1) $\mathbb{Z}_6 = \{0, 1, \ldots, 5\}$

Thm 4.2

$a \in G$, $|a| = n$, $k \in \mathbb{N}$

(i) $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

(ii) $|a^k| = n/\gcd(n,k)$

Pf.

Let $a \in G$, $|a| = n$, $k \in \mathbb{N}$

(i) Let $d = \gcd(n,k)$

Let $x \in \langle a^k \rangle$,

$x = a^{ki}$

Let $k = dj$,

$x = a^{dji} \in \langle a^d \rangle$

$\therefore \langle a^k \rangle \subseteq \langle a^d \rangle$

Let $x \in \langle a^d \rangle$.

$x = a^{di}$

$\gcd(n,k) = ns + kt, \quad s,t \in \mathbb{Z}$

$x = a^{(ns+kt)i}$

$= a^{nsi} a^{kti}$

$= e a^{kti}$

$= a^{kti} \in \langle a^k \rangle$

$\therefore \langle a^d \rangle \subseteq \langle a^k \rangle$

$\therefore \langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ //

(ii) Let d be a divisor of n, k

W.T.S $|a^k| = n/\gcd(n,k)$

$(a^d)^{n/d} = a^n = e$

$\therefore |a^d| \leq n/d$

Let $i \leq n/d$: $(a^d)^i = e$

$|a| = n \Rightarrow di \geq n \Rightarrow i \geq n/d$

$(\Rightarrow\Leftarrow)$

$\therefore |a^d| = n/d$

Let d be $\gcd(n,k)$,

By Thm 4.2 (i), Corollary 1,

$$|a^k| = |\langle a^k \rangle| = |\langle a^d \rangle|$$

$$= |a^d|$$

$$= n/d \;//$$

By Corollary 4,

$k \in \mathbb{Z}_n$, $k \in \mathbb{Z}$

$\langle k \rangle = \mathbb{Z}_n \iff \gcd(n, k) = 1$

$\therefore \langle k \rangle = \mathbb{Z}_6 \iff \gcd(6, k) = 1$

$k \in \{1, 5\}$

$\therefore \mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$

$\langle k \rangle = \mathbb{Z}_8 \iff \gcd(8, k) = 1$

$k \in \{1, 3, 5, 7\}$

$\therefore \mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$

$\langle k \rangle = \mathbb{Z}_{20} \iff \gcd(20, k) = 1$

$k = \{1, 3, 7, 9, 11, 13, 17, 19\}$

$\therefore \mathbb{Z}_{20} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$

$= \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle = \langle 19 \rangle$ //

3) $\langle 20 \rangle = \{20, 10, 0\}$ //

$\langle 10 \rangle = \{10, 20, 0\}$ //

Let $a \in G : |a| = 30$,

$\langle a^{20} \rangle = \{a^{20}, a^{10}, e\}$ //

$\langle a^{10} \rangle = \{a^{10}, a^{20}, e\}$ //

5) $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$

$\langle 3 \rangle = \{3, 9, 7, 1\}$ //

$\langle 7 \rangle = \{7, 9, 3, 1\}$ //

9) Thm 4.3

(i) $G = \langle a \rangle, a \in G \Rightarrow \forall H \leq G, H = \langle b \rangle, b \in H.$

(ii) $|\langle a \rangle| = n \Rightarrow H \leq \langle a \rangle, |H| \mid n$

(iii) $\forall k \mid n, k \in \mathbb{N}, \exists! H \leq \langle a \rangle :$
$|H| = k, H = \langle a^{n/k} \rangle.$

Pf.

(i) Let $G = \langle a \rangle, a \in G,$

Let $H \leq G = \langle a \rangle,$

$\forall x \in H, x = a^t,$

If $t < 0 : a^t \in H,$

then $a^{-t} \in H, -t > 0,$

$\therefore \exists a^t \in H, t > 0.$

Let $a^m \in H$, m is the least positive integer,

Let $b \in H \leq \langle a \rangle$,

$b = a^k$,

$k = mq + r$, $0 \leq r < m$

$a^k = a^{mq} a^r \Rightarrow a^r = a^{-mq} a^k \in H$

$0 \leq r < m \Rightarrow r = 0$

$\therefore k = mq \Rightarrow a^k = a^{mq} \in \langle a^m \rangle$

$\therefore H \subseteq \langle a^m \rangle$

Let $x \in \langle a^m \rangle$, $x = a^{mi}$

By closure, $a^m \in H \Rightarrow a^{mi} \in H$, $i \in \mathbb{Z}$,

$\therefore \langle a^m \rangle \subseteq H$

$\therefore H = \langle a^m \rangle$ //

(ii) Let $|\langle a \rangle| = n$

WTS $H \leq \langle a \rangle$, $|H| | n$

$|\langle a \rangle| = |a| = n$

Let $H \leq \langle a \rangle$, $|H| = k$.

By (i), $H = \langle a^m \rangle$,

$a^{mk} = e = a^n$

$\therefore n = mk \Rightarrow k | n$ //

(iii) Let $k | n$, $k \in \mathbb{N}$,

$H_1, H_2 \leq \langle a \rangle$, $|H_1| = |H_2| = k$,

$H_1 = \langle a^{m_1} \rangle, \quad H_2 = \langle a^{m_2} \rangle$

$a^{m_1 k} = e, \quad a^{m_2 k} = e$

$\therefore m_1 k = m_2 k$

$m_1 = m_2$

$\therefore H_1 = H_2$

$mk = n \Rightarrow m = n/k$

$\therefore H = \langle a^m \rangle = \langle a^{n/k} \rangle$ //

By Corollary 4.3.1,

$\forall k \mid n, \; k > 0, \; \exists! \langle n/k \rangle \leq \mathbb{Z}_n : |\langle n/k \rangle| = k$

$1, 2, 4, 5, 10, 20 \mid 20$

$\therefore \langle 20\rangle, \langle 10\rangle, \langle 5\rangle, \langle 4\rangle, \langle 2\rangle, \langle 1\rangle \leq \mathbb{Z}_{20}$

$\mathbb{Z}_{20}$ has 6 subgroups.

Let $G = \langle a\rangle$, $|a| = 20$.

By Thm 4.3 (ii),

$H \leq \langle a\rangle$, $|H| \mid 20$,

$|H| \in \{1, 2, 4, 5, 10, 20\}$

By Thm 4.3 (iii),

$\forall k \mid 20$, $\exists! H \leq \langle a\rangle : |H| = k$,

$\therefore$ G has 5 subgroups.

$H_1 = \langle a^{20}\rangle$, $H_3 = \langle a^5\rangle$, $H_5 = \langle a^2\rangle$

$H_2 = \langle a^{10}\rangle$, $H_4 = \langle a^4\rangle$, $H_6 = \langle a^1\rangle$

11) $a \in G$. WTS $\langle a^{-1} \rangle = \langle a \rangle$

Let $x \in \langle a \rangle$,

$x = a^i = (a^{-1})^{-i} \in \langle a^{-1} \rangle$

$\therefore \langle a \rangle \subseteq \langle a^{-1} \rangle$

Let $x \in \langle a^{-1} \rangle$,

$x = (a^{-1})^i = \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{i}$

$= a^{-i} \in \langle a \rangle$

$\therefore \langle a^{-1} \rangle \subseteq \langle a \rangle$

$\therefore \langle a \rangle = \langle a^{-1} \rangle$ //

13) $\mathbb{Z}_{24} = \{0, 1, \ldots, 23\}$

$\langle 21 \rangle = \{21, 18, 15, 12, 9, 6, 3, 0\}$

$\langle 10 \rangle = \{10, 20, 6, 16, 2, 12, 22, 8, 18, 4, 14, 0\}$

$\langle 21 \rangle \cap \langle 10 \rangle = \{18, 12, 6, 0\}$

$\langle 18 \rangle = \{18, 12, 6, 0\}$

$\langle 12 \rangle = \{12, 0\}$

$\langle 6 \rangle = \{6, 12, 18, 0\}$

$\langle 21 \rangle \cap \langle 6 \rangle = \langle 18 \rangle = \langle 6 \rangle$

$|a| = 24$

$\langle a^{21} \rangle = \{a^{21}, a^{18}, a^{15}, a^{12}, a^{9}, a^{6}, a^{3}, e\}$

$\langle a^{10} \rangle = \{a^{10}, a^{20}, a^{6}, a^{16}, a^{2}, a^{12}, a^{22},$

$a^8, a^{18}, a^4, a^{14}, e\}$

$\langle a^{21}\rangle \cap \langle a^{10}\rangle = \{a^{18}, a^{12}, a^6, e\}$

$\langle a^{18}\rangle = \{a^{18}, a^{12}, a^6, e\}$

$\langle a^6\rangle = \{a^6, a^{12}, a^{18}, e\}$

$\therefore \langle a^{21}\rangle \cap \langle a^{10}\rangle = \langle a^{18}\rangle = \langle a^6\rangle$ //

21) $a \in G$

a) $a^{12} = e$, $|a| \leq 12$

b) $a^m = e$, $|a| \leq m$

c) $|G| = 24$, G is cyclic,

$a^8 \neq e$, $a^{12} \neq e$

WTS $\langle a\rangle = G$

Let $x \in \langle a\rangle$,

$x = a^i$

$a \in G_1 \Rightarrow a^i \in G_1$

$\therefore \langle a \rangle \subseteq G_1$

Let $x \in G_1$,

$a \in G_1, |G_1| = 24 \Rightarrow x = a^i \in \langle a \rangle$

$\therefore G_1 \subseteq \langle a \rangle$

$\therefore \langle a \rangle = G_1$ //

29) By Thm 4.4,

$|\mathbb{Z}_{8000000}| = 8000000$,

$8 | 8000000$,

of $x \in \mathbb{Z}_{8000000}$; $|x| = 8$ is

$\phi(8) = 4$

- By Thm 4.3 (iii),

$8 \mid 8000000$,

$\mathbb{Z}_{8000000} = \langle 1 \rangle$

$|\langle (8000000/8)(1) \rangle| = |\langle 1000000 \rangle|$

$= |1000000|$

$= 8$

$\langle 1000000 \rangle$ is a unique subgroup of $\mathbb{Z}_{8000000}$.

$\langle 3000000 \rangle = \{3000000, 6000000, 1000000, 4000000, 7000000, 2000000, 5000000, 0\}$

$$= \langle 100000 \rangle$$

$$\langle 50000 \rangle = \{ 50000, 20000, 10000, 5000, 2000, 1000, 500, 200, 100, 50, 20, 10, 5, 2, 1, 0 \}$$

$$= \{ 100000 \}$$

$$\langle 70000 \rangle = \{ 70000, 35000, 14000, 7000, 2800, 1400, 700, 280, 140, 70, 28, 14, 7, 2, 1, 0 \}$$

$$= \langle 10000 \rangle$$

$\therefore \langle 10000 \rangle, \langle 50000 \rangle, \langle 70000 \rangle$

// GCD = 10000

a^{100000}, a^{300000}, a^{500000}, a^{700000} //

31) $|G| = n$, $n \in \mathbb{N}$

$a \in G$, $e, a, a^2, \ldots, a^{n-1}, a^n = e$ //

33) $\mathbb{Z}_8 = \{0, 1, \ldots, 7\}$

$\mathbb{Z}_8 = \langle 1 \rangle$

$\langle 2 \rangle = \{2, 4, 6, 0\}$

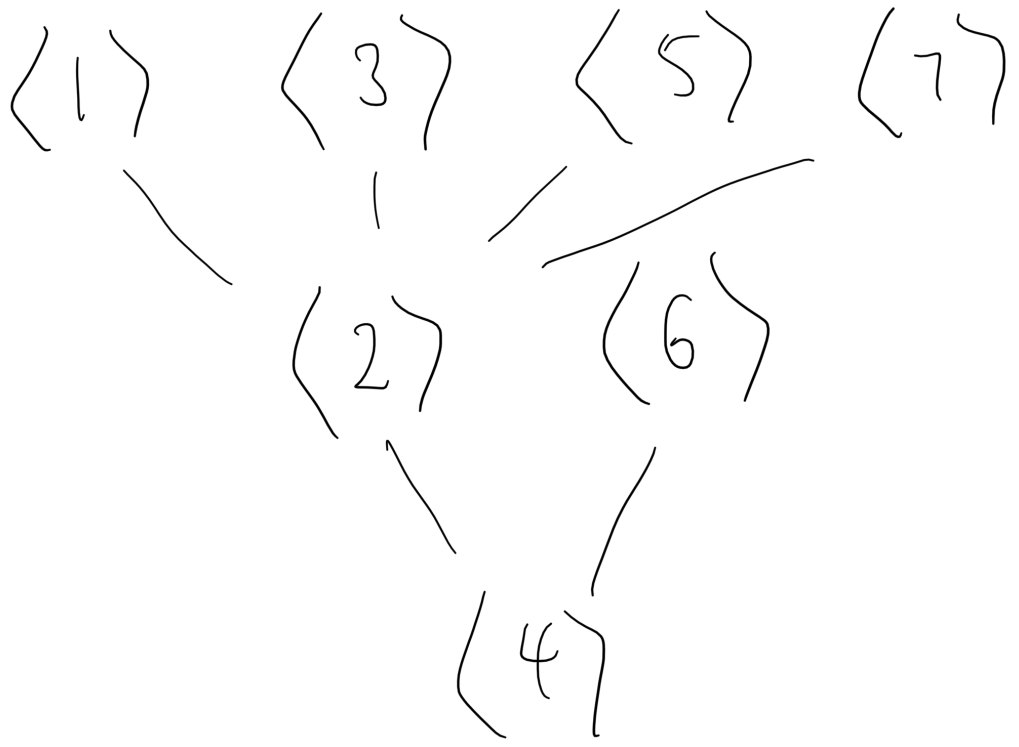
$\langle 3 \rangle = \{3, 6, 1, 4, 7, 2, 5, 0\} = \mathbb{Z}_8$

$\langle 4 \rangle = \{4, 0\}$

$\langle 5 \rangle = \{5, 2, 7, 4, 1, 6, 3, 0\} = \mathbb{Z}_8$

$\langle 6 \rangle = \{6, 4, 2, 0\} = \langle 2 \rangle$

$\langle 7 \rangle = \{7, 6, 5, 4, 3, 2, 1, 0\} = \mathbb{Z}_8$



37) $\mathbb{Z}_6$

41) $a \in G$, $|a| = 100$

By Thm 4.2,

$$|a^{98}| = 100/\gcd(100, 98)$$

$$= 100/2$$

$$= 50$$

$$|a^{70}| = 100/\gcd(100, 70)$$

$$= 100/10 = 10$$

43) $H \leq G$, $|H| = 10$.

$a \in G$, $a^6 \in H$, $|a| = ?$

$a^6 \in H$, $|H| = 10 \Rightarrow (a^6)^{10} = a^{60} = e$

$|a| \leq 60 \Rightarrow |G| \leq 60$

$|a| \in \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$

//

53) $\mathbb{Z}_{40} = \{0, 1, \ldots, 39\}$

$|\mathbb{Z}_{40}| = 40$

$4, 8, 12, 16, 20, 24, 28, 32, 36, 0$

$|4| = 10 \Rightarrow |\langle 4 \rangle| = 10$

By Thm 4.3 (iii),

$|G|40 \Rightarrow \exists H \leq \mathbb{Z}_{40} : |H| = 10$

$\langle 12 \rangle = \{12, 24, 36, 8, 20, 32, 4, 16, 28, 0\} = \langle 4 \rangle$

$\langle 28 \rangle = \{28, 16, 4, 32, 20, 8, 36, 24, 12, 0\} = \langle 4 \rangle$

$\langle 36 \rangle = \{36, 32, 28, 24, 20, 16, 12, 8, 4, 0\} = \langle 4 \rangle$

$\therefore 4, 12, 28, 36$ //

$|x| = 40, \langle x \rangle = \{x, x^2, \cdots, x^{39}, e\}$

$|x^4| = 10 = |\langle x^4 \rangle|$

$\langle x^4 \rangle = \langle x^{12} \rangle = \langle x^{28} \rangle = \langle x^{36} \rangle$

$\therefore x^4, x^{12}, x^{28}, x^{36}$ //

7) $U(8) = \{1, 3, 5, 7\}$

$\langle 1 \rangle = \{1\}$

$\langle 3 \rangle = \{3, 1\}$

$\langle 5 \rangle = \{5, 1\}$

$\langle 7 \rangle = \{7, 1\}$

8) $a \in G, |a| = 15$

a) By Thm 4.2, (ii), $a \in G$, $|a| = n$

$\Rightarrow |a^k| = n / \gcd(n, k)$

$|a^3| = 15 / \gcd(15, 3)$

$= 15/3$

$= 5, \langle a^3 \rangle = \{a^3, a^6, a^9, a^{12}, e\}$

By Thm 4.2 (i), $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$,

$\gcd(15, 6) = \gcd(15, 9) = \gcd(15, 12) = 3$

$\therefore \langle a^6 \rangle = \langle a^9 \rangle = \langle a^{12} \rangle = \langle a^3 \rangle$

$\therefore |a^6| = |a^9| = |a^{12}| = |a^3| = 5$ //

b) $|a^5| = 15/\gcd(15,5) = 5$

$\langle a^{10} \rangle = \langle a^{\gcd(15,10)} \rangle = \langle a^5 \rangle$

$\therefore |a^{10}| = |a^5| = 5$ //

c) $|a^2| = 15/\gcd(15,2) = 2$

$\gcd(15,4) = \gcd(15,8) = \gcd(15,14) = 2$

$\therefore \langle a^2 \rangle = \langle a^4 \rangle = \langle a^8 \rangle = \langle a^{14} \rangle$

$\therefore |a^2| = |a^4| = |a^8| = |a^{14}| = 2$ //

18) Let $a \in G$, $G = \langle a \rangle$

$\therefore |G| = |\langle a \rangle| = |a| = \infty$

$e \in G$, $|e| = 1$

let $|a^j| = n$,

$\therefore (a^j)^n = a^{jn} = e$

By Corollary 4.1.2,

$a^{jn} = e \iff |a| \mid jn$

But $|a| = \infty$ ($\Rightarrow\Leftarrow$)

$\therefore \{e\}$ is the only finite subgroup //

34) $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$\mathbb{Z}_8 = \langle 1 \rangle$

By Corollary 4.3.1,

$\forall k \in \mathbb{N} : k \mid n, \exists! \langle n/k \rangle \leq \mathbb{Z}_n : |\langle n/k \rangle| = k$

$\therefore H \leq \mathbb{Z}_n, |H| \mid n, H = \langle n/k \rangle$

divisors of $8 = \{0, 1, 2, 4, 8\}$

$\therefore H \in \{\langle 0\rangle, \langle 8\rangle, \langle 4\rangle, \langle 2\rangle, \langle 1\rangle\}$

$\langle 0\rangle = \{0\}$

$\langle 8\rangle = \{0\}$

$\langle 4\rangle = \{4, 0\}$

$\langle 2\rangle = \{2, 4, 6, 0\}$

$\langle 1\rangle$

|

$\langle 2\rangle$

|

$\langle 4\rangle$

|

$\langle 0\rangle$

26) $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

$\langle a \rangle = \langle a^{-1} \rangle$

52) $|U(49)| = 42$, $U(49)$ is cyclic

By Thm 4.4, G is cyclic, $|G| = n$,

$d \mid n \Rightarrow \#a \in G : |a| = d$ is $\phi(d)$.

$\therefore 42 \mid |U(49)| = 42$

$\therefore \#a \in U(49) : |a| = 42$ is

$\phi(42) = 13$ //

1, 5, 11, 13, 15, 17, 19, 23, 25, 29, 31, 37, 41