Linear diophantine equations:

$$3x + 5y = 2$$

$$3x \equiv 2 \bmod 5 \iff x \equiv 4 \bmod 5$$

$x = 4 \quad y = -2$

$ax + by = c$, where a, b, c are integers.

All solutions to this eq^n.

$ax + by = c$ $\boxed{\gcd(a,b) = 1}$

$\Rightarrow\ ax \equiv c \mod b.$

$\Leftrightarrow\ \boxed{x \equiv a^{-1} c \mod b}$ $y = \boxed{\dfrac{c - ax}{b}}$

how to compute it ?

$3x + 5y = 2$

$3x \equiv 2 \mod 5$

$\boxed{x \equiv 4 \mod 5}$

$x = 5t + 4$

$y = \dfrac{2 - 3(5t+4)}{5} = \boxed{-3t - 2}$

$(5t+4, -3t-2) \quad t \in \mathbb{Z}$

$(4, -2)$
$+5 \quad -3$

$(4,-2) + (5t, -3t)$

$$\gcd(a,b) \neq 1$$
$$\underset{g}{\parallel}$$

$$ax + by = c$$

$$g \mid \underline{a}x \qquad g \mid \underline{b}y \implies g \mid c$$

$$4x + 6y = 5 \quad \times$$ no solutions.

$$\frac{a}{g}x + \frac{b}{g}y = \frac{c}{g}$$

$$\gcd(a/g, b/g) = 1$$

Q) How to find $a^{-1} \bmod b$?

Euclidean algorithm

Fast, # iterations, $O(\log(\min(a,b)))$.

e.g. → $a=5, b=7$

Idea: To find integers m,n such that $5m + 7n = 1$

$$5m \equiv 1 \bmod 7$$

$$m \equiv 5^{-1} \bmod 7$$

$$7 = 1 \times 5 + 2$$

$$5 = 2 \times 2 + 1$$

$$\begin{aligned} 1 &= 5 + (-2) \times 2 \\ &= 5 + (-2)(7-5) \\ &= 3 \times 5 + (-2) \times 7 \end{aligned}$$

$a^{-1} \bmod p.$ $\quad \gcd(a,p)=1$

prime p: Fermat's Theorem

$$a^{p-1} \equiv 1 \bmod p$$

$$\Rightarrow a \cdot a^{p-2} \equiv 1 \bmod p.$$

$$\Rightarrow a^{p-2} \equiv a^{-1} \bmod p.$$

exponentiation, fast.

$a^{-1} \bmod b.$ Euler's Theorem

$\phi(b)=$ number of +ve integers in $\{1,2,\dots,b\}$ which are coprime to b.

Not fast to compute.

$$a^{\phi(b)} \equiv 1 \bmod b.$$

$$a^{-1} \equiv a^{\phi(b)-1} \bmod b$$

Problem Statement

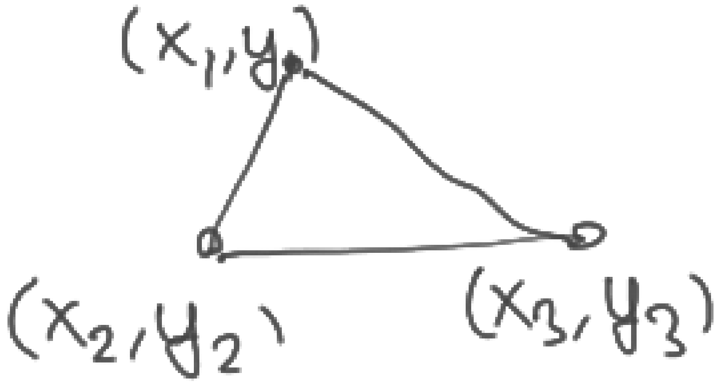
You are given integers X and Y, which satisfy at least one of $X \neq 0$ and $Y \neq 0$.

Find a pair of integers (A, B) that satisfies all of the following conditions. If no such pair exists, report so.

- $-10^{18} \leq A, B \leq 10^{18}$
- The area of the triangle with vertices at points $(0, 0), (X, Y), (A, B)$ on the xy-plane is 1.

Constraints

- $-10^{17} \leq X, Y \leq 10^{17}$
- $(X, Y) \neq (0, 0)$
- X and Y are integers.



$$\frac{1}{2}\left|\cancel{x_1}^{\,0}(y_2-y_3)+x_2(y_3-y_1)+x_3(y_1-y_2)\right|$$

$$=\frac{1}{2}\left|XB-AY\right|$$

$\gcd(X,Y) \mid 2$

$X=4 \quad Y=6$

$(A,B)=(1+2t,\ 2+3t)$

$\underline{BX-AY}=2 \longrightarrow 2B-3A=1$

$BX-AY=-2$

Euler Totient Function.

$\phi(n)$: number of integers $a \in \{1, 2, \ldots, n\}$ such that $\gcd(a, n) = 1$.

$n \in \mathbb{N}$

$\phi(6) = 2$ 1, 2, 3, 4, 5, 6

$\phi(p) = p - 1$ 1, 2, ..., $p-1$, p

m, n : coprime : $\boxed{\phi(m)\phi(n) = \phi(mn)}$

$m=3 \qquad n=4$

$a \equiv \boxed{1 \bmod 3} \quad a \equiv 2 \bmod 4$

$a \equiv 10 \bmod 12$

$a = \boxed{3t+1} \qquad \boxed{3t \equiv 1 \bmod 4}$

$t \equiv 3 \bmod 4$

$t = 4k+3$

$a \equiv 12k+10$

$t \equiv -3t \equiv -1 \equiv 3$

$x \equiv 2 \bmod 3 \quad x \equiv 1 \bmod 4$

$\Updownarrow$

$x \equiv 5 \bmod 12$

~~$x \equiv 2 \bmod 3$ & $x \equiv 1 \bmod 4$~~ $\quad x \equiv 5 \bmod 12$

coprime m, n

$$\left.\begin{array}{l} x \equiv \underline{a} \bmod m \\ x \equiv \underline{b} \bmod n \end{array}\right. \Longleftrightarrow x \equiv c \bmod mn$$

Chinese Remainder Theorem.

Let m, n be coprime naturals, and let $a, b \in \mathbb{Z}$.

Then $\exists$ a unique (mod mn) integer c such that

$$\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases} \iff x \equiv c \bmod mn.$$

$m \times n$ "possibilities"

mn possibilities.

$\rightarrow$ More general statements hold.

$$\overset{a}{\underline{\phi(m)}}\,\overset{b}{\phi(n)} = \overset{c}{\phi(mn)}.$$

Number of integers $a \in \{1, \ldots, m\}$
$b \in \{1, \ldots, n\}$

s.t.

$\underline{\gcd(a,m)} = 1$

and $\underline{\gcd(b,n)} = 1$

$$\begin{aligned} x &\equiv a \bmod \underline{m} \\ x &\equiv b \bmod \underline{n} \end{aligned} \iff x \equiv c \bmod mn$$

$\gcd(x, mn) = 1$

For every a coprime to m, b coprime to n, the corresponding "c" in CRT is coprime to mn.

$$\phi(mn) = \phi(m)\,\phi(n)$$

$$\underline{n} = \underline{p_1}^{a_1}\,\underline{p_2}^{a_2} \cdots \underline{p_k}^{a_k}$$

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

Q) Find $\phi(1), \underline{\underline{\phi(2), \ldots,}}\ \phi(n)$. Can we do this faster?

Q) Compute $\phi(1), \phi(2), \ldots, \phi(n)$.

Time: $O(n \log\log n)$.

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

→ For any prime $p \mid n$, we want to multiply $1-\frac{1}{p}$ to its corresponding ϕ.

$A[1] = 1$

$A[2] = 2 \times \left(1-\frac{1}{2}\right)$

$A[3] = 3 \times \left(1-\frac{1}{3}\right)$

$A[4] = 4 \times \left(1-\frac{1}{2}\right)$

$A[5] = 5 \times \left(1-\frac{1}{5}\right)$

$A[6] = 6 \times \left(1-\frac{1}{2}\right) \times \left(1-\frac{1}{3}\right)$

$$n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

$A[1] = 1$

$\boxed{A[2] = 2} \times \left(1 - \frac{1}{2}\right)$

$A[3] = 3 \times \left(1 - \frac{1}{3}\right)$

$A[4] = 4 \times \left(1 - \frac{1}{2}\right)$

$A[5] = 5 \times \left(1 - \frac{1}{5}\right)$

$A[6] = 6 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right)$

$A[7] = 7 \times \left(1 - \frac{1}{7}\right)$

$A[8] = 8 \times \left(1 - \frac{1}{2}\right)$

$\vdots$

$A[n] = n$

"Sieve" method to find primes

$$\phi(n) = n \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

Time complexity : $p < n$

$$O(n) + \frac{n}{2} + \frac{n}{3} + \frac{n}{5} + \frac{n}{7} + \dots + \frac{n}{p}$$

$$= \Theta(n \log \log n).$$

$n/1 + n/2 + n/3 + \dots$

Today Pari and Arya are playing a game called Remainders.

Pari chooses two positive integer x and k, and tells Arya k but not x. ~~Arya have to find the value~~ $x \mod k$. There are n ancient numbers $c_1, c_2, ..., c_n$ and Pari has to tell Arya $x \mod c_i$ if Arya wants. Given k and the ancient values, tell us if Arya has a winning strategy independent of value of x or not. Formally, is it true that Arya can understand ~~the value~~ $x \mod k$ for any positive integer x?

Note, that $x \mod y$ means the remainder of x after dividing it by y.

Input

The first line of the input contains two integers n and k ($1 \le n, \ k \le 1\,000\,000$) — the number of ancient integers and value k that is chosen by Pari.

$k \mid \mathrm{lcm}(c_1, .., c_n)$

The second line contains n integers $c_1, c_2, ..., c_n$ ($1 \le c_i \le 1\,000\,000$).

Output

Print "Yes" (without quotes) if Arya has a winning strategy independent of value of x, or "No" (without quotes) otherwise.

CRT

what is known?

$$\left.\begin{array}{l} x \equiv a_1 \bmod c_1 \\ x \equiv a_2 \bmod c_2 \\ \vdots \\ x \equiv a_n \bmod c_n \end{array}\right\} \Longleftrightarrow \boxed{x \equiv a \bmod \mathrm{lcm}(c_1, \ldots, c_n)} \text{ for some } a.$$

AND we know k.

$$\Downarrow$$

$$\boxed{k \mid \mathrm{lcm}(c_1, \ldots, c_n)}$$

$x \equiv 6 \bmod 8$

$\Downarrow$

$x \equiv \cancel{2}\, 6 \bmod 4$

$\Downarrow$

$x \equiv 0 \bmod 2$

CRT

$m_1, m_2, \dots, m_T$: +ve integers, not necessarily coprime.

$a_1, \dots a_T \in \mathbb{Z}$

$$\left.\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \\ x &\equiv a_T \bmod m_T \end{aligned}\right\}$$

→ either has NO solutions

→ equivalent to

$x \equiv c \bmod \operatorname{lcm}(m_1, m_2, \dots, m_T)$.

for some c.

e.g. →

$x \equiv 2 \bmod 4$: $x = 4t+2$

$x \equiv 4 \bmod 6$

$4t+2 \equiv 4 \bmod 6$

$\Leftrightarrow 4t \equiv 2 \bmod 6$

$\Leftrightarrow 6 \mid 4t-2$

$\Leftrightarrow 3 \mid 2t-1$

$\Leftrightarrow 2t \equiv 1 \bmod 3$

$\Leftrightarrow t \equiv 2 \bmod 3$ $t = 3k+2$

$6 \mid 4t-8$

$x \equiv 10 \bmod 12$.

The Farey sequence of order n is the sequence of completely reduced fractions between 0 and 1 which, when in lowest terms, have denominators less than or equal to n, arranged in ascending order. Farey sequence for different values of n are shown in the figure on the left below:

$$F_1 = \{\tfrac{0}{1}, \tfrac{1}{1}\}$$

$$F_4 = \{\tfrac{0}{1}, \tfrac{1}{4}, \tfrac{1}{3}, \tfrac{1}{2}, \tfrac{2}{3}, \tfrac{3}{4}, \tfrac{1}{1}\}$$

$$F_7 = \{\tfrac{0}{1}, \tfrac{1}{7}, \tfrac{1}{6}, \tfrac{1}{5}, \tfrac{1}{4}, \tfrac{2}{7}, \tfrac{1}{3}, \tfrac{2}{5}, \tfrac{3}{7}, \tfrac{1}{2}, \tfrac{4}{7}, \tfrac{3}{5}, \tfrac{2}{3}, \tfrac{5}{7}, \tfrac{3}{4}, \tfrac{4}{5}, \tfrac{5}{6}, \tfrac{6}{7}, \tfrac{1}{1}\}$$

Figure 1:

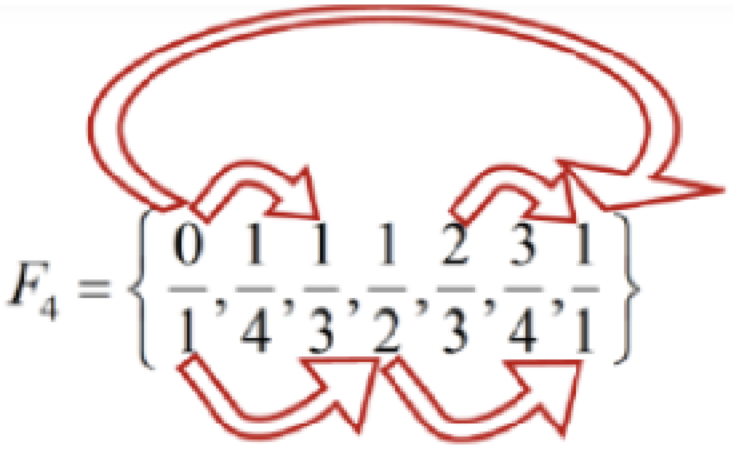


Figure 2: Five desired pairs in F4

It is very well known that if $\frac{m_1}{n_1}$ and $\frac{m_2}{n_2}$ and are two consecutive fractions of a Farey Sequence then $m_2n_1 - m_1n_2 = 1$. But many fractions which are not consecutive also show this property. For example, in F_7, $\frac{2}{5}$ and $\frac{1}{2}$ also show this property although they are not consecutive fractions in F_7. Given the value of n, your job is to find number of pair of non-consecutive fractions $\frac{m_i}{n_i}$ and $\frac{m_j}{n_j}$, such that $m_jn_i - m_in_j = 1$.

Input

Input file contains at most 20000 lines of input. Each line contains a positive integer which denotes the value of n ($0 < n < 1000001$). Input is terminated by a line containing a single zero. This line should not be processed.

Output

For each line of input produce one line of output. This line contains number of pair of non-consecutive fractions $\frac{m_i}{n_i}$ and $\frac{m_j}{n_j}$, ($j - i > 1$) in Farey Series F_n, such that $m_jn_i - m_in_j = 1$.

$F_2 : \frac{0}{1}, \frac{1}{2}, \frac{1}{1}$

$F_3 : \frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$

$F_4 : \frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}$

F_{n+1} : $\quad 1/n+1$

F_n : $\frac{0}{1}, \frac{1}{n}, \ldots\ldots, \quad \frac{1}{2}, \; - - - - , \; \frac{n-1}{n}, \frac{1}{1}$

$F_{n+1} \setminus F_n$: fractions with denominator $\frac{a}{n+1}$, $\gcd(a, n+1) = 1$

$\phi(n+1)$ "new" fractions.

each new added fraction creates two non-consec fractions satisfying (*).

output

$F_1 : \left\langle \frac{0}{1}, \frac{1}{1} \right\rangle$: 0.

$F_2 : \left\langle \frac{0}{1}, \frac{1}{2}, \frac{1}{1} \right\rangle$: 1

$F_3 : \left\langle \frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1} \right\rangle$: $1+2$

$F_4 : \left\langle \frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1} \right\rangle$: $1+2+2$

F_n : $\boxed{\phi(2)+\phi(3)+\phi(4)+\dots+\phi(n)}$

(*)

$\frac{m}{n}, \frac{p}{q}$ $\quad qm - pn = 1$

1) compute $\phi(1), \phi(2), \ldots, \phi(N)$ $\qquad O(N \log\log N)$

2) compute $\phi(2), \phi(2)+\phi(3),$

A: $\phi(2)+\phi(3)+\phi(4), \ldots, \sum_{i=2}^{N} \phi(i)$ $\qquad O(N)$

3) For each test case n, output A[n] $\qquad O(T)$

$$O(T + N \log\log N)$$