9. Congruence classes (continued)

Definition. Let R be a ring with 1. An element $a \in R$ is called <u>invertible</u> 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. "$\Rightarrow$" Suppose that $[a] \in \mathbb{Z}_n$ is invertible. This means that $[a][k] = [1]$ for some $k \in \mathbb{Z}$ or, equivalently $[ak] = [1]$ for some $k \in \mathbb{Z}$. Hence $ak \equiv 1 \mod n$, so $1 - ak = nl$ for some $k, l \in \mathbb{Z}$ or, equivalently, $ak + nl = 1$. Since $gcd(a, n)$ divides both a and n and hence also divides $ak + nl$, this forces $gcd(a, n) = 1$, so a and n are coprime.

"$\Leftarrow$" Suppose a and n are coprime. Then by GCD Theorem there exist $k, l \in \mathbb{Z}$ such that $ak + nl = 1$. From this point we can argue as in the proof of "$\Rightarrow$" (but reversing the order of steps) to conclude that $[a]$ is invertible in $\mathbb{Z}_n$. □

9.1. Zero divisors in $\mathbb{Z}_n$.

Definition. Let R be a commutative ring. An element $a \in R$ is called a <u>zero divisor</u> if a is nonzero and there exists a nonzero element $b \in R$ such that $ab = 0$.

For instance, the element [2] of the ring $R = \mathbb{Z}_6$ is a zero divisor. Indeed, $[2] \neq [0]$ since $6 \nmid (2 - 0)$ and similarly $[3] \neq [0]$. But $[2] \cdot [3] = [6] = [0]$.

We already know that fields have no zero divisors – this is precisely the assertion of Problem 2 in HW#1. Thus, the existence of zero divisors in $\mathbb{Z}_6$ provides another proof of the fact that $\mathbb{Z}_6$ is not a field (we have already established this in Lecture 8 after computing the multiplication table). The converse of the above statement is not true, that is, if R is a commutative ring with 1 without zero divisors, then R does not have to be a field (e.g. integers $\mathbb{Z}$ is not a field, but does not have zero divisors). It turns out, however, that for the rings of congruence classes $\mathbb{Z}_n$ being a field is equivalent to having no zero divisors, and both conditions hold if and only if n is prime:

Theorem 9.2. *Let $n \geq 2$ be an integer. The following are equivalent:*

(1) *n is prime*
(2) *$\mathbb{Z}_n$ is a field*
(3) *$\mathbb{Z}_n$ has no zero divisors*

Proof. We will prove the equivalence of these three conditions "cyclically" by first showing the implication (1)⇒(2), then (2)⇒(3) and finally (3)⇒(1).

"(1)⇒(2)" Recall that a field is a commutative ring with 1 in which every nonzero element is invertible and $0 \neq 1$. Assume that n is prime. Since $n \geq 2$, we clearly have $[0] \neq [1]$ in $\mathbb{Z}_n$. Since $\mathbb{Z}_n \setminus \{[0]\} = \{[1], [2], \ldots, [n-1]\}$, it remains to show that $[a]$ is invertible in $\mathbb{Z}_n$ for every $1 \leq a \leq n-1$. Since n is prime, every such a is coprime to n, so by Theorem 9.1, $[a]$ is invertible in $\mathbb{Z}_n$ for every such a.

"(2)⇒(3)" This implication holds since a field cannot have zero divisors by HW#1.2 (no specific properties of $\mathbb{Z}_n$ are used here).

"(3)⇒(1)" We will prove this implication by contrapositive: if n is not prime, then $\mathbb{Z}_n$ has zero divisors.

So assume that n is not prime. Since we also assume that $n \geq 2$, by definition of a prime number, n must have a positive divisor k different from 1 and n, in which case we must have $1 < k < n$. Thus $n = kl$ for some $l \in \mathbb{Z}$, and since $1 < k < n$, we also have $1 < l < n$. In particular, this implies that $n \nmid k$ and $n \nmid l$, so both $[k]$ and $[l]$ are nonzero elements of $\mathbb{Z}_n$. But $[k][l] = [kl] = [n] = [0]$, so $\mathbb{Z}_n$ has a zero divisor, namely $[k]$. □

9.2. **Solving equations in $\mathbb{Z}_n$.**

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).*

9.3. **Some concluding remarks.** 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 $\{0,1,\ldots,n-1\}$ 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 $\mathbb{Z}_n=\{0,1\ldots,n-1\}$ 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.