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，$a \times b (\mathrm{mod}\ p) \in Z_p*$ であることを示せば良い．$Z_p* = \{1, 2, \cdots, p-1\}$ より，$a \times b (\mathrm{mod}\ p) \in Z_p*$ が成り立たない場合は，$a \times b (\mathrm{mod}\ p) = 0$ のときである．背理法により $a \times b (\mathrm{mod}\ p) = 0$ 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，$a \times b (\mathrm{mod}\ p) = 0$ と仮定する．$a \times b (\mathrm{mod}\ p) = 0$ 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，$a \times b (\mathrm{mod}\ p) = 0$ 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，

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

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

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 $a^{p-1}(\mathrm{mod}\ p) = 1$($a$ は Z_p* の任意の要素) を示せ．

はじめに，$a, b, c \in Z_p*$, $b \neq c$ のとき，$a \times b \neq a \times c$ を背理法を用いて示す．$a, b, c \in Z_p*$, $b \neq c$ のとき $a \times b = a \times c$ と仮定する．両辺に左から a の逆元をかけると

$$\begin{aligned} a^{-1}(a \times b) &= a^{-1}(a \times c) \quad (5) \\ b &= c \quad (6) \end{aligned}$$

となり，$b \neq c$ と矛盾する．$a, b, c \in Z_p*$, $b \neq c$ のとき，$a \times b \neq a \times c$ は成り立つ．Z_p* の要素をすべてかけたものを考える．

$$1 \times 2 \times \cdots \times (p-1) \quad (7)$$

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．

$$(1 \times a) \times (2 \times a) \times \cdots \times \{(p-1) \times a\} \quad (8)$$

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 (7),(8) 式は等しい．

$$\begin{aligned} 1 \times 2 \times \cdots \times (p-1) &= (1 \times a) \times (2 \times a) \times \cdots \times \{(p-1) \times a\} \quad (9) \\ &= a^{p-1}(1 \times 2 \times \cdots \times (p-1)) \quad (10) \end{aligned}$$

となり，

$$a^{p-1}(\mathrm{mod}\ p) = 1 \quad (11)$$

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

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

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

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

$$ed = 1 (\mathrm{mod}\ \lambda) \iff e5 = 1 (\mathrm{mod}\ 12) \quad \therefore e = 5$$

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

$$c_1 = 11^5 (\mathrm{mod}\ 91) = 11^2 \cdot 11^2 \cdot 11 (\mathrm{mod}\ 91) = 30 \cdot 30 \cdot 11 (\mathrm{mod}\ 91) = 81 \cdot 11 (\mathrm{mod}\ 91) = 72$$

$$c_2 = 9^5 (\mathrm{mod}\ 91) = 9^3 \cdot 9^2 (\mathrm{mod}\ 91) = 1 \cdot 9^2 (\mathrm{mod}\ 91) = 81$$

$$c_3 = 20^5 (\mathrm{mod}\ 91) = 20^2 \cdot 20^2 \cdot 20 (\mathrm{mod}\ 91) = 36 \cdot 36 \cdot 20 (\mathrm{mod}\ 91) = 36 \cdot 83 (\mathrm{mod}\ 91) = 76$$

となる．また復元化コードは

$$x_1 = a$$

$$x_2 = a$$

$$x_3 = a$$

となり文字コードと一致する．