O Teorema Chinês dos Restos

1 Como conseguiram chegar nisso?

Ao fazer um problema de olímpiada de teoria dos números, podemos querer achar algum número com propriedades específicas, sendo ao mesmo tempo MUITO grande. Se essa propriedade for só com congruências, estamos com sorte!

- **Teorema (TCR):** Sejam $a_1, a_2, ..., a_n, b_1, b_2, ..b_n$ $2n$ números com os a_i's dois a dois coprimos. Então $\exists\ A \in \mathbb{Z}$ tal que

$$\begin{cases} A \equiv b_1 \pmod{a_1} \\ A \equiv b_2 \pmod{a_2} \\ \vdots \quad \vdots \qquad \vdots \\ A \equiv b_n \pmod{a_n} \end{cases}$$

Prova: Queremos achar um número que cumpra o sistema de equações, mas, primeiro, vamos tentar achar um número que seja congruente a b_i para algum a_i e seja divisível por todos os outros a_j's, Sejam:

$$P_i = \frac{a_1 a_2 \dots a_n}{a_i}$$
$$L_i \equiv (P_i)^{-1} \pmod{a_i},\ L_i \in \mathbb{Z}$$

Daí, temos:

$$b_i P_i L_i \equiv b_i \pmod{a_i}$$
$$b_i P_i L_i \equiv 0 \pmod{a_j}, \forall j \neq i$$

(Aqui, usamos $a^{-1} \pmod{b}$ sendo o inverso multiplicativo de $a \pmod{b}$.)

Assim, temos uma solução como queríamos. Veja que se somarmos todas essas soluções, temos o nosso A desejado:

$$A = \sum_{k=1}^{n} b_k P_k L_k \equiv b_m \pmod{a_m} \forall\ m \in \{1, 2, \dots, n\}$$

Pois $a_m \mid b_i P_i L_i$ se $i \neq m$ e $b_m P_m L_m \equiv b_m \pmod{a_m}$ Provando assim o teorema!

Nota: *Se somarmos $a_m a_{m-1} \dots a_2 a_1$ ao A ele ainda vai cumprir as congruências, então temos infinitos A's possíveis!*

2 Problemas Resolvidos

(Problema 1): (Schur) Seja $P \in \mathbb{Z}[x]$ um polinômio de coeficientes inteiros não-constante. Prove que existem infinitos primos que dividem $P(x)$, para algum $x \in \mathbb{Z}$.

Suponha que exista um P não constante com finitos divisores primos. Seja $P = \{p_1, p_2, \ldots, p_k\}$ o conjunto dos primos que dividem $P(x)$ para algum x seja $v_{p_i}(P(0)) = \alpha_i$. Assim, seja $Q = p_1^{\alpha_1+1} p_2^{\alpha_2+1} \ldots p_k^{\alpha_k+1}$ e $Q^* = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Veja que:

$$x \equiv 0 \pmod{Q} \implies P(x) \equiv P(0) \equiv P^* \pmod{Q}$$

Como $P(x)$ não pode ter nenhum fator primo além dos já escritos, (já temos os expoentes escritos de cada primo que divide $P(x)$ e sabemos que nenhum outro pode dividí-lo) temos que $P(x) = Q^* \forall x \equiv 0 \pmod{Q}$. Logo, $P(x) - Q^*$ é um polinômio com infinitas raízes! Assim, $P(x) - P^* \equiv 0$ (identicamente nulo) então $P \equiv Q^*$. Um polinômio constante$\rightarrow$ *Abs*!. Como queríamos demonstrar. Assim, provando o teorema
Nota: Optei por escrever essa solução sem TCR para facilitar o entendimento da solução, mas veja que essa solução nos dá uma ideia muito boa para TCR: Podemos cotar v_p's a partir de TCR! Basta usar o número que você quer pra ser congruente a uma potência de primo anterior à que você usa no módulo! Ideia legal, não?

(Problema 2): Prove que para todo polinômio P de coeficientes inteiros não-constante existe um $x \in \mathbb{Z}$ tal que $P(x)$ tem pelo menos k fatores primos.

Por Schur, existem infinitos primos que dividem $P(x)$, para algum $x \in \mathbb{Z}$. Em particular, existem k primos distintos que dividem $P(x)$ para algum $x \in \mathbb{Z}$. Sejam eles $p_1, p_2, \ldots, p_k$ e sejam $x_1, x_2, \ldots, x_k$ tais que $p_i \mid x_i, \forall\, 1 \leq i \leq k$ por TCR, existe x tal que

$$\begin{aligned} x &\equiv x_1 \pmod{p_1} \\ x &\equiv x_2 \pmod{p_2} \\ &\vdots \\ x &\equiv x_k \pmod{p_k} \end{aligned}$$

Veja que $P(x) \equiv P(x_i) \equiv 0 \pmod{p_i}, \forall\, 1 \leq i \leq k$, já que $x \equiv x_i \pmod{p_i}$.
Assim,

$$P(x) \equiv 0 \pmod{()p_1 p_2 \ldots p_k}$$

Logo, $P(x)$ tem mais de k divisores primos, como queríamos.

(Problema 3): Sejam a, b números tais que $a^n + n \mid b^n + n$ para todo n inteiro positivo. Prove que $a = b$

Solução: Por TCR, existe n tal que

$$\begin{aligned} n &\equiv 1 \pmod{p-1} \\ n &\equiv -a \pmod{p} \end{aligned}$$

Onde p é um primo grande. Vejamos agora o que acontece tomando tal n:
Primeiramente, veja que $p \mid a^n + n$, pois

$$a^n + n \equiv a^1 - a \equiv 0 \pmod{p}$$

(Lembre-se que pelo teorema de fermat $a^{p-1} \equiv 1$)
além disso, veja que

$$b^n + n \equiv b - a \pmod p$$

Como $p \mid a^n + n \mid b^n + n$, temos que $p \mid b - a$ para todo p primo grande. Logo, $b - a = 0 \implies a = b$, como queríamos.

(Problema 4):Seja P um polinômio de coeficientes inteiros e n um inteiro positivo. definimos P_n como o número de pares $(a, b), a < b \leq n$ de inteiros positivos tais que

$$n \mid |P(a)| - |P(b)|$$

Ache todos os polinômios tais que $P_n \leq 2023$ para todo $n \in \mathbb{N}$

Solução: Inicialmente, veja que se P é linear, então

$$P(x) = x + c \text{ ou } -x - c$$

Onde $c \geq -2023$. Veja que se $P(x) = mx + c$, então, para n grande múltiplo de m, além disso, $\exists\ M \mid \forall\ s \geq M, P(s)$ terá sempre o mesmo sinal. Assim, para a, b grandes,

$$|P(a)| - |P(b)| = m(a - b)$$

Que é divisível por $n \iff \dfrac{n}{m} \mid a - b$. veja que se $m \geq 2$ teremos pelo menos $\frac{n}{m}$ soluções para essa divisibilidade:

$$(a, b) = (1, \frac{n}{m} + 1), (2, \frac{n}{m} + 2) \ldots (\frac{n}{m}, \frac{n}{m} + \frac{n}{m})$$

Assim, se tomarmos n para ser um número muito grande, $dfracnm > M + 2024$ (para que existam mais que 2023 pares de caras maiores que M) teremos pelo menos 2024 soluções para a divisibilidade! Logo, $m = 1$. Deixamos a parte de $c \geq -2023$ como exercício para o leitor.
Agora, vamos supor que $degP \geq 2$.
Lema 1: Suponha que exista p tal que exista um c tal que $P(x) \not\equiv c \pmod p$ então existem pelo menos n c's tais que

$$P(x) \not\equiv c \pmod{n)p}$$

Onde n é um número tal que $p \nmid n$
Prova: Inicialmente, veja que se $a \equiv c \pmod p \implies$ não existe x tal que $P(x) \equiv a \pmod{n)p}$, (pois se $P(x) \equiv a \pmod{n)p} \implies P(x) \equiv a \equiv c \pmod p \to Abs!$).
Além disso, por TCR, existem exatamente n a's cumprindo $a \equiv c \pmod p$, $a \leq np$, Basta ver as soluções para

$$x \equiv c \pmod p$$
$$x \equiv k \pmod n$$

Onde $1 \leq k \leq n$. Assim, se existe um p com um elemento que não aparece como resíduo $\pmod p$ então existem um n com quantos números eu queira que não apareçam como resíduos de P $\pmod n$.

Lema 2: Se existem k números menores que n que não são resíduos de $P \pmod{n}$, então existem pelo menos k pares (a, b) tais que

$$P(a) \equiv P(b) \pmod{n}$$

Prova: por PCP, como temos $n - k$ possíveis resíduos e n números a se colocar neles, é fácil ver que teremos pelo menos k pares ao longo dos resíduos. Assim, como conseguimos k suficientemente grande, para algum n se existe um primo p e um inteiro c tal que

$$P(x) \not\equiv c \pmod{p}$$

Então $P(x)$ para $x = 0, 1, 2, \ldots, p-1$ é um sistema completo de resíduos para todo p primo. Porém, veja que $Q(x) = P(x+1) - P(x)$ tem infinitos divisores primos por Schur, já que $deg\ Q = deg\ P - 1$ (confira!) logo, existem infinitos q's primos tais que existe um s tal que $P(s+1) \equiv P(s) \implies P$ não forma um sistema completo de resíduos $\pmod{q}$! Absurdo, como queríamos, logo, as únicas soluções são as que demos no começo.