Lisbon Summer School (2011) Problem Set 2
Christopher Skinner

These exercises vary in difficulty and importance. Try the ones that interest you. As in the lectures, p is always a prime number.

1. Let $F(x) \in \mathbf{Z}_p[x]$. Show that if $a, b \in \mathbf{Z}_p$ are congruent modulo p^k, $k \geq 1$, (that is, $a \equiv b \bmod p^k$) then $F(a) \equiv F(b) \bmod p^k$. Show also that $F'(a) \equiv F'(b) \bmod p^k$.

2. Prove that there is a (multiplicative) homomorphism $\omega : (\mathbf{Z}/p)^\times \to \mathbf{Z}_p^\times$ such that $\omega(a) \equiv a \bmod p$. Hint: Hensel's Lemma.

3. a) Give an example of an $0 \neq x \in \mathbf{Q}$ such that $x, 1/x \notin \mathbf{Z}$.

   b) Let $0 \neq x \in \mathbf{Q}_p$. Show that either $x \in \mathbf{Z}_p$ or $1/x \in \mathbf{Z}_p$.

4. a) What is the 3-adic expansion of -1? the 5-adic? the p-adic?

   b) Show that the 3-adic expansion with repeating coefficients

$$2 + 1 \cdot 3 + 2 \cdot 3^2 + 1 \cdot 3^3 + 2 \cdot 3^4 + \cdots$$

   is the 3-adic expansion of a rational number.

   c) Show that if the coefficients of the p-adic expansion of $x \in \mathbf{Q}_p$ are eventually periodic, then $x \in \mathbf{Q}$.

   d) What do you think is true in general about the coefficients of the p-adic expansion of a rational number?

5. Let ω be as in problem 2. Show that $\mathcal{R} = \{0, \omega(1), ..., \omega(p-1)\}$ is a complete set of representatives for the residue classes $\mathbf{Z}/p$. Show that every p-adic number $x \in \mathbf{Q}_p$ has an unique expansion

$$x = \sum_{i=-n}^{\infty} r_i p^{-i}, \quad r_i \in \mathcal{R}.$$

   You may want to think about how this expansion compares to the usual p-adic expansion (usefulness, ease of computation, etc.).

6. This exercise is taken from a problem set for a course on elliptic curves given by Kevin Buzzard. It establishes that the equation $3x^3 + 4y^3 = 5$ has a solution in $\mathbf{Q}_p$ for all primes p. This is the oft-cited example of Selmer of a genus one curve that has points in all completions of $\mathbf{Q}$ (that is, in $\mathbf{R}$ and each $\mathbf{Q}_p$) but not in $\mathbf{Q}$. The key to the exercise is Hensel's Lemma.

   a) Accept for the moment that there exists $y \in \mathbf{Q}_3$ such that $4y^3 = 5$. Deduce that there is a solution to $3x^3 + 4y^3 = 5$ in $\mathbf{Q}_3$. We will return to this fact in a later exercise (but go ahead and try to prove it).

   b) Prove that there exists $x \in \mathbf{Q}_5$ such that $3x^3 = 1$. Deduce that there is a solution to $3x^3 + 4y^3 = 5$ in $\mathbf{Q}_5$.

c) Suppose $p \neq 3, 5$. Show that either 3, 5, 15, or 45 is a cube in $\mathbf{Q}_p$. Hint: Divide $(\mathbf{Z}/p)^\times$ by the subgroup of cubes; this quotient has order either 1 or 3.

(i) If 3 is a cube in $\mathbf{Q}_p$, then show that there is a solution in $\mathbf{Q}_p$ with $y = 1$.

(ii) If 5 is a cube in $\mathbf{Q}_p$, then show that there is a solution in $\mathbf{Q}_p$ with $x = -y$.

(iii) If 15 is a cube in $\mathbf{Q}_p$, then show that there is solution in $\mathbf{Q}_p$ with $y = 5/7$.

(iv) If 45 is a cube in $\mathbf{Q}_p$, then show that there is a solution in $\mathbf{Q}_p$ with $y = 0$.