Teorema Chinês dos Restos

Samuel Barbosa

22 de março de 2006

Teorema 1. *(Bézout) Sejam a e b inteiros não nulos e d seu mdc. Então existem inteiros x e y tais que $d = ax + by$. Se a e b são positivos podemos escolher $x > 0$ e $y < 0$, ou vice-versa.*

Prova. *Seja $P = \{ax+by | ax+by > 0 \text{ e } x, y \in \mathbb{Z}\}$. O conjunto P é não vazio pois $0 < a^2+b^2 = a\times a+b\times b \in P$. Seja f o menor elemento de P. Claramente $d = mdc(a, b) | f$ Como $f, d > 0$, para mostrarmos que $d = f$ basta que $f | d$. Seja $a = qf + r$, com $q \in \mathbb{Z}$ e $0 \leq r < f$. Assim $0 \leq r = a(1 - qx) + b(-qy) \in \mathbb{Z}$. Como $r < f \Rightarrow r = 0$. Analogamente $f | b$. Então $f | mdc(a, b) = d$. A outra parte é deixada para o leitor.*

Teorema 2. *Se $mdc(a, m) = 1$, então existe um inteiro x tal que $ax \equiv 1 \pmod{m}$. Quaisquer dois tais x são congruentes $\pmod{m}$ e se $mdc(a, m) > 1$ não existe solução.*

Prova. *Pelo teorema de Bézout, se $mdc(a, m) = 1$ existem x e y tais que $ax + my = 1$. mas isto significa que $ax \equiv 1 \pmod{m}$. Reciprocamente, se $ax \equiv 1 \pmod{m}$ existe um y tal que $ax + my = 1 \Rightarrow mdc(a, m) = 1$. Se $ax_1 \equiv 1 \equiv ax_2 \pmod{m} \Rightarrow a(x_1 - x_2) \equiv 0 \pmod{m}$, mas $mdc(a, m) = 1 \Rightarrow m | (x_1 - x_2) \Rightarrow x_1 \equiv x_2 \pmod{m}$*

Tal inteiro x é chamado de inverso de a módulo m. Acabamos de mostrar que se $mdc(a, m) = 1$, o inverso de a existe é único módulo m. Dizemos que os inteiros $a_1, a_2, \ldots, a_m$ são primos entre si, dois a dois, se $mdc(a_i, a_j) = 1$ *quando* $i \neq j$. Vejamos nosso resultado principal:

Teorema 3. *(***Teorema Chinês dos Restos***) Sejam $m_1, m_2, \ldots, m_r$, r inteiros positivos que são primos entre si, dois a dois, e sejam $a_1, a_2, \ldots, a_r$, r inteiros quaisquer. Então, o sistema de conguências:*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

admite uma solução x. Além disso, as soluções são únicas módulo $m = m_1 m_2 \ldots m_r$.

Prova. *Escrevendo $m = m_1 m_2 \ldots m_r$, vemos que $\dfrac{m}{m_j}$ é um inteiro e $mdc\left(\dfrac{m}{m_j}, m_j\right) = 1$. Então pelo teorema 2, para cada j, existe um inteiro b_j tal que $\left(\dfrac{m}{m_j}\right) b_j \equiv 1 \pmod{m_j}$. Claramente $\left(\dfrac{m}{m_j}\right) b_j \equiv 0 \pmod{m_i}$ para $i \neq j$. Definamos*

$$x_0 = \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j$$

Consideremos x_0 módulo m_i: $x_0 \equiv \dfrac{m}{m_i} b_j a_j \equiv a_i \pmod{m_i}$. Então x_0 é uma solução do nosso sistema. Se x_0 e x_1 são soluções do nosso sistema então: $x_0 \equiv x_1 \pmod{m_i}$ para cada i. Como $mdc(m_i, m_j) = 1$ se $i \neq j$ então $x_0 \equiv x_1 \pmod{m}$.

Exemplo 1. *Encontre o menor inteiro positivo x tal que $x \equiv 5 \pmod 7$, $x \equiv 7 \pmod{11}$ e $x \equiv 3 \pmod{13}$.*

Usando o teorema anterior com $m_1 = 5, m_2 = 7, m_3 = 11, a_1 = 5, a_2 = 7$ e $a_3 = 3$ podemos achar $x \equiv 887(\text{ mod } 1001 = 7.11.13)$. Como a solução é única módulo m, isto significa que, dentre os números $1, 2, \cdots, 1001$ a menor solução positiva é 887.

Exercício 1. *(Estônia 2000) Determine todos os restos possíveis da divisão do quadrado de um número primo com 120 por 120.*

Aconselhamos que o leitor faça alguns exemplos numéricos até se acostumar com o algoritmo usado para encontrar x_0. Provamos no teorema passado que todas as soluções daquele sistema de congruências são os termos de uma $P.A$ de razão m. Em geral, usamos o teorema 3 apenas para garantir que um sistema de congruências admite uma solução. Os próximos exemplos devem deixar isto mais claro.

Exemplo 2. *Para cada número natural n, existe uma sequência arbitrariamente longa de números naturais consecutivos, cada um deles sendo divisível por uma s-ésima potência de um número natural maior que 1.*

Prova. *Dado $m \in \mathbb{N}$ considere o cunjunto $\{p_1, p_2, \ldots, p_m\}$ de primos distintos. Como $mdc(p_i^s, p_j^s) = 1$, então pelo teorema 3, existe x tal que $x \equiv -i \pmod{p_i^s}$ para $i = 1, 2, \ldots m$. Cada um dos números do conjunto $\{x+1, x+2, \ldots, x+m\}$ é divisível por um número da forma p_i^s.*

Exemplo 3. *(USAMO 1986)*

(a) Existem 14 inteiros positivos consecutivos tais que, cada um é divisível por um ou mais primos p do intervalo $2 \leq p \leq 11$?

(b) Existem 21 inteiros positivos consecutivos tais que, cada um é divisível por um ou mais primos p do intervalo $2 \leq p \leq 13$?

Solução. *(a) Não. Suponha que existam tais inteiros. Da nossa lista de 14 inteiros consecutivos, 7 são números pares. Vamos observar os ímpares: $a, a+2, a+4, a+6, a+8, a+10$ e $a+12$. Podemos ter no máximo três deles divisíveis por 3, dois por 5, um por 7 e um por 11. Veja que $3 + 2 + 1 + 1 = 7$. Pelo Princípio da Casa dos Pombos, cada um desses ímpares é divisível por exatamente um primo do conjunto $\{3, 5, 7, 11\}$. veja que os múltiplos de 3 só podem ser $\{a, a+6, a+12\}$. Dois dos números restantes $(a+2, a+4, a+8,$ e $a+10)$ são divisíveis por 5. Mas isto é impossível. (b) Sim. Como os números $\{210, 11, 13\}$ são primos entre si, dois a dois, pelo teorema 3 existe um inteiro positivo $n > 10$ tal que:*

$$n \equiv 0(\text{ mod } 210 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot)$$
$$n \equiv 1(\text{ mod } 11)$$
$$n \equiv -1(\text{ mod } 13)$$

Veja que o conjunto $\{n-10, n-9, \ldots, n+9, n+10\}$ satisfaz as condições do item (b).

Exemplo 4. *(Olimpíada de São Petesburgo 1990) Dado um polinômio $F(x)$ com coeficientes inteiros, tal que, para cada inteiro n, o valor de $F(n)$ é divisível por pelo menos umm dos inteiros $a_1, a_2, \cdots, a_m$. Prove que podemos encontrar um índice k tal que $F(n)$ é divisível por a_k para cada inteiro positivo n.*

Solução. *Suponha que não exista tal índice. Para cada índice k $(k = 1, 2, \ldots, m)$ existe um inteiro x_k, tal que , $F(x_k)$ não é divisível por a_k. Assim, existem números $d_k = p_k^{\alpha_k}$ onde os p_k são primos, tais que, d_k divide a_k mas não dividem $F(x_k)$. Se exitem potências do mesmo primo entre esses números, podemos apagar aquelas deixando apenas uma que tem expoente mínimo. Caso $F(x)$ não seja divisível por uma*

potência apagada, não será pela potência que tem expoente mínimo. Essa deleções garatem que nossa nova coleção $d_1, d_2, \ldots, d_j$ de potências de primos contém apenas inteiros primos entre si, dois a dois. Pelo teorema 3, exite um inteiro N, tal que, $N \equiv x_k (\mod d_k)$ para $k \in \{1, 2, \ldots, j\}$. Suponhamos que $d_k | F(N)$. Sabemos que $x - y | F(x) - F(y) \Rightarrow N - x_k | F(N) - F(x_k)$. Mas $d_k | N - x_k$ e $d_k | F(N) \Rightarrow d_k | F(x_k)$. Uma contradição! Logo $F(N)$ não é divispivel por nenhum d_k, mas isto contradiz a hipótese sobre os a_i.

Teorema 4. *(***Paul Erdös***) Existe uma progressão aritmética infinita de números ímpares, nenhum deles da forma $2^k + p$, onde $k \in \mathbb{Z}_+$, e p é um primo.*

Lema. *Todo número natural satisfaz pelo menos uma das seguintes congruências:*

$$\begin{array}{lll} (1)\ k \equiv 0 (\mod 2) & (2)\ k \equiv 0 (\mod 3) & (3)\ k \equiv 1 (\mod 4) \\ (4)\ k \equiv 3 (\mod 8) & (5)\ k \equiv 7 (\mod 12) & (6)\ k \equiv 23 (\mod 24) \end{array}$$

Prova. *Se um número k não satisfaz (1) ou (2), então não é divisível por 2 ou 3.Então deve ser da forma $24t + r$ onde t é um inteiro e r é m dos números $1, 5, 7, 11, 13, 17, 19, 23$. Uma verificação direta mostra que k tem que satisfazer as congruências $(3), (3), (5), (4), (3), (3), (4), (6)$, respectivamente.*

Corolário. *Se k é um inteiro não-negativo, então pelo menos uma das seguintes congruências é satisfeita:*

$$\begin{array}{lll} (7)\ 2^k \equiv 1 (\mod 3) & (8)\ 2^k \equiv 1 (\mod 7) & (9)\ 2^k \equiv 2 (\mod 5) \\ (10)\ 2^k \equiv 2^3 (\mod 17) & (11)\ 2^k \equiv 2^7 (\mod 13) & (12)\ 2^k \equiv 2^{23} (\mod 241) \end{array}$$

Prova. *Basta verificarmos que $2^2 \equiv 1 (\mod 3)$, $2^3 \equiv 1 (\mod 7)$, $2^4 \equiv 1 (\mod 5)$, $2^8 \equiv 1 (\mod 17)$, $2^{12} \equiv 1 (\mod 13)$, $2^{12} \equiv -1 (\mod 241)$, então $2^{24} \equiv 1 (\mod 241)$. Devido à estas, as congruências $(1), (2), (3), (4), (5), (6)$ implicam em $(7), (8), (9), (10), (11), (12)$, respectivamente.*

Prova do Teorema. *Em virtude do Teorema Chinês dos Restos, existe um natural a que satisfaz as congruências:*

$$\begin{array}{lll} a \equiv 1 (\mod 2 = m_1) & a \equiv 1 (\mod 3 = m_2) & a \equiv 1 (\mod 7 = m_3) \\ a \equiv 2 (\mod 5 = m_4) & a \equiv 2^3 (\mod 17 = m_5) & a \equiv 2^7 (\mod 13 = m_6) \\ a \equiv 2^{23} (\mod 241 = m_7) & a \equiv 3 (\mod 31 = m_8) & \end{array}$$

Além disso, existem infinitas progressões aritméticas de a´s que satisfazem essas congruências. Todas essas progressões tem razão múltipla de m , onde $m = m_1 m_2 \ldots m_8$, como no enunciado do teorema 3. Claramente, os termos dessas progressões são ímpares. Se a é qualquer termo de uma dessas progressões, o corolário do lema diz que $a - 2^k$ é divisível por pelo menos um dos primos $3, 7, 5, 17, 13, 241$. Por outro lado, $a \equiv 3 (\mod 31)$ e para qualquer $k \in \mathbb{Z}_+$ o número 2^k é congruente a um dos números $1, 2, 4, 8 (\mod 31)$. Consequentemente, $a - 2^k$ é congruente a um dos números $2, 1, -9, -5, -13 (\mod 31)$. Mas nenhum desses números é congruente mod 31 *a qualquer um dos números $3, 7, 5, 17, 13, 241$. Então o número $a - 2^k$ não pode ser $3, 7, 5, 17, 13$ ou 241, por outro lado, é divisível por pelo menos um deles. Então é um número composto. Assim não existe um primo p tal que $a = 2^k + p$.*

Corolário. *(Sierpiński) Existem infinitos números naturais n tais que, cada um dos números $n2^k + 1$, $k \in \mathbb{Z}_+$, é composto.*

Prova. *A prova do teorema anterior, mostra que existem infinitos naturais n tais que para qualquer inteiro não-negativo k, o número $-n - 2^k$ (ou melhor dizendo $2^k + n$) é divisível por pelo menos um dos números $3, 7, 5, 17, 13, 241$. Seja P o produto de todos esses primos. Em virtude do provado acima, o número $n + 2^{k[\phi(P)-1]}$ admite um divisor primo $p | P$. Mas $2^{k\phi(P)} \equiv 1 (\mod P)$, como $n + 2^{k[\phi(P)-1]} \equiv 0 (\mod p) \Rightarrow n2^k + 1 \equiv 0 (\mod p)$. Claramente este numero é composto se $n > 241 \geq p$.*

O próximo exemplo é uma generalização de um problema do Banco da IMO de 1992.

Exemplo 5. *Prove que dado $n \in \mathbb{N}$ existe um conjunto de n elementos $A \subset \mathbb{N}$ tal que para todo $B \subset A$, $B \neq \emptyset$, $\sum_{x \in B} x$ é um potência não trivial (isto é, um número da forma m^k , onde m e k são inteiros maiores ou iguais a 2).*

Solução. *$A = \{4\}$ e $A = \{9, 16\}$ são soluções para $n = 1$ e $n = 2$ respectivamente. Estes serão nossos caso iniciais de indução. Suponha que $A = \{x_1, x_2, \cdots, x_n\}$ é um conjunto com n elementos e para todo $B \subset A$, $B \neq \emptyset$, $\sum_{x \in B} x = m_B^{k_B}$. Vamos mostrar que existe $c \in \mathbb{N}$ tal que $\tilde{A} = \{cx_1, cx_2, \cdots, cx_n, c\}$ satisfaz o enunciado. Seja $l = mmc\{k_B, B \subset A, B \neq \emptyset\}$. Para cada $B \subset A, B \neq \emptyset$ associemos um primo $p_B > l$, de forma que $B_1 \neq B_2 \Rightarrow p_{B_1} \neq p_{B_2}$, e associemos um natural r com $r_B \equiv 0 (mod\, p_X), \forall X \neq B, l r_B + 1 \equiv 0 (mod\, p_B)$ (tal r_B existe pelo Teorema Chinês dos Restos). Defina $c = \prod_{\substack{B \subset A \\ B \neq \emptyset}} (1 + m_B^{k_B})^{l r_B}$*

Como c é uma potência l-ésima, c é um potência k_B-ésima para todo $B \subset A$, $B \neq \emptyset$, portanto, para $B' \subset \{cx_1, cx_2, \cdots, cx_n\}, B' \neq \emptyset$ teremos $B' = \{cx | x \in B\}$ para algum $B \subset A, B \neq \emptyset$. Logo $\sum_{x \in B'} x$ será uma potência k_B-ésima. Além disso,

$$\sum_{x \in B' \cup \{c\}} x = \left[\prod_{\substack{X \subset A \\ X \neq \emptyset, B}} (1 + m_X^{k_B})^{l r_X} \right] \cdot (1 + m_b^{k_B})^{l r_b + 1}$$

é uma p_B-ésima potência.

Problemas

Problema 1. *Existem n inteiros consecutivos tal que cada um contém um fator primo repetido k vezes?*

Problema 2. *Um ponto $(x, y) \in Z^2$ é legal se $mdc(x, y) = 1$. Prove ou disprove: Dado um inteiro positivo n, existe um ponto $(a, b) \in Z^2$ cuja distância a todo ponto legal e pelo menos n?*

Problema 3. *Sejam $m_o, m_1, ..., m_r$ inteiros positivos que são primos entre si, dois a dois. Mostre que existem $r + 1$ inteiros consecutivos $s, s + 1, ..., s + r$ tal que m_i divide $s + i$ para $i = 0, 1, ..., r$.*

Problema 4. *Seja $P(X)$ um polinômio com coeficientes inteiros e k é um inteior qualquer. Prove que existe um inteiro m tal que $P(m)$ tem pelo menos k fatores primos distintos.*

Problema 5. *(Koréia 1999) Encontre todos os inteiros n tais que $2^n - 1$ é um múltiplo de 3 e $\frac{2^n - 1}{3}$ é um divisor de $4m^2 + 1$ para algum inteiro m.*

Problema 6. *(Romênia 1995) Seja $f : \mathbb{N} - \{0, 1\} \to \mathbb{N}$ definida por $f(n) = mmc[1, 2, ..., n]$. Prove que para todo $n \geq 2$, existem n números consecutivos para os quais f é constante.*

Problema 7. *(Olimpíada Nórdica 1998)*

(a) Para quais inteiros positivos n existe um sequência $x_1, x_2, \ldots, x_n$ contendo cada um dos inteiros $1, 2, \ldots, n$ exatamente uma vez, e tal que k divide $x_1 + x_2 + \cdots + x_k$ para $k = 1, 2, \cdots, n$?

(b) Existe uma sequência infinita $x_1, x_2, \ldots$ contendo todo inteiro positivo exatamente uma vez, e tal que para cada inteiro positivo k, k divide $x_1 + x_2 + \cdots + x_k$?

Problema 8. *Seja n um número natural arbitrário. Prove que existe um par de naturais (a, b) tais que $mdc(a + r, b + s) > 1 \ \forall \ r, s = 1, 2, \ldots, n$.*

Problema 9. *(OBM 2005) Dados os inteiros positivos a, c e o inteiro b, prove que existe um inteiro positivo x tal que $a^x + x \equiv b \pmod{c}$.*

Problema 10. *(Cone Sul 2003) Demonstrar que existe uma sequência de inteiros positivos $x_1, x_2, \ldots$ que satisfaz as duas condições seguintes:*

(a) contém exatamente uma vez cada um dos inteiros positivos,

(b) a soma parcial $x_1 + x_2 + \ldots x_n$ é divisível por n^n.

Problema 11. *(República Tcheca e Eslovaca 1997) Mosrte que existe uma sequência crescente $\{a_n\}_{n=1}^{\infty}$ de números naturais tais que para $k \geq 0$, a sequência $\{a_n + k\}$ contém um número finito de primos.*

Problema 12. *Considere o inteiro $c \geq 1$ e a sequência definida por $a_1 = c$ e $a_{i+1} = c^{a_i}$. Mostre que esta sequência se torna eventualmente constante quando reduzimos módulo n para algum inteiro positivo n (isto significa que $a_m \equiv a_j \pmod{n}$ se $m \geq j$).*

Problema 13. *(Putnam 1994) Pra qualquer intiro positivo a, seja $n_a = 101a - 100 \cdot 2^a$. Mostre que para $0 \leq a, b, c, d, \leq 99, n_a + n_b \equiv n_c + n_d \pmod{10100}$ implica $\{a, b\} = \{c, d\}$.*

Problema 14. *Seja a_n a sequência definida por*

$$a_n = \begin{cases} 1999 & se \;\; n = 1, \\ a_{n-1} + p(n) & se \;\; n > 1 \end{cases}$$

onde $p(n)$ é o menor divisor primo de n. Mostre que a_n possui infinitos múlriplos de 7.

Problema 15. *Considere a sequência de inteiros positivos $\{a_n\}$, $n = 1, 2, 3, \ldots$ satisfazendo a condição*

$$0 < a_{n+1} - a_n \leq 2001$$

para todo $n = 1, 2, 3, \ldots$. Prove que existe um número infinito de pares de inteiros positivos (p, q) tais que $p < q$ e a_p é um divisor de a_q.

Problema 16. *O conjunto $S = \{1/r : 1, 2, 3, \ldots\}$ contém progressões aritméticas de vários tamanhos. Por exemplo, $\{1/20; 1/8; 1/5\}$ é uma de tais progressões, de tamanho 3 (e razão $3/40$). Mais ainda, essa é uma progressão maximal em S de tamanho 3 pois ela não pode ser estendida à esquerda ou à direita ($-1/40$ e $11/40$) não são elementos de S. Mostre que existe uma progressão maximal em S de tamanho m para todo $m \geq 3$.*