Discrete Math 37110 - Class 2 (2016-09-29)

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

Administrative Manners

- Discussion section Thursday 4:30-5:30 Ryerson 276 (Annex) [Starts today!]
- TA office hours:
  - Joseph Tsang - Monday 5-6pm Ryerson 162
  - Kai Li - Thursday 10:30-11:30am Ryerson 162

2.1 Material

Example 2.1 (Relation)**.** A is the set of triangles in the plane, R is the set of congruent pairs. Given t_1, t_2 triangles, $(t_1, t_2) \in R$ if and only if $t_1 \cong t_2$.

$A = \mathbb{Z}$, $R = \{(a, b) \mid a < b\}$ (less than relation) or $D = \{(a, b) \mid a < b\}$ (divides relation)

Definition 2.2 (Relation)**.** A relation R on a set A is a set $R \subseteq A \times A$. If $(a, b) \in R$, we write aRb.

Some properties a relation R can have:

Reflexive $(\forall a \in A)(aRa)$

Symmetric $(\forall a, b \in A)(aRb \implies bRa)$

Transitive $(\forall a, b, c \in A)((aRb)\ \&\ (bRc) \implies aRc)$
(Note that this must hold even if $a = c$)

Example 2.3. Reflexivity:

$<$	$a \not< a$	(This is actually irreflexive: $(\forall a)(a \not R a)$)
$\mid$	$a \mid a$	divisibility is reflexive
$\cong \triangle$	$a \cong a$	congruence of triangles is reflexive
"sibling or equal"	reflexive	

Symmetry:

$<$	NO
$\mid$	NO
$\cong \triangle$	YES
"sibling or equal"	YES

Transitivity:

$<$	YES
$\mid$	YES
$\cong \triangle$	YES
"sibling or equal"	YES

Definition 2.4 (Equivalence relation)**.** A relation R is an equivalence relation if it is reflexive, transitive, and symmetric.

Note: The only relations above that are equivalence relations are congruence of triangles and "sibling or equal."

Definition 2.5 (Partition)**.** A partition of A is a collection of non-empty disjoint sets of which the union is A.

$$A = B_1 \dot\cup \ldots \dot\cup B_k$$

The B_i are the *blocks* of the partition. The partition $\Pi = \{B_1, \ldots, B_k\}$ defines an equivalence relation R_Π if: $aR_\Pi b$ if $(\exists i)(a, b \in B_i)$ (meaning they belong to the same block).

Theorem 2.6 (Fundamental Theorem of Equivalence Relations)**.** *For every equivalence relation R over a set A, $\exists!$(unique) partition Π of A such that $R = R_\pi$.*

The blocks of Π are called the *equivalence classes* of R.

Note that equivalence relations are the way we form new *concepts* in mathematics as well as in real life: rational numbers are equivalence classes of fractions, colors are equivalence classes of objects (of the same color). Of course in real life, the boundaries are blurred.

DO 2.7. Prove this theorem.

Hint: For $a \in A$ let $[a] := \{b \in A \mid bRa\}$. Prove that $(\forall a, c)([a] = [c]$ or $[a] \cap [c] = \emptyset)$.

Example 2.8. To define the notion of "rational numbers," we define an equivalence relation on fractions with nonzero denominator:

$$\frac{a}{b} R \frac{c}{d} \text{ if } ad = bc$$

Prove that this is an equivalence relation. The rational numbers are the equivalence classes of this relation.

DO 2.9. Prove that divisibility is transitive:

$$(a \mid b \;\&\; b \mid c) \implies (a \mid c)$$

From what property of multiplication does this follow?

Definition 2.10 (Congruence modulo m)**.** $a \equiv b \mod m$ if $m \mid a - b$. In this case we say "a and b are congruent modulo m."

Example 2.11.

$$24 \equiv 3 \mod 7$$

$$-24 \equiv 4 \mod 7$$

DO 2.12. Prove that congruence modulo a fixed number m is an equivalence relation.

Example 2.13. When is $a \equiv b \mod 1$? (Always: $(\forall a, b)(1 \mid a - b)$)

When is $a \equiv b \mod 2$? (If a, b are both odd or both even; equivalently, when they have the same parity.)

When is $a \equiv b \mod 0$? (If and only if $a = b$)

$(\forall a)(a \equiv 0 \mod a)$

Definition 2.14 (Residue classes)**.** The equivalence classes of mod m congruence are called *residue classes* mod m.

DO 2.15. The number of residue classes mod m is $|m|$ except when $m = 0$. In that case, the residue classes are singletons $\{a\}$, and there are infinitely many of them.

Example 2.16. Residue classes mod 5:

$$\begin{array}{ccccc}
\vdots & \vdots & \vdots & \vdots & \vdots \\
-10 & -9 & -8 & -7 & -6 \\
-5 & -4 & -3 & -2 & -1 \\
\mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} \\
5 & 6 & 7 & 8 & 9 \\
10 & 11 & 12 & 13 & 14 \\
15 & 16 & 17 & 18 & 19 \\
\vdots & \vdots & \vdots & \vdots & \vdots
\end{array}$$

DO 2.17. Let $m > 0$. Prove: the residue classes mod m are $m\mathbb{Z}, m\mathbb{Z}+1, \ldots, m\mathbb{Z}+(m-1)$.

Definition 2.18. Modular addition: $[a]+[b] := [a+b]$ Modular subtraction: $[a]-[b] := [a-b]$

DO 2.19. Prove that:

$$(a \equiv a' \ (m)) \ \& \ (b \equiv b' \ (m)) \implies (a - b \equiv a' - b' \ (m)) \ \& \ (a + b \equiv a' + b' \ (m))$$

What property of divisibility does this depend on?

DO 2.20. Lemma: $a \equiv b \ (m) \implies ax \equiv bx \ (m)$

Theorem 2.21.

$$(a \equiv a' \ (m)) \ \& \ (b \equiv b \ (m)) \implies ab \equiv a'b' \ (m)$$

Sketch. Using the above DO exercise,

$$ab \equiv ab' \equiv a'b' \implies \text{(by transitive property of congruence) } ab \equiv a'b'.$$

□

Definition 2.22 (GCD)**.** d is **a** greatest common divisor of a and b if

1. d is a common divisior, meaning $d \mid a$ & $d \mid b$
2. d is a common multiple of all common divisors, i.e., $(\forall e)(((e \mid a) \,\&\, (e \mid b)) \implies (e \mid d))$

Note the indefinite article in the expression "a greatest common divisor" in this definition. Under this definition, d is not unique: if a number d satisfies this definition then $-d$ also satisfies it. So for instance both 4 and -4 are greatest common divisors of 8 and 12.

Such a "definition by wish-list" must be accompanied by a theorem that says that our wishes can be satisfied.

Theorem 2.23. *Every pair of integers has a greatest common divisor.*

(We shall prove this later.) Note that there is no exception here. What is a greatest common divisor of 0 and 0?

DO 2.24. Prove that the greatest common divisor is unique up to sign, i.e., if d and e are greatst common divisors of a and b, then $e = \pm d$.

Notation 2.25. If d and $-d$ are the greatest common divisors of a and b, we write $\gcd(a, b) = |d|$. For instance, $\gcd(8, 12) = 4$ and also $\gcd(8, -12) = 4$.

DO 2.26. Prove: $(\forall a)(\gcd(a, a) = \gcd(a, 0) = |a|)$. (Note: even $a = 0$ is not an exception: $\gcd(0, 0) = 0$. Most Discrete Math textbooks miss this; the definition of gcd as the "greatest" (in magnitude) common divisor would fail here.)

Definition 2.27 (Relatively prime)**.** a, b are relatively prime if $\gcd(a, b) = 1$

DO 2.28. Give an analogous definition of the least common multiple (lcm)

Proposition 2.29. *If* $\gcd(a, c) = 1$*, then* $\gcd(a, b) = \gcd(a, bc)$*.*

Theorem 2.30 (Fermat's Little Theorem)**.** *Let* p *be prime. Then if* $\gcd(a, p) = 1$*, then* $a^{p-1} \equiv 1 \mod p$*.*

HW 2.31. Give a direct proof of Fermat's Little Theorem for $p = 2, 3, 5$.

NOTE: check the course website for more HW problems.