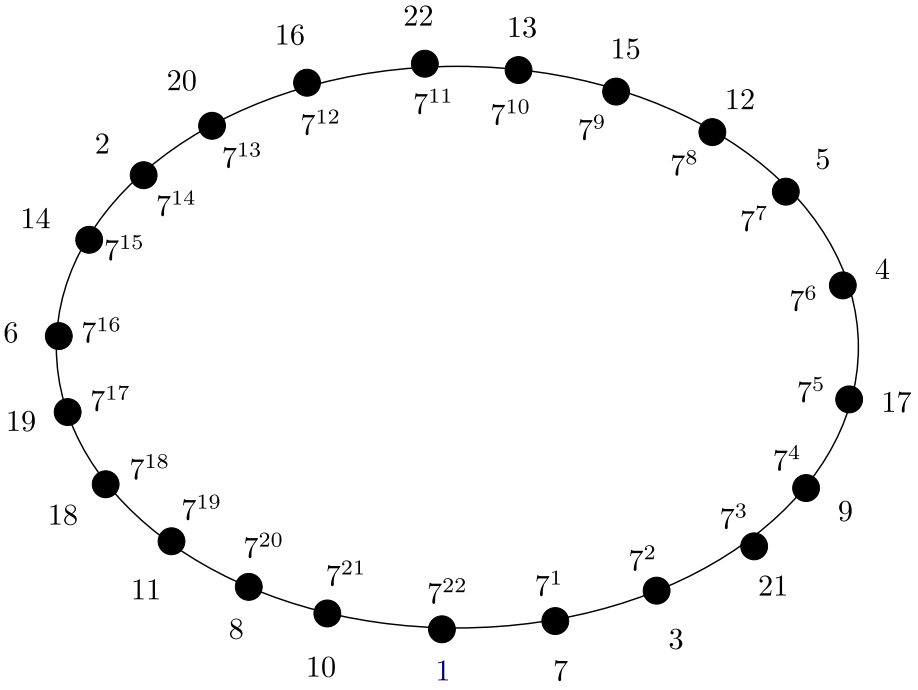
計算数学特論 レポート課題2　機械知能工学専攻　16344217　津上 祐典

課題 1

$p = 23$ の原始元は $a = 7$ であるので空欄を埋めると以下のようになる．



秘密鍵を $x = 20$ とすると公開鍵は

$$p = 23 \tag{1}$$

$$g = 7 \tag{2}$$

$$\begin{aligned} y &= g^x \\ &= 7^{20} \\ &= 7^2 \cdot 7^2 \cdot 7^2 \cdot 7^2 \cdot 7^2 \cdot 7^2 \cdot 7^2 \cdot 7^2 \cdot 7^2 \cdot 7^2 \\ &= 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 4 \cdot 4 \cdot 4 \cdot 3 = 8 \end{aligned} \tag{3}$$

となる．次に乱数 $k = 9$ とし $M = 5$ を送信する．これ暗号化すると，

$$C_1 = g^k = 7^9 = 5 \tag{4}$$

$$\begin{aligned} C_2 &= M \cdot y^k \\ &= 5 \cdot 8 \cdot 8^2 \cdot 8^2 \cdot 8^2 \cdot 8^2 \\ &= 17 \cdot 18 \cdot 18 \cdot 18 \cdot 18 \\ &= 17 \cdot 2 \cdot 2 = 22 \end{aligned} \tag{5}$$

となる．また，復号化すると，

$$\begin{aligned} M' &= C_2 \cdot \{(C_1)^x\}^{-1} \\ &= 22 \cdot \left\{15^{20}\right\}^{-1} \\ &= 22 \cdot 15^2 \\ &= 22 \cdot 18 = 5 \end{aligned} \tag{6}$$

となり M と一致する．

課題２

(1) $p = 23$ の原始元を全部求めよ．

$p = 23$ の約数は $1, 2, 11, 22$ であるので

(2) 原始元 α，乱数 a, b を与えて共有鍵を持てることを確認せよ．

$\alpha = 7$ とすると，