**Aufgabe 5.1** (3 Pkt.)

a) Geben Sie die Multiplikationstabelle für $\mathbb{Z}_{15}^*$ an!

b) Geben Sie eine Tabelle an, in der man zu jedem $x \in \mathbb{Z}_{15}^*$ das Inverse $x^{-1}$ ablesen kann.

c) Listen Sie zu jeder Zahl $z \in \mathbb{Z}_{15}$ alle Quadratwurzeln von $z$ auf!

**Aufgabe 5.2** (2 Pkt.)

a) Bestimmen Sie die Lösungen $x \in \mathbb{Z}_{53}$ der Gleichung $x^{191} \equiv 4 \pmod{53}$.

b) Berechnen Sie die letzten beiden Dezimalziffern von $17^{162}$.

**Aufgabe 5.3** (2 Pkt.)

Das Problem Jein-SAT ist wie folgt definiert:

*Gegeben:* Eine boolesche Formel $F$.
*Gefragt:* Gibt es für $F$ mindestens eine erfüllende und eine nicht erfüllende Belegung?

Zeigen Sie: Jein-SAT ist NP-vollständig.

**Aufgabe 5.4** (1+3 Pkt.)

Die Fehlerwahrscheinlichkeit $p$ eines probabilistischen Algorithmus $A$ kann durch mehrmaliges Ausführen von $A$ reduziert werden. Wenn jede Ausführung von $A$ ein Ergebnis aus $\{0,1\}$ liefert, erhält man bei $t$-maliger Ausführung von $A$ einen Ergebnisvektor $v \in \{0,1\}^t$. Durch Anwendung einer geeigneten Funktion $f\colon \{0,1\}^t \to \{0,1\}$ bestimmt man daraus ein Gesamtergebnis $f(v)$, das mit deutlich geringerer Wahrscheinlichkeit $\varepsilon \ll p$ vom richtigen Ergebnis abweichen soll.

a) Für welches $f$ erhält man bei einem RP-Algorithmus $\varepsilon \leq p^t$? Begründen Sie Ihre Antwort!

b) Zeigen Sie: Bei einem BPP-Algorithmus erreicht man $\varepsilon \leq \delta^t$ (für ein $\delta < 1$) mit der Funktion

$$f(v) \coloneqq \begin{cases} 1 & \text{falls mehr als die Hälfte der Bits in } v \text{ Wert 1 haben} \\ 0 & \text{sonst.} \end{cases}$$

Wie hängt $\delta$ von $p$ ab? *Tipp:* Beweisen Sie zunächst

$$\varepsilon \leq (1-p)^{t/2} p^{t/2} \sum_{i=0}^{\lfloor t/2 \rfloor} \binom{t}{i}.$$

**Aufgabe 5.5** (2 Pkt.)

Beim Wurf einer gezinkten Münze erhält man „Kopf“ mit Wahrscheinlichkeit $p$ und „Zahl“ mit Wahrscheinlichkeit $(1-p)$. Beweisen Sie: Im Mittel muss $(1/p)$-mal geworfen werden, bis zum ersten Mal „Kopf“ erscheint.

**Aufgabe 5.6** (3 Pkt.)

Die Komplexitätsklasse RP ist die Menge aller Entscheidungsprobleme $L$, für die ein deterministischer Algorithmus $A$ mit folgenden Eigenschaften existiert:

- $A$ bekommt außer der Eingabe $x$ einen zufälligen Wert $z$ übergeben, der unter Gleichverteilung aus einer Menge $M$ gezogen wird.
- Dabei ist $\log_2 |M|$ höchstens polynomiell in der Länge der Eingabe $x$.
- Für alle Eingaben $x$ ist $\Pr[A(x, z) = 1] > \frac{1}{2}$ falls $x \in L$, und $\Pr[A(x, z) = 1] = 0$ falls $x \notin L$.
- Die Worst-Case-Laufzeit von $A$ ist polynomiell in der Länge der Eingabe $x$.

Die Klasse co-RP enthält alle Entscheidungsprobleme $L$, deren Komplement $\overline{L}$ in RP liegt.

Die Komplexitätsklasse ZPP (*zero-error probabilisitic polynomial time*) sei die Menge der Entscheidungsprobleme, für die es stochastische Algorithmen $B$ gibt mit folgenden Eigenschaften:

- $B$ liefert niemals eine falsche Antwort.
- Der Erwartungswert der Laufzeit von $B$ ist polynomiell in der Länge der Eingabe.

Beweisen Sie: $\mathsf{ZPP} = \mathsf{RP} \cap \text{co-}\mathsf{RP}$.