Polos Olímpicos de Treinamento
Curso de Teoria dos Números - Nível 3
Carlos Gustavo Moreira

Aula 18

Sequências recorrentes e testes de primalidade

1 A Sequência de Fibonacci

A sequência de Fibonacci é definida por $F_0 = 0$, $F_1 = 1$ e $F_{n+2} = F_{n+1} + F_n$, $\forall n \in \mathbb{N}$. Queremos achar uma fórmula explícita para F_n em função de n. Para isso usaremos uma ideia que será bastante útil também no caso geral: procuraremos progressões geométricas que satisfazem a mesma recorrência que (F_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, sequências 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, e portanto sequências da forma $y_n = a\left(\frac{1+\sqrt{5}}{2}\right)^n + b\left(\frac{1-\sqrt{5}}{2}\right)^n$ também satisfazem a recorrência acima.

Basta agora encontrar valores de a e b tais que $y_0 = 0$ e $y_1 = 1$ para que tenhamos $y_n = F_n$ para todo n (de fato, teríamos $y_0 = F_0$, $y_1 = F_1$ e, por indução se $k \geq 2$ e $y_n = F_n$ para todo $n < k$, temos $y_k = y_{k-1} + y_{k-2} = F_{k-1} + F_{k-2} = F_k$). 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

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

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

Provaremos a seguir uma identidade útil sobre números de Fibonacci:

Proposição 1. $F_{m+n} = F_m F_{n-1} + F_{m+1} F_n$, $\forall m, n \in \mathbb{N}$, $n \geq 1$.

Demonstração. Sejam $y_m = F_{m+n}$ e $z_m = F_m F_{n-1} + F_{m+1} F_n$. Temos que (y_n) e (z_n) satisfazem a recorrência $x_{n+2} = x_{n+1} + x_n$, $\forall n \in \mathbb{N}$. Por outro lado, $y_0 = F_n$, $y_1 = F_{n+1}$, $z_0 = 0 \cdot F_{n-1} + 1 \cdot F_n = F_n = y_0$ e $z_1 = 1 \cdot F_{n-1} + 1 \cdot F_n = F_{n+1} = y_1$, 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 sequência (F_n), que pode ser generalizado para as chamadas sequências de Lucas, as quais são úteis para certos testes de primalidade:

Teorema 2. $\text{mdc}(F_m, F_n) = F_{\text{mdc}(m,n)}$, $\forall m, n \in \mathbb{N}$.

Demonstração. Observemos primeiro que $\text{mdc}(F_n, F_{n+1}) = 1$, $\forall n \in \mathbb{N}$. Isso vale para $n = 0$ pois $F_1 = 1$ e, por indução,

$$\text{mdc}(F_{n+1}, F_{n+2}) = \text{mdc}(F_{n+1}, F_{n+1} + F_n) = \text{mdc}(F_{n+1}, F_n) = 1.$$

Além disso, se $m = 0$, $\text{mdc}(F_m, F_n) = \text{mdc}(0, F_n) = F_n = F_{\text{mdc}(m,n)}$, $\forall n \in \mathbb{N}$, e se $m = 1$, $\text{mdc}(F_m, F_n) = \text{mdc}(1, F_n) = 1 = F_1 = F_{\text{mdc}(m,n)}$, $\forall n \in \mathbb{N}$. 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 $\text{mdc}(F_k, F_n) = F_{\text{mdc}(k,n)}$ para todo $n \in \mathbb{N}$. Faremos isso por indução em n. Note que, se $n < k$, $\text{mdc}(F_k, F_n) = \text{mdc}(F_n, F_k) = F_{\text{mdc}(n,k)} = F_{\text{mdc}(k,n)}$, por hipótese de indução (sobre m). Já se $n \geq k$, $F_n = F_{(n-k)+k} = F_{n-k} F_{k-1} + F_{n-k+1} F_k$, e logo $\text{mdc}(F_k, F_n) = \text{mdc}(F_k, F_{n-k} F_{k-1} + F_{n-k+1} F_k) = \text{mdc}(F_k, F_{n-k} F_{k-1}) = \text{mdc}(F_k, F_{n-k})$ (pois $\text{mdc}(F_k, F_{k-1}) = 1$) $= F_{\text{mdc}(k,n-k)} = F_{\text{mdc}(k,n)}$. □

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

1.1 Testes de Primalidade Baseados em Fatorações de $n - 1$

Veremos inicialmente alguns algoritmos determinísticos que funcionam para valores especiais de n, para os quais uma fatoração (talvez incompleta) de $n-1$ é conhecida.

Proposição 4. *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.*

Demonstração. Seja q^{k_q} a maior potência de q que divide $n - 1$. A ordem de a_q em $(\mathbb{Z}/(n))^\times$ 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 5 (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 $\text{mdc}(a^{(n-1)/q} - 1, n) = 1$ então qualquer fator primo de n é côngruo a 1 módulo q^k.*

Demonstração. 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, $q^k \mid \mathrm{ord}_p\, a \mid p-1$, donde $p \equiv 1 \pmod{q^k}$. □

Corolário 6. *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.*

Demonstração. 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 consequências 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. Até outubro de 2011 o menor número de Fermat que se desconhece se é primo ou composto é F_{33}, 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 7 (Teste de Pépin)**.** *Seja $F_n = 2^{2^n} + 1$; F_n é primo se, e somente se, $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.*

Demonstração. Se $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ então a primalidade de F_n segue da Proposição 4. Por outro lado, se F_n é primo então pelo critério de Euler e a lei de reciprocidade quadrática temos

$$3^{(F_n-1)/2} \equiv \left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1 \pmod{F_n}$$

□

Teorema 8 (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 $a^{(n-1)/2} \equiv -1 \pmod{n}$.*

Demonstração. Se n é primo, podemos tomar a qualquer com $\left(\frac{a}{n}\right) = -1$; ou seja, metade dos inteiros entre 1 e $n-1$ serve como a. A recíproca segue do corolário 6 com $F = 2^k$. □

Corolário 9. *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 $\mathrm{mdc}(a^{(n-1)/q} - 1, n) = 1$.*

Demonstração. Se n é primo, podemos tomar a qualquer que não seja da forma x^q módulo n (que existe pois n admite raiz primitiva); ou seja, uma proporção de $(q-1)/q$ dentre os inteiros entre 1 e $n-1$ serve como a. A recíproca segue do corolário 6 com $F = q^k$. □

Muitos dentre os maiores primos conhecidos estão nas condições do teorema de Proth. Isto se deve ao fato de primos desta forma serem frequentes (mais frequentes do que, por exemplo, primos de Mersenne) e que sua primalidade é facilmente demonstrada usando este resultado.

2 Extensões Quadráticas

Seja d um inteiro que não é um quadrado perfeito. O conjunto

$$\mathbb{Z}[\sqrt{d}] \stackrel{\text{def}}{=} \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

é um subanel de $\mathbb{C}$: este conjunto é claramente fechado por soma e subtração e também por produto, já que

$$(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d}.$$

Como no caso dos inteiros de Gauß e Eisenstein, podemos tentar estender o estudo de propriedades aritméticas a este anel também. Alguns conceitos se estendem de forma imediata. Por exemplo, podemos definir divisibilidade da maneira usual: dados $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$,

$$\alpha \mid \beta \iff \text{existe } \gamma \in \mathbb{Z}[\sqrt{d}] \text{ tal que } \beta = \alpha\gamma.$$

Da mesma forma, definimos a relação de congruência

$$\alpha \equiv \beta \pmod{\delta} \iff \delta \mid \alpha - \beta$$

e o anel quociente $\mathbb{Z}[\sqrt{d}]/(\delta)$, cujos elementos são as classes de congruência módulo δ. Por exemplo, temos a seguinte generalização do pequeno teorema de Fermat:

Teorema 10. *Seja $p \in \mathbb{Z}$ um número primo tal que $p \neq 2$ e $p \nmid d$. Para todo elemento $\alpha \in \mathbb{Z}[\sqrt{d}]$,*

$$\alpha^{p^2} \equiv \alpha \pmod{p}.$$

Demonstração. Escrevendo $\alpha = a + b\sqrt{d}$ com $a, b \in \mathbb{Z}$, temos

$$\alpha^p = (a + b\sqrt{d})^p = \sum_{0 \leq i \leq p} \binom{p}{i} a^{p-i}(b\sqrt{d})^i \equiv a^p + b^p(\sqrt{d})^p \pmod{p}$$

pois $p \mid \binom{p}{i}$ para $i = 1, 2, \ldots, p-1$. Porém, pelo pequeno teorema de Fermat, $p \mid a^p - a$ e $p \mid b^p - b$ em $\mathbb{Z}$ (e portanto em $\mathbb{Z}[\sqrt{d}]$ também). Assim,

$$\alpha^p \equiv a + b \cdot (\sqrt{d})^p \pmod{p}.$$

Elevando novamente a p, obtemos portanto

$$\alpha^{p^2} \equiv a + b \cdot (d^{p-1})^{(p+1)/2}\sqrt{d} \pmod{p}.$$

Como $p \neq 2$ e $p \nmid d$, temos que $(p+1)/2$ é inteiro e pelo pequeno teorema de Fermat $(d^{p-1})^{(p+1)/2} \equiv 1 \pmod{p}$. Assim, $\alpha^{p^2} \equiv \alpha \pmod{p}$. □

Se n é um inteiro positivo, temos que o anel $\mathbb{Z}[\sqrt{d}]/(n)$ possui n^2 elementos:

$$\mathbb{Z}[\sqrt{d}]/(n) = \left\{\overline{a + b\sqrt{d}} \mid a, b = 0, 1, 2, \ldots, n-1\right\}.$$

A seguinte proposição fornece um critério para decidir quando este anel é um corpo:

Proposição 11. *Seja p um primo tal que $p \nmid d$. Então $\mathbb{Z}[\sqrt{d}]/(p)$ é um corpo (com p^2 elementos) se, e somente se, $\left(\frac{d}{p}\right) = -1$.*

Demonstração. Suponha inicialmente que $\left(\frac{d}{p}\right) = -1$ e seja $a+b\sqrt{d} \not\equiv 0 \pmod{p}$, $a, b \in \mathbb{Z}$, ou seja, ou a ou b não é divisível por p. Temos que $a^2 - b^2 d$ é invertível módulo p: isto é claro se $b \equiv 0 \pmod{p}$ (pois neste caso $a \not\equiv 0 \pmod{p}$); e se $b \not\equiv 0 \pmod{p}$ então $a^2 - b^2 d \equiv 0 \pmod{p} \implies (\frac{a}{b})^2 \equiv d \pmod{p}$, o que contradiz $\left(\frac{d}{p}\right) = -1$. Logo

$$(a + b\sqrt{d}) \cdot \frac{a - b\sqrt{d}}{a^2 - b^2 d} \equiv 1 \pmod{p}$$

mostra que $a + b\sqrt{d}$ também é invertível módulo p, logo $\mathbb{Z}[\sqrt{d}]/(p)$ é corpo.

Reciprocamente, se $\left(\frac{d}{p}\right) = 1$ e $a^2 \equiv d \pmod{p}$, $a \in \mathbb{Z}$, então $a \pm \sqrt{d} \bmod p$ seriam não nulos em $\mathbb{Z}[\sqrt{d}]/(p)$ mas não teriam inversos pois

$$(a + \sqrt{d})(a - \sqrt{d}) \equiv 0 \pmod{p}.$$

□

Quando $d \equiv 1 \pmod{4}$, podemos definir também o subanel de $\mathbb{C}$

$$\mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big] \stackrel{\text{def}}{=} \left\{a + b \cdot \frac{1+\sqrt{d}}{2} \;\Big|\; a, b \in \mathbb{Z}\right\}$$

que é claramente fechado por soma e subtração, mas também produto: note que $\theta = \frac{1+\sqrt{d}}{2}$ satisfaz a equação mônica com coeficientes inteiros

$$\theta^2 - \theta + \frac{1-d}{4} = 0 \iff \theta^2 = \theta + \frac{d-1}{4}$$

de modo que

$$(a_1 + b_1\theta)(a_2 + b_2\theta) = \left(a_1 a_2 + b_1 b_2 \cdot \frac{d-1}{4}\right) + (a_1 b_2 + a_2 b_1 + b_1 b_2) \cdot \theta.$$

Exemplo 12. *Seja F_n o n-ésimo número de Fibonacci e $p \neq 5$ um número primo. Mostre que $p \mid F_{p^2-1}$.*

SOLUÇÃO: O resultado é claro para $p = 2$, logo podemos assumir que $p \neq 2, 5$. Sejam $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2} = 1 - \alpha$ as raízes do polinômio $x^2 - x - 1$. Trabalhando no anel $\mathbb{Z}[\alpha]$, basta mostrar que

$$F_{p^2-1} = \frac{\alpha^{p^2-1} - \beta^{p^2-1}}{\alpha - \beta} \equiv 0 \pmod{p}$$

pois se F_{p^2-1} é múltiplo de p em $\mathbb{Z}[\alpha]$, então F_{p^2-1} é múltiplo de p em $\mathbb{Z}$: se $a, b \in \mathbb{Z}$ são tais que $F_{p^2-1} = p \cdot (a + b\alpha)$, então $b = 0$ e $F_{p^2-1} = pa$ pois 1 e α são linearmente independentes sobre $\mathbb{Q}$ (i.e., $\alpha \notin \mathbb{Q}$). Note ainda que $\alpha - \beta = \sqrt{5}$ é invertível módulo p pois $(\sqrt{5})^{2(p-1)} \equiv 1 \pmod{p}$ pelo pequeno teorema de Fermat. Assim, o problema se resume a mostrar que

$$\alpha^{p^2-1} \equiv \beta^{p^2-1} \pmod{p}.$$

Mas como na demonstração do teorema anterior, aplicando o fato de que $(x + y)^p \equiv x^p + y^p \pmod{p}$ e o pequeno teorema de Fermat ($p \neq 2, 5$ por hipótese), obtemos

$$\alpha^{p^2} \equiv \frac{1^{p^2} + (\sqrt{5})^{p^2}}{2^{p^2}} \pmod{p} \iff \alpha^{p^2} \equiv \frac{1+\sqrt{5}}{2} = \alpha \pmod{p}.$$

Como α é invertível em $\mathbb{Z}[\alpha]$ ($\alpha\beta = -1$), obtemos portanto $\alpha^{p^2-1} \equiv 1 \pmod{p}$. Analogamente, $\beta^{p^2-1} \equiv 1 \pmod{p}$, o que completa a prova. □

3 Sequências Recorrentes e Testes de Primalidade

Nesta seção veremos aplicações de certas sequências recorrentes lineares a testes de primalidade.

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

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

Tais sequências são denominadas *sequências de Lucas*. 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

$$U_{m+1} = \frac{PU_m + V_m}{2}, \qquad V_{m+1} = \frac{DU_m + PV_m}{2}$$

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 $m = \sum_{0 \le i < M} a_i 2^i$ com $a_i \in \{0, 1\}$, definimos

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

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

Lembramos (proposição 11) que se $p > 2$ é primo e d não é um quadrado módulo p então $K = \mathbb{Z}[\sqrt{d}]/(p)$ é um corpo com p^2 elementos. Além disso, em K temos pela fórmula do binômio que

$$(a + b)^p = a^p + b^p \qquad a, b \in K$$

já que p divide todos os coeficientes binomiais $\binom{p}{j}$ com $0 < j < p$.

Proposição 13. *Se n é primo e D não é um quadrado módulo n então $\alpha^n = \overline{\alpha}$ em $K = \mathbb{Z}[\sqrt{D}]/(n)$.*

Demonstração. Temos em K

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

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

Analogamente, 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 14. *Se n é primo ímpar, $\left(\frac{D}{n}\right) = -1$ e as sequências 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 $U_{n+1} \equiv 0 \pmod{n}$.

Demonstração. Acima. □

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

Proposição 15. *Se $n \neq 2$ é primo, $n \nmid Q$, $n \nmid D$ e D é quadrado módulo n então $U_{n-1} \equiv 0 \pmod{n}$.*

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

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

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

Proposição 16. *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 $m = n - \left(\frac{D}{n}\right)$.*

Demonstração. Vamos supor, por 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 17. *Seja $r \geq 1$ com $\mathrm{mdc}(r, Q) = 1$. 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 $\mathrm{ord}_r U$.

Demonstração. Observemos inicialmente que para todo $m, n \in \mathbb{N}$, $n \neq 0$ temos $U_{m+n} = U_m U_{n+1} - Q U_{m-1} U_n$. 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 $n = 0$, $U_{m+0} = U_m \cdot U_1 - Q U_{m-1} \cdot U_0$ (pois $U_1 = 1$ e $U_0 = 0$), e, para $m = 1$, $U_{m+1} = U_m \cdot U_2 - Q U_{m-1} \cdot U_1$ (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 consequência, se $r \mid U_m$ 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 $\text{mdc}(Q, r) = 1$ e $\text{mdc}(U_{\ell-1}, U_\ell)$ divide $Q^{\ell-1}$ (o que pode ser facilmente provado por indução a partir de $U_{\ell+1} = PU_\ell - QU_{\ell-1}$), donde $\text{mdc}(r, U_{\ell-1})$ 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). □

Observação 18. *Se* $\text{mdc}(r, Q) > 1$ *e* $\text{mdc}(d, D) = 1$ *então* U_k *não será múltiplo de* r *para nenhum* $k \geq 1$.

De fato, seja q *um fator primo de* $\text{mdc}(r, Q) > 1$. *Temos* $q \nmid P$, *caso contrário* $q \mid P^2 - 4Q = D$, *contradição. De* $U_{m+2} = PU_{m+1} - QU_m, \forall m \geq 0$, *e de* $U_1 = 1$, *segue que* $U_k \equiv P^{k-1} \pmod{q}, \forall k \geq 1$, *e, como* $q \nmid P$, *segue que* $q \nmid U_k, \forall k \geq 1$, *donde* $r \nmid U_k, \forall k \geq 1$.

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

Proposição 19. *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 sequência de Lucas* $U_n^{(r)}$ *associada a inteiros* $P^{(r)}, Q^{(r)}$ *e um inteiro* $m^{(r)}$ *primo com* N *com* $D^{(r)} = (P^{(r)})^2 - 4Q^{(r)} \equiv d(m^{(r)})^2 \pmod{N}$ *tal que* $N \mid U_{N+1}^{(r)}$ *e* $\text{mdc}(U_{\frac{N+1}{r}}^{(r)}, N) = 1$ *então cada fator primo* ℓ *de* N *satisfaz* $\ell \equiv \left(\frac{d}{\ell}\right) \pmod{F}$.

Demonstração. Se $F = r_1^{\alpha_1} r_2^{\alpha_2} \dots r_k^{\alpha_k}$ é a fatoração canônica de F então $\text{ord}_N U^{(r_i)} \mid N + 1$ para $1 \leq i \leq k$. Se ℓ é um fator primo de N, também temos $\text{ord}_\ell U^{(r_i)} \mid N + 1$. Como $\text{mdc}(N, U_{\frac{N+1}{r_i}}^{(r_i)}) = 1$ segue que $\ell \nmid U_{\frac{N+1}{r_i}}^{(r_i)}$, donde $\text{ord}_\ell U^{(r_i)} \nmid \frac{N+1}{r_i}$, e portanto $r_i^{\alpha_i}$ divide $\text{ord}_\ell U^{(r_i)}$ para $1 \leq i \leq k$. Por outro lado, $\text{ord}_\ell U^{(r_i)}$ divide $\ell - \left(\frac{d}{\ell}\right)$ (note que, pela observação acima, $\ell \nmid Q^{(r)}$), donde $r_i^{\alpha_i}$ divide $\ell - \left(\frac{d}{\ell}\right)$ para $1 \leq i \leq k \implies F$ divide $\ell - \left(\frac{d}{\ell}\right) \implies \ell \equiv \left(\frac{d}{\ell}\right) \pmod{F}$. □

Corolário 20. *Nas condições da proposição, se* $F > R$ *então* N *é primo.*

Demonstração. 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 21. *Seja* $n > 1$ *um inteiro ímpar. Se para todo fator primo* r *de* $n+1$ *existem* $P^{(r)}, Q^{(r)}$ *inteiros com* $\text{mdc}(D^{(r)}, n) = 1$ *onde* $D^{(r)} = (P^{(r)})^2 - 4Q^{(r)}$

tais que a sequência 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.*

Demonstração. 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 $\ell - \left(\frac{D^{(r)}}{\ell}\right)$, 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 uma prova do critério de Lucas-Lehmer usando os resultados anteriores.

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

Teorema 22. *Seja* S_k *a sequência 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.

Demonstração. A sequência 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

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

(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 algum fator de M_n divide $U_{\frac{M_n+1}{2}}$, divide também $2^{2^{n-1}+2}$, logo é igual a 1. Assim, pela proposição anterior, M_n é primo (note que, de $V_{2^{n-1}}^2 - 12U_{2^{n-1}}^2 = 2^{2^{n-1}+2}$ e de $M_n \mid V_{2^{n-1}}$ segue que $\mathrm{mdc}(M_n, D) = \mathrm{mdc}(M_n, 12) = 1$).

Por outro lado, se M_n é primo, como $D = 12$, $\left(\frac{12}{M_n}\right) = \left(\frac{3}{M_n}\right) = -\left(\frac{M_n}{3}\right) = -1$ (já sabemos que n deve ser um primo ímpar), logo M_n divide $U_{M_n+1} = U_{2^n}$, e, como

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

pois $2 \equiv 2^{n+1} \equiv (2^{\frac{n+1}{2}})^2 \pmod{M_n}$. 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 $K = \mathbb{Z}[\sqrt{3}]/(M_n)$ (pois $\left(\frac{3}{M_n}\right) = -1$) 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 demonstração do critério de Lucas-Lehmer. □

Se N é um primo ímpar e d não é quadrado módulo N, então $K = \mathbb{Z}[\sqrt{d}]/(N)$ 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 $\left(\frac{D}{N}\right) = -1$. Pela proposição 14, $U_{N+1} \equiv 0 \pmod{N}$. 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 13, $\overline{x} = x^N$, logo $x^{(N-1)m} = 1$, absurdo, pois $\mathrm{ord}_K\, x = N^2 - 1 = (N - 1)(N + 1) > (N - 1)m$. Assim, $\mathrm{ord}_N\, U = N + 1$. Isto fornece recíprocas para vários resultados desta seção.

Problemas Propostos

Problema 23 (Lucas-Lehmer-Riesel)**.** *Sejam a e $M_{n,a} = a \cdot 2^n - 1$ números primos com 6 tais que $2^n > a$. Definimos recursivamente a sequência $\{S_j\}$ onde $S_0 = (2 + \sqrt{3})^a + (2 - \sqrt{3})^a$ e $S_{j+1} = S_j^2 - 2$. Mostre que $M_{n,a}$ é primo se, e somente se, S_{n-2} é divisível por $M_{n,a}$.*

Dicas e Soluções

Em breve

Referências

[1] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha, E. Tengan - Teoria dos Números - um passeio com primos e outros números familiares pelo mundo inteiro, Projeto Euclides, IMPA, 2010.