algorithm template

zinan.xu.dev@gmail.com

December 19, 2025

Contents

数论

素性检测

```cpp
#include<vector>
namespace PrimeTest {
    long long mul(long long a, long long b, long long mod){
        return (__int128) a * b % mod;
    }

    long long Pow(long long a, long long b, long long mod){
        //mod <= 10^18.
        long long res = 1;
        while(b){
            if (b&1) res = mul(res, a, mod);
            b >>= 1;
            a = mul(a, a, mod);
        }
        return res;
    }

    std::vector<long long> pr = {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31,
    ↪  37};

    bool rabin_test(long long a, long long n, long long s, long long d){
        long long u = Pow(a, d, n);
        if (u == 1 or u == n - 1) return false;

        for(long long i = 1; i < s; i++){
            u = mul(u, u, n);
            if (u == n - 1) return false;
        }
        return true;
    }

    bool rabin_miller(long long n){
        if (n < 2) return false;
        if (n % 2 == 0) return n==2;
        long long res = 1;
        long  s = 0, d = n-1;
        while(d%2==0) {
            s++;
            d>>=1;
        }

```

```
41          for(long long i = 0;i<pr.size();i++){
42              if (n%pr[i] == 0) {
43                  return n == pr[i];
44              }
45              if (rabin_test(pr[i], n, s, d)){
46                  return false;
47              }
48          }
49          return true;
50      }
51  }
```