Slowinski
$391581\cdot 2^{216193}-1$	65087	1989	Amdahl Six
$2^{756839}-1$	227832	1992	Slowinski & Gage
$2^{859433}-1$	258716	1994	Slowinski & Gage
$2^{1257787}-1$	378632	1996	Slowinski & Gage
$2^{1398269}-1$	420921	1996	Armengaud, Woltman, et al. [GIMPS]

O maior primo conhecido ao longo da história (Continuação)

Primo	Nº de dígitos	Data	Descobridores
$2^{2976221}-1$	895932	1997	Spence, Woltman, et al. [GIMPS]
$2^{3021377}-1$	909526	1998	Clarkson, Woltman, Kurowski, et al. [GIMPS, PrimeNet]
$2^{6972593}-1$	2098960	1999	Hajratwala, Woltman, Kurowski, et al. [GIMPS, PrimeNet]
$2^{13466917}-1$	4053946	2001	Cameron, Woltman, Kurowski, et al. [GIMPS, PrimeNet]
$2^{20996011}-1$	6320430	2003	Shafer, GIMPS et al.
$2^{24036583}-1$	7235733	2004	Findley, GIMPS et al.
$2^{25964951}-1$	7816230	2005	Nowak, GIMPS et. al.
$2^{30402457}-1$	9152052	2005	Cooper, Boone, GIMPS et al.
$2^{32582657}-1$	9808358	2006	Cooper, Boone, GIMPS et al.

Os cem maiores primos conhecidos (em março de 2008)

	Primo	Dígitos	Data	Comentário
1	$2^{32582657}-1$	9808358	2006	Mersenne 44
2	$2^{30402457}-1$	9152052	2005	Mersenne 43
3	$2^{25964951}-1$	7816230	2005	Mersenne 42
4	$2^{24036583}-1$	7235733	2004	Mersenne 41
5	$2^{20996011}-1$	6320430	2003	Mersenne 40
6	$2^{13466917}-1$	4053946	2001	Mersenne 39
7	$19249\cdot 2^{13018586}+1$	3918990	2007	Seventeen or Bust 10
8	$27653\cdot 2^{9167433}+1$	2759677	2005	Seventeen or Bust 8
9	$28433\cdot 2^{7830457}+1$	2357207	2004	Seventeen or Bust 7
10	$33661\cdot 2^{7031232}+1$	2116617	2007	Seventeen or Bust 11
11	$2^{6972593}-1$	2098960	1999	Mersenne 38
12	$5359\cdot 2^{5054502}+1$	1521561	2003	Seventeen or Bust 6
13	$24518^{262144}+1$	1150678	2008	Fermat Generalizado
14	$938237\cdot 2^{3752950}-1$	1129757	2007	Woodall
15	$3139\cdot 2^{3321905}-1$	999997	2008	
16	$4847\cdot 2^{3321063}+1$	999744	2005	Seventeen or Bust 9
17	$3\cdot 2^{3136255}-1$	944108	2007	
18	$2^{3021377}-1$	909526	1998	Mersenne 37
19	$7\cdot 2^{3015762}+1$	907836	2008	
20	$2^{2976221}-1$	895932	1997	Mersenne 36
21	$222361\cdot 2^{2854840}+1$	859398	2006	
22	$1372930^{131072}+1$	804474	2003	Fermat Generalizado
23	$1361244^{131072}+1$	803988	2004	Fermat Generalizado
24	$1176694^{131072}+1$	795695	2003	Fermat Generalizado
25	$342673\cdot 2^{2639439}-1$	794556	2007	
26	$572186^{131072}+1$	754652	2004	Fermat Generalizado
27	$3\cdot 2^{2478785}+1$	746190	2003	
28	$26773\cdot 2^{2465343}-1$	742147	2006	
29	$737\cdot 2^{2382804}-1$	717299	2007	
30	$1183953\cdot 2^{2367907}-1$	712818	2007	Woodall
31	$275293\cdot 2^{2335007}-1$	702913	2006	
32	$3\cdot 2^{2312734}-1$	696203	2005	
33	$450457\cdot 2^{2307905}-1$	694755	2006	
34	$130816^{131072}+1$	670651	2003	Fermat Generalizado
35	$19\cdot 2^{2206266}+1$	664154	2006	
36	$114487\cdot 2^{2198389}-1$	661787	2006	
37	$196597\cdot 2^{2178109}-1$	655682	2006	

Os cem maiores primos conhecidos (Continuação)

	Primo	Dígitos	Data	Comentário
38	$7 \cdot 2^{2167800} + 1$	652574	2007	
39	$3 \cdot 2^{2145353} + 1$	645817	2003	
40	$7 \cdot 2^{2139912} + 1$	644179	2007	
41	$62722^{131072} + 1$	628808	2003	Fermat Generalizado
42	$121 \cdot 2^{2033941} - 1$	612280	2006	
43	$251749 \cdot 2^{2013995} - 1$	606279	2007	Woodall
44	$467917 \cdot 2^{1993429} - 1$	600088	2005	
45	$137137 \cdot 2^{1993201} - 1$	600019	2007	
46	$17 \cdot 2^{1990299} + 1$	599141	2006	
47	$121 \cdot 2^{1954243} - 1$	588288	2006	
48	$214519 \cdot 2^{1929114} + 1$	580727	2006	
49	$345067 \cdot 2^{1876573} - 1$	564911	2005	
50	$13 \cdot 2^{1861732} + 1$	560439	2005	
51	$137 \cdot 2^{1849238} - 1$	556679	2007	
52	$3 \cdot 2^{1832496} + 1$	551637	2007	
53	$21 \cdot 2^{1830919} + 1$	551163	2004	
54	$417643 \cdot 2^{1800787} - 1$	542097	2005	
55	$357659 \cdot 2^{1779748} - 1$	535764	2005	
56	$5 \cdot 2^{1777515} + 1$	535087	2005	
57	$253 \cdot 2^{1722623} - 1$	518564	2007	
58	$121 \cdot 2^{1695499} - 1$	510399	2005	
59	$15 \cdot 2^{1667744} + 1$	502043	2007	
60	$149183 \cdot 2^{1666957} + 1$	501810	2005	
61	$469949 \cdot 2^{1649228} - 1$	496473	2007	
62	$81 \cdot 2^{1606848} + 1$	483712	2007	Fermat Generalizado
63	$15 \cdot 2^{1597510} + 1$	480900	2006	
64	$58753 \cdot 2^{1594323} - 1$	479944	2006	
65	$737 \cdot 2^{1592724} - 1$	479461	2006	
66	$110413 \cdot 2^{1591999} - 1$	479245	2005	
67	$1179 \cdot 2^{1591362} + 1$	479051	2006	
68	$121 \cdot 2^{1589157} - 1$	478387	2005	
69	$19502212^{65536} + 1$	477763	2005	Fermat Generalizado
70	$17684828^{65536} + 1$	474979	2007	Fermat Generalizado

Os cem maiores primos conhecidos (Continuação)

	Primo	Dígitos	Data	Comentário
71	$17655444^{65536}+1$	474932	2007	Fermat Generalizado
72	$17629398^{65536}+1$	474890	2007	Fermat Generalizado
73	$29\cdot 2^{1574753}+1$	474050	2008	
74	$139\cdot 2^{1567874}+1$	471980	2006	
75	$81\cdot 2^{1544545}+1$	464957	2007	
76	$234847\cdot 2^{1535589}-1$	462264	2005	
77	$121\cdot 2^{1526097}-1$	459404	2005	
78	$13\cdot 2^{1499876}+1$	451509	2004	
79	$7\cdot 2^{1491852}+1$	449094	2005	
80	$2232007\cdot 2^{1490605}-1$	448724	2003	
81	$29\cdot 2^{1478344}-1$	445028	2005	
82	$27\cdot 2^{1476347}+1$	444427	2005	
83	$325627\cdot 2^{1472117}-1$	443157	2005	
84	$1467763\cdot 2^{1467763}-1$	441847	2007	Woodall
85	$77\cdot 2^{1467554}-1$	441780	2006	
86	$23\cdot 2^{1448461}+1$	436032	2008	
87	$21\cdot 2^{1421741}+1$	427989	2005	
88	$15\cdot 2^{1418605}+1$	427044	2006	
89	$29\cdot 2^{1416873}+1$	426523	2007	
90	$149797\cdot 2^{1414137}-1$	425703	2005	
91	$127\cdot 2^{1398889}-1$	421110	2008	
92	$1564347\cdot 2^{1398269}-1$	420928	2008	
93	$2^{1398269}-1$	420921	1996	Mersenne 35
94	$192089\cdot 2^{1395688}-1$	420150	2004	
95	$17\cdot 2^{1388355}+1$	417938	2005	
96	$15\cdot 2^{1368428}+1$	411940	2006	
97	$241489\cdot 2^{1365062}+1$	410930	2005	
98	$1828502^{65536}+1$	410393	2005	Fermat Generalizado
99	$35\cdot 2^{1357881}+1$	408765	2006	
100	$338707\cdot 2^{1354830}+1$	407850	2005	Cullen

Obs: um primo é dito de *Cullen* se é da forma $n\cdot 2^n+1$, de *Woodall* se é da forma $n\cdot 2^n-1$ e *Fermat generalizado* se é da forma $a^{2^n}+1$. Comentários do tipo "Seventeen or Bust m" referem-se ao m-ésimo primo encontrado pelo projeto Seventeen or Bust (ver apêndice 2 do capítulo 3).

Referências

[**AGP**] W. R. Alford, A. Granville e C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math., 140 (1994) 703-722.

[**AKS**] M. Agrawal, N. Kayal e N. Saxena, *PRIMES is in* P, Annals of Math., 160, no. 2 (2004), pp. 781-793 (ver também `http://www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf`).

[**AMM**] A. Arbieto, C. Matheus, C. G. Moreira, *Aspectos Ergódicos da Teoria dos Números*, 26º Colóquio Brasileiro de Matemática, IMPA, 2007.

[**APR**] L. M. Adleman, C. Pomerance e R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. Math. (2) 117 (1983) 173-206.

[**Bach**] Eric Bach, *Explicit bounds for primality testing and related problems*, Math. of Comp. 55, 1990, pp. 355-380.

[**BCR**] R. P. Brent, G. L. Cohen e H. J. J. te Riele, *Improved techniques for lower bounds for odd perfect numbers*, Math. Comp., 57 (1991) 857-868 (MR 92c:11004).

[**BLS**] J. Brillhart, D. H. Lehmer e J. L. Selfridge, *New primality criteria and factorizations of* $2m \pm 1$, Math. Comp., 29 (1975) 620-647.

[**Bruce**] J. W. Bruce, *A really trivial proof of the Lucas-Lehmer test*, Amer. Math. Monthly, April (1993) 370-371.

[**Cipolla**] M. Cipolla, *Sui numeri composti* P, *che verificano la congruenza di Fermat* $a^{P-1} \equiv 1 \pmod{P}$, Annali di Matematica, (3), 9, 1904, 139-160.

[**CB**] M. Clausen e U. Baum, *Fast Fourier Transforms*, BI-Wiss.-Verl., 1993.

[**CF**] R. Crandall e B. Fagin, *Discrete weighted transforms and large-integer arithmetic*, Math. Comp., 62:205 (1994) 305-324.

[**Co**] S. C. Coutinho, *Primalidade em Tempo Polinomial*, SBM, 2004.

[**Erdös**] Paul Erdös, *On a new method in elementary number theory which leads to an elementary proof of the prime number theorem*, Proc. Nat. Acad. Sci. (Washington) 35 (1949) 374-384.

[**EP**] Paul Erdös e Carl Pomerance, *On the number of false witnesses for a composite number*, Math. Comp., 46 (1986) 259-279.

[**GK**] S. Goldwasser e J. Kilian, *Almost all primes can be quickly certified*, Proc. 18th STOC (Berkeley, May 28-30, 1986), ACM, New York, 1986, 316-329.

[**GPY1**] D. A. Goldston, J. Pintz, C. Y. Yıldırım, *Primes in Tuples I*, `http://arxiv.org/abs/math.NT/0508185` (a ser publicado em Annals of Math.).

[**GPY2**] D. A. Goldston, J. Pintz, C. Y. Yıldırım, *Primes in Tuples II*, `http://arxiv.org/abs/0710.2728`

[**GT**] Ben Green, Terence Tao, The primes contain aribtrarily long arithmetic progressions, Annals of Math., vol. 167, no. 2 (2008) 481-548 (ver também `http://arxiv.org/abs/math.NT/0404188`).

[**Guy**] Richard K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, New York, 1994 (QA241.G87, ISBN 3-540-94289-0).

[**HW**] G. H. Hardy e E. M. Wright, *An Introduction to the Theory of Numbers 5e*, Oxford University Press, 1979.

[**KP**] Su Hee Kim e Carl Pomerance, *The probability that a random probable prime is composite*, Math. Comp., 53:188 (1989) 721-741.

[**Lehmer**] Derrick H. Lehmer, *An extended theory of Lucas' functions*, Ann. Math. 31 (1930) 419-448. Reprinted in *Selected Papers* (ed. D. McCarthy), Vol 1, Ch. Babbage Res. Center, St. Pierre, Manitoba Canada, 11-48, 1981.

[**Lucas**] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math., 1, 1878, 184-240 e 289-321.

[**Maier**] H. Maier, *Primes in short intervals*, Michigan math. J., 32 (1985) 221-225.

[**Mills**] W. H. Mills, *A prime representing function*, Bull. Amer. Math. Soc., 53 604.

[**Mollin**] R. A. Mollin, *Prime-producing polynomials*, Amer. Math. Monthly 104 (June-July 1997) 529-544.

[**Pintz**] János Pintz, *Very large gaps between consecutive primes*, J. Number Theory 63 (1997), no. 2, 286-301.

[**PSW**] C. Pomerance, J. L. Selfridge e S. S. Wagstaff Jr., *The pseudoprimes to 25.109*, Math. Comp., 35 (1980) 1003-1026.

[**Pomerance**] C. Pomerance, *A new lower bound for the pseudoprimes counting function*, Illinois J. Math, 26, 1982, 4-9.

[**Ribenboim95**] P. Ribenboim, *The New Book of Prime Number Records*, 3ed., Springer-Verlag New York, 1995 (QA246 .R47 ISBN 0-387-94457-5).

[**Ribenboim97**] P. Ribenboim, *Vendendo primos*, Rev. Mat. Univ., 22/23, 1997, 1-13 (tradução de *Selling primes*, Math. Mag., 68 (1995) 175-182).

[**Riesel56**] H. Riesel, *Naagra stora primtal* (Sueco: *Alguns primos grandes*), Elementa 39 (1956) 258-260.

[**Riesel94**] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Progress in Mathematics, Birkhauser Boston, vol. 57, 1985; and vol. 126, 1994.

[**Selberg**] A. Selberg, *An elementary proof of the prime number theorem*, Annals of Math. 50 (1949) 305-13.

[**Sierpinski**] W. Sierpinski, *Sur un problème concernant les nombres* $k \cdot 2^n + 1$, Elem. Math., 15 (1960) 73-74. Corrigendum: Elem. Math., 17 (1963) 85.

[**Westzynthius**] E. Westzynthius, *Über die Verteilung der Zahlen die zu den* n *ersten Primzahlen teilerfremd sind*, Comm. Phys. math. Helsingfors, 5:5 (1931) 1-37.

[**Wilf**] H. Wilf, *What is an answer?* Am. Math. Monthly, 89 (1982), 289-292.

[**WD**] H. C. Williams e H. Dubner, *The primality of R1031*, Math. Comp., 47 (1986) 703-711.

[**YP**] J. Young e A. Potler, *First occurence of primes gaps*, Math. Comp., 52 (1989) 221-224.