CH. 5 CONTRAPOSITIVE PROOF

$P \Rightarrow Q$ IS LOGICALLY EQUIVALENT TO $\sim Q \Rightarrow \sim P$

CONTRAPOSITIVE FORM OF $P \Rightarrow Q$

EX. WRITE THE CONTRAPOSITIVE:

IF IT IS RAINING THEN I WILL STAY INSIDE.

$(R \Rightarrow S) = (\sim S \Rightarrow \sim R)$: IF I DON'T STAY INSIDE THEN IT ISN'T RAINING.

IF YOU ARE NOT A US CITIZEN THEN YOU CANNOT RUN FOR POTUS.

$(\sim C \Rightarrow \sim R) = (R \Rightarrow C)$: IF YOU CAN RUN FOR PRESIDENT THEN YOU ARE A US CITIZEN.

THE LECTURE WILL BE GIVEN ONLY IF THERE ARE AT LEAST 10 PEOPLE THERE.

$(L \Rightarrow T) = (\sim T \Rightarrow \sim L)$: IF THERE ARE NOT AT LEAST 10 PEOPLE THERE THEN THE LECTURE WILL NOT BE GIVEN.

Outline for Contrapositive Proof

Proposition If P, then Q.

Proof. Suppose $\sim Q$.

$\vdots$

Therefore $\sim P$. ■

EX. **4.** Suppose $a,b,c \in \mathbb{Z}$. If a does not divide bc, then a does not divide b.

$a \nmid bc$ MEANS $\sim(\exists n \in \mathbb{Z},\ bc = na)$

$\forall n \in \mathbb{Z},\ bc \neq na$ ← MAYBE NOT SO EASY TO WORK WITH.

PROOF. WE PROVE THE CONTRAPOSITIVE STATEMENT.
ASSUME $a \mid b$. THAT IS, $b = na$ FOR SOME $n \in \mathbb{Z}$.
THEN $bc = nac = anc$
SET $m = nc \in \mathbb{Z}$. THEN $bc = am$.
THEREFORE $a \mid bc$.

ex. **PROPOSITION:** LET $a, b \in \mathbb{Z}$. IF BOTH ab AND $a+b$ ARE EVEN THEN BOTH a AND b ARE EVEN.

PROOF. WE PROVE THE CONTRAPOSITIVE STATEMENT.
ASSUME IT IS NOT THE CASE THAT BOTH a AND b ARE EVEN.
THAT IS, a IS ODD OR b IS ODD (OR BOTH).
WE WILL SHOW THAT IT IS NOT THE CASE THAT BOTH ab & $a+b$ ARE EVEN.
THAT IS, WE WILL SHOW THAT ab IS ODD OR $a+b$ IS ODD (OR BOTH).

CASE 1: ONE ODD, ONE EVEN.

WLOG, ASSUME a IS ODD & b IS EVEN.
BY DEF, $a = 2n+1$ AND $b = 2m$ FOR SOME $n, m \in \mathbb{Z}$.
THEN $a+b = 2n+1+2m = 2(n+m)+1 = 2y+1$, $y = n+m \in \mathbb{Z}$.
THEREFORE $a+b$ IS ODD.

CASE 2: BOTH ODD.

BY DEF, $a = 2n+1$ AND $b = 2m+1$ FOR SOME $m, n \in \mathbb{Z}$.
THEN $ab = (2n+1)(2m+1) = 4mn + 2m + 2n + 1 = 2x+1$, $x = 2mn+m+n \in \mathbb{Z}$.
THEREFORE ab IS ODD.

IN EITHER CASE, IT IS NOT THE CASE THAT BOTH ab AND $a+b$ ARE EVEN. $\blacksquare$

ALT. LET $a, b \in \mathbb{Z}$. IF BOTH ab AND $a+b$ ARE EVEN THEN BOTH a AND b ARE EVEN.

DIRECT PROOF

$ab = 2n$ AND $a+b = 2m$ FOR SOME $m, n \in \mathbb{Z}$.

$a = \frac{2n}{b}$ $\qquad$ $a = 2m - b$

$$\frac{2n}{b} = 2m - b$$

$$2n = b(2m-b)$$

SINCE PRODUCT OF 2 ODD #'S IS ODD, EITHER b IS EVEN OR $2m-b$ IS EVEN. EITHER WAY, b IS EVEN.
A SIMILAR ARGUMENT SHOWS a IS EVEN.

§ 5.2 Congruence of Integers

Def: Two integers a, b are **congruent modulo n** if $\underbrace{n \mid (a-b)}$.

$\exists x \in \mathbb{Z},\ a-b = nx$

(i.e. a & b have same remainder when divided by n)

Written: $a \equiv b \pmod{n}$.

Opposite: $a \not\equiv b \pmod{n}$.

ex.

24-hour time $\quad 13 \equiv 1 \pmod{12} \quad$ 12-hour time

$21 \equiv 9 \pmod{12}$

$3 \equiv -1 \pmod{4}$

ex. **Proposition.** Suppose $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$.
If $12a \not\equiv 12b \pmod{n}$,
then $n \nmid 12$.

Proof. (Contrapositive) Assume $n \mid 12$. That is, $\exists x \in \mathbb{Z}$, $12 = nx$.
Then $12(a-b) = nx(a-b)$. Set $y = x(a-b) \in \mathbb{Z}$.
$12a - 12b = ny$
$\therefore\ 12a \equiv 12b \pmod{n}$. ∎

ex. **24.** If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

Proof. (Direct) Assume $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.
By def, $a-b = nx$ and $c-d = ny$ for some $x, y \in \mathbb{Z}$.
Then $a = b + nx$, $c = d + ny$, and so

$$ac = (b+nx)(d+ny) = bd + n(by + dx + nxy).$$

Set $k = by + dx + nxy \in \mathbb{Z}$. Then $ac - bd = nk$.
Therefore $ac \equiv bd \pmod{n}$. ∎