

(1) (a)

H が G の部分群である $\Leftrightarrow H \leq G \Leftrightarrow \forall h_1, h_2 \in H, (h_1 h_2)^{-1} \in H$

・条件 = G が可換群である。

$$H \leq G \Leftrightarrow \forall h_1, h_2 \in H, h_1 h_2^{-1} \in H$$

$$(h_1 h_2)^{-1} = h_2^{-1} h_1^{-1}$$

$$= h_1 h_2^{-1}$$

$$h_1 h_2^{-1} \in H, h_2 h_2^{-1} \in K \text{ であるから}$$

$$h_1 h_2^{-1} h_2 h_2^{-1} \in H \cap K$$

(b)

G を 3 次の置換群 $\{ \sigma \mid (\sigma(1) \ \sigma(2) \ \sigma(3)) \}$

$H = \{ (1 \ 2 \ 3), (1 \ 3 \ 2) \}$, $K = \{ (1 \ 2 \ 3), (2 \ 1 \ 3) \}$ とする。

H, K は G の部分群である。また、 $H \cap K$ は

$$H \cap K = \{ (1 \ 2 \ 3) (1 \ 2 \ 3), (1 \ 2 \ 3) (2 \ 1 \ 3),$$

$$(1 \ 3 \ 2) (1 \ 2 \ 3), (1 \ 3 \ 2) (2 \ 1 \ 3) \}$$

$$= \{ (1 \ 2 \ 3), (2 \ 1 \ 3), (1 \ 3 \ 2), (3 \ 1 \ 2) \}$$

とある。 $H \cap K \ni (2 \ 1 \ 3), (3 \ 1 \ 2) \notin H$

$$(2 \ 1 \ 3) (3 \ 1 \ 2) = (3 \ 2 \ 1) \notin H \cap K \text{ であるから}$$

$H \cap K$ は G の部分群ではない。

(2)

(a) 第1同型定理より

$$H/\text{Ker } \phi \cong G$$

であるから、

$$|H/\text{Ker } \phi| = |H|/|\text{Ker } \phi| = |G|$$

$$\Leftrightarrow |H| = |G| |\text{Ker } \phi|$$

である。また、

$$G = \langle g_1 \rangle \times \langle g_2 \rangle$$

$$\cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\cong \mathbb{Z}/14\mathbb{Z}$$

$\therefore |G| = 14$ である。 $|H|$ は 14 の倍数。

$$|\cup(\mathbb{Z}/p_i^{e_i}\mathbb{Z})| = p_i^{e_i-1}(p_i-1) \quad \dots \textcircled{1} \quad (p_i: \text{素数}, e_i \in \mathbb{Z}, e_i \geq 1)$$

また、

相異なる素数 p_1, \dots, p_m 及び $e_1, \dots, e_m \in \mathbb{Z}, e_1, \dots, e_m \geq 1$ に対し、CRT, ①より、

$$\begin{aligned} |\cup(\mathbb{Z}/(p_1^{e_1} \cdots p_m^{e_m})\mathbb{Z})| &= \prod_{i=1}^m |\cup(\mathbb{Z}/p_i^{e_i}\mathbb{Z})| \\ &= \prod_{i=1}^m (p_i^{e_i-1}(p_i-1)) \quad \dots \textcircled{2} \end{aligned}$$

$|H_n|$ が ①か②のいずれかに等しくなるような p_i, e_i はある。

• $|H| = 14$ のとき、②式に $n=1$ と、成立する p_i, e_i の組、及び m は存在しない。

$$\left(\begin{array}{l} p_i = 2, e_i = 2 \text{ のとき、 } p_i^{e_i-1}(p_i-1) = 2 \text{ となるから、} \\ p_i^{e_i-1}(p_i-1) = 7 \text{ となる } p_i, e_i \text{ は存在しないため。} \end{array} \right)$$

よって、不適当。

$|H| = 280 \text{ 個}$ 、①式に代入して、 $p_i = 29$, $e_i = 1$ とすれば成立する。

よって、最小の n は $n = 29$ //

また、 $\forall (g_1^i, g_2^j) \in G$ に対して、 (i, j) が存在すれば、
 全射と分かる。

$$H_{29} = U(\mathbb{Z}/29\mathbb{Z}) \cong \mathbb{Z}/28\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

$$\text{よって } (i, j) \in \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

のようた (i, j) をとればよい

(b)

H_{29} の生成元の集合は、 $\{7, 17\}$ であり、 $\text{ord}(7) = 7$, $\text{ord}(17) = 4$
 と分かる。

$$\phi : H_{29} \longrightarrow G$$

$$7^i 17^j \longmapsto (g_1^i, g_2^j) \quad (i, j \in \mathbb{Z}) \quad \text{と定めて}$$

$$H_{29} \ni 7^{\hat{i}_1} 17^{\hat{j}_1}, 7^{\hat{i}_2} 17^{\hat{j}_2} \text{ に対して}$$

$$\phi(7^{\hat{i}_1} 17^{\hat{j}_1} \cdot 7^{\hat{i}_2} 17^{\hat{j}_2}) = \phi(7^{\hat{i}_1 + \hat{i}_2} \cdot 17^{\hat{j}_1 + \hat{j}_2})$$

$$= (g_1^{\hat{i}_1 + \hat{i}_2}, g_2^{\hat{j}_1 + \hat{j}_2})$$

$$= (g_1^{\hat{i}_1}, g_2^{\hat{j}_1}) (g_1^{\hat{i}_2}, g_2^{\hat{j}_2})$$

$$= \phi(7^{\hat{i}_1} 17^{\hat{j}_1}) \phi(7^{\hat{i}_2} 17^{\hat{j}_2}) \quad \square$$

(C) G の部分群 G' に対し、準同型定理より、

$$H/\text{Ker}\phi \cong G' \subset G$$

である。今、 ϕ は単射であるから $|\text{Ker}\phi| = 1$ であり、

$$|H/\text{Ker}\phi| = |H| / |\text{Ker}\phi| = |G'|$$

$$\Leftrightarrow |H| = |G'|$$

ラグランジュの定理より $|G'|$ は、 $|G| = 14$ の約数。

$\therefore |H| = 1, 2, 7, 14$ のいずれかである。

○ $|H| = 1$ のとき、

①式において、 $p_i = 2, e_i = 1$ のときのみ成立。 $n = 2$ となる。

○ $|H| = 7$ のとき、

①式を満たさなうから p_i, e_i は存在しない。

○ $|H| = 14$ のとき、

(A) と同様にし、不適切。

○ $|H| = 2$ のとき、

②) において、 $|U(\mathbb{Z}/p_1^{e_1} \cdots p_m^{e_m})\mathbb{Z}| = 2$ となるように

(p_i, e_i) , m のうち、 n が最大となるのは、

$m = 2, p_1 = 2, e_1 = 1, p_2 = 3, e_2 = 1$ であり、このときの n は

$$n = 6 //$$

(d) H_6 の生成元は $5\mathbb{Z}$ にあらず。

$$\phi: H_6 \longrightarrow G$$

$$5^{\tilde{v}} \longmapsto (1, \beta_2^{\tilde{v}}) \quad (\tilde{v} \in \mathbb{Z}) \quad \text{ただし}$$

$$H_6 \ni 5^{\tilde{v}_1}, 5^{\tilde{v}_2} (=x \neq 1,$$

$$\phi(5^{\tilde{v}_1}, 5^{\tilde{v}_2}) = \phi(5^{\tilde{v}_1 + \tilde{v}_2})$$

$$= (1, \beta_2^{\tilde{v}_1 + \tilde{v}_2})$$

$$= (1, \beta_2^{\tilde{v}_1}) (1, \beta_2^{\tilde{v}_2})$$

$$= \phi(5^{\tilde{v}_1}) \phi(5^{\tilde{v}_2}) \quad \square$$

(3)

$90 = 2 \times 3^2 \times 5$ で表わす。

$p=2, q=3^2=9, r=5$ とする。

オイラー関数 φ について、 $\varphi(p)=1, \varphi(q)=6, \varphi(r)=4$ である。

$7 \cdot 7^{29} \bmod p \equiv 1^{29} \equiv 1 \quad \dots \textcircled{1}$

$7 \cdot 7^{29} \bmod q \equiv 5^{29} \equiv (5^6)^4 \cdot 5^5 \equiv 5^5 \equiv 2 \quad \dots \textcircled{2}$

$7 \cdot 7^{29} \bmod r \equiv 2^{29} \equiv (2^4)^7 \cdot 2 \equiv 2 \quad \dots \textcircled{3}$

$px + ry = 1$ となる x, y を求める。 $x = -2, y = 1$ である。

$S_1 = px = -8, S_2 = 5$ とする。

$7 \cdot 7^{29} \bmod pr \equiv S_1 \cdot 2 + S_2 \cdot 1 \equiv -8 + 5 \equiv 7 \quad \dots \textcircled{4}$

また、 $prx + qy = 1$ となる x, y を求める。 $x = 1, y = -1$ である。

$S_1 = prx = 10, S_2 = qy = -9$ とする。

$7 \cdot 7^{29} \bmod pqr \equiv S_1 \cdot 2 + S_2 \cdot 7 \equiv 20 - 63 \equiv -43 \equiv 47 \quad \dots \textcircled{5}$

法の部分割や、一次不定方程式を解く際には、オンラインで計算可能であるため、実際の計算量の測定には、それ以外の部分を考えるはない。

計算量の指標として、法乗算を数える。

- | | |
|--------|-------------|
| ① : 0回 | ④ : 2回 |
| ② : 4回 | ⑤ : 2回 |
| ③ : 0回 | 計 : 8回 とする。 |

①, ②, ③ においては、オイラーの定理を用いた計算量の削減が可能である。オイラー関数の値は互いに素な小さい値を出力する傾向にあるため、法の値は、小さいほど小さいと考える。

このように剰余の分割をした。