Chapter 2. The Ring of Integers Modulo N

2.1 Definition: A (commutative) **ring** (with 1) is a set R with two elements $0, 1 \in R$ (usually assumed to be distinct) and two binary operations, $+, \times : R \times R \to R$ (usually called *addition* and *multiplication*) where, for $a, b \in R$, we write $+(a, b)$ as $a + b$ and we write $\times(a, b)$ as $a \times b$ or $a \cdot b$ or ab, which satisfy the following axims.

R1. $+$ is associative: $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$,
R2. $+$ is commutative: $a + b = b + a$ for all $a, b, c \in R$,
R3. 0 is an additive identity: $a + 0 = a$ for all $a \in R$,
R4. every $a \in R$ has an additive inverse: for all $a \in R$ there exists $b \in R$ such that $a + b = 0$,
R5. $\times$ is associative: $(ab)c = a(bc)$ for all $a, b, c \in R$,
R6. $\times$ is commutative: $a * b = b * a$ for all $a, b \in R$,
R7. 1 is a multiplicative identity: $a \times 1 = a$ for all $a \in R$, and
R8. $\times$ is distributive over $+$: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in R$.

For $a \in R$ we say that a is **invertible** (or that a is a **unit**) when there is an element $b \in R$ with $ab = 1$. A **field** is a commutative ring F in which $0 \neq 1$ and

R9. every non-zero element is a unit: for all $0 \neq a \in F$ there exists $b \in F$ such that $ab = 1$.

2.2 Example: $\mathbb{Z}$ is a ring, and $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

2.3 Example: Let $d \in \mathbb{Z}$ be a non-square (that is $d \neq s^2$ with $s \in \mathbb{Z}$). When $d > 0$ we have $\sqrt{d} \in \mathbb{R}$ and when $d < 0$ we write $\sqrt{d} = \sqrt{|d|}\, i \in \mathbb{C}$. Let

$$\mathbb{Z}\big[\sqrt{d}\,\big] = \big\{a + b\sqrt{d} \,\big|\, a, b \in \mathbb{Z}\big\},$$
$$\mathbb{Q}\big[\sqrt{d}\,\big] = \big\{a + b\sqrt{d} \,\big|\, a, b \in \mathbb{Q}\big\}.$$

Verify that $\mathbb{Z}\big[\sqrt{d}\,\big]$ is a ring and that $\mathbb{Q}\big[\sqrt{d}\big]$ is a field. When $d > 0$ so $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Q}[\sqrt{d}] \subseteq \mathbb{R}$, we say that $\mathbb{Z}[\sqrt{d}]$ is a **real quadratic ring** and $\mathbb{Q}[\sqrt{d}]$ is a **real quadratic field**, and when when $d < 0$ so $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Q}[\sqrt{d}] \subseteq \mathbb{C}$ and we say that $\mathbb{Z}[\sqrt{d}]$ is a **complex quadratic ring** and $\mathbb{Q}[\sqrt{d}]$ is a **complex quadratic field**. The ring $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ is called the ring of **Gaussian integers**.

2.4 Example: Many students will be familiar with the ring $\mathbb{Z}_n$ of integers modulo n. Later in this chapter, we shall define the ring $\mathbb{Z}_n$ and show that $\mathbb{Z}_n$ is a field if and only if n is prime.

2.5 Remark: When R is a commutative ring, the set $R[x]$ of polynomials with coefficients in R is a commutative ring and, when $n \in \mathbb{Z}$ with $n \geq 2$, the set $M_n(R)$ of $n \times n$ matrices with entries in R is an example of a *non-commutative* ring (Axiom R6 does not hold).

2.6 Theorem: *(Uniqueness of Identity and Inverse) Let R be a ring. Then*

(1) the additive identity element 0 is unique in the sense that if $e \in R$ has the property that $a + e = a$ for all $a \in R$ then $e = 0$,
(2) the multiplicative identity element 1 is unique in the sense that for all $u \in R$, if $au = a$ for all $a \in R$ then $u = 1$,
(3) the additive inverse of each $a \in R$ is unique in the sense that for all $a, b, c \in R$ if $a + b = 0$ and $a + c = 0$ then $b = c$, and
(4) the multiplicative inverse of each unit $a \in R$ is unique in the sense that for all $a \in R$, if there exist $b, c \in R$ such that $ab = 1$ and $ac = 1$ then $b = c$.

Proof: The proof is left as an exercise.

2.7 Notation: Let R be a ring. For $a \in R$ we denote the unique additive inverse of $a \in R$ by $-a$, and for $a, b \in R$ we write $b - a$ for $b + (-a)$. If a is a unit we denote its unique multiplicative inverse by a^{-1}. When F is a field, and $a, b \in F$ with $b \neq 0$ we also write b^{-1} as $\frac{1}{b}$ and we write ab^{-1} as $\frac{a}{b}$.

2.8 Theorem: *(Cancellation Under Addition) Let R be a ring. Then for all $a, b, c \in R$,*
(1) if $a + b = a + c$ then $b = c$,
(2) if $a + b = b$ then $a = 0$, and
(3) if $a + b = 0$ then $a = -b$.

Proof: The proof is left as an exercise.

2.9 Note: We do not, in general, have similar rules for cancellation under multiplication. In general, for a, b, c in a ring R, $ab = ac$ does not imply that $b = c$, $ab = b$ does not imply that $a = 1$, and $ac = 0$ does not imply that $a = 0$ or $b = 0$ (and in the case that R is not commutative, $ac = 1$ does not imply that $ca = 1$). When $ac = 0$ but $a \neq 0$ and $b \neq 0$, we say that a and b are **zero divisors**. A commutative ring with 1 which has no zero divisors is called an **integral domain**.

2.10 Theorem: *(Cancellation Under Multiplication) Let R be a ring. For all $a, b, c \in R$, if $ab = ac$ then either $a = 0$ or $b = c$ or a is a zero divisor.*

Proof: Suppose $ab = ac$. Then $ab - ac = 0$ so $a(b - c) = 0$. By the definition of a zero divisor, either $a = 0$ or $b - c = 0$ (hence $b = c$), or else both a and $b - c$ are zero divisors.

2.11 Theorem: *(Basic Properties of Rings) Let R be a ring. Then*
(1) $0 \cdot a = 0$ for all $a \in R$,
(2) $(-a)b = -(ab) = a(-b)$ for all $a, b \in R$,
(3) $(-a)(-b) = ab$ for all $a, b \in R$,
(4) $(-1)a = -a$ for all $a \in R$.

Proof: Let $a \in R$. Then $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$. Thus $0 \cdot a = 0$ by additive cancellation. The proof that $a \cdot 0 = 0$ is similar, and the other proofs are left as an exercise.

2.12 Remark: In a ring R, we usually assume that $0 \neq 1$. Note that if $0 = 1$ then in fact $R = \{0\}$ because for all $a \in R$ we have $a = a \cdot 1 = a \cdot 0 = 0$. The ring $R = \{0\}$ is called the **trivial ring**.

2.13 Notation: Let R be a ring. For $a \in R$ and $k \in \mathbb{Z}$ we define $ka \in R$ as follows. We define $0a = 0$, and for $k \in \mathbb{Z}^+$ we define $ka = a + a + \cdots + a$ with k terms in the sum, and we define $(-k)a = k(-a)$. For $a \in R$ and $k \in \mathbb{N}$ we define $a^k \in R$ as follows. We define $a^0 = 1$ and for $k \in \mathbb{Z}^+$ we define $a^k = a \cdot a \cdot \ldots \cdot a$ with k terms in the product. When a is a unit and $k \in \mathbb{Z}^+$, we also define $a^{-k} = (a^{-1})^k$. For all $k, l \in \mathbb{Z}$ and all $a \in R$ we have $(k + l)a = ka + la$, $(-k)a = -(ka) = k(-a)$, $-(-a) = a$, $-(a + b) = -a - b$, $(ka)(lb) = (kl)(ab)$. For all $k, l \in \mathbb{N}$ and all $a \in R$ we have $a^{k+l} = a^k a^l$. When a and b are units, for all $k, l \in \mathbb{Z}$ we have $a^{k+l} = a^k a^l$, $a^{-k} = (a^k)^{-1}$, $(a^{-1})^{-1} = a$ and $(ab)^{-1} = b^{-1}a^{-1}$.

2.14 Definition: Let $n \in \mathbb{Z}^+$. For $a, b \in \mathbb{Z}$ we say that a is equal (or **congruent**) to b **modulo** n, and we write $a = b \bmod n$, when $n\big|(a-b)$ or, equivalently, when $a = b + kn$ for some $k \in \mathbb{Z}$.

2.15 Theorem: *Let $n \in \mathbb{Z}^+$. For $a, b \in \mathbb{Z}$ we have $a = b \bmod n$ if and only if a and b have the same remainder when divided by n. In particular, for every $a \in \mathbb{Z}$ there is a unique $r \in \mathbb{Z}$ with $a = r \bmod n$ and $0 \leq r < n$.*

Proof: Let $a, b \in \mathbb{Z}$. Use the Division Algorithm to write $a = qn + r$ with $0 \leq r < n$ and $b = pn + s$ with $0 \leq s < n$. We need to show that $a = b \bmod n$ if and only if $r = s$. Suppose that $a = b \bmod n$, say $a = b + kn$ where $k \in \mathbb{Z}$. Then since $a = qn + r$ and $a = b + kn = (pn + s) + kn = (p+k)n + s$ with $0 \leq r < n$ and $0 \leq s < n$, it follows that $q = p + s$ and $r = s$ by the uniqueness part of the Division Algorithm. Conversely, suppose that $r = s$. Then we have $0 = r - s = (a - qn) - (b - pn)$ so that $a = b + (q-p)n$, and hence $a = b \bmod n$.

2.16 Example: Find $117 \bmod 35$.

Solution: We are being asked to find the unique integer r with $0 \leq r < n$ such that $117 = r \bmod 35$ or, in other words, to find the remainder r when 117 is divided by 35. Since $117 = 3 \cdot 35 + 12$ we have $117 = 12 \bmod 35$.

2.17 Definition: An **equivalence relation** on a set S is a binary relation $\sim$ on S such that

E1. $\sim$ is reflexive: for every $a \in S$ we have $a \sim a$,
E2. $\sim$ is symmetric: for all $a, b \in S$, if $a \sim b$ then $b \sim a$, and
E3. $\sim$ is transitive: for all $a, b, c \in S$, if $a \sim b$ and $b \sim c$ then $a \sim c$.

When $\sim$ is an equivalence relation on S and $a \in S$, the **equivalence class** of a in S is the set

$$[a] = \big\{x \in S \big| x \sim a\big\}.$$

2.18 Theorem: *Let $n \in \mathbb{Z}^+$. Then congruence modulo n is an equivalence relation on $\mathbb{Z}$.*

Proof: Let $a \in \mathbb{Z}$. Since $a = a + 0 \cdot n$ we have $a = a \bmod n$. Thus congruence modulo n satisfies Property E1. Let $a, b \in \mathbb{Z}$ and suppose that $a = b \bmod n$, say $a = b + kn$ with $k \in \mathbb{Z}$. Then $b = a + (-k)n$ so we have $b = a \bmod n$. Thus congruence modulo n satisfies Property E2. Let $a, b, c \in \mathbb{Z}$ and suppose that $a = b \bmod n$ and $b = c \bmod n$. Since $a = b \bmod n$ we can choose $k \in \mathbb{Z}$ so that $a = b + kn$. Since $b = c \bmod n$ we can choose $\ell \in \mathbb{Z}$ so that $b = c + \ell n$. Then $a = b + kn = (c + \ell n) + kn = c + (k + \ell)n$ and so $a = c \bmod n$. Thus congruence modulo n satisfies Property E3.

2.19 Definition: A **partition** of a set S is a set P of nonempty disjoint subsets of S whose union is S. This means that

P1. for all $A \in P$ we have $\emptyset \neq A \subseteq S$,
P2. for all $A, B \in P$, if $A \neq B$ then $A \cap B = \emptyset$, and
P3. for every $a \in S$ we have $a \in A$ for some $A \in P$.

2.20 Example: $P = \big\{\{1,3,5\}, \{2\}, \{4,6\}\big\}$ is a partition of $S = \{1,2,3,4,5,6\}$.

2.21 Theorem: *Let $\sim$ be an equivalence relation on a set S. Then $P = \big\{[a]\big|a \in S\big\}$ is a partition of S.*

Proof: For $a \in S$, it is clear from the definition of $[a]$ that $[a] \subseteq S$, and we have $[a] \neq \emptyset$ because $a \sim a$ so $a \in [a]$. This shows that P satisfies P1.

Let $a, b \in S$. We claim that $a \sim b$ if and only if $[a] = [b]$. Suppose that $a \sim b$. Let $x \in S$. Suppose that $x \in [a]$. Then $x \sim a$ by the definition of $[a]$. Since $x \sim a$ and $a \sim b$ we have $x \sim b$ since $\sim$ is transitive. Since $x \sim b$ we have $x \in [b]$. This shows that $[a] \subseteq [b]$. Since $a \sim b$ implies that $b \sim a$ by symmetry, a similar argument shows that $[b] \subseteq [a]$. Thus we have $[a] = [b]$. Conversely, suppose that $[a] = [b]$. Then since $a \sim a$ we have $a \in [a]$. Since $a \in [a]$ and $[a] = [b]$, we have $a \in [b]$. Since $a \in [b]$, we have $a \sim b$. Thus $a \sim b$ if and only if $[a] = [b]$, as claimed.

Let $a, b \in S$. We claim that if $[a] \neq [b]$ then $[a] \cap [b] = \emptyset$. Suppose that $[a] \cap [b] \neq \emptyset$. Choose $c \in [a] \cap [b]$. Since $c \in [a]$ so that $c \sim a$ we have $[c] = [a]$ (by the above claim). Since $c \in [b]$ so that $c \sim b$ we have $[c] = [b]$. Thus $[a] = [c] = [b]$, as required. This completes the proof that P satisfies P2.

Finally, note that P satisfies P3 because given $a \in S$ we have $a \in [a] \in P$.

2.22 Definition: Let $\sim$ be an equivalence relation on a set S. The **quotient** of the set S by the relation $\sim$, denoted by $S/\!\sim$, is the partition P of the above theorem, that is

$$S/\!\sim\; = \big\{[a]\big|a \in S\big\}.$$

2.23 Definition: Let $n \in \mathbb{Z}^+$. Let $\sim$ be the equivalence relation on $\mathbb{Z}$ defined for $a, b \in \mathbb{Z}$ by $a \sim b \Longleftrightarrow a = b \bmod n$, and write $[a] = \{x \in \mathbb{Z} | x \sim a\} = \{x \in \mathbb{Z} | x = a \bmod n\}$. The set of **integers modulo n**, denoted by $\mathbb{Z}_n$, is defined to be the quotient set

$$\mathbb{Z}_n = \mathbb{Z}/\!\sim\; = \big\{[a]\big|a \in \mathbb{Z}\big\}.$$

Since every $a \in \mathbb{Z}$ is congruent modulo n to a unique $r \in \mathbb{Z}$ with $0 \leq r < n$, we have

$$\mathbb{Z}_n = \big\{[0], [1], [2], \cdots, [n-1]\big\}$$

and the elements listed in the above set are distinct so that $\mathbb{Z}_n$ is an n-element set.

2.24 Example: We have

$$\mathbb{Z}_3 = \big\{[0], [1], [2]\big\} = \big\{\{\cdots,-3, 0, 3, 6, \cdots\}, \{\cdots,-2, 1, 4, 7, \cdots\}, \{\cdots,-1, 2, 5, 8, \cdots\}\big\}.$$

2.25 Theorem: *(Addition and Multiplication Modulo n) Let $n \in \mathbb{Z}^+$. For $a, b, c, d \in \mathbb{Z}$, if $a = c \bmod n$ and $b = d \bmod n$ then $a + b = c + d \bmod n$ and $ab = cd \bmod n$. It follows that we can define addition and multiplication operations on $\mathbb{Z}_n$ by defining*

$$[a] + [b] = [a + b] \quad \textit{and} \quad [a]\,[b] = [ab]$$

for all $a, b \in \mathbb{Z}$. When $n \geq 2$, the set $\mathbb{Z}_n$ is a commutative ring using these operations with zero and identity elements $[0]$ and $[1]$ (in $\mathbb{Z}_1$ we have $[0] = [1]$, so $\mathbb{Z}_1$ is the trivial ring).

Proof: Let $a, b, c, d \in \mathbb{Z}$. Suppose that $a = c \bmod n$ and $b = d \bmod n$. Since $a = c \bmod n$ we can choose $k \in \mathbb{Z}$ so that $a = c + kn$. Since $b = d \bmod n$ we can choose $\ell \in \mathbb{Z}$ so that $b = d + \ell n$. Then $a + b = (c + kn) + (d + \ell n) = (c + d) + (k + \ell)n$ so that $a + b = c + d \bmod n$, and $ab = (c + kn)(d + \ell n) = cd + c\ell n + knd + kn\ell n = cd + (kd + \ell c + k\ell n)n$ so that $ab = cd \bmod n$.

It follows that we can define addition and multiplication operations in $\mathbb{Z}_n$ by defining $[a] + [b] = [a + b]$ and $[a]\,[b] = [ab]$ for all $a, b \in \mathbb{Z}$. It is easy to verify that these operations satisfy all of the Axioms R1 - R8 which define a commutative ring. As a sample proof, we shall verify that one half of the distributivity Axiom R7 is satisfied. Let $a, b, c \in \mathbb{Z}$. Then

$$\begin{aligned}
[a]\big([b] + [c]\big) &= [a]\,[b + c] \text{ , by the definition of addition in } \mathbb{Z}_n \\
&= \big[a(b + c)\big] \text{ , by the definition of multiplication in } \mathbb{Z}_n, \\
&= [ab + ac] \text{ , by distributivity in } \mathbb{Z}. \\
&= [ab] + [ac] \text{ , by the definition of addition in } \mathbb{Z}_n, \\
&= [a]\,[b] + [a]\,[c] \text{ , by the definition of multiplication in } \mathbb{Z}_n.
\end{aligned}$$

2.26 Note: When no confusion arises, we shall often omit the square brackets from our notation so that for $a \in \mathbb{Z}$ we write $[a] \in \mathbb{Z}_n$ simply as $a \in \mathbb{Z}_n$. Using this notation, for $a, b \in \mathbb{Z}$ we have $a = b$ in $\mathbb{Z}_n$ if and only if $a = b \bmod n$ in $\mathbb{Z}$.

2.27 Example: Addition and multiplication in $\mathbb{Z}_6$ are given by the following tables.

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	4
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

2.28 Example: Find $251 \cdot 329 + (41)^2 \bmod 16$.

Solution: Since $251 = 15 \cdot 16 + 11$ and $329 = 20 \cdot 16 + 9$ and $41 = 2 \cdot 16 + 9$, working in $\mathbb{Z}_{16}$ we have $251 = 11$ and $329 = 41 = 9$ so that

$$251 \cdot 329 + (41)^2 = 11 \cdot 9 + 9^2 = (11 + 9) \cdot 9 = 20 \cdot 9 = 4 \cdot 9 = 36 = 4.$$

Thus $251 \cdot 329 + (41)^2 = 4 \bmod 16$.

2.29 Example: Show that for all $a \in \mathbb{Z}$, if $a = 3 \bmod 4$ then a is not equal to the sum of 2 perfect squares.

Solution: In $\mathbb{Z}_4$ we have $0^2 = 0$, $1^2 = 1$, $2^2 = 4 = 0$ and $3^2 = 9 = 1$ so that $x^2 \in \{0, 1\}$ for all $x \in \mathbb{Z}_4$. It follows that for all $x, y \in \mathbb{Z}_4$ we have $x^2 + y^2 \in \{0+0, 0+1, 1+0, 1+1\} = \{0, 1, 2\}$ so that $x^2 + y^2 \neq 3$. Equivalently, for all $x, y \in \mathbb{Z}$ we have $x^2 + y^2 \neq 3 \bmod 4$.

2.30 Example: Show that there do not exist integers x and y such that $3x^2+4=y^3$.

Solution: In $\mathbb{Z}_9$ we have

x	0	1	2	3	4	5	6	7	8
x^2	0	1	4	0	7	7	0	4	1
x^3	0	1	8	0	1	8	0	1	8
$3x^2$	0	3	3	0	3	3	0	3	3
$3x^2+4$	4	7	7	4	7	7	4	7	7

From the table we see that for all $x,y\in\mathbb{Z}_9$ we have $3x^2+4\in\{4,7\}$ and $y^3\in\{0,1,8\}$ and so $3x^2+4\neq y^3$. It follows that for all $x,y\in\mathbb{Z}$ we have $3x^2+4\neq y^3$.

2.31 Example: There are several well known tests for divisibility which can be easily explained using modular arithmetic. Suppose that a positive integer n is written in decimal form as $n=d_\ell\cdots d_1d_0$ where each d_i is a decimal digit, that is $d_i\in\{0,1,\cdots,9\}$. This means that

$$n=\sum_{k=0}^{\ell}10^id_i.$$

Since $2\big|10$ we have $10=0 \bmod 2$. It follows that in $\mathbb{Z}_2$ we have $10=0$ so $n=\sum_{i=0}^{\ell}10^id_i=d_0$. Thus in $\mathbb{Z}$, we have $2|n\Longleftrightarrow n=0 \bmod 2\Longleftrightarrow d_0=0 \bmod 2\Longleftrightarrow 2|d_0$. In other words,

2 divides n if and only if 2 divides the final digit of n.

More generally for $k\in\mathbb{Z}$ with $1\leq k\leq\ell$, since $2^k\big|10^k$ it follows that in $\mathbb{Z}_{2^k}$ we have $10^k=0$, hence $10^i=0$ for all $i\geq k$, and so $n=\sum_{i=0}^{\ell}10^id_i=\sum_{i=0}^{k-1}10^id_i$. Thus in $\mathbb{Z}$, we have $2^k\big|n$ if and only if $2^k\Big|\sum_{i=0}^{k-1}10^id_i$. In other words,

2^k divides n if and only if 2^k divides the tailing k-digit number of n.

Similarly, since $5^k\big|10^k$ it follows that

5^k divides n if and only if 5^k divides the tailing k-digit number of n.

Since $10=1 \bmod 3$ it follows that in $\mathbb{Z}_3$ we have $10=1$ so that $n=\sum_{i=1}^{\ell}10^id_i=\sum_{i=0}^{\ell}d_i$. Thus in $\mathbb{Z}$, $3|n\Longleftrightarrow n=0 \bmod 3\Longleftrightarrow \sum_{i=0}^{\ell}d_i=0 \bmod 3\Longleftrightarrow 3\Big|\sum_{i=0}^{\ell}$. In other words, 3 divides n if and only if 3 divides the sum of the digits of n. Similarly, since $10=1 \bmod 9$,

9 divides n if and only if 9 divides the sum of the digits of n.

Since $10=-1 \bmod 11$, in $\mathbb{Z}_{11}$ we have $10=-1$ so that $n=\sum_{i=0}^{\ell}10^id_i=\sum_{i=0}^{\ell}(-1)^id_i$. Thus in $\mathbb{Z}$, $11\big|n\Longleftrightarrow 11\Big|\sum_{i=0}^{\ell}(-1)^id_i$. In other words,

11 divides n if and only if 11 divides the alternating sum of the digits of n.

2.32 Exercise: Use the divisibility tests described in the above example to find the prime factorization of the number 28880280. Also, consider the problem of factoring the number 28880281.

2.33 Remark: For $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ note that if $a = b \bmod n$ so that $[a] = [b] \in \mathbb{Z}_n$ then we have $\gcd(a, n) = \gcd(b, n)$ and so it makes sense to define $\gcd([a], n) = \gcd(a, n)$.

2.34 Theorem: *(Inverses Modulo n) Let $n \in \mathbb{Z}$ with $n \geq 2$. For $a \in \mathbb{Z}$, $[a]$ is a unit in $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$ in $\mathbb{Z}$.*

Proof: Let $a \in \mathbb{Z}$ and let $d = gcd(a, n)$. Suppose that $[a]$ is a unit in $\mathbb{Z}_n$. Choose $b \in \mathbb{Z}$ so that $[a]\,[b] = [1] \in \mathbb{Z}_n$. Then $[ab] = [1] \in \mathbb{Z}_n$ and so $ab = 1 \bmod n$ in $\mathbb{Z}$. Since $ab = 1 \bmod n$ we can choose k so that $ab = 1 + kn$. Then we have $ab - kn = 1$. Since $d|a$ and $d|n$ it follows that $d\big|(ax + ny)$ for all $x, y \in \mathbb{Z}$ so in particular $d\big|(ab - kn)$, that is $d|1$. Since $d|1$ and $d \geq 0$, we must have $d = 1$.

Conversely, suppose that $d = 1$. By the Euclidean Algorithm with Back-Substitution, we can choose $s, t \in \mathbb{Z}$ so that $as + nt = 1$. Then we have $as = 1 - nt$ so that $as = 1 \bmod n$. Thus in $\mathbb{Z}_n$, we have $[as] = [1]$ so that $[a][s] = [1]$. Thus $[a]$ is a unit with $[a]^{-1} = [s]$.

2.35 Corollary: *For $n \in \mathbb{Z}^+$, the ring $\mathbb{Z}_n$ is a field if and only if n is prime.*

Proof: The proof is left as an exercise.

2.36 Example: Determine whether 125 is a unit in $\mathbb{Z}_{471}$ and if so find 125^{-1}.

Solution: The Euclidean Algorithm gives

$$471 = 3 \cdot 125 + 96\ ,\ 125 = 1 \cdot 96 + 29\ ,\ 96 = 3 \cdot 29 + 9\ ,\ 29 = 3 \cdot 9 + 2\ ,\ 9 = 4 \cdot 2 + 1$$

and so $d = \gcd(125, 471) = 1$ and it follows that 125 is a unit in $\mathbb{Z}_{471}$. Back-Substitution gives the sequence

$$1\ ,\ -4\ ,\ 13\ ,\ -43\ ,\ 56\ ,\ -211$$

so we have $125(-211) + 471(56) = 1$. It follows that in $\mathbb{Z}_{471}$ we have $125^{-1} = -211 = 260$.

2.37 Example: Solve the pair of equations $3x + 4y = 7$ (1) and $11x + 15y = 8$ (2) for $x, y \in \mathbb{Z}_{20}$.

Solution: We work in $\mathbb{Z}_{20}$. Since $3 \cdot 7 = 21 = 1$ we have $3^{-1} = 7$. Multiply both sides of Equation (1) by 7 to get $x + 8y = 9$, that is $x = 9 - 8y$ (3). Substitute $x = 9 - 8y$ into Equation (2) to get $11(9 - 8y) + 15y = 8$, that is $19 - 8y + 15y = 8$ or equivalently $7y = 9$ (4). Multiply both sides of Equation (4) by $7^{-1} = 3$ to get $y = 7$. Put $y = 7$ into Equation (3) to get $x = 9 - 8 \cdot 7 = 9 - 16 = 13$. Thus the only solution is $(x, y) = (13, 7)$.

2.38 Definition: A **group** is a set G with an element $e \in G$ and a binary operation $* : G \times G \to G$, where for $a, b \in G$ we write $*(a, b)$ as $a * b$ or simply as ab, such that

G1. $*$ is associative: for all $a, b, c \in G$ we have $(ab)c = a(bc)$,
G2. e is an identity element: for all $a \in G$ we have $ae = ea = a$, and
G3. every $a \in G$ has an inverse: for every $a \in G$ there exists $b \in G$ such that $ab = ba = e$.

A group G is called **abelian** when

G4. $*$ is commutative: for all $a, b \in G$ we have $ab = ba$.

2.39 Definition: When R is a ring under the operations $+$ and $\times$, the set R is also a group under the operation $+$ with identity element 0. The group R under $+$ is called the **additive group** of R. The set R is not a group under the operation $\times$ because not every element $a \in R$ has an inverse under $\times$ (in particular, the element 0 has no inverse). The set of all invertible elements in R, however, is a group under multiplication, and we denote it by R^*, so we have

$$R^* = \big\{a \in R \big| a \text{ is a unit}\big\}.$$

The group R^* is called the **group of units** of R.

2.40 Example: When F is a field, every nonzero element in F is invertible so we have $F^* = F \setminus \{0\}$. In $\mathbb{Z}$, the only invertible elements are ± 1 and so $\mathbb{Z}^* = \{1, -1\}$.

2.41 Definition: For $n \in \mathbb{Z}$ with $n \geq 2$, the group of units of $\mathbb{Z}_n$ is called the **group of units modulo** n and is denoted by U_n. Thus

$$U_n = \big\{a \in \mathbb{Z}_n \big| \gcd(a,n) = 1\big\}.$$

For convenience, we also let U_1 be the trivial group $U_1 = \mathbb{Z}_1 = \{1\}$. For a set S, let $|S|$ denote the cardinality of S, so that in particular when S is a finite set, $|S|$ denotes the number of elements in S. We define the **Euler phi function**, also called the **Euler totient function**, $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ by

$$\varphi(n) = \big|U_n\big|$$

so that $\varphi(n)$ is equal to the number of elements $a \in \{1, 2, \cdots, n\}$ such that $\gcd(a,n) = 1$.

2.42 Example: Since $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$ we have $\varphi(20) = 8$.

2.43 Example: When p is a prime number and $k \in \mathbb{Z}^+$ notice that

$$U_{p^k} = \{1, 2, 3, \cdots, p^k\} \setminus \{p, 2p, 3p, \cdots, p^k\}$$

and so

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k\left(1 - \tfrac{1}{p}\right).$$

At the end of this chapter (see Theorem 2.51) we will show, more generally, that when $p_1, \cdots, p_\ell$ are distinct prime numbers and $k_1, \cdots, k_\ell \in \mathbb{Z}^+$ we have

$$\varphi\Big(\prod_{i=1}^{\ell} {p_i}^{k_i}\Big) = \prod_{i=1}^{\ell} \varphi\big({p_i}^{k_i}\big) = \prod_{i=1}^{\ell} p_i^{k_i - 1}(p_i - 1) = \prod_{i=1}^{\ell} {p_i}^{k_1}\left(1 - \tfrac{1}{p_i}\right) = n \cdot \prod_{i=1}^{\ell}\left(1 - \tfrac{1}{p_i}\right).$$

2.44 Theorem: *(The Linear Congruence Theorem) Let $n \in \mathbb{Z}^+$, let $a, b \in \mathbb{Z}$, and let $d = \gcd(a,n)$. Consider the congruence $ax = b \bmod n$.*

(1) The congruence has a solution $x \in \mathbb{Z}$ if and only if $d|b$, and

(2) if $x = u$ is one solution to the congruence, then the general solution is

$$x = u \bmod \tfrac{n}{d}.$$

Proof: Suppose that the congruence $ax = b \bmod n$ has a solution. Let $x = u$ be a solution so we have $au = b \bmod n$. Since $au = b \bmod n$ we can choose $k \in \mathbb{Z}$ so that $au = b + kn$, that is $au - nk = b$. Since $d|a$ and $d|n$ it follows that $d|(ax + ny)$ for all $x, y \in \mathbb{Z}$, and so in particular $d\big|(au - nk)$, hence $d|b$. Conversely, suppose that $d|b$. By the Linear Diophanitine Equation Theorem, the equation $ax + ny = b$ has a solution. Choose $u, v \in \mathbb{Z}$ so that $au + nv = b$. Then since $au = b - nv$ we have $au = b \bmod n$ and so the congruence $ax = b \bmod n$ has a solution (namely $x = u$).

Suppose that $x = u$ is a solution to the given congruence, so we have $au = b \bmod n$. We need to show that for every $k \in \mathbb{Z}$ if we let $x = u + k\frac{n}{d}$ then we have $ax = b \bmod n$ and, conversely, that for every $x \in \mathbb{Z}$ such that $ax = b \bmod n$ there exists $k \in \mathbb{Z}$ such that $x = u + k\frac{n}{d}$. Let $k \in \mathbb{Z}$ and let $x = u + k\frac{n}{d}$. Then $ax = a\big(u + k\frac{n}{d}\big) = au + \frac{ka}{d}\, n$. Since $ax = au + \frac{ka}{d}\, n$ and $d|a$ so that $\frac{ka}{d} \in \mathbb{Z}$, it follows that $ax = au \bmod n$. Since $ax = au \bmod n$ and $au = b \bmod n$ we have $ax = b \bmod n$, as required.

Conversely, let $x \in \mathbb{Z}$ and suppose that $ax = b \bmod n$. Since $ax = b \bmod n$ and $au = b \bmod n$ we have $ax = au \bmod n$. Since $ax = au \bmod n$ we can choose $\ell \in \mathbb{Z}$ so that $ax = au + \ell n$. Then we have $a(x - u) = \ell n$ and so $\frac{a}{d}(x - u) = \frac{n}{d}\ell$. Since $\frac{n}{d}\big|\frac{a}{d}(x - u)$ and $\gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, it follows that $\frac{n}{d}\big|(x - u)$. Thus we can choose $k \in \mathbb{Z}$ so that $x - u = k\frac{n}{d}$ and then we have $x = u + k\frac{n}{d}$, as required.

2.45 Example: Solve $221x = 595 \bmod 323$.

Solution: The Euclidean Algorithm gives

$$323 = 1 \cdot 221 + 102 \ , \ 221 = 2 \cdot 102 + 17 \ , \ 102 = 6 \cdot 17 + 0$$

and so $\gcd(221, 323) = 17$. Note that $\frac{595}{17} = 35$, so the congruence has a solution. Back-Substitution gives the sequence

$$1 \ , \ -2 \ , \ 3$$

so we have $221 \cdot 3 - 323 \cdot 2 = 17$. Multiply by 35 to get $221 \cdot 105 - 323 \cdot 70 = 595$. Thus one solution to the given congruence is $x = 105$. Since $\frac{323}{17} = 19$ and $105 = 5 \cdot 19 + 10$, the general solution is given by $x = 105 = 10 \bmod 19$.

2.46 Theorem: *(The Chinese Remainder Theorem) Let $n, m \in \mathbb{Z}^+$ and let $a, b \in \mathbb{Z}$. Consider the pair of congruences*

$$x = a \bmod n,$$
$$x = b \bmod m.$$

(1) The pair of congruences has a solution $x \in \mathbb{Z}$ if and only if $\gcd(n, m) \big| (b - a)$, and
(2) if $x = u$ is one solution, then the general solution is $x = u \bmod \operatorname{lcm}(n, m)$.

Proof: Suppose that the given pair of congruences has a solution and let $d = \gcd(n, m)$. Let $x = u$ be a solution, so we have $u = a \bmod n$ and $u = b \bmod m$. Since $u = a \bmod n$ we can choose $k \in \mathbb{Z}$ so that $u = a + kn$. Since $u = b \bmod m$ we can choose $\ell \in \mathbb{Z}$ so that $u = b + \ell m$. Since $u = a + kn = b + \ell n$ we have $b - a = nk - m\ell$. Since $d|n$ and $d|m$ it follows that $d\big|(nx + my)$ for all $x, y \in \mathbb{Z}$ so in particular $d\big|(nk - m\ell)$, hence $d|(b - a)$. Conversely, suppose that $d|(b - a)$. By the Linear Diophantine Equation Theorem, the equation $nx + my = b - a$ has a solution. Choose $k, \ell \in \mathbb{Z}$ so that $nk - m\ell = b - a$. Then we have $a + nk = b + m\ell$. Let $u = a + nk = b + m\ell$. Since $u = a + nk$ we have $u = a \bmod n$ and since $u = b + m\ell$ we have $u = b \bmod m$. Thus $x = u$ is a solution to the pair of congruence.

Now suppose that $u = a \bmod n$ and $u = b \bmod m$. Let $\ell = \operatorname{lcm}(n, m)$. Let $k \in \mathbb{Z}$ be arbitrary and let $x = u + k\ell$. Since $x - u = k\ell$ we have $\ell\big|(x - u)$. Since $n|\ell$ and $\ell\big|(x - u)$ we have $n\big|(x - u)$ so that $x = u \bmod n$. Since $x = u \bmod n$ and $u = a \bmod n$ we have $x = a \bmod n$. Similarly $x = b \bmod m$.

Conversely, let $x \in \mathbb{Z}$ and suppose that $x = a \bmod n$ and $x = b \bmod m$. Since $x = a \bmod n$ and $u = a \bmod n$ we have $x = u \bmod n$ so that $n\big|(x - u)$. Since $x = b \bmod m$ and $u = b \bmod m$ we have $x = u \bmod m$ so that $m\big|(x - u)$. Since $n\big|(x - u)$ and $m\big|(x - u)$ and $\ell = \operatorname{lcm}(n, m)$, it follows that $\ell\big|(x - u)$ so that $x = u \bmod \ell$.

2.47 Example: Solve the pair of congruences $x = 2 \bmod 15$ and $x = 13 \bmod 28$.

Solution: We want to find $k, \ell \in \mathbb{Z}$ such that $x = 2+15k = 13+28\ell$. We need $15k-28\ell = 11$. The Euclidean Algorithm gives

$$28 = 1 \cdot 15 + 13 \ , \ 15 = 1 \cdot 13 + 2 \ , \ 13 = 6 \cdot 2 + 1$$

so that $\gcd(15, 28) = 1$ and Back-Substitution gives the sequence

$$1 \ , \ -6 \ , \ 7 \ , \ -13$$

so that $(15)(-13) + (28)(7) = 1$. Multiplying by 11 gives $(15)(-143) + (28)(77) = 11$, so one solution to the equation $15k - 28\ell = 11$ is given by $(k, l) = (-143, 77)$. It follows that one solution to the pair of congruences is given by $u = 2 + 15k = 2 - 15 \cdot 143 = -2143$. Since $\mathrm{lcm}(15, 28) = 15 \cdot 28 = 420$, and $-2143 = -6 \cdot 420 + 377$, the general solution to the pair of congruences is $x = -2143 = 377 \bmod 420$.

2.48 Exercise: Solve the congruence $x^3 + 2x = 18 \bmod 35$.

2.49 Exercise: Solve the system $x = 17 \bmod 25$, $x = 14 \bmod 18$ and $x = 22 \bmod 40$.

2.50 Theorem: *(Euler's Totient Function) Let $n = \prod {p_i}^{k_i}$ where $p_1, \cdots, p_\ell$ are distinct primes and $k_1, \cdots, k_\ell \in \mathbb{Z}^+$. Then*

$$\varphi(n) = \prod_{i=1}^{\ell} \varphi({p_i}^{k_i}) = \prod_{i=1}^{\ell} \left({p_i}^{k_i} - {p_i}^{k_i - 1}\right).$$

Proof: As mentioned earlier (in Example 2.43) when $n = p^k$ we have

$$U_{p^k} = \left\{1, 2, \cdots, p^k\right\} \setminus \left\{p, 2p, 3p, \cdots, p^k\right\}$$

and hence $\varphi(p^k) = p^k - p^{k-1}$. Thus it suffices to prove that if $k, \ell \in \mathbb{Z}$ with $\gcd(k, \ell) = 1$ then we have $\varphi(k\ell) = \varphi(k)\varphi(\ell)$.

Let $k, \ell \in \mathbb{Z}$ with $\gcd(k, \ell) = 1$. Define $F : \mathbb{Z}_{k\ell} \to \mathbb{Z}_k \times \mathbb{Z}_\ell$ by $F(x) = (x, x)$ where $x \in \mathbb{Z}$. Note that F is well-defined because if $x = y \bmod kl$ then $x = y \bmod k$ and $x = y \bmod \ell$. Note that F is bijective by the Chinese Remainder Theorem: indeed F is surjective because given $a, b \in \mathbb{Z}$ there exists a solution $x \in \mathbb{Z}$ to the pair of congruences $x = a \bmod k$ and $x = b \bmod \ell$, and F is injective because the solution x is unique modulo $k\ell$. We claim that the restriction of F to $U_{k\ell}$ is a bijection from $U_{k\ell}$ to $U_k \times U_\ell$. Note that if $x \in U_{k\ell}$ then we have $\gcd(x, k\ell) = 1$ so that $\gcd(x, k) = 1$ and $\gcd(x, \ell) = 1$, and hence $x \in U_k$ and $x \in U_\ell$, and so we have $F(x) = (x, x) \in U_k \times U_\ell$. Suppose, on the other hand, that $a \in U_k$ and $b \in U_\ell$ and let $xF^{-1}(a, b) \in \mathbb{Z}_{k\ell}$, so we have $x = a \bmod k$ and $x = b \bmod \ell$. Since $x = a \bmod k$ we have $\gcd(x, k) = \gcd(a, k) = 1$ and since $x = b \bmod \ell$ we have $\gcd(x, \ell) = \gcd(b, \ell) = 1$. Since $\gcd(x, k) = 1$ and $\gcd(x, \ell = 1)$ it follows that $\gcd(x, k\ell) = 1$ and so we have $x \in U_{k\ell}$. Thus the restriction of F to $U_{k\ell}$ is a well-defined bijective map from $U_{k\ell}$ to $U_k \times U_\ell$. It follows that

$$\varphi(k\ell) = \left|U_{k\ell}\right| = \left|U_k \times U_\ell\right| = \left|U_k\right| \cdot \left|U_\ell\right| = \varphi(k)\varphi(\ell),$$

as required.

2.51 Theorem: *(The Generalized Chinese Remainder Theorem) Let $\ell \in \mathbb{Z}^+$, let $n_i \in \mathbb{Z}^+$ and $a_i \in \mathbb{Z}$ for all indices i with $1 \le i \le \ell$. Consider the system of ℓ congruences $x = a_i \bmod n_i$ for all indices i with $1 \le i \le \ell$.*

(1) The system has a solution x if and only if $\gcd(n_i, n_j)\big|(a_i - a_j)$ for all i, j, and
(2) if $x = u$ is one solution then the general solution is $x = u \bmod \mathrm{lcm}(n_1, n_2, \cdots, n_\ell)$.

Proof: The proof is left as an exercise.