Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 3

Carlos Gustavo Moreira

Aula 6

Teoremas de Fermat, Wilson, Wolstenholme e Euler

1 Os teoremas de Wilson e Wolstenholme

Uma aplicação do inverso multiplicativo é o famoso *teorema de Wilson*. Primeiramente precisamos de um lema.

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

Demonstração. Temos

$$\begin{aligned} x^2 \equiv 1 \pmod{p} &\iff p \mid (x^2 - 1) \iff p \mid (x-1)(x+1) \\ &\iff p \mid x-1 \text{ ou } p \mid x+1 \\ &\iff x \equiv 1 \pmod{p} \text{ ou } x \equiv -1 \pmod{p} \end{aligned}$$

donde o resultado segue. □

Teorema 2 (Wilson). *Seja $n > 1$. Então $n \mid (n-1)! + 1$ se, e somente se, n é primo. Mais precisamente,*

$$(n-1)! \equiv \begin{cases} -1 \pmod{n} & \text{se } n \text{ é primo} \\ 0 \pmod{n} & \text{se } n \text{ é composto e } n \neq 4. \end{cases}$$

Demonstração. 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 são fatores de $(n-1)!$ e portanto $(n-1)! \equiv 0 \pmod{n}$. Se $n = p^2$, $p > 2$, então p e $2p$ são fatores de $(n-1)!$ e novamente $(n-1)! \equiv 0 \pmod{n}$; isto demonstra que para todo $n \neq 4$ composto temos $(n-1)! \equiv 0 \pmod{n}$.

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

Vejamos uma aplicação do teorema de Wilson.

Teorema 3 (Teorema de Wolstenholme). *Seja $p > 3$ um número primo. Então o numerador do número*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

é divisível por p^2.

Demonstração. Note que somando os "extremos" temos

$$\sum_{1 \le i \le p-1} \frac{1}{i} = \sum_{1 \le i \le \frac{p-1}{2}} \left(\frac{1}{i} + \frac{1}{p-i} \right) = p \sum_{1 \le i \le \frac{p-1}{2}} \frac{1}{i(p-i)}.$$

Como o mmc dos números de 1 a $p-1$ não é divisível por p, basta mostrar que o numerador da última soma é múltiplo de p. Equivalentemente, como $p \nmid (p-1)!$, devemos mostrar que o inteiro

$$S \stackrel{\text{def}}{=} \sum_{1 \le i \le \frac{p-1}{2}} \frac{(p-1)!}{i(p-i)}$$

é um múltiplo de p. Para $1 \le i \le p-1$, denote por r_i o inverso de i mod p, ou seja, $ir_i \equiv 1 \pmod{p}$. Note que $r_{p-i} \equiv -r_i \pmod{p}$, assim

$$\begin{aligned} S &\equiv \sum_{1 \le i \le \frac{p-1}{2}} \frac{(p-1)!}{i(p-i)} \cdot ir_i(p-i)r_{p-i} \\ &\equiv \sum_{1 \le i \le \frac{p-1}{2}} (p-1)! r_i r_{p-i} \equiv \sum_{1 \le i \le \frac{p-1}{2}} r_i^2 \pmod{p} \end{aligned}$$

pelo teorema de Wilson. Note que como cada r_i é congruente a um dos números $\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}$, temos que os r_i^2 são congruentes a um dos números $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ módulo p. Vamos mostrar que todos eles aparecem. De fato, se $r_i^2 \equiv r_j^2 \pmod{p}$, então $p \mid (r_i - r_j)(r_i + r_j)$, isto é, $r_i \equiv \pm r_j \pmod{p}$. Multiplicando por ij, temos que $j \equiv \pm i \pmod{p}$, o implica $i = j$ pois $1 \le i, j \le \frac{p-1}{2}$.

Assim, $S \equiv \sum_{1 \le i \le \frac{p-1}{2}} i^2 \pmod{p}$ e como $\sum_{1 \le i \le \frac{p-1}{2}} i^2 = \frac{p(p^2-1)}{24}$ é um múltiplo de p (pois $\text{mdc}(p, 24) = 1$), o resultado segue. □

O teorema de Wilson produz ainda resultados interessantes sobre os coeficientes binomiais. Suponhamos que k e h são inteiros positivos tais que $k + h = p - 1$ onde p é primo. Então

$$\begin{aligned} h!k! &\equiv (-1)^h (p-1)(p-2)\cdots(p-h)k! = (-1)^k (p-1)! \\ &\equiv (-1)^{k+1} \pmod{p}. \end{aligned}$$

Portanto

$$\begin{aligned} & h!k!\binom{p-1}{k} \equiv (p-1)! \pmod{p} \\ \iff & (-1)^{k+1}\binom{p-1}{k} \equiv -1 \pmod{p} \\ \iff & \binom{p-1}{k} \equiv (-1)^k \pmod{p}. \end{aligned}$$

Exemplo 4. *Demonstre que se $p > 3$ é primo, então $p^3 \mid \binom{2p}{p} - 2$.*

SOLUÇÃO: Primeiramente, vamos relembrar algumas identidades com coeficientes binomiais bem conhecidas. Para todo $1 \leq i \leq p-1$, temos que $\binom{p}{i} = \frac{p}{i}\binom{p-1}{i-1}$ (basta utilizar a definição) enquanto que

$$\binom{2p}{p} = \binom{p}{0}^2 + \binom{p}{1}^2 + \cdots + \binom{p}{p}^2$$

pois podemos escolher p objetos dentre $2p$ escolhendo i objetos dentre os p primeiros e $p-i$ dos p últimos para todo i entre 0 e p, logo

$$\binom{2p}{p} = \sum_{0 \leq i \leq p} \binom{p}{i}\binom{p}{p-i} = \sum_{0 \leq i \leq p} \binom{p}{i}^2.$$

Utilizando estas identidades, temos que

$$\binom{2p}{p} - 2 = \sum_{1 \leq i \leq p-1} \frac{p^2}{i^2}\binom{p-1}{i-1}^2 = p^2 \sum_{1 \leq i \leq p-1} \frac{1}{i^2}\binom{p-1}{i-1}^2.$$

Note que $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ é um múltiplo de p para $1 \leq i \leq p-1$ pois o denominador desta fração não é divisível por p. Assim, $\frac{1}{i^2}\binom{p-1}{i-1}^2 = \frac{1}{p^2}\binom{p}{i}^2$ é inteiro e portanto a soma $\sum_{1 \leq i \leq p-1} \frac{1}{i^2}\binom{p-1}{i-1}^2$ é inteira e devemos mostrar que ela é um múltiplo de p. Para isto, observemos que cada i ($1 \leq i \leq p-1$) é invertível módulo p; seja r_i tal que $1 \leq r_i \leq p-1$ e $ir_i \equiv 1 \pmod{p}$. Pela unicidade de r_i módulo p, temos que os r_i's formam uma permutação de $1, 2, \ldots, p-1$. Assim, como $\binom{p-1}{i-1} \equiv (-1)^{i-1} \pmod{p}$, temos

$$\sum_{1 \leq i \leq p-1} \frac{1}{i^2}\binom{p-1}{i-1}^2 \equiv \sum_{1 \leq i \leq p-1} \frac{(ir_i)^2}{i^2}\binom{p-1}{i-1}^2 \pmod{p}$$

$$\iff \sum_{1 \leq i \leq p-1} \frac{1}{i^2}\binom{p-1}{i-1}^2 \equiv \sum_{1 \leq i \leq p-1} r_i^2 = \sum_{1 \leq i \leq p-1} i^2 \pmod{p}.$$

Como $\sum_{1 \leq i \leq p-1} i^2 = \frac{p(p-1)(2p-1)}{6}$ é um múltiplo de p (pois $\mathrm{mdc}(p, 6) = 1$), a prova acaba. □

2 A Função de Euler e o Teorema de Euler-Fermat

Dizemos que um conjunto de n números inteiros $a_1, \ldots, a_n$ forma um *sistema completo de restos módulo n* (scr) 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 scr módulo n. Equivalentemente, podemos

dizer que $a_1, a_2, \ldots, a_n$ formam um scr módulo n se, e somente se, $a_i \equiv a_j \pmod{n}$ implicar $i = j$.

De igual forma, dizemos que os números inteiros $b_1, b_2, \ldots, b_{\varphi(n)}$ formam um *sistema completo de invertíveis módulo n* (sci) se

$$\{\overline{b}_1, \overline{b}_2, \ldots, \overline{b}_{\varphi(n)}\} = (\mathbb{Z}/(n))^{\times},$$

onde $\varphi(n)$ representa o número de elementos de $(\mathbb{Z}/(n))^{\times}$. Em outras palavras, $b_1, b_2, \ldots, b_{\varphi(n)}$ formam um sci módulo n se, e somente se, representam todas as classes de congruência invertíveis módulo n ou, equivalentemente, $\text{mdc}(b_i, n) = 1$ para todo i e $b_i \equiv b_j \pmod{n}$ implica $i = j$. O conjunto $\{k \in \mathbb{Z} \mid 1 \leq k \leq n \text{ e } \text{mdc}(n, k) = 1\}$ é um exemplo de sci módulo n.

Definição 5. *A função*

$$\varphi(n) \stackrel{\text{def}}{=} |(\mathbb{Z}/n\mathbb{Z})^{\times}|$$

é chamada de função phi 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 $\text{mdc}(a, p^k) = 1$ se, e somente se, a não é múltiplo de p e há p^{k-1} múltiplos de p no intervalo $1 \leq a \leq p^k$. Para calcular a função φ no caso geral, vamos mostrar que se $\text{mdc}(n, m) = 1$, então $\varphi(nm) = \varphi(n)\varphi(m)$. Consideremos os números $1, 2, \ldots, nm$, onde $\text{mdc}(n, m) = 1$ e os arrumamos em forma matricial assim:

$$\begin{array}{ccccc} 1 & 2 & 3 & \ldots & n \\ n+1 & n+2 & n+3 & \ldots & 2n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n(m-1)+1 & n(m-1)+2 & n(m-1)+3 & \ldots & n(m-1)+n \end{array}$$

Note que, como $\text{mdc}(ni + j, n) = \text{mdc}(j, n)$, se um número nesta tabela é primo relativo com n, então todos os números nessa coluna são primos relativos com n. Logo, existem $\varphi(n)$ colunas nas quais todos os números são primos relativos com n. Por outro lado, toda coluna possui um conjunto completo de restos módulo m: se duas entradas são tais que $ni_1 + j \equiv ni_2 + j \pmod{m}$, então $i_1 \equiv i_2 \pmod{m}$ pois n é invertível módulo m já que $\text{mdc}(m, n) = 1$, logo como $0 \leq i_1, i_2 < m$ devemos ter $i_1 = i_2$. Desta forma, em cada coluna existem exatamente $\varphi(m)$ números que são primos relativos com m e portanto, o total de números nesta tabela que são simultaneamente primos relativos com m e n (i.e. primos com nm) é $\varphi(nm) = \varphi(n)\varphi(m)$.

Assim, se $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ é a fatoração de n em potências de primos distintos p_i, temos que

$$\varphi(n) = \prod_{1 \leq i \leq k} \varphi(p_i^{\alpha_i}) = \prod_{1 \leq i \leq k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{1 \leq i \leq k} \left(1 - \frac{1}{p_i}\right).$$

Agora estamos prontos para enunciar e provar o importante

Teorema 6 (Euler-Fermat). *Sejam a e $m > 0$ são dois inteiros com* $\text{mdc}(a, m) = 1$*, então*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Demonstração. Observemos que se $r_1, r_2, \ldots, r_{\varphi(m)}$ é um sistema completo de invertíveis módulo m e a é um número natural tal que $\text{mdc}(a, m) = 1$, então $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ também é um sistema completo de invertíveis módulo m. De fato, temos que $\text{mdc}(ar_i, m) = 1$ para todo i e se $ar_i \equiv ar_j \pmod{m}$, então $r_i \equiv r_j \pmod{m}$ pois a é invertível módulo m, logo $r_i = r_j$ e portanto $i = j$. Consequentemente cada ar_i deve ser congruente com algum r_j e, portanto,

$$\prod_{1 \le i \le \varphi(m)} (ar_i) \equiv \prod_{1 \le i \le \varphi(m)} r_i \pmod{m}$$
$$\iff a^{\varphi(m)} \cdot \prod_{1 \le i \le \varphi(m)} r_i \equiv \prod_{1 \le i \le \varphi(m)} r_i \pmod{m}.$$

Mas como cada r_i é invertível módulo m, simplificando o fator $\prod_{1 \le i \le \varphi(m)} r_i$, obtemos o resultado desejado. □

Como caso particular do teorema anterior obtemos o

Teorema 7 (Pequeno Teorema de Fermat)**.** *Seja a um inteiro positivo e p um primo, então*

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

Demonstração. De fato, observemos que se $p \mid a$ o resultado é evidente. Então, podemos supor que $\text{mdc}(a, p) = 1$. Como $\varphi(p) = p - 1$, pelo teorema de Euler temos $a^{p-1} \equiv 1 \pmod{p}$, logo multiplicando por a obtemos o resultado desejado. □

Observação 8. *O teorema de Euler-Fermat também pode ser provado utilizando-se o seguinte corolário do teorema de Lagrange em Teoria dos Grupos: se G é um grupo finito e $g \in G$, então $g^{|G|} = e$ (identidade). Aplicando este resultado para $G = (\mathbb{Z}/m\mathbb{Z})^\times$, temos que $\overline{a}^{\varphi(m)} = \overline{1}$ para todo $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$, que é uma formulação equivalente para o teorema de Euler-Fermat.*

Observemos que o teorema de Euler-Fermat pode ser otimizado da seguinte forma:

Proposição 9. *Sejam a e n números inteiros tais que* $\text{mdc}(a, n) = 1$ *e n se fatora como $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ em potências de primos distintos. Então*

$$a^M \equiv 1 \pmod{n} \quad \text{onde} \quad M = \text{mmc}(\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), \ldots, \varphi(p_k^{\alpha_k})).$$

Demonstração. Pelo teorema de Euler-Fermat sabemos que $a^{\varphi(p_j^{\alpha_j})} \equiv 1 \pmod{p_j^{\alpha_j}}$ para todo $j = 1, \ldots k$. Elevando a $M/\varphi(p_j^{\alpha_j})$, obtemos $a^M \equiv 1 \pmod{p_j^{\alpha_j}}$. Assim, $a^M - 1$ é múltiplo de $p_j^{\alpha_j}$ para todo j, e como estes números são dois a dois primos entre si, concluímos que $n \mid a^M - 1 \iff a^M \equiv 1 \pmod{n}$, como desejado. □

Vejamos agora algumas aplicações do teorema de Euler-Fermat.

Exemplo 10. *Mostre que existem infinitos números da forma*

$$20000\ldots009$$

que são múltiplos de 2009*.*

Demonstração. O problema é equivalente a encontrar infinitos naturais k tais que

$$\begin{aligned} 2\cdot 10^k + 9 \equiv 0 \pmod{2009} &\iff 2\cdot 10^k + 9 \equiv 2009 \pmod{2009} \\ &\iff 10^{k-3} \equiv 1 \pmod{2009} \end{aligned}$$

pois 2000 é invertível módulo 2009. Como $\mathrm{mdc}(10, 2009) = 1$, pelo teorema de Euler-Fermat temos que $10^{\varphi(2009)} \equiv 1 \pmod{2009} \implies 10^{\varphi(2009)t} \equiv 1 \pmod{2009}$ para todo $t \in \mathbb{N}$, logo basta tomar $k = \varphi(2009)t + 3$. □

Exemplo 11. *Encontre um número $n \in \mathbb{N}$ tal que $2^n > 10^{2000}$ e 2^n tenha entre suas 2000 últimas casas decimais pelo menos 1000 zeros consecutivos.*

Solução: Sabemos que $2^{\varphi(5^{2000})} \equiv 1 \pmod{5^{2000}}$ pelo teorema de Euler-Fermat. Portanto existe $b \in \mathbb{N}$ com

$$2^{\varphi(5^{2000})} = 5^{2000}b + 1 \implies 2^{2000+\varphi(5^{2000})} = 10^{2000}b + 2^{2000}.$$

Logo os 2000 últimos dígitos de $2^{2000+\varphi(5^{2000})}$ coincidem com a representação decimal de 2^{2000}, que tem no máximo 667 dígitos pois $2^{2000} < (2^3)^{667} < 10^{667}$. Desta forma, há pelo menos $2000 - 667 = 1333$ zeros consecutivos dentre as 2000 últimas casas decimais de $2^{2000+\varphi(5^{2000})}$ e assim $n = \varphi(5^{2000}) + 2000 = 4\cdot 5^{1999} + 2000$ satisfaz as condições do enunciado. □

Exemplo 12. *Mostre que não existe inteiro x tal que $103 \mid x^3 - 2$.*

Solução: Note primeiramente que 103 é primo. Agora suponha que $x^3 \equiv 2 \pmod{103}$, de modo que $103 \nmid x$. Elevando ambos os lados desta congruência a $(103-1)/3 = 34$, obtemos $x^{102} \equiv 2^{34} \pmod{103}$ e sabemos pelo teorema de Euler-Fermat que $x^{102} \equiv 1 \pmod{103}$. Porém, fazendo as contas, obtemos que $2^{34} \equiv 46 \pmod{103}$, que é uma contradição. Logo não há inteiro x tal que $103 \mid x^3 - 2$. □

Utilizando o mesmo raciocínio do exemplo anterior, temos que se p é um primo tal que $p \equiv 1 \pmod 3$ e $p \nmid a$, então uma condição necessária para que $x^3 \equiv a \pmod p$ tenha solução em x é que $a^{(p-1)/3} \equiv 1 \pmod p$. Esta condição também é suficiente, pela existência de raízes primitivas módulo p, como mostraremos no final deste capítulo.

Exemplo 13. *Demonstre que se $p > 2$ é primo, então*

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv p + (p-1)! \pmod{p^2}.$$

SOLUÇÃO: Pelo pequeno teorema de Fermat, sabemos que $i^{p-1} \equiv 1 \pmod{p}$ para todo $1 \leq i \leq p-1$, isto é, que $i^{p-1} = k_i p + 1$ onde k_i é um inteiro. Assim, $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} = (k_1 + k_2 + \cdots + k_{p-1})p + p - 1$ e portanto devemos mostrar que $(k_1 + k_2 + \cdots + k_{p-1})p \equiv (p-1)! + 1 \pmod{p^2}$.

Multiplicando as equações $i^{p-1} = k_i p + 1$, temos

$$(k_1 p + 1)(k_2 p + 1) \cdots (k_{p-1} p + 1) = 1^{p-1} 2^{p-1} \cdots (p-1)^{p-1} = ((p-1)!)^{p-1}.$$

Por um lado, $(k_1 p + 1)(k_2 p + 1) \cdots (k_{p-1} p + 1) \equiv (k_1 + k_2 + \cdots + k_{p-1})p + 1 \pmod{p^2}$. Por outro, pelo teorema de Wilson sabemos que $(p-1)! \equiv -1 \pmod{p}$, ou seja, $(p-1)! = Kp - 1$ para algum K inteiro. Segue que

$$\begin{aligned}
&(k_1 + k_2 + \cdots + k_{p-1})p + 1 \equiv (Kp - 1)^{p-1} \pmod{p^2} \\
\implies &(k_1 + k_2 + \cdots + k_{p-1})p + 1 \equiv 1 - \binom{p-1}{1} Kp \pmod{p^2} \\
\implies &(k_1 + k_2 + \cdots + k_{p-1})p \equiv Kp \pmod{p^2} \\
\implies &(k_1 + k_2 + \cdots + k_{p-1})p \equiv (p-1)! + 1 \pmod{p^2}
\end{aligned}$$

o que encerra a prova. □

Concluímos esta seção apresentando brevemente uma aplicação do Teorema de Euler que tem particular interesse prático: a *Criptografia RSA*. Trata-se de um método de criptografia com chave pública, isto é, um método que permite a qualquer pessoa transmitir mensagens por uma via insegura (ou seja, que pode ser monitorada por espiões) de modo que, na prática, apenas o legítimo destinatário, que conhece uma *chave*, pode recuperar a mensagem original. A sigla vem dos nomes de Ron Rivest, Adi Shamir, e Leonard Adleman, que desenvolveram esse método.

Para isso, o receptor publica um inteiro N que é o produto de dois primos razoavelmente grandes p e q (aproximadamente da mesma ordem de grandeza); N é público mas a sua fatoração pq só é conhecida pelo receptor. O receptor também publica um expoente s (em geral não muito grande) com $\text{mdc}(s, (p-1)(q-1)) = 1$. O receptor calcula (usando o algoritmo de Euclides) o inverso de s mod $(p-1)(q-1) = \varphi(N)$, isto é, um natural $r < (p-1)(q-1)$ com $rs \equiv 1 \pmod{(p-1)(q-1)}$ (donde $rs = 1 + k\varphi(N)$, para algum natural k); esse r é chamado a *chave privada* da criptografia. Note que apesar de N e s serem públicos, não parece ser fácil calcular $\varphi(N)$ ou r (neste contexto, calcular $\varphi(N) = (p-1)(q-1)$ dado $N = pq$ é equivalente a fatorar N, i.e., a encontrar os fatores primos p e q).

Uma mensagem é um número natural $m < N$. O emissor envia (ou publica) $\tilde{m} := m^s \pmod{N}$, com $0 < \tilde{m} < N$. O receptor recupera m via

$$m \equiv \tilde{m}^r \pmod{N}.$$

Para verificar essa equivalência, podemos observar que

$$\tilde{m}^r \equiv (m^s)^r = m^{rs} = m^{1+k(p-1)(q-1)} = m \cdot (m^{p-1})^{k(q-1)} \equiv m \pmod{p}.$$

Note que, se $p \mid m$, os dois lados são 0 mod p, e, caso contrário, $m^{p-1} \equiv 1 \pmod{p}$; analogamente $\tilde{m}^r \equiv m \pmod{q}$, donde $\tilde{m}^r \equiv m \pmod{N}$. Essas tarefas são relativamente rápidas computacionalmente. Mais precisamente, veremos a seguir que existem algoritmos polinomiais para testar primalidade, assim como para as demais operações necessárias (veja o capítulo 7, especialmente a seção sobre o teste de Agrawal, Kayal e Saxena que garante que testar primalidade de um número da ordem de N leva tempo no máximo polinomial em $\log N$).

Se existem algoritmos polinomiais para testar primalidade, não é verdade que sejam conhecidos algoritmos polinomiais (e *determinísticos*) para obter primos "novos" de uma determinada ordem de grandeza. Pelo teorema dos números primos (capítulo 5 e apêndice A), para todo N grande, a probabilidade de um número escolhido ao acaso entre N e $2N$ ser primo é $(1 + o(1))/\log N$, o que implica que, se testarmos $C \log N$ números ao acaso entre N e $2N$, a probabilidade de algum deles ser primo é da ordem de $1 - \exp(-C(1 + o(1)))$, que está muito perto de 1 para C grande. Se ao invés de sortear números procurarmos o menor primo maior ou igual a N (testando um por um) então, novamente pelo teorema dos números primos, o número de tentativas será *em média* da ordem de $\log(n)$. Entretanto, há gaps bem maiores do que $\log N$ e sabe-se muito pouco sobre o tamanho dos gaps (para um primo p, o gap $g(p)$ é igual a $q - p$ onde q é o menor primo maior do que p). Por exemplo, Harald Cramér conjectura que $g(p) < C(\log(p))^2$ (para algum $C > 0$; [2]): se isto for verdade então o algoritmo proposto acima é realmente polinomial. Pode ser que outra estratégia permita encontrar primos sem demonstrar esta conjectura, mas nada de tempo polinomial é conhecido. Há um projeto Polymath sobre este assunto: veja o preprint [4] e as páginas indicadas juntamente nas referências. Ainda assim, podemos considerar que o problema de obter primos é razoavelmente fácil e rápido para aplicações práticas pois aí devemos permitir algoritmos que dependem de sorteios e que obtêm o que é pedido em tempo polinomial com probabilidade quase igual a 1. No interessante artigo de divulgação [6] é discutido o problema de gerar primos grandes, e em particular é apresentado um algoritmo que funciona em muitos casos e gera primos grandes, cuja primalidade pode ser verificada por critérios bem mais simples que o teste de Agrawal, Kayal e Saxena, como o teste de Pocklington (veja o capítulo 7).

Não se conhecem algoritmos polinomiais para fatorar inteiros (grandes). A maioria dos especialistas duvida que exista tal algoritmo mas é preciso enfatizar que a não-existência de um tal algoritmo não é um teorema. Mais do que isso: a não-existência de tal algoritmo implica diretamente em $P \neq NP$ (um dos mais importantes problemas em aberto da matemática) mas $P \neq NP$ não parece implicar a não existência do algoritmo.

Existe ainda a possibilidade de que não exista um algoritmo rápido, mas que ainda assim exista uma máquina (no sentido literal) capaz de fatorar inteiros rapidamente. De fato, a mecânica quântica parece permitir a construção de um *computador quântico* e Peter Shor encontrou um "algoritmo" que permite a um computador quântico fatorar inteiros em tempo polinomial [7]. Até 2010 foram construídos computadores quânticos mínimos, suficientes para fatorar o número 15 pelo algoritmo de Shor, mas insuficientes para números maiores [5].

Não é claro se será possível construir computadores quânticos maiores.

Resumindo, a criptografia RSA é eficiente e segura pois é muito mais rápido achar primos grandes do que fatorar números grandes e ele é bastante utilizado para encriptar mensagens transmitidas pela internet. Para mais informações sobre a criptografia RSA, veja [1].

Exemplo 14. *Sabendo que a chave pública de criptografia RSA são os números* $N = 24797$ *e* $s = 143$*, determine a chave privada.*

Solução: Vamos fatorar $N = 24797$ usando o método de Fermat que consiste em encontrar dois números a e b tais que $N = a^2 - b^2$. De fato, se $x_0 = \lfloor\sqrt{24797}\rfloor + 1 = 158$ temos

x_i	$\sqrt{x_i^2 - 24797}$
158	$\sqrt{167}$
159	22

,

logo $24797 = (159 + 22) \cdot (159 - 22) = 181 \cdot 137$. Observemos que o método de Fermat é computacionalmente efetivo quando os dois fatores do número estão próximos. Portanto $\varphi(24797) = \varphi(181) \cdot \varphi(137) = 180 \cdot 136 = 24480$. Segue que a chave privada é a solução da congruência $143x \equiv 1 \pmod{24480}$. Esta congruência pode ser resolvida usando o algoritmo estendido da divisão

resto	quociente	x
24480	$*$	0
143	$*$	1
27	171	-171
8	5	856
3	3	-2739
2	2	6634
1	1	-9073

Portanto a chave privada é $24480 - 9073 = 15407$.

□

Problemas Propostos

Problema 15. *Encontre um número positivo* $k < 50$ *tal que* $a^k \equiv 1 \pmod{99}$ *para todo inteiro* a *primo relativo com* 99*.*

Problema 16. *Mostre que para todo inteiro* a *temos que* $a^{561} \equiv a \pmod{561}$ *e* $a^{1105} \equiv a \pmod{1105}$*, mas* 561 *e* 1105 *não são primos, o que mostra que o recíproco do pequeno teorema de Fermat é falso.*

Problema 17. *Mostre que*

$$a^{12} \equiv b^{12} \pmod{91} \iff \text{mdc}(a, 91) = \text{mdc}(b, 91).$$

Problema 18 (OBM1991). *Demonstre que existem infinitos múltiplos de* 1991 *que são da forma* $19999\ldots99991$.

Problema 19. *Seja* $p > 2$ *um número primo. Demonstre que*

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

Problema 20 (AusPol1996). *Mostre que não existem inteiros não negativos* m, n *tais que* $m! + 48 = 48(m+1)^n$.

Problema 21. *Seja* p *um número primo. Demonstre que* $(p-1)! + 1$ *é uma potência de* p *se, e somente se,* $p = 2$, 3 *ou* 5.

Problema 22. *Demonstre que para todo número primo* $p > 3$, *o número* $\binom{np}{p} - n$ *é divisível por* p^{3+r} *onde* p^r *é a maior potência de* p *que divide* n.

Problema 23. *Demonstre que se* $\mathrm{mdc}(a, b) = 1$, *então todos os divisores primos ímpares de* $a^2 + b^2$ *são da forma* $4k + 1$.

Problema 24. *Demonstre que existem infinitos primos da forma* $4k + 1$.

Problema 25. *Sejam* m, n *inteiros positivos. Demonstre que* $4mn - m - n$ *nunca pode ser o quadrado de um número inteiro.*

Problema 26. *Demonstre que se* $p \mid (a^p - b^p)$, *então* $p^2 \mid (a^p - b^p)$.

Problema 27. *Demonstre que para cada inteiro positivo* n *existe um inteiro* m *tal que* 2^m *tem no mínimo* $\frac{2}{3}n - 1$ *zeros entre seus últimos* n *algarismos em notação base* 10.

Problema 28 (IMO2003). *Seja* p *um número primo ímpar. Demonstre que existe um primo* q *tal que para todo* n, *o número* $n^p - p$ *não é divisível por* q.

Problema 29. *Sem usar computador (mas podendo usar calculadora) e sabendo que os fatores de* n *estão perto um do outro, use o método de Fermat para determinar os fatores de*

(a) $n = 62236177$.

(b) $n = 6218583803$.

Problema 30. *Fatore (sem usar computador)* 801621073 *sabendo que tem três fatores primos: um muito pequeno e os outros dois muito próximos.*

Problema 31. *Encontre os fatores de* 521827 *sabendo que é produto de dois primos e* $\varphi(521827) = 520056$.

Problema 32. *Sabendo que a chave pública de criptografia RSA são os números* $N = 26549$ *e* $s = 101$, *determine a chave privada.*

Dicas e Soluções

15. Temos $99 = 3^2 \cdot 11$, $\varphi(3^2) = 6$ e $\varphi(11) = 10$, e, se $\text{mdc}(a, 99) = 1$ então $\text{mdc}(a, 3^2) = 1$ e $\text{mdc}(a, 11) = 1$. Como 30 é múltiplo de 6 e de 10, temos que, se $\text{mdc}(a, 99) = 1$, então $a^{30} \equiv 1 \pmod{3^2}$ e $a^{30} \equiv 1 \pmod{11}$, donde $a^{30} \equiv 1 \pmod{99}$.

16. Note que $561 = 3 \cdot 11 \cdot 17$, e 560 é múltiplo de $3 - 1$, de $11 - 1$ e de $17 - 1$. Analogamente, $1105 = 5 \cdot 13 \cdot 17$, e 560 é múltiplo de $5 - 1$, de $13 - 1$ e de $17 - 1$.

18. Note que $19999\ldots99991$, com n 9's é igual a $2 \cdot 10^{n+1} - 9$, e $1991 = 2 \cdot 10^3 - 9$, donde $2 \cdot 10^3 \equiv 9 \pmod{1991}$. Como $2^{k \cdot \varphi(1991)} \equiv 1 \pmod{1991}, \forall k \in \mathbb{N}$, temos $2 \cdot 10^{k \cdot \varphi(1991)+3} \equiv 9 \pmod{1991}, \forall k \in \mathbb{N}$, e logo $2 \cdot 10^{k \cdot \varphi(1991)+3} - 9$ é múltiplo de 1991, para todo $k \in \mathbb{N}$.

20. Temos que 48 divide $m!$, donde $m \geq 6$, e logo $m + 1 > 6$. Se $m + 1$ é composto, $m + 1$ divide $m!$, donde $m + 1$ divide 48, e logo $m + 1 \in \{8, 12, 16, 24, 48\}$. Em particular, $m + 1$ é par. Se $m + 1 > 8$, $m!$ e $48(m + 1)^n$ são múltiplos de 32, mas 48 não é, absurdo. Se $m + 1 = 8$, a equação fica $7! + 48 = 48 \cdot 8^n$, ou $106 = 8^n$, absurdo. Finalmente, se $m + 1$ é primo, pelo teorema de Wilson $m + 1$ divide $m! + 1$, donde $m + 1$ divide $m! + 48 - (m! + 1) = 47$, e logo $m + 1 = 47$. Teríamos então $46!/48 = 47^n - 1$. Em particular, n é par, senão $47^n \equiv 3 \pmod 4$, o que contradiria o fato de $46!/48$ ser múltiplo de 4. Por outro lado,

$$47^n - 1 = (1 + 2 \cdot 23)^n - 1 = 2n \cdot 23 + \binom{n}{2}(2 \cdot 23)^2 + \cdots \equiv 2n \cdot 23 \pmod{23^2},$$

e logo, como $46!/48$ é múltiplo de 23^2, n é múltiplo de 23, e, como n é par, $n \geq 46$, absurdo, pois $46!/48 + 1 < 47^{46}$.

21. Para todo $p \geq 5$ ímpar, a maior potência de 2 que divide $(p-1)!$ é maior ou igual a $2^{\frac{p+1}{2}}$, como pode ser provado facilmente por indução. Suponhamos que $(p - 1)! + 1 = p^r$. Temos então que $2^{\frac{p+1}{2}} \mid p^r - 1$. Se 2^k é a maior potência de 2 que divide $p + 1$ ou $p - 1$, e 2^s é a maior potência de 2 que divide r então a maior potência de 2 que divide $p^r - 1$ é 2^{k+s} caso r seja par (o que pode ser provado por indução em s), e é igual à maior potência de 2 que divide $p - 1$ (a qual é no máximo 2^k), caso r seja ímpar. Portanto, em qualquer caso, é no máximo $2^{k+s} = 2^k \cdot 2^s \leq (p + 1) \cdot r$. Como $(p - 1)! + 1 < p^p$ para todo $p \geq 2$, temos $r \leq p - 1$, donde $p^2 - 1 = (p + 1)(p - 1) \geq (p + 1)r \geq 2^{\frac{p+1}{2}}$. Por outro lado, $2^{\frac{p+1}{2}} > p^2 - 1$ para todo $p \geq 17$, como pode ser facilmente provado por indução. Assim, $p < 17$. Se $r \leq 12$ e $p \in \{11, 13\}$, a maior potência de 2 que divide $p^r - 1$ é no máximo $13^2 - 1 = 168$, e logo é no máximo 2^7, mas a maior potência de 2 que divide $10!$ (que por sua vez divide $12!$) é 2^8. Assim, $p < 11$. Para $p = 7$, deveríamos ter $7^r = 6! + 1 = 721$, absurdo. Para $p = 5$, devemos ter $5^r = 4! + 1 = 25$, o que vale para $r = 2$. Para $p = 3$, devemos ter $3^r = 2! + 1 = 3$, o que vale para $r = 1$, e, finalmente, para $p = 2$, devemos ter $2^r = 1! + 1 = 2$, o que vale para $r = 1$.

23. Seja p um primo ímpar que divide $a^2 + b^2$. Como $\text{mdc}(a, b) = 1$, então $p \nmid a$ ou $p \nmid b$. Suponhamos sem perda de generalidade que $p \nmid b$. Então b é invertível módulo p, e $(ab^{-1})^2 \equiv -1 \pmod{p}$. Se p fosse da forma $4k + 3$, teríamos $(ab^{-1})^{p-1} = ((ab^{-1})^2)^{2k+1} \equiv (-1)^{2k+1} = -1 \pmod{p}$, contradizendo o teorema de Euler-Fermat. Assim, p deve ser da forma $4k + 1$.

24. Suponha por absurdo que $p_1, p_2, \ldots, p_k$ sejam todos os primos da forma $4k + 1$. Seja $n = 2p_1p_2 \ldots p_k$. Temos que $n^2 + 1$ é ímpar, e portanto, pelo exercício anterior, qualquer fator primo de $n^2 + 1$ deve ser da forma $4k+1$, ou seja, deve ser algum dos p_j, absurdo, pois $n^2 + 1 \equiv 1 \pmod{p_j}$ para todo j.

25. Temos $4mn-m-n = ((4m-1)(4n-1)-1)/4$. Assim, se $4mn-m-n = k^2$, teríamos $(2k)^2 + 1 = 4k^2 + 1 = (4m - 1)(4n - 1)$. Assim, $4m - 1$ é um inteiro positivo congruente a 3 módulo 4, que deve necessariamente ter algum fator primo p congruente a 3 módulo 4, mas p dividiria $(2k)^2 + 1$, contradizendo o exercício 23.

28. Seja $N = (p^p - 1)/(p - 1) = 1 + p + p^2 + \cdots + p^{p-1} \equiv p + 1 \not\equiv 1 \pmod{p^2}$. Então N tem um fator primo q com $q \not\equiv 1 \pmod{p^2}$. Temos que $p^p \equiv 1 \pmod{q}$, mas $p \not\equiv 1 \pmod{q}$, senão $N = 1 + p + p^2 + \cdots + p^{p-1} \equiv 1+1+1+\cdots+1 = p \pmod{q}$, donde $q \mid p$, e logo $p = q \mid N$, contradição, pois $N \equiv 1 \pmod{p}$. Suponha agora que $q \mid n^p - p$ para algum inteiro n. Então $n^p \equiv p \not\equiv 1 \pmod{q}$, e $n^{p^2} \equiv p^p \equiv 1 \pmod{q}$. Pelo teorema de Euler-Fermat, também temos $n^{q-1} \equiv 1 \pmod{q}$. Como $q \not\equiv 1 \pmod{p^2}$, $\text{mdc}(p^2, q - 1) \mid p$, e logo existem x, y inteiros com $p^2x + (q - 1)y = p$, e $n^p = (n^{p^2})^x (n^{q-1})^y \equiv 1^x 1^y = 1 \pmod{q}$, absurdo.

30. Procurando fatores primos pequenos descobrimos que $801621073 = 11 \cdot 72874643$. Temos $\lfloor\sqrt{72874643}\rfloor + 1 = 8537$, $\sqrt{8537^2 - 72874643} \notin \mathbb{N}$ mas $\sqrt{8538^2 - 72874643} = 151$, donde $72874643 = (8538+151)(8538-151) = 8689 \cdot 8387$, e logo $801621073 = 11 \cdot 8387 \cdot 8689$. É possível verificar que 8387 e 8689 são de fato primos.

32. Fatoremos 26549: temos $\lfloor\sqrt{26549}\rfloor + 1 = 163$, $\sqrt{163^2 - 26549} \notin \mathbb{N}$, $\sqrt{164^2 - 26549} \notin \mathbb{N}$ mas $\sqrt{165^2 - 26549} = 26$, donde $26549 = (165 - 26)(165 + 26) = 139 \cdot 191$. É fácil verificar que 139 e 191 são de fato primos. Assim, $\varphi(26549) = 138 \cdot 190 = 26220$. Usando o algoritmo de Euclides podemos calcular o inverso de 101 módulo 26220, que é 12461 (de fato, $12461 \cdot 101 - 48 \cdot 26220 = 1$). Assim, a chave privada procurada é 12461.

Referências

[1] S. C. Coutinho, *Números inteiros e criptografia RSA*, Coleção Computação e Matemática, SBM e IMPA (2000).

[2] H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*, Acta Arithmetica 2: 23–46 (1936).

[3] 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.

[4] D. H. J. Polymath, *Deterministic methods to find primes*, preprint, `http://polymathprojects.files.wordpress.com/2010/07/polymath.pdf`; veja também `http://polymathprojects.org/2009/08/09/research-thread-ii-deterministic-way-to-find-primes/` e `http://michaelnielsen.org/polymath1/index.php? title=Finding_primes`

[5] A. Politi, J. C. F. Matthews, J. L. O'Brien, *Shor's Quantum Factoring Algorithm on a Photonic Chip*, Science 4 September 2009: Vol. 325. no. 5945, p. 1221.

[6] P. Ribenboim, *Selling primes*, Math. Mag. 68 (1995), 175–182. Traduzido como *Vendendo primos*, Rev. Mat. Univ. 22/23 (1997), 1–13.

[7] P. W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Comput. 26 (5), 1484-1509 (1997). Também em `arXiv:quant-ph/9508027v2`.