Honors Discrete Mathematics

Instructor: Alexander Razborov, University of Chicago
razborov@uchicago.edu
Course Homepage: www.cs.uchicago.edu/~razborov/teaching/autumn25.html

Autumn Quarter, 2025

`Prove all of your answers with reasonable degree of mathematical rigor (feel free to ask us when in doubt). 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, and using AI or StackExchange is strictly prohibited, it` **shall be considered academic dishonesty and treated accordingly.**

Homework 3, due October 29

1. Prove that for any $n \geq 2$, $\phi(n^2)$ is *not* a perfect square.

2. The Mathematical Institute of Anchuria has been able to prove that there exist infinitely many primes p for which $q \stackrel{\text{def}}{=} 2p^2 + 1$ is also a prime. The Anchurian Central Bank has decided to commemorate this feat[1] by using in their RSA transactions only pairs (p, q) of that special form.

   Show how to break this version of RSA.

3. Let us call a function $f : X \longrightarrow Y$ *gorgeous* if for any function $g : Z \longrightarrow Y$ with $|Z| \leq 19$ there exists an injective function $h : Z \rightarrowtail X$ such that $g = f \circ h$. Let us call f *co-gorgeous* if for any $g : X \longrightarrow Z$, again with $|Z| \leq 19$, there exists a surjective $h : Y \twoheadrightarrow Z$ such that $g = h \circ f$.

[1] No sarcasm intended, if you are interested in the context, consult Wikipedia's article entitled "Landau's Problems"

(a) Describe the set of those positive integers n for which there exists a gorgeous function $f : [100] \longrightarrow [n]$.

(b) Describe the set of those positive integers n for which there exists a co-gorgeous function $f : [100] \longrightarrow [n]$.

4. Solve the following system of congruences:

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{5} \\ x \equiv 4 \pmod{7} \\ x \equiv 4 \pmod{9} \\ x \equiv 4 \pmod{11}. \end{cases}$$

5. Give a closed form expression for the number of ordered tuples $\langle A_1, \ldots, A_m \rangle$, where $A_1, A_2, \ldots, A_m \in \mathcal{P}([n])$ are such that $A_1 \subseteq A_2 \subseteq \ldots \subseteq A_m$.