Zahlentheorie – Blatt 9

Abgabe am 20.6.2017 bis 10:30 Uhr

1	2	3	4	Σ

.....
Name und Matr-Nr.

Bitte drucken Sie diese Seite aus und verwenden Sie sie als Deckblatt für Ihre Lösungen.

Wie üblich sind alle Antworten zu begründen/beweisen.

Aufgabe 1 (4 Punkte):

(a) Bestimmen Sie das Legendre-Symbol $\left(\frac{92}{167}\right)$.

(b) Wie viele Lösungen modulo 275 hat die Gleichung $X^2 + 3X + 5 = 0$?

Schreiben Sie jeweils auch Ihren Rechenweg auf.

Aufgabe 2 (4 Punkte):

(a) Zeigen Sie: Ist p eine Primzahl $\equiv 3 \mod 4$ und ist a ein quadratischer Rest modulo p, so sind die Lösungen von $X^2 \equiv a \mod p$ genau $X = \pm a^{\frac{p+1}{4}}$.

(b) Sei nun p eine Primzahl $\equiv 1 \mod 4$, und sei a ein quadratischer Rest modulo p. Kann es ein $r \in \mathbb{N}$ geben, so dass a^r eine Lösung modulo p von $X^2 = a$ ist? Gibt es immer ein solches r? Begründen Sie.

Aufgabe 3 (6 Punkte):

(a) Finden Sie alle Primzahlen $p \geq 5$, so dass -3 quadratischer Rest modulo p ist.
Hinweis: Bestimmen Sie, ob 3 und ob -1 ein quadratischer Rest modulo p ist.

(b) Zeigen Sie: Ist $a \in \mathbb{Z}$ und ist b ein Teiler von $4a^2 + 3$, so ist $b \not\equiv 2 \mod 3$.
Hinweis: Verwenden Sie (a); nehmen Sie zunächst an, dass b prim ist.

(c) Zeigen Sie, dass es unendlich viele Primzahlen $\equiv 1 \mod 3$ gibt.
Hinweis: Verwenden Sie (b).

Aufgabe 4 (2 Punkte):

Zeigen Sie: 7 ist Primitivwurzel modulo p für jede Primzahl der Form $p = 2^n + 1$ mit $n \geq 2$ und $3 \nmid n$.

Hinweis: Es reicht zu zeigen, dass 7 ein quadratischer Nichtrest modulo p ist. (Warum?)