teoria de números computacional

cláudia mendes araújo

2024/2025

lcc+lmat | uminho

congruências

definição. Seja $n \in \mathbb{N}$. Diz-se que um inteiro a é congruente módulo n com um inteiro b, e escreve-se $a \equiv b \pmod n$, se n é um divisor de $a - b$, i.e., se $a - b = nk$, para algum $k \in \mathbb{Z}$.

teorema. Para quaisquer inteiros a e b,

$a \equiv b \pmod n$ se e só se a e b têm o mesmo resto na divisão por n.

corolário. Para todo o inteiro a, a é congruente módulo n com o resto da sua divisão por n.

Assim, cada inteiro a é congruente módulo n com um e um só dos inteiros

$$0, 1, 2, \cdots, n-2, n-1.$$

definição. Seja $n \in \mathbb{N}$. Um conjunto de n inteiros $\{a_1, a_2, \cdots, a_n\}$ diz-se um sistema completo de resíduos módulo n se todo o inteiro é congruente módulo n com um e um só a_k ($k \in \{1, 2, ..., n\}$).

exemplo. Os conjuntos $A = \{0, 1, 2, 3, 4\}$ e $B = \{-13, -5, 1, 13, 24\}$ são sistemas completos de resíduos módulo 5.

Os conjuntos $C = \{-13, -5, 0, 1, 13\}$ e $D = \{0, 1, 2, 3, 4, 5\}$ não são sistemas completos de resíduos módulo 5.

teorema. Sejam $a, b, c, d \in \mathbb{Z}$. Então,

(i) $a \equiv a (\mathrm{mod}\, n)$;

(ii) $a \equiv b (\mathrm{mod}\, n) \Rightarrow b \equiv a (\mathrm{mod}\, n)$;

(iii) $(a \equiv b (\mathrm{mod}\, n)$ e $b \equiv c (\mathrm{mod}\, n)) \Rightarrow a \equiv c (\mathrm{mod}\, n)$;

(iv) $a \equiv b (\mathrm{mod}\, n) \Rightarrow \begin{cases} ac \equiv bc (\mathrm{mod}\, n) \\ a + c \equiv b + c (\mathrm{mod}\, n) \end{cases}$;

(v) $ac \equiv bc (\mathrm{mod}\, n) \Rightarrow a \equiv b (\mathrm{mod}\, \frac{n}{\mathrm{m.d.c.}(n,c)})$;

(vi) $(ac \equiv bc (\mathrm{mod}\, n)$ e $\mathrm{m.d.c.}(n, c) = 1) \Rightarrow a \equiv b (\mathrm{mod}\, n)$;

(vii) $(a \equiv b (\mathrm{mod}\, n)$ e $c \equiv d (\mathrm{mod}\, n)) \Rightarrow \begin{cases} ac \equiv bd (\mathrm{mod}\, n) \\ a + c \equiv b + d (\mathrm{mod}\, n) \end{cases}$;

(viii) $a \equiv b (\mathrm{mod}\, n) \Rightarrow a^k \equiv b^k (\mathrm{mod}\, n)$, para todo $k \in \mathbb{N}$;

(ix) $$\left.\begin{array}{c} a \equiv b (\mathrm{mod}\, n_1) \\ a \equiv b (\mathrm{mod}\, n_2) \\ \vdots \\ a \equiv b (\mathrm{mod}\, n_k) \end{array}\right\} \Rightarrow a \equiv b (\mathrm{mod}\, \mathrm{m.m.c.}(n_1, n_2, \ldots, n_k));$$

definição. Chama-se congruência linear a toda a expressão da forma $ax \equiv b (\mathrm{mod}\, n)$ em que $a, b \in \mathbb{Z}$, $a \neq 0$ e x é um símbolo.

Chama-se solução da congruência linear $ax \equiv b (\mathrm{mod}\, n)$ a qualquer inteiro x_0 tal que "$ax_0 \equiv b (\mathrm{mod}\, n)$" é uma afirmação verdadeira.

Resolver uma congruência linear é determinar o conjunto de todas as soluções dessa congruência linear.

exemplo. A congruência linear $2x \equiv 3 (\mathrm{mod}\, 4)$ não tem soluções em $\mathbb{Z}$. De facto, para qualquer $x_0 \in \mathbb{Z}$, $2x_0 - 3$ é um número ímpar e, portanto, não divisível por 4.

exemplo. A congruência linear $2x \equiv 4 (\mathrm{mod}\, 12)$ admite, entre outras, as soluções

$x_0 = 2$, $x_1 = 8$ e $x_2 = -10$.

teorema. Sejam $a, b \in \mathbb{Z}$ e $a \neq 0$. A congruência linear $ax \equiv b \pmod n$ admite solução se e só se $\mathrm{m.d.c.}(a, n) \mid b$.

teorema. Sejam $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ e $d = \mathrm{m.d.c.}(a, n)$. Se x_0 é solução da congruência linear $ax \equiv b \pmod n$, então,

$$x_0,\ x_0 + \frac{n}{d},\ x_0 + \frac{2n}{d}, \cdots,\ x_0 + \frac{(d-1)n}{d}$$

é a lista completa das soluções da congruência linear $ax \equiv b \pmod n$, não congruentes módulo n duas a duas.

corolário. Se $\mathrm{m.d.c.}(a, n) = 1$, então, a congruência linear $ax \equiv b \pmod n$ tem uma e uma só solução módulo n.

exemplo. Queremos resolver a congruência linear

$$18x \equiv 30 \pmod{42}.$$

Como $\mathrm{m.d.c.}(18, 42) = 6$ e $6 \mid 30$, a congruência admite exactamente 6 soluções não congruentes módulo 42, duas a duas.

Uma solução possível é 4 porque

$$18 \times 4 = 72 \equiv 30 \pmod{42}.$$

Logo, as 6 soluções referidas são

$$x \equiv 4 + \frac{42}{6} t \pmod{42}, \qquad t \in \{0, 1, 2, 3, 4, 5\},$$

i.e.,

$$x_1 \equiv 4 \pmod{42}, \qquad x_2 \equiv 11 \pmod{42}, \qquad x_3 \equiv 18 \pmod{42}$$
$$x_4 \equiv 25 \pmod{42}, \qquad x_5 \equiv 32 \pmod{42}, \qquad x_6 \equiv 39 \pmod{42}.$$

Assim, o conjunto das soluções da congruência linear $18x \equiv 30 (\mathrm{mod}\, 42)$ é

$$C.S. = \{x \in \mathbb{Z} \mid x \equiv 4 (\mathrm{mod}\, 42) \vee x \equiv 11 (\mathrm{mod}\, 42) \vee x \equiv 18 (\mathrm{mod}\, 42) \vee \\ \vee x \equiv 25 (\mathrm{mod}\, 42) \vee x \equiv 32 (\mathrm{mod}\, 42) \vee x \equiv 39 (\mathrm{mod}\, 42)\}.$$

proposição. Sejam $ax \equiv b (\mathrm{mod}\, n)$ uma congruência linear que admite soluções e $d = \mathrm{m.d.c.}(a, n)$. Então,

$$ax \equiv b (\mathrm{mod}\, n) \Leftrightarrow \frac{a}{d} x \equiv \frac{b}{d} (\mathrm{mod}\, \frac{n}{d}).$$

observação. $\mathrm{m.d.c.}\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, pelo que $ax \equiv b (\mathrm{mod}\, n)$ admite uma e uma só solução módulo $\frac{n}{d}$.

exemplo. Consideremos novamente a congruência linear

$$18x \equiv 30 (\mathrm{mod}\, 42).$$

Como $\mathrm{m.d.c.}(18, 42) = 6$ e $6 \mid 30$,

$$\begin{aligned} 18x \equiv 30 (\mathrm{mod}\, 42) &\Leftrightarrow \frac{18}{6} x \equiv \frac{30}{6} (\mathrm{mod}\, \frac{42}{6}) \\ &\Leftrightarrow 3x \equiv 5 (\mathrm{mod}\, 7) \end{aligned}$$

e, portanto, $18x \equiv 30 (\mathrm{mod}\, 42)$ admite uma e uma só solução módulo 7.

A solução é 4 porque

$$3 \times 4 \equiv 5 (\mathrm{mod}\, 7).$$

Logo, o conjunto das soluções da congruência linear dada é

$$C.S. = \{x \in \mathbb{Z} \mid x \equiv 4 (\mathrm{mod}\, 7)\}.$$

Consideremos a congruência linear

$$ax \equiv 1(\mathrm{mod}\, n).$$

Sabemos que a congruência tem solução se e só se $\mathrm{m.d.c.}(a, n) = 1$ e, nesse caso, a solução é única módulo n.

Se $\mathrm{m.d.c.}(a, n) = 1$, a solução da congruência $ax \equiv 1(\mathrm{mod}\, n)$ é o inverso de a em $\mathbb{Z}_n$, denotado por a^{-1}.

Dado um natural n, denotamos por $\mathbb{Z}_n^*$ o conjunto dos elementos a de $\mathbb{Z}_n$ invertíveis (*i.e.*, a tal que $\mathrm{m.d.c.}(a, n) = 1$).

Dado um primo p, sabemos que

$$\mathbb{Z}_p^* = \{1, \ldots, p-1\}.$$

$(\mathbb{Z}_p^*, +, \cdot)$ é um corpo. Em particular, $(\mathbb{Z}_p^*, \cdot)$ é um grupo comutativo (cíclico).

Mais tarde, precisamos saber quais inteiros são os seus próprios inversos módulo p, onde p é primo. O próximo teorema diz-nos quais inteiros têm esta propriedade.

teorema. Seja p um número primo. O inteiro positivo a é o seu próprio inverso módulo p se e só se $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$.

demonstração. Suponhamos que $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$.

Então, $a^2 \equiv 1 \pmod{p}$, o que implica que a é o seu próprio inverso módulo p.

Reciprocamente, se a é o seu próprio inverso módulo p, então $a^2 = a \cdot a \equiv 1 \pmod{p}$. Assim, $p \mid (a^2 - 1)$.

Como $a^2 - 1 = (a-1)(a+1)$, isto implica que $p \mid (a-1)$ ou $p \mid (a+1)$. Portanto, $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$.

observação. Se n for um natural para o qual existe a tal que $a^2 \equiv 1 \pmod{n}$, mas $a \not\equiv 1 \pmod{n}$ e $a \not\equiv -1 \pmod{n}$, podemos concluir que n não é primo.

definição. Chama-se sistema de congruências lineares a um sistema do tipo

$$(S) \qquad \begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \vdots \\ a_k x \equiv b_k \pmod{n_k} \end{cases}$$

onde $k \in \mathbb{N} \backslash \{1\}$ e, para todo $i \in \{1, ..., k\}$, $a_i, b_i \in \mathbb{Z}$ e $n_i \in \mathbb{N}$.

Uma solução de (S) é qualquer inteiro que é solução de todas as congruências de (S).

exemplo. O sistema de congruências lineares

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{4} \end{cases}$$

admite a solução $x_0 = 5$.

exemplo. O sistema de congruências lineares

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 4 \pmod{6} \end{cases}$$

não admite soluções inteiras.

Teorema Chinês dos Restos (TCR). Sejam $k \in \mathbb{N}\backslash\{1\}$, $a_1, a_2, ..., a_k \in \mathbb{Z}$ e $n_1, n_2, ..., n_k \in \mathbb{N}$ tais que

$$\forall i, j \in \{1, ..., k\} \qquad (i \neq j \Longrightarrow \text{m.d.c.}(n_i, n_j) = 1).$$

Então, o sistema de congruências lineares

$$(S) \begin{cases} x \equiv a_1 (\mathrm{mod}\, n_1) \\ x \equiv a_2 (\mathrm{mod}\, n_2) \\ \vdots \\ x \equiv a_k (\mathrm{mod}\, n_k) \end{cases}$$

tem uma e uma só solução módulo $n_1 n_2 \cdots n_k$.

demonstração Seja $n = n_1 \times n_2 \times \cdots \times n_k$. Para cada $i \in \{1, 2, ..., k\}$, seja

$$N_i = \frac{n}{n_i} = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$$

.

Como, para $i \neq j$, n_i e n_j são primos entre si, também $\mathrm{m.d.c.}(N_i, n_i) = 1$ e, portanto, para cada i, a congruência linear $N_i x \equiv 1 (\mathrm{mod}\, n_i)$ admite solução única módulo n_i. Seja ela x_i.

Mostremos que o inteiro

$$x_0 = x_1 N_1 a_1 + x_2 N_2 a_2 + \cdots + x_k N_k a_k$$

é solução de (S).

Comecemos por observar que, para $r, i \in \{1, 2, ..., k\}$ e $r \neq i$, como $n_r \mid N_i$, $N_i \equiv 0 (\mathrm{mod}\, n_r)$ e, portanto,

$$x_0 = x_1 N_1 a_1 + x_2 N_2 a_2 + \cdots + x_k N_k a_k \equiv a_r N_r x_r (\mathrm{mod}\, n_r).$$

Como x_r é solução de $N_r x \equiv 1 (\mathrm{mod}\, n_r)$, obtemos

$$x_0 \equiv a_r (\mathrm{mod}\, n_r).$$

Portanto, o sistema (S) admite a solução x_0.

Suponhamos de seguida que x' é outra solução de (S).

Então,

$$x_0 \equiv x' (\operatorname{mod} n_r),$$

para qualquer $r \in \{1, 2, ..., k\}$.

Portanto, $n_r \mid x_0 - x'$, para cada $r \in \{1, 2, ..., k\}$.

Como $\mathrm{m.d.c.}(n_i, n_j) = 1$ $(i \neq j)$, obtemos

$$n_1 n_2 \cdots n_k \mid x_0 - x'.$$

Assim, $x_0 \equiv x' (\operatorname{mod} n)$.

Problema de Sun-Tsu. Encontre um número que tem resto 2, 3 e 2 na divisão por 3, 5 e 7, respectivamente.

O problema traduz-se na resolução do seguinte sistema de congruências lineares

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}.$$

Sejam

$$n = 3 \times 5 \times 7 = 105$$

e

$$N_1 = \frac{n}{3} = 35,$$

$$N_2 = \frac{n}{5} = 21$$

e

$$N_3 = \frac{n}{7} = 15.$$

Como $\mathrm{m.d.c.}(35,3) = \mathrm{m.d.c.}(21,5) = \mathrm{m.d.c.}(15,7) = 1$, temos que cada uma das congruências lineares

$$35x \equiv 1 (\mathrm{mod}\, 3), \qquad 21x \equiv 1 (\mathrm{mod}\, 5), \qquad 15x \equiv 1 (\mathrm{mod}\, 7)$$

admite uma e uma só solução módulo 3, 5 e 7: $x_1 = 2$, $x_2 = 1$ e $x_3 = 1$, respectivamente.

Pelo TCR,

$$x_0 = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 233$$

é uma solução do sistema inicial.

Logo, a única solução do sistema módulo 105 é

$$x \equiv 233 (\mathrm{mod}\, 105), \text{ ou seja, é } x \equiv 23 (\mathrm{mod}\, 105).$$

O TCR fornece uma forma de realizar aritmética computacional com inteiros grandes.

Armazenar inteiros muito grandes e efetuar operações aritméticas com eles requer técnicas especiais.

O TCR diz-nos que, dados módulos $m_1, m_2, \ldots, m_r$, primos entre si dois a dois, um inteiro positivo n tal que $n < M = m_1 m_2 \ldots m_r$ é determinado univocamente pelos seus menores resíduos positivos módulo m_j para $j = 1, 2, \ldots, r$.

exemplo. Suponhamos que uma máquina opera apenas com números inferiores a 100, mas queremos calcular $123 + 456$.

Primeiro, encontramos inteiros primos entre si dois a dois menores ou iguais a 100, cujo produto exceda o valor que pretendemos calcular. Por exemplo, podemos escolher $m_1 = 99$ e $m_2 = 98$.

De seguida, convertemos $a = 123$ e $b = 456$ em pares formados pelos seus menores resíduos positivos módulo m_1 e m_2.

Temos que a é associado ao par $(24, 25)$ e b ao par $(60, 64)$, uma vez que

$$a \equiv 24 \pmod{99} \quad \text{e} \quad a \equiv 25 \pmod{98}$$

e

$$b \equiv 60 \pmod{99} \quad \text{e} \quad b \equiv 64 \pmod{98}.$$

Sabemos que

$$a + b \equiv 24 + 60 \pmod{99} \quad \text{e} \quad a + b \equiv 25 + 64 \pmod{98}$$

Pelo TCR, sabemos que $a + b$ é univocamente determinado pelos seus menores resíduos positivos módulo m_1 e m_2, uma vez que existe uma única solução módulo $m_1 \times m_2 = 9702$ do sistema

$$\begin{cases} x \equiv 84 \pmod{99} \\ x \equiv 89 \pmod{98} \end{cases}.$$

Usando o TCR, obtemos a solução $x \equiv 579 \pmod{9702}$, o que nos permite concluir que $123 + 456 = 579$ (pois claramente $123 + 456 < 9702$).

exemplo. Suponhamos, agora, que pretendemos calcular 123×456 numa máquina que opera apenas com números inferiores a 100.

Sabemos que

$$123 \times 456 \equiv 24 \times 60 (\mathrm{mod}\, 99) \quad \text{e} \quad 123 \times 456 \equiv 25 \times 64 (\mathrm{mod}\, 98).$$

Pelo TCR, sabemos que 123×456 é univocamente determinado pelos seus menores resíduos positivos módulo 99 e 98, uma vez que existe uma única solução módulo $99 \times 98 = 9702$ do sistema

$$\begin{cases} x \equiv 54 (\mathrm{mod}\, 99) \\ x \equiv 32 (\mathrm{mod}\, 98) \end{cases}.$$

Usando o TCR, obtemos a solução $x \equiv 7578 (\mathrm{mod}\, 9702)$, mas, obviamente, $123 \times 456 > 7578$. Por este processo, apenas concluímos que $123 \times 456 \equiv 7578 (\mathrm{mod}\, 9702)$.

Para contornar esta questão, podemos usar representações de 123 e 456 como ternos ordenados de resíduos em $\mathbb{Z}_{99}$, $\mathbb{Z}_{98}$ e $\mathbb{Z}_{m_3}$, com $m_3 < 100$ (suficientemente grande) que seja primo com 99 e com 98.

Consideremos $m_3 = 97$.

Sabemos que

$123 \times 456 \equiv 24 \times 60 \pmod{99}$, $123 \times 456 \equiv 25 \times 64 \pmod{98}$ e $123 \times 456 \equiv 26 \times 68 \pmod{97}$.

Pelo TCR, sabemos que 123×456 é univocamente determinado pelos seus menores resíduos positivos módulo 99, 98 e 97, uma vez que existe uma única solução módulo $99 \times 98 \times 97 = 941094$ do sistema

$$\begin{cases} x \equiv 54 \pmod{99} \\ x \equiv 32 \pmod{98} \\ x \equiv 22 \pmod{97} \end{cases}.$$

Usando o TCR, obtemos a solução $x \equiv 56088 \pmod{941094}$, o que nos permite concluir que $123 \times 456 = 56088$ (uma vez que, claramente, $123 \times 456 < 941094$).

O algoritmo de fatorização ρ-Pollard é um algoritmo probabilístico para fatorizar números inteiros grandes.

John Pollard inventou este algoritmo de factorização em 1975. É relativamente rápido para números com fatores primos pequenos, mesmo que esses números sejam grandes, e tem um consumo de memória muito reduzido, tornando-se assim uma ferramenta útil para uma análise inicial.

Explora a ideia de que, se tivermos dois números x_i e x_j que são congruentes módulo um fator primo de n, mas não módulo n inteiro, então podemos extrair um fator não trivial de n usando o máximo divisor comum.

O primeiro passo é escolher uma sequência pseudoaleatória $x_0, x_1, \ldots, x_s$. Escolhemos um número inicial x_0 e definimos uma sequência recorrente dada por uma função polinomial $f(x) \in \mathbb{Z}[x]$, tipicamente:

$$x_{k+1} \equiv f(x_k) \pmod{n}.$$

Um polinómio simples e comum é $f(x) = x^2 + 1$ (ou $f(x) = x^2 \pm a$, onde $a \neq 0, 2$), pois gera bons números pseudoaleatórios quando considerado com vários módulos.

O segundo passo do algoritmo é procurar "colisões" módulo um fator de n.

A ideia-chave é que, se n for composto e tivermos o seu menor fator primo p, então os números da sequência terão comportamentos diferentes quando tomamos restos módulo n e módulo p.

Em particular, queremos encontrar dois índices i e j (com $i < j$) tais que:

$$x_i \equiv x_j \pmod{p} \quad \text{(iguais módulo } p\text{),}$$

mas

$$x_i \not\equiv x_j \pmod{n} \quad \text{(diferentes módulo } n\text{).}$$

Ou seja, os valores repetem-se módulo p, mas não módulo n. Isto acontece porque a sequência repete-se mais cedo quando reduzida módulo p, criando um ciclo.

Se conseguirmos obter tais inteiros, então, dado que p divide $(x_j - x_i)$ e p divide n, e dado que n não divide $(x_j - x_i)$, segue-se que

$$p \leq \mathrm{m.d.c.}(x_j - x_i, n) \leq n$$

e, portanto, $\mathrm{m.d.c.}(x_j - x_i, n)$ seria um fator não trivial de n.

Como assumimos que p é pequeno, é provável que rapidamente encontremos x_i e x_j, com $i < j$, tais que $x_j - x_i \equiv 0 (\bmod p)$, (pois módulo p existem apenas p valores distintos), mas ao mesmo tempo $x_j - x_i \not\equiv 0 (\bmod n)$.

Obviamente, não podemos testar diretamente esta congruência, pois não conhecemos p, mas podemos calcular $\mathrm{m.d.c.}(x_j - x_i, n)$ e verificar se o resultado é diferente de 1 e de n.

Suponhamos que, ao longo do processo, encontramos x_i e x_j tais que $x_i \equiv x_j \pmod{p}$. Depois do índice i, estes valores irão repetir-se a cada $j - i$ elementos. Por exemplo, se $i = 22$ e $j = 27$, então a repetição ocorre a cada 5 elementos a partir de $i = 22$.

Dado isto, seja s o menor múltiplo de $j - i$ que seja maior ou igual a i. Como $2s - s = s$ é um múltiplo de $j - i$, segue-se que

$$x_{2s} \equiv x_s \pmod{p}.$$

Muito provavelmente também teremos

$$x_{2s} \not\equiv x_s \pmod{n},$$

e assim x_{2s} e x_s serão úteis para encontrar um fator de n.

Mas como podemos encontrar s sem saber i ou j?

Simplesmente continuamos a calcular a sequência e testamos apenas x_{2s} e x_s.

Mais uma vez, não conseguimos testar diretamente $x_{2s} \equiv x_s \pmod{p}$, pois não conhecemos p, mas podemos calcular

$$\mathrm{m.d.c.}(x_{2s} - x_s, n)$$

e verificar se o resultado é diferente de 1 e n.

É possível (embora, na prática, improvável) que as repetições sejam congruentes módulo n assim como módulo p, o que resultaria num máximo divisor comum igual a n. Nesse caso, o algoritmo falha. Quando isso acontece, tentamos um valor inicial diferente ou, eventualmente, um polinómio distinto.

Se n for primo, o algoritmo ρ-Pollard falha em encontrar um fator, pois ele depende da existência de um divisor próprio de n para funcionar.

exemplo. Vamos fatorizar $n = 1111$. Definimos $x_0 = 2$ e $f(x) = x^2 + 1$.

Calculemos:

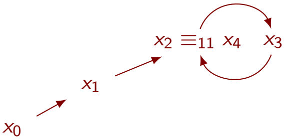
$$f(x_0) = 2^2 + 1 = 5; \quad x_1 \equiv 5 \pmod{1111},$$
$$f(x_1) = 5^2 + 1 = 26; \quad x_2 \equiv 26 \pmod{1111},$$
$$\text{m.d.c.}(x_2 - x_1, n) = \text{m.d.c.}(26 - 5, 1111) = 1,$$
$$f(x_2) = 26^2 + 1 = 677; \quad x_3 \equiv 677 \pmod{1111},$$
$$f(x_3) = 677^2 + 1 = 458330; \quad x_4 \equiv 598 \pmod{1111},$$
$$\text{m.d.c.}(x_4 - x_2, n) = \text{m.d.c.}(598 - 26, 1111) = 11.$$

Sabemos, assim, que 11 é um fator de n.

algoritmo de fatorização ρ-Pollard | exemplo

Temos

$$
\begin{aligned}
x_0 &\equiv 2 \pmod{11},\\
x_1 &\equiv 5 \pmod{11},\\
x_2 &\equiv 4 \pmod{11},\\
x_3 &\equiv 6 \pmod{11},\\
x_4 &\equiv 4 \pmod{11},\\
x_5 &\equiv 6 \pmod{11},\\
&\ \vdots
\end{aligned}
$$



exemplo. Vamos fatorizar $n = 5293$. Definimos $x_0 = 2$ e $f(x) = x^2 + 1$.

Calculemos:

$$
\begin{aligned}
&f(x_0) = 2^2 + 1 = 5; \quad x_1 \equiv 5 \pmod{5293},\\
&f(x_1) = 5^2 + 1 = 26; \quad x_2 \equiv 26 \pmod{5293},\\
&\text{m.d.c.}(x_2 - x_1, n) = 1,\\
&f(x_2) = 26^2 + 1 = 677; \quad x_3 \equiv 677 \pmod{5293},\\
&f(x_3) = 677^2 + 1 = 458330; \quad x_4 \equiv 3132 \pmod{5293},\\
&\text{m.d.c.}(x_4 - x_2, n) = 1,\\
&f(x_4) = 3132^2 + 1 = 9809425; \quad x_5 \equiv 1495 \pmod{5293},\\
&f(x_5) = 1496^2 + 1 = 2238017; \quad x_6 \equiv 4371 \pmod{5293},\\
&\text{m.d.c.}(x_6 - x_3, n) = 1,\\
&f(x_6) = 4371^2 + 1 = 19105642; \quad x_7 \equiv 3205 \pmod{5293},\\
&f(x_7) = 3205^2 + 1 = 10272026; \quad x_8 \equiv 3606 \pmod{5293},\\
&\text{m.d.c.}(x_8 - x_4, n) = 79.
\end{aligned}
$$

Sabemos, assim, que 79 é um fator de n.

Vejamos que os números $x_0, \ldots, x_8$ são incongruentes dois a dois módulo 5293, mas há "colisão" módulo 79:

$x_0 \equiv 2 \pmod{5293}$	$x_0 \equiv 2 \pmod{79}$
$x_1 \equiv 5 \pmod{5293}$	$x_1 \equiv 5 \pmod{79}$
$x_2 \equiv 26 \pmod{5293}$	$x_2 \equiv 26 \pmod{79}$
$x_3 \equiv 677 \pmod{5293}$	$x_3 \equiv 45 \pmod{79}$
$x_4 \equiv 3132 \pmod{5293}$	$x_4 \equiv 51 \pmod{79}$
$x_5 \equiv 1495 \pmod{5293}$	$x_5 \equiv 73 \pmod{79}$
$x_6 \equiv 4371 \pmod{5293}$	$x_6 \equiv 26 \pmod{79}$
$x_7 \equiv 3205 \pmod{5293}$	$x_7 \equiv 45 \pmod{79}$
$x_8 \equiv 3606 \pmod{5293}$	$x_8 \equiv 51 \pmod{79}$

input: inteiro n composto
output: um fator não trivial de n
passo 1.: $a \leftarrow 2$, $b \leftarrow 2$
passo 2.:

2.1. calcular
$b = b^2 + 1$
$a = a^2 + 1$
$a = a^2 + 1$

2.2. calcular
$d = \mathrm{m.d.c.}(a - b, n)$

2.3. se $d = 1$, voltar ao passo **2.1.**

2.4. se $1 < d < n$, devolver o fator d.

2.5. se $d = n^{(*)}$, terminar sem sucesso.

obs.: a probabilidade de $(*)$ acontecer é quase nula.

teorema (Teorema de Wilson). Se p é um número primo, então, $(p-1)! \equiv -1 \pmod{p}$.

Antes de provar o teorema de Wilson, usamos um exemplo para ilustrar a ideia por detrás da demonstração.

exemplo. Seja $p = 7$. Temos $(7-1)! = 6! = 1 \times 2 \times 3 \times 4 \times 5 \times 6$. Rearranjamos os fatores no produto, agrupando pares de inversos módulo 7. Notamos que

$$2 \times 4 \equiv 1 \pmod{7} \quad \text{e} \quad 3 \times 5 \equiv 1 \pmod{7}.$$

Assim,

$$\begin{aligned} 6! &\equiv 1 \times (2 \times 4) \times (3 \times 5) \times 6 \pmod{7} \\ &\equiv 1 \times 1 \times 1 \times 6 \pmod{7} \\ &\equiv -1 \pmod{7}. \end{aligned}$$

demonstração (teorema de Wilson). A verificação da condição para $p = 2$ e $p = 3$ é trivial.

Consideremos $p > 3$. Seja $a \in \{1, 2, 3, ..., p-1\}$. Consideramos a congruência linear

$$ax \equiv 1 (\mathrm{mod}\, p).$$

Como $\mathrm{m.d.c.}(a, p) = 1$, existe uma e uma só solução módulo p desta congruência linear. Note-se que essa solução é o inverso de a em $\mathbb{Z}_p$, a^{-1}.

Então,

$$1 \leq a^{-1} \leq p - 1 \text{ e } aa^{-1} \equiv 1 (\mathrm{mod}\, p).$$

Se $a = a^{-1}$ temos

$$\begin{aligned} a^2 \equiv 1 (\bmod p) \quad &\Leftrightarrow p \mid a^2 - 1 \\ &\Leftrightarrow p \mid (a-1)(a+1) \\ &\Leftrightarrow p \mid a - 1 \qquad ou \qquad p \mid a + 1 \\ &\Leftrightarrow a \equiv 1 (\bmod p) \qquad ou \qquad a \equiv -1 (\bmod p). \end{aligned}$$

Se $a \neq a^{-1}$, temos então que

$$a \in \{2, 3, 4, ..., p-3, p-2\}.$$

Os $p - 3$ elementos deste conjunto podem ser agrupados em pares (a, a^{-1}) tais que $a \neq a^{-1}$ e $aa^{-1} \equiv 1 (\bmod p)$.

Obtemos $\frac{p-3}{2}$ pares e, portanto, $\frac{p-3}{2}$ expressões do tipo $aa^{-1} \equiv 1 (\bmod p)$.

Assim,

$$2 \times 3 \times \cdots \times (p-3) \times (p-2) \equiv 1 (\bmod p),$$

i.e.,

$$(p-2)! \equiv 1 (\bmod p).$$

Logo,

$$(p-1)! = (p-1)(p-2)! \equiv p-1 (\bmod p)$$

e, portanto,

$$(p-1)! \equiv -1 (\bmod p).$$

exemplo. Vejamos que o resto da divisão de 18! por 19 é 18, ilustrando a demonstração do Teorema de Wilson.

Seja $p = 19$. Da lista

$2 - 3 - 4 - 5 - 6 - 7 - 8 - 9 - 10 - 11 - 12 - 13 - 14 - 15 - 16 - 17$

podemos formar 8 pares de números e com eles formar as 8 congruências:

$$2 \times 10 \equiv 1 \pmod{19}$$

$$3 \times 13 \equiv 1 \pmod{19}$$

$$4 \times 5 \equiv 1 \pmod{19}$$

$$6 \times 16 \equiv 1 \pmod{19}$$

$$7 \times 11 \equiv 1 \pmod{19}$$

$$8 \times 12 \equiv 1 \pmod{19}$$

$$9 \times 17 \equiv 1 \pmod{19}$$

$$14 \times 15 \equiv 1 \pmod{19}.$$

Então,

$2 \times 10 \times 3 \times 13 \times 4 \times 5 \times 6 \times 16 \times 7 \times 11 \times 8 \times 12 \times 9 \times 17 \times 14 \times 15 \equiv 1 \pmod{19}$, i.e.,

$$17! \equiv 1 \pmod{19}.$$

Logo,

$$18! = 18 \times 17! \equiv 18 \times 1 \pmod{19},$$

i.e.,

$$(19-1)! \equiv -1 \pmod{19}.$$

teorema. Se $(n-1)! \equiv -1 \pmod{n}$, então n é primo.

demonstração. Suponhamos que n não é primo. Então, $n = ab$ para alguns naturais a, b tais que $1 < a, b \leq n-1$.

Como $1 < a \leq n-1$ concluímos que $a \mid (n-1)!$.

De $a \mid n$, como $n \mid (n-1)! + 1$ por hipótese, concluímos que $a \mid (n-1)! + 1$.

Logo,

$$a \mid (n-1)! + 1 - (n-1)!,$$

ou seja, $a \mid 1$, o que contradiz o facto de $1 < a$.

Portanto, n é primo.

observação. Um inteiro positivo n é primo se e só se $(n-1)! \equiv -1 (\mathrm{mod}\, n)$.

Os primos de Wilson são números primos p que satisfazem a seguinte propriedade

$$(p-1)! \equiv -1 (\mathrm{mod}\, p^2),$$

ou seja, além da condição do teorema de Wilson $(p-1)! \equiv -1 (\mathrm{mod}\, p)$, o fatorial de $p-1$ também é congruente a -1 módulo p^2.

Os primos de Wilson são extremamente raros. Conhecem-se apenas três números que satisfazem essa condição:

$$p = 5, 13, 563$$

Nenhum outro primo menor que 5×10^8 foi encontrado como primo de Wilson.

A propriedade que define um primo de Wilson envolve fatoriais, que crescem rapidamente, tornando a verificação para números grandes computacionalmente difícil.

Conjetura-se que há um número infinito de primos de Wilson.

teorema. (Pequeno Teorema de Fermat) Se p é primo e a é um inteiro não divisível por p, então, $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

demonstração. Consideremos os seguintes $p-1$ múltiplos de a:

$$a \qquad 2a \qquad 3a \qquad \cdots \qquad (p-1)a. \qquad\qquad (*)$$

Como p não divide a, temos, para todos $r, s \in \{1, 2, ..., p-1\}$ (com $r \neq s$), que

$$ra \not\equiv sa (\mathrm{mod}\, p) \qquad \text{e} \qquad ra \not\equiv 0 (\mathrm{mod}\, p).$$

Temos, assim, em $(*)$, $p-1$ inteiros não congruentes dois a dois módulo p; logo, $a, 2a, 3a, \cdots, (p-1)a$ são congruentes módulo p com um e um só dos números $1, 2, 3, ..., p-1$.

Portanto,

$$a \times 2a \times 3a \times \cdots \times (p-1)a \equiv 1 \times 2 \times 3 \times \cdots \times (p-1) \pmod{p}.$$

Logo, $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$.

Mas, $\mathrm{m.d.c.}(p,(p-1)!) = 1$, pelo que

$$a^{p-1} \equiv 1 \pmod{p}.$$

corolário. Se p é primo, então $a^p \equiv a \pmod{p}$, para qualquer inteiro a.

demonstração. Por um lado, se $p \mid a$, então, $a \equiv 0 \pmod{p}$, pelo que $a^p \equiv 0 \pmod{p}$. Logo, $a^p \equiv a \pmod{p}$.

Por outro lado, se $p \nmid a$, então, pelo Pequeno Teorema de Fermat, $a^{p-1} \equiv 1 \pmod{p}$, ou seja, $a^p \equiv a \pmod{p}$.

exemplo. Queremos provar que $5^{33} \equiv 6 \pmod 7$. Como 7 é primo e $7 \nmid 5$, podemos afirmar, pelo Pequeno Teorema de Fermat, que

$$5^6 \equiv 1 \pmod 7.$$

Assim,

$$5^{33} = (5^6)^5 \times 5^3 \equiv 5^3 \pmod 7.$$

Como $5^2 = 25 \equiv 4 \pmod 7$, temos que $5^3 \equiv 4 \times 5 \pmod 7$, ou seja, $5^3 \equiv 6 (mod 7)$.

Concluímos, então, que $5^{33} \equiv 6 \pmod 7$.

observação. Dado $n \in \mathbb{N}$, se existe $a \in \mathbb{Z}$ tal que $a^n \not\equiv a (\mod n)$, então n não é um número primo.

exemplo. Mostremos que 117 não é um número primo. Consideremos $a = 2$ e vejamos que $2^{117} \not\equiv 2 \pmod{117}$.

Calculemos o resto da divisão de 2^{117} por 117. A potência de 2 mais próxima de 117 é $2^7 = 128$.

Sabemos que

$$2^7 = 128 \equiv 11 \pmod{117}.$$

Assim, temos que

$$
\begin{aligned}
2^{117} = 2^{7\times 16+5} \equiv 11^{16} \times 2^5 \pmod{117} \quad & \Leftrightarrow 2^{117} \equiv 11^{2\times 8} \times 2^5 \pmod{117} 6pt \\
& \Leftrightarrow 2^{117} \equiv (11^2)^8 \times 2^5 \pmod{117} \\
& \Leftrightarrow 2^{117} \equiv 121^8 \times 2^5 \pmod{117} \\
& \Leftrightarrow 2^{117} \equiv 4^8 \times 2^5 \pmod{117} \\
& \Leftrightarrow 2^{117} \equiv 2^{16} \times 2^5 \pmod{117} \\
& \Leftrightarrow 2^{117} \equiv 2^{21} \pmod{117} \\
& \Leftrightarrow 2^{117} \equiv (2^7)^3 \pmod{117} \\
& \Leftrightarrow 2^{117} \equiv 11^3 \pmod{117} \\
& \Leftrightarrow 2^{117} \equiv 121 \times 11 \pmod{117} \\
& \Leftrightarrow 2^{117} \equiv 4 \times 11 \pmod{117} \\
& \Leftrightarrow 2^{117} \equiv 44 \pmod{117}.
\end{aligned}
$$

Logo, $2^{117} \not\equiv 2 \pmod{117}$, pelo que podemos concluir que 117 não é primo.

exemplo. Vejamos que existem inteiros a e p para os quais $a^{p-1} \equiv 1 \pmod{p}$ e p não é primo.

Como $4^2 = 16 \equiv 1 \pmod{15}$, temos que $4^{14} \equiv 1^7 \pmod{15}$, ou seja, $a^{15-1} \equiv 1 \pmod{15}$.

No entanto, 15 não é um número primo.

O seguinte resultado é consequência do Pequeno Teorema de Fermat.

teorema. Se p é primo e a é um inteiro tal que $p \nmid a$, então a^{p-2} é um inverso de a módulo p.

demonstração. Se $p \nmid a$, pelo pequeno teorema de Fermat, sabemos que

$$a \times a^{p-2} = a^{p-1} \equiv 1 \pmod{p}.$$

Logo, a^{p-2} é um inverso de a módulo p.

exemplo. Pelo teorema anterior, sabemos que $2^9 = 512 \equiv 6 \pmod{11}$ é um inverso de 2 módulo 11.

O teorema anterior dá-nos uma outra forma de resolver congruências lineares em relação a módulos primos.

corolário. Se a e b são números inteiros positivos e p é primo com $p \nmid a$, então as soluções da congruência linear $ax \equiv b \pmod{p}$ são os inteiros x tais que $x \equiv a^{p-2} b \pmod{p}$.

demonstração. Suponhamos que $ax \equiv b \pmod{p}$. Como $p \nmid a$, sabemos, pelo teorema anterior, que a^{p-2} é um inverso de a módulo p. Multiplicando ambos os lados da congruência original por a^{p-2}, temos

$$a^{p-2}\ ax \equiv a^{p-2}\ b \pmod{p}.$$

Logo,

$$x \equiv a^{p-2} b \pmod{p}.$$

O Pequeno Teorema de Fermat é a base de um método de fatorização inventado por John Pollard em 1974, o algoritmo $(p-1)$-Pollard.

Este método consegue encontrar um fator não trivial de um inteiro n quando n tem um fator primo p tal que os primos que dividem $p-1$ são relativamente pequenos.

Para entender como este método funciona, suponhamos que queremos encontrar um fator do inteiro positivo n.

Além disso, suponhamos que n tem um fator primo p tal que $p-1$ divide $k!$, onde k é um inteiro positivo.

Queremos que $p-1$ tenha apenas fatores primos pequenos, de modo que exista um inteiro k que não seja muito grande.

A razão pela qual queremos que $p-1$ divida $k!$ é para que possamos aplicar o Pequeno Teorema de Fermat.

Pelo Pequeno Teorema de Fermat, sabemos que:

$$2^{p-1} \equiv 1 \pmod{p}.$$

Como $p-1$ divide $k!$, temos que $k! = (p-1)q$, para algum inteiro q. Assim, podemos escrever:

$$2^{k!} = 2^{(p-1)q} = (2^{p-1})^q \equiv 1^q = 1 \pmod{p},$$

o que implica que p divide $2^{k!}-1$.

Seja M o resto da divisão de $2^{k!}-1$ por n.

Temos que

$$2^{k!} - 1 = nt + M,$$

para algum inteiro t, pelo que

$$M = (2^{k!} - 1) - nt.$$

Note-se que $p \mid M$, uma vez que $p \mid (2^{k!}-1)$ e $p \mid n$. Portanto, $p \mid \mathrm{m.d.c.}(M, n)$.

Para encontrar um divisor de n, basta então calcular o máximo divisor comum de M e n, o que pode ser feito rapidamente utilizando o algoritmo de Euclides.

Para que este divisor seja um divisor não trivial, é necessário que M seja não nulo, correspondendo ao caso em que n não divide $2^{k!}-1$, o que é bastante provável quando n tem fatores primos grandes.

Para usar o algoritmo de fatorização $(p-1)$-Pollard, precisamos de calcular $2^{k!}$, onde k é um inteiro positivo.

Este cálculo pode ser feito de forma eficiente usando a **exponenciação modular**.

Para encontrar o menor resíduo positivo de $2^{k!}$ módulo n, definimos $r_1 = 2$ e usamos a seguinte sequência de cálculos:

$$r_2 \equiv r_1^2 \pmod{n}, \quad r_3 \equiv r_2^3 \pmod{n}, \quad r_4 \equiv r_3^4 \pmod{n}, \quad \ldots, \quad r_k \equiv r_{k-1}^k \pmod{n}.$$

exemplo. Determinemos, usando exponenciação modular, $2^{9!} \pmod{5157437}$.

Sejam $n = 5157437$ e $r_1 = 2$. Temos que

$$\begin{aligned}
r_2 &\equiv r_1^2 = 2^2 \equiv 4 \pmod{n},\\
r_3 &\equiv r_2^3 = 4^3 \equiv 64 \pmod{n},\\
r_4 &\equiv r_3^4 = 64^4 \equiv 1304905 \pmod{n},\\
r_5 &\equiv r_4^5 = 1304905^5 \equiv 404913 \pmod{n},\\
r_6 &\equiv r_5^6 = 404913^6 \equiv 2157880 \pmod{n},\\
r_7 &\equiv r_6^7 = 2157880^7 \equiv 4879227 \pmod{n},\\
r_8 &\equiv r_7^8 = 4879227^8 \equiv 4379778 \pmod{n},\\
r_9 &\equiv r_8^9 = 4379778^9 \equiv 4381440 \pmod{n}.
\end{aligned}$$

Logo,

$$2^{9!} \equiv 4381440 \pmod{5157437}.$$

input: inteiro n composto
output: um fator não trivial de n
passo 1.: $a = 2$, $i = 2$
passo 2.:

2.1. calcular
$a = a^i \pmod n$
$i = i + 1$

2.2. calcular
$d = \mathrm{m.d.c.}(a - 1, n)$

2.3. se $d = 1$, voltar ao passo **2.1.**

2.4. se $1 < d < n$, devolver o fator d.

2.5. se $d = n$, terminar sem sucesso.

exemplo. Consideremos, novamente, $n = 5157437$ e a sequência $r_1, r_2, r_3, \ldots$ determinada no exemplo anterior.

Temos que $\mathrm{m.d.c.}(r_k - 1, n) = 1$, para $k = 1, 2, \ldots, 8$, mas

$$\mathrm{m.d.c.}(r_9 - 1, n) = 2269.$$

Segue-se, assim, que 2269 é um fator de 5157437.

exemplo. Consideremos, agora, $n = 1403$. Tomando $r_1 = 2$, segue-se que

$$\begin{aligned}
& r_2 \equiv r_1^2 = 2^2 \equiv 4 \pmod{n}, \\
& \mathrm{m.d.c.}(3, n) = 1, \\
& r_3 \equiv r_2^3 = 4^3 \equiv 64 \pmod{n}, \\
& \mathrm{m.d.c.}(63, n) = 1, \\
& r_4 \equiv r_3^4 = 64^4 \equiv 142 \pmod{n}, \\
& \mathrm{m.d.c.}(141, n) = 1, \\
& r_5 \equiv r_4^5 = 142^5 \equiv 794 \pmod{n}, \\
& \mathrm{m.d.c.}(793, n) = 61.
\end{aligned}$$

Assim, 61 é um fator de 1403.