Divisibility

a supplement to

Number Systems

by Sergei Ovchinnikov

AMS 2015

ISBN 978-1-4704-2018-5

Contents

0 About the Supplement

The first two chapters of the textbook "Number Systems" [1] are devoted to the rigorous development of the theory of integers (including natural numbers in Chapter 1). To keep the volume of the book down to acceptable limits, some properties of integers are not included in the text. Most notably, the notion of *divisibility* of integers is absent from the book.

Divisibility is one of the basic concepts of arithmetic and number theory, associated with the division operation. From the point of view of set theory, the divisibility of integers is a relation defined on the set of integers.

Only very basic properties of the divisibility relation are established in the Supplement. The highlights of the presentation include the *Euclidean Algorithm* for finding the Greatest Common Divisor of two integers and the *Fundamental Theorem of Arithmetic* also known as the *Unique Factorization Theorem*.

I hope that the material of this Supplement can serve as a launching pad for reader's studies of other topics in number theory.

Sergei Ovchinnikov
sergei@sfsu.edu
July 2022

1 Basic Definitions and Properties

Definition 1.1 *Let a and b be integers. We say that a* divides *b, and write $a \mid b$, if there is an integer q such that $b = a \cdot q$. In this case, we also say that b is* divisible *by a and call a and q* divisors *or* factors *of b.*

If a does not divide b, we write $a \nmid b$.

The following are trivial instances of these concepts:

(a) Every integer divides 0. ($0 = a \cdot 0$, $a \in \mathbf{Z}$.)

(b) Numbers 1 and -1 divide every integer. ($b = 1 \cdot b$ and $b = (-1)(-b)$, $b \in \mathbf{Z}$.)

(c) Every integer is divisible by itself. ($b = b \cdot 1$, $b \in \mathbf{Z}$.)

Theorem 1.1 *If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.*

In words: a number cannot divide a smaller nonzero number.

Proof. Because $b = a \cdot q$ for some $q \in \mathbf{Z}$, we have $|b| = |a| \cdot |q|$. If $|q| = 1$, then $|b| = |a|$. Otherwise, because $|q| > 1$, we have $|b| = |a| \cdot |q| > |a| \cdot 1 = |a|$, by Theorem 2.21 b) in [1]. □

It follows immediately that, if $a \mid b$ and $b \mid a$, then $|a| = |b|$.

Theorem 1.2 *Let $a, b, c, m, n \in \mathbf{Z}$. Then*

(a) *If $a \mid b$ and $b \mid c$, then $a \mid c$.*

(b) *If $a \mid b$, then $a \mid bc$.*

(c) *If $a \mid b$, then $ac \mid bc$.*

(d) *If $ac \mid bc$ and $c \neq 0$, then $a \mid b$.*

(e) *If $a \mid b$ and $a \mid c$, then $a \mid mb + nc$.*

Proof. (a) There are $p, q \in \mathbf{Z}$ such that $b = ap$ and $c = bq$. It follows that $c = bq = (ap)q = a(pq)$, so $a \mid c$.

(b) There is $q \in \mathbf{Z}$ such that $b = aq$. Hence, $bc = (aq)c = a(qc)$, so $a \mid bc$.

(c) There is $q \in \mathbf{Z}$ such that $b = aq$. Therefore, $bc = (aq)c = (ac)q$. Hence, $ac \mid bc$.

(d) There is $q \in \mathbf{Z}$ such that $bc = (ac)q$. Hence, $c(b - aq) = bc - (ac)q = 0$. Because $c \neq 0$, $b = aq$, by Theorem 2.32 in [1]. Therefore, $a \mid b$.

(e) There are $p, q \in \mathbf{Z}$ such that $b = ap$ and $c = aq$. We have

$$mb + nc = map + naq = a(mp + nq).$$

Hence, $a \mid mb + nc$. □

2 The Division Algorithm

We recall the definition of the *signum* function (cf. [1, p. 118]):

$$\operatorname{sgn} x = \begin{cases} 1, & \text{if } x > 0, \\ 0, & \text{if } x = 0, \\ -1, & \text{if } x < 0, \end{cases} \qquad x \in \mathbf{R}.$$

Clearly, for any real number x, $|x| = x \operatorname{sgn} x$.

Theorem 2.1 (The Division Algorithm). *Let a and b be integers with $b \neq 0$. Then there exist unique integers q and r such that*

$$a = bq + r, \qquad \text{and} \quad 0 \leq r < |b|.$$

The integers q and r in Theorem 2.1 are called the *quotient* and *remainder*, respectively, upon dividing a by b.

Proof. (Existence.) If $b \mid a$, then there is an integer q such that $a = bq + 0$, so $r = 0$.

Suppose that $b \nmid a$ and let

$$S = \{a - bn : n \in \mathbf{Z} \text{ and } a - bn > 0\}.$$

We show that S is a nonempty set.

There are three mutually exclusive cases:

1) $a = 0$. For $n = -b$ we have $a - bn = b^2 > 0$.

2) $a > 0$. For $n = -\operatorname{sgn} b$ we have $a - bn = a + |b| > 0$.

3) $a < 0$. For $n = 2a(\operatorname{sgn} b)$ we have

$$a - bn = a - b(2a(\operatorname{sgn} b)) = -a(2|b| - 1) > 0.$$

Hence, $S \neq \varnothing$. By the Well-Ordering Principle (cf. Theorem 1.25 in [1]), the set S contains a least element that we denote by r. Thus there is an integer q such that $a = bq + r$. Clearly, $r > 0$. Suppose that $r \geq |b|$. Note that $r \neq |b|$, because $b \nmid a$. We have

$$a - b(q + \operatorname{sgn} b) = a - bq - b \operatorname{sgn} b = r - |b| > 0,$$

so $r - |b| \in S$. This contradicts our assumption that r is the least element of S, because $r - |b| < r$. It follows that $r < |b|$.

(Uniqueness.) Suppose that

$$a = bq_1 + r_1 = bq_2 + r_2.$$

If $r_1 = r_2$, then $b(q_1 - q_2) = 0$, so $q_1 = q_2$ (cf. Theorem 2.16 in [1]). Otherwise,

$$|r_1 - r_2| = |b| \cdot |q_2 - q_1|,$$

so $|b|$ divides $|r_1 - r_2| \neq 0$. This contradicts Theorem 1.1, because $|r_1 - r_2| < |b|$ (cf. Exercise 25 on p. 82 in [1]). □

Example 2.1 a) By dividing 33 by 5, we obtain $33 = 5 \cdot 6 + 3$. The quotient is 6, the remainder is 3.

b) By dividing -33 by 5, we obtain $-33 = 5(-7) + 2$. The quotient is -7, the remainder is 2.

Example 2.2 (Even and odd integers.) For any integer a we have $a = 2b + r$, $r = 0$ or 1, for some integer b. If $r = 0$, then a is an *even* integer. Otherwise, it is an *odd* integer (cf. Exercise 11 on p. 30 in [1]).

The drawing in Figure 1 illustrates the Division Algorithm.

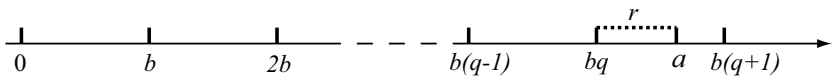

Figure 1: $a = bq + r$ on the number line for $0 < b < a$.

3 The Greatest Common Divisor

A *common divisor* of two integers is an integer that divides each of the integers. The set C of all common divisors of two nonzero integers is not empty, because $1 \in C$. By Theorem 1.1, this set is bounded and therefore finite. This argument justifies the following definition.

Definition 3.1 *The* greatest common divisor (GCD) *of two nonzero integers a and b is the largest of all common divisors of a and b. It is denoted by* $\gcd(a, b)$.

If $\gcd(a, b) = 1$*, then the integers a and b are said to be* coprime *(or* relatively prime*).*

If d is a divisor of an integer, so is $-d$. Therefore, $\gcd(a, b)$ is a positive integer.

Theorem 3.1 *If d is the greatest common divisors of a and b, then there exist integers m and n such that*

$$d = am + bn.$$

Proof. Let

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

Because $a \cdot a + b \cdot 0 = a^2 > 0$, the set S is a nonempty set of positive integers. By the Well-Ordering Principle (cf. Theorem 1.25 in [1]), the set S contains a least element $l = ax_0 + by_0 > 0$. Below, we show that $d = l$.

First, we show that $l \mid a$ and $l \mid b$. Suppose to the contrary that $l \nmid a$. By Theorem 2.1, there are integers q and r such that

$$a = lq + r, \qquad 0 < r < l.$$

Then

$$r = a - lq = a - (ax_0 + by_0)q = a(1 - x_0q) + b(-y_0q),$$

so $r \in S$. Because $r < l$, this contradicts the fact that l is the least element in the set S. Hence, $l \mid a$. A similar argument shows that $l \mid b$. It follows that l is a common divisor of a and b.

Now, because d is the GCD of a and b, we have $a = da_0$ and $b = db_0$ for some $a_0, b_0 \in \mathbf{Z}$. Therefore,

$$l = ax_0 + by_0 = d(a_0x_0 + b_0y_0),$$

so $d \mid l$. By Theorem 1.1, $d \leq l$. Because d is the GCD of a and b, $l \leq d$. Hence, $d = l$. □

In the case of coprime integers we have a stronger result

Theorem 3.2 *Two integers a and b are coprime if and only if there exist integers m and n such that*

$$am + bn = 1.$$

Proof. (Necessity.) Follows immediately from the previous theorem (Theorem 3.1).

(Sufficiency.) Suppose that there are $m, n \in \mathbf{Z}$ such that $am+bn = 1$. Then, by Theorem 1.2(e), any common divisor of a and b is a divisor of 1. Clearly, $\gcd(a, b) = 1$. □

The result of the next theorem is often used as a definition of the GCD of two integers.

Theorem 3.3 *A positive integer d is the GCD of nonzero integers a and b if and only if it is a positive common divisor of a and b which is divisible by every common divisor of these integers.*

Proof. (Necessity.) Let $d = \gcd(a, b)$ and c be a common divisor of a and b. By Theorem 3.1, there are $m, n \in \mathbf{Z}$ such that $d = am+bn$. By Theorem 1.2(e), c divides d.

(Sufficiency.) Let c and $d > 0$ be common divisors of a and b. If $c \mid d$, then, by Theorem 1.1, $c \leq d$. Hence, d is the GCD of a and b. □

We conclude this section by establishing three properties of coprime integers. Note that two integers are coprime if and only if they have no common divisors different from 1 and -1.

Theorem 3.4 *If an integer a is coprime with integers b and c, it is coprime with their product bc.*

Proof. By Theorem 3.2, there are integers a_1, b_1, a_2 and c_1 such that

$$aa_1 + bb_1 = 1 \quad \text{and} \quad aa_2 + cc_1 = 1.$$

By multiplying these identities, we obtain

$$\begin{aligned}(aa_1 + bb_1)(aa_2 + cc_1) &= aa_1aa_2 + aa_1cc_1 + bb_1aa_2 + bb_1cc_1 \\ &= a(a_1aa_2 + a_1cc_1 + bb_1a_2) + (bc)(b_1c_1) = 1.\end{aligned}$$

By the same theorem, a is coprime with bc. □

Theorem 3.5 *If integers a and b are coprime and $a \mid bc$, then $a \mid c$.*

Proof. Because $a \mid bc$, there is an integer d such that $bc = ad$. By Theorem 3.2, there are integers a_1 and b_1 such that $aa_1 + bb_1 = 1$. Hence,

$$c = c(aa_1 + bb_1) = aca_1 + bcb_1 = aca_1 + adb_1 = a(ca_1 + db_1).$$

It follows that $a \mid c$. □

Theorem 3.6 *If integers a and b are coprime, $a \mid c$, and $b \mid c$, then $ab \mid c$.*

Proof. Because $b \mid c$, there is an integer d such that $c = bd$. Hence, $a \mid bd$ and $\gcd(a, b) = 1$. By Theorem 3.5, $a \mid d$, so there is an integer r such that $d = ar$. Hence, $c = bd = (ab)r$, so $ab \mid c$. □

4 The Euclidean Algorithm

The result of Theorem 2.1 is not a practical method for calculating the GCD of two integers a and b. Below we describe a recursive procedure for finding $\gcd(a, b)$, which is known as the *Euclidean Algorithm*. Arguably, it first appeared as Proposition 2 in Book VII of Euclid's **Elements** [2].

It is not difficult to see that

$$\gcd(a, -b) = \gcd(-a, b) = \gcd(a, b)$$

for nonzero integers a and b. Hence to compute $\gcd(a, b)$ it suffices to consider only positive integers a and b. Moreover, by symmetry, we may assume that $0 < b \leq a$. Clearly, $\gcd(a, a) = a$, so below we assume that $0 < b < a$.

The key element of the Euclidean Algorithm is the Division Algorithm (cf. Theorem 2.1) augmented with the result of the following theorem.

Theorem 4.1 *If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.*

Proof. Let d be a common divisor of a and b, that is, $d \mid a$ and $d \mid b$. By Theorem 1.2(e), d is a divisor of $r = a - bq$ and therefore a common divisor of b and r.

On the other hand, if d is a common divisor of b and r, it is also a common divisor of a and b, by the same theorem.

It follows that the sets of common divisors of a and b and common divisors of b and r are identical. Therefore, $\gcd(a, b) = \gcd(b, r)$. □

Example 4.1 (a) Two consecutive integers, n and $n+1$, are coprime, because $n+1 = n \cdot 1 + 1$, so

$$\gcd(n+1, n) = \gcd(n, 1) = 1.$$

(b) Similarly, two consecutive odd integers, $2n+1$ and $2n+3$, are coprime, because

$$\gcd(2n+3, 2n+1) = \gcd(2n+1, 2) = 1.$$

In the next paragraph, we present the Euclidean Algorithm.

For integers $a > b > 0$, we make a repeated application of the Division Algorithm to obtain a chain of equations

$$\begin{aligned}
a &= bq_1 + r_1, & 0 < r_1 < b,\\
b &= r_1q_2 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2,\\
&\cdots\\
r_{n-2} &= r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1},\\
r_{n-1} &= r_nq_{n+1} + 0.
\end{aligned}$$

Thus this chain of equations is derived by dividing a by b, b by r_1, r_1 by r_2, ... , r_{n-1} by r_n. Because $r_1 > r_2 > r_3 > \cdots > 0$, the process stops, by the Well-Ordering Principle, when the division is exact. Clearly, $\gcd(r_{n-1}, r_n) = r_n$. Hence, by Theorem 4.1,

$$\begin{aligned}
r_n = \gcd(r_{n-1}, r_n) &= \gcd(r_{n-2}, r_{n-1}) = \cdots\\
&= \gcd(r_2, r_1) = \gcd(r_1, b) = \gcd(a, b).
\end{aligned}$$

Clearly, $\gcd(a, b) = b$, so we assume in the above chain of equations that $r_1 > 0$.

Example 4.2 Find the GCD of 48 and 18. We have

$$\begin{aligned}
48 &= 18 \cdot 2 + 12,\\
18 &= 12 \cdot 1 + 6,\\
12 &= 6 \cdot 2 + 0.
\end{aligned}$$

Hence, $\gcd(48, 18) = 6$.

The above equations can be used to represent $6 = \gcd(48, 18)$ as a linear combination of 48 and 18 (cf. Theorem 3.1):

$$\begin{aligned}
12 &= 48 + 18 \cdot (-2),\\
6 &= 18 + 12 \cdot (-1)\\
&= 18 + (48 + 18 \cdot (-2))(-1)\\
&= 48 \cdot (-1) + 18 \cdot 3.
\end{aligned}$$

5 The Least Common Multiple

Definition 5.1 *The* least common multiple (LCM) *of two nonzero integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by* $\operatorname{lcm}(a, b)$.

Because $|a||b| = (\operatorname{sgn} a \cdot \operatorname{sgn} b)ab > 0$, the set of positive common multiples of a and b is not empty and therefore, by the Well-Ordering Principle, has the least element. Hence, $\operatorname{lcm}(a, b)$ exists and unique.

As we noted in the previous section,

$$\gcd(a, -b) = \gcd(-a, b) = \gcd(a, b).$$

Clearly, also

$$\operatorname{lcm}(a, -b) = \operatorname{lcm}(-a, b) = \operatorname{lcm}(a, b).$$

For this reason, we assume in this section that the integers a and b in $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ are positive numbers.

Theorem 5.1 *The LCM of two integers a and b divides every common multiple of these integers.*

Proof. Let $k = \operatorname{lcm}(a, b)$ and k_1 be a common multiple of a and b. Suppose to the contrary that $k_1 = kq + r$, $0 < r < k$ for some integer q (cf. Theorem 2.1). Then $r = k_1 - kq$ is divisible by a and b (cf. Theorem 1.2(e)), a contradiction, because $r < k = \operatorname{lcm}(a, b)$. □

Theorem 5.2 *For any two nonzero integers a and b,*

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab.$$

Proof. Let $k = \operatorname{lcm}(a, b)$. By Theorem 5.1, $ab = dk$ for some integer d. We need to show that $d = \gcd(a, b)$.

Let $k = aa_1$ and $k = bb_1$. Because $ab = dk$, we have $ab = daa_1$, so $b = da_1$. Similarly, $a = db_1$. Hence, d is a common divisor of a and b.

Let d_1 be a common divisor of a and b. Then $ab = k_1 d_1$ for some integer k_1 and $a = d_1 a_2$, $b = d_1 b_2$ for some integers a_2, b_2. Therefore,

$$d_1 a_2 d_1 b_2 = k_1 d_1,$$

so

$$k_1 = d_1 a_2 b_2 = ab_2 = ba_2.$$

Hence, k_1 is a common multiple of a and b. By Theorem 5.1, there is an integer q such that $k_1 = kq$. Because $ab = dk = k_1 d_1$ and $k_1 = kq$, d_1 divides d. By Theorem 3.3, $d = \gcd(a, b)$. □

It is easy to see that $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = |a||b|$, if nonzero integers a and b are not necessarily both positive.

6 Prime Factorization

Recall that a *prime* is a natural number greater than 1 whose only positive divisors are 1 and the number itself. The numbers greater than 1 that are not prime are called *composite* numbers.

It follows immediately from the definition that, if a prime p does not divide a nonzero integer a, then $\gcd(p, a) = 1$, that is, p and a are coprime.

The statement of the following theorem is known as **Euclid's Lemma** (Proposition 30, Book VII in [2]).

Theorem 6.1 *Let p be a prime and a and b integers. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. If $p \mid a$, we are done. Suppose that $p \nmid a$, so p and a are coprime. By Theorem 3.5 , $p \mid b$. □

The next theorem is a generalization of Euclid's Lemma.

Theorem 6.2 *Suppose that $a_1, a_2, \ldots, a_n$ are integers and p is a prime. If $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_k$ for some $k = 1, 2, \ldots, n$.*

Proof. The proof is by mathematical induction. The base step, $n = 2$, is Euclid's Lemma (Theorem 6.1).

Suppose that the statement holds for some $n \geq 2$ and $p \mid a_1 a_2 \cdots a_n a_{n+1}$. If $p \mid a_1$, we are done. Otherwise, again by Theorem 6.1, $p \mid a_2 a_3 \cdots a_n a_{n+1}$. By the induction hypothesis, there is k, $2 \leq k \leq n + 1$, such that $p \mid a_k$. □

Euclid's Lemma plays a pivotal role in the proof of the *Fundamental Theorem of Arithmetic*. The theorem states that every integer greater than 1 is either prime or can be represented uniquely as a product of primes. Originally, the existence of prime factorization was established in Euclid's *Elements* (Propositions 30–32, Book VII in [2]). A rigorous proof of the uniqueness part of the theorem was given by Gauss in his *Disquisitiones Arithmeticae* published in 1801.

Theorem 6.3 (Fundamental Theorem of Arithmetic). *Every integer greater than 1 is a prime or a product of primes. This product is unique, up to the order of factors.*

Proof. (Existence.) Below we reproduce the proof given in [1, Example 1.48] that uses the Strong Principle of Induction (Theorem 1.47 in [1]).

The property $P(n)$ states "$n > 1$ is either prime or a product of primes". Suppose $P(k)$ is true for all $2 \leq k < m$. There are two mutually exclusive cases:

Case 1. m is a prime number. Then $P(m)$ is true and we are done.

Case 2. m is a composite number. Then it is a product of two natural numbers each of which is different from 1. By the induction hypothesis each of these two numbers is a product of primes. It follows that m itself is a product of primes, that is, $P(m)$ holds.

(Uniqueness.) Suppose that there is an integer $n > 1$ that admits two distinct prime factorizations:

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

where

$$p_1 \le p_2 \le \cdots \le p_r \qquad \text{and} \qquad q_1 \le q_2 \le \cdots \le q_s.$$

By the Well-Ordering Principle (cf. Theorem 1.25 in [1]), we may assume that n is the smallest integer greater than 1 satisfying this property.

By Theorem 6.2, there is $1 \le k \le s$ such that $p_1 \mid q_k$, because $p_1 \mid n$. Since q_k is prime, $p_1 = q_k$. Similarly, there is $1 \le l \le r$ such that $q_1 = p_l$. Then, $p_1 = q_k \ge q_1 = p_l \ge p_1$. It follows that $p_1 = q_1$. By the Cancellation Law of Multiplication (cf. Theorem 2.32 in [1]), we have two distinct prime factorization of the integer

$$m = p_2 \cdots p_r = q_2 \cdots q_s.$$

We obtained a contradiction, because $m < n$. □

In contemporary terminology, Theorem 6.3 claims that the ring $\mathbf{Z}$ is a *unique factorization domain*. The following examples demonstrate that there are rings that are not unique factorization domains.

Example 6.1 Let $R = 2\,\mathbf{Z}$ be the ring from Example 2.27c) in [1]. The numbers 2, 6, 10, 14, ... are *primes* in R, because they are not products of positive elements of R. We have two distinct factorization of $60 \in R$ into primes:

$$60 = 6 \cdot 10 = 2 \cdot 30.$$

The ring $2\,\mathbf{Z}$ from the above example is not an integral domain. The ring in the next example is an integral domain which is not a unique factorization domain.

Example 6.2 Let R be the set of complex numbers defined by

$$R = \{z \in \mathbf{C} : z = x + \sqrt{5}y\boldsymbol{i},\ x, y \in \mathbf{Z}\}.$$

It is easy to verify that R is closed under addition and multiplication of complex numbers with the zero and identity elements 0 and 1, respectively. Because $\mathbf{C}$ is a field, it follows that R is an integral domain (cf. Definition 2.31 in [1]). It is denoted by $\mathbf{Z}[\sqrt{-5}]$.

We say that $z \in R$ is *factored* if there are $z_1, z_2 \in R$ such that

$$z = z_1 \cdot z_2, \qquad \text{where } |z_1| > 1 \text{ and } |z_2| > 1.$$

Note that the only complex numbers $z \in R$ with $|z| \le 1$ are integers 0, 1, -1. Hence our definition of factoring excludes trivial factorings $z = 1 \cdot z = (-1) \cdot (-z)$.

A number $z \in R$ with $|z| > 1$ that cannot be factored is called a *prime* in R. We show that numbers 2 and 3 are primes in R. Indeed, suppose, for instance,

that $2 = z_1 \cdot z_2$ where $z_1 = x_1 + \sqrt{5}y_1\boldsymbol{i}$, $z_2 = x_2 + \sqrt{5}y_2\boldsymbol{i}$. Clearly, $y_1, y_2 \neq 0$. We have

$$2 = |2| = |z_1| \cdot |z_2| = \sqrt{x_1^2 + 5y_1^2} \cdot \sqrt{x_2^2 + 5y_2^2} \geq 5,$$

a contradiction. The same argument shows that 3 is prime in R.

Finally,

$$6 = 2 \cdot 3 = (1 + \sqrt{5}\boldsymbol{i})(1 - \sqrt{5}\boldsymbol{i})$$

proves that there is no unique prime factorization of $6 \in R$. (Note that this conclusion does not require showing that $1 + \sqrt{5}\boldsymbol{i}$ and $1 - \sqrt{5}\boldsymbol{i}$ are primes in R, although they are.)

How many primes are there? To answer this question, we prove the following theorem (cf. Book IX, Proposition 20 in Euclid's *Elements* [2]).

Theorem 6.4 *Let $S = \{p_1, \ldots, p_n\}$ be a finite set of primes. There exists a prime that does not belong to S.*

Proof. Let $q = p_1 p_2 \cdots p_n + 1$. If q is a prime, then $q \notin S$, because $q > p_k$ for all $1 \leq k \leq n$. Otherwise, let p be a prime factor of q. If $p = p_k$ for some $1 \leq k \leq n$, then $p \mid q$ and $p \mid (q-1)$. By Theorem 1.2(e), p divides $q-(q-1) = 1$, a contradiction. Hence, $p \notin S$. □

The result of the above theorem, clearly, implies that there are infinitely many primes. However, as the next example demonstrates, primes are rather "rare" elements of the set of integers **N**. Namely, it shows that for any positive integer n there exist n consecutive composite integers.

Example 6.3 For $n > 0$, consider n consecutive integers

$$(n+1)! + 2, \;\; (n+1)! + 3, \;\ldots\; (n+1)! + k, \;\ldots\; (n+1)! + n + 1.$$

Each integer in this sequence is composite, because k divides $(n+1)! + k$ for $2 \leq k \leq n+1$.

7 Congruences

Definition 7.1 *Let m be a nonzero integer. Two integers a and b are said to be* congruent modulo m *if m divides $a - b$. In this case, we write*

$$a \equiv b \pmod{m}.$$

The integer m is called a modulus.

Because $a - b$ is divisible by m if and only if it is divisible by $-m$, we may assume that the modulus is a positive integer. Clearly, any two integers are congruent modulo 1. In the rest of this section, the modulus m is an integer greater than 1.

When $a = qm + r$, where q is the quotient and r is the remainder upon dividing a by m (cf. Theorem 2.1), we write

$$a \bmod m = r \quad \text{or} \quad a = r \bmod m,$$

and say that r *is a modulo* m. (Note that, in this case, $a \equiv r \pmod{m}$.)

It follows immediately from the definition that $a \equiv b \pmod{m}$ if and only if $a = b + mq$ for some integer q. Below, we use this fact without referring to it explicitly.

The two properties of the congruence relation in the following theorem are basic in *modular arithmetic*.

Theorem 7.1 *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then*

$$a + c \equiv b + d \pmod{m} \qquad \textit{and} \qquad ac \equiv bd \pmod{m}.$$

Proof. We have $a = b + mq$ and $c = d + mq'$ for some $q, q' \in \mathbf{Z}$. Then

$$(a + c) - (b + d) = (b + mq + d + mq') - (b + d) = m(q + q'),$$

so $m \mid [(a + c) - (b + d)]$. Hence, $a + c \equiv b + d \pmod{m}$.

Furthermore,

$$\begin{aligned} ac - bd &= (b + mq)(d + mq') - bd = \\ &= bd + bmq' + mqd + mqmq' - bd = m(bq' + qd + qmq'), \end{aligned}$$

so $m \mid (ac - bd)$. Therefore, $ac \equiv bd \pmod{m}$. □

By the Cancellation Law of Multiplication for integers (cf. Exercise 8, Chapter 2, in [1]), if $ac = bc$ and $c \neq 0$, then $a = b$. More care must be used in dividing a congruence through by c, as the following example suggests.

Example 7.1 We have $2 \cdot 3 \equiv 4 \cdot 3 \pmod{6}$. However, $2 \not\equiv 4 \pmod{6}$.

Theorem 7.2 (Cancellation Law of Congruence.) *If* $ac \equiv bc \pmod{m}$ *and* $\gcd(c, m) = 1$, *then* $a \equiv b \pmod{m}$.

Proof. By Theorem 3.5, $m \mid c(a - b)$ and $\gcd(c, m) = 1$ imply $m \mid a - b$. Hence, $a \equiv b \pmod{m}$. □

The next theorem generalizes properties established in Theorem 7.1.

Theorem 7.3 *Let*

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0, \quad x, c_n, \ldots, c_1, c_0 \in \mathbf{Z}$$

be a polynomial of degree n *considered as a function* $f : \mathbf{Z} \to \mathbf{Z}$.

If $a \equiv b \pmod{m}$, *then* $f(a) \equiv f(b) \pmod{m}$.

The following proof can be easily made rigorous by using mathematical induction.

Proof. We apply Theorem 7.1 repeatedly to obtain $a^2 \equiv b^2 \pmod m$, $a^3 \equiv b^3 \pmod m$, $\ldots$, $a^n \equiv b^n \pmod m$, then $c_k a^k \equiv c_k b^k \pmod m$ for $k = 0, 1 \ldots, n$, and, finally,

$$c_n a^n + \cdots + c_1 a + c_0 \equiv c_n b^n + \cdots + c_1 b + c_0 \pmod m,$$

so $f(a) \equiv f(b) \pmod m$. □

Example 7.2 (Tests for Divisibility.) Clearly, $10 \equiv 1 \pmod 3$. Suppose that we have a natural number N whose decimal expansion is $c_n c_{n-1} \ldots c_1 c_0$. This means that

$$N = c_n 10^n + c_{n-1} 10^{n-1} + \cdots + c_1 10 + c_0.$$

By Theorem 7.3,

$$N \equiv c_n + c_{n-1} + \cdot + c_1 + c_0 \pmod 3.$$

We obtained a well-known test for divisibility by 3: add up the digits of the number in base 10, and check if the result is divisible by 3. (Repeat, if necessary.)

Because $10 \equiv 1 \pmod 9$, the same test works for divisibility by 9.

The following theorem is known as *Fermat's Little Theorem*. It is one of the fundamental results in elementary number theory.

Theorem 7.4 *If p is a prime, then $a^p \equiv a \pmod p$ for every integer a.*

Proof. We assume that $a > 0$ and prove the claim by mathematical induction on a. The base step, $a = 1$, trivially holds. Suppose that $a^p \equiv a \pmod p$ for some $a \geq 1$. By the binomial theorem,

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{k} a^{p-k} + \cdots + \binom{p}{p-1} a + 1,$$

where

$$\binom{p}{k} = \frac{p \cdot (p-1) \cdots (p-k+1)}{1 \cdot 2 \cdots k}, \qquad 0 < k < p.$$

Clearly, p divides $\binom{p}{k}$ for every k, $0 < k < p$. By Theorem 7.1, all middle terms in the above binomial expansion are congruent to zero. Therefore, by the induction hypothesis,

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod p.$$

Hence the result.

Clearly, $0 \equiv 0 \pmod p$. For a negative integer a the result follows from the identities $(-a)^p = -a^p$ for $p > 2$, and $(-a)^2 = a^2$. □

Fermat's Little Theorem is often stated in the following equivalent form.

Theorem 7.5 *If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. By Theorem 7.2, $a^p \equiv a \pmod{p}$ implies $a^{p-1} \equiv 1 \pmod{p}$, provided that $p \nmid a$. □

By definition, $\equiv$ is a binary relation on the set of integers $\mathbf{Z}$. Note that this relation depends on the choice of modulus m.

Theorem 7.6 *The relation $\equiv$ is an equivalence relation on $\mathbf{Z}$.*

Proof. We need to establish three properties defining an equivalence relation (cf. Section **A.3** on page 132 in [1]).

Reflexivity. Clearly, $a \equiv a \pmod{m}$ for all $a \in \mathbf{Z}$.

Symmetry. If $a = b + mq$, then $b = a + m(-q)$. Hence, $a \equiv b \pmod{m}$ implies $b \equiv a \pmod{a}$.

Transitivity. Suppose that $a = b + mq$ and $b = c + mq'$. Then,

$$a = c + m(q + q').$$

Therefore, $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ imply $a \equiv c \pmod{m}$. □

For $a \in \mathbf{Z}$, the equivalence class $[a]$ of the relation $\equiv$ (cf. Section **A.3** on page 132 in [1], especially, Theorem **A.8** there) is called the *residue class of a modulo m*. Clearly,

$$[a] = \{a + mq : q \in \mathbf{Z}\} = \{\ldots a - 2m, a - m, a, a + m, a + 2m, \ldots\}.$$

By Theorem 2.1, for every a there exist unique integers q and r such that $a = mq + r$ and $0 \le r < m$. Because $a \equiv r \pmod{m}$, we have $[a] = [r]$. It follows that there are exactly m distinct residue classes modulo m:

$$[0], [1], [2], \ldots, [m - 1].$$

Definition 7.2 *The set*

$$\mathbf{Z}_m = \{[a] : a \in \mathbf{Z}\} = \{[0], [1], [2], \ldots, [m - 1]\}$$

is called the ring of integers modulo m *or, simply,* integers modulo m.

Operations of addition, $+$, and multiplication, $\cdot$ are defined on $\mathbf{Z}_m$ by

$$[a] + [b] = [a + b] \qquad \text{and} \qquad [a] \cdot [b] = [a \cdot b],$$

respectively. By Theorem 7.1, these definitions are unambiguous.

Theorem 7.7 *The set $\mathbf{Z}_m$ endowed with operations $+$ and $\cdot$ is a ring.*

Proof. We need to verify conditions **R1**–**R5** of Definition 2.24 on page 49 in [1]. Below, a, b, and c are integers.

R1. Because $a + b = b + a$, we have

$$[a] + [b] = [a + b] = [b + a] = [b] + [a].$$

R2. Because $a + (b + c) = (a + b) + c$, we have

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

R3. Let $x = [b - a]$. Then

$$[a] + x = [a] + [b - a] = [a + (b - a)] = [b].$$

R4. We have

$$[a] \cdot ([b] \cdot [c]) = [a] \cdot [b \cdot c] = [a \cdot (b \cdot c)] = [(a \cdot b) \cdot c] = [a \cdot b] \cdot [c] = ([a] \cdot [b]) \cdot [c].$$

R5. We have

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

Similarly, $([b] + [c]) \cdot [a] = [b] \cdot [a] + [c] \cdot [a]$. □

Clearly, [0] is the zero element of the ring $\mathbf{Z}_m$, and [1] is its unity.

Theorem 7.8 *The ring $\mathbf{Z}_m$ is a field if and only if m is prime.*

Proof. (Necessity.) Suppose to the contrary that m is not prime, so there is a nontrivial factorization $m = a \cdot b$. Then $[a] \cdot [b] = [0]$, so $\mathbf{Z}_m$ is not an integral domain, a contradiction (cf. the note on the bottom of page 70 in [1]).

(Sufficiency.) Let $m = p$ be a prime. For $[a] \neq [0]$ in $\mathbf{Z}_p$, we have $p \nmid a$. By Fermat's Little Theorem (Theorem 7.5), $a \cdot a^{p-2} \equiv 1$. Hence, $[a^{p-2}]$ is the multiplicative inverse of $[a]$, so $\mathbf{Z}_p$ is a field. □

Addition and multiplication tables for rings $\mathbf{Z}_2$, $\mathbf{Z}_3$, and $\mathbf{Z}_4$ are found in Examples 2.27 b), 3.22, and Exercise 24 (Chapter 2), respectively, in [1].

The ring $\mathbf{Z}_m$ is often defined as an algebraic structure $\langle \mathbb{Z}_m, +, \cdot \rangle$, where

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m - 1, m\}$$

and operations of addition, $+$, and multiplication, $\cdot$, are defined by

$$a + b = (a + b) \bmod m \qquad \text{and} \qquad a \cdot b = (a \cdot b) \bmod m,$$

respectively. It can be shown that the algebraic structure $\langle \mathbb{Z}_m, +, \cdot \rangle$ is a ring isomorphic to the ring $\mathbf{Z}_m$.

References

[1] Ovchinnikov, S. *Number Systems. An Introduction to Algebra and Analysis*, American Mathematical Society, Providence, Rhode Island, 2015.

[2] Fitzpatrick, R. *Euclid's Elements of Geometry*, a modern English translation, `http://farside.ph.utexas.edu/Books/Euclid/Elements.pdf`, 2008.