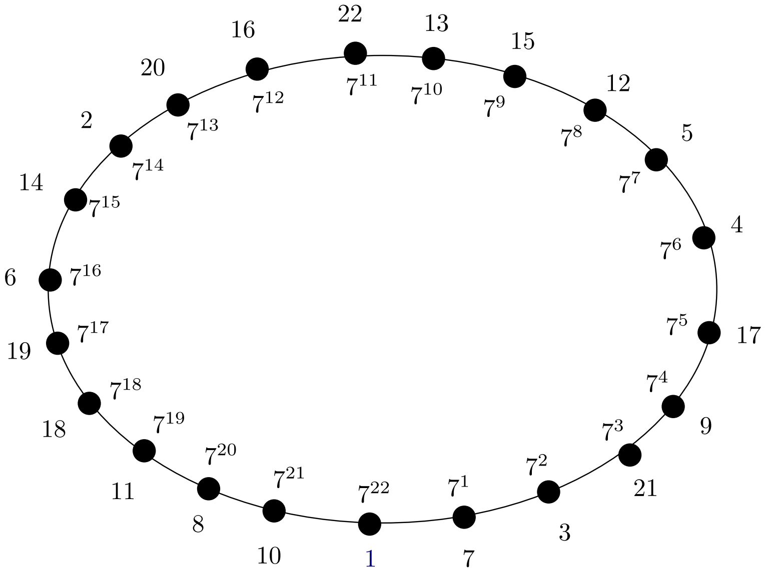
課題 1

$a = 7$ は $p = 23$ の原始元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，

$$C_1 = g^k (\mathrm{mod}\ 23) = 7^9 = 15 \tag{4}$$

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

となる．また，復号化すると，

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

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，またフェルマーの小定理より $a^{23-1} = a^{22} = 1$ であるから，

$2^1 = 2$, $2^2 = 4$, $2^{11} = 2 \cdot 2^5 \cdot 2^5 = 2 \cdot 9 \cdot 9 = 1$

$3^1 = 3$, $3^2 = 9$, $3^{11} = (3^3)^2 \cdot 3^2 = 4^3 \cdot 9 = 18 \cdot 9 = 1$

$4^1 = 4$, $4^2 = 16$, $4^{11} = (4^3)^3 \cdot 4^2 = 18^3 \cdot 16 = 18 \cdot 18 \cdot 18 \cdot 16 = 2 \cdot 2 = 1$

$5^1 = 5$, $5^2 = 25 = 2$, $5^{11} = (5^2)^5 \cdot 5 = 2^5 \cdot 5 = 9 \cdot 5 = 22$

$6^1 = 6$, $6^2 = 36 = 13$, $6^{11} = (6^2)^5 \cdot 6 = 13^5 \cdot 6 = 13^2 \cdot 13^2 \cdot 13 \cdot 6 = 8 \cdot 8 \cdot 9 = 18 \cdot 9 = 1$

$7^1 = 7$, $7^2 = 49 = 3$, $7^{11} = (7^2)^5 \cdot 7 = 3^5 \cdot 7 = 3^3 \cdot 3^2 \cdot 7 = 4 \cdot 9 \cdot 7 = 13 \cdot 7 = 22$

$8^1 = 8$, $8^2 = 64 = 18$, $8^{11} = (8^2)^5 \cdot 8 = 18^5 \cdot 8 = 18^2 \cdot 18^2 \cdot 18 \cdot 8 = 2 \cdot 2 \cdot 6 = 1$

$9^1 = 9$, $9^2 = 81 = 12$, $9^{11} = (9^2)^5 \cdot 9 = 12^5 \cdot 9 = 12^2 \cdot 12^2 \cdot 12 \cdot 9 = 6 \cdot 6 \cdot 16 = 6 \cdot 4 = 1$

$10^1 = 10$, $10^2 = 100 = 8$, $10^{11} = (10^2)^5 \cdot 10 = 8^5 \cdot 10 = 8^2 \cdot 8^2 \cdot 8 \cdot 10 = 18 \cdot 18 \cdot 11 = 22$

$11^1 = 11$, $11^2 = 121 = 6$, $11^{11} = (11^2)^5 \cdot 11 = 6^5 \cdot 11 = 6^2 \cdot 6^2 \cdot 6 \cdot 11 = 13 \cdot 13 \cdot 20 = 13 \cdot 7 = 22$

$12^1 = 12$, $12^2 = 144 = 6$, $12^{11} = (12^2)^5 \cdot 12 = 6^5 \cdot 12 = 6^2 \cdot 6^2 \cdot 6 \cdot 12 = 13 \cdot 13 \cdot 3 = 13 \cdot 16 = 1$
$13^1 = 13$, $13^2 = 169 = 8$, $13^{11} = (13^2)^5 \cdot 13 = 8^5 \cdot 11 = 8^2 \cdot 8^2 \cdot 8 \cdot 13 = 18 \cdot 18 \cdot 12 = 2 \cdot 12 = 1$
$14^1 = 14$, $14^2 = 196 = 12$, $14^{11} = (14^2)^5 \cdot 14 = 12^5 \cdot 11 = 12^2 \cdot 12^2 \cdot 12 \cdot 14 = 6 \cdot 6 \cdot 7 = 13 \cdot 7 = 22$
$15^1 = 15$, $15^2 = 225 = 18$, $15^{11} = (15^2)^5 \cdot 15 = 18^5 \cdot 15 = 18^2 \cdot 18^2 \cdot 18 \cdot 15 = 2 \cdot 2 \cdot 17 = 22$
$16^1 = 16$, $16^2 = 256 = 3$, $16^{11} = (16^2)^5 \cdot 16 = 3^5 \cdot 16 = 3^3 \cdot 3^2 \cdot 16 = 4 \cdot 6 = 1$
$17^1 = 17$, $17^2 = 289 = 13$, $17^{11} = (17^2)^5 \cdot 17 = 13^5 \cdot 17 = 13^2 \cdot 13^2 \cdot 13 \cdot 17 = 8 \cdot 8 \cdot 14 = 18 \cdot 14 = 22$
$18^1 = 18$, $18^2 = 324 = 2$, $18^{11} = (18^2)^5 \cdot 18 = 2^5 \cdot 18 = 2^5 \cdot 18 = 9 \cdot 18 = 1$
$19^1 = 19$, $19^2 = 361 = 6$, $19^{11} = (19^2)^5 \cdot 19 = 16^5 \cdot 19 = 16^2 \cdot 16^2 \cdot 16 \cdot 19 = 3 \cdot 3 \cdot 5 = 22$
$20^1 = 20$, $20^2 = 400 = 9$, $20^{11} = (20^2)^5 \cdot 20 = 9^5 \cdot 20 = 9^2 \cdot 9^2 \cdot 9 \cdot 20 = 12 \cdot 12 \cdot 19 = 6 \cdot 19 = 22$
$21^1 = 21$, $21^2 = 441 = 4$, $21^{11} = (21^2)^5 \cdot 21 = 4^5 \cdot 21 = 4^3 \cdot 4^2 \cdot 21 = 18 \cdot 4 \cdot 15 = 18 \cdot 14 = 22$
$22^1 = 11$, $22^2 = 484 = 1$
より，$p = 23$ の原始元は $5, 7, 10, 11, 14, 15, 17, 19, 20, 21$ である．

(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，

$$\alpha^{ab} = (\alpha^b)^a = 15^6 (\mathrm{mod}\ 23) = (15^2)^3 = 18^3 = 18^2 \cdot 18 = 2 \cdot 18 = 13 \tag{9}$$
$$\alpha^{ab} = (\alpha^a)^b = 4^9 (\mathrm{mod}\ 23) = (4^3)^3 = 18^3 = 13 \tag{10}$$

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．