

Math 575, Homework 3 (due Friday, Oct. 5).

Look at the problems in Niven, Zuckerman and Montgomery (Sect. 2.6, 2.7) to make sure you understand the material. Then hand in the following.

1. Let $f(x) = x^2 - x$ throughout.

(a) Show that for every prime number p and every positive integer k , the congruence $f(x) \equiv 0 \pmod{p^k}$ has precisely two solutions.

(b) Let m be a positive integer, and let s denote the number of different prime numbers dividing m . Show that the congruence $f(x) \equiv 0 \pmod{m}$ has precisely 2^s solutions.

2. (a) What are the solutions of the congruence $x^4 \equiv 1 \pmod{16}$?

(b) Apply Hensel's lemma to determine the number of solutions to the congruence $x^4 \equiv 1 \pmod{2^k}$ when $k \geq 5$.

(c) Prove that no integer $n \equiv 15 \pmod{16}$ can be the sum of 14 fourth powers. That is, prove for such n there are no integers x_1, \dots, x_{14} such that

$$x_1^4 + x_2^4 + \dots + x_{14}^4 = n.$$

3. Let $p \geq 2$ be a prime.

(a) Suppose that a and b are integers satisfying $D = a^2 - 4b \not\equiv 0 \pmod{p}$. Determine the possible number of solutions to the congruence

$$x^2 + ax + b \equiv 0 \pmod{p^k}.$$

[There are two possible answers.]

(b) Suppose that $p^r \mid (a^2 - 4b)$, with $r \geq 1$. Determine the possible number of solutions to the congruence

$$x^2 + ax + b \equiv 0 \pmod{p^k}.$$

(c) Suppose that the integer m has precisely s distinct prime divisors. Show that when $D = a^2 - 4b$ is nonzero, then the number of solutions of the congruence

$$x^2 + ax + b \equiv 0 \pmod{m},$$

is at most $2^s |D|^{\frac{1}{2}}$.

4. Suppose that $p \geq 5$ is prime, and that $(a, p) = 1$, and that the congruence $x^3 \equiv a \pmod{p}$ is solvable. By applying Hensel's lemma, show that the equation $x^3 \equiv a \pmod{p}$ has a p -adic solution. Deduce that the equation $x^3 = a$ has at most 3 solutions over the p -adic field \mathbb{Q}_p .

5. (a) Find a (nontrivial) solution of the congruence

$$x_1^3 + 2x_2^3 + 4x_3^3 + 7(x_4^3 + 2x_5^3) + 49(x_6^3 + 2x_7^3) \equiv 0 \pmod{7}.$$

(b) By fixing 6 of the 7 variables x_i , demonstrate by an application of Hensel's lemma that the equation

$$x_1^3 + 2x_2^3 + 4x_3^3 + 7(x_4^3 + 2x_5^3) + 49(x_6^3 + 2x_7^3) = 0.$$

has a nontrivial 7-adic solution.

(c) Use the same strategy to show that the number of solutions $N(7^k)$ of the congruence

$$x_1^3 + 2x_2^3 + 4x_3^3 + 7(x_4^3 + 2x_5^3) + 49(x_6^3 + 2x_7^3) \equiv 0 \pmod{7^k}.$$

is at least as large as $c_0 7^{6k}$ for some positive c_0 .

Note. One can conclude from (c) that the 7-adic density of solutions to the above equation is positive, in the sense that

$$\liminf_{k \rightarrow \infty} \frac{N(7^k)}{7^{6k}} > 0.$$