Lecture 2 Modular Arithmetic

$\mathbb{Z}$ - denotes the set of all integers.

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

$$\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\},$$

is the set of nonnegative integers

$$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$$

or

$$\mathbb{N}^+ = \{1, 2, 3, \ldots\}$$

is the set of positive integers

Read Properties of Integers on my webpage.

Division Algorithm:

If $a, b \in \mathbb{Z}$ with $b > 0$,
then there exist unique integers
q and r with $0 \leq r < b$ such
that

$$a = q \cdot b + r$$

q is called the quotient when
a is divided by b, and r
is called the least nonnegative
remainder when a is divided by b.

Note: It is the restriction
$0 \leq r < b$ that makes this unique.

Proof: On webpage, uses well-ordering prop.

Ex 1: Let $a = -10$, and $b = 3$

$$-10 = -12 + 2 = (-4)\cdot 3 + 2$$

(q = -4, r = 2)

$$(-10 = (-3)\cdot 3 + (-1) \quad r \text{ is not } \geq 0)$$

(q = -3, r = -1)

Def: Let $m \in \mathbb{Z}^+$, $m > 1$, for $a, b \in \mathbb{Z}$, we say that **a is congruent to b modulo m** if and only if $a - b$ is a multiple of m, i.e.

$$a - b = k \cdot m$$

for some integer k.

Note: Congruence modulo m is an **equivalence relation**, i.e.

(i) $a \equiv a \pmod{m}$ for every $a \in \mathbb{Z}$

(ii) if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$

(iii) if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$

Theorem: If $m \in \mathbb{Z}^+$ with $m > 1$, then $a \equiv b \pmod{m}$ if and only if a and b leave the same least nonnegative remainder when divided by m.

Proof on webpage.

Note: modular arithmetic, i.e. addition, subtraction, and multiplication behave exactly like the usual arithmetic operations.

Theorem: If $m \in \mathbb{Z}^+$, $m > 1$

and $a, b, c, d \in \mathbb{Z}$ with

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

then:

(i) $a + c \equiv b + d \pmod{m}$

(ii) $a \cdot c \equiv b \cdot d \pmod{m}$

In mod m equations can always reduce integers mod m before or after the arithmetic operations.

Ex 2: Find r where $0 \le r < 7$ in the following:

(a). $5 + 12 \equiv r \pmod 7$

$5 + 12 \equiv 17 \equiv 2 \cdot 7 + 2 \equiv 2 \pmod 7$

(b). $50 + 73 \equiv r \pmod 7$

$50 + 73 \equiv 1 + 3 \equiv 4 \pmod 7$

(c). $2 - 48 \equiv r \pmod 7$

$2 - 48 \equiv 2 - (-1) \equiv 3 \pmod 7$

(d). $12 \cdot 16 \equiv r \pmod 7$

$12 \cdot 16 \equiv 5 \cdot 2 \equiv 10 \equiv 3 \pmod 7$

(e) $701 \cdot 702 \cdot 703 \cdot 704 \equiv r \pmod 7$

$1 \cdot 2 \cdot 3 \cdot 4 \equiv 24 \equiv 3 \pmod 7$

(f) $222^{222} \equiv r \pmod 7$

$222 = 7 \cdot 31 + 5$ So

$$\boxed{222 \equiv 5 \pmod 7}$$

and $$222^{222} \equiv 5^{222} \pmod 7$$

Note: $5^2 \equiv 25 \equiv (-2)\cdot(-2) \equiv 4 \pmod 7$

$5^3 \equiv 5 \cdot 4 \equiv 20 \equiv -1 \pmod 7$

So $5^6 \equiv (-1)\cdot(-1) \equiv 1 \pmod 7$

Now $222 = 37 \cdot 6$ So

$$222^{222} \equiv 5^{222} \equiv 5^{37\cdot 6} \equiv (5^6)^{37} \equiv 1^{37} \equiv 1 \pmod 7$$

And $222^{222} \equiv 1 \pmod 7$

Ex 3:

If it is now x o'clock what time will it be 2500 hours from now?

$$d = \begin{cases} 1 & \text{spring daylight savings} \\ 0 & \text{not daylight savings} \\ -1 & \text{fall daylight savings} \end{cases}$$

$$x + 2500 + d \equiv x + d + 2400 + 100$$

$$\equiv x + d + 0 + 4 \cdot 24 + 4$$

$$\equiv x + d + 4 \pmod{24}$$

Ex4: Code days of the week as

Sun	M	T	W	R	F	Sat
0	1	2	3	4	5	6

Valentine's day lands on the x^{th} day of the week in the current year.
What day of the week is Valentine's day in 2026?

"# of years" = 2026 − "current year"

$$x + (\#\text{ of years}) \cdot 365 + (\#\text{ of leap years})$$

$$\equiv x + (\#\text{ of years}) \cdot 1 + (\#\text{ of leap years}) \pmod 7$$

Note: $365 \equiv 1 \pmod 7$

Ex: Keystone kidnapper

1	2	3	4	5	6	7
13	12	11	10	9	8	
	14	15	16	17	18	19
25	24	23	22	21	20	
	26	27	28	29	30	31
				33	32	
37	36	35	34			
	38.	—				

Key in casket # 54321

$54321 \equiv 9 \pmod{12}$

Key is in casket # 5.

Since

1st col: all numbers $\equiv 1 \pmod{12}$

2nd col: all numbers $\equiv 0, 2 \pmod{12}$

3rd col: all numbers $\equiv 3, 11 \pmod{12}$

4th col: all numbers $\equiv 4, 10 \pmod{12}$

5th col: all numbers $\equiv 5, 9 \pmod{12}$

6th col: all numbers $\equiv 6, 8 \pmod{12}$

7th col: all numbers $\equiv 7 \pmod{12}$

Lecture 2 (Cont.)

Recall: If $m > 1$ is a positive integer, and a, b are integers, then we say that

a is congruent to b modulo m

iff $a - b = k \cdot m$ for some integer k,

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

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

iff a and b have the same least nonnegative remainder when divided by m (using the div. alg.)

Note: If $m > 1$, and a is an integer, then from the division algorithm we know

$$a = q \cdot m + r$$

where $0 \leq r < m$. (uniquely)

The only possible remainders when a is divided by m are

$$0, 1, 2, \ldots, m-1$$

So the congruence relation $\equiv \pmod{m}$ partitions the set of integers $\mathbb{Z}$ into disjoint subsets (m of them)

called congruence classes

$[0], [1], [2], \ldots, [m-1]$

$[0] = \{0 + m \cdot x \mid x \text{ is an integer}\}$

$[1] = \{1 + m \cdot x \mid x \text{ is an integer}\}$

$[2] = \{2 + m \cdot x \mid x \text{ is an integer}\}$

$\vdots$

$[m-1] = \{m-1 + m \cdot x \mid x \text{ is an integer}\}$

Can write $\mathbb{Z} = \bigcup_{k=0}^{m-1} [k]$

(disjoint union)

Ex: If $m = 2$, possible remainders are $r = 0$ and $r = 1$

$[0] = \{0 + 2 \cdot k\} = \{2 \cdot k \mid k \text{ an integer}\}$ (even)

$[1] = \{1 + 2 \cdot k\} = \{2 \cdot k + 1 \mid k \text{ is integer}\}$ (odd)

Ex: $m = 3$, possible remainders are $0, 1, 2$

Congruence classes: $[0], [1], [2]$

Every integer has exactly one of the forms

$$a = 3 \cdot k$$

or $$a = 3 \cdot k + 1$$

or $$a = 3 \cdot k + 2$$

Ex: $m = 3$, let a be an integer, then

(i) if $a = 3k$, then $a^2 = 9k^2$ so

$$a^2 \equiv 0 \pmod 3$$

(ii) if $a = 3k+1$, then $a^2 = 9k^2 + 6k + 1$

so $$a^2 \equiv 1 \pmod 3$$

if $a = 3k+2$ then

$a^2 = 9k^2 + 12k + 4 = 9k^2 + 12k + 3 + 1$

so $a^2 \equiv 1 \pmod 3$

· Square of an integer $\equiv 0$ or $1 \pmod 3$

Theorem: if $m \in \mathbb{Z}^+$, and $m > 1$,

and $a, b \in \mathbb{Z}$ with $0 \leq a, b < m$

if $a \equiv b \pmod m$, then $a = b$.

proof:

Since $a \equiv b \pmod m$ then

$a - b = k \cdot m$ for some integer k

Since $0 \leq a \leq m-1$ and $0 \leq b \leq m-1$

then

$0 \leq a \leq m-1$ and $-(m-1) \leq -b \leq 0$

add them two inequalities:

$$-(m-1) \leq a-b \leq m-1$$

and $a-b$ is a multiple of m

and so $a-b = 0 \cdot m = 0$

that is, $a = b$.

∎

Note: if $a, b \in \mathbb{Z}$ with $b > 0$

then the d.v. algorithm says:

$$a = b \cdot q + m$$

where $0 \leq m < b$ (original

the quotient $\frac{a}{b}$ is an integer

if $m = 0$.

Remark: If we want to solve the congruence

$$3x \equiv 2 \pmod 7$$

can't divide by 3, but we can isolate the x by multiplying by 5 to get

$$5 \cdot 3x \equiv 5 \cdot 2 \equiv 10 \equiv 3 \pmod 7$$

$15 \equiv 1 \pmod 7$ so

$$1 \cdot x \equiv 3 \pmod 7$$

or $$x \equiv 3 \pmod 7$$

The integer 5 is called the multiplicative inverse of 3 modulo 7 since $5 \cdot 3 \equiv 1 \pmod 7$

Def: Two integers a and b are said to be **multiplicative inverses modulo m** iff $a \cdot b \equiv 1 \pmod{m}$

and in this case we write

$$b \equiv a^{-1} \pmod{m} \quad \text{or} \quad a \equiv b^{-1} \pmod{m}$$

Ex: Find the multiplicative inverses (mod 7) of $1, 2, 3, 4, 5, 6$

$1 \cdot 1 \equiv 1 \pmod{7}$, $2 \cdot 4 \equiv 1 \pmod{7}$

$3 \cdot 5 \equiv 1 \pmod{7}$, $6 \cdot 6 \equiv 1 \pmod{7}$

Ex: Solve for x:

$$3 \cdot (x-2) \equiv -4 \pmod 7$$

$$3x - 6 \equiv -4 \pmod 7$$

$$3x \equiv 6 - 4 \pmod 7$$

$$3x \equiv 2 \pmod 7$$

$$5 \cdot 3x \equiv 5 \cdot 2 \pmod 7$$

$$1 \cdot x \equiv 3 \pmod 7$$

So $x \equiv 3 \pmod 7$

Theorem: (Mult. Inverses modulo m)

a has a multiplicative inverse modulo m if a and m are relatively prime.

ie. they have no positive common factors except 1.

Def: If a is nonzero integer and $m > 1$, then an integer b such that

$$a \cdot b \equiv 1 \pmod{m}$$

is called the inverse of a modulo m

denoted by $b = \bar{a}^1 \pmod{m}$

Note: Suppose that $a \cdot b \equiv 1 \pmod{m}$ and $a \cdot b' \equiv 1 \pmod{m}$ then

$$\boxed{a \cdot b \equiv a \cdot b' \pmod{m}}$$

So a relatively prime term then by the cancellation law $b \equiv b' \pmod{m}$

- Modular inverses are unique. ∎

Theorem: (Cancellation Law)

If $a \cdot c \equiv b \cdot c \pmod{m}$

and c and m are relatively prime

(no common factors other than ± 1),

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

Ex: $1 \cdot (2) \equiv 4 \cdot (2) \pmod{2}$

(2) and 2 are not relatively prime

so if $1 \cdot \not{2} \equiv 4 \cdot \not{2} \pmod{2}$

this says that $1 \equiv 4 \pmod{2}$

which is not true.

Ex: $1 \cdot \not{3} \equiv 7 \cdot \not{3} \pmod{2}$ Cancel 3's

Since 2 and 3 are relatively prime.

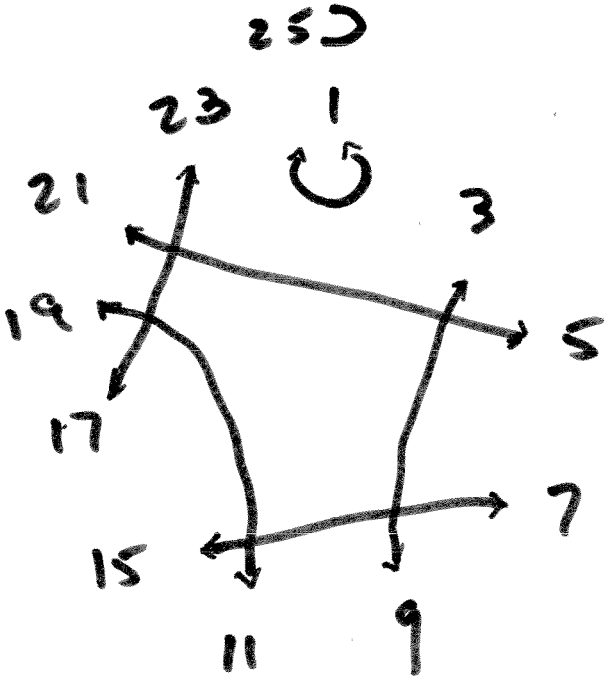
So $1 \equiv 7 \pmod{2}$

Ex: Find all the integers between 1 and 26 which an inverse mod 26.

These will be the integers that are relatively prime to 26.

1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25

Have inverses modulo 26.



$1 \equiv 27 \equiv 3 \cdot 9 \equiv (-3)(-9)$

$\equiv 23 \cdot 17$

$1 \equiv 53 \equiv 79$

$\equiv 105 \equiv 3 \cdot 5 \cdot 7 \equiv 5 \cdot 21$

$\equiv 7 \cdot 15 \equiv (-7) \cdot (-15)$

$\equiv 19 \cdot 11$

Ex: Solve for x:

$$y \equiv 7x + 6$$

$7^{-1} = 15$, so mult by 15

to get

$$15y \equiv 15 \cdot 7x + 15 \cdot 6$$

i.e.

$$15y \equiv 1 \cdot x + 90 \equiv x + 12 \pmod{26}$$

so $x \equiv 15y - 12 \pmod{26}$

End of Lecture 2. (Modular Arithmetic)