# Math 312, lecture 6, 23/08/2018

Last time: (1) Diophantine equations

(2) Congruence

Today: Congruence

Recall: $a \equiv b \pmod{m}$ means (either of:)

(1) $m \mid a-b$

(2) $a-b = km$ ← "implicit unknown"

(3) $a = b + km$

informally, "a and b are equal, up to a multiple of m".

Claim: congruence behaves like equality, and respects arithmetic

Example: congruence mod 2.

idea: this is just evens & odds

(0) $a \equiv 0$ (2) $\iff 2 \mid (a-0)$ ie. $2 \mid a$ or $a = 2k$

(1) $a \equiv$ (1) (2) $\iff 2 \mid a-1$ ie. $a = 2k+1$

# Arithmetic mod 2

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| · | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

$1+1 = 2 \equiv 0 \pmod 2$

| + | even | odd |
|---|---|---|
| even | even | odd |
| odd | odd | even |

eg. even + even = even;

$0 + 0 = 0$

So $6 + (-4) \equiv \#8 \pmod 2$

## Mod 3

← no column "3" since $3 \equiv 0 \pmod 3$

| + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

$-1 \equiv 2 \pmod 3$

or

$1 + 2 \equiv 0 \pmod 3$

| · | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

1

$2 \cdot 2 \equiv 1 \pmod 3$

**Observation:** If $x \not\equiv 0 \pmod 2$ $\exists y$ s.t. $xy \equiv 1 \pmod 2$

$x \not\equiv 0 \pmod 3$ $\exists y$ s.t. $xy \equiv 1 \pmod 3$

## Mod 4

| · | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

$3 \cdot 3 = 9 = 8 + 1 \equiv 1 \ (4)$

$3 \cdot 3 \equiv (-1) \cdot (-1) \equiv 1 \ (4)$

$2 \not\equiv 0 \ (4)$

But

$2 \cdot 2 \equiv 0 \ (4)$

Observe: If $m$ is composite (say $m = ab$), $1 < a, b < m$)

then $a \cdot b = m \equiv 0 \ (m)$

but $m \nmid a$, $m \nmid b$ so $a, b \not\equiv 0 \ (m)$

(we say $a, b$ are "zero-divisors")

If $p$ is prime, $p \nmid a$, $p \nmid b$ then $p \nmid ab$ i.e.

if $a \not\equiv 0 \ (p)$, $b \not\equiv 0 \ (p)$ then $ab \not\equiv 0 \ (p)$

---

Aside: Meaning of "prime" can matter, $(\sqrt{5}+1)(\sqrt{5}-1) = 2 \cdot 2$ in the number system $\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$

---

Notes $a \equiv 0 \ (m) \iff m \mid a$

**Division thm** for Every $a \in \mathbb{Z}$ there is a unique $0 \le r < m$ s.t. $a = qm + r$

i.e. $a \equiv r \ (m)$

We call $r$ the "reduced", "residue" of $a$ mod $m$

---

**Props** (1) $a \equiv a \ (m)$, $a \equiv b \ (m)$ iff $b \equiv a \ (m)$,

$a \equiv b \ (m)$ and $b \equiv c \ (m)$ means $a \equiv c \ (m)$

(2) $a \equiv a' \ (m)$ and $b \equiv b' \ (m)$ then $a \pm b \equiv a' \pm b' \ (m)$

$ab \equiv a'b' \ (m)$

**Pfs** (1) $a - a = 0$, $m \mid 0$ and

$b - a = -(a-b)$ so $m \mid a-b$ iff $m \mid b-a$

if $m \mid a-b$ and $m \mid b-c$ then $m \mid (a-b)+(b-c) = a-c$

(2) $(a \pm b) - (a' \pm b') = (a-a') \pm (b-b')$

if $m$ divides RHS

$$ab - a'b' = ab - a'b + a'b - a'b'$$
$$= (a-a')b + a'(b-b')$$

div by $m$ div by $m$

so div by $m$

# Divisibility Tests

Observe: $10 \equiv 0 \ (2)$

so if $n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 1000 + \ldots$

$a_0, a_1, \ldots \in \{0, 1, \ldots, 9\}$

then $n \equiv a_0 + a_1 \cdot 0 + a_2 \cdot 0^2 + a_3 \cdot 0^3 + \ldots \equiv a_0 \ (2)$

(n is even iff the ones digit is even)

---

Observe: $10 \equiv 1 \ (9)$

So $786 = 7 \cdot 10^2 + 8 \cdot 10 + 6 \cdot 1 \equiv 7 \cdot 1^2 + 8 \cdot 1 + 6 \cdot 1$

$\equiv 7 + 8 + 6 = 21 \equiv 3 \ (9)$