MRPTest. Тест Миллера - Рабина

Имя входного файла: `mrptest.in`
Имя выходного файла: `mrptest.out`

Пусть n — нечётное число вида $n = 2^k \cdot m + 1$, где $k \geq 1$ и m нечётно. Число a $(0 < a < n)$ называется *свидетелем* того, что число n является составным в тесте Миллера-Рабина если выполнено хотя бы одно из двух условий:

- $a^{n-1} \not\equiv 1 \pmod{n}$;
- существует u, такое что $0 \leqslant u < k$, $a^{2^u m} \not\equiv \pm 1 \pmod{n}$ и $a^{2^{u+1} m} \equiv 1 \pmod{n}$.

Дано два натуральных числа a и n. Требуется определить, является ли число a свидетелем того, что число n составное в тесте Миллера-Рабина.

Формат входного файла

Первая строка входного файла содержит нечётное число n $(2 \leqslant n \leqslant 10^{100})$, вторая строка содержит число a $(0 < a < n)$. Числа заданы в десятичной системе счисления без ведущих нулей.

Формат выходного файла

Выведите «YES» если число a является свидетелем того, что n составное и «NO» в противном случае.

Примеры

mrptest.in	mrptest.out
239 37	NO
561 400	YES
561 50	NO
101 81	NO
12345 5432	YES
586966732105622739705827 2	YES

SSPTest. Тест Соловея-Штрассена

Имя входного файла: `ssptest.in`
Имя выходного файла: `ssptest.out`

Пусть n — нечётное число. Число a $(0 < a < n)$ называется *свидетелем* того, что число n является составным в тесте Соловея-Штрассена если выполнено хотя бя одно из двух условий:

- $gcd(a, n) \neq 1$
- $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$

Дано два натуральных числа a и n. Требуется определить, является ли число a свидетелем того, что число n составное в тесте Соловея-Штрассена.

Формат входного файла

Первая строка входного файла содержит число n $(2 \leqslant n \leqslant 10^{100})$, вторая строка содержит число a $(0 < a < n)$. Числа заданы в десятичной системе счисления без ведущих нулей.

Формат выходного файла

Выведите «YES» если число a является свидетелем того, что n составное и «NO» в противном случае.

Примеры

ssptest.in	ssptest.out
239 37	NO
561 400	NO
561 50	NO
101 81	NO
12345 5432	YES
586966732105622739705827 2	YES