CSE 311 Lecture 12: Modular Arithmetic and Applications

Emina Torlak and Kevin Zatloukal

Topics

Modular arithmetic basics

Review of Lecture 11.

Modular arithmetic properties

Congruence, addition, multiplication, proofs.

Modular arithmetic and integer representations

Unsigned, sign-magnitude, and two's complement representation.

Applications of modular arithmetic

Hashing, pseudo-random numbers, ciphers.

Modular arithmetic basics

Review of Lecture 11.

Key definition: divisibility

Definition: $\mathbf{a}$ divides $\mathbf{b}$, written as $\mathbf{a|b}$.

For $a \in \mathbb{Z}, b \in \mathbb{Z}, a|b \leftrightarrow \exists k \in \mathbb{Z}.\, b = ka$.

We also say that b is divisible by a when $a|b$.

Key theorem: division theorem

Division theorem

For $a \in \mathbb{Z}, d \in \mathbb{Z}$ with $d > 0$,
there exist *unique* integers q, r with $0 \leq r < d$
such that $a = dq + r$.

That is, if we divide a by d, we get a unique

- **quotient** $q = a \operatorname{div} d$ and
- non-negative **remainder** $r = a \bmod d$.

So, $a = d(a \operatorname{div} d) + (a \bmod d)$.

Modular arithmetic properties

Congruence, addition, multiplication, proofs.

Congruence modulo a positive integer

Definition: $\mathbf{a}$ is congruent to $\mathbf{b}$ modulo $\mathbf{m}$, written as $\mathbf{a \equiv b \pmod{m}}$

For $a, b, m \in \mathbb{Z}$ with $m > 0$, $a \equiv b \pmod{m} \leftrightarrow m|(a-b)$

We read "$a \equiv b \pmod{m}$" as "a is congruent to b modulo m", which means $m|(a-b)$.

So, "congruence modulo m" is a predicate on integers, written using the notation "$\equiv \pmod{m}$".

Congruence and equality

Congruence property

Let $a, b, m \in \mathbb{Z}$ with $m > 0$.

Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Congruence and equality

Congruence property

Let $a, b, m \in \mathbb{Z}$ with $m > 0$.

Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Proof:

Suppose that $\mathbf{a \equiv b \pmod{m}}$.

Suppose that $\mathbf{a \bmod m = b \bmod m}$.

Congruence and equality

Congruence property

Let $a, b, m \in \mathbb{Z}$ with $m > 0$.

Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Proof:

Suppose that $\mathbf{a \equiv b \pmod{m}}$. Then $m | a - b$ by definition of congruence.

Suppose that $\mathbf{a \bmod m = b \bmod m}$.

Congruence and equality

Congruence property

Let $a, b, m \in \mathbb{Z}$ with $m > 0$.

Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Proof:

Suppose that $\mathbf{a \equiv b \pmod{m}}$. Then $m | a - b$ by definition of congruence. So $a - b = km$ for some $k \in \mathbb{Z}$ by definition of divides.

Suppose that $\mathbf{a \bmod m = b \bmod m}$.

Congruence and equality

Congruence property

Let $a, b, m \in \mathbb{Z}$ with $m > 0$.

Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Proof:

Suppose that $\mathbf{a \equiv b \pmod{m}}$. Then $m|a-b$ by definition of congruence. So $a - b = km$ for some $k \in \mathbb{Z}$ by definition of divides. Therefore, $a = b + km$.

Suppose that $\mathbf{a \bmod m = b \bmod m}$.

Congruence and equality

Congruence property

Let $a, b, m \in \mathbb{Z}$ with $m > 0$.

Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Proof:

Suppose that $\mathbf{a \equiv b \pmod{m}}$. Then $m | a - b$ by definition of congruence. So $a - b = km$ for some $k \in \mathbb{Z}$ by definition of divides. Therefore, $a = b + km$. By the division theorem, we can write $a = qm + r$ where $r = a \bmod m$.

Suppose that $\mathbf{a \bmod m = b \bmod m}$.

Congruence and equality

Congruence property

Let $a, b, m \in \mathbb{Z}$ with $m > 0$.

Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Proof:

Suppose that $\mathbf{a \equiv b \pmod{m}}$. Then $m|a - b$ by definition of congruence. So $a - b = km$ for some $k \in \mathbb{Z}$ by definition of divides. Therefore, $a = b + km$. By the division theorem, we can write $a = qm + r$ where $r = a \bmod m$. Combining this with $a = b + km$, we have $b + km = qm + r$, so $b = (q - k)m + r$.

Suppose that $\mathbf{a \bmod m = b \bmod m}$.

Congruence and equality

Congruence property

Let $a, b, m \in \mathbb{Z}$ with $m > 0$.

Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Proof:

Suppose that $\mathbf{a \equiv b \pmod{m}}$. Then $m|a - b$ by definition of congruence. So $a - b = km$ for some $k \in \mathbb{Z}$ by definition of divides. Therefore, $a = b + km$. By the division theorem, we can write $a = qm + r$ where $r = a \bmod m$. Combining this with $a = b + km$, we have $b + km = qm + r$, so $b = (q - k)m + r$. By the uniqueness condition of the division theorem, $r = b \bmod m$, so we have $a \bmod m = r = b \bmod m$.

Suppose that $\mathbf{a \bmod m = b \bmod m}$.

Congruence and equality

Congruence property

Let $a, b, m \in \mathbb{Z}$ with $m > 0$.

Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Proof:

Suppose that $\mathbf{a \equiv b \pmod{m}}$. Then $m|a - b$ by definition of congruence. So $a - b = km$ for some $k \in \mathbb{Z}$ by definition of divides. Therefore, $a = b + km$. By the division theorem, we can write $a = qm + r$ where $r = a \bmod m$. Combining this with $a = b + km$, we have $b + km = qm + r$, so $b = (q - k)m + r$. By the uniqueness condition of the division theorem, $r = b \bmod m$, so we have $a \bmod m = r = b \bmod m$.

Suppose that $\mathbf{a \bmod m = b \bmod m}$. By the division theorem, $a = mq + (a \bmod m)$ and $b = ms + (b \bmod m)$ for some $q, s \in \mathbb{Z}$.

Congruence and equality

Congruence property

Let $a, b, m \in \mathbb{Z}$ with $m > 0$.

Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Proof:

Suppose that $\mathbf{a \equiv b \pmod{m}}$. Then $m|a-b$ by definition of congruence. So $a-b=km$ for some $k \in \mathbb{Z}$ by definition of divides. Therefore, $a=b+km$. By the division theorem, we can write $a=qm+r$ where $r=a \bmod m$. Combining this with $a=b+km$, we have $b+km=qm+r$, so $b=(q-k)m+r$. By the uniqueness condition of the division theorem, $r=b \bmod m$, so we have $a \bmod m=r=b \bmod m$.

Suppose that $\mathbf{a \bmod m = b \bmod m}$. By the division theorem, $a=mq+(a \bmod m)$ and $b=ms+(b \bmod m)$ for some $q, s \in \mathbb{Z}$. Then,

$a-b=(mq+(a \bmod m))-(ms+(b \bmod m))$

Congruence and equality

Congruence property

Let $a, b, m \in \mathbb{Z}$ with $m > 0$.

Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Proof:

Suppose that $\mathbf{a \equiv b \pmod{m}}$. Then $m|a - b$ by definition of congruence. So $a - b = km$ for some $k \in \mathbb{Z}$ by definition of divides. Therefore, $a = b + km$. By the division theorem, we can write $a = qm + r$ where $r = a \bmod m$. Combining this with $a = b + km$, we have $b + km = qm + r$, so $b = (q - k)m + r$. By the uniqueness condition of the division theorem, $r = b \bmod m$, so we have $a \bmod m = r = b \bmod m$.

Suppose that $\mathbf{a \bmod m = b \bmod m}$. By the division theorem, $a = mq + (a \bmod m)$ and $b = ms + (b \bmod m)$ for some $q, s \in \mathbb{Z}$. Then,

$a - b = (mq + (a \bmod m)) - (ms + (b \bmod m)) = m(q - s) + (a \bmod m - b \bmod m)$

Congruence and equality

Congruence property

Let $a, b, m \in \mathbb{Z}$ with $m > 0$.
Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Proof:

Suppose that $\mathbf{a \equiv b \pmod{m}}$. Then $m|a - b$ by definition of congruence. So $a - b = km$ for some $k \in \mathbb{Z}$ by definition of divides. Therefore, $a = b + km$. By the division theorem, we can write $a = qm + r$ where $r = a \bmod m$. Combining this with $a = b + km$, we have $b + km = qm + r$, so $b = (q - k)m + r$. By the uniqueness condition of the division theorem, $r = b \bmod m$, so we have $a \bmod m = r = b \bmod m$.

Suppose that $\mathbf{a \bmod m = b \bmod m}$. By the division theorem, $a = mq + (a \bmod m)$ and $b = ms + (b \bmod m)$ for some $q, s \in \mathbb{Z}$. Then,
$a - b = (mq + (a \bmod m)) - (ms + (b \bmod m)) = m(q - s) + (a \bmod m - b \bmod m)$
$= m(q - s)$, since $a \bmod m = b \bmod m$.

Congruence and equality

Congruence property

Let $a, b, m \in \mathbb{Z}$ with $m > 0$.

Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Proof:

Suppose that a $\equiv$ b $\pmod{\mathbf{m}}$. Then $m | a - b$ by definition of congruence. So $a - b = km$ for some $k \in \mathbb{Z}$ by definition of divides. Therefore, $a = b + km$. By the division theorem, we can write $a = qm + r$ where $r = a \bmod m$. Combining this with $a = b + km$, we have $b + km = qm + r$, so $b = (q - k)m + r$. By the uniqueness condition of the division theorem, $r = b \bmod m$, so we have $a \bmod m = r = b \bmod m$.

Suppose that a $\mathbf{mod\ m = b\ mod\ m}$. By the division theorem, $a = mq + (a \bmod m)$ and $b = ms + (b \bmod m)$ for some $q, s \in \mathbb{Z}$. Then,

$a - b = (mq + (a \bmod m)) - (ms + (b \bmod m)) = m(q - s) + (a \bmod m - b \bmod m)$
$= m(q - s)$, since $a \bmod m = b \bmod m$. Therefore, $m | (a - b)$ and so $a \equiv b \pmod{m}$.

The $\mathbf{mod\ m}$ function vs the $\equiv \pmb{(\mathrm{mod}\ m)}$ predicate

The $\bmod m$ function takes any $a \in \mathbb{Z}$ and maps it to a remainder $a \bmod m \in \{0, 1, \dots, m-1\}$.

In other words, $\bmod m$ places all integers that have the same remainder modulo m into the same "group" (a.k.a. "congruence class").

The $\equiv \pmod m$ predicate compares $a, b \in \mathbb{Z}$ and returns true if and only if a and b are in the same group according to the $\bmod m$ function.

Modular addition property

Modular addition property

Let m be a positive integer ($m \in \mathbb{Z}$ with $m > 0$).
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

Modular addition property

Modular addition property

Let m be a positive integer ($m \in \mathbb{Z}$ with $m > 0$).
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

Proof:

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

Modular addition property

Modular addition property

Let m be a positive integer ($m \in \mathbb{Z}$ with $m > 0$).
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

Proof:

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. By definition of congruence, there are k and j such that $a - b = km$ and $c - d = jm$.

Modular addition property

Modular addition property

Let m be a positive integer ($m \in \mathbb{Z}$ with $m > 0$).
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

Proof:

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. By definition of congruence, there are k and j such that $a - b = km$ and $c - d = jm$. Adding these equations together, we get $(a + c) - (b + d) = m(j + k)$.

Modular addition property

Modular addition property

Let m be a positive integer ($m \in \mathbb{Z}$ with $m > 0$).
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

Proof:

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. By definition of congruence, there are k and j such that $a - b = km$ and $c - d = jm$. Adding these equations together, we get $(a + c) - (b + d) = m(j + k)$. Reapplying the definition of congruence, we get that $(a + c) \equiv (b + d) \pmod{m}$.

Modular multiplication property

Modular multiplication property

Let m be a positive integer ($m \in \mathbb{Z}$ with $m > 0$).

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Modular multiplication property

Modular multiplication property

Let m be a positive integer ($m \in \mathbb{Z}$ with $m > 0$).
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof:

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

Modular multiplication property

Modular multiplication property

Let m be a positive integer ($m \in \mathbb{Z}$ with $m > 0$).
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof:

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. By definition of congruence, there are k and j such that $a - b = km$ and $c - d = jm$.

Modular multiplication property

Modular multiplication property

Let m be a positive integer ($m \in \mathbb{Z}$ with $m > 0$).
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof:

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. By definition of congruence, there are k and j such that $a - b = km$ and $c - d = jm$.
So, $a = km + b$ and $c = jm + b$.

Modular multiplication property

Modular multiplication property

Let m be a positive integer ($m \in \mathbb{Z}$ with $m > 0$).
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof:

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. By definition of congruence, there are k and j such that $a - b = km$ and $c - d = jm$. So, $a = km + b$ and $c = jm + b$. Multiplying these equations together, we get $ac = (km + b)(jm + d) = kjm^2 + kmd + bjm + bd$.

Modular multiplication property

Modular multiplication property

Let m be a positive integer ($m \in \mathbb{Z}$ with $m > 0$).
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof:

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. By definition of congruence, there are k and j such that $a - b = km$ and $c - d = jm$. So, $a = km + b$ and $c = jm + b$. Multiplying these equations together, we get $ac = (km + b)(jm + d) = kjm^2 + kmd + bjm + bd$. Rearranging gives us $ac - bd = m(kjm + kd + bj)$.

Modular multiplication property

Modular multiplication property

Let m be a positive integer ($m \in \mathbb{Z}$ with $m > 0$).
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof:

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. By definition of congruence, there are k and j such that $a - b = km$ and $c - d = jm$. So, $a = km + b$ and $c = jm + b$. Multiplying these equations together, we get $ac = (km + b)(jm + d) = kjm^2 + kmd + bjm + bd$. Rearranging gives us $ac - bd = m(kjm + kd + bj)$. Reapplying the definition of congruence, we get that $ac \equiv bd \pmod{m}$.

Example: a proof using modular arithmetic

Let $n \in \mathbb{Z}$, and prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

Example: a proof using modular arithmetic

Let $n \in \mathbb{Z}$, and prove that $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

Let's look at a few examples:

$$\begin{aligned} 0^2 &= 0 \equiv 0 \pmod 4 \\ 1^2 &= 1 \equiv 1 \pmod 4 \\ 2^2 &= 4 \equiv 0 \pmod 4 \\ 3^2 &= 9 \equiv 1 \pmod 4 \\ 4^2 &= 16 \equiv 0 \pmod 4 \end{aligned}$$

Example: a proof using modular arithmetic

Let $n \in \mathbb{Z}$, and prove that $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

Let's look at a few examples:

$$0^2 = 0 \equiv 0 \pmod 4$$
$$1^2 = 1 \equiv 1 \pmod 4$$
$$2^2 = 4 \equiv 0 \pmod 4$$
$$3^2 = 9 \equiv 1 \pmod 4$$
$$4^2 = 16 \equiv 0 \pmod 4$$

It looks like

$$n \equiv 0 \pmod 2 \rightarrow n^2 \equiv 0 \pmod 4$$
$$n \equiv 1 \pmod 2 \rightarrow n^2 \equiv 1 \pmod 4$$

Example: a proof using modular arithmetic

Let $n \in \mathbb{Z}$, and prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

Let's look at a few examples:

$0^2 = 0 \equiv 0 \pmod{4}$
$1^2 = 1 \equiv 1 \pmod{4}$
$2^2 = 4 \equiv 0 \pmod{4}$
$3^2 = 9 \equiv 1 \pmod{4}$
$4^2 = 16 \equiv 0 \pmod{4}$

It looks like

$n \equiv 0 \pmod{2} \rightarrow n^2 \equiv 0 \pmod{4}$
$n \equiv 1 \pmod{2} \rightarrow n^2 \equiv 1 \pmod{4}$

Proof by cases:

Case 1 (n is even).

Case 2 (n is odd).

Example: a proof using modular arithmetic

Let $n \in \mathbb{Z}$, and prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

Let's look at a few examples:

$$0^2 = 0 \equiv 0 \pmod{4}$$
$$1^2 = 1 \equiv 1 \pmod{4}$$
$$2^2 = 4 \equiv 0 \pmod{4}$$
$$3^2 = 9 \equiv 1 \pmod{4}$$
$$4^2 = 16 \equiv 0 \pmod{4}$$

It looks like

$$n \equiv 0 \pmod{2} \rightarrow n^2 \equiv 0 \pmod{4}$$
$$n \equiv 1 \pmod{2} \rightarrow n^2 \equiv 1 \pmod{4}$$

Proof by cases:

Case 1 (n is even). Suppose $n \equiv 0 \pmod{2}$.

Case 2 (n is odd).

Example: a proof using modular arithmetic

Let $n \in \mathbb{Z}$, and prove that $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

Let's look at a few examples:

$0^2 = 0 \equiv 0 \pmod 4$
$1^2 = 1 \equiv 1 \pmod 4$
$2^2 = 4 \equiv 0 \pmod 4$
$3^2 = 9 \equiv 1 \pmod 4$
$4^2 = 16 \equiv 0 \pmod 4$

It looks like

$n \equiv 0 \pmod 2 \rightarrow n^2 \equiv 0 \pmod 4$
$n \equiv 1 \pmod 2 \rightarrow n^2 \equiv 1 \pmod 4$

Proof by cases:

Case 1 ($\mathbf{n}$ is even). Suppose $n \equiv 0 \pmod 2$.
Then $n = 2k$ for some integer k.

Case 2 ($\mathbf{n}$ is odd).

Example: a proof using modular arithmetic

Let $n \in \mathbb{Z}$, and prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

Let's look at a few examples:

$0^2 = 0 \equiv 0 \pmod{4}$
$1^2 = 1 \equiv 1 \pmod{4}$
$2^2 = 4 \equiv 0 \pmod{4}$
$3^2 = 9 \equiv 1 \pmod{4}$
$4^2 = 16 \equiv 0 \pmod{4}$

It looks like

$n \equiv 0 \pmod{2} \rightarrow n^2 \equiv 0 \pmod{4}$
$n \equiv 1 \pmod{2} \rightarrow n^2 \equiv 1 \pmod{4}$

Proof by cases:

Case 1 ($\mathbf{n}$ is even). Suppose $n \equiv 0 \pmod{2}$. Then $n = 2k$ for some integer k. So $n^2 = (2k)^2 = 4k^2$.

Case 2 ($\mathbf{n}$ is odd).

Example: a proof using modular arithmetic

Let $n \in \mathbb{Z}$, and prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

Let's look at a few examples:

$0^2 = 0 \equiv 0 \pmod{4}$
$1^2 = 1 \equiv 1 \pmod{4}$
$2^2 = 4 \equiv 0 \pmod{4}$
$3^2 = 9 \equiv 1 \pmod{4}$
$4^2 = 16 \equiv 0 \pmod{4}$

It looks like

$n \equiv 0 \pmod{2} \to n^2 \equiv 0 \pmod{4}$
$n \equiv 1 \pmod{2} \to n^2 \equiv 1 \pmod{4}$

Proof by cases:

Case 1 ($\mathbf{n}$ is even). Suppose $n \equiv 0 \pmod{2}$. Then $n = 2k$ for some integer k. So $n^2 = (2k)^2 = 4k^2$. Therefore, by definition of congruence, $n^2 \equiv 0 \pmod{4}$.

Case 2 ($\mathbf{n}$ is odd).

Example: a proof using modular arithmetic

Let $n \in \mathbb{Z}$, and prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

Let's look at a few examples:

$$0^2 = 0 \equiv 0 \pmod{4}$$
$$1^2 = 1 \equiv 1 \pmod{4}$$
$$2^2 = 4 \equiv 0 \pmod{4}$$
$$3^2 = 9 \equiv 1 \pmod{4}$$
$$4^2 = 16 \equiv 0 \pmod{4}$$

It looks like

$$n \equiv 0 \pmod{2} \rightarrow n^2 \equiv 0 \pmod{4}$$
$$n \equiv 1 \pmod{2} \rightarrow n^2 \equiv 1 \pmod{4}$$

Proof by cases:

Case 1 ($\mathbf{n}$ is even). Suppose $n \equiv 0 \pmod{2}$. Then $n = 2k$ for some integer k. So $n^2 = (2k)^2 = 4k^2$. Therefore, by definition of congruence, $n^2 \equiv 0 \pmod{4}$.

Case 2 ($\mathbf{n}$ is odd). Suppose $n \equiv 1 \pmod{2}$.

Example: a proof using modular arithmetic

Let $n \in \mathbb{Z}$, and prove that $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

Let's look at a few examples:

$0^2 = 0 \equiv 0 \pmod 4$
$1^2 = 1 \equiv 1 \pmod 4$
$2^2 = 4 \equiv 0 \pmod 4$
$3^2 = 9 \equiv 1 \pmod 4$
$4^2 = 16 \equiv 0 \pmod 4$

It looks like

$n \equiv 0 \pmod 2 \rightarrow n^2 \equiv 0 \pmod 4$
$n \equiv 1 \pmod 2 \rightarrow n^2 \equiv 1 \pmod 4$

Proof by cases:

Case 1 (n is even). Suppose $n \equiv 0 \pmod 2$. Then $n = 2k$ for some integer k. So $n^2 = (2k)^2 = 4k^2$. Therefore, by definition of congruence, $n^2 \equiv 0 \pmod 4$.

Case 2 (n is odd). Suppose $n \equiv 1 \pmod 2$. Then $n = 2k + 1$ for some integer k.

Example: a proof using modular arithmetic

Let $n \in \mathbb{Z}$, and prove that $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

Let's look at a few examples:

$0^2 = 0 \equiv 0 \pmod 4$
$1^2 = 1 \equiv 1 \pmod 4$
$2^2 = 4 \equiv 0 \pmod 4$
$3^2 = 9 \equiv 1 \pmod 4$
$4^2 = 16 \equiv 0 \pmod 4$

It looks like

$n \equiv 0 \pmod 2) \rightarrow n^2 \equiv 0 \pmod 4$
$n \equiv 1 \pmod 2) \rightarrow n^2 \equiv 1 \pmod 4$

Proof by cases:

Case 1 ($\mathbf{n}$ is even). Suppose $n \equiv 0 \pmod 2$. Then $n = 2k$ for some integer k. So $n^2 = (2k)^2 = 4k^2$. Therefore, by definition of congruence, $n^2 \equiv 0 \pmod 4$.

Case 2 ($\mathbf{n}$ is odd). Suppose $n \equiv 1 \pmod 2$. Then $n = 2k + 1$ for some integer k. So $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$.

Example: a proof using modular arithmetic

Let $n \in \mathbb{Z}$, and prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

Let's look at a few examples:

$$0^2 = 0 \equiv 0 \pmod{4}$$
$$1^2 = 1 \equiv 1 \pmod{4}$$
$$2^2 = 4 \equiv 0 \pmod{4}$$
$$3^2 = 9 \equiv 1 \pmod{4}$$
$$4^2 = 16 \equiv 0 \pmod{4}$$

It looks like

$$n \equiv 0 \pmod{2} \to n^2 \equiv 0 \pmod{4}$$
$$n \equiv 1 \pmod{2} \to n^2 \equiv 1 \pmod{4}$$

Proof by cases:

Case 1 ($\mathbf{n}$ is even). Suppose $n \equiv 0 \pmod{2}$. Then $n = 2k$ for some integer k. So $n^2 = (2k)^2 = 4k^2$. Therefore, by definition of congruence, $n^2 \equiv 0 \pmod{4}$.

Case 2 ($\mathbf{n}$ is odd). Suppose $n \equiv 1 \pmod{2}$. Then $n = 2k + 1$ for some integer k. So $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$. Therefore, by definition of congruence, $n^2 \equiv 1 \pmod{4}$.

Modular arithmetic and integer representations

Unsigned, sign-magnitude, and two’s complement representation.

Unsigned integer representation

Represent integer $\mathbf{x}$ as a sum of $\mathbf{n}$ powers of 2:

If $x = \sum_{i=0}^{n-1} b_i 2^i$ where each $b_i \in \{0, 1\}$,
then the representation is $b_{n-1} \ldots b_2 b_1 b_0$.

Unsigned integer representation

Represent integer $\mathbf{x}$ as a sum of $\mathbf{n}$ powers of 2:

If $x = \sum_{i=0}^{n-1} b_i 2^i$ where each $b_i \in \{0, 1\}$,
then the representation is $b_{n-1} \ldots b_2 b_1 b_0$.

Examples:

$99 = 64 + 32 + 2 + 1$
$18 = 16 + 2$

So for $\mathbf{n = 8}$:

$99 = 0110\ 0011$
$18 = 0001\ 0010$

Unsigned integer representation

Represent integer $\mathbf{x}$ as a sum of $\mathbf{n}$ powers of 2:

If $x = \sum_{i=0}^{n-1} b_i 2^i$ where each $b_i \in \{0, 1\}$,
then the representation is $b_{n-1} \ldots b_2 b_1 b_0$.

Examples:

$99 = 64 + 32 + 2 + 1$
$18 = 16 + 2$

So for $\mathbf{n = 8}$:

$99 = 0110\ 0011$
$18 = 0001\ 0010$

This works for unsigned integers. How do we represented signed integers?

Sign-magnitude integer representation

If $-2^{n-1} < x < 2^{n-1}$, represent x with n bits as follows:

Use the first bit as the sign (0 for positive and 1 for negative), and the remaining $n-1$ bits as the (unsigned) value.

Examples:

$$99 = 64 + 32 + 2 + 1$$
$$18 = 16 + 2$$

So for $n = 8$:

$$99 = 0110\ 0011$$
$$-18 = 1001\ 0010$$

Sign-magnitude integer representation

If $-2^{n-1} < x < 2^{n-1}$, represent x with n bits as follows:

Use the first bit as the sign (0 for positive and 1 for negative), and the remaining $n - 1$ bits as the (unsigned) value.

Examples:

$$99 = 64 + 32 + 2 + 1$$
$$18 = 16 + 2$$

So for $n = 8$:

$$99 = 0110\ 0011$$
$$-18 = 1001\ 0010$$
$$81 = 0101\ 0001$$

The problem with this representation is that our standard arithmetic algorithms no longer work, e.g., adding the representation of -18 and 99 doesn't give the representation of 81.

Two's complement integer representation

Represent $\mathbf{x}$ with $\mathbf{n}$ bits as follows:

If $0 \leq x < 2^{n-1}$, use the n-bit unsigned representation of x.

If $-2^{n-1} \leq x < 0$, use the n-bit unsigned representation of $2^n - |x|$.

Two's complement integer representation

Represent $\mathbf{x}$ with $\mathbf{n}$ bits as follows:

If $0 \leq x < 2^{n-1}$, use the n-bit unsigned representation of x.

If $-2^{n-1} \leq x < 0$, use the n-bit unsigned representation of $2^n - |x|$.

Key property:

Two's complement representation of any number y is equivalent to $y \bmod 2^n$ so arithmetic works $\bmod 2^n$.

Two's complement integer representation

Represent $\mathbf{x}$ with $\mathbf{n}$ bits as follows:

If $0 \leq x < 2^{n-1}$, use the n-bit unsigned representation of x.
If $-2^{n-1} \leq x < 0$, use the n-bit unsigned representation of $2^n - |x|$.

Key property:

Two's complement representation of any number y is equivalent to $y \bmod 2^n$ so arithmetic works $\bmod 2^n$.

Examples:

$99 = 64 + 32 + 2 + 1$
$18 = 16 + 2$
$2^8 - 18 = 256 - 18 = 238 = 128 + 64 + 32 + 8 + 4 + 2$
$81 = 64 + 16 + 1$

So for $\mathbf{n} = \mathbf{8}$:

$99 = 0110\ 0011$
$-18 = 1110\ 1110$
$81 = 0101\ 0001$

Computing the two's complement representation

For $-2^{n-1} \leq x < 0, x$ is represented using the n-bit unsigned representation of $2^n - |x|$. To compute this value:

- Compute the n-bit unsigned representation of $|x|$.
- Flip the bits of $|x|$ to get the representation of $2^n - 1 - |x|$.
- Add 1 to get $2^n - |x|$.
- This works because $x + \overline{x}$ is all 1s, which represents $2^n - 1$. So $\overline{x} = 2^n - 1 - x$ and $\overline{x} + 1 = 2^n - x$.

Computing the two's complement representation

For $-2^{n-1} \leq x < 0$, x is represented using the n-bit unsigned representation of $2^n - |x|$. To compute this value:

- Compute the n-bit unsigned representation of $|x|$.
- Flip the bits of $|x|$ to get the representation of $2^n - 1 - |x|$.
- Add 1 to get $2^n - |x|$.
- This works because $x + \overline{x}$ is all 1s, which represents $2^n - 1$. So $\overline{x} = 2^n - 1 - x$ and $\overline{x} + 1 = 2^n - x$.

Example: -18 in 8-bit two's complement

Computing the two's complement representation

For $-2^{n-1} \leq x < 0$, x is represented using the n-bit unsigned representation of $2^n - |x|$. To compute this value:

- Compute the n-bit unsigned representation of $|x|$.
- Flip the bits of $|x|$ to get the representation of $2^n - 1 - |x|$.
- Add 1 to get $2^n - |x|$.
- This works because $x + \overline{x}$ is all 1s, which represents $2^n - 1$. So $\overline{x} = 2^n - 1 - x$ and $\overline{x} + 1 = 2^n - x$.

Example: -18 in 8-bit two's complement

18 in 8-bit unsigned: $0001\ 0010$

Computing the two's complement representation

For $-2^{n-1} \leq x < 0, x$ is represented using the n-bit unsigned representation of $2^n - |x|$. To compute this value:

- Compute the n-bit unsigned representation of $|x|$.
- Flip the bits of $|x|$ to get the representation of $2^n - 1 - |x|$.
- Add 1 to get $2^n - |x|$.
- This works because $x + \overline{x}$ is all 1s, which represents $2^n - 1$. So $\overline{x} = 2^n - 1 - x$ and $\overline{x} + 1 = 2^n - x$.

Example: -18 in 8-bit two's complement

18 in 8-bit unsigned: $0001\ 0010$

Flip the bits: $1110\ 1101$

Computing the two's complement representation

For $-2^{n-1} \le x < 0, x$ is represented using the n-bit unsigned representation of $2^n - |x|$. To compute this value:

- Compute the n-bit unsigned representation of $|x|$.
- Flip the bits of $|x|$ to get the representation of $2^n - 1 - |x|$.
- Add 1 to get $2^n - |x|$.
- This works because $x + \overline{x}$ is all 1s, which represents $2^n - 1$. So $\overline{x} = 2^n - 1 - x$ and $\overline{x} + 1 = 2^n - x$.

Example: -18 in 8-bit two's complement

18 in 8-bit unsigned: $0001\ 0010$
Flip the bits: $1110\ 1101$
Add 1: $1110\ 1110$

Applications of modular arithmetic

Hashing, pseudo-random numbers, ciphers.

Hashing

Problem:

We want to map a small number of data values from a large domain $\{0, 1, \ldots, M - 1\}$ into a small set of locations $\{0, 1, \ldots, n - 1\}$ to be able to quickly check if a value is present.

Solution:

Compute $\mathrm{hash}(x) = x \bmod p$ for a prime p close to n.

Or, compute $\mathrm{hash}(x) = ax + b \bmod p$ for a prime p close to n.

This approach depends on all of the bits of data the data.

Helps avoid collisions due to similar values.

But need to manage them if they occur.

Pseudo-random number generation

Linear Congruential method

$$x_{n+1} = (ax_n + c) \bmod m$$

Choose x_0 randomly and a, c, m carefully to produce a sequence of x_n's.

Pseudo-random number generation

Linear Congruential method

$$x_{n+1} = (ax_n + c) \bmod m$$

Choose x_0 randomly and a, c, m carefully to produce a sequence of x_n's.

Example

$a = 1103515245, c = 12345, m = 2^{31}$ from BSD

$x_0 = 311$

$x_1 = 1743353508, x_2 = 1197845517, x_3 = 1069836226, \ldots$

Simple ciphers

Ceasar or shift cipher

Treat letters as numbers: A = 0, B = 1, …

$$f(p) = (p + k) \bmod 26$$

$$f^{-1}(p) = (p - k) \bmod 26$$

More general version

$$f(p) = (ap + b) \bmod 26$$

$$f^{-1}(p) = (a^{-1}(p - b)) \bmod 26$$

Summary

Modular arithmetic is arithmetic over a finite domain.

Key notions are divisibility and congruence modulo m.

Thanks to addition and multiplication properties, modular arithmetic supports familiar algebraic manipulations such as adding and multiplying together $\equiv \pmod{m}$ equations.

Modular arithmetic is the basis of computing.

Used with two's complement representation to implement computer arithmetic.

Also used in hashing, pseudo-random number generation, and cryptography.