MAT 311 Introduction to Number Theory

Problem Set 3

Some solutions

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

Solution. Write $n = 10a+b$, with $0 \le b < 9$, then $n^2 = 100a^2+20ab+b^2$. The first term, $100a^2$, ends in two zeroes; the second ends in 0 and has an even digit in the tens place. Thus n^2 can only end in two odd digits if both digits in b^2 are odd. Looking at squares of all numbers from 0 to 9, we see that this never happens. (We can reduce the number of cases by looking at 1,3,5,7 and 9 only, as an even b would contribute an even last digit.

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).

Solution. If the last digit of n^2 is 5, $5|n^2$ and so $5|n$ (by prime decomposition theorem, for example: if 5 doesn't appear in prime decomposition of n, it won't appear in n^2). Then $n = 5k$, and k must be odd, for otherwise $10|n$ and n^2 ends in 0. So $n = 5(2a+1) = 10a+5$, and $n^2 = 100a^2 + 100a + 25$ ends in 25.

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: $123456 \equiv -1+2-3+4-5+6 \mod 11$.)

Solution. A number with digits $a_n a_{n-1} \dots a_2 a_1 a_0$ equals to $a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_2 10^2 + a_1 10 + a_0$ and is congruent to $\pm a_n \mp a_{n-1} \cdots + a_2 - a_1 + a_0$ since $10 \equiv -1 \mod 11$ and so $10^n \equiv 1$ for n even, $10^n \equiv -1$ for n odd (because we can multiply congruences and take powers).

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.

Solution. This follows from the fact that we can add congruences and multiply them.

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?

Solution. In plain language, solutions for $f(x)g(x) \equiv 0 \mod p$ are the residues x such that p divides the product $f(x)g(x)$. Given that p is prime and never divides $g(x)$, x can only be a solution if $p|f(x)$, so x must be among k solutions of $f(x) \equiv 0 \mod p$. Obviously, all of those solutions satisfy $f(x)g(x) \equiv 0 \mod p$.