Matemáticas

Redigonda Maximiliano

Índice

Primos

Primos

El número 1 es una “unidad atómica” (indivisible), y todos los números naturales se pueden formar con él de forma única bajo la operación de suma.

Los números primos son una “unidad atómica” (indivisibles), y todos los números naturales se pueden formar con ellos de forma única bajo la operación producto.

Un número es **primo** si tiene exactamente dos divisores.

El 1 no es primo (rompe nuestro teorema, que por cierto se llama teorema fundamental de la aritmética).

Primos

No es sorpresa que gracias a tremendas propiedades aparezcan todo el tiempo en todos lados.

Ver ejemplos de representaciones de:

- 7
- 64
- 35
- 12

Primos

Cómo saber si un número es primo?

- Probar de 1 hasta n
- Mejor: probar desde 2 hasta n-1
- Mejor: probar desde 2 hasta sqrt(n) (inclusive)
- Mejor: probar solo con primos desde 2 hasta sqrt(n)

Primos

Cómo obtener los primeros números primos?

- Recorrer cada uno y verificar si es primo
- Utilizar una “criba de Eratóstenes”

Comparar complejidades.

Primos

Cómo obtener la **descomposición en primos** de un número?

- Recorrer hasta la raíz, O(sqrt(n))
- Otra “criba de Eratóstenes” O(log(n))

La primera es usable para números hasta 10^{12} o 10^{13}, pero la segunda es más rápida si los números están acotados.

Primos

Relaciones entre operaciones con la descomposición en primos de los números.

- Multiplicación
- División (y divisibilidad)
- Raíz cuadrada (y criterio para cuadrado perfecto)
- GCD (y como calcularlo)
- MCM
- Suma

Primos

Notas:

- Cantidad de divisores impar si y sólo si cuadrado perfecto.
- Hay infinitos.
- La cantidad de primos hasta n se puede aproximar como n/ln(n)
- Se puede verificar si un número es primo y obtener su factorización en primos incluso si el número es muy grande con Rabin-Miller y Pollard-Rho.

Aritmética Modular

Aritmética Modular - Introducción

Decimos que dos números a y b son congruentes módulo n si tienen el mismo resto en la división por n. En este caso notamos $a \equiv b \pmod{n}$.

Llamamos resto de a módulo n al número r entre 0 y n-1 tal que $a \equiv r \pmod{n}$.

Ejemplos:

$10 \equiv 0 \pmod{2}$ $10 \equiv 3 \pmod{7}$ $12 \equiv 12 \pmod{45}$ $0 \equiv 0 \pmod{37}$

$8 \equiv 3 \pmod{5}$ $100 \equiv 1 \pmod{9}$ $32 \equiv 2 \pmod{6}$ $9 \equiv 1 \pmod{2}$

Aritmética Modular - Introducción

La idea es trabajar con los restos de los números, en vez de con los números en sí.

Esto tiene algunas ventajas, una de las más claras, es trabajar en un rango acotado de números (si el módulo es n, se trabaja con números entre 0 y n-1).

En problemas de contar, muchas veces se nos pide la respuesta módulo un número primo grande, porque el número verdadero sería demasiado grande (se necesitaría bigint, y sería lento).

Aritmética Modular - Introducción

Uno pensaría que necesita contar la cantidad que le pide el problema, y luego tomar módulo del resultado, esto llevaría a trabajar con números muy grandes de todas formas.

Pero podemos trabajar con los restos en todas las operaciones intermedias!

Si $a + b \equiv r \pmod n$, entonces $(a \% n) + (b \% n) \equiv r \pmod n$
Si $a - b \equiv r \pmod n$, entonces $(a \% n) - (b \% n) \equiv r \pmod n$
Si $a \times b \equiv r \pmod n$, entonces $(a \% n) \times (b \% n) \equiv r \pmod n$

Las divisiones son otra historia.

Aritmética Modular - Potencia

Podemos elevar números a una potencia grande muy rápidamente con “exponenciación binaria”.

Si tenemos que calcular a^n lo obvio es hacer la multiplicación de los n términos e ir tomando los restos, esto es O(n).

Pero tenemos una mejor forma de obtener el mismo resultado! (pizarrón).

Esto es O(log n), lo que significa que el exponente puede tener un millón de dígitos, y aún nos tardaría menos de un segundo en calcular.

Aritmética Modular - Código Potencia

```
int expmod(int b, int e){
  if (e == 0) return 1;
  if (e == 1) return b;
  if (e % 2 == 1) return (long long) b * expmod(b, e - 1) % P;
  int k = expmod(b, e/2);
  Return (long long) k * k % P;
}
```

Se puede escribir iterativamente, y es recomendable.

Aritmética Modular - Consejos

Generalmente, para tener un código lindo, vamos a querer operar número módulo n usando funciones especiales.

Las definimos como add, subtract, mul, etc. Existen muchas formas de hacer esto, buscar una bonita y adoptarla como estándar del equipo.

Una vez que se tienen esas funciones, se asume que siempre se está trabajando con números entre 0 y n-1.

Aritmética Modular - División

Qué es dividir módulo n?

Podemos ver una división como una multiplicación por el “inverso”.

Para poder dividir entonces, necesitamos encontrar el inverso de un número.

El número a tiene cómo inverso a a^{-1} si la multiplicación $a \times a^{-1} \equiv 1 \pmod{n}$.

Este número no siempre existe (inverso de 2 módulo 6?), pero siempre existe cuando n es primo!

Aritmética Modular - División (Fermat)

En muchos casos, el módulo del problema va a ser un primo P (uno de los más comunes es 10^9+7).

Ahora, cómo encontramos este número inverso?

El teorema de Fermat dice que si P es primo y a no es 0, entonces $a^{p-1} \equiv 1 \pmod{p}$.

Esto significa que el número que estamos buscando es a^{p-2} (y ahora podemos encontrarlo rápido)! Ver ejemplos en el pizarrón.

Aritmética Modular - División

Y si el número no es primo?

Vimos que el inverso puede incluso no existir.

El inverso existe si y sólo si a (el número al que le quiero encontrar el inverso) y n (el número con el cual modulo) son **coprimos**.

Coprimos significa que no tienen primos en común.

Aritmética Modular - División

Existe una función llamada Phi, que cuenta la cantidad de enteros positivos hasta n que son coprimos con n.

Por ejemplo:

- Phi(5) = 4
- Phi(10) = 4
- Phi(41) = 40
- Phi(30) = 8

Aritmética Modular - División

Es claro que si P es primo, entonces Phi(P) = P - 1.

Vemos que Phi(P^k) = P^k - P^{k-1} (a la totalidad, le restamos los múltiplos de P, ya que si no son coprimos, el GCD es mayor que 1, y sólo puede ser múltiplo de P).

Phi de cualquier otro número sale usando que Phi es una **función multiplicativa**.

Una función F es multiplicativa si para n, m coprimos, entonces F(n x m) = F(n) x F(m).

Aritmética Modular - División

Volviendo, esta función Phi resulta útil para dividir en caso de que el módulo no sea primo.

Teorema de Euler (uno de los muchos):

Si a y n son coprimos, entonces $a^{Phi(n)} \equiv 1 \pmod{n}$

Es una generalización del Fermatito.

Combinatoria

Combinatoria - Factoriales

Cuántas formas tenemos de sentar 6 personas en una mesa?

Hay 6 lugares posibles, para la primera persona que vamos a sentar vamos a tener 6 posibilidades, luego quedarán 5 lugares para la segunda persona, luego 4, 3, 2, 1, BOOM.

Esto nos da un total de 6 x 5 x 4 x 3 x 2 x 1 = 720 formas.

Denotamos este número como “6!” y se lee “seis factorial”.

Estamos usando implícitamente la “regla del producto”, el principio fundamental del conteo.

Combinatoria - Coeficientes Binomiales

El coeficiente binomial “n tomado de k” nos da el número de formas en que podemos seleccionar un subconjunto de k elementos de uno con n elementos.

Por conjunto estamos hablando matemáticamente (el orden no importa).

N tomado de K = N-1 tomado de K-1 + N-1 tomado de K

Esta fórmula recursiva nos permite calcular los números combinatorios con una tabla (triángulo de pascal).

Combinatoria - Coeficientes Binomiales

Otras propiedades se cumplen como:

N tomado de K = N tomado de (N - K)

La suma de los coeficientes binomial desde N tomado de 0 hasta N tomado de N nos da 2^n (es decir, la cantidad de subconjuntos posibles de un conjunto).

Se pueden calcular también como N! / K! / (N - K)!

Combinatoria - Coeficientes Multinomiales

Cuántas palabras distintas podemos formar con ICPC? Y con MISSISSIPPI?

Si no hubiera repeticiones de letras, simplemente sería el factorial del tamaño de la cadena.

Pero tenemos ciertos grupos que se repiten, con lo que tenemos que dividir por la cantidad de formas órdenes de esos grupos.

Un coeficiente multinomial nos da la cantidad de formas en que n elementos pueden ser divididos en subconjuntos de tamaños k_1, k_2, ..., k_m cuya suma da n.

Combinatoria - Bolas y cajas

Tenemos N cajas, y queremos ubicar K bolas en ellas.

Si podemos poner a lo sumo una bola en cada caja, la cantidad de formas de ubicarlas es N tomado de K.

Si podemos poner más de una bola en cada caja, podemos representar esto como una cadena de texto con caracteres “o” y “m”.

La “o” significa poner una bola en la caja actual, y la “m” es moverse a la caja de la derecha. Ejemplos en el pizarrón.

Combinatoria - Bolas y cajas

Si tenemos N cajas, vamos a tener N-1 símbolos de “m”.

La solución es entonces N-1 + K tomado de K (o de N-1, es lo mismo).

Para calcular los coeficientes binomiales podemos usar la tabla o podemos usar factoriales e inversos modulares.

Combinatoria - #Divisores

Cuántos números podemos formar tal que su factorización en primos sea un subconjunto de la de N si $N = p_1^{e1} p_2^{e2} \ldots p_m^{em}$.

De cada factor primo p_i podemos tener 0, 1, 2, ..., e_i.

Es decir, tenemos $e_1 + 1$ formas para el primer factor primo, $e_2 + 1$ formas para el segundo, etc.

Esto nos da la cuenta: $(e_1 + 1)(e_2 + 1)\ldots(e_m + 1)$

Problemas

230B

Hay 3n gnomos (numerados de 0 a 3n-1) sentados en una mesa circular, cada uno tiene 1, 2 o 3 monedas.

Tanya estará contenta si hay 3 gnomos en las posiciones i, i + n, i + 2n, con i < n, la suma de sus monedas da distinto de 6.

Dado $n \leq 10^5$, contar la cantidad de configuraciones en las que Tanya estará contenta, módulo 10^9+7.

1062B

En el pizarrón hay escrito un número $n \leq 10^9$, y podemos aplicarle 0 o más operaciones del siguiente tipo:

- mul x, multiplicamos el número por x, un entero positivo arbitrario.
- sqrt, tomamos raíz cuadrada del número

Debemos obtener el menor número posible que podemos formar, y la mínima cantidad de operaciones que debemos aplicar para lograrlo.

1033D

Nos dan $n \leq 500$ enteros con 3, 4 o 5 divisores (cada uno $\leq 10^{18}$). Cuántos divisores tiene la multiplicación de todos ellos?

Leer

Recursos

- Aventuras Matemáticas (Cagliero, Tirao, Penazzi, Rossetti, Sustar).
  - Primos
  - Combinatoria
  - Aritmética Modular
- Guide to Competitive Programming (Laaksonen)
  - Mathematics