Leibniz Universität Hannover
Fakultät für Mathematik und Physik
Prof. Dr. M. Schütt
MSc. S. Brandhorst

12. April 2016

Einführung in die Algebraische Zahlentheorie
Sommersemester 2016
Blatt 2

Hinweis: Für manche (Teil)Aufgaben ist der Einsatz eines gängigen Computeralgebra-Systems empfehlenswert

1. Sei K ein Körper.
   (a) Sei $K \subset L$ eine endliche Körpererweiterung. Zeige, dass L der ganze Abschluß von K in L ist.
   (b) Sei $K(t)$ der Körper der rationalen Funktionen über K. Zeige, dass K ganzabgeschlossen in $K(t)$ ist.

2. Sei $\mathbb{Q} \subset K$ eine quadratische Körpererweiterung und sei $x \in K$. Zeige, dass x genau dann ganz über $\mathbb{Q}$ ist, wenn $N_{K/\mathbb{Q}}(x)$ und $Tr_{K/\mathbb{Q}}(x)$ ganze Zahlen sind.

3. Finde eine Formel für die Anzahl von Möglichkeiten, eine gegebene ganze Zahl n als Summe von zwei Quadraten zu schreiben (In Abhängigkeit von der Primfaktorzerlegung von n).

   (a) Berechnen Sie die Legendre-Symbole $\left(\frac{79}{97}\right)$, $\left(\frac{307}{877}\right)$ und $\left(\frac{3163}{7001}\right)$.

   (b) Für welche Primzahlen $p \geq 7$ ist -15 ein quadratischer Rest modulo p?
   Geben Sie Ihre Antwort in Abhängigkeit von der Restklasse von p modulo 60 an.

   Hinweis: Die möglichen Reste einer Primzahl $p \geq 7$ modulo 60 sind gegeben durch $\mathbb{Z}_{60}^{\times}$ (warum?). Berechnen Sie das Legendre–Symbol $\left(\frac{-15}{p}\right)$.

   (c) Wie bestimmt man eine Lösung von $x^2 \equiv a \bmod p$ falls $\left(\frac{a}{p}\right) = +1$? Zeigen Sie:
   (i) Falls $p \equiv 3 \bmod 4$, so ist $x = a^{\frac{p+1}{4}} \bmod p$ eine Lösung.
   (ii) Falls $p \equiv 5 \bmod 8$, so ist $a^{\frac{p-1}{4}} \equiv \pm 1 \bmod p$ (warum?) und

$$\left.\begin{array}{ll} x = a^{\frac{p+3}{8}} \bmod p, & \text{falls } a^{\frac{p-1}{4}} \equiv +1 \bmod p; \\ x = 2a \cdot (4a)^{\frac{p-5}{8}} \bmod p, & \text{falls } a^{\frac{p-1}{4}} \equiv -1 \bmod p; \end{array}\right\} \text{ eine Lösung.}$$

   Hinweis: Gute Ideen für $p \equiv 1 \bmod 8$ sind herzlich willkommen!