More modular arithmetic

Last time, for any given positive integer n, we introduced the set $\mathbb{Z}_n$, which is obtained from $\mathbb{Z}$ by identifying integers which differ by a multiple of n. We defined a group operation on $\mathbb{Z}_n$ called "+" which is inherited from addition in $\mathbb{Z}$. In this lecture we continue studying further algebraic properties and structures on $\mathbb{Z}_n$.

Another natural operation to consider on $\mathbb{Z}_n$ is multiplication: writing $a \pmod n$ for the equivalence class of $a \in \mathbb{Z}$, we define the product of $a \pmod n$ and $b \pmod n$ to be $ab \pmod n$. Alternatively, if we write $[a]$ for the equivalence class of $a \in \mathbb{Z}$, our definition is:

$$[a][b] = [ab]$$

This is well-defined: if $[a'] = [a]$ and $[b'] = [b]$, then $a' - a = nk$ and $b' - b = nl$ for some $k, l \in \mathbb{Z}$, so $a'b' - ab = a'(b' - b) + b(a' - a) = n(la' + kb)$, and therefore $[a'b'] = [ab]$.

▶ **The operations of addition and multiplication on $\mathbb{Z}_n$ satisfy the properties:**

$$\begin{array}{r|l}
\text{(Associativity for } +) & a + (b + c) \equiv (a + b) + c \pmod n \\
\text{(Associativity for } \times) & a(bc) \equiv (ab)c \pmod n \\
\text{(Identity for } +) & a + 0 \equiv 0 + a \equiv a \pmod n \\
\text{(Identity for } \times) & 1 \cdot a \equiv a \cdot 1 \equiv a \pmod n \\
\text{(Inverses for } +) & a + (-a) \equiv (-a) + a \equiv 0 \pmod n \\
\text{(Distributivity)} & a(b + c) \equiv ab + ac \pmod n \\
\text{(Commutativity for } +) & a + b \equiv b + a \pmod n \\
\text{(Commutativity for } \times) & ab \equiv ba \pmod n
\end{array}$$

In short, all the formal properties you are familiar with in $\mathbb{Z}$ hold in $\mathbb{Z}_n$. A structure with two operations ("addition" and "multiplication") satisfying all of the above formal properties is called a (commutative) *ring*. However we will hold off on studying general rings.

Included in the above list are the axioms for $(\mathbb{Z}_n, +)$ to be an abelian group. However, except in the degenerate case $n = 1$ for which $0 \equiv 1 \pmod 1$, the set $\mathbb{Z}_n$ with *multiplication* does not form a group. This is because $0 \in \mathbb{Z}_n$ does not have a multiplicative inverse. The problem is not just 0, however. For example, in $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ we have:

$$2 \cdot 0 \equiv 0 \pmod 4, \quad 2 \cdot 1 \equiv 2 \pmod 4, \quad 2 \cdot 2 \equiv 0 \pmod 4, \quad 2 \cdot 3 \equiv 2 \pmod 4$$

Thus there is no element of $\mathbb{Z}_4$ which is a multiplicative inverse for 2; such an element $x \in \mathbb{Z}_4$ would have to have $2 \cdot x \equiv 1 \pmod 4$. After reviewing some basic properties of the integers we will show how to "correct" this problem, by eliminating certain elements from $\mathbb{Z}_n$ so that it becomes a group with multiplication.

The group $\mathbb{Z}_n^\times$

An integer d is a *divisor* of an integer a if $a = dk$ for some $k \in \mathbb{Z}$. An positive integer d is a *greatest common divisor* of a and b, written $d = \gcd(a,b)$, if it satisifes the following property: for any integer d' dividing both a and b, we have that d' divides d. A good exercise is to check that there is a unique greatest common divisor for any $a, b \in \mathbb{Z}$. As an example, we have $\gcd(9,24) = 3$. The key property we are after is:

▶ **Let $a, b \in \mathbb{Z}$ be non-zero integers. Then there exist integers $r, s \in \mathbb{Z}$ such that**

$$\gcd(a,b) = ar + bs$$

As an illustration, we can see directly that this is true for $a = 9, b = 24$:

$$9(3) + 24(-1) = 3$$

so upon choosing $r = 3, s = -1$ we have the desired relation.

To prove the statement in general, we proceed by considering the subset of $\mathbb{Z}$ defined by

$$S = \{am + bn : \; m, n \in \mathbb{Z}, \; am + bn > 0\}$$

As a, b are non-zero, the set S is non-empty. For example, with $m = a$ and $n = b$ we have $am + bn = a^2 + b^2 > 0$, so $a^2 + b^2$ is in S. Let d be the smallest element in S. Then $d = ar + bs$ for some $r, s \in \mathbb{Z}$. The claim is that $d = \gcd(a,b)$. To prove this we use division with remainder for integers, applied to a divided by d: that is, we can write

$$a = dq + r'$$

where $q, r' \in \mathbb{Z}$ and $0 \leqslant r' < d$ (the remainder). We can then write

$$r' = a - dq = a - (ar + bs)q = a(1 - rq) - b(sq)$$

If $r' > 0$ then $r' \in S$ and is less than d, a contradiction to our minimality assumption on d. Thus $r' = 0$, and $a = dq$, so d divides a. A similar argument shows d divides b. Thus d divides both a and b. Finally, we must show that if d' divides both a and b then it divides d. If d' divides a then $a = d'k$ and if d' divides b then $b = d'l$. So $d = ar + bs = d'kr + d'ls = d'(kr + ls)$, and thus d' divides d. Therefore $d = \gcd(a,b)$. This completes the proof.

▶ **In $\mathbb{Z}_n$, $a \pmod n$ has a multiplicative inverse if and only if $\gcd(a,n) = 1$.**

To see this, first suppose $a \pmod n$ has a multiplicative inverse, i.e. there is some integer b such that $ab \equiv 1 \pmod n$, or equivalently $ab - 1 = nk$ for some integer k. Thus $ab - nk = 1$. If d divides a and n, it divides $ab - nk = 1$, so d divides 1. Thus $\gcd(a,n) = 1$. Conversely, suppose $\gcd(a,n) = 1$. There exists $r, s \in \mathbb{Z}$ such that $\gcd(a,n) = ar + ns$. Then $ar - 1 = -ns$, so $ar \equiv 1 \pmod n$. Thus $r \pmod n$ is a multiplicative inverse for $a \pmod n$.

If $\gcd(a, b) = 1$ then a, b are said to be *relatively prime*. This motivates the following definition: we let $\mathbb{Z}_n^\times$ denote the subset of $\mathbb{Z}_n$ consisting of elements relatively prime to n:

$$\mathbb{Z}_n^\times = \{ \ a \pmod{n} : \quad \gcd(a, n) = 1 \ \}$$

▶ **The set $\mathbb{Z}_n^\times$ equipped with the operation of multiplication defines a group.**

Let us look at some examples. First, consider the integers mod 4, i.e. $\mathbb{Z}_4$. Then we have

$$\mathbb{Z}_4^\times = \{1, 3\} \subset \mathbb{Z}_4 = \{0, 1, 2, 3\}$$

As is often done, we have just written "1" etc. for the equivalence class "1 (mod 4)" which we also previously wrote as "[1]". In conclusion, $\mathbb{Z}_4^\times$ is a finite abelian group of order 2.

Next, consider $\mathbb{Z}_{10}$, the integers modulo 10. In this case we find:

$$\mathbb{Z}_{10}^\times = \{1, 3, 7, 9\} \subset \mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

Thus $\mathbb{Z}_{10}^\times$ is a finite abelian group of order 4. For example, $3 \cdot 7 \equiv 21 \equiv 1 \pmod{10}$, so the inverse of $3 \pmod{10}$ is $7 \pmod{10}$, and conversely. Here is the Cayley table for $(\mathbb{Z}_{10}^\times, \times)$:

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

When n is a prime number p, then $\mathbb{Z}_p^\times = \{1, \ldots, p-1\}$. For example, $\mathbb{Z}_7^\times = \{1, 2, 3, 4, 5, 6\}$.

▶ **Suppose $\gcd(a, n) = 1$ and b any integer. Then the equation in $\mathbb{Z}_n$ given by**

$$ax \equiv b \pmod{n}$$

can always be solved for x, and the solution x is unique as an element of $\mathbb{Z}_n$.

To see that this statement is true, we use the fact that $a \pmod{n}$ has an inverse in $\mathbb{Z}_n^\times$ and multiply both sides of the equation by this inverse.

For example, consider the equation $7x \equiv 6 \pmod{10}$ in $\mathbb{Z}_{10}$. Then multiply both sides by $3 \pmod{10}$ to get $x \equiv 18 \equiv 8 \pmod{10}$. On the other hand, we saw earlier that $2x \equiv 1 \pmod{4}$ has no solutions, but in this case $\gcd(2, 4) = 2 \neq 1$.

Euclidean Algorithm

Above we have seen that $a \pmod n$ is invertible in $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$. In practice, how can we find the inverse? We use the Euclidean algorithm.

The algorithm takes two integers a, b and computes $\gcd(a, b)$. By recording each step of the algorithm one has the information to find $r, s \in \mathbb{Z}$ such that

$$ar + bs = \gcd(a, b).$$

In the case that $b = n$ and $\gcd(a, n) = 1$, the inverse of $a \pmod n$ is given by $r \pmod n$.

The algorithm is as follows. Assume $a > b > 0$. Set $r_1 = a$, $r_2 = b$. Divide a by b to obtain

$$r_1 = r_2 q_1 + r_3$$

where $0 \leqslant r_3 < r_2$ is the remainder. Continue in this fashion to obtain a sequence of non-negative integers $r_1, r_2, r_3, \ldots$: if one has computed up to r_k, then divide r_{k-1} by r_k to obtain

$$r_{k-1} = r_k q_{k-1} + r_{k+1}$$

where $0 \leqslant r_{k+1} < r_k$ is the remainder. As each r_k is non-negative and smaller than the previous entry r_{k-1}, this process must eventually stop. The last non-zero r_k obtained is $\gcd(a, b)$!

Let us do a simple example: $a = 17$, $b = 11$. We compute:

$$\begin{aligned} 17 &= 11 \cdot 1 + 6 & \qquad 6 &= 17 - 11 \\ 11 &= 6 \cdot 1 + 5 & 5 &= 11 - 6 \\ 6 &= 5 \cdot 1 + 1 & 1 &= 6 - 5 \end{aligned}$$

The left column shows the algorithm as described; it terminates at "1" which is $\gcd(17, 11)$. But we can say more! In the right column we have rearranged each equation to solve for the remainder. Now starting from "1" (the gcd) we continually substitute the expressions in the right column to obtain an end result in terms of the original $a = 17$ and $b = 11$:

$$\begin{aligned} \gcd(17, 11) = 1 &= 6 - 5 \\ &= (17 - 11) - (11 - 6) \\ &= 17 - 2(11) + 6 \\ &= 17 - 2(11) + (17 - 11) \\ &= 2(17) - 3(11) \end{aligned}$$

In particular, we see that $-3(11) \equiv 1 \pmod{17}$, and so $-3 \pmod{17}$, which is the same as $14 \pmod{17}$, is the inverse of $11 \pmod{17}$.