課題 1

(1) $(Z_p*, \times)$ が群の構造を持つことを示せ.

条件 1. 演算 $\times$ が閉じている.

演算 $\times$ が閉じている，つまり $a, b \in Z_p*$ のとき，$a \times b (\bmod p) \in Z_p*$ であることを示せば良い．$Z_p* = \{1, 2, \cdots, p-1\}$ より，$a \times b (\bmod p) \in Z_p*$ が成り立たない場合は，$a \times b (\bmod p) = 0$ のときである．背理法により $a \times b (\bmod p) = 0$ が成り立たないことを示すことで演算 $\times$ が閉じていることを示す.

はじめに，$a \times b (\bmod p) = 0$ と仮定する．$a \times b (\bmod p) = 0$ となるのは

$$a \times b = kp \tag{1}$$

となるときである．ただし k は自然数である．式変形すると，

$$\frac{a \times b}{p} = k \tag{2}$$

となる．右辺の k は自然数であるから，左辺も自然数でないとならない．しかし，左辺の分母 p は素数である．また $a, b \in Z_p*$ であり，$a \neq p, b \neq p$ であるから左辺は約分できず自然数とならない．よって，(2) 式また (1) 式は成り立たない．これは最初の仮定に矛盾する．よって，$a \times b (\bmod p) = 0$ は成り立たず，演算 $\times$ が閉じていると言える.

条件 2. 結合法則が成立する.

$a, b, c \in Z_p*$ とすると，a, b, c は自然数であるから，結合法則 $a \times (b \times c) = (a \times b) \times c$ は成り立つ.

条件 3. 単位元，逆元がある.

$a \in Z_p*$ とすると，$a \times 1 = 1 \times a = a$ が成り立ち，単位元である 1 が存在する．また，$ax + py = \gcd(a, p) = 1$ とすると，

$$ax + py = 1 \tag{3}$$

$$ax = 1 (\bmod p) = 1 \tag{4}$$

となり，a の逆元は x であり逆元は存在する．以上の 3 つの条件全て満たしているので，$(Z_p*, \times)$ が群の構造を持つ.

(2) (1) を用いて，フェルマーの小定理 $a^{p-1} (\bmod\ p) = 1$(a は Z_p* の任意の要素) を示せ.

Z_p* の要素をすべてかけたものを考える.

$$1 \times 2 \times \cdots \times (p-1) \tag{5}$$

次に，Z_p* の要素に $a \in Z_p*$ をかけて，そのすべてをかけたもの考える.

$$(1 \times a) \times (2 \times a) \times \cdots \times \{(p-1) \times a\} \tag{6}$$

ここで $a, b, c \in Z_p*$ ，$b \neq c$ のとき，$a \times b \neq a \times c$ より，式の $(1 \times a), (2 \times a), \cdots, (p-1) \times a$ はすべて異なる要素である．また，課題 1(1) より演算 $\times$ は閉じているので (5),(6) 式は等しい.

$$\begin{aligned} 1 \times 2 \times \cdots \times (p-1) &= (1 \times a) \times (2 \times a) \times \cdots \times \{(p-1) \times a\} && (7) \\ &= a^{p-1}(1 \times 2 \times \cdots \times (p-1)) && (8) \end{aligned}$$

となり，

$$a^{p-1} (\bmod p) = 1 \tag{9}$$

が成り立つ.

課題２

(1) $p=7, q=13$ で公開鍵 e と秘密鍵 d を設定せよ．

公開鍵 e と秘密鍵 d は

$$n = p \times q = 7 \times 13 = 91$$

$$\lambda = \mathrm{lcm}(p-1, q-1) = \mathrm{lcm}(7-1, 13-1) = \mathrm{lcm}(6, 12) = 12$$

$$1 = \gcd(d, \lambda) \iff \gcd(d, 12) = 1 \quad \therefore d = 5$$

$$ed = 1(\bmod\ \lambda) \iff e5 = 1(\bmod\ 12) \quad \therefore e = 5$$

より $e=5,\ d=5$ となる．

(2) コーディングを以下とする．a=1,$\cdots$,z=26,A=27,$\cdots$,Z=52,0=60,$\cdots$,9=69

(a) kit を送受信せよ．

k,i,t の文字コードはそれぞれ $x_1=11, x_2=9, x_3=20$ であるので暗号化コード c_1, c_2, c_3 は

$$c_1 = 11^5(\bmod\ 91) = 11^2 \cdot 11^2 \cdot 11(\bmod\ 91) = 30 \cdot 30 \cdot 11(\bmod\ 91) = 81 \cdot 11(\bmod\ 91) = 72$$

$$c_2 = 9^5(\bmod\ 91) = 9^3 \cdot 9^2(\bmod\ 91) = 1 \cdot 9^2(\bmod\ 91) = 81$$

$$c_3 = 20^5(\bmod\ 91) = 20^2 \cdot 20^2 \cdot 20(\bmod\ 91) = 36 \cdot 36 \cdot 20(\bmod\ 91) = 36 \cdot 83(\bmod\ 91) = 76$$

となる．また復元化コードは

$$X_1 = 72^5(\bmod\ 91) = 72^2 \cdot 72^2 \cdot 72(\bmod\ 91) = 88 \cdot 88 \cdot 72(\bmod\ 91) = 9 \cdot 72(\bmod\ 91) = 11$$

$$X_2 = 81^5(\bmod\ 91) = 81^2 \cdot 81^2 \cdot 81(\bmod\ 91) = 9 \cdot 9 \cdot 81(\bmod\ 91) = 9$$

$$X_3 = 76^5(\bmod\ 91) = 76^2 \cdot 76^2 \cdot 76(\bmod\ 91) = 43 \cdot 43 \cdot 76(\bmod\ 91) = 29 \cdot 76(\bmod\ 91) = 20$$

となり文字コードと一致する．

(b) 各人のイニシャル２文字を送受信せよ．

私のイニシャル YT の文字コードは $x_1=51, x_2=46$ であるので暗号化コード c_1, c_2 は

$$c_1 = 51^5(\bmod\ 91) = 51^2 \cdot 51^2 \cdot 51(\bmod\ 91) = 53 \cdot 53 \cdot 51(\bmod\ 91) = 79 \cdot 51(\bmod\ 91) = 25$$

$$c_2 = 46^5(\bmod\ 91) = 46^2 \cdot 46^2 \cdot 46(\bmod\ 91) = 23 \cdot 23 \cdot 46(\bmod\ 91) = 74 \cdot 46(\bmod\ 91) = 37$$

となる．また復元化コードは

$$X_1 = 25^5(\bmod\ 91) = 25^2 \cdot 25^2 \cdot 25(\bmod\ 91) = 79 \cdot 79 \cdot 25(\bmod\ 91) = 53 \cdot 25(\bmod\ 91) = 51$$

$$X_2 = 37^5(\bmod\ 91) = 37^2 \cdot 37^2 \cdot 37(\bmod\ 91) = 4 \cdot 4 \cdot 37(\bmod\ 91) = 46$$

となり文字コードと一致する．

(c) 学籍番号の下４桁を送受信せよ．

文字コードは $x_1=64, x_2=62, x_3=61, x_4=67$ であるので暗号化コード c_1, c_2, c_3, c_4 は

$$c_1 = 64^5(\bmod\ 91) = 64^2 \cdot 64^2 \cdot 64(\bmod\ 91) = 1 \cdot 1 \cdot 64(\bmod\ 91) = 64$$

$$c_2 = 62^5(\bmod\ 91) = 62^2 \cdot 62^2 \cdot 62(\bmod\ 91) = 22 \cdot 22 \cdot 62(\bmod\ 91) = 29 \cdot 62(\bmod\ 91) = 69$$

$$c_3 = 61^5(\bmod\ 91) = 61^2 \cdot 61^2 \cdot 61(\bmod\ 91) = 81 \cdot 81 \cdot 61(\bmod\ 91) = 9 \cdot 61(\bmod\ 91) = 3$$

$$c_4 = 67^5(\bmod\ 91) = 67^2 \cdot 67^2 \cdot 67(\bmod\ 91) = 30 \cdot 30 \cdot 67(\bmod\ 91) = 81 \cdot 67(\bmod\ 91) = 58$$

となる．また復元化コードは

$$X_1 = 64^5(\bmod\ 91) = 64^2 \cdot 64^2 \cdot 64(\bmod\ 91) = 1 \cdot 1 \cdot 64(\bmod\ 91) = 64$$

$$X_2 = 69^5(\bmod\ 91) = 69^2 \cdot 69^2 \cdot 69(\bmod\ 91) = 29 \cdot 29 \cdot 69(\bmod\ 91) = 22 \cdot 69(\bmod\ 91) = 62$$

$$X_3 = 3^5(\bmod\ 91) = 61$$

$$X_4 = 58^5(\bmod\ 91) = 58^2 \cdot 58^2 \cdot 58(\bmod\ 91) = 88 \cdot 88 \cdot 58(\bmod\ 91) = 9 \cdot 58(\bmod\ 91) = 67$$

となり文字コードと一致する．