Summary on Lecture 9, April 15th, 2015

Integers mod n.

Recall an important example. Let $n \in \mathbf{Z}_+$ be a positive integer. We define an equivalence relation on $\mathbf{Z}$ as follows: $m \sim m'$ iff $m - m'$ is divisible by n. Then we have n different classes of equivalent integers:

$$\begin{array}{ccl} \mathbf{0} & := & \{0, \pm n, \pm 2 \cdot n, \ldots\}, \\ \mathbf{1} & := & \{1, 1 \pm n, 1 \pm 2 \cdot n, \ldots\}, \\ \mathbf{2} & := & \{2, 2 \pm n, 2 \pm 2 \cdot n, \ldots\}, \\ \cdots & & \cdots\cdots\cdots \\ \mathbf{n} - 1 & := & \{n-1, n-1 \pm n, n-1 \pm 2 \cdot n, \ldots\}. \end{array}$$

We obtain that $\mathbf{Z} = \bigcup_{i=0}^{n-1} \mathbf{i}$, and clearly the sets $\mathbf{i}$ and $\mathbf{i}'$ do not intersect if $i \neq i'$. The set of equivalent classes $\{\mathbf{0}, \mathbf{1}, \ldots, \mathbf{n} - 1\}$ is denoted by $\mathbf{Z}/n$. There are well-defined sum and product operations on $\mathbf{Z}/n$:

$$\mathbf{i} + \mathbf{i}' \quad \text{and} \quad \mathbf{i} \cdot \mathbf{i}'$$

Here are the addition and multiplication tables in $\mathbf{Z}/5$:

+	0	1	2	3	4
0	0	1	2	3	3
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Next, we have the following addition and multiplication tables in $\mathbf{Z}/6$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

We notice that $\mathbf{2} \cdot \mathbf{3} = \mathbf{0}$, $\mathbf{4} \cdot \mathbf{3} = \mathbf{0}$, and $\mathbf{3} \cdot \mathbf{3} = \mathbf{3}$.

Thus we can add and multiply numbers in $\mathbf{Z}/n = \{\mathbf{0}, \mathbf{1}, \ldots, \mathbf{n} - 1\}$. There are two special elements here: $\mathbf{0}$ and $\mathbf{1}$:

$$\mathbf{k} + \mathbf{0} = \mathbf{k}, \quad \mathbf{k} \cdot \mathbf{1} = \mathbf{k}$$

Moreover, the addition and product of integers mod n are commutative and associative:

$$\mathbf{k} + \mathbf{m} = \mathbf{m} + \mathbf{k}, \quad (\mathbf{i} + \mathbf{k}) + \mathbf{m} = \mathbf{i} + (\mathbf{k} + \mathbf{m}), \quad \text{and} \quad \mathbf{k} \cdot \mathbf{m} = \mathbf{m} \cdot \mathbf{k}, \quad (\mathbf{i} \cdot \mathbf{k}) \cdot \mathbf{m} = \mathbf{i} \cdot (\mathbf{k} \cdot \mathbf{m})$$

We call $\mathbf{Z}/n$ the *ring of integers modulo* n. Here we say that $\mathbf{Z}/n$ is a ring since it has two operations: addition $+$ and multiplication $\cdot$ which satisfy several properties:

(1) $a + b = b + a$ for all $a, b \in \mathbf{Z}/n$,
(2) $(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathbf{Z}/n$,
(3) for each $a \in \mathbf{Z}/n$ there exists $b \in \mathbf{Z}/n$ such that $a + b = \mathbf{0}$,
(4) $a \cdot b = b \cdot a$ for all $a, b \in \mathbf{Z}/n$,
(5) $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$,
(6) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in \mathbf{Z}/n$,
(7) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in \mathbf{Z}/n$,
(8) $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in \mathbf{Z}/n$.

The properties (1)–(3) mean that $\mathbf{Z}/n$ is an abelian (commutative) group with respect to the addition $+$. The properties (4)–(8) are general for a commutative ring with a unit. Please see all definitions in section 14.1.

There is one more important definition. We say that a commutative and associative ring $(R, +, \cdot)$ with a unit is a *field* if for any $a \in R$, $a \neq \mathbf{0}$, there exists a multiplicative inverse b, i.e., such that $a \cdot b = \mathbf{1}$.

We have seen that $\mathbf{Z}/5$ is a field, and $\mathbf{Z}/6$ is not a field: we have seen that $\mathbf{5} \cdot \mathbf{5} = \mathbf{1}$, however, $\mathbf{2} \cdot \mathbf{k} \neq \mathbf{1}$ for any $\mathbf{k} \in \mathbf{Z}/6$.

Lemma 1. Let $(R, +, \cdot)$ be a field. Then R does not have zero divisors, i.e. if $a \cdot b = 0$, then either $a = 0$ or $b = 0$.

Proof. Assume $a \cdot b = 0$, then if $b \neq 0$, we find b^{-1} such that $b \cdot b^{-1} = 1$. Then we multiply by b^{-1} both sides of $a \cdot b = 0$. We obtain: $a \cdot b \cdot b^{-1} = a = 0$, i.e. $a = 0$. □

Theorem 1. The ring $\mathbf{Z}/n$ is a field if and only if n is a prime integer.

Proof. Assume n is a prime integer, and $0 < k < n$. Then $\gcd(n, k) = 1$, thus there exist integers t, s such that $t \cdot n + s \cdot k = 1$. This means that $s \cdot k \equiv 1 \mod n$. Thus every such k has an inverse. Assume that n is not a prime, i.e. $n = n_1 \cdot n_2$, where $1 < n_1, n_2 < n$. We obtain that $n_1 \cdot n_2 \equiv 0 \mod n$. Thus $\mathbf{Z}/n$ cannot be a field by Lemma 1. □

An element $a \in \mathbf{Z}/n$ is a unit if there exists a multipicative inverse, i.e. such $b \in \mathbf{Z}/n$ that $a \cdot b = 1$. Say, $1, 5 \in \mathbf{Z}/6$ are units, but $2, 3, 4 \in \mathbf{Z}/6$ are not.

Theorem 2. An element $k \in \mathbf{Z}/n$ is a unit if and only if $\gcd(k, n) = 1$.

Proof. Indeed, assume $\gcd(k, n) = 1$. Then there exist integers t, s such that $t \cdot n + s \cdot k = 1$. This means that $s \cdot k \equiv 1 \mod n$. Assume there exist inverse s of k, i.e. $k \cdot s \equiv 1 \mod n$, or $k \cdot s = n \cdot t + 1$ for some t. Thus $1 = k \cdot s + n \cdot (-t)$ which mens that $\gcd(k, n) = 1$. □

Example. Recall that $2015 = 5 \cdot 13 \cdot 31$. We find the inverse of 101 in $\mathbf{Z}/2015$:

$$\begin{array}{ll} 2015 = 101 \cdot 19 + 96, & 96 = 2015 - 101 \cdot 19 \\ 101 = 96 \cdot 1 + 5, & 5 = 101 - 96 \cdot 1 \\ 96 = 5 \cdot 19 + 1, & 1 = 96 - 5 \cdot 19. \end{array}$$

We have:

$$\begin{aligned} 1 &= 96 - 5 \cdot 19 = 96 - (101 - 96 \cdot 1) \cdot 19 \\ &= 96 \cdot 20 - 101 \cdot 19 = (2015 - 101 \cdot 19) \cdot 20 \\ &= 2015 \cdot 20 - 101 \cdot 399 \end{aligned}$$

We obtain that $101 \cdot (-399) \equiv 1 \mod 2015$. We have that $-399 \equiv 1606 \mod 2015$. Thus $101^{-1} = 1606$ in $\mathbf{Z}/2015$.

Exercise. Compute 17^{-1} in $\mathbf{Z}/35$, 25^{-1} in $\mathbf{Z}/72$.

Euler function. Recall that for a for given positive integer n, consider the set of numbers m such that $1 \leq m < n$ and $\gcd(m, n) = 1$. Leonhard Euler defined the function:

$$\phi(n) = |\{ \ m \mid 1 \leq m < n, \text{ and } \gcd(m, n) = 1 \ \}|.$$

Here is the values of $\phi(n)$ for some n:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\phi(n)$	1	2	2	4	2	6	4	9	4	10	4	12	6	8	8	16

There is a simple formula to compute $\phi(n)$. Recall that for every integer n there exist primes $p_1, \ldots, p_s$ and positive $e_1, \ldots, e_s$ such that $n = p_1^{e_1} \cdots p_s^{e_s}$. Here is the formula:

$$\phi(n) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right)$$

Theorem 3. Let $n \geq 2$. Then there are exactly $\phi(n)$ units in $\mathbf{Z}/n$.