

情報数学 II - 第 3 章レポート-

1111 meswanko

(協力者:)

-2017 年 7 月 10 日-

問題 3 - 1

1

$a = a_0 + a_1 \cdot 10 + \cdots + a_n \cdot 10^n$ を整数 $a > 0$ の 10 進数表示とする.

$10 \equiv 1 \pmod{3}$ より, $10^k \equiv 1 \pmod{3}$ が得られるから,

$$a \equiv a_0 + a_1 + \cdots + a_n \pmod{3}$$

したがって, $a \equiv 0 \pmod{3} \Leftrightarrow a_0 + a_1 + \cdots + a_n \equiv 0 \pmod{3}$.

1 追加問題

- 7 の倍数

$10^3 \equiv -1 \pmod{7}$ より, $10^{3k} \equiv (-1)^k \pmod{7}$ が得られるから,

$$a \equiv a_0a_1a_2 - a_3a_4a_5 + a_6a_7a_8 - \cdots \pmod{7}$$

したがって, $a \equiv 0 \pmod{7} \Leftrightarrow a \equiv a_0a_1a_2 - a_3a_4a_5 + a_6a_7a_8 - \cdots \pmod{7}$.

- 13 の倍数

$10^3 \equiv -1 \pmod{13}$ より, $10^{3k} \equiv (-1)^k \pmod{11}$ が得られるから,

$$a \equiv a_0a_1a_2 - a_3a_4a_5 + a_6a_7a_8 - \cdots \pmod{11}$$

したがって, $a \equiv 0 \pmod{7} \Leftrightarrow a \equiv a_0a_1a_2 - a_3a_4a_5 + a_6a_7a_8 - \cdots \pmod{11}$.]

- 37 の倍数

$10^3 \equiv 1 \pmod{37}$ より, $10^{3k} \equiv 1 \pmod{37}$ が得られるから,

$$a \equiv a_0a_1a_2 + a_3a_4a_5 + a_6a_7a_8 + \cdots \pmod{37}$$

したがって, $a \equiv 0 \pmod{37} \Leftrightarrow a \equiv a_0a_1a_2 + a_3a_4a_5 + a_6a_7a_8 + \cdots \pmod{37}$.

2

$$\begin{aligned}(42899634253)_{12} &= 4 \times 12^{10} + 2 \times 12^9 + 8 \times 12^8 \\ &\quad + 9 \times 12^7 + 9 \times 12^6 + 6 \times 12^5 + 3 \times 12^4 \\ &\quad + 4 \times 12^3 + 2 \times 12^2 + 5 \times 12^1 + 3\end{aligned}$$

また, $12^k \equiv 1 \pmod{11}$ より

$$\begin{aligned}(42899634253)_{12} &\equiv 4 + 2 + 8 + 9 + 9 + 6 \\ &\quad + 3 + 4 + 2 + 5 + 3 \pmod{11} \\ &\equiv 55 \\ &\equiv 0 \pmod{11}\end{aligned}$$

より, $(42899634253)_{12}$ は $(11)_{10}$ で割り切れる.

3

$$\begin{aligned}(3A6F2B1)_{16} &= (3 \times 16^6 + 10 \times 16^5 + 6 \times 16^4 \\ &\quad + 15 \times 16^3 + 2 \times 16^2 + 11 \times 16^1 + 1)_{10}\end{aligned}$$

また, $(16)_{10}^k \equiv 1 \pmod{15}$ より

$$\begin{aligned}(3A6F2B1)_{16} &\equiv (3 + 10 + 6 + 15 + 2 + 11 + 1)_{10} \\ &\equiv (48)_{10} \\ &\equiv (3)_{10} \pmod{15} \\ &\equiv (3)_{16} \pmod{F}\end{aligned}$$

4

5

6

7

8

9

Option 7 の倍数の判定法の証明.

$$\begin{cases} N = 10a + b \\ M = a - 2b \end{cases}$$

とすると,

$$M \equiv 0 \pmod{7} \Leftrightarrow \exists k \in \mathbb{Z} \text{ s.t. } a - 2b = 7k$$

のとき,

$$\begin{aligned} N &= 10(7k + 2b) + b \\ &= 7 \cdot 10k + 21b \\ &= 7(10k + 3b) \\ &\equiv 0 \pmod{7} \end{aligned}$$

より, $7|(a - 2b)$, $7|(10a + b)$ となるので, 題意を満たす.

問題 3 - 2

1

2

$\{59, 162, -353, 107, 77, -50, 116\}$ より,

$$59 \equiv 3 \pmod{7}$$

$$162 \equiv 2 \pmod{7}$$

$$-353 \equiv 4 \pmod{7}$$

$$107 \equiv 2 \pmod{7}$$

$$77 \equiv 0 \pmod{7}$$

$$-50 \equiv 6 \pmod{7}$$

$$116 \equiv 4 \pmod{7}$$

より, 7 を法とする 完全代表系とはならない.

3

$\{-141, 65, 103, 70, -6, 199, 32\}$ より,

$$-141 \equiv 6 \pmod{7}$$

$$65 \equiv 2 \pmod{7}$$

$$103 \equiv 5 \pmod{7}$$

$$70 \equiv 0 \pmod{7}$$

$$-6 \equiv 1 \pmod{7}$$

$$199 \equiv 3 \pmod{7}$$

より, 7 を法とする 完全代表系とはなる.

4

5

問題 3 - 3

1

2

3

4

5

6

7

$$\begin{cases} x \equiv c_1 \pmod{2} \\ x \equiv c_2 \pmod{3} \\ x \equiv c_3 \pmod{5} \\ x \equiv c_4 \pmod{7} \end{cases}$$

より, 第 1 式を満たす整数は,

$$x = c_1 + 2r \quad (A)$$

の形である. これが第 2 式を満たすように r を定める.

(A) を第 2 式に代入すると,

$$c_1 + 2r \equiv c_2 \pmod{3}$$

であるから, そのためには $d_1 \equiv c_1 - c_2 \pmod{3}$ として r を

$$2r \equiv d_1 \quad (B)$$

を満たすようにとればよい. $(2, 3) = 1$ より, (B) の解は 3 を法としてただ 1 つ存在する. それを $r = r_1 \pmod{3}$ とすると, (B) を満たす整数は,

$$r = r_1 + 3s$$

の形である. したがってこれを (A) に代入し, $x_2 = c_1 + 2r_1$ とおくと,

$$x = x_2 + 2 \times 3 \times s = x_2 + 6s$$

が 第 1 式, 第 2 式をともに満たす整数となる.

次にこれが第 3 式を満たすように s を定める. そして上と同様にして 第 1 式から第 3 式までを満たす整数が,

$$x = x_3 + 2 \times 3 \times 5 \times t = x_3 + 30t$$

の形でえられる. ($x_3 = x_2 + 6s_1$)

さらにこれが第 4 式を満たすように t を定める. そして上と同様にして 第 1 式から第 4 式までを満たす整数が,

$$x = x_4 + 2 \times 3 \times 5 \times 7 \times u = x_4 + 210u$$

の形でえられる. ($x_4 = x_3 + 30t_1$)

したがって, 求める解は,

$$\begin{aligned} x &\equiv x_4 \pmod{210} \\ &\equiv x_3 + 30t_1 \pmod{210} \\ &\equiv x_2 + 6s_1 + 30t_1 \pmod{210} \\ &\equiv c_1 + 2r_1 + 6s_1 + 30t_1 \pmod{210} \end{aligned}$$

8

9

10

11

問題 3 - 4

1

(i)

$$\begin{aligned}3^{47} &\equiv (3^3)^{15} \times 3^2 \\&\equiv 4^{15} \times 3^2 \quad (\because 3^3 \equiv 27 \equiv 4 \pmod{23} \text{ より}) \\&\equiv (4^3)^5 \times 3^2 \\&\equiv 18^5 \times 3^2 \quad (\because 4^3 \equiv 64 \equiv 18 \pmod{23} \text{ より}) \\&\equiv (-5)^5 \times 3^2 \quad (\because 18 \equiv -5 \pmod{23} \text{ より}) \\&\equiv \{(-5)^2\}^2 \times (-5) \times 3^2 \\&\equiv 2^2 \times (-5) \times 3^2 \quad (\because (-5)^2 \equiv 25 \equiv 2 \pmod{23} \text{ より}) \\&\equiv -19 \\&\equiv 4 \pmod{23}\end{aligned}$$

(ii)

$$\begin{aligned}7^{1000} &\equiv (7^2)^{500} \\&\equiv 1^{500} \quad (\because 7^2 \equiv 49 \equiv 1 \pmod{24} \text{ より}) \\&\equiv 1 \pmod{24}\end{aligned}$$

2

3 いずれも Mathematica で素因数分解の計算を行った

(i) $n = 127281 = 3 \times 7 \times 11 \times 19 \times 29$ より,

$$\begin{aligned}\varphi(n) &= 127281 \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{11}\right) \left(1 - \frac{1}{19}\right) \left(1 - \frac{1}{29}\right) \\&= 60480\end{aligned}$$

また,

$$\mu(n) = (-1)^5 = -1$$

(ii) $n = 18538 = 2 \times 13 \times 23 \times 31$ より,

$$\begin{aligned}\varphi(n) &= 18538 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{13}\right) \left(1 - \frac{1}{23}\right) \left(1 - \frac{1}{31}\right) \\ &= 7920\end{aligned}$$

また,

$$\mu(n) = (-1)^4 = 1$$

(iii) $n = 200655 = 3^2 \times 5 \times 7^3 \times 13$ より,

$$\begin{aligned}\varphi(n) &= 200655 \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{13}\right) \\ &= 84672\end{aligned}$$

また,

$$\mu(n) = 0$$

4

5

6

7

8

9

10

RSA

問題 3 - 5

2

3

4

5

6

問題 3 - 6

1

2

3

4

5

6

7

8

9

10

11

問題 3 - 6

FGLM

定理証明