Übungen zur Zahlentheorie, WWU Münster, Mathematisches Institut, SoSe 2016
U. Hartl, K. Halupczok **Blatt Nr. 7**, 02.06.16

Abgabe: **Donnerstag, 9. Juni 2016**, bis 8:30 Uhr in die Briefkästen im Hörsaalgebäude

Leseaufgabe: Kapitel 3.2 bis Montag 6.6. und Kapitel 3.3 und 3.4 bis Donnerstag 9.6.

Aufgabe 1

(a) Sei p prim. Zeigen Sie durch Reduktion der Faktoren $1, \ldots, p-1$ in $(p-1)!$ auf den absolut kleinsten Rest mod p, dass gilt:

$$(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \bmod p.$$

(b) Geben Sie für $p \equiv 1 \bmod 4$ prim die Lösungen der Kongruenz $r^2 \equiv -1 \bmod p$ explizit an. Finden Sie auf diesem Wege die beiden Lösungen von $r^2 \equiv -1 \bmod 29$ (nach jeder Multiplikation kann mod 29 reduziert werden, um kleinere Zahlen zu erhalten).

(c) Sei $p \equiv 1 \bmod 4$ prim und $r \in \mathbb{Z}$ mit $r^2 \equiv -1 \bmod p$. Zeigen Sie, dass zwei der Zahlen $yr - x \in \mathbb{Z}$ (für natürliche Zahlen $x, y < \sqrt{p} + 1$) kongruent mod p sein müssen.

(d) Bestimmen Sie mit dem Ergebnis aus (c) für $p \equiv 1 \bmod 4$ prim zwei ganze Zahlen u, v mit $p = u^2 + v^2$, speziell auch für $p = 29$.

Aufgabe 2

(a) Sei $p \equiv 1 \bmod 4$ prim. Begründen Sie, warum die Kongruenz $x^2 + y^2 \equiv -1 \bmod p$ lösbar mit $y = 0$ ist.

(b) Sei $p \equiv 3 \bmod 4$ prim und $a \geq 2$ der kleinste quadratische Nichtrest mod p. Begründen Sie, warum die Kongruenzen $x^2 \equiv -a \bmod p$ und $y^2 \equiv a - 1 \bmod p$ beide lösbar sind und eine Lösung von $x^2 + y^2 \equiv -1 \bmod p$ ergeben.

(c) Leiten Sie aus (a) und (b) und der Euler-Identität Lemma 2.4.6 her, dass für jede natürliche Zahl n ein Vielfaches kn gleich der Summe von vier Quadratzahlen ist. (Der 4-Quadrate-Satz 2.4.5 von Lagrange besagt, dass dies bereits mit $k = 1$ der Fall ist.)

(d) Schreiben Sie ein Vielfaches der Zahl $n = 203 = 7 \cdot 29$ als Summe von vier Quadratzahlen, indem Sie (a), (b) und (c) explizit durchführen.

Aufgabe 3

(a) Zeigen Sie durch Untersuchung von Hindernissen modulo 8: Eine natürliche Zahl der Form $8m + 7$, $m \in \mathbb{N}_0$, lässt sich nicht als Summe dreier Quadratzahlen darstellen.

(b) Zeigen Sie durch Untersuchung von Hindernissen modulo 9: Eine natürliche Zahl der Form $9m + 4$ oder $9m + 5$, $m \in \mathbb{N}_0$, lässt sich nicht als Summe von drei oder weniger (positiven) Kubikzahlen schreiben.

bitte wenden

Aufgabe 4 (zur Klausurvorbereitung)

4.1 In $\mathbb{Z}/m\mathbb{Z}$ hat die Kongruenz $x^2 \equiv 1 \bmod m$ genau ____ Lösungen für $m = 105$, genau ____ Lösungen für $m = 21$ und genau ____ Lösungen für $m = 5$.

4.2 Sei p eine Primzahl > 2, und sei g eine primitive Wurzel mod p.
Dann ist g ein quadratischer _____ mod p.
Ist umgekehrt *jeder* quadratische Nichtrest eine primitive Wurzel mod p, dann ist p von der Gestalt $p = 1+$_____; hätte nämlich $p-1$ einen Primteiler $q \neq 2$, so wäre g^q ein quadratischer Nichtrest, aber keine primitive Wurzel mod p. Denn

$$\left(\frac{g^q}{p}\right) = \_\_\_\_ = (-1)^q = \_\_\_\_ \text{ und } \operatorname{ord}(g^q) = \_\_\_\_ \neq p-1 \text{ in } (\mathbb{Z}/p\mathbb{Z})^\times.$$

4.3 Ganze Zahlen x, y mit $92x + 125y = 1$ sind $x =$ ____, $y =$ ____.

4.4 Die Gruppe $(\mathbb{Z}/3^6\mathbb{Z})^\times$ hat die Ordnung $N =$ _____.