MAT 311 Introduction to Number Theory

# Problem Set 3

due Wednesday, February 18

Please prove all your answers.

**Problem 1.** Prove that a square of an integer cannot end by two odd digits (in decimal notation).

**Problem 2.** For $n$ integer, prove that if the last digit of $n^2$ is 5, then $n^2$ ends by 25 (in decimal notation).

**Problem 3.** Prove the following criterion for divisibility by 11: a natural number is congruent modulo 11 to an alternating sum of its digits. "Alternating" means taken with alternating signs, + for the units, − for tens, + for hundreds, etc. (Example: $123456 \equiv -1+2-3+4-5+6 \mod 11$.)

**Problem 4.** Let $f(x)$ be a polynomial with integer coefficients, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Suppose we are looking for (integer) solutions of a congruence $f(x) \equiv b \mod m$. Show that if two numbers are congruent mod $m$, and one is a solution, then the other is also a solution.
Thus it makes sense to talk about classes of solutions, or pick solutions in a complete residue system. By *number of solutions* for such a congruence we will understand the number of solutions in a complete residue system.

**Problem 5.** Let $f(x), g(x)$ be polynomials with integer coefficients, $p$ prime. Suppose

$$f(x) \equiv 0 \mod p$$

has exactly $k$ solutions (in the sense of Problem 4) while

$$g(x) \equiv 0 \mod p$$

has none. Show that

$$f(x)g(x) \equiv 0 \mod p$$

has exactly $k$ solutions. Is the same true if $p$ is not prime?

**Problem 6.** Exhibit (with proof) a reduced residue system modulo 7 composed entirely of powers of 3.

**Problem 7.** Solve the congruence $20x \equiv 4 \mod 30$ from scratch.

("From scratch" means if you find a theorem in the book that tells you how to get the answer, you may not just plug in numbers into that theorem. Neither may you copy the proof of such a theorem from the book, and then plug in numbers. I'd like you to figure out how to deal with this congruence!)