Today: • contrapositive
• congruence of integers

Logical equivalence: $(P \Rightarrow Q) \equiv (\sim Q \Rightarrow \sim P)$

$\sim Q \Rightarrow \sim P$: contrapositive of $P \Rightarrow Q$

(in contrast, the converse is $Q \Rightarrow P$)

Let's prove this equivalence and De Morgan Laws:
truth tables:

P	Q	~P	~Q	P ⇒ Q	~Q ⇒ ~P (contrapositive)	~P ⇒ ~Q
T	T	F	F	T	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	F
F	F	T	T	T	T	T

mystery statement: contrapositive to the converse

Compare this with negation of $P \Rightarrow Q$:

~(P ⇒ Q)
F
T
F
F

Note: When you negate $P \Rightarrow Q$, you do NOT get a conditional! → negation of the whole conditional statement

in two steps:
converse: $Q \Rightarrow P$
contrapositive to this: $\sim P \Rightarrow \sim Q$

Important Note: about negating $P \Rightarrow Q$:

To make a negation of $P \Rightarrow Q$, we exploit one more logical equivalence:

can express $P \Rightarrow Q$ using just $\wedge$, $\vee$:

P	Q	$\sim P$	$\sim P \vee Q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

↑ same as $P \Rightarrow Q$

So we have:

$$(P \Rightarrow Q) \equiv \sim P \vee Q.$$

The only way for $(P \Rightarrow Q)$ to be false is if P holds but Q doesn't hold

This says:

$$\sim(P \Rightarrow Q) \equiv \sim(\sim P \vee Q)$$

$$= (\sim\sim P) \wedge \sim Q \quad \text{(DeMorgan)}$$

$$= P \wedge \sim Q$$

Worksheet 4: Contrapositive; congruence

1. Prove that: for a an integer, $3 \mid 5a$ if and only if $3 \mid a$.

P: $3 \mid 5a$ Q: $3 \mid a$

P if and only if Q: P $\Leftrightarrow$ Q

P if Q: Q $\Rightarrow$ P

P only if Q: P $\Rightarrow$ Q

Need to prove two statements:

1) P $\Rightarrow$ Q

2) Q $\Rightarrow$ P

2. What's wrong with the following:

we are using 2019 instead of "3". compared to problem 1

Problem: for a an integer, prove that if $2019 \mid 5a$ *then* $2019 \mid a$.

Proof: Proof by contrapositive – suppose 2019 does not divide a. Then we need to prove that 2019 does not divide $5a$. Divide a by 2019 with remainder: we write $a = 2019q + r$, and our assumption means that $r \neq 0$. Then $5a = 5(2019q + r) = 2019(5q) + 5r$. Since $r \neq 0$, then $5r \neq 0$, so the number $5a$ has remainder $5r \neq 0$ when divided by 2019. Therefore $5a$ is not divisible by 2019. Thus we assumed $\sim Q$ and proved $\sim P$, so by the contrapositive argument, the proof is complete.

5a has the same remainder as 5r (5r could be bigger than 2019)

How do we know that $2019 \nmid 5r$?

Back to the same problem, with $1 \leq r \leq 2018$.

Could check 2018 cases ... needed to complete this proof. Will soon learn a clever trick proving this statement.

3. Prove that any integer is congruent to the sum of its digits mod 9.

1. P if Q = if Q then P so it says $Q \Rightarrow P$

P only if Q : the converse of $Q \Rightarrow P$

it says : $P \Rightarrow Q$. ← P is sufficient for Q.

Example: you can pass the course only if you do homework.

(Q is necessary for P) = doing homework is necessary for passing the course

= passed the course $\Rightarrow$ did homework

= if you don't do homework, you will not pass the course

Our problem: need to prove

1) $3 \mid 5a \Rightarrow 3 \mid a$ ← hard.

2) $3 \mid a \Rightarrow 3 \mid 5a$ ← easy

First prove (2): $3 \mid a \Rightarrow 3 \mid 5a$. ("only if" part)

$3 \mid a$ means that $a = 3k$ for some $k \in \mathbb{Z}$.

Then $5a = 15k = 3 \cdot (5k)$

so $5a = 3 \cdot l$ where $l = 5k$ is an integer.

so $3 \mid 5a$.

Prove (1): Try direct.

we have: $3 \mid 5a$, so $5a = 3k$ for some $k \in \mathbb{Z}$.

Then $a = 3 \cdot \frac{k}{5}$ ← this doesn't have to be an integer unless we know something about k!

how do we prove that $5 \mid k$??

STUCK.

Try contrapositive.

if $3 \mid 5a$ then $3 \mid a$. — our statement

contrapositive: if $3 \nmid a$ then $3 \nmid 5a$.

Assume $3 \nmid a$.

Then $a = 3k+1$ or $a = 3k+2$ for some $k \in \mathbb{Z}$.

(Then: use division with remainder.)

($a = 3k+1$: remainder 1; $a = 3k+2$: remainder 2.)

Case 1: $a = 3k+1$

Then $5a = 5(3k+1) = 15k + 5 = 3(5k+1) + 2$

$= 3\ell + 2$ ← has remainder 2 when divided by 3.

In this case, we got $3 \nmid 5a$ (in fact, has remainder 2)

Case 2: $a = 3k+2$

Then $5a = 5 \cdot (3k+2) = 15k + 10$

$= 3(5k+3) + 1$ — has remainder 1.

($5k+3 = \ell$)

This completes the proof.

Congruence of integers.

Def Let $a, b \in \mathbb{Z}$. Let $d \in \mathbb{Z}$, $d \neq 0$.

We say that $\boxed{a \equiv b \bmod d}$

"a is congruent to b modulo d"

if $d \mid b-a$

↑ in a definition, means 'if and only if'

Examples: $10 \equiv 1 \bmod 3$

$2020 \equiv 1 \bmod 2019$

$26 \equiv 6 \bmod 5$ ← note: 6 is not the remainder of 26 mod 5. But congruence is true.

Lemma: assumption: Let $a \in \mathbb{Z}$, let $d \in \mathbb{N}$. Divide a by d with remainder: $a = dq + r$, where $q \in \mathbb{Z}$ and $0 \leq r < d$

Then $a \equiv r \bmod d$.

What does it say: take $a = 10$ (for example), $d = 3$.

divide a by d with remainder: $10 = 3 \cdot 3 + \boxed{1}$ ← this is r.

Lemma says: $10 \equiv 1 \bmod 3$.

Proof: we have: $a = dq + r$.

Need to prove: $a \equiv r \bmod d$, which means, by definition, that $d \mid a-r$.

This is easy: $a - r = dq$ by def. of remainder, so $d \mid a-r$, we are done!

Proposition: Let $a, b \in \mathbb{Z}$
$d \in \mathbb{N}$

Then $a \equiv b \mod d \iff$ a and b have the same remainder when divided by d.

(if and only if)

Think about it.