ELEMENTARE ZAHLENTHEORIE
12. ÜBUNGSBLATT

DR. BAPTISTE ROGNERUD

Aufgabe 1. [2+1+2 Punkte] Sei $p \in \mathbb{P}_{>3}$. Zeigen Sie:

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

(b)
$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv 1 \pmod{6} \\ -1 & \text{falls } p \equiv -1 \pmod{6}. \end{cases}$$

(c) Zeigen Sie, dass es unendlich viele Primzahlen der From $6k+1$ für $k \in \mathbb{N}$ gibt.
(Hinweis: Betrachten Sie $(2p_1 \cdots p_t)^2 + 3$ and benutzen Sie $\left(\frac{-3}{p}\right)$ wie in Aufgabe 1 (a).)

Aufgabe 2. [3 Punkte]

(a) Berechnen Sie die Jacobi-Symbole
$$\left(\frac{6531}{2467}\right) \text{ und } \left(\frac{1356}{2467}\right).$$

(b) Ist 1356 ein quadratischer Rest modulo 2467?

Aufgabe 3. [4 Punkte]

Lösen Sie die Gleichung
$$x^2 \equiv 211 \pmod{159}.$$

Aufgabe 4. [4 Punkte] Sei $n \geqslant 3$. Zeigen Sie:

Die quadratischen Reste modulo 2^n sind $8m+1$ für $m \in \{0, 1, \cdots, \lfloor \frac{2^{n-1}-1}{4} \rfloor\}$.

(Hinweis: Zeigen Sie für $n \geqslant 3$ und $f = X^2 - (8m+1)$:

ist $f(c) \equiv 0 \pmod{2^n}$, so gilt entweder $f(c) \equiv 0 \pmod{2^{n+1}}$ oder $f(c + 2^{n-1}) \equiv 0 \pmod{2^{n+1}}$.)

Abgabe: Freitag, 6. Juli 2018, bis 10 Uhr in die Postfächer der Tutoren in V3-126.