Technische Universität München
Institut für Informatik
Lehrstuhl für Effiziente Algorithmen
Prof. Dr. Angelika Steger

WS 1999/2000
Übungsblatt 12
10. Februar 2000

Diskrete Strukturen I

Abgabetermin Computeraufgaben: Freitag, 18. Februar 2000
Hausaufgaben: Mittwoch, 23. Februar 2000

Tutoraufgabe 1

Beweisen Sie ausführlich folgenden Satz (4.87) aus der Vorlesung:

Satz 0.1. *Für jeden Körper K und jedes Polynom $\pi(x) \in K[x]$ bildet $K[x]/\pi(x)$ bezüglich der Addition $[f(x)]_\pi + [g(x)]_\pi = [f(x) + g(x)]_\pi$ und der Multiplikation $[f(x)]_\pi \cdot [g(x)]_\pi = [f(x) \cdot g(x)]_\pi$ einen Ring.*

Überzeugen Sie sich insbesondere, dass die Definitionen der Addition und der Multiplikation in $K[x]/\pi(x)$ korrekt sind.

Tutoraufgabe 2

Decodieren Sie die mit RSA verschlüsselte Nachricht

$$47651,\ 44631,\ 232711,\ 26471,\ 154791,$$

wenn der öffentliche Schlüssel $(e, n) = (34679, 295927)$ war.

Hausaufgabe 1 (10 Punkte)

Sei $p \geq 3$ eine Primzahl. Beweisen Sie, dass für jedes $a \in \mathbb{Z}_p^*$ gilt

$$x^2 \equiv a \bmod p \text{ besitzt eine Lösung } x \iff a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

Hausaufgabe 2 (10 Punkte)

Zeigen Sei, dass $15x^2 - 7y^2 = 9$ keine ganzzahligen Lösungen $(x, y) \in \mathbb{Z}^2$ besitzt.

Computeraufgabe 1 (10 Punkte)

Sei $R = \mathbb{Z}_{7919}[x]/(2x^2 + 5x - 3)$. Ein Element $a \in R$, $a \neq 0$, zu dem ein von Null verschiedenes Element $b \in R$ existiert, sodass $a \cdot b = 0$, heißt *Nullteiler*. Wieviele verschiedene Nullteiler gibt es in R?

Computeraufgabe 2 (10 Punkte)

Finden Sie ein $x \in \mathbb{Z}_{6469693230}$, sodass

$$95041567x \equiv 31 \bmod 6469693230.$$