LECTURE 12

Modular Arithmetic

The following rules for adding and multiplying even and odd integers should be familar.

$$\begin{array}{ll} e+e=e & e\cdot e=e \\ e+o=o & e\cdot o=e \\ o+o=e & o\cdot o=o \end{array}$$

That is to say, the sum of two even integers is always an even integer, the sum of an even and an odd integer is always an odd integer, etc. These simple rules actually provide us with a primitive sort of arithmetic that we can define for the two elements of

$$\mathbb{Z}_2 = \{[0]_2, [1]_2\} = \{\{\text{even integers}\}, \{\text{odd integers}\}\}$$

This begs the question: can we define operations like addition and subtraction on a more general $\mathbb{Z}_n$;

$$\begin{array}{rcl} [a]_n + [b]_n & = & ? \\ [a]_n \times [b]_n & = & ? \end{array} \tag{1}$$

Because $[a]_n$ and $[b]_n$ are infinite sets rather than numbers, it is not so clear how one can combine them in such a way as to get another element of $\mathbb{Z}_n$. Here is a *tentative* definition for the right hand side of (1)

$$\begin{array}{rcl} [a]_n + [b]_n & = & [a+b]_n \\ [a]_n \times [b]_n & = & [ab]_n \end{array} , \tag{2}$$

that is to say, the "sum" of the congruence class of a and the congruence class of b is the congruence class of $a+b$, and the "product" of the congruence class of a and the congruence class of b is the congruence class of ab. Even more explicitly,

$$\begin{array}{rl} & \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\} \text{ '+' } \{\ldots, b-2n, b-n, a, b+n, b+2n, \ldots\} \\ \equiv & {}^{def} \{\ldots, a+b-2n, a+b-n, a+b, a+b+n, a+b+2n, \ldots\} \end{array}$$

and

$$\begin{array}{rl} & \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\} \text{ '}\cdot\text{' } \{\ldots, b-2n, b-n, a, b+n, b+2n, \ldots\} \\ \equiv & {}^{def} \{\ldots, ab-2n, ab-n, ab, ab+n, ab+2n, \ldots\} \end{array}$$

However, there may be a problem with such a naive definition of addition and subtraction: How do we know that it's self-consistent?

Example:

Consider the following three sets

$$\begin{array}{rcl} P & = & \{\text{prime numbers}\} \\ C & = & \{\text{composite numbers}\} \\ A & = & \{-1, 0, 1\} \end{array}$$

and set $\mathbb{X} = \{P, C, A\}$. Just as in the situation for congruence classes, every integer $z \in \mathbb{Z}$ is an element of one and only one of these three sets. Let (z), $z \in \mathbb{Z}$, denote the set (P, C, or A) containing z. Thus,

$$\begin{aligned} P &= (\pm 2) = (\pm 3) = (\pm 5) = \cdots \\ C &= (\pm 4) = (\pm 6) = (\pm 8) = \cdots \\ A &= (-1) = (0) = (1) \quad . \end{aligned}$$

Now, to define the sum of two elements of $\mathbb{X}$, we might try setting

$$(x) + (y) = (x + y) \quad ; \tag{3}$$

however, this turns out to be inconsistent. For

$$P = (2) = (3) = (5)$$

but according to (3)

$$P + P = (2) + (3) = (5) = P$$

and

$$P + P = (5) + (3) = (8) = C \quad .$$

Thus, this definition of addition is not self-consistent.

The basic problem with the example above is that the result of the addition defined by $(x) + (y) = (x + y)$ depends on the choice of the "representatives" x and y one chooses from the sets P and C, and A. In order to show that the definition (**??**) of addition and multiplication in $\mathbb{Z}_n$ is self-consistent, we must first prove that these operations do not depend on how we choose representatives $a + ns \in [a]$ and $b + nt \in [b]$.

THEOREM 12.1. *If* $[a]_n = [b]_n$ *and* $[c]_n = [d]_n$ *in* $\mathbb{Z}_n$, *then*

$$[a + c]_n = [b + d]_n \qquad \text{and} \qquad [ac]_n = [bd]_n \quad .$$

Proof.

By Theorem 2.3, since $[a]_n = [b]_n$ we know that $a \equiv b \pmod{n}$. Similarly, $c \equiv d \pmod{n}$. Therefore,

$$a - b = kn \qquad \text{for some } k \in \mathbb{Z} \tag{4}$$

$$c - d = k'n \qquad \text{for some } k' \in \mathbb{Z} \tag{5}$$

Adding these two equations, we get

$$a + c - (b + d) = (k + k')\, n$$

and so

$$a + c \equiv b + d \pmod{n}.$$

Hence by Theorem 2.3 again

$$[a + c]_n = [b + d]_n \quad .$$

Next, let's rewrite (4) and (5) as

$$\begin{aligned} a &= b + kn \\ c &= d + k'n \end{aligned}$$

The product of the left hand sides must equal the products of the right hand sides so

$$ac = (b + kn)\,(d + k'n) = bd + n\,(kd + k'b + kk'n) \quad \Rightarrow \quad ac \equiv bd \pmod{n}$$

and so by Theorem 2.3

$$[ac]_n = [bd]_n$$

□

Because of this theorem we now know that the following formal definition of addition and multiplication is independent of the choice of representatives from each congruence class.

DEFINITION 12.2. *Addition and multiplication in $\mathbb{Z}_n$ are defined by*

$$[a]_n \oplus [b]_n = [a+b]_n$$

and

$$[a]_n \times [b]_n = [ab]_n \quad .$$

Recall that a binary operation on a set S is a rule for associating with any pair of elements $\{a, b\}$ of S another element $a \star b$ of S. Last time we were discussing how to define binary operations on congruence classes corresponding to the operations of addition and multiplication in $\mathbb{Z}$. This is was seen to be a little tricky, since not only do we have to define a rule for combining sets of integers that is also a binary operation (set union does not work), but it also has to be self-consistent. We were led to the above definition; viz.,

$$[a]_n \oplus [b]_n \equiv [a+b]_n$$

and

$$[a]_n \times [b]_n \equiv [ab]_n \quad .$$

This at least seems to be a binary operation on $\mathbb{Z}_n$ since the congruence classes $[a]_n$, $[b]_n$, $[a+b]_n$, and $[ab]_n$ are all elements of $\mathbb{Z}_n$. But note that in order to compute the sum or product of two congrence classes, say A and B in $\mathbb{Z}_n$, we first have to choose integers a and b "representing" each class,

$$\begin{aligned} A &= [a]_n \\ B &= [b]_n \end{aligned}$$

and then (and only then) we can define the sum $A \oplus B$ as the congruence class of $a+b$ and the product of $A \times B$ as the congruence class of ab. The cruxt of the matter is that this method of computing $A \oplus B$ and $A \times B$ is self-consistent in the following sense

(i) If $[a]$ is the same congruence class as $[c]_n$ and $[b]_n$ is the same congruence class as $[d]_n$, then we need

$$[a]_n \oplus [b]_n = [c]_n \oplus [d]_n \quad .$$

(ii) If $[a]$ is the same congruence class as $[c]$ and $[b]$ is the same congruence class as $[d]$, then we need

$$[a]_n \times [b]_n = [c]_n \times [d]_n \quad .$$

These two conditions are guaranteed by the following theorem.

THEOREM 12.3. *If $[a]_n = [b]_n$ and $[c]_n = [d]_n$ in $\mathbb{Z}_n$, then*

$$[a+c]_n = [b+d]_n \qquad \textit{and} \qquad [ac]_n = [bd]_n \quad .$$

Proof.

By Theorem 2.3, since $[a]_n = [b]_n$ we know that $a \equiv b \pmod{n}$. Similarly, $c \equiv d \pmod{n}$. Therefore, by Theorem 2.2,

$$a + c \equiv b + d \pmod{n} \qquad \text{and} \qquad ac \equiv bd \pmod{n} \quad .$$

Hence by Theorem 2.3 again

$$[a+c]_n = [b+d]_n \qquad \text{and} \qquad [ac]_n = [bd]_n \quad .$$

□

Example:

Let's compute the addition and multiplication tables for $\mathbb{Z}_3$. In this case we have only three distinct congruence classes; $[0]_3$, $[1]_3$, and $[2]_3$.

$$\begin{aligned}
[0]_3 + [0]_3 &= [0+0]_3 = [0]_3 \\
[0]_3 + [1]_3 &= [0+1]_3 = [1]_3 \\
[0]_3 + [2]_3 &= [0+2]_3 = [2]_3 \\
[1]_3 + [0]_3 &= [1+0]_3 = [1]_3 \\
[1]_3 + [1]_3 &= [1+1]_3 = [2]_3 \\
[1]_3 + [2]_3 &= [1+2]_3 = [3]_3 = [0]_3 \\
[2]_3 + [0]_3 &= [2+0]_3 = [2]_3 \\
[2]_3 + [1]_3 &= [2+1]_3 = [3]_3 = [0]_3 \\
[2]_3 + [2]_3 &= [2+2]_3 = [4]_3 = [1]_3
\end{aligned}$$

$$\begin{aligned}
[0]_3 \times [0]_3 &= [0 \cdot 0]_3 = [0]_3 \\
[0]_3 \times [1]_3 &= [0 \cdot 1]_3 = [0]_3 \\
[0]_3 \times [2]_3 &= [0 \cdot 2]_3 = [0]_3 \\
[1]_3 \times [0]_3 &= [1 \cdot 0]_3 = [0]_3 \\
[1]_3 \times [1]_3 &= [1 \cdot 1]_3 = [1]_3 \\
[1]_3 \times [2]_3 &= [1 \cdot 2]_3 = [2]_3 \\
[2[\times [0]_3 &= [2 \cdot 0]_3 = [0]_3 \\
[2]_3 \times [1]_3 &= [2 \cdot 1]_3 = [2]_3 \\
[2]_3 \times [2]_3 &= [2 \cdot 2]_3 = [4]_3 = [1]_3
\end{aligned}$$

THEOREM 12.4. *For any classes $[a]_n$, $[b]_n$, $[c]_n$ in $\mathbb{Z}_n$,*

(1) *If $[a]_n \in \mathbb{Z}_n$ and $[b]_n \in \mathbb{Z}_n$, then $[a]_n + [b]_n \in \mathbb{Z}_n$.*
(2) $[a]_n + ([b]_n + [c]_n) = ([a]_n + [b]_n) + [c]_n$.
(3) $[a]_n + [b]_n = [b]_n + [a]_n$.
(4) $[a]_n + [0]_n = [a]_n$.
(5) *For each $[a]_n \in \mathbb{Z}_n$, the equation $[a]_n + X = [0]_n$, has a solution in $\mathbb{Z}_n$.*
(6) *If $[a]_n \in \mathbb{Z}_n$ and $[b]_n \in \mathbb{Z}_n$, then $[a]_n \times [b]_n \in \mathbb{Z}_n$.*
(7) $[a]_n \times ([b]_n \times [c]_n) = ([a]_n \cdot [b]_n) \cdot [c]_n$.
(8) $[a]_n \times ([b]_n + [c]_n) = ([a]_n \times [b]_n) + ([a]_n \times [c]_n)$.
(9) $[a]_n \times [b]_n = [b]_n \times [a]_n$.
(10) $[a]_n \times [1]_n = [a]_n$.

New Notation:

When it is clear from the context that we are working in $\mathbb{Z}_n$ we shall often denote a congruence class $[a]_n$ by simply a and the operations $+$ and $\times$ on $\mathbb{Z}_n$ by simply $+$ and $\cdot$. Thus, for example in the context of arithmetic in $\mathbb{Z}_3$, you might see

$$1 + 2 = 0$$

because

$$[1]_3 + [2]_3 = [3]_3 = [0]_3 \quad .$$