(1) (a)

HK が G の部分群となる $\Longleftrightarrow$ $HK \ni {}^{\forall} h_1k_1, h_2k_2$, $(h_1k_1)(h_2k_2)^{-1} \in HK$

・条件：G が可換群である.

$HK \ni {}^{\forall} h_1k_1, h_2k_2$ に対し

$(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}$

$= h_1h_2^{-1}k_1k_2^{-1}$

$h_1h_2^{-1} \in H$, $k_1k_2^{-1} \in K$ であるから.

$h_1h_2^{-1}k_1k_2^{-1} \in HK$

(b)

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

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

H, K は G の部分群である。また. HK は

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

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

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

となる。$HK \ni (2\ 1\ 3), (3\ 1\ 2)$ に対し

$(2\ 1\ 3)(3\ 1\ 2) = (3\ 2\ 1) \notin HK$ であるから

HK は G の部分群ではない.

(2)

(a) 準同型定理より、

$H/\mathrm{Ker}\,\phi \cong G$

であるから、

$|H/\mathrm{Ker}\,\phi| = |H|/|\mathrm{Ker}\,\phi| = |G|$

$\Leftrightarrow |H| = |G|\,|\mathrm{Ker}\,\phi|$

となる。また、

$G_1 = \langle e_{71}\rangle \times \langle e_{72}\rangle$

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

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

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

$|U(\mathbb{Z}/p_i^{e_i}\mathbb{Z})| = p_i^{e_i-1}(p_i-1)$ ・・・ ① (p_i:素数, $e_i \in \mathbb{Z}$, $e_i \geq 1$)

また、

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

$$|U(\mathbb{Z}/p_1^{e_1}\cdots p_m^{e_m}\mathbb{Z})| = \prod_{i=1}^{m} |U(\mathbb{Z}/p_i^{e_i}\mathbb{Z})|$$

$$= \prod_{i=1}^{m} \left(p_i^{e_i-1}(p_i-1)\right) \quad \cdots ②$$

$|H_n|$ が①かつ②のいずれかに等しくなるような n があればよい。

・$|H| = 14$ のとき、②式について、成立する p_i, e_i の組、及び m は存在しない

($p_i = 2, e_i = 2$ のとき、$p_i^{e_i-1}(p_i-1) = 2$ となるが、

$p_i^{e_i-1}(p_i-1) = 7$ となる p_i, e_i は存在しないため。)

よって、不適。

・$|H|=28$ のとき、(1)の式において、$p_i=29$, $e_i=1$ とすれば成立する。
よって、最小の n は $n=29$ //
また、$\forall(\zeta_7^{i}, \zeta_2^{j}) \in G$ に対して、(i,j) が存在すれば、
全射となるわけ。
$H_{29} = U(\mathbb{Z}/29\mathbb{Z}) \cong \mathbb{Z}/28\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
より、$(i,j) \in \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
のような (i,j) をとればよい

(6)
H_{29} の生成元の集合は、$\{17, 17^3\}$ であり、$\mathrm{ord}(17)=7$, $\mathrm{ord}(17^3)=4$
となるから、

$$\phi : H_{29} \longrightarrow G$$
$$17^i 17^j \longmapsto (\zeta_7^{i}, \zeta_2^{j}) \quad (i,j \in \mathbb{Z}) \text{ とすると、}$$

$H_{29} \ni 17^{i_1}17^{j_1}, 17^{i_2}17^{j_2}$ に対し、
$\phi(17^{i_1}17^{j_1} \cdot 17^{i_2}17^{j_2}) = \phi(17^{i_1+i_2} \cdot 17^{j_1+j_2})$
$= (\zeta_7^{i_1+i_2}, \zeta_2^{j_1+j_2})$
$= (\zeta_7^{i_1}, \zeta_2^{j_1})(\zeta_7^{i_2}, \zeta_2^{j_2})$
$= \phi(17^{i_1}17^{j_1})\phi(17^{i_2}17^{j_2})$ ■

(C) Gの部分群 G' に対し、準同型定理より
$H_n/\mathrm{Ker}\phi \cong G' \subset G$
である。今、ϕは単射であるから$|\mathrm{Ker}\phi|=1$であり、
$|H_n/\mathrm{Ker}\phi| = |H_n|/|\mathrm{Ker}\phi| = |G'|$
$\Leftrightarrow |H_n| = |G'|$
ラグランジュの定理より$|G'|$は、$|G|=14$の約数。
$\therefore |H_n| = 1, 2, 7, 14$ のいずれかである。

- $|H_n|=1$ のとき
  ①式において、$p_i=2$, $e_i=1$のときの2成立。$n=2$ となる。
- $|H_n|=7$のとき
  ①式を満たすようなp_i, e_iは存在しない
- $|H_n|=14$のとき
  (a)と同様にして、不適切。
- $|H_n|=2$ のとき
  自然数において、$|U(\mathbb{Z}/(p_1^{e_1}\cdots p_m^{e_m})\mathbb{Z}|=2$ となるような
  (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 6 であるから.

$\phi : H_6 \longrightarrow G$

$\zeta^i \longmapsto (1, \zeta_2^i)$ $(i \in \mathbb{Z})$ とすると

$H_6 \ni \zeta^{i_1}, \zeta^{i_2}$ に対し,

$\phi(\zeta^{i_1} \cdot \zeta^{i_2}) = \phi(\zeta^{i_1+i_2})$

$= (1, \zeta_2^{i_1+i_2})$

$= (1, \zeta_2^{i_1})(1, \zeta_2^{i_2})$

$= \phi(\zeta^{i_1})\phi(\zeta^{i_2})$ ■

(3)

$90 = 2 \times 3^2 \times 5$ であるから.

$p=2,\ q=3^2=9,\ r=5$ とする.

オイラー関数 φ に対し, $\varphi(p)=1,\ \varphi(q)=6,\ \varphi(r)=4$ である.

$7^{7^{29}} \bmod p \equiv 1^{29} \equiv 1$ ・・・①

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

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

$px+ry=1$ となる $\mathbb{Z}$ の x, y を求めると. $x=-2,\ y=1$ であるから.

$s_1 = px = -4,\ s_2 = 5$ とすると.

$7^{7^{29}} \bmod pr \equiv s_1 \cdot 2 + s_2 \cdot 1 \equiv -8+5 \equiv 7$ ・・・④

また. $prx+qy=1$ となる $\mathbb{Z}$ の x, y を求めると. $x=1,\ y=-1$ であるから.

$s_1 = prx = 10,\ s_2 = qy = -9$ とすると

$7^{7^{29}} \bmod pqr \equiv s_1 \cdot 2 + s_2 \cdot 7 \equiv 20 - 63 \equiv -43 \equiv 47$ // ・・・⑤

法の分割や, 一次不定方程式を解く際には, オフラインで計算可能である.
そのため, 実際の計算量の測定には, それ以外の部分を考えればよい.
計算量の指標として, 法乗算を考えると

①：0回　　④：2回

②：4回　　⑤：2回

③：0回　　計：8回　　となる.

①, ④, ⑤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引数が小さいほど小さい値を出力する傾向にあるため, 法の値は, 小さいほど好ましいと考え,
このような剰余の分割をとった。