情報理論 配布資料 #14：演習問題13解答例

担当：井上 純一 (情報科学研究科棟 8-13)
URL：http://chaosweb.complex.eng.hokudai.ac.jp/~j_inoue/

平成17年8月8日

演習問題13の解答例

1. $GF(5)$ に対し, a^j, $j = 1, 2, 3, 4$ と $a^j \pmod 5$ の表を書いてみると

$a^j \setminus j$	1	2	3	4
2	2	4	4	1
3	3	4	2	1
4	4	1	4	1

となる．従って, $a = 2, 3$ のときには $j = p - 1 = 5 - 1 = 4$ で初めて $a^j = 1 \pmod 5$ となるので, $GF(5)$ の原始元は $a = 2, 3$ である．

2. もう一つの公開暗号鍵 β は

$$\beta \quad = \quad \alpha^a \pmod{17} = 5^{17} \pmod{17} \tag{1}$$

で与えられるが

$$5^{15} \quad = \quad (125)^5 = (7 \times 17 + 6)^5 \tag{2}$$

であるから2項定理より

$$(7 \times 17 + 6)^5 \quad = \quad 6^5 + \sum_{k=1}^{5} {}_5C_k (7 \times 17)^k 6^{5-k} \tag{3}$$

となり, 上式の右辺第2項は17で割り切れるので

$$\beta \quad = \quad 5^{17} \pmod{17} = 6^5 \pmod{17} = 7 \tag{4}$$

であり, 求める公開鍵は $\beta = 7$ である．

以下でエルガマル暗号の暗号化および復号化のプロセスについて考える．

(A) **暗号化**

乱数が $k = 6$ であるとすると, 送信すべき暗号文の一つ c_1 は

$$c_1 \quad = \quad 5^6 \pmod{17} \tag{5}$$

であるが

$$5^6 \quad = \quad (5^3)^2 = (125)^2 = (17 \times 7 + 6)^2 = 6^2 + \sum_{k=1}^{2} {}_2C_k (17 \times 7) 6^{2-k} \tag{6}$$

であり, 最終項は 17 の倍数であるから

$$c_1 \quad = \quad 5^6 \pmod{17} = 6^2 \pmod{17} = 2 \tag{7}$$

となり, 暗号文の一つは $c_1 = 2$ である.
一方の c_2 は

$$c_2 \quad = \quad 10 \times 7^6 \pmod{17} \tag{8}$$

であるが, これは c_1 の計算と同様に

$$c_2 \quad = \quad 10 \times 7^6 \pmod{17} = 10 \times 3^2 \pmod{17} = 5 \tag{9}$$

となるので, 結局, 送信すべき暗号文は $(c_1, c_2) = (2, 5)$ である.

(B) **復号化**

$$c_1^a \pmod{17} = 2^{15} \pmod{17} = (2^7)^2 \cdot 2 \pmod{17} = 81 \cdot 2 \pmod{17} = 9 \pmod{17} \tag{10}$$

であるから, $9 \cdot 2 \pmod{17} = 1 \pmod{17}$ であるから, $(c_1^a)^{-1} = 2 \pmod{17}$ である. 従って

$$w \quad = \quad (c_1^a)^{-1} \cdot c_2 \pmod{17} = 2 \cdot 5 \pmod{17} = 10 \pmod{17} \tag{11}$$

となり, 確かに平文 $w = 10$ が復元される.