Chapter 27
Modular Arithmetic

You began your mathematical education adding, subtracting, multiplying, and dividing integers. From there you moved on to rational numbers, then to real numbers, and, perhaps, to complex numbers. But this is not the only kind of arithmetic mathematicians study. In fact, there's a very different kind of arithmetic that you use every single day. The popular name for these calculations is *clock arithmetic*, and it is indeed based upon the clock.

Consider the following scenario: Suppose it is now 3:00 P.M., and you start on a 28-hour trip. What time will it be when you return? A quick calculation yields an answer of 7:00 P.M. How did you arrive at this answer? You did something we all find natural—you did clock arithmetic. We will build carefully upon this idea, and we will apply many of the concepts we have already covered to help us understand it.

Clock arithmetic isn't done on numbers, but rather on equivalence classes of numbers. So we need to find the right equivalence relation. Recall that for two integers a and b with $a \neq 0$, we say that a divides b, written $a \mid b$, if there is an integer k such that $b = ak$. Now we are ready for the equivalence relation. Let $n \in \mathbb{Z}$ be such that $n > 1$. Two integers x and y will be related if $n|(y-x)$. In this case we say x **is congruent to** y **modulo** n, and we will write $x \equiv y \pmod{n}$.

Exercise 27.1. Find five different solutions to each of the problems below, and then find five integers that are not solutions.

(a) Find $x \in \mathbb{Z}$ such that $5 \equiv x \pmod{12}$.
(b) Find $x \in \mathbb{Z}$ such that $x > 1$ and $-3 \equiv 39 \pmod{x}$. ○

Theorem 27.2. *Let $n > 1$ be an integer. The relation congruence modulo n is an equivalence relation on $\mathbb{Z}$.*

The proof of this theorem is left as Problem 27.3.

For an integer $n > 1$, the set of all equivalence classes with respect to the relation congruence modulo n is called the **integers modulo** n and denoted by $\mathbb{Z}_n$. It follows from Theorem 11.4 that $\mathbb{Z}_n$ is a partition of $\mathbb{Z}$. There will be times when we will

U. Daepp and P. Gorkin, *Reading, Writing, and Proving: A Closer Look at Mathematics*, Undergraduate Texts in Mathematics, DOI 10.1007/978-1-4419-9479-0_27,

need to refer to the elements of $\mathbb{Z}_n$, and since these are equivalence classes and not just integers, the notation must be chosen carefully. So we introduce the following: for $m \in \mathbb{Z}$, we write $[m]_n = \{x \in \mathbb{Z} : n|(x-m)\}$.

Note that we now have two ways of denoting exactly the same thing. For integers a, b, and n with $n > 1$, the two statements "$a \equiv b \pmod{n}$" and "$[a]_n = [b]_n$" are equivalent.

Let us stop and think about what this all means in the context of time. Suppose we are told that, "in this camp, breakfast is served at 7:00 A.M." What does this mean? Is there exactly one instant on a certain day and time at which breakfast is served? This can hardly be the case, since we eat breakfast every day. What it must mean is that breakfast is served at 7:00 A.M. today, tomorrow, yesterday, and in a week. So 7:00 A.M. actually represents many different times, as long as the difference between that time and 7:00 A.M. is a multiple of 24 hours. Mathematically, this idea is expressed by an equivalence class. The class of 7 modulo 24 is the set of all integers that differ from 7 by a multiple of 24. Thus,

$$[7]_{24} = [31]_{24} = [-41]_{24} = \cdots = \{\ldots, -41, -17, 7, 31, 55, \ldots\}.$$

The "numbers" in modular arithmetic are sets of numbers.

Before exploring some of the properties of the integers modulo n, we need to learn a bit more about the integers themselves. You are no doubt familiar with these properties of the integers, but you may not know the rigorous definitions or the exact statements of the theorems. The first statement, which was introduced in Problem 13.22, is simply about division of one integer by another.

Theorem 27.3 (Division algorithm). *Let m and n be integers with $n \neq 0$. Then there exist unique integers q and r such that $m = nq + r$ and $0 \leq r < |n|$.*

In plain English, the division algorithm says that for two integers, m and n, we can write m as a multiple of n plus what's left over. Of course, that's just the statement that q is the quotient and r the remainder when we divide m by n. You might not understand why we need to prove this—after all, you have been using it for a long time. But did you ever stop to think about what it really means and why it is true? In fact, if you worked Problem 13.22, then you already proved this theorem following the outline that was provided. (The statement of the result was presented in Theorem 13.6.) If you have not already done so, this would be the right moment to return to that problem and the outline and produce a proof of the division algorithm. We'll need this result very soon.

Let's move on to another old friend from the past. Given two numbers, say 28 and 42, what is the gcd (or greatest common divisor) of the two numbers? You can probably figure out, without too much trouble, that the answer is l4. But now that you have much more mathematical experience, we are able to ask (and answer) the more complicated questions of "how can we give a precise definition of gcd?" and "is there an algorithm to find its value?"

Define the **greatest common divisor** d (which we'll soon see is unique) of two integers m and n, where m and n are not both zero, to be the positive integer d that satisfies

(i) $d|m$ and $d|n$, and
(ii) if s is a positive integer such that $s|m$ and $s|n$, then $s|d$.

We denote the greatest common divisor of m and n by $\gcd(m,n)$. We say m and n are **relatively prime** if $\gcd(m,n) = 1$.

Exercise 27.4. (a) What does condition (i) of the definition of the greatest common divisor really say?
(b) What does condition (ii) really say?
(c) We mentioned that the gcd of two numbers is unique. How would you try to prove this? ○

Exercise 27.5. Find $\gcd(-16,40)$, $\gcd(0,45)$, and $\gcd(-30,-27)$. ○

The next theorem tells us that the gcd always exists and is, as we promised, unique.

Theorem 27.6. *Let m and n be integers, not both zero. Then their greatest common divisor exists, is unique, and there are integers k and l such that* $\gcd(m,n) = km+ln$.

This theorem actually tells us more than the existence and uniqueness of the greatest common divisor. It tells us that the gcd can be expressed as the sum of multiples of the two numbers m and n. This fact is certainly not obvious, and it will turn out to be very useful. A sum of the form $km+ln$ where k and l are integers is called a linear combination of m and n. Theorem 27.6 is usually proved by first showing that $\gcd(m,n) = km+ln$. The proof looks at the set A of all the linear combinations of m and n that yield a positive integer. Since A will be a nonempty set of positive integers, the well-ordering principle tells us that this set has a smallest element. It turns out that this element will satisfy both (i) and (ii) in the definition of greatest common divisor. Once we have shown this, we will still need to present an argument that there is no other integer that is also the gcd of m and n.

Proof. For $m,n \in \mathbb{Z}$ not both zero, define $A = \{xm+yn : x,y \in \mathbb{Z} \text{ and } xm+yn > 0\}$. First we'll show that $A \neq \emptyset$. We know that $m,n \in \mathbb{Z}$, and so we may set $x = m$ and $y = n$. Since $m \neq 0$ or $n \neq 0$, we conclude that $xm+yn = m^2+n^2 > 0$, and hence $m^2+n^2 \in A$. Thus $A \neq \emptyset$. By the well-ordering principle, every nonempty set of positive integers has a smallest element, and we call this element d. Since $d \in A$, there exist $x_0, y_0 \in \mathbb{Z}$ such that $d = x_0m+y_0n$. We will show that $d = \gcd(m,n)$, proving two parts of the theorem, namely, that a greatest common divisor exists, and that this divisor can be written in the form $km+ln$ for some $k,l \in \mathbb{Z}$.

Since $d \in A$, we know that $d > 0$. By the division algorithm (Theorem 27.3), we can write $m = qd+r$, where q and r are two integers with $0 \leq r < d$. Therefore $r = m-dq = m-(x_0m+y_0n)q = (1-x_0q)m+(-y_0q)n$, where $1-x_0q$ and $-y_0q$ are integers. Now if $r > 0$, then r would be an element of A. But $r < d$ and d is the smallest element of A. This means that $r \notin A$. Hence it must be the case that $r = 0$;

in other words, $d|m$. Exactly the same argument shows that $d|n$. Thus $d|m$ and $d|n$, and (i) in the definition of gcd holds.

Suppose that s is a positive integer such that $s|m$ and $s|n$. Since $d = x_0m + y_0n$, we conclude that $s|d$. (You are asked to write out the details of this last step in Problem 27.1.) Hence (ii) also holds for d. We now know that a greatest common divisor exists and has the right form. It remains to show that it is unique.

So suppose that d and t are both greatest common divisors of m and n. Then, since d is a gcd, property (ii) of the definition says that $t|d$. On the other hand, t is a gcd, so $d|t$. We conclude that $t|d$ and $d|t$. Since both t and d are positive integers it follows (see Problem 27.2) that $t = d$, completing the proof of uniqueness. □

Incidentally, while the greatest common divisor d is unique, the integers x_0 and y_0, as defined in the proof, are not. Here is a simple example: Consider the integers $m = 6$ and $n = 9$. Then

$$\gcd(6,9) = 3 = 2 \cdot 6 + (-1) \cdot 9 = (-1) \cdot 6 + 1 \cdot 9.$$

Unfortunately, the proof of Theorem 27.6 was not constructive; that is, it's a nice enough proof, but it doesn't really tell us how to find $\gcd(m,n)$. However, there is an algorithm to do just that—one that appeared in Euclid's *Elements* over 2,300 years ago. The algorithm is appropriately called the *Euclidean algorithm* and you will learn to apply it in Problem 27.20 to calculate the gcd of two integers.

We now return to modular arithmetic. To get you back into the proper state of mind, we suggest that you reread (in the beginning of this chapter) what it means for two integers to be equivalent modulo n, where $n > 1$. Then work the following exercise:

Exercise 27.7. Show that for integers m and n with $n > 1$, there exists an integer r satisfying $0 \leq r < n$ such that $m \equiv r \pmod{n}$. ○

One good thing about the integers is that we can perform basic algebraic manipulations on them, like adding, subtracting, and multiplying. Can we do this on $\mathbb{Z}_n$ also? The answer is yes, but we must first carefully define how these operations work on the equivalence classes that make up the set $\mathbb{Z}_n$. That's what we will do right after we work an example to remind you what it means for two equivalence classes modulo n to be the same.

Example 27.8. For integers r, s, and n with $n > 1$, prove that $[r]_n = [s]_n$ if and only if there exists $k \in \mathbb{Z}$ such that $r - s = kn$.

Proof. By Problem 10.10, $[r]_n = [s]_n$ if and only if $r \sim s$. Thus $[r]_n = [s]_n$ if and only if $r \equiv s \pmod{n}$. Hence $[r]_n = [s]_n$ if and only if there exists an integer k such that $r - s = kn$. □

Be sure to keep this fact in mind as you read on in the text, and especially as you work your way through Example 27.9, in which we will show that multiplication on $\mathbb{Z}_n$, as introduced below, is well-defined.

Fix an integer $n > 1$. Now $\mathbb{Z}_n$ is closely related to $\mathbb{Z}$, so we will try to modify the operations of $\mathbb{Z}$ so that they apply to $\mathbb{Z}_n$. For $r, s \in \mathbb{Z}$, define

$$[r]_n + [s]_n = [r+s]_n,\ [r]_n - [s]_n = [r-s]_n,\ \text{and}\ [r]_n \cdot [s]_n = [rs]_n.$$

Before going on, convince yourself that

$$[12]_5 + [7]_5 = [4]_5,\ [12]_5 - [7]_5 = [0]_5,\ \text{and}\ [12]_5 \cdot [7]_5 = [4]_5.$$

These definitions amount to defining three functions from $\mathbb{Z}_n \times \mathbb{Z}_n$ to $\mathbb{Z}_n$, and we need to show that they are well-defined. We will provide a complete proof for the operation of multiplication, and we will leave addition and subtraction to you in Problem 27.11.

Example 27.9. Define $f : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, by $f([r]_n, [s]_n) = [rs]_n$. Then f is a well-defined function that yields a multiplication on $\mathbb{Z}_n$.

"Understanding the problem." To show that a function is well-defined, we need to prove two things. (i) We must show that f maps $\mathbb{Z}_n \times \mathbb{Z}_n$ into $\mathbb{Z}_n$. In other words, we must show that for every element x in $\mathbb{Z}_n \times \mathbb{Z}_n$, there exists an element y in $\mathbb{Z}_n$ such that $f(x) = y$. It is important to recall that when an element of a set can be written in a special form, as is the case with x in $\mathbb{Z}_n \times \mathbb{Z}_n$, we should take advantage of it. So if x is in $\mathbb{Z}_n \times \mathbb{Z}_n$, then there exist integers r and s such that $x = ([r]_n, [s]_n)$.

(ii) We must also show that, for x in $\mathbb{Z}_n \times \mathbb{Z}_n$, if $f(x) = y$ and $f(x) = z$, then $y = z$. Again, we will expect to use the special form of x, y, and z. Now x can be written as $([r]_n, [s]_n)$ for some integers r and s. Our function f is supposed to look at the pair of equivalence classes, choose an integer from each (they could be r and s, but don't have to be), multiply these together, and produce the resulting equivalence class.

What could possibly go wrong? Let us look at an example. We know that $[7]_6 = [19]_6$, because $6|(19-7)$. By the definition of multiplication in $\mathbb{Z}_6$, we write $[7]_6 \cdot [4]_6 = [28]_6$ and $[19]_6 \cdot [4]_6 = [76]_6$. The left sides of both equations are the same, so the right sides had better be the same as well, or we have a fatal problem on our hands. Are they the same? Our proof will need to show that the result of the multiplication operation is independent of the particular integers we used to represent the equivalence classes.

"Devising a plan." To prove part (i), we have to show that f is defined for every element of $\mathbb{Z}_n \times \mathbb{Z}_n$, and yields an element in $\mathbb{Z}_n$. For part (ii), we let $x \in \mathbb{Z}_n \times \mathbb{Z}_n$ and suppose that $f(x) = y$ and $f(x) = z$. We must show that $y = z$. Now, we can assume that there exist integers r, s, u, and v such that $x = ([r]_n, [s]_n) = ([u]_n, [v]_n)$ and $y = f([r]_n, [s]_n) = [rs]_n$, while $z = f([u]_n, [v]_n) = [uv]_n$. Therefore we must show that $[rs]_n = [uv]_n$. By Example 27.8, we know that this means that we must show that there exists an integer m such that $rs - uv = mn$. How can we show that such an integer m exists? By using what we know, namely, that $([r]_n, [s]_n) = ([u]_n, [v]_n)$. Looks like we are now ready to carry out our plan.

Proof. Let $x \in \mathbb{Z}_n \times \mathbb{Z}_n$. Then $x = ([r]_n, [s]_n)$ for some $r, s \in \mathbb{Z}$. Hence, $rs \in \mathbb{Z}$, and therefore $[rs]_n \in \mathbb{Z}_n$. By the definition of f, we have $f(x) = [rs]_n$. Thus, f maps $\mathbb{Z}_n \times \mathbb{Z}_n$ to $\mathbb{Z}_n$.

Again let $x \in \mathbb{Z}_n \times \mathbb{Z}_n$. We consider two arbitrary representations of x, say $x = ([r]_n, [s]_n)$ and $x = ([u]_n, [v]_n)$. Then $f(x) = [rs]_n$ and $f(x) = [uv]_n$. We need to show that $[rs]_n = [uv]_n$. Since $([r]_n, [s]_n) = ([u]_n, [v]_n)$, the definition of ordered pair implies that $[r]_n = [u]_n$ and $[s]_n = [v]_n$. Thus

$$u - r = kn, \quad \text{for some } k \in \mathbb{Z}, \text{ and} \tag{27.1}$$
$$v - s = ln, \quad \text{for some } l \in \mathbb{Z}. \tag{27.2}$$

To show that $[rs]_n = [uv]_n$, we calculate

$$\begin{aligned} uv - rs &= uv - rv + rv - rs \\ &= (u - r)v + r(v - s) \\ &= knv + rln \qquad \text{(using equations (27.1) and (27.2))} \\ &= (kv + rl)n. \end{aligned}$$

Now $kv + rl \in \mathbb{Z}$ and, by Example 27.8, $[rs]_n = [uv]_n$. Thus f is well-defined, as desired. □

Exercise 27.10. Define "modular exponentiation" as follows: For an integer $n > 1$ and $a, b \in \mathbb{Z}$, define $[a]_n^{[b]_n} = [a^b]_n$. Either prove that this operation is well-defined, or give an example to show that modular exponentiation is not well-defined. ○

In $\mathbb{Z}_n$, the operations of multiplication and addition are commutative and associative. The set $\mathbb{Z}_n$ has an additive identity; that is, there is an element $\theta \in \mathbb{Z}_n$ such that $x + \theta = x$ for all $x \in \mathbb{Z}_n$ (namely, $\theta = [0]_n$). Similarly, $\mathbb{Z}_n$ has a multiplicative identity; that is, there is an element $e \in \mathbb{Z}_n$ such that $x \cdot e = x$ for all $x \in \mathbb{Z}_n$ (namely, $e = [1]_n$). Further, every element of $\mathbb{Z}_n$ has an additive inverse; that is, for every $x \in \mathbb{Z}_n$ there is $y_x \in \mathbb{Z}_n$ such that $x + y_x = [0]_n$ (if $x = [r]_n$, then $-x = [-r]_n$). Multiplication is also distributive over addition. (See Problem 27.14.) Thus, they satisfy everything you might reasonably hope an operation would satisfy except for one thing: not every nonzero element has a multiplicative inverse. The following immediate consequence of Theorem 27.6 tells us something about reciprocals in $\mathbb{Z}_n$.

Corollary 27.11. *Let n be a positive integer with $n > 1$. Then for every integer a with $\gcd(a, n) = 1$, there exists an integer b such that $ab \equiv 1 \pmod{n}$.*

Before proceeding to the proof of the corollary, write out what it means to say that $ab \equiv 1 \pmod{n}$.

Proof. Since $\gcd(a, n) = 1$, Theorem 27.6 tells us that there exist $b, c \in \mathbb{Z}$ such that $ba + cn = 1$. Then $ba - 1 = (-c)n$ and $-c \in \mathbb{Z}$. Thus, $ab \equiv 1 \pmod{n}$. □

For an integer a to satisfy the hypothesis of this corollary, a needs to be relatively prime to the modulus n. Is it possible that we have two integers, a and b with $a \equiv b \pmod{n}$, such that one of the integers, say a, satisfies the hypothesis and the other one, b, does not? The answer to this query is no, as we see from the following lemma:

Lemma 27.12. *Let a, c, and n be integers with $n > 1$ and such that $a \equiv c \pmod{n}$. Then $\gcd(a,n) = 1$ if and only if $\gcd(c,n) = 1$. Further, if b and d are integers such that $ab \equiv 1 \pmod{n}$ and $cd \equiv 1 \pmod{n}$, then $b \equiv d \pmod{n}$.*

The proof of this lemma requires the multiplication defined on $\mathbb{Z}_n$ earlier in this chapter, and the (easily checked) algebraic properties of this multiplication. (See Problem 27.14.)

Proof. For the first part of the proof, we prove the contrapositive; that is, we prove that if $\gcd(c,n) \neq 1$, then $\gcd(a,n) \neq 1$. So assume that $\gcd(c,n) = k > 1$. Since $a \equiv c \pmod{n}$, we conclude that $a - c = ln$ for some $l \in \mathbb{Z}$. Hence $a = c + ln$. But $k|c$ and $k|n$, so $k|a$. By (ii) in the definition of gcd, we conclude that $k|\gcd(a,n)$. Thus $\gcd(a,n) > 1$. The converse is obtained by interchanging the roles of a and c.

For the second part of the proof, we use our assumptions: $[a]_n[b]_n = [ab]_n = [1]_n$, $[c]_n[d]_n = [cd]_n = [1]_n$, and $[a]_n = [c]_n$. Thus, we calculate

$$[b]_n = [bcd]_n = [bad]_n = [abd]_n = [d]_n,$$

and we conclude that $b \equiv d \pmod{n}$. □

Taken together, the corollary and the lemma tell us that if an integer a is relatively prime to n, then there exists an integer b such that the equivalence classes satisfy $[a]_n \cdot [b]_n = 1$. So, for a relatively prime to n, the equivalence class has something that should remind you of a reciprocal. This leads to the following definition: For a, b, and $n \in \mathbb{Z}$ with $n > 1$, we call b a **reciprocal modulo** n of a if $ab \equiv 1 \pmod{n}$. The notation is $b \equiv a^{-1} \pmod{n}$.

Exercise 27.13. (a) Find the reciprocals modulo 7 of $3, 5$, and 6.
(b) Which elements of $\mathbb{Z}_6$ have reciprocals modulo 6 and which do not? ○

The use of modular arithmetic is widespread. Every time you are on the Web, your browser is likely to make your transactions secure using an encryption that is based on modular arithmetic. (Work Project 29.13 on codes to see one such use.) We motivated the ideas in the chapter using time and calculations modulo 24. If you schedule tasks by days of the week you probably want to calculate with modulus 7; if you are interested in a monthly schedule, the modulus is 12. In fact, now that we've mentioned it, you can surely think of many other times when you have used modular arithmetic.

Definitions

Definition 27.1. Let $n \in \mathbb{Z}$ with $n > 1$. Integers x and y will be related if $n|(y - x)$. In this case, we say that x **is congruent to** y **modulo** n, and we write $x \equiv y \pmod{n}$.

Definition 27.2. For an integer $n > 1$, the set of all equivalence classes with respect to the relation congruence modulo n is called the **integers modulo** n and denoted by $\mathbb{Z}_n$.

Definition 27.3. The **greatest common divisor** of two integers m and n, where m and n are not both zero, is the positive integer d that satisfies

(i) $d|m$ and $d|n$, and
(ii) if s is a positive integer such that $s|m$ and $s|n$, then $s|d$.

It is denoted by $\gcd(m,n)$.

Definition 27.4. Two integers m and n are **relatively prime** if $\gcd(m,n) = 1$.

Definition 27.5. For a, b, and $n \in \mathbb{Z}$ with $n > 1$, we call b a **reciprocal modulo** n of a if $ab \equiv 1 \pmod{n}$. The notation is $b \equiv a^{-1} \pmod{n}$.

Solutions to Exercises

Solution (27.1).

(a) We defined $5 \equiv x \pmod{12}$ by $12 \mid (x-5)$. Some possible values for x are: $5, 17, 125, -7, -115$. Some values that do not work are: $0, 7, 1200, -5, -12$.
(b) The equivalence $-3 \equiv 39 \pmod{x}$ is defined by $x|42$ where x is an integer greater than 1. The set of all positive factors greater than 1 of 42 is the set $A = \{2, 3, 6, 7, 14, 21, 42\}$. Any five integers from A will work. The five non-solutions must be chosen from the integers greater than 1 that are not in A.

Solution (27.4).

(a) Condition (i) says that the greatest common divisor divides both integers. In other words, it is a statement about being a common divisor.
(b) Condition (ii) says that every other positive integer that divides both m and n also divides the $\gcd(m,n)$, and therefore is a factor of it. In other words, the second condition explains the choice of the word "greatest."
(c) We will need to prove the uniqueness of the greatest common divisor. To do so, we will prove that if there are integers d_1 and d_2, both satisfying the definition of greatest common divisor, then $d_1 = d_2$.

Solution (27.5). We list the answers here: $\gcd(-16, 40) = 8$, $\gcd(0, 45) = 45$, and $\gcd(-30, -27) = 3$.

Solution (27.7). The integers m and n are given and $n > 1$. By Theorem 27.3, there are $q, r \in \mathbb{Z}$ such that $m = nq + r$ and $0 \leq r < n$. Hence $m - r = nq$ for some $q \in \mathbb{Z}$. Thus $m \equiv r \pmod{n}$ and $0 \leq r < n$.

Solution (27.10). This is not well-defined. Let $n = 5$. Then $2 \equiv 7 \pmod{5}$. Now $[3]_5^{[2]_5} = [4]_5$ and $[3]_5^{[7]_5} = [2]_5$, but $4 \not\equiv 2 \pmod{5}$.

Solution (27.13).

(a) Check that $3^{-1} \equiv 5 \pmod 7$, $5^{-1} \equiv 3 \pmod 7$, and $6^{-1} \equiv 6 \pmod 7$.
(b) By Corollary 27.11, the integers 1 and 5 have reciprocals modulo 6; it is easy to check that none of the others does.

Problems

Problem 27.1. Let a, b, c, x, and $y \in \mathbb{Z}$. Prove that if $a|b$ and $a|c$, then $a|(bx+cy)$.

Problem 27.2. Let a and b be positive integers such that $a|b$ and $b|a$. Prove that $a = b$.

Problem 27.3. Prove Theorem 27.2. (Note that this generalizes part (c) of Problem 10.2.)

Problem 27.4. Carefully read the definition of greatest common divisor. What should the least common multiple of two integers be? Make up a definition for it. The least common multiple of two integers m and n is denoted by $\text{lcm}(m,n)$.

Problem 27.5. Using your definition from Problem 27.4 and the notation defined above, prove that if m and n are positive integers, then

$$\gcd(m,n) \cdot \text{lcm}(m,n) = mn.$$

Problem 27.6. Let $m, n \in \mathbb{Z}$, not both zero. Suppose that a is an integer that divides both m and n and whenever s is an integer dividing both m and n, then $s \leq a$. Prove that $a = \gcd(m,n)$.

Problem 27.7. Let $m, n \in \mathbb{Z}$ and assume that $m \neq 0$. Prove the following statements.

(a) For all positive integers k, we have $\gcd(mk,nk) = k \gcd(m,n)$.
(b) If $d = \gcd(m,n)$ and $k, l \in \mathbb{Z}$, then $\gcd(m,n) | \gcd(m+kd, n+ld)$.

Problem 27.8. Let p be a prime number and $a, b \in \mathbb{Z}$. Prove that if $p|ab$, then $p|a$ or $p|b$. (You may use Theorem 27.6 to solve this problem.)

Problem 27.9. Here is another theorem that you have been using for a long time.

Theorem 27.14 (Fundamental theorem of arithmetic). *Every integer n, where $n \geq 2$, is the product of prime numbers. This factorization is unique, up to the order of the factors.*

If you worked Problem 18.21, then you already proved that such a factorization exists. You will still need to prove uniqueness of the factorization. (You may use induction and the result of Problem 27.8 to do so.)

Problem 27.10. Let $p > 1$ be an integer with the property that for all integers a and b, if $p|ab$, then $p|a$ or $p|b$. Prove that p is prime.

(In your future mathematics courses you will see that this is a more useful definition of prime than the one to which you have become accustomed.)

Problem 27.11. Let $n > 1$ be an integer.

(a) Define $g : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ by $g([r]_n, [s]_n) = [r+s]_n$. Prove that g is well-defined.
(b) Define $h : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ by $h([r]_n, [s]_n) = [r-s]_n$. Prove that h is well-defined.

Problem 27.12. Define $f : \mathbb{Z}_{12} \to \mathbb{Z}_{24}$ by $f([x]_{12}) = [3x]_{24}$. Is f well-defined? Prove your claim.

Problem 27.13. Let p be an odd prime and define $f : \mathbb{Z}_p \to \mathbb{Z}_p$ by $f([x]_p) = [2x]_p$. Prove that f is well-defined and that f is a bijection.

Problem[#] 27.14. Let $n > 1$ be an integer. Using the addition and multiplication defined on $\mathbb{Z}_n$ in this chapter, prove the following statements:

(a) $([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$ for all $a, b, c \in \mathbb{Z}$;
(b) there is an integer $\theta \in \mathbb{Z}$ such that
    (i) $[a]_n + [\theta]_n = [\theta]_n + [a]_n = [a]_n$ for all $a \in \mathbb{Z}$, and
    (ii) for every $a \in \mathbb{Z}$, there is $b \in \mathbb{Z}$ such that $[a]_n + [b]_n = [b]_n + [a]_n = [\theta]_n$;
(c) $[a]_n + [b]_n = [b]_n + [a]_n$ for all $a, b \in \mathbb{Z}$;
(d) $([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$ for all $a, b, c \in \mathbb{Z}$;
(e) $[a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$ and
    $([a]_n + [b]_n) \cdot [c]_n = [a]_n \cdot [c]_n + [b]_n \cdot [c]_n$ for all $a, b, c \in \mathbb{Z}$;
(f) there is an element $e \in \mathbb{Z}$ such that $[a]_n \cdot [e]_n = [e]_n \cdot [a]_n = [a]_n$ for all $a \in \mathbb{Z}$;
(g) $[a]_n \cdot [b]_n = [b]_n \cdot [a]_n$ for all $a, b \in \mathbb{Z}$.

(A set with two well-defined operations satisfying (a)–(g) is called a "commutative ring with identity.")

Problem 27.15. You may know the following criterion for divisibility by nine: A positive integer is divisible by nine if and only if the sum of its digits is divisible by nine.

(a) Prove this criterion.
(b) Is 47832973 divisible by 9?

A variation of the divisibility criterion is the calculation check called "casting out nines." We may use this to check an addition, subtraction, multiplication, or division (turning the division into a multiplication before checking) of integers by replacing each integer by the sum of its digits (repeating the summation until the integer is a single digit). If our computation does not pass this check, it was incorrect. (However, it may pass the check and still be an incorrect computation!) For instance: To check that

$$56782351912/25785 = 2202146 \text{ plus a remainder of } 17302,$$

we first write this as

$$56782351912 = 25785 \cdot 2202146 + 17302.$$

Now we "cast out nines":

$$4 = 0 \cdot 8 + 4,$$

and we see that our "check" is consistent with the process of casting out nines. However, if we had

$$56782341912 = 25785 \cdot 2202146 + 17202,$$

our "check" would yield

$$4 = 0 \cdot 8 + 3,$$

and we would be alerted to an error.

(c) Explain "casting out nines" (use your work from part (a)).
(d) Find an example that shows that it is possible to have a situation in which the check works, but the original computation is incorrect.

Problem 27.16. Let n be an integer with $n > 1$. Prove that the following are equivalent.

1. For all m, if $m \not\equiv 0 \pmod{n}$, then m has a reciprocal modulo n.
2. The integer n is prime.

(This makes $\mathbb{Z}_p$, where p is prime, as good a set to do arithmetic in as $\mathbb{Q}$. As far as multiplication is concerned, $\mathbb{Z}_p$ is better than $\mathbb{Z}$, because very few numbers (two, to be exact) in $\mathbb{Z}$ have reciprocals that also lie in $\mathbb{Z}$. The set, $\mathbb{Z}_p$, for p a prime, is what is called a "field" in mathematics. Other examples include $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$. The set $\mathbb{Z}$ is not a field.)

Problem 27.17. *(This problem is appropriate only if you studied Chapter 22.)* Use the result of Exercise 27.7 to show that $|\mathbb{Z}_n| = n$.

Problem 27.18. Find *all* solutions in $\mathbb{Z}_n$ for the following equivalences:

(a) $3x \equiv 0 \pmod{12}$;
(b) $3x \equiv 0 \pmod{17}$;
(c) $3x \equiv 0 \pmod{10}$.

Problem 27.19. Find *all* solutions in $\mathbb{Z}_n$ for the following equivalences:

(a) $4x \equiv 1 \pmod{11}$;
(b) $4x \equiv 1 \pmod{9}$;
(c) $3x \equiv 1 \pmod{11}$;
(d) $3x \equiv 1 \pmod{9}$.

Problem# 27.20. Here's a brief explanation of the Euclidean algorithm, which is an effective way to find the greatest common divisor of two integers m and n, not both zero. This algorithm is in the seventh book of Euclid's *Elements*, but was likely known earlier.

There are two trivial cases that must be considered before moving to the interesting one. If $m = n$, then the greatest common divisor is obviously $|m|$. If one of the integers is zero (remember that both can't be zero), then the greatest common divisor is the absolute value of the nonzero integer. Now for the main case, note that the positive divisors of an integer m are the same as the ones of $-m$. For this reason, we may assume that both m and n are positive. After possible relabeling of the two numbers, we may further assume that $m > n > 0$.

The Euclidean algorithm is a repeated application of the division algorithm, Theorem 27.3. Each line is obtained from the previous one by shifting the divisor to the spot previously occupied by the dividend, and the remainder to the spot previously occupied by the divisor. It's easier to see than to say. Here is the way to see it:

$$\begin{aligned} m &= q_1 n + r_1, \\ n &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ &\dots \\ r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1}, \\ r_{k-2} &= q_k r_{k-1} + r_k, \\ r_{k-1} &= q_{k+1} r_k. \end{aligned}$$

By the division algorithm, the remainders satisfy the inequalities

$$n > r_1 > \dots > r_i > r_{i+1} > \dots > 0.$$

This guarantees that the algorithm comes to a halt after finitely many steps. We label the last nonzero remainder r_k and solve for r_k as follows:

$$\begin{aligned} r_k &= r_{k-2} - q_k r_{k-1} \\ &= r_{k-2} - q_k(r_{k-3} - q_{k-1} r_{k-2}) = -q_k r_{k-3} + (1 + q_k q_{k-1}) r_{k-2} \\ &\dots \\ &= x_0 m + y_0 n. \end{aligned}$$

It can be shown (but we won't ask you to do it) that $r_k = \gcd(m,n)$.

We'll work out one example for you, so you can see how this is done. We will find the greatest common divisor of 8 and 27 and express it as a linear combination of the given integers. Now we need $m > n$, so $m = 27$ and $n = 8$. We now proceed with the algorithm. The remainders are underlined, and will be replaced with what we obtained in the column on the left.

$$\begin{array}{r|l} 27 = 3\cdot 8+\underline{3} & \text{so } \underline{1} = 3-1\cdot\underline{2} \\ 8 = 2\cdot 3+\underline{2} & \quad = 3-1\cdot(8-2\cdot 3) \quad = -8+3\cdot\underline{3} \\ 3 = 1\cdot 2+\underline{1} & \quad = -8+3(27-3\cdot 8) = 3\cdot 27-10\cdot 8 \\ 2 = 2\cdot 1 & \end{array}$$

So our algorithm tells us that $1 = 3\cdot 27 - 10\cdot 8$, and you can now check that this answer is correct.

You'll understand the algorithm better if you use it to calculate the gcd of two numbers. Do so for the following pairs of integers (m,n) and find the corresponding integers x_0 and y_0:

(a) $(2745, 135)$;
(b) $(528, 627)$;
(c) $(4746, 894)$.

Problem 27.21. Use the Euclidean algorithm of Problem 27.20 to show that 2542 and 4095 are relatively prime.

Problem 27.22. On a calculator or a computer, program the Euclidean algorithm as outlined in Problem 27.20. Check your program by trying it out on parts (a) through (c) in that problem.

Problem 27.23. In the text we defined what it means for an integer p to be prime. We also defined what it means for two integers a and b to be relatively prime. Give an alternate definition for an integer p to be prime by requiring a and p to be relatively prime for certain integers a. Prove that the original and the alternate definition of prime are equivalent.

Problem 27.24. It is possible to define a function f that tells you the day of the week your birthday will fall on each year. To construct such a function, you need to find out what day of the week you were born. (Encode the weekdays as: 0—Sunday, 1—Monday, and so on.) Letting s denote the encoded week day of your birth, a the year you were born, and b the year in which you want to know the weekday of your birthday, you will need to define f in terms of s, a, and b. Thus, the required function f will be a map from $\mathbb{Z}_7 \times \mathbb{Z} \times \mathbb{Z}$ into $\mathbb{Z}_7$. (The formula will depend on whether your birthday is before, after, or on February 29 of your birth year.)

Use modular arithmetic, but keep in mind that there are leap years. (The year 2000 was a leap year. The formula becomes considerably more complicated if you want to extend it past 2100, because that year will not be a leap year.)

To find out the day of your birth and to check your formula, access one of the perpetual calendars on the Web such as [38].