Honors Discrete Mathematics

Instructor: Alexander Razborov, University of Chicago
razborov@math.uchicago.edu
Course Homepage: www.cs.uchicago.edu/~razborov/teaching/autumn17.html

Autumn Quarter, 2017

```
   Prove all of your answers.  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 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 at the Canvas.
```

Homework 3, due October 25

1. (**challenge problem**) An element e of a commutative ring is called an *idempotent* if $e^2 = e$.

   (a) How many idempotents does the ring $\mathbb{Z}_{100000}$ have?

   (b) How many solutions in that ring are there to the equation $x^3 = x$?

   ```
   Note.  A computational solution without justifying your answer
   will bring you zero credit.
   ```

2. Prove that in the ring $\mathbb{Z}[\sqrt{5}]$, 2017 and $1+\sqrt{5}$ are relatively prime, that is the ideal $(2017, 1+\sqrt{5})$ generated by them contains 1.

3. An equivalence relation $\approx$ is *finer* than another equivalence relation $\approx_1$ with the same ground set S if for all $x, y \in S$, $x \approx y$ implies $x \approx_1 y$. Given an arbitrary binary predicate $R(x, y)$, its *transitive symmetric*

closure (cf. [Rosen, Sct. 9.4]) is defined as the finest equivalence relation $\approx$ that contains R.

Determine transitive symmetric closures of the predicate $R(x, y) \equiv y \geq x + 3$ on the set $[n] \stackrel{\text{def}}{=} \{1, 2, \ldots, n\}$ for $n = 3, 4, 5, 6$.

4. Solve the following system of congruences:

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{5} \\ x \equiv 4 \pmod{7} \\ x \equiv 4 \pmod{13}. \end{cases}$$

`Note. For this exercise you may find useful to read the` *`constructive`* `proof of Chinese Remainder Theorem in Rosen's book.`