UNIVERSITÄT DES SAARLANDES
Fachrichtung 6.1 - Mathematik
Christian Bopp

Übungen zur Elementaren Zahlentheorie

Sommersemester 2018

Die Lösungen des Übungsblattes sind bis spätestens 14.00 Uhr, am 11.07.2018, in die Briefkästen vor dem Zeichensaal in Geb. E2 5, einzuwerfen.
Alle Übungsblätter und Informationen zur Vorlesung werden auf der Seite unserer Arbeitsgruppe unter *Teaching* zu finden sein: www.math.uni-sb.de/ag-schreyer/

Blatt 13 — 04.07.2018

Aufgabe 1. Bestimmen Sie die Anzahl der $x \in \mathbb{Z}$ mit $0 \leq x \leq 209$, welche die folgende Gleichung erfüllen.

$$7x^3 + 5x^2 + 3x \equiv 0 \mod 210$$

(Hinweis: Verwenden Sie den chinesischen Restsatz.)

Aufgabe 2. Sei $m = p \cdot q$ das Produkt aus zwei unterschiedlichen Primzahlen. Zeigen Sie, dass keine Primitivwurzel modulo m existiert.

Aufgabe 3. Finden Sie alle Lösungen $x \in \mathbb{Z}$ der folgenden Gleichungen

(a) $5x^5 \equiv 7 \mod 13$
(b) $5x^6 \equiv 2 \mod 13$
(c) $2^x \equiv 7 \mod 13$
(d) $7^x \equiv 2 \mod 13$

(Hinweis: Überlegen Sie sich, welche Zahlen Primitivwurzeln modulo 13 sind.)

Aufgabe 4. Zeigen Sie, dass falls n eine Pseudoprimzahl zur Basis $b = 2$ ist, so ist auch $2^n - 1$ eine Pseudoprimzahl zur Basis 2. Folgern Sie, dass es unendlich viele Pseudoprimzahlen zur Basis $b = 2$ gibt.

Bitte wenden.

Bonusaufgabe 1. Sei K ein Körper und seien $0 \neq f(x), g(x) \in K[x]$. Sei ferner

$$d(x) = \mathrm{ggT}(f(x), g(x)).$$

(Für die Definition des größten gemeinsamen Teilers zweier Polynome siehe Blatt 12.)

(a) Zeigen Sie, dass Polynome $s(x), t(x) \in K[x]$ existieren mit

$$d(x) = s(x)f(x) + t(x)g(x).$$

(b) Seien $s(x), t(x) \in K[x]$. Zeigen Sie, dass das Polynom $s(x)f(x)+t(x)g(x)$ durch $d(x)$ teilbar ist

(c) Berechnen Sie den größten gemeinsamen Teiler der beiden Polynome $f(x) = x^2 + \frac{1}{2}x + \frac{1}{2} \in \mathbb{Q}[x]$ und $g(x) = 2x - 1 \in \mathbb{Q}[x]$. Berechnen Sie auch die Darstellung des größten gemeinsamen Teilers aus Aufgabenteil (a).

Bonusaufgabe 2. Sei K ein Körper. Ein Polynom $f(x) \in K[x]$ heißt *reduzibel*, falls ein Polynom $g(x) \in K[x]$ existiert mit $1 < \mathrm{Grad}(g(x)) < \mathrm{Grad}(f(x))$ und $g(x) \big| f(x)$. Andernfalls heißt $f(x)$ *irreduzibel*. Irreduziblität hängt von der Wahl des Grundkörpers ab, so ist z.B. $x^2 - 2 \in \mathbb{R}[x]$ reduzibel aber $x^2 - 2 \in \mathbb{Q}[x]$ irreduzibel.

(a) Zeigen Sie, dass jedes Polynom $f(x) \in K[x]$ mit $\mathrm{Grad}(f(x)) = 1$ irreduzibel ist.

(b) Zeigen Sie, dass ein Polynom $f(x) \in K[x]$ vom Grad 2 oder 3 genau dann irreduzibel ist, wenn $f(x)$ keine Nullstelle in K hat.

(c) Sei $K = \mathbb{Z}/5\mathbb{Z}$. Ist das Polynom $f(x) = x^4 + 1 \in K[x]$ irreduzibel?

Bonusaufgabe 3. Seien $f(x), g(x), h(x) \in K[x]$ Polynome mit $f(x) \neq 0$. Man sagt, dass $g(x)$ *kongruent* zu $h(x)$ modulo $f(x)$ ist, falls $f(x) \big| (g(x) - h(x))$. Wir schreiben hierfür

$$g(x) \equiv h(x) \mod f(x).$$

Analog zu den ganzen Zahlen definiert die Kongruenz modulo einem festen Polynom $f(x) \in K[x]$ eine Äquivalenzrelation auf dem Ring $K[x]$. Die Menge der Äquivalenzklassen bezüglich dieser Äquivalenzrelation bezeichnen wir mit $K[x]/\langle f(x)\rangle$.

Seien nun $f(x), g(x) \in K[x]$ Polynome mit $f(x) \neq 0$.

(a) Zeigen Sie, dass ein eindeutiges Polynom $h(x) \in K[x]$ existiert mit

$$\mathrm{Grad}(h(x)) < \mathrm{Grad}(f(x)) \text{ und } g(x) \equiv h(x) \mod f(x).$$

(b) Sei K ein endlicher Körper mit q Elementen und sei $f(x) \in K[x]$ ein Polynom vom Grad $n \geq 1$. Zeigen Sie, dass $K[x]/\langle f(x)\rangle$ genau q^n viele Elemente hat.

(c) Bestimmen Sie ein Repräsentantensystem der Elemente in $K[x]/\langle x^2 + x - 1\rangle$ für $K = \mathbb{Z}/3\mathbb{Z}$.

Bonusaufgabe 4. Sei K ein Körper und $f(x) \in K[x]$ ein Polynom vom Grad $n \geq 1$. Analog zu der Konstruktion des Ringes $\mathbb{Z}/m\mathbb{Z}$ können wir auch auf der Menge $K[x]/\langle f(x)\rangle$ repräsentantenweise eine wohldefinierte Addition und Multiplikation definieren. Die Menge $K[x]/\langle f(x)\rangle$ wird so zu einem kommutativen Ring mit Einselement.
Für ein Polynom $g(x) \in K[x]$ bezeichnen wir mit $[g(x)]$ die Äquivalenzklasse von $g(x)$ in $K[x]/\langle f(x)\rangle$. Falls ein Polynom $h(x) \in K[x]$ existiert mit $g(x) \cdot h(x) \equiv 1 \mod f(x)$, so definiert die Klasse $[h(x)]$ ein multiplikatives Inverses zu $[g(x)] \in K[x]/\langle f(x)\rangle$.

Zeigen Sie, dass $[g(x)] \in K[x]/\langle f(x)\rangle$ genau dann ein multiplikatives Inverses in dem Ring $K[x]/\langle f(x)\rangle$ hat, wenn $\mathrm{ggT}(g(x), f(x)) = 1$ ist. Insbesondere ist $K[x]/\langle f(x)\rangle$ genau dann ein Körper, wenn $f(x) \in K[x]$ irreduzibel ist.