You're well-acquainted with arithmetic mod 12:

this class starts at 2:00
my other class starts 3 hours earlier
↪ at 11:00

$$2 - 3 \equiv 11 \pmod{12}$$

several ways to think about:
$2 \equiv 14 \pmod{12}$ and $14 - 3 = 11$
or $2 - 3 = -1$ and $-1 \equiv 11 \pmod{12}$
or $-3 \equiv 9 \pmod{12}$ and $2 + 9 = 11$

---

when we say if $a \equiv a' \pmod{m}$
and $b \equiv b' \pmod{m}$
then $a + b \equiv a' + b'$ "
$ab \equiv a'b'$ "

know it well when $m = 2$:
even + even = even
even + odd = odd
odd + odd = even
even · odd = even
etc.

Many question on §1.3 example 2 (page 23)

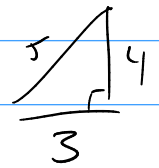
how could it happen that $a^2 + b^2$ ends in a 5

i.e. $a^2 + b^2 \equiv 5 \pmod{10}$

when a and b aren't multiples of 5?

possible: $3^2 + 4^2 = 5^2$

$9 + 16 = 25$



on Wed. looked at the squares mod 10:

$n \equiv$	0	1	2	3	4	5	6	7	8	9	(mod 10)
$n^2 \equiv$	0	1	4	9	6	5	6	9	4	1	"

how could those add up to 5?

either $0+5$ or $1+4$ or $6+9$

then both are mults. of 5

$a^2 \equiv 1$ so $a \equiv 1$ or 9

$b^2 \equiv 4$ so $b \equiv 2$ or 8

$a^2 \equiv 6$ so $a \equiv 4$ or 6

$b^2 \equiv 9$ so $b \equiv 3$ or 7

Fermat's little theorem: (Prop 3.3)

if p is prime then $\forall n \in \mathbb{Z}$,

$$n^p \equiv n \pmod{p}$$

Comments: ✡ if $p=2$, this is familiar:

$\text{even}^2 = \text{even}$

$\text{odd}^2 = \text{odd}$.

✡ fails if p is not prime.

e.g. with $p=4$

and $n=2$, $2^4 = 16 \equiv 0$ not $2 \pmod 4$

$n=3$... $3^4 = 81 \equiv 1$ not $3 \pmod 4$

Proof. do $p=3$ first, for fun.

induction on n:

for $n=1$, claim is $1^3 \equiv 1 \pmod 3$ which is true.

Suppose the claim holds for n.

Then $(n+1)^3 = n^3 + 3n^2 + 3n + 1$

$\equiv n^3 + 1 \pmod 3$

$\equiv n + 1 \pmod 3$ by our inductive hypothesis.

so the claim holds for $n+1$.

↳ so it's true for all $n \geq 1$.

for negative numbers: if $n > 0$ then

$$(-n)^3 = (-1)^3 \cdot n^3 = -n^3 \equiv -n \pmod 3$$

we proved it above.

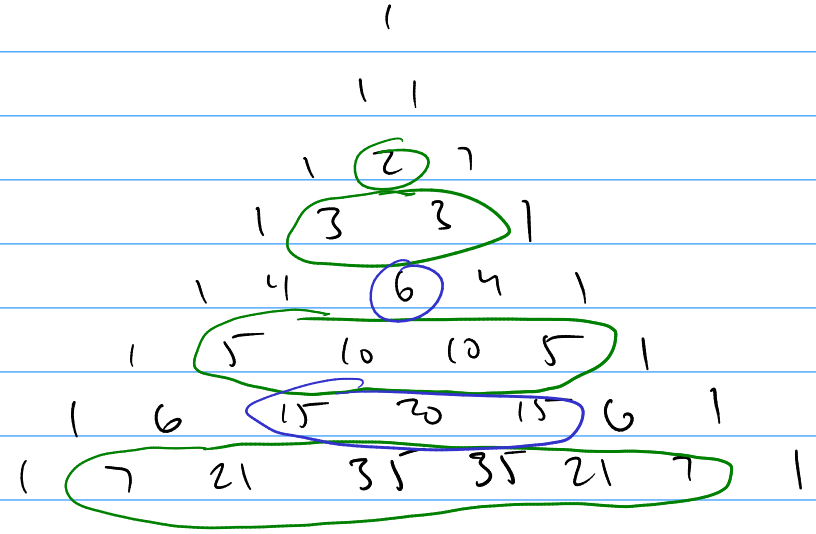
so it's true for $-n$.

---

now for general prime p.

need to know: if $0 < k < p$

then $\binom{p}{k}$ is a multiple of p



(real proof in a second.)

$$\text{so } (n+1)^p = n^p + \underset{=}{p}n^{p-1} + \underset{=}{\binom{p}{2}}n^{p-2} + \underset{=}{\binom{p}{3}}n^{p-3}$$

$$+ \cdots + \underset{=}{\binom{p}{p-2}}n^2 + \underset{=}{\binom{p}{p-1}}n + 1$$

$$\equiv n^p + 1 \pmod p$$

now just adopt the proof we gave for $p = 3$.

Why then does $p \mid \binom{p}{k}$ for $0 < k < p$?

$$\binom{p}{k} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{k(k-1)(k-2)\cdots 1}$$

because $k > 0$, we get a p in the numerator

because $k < p$, nothing in the denominator can cancel that p upstairs.

e.g. $\binom{7}{3} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2 \cdot 1}$