

# HW 3

Monday, February 15, 2021 5:52 PM

## HW 3 (due 2/18)

Read Section 2.1 and 2.2 of Sundstrom. One thing Sundstrom does particularly well, I think, is talk openly about the connections between the English phrasing and the mathematical notations. Progress Check 2.1 on page 37 (online version), for example, is something most authors don't pause to address, but can really trip you up. Likewise for negating conditionals on page 46-47.

### Homework problems:

1) 2.2, #9, parts a-cg.

2) 2.2, #11 parts a-cg.

3) Submit a proposal for an article you could read for your second paper. Some good places to look are Mathematics Magazine, the College Mathematics Journal, and the Journal of Number Theory. It's also worth getting to know your way around the library website if you don't -- they have access to a lot of journal articles. When choosing an article, aim for something approximately on par with the Kiersten article in terms of difficulty. It shouldn't be easy enough that you instantly understand everything on your first read-through, but shouldn't be terrifying either. Ideally, it will focus on a topic that you find particularly interesting as well! (Note: This proposal doesn't lock you into this paper, but do spend the time to choose something good. We can always adjust together if it looks too easy or hard afterwards). If you have a perfect seeming paper but can't access it electronically, let me know, and I can try to help.

9. Use previously proven logical equivalencies to prove each of the following 11. Let  $a, b$ , and  $c$  be integers. Consider the following conditional statement:  
If  $a$  divides  $bc$ , then  $a$  divides  $b$  or  $a$  divides  $c$ .

Which of the following statements have the same meaning as this conditional statement and which ones are negations of this conditional statement?

The note for Exercise (10) also applies to this exercise.

- (a) If  $a$  divides  $b$  or  $a$  divides  $c$ , then  $a$  divides  $bc$ .  
(b) If  $a$  does not divide  $b$  or  $a$  does not divide  $c$ , then  $a$  does not divide  $bc$ .  
(c)  $a$  divides  $bc$ ,  $a$  does not divide  $b$ , and  $a$  does not divide  $c$ .  
(d) If  $a$  does not divide  $b$  and  $a$  does not divide  $c$ , then  $a$  does not divide  $bc$ .  
(e)  $a$  does not divide  $bc$  or  $a$  divides  $b$  or  $a$  divides  $c$ .  
(f) If  $a$  divides  $bc$  and  $a$  does not divide  $c$ , then  $a$  divides  $b$ .  
(g) If  $a$  divides  $bc$  or  $a$  does not divide  $b$ , then  $a$  divides  $c$ .

a)  $\neg P \rightarrow (Q \wedge \neg Q) \equiv \neg(Q \wedge \neg Q) \rightarrow \neg(\neg P)$  Always False  
 $(\neg Q \vee Q) \rightarrow P \equiv \neg(Q \vee \neg Q) \vee P \equiv (Q \wedge \neg Q) \vee P \equiv P$

c)  $\neg(P \leftrightarrow Q) \equiv \neg[(P \rightarrow Q) \wedge (Q \rightarrow P)] \equiv \neg(P \rightarrow Q) \vee \neg(Q \rightarrow P)$   
 $\equiv \neg(\neg P \vee Q) \vee \neg(\neg Q \vee P) \equiv (P \wedge \neg Q) \vee (Q \wedge \neg P)$

e)  $(P \rightarrow Q) \rightarrow R \equiv (\neg P \vee Q) \rightarrow R \equiv \neg(\neg P \vee Q) \vee R$   
 $\equiv (P \wedge \neg Q) \vee R \equiv (P \vee R) \wedge (\neg Q \vee R) \equiv (\neg P \rightarrow R) \wedge (Q \rightarrow R)$   
Shortcut by conditionals w/ disjunctions

g)  $[(P \wedge Q) \rightarrow (R \vee S)] \equiv [\neg(P \wedge Q) \vee (R \vee S)]$   
 $\equiv (\neg P \vee \neg Q) \vee (R \vee S) \equiv \neg P \vee \neg Q \vee R \vee S \equiv (\neg P \vee \neg Q \vee R) \vee S$   
 $\equiv \neg(\neg P \vee \neg Q \vee R) \rightarrow S \equiv (P \wedge Q \wedge \neg R) \rightarrow S$

i)  $\neg[(P \wedge Q) \rightarrow (R \vee S)] \equiv \neg[\neg(P \wedge Q) \vee (R \vee S)]$   
 $\equiv \neg[\neg(\neg P \vee \neg Q) \vee (R \vee S)] \equiv \neg[\neg P \vee \neg Q \vee R \vee S]$   
 $\equiv (P \wedge Q \wedge \neg R \wedge \neg S)$

Assumption:  $a, b, c \in \mathbb{Z}$ ; Consider  $P: a|bc$   
 $Q: a|b$   
 $R: a|c$   
Now  $(a|bc) \rightarrow ((a|b) \vee (a|c)) \equiv P \rightarrow (Q \vee R) \equiv \neg(P \vee \neg(Q \vee R))$   
 $\neg(P \rightarrow (Q \vee R)) \equiv \neg(\neg P \vee Q \vee R) \equiv (P \wedge \neg Q \wedge \neg R)$

A.  $(Q \vee R) \rightarrow P \equiv \neg(Q \vee R) \vee P$   
 $\equiv (\neg Q \wedge \neg R) \vee P \neq (Q \vee R \vee \neg P)$   
 $\equiv \neg(\neg(\neg Q \wedge \neg R) \wedge \neg P) \equiv \neg((Q \vee R) \wedge \neg P)$  **NEITHER**

C.  $(P \wedge \neg Q \wedge \neg R):$  **NEGATION**

E.  $(\neg P \vee Q \vee R):$  **Logically Equivalent**

G.  $(P \vee \neg Q) \rightarrow R \equiv \neg(P \vee \neg Q) \vee R$   
 $\neq (\neg P \vee Q \vee R)$   
 $\equiv \neg(\neg(\neg P \vee Q)) \wedge R \equiv \neg(\neg(\neg P \wedge Q)) \wedge R$   
 $\neq P \wedge \neg Q \wedge R$  **Neither**



"Why throw a stone in the water if not to..."



"Why throw a stone in the water if not to stay and watch the ripples"

"Ripple (XRP)  
White Paper"

Research Paper Proposal

For the 2nd paper I would like to use the Whitepaper for the cryptocurrency Ripple, Ticker XRP. It is available open sourced here: <https://www.allcryptowhitepapers.com/Ripple-Whitepaper/> The Mathematics behind this paper delve into the Byzantine Generals problem in the context of correctness of the currencies recorded transactions. From my brief overview aspects of game, probability, set, and graph theory seem relevant to the paper. This is a currency I hold, so it is of interest to me, while the paper seems of both similar length and difficulty to the prior.