Chapter 3. The Group of Units Modulo N

3.1 Note: For $a \in \mathbb{Z}_n$, when we make a list of powers a^k for $k \in \mathbb{N}$, the list must eventually repeat (because $\mathbb{Z}_n$ is finite). In this chapter we study this repetition and consider the problem of determining how fast the list of powers of a repeats in $\mathbb{Z}_n$.

3.2 Example: If today is Tuesday, then what day will it be in 2^{100} days (under the unreasonable assumption that our solar system still exists in 2^{100} days)?

Solution: In $\mathbb{Z}_7$ we have

k	0	1	2	3	4	5
2^k	1	2	4	1	2	4

and we see that the list of powers of 2 repeats every 3 terms beginning with $2^0 = 1$. Since $100 = 1 \bmod 3$ it follows that $2^{100} = 2^1 = 2 \bmod 7$. Thus if today is Tuesday, then in 2^{100} days it will be Thursday.

3.3 Example: If it is currently 2:00 pm, then what time will it be in 2^{100} hours?

Solution: In $\mathbb{Z}_{24}$ we have

k	0	1	2	3	4	5
2^k	1	2	4	8	16	8

and we see that the list of powers of 2 repeats every 2 terms beginning with $2^3 = 8$. Since $100 = 0 = 4 \bmod 2$ we must have $2^{100} = 2^4 = 16 \bmod 24$. If it is currently 2:00 pm, then in 2^{100} hours it will be 6:00 am.

3.4 Example: Here are a few tables showing the powers a^k, until all lists of powers repeat, in $\mathbb{Z}_n$ for various values of n.

$\mathbb{Z}_2$

k	0	1	2
0^k	1	0	0
1^k	1	1	1

$\mathbb{Z}_3$

k	0	1	2	3
0^k	1	0	0	0
1^k	1	1	1	1
2^k	1	2	1	2

$\mathbb{Z}_4$

k	0	1	2	3	4
0^k	1	0	0	0	0
1^k	1	1	1	1	1
2^k	1	2	0	0	0
3^k	1	3	1	3	1

$\mathbb{Z}_5$

k	0	1	2	3	4	5
0^k	1	0	0	0	0	0
1^k	1	1	1	1	1	1
2^k	1	2	4	3	1	2
3^k	1	3	4	2	1	3
4^k	1	4	1	4	1	4

$\mathbb{Z}_6$

k	0	1	2	3
0^k	1	0	0	0
1^k	1	1	1	1
2^k	1	2	4	2
3^k	1	3	3	3
4^k	1	4	4	4
5^k	1	5	1	5

$\mathbb{Z}_7$

k	0	1	2	3	4	5	6	7
0^k	1	0	0	0	0	0	0	0
1^k	1	1	1	1	1	1	1	1
2^k	1	2	4	1	2	4	1	2
3^k	1	3	2	6	4	5	1	3
4^k	1	4	2	1	4	2	1	4
5^k	1	5	4	6	2	3	1	5
6^k	1	6	1	6	1	6	1	6

$\mathbb{Z}_8$

k	0	1	2	3	4	5
0^k	1	0	0	0	0	0
1^k	1	1	1	1	1	1
2^k	1	2	4	0	0	0
3^k	1	3	1	3	1	3
4^k	1	4	0	0	0	0
5^k	1	5	1	5	1	5
6^k	1	6	4	0	0	0
7^k	1	7	1	7	1	7

As an exercise, make a few more such tables, search for patterns, and make some conjectures. One conjecture that you might make is that, when n is a prime number, all of the rows in the table repeat every $n-1$ terms (see Fermat's Litle Theorem, below) and that, when n is a composite number, the rows repeat faster (see the Euler-Fermat Theorem).

3.5 Theorem: *(Fermat's Little Theorem) Let p be a prime number.*

(1) For all $a \in U_p$ we have $a^{p-1} = 1$. Equivalently, for all $a \in \mathbb{Z}$ with $\gcd(a,p) = 1$ we have $a^{p-1} = 1 \bmod p$.
(2) For all $a \in \mathbb{Z}_p$ we have $a^p = a$. Equivalently, for all $a \in \mathbb{Z}$ we have $a^p = a \bmod p$.

Proof: To prove Part (1), let $a \in U_p$ or, equivalently, let $a \in \mathbb{Z}$ with $\gcd(a,p) = 1$. Define $F : U_p \to U_p$ by $F(x) = ax$ (note that when a and x are units in a ring, the product ax is also a unit with $(ax)^{-1} = x^{-1}a^{-1}$, so the map F is well-defined). Notice that F is bijective with inverse $G : U_p \to U_p$ given by $G(x) = a^{-1}x$. Since F is bijective, it follows that the list of elements $1a, 2a, 3a, \cdots, (p-1)a$ is a permutation (that is a a re-orderring) of the list $1, 2, 3, \cdots, p-1$. Thus in U_p we have

$$1a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$$
$$(p-1)!\, a^{p-1} = (p-1)!$$

Multiply both sides by the inverse of $(p-1)!$ in U_p to get $a^{p-1} = 1$ in U_p, as required.

To prove Part (2), let $a \in \mathbb{Z}$ be arbitrary. If $\gcd(a,p) = 1$ then by Part (1) we have $a^{p-1} = 1 \bmod p$ and so we can multiply by a to get $a^p = a \bmod p$. If $\gcd(a,p) \neq 1$ then since p is prime it follows that $p|a$, and so we have $a = 0 \bmod p$ hence $a^p = 0^p = 0 = a \bmod p$. In either case, we have $a^p = a \bmod p$, as required.

3.6 Example: Show that $2^{70} + 3^{70}$ is not prime.

Solution: Our strategy here is to calculate $2^{70} + 3^{70} \bmod p$ for various primes p. If we find a prime p for which $2^{70} + 3^{70} = 0$ then we know that $p\big|(2^{70} + 2^{70})$ and hence $2^{70} + 3^{70}$ is not prime. In $\mathbb{Z}_2$ we have $2^{70} + 3^{70} = 0^{70} + 1^{70} = 1 \neq 0$. In $\mathbb{Z}_3$, we have $2^{70} + 3^{70} = (-1)^{70} + 0^{70} = 1 \neq 0$. In $\mathbb{Z}_5$, by Fermat's Little Theorem the list of powers of 2 and 3 repeats every 4 terms, and $70 = 2 \bmod 4$, so we have $2^{70} + 3^{70} = 2^2 + 3^2 = 4 + 9 = 3 \neq 0$. In $\mathbb{Z}_7$, the list of powers of 2 and 3 repeats every 6 terms, and $70 = 4 \bmod 6$, so we have $2^{70} + 3^{70} = 2^4 + 3^4 = 4^2 + 9^2 = 4^2 + 2^2 = 2 + 4 = 6 \neq 0$. In $\mathbb{Z}_{11}$, the list of powers of 2 and 3 repeats every 10 terms, and $70 = 0 \bmod 10$, so we have $2^{70} + 3^{70} = 2^0 + 3^0 = 1 + 1 = 2 \neq 0$. In $\mathbb{Z}_{13}$, the list of powers of 2 and 3 repeats every 12 terms, and $70 = 10 \bmod 12$, so we have $2^{70} + 3^{70} = 2^{10} + 3^{10} = 2^4 \cdot 2^4 \cdot 2^2 + 3^3 \cdot 3^3 \cdot 3^1 = 3 \cdot 3 \cdot 4 + 1 \cdot 1 \cdot 3 = 10 + 3 = 0$. Since $2^{70} + 3^{70} = 0 \in \mathbb{Z}_{13}$ it follows that $13\big|(2^{70} + 3^{70})$ in $\mathbb{Z}$, and so $2^{70} + 3^{70}$ is not prime.

3.7 Theorem: *(The Euler-Fermat Theorem) Let $n \in \mathbb{Z}^+$. For all $a \in U_n$ we have $a^{\varphi(n)} = 1$. Equivalently, for all $a \in \mathbb{Z}$ with $\gcd(a,n) = 1$ we have $a^{\varphi(n)} = 1 \bmod n$.*

Proof: Let $a \in U_n$ or, equivalently, let $a \in \mathbb{Z}$ with $\gcd(a,n) = 1$. Let $\varphi = \varphi(n)$ and let $x_1, x_2, \cdots, x_\varphi$ be a list of all the elements in U_n. Define $F : U_n \to U_n$ by $F(x) = ax$. Then F is bijective with inverse $G : U_n \to U_n$ given by $G(x) = a^{-1}x$. Since F is bijective, it follows that the list $ax_1, ax_2, \cdots, ax_\varphi$ is a permutation of the list $x_1, x_2, \cdots, x_\varphi$, and so in U_n we have

$$ax_1 \cdot ax_2 \cdot \ldots \cdot ax_\varphi = x_1 \cdot x_2 \cdot \cdots \cdot x_\varphi$$
$$\Big(\prod_{i=1}^{\varphi} x_i\Big) a^\varphi = \prod_{i=1}^{\varphi} x_i$$

Multiply both sides by the inverse of $\prod\limits_{i=1}^{\varphi} x_i$ in U_n to get $a^\varphi = 1$ in U_n, as required.

3.8 Remark: For any finite abelian group G, the above proof is valid and it shows that $a^{|G|} = e$ for all $a \in G$. The same result holds even in non-abelian finite groups, but a different proof is required.

3.9 Theorem: *(The Refined Euler-Fermat Theorem) Let* $n = \prod {p_i}^{k_i}$ *where* $p_1, \cdots, p_\ell$ *are distinct prime numbers and* $k_1, \cdots, k_\ell \in \mathbb{Z}^+$*. Let* $\kappa = \kappa(n) = \max\{k_1, k_2, \cdots, k_\ell\}$ *and let* $\psi = \psi(n) = \operatorname{lcm}\big(\varphi({p_1}^{k_1}), \varphi({p_2}^{k_2}), \cdots, \varphi({p_\ell}^{k_\ell})\big)$.

(1) For all $a \in U_n$ *we have* $a^\psi = 1$.
(2) For all $a \in \mathbb{Z}_n$ *we have* $a^{\kappa+\psi} = a^\kappa$.

Proof: To prove Part 1, suppose that $a \in U_n$ or, equivalently, let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Fix an index i. Since $\gcd(a, n) = 1$ we have $p_i \not| a$ so that $a \in U_{{p_i}^{k_i}}$. By the Euler-Fermat Theorem, we have $a^{\varphi({p_i}^{k_i})} = 1 \bmod {p_i}^{k_i}$. It follows that $a^m = 1 \bmod {p_i}^{k_i}$ for every multiple m of $\varphi({p_i}^{k_i})$ and, in particular, $a^\psi = 1 \bmod {p_i}^{k_i}$. Since $a^\psi = 1 \bmod {p_i}^{k_i}$ for all indices i, it follows that $a^\psi = 1 \bmod n$, by the Chinese Remainder Theorem.

To prove Part 2, let $a \in \mathbb{Z}$ be arbitrary. Fix an index i. Case 1: suppose that $p_i \big| a$. Then ${p_i}^{k_i} \big| a^{k_i}$ so that $a^{k_i} = 0 \in \mathbb{Z}_{{p_i}^{k_i}}$, hence $a^j = 0 \in \mathbb{Z}_{{p_i}^{k_i}}$ for all $j \geq k_i$ and so, in particular, $a^\kappa = a^{\kappa+\psi} = 0 \in \mathbb{Z}_{{p_i}^{k_i}}$. Case 2: suppose that $p_i \not| a$. Then we have $a \in U_{{p_i}^{k_i}}$, hence $a^{\varphi({p_i}^{k_i})} = 1 \in U_{{p_i}^{k_i}}$ by the Euler-Fermat Theorem, and so $a^m = 1 \in U_{{p_i}^{k_i}}$ for every multiple m of $\varphi({p_i}^{k_i})$. In particular, we have $a^\psi = 1 \in U_{{p_i}^{k_i}}$ and hence $a^{\kappa+\psi} = a^\kappa \in U_{{p_i}^{k_i}}$. In either case, we have $a^{\kappa+\psi} = a^\kappa \bmod {p_i}^{k_i}$ in $\mathbb{Z}$. Since $a^{\kappa+\psi} = a^\kappa \bmod {p_i}^{k_i}$ for all indices i, it follows from the Chinese Remainder Theorem that $a^{\kappa+\psi} = a^\kappa \bmod n$.

3.10 Remark: Part 2 of the Refined Euler-Fermat Theorem implies that for $a \in \mathbb{Z}_n$, the list of powers a^k repeats every ψ terms beginning with the term a^κ. For example, when $n = 540 = 2^2 \cdot 3^3 \cdot 5$ we have $\kappa(n) = \max\{2, 3, 1\} = 3$ and $\psi = \operatorname{lcm}\big(\phi(2^2), \varphi(3^3), \varphi(5)\big) = \operatorname{lcm}(2, 18, 4) = 36$ and so the list of powers repeats every 36 terms beginning with a^3.

For some particular values of a, the list of powers may repeat more quickly (for example when $a = 1$ the list repeats every term and when $a = n - 1 = -1$ the list repeats every 2 terms). For some particular values of n, the list of powers a^k repeats more quickly for every $a \in \mathbb{Z}_n$. Indeed, we shall see below that when $n = 8k$ the powers a^k repeat every $\psi/2$ terms for all $a \in \mathbb{Z}_n$. For example, as you can see from the last table in Example 3.4, although $\psi(8) = 4$, in $\mathbb{Z}_8$ the powers a^k repeat every 2 terms beginning with a^3.

In order to obtain a deeper understanding of the period of repetition of powers modulo n, we shall study the structure of the group of units modulo n.

3.11 Notation: When G is an *additive* group, (meaning that the operation is addition, which is commutative, and the identity element is denoted by 0) for $a \in G$ and $k \in \mathbb{Z}^+$ we write $0a = 0$, $ka = a + a + a + \cdots + a$ with k terms in the sum, and $(-k)a = -(ka)$. Verify, as an exercise, that for $a, b \in G$ and $k, \ell \in \mathbb{Z}$ we have $(-k)a = -(ka)$ and $(k+\ell)a = ka + \ell a$ and $k(a + b) = ka + kb$.

When G is a *multiplicative group* (meaning that the operation is multiplication and the identity element is denoted by e or 1 or I), we write $a^0 = e$, and $a^k = a \cdot a \cdot a \cdot \ldots \cdot a$ with k terms in the product, and $a^{-k} = (a^k)^{-1}$. Verify, as an exercise, that for $a, b \in G$ and $k, \ell \in \mathbb{Z}$ we have $a^{-k} = (a^{-1})^k$ and $a^{k+\ell} = a^k a^\ell$ and if G is abelian then $(ab)^k = a^k b^k$.

3.12 Note: When G is a finite additive group and $a \in G$, the list of multiples of a must eventually repeat, that is we must have $ka = \ell a$ for some $0 \leq k < \ell$. When $ka = \ell a$ with $0 \leq k < \ell$, we have $(\ell - k)a = \ell a - ka = 0$, and so there exists $m \in \mathbb{Z}+$ such that $ma = 0$. Similarly, when G is a finite multiplicative group and $a \in G$, the list of powers a^k must eventually repeat and there exists $m \in \mathbb{Z}^+$ such that $a^m = e$.

3.13 Definition: Let G be a finite group and let $a \in G$. The **order** of the group G, denoted by $|G|$, is the number of elements in G. When G is an *additive* group, the **order** of a in G is the smallest $m \in \mathbb{Z}^+$ such that $ma = 0$. When G is a *multiplicative* group, the **order** of a in G is the smallest $m \in \mathbb{Z}^+$ such that $a^m = e$. In either case, the order of a in G is denoted by $\operatorname{ord}(a)$ or $\operatorname{ord}_G(a)$. When $G = U_n$ we also write $\operatorname{ord}_G(a)$ as $\operatorname{ord}_n(a)$.

3.14 Definition: A **subgroup** of a group G is a subset $H \subseteq G$ which is also a group using the same operation which is used in G.

3.15 Definition: Let G be a finite group and let $a \in G$. When G is additive, we let $\langle a \rangle = \{ka \,|\, k \in \mathbb{Z}\} \subseteq G$. When G is multiplicative, we let $\langle a \rangle = \{a^k \,|\, k \in \mathbb{Z}\} \subseteq G$. In either case, verify that $\langle a \rangle$ is a subgroup of G. The group $\langle a \rangle$ is called the **cyclic group** in G **generated by** a. When $G = \langle a \rangle$ for some $a \in G$ we say that G is **cyclic**.

3.16 Example: The additive group $\mathbb{Z}_n$ is a cyclic group generated by the element 1.

3.17 Example: The multiplicative group $C_n = \{z \in \mathbb{C}^* \,|\, z^n = 1\}$ is a cyclic group in $\mathbb{C}^*$ which is generated by the element $\alpha = e^{i\,2\pi/n}$.

3.18 Example: We have $U_{18} = \{1, 5, 7, 11, 13, 17\}$. In U_{18}, we have

k	0	1	2	3	4	5	6
5^k	1	5	7	17	13	11	1

so $\operatorname{ord}_{18}(5) = 6$, and we have $\langle 5 \rangle = \{1, 5, 7, 17, 13, 11\} = U_{18}$, so that U_{18} is cyclic.

3.19 Theorem: *(Elements of a Cyclic Group) Let G be a finite group, let $a \in G$, and let $m = \operatorname{ord}_G(a)$. Then*

(1) If G is additive then for $k, \ell \in \mathbb{Z}$ we have $ka = \ell a \iff k = \ell \bmod m$.
(2) If G is multiplicative then for $k, \ell \in \mathbb{Z}$ we have $a^k = a^\ell \iff k = \ell \bmod m$.

Proof: We prove Part 2 (the proof of Part 1 is similar but uses additive notation). Let $k, \ell \in \mathbb{Z}$. Suppose that $a^k = a^\ell$. Note that $a^{\ell - k} = a^\ell a^{-k} = a^\ell (a^k)^{-1} = a^k (a^k)^{-1} = e$. Write $\ell - k = qm + r$ with $0 \leq r < n$. Then $e = a^{\ell - k} = a^{qm + r} = (a^m)^q a^r = a^r$. Since $\operatorname{ord}(a) = m$ we must have $r = 0$. Thus $\ell - k = qm$ hence $k = \ell \bmod m$. Suppose, conversely, that $k = \ell \bmod m$, say $k = \ell + qm$. Then we have $a^k = a^{\ell + qm} = a^\ell (a^m)^q = a^\ell$.

3.20 Corollary: *Let G be a finite group, let $a \in G$, and let $m = \operatorname{ord}_G(a)$. Then*

(1) If G is additive then for $k \in \mathbb{Z}$ we have $ka = 0 \iff m \big| k$.
(2) If G is multiplicative then for $k \in \mathbb{Z}$ we have $a^k = e \iff m \big| k$.

3.21 Corollary: *Let G be a finite group, let $a \in G$, and let $m = \operatorname{ord}_G(a)$.*

(1) If G is additive then $\langle a \rangle = \{0, a, 2a, 3a, \cdots, (m-1)a\}$ with the listed elements distinct.
(2) If G is multiplicative then $\langle a \rangle = \{1, a, a^2, \cdots, a^{m-1}\}$ with the listed elements distinct.

3.22 Corollary: *Let G be a finite group and let $a \in G$. Then* $\operatorname{ord}(a) = \big|\langle a \rangle\big|$.

3.23 Theorem: *(Subgroups of a Cyclic Group) Let G be finite group, let $a \in G$, and let $m = \text{ord}_G(a)$.*

(1) If G is additive then every subgroup of $\langle a\rangle$ is of the form $\langle ka\rangle$ for some $k \in \mathbb{Z}$ and for $k, \ell \in \mathbb{Z}$ we have $\langle ka\rangle = \langle \ell a\rangle \iff \gcd(k,m) = \gcd(\ell,m)$. It follows that the distinct subgroups of $\langle a\rangle$ are the groups $\langle da\rangle = \big\{0, da, 2da, \cdots, (m-d)a\big\}$ where d is a positive divisor of m.

(2) If G is multiplicative then every subgroup of $\langle a\rangle$ is of the form $\langle a^k\rangle$ for some $k \in \mathbb{Z}$ and for $k, \ell \in \mathbb{Z}$ we have $\langle a^k\rangle = \langle a^l\rangle \iff \gcd(k,n) = \gcd(l,n)$. It follows that the distinct subgroups of $\langle a\rangle$ are the groups $\langle a^d\rangle = \big\{e, a^d, a^{2d}, \cdots, a^{m-d}\big\}$ where d is a positive divisor of m.

Proof: We prove Part 2 (the proof of Part 1 is similar but uses additive notation). First we show that every subgroup of $\langle a\rangle$ is cyclic. Let H be a subgroup of $\langle a\rangle$. If $H = \{e\}$ then $H = \langle e\rangle$, which is cyclic. Suppose that $H \neq \{e\}$. Since $H \subseteq \langle a\rangle = \big\{a^k \,\big|\, k \in \mathbb{Z}\big\}$ and $H \neq \{e\}$ we can choose $0 \neq i \in \mathbb{Z}$ such that $a^i \in H$ and, since we also have $a^{-i} = (a^i)^{-1} \in H$, it follows that for $j = |i|$ we have $j \in \mathbb{Z}^+$ and $a^j \in H$. Let k be the smallest positive integer such that $a^k \in H$. We claim that $H = \langle a^k\rangle$. Since $a^k \in H$ and H is a group, it follows that $(a^k)^j \in H$ for all $j \in \mathbb{Z}$ and so $\langle a^k\rangle \subseteq H$. Let $a^\ell \in H$, where $\ell \in \mathbb{Z}$. Write $\ell = kq + r$ with $0 \leq r < k$. Then $a^\ell = a^{kq}a^r$ so we have $a^r = a^\ell (a^{kq})^{-1} \in H$. By our choice of k we must have $r = 0$, so $\ell = qk$ and hence $a^\ell \in \langle a^k\rangle$. Thus $H \subseteq \langle a^k\rangle$.

Note that for any divisor $d\big|m$ we have $\langle a^d\rangle = \big\{a^0, a^d, a^{2d}, \cdots, a^{m-d}\big\}$ with the listed elements distinct so that $\text{ord}(a^d) = \frac{m}{d}$. We claim that $\langle a^k\rangle = \langle a^d\rangle$ where $d = \gcd(k,m)$. Since $d\big|k$ we have $a^k \in \langle a^d\rangle$ so $\langle a^k\rangle \subseteq \langle a^d\rangle$. Choose $s, t \in \mathbb{Z}$ so that $ks + mt = d$. Then $a^d = a^{ks+mt} = (a^k)^s (a^m)^t = (a^k)^s \in \langle a^k\rangle$ and so $\langle a^d\rangle \subseteq \langle a^k\rangle$. Thus $\langle a^k\rangle = \langle a^d\rangle$, as claimed. Now if $\langle a^k\rangle = \langle a^\ell\rangle$ and $d = \gcd(k,m)$ and $c = \gcd(\ell,m)$ then $\langle a^d\rangle = \langle a^k\rangle = \langle a^\ell\rangle = \langle a^c\rangle$ and so $\big|\langle a^d\rangle\big| = \big|\langle a^c\rangle\big|$, that is $\frac{m}{d} = \frac{m}{c}$, and so $d = c$. Conversely, if $d = \gcd(k,m) = \gcd(\ell,m) = c$ then we have $\langle a^k\rangle = \langle a^d\rangle = \langle a^\ell\rangle$.

3.24 Corollary: *(Orders of Elements in a Cyclic Group) Let G be a finite group, let $a \in G$, and let $m = \text{ord}_G(a)$.*

(1) If G is additive then for $k \in \mathbb{Z}$ we have $\text{ord}_G(ka) = \frac{m}{\gcd(k,m)}$.
(2) If G is multiplicative then for $k \in \mathbb{Z}$ we have $\text{ord}_G(a^k) = \frac{m}{\gcd(k,m)}$.

3.25 Corollary: *(Generators of a Cyclic Group) Let G be a finite group, let $a \in G$, and let $m = \text{ord}_G(a)$. Then*

(1) If G is additive then for $k \in \mathbb{Z}$ we have $\langle ka\rangle = \langle a\rangle \iff \gcd(k,m) = 1$.
(2) If G is multiplicative then for $k \in \mathbb{Z}$ we have $\langle a^k\rangle = \langle a\rangle \iff \gcd(k,m) = 1$.

3.26 Corollary: *(The Number of Elements of Each Order in a Cyclic Group) Let G be a finite group, let $a \in G$, and let $m = \text{ord}_G(a)$. Then the order of each element in $\langle a\rangle$ is a positive divisor of m and, for each positive divisor $d\big|m$, the number of elements in $\langle a\rangle$ of order d is equal to $\varphi(d)$.*

3.27 Corollary: *For $n \in \mathbb{Z}^+$ we have $\sum\limits_{d|n} \varphi(d) = n$.*

3.28 Exercise: To illustrate the above corollaries, for each subgroup of $\mathbb{Z}_{12}$, list all of the elements in the subgroup and circle all the elements which generate the subgroup. Then do the same for the group $C_{12} = \langle \alpha\rangle = \big\{\alpha^k \,\big|\, k \in \mathbb{Z}_{12}\big\}$ where $\alpha = e^{i\,\pi/6}$.

3.29 Definition: Let G be a group using the operation $*$ and let H be a group using the operation $\times$. An **isomorphism** from G to H is a bijective function $\phi : G \to H$ such that $\phi(a * b) = \phi(a) \times \phi(b)$ for all $a, b \in G$. Note that when $\phi : G \to H$ is an isomorphism, the inverse map $\psi = \phi^{-1} : H \to G$ is also an isomorphism because, given $c, d \in H$, if we let $a = \psi(c)$ and $b = \psi(d)$ so that $c = \phi(a)$ and $d = \phi(b)$, then we have

$$\psi(c \times d) = \psi\big(\phi(a) \times \phi(b)\big) = \psi\big(\phi(a * b)\big) = a * b = \psi(c) * \psi(d).$$

When there exists an isomorphism from G to H we say that G and H are **isomorphic** and we write $G \cong H$.

3.30 Remark: In algebra, isomorphic groups are considered to be essentially equivalent.

3.31 Example: Let G be a finite group, let $a \in G$, and let $m = \text{ord}_{_G}(a)$. Then the map $\phi : \mathbb{Z}_n \to \langle a \rangle$ given by $\phi(k) = a^k$ is an isomorphism, so we have $\langle a \rangle \cong \mathbb{Z}_m$. Thus all cyclic groups of order m are isomorphic.

3.32 Theorem: *Let $\phi : G \to H$ be an isomorphism of finite groups. Then*
(1) $\phi(e_{_G}) = e_{_H}$,
(2) $\phi(a^{-1}) = \phi(a)^{-1}$ for all $a \in G$,
(3) $\phi(a^k) = \phi(a)^k$ for all $a \in G$ and all $k \in \mathbb{Z}$,
(4) $\text{ord}_{_G}(a) = \text{ord}_{_H}\big(\phi(a)\big)$ for all $a \in G$, and hence
(5) G and H have the same number of elements of each order.

Proof: To prove Part 1 note that $\phi(e_G) \times \phi(e_G) = \phi(e_{_G} * e_{_G}) = \phi(e_{_G})$, then multiply both sides by the inverse of $\phi(e_{_G})$ in H to get $\phi(e_{_G}) = e_H$. To prove part 2, note that for $a \in G$ we have $\phi(a) \times \phi(a^{-1} = \phi(a * a^{-1}) = \phi(e_{_G}) = e_{_H}$, then multiply both sides on the left by the inverse of $\phi(a)$ in H to get $\phi(a^{-1}) = \phi(a)^{-1}$. Part 3 holds for $k = 0$ by Part 1, and it holds for $k > 0$ by induction, and it holds for $k < 0$ by Part 2. Part 4 then follows because for $a \in G$ we have $a^k = e_{_G} \iff \phi(a^k) = \phi(e_{_G}) \iff \phi(a)^k = e_{_H}$. Part 5 then follows because, by Part 4, for each $d \in \mathbb{Z}^+$ the map $\phi : G \to H$ restricts to give a bijective map from the set $\big\{a \in G \,\big|\, \text{ord}_{_G}(a) = d\big\}$ to the set $\big\{b \in H \,\big|\, \text{ord}_{_H}(b) = d\big\}$.

3.33 Remark: There is a converse to Part 5, for finite abelian groups, which is considerably more difficult to prove: if G and H are finite abelian groups which have the same number of elements of each order then $G \cong H$.

3.34 Definition: If G and H are groups with identities $e_{_G}$ and $e_{_H}$, then the **product**

$$G \times H = \big\{(a, b)\big|a \in G, b \in H\big\}$$

is a group under the operation given by $(a, b)(c, d) = (ac, bd)$ with identity $e_{_{G\times H}} = (e_{_G}, e_{_H})$. More generally, if $G_1, G_2, \cdots, G_n$ are groups then the product

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n = \big\{(a_1, a_2, \cdots, a_n)\big|a_i \in G_i\big\}$$

is a group under the operation $(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n) = (a_1b_1, a_2b_2, \cdots, a_nb_n)$.

3.35 Example: For groups G, H, K and L, verify as an exercise that
(1) $G \times \{e\} \cong G$,
(2) $G \times H \cong H \times G$,
(3) $(G \times H) \times K \cong G \times (H \times K) \cong G \times H \times K$, and
(4) if $G \cong K$ and $H \cong L$ then $G \times H \cong K \times L$.

3.36 Note: Note that when G and H are groups we have $\big|G\times H\big| = |G|\,|H|$. Also note that for $a\in G$ and $b\in H$ we have

$$\mathrm{ord}_{{}_{G\times H}}(a,b) = \mathrm{lcm}\big(\mathrm{ord}_{{}_G}(a),\,\mathrm{ord}_{{}_H}(b)\big)\,.$$

Indeed if $\mathrm{ord}_{{}_G}(a)=n$ and $\mathrm{ord}_{{}_H}(b)=m$ then for $k\in\mathbb{Z}$ we have

$$\begin{aligned}(a,b)^k = e_{{}_{G\times H}} &\iff (a^k,b^k)=(e_{{}_G},e_{{}_H}) \iff \big(a^k=e_{{}_G} \text{ and } b^k=e_{{}_H}\big)\\ &\iff n\big|k \text{ and } m\big|k\big) \iff \ k \text{ is a common multiple of } n \text{ and } m.\end{aligned}$$

3.37 Example: Find the number of elements of each order in the group $\mathbb{Z}_9\times\mathbb{Z}_{15}$.

Solution: We use Corollary 3.26 to determine the number of elements of each order in $\mathbb{Z}_9$ and in $\mathbb{Z}_{15}$ then we use Note 3.36 to calculate $\mathrm{ord}(a,b)$ for $a\in\mathbb{Z}_9$ and $b\in\mathbb{Z}_{15}$.

$\mathrm{ord}(a)$	# of a	$\mathrm{ord}(b)$	# of b	$\mathrm{ord}(a,b)$	# of (a,b)
1	1	1	1	1	1
		3	2	3	2
		5	4	5	4
		15	8	15	8
3	2	1	1	3	2
		3	2	3	4
		5	4	15	8
		15	8	15	16
9	6	1	1	9	6
		3	2	9	12
		5	4	45	24
		15	8	45	48

Summary

$\mathrm{ord}(a,b)$	# of (a,b)
1	1
3	8
5	4
9	18
15	32
45	72

3.38 Theorem: *For all $k,\ell\in\mathbb{Z}^+$ we have $\mathbb{Z}_k\times\mathbb{Z}_\ell\cong\mathbb{Z}_{k\ell} \iff \gcd(k,\ell)=1$.*

Proof: Let $k,\ell\in\mathbb{Z}^+$. Suppose that $\gcd(k,\ell)=1$. Then

$$\mathrm{ord}_{\mathbb{Z}_k\times\mathbb{Z}_\ell}(1,1) = \mathrm{lcm}\big(\mathrm{ord}_{\mathbb{Z}_k}(1),\,\mathrm{ord}_{\mathbb{Z}_\ell}(1)\big) = \mathrm{lcm}(k,\ell)=k\ell\,.$$

Since $\big|\mathbb{Z}_k\times\mathbb{Z}_\ell\big| = k\ell = \mathrm{ord}_{\mathbb{Z}_k\times\mathbb{Z}_\ell}(1,1)$, it follows that $\mathbb{Z}_k\times\mathbb{Z}_\ell=\big\langle(1,1)\big\rangle$. Thus $\mathbb{Z}_k\times\mathbb{Z}_\ell$ is a cyclic group of order $k\ell$, so it is isomorphic to $\mathbb{Z}_{k\ell}$.

Now suppose that $\gcd(k,\ell)=d>1$. Let $a\in\mathbb{Z}_k$ and $b\in\mathbb{Z}_\ell$. Let $n=\mathrm{ord}_{\mathbb{Z}_k}(a)$ and let $m=\mathrm{ord}_{\mathbb{Z}_m}(b)$. Since $n\big|k$ and $m\big|\ell$ it follows that $\mathrm{lcm}(n,m)\big|\,\mathrm{lcm}(k,\ell)$, that is $\mathrm{ord}_{\mathbb{Z}_k\times\mathbb{Z}_\ell}(a,b)\big|\frac{k\ell}{d}$, hence $\mathrm{ord}_{Z_k\times\mathbb{Z}_\ell}(a,b)\le\frac{k\ell}{d}<k\ell$. Since $\mathbb{Z}_k\times\mathbb{Z}_\ell$ has no elements of order $k\ell$, it cannot be cyclic.

3.39 Theorem: *(Classification of Finite Abelian Groups) For every finite abelian group $G\neq\{e\}$, we have*

$$G\cong\mathbb{Z}_{{p_1}^{k_1}}\times\mathbb{Z}_{{p_2}^{k_2}}\times\cdots\times\mathbb{Z}_{{p_\ell}^{k_\ell}}$$

for some $\ell\in\mathbb{Z}^+$, some prime numbers $p_1,\cdots,p_\ell$ and some positive integers $k_1,\cdots,k_\ell$. The primes p_i and the exponents k_i are uniquely determined if we insist that $p_i\le p_{i+1}$ for all $1\le i<\ell$ and that whenever $p_i=p_{i+1}$ we have $k_i\le k_{i+1}$.

Proof: We shall omit the proof, which is quite difficult.

3.40 Remark: We shall not use the above theorem in any of our proofs, but it is relevant. Our main goal in the remainder of this chapter is to determine the structure of the group of units U_n, that is to determine how the group U_n decomposes as a product of cyclic groups of prime power order, in accordance with the Classification of Finite Abelian Groups.

3.41 Theorem: *If $n = \prod {p_i}^{k_i}$ where $p_1, \cdots, p_\ell$ are distinct prime numbers and $k_1, \cdots, k_\ell$ are positive integers, then we have*

$$U_n \cong \prod_{i=1}^{\ell} U_{{p_i}^{k_i}}\,.$$

Proof: It suffices to prove that, if $k, \ell \in \mathbb{Z}^+$ with $\gcd(k, \ell) = 1$ then $U_{k\ell} \cong U_k \times U_\ell$. Let $k, \ell \in \mathbb{Z}^+$ with $\gcd(k, \ell) = 1$. In the proof of Theorem 2.50 we showed that the map $F : U_{k\ell} \to U_k \times U_\ell$ given by $F(x) = (x, x)$ for $x \in \mathbb{Z}$ is well-defined and bijective. Since $F(xy) = (xy, xy) = (x, x)(x, y) = F(x)F(y)$ for all $x, y \in \mathbb{Z}$, it follows that F is a group isomorphism.

3.42 Theorem: *(The Group of Units Modulo 2^k) We have $U_1 = \{1\} = \langle 1 \rangle \cong \mathbb{Z}_1$ and $U_2 = \{1\} = \langle 1 \rangle \cong \mathbb{Z}_1$ and $U_4 = \{1, 3\} = \langle 3 \rangle \cong \mathbb{Z}_2$, and for $k \geq 3$ we have*

$$U_{2^k} = \left\{ \pm 5^j \,\middle|\, 0 \leq j < 2^{k-2} \right\} \cong \langle -1 \rangle \times \langle 5 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}.$$

Proof: The statements about U_1, U_2 and U_4 are clear. Let $k \geq 3$ and let $n = 2^k$ and consider the group U_n. We have $|U_n| = \varphi(n) = \varphi(2^k) = 2^{k-1}$. Note that U_n is not cyclic because, in U_n we have $(-1)^2 = 1$ and $(2^{k-1} \pm 1)^2 = 1$ so that U_n has at least 3 elements of order 2, but a cyclic group can only have $\varphi(2) = 1$ element of order 2. Let us calculate $\operatorname{ord}(5)$ (the order of the element 5 in the group U_n). By the Euler Fermat Theorem, we know that $5^{\varphi(n)} = 1$ so $\operatorname{ord}(5) \big| \varphi(n)$, that is $\operatorname{ord}(5) \big| 2^{k-1}$. Thus $\operatorname{ord}(5) = 2^j$ for some $1 \leq j \leq 2^{k-1}$. Since U_n is not cyclic, so $U_n \neq \langle 5 \rangle$, we cannot have $\operatorname{ord}(5) = 2^{k-1}$ and so $\operatorname{ord}(5) = 2^j$ for some $1 \leq j \leq 2^{k-2}$. We claim that $\operatorname{ord}(5) = 2^{k-2}$. We shall prove this by showing that $5^{2^{k-3}} \neq 1$ and $5^{2^{k-2}} = 1$ in U_n, and we shall do this by calculating $e_2\big(5^{2^j} - 1\big)$ $\big($ the exponent of 2 in the prime factorization of the number $5^{2^j} - 1\big)$, recursively. We have

$$\begin{aligned} 5^{2^0} - 1 &= 5^1 - 1 = 4 \text{ and } e_2(4) = 2, \\ 5^{2^1} - 1 &= 5^2 - 1 = 24 \text{ and } e_2(24) = 3, \\ 5^{2^2} - 1 &= 5^4 - 1 = 624 \text{ and } e_2(624) = 4. \end{aligned}$$

Let $j \geq 0$ and suppose, inductively, that $e_2\big(5^{2^j} - 1\big) = j + 2$, say $5^{2^j} - 1 = 2^{j+2}q$ where q is an odd positive integer. Then

$$5^{2^{j+1}} - 1 = \big(5^{2^j}\big)^2 - 1 = \big(2^{j+2}q + 1\big)^2 - 1 = 2^{2j+4}q^2 + 2^{j+3}q = 2^{j+3}\big(q + 2^{j+1}q\big) = 2^{j+3}r$$

where $r = q + 2^{j+1}q$ which is an odd positive integer. and so we have $e_2\big(5^{2^{j+1}} - 1\big) = j + 3$. By induction, we have $e_2\big(5^{2^j} - 1\big) = j + 2$ for all $j \geq 0$. Since $e_2\big(5^{k-3} - 1\big) = k - 1$ and $e_2\big(5^{k-2} - 1\big) = k$, it follows that $5^{k-3} - 1 \neq 0 \bmod 2^k$ and $5^{k-2} - 1 = 0 \bmod 2^k$. Thus $5^{k-3} \neq 1 \in U_n$ and $5^{k-2} = 1 \in U_n$ and so $\operatorname{ord}(5) = 2^{k-2}$ as claimed. Since $\operatorname{ord}(5) = 2^{k-2}$ we know that

$$\langle 5 \rangle = \left\{ 5^j \,\middle|\, 0 \leq j < 2^{k-2} \right\} \cong \mathbb{Z}_{2^{k-2}}.$$

Note that $5^i \neq -5^j \in U_n$ for any $i, j \in \mathbb{Z}$ because $5^i = 1 \bmod 4$ and $-5^j = -1 \bmod 4$. Since, in the group U_n, which has 2^{k-1} elements the elements 5^j with $0 \leq j < 2^{k-2}$ are distinct, and the elements -5^j with $0 \leq j < 2^{k-2}$ are distinct, and we have $5^i \neq 5^j$ for any i, j, it follows that

$$U_n = \left\{ \pm 5^j \,\middle|\, 0 \leq j < 2^{k-2} \right\}$$

with all of the listed elements distinct. Finally, note that the map $F : \langle -1 \rangle \times \langle 5 \rangle \to U_n$ given by $F(1, 5^k) = 5^k$ and $F(-1, 5^k) = -5^k$ is a group isomorphism.

3.43 Theorem: *(The Group of Units Modulo p) Let p be an odd prime number. Then*

$$U_p \cong \mathbb{Z}_{\varphi(p)} = \mathbb{Z}_{p-1}.$$

Proof: We have $|U_p| = \varphi(p) = p-1$. To show that U_p is cyclic, we need to show that there is an element $a \in U_p$ with $\operatorname{ord}(a) = p-1$, and we shall do this by showing that for every positive divisor $d\big|(p-1)$ there are exactly $\varphi(d)$ elements of order d in U_p. For each positive divisor $d\big|(p-1)$, let

$$A_d = \big\{a \in U_p \,\big|\, \operatorname{ord}(a) = d\big\}.$$

Note that U_p is equal to the disjoint union of the sets A_d and so we have

$$p-1 = |U_p| = \sum_{d|(p-1)} |A_d|\,.$$

Recall, from Corollary 3.27, that we also have $p-1 = \sum\limits_{d|(p-1)} \varphi(d)$ and so

$$\sum_{d|(p-1)} \big(\varphi(d) - |A_d|\big) = 0,$$

so it suffices to show that $|A_d| \leq \varphi(d)$ for al positive divisors $d\big|(p-1)$ (then all of the terms in the above sum are non-negative and they add to 0 so they must all be zero). Let d be a positive divisor of $p-1$. To show that $|A_d| \leq \varphi(d)$ we shall show that either $|A_d| = 0$ or $|A_d| = \varphi(d)$. Suppose that $|A_d| \neq 0$ (so $A_d \neq \emptyset$). Choose an element $a \in A_d$, that is choose $a \in U_d$ with $\operatorname{ord}(a) = d$. Then $\langle a\rangle = \big\{1, a, a^2, \cdots, a^{d-1}\big\}$ with the listed elements distinct. For each k the element $x = a^k$ satisfies $x^d = a^{kd} = (a^d)^k = 1^k = 1$, so the elements $1, a, a^2, \cdots, a^{d-1}$ are the roots in $\mathbb{Z}_p$ of the polynomial $f(x) = x^d - 1$. On the other hand, for every $x \in A_d$, since $\operatorname{ord}(x) = d$ we have $x^d = 1$, so that x is a root of the polynomial $f(x) = x^d - 1$, and so every $x \in A_d$ must be equal to one of the elements $\langle a\rangle = \big\{1, a, a^2, \cdots, a^{d-1}\big\}$. Thus A_d is equal to the set of elements of order d in $\langle a\rangle$, and we know that there are exactly $\varphi(d)$ such elements, so $|A_d| = \varphi(d)$, as required.

3.44 Theorem: *(The Group of Units Modulo p^2) Let p be an odd prime number. Then*

$$U_{p^2} \cong \mathbb{Z}_{\varphi(p^2)} = \mathbb{Z}_{p(p-1)}.$$

Indeed for $a \in \mathbb{Z}$ with $p \not| a$, if $U_p = \langle a\rangle$ then either $U_{p^2} = \langle a\rangle$ or $U_{p^2} = \langle a+p\rangle$.

Proof: Let $a \in \mathbb{Z}$ with $p \not| a$ so that $a \in U_p$ and suppose that $U_p = \langle a\rangle$ but $U_{p^2} \neq \langle a\rangle$. We claim that $U_{p^2} = \langle a+p\rangle$. Let $n = \operatorname{ord}_{p^2}(a)$. Since $\operatorname{ord}_{p^2}(a)\big|\varphi(p^2)$ we have $n\big|p(p-1)$. Also, since $a^n = 1 \bmod p^2$ we have $a^n = 1 \bmod p$ so that $a^n = 1 \in U_p$, and so n must be a multiple of $\operatorname{ord}_p(a) = p-1$. Since $n\big|p(p-1)$ and $(p-1)\big|n$, either $n = p-1$ or $n = p(p-1)$. Since we are assuming that $U_{p^2} \neq \langle a\rangle$ we cannot have $n = p(p-1)$ and so we must have $n = p-1$.

Let $m = \operatorname{ord}_{p^2}(a+p)$. Note that $a = a+p \bmod p$ so we have $U_p = \langle a\rangle = \langle a+p\rangle$. As above, we musy have $m = p-1$ or $m = p(p-1)$. We need to show that $m \neq p-1$ and we shall do this by showing that $(a+p)^{p-1} \neq 1 \bmod p^2$. By the Binomial Theorem, we have

$$(a+p)^{p-1} = a^{p-1} + (p-1)a^{p-2}\cdot p + \text{ terms involving } p^2$$

and so

$$\begin{aligned}(a+p)^{p-1} &= a^{p-1} - a^{p-2}p \bmod p^2\\ &= 1 - a^{p-2}p \bmod p^2\\ &\neq 1 \bmod p^2\end{aligned}$$

because $p \not| a$ and so $p \not| a^{p-2}$.

3.45 Theorem: *(The group of Units Modulo p^k) Let p be an odd prime number and let $k\in\mathbb{Z}^+$. Then*

$$U_{p^k}\cong\mathbb{Z}_{\varphi(p^k)}=\mathbb{Z}_{p^{k-1}(p-1)}.$$

Indeed for $b\in\mathbb{Z}$ with $p\nmid b$, if $U_{p^2}=\langle b\rangle$ then $U_{p^j}=\langle b\rangle$ for all $j\geq 2$.

Proof: Let $b\in\mathbb{Z}$ with $p\nmid b$. Let $j\geq 2$ and suppose, inductively, that $U_{p^j}=\langle b\rangle$. Note that $\varphi(p^j)=p^{j-1}(p-1)$ and $\varphi(p^{j+1})=p^j(p-1)$. We need to show that $U_{p^{j+1}}=\langle b\rangle$ and we shall do this by showing that $\operatorname{ord}_{p^{j+1}}(b)=\varphi(p^{j+1})=p^j(p-1)$. Let $m=\operatorname{ord}_{p^{j+1}}(b)$. Since $p\nmid b$ so that $b\in U_{p^{j+1}}$, we have $b^{\varphi(p^{j+1})}=1\in U_{p^{j+1}}$ and so $m\big|\varphi(p^{j+1})$, that is $m\big|p^j(p-1)$. Since $b^m=1\in U_{p^{j+1}}$, that is $b^m=1 \bmod p^{j+1}$, we also have $b^m=1 \bmod p^j$, that is $b^m=1\in U_{p^j}$, and so we must have $\varphi(p^j)\big|m$, that is $p^{j-1}(p-1)\big|m$. Since $p^{j-1}(p-1)\big|m$ and $m\big|p^j(p-1)$, it follows that either $m=p^{j-1}(p-1)$ or $m=p^j(p-1)$. We need to show that $m\neq p^{j-1}(p-1)$ and we shall do this by showing that $b^{p^{j-1}(p-1)}\neq 1 \bmod p^{j+1}$.

Consider $b^{p^{k-2}(p-1)}$. Since $U_{p^j}=\langle b\rangle$ we also have $U_{p^{j-1}}=\langle b\rangle$ so $b^{\varphi(p^{j-1})}=1\in U_{p^{j-1}}$, that is $b^{p^{j-2}(p-1)}=1 \bmod p^{j-1}$. On the other hand, since $U_{p^j}=\langle b\rangle$ we know that $b^{p^{j-2}(p-1)}\neq 1 \bmod p^j$. Since $b^{p^{j-2}(p-1)}=1 \bmod p^{j-1}$ and $b^{p^{j-2}(p-1)}\neq 1 \bmod p^j$ it follows that

$$b^{p^{j-2}(p-1)}=1+t\,p^{j-1}\text{ for some }t\in\mathbb{Z}^+\text{ with }p\nmid t.$$

By the Binomial Theorem,

$$b^{p^{j-1}(p-1)}=\big(1+tp^{j-1}\big)^p=1+t\,p^j+\tfrac{p(p-1)}{2}\,t^2p^{2j-2}+\text{ higher order terms in }p$$

so that

$$b^{p^{j-1}(p-1)}=1+tp^j \bmod p^{j+1}.$$

Since $p\nmid t$ it follows that $b^{p^{j-1}(p-1)}\neq 1 \bmod p^{j+1}$, as required.

3.46 Theorem: *(The Structure of The Group of Units Modulo n)*
(1) If $n=\prod {p_i}^{k_1}$ where $p_1,\cdots,p_\ell$ are distinct primes and $k_1,\cdots k_\ell\in\mathbb{Z}^+$ then

$$U_n\cong\prod_{i=1}^{\ell}U_{{p_i}^{k_i}}.$$

(2) We have $U_1\cong U_2\cong\mathbb{Z}_1$ and $U_4\cong\mathbb{Z}_2$ and for $k\geq 3$ we have $U_{2^k}\cong\mathbb{Z}_2\times\mathbb{Z}_{2^{k-2}}$.
(3) If p is an odd prime and $k\in\mathbb{Z}^+$ then $U_{p^k}\cong\mathbb{Z}_{p^{k-1}(p-1)}$.

Proof: This is just a summary of the 5 previous theorems.

3.47 Exercise: Find the number of elements of each order in the group U_{980}.

3.48 Definition: For a finite abelian group G, the **universal exponent** of G, denoted by $\lambda(G)$, is the maximum of the orders of the elements in G. When $G=U_n$, the universal exponent is also called the **Carmichael exponent** of n and we write $\lambda(n)=\lambda(U_n)$.

3.49 Note: By the above Structure Theorem, when $n=\prod {p_i}^{k_i}$, where $p_1,\cdots,p_\ell$ are distinct primes and $k_1,\cdots,k_\ell\in\mathbb{Z}^+$, we have

$$\lambda(n)=\operatorname{lcm}\big(\lambda({p_1}^{k_1}),\cdots,\lambda({p_\ell}^{k_\ell})\big)$$

with $\lambda(2)=\varphi(2)=1$, $\lambda(4)=\varphi(4)=2$, and $\lambda(2^k)=\frac{1}{2}\varphi(2^k)=2^{k-2}$ for $k\geq 3$, and with $\lambda(p^k)=\varphi(p^k)=p^{k-1}(p-1)$ when p is an odd prime and $k\in\mathbb{Z}^+$. Note that we can improve the Refined Euler-Fermat Theorem by replacing $\psi(n)$ by $\lambda(n)$ and that this is the best possible improvement.