Math 2001. Lecture 25.

03. 18. 2022.

Last time:

- GCDs and the Euclidean algorithm
- Constructive vs. non-constructive proofs

Today:

- more problems / HW hints (Ch. 7)
- Proving set containments ("$A \subseteq B$", Ch. 8.)

1. Some more examples

↗ Look up "geometric sequences" if you want $q^0 + q^1 + \dots + q^n$.

<u>7.19</u> If $n \in \mathbb{Z}_{\geq 0}$, then $2^0 + 2^1 + 2^2 + \dots + 2^n = 2^{n+1} - 1$

e.g. $n=2$: $1 + 2 + 4 = 8 - 1$

$n=3$: $1 + 2 + 4 + 8 = 16 - 1$.

pf sketch: prove $1 (= 2^0)$ to the left and prove

$$1 + 2^0 + 2^1 + 2^2 + \dots + 2^n = 2^{n+1}$$

Note that LHS $= (1 + 2^0) + 2^1 + 2^2 + \dots + 2^n$

$= (2^0 + 2^0) + 2^1 + \dots + 2^n = (2 \cdot 2^0) + 2^1 + \dots + 2^n$

$= (2^1 + 2^1) + 2^2 + \dots + 2^n = 2 \cdot 2^1 + 2^2 + \dots + 2^n = (2^2 + 2^2) + \dots\dots$

7.23. Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $a \mid b^2 - c$, then $a \mid c$.

Key idea: Note $c = \underbrace{-(b^2-c)}_{(i)} + \underbrace{b^2}_{(ii)}$ and show that (i) and (ii) are divisible by a.

7.26. Let $n \in \mathbb{Z}_{\geq 1}$. The product of n consecutive positive integers is always divisible by $n!$

e.g. $n = 7$.

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \mid 101 \cdot 102 \cdot 103 \cdot 104 \cdot 105 \cdot 106 \cdot 107.$$

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \mid 324 \cdot 325 \cdot 326 \cdot 327 \cdot 328 \cdot 329 \cdot 330$$

Hint: Let N be the largest of the n consecutive numbers and consider $\binom{N}{n}$.

7.31. If $n \in \mathbb{Z}$, then $\gcd(n, n+1) = 1$.

e.g. $\gcd(24, 25) = 1$. $\gcd(72139, 72140) = 1$.

7.32. If $n \in \mathbb{Z}$, then $\gcd(n, n+2) \in \{1, 2\}$.

e.g. $\gcd(7, 9) = 1$, $\gcd(24, 26) = 2$.

Hint: You can use the fact we proved that $\forall a, b \in \mathbb{Z}$

$$\gcd(a, b) = (\text{min positive number of the form } ax + by \text{ where } x, y \in \mathbb{Z}).$$

Note that the assertions themselves are interesting.

2. Proving set containment

Recall: Let A, B be sets. To prove $A \subseteq B$, we need to show that every elt in A is also in B.

Examples:

8.5: Prove that $\{x \in \mathbb{Z} : 18 \mid x\} \subseteq \{x \in \mathbb{Z} : 6 \mid x\}$.

Pf: Suppose $y \in \{x \in \mathbb{Z} : 18 \mid x\}$.

Then $18 \mid x$, so $y = 18 \cdot k$ for some $k \in \mathbb{Z}$.

Thus, $y = 18 \cdot k = 6 \cdot 3 \cdot k = 6 \cdot (3k)$, so $6 \mid y$.

So $y \in \{x \in \mathbb{Z} : 6 \mid x\}$. Therefore $\{x \in \mathbb{Z} : 18 \mid x\} \subseteq \{x \in \mathbb{Z} : 6 \mid x\}$.

8.7: Show that $\{(x,y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod{6}\} \subseteq \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod{3}\}$.

Pf: Suppose $(a,b) \in \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod{6}\}$.

Then $a \equiv b \pmod{6}$, i.e., $6 \mid a-b$.

Since $3 \mid 6$, it follows that $3 \mid a-b$, so $a \equiv b \pmod{3}$.

So $(a,b) \in \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod{3}\}$. $\square$

8.8: Prove that if A, B are sets, then $\underbrace{\mathcal{P}(A) \cup \mathcal{P}(B)}_{X} \subseteq \underbrace{\mathcal{P}(A \cup B)}_{Y}$.

Pf: Take an elt / set $x \in X$. Then $x \in \mathcal{P}(A)$ or $x \in \mathcal{P}(B)$.

If $x \in \mathcal{P}(A)$, x is a subset of A, hence x is a subset of $A \cup B$.

Similarly, if $x \in \mathcal{P}(B)$, then x is a subset of B and hence of $A \cup B$.

So $x \in Y$. Therefore $X \subseteq Y$.

Recall: For a set S, the power set $\mathcal{P}(S)$ is the set of all subsets of S, so to be an elt in $\mathcal{P}(S)$ is to be a subset of S.

e.g. $S = \{1, 2\} \Rightarrow \mathcal{P}(S) = \{ \{1, 2\}, \{1\}, \{2\}, \phi \}$

e.g.: Let A, B be sets. If $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, then $A \subseteq B$.

pf: Suppose $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. We want to show $A \subseteq B$.

($A \subseteq B$) Suppose $a \in A$. Then $\{a\} \subseteq A$, i.e., $\{a\} \in \mathcal{P}(A)$

Since $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, it follows that $\{a\} \in \mathcal{P}(B)$, i.e., $\{a\}$ is

a subset of B. It follows that a, an elt in $\{a\}$, is in B.

So $a \in B$. Therefore $A \subseteq B$. $\square$

Next: Proving set equality "$A = B$" by proving $A \subseteq B$ and $B \subseteq A$.