

演習問題 (略解)

1.

$$3x \equiv 1 \pmod{7}$$

$$x \equiv 5 \pmod{7}$$

2.

$$10x \equiv 11 \pmod{23}$$

$$x \equiv 8 \pmod{23}$$

3.

$$38x \equiv 24 \pmod{52}$$

$$x \equiv 2, 28 \pmod{52}$$

4.

$$11x \equiv 3 \pmod{33}$$

解なし

5.

$$21x \equiv 42 \pmod{140}$$

$$x \equiv 2, 22, 42, 62, 82, 102, 122 \pmod{140}$$

6.

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{7} \\ x \equiv 3 \pmod{11} \end{cases}$$

$$x \equiv 58 \pmod{231}$$

7.

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{7} \\ x \equiv 4 \pmod{11} \end{cases}$$

$$x \equiv 59 \pmod{231}$$

8.

$$\begin{cases} 3x \equiv 2 \pmod{5} \\ 5x \equiv 3 \pmod{7} \end{cases}$$

$$x \equiv 9 \pmod{35}$$

9.

$$\begin{cases} 10x \equiv 6 \pmod{12} \\ 7x \equiv 1 \pmod{11} \end{cases}$$

$$x \equiv 63, 129 \pmod{132}$$

10.

$$x^2 \equiv 10 \pmod{13}$$

$$x \equiv 6, 7 \pmod{13}$$

11.

$$x^2 \equiv 7 \pmod{11}$$

解なし

12. (hint: $221 = 13 \times 17$)

$$x^2 \equiv 1 \pmod{221}$$

$$x \equiv 1, 103, 118, 220 \pmod{221}$$

13. $p = 11$ であるとき、剰余類 R_p について、加算と乗算の演算表をそれぞれ作成しなさい。

(省略) 教科書 p.18 表 2.2 のような表を作成すればよい

14. $p = 11$ であるとき、剰余類 R_p について、非零の各元の (乗法に関する) 指数をそれぞれ求めなさい。

| 元 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|----|---|----|---|---|---|----|----|----|---|----|
| 指数 | 1 | 10 | 5 | 5 | 5 | 10 | 10 | 10 | 5 | 2 |

15. $q = 24$ であるとき、既約剰余類 \tilde{R}_q の要素を列挙しなさい。

$$1, 5, 7, 11, 13, 17, 19, 23$$

16. $q = 24$ であるとき、既約剰余類 \tilde{R}_q の各元について、その (乗法に関する) 逆元を求めなさい。

| 元 | 1 | 5 | 7 | 11 | 13 | 17 | 19 | 23 |
|----|---|---|---|----|----|----|----|----|
| 逆元 | 1 | 5 | 7 | 11 | 13 | 17 | 19 | 23 |

17. $q = 512$ であるとき、既約剰余類 \tilde{R}_q の要素の数 (=位数) はいくらか。

256

18. $q = 600$ であるとき、オイラーの関数 $\varphi(q)$ の値を求めなさい。

160

- 19.

$$7^{322} \bmod 600$$

49 mod 600

- 20.

$$7^{159} \bmod 600$$

343 mod 600