Lecture 9

Residue class Rings

<u>Def</u>. A ring is a triplet $(R, +, \cdot)$ such that:

$(R, +)$ is an abelian group,

and $(R, \cdot)$ is a semigroup.

~~If~~ In addition $\forall x, y, z \in R$

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$

$$(x + y) \cdot z = (x \cdot z) + (y \cdot z)$$

The ring is called commutative if the semigroup $(R, \cdot)$ is commutative.

A unit element of the ring is a neutral element of the semigroup.

We remind that a pair $(H, \circ)$ is a semigroup of a set H and operation $\underline{\circ}$ on H is <u>associative</u>

<u>Examples of Rings.</u>

1. The triplet $(\mathbb{Z}, +, \cdot)$ is a commutative ring with unite element 1.
2. The triplet $(\mathbb{Z}/m\mathbb{Z}, +, \circ)$ is a commutative ring with unit element $1 + m\mathbb{Z}$. This ring is called the residual class ring modulo m.

<u>Def.</u> If R is finite set, then $(R, +, \circ)$ is called a finite ring

<u>Def.</u> Let R be a ring with unit element, i.e. $(R, \circ)$ is monoid.
An element $a \in R$ is called invertible or a <u>unit element</u> if it is invertible in the multiplication semigroup of R

The element $a \in R$ is called a zero divisor if

- it is nonzero $a \neq 0$
- there is a nonzero $b \in R$ with
  $a \circ b = 0$ or $b \circ a = 0$

A test

Show that the units of a commutative ring form a group. It is called the unit group of R and is denoted by R^*.

Ex. 1. Let's consider the neutral element $\tilde{e}=1$ of ~~the~~ the multiplicative semigroup $(R, \cdot)$

It is clear, that $\tilde{e} = \tilde{e}^{-1}$, that $\tilde{e}$ is invertible, or a unit element

Ex. 2 Let's take $a \in R$ which is invertible, i.e. there exists $a^{-1} \in R$, such that $a \cdot a^{-1} = 1$

It is easy to show that

$$(a^{-1})^{-1} = a$$

thus a^{-1} is also a unit element.

Let's denote

$$(a^{-1})^{-1} = b \Rightarrow (a^{-1}) \cdot b = 1$$

But we have by the definition that

$$(a^{-1}) \cdot a = 1$$

and the inverse element is unique, thus

$$\boxed{(a^{-1})^{-1} = a}$$

Ex. 1. The ring of integers $\mathbb{Z}$ contains no zero divisors.

Th. Let's consider the residue class ring $\mathbb{Z}/m\mathbb{Z}$. The residue classes

$a + m\mathbb{Z}$ are zero divisors

if and only iff

$1 < \gcd(a, m) < m.$

Proof. Necessary condition

If $a + m\mathbb{Z}$ is a zero divisor of $\mathbb{Z}/m\mathbb{Z}$
then there is an integer b with ($b + m\mathbb{Z}$ class)

$ab \equiv 0 \mod m$ but neither

$a \equiv 0 \mod m$ nor $b \equiv 0 \mod m$
($b + m\mathbb{Z}$ is class)

Hence m is divisor of ab but not of a nor of b. This means that

$1 < \gcd(a, m) < m,$

because if $\gcd(a, m) = 1$ then m is a divisor of b.

Sufficiency.

Conversely if

$\boxed{1 < \gcd(a, m) < m}$, and take

and $b = m / \gcd(a,m)$ then

$\boxed{1 < b < m}$,

$a \not\equiv 0 \mod m$, $ab \equiv 0 \mod m$

and $b \not\equiv 0 \mod m$.

Therefore

$a + m\mathbb{Z}$ is a zero divisor of $\mathbb{Z}/m\mathbb{Z}$.

▷

Conclusion.

If m is prime, then $\mathbb{Z}/m\mathbb{Z}$ contains no zero divisors

Def. A field is a commutative ring in which every nonzero element is invertible. (i.e. $(R, \cdot)$ is abelian group), not only semigroup, as for a ring).

Example. The ring $(\mathbb{Z}, +, \cdot)$ is not a field, because most integers $x \in \mathbb{Z}$ are not invertible (with respect to multiplication).

The ring of rational numbers $(\mathbb{Q}, +, \cdot)$ is the field.

For any $a \in \mathbb{Q}$ and $a \neq 0$ there exist an inverse (it is unique number).

$$a \in \mathbb{Q} \Rightarrow a = \frac{m}{n}, \quad m, n \in \mathbb{Z}$$

and $m \neq 0$. Then

$$a^{-1} = \frac{n}{m} \Rightarrow a a^{-1} = \frac{m}{n} \cdot \frac{n}{m} = 1.$$

Example. We will see that the residue class ring $\mathbb{Z}/p\mathbb{Z}$ modulo a prime p number is a field.

Let R be a ring and let $a, n \in R$.

<u>Def.</u> We say that a divides n if there is $a, b \in R$ such that

$$n = a \cdot b.$$

Then a is called a divisor of n and n is called a multiple of a, and we write $a | n$.

Now our aim is find which elements of the residue class ring mod m are invertible.

The residue class $a + m\mathbb{Z}$ is invertible in $\mathbb{Z}/m\mathbb{Z}$ if and only if the congruence

$$a x \equiv 1 \bmod m$$

is solvable.

Th. 6. The residue class $a + m\mathbb{Z}$ is invertible in $\mathbb{Z}/m\mathbb{Z}$ if and only if

$$\gcd(a, m) = 1$$

If $\gcd(a, m) = 1$ then the inverse of $a + m\mathbb{Z}$ is uniquely determined.

Proof. Let $g = \gcd(a, m)$ and let x be a solution of

$$a \cdot x \equiv 1 \mod m.$$

Then g is a divisor of m and therefore it is a divisor of $ax - 1$.

But g is also a divisor of a.

Hence, g is a divisor 1, i.e. $g = 1$.

Conversely, let $g = 1$. Then, there are numbers x and y with

$$ax + my = 1, \text{ i.e. } ax - 1 = -my.$$

This shows that is x is a solution of

$$ax \equiv 1 \mod m.$$

and that $x + m\mathbb{Z}$ is the inverse of $a + m\mathbb{Z}$ in $\mathbb{Z}/m\mathbb{Z}$.

<u>Uniqueness.</u> Let $u + m\mathbb{Z}$ be another inverse of $a + m\mathbb{Z}$.

Then $ax \equiv au \mod m$.

Therefore m divides $a(x-u)$.

Because $\gcd(a,m) = 1$, this implies that m is a divisor of $x - u$. This gives

$$x \equiv u \mod m$$

Th.7 The residue class ring $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is a prime number.

<u>Proof</u>. By Th.6 the ring $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if

$$\gcd(k, m) = 1, \quad \forall\ 1 \le k < m.$$

This is true if and only if m is a prime number. $\triangleright$

Ex 1. Find which residue classes $a + 12\mathbb{Z}$ have inverse?
(i.e. $\gcd(a, 12) = 1$)

Ex 2. Find the inverse of $5 + 12\mathbb{Z}$
(i.e. $a = 5$, $\gcd(5, 12) = 1$)

The following result is of critical importance in cryptography.

Th. 8. The set of all invertible residue classes modulo m is a finite abelian group with respect to multiplication.

Proof. By Th. 6 this set is the <u>unit</u> group of the residue class rings mod m. ▷

This group of invertible residue classes modulo m is called the multiplicative group of residues modulo m and is written $(\mathbb{Z}/m\mathbb{Z})^*$.

Its order is the Euler φ-function $\varphi(m)$.