Aritmética

Fernando Martínez

Departament de Matemàtiques • Universitat Politècnica de Catalunya

2 de septiembre de 2022

Trabajaremos con enteros de tamaño arbitrario

643353183200092094287771675345221470010077629570715127404791684658292676146
258015596958199149307800248646412074806402713345405555081170237753105542354
684208619132518842723761824119200367033102378675040596360890232050015927575
092514853608500408281492709084825821114563373317007098338129291091372712149
614623307473988341465977307145752705448273512348134128938358986609643424139
880228535842593559221687695145242873591558628568048836430658763963628457559
544656711786049228438123628688782475462783972073491969055071501707972940833
772753016350946584992156170455681183858334172706286837128565378248759075309
162659580574430676771515129978897420613649359259526062256680143079870493073
398084497931098873418020976977974721325500443350148701944644764873813928657
096695060301865446376943751792046183219540156504462769309116980510428926960
863497599865711668561576864719822190421309237150056376914612222922525939922
046810299500313041779504422706733308439869413686737049578366809035296945443
953798010938544066680985820077138377974822115049336106352949077227851726631
333176196420428097177276681272065534315670606060953264744935518704733533552
192151247631322510337116144318115750922555584769639254837994316871502659521
941029235075453497312888953021303

www.fib.upc.edu 4096 bits, más de 1200 cifras decimales

Coste operaciones

n y m enteros, $n > m$.

Suma $n + m$

$\mathcal{O}(\log n)$

Producto $n \cdot m$

$\mathcal{O}(\log^2 n)$;
Karatsuba[a] $\mathcal{O}((\log n)^{\log_2 3})$;
Schönhage-Strassen $\mathcal{O}(\log n \ \log\log n \ \log\log\log n)$;
Integer multiplication in time $\mathcal{O}(\log n \ \log\log n)$ D, Harvey and J. van der Hoeven Annals of Mathematics, March 2021

---

[a] $N = a2^{t/2} + b, M = c2^{t/2} + d,$
$N \cdot M = ac2^t + (bc + ad)2^{t/2} + bd = ac2^t + (ac + bd - (a - b)(c - d))2^{t/2} + bd$

Divisibilidad

Diremos que $a \neq 0$ divide a b si existe q tal que $b = q\,a$. Si a divide a b escribiremos $a|b$.

Teorema división euclidiana

Sean $a, b \in \mathbb{Z}$, $b \geq 1$, entonces existen $q, r \in \mathbb{Z}$ tales que

$$a = q \cdot b + r \quad 0 \leq r < b.$$

q (cociente) y r (resto) son únicos.

Máximo común divisor

$d > 0$ es el máximo común divisor de a y $b \neq 0$ si:

1. $d|a$, $d|b$,
2. $\forall c$ tal que $c|a$ y $c|b$ entonces $c|d$.

Escribiremos $d = (a, b) = mcd(a, b) = gcd(a, b)$

Algoritmo extendido de Euclides

Identidad de Bezout

Dados a, b y (a,b) existen x e y tales que $ax + by = (a,b)$

Ensure: $a > b > 0$

procedure EXGCD(a,b)

$r_0 = a, r_1 = b$

$x_0 = 1, x_1 = 0$

$y_0 = 0, y_1 = 1$

$k = 1$

while $r_k \neq 0$ **do**

$r_{k-1} = q_k r_k + r_{k+1}, \quad 0 \leq r_{k+1} < r_k$

$x_{k+1} = x_{k-1} - q_k x_k$

$y_{k+1} = y_{k-1} - q_k y_k$

end while

return $(a,b) = r_{k-1}, x = x_{k-1}, y = y_{k-1}$ ▷ último resto no nulo

end procedure

Coste $\mathcal{O}(\log^2 n)$

Número primo

$p \geq 2$ es un número primo si solamente es divisible por ± 1 y $\pm p$.

$n \geq 2$ es compuesto si no es primo.

Teorema

Hay infinitos números primos.

Distribución números primos

Sea $\Pi(x)$ el # de números primos menores o iguales que x, entonces

$$\lim_{x \to \infty} \frac{\Pi(x)}{\frac{x}{\ln x}} = 1.$$

Teorema fundamental de la aritmética

Sea $n > 1$, entonces

$$n = \prod_i p_i^{\alpha_i},$$

p_i primo, $\alpha_i \geq 0$.

Función φ de Euler

a y b son relativamente primos o coprimos si (a, b)=1.

Sea $n > 0$, denotaremos por $\varphi(n)$ el número de enteros positivos menores o iguales que n y que son relativamente primos con n,

$$\varphi(n) = |\{1 \leq b \leq n : (b, n) = 1\}|$$

Propiedades:

$\varphi(1) = 1$.

$\varphi(p) = p - 1$, p primo.

$\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, p primo, $\alpha \geq 1$.

Si $(a, b) = 1$, $\varphi(a\,b) = \varphi(a)\,\varphi(b)$.

Si $n = \prod p_i^{\alpha_i}$, $\varphi(n) = \prod p_i^{\alpha_i - 1}(p_i - 1) = n \prod \left(1 - \frac{1}{p_i}\right)$.

Aritmética modular

Sea $n \geq 1$, a es congruente con b módulo n si $n|(a-b)$

$$a \equiv b \mod n.$$

Un conjunto de números enteros tales que cualquier entero es congruente módulo n con exactamente un elemento del conjunto recibe el nombre de conjunto completo de residuos módulo n.

$\mathbb{Z}_n$: cualquier conjunto completo de residuos módulo n.

$$\mathbb{Z}_n = \{0, 1, \ldots, n-2, n-1\} = \{1, 2, \ldots, n-1, n\}.$$

Coste suma módulo n (suma en $\mathbb{Z}_n$): $\mathcal{O}(\log n)$
Coste producto módulo n (producto en $\mathbb{Z}_n$): $\mathcal{O}(\log^2 n)$

Aritmética modular

Diremos que $a \in \mathbb{Z}_n$ es invertible si $\exists b \in \mathbb{Z}_n$ tal que $a\,b \equiv 1 \mod n$.

Teorema

$a \in \mathbb{Z}_n$ es invertible $\Leftrightarrow (a, n) = 1$.

Coste de cálculo de inversos módulo n usando el algoritmo extendido de Euclides: $\mathcal{O}(\log^2 n)$

$\mathbb{Z}_n^*$: Conjunto de los elementos invertibles de $\mathbb{Z}_n$.

Notemos que $|\mathbb{Z}_n^*| = \varphi(n)$.

Pequeño teorema de Fermat

Pequeño teorema de Fermat

Sea p primo, entonces:

1. $\forall a$ *tal que* $(p, a) = 1, \quad a^{p-1} \equiv 1 \mod p.$
2. $\forall a, \quad a^p \equiv a \mod p.$

Corolario

Si $(p, a) = 1$, p primo y $r \equiv s \mod p - 1$ entonces $a^r \equiv a^s \mod p$.

Teorema de Euler

Teorema de Euler

Si $(n, a) = 1$ entonces

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Corolario:

Si $(n, a) = 1$ y $r \equiv s \mod \varphi(n)$ entonces $a^r \equiv a^s \mod n$.

Observación: En las exponenciaciones modulares podemos suponer que el tamaño del exponente es menor que n.

Corolario:

Si $(n, a) = 1$ entonces $a^{-1} \equiv a^{\varphi(n)-1} \mod n$.

Exponenciación modular $a^e \mod n$[1]

Sea $e = e_r 2^r + \cdots + e_1 2 + e_0$, $e_i \in \{0, 1\}$, $e_r = 1$

procedure POWERMOD(a, e, n)
  $y \leftarrow 1$, $i \leftarrow r$
  while $i \geq 0$ **do**
    $y \leftarrow y^2 \mod n$ ▷ No es lo mismo elevar al cuadrado que multiplicar
    if $e_i = 1$ **then**
      $y \leftarrow y \cdot a \mod n$ ▷ No es lo mismo elevar al cuadrado que multiplicar
    end if
    $i \leftarrow i - 1$
  end while
  return y
end procedure

Coste de calcular $a^e \mod n$: $\mathcal{O}(\log^3 n)$

Coste de calcular $a^{-1} \equiv a^{\varphi(n)-1} \mod n$: $\mathcal{O}(\log^3 n)$

[1] La exponenciación de Montgomery es más eficiente.

Tereoma chino de los restos

Sean $n_1, \ldots, n_k \geq 1$ tales que $(n_i, n_j) = 1,\ i \neq j$. El sistema

$$\begin{aligned} x &\equiv a_1 \mod n_1 \\ &\vdots \\ x &\equiv a_k \mod n_k \end{aligned}$$

tiene una única solución módulo $n = n_1\, n_2 \ldots n_k$.

La solución es

$$\sum_i M_i L_i a_i \mod n$$

siendo $L_i = \frac{n}{n_i}$ y M_i el inverso de L_i módulo n_i.

Coste: $\mathcal{O}(\log^2 n)$