Algebraic Number Theory

Problem sheet 7

to be handed in until 15th November 2018

The following problems build somewhat on each other. The goal here is to show the first case (ie. assuming $p \nmid xyz$) of Fermat's Last Theorem ($x^p + y^p = z^p \Rightarrow xyz = 0$) for regular (ie. p does not divide the class number of $\mathbb{Q}(\mu_p)$) primes.

1. (3 points) Verify that $\frac{u}{\overline{u}}$ is a root of unity for any unit $u \in \mathcal{O}_n^\times$ where $\mathcal{O}_n$ denotes the ring of integers in the nth cyclotomic field. Show moreover, that whenever $n = p^k$ for some odd prime p then $\frac{u}{\overline{u}}$ is even a p^kth root of unity. In particular, we have 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 and denote by $\mathcal{O}_{p^k}$ the ring of integers in the p^kth cyclotomic field. Show that any unit $u \in \mathcal{O}_{p^k}^\times$ can be written as $u = \zeta v$ where ζ is a p^kth root of unity and $v \in \mathbb{Z}[\zeta] \cap \mathbb{R}$ is real.

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

3. (1+1 pont) Reducing modulo 9 show $p \neq 3$. Reducing modulo 25 show $p \neq 5$.

   Assume from now on $p > 5$ and let ζ be a fixed primitive pth root of 1.

4. (1 pont) Reduce to the case when the numbers x, y, z are pairwise coprime and $p \nmid x - y$.

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

6. (2 points) Show that for any $\alpha \in \mathcal{O}_p$ we have $\alpha^p \in \mathbb{Z} + p\mathcal{O}_p$ (ie. there exists $a \in \mathbb{Z}$ 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 $i \in \{0, \dots, p-1\}$. Verify that whenever α lies in $n\mathcal{O}_p$ for some $n \in \mathbb{Z}$ then we have $n \mid a_i$ for all $i = 0, \dots, p-1$.

8. (2 points) Show that if p does not divide the class number of a number field K and A^p is principal for some ideal $A \lhd \mathcal{O}_K$ then in fact A is principal.

9. (3 points) Assume that p does not divide the class number of $\mathcal{O}_p$. Show that Fermat's equation $x^p + y^p = z^p$ does not admit a solution with $p \nmid xyz$. Hint: write the equation as $\prod_{j=0}^{p-1}(x + y\zeta^j) = (z)^p$. Factorize both sides in $\mathcal{O}_p$ as a product of prime ideals. Note that we have $x + \zeta^j y = u_j \alpha_j^p$ for some unit $u_j \in \mathcal{O}_p^\times$ and $\alpha_j \in \mathcal{O}$ $(j = 0, \ldots, p-1)$. 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 $v \in \mathbb{R}$ and $a \in \mathbb{Z}$. Conjugate the last congruence to deduce $p \mid x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y$. Obtain a contradiction using problem 7.