**Shanks baby step giant step**

/\*

for the equation: b = a^x % MOD where a, b, MOD known, finds x

works only when MOD is an odd prime

\*/

long long shank(long long a, long long b)

{

long long i, j, m, c, aj, im;

map< long long, long long > M;

map< long long, long long > :: iterator it;

m = (long long)ceil(sqrt((double)(MOD)));

M.insert(make\_pair(1, 0));

for(j = 1, aj = 1; j < m; j++)

{

aj = (aj \* a) % MOD;

M.insert(make\_pair(aj, j));

}

im = ModInverse(Bigmod(a, m));

for(c = b, i = 0; i < m; i++)

{

it = M.find(c); //finds in only first value of map elements

if(it != M.end()) return i \* m + it->second;

c = (c \* im) % MOD;

}

return 0;

}