

問2. 2

(1)

a	1	2	3	4	5	6
a^{-1}	1	4	5	2	3	6

(2)

a	1	2	3	4	5	6	7	8	9
a^{-1}	1	無	7	無	無	無	3	無	9

(3)

a	1	2	3	4	5	6	7	8	9	10
a^{-1}	1	6	4	3	9	2	8	7	5	10

(4)

a	1	2	3	4	5	6	7	8	9	10	11
a^{-1}	1	無	無	無	5	無	7	無	無	無	11

(5)

a	1	2	3	4	5	6	7	8	9	10	11	12
a^{-1}	1	7	9	10	8	11	2	5	3	4	6	12

問2. 3

$$ax \equiv b \pmod{n}$$

$$\Leftrightarrow a'dx \equiv b'd \pmod{n'd}$$

$$\Leftrightarrow \frac{a'dx - b'd}{n'd} \text{ が整数}$$

$$\Leftrightarrow \frac{a'x - b'}{n'} \text{ が整数}$$

$$\Leftrightarrow a'x \equiv b' \pmod{n'}. \quad Q.E.D.$$

問2. 4

まず, $d = \gcd(c, n)$ より, ある整数 c' が存在して, $c = c'd$.

$$ca \equiv cb \pmod{n}$$

$$\Rightarrow c'da \equiv c'db \pmod{n'd}$$

$$\Rightarrow \text{ある整数 } t \text{ が存在して, } c'd(a-b) = n'dt$$

$$\Rightarrow c'(a-b) = n't.$$

ここで, [1. 2. 6]より, c' と n' は互いに素なので, ある整数 t' が存在して, $t = c't'$ と書ける.

よって,

$$c'(a-b) = n't$$

$$\Rightarrow c'(a-b) = n'c't'$$

$$\Rightarrow a-b = n't'$$

$$\Rightarrow a \equiv b \pmod{n'}. \quad Q.E.D.$$

問2. 5

(1)