Last time: For all integers a & b

ab is even $\iff$ a is even or b is even

Proof: ($\Leftarrow$) Suppose a is even or b is even

We deal with these two cases separately

Case 1: a is even

There is some $c \in \mathbb{Z}$ s.t. $a = 2c$.

Then $a \cdot b = (2c) \cdot b = 2 \cdot cb$

which is even, as desired.

Case 2: b is even

See Ch 4.5 ⇝ This is similar to Case 1.

($\Rightarrow$) We prove the contrapositive, namely

"If a is odd and b is odd then ab is odd"

If a, b are odd, there are integers c, d s.t.

$a = 2c+1$, $b = 2d+1$.

Then $ab = (2c+1)(2d+1) = 4cd + 2c + 2d + 1 = 2(2cd + c + d) + 1$

which is odd, as desired. ■

Comments about Proofs (Ch 5.3)

- Make your sentences unambiguous.
  - Avoid "it" "this" "that"

    "It is even" ✗ "The integer a is even" ✓
  - Define every new symbol you use.

    "Let S be the set ..."
  - When you refer to a mathematical object, remind the reader what type it is

    "Consider n" ✗ "Consider the integer n" ✓
- Use words to link your proof together

  "$S \subseteq T$, $x \in S$" "$S \subseteq T$, therefore $x \in S$"

  "therefore", "because", etc.

  "S is a subset of T, therefore $x \in S$"

In general, first make sure it's unambiguous and understandable. THEN try to be concise

Congruence (Ch 5.2)

Remember, if a, n are integers, we say

$n \mid a$ if there's some $c \in \mathbb{Z}$ s.t. $a = n \cdot c$

"n divides a"

Def: Suppose $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$.

We say $a \equiv b \pmod{n}$ if $n \mid (a-b)$

"a is congruent to b modulo n"

Ex: a is odd $\iff$ $a \equiv 1 \bmod 2$

even $\equiv 0 \bmod 2$

$9 \equiv 16 \pmod{7}$ Check:

Is it true that $7 \mid (9-16)$?

$7 \mid -7$? yes

because $-7 = 7 \cdot (-1)$

both true.

$2 \equiv -3 \pmod{5}$

$9 \equiv 2 \pmod{7}$

In general, any integer a is congruent to one of $0, 1, 2, \ldots, n-1$ modulo n.

Exercise: Suppose $a \equiv b \pmod{n}$.

Prove that for any $c \in \mathbb{Z}$,

$$a + c \equiv b + c \pmod{n}$$

and $$a \cdot c \equiv b \cdot c \pmod{n}$$

Exercise: Prove that if n is any integer,

$$3 \nmid n \Rightarrow 3 \mid n^2 - 1$$

Exercise: Prove that for all integers a, b,

$$3 \mid ab \Rightarrow 3 \mid a \text{ or } 3 \mid b.$$

Exercise: If n is an integer,

If n is not even and n is not divisible by 3, then $6 \mid n^2 - 1$

~~Exercise: For any integer n, if $n \equiv 3 \pmod{4}$~~

~~then~~

Prop: For any integers a, b s.t. $a \equiv b \pmod n$, and any integer c,

$a+c \equiv b+c \pmod n$ ① and $ac \equiv bc \pmod n$ ②

Pf: If $a \equiv b \pmod n$, then $n \mid a-b$.

① Since the expressions $(a+c)-(b+c)$ and $a-b$ are equal, it follows that $n \mid (a+c)-(b+c)$, and therefore $a+c \equiv b+c \pmod n$

② There is some integer x s.t. $nx = a-b$.
Then $n \cdot xc = (a-b)c = ac-bc$.
Thus, $n \mid ac-bc$, so $ac \equiv bc \pmod n$. ∎

Prop: For any integer n, $3 \nmid n \Rightarrow 3 \mid n^2-1$.

Pf: For any integer n, $n \equiv 0 \pmod 3$ or $n \equiv 1 \pmod 3$ or $n \equiv 2 \pmod 3$
We are given that $3 \nmid n$, so the first case is impossible.
We treat the remaining two cases separately. In each it suffices to show $n^2 \equiv 1 \pmod 3$.

Case 1: $n \equiv 1 \pmod 3$ Then $n^2 \equiv 1 \cdot 1 \equiv 1 \pmod 3$.

Case 2: $n \equiv 2 \pmod 3$. Then $n^2 \equiv 2 \cdot 2 \equiv 4 \equiv 1 \pmod 3$. ∎

Prop: For any integers a and b, $3 \mid ab \Rightarrow (3 \mid a$ or $3 \mid b)$

Pf: We instead prove the contrapositive, namely "$(3 \nmid a$ and $3 \nmid b) \Rightarrow 3 \nmid ab$"
Suppose a and b are not divisible by 3.

Case 1: $a \equiv 1 \pmod 3$, $b \equiv 1 \pmod 3$. Then $ab \equiv 1 \cdot 1 \equiv 1 \pmod 3$

Case 2: $a \equiv 1 \pmod 3$ $b \equiv 2 \pmod 3$ Then $ab \equiv 1 \cdot 2 \equiv 2 \pmod 3$

Case 3: $a \equiv 2 \pmod 3$ $b \equiv 1 \pmod 3$ Then $ab \equiv 2 \cdot 1 \equiv 2 \pmod 3$

Case 4: $a \equiv 2 \pmod 3$ $b \equiv 2 \pmod 3$ Then $ab \equiv 2 \cdot 2 \equiv 4 \equiv 1 \pmod 3$

In each case $3 \nmid ab$. ∎

Prop: If n is an integer, then

$$2 \nmid n \text{ and } 3 \nmid n \implies 6 \mid n^2 - 1$$

Pf: The integer n is congruent to one of $0, 1, 2, 3, 4, 5 \pmod 6$. We consider these cases separately.

Case 0: $n \equiv 0 \bmod 6$. Then $6 \mid n$. So there is some $x \in \mathbb{Z}$ s.t. $n = 6x$. Then $n = 2 \cdot (3x)$, so $2 \mid n$. Thus, the premise is invalid.

Case 1: $n \equiv 1 \bmod 6$. Then $n^2 \equiv 1 \cdot 1 \equiv 1 \pmod 6$.

Case 2: $n \equiv 2 \bmod 6$. Then $6 \mid n-2$. ~~[illegible]~~

Then there is some $x \in \mathbb{Z}$ s.t. $n - 2 = 6x$. Then $n = 6x + 2 = 2(3x+1)$, so $2 \mid n$.

Case 3: $n \equiv 3 \bmod 6$. Then $6 \mid n-3$. Thus there is some $x \in \mathbb{Z}$ s.t. $n - 3 = 6x$. Then $n = 6x + 3 = 3(2x+1)$ so $3 \mid n$

Case 4: $n \equiv 4 \bmod 6$. Similar to Case 2

Case 5: $n \equiv 5 \bmod 6$. Then $n^2 \equiv 5 \cdot 5 \equiv 25 \equiv 1 \pmod 6$. ∎