1	2	3	4	Σ

.....
Name und Matr-Nr.

Zahlentheorie – Blatt 7

Abgabe am 6.6.2017 bis 10:30 Uhr

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) In welchen der folgenden Fälle gibt es ganze Zahlen x_j, y_j, so dass $a_j x_j + b_j y_j = c_j$ ist? Geben Sie ggf. solche x_j, y_j an oder begründen Sie, dass es sie nicht gibt.

(i) $a_1 = 15, b_1 = 24, c_1 = 12$ (ii) $a_2 = 15, b_2 = 24, c_2 = 10$

(b) In welchen der folgenden Fälle ist der angegebene Ringhomomorphismus

$$\mathbb{Z}/a_j b_j \mathbb{Z} \to \mathbb{Z}/a_j\mathbb{Z} \times \mathbb{Z}/b_j\mathbb{Z}, \qquad n \bmod a_j b_j \mapsto (n \bmod a_j, n \bmod b_j)$$

ein Isomorphismus? Geben Sie entweder ein Element von $(\mathbb{Z}/a_j b_j \mathbb{Z}) \setminus \{0\}$ an, das auf 0 abgebildet wird oder geben Sie Urbilder von $(0,1)$ und $(1,0)$ unter der obigen Abbildung an und begründen Sie, dass aus der Existenz dieser Urbilder schon folgt, dass es sich um einen Isomorphismus handelt.

(i) $a_1 = 10, b_1 = 14$ (ii) $a_2 = 11, b_2 = 15$

Aufgabe 2 (3 Punkte):

(a) Gibt es ein Polynom $f \in \mathbb{Z}[X_1, \ldots, X_n]$, so dass $f = 0$ eine Lösung modulo q hat genau dann, wenn $q < 10$ ist?

(b) Gibt es ein Polynom $f \in \mathbb{Z}[X_1, \ldots, X_n]$, so dass $f = 0$ eine Lösung modulo q hat genau dann, wenn q keine Primzahl ist?

(c) Gibt es ein Polynom $f \in \mathbb{Z}[X_1, \ldots, X_n]$, so dass $f = 0$ eine Lösung modulo q hat genau dann, wenn $q = 1$, 2, 3, 4, 6 oder 12 ist?

Geben Sie jeweils entweder so ein Polynom an oder begründen Sie, warum es keins gibt.

Aufgabe 3 (3 Punkte):

Bestimmen Sie für jede der folgenden Gleichungen, ob es keine, eine oder mehrere Lösungen modulo 3^{100} gibt. Begründen Sie Ihre Antwort.

(a) $X^4 = X - 4$

(b) $X^2(X + 3) = 13$

(c) $X^3 + Y^3 = Z^2 + 1$

Aufgabe 4 (6 Punkte):

Für natürliche Zahlen q soll die Äquivalenz der folgenden Aussagen gezeigt werden:

(i) q ist durch 9 oder durch eine Primzahl der Form $3k + 1$ teilbar.

(ii) $\phi(q)$ ist durch 3 teilbar.

(iii) Die Gleichung $X^3 = 1$ besitzt mehrere Lösungen in $\mathbb{Z}/q\mathbb{Z}$.

(iv) Es gibt zu q teilerfremde Zahlen a, so dass die Gleichung $X^3 \equiv a \mod q$ keine Lösung besitzt.

Eine mögliche Vorgehensweise:

(a) Zeigen Sie (i) $\iff$ (ii).

(b) Zeigen Sie (iii) $\iff$ (iv), indem Sie zeigen, dass $b \mapsto b^3$ einen Gruppenhomomorphismus $(\mathbb{Z}/q\mathbb{Z})^\times \to (\mathbb{Z}/q\mathbb{Z})^\times$ definiert.

(c) Zeigen Sie (ii) $\iff$ (iii) unter Verwendung des folgenden Satzes (den Sie nicht beweisen müssen): Ist p eine Primzahl, so besitzt eine Gruppe G Elemente der Ordnung p genau dann, wenn $p \mid \#G$.

Zur Erinnerung: Die *Ordnung* eines Gruppenelements $a \in G$ ist die kleinste natürliche Zahl n, so dass $a^n = 1$ ist (wobei 1 das neutrale Element der Gruppe bezeichnet).