Algebraische Zahlentheorie
1. Übungsblatt

TECHNISCHE UNIVERSITÄT DARMSTADT

Fachbereich Mathematik
Prof. Dr. J. H. Bruinier
Dipl.-Math. E. Hofmann

SS 2010
21. April 2010

Gruppenübung

Aufgabe G1 (Fermat Vermutung für $n = 4$)
In dieser Aufgabe soll die Fermatsche Vermutung für den Fall $n = 4$ durch ein Abstiegsargument bewiesen werden. Grundlage dafür ist folgende Beobachtung:
Hat die Gleichung $x^4 + y^4 = z^4$ eine Lösung in positiven ganzen Zahlen, so auch die Gleichung $x^4 + y^4 = w^2$. Sei nun x, y, w eine Lösung mit w kleinstmöglich. Dann bilden x^2, y^2 und w ein primitives Pythagoräisches Tripel.
Wir nehmen oBdA an, x sei ungerade und schreiben nun

$$x^2 = m^2 - n^2,\ y^2 = 2mn \qquad \text{und} \quad w = m^2 + n^2,$$

mit m und n teilerfremden ganzen Zahlen, die nicht beide ungerade sind.

(a) Zeigen Sie: Es gibt positive ganze Zahlen r und s, so dass gilt

$$x = r^2 - s^2,\ n = 2rs \qquad \text{und} \quad m = r^2 + s^2.$$

Dabei sind r und s teilerfremd und nicht beide ungerade.

(b) Weisen Sie nach, dass r, s und m paarweise koprim sind.
Folgern Sie weiter aus der Gleichung $y^2 = 4rsm$, dass r, s und m Quadrate positiver ganzer Zahlen sind.

(c) Beweisen Sie nun: Schreibt man $r = a^2$, $s = b^2$ und $m = c^2$, so hat man $a^4 + b^4 = c^2$, im *Widerspruch* zur Minimalität von w.

In den folgenden Aufgaben bezeichne p eine ungerade Primzahl und ω die p-te Einheitswurzel $\omega = e^{2\pi i/p}$. Weiter seien x, y und z positive ganzzahlige Lösungen der Fermat Gleichung

$$x^p + y^p = z^p, \tag{**}$$

wobei wir annehmen, dass $\mathrm{ggT}(x, y, z) = 1$ und $p \nmid x, y, z$ gilt (erster Fall in der Vorlesung). Wie in der Vorlesung denke man sich (**) als multiplikative Gleichung in $\mathbb{Z}[\omega]$ geschrieben

$$\left(x + y\right)\left(x + y\omega\right) \cdot \dots \cdot \left(x + y\omega^{p-1}\right) = z^p. \tag{***}$$

Aufgabe G2
Weisen Sie folgende Identität nach (Hinweis: Kreisteilungspolynom)

$$\left(1 - \omega\right)\left(1 - \omega^2\right) \cdot \dots \cdot \left(1 - \omega^{p-1}\right) = p.$$

Aufgabe G3
Wir nehmen an, $\mathbb{Z}[\omega]$ sei ein faktorieller Ring. Es gelte nun $\pi \mid x + y\omega$ für ein Primelement π von $\mathbb{Z}[\omega]$.
Weisen Sie nach: π teilt keinen weiteren Faktor der linken Seite von (***).
Zeigen Sie hierzu, dass andernfalls π sowohl z als auch yp teilen würde. Aber z und yp wurden als teilerfremd angenommen; also hat man $zm + ypn = 1$. Dies ist ein Widerspruch (Begründung!).

Aufgabe G4
Benutzen Sie Aufgabe G3 um folgende Aussagen zu beweisen. Ist $\mathbb{Z}[\omega]$ faktorieller Ring, so gilt

$$x + y\omega = u\alpha^p,$$

mit $\alpha \in \mathbb{Z}[\omega]$ und einer Einheit u aus $\mathbb{Z}[\omega]^\times$.