Übungen zur Elementaren Zahlentheorie

-4. Blatt-

Prof. Dr. K. Wingberg — SS 2007

J. Bartels — abzugeben bis Montag, den 21. Mai 2007 um elf Uhr

http://www.mathi.uni-heidelberg.de/~bartels/Uebungen.htm

Übungsleiter:

Aufgabe	1	2	3	4	$\sum$
Punkte					

„... Das Reziprozitätsgesetz erlaubt nun, für zwei gegebene Primzahlen p, q, läßt einen wissen, ob q ein quadratischer Rest modulo p ist oder nicht, vorausgesetzt, man weiß sowohl, ob a) p ein quadratischer Rest modulo q ist oder nicht und ob b) p und q kongruent 1 oder -1 modulo 4 sind. ... So, wie sich dasselbe Problem für zusammengesetzte Zahlen a leicht auf das Problem für Primzahlen zurückführen läßt, liefert dies Gesetz ein gutes Mittel, festzustellen, ob a ein quadratischer Rest modulo p ist oder nicht, unter der Bedingung, daß man ihre Primfaktorzerlegung kennt. Doch ist dieser praktische Nutzen rein gar nichts. Das Wichtige besteht in der Gesetzmäßigkeit. Es ist klar, daß die quadratischen Reste Progressionen liefern. Ist a ein quadratischer Rest modulo m, dann auch alle $a + mx$, doch ist es schön und überraschend, daß die Primzahlen p modulo denen m selbst ein quadratischer Rest ist, genau diejenigen sind, welche in gewissen Progressionen $\{b+x4m|x \in \mathbb{N}\}$ liegen. Für die Primzahlen in den anderen Progressionen ist m kein Quadrat modulo p. Das ist umso erstaunlicher, da man überhaupt nicht weiß über die Verteilung der Primzahlen innerhalb einer arithmetischen Progression..." *A. Weil, Une lettre à Simone Weil, 1940.*

---

1 . Aufgabe (6 Punkte):

Zeige:

a) Ist $p \neq 2$ eine Primzahl, dann ist $(\mathbb{Z}/p^n\mathbb{Z})^*$ zyklisch für jedes $n \in \mathbb{N}$.

Warum ist dies eine Gruppe? Bezüglich welcher Verknüpfung? Wieviele Elemente hat sie? Wieviele Quadrate gibt es darin? Nehmen wir die Zahlen 691 und 667. Woraus bestehen $(\mathbb{Z}/691^{5000}\mathbb{Z})^*$ und $(\mathbb{Z}/667^{5000}\mathbb{Z})^*$?

b) Für $p = 2$ gilt

$$(\mathbb{Z}/2^n\mathbb{Z})^* \approx \begin{cases} \mathbb{Z}/\mathbb{Z} & \text{wenn } n = 1 \\ \mathbb{Z}/2\mathbb{Z} & \text{wenn } n = 2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} & \text{wenn } n \geq 3 \end{cases} .$$

Man gebe Erzeuger von $(\mathbb{Z}/2^n\mathbb{Z})^*$ an. (Mit Begründung, warum es sich um solche handelt.) Wieviele Quadrate gibt es in $(\mathbb{Z}/2^n\mathbb{Z})^*$?

c) Für welche $m \in \mathbb{N}$ ist $(\mathbb{Z}/m\mathbb{Z})^*$ zyklisch?

2 . Aufgabe (6 Punkte):
Es sind folgende Aussagen gleichwertig:
I) Für ungerade Primzahlen p, q gilt

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

II) Für ungerade Primzahlen p, q und eine ganze Zahl $a \geq 1$ hat man für den Fall, daß $p \equiv \pm q (mod\ 4a), p \not| a$ gilt, folgende Gleichung

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

3 . Aufgabe (6 Punkte):
a) Wenn p eine Primzahl ist und a, b natürliche, (d.h. positive ganze $\sim$) Zahlen sind, dann folgt aus

$$2^p + 3^p = a^n, \text{ daß } n = 1 \text{ gilt.}$$

b) Für welche Werte a aus $\mathbb{Z}$ hat die Gleichung

$$x^2 + axy + y^2 = 1$$

unendlich viele Lösungen in $\mathbb{Z}$?

4 . Aufgabe (6 Punkte):
a) Finde alle Lösungen in den nicht-negativen ganzen Zahlen der Gleichung

$$a^2 + 5b^2 - 2c^2 - 2cd - 3d^2 = 0$$

b) Hat die Gleichung

$$x^2 + y^2 + z^2 + u^2 + v^2 = xyzuv - 65$$

eine Lösung in $\mathbb{Z}$, bei der jede dieser Zahlen größer als 7000 ist?
Hinweis: Man nehme sich eine Lösung und konstruiere eine, die aus größeren Zahlen besteht.