Example

Prove that for the square of any integer a ~~is of the form~~

~~$3k$ or $3k+1$~~

$a^2 \equiv 0 \pmod 3$ or $a^2 = 1 \pmod 3$

check all possible mod 3 numbers

0	$0^2 \equiv 0$	✓
1	$1^2 \equiv 1$	✓
2	$2^2 \equiv 1$	✓

$(x+1)^2 \pmod 2$

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

$(x+1)^3 = x^3 + 1$ in what mod?

$x^3 + 3x^2 + 3x + 1 \equiv x^3 + 1 \pmod 3$

HW discussion

Proof

Let $[a] = [b]$ in $\mathbb{Z}_n$

$a \equiv b \pmod{n} \rightarrow$ $a-b = nk$, $a = nk+b$, $b = a-nk$

Let $(a, n) = d$ and $(b, n) = e$

$a = ds$ $n = dr$

$d = au + nv$

$d = (nk+b)u + nv$

$d = ewku + emu + ewv$

$d = e(wku + mu + wv)$

$e \mid d$

$b = em$ $n = ew$

$e = bu + nv$

$e = (a-nk)u + nv$

$e = dsu - drku + drv$

$e = d(su - rku + rv)$

$d \mid e$

So $d = e$

In $\mathbb{Z}_n$ (integers mod n)

$a \in \mathbb{Z}_n$ is a <u>zero divisor</u>

if $a \cdot b = 0$ for some $b \in \mathbb{Z}$

and $a \neq 0$, $b \neq 0$

In $\mathbb{Z}_6$, 2 and 3 are zero-divisors