DISKRETE MATHEMATIK

Prof. Dr. Thomas Ihringer

Aufgabenblatt Nr. 9

121. Entschlüssele folgenden Merksatz:

CSMROBROSD VSOQD KVVOSX SW CMRVEOCCOV.

122. Welche der folgenden Funktionenfamilien bilden ein Kryptosystem auf $M=\{a,b,c\}$, $C=\{1,2,3,4\}$?

x	a	b	c
$f_1(x)$	1	2	4
$f_2(x)$	2	2	3
$f_3(x)$	3	1	2

x	a	b	c
$f_1(x)$	1	2	4
$f_2(x)$	1	2	3
$f_3(x)$	3	1	2

x	a	b	c
$f_1(x)$	1	2	4
$f_2(x)$	c	2	3
$f_3(x)$	3	1	2

123. Wie in 5.5 im Buch werde ein affines Kryptosystem mit $N=26$ und den üblichen Alphabet verwendet:

a) Berechne 5^{-1} in $\mathbb{Z}_{26}$. b) Berechne die Inverse von $f_{5,10}(x)=5x+10$.

124. Mit obiger Verschlüsselungsfunktion $f_{5,10}$ hat sich das Kryptogramm ICRREIB ergeben. Finde den Klartext.

---

125. a) Führe für die Zahlen 13 und 33 den euklidischen Algorithmus durch.

b) Finde/berechne ganze Zahlen k und L mit $1=k\cdot 13+L\cdot 33$.

126. Bestimme 13^{-1} im Ring $\mathbb{Z}_{33}$.

127. Beweise: a) Für je zwei verschiedene Primzahlen p,q gilt $\varphi(pq)=(p-1)(q-1)$.

b) Für jede Primzahlpotenz p^α mit $\alpha\geq 1$ gilt $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$.

128. Wie lauten die letzten beiden Ziffern der ausgerechneten Zahlen 7^{99} bzw. 9^{99}?

---

129. Zeige mit einem Gegenbeispiel, daß 7.1 im Buch ohne die Voraussetzung „n quadratfrei" falsch wird.

130. Bestimme die Zahlen p,q und $\varphi(n)$ die der Benutzer des RSA-Kryptosystems mit öffentlichem Schlüssel $(n,e)=(779,103)$ benutzt hat.

131. Derselbe Teilnehmer möchte sich mit seiner Chipkarte ausweisen (Authentikation), wobei wieder das Kryptosystem aus 130 verwendet wird. Der Kontrollrechner bietet die Zahl $y=152$ an. Welche Zahl x sollte die Chipkarte zurückgeben?

132. Es wird das RSA-kryptosystem mit dem öffentlichen Schlüssel $(n,e)=(33,13)$ verwendet. Berechne die zugehörige Zahl d.

H133. Für das folgende Kryptogramm wurde eine Vigenère-Chiffre verwendet. Das Schlüsselwort besteht übrigens aus den Initialen einer im Abschnitt „Sicherung gegen unbefugten Zugriff" genannten Person:

ROCTJWAKPGWOXPJVWQEGVDNTFCAUMKNVJINYDTMGW
VAWNDNTMGAYRPMTRUBXXPMGWDJGDONPMCBNJWKEJ
TNKBVREQPJEQFNWCULJUCWFQKWWNDNT

H134. Berechne mit dem square-and-multiply-Verfahren 13^{31} (33).

*H135. Es soll Aufgabe 132 fortgesetzt werden: Entziffere den Schlüsseltext

ABAAALBBBABFBDARBFAT

(26-elementiges Alphabet, k=1, L=2, vgl. mit 7.2 im Buch).

Umseitig: Miniprojekt Nr. 3

MINIPROJEKT NR. 3 (Thema: Primzahltests). Die Darstellung sollte vollständiger sein als die Andeutungen im Buch. Sie kann z.B. die Punkte (1)–(3) behandeln. Punkt (4) ist schwieriger.

(1) Wofür sind Primzahltests wichtig?

(2) Beweise, daß $U := \{x \in \mathbb{Z}_n \mid x^{n-1} = 1 (n)\}$ eine Untergruppe von $(\mathbb{Z}_n^*; \cdot)$ ist. Wie groß ist der Quotient $|\mathbb{Z}_n^*|/|U|$ höchstens, falls $U \neq \mathbb{Z}_n^*$ gilt, d.h. falls n weder eine Primzahl noch eine Carmichael-Zahl ist?

(3) Was folgt hieraus für die Wahrscheinlichkeit, daß $x^{n-1} = 1 (n)$ von einem zufällig ausgewählten $x \in \mathbb{Z}_n$ erfüllt wird? Wie effektiv ist ein Primzahltest, bei dem $x^{n-1} = 1 (n)$ für k zufällig ausgewählte Zahlen $x_1, \ldots, x_k$ getestet wird, d.h. mit welcher Wahrscheinlichkeit wird entdeckt, wenn n keine Primzahl ist?

(4) Diskutiere in ähnlicher Weise einen Primzahltest für n, der auf der Gleichung

$$x^{\frac{n-1}{2}} = \left(\frac{x}{n}\right) \quad (n)$$

beruht. Hierbei ist $\left(\frac{x}{n}\right)$ das sog. Jacobi-Symbol.
Anmerkung. Mit diesem Test kann jede Nichtprimzahl mit hoher Wahrscheinlichkeit „entlarvt" werden. Ausnahmen wie die Carmichael-Zahlen gibt es hierbei nicht.

Im Semesterapparat findet man das Buch „A course in number theory and cryptography" von N. Koblitz, in dem man sich über Primzahltests (und die Definition des Jacobi-Symbols) informieren kann. Außerdem steht im Semesterapparat das Buch „Kryptologie" von A. Beutelspacher.