3/3

Announcements:

1. HW #4 Due Friday @ 5PM
2. RR 3.2 Due Friday before class

Congruence

Def: Let $n \in \mathbb{N}$. If a, b are integers we say a is congruent b b modulo n if and only if n divides $a-b$.

We use the notation $a \equiv b \pmod{n}$

"a is congruent to b modulo n"

Note:

$$a \equiv b \pmod{n} \iff n \mid (a-b)$$
$$\iff (\exists k \in \mathbb{Z})(a-b = nk)$$
$$\iff (\exists k \in \mathbb{Z})(a = b + nk)$$

E.g. $n = 6$

$14 \equiv 2 \pmod{6}$ since $14-2 = 12$ and $6 \mid 12$.

The set of integers that are congruent to 2 modulo 6 are

$$\{\ldots, -16, -10, -4, 2, 8, 14, 20, \ldots\}$$
$$= \{a \in \mathbb{Z} \mid a \equiv 2 \pmod{6}\}$$
$$= \{2 + 6n \mid n \in \mathbb{Z}\}$$

Prop: For all integers a, b, if $a \equiv 5 \pmod 8$ and $b \equiv 6 \pmod 8$ then $a+b \equiv 3 \pmod 8$.

Know - Show:

Step	Know	Reason
P	$a, b \in \mathbb{Z}$, $a \equiv 5 \pmod 8$, $b \equiv 6 \pmod 8$	Hypothesis
P_1	$8 \mid (a-5)$ and $8 \mid b-6$	def of congruence
P_2	$a-5 = 8j$, $b-6 = 8k$ for some $k, j \in \mathbb{Z}$	def of divides
	$(a-5)+(b-6) = 8j + 8k$ $a+b-11 = 8j+8k+8$ (+8) $a+b-3 = 8j+8k+8$ $= 8(j+k+1)$	Algebra
Q_2	$a+b-3 = 8m$ for some $m \in \mathbb{Z}$	Set $m = j+k+1 \in \mathbb{Z}$ and integers are closed under addition
Q_1	$8 \mid (a+b-3)$	def. of divides
Q	$a+b \equiv 3 \pmod 8$	definition of congruence

Prop: For all integers a, b if $a \equiv 5 \pmod 8$ and $b \equiv 6 \pmod 8$ then $a+b \equiv 3 \pmod 8$.

Proof: Let $a, b \in \mathbb{Z}$ and assume $a \equiv 5 \pmod 8$ and $b \equiv 6 \pmod 8$. We'll show $a+b \equiv 3 \pmod 8$. By definition of congruence mod 8, we know 8 divides $a-5$ and $b-6$. So by definition of divides there exists j and k in the integers such that

$$a-5 = 8j$$
$$b-6 = 8k$$

So $a = 8j + 5$ and $b = 8k + 6$. Now we have

$$\begin{aligned} a + b - 3 &= (8j + 5) + (8k + 6) - 3 \\ &= 8j + 8k + 8 \\ &= 8(j + k + 1) \end{aligned}$$

Since the integers are closed under addition, $j + k + 1 \in \mathbb{Z}$, so 8 divides $a + b - 3$ which means $a + b \equiv 3 \pmod 8$. This completes the proof. ▨

Some tips for proofwriting:

1. Know your audience!
   - ↳ In this class write proofs that your fellow classmates can understand!
2. Use complete sentences and paragraphs.
3. Keep it simple! Don't say more than you need to.
4. Write a first draft on separate paper.
5. don't use $*$ or $\times$ for multiplication or $\wedge$ for exponentiation
   use $\cdot$ instead if necessary or ax or $a(b+c)$
6. Don't start sentences with symbols
7. Use English to minimize notation and make it readable

~~$\exists z \in \mathbb{Z} \ni 3z = 10 \ \forall$ - - -~~

There exists an integer z such that $3z = 10$ and for all

Other Methods of Proofs

One way to prove a mathematical statement is to instead prove any statement which it is logically equivalent to

Eg Prove "5 is not even" easier to prove "5 is odd."

↓

Show it impossible to write

$5 = 2n$

demonstrate

$5 = 2 \cdot 2 + 1$

For example consider the statement:

"Let $n \in \mathbb{Z}$. If n^2 is even (P) then n is even (Q)."

If we try to prove this directly, the known steps table would be

n^2 is an even integer	hypothesis
$n^2 = 2x$ for some $x \in \mathbb{Z}$	def. of even integer
? $n = \sqrt{2x}$ no obvious way to connect these statements	
$n = 2q$ for some $q \in \mathbb{Z}$	
n is an even integer	def of even integer

We know $(P \to Q) \equiv (\neg Q \to \neg P)$ Contrapositive

Contrapositive: If n is not even then n^2 is not even

OR better: If n is odd then n^2 is odd.

The seems more reasonable! Why $n = 2k+1 \Rightarrow n^2 = 4k^2 + 4k + 1$

$= 2(2k^2 + 2k) + 1$

Proofs Using the Contrapositive:

- A conditional statement $P \to Q$ is always logically equivalent to its contrapositive $\neg Q \to \neg P$

So to prove $P \to Q$, you can instead prove $\neg Q \to \neg P$.

WARNING! Make sure you accurately negate P and Q and have the correct contrapositive.

Guidelines & Tips

- Consider using the contrapositive when P and Q are negative statements

(OR if it switches the statement from odd/even, prime/composite, positive/negative . . .)

- If you decide to use the contrapositive in a proof you should warn the reader and clearly state the contrapositive!

"We will prove the theorem by proving its contrapositive, which is - - - - "

Theorem Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Proof: We will prove the theorem by proving its contrapositive which is if n is odd then n^2 is odd.

Let $n \in \mathbb{Z}$ and assume n is odd. Then by definition of odd integer, there exists $x \in \mathbb{Z}$ such that $n = 2x + 1$. Thus

$$n^2 = (2x+1)^2 = 4x^2 + 4x + 1$$
$$= 2(2x^2 + 2x) + 1$$

Since $\mathbb{Z}$ is closed under multiplication, $2x^2 + 2x$ is an integer, So n^2 is an odd integer by definition of odd integer. This proves the contrapositive, and hence the theorem. ∎