Discrete Math 37110 - Class 1 (2016-09-27)

Instructor: László Babai
Notes taken by Jacob Burroughs
Proofread by instructor

Administrative Matters

EX 1: Send email with subject "questionnaire" answering questions from website

- Exercise types:

  DO exercises to complete but don't hand in

  HW problems due next class unless otherwise stated

  CH challenge exercises; important for theory work

- Can ask to discuss problem at discussion section on Thursdays
- If regular HW takes too much time, speak to instructor. Don't wait until too late.
- Remember to raise hands for questions rather than calling out
- Not in our own interest to find solutions to problems online, since we want to actually learn the material from the class (and we won't have access to them on our tests)
- Tests are closed books, no electronics
- For new problems, collaboration is encouraged. (Obviously, make sure that all collaborators are thinking about the problems, or some people won't get much of anything out of it.) Make sure you credit your collaborators in what you turn in. Also cite electronic or paper sources you use (these sources are discouraged, electronic more than paper). Communication of our work is nearly as important as our ability to do it.
- If you can, submit solutions in LaTeX on paper. Don't email unless there is an extenuating circumstance.

Material

DO 1.1. Review limits of sequences (calculus)

DO 1.2. Review sets, functions, and relations

Notation 1.3. $\forall$ For all (universal quantifier)

$\exists$ There exists (x) such that (existential quantifier)

Definition 1.4 (Integers)**.** Integers:

$$\mathbb{Z} = \text{set of integers} = \{0 \pm 1, \pm 2, \dots\}$$

Definition 1.5 (Divisibility)**.** "a divides b", notated as $a \mid b$, if $(\exists x)(b = ax)$

Can be expressed as "a divides b", "a is a divisor of b", "b is a multiple of a", "b is divisible by a"

Example 1.6. For what numbers b is it the case that $(\forall a)(b \mid a)$?
Solutions: $b = 1$, $b = -1$

DO 1.7. Prove that there exists no other solutions to the above example

Example 1.8. For what c is it true that $(\forall d)(d|c)$?
Solutions: $c = 0$

This becomes strange when we consider the statement $0 \mid 0$. However, this confusion can be resolved since divisibility is defined by multiplication, not division. (Therefore the constraint that we cannot divide by zero is not violated.)

Proposition 1.9 (Distributivity of multiplication over addition)**.** $(\forall x, y, z)(x(y + z) = xy + xz)$

This is a universal formula. (All variables are universally qantified.) When stating identities like this, we often omit the universal quantifiers.

Proposition 1.10 (Associativity of multiplication)**.** $(xy)z = x(yz)$

Proposition 1.11 (Commutativity of multiplication)**.** $(xy)z = x(yz)$

DO 1.12. Prove that if $a \mid b$ and $a \mid c$, then $a \mid b + c$ and $a \mid b - c$. Without English:

$$(\forall a, b, c)((a \mid b \;\&\; a \mid c) \implies a \mid b + c)$$

$$(\forall a, b, c)((a \mid b \;\&\; a \mid c) \implies a \mid b - c)$$

Answer what property of arithmetic is needed for this proof?

Definition 1.13. Given $A, B \subseteq \mathbb{Z}$, $c \in \mathbb{Z}$

$$A + B := \{a + b \mid a \in A, b \in B\}$$

$$AB := \{ab \mid a \in A, b \in B\}$$

$$A + c := A + \{c\} = \{a + c \mid a \in A\}$$

Example 1.14.

$$\begin{aligned} A &= \{2,7,9\} \\ c &= 5 \\ A+c &= \{7,12,14\} \\ B &= \{-1,2,5\} \\ A+B &= \{1,4,7,6,9,12,8,11,14\} \end{aligned}$$

$$\begin{aligned} D = \{1,2,3\} &= E \\ D+E &= \{2,3,4,5,6\} \end{aligned}$$

Definition 1.15 (Cardinality)**.** $|A|$ denotes the cardinality of A, i.e., the number of elements of A.

Example 1.16. Suppose A, B are finite sets.

$$|A+B| \leq |A|\,|B|$$

Example 1.17.

HW 1.18. Prove that, when A, B are non-empty, finite sets, $|A| + |B| - 1 \leq |A+B|$

Definition 1.19. An n-set is a set of n elements. If A is a set then B is a k-subset of A if $B \subseteq A$ and $|B| = k$.

Definition 1.20. The number of k-subsets of an n-set is denoted $\binom{n}{k}$ ("n choose k").

DO 1.21.

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots = 2^n.$$

Definition 1.22. Let $S(n,k)$ denote the number of subsets of a n-set that have a cardinality divisible by k. So

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = S(n,2)$$
$$\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \cdots = S(n,3)$$

DO 1.23.

$$S(n,2) = \frac{1}{2}2^n = 2^{n-1}$$

(This should be a "aha" proof)

CH 1.24. Show that

$$\left| S(n,3) - \frac{2^n}{3} \right| < 1$$

Definition 1.25. Where $A \subseteq \mathbb{Z}$ and $c \in \mathbb{Z}$:

$$cA := \{ca \mid a \in A\}$$

Example 1.26. $2\mathbb{Z}$ is the set of even numbers; $2\mathbb{Z} + 1$ is the set of odd numbers

HW 1.27. Let us for now accept the following fact without proof.

$$(\forall a, b)(\exists c)(a\mathbb{Z} \cap b\mathbb{Z} = c\mathbb{Z})$$

Express c in terms of a and b. (The answer should be half a line in unambiguous English; no proof is required.)