20. Let a, b, n be integers with $n > 1$. Suppose that $a = nq_1 + r_1$ with $0 \leq r_1 < n$ and $b = nq_2 + r_2$ with $0 \leq r_2 < n$. Prove that $n \mid (a - b)$ if and only if $r_1 = r_2$.

21. Show that any nonempty set of integers that is closed under subtraction must also be closed under addition. (Thus part of the hypothesis of Theorem 1.1.4 is redundant.)

22. Let a, b, q, r be integers such that $b \neq 0$ and $a = bq + r$. Prove that $(a, b) = (b, r)$ by showing that (b, r) satisfies the definition of the greatest common divisor of a and b.

23. Perhaps a more natural definition of the greatest common divisor is the following: Let a and b be integers, not both zero. An integer d is called the greatest common divisor of the nonzero integers a and b if (i) $d \mid a$ and $d \mid b$, and (ii) $c \mid a$ and $c \mid b$ implies $d \geq c$. Show that this definition is equivalent to Definition 1.1.5.

24. Show that 3 divides the sum of the cubes of any three consecutive positive integers.

25.† Find all integers x such that $3x + 7$ is divisible by 11.

26. Prove the following proposition. Let $a, b, n \in \mathbf{Z}$ with $(a, b) = d$, and let x_0, y_0 be a particular solution to the equation $ax + by = n$. Then every solution to $ax + by = n$ has the form $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$, for some $t \in \mathbf{Z}$. Furthermore, for every $t \in Z$ the integers $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$, yield a solution to $ax + by = n$.

27. Prove the following proposition. Let $a, b \in \mathbf{Z}^+$ with $(a, b) = 1$. Then the equation $ax + by = n$ has solutions $x, y \in \mathbf{Z}$ with $x \geq 0$, $y \geq 0$ if $n > ab - a - b$. Moreover, if $n = ab - a - b$, then there are no such solutions.

28. Formulate a definition of the greatest common divisor of three integers a, b, c (not all zero). With the appropriate definition you should be able to prove that the greatest common divisor is a linear combination of a, b and c.

1.2 Primes

The main focus of this section is on prime numbers. Our method will be to investigate the notion of two integers which are relatively prime, that is, those which have no common divisors except ± 1. Using some facts which we will prove about them, we will be able to prove the prime factorization theorem, which states that every nonzero integer can be expressed as a product of primes. Finally, we will be able to use prime factorizations to learn more about greatest common divisors and least common multiples.

1.2.1 Definition. *The nonzero integers a and b are said to be* ***relatively prime*** *if* $(a, b) = 1$.

1.2.2 Proposition. *Let a, b be nonzero integers. Then $(a, b) = 1$ if and only if there exist integers m, n such that $ma + nb = 1$.*

Proof. If a and b are relatively prime, then by Theorem 1.1.6 integers m and n can be found for which $ma + nb = 1$. To prove the converse, we only need to note that if there exist integers m and n with $ma + nb = 1$, then 1 must be the smallest positive linear combination of a and b, and thus $(a, b) = 1$, again by Theorem 1.1.6. □

Proposition 1.2.2 will be used repeatedly in the proof of the next result. A word of caution—it is tempting to jump from the equation $d = ma + nb$ to the conclusion that $d = (a, b)$. For example, $16 = 2 \cdot 5 + 3 \cdot 2$, but obviously $(5, 2) \neq 16$. The most that it is possible to say (using Theorem 1.1.6) is that d is a multiple of (a, b). Of course, if $ma+nb = 1$, then Proposition 1.2.2 implies that $(a, b) = 1$.

1.2.3 Proposition. *Let a, b, c be integers, where $a \neq 0$ or $b \neq 0$.*

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

(b) *If $b \mid ac$ and $(a, b) = 1$, then $b \mid c$.*

(c) *If $b \mid a$, $c \mid a$ and $(b, c) = 1$, then $bc \mid a$.*

(d) *$(a, bc) = 1$ if and only if $(a, b) = 1$ and $(a, c) = 1$.*

Proof. (a) Assume that $b \mid ac$. To show that $b \mid (a, b) \cdot c$, we will try to find an expression for $(a, b) \cdot c$ that has b as an obvious factor. We can write $(a, b) = ma + nb$ for some $m, n \in \mathbf{Z}$, and then multiplying by c gives

$$(a, b) \cdot c = mac + nbc .$$

Now b is certainly a factor of nbc, and by assumption it is also a factor of ac, so it is a factor of mac and therefore of the sum $mac + nbc$. Thus $b \mid (a, b) \cdot c$.

(b) Simply letting $(a, b) = 1$ in part (a) gives the result immediately.

(c) If $b \mid a$, then $a = bq$ for some integer q. If $c \mid a$, then $c \mid bq$, so if $(b, c) = 1$, it follows from part (b) that $c \mid q$, say with $q = cq_1$. Substituting for q in the equation $a = bq$ gives $a = bcq_1$, and thus $bc \mid a$.

(d) Suppose that $(a, bc) = 1$. Then $ma + n(bc) = 1$ for some integers m and n, and by viewing this equation as $ma + (nc)b = 1$ and $ma + (nb)c = 1$ we can see that $(a, b) = 1$ and $(a, c) = 1$.

Conversely, suppose that $(a, b) = 1$ and $(a, c) = 1$. Then $m_1a + n_1b = 1$ for some integers m_1 and n_1, and $m_2a + n_2c = 1$ for some integers m_2 and n_2. Multiplying these two equations gives

$$(m_1m_2a + m_1n_2c + m_2n_1b)a + (n_1n_2)bc = 1,$$

which shows that $(a, bc) = 1$. □

1.2.4 Definition. *An integer $p > 1$ is called a* ***prime number*** *if its only divisors are ± 1 and $\pm p$. An integer $a > 1$ is called* ***composite*** *if it is not prime.*

To determine whether or not a given integer $n > 1$ is prime, we could just try to divide n by each positive integer less than n. This method of trial division is very inefficient, and for this reason various sophisticated methods of "primality testing" have been developed. The need for efficient tests has become particularly apparent recently, because of applications to computer security that make use of cryptographic algorithms. To determine the complete list of all primes up to some bound, there is a useful procedure handed down from antiquity.

Example 1.2.1 (Sieve of Eratosthenes).

The primes less than a fixed positive integer a can be found by the following procedure. List all positive integers less than a (except 1), and cross off every even number except 2. Then go to the first number that has not been crossed off, which will be 3, and cross off all higher multiples of 3. Continue this process to find all primes less than a. You can stop after you have crossed off all proper multiples of primes p for which $p < \sqrt{a}$, since you will have crossed off every number less than a that has a proper factor. (If b is composite, say $b = b_1 b_2$, then either $b_1 \leq \sqrt{b}$ or $b_2 \leq \sqrt{b}$.) For example, we can find all primes less than 20 by just crossing off all multiples of 2 and 3, since $5 > \sqrt{20}$:

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	.

This method is attributed to the Greek mathematician Eratosthenes, and is called the **sieve of Eratosthenes**.

Similarly, the integers less than a and relatively prime to a can be found by crossing off the prime factors of a and all of their multiples. For example, the prime divisors of 36 are 2 and 3, and so the positive integers less than 36 and relatively prime to it can be found as follows:

1	~~2~~	~~3~~	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~
13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~
25	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~	35	.

□

Euclid's lemma, the next step in our development of the fundamental theorem of arithmetic, is the one that requires our work on relatively prime numbers. We will use Proposition 1.2.3 (b) in a crucial way.

1.2.5 Lemma (Euclid). *An integer $p > 1$ is prime if and only if it satisfies the following property: for all integers a and b, if $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

Proof. Suppose that p is prime and $p \mid ab$. We know that either $(p,a) = p$ or $(p,a) = 1$, since (p,a) is always a divisor of p and p is prime. In the first case $p \mid a$ and we are done. In the second case, since $(p,a) = 1$, we can apply Proposition 1.2.3 (b) to show that $p \mid ab$ implies $p \mid b$. Thus we have shown that if $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Conversely, suppose that p satisfies the given condition. If p were composite, then we could write $p = ab$ for some positive integers smaller than p. The condition would imply that either $p \mid a$ or $p \mid b$, which would be an obvious contradiction. □

The following corollary extends Euclid's lemma to the product of more than two integers. In the proof we will use mathematical induction, which we hope is familiar to you. If you do not remember how to use induction, you should read the discussion in Appendix A.4.

1.2.6 Corollary. *If p is a prime number, and $p \mid a_1 a_2 \cdots a_n$ for integers $a_1, a_2, \ldots, a_n$, then $p \mid a_i$ for some i with $1 \leq i \leq n$.*

Proof. In order to use the principle of mathematical induction, let P_n be the following statement: if $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some $1 \leq i \leq n$. The statement P_1 is clearly true. Next, assume that the statement P_k is true, that is, if $p \mid a_1 a_2 \cdots a_k$, then $p \mid a_i$ for some $1 \leq i \leq k$. If $p \mid a_1 a_2 \cdots a_k a_{k+1}$, for integers $a_1, a_2, \ldots, a_k, a_{k+1}$, then applying Euclid's lemma to $a = a_1 a_2 \cdots a_k$ and $b = a_{k+1}$ yields that $p \mid a_1 a_2 \cdots a_k$ or $p \mid a_{k+1}$. In case $p \mid a_1 a_2 \cdots a_k$, the truth of the statement P_k implies that $p \mid a_i$ for some $1 \leq i \leq k$. Thus, in either case, $p \mid a_i$ for some $1 \leq i \leq k+1$, and hence the statement P_{k+1} is true. By the principle of mathematical induction (as stated in Theorem A.4.2 of Appendix A.4), the statement P_n holds for all positive integers n. □

The next theorem, on prime factorization, is sometimes called the fundamental theorem of arithmetic. The naive way to prove that an integer a can be written as a product of primes is to note that either a is prime and we are done, or else a is composite, say $a = bc$. Then the same argument can be applied to b and c, and continued until a has been broken up into a product of primes. (This process must stop after a finite number of steps because of the well-ordering principle.) We also need to prove that any two factorizations of a number are in reality the same. The idea of the proof is to use Euclid's lemma to pair the primes in one factorization with those in the other. In fact, the proof of the uniqueness of the factorization requires a more delicate argument than the proof of the existence of the factorization.

1.2.7 Theorem (Fundamental Theorem of Arithmetic). *Any integer $a > 1$ can be factored uniquely as a product of prime numbers, in the form*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} ,$$

where $p_1 < p_2 < \ldots < p_n$ and the exponents $\alpha_1, \alpha_2, \ldots, \alpha_n$ are all positive.

Proof. Suppose that there is some integer greater than 1 that cannot be written as a product of primes. Then the set of all integers $a > 1$ that have no prime factorization must be nonempty, so as a consequence of the well-ordering principle it must have a smallest member, say b. Now b cannot itself be a prime number since then it would have a prime factorization. Thus b is composite, and we can write $b = cd$ for positive integers c, d that are smaller than b. Since b was assumed to be the smallest positive integer not having a factorization into primes, and c and d are smaller, then both c and d must have factorizations into products of primes. This shows that b also has such a factorization, which is a contradiction. Since multiplication is commutative, the prime factors can be ordered in the desired manner.

If there exists an integer > 1 for which the factorization is not unique, then by the well-ordering principle there exists a smallest such integer, say a. Assume that a has two factorizations $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ and $a = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$, where $p_1 < p_2 < \ldots < p_n$, and $q_1 < q_2 < \ldots < q_m$, with $\alpha_i > 0$ for $i = 1, \ldots, n$, and $\beta_i > 0$ for $i = 1, \ldots, m$. By Corollary 1.2.6 of Euclid's lemma, $q_1 \mid p_k$ for some k with $1 \leq k \leq n$ and $p_1 \mid q_j$ for some j with $1 \leq j \leq m$. Since all of the numbers p_i and q_i are prime, we must have $q_1 = p_k$ and $p_1 = q_j$. Then $p_1 = q_1$ since $q_1 \leq q_j = p_1 \leq p_k = q_1$. Hence we can let

$$s = \frac{a}{p_1} = \frac{a}{q_1} = p_1^{\alpha_1 - 1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} = q_1^{\beta_1 - 1} q_2^{\beta_2} \cdots q_m^{\beta_m} .$$

If $s = 1$ then $a = p_1$ has a unique factorization, contrary to the choice of a. If $s > 1$, then since $s < a$ and s has two factorizations, we again have a contradiction to the choice of a. □

If the prime factorization of an integer is known, then it is easy to list all of its divisors. If $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, then b is a divisor of a if and only if $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, where $\beta_i \leq \alpha_i$ for all i. Thus we can list all possible divisors of a by systematically decreasing the exponents of each of its prime divisors.

Example 1.2.2 (Divisor diagrams).

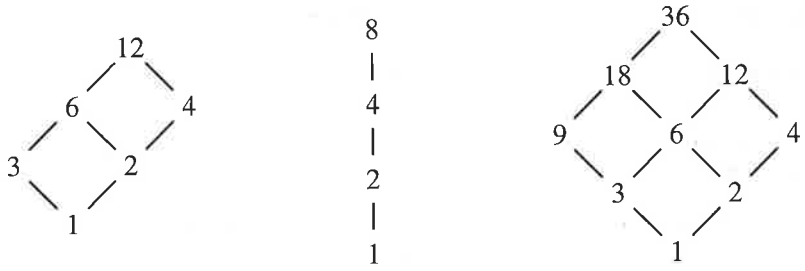
The positive divisors of 12 are $1, 2, 3, 4, 6, 12$; the positive divisors of 8 are $1, 2, 4, 8$; and the positive divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. In Figure 1.2.1, we have arranged the divisors so as to show the divisibility relations

among them. There is a path (moving upward only) from a to b if and only if $a \mid b$.

In constructing the first diagram in Figure 1.2.1, it is easiest to use the prime factorization of 12. Since $12 = 2^2 3$, we first divide 12 by 2 to get 6 and then divide again by 2 to get 3. This gives the first side of the diagram, and to construct the opposite side of the diagram we divide each number by 3.

If the number has three different prime factors, then we would need a three-dimensional diagram. (Visualize the factors as if on the edges of a box.) With more than three distinct prime factors, the diagrams lose their clarity. □

Figure 1.2.1:



The following proof, although easy to follow, is an excellent example of the austere beauty of mathematics.

1.2.8 Theorem (Euclid). *There exist infinitely many prime numbers.*

Proof. Suppose that there were only finitely many prime numbers, say p_1, p_2, $\ldots$, p_n. Then consider the number $a = p_1 p_2 \cdots p_n + 1$. By Theorem 1.2.7, the number a has a prime divisor, say p. Now p must be one of the primes we listed, so $p \mid (p_1 p_2 \cdots p_n)$, and since $p \mid a$, it follows that $p \mid (a - p_1 p_2 \cdots p_n)$. This is a contradiction since p cannot be a divisor of 1. □

Example 1.2.3 (Mersenne numbers).

An integer of the form $2^n - 1$, for $n \in \mathbf{Z}^+$, is called a **Mersenne number**. It has been conjectured that infinitely many Mersenne numbers are prime.

Consider the numbers $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^4 - 1 = 15$, $2^5 - 1 = 31$, and $2^6 - 1 = 63$. The prime exponents each give rise to a prime, while the composite exponents each give a composite number. Is this true in general? Continuing to investigate prime exponents gives $2^7 - 1 = 127$, which is

prime, but $2^{11} - 1 = 2047 = 23 \cdot 89$. Thus a prime exponent may or may not yield a prime number.

On the other hand, it is always true that a composite exponent yields a composite number. To prove this, let n be composite, say $n = qm$ (where q and m are integers greater than 1), and consider $2^n - 1 = 2^{qm} - 1$. We need to find a nontrivial factorization of $2^{qm} - 1 = (2^q)^m - 1$. We can look at this as $x^m - 1$, and then we have the familiar factorization

$$x^m - 1 = (x-1)(x^{m-1} + x^{m-2} + \ldots + x^2 + x + 1) .$$

Substituting $x = 2^q$ shows that $2^q - 1$ is a factor of $2^n - 1$. Now $1 < 2^q - 1 < 2^n - 1$ since both q and m are greater than 1, and so we have found a nontrivial factorization of $2^n - 1$. □

Example 1.2.4 ($(2^m - 1, 2^n - 1) = 1$ if and only if $(m, n) = 1$).

Let m and n be positive integers. We will prove that $(2^m - 1, 2^n - 1) = 1$ if and only if $(m, n) = 1$, for any positive integers m and n.

Comment: Since this statement is "if and only if", the proof will have two parts. We first show the "only if" part, since it is shorter.

Proof: Suppose that $(m, n) \neq 1$, say $(m, n) = d$. Then there exist $p, q \in \mathbf{Z}$ with $m = dq$ and $n = dp$. The factorization given in Example 1.2.3 shows that $2^d - 1$ is a proper nontrivial divisor of both $2^{dq} - 1$ and $2^{dp} - 1$, and therefore $(2^m - 1, 2^n - 1) \neq 1$.

To prove that $(2^m - 1, 2^n - 1) = 1$ if $(m, n) = 1$, we start by assuming that $(m, n) = 1$. Then we can write $am + bn = 1$ for integers a, b, where we can assume without loss of generality that $a < 0$ and $b > 0$. Then, as in Example 1.2.3, $2^m - 1$ is a factor of $2^{-am} - 1$, say $2^{-am} - 1 = (2^m - 1)s$, and $2^n - 1$ is a factor of $2^{bn} - 1$, say $2^{bn} - 1 = (2^n - 1)t$, for positive integers s, t. Then $bn = 1 + (-a)m$, so

$$\begin{aligned} (2^n - 1)t &= 2^{bn} - 1 = 2^{1+(-a)m} - 1 \\ &= 2(2^{-am}) - 1 = 2(2^{-am} - 1) + 2 - 1 \\ &= 2(2^m - 1)s + 1 \end{aligned}$$

and therefore $t(2^n - 1) - 2s(2^m - 1) = 1$. This shows that $(2^m - 1, 2^n - 1) = 1$, and completes the proof. □

The final concept we study in this section is the least common multiple of two integers. Its definition is parallel to that of the greatest common divisor. We can characterize it in terms of the prime factorizations of the two numbers, or by the fact that the product of two numbers is equal to the product of their least common multiple and greatest common divisor.

1.2.9 Definition. *A positive integer m is called the* ***least common multiple*** *of the nonzero integers a and b if*

(i) *m is a multiple of both a and b, and*

(ii) *any multiple of both a and b is also a multiple of m.*

We will use the notation $\operatorname{lcm}[a,b]$ *or* $[a,b]$ *for the least common multiple of a and b.*

When written out in symbols, the definition of the least common multiple looks like this: $m = \operatorname{lcm}[a,b]$ if (i) $a \mid m$ and $b \mid m$, and (ii) if $a \mid c$ and $b \mid c$, then $m \mid c$.

There are times, as in next proposition, when it is convenient to allow the prime factorization of a number to include primes with exponent 0. This leads to a representation that is no longer unique, but it is particularly useful to be able to write the prime factorizations of two different integers in terms of the *same* primes.

1.2.10 Proposition. *Let a and b be positive integers with prime factorizations $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, where $\alpha_i \geq 0$ and $\beta_i \geq 0$ for all i.*

(a) *Then $a \mid b$ if and only if $\alpha_i \leq \beta_i$ for $i = 1, 2, \ldots, n$.*

(b) *For each i, let $\delta_i = \min\{\alpha_i, \beta_i\}$ and $\mu_i = \max\{\alpha_i, \beta_i\}$. Then*

$$\gcd(a,b) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n} \quad \text{and} \quad \operatorname{lcm}[a,b] = p_1^{\mu_1} p_2^{\mu_2} \cdots p_n^{\mu_n} .$$

Proof. (a) Suppose that $\alpha_i \leq \beta_i$ for $i = 1, 2, \ldots, n$. Let $\gamma_i = \beta_i - \alpha_i$, for $i = 1, 2, \ldots, n$, and set $c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$ (note that $\gamma_i \geq 0$ for $i = 1, 2, \ldots, n$). Then

$$\begin{aligned} ac &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n} = p_1^{\alpha_1+\gamma_1} p_2^{\alpha_2+\gamma_2} \cdots p_n^{\alpha_n+\gamma_n} \\ &= p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n} = b . \end{aligned}$$

Since $b = ac$, we have $a \mid b$.

Conversely, suppose that $a \mid b$. Then there exists $c \in \mathbf{Z}$ such that $b = ac$. For any prime p such that $p \mid c$, we have $p \mid b$, and so $p = p_j$ for some j with $1 \leq j \leq n$. Thus c has a factorization $c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$, where $\gamma_i \geq 0$ for $i = 1, 2, \ldots, n$. Since $b = ac$, we have

$$p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n} = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n} = p_1^{\alpha_1+\gamma_1} p_2^{\alpha_2+\gamma_2} \cdots p_n^{\alpha_n+\gamma_n} ,$$

where $\beta_i = \alpha_i + \gamma_i$ for $i = 1, 2, \ldots, n$. Because $\gamma_i \geq 0$, we have $\alpha_i \leq \beta_i$ for $i = 1, 2, \ldots, n$.

(b) The proof follows immediately from part (a) and the definitions of the least common multiple and greatest common divisor. □

As a corollary of Proposition 1.2.10, it is clear that $\gcd(a,b) \cdot \text{lcm}[a,b] = ab$. This can also be shown directly from the definitions, as we have noted in Exercise 19.

For small numbers it is probably easiest to use their prime factorizations to find their greatest common divisor and least common multiple. It takes a great deal of work to find the prime factors of a large number, even on a computer making use of sophisticated algorithms. In contrast, the Euclidean algorithm is much faster, so its use is more efficient for finding the greatest common divisor of large numbers.

Example 1.2.5.

In the previous section we computed $(126, 35)$. To do this using Proposition 1.2.10 we need the factorizations $126 = 2^1 \cdot 3^2 \cdot 7^1$ and $35 = 5^1 \cdot 7^1$. We then add terms so that we have the same primes in each case, to get $126 = 2^1 \cdot 3^2 \cdot 5^0 \cdot 7^1$ and $35 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^1$. Thus we obtain $(126, 35) = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 = 7$ and $[126, 35] = 2^1 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 630$. □

Example 1.2.6 ($(a,b) = 1$ if and only if $(a^2, b^2) = 1$).

We will give two essentially different proofs that $(a,b) = 1$ if and only if $(a^2, b^2) = 1$, for any positive integers a, b.

First proof: Proposition 1.2.3 (d) states that $(a, bc) = 1$ if and only if $(a,b) = 1$ and $(a,c) = 1$. Using $c = b$ gives $(a, b^2) = 1$ if and only if $(a,b) = 1$. Then a similar argument yields $(a^2, b^2) = 1$ if and only if $(a, b^2) = 1$.

Second Proof: Proposition 1.2.10 shows that $(a,b) = 1$ if and only if a and b have no prime divisors in common. By Euclid's Lemma (1.2.5), this happens if and only if a^2 and b^2 have no prime divisors in common, and this is equivalent to the statement that $(a^2, b^2) = 1$. □

EXERCISES: SECTION 1.2

When proving results in these exercises, we recommend that you first try to use Proposition 1.2.2, Proposition 1.2.3, or Lemma 1.2.5, before trying to use the very powerful fundamental theorem of arithmetic.

1. Find the prime factorizations of each of the following numbers, and use them to compute the greatest common divisor and least common multiple of the given pairs of numbers.

†(a) 35, 14

(b) 15, 11

†(c) 252, 180

(d) 7684, 4148

†(e) 6643, 2873

2. Use the sieve of Eratosthenes to find all prime numbers less than 200.

3.†For each composite number a, with $4 \leq a \leq 20$, find all positive numbers less than a that are relatively prime to a.

4. Find all positive integers less than 60 and relatively prime to 60.
Hint: Use techniques similar to the sieve of Eratosthenes.

5. Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$ be the sequence of prime numbers, and set $a_1 = p_1 + 1$, $a_2 = p_1 p_2 + 1$, $a_3 = p_1 p_2 p_3 + 1, \ldots$. What is the least n such that a_n is composite?

6.†For each of the numbers 9, 15, 20, 24 and 100, give a diagram of all divisors of the number, showing the divisibility relationships. (See Example 1.2.2.)

7. For each of the following numbers, give a diagram of all divisors of the number, showing the divisibility relationships.

(a) 60

(b) 1575

8. Let m and n be positive integers such that $m + n = 57$ and $[m, n] = 680$. Find m and n.

9.†(a) For which $n \in \mathbf{Z}^+$ is $n^3 - 1$ a prime number?

†(b) For which $n \in \mathbf{Z}^+$ is $n^3 + 1$ a prime number?

†(c) For which $n \in \mathbf{Z}^+$ is $n^2 - 1$ a prime number?

†(d) For which $n \in \mathbf{Z}^+$ is $n^2 + 1$ a prime number?

10.†Prove that $n^4 + 4$ is composite if $n > 1$.

11. Prove that $n^4 + 4^n$ is composite if $n > 1$.

12. Let a, b be positive integers, and let $d = (a, b)$. Since $d \mid a$ and $d \mid b$, there exist integers h, k such that $a = dh$ and $b = dk$. Show that $(h, k) = 1$.

13. Let a, b, c be positive integers, and let $d = (a, b)$. Since $d \mid a$, there exists an integer h with $a = dh$. Show that if $a \mid bc$, then $h \mid c$.

14. Show that $a\mathbf{Z} \cap b\mathbf{Z} = [a, b]\mathbf{Z}$.

15. Let a, b be nonzero integers, and let p be a prime. Show that if $p \mid [a, b]$, then either $p \mid a$ or $p \mid b$.

16. Let a, b, c be nonzero integers. Show that $(a, b) = 1$ and $(a, c) = 1$ if and only if $(a, [b, c]) = 1$.

17. Let a, b be nonzero integers. Prove that $(a, b) = 1$ if and only if $(a + b, ab) = 1$.

18.‡Let a, b be nonzero integers with $(a, b) = 1$. Compute $(a + b, a - b)$.

19. Let a and b be positive integers, and let m be an integer such that $ab = m(a, b)$. Without using the prime factorization theorem, prove that $(a, b)[a, b] = ab$ by verifying that m satisfies the necessary properties of $[a, b]$.

20. A positive integer a is called a **square** if $a = n^2$ for some $n \in \mathbf{Z}$. Show that the integer $a > 1$ is a square if and only if every exponent in its prime factorization is even.

21. Show that if the positive integer a is not a square, then $a \neq b^2/c^2$ for integers b, c. Thus any positive integer that is not a square must have an irrational square root. *Hint*: Use Exercise 20 to show that $ac^2 \neq b^2$.

22.‡Show that if a, b are positive integers such that $(a, b) = 1$ and ab is a square, then a and b are also squares.

23. Let p and q be prime numbers. Prove that $pq + 1$ is a square if and only if p and q are twin primes.

24. A positive integer is called **square-free** if it is a product of distinct primes. Prove that every positive integer can be written uniquely as a product of a square and a square-free integer.

25.†For which $n \in \mathbf{Z}^+$ is $n(n + 30)$ a square?

26. Prove that if $a > 1$, then there is a prime p with $a < p \leq a! + 1$.

27. Show that for any $n > 0$, there are n consecutive composite numbers.

28. (a) Show that if 2^k is the highest power of 2 that is a factor of any element of the set $\{1, 2, \ldots, n\}$, then 2^k is the only multiple of 2^k in the set.

(b) Show that $1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ is not an integer for $n \geq 2$.

29. Show that $\log 2 / \log 3$ is not a rational number.

30.‡If a, b, c are positive integers such that $a^2 + b^2 = c^2$, then (a, b, c) is called a **Pythagorean triple**. For example, $(3, 4, 5)$ and $(5, 12, 13)$ are Pythagorean triples. Assume that (a, b, c) is a Pythagorean triple in which the only common divisors of a, b, c are ± 1.

(a) Show that a and b cannot both be odd.

(b) Assume that a is even. Show that there exist relatively prime integers m and n such that $a = 2mn$, $b = m^2 - n^2$, and $c = m^2 + n^2$.
Hint: Factor $a^2 = c^2 - b^2$ after showing that $(c + b, c - b) = 2$.