Zahlentheorie: Übungsblatt 6
(für die Übungen am 29./30. November 2012)

Aufgabe 1 (schriftlich)**.** (a) Berechnen Sie $\left(\frac{29}{53}\right)$.

(b) Sei p eine Primzahl. Zeigen Sie, dass 5 genau dann ein quadratischer Rest modulo p ist, wenn $p \equiv 1, 2, 9, 11$ oder $19 \pmod{20}$ ist.

Aufgabe 2 (schriftlich)**.** Sei p eine Primzahl der Form $p = 2^{4n} + 1$ (mit $n \in \mathbb{N}$).

(a) Zeigen Sie, dass $p \equiv 3$ oder $5 \pmod 7$.

(b) Zeigen Sie, dass 7 eine Primitivwurzel modulo p ist.

Aufgabe 3 (mündlich)**.** Sei $1 \neq a \in \mathbb{N}$ ungerade und $n \geq 3$ eine ganze Zahl. Zeigen Sie, dass a modulo 2^n genau Ordnung 2^{n-2} hat. Folgern Sie, dass es keine Primitivwurzeln modulo 2^n geben kann.

Aufgabe 4 (mündlich)**.** Sei p eine Primzahl der Form $4k + 1$ mit $k \in \mathbb{N}$. Ferner sei $h \in \mathbb{Z}$ mit $h^2 \equiv -1 \pmod p$ und $0 < h < p/2$.

(a) Zeigen Sie, dass p/h sich als Kettenbruch der Form $a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots\frac{1}{a_n+}\frac{1}{a_n+}\frac{1}{a_{n-1}+}\cdots\frac{1}{a_0}$ darstellen lässt.

(b) Setze $x = [a_0, \ldots, a_n]$ (in der Notation von Blatt 2) und $y = [a_0, \ldots, a_{n-1}]$. Zeigen Sie, dass $p = x^2 + y^2$.

(c) Benutzen Sie die ersten beiden Teile um 29 als Summe von zwei Quadraten zu schreiben.

Aufgabe 5 (mündlich)**.** Seien p und q ungleiche und ungerade Primzahlen. Sie dürfen in dieser Übung verwenden, dass

$$\left(\frac{q}{p}\right) = (-1)^{\sum_n [qn/p]},$$

wobei n in der Summe die geraden Zahlen $2, 4, \ldots, p-1$ durchläuft und $[k]$ die Gauss-Klammer einer Zahl k bezeichnet, also die größte ganze Zahl, die kleiner als k ist.

(a) Zeichnen Sie ein Rechteck R im $\mathbb{R}^2$ mit Endpunkten $(0,0), (p,0), (p,q)$ und $(0,q)$. Die Punkte mit ganzzahligen Koordinaten innerhalb oder auf dem Rand von R nennen wir die Gitterpunkte von R.

(b) Beweisen Sie das quadratische Reziprozitätsgesetz durch Zählen von Gitterpunkten (und unter Verwendung der obigen Formel), d.h. zeigen Sie, dass

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

http://www.mathematik.uni-stuttgart.de/studium/infomat/ZahlTheo-Koenig/