9. Congruence classes (continued)

Definition. Let R be a ring with 1. An element $a \in R$ is called invertible if there exists $b \in R$ such that $ab = ba = 1$.

Theorem 9.1. *Let $n \geq 2$ be an integer. Then an element $[a] \in \mathbb{Z}_n$ is invertible $\iff$ a and n coprime.*

Proof. See Theorem 2.31 in Section 2.6 of the book. □

Corollary 9.2. *Let $n \geq 2$ be an integer. Then $\mathbb{Z}_n$ is a field $\iff$ n is prime.*

Proof. See Corollary 2.32 in Section 2.6 of the book. □

Example 1. *Let n be a prime. Find all $z \in \mathbb{Z}_n$ such that $z^2 = [1]$.*

Solution 1: (working inside $\mathbb{Z}_n$) Suppose that $z^2 = [1]$. Subtracting $[1]$ from both sides, we get $z^2 - [1] = [0]$. Since $[1] = [1]^2$, we get

$$(z - [1])(z + [1]) = [0]. \qquad (***)$$

Since n is prime, $\mathbb{Z}_n$ is a field. Hence by HW #1.2, we conclude from (***) that $z - [1] = 0$ or $z + [1] = 0$. Thus, either $z = [1]$ or $z = -[1] = [-1] = [n-1]$.

So far we showed that equality $z^2 = [1]$ implies $z = [1]$ or $z = [n-1]$, so there are at most two solutions. To check that $[1]$ and $[n-1]$ are indeed solutions, we plug them into the original equation: $[1]^2 = [1^2] = [1]$ and $[n-1]^2 = [-1]^2 = [(-1)^2] = [1]$, so both 1 and $[n-1]$ are solutions.

Final answer: $z = [1]$ or $[n-1]$.

Solution 2: (reducing to question about integers) We know that $z = [x]$ for some $x \in \mathbb{Z}$. Thus our equation is $[x]^2 = [1]$ which can be rewritten as $[x^2] = [1]$. The latter means that $x^2 \equiv 1 \mod n$, that is, $n \mid (x^2 - 1)$.

Thus, $n \mid (x-1)(x+1)$, and by Euclid's lemma (recall that n is prime), we have $n \mid (x-1)$ or $n \mid (x+1)$. Hence either $x \equiv 1 \mod n$, in which case $[x] = [1]$, or $x \equiv -1 \mod n$, in which case $[x] = [-1] = [n-1]$. As in Solution 1, we check that $z = [1]$ and $z = [n-1]$ are solutions by plugging them into the original equation.

Exercise 1. *Show (by an explicit example) that if n is not prime, the equation $z^2 = [1]$ may have more than 2 solutions (this is true for some, but not all non-prime n).*

We finished the lecture by discussing the connection between the ring $\mathbb{Z}_n$ introduced in Lecture 8 (referred below as "new" $\mathbb{Z}_n$) and the "hypothetical ring $\mathbb{Z}_n$" discussed in Lecture 2 (referred below as "old" $\mathbb{Z}_n$). Recall that in Lecture 2 we defined $\mathbb{Z}_n$ to be the set of integers $\{0, 1, \dots, n-1\}$ and asked the following question: can we define operations $\oplus$ and $\odot$ on $\mathbb{Z}_n$ such that

(i) $\mathbb{Z}_n$ with these operations is a commutative ring with 1

(ii) $x \oplus y = x + y$ whenever $0 \leq x + y \leq n - 1$ and $x \odot y = xy$ whenever $0 \leq xy \leq n - 1$ (where the sum and the product on the right-hand sides are the usual addition and multiplication)?

We can now answer this question in the affirmative: take the addition and multiplication tables for the new $\mathbb{Z}_n$, remove all the brackets and relabel the operations as $\oplus$ and $\odot$. Then it is easy to see (i) and (ii) will hold.

A natural question is whether there are explicit formulas for $\oplus$ and $\odot$ on the "old" $\mathbb{Z}_n$. The answer is yes, but we need an additional notation. Given $x \in \mathbb{Z}$, denote by $\overline{x}$ the remainder of dividing x by n (that is, $\overline{x}$ is the unique integer between 0 and $n-1$ such that $x \equiv \overline{x} \mod n$). Then the operations $\oplus$ and $\odot$ on the "old" $\mathbb{Z}_n$ are given by the formulas

$$x \oplus y = \overline{x + y} \quad \text{and} \quad x \odot y = \overline{xy} \qquad (***)$$

One may wonder now why we had to define $\mathbb{Z}_n$ in a fancy way as the set of congruence classes mod n instead of presumably simpler old definition $\mathbb{Z}_n = \{0, 1 \dots, n-1\}$ with operations defined by (***). The answer is that if operations were defined by (***), it would have required much more work to verify the ring axioms. In addition, the fact that in the new definition we can consider $[x]$ as an element of $\mathbb{Z}_n$ for every $x \in \mathbb{Z}$ (not just x between 0 and $n-1$) turns out to be extremely convenient.