Math 2001. Lecture 13.

06.17.2022.

Last time:

- foundational definitions related to integer division
- direct proofs of conditional statements

Today:

- more direct proofs
- two worksheets: Counting.2. (multisets)

  & Proofs.1. (direct proofs)

1. More direct proofs

Prop from yesterday (we proved (1))

Prop 6. 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 $k \in \mathbb{Z}_{>0}$.

Pfs of (2) and (3): Part (3) follows from repeated applications of part (2),

$$\left(\left.\begin{array}{l} a \equiv b \pmod{n} \\ a \equiv b \pmod{n} \\ \vdots \\ a \equiv b \pmod{n} \end{array}\right\} k \text{ times} \implies \underbrace{a a \cdots a}_{k} \equiv \underbrace{b b \cdots b}_{k} \pmod{n}, \text{ i.e., } a^k \equiv b^k \pmod{n}. \right.$$

So it suffices to prove (2).

(2) : Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.

Then $a-b = kn$ and $c-d = ln$ for some $k, l \in \mathbb{Z}$.

Thus, $ac - bd = ac - bc + bc - bd = (a-b)c + b(c-d)$

$$= knc + bln$$

$$= n(kc + bl)$$

(Since $k, l, b, c \in \mathbb{Z}$, we have $kc + bl \in \mathbb{Z}$.)

So $ac \equiv bd \pmod{n}$, and we are done. $\square$

Example: Prove that every (integer) multiple of 4 equals

$$1 + (-1)^n (2n-1)$$

for some nonnegative integer n.

Note: Yesterday we proved the converse statement (which is not equivalent!): for every nonnegative int n, the number $1+(-1)^n(2n-1)$ is a multiple of 4.

Combined, the statements say that an int. is divisible by 4 iff it has the form $1+(-1)^n\cdot(2n-1)$ for some $n \in \mathbb{Z}_{\geq 0}$.

Examples / trials: $N=0$, what n works? $n=0$? $1+(-1)^n(2\cdot 0-1)$

$$= 1 + (-1) = 0. \quad \checkmark$$

$N=4$, ...? $n=1$? $n=2$?

$\checkmark$ $1+(-1)^2\cdot 3 = 4$.

$N = 8$? want $\underbrace{1 + (-1)^n (2n-1)} = 8$. $n = 4$? ✓

approximately $2n$ or $-2n$, $1 + (-1)^4 \cdot (8-1) = 8$.

so try $n \approx \frac{N}{2}$ or $n \approx -\frac{N}{2}$.

try some nonnegative integers close to $\lfloor \frac{N}{2} \rfloor$.

$N = 24$? Does $n = \frac{24}{2} = 12$ work? $\to$ $1 + (-1)^{12} \cdot (24-1) = 24$. ✓

$N = -4$? want $1 + (-1)^n (2n-1) = -4$.

try a number close to $\left\{ \frac{-4}{2}, -\frac{-4}{2} \right\} \cap \mathbb{Z}_{\geq 0} = \{+2\}$.

wouldn't work by earlier example.

How about 1 ? $-1 + (-1) \cdot 1 = -2$

3 ? $1 - 1 \cdot 5 = -4$. ✓

$N = -8$. try. $4, 3, 5$.

$4 \to 8$, $3 \to -4$ by earlier examples

$5 \to 1 - 1 \cdot (9) = -8$. ✓

Conjecture: if $N = 0 \longrightarrow$ pick $n = 0$ ✓

$N > 0 \longrightarrow$ use $n = \frac{N}{2}$

$\left(N = 4k,\ n = \frac{N}{2} = 2k,\ \text{so } 1 + (-1)^n (2n - 1) = 1 + 4k - 1 = 4k = N \right)$ ✓

$N < 0 \longrightarrow$ use $n = -\frac{N}{2} + 1$.

$\left(N = 4k.\ n = -2k + 1,\ \text{so } 1 + (-1)^n (2n - 1) = 1 - 1 . (-4k + 2 - 1) = 4k = N. \right)$

Pf: Let $N = 4k$ be an arbitrary multiple of 4.

We show that $N = 1 + (-1)^n (2n-1)$ for some $n \in \mathbb{Z}_{\geq 0}$.

We discuss three cases:

(1) $N = 0$. We note that $n = 0$ works since

$$1 + (-1)^0 (2 \cdot 0 - 1) = 0 = N.$$

(2) $N > 0$. Then $N = 4k$ for some $k \in \mathbb{Z}_{>0}$. Take $n = \frac{N}{2} = 2k > 0$.

Then $\quad 1 + (-1)^n (2n-1) = 1 + 1 \cdot (4k-1) = 4k = N$,

so we have found the desired number n.

(3) $N < 0$. Then $N = 4k$ for some $k < 0$. Take $n = -\frac{N}{2} + 1 = -2k + 1$.

Then $\quad 1 + (-1)^n (2n-1) = 1 - 1(-4k + 2 - 1) = 4k + 1 - 1 = 4k = N$.

Since $k < 0$, $-2k+1 \geq 0$, so n suffices as the desired int. $\square$