#include <iostream>

#define ull unsigned long long

using namespace std;

// x^y를 mod로 나눈 나머지를 반환하는 함수

ull Power(ull x, ull y, ull mod) {

    ull ret = 1;

    x %= mod;

    while (y) {

        if (y % 2 == 1)

            ret = (ret \* x) % mod;

        y /= 2;

        x = (x \* x) % mod;

    }

    return ret;

}

// Miller-Rabin 소수 판별 알고리즘을 위한 보조 함수

// a가 n의 소수 여부를 확인하는 함수

bool isPrime(ull n, ull a) {

    if (a % n == 0)

        return true;

    ull k = n - 1;

    while (1) {

        ull temp = Power(a, k, n);

        if (temp == n - 1)

            return true;

        if (k % 2 == 1)

            return (temp == 1 || temp == n - 1);

        k /= 2;

    }

}

// Miller-Rabin 소수 판별 알고리즘을 구현하는 함수

// n을 k번 테스트하여 소수 여부를 확인

bool millerRabin(ull n, int k) {

    if (n <= 1)

        return false;

    if (n == 2 || n == 3)

        return true;

    if (n % 2 == 0)

        return false;

    ull d = n - 1;

    while (d % 2 == 0)

        d /= 2;

    // 테스트를 k번 반복

    for (int i = 0; i < k; i++) {

        ull a = rand() % (n - 3) + 2; // 2부터 n-2 사이의 난수 생성

        if (!isPrime(n, a))

            return false;

    }

    return true;

}

int main() {

    ull n;

    cin >> n;

    // Miller-Rabin 소수 판별 알고리즘을 이용하여 n이 소수인지 판별

    if (millerRabin(n, 5)) { // 테스트 반복 횟수를 조절할 수 있음

        cout << "1\n"; // 소수인 경우

    } else {

        cout << "0\n"; // 소수가 아닌 경우

    }

    return 0;

}

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명