ELEMENTARE ZAHLENTHEORIE
6. Übungsblatt

Julia Sauter, Andrew Hubery

Aufgabe 1.

(a) Bestimmen Sie alle Lösungen x modulo 225 des folgenden Kongruenzensystems:

$$10x \equiv 15 \pmod{25} \qquad \text{und} \qquad 3x \equiv 6 \pmod{9}.$$

(b) Bestimmen Sie alle Lösungen x modulo 459 des folgenden Kongruenzensystems:

$$5x \equiv 4 \pmod{27} \qquad \text{und} \qquad 12x \equiv 9 \pmod{51}.$$

(je 2 Punkte)

Aufgabe 2.

(a) Eine Zahl $n \in \mathbb{Z}$ heißt quadratfrei, falls $p^2 \nmid n$ für alle Primzahlen p.

(i) Sei $k \geq 1$. Zeigen Sie, dass es eine Folge $x, x+1, \ldots, x+k-1$ von k aufeinanderfolgenden nicht quadratfreien ganze Zahlen gibt.

Hinweis: Seien $p_1, \ldots, p_k$ paarweise verschiedene Primzahlen und betrachten Sie ein passendes System von Kongruenzen modulo p_i^2.

(ii) Geben Sie ein Beispiel für $k = 3$.

(b) Sei p eine Primzahl und $x \in \mathbb{Z}$ mit $\mathrm{ggT}(x, p) = 1$. Der kleine Satz von Fermat sagt, dass $x^{p-1} \equiv 1 \pmod{p}$. Es folgt, dass $x = 1 + ps$ für eine $s \in \mathbb{Z}$.

(i) Zeigen Sie nun, dass $x^{p(p-1)} \equiv 1 \pmod{p^2}$. Es folgt, dass $x^{p(p-1)} = 1 + p^2 t$ für eine $t \in \mathbb{Z}$.

(ii) Ziegen Sie per Induktion, dass $x^{p^k(p-1)} \equiv 1 \pmod{p^{k+1}}$ für alle $k \geq 1$.

(2+1+1+2 Punkte)

Aufgabe 3.

Sei R ein (kommutativer) Ring. Ein Element $x \in R$ heißt nilpotent, falls $x^n = 0$ für eine $n \in \mathbb{N}$.

(a) Zeigen Sie, dass $N \coloneqq \{x \in R \mid x \text{ nilpotent}\}$ eine Ideal in R ist. Man nennt N das Nilradikal von R, geschrieben $\mathrm{nil}(R)$.

Hinweis. Falls $x^m = 0 = y^n$ betrachten Sie $(x+y)^{m+n}$.

(b) Was ist das Nilradikal von $\mathbb{Z}/n\mathbb{Z}$?

(2+1 Punkte)

Abgabe: Montag 27. Mai, bis 12 Uhr in die Postfächer der Tutoren im V3–126

Aufgabe 4.

(a) Sei R ein (kommutativer) Ring, und $I \subseteq J$ zwei Ideale in R. Zeigen Sie, dass es ein Ringhomomorphismus

$$\pi\colon R/I \to R/J, \quad r + I \mapsto r + J,$$

gibt. Beweisen Sie weiterhin, dass π surjectiv ist mit Kern $J/I = \{x + I \mid x \in J\}$.

(b) Sei $n \in \mathbb{Z}$ und $J = (n, X)$ die von n und X erzeugten Ideal in $\mathbb{Z}[X]$. (Also J enthält genau die Elemente $f \in \mathbb{Z}[X]$, die als $f = ng + Xh$ mit $g, h \in \mathbb{Z}[X]$ geschrieben sein können.)

Zeigen Sie, dass $\mathbb{Z}[X]/J \cong \mathbb{Z}/n\mathbb{Z}$.

Hinweis: Man könnte zuerst das Ideal $I = (X)$ betrachten und (a) verwenden.

(c) Sei K eine Körper und $K[X_1, \ldots, X_n]$ das Polynomring mit n Variabeln.

(i) Sei $a = (a_1, \ldots, a_n) \in K^n$. Zeigen Sie, dass es ein surjektiven Ringhomomorphismus $\mathrm{ev}_a\colon K[X_1, \ldots, X_n] \to K$, $X_i \mapsto a_i$, gibt. Man schreibt auch $f(a)$ statt $\mathrm{ev}_a(f)$, und nennt a eine Nullstelle von f falls $f(a) = 0$.

(ii) Sei nun $U \subseteq K^n$ eine Teilmenge. Wir definieren

$$I(U) \coloneqq \{f \in K[X_1, \ldots, X_n] \mid f(a) = 0 \text{ für alle } a \in U\}.$$

Zeigen Sie, dass $I(U)$ ein Ideal in $K[X_1, \ldots, X_n]$ ist, und dass $I(U \cup U') = I(U) \cap I(U')$ gilt.

(2+2+1+2 Punkte)