Teoría de números

MSc Edson Ticona Zegarra

Campamento de Programación

Contenido

Contenido

Problemas Adhoc

- Algunos problemas describen alguna forma de secuencia, fórmula o patrón, un abordaje directo usuamente termina en TLE

Problemas Adhoc

- Algunos problemas describen alguna forma de secuencia, fórmula o patrón, un abordaje directo usuamente termina en TLE
- Algunos problemas implican el manejo de números grandes, haciendo necesario uso de `long long` o `unsigned long long`

Problemas Adhoc

- Algunos problemas describen alguna forma de secuencia, fórmula o patrón, un abordaje directo usuamente termina en TLE
- Algunos problemas implican el manejo de números grandes, haciendo necesario uso de `long long` o `unsigned long long`
- Evitar el uso de `float` hasta el final, el error de representación se amplifica en cada operación

Contenido

Aritmética básica

- Si d es un divisor de a y de b, entonces se dice que d es un divisor común de a y b.

Aritmética básica

- Si d es un divisor de a y de b, entonces se dice que d es un divisor común de a y b.
- Si d es divisor de a y b, entonces d es divisor de $a+b$ y $a-b$

Aritmética básica

- Si d es un divisor de a y de b, entonces se dice que d es un divisor común de a y b.
- Si d es divisor de a y b, entonces d es divisor de $a+b$ y $a-b$
- En general, si d es divisor de a y b, entonces d es divisor de $ax+by$ para cualquier par de enteros x y y

Aritmética básica

- El *máximo común divisor* de a y b (gcd en inglés), es el divisor común mayor de a y b, cumpliendo las siguientes propiedades

Aritmética básica

- El *máximo común divisor* de a y b (gcd en inglés), es el divisor común mayor de a y b, cumpliendo las siguientes propiedades
  1. $gcd(a, b) = gcd(b, a)$

Aritmética básica

- El *máximo común divisor* de a y b (gcd en inglés), es el divisor común mayor de a y b, cumpliendo las siguientes propiedades
  1. $gcd(a, b) = gcd(b, a)$
  2. $gcd(a, b) = gcd(-a, b)$

Aritmética básica

- El *máximo común divisor* de a y b (gcd en inglés), es el divisor común mayor de a y b, cumpliendo las siguientes propiedades
  1. $gcd(a, b) = gcd(b, a)$
  2. $gcd(a, b) = gcd(-a, b)$
  3. $gcd(a, b) = gcd(|a|, |b|)$

Aritmética básica

- El *máximo común divisor* de a y b (gcd en inglés), es el divisor común mayor de a y b, cumpliendo las siguientes propiedades
  1. $gcd(a, b) = gcd(b, a)$
  2. $gcd(a, b) = gcd(-a, b)$
  3. $gcd(a, b) = gcd(|a|, |b|)$
  4. $gcd(a, 0) = |a|$

Aritmética básica

- El *máximo común divisor* de a y b (gcd en inglés), es el divisor común mayor de a y b, cumpliendo las siguientes propiedades
  1. $gcd(a, b) = gcd(b, a)$
  2. $gcd(a, b) = gcd(-a, b)$
  3. $gcd(a, b) = gcd(|a|, |b|)$
  4. $gcd(a, 0) = |a|$
  5. $gcd(a, ka) = |a|$

Aritmética básica

- El *máximo común divisor* de a y b (gcd en inglés), es el divisor común mayor de a y b, cumpliendo las siguientes propiedades
  1. $gcd(a, b) = gcd(b, a)$
  2. $gcd(a, b) = gcd(-a, b)$
  3. $gcd(a, b) = gcd(|a|, |b|)$
  4. $gcd(a, 0) = |a|$
  5. $gcd(a, ka) = |a|$
- Para calcular rápidamente el *gcd* usamos el algoritmo de Euclides: $gcd(a, b) = gcd(b, a \mod b)$

Aritmética básica

- El *máximo común divisor* de a y b (gcd en inglés), es el divisor común mayor de a y b, cumpliendo las siguientes propiedades
  1. $gcd(a, b) = gcd(b, a)$
  2. $gcd(a, b) = gcd(-a, b)$
  3. $gcd(a, b) = gcd(|a|, |b|)$
  4. $gcd(a, 0) = |a|$
  5. $gcd(a, ka) = |a|$
- Para calcular rápidamente el *gcd* usamos el algoritmo de Euclides: $gcd(a, b) = gcd(b, a \mod b)$
- El *mínimo común múltiplo*, (lcm en inglés) puede ser calculado a partir del gcd: $lcm(a, b) = a * b / gcd(a, b)$

Números primos

- Se dice que un número es *primo* si tiene como divisores al 1 y a sí mismo.

Números primos

- Se dice que un número es *primo* si tiene como divisores al 1 y a sí mismo.
- Se dice que un par de números son *primos entre sí* si tiene como único divisor común al 1, es decir, $gcd(a, b) = 1$

Teorema fundamental de la aritmética

- Todo número puede ser descompuesto como el producto de sus factores primos

Teorema fundamental de la aritmética

- Todo número puede ser descompuesto como el producto de sus factores primos
- Tal representación se le conoce como *representación canónica*

Teorema fundamental de la aritmética

- Todo número puede ser descompuesto como el producto de sus factores primos
- Tal representación se le conoce como *representación canónica*
- $\forall n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... p_k^{\alpha_k}$

Criba de Eratóstenes

input : Entero n
$sieve \leftarrow$ arreglo de tamaño n;
for $p \leftarrow 2$ **to** $\sqrt{n}$ **do**
  if $sieve[p] = \mathtt{false}$ **then**
    for $i \leftarrow p^2$ **to** n p **do**
      $sieve[i] \leftarrow \mathtt{true}$;
    end
  end
end

Contenido

Aritmética modular

- Consideramos la operación de módulo, también conocida como *suma cerrada*, como una suma sobre un conjunto finito

Aritmética modular

- Consideramos la operación de módulo, también conocida como *suma cerrada*, como una suma sobre un conjunto finito
- Una forma útil de pensar en la operación de módulo, es como un reloj tal que al sumar 4 horas a 22, se pasa a 2 horas y no a 26.

Aritmética modular

- Consideramos la operación de módulo, también conocida como *suma cerrada*, como una suma sobre un conjunto finito
- Una forma útil de pensar en la operación de módulo, es como un reloj tal que al sumar 4 horas a 22, se pasa a 2 horas y no a 26.
- Lo anterior lo podemos expresar: $(22 + 4) \mod 24 = 2$

Aritmética modular

- Propiedades de la operación módulo

Aritmética modular

- Propiedades de la operación módulo
  1. $(a+b) \mod m = ((a \mod m) + (b \mod m)) \mod m$

Aritmética modular

- Propiedades de la operación módulo
  1. $(a+b) \mod m = ((a \mod m) + (b \mod m)) \mod m$
  2. $(a-b) \mod m = ((a \mod m) - (b \mod m)) \mod m$

Aritmética modular

- Propiedades de la operación módulo
  1. $(a + b) \mod m = ((a \mod m) + (b \mod m)) \mod m$
  2. $(a - b) \mod m = ((a \mod m) - (b \mod m)) \mod m$
  3. $(a * b) \mod m = ((a \mod m) * (b \mod m)) \mod m$

Aritmética modular

- Propiedades de la operación módulo
  1. $(a + b) \mod m = ((a \mod m) + (b \mod m)) \mod m$
  2. $(a - b) \mod m = ((a \mod m) - (b \mod m)) \mod m$
  3. $(a * b) \mod m = ((a \mod m) * (b \mod m)) \mod m$