Math 2001. Lecture 20.

03. 04. 2022.

Last time: · practice problems/worksheet on direct proofs

Today: · congruence of integers

· Contrapositive proof of conditional statements (Ch. 5.)

· * recommended practices for math. writing.

1. Congruence of integers

Def: Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$. We say that a and b are <u>congruent modulo n</u> if $n \mid a-b$. We write $a \equiv b \pmod{n}$ if this is the case and write $a \not\equiv b \pmod{n}$ otherwise.

E.g.

$9 \equiv 1 \pmod 4$ because $4 \mid 9-1$ (and $1 \equiv 9$ since $4 \mid 1-9$) symmetry

$9 \not\equiv 1 \pmod 3$ since $3 \nmid (9-1)$

$10 \not\equiv 3 \pmod 4$ because $4 \nmid 10-3$

$43 \equiv 15 \pmod 4$ because $43-15 = 28$ and $4 \mid 28$.

Note: We have $a \equiv b \pmod n$ iff a and b have the same remainder when divided by n.

e.g. $43 = 4 \times 10 + \underline{\underline{3}}$, $15 = 4 \times 3 + \underline{\underline{3}}$, so $43 - 15 = 4 \times 10 - 4 \times 3$, which is divisible by 4.

so $43 \equiv 15 \pmod 4$

Prop 1: (Modular arithmetic) Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$.

(1) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a+c \equiv b+d \pmod{n}$.

(2) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$

(3) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for every $k \in \mathbb{Z}_{>0}$.

Pf: Note that (3) follows from (2) by considering k copies of the congruence

$a \equiv b \pmod{n}$. So it suffices to prove (1) and (2).

(2). Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $a-b = nk$ and $c-d = nl$ for some $k, l \in \mathbb{Z}$. Thus, we have

$$ac - bd \overset{\text{trick}}{=\!=} ac \underbrace{-bc + bc}_{} - bd = (ac-bc) + (bc-bd) = (a-b)c + b(c-d) = nkc + bnl = n(kc+bl)$$

So $n \mid ac-bd$ and $ac \equiv bd \pmod{n}$, so (2) follows. Ex: Prove (1). $\square$

2. Contrapositive proofs

Recall: Every conditional statement "if P then Q" is logically equivalent to its contrapositive statement "if not Q then not P".

So, to prove "if P then Q" it is sufficient/equivalent to prove "if not Q then not P".

Intuitively, it's sufficient to do so because if we know that P cannot happen whenever Q does not happen, then whenever P does happen Q must happen, or we'd get the contradiction that P doesn't happen.

Why use contrapositive proofs? Because it might be more natural in some cases to pass information from the "Q-side" to the "P-side".

Example:

Prop. Let $x \in \mathbb{Z}$. If $\underbrace{7x+9 \text{ is even}}_{P}$, then $\underbrace{x \text{ is odd}}_{Q}$.

pf 1. (direct proof) Suppose $7x+9$ is even.

Then $7x+9 = 2n$ for some $n \in \mathbb{Z}$.

Thus, (trick:) we have $x = 2n - 9 - 6x = 2(n - 3x - 5) + 1$

Then x is odd, so we are done.

pf 2. (contrapositive proof) We prove the contrapositive, i.e., we prove that if x is not odd, then $7x+9$ is not even. So suppose x is not odd. Then x is even, hence $x = 2k$ for some $k \in \mathbb{Z}$. Thus, $7x+9 = 7\cdot(2k)+9 = 14k+9 = 2(7k+4)+1$.

So $7x+9$ is odd and not even and we are done.

Prop: Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$. If $\underbrace{12a \not\equiv 12b \pmod{n}}_{P}$, then $\underbrace{n \nmid 12}_{Q}$.

pf: We prove the contrapositive. ie, we prove that <u>if $n \mid 12$, then $12a \equiv 12b \pmod{n}$</u>.

So suppose $n \mid 12$. Then $12 = nk$ for some $k \in \mathbb{Z}$.

Thus, $12a - 12b = 12(a-b) = nk(a-b)$,

so $n \mid 12a - 12b$, hence $12a \equiv 12b \pmod{n}$, as desired. □

Prop: Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$. If $12a \not\equiv 12b \pmod{n}$, then $a \not\equiv b \pmod{n}$.

pf: We prove the contrapositive, ie. we prove that <u>if $a \equiv b \pmod{n}$ then</u>

<u>$12a \equiv 12b \pmod{n}$</u>. The underlined statement is true by Prop 1.(2). □

Next time: · writing tips · proofs by contradiction (Ch. 6.)