

2022

U) (a)

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

$$n_{11} = 49, n_{12} = 13 \in \mathbb{Z} \text{ 且 } \gcd(n_{11}, n_{12}) = 1 \text{ 且 } n_{11}x + n_{12}y = 1 \text{ 且 } 3$$

$$\mathbb{Z} \ni x, y \text{ 且 } 3 \in \mathbb{Z}$$

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

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

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

$$s_1 = 49 \cdot 4 = 196, s_2 = -195$$

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

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

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

$$(b) n_{21} = 23, n_{22} = 29 \in \mathbb{Z} \text{ 且 } \gcd(n_{21}, n_{22}) = 1$$

$$23 \cdot (-5) + 29 \cdot 4 = 1 \text{ 且 } 3 \in \mathbb{Z}$$

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

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

$$2 \cdot 3 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \cdot 101 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 127 \cdot 131 \cdot 137 \cdot 139 \cdot 143 \cdot 149 \cdot 151 \cdot 157 \cdot 163 \cdot 167 \cdot 173 \cdot 179 \cdot 181 \cdot 187 \cdot 191 \cdot 193 \cdot 197 \cdot 199 \cdot 211 \cdot 223 \cdot 227 \cdot 229 \cdot 233 \cdot 239 \cdot 241 \cdot 251 \cdot 257 \cdot 263 \cdot 269 \cdot 271 \cdot 277 \cdot 281 \cdot 283 \cdot 293 \cdot 307 \cdot 311 \cdot 313 \cdot 317 \cdot 331 \cdot 337 \cdot 347 \cdot 353 \cdot 359 \cdot 367 \cdot 373 \cdot 379 \cdot 383 \cdot 389 \cdot 397 \cdot 401 \cdot 409 \cdot 419 \cdot 421 \cdot 431 \cdot 433 \cdot 439 \cdot 443 \cdot 449 \cdot 457 \cdot 461 \cdot 463 \cdot 467 \cdot 473 \cdot 479 \cdot 487 \cdot 491 \cdot 499 \cdot 503 \cdot 509 \cdot 521 \cdot 523 \cdot 527 \cdot 539 \cdot 541 \cdot 547 \cdot 557 \cdot 563 \cdot 569 \cdot 571 \cdot 577 \cdot 587 \cdot 593 \cdot 599 \cdot 601 \cdot 607 \cdot 613 \cdot 617 \cdot 619 \cdot 623 \cdot 629 \cdot 631 \cdot 637 \cdot 641 \cdot 643 \cdot 647 \cdot 653 \cdot 659 \cdot 661 \cdot 667 \cdot 671 \cdot 673 \cdot 677 \cdot 683 \cdot 687 \cdot 691 \cdot 697 \cdot 701 \cdot 709 \cdot 713 \cdot 719 \cdot 727 \cdot 733 \cdot 739 \cdot 743 \cdot 751 \cdot 757 \cdot 761 \cdot 769 \cdot 773 \cdot 787 \cdot 797 \cdot 809 \cdot 811 \cdot 821 \cdot 823 \cdot 827 \cdot 833 \cdot 839 \cdot 847 \cdot 853 \cdot 857 \cdot 859 \cdot 863 \cdot 869 \cdot 877 \cdot 881 \cdot 883 \cdot 887 \cdot 893 \cdot 897 \cdot 901 \cdot 907 \cdot 911 \cdot 913 \cdot 919 \cdot 929 \cdot 937 \cdot 941 \cdot 947 \cdot 953 \cdot 967 \cdot 971 \cdot 973 \cdot 977 \cdot 983 \cdot 989 \cdot 991 \cdot 997$$

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

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

$$\phi: \mathbb{Z}[X] \longrightarrow \mathbb{Z}/2\mathbb{Z}[X]$$

$$\sum a_i X^i \longmapsto \sum a_i \pmod{2} X^i$$

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

$$\phi(f(X) + g(X)) = \phi(\sum (a_i + b_i) X^i)$$

$$= \sum (a_i + b_i) \pmod{2} X^i$$

$$= \sum a_i \pmod{2} X^i + \sum b_i \pmod{2} X^i$$

$$= \phi(f(X)) + \phi(g(X))$$

$$\phi(f(X)g(X)) = \phi((\sum a_i X^i)(\sum b_i X^i))$$

$$= \phi\left(\sum_k \sum_{i=0}^k (a_i b_{k-i}) X^k\right)$$

$$= \sum_k \sum_{i=0}^k (a_i b_{k-i} \pmod{2}) X^k$$

$$= (\sum a_i \pmod{2} X^i) (\sum b_i \pmod{2} X^i)$$

$$= \phi(f(X)) \phi(g(X))$$

$$\phi(1_{\mathbb{Z}[X]}) = 1 \pmod{2}$$

$$= 1_{\mathbb{Z}/2\mathbb{Z}[X]}$$

よって、 $\phi$  は環準同型写像である。

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

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

$\phi(f(X)) = \phi(g(X)) \phi(h(X))$  とある。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。反対に、 $\mathbb{Z}/2\mathbb{Z}[X]$  上不可約ならば、

$\mathbb{Z}[X]$  上不可約である。

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

o  $\deg(g) = 1$  かつ  $g \in \mathbb{Z}/2\mathbb{Z}[x]$  かつ  $g$  は不可逆な元でない。

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

$$= x^4 + (a+d)x^3 + (ad+b)x^2 + (bd+c)x + cd \quad \text{と仮定}$$

両辺比較して、

$$\begin{cases} a+d=1 \\ ad+b=1 \\ bd+c=1 \\ cd=1 \end{cases}$$

と仮定する。ここで満たす  $a, b, c, d$  は存在しない。

o  $\deg(g) = 2$  かつ  $g \in \mathbb{Z}/2\mathbb{Z}[x]$  かつ  $g$  は不可逆な元でない

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

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

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

と仮定する。

よって、 $f(x)$  は  $\mathbb{Z}/2\mathbb{Z}[x]$  上の不可逆な元でない。

(3) (a)  $H_8 = \{1, 3, 5, 7\}$ ,  $\{3, 5\}$  は  $H_8$  に生成される.

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

$$3^{\tilde{v}} 5^{\tilde{z}} \longmapsto (1\ 2)^{\tilde{v}} (3\ 4)^{\tilde{z}}, \quad \tilde{v}, \tilde{z} \in \mathbb{Z}/2\mathbb{Z}$$

$\hookrightarrow$  定義する.  $\mathbb{Z}/2\mathbb{Z} \ni \tilde{v}_1, \tilde{z}_1, \tilde{v}_2, \tilde{z}_2 \mapsto \tilde{v}_1 + \tilde{v}_2$

$$\begin{aligned} \phi_8(3^{\tilde{v}_1} 5^{\tilde{z}_1} \cdot 3^{\tilde{v}_2} 5^{\tilde{z}_2}) &= \phi_8(3^{\tilde{v}_1 + \tilde{v}_2} 5^{\tilde{z}_1 + \tilde{z}_2}) \\ &= (1\ 2)^{\tilde{v}_1 + \tilde{v}_2} (3\ 4)^{\tilde{z}_1 + \tilde{z}_2} \end{aligned}$$

$$= (1\ 2)^{\tilde{v}_1} (3\ 4)^{\tilde{z}_1} \cdot (1\ 2)^{\tilde{v}_2} (3\ 4)^{\tilde{z}_2}$$

$$= \phi_8(3^{\tilde{v}_1} 5^{\tilde{z}_1}) \phi_8(3^{\tilde{v}_2} 5^{\tilde{z}_2})$$

$\therefore$  任意の  $\phi_8$  は準同型写像.

次に:  $\forall 3^{\tilde{v}_1} 5^{\tilde{z}_1}, 3^{\tilde{v}_2} 5^{\tilde{z}_2} \in H_8 (\tilde{v}_1, \tilde{z}_1, \tilde{v}_2, \tilde{z}_2 \in \mathbb{Z}/2\mathbb{Z})$  について

$$\phi(3^{\tilde{v}_1} 5^{\tilde{z}_1}) = \phi(3^{\tilde{v}_2} 5^{\tilde{z}_2})$$

$$\Leftrightarrow (1\ 2)^{\tilde{v}_1} (3\ 4)^{\tilde{z}_1} = (1\ 2)^{\tilde{v}_2} (3\ 4)^{\tilde{z}_2}$$

$$\Leftrightarrow (1\ 2)^{\tilde{v}_1 - \tilde{v}_2} (3\ 4)^{\tilde{z}_1 - \tilde{z}_2} = 1_{S_4}$$

$$\Leftrightarrow \tilde{v}_1 - \tilde{v}_2 = 0, \tilde{z}_1 - \tilde{z}_2 = 0$$

$$\Leftrightarrow \tilde{v}_1 = \tilde{v}_2, \tilde{z}_1 = \tilde{z}_2$$

$\therefore \phi_8$  は単射.  $\square$

c)  $H_5 = \{1, 2, 3, 4\}$  かつ  $|H_5| = 4$ ,  $\{2\}$  は  $H_5$  に生成される.

(d)  $\phi_5: H_5 \longrightarrow S_4$

$$2^{\tilde{v}} \longmapsto (2\ 3\ 4\ 1)^{\tilde{v}} \quad (\tilde{v} \in \mathbb{Z}/4\mathbb{Z})$$

$\hookrightarrow$  定義する.  $\mathbb{Z}/4\mathbb{Z} \ni \tilde{v}, \tilde{z} \mapsto \tilde{v} + \tilde{z}$

$$\phi_5(2^{\tilde{v}} \cdot 2^{\tilde{z}}) = \phi_5(2^{\tilde{v} + \tilde{z}})$$

$$= (2\ 3\ 4\ 1)^{\tilde{v} + \tilde{z}} = (2\ 3\ 4\ 1)^{\tilde{v}} (2\ 3\ 4\ 1)^{\tilde{z}}$$

$$= \phi_5(2^{\tilde{v}}) \phi_5(2^{\tilde{z}}) \quad \therefore \text{任意の } \phi_5 \text{ は準同型}$$

次に:  $\forall 2^{\tilde{v}}, 2^{\tilde{z}} \in H_5 (\tilde{v}, \tilde{z} \in \mathbb{Z}/4\mathbb{Z})$  について

$$\phi_5(2^{\tilde{v}}) = \phi_5(2^{\tilde{z}}) \Leftrightarrow (2\ 3\ 4\ 1)^{\tilde{v}} = (2\ 3\ 4\ 1)^{\tilde{z}} \Leftrightarrow (2\ 3\ 4\ 1)^{\tilde{v} - \tilde{z}} = 1_{S_4}$$

$$\Leftrightarrow \tilde{v} - \tilde{z} = 0 \Leftrightarrow \tilde{v} = \tilde{z}$$

$\therefore \phi_5$  は単射  $\square$