Uppsala University
Department of Mathematics
Ernst Dieterich

Algebraic number theory
Spring term 2012
March 29

Home assignments

Third set

9. Prove that if p is a prime number and $(x, y, z) \in \mathbb{Z}^3$ is a primitive non-trivial solution to $X^p + Y^p = Z^p$, then $\gcd(x, y) = 1$.

10. During the lectures we proved for every prime number p and $\zeta = e^{\frac{2\pi}{p} i}$ the following

Proposition 7. *Let $x, y \in \mathbb{Z}$ be relatively prime.*

(i) If $p \not| (x + y)$, then $(x + \zeta^i y) + (x + \zeta^j y) = \mathbb{Z}[\zeta]$ for all $0 \leq i < j \leq p - 1$.

(ii) If $p|(x + y)$, then $(x + \zeta^i y) \subset (\zeta - 1) \neq \mathbb{Z}[\zeta]$ for all $0 \leq i \leq p - 1$.

Rewrite the statements of Proposition 7 and find elementary proofs for them in the special case $p = 2$.

11. Let p be a prime number, $\zeta = e^{\frac{2\pi}{p} i}$, and $\Phi_p(X) = 1 + X + \ldots + X^{p-1}$.

(a) Show that the evaluation map

$$\varepsilon : \mathbb{Z}[X] \to \mathbb{Z}[\zeta], \ \varepsilon(f(X)) = f(\zeta)$$

induces a ring isomorphism

$$\varepsilon_1 : \mathbb{Z}[X]/(\Phi_p(X)) \xrightarrow{\sim} \mathbb{Z}[\zeta],$$

a bijection of ideals

$$\varepsilon_2 : (X - 1, \Phi_p(X))/(\Phi_p(X)) \xrightarrow{\sim} (\zeta - 1),$$

and an isomorphism of quotient rings

$$\varepsilon_3 : \mathbb{Z}[X]/(X - 1, \Phi_p(X)) \xrightarrow{\sim} \mathbb{Z}[\zeta]/(\zeta - 1).$$

Please turn over!

(b) Show that the evaluation map

$$\delta : \mathbb{Z}[X] \to \mathbb{Z},\ \delta(f(X)) = f(1)$$

induces a ring isomorphism

$$\delta_1 : \mathbb{Z}[X]/(X-1) \xrightarrow{\sim} \mathbb{Z},$$

a bijection of ideals

$$\delta_2 : (X-1, \Phi_p(X))/(X-1) \xrightarrow{\sim} (p),$$

and an isomorphism of quotient rings

$$\delta_3 : \mathbb{Z}[X]/(X-1, \Phi_p(X)) \xrightarrow{\sim} \mathbb{Z}/(p).$$

(c) Combine (a) and (b) to establish a ring isomorphism $\varphi : \mathbb{Z}[\zeta]/(\zeta-1) \xrightarrow{\sim} \mathbb{Z}/(p)$.

(d) Conclude that $\zeta - 1$ is a prime element in the ring $\mathbb{Z}[\zeta]$.

12. Prove statement (ii) of the following

Proposition 8. *Let p be a prime number, and $\zeta = e^{\frac{2\pi}{p}i}$.*

(i) If p is regular, then all ideals I in $\mathbb{Z}[\zeta]$ satisfy: if I^p is principal, then I is principal.

(ii) If p is irregular, then there exists an ideal I in $\mathbb{Z}[\zeta]$ which satisfies: I^p is principal and I is not principal.

Comment. During the lectures we proved statement (i), which marks one of two instances in Kummer's approach to Fermat's Last Theorem where regularity of the prime exponent p is needed. For a proof of statement (ii) I give the hint to make use of Cauchy's Theorem, which is a special case (and a historical predecessor) of the First Sylow Theorem.

Every exercise gives at most 5 points. Your assignments should be handed in to me or my mailbox not later than Monday, April 16, 10 a.m. Delayed exercises will in general be ignored. Exceptions are possible, but they require your explanation and my approval in advance.