# 20

# *The Integers*

**Number theory** IS CONCERNED with the integers and their properties. In this chapter the rules of the arithmetic of integers are reviewed. The surprising fact is that all the dozens of rules and tricks you know for working with integers (and for doing algebra, which is just arithmetic with symbols) are consequences of just a few basic facts. The list of facts given in sections 20.1 and 20.2 is actually longer than necessary; several of these rules can be derived from the others.

## *20.1 Integer operations*

The set of **integers**, $\{\cdots, -2, -1, 0, 1, 2, \cdots\}$, is denoted by the symbol $\mathbb{Z}$. The two familiar arithmetic operations for the integers, addition and multiplication, obey several basic rules. First, notice that addition and multiplication are **binary operations**. In other words, these two operations combine a pair of integers to produce a value. It is not possible to add (or multiply) three numbers at a time. We can figure out the sum of three numbers, but it takes two steps: we select two of the numbers, and add them up, and then add the third to the preliminary total. Never are more than two numbers added together at any time. A list of the seven fundamental facts about addition and multiplication of integers follows.

(1) The integers are **closed** with respect to addition and multiplication.

That means that when two integers are added or multiplied, the result is another integer. In symbols, we have

$$\forall a, b \in \mathbb{Z},\ ab \in \mathbb{Z} \text{ and } a + b \in \mathbb{Z}.$$

(2) Addition and multiplication of integers are **commutative** operations.

That means that the *order* in which the two numbers are combined has no effect on the final total. Symbolically, we have

$$\forall a, b \in \mathbb{Z},\ a + b = b + a \text{ and } ab = ba.$$

(3) Addition and multiplication of integers are **associative** operations. In other words, when we compute the sum (or product) of three integers, it does not matter whether we combine the first two and then add the third to the total, or add the first to the total of the last two. The final total will be the same in either case. Expressed in symbols, we have

$$\forall a, b, c \in \mathbb{Z},\ a(bc) = (ab)c \text{ and } a + (b + c) = (a + b) + c.$$

(4) There is an **additive identity** denoted by 0. It has the property that when it is added to any number the result is that number right back again. In symbols, we see that

$$0 + a = a = a + 0 \text{ for all } a \in \mathbb{Z}.$$

(5) Every integer has an **additive inverse**: $\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z}$ so that $n + m = 0 = m + n$. As usual, $m$ is denoted by $-n$. So, we write $n + (-n) = (-n) + n = 0$.

(6) 1 is a **multiplicative identity**. That is, we have $1a = a = a1$ for all $a \in \mathbb{Z}$.

And finally, there is a rule which establishes a connection between the operations of addition and multiplication.

(7) Multiplication **distributes** over addition. Again, we symbolically write

$$\forall a, b, c \in \mathbb{Z},\ a(b+c) = ab + ac.$$

The seven facts in section 20.1, together with a few concerning ordering stated in section 20.2, tell all there is to know about arithmetic. Every other fact can be proved from these. For example, here is a proof of the cancellation law for addition using the facts listed above.

**Theorem 20.1** (Integer cancellation law)**.** *For integers $a, b, c$, if $a + c = b + c$ then $a = b$.*

**Proof.** *Suppose $a + c = b + c$. Add $-c$ to both sides of that equation (applying fact 5 above) to get $(a + c) + (-c) = (b + c) + (-c)$. Using the associative rule, that equation can be rewritten as $a + (c + (-c)) = b + (c + (-c))$, and that becomes $a + 0 = b + 0$. By property 4 above, that means $a = b$.* ♣

**Theorem 20.2.** *For any integer $a$, $a0 = 0$.*

**Proof.** *Here are the steps in the proof. You supply the justifications for the steps.*

$$\begin{aligned} a0 &= a(0+0) \\ a0 &= a0 + a0 \\ a0 + (-(a0)) &= (a0 + a0) + (-(a0)) \\ a0 + (-(a0)) &= a0 + (a0 + (-(a0))) \\ 0 &= a0 + 0 \\ 0 &= a0 \end{aligned}$$

♣

Your justification for each step should be stated as using one, or more, of the fundamental facts as applied to the specific circumstance in each line.

## 20.2 *Order properties*

The integers also have an order relation, *a is less than or equal to b*: $a \leq b$. This relation satisfies three fundamental order properties: $\leq$ is a reflexive, antisymmetric, and transitive relation on $\mathbb{Z}$.

The notation $b \geq a$ means the same as $a \leq b$. Also $a < b$ (and $b > a$) are shorthand ways to say $a \leq b$ and $a \neq b$.

The **trichotomy law** holds: for $a \in \mathbb{Z}$ exactly one of $a > 0, a = 0$, or $a < 0$ is true.

The ordering of the integers is related to the arithmetic by several rules:

(1) If $a < b$, then $a + c < b + c$ for all $c \in \mathbb{Z}$.

(2) If $a < b$ and $c > 0$, then $ac < bc$.

(3) If $a < b$ and $c < 0$, then $bc < ac$.

And, finally, the rule that justifies proofs by induction:

The Well Ordering Principle for $\mathbb{Z}$: The set of positive integers is **well-ordered**: every nonempty subset of positive integers has a least element.

## 20.3 Exercises

**Exercise 20.1.** *Prove that if $a > 0$ and $b > 0$, then $ab > 0$.*

**Exercise 20.2.** *Prove that if $ab = 0$, then $a = 0$ or $b = 0$. Hint: Try an indirect proof with four cases. Case 1: Show that if $a > 0$ and $b > 0$, then $ab \neq 0$. Case 2: Show that if $a > 0$ and $b < 0$, then $ab \neq 0$. There are two more similar cases. (This fact is called the zero property.)*

**Exercise 20.3.** *Prove the cancellation law for multiplication: For integers $a, b, c$, with $c \neq 0$, if $ac = bc$, then $a = b$. (Hint: Use exercise 20.2)*

## 20.4 Problems

**Problem 20.1.** *Prove that if $a > 0$ and $b < 0$, then $ab < 0$.*

**Problem 20.2.** *Prove that if $n$ is an integer, then $n^2 \geq 0$.*

**Problem 20.3.** *Prove that is $m^2 = n^2$, then $m = n$ or $m = -n$.*
*(Hint from algebra: $a^2 - b^2 = (a + b)(a - b)$.)*

# 21

# *The divides Relation and Primes*

Given integers $a$ and $b$ we say that $a$ **divides** $b$ and write $a|b$ provided[1] there is an integer $c$ with $b = ac$. In that case we also say that $a$ is a **factor** of $b$, or that $a$ is a **divisor** of $b$, or that $b$ is a **multiple** of $a$. For example $3|12$ since $12 = 3 \cdot 4$. Keep in mind that *divides* is a relation. When you see $a|b$ you should think *is that true or false*. Don't write things like $3|12 = 4$! If $a$ does not divide $b$, write $a \not| b$. For example, it is true[2] that $3 \not| 13$.

[1] That is, $a$ divides into $b$ **evenly**.

[2] Fact: 3 does not divide into 13 **evenly**.

## 21.1 *Properties of divides*

Here is a list of a few simple facts about the divisibility relation.

**Theorem 21.1.** *For $a, b, c \in \mathbb{Z}$ we have*

*(1)* $a|0$

*(2)* $\pm 1|a$

*(3) If $a|b$, then $-a|b$*

*(4) If $a|b$ and $b|c$, then $a|c$. So $a|b$ is a transitive relation on $\mathbb{Z}$*

*(5)* $a|-a$

*(6) If $a|b$ and $b \neq 0$, then $0 < |a| \leq |b|$*

*(7) If $a|1$, then $a = \pm 1$*

*(8) If $a|b$ and $b|a$, then $a = \pm b$*

(9) *$a|b$ and $a|c$, then $a|(mb+nc)$ for all $m, n \in \mathbb{Z}$*

(10) *If $a|b$, then $a|bc$ for all $c \in \mathbb{Z}$*

Here are the proofs of a few of these facts.

(1) ***Proof.*** *For any integer $a$, $a0 = 0$, so $a|0$.* ♣

(4) ***Proof.*** *Suppose $a|b$ and $b|c$. That means there are integers $s, t$ so that $as = b$ and $bt = c$. Substituting $as$ for $b$ in the second equation gives $(as)t = c$, which is the same as $a(st) = c$. That shows $a|c$.* ♣

(9) ***Proof.*** *Suppose $a|b$ and $a|c$. That means there are integers $s, t$ such that $as = b$ and $at = c$. Multiply the first equation by $m$ and the second by $n$ to get $a(sm) = mb$ and $a(tn) = nc$. Now add those two equations: $a(sm) + a(tn) = mb + nc$. Factoring out the $a$ on the left shows $a(sm + tn) = mb + nc$, and so we see $a|(mb + nc)$.* ♣

## 21.2 *Prime numbers*

The prime integers play a central role in number theory. A positive integer larger than 1 is said to be **prime** if its only positive divisors are 1 and itself. The first few primes are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$.

A positive integer larger than 1 which is not prime is **composite**. So a composite number $n$ has a positive divisor $a$ which is neither 1 nor $n$. By part (6) of the theorem above, $1 < a < n$.

So, to check if an integer $n$ is a prime, we can trial divide it in turn by $2, 3, 4, 5, \cdots n-1$, and if we find one of these that divides $n$, we can stop, concluding that $n$ is not a prime. On the other hand, if we find that none of those divide $n$, then we can conclude $n$ is a prime. This algorithm for checking a number for primeness can be made more efficient. For example, there is really no need to test to see if 4 divides $n$ if we have already determined that 2 does not divide $n$. And the same reasoning shows that to test $n$ for primeness we need only check in to see if $n$ is divisible by any of $2, 3, 5, 7, 11, 13$ and so on up to the largest prime less than $n$. For example, to test 15 for primeness, we would trial divide by the six values $2, 3, 5, 7, 11, 13$. But even this improved algorithm can be made more efficient by the following theorem.

**Theorem 21.2.** *Every composite number $n$ has a divisor $a$, with*

$$2 \leq a \leq \sqrt{n}.$$

**Proof.** *Suppose $n$ is a composite integer. That means $n = ab$ where $1 < a, b < n$. Not both $a$ and $b$ are greater than $\sqrt{n}$, for if so $n = ab > \sqrt{n}\sqrt{n} = (\sqrt{n})^2 = n$, and that is a contradiction.* ♣

So, if we haven't found a divisor of $n$ by the time we reach $\sqrt{n}$, then $n$ must be a prime.

We can be a little more informative, as the next theorem shows.

**Theorem 21.3.** *Every integer $n > 1$ is divisible by a prime.*

**Proof.** *Let $n > 1$ be given. The set, $D$, of all integers greater than 1 that divide $n$ is nonempty since $n$ itself is certainly in that set. Let $m$ be the smallest integer in that set. Then $m$ must be a prime since if $k$ is an integer with $1 < k < m$ and $k|m$, then $k|n$, and so $k \in D$. That is a contradiction since $m$ is the smallest element of $D$. Thus $m$ is a prime divisor of $n$.* ♣

Among the more important theorems in number theory is the following.

**Theorem 21.4.** *The set of prime integers is infinite.*

**Proof.** *Suppose that there were only finitely many primes. List them all: $2, 3, 5, 7, \cdots, p$. Form the number $N = 1 + 2 \cdot 3 \cdot 5 \cdot 7 \cdots p$. According to the last theorem, there must be a prime that divides $N$, say $q$. Certainly $q$ also divides $2 \cdot 3 \cdot 5 \cdot 7 \cdots p$ since that is the product of all the primes, so $q$ is one of its factors. Hence $q$ divides $N - 2 \cdot 3 \cdot 5 \cdot 7 \cdots p$. But that's crazy since $N - 2 \cdot 3 \cdot 5 \cdot 7 \cdots p = 1$. We have reached a contradiction, and so we can conclude there are infinitely many primes.* ♣

## 21.3 The division algorithm for integers

**Theorem 21.5** (The Division Algorithm for Integers)**.** *If $a, d \in \mathbb{Z}$, with $d > 0$, there exist unique integers $q$ and $r$, with $a = qd + r$, and $0 \leq r < d$.*

The quantities $q$ and $r$ are called the **quotient** and **remainder** when $a$ is divided by $d$.

**Proof.** *Let $S = \{a - nd | n \in \mathbb{Z}, \text{ and } a - nd \geq 0\}$. Then $S \neq \emptyset$, since $a - (-|a|)d \in S$ for sure. Thus, by the Well Ordering Principle, $S$ has a*

*least element, call it $r$. Say $r = a - qd$. Then we have $a = qd + r$, and $0 \leq r$. If $r \geq d$, then $a = (q+1)d + (r-d)$, with $0 \leq r - d$ contradicting the minimality of $r$.*

*To prove uniqueness, suppose that $a = q_1 d + r_1 = q_2 d + r_2$, with $0 \leq r_1, r_2 < d$. Then $d(q_1 - q_2) = r_2 - r_1$ which implies that $r_2 - r_1$ is a multiple of $d$. Since $0 \leq r_1, r_2 < d$, we have $-d < r_2 - r_1 < d$. Thus the only multiple of $d$ which $r_2 - r_1$ can possibly be is $0d = 0$. So $r_2 - r_1 = 0$ which is the same thing as $r_1 = r_2$. Thus $d(q_1 - q_2) = 0 = d0$. Since $d \neq 0$ we can cancel $d$ to get $q_1 - q_2 = 0$, whence $q_1 = q_2$.* ♣

## 21.4 Exercises

**Exercise 21.1.** *Determine the quotient and remainder when* 107653 *is divided by* 22869*.*

**Exercise 21.2.** *Determine if* 1297 *is a prime.*

**Exercise 21.3.** *Prove or give a counterexample: The divides relation is reflexive.*

**Exercise 21.4.** *Prove or give a counterexample: The divides relation is symmetric.*

**Exercise 21.5.** *Prove or give a counterexample: The divides relation is transitive.*

**Exercise 21.6.** *What is wrong with the expression* $4|12 = 3$*?*

**Exercise 21.7.** *Show that none of the* 1000 *consecutive integers* $1001! + 2$ *to* $1001! + 1001$ *are primes.*

**Exercise 21.8.** *Prove: For* $a, b, c \in \mathbb{Z}$*, if* $a|b$*, then* $-a|b$*.*

## 21.5 Problems

**Problem 21.1.** *For positive integers, a and b, if the quotient when a is divided by b is q, what are the possible quotients when* $a + 1$ *is divided by b?*

**Problem 21.2.** *For positive integers, a and b, if the quotient when a is divided by b is q, what are the possible quotients when* $2a$ *is divided by b?*

**Problem 21.3.** *Prove: For integers* $a, b$*, if* $a|b$*, then* $-a|b$*.*

**Problem 21.4.** *Prove or give a counterexample: If p is a prime, then* $2p + 1$ *is a prime.*

**Problem 21.5.** *Determine all the integers that* 0 *divides.*
*(Hint: Think about the definition of the divides relation.*
*The correct answer is probably not what you expect.)*

**Problem 21.6.** *Determine if* 3599 *is a prime. (Hint: This is easy since* $3599 = 3600 - 1$*)*

**Problem 21.7.** *Determine if* 5129 *is a prime.*

**Problem 21.8.** *Prove property 10 of Theorem 21.1: For integers $a, b, c$, if $a|b$, then $a|bc$.*

**Problem 21.9.** *Suppose the remainder when $a$ is divided by $b$ is $r$. Determine the remainder when $a + 2b$ is divided by $b$. More generally, if $k$ is any integer, determine the remainder when $a + kb$ is divided by $b$.*

**Problem 21.10.** *Show that for any integer $n$, there are $n$ consecutive non-prime integers.*