Chapter V

Theory of the Integers

Mathematics is the queen of the sciences and number theory is the queen of mathematics. Carl Friedrich Gauss

One of the oldest surviving mathematical texts is Euclid's *Elements*, a collection of 13 books. This work, dating back to several hundred years BC, is one of the earliest examples of logical reasoning in mathematics still available for us to read. Although most of the books are devoted to theorems concerning geometry (many of which you may have seen in some form in a high school geometry class), books seven and nine deal with the arithmetic of the integers. In this chapter we will study some of the material found in these two books.

In particular, Euclid dealt with the topics of divisibility and greatest common divisors. It is remarkable that, thousands of years before the advent of electronic computers, Euclid wrote down a very efficient algorithm for computing GCDs that is still used essentially without change in modern computer systems.

In addition, Euclid defines prime numbers, proves that there are infinitely many primes, and proves the *Fundamental Theorem of Arithmetic*, which states that every natural number greater than 1 has a unique factorization into prime numbers.

The results that we present in this chapter have thus stood the test of time and have been studied by mathematicians over millennia. Besides being important and useful results on their own, they form a significant part of the common heritage of mathematics.

17 Divisibility

17.A Divisibility and common divisors

We now prove several facts about divisibility, some of which we took for granted in previous sections (often treating them as axioms).

Theorem 17.1. *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. If $a \mid b$, then $|a| \leq |b|$.*

Proof. Assume that $a \mid b$. Then $b = ak$ for some $k \in \mathbb{Z}$. Note that $k \neq 0$ since $b \neq 0$, and so $|k| \geq 1$. We conclude that

$$|b| = |ak| = |a||k| \geq |a|. \qquad \square$$

Corollary 17.2. *Let $a, b \in \mathbb{Z}$ be nonzero. If $a \mid b$ and $b \mid a$, then $a = \pm b$.*

Proof. Assume that $a \mid b$ and $b \mid a$. Then by Theorem 17.1, $|a| \leq |b|$ and $|b| \leq |a|$. Hence, $|a| = |b|$, so $a = \pm b$. $\square$

Theorem 17.3. *Let $b \in \mathbb{Z}$ with $b \neq 0$. There are finitely many integers that divide b.*

Proof. If $a \in \mathbb{Z}$ divides b, then $|a| \leq |b|$ by Theorem 17.1. Hence, $a \in \{-|b|, \ldots, |b|\}$. This set is finite, so there are only finitely many possibilities for a. $\square$

Example 17.4. If $b = 12$, the divisors of b are

$$\{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}. \qquad \triangle$$

Definition 17.5. A *common divisor* of two integers a and b is an integer c such that $c \mid a$ and $c \mid b$.

Example 17.6. If $a = 12$ and $b = 18$, then the common divisors of a and b are precisely ± 1, ± 2, ± 3, and ± 6. $\triangle$

Theorem 17.7. *Let a and b be integers, not both 0. The set of common divisors of a and b has a largest element.*

Proof. Without loss of generality, let $a \neq 0$. The set of divisors of a is finite and includes the set of common divisors of a and b, so the set of common divisors is finite. Since it is finite and nonempty (as 1 is an element), this set has a largest element. $\square$

Definition 17.8. Given two integers a and b, their *greatest common divisor* (GCD) is written as $\gcd(a, b)$; it is the largest common divisor of a and b when a and b are not both 0, otherwise it is 0.

Some authors leave $\gcd(0, 0)$ undefined, since every integer divides 0. However, most follow the convention of putting $\gcd(0, 0) = 0$, as we have done.

We next give two examples of GCDs.

Example 17.9. If $a = 12$ and $b = 18$, the list of divisors of a is

$$\{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$$

and the list of divisors of b is

$$\{-18, -9, -6, -3, -2, -1, 1, 2, 3, 6, 9, 18\}.$$

The set of numbers common to both of these sets (i.e., their intersection) is

$$\{-6, -3, -2, -1, 1, 2, 3, 6\}.$$

Hence, the greatest common divisor of 12 and 18 is 6. △

Example 17.10. Let $a \in \mathbb{Z}$ be nonzero. Then every divisor of a is less than or equal to $|a|$, and in fact $|a|$ is a divisor of a. In addition, $|a|$ is a divisor of 0. Hence,

$$\gcd(a, 0) = |a|.$$

This rule also works when $a = 0$. △

Remark 17.11. Some mathematicians write (a, b) for $\gcd(a, b)$. We will avoid that notation in this book since it already has two other meanings (as an open interval and as an ordered pair). ▲

We finish this subsection by stating a standard result about the GCD (the proof is left to the motivated reader).

Lemma 17.12. *Let $a, b \in \mathbb{Z}$. We have both*

- $\gcd(a, b) = \gcd(b, a)$ *and*
- $\gcd(a, b) = \gcd(|a|, |b|)$.

17.B The division algorithm

A fundamental property of the integers that relates addition and multiplication is the division algorithm. The fact that we can divide integers and get a unique quotient and remainder is the key to understanding divisibility, congruence, and modular arithmetic.

Theorem 17.13 (The Division Algorithm)**.** *Let $n, d \in \mathbb{Z}$ with $d \neq 0$. Then there are unique integers q, r such that*

$$n = qd + r$$

and $0 \leq r < |d|$.

We will prove the division algorithm in stages. First, we will prove the uniqueness of the quotient and remainder, as a lemma. After that, we will handle existence, but only in the case when the numerator is nonnegative and the denominator is positive. The other cases are left for the reader in Exercise 17.8.

Lemma 17.14. *Let $d, q, r, q', r' \in \mathbb{Z}$ with $d \neq 0$. If $qd + r = q'd + r'$ with $0 \leq r < |d|$ and $0 \leq r' < |d|$, then $q = q'$ and $r = r'$.*

Proof of Lemma. Let $d, q, r, q', r' \in \mathbb{Z}$ with $d \neq 0$. Working directly, assume that $qd + r = q'd + r'$, with $0 \leq r < |d|$ and $0 \leq r' < |d|$. Without loss of generality, we may assume that $r \leq r'$, which will be useful later. Rearranging the equality, we find

$$(q - q')d = r' - r. \tag{17.15}$$

Note that since $r' < |d|$ and $r \geq 0$, we have $0 \leq r' - r \leq r' < |d|$, so that $|r' - r| < |d|$. However, by (17.15), we know $d \,|\, (r' - r)$. Hence, by Theorem 17.1, we see that it must be the case that $r' - r = 0$, so that $r' = r$. Since $d \neq 0$, (17.15) now implies that $q = q'$. □

As mentioned above, we will prove the existence of q and r only in the case when $n \geq 0$ and $d > 0$. The other cases of the proof (when n is negative, or when d is negative) will be left to the exercises (see Exercise 17.8).

Partial proof of Theorem 17.13. Let $d > 0$ be an integer, and fix $P(n)$ to be the open sentence

$$P(n)\text{: There are integers } q_n, r_n \text{ such that } n = q_n d + r_n \text{ and } 0 \leq r_n < d.$$

We work by induction to show that $P(n)$ is true for each integer $n \geq 0$.

Base Case: We note that taking $q_0 = r_0 = 0$, then we have $0 = q_0 d + r_0$, and $0 \leq r_0 < d$. Hence, $P(0)$ is true.

Inductive Step: Assume that $P(k)$ is true for some integer $k \geq 0$; in other words, assume that there are integers q_k and r_k such that $k = q_k d + r_k$, with $0 \leq r_k < d$. Then we have that

$$k + 1 = q_k d + r_k + 1.$$

Note that $0 \leq r_k < r_k + 1 \leq d$. We now break the proof up into cases, depending on whether $r_k + 1 = d$ or not.

Case 1: If $r_k + 1 < d$, then we see that $P(k+1)$ is true (with $q_{k+1} = q_k$ and $r_{k+1} = r_k + 1$).

Case 2: If $r_k + 1 = d$, then $k + 1 = q_k d + d = (q_k + 1)d + 0$, so $P(k+1)$ is true (with $q_{k+1} = q_k + 1$ and $r_{k+1} = 0$).

Hence, by induction $P(n)$ is true for each integer $n \geq 0$, when $d > 0$. □

Advice 17.16. This proof of the division algorithm does not immediately give us an easy way to find the quotient and remainder. However, finding q and r is a simple task using standard long division with remainder, as taught in many elementary schools. Although we will not review long division, we demonstrate the work to compute q and r for $n = 978$ and $d = 13$.

$$\begin{array}{r} 75 \\ 13\overline{)978} \\ \underline{91} \\ 68 \\ \underline{65} \\ 3 \end{array}$$

Hence, we find that $q = 75$ and $r = 3$, so that $978 = 75 \cdot 13 + 3$.

17.C Computing the GCD

Listing all the divisors of a and b, as we did in Example 17.9, is a very inefficient way of computing the GCD. The next theorem will give us a very efficient tool to help compute $\text{GCD}(a, b)$.

Theorem 17.17 (The GCD-switching Theorem)**.** *Let $a, b, c, z \in \mathbb{Z}$ and assume that $a = zb + c$. Then* $\text{GCD}(a, b) = \text{GCD}(b, c)$.

Proof. If $b = 0$, then the theorem is obviously true. So we may assume that $b \neq 0$. Fix S to be the set of common divisors of a and b. Similarly, fix T to be the set of common divisors of b and c. We will show that $S = T$. Once this is shown, the largest element of S must be the same as the largest element of T, and the theorem will be proved.

($S \subseteq T$): Assume that $d \in S$. Then $d \,|\, a$ and $d \,|\, b$. Now $c = a - zb$, so we must have $d \,|\, c$. Hence, d is a common divisor of b and c, so $d \in T$. Thus, $S \subseteq T$.

($T \subseteq S$): Now assume that $d \in T$. Then $d \,|\, b$ and $d \,|\, c$. Since $a = zb + c$, we see that $d \,|\, a$. Hence, d is a common divisor of a and b, so $d \in S$. Therefore, $T \subseteq S$.

Hence, $S = T$. □

The next two examples shows how one can use the GCD-switching Theorem.

Example 17.18. Suppose that we wish to compute the GCD of 57 and 39. By the division algorithm we know that $57 = 1 \cdot 39 + 18$. So, the GCD-switching Theorem tells us that

$$\text{GCD}(57, 39) = \text{GCD}(39, 18).$$

These are smaller numbers, so we have made some progress. Next, since $39 = 2 \cdot 18 + 3$, then the GCD-switching Theorem tells us that

$$\text{GCD}(39, 18) = \text{GCD}(18, 3).$$

Again these are smaller numbers, so we have made some more progress. Finally, since $18 = 6 \cdot 3 + 0$, then the GCD-switching Theorem tells us that

$$\text{GCD}(18, 3) = \text{GCD}(3, 0) = 3.$$

Thus, we have found the GCD of 57 and 39 is 3. We did this without listing all the possible divisors.

The computations above can be streamlined by just writing

$$\begin{aligned} 57 &= 1 \cdot 39 + 18 \\ 39 &= 2 \cdot 18 + 3 \\ 18 &= 6 \cdot 3 + 0 \end{aligned}$$

and concluding that $\text{GCD}(57, 39) = 3$. △

In the GCD-switching Theorem, it is not required that $c < |b|$, so the theorem applies in situations where we do not necessarily use the division algorithm. The following example gives just one instance of how this can be useful.

Example 17.19. Let $n \in \mathbb{Z}$. We will compute the possible GCDs for the numbers $3n + 1$ and $n - 2$. Notice that

$$3n + 1 = 3(n - 2) + 7.$$

Thus, by the GCD-switching theorem, we have $\text{GCD}(3n + 1, n - 2) = \text{GCD}(n - 2, 7)$. The only possibilities are $1, 7$.

Can both possibilities happen? Yes, but it depends on the value of n. For example, if $n = 1$, then

$$\text{GCD}(3n + 1, n - 2) = \text{GCD}(4, -1) = 1.$$

If $n = 2$, then

$$\text{GCD}(3n + 1, n - 2) = \text{GCD}(7, 0) = 7.$$ △

17.D The Euclidean algorithm

We now describe the Euclidean algorithm, which very efficiently computes $\text{GCD}(a, b)$, for any $a, b \in \mathbb{Z}$. By Lemma 17.12, we may as well work with only nonnegative integers $a \geq b \geq 0$. The Euclidean algorithm involves nothing more than repeated applications of the division algorithm; in particular, it does not involve computing divisors of a and b. After describing the algorithm, we will prove that it gives the correct output.

Algorithm 17.20. Take as input two integers a and b satisfying $a \geq b \geq 0$.

If $b = 0$, output a, and terminate the algorithm.

If $b \neq 0$, divide a by b to get $a = qb + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < b$, and then rerun the algorithm on the new integers b and r.

To show that an algorithm works correctly there are two things that need to be demonstrated. First, the algorithm must terminate after finitely many steps; it does us no good if the algorithm runs forever and never returns an answer. Second, the output of the algorithm must be correct. We will demonstrate that both of these facts hold true for our algorithm.

First, we show termination. The only possible issue is that we might rerun the algorithm infinitely often. However, each time we rerun the algorithm, we have replaced the second integer b with a smaller nonnegative integer r. Thus, after no more than $|b| + 1$ steps, we must reach a zero remainder.

Second, we show correctness of the output. If $b = 0$, then the output is correct by Example 17.10. If $b \neq 0$, the GCD is unchanged by the GCD-switching Theorem, which is Theorem 17.17.

In the next example, we demonstrate a concrete use of the Euclidean algorithm.

Example 17.21. We will find $\text{GCD}(1073, -1537)$. After applying Lemma 17.12, we have $a = 1537$ and $b = 1073$. Using Algorithm 17.20 produces the chain:

$$\begin{aligned} 1537 &= 1 \cdot 1073 + 464 \\ 1073 &= 2 \cdot 464 + 145 \\ 464 &= 3 \cdot 145 + 29 \\ 145 &= 5 \cdot 29 + 0 \end{aligned}$$

In the last equality, the remainder is 0. Thus, in the next step, the algorithm ends by outputting 29. Hence, $\text{GCD}(1073, -1537) = 29$. Note that 29 is also the last nonzero remainder, circled in red above. △

Remark 17.22. Notice that the number of divisions is actually significantly less than $|b|$. In fact, it can be shown (although we will not prove it) that the number of divisions required is always less than $5 \log_{10} |b|$, which is actually slightly less than 5 times the number of digits in $|b|$. Hence, for example, if b is a four digit number, no more than 20 divisions will ever be needed. ▲

17.E Exercises

Exercise 17.1. For the given values of n and d, compute the values of q and r guaranteed by the division algorithm.

(a) Fix $n = 17$ and $d = 5$.
(b) Fix $n = 17$ and $d = -5$.
(c) Fix $n = -17$ and $d = 5$.
(d) Fix $n = -17$ and $d = -5$.
(e) Fix $n = 256$ and $d = 25$.
(f) Fix $n = 256$ and $d = -25$.
(g) Fix $n = -256$ and $d = 25$.
(h) Fix $n = -256$ and $d = -25$.

Exercise 17.2. Let a be an integer. Recall that a is even if there is some $k \in \mathbb{Z}$ such that $a = 2k$, and recall that a is odd if there is some $\ell \in \mathbb{Z}$ such that $a = 2\ell + 1$. Prove the following statements, which we took for granted previously. (Hint: Use the division algorithm with $d = 2$.)

(a) Every integer is even or odd.
(b) No integer is both even and odd.

Exercise 17.3. Write out all the divisors of 60 in a list, and then all the divisors of 42 in a separate list. Write the common divisors in a third list, and find the GCD. (All the lists should be ordered from least to greatest.)

Exercise 17.4. Use the Euclidean algorithm to compute the following GCDs.

(a) $\text{GCD}(60, 42)$.
(b) $\text{GCD}(667, 851)$.
(c) $\text{GCD}(1855, 2345)$.
(d) $\text{GCD}(589, 437)$.

Exercise 17.5. Recall that the Fibonacci numbers are defined by setting $F_1 = 1$, setting $F_2 = 1$, and for any integer $n \geq 3$ setting $F_n = F_{n-1} + F_{n-2}$.

Prove by induction that $\text{GCD}(F_{n+1}, F_n) = 1$, for each $n \in \mathbb{N}$.

Exercise 17.6. Let $n \in \mathbb{Z}$. Prove that $\text{GCD}(2n + 1, 4n + 3) = 1$.

Exercise 17.7. Let $n \in \mathbb{Z}$. Prove that $\text{GCD}(6n + 2, 12n + 6) = 2$.

Exercise 17.8. Complete the proof of Theorem 17.13 as follows.

(a) Using the fact that the theorem is true for arbitrary integers $n \geq 0$ and $d > 0$, next prove the theorem for arbitrary integers $n < 0$ and $d > 0$. (Hint: If $n < 0$, then $-n > 0$. Use the proven case of the division algorithm to write $-n = qd + r$, for some $q, r \in \mathbb{Z}$ with $0 \leq r < d$. Then $n = (-q)d - r$. If $r = 0$, we are done; otherwise, we need to make an adjustment to get the remainder between 0 and d.)
(b) Using the fact, from part (a), that the theorem is true for any integer n and any integer $d > 0$, prove the theorem for any integer n and any integer $d < 0$. (This will complete the proof.)

18 The extended Euclidean algorithm

18.A The GCD as a linear combination

We now recall the result of Exercise 13.7.

Theorem 18.1. *Each nonempty subset of* $\mathbb{N}$ *has a least element.*

We will use this theorem to prove an important and useful statement about $\text{GCD}(a, b)$, for any $a, b \in \mathbb{Z}$. The next definition will help us to state the result.

Definition 18.2. An (*integral*) *linear combination* of two integers a and b is a number of the form $ax + by$ where $x, y \in \mathbb{Z}$.

Example 18.3. Fix $a = 16$ and $b = 21$. We will list some of the linear combinations of a and b.

We see that 37 is a linear combination of 16 and 21, since

$$37 = 16 + 21 = a + b = a \cdot 1 + b \cdot 1.$$

We see that $0 = a \cdot 0 + b \cdot 0$ is a linear combination of 16 and 21. (Will 0 be an integral linear combination of any two integers a and b?)

What is the smallest linear combination of a and b? (By smallest, we will mean in the ordering on the integers.) There isn't a smallest combination! For instance

$$a \cdot (-100) + b \cdot (-100) = -3700.$$

We can form negative numbers that can be as "small" as we like.

However, there is a smallest *positive* linear combination of a and b . We see that

$$1 = 16 \cdot 4 + 21 \cdot (-3).$$

There are no positive integers smaller than 1, so this is indeed the smallest. △

Example 18.4. When performing the division algorithm, the remainder is a linear combination of the numerator and denominator. Indeed,

$$r = n - qd = n \cdot 1 + d \cdot (-q).$$ △

Theorem 18.5. *Let a and b be integers, not both equal to 0. The smallest positive integral linear combination of a and b is* $\text{GCD}(a, b)$.

Proof. Fix S to be the set of positive integral linear combinations of a and b. In other words,

$$S = \{ax + by \,:\, x, y \in \mathbb{Z} \text{ and } ax + by > 0\}.$$

It is clear that S is a subset of the natural numbers, since its elements are positive integers. In addition, S is nonempty since it contains at least one of the following:

$$a = a \cdot 1 + b \cdot 0, \quad -a = a \cdot (-1) + b \cdot 0, \quad b = a \cdot 0 + b \cdot 1, \quad -b = a \cdot 0 + b \cdot (-1).$$

Hence, S has a least element, which we call s. From the definition of S, there exist some elements $x, y \in \mathbb{Z}$ satisfying $s = ax + by$. Note that $s > 0$.

Fix $d = \text{GCD}(a, b)$. Then $d \,|\, a$ and $d \,|\, b$, so by Theorem 7.15, $d \,|\, ax + by$, and we have that $d \,|\, s$. Hence, $d \leq s$.

Now we use the division algorithm to write $a = qs + r$ with $0 \leq r < s$. Then

$$r = a - qs = a - q(ax + by) = a(1 - qx) + b(-qy)$$

is an integral linear combination of a and b. If r were positive, then r would be an element of S that is smaller than s (which would contradict the minimality of s). Hence, r must be 0. Therefore $a = qs$ and we see that $s \,|\, a$. A similar argument shows that $s \,|\, b$. Since s is a common divisor of a and b, it cannot be larger than the greatest common divisor d. Hence, $s \leq d$.

Combining the facts that $d \leq s$ and $s \leq d$, we see that $d = s$. □

Using Theorem 18.5, one can show that the linear combinations of a and b are exactly the integer multiples of $\text{GCD}(a, b)$, see Exercise 18.4.

Example 18.6. Fix $a = 6$ and $b = 9$. The theorem asserts that $3 = \text{GCD}(6, 9)$ should be the smallest positive linear combination of a and b.

We see that $3 = 6(-1)+9(1)$ is indeed a linear combination. If we had $2 = 6x+9y$, then since $3 \,|\, 6$ and $3 \,|\, 9$, we would have $3 \,|\, 2$, a contradiction. Similarly, 1 cannot be a linear combination of a and b. Therefore 3 is indeed the smallest positive linear combination and is the GCD.

Note that $-15 = 3 \cdot (-5)$ is a multiple of $3 = \text{GCD}(6, 9)$. Hence, as indicated in the sentence preceding this example, we expect -15 to be a linear combination of 6 and 9. Note that

$$-15 = 3 \cdot (-5) = (6(-1) + 9(1)) \cdot (-5) = 6(5) + 9(-5)$$

is indeed a linear combination of 6 and 9. △

18.B Calculating the GCD as a linear combination

Now that we know that $\text{GCD}(a, b)$ can be written as an integral linear combination of a and b, the natural question is how to compute x and y so that

$$\text{GCD}(a, b) = ax + by.$$

The main idea is to first find the GCD using the Euclidean algorithm; this gives us a sequence of equations arising from the division algorithm. We rewrite these equations by solving for the remainders. Working backwards through this new list of equations, we can write the GCD as a linear combination of each of the previous numerators and denominators.

We demonstrate how this works with a couple of examples.

Example 18.7. We find $\text{GCD}(493, 391)$, and we also find some $x, y \in \mathbb{Z}$ such that $\text{GCD}(493, 391) = 493x + 391y$.

First, we perform the Euclidean algorithm, and solve each of the resulting equations (except the very last one) for the remainder.

$$\begin{aligned} \underline{493} &= 1 \cdot \underline{391} + \underline{102} \quad &\mapsto \quad \underline{102} &= \underline{493} - 1 \cdot \underline{391} \\ \underline{391} &= 3 \cdot \underline{102} + \underline{85} \quad &\mapsto \quad \underline{85} &= \underline{391} - 3 \cdot \underline{102} \\ \underline{102} &= 1 \cdot \underline{85} + \underline{17} \quad &\mapsto \quad \underline{17} &= \underline{102} - 1 \cdot \underline{85} \\ \underline{85} &= 5 \cdot \underline{17} + \underline{0} \end{aligned}$$

Note that we have underlined the numerators, denominators, and remainders, but not the quotients. This will help us keep track of things more easily. The last nonzero remainder is 17, so we know that $\text{GCD}(493, 391) = 17$.

Now we see that $\underline{17} = \underline{102} - 1 \cdot \underline{85}$, from the bottom right equation. In other words, we have now written 17 as a linear combination of 102 and 85. Our next goal is to write 17 as a combination of the previous numerator and denominator, 391 and 102. Looking at the preceding equation (the second one from the bottom, on the right), we see an expression for 85 that we plug into this equation, so

$$\begin{aligned} \underline{17} &= \underline{102} - 1 \cdot (\quad \underline{85} \quad) \\ &= \underline{102} - 1 \cdot (\underline{391} - 3 \cdot \underline{102}) \\ &= \underline{102} - 1 \cdot \underline{391} + 3 \cdot \underline{102} \\ &= 4 \cdot \underline{102} - 1 \cdot \underline{391}. \end{aligned}$$

So, now 17 is a linear combination of 391 and 102. Going one equation higher, we see an expression for 102; namely, $\underline{102} = \underline{493} - 1 \cdot \underline{391}$. We plug this into our expression for 17 to get

$$\begin{aligned} \underline{17} &= 4 \cdot (\quad \underline{102} \quad) - 1 \cdot \underline{391} \\ &= 4 \cdot (\underline{493} - 1 \cdot \underline{391}) - 1 \cdot \underline{391} \\ &= 4 \cdot \underline{493} - 4 \cdot \underline{391} - 1 \cdot \underline{391} \\ &= 4 \cdot \underline{493} - 5 \cdot \underline{391}, \end{aligned}$$

and we now have expressed

$$\text{GCD}(493, 391) = 17 = 493 \cdot 4 + 391 \cdot (-5)$$

as a linear combination of 493 and 391. △

Advice 18.8. Probably the most difficult part of this algorithm is the temptation to oversimplify the expression for the GCD. Taken to the extreme, each expression for 17 above can be simplified to equal 17. It is important to keep track of the remainders (perhaps by underlining them or boxing them) and treat them as if they were variables rather than numbers.

Example 18.9. We will now find the GCD of 221 and 136, and write it as an integral linear combination of 221 and 136.

We perform the Euclidean algorithm, and solve each of the resulting equations for the remainder. In order to remind ourselves to treat the original numbers and the remainders as if they were variables, we will again underline them.

$$\begin{aligned}
\underline{221} &= 1\cdot\underline{136}+\underline{85} &\mapsto\quad \underline{85} &= \underline{221}-1\cdot\underline{136}\\
\underline{136} &= 1\cdot\underline{85}+\underline{51} &\mapsto\quad \underline{51} &= \underline{136}-1\cdot\underline{85}\\
\underline{85} &= 1\cdot\underline{51}+\underline{34} &\mapsto\quad \underline{34} &= \underline{85}-1\cdot\underline{51}\\
\underline{51} &= 1\cdot\underline{34}+\underline{17} &\mapsto\quad \underline{17} &= \underline{51}-1\cdot\underline{34}\\
\underline{34} &= 2\cdot\underline{17}+\underline{0}
\end{aligned}$$

The last nonzero remainder is $\underline{17}$, and we have $\underline{17} = \underline{51} - 1\cdot\underline{34}$ (from the bottom equation on the right). The previous equation is $\underline{34} = \underline{85} - 1\cdot\underline{51}$. Substituting for $\underline{34}$, we obtain

$$\begin{aligned}
\underline{17} &= \underline{51} - 1\cdot(\quad \underline{34} \quad)\\
&= \underline{51} - 1\cdot(\underline{85} - 1\cdot\underline{51})\\
&= \underline{51} - 1\cdot\underline{85} + 1\cdot\underline{51}\\
&= 2\cdot\underline{51} - 1\cdot\underline{85},
\end{aligned}$$

where we have been careful to treat underlined numbers as variables, and not combine them with other numbers.

The equation we use to substitute for $\underline{51}$ is $\underline{51} = \underline{136} - 1\cdot\underline{85}$, so

$$\begin{aligned}
\underline{17} &= 2\cdot(\quad \underline{51} \quad) - 1\cdot\underline{85}\\
&= 2\cdot(\underline{136} - 1\cdot\underline{85}) - 1\cdot\underline{85}\\
&= 2\cdot\underline{136} - 2\cdot\underline{85} - 1\cdot\underline{85}\\
&= 2\cdot\underline{136} - 3\cdot\underline{85}.
\end{aligned}$$

Finally, we have $\underline{85} = \underline{221} - 1\cdot\underline{136}$. Substituting in for $\underline{85}$ we obtain the following:

$$\begin{aligned}
\underline{17} &= 2\cdot\underline{136} - 3\cdot(\quad \underline{85} \quad)\\
&= 2\cdot\underline{136} - 3\cdot(\underline{221} - 1\cdot\underline{136})\\
&= 2\cdot\underline{136} - 3\cdot\underline{221} + 3\cdot\underline{136}\\
&= 5\cdot\underline{136} - 3\cdot\underline{221}.
\end{aligned}$$

Hence, $\mathrm{GCD}(221, 136) = 17 = 136\cdot 5 + 221\cdot(-3)$. △

18.C Relative primality

The fact that $\text{GCD}(a, b)$ can be written as an integral linear combination of a and b has many important consequences. In particular, we saw in the proof of Theorem 18.5 that $\text{GCD}(a, b)$ is in fact the smallest positive integral linear combination of a and b. This yields the following theorem.

Theorem 18.10. *Let $a, b \in \mathbb{Z}$. Then $\text{GCD}(a, b) = 1$ if and only if $1 = ax + by$ for some $x, y \in \mathbb{Z}$.*

Proof. If $\text{GCD}(a, b) = 1$, Theorem 18.5 tells us that $1 = ax + by$ for some $x, y \in \mathbb{Z}$.

Conversely, if $1 = ax + by$ for some $x, y \in \mathbb{Z}$, then 1 is the smallest positive number that can be written as an integral linear combination of a and b (since there are no positive integers smaller than 1). Hence, $1 = \text{GCD}(a, b)$. □

We give a special name to a pair of numbers that have GCD equal to 1.

Definition 18.11. Let $a, b \in \mathbb{Z}$. If $\text{GCD}(a, b) = 1$, then we say that a and b are *relatively prime.*

Example 18.12. Since $\text{GCD}(15, 7) = 1$, the numbers 15 and 7 are relatively prime. On the other hand, $\text{GCD}(5, 30) = 5$, so 5 and 30 are not relatively prime. △

We now prove two useful properties of relatively prime integers.

Theorem 18.13. *Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $\text{GCD}(a, b) = 1$, then $a \mid c$.*

Proof. Let $a, b, c \in \mathbb{Z}$. Assume that $a \mid bc$ and $\text{GCD}(a, b) = 1$. Since $a \mid bc$, we see that $bc = ak$ for some $k \in \mathbb{Z}$. Also, for some $x, y \in \mathbb{Z}$, we have $1 = ax + by$. Multiplying this last equation by c, we obtain

$$c = c \cdot 1 = c(ax + by) = (ac)x + (bc)y = (ac)x + (ak)y = a(cx + ky).$$

Hence, since $cx + ky \in \mathbb{Z}$, we see that $a \mid c$. □

As a nice application of this theorem we have the following:

Example 18.14. Assume that $3x$ is even. Then $2 \mid 3x$. Since $\text{GCD}(2, 3) = 1$, we see that $2 \mid x$. So x is even. (Previously we proved the implication "if $3x$ is even then x is even" contrapositively.) △

The next theorem gives us sufficient conditions under which we can expect the product of two numbers to divide into another number.

Theorem 18.15. *Let $a, b, c \in \mathbb{Z}$. If $a \mid c$ and $b \mid c$ and $\text{GCD}(a, b) = 1$, then $ab \mid c$.*

Proof. Let $a, b, c \in \mathbb{Z}$. Assume that $a \mid c$ and $b \mid c$ and $\text{GCD}(a, b) = 1$. Then for some $k, \ell, x, y \in \mathbb{Z}$, we have $c = ak$, $c = b\ell$, and $1 = ax + by$. Multiplying this last equation by c, we get

$$c = cax + cby = (b\ell)ax + (ak)by = ab(x\ell + ky).$$

Since $x\ell + ky \in \mathbb{Z}$, we see that $ab \mid c$. □

Example 18.16. If $2 \mid x$ and $3 \mid x$, we see that $6 \mid x$, since $\text{GCD}(2, 3) = 1$. △

Warning 18.17. Note that neither of the previous two theorems is true if we replace the assumption $\text{GCD}(a, b) = 1$ with $a \nmid b$. For the first theorem, taking $a = 4$, $b = 6$, and $c = 2$, we have that $4 \mid (6 \cdot 2)$, and $4 \nmid 6$, but it is not the case that $4 \mid 2$.

For the second theorem, taking $a = 12$, $b = 18$, and $c = 36$, we see that both a and b divide 36, but $ab \nmid 36$. (Can you find simpler counterexamples?)

18.D Exercises

Exercise 18.1. For each pair of numbers a and b below, calculate $\text{GCD}(a, b)$ and find $x, y \in \mathbb{Z}$ such that $\text{GCD}(a, b) = ax + by$.

(a) Take $a = 15$ and $b = 27$.
(b) Take $a = 29$ and $b = 23$.
(c) Take $a = 91$ and $b = 133$.
(d) Take $a = 221$ and $b = 377$.

Exercise 18.2. Let $a, n \in \mathbb{Z}$. Assume that $\text{GCD}(a, n) = 1$. Prove that there is some $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{n}$. (Hint: Use Theorem 18.10.)

Informally, this result says that there is an element b that acts like the reciprocal of a, modulo n.

Exercise 18.3. Let $a, b \in \mathbb{Z}$, with $b \neq 0$, and fix $d = \text{GCD}(a, b)$.

(a) Must it be the case that $\text{GCD}(a, b/d) = 1$? Prove your answer.
(b) Prove or disprove: If c is a positive common divisor of a and b, and $c = ax + by$ for some $x, y \in \mathbb{Z}$, then $c = d$. (Hint: Can you show that $c \leq d$? Can you show that $d \leq c$?)

Exercise 18.4. Let $a, b, n \in \mathbb{Z}$, and fix $d = \text{GCD}(a, b)$. Prove that $d \mid n$ if and only if n is a linear combination of a and b.

Exercise 18.5. Let $a, b, c, d \in \mathbb{Z}$. Assume that $\text{GCD}(a, b) = 1$. Prove that if $c \mid a$ and $d \mid b$, then $\text{GCD}(c, d) = 1$.

Exercise 18.6. The following steps lead one through a proof of the existence and uniqueness of the lowest terms representation of a rational number.

(a) Let $a, b \in \mathbb{Z}$, not both zero, and fix $d = \text{GCD}(a, b)$. Prove that

$$\text{GCD}\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

(Hint: Use Theorem 18.10.)

(b) Prove that any rational number a/b (with $a, b \in \mathbb{Z}$ and $b \neq 0$) can be represented as a fraction r/s (with $r, s \in \mathbb{Z}$ and $s \neq 0$) satisfying $\text{GCD}(r, s) = 1$. (Hint: Fix $d = \text{GCD}(a, b)$. Define r and s in terms of a, b, and d, and use part (a).)

(c) Prove that in part (b) we can also guarantee that $s > 0$. (Hint: Modify the definitions of r and s if needed.)

(d) Prove that every rational number has a *unique* representation as in part (c). This is the *lowest terms* representation of the rational number. (Hint: Assume that $r/s = r'/s'$ with
(1) $r, r', s, s' \in \mathbb{Z}$,
(2) $s, s' > 0$, and
(3) $\text{GCD}(r, s) = 1 = \text{GCD}(r', s')$.
Prove that $s = s'$, and then that $r = r'$.)

Exercise 18.7. Let a, b be positive integers. A *common multiple* of a and b is an integer n such that $a \mid n$ and $b \mid n$. The *least common multiple* of a and b, written $\text{LCM}(a, b)$, is the smallest positive common multiple of a and b.

(a) Determine the LCM of 12 and 18.

(b) Determine the LCM of 21 and 35.

(c) Prove that $\text{LCM}(a, b) = \frac{ab}{d}$, where $d = \text{GCD}(a, b)$.
(Hint: Show that ab/d is a common multiple of a and b. Then show that it divides (and is thus no larger than) every other positive common multiple of a and b. You may wish to factor $a = a'd$ and $b = b'd$ and use the fact (from Exercise 18.6(a)) that $\text{GCD}(a', b') = 1$.)

19 Prime numbers

Now that we have a good understanding of divisibility in the integers we are prepared to define and study the multiplicative building blocks of the integers. As far as multiplication is concerned, prime numbers are the "atoms" from which other integers are formed.

19.A Definition of prime numbers

Definition 19.1. A natural number p is *prime* if $p > 1$ and the only positive divisors of p are 1 and p. A natural number n is *composite* if $n > 1$ and n is not prime.

Example 19.2. We know that all positive divisors of a positive integer n are between 1 and n, so we may check whether a given integer is prime. The integer 2 is prime, since there are no integers between 1 and 2. The integer 3 is prime, since it is not divisible by 2. Similarly 5 is prime, since it is not divisible by 2, 3, or 4. Note that 4 is not prime, since it is divisible by 2.

The first few prime numbers are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73. \qquad \triangle$$

If a number is composite, then it has a positive factor besides itself and 1. We expand a bit on this fact in the following theorem.

Theorem 19.3. *Let $a \in \mathbb{N}$. If a is composite, then there are positive integers b and c, both strictly between 1 and a, such that $a = bc$.*

Proof. Assume a is composite. Since $a > 1$ and a is not prime, it has a positive divisor b with $1 < b < a$. So $a = bc$ for some $c \in \mathbb{Z}$. Clearly c is positive, and c not equal to 1 since $a \neq b$. Hence, $c > 1$.

On the other hand, by Theorem 17.1, since $c \,|\, a$ we have $c \leq a$. But $c \neq a$ since $b \neq 1$, so $1 < c < a$. $\square$

Examples of the previous theorem in action, for small composite numbers, include:

$$4 = 2 \cdot 2, \qquad 6 = 2 \cdot 3 = 3 \cdot 2, \qquad 8 = 2 \cdot 4 = 4 \cdot 2,$$
$$9 = 3 \cdot 3, \qquad 10 = 2 \cdot 5 = 5 \cdot 2, \qquad \text{and} \qquad 12 = 2 \cdot 6 = 3 \cdot 4 = 4 \cdot 3 = 6 \cdot 2.$$

We next prove the following useful fact about prime numbers.

Theorem 19.4. *Let p be a prime number and let $a \in \mathbb{Z}$. Then*

$$\mathrm{GCD}(p, a) = \begin{cases} p & \text{if } p \,|\, a, \\ 1 & \text{if } p \nmid a. \end{cases}$$

Proof. We know that $\text{GCD}(p, a)$ must be a positive divisor of p, so it must be 1 or p. If $p \mid a$ then p is clearly the largest common divisor; similarly, if $p \nmid a$, then 1 is the largest common divisor. □

When we combine Theorem 19.4 with Theorem 18.13 we obtain the following important description of prime numbers. The implication (1) ⇒ (2) in the following theorem is known as *Euclid's Lemma*, since Euclid proved it in the *Elements*.

Theorem 19.5. *Let $a \in \mathbb{N}$ with $a > 1$. The following are equivalent:*
(1) *The number a is prime.*
(2) *For any $b, c \in \mathbb{Z}$, if $a \mid bc$, then $a \mid b$ or $a \mid c$.*

Proof. (1) ⇒ (2): Assume that a is a prime number, and that $a \mid bc$ and $a \nmid b$. Then $\text{GCD}(a, b) = 1$, so by Theorem 18.13 we see that $a \mid c$.

(2) ⇒ (1): Working contrapositively, suppose that a is not prime, so that (1) is false. Then a is composite, and thus $a = bc$ for some integers b, c between 1 and a by Theorem 19.3. Now $a \mid bc$ and $a \nmid b$ and $a \nmid c$ (since b and c are positive and smaller than a). Hence, (2) is false. □

In Exercise 19.2 you will use induction to prove the following natural extension of Euclid's Lemma.

Theorem 19.6. *Let p be a prime number, let n be a natural number, and let $a_1, \ldots, a_n \in \mathbb{Z}$. If*

$$p \mid a_1 a_2 \cdots a_n,$$

then $p \mid a_i$ for some $1 \leq i \leq n$.

19.B Divisibility by primes

We know that if a number is composite, then it has a factorization into smaller numbers. One might wonder if it is possible to guarantee that these smaller numbers *must* also be composite. In other words, is it possible to find a number that is so composite that all of its factors are composite? The following theorem answers that question (in the negative).

Theorem 19.7. *Every integer larger than 1 is divisible by a prime number.*

Proof. Let $a > 1$ be an integer. The set

$$S = \{b \in \mathbb{N} : b \mid a \text{ and } b > 1\}$$

is nonempty (since a is an element), so it has a least element p. By Exercise 19.3, we conclude that p is prime. □

Next, we prove that every positive integer is a product of primes. Note that in this theorem we allow the possibility that a number (namely 1) can be a product of *zero* primes, or (if it is prime) a product of a single prime.

Theorem 19.8. *Let $a \in \mathbb{N}$. Then a is a product of primes.*

Proof. Fix $P(n)$ to be the open sentence

$$P(n)\text{: } n \text{ is a product of primes.}$$

We wish to prove that $P(n)$ is true for each integer $n \geq 1$, by strong induction.

Base Case: We note that $P(1)$ is true, since 1 is a product of zero primes.

Inductive Step: Suppose, for some integer $k \geq 1$, that $P(1), \ldots, P(k)$ are each true. In other words, assume that each integer from 1 to k is a product of primes.

Our next goal is to show that $P(k+1)$ is true. To do so, we now break the proof into cases depending on whether $k+1$ is prime or composite.

Case 1: Suppose $k+1$ is prime. Then $P(k+1)$ is true; $k+1$ is a product of the single prime $k+1$.

Case 2: Suppose $k+1$ is composite. Then we may factor $k+1 = bc$, with $1 < b < k+1$ and $1 < c < k+1$ (so $2 \leq b \leq k$ and $2 \leq c \leq k$). Hence, by our inductive hypothesis, $P(b)$ and $P(c)$ are both true; both b and c are products of primes. Hence, the product bc is a product of primes, so $P(k+1)$ is true.

Therefore, by induction the theorem is true. □

This theorem can be greatly strengthened; we will now prove that every integer not only has a prime factorization, but that its prime factorization is unique. The importance of this theorem is evident from its name: The Fundamental Theorem of Arithmetic.

Theorem 19.9 (The Fundamental Theorem of Arithmetic)**.** *Any integer $n > 1$ has a factorization into primes, written*

$$n = p_1 p_2 \cdots p_r$$

(for some $r \in \mathbb{N}$) with $p_1 \leq p_2 \leq \ldots \leq p_r$, and this factorization is unique.

Proof. We have already seen that n can be written as a product of one or more primes. We order the primes so that they are in nondecreasing order. All that remains to be proved is the uniqueness statement, which we will prove by strong induction.

Fix $P(n)$ to be the open sentence

$$P(n)\text{: } n \text{ has a unique factorization into prime numbers.}$$

Base Case: Clearly, $P(2)$ is true; 2 is prime, so the only way to factor it into $2 = p_1 \cdots p_r$ is to have $r = 1$ and $p_1 = 2$. A similar argument works for any prime p; hence $P(p)$ is true.

Inductive Step: Assume, for some integer $k \geq 2$, that $P(2), \ldots, P(k)$ are each true. In other words, assume that each integer from 2 to k has a unique prime factorization. We wish to prove that $P(k+1)$ is true. We divide the proof into two cases.

Case 1: If $k+1$ is prime, then $P(k+1)$ is true as explained above.

Case 2: If $k+1$ is not prime, assume that

$$k+1 = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_\ell$$

has two prime factorizations, with $p_1, p_2, \ldots, p_m, q_1, q_2, \ldots, q_\ell$ all prime, and such that $p_1 \leq p_2 \leq \ldots \leq p_m$ and $q_1 \leq q_2 \leq \ldots \leq q_\ell$. Note that $p_1 \,|\, k+1$, so

$$p_1 \,|\, q_1 q_2 \cdots q_\ell.$$

Hence, by Exercise 19.2, we have that $p_1 \,|\, q_i$ for some index i. Since q_i is prime and $p_1 \neq 1$, we must have $p_1 = q_i$. This yields $q_1 \leq q_i = p_1$.

By a similar argument $p_1 \leq q_1$. Thus, $p_1 = q_1$.

Now, $(k+1)/p_1 = p_2 \cdots p_m = q_2 \cdots q_\ell$. Since $2 \leq (k+1)/p_1 \leq k$, we see that $(k+1)/p_1$ has a unique factorization into primes, by our inductive hypothesis. Hence $m = \ell$, and $p_i = q_i$ for each index i from 2 to m. Since $p_1 = q_1$, we see that the two factorizations that we had for $k+1$ were identical. Hence, $k+1$ has a unique factorization into primes, and $P(k+1)$ is true.

Thus, by induction, every integer $n > 1$ has a unique factorization into primes. □

Remark 19.10. We note that typically the factorization of a number into primes will be simplified by combining copies of the same prime together. For instance, if we wish to factor 720, rather than writing $720 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$ we might write

$$720 = 2^4 \cdot 3^2 \cdot 5.$$

This is a more compact representation of the factorization. Using this convention, we can restate Theorem 19.9 as saying that every integer $n > 1$ can be uniquely written in the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = \prod_{i=1}^{k} p_i^{a_i},$$

with $k \in \mathbb{N}$, each p_i prime, $p_1 < \ldots < p_k$, and with each $a_i \in \mathbb{N}$. (Note that the symbol $\prod_{i=1}^{k}$ works just like the symbol $\sum_{i=1}^{k}$, except for multiplication instead of addition.) A factorization of this form has a special name as in the next definition. ▲

Definition 19.11. Let $n > 1$ be an integer. The prime factorization

$$n = \prod_{i=1}^{k} p_i^{a_i}$$

with $k \in \mathbb{N}$, with $p_1 < \ldots < p_k$ all prime, and with each $a_i \in \mathbb{N}$, is called the *canonical factorization* of n.

Example 19.12. The canonical factorization of 5040 is $2^4 \cdot 3^2 \cdot 5^1 \cdot 7^1$. In the notation of Definition 19.11 we have $p_1 = 2$, $a_1 = 4$, $p_2 = 3$, $a_2 = 2$, $p_3 = 5$, $a_3 = 1$, $p_4 = 7$, and $a_4 = 1$. △

Remark 19.13. The statement of the Fundamental Theorem of Arithmetic is not constructive. It provides no algorithm for actually finding a prime factorization. The theorem does guarantee that whatever (correct) method we use to find a factorization will yield the same answer as any other method.

One simple method of finding a prime factorization is trial division. Given an integer $n \geq 2$, start with $k = 2$ and divide to check if n is divisible by k. If it is, add k to the list of factors of n, replace n by n/k, and repeat the process by finding the factors of n/k. (Stop if $n/k = 1$.) If n is not divisible by k, replace k by $k + 1$ and repeat the process.

We demonstrate this method by finding the prime factorization of 45. First, 45 is not divisible by 2. Hence, we check whether it is divisible by 3. It is, so we add 3 to the list of prime factors, and replace 45 by 15. Now 15 is divisible by 3, so we add 3 again to the list of prime factors, and replace 15 by $15/3 = 5$. Now 5 is not divisible by 3 or by 4, but it is divisible by 5, so we add 5 to the list of prime factors, and replace 5 by $5/5 = 1$. We are now done. The prime factorization of 45 is $3 \cdot 3 \cdot 5$.

The method just described is a very inefficient method of factoring and can in fact (with just a little thought) be improved greatly. However, factoring integers seems to be an inherently difficult problem. The search for efficient factorization techniques is an ongoing research effort, even today. ▲

19.C The infinitude of primes

Thousands of years ago, the ancient Greeks knew that there were infinitely many primes. We give here an adaptation of the proof given by Euclid of this fact. What we will prove is actually that any finite set of primes is missing some prime. This clearly implies that the set of all primes must be infinite.

Theorem 19.14. *There are infinitely many prime numbers.*

Proof. Let S be any finite set of prime numbers. Fix

$$N = 1 + \prod_{p \in S} p.$$

Then $N \geq 2$, so N is divisible by some prime q by Theorem 19.7.

Using the division algorithm to divide N by any given prime $p \in S$ leaves a remainder of 1, so no prime in S divides N. Hence, q is a prime that is not in S. Therefore, S is missing some prime.

Since each finite set of primes is missing some prime, there must be infinitely many primes. □

Remark 19.15. We can test this proof in specific situations by selecting any finite set of primes that we wish to consider, and constructing a prime not in that set. For instance, fix $S = \{2, 3, 5, 7, 11\}$. Then $N = 2311$. In this case, N is prime and $N \notin S$.

Now suppose that $S = \{2, 3, 5, 7, 11, 13, 17, 19\}$. Then $N = 9699691 = 347 \cdot 27953$. Both 347 and 27953 are primes not in S. ▲

19.D Exercises

Exercise 19.1. For each of the following integers n, give its canonical prime factorization.

(a) $n = 27$. (b) $n = 3072$. (c) $n = 60$.

Exercise 19.2. Let p be a prime number. Fix $P(n)$ to be the open sentence

If p divides any product of n integers, then p divides one of those integers.

Prove by induction that $P(n)$ is true for each $n \in \mathbb{N}$. (Hint: The case $n = 2$ is Theorem 19.5. For the inductive step, when showing $P(k+1)$ you should assume its premise, namely that $p \mid a_1 \cdots a_k a_{k+1}$, for some $a_1, \ldots, a_{k+1} \in \mathbb{Z}$.)

Exercise 19.3. Let $n > 1$ be a natural number. Prove that the smallest divisor d of n that is greater than 1 is prime.

Exercise 19.4. The goal of this exercise is to prove that there are infinitely many primes that are congruent to -1 modulo 3. We will do this in a series of steps.

(a) Prove that, with only one exception, each prime number is either congruent to 1 modulo 3 or congruent to -1 modulo 3.

(b) Prove that for any $n \in \mathbb{N}$ and any $a_1, \ldots, a_n \in \mathbb{Z}$, if $a_i \equiv 1 \pmod 3$ for each $1 \leq i \leq n$, then the product $a_1 a_2 \cdots a_n$ is also congruent to 1 modulo 3. (Use induction.)

(c) Let $N \in \mathbb{N}$. Prove that if $N \equiv -1 \pmod 3$, then N is divisible by some prime p such that $p \equiv -1 \pmod 3$. (Hint: Working contrapositively, assume that no prime factor of N is congruent to -1 modulo 3. Break into cases, considering first what happens if all the prime factors are congruent to 1 modulo 3. The previous two parts of the problem may be useful; don't forget that there is an exceptional prime.)

(d) Finish the proof that there are infinitely many primes p such that

$$p \equiv -1 \pmod 3.$$

(Hint: Let $\{p_1, \ldots, p_n\}$ be any finite set of primes that are each congruent to -1 modulo 3. Adjust the proof of Theorem 19.14, using $-1 + 3(p_1 p_2 \cdots p_n)$ in place of N.)

Exercise 19.5. Prove that there are infinitely many primes p such that

$$p \equiv -1 \pmod 4.$$

(Hint: Do steps (a) through (d) of the previous exercise with 3 replaced by 4 everywhere.)