Chapter 5

Divisibility and Congruences

Given two integers a and b, we say a divides b or that b is a multiple of a or $a|b$ if there exists an integer q with $b = aq$. Some basic properties divisibility are given in the exercises. It is a much subtler relation than $\leq$. A natural number p is called *prime* if $p \geq 2$ and if the only natural numbers dividing are 1 and p itself.

Lemma 5.1. *Every natural number $n \geq 2$ is divisible by a prime.*

Proof. Let $D = \{m \,|\, m|n \text{ and } m \geq 2\}$. D is nonempty since it contains n. Let p be the smallest element of D. If p is not prime, there exists $d|p$ with $2 \leq d < p$. Then $d \in D$ by exercise 1 of this chapter, but this contradicts the minimality of p. □

Corollary 5.2. *(Euclid) There are infinitely many primes.*

Proof. Suppose that are only finite many primes, say $p_1, p_2, \ldots p_n$. Then consider $N = p_1 p_2 \ldots p_n + 1$. Then N must be divisible by a prime which would have to be one of the primes on the list. Suppose it's p_k. Then by exercise 2, $1 = N - p_1 p_2 \ldots p_n$ would be divisible by p_k, but this is impossible. □

The following is half of the fundamental theorem of arithmetic. What's missing is the uniqueness statement and this will be proved later.

Corollary 5.3. *Every natural number $n \geq 2$ is a product of primes.*

The statement will be proved by induction on n. Note that we have to start the induction at $n = 2$. This does not entail any new principles, since we can change variables to $m = n - 2$, and do induction on $m \geq 0$.

Proof. $n = 2$ is certainly prime. By induction, we assume that the statement holds for any $2 \leq n' < n$. By the lemma, $n = pn'$ with p prime and n' a natural number. If $n = p$ then we are done. Otherwise $n' \geq 2$, so that it can be written as a product of primes. Therefore the same goes for $n = pn'$. $\square$

The proofs can be turned into a method, or algorithm, for factoring an integer. In fact, it's the obvious one. Start with n, try to divide by $2, 3, 4 \ldots n-1$. If none of these work, then n is prime. Otherwise, record the first number, say p, which divides it; it's a prime factor. Replace n by n/p and repeat. Similarly, we get an algorithm for testing whether n is prime, by repeatly testing divisibility by $2, 3, 4 \ldots n - 1$. Note that we can do slightly better (ex. 3)

Fix a positive integer n. For doing computations in $\mathbb{Z}_n$ with paper and pencil, it's very convenient to introduce the $\equiv$ symbol. We will say that $a \equiv_n b$ if $a - b$ is divisible by n, or equivalently if a and b. One can work with $\equiv$ symbol as one would for $=$ thanks to:

Proposition 5.4. *The follow hold:*

1. *$\equiv_n$ is reflexive, i.e. $x \equiv_n x$.*
2. *$\equiv_n$ is symmetric, i.e. $x \equiv_n y$ implies $y \equiv_n x$.*
3. *$\equiv_n$ is transitive, i.e. $x \equiv_n y$ and $y \equiv_n z$ implies that $x \equiv_n z$.*
4. *If $a \equiv_n b$ and $c \equiv_n d$ then $a + c \equiv_n b + d$.*

Proof. We prove the transitivity (3). The other statements are left as an exercise. Suppose that $x \equiv_n y$ and $y \equiv_n x$, then $x - y = na$ and $y - z = nb$ for some $a, b \in \mathbb{Z}$. Then $x - z = x - y + y - z = n(a + b)$, which proves that $x \equiv_n z$. $\square$

A relation satisfying the first three properties above is called an *equivalence relation*.

Lemma 5.5. *Given an integer x and a positive integer n, there exist a unique element $(x \, mod \, n) \in \{0, 1, \ldots n - 1\}$ such that $x \equiv_n (x \, mod \, n)$*

A warning about notation. Typically, in most math books, they would write $x \equiv y \ (\ mod \, n)$ instead of $x \equiv_n y$.

Proof. First suppose $x \geq 0$. In this case, there are no surprises. The division algorithm gives $x = qn + r$ with $r \in \{0, \ldots n - 1\}$. $x \equiv_n r$ since n divides $x - r$. So we can take $x \, mod \, n = r$.

Suppose that $x < 0$. If x is divisible by n, then we take $x \, mod \, n = 0$. Suppose is x is not divisible by n, then applying the division algorithm to $-x$ yields $-x = qn + r$ with $0 < r < n$. Therefore

$$x = -qn - r = -qn - n + n - r = -(q + 1)n + (n - r)$$

with $0 < n - r < n$. So we can take $x \, mod \, n = n - r$. We leave it as an exercise to check the uniqueness. $\square$

$x \to x \, mod \, n$ can be visualized as follows when $n = 3$

$$\begin{array}{ccccccc} -3 & -2 & -1 & 0 & 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 \end{array}$$

The rule for adding in $\mathbb{Z}_n$ is now quite easy with this notation. Given $x, y \in \{0, 1, \dots n-1\}$

$$x \oplus y = (x + y) \, mod \, n$$

Now we can finally prove:

Theorem 5.6. *$(\mathbb{Z}_n, +, 0)$ is an Abelian group.*

Proof. We assume that the variables $x, y, z \in \{0, 1, \dots n-1\}$. Let's start with the easy properities first.

$$x \oplus y = (x + y) \, mod \, n = (y + x) \, mod \, n = y \oplus x$$

$$x \oplus 0 = (x + 0) \, mod \, n = x$$

Set

$$\ominus x = (-x) \, mod \, n$$

Then, either $x = 0$ in which case

$$x \oplus (\ominus x) = 0 + 0 \, mod \, n = 0,$$

or else $x \neq 0$ in which case $\ominus x = n - x$ so that

$$x \oplus (\ominus x) = (x + n - x) \, mod \, n = 0.$$

Finally, we have to prove the associative law. We have

$$y + z \equiv_n (y + z \, mod \, n) = y \oplus z$$

by definition. Therefore by proposition 5.4

$$x + (y + z) \equiv_n x + (y \oplus z) \equiv_n (x + (y + z \, mod \, n)) \, mod \, n = x \oplus (y \oplus z)$$

On the other hand

$$x + y \equiv_n (x + y \, mod \, n) = x \oplus y$$

so that

$$(x + y) + z \equiv_n (x \oplus y) + z \equiv_n ((x \oplus y) + z) \, mod \, n = (x \oplus y) \oplus z$$

Since $x + (y + z) = (x + y) + z$, we can combine these congruences to obtain

$$x \oplus (y \oplus z) \equiv_n (x \oplus y) \oplus z$$

We can conclude that the two numbers are the same by the uniquess statement of lemma 5.5.

$\square$

5.7 Exercises

1. Prove that $|$ is transitive, and that $a|b$ implies that $a \leq b$ provided that $b > 0$.

2. Prove that $a|b$ and $a|c$ implies $a|(b'b + c'c)$ for any pair of integers b', c'.

Let $b \geq 2$ be an integer. A base b expansion of a natural number N is a sum $N = a_n b^n + a_{n-1} b^{n-1} + \ldots a_0$ where each a_i is an integer satisfying $0 \leq a_i < b$. Base 10 (decimal) expansions are what we normally use, but $b = 2, 8, 16$ are useful in computer science.

3 Show that a_0 is the remainder of division of N by b.

4 For any $b \geq 2$, prove that any natural number N has a base b expansion by induction. (Use the division algorithm.)

5 Turn the proof around to find a method for calculating the coefficients a_i. Find a base 8 expansion of 1234.

6 Finish the proof of proposition 5.4.