# 暗号の数理問題解説 #7

河野

**演習問題 3.3**　$\mathbb{Z}_{15}^*$ の任意の元 $g$ に対し

$$\left(g^E\right)^D = g$$

が成立することを示せ。

理論的に証明されていることであるが，　mod　の計算になれるために問題にした。$[2]^3 = [8], [8]^3 = [2]$ はすでに計算したので他のものについて計算すると

$$\begin{aligned}
[1]^3 &= [1] \cdot [1] = [1] \\
[4]^3 &= [4 \cdot 4] \cdot [4] = [16] \cdot [4] = [1] \cdot [4] = [4] \\
[7]^3 &= [7 \cdot 7] \cdot [7] = [49] \cdot [7] = [4] \cdot [7] = [28] = [13] \\
[11]^3 &= [11 \cdot 11] \cdot [11] = [121] \cdot [11] = [1] \cdot [11] = [11] \\
[13]^3 &= [13 \cdot 13] \cdot [13] = [169] \cdot [13] = [4] \cdot [13] = [52] = [7]
\end{aligned}$$

となる。$E = D = 3$ なので

$$\begin{aligned}
\left([1]^E\right)^D &= [1]^D = [1] \\
\left([2]^E\right)^D &= [8]^D = [2] \\
\left([4]^E\right)^D &= [4]^D = [4] \\
\left([7]^E\right)^D &= [13]^D = [7] \\
\left([11]^E\right)^D &= [11]^D = [11] \\
\left([13]^E\right)^D &= [7]^D = [13]
\end{aligned}$$

となる。

**演習問題 3.4**　2 つの自然数 $m, n$ を入力すると，その最大公約数 $GCD(m, n)$ 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。

この問題については特段の解説はしないが,

- ユークリッドアルゴリズムを理解している。
- JAVA のプログラミングの基礎的部分を理解している。
- BigInteger クラスを理解している。

の 3 つが前提となる。3 つを理解している人には難しくはないであろう。

**演習問題 3.5**　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。

この問題も，(1) が拡張ユークリッドアルゴリズムに変わる点を除けば，前問と同様である。