

Composite number

判断给定的数是否是一个合数

每一个大于1的整数若不是质数，就会是合数。所以问题可以转换为求一个数是否是一个质数

Fermat's little theorem (费马小定理)

如果 p 是一个质数，那么对于每一个 a ($1 < a < p - 1$)，都有 $a^{(p-1)} \% p = 1$ 即 $a^{(p-1)} \equiv 1 \pmod{p}$

```
// C++program to find the smallest twin in given range
#include <bits/stdc++.h>

using namespace std;

bool power(int a, int p) {
    return ((int)pow(a, p - 1) % p) == 1;
}

bool isPrime(unsigned int n, int k) {
    // Corner cases
    if (n <= 1 || n == 4) return false;
    if (n <= 3) return true;

    // Try k times
    while (k > 0) {
        // Pick a random number in [2..n-2]
        // Above corner cases make sure that n > 4
        int a = 2 + random() % (n - 4);

        // Fermat's little theorem
        if (power(a, n) != 1)
            return false;

        k--;
    }

    return true;
}

// Driver Program to test above function
int main() {
    int k = 3;
    isPrime(11, k) ? cout << " true\n" : cout << " false\n";
    isPrime(15, k) ? cout << " true\n" : cout << " false\n";
}
```

```
    return 0;  
}
```

质数一定满足费马小定理，但是存在不是质数同样满足费马小定理的数，这种数被称为 **Carmichael numbers** 所以费马小定理只能保证大概率上是一个质数