MDC, MMC e Números Primos

Caique Paiva

Março 2023

Quase todo já estudou sobre um número primo, mas o que pouca gente sabe é a quantidade de propiedades úteis que ele tem. Esse é um dos conteúdos mais importantes de toda a teoria dos números, pois até nos problemas mais díficeis, os números primos tem papeis importantes neles. Além disso, muita coisa dos números primos são um mistério ainda. Por exemplo, não se sabe se tem infinitos números primos p tal que $p+2$ também é primo. Incrivel não? Vamos conhecer eles melhores

§1 Números Primos

Definição 1.1. Dizemos que um número é **primo** se, e somente se, os únicos divisores deles são 1 e ele mesmo.

Exemplos de primos são: $2, 3, 5, 7, 11, \cdots$.

É uma definição bem simples, mas eles escondem propiedades incriveis. Vamos provar algumas delas.

Lema 1.2

Todo número inteiro positivo, maior do que 1, pode ser escrito como um produto de vários números primos.

Prova. Vamos fazer uma indução para provar isso!

Caso Base: $(n = 2)$ Trivial.

Hipótese: Suponha que existe um $n > 2$ tal que $\forall k < n, k \in \mathbb{N}, k > 1$, k pode ser fatorado em números primos.

Passo Indutivo: Se n for primo, acabou, pois n vai ser um produto de vários (1) números primos.

Senão, como ele é composto, existe um inteiro $a \neq n, 1$ que $a \mid n$, logo $n = ab$, com $a, b \in \mathbb{N}, 1 < a, b < n$, portanto, pela hipótese, tanto a quanto b são produto de números primos, portanto, ab também é, então n também é, como queriamos provar.

□

Legal! Com isso, vamos chamar de **fatoração** de n a maneira de escrever n como números primos, e normalmente nós escrevemos assim:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$$

Com p_i primo e α_i inteiro maior ou igual a 1.

Além disso, só o fato dessa fatoração existir já nos ajuda em vários problemas. Vamos ver um exemplo.

Lema 1.3 (Euclides)
Existem infinitos números primos.

Prova. Suponha por absurdo que existem finitos números primos, e chame eles de $p_1 < p_2 < \cdots < p_n$. Então, pegue o número $n = p_1 p_2 \cdots p_n + 1$, então, nem $p_1, p_2, \cdots p_n$ dividem n, então n é primo, pois todo número tem uma fatoração em primos, mas isso é absurdo, pois $n > p_n > p_{n-1} > \cdots p_1$. Logo, temos infinitos primos. □

Além disso, nós conseguimos provar que essa fatoração é única!! Porém, para provar isso, vamos precisar de uma nova função que você provavelmente já conhece, porém nós vamos nos afundar mais nas suas propiedades.

§2 MDC, Euclides e Bezout

Definição 2.1. O Máximo Divisor Comum de dois números a, b, denotado de $\text{mdc}(a, b)$ como o maior inteiro d tal que $d \mid a$ e $d \mid b$.

O mdc também tem várias propiedades interessantes, vamos ver alguma delas!

Lema 2.2 (Algoritmo de Euclides)
Sejam a, b dois inteiros, logo, $\text{mdc}(a, b) = \text{mdc}(a - b, b)$.

Prova. Seja $d = \text{mdc}(a, b)$ e $d' = mdc(a - b, b)$. Vamos provar que eles são os mesmos. Primeiro veja que

$$\begin{cases} d \mid a \\ d \mid b \end{cases} \implies \begin{cases} d \mid a - b \\ d \mid b \end{cases}$$

Portanto, d é um divisor comum de $a - b$ e b, e como d' é o maior, $d' \geq d$
Além disso, temos que

$$\begin{cases} d' \mid a - b \\ d' \mid b \end{cases} \implies \begin{cases} d' \mid a \\ d' \mid b \end{cases}$$

Portanto, d' é um divisor comum de a e b, e como d é o maior, $d \geq d'$
Então, $d \geq d' \geq d \implies d' = d$. □

O mais legal disso é que, se fizermos $a = bq + r$, então $\text{mdc}(a, b) = \text{mdc}(b, r)$, pois nós aplicamos essa operação de diferença q vezes. Então, temos um algoritmo extremamente rápido para calcular o mdc de dois números grandes. Além disso, isso nos da que o mdc é invariante quando pegamos a diferença de dois números. Agora, vamos para o teorema de Bezout, que é tão poderoso quanto.

Teorema 2.3 (Teorema de Bezout)
Sejam a, b, c inteiros positivos, então, a equação

$$ax + by = c$$

Tem solução se, e somente se, $\text{mdc}(a, b) \mid c$.

Prova. Vamos primeiro fazer a ida que é o mais fácil. Se existe uma solução, então, faça $\text{mdc}(a, b) = d$. Portanto, $a = dk, b = dl$ com $k, l \in \mathbb{Z}$, portanto

$$ax + by = dkx + dly = d(kx + ly) = c \Longrightarrow d \mid c$$

Então, agora se $d = \text{mdc}(a, b) \mid c$, vamos provar que a equação

$$ax + by = d$$

Tem solução, pois dai basta multiplicar ela toda pro $\frac{c}{\text{mdc}(a,b)}$ que vai continuar sendo verdadeira.

Vamos aplicar o lema de euclides várias vezes, ou seja, faça $a = bq_1 + r_1$, $b = q_2r_1 + r_2$, $r_1 = q_3r_2 + r_3 \cdots$, $r_n = q_{n+2}r_{n+1} + 0$, pois eventualmente o algoritmo acaba, que é quando cheagamos em $\text{mdc}(x, 0) = x$. Então, temos que $\text{mdc}(a, b) = \text{mdc}(b, r_1) = \cdots = \text{mdc}(r_{n+1}, 0) = r_{n+1}$, logo, queremos escrever r_{n+1} como $ax + by$. Com isso, vamos fazer uma indução nos r_i para provar isso!

Caso base: Veja que $r_1 = a - bq_1$ e $r_2 = b - q_2(a - bq_1) = -aq_2 + b(q_1 + 1)$, logo, r_1 e r_2 são os nossos casos bases.

Hipótese: Suponha que $\exists m$ tal que $\forall k < m, r_k$ pode ser escrito da forma $ax + by$.

Passo indutivo: Veja que

$$r_{m-2} = q_{m+1}r_{m-1} + r_m \Longrightarrow r_m = r_{m-2} - q_{m+1}r_{m-1}$$

Então, faça $r_{m-2} = ax_1 + by_1$ e $r_{m-1} = ax_2 + by_2$, logo

$$r_m = q_{m+1}(ax_2 + by_2) + ax_1 + by_1 = a(x_1 + q_{m+1}x_2) + b(y_1 + q_{m+1}y_2)$$

Logo r_m pode ser escrito da forma $ax + by$ para todo m. Em específico, r_{n+1} □

Perfeito, vamos provar agora que toda fatoração em primos é única! Mas para isso, vamos precisar de um lema bem importante. ´

Lema 2.4

Seja p um primo, logo, $p \mid ab \Longrightarrow p \mid a$ ou $p \mid b$.

Prova. Suponha que $p \nmid a$, então $\text{mdc}(a, p) = 1$, logo, por bezout, temos que existem x, y inteiros tal que

$$ax + py = 1 \Longrightarrow abx + bpy = b$$

Mas $p \mid p$ e $p \mid ab$, logo $p \mid abc + bpy \Longrightarrow p \mid b$. □

Lema 2.5

Toda fatoração em primos é única

Veja que nós provamos que todo número tem uma fatoração, mas não provamos que ela é única.

Prova. Suponha que existe um n com duas fatorações em primos diferentes. Ou seja

$$n = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_m^{\alpha_m} = q_1^{\beta_1}q_2^{\beta_2} \cdots q_k^{\beta_k}$$

Então, suponha sem perda de generalidade que nenhuma fatoração em primos tem um primo em comum (Se tiver, basta dividir tudo por esse primo). Então, temos que

$$p_i \mid q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k} \implies p_i \mid q_1^{\beta_1} \text{ ou } p_i \mid q_2^{\beta_2} \text{ ou } \cdots p_i \mid q_k^{\beta_k}$$

Porém, se $p \mid a^t \implies p \mid a$ ou $p \mid a$ ou $\cdots p \mid a \implies p \mid a$, então

$$p_i \mid q_1 \text{ ou } p_i \mid q_2 \text{ ou } \cdots p_i \mid q_k$$

Mas o único número que divide q_j é um ou ele mesmo, pois ele é primo, portanto, ou $p_i = 1$ o que é absurdo, ou ele é igual a algum dos q_j, o que é absurdo, pois supomos que eles são diferentes. □

Lema 2.6

Se $a \mid c$, $b \mid c$ e $\text{mdc}(a, b) = 1$, então $ab \mid c$

Prova. Seja p^α um primo que divide a. Ele não divide b pois $\text{mdc}(a, b) = 1$, e como $a \mid c$ então $p^\alpha \mid c$, logo p^α está na fatoração de c, e como a fatoração de a, b são disjuntas, então $ab \mid c$. □

Nós vamos ver que ela flui muito bem com números primos, principalmente por conta desse lema:

Lema 2.7

Dados dois números a, b com sua fatoração em primos sendo $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}, b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$ (Vamos fazer com que α_i possa ser igual a 0, o que significa que p_i não divide a). Portanto

$$\text{mdc}(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_n^{\min(\alpha_n,\beta_n)}$$

Prova. Veja que $p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_n^{\min(\alpha_n,\beta_n)} \mid a$ e $p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_n^{\min(\alpha_n,\beta_n)} \mid b$ pois $p_i^k \mid p_i^l$ se $k \leq l$, pois $p_i^l = p_i^k \cdot p_i^{l-k}$ e $l-k \geq 0$, Portanto, $p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_n^{\min(\alpha_n,\beta_n)} \mid \text{mdc}(a, b) \implies \text{mdc}(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_n^{\min(\alpha_n,\beta_n)} \cdot k$ com $k \geq 1$.

Agora, se k for maior que 1, então existe um primo p que divide k. Sem perda de generalidade, seja ele p_1. Além disso, suponha sem perda de generalidade que $\alpha_1 \geq \beta_1$, logo, temos que $p_1^{\alpha_1+1} \mid a$, absurdo, pois $\alpha_1 + 1 > \alpha_1$. Portanto, $k = 1$

□

Certo, perceba que em várias provas desses lemas estamos pegando o expoente da fatoração em primos de um número. Isso é útil para resolver vários problemas inclusive, então, vale a pena nós definimos uma função para trabalharmos mais facilmente com isso!

Definição 2.8. Dado um inteiro a e um primo p, chamamos de $\nu_p(a)$ como o expoente de p na fatoração em primos de a

Vamos ter um material focado só nas propiedades dessa função, mas já deixe ela guardada para formalizar os problemas que você fizer mais facilmente.

Lema 2.9

Sejam a, b, c inteiros, então, se $c \mid a$ e $c \mid b$ então $c \mid \text{mdc}(a, b)$

Prova. Suponha que $c \nmid d$ então, isso implica que existe um primo p tal que $\nu_p(c) > \nu_p(d)$ (Isso é lógico, pois se todos os expoentes na fatoração em primos de c forem menores ou iguais a d, então $c \mid d$), mas $c \mid a$ e $c \mid b$, logo $\nu_p(c) \leq \nu_p(a)$ e $\nu_p(c) \leq \nu_p(b) \implies \nu_p(c) \leq \min(\nu_p(a), \nu_p(b)) = \nu_p(d)$, absurdo. □

Lema 2.10

Sejam a, b inteiros, e $d = \text{mdc}(a, b)$, então, seja $x = \frac{a}{d}$ e $y = \frac{b}{d}$, logo, $\text{mdc}(x, y) = 1$

Prova. Seja $q = \text{mdc}(x, y)$, logo, $q \mid x \implies q \mid \frac{a}{d} \implies qd \mid a$, analogamente $qd \mid b$, então, temos que $qd \mid d$, logo $q = 1$ □

§3 Mínimo Múltiplo Comum

Como definimos o máximo divisor comum, faz sentido definirmos algo análogo para múltiplos!

Definição 3.1. O mínimo múltiplo comum de a, b é o menor número m tal que $a \mid m$ e $b \mid m$, e escrevemos como $\text{mmc}(a, b)$.

Lema 3.2

Seja $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, b = p_1^{\beta_1} \cdots p_k^{\beta_k}$, então

$$\text{mmc}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdots p_k^{\max(\alpha_k, \beta_k)}$$

Proof. Temos que se $p^\alpha \mid a$ e $p^\beta \mid b$, então $p^\alpha \mid \text{mmc}(a, b)$ e $p^\beta \mid \text{mmc}(a, b)$, então $p^{\max(\alpha, \beta)‘} \mid \text{mmc}(a, b)$, então,

$$p_1^{\max(\alpha_1, \beta_1)} \cdots p_k^{\max(\alpha_k, \beta_k)} \mid \text{mmc}(a, b)$$

$$\implies p_1^{\max(\alpha_1, \beta_1)} \cdots p_k^{\max(\alpha_k, \beta_k)} \leq \text{mmc}(a, b)$$

Porém, sabemos que $a \mid p_1^{\max(\alpha_1, \beta_1)} \cdots p_k^{\max(\alpha_k, \beta_k)}$ e $b \mid p_1^{\max(\alpha_1, \beta_1)} \cdots p_k^{\max(\alpha_k, \beta_k)}$, então, como $\text{mmc}(a, b)$ é o menor múltiplo comum de a, b, então $\text{mmc}(a, b) \leq p_1^{\max(\alpha_1, \beta_1)} \cdots p_k^{\max(\alpha_k, \beta_k)} \leq mmc(a, b) \implies p_1^{\max(\alpha_1, \beta_1)} \cdots p_k^{\max(\alpha_k, \beta_k)} = \text{mmc}(a, b)$. □

Veja que isso implica que $\text{mdc}(a, b) \cdot \text{mmc}(a, b) = ab$.

Certo, vamos para os problemas!!

§4 Problemas Resolvidos

Exemplo 4.1

Prove que $\text{mdc}(a^x - 1, a^y - 1) = a^{\text{mdc}(x,y)} - 1$

Solução. Temos que

$$\text{mdc}(a^x - 1, a^y - 1) = \text{mdc}(a^x - 1 - a^{x-y}(a^y - 1), a^y - 1) = \text{mdc}(a^{x-y} - 1, a^y - 1)$$

Então, saimos de (x, y) para $(x - y, y)$, logo, por euclides, conseguimos chegar em $(\text{mdc}(x, y), 0)$, então $\text{mdc}(a^x - 1, a^y - 1) = \text{mdc}(a^{\text{mdc}(x,y)} - 1, a^0 - 1) = a^{\text{mdc}(x,y)} - 1$. □

Exemplo 4.2 (Teste Cone-sul)

Sejam a, b números inteiros positivos tais que $q = \frac{a^2+b^2}{ab}$ é inteiro. Ache todos os valores possíveis de q.

Solução. Veja que $ab \mid a^2 + b^2$. Seja $d = \text{mdc}(a, b), x = \frac{a}{d}$ e $y = \frac{b}{d}$ com $\text{mdc}(x, y) = 1$. Portanto, temos que

$$d^2xy \mid d^2x^2 + d^2y^2 \implies xy \mid x^2 + y^2 \implies x \mid y^2$$

E como $\text{mdc}(x, y) = 1 \implies x \mid 1 \implies x = 1$. Analogamente $y = 1$, então $a = b = d$, então $\frac{a^2+b^2}{ab} = \frac{2a^2}{a^2} = 2$ □

Exemplo 4.3 (Rússia)

Sejam a, b inteiros positivos tal que $\frac{a+1}{b} + \frac{b+1}{a}$ é inteiro. Prove que

$$\text{mdc}(a, b) \leq \sqrt{a + b}$$

Solução. Seja $d = \text{mdc}(a, b)$, $a = dx, b = dy, \text{mdc}(x, y) = 1$. Então

$$\frac{a+1}{b} + \frac{b+1}{a} = \frac{a^2 + b^2 + a + b}{ab} \implies ab \mid a^2 + b^2 + a + b$$

$$\implies d^2xy \mid d^2(x^2 + y^2) + d(x + y) \implies dxy \mid d(x^2 + y^2) + x + y$$

Então $d \mid x + y \implies x + y \geq d$.
Além disso

$$d \leq \sqrt{a + b} \iff d \leq \sqrt{d}\sqrt{x + y} \iff \sqrt{d} \leq \sqrt{x + y} \iff d \leq x + y$$

O que é verdade. □

Exemplo 4.4 (OBM 2019 N2)

Sejam a, b, k inteiros positivos com $k > 1$ tais que

$$\text{mmc}(a, b) + \text{mdc}(a, b) = k(a + b)$$

Prove que $a + b \geq 4k$

Solução. Seja $\text{mdc}(a, b) = d, a = dx, b = dy$ com $\text{mdc}(x, y) = 1$.

Veja que $\text{mdc}(a, b) \cdot \text{mmc}(a, b) = ab \implies d\text{mmc}(a, b) = d^2xy \implies \text{mmc}(a, b) = dxy$, então

$$dxy + d = kd(x + y) \implies xy + 1 = k(x + y)$$

Então, queremos provar que $a + b \geq 4k \implies d(x + y) \geq 4k$, porém, temos que

$$x + y \geq 4k \iff x + y \geq \frac{4(xy + 1)}{x + y} \iff (x + y)^2 \geq 4xy + 4$$

$$\iff x^2 + 2xy + y^2 \geq 4xy + 4 \iff x^2 - 2xy + y^2 \geq 4$$

$$\iff |x - y| \geq 2$$

Logo queremos provar que $|x - y| \geq 2$, então, vamos fazer os casos

- Se $x - y = 0$

Então

$$x^2 + 1 = 2xk \implies x \mid x^2 + 1 \implies x \mid 1 \implies x = 1 \implies k = 1$$

Absurdo pois $k > 1$.

- Se $y - x = 1$

Então

$$x(x + 1) + 1 = k(x + x + 1) \implies x^2 + x + 1 = k(2x + 1) \implies 2x + 1 \mid x^2 + x + 1$$

$$\implies 2x + 1 \mid 2(x^2 + x + 1) - x(2x + 1) \implies 2x + 1 \mid x + 2 \implies x + 2 \geq 2x + 1 \implies$$

$$1 \geq x \implies x = 1 \implies 3 = 3k \implies k = 1$$

Absurdo pois $k > 1$, então $|x - y| \geq 2$, e o problema acabou. $\square$

§5 Problemas Propostos

Problem 5.1. (Rússia) A sequência $a_1, a_2, \cdots, a_n, \cdots$ satisfaz

$$\text{mdc}(a_i, a_j) = \text{mdc}(i, j)$$

para todo $i \neq j$. Prove que $a_i = i \forall i$.

Problem 5.2 (Inglaterra)**.** Sejam x, y naturais tais que $2xy$ divide $x^2 + y^2 - x$. Prove que x é quadrado perfeito

Problem 5.3 (Reino Unido)**.** Sejam x, y, z inteiros positivos tais que

$$\frac{1}{x} - \frac{1}{y} = \frac{1}{z}$$

Seja d o maior divisor comum de x, y, z. Prove que $dxyz$ e $d(y-x)$ são ambos quadrados perfeitos.

Problem 5.4 (Hungria)**.** Dado p primo, ache todos $x, y \in \mathbb{N}$ tais que

$$\frac{2}{p} = \frac{1}{x} + \frac{1}{y}$$

Problem 5.5 (IMO)**.** Chamamos um conjunto A de inteiros de "poggers" se ele cumpre a seguinte propiedade:

- Se $x, y \in A$ (Possivelmente $x = y$), então $x^2 + kxy + y^2 \in A$ para todo inteiro k.

Determine todos os pares de inteiros m, de inteiros não nulos tal que o único conjunto poggers contendo m e n é o conjunto de todos os inteiros.

Problem 5.6 (IMO)**.** Ache todos os inteiros positivos $n \geq 1$ tal que existe um par (a, b) de inteiros positivos tal que $a^2 + b + 3$ não é divisível por um cubo de qualquer primo e

$$n = \frac{ab + 3b + 8}{a^2 + b + 8}$$