# 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.

**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 $p = 2$?

**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 $y \in \mathbb{Z}_p^\times$.

[1]This assignment is due Thursday, 07.11.19.

(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 $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ 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 $b \equiv \pm 1 \pmod{9}$.

*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?

**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 $\alpha_1$ such that $\alpha_1^2 \equiv b \pmod{p\mathbb{Z}_p}$, then $b$ is the square of an element of $\mathbb{Z}_p^\times$.

**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 $\mathbb{Q}$.