Lecture 9 Modular arithmetic

Let m be a positive integer.
Recall that $m\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.
The cosets of $m\mathbb{Z}$ are

$$m\mathbb{Z},\ 1+m\mathbb{Z},\ 2+m\mathbb{Z},\ \cdots$$
$$\cdots\ (m+1)+m\mathbb{Z}.$$

For integers a and b, the following statements are equivalent:

(1) $a + m\mathbb{Z} = b + m\mathbb{Z}$

(2) $a - b$ is divisible by m.

(3) a and b leave the same remainder when divided by m.

Notation

(1) We will write

$$a \equiv b \pmod{m}$$

if m divides $a-b$.

This is read as "a is congruent to b modulo m".

This just means that a and b are in the same coset of $m\mathbb{Z}$.

(2) The statement "m divides x" will be written symbolically as "$m \mid x$".

Easy results

(1) Addition

$a \equiv b \pmod{m}$ and

$c \equiv d \pmod{m}$

$\implies a+c \equiv b+d \pmod{m}$.

Proof $m \mid a-b \implies a-b \equiv mx$ for some $x \in \mathbb{Z}$.

$m \mid c-d \implies c-d = my$ for some $y \in \mathbb{Z}$

So $(a+c)-(b+d) = (a-b)+(c-d)$

$$= mx + my$$

$$= m(x+y).$$

So $a+c \equiv b+d \pmod{m}$. //

(2) <u>Multiplication</u>

$a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$

$\implies ac \equiv bd \pmod{m}$

<u>Proof</u>: $a - b = mx$ and $c - d = my$

for some $x, y \in \mathbb{Z}$

So, $ac - bd = (b+mx)(d+my) - bd$

$= m(xd + by + mxy)$

This shows that $ac \equiv bd \pmod{m}$

This means that we can define binary operations $+$ and $\times$ on $\mathbb{Z}/m\mathbb{Z}$.

Binary operations on $\mathbb{Z}/m\mathbb{Z}$

Given two cosets $a + m\mathbb{Z}$ and $b + m\mathbb{Z}$, we can define $(a+m\mathbb{Z}) + (b+m\mathbb{Z})$ as follows:

Pick any element x of $a+m\mathbb{Z}$

Pick any element y of $b+m\mathbb{Z}$

Define $(a+m\mathbb{Z}) + (b+m\mathbb{Z})$ to be $(x+y) + m\mathbb{Z}$.

Notice that the answer does not depend on the choice of x and y. Indeed suppose we had picked some element $x_1 \in a + m\mathbb{Z}$ instead of x and $y_1 \in b + m\mathbb{Z}$ instead of y.

Then, as x and x_1 are in the same coset,

$x \equiv x_1 \pmod{m}$

Similarly $y \equiv y_1 \pmod{m}$.

So, $x+y \equiv x_1+y_1 \pmod{m}$

So, $(x+y)+m\mathbb{Z} = (x_1+y_1)+m\mathbb{Z}$

Similarly, we can define multiplication on $\mathbb{Z}/m\mathbb{Z}$.

<u>Basic properties</u>:

1) $(\mathbb{Z}/m\mathbb{Z}, +)$ is a group.

<u>Proof</u>: $m\mathbb{Z}$ is the identity.

Indeed, $(m\mathbb{Z}) + (a + m\mathbb{Z})$
$= (0 + a) + m\mathbb{Z} = a + m\mathbb{Z}$

Similarly $(a+m\mathbb{Z}) + (m\mathbb{Z}) = (a+m\mathbb{Z})$

<u>Inverses</u>: $(a+m\mathbb{Z}) + ((-a)+m\mathbb{Z})$

$$= (a+(-a)) + m\mathbb{Z}$$

$$= m\mathbb{Z}$$

<u>Associativity</u>

$$(a+m\mathbb{Z}) + ((b+m\mathbb{Z}) + (c+m\mathbb{Z}))$$

$$= (a+m\mathbb{Z}) + ((b+c) + m\mathbb{Z})$$

$$= (a + (b + c)) + m\mathbb{Z}$$

$$= ((a+b) + c) + m\mathbb{Z}$$

$$= ((a+b) + m\mathbb{Z}) + (c + m\mathbb{Z})$$

$$= ((a + m\mathbb{Z}) + (b + m\mathbb{Z})) + (c + m\mathbb{Z}).$$

Thus, $(\mathbb{Z}/m\mathbb{Z}, +)$ is a group.

Multiplication

$\mathbb{Z}/m\mathbb{Z}$ is not a group under multiplication.

However, $(1 + m\mathbb{Z})$ is the identity for multiplication.

Multiplication is also associative.

Distributive property

Recall that in $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$, multiplication distributes over addition. In other words

$$(a+b)\cdot c = ac + bc$$

and $a\cdot(b+c) = ab + ac$.

We get such identities in $\mathbb{Z}/m\mathbb{Z}$ as well.

Multiplicative inverses in $\mathbb{Z}/m\mathbb{Z}$

We say that an element $(a+m\mathbb{Z})$ on $\left(\mathbb{Z}/m\mathbb{Z}\right)$ is <u>invertible</u> if it has a multiplicative inverse, i.e. if there exists an integer b such that $(a+m\mathbb{Z})\cdot(b+m\mathbb{Z}) = 1+m\mathbb{Z}$.

Question: Which elements of $\mathbb{Z}/m\mathbb{Z}$ are invertible?

Suppose $a + m\mathbb{Z}$ has a multiplicative inverse $b + m\mathbb{Z}$. Then $ab + m\mathbb{Z} = 1 + m\mathbb{Z}$, i.e. $ab \equiv 1 \pmod{m}$.

Thus $m \mid ab - 1$.

Let d be any common factor of m and a.

Thus $m = dx$ and $a = dy$ for some $x, y \in \mathbb{Z}$

As $m \mid ab-1$, $ab-1 = mz$ for some $z \in \mathbb{Z}$.

So $1 = ab - mz$

$= (dy)b - (dx)z$

$= d(yb - xz)$

So $d \mid 1$

So $d = +1$ or -1.

Thus, we see that the only common factors of m and a are ± 1.

So, we have proved that

$\boxed{a + m\mathbb{Z} \text{ is invertible only if } \gcd(a, m) = 1, \text{ i.e. } a \text{ and } m \text{ are coprime.}}$

<u>Question</u>: If $\gcd(a, m) = 1$, is it true that $a + m\mathbb{Z}$ is invertible?

Lemma 1 Let $m \in \mathbb{Z}$, $m > 0$. If $\gcd(a, m) = 1$, then for any element $x \in a + m\mathbb{Z}$, we have $\gcd(x, m) = 1$.

Proof: Let d be a common factor of x and m. So $x = dr$ and $m = ds$, for some $r, s \in \mathbb{Z}$

As $x \in a + m\mathbb{Z}$, $x = a + mt$ for some $t \in \mathbb{Z}$.

So $dr = a + dst$.

Thus, $a = d(r - st)$.

So $d \mid a$. But $\gcd(a, m) = 1$

$\Rightarrow d = \pm 1$. Thus $\gcd(x, m) = 1$. //

Definition We say that an element $a + m\mathbb{Z}$ of $\mathbb{Z}/m\mathbb{Z}$ is coprime to m if $\gcd(a, m) = 1$.

The set of all elements of $\mathbb{Z}/m\mathbb{Z}$ coprime to m is denoted by $U(m)$.

Note $1 + m\mathbb{Z}$ is in $U(m)$ if $m > 1$.

Notation

If we <u>fix</u> the integer m, we may write the element $a + m\mathbb{Z}$ of $\mathbb{Z}/m\mathbb{Z}$ as $\overline{a}$.

So, $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{(m-1)}\}$

Also, $\overline{m+1} = \overline{1}$, etc.

Let us fix the integer m for the rest of this lecture.

We will denote elements of $\mathbb{Z}/m\mathbb{Z}$ as $\bar{a}$, $\bar{b}$, etc.

Lemma 2: If a, b are integers such that $\overline{a}, \overline{b} \in U(m)$, then $\overline{ab} \in U(m)$.

Proof: If $\gcd(a, m) = 1$ and $\gcd(b, m) = 1$, then $\gcd(ab, m) = 1$. (Prove this as an exercise.) //

Lemma 3 Let $\bar{a}, \bar{x}, \bar{y} \in \mathbb{Z}/m\mathbb{Z}$

Suppose $\bar{a} \in U(m)$.

If $\bar{a}\,\bar{x} = \bar{a}\,\bar{y}$, then $\bar{x} = \bar{y}$.

Proof: $\bar{a}\bar{x} = \bar{a}\bar{y} \implies m \mid a(x-y)$.

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

So this implies that $m \mid x-y$.

So $\bar{x} = \bar{y}$. //

__Theorem__: Let m be a positive integer. If $\bar{a} \in U(m)$, there exists $\bar{b}$ in $U(m)$ such that $\bar{a} \cdot \bar{b} = \bar{1}$.

__Proof__: Define $\varphi : U(m) \to U(m)$ by $\varphi(\bar{x}) = \bar{a} \cdot \bar{x}$.
(Lemma 2 $\Longrightarrow$ $\bar{a} \cdot \bar{x} \in U(m)$.)

By Lemma 2, φ is a one-to-one function.

As $U(m)$ is a finite set, φ is a 1-1 correspondence.

So φ is onto.

So, $\exists\ \bar{b} \in U(m)$ such that $\varphi(\bar{b}) = \bar{1}$.

So $\overline{a} \cdot \overline{b} = \overline{1}$.

This proves the theorem.

Corollary: $U(m)$ is a group under multiplication.

Example $m = 6$

$U(6) = \{\bar{1}, \bar{5}\}$

Note that $\bar{5}^2 = \overline{25} = \bar{1}$.

Example $m = 10$

$U(10) = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$

$\bar{3}^2 = \bar{9}$, $\bar{3}^3 = \overline{27} = \bar{7}$. So,

$U(10) = \{\bar{1}, \bar{3}, \bar{3}^2, \bar{3}^3\}$