Algebraic Number Theory

Problem sheet 7

The following problems somewhat build on each other. The goal here is to verify the first case of Fermat's Last Theorem for regular prime exponents.

1. (3 points) Let $\mathcal{O}_n$ be the ring of integers in the nth cyclotomic field and $u \in \mathcal{O}_n^\times$ be a unit. Verify that $\frac{u}{\overline{u}}$ is a root of unity. Show, moreover, that $\frac{u}{\overline{u}}$ is a p^kth root of unity whenever $n = p^k$ for some odd prime p prímre, ie. there is a group homomorphism
$$\begin{aligned} \mathcal{O}_{p^k}^\times &\to \mu_{p^k} \\ u &\mapsto \frac{u}{\overline{u}} \,. \end{aligned}$$

2. (3 points) Let p be an odd prime. Show that any element u in $\mathcal{O}_{p^k}^\times$ can be written as $u = \zeta v$ where ζ is some p^kth root of unity and $v \in \mathcal{O}_{p^k} \cap \mathbb{R}$ is real.

   Assume from now on that $p \nmid xyz$ are integers such that $x^p + y^p = z^p$ ($2 < p$ prime).

3. (1+1 points) Investigating modulo 9 and modulo 25 show that $p \neq 3, 5$.

   Assume from now on that $p > 5$ and put ζ for a fixed primitive pth root of unity.

4. (1 point) Show that we may assume that x, y, z are pairwise coprime and $p \nmid x - y$.

5. (2 points) Verify that $x + y, x + y\zeta, \dots, x + y\zeta^{p-1}$ are pairwise coprime in $\mathcal{O}_p$.

6. (2 points) Show that $\alpha^p \in \mathbb{Z} + p\mathcal{O}_p$ for all $\alpha \in \mathcal{O}_p$ (ie. there is an $a \in \mathbb{Z}$ such that $a - \alpha^p$ is divisible by p).

7. (2 points) Let $\alpha = a_0 + a_1\zeta + \dots a_{p-1}\zeta^{p-1}$ where $a_i \in \mathbb{Z}$ ($i = 0, \dots, p-1$) and $a_i = 0$ for at least one index i. Assume $\alpha \in n\mathcal{O}_p$ for some integer $n \in \mathbb{Z}$ and show that $n \mid a_i$ for all $i = 0, \dots, p-1$.

8. (2 points) Show that if the class number of a number field is not divisible by p and the pth power of an ideal is principal then the ideal itself is principal.

9. (3 points) Assume p does not divide the class number of $\mathcal{O}_p$. Prove that the equation $x^p + y^p = z^p$ does not have any integral solutions with $p \nmid xyz$.

   Hint: write the equation as $\prod_{j=0}^{p-1}(x + y\zeta^j) = (z)^p$. Write both sides as a product of prime ideals in $\mathcal{O}_p$. Using previous problems we may write $x + \zeta^j y$ in the form $x + \zeta^j y = u_j\alpha_j^p$ where $u_j \in \mathcal{O}_p^\times$ is a unit and $\alpha_j \in \mathcal{O}_p$. Now apply Problem 6 to α_1 and Problem 2 to u_1 in order to find an integer $r \in \mathbb{Z}$ such that $x + \zeta y \equiv \zeta^r va \pmod{p}$ where $v \in \mathbb{R}$, $a \in \mathbb{Z}$. Conjugating the previous congruence we obtain $p \mid x + \zeta y - \zeta^{2r}x - \zeta^{2r-1}y$. Deduce a contradiction using Problem 7.