**Math 254A, UC Berkeley, Fall 2001 (Kedlaya)**
**Lecture 14: The $p$-adic Numbers**
**September 28, 2001**

**Reference**. Neukirch, Sections 2.1 and 2.2.

**Outline of lecture**.

1. Define the $p$-adic integers $\mathbb{Z}_p$ naively, as "infinite series in $p$." Demonstrate addition, multiplication, additive inverses, multiplicative inverses. Define the $p$-adic numbers $\mathbb{Q}_p$ as infinite series in $p$ with finitely many places after the decimal point.

2. Define the $p$-adic integers less naively, as coherent sequences in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \cdots$.

3. Define the $p$-adic integers (resp., the $p$-adic numbers) even less naively, as the completion of $\mathbb{Z}$ (resp., of $\mathbb{Q}$) under the $p$-adic valuation. (We'll repeat this more generally in the next lecture.)

4. Notice that $\mathbb{Z}_p$ is a local ring with maximal ideal $p\mathbb{Z}_p$. (That is, every element of $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ is a unit.) In particular, any rational $r/s$, where $s$ is coprime to $p$, is a $p$-adic integer (in fact, a terminating or rational one, and conversely).

5. Demonstrate some simple cases of Hensel's lemma (simplest form: any monic polynomial over $\mathbb{Z}_p$ with a simple root modulo $p$ has a root in $\mathbb{Z}_p$). For example, if $n$ is a quadratic residue modulo $p$, then $n$ has two square roots in $\mathbb{Z}_p$. Consequence: the $p$-adic numbers include lots of algebraic numbers!

6. Note that since $\mathbb{Z}_p$ is complete with respect to the $p$-adic valuations, we can define some functions in terms of convergent power series. For example, if $p \neq 2$, then $\exp(x) = \sum_{n=0}^{\infty} x^n/n!$ and $\log(1+x) = \sum_{n=1}^{\infty} (-1)^{n-1} x^n/n$ converge for $x \in p\mathbb{Z}_p$

7. Mention that a polynomial $F(x_1, \ldots, x_n)$ has a zero in the $p$-adic integers if and only if it has a zero modulo every power of $p$.