18.781 Problem Set 5

Thursday, April 5.

Collaboration is allowed and encouraged. However, your writeups should be your own, and you must note on the front the names of the students you worked with.

Extensions will only be given for extenuating circumstances.

1. Solve $x^2 \equiv 21 \pmod{41}$ using Tonelli's algorithm.
2. Let p be a prime congruent to 2 modulo 3, and let $(a, p) = 1$. Show that the congruence $x^3 \equiv a \pmod{p}$ has the unique solution $x \equiv a^{(2p-1)/3} \pmod{p}$.
3. (a) Let $f(x) = ax^2 + bx + c$, and let $D = b^2 - 4ac$ be the discriminant of this quadratic polynomial. Let p be an odd prime, such that $p \nmid a$. Show that if $p|D$ then $f(x) \equiv 0 \pmod{p}$ has exactly one solution. If $p \nmid D$ then $f(x) \equiv 0 \pmod{p}$ has either 0 or 2 solutions, and if x_0 is a solution, then $f'(x_0) \not\equiv 0 \pmod{p}$.

   (b) Show that if p is an odd prime, e a natural number, and $(a, p) = 1$, then $x^2 \equiv a \pmod{p^e}$ has exactly

   $$1 + \left(\frac{a}{p}\right)$$

   solutions.
4. Which of the following congruences have solutions, and how many?

   (a) $x^2 \equiv -2 \pmod{118}$.

   (b) $x^2 \equiv -1 \pmod{244}$.

   (c) $x^2 \equiv -1 \pmod{365}$.

   (d) $x^2 \equiv 7 \pmod{227}$.

   (e) $x^2 \equiv 267 \pmod{789}$.
5. Show that for all primes p, the congruence $x^8 \equiv 16 \pmod{p}$ has a solution.
6. Prove that there are infinitely many primes of the form $8k + 7$.
7. Determine, by congruence conditions, the set of primes p such that

   $$\left(\frac{10}{p}\right) = 1.$$
8. (a) Determine, by congruence conditions, the set of primes p such that -3 is a quadratic residue mod p.

   (b) Prove that there are infinitely many primes of the form of each of the forms $3k + 1$ and $3k - 1$.
9. (a) Let p be an odd prime, and let $(k, p) = 1$. Show that the number of solutions (x, y) to $y^2 \equiv x^2 + k \pmod{p}$ is exactly $p - 1$. (Hint: establish a bijection with solutions to $zw \equiv k \pmod{p}$.)

(b) Show that

$$\sum_{x=1}^{p} \left(\frac{x^2+k}{p} \right) = -1.$$

(c) Now let $(ab, p) = 1$. Show that the number of solutions of the congruence $ax^2 + by^2 \equiv 1 \pmod{p}$ is

$$p - \left(\frac{-ab}{p} \right).$$

10. Write a gp program to calculate the number of quadratic residues R and quadratic non-residues N in the set $\{1, 2, \ldots, (p-1)/2\}$ for any given odd prime p. Tabulate results for the first 100 odd primes. What do you observe? (Bonus) Supply a proof.

11. (Bonus) Let the residue classes $1, 2, \ldots, p-1$ modulo an odd prime p be divided into two nonempty sets S_1 and S_2 such that the product of two elements of the same set is in S_1, whereas the product of an element of S_1 and an element of S_2 is in S_2. Prove that S_1 consists of the quadratic residues and S_2 consists of the quadratic non-residues modulo p.

12. (Bonus) Properties of sign of a permutation. Recall that we defined the sign of a permutation σ to be (-1) raised to the number of inversions (i.e. pairs (i, j) such that $i < j$ but $\sigma(i) > \sigma(j)$).

    (a) Let s_i be the transposition $(i, i+1)$, i.e. the permutation which exchanges i and $i+1$ and leaves the other elements fixed. For two permutations π and σ of $\{1, 2, \ldots, n\}$ let $\pi\sigma = \pi \circ \sigma$ be the permutation σ followed by π. Check that πs_i is the permutation which takes j to $\pi(j)$ if $j \neq i, i+1$ and takes i to $\pi(i+1)$ and $i+1$ to $\pi(i)$. Show that the number of inversions of πs_i is one more or one less than the number of inversions of π.

    (b) Show that every permutation of $\{1, 2, \ldots, n\}$ is a product of transpositions of the form s_i.

    (c) Show that the sign of $\pi\sigma$ is the product of the signs of π and σ.

    (d) Show that the sign of a k-cycle is $(-1)^{k-1}$, and therefore that the sign of any permutation is (-1) raised to the number of even cycles in its disjoint cycle decomposition.