189-346/377B: Number Theory

Assignment 4

Due: Monday, March 7

1. Show that there is a unique $t \in \mathbf{Z}/(2 \cdot 3^{53}\mathbf{Z})$ satisfying the congruence equation

$$4^t = 7 \pmod{3^{54}},$$

and find its value using Pari. (You should check that your value of t is corect by plugging it into the equation above, at the end!)

2. Let p be a prime and let a be an integer which is relatively prime to p. Show that the sequence $a_n = a^{p^n}$ is a Cauchy sequence relative to the p-adic distance, and prove that its limit is a $(p-1)st$ root of unity in $\mathbf{Z}_p \subset \mathbf{Q}_p$, which is congruent to a modulo p.

3. Using the result of exercise 2 (or otherwise), show that there is a unique $(p-1)$-st root of unity in $\mathbf{Z}_p$ which is congruent to a modulo p.

4. Let $x_1, \ldots, x_n, \ldots$ be any sequence of elements of $\mathbf{Z}_p$. Show that there is an element $x \in \mathbf{Z}_p$ satisfying

$$x \neq x_n \pmod{p^n}, \qquad \text{for all } n \geq 1.$$

Use this to conclude that $\mathbf{Z}_p$ (and hence, *a fortiori*, $\mathbf{Q}_p$) is *uncountable*.

5. Let t be an integer and let p be a prime. Show that every element of $\mathbf{Z}/p\mathbf{Z}$ has a (unique) t-th root in $\mathbf{Z}/p\mathbf{Z}$ if and only if t is relatively prime to $p-1$.

6. Notations being as in question 5, show that the t-th root b of a can be written explicitly as

$$b = a^{\frac{1+(p-1)e}{t}} \pmod{p}$$

where e is any integer solution to the congruence equation

$$(p-1)e = -1 \pmod{t}.$$

Use this to describe an efficient, and completely deterministic, algorithm for extracting t-th roots in $\mathbf{Z}/p\mathbf{Z}$, under the assumption that $\gcd(t, p-1) = 1$.

7. Evaluate the Legendre symbols $(\frac{503}{777})$ and $(\frac{501}{777})$ using the law of quadratic reciprocity.

For Math 377 students only.

8. By adapting Hensel's Lemma (a.k.a. Newton iteration) to the more general setting where polynomials are replaced by power series, show that equation

$$x \log x = 3$$

has a unique solution in $1+3\mathbf{Z}_3$, and compute this solution modulo 3^{40} using PARI. (Here $\log(x)$ refers to the 3-adic logarithm, which is given on $1+3\mathbf{Z}$ by the formula

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