These problems are related to the material covered in Lectures 8-9. I have made every effort to proof-read them, but there are may be errors that I have missed. The first person to spot each error will receive 1-5 points of extra credit.

The problem set is due by the start of class on 10/08/2013 and should be submitted electronically as a pdf-file e-mailed to the instructor. You can use the latex source for this problem set as a template for writing up your solutions; be sure to include your name in your solutions and remember to identify all collaborators and any sources that you consulted that are not listed in the syllabus.

Problem 1. A stronger form of Hensel’s lemma. (30 points)

(a) Let \( f \in \mathbb{Z}_p[x] \) and suppose \( |f(a)|_p < |f'(a)|_p^2 \) for some \( a \in \mathbb{Z}_p \). Let \( a_1 = a \), and for \( n \geq 1 \) let
\[
a_{n+1} = a_n - f(a_n)/f'(a_n).
\]
Prove that this defines a Cauchy sequence \((a_n)\) in \( \mathbb{Z}_p \) whose limit \( b \) uniquely satisfies \( f(b) = 0 \) and \( |a - b|_p < |f'(b)|_p \), and moreover, \( |f(a)|_p = |f'(b)|_p \). (you may find it helpful to reword this in terms of \( v_p \) and work with congruences modulo powers of \( p \)).

(b) Prove that the hypothesis in (a) is necessary in the following sense. Suppose that \( b \) is a simple root of a polynomial \( f \in \mathbb{Z}_p[x] \). Prove that for any \( a \in \mathbb{Z}_p \), if \( |a - b|_p < |f'(b)|_p \) then \( |f(a)|_p < |f'(a)|_p^2 \). Conclude that if no \( a \in \mathbb{Z}_p \) satisfies the hypothesis of (a), then \( f(x) \) does not have a simple root in \( \mathbb{Z}_p \).

(c) Use (a) to compute a square root of 57 in \( \mathbb{Z}_2 \) to 16 digits of 2-adic precision using \( a = 1 \). How many \( a_n \) do you need to compute to achieve this precision?

Problem 2. A faster form of Hensel’s lemma. (20 points)

(a) Let \( R \) be a commutative ring, let \( f \in R[x] \), and let \( m \in R \). Suppose that \( x_0, z_0 \in R \) satisfy \( f(x_0) \equiv 0 \mod m \) and \( f'(x_0)z_0 \equiv 1 \mod m \) (note that \( a \equiv b \mod m \) simply means that \( a - b \) is an element of the \( R \)-ideal \((m)) \). Let
\[
x_1 = x_0 - f(x_0)z_0,
\]
\[
z_1 = 2z_0 - f'(x_1)z_0^2.
\]
Prove that
\[
(i) \ x_1 \equiv x_0 \mod m,
(ii) \ f(x_1) \equiv 0 \mod m^2,
(iii) \ f'(x_1)z_1 \equiv 1 \mod m^2,
\]
and that (i) and (ii) uniquely characterize \( x_1 \) modulo \( m^2 \).

(b) Use part (a) to compute a cube-root of 9 in the ring \( \mathbb{Z}_{10} \) to 64 digits of 10-adic precision by working modulo \( 10, 10^2, 10^4, 10^8, 10^{16}, 10^{32}, 10^{64} \).

(c) Prove that Fermat’s last theorem is false in \( \mathbb{Z}_{10} \).
Problem 3. Applications of Hensel’s lemma (50 points)

Recall that every element of \( \mathbb{Q}_p^\times \) can be uniquely written as \( p^ru \) with \( r \in \mathbb{Z} \) and \( u \in \mathbb{Z}_p^\times \). Let \( \mathbb{Q}_p^{\times n} = \{ x^n : x \in \mathbb{Q}_p \} \) denote the set of \( n \)th powers in \( \mathbb{Q}_p^\times \).

(a) For all odd primes \( p \), prove that \( p^ru \) is a square in \( \mathbb{Q}_p^\times \) if and only if \( r \) is even and \( u \) is a square modulo \( p \). Conclude that \( \mathbb{Q}_p^\times /\mathbb{Q}_p^{\times 2} \cong (\mathbb{Z}/2\mathbb{Z})^2 \) (as finite abelian groups).

(b) Using the strong form of Hensel’s lemma, prove that \( 2^ru \) is a square in \( \mathbb{Q}_2^\times \) if and only if \( r \) is even and \( u \equiv 1 \mod 8 \). Conclude that \( \mathbb{Q}_2^\times /\mathbb{Q}_2^{\times 2} \cong (\mathbb{Z}/2\mathbb{Z})^3 \).

(c) Determine the structure of \( \mathbb{Q}_p^\times /\mathbb{Q}_p^{\times n} \) for all primes \( p \) and odd primes \( n \).

Let \( \mu_{n,p} = \{ x \in \mathbb{Q}_p : x^n = 1 \} \) denote the set of \( n \)th roots of unity in \( \mathbb{Q}_p \).

(d) Prove that \( \mu_{n,p} \) is a subgroup of \( \mathbb{Z}_p^\times \).

(e) Use Hensel’s lemma to prove that for \( p \nmid n \) the group \( \mu_{n,p} \) is cyclic of order \( \gcd(n,p-1) \).

(f) Let \( p \) be odd. Use the strong form of Hensel’s lemma to prove that \( \mu_{p,p} \) is trivial. Conclude that there are exactly \( p - 1 \) roots of unity in \( \mathbb{Q}_p \) (be sure to address \( \mu_{p^r,p} \)).

(g) Prove that \( \mu_{4,2} = \mu_{2,2} = \{ \pm 1 \} \). Conclude that \( \pm 1 \) are the only roots of unity in \( \mathbb{Q}_2 \).

Problem 4. Survey

Complete the following survey by rating each problem on a scale of 1 to 10 according to how interesting you found the problem (1 = “mind-numbing,” 10 = “mind-blowing”), and how difficult you found the problem (1 = “trivial,” 10 = “brutal”). Also estimate the amount of time you spent on each problem.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Interest</th>
<th>Difficulty</th>
<th>Time Spent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem 3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please rate each of the following lectures that you attended, according to the quality of the material (1 = “useless”, 10 = “fascinating”), the quality of the presentation (1 = “epic fail”, 10 = “perfection”), the pace (1 = “way too slow”, 10 = “way too fast”), and the novelty of the material (1 = “old hat”, 10 = “all new”).

<table>
<thead>
<tr>
<th>Date</th>
<th>Lecture Topic</th>
<th>Material</th>
<th>Presentation</th>
<th>Pace</th>
<th>Novelty</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/1</td>
<td>Hensel’s lemma</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/3</td>
<td>Quadratic forms</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Feel free to record any additional comments you have on the problem sets or lectures; in particular, how you think they might be improved.

---

1 Anytime \( \mathbb{Z}/p\mathbb{Z} \) (or any ring for that matter) appears in a context where a group is required, you can assume it is the additive group that is being referred to (one uses \( (\mathbb{Z}/p\mathbb{Z})^\times \) for the multiplicative group).