189-346/377B: Number Theory

Assignment 4

Due: Monday, March 7

1. Solve the equation
$$6^x = 11 \pmod{5^{12}}$$
by using the power series expansion for the logarithm, as seen in class. Some of this calculation is a bit tedious so you may want to do it on the computer. Check that the value of x you obtain is the correct one by computing $6^x \pmod{5^{12}}$ directly.

2. Show that 10^{101^j} converges to a square root of -1 in the field $\mathbf{Q}_{101}$ of 101-adic numbers.

3. Show that, if $\zeta = e^{(2\pi i)/5} = \cos 2\pi/5 + i \sin 2\pi/5$ is the primitive 5th root of unity, and if $\omega = \frac{-1+\sqrt{5}}{2}$ is the golden ratio, then
$$\zeta + \zeta^{-1} = \omega.$$
Use this to show that, if p is an odd prime, the Legendre symbol $(\frac{5}{p})$ is equal to 1 if and only $p \equiv \pm 1 \pmod 5$.

4. 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 there is a polynomial time algorithm (in $\log(p)$) for calculating square roots mod p.

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

6. 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.)

7. If n is an integer that is prime to 3, show that the all the odd primes dividing n^2+3 are congruent to 1 modulo 3. Use this to show that there are infinitely many primes of the form $3k+1$.

For Math 377 students only.

8. What can you say about exercise 4 when $p \equiv 1 \pmod{4}$?

9. 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.)

10. Can Hensel's lemma, which is used to solve equations of the form $f(x) = 0$ over the p-adic numbers when f is a polynomial, be extended to the setting where f is a *power series* with rational coefficients? Discuss. Use what you have learned to solve the equation

$$x + \log(x) = 4 \pmod{3^{10}}$$

numerically (on the computer). (Here $\log(x)$ refers to the 3-adic logarithm, which is given on $1+3\mathbf{Z}$ by the formula

$$\log(1+t) = \sum_{j=1}^{\infty}(-1)^{j+1}t^j/j.)$$