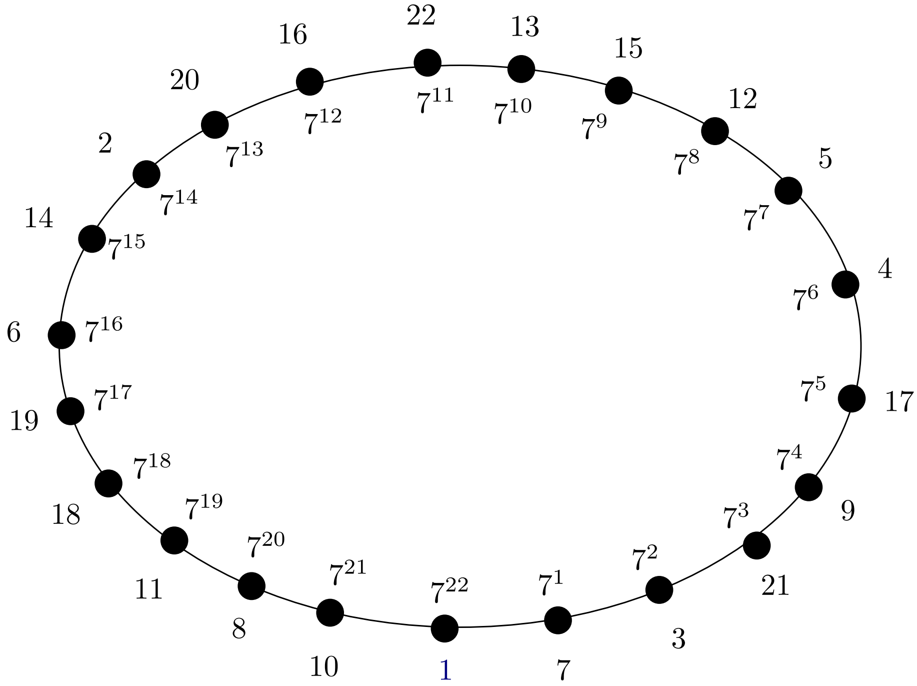
課題 1

$p = 23$ 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

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

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

$$y = g^x (\mathrm{mod}\ 23) = 7^{20} = (7^2)^{10} = 3^{10} = (3^3)^3 \cdot 3 = 4^3 \cdot 3 = 8 \tag{3}$$

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，

$$C_1 = g^k (\mathrm{mod}\ 23) = 7^9 = 5 \tag{4}$$

$$C_2 = M \cdot y^k (\mathrm{mod}\ 23) = 5 \cdot 8^9 = 5 \cdot 8 \cdot (8^2)^4 = 17 \cdot 18^4 = 17 \cdot 18^2 \cdot 18^2 = 17 \cdot 2 \cdot 2 = 22 \tag{5}$$

となる．また，復号化すると，

$$M' = C_2 \cdot \{(C_1)^x\}^{-1} (\mathrm{mod}\ 23) = 22 \cdot \left\{15^{20}\right\}^{-1} = 22 \cdot 15^2 h = 22 \cdot 18 = 5 \tag{6}$$

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．

1. $a = 6, b = 9$ のとき

α^a, α^b を求めると課題 1 よりそれぞれ，

$$\alpha^a = 7^6 (\mathrm{mod}\ 23) = 4 \tag{7}$$

$$\alpha^b = 7^9 (\mathrm{mod}\ 23) = 15 \tag{8}$$

となり，α^{ab} はそれぞれ，

$$\alpha^{ab} = (\alpha^b)^a = 15^6 (\mathrm{mod}\ 23) = (15^2)^3 = 18^3 = 18^2 \cdot 18 = 2 \cdot 18 = 3 \tag{9}$$

$$\alpha^{ab} = (\alpha^a)^b = 4^9 (\mathrm{mod}\ 23) = (4^3)^3 = 18^3 = 3 \tag{10}$$

となり一致する．

2. $a = 14, b = 16$ **のとき**

α^a, α^b を求めると課題 1 よりそれぞれ，

$$\alpha^a = 7^{14} (\mathrm{mod}\ 23) = 2 \tag{11}$$

$$\alpha^b = 7^{16} (\mathrm{mod}\ 23) = 6 \tag{12}$$

となり，α^{ab} はそれぞれ，

$$\alpha^{ab} = (\alpha^b)^a = 6^{14} (\mathrm{mod}\ 23) = (6^2)^7 = 13^7 = 8 \cdot 8 \cdot 8 \cdot 13 = 18 \cdot 12 = 9 \tag{13}$$

$$\alpha^{ab} = (\alpha^a)^b = 2^{16} (\mathrm{mod}\ 23) = 2^5 \cdot 2^5 \cdot 2^6 = 9 \cdot 9 \cdot 18 = 12 \cdot 18 = 9 \tag{14}$$

となり一致する．

3. $a = 20, b = 7$ **のとき**

α^a, α^b を求めると課題 1 よりそれぞれ，

$$\alpha^a = 7^{20} (\mathrm{mod}\ 23) = 8 \tag{15}$$

$$\alpha^b = 7^7 (\mathrm{mod}\ 23) = 5 \tag{16}$$

となり，α^{ab} はそれぞれ，

$$\alpha^{ab} = (\alpha^b)^a = 5^{20} (\mathrm{mod}\ 23) = (5^2)^{10} = 2^{10} = 2^5 \cdot 2^5 = 9 \cdot 9 = 12 \tag{17}$$

$$\alpha^{ab} = (\alpha^a)^b = 8^7 (\mathrm{mod}\ 23) = (8^2)^3 \cdot 8 = 18^3 \cdot 8 = 18^2 \cdot (18 \cdot 8) = 2 \cdot 6 = 12 \tag{18}$$

となり一致する．