Martin Ziegler

Ausgabe am 19.1.2011
Abzugeben am 26.1.2011 11h40

Komplexitätstheorie

WS 2010/2011, Aufgabenzettel #11

AUFGABE 28:

a) Sei $n \in \mathbb{N}$. Weisen Sie nach, dass die Menge $\mathbb{Z}_n := \{0,1,\ldots,n-1\}$ einen kommutativen Ring bildet bezüglich der Operationen $x \oplus y := (x+y)$ rem n und $x \otimes y := (x \cdot y)$ rem n. Zeigen Sie: $(x \text{ rem } n)+(y \text{ rem } n) = (x+y)$ rem n und $(x \text{ rem } n) \cdot (y \text{ rem } n) = (x \cdot y)$ rem n für alle $x, y \in \mathbb{Z}$.

b) i) Jedes $x \in \mathbb{Z}_n$ teilerfremd zu n besitzt ein multiplikatives Inverses $x^{-1} \in \mathbb{Z}_n$.
ii) Ist p sogar Primzahl, so gilt der Kleine Satz von Fermat: Für jedes $x \in \mathbb{Z}_p$ is $x^p = x$.
iii) Sind p, q teilerfremd und $a, b \in \mathbb{Z}$ mit $a \equiv b \bmod p$ und $a \equiv b \bmod q$, so $a \equiv b \bmod pq$.

Tipp: Zu teilerfremden $a, b \in \mathbb{Z}$ liefert der erweiterte Euklidische Algorithmus $r, s \in \mathbb{Z}$ mit $ra + sb = 1$. Weiterhin dürfen Sie den Satz von Lagrange verwenden.

c) Seien p, q verschiedene Primzahlen, $n := p \cdot q$ und $\varphi := (p-1) \cdot (q-1)$. Weiter sei $1 \neq e \in \mathbb{Z}_\varphi$ teilerfremd zu φ und $d := e^{-1}$ rem φ gemäß b). Zeigen Sie, dass die Funktionen

$$E(\tilde{e}) : \mathbb{Z}_n \setminus \{0\} \ni x \mapsto x^e \text{ rem } n \in \mathbb{Z}_n \quad \text{und} \quad D(\tilde{d}) : \mathbb{Z}_n \setminus \{0\} \ni y \mapsto y^d \text{ rem } n \in \mathbb{Z}_n$$

polynomialzeitberechenbar sind und $D\big(\tilde{d}, E(\tilde{e}, x)\big) = x$ sowie $E\big(\tilde{e}, D(\tilde{d}, y)\big) = y$ erfüllen, wobei $\tilde{e} := \langle e, n \rangle$ und $\tilde{d} := \langle d, n \rangle$.

d) Das *public-key* System aus c) heißt RSA nach seinen Erfindern RIVEST, SHAMIR und ADLEMAN. Dabei dient $\tilde{e}$ als öffentlicher Schlüssel und $\tilde{d}$ als privater. Wie sind damit die Operationen Verschlüsseln und Signieren zu realisieren? Nehmen Sie an, Faktorisieren ganzer Zahlen gelänge in polynomieller Zeit. In wiefern würde RSA dadurch kompromittiert?

AUFGABE 29:

a) Sei $\vec{x} \in \{0,1\}^n$ fest und $\vec{y}$ ein zufälliger Binärstring der Länge n. Dann ist die Wahrscheinlichkeit, dass $\vec{x}$ und $\vec{y}$ sich an genau j Positionen unterscheiden, gegeben durch $\binom{n}{j} \cdot 2^{-n}$.

b) Sei X ein 0/1-Zufallsexperiment (d.h. eine Bernoulli-Zufallsvariable), das mit (potentiell sehr kleiner) Wahrscheinlichkeit $p > 0$ gelingt. Zeigen Sie: Bei $\frac{20}{p}$-facher Wiederholung gelingt mindestens eines der durchgeführten Experimente mit (nahezu sicherer) Wahrscheinlichkeit $\geq 1 - e^{-20}$.

c) Sei X wieder eine Bernoulli-Zufallsvariable mit Erfolgswahrscheinlichkeit p. Berechnen Sie die Wahrscheinlichkeit, dass bei n-maliger Wiederholung mehr als die Hälfte der Versuche gelingt. Bestimmen Sie den Erwartungswert μ und die Varianz σ^2 der Zufallsvariablen $Y := \sum_{j=1}^{n} X_j$, die die Anzahl erfolgreicher Versuche beschreibt.

d) Sei X wieder eine Bernoulli-Zufallsvariable mit $p \geq 1/2 + \varepsilon$ und $n := 40/\varepsilon^2$. Zeigen Sie, dass bei n-facher Wiederholung von X nahezu sicher mehr als die Hälfte der Versuche gelingt; und dass im Fall $p \leq 1/2 - \varepsilon$ fast sicher weniger als die Hälfte der Versuche gelingt. Tipp: Chernoff-Ungleichung nachschlagen und anwenden. Was liefert die Tschebyscheff-Ungleichung?