Section 4 — Congruences

AKA Modular Arithmetic

Q: If the hour hand is pointing at 9, what will it be pointing at in 5 hours?

So on a clock: $9+5 \equiv 2 \pmod{12}$

Also: $5+12 \equiv 5 \pmod{12}$

Also: $5+24 \equiv 5 \pmod{12}$

* we are reducing multiples of 12 to 0

Q: Let's call Monday the 1st day of the week. If today is Monday, what day of the week will it be in 9 days?

We have: $3+9 \equiv 5 \pmod{7}$

Also: $3+7 \equiv 3 \pmod{7}$

Also: $3+14 \equiv 3 \pmod{7}$

* we are reducing multiples of 7 to 0

Towards a definition...

mod 12

9+5

$14 = 2 + 12$ ← $14-2=12$

$23 = 11 + 12$ ← → $23-11=12$

$27 = 3 + 24$ ← → $27-3=24$

think $m = 12$

Def Let m be a positive integer. Let $a, b \in \mathbb{Z}$. We write $a \equiv b \pmod{m}$ if $m \mid (a-b)$. We read this "a is congruent to b modulo m."

* $a \equiv b \pmod{m} \iff a - b = k \cdot m$ for some $k \in \mathbb{Z}$ — Theorem 1

$\iff$ $a = b + km$ for some $k \in \mathbb{Z}$

$\iff$ a and b differ by a multiple of m.

Ex T/F — explain

(a) $26 \equiv 2 \pmod{12}$ T, $12 \mid (24 - 2)$

(b) $2 \equiv 26 \pmod{12}$

(c) $26 \equiv 2 \pmod{7}$

(d) $26 \equiv -2 \pmod{7}$

(e) $35 \equiv 0 \pmod{7}$

(f) $7^2 \equiv 1 \pmod{3}$

Ex Find all a s.t. $a \equiv 2 \pmod{3}$

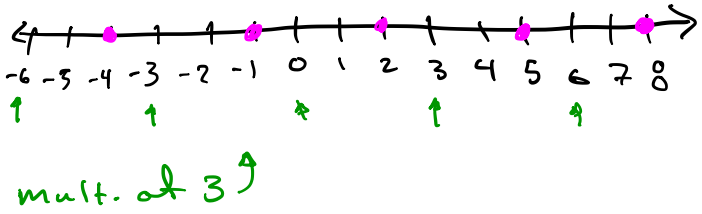
$a \equiv 0 \pmod{3} \iff a = 2 + 3k$ for $k \in \mathbb{Z}$

Ans. all numbers of the form $a = 2 + 3k$ for $k \in \mathbb{Z}$

OR all numbers that are 2 more than a multiple of 3

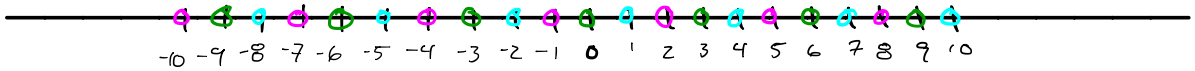
More concretely

k	...	-1	0	1	2	...
a		-1	2	5	8	



Ex Make a number line from -10 to 10.

- label all numbers cong. to $0 \bmod 3$ in green.
- " " " " " 1 " " " blue
- " " " " " 2 " " " red.



! Note that every number has one and only one color.

Theorem 2 If $n \in \mathbb{Z}$, then n is congruent modulo m to exactly one of $0, 1, \ldots, m-1$. This number is called the **least residue** modulo m.

* In previous example, this says that every integer is either 0 (green), 1 (blue), or 2 (red) modulo 3.

pf Let $n \in \mathbb{Z}$. By the division algorithm, $n = qm + r$ for $q, r \in \mathbb{Z}$ with $0 \leq r < m-1$. Thus, $n = r + qm$, so $n \equiv r \pmod{m}$. □

Ex Find the least residue of 71 modulo 2? mod 5? mod 11?

$$2 \overline{)71}\ 35,\ 70,\ 1$$

Ex Find the least residue of each of the following modulo 3:
$31, 30, 63, 7, 11$.

Theorem 3 $a \equiv b \pmod{m} \iff$ a and b have the same least residue modulo m (i.e. if they have the same remainder on division by m.

pf book.

Ex T/F $79 \equiv 123 \pmod{11}$

Two approaches:

① The def. $79 \equiv 123 \pmod{11} \iff 11 \mid (79-123)$

$\iff 11 \mid -44$

TRUE

② Theorem 3 $79 \equiv 2 \pmod{11}$ — least residue

$123 \equiv 2 \pmod{11}$

same least residue

so TRUE

Some Properties of Congruence

* Congruence behaves in many ways like equality.

Lemma 1 Let $m \in \mathbb{Z}^+$. Let $a, b, c, d \in \mathbb{Z}$.

≡ mod m is an equiv. relation

(a) $a \equiv a \pmod{m}$

(b) $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$

(c) $[a \equiv b \pmod{m}$ AND $b \equiv c \pmod{m}] \implies a \equiv c \pmod{m}$

(d,e) $[a \equiv_m b$ AND $c \equiv_m d] \implies a+c \equiv_m b+d$ AND $ac \equiv_m bd$

pf (of some)

(c) Assume $a \equiv_m b$ and $b \equiv_m c$. WTS $m \mid (a-c)$.

- $a \equiv_m b \implies m \mid (a-b)$
- $b \equiv_m c \implies m \mid (b-c)$

$\implies m \mid [(a-b)+(b-c)]$

Thus $m \mid (a-c)$, so $a \equiv_m c$ (by definition).

(d) Assume $a \equiv_m b$ AND $c \equiv_m d$. WTS $m \mid [(a+c)-(b+d)]$

- $m \mid (a-b)$
- $m \mid (c-d)$

$\implies m \mid (a-b+c-d)$

Thus, $m \mid [a+c-(b+d)]$, so $a+c \equiv_m b+d$. □

Ex In each case, find the least residue of a mod 7.

(a) $a = 17 + 700 \cdot 53$

$17 + 700 \cdot 53 \equiv 17 + 0 \cdot 53 \pmod 7$

$\equiv 17$ " $3+14$

$\equiv \boxed{3}$ "

(b) $a = 8^7$

(c) $a = 6^7$ $\quad 6 \equiv -1$

(d) $a = 2^{300}$ $\quad (2^3)^{100} \equiv 1^{100}$

(e) $a = 2^{301} + 5$ $\quad 2^{300} \cdot 2^1 \equiv 2 \ldots$

Ex Find all solutions to each of the following

(a) $2x \equiv 4 \mod 6$

$x \equiv 2$ any thing else — let's check

can't just cancel → $x \equiv 5$ $\quad (2x \equiv 4 \equiv -2 \Rightarrow x \equiv -1 \equiv 5)$

x	$2x$
0	0
1	2
2	4
3	$6 \equiv 0$
4	$8 \equiv 2$
5	$10 \equiv 4$

(b) $2x \equiv 4 \mod 5$

check

(c) $x^2 \equiv -1 \mod 5$ $\quad (-1 \equiv 4)$ ← that should be suprising (no solution in $\mathbb{Z}$)

⚠ we can not always cancel

⚠ using a table can be effective

will be used later

Theorem 4 (cancellation mod m) If $ac \equiv bc \pmod m$ AND if $(c, m) = 1$, then $a \equiv b \pmod m$

* in words: you can cancel numbers that are relatively prime to the modulus

pf $ac \equiv_m bc \Rightarrow m \mid (ac - bc) \Rightarrow m \mid c(a-b)$

$\xRightarrow{\text{Thm 5 - Sect. 1}} m \mid (a-b) \Rightarrow a \equiv_m b$ □

So what if $(c,m) \neq 1$?

Theorem 5 If $ac \equiv bc \pmod{m}$ and $(c,m) = d$, then $a \equiv b \pmod{m/d}$.

* you can always cancel if you change the modulus — but you usually don't want to.

Applications — Divisibility Checks

Ex Show that, for any $k \in \mathbb{Z}^+$, $9^k - 1$ is divisible by 8.

Let $a = 9^k - 1$. **Note:** $8 \mid a \iff a \equiv 0 \pmod 8$.

observe: $a = 9^k - 1 \equiv 1^k - 1 = 0 \pmod 8$. Thus $8 \mid a$.

Ex Show that $71534 \equiv 7+1+5+3+4 \pmod 3$

This is the idea behind...

Thm An integer is divisible by 3 $\iff$ the sum of its digits is divisible by 3.

Remember that

$$71534 = 7 \cdot 10^4 + 1 \cdot 10^3 + 5 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0$$

So if we say $d_k d_{k-1} \cdots d_1 d_0$ are the digits of n, we mean

$$n = d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_1 \cdot 10 + d_0$$

pf

write $n = d_k \cdot 10^k + \cdots + d_1 \cdot 10 + d_0$.

Then $n \equiv d_k 1^k + \cdots + d_1 \cdot 1 + d_0 \pmod 3$

$$n \equiv d_k + \cdots + d_1 + d_0 \pmod 3.$$

Now,

$$3 \mid n \iff n \equiv 0 \pmod 3$$
$$\iff d_k + \cdots + d_1 + d_0 \equiv 0 \pmod 3$$
$$\iff 3 \mid d_k + \cdots + d_1 + d_0$$

□

OPTIONAL

Thm An integer is divisible by 11 $\iff$ the alternating sum of its digits is divisible by 11.

Ex T/F : $11 \mid 73451$? $11 \mid 83556$?

Another application

Ex Find the least residue of each mod 10 : 81, 273, 1752. Notice anything?

Lemma Let $n \in \mathbb{Z}$ and let d_0 be the ones digit of n. Then $n \equiv d_0 \pmod{10}$.

pf $n = d_k 10^k + \cdots + d_1 10 + d_0$ where $d_k, \ldots, d_0$ are the digits of n. Thus $n \equiv d_0 \pmod{10}$. □

Q: what are the square integers?

0, 1, 4, 9, 16, 25, 36, 49, 64, ...

Q: Is it possible that (give me 5 #s...) $723458 \equiv$ is a square? No.

Thm If $n \in \mathbb{Z}$ and n is a square, then the last digit of n is one of $0, 1, 4, 5, 6, 9$.

pf Assume $n = m^2$. Thus $n \equiv m^2 \pmod{10}$, what are the squares mod 10?

m	m^2 mod 10
0	0
1	1
2	4
3	9
4	$16 \equiv 6$
5	$25 \equiv 5$
$-4 \equiv 6$	$16 \equiv 6$
$-3 \equiv 7$	9
$-2 \equiv 8$	4
$-1 \equiv 9$	1

$\Rightarrow n \equiv 0, 1, 4, 5, 6, 9 \pmod{10}$

$\Rightarrow$ last digit of n is $0, 1, 4, 5, 6, 9$ by previous lemma.

□