Lisbon Summer School (2011) Problem Set 3

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 $F(x) \in \mathbf{Z}_p[x]$. Suppose that $a_1 \in \mathbf{Z}_p$ is such that $F(a_1) \equiv 0 \bmod p$ but $F'(a_1) \not\equiv 0 \bmod p$. Hensel's Lemma asserts that the sequence $\{a_n\}$ defined recursively by

$$a_n = a_{n-1} - F(a_{n-1})/F'(a_{n-1})$$

converges in $\mathbf{Z}_p$ to a solution of $F(x) = 0$ (why is $a_n \in \mathbf{Z}_p$?). Show that this convergence is pretty fast: by an analysis of the proof of Hensel's Lemma, show that

$$F(a_n) \equiv 0 \bmod p^{2^n}.$$

(Note that the exponent of p is growing exponentially.)

2. Let Σ_n, $n \geq 1$, be non-empty finite sets. For each n, let $\phi_n : \Sigma_{n+1} \to \Sigma_n$ be a map of sets. Let

$$\Sigma = \{(\sigma_n) \in \prod_{n=1}^{\infty} \Sigma_n \ : \ \phi_n(\sigma_{n+1}) = \sigma_n\}.$$

Note that the definition of Σ does not preclude the possibility that Σ is empty.

a) Show that if the ϕ_n are all surjective, then Σ is non-empty.

b) For $m > n$, let $\Sigma_{n,m} \subseteq \Sigma_n$ be the image of

$$\phi_n \circ \phi_{n+1} \circ \cdots \circ \phi_{m-1} : \Sigma_m \to \Sigma_n.$$

(i) Show that for each n there exists $N_n > n$ such that $\Sigma_{n,m} = \Sigma_{n,N_n}$ if $m \geq N_n$.

(ii) Let $S_n = \Sigma_{n,N_n}$. Show that $\phi : S_{n+1} \to S_n$ is surjective

c) Using a) and b), conclude that Σ is non-empty.

3. Apply Problem 2 to solutions to equations in $\mathbf{Z}_p$: For $F(x_1, ..., x_s) \in \mathbf{Z}_p[x_1, ..., x_s]$, let

$$\Sigma_n := \{a = (a_1, ..., a_s) \in (\mathbf{Z}/p^n)^s \ : \ F(a) = 0\}$$

and $\phi_n : \Sigma_{n+1} \to \Sigma_n$ be

$$\phi_n(a) = (a_1 \bmod p^n, \ldots, a_s \bmod p^n) \in \Sigma_n.$$

Deduce that if $\Sigma_n \neq \emptyset$ for all n then $F(x_1, ..., x_n) = 0$ has a solution in $\mathbf{Z}_p$.

4. Evaluate the following:

a) $|15/7|_3$

b) $|2/25|_5$

5. Show that the numbers $\mathrm{ord}_p(2^n - 1)$ are unbounded (as $n > 0$ grows) for every prime $p \neq 2$. What about at 2?

6. Prove that
$$|a_1 + a_2 + \cdots + a_n|_p \leq \max\{|a_1|_p, ..., |a_n|_p\}.$$

7. Find a solution to $4y^3 \equiv 5 \mod 3^3$. Deduce that $4y^3 = 5$ has solution in $\mathbf{Q}_3$. This is the missing ingredient in the proof given in Problem 6, Problem Set 2, that the equation $3x^3 + 4y^3 = 5$ has solution in $\mathbf{Q}_p$ for each prime p.

8. This exercise marches you through a proof of Ostrowski's Theorem. Let $f : \mathbf{Q} \to \mathbf{R}_{\geq 0}$ be a non-trivial absolute value. That is:
$$(i)\ f(x) = 0 \iff x = 0, \quad (ii)\ f(xy) = f(x)f(y), \quad (iii)\ f(x + y) \leq f(x) + f(y),$$
and $f(x) \neq 1$ for some $x \neq 0$.

   <u>First Step</u>. Show that $f(\pm 1) = 1$. Show that $f(x)$ is completely determined by its values on the positive integers. Show that for any integer $a \geq 0$, $f(ax) \leq af(x)$.

   Now consider two cases:

   <u>Case I</u>. For at least one integer $m > 0$, $f(m) > 1$.

   a) Let $m > 1$ be the smallest positive integer such that $f(m) > 1$. Let $n > 1$ be any other integer. For any integer $t > 0$, write m^t in base n: $m^t = a_0 + a_1 n + \cdots + a_k n^k$ with $0 \leq a_i \leq m - 1$. Note that $k \leq t\frac{\log m}{\log n}$. By repeatedly using the triangle inequality (i.e., property (iii) of f) show that if $f(n) \leq 1$ then
$$f(m)^t = f(m^t) \leq (t\frac{\log m}{\log n} + 1)(n - 1).$$
   Deduce that this implies $f(m) \leq 1$, a contradiction. Conclude that $f(n) > 1$ for all $n > 1$. Hint: take tth roots and let $t \to \infty$.

   b) Let $m, n > 1$. By writing n^t in base m and m^t in base n, show that
$$f(n^t) \leq (t\frac{\log n}{\log m} + 1)(m - 1)f(m)^{t\frac{\log n}{\log m}}$$
   and
$$f(m^t) \leq (t\frac{\log m}{\log n} + 1)(n - 1)f(n)^{t\frac{\log m}{\log n}}.$$
   Take tth roots and let $t \to \infty$. Deduce that
$$f(n) = f(m)^{\frac{\log n}{\log m}}.$$

Writing $f(m) = |m|_\infty^\alpha$, with $|\cdot|_\infty$ the usual absolute value and $\alpha > 0$ a real number, conclude that

$$f(x) = |x|_\infty^\alpha$$

for all $x \in \mathbf{Q}$. So in this case, f is a power of the usual absolute value $|\cdot|_\infty$.

c) Show that $0 < \alpha \leq 1$. Hint: consider the triangle inequality.

<u>Case II</u>. For all integers $n > 0$, $f(n) \leq 1$. Since f is non-trivial, it must be that $f(m) < 1$ for some integer $m > 1$.

a) Let $m > 1$ be the smallest integer such that $f(m) < 1$. Show that m is a prime number, say p. Hint: if m is not prime, consider a factorization $m = ab$.

b) Let $n > 1$ be an integer prime to p (so $p \nmid n$). Show that $f(n) = 1$. Hint: write $1 = a_t p^t + b_t n$ for some integers a_t, b_t that may depend on t, and deduce that $1 \leq f(p)^t + f(n)$ and then let $t \to \infty$.

c) Conclude that $f(x) = |x|_p^\alpha$ for some $\alpha \geq 1$. Hint: write an integer n as $n = p^k m$ with $p \nmid m$; then $f(n) = f(p^k m) = f(p^k)f(m) = f(p^k) = f(p)^k$.

9. This problem shows that the congruence conditions in Problem I.4(iii) of Brian Conrad's lectures are equivalent to having a non-zero solution in $\mathbf{Q}_p$ to the ternary quadratic for all primes $p > 2$.

   Let $c_1, c_2, c_3 \in \mathbf{Z}\backslash\{0\}$ be pairwise coprime: $gcd(c_i, c_j) = 1$ if $i \neq j$. Let

$$F(x_1, x_2, x_3) = c_1 x_1^2 + c_2 x_2^2 + c_3 x_3^2.$$

   The congruence conditions are:

$$-c_i c_j \equiv \square \bmod c_k, \quad \{i, j, k\} = \{1, 2, 3\}.$$

   Assume these hold. Let p be an odd prime.

   a) Suppose $p \nmid c_1 c_2 c_3$. Show that there is a non-zero solution in $\mathbf{Q}_p$ to $F(x_1, x_2, x_3) = 0$. Hint: already done in the lectures.

   b) Suppose $p | c_1 c_2 c_3$. After renumbering the c_i if necessary, you may assume that $p | c_1$. Explain why c_2 and c_3 are not divisible by 3. Show that $c_2 = -c_1 a^2$ for some $a \in \mathbf{Z}_p^2$. Conclude that there is a non-zero solution in $\mathbf{Q}_p$ to the equation $F(x_1, x_2, x_3) = 0$.