

中間試験

[1]

解答参照

補足1: $a|c$ と $a|l$ から $a|r$ が導かれることについて.

$a|l$ より, $l = ka (k \in \mathbb{N})$ と書ける. このとき, $c = kaq + r$ となる. $a|c$ より, $kaq + r$ は a の倍数である. よって

$kaq + r = a \left(kq + \frac{r}{a} \right)$ となり, $kq + \frac{r}{a}$ は整数でなければならない. ここで, kq は整数なので, $\frac{r}{a}$ が整数でなければならない.

ない. よって, $a|r$ でなければならないことがわかる.

補足2: (7) について.

(2), (3) より $0 \leq r \leq l-1$ が成り立っているので, $r < l$ である.

[2]

(1)

$$\sum_{i=1}^6 ia_i = a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 \equiv a_6 + 6a_6 = 7a_6 \equiv 0 \pmod{7}. \quad Q.E.D.$$

$$(\uparrow \because a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 \equiv a_6 \pmod{7})$$

(2)

$$a_2 + 2a_1 + 3a_3 + 4a_4 + 5a_5 + 6a_6 = -a_2 + a_1 + a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 \equiv a_1 - a_2 \not\equiv 0 \pmod{7}.$$

$$(\uparrow \because a_1 \not\equiv a_2)$$

よって, (1) の関係式を満たさなくなるので, 誤りを検出できる. $Q.E.D.$

[3]

(G0) を示す.

$$(a, x), (b, y) \in G$$

$$\Rightarrow (a, x) \cdot (b, y) = (ay + bx, xy).$$

ここで, $ay + bx \in \mathbb{Z}_p, xy \in \mathbb{Z}_p^*$ より,

$$(a, x) \cdot (b, y) \in G.$$

(G1) を示す.

$$(a, x), (b, y), (c, z) \in G \text{ とすると,}$$

$$((a, x) \cdot (b, y)) \cdot (c, z) = (ay + bx, xy) \cdot (c, z) = (ayz + bxz + cxy, xyz),$$

$$(a, x) \cdot ((b, y) \cdot (c, z)) = (a, x) \cdot (bz + cy, yz) = (ayz + bxz + cxy, xyz).$$

$$\text{よって, } ((a, x) \cdot (b, y)) \cdot (c, z) = (a, x) \cdot ((b, y) \cdot (c, z)).$$

(G2) を示す.

$$e = (0, 1) \text{ とすれば,}$$

$$(a, x) \cdot e = (a, x) \cdot (0, 1) = (a, x),$$

$$e \cdot (a, x) = (0, 1) \cdot (a, x) = (a, x).$$

$$\text{よって, } (a, x) \cdot e = e \cdot (a, x).$$