Goethe-Universität Frankfurt
Institut für Mathematik

Prof. Dr. Jakob Stix
Theresa Kumpitsch

Elementare Zahlentheorie

Wintersemester 2021/22

Übungsblatt 11 14.01.21

Aufgabe 1 (Obligatorische Primzahlaufgabe, 2 Punkte)**.**
Zeigen Sie, dass es unendlich viele Primzahlen $\equiv b \bmod 8$ für $b = 3, 5$ gibt.
Hinweis: Nehmen Sie dazu an, es gibt nur endlich viele Primzahlen $\equiv b \bmod 8$. Bezeichne n_b ihr Produkt. Betrachten Sie jeweils die Primfaktoren der Ausdrücke $n_b^2 + b - 1$ um den üblichen Widerspruch herzuleiten.

Aufgabe 2 (Hyperbeln, 4 Punkte)**.**
Sei p eine ungerade Primzahl und $(a, p) = 1$. Wir betrachten eine Hyperbel über $\mathbb{F}_p$ gegeben durch

$$H \coloneqq \left\{(x, y) \in \mathbb{F}_p \mid x^2 - y^2 \equiv a \pmod{p}\right\}.$$

(a) Zeigen Sie, dass H eine Parametrisierung über $\mathbb{F}_p$ besitzt, welche gegeben ist durch

$$x = \frac{at^{-1} + t}{2},\ y = \frac{at^{-1} - t}{2}, \quad t \not\equiv 0 \bmod p.$$

Tipp: Faktorisieren Sie $x^2 - y^2$.

(b) Folgern Sie, dass $\#H = p - 1$.

Aufgabe 3 (Affine diagonale Quadriken, 6 Punkte)**.**
Sei p eine ungerade Primzahl und a, b, c zu p teilerfremde ganze Zahlen. Wir betrachten eine affine Quadrik über $\mathbb{F}_p$, d.h.

$$Q \coloneqq \left\{(u, v) \in \mathbb{F}_p^2 : au^2 + bv^2 + c \equiv 0 \pmod{p}\right\}.$$

(a) Zeigen Sie, dass $\#\left\{x \in \mathbb{F}_p \mid x^2 \equiv j \pmod{p}\right\} = 1 + \left(\frac{j}{p}\right)$.

(b) Folgern Sie, dass

$$\#Q = \sum_{\substack{u,v, \bmod p \\ au+bv \equiv -c \bmod p}} \left(1 + \left(\frac{u}{p}\right)\right)\left(1 + \left(\frac{v}{p}\right)\right).$$

(c) Folgern Sie, dass

$$\#Q = p + \left(\frac{-b}{p}\right) \sum_{k=1}^{p-1} \left(\frac{ck^{-1} + a}{p}\right).$$

Tipp: In der Vorlesung wurde gezeigt, dass $\sum_{j=0}^{p-1} \left(\frac{j}{p}\right) = 0$. Überlegen Sie sich ferner, dass für alle $j \not\equiv 0 \bmod p$ gilt $\left(\frac{j^{-1}}{p}\right) = \left(\frac{j}{p}\right)$.

(d) Folgern Sie $\#Q = p - \left(\frac{-ab}{p}\right)$.

Aufgabe 4 (Kreisgleichung und Ergänzungssätze, 6 Punkte)**.**
Es sei $p > 2$ eine Primzahl. Für $a \in \mathbb{Z}$ mit $p \nmid a$ definieren wir

$$K_a \coloneqq \left\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid x^2 + y^2 \equiv a \pmod{p}\right\}.$$

(a) Zeigen Sie: $\#K_2 \equiv 4 + 2\left(\left(\frac{2}{p}\right) + 1\right) \pmod 8$.

Tipp: Sei $D_4 = \langle \sigma, \tau \mid \sigma^2 = \tau^2 = (\sigma\tau)^4 = 1 \rangle$ die Diedergruppe der Ordnung 8 . Betrachten Sie die Gruppenwirkung auf K_2 von D_4, die für $(x, y) \in K_2$ gegeben ist durch

$$\sigma(x, y) \coloneqq (x, -y) \text{ und } \tau(x, y) \coloneqq (y, x).$$

Sie dürfen davon ausgehen, dass es sich hier um eine wohldefinierte Gruppenwirkung handelt. Für welchen Punkt $(x, y) \in K_2$ hat die Bahn unter dieser Gruppenwirkung die Länge 8? Welche Bahnlänge haben dann die restlichen Punkte?

(b) Folgern Sie den ersten Ergänzungssatz:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4, \\ -1, & p \equiv 3 \pmod 4. \end{cases}$$

Tipp: Nutzen Sie Aufgabe 3.

(c) Folgern Sie den zweiten Ergänzungssatz:

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod 8, \\ -1, & p \equiv \pm 3 \pmod 8. \end{cases}$$

Tipp: Nutzen Sie Aufgabe 3.

Aufgabe 5 (Summe zweier Quadrat mod p, 2 Punkte)**.**
Sei p eine Primzahl. Zeigen Sie, dass sich jedes Element von $\mathbb{F}_p$ als Summe zweier Quadrate schreiben lässt.

Abgabe: Am kommenden Freitag, den **21.01.21**, bis um 12:00 digital auf OLAT.
