# Math 2001. Lecture 12.

06.16.2022.

**Last time:**

- the pigeonhole and division principles
- more combinatorial identities and pfs

**Today:** Start Ch 4. beginning proofs

- (recollection of) definitions: parity, division relations, prime numbers, gcd and lcm, ...
- Direct proofs of if-then statements: strategy and examples.
  - template

# 1. Definitions (they'll be used for much of the rest of the course)

**Def 1.** Let $a, b \in \mathbb{Z}$. We say that $a$ *divides* $b$, and write $a \mid b$, if there exists some $k \in \mathbb{Z}$ s.t. $b = ak$.

e.g. $3 \mid 6$ since $6 = 3 \cdot 2$, $3 \nmid 5$ since $5 = 3k$ for no int $k$, $0 \mid 0$, $0 \nmid 1$.

**Def 2.** Let $n \in \mathbb{Z}$. We say that $n$ is even if $2 \mid n$, and we say that is odd if $2 \nmid n$. Equivalently, an int. $n$ is even if it's of the form $n = 2k$ for some $k \in \mathbb{Z}$, and an int. $n$ is odd if it's of the form $n = 2k+1$ for some $k \in \mathbb{Z}$.

Why we have the equivalence:

- Recall the division algorithm: given $n, k \in \mathbb{Z}$ with $k \neq 0$, there exist unique numbers $q$ and $r$ s.t. $n = k \cdot q + r$ and $r \in \{0, 1, 2, \cdots, |k|-1\}$.

  eg. $k = 5$. $10 = 5 \cdot 2 + 0$, $11 = 5 \cdot 2 + 1$, $12 = 5 \cdot 2 + 2$,

  $13 = 5 \cdot 2 + 3$, $14 = 5 \cdot 2 + 4$, $15 = 5 \cdot 3 + 0$, .....


- When $k = 2$, we hence have a dichotomy: either $r = 0$, whence $n = 2q$ and $n$ is even, or $r = 1$, whence $n = 2q + 1$ and $n$ is odd.

  (for some $q$)

  (for some $q$)

**Def 3.** Let $n \in \mathbb{Z}_{>1}$. We say $n$ is prime if $n$ has (only) exactly two positive integer divisors, i.e., $1$ and $n$. Otherwise we say $n$ is composite.

eg. 2 is prime, 3 is prime, 4 is composite $(4 = 2 \cdot 2)$,

5 is prime, 6 is composite $(6 = 2 \cdot 3)$.

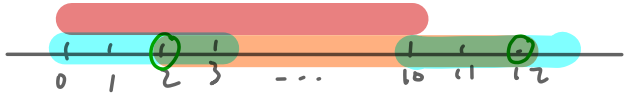
In other words, $n$ is composite if $\exists\ a, b \in \mathbb{Z}$ with $1 < a, b < n$ s.t. $n = a \cdot b$.

By convention, the number 1 is neither prime nor composite.

**Def 4.** Given $k, a, b \in \mathbb{Z}$ with $k \neq 0$. We say $a$ is congruent to $b$ modulo $k$ and write $a \equiv b \pmod{k}$ if $k \mid a - b$.

**Note:** In the "above" setting, we note that

$a \equiv b \pmod{k}$ $\overset{*}{\iff}$ $a$ and $b$ have the same remainder when divided by $k$.




eg. $12 \equiv 2 \pmod{5}$

Since $5 \mid 10 = 12 - 2$

$12 = 5 \cdot 2 + 2$

$2 = 5 \cdot 0 + 2$ $\Big\} \Rightarrow 12 - 2 = 5 \cdot (2 - 0)$

the reason for (*) in general: Say $a = kq_1 + r_1$ and $b = kq_2 + r_2$ with $q_1, q_2 \in \mathbb{Z}$ and $r_1, r_2 \in \{0, 1, 2, \dots, k-1\}$. Then

$$a - b = \underbrace{k(q_1 - q_2)}_{\text{div. by } k} + (r_1 - r_2)$$

is divisible by $k$ iff $k \mid r_1 - r_2$, iff $r_1 = r_2$.

**Def:** · Let $a, b \in \mathbb{Z}_{\neq 0}$. · We define the greatest common divisor to be the largest int. (necessarily positive) $k$ s.t. $k|a$ and $k|b$.

We denote the greatest common divisor by $\gcd(a,b)$ or $GCD(a,b)$.

e.g. $\gcd(2,3) = 1$, $\gcd(2,4) = 2$, $\gcd(9,15) = 3$,
$\gcd(12,16) = 4$.

- Similarly, we define the least common multiple of $a, b$ to be the smallest int $n$. s.t. $a|n$ and $b|n$.

e.g. $\text{lcm}(2,3) = 6$, $\text{lcm}(12,16) = 2\cdot 2\cdot 2\cdot 2\cdot 3 = 48$.
(2·2·3 and 2·2·2·2; "for otherwise they share a prime factor")

- We say that $a$ and $b$ are coprime or relatively prime if $\gcd(a,b) = 1$.

## 2. Direct proofs (of conditional statements)

A typical template for proving "if $P$, then $Q$".

**Prop.** $P \Rightarrow Q$.

**Todo:** prove that $Q$ holds whenever $P$ holds.

**Pf:** Suppose $P$ holds.

↓

[ unpack / rephrase $P$ (often using definitions) and set up some "workable" notation. then work towards establishing $Q$. ]

Therefore $Q$ holds. It follows that if $P$ then $Q$.

## Examples.

· Prop 1: If $x$ is an odd integer, then $x^2$ is an odd integer.

pf: Suppose $x$ is an odd integer.

Then $\exists\, k \in \mathbb{Z}$ s.t. $x = 2k+1$. It follows that

$$x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Since $k \in \mathbb{Z}$, $2k^2 + 2k \in \mathbb{Z}$. So $x^2 = 2N + 1$ for some $N \in \mathbb{Z}$.

Therefore $n^2$ is an odd integer, and we are done / we have proved the implication.

- **Prop 2:** Let $x, y \in \mathbb{Z}$. If $x$ is even, then $xy$ is even.

**Pf:** Suppose $x$ is even. Then $\exists k \in \mathbb{N}$ s.t. $x = 2k$.

Thus, $xy = (2k) \cdot y = 2(ky)$.

Since $k \in \mathbb{Z}$ and $y \in \mathbb{Z}$, $ky \in \mathbb{Z}$.

So $xy$ is even, and we are done. □

**Ex.**

- If $x \in \mathbb{Z}$ is even, then $x^2$ is even.

- If $x \in \mathbb{Z}$ is even, then $x^2 - 6x + 5$ is odd.

**Prop 3:** Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

(So "divides" is a transitive relation)

**Pf:** Suppose $a \mid b$ and $b \mid c$.

Then $\exists\, m, n \in \mathbb{Z}$ s.t. $b = a \cdot m$ and $c = b \cdot n$.

(or, "then $b = am$ and $c = bn$ for some $m, n \in \mathbb{Z}$.")

$$c = bn = (am)n = a(mn).$$

Since $m, n \in \mathbb{Z}$, we have $mn \in \mathbb{Z}$.

So $a \mid c$, and we are done. □

say/write "we have" so that you don't start (part of) a sentence with a symbol.

A word on cases: Sometimes a proof requires a discussion of cases that require different techniques / ideas.

Eg. Prop 4: If $n \in \mathbb{Z}$, then $1 + (-1)^n \cdot (2n-1)$ is a multiple of 4.

↓ the value depends on the parity of $n$, which suggests using two cases based on the parity.

Pf: Suppose $n \in \mathbb{Z}$. (Let $n \in \mathbb{Z}$.)

(For convenience), let $x = 1 + (-1)^n \cdot (2n-1)$.

We consider the two possible cases:

(1) $n$ is even. Then $(-1)^n = 1$ and $n = 2k$ for some $k \in \mathbb{Z}$.

Thus, $x = 1 + 1 \cdot (2 \cdot 2k - 1) = 1 + 4k - 1 = 4k$

Since $k \in \mathbb{Z}$, we have $4 \mid x$ in this case.

(2) $n$ is odd. Then $(-1)^n = -1$ and $n = 2k+1$ for some $k \in \mathbb{Z}$.

Thus, $x = 1 - 1 \cdot (2 \cdot (2k+1) - 1) = 1 - (4k + 2 - 1)$

$= 1 - (4k + 1)$

$= 1 - 4k - 1 = -4k = 4 \cdot (-k)$

Since $k \in \mathbb{Z}$, $-k \in \mathbb{Z}$. So $4 \mid x$ in this case.

By (1) and (2), we have $x$ is a multiple of 4 in all cases. as desired. □

**Prop 5**: Let $a, b \in \mathbb{Z}$. If $a, b$ have opposite parities (one even, one odd), then $a+b$ is odd.

**Pf**: Suppose that $a, b$ have different parities. Then we have two possible cases:

c1) $a$ is even, whence $b$ must be odd.

Then $a = 2k$ and $b = 2l+1$ for some $k, l \in \mathbb{Z}$. Thus, we have

$$a+b = 2k+(2l+1) = 2k+2l+1 = 2(k+l)+1.$$

Since $k, l \in \mathbb{Z}$, $k+l \in \mathbb{Z}$. so $a+b$ is odd.

c2) $a$ is odd. whence $b$ must be even.

Then $a = 2k+1$ and $b = 2l$ for some $k, l \in \mathbb{Z}$. Thus, we have

$$a+b = (2k+1)+2l = 2k+2l+1 = 2(k+l)+1.$$

Since $k, l \in \mathbb{Z}$, $k+l \in \mathbb{Z}$, so $a+b$ is odd.

entirely analogous to c1), so we can say "then by a similar argument $a+b$ is odd!"

By c1) and c2), we see that $a+b$ is odd, so we are done.

Yet another way to save repeating the similar/same argument:

Say at the beginning of the pf

"Without loss of generality (WLOG) we may assume that

a is even and b is odd"

and just use the argument in part (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 $a+c \equiv b+d \pmod n$.

modular arithmetic

(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:** (1) Suppose $a \equiv b \pmod n$ and $c \equiv d \pmod n$.

Then $n \mid a-b$ and $n \mid c-d$, ie. $a-b = n\cdot k$ and $c-d = n\ell$ for some $k, \ell \in \mathbb{Z}$.

Thus, $(a+c)-(b+d) = (a-b)+(c-d) = nk+n\ell = n(k+\ell)$

(Since $k, \ell \in \mathbb{Z}$, $k+\ell \in \mathbb{Z}$.) So $n \mid (a+c)-(b+d)$.

So $a+b \equiv c+d \pmod n$, as desired.