CHAPTER 5

Number Theory

1. Integers and Division

1.1. Divisibility.

DEFINITION 1.1.1. *Given two integers a and b we say a* **divides** *b if there is an integer c such that $b = ac$. If a divides b, we write $a|b$. If a does not divide b, we write $a \nmid b$.*

Discussion

EXAMPLE 1.1.1. *The number 6 is divisible by 3, $3|6$, since $6 = 3 \cdot 2$.*

EXERCISE 1.1.1. *Let a, b, and c be integers with $a \neq 0$. Prove that if $ab|ac$, then $b|c$.*

Using this definition, we may define an integer to be *even* if it is divisible by 2 and *odd* if it is not divisible by 2. This concept is one of the simplest of properties of numbers to define, yet it is among the most complicated of all mathematical ideas. Keep in mind that we are talking about a very restricted notion of what it means for one number to "divide" another: we can certainly divide 7 by 3 and get the rational number $\frac{7}{3} = 2.3333\cdots$, but, since the result is not an integer, we say that 3 does not divide 7, or $3 \nmid 7$. For this reason, you should *avoid using fractions* in any discussion of integers and integer arithmetic.

1.2. Basic Properties of Divisibility.

THEOREM 1.2.1. *For all integers a, b, and c,*

1. *If $a|b$ and $a|c$, then $a|(b + c)$.*
2. *If $a|b$, then $a|(bc)$.*
3. *If $a|b$ and $b|c$, then $a|c$.*

Discussion

Theorem 1.2.1 states the most basic properties of division. Here is the proof of part 3:

Proof of part 3. Assume a, b, and c are integers such that $a|b$ and $b|c$. Then by definition, there must be integers m and n such that $b = am$ and $c = bn$. Thus

$$c = bn = (am)n = a(mn).$$

Since the product of two integers is again an integer, we have $a|c$. □

EXERCISE 1.2.1. *Prove part 1 of Theorem 1.2.1.*

EXERCISE 1.2.2. *Prove part 2 of Theorem 1.2.1.*

1.3. Theorem 1.3.1 - The Division Algorithm.

THEOREM 1.3.1. (Division Algorithm) *Given integers a and d, with $d > 0$, there exists unique integers q and r, with $0 \leq r < d$, such that $a = qd + r$.*

NOTATION 1.3.1. *We call a the* **dividend***, d the* **divisor***, q the* **quotient***, and r the* **remainder***.*

Discussion

The division algorithm is probably one of the first concepts you learned relative to the operation of division. It is not actually an algorithm, but this is this theorem's traditional name. For example, if we divide 26 by 3, then we get a quotient of 8 and remainder of 2. This can be expressed $26 = 3 \cdot 8 + 2$. It is a little trickier to see what q and r should be if $a < 0$. For example, if we divide -26 is by 3, then the remainder is *not* -2. We can, however, use the equation $26 = 3 \cdot 8 + 2$ to our advantage:

$$-26 = 3 \cdot (-8) - 2 = [3 \cdot (-8) - 3] - 2 + 3 = 3(-9) + 1$$

So dividing -26 by 3 gives a quotient of -9 and remainder 1. The condition $0 \leq r < d$ makes r and q unique for any given a and d.

1.4. Proof of Division Algorithm.

Proof. Suppose a and d are integers, and $d > 0$. We will use the well-ordering principle to obtain the quotient q and remainder r. Since we can take $q = a$ if $d = 1$, we shall assume that $d > 1$.

Let S be the set of all **natural numbers** of the form $a - kd$, where k is an integer. In symbols

$$S = \{a - kd | k \in \mathbf{Z} \text{ and } a - kd \geq 0\}.$$

If we can show that S is nonempty, then the well-ordering principle will give us a least element of S, and this will be the remainder r we are looking for. There are two cases.

Case 1: $a \geq 0$. In this case, we can set $k = 0$ and get the element $a - 0 \cdot d = a \geq 0$ of S.

Case 2: $a < 0$. In this case, we can set $k = a$. Then $a - kd = a - ad = a(1 - d)$. Since $a < 0$ and $d > 1$, $a(1 - d) > 0$; hence is an element of S.

Thus, $S \neq \emptyset$, and so S has a least element $r = a - qd$ for some integer q. Thus, $a = qd + r$ and $r \geq 0$. We are left to show (i) $r < d$ and (ii) q and r are unique.

(i) Suppose $r \geq d$. Then $r = d + r'$, where $0 \leq r' < r$. Then $a = qd + r = qd + d + r' = (q + 1)d + r'$,
so that $r' = a - (q + 1)d$ is an element of S smaller than r. This contradicts the fact that r is the least element of S. Thus, $r < d$.

(ii) Suppose integers q' and r' satisfy $a = q'd + r'$ and $0 \leq r' < d$. Without loss of generality, we may assume $r' \geq r$, so that $0 \leq r - r' < d$. Since $a = q'd + r' = qd + r$,

$$r - r' = d(q' - q).$$

This means that d divides $r - r'$, which implies either $r - r' \geq d$ or $r - r' = 0$. But but we know $0 \leq r - r' < d$. Thus, $r' = r$, which, in turn, implies $q' = q$. That is, q and r are unique.

1.5. Prime Numbers, Composites.

Definition 1.5.1. *If p is an integer greater than 1, then p is a* **prime number** *if the only divisors of p are 1 and p.*

Definition 1.5.2. *A positive integer greater than 1 that is not a prime number is called* **composite**.

Discussion

Prime numbers are the building blocks of arithmetic. At the moment there are no efficient methods (algorithms) known that will determine whether a given integer is prime or find its prime factors. This fact is the basis behind many of the cryptosystems currently in use. One problem is that there is no known procedure that will generate prime numbers, even recursively. In fact, there are many things about prime numbers that we don't know. For example, there is a conjecture, known as Goldbach's Conjecture, that there are infinitely many *prime pairs*, that is, consecutive odd prime numbers, such as 5 and 7, or 41 and 43, which no one so far has been able to prove or disprove. As the next theorem illustrates, it is possible, however, to prove that there are infinitely many prime numbers. Its proof, attributed to Euclid, is one of the most elegant in all of mathematics.

Theorem 1.5.1. *There are infinitely many prime numbers.*

PROOF. We prove the theorem by contradiction. Suppose there are only finitely many prime numbers, say, $p_1, p_2, ..., p_n$. Let

$$N = p_1 p_2 \cdots p_n + 1.$$

Then N is an integer greater than each of $p_1, p_2, ..., p_n$, so N cannot be prime. In Example 9, Module 3.3, we showed that N can be written as a product of prime numbers; hence, some prime p divides N. We may assume, by reordering $p_1, p_2, ..., p_n$, if necessary, that $p = p_1$. Thus $N = p_1 a$ for some integer a. Substituting, we get

$$p_1 a = p_1 p_2 \cdots p_n + 1$$

$$p_1 a - p_1 p_2 \cdots p_n = 1$$

$$p_1(a - p_2 \cdots p_n) = 1.$$

Thus, $a - p_2 \cdots p_n$ is a positive integer. Since p_1 is a prime number, $p_1 > 1$, and so

$$p_1(a - p_2 \cdots p_n) > 1.$$

But this contradicts the equality above. □

1.6. Fundamental Theorem of Arithmetic.

THEOREM 1.6.1. (Fundamental Theorem of Arithmetic) *Every positive integer greater than one can be written uniquely as a product of primes, where the prime factors are written in nondecreasing order.*

Discussion

We have already given part of the proof Theorem 1.6.1 in an example of *Module 3.3 Induction*. There we showed that every positive integer greater than 1 can be written as a product of prime numbers. The *uniqueness* of the factors is important, and the proof that they are unique, which requires a few additional ideas, will be postponed until the next module.

The prime factorization of 140 is $2 \cdot 2 \cdot 5 \cdot 7$. You can see one reason why we do not want 1 to be prime: There is no limit to the number of times 1 may be repeated as a factor, and that would give us non-unique prime factorizations.

1.7. Factoring.

THEOREM 1.7.1. *If n is a composite integer, then n has a factor less than or equal to $\sqrt{n}$.*

Discussion

Theorem 1.7.1 can be helpful in narrowing down the list of possible prime factors of a number. It was proved in an example of *Module 3.2 Methods of Proof* and exploited in another example of that module. If the number 253 is composite, for example, it must have a factor less than or equal to 15. Thus we need only check the primes 2, 3, 5, 7, 11, and 13. It turns out $253 = 11 \cdot 23$.

1.8. Mersenne Primes.

Definition 1.8.1. *A prime number of the form $2^p - 1$, where p is a prime number, is called a* **Mersenne prime**.

Discussion

Mersenne primes are a special class of primes, which lend themselves to a nice theoretical development. Not all primes are Mersenne, though, and not all numbers of the form $2^p - 1$ are prime. For example, $2^p - 1$ is prime for $p = 2$, 3, 5, and 7, but $2^{11} - 1 = 2047 = 23 \cdot 89$, which is not prime. On the other hand, the primes 5 and 11 cannot be written in this form.

1.9. Greatest Common Divisor and Least Common Multiple.

Definitions 1.9.1. *Given integers a and b*

1. *The* **greatest common divisor** *of a and b, denoted* GCD (a, b), *is the largest positive integer d such that $d|a$ and $d|b$.*
2. *The* **least common multiple** *of a and b, denoted* LCM (a, b), *is the smallest positive integer m such that $a|m$ and $b|m$.*
3. *a and b are called* **relatively prime** *if* GCD $(a, b) = 1$.
4. *The integers $a_1, a_2, a_3, \ldots, a_n$ are called* **pairwise relatively prime** *if* $\mathrm{GCD}(a_i, a_j) = 1$ *for* $1 \leq i < j \leq n$.
5. *The* **Euler ϕ function** *is the function $\phi : \mathbb{Z}^+ \to \mathbb{N}$ defined by $\phi(n) =$ the number of positive integers less than n that are relatively prime to n.*

Lemma 1.9.1. *Suppose a and b are integers and $m = \mathrm{LCM}(a, b)$. If c is a positive integer such that $a|c$ and $b|c$, then $m|c$.*

Proof. Suppose $a|c$ and $b|c$, but $m \not| c$. By the division algorithm there are (unique) positive integers q and r such that $c = mq + r$ and $0 \leq r < m$. Since $m \not| c$, $r \neq 0$; that is, $r > 0$. Write $r = c - mq$. Since a and b both divide c and m, a and b both divide r. But this contradicts the fact that m is supposed to be the least positive integer with this property. Thus $m|c$. □

THEOREM 1.9.1. *$ab = \text{GCD}(a, b) \cdot \text{LCM}(a, b)$.*

Discussion

The proof of Theorem 1.9.1 will be discussed in the next module.

EXAMPLE 1.9.1. *Here are some examples to illustrate the definitions above.*

(1) $\text{GCD}(45, 60) = 15$, *since* $45 = 15 \cdot 3$ *and* $60 = 15 \cdot 4$ *and 15 is the largest number that divides both 45 and 60.*
(2) $\text{LCM}(45, 60) = 180$, *since* $180 = 45 \cdot 4 = 60 \cdot 3$ *and 180 is the smallest number that both 45 and 60 divide.*
(3) 45 and 60 are not relatively prime.
(4) 45 and 16 are relatively prime since $\text{GCD}(45, 16) = 1$.
(5) 4, 7, 13 and 55 are pairwise relatively prime.
(6) $\phi(15) = 8$

If we are given the prime factorizations of two integers, then it is easy to find their GCD and LCM. For example, $600 = 2^3 \cdot 3 \cdot 5^2$ and $220 = 2^2 \cdot 5 \cdot 11$ has greatest common divisor $2^2 \cdot 5 = 20$ and least common multiple $2^3 \cdot 3 \cdot 5^2 \cdot 11 = 6600$. Since prime factorizations can be difficult to find, however, this idea does not lead to an efficient way to compute GCD's. We will introduce an efficient algorithm in the next module that does not involve knowledge about prime factorizations.

EXERCISE 1.9.1. *Let $F(n)$ denote the n-th term of the Fibonacci Sequence. Prove using induction that* $\text{GCD}(F(n), F(n-1)) = 1$ *for all integers $n \geq 2$.*

1.10. Modular Arithmetic.

DEFINITION 1.10.1. *Given integers a and m, with $m > 0$,*
*a **mod** m is defined to be the remainder when a is divided by m.*

DEFINITION 1.10.2. *$a \equiv b (mod\ m)$, read "a is congruent to b modulo (or mod) m," if*
*$m|(a - b)$; that is, $(a - b)$ **mod** $m = 0$.*

THEOREM 1.10.1. *Given integers a, b, and m,*

1. *$a \equiv b\ (mod\ m)$ if and only if a **mod** $m = b$ **mod** m.*
2. *$a \equiv b\ (mod\ m)$ if and only if $a = b + km$ for some integer k.*
3. *If $a \equiv b\ (mod\ m)$ and $c \equiv d\ (mod\ m)$ then*
   (a) *$a + c \equiv b + d\ (mod\ m)$*
   (b) *$a \cdot c \equiv b \cdot d\ (mod\ m)$*

Discussion

The **mod** operation is derived from the Division Algorithm: If we divide the integer a by the positive integer m, we get a unique quotient q and remainder r satisfying $a = mq + r$ and $0 \leq r < m$. The remainder r is *defined* to be the value of a **mod** m. One of the notational aspects that may seem a little unusual is that we write $a + b(\text{mod } m)$ for $(a + b)(\text{mod } m)$. Also, the symbol (mod m) may occasionally be omitted when it is understood.

EXAMPLE 1.10.1. *Here are some examples.*

(a) 12 **mod** $5 = 2$
(b) 139 **mod** $5 = 4$
(c) 1142 **mod** $5 = 2$
(d) $1142 \equiv 12 \equiv 2(\text{mod } 5)$
(e) $1142 + 139 \equiv 2 + 4 \equiv 6 \equiv 1(\text{mod } 5)$
(f) $1142 \cdot 139 \equiv 2 \cdot 4 \equiv 8 \equiv 3(\text{mod } 5)$

One of the differences to note between the concept of congruence modulo m verses the **mod** operator is that an integer, k may be *congruent* to infinitely many other integers modulo m, however, k **mod** m is equal to one single integer. For example, 139 **mod** $5 = 4$, but 139 is *congruent* to all the elements of $\{\dots, -6, -1, 4, 9, 14, 19, \dots\}$.

EXERCISE 1.10.1. *Given a positive integer m, prove that the assignment $a \mapsto a$ **mod** m defines a function $f \colon \mathbf{Z} \to \mathbf{Z}$. Is f one-to-one? onto? What is its range?*

*$a \mapsto a$ **mod** m is another way to write $f(a) = a$ **mod** m.*

Here is a proof of part 3b of Theorem 1.10.1:

Proof of 3b. Since $a \equiv b(\text{mod } m)$ and $c \equiv d(\text{mod } m)$, there must be integers s and t such that $b = a + sm$ and $d = c + tm$ (part 2). Thus

$$\begin{aligned} bd &= (a + sm)(c + tm) \\ &= ac + atm + smc + stm^2 \\ &= ac + (at + sc + stm)m \end{aligned}$$

Since a, c, t, and s are all integers, $at + sc + st$ is as well. Thus, by part 2,

$$ac \equiv bd(\text{mod } m).$$

$\square$

EXERCISE 1.10.2. *Prove part 3a of Theorem 1.10.1.*

1.11. Applications of Modular Arithmetic.

1. Hashing Functions
2. Pseudorandom Number Generators
3. Cryptology

Discussion

There are many applications of modular arithmetic in computer science. One such application is in the construction of pseudorandom number generators. Numbers that seem to be somewhat random may be produced using the **linear congruential method**. As you will see, it does not produce truly random numbers, but rather a sequence of numbers that will eventually repeat.

To generate a sequence we choose a **modulus** m, **multiplier** a, and an **increment** c. Then we start with a *seed* number x_0 and then construct a sequence of numbers recursively using the formula

$$x_{n+1} = (ax_n + c) \textbf{ mod } m.$$

EXAMPLE 1.11.1. *Suppose we choose* $m = 11$, $a = 7$, $c = 3$, *and* $x_0 = 1$. *Then we get*

$x_0 = 1$

$x_1 = (7 \cdot 1 + 3)\textbf{mod } 11 = 10$

$x_2 = (7 \cdot 10 + 3)\textbf{mod } 11 = 7$

$x_3 = (7 \cdot 7 + 3)\textbf{mod } 11 = 8$

$x_4 = (7 \cdot 8 + 3)\textbf{mod } 11 = 4$

$x_5 = (7 \cdot 4 + 3)\textbf{mod } 11 = 9$

$x_6 = (7 \cdot 9 + 3)\textbf{mod } 11 = 0$

$x_7 = (7 \cdot 0 + 3)\textbf{mod } 11 = 3$

etc.

The sequence will be 1, 10, 7, 8, 4, 9, 0, 3, etc. If we wanted a "random" sequence of bits, 0 and 1, we could then reduce each x_n **mod** *2. In practice, large Mersenne primes are often chosen for the modulus, and the repetition period for such sequences can be made to be quite large.*

EXERCISE 1.11.1. *Prove that for a given modulus m, and arbitrary multiplier a, increment c, and seed x_0, the sequence $x_0, x_1, x_2, \ldots$ must eventually repeat.*