Algebraische Zahlentheorie
2. Übungsblatt

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

SS 2010
28. April 2010

Gruppenübung

Auch auf diesem Blatt bezeichne p ein ungerade Primzahl, und ω eine primitive p-te Einheitswurzel $\omega = e^{2\pi i/p}$.

Im Folgenden sind Kongruenzen modulo p in $\mathbb{Z}[\omega]$ bezüglich des von p erzeugten Hauptideals $p\mathbb{Z}[\omega]$ aufzufassen ebenso Teilbarkeit durch p.

Aufgabe G1
Weisen Sie nach, dass es zu jedem Element α in $\mathbb{Z}[\omega]$ eine ganze Zahl $a \in \mathbb{Z}$ mit

$$\alpha^p \equiv a \mod p.$$

(Hinweis: Benutzen Sie die Linearität modulo p des Frobeniushomomorphismus.)

In den folgenden Aufgaben sei $p \geq 5$. Wir bezeichen mit x, y und z eine Lösung in positiven ganzen Zahlen der Fermatgleichung $x^p + y^p = z^p$, wobei angenommen werden soll, dass x, y, z und p (paarweise) koprim sind.

Es soll gezeigt werden, dass aus $x + y\omega \equiv u\alpha^p \mod p$, mit $\alpha \in \mathbb{Z}[\omega]$ und u eine Einheit aus $\mathbb{Z}[\omega]^\times$, die Kongruenz $x \equiv y \mod p$ folgt.

Dazu wird folgendes Lemma benötigt:

Lemma 1 (Dirchlet)**.** *Ist u eine Einheit in $\mathbb{Z}[\omega]$ und $\bar{u}$ das komplex Konjugierte von u, so ist $\bar{u}/u$ eine Potenz von ω.*

Aufgabe G2
Zeigen Sie: Hat man $x + y\omega \equiv u\alpha^p \mod p$, so gibt es eine ganze Zahl k, für die gilt

$$x + y\omega \equiv \left(x + y\omega^{-1}\right)\omega^k \mod p.$$

Aufgabe G3
Nun soll die Aussage der Aufgabe G2 zu einem Widerspruch geführt werden, falls $k \not\equiv 1 \mod p$. Zeigen Sie zuerst Folgendes. Für $\alpha \in \mathbb{Z}[\omega]$ gelte $p \mid \alpha$. Schreibt man nun α als

$$\alpha = a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}, \quad \text{mit} \quad a_i \in \mathbb{Z},$$

so sind alle a_i durch p teilbar. Leiten Sie dann den behaupteten Widerspruch her.
(Hinweise: Nach Voraussetzung ist $p \geq 5$ und $p \nmid xy$, außerdem ist ω Wurzel des p-ten Kreisteilungspolynoms.)

Aufgabe G4
Zeigen Sie nun: Es gilt $x \equiv y \mod p$.

Aufgabe G5
Sei nun $\omega = \exp(2\pi i/23)$. Überprüfen Sie, dass das Produkt

$$\left(1+\omega^2+\omega^4+\omega^5+\omega^6+\omega^{10}+\omega^{11}\right)\cdot\left(1+\omega+\omega^5+\omega^6+\omega^7+\omega^9+\omega^{11}\right)$$

in $\mathbb{Z}[\omega]$ durch 2 teilbar ist, jedoch keiner der beiden Faktoren.

Bemerkung. *Man kann zeigen, dass* 2 *ein irreduzibles Element in* $\mathbb{Z}[\omega]$ *ist. Man sieht also:* $\mathbb{Z}[\omega]$ *ist kein faktorieller Ring.*