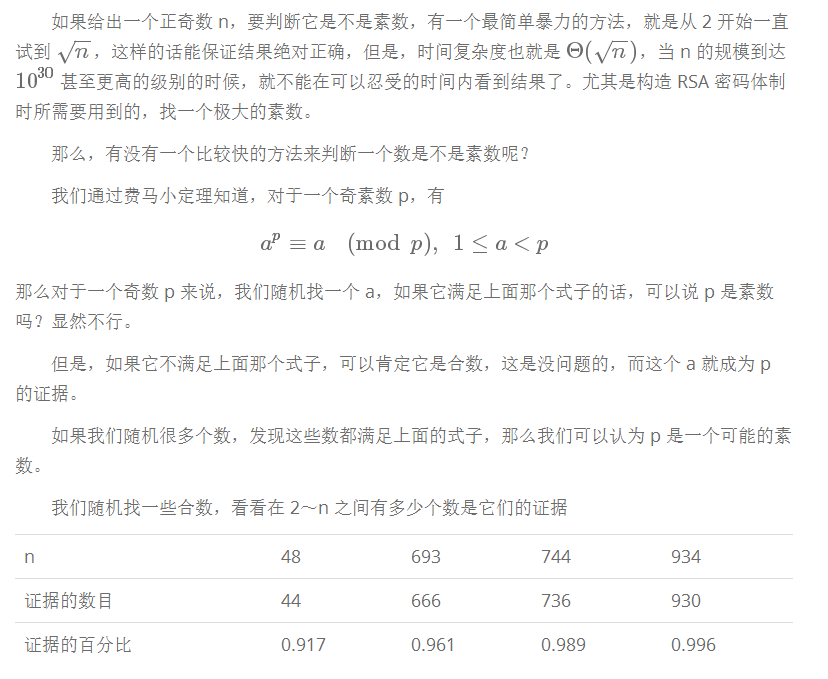
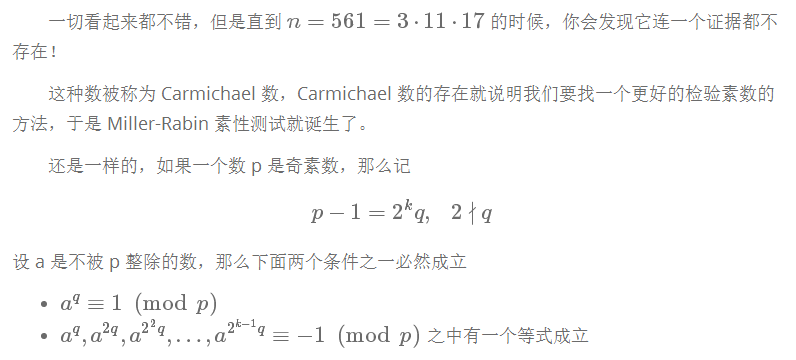
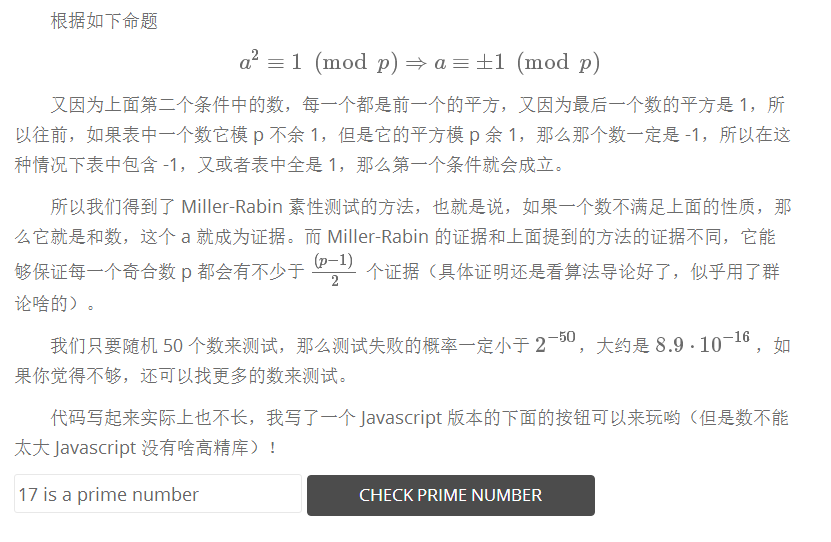
**[数论]Miller-Rabin素性测试**







long long power(long long v, long long p, long long m)

{

long long r = 1;

while(p)

{

if(p & 1) r = r \* v % m;

v = v \* v % m;

p >>= 1;

}

return r;

}

bool witness(long long a, long long p)

{

int k = 0;

long long q = p - 1;

while((q & 1) == 0)

++k, q >>= 1;

long long v = power(a, q, p);

if(v == 1 || v == p - 1)

return false;   // probably prime number

while(k-- != 0)

{

v = v \* v % p;

if(v == p - 1)

return false;

}

return true; // composite number

}

bool miller\_rabin(long long p)

{

if(p == 2) return true;

if(p % 2 == 0) return false;

for(int i = 0; i != 50; ++i)

{

long long a = std::rand() % (p - 1) + 1;

if(witness(a, p))

return false;

}

return true;

}