1.4 Integers Modulo n

In working with congruences, we have established that in computations involving addition, subtraction, and multiplication, we can consider congruent numbers to be interchangeable. In this section we will formalize this point of view. We will now consider entire congruence classes as individual entities, and we will work with these entities much as we do with ordinary numbers. The point of introducing the notation given below is to allow us to use our experience with ordinary numbers as a guide to working with congruence classes. Most of the laws of integer arithmetic hold for the arithmetic of congruence classes. The notable exception is that the product of two nonzero congruence classes may be zero.

1.4.1 Definition. *Let a and $n > 0$ be integers. The set of all integers which have the same remainder as a when divided by n is called the* ***congruence class of a modulo n****, and is denoted by $[a]_n$, where*

$$[a]_n = \{x \in \mathbf{Z} \mid x \equiv a \ (mod\ n)\} .$$

The collection of all congruence classes modulo n is called the ***set of integers modulo n****, denoted by $\mathbf{Z}_n$.*

Note that $[a]_n = [b]_n$ if and only if $a \equiv b \pmod{n}$. When the modulus is clearly understood from the context, the subscript n can be omitted and $[a]_n$ can be written simply as $[a]$.

A given congruence class can be denoted in many ways. For example, $x \equiv 5 \pmod{3}$ if and only if $x \equiv 8 \pmod{3}$, since $5 \equiv 8 \pmod{3}$. This shows that $[5]_3 = [8]_3$. We sometimes say that an element of $[a]_n$ is a **representative of the congruence class**. Each congruence class $[a]_n$ has a unique nonnegative representative that is smaller than n, namely, the remainder when a is divided by n. This shows that there are exactly n distinct congruence classes modulo n. For example, the congruence classes modulo 3 can be represented by 0, 1, and 2.

$$\begin{aligned} [0]_3 &= \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} \\ [1]_3 &= \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} \\ [2]_3 &= \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\} \end{aligned}$$

Each integer belongs to exactly one congruence class modulo 3, since the remainder on division by 3 is unique. In general, each integer belongs to a unique congruence class modulo n. Hence we have

$$\mathbf{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\} .$$

The set $\mathbf{Z}_2$ consists of $[0]_2$ and $[1]_2$, where $[0]_2$ is the set of even numbers and $[1]_2$ is the set of odd numbers. With the new notation, the familiar rules

"even + even = even," "odd + even = odd," "odd + odd = even"

can be expressed as

$$[0]_2 + [0]_2 = [0]_2\,, \qquad [1]_2 + [0]_2 = [1]_2\,, \qquad [1]_2 + [1]_2 = [0]_2\,.$$

Similarly,

"even × even = even," "even × odd = even," "odd × odd = odd"

can be expressed as

$$[0]_2 \cdot [0]_2 = [0]_2\,, \qquad [0]_2 \cdot [1]_2 = [0]_2\,, \qquad [1]_2 \cdot [1]_2 = [1]_2\,.$$

These rules can be summarized by giving an addition table and a multiplication table (Table 1.4.1).

Table 1.4.1: Addition and Multiplication in $\mathbf{Z}_2$

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

·	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

To use the addition table, select an element a from the first column, and an element b from the top row. Read from left to right in the row to which a belongs, until reaching the column to which b belongs. The corresponding entry in the table is $a + b$. In this table, as we will sometimes do elsewhere, we have simplified our notation for congruence classes by omitting the subscript in $[a]_n$.

A similar addition and multiplication can be introduced in $\mathbf{Z}_n$, for any n. Given congruence classes in $\mathbf{Z}_n$, we add (or multiply) them by picking representatives of each congruence class. We then add (or multiply) the representatives, and find the congruence class to which the result belongs. This can be written formally as follows.

Addition: $[a]_n + [b]_n = [a + b]_n$

Multiplication: $[a]_n \cdot [b]_n = [ab]_n$

In $\mathbf{Z}_{12}$, for example, we have $[8]_{12} = [20]_{12}$ and $[10]_{12} = [34]_{12}$. Adding congruence classes gives the same answer, no matter which representatives we use: $[8]_{12} + [10]_{12} = [18]_{12} = [6]_{12}$ and also $[20]_{12} + [34]_{12} = [54]_{12} = [6]_{12}$.

1.4.2 Proposition. *Let n be a positive integer, and let a, b be any integers. Then the addition and multiplication of congruence classes given below are well-defined:*

$$[a]_n + [b]_n = [a+b]_n \ , \qquad [a]_n \cdot [b]_n = [ab]_n \ .$$

Proof. We must show that the given formulas do not depend on the integers a and b which have been chosen to represent the congruence classes with which we are concerned. Suppose that x and y are any other representatives of the congruence classes $[a]_n$ and $[b]_n$, respectively. Then $x \equiv a \pmod{n}$ and $y \equiv b \pmod{n}$, and so we can apply Proposition 1.3.3. It follows from that proposition that $x + y \equiv a + b \pmod{n}$ and $xy \equiv ab \pmod{n}$, and thus we have $[x]_n + [y]_n = [a+b]_n$ and $[x]_n \cdot [y]_n = [ab]_n$. Since the formulas we have given do not depend on the particular representatives chosen, we say that addition and multiplication are "well-defined." □

The familiar rules for addition and multiplication carry over from the addition and multiplication of integers. A complete discussion of these rules will be given in Chapter 5, when we study ring theory. If $[a]_n, [b]_n \in \mathbf{Z}_n$ and $[a]_n + [b]_n = [0]_n$, then $[b]_n$ is called an **additive inverse** of $[a]_n$. By Proposition 1.3.3 (b), additive inverses are unique. We will denote the additive inverse of $[a]_n$ by $-[a]_n$. It is easy to see that $-[a]_n$ is in fact equal to $[-a]_n$, since $[a]_n + [-a]_n = [a-a]_n = [0]_n$.

For any elements $[a]_n, [b]_n, [c]_n$ in $\mathbf{Z}_n$, the following laws hold.

Associativity:
$$([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$$
$$([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$$

Commutativity:
$$[a]_n + [b]_n = [b]_n + [a]_n$$
$$[a]_n \cdot [b]_n = [b]_n \cdot [a]_n$$

Distributivity:
$$[a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$$

Identities:
$$[a]_n + [0]_n = [a]_n$$
$$[a]_n \cdot [1]_n = [a]_n$$

Additive inverses:
$$[a]_n + [-a]_n = [0]_n$$

We will give a proof of the distributive law and leave the proofs of the remaining properties as an exercise. If $a, b, c \in \mathbf{Z}$, then

$$\begin{aligned} [a]_n \cdot ([b]_n + [c]_n) &= [a]_n \cdot ([b+c]_n) = [a(b+c)]_n \\ &= [ab+ac]_n = [ab]_n + [ac]_n \\ &= [a]_n \cdot [b]_n + [a]_n \cdot [c]_n \ . \end{aligned}$$

The steps in the proof depend on the definitions of addition and multiplication and the equality $a(b + c) = ab + ac$, which is the distributive law for $\mathbf{Z}$.

Looking ahead.

The preceding remarks on addition and multiplication of congruence classes will be used in Chapter 3 to show that $\mathbf{Z}_n$ is a group, and in Chapter 5 to show that $\mathbf{Z}_n$ is a commutative ring.

In doing computations in $\mathbf{Z}_n$, the one point at which particular care must be taken is the cancellation law, which no longer holds in general. Otherwise, in almost all cases your experience with integer arithmetic can be trusted when working with congruence classes. A quick computation shows that $[6]_8 \cdot [5]_8 = [6]_8 \cdot [1]_8$, but $[5]_8 \neq [1]_8$. It can also happen that the product of nonzero classes is equal to zero. For example, $[6]_8 \cdot [4]_8 = [0]_8$.

1.4.3 Definition. *If $[a]_n$ belongs to $\mathbf{Z}_n$, and $[a]_n[b]_n = [0]_n$ for some nonzero congruence class $[b]_n$, then $[a]_n$ is called a **divisor of zero**.*

If $[a]_n$ is not a divisor of zero, then in the equation $[a]_n[b]_n = [a]_n[c]_n$ we may cancel $[a]_n$, to get $[b]_n = [c]_n$. To see this, if $[a]_n[b]_n = [a]_n[c]_n$, then $[a]_n([b]_n - [c]_n) = [a]_n[b - c]_n = [0]_n$, and so $[b]_n - [c]_n$ must be zero since $[a]_n$ is not a divisor of zero. This shows that $[b]_n = [c]_n$.

1.4.4 Definition. *If $[a]_n$ belongs to $\mathbf{Z}_n$, and $[a]_n[b]_n = [1]_n$, for some congruence class $[b]_n$, then $[b]_n$ is called a **multiplicative inverse** of $[a]_n$ and is denoted by $[a]_n^{-1}$.*

*In this case, we say that $[a]_n$ is an **invertible** element of $\mathbf{Z}_n$, or a **unit** of $\mathbf{Z}_n$.*

The next proposition (which is just a restatement of Proposition 1.3.4) shows that a has a multiplicative inverse modulo n if and only if $(a, n) = 1$. When a satisfies this condition, it follows from Proposition 1.3.3 (b) that any two solutions to $ax \equiv 1 \pmod{n}$ are congruent modulo n, and so we are justified in referring to *the* multiplicative inverse of $[a]_n$, whenever it exists.

In $\mathbf{Z}_7$, each nonzero congruence class contains representatives which are relatively prime to 7, and so each nonzero congruence class has a multiplicative inverse. We can list them as $[1]_7^{-1} = [1]_7$, $[2]_7^{-1} = [4]_7$, $[3]_7^{-1} = [5]_7$, and $[6]_7^{-1} = [6]_7$. We did not need to list $[4]_7^{-1}$ and $[5]_7^{-1}$ since, in general, if $[a]_n^{-1} = [b]_n$, then $[b]_n^{-1} = [a]_n$.

From this point on, if the meaning is clear from the context we will omit the subscript on congruence classes. Using this convention in $\mathbf{Z}_n$, we note that if $[a]$ has a multiplicative inverse, then it cannot be a divisor of zero, since $[a][b] = [0]$ implies $[b] = [a]^{-1}([a][b]) = [a]^{-1}[0] = [0]$.

1.4.5 Proposition. *Let n be a positive integer.*

(a) *The congruence class $[a]_n$ has a multiplicative inverse in $\mathbf{Z}_n$ if and only if $(a, n) = 1$.*

(b) *A nonzero element of $\mathbf{Z}_n$ either has a multiplicative inverse or is a divisor of zero.*

Proof. (a) If $[a]$ has a multiplicative inverse, say $[a]^{-1} = [b]$, then $[a][b] = [1]$. Therefore $ab \equiv 1 \pmod{n}$, which implies that $ab = 1 + qn$ for some integer q. Thus $ab + (-q)n = 1$, and so $(a, n) = 1$.

Conversely, if $(a, n) = 1$, then there exist integers b and q such that $ab + qn = 1$. Reducing modulo n shows that $ab \equiv 1 \pmod{n}$, and so $[b] = [a]^{-1}$.

(b) Assume that a represents a nonzero congruence class, so that $n \nmid a$. If $(a, n) = 1$, then $[a]$ has a multiplicative inverse. If not, then $(a, n) = d$, where $1 < d < n$. In this case, since $d \mid n$ and $d \mid a$, we can find integers k, b with $n = kd$ and $a = bd$. Then $[k]$ is a nonzero element of $\mathbf{Z}_n$, but

$$[a][k] = [ak] = [bdk] = [bn] = [0],$$

which shows that $[a]$ is a divisor of zero. □

1.4.6 Corollary. *The following conditions on the modulus $n > 0$ are equivalent.*

(1) *The number n is prime.*

(2) *$\mathbf{Z}_n$ has no divisors of zero, except $[0]_n$.*

(3) *Every nonzero element of $\mathbf{Z}_n$ has a multiplicative inverse.*

Proof. Since n is prime if and only if every positive integer less than n is relatively prime to n, Corollary 1.4.6 follows from Proposition 1.4.5. □

The proof of Proposition 1.4.5 (a) shows that if $(a, n) = 1$, then the multiplicative inverse of $[a]$ can be computed by using the Euclidean algorithm.

Example 1.4.1.

For example, to find $[11]^{-1}$ in $\mathbf{Z}_{16}$ using the matrix form of the Euclidean algorithm (see the discussion preceding Example 1.1.5) we have the following computation:

$$\begin{bmatrix} 1 & 0 & 16 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow$$

$$\begin{bmatrix} 1 & -1 & 5 \\ -2 & 3 & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 11 & -16 & 0 \\ -2 & 3 & 1 \end{bmatrix}.$$

Thus $16(-2) + 11 \cdot 3 = 1$, which shows that $[11]_{16}^{-1} = [3]_{16}$.

When the numbers are small, as in this case, it is often easier to use trial and error. The positive integers less than 16 and relatively prime to 16 are $1, 3, 5, 7, 9, 11, 13, 15$. It is easier to use the representatives $\pm 1, \pm 3, \pm 5, \pm 7$ since if $[a][b] = [1]$, then $[-a][-b] = [1]$, and so $[-a]^{-1} = -[a]^{-1}$. Now we observe that $3 \cdot 5 = 15 \equiv -1 \pmod{16}$, so $3(-5) \equiv 1 \pmod{16}$. Thus $[3]_{16}^{-1} = [-5]_{16} = [11]_{16}$ and $[-3]_{16}^{-1} = [5]_{16}$. Finally, $7 \cdot 7 \equiv 1 \pmod{16}$, so $[7]_{16}^{-1} = [7]_{16}$ and $[-7]_{16}^{-1} = [-7]_{16} = [9]_{16}$. □

Another way to find the inverse of an element $[a] \in \mathbf{Z}_n$ is to take successive powers of $[a]$. If $(a, n) = 1$, then $[a]$ is not a zero divisor, and so no power of $[a]$ can be zero. We let $[a]^0 = [1]$. The set of powers $[1]$, $[a]$, $[a]^2$, $[a]^3$, ... must contain fewer than n distinct elements, so after some point there must be a repetition. Suppose that the first repetition occurs for the exponent m, say $[a]^m = [a]^k$, with $k < m$. Then $[a]^{m-k} = [a]^0 = [1]$ since we can cancel $[a]$ from both sides a total of k times. This shows that for the first repetition we must have had $k = 0$, so actually $[a]^m = [1]$. From this we can see that $[a]^{-1} = [a]^{m-1}$.

Example 1.4.2.

To find $[11]_{16}^{-1}$, we can list the powers of $[11]_{16}$. We have $[11]^2 = [-5]^2 = [9]$, $[11]^3 = [11]^2[11] = [99] = [3]$, and $[11]^4 = [11]^3[11] = [33] = [1]$. Thus again we see that $[11]_{16}^{-1} = [3]_{16}$. □

As for integers, we will say that the congruence class $[b] \in \mathbf{Z}_n$ is a **multiple** of $[a] \in \mathbf{Z}_n$ if $[b] = [ma]$ for some $m \in \mathbf{Z}$. The next example looks at multiples in $\mathbf{Z}_n$, and implies that if $(a, n) = 1$, then every element in $\mathbf{Z}_n$ is a multiple of $[a]$.

Example 1.4.3 (Sets of multiples)**.**

We will show that if $0 < a < n$, with $(a, n) = d$, then the multiples of $[a]$ in $\mathbf{Z}_n$ are just the multiples of $[d]$ in $\mathbf{Z}_n$.

Proof: Let $0 < a < n$, with $(a, n) = d$, and suppose that $a = kd$. Then for any integer m we have $[ma] = [(mk)d]$, showing that every multiple of $[a]$ is a multiple of $[d]$.

On the other hand, let $[md]$ be a multiple of $[d]$. We can write $d = sa + tn$ for some integers s, t, so $[md] = [m(sa + tn)] = [(ms)a] + [(mt)n] = [(ms)a]$ since $[(mt)n] = [0]$. Thus every multiple of $[d]$ is also a multiple of $[a]$. □

We are now ready to continue our study of equations in $\mathbf{Z}_n$. A linear congruence of the form $ax \equiv b \pmod{n}$ can be viewed as a linear equation $[a]_n[x]_n = [b]_n$ in $\mathbf{Z}_n$. If $[a]_n$ has a multiplicative inverse, then there is a unique congruence class

$[x]_n = [a]_n^{-1}[b]_n$ that is the solution to the equation. Without the notation for congruence classes we would need to modify the statement regarding uniqueness to say that if x_0 is a solution of $ax \equiv b \pmod{n}$, then so is $x_0 + qn$, for any integer q.

It is considerably harder to solve nonlinear congruences of the form $a_k x^k + \ldots + a_1 x + a_0 \equiv 0 \pmod{n}$, where $a_k, \ldots, a_0 \in Z$. It can be shown that in solving congruences modulo n of degree greater than or equal to 1, the problem reduces to solving congruences modulo p^α for the prime factors of n. This question is usually addressed in a course on elementary number theory, where the Chinese remainder theorem is used to show how to determine the solutions modulo a prime power p^α (for integers $\alpha \geq 2$) from the solutions modulo p. Then to determine the solutions modulo p we can proceed by trial and error, simply substituting each of $0, 1, \ldots, p-1$ into the congruence. Fermat's theorem (Corollary 1.4.12) can be used to reduce the problem to considering polynomials of degree at most $p-1$.

We will prove this theorem of Fermat as a special case of a more general theorem due to Euler. Another proof will also be given in Section 3.2, which takes advantage of the concepts we will have developed by then. The statement of Euler's theorem involves a function of paramount importance in number theory and algebra, which we now introduce.

1.4.7 Definition. *Let n be a positive integer. The number of positive integers less than or equal to n which are relatively prime to n will be denoted by $\varphi(n)$. This function is called* ***Euler's φ-function****, or the* ***totient function****.*

In Section 1.2 we gave a procedure for listing the positive integers less than n and relatively prime to n. However, in many cases we only need to determine the numerical value of $\varphi(n)$, without actually listing the numbers themselves. With the formula in Proposition 1.4.8, $\varphi(n)$ can be given in terms of the prime factorization of n. Note that $\varphi(1) = 1$.

1.4.8 Proposition. *If the prime factorization of n is $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where $\alpha_i > 0$ for $1 \leq i \leq k$, then*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Proof. See Exercises 19, 31, and 32. A proof of this result will also be presented in Section 3.5. □

Example 1.4.4.

Using the formula in Proposition 1.4.8, we have

$$\varphi(10) = 10\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 4 \qquad \text{and} \qquad \varphi(36) = 36\left(\frac{1}{2}\right)\left(\frac{2}{3}\right) = 12\,. \ \square$$

1.4.9 Definition. *The set of units of* $\mathbf{Z}_n$*, the congruence classes* $[a]$ *such that* $(a, n) = 1$*, will be denoted by* $\mathbf{Z}_n^\times$.

1.4.10 Proposition. *The set* $\mathbf{Z}_n^\times$ *of units of* $\mathbf{Z}_n$ *is closed under multiplication.*

Proof. This can be shown either by using Proposition 1.2.3 (d) or by using the formula $([a][b])^{-1} = [b]^{-1}[a]^{-1}$. $\square$

The number of elements of $\mathbf{Z}_n^\times$ is given by $\varphi(n)$. The next theorem should be viewed as a result on powers of elements in $\mathbf{Z}_n^\times$, although it is phrased in the more familiar congruence notation.

1.4.11 Theorem (Euler). *If* $(a, n) = 1$*, then* $a^{\varphi(n)} \equiv 1 \ (mod\ n)$.

Proof. In the set $\mathbf{Z}_n$, there are $\varphi(n)$ congruence classes which are represented by an integer relatively prime to n. Let these representatives be $a_1, \ldots, a_{\varphi(n)}$. For the given integer a, consider the congruence classes represented by the products $aa_1, \ldots, aa_{\varphi(n)}$. By Proposition 1.3.3 (b) these are all distinct because $(a, n) = 1$. Since each of the products is still relatively prime to n, we must have a representative from each of the $\varphi(n)$ congruence classes we started with. Therefore

$$a_1 a_2 \cdots a_{\varphi(n)} \equiv (aa_1)(aa_2)\cdots(aa_{\varphi(n)}) \equiv a^{\varphi(n)} a_1 a_2 \cdots a_{\varphi(n)} \pmod{n}.$$

Since the product $a_1 \cdots a_{\varphi(n)}$ is relatively prime to n, we can cancel it in the congruence

$$a_1 a_2 \cdots a_{\varphi(n)} \equiv a^{\varphi(n)} a_1 a_2 \cdots a_{\varphi(n)} \pmod{n},$$

and so we have $a^{\varphi(n)} \equiv 1 \pmod{n}$. $\square$

1.4.12 Corollary (Fermat). *If* p *is a prime number, then for any integer* a *we have* $a^p \equiv a \ (mod\ p)$.

Proof. If $p \mid a$, then trivially $a^p \equiv a \equiv 0 \pmod{p}$. If $p \nmid a$, then $(a, p) = 1$ and Euler's theorem gives $a^{\varphi(p)} \equiv 1 \pmod{p}$. Then since $\varphi(p) = p - 1$, we have $a^p \equiv a \pmod{p}$. □

It is instructive to include another proof of Fermat's "little" theorem, one that does not depend on Euler's theorem. Expanding $(a + b)^p$ we obtain

$$(a+b)^p = a^p + pa^{p-1}b + \frac{p(p-1)}{1 \cdot 2}a^{p-2}b^2 + \ldots + pab^{p-1} + b^p.$$

For $k \neq 0, k \neq p$, each of the coefficients

$$\frac{p!}{k!(p-k)!}$$

is an integer and has p as a factor, since p is a divisor of the numerator but not the denominator. Therefore

$$(a+b)^p \equiv a^p + b^p \pmod{p}\ .$$

Using induction, this can be extended to more terms, giving $(a + b + c)^p \equiv a^p + b^p + c^p \pmod{p}$, etc. Writing a as $(1 + 1 + \ldots + 1)$ shows that

$$a^p = (1 + 1 + \ldots + 1)^p \equiv 1^p + \ldots + 1^p \equiv a \pmod{p}.$$

Example 1.4.5.

Note that if $(a, n) = 1$, then the multiplicative inverse of $[a]_n$ can be given explicitly as $[a]_n^{\varphi(n)-1}$, since by Euler's theorem, $a \cdot a^{\varphi(n)-1} \equiv 1 \pmod{n}$. Note also that for a given n the exponent $\varphi(n)$ in Euler's theorem may not be the smallest exponent possible. For example, in $\mathbf{Z}_8$ the integers $\pm 1, \pm 3$ are relatively prime to 8, and Euler's theorem states that $a^4 \equiv 1 \pmod{8}$ for each of these integers. In fact, $a^2 \equiv 1 \pmod{8}$ for $a = \pm 1, \pm 3$. □

EXERCISES: SECTION 1.4

1. Make addition and multiplication tables for the following sets.
   (a) $\mathbf{Z}_3$
   (b) $\mathbf{Z}_4$
   †(c) $\mathbf{Z}_{12}$

2. Make multiplication tables for the following sets.
   (a) $\mathbf{Z}_6$
   (b) $\mathbf{Z}_7$
   (c) $\mathbf{Z}_8$

3. Find the multiplicative inverses of the given elements (if possible).
   †(a) [14] in $\mathbf{Z}_{15}$
   (b) [38] in $\mathbf{Z}_{83}$
   †(c) [351] in $\mathbf{Z}_{6669}$
   (d) [91] in $\mathbf{Z}_{2565}$

4. Let a and b be integers.
   (a) Prove that $[a]_n = [b]_n$ if and only if $a \equiv b \pmod{n}$.
   (b) Prove that either $[a]_n \cap [b]_n = \emptyset$ or $[a]_n = [b]_n$.

5. Prove that each congruence class $[a]_n$ in $\mathbf{Z}_n$ has a unique representative r that satisfies $0 \leq r < n$.

6. Let $m, n \in \mathbf{Z}^+$ such that $m \mid n$. Show that for any integer a, the congruence class $[a]_m$ is the union of the congruence classes $[a]_n, [a+m]_n, [a+2m]_n, \ldots, [a+n-m]_n$.

7. Prove that the associative and commutative laws hold for addition and multiplication of congruence classes, as defined in Proposition 1.4.2.

8. Use Proposition 1.3.3 (b) to show that if $[b]$ and $[c]$ are both multiplicative inverses of $[a]$ in $\mathbf{Z}_n$, then $b \equiv c \pmod{n}$.

9. Let $(a, n) = 1$. The smallest positive integer k such that $a^k \equiv 1 \pmod{n}$ is called the **multiplicative order** of $[a]$ in $\mathbf{Z}_n^\times$.
   †(a) Find the multiplicative orders of [5] and [7] in $\mathbf{Z}_{16}^\times$.
   (b) Find the multiplicative orders of [2] and [5] in $\mathbf{Z}_{17}^\times$.

10. Let $(a, n) = 1$. If $[a]$ has multiplicative order k in $\mathbf{Z}_n^\times$, show that $k \mid \varphi(n)$.

11. Let $n \in \mathbf{Z}$ with $n > 1$. Show that $n \nmid 2^n - 1$.

12. †In $\mathbf{Z}_9^\times$ each element is equal to a power of [2]. (Verify this.) Can you find a congruence class in $\mathbf{Z}_8^\times$ such that each element of $\mathbf{Z}_8^\times$ is equal to some power of that class? Answer the same question for $\mathbf{Z}_7^\times$.

13. Generalizing Exercise 12, we say that the set of units $\mathbf{Z}_n^\times$ of $\mathbf{Z}_n$ is **cyclic** if it has an element of multiplicative order $\varphi(n)$. Show that $\mathbf{Z}_{10}^\times$ and $\mathbf{Z}_{11}^\times$ are cyclic, but $\mathbf{Z}_{12}^\times$ is not.

14. ‡Show that $\mathbf{Z}_{17}^\times$ is cyclic.
   Hint: Just use trial and error. (It is known that if p is prime, then $\mathbf{Z}_p^\times$ is cyclic.)

15. An element $[a]$ of $\mathbf{Z}_n$ is said to be **idempotent** if $[a]^2 = [a]$.

    †(a) Find all idempotent elements of $\mathbf{Z}_6$ and $\mathbf{Z}_{12}$.

    (b) Find all idempotent elements of $\mathbf{Z}_{10}$ and $\mathbf{Z}_{30}$.

16. If p is a prime number, show that [0] and [1] are the only idempotent elements in $\mathbf{Z}_p$.

17. If n is not a prime power, show that $\mathbf{Z}_n$ has an idempotent element different from [0] and [1].
    Hint: Suppose that $n = bc$, with $(b, c) = 1$. Solve the simultaneous congruences $x \equiv 1 \pmod{b}$ and $x \equiv 0 \pmod{c}$.

18. An element $[a]$ of $\mathbf{Z}_n$ is said to be **nilpotent** if $[a]^k = [0]$ for some k. Show that $\mathbf{Z}_n$ has no nonzero nilpotent elements if and only if n has no factor that is a square (except 1).

19. ‡Using the formula for $\varphi(n)$, compute $\varphi(27)$, $\varphi(81)$, and $\varphi(p^\alpha)$, where p is a prime number. Give a proof that the formula for $\varphi(n)$ is valid when $n = p^\alpha$, where p is a prime number.

20. Show that if a and b are positive integers such that $a \mid b$, then $\varphi(a) \mid \varphi(b)$.

21. Show that $\varphi(1) + \varphi(p) + \ldots + \varphi(p^\alpha) = p^\alpha$ for any prime number p and any positive integer α.

22. Show that if $n > 2$, then $\varphi(n)$ is even.

23. For $n = 12$ show that $\sum_{d \mid n} \varphi(d) = n$. Do the same for $n = 18$.

24. Show that if $n > 1$, then the sum of all positive integers less than n and relatively prime to n is $n\varphi(n)/2$. That is, $\sum_{0<a<n,\,(a,n)=1} a = n\varphi(n)/2$.

25. Show that if p is a prime number, then the congruence $x^2 \equiv 1 \pmod{p}$ has only the solutions $x \equiv 1$ and $x \equiv -1$.

26. Let a, b be integers, and let p be a prime number of the form $p = 2k + 1$. Show that if $p \nmid a$ and $a \equiv b^2 \pmod{p}$, then $a^k \equiv 1 \pmod{p}$.

27. Let $p = 2k + 1$ be a prime number. Show that if a is an integer such that $p \nmid a$, then either $a^k \equiv 1 \pmod{p}$ or $a^k \equiv -1 \pmod{p}$.

28. Prove Wilson's theorem, which states that if p is a prime number, then $(p-1)! \equiv -1 \pmod{p}$.
    Hint: $[(p-1)!]$ is the product of all elements of $\mathbf{Z}_p^\times$. Pair each element with its inverse, and use Exercise 25. For three special cases see Exercise 11 of Section 1.3.

29. (a) Prove the converse of Wilson's theorem.

    (b) Show that if m is composite and $m > 4$, then $(m-1)! \equiv 0 \pmod{m}$.

30. Prove that if $(m, n) = 1$, then $n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod{mn}$.

31.‡Prove that if m, n are positive integers with $(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$. *Hint*: Use the Chinese remainder theorem to show that each pair of elements $[a]_m$ and $[b]_n$ (in $\mathbf{Z}_m$ and $\mathbf{Z}_n$ respectively) corresponds to a unique element $[x]_{mn}$ in $\mathbf{Z}_{mn}$. Then show that under this correspondence, $[a]$ and $[b]$ are units if and only if $[x]$ is a unit.

32.‡Use Exercise 19 and Exercise 31 to prove Proposition 1.4.8.

33. (a) Find all integers $n > 1$ such that $\varphi(n) = n/2$.
    (b) Find all integers $n > 1$ such that $\varphi(n) = \varphi(2n)$.

34. (a) Find all integers $n > 1$ such that $\varphi(n) = 2$.
    (b) Find all integers $n > 1$ such that $\varphi(n) = 12$.

Notes

The prime numbers are the basic the basic building blocks in number theory, since every positive integer can be written (essentially uniquely) as a product of prime numbers. (If you are reading this before studying the chapter, perhaps we need to remind you that an integer $p > 1$ is called prime if its only positive divisors are 1 and p.) Euclid considered primes and proved that there are infinitely many. When we look at the sequence of primes

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$$

we observe that except for 2, all primes are odd. Any two odd primes on the list must differ by at least 2, but certain pairs of "twin primes" that differ by the minimal amount 2 do appear, for example,

$$(3, 5),\ (5, 7),\ (11, 13),\ (17, 19),\ (29, 31),\ (41, 43), \ldots.$$

Are there infinitely many "twin prime" pairs? The answer to this seemingly innocent question is unknown.

Although any positive integer is a product of primes, what about sums? Another open question is attributed to Christian Goldbach (1690–1764). He asked whether every even integer greater than 2 can be written as the sum of two primes. (Since the sum of two odd primes is even, the only way to write an odd integer as a sum of two primes is to use an odd prime added to 2. That means that the only odd primes that can be represented as a sum of two primes are the ones that occur as the larger prime in a pair of "twin primes.") We invite you to experiment in writing some even integers as sums of two primes.

A beautiful theorem proved by Joseph Louis Lagrange (1736–1813) in 1770 states that every positive integer can be written as the sum of four squares (where an integer of the form n^2 is called a square). Could we get by with fewer than

four squares? The answer is no; try representing 7 as a sum of three squares. This naturally leads to the question of which positive integers can be written as the sum of three squares. The answer is that n can be written as a sum of three squares if and only if n is not of the form $4^m(8k + 7)$, where m, k are any nonnegative integers. This theorem was first correctly proved by Gauss and appears in his famous book *Disquisitiones Arithmeticae* (1801).

This raises the question of which positive integers can be written as the sum of two squares. The answer in this case is slightly more complicated. It is that n can be written as the sum of two squares if and only if when we factor n as a product of primes, all those primes that give a remainder of 3 upon division by 4 have even exponents. The first published proof of this fact (dating from 1749) is due to Leonhard Euler (1707–1783). Around 1640 Pierre de Fermat (1601–1665) had stated, without proof, all three of these theorems on the representation of n as a sum of squares.

Our fourth and final topic deals with another statement of Fermat, usually known as "Fermat's last theorem." The ancient Greeks (the Pythagoreans, in particular) knew that certain triples (x, y, z) of nonzero integers can satisfy the equation

$$x^2 + y^2 = z^2 ,$$

for example,

$$(3, 4, 5),\ (5, 12, 13),\ (8, 15, 17),\ (7, 24, 25), \ldots .$$

(See Exercise 30 of Section 1.2.) Fermat considered a generalization of this equation, and asked whether for any integer $n > 2$ there exists a triple (x, y, z) such that

$$x^n + y^n = z^n .$$

In the margin of his copy of a number theory text he stated that he had a wonderful proof that there exists no such triple for $n \geq 3$, but he went on to say that the margin was not wide enough to write it out. His assertion dates from 1637, and mathematicians have spent the last 350 years searching for a proof! Finally, in 1993, Andrew Wiles announced that he had completed the proof of "Fermat's last theorem." A gap was found in his initial proof, but within a year, Wiles, with the assistance of Richard Taylor, found a way to complete the proof. A long paper by Wiles, together with a shorter one by Taylor and Wiles, fill the May, 1995 issue of the *Annals of Mathematics*. This proof will stand as one of the major accomplishments of our time.

Fermat is clearly the first truly modern number theorist, and he deserves much of the credit for the subject as we know it today. Another important milestone in modern number theory is Gauss's *Disquisitiones Arithmeticae*, which changed number theory from a "hodge-podge" of results into a coherent subject. The material on congruences in Section 1.3 first appeared there, and contributed much to the systematic organization of number theory.