Honors Discrete Mathematics

Instructor: Alexander Razborov, University of Chicago
razborov@math.uchicago.edu
Course Homepage: www.cs.uchicago.edu/~razborov/teaching/autumn19.html

Autumn Quarter, 2019

Prove all of your answers with reasonable degree of mathematical rigor. If you work with others put their names clearly at the top of the assignment. Everyone must turn in their own independently written solutions. Shopping for solutions on the Internet is strongly discouraged: if you do it nonetheless, you *must* cite your source and, as the very least, explain the solution in your own words.

Homework is due at the beginning of Wednesday class *unless* submitted by e-mail as a PDF file prepared from a TeX source. Electronic submissions conforming to these standards (no scans please!) are encouraged and accepted until Wednesday midnight by Leo at lenacore@uchicago.edu.

Homework 2, due October 23

1. An ordinal number α is *prime* if $\alpha = \beta\gamma$ implies that either $\beta = \alpha$ or $\gamma = \alpha$.

   (a) Prove that every ordinal α has a prime decomposition into finitely many prime ordinals: $\alpha = \mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_t$ (the order matters this time, of course, but we omit the brackets as multiplication is still associative).

   (b) Describe explicitly all prime ordinals $\alpha \leq \omega^2$.

   (c) Is the decomposition in item (a) always unique?

2. Which of the following facts are true for all $a, b, c \in \mathbb{N}$:

   (a) $\gcd(a + b, c) \leq \gcd(a, c) + \gcd(b, c)$

   (b) $\gcd(ab, c) \leq \gcd(a, c)\gcd(b, c)$

(c) $\gcd(ab, c) = \gcd(a, c)\gcd(b, c)$

(d) $\gcd(a, b) \cdot c = \gcd(ac, bc)$?

3. The *least common multiple* $\mathrm{lcm}(a, b)$ is defined as the smallest positive integer that is divisible by both a and b. Prove the identity

$$\mathrm{lcm}(\gcd(a, b), c) = \gcd(\mathrm{lcm}(a, c), \mathrm{lcm}(b, c)).$$

4. Describe explicitly the set of positive integers

$$\left\{ \gcd(n^2 + n + 1, n^2 - 3) \mid n \in \mathbb{N} \right\}.$$

5. Let R be a commutative ring, and $\mathcal{I}$ be the set of all its ideals (including trivial ones). For $I, J \in \mathcal{I}$, let

$$I + J \stackrel{\text{def}}{=} \{a + b \mid a \in I,\ b \in J\}$$
$$I \cdot J \stackrel{\text{def}}{=} \{a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \mid n \in \mathbb{N},\ a_1, \ldots, a_n \in I,\ b_1, \ldots, b_n \in J\}.$$

(a) Verify that $I + J$ and $I \cdot J$ are also ideals and that these two operations on $\mathcal{I}$ satisfy[1] all axioms of a commutative ring, except for one. For the written submission, identify this exceptional axiom and show you work for distributivity:

$$I \cdot (J + K) = IJ + IK,$$

$I, J, K \in \mathcal{I}$.

(b) Prove that

$$(I + K) \cdot (J + K) \subseteq IJ + K,$$

again for any ideals I, J, K.

(c) Is it always true that

$$(I + K) \cdot (J + K) = IJ + K?$$

[1] you will have to figure out first what ideals play roles of 0 and 1