2022

U) (a)

$X_1 = 3^{31} \bmod (17^2 \cdot 13)$

$n_{11} = 49$, $n_{12} = 13$ とおく. 拡張ECDより $n_{11}x + n_{12}y = 1$ となる

$\mathbb{Z}$ の x, y を求めると.

$49 = 13 \cdot 3 + 10$ $\quad 1 = 10 - 3 \cdot 3$

$13 = 10 \cdot 1 + 3$ $\quad = 10 - (13 - 10 \cdot 1) \cdot 3 = 13 \cdot (-3) + 10 \cdot 4$

$10 = 3 \cdot 3 + 1$ $\quad = 13 \cdot (-3) + (49 - 13 \cdot 3) \cdot 4 = 49 \cdot 4 + 13 \cdot (-15)$

$S_1 = 49 \cdot 4 = 196$, $S_2 = -195$

$3^{31} \bmod 49 \equiv (3^5)^6 \cdot 3 \equiv (-2)^6 \cdot 3 \equiv 45$

$3^{31} \bmod 13 = (3^3)^{10} \cdot 3 \equiv 3$

$3^{31} \bmod n_1 \equiv 45 \cdot (-195) + 3 \cdot 196 \equiv -8775 + 588 \equiv -8187 \equiv 94$

(b) $n_{21} = 23$, $n_{22} = 29$ とおくと拡張ECDより

$23 \cdot (-5) + 29 \cdot 4 = 1$ となる また.

$3^{31} \bmod 23 \equiv (3^3)^{10} \cdot 3 = 4^{10} \cdot 3 \equiv 48 \cdot 16^4 \equiv 2 \cdot 3^2 \equiv 18$

$3^{31} \bmod 29 \equiv (3^3)^{10} \cdot 3 = (-2)^{10} \cdot 3 = 3072 \equiv 27$

よって求める. 中国剰余定理より

$3^{31} \bmod \underset{667}{n_2} \equiv \underset{621}{27 \cdot 23 \cdot (-5)} + 18 \cdot 29 \cdot 4 \equiv -3105 + 2088 \equiv -1017 \equiv 317$

(2) $\mathbb{Z}$上既約を示す。写像ϕを以下のように定義する。

$$\phi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/2\mathbb{Z}[X]$$
$$\sum a_i X^i \longmapsto \sum a_i \pmod 2 \, X^i$$

$\mathbb{Z}[X] \ni f(X) = \sum a_i X^i$, $g(X) = \sum b_i X^i$

$$\begin{aligned}\phi(f(X)+g(X)) &= \phi\left(\sum (a_i + b_i) X^i\right) \\ &= \sum (a_i + b_i) \pmod 2 \, X^i \\ &= \sum a_i \pmod 2 \, X^i + \sum b_i \pmod 2 \, X^i \\ &= \phi(f(X)) + \phi(g(X))\end{aligned}$$

$$\begin{aligned}\phi(f(X)g(X)) &= \phi\left(\left(\sum a_i X^i\right)\left(\sum b_i X^i\right)\right) \\ &= \phi\left(\sum_k \sum_{i=0}^{k} (a_i b_{k-i}) X^k\right) \\ &= \sum_k \sum_{i=0}^{k} (a_i b_{k-i}) \pmod 2 \, X^k \\ &= \left(\sum a_i \pmod 2 \, X^i\right)\left(\sum b_i \pmod 2 \, X^i\right) \\ &= \phi(f(X))\,\phi(g(X))\end{aligned}$$

$$\begin{aligned}\phi(1_{\mathbb{Z}[X]}) &= 1 \pmod 2 \\ &= 1_{\mathbb{Z}/2\mathbb{Z}[X]}\end{aligned}$$

よって、ϕは環準同型写像である。

$f(X)$を可約とすると、$f(X) = g(X)h(X)$ $(0 < \deg(g), \deg(h) < \deg(f))$

となる$\mathbb{Z}[X] \ni g(X), h(X)$が存在する。このとき、$\phi$の環準同型性より

$\phi(f(X)) = \phi(g(X))\,\phi(h(X))$となる。つまり$f(X)$が$\mathbb{Z}[X]$上可約

ならば、$\mathbb{Z}/2\mathbb{Z}[X]$上可約である。対偶をとると、$\mathbb{Z}/2\mathbb{Z}[X]$上既約ならば、

$\mathbb{Z}[X]$上既約である。

$f(X) = X^4 + X^3 + X^2 + X + 1$が$\mathbb{Z}/2\mathbb{Z}$上既約であることを示す。

・$\deg(g)=1$ または 3 となる $g\in\mathbb{Z}/2\mathbb{Z}$ で割り切れるとき.

$f(x)=(x^3+ax^2+bx+c)(x+d)$ $(a,b,c,d\in\mathbb{Z}/2\mathbb{Z})$

$=x^4+(a+d)x^3+(ad+b)x^2+(bd+c)x+cd$ となる.

両辺比較して, $\begin{cases} a+d=1 \\ ad+b=1 \\ bd+c=1 \\ cd=1 \end{cases}$ となるが, これを満たす a,b,c,d は存在しない.

・$\deg(g)=2$ となる $g\in\mathbb{Z}/2\mathbb{Z}[x]$ で割り切れるとき

$f(x)=(x^2+ax+b)(x^2+cx+d)$ $(a,b,c,d$ ～)

$=x^4+(a+c)x^3+(b+d+ac)x^2+(ad+bc)x+bd$

～ $\begin{cases} a+c=1 \\ b+d+ac=1 \\ ad+bc=1 \\ bd=1 \end{cases}$ となり ――――

よって, $f(x)$ は $\mathbb{Z}/2\mathbb{Z}[x]$ 上既約であり, $\mathbb{Z}[x]$ も既約

(3) (a) $H_8=\{1,3,5,7\}$, $\{3,5\}$は H_8を生成する.

(b) $\phi_8 : H_8 \longrightarrow S_4$

$3^{\bar{i}}5^{\bar{j}} \longmapsto (1\ 2)^{\bar{i}}(3\ 4)^{\bar{j}}$, $\bar{i},\bar{j}\in\mathbb{Z}/2\mathbb{Z}$

と定義すると. $\mathbb{Z}/2\mathbb{Z}\ni \bar{i}_1,\bar{j}_1,\bar{i}_2,\bar{j}_2$に対し

$\phi_8(3^{\bar{i}_1}5^{\bar{j}_1}\cdot 3^{\bar{i}_2}5^{\bar{j}_2})=\phi_8(3^{\bar{i}_1+\bar{i}_2}5^{\bar{j}_1+\bar{j}_2})$

$=(1\ 2)^{\bar{i}_1+\bar{i}_2}(3\ 4)^{\bar{j}_1+\bar{j}_2}$

$=(1\ 2)^{\bar{i}_1}(3\ 4)^{\bar{j}_1}\cdot(1\ 2)^{\bar{i}_2}(3\ 4)^{\bar{j}_2}$

$=\phi_8(3^{\bar{i}_1}5^{\bar{j}_1})\phi_8(3^{\bar{i}_2}5^{\bar{j}_2})$

であるから. ϕ_8は準同型写像.

次に. $\forall 3^{\bar{i}_1}5^{\bar{j}_1}, 3^{\bar{i}_2}5^{\bar{j}_2}\in H_8$ $(\bar{i}_1,\bar{j}_2\in\mathbb{Z}/2\mathbb{Z})$ について

$\phi(3^{\bar{i}_1}5^{\bar{j}_1})=\phi(3^{\bar{i}_2}5^{\bar{j}_2})$

$\Leftrightarrow (1\ 2)^{\bar{i}_1}(3\ 4)^{\bar{j}_1}=(1\ 2)^{\bar{i}_2}(3\ 4)^{\bar{j}_2}$

$\Leftrightarrow (1\ 2)^{\bar{i}_1-\bar{i}_2}(3\ 4)^{\bar{j}_1-\bar{j}_2}=1_{S_4}$

$\Leftrightarrow \bar{i}_1-\bar{i}_2=\bar{0}$, $\bar{j}_1-\bar{j}_2=\bar{0}$

$\Leftrightarrow \bar{i}_1=\bar{i}_2$, $\bar{j}_1=\bar{j}_2$

$\therefore$ ϕ_8は単射. ■

(c) $H_5=\{1,2,3,4\}$より. $|H_5|=4$, $\{2\}$は H_5を生成する.

(d) $\phi_5 : H_8 \longrightarrow S_4$

$2^{\bar{i}} \longmapsto (2\ 3\ 4\ 1)^{\bar{i}}$ $(\bar{i}\in\mathbb{Z}/4\mathbb{Z})$

と定義すると. $\mathbb{Z}/4\mathbb{Z}\ni\bar{i},\bar{j}$に対し

$\phi_5(2^{\bar{i}}\cdot 2^{\bar{j}})=\phi_5(2^{\bar{i}+\bar{j}})$

$=(2\ 3\ 4\ 1)^{\bar{i}+\bar{j}}=(2\ 3\ 4\ 1)^{\bar{i}}(2\ 3\ 4\ 1)^{\bar{j}}$

$=\phi_5(2^{\bar{i}})\phi_5(2^{\bar{j}})$ であるから ϕ_5は準同型 ー ー

次に. $\forall 2^{\bar{i}}, 2^{\bar{j}}\in H_8$ $(\bar{i},\bar{j}\in\mathbb{Z}/4\mathbb{Z})$ について

$\phi_5(2^{\bar{i}})=\phi_5(2^{\bar{j}})\Leftrightarrow(2\ 3\ 4\ 1)^{\bar{i}}=(2\ 3\ 4\ 1)^{\bar{j}}\Leftrightarrow(2\ 3\ 4\ 1)^{\bar{i}-\bar{j}}=1_{S_4}$

$\Leftrightarrow \bar{i}-\bar{j}=0 \Leftrightarrow \bar{i}=\bar{j}$ $\therefore$ ϕ_5は単射 ■