

Domácí úkol do semináře z teorie čísel, 12. týden (5.12.2013)

Nechť p je libovolné prvočíslo splňující $p \equiv 1 \pmod{8}$. Cílem tohoto úkolu je dokázat, že grupa $C(-4p)$ tříd forem diskriminantu $-4p$ obsahuje prvek řádu 4.

1. Dokažte, že $C(-4p) \cong \mathbb{Z}_{2^a} \times G$ pro vhodnou grupu G lichého řádu a vhodné $a \in \mathbb{N}$.
2. Dokažte, že existuje liché $b \in \mathbb{Z}$ nesoudělné s p tak, že $b^2 \equiv \frac{p+1}{2} \pmod{p}$.
3. Dokažte, že forma $f = 2x^2 + 2xy + \frac{p+1}{2}y^2$ je redukovaná forma diskriminantu $-4p$, a určete řád třídy, která ji obsahuje, v grupě $C(-4p)$.
4. Dokažte, že f i hlavní forma $x^2 + py^2$ patří do stejného genu.
5. Dokažte, že grupa $C(-4p)$ tříd forem diskriminantu $-4p$ obsahuje právě dvě (navzájem inverzní) třídy řádu 4.

[Návod:

1. Vysvětlete, proč z věty o struktuře konečných komutativních grup plyne, že stačí ověřit, že v $C(-4p)$ existuje právě jeden prvek řádu 2. K tomu stačí spočítat μ pro $D = -4p$ pomocí Proposition 3.11.

2. Užijte vzorec pro Legendreův symbol $\left(\frac{2}{p}\right)$.

3. Užijte Lemma 3.10.

4. Ukažte, že obě formy vyjadřují čísla ze zbytkové třídy $\left[\frac{p+1}{2}\right]_{4p}$.

5. Užijte větu 3.15.]