Power (log N)

template <typename T>

T power(T val, T p, T mod) {

val %= mod;

T result = 1;

while (p > 0) {

if (p & 1) result = (result \* val) % mod;

val = (val \* val) % mod;

p >>= 1;

}

return result;

}

Fermat Theorem

bool fermatIsPrime (int n, int k = 5){

if(n <= 1 || n == 4) return false;

if(n <= 3) return true;

while(k--){

int a = 2 + rand() % (n - 4);

if(power(a, n-1, n) != 1)

return false;

}

return true;

}

MiillerTest

bool miillerTest(int d, int n){

int a = 2 + rand() % (n - 4);

int x = power(a, d, n);

if(x == 1 || x == n-1) return true;

while(d != n-1){

x = (x \* x) % n;

d <<= 1;

if(x == 1) return false;

if(x == n-1) return true;

}

return false;

}

Miiller Theorem

bool miillerIsPrime(int n, int k = 5){

if(n <= 1 || n == 4) return false;

if(n <= 3) return true;

int d = n - 1;

while(d%2 == 0) d >>= 1;

while(k--)

if(!miillerTest(d, n))

return false;

return true;

}