Homework
p-Adic Numbers

26th of July, 1999

Ali Nesin

Hensel's Lemma. *Let $f(X) \in \mathbb{Z}_p[X]$ and assume that there is an $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) \equiv 0 \pmod p$ and $f'(\alpha) \neq 0 \pmod p$. Then there is a $\beta \in \mathbb{Z}_p$ such that $f(\beta) = 0$ and $\beta \equiv \alpha \pmod p$.*

0. Prove Hensel's Lemma.

1. For what values of p does $x^2 + 1$ has a solution in $\mathbb{Q}_p$?

2. Show that an element $x \in \mathbb{Q}_p^*$ is a square if and only if it can be written as $x = p^{2n}y^2$ with $y \in \mathbb{Z}_p^*$. Conclude that $|\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2| = 2|\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2|$ and that if A is a set of representatives of $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2$, then $A \cup pA$ is a set of representatives of $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$.

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

3a. Show that there is an integer a such that

a) a is not a square in $\mathbb{Q}$,
b) p does not divide a,
c) $x^2 \equiv a \pmod p$ has a solution.

3b. Construct a sequence $(x_n)_{n \in \mathbb{N}}$ such that

a) $x_n \equiv x_{n-1} \pmod{p^n}$
b) $x_n^2 \equiv a \pmod{p^{n+1}}$

3c. Conclude that $\mathbb{Q}$ is not a complete field with respect to the p-adic valuation.

4. Show that a finite multiplicative subgroup of a field is cyclic. (**Hint:** We may suppose that the group is a p-group for some p).

5. Let p be a prime and m a nonzero integer.

5a. Let $1 \neq x \in 1 + p\mathbb{Z}_p$. Show that if $x^m = 1$ then p divides m.

5b. Let m not divisible by p. Let $A = \{x \in \mathbb{Q}_p : x^m = 1\}$. Show that $A \subseteq \mathbb{Z}_p$ and that the canonical map $\varphi : A \to \mathbb{Z}_p/p\mathbb{Z}_p$ is one-to-one.

5c. Conclude that if p does not divide m and if $\mathbf{Q}_p$ has a primitive m^{th} root of unity then, m divides $p - 1$.

5d. Conclude that $\mathbb{Q}_p$ is not an algebraically closed field.

6. Let p be a prime and m a nonzero integer that divides $p - 1$. Show that $\mathbb{Q}_p$ has a primitive m^{th} root of unity.

7a. Let $p \neq 2$ be a prime and let $a \in \mathbb{Z}_p^*$. Show that if there exists an element $b \in \mathbb{Z}_p$ such that $b^2 \equiv a \pmod{p\mathbb{Z}_p}$, then a is the square of an element in $\mathbb{Z}_p$.

7b. Conclude that if $p \neq 2$, then $\mathbf{Q}_p^*/ (\mathbf{Q}_p^*)^2 \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and if $c \in \mathbb{Z}_p^*$ is any element which is not a square modulo p, then the set $\{1, p, c, cp\}$ is a complete set of representatives of $\mathbb{Q}_p^*/ (\mathbb{Q}_p^*)^2$.

7c. Let $a \in \mathbb{Z}_2^*$. Show that a is a square in $\mathbb{Z}_2$ iff $a \equiv 1 \pmod 8$. Conclude that $\mathbb{Q}_2^*/ (\mathbb{Q}_2^*)^2 \approx (\mathbb{Z}/2\mathbb{Z})^3$ and $\{1, -1, 5, -5, 2, -2, 10, -10\}$ is a complete set of representatives of $\mathbb{Q}_p^*/ (\mathbb{Q}_p^*)^2$. (**Hint:** One needs a stronger version of Hensel's Lemma).