暗号の数理問題解説 #7

河野

演習問題 2.3　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。

この問題は第 2 回レポート問題とほとんど同じです。「ほとんど同じである」という点だけ解説しておきましょう。

m と n が互いに素なとき $mp + nq = 1$ を満たす整数 p, q が見つかったとします。このとき両辺を m で割った余りを考えることにより

$$nq \equiv 1 \pmod{n}$$

が成立する。よって $\mathbb{Z}_m^*$ での n の逆元は q である。q が $q < 0$ または $q \geq m$ のときは適当な整数 k を用いて

$$0 \leq q + km < m$$

とできる。$q + km \equiv q$ なので $q + km$ が求めるものである。