

§5 Divisibility

In this paragraph, we remind the reader of certain properties of integers concerning divisibility. First we recall the definition.

5.1 Definition: Let $a, b \in \mathbb{Z}$. If $a \neq 0$ and if there is a c such that $ac = b$, then a is called a *divisor* or a *factor* of b , and b is said to be divisible by a . We also say a divides b .

We write $a|b$ to express that a divides b . Whenever we employ the notation $a|b$, it will be assumed of course $a \neq 0$. We shall write $a \nmid b$ when $a \neq 0$ and b is not divisible by a . Thus we have $3|6$, $3|9$, $2|8$, $5 \nmid 9$, $5|10$, $3 \nmid 7$, $4|8$, $-3|6$, $2|-4$, $-2|-4$. The notations $0|b$ and $0 \nmid b$ are meaningless: not true or false, simply undefined.

Some basic properties of divisibility are collected below.

5.2 Lemma: Let $a, b, c, m, n, m_1, m_2, \dots, m_s, b_1, b_2, \dots, b_s$, be integers.

- (1) If $a|b$, then $a|-b$, $-a|-b$, $-a|b$.
- (2) If $a|b$ and $b|c$, then $a|c$.
- (3) If $a|b$ and $c \neq 0$, then $ac|bc$.
- (4) If $ac|bc$, then $a|b$.
- (5) If $a|b$ and $a|c$, then $a|b + c$.
- (6) If $a|b$ and $a|c$, then $a|b - c$.
- (7) If $a|b$ and $a|c$, then $a|mb + nc$.
- (8) If $a|b_1, a|b_2, \dots, a|b_s$, then $a|m_1b_1 + m_2b_2 + \dots + m_sb_s$.
- (9) If $a \neq 0$, then $a|0$.
- (10) $1|a$ and $-1|a$.
- (11) If $a|b$ and $b \neq 0$, then $|a| \leq |b|$.
- (12) If $a|b$ and $b|a$, then $|a| = |b|$.

Proof:(1) If $a|b$, then $a \neq 0$ and $ak = b$ for some $k \in \mathbb{Z}$. So $a \neq 0$ and $a(-k) = -b$; $a \neq 0$ and $(-a)k = -b$; $a \neq 0$ and $(-a)(-k) = b$; with $k, -k \in \mathbb{Z}$. Hence $a|-b$, $-a|-b$, $-a|b$.

(2) If $a|b$ and $b|c$, then $a \neq 0 \neq b$ and $ak = b$ and $bh = c$ for some $k, h \in \mathbb{Z}$. So $a(kh) = bh = c$ and, since $kh \in \mathbb{Z}$, we obtain $a|c$.

(3) If $a|b$, then $a \neq 0$ and $ak = b$ for some $k \in \mathbb{Z}$. So $(ac)k = bc$. From $a \neq 0$, $c \neq 0$, we conclude $ac \neq 0$. Hence $ac|bc$.

(4) If $ac|bc$, then $ac \neq 0$ and $(ac)k = bc$ for some $k \in \mathbb{Z}$. From $ac \neq 0$, we obtain $a \neq 0$ and $c \neq 0$. Since $c \neq 0$, we have $ak = b$. Since $a \neq 0$, we can write $a|b$.

(5) If $a|b$ and $a|c$, then $a \neq 0$, and $ak = b$, $ah = c$ for some $k, h \in \mathbb{Z}$. So $a(k+h) = b + c$. Since $k+h \in \mathbb{Z}$ and $a \neq 0$, we have $a|b+c$.

(6) This can be proved in the same way as (5). We might also observe that $a|-c$ if $a|c$ by (1), hence $a|b+(-c)$ by (5), so $a|b-c$.

(7) If $a|b$ and $a|c$, then $a \neq 0$, and $ak = b$, $ah = c$ for some $k, h \in \mathbb{Z}$. So $a(km+hn) = ak.m + ah.n = bm + cn = mb + nc$. Since $km + hn \in \mathbb{Z}$ and $a \neq 0$, we have $a|mb+nc$.

(8) This can be proved by a simple application of the principle of mathematical induction.

(9) $a0 = 0$ for any $a \in \mathbb{Z}$. If $a \neq 0$, we can write $a|0$.

(10) $a = 1.a = (-1)(-a)$. Hence $1|a$ and $-1|a$.

(11) If $a|b$, then $a \neq 0$ and $ak = b$ for some $k \in \mathbb{Z}$. So $|a||k| = |b|$. Since $b \neq 0$, we have $|k| \geq 1$. Thus $|b| = |a||k| \geq |a|$.

(12) If $a|b$ and $b|a$, then $a \neq 0$ and $b \neq 0$, so we may apply (11) to get $|a| \leq |b|$ and $|b| \leq |a|$. Thus $|a| = |b|$. \square

5.3 Theorem (Division algorithm): Let $a, b \in \mathbb{Z}$, $b > 0$. Then there are unique integers $q, r \in \mathbb{Z}$ such that

$$a = qb + r, \quad 0 \leq r < b.$$

(The integer q is called the *quotient*, and r is called the *remainder* obtained when a is divided by b .)

Proof: There are two claims in this theorem: (1) that there are integers q,r , with the stated properties and (2) that these are unique, that is, the pair of integers q,r is the only one which has the stated properties. The proof of this theorem will accordingly consist of two parts. In the first part, we prove the existence of q,r , in the second part, their uniqueness.

Existence. Consider the set $T = \{a - ub : u \in \mathbb{Z}\} \subseteq \mathbb{Z}$. This set T contains nonnegative integers (for example, $a - (-|a|)b$ is nonnegative). We choose the smallest nonnegative integer in T . Let it be called r . Thus $r \geq 0$ and, by the very definition of T , we infer $r = a - qb$ for some $q \in \mathbb{Z}$. We claim $r < b$. If we had $r \geq b$, then, since $b > 0$, we would get

$$r > r - b = a - (q + 1)b > 0$$

and $r - b$ would be a nonnegative integer in T , smaller than the smallest nonnegative integer in T , which is absurd. So $r \geq b$ is impossible and $r < b$. Hence there are integers q,r such that

$$a = qb + r, \quad 0 \leq r < b.$$

Uniqueness. Let $a = qb + r$, $0 \leq r < b$, and $a = q_1b + r_1$, $0 \leq r_1 < b$, where q,r,q_1,r_1 are integers. We wish to prove $q_1 = q$ and $r_1 = r$. It suffices to prove $q_1 = q$, for then we would get $r_1 = a - q_1b = a - qb = r$ also. Suppose, by way of contradiction, that $q \neq q_1$. Then there are two possibilities: $q > q_1$ or $q < q_1$. Interchanging q,r with q_1,r_1 if necessary, we may assume $q > q_1$ without loss of generality (make sure that you understand this reasoning). From $q > q_1$, we get $q - q_1 \geq 1$, hence

$$r_1 = r_1 - 0 \geq r_1 - r = (a - q_1b) - (a - qb) = (q - q_1)b \geq 1 \cdot b = b,$$

a contradiction. So $q_1 = q$ and $r_1 = r$. □

This theorem formalizes what everybody learns at primary school: When we divide a by b , we get a quotient, and a remainder smaller than b . At primary school, one learns it in the case a is positive, but here a can be negative. Also, division is carried out by successive subtractions

$$\begin{array}{r} a \quad | \quad \underline{b} \\ \dots \quad \quad q \\ \dots \\ r \end{array}$$

We subtract b from a until we get a number r smaller than b . This is exactly what happens when we perform division, and this is essentially the proof of Theorem 5.3.

Given any two integers a, b , an integer d is said to be a *common divisor of a and b* if $d|a$ and $d|b$. Using the division algorithm, we can show that any two integers have a greatest common divisor, provided only that not both of them are equal to zero.

5.4 Theorem: *Let $a, b \in \mathbb{Z}$, not both zero. Then there is a unique integer d such that*

- (i) $d|a$ and $d|b$,
- (ii) for all $d_1 \in \mathbb{Z}$, if $d_1|a$ and $d_1|b$, then $d_1|d$,
- (iii) $d > 0$.

Proof: The proof will be similar to the proof of Theorem 5.3. We consider the set $U = \{ax - by \in \mathbb{Z} : x, y \in \mathbb{Z}\}$. Now U contains positive integers. (For example, $a(\mp 1) - b0$ is positive when $a \neq 0$ and the sign is chosen suitably. When $a = 0$, $a1 - b(\mp 1) = \mp b$ is positive, provided we choose the sign appropriately, since $b \neq 0$ when $a = 0$ by hypothesis.) We choose the smallest positive integer in U . Let it be called d . So $d > 0$ and d satisfies (iii). Moreover, if $d_1|a$ and $d_1|b$, then $d_1|ax - by$ for any $x, y \in \mathbb{Z}$ by Lemma 5.2(7), so d_1 divides every element of U . In particular, $d_1|d$. Thus (ii) is satisfied. It remains to prove (i).

By the very definition of U , we have $d = ax_0 - by_0$ for some $x_0, y_0 \in \mathbb{Z}$. We want to prove $d|a$ and $d|b$. Using the division algorithm, we write $a = qd + r$, where $0 \leq r < d$. Then

$$\begin{aligned} a &= q(ax_0 - by_0) + r, \\ r &= a - (ax_0 - by_0) \\ &= a(1 - qx_0) - b(-y_0), \text{ with } 1 - qx_0, -y_0 \in \mathbb{Z}, \end{aligned}$$

so r is an element of U and $0 \leq r < d$. Since d is the smallest positive integer in U and $r < d$, we have necessarily $r = 0$. This gives $a = qd$, so $d|a$. The proof of $d|b$ is similar and will be omitted.

Now the uniqueness of d . Suppose d' satisfies the conditions (i), (ii), (iii), too. Then $d'|a$, $d'|b$ by (i), and so $d'|d$ by (ii). Also, $d|a$, $d|b$ by (i), and so

$d|d'$ by (ii). By Lemma 5.2(12), we obtain $|d| = |d'|$. From (iii), we get $d > 0$, $d' > 0$, which yields $d = d'$. Thus d is unique. \square

5.5 Definition: Let $a, b \in \mathbb{Z}$, not both zero. The unique integer d in Theorem 5.4 is called the *greatest common divisor of a and b* .

The greatest common divisor of a and b will be denoted by (a, b) . This notation is standard. The reader should not confuse it with an ordered pair. The greatest common divisor of a and b is a natural number, not an ordered pair.

Definition 5.5 and the proof of Theorem 5.4 enables us to write the

5.6 Theorem: Let $a, b \in \mathbb{Z}$, not both zero. Then (a, b) is the smallest positive integer in the set $\{ax - by \in \mathbb{Z} : x, y \in \mathbb{Z}\}$. \square

Theorem 5.4 is a typical existence theorem. It tells us that the greatest common divisor (a, b) of any pair of integers a, b exists (provided a and b are not both zero), but gives no method for finding it. If a and b are small in absolute value, we might try to find the smallest positive integer in the set $\{ax - by \in \mathbb{Z} : x, y \in \mathbb{Z}\}$. This is not very satisfactory, of course. Also, it is almost impossible if a and b are rather large. We propose to give a systematic method for finding (a, b) for any pair of integers a, b , not both zero. This method will prove anew the existence of (a, b) and in addition will give us a systematic method of finding integers x, y such that $(a, b) = ax - by$. It is Proposition 2 in Euclid's *Elements*, Book VII. (in algebraic notation) and is known as the Euclidean algorithm.

We first observe that the set U in Theorem 5.6 does not change if we write $-a$ in place of a or $-b$ in place of b . This yields

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

for all a, b , not both zero. Hence $(a, b) = (|a|, |b|)$ and, when we want to find (a, b) , we may assume $a \geq 0$, $b \geq 0$ (the case $a = 0$, $b = 0$ is excluded) without loss of generality. Moreover, the set U in Theorem 5.6 remains unaltered if we interchange a and b . Thus

$$(a, b) = (b, a).$$

Therefore, when we want to find (a,b) , we may assume $a \geq b$ without loss of generality. (Instead of appealing to Theorem 5.6, we could use the definition to obtain $(a,b) = (-a,b) = (-a,-b) = (a,-b) = (b,a)$.)

The greatest common divisor of $a \in \mathbb{Z}$ ($a \neq 0$) and 0 is easily found. We have $(a,0) = |a|$, as follows from Theorem 5.6 or immediately from Theorem 5.4.

Suppose now $a \geq b > 0$ and we want to find (a,b) . We divide a by b and get

$$a = q_1 b + r_1, \quad 0 \leq r_1 < b.$$

Here r_1 may be zero. If $r_1 \neq 0$, we divide b by r_1 and get

$$b = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1.$$

Here r_2 may be zero. If $r_2 \neq 0$, we divide r_1 by r_2 and get

$$r_1 = q_3 r_2 + r_3, \quad 0 \leq r_3 < r_2.$$

We proceed in this way. We have $b > r_1 > r_2 > r_3 > \dots$. Since the r_j 's are nonnegative integers and b is a finite positive integer, this process cannot go on indefinitely. Sooner or later, we will meet a division in which the remainder is zero, say at the $(k+1)$ -st step ($k \geq 0$):

$$r_{k-2} = q_k r_{k-1} + r_k, \quad 0 \leq r_k < r_{k-1}.$$

$$r_{k-1} = q_{k+1} r_k + r_{k+1}, \quad 0 = r_{k+1}.$$

We claim that r_k , the last nonzero remainder, is the greatest common divisor of a and b , and that it can be written in the form $ax - by$, where x,y are integers.

5.7 Theorem: *Let $a \geq b > 0$ be integers and let*

$$a = q_1 b + r_1, \quad 0 \leq r_1 < b,$$

$$b = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1,$$

$$r_1 = q_3 r_2 + r_3, \quad 0 \leq r_3 < r_2,$$

.....

$$r_{i-1} = q_{i+1} r_i + r_{i+1}, \quad 0 \leq r_{i+1} < r_i,$$

.....

$$r_{k-2} = q_k r_{k-1} + r_k, \quad 0 \leq r_k < r_{k-1},$$

$$r_{k-1} = q_{k+1} r_k$$

be the equations we obtain when we use the division algorithm (Theorem 5.3) succesively until we get a nonzero remainder. (This chain of equations is known as the *Euclidean algorithm*.) Then the last nonzero remainder r_k is the greatest common divisor of a and b . Moreover, r_k can be written in the form $r_{i-1}x - r_iy$; $x, y \in \mathbb{Z}$ for $i = k - 1, k - 2, \dots, 2, 1, 0$ (we put $r_0 = b, r_{-1} = a$). In particular, there are integers x_0, y_0 such that $(a, b) = ax_0 - by_0$, and eliminating r_1, r_2, \dots, r_{k-1} from the equations above gives a systematic way of finding the integers x_0, y_0 .

Proof: We must show that r_k satisfies the conditions (i),(ii),(iii) of Theorem 5.4. We know $r_k > 0$ from the k -th equation in the Euclidean algorithm, so (iii) of Theorem 5.4 is satisfied.

We prove (i) of Theorem 5.4, namely that $r_k|a$ and $r_k|b$. We start from the last equation in the algorithm and go up through the algorithm. From the $(k+1)$ -st equation, we get $r_k|r_{k-1}$. Using Lemma 5.2, we get $r_k|r_{k-2}$ from the k -th equation. So $r_k|r_{k-1}$ and $r_k|r_{k-2}$. From the $(k-1)$ -st equation, we get $r_k|r_{k-3}$, so $r_k|r_{k-2}$ and $r_k|r_{k-3}$. In general, if we have $r_k|r_{i+1}$ and $r_k|r_i$, the $(i+1)$ -st equation gives $r_k|r_{i-1}$, so we have $r_k|r_i$ and $r_k|r_{i-1}$. Going through the equations in this way, we finally get $r_k|r_0$ and $r_k|r_{-1}$, that is, we get $r_k|b$ and $r_k|a$. This proves (i) of Theorem 5.4.

Now (ii) of Theorem 5.4. Assume $e|a$ and $e|b$. We must prove $e|r_k$. We start from the first equation in the algorithm and go down through the algorithm. From the first equation, we get $e|a - q_1b$ and $e|r_1$ by Lemma 5.2. So $e|b$ and $e|r_1$. From the second equation, we get $e|b - q_2r_1$ and $e|r_2$. So $e|r_1$ and $e|r_2$. In general, if we have $e|r_{i-1}$ and $e|r_i$, the $(i+1)$ -st equation gives $e|r_{i-1} - q_{i+1}r_i$ and $e|r_{i+1}$. So $e|r_i$ and $e|r_{i+1}$. Going through the equations in this way, we finally get $e|r_k$. This proves (ii) of Theorem 5.4.

Hence r_k is the greatest common divisor of a and b .

Finally, we show the representability of r_k in terms of r_{i-1}, r_i as described. We start from the penultimate equation in the algorithm and go up through the algorithm. From the k -th equation, we obtain

$r_k = r_{k-2} - r_{k-1}q_k$, so r_k can be represented as $r_{k-2}x - r_{k-1}y$, namely with $x = 1, y = q_k$. Substituting $r_{k-3} - q_{k-1}r_{k-2}$ for r_{k-1} in this equation, we get

$$\begin{aligned} r_k &= r_{k-2} - r_{k-1}q_k = r_{k-2} - (r_{k-3} - q_{k-1}r_{k-2})q_k \\ &= r_{k-3}(-q_k) + r_{k-2}(1 + q_{k-1}q_k), \end{aligned}$$

so r_k can be represented as $r_{k-3}x - r_{k-2}y$, namely with $x = -q_k$, $y = -(1 + q_{k-1}q_k)$. In general, if r_k can be written in the form

$$r_i x - r_{i+1} y, \quad x, y \in \mathbb{Z},$$

we get, using the $(i+1)$ -st equation in the Euclidean algorithm,

$$\begin{aligned} r_k &= r_i x - r_{i+1} y \\ &= r_i x - (r_{i-1} - q_{i+1} r_i) y \\ &= r_{i-1} (-y) + r_i (x + q_{i+1} y), \end{aligned}$$

which shows that r_k can be written also in the form $r_{i-1} x_1 - r_i y_1$, namely with $x_1 = -y$, $y_1 = -(x + q_{i+1} y)$. Going through the equations in this way, we finally obtain

$$r_k = ax_0 - by_0$$

for some $x_0, y_0 \in \mathbb{Z}$. This completes the proof. \square

5.8 Example: To find the greatest common divisor of 14732 and 37149, and to express it in the form $14732x - 37149y$, with $x, y \in \mathbb{Z}$.

We have

$$\begin{aligned} 37149 &= 2 \cdot 14732 + 7685 \\ 14732 &= 1 \cdot 7685 + 7047 \\ 7685 &= 1 \cdot 7047 + 638 \\ 7047 &= 11 \cdot 638 + 29 \\ 638 &= 22 \cdot 29 \end{aligned}$$

and the last nonzero divisor is 29. So $(14732, 37149) = 29$. Also

$$\begin{aligned} 29 &= 7047 - 11 \cdot 638 \\ &= 7047 - 11(7685 - 1 \cdot 7047) \\ &= 12 \cdot 7047 - 11 \cdot 7685 \\ &= 12(14732 - 1 \cdot 7685) - 11 \cdot 7685 \\ &= 12 \cdot 14732 - 23 \cdot 7685 \\ &= 12 \cdot 14732 - 23(37149 - 2 \cdot 14732) \\ &= 58 \cdot 14732 - 23 \cdot 37149, \end{aligned}$$

so $29 = 14732x - 37149y$ with $x = 58$, $y = 23$.

5.9 Definition: Let a, b be integers, not both zero. a is said to be *relatively prime to b* if $(a, b) = 1$.

Since $(a, b) = (b, a)$, b is relatively prime to a in case a is relatively prime to b . This observation enables us to use a symmetric phrase in this case. We say a and b are relatively prime if $(a, b) = 1$.

5.10 Lemma: *Let a, b be integers, not both zero. Then a and b are relatively prime if and only if there are integers x_0, y_0 such that $ax_0 - by_0 = 1$.*

Proof: If $(a, b) = 1$, then there are integers x_0, y_0 such that $ax_0 - by_0 = 1$ by Theorem 5.6 or also by Theorem 5.7. Conversely, if there are integers x_0, y_0 with $ax_0 - by_0 = 1$, then 1 is certainly the smallest positive integer in the set $\{ax - by \in \mathbb{Z} : x, y \in \mathbb{Z}\}$, hence $(a, b) = 1$ by Theorem 5.6. \square

5.11 Lemma: *Let a, b be integers, not both zero, and let $d = (a, b)$. Then a/d and b/d are relatively prime.*

Proof: $a/d, b/d$ are integers, not both of them zero. We have $ax - by = d$ for suitable integers $x, y \in \mathbb{Z}$ by Theorem 5.7. Dividing both sides of this equation by $d > 0$, we get

$$(a/d)x - (b/d)y = 1,$$

and so $(a/d, b/d) = 1$ by Lemma 5.10 \square

Using Lemma 5.10, we prove an important result that will be crucial in the proof of the fundamental theorem of arithmetic.

5.12 Theorem: *Let a, b, c be integers. If $a|bc$ and $(a, b) = 1$, then $a|c$.*

Proof: Since $(a, b) = 1$, we have $ax - by = 1$ with some $x, y \in \mathbb{Z}$. Multiplying both sides of this equation by c , we obtain $acx - bcy = c$. Now $a|acx$ and, since $a|bc$ by hypothesis, $a|bcy$; hence $a|acx - bcy$ by Lemma 5.2. So $a|c$. \square

We separate $\mathbb{Z} \setminus \{0\}$ into three subsets: (1) units, (2) prime numbers, (3) composite numbers. The numbers 1 and -1 will be called *units*. The units divide every integer by Lemma 5.2(10). Any other integer a has at least four divisors: $\mp 1, \mp a$. These are called the *trivial divisors* of a . A divisor of a , which is not one of the four trivial divisors of a , is called a *proper*

divisor of a . If a nonzero integer a is not a unit and has no proper divisors, then a is called a *prime* number. Thus 2, -3, 5, 7, -11 are prime numbers. A nonzero integer, which is neither a unit nor a prime number, will be called a *composite* number. So $a \in \mathbb{Z} \setminus \{0\}$ is a composite number if and only if there is a $d \in \mathbb{Z}$ with $1 < |d| < |a|$ and $d|a$.

Prime numbers are the building blocks of integers in the following sense.

5.13 Theorem: *Any nonzero integer, which is not a unit, is either a prime number or a product of prime numbers.*

Proof: Take an integer $n \neq 0$, and assume that n is not a unit. If n is prime, there is nothing to prove. If n is composite, then $n = n_1 n_2$ for some $n_1, n_2 \in \mathbb{Z}$, $1 < |n_1| < |n|$, $1 < |n_2| < |n|$. If n_1 and n_2 are prime, we are through. Otherwise, factor n_1 and n_2 into two numbers. Keep factoring until you get down to prime numbers. Since the factors get smaller and smaller in absolute value, we will reach prime numbers at the end. This is the basic idea and we make this reasoning into a rigorous proof by induction.

We use Principle 4.5. Let q_n be the statement that $n \in \mathbb{N}$ is a prime number or a product of prime numbers. We begin induction at $n = 2$. Since 2 is a prime number, q_2 is true. q_3 is also true, for 3 is prime. q_4 is true, for $4 = 2 \cdot 2$ is a product of the prime numbers 2 and 2.

Suppose now $q_2, q_3, q_4, \dots, q_{k-1}$ are true, so that 2, 3, 4, \dots , $k-1$ are either prime numbers or products of prime numbers. We want to prove that k is a prime number or a product of prime numbers. If k is prime, we are done. If k is not prime, we have $k = k_1 k_2$, $1 < k_1 < k$, $1 < k_2 < k$, for some integers k_1, k_2 . Since q_{k_1} and q_{k_2} are true by the induction hypothesis, each of k_1, k_2 is either a prime number or a product of prime numbers:

$$k_1 = p_1 p_2 \cdots p_r \quad k_2 = p'_1 p'_2 \cdots p'_s$$

where $p_1, p_2, \dots, p_r, p'_1, p'_2, \dots, p'_s$ are prime numbers ($r = 1$ or $s = 1$ is possible, in which case $k_1 = p_1$ or $k_2 = p'_1$ are prime numbers), and so

$$k = k_1 k_2 = p_1 p_2 \cdots p_r p'_1 p'_2 \cdots p'_s,$$

is a product of prime numbers. Hence q_k is true.

This proves the theorem for positive integers. For a negative integer $-n$, where $-n$ is not a unit, we have

$$n = p_1 p_2 \cdots p_t$$

for some prime numbers p_1, p_2, \dots, p_t by what we proved above (possibly $t = 1$). Hence

$$-n = (-p_1) p_2 \cdots p_t$$

is prime or is a product of prime numbers. □

After reading the proof of this theorem, it will be clear to the reader that an abbreviation of the phrase "prime number or a product of prime numbers" will be very useful. When we speak of a product, we mean a product of two, three, or more terms. We now extend this to one factor. A single term will be called a product of one factor (or of one factors). A prime number is also a product of prime numbers with this convention. Our theorem reads now more shortly as follows.

5.13 Theorem: *Any nonzero integer, which is not a unit, is a product of prime numbers.* □

Now that we know any integer, which is not zero or a unit, can be expressed as a product of prime numbers, we ask if it can be written as a product of prime numbers in different ways. By way of example, let us begin decomposing 60 into prime numbers as in the proof of Theorem 5.13. We can begin from any decomposition of 60 into factors. For instance,

$$60 = 10 \cdot 6 \qquad 60 = 15 \cdot 4$$

Now we are to decompose each one of the factors 10, 6, 15, 4 into smaller factors until we get prime numbers. Will we reach the same prime numbers if we use the two different decompositions as our starting point? We know of course that further decomposition

$$60 = (2 \cdot 5)(2 \cdot 3) \qquad 60 = (3 \cdot 5)(2 \cdot 2)$$

yields the same prime numbers 2, 2, 3, 5 (aside from order). Nevertheless, our question should not be taken lightly. It is a very pertinent question. We remark that Theorem 5.13 says nothing in this regard. Theorem 5.13 says that, after enough factorizations, the factors will be prime. As it is, the prime numbers we obtain may very well be distinct if we start with

different factorizations. Indeed, if you start with different things, why on earth should you end with the same things? If 60 can be written as a product of factors in two different ways, as above, why should it not be written as a product of prime factors in two different ways? The reader's experience with the uniqueness of prime factors of integers should not mislead him (or her) to believe the uniqueness is obvious. It is anything but obvious.

Let us clarify what we mean by uniqueness. The two decompositions

$$2.5.2.3$$

$$3.5.2.2$$

of 60 involve the same prime numbers. Their order in the two decompositions are different, but nobody would consider these decompositions as very distinct. After all, multiplication of integers is commutative, and we can permute the factors without changing the value of the product. It would be foolish to regard two factorizations as different when they consist of the same prime numbers in different orders.

Moreover, we have $(-2)(5)(2)(-3) = 2.5.2.3$, where the numbers appearing are prime. These decompositions of 60 are not essentially distinct, of course. Given two nonzero integers a, b , we say a is *associate to b* if $a = b$ or $a = -b$. Then b is associate to a as well. Hence we may also say that a and b are associate. This means $a|b$ and $b|a$. It is clear from the definition that, whenever p and q are associate and p is prime, then q is a prime number, too. When we say uniqueness, we shall mean that the prime numbers in the decompositions of an integer are associate; we shall not mean that they are identical.

With this understanding, we will prove that any integer ($\neq 0, 1, -1$) has a unique decomposition into prime numbers. We need some lemmas.

5.14 Lemma: *Let a be an integer and p be a prime number. If $p \nmid a$, then $(a, p) = 1$.*

Proof: Let $d = (a, p)$. Then $d|p$. Since p is a prime number and $d > 0$, either $d = \pm p$ or $d = 1$. From $d|a$, $p \nmid a$, we conclude $d \neq \pm p$. So $d = 1$. \square

Our proof will depend heavily on the following corollary to Theorem 5.12. It is Proposition 30 in Euclid's *Elements*, Book VII. We shall refer to it as Euclid's lemma.

5.15 Lemma (Euclid's lemma): *Let a, b, p be integers. If p is prime and $p|ab$, then $p|a$ or $p|b$.*

Proof: If $p|a$, the lemma is proved. If $p \nmid a$, then $(a, p) = 1$ by Lemma 5.14 and, since $p|ab$, we get $p|b$ by Theorem 5.12 (with p, a, b in place of a, b, c , respectively). \square

5.16 Lemma: *Let a_1, a_2, \dots, a_n, p be integers. If p is prime and $p|a_1 a_2 \dots a_n$, then $p|a_1$ or $p|a_2$ or ... or $p|a_n$.*

Proof: This follows from Euclid's lemma by a routine induction argument. The details are left to the reader. \square

We can now prove uniqueness aside from trivial variations.

5.17 Theorem (Fundamental theorem of arithmetic): *Every integer, which is not zero or a unit, can be expressed as a product of prime numbers in a unique way, apart from the order of the factors and ambiguity of associate numbers.*

Proof: Let $n \in \mathbb{Z}$, $n \neq 0$, $n \neq \text{unit}$. By Theorem 5.13, n can be expressed as a product of prime numbers. We must show uniqueness. This will be done by induction on $|n| \in \mathbb{N}$. Given two decompositions

$$p_1 p_2 \dots p_r = n = q_1 q_2 \dots q_s$$

of n into prime factors, we have to show that

$$r = s$$

and that

p_1, p_2, \dots, p_r are, in some order, associate to q_1, q_2, \dots, q_s .

Assume first $|n| = 2$. Then $n = 2$ or $n = -2$ is prime and $n = \mp 2$ is the unique representation of n as a product of prime numbers (having only one factor). So the theorem is true for n if $|n| = 2$.

Now we make the inductive hypothesis that $|n| > 2$ and that the theorem is true for all $k \in \mathbb{Z}$ with $2 \leq |k| \leq n - 1$, and prove it for n .

If n is a prime number and

$$p_1 p_2 \cdots p_r = n = q_1 q_2 \cdots q_s \quad (r, s \in \mathbb{N}; p\text{'s and } q\text{'s are prime),$$

then necessarily $r = 1$, $s = 1$, $|p_1| = |n| = |q_1|$, so $p_1 = \mp q_1$. So p_1 and q_1 are associate and the decomposition is unique.

Assume now that

$$p_1 p_2 \cdots p_r = n = q_1 q_2 \cdots q_s \quad (r, s \in \mathbb{N}; p\text{'s and } q\text{'s are prime),$$

and that n is not a prime number. From $p_r | p_1 p_2 \cdots p_r$, we get $p_r | q_1 q_2 \cdots q_s$. By Lemma 5.16, $p_r | q_i$ for some $i = 1, 2, \dots, s$. Changing the order of the q 's if necessary, we may assume $p_r | q_s$. The divisors of q_s are $\mp 1, \mp q_s$. Since p_r is prime, so not a unit, and since $p_r | q_s$, we obtain $p_r = q_s$ or $p_r = -q_s$. Let $p_r = \mathbb{E} q_s$, with the appropriate unit $\mathbb{E} = \mp 1 \in \mathbb{Z}$. Then we get

$$\begin{aligned} \mathbb{E} p_1 p_2 \cdots p_r &= \mathbb{E} n = q_1 q_2 \cdots (\mathbb{E} q_s) \\ &= q_1 q_2 \cdots q_{s-1} p_r \end{aligned}$$

so

$$\mathbb{E} p_1 p_2 \cdots p_{r-1} = \mathbb{E} n / p_r = q_1 q_2 \cdots q_{s-1}$$

as two decompositions of $|\mathbb{E} n / p_r|$ into prime numbers. Since n is not a prime number and $|p_r| > 1$, we have $1 < |\mathbb{E} n / p_r| < n$. The induction hypothesis tells us that the two decompositions

$$\mathbb{E} p_1 p_2 \cdots p_{r-1} = q_1 q_2 \cdots q_{s-1}$$

of $|\mathbb{E} n / p_r|$ are essentially the same:

$$r - 1 = s - 1$$

and $\mathbb{E} p_1 p_2, \dots, p_{r-1}$ are, in some order, associate to q_1, q_2, \dots, q_{s-1} . Then

$$r = s$$

and $p_1 p_2, \dots, p_{r-1}$ are, in some order, associate to q_1, q_2, \dots, q_{s-1} ; and p_r is associate to q_s . This completes the proof. \square

5.18 Remarks: Collecting the same prime divisors of $n \in \mathbb{N}$ ($n > 1$) in a single prime power, we can write

$$n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}, \quad (*)$$

where $0 < p_1 < p_2 < \dots < p_r$ are the distinct prime divisors of n , and a_1, a_2, \dots, a_r positive integers. Then (*) is called the *canonical decomposition of n* into prime numbers.

Sometimes it is convenient to relax the condition that the exponents a_i be all positive to the condition that they be nonnegative. For example, the divisors of $n \in \mathbb{N}$, whose canonical decomposition is (*), are exactly the numbers

$$\mp p_1^{b_1} p_2^{b_2} \dots p_r^{b_r},$$

where $0 \leq b_i \leq a_i$ for all $i = 1, 2, \dots, r$. If m and n are two natural numbers and

$$m = p_1^{c_1} p_2^{c_2} \dots p_r^{c_r}, \quad n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r},$$

where p_1, p_2, \dots, p_r are distinct prime numbers and $c_i \geq 0, e_i \geq 0$ for all $i = 1, 2, \dots, r$, then (m, n) is given by

$$(m, n) = p_1^{t_1} p_2^{t_2} \dots p_r^{t_r}$$

with $t_i = \min\{c_i, e_i\}$ for all $i = 1, 2, \dots, r$. Here $\min\{x, y\}$ denotes the smaller (minimum) of x and y when $x \neq y$ and denotes x when $x = y$.

It can be shown that $((a, b), c) = (a, (b, c))$ for any $a, b, c \in \mathbb{Z}$, provided a, b are not both equal to zero and b, c are not both equal to zero. The positive number $((a, b), c)$ is called the *greatest common divisor* of a, b, c , and is denoted shortly by (a, b, c) . One proves easily that (a, b, c) is the unique integer d such that

- (i) $d|a, d|b, d|c$,
- (ii) for all $d_1 \in \mathbb{Z}$, if $d_1|a, d_1|b, d_1|c$, then $d_1|d$,
- (iii) $d > 0$,

and that there are integers x, y, z satisfying

$$ax + by + cz = (a, b, c).$$

Inductively, if the greatest common divisor of $n-1$ integers a_1, a_2, \dots, a_{n-1} has already been defined and denoted as $(a_1, a_2, \dots, a_{n-1})$, then the greatest common divisor $(a_1, a_2, \dots, a_{n-1}, a_n)$ of n integers $a_1, a_2, \dots, a_{n-1}, a_n$

is defined to be $((a_1, a_2, \dots, a_{n-1}), a_n)$. One can show that their greatest common divisor $(a_1, a_2, \dots, a_{n-1}, a_n)$ is the unique integer d such that

- (i) $d|a_1, d|a_2, \dots, d|a_{n-1}, d|a_n$
- (ii) for all $d_1 \in \mathbb{Z}$, if $d_1|a_1, d_1|a_2, \dots, d_1|a_{n-1}, d_1|a_n$, then $d_1|d$,
- (iii) $d > 0$.

In addition, one proves that there are integers $x_1, x_2, \dots, x_{n-1}, x_n$ such that

$$a_1x_1 + a_2x_2 + \dots + a_{n-1}x_{n-1} + a_nx_n = (a_1, a_2, \dots, a_{n-1}, a_n).$$

If $(a_1, a_2, \dots, a_{n-1}, a_n) = 1$, we say that $a_1, a_2, \dots, a_{n-1}, a_n$ are relatively prime. In this case, there are integers $x_1, x_2, \dots, x_{n-1}, x_n$ satisfying

$$a_1x_1 + a_2x_2 + \dots + a_{n-1}x_{n-1} + a_nx_n = 1.$$

The proofs of these assertions are left to the reader.

Our final topic in this paragraph will be the least common multiple of two nonzero integers. If $a, b \in \mathbb{Z}$ and $a|b$, we say that b is a *multiple* of a .

5.19 Theorem: *Let $a, b \in \mathbb{Z}$, neither of them zero (i.e., $a \neq 0 \neq b$). Then there is a unique integer such that*

- (i) $a|m$ and $b|m$,
- (ii) for all $m_1 \in \mathbb{Z}$, if $a|m_1$ and $b|m_1$, then $m|m_1$,
- (iii) $m > 0$.

Proof: The proof will be similar to that of Theorem 5.4. We consider the set $V = \{n \in \mathbb{N} : a|n \text{ and } b|n\}$. This set is not empty, since, for example, $|ab|$ is in V (here we use the hypothesis $a \neq 0 \neq b$). We choose the smallest positive integer in V . Let it be called m . Thus $m > 0$ and m satisfies (iii). Also, $a|m$ and $b|m$ since $m \in V$, and m satisfies (i). It remains to show that m satisfies (ii).

Suppose $m_1 \in \mathbb{Z}$, and $a|m_1$ and $b|m_1$. We divide m_1 by m and get, say, $m_1 = qm + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < m$. Since $a|m$, $a|m_1$ and $b|m$, $b|m_1$, the equation $m_1 = qm + r$ yields that $a|r$ and $b|r$. Hence $r \in V$. We know $0 \leq r < m$. If r were not zero, then r would be a natural number

in V smaller than the smallest natural number m in V , which is absurd. Thus $r = 0$, so $m_1 = qm$, and $m|m_1$. This shows that m satisfies (ii).

Now the uniqueness of m . Suppose m' satisfies the conditions (i), (ii), (iii), too. Then $a|m'$, $b|m'$ by (i), and so $m|m'$ by (ii). Also, $a|m$, $b|m$ by (i), and so $m'|m$ by (ii). Hence $m|m'$ and $m'|m$. By Lemma 5.2(12), we obtain $|m| = |m'|$. From (iii), we have $m > 0$, $m' > 0$, which yields $m = m'$. Thus m is unique. \square

5.20 Definition: Let $a, b \in \mathbb{Z}$, neither of them zero. The unique integer m in Theorem 5.19 is called the *least common multiple of a and b* .

The least common multiple of a and b will be denoted by $[a, b]$. From the proof of Theorem 5.19, we see that $[a, b]$ is indeed the smallest of the positive multiples of a and b ($[a, b]$ is the smallest number in V). From the fact that $a|m$ and $-a|m$ are equivalent, and likewise that $b|m$ and $-b|m$ are equivalent, it follows that the defining conditions (i), (ii), (iii) do not change when we replace a by $-a$ or b by $-b$. Therefore, $[a, b] = [-a, b] = [-a, -b] = [a, -b]$. In the same way, the conditions (i), (ii), (iii) in Theorem 5.19 are symmetric in a and b , and this gives $[a, b] = [b, a]$.

The greatest common divisor and the least common multiple of two integers will be connected in Lemma 5.22. We need a preliminary result.

5.21 Lemma: Let a, b, m be integers and $a \neq 0$, $b \neq 0$. If $a|m, b|m$ and $(a, b) = 1$, then $ab|m$.

Proof: This follows immediately from the fundamental theorem of arithmetic (Theorem 5.17), but we give another proof. Since $a|m$ and $b|m$, there are integers a_1, b_1 such that $aa_1 = m = bb_1$. Hence $a|bb_1$. Since $(a, b) = 1$, Theorem 5.12 yields $a|b_1$. So $b_1 = ac$ for some integer c and $m = bb_1 = bac = abc$, so $ab|m$, as claimed. \square

5.22 Lemma: Let a and b be integers, neither of them zero. Then we have $[a, b] = |ab|/(a, b)$.

Proof: As neither $[a,b]$, nor (a,b) , nor $|ab|$ changes when we replace a and b by their absolute values, we assume, without loss of generality, that $a > 0$, $b > 0$. We put $d = (a,b)$. We show that ab/d satisfies the three conditions (i), (ii), (iii) in Theorem 5.19. Let $a = a_1d$, $b = b_1d$, so that $(a_1, b_1) = 1$ by Lemma 5.11.

We have $a|ab_1$, so $a|a(b/d)$; and $b|a_1b$, so $b|(a/d)b$. Thus a divides ab/d and b divides ab/d . Hence ab/d satisfies (i). Clearly $ab/d > 0$, so ab/d satisfies (iii). We now show that ab/d satisfies (ii) as well; i.e., we show that ab/d divides m_1 whenever $a|m_1$ and $b|m_1$. Let $m_1 \in \mathbb{Z}$ and $a|m_1$, $b|m_1$. Then $d|m_1$ and in fact a_1 divides m_1/d and b_1 divides m_1/d . By Lemma 5.21 (with $a_1, b_1, m_1/d$ in place of a, b, m , respectively), we get a_1b_1 divides m_1/d , so $ab|m_1d$, so ab/d divides m_1 . Thus ab/d satisfies (ii) and $ab/d = [a,b]$ □

It can be shown that $[[a,b],c] = [a,[b,c]]$ for any $a,b,c \in \mathbb{Z}$, provided a,b,c are all distinct from zero. The positive number $[[a,b],c]$ is called the *least common multiple of a,b,c* , and is denoted shortly by $[a,b,c]$. One proves easily that $[a,b,c]$ is the unique integer m such that

- (i) $a|m$, $b|m$, $c|m$,
- (ii) for all $m_1 \in \mathbb{Z}$, if $a|m_1$, $b|m_1$, $c|m_1$, then $m|m_1$,
- (iii) $m > 0$.

Inductively, if the least common multiple of $n - 1$ integers a_1, a_2, \dots, a_{n-1} has already been defined and denoted as $[a_1, a_2, \dots, a_{n-1}]$, then the least common multiple $[a_1, a_2, \dots, a_{n-1}, a_n]$ of n integers $a_1, a_2, \dots, a_{n-1}, a_n$ is defined to be $[[a_1, a_2, \dots, a_{n-1}], a_n]$. One can show that their least common multiple $[a_1, a_2, \dots, a_{n-1}, a_n]$ is the unique integer m such that

- (i) $a_1|m$, $a_2|m$, \dots , $a_{n-1}|m$, $a_n|m$,
- (ii) for all $m_1 \in \mathbb{Z}$, if $a_1|m_1$, $a_2|m_1$, \dots , $a_{n-1}|m_1$, $a_n|m_1$, then $m|m_1$,
- (iii) $m > 0$.

Exercises

1. Find $(10897, 16949)$ and express it in the form $10897x + 16949y$, where x and y are integers.

2. Assume $m, n \in \mathbb{N}$ and $m \neq n$. What is $(2^{2^m} + 1, 2^{2^n} + 1)$?

3. Let $a, b \in \mathbb{Z}$, neither of them equal to zero, and assume $(a, b) = 1$. Let x_0, y_0 be integers such that $ax_0 + by_0 = 1$. Prove that all integer pairs x, y satisfying $ax + by = 1$ are given by

$$x = x_0 + bt, \quad y = y_0 - at$$

as t runs through all integers.

4. Let a, b, c be integers, none of them equal to zero, and let $(a, b) = d$. Prove that there are integers x, y satisfying $ax + by = c$ if and only if $d|c$. Moreover, if $d|c$ and x_0, y_0 are integers such that $ax_0 + by_0 = c$, prove that all integer pairs x, y satisfying $ax + by = c$ are given by

$$x = x_0 + (b/d)t, \quad y = y_0 - (a/d)t$$

as t runs through all integers.

5. Prove the assertions in Remark 5.18.

6. Let m and n be two natural numbers and

$$m = p_1^{c_1} p_2^{c_2} \dots p_r^{c_r}, \quad n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r},$$

where p_1, p_2, \dots, p_r are distinct prime numbers and $c_i \geq 0, e_i \geq 0$ for all $i = 1, 2, \dots, r$. Show that

$$[m, n] = p_1^{u_1} p_2^{u_2} \dots p_r^{u_r}$$

with $u_i = \max\{c_i, e_i\}$ for all $i = 1, 2, \dots, r$. Here $\max\{x, y\}$ denotes the greater (maximum) of x and y when $x \neq y$ and denotes x when $x = y$.

7. Prove or disprove: $(a, [b, c]) = [(a, b), (a, c)]$ for all $a, b, c \in \mathbb{N}$.

8. Let $a, b \in \mathbb{Z}$, $b > 0$, and $a = qb + r$, with $q, r \in \mathbb{Z}$, $0 \leq r < b$. Prove directly that $(a, b) = (a, r)$.

9. Let $a, b \in \mathbb{Z}$ and $(a, b) = 1$. Show that $(a - b, a + b) = 1$ or 2 .

10. Let a, m, n be natural numbers. Show that $(a^m - 1, a^n - 1) = a^{(m, n)} - 1$.