教育課題演習　第 15 回　素数と擬素数

RSA 暗号

公開鍵の作り方。

大きい素数 2 個 p, q を用意し，$m=pq$ とする。

$\phi(m)=(p-1)(q-1)$と互いに素な正の整数を選び，公開鍵 k とする。

$ku \equiv 1 \pmod{\phi(m)}$ となる正の整数 u を秘密鍵とする。

p, q として素数リストから選べる程度の大きさの素数を使うと簡単に破られてしまう。

現実の通信には，適当に発生させた乱数のなかから「確率的素数」と判定された数を使う。

確率的素数…素数の可能性が高い数

確率的素数の判定　Miller-Rabin テスト（フェルマー・テストの改良版）

フェルマーの小定理

p を素数とする。a が p の倍数でないとき，$a^{p-1} \equiv 1 \pmod{p}$

フェルマー・テストと擬素数

a を m より小さく 1 より大きい正の整数をとする。

m が素数であれば，$a^{m-1} \equiv 1 \pmod{m}$となるので,

$a^{m-1} \not\equiv 1 \pmod{m}$であれば，$m$ は素数ではない。

ただし，$a^{m-1} \equiv 1 \pmod{m}$　であっても m が素数であるかどうかはわからない。

$a^{m-1} \equiv 1 \pmod{m}$であるような合成数 m を(a を底とする)**擬素数**と呼ぶ。

高速累乗法

a^k の計算を，$a^2=a\times a$，$a^3=a^2\times a$，$a^4=a^3\times a$，……のように行うと，k 乗の計算に$(k-1)$回の乗算が必要。

しかし，たとえば，a^{100} を $a^{100}=a^{64}a^{32}a^4$ と書き換えると，a^2, a^4, a^8, a^{16}，a^{32}，a^{64} を順に計算し，必要な部分だけ取り出して掛算すれば少ない乗算回数で求まる。

要点：指数を 2^k の形の数の和で書く。最大の 2^k の形の数を順に取り出す。

2^k（k=1,2,3,…）：　2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, …

例　208=128+80=128+64+16

∴ $a^{208}=a^{128}a^{64}a^{16}$

☆コンピュータ内部では，整数は 2 進法で表現されるので，この変形は容易。

剰余系における乗算

209 を法とするとき,

$2^2 = 4$

$2^4 = 4^2 = 16$

$2^8 = 16^2 = 256 \equiv 47$

$2^{16} \equiv 47^2 = 2209 \equiv 119$

$2^{32} \equiv 119^2 = 14161 \equiv 158$

$2^{64} \equiv 158^2 = 26964 \equiv 93$

$2^{128} \equiv 3^2 = 80$

$2^{208} = 2^{128} \times 2^{64} \times 2^{16} \equiv 93 \times 80 \times 119 = 7440 \times 119 \equiv 125 \times 119 = 14875 \equiv 36$

だから，209 は素数ではない。

☆法 m における a^{m-1} の計算には，m^2 までの整数が正確に表現できれば十分。

課題 次の値を求めよ。

(1) $2^{106} \bmod 107$

(2) $2^{340} \bmod 341$

(3) $3^{340} \bmod 341$