問6.1

(1)「群Gに対し、Gが巡回群かつ群の位数の約数がk個存在するならば、Gの部分群の個数はkとなる。」①

①において$k=4$となる最小のnは、$n=7$。部分群と生成元は、

$\langle 1\rangle=\{1\}$, $\langle 6\rangle=\{1,6\}$, $\langle 2\rangle=\langle 4\rangle=\{1,2,4\}$,

$\langle 3\rangle=\langle 5\rangle=\{1,2,3,4,5,6\}$

(2) ①において$k=3$となればよい。約数の個数が3になるのは、もとの群の位数が素数の二乗と等しいときである。

(3) $U(\mathbb{Z}/n\mathbb{Z})$が巡回群とならない最大の$n$を求めればよい。

互いに素な$k,l\in\mathbb{N}$に対し、$U(\mathbb{Z}/k\mathbb{Z})$, $U(\mathbb{Z}/l\mathbb{Z})$が巡回群かつその部分群の個数が2以上であるとき、$U(\mathbb{Z}/kl\mathbb{Z})$は巡回群とならない。

$n\leq 20$なるnに対し、この条件を満たすk,lは$k=4, l=5$のときであり、$n=20$となる。

問6.2

$2^{13} \bmod p_1 = 0$

$2^{13} \bmod p_2 = 17$

$2^{13} \bmod p_3 = 8$

である。

$2^{13} \bmod p_2 p_3$ を求めるために $p_2 x + p_3 y = 1$ を満たす x, y を求めると、$x = 4$, $y = -9$ となる。

よって $S_1 = 25 \cdot 4 = 100$, $S_2 = 11 \cdot (-9) = -99$

$2^{13} \bmod p_2 p_3 = (17 \cdot (-99) + 8 \cdot 100) \bmod 275 = 217$

次に、$2^{13} \bmod p_1 p_2 p_3$ を求めるために、$p_1 x + p_2 p_3 y$ を満たす x, y を求めると $x = 43$, $y = -5$ となる。

よって $S_1 = 32 \cdot 43 = 1376$, $S_2 = 275 \cdot (-5) = -1375$

$\therefore 2^{13} \bmod p_1 p_2 p_3 = (217 \cdot 1376 + 0 \cdot (-1375)) \bmod 8800 = 8192$