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.** “⇒” 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 $ak \equiv 1 \pmod{n}$, 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.

“⇐” 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 “⇒” (but reversing the order of steps) to conclude that $[a]$ is invertible in $\mathbb{Z}_n$. □

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

**Proof.** It will be convenient to start by formulating explicitly what it means for $\mathbb{Z}_n$ to be a field. We already know that $\mathbb{Z}_n$ is a commutative ring with 1 (and 1 \neq 0 in $\mathbb{Z}_n$ since $n \geq 2$). Thus $\mathbb{Z}_n$ is a field $\iff$ every nonzero element of $\mathbb{Z}_n$ is invertible. Since $\mathbb{Z}_n \setminus \{[0]\} = \{[1], [2], \ldots, [n - 1]\}$, we conclude that $\mathbb{Z}_n$ is a field $\iff [a]$ is invertible in $\mathbb{Z}_n$ for every $a \in \mathbb{Z}$ with $1 \leq a \leq n - 1$.

We now proceed with the proof.

“⇐” Suppose that $n$ is prime. Then every integer $a$ with $1 \leq a \leq n - 1$ is coprime to $n$, so by Theorem 9.1, $[a]$ is invertible in $\mathbb{Z}_n$ for every such $a$. The first paragraph of the proof now implies that $\mathbb{Z}_n$ is a field.

“⇒” We will prove this direction by contrapositive (if $n$ is not prime, then $\mathbb{Z}_n$ is not a field). So assume that $n$ is not prime. Since $n \geq 2$, this means that $n = ab$ for some integers $a, b$ with $1 < a, b < n$. Then $a$ is NOT coprime to $n$, so (again by Theorem 9.1), $[a]$ is not invertible in $\mathbb{Z}_n$. Since $1 \leq a \leq n - 1$, the first paragraph of the proof shows that $\mathbb{Z}_n$ is not a field. □
**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

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

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 $z = -[1] = [n-1]$.

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 $[n-1]^2 = [(-1)^2] = [1]$, 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 $\{0, 1, \ldots, n-1\}$ 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

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

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 $\overline{x}$ 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.