Homework 4

The homeworks are due on the Thursday of the week after the assignment was posted online[1]. Please hand in your homework at the beginning of the tutorial or bring it to the lecture on Thursday morning. You can work on and submit your homework in groups of two. Please staple your pages and write your names and matriculation numbers on the first page.

Problem 10 (10 pts.)

(i) Show that in Hensel's Lemma (as formulated in Corollary 1.2 in the script) one can weaken the condition $F'(\alpha_1) \not\equiv 0$ by replacing it with the condition

$$|F(\alpha_1)|_p < |F'(\alpha_1)|_p^2.$$

(ii) Show that there exists a *unique* $\alpha \in \mathbb{Z}_p$ with $F(\alpha) = 0$ and

$$|\alpha - \alpha_1|_p < |F'(\alpha_1)|_p.$$

(iii) Show that this version of Hensel's Lemma is more general than Corollary 1.2, in the sense that this version implies Corollary 1.2.

(iv) Find an example where this version can be used, but Corollary 1.2 cannot.

Solution. (i) The idea is to construct a Cauchy sequence $(\alpha_n)_{n\geq 1}$ satisfying $F(\alpha_n) \equiv 0 \pmod{p^n}$ and $\alpha_n \equiv \alpha_{n+1} \pmod{p^n}$.
We use the p-adic Newton method and define

$$\alpha_{n+1} = \alpha_n - \frac{F(\alpha_n)}{F'(\alpha_n)}.$$

Let $C := \left|\frac{F(\alpha_1)}{F'(\alpha_1)}\right|_p < 1$. By induction it is easy to show that the sequence (α_n) satisfies

1. $|\alpha_n|_p \leq 1$ for all n,
2. $|F'(\alpha_n)| = |F'(\alpha_1)|_p$,
3. $|F(\alpha_n)|_p \leq |F'(\alpha_1)|_p^2 C^{2^{n-1}}$.

Hint: use the following two identities. If $f \in \mathbb{Z}_p[X]$ and $x, y \in \mathbb{Z}_p$, then there is a $z \in \mathbb{Z}_p$ with

$$f(x+y) = f(x) + f'(x)y + zy^2$$

[1] This assignment is due Thursday, 07.11.19.

(just write $f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2$ for some $g \in \mathbb{Z}_p[X,Y]$) and also,

$$f(x) - f(y) = (x-y)G(X,Y)$$

for another poynomial $G(X,Y) \in \mathbb{Z}_p[X,Y]$. Thus, $|f(x)-f(y)|_p \leq |x-y|_p$.
Showing that the sequence is Cauchy is easy:

$$|\alpha_{n+1} - \alpha_n|_p = \left|\frac{F(\alpha_n)}{F'(\alpha_n)}\right|_p \leq |F'(\alpha_1)|_p C^{2^{n-1}}$$

and thus $|\alpha_{n+1} - \alpha_n|_p$ converges to 0.
The limit $\alpha = \lim_{n\to\infty} \in \mathbb{Z}_p$ satisfies $F(\alpha) = 0$ and $|F'(\alpha)|_p = |F'(\alpha_1)|_p$.
(ii) We have in fact

$$|\alpha_n - \alpha_1|_p = \left|\frac{F(\alpha_1)}{F'(\alpha_1)}\right|_p < |F'(\alpha_1)|_p$$

for all n. This is clear for $n = 2$ and for $n > 2$ it follows by induction. Taking the limit proves the claim.
(iii) Suppose $\beta \in \mathbb{Z}_p$ with $F(\beta) = 0$ and $|\beta - \alpha_1|_p < |F'(\alpha_1)|_p$. Thus, $|\beta - \alpha|_p < |F'(\alpha_1)|_p$ (all points in the ball are a center) and hence, if we write $\beta - \alpha = x$, then

$$0 = F(\beta) = F(\alpha + x) = F(\alpha) + F'(\alpha)x + zx^2 = F'(\alpha)x + zx^2$$

for some $z \in \mathbb{Z}_p$ as above. Suppose that $x \neq 0$ and hence $\beta \neq \alpha$. Then

$$F'(\alpha) = -zx$$

which yields the contradiction

$$|F'(\alpha)|_p \leq |x|_p < |\beta - \alpha|_p < |F'(\alpha)|_p.$$

Thus, $\beta = \alpha$ is the only root of F in the open ball of radius $|F'(\alpha_1)|_p$ around α_1.
(iv) Take, e.g., the polynomial $F(X) = X^2 - 17$ from Exercise 15. □

Problem 11 (10 pts.)

Prove that, for any prime p and any positive integer m not divisible by p, there exists a primitive m-th root of unity in $\mathbb{Q}_p$ if and only if m divides $p-1$.
Bonus (5 pts.): Let $p \neq 2$ be a prime number. Show that there are no primitive roots of unity of order p^n in $\mathbb{Q}_p$ for any $n \geq 1$. That is, the roots of unity in $\mathbb{Q}_p$ are exactly the $(p-1)$-st roots of unity.
Bonus (5 pts.): What about $p = 2$?

Solution. "⇐" First suppose $m \mid p-1$. The polynomial $f(X) = X^m - 1$ has m distinct roots modulo p because $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group of order $p-1$, and each of these roots lifts to $\mathbb{Z}_p$ by Hensel's Lemma. Among these roots, precisely $\varphi(m)$ have order m. "⇒" For the converse, notice that if $\alpha \in \mathbb{Q}_p$ has order m, then, since f is monic, it must be in fact that $\alpha \in \mathbb{Z}_p$ and (by Hensel) α is (congruent to) an element of order m modulo p, therefore $m \mid p-1$.
As for the bonus parts, we will show the only pth root of unity in $\mathbb{Z}_p^\times$ is 1 for odd p and the only 4th roots of unity in $\mathbb{Z}_2^\times$ are ± 1. This implies the only pth power roots of unity in $\mathbb{Z}_p^\times$ are 1 for odd p and ± 1 for $p = 2$ (since otherwise there would be pth roots of unity in

$\mathbb{Q}_p$, but we are going to show there aren't any).
Note that if $x^n = 1$ in $\mathbb{Q}_p$, then $|x^n|_p = 1$, which means $x \in \mathbb{Z}_p^\times$. For $p \neq 2$ suppose that $\zeta^p = 1$ in $\mathbb{Z}_p^\times$. Since $\zeta^p \equiv \zeta \pmod{p\mathbb{Z}_p}$, we have $\zeta \equiv 1 \pmod{p\mathbb{Z}_p}$. For the polynomial $f(X) = X^p - 1$ we have $|f'(\zeta)|_p = |p\zeta^{p-1}|_p = 1/p$ and the uniqueness in Hensel's Lemma implies that the ball

$$\{x \in \mathbb{Q}_p : |x - \zeta|_p < |f'(\zeta)|_p\} = \{x \in \mathbb{Q}_p : |x - \zeta|_p \leq 1/p^2\} = \zeta + p^2\mathbb{Z}_p$$

contains no pth root of unity except for ζ. We will now show that $\zeta \equiv 1 \pmod{p^2\mathbb{Z}_p}$, so 1 is in that ball and thus $\zeta = 1$. Write then $\zeta = 1 + py$, with $y \in \mathbb{Z}_p$, so that

$$1 = \zeta^p = (1 + py)^p = 1 + p^2 y + \sum_{k=2}^{p-1} \binom{p}{k} (py)^k + (py)^p.$$

For $2 \leq k \leq p - 1$, the binomial coefficient $\binom{p}{k}$ is divisible by p, so all terms in the sum over $2 \leq k \leq p - 1$ are divisible by p^3, and the $(py)^p$ is also divisible by p^3 (since $p \geq 3$). Therefore, reduction modulo 3 yields $1 \equiv 1 + p^2 y \pmod{p^3}$, hence $y \equiv 0 \pmod{p}$ and $\zeta \equiv 1 \pmod{p^2}$, which forces $\zeta = 1$.
Finally, if $\pm 1 \neq \zeta \in \mathbb{Z}_2^\times$ is a 4th root of unity, then $\zeta^2 = -1$, so $\zeta^2 \equiv -1 \pmod{4\mathbb{Z}_2}$. However, $\zeta \in \mathbb{Z}_2^\times \Longrightarrow \zeta \equiv 1 \text{ or } 3 \pmod{4\mathbb{Z}_2} \Longrightarrow \zeta^2 \equiv 1 \pmod{4\mathbb{Z}_2}$, and $1 \not\equiv -1 \pmod{4\mathbb{Z}_2}$. □

Problem 12 (10 pts.)

(i) Let $p \neq 2$ be a prime. Prove that the quotient group $G = \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ has order 4. Prove further that if $a \in \mathbb{Z}_p^\times$ is any element whose reduction modulo p is not a quadratic residue, then the set $\{1, a, p, ap\}$ is a complete set of coset representatives for G.
Hint: Prove that an element $x \in \mathbb{Q}_p$ is a square if and only if it can be written as $x = p^{2n}y^2$ with $n \in \mathbb{Z}$ and $y \in \mathbb{Z}_p^\times$.

(ii) Show that if $b \in \mathbb{Z}_2$ and $b \equiv 1 \pmod{8\mathbb{Z}_2}$ (so that in particular b is a 2-adic unit), then b is a square in $\mathbb{Z}_2$. Conversely, show that any 2-adic unit which is a square is congruent to 1 modulo 8. Conclude that the group $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ has order 8, and that it is generated by the classes of $-1, 5$ and 2 (so that a complete set of coset representatives is given by $\{1, -1, 5, -5, 2, -2, 10, -10\}$).

(iii) **Bonus (5 pts):** Let $p \neq 3$ be a prime and let $b \in \mathbb{Z}_p^\times$ be a p-adic unit. If there exists $c \in \mathbb{Z}_p$ such that $b \equiv c^3 \pmod{p}$, prove that b is a cube in $\mathbb{Z}_p$. Prove, further, that a 3-adic unit b is a cube in $\mathbb{Z}_3$ if and only if $b \equiv \pm 1 \pmod{9}$.

Solution. (i) This basically follows from the hint. (ii) The first assertion is yet another application of the stronger Hensel's Lemma. For the second, write a 2-adic unit in the form $1 + 2x$, square it, $(1 + 2x)^2 = 1 + 4x(x + 1)$, etc. To prove the final claim, one can argue in a similar way to part (i). Taking quotients in $\mathbb{Q}_2^\times$, any representative is of the form $1, 2, y$ or $2y$ for $y \in \mathbb{Z}_2^\times$ a 2-adic unit. Now, we know that y is a square iff $y \equiv 1 \pmod{8}$, so there are 3 choices for a non-square y in $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$, namely $-5, 5$ and -1. The conclusion now follows easily. (iii) Apply the stronger Hensel to $X^3 - b$. As for the second claim, there is an $e \in \{0, \pm 1\}$ such that $b \equiv \pm(1 + 3e)^3 \pmod{27}$. Now apply stronger Hensel to $f(X) = X^3 - b$ with $a_0 = \pm(1 + 3e)$. □

The following exercises will be discussed in the tutorial and you do not need to hand in solutions for them.

Exercise 13

Is it true that a polynomial $f \in \mathbb{Z}[X]$ is irreducible in $\mathbb{Q}[X]$ if and only if it is irreducible in $\mathbb{Q}_p[X]$ for every $p \leq \infty$? What happens if we replace irreducible by reducible?

Solution. The "if" part is true, because if a polynomial is reducible over $\mathbb{Q}$, it certainly is reducible over every $\mathbb{Q}_p$. The "only if" part is not; for instance, take $X^2 - 6$, which is reducible over $\mathbb{Q}_5$, or $X^2 + 1$, which is reducible over $\mathbb{Q}_2$, as $X^2 + 1 = (X + 1)^2$ modulo 2. In general, $X^4 + 1$ is a polynomial that is irreducible over $\mathbb{Q}$, but reducible over every $\mathbb{Q}_p$. This can be seen with a bit of number theory. We know that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

and

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$$

If 2 is a square mod p, that is, $p \equiv \pm 1 \pmod 8$, there exists a such that $a^2 = 2 \pmod p$, and we write $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 + 1 - aX)(X^2 + 1 + aX)$. If -2 is a square mod p, that is, $p \equiv 1$ or $3 \pmod p$, there exists b such that $b^2 = -2 \pmod p$, and we write $X^4 + 1 = (X^2 - 1)^2 - (-2)X^2 = (X^2 - 1 - bX)(X^2 - 1 + bX)$. If -1 is a square mod p, that is, $p \equiv \pm 1 \pmod 4$, then we have $X^4 + 1 = X^4 - (-1) = (X^2 - c)(X^2 + c)$, for some c such that $c^2 = -1 \pmod p$. This shows that the statement with "irreducible" replaced by "reducible" is also false. □

Exercise 14

Let $p \neq 2$ be a prime, and let $b \in \mathbb{Z}_p^\times$ be a p-adic unit. If there exists α_1 such that $\alpha_1^2 \equiv b \pmod{p\mathbb{Z}_p}$, then b is the square of an element of $\mathbb{Z}_p^\times$.

Solution. Apply Hensel's Lemma to $X^2 - b$. Clearly, as $b \in \mathbb{Z}_p^\times$ and $p \neq 2$, we have $2\alpha_1 \not\equiv 0 \pmod p$. □

Exercise 15

Show that the equation

$$(X^2 - 2)(X^2 - 17)(X^2 - 34) = 0$$

has a root in $\mathbb{Q}_p$ for all $p \leq \infty$, but it has no roots in $\mathbb{Q}$.

Solution. Let $f(X) = (X^2 - 2)(X^2 - 17)(X^2 - 34)$. Certainly f has real roots (recall that $\mathbb{Q}_\infty = \mathbb{R}$) and no rational roots. For $p \neq 2, 17$, one applies again Hensel's Lemma. If neither 2 nor 17 are squares modulo p, then their product is. (This can be easily seen either by using Legendre symbols, $\left(\frac{34}{p}\right) = \left(\frac{17}{p}\right)\left(\frac{2}{p}\right) = (-1)(-1) = 1$, or by recalling that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, hence being a square means being an even power of the generator, so that the product of two non-squares is the product of two odd powers of the generator.) In other words, there is α such that $f(\alpha) \equiv 0 \pmod p$ and it is clear that $f'(\alpha) = 2\alpha \not\equiv 0 \pmod p$,

hence there is a solution $x \equiv \alpha \pmod{p\mathbb{Z}_p}$ of $f(X) = 0$.
For $p = 2$, note that 17 is a square in $\mathbb{Q}_2$. For example, this can be seen using Hensel's Lemma as formulated in Problem 10. For $p = 17$, note that $6^2 \equiv 2 \pmod{17}$ and one can use the normal Hensel Lemma. □