Math 254A, UC Berkeley, Fall 2001 (Kedlaya)
Problem Set 6: The p-adic Numbers/Completions
Due in class Monday, October 8

Please submit *eight* of the following problems. If you took the 1997 Putnam exam, please do not submit More on Valuations 1.

References. Neukirch, Sections 2.1 and 2.2 for valuations and the p-adic numbers; Section 2.4 for completions.

More on Valuations.

1. (1997 Putnam competition) For each positive integer n, write the sum $\sum_{m=1}^{n} \frac{1}{m}$ in the form $\frac{p_n}{q_n}$, where p_n and q_n are relatively prime positive integers. Determine all n such that 5 does not divide q_n.

2. (Manjul Bhargava) Let S be an infinite subset of $\mathbb{Z}$ and p a prime number. Pick $a_0 \in S$, then recursively define a_n as an integer $m \in S$ minimizing $v_p(m-a_0)+\cdots+v_p(m-a_{n-1})$. Prove that a polynomial with rational coefficients takes integer values on S if and only if it is an integer linear combination of the polynomials $P_n(x) = \prod_{i=0}^{n-1}(x-a_i)/(a_n-a_i)$. Optional bizarre consequence: the quantities $v_p(a_n-a_0)+\cdots+v_p(a_n-a_{n-1})$ for $n = 0, 1, \ldots$ do not depend on any choices made in defining the a_i.

3. Let K be a number field. Prove that $\alpha \in K$ is an algebraic integer if and only if $|\alpha|_{\mathfrak{p}} \leq 1$ for all nonzero prime ideals $\mathfrak{p}$ of $\mathfrak{o}_K$.

The p-adic Numbers.

1. Neukirch exercise II.1.1: A p-adic number a is a rational number if and only if its sequence of digits becomes periodic at some point. (Hint: write $p^m a = b + cp^l/(1-p^n)$ for $0 \leq b < p^l$, $0 \leq c < p^n$.)

2. Neukirch exercise II.2.4, modified: let $\epsilon \in 1 + p\mathbb{Z}_p$. Show that the function from $\mathbb{Z}$ to $\mathbb{Z}_p$ defined by $n \mapsto \epsilon^n$ extends to a function from $\mathbb{Z}_p$ to itself which is continuous with respect to the p-adic valuation. (Hint: one way to do this involves the binomial series $(1+x)^n = \sum_i \binom{n}{i} x^i$.)

3. Neukirch exercise II.2.6: The fields $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are not isomorphic unless $p = q$. (Hint: when do elements of $\mathbb{Q}_p$ have p-th roots?)

4. Neukirch exercise II.2.9 (p-adic Weierstrass Preparation Theorem): every nonzero power series $f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Z}_p[\![x]\!]$ admits a unique representation $f(x) = p^m P(x)U(x)$, where $U(x)$ is a unit in $\mathbb{Z}_p[\![x]\!]$ and $P(x) \in \mathbb{Z}_p[x]$ is a monic polynomial satisfying $P(x) \equiv x^l \bmod p$, where l is the degree of P.

5. Here's why not to define the n-adic numbers for n not prime. Let n be a composite positive integer, and define the ring $\mathbb{Z}_n$ as the set of sequences $\{x_i\}_{i=1}^{\infty}$, where $x_i \in \mathbb{Z}/n^i\mathbb{Z}$ and $x_{i+1} \equiv x_i \pmod{n^i}$. Prove that:

   (a) if n is a power of a prime p, then $\mathbb{Z}_n \cong \mathbb{Z}_p$;

   (b) if n is not a power of a prime, then $\mathbb{Z}_n$ has zerodivisors.

   Optional: prove that $\mathbb{Z}_n \cong \prod_p \mathbb{Z}_p$, where the product runs over all primes dividing n.

Completions.

Throughout this section, let R be a complete discrete valuation ring with maximal ideal $\mathfrak{m}$. If you wish, you may take R to be the valuation ring of a finite extension of $\mathbb{Q}_p$. You may even take $R = \mathbb{Z}_p$ if you wish.

1. (Newton's iteration) Let $P(x)$ be a monic polynomial over R and $r_0 \in R$ an element such that $|P(r_0)| < |P'(r_0)|^2$. Prove that the sequence $\{r_n\}_{n=0}^{\infty}$ given by the iteration $r_{n+1} = r_n - P(r_n)/P'(r_n)$ converges to a root r of $P(x)$, and that $v_p(r_n - p) \geq 2^{n-c}$ for some c. This gives a much faster method for computing (approximate) roots of polynomials than does the proof of Hensel's lemma.

2. Find a version of Newton's iteration that allows you to compute the multiplicative inverse of a unit $r \in R$ using only multiplications and additions, with a similar rate of convergence (i.e., you should need about $\log n$ steps to compute the inverse modulo $\mathfrak{m}^n$). Optional: implement your method in Magma.

3. (Eisenstein's irreducibility criterion) Let $P(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$ be a polynomial over R such that $a_1, \dots, a_n \in \mathfrak{m}$ and $a_n \notin \mathfrak{m}^2$. Prove that $P(x)$ is irreducible over R. Optional: use this to prove the polynomial $x^{p-1} + \cdots + x + 1$ is irreducible over $\mathbb{Z}$.

4. Assume $\mathfrak{m}$ is generated by the prime number $p \in \mathbb{Z}$ and that the map $x \mapsto x^p$ on $R/\mathfrak{m}$ is a bijection. (In other words, $R/\mathfrak{m}$ is *perfect*. For example, this is true if R is the valuation ring of a finite *unramified* extension of $\mathbb{Q}_p$.) Prove that for each $x \in R/\mathfrak{m}$, there exists a unique $y \in R$ which reduces to x modulo $\mathfrak{m}$, such that y has a p^n-th root for $n = 1, 2, \dots$. The element y is called the *Teichmüller lift* of x. (Hint: prove that x^{p^n} modulo p^{n+1} depends only on x modulo p.)

5. Show that for every automorphism τ of $R/\mathfrak{m}$, there exists a unique automorphism of R inducing τ on $R/\mathfrak{m}$. (Hint: every element of R can be written as a power series $\sum_{n=0}^{\infty} p^n y_n$, where each y_n is a Teichmüller lift.) If τ is the map $x \mapsto x^p$, the resulting automorphism of R is called the *Frobenius automorphism*.