TEOREMA CHINÊS DOS RESTOS

Ramyro Corrêa

1 Introdução

O Teorema Chinês dos Restos é uma ferramenta muito utilizada em problemas de teoria dos números em olimpíadas de matemática, geralmente com a ideia de tomar algum número esperto com a finalidade de conseguir algumas propriedades interessantes.

2 O Teorema

2.1 Teorema Chinês dos Restos

Seja $n \geq 2, n \in N$, e $a_1, a_2, ..., a_n \in Z; b_1, b_2, ..., b_n \in N$ com $b_1, b_2, ..., b_n$ 2 a 2 primos entre si. Então, existe $M \in N$ tal que

$$M \equiv a_1 \pmod{b_1}$$

$$M \equiv a_2 \pmod{b_2}$$

$$...$$

$$M \equiv a_n \pmod{b_n}$$

Prova: Seja $B = b_1.b_2...b_n$ e defina $M_i = \frac{B}{b_i}$. Como $mdc(M_i, b_i) = 1$, então existe c_i tal que $M_i c_i \equiv 1 \pmod{b_i}$. Então, tome

$$M = \sum_{i=1}^{n} M_i a_i c_i$$

Então, $M \equiv a_i \pmod{b_i}$ para todo $i = 1, 2, ..n$, como desejado.

2.2 Exemplos

2.3 Exemplo 1

(Teorema de Schur) Seja $P(x)$ um polinômio de coeficientes inteiros não-constante e não-nulo. Então, a sequência $P(1), P(2), ...$ possui infinitos fatores primos.

Prova: Suponha que a sequência $P(0), P(1), P(2), ...$ possua um número finito de fatores primos $p_1, p_2, ..., p_n$. Então, para cada $i = 1, 2, ..., n$, existe a_i tal que $P(a_i) \equiv 0 \pmod{p_i}$. Portanto, pelo Teorema Chinês dos Restos, existe $M \in N$ tal que

$$M \equiv a_1 \pmod{p_1}$$

$$M \equiv a_2 \pmod{p_2}$$

$$...$$

$$M \equiv a_n \pmod{p_n}$$

Logo, aplicando P em ambos os lados, temos que

$$P(M) \equiv P(a_1) \equiv 0 \pmod{p_1}$$

$$P(M) \equiv P(a_2) \equiv 0 \pmod{p_2}$$

$$\dots$$

$$P(M) \equiv P(a_n) \equiv 0 \pmod{p_n}$$

Agora, tome o polinômio auxiliar Q tal que $Q(x) = P(x+M)$. Daí, temos que $p_i | Q(0)$ para todo $i = 1, 2, \dots, n$, portanto $p_i | Q(Q(0)) = Q(0).A$, com $mdc(Q(0), A) = 1$, já que $A \equiv 1 \pmod{A}$. Então, existe um primo q diferente de $p_1, p_2, \dots, p_n$ dividindo $Q(Q(0)) = P(Q(0)+M) = P(P(M)+M)$, que está na sequência $P(0), P(1), P(2), \dots$, um absurdo. Logo a sequência $P(0), P(1), P(2), \dots$ possui infinitos fatores primos.

2.4 Exemplo 2

(EMC 2016/1) Determine se existe uma sequência $a_1, \dots, a_{2016}$ de números inteiros positivos, de modo que cada soma

$$a_r + a_{r+1} + \dots + a_{s-1} + a_s$$

(com $1 \leq r \leq s \leq 2016$) é um número composto, mas:

a) $mdc(a_i, a_{i+1}) = 1$ para todos os $i = 1, 2, \dots, 2015$;

b) $mdc(a_i, a_{i+1}) = 1$ para todos os $i = 1, 2, \dots, 2015$ e $mdc(a_i, a_{i+2}) = 1$ para todos os $i = 1, 2, \dots, 2014$.

Solução: A resposta é sim. Veja que basta dar um exemplo que satisfaça as condições da parte (b), então vamos fazer exatamente isso.

Escolha um número primo ímpar p e outro conjunto de números primos ímpares (distintos 2 a 2 e também distintos de p), digamos, $p_1, p_2, \dots, p_{2016}, q_1, q_2, \dots, q_{2016}$. Agora, pelo Teorema Chinês dos Restos, podemos escolher a_0 de modo que:

$$a_0 \equiv 1 \pmod{2}$$

$$a_0 \equiv 1 \pmod{p}$$

$$\dots$$

$$a_0 + 2ip \equiv 0 \pmod{p_i q_i}$$

para todo $i = 1,2,3,...,2016$. Agora, defina $a_i = a_0 + 2ip$ para $i = 1,2,...,2016$. Provemos que isso funciona. De fato, como os a_is estão em uma progressão aritmética, temos

$$a_r + a_{r+1} + ... + a_{s-1} + a_s = \frac{a_r + a_s}{2}(s - r + 1)$$

Agora, observe que $\frac{a_r+a_s}{2}$ é sempre um número inteiro, porque, por construção, a_0 e, portanto, todos os a_i são ímpares. Para $r \neq s$, a soma acima é claramente composta, e para $r = s$, a soma acima reduz para a_r, que é composta porque $p_r q_r | a_r$.

Agora resta verificar a condição do mdc: $mdc(a_i, a_{i+2}) = mdc(a_i, a_i + 4p) = mdc(a_i, 4p)$, que não excede 1, pois tomamos o cuidado de definir $a_i \equiv a_0 \equiv 1 \pmod 2$ e $a_i \equiv a_0 \pmod p$. A verificação do $mdc(a_i, a_{i+1})$ é análoga.

2.5 Exemplo 3

(USAMO 2008) Para cada inteiro positivo n, prove que existem $k_0, k_1, k_2, ..., k_n \geq 1$ inteiros positivos coprimos dois a dois de modo que $k_0 k_1 k_2 ... k_n - 1$ é o produto de dois inteiros consecutivos.

Solução: Observe que $k_0 k_1 k_2 ... k_n - 1 = M(M+1) \iff k_0 k_1 k_2 ... k_n = M^2 + M + 1$, isto é, queremos provar que o polinômio $P(X) = X^2 + X + 1$ possui uma quantidade de fatores primos tão grande quanto desejarmos. Então, pelo Teorema de Schur, $P(1), P(2), ...$ possui infinitos fatores primos, logo, para todo inteiro positivo n, conseguimos selecionar primos distintos $p_0, p_1, ..., p_n$ tais que $p_i | P(a_i)$ para todo $i = 0, 1, ..., n$ e para algum $a_i \in N$. Pelo Teorema Chinês dos Restos, existe $M \in N$ tal que

$$\begin{aligned} M &\equiv a_0 \pmod{p_0} \\ M &\equiv a_1 \pmod{p_1} \\ &... \\ M &\equiv a_n \pmod{p_n} \end{aligned}$$

Logo, aplicando P em ambos os lados, temos que

$$\begin{aligned} P(M) &\equiv P(a_0) \equiv 0 \pmod{p_0} \\ P(M) &\equiv P(a_1) \equiv 0 \pmod{p_1} \\ &... \end{aligned}$$

$$P(M) \equiv P(a_n) \equiv 0 \pmod{p_n}$$

Então, como $p_0, p_1, ..., p_n$ são coprimos dois a dois, $p_0 p_1 ... p_n | P(M) = M^2 + M + 1 \iff M^2 + M + 1 = A.p_0 p_1 ... p_n = k_0 k_1 ... k_n$ para determinados $k_0, k_1, ..., k_n$ (basta ajustar os fatores primos de A com o restante dos p_i's), como desejávamos.

3 Problemas

1.(OBM N2 2017/6) Demonstre que, para todo n inteiro positivo, existem inteiros positivos a e b, sem fatores primos em comum, de modo que $a^2 + 2017b^2$ possui mais de n fatores primos distintos.

2.(IMO 1989) Prove que para cada número inteiro positivo n existem n números inteiros positivos consecutivos, nenhum dos quais é uma potência perfeita de um número primo.

3.(IMO 2009/1) Seja n um número inteiro positivo e $a_1, a_2, a_3, ..., a_k$ $(k \geq 2)$ sejam números inteiros distintos no conjunto $1, 2, ..., n$ de modo que n divide $a_i(a_{i+1} - 1)$ para $i = 1, 2, ..., k-1$. Prove que n não divide $a_k(a_1 - 1)$.

4.(APMO 2009/4) Prove que, para qualquer número inteiro positivo k, existe uma sequência aritmética $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, ..., \frac{a_k}{b_k}$ de números racionais, em que a_i, b_i são números inteiros positivos relativamente primos para cada $i = 1, 2, ..., k$, de modo que os números inteiros positivos $a_1, b_1, a_2, b_2, ..., a_k, b_k$ são todos distintos.

5.(OBM 2013/2) Arnaldo e Bernaldo jogam o seguinte jogo: dado um conjunto finito fixo de números inteiros positivos A conhecidos por ambos os jogadores, Arnaldo escolhe um número $a \in A$, mas não o diz a ninguém. Bernaldo escolhe um número inteiro positivo arbitrário b (não necessariamente em A). Então Arnaldo conta o número de divisores de ab. Mostre que Bernaldo pode escolher b de maneira a descobrir o número a escolhido por Arnaldo.

6. (IMO 2016/4) Um conjunto de números inteiros positivos é chamado fragante se contiver pelo menos dois elementos e cada um de seus elementos tiver um fator primo em comum com pelo menos um dos outros elementos. Seja $P(n) = n^2 + n + 1$. Qual é o menor valor inteiro positivo possível de b, de modo que exista um número inteiro não negativo a para o qual o conjunto

$$\{P(a+1), P(a+2), ..., P(a+b)\}$$

é fragante?

7.(IMO SL 2005/N4) Encontre todos os números inteiros positivos n, de modo que exista um número inteiro único a, de modo que $0 \leq a < n!$, Com a

seguinte propriedade:

$$n!|a^n+1$$

8.(USA TST 2015/2) Prove que para cada $n \in N$, existe um conjunto S de n números inteiros positivos, de modo que, para quaisquer dois elementos distintos $a,b \in S$, $a-b$ divide a e b, mas nenhum dos outros elementos de S.

4 Dicas

1. Use o Teorema de Schur.
2. Force $p_i q_i | x+i$ para primos p_i, q_i.
3. Assuma que o problema é falso.
4. Use o Teorema Chinês dos Restos de maneira inteligente para conseguir alguma condição boa no problema.
5. Use o Teorema Chinês dos Restos de maneira esperta para chegar em uma situação agradável no problema.
6. Faça casos pequenos e conjecture a resposta.
7. Use o Teorema Chinês dos Restos no fim do problema.
8. Faça casos pequenos.

5 Bibliografia

1. https://www.urantiagaia.org/educacional/matematica/teoria$_n umeros3/Aula08-Teorema_C hines_d os_R estos.pdf$
2. https://web.evanchen.cc/handouts/CRT/CRT.pdf