Primos, Divisibilidades e Fatorações

Alessandro Machado

1 Introdução

1.1 Contextualização

A ideia de fatorar em números primos é, em sua essencia, uma forma de extrair a maior quantidade de informações sobre um número inteiro, "reduzindo-o a sua forma raiz".

Pense em primos como se fossem a forma mais simples de um inteiro (por mais que sua forma seja simples, veremos que números primos escondem, em sua natureza que são os mais complexos e belos números na *Teoria dos Números*), sendo considerados sua "fundação". Podemos associar primos com inteiros como se fossem tijolos de um muro.

1.2 Esclarecimentos

Veremos que, números primos positivos se comportam exatamente como primos negativos, mas por simplicidade e convenção, na maioria dos casos olharemos apenas para os primos positivos.

2 Definições

2.1 Primos

2.1.1 Inspiração

Como citado anteriormente em "**1.1**", trabalhamos com primos para tentar extrair o máximo de informações de um inteiro, pois os primos são a "forma irredutível" deles. Assim, podemos interpretá-los como um multiconjunto (os fatores primos de um número, que podem ser contados mais de uma vez), na qual para que um divida o outro, um multiconjunto será subconjunto de outro. Por exemplo: $12 = 2 \cdot 2 \cdot 3$, então associaremos-o com o multiconjunto $C_{12} = [2,\ 2,\ 3]$ e $120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$, logo seu multiconjunto será $C_{120} = [2,\ 2,\ 2,\ 3,\ 5]$ e de fato $C_{12} \subseteq C_{120}$, então $12|120$ (definição formal posteriormente).

2.1.2 Definição

Denotamos por $\mathbb{P}$ como o conjunto dos números primos, onde $p > 1 \in \mathbb{P} \iff \forall\ d|p \implies |d| \in \{1, p\}$, ou seja, p é um número primo se, e somente se os divisores positivos de p são apenas 1 e p. Chamamos-o de composto caso contrário (1 não é composto por definição).

Perceba que, para saber se um número é primo, precisamos checar apenas a divisibilidade por outros primos, pois se $d|p$, então d é primo ou existe $q \in \mathbb{P}/\ q|d$, ou seja, um fator primo de d. Note que definimos que 1 não é primo, pois $1 \cdot n = n$ e isso removeria a unicidade de alguns teoremas.

Exemplo.

Se p e q são dois primos ímpares consecultivos, mostre que $p+q$ tem pelo menos 3 fatores primos (não nescessariamente distintos).

Solução. Suponha sem perda de generalidade que $p < q$, como p e q são ímpares, então $p+q$ é par, logo $\dfrac{p+q}{2}$ é inteiro. Basta mostrar que $\dfrac{p+q}{2}$ não é primo, pois assim terá 2 fatores primos ao mínimo (totalizando 3, contando o 2 inicial). Suponha que $\dfrac{p+q}{2}$ seja primo, note que $p < \dfrac{p+q}{2} < q$, pois $p < q$. Sendo que p e q são primos consecultivos, logo $\dfrac{p+q}{2}$ não pode ser primo!

.....

2.1.3 Teoremas

Teorema de Euclides. Existem infinitos números primos.

Prova. Seja $\mathbb{P} = \{p_1, p_2, \ldots, p_k\}$ o conjunto finito dos números primos, contendo k primos. Provaremos então, que existe um primo que não está nesse conjunto.

Considere $M = p_1 p_2 \ldots p_k$ e perceba que todo primo p_i divide M, pois M é a multiplicação de todos os primos. Agora, analisaremos $M+1$. Sabemos que $\forall\ 1 \leq i \leq k, p_i|M$, então como $M+1 > p_1, p_2, \ldots, p_k \implies M+1 \notin \mathbb{P}$, ou seja, $M+1$ não é primo. Portanto existe $1 \leq j \leq k$ tal que $p_j|M+1$, porém $p_j|M \implies p_j|1 \implies p_j = 1$, absurdo!

Então, partindo da suposição que $\mathbb{P}$ era finito, conseguimos tomar M como sendo o produto de todos os primos, logo existem infinitos primos ■

Exemplo.

Prove que existem infinitos primos da forma $4k+3$.

Solução. Suponha que exista uma quantidade finita de primos da forma $4k+3$. Denote por $M = \{p_1, p_2, \ldots, p_i\}$ com $3 = p_1 < p_2 < \cdots < p_i$ o conjunto de todos eles. Agora, considere o número $N = 4p_1p_2 \ldots p_i - 1$. Se N é primo, então $N = 4(p_1p_2 \ldots p_i - 1) + 3$, mas $N > p_i$, absurdo! Então N é composto. Tome q para ser um fator primo qualquer de N e note que N é ímpar, então $q \equiv 1 \pmod 4$ ou $q \equiv 3 \pmod 4$. Se $q \equiv 3 \pmod 4$, então $q \in M \implies q|p_1p_2 \ldots p_i$, portanto q terá que dividir -1, absurdo! Logo

todo fator primo de N é da forma $4k+1$ (pois q era um primo qualquer que dividia N). Mas se $N = q_1 q_2 \dots q_j$, então $N = (4k_1+1)(4k_2+1)\dots(4k_j+1) \equiv 1 \pmod 4$, porém $N = 4p_1p_2\dots p_i - 1 \equiv 3 \pmod 4$, absurdo! Então nossa suposição de que existiam finitos primos da forma $4k+3$ é falsa (fez com que nós pudéssemos tomar $N = 4p_1p_2\dots p_i - 1$), logo existem infinitos primos da forma $4k+3$ ■

. . . . . .

Crivo de Eratóstenes. Se $n \in \mathbb{N}$ é um número composto, então existe um primo $p \leq \sqrt{n}$ tal que $p|n$.

Prova. Como n é composto, podemos escrevê-lo como a multiplicação de dois inteiros $a \geq b > 1$. Então $n = ab$, suponha que $b > \sqrt{n} \implies a > \sqrt{n} \implies n = ab > \sqrt{n}\sqrt{n} = n$, absurdo! Logo, $b \leq \sqrt{n}$. Se b for primo, o enunciado é verdade, então suponha b composto. Logo existe um primo p que divide b, portanto $p \leq b \leq \sqrt{n}$ ■

Exemplo. *(OBM 2022)*

Inicialmente um número está escrito no quadro. Então, a cada minuto, Esmeralda escolhe um divisor $d > 1$ do número n escrito na lousa, apaga n e escreve $n+d$. Se o número inicial é 2022, qual é o maior número composto que Esmeralda nunca poderá escrever no quadro?

Solução. Note que todo número par a partir de 2022 pode ser escrito, pois 2022 é par, logo $2022+2$ pode ser escrito, então como $2022+2$ é par, $2022+2+2$ pode ser escrito... Então, se $n > 2022$ não pode ser escrito e $p|n$, portanto $p|n-p$. Porém, se $p = 2$ então n é par, absurdo! Mas como n e p são ímpares, $n-p$ é par, logo se $n-p \geq 2022$, $n-p$ pode ser escrito, sendo que $p|n-p$ então $(n-p)+p = n$ também poderá ser escrito.

Logo, se n não pode ser escrito, então para todo primo p que divide n, $n-p < 2022 \implies p > n-2022$. Mas para chegar em um absurdo, queremos tomar o menor p possível. Temos que, como n é composto, por *Crivo de Eratóstenes* existe um primo $q \leq \sqrt{n}$ que divide n. Faça $p = q \implies \sqrt{n} \geq q > n-2022 \implies n > (n-2022)^2 = n^2 - 4044n + 2022^2 \implies n^2 - 4045n + 2022^2 < 0$, mas se $r_1 > r_2$ são as raízes do polinômio $P(x) = n^2 - 4045n + 2022^2$, então como o coeficiente líder é positivo, se $x > r_1 \implies P(x) > 0$.

Agora, usando a *Fórmula de Bháskara* para achar as raízes de $P(x)$:

$$r_1 = \frac{4045 \pm \sqrt{4045^2 - 4 \cdot 2022^2}}{2} = \frac{4045 \pm \sqrt{4045^2 - 4044^2}}{2} = \frac{4045 \pm \sqrt{4045+4044}}{2},$$

sendo que r_2 é a maior raiz, logo $r_2 = \dfrac{4045+\sqrt{8089}}{2} < \dfrac{4045+\sqrt{8100}}{2} = \dfrac{4045+90}{2} = 2067,5$. Então, para $n > 2067$, $n^2 - 4045n + 2022^2 > 0$ o que é um absurdo! Logo $n \leq 2067$ e testando casos descobrimos que o maior número composto que Esmeralda nunca poderá escrever no quadro é 2033.

Teorema Fundamental da Aritmética. Se $n \in \mathbb{N}_{>1}$, então n pode ser escrito como fatoração de primos de forma única. Ou seja, $\exists!\ p_1 < p_2 < \cdots < p_k \in \mathbb{P}, \alpha_1, \alpha_2, \ldots, \alpha_k \geq 1 \mid n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ (também chamada de fatoração canônica de n).

Prova. Primeiro provaremos que existe tal fatoração, depois mostraremos que é única. Para isso usaremos indução forte!

Base: $2 = 2^1$, $3 = 3^1$, $4 = 2^2$, $5 = 5^1$ e $6 = 2^1 \cdot 3^1$.

Hipótese de indução: Para todo $m \leq n$, é possível escrevê-lo como fatoração de primos.

Passo indutivo: Se $n+1$ for primo, então essa é sua fatoração, se for composto, então escreva $n+1 = ab$ onde $1 < a, b < n+1$. Como a e b são menores que $n+1$, podemos aplicar a hipótese de indução neles. $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ e $b = q_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l}$, então $n+1 = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l}$, fatorado (basta combinar os fatores primos iguais)!

Por fim, suponha que $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l}$, então se houver algum primo em $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ que não houver em $q_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l}$, adicione-o com expoente 0. Ou seja, $r_1^{x_1} r_2^{x_2} \ldots r_k^{x_k} = r_1^{y_1} r_2^{y_2} \ldots r_k^{y_k}$ onde $r_i \in \mathbb{P}\ \forall\ 1 \leq i \leq k$ e $x_i, y_i \geq 0\ \forall\ 1 \leq i \leq k$.

Como estamos supondo que as fatorações são diferentes, então temos que existe $1 \leq i \leq k$ para o qual $x_i \neq y_i$. Mas $r_i^{x_i} | r_1^{y_1} r_2^{y_2} \ldots r_k^{y_k} \implies r_i^{x_i} | r_i^{y_i}$, logo $x_i \leq y_i$, entretanto $y_i \leq x_i$ analogamente, ou seja, $x_i = y_i$, absurdo! Portanto a *fatoração canônica* é única.

Corolário. Sejam $a, b \in \mathbb{N}$ com $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, então:

$a | b \iff b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k} p_{k+1}^{\beta_{k+1}} \ldots p_l^{\beta_l}$ onde $\beta_i \geq \alpha_i\ \forall\ 1 \leq i \leq k$.

OBS.: Perceba que, como dito em "**2.1.1**" $C_a \subseteq C_b$.

2.2 Fatores comuns

2.2.1 Inspiração

Muitas vezes queremos saber como se comportam os fatores comuns de dois inteiros, ou até mesmo simplificá-los, como por exemplo se $12 | 24 \cdot 5$, sabemos que $12 | 24$ pois 12 e 5 não possuem "fatores em comum".

Ou como interpretado em "**2.1.1**", $C_{12} = [2,\ 2,\ 3]$ e $C_{120} = [2,\ 2,\ 2,\ 3,\ 5]$ sendo que $C_{12} \subset C_{120}$ e $5 \in C_{120}$, mas $5 \notin C_{12}$, então $C_{12} \subseteq (C_{120} - [5])$.

Em geral, denotamos por fatores comuns de a e b como $C_a \cap C_b$. Então $C_a \subseteq (C_b \cup C_c) \implies (C_a - C_a \cap C_b) \subseteq ((C_b - C_a \cap C_b) \cup C_c)$, sendo que $(C_a - C_a \cap C_b) \cap (C_b - C_a \cap C_b) = \emptyset$, logo $(C_a - C_a \cap C_b) \subseteq C_c$ (técnica explicada posteriormente).

2.2.2 Definição

Definimos por $mdc(a,b)$ como o maior d tal que $d|a$ e $d|b$. Também interpretado como $C_a \cap C_b$ onde $\prod_{k \in C_n} k = n$ e $\forall\ k \in C_n \implies k \in \mathbb{P}$.

Ou seja, se $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, representamos-o como:

$$C_n = [\underbrace{p_1, \dots, p_1}_{\alpha_1 \text{vezes}}, \underbrace{p_2, \dots, p_2}_{\alpha_2 \text{vezes}}, \dots, \underbrace{p_k, \dots, p_k}_{\alpha_k \text{vezes}}]$$

E $mmc(a,b)$ como o menor m tal que $a|m$ e $b|m$, ou $C_a \cup C_b$.

Note que $mdc(a,b) = mdc(a,-b)$, logo apenas analisamos $a, b \in \mathbb{N}$ por simplicidade.

2.2.3 Propriedades

1. $mdc(a,a) = mdc(a,0) = a, mdc(a,b) = mdc(a,-b) = mdc(b,a), mdc(a,1) = 1$;
2. $a|b \implies mdc(a,b) = a$ e $mmc(a,b) = b$;
3. $a, b \in \mathbb{N}$ com $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ e $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$
   $\implies mdc(a,b) = p_1^{min(\alpha_1,\beta_1)} p_2^{min(\alpha_2,\beta_2)} \dots p_k^{min(\alpha_k,\beta_k)}$;
4. $a, b \in \mathbb{N}$ com $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ e $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$
   $\implies mdc(a,b) = p_1^{max(\alpha_1,\beta_1)} p_2^{max(\alpha_2,\beta_2)} \dots p_k^{max(\alpha_k,\beta_k)}$;
5. $mdc(a,b) \cdot mmc(a,b) = ab$;
6. $a|b$ e $a|c \implies a|mdc(b,c)$ e, $x|z$ e $y|z \implies mmc(x,y)|z$;
7. $mdc(a,b,c) = mdc(mdc(a,b),c)$;
8. $c \neq 0 \implies mdc(ca,cb) = c \cdot mdc(a,b)$;
9. $mdc(a,b) = mdc(a, b \pm ax)$;
10. $a|bc \implies \frac{a}{mdc(a,b)}|c$;

2.2.4 Demonstrações

1. Note que $d|a \implies d \leq |a|$ e $a|a$, então $mdc(a,a) = a$, analogamente para $mdc(a,0)$. E perceba que podemos supor que são positivos, pois $mdc(a,-b) = mdc(a,b) = d$ já que $d|b \iff d|-b$;
2. Note que $mdc(a,b)|a \implies mdc(a,b) \leq a$, mas $a|a$ e $a|b$, logo $mdc(a,b) = a$. E, $b|mmc(a,b) \implies mmc(a,b) \geq b$, mas $a|b$ e $b|b$, então $mmc(a,b) = b$;

3. Seja $mdc(a,b) = p_1^{\gamma_1}p_2^{\gamma_2}\dots p_k^{\gamma_k}$ (note que se $q|mdc(a,b) \implies q|a$ e $q|b$, então não há primo que esteja na fatoração do $mdc(a,b)$, mas não em a ou b). Perceba que $mdc(a,b)|a \implies p_i^{\gamma_i}|p_i^{\alpha_i} \implies \gamma_i \leq \alpha_i$, analogamente $\gamma_i \leq \beta_i$, então $\gamma_i \leq min(\alpha_i, \beta_i)\ \forall\ 1 \leq i \leq k$. Sendo que de fato $p_1^{min(\alpha_1,\beta_1)}p_2^{min(\alpha_2,\beta_2)}\dots p_k^{min(\alpha_k,\beta_k)}$ divide a e b (pois $min(x,y) \leq x, y$);

4. Análogo ao item anterior;

5. Isso vem do fato de que $p^x p^y = p^{x+y}$ e $min(x,y) + max(x,y) = x + y$, pois supondo (sem perda de generalidade) que $x \geq y \implies min(x,y) = y$ e $max(x,y) = x \implies min(x,y) + max(x,y) = x + y$;

6. Seja $a = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$, $b = p_1^{\beta_1}p_2^{\beta_2}\dots p_k^{\beta_k}$ e $c = p_1^{\gamma_1}p_2^{\gamma_2}\dots p_k^{\gamma_k}$ onde cada primo de $p_1, p_2, \dots p_k$ é fator de a, b ou c. E $a|b \implies \alpha_i \leq \beta_i$, também $a|c \implies \alpha_i \leq \gamma_i \implies \alpha_i \leq min(\beta_i, \gamma_i)\ \forall\ 1 \leq i \leq k$, como $\alpha_i \leq min(\beta_i, \gamma_i) \implies p_i^{\alpha_i}|p_i^{min(\beta_i,\gamma_i)} \implies a|mdc(b,c)$. A segunda parte é análoga;

7. Se $d|a$ e $d|b \implies d|mdc(a,b)$ e $d|c \implies d|mdc(mdc(a,b),c)$ (em geral, mdc é comutativo, pois dizer que "$d|a$ e $d|b$" ou que "$d|b$ e $d|a$" é análogo);

8. Temos que $mdc(a,b)|a \implies c \cdot mdc(a,b)|ca$ e $mdc(a,b)|b \implies c \cdot mdc(a,b)|cb \implies c \cdot mdc(a,b)|mdc(ca,cb)$, mas $mdc(ca,cb)|ca \implies \frac{mdc(ca,cb)}{c}|a$ e $\frac{mdc(ca,cb)}{c}|b$ (pois $\frac{mdc(ca,cb)}{c}$ é inteiro, já que $c|ca$ e $c|cb \implies c|mdc(ca,cb)$), então $\frac{mdc(ca,cb)}{c}|mdc(a,b) \implies mdc(ca,cb)|c \cdot mdc(a,b)$, e mostramos que $c \cdot mdc(a,b)|mdc(ca,cb)$, logo obtemos que $c \cdot mdc(a,b) = mdc(ca,cb)$ (análogo para $mdc(\frac{a}{c}, \frac{b}{c})$, onde $c|a$ e $c|b$);

9. Note que $mdc(a,b)|a \implies mdc(a,b)|ax$ e $mdc(a,b)|b \implies mdc(a,b)|mdc(a, b \pm ax)$, sendo que $mdc(a, b \pm ax)|a \implies mdc(a, b \pm ax)|ax$ e $mdc(a, b \pm ax)|b \pm ax \implies mdc(a, b \pm ax)|b \implies mdc(a, b \pm ax)|mdc(a,b) \implies mdc(a,b) = mdc(a, b \pm ax)$;

10. Seja $a = da_0$ e $b = db_0$, onde $d = mdc(a,b) \implies mdc(a_0, b_0) = mdc(\frac{a}{d}, \frac{b}{d}) = \frac{mdc(a,b)}{d} = 1$, então temos que $a_0|b_0c$, e queremos provar que $a_0|c$. Sejam $a_0 = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$, $b_0 = p_1^{\beta_1}p_2^{\beta_2}\dots p_k^{\beta_k}$ e $c = p_1^{\gamma_1}p_2^{\gamma_2}\dots p_k^{\gamma_k}$, então $\forall\ 1 \leq i \leq k$, α_i ou β_i é zero, pois caso contrário, então $p_i|a_0$ e $p_i|b_0 \implies p_i|mdc(a_0,b_0) = 1 \implies p_i = 1$, absurdo! Logo, $p_i^{\alpha_i}|p_i^{\beta_i}p_i^{\gamma_i} \implies \alpha_i \leq \beta_i + \gamma_i$, sendo que se $\alpha_i = 0$, como $\gamma_i \geq 0 \implies \alpha_i \leq \gamma_i$, caso contrário, $\beta_i = 0 \implies \alpha_i \leq \gamma_i\ \forall\ 1 \leq i \leq k$, então sempre temos que $\alpha_i \leq \gamma_i$, portanto $a_0|c \implies \frac{a}{mdc(a,b)}|c$. Note que a mesma prova foi feita em "**2.2.1**", pois $d = C_a \cap C_b$, então $a_0 = C_a - d = C_a - C_a \cap C_b$ e $b_0 = C_b - d = C_b - C_a \cap C_b$, na qual $(C_a - C_a \cap C_b) \cap (C_b - C_a \cap C_b) = \emptyset$ representa $mdc(a_0,b_0) = 1$, então por propriedades de conjuntos disjuntos, obtemos que $(C_a - C_a \cap C_b) \subseteq C_c$, ou seja, que $a_0|c$;

2.3 Exemplos

Exemplo 1.

Sejam $m, n \in \mathbb{N}$, prove que $\sqrt[n]{m}$ é irracional se não for inteiro.

Solução. Suponha que $\sqrt[n]{m}$ seja racional, ou seja, existem $a, b \in \mathbb{N}$ tais que $\sqrt[n]{m} = \dfrac{a}{b}$ onde $\dfrac{a}{b} \notin \mathbb{Z}$, $a \nmid b$ no caso. Seja $mdc(a, b) = d$ e escreva $a = da_0$ e $b = db_0$, logo $mdc(a_0, b_0) = 1$ e $\sqrt[n]{m} = \dfrac{da_0}{db_0} = \dfrac{a_0}{b_0} \implies b_0^n m = a_0^n \implies b_0 | a_0^n$, mas $mdc(a_0, b_0) = 1 \implies b_0 = 1 \implies \sqrt[n]{m} = a_0 \in \mathbb{Z}$, absurdo! Então, se $\sqrt[n]{m} \notin \mathbb{Z} \implies \sqrt[n]{m} \notin \mathbb{Q}$.

Exemplo 2.

Sejam a, b, c e d inteiros positivos tais que $ab = cd$. Prove que $a + b + c + d$ não é um número primo.

Solução. Seja $d_1 = mdc(a, c)$ e $d_2 = mdc(b, d)$, então $a = d_1 a_0$, $c = d_1 c_0$, $b = d_2 b_0$ e $d = d_2 d_0$, note que $mdc(a_0, c_0) = mdc(b_0, d_0) = 1 \implies d_1 a_0 d_2 b_0 = d_1 c_0 d_2 d_0 \implies a_0 b_0 = c_0 d_0 \implies a_0 | c_0 d_0$, mas $mdc(a_0, c_0) = 1 \implies a_0 | d_0$, porém $d_0 | a_0$ analogamente, logo $a_0 = d_0 = x$ e também $b_0 = c_0 = y$, portanto $a + b + c + d = d_1 x + d_1 y + d_2 x + d_2 y = d_1(x + y) + d_2(x + y) = (d_1 + d_2)(x + y)$ e $d_1 + d_2, x + y \geq 2$, logo é o produto de dois números maiores que 1, então $a + b + c + d$ não é primo ■

Exemplo 3. *(St. Petersburg 1996)*

Ache todos os inteiros positivos n tais que

$$3^{n-1} + 5^{n-1} | 3^n + 5^n$$

Solução. Como $3^{n-1} + 5^{n-1} | 3^{n-1} + 5^{n-1}$ e $3^{n-1} + 5^{n-1} | 3^n + 5^n \implies 3^{n-1} + 5^{n-1} | 3^n + 5^n - 3(3^{n-1} + 5^{n-1}) = 5 \cdot 5^{n-1} - 3 \cdot 5^{n-1} = 2 \cdot 5^{n-1}$, fizemos isso para ficar uma potêcia única de primo (cancelar o 3^n). Ou seja, $3^{n-1} + 5^{n-1} | 2 \cdot 5^n$, portando $3^{n-1} + 5^{n-1}$ é 5^k ou $2 \cdot 5^k$. Entretanto, note que o mesmo é par, então $3^{n-1} + 5^{n-1} = 2 \cdot 5^k$. Sendo que se $n = 1 \implies 2 | 8$, verdade! Logo, suponha $n > 1 \implies k > 1 \implies 5 | 3^{n-1}$ (pois $5 | 5^k$ e $5 | 5^{n-1}$), absurdo! Portanto a única solução é $n = 1$.

Exemplo 4. *(Iran 2005)*

Sejam $n, p > 1$ inteiros positivos e p um primo. Dado que $n|p-1$ e $p|n^3-1$, prove que $4p-3$ é um quadrado perfeito.

Solução. Note que como $n|p-1 \implies p \geq n+1$ e que $p = nk+1$. Como $p|n^3-1 = (n-1)(n^2+n+1) \implies p|n^2+n+1 \implies p \leq n^2+n+1$, pois $p \nmid n-1$ (porque $p \geq n+1$) então $mdc(p, n-1) = 1$ (por p ser primo). Logo $nk+1|n^2+n+1|kn^2+kn+k$, então $nk+1|kn^2+kn+k-n(nk+1) = nk+k-n \implies nk+1 \leq nk+k-n \implies n+1 \leq k$, sendo que $n^2+n+1 = n(n+1)+1 \leq nk+1 = p \leq n^2+n+1 \implies p = n^2+n+1$, logo $4p-3 = 4n^2+4n+4-3 = 4n^2+4n+1 = (2n+1)^2$ ■

. . . . . .

Exemplo 5. *(IMO 1959)*

Prove que para todo natural n, a fração

$$\frac{21n+4}{14n+3}$$

é irredutível.

Solução. Para isso, temos que provar que $mdc(21n+4, 14n+3) = 1$ para todo n natural. Note que $mdc(21n+4, 14n+3) = mdc(21n+4-(14n+3), 14n+3) = mdc(7n+1, 14n+3) = mdc(7n+1, 14n+3-2(7n+1)) = mdc(7n+1, 1) = 1$ ■

. . . . . .

Exemplo 6. *(All Russia Mathematics Olympiad 1995)*

Sejam m e n inteiros positivos tais que

$$mdc(m,n) + mmc(m,n) = m+n$$

Mostre que um deles é divisível pelo outro.

Solução. Seja $d = mdc(m,n)$, note que $mdc(m,n) \cdot mmc(m,n) = mn$, então escreva $m = dx$ e $n = dy$, logo $d \cdot mmc(m,n) = d^2x, y \implies mmc(m,n) = dxy$. Substituindo temos que $d + dxy = dx + dy \implies xy + 1 = x + y \implies xy - x - y + 1 = 0$, sendo que $xy - x - y + 1 = x(y-1) - (y-1) = (x-1)(y-1) = 0$, logo $x - 1 = 0$ ou $y - 1 = 0$, então x ou y é 1, suponha que seja x sem perda de generalidade. Então $m = d$ e $n = dy$ $\implies m|n$ ■

. . . . . .

Exemplo 7. *(Romania Mathematical Olympiad)*

Sejam a e b inteiros positivos tais que existe um primo p com a propriedade que $mmc(a, a+p) = mmc(b, b+p)$, prove que $a = b$.

Solução. Lembre-se que $mdc(x, y) \cdot mmc(x, y) = xy$, então multiplique por $mdc(a, a+p)$ e $mdc(b, b+p)$ em ambos os lados da equação. $mmc(a, a+p) \cdot mdc(a, a+p) \cdot mdc(b, b+p) = mmc(b, b+p) \cdot mdc(a, a+p) \cdot mdc(b, b+p) \implies a(a+p)mdc(b, b+p) = b(b+p)mdc(a, a+p) \implies a(a+p)mdc(b, p) = b(b+p)mdc(a, p)$.

Mas, como p é primo, $mdc(a, p)$ pode ser 1 ou p, 1 se $p \nmid a$ e p se $p|a$.

Caso 1. Suponha que p divida ambos. Logo $a = px$ e $b = py \implies px(px+p)p = py(py+p)p \implies x(x+1) = y(y+1) \implies x^2 + x = y^2 + y \implies x^2 - y^2 = -(x-y) \implies (x-y)(x+y) = -(x-y) \implies x + y = -1$ se $x \neq y$, absurdo!

Caso 2. Suponha que p não divida nenhum. Logo, $mdc(a, p) = mdc(b, p) = 1 \implies a(a+p) = b(b+p) \implies a^2 + ap = b^2 + bp \implies a^2 - b^2 = -(ap - bp) \implies (a-b)(a+b) = -p(a-b) \implies a + b = -p$ se $a \neq b$, absurdo!

Caso 3. Suponha que p divida a, mas não b (o oposto é análogo). Então $a(a+p)p = b(b+p) \implies p|b(b+p)$, mas como p é primo, $p|b$ ou $p|b+p \implies p|b$, absurdo (pois supomos que $p \nmid b$)!

. . . . . .

Exemplo 8. *(Russia 2001)*

Ache todos os primos p e q tais que $p + q = (p-q)^3$.

Solução. Temos que $p + q|(p-q)^3$, sendo que $(p-q)^3 \equiv (2q)^3 \pmod{p+q}$, então $p+q|8q^3$, portanto $p+q = 2^a q^b$ com $0 \leq a, b \leq 3$, mas se $b > 0 \implies q|p+q \implies q|p \implies p = q$, substituindo temos que $p + q = 0$, absurdo! Logo $p + q$ é 2, 4 ou 8. $p + q = 2 \implies p = q = 1$, o que é impossível. $p + q = 4 \implies p = q = 2 \implies 2 + 2 = (2-2)^3 = 0$, também impossível. Por fim, $p + q = 8 \implies p = 5$ e $q = 3$ ($p > q$, pois $(p-q)^3 > 0$). E de fato, $5 + 3 = (5-3)^3 = 8$. Logo, a única solução é $(p, q) = (5, 3)$.

. . . . . .

Exemplo 9. *(Madhava 2020)*

Sejam $a_1, a_2, \ldots$ inteiros positivos tais que $mdc(a_i, a_j) = mdc(i, j)\ \forall\ i \neq j$. Mostre que $a_i = i\ \forall\ i$.

Solução. Faça $j = 2i$, então $mdc(a_i, a_{2i}) = mdc(i, 2i) = i$, mais especificamente, $i|a_i$. Agora faça $j = a_i$, logo $mdc(a_i, a_{a_i}) = mdc(i, a_i) = i$, pois $i|a_i$. Mas $a_i|a_i$ e $a_i|a_{a_i}$ (pois $k|a_k$, então basta tomar $k = a_i$) $\implies a_i|mdc(a_i, a_{a_i}) = i$ e, como $i|a_i \implies a_i = i\ \forall\ i$ ■

Exemplo 10. *(OBM 2019)*

Sejam a, b e k inteiros positivos com $k > 1$ tais que $mdc(a,b)+mmc(a,b) = k(a+b)$. Prove que $a + b \geq 4k$.

Solução. Tome $d = mdc(a,b)$ e escreva $a = dx$ e $b = dy$, então $mdc(a,b) \cdot mmc(a,b) = ab \implies d \cdot mmc(a,b) = d^2xy \implies mmc(a,b) = dxy$. Substituindo, temos que $d + dxy = k(dx + dy) \implies xy + 1 = k(x + y)$.

Queremos provar que $a + b \geq 4k$, sendo que $k = \dfrac{xy+1}{x+y} \iff a + b \geq 4\dfrac{xy+1}{x+y} \iff d(x+y)^2 \geq 4xy + 4$, mas se tivermos que $(x+y)^2 \geq 4xy + 4$, então é verdade (e perceba que temos que ter isso, pois nos "livramos" de d, então d está livre na desigualdade). Queremos que $(x+y)^2 \geq 4xy + 4 \iff (x-y)^2 \geq 4 \iff |x-y| \geq 2$.

Agora suponha que $x \geq y$ (sem perda de generalidade), basta eliminar os casos que $x = y$ e $x = y + 1$, pois daí $x \geq y + 2 \implies x - y \geq 2$.

Caso 1. Se $x = y$, temos que $mdc(x,y) = mdc(\frac{a}{d}, \frac{b}{d}) = \frac{mdc(a,b)}{d} = 1$, mas $mdc(x,y) = mdc(x,x) = x \implies x = y = 1$, logo $k = \dfrac{xy+1}{x+y} = \dfrac{1 \cdot 1 + 1}{1+1} = 1$, absurdo! (pois $k > 1$)

Caso 2. Se $x = y + 1$, temos que a única equação que pode nos gerar absurdo é $k = \dfrac{xy+1}{x+y}$ pois, como $k \in \mathbb{Z}$, queremos que $x+y|xy+1$. Logo, $(y+1)+y|(y+1)y+1 \implies 2y+1|y^2+y+1 \implies 2y+1|2(y^2+y+1)-y(2y+1) = y+2 \implies 2y+1|2(y+2)-(2y+1) = 3 \implies y = 1 \implies x = 2$. Então $k = \dfrac{xy+1}{x+y} = \dfrac{2 \cdot 1 + 1}{2+1} = 1$, absurdo (pois $k > 1$)!

Portanto, se $x \geq y$, temos que $x \neq y$ e $x \neq y + 1 \implies x \geq y + 2 \implies |x - y| \geq 2 \implies a + b \geq 4k$ ■

---

3 Problemas

Problema 1.

Mostre que se $n \geq 6$ é composto, então n divide $(n-1)!$.

Problema 2.

Seja $n \geq 6$ um inteiro positivo. Demonstre que $(n-1)! + 1$ não pode ser uma potência de n.

Problema 3.

Sejam a, b, c e d inteiros positivos tais que $ab = cd$. Prove que

$$mdc(a, c) \cdot mdc(a, d) = a \cdot mdc(a, b, c, d).$$

Problema 4.

Sejam a e b inteiros positivos tais que

$$\frac{a+1}{b} + \frac{b+1}{a}$$

é inteiro. Prove que $mdc(a, b) \leq \sqrt{a+b}$.

Problema 5. *(Triplas Pitagóricas)*

Encontre todas as soluções $x, y, z \in \mathbb{N}$ para $x^2 + y^2 = z^2$.

Problema 6. *(Japan Mathematics Olympiad Finals 2017)*

Prove que não existem inteiros positivos a, b e c tais que

$$mmc(a, b) = mmc(a + c, b + c).$$

Problema 7. *(Austria National Competition Final Round)*

Sejam a, b e c inteiros positivos tais que

$$\frac{ab}{c} + \frac{bc}{a} + \frac{ca}{b}$$

é um inteiro. Prove que cada um dos números

$$\frac{ab}{c}, \frac{bc}{a} \text{ e } \frac{ca}{b}$$

é um inteiro.

. . . . . .

Problema 8. *(BMO 1991)*

Sejam x e y inteiros positivos tais que $2xy|x^2+y^2-x$. Prove que x é um quadrado perfeito.

. . . . . .

Problema 9. *(ELMO 2017)*

Sejam $a_1, a_2, \ldots, a_n$ inteiros positivos com produto P, na qual n é um inteiro positivo ímpar. Prove que

$$mdc(a_1^n + P, a_2^n + P, \ldots, a_n^n + P) \leq 2 \cdot mdc(a_1, a_2, \ldots, a_n)^n.$$

. . . . . .

Problema 10. *(IMO Shortlist 2015)*

Sejam $m > n$ inteiros positivos. Defina $x_k = \dfrac{m+k}{n+k}$ para $k = 1, 2, \ldots, n+1$. Prove que se todos os números $x_1, x_2, \ldots, x_{n+1}$ são inteiros, então $x_1 x_2 \ldots x_{n+1} - 1$ é divisível por um primo ímpar.

. . . . . .

3.1 Conclusão

Na maioria dos problemas de *Teoria dos Números*, as ideias aplicadas nesse material são frequentes. Tais como: diferença de quadrados (além de outras fatorações algébricas), fatorar o *mdc*, analisar fatores primos, desigualdades (principalmente com divisibilidade)...

Também vimos que podemos interpretar a fatoração em primos de um número como um multiconjunto para melhor visualização, entre outras técnicas (além do conteúdo visto). Esse tipo de ideia é desenvolvida principalmente com a prática repetitiva, pensando em (e até resolvendo) muitos problemas variados. Lembrando que, procurar entender o porquê e se questionar se tal propriedade faz sentido é essencial para absorver conhecimento, pois apenas depois de nos questionarmos que saberemos se realmente entendemos.

4 Bibliografia

- **Modern Olympiad Number Theory, Aditya Khurmi**

"A matemática, vista corretamente, possui não apenas verdade, mas também suprema beleza - uma beleza fria e austera, como a da escultura."
–Bertrand Russell