The Division Algorithm, Bézout's Lemma, and $\mathbb{Z}_n$

R. C. Daileda

Let $n \in \mathbb{Z}$. Under addition and multiplication modulo n (the binary operations of *modular arithmetic*), the residue classes (remainders) of integers modulo n yield two abelian groups. Although modular arithmetic is relatively straightforward, proving that addition and multiplication modulo n satisfy the axioms defining a group is somewhat challenging. There are (at least) two standard ways to construct the groups we seek ($\mathbb{Z}_n$ and $\mathbb{Z}_n^\times$), but there are inherent difficulties with both. The first approach (which we illustrate below) is elementary, using only integers and the division algorithm. But its simplicity evaporates when we actually try to prove anything (we have no tools with which to work). On the other hand, the irritating aspects of the elementary approach are *automatically* resolved in the second approach, at the expense of moving all of the real work up front: the set of ordinary integers $\{0, 1, 2, \ldots, n-1\}$ must be replaced by a quotient (collection of equivalence classes)of $\mathbb{Z}$, and one must utilize the First Isomorphism Theorem of group theory. In practice, the latter construction is easier to work with in the context of groups and elsewhere, but this would preclude the introduction of $\mathbb{Z}_n$ in a course on group theory until after a good deal of abstract machinery has been developed. Since the groups $\mathbb{Z}_n$ and $\mathbb{Z}_n^\times$ serve as fundamental (and essential) examples of finite abelian groups, this is undesirable. We will therefore provide a careful exposition of the elementary construction of these groups in what follows. We begin with the fundamental results from number theory that are necessary for this construction, before moving on to apply them in the context of modular arithmetic.

1 Number Theory

In number theory (or ring theory more generally), given $m, n \in \mathbb{Z}$ one says that m *divides* n (denoted $m|n$) provided there is a $q \in \mathbb{Z}$ so that $mq = n$. In this case, one says that m is a *factor* or *divisor* of n or that n is *divisible* by m. It is not hard to show that divisibility yields a partial ordering on $\mathbb{Z}$, but it is not total: given two integers, it is usually *not* the case that one divides the other. The Division Algorithm fills this gap by giving the "approximate" divisibility relationship that exists between two integers in any case.

Theorem 1 (The Division Algorithm)**.** *Let $n \in \mathbb{N}$. For any $m \in \mathbb{Z}$, there exist unique $q \in \mathbb{Z}$ and $r \in \{0, 1, 2, \ldots, n-1\}$ so that*

$$m = qn + r.$$

Proof (Sketch). The set

$$S = \{m - qn \geq 0 \,|\, q \in \mathbb{Z}\}$$

is a nonempty subset of $\mathbb{N}_0$ (this is clear if $m \geq 0$; otherwise take q to be extremely large and negative). Let $r \in S$ so that $m - qn = r$ for some $q \in \mathbb{Z}$. If $r \geq n$, subtracting n from both sides of the preceding equality yields $m - (q+1)n = r - n \geq 0$. Therefore $r - n \in S$. So if we take r to be the least element of S (which exists by the Well Ordering Principle), it must be the case that $r < n$, lest $r - n$ be a smaller member of S. We then have $r = m - qn$ for some $q \in \mathbb{Z}$ with $0 \leq r < n$. This proves the existence portion of the theorem.

As for uniqueness, suppose that $m = q'n + r'$ for some $q' \in \mathbb{Z}$ and $0 \leq r' < n$. Then

$$r' = m - q'n \in S.$$

Since the difference of any two elements of S is divisible by n, we find that $n | r - r'$. However, $|r - r'| < n$, so the only way this is possible is if $r - r' = 0$, or $r = r'$. That $q = q'$ follows at once, establishing that r and q are indeed unique. □

Let $n \in \mathbb{N}$ and $m \in \mathbb{Z}$. Use the Division Algorithm to write $m = qn + r$ with $q \in \mathbb{Z}$ and $r \in \{0, 1, 2, \ldots, n-1\}$. The (unique) integers q and r in this equation are called the *quotient* and *remainder* (resp.) when m is divided by n. An important feature of the uniqueness of quotients and remainders is the following. No matter how we arrive at an expression of the form $m = q'n + r'$, if $q' \in \mathbb{Z}$ and $r' \in \{0, 1, 2, \ldots, n-1\}$, then q' *must* be the quotient, and r' *must* be the remainder. This is one of the most useful features of the Division Algorithm. For instance, it can be used to show that n divides m if and only if $r = 0$. This shows that the Division Algorithm subsumes and generalizes the notion of divisibility in $\mathbb{Z}$.

The next result concerns greatest common divisors, and may appear somewhat mysterious to the uninitiated. Given $a, b \in \mathbb{Z}$, recall that their *greatest common divisor* is defined to be the largest $c \in \mathbb{N}_0$ so that $c|a$ and $c|b$, and is denote by $\gcd(a, b)$ or simply (a, b). Because $a|0$ for all $a \in \mathbb{Z}$, the case $a = b = 0$ must be treated separately. Informed by the result below, in this case we set $(0, 0) = 0$. Bézout's Lemma simply states that (a, b) is always a $\mathbb{Z}$-linear combination of a and b. Taken out of context, the statement and proof of Bézout's Lemma lack any intuition. Its tremendous utility should nonetheless serve to make up for the apparent "randomness" of this result. The essential observation to be made is that any common divisor of a and b must divide any $\mathbb{Z}$-linear combination of a and b. We leave the simple proof of this fact to the reader.

Theorem 2 (Bézout's Lemma)**.** *Let $a, b \in \mathbb{Z}$. There exist $r, s \in \mathbb{Z}$ so that*

$$(a, b) = ra + sb.$$

Proof. If a and b are not both zero, let

$$S = \{ra + sb > 0 \,|\, r, s \in Z\}.$$

Then S is a nonempty subset of $\mathbb{N}$, and it therefore has a least element $c = ra + sb$. Use the Division Algorithm to write $a = qc + r'$ with $0 \leq r' < c$. Then

$$r' = a - qc = a - q(ra + sb) = (1 - qr)a - qsb.$$

If $r' > 0$, this shows that $r' \in S$, and hence $c \leq r'$. But this contradicts $r' < c$. Therefore $r' = 0$, so that $a = qc$. That is, $c|a$. Likewise, one has $c|b$ as well. So c is a (positive) common divisor of a and b, which means that $c \leq (a, b)$. But (a, b) divides both a and b, and hence (a, b) divides every element of S. Since $c \in S$, this implies $(a, b) \leq c$. It now follows that $c = (a, b)$, which completes the proof. □

The proof we have given here is standard but entirely nonconstructive: it gives no means by which to actually determine r and s. In many applications of Bézout's Lemma this is immaterial. As we shall see, however, there are instances in which explicit knowledge of the coefficients r and s would be useful. Fortunately one can give an alternate constructive proof of Bézout's Lemma using the *Euclidean Algorithm* for computing GCDs. But this is beyond the scope of this note.

2 The Groups $\mathbb{Z}_n$ and $\mathbb{Z}_n^\times$

Throughout this section $n \in \mathbb{N}$ is fixed. Let

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\},$$

which is simply the set of possible remainders in the division algorithm. Given $m \in \mathbb{Z}$, let $R_n(m) \in \mathbb{Z}_n$ denote the remainder when m is divided by n using the Division Algorithm. That is, $R_n(m)$ is the unique member of $\mathbb{Z}_n$ for which there is an integer q so that

$$m = qn + R_n(m).$$

Observe that if $a \in \mathbb{Z}_n$, then $R_n(a) = a$, since $a = 0 \cdot n + a$ expresses a in the unique form given by the Division Algorithm.

Given $a, b \in \mathbb{Z}_n$ define

$$a \oplus b = R_n(a+b), \tag{1}$$

$$a \otimes b = R_n(ab). \tag{2}$$

Because $R_n : \mathbb{Z} \to \mathbb{Z}_n$, we see immediately that $\oplus$ and $\otimes$ are binary operations on $\mathbb{Z}_n$. We call them *addition modulo* (or just "mod") n and *multiplication modulo* n. These are the fundamental operations of modular arithmetic.

Because ordinary addition and multiplication are commutative operations on $\mathbb{Z}$, the same holds for their modular counterparts. For instance, for any $a, b \in \mathbb{Z}$ we have

$$a \oplus b = R_n(a+b) = R_n(b+a) = b \oplus a.$$

Both modular operations have the usual identities: 0 for $\oplus$ and 1 for $\otimes$. To see this we simply note that for any $a \in \mathbb{Z}_n$, by the remark at the end of the preceding paragraph one has

$$a \oplus 0 = R_n(a+0) = R_n(a) = a,$$

and likewise for $\otimes$. We remark that the "two-sided-ness" of these identities is automatic in light of the fact that both operations are commutative.

Both addition modulo n and multiplication modulo n are associative, but this isn't entirely trivial to prove. To see why, let $a, b, c \in \mathbb{Z}_n$. Then

$$a \oplus (b \oplus c) = a \oplus R_n(b+c) = R_n(a + R_n(b+c))$$

whereas

$$(a \oplus b) \oplus c = R_n(a+b) \oplus c = R_n(R_n(a+b) + c).$$

To show that these are the same we require the following lemma quantifying the failure of the function $R_n : \mathbb{Z} \to \mathbb{Z}_n$ to be injective.

Lemma 1. *Let $n \in \mathbb{Z}$ and $a, b \in \mathbb{Z}$. Then $R_n(a) = R_n(b)$ if and only if $n|a - b$.*

Proof. We begin by writing $a = qn + R_n(a)$ and $b = q'n + R_n(b)$ for some $q, q' \in \mathbb{Z}$ so that

$$a - b = (q - q')n + R_n(a) - R_n(b).$$

If $R_n(a) = R_n(b)$, this implies at once that $n|a - b$. Conversely, if $a - b = cn$ for some $c \in \mathbb{Z}$, we find that

$$a = b + cn = (q' + c)n + R_n(b).$$

The uniqueness of remainders in the Division Algorithm now implies $R_n(a) = R_n(b)$, as needed. □

We can now easily show that $\oplus$ is associative. Since

$$(a + R_n(b + c)) - (a + b + c) = R_n(b + c) - (b + c)$$

is a multiple of n, Lemma 1 tells us that

$$R_n(a + R_n(b + c)) = R_n(a + b + c).$$

But this is true for all integers a, b, c, so we also have

$$R_n(R_n(a + b) + c) = R_n(c + R_n(a + b)) = R_n(c + a + b) = R_n(a + b + c).$$

Therefore

$$R_n(a + R_n(b + c)) = R_n(a + b + c) = R_n(R_n(a + b) + c),$$

proving that $\oplus$ is associative.

We can treat $\otimes$ in a similar fashion. We have

$$aR_n(bc) - abc = a(R_n(bc) - bc),$$

which is a multiple of n. Therefore, by Lemma 1,

$$a \otimes (b \otimes c) = R_n(aR_n(bc)) = R_n(abc).$$

Since a, b and c are arbitrary, we may freely interchange them to see that

$$(a \otimes b) \otimes c = c \otimes (a \otimes b) = R_n(cab) = R_n(abc).$$

The associativity of $\otimes$ now follows as above. A nearly identical argument can be used to prove that $\otimes$ distributes over $\oplus$ as well:

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c).$$

We won't need this fact here and leave the details of its proof to the reader.

The element $0 \in \mathbb{Z}_n$ is easily seen to be its own inverse under addition modulo n, since $0 + 0 = 0$ in $\mathbb{Z}$. If $a \in \mathbb{Z}_n$ is nonzero, then $0 < a < n$ implies $0 < n - a < n$, so that $n - a \in \mathbb{Z}_n$. We then have

$$a \oplus (n - a) = R_n(a + n - a) = R_n(n) = 0,$$

which proves $n - a$ is the additive inverse of a in $\mathbb{Z}_n$.

We can actually prove that every element of $\mathbb{Z}_n$ has an additive inverse modulo n in a case free manner as follows. Let $a \in \mathbb{Z}_n$. Then $-a - R_n(-a)$ is divisible by n, so that $a + R_n(-a)$ is divisible by n, too. Thus

$$a \oplus R_n(-a) = R_n(a + R_n(-a)) = 0.$$

Hence, $R_n(-a) \in \mathbb{Z}_n$ is the additive inverse of a.

We have now established the following:

Theorem 3. *Let $n \in \mathbb{N}$. Then $(\mathbb{Z}_n, \oplus)$ is an abelian group.*

The group-theoretic nature of $\mathbb{Z}_n$ under multiplication modulo n is a bit more subtle, because not every element of $\mathbb{Z}_n$ necessarily has a multiplicative inverse. For instance consider $2 \in \mathbb{Z}_4$. If $a \otimes 2 = 1$ in $\mathbb{Z}_4$, we would then have

$$2 = 1 \otimes 2 = (a \otimes 2) \otimes 2 = a \otimes (2 \otimes 2) = a \otimes 0 = 0,$$

which is impossible. This means that 2 *cannot* have a multiplicative inverse in $\mathbb{Z}_4$.

It turns out that it is not difficult to completely characterize the elements of $\mathbb{Z}_n$ with multiplicative inverses by using Bézout's Lemma. Let $a, b \in \mathbb{Z}_n$ and suppose that $a \otimes b = 1$. This means that $R_n(ab) = 1$, so that there is an integer q satisfying $ab = qn + 1$. If we rewrite this as $ab - qn = 1$, we find that neither a nor b can have any positive (integer) factors in common with n other than 1, since any such factor necessarily divides $ab - qn$. This implies that $(a, n) = (b, n) = 1$. Put another way, any member of $\mathbb{Z}_n$ with a multiplicative inverse must be *relatively prime* (or *coprime*) to n.

Bézout's Lemma implies that the converse is also true. To see why, suppose $a \in \mathbb{Z}_n$ and $(a, n) = 1$. Then according to Bézout's Lemma there exist $r, s \in \mathbb{Z}$ so that $ra + sn = 1$. It follows that $ra - 1$ is divisible by n so that by Lemma 1 we have

$$a \otimes r = R_n(ar) = R_n(1) = 1.$$

However, we need not have $r \in \mathbb{Z}_n$. So we replace it with its remainder $R_n(r)$. First,

$$ar - aR_n(r) = a(r - R_n(r))$$

is divisible by n. So by Lemma 1 we now have

$$a \otimes R_n(r) = R_n(aR_n(r)) = R_n(ar) = 1,$$

which shows that $R_n(r)$ is a multiplicative inverse for a in $\mathbb{Z}_n$. We have now proven:

Theorem 4. *Let $n \in \mathbb{N}$ and set*

$$\mathbb{Z}_n^\times = U(n) = \{a \in \mathbb{Z}_n \,|\, (a, n) = 1\}.$$

Then $(\mathbb{Z}_n^\times, \otimes)$ is an abelian group.

Notice that our computations above show that the multiplicative inverse of $a \in \mathbb{Z}_n^\times$ is (the remainder of) the coefficient r in the Bézout relation $ra + sn = 1$. This means that the computation of multiplicative modular inverses requires a constructive proof of Bézout's Lemma. As we have already noted, the proof we have given above is insufficient in this regard, but an efficient constructive proof is readily available elsewhere.

Remark. Although we haven't stated them in quite this form, in the course of our work above we have effectively proven the following identities:

$$a \oplus b = a \oplus R_n(b), \tag{3}$$

$$a \otimes b = a \otimes R_n(b), \tag{4}$$

for all $a, b \in \mathbb{Z}$. These can be used to show that when performing computations involving modular arithmetic, we are free to replace any given integer with another having the same remainder upon division by n. For instance, suppose $R_n(b) = R_n(c)$. Then

$$a \otimes b = a \otimes R_n(b) = a \otimes R_n(c) = a \otimes c.$$

As an example, suppose we are working modulo 9 and need to compute the powers of 2 modulo 9. The first three are 2, 4 and 8. But $8 - (-1)$ is divisible by 9, so we can replace 8 by -1 and continue to multiply by 2. We then have -2, -4 and -8. These have the remainders 7, 5 and 1, respectively. At this point we find that continuing to multiply by 2 will simply cycle through the powers already found, so that the powers of 2 in $\mathbb{Z}_9^\times$ are $\{1, 2, 4, 8, 7, 5\}$. This is a simple example, to be sure, but the technique we have employed can be extremely useful in other settings.