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

2

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

また, $12^k \equiv 1(mod 11)$ より

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

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

3

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

また, $(16)_{10}^k \equiv 1(mod 15)$ より

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

問題 3 - 2

1

2

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

$$\begin{aligned}59 &\equiv 3(mod\ 7)\\162 &\equiv 2(mod\ 7)\\-353 &\equiv 4(mod\ 7)\\107 &\equiv 2(mod\ 7)\\77 &\equiv 0(mod\ 7)\\-50 &\equiv 6(mod\ 7)\\116 &\equiv 4(mod\ 7)\end{aligned}$$

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,

$$\begin{aligned}-141 &\equiv 6(mod\ 7)\\65 &\equiv 2(mod\ 7)\\103 &\equiv 5(mod\ 7)\\70 &\equiv 0(mod\ 7)\\-6 &\equiv 1(mod\ 7)\\199 &\equiv 3(mod\ 7)\\32 &\equiv 4(mod\ 7)\end{aligned}$$

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

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

より, 第 1 式を満たす整数は,

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

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,

$$c_1 + 2r \equiv c_2 (mod\ 3)$$

であるから, そのためには $d_1 \equiv c_1 - c_2 (mod\ 3)$ として r を

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

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 $r = r_1 (mod\ 3)$ 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,

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

8

9

10

11

問題 3 - 4

1

(i)

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

(ii)

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

2

3

4

5

6

7

8

9

10

RSA

問題 3 - 5

2

3

4

5

6

問題 3 - 6

問題 3 - 6

FGLM

定理証明