Lecture 7
Number Theory

Euiseong Seo
(euiseong@skku.edu)
Number Theory

- God created the integers. All else is the work of man – Leopold Kronecker
- Study of the property of the integers
  - Specifically, integer divisibility
  - Full of beautiful proofs and surprising results
- b divides a
  - b|a
  - a = bk for some integer k
  - b is a divisor of a
  - a is a multiple of b
Prime Numbers

- **Prime Numbers**
  - integers $p > 1$ which are only divisible by 1 and itself
  - if $p$ is a prime number, then $p = a \times b$ for integers $a \leq b$ implies that $a = 1$ and $b = p$

- **Fundamental theorem of arithmetic**
  - Every integer can be expressed in only one way as the product of primes
  - Examples
    - $105 = 3 \times 5 \times 7$
    - $32 = 2 \times 2 \times 2 \times 2 \times 2$
  - Prime factorization

- **Any number which is not prime is a composite**
Primality Testing and Factorization

- There are an infinite number of primes (Euclid’s proof)
- $x / \ln x$ number of primes that are less than or equal to $x$
- The smallest prime factor of $n$ is at most $\sqrt{n}$ unless $n$ is a prime
Constructing All Divisors

- Every divisor is the product of some subset of these prime factors
- Such subsets can be constructed using backtracking techniques
  - Be careful about duplicate prime factors
  - 12 has three terms but has only six divisors
Greatest Common Divisor

- Largest divisor shared by a given pair of integers
- Used to obtain the reduced form of a fraction
- Euclid’s GCD algorithms
  - If $b|a$, then $\gcd(a,b) = b$
  - If $a = bt + r$ for integers $t$ and $r$, then $\gcd(a,b) = \gcd(b,r)$
- $ax + by = \gcd(a,b)$
Greatest Common Divisor

/* Find the gcd(p,q) and x,y such that p*x + q*y = gcd(p,q) */

long gcd(long p, long q, long *x, long *y)
{
    long x1, y1; /* previous coefficients */
    long g; /* value of gcd(p,q) */

    if (q > p) return(gcd(q,p,y,x));

    if (q == 0) {
        *x = 1;
        *y = 0;
        return(p);
    }

    g = gcd(q, p%q, &x1, &y1);

    *x = y1;
    *y = (x1 - floor(p/q)*y1);

    return(g);
}
Least Common Multiple

- The smallest integer which is divided by both of a given pair of integers
- \( \text{lcm}(x,y) = \frac{xy}{\gcd(x,y)} \)
Modular Arithmetic

- What day of the week will your birthday fall on next year?
- Modular arithmetic
  - modulus
  - residue

\[(x+y) \mod n = ((x \mod n) + (y \mod n)) \mod n\]

\[(12 \mod 100) - (53 \mod 100) = -41 \mod 100 = 59 \mod 100\]

\[xy \mod n = (x \mod n)(y \mod n) \mod n\]

\[x^y \mod n = (x \mod n)^y \mod n\]
Modular Arithmetic

- Finding the last digit – What is the last digit of $2^{100}$?
Light, More Light

There is man named Mabu who switches on-off the lights along a corridor at our university. Every bulb has its own toggle switch that changes the state of the light. If the light is off, pressing the switch turns it on. Pressing it again will turn it off. Initially each bulb is off.

He does a peculiar thing. If there are \( n \) bulbs in a corridor, he walks along the corridor back and forth \( n \) times. On the \( i \)th walk, he toggles only the switches whose position is divisible by \( i \). He does not press any switch when coming back to his initial position. The \( i \)th walk is defined as going down the corridor (doing his peculiar thing) and coming back again. Determine the final state of the last bulb. Is it on or off?

Input

The input will be an integer indicating the \( n \)th bulb in a corridor, which is less than or equal to \( 2^{32} - 1 \). A zero indicates the end of input and should not be processed.

Output

Output “yes” or “no” to indicate if the light is on, with each case appearing on its own line.
Light, More Light

Sample Input

3
6241
8191
0

Sample Output

no
yes
no

There is a man named Mabu who switches on-off the lights along a corridor at our university. Every bulb has its own toggle switch that changes the state of the light. If the light is off, pressing the switch turns it on. Pressing it again will turn it off. Initially each bulb is off.

He does a peculiar thing. If there are $n$ bulbs in a corridor, he walks along the corridor back and forth $n$ times. On the $i$th walk, he toggles only the switches whose position is divisible by $i$. He does not press any switch when coming back to his initial position. The $i$th walk is defined as going down the corridor (doing his peculiar thing) and coming back again. Determine the final state of the last bulb. Is it on or off?

Input

The input will be an integer indicating the $n$th bulb in a corridor, which is less than or equal to $2^{32} - 1$. A zero indicates the end of input and should not be processed.

Output

Output "yes" or "no" to indicate if the light is on, with each case appearing on its own line.

Sample Input

3
6241
8191
0

Sample Output

no
yes
no

Light, More Light
The factorial function, $n!$, is defined as follows for all non-negative integers $n$:

$$\begin{align*}
0! & = 1 \\
n! & = n \times (n - 1)! \quad (n > 0)
\end{align*}$$

We say that $a$ divides $b$ if there exists an integer $k$ such that

$$k \times a = b$$

**Input**

The input to your program consists of several lines, each containing two non-negative integers, $n$ and $m$, both less than $2^{31}$.

**Output**

For each input line, output a line stating whether or not $m$ divides $n!$, in the format shown below.
Factovisors

Sample Input

6 9
6 27
20 10000
20 100000
1000 1009

Sample Output

9 divides 6!
27 does not divide 6!
10000 divides 20!
100000 does not divide 20!
1009 does not divide 1000!