暗号の数理問題解説 #6

河野

演習問題 1.9　定理 1.21 および演習問題 1.7 を用いて，定理 1.30 の定理を証明せよ。

$G = \mathbb{Z}_m^*$ とおく。G の位数は $\varphi(m)$ である。即ち $|G| = \varphi(m)$ が成立する。$[a]$ で生成される G の部分群を H とする。即ち $H = \langle [a] \rangle$ とする。このとき演習問題 1.7 より $|H| = |[a]|$ が成立する。元の位数を $q = |[a]|$ とすると元の位数の定義より $[a]^q = [1]$ が成立している。定理 1.21 より元の位数 q は群の位数 $\varphi(m)$ の約数である。即ちある自然数 p が存在して $\varphi(m) = qp$ となっている。このとき

$$[a]^{\varphi(m)} = [a]^{qp} = ([a]^q)^p = [1]^p = [1]$$

が成立する。これを mod で書き直すと

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

となる。

演習問題 1.10　互いに素である 2 つの自然数 m, n を入力すると，$\mathbb{Z}_m^*$ における n の逆元 n^{-1} を出力するプログラムを作れ。可能なものは BigInteger クラスを用いていくらでも大きい自然数に対応可能なものを作れ。

これは冬休みのレポート問題です。$pm + qn = 1$ となる q を見つければ q が n の逆元 n^{-1} になります。拡張ユークリッドアルゴリズムを理解していれば，アルゴリズムに関しては問題がないでしょう。一応簡単に書いておくと，m, n が与えられたときユークリッドの互除法で r_i を求めて行きます。このときに $r_i = q_{i+2}r_{i+1} + r_{i+2}$ という関係式を記憶しておきます。m, n は互いに素なのである s で

$$r_s = q_{s+2}r_{s+1} + 1$$

となります。($r_{s+2} = 1$ となる) このとき

$$Pr_s + Qr_{s+1} = 1 \tag{1}$$

となる P, Q が見つかったと言えます ($P = 1, Q = -q_{s+2}$)。ここで記憶していた $r_{s-1} = q_{s+1}r_s + r_{s+1}$ という式を $r_{s+1} = r_{s-1} - q_{s+1}r_s$ として (1) に代入して整理すると

$$P'r_{s-1} + Q'r_s = 1$$

という式が得られます。この操作を続けていくと最終的に

$$pr_{-1} + qr_0 = 1$$

という式が得られます。ここで $r_0 = n, r_{-1} = m$ なので求める p, q が得られる。

そんなにたくさん r_i を憶えておきたくないという人はアルゴリズムを工夫して下さい。うまくいくかもしれません。