5. In $\mathbb{Z}$ $a \sim b$ if and only if $a = b$ + some multiple of 3

6. In $\mathbb{R} \times \mathbb{R}$ - $\{(0, 0)\}$, the real plane with the origin removed, $(x_1, y_1) \sim (x_2, y_2)$ if and only if $x_1y_2 = x_2y_1$

7. In $\mathbb{R} \times \mathbb{R}$ $(x_1, y_1) \sim (x_2, y_2)$ if and only if $x_1^2 + y_1^2 = x_2^2 + y_2^2$

8. In $\mathbb{R} \times \mathbb{R}$ $(x_1, y_1) \sim (x_2, y_2)$ if and only if $3y_1 - 5x_1 = 3y_2 - 5x_2$

9. Show that the relation on $\mathbb{R}$ defined in Example 0.2.5 is an equivalence relation.

10. In $\mathbb{R}$ consider the half-open, half-closed intervals $(n, n + 2]$, where n is any even integer. Show that the collection of these intervals is a partition of $\mathbb{R}$, and describe the equivalence relation this partition determines.

11. In the plane $\mathbb{R} \times \mathbb{R}$, explain why defining $(x_1, y_1) \sim (x_2, y_2)$ if and only if $x_1y_2 = x_2y_1$ does not give an equivalence relation.

12. Fix an integer n and define on $\mathbb{Z}$ the relation $a \sim b$ if and only if $a - b$ is divisible by n. Show that this is an equivalence relation on $\mathbb{Z}$ and describe the equivalence classes.

13. Let ϕ: $S \to T$ be any map and define a relation $\sim$ on S by letting $a \sim b$ if and only if $\phi(a) = \phi(b)$. Show that $\sim$ is an equivalence relation on S.

0.3 Properties of $\mathbb{Z}$

In this section we establish some basic properties of the integers, many of which will be important later in identifying examples of various kinds of algebraic structures, where $\mathbb{Z}$ will play the role of a basic model. We begin with properties of the usual order relation on $\mathbb{Z}$ and then turn to properties involving the familiar operations of addition, subtraction, multiplication, and division. Finally, we introduce new algebraic structures closely related to the integers, called the *integers mod n*, for any integer $n > 1$.

Induction

Many proofs and constructions are based on the following fundamental property of the positive integers.

0.3.1 AXIOM (Well-ordering principle) Every nonempty set of positive integers contains a least element. ☆

Frequently in proving some theorem or constructing some structure we will want to pick the least element from some given nonempty set of positive integers. The well-ordering principle tells us such a least element always exists.
Closely related to the well-ordering principle is another principle, mathematical induction, that is equally important in proofs and constructions. We use the well-ordering principle to prove the principle of mathematical induction.

0.3.2 THEOREM (Principle of mathematical induction) Let $P(n)$ be a statement about a positive integer n such that

(1) $P(1)$ is true.

(2) If $P(k)$ is true, then $P(k + 1)$ is true.

Then $P(n)$ is true for all positive integers n.

Proof The proof will be by contradiction. Suppose there exists a positive integer n for which $P(n)$ is not true. Then the set S of all positive integers n for which $P(n)$ is not true is nonempty. By the well-ordering principle, S must have a least element m. By assumption (1), this least element cannot be 1, since $P(1)$ is true. So $m - 1$ is still positive. Since $m - 1 < m$, and m was the least positive integer for which the statement was not true, $P(m - 1)$ is true. So by assumption (2), $P((m - 1) + 1)$ is true, which is to say $P(m)$ is true. This is a contradiction, which shows that our original supposition that $P(n)$ was not true for some positive integers n is false. □

It is impossible to overemphasize the usefulness of mathematical induction. We next use it in a variety of examples to show something of the diversity of problems to which it can be applied.

0.3.3 EXAMPLE Let us prove that for any positive integer n the sum of the first n odd numbers is the square of n, or $1 + 3 + 5 + \ldots + (2n - 1) = n^2$. As in all proofs by mathematical induction, we begin with the base step, proving the statement for 1. In this case the statement for 1 is just $1 = 1^2$, which is clear. Next we do the induction step, making the assumption, called the *induction hypothesis*, that the statement holds for k, and using this assumption to prove that the statement holds for $k + 1$. So what we are assuming is that $1 + 3 + 5 + \ldots + (2k - 1) = k^2$, and what we want to prove is that $1 + 3 + 5 + \ldots + (2k - 1) + (2(k + 1) - 1) = (k+1)^2$. What our assumption tells us is that $1 + 3 + 5 + \ldots + (2k - 1) + (2(k + 1) - 1) = k^2 + (2(k + 1) - 1)$, and we easily see that $k^2 + (2(k + 1) - 1) = k^2 + 2k + 1 = (k+1)^2$, as required to complete the proof. ◇

0.3.4 EXAMPLE Let us prove that for any $n \geq 0$, a set S with n elements has exactly 2^n subsets. First let us dispose of the case $n = 0$. In this case the only set with n elements is the empty set $\varnothing$, and this has only one subset, itself, while $2^0 = 1$, so the statement is true in this case. Now consider the case $n = 1$. In this case a set $S = \{a\}$ with one element has just two subsets, $S = \{a\}$ and $\varnothing$, while $2^1 = 2$, so the statement is true in this case also. Now for the induction step. We assume that every set with k elements has 2^k subsets and want to prove that every set with $k + 1$ elements has 2^{k+1}

subsets. So let S be any set with $k + 1$ elements. Let a be any element of S, and consider the set $T = S - \{a\}$ consisting of S with a removed. T is a set with k elements, and so has 2^k subsets by assumption. The subsets of S that do not contain a are just the subsets of T. Therefore S has 2^k such subsets. Any subset of S that *does* contain a consists of a subset that does not, with a added to it. So there are again 2^k such subsets. Then, S has $2^k + 2^k = 2^{k+1}$ subsets, as required to complete the proof. ◇

0.3.5 EXAMPLE Let us prove that for any real numbers a, b and any integer $n \geq 1$ we have $a^{n+1} - b^{n+1} = (a - b)(a^n + a^{n-1}b + \ldots + ab^{n-1} + b^n)$. For the base step $n = 1$ the statement is just $a^2 - b^2 = (a - b)(a + b)$, which is clear. For the induction step, assume $a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \ldots + ab^{k-2} + b^{k-1})$. We then have

$$(a - b)(a^k + a^{k-1}b + \ldots + ab^{k-1} + b^k) =$$
$$(a - b)[a(a^{k-1} + a^{k-2}b + \ldots + ab^{k-2} + b^{k-1}) + b^k) =$$
$$a(a - b)(a^{k-1} + a^{k-2}b + \ldots + ab^{k-2} + b^{k-1}) + (a - b)b^k =$$
$$a(a^k - b^k) + (a - b)b^k = a^{k+1} - ab^k + ab^k - b^{k+1} = a^{k+1} - b^{k+1}$$

as required to complete the proof. ◇

Often it is convenient to use a slightly different strong version of mathematical induction, which is actually equivalent to the ordinary version used in the preceding examples. (See Exercise 11 at the end of this section.) The difference between this version and the original version of the principle is that the induction hypothesis is stronger. We do not just assume the statement we are interested in holds for $m - 1$ in order to prove it for m. Instead, we assume the statement holds for *all* $1 \leq k < m$.

0.3.6 THEOREM (Strong induction) Let $P(n)$ be a statement about a positive integer n such that

(1) $P(1)$ is true.

(2) If $P(k)$ is true for all k, $1 \leq k < m$, then $P(m)$ is true.

Then $P(n)$ is true for all positive integers n.

Proof Let $Q(n)$ be the statement that $P(k)$ holds for all $1 \leq k \leq n$. We prove that $Q(n)$ holds for all positive integers n by ordinary mathematical induction (as in Theorem 0.3.2). Since $Q(n)$ implies $P(n)$, this implies that $P(n)$ holds for all positive integers n. For the base step, $Q(1)$ just amounts to $P(1)$ and is true by assumption (1). For the induction step, we assume $Q(m)$ holds and prove that $Q(m + 1)$ holds. Here $Q(m + 1)$ is the statement that $P(k)$ holds for all $1 \leq k \leq m + 1$. For $1 \leq k \leq m$, $P(k)$ follows from $Q(m)$. For $k = m + 1$, $P(m + 1)$ then follows by assumption (2), as required to complete the proof. □

Suppose that in Theorem 0.3.6 instead of (1) and (2), we assume for some positive integer n_0:

(1') $P(n_0)$ is true.

(2') If $P(k)$ is true for all k, $n_0 \leq k < m$, then $P(m)$ is true.

Then it follows that $P(n)$ is true for all $n \geq n_0$. (See Exercise 10 at the end of this section.)
Our next result is important not only as an illustration of proof by induction, but for its own sake.

0.3.7 EXAMPLE Given two real numbers a, b, by multiplying out we can obtain the following formulas for the first few powers of $a + b$:
$(a + b)^2 = a^2 + 2ab + b^2$
$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$
$(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$
It does become cumbersome after a while to calculate all these powers! ◇

0.3.8 THEOREM (Binomial theorem) Given any real numbers a, b, then for any integer $n \geq 1$ we have

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-2}a^2b^{n-2} + \binom{n}{n-1}ab^{n-1} + b^n$$

where the **binomial coefficients** are given by

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

for $0 \leq r \leq n$.

Proof For $n = 1$ the statement is just $(a + b)^1 = a^1 + b^1$, which is true. Assume the statement holds for k. We then have

$$(a + b)^{k+1} = (a + b)(a + b)^k =$$

$$(a+b)\left[\, a^k + \binom{k}{1}a^{k-1}b + \binom{k}{2}a^{k-2}b^2 + \ldots + \binom{k}{k-2}a^2b^{k-2} + \binom{k}{k-1}ab^{k-1} + b^k \,\right] =$$

$$a^{k+1} + \binom{k}{1}a^kb + \binom{k}{2}a^{k-1}b^2 + \ldots + \binom{k}{k-2}a^3b^{k-2} + \binom{k}{k-1}a^2b^{k-1} + ab^k +$$
$$+ a^kb + \binom{k}{1}a^{k-1}b^2 + \binom{k}{2}a^{k-2}b^3 + \ldots + \binom{k}{k-2}a^2b^{k-1} + \binom{k}{k-1}ab^k + b^{k+1} =$$

$$a^{k+1} + \left[\binom{k}{1} + 1\right]a^kb + \left[\binom{k}{2} + \binom{k}{1}\right]a^{k-1}b^2 + \ldots + \left[\binom{k}{r} + \binom{k}{r-1}\right]a^{k-r+1}b^r + \ldots + b^{k+1}$$

To complete the proof that $(a + b)^{k+1} =$

$$a^{k+1} + \binom{k+1}{1}a^kb + \binom{k+1}{2}a^{k-1}b^2 + \ldots + \binom{k+1}{k-1}a^2b^{k-1} + \binom{k+1}{k}ab^k + b^{k+1}$$

it will suffice to prove the following claim.
Claim (Pascal's identity)

$$\binom{k}{r} + \binom{k}{r-1} = \binom{k+1}{r}$$

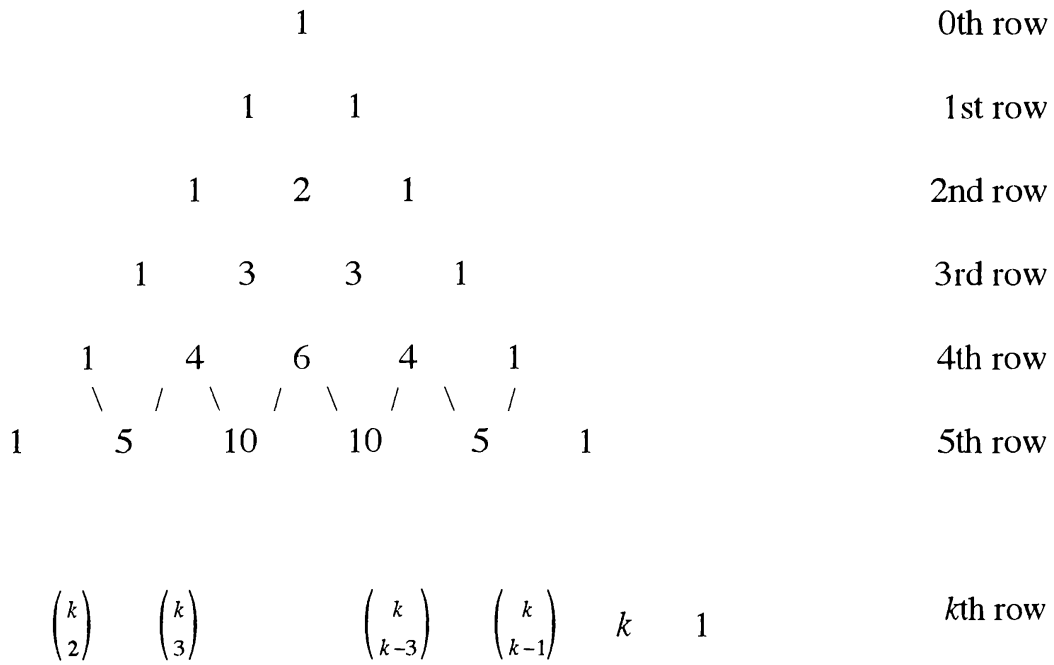
Proof of claim We have

$$\binom{k}{r} + \binom{k}{r-1} = \frac{k!}{r!(k-r)!} + \frac{k!}{(r-1)!(k-r+1)!} =$$

$$\frac{k!(k-r+1)+rk!}{r!(k-r+1)!} = \frac{(k+1)!}{r!(k-r+1)!} = \binom{k+1}{r}$$

to complete the proof. □

0.3.9 EXAMPLE (Pascal's triangle)
Pascal's identity (the claim in the preceding proof) underlies the construction of the well-known **Pascal's triangle**:



As the lines indicate in the case of the 5th row, each entry in a row, except for the two 1s on the outside, is the sum of the two adjacent entries above it in the preceding row. ◇

Division Algorithm

We have all been familiar since elementary school with the process of division, by which a given integer a can always be represented as the sum of a multiple of another given integer $b \geq 1$ plus a remainder that is less than b. We see in the next theorem that the well-ordering principle guarantees the possibility of carrying out this process.

0.3.10 EXAMPLE We indicate the result of the process of division in the case of a few pairs of integers.
For 84 and 60 we have $84 = 1 \cdot 60 + 24$
For 924 and 105 we have $924 = 8 \cdot 105 + 84$
For -10 and 3 we have $-10 = (-4) \cdot 3 + 2$
In each case the first number is the sum of a multiple of the second number plus a nonnegative integer that is less than the second number. ◇

0.3.11 THEOREM (Division algorithm) Let a be any integer and b any integer with $b \geq 1$. Then there exist unique integers q and r such that
(1) $a = qb + r$
(2) $0 \leq r < b$

Proof Let $S = \{a - kb \mid k \in \mathbb{Z} \text{ and } a - kb \geq 0\}$. If $a \geq 0$, then $a - 0 \cdot b \in S$. If $a < 0$, then $a - 2ab \in S$. So in either case S is nonempty. By the well-ordering principle S has a least element r. Since $r \in S$, we have $r = a - qb$ or, equivalently, $a = qb + r$ for some integer q, and we have $r \geq 0$. It remains to show that $r < b$. But if we had $r \geq b$, then we would have $0 \leq r - b = a - (q + 1)b$ and therefore $a - (q + 1)b \in S$ while $a - (q + 1)b < r$, contrary to the choice of r as the *least* element of S. Thus the existence of a pair of integers q, r satisfying conditions (1) and (2) is proved.
Now let us prove uniqueness. Suppose we have another pair of integers q', r' also satisfying conditions (1) and (2). Let us assume $r \leq r'$. (The proof is similar on the opposite assumption.) We have $a = qb + r = q'b + r'$, from which we derive $0 \leq (q - q')b = r' - r < b$. Thus $(q - q')b$ is a nonnegative integer, a multiple of b, and less than b, which is only possible if $q - q' = 0$. Thus we have $q = q'$ and hence also $r = a - qb = a - q'b = r'$. □

The numbers q and r in Theorem 0.3.11 are called the **quotient** and **remainder** on dividing a by b.

0.3.12 DEFINITION Given two integers a and d, we say d is a **divisor** of a, written $d \mid a$, if $a = qd$ for some integer q. Note that we may have $d \leq 0$ in this definition. ○

0.3.13 DEFINITION Given two integers a and b, an integer d such that $d \mid a$ and $d \mid b$ is called a **common divisor** of a and b. ○

0.3.14 EXAMPLE 252 and 180 have the common positive divisors 1, 2, 3, 4, 6, 9, 12, 18, and 36. There is no common positive divisor larger than 36. ◇

We will often be interested in finding the largest among the common divisors of two integers.

0.3.15 DEFINITION Given two integers a and b, not both zero, the **greatest common divisor** of a and b is an integer $d \geq 1$ such that
(1) $d \mid a$ and $d \mid b$
(2) For any integer k, if $k \mid a$ and $k \mid b$, then $k \mid d$.
In this case we write $d = \gcd(a, b)$. ○

The division algorithm, with another application of the well-ordering principle, guarantees the existence of gcd(a, b), as shown in the next theorem.

0.3.16 THEOREM Let a and b be integers not both zero. Then
(1) $d = \gcd(a,b)$ exists.
(2) There exist integers u and v such that $d = ua + vb$.

Proof Let $S = \{xa + yb \mid x, y \in \mathbb{Z} \text{ and } xa + yb \geq 1\}$. S is nonempty since $aa + bb \in S$. The well-ordering principle implies S has a least element d. Since $d \in S$ we have $d = sa + tb$ for some $s, t \in \mathbb{Z}$, and $d \geq 1$. If k is a common divisor of a and b, we have $a = uk$ and $b = vk$ for some $u, v \in \mathbb{Z}$, and so $d = sa + tb = (su + tv)k$ and k is a divisor of d. Finally, to show $d = \gcd(a, b)$ it remains to show that d is a common divisor of a and b. Applying the division algorithm, we have $a = qd + r$, where $0 \leq r < d$. Hence $0 \leq r = a - qd = a - q(sa + tb) = (1 - qs)a + (-qt)b$. Since d was the least element of S, we cannot have $r \geq 1$, and so must have $r = 0$, so that $a = qd$ and d is a divisor of a. The proof that d is a divisor of b is exactly the same. □

Theorem 0.3.16, part (1), guarantees the existence of gcd(a,b). Theorem 0.3.16, part (2), which says that gcd(a,b) can be expressed as a **linear combination** $ua + vb$ of a and b, may at first glance appear less interesting, but in fact turns out to be extremely useful.

0.3.17 EXAMPLE Let us illustrate how to calculate the greatest common divisor in a simple case. We find gcd(84,60) by repeatedly applying the division algorithm, as follows:

$$84 = 1 \cdot 60 + 24$$
$$60 = 2 \cdot 24 + 12$$
$$24 = 2 \cdot 12 + 0$$

From the third equation we know that 12|12 and 12|24. Hence the second equation implies that 12|60. And since 12|24 and 12|60, the first equation implies 12|84. So 12 is a common divisor of 84 and 60. If d' is any other common divisor of 84 and 60, we see from the first equation that $d' | 24$. Since $d' | 60$ and $d' | 24$, we see from the second equation that $d' | 12$. Therefore, $12 = \gcd(84, 60)$. ◇

0.3.18 PROPOSITION For any pair of integers a and $b \geq 1$ we can calculate gcd(a,b) by repeated application of the division algorithm, as follows:

$$a = q_1 b + r_1 \qquad \text{where } 0 \leq r_1 < b$$
$$b = q_2 r_1 + r_2 \qquad \text{where } 0 \leq r_2 < r_1$$
$$r_1 = q_3 r_2 + r_3 \qquad \text{where } 0 \leq r_3 < r_2$$
$$\vdots$$

stopping when we obtain a remainder of zero:

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \qquad \text{where } 0 \leq r_{n-1} < r_{n-2}$$
$$r_{n-2} = q_n r_{n-1} + r_n \qquad \text{where } 0 \leq r_n < r_{n-1}$$
$$r_{n-1} = q_{n+1} r_n + 0$$

The last nonzero remainder $r_n = \gcd(a, b)$. This method of calculating the $\gcd(a, b)$ is called the **Euclidean algorithm**.

Proof That we must eventually come to a remainder of zero follows from the well-ordering principle, which implies that the set of positive remainders must have a least element. Since the sequence of remainders $b > r_1 > r_2 > r_3 > \ldots$ is strictly decreasing, the least positive remainder must be the *last* positive remainder, after which the next remainder must be zero. It follows as in the preceding example that if r_n is this last positive remainder, then $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{i-1}, r_i) = \ldots = \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) = r_n$. □

0.3.19 EXAMPLE Let us calculate the gcd(924,105).

$$924 = 8 \cdot 105 + 84$$
$$105 = 1 \cdot 84 + 21$$
$$84 = 4 \cdot 21 + 0$$

So gcd(924, 105) = 21. From the second equation we obtain 21 = 105 - 84. From the first equation we obtain 84 = 924 - 8 · 105. Combining, we get 21 = 105 - (924 - 8 · 105) = -924 + 9 · 105, and we have found a way of expressing the gcd(924, 105) as a linear combination $u924 + v105$. ◇

Fundamental Theorem of Arithmetic

Another important consequence of the division algorithm and the well-ordering principle is that every integer $n > 1$ can be written as a product of primes, numbers that cannot themselves be written as products in a nontrivial way.

0.3.20 EXAMPLE Let us calculate the gcd(385, 48).

$$385 = 8 \cdot 48 + 1$$
$$48 = 48 \cdot 1 + 0$$

So gcd(385, 48) = 1, or in other words, 1 is the largest, and therefore the only, positive integer that divides both 385 and 48. ◇

0.3.21 DEFINITION Two integers a and b are said to be **relatively prime** if $\gcd(a, b) = 1$, or in other words, if their only positive common divisor is 1. An integer $p > 1$ is said to be **prime** if its only positive divisors are 1 and p itself. ○

The next proposition is one of the important consequences of Theorem 0.3.16, part (2), as we will see in the proof of Theorem 0.3.26.

0.3.22 PROPOSITION Let a and b be relatively prime and c an integer. Then

(1) Any common divisor of a and bc is a common divisor of a and c.

(2) If a divides bc, then a divides c.

(3) If a and c are relatively prime, then a and bc are relatively prime.

Proof (1) Let $\gcd(a, b) = 1$ and let $d|a$ and $d|bc$. Then $1 = sa + tb$ for some integers s, t, by Theorem 0.3.16, and $a = dx$ and $bc = dy$ for some integers x and y. We then have

$$c = c \cdot 1 = c(sa + tb) = acs + bct = dxcs + dyt = d(xcs + yt)$$

and so $d|c$ as required to prove (1). Then (2) and (3) are immediate from (1). □

An immediate consequence is the following important corollary.

0.3.23 COROLLARY (Euclid's lemma) Let b and c be integers. If p is prime and $p|bc$, then $p|b$ or $p|c$.

Proof If we have $p|b$, there is nothing to prove. If we do not have $p|b$, then we must have $\gcd(p, b) = 1$, because 1 is the only positive divisor of p besides p itself. Therefore, we have $p|c$ by the preceding proposition. □

0.3.24 EXAMPLE It is very important in Euclid's lemma that p is a prime. Consider 6, which divides $3 \cdot 4 = 12$. We have neither $6|3$ nor $6|4$.

For the proof of the fundamental theorem of arithmetic we need Euclid's lemma in a more general form, provided by the next corollary.

0.3.25 COROLLARY Let $b_1, b_2, \ldots, b_r$ be integers. If p is a prime and $p|b_1b_2\ldots b_r$, then $p|b_i$ for some i with $1 \le i \le r$.

Proof We use induction on r. For $r = 1$ there is nothing to prove. The case $r = 2$ is Corollary 0.3.23. So assume the statement is true for $r = k$ and suppose $p|(b_1b_2\ldots b_k)b_{k+1}$. By Corollary 0.3.23, either $p|b_{k+1}$, in which case we are done, or $p|b_1b_2\ldots b_k$, in which case by our induction hypothesis $p|b_i$ for some i, $1 \le i \le k$. □

0.3.26 THEOREM (Fundamental theorem of arithmetic) Let n be an integer, $n > 1$. Then

(1) n is either a prime or a product of primes.

(2) The factorization of n into a product of primes is unique except for the order of the primes. That is, if

$$n = p_1p_2\ldots p_r \text{ and } n = q_1q_2\ldots q_s$$

where the p_i and q_j are primes, then $r = s$ and by reordering the q_j we can obtain $p_i = q_i$ for all i.

Proof For both statements (1) and (2) we use strong induction (Theorem 0.3.6 and Exercise 10) to prove that the statement holds for all $n \ge 2$.

(1) (Existence of the prime factorization of n) For $n = 2$, statement (1) is immediate, since 2 is itself a prime. So assume (1) holds for any integer k, $2 \le k < n$, to prove (1) holds for n. If n is a prime, we are done. If n is not a prime, there are integers u and v, $1 < u, v < n$ such that $u \cdot v = n$. By our induction hypothesis, each of

u, v is either a prime or can be written as a product of primes, and it follows that $n = uv$ can be written as a product of primes.

(2) (Uniqueness of the prime factorization of n) For $n = 2$, statement (2) is immediate, since the prime 2 cannot be written as a product of other primes because any other prime is greater than 2. So assume (2) holds for any integer k, $2 \le k < n$, to prove (2) holds for n. Suppose

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

Then since $p_1 | n$ we have $p_1 | q_1 q_2 \dots q_s$. By Corollary 0.3.25 $p_1 | q_i$ for some i, $1 \le i \le s$. We may reorder the q_j so that this q_i becomes q_1, and we have $p_1 | q_1$ and since q_1 is prime, we obtain $p_1 = q_1$. Now consider $k = n/p_1 = n/q_1 < n$. We have

$$k = p_2 \dots p_r = q_2 \dots q_s$$

By our induction hypothesis, the number of primes in each factorization must be the same. That is, $r - 1 = s - 1$, implying $r = s$. Also, the p_i, $2 \le i \le r$ and q_j, $2 \le j \le r$ must be the same except for order, completing the proof. □

The fundamental theorem of arithmetic we have just proved implies that given any integer $n > 1$, we can write n as a product $p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, where the p_i are distinct primes, and that these primes p_i, and their exponents a_i, are unique. When numbers are written this way, it is easy to find their greatest common divisor, as the next example illustrates.

0.3.27 EXAMPLE Consider the integers 924 and 105 from Example 0.3.19. In that example we found gcd(924, 105) = 21. We have

$$924 = 2^2 \cdot 3^1 \cdot 7^1 \cdot 11^1 \qquad 105 = 3^1 \cdot 5^1 \cdot 7^1 \qquad 21 = 3^1 \cdot 7^1$$

For purposes of comparison, we can write

$$924 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^1 \qquad 105 = 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^0$$

$$21 = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^0$$

We see that the exponent on a prime in the factorization of 21 is whichever is less of the exponents on that same prime in the factorizations of 924 and 105. Suppose that instead we take whichever exponent is greater. Then we get the number

$$2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^1 = 4620$$

Whereas 21 is the greatest integer that divides both the given numbers, 4620 is the least positive integer that both the given numbers divide. ◇.

0.3.28 DEFINITION Given two integers n and m, not both 0, the **least common multiple** of a and b is an integer $l \ge 1$such that

(1) $n | l$ and $m | l$

(2) For any integer k, if $n | k$ and $m | k$, then $l | k$.

In this case we write $l = \text{lcm}(n, m)$. ○

0.3.29 PROPOSITION Given

$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ and $m = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$

where the p_i are distinct primes and a_i, $b_i \ge 0$, we have

(1) $\gcd(n, m) = p_1^{c_1}p_2^{c_2}\ldots p_k^{c_k}$, where $c_i = \min(a_i, b_i)$

(2) $\text{lcm}(n, m) = p_1^{d_1}p_2^{d_2}\ldots p_k^{d_k}$, where $d_i = \max(a_i, b_i)$

(3) $\text{lcm}(n, m) \cdot \gcd(n, m) = nm$

Proof See Exercises 19 through 21 at the end of this section. □

Integers mod *n*

We end this section by returning to the topic of equivalence relations. We examine one particular equivalence relation on $\mathbb{Z}$ that was mentioned in the preceding section.

0.3.30 DEFINITION Let $n > 0$ be a fixed positive integer. For any two integers a and b we say a and b are **congruent mod** n, and write $a \equiv b \bmod n$ if $n|(a - b)$. ○

0.3.31 PROPOSITION

(1) The relation of congruence mod n is an equivalence relation on $\mathbb{Z}$.

(2) This equivalence relation has exactly n equivalence classes:

$$n\mathbb{Z},\ 1 + n\mathbb{Z},\ 2 + n\mathbb{Z},\ \ldots,\ (n - 1) + n\mathbb{Z}$$

(3) If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then

$$a + c \equiv b + d \bmod n \qquad ac \equiv bd \bmod n$$

(4) If a and n are relatively prime, then

$$ab \equiv ac \bmod n \text{ implies } b \equiv c \bmod n$$

Proof (1) For all $a, b, c \in \mathbb{Z}$ we have the following. First, $a \equiv a$ since $n|(a - a) = 0$. Second, if $a \equiv b$, then $n|(a - b) = -(b - a)$, so $n|(b - a)$ and $b \equiv a$. Third, if $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $n|(a - b)$ and $n|(a - c)$ and so $n|((a - b) + (b - c)) = (a - c)$, and $a \equiv c \bmod n$.

(2) For any $a \in \mathbb{Z}$, let $[a]$ denote the equivalence class of $a \in \mathbb{Z}$. By the division algorithm we have $a = qn + r$ for some $q, r \in \mathbb{Z}$ with $0 \le r < n$. It follows that $a \equiv r$ and so $[a] = [r]$. So there are only the n equivalence classes

$$[0] = n\mathbb{Z},\ [1] = 1 + n\mathbb{Z},\ \ldots,\ [n - 1] = (n - 1) + n\mathbb{Z}$$

These are all distinct since for r, s with $0 \le r, s < n$ we have $n|(r - s)$ if and only if $r = s$.

(3) If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $n|(a - b)$ and $n|(c - d)$, hence

$$n|((a - b) + (c - d)) = (a + c) - (b + d)$$

and $a + c \equiv b + d \bmod n$. Likewise

$$n|((a - b)c + (c - d)b = ac - bd$$

and $ac \equiv bd \bmod n$.

(4) If a and n are relatively prime and $ab \equiv ac \bmod n$, then

$$n|(ab - ac) = a(b - c)$$

and by Proposition 0.3.22 we have $n|(b - c)$ and $b \equiv c \bmod n$. □

0.3.32 EXAMPLE Let $\mathbb{Z}_5$ be the set consisting of the five equivalence classes of congruence mod 5. So $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$. Proposition 0.3.31 guarantees that if $[r_1] = [r_2]$ and $[s_1] = [s_2]$, then $[r_1 + s_1] = [r_2 + s_2]$. So we can define unambiguously an addition operation on equivalence classes by setting $[r] + [s] = [r + s]$. Similarly, $[r_1 s_1] = [r_2 s_2]$ and we can define unambiguously a multiplication operation on equivalence classes by setting $[r] \cdot [s] = [rs]$. The tables for these operations are as follows.

TABLE 1 Addition mod 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

TABLE 2 Multiplication mod 5

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

In the tables we have omitted the brackets, as is often done. ◇

0.3.33 DEFINITION For any $n > 0$, let $\mathbb{Z}_n = \{[0], [1], \ldots, [n - 1]\}$, the set of equivalence classes of congruence mod n. Just as in the preceding example, Proposition 0.3.31 guarantees that the operations $[r] + [s] = [r + s]$ and $[r][s] = [rs]$ of **addition and multiplication mod** n are well defined in $\mathbb{Z}_n$, since if $[r_1] = [r_2]$ and $[s_1] = [s_2]$ in $\mathbb{Z}_n$, then

$$[r_1] + [s_1] = [r_1 + s_1] = [r_2 + s_2] = [r_2] + [s_2]$$
$$[r_1][s_1] = [r_1 s_1] = [r_2 s_2] = [r_2][s_2]$$

$\mathbb{Z}_n$ with these operations is called the **integers mod** n. ○.

The next proposition collects some basic properties of addition and multiplication in the integers mod n.

0.3.34 PROPOSITION For any $[r]$, $[s]$, and $[t]$ in $\mathbb{Z}_n$ we have

(1) **Commutative laws**

$[r] + [s] = [s] + [r]$ $\qquad$ $[r][s] = [s][r]$

(2) **Associative laws**

$[r] + ([s] + [t]) = ([r] + [s]) + [t]$ $\qquad$ $[r]([s][t]) = ([r][s])[t]$

(3) **Distributitivite law**

$[r]([s] + [t]) = [r][s] + [r][[t]$

(4) **Identity laws**

$[0] + [r] = [r] = [r] + [0]$ $\qquad$ $[1][r] = [r] = [r][1]$

Proof Left to the reader (as Exercises 27 through 30 at the end of this section) □

0.3.35 EXAMPLE In $\mathbb{Z}_{10} = \{[0], [1], \ldots, [9]\}$ consider the subset $U(10) = \{[1], [3], [7], [9]\}$ that consists of those equivalence classes [s] mod 10, $1 \leq s \leq 9$, such that $\gcd(10, s) = 1$. Let us work out the multiplication table mod 10 for $U(10)$.

TABLE 3 Multiplication in $U(10)$

·	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Calculating the table, we find that if $[r], [s] \in U(10)$, then $[r][s] \in U(10)$. The reason why will be seen in the next proposition. We also find that for any $[r] \in U(10)$ there is an $[s] \in U(10)$ such that $[r][s] = 1$. The reason is that if $\gcd(r,10) = 1$, then it follows from Theorem 0.3.16 that $rs + 10t = 1$ for some integers s and t, from which it follows that $rs \equiv 1 \bmod 10$ and $[r][s] = [1]$. ◇

0.3.36 DEFINITION In $\mathbb{Z}_n$ let $U(n)$ be the set of all equivalence classes $[s]$ mod n with $1 \leq s < n$ and $\gcd(n,s) = 1$. The elements of $U(n)$ are called the **units mod** n. ○

0.3.37 PROPOSITION For any $[r], [s] \in U(n)$ we have $[r][s] = [rs] \in U(n)$

Proof If $[r], [s] \in U(n)$ then we have $\gcd(n, s) = \gcd(n, r) = 1$. By Proposition 0.3.22, part (3), it follows that $\gcd(n, rs) = 1$, and hence $[rs] \in U(n)$. □

0.3.38 PROPOSITION For any $[r] \in U(n)$ there is an $[s] \in U(n)$ such that $[r][s] = [1]$.

Proof Left to the reader (as Exercise 33 at the end of this section). □

Exercises 0.3

In Exercises 1 through 5 prove the statements by induction on n.

1. $1 + 2 + 3 + \ldots + n = n(n + 1)/2$ $\quad n \geq 1$

2. $1^2 + 2^2 + 3^2 + \ldots + n^2 = n(n + 1)(2n + 1)/6$ $\quad n \geq 1$

3. $1^3 + 2^3 + 3^3 + \ldots + n^3 = n^2(n + 1)^2/4$ $\quad n \geq 1$

4. If $0 \leq x \leq y$, then $x^n \leq y^n$ $\quad n \geq 0$

5. $n < 2^n$ $\quad n \geq 0$