189-346/377B: Number Theory

Assignment 4

Due: Monday, February 26

1. Let d and p be primes. How many soltions to the equation $x^d = 1$ are there in $(\mathbf{Z}/p\mathbf{Z})^\times$? How many dth powers are there in $(\mathbf{Z}/p\mathbf{Z})^\times$?

2. Suppose p is a prime, and n and a are integers that are not divisible by p. Show that the number of solutions of the congruence equation

$$x^n \equiv a \pmod{p^e}, \quad 1 \leq x \leq p^e,$$

does not depend on e.

3. If the prime p does not divide the integer a, show that the sequence $a_n = a^{p^n}$ converges in $\mathbf{Q}_p$ (i.e., is Cauchy for the p-adic distance.) Show that $\alpha := \lim_{n\to\infty} a_n$ is a $(p-1)$st root of unity, and that all solutions to $x^{p-1} - 1$ in $\mathbf{Q}_p$ can be obtained in this way. Conclude that $i := \lim 2^{5^n}$ is a square root of -1 in $\mathbf{Q}_5$.

4. Apply the Gauss Lemma to directly compute the value of the Legendre symbol $(\frac{-2}{p})$ as a function of the prime p. Show that the result is consistent with the values for $(\frac{-1}{p})$ and $(\frac{2}{p})$ obtained in class.

5. Let p be a prime which is congruent to 3 modulo 4. Show that the square root of a mod p, if it exists, is equal to $a^{\frac{p+1}{4}}$. Conclude that therre is a polynomial time algorithm (in $\log(p)$) for calculating square roots mod p. (**377**: What if $p \equiv 1 \pmod 4$?)

6. Show that if p and $q = 2p+1$ are both odd primes, then -4 is a primitive root mod q.

7. Evaluate the Legendre symbols $(\frac{503}{773})$ and $(\frac{501}{773})$ using the law of quadratic reciprocity.

8. Decide (by hand, without a computer!) which of the following congruences have a solution:

a) $x^2 \equiv 2455 \pmod{4993}$;

b) $1709x^2 \equiv 2455 \pmod{4993}$;

c) $x^2 \equiv 245 \pmod{27496}$;

d) $x^2 \equiv 5473 \pmod{27496}$;

Try your hand at solving the congruence equations (either by hand, or, if you get tired, by computer.)

9. Show that for $p > 3$ prime, the congruence $x^2 \equiv -3 \pmod{p}$ is solvable if and only if p is of the form $3k+1$. **377:** Use this to show that there are infinitely many primes of the form $3k+1$.

10. **377**: Let a be an element of $(\mathbf{Z}/p\mathbf{Z})^\times$, and view the function $x \mapsto ax$ as a permutation on the $p-1$ elements in $(\mathbf{Z}/p\mathbf{Z})^\times$. Show that this permutation is even if $(\frac{a}{p}) = 1$, and is odd if $(\frac{a}{p}) = -1$. (This statement is known as Zolotarev's lemma.)