Por que você deveria ter resolvido o problema 2 da OBM 2007

Vamos fazer um tratado geral sobre raízes primitivas e resíduos quadráticos em geral e depois resolveremos o problema acima. Aproveitamos para tratar de outros assuntos às vezes esquecidos como o lema de Thue e apresentamos um teorema novinho do nosso amigo Hensel!

1. Polinômios mód p

Quando trabalhamos em um corpo (como por exemplo, os reais, os racionais e os números mód p), existe divisão euclidiana de polinômios e fatoração única. A divisão euclidiana vem diretamente do algoritmo da chave de divisão e o fato de que é possível dividir por qualquer $a \not\equiv 0 \pmod{p}$; a fatoração única vem do fato de que se $f(x)$ é irredutível então $f(x) \mid g(x)h(x) \iff f(x) \mid g(x)$ ou $f(x) \mid h(x)$, que por sua vez vem da divisão euclidiana.

Além disso, o teorema do resto para polinômios também é válido em Z/pZ.

Com tudo isso, vem à tona o seguinte

Teorema 1.1. *Seja $f(x)$ um polinômio com coeficientes inteiros e de grau d e p um primo. Então a congruência $f(x) \equiv 0 \pmod{p}$ tem no máximo d raízes mód p, contando multiplicidades.*

Demonstração

Indução em d. Para $d = 0$, não há raízes e para $d = 1$, o polinômio é da forma $ax + b$, $a \not\equiv 0 \pmod{p}$, cuja raiz é $x = -b \cdot a^{-1}$ mód p.

Seja $f(x)$ de grau d e r uma raiz de f (caso f não tenha raízes, o teorema está demonstrado, pois $d \geq 0$). Então, pelo teorema do resto, $f(x) \equiv (x-r)g(x) \pmod{p}$, sendo g de grau $d-1$. Pela hipótese de indução, g tem no máximo $d-1$ raízes, e o resultado segue. ∎

Note que esse resultado não é válido para módulos compostos. Por exemplo, $x^2 - 1 \equiv 0 \pmod{8}$ tem 4 soluções.

Exercícios

01. Seja $f(x)$ um polinômio de coeficientes inteiros com grau d. Prove que a congruência $f(x) \equiv 0 \pmod{p}$, p primo, tem d soluções não congruentes mód p se, e somente se, na divisão euclidiana de $x^p - x$ por $f(x)$, $x^p - x = f(x)q(x) + r(x)$, o resto $r(x)$ tiver todos os seus coeficientes múltiplos de p.

2. Raízes primitivas

Primeiro, vamos definir ordem.

Definição 2.1. *Sejam a e m inteiros primos entre si. A ordem de a mód m, denotada por $\mathrm{ord}_m\, a$, é o menor inteiro positivo d tal que $a^d \equiv 1 \pmod{m}$.*

O seguinte lema é particularmente útil.

Lema 2.1. *Se $a^t \equiv 1 \pmod{m}$ então $\mathrm{ord}_m\, a \mid t$. Em particular, $\mathrm{ord}_m\, a \mid \phi(m)$.*

Demonstração

Basta realizar a divisão euclidiana de t por $\mathrm{ord}_m\, a$: $t = q \cdot \mathrm{ord}_m\, a + r$, $0 \leq r < \mathrm{ord}_m\, a$. Então $a^t = (a^{\mathrm{ord}_m\, a})^q \cdot a^r \equiv a^r \pmod{m}$. Como $r < \mathrm{ord}_m\, a$ e $\mathrm{ord}_m\, a$ é mínimo, r só pode ser zero, e portanto $\mathrm{ord}_m\, a \mid t$.

A segunda afirmação decorre imediatamente do teorema de Euler-Fermat. ∎

Já temos que $\text{ord}_m a \leq \phi(m)$. Será que é possível $\text{ord}_m a = \phi(m)$. E se isso acontecer, será que isso é útil?

É tão útil que números com essa propriedade ganham até um nome especial.

Definição 2.2. *Dizemos que g é raiz primitiva de m quando* $\text{ord}_m g = \phi(m)$.

Vamos entender o porquê desse nome demonstrando o próximo teorema, que é bastante útil.

Teorema 2.1. *Se g é raiz primitiva de m então $1, g, g^2, \ldots, g^{\phi(m)-1}$ mód m são todos os restos primos com m. Isto é, se $\text{mdc}(a, m) = 1$ então existe i tal que $a \equiv g^i \pmod{m}$.*

Demonstração

Note que, sendo $\phi(m) > i \geq j \geq 0$, $g^i \equiv g^j \pmod{m} \iff g^{i-j} \equiv 1 \pmod{m}$. Pelo lema da ordem, $\text{ord}_m g \mid i - j \iff \phi(m) \mid i - j$. Como $0 \leq i - j < \phi(m)$, $i - j = 0 \iff i = j$. Isto quer dizer que não aparecem números repetidos mód m entre os $\phi(m)$ números $1, g, g^2, \ldots, g^{\phi(m)-1}$, de modo que eles só podem ser *todos* os $\phi(m)$ números primos com m. ∎

Parece promissor, não? Pena que nem todos os números admitem raízes primitivas.

Teorema 2.2. *Os números que admitem raízes primitivas são 2, 4, p^n e $2p^n$, sendo p primo ímpar.*

Vamos provar esse teorema em várias partes.

Parte 1. *Se m tem dois fatores primos ímpares distintos p e q então m não admite raiz primitiva.*

Demonstração

Se m admite dois fatores primos ímpares distintos p e q então podemos escrever $m = a \cdot b$, com $\text{mdc}(a, b) = 1$, $a, b > 1$, $p \mid a$ e $q \mid b$. Note que $p - 1 \mid \phi(a)$ e $q - 1 \mid \phi(b)$. Em particular, $\phi(a)$ e $\phi(b)$ são ambos pares, ou seja, $\phi(a)/2$ e $\phi(b)/2$ são ambos inteiros. Assim, sendo x primo com m, $x^{\phi(a)} \equiv 1 \pmod{a} \implies x^{\phi(a)\phi(b)/2} \equiv 1 \pmod{a}$. Analogamente, $x^{\phi(a)\phi(b)/2} \equiv 1 \pmod{b}$. Como a e b são primos entre si, concluímos que $x^{\phi(a)\phi(b)/2} \equiv 1 \pmod{ab}$, de modo que $\text{ord}_m x \leq \phi(a)\phi(b)/2 = \phi(ab)/2 = \phi(m)/2 < \phi(m)$; ou seja, m não admite raiz primitiva. ∎

Parte 2. *2 e 4 admitem raiz primitiva, mas 2^n, $n \geq 3$ não.*

Demonstração

Primeiro, 1 e 3 são raízes primitivas de 2 e 4, respectivamente. Seja x ímpar. Temos $x^2 \equiv 1 \pmod{8}$ e, para $n \geq 3$, $x^{2^{n-2}} - 1 = (x^2 - 1)(x^2 + 1)(x^4 + 1) \ldots (x^{2^{n-3}} + 1)$ tem pelo menos n fatores 2, já que $2^3 \mid x^2 - 1$ e $2 \mid x^{2^i} + 1$, $i = 1, 2, \ldots, n - 3$. Logo $x^{2^{n-2}} \equiv 1 \pmod{2^n}$, ou seja, $\text{ord}_{2^n} x \leq 2^{n-2} < \phi(2^n)$ para todo x ímpar. Assim, 2^n não admite raízes primitivas para $n \geq 3$. ∎

Parte 3. *Se $4 \mid m$ e $m > 4$ então m não admite raiz primitiva.*

Demonstração

Seja $m = 2^k \ell$, ℓ ímpar e $k \geq 2$. O caso $\ell = 1$ já foi estudado na parte 2. Nos demais casos, basta repetir a demonstração da parte 1 com 4 no lugar de p e q sendo um divisor de ℓ. ∎

Parte 4. *Todo primo ímpar p admite raiz primitiva.*

Demonstração

Essa é a parte mais difícil do teorema e é aqui que utilizaremos o teorema sobre polinômios mód p.

Considere o seguinte algoritmo para encontrar uma raiz primitiva de qualquer primo p:

Algoritmo

(1) Tome $a = 2$.

(2) Seja $d_a = \operatorname{ord}_p a$. Se $d_a = p - 1$, a é raiz primitiva de p; caso contrário, tome o menor número b que não é congruente a algum a^i mód p.

(3) Seja $d_b = \operatorname{ord}_p b$. Se $d_b = p-1$, b é raiz primitiva de p; se não, tome m e n tais que $\operatorname{mdc}(m, n) = 1$, $m \mid d_a$, $n \mid d_b$ e $mn = \operatorname{mmc}(d_a, d_b)$ (por que eles existem?).

(4) Troque a por $c = a^{d_a/m} b^{d_b/n}$ e volte ao passo 2.

Vamos provar que esse algoritmo funciona e, o mais importante, termina. Supondo que termine, ele funciona porque os sinais de término são quando encontramos uma raiz primitiva.

Agora, provemos que o algoritmo termina, o que é mais interessante. Primeiro note que d_b não divide d_a, pois se dividisse teríamos $b^{d_a} \equiv 1 \pmod{p}$, o que não pode ocorrer pois a equação $x^{d_a} \equiv 1 \pmod{p}$ admite no máximo d_a soluções, que são 1, a, a^2, $\ldots$, $a^{d_a - 1}$, e b não é congruente a algum a^i. Isso implica $\operatorname{mmc}(d_a, d_b) > d_a$. Além disso, seja $k = \operatorname{ord}_p c$. Então $(a^{d_a/m} b^{d_b/n})^k \equiv 1 \pmod{p}$. Elevando ambos os membros por m, obtemos $a^{d_a k} b^{d_b mk/n} \equiv 1 \pmod{p} \iff b^{d_b mk/n} \equiv 1 \pmod{p}$. Lembrando que $d_b = \operatorname{ord}_p b$, $d_b \mid d_b mk/n \iff n \mid mk$. Sendo $\operatorname{mdc}(m, n) = 1$, temos $n \mid k$. Analogamente, $m \mid k$ e, portanto $mn \mid k$. Observando ainda que $c^{mn} \equiv 1 \pmod{p}$, temos $\operatorname{ord}_p c = mn = \operatorname{mmc}(d_a, d_b) > d_a$. Isto quer dizer quem a cada iteração do algoritmo a ordem do próximo valor aumenta. Portanto, em algum momento iguala o seu máximo, que é $p - 1$ (note que a escolha de b no algoritmo depende de $\operatorname{ord}_p a \neq p - 1$). ∎

Parte 5. *Se g é raiz primitiva de p mas não de p^2, então $g + p$ é raiz primitiva de ambos.*

Demonstração

Seja $d = \operatorname{ord}_{p^2} g$. Então $g^d \equiv 1 \pmod{p^2} \implies g^d \equiv 1 \pmod{p} \implies p - 1 \mid d$. Logo, como $d \neq p(p-1)$ e $d \mid p(p-1)$, $d = p - 1$, isto é, $g^{p-1} \equiv 1 \pmod{p^2}$.

Para conseguirmos provar essa parte, basta demonstrarmos que $(g + p)^{p-1} \not\equiv 1 \pmod{p^2}$. E esse é um trabalho para o binômio de Newton! Temos $(g + p)^{p-1} \equiv g^{p-1} + \binom{p-1}{1} g^{p-2} p \pmod{p^2}$ (você consegue ver por que não precisamos escrever os demais termos do binômio de Newton?). Substituindo $g^{p-1} \equiv 1 \pmod{p^2}$ e desenvolvendo as contas: $(g + p)^{p-1} \equiv 1 + (p-1)pg^{p-2} \equiv 1 - pg^{p-2} \pmod{p^2}$, que não é 1, pois $g^{p-2} \not\equiv 0 \pmod{p}$. Logo $g + p$ é raiz primitiva de p^2 (e de p também!) ∎

Parte 6. *Se g é raiz primitiva de p e p^2 então é raiz primitiva de p^n, e portanto p^n admite raiz primitiva.*

Demonstração

Indução sobre n. A base de indução ($n = 1$ e $n = 2$) está na hipótese. Suponha que g seja raiz primitiva de p^{n-1}. Seja $d = \operatorname{ord}_{p^n} g$. Então $g^d \equiv 1 \pmod{p^n} \implies g^d \equiv 1 \pmod{p^{n-1}} \implies \operatorname{ord}_{p^{n-1}} g \mid d \implies p^{n-2}(p-1) \mid d$. Como $d \mid \phi(p^n) \iff d \mid p^{n-1}(p-1)$, temos $d = p^{n-2}(p-1)$ ou $d = p^{n-1}(p-1)$. Para provar que não ocorre o primeiro caso, vamos usar o lema de Hensel:

Lema 2.2. *Seja p um primo ímpar, a um inteiro e n um inteiro positivo. Se $p^\alpha \parallel a-1$, $\alpha > 0$ e $p^\beta \parallel n$ então $p^{\alpha+\beta} \parallel a^n - 1$. Além disso, se n é ímpar, $p^\alpha \parallel a+1$, $\alpha > 0$ e $p^\beta \parallel n$ então $p^{\alpha+\beta} \parallel a^n + 1$.*

(Dizemos que p^α *divide exatamente* m e denotamos por $p^\alpha \parallel m$ o fato de que m contém exatamente α fatores primos p.)

Note que como $p \mid g^{p-1} - 1$ e p^2 não divide $g^{p-1} - 1$ (caso contrário, g não seria raiz primitiva de p^2), $p \parallel g^{p-1} - 1$. Assim, pelo lema de Hensel, a maior potência de p que divide $g^{p^{n-2}(p-1)} - 1 = (g^{p-1})^{p^{n-2}} - 1$ é $p^{1+n-2} = p^{n-1}$. Assim, p^n não divide $g^{p^{n-2}(p-1)} - 1$, o que é equivalente a $g^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n}$. Logo $\mathrm{ord}_{p^n} g = p^{n-1}(p-1) = \phi(p^n)$ e, portanto, g é raiz primitiva de p^n. ∎

Parte 7. *$2p^n$ admite raiz primitiva.*

Demonstração

Seja g uma raiz primitiva de p^n. Note que $\phi(2p^n) = \phi(p^n)$ (verifique!) e considere g ou $g + p^n$, o que for ímpar. Sendo d a ordem desse número, que denotaremos por h, $h^d \equiv 1 \pmod{2p^n} \implies h^d \equiv 1 \pmod{p^n} \implies \phi(p^n) \mid d$. Assim, $d = \phi(2p^n)$. ∎

Exercícios

02. Sejam x e y inteiros positivos. Prove que existem inteiros positivos m e n tais que $m \mid x$, $n \mid y$, $\mathrm{mdc}(m,n) = 1$ e $mn = \mathrm{mmc}(x,y)$.

03. Há outra maneira de provar que p admite raiz primitiva. Como? Siga os itens!

(a) Prove que $\sum_{d|n} \phi(d) = n$. *Dica: conte de duas maneiras a quantidade de pares (x,d) em que* $\mathrm{mdc}(x,n) = d$.

(b) Prove que se $d \mid p-1$ a congruência $x^d \equiv 1 \pmod{p}$ tem exatamente d soluções distintas mód p.

(c) Seja d um divisor de $p-1$ e $r(d)$ a quantidade de números mód p com ordem igual a d. Prove que $r(d) \leq \phi(d)$.

(d) Prove que, na verdade, $r(d) = \phi(d)$. Em particular, p admite $\phi(p-1)$ raízes primitivas (isso pode ser generalizado: se m admite raiz primitiva, então admite $\phi(\phi(m))$ raízes primitivas).

04. (OBM 1995, Problema 5) Encontre todas as funções $f\colon Z_+ \to R$ tais que, para todos x, y inteiros não negativos,

$$f(x)f(y) = f(xy) \quad \text{e} \quad f(x+1019) = f(x)$$

05. (IMO Shortlist 2001) Seja $p > 3$ um primo. Prove que existe a com $1 \leq a < p-1$ tal que $a^{p-1} - 1$ e $(a+1)^{p-1} - 1$ não são divisíveis por p^2.

06. Encontre todos os números inteiros positivos n tais que $x^{25} \equiv x \pmod{n}$ para todo inteiro x.

07. Sendo k um inteiro positivo dado, encontre todos os inteiros positivos n tais que $7^n + 1$ é múltiplo de 5^k.

3. Resíduos quadráticos

Definição 3.1. *Dizemos que c é resíduo quadrático mód m quando existe x inteiro tal que $x^2 \equiv c$ (mód. m).*

Podemos reduzir qualquer congruência quadrática a encontrar resíduos quadráticos. De fato, sendo $D = b^2 - 4ac$,

$$\begin{aligned} ax^2 + bx + c \equiv 0 \pmod{m} &\iff 4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4am} \\ &\iff (2ax+b)^2 \equiv D \pmod{4am} \end{aligned}$$

Primeiro, vamos nos preocupar somente com c primo com m.

Lema 3.1. *Seja $d = \text{mdc}(c, m)$, $d = k^2\ell$, ℓ livre de quadrados, $c = dc'$, $m = dm'$. Então $x^2 \equiv c \pmod{m}$ tem solução se, e somente se, $x^2 \equiv \ell c' \pmod{m'}$ tem solução e $\text{mdc}(\ell, m') = 1$. Note que $\text{mdc}(\ell c', m') = 1$.*

Demonstração

Primeiro, note que $x^2 \equiv c \pmod{m} \iff x^2 = c + mt = k^2\ell(c' + m't)$. Assim, lembrando que ℓ é livre de quadrados, $k\ell \mid x$. Sendo $x = k\ell x'$, obtemos $\ell(x')^2 = c' + m't$, de modo que $(\ell x')^2 \equiv \ell c' \pmod{m'}$. Reciprocamente, $x^2 \equiv \ell c' \pmod{m'} \iff (xk)^2 \equiv \ell k^2 c' \pmod{k^2 m'} \iff (xk)^2 \equiv c \pmod{m/\ell} \implies (xk)^2 \equiv c \pmod{m}$.

Além disso, suponha que $\text{mdc}(\ell, m') = u > 1$. Então, $\ell(x')^2 = c' + m't \implies u \mid c' \implies du \mid c$, o que é um absurdo pois $du \mid m$ e isso implicaria $\text{mdc}(c, m) = du > d$. De fato, $\text{mdc}(c', m') = 1$. ∎

A partir daqui, vamos supor sempre que $\text{mdc}(c, m) = 1$.

Lema 3.2. *c é resíduo quadrático de $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ se, e somente se, c é resíduo quadrático de $p_i^{\alpha_i}$, $i = 1, 2, \ldots, k$.*

Demonstração

Um dos lados é trivial; o outro é uma aplicação do Teorema Chinês dos Restos. ∎

Agora a idéia é encontrar critérios para verificar se um número é resíduo quadrático módulo potência de primo. Há dois casos a considerar.

3.1. Resíduos quadráticos mód 2^n

Nesse caso, podemos descrever todos os resíduos quadráticos de modo simples:

Teorema 3.1. *Os resíduos quadráticos mód 2^n são os números da forma $8k + 1$, k inteiro.*

Demonstração

Primeiro, provemos que os resíduos quadráticos devem ser da forma $8k + 1$: para ver isso, basta notar que $(2t + 1)^2 = 8\frac{t(t+1)}{2} + 1 \equiv 1 \pmod{8}$.

Se $n = 1$ ou $n = 2$, o único ímpar da forma $8k + 1$ que é um resíduo é 1, que de fato é o único resíduo quadrático. Nos demais casos, uma contagem basta: há, em princípio, 2^{n-1} resíduos possíveis (todos os ímpares mód 2^n). Mas há repetições: de fato, $x^2 \equiv y^2 \pmod{2^n} \iff 2^n \mid (x - y)(x + y)$. Como x e y são ímpares, a maior potência de 2 que divide ambos (e, portanto, sua soma $(x - y) + (x + y) = 2x$) é 2. Assim, sendo $n > 2$, $2^{n-2} \mid \frac{x-y}{2} \cdot \frac{x+y}{2} \iff 2^{n-2} \mid \frac{x-y}{2}$ ou $2^{n-2} \mid \frac{x+y}{2} \iff x \equiv \pm y \pmod{2^{n-1}} \iff x \equiv \pm y \pmod{2^n}$ ou $x \equiv \pm y + 2^{n-1} \pmod{2^n}$.

Deste modo, cada resíduo quadrático está sendo contado exatamente quatro vezes, de modo que o total de resíduos quadráticos mód 2^n é $2^{n-1}/4 = 2^{n-3}$. Porém, todos devem ser da forma $8k + 1$ e, por uma grande coincidência, há 2^{n-3} resíduos da forma $8k+1$ mód 2^n. Então *todo* número da forma $8k+1$ é resíduo quadrático mód 2^n. ∎

3.2. Resíduos quadráticos mód p^n, $p > 2$

Nesse caso, o problema é mais simples, simplesmente porque potências de primos ímpares admitem raízes primitivas (veremos por que mais para frente).

Teorema 3.2. *c é resíduo quadrático módulo p^n se, e somente se, $c^{\phi(p^n)/2} \equiv 1 \pmod{p^n}$.*

Demonstração

Se c é resíduo quadrático mód p^n então existe um inteiro x tal que $x^2 \equiv c \pmod{p^n} \implies (x^2)^{\phi(p^n)/2} \equiv c^{\phi(p^n)/2} \pmod{p^n} \iff x^{\phi(p^n)} \equiv c^{\phi(p^n)/2} \pmod{p^n} \iff c^{\phi(p^n)/2} \equiv 1 \pmod{p^n}$.

Reciprocamente, seja g uma raiz primitiva de p^n. Então $c \equiv g^k \pmod{p^n}$ para algum k. O nosso propósito é provar que k é par, de modo que $x = g^{k/2}$ é uma raiz de $x^2 \equiv \pmod{p^n}$. Mas isso é simples: de fato, $c^{\phi(p^n)/2} \equiv 1 \pmod{p^n} \iff g^{k\phi(p^n)/2} \equiv 1 \pmod{p^n}$. Como $\mathrm{ord}_{p^n} g = \phi(p^n)$, concluímos que $\phi(p^n) \mid k\phi(p^n)/2$, o que implica que k é par. ∎

Esse último teorema é conhecido como *critério de Euler*.

4. O problema 2 da OBM 2007

Com isso, podemos resolver o problema 2 da OBM 2007.

Problema 2, OBM 2007. *Para quantos números inteiros c, $-2007 \leq c \leq 2007$, existe um inteiro x tal que $x^2 + c$ é múltiplo de 2^{2007}?*

Resolução

Poderíamos simplesmente aplicar dois dos lemas anteriores (procure-os!), mas vamos dar uma solução diferente, utilizando uma das melhores amigas da Teoria dos Números: a indução.

Vamos nos preocupar primeiro com os resíduos quadráticos primos com 2^n, que são os ímpares. Como antes, sendo $x = 2t + 1$ ímpar, $x^2 = 8 \cdot \frac{t(t+1)}{2} + 1 \equiv 1 \pmod{8}$.

Provemos, por indução, que os resíduos quadráticos ímpares mód 2^n são *todos* os inteiros da forma $8k+1$. A base de indução é para $n = 3$ e é imediata. Além disso, suponha que m seja resíduo quadrático mód 2^n, ou seja, $x^2 \equiv m \pmod{2^n}$. Se $x^2 \equiv m \pmod{2^{n+1}}$, acabou. Caso contrário, $x^2 \equiv m + 2^n \pmod{2^{n+1}}$. Para consertar isso, tome $x' = x + 2^{n-1}$. Temos $(x')^2 \equiv x^2 + 2 \cdot 2^{n-1} + 2^{2n-2} \equiv (m + 2^n) + 2^n + 0 \equiv m \pmod{2^{n+1}}$, pois $n \geq 2 \iff 2n - 2 \geq n$. Portanto m é resíduo quadrático mód 2^{n+1} também.

Agora, vamos considerar os resíduos quadráticos pares. Note que se $m = 2^{2r}\ell$, ℓ ímpar, $2r \leq n - 3$, então $x^2 \equiv m \pmod{2^n} \iff x^2 = 2^{2r}\ell + 2^n u = 2^{2r}(\ell + 2^{n-2r}u) \implies 2^{2r} \mid x^2 \iff 2^r \mid x$. Sendo $x = 2^r x_0$, $x^2 \equiv m \pmod{2^n} \iff x_0^2 \equiv \ell \pmod{2^{n-2r}}$. Como $n - 2r \geq 3$, ℓ deve ser da forma $8k + 1$.

Se $n = 2^{2r+1}\ell$, ℓ ímpar, $2r + 1 < n$, então $x^2 \equiv m \pmod{2^n} \iff x^2 = 2^{2r+1}\ell + 2^n u = 2^{2r+1}(\ell + 2^{n-2r-1}u)$. Como $\ell + 2^{n-2r-1}u$ é ímpar, não existe x satisfazendo tal condição, já que x^2 deve ter uma quantidade par de fatores 2.

Falta somente estudar os casos em que $m = 2^{2r}\ell = 2^{n-2}\ell$ ou $m = 2^{2r}\ell = 2^{n-1}\ell$, ℓ ímpar. Esses casos são testados manualmente: se $m = 2^{n-2}\ell$, basta testar $m = 2^{n-2}$ e $m = 3 \cdot 2^{n-2}$. Já sabemos que $m = 2^{n-2}$ é da forma $2^{2r}(8k + 1)$. Uma rápida análise mostra que $3 \cdot 2^{n-2}$ não é possível (fazendo as mesmas contas anteriores, encontramos $x_0^2 \equiv 3 \pmod{4}$, o que é uma contradição). Da mesma forma, se $m = 2^{n-1}\ell$, basta somente testar $m = 2^{n-1}$, que também é da forma $2^{2r}(8k + 1)$.

Só nos resta mostrar que $m = 2^{2k}(8k+1)$ é resíduo quadrático mód 2^n. Mas isso é simples: basta tomar $x = 2^k m'$, em que $(m')^2 \equiv 8k + 1 \pmod{2^n}$.

O resto é uma contagem simples: basta contar todos os números da forma $2^{2k}(8k + 1)$ no intervalo $[-2007, 2007]$. Isso é razoavelmente rotineiro, já que $0 \leq k \leq 6$. Contando, você encontra 670 valores.

4.1. O lema de Hensel aplicado para resíduos quadráticos

O fato é que existe uma outra versão do lema de Hensel, utilizada bastante em análise em p-ádicos, que enunciamos aqui.

Lema 4.1. *Seja $f(x)$ um polinômio de coeficientes inteiros, $k > 1$ um inteiro e p primo. Suponha que exista r inteiro tal que $f(r) \equiv 0 \pmod{p^{k-1}}$. Então*

- *Se $f'(r) \not\equiv 0 \pmod{p}$, então existe um único inteiro t tal que $0 \leq t < p$ e $f(r + tp^{k-1}) \equiv 0 \pmod{p^k}$, sendo t definido por $t \cdot f'(r) \equiv -(f(r)/p^{k-1}) \pmod{p}$.*
- *Se $f'(r) \equiv 0 \pmod{p}$ e $f(r) \equiv 0 \pmod{p^n}$ então $f(r + tp^{k-1}) \equiv 0 \pmod{p^n}$ para todo inteiro t.*

- *Se* $f'(r) \equiv 0 \pmod{p}$ *e* $f(r) \not\equiv 0 \pmod{p^n}$ *então* $f(r + tp^{k-1}) \not\equiv 0 \pmod{p^n}$ *para todo inteiro* t.

Demonstração

Parece difícil demonstrar isso, certo? Na verdade, não é tão complicado quanto parece. É só saber usar o sinal do somatório e utilizar, com parcimônia, o binômio de Newton.

Para facilitar as contas, primeiro note que, do binômio de Newton, $(r+tp^{k-1})^i = \binom{i}{0}r^i + \binom{i}{1}r^{i-1}tp^{k-1} + \binom{i}{2}r^{i-2}(tp^{k-1})^2 + \cdots + \binom{i}{i}(tp^{k-1})^i$. Mas, sendo $k \geq 2$, $2(k-1) \geq k$, assim reduzindo mód p^k obtemos $(r + tp^{k-1})^i \equiv r^i + i \cdot r^{i-1}tp^{k-1} \pmod{p^k}$.

Agora, podemos terminar as contas mais tranquilamente. Fazer as contas em "prestações" é uma boa prática: você consegue estruturar melhor as contas, separar as dificuldades individuais de cada parte, é mais difícil errar e mais fácil achar os erros, se esses acontecerem. É claro que pode ser mais fácil juntar as somas e manipulá-las ao mesmo tempo, mas não é o caso aqui.

Enfim, seja $f(x) = \sum_{i=0}^{n} a_i x^i$. Note que $f'(x) = \sum_{i=1}^{n} a_i i x^{i-1}$. Temos $f(r + tp^{k-1}) = \sum_{i=0}^{n} a_i(r + tp^{k-1})^i \equiv \sum_{i=0}^{n} a_i(r^i + i \cdot r^{i-1}tp^{k-1}) = \sum_{i=0}^{n}(a_i r^i + a_i i r^{i-1}tp^{k-1}) = f(r) + tp^{k-1}f'(r) \pmod{p^k}$. Então, lembrando que $f(r) \equiv 0 \pmod{p^{k-1}}$, temos $f(r + tp^{k-1}) \equiv 0 \pmod{p^k} \iff f(r) + tp^{k-1}f'(r) \equiv 0 \pmod{p^k} \iff t \cdot f'(r) \equiv -f(r)/p^{k-1} \pmod{p}$. Isso prova os três itens do lema de Hensel. ∎

O lema de Hensel é bastante poderoso; dada a solução de uma congruência polinomial mód p, ele permite resolver a mesma congruência mód p^n.

Com isso, é possível, por exemplo, caracterizar todos os resíduos quadráticos mód p^n, p primo ímpar.

Lema 4.2. *Existem* $\phi(p^n)/2 = p^{n-1}(p-1)/2$ *resíduos quadráticos mód* p^n. *Em particular, há* $(p-1)/2$ *resíduos quadráticos mód* p.

Demonstração

Fica a cargo do leitor. (Dica: faça uma contagem semelhante ao dos resíduos quadráticos mód 2^n)

Lema 4.3. *Se* c *é resíduo quadrático mód* p *então é resíduo quadrático mód* p^n.

Demonstração

Uma indução, aliada ao lema de Hensel, basta: seja $f(x) = x^2 - c$. Se $r^2 \equiv c \pmod{p^n} \iff f(r) \equiv 0 \pmod{p^n}$, sendo $f'(r) \not\equiv 0 \pmod{p}$, pelo lema de Hensel existe um único t, $0 \leq t < p$, tal que $f(r+tp^n) \equiv 0 \pmod{p^{n+1}} \iff (r + tp^n)^2 \equiv c \pmod{p^{n+1}}$. A base de indução é a própria hipótese do lema, então a demonstração está completa. ∎

Teorema 4.1. *Sejam* $a_1, a_2, \ldots, a_{(p-1)/2}$ *os resíduos quadráticos mód* p. *Então os resíduos quadráticos mód* p^n *são todos os números da forma* $kp + a_i$, $i = 1, 2, \ldots, (p-1)/2$.

Demonstração

Basta combinar os dois lemas anteriores. ∎

Exercícios

08. (IMO 1996, Problema 4) Os inteiros positivos a e b são tais que os números $15a + 16b$ e $16a - 15b$ são ambos quadrados perfeitos. Ache o menor valor possível que o menor destes dois quadrados pode assumir.

09. Encontre todos os inteiros positivos k tais que existe um inteiro a tal que $(a + k)^3 - a^3$ é múltiplo de 2007.

10. (OBM 1996, Problema 6) Seja $T(x) = x^3 + 14x^2 - 2x + 1$. Denotamos $T^n(x) = T(T^{n-1}(x))$ e $T^0(x) = x$. Prove que existe um inteiro positivo N tal que $T^N(x) - x$ é divisível por 101 para todo inteiro x. *Dica: Prove que* $T(x) \equiv T(y) \pmod{101} \iff x \equiv y \pmod{101}$ *e aplique casa dos pombos.*

11. (Generalizando o critério de Euler) Seja p um primo ímpar e c e $k > 1$ inteiros. Prove que existe um inteiro x tal que $x^k \equiv c \pmod{p^n}$ se, e somente se, $c^{\phi(p^n)/d} \equiv 1 \pmod{p^n}$, sendo $d = \text{mdc}(k, \phi(p^n))$.

12. Encontre todos os números inteiros c tais que existe um inteiro x tal que $x^3 - c$ é múltiplo de 3^{2007}.

13. (Vietnã 2000) Seja $p(x) = x^3 + 153x^2 - 111x + 38$. Mostre que $p(n)$ é divisível por 3^{2000} para pelo menos nove inteiros positivos n menores que 3^{2000}. Para quantos valores de n é divisível?

5. O teorema da reciprocidade quadrática

Esse era um dos teoremas favoritos de Gauss. Ele gostava tanto desse teorema que fez nada menos do que oito demonstrações.

Antes, para facilitar, vamos definir uma notação "legendrária" para resíduos quadráticos.

Definição 5.1. *Seja c inteiro e p primo. Definimos o símbolo de Legendre $\left(\frac{c}{p}\right)$, lido "c Legendre p", por*

$$\left(\frac{c}{p}\right) = \begin{cases} 0 & \text{se } p \mid c \\ 1 & \text{se } c \text{ é resíduo quadrático mód } p \\ -1 & \text{se } c \text{ não é resíduo quadrático mód } p \end{cases}$$

Assim, por exemplo, temos $\left(\frac{2}{7}\right) = 1$, $\left(\frac{20}{5}\right) = 0$ e $\left(\frac{25}{p}\right) = 1$ para todo primo p.

Note que podemos enunciar o critério de Euler mais diretamente:

Critério de Euler. *Sendo c inteiro e p primo ímpar,*

$$\left(\frac{c}{p}\right) \equiv c^{\frac{p-1}{2}} \pmod{p}$$

Com isso, você deve provar sem dificuldades as seguintes propriedades:

Teorema 5.1. *Sejam a, b inteiros e p primo ímpar. Então*

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$
- *Se* $a \equiv b \pmod{p}$, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ ∎

Agora vamos enunciar outro critério para resíduos quadráticos, o *lema de Gauss*.

Lema 5.1. *Seja k a quantidade de inteiros j, $1 \leq j \leq (p-1)/2$, tais que $cj \bmod p > p/2$ (isto é, o resto da divisão de cj por p é maior que $p/2$). Então*

$$\left(\frac{c}{p}\right) = (-1)^k$$

Demonstração

A principal sacada aqui é escrever $c^{\frac{p-1}{2}} \bmod p$ de outro modo, utilizando os resíduos maiores que $p/2$. E utilizamos aqui uma idéia parecida com uma das demonstrações do teorema de Euler-Fermat, o "gira-gira".

Considere todos os números da forma cj, $1 \leq j \leq (p-1)/2$. Note que

$$\prod_{j=1}^{\frac{p-1}{2}} cj \equiv c^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}$$

Porém, podemos também reduzir os fatores mód p *antes* de multiplicá-los. De fato, seja

$$c_j = \text{mín}\{cj \text{ mód } p, p - cj \text{ mód } p\},$$

de modo que $c_j = p - cj$ mód p se, e somente se, cj mód $p > p/2$. Não é difícil provar que $c_i = c_j \iff i = j$: de fato, $c_i = c_i \iff i \equiv \pm j \pmod{p}$ e, sendo $1 \leq i, j < p/2$, devemos ter $i = j$.

Ao multiplicar os c_j's mód p, obtemos de novo todos os resíduos entre 1 e $(p-1)/2$ (note que os $(p-1)/2$ números multiplicados são todos diferentes mód p e com restos menores do que $p/2$). E esse produto é exatamente igual ao produto dos cj's, com exceção das k mudanças de sinal quando $c_j = p - cj$ mód p. Assim,

$$\prod_{j=1}^{\frac{p-1}{2}} cj \equiv (-1)^k \prod_{j=1}^{\frac{p-1}{2}} c_j \equiv (-1)^k \left(\frac{p-1}{2}\right)! \pmod{p}$$

Das duas equações obtidas,

$$c^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^k \left(\frac{p-1}{2}\right)! \pmod{p} \iff c^{\frac{p-1}{2}} \equiv (-1)^k \pmod{p},$$

e, do critério de Euler, o resultado segue. ∎

E para que serve essa conta? Não parece ser mais fácil do que o critério de Euler em si! O fato é que esse resultado é um dos passos decisivos para obtermos a lei da reciprocidade quadrática.

Vamos dar mais um passo adiante em direção a ela.

Lema 5.2. *Se c é ímpar e p é primo ímpar, então*

$$\left(\frac{c}{p}\right) = (-1)^M \quad \textit{em que} \quad M = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{cj}{p} \right\rfloor$$

Demonstração

O que é exatamente $\lfloor \frac{cj}{p} \rfloor$? Simplesmente é o *quociente* da divisão de cj por p. Então parece interessante pensarmos na divisão euclidiana de cj por p. Assim, seja r_j o resto da divisão de cj por p, de modo que $cj = p \cdot \lfloor \frac{cj}{p} \rfloor + r_j$. Assim, como é de se esperar, vamos fazer uso de uma idéia muito importante na Teoria dos Números: somar tudo e ver o que acontece!

$$\sum_{j=1}^{\frac{p-1}{2}} cj = p \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{cj}{p} \right\rfloor + \sum_{j=1}^{\frac{p-1}{2}} r_j$$

Você reconhece r_j? Não é, na verdade, cj mód p? Assim, lembrando da notação do lema de Gauss, temos $c_j = \text{mín}\{r_j, p - r_j\}$. Lembrando que os c_j's nada mais são do que uma permutação dos números 1, 2, ..., $(p-1)/2$, temos

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} c_j = \sum_{r_j < p/2} r_j + \sum_{r_j > p/2} (p - r_j) = \sum_{r_j < p/2} r_j - \sum_{r_j > p/2} r_j + kp$$

Subtraindo os dois resultados, obtemos

$$(c-1) \sum_{j=1}^{\frac{p-1}{2}} j = p \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{cj}{p} \right\rfloor + 2 \sum_{r_j > p/2} r_j - kp$$

Enfim, sendo c e p ímpares, vendo mód 2 (afinal, só estamos interessados em saber se $(-1)^M = (-1)^k$) chegamos ao resultado, já que $p \equiv 1 \pmod 2$ e $c - 1 \equiv 0 \pmod 2$:

$$0 \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{cj}{p} \right\rfloor - k \pmod 2 \iff \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{cj}{p} \right\rfloor \equiv k \pmod 2$$

∎

Estamos prontos para ver quando 2 é resíduo quadrático de outro primo.

Teorema 5.2. *Sendo p primo ímpar,*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Demonstração

É só fazer $c = 2$ no teorema acima e utilizar a última equação antes de utilizarmos que c é ímpar:

$$(2-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{2j}{p} \right\rfloor + 2\sum_{r_j > p/2} r_j - kp$$

Sendo $\sum_{j=1}^{\frac{p-1}{2}} j = \frac{1}{2}\frac{p-1}{2}\frac{p+1}{2} = (p^2-1)/8$ e $0 < j < p/2 \iff 0 < 2j < p \iff \lfloor \frac{2j}{p} \rfloor = 0$, vendo mód 2 obtemos

$$\frac{p^2-1}{8} \equiv k \pmod 2$$

e o resultado segue. ∎

Mais um fato antes do nosso resultado principal:

Lema 5.3. *Sejam p e q primos ímpares distintos. Então*

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor + \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{pk}{q} \right\rfloor = 1$$

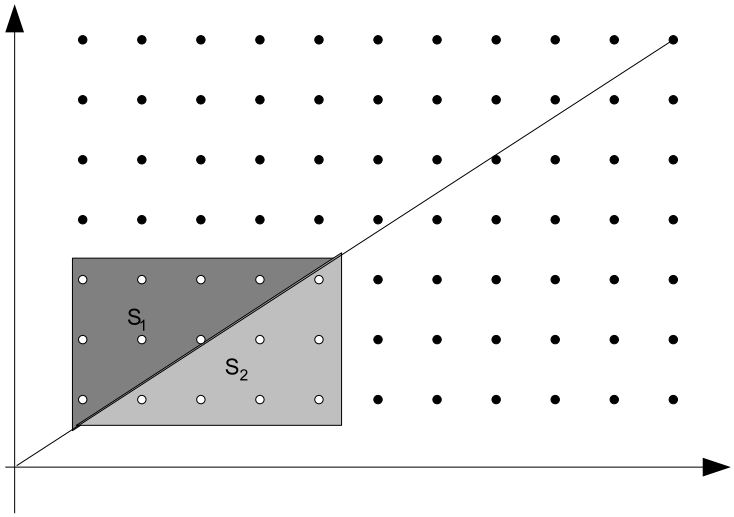
Demonstração

Sejam $S = \{(a,b) : 1 \le a \le (p-1)/2 \text{ e } 1 \le b \le (q-1)/2\}$, $S_1 = \{(a,b) \in S : aq < bp\}$ e $S_2 = \{(a,b) \in S : aq > bp\}$. Note que, para todos $a, b \in S$, $ap \neq bq$; assim, S_1 e S_2 formam uma partição de S.

Contemos as cardinalidades de S, S_1 e S_2. A de S é fácil: $|S| = \frac{p-1}{2} \cdot \frac{q-1}{2}$. Vamos à de S_1: fixe b. Então $a < bp/q$. Note que $bp/q < p/2$, de modo que há, então, $\lfloor \frac{bp}{q} \rfloor$ valores para a, com b fixado. Portanto $|S_1| = \sum_{j=1}^{(q-1)/2} \lfloor \frac{jp}{q} \rfloor$. Analogamente, $|S_2| = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor$. Substituindo em $|S| = |S_1| + |S_2|$, o resultado segue. ∎

Você pode se sentir mais à vontade com esse fato observando a seguinte figura, que exibe a identidade

acima para $p = 7$ e $q = 11$:



E chegamos enfim à celebrada lei da reciprocidade quadrática:

Teorema 5.3. *Sejam p e q primos ímpares. Então*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Demonstração

Basta juntar os lemas anteriores: sendo $M = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor$ e $N = \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{pk}{q} \right\rfloor = 1$ e lembrando que $M + N = \frac{p-1}{2} \cdot \frac{q-1}{2}$,

$$\left(\frac{p}{q}\right) = (-1)^N \quad \text{e} \quad \left(\frac{q}{p}\right) = (-1)^M \implies \left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

∎

Isto quer dizer que o problema de saber se c é resíduo quadrático módulo qualquer número está completamente resolvido.

Exemplo 5.1.

Verificar se 1028 é resíduo quadrático de 2008.

Resolução

Primeiro, note que $\text{mdc}(1028, 2008) = 4$. Então basta verificar se $1028/4 = 257$ é resíduo quadrático de $2008/4 = 502$. Como $502 = 2 \cdot 251$, basta ver se 257 é resíduo quadrático de 2 e 251. De 2 certamente é. Vejamos se é 251:

$$\left(\frac{257}{251}\right) = \left(\frac{6}{251}\right) = \left(\frac{2}{251}\right)\left(\frac{3}{251}\right)$$

Poderíamos calcular 2^{125} e 3^{125} módulo 251, mas para que correr o risco de errar conta? Basta usar a reciprocidade quadrática: para o 2,

$$\left(\frac{2}{251}\right) = (-1)^{\frac{251^2-1}{8}} = (-1)^{\frac{250 \cdot 252}{8}} = (-1)^{125 \cdot 126} = 1$$

e para o 3

$$\left(\frac{3}{251}\right)\cdot\left(\frac{251}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{251-1}{2}} \iff \left(\frac{3}{251}\right)\cdot\left(\frac{2}{3}\right) = 1 \iff \left(\frac{3}{251}\right) = -1$$

Assim, $\left(\frac{257}{251}\right) = 1\cdot(-1) = -1$ e, portanto, 1028 não é resíduo quadrático de 2008.

Exercícios

14. Prove que $2^{509} \equiv -1 \pmod{1019}$ sem calcular 2^{509} mód 1019.
15. Prove que se $2^{2^n}+1$ é primo, então todo número inteiro é seu resíduo quadrático ou raiz primitiva.
16. Prove que $F_n = 2^{2^n}+1$ é primo se, e somente se, $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.
17. Encontre o conjunto de todos os divisores primos de $f(x) = x^2+2$, sendo x inteiro.
18. Encontre o conjunto de todos os divisores primos de $f(x) = x^2-15$, sendo x inteiro.
19. Existe um quadrado perfeito com seus quatro últimos algarismos não nulos e iguais?
20. Seja $f(x) = (x^2-13)(x^2-17)(x^2-221)$. Prove que $f(x) \equiv 0 \pmod{n}$ sempre tem solução.
21. Seja $p = 4k+1$ um primo, k inteiro positivo. Prove que $k^k - 1$ é múltiplo de p.

6. Outras potências mód p

Agora, vamos estudar algumas somas.

Teorema 6.1. *Seja $S_k = 1^k + 2^k + 3^k + \cdots + (p-1)^k$. Então*

$$S_k \equiv \begin{cases} p-1 \pmod{p} & \text{se } p-1 \mid k \\ 0 \pmod{p} & \text{caso contrário} \end{cases}$$

Demonstração

Se $p-1 \mid k$ então $i^k \equiv 1 \pmod{p}$ para $i = 1, 2, \ldots, p-1$ e, portanto, $S_k \equiv p-1 \pmod{p}$.

Caso contrário, seja g uma raiz primitiva de p. Então note que os números 1, g, g^2, $\ldots$, g^{p-2} são todos os números 1, 2, $\ldots$, $p-1$ mód p. Assim, como $g^k \not\equiv 1 \pmod{p}$,

$$S_k \equiv 1^k + g^k + g^{2k} + \cdots + g^{(p-2)k} = \frac{g^{(p-1)k}-1}{g^k-1} \equiv 0 \pmod{p}$$

∎

E se quisermos saber os resíduos módulo p^2 ou uma potência maior? Nesse caso, utilizamos binômio de Newton ou a sua generalização:

Teorema 6.2. *Seja α real. Sendo*

$$\binom{\alpha}{k} = \begin{cases} 1 & \text{se } k = 0 \\ \frac{\alpha(\alpha-1)(\alpha-2)\cdots(\alpha-k+1)}{k!} & \text{se } k > 0 \end{cases}$$

então

$$(x+y)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k y^{\alpha-k}$$

Demonstração

É só expandir $(1+y/x)^\alpha$ na série de Taylor. ∎

Exemplo 6.1.

Prove que o numerador de S_{-1}, quando este é escrito em forma de fração irredutível, é múltiplo de p^2, para $p > 3$.

Resolução

Temos $S_{-1} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$. Como usar binômio de Newton nesse caso? Basta usar em $(p-i)^{-1}$:

$$(p-i)^{-1} = \sum_{k=0}^{\infty} \binom{-1}{i} p^k (-i)^{-1-k} \equiv (-i)^{-1} + (-1)p(-i)^{-2} \pmod{p^2}$$

Parece uma grande roubalheira, mas está certo! De fato, sendo i^{-1} o inverso de i mód p^2,

$$(p-i)(-i^{-1} - pi^{-2}) \equiv -pi^{-1} - p^2 i^{-2} + ii^{-1} + pii^{-2} \equiv -pi^{-1} + 1 + pi^{-1} \equiv 1 \pmod{p^2}$$

Assim, somando todas as congruências

$$(p-i)^{-1} + i^{-1} \equiv -pi^{-2} \pmod{p^2}$$

obtemos

$$2S_{-1} \equiv -p \sum_{i=1}^{p-1} i^{-2} \pmod{p^2}$$

Basta então provar que

$$-p \sum_{i=1}^{p-1} i^{-2} \equiv 0 \pmod{p^2} \iff \sum_{i=1}^{p-1} i^{-2} \equiv 0 \pmod{p},$$

o que é verdade, já que $p-1$ não divide -2 (isso, é claro, se $p > 3$).

Um pequeno detalhe é que fizemos a transição de i^{-1} ser o inverso de i mód p^2 para ser o inverso de i mód p. Isso é verdade, mas o caminho contrário não pode ser tomado. Então tome cuidado ao trabalhar com inversos em diversos módulos! ∎

Provemos agora o teorema de Wolstenholme:

Teorema 6.3. *Seja $p > 3$ primo. Então*

$$\binom{2p-1}{p-1} \equiv 1 \pmod{\text{mód. } p^3}$$

Demonstração

É "só" abrir:

$$\binom{2p-1}{p-1} = \frac{2p-1}{p-1} \cdot \frac{2p-2}{p-2} \cdot \frac{2p-3}{p-3} \cdot \ldots \cdot \frac{p+1}{1} = \left(1 + \frac{p}{p-1}\right)\left(1 + \frac{p}{p-2}\right)\left(1 + \frac{p}{p-3}\right) \cdots \left(1 + \frac{p}{1}\right)$$

Lembrando que $(x+x_1)(x+x_2)\cdots(x+x_n) = x^n + \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \cdots + \sigma_n$, sendo σ_k a soma de todos os $\binom{n}{k}$ produtos de k números distintos entre $x_1, x_2, \ldots, x_n$,

$$\binom{2p-1}{p-1} = 1^{p-1} + \left(\frac{p}{p-1} + \frac{p}{p-2} + \frac{p}{p-3} + \cdots + \frac{p}{1}\right) 1^{p-2} + \sigma_2 1^{p-3} + \cdots + \sigma_{p-1}$$

Utilizando a famosa identidade $\sigma_2 = ((\sigma_1)^2 - s_2)/2$ e que os denominadores de σ_k são múltiplos de p^3 para $k \geq 3$, temos

$$\binom{2p-1}{p-1} = 1 + pS_1 + \frac{p^2}{2}(S_1^2 - 2S_2) + \frac{p^3 A}{B}$$

em que

$$S_1 = \frac{1}{p-1} + \frac{1}{p-2} + \frac{1}{p-3} + \cdots + \frac{1}{1} \quad \text{e} \quad S_2 = \frac{1}{(p-1)^2} + \frac{1}{(p-2)^2} + \frac{1}{(p-3)^2} + \cdots + \frac{1}{1^2}$$

Como já provamos que S_1 tem numerador múltiplo de p^2 e S_2 tem numerador múltiplo de p, o resultado segue. ∎

Exercícios

22. Seja $p > 3$ um primo. Sendo

$$\frac{1}{1^3} + \frac{1}{2^3} + \frac{1}{3^3} + \cdots + \frac{1}{(p-1)^3} = \frac{m}{n}$$

com m e n inteiros primos entre si, prove que p^3 divide m.

23. Seja $p > 3$ um primo. Sendo

$$\frac{1}{1^p} + \frac{1}{2^p} + \frac{1}{3^p} + \cdots + \frac{1}{(p-1)^p} = \frac{m}{n}$$

com m e n inteiros primos entre si, prove que p^3 divide m.

24. Seja $p > 3$ um primo. Prove que $\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}$.

7. O lema de Thue

Muitos dos fatos mais interessantes da Teoria dos Números podem ser obtidos utilizando o princípio da casa dos pombos.

Lema 7.1. *Sejam m e n inteiros positivos primos entre si e sejam a e b inteiros positivos tais que $ab > n$. Então existe $x \in \{1, 2, \ldots, a-1\}$ e $y \in \{1, 2, \ldots, b-1\}$ tais que*

$$mx \equiv \pm y \pmod{n}$$

Demonstração

Considere as ab expressões da forma $mx + y$

$$\begin{array}{ccccc} m\cdot 1+1 & m\cdot 1+2 & m\cdot 1+3 & \cdots & m\cdot 1+b \\ m\cdot 2+1 & m\cdot 2+2 & m\cdot 2+3 & \cdots & m\cdot 2+b \\ m\cdot 3+1 & m\cdot 3+2 & m\cdot 3+3 & \cdots & m\cdot 3+b \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m\cdot a+1 & m\cdot a+2 & m\cdot a+3 & \cdots & m\cdot a+b \end{array}$$

Como $ab > n$, existem duas expressões que deixam o mesmo resto na divisão por n, digamos $mx_1 + y_1$ e $mx_2 + y_2$, com $x_1 > x_2$. Assim,

$$mx_1 + y_1 \equiv mx_2 + y_2 \pmod{n} \iff m(x_1 - x_2) \equiv y_2 - y_1 \pmod{n}$$

Note que $y_1 \neq y_2$ pois senão $x_1 = x_2$. Assim, sendo $x = x_1 - x_2$ e $y = |y_1 - y_2|$, temos $0 < x \leq a - 1$ e $0 < y \leq b - 1$ e

$$mx \equiv \pm y \pmod{n}$$

∎

Lema 7.2. *Se $p = 4k + 1$ é primo, existe x tal que $x^2 \equiv -1 \pmod{p}$.*

Demonstração

Poderíamos aplicar diretamente o critério de Euler (e o resultado seria imediato) para verificar se -1 é resíduo quadrático ou mesmo tomar diretamente $x = ((p-1)/2)!$ e utilizar o teorema de Wilson ($(p-1)! \equiv -1 \pmod{p}$), mas vamos mostrar mais uma aplicação interessante da Combinatória, agora com contagem.

Vamos repartir o conjunto $\{1, 2, \ldots, p-1\}$ em conjuntos da forma $C_a = \{a, p-a, a^{-1}, p-a^{-1}\}$, em que a^{-1} é o inverso de a mód p. Note que $C_1 = \{1, p-1\}$, pois o inverso de 1 mód p é 1. Além desse conjunto, como $p - 1 = 4k$ é múltiplo de 4, deve haver mais um conjunto C_m com 2 elementos. Isso ocorre quando $m \equiv p - m^{-1} \pmod{p} \iff m^2 \equiv -1 \pmod{p}$. Note que não pode ocorrer $m \equiv p - m \pmod{p}$ nem $m \equiv m^{-1} \pmod{p}$. ∎

Agora, vamos provar um dos teoremas mais belos da Teoria dos Números.

Teorema 7.1. *Todo primo da forma $p = 4k + 1$ pode ser escrito como soma de dois quadrados.*

Demonstração

Seja m tal que $m^2 \equiv -1 \pmod{p}$ (ele existe pelo lema anterior). Assim, sendo $\lceil \sqrt{p} \rceil^2 > p$, pelo lema de Thue, existem inteiros $x \in \{1, 2, \ldots, \lceil \sqrt{p} \rceil - 1\}$ e $y \in \{1, 2, \ldots, \lceil \sqrt{p} \rceil - 1\}$ tais que

$$mx \equiv \pm y \pmod{p} \implies m^2x^2 \equiv y^2 \pmod{p} \iff x^2 + y^2 \equiv 0 \pmod{p}$$

Assim, $x^2 + y^2$ é múltiplo de p e, como $0 < x, y < \lceil \sqrt{p} \rceil$, $0 < x^2 < p$ e $0 < y^2 < p$, $0 < x^2 + y^2 < 2p$. Mas o único múltiplo de p entre 0 e $2p$ é p, ou seja, $p = x^2 + y^2$ pode ser escrito como soma de dois quadrados. ∎

Exercícios

Alguns dos exercícios não são exatamente relacionados com os tópicos tratados aqui, mas são legais, então decidi colocá-los assim mesmo!

25. (Romênia 1997) Seja A o conjunto dos inteiros da forma $a^2 + 2b^2$, sendo a e b inteiros com $b \neq 0$. Prove que se p é primo e $p^2 \in A$ então $p \in A$.

26. Encontre todos os primos que podem ser escritos na forma $x^2 + 3y^2$.

27. Encontre todos os primos que podem ser escritos na forma $a^2 + ab + b^2$.

28. Encontre todos os primos que podem ser escritos na forma $a^2 + ab - b^2$.

29. (OBM 2007, Nível 2, Problema 3) Mostre que existe um inteiro positivo a tal que $\frac{a^{29}-1}{a-1}$ tem pelo menos 2007 fatores primos distintos.

Dica: use mdc*, mas use mesmo! Um possível valor de a é $2^{2^{2007}}$.*

30. (OBM 2005, Problema 6) Dados a, c inteiros positivos e b inteiro, prove que existe x inteiro positivo tal que

$$a^x + x \equiv b \pmod{c},$$

ou seja, existe x inteiro positivo tal que c é um divisor de $a^x + x - b$.

Dica: use Euler-Fermat e o teorema chinês dos restos:

Teorema 7.2. *Sejam $m_1, m_2, \ldots, m_k$ inteiros primos dois a dois. Então o sistema de congruências a seguir admite solução.*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

31. (Um resultado clássico, mas interessante) Sejam $f(x)$ um polinômio não constante com coeficientes inteiros e k um inteiro positivo. Prove que existe um inteiro n tal que $f(n) \neq 0$ tem pelo menos k fatores primos distintos.

Dica: Primeiro prove que uma infinidade de divisores primos divide algum $f(n)$, da seguinte maneira: suponha que o conjunto dos primos que dividam todos os $f(n)$'s seja finito; considere um t inteiro tal $f(t) \neq 0$ e seja N tal que os expoentes dos primos p que dividem $f(t)$ sejam maiores em $N!$ do que em $f(t)$; então, os expoentes de todos os primos p_i que dividem $f(N! + t) = f(t) + M \cdot N!$ são limitados pelo expoente de p_i em $f(t)$; finalize com casa dos pombos para provar que $f(x) = k$ tem infinitas soluções para algum k, chegando a uma contradição; para fechar, é só usar o teorema chinês dos restos.

8. Referências bibliográficas

[1] Como já virou costume, muitos dos problemas foram extraídos do Mathlinks e do site do John Scholes...

`http://www.mathlinks.ro/`

`http://www.kalva.demon.co.uk/`

[2] ... exceto, é claro, os problemas mais recentes (após 1996) da OBM, que são do site oficial da OBM:

`http://www.obm.org.br/`

[3] Um grande livro de Teoria dos Números: *Fundamental Number Theory with Applications*, de Richard Mollin. Foi a base da parte sobre resíduos quadráticos e teorema de Thue.

[4] Mais um livro legal sobre primos: *Números primos: mistérios e recordes*, do grande especialista de Teoria dos Números (e brasileiro!) Paulo Ribenboim. A demonstração de que existe raiz primitiva módulo primo ímpar é de lá.

[5] A Wikipedia tem alguns artigos legais sobre Teoria dos Números! O nosso novo lema de Hensel foi extraído de

`http://en.wikipedia.org/wiki/Hensel's_lemma/`

[6] Você pode encontrar mais sobre raízes primitivas (e um monte de outros fatos da Teoria dos Números) na Eureka! 2: *Divisibilidade, Congruências e Aritmética Módulo n*, de Carlos G. T. de A. Moreira.

[7] Você pode encontrar mais sobre reciprocidade quadrática na Eureka! 15: *Reciprocidade Quadrática*, Carlos Gustavo T. de A. Moreira e Nicolau Corção Saldanha.