ELEMENTARE ZAHLENTHEORIE
11. Übungsblatt

Julia Sauter, Andrew Hubery

Aufgabe 1.

(a) Sei $p \geq 5$ eine Primzahl. Zeigen Sie, dass

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv \pm 1 \pmod{12} \\ -1 & \text{falls } p \equiv \pm 5 \pmod{12}. \end{cases}$$

(b) Zeigen Sie, dass es unendlich viele Primzahlen p gibt, mit $p \equiv 7 \pmod{12}$.

Hinweis: Seien $p_1, \ldots, p_r$ Primzahlen mit $p_i \equiv 7 \pmod{12}$. Setze $N \coloneqq (2p_1 \cdots p_r)^2 + 3$ und zeigen Sie, dass es eine Primteiler von N gibt, mit $q \equiv 7 \pmod{12}$ und $q \neq p_i$ für alle i.

(2+2 Punkte)

Aufgabe 2.

Betrachten Sie die Abbildung $(\mathbb{Z}/2^n\mathbb{Z})^\times \to (\mathbb{Z}/2^n\mathbb{Z})^\times$, $x \mapsto x^2$ für $n \geq 3$, mit Bild

$$QR = \{x^2 \pmod{2^n} \mid \mathrm{ggT}(2, x) = 1\}.$$

Seien $x, y \in (\mathbb{Z}/2^n\mathbb{Z})^\times$.

(a) Zeigen Sie, dass $x^2 \equiv 1 \pmod{2^n}$ genau dann, wenn $x \equiv \pm 1 \pmod{2^{n-1}}$.

(b) Zeigen Sie, dass $x^2 \equiv y^2 \pmod{2^n}$ genau dann, wenn $x \equiv \pm y \pmod{2^{n-1}}$. Es folgt, dass die Abbildung 4-zu-1 ist. Berechnen Sie $|Q|$.

(c) Wir wissen schon, dass jedes Element $x \in (\mathbb{Z}/2^n\mathbb{Z})^\times$ eindeutig als $(-1)^a 3^b$ mit $(a, b) \in (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z})$ geschrieben sein kann. Es folgt, dass $x^2 \equiv 3^{2b} \pmod{2^n}$.

Sei $T = \{1 + 8m \pmod{2^n}\}$. Zeigen Sie, dass $QR \subseteq T$ und dass $|Q| = |T|$. Folgern Sie, dass $QR = T$, also die quadratische Reste modulo 2^n sind genau die Restklassen der Form $1 + 8m \pmod{2^n}$.

(2+2+2 Punkte)

Aufgabe 3.

(a) Berechnen Sie die Jacobi-Symbole

$$\left(\frac{60}{233}\right), \qquad \left(\frac{62}{263}\right), \qquad \left(\frac{11847}{12707}\right).$$

(b) Ist 11847 ein quadratischer Rest modulo 12707?

(3+2 Punkte)

Abgabe: Montag 1. Juli, bis 12 Uhr in die Postfächer der Tutoren im V3–126

Aufgabe 4.

Sei $f = x^3 + x^2 + 20x + 3 \in \mathbb{Z}[x]$.

(a) Lösen Sie die Gleichung $f(x) \equiv 0 \pmod{5^k}$ für $k = 1, 2, 3$.

(b) Zeigen Sie, dass für alle $k \geq 3$ bestitzt f genau fünf Nullstellen $c \pmod{5^k}$ mit $c \equiv 6 \pmod{25}$.

Hinweis: Benutzen Sie Übungsblatt 10, Aufgabe 2 mit $k = 2$ und $m = 2$ um zu zeigen, welche von die fünf Zahlen $6 + 25a$ eine Nullstelle modulo 625 ist. Sei jetzt $6 + 25a_1$ eine Nullstelle modulo 125. Benutzen Sie 10.2 mit $k = 3$ und $m = 1$ um zu zeigen, dass jede $6 + 25a_1 + 125b$ eine Nullstelle modulo 625 ist.

Nun verwenden Sie Induktion. Seien $c + 5^{k-1}a$ die fünf Nullstellen modulo p^k. Benutzen Sie Übungsblatt 10, Aufgabe 2 mit $k - 1$ und $m = 2$ um zu zeigen, dass genau eine von den, sagen wir $\hat{c} = c + 5^{k-1}a_1$, kann zu einer Nullstelle modulo 5^{k+1}. Benutzen Sie nun k und $m = 1$ um zu zeigen, dass wir Nullstellen $\hat{c} + 5^k b$ modulo 5^{k+1} haben.

(c) Zeigen Sie, dass f genau elf Nullstellen modulo 5^k für alle $k \geq 3$ hat.

(2+2+1 Punkte)