Seqüências Recorrentes

Carlos Gustavo Moreira

IMPA

Seqüências recorrentes são seqüências $x_0, x_1, x_2, \ldots$ em que cada termos é determinado por uma dada função dos termos anteriores. Dado um inteiro positivo k, uma *seqüência recorrente de ordem k* é uma seqüência e que cada termo é determinado como uma função dos k termos anteriores:

$$x_{n+k} = f(x_{n+k-1}, x_{n+k-2}, \ldots, x_{n+1}, x_n), \quad \forall\ n \in \mathbb{N}.$$

Com essa generalidade, o estudo geral de seqüências recorrentes se confunde em large medida com a teoria dos Sistemas Dinâmicos, e o comportamento de tais seqüências pode ser bastante caótico e de descrição muito difícil, mesmo qualitativamente. Um caso particular muito importante ocorre quando a função f é linear: existem constantes $C_1, C_2, \ldots, C_n$ com

$$x_{n+k} = C_1 x_{n+k-1} + C_2 x_{n+k-2} + \cdots + C_k x_n, \quad \forall\ n \in \mathbb{N}.$$

Tais seqüências são conhecidas como seqüências recorrentes lineares, e generalizam simultaneamente as progressões geométricas, aritméticas e os polinômios. Estas seqüências serão o objeto principal dessas notas. Não obstante, algumas recorrências não-lineares serão consideradas, como a recorrência $x_{n+1} = x_n^2 - 2$, que tem grande interesse do ponto de vista de sistemas dinâmicos e por suas aplicações à teroria dos números.

Essas notas são inspiradas no excelente livreto "Seqüências Recorrentes", de A. Markuchevitch, publicado na coleção "Iniciação na matemática", da editora MIR, no qual o autor aprendeu bastante sobre o tema no início de sua formação matemática. A seção 4, onde é deduzida a fórmula para o termo geral de uma seqüência recorrente linear, é adaptada do artigo "Equações de recorrência", de Héctor Soza Pollman, publicado no número 9 da revista Eureka! (de fato, o artigo original submetido à revista enunciava esta fórmula sem demonstração, a qual foi incluída no artigo pelo autor destas notas, que é um dos editores da Eureka!).

1 – Seqüências recorrentes lineares:

Uma seqüência $(x_n)_{n\in\mathbb{N}}$ é uma seqüência recorrente linear de ordem k (onde k é um inteiro positivo) se existem constantes (digamos reais ou complexas) $C_1, C_2, \ldots, C_k$ tais que

$$x_{n+k} = \sum_{j=1}^{k} C_j x_{n+k-j} = C_1 x_{n+k-1} + C_2 x_{n+k-2} + \cdots + C_k x_n, \quad \forall\ n \in \mathbb{N}.$$

Tais seqüências são determinadas pelos seus k primeiros termos $x_0, x_1, \ldots, x_{k-1}$.

Os exemplos mais simples (e fundamentais, como veremos a seguir) de seqüências recorrentes lineares são as progressões geométricas: se $x_n = a \cdot q^n$ então $x_{n+1} = qx_n$, $\forall\ n \in \mathbb{N}$, donde (x_n) é uma seqüência recorrente linear de ordem 1.

Se (x_n) é uma progressão aritmética, existe uma constante r tal que $x_{n+1} - x_n = r$, $\forall\, n \in \mathbb{N}$, donde $x_{n+2} - x_{n+1} = x_{n+1} - x_{n+1} - x_n$, $\forall\ n \in \mathbb{N}$, e logo $x_{n+2} = 2x_{n+1} - x_n$, $\forall\ n \in \mathbb{N}$, ou seja, (x_n) é uma seqüência recorrente linear de ordem 2.

Se $x_n = P(n)$ onde P é um polinômio de grau k, então (x_n) satisfaz a recorrência linear de ordem $k+1$ dada por

$$x_{n+k+1} = \sum_{j=0}^{k} (-1)^j \binom{k+1}{j+1} x_{n+k-j}, \quad \forall\ n \in \mathbb{N}. \qquad (*)$$

Isso é evidente se $k = 0$ (isto é, se P é constante), pois nesse caso (*) se reduz a $x_{n+1} = x_n$, $\forall\ n \in \mathbb{N}$, e o caso geral pode ser provado por indução: se P é um polinômio de grau $k \geq 1$ então $A(x) = P(x+1) - P(x)$ é um polinômio de grau $k-1$, donde $y_n = x_{n+1} - x_n = Q(n)$ satisfaz a recorrência $y_{n+k} = \sum_{j=0}^{k-1} (-1)^j \binom{k}{j+1} y_{n+k-1-j}$, $\forall\ n \in \mathbb{N}$, donde

$$x_{n+k+1} - x_{n+k} = \sum_{j=0}^{k-1} (-1)^j \binom{k}{j+1} (x_{n+k-j} - x_{n+k-j-1}), \quad \forall\ n \in \mathbb{N},$$

e logo

$$x_{n+k+1} = \sum_{j=0}^{k} (-1)^j \left(\binom{k}{j+1} + \binom{k}{j} \right) x_{n+k-j} = \sum_{j=0}^{k} (-1)^j \binom{k+1}{j+1} x_{n+k-j}, \forall\ n \in \mathbb{N}.$$

Um outro exemplo é dado por seqüências do tipo $x_n = (an + b) \cdot q^n$, onde a, b e q são constantes. Temos que $x_{n+1} - qx_n = (a(n+1)+b)q^{n+1} - q(an+b) \cdot q^n = q^{n+1}(a(n+1)+b-(an+b)) = aq^{n+1}$ é uma progressão geométrica de razão q, e logo $x_{n+2} - qx_{n+1} = q(x_{n+1} - qx_n)$, donde $x_{n+2} = 2qx_{n+1} - q^2x_n$, $\forall\ n \in \mathbb{N}$, e portanto (x_n) é uma seqüência recorrente linear de ordem 2.

Vamos agora considerar a famosa e popular seqüência de Fibonacci, dada por $U_0 = 0$, $U_1 = 1$ e $U_{n+2} = U_{n+1} + U_n$, $\forall\ n \in \mathbb{N}$. Seus primeiros termos são $U_0 = 0$, $U_1 = 1$, $U_2 = 1$, $U_3 = 2$, $U_4 = 3$, $U_5 = 5$, $U_6 = 8$, $U_7 = 13$, $U_8 = 21, \ldots$. Mostraremos na próxima seção como achar uma fórmula explícita para seu termo geral U_n em função de n, o que será generalizado para seqüências recorrentes lineares quaisquer, e veremos algumas de suas propriedades aritméticas.

Antes porém, concluiremos esta seção com alguns fatos gerais sobre seqüências recorrentes lineares, que serão úteis nas seções subsequentes.

O conjunto das seqüências que satisfazem uma dada recorrência linear

$$x_{n+k} = \sum_{j=1}^{k} C_j x_{n+k-j}, \quad \forall\ n \in \mathbb{N}$$

é um *espaço vetorial*, isto é, dadas duas seqüências (y_n) e (z_n) que satisfazem esta recorrência (ou seja, $y_{n+k} = \sum_{j=1}^{k} C_j y_{n+k-j}$ e $z_{n+k} = \sum_{j=1}^{k} C_j z_{n+k-j}$, $\forall\ n \in \mathbb{N}$) e uma constante a, a seqüência (w_n) dada por $w_n = y_n + az_n$ satisfaz a mesma recorrência: $w_{n+k} = \sum_{j=1}^{k} C_j w_{n+k-j}$, $\forall\ n \in \mathbb{N}$.

É bastante usual, dada uma seqüência (x_n), estudar a seqüência obtida pela soma de seus n primeiros termos $s_n = \sum_{k \le n} x_k$. Se (x_n) é uma seqüência recorrente linear, (s_n) também é. De fato, $s_{n+1} - s_n = \sum_{k \le n+1} x_k - \sum_{k \le n} x_k = x_{n+1}$, $\forall\ n \in \mathbb{N}$. Se $x_{n+k} = \sum_{j=1}^{k} C_j x_{n+k-j}$, temos $s_{n+k+1} - s_{n+k} = \sum_{j=1}^{k} C_j (s_{n+k+1-j} - s_{n+k-j})$, $\forall\ n \in \mathbb{N}$ donde

$$s_{n+k+1} = (1 + C_1)s_{n+k} + \sum_{j=1}^{k-1} (C_{j+1} - C_j)s_{n+k-j} - C_k s_n = \sum_{i=1}^{k+1} d_i s_{n+k+1-i}$$

, onde $d_1 = 1 + C_1$, $d_i = C_i - C_{i-1}$ para $2 \le i \le k$ e $d_{k+1} = -C_k$, $\forall\ n \in \mathbb{N}$, e portanto (s_n) é uma seqüência recorrente linear de ordem $k + 1$.

2 – A seqüência de Fibonacci:

A seqüência de Fibonacci é definida por $U_0 = 0$ $U_1 = 1$ e $U_{n+2} = U_{n+1} + U_n$, $\forall\ n \in \mathbb{N}$. Queremos achar uma fórmula explícita para U_n em função de n. Para isso usaremos uma idéia que será bastante útil também no caso geral: procuraremos progressões geométricas que satisfazem a mesma recorrência que (U_n): se $x_n = a \cdot q^n$ com a e q não nulos satisfaz $x_{n+2} = x_{n+1} + x_n$, $\forall\ n \in \mathbb{N}$, teremos $a \cdot q^{n+2} = a \cdot q^{n+1} + a \cdot q^n = a \cdot q^n(q+1)$, donde $q^2 = q + 1$. Temos assim dois valores possíveis para q: as duas raízes da equação $q^2 - q - 1 = 0$, que são $\frac{1+\sqrt{5}}{2}$ e $\frac{1-\sqrt{5}}{2}$. Assim, seqüências da forma $a\left(\frac{1+\sqrt{5}}{2}\right)^n$ e da forma $b\left(\frac{1-\sqrt{5}}{2}\right)^n$ satisfazem a recorrência acima, bem como seqüências da forma $y_n = a\left(\frac{1+\sqrt{5}}{2}\right)^n + b\left(\frac{1-\sqrt{5}}{2}\right)^n$, pela observação da seção anterior.

Basta agora encontrar valores de a e b tais que $y_0 = 0$ e $y_1 = 1$ para que tenhamos $y_n = U_n$ para todo n (de fato, teríamos $y_0 = U_0$, $y_1 = U_1$ e, por indução se $k \geq 2$ e $y_n = U_n$ para todo $n < k$, temos $y_k = y_{k-1} + y_{k-2} = U_{k-1} + U_{k-2} = U_k$). Para isso, devemos ter:

$$\begin{cases} a + b = 0 \\ a\left(\frac{1+\sqrt{5}}{2}\right) + b\left(\frac{1-\sqrt{5}}{2}\right) = 1 \end{cases}$$

e portanto $a = \frac{1}{\sqrt{5}}$ e $b = -\frac{1}{\sqrt{5}}$. Mostramos assim que

$$U_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right), \quad \forall\ n \in \mathbb{N}.$$

É curioso que na fórmula do termo geral de uma seqüência de números inteiros definida de modo tão simples quanto (U_n) apareçam números irracionais.

Provaremos a seguir uma identidade útil sobre números de Fibonacci:

Proposição: $U_{m+n} = U_m U_{n-1} + U_{m+1} U_n$, $\forall\ m, n \in \mathbb{N}$, $n \geq 1$.

Prova: Sejam $y_m = U_{m+n}$ e $Z_m = U_m U_{n-1} + U_{m+1} U_n$. Temos que (y_n) e (Z_m) satisfazem a recorrência $x_{n+2} = x_{n+1} + x_n$, $\forall\ n \in \mathbb{N}$. Por outro lado, $y_0 = U_n$, $y_1 = U_{n+1}$, $Z_0 = 0 \cdot U_{n-1} + 1 \cdot U_n = U_n = y_0$ e $Z_1 = 1 \cdot U_{n-1} + 1 \cdot U_n = U_{n+1} = y_1$, e portanto, como antes, $Z_n = y_n$, $\forall\ n \in \mathbb{N}$. ■

Podemos usar este fato para provar o seguinte interessante fato aritmético sobre a seqüência (U_n), que pode ser generalizado para as chamadas seqüências de Lucas, as quais são úteis para certos testes de primalidade, como veremos mais tarde:

Teorema: $\text{mdc}(U_m, U_n) = U_{\text{mdc}(m,n)}$, $\forall\ m, n \in \mathbb{N}$.

Prova: Observemos primeiro que $\text{mdc}(U_n, U_{n+1}) = 1$, $\forall\ n \in \mathbb{N}$. Isso vale para $n = 0$ pois $U_1 = 1$ e, por indução, $\text{mdc}(U_{n+1}, U_{n+2}) = \text{mdc}(U_{n+1}, U_{n+1} + U_n) = \text{mdc}(U_{n+1}, U_n) = 1$. Além disso, se $m = 0$, $\text{mdc}(U_m, U_n) = \text{mdc}(0, U_n) = U_n = U_{\text{mdc}(m,n)}$, $\forall\ n \in \mathbb{N}$, e se $m = 1$, $\text{mdc}(U_m, U_n) = \text{mdc}(1, U_n) = 1 = U_1 = U_{\text{mdc}(m,n)}$, $\forall\ n \in \mathbb{N}$. Vamos então provar o fato acima por indução em m. Suponha que a afirmação do enunciado seja válida para todo $m < k$ (onde $k \geq 2$ é um inteiro dado) e para todo $n \in \mathbb{N}$. Queremos provar que ela vale para $m = k$ e para todo $n \in \mathbb{N}$, isto é, que $\text{mdc}(U_k, U_n) = U_{\text{mdc}(k,n)}$ para todo $n \in \mathbb{N}$. Note que, se $n < k$, $\text{mdc}(U_k, U_n) = \text{mdc}(U_n, U_k) = U_{\text{mdc}(n,k)} = U_{\text{mdc}(k,n)}$, por hipótese de indução. Já se $n \geq k$, $U_n = U_{(n-k)+k} = U_{n-k}U_{k-1} + U_{n-k+1}U_k$, e logo $\text{mdc}(U_k, U_n) = \text{mdc}(U_k, U_{n-k}U_{k-1} + U_{n-k+1}U_k) = \text{mdc}(U_k, U_{n-k}U_{k-1}) = \text{mdc}(U_k, U_{n-k})$ (pois $\text{mdc}(U_k, U_{k-1}) = 1$) $= U_{\text{mdc}(k,n-k)} = U_{\text{mdc}(k,n)}$. ■

Corolário: Se $m \geq 1$ e m é um divisor de n então U_m divide U_n. Além disso, se $m \geq 3$ vale a recíproca: se U_m divide U_n então m divide n.

3 – A recorrência $x_{n+1} = x_n^2 - 2$

Consideremos as seqüências $(x_n)_{n\in\mathbb{N}}$ de números reais que satisfazem a recorrência $x_{n+1} = x_n^2 - 2$, $\forall\ n \in \mathbb{N}$. Suponha que $x_0 = \alpha + \alpha^{-1}$ para um certo α (real ou complexo). Então podemos provar por indução que $x_n = \alpha^{2^n} + \alpha^{-2^n}$, $\forall\ n \in \mathbb{N}$. De fato, se vale a fórmula para x_n, teremos

$$x_{n+1} = x_n^2 - 2 = (\alpha^{2^n} + \alpha^{-2^n})^2 - 2 = \alpha^{2^{n+1}} + 2 + \alpha^{-2^{n+1}} - 2 = \alpha^{2^{n+1}} + \alpha^{-2^{n+1}}.$$

Se $|x_0| > 2$, temos $x_0 = \alpha + \alpha^{-1}$ para $\alpha = \frac{x_0 + \sqrt{x_0^2 - 4}}{2} \in \mathbb{R}$.

Se $|x_0| \leq 2$, vale a mesma fórmula para α, mas nesse caso α é um número complexo de mótulo 1, e pode ser escrito como $\alpha = e^{i\theta} = \cos\theta + i\,\mathrm{sen}\,\theta$. Nesse caso, $x_n = e^{2^n i\theta} + e^{-2^n i\theta} = (\cos(2^n\theta) + i\,\mathrm{sen}(2^n\theta)) + (\cos(2^n\theta) - \mathrm{sen}(2^n\theta)) = 2\cos(2^n\theta)$.

Podemos ver isso de outra forma: se $|x_0| \leq 2$, escrevemos $x = 2\cos\theta$, com $\theta \in [0, \pi]$. Podemos mostrar então por indução que $x_n = 2\cos(2^n\theta)$, para todo $n \in \mathbb{N}$. De fato, $x_{n+1} = x_n^2 - 2 = 4\cos^2(2^n\theta) - 2 = 2(2\cos^2(2^n\theta) - 1) = 2\cos(2^{n+1}\theta)$, pois $\cos(2x) = 2\cos^2 x - 1$, $\forall\ x \in \mathbb{R}$. Podemos usar esta expressão para obter diversos tipos de comportamento possível para uma tal seqüência (x_n). Se $x_0 = 2\cos\theta$ e θ/π é racional e tem representação binária periódica de período n então $(x_n) = (2\cos(2^n\theta))$, podemos ter $x_0 = 2\cos\theta$ onde θ/π tem representação binária como

$$0,0100011011000001010011100101110111...$$

em que todas as seqüências finitas de zeros e uns aparecem em algum lugar (isso acontece para a "maioria" dos valores de θ).

Nesse caso, a seqüência (x_n) é *densa* em $[-2, 2]$, isto é, qualquer ponto de $[-2, 2]$ pode ser apromado por elementos de (x_n), com erro arbitrariamente pequeno.

No caso em que $x_0 \in \mathbb{R}$, a seqüência (x_n) pode ter propriedades aritméticas muito interessantes. Em particular, se $x_0 = 4$ (e logo $x_n = (2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}$, $\forall\ n \in \mathbb{N}$) vale o famoso critério de Lucas-Lehmer para testar a primalidade de números de Mersenne: se $n \geq 3$ então $2^n - 1$ é primo se e somente se $2^n - 1$ é um divisor de x_{n-2} (por exemplo, $2^3 - 1 = 7$ é primo e é um divisor de $x_{3-1} = x_1 = x_0^2 - 2 = 4^2 - 2 = 14$).

Exercício: Seja $x_0 \geq 3$ um inteiro ímpar.

i) Prove que se p é um número primo então existe no máximo um valor de $n \in \mathbb{N}$ tal que p divide x_n.

ii) Prove que se p é um fator primo de x_n então $p > n$.

Sugestão: Considere a seqüência $x_n (\mathrm{mod}\ p)$.

Esse exercício pode ser generalizado para outras recorrências. Nesse caso particular da recorrência $x_{n+1} = x_n^2 - 2$ é possível mostrar um resltado mais forte: se p é um fator primo de x_n então $p \geq 2^{n+2} - 1$ (note que quando $p = 2^q - 1$ é primo, com $q \geq 3$ e $n = q - 2$, vale a igualdade $p = 2^{n+2} - 1$ e $p|x_n$, pelo critério de Lucas-Lehmer enunciado acima).

4 - Fórmulas gerais para seqüências recorrentes lineares:

Considere a equação

$$a_k x_{n+k} + a_{k-1} x_{n+k-1} + \cdots + a_0 x_n = 0, \quad n \geq 0 \tag{2}$$

em que $a_0, \ldots, a_k$ são constantes, e os valores de x_i são conhecidos para $i = 0, \ldots, k-1$. Supondo que a equação (2) admite uma solução do tipo: $x_n = \lambda^n$, em que λ é um parâmetro inteiro, e substituindo em (2) temos

$$a_k \lambda^{n+k} + a_{k-1} \lambda^{n+k-1} + \cdots + a_0 \lambda^n = 0.$$

Se $\lambda \neq 0$ então obtemos a *equação característica* associada a equação (2)

$$a_l a^k + a_{k-1} \lambda^{k-1} + \cdots + a_0 \lambda^0 = 0.$$

Vamos mostrar que se esta equação tem as raízes complexas $\lambda_1, \ldots, \lambda_r$ com multiplicidades $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}$, respectivamente, então as soluções de (2) são exatamente as seqüências (x_n) da forma $x_n = Q_1(n)\lambda_1^n + Q_2(n)\lambda_2^n + \cdots + Q_r(n)\lambda_r^n$, onde $Q_1, \ldots, Q_r$ são polinômios com grau $(Q_i) < \alpha_i$, $1 \leq i \leq r$ (em particular, se λ_i é uma raiz simples então Q_i é constante).

Seja $P(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$ um polinômio.

Dizemos que uma seqüência $(x_n)_{n \in \mathbb{N}}$ satisfaz a propriedade $\mathrm{Rec}(P(x))$ se $a_k x_{n+k} + a_{k-1} x_{n+k-1} + \cdots + a_0 x_n = 0$, $\forall\ n \in \mathbb{N}$. Não é difícil verificar os seguintes fatos:

i) Se (X_n) e (Y_n) satisfazem $\mathrm{Rec}(P(x))$ e $c \in \mathbb{C}$ então $(Z_n) = X_n + cY_n$ satisfaz $\mathrm{Rec}(P(x))$.

ii) Se $Q(x) = b_r X^r + b_{r-1}X^{r-1} + \cdots + b_0$ e (X_n) satisfaz $\mathrm{Rec}(P(x))$ então (X_n) satisfaz $\mathrm{Rec}(P(x)Q(x))$ (isso segue de $\sum_{j=0}^{r} b_j(a_k X_{n+j+k} + a_{k-1}X_{n+j+k-1} + \cdots + a_0 X_{n+j}) = 0$, $\forall\ n \in \mathbb{N}$)

iii) (X_n) satisfaz $\mathrm{Rec}(P(x))$ se e só se $(Y_n) = (X_n/\lambda^n)$ satisfaz $\mathrm{Rec}(P(\lambda X))$ (substitua $X_{n+j} = \lambda^{n+j}Y_{n+j}$ em $\sum_{j=0}^{k} a_j X_{n+j} = 0$).

iv) Se $S_n = \sum_{k=0}^{n} x_k$ então (x_n) satisfaz $\mathrm{Rec}(P(x))$ se e só se (S_n) satisfaz $\mathrm{Rec}((x-1)P(x))$ (escreva $x_{n+j+1} = S_{n+j+1} - S_{n+j}$ e substitua em $\sum_{j=0}^{n} a_j x_{n+j+1} = 0$).

Por iii), para ver que, para todo polinômio $Q(x)$ de grau menor que m, $X_n = Q(n)\lambda^n$ satisfaz $\mathrm{Rec}((x-\lambda)^m)$, basta ver que $(Y_n) = (Q(n))$ satisfaz $\mathrm{Rec}((x-1)^m)$, o que faremos por indução. Isso é claro que $m = 1$, e em geral, se $Z_n = Y_{n+1} - Y_n = Q(n+1) - Q(n)$, como $\tilde{Q}(x) = Q(x+1) - Q(x)$ tem grau menor que $m-1$, (Z_n) satisfaz $\mathrm{Rec}((x-1)^{m-1})$ (por hipótese de indução), e logo, por (iv), $Y_n)$ satisfaz $\mathrm{Rec}((x-1)^m)$. Essa observação, combinada com ii), mostra que se $(P(x) = (x-\lambda_1)^{\alpha_1}(x-\lambda_2)^{\alpha_2}(x-\lambda_2)^{\alpha_2}\ldots(x-\lambda_r)^{\alpha_r}$, e grau $Q_i) < \alpha_i$ para $1 \le i \le r$ então $x_n = \sum_{i=1}^{r} Q_i(n)\lambda_i^n$ satisfaz $\mathrm{Rec}(P(x))$.

Para ver que se (x_n) satisfaz $\mathrm{Rec}(P(x))$ então x_n é da forma acima, usaremos indução novamente.

Supomos $\lambda_1 \neq 0$ e tomamos $Y_n = X_n/\lambda_1^n$, $Z_n = Y_{n+1} - Y_n$ (com $Z_0 = Y_0$).

Por iii) e iv), Z_n satisfaz $\mathrm{Rec}(P(\lambda_1 x)/(x-1))$ e, portanto por hipótese de indução, $Z_n = \tilde{Q}_1(x) + \tilde{Q}_2(x)(\lambda_2/\lambda_1)^n + \cdots + \tilde{Q}_r(x)(\lambda_r/\lambda_1)^n$, onde grau $\tilde{Q}_i < \alpha_i$ para $2 \le i \le r$ e grau $\tilde{Q}_1 < \alpha_1 - 1$.

Para terminar a prova, vamos mostrar que se existem polinômios $P_1, P_2, \ldots, P_k$ tais que $Y_{n+1} - Y_n = P_1(n) + P_2(n)\beta_2^n + \cdots + P_k(n)\beta_k^n$ (onde $1, \beta_2, \ldots, \beta_k$ são complexos dististos e $P_i \neq 0$, $\forall\ i \ge 2$) então $Y_n = \tilde{P}_1(n) + \tilde{P}_2(n)\beta_2^n + \cdots + \tilde{P}_k(n)\beta_k^n$, onde $\tilde{P}_1, \ldots, \tilde{P}_k$ são polinômios com grau $P_i =$ grau $\tilde{P}_i$ para $i \ge 2$ e grau $\tilde{P}_1 =$ grau $P_1 + 1$, por indução na soma dos graus dos polinômios P_i, onde convencionamos que o grau do polinômio nulo é -1.

(no nosso caso temos $\beta_i = \lambda_i/\lambda_1$, e como $X_n = \lambda_1^n Y_n$ o resultado segue imediatamente).

Para provar essa afirmação observamos inicialmente que, se a soma dos grau de P_i é -1, então $Y_{n+1} - Y_n = 0$, $\forall\ n$, e logo, Y_n é constante e, em geral, consideramos 2 casos:

a) $P_1(x) = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_0$, $c_m \neq 0$. Nesse caso definimos $\tilde{Y}_n = Y_n - \frac{c_m n^{m+1}}{m+1}$, e temos $\tilde{Y}_{n+1} - \tilde{Y}_n = Q_1(n) + P_2(n)\beta_1^n + \cdots + P_k(n)\beta_k^n$, com grau $Q < m$. Por hipótese de indução, $\tilde{Y}_n$ (e logo Y_n) é da forma desejada.

b) $P_2(x) = d_s x^s + d_{s-1}x^{s-1} + \cdots + d_0$, $d_s \neq 0$. Nesse caso, definimos $\tilde{Y}_n = Y_n - \frac{d_s n^s \lambda_2^n}{\lambda_2 - 1}$, e temos $\tilde{Y}_{n+1} - \tilde{Y}_n = P_1(n) + Q(n)\beta_2^n + P_3(n)\beta_3^n + \cdots + P_k(n)\beta_k^n$, com grau $Q < s$. Por hipótese de indução, $\tilde{Y}_n$ (e logo Y_n) é da forma desejada. ■

Vimos na primeira parte da demonstração acima que (x_n) satisfaz Rec$(P(x))$, onde $P(x) = (x-\lambda_1)^{\alpha_1}(x-\lambda_2)^{\alpha_2}\ldots(x-\lambda_r)^{\alpha_r}$ sempre que $x_n = Q_1(n)\lambda_1^n + Q_2(n)\lambda_2^n + \cdots + Q_r(n)\lambda_r^n$, onde $Q_1, Q_2, \ldots, Q_r$ são polinômios com grau$(Q_j) < \alpha_j$, $\forall\ j \leq r$. Vamos apresentar um argumento alternativo, motivado por conversas do autor com Bruno Fernandes Cerqueira Leite, para mostrar que todas as seüências que satisfazem as recorrência são dessa forma.

Cada polinômio $Q_i(n)$ tem α_i coeficientes (dos monômios cujos graus são $0, 1, 2, ; s\alpha_i - 1$). Como o espaço vetorial das seqüências que satisfazem Rec$(P(x))$ tem dimensão grau$(P(x)) = \sum_{i=1}^{r} \alpha_i$, basta ver que há unicidade na representação de uma seqüência na forma cima. Para isso, dvemos mostrar que, se $\lambda_1, \lambda_2, \ldots, \lambda_r$ são números complexos distintos e $Q_1, Q_2, \ldots, Q_r$ são polinômis tais que $Q_1(n)\lambda_1^n + Q_2(n)\lambda_2^n + \cdots + Q_r(n)\lambda_r^n = 0$, $\forall\ n \in \mathbb{N}$, então $Q_j \equiv 0$, $\forall\ j \leq r$.

Vamos supor por absurdo que não seja assim. supomos sem perda de generalidade que, para certos s e t com $1 \leq s \leq t \leq r$, $|\lambda_1| = |\lambda_i| > |\lambda_j|$, $\forall\ i \leq t$, $j > t$, e grau$(Q_1) =$ grau$(Q_i) >$ grau(Q_j), se $i \leq s < j \leq t$. Se os polinômios Q_j não são todos nulos, temos Q_1 não nulo. Seja d o grau de Q_1. Se $|\lambda_j| < |\lambda_1|$ então $\lim_{n\to\infty} \frac{Q_j(n)\lambda_j^n}{n^d \cdot \lambda_1^n} = 0$, e se $|\lambda_i| = |\lambda_1|$ e grau$(Q) < d$, também temos $\lim_{n\to\infty} \frac{Q(n)\lambda_i^n}{n^d\lambda_1^n} = 0$. Portanto, se $Q_1(n)\lambda_1^n + Q_2(n)\lambda_2^n + \cdots + Q_r(n)\lambda_r^n = 0$, $\forall\ n \in \mathbb{N}$e o coeficiente de n^d em Q_i é a_i para $i \leq s$, dividindo por $n^d\lambda_1^n$ e tomando o limite, temos

$$\lim_{n\to\infty}\left(a_1 + \sum_{2\leq i\leq s} a_i\left(\frac{\lambda_i}{\lambda_1}\right)^n\right) = 0,$$

donde

$$\begin{aligned}
0 &= \lim_{n\to\infty}\left(\frac{1}{n}\sum_{k=1}^{n}\left(a_1+\sum_{2\le i\le s}a_i\left(\frac{\lambda_i}{\lambda_1}\right)^k\right)\right)\\
&= \lim_{n\to\infty}\left(a_1+\frac{1}{n}\sum_{k=1}^{n}\sum_{2\le i\le s}a_i\left(\frac{\lambda_i}{\lambda_1}\right)^k\right)\\
&= a_1+\sum_{2\le i\le s}a_i\cdot\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{n}\left(\frac{\lambda_i}{\lambda_1}\right)^k\\
&= a_1+\sum_{2\le i\le s}a_i\cdot\lim_{n\to\infty}\left(\frac{1}{n}\cdot\frac{(\lambda_i/\lambda_1)^{n+1}-(\lambda_i/\lambda_1)}{(\lambda_i/\lambda_1)-1}\right)=a_1,
\end{aligned}$$

pois, para $2\le i\le s$, $\lambda_i/\lambda_1\neq 1$ é um complexos de módulo 1, donde

$$\left|\frac{(\lambda_i/\lambda_1)^{n+1}-(\lambda_i/\lambda_1)}{(\lambda_i/\lambda_1)-1}\right|\le\frac{2}{|(\lambda_i/\lambda_1)-1|},$$

e logo

$$\lim_{n\to\infty}\frac{1}{n}\left(\frac{(\lambda_i/\lambda_1)^{n+1}-(\lambda_i/\lambda_1)}{(\lambda_i/\lambda_1)-1}\right)=0.$$

Entretanto, isso é um absurdo, pois grau$(Q_1)=d$, e logo $a_1\neq 0$.

Exemplo: $x_n=\operatorname{sen}(n\alpha)$ satisfaz uma recorrência linear. De fato,

$x_{n+1}=\operatorname{sen}(n\alpha+\alpha)=\operatorname{sen}(n\alpha)\cos\alpha+\cos(n\alpha)\operatorname{sen}\alpha\Rightarrow$

$x_{n+2}=\operatorname{sen}(n\alpha+2\alpha)=\operatorname{sen}(n\alpha)\cos 2\alpha+\cos(n\alpha)\operatorname{sen}2\alpha\Rightarrow$

$\Rightarrow x_{n+2}-\frac{\operatorname{sen}2\alpha}{\operatorname{sen}\alpha}x_{n+1}=(\cos 2\alpha-\frac{\operatorname{sen}2\alpha}{\operatorname{sen}\alpha}\cos\alpha)x_n$, ou seja,

$x_{n+2}=2\cos\alpha X_{n+1}-X_n$. Note que x_n não parece ser da forma geral descrita nesta seção, mas de fato

$$x_n=\frac{e^{in\alpha}-e^{-in\alpha}}{2i}=\frac{1}{2i}(e^{i\alpha})^n-\frac{1}{2i}(e^{-i\alpha})^n=\frac{1}{2i}(\cos\alpha+i\operatorname{sen}\alpha)^n-\frac{1}{2i}(\cos\alpha-i\operatorname{sen}\alpha)^n$$

.

Observação: Se (x_n) safisfaz Rec$((x-1)P(x))$, onde $P(x)=a_nx^k+a_{k-1}x^{k-1}+\cdots+a_0$, então, se definirmos $Y_n=a_kx_{n+k}+a_{k-1}x_{n+k-1}+\cdots+a_0x_n$, teremos $Y_{n+1}=Y_n$, $\forall\ n\in\mathbb{N}$, ou seja, Y_n é

constante. Assim, $a_k x_{n+k} + \cdots + a_0 x_n$ é um invariante da seqüência x_n, o que é uma observação útil para muitos problemas envolvendo recorrência.

Vamos agora ver um problema resolvido em que se usam estimativas assintóticas de seqüências recorrentes para provar um resultado de teoria dos números:

Problema. (Problema 69 da Revista Eureka! n^o. 14) Sejam a e b inteiros positivos tais que $a^n - 1$ divide $b^n - 1$ para todo inteiro positivo n.

Prove que existe $x \in \mathbb{N}$ tal que $b = a^k$.

Solução de Zoroastro Azambuja Neto (Rio de Janeiro-RJ):

Suponha por absurdo que b não seja uma potência de a.

Então existe $k \in \mathbb{N}$ tal que $a^k < b < a^{k+1}$. Consideremos a seqüência $x_n = \frac{b^n - 1}{a^n - 1} \in \mathbb{N}$, $\forall\ n \geq 1$. Como $\frac{1}{a^n - 1} = \frac{1}{a^n} + \frac{1}{a^{2n}} + \cdots = \sum_{j=1}^{\infty} \frac{1}{a^{jn}}$, temos

$$x_n = \sum_{j=1}^{\infty} \frac{b^n}{a^{jn}} - \sum_{j=1}^{\infty} \frac{1}{a^{jn}} = \left(\frac{b}{a}\right)^n + \left(\frac{b}{a^2}\right)^n + \ldots \left(\frac{b}{a^k}\right)^n + \frac{b^n}{a^{kn}(a^n - 1)} - \frac{1}{a^n - 1}.$$

Note que como $\frac{b^n}{a^{kn}(a^n - 1)} = \frac{(b/a^{k+1})^n}{1 - a^{-n}}$ e $\frac{1}{a^n - 1}$ tendem a 0 quando n cresce, se definimos

$$y_n - \left(\frac{b}{a}\right)^n + \left(\frac{b}{a^2}\right) + \cdots + \left(\frac{b}{a^k}\right)^n = \sum_{j=1}^{k} \left(\frac{b}{a^j}\right)^n,$$

temos que

$$x_n - y_n = \frac{b^n}{a^{kn}(a^n - 1)} - \frac{1}{a^n - 1}$$

tende a 0 quando n tende a infinito. Por outro lado, como y_n é uma soma de k progressões geométricas de razões b/a^j, $1 \leq j \leq k$, y_n satisfaz a equação de recorrência $C_0 y_{n+k} + C_1 y_{n+k-1} + \cdots + C_k y_n = 0$, $\forall\ n \geq 0$, onde

$$C_0 x^k + C_1 x^{k-1} + \cdots + C_{k-1} x + C_k = a^{k(k+1)/2} \left(x - \frac{b}{a}\right)\left(x - \frac{b}{a^2}\right) \ldots \left(x - \frac{b}{a^k}\right)$$

Note que todos os C_i são inteiros. Note também que

$$C_0 x_{n+k} + C_1 x_{n+k-1} + \cdots + C_k x_n = C_0(x_{n+k} - y_{n+k}) + C_1(x_{n+k-1} - y_{n+k-1}) + \cdots + C_k(x_n - y_n)$$

tende a 0 quando n tende a infinito, pois $x_{n+j} - y_{n+j}$ tende a 0 para todo j com $0 \leq j \leq k$ (e k está fixo). Como os C_i e os x_n são todos inteiros, isso mostra que $C_0 x_{n+k} + C_1 x_{n+k-1} + \cdots + C_k x_n = 0$ para todo n grande.

Agora, como

$$x_n = y_n + \left(\frac{b}{a^{k+1}}\right)^n + \frac{b^n}{a^{(k+1)n}(a^n - 1)} - \frac{1}{a^n - 1},$$

temos

$$C_0 x_{n+k} + C_1 x_{n+k-1} + \cdots + C_k x_n = \sum_{j=0}^{k} C_j \left(\left(\frac{b}{a^{k+1}}\right)^{n+k-j} + z_{n+k-j} \right),$$

onde

$$z_m = \frac{b^m}{a^{(k+1)m}(a^m - 1)} - \frac{1}{a^m - 1}.$$

Note que

$$\sum_{j=0}^{k} C_k \left(\frac{b}{a^{k+1}}\right)^{n+k-j} = P\left(\frac{b}{a^{k+1}}\right) \cdot \left(\frac{b}{a^{k+1}}\right)^n,$$

onde

$$P(x) = C_0 x^k + C_1 x^{k-1} + \cdots + C_{k-1} x + C_k = a^{k(k+1)/2} \left(x - \frac{b}{a}\right)\left(x - \frac{b}{a^2}\right) \ldots \left(x - \frac{b}{a^k}\right),$$

donde $P\left(\frac{b}{a^{k+1}}\right) \neq 0$. Por outro lado, para todo j com $0 \leq j \leq k$, $z_{n+k-j} \Big/ \left(\frac{b}{a^{k+1}}\right)^n = \frac{(b/a^{k+1})^{k-j}}{a^{n+k-j}-1} - \frac{1}{(a^{k-j}-a^{-n})(b/a^k)^n}$, que tende a 0 quando n tende a infinito, donde $x_n = \left(\sum_{j=0}^{k} C_j x_{n+k-j}\right) \Big/ \left(\frac{b}{a^{k+1}}\right)^n$ tende a $P\left(\frac{b}{a^{k+1}}\right) \neq 0$, o que é um absurdo, pois, como vimos antes, w_n é igual a 0 para todo n grande.

Testes de Primalidade e Seqüências Recorrentes

1 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* $\text{mdc}(a^{(n-1)/q} - 1, n) = 1$.

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.

2 Primos de Mersenne

Um número de Mersenne é um número da forma $M_p = 2^p - 1$. Quando esse número é primo, dizemos que é um primo de Mersenne. Atualmente, os 4 maiores primos conhecidos são primos de Mersenne, e têm mais de dois milhões de dígitos: $2^{24036583} - 1, 2^{20996011} - 1, 2^{13466917} - 1$ e $2^{6972593} - 1$. Isto se deve principalmente à existência de um algoritmo especialmente eficiente para testar a primalidade de números de Mersenne: o critério de Lucas-Lehmer, que discutiremos mais adiante. 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 $2^{p-1}M_p$ 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 $2^{k+1}b = (2^{k+1} - 1)\sigma(b)$, Assim, como $(2^{k+1} - 1)|2^{k+1}b$ e $(2^{k+1} - 1, 2^{k+1}) = 1$, temos $(2^{k+1} - 1)|b$. Por outro lado, se b não é igual a $2^{k+1} - 1$, podemos escrever $b = (2^{k+1} - 1)c$, com $c > 1$, donde $\sigma(b) \geq b + c + 1$, e logo $(2^{k+1} - 1)\sigma(b) \geq (2^{k+1} - 1)(b + c + 1) = 2^{k+1}b + 2^{k+1} - 1 > 2^{k+1}b$, absurdo. Assim $b = 2^{k+1} - 1$ e $2^{k+1}b = (2^{k+1} - 1)(b + 1)$, donde $\sigma(b) = b + 1$ e logo 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 $p_0 = 18458709 \cdot 2^{32611} - 1$; assim, pela proposição anterior, M_{p_0} é composto. Sabe-se também que se $\pi_{\mathrm{SG}}(x)$ denota o número de primos de Sophie Germain menores do que x então existe C tal que para todo x

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

Acredita-se que $\pi_{\mathrm{SG}}(x)$ 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 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, $\alpha\beta = Q$, que é invertível em K). Do mesmo modo, $\beta^{n-1} = 1$ em K e portanto temos, em K,

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

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 β^m se $m = n - (\frac{D}{n})$ no anel $K = \mathbb{Z}/(n)[\sqrt{D}]$. Observemos agora que se $\alpha^m = \beta^m$ em K então existe um inteiro r tal que

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

pois $\frac{\alpha^m - \beta^m}{\sqrt{D}} \in \mathbb{Z}$. 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 $\alpha^{m \cdot n^{k-1}} = \beta^{m \cdot n^{k-1}} + n^k r_k \sqrt{D}$, $r_k \in \mathbb{Z}$. Elevando os dois lados da equação à n-ésima potência temos

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

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 $A_r = \{k \in \mathbb{N}^* \mid U_k \text{ é múltiplo de } r\}$ 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, $m, n \in A_r \Rightarrow m + n \in A_r$, e $\ell, s \in A_r$, $\ell < s \Rightarrow s - \ell \in A_r$, 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 $\operatorname{ord}_n U^{(r_i)}$ 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 $\operatorname{ord}_{\ell_j^{\beta_j}} U^{(r_i)}$ 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 $\operatorname{mdc}(n, d) = 1$, 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 $M = mmc\{\ell_j^{\beta_j - 1}(\ell_j - (\frac{d}{\ell_j})),\ 1 \leq j \leq d\}$ 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 $r_i^{\alpha_i} | \operatorname{ord}_n U^{(r_i)} | M$ 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

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

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* $\operatorname{mdc}(U_{\frac{N+1}{r}}^{(r)}, N) = 1$ *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 $1 \leq i \leq k$. Se ℓ é um fator primo de N, também temos $\mathrm{ord}_\ell U^{(r_i)} \mid N+1$. Como $\mathrm{mdc}(N, U^{(r_i)}_{\frac{N+1}{r_i}}) = 1$ segue que $\ell \nmid U^{(r_i)}_{\frac{N+1}{r_i}}$, 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 $1 \leq i \leq k$. 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 $1 \leq i \leq k \Rightarrow F$ 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 $U^{(r)}_{n+1} \equiv 0 \pmod n$ e $\mathrm{mdc}(U^{(r)}_{\frac{n+1}{r}}, n) = 1$ então n é primo.*

Dem: Seja ℓ um fator primo de n. Para cada fator primo r de $n+1$ temos que $U^{(r)}_{n+1} \equiv 0 \pmod \ell$ e $U^{(r)}_{\frac{n+1}{r}} \not\equiv 0 \pmod \ell$. 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, $\ell^2 - 1 \geq n+1$ 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.

Apêndice: Elementos de Teoria dos Números

Veremos inicialmente os tópicos básicos de teoria dos números, como divisibilidade, congruências e aritmética módulo n.

4 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.

5 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)

1. $a \equiv a \pmod{n}$*;*
2. *se* $a \equiv b \pmod{n}$ *então* $b \equiv a \pmod{n}$*;*
3. *se* $a \equiv b \pmod{n}$ *e* $b \equiv c \pmod{n}$ *então* $a \equiv c \pmod{n}$*;*
4. *se* $a \equiv a' \pmod{n}$ *e* $b \equiv b' \pmod{n}$ *então* $a + b \equiv a' + b' \pmod{n}$*;*
5. *se* $a \equiv a' \pmod{n}$ *então* $-a \equiv -a' \pmod{n}$*;*
6. *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* 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 $a \equiv a' \pmod m$ 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.

6 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 $(n-1)! \equiv -1 \pmod{n}$.

■

7 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 $y = a^u$. ■

8 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 $a^{\frac{-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$; 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

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

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 $1 \leq 2j \leq \frac{p-1}{2}$ para $j \leq k$ e $\frac{p-1}{2} < 2j \leq p-1$ para $k+1 \leq j \leq 2k$, 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 $1 \leq j \leq k$ temos $1 \leq 2j \leq \frac{p-1}{2}$ e para $k+1 \leq j \leq 2k+1$ temos $\frac{p-1}{2} < 2j \leq p-1$, 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 $-(p-1)/2 \leq qj - py < 0$. 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

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

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. ■

9 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 $(a,b)\neq(0,0)\Rightarrow a\neq 0\Rightarrow a^2\neq 0$.

■