Chapter 1 Arithmetic in $\mathbb{Z}$

You learn the basics of arithmetic in $\mathbb{Z}$ in grade school. Most everything in this chapter is familiar to you, but now we will actually prove the results you already know. This is a good way to start in abstract algebra as you work with objects you already know.

We start with the division algorithm, which is really just division with remainder.

Theorem 1.1.1 (Division algorithm): Let $a, b \in \mathbb{Z}$ with $b > 0$. There exist unique integers q, r with $0 \leq r < b$ so that

$$a = bq + r.$$

Before we prove this, a quick example.

Example: Let $a = 13$, $b = 3$. Then

$$\begin{array}{r} 4 \\ 3\overline{)13} \\ \underline{12} \\ 1 \end{array}$$

so $13 = 3(4) + r$ $\quad b = 4$, $r = 1$.

Proof: Let a, b be as in the statement of the theorem and consider the set

$$S = \{a - bm : a - bm \geq 0, m \in \mathbb{Z}\}.$$

We first show S is nonempty. Since $b \geq 1$, we have $|a| b \geq |a|$. ~~Since~~ By definition we have $|a| \geq -a$, so $|a| b \geq -a$, and so $a + b|a| \geq 0$. Thus, if we take $m = -|a|$, then $a + b|a| \in S$ so $S \neq \emptyset$.

Since S is a subset of $\mathbb{Z}_{\geq 0}$ and is nonempty, the well-ordering axiom gives there is a smallest element of S, say r. We have $r = a - bq$ for some $q \in \mathbb{Z}$, ie, $a = bq + r$. It only remains to show $0 \leq r < b$ and r, q are unique.

Claim: $r < b$.

Pf: Suppose $r \geq b$. Then

$$\begin{aligned} 0 \leq r - b &= (a - bq) - b \\ &= a - b(q+1). \end{aligned}$$

Since $a - b(q+1) \geq 0$, it is in S. Since $b > 0$, $r - b$ ~~$>$ b~~ $< r$, so $a - b(q+1) < r$ and in S. This contradicts r being the smallest element of S. Thus, $r < b$.

Claim: $0 \leq r$

This is clear because $r \in S$.

It only remains to show q, r are unique.

Suppose there exist q_1, q_2, r_1, r_2 w/ $0 \le r_1, r_2 < b$

and
$$a = bq_1 + r_1$$
$$= bq_2 + r_2.$$

Thus,
$$b(q_1 - q_2) = r_2 - r_1 \quad (*)$$

Since $0 \le r_1 < b$, we have $-b < -r_1 \le 0$ and $0 \le r_2 < b$

implies $-b < r_2 - r_1 < b$.

$(*)$ gives
$$-b < b(q_1 - q_2) < b$$
$$\Rightarrow \quad -1 < q_1 - q_2 < 1.$$

Thus, $q_1 - q_2 = 0$, i.e. $q_1 = q_2$.

This also gives $r_1 = r_2$ and we are done. ☒

1.2 Divisibility:

Def: Let $a, b \in \mathbb{Z}$, $b \neq 0$. We say <u>b divides a</u>, and write $b \mid a$, if there exists $c \in \mathbb{Z}$ so that $a = bc$. If there is no such c we say b does not divide a and write $b \nmid a$.

Example: $5 \mid 15$ because $15 = 5 \cdot 3$.

Lemma 1.2.1: Let $n \in \mathbb{Z}$. Then n has only finitely many divisors.

Proof: This follows immediately from the fact that if $a \mid n$, then $|a| \leq |n|$, which we now prove. Suppose $a \mid n$. Then there exists $c \in \mathbb{Z}$ so that $n = ac$. Thus, $|n| = |a|\,|c|$. Since $c \in \mathbb{Z}$, $c \neq 0$, we have $|c| \geq 1$ so $|a| \leq |n|$. ∎

Let $a, b \in \mathbb{Z}_{\neq 0}$. Since each has only finitely many divisors, the collection of common divisors is finite. This means among the common divisors there is a greatest element.

Def: Let $a, b \in \mathbb{Z}$, not both 0. The greatest common divisor of a and b, denoted $\gcd(a,b)$, is the largest integer that divides a and b, i.e., $d = \gcd(a,b)$ if

1) $d \mid a$ and $d \mid b$

2) if $c \in \mathbb{Z}$ satisfies $c \mid a$ and $c \mid b$, then $c \leq d$.

Example: $\gcd(12, 16) = 4$.

Theorem 1.2.2: Let $a, b \in \mathbb{Z}$, not both 0; $d = \gcd(a,b)$. Then there exists $m, n \in \mathbb{Z}$ so that $am + bn = d$.

Proof: Let

$$S = \{ax+by : x, y \in \mathbb{Z}, \ ax+by > 0\}.$$

Note $a^2+b^2 > 0$ since a,b are not both 0, so $S \neq \emptyset$. Let $e = ax+by$ be the smallest element of S. Thus, $e = am+bn$ for some $m, n \in \mathbb{Z}$. Since $d \mid a$ and $d \mid b$, there exist $c_1, c_2 \in \mathbb{Z}$ so that $a = dc_1$, $b = dc_2$ so $e = dc_1 m + dc_2 n = d(c_1 m + c_2 n)$. Thus, $d \mid e$, and so $d \leq e$. Thus, if we can show $e \mid a$ and $e \mid b$ we will have $d = e$ and e is the gcd.

Write $a = eq + r$ for $0 \leq r < e$.

Then we have

$$r = a - eq$$

$$= a - (am+bn)q = (1-m)a + b(-q).$$

Thus, $r \in S$. Since e is the smallest element of S and $0 \leq r < e$, we must have $r=0$. Thus, $e|a$. Similarly for b. ■

<u>Cor 1.2.3:</u> Let a, b be as above. Then $d = \gcd(a,b)$ iff

1) $d|a$ and $d|b$

and

2) if $c|a$ and $c|b$, then $c|d$.

<u>Proof:</u> Let e satisfy these conditions, ie. $e|a$ and $e|b$ and if $c|a$ and $c|b$, then $c|e$. We must show $e=d$. Since e is a common divisor, we have $e \leq d$ by definition. Conversely, since $d|a$ and $d|b$, we must have by 2) above that ~~$e|d$~~. $d|e$. Thus, $e=d$. ■

<u>Lemma 1.2.4:</u> If $a = bq+r$, then $\gcd(a,b) = \gcd(b,r)$.

<u>Proof:</u> Let $d = \gcd(a,b)$ and $e = \gcd(b,r)$. Since $r = a-bq$, we have $d \mid a-bq=r$. Thus, d is a common divisor of b and r, so $d \leq e$. Similarly, if $e|b$ and $e|r$, so $e|a$. Thus $e \leq d$. Hence, $d=e$. ■

We can use this last result to give an algorithm for calculating $\gcd(a,b)$. We can write:

$$a = bq_1 + r_1 \qquad 0 \le r_1 < b$$

$$b = r_1 q_2 + r_2 \qquad 0 \le r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3 \qquad 0 \le r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n \qquad 0 \le r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1}$$

Note since the sequence $\{r_1, r_2, r_3, \dots\}$ is a strictly decreasing sequence of nonnegative integers after finitely many steps we must get 0. Lemma 1.2.4 now gives

$$\gcd(a,b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n.$$

Thus, $\gcd(a,b) = r_n$, the last nonzero remainder.

<u>Example:</u> We saw before $\gcd(12,16) = 4$.

$$16 = 12 \cdot 1 + 4$$

$$12 = 4 \cdot 3 + 0$$

So $\gcd(12,16) = 4$ by this method as well.

We can also use this to find $m, n \in \mathbb{Z}$ so that

$$am + bn = d$$

by back substitution.

Example: Let $a = 12378$, $b = 3054$. We have

$$12378 = 4 \cdot 3054 + 162$$
$$3054 = 18 \cdot 162 + 138$$
$$162 = 1 \cdot 138 + 24$$
$$138 = 5 \cdot 24 + 18$$
$$24 = 1 \cdot 18 + 6$$
$$18 = 3 \cdot 6 + 0.$$

Thus, $\gcd(12378, 3054) = 6$. To find m, n we back substitute:

$$6 = 24 + 18(-1) \qquad (1)$$
$$18 = 138 + 24(-5) \qquad (2)$$
$$24 = 162 + 138(-1) \qquad (3)$$
$$138 = 3054 + 162(-18) \qquad (4)$$
$$162 = 12378 + 3054(-4) \qquad (5)$$

$(1) \to (2)$: $6 = 24 + (-1)(138 + 24(-5)) = 6(24) + 138(-1)$

$(3) \to$ this : $6 = 6(162 + 138(-1)) + 138(-1)$

$$= 6(162) + (-7)(138)$$

(4) → this:

$$6 = 6(162) + (-7)(3054 + 162(-18))$$

$$= 6(162) + 126(162) + (-7)(3054)$$

$$= 132\overset{162)}{(\cancel{0}} + (-7)(3054)$$

(5) → this:

$$6 = 132(12378 + 3054(-4)) + (-7)(3054)$$

$$= 12328(132) + 3054(-535).$$

<u>Theorem 1.2.5 (Euclid's Lemma):</u> If $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$.

<u>Proof:</u> Since $\gcd(a,b) = 1$, there exist $m, n \in \mathbb{Z}$ so that $am + bn = 1$. Multiply this by c: $c = acm + bcn$. Since $a \mid bc$, there exists $k \in \mathbb{Z}$ so that $bc = ak$. Thus,

$$c = a(cm + kn),$$

and $a \mid c$. ▣

Note that if we write $am + bn = d$ this does <u>NOT</u> in general imply that $\gcd(a,b) = d$. For example, $5 = 3(5) + 2(-5)$, but

$\gcd(2,3) = 1$, not 5.

<u>Prop. 1.2.6:</u> If $am + bn = 1$ for some $m, n \in \mathbb{Z}$ then $\gcd(a,b) = 1$.

<u>Proof:</u> Let $d = \gcd(a,b)$. Then $d \mid a$ and $d \mid b$, so $d \mid (am+bn) = 1$. (See book problem). Thus, $d \mid 1 \rightarrow d = 1$. ■

1.3 Prime and Unique Factorization:

<u>Def:</u> We say $p \in \mathbb{Z}_{>1}$ is <u>prime</u> if the only divisors of p are 1 and p.

<u>Example:</u> 7 is prime, but 6 is not.

(Note the book allows negative primes; we do not. Most sources only consider positive numbers to be prime so we follow that convention.)

<u>Theorem 1.3.1:</u> Let $p \in \mathbb{Z}$. We have p is prime iff whenever $p \mid ab$, $p \mid a$ or $p \mid b$.

<u>Proof:</u> First suppose p is prime. If and assume $p \mid ab$.

If $p \mid a$ we are done. Assume $p \nmid a$. Since p is prime this gives $\gcd(p, a) = 1$. Thus, Euclid's lemma gives $p \mid b$.

Now assume that whenever $p \mid ab$, that $p \mid a$ or $p \mid b$. If p is not prime, we can write $p = mn$ with $m, n \in \mathbb{Z}_{\geq 1}$. But then $m, n < p$ so $p \nmid m$, $p \nmid n$. This is a contradiction, so it must be the case p is prime. ■

<u>Cor 1.3.2:</u> Let p be prime and $p \mid a_1 \cdots a_n$. Then $p \mid a_j$ for some $1 \leq j \leq n$.

<u>Proof:</u> Exercise. ■

<u>Theorem 1.3.3:</u> Let $n \in \mathbb{Z}_{\geq 2}$. Then n can be factored into primes.

<u>Proof:</u> Let S be the subset of $\mathbb{Z}_{\geq 2}$ consisting of elements that do not factor into primes. Suppose $S \neq \emptyset$. The Well-ordering axiom says S has a smallest element, say m. Since m cannot be factored into primes, it cannot be prime itself. Write $m = a_1 a_2$ with $a_1, a_2 \in \mathbb{Z}_{\geq 1}$. Then $a_1, a_2 < m$ so they cannot be in S, so they have prime factorizations. This is a contradiction because their factorization provides a factorization of m. Thus, $S = \emptyset$. ■

Note if $n \in \mathbb{Z}_{<0}$, then $-n \in \mathbb{Z}_{>0}$. This means we can factor any $n \in \mathbb{Z}$, $n \neq 0, \pm 1$ by setting if $n \in \mathbb{Z}_{<-2}$, write $-n \in \mathbb{Z}_{>2}$ as . $-n = p_1 \cdots p_k$, so $n = (-1)\, p_1 \cdots p_k$.

<u>Theorem 1.3.4 (Fundamental Theorem of Arithmetic):</u> Let $n \in \mathbb{Z}_{\geq 2}$. Then n can be factored into primes uniquely up to the order of the primes.

<u>Proof:</u> Suppose we have

$$n = p_1 \cdots p_k = q_1 \cdots q_s.$$

with the p_i, q_j primes. WLOG assume $k \leq s$. Note $p_1 \mid q_1 \cdots q_s$, so by Cor. 1.3.2 we have $p_1 \mid q_j$ for some $1 \leq j \leq s$. However, since these are both prime we must have $p_1 = q_j$. WLOG assume $j = 1$.

Then cancelling we have

$$p_2 \cdots p_k = q_2 \cdots q_s.$$

Continuing like this we have

$$1 = q_{k+1} \cdots q_s.$$

Thus, $s = k$ and the factorization is unique. ▣

Primes are essentially the building blocks of the integers so they are of fundamental importance to studying $\mathbb{Z}$. One should take number theory to really see this.