6. Übung zur Diskreten Mathematik

Aufgaben für den 12.11.2013

31. Verwenden Sie fogende Codierung der Buchstaben:

a	b	c	d	e	f	g	h	i	j	k	l	m	n
00	01	02	03	04	05	06	07	08	09	10	11	12	13
o	p	q	r	s	t	u	v	w	x	y	z		
14	15	16	17	18	19	20	21	22	23	24	25		

Ihre Daten bei RSA sind $p = 17$, $q = 59$, $e = 3$. Berechnen Sie Ihr m, $\varphi(m)$, und die Koeffizienten $x > 0, y$ der Bezout'schen Identität $xe + y\varphi(m) = 1$. Wir verwenden stets Blöcke β_i der Länge 3. Als Füllzeichen am Ende wird 'x' eingesetzt.

Beantworten Sie die Frage, die Sie verschlüsselt in den Blöcken

$$811 \quad 517 \quad 005 \quad 732 \quad 313 \quad 975 \quad 854 \quad 249$$

erhalten, und schreiben Sie die Antwort verschlüsselt für den Benutzer mit $m' = 703$ und $e' = 7$.

Hinweis: Verwenden Sie den erweiterten Euklidischen Algorithmus zur Bestimmung von x, achten Sie darauf, ein $x > 0$ zu finden, und potenzieren Sie wie in der Vorlesung besprochen.

32. Der alte ISBN-Code ist eine Folge $x_1 \dots x_{10}$ von zehn Elementen x_i aus der Menge $\{0, 1, \dots, 9, X\}$. Diese Folge besteht aus aufeinanderfolgenden Teilfolgen, die durch Bindestriche voneinander getrennt sind und wechselnde Längen haben können.

   (a) Die erste Teilfolge $x_1 \dots$ (meist von der Länge 1) codiert den Sprachraum, in dem das Buch gedruckt wurde (nicht notwendig die Sprache, in dem es geschrieben ist!). 0 steht beispielsweise für den englischsprachigen, 3 für den deutschsprachigen Raum.

   (b) Die nächste Teilfolge codiert den Verlag, es sind mindestens zwei Einträge.

   (c) Die Folge der nächsten Koordinaten $\dots x_9$ ist eine Buchnummer, die vom Verlag festgesetzt wird. Dabei werden $x_1, \dots, x_9$ aus der Menge $\{0, 1, \dots, 9\}$ gewählt.

   (d) Die letzte Stelle x_{10} wird so bestimmt, dass $x_{10} \equiv \sum_{i=1}^{9} i \cdot x_i \bmod 11$ ist. Falls $x_{10} = 10$, setzt man $x_{10} := X$.

   Zeigen Sie, dass dieser Code (i) ein falsch gelesenes Zeichen, (ii) eine Vertauschung zweier benachbarter Stellen $x_i \neq x_{i+1}$, $1 \leq i < 10$, erkennen kann, und (iii) dass man eine undeutlich geschriebene Ziffer rekonstruieren kann. (iv) Berechnen Sie die Prüfziffer von 3-540-64502-?. (v) Wie heißt die vollständige ISBN-Nummer von 3-446-?9313-8?

33. Sei $m \in \mathbb{Z}_{>35}$. Zeigen Sie, dass die Restklasse $\overline{33} \in \mathbb{Z}_m$ abzählbar ist.

34. Lösen Sie die simultane Kongruenz:

$$\begin{aligned} x &\equiv 2 \bmod 753 \\ x &\equiv 7 \bmod 221. \end{aligned}$$

35. Seien X und Y endliche Mengen. Beweisen Sie mit Induktion über $|X|$ und unter Verwendung von Satz 7.5 aus der Vorlesung, dass Y^X endlich ist und die Mächtigkeit $|Y|^{|X|}$ besitzt.

    Hinweis: Bei dem Induktionsschluss drücken Sie Y^X als kartesisches Produkt zweier geeigneter Mengen aus. Beweisen Sie exakt, dass dies eine bijektive Beziehung zwischen Y^X und dem kartesischen Produkt ist.

Zusatzaufgaben:

1. Zeigen Sie, dass die simultane Kongruenz

$$\begin{aligned} x &\equiv a \bmod m \\ x &\equiv b \bmod n \end{aligned}$$

   genau dann lösbar ist, wenn $a \equiv b \bmod \mathrm{ggT}(n, m)$.

2. Seien A, B Mengen. Eine Funktion $f\colon A \to B$ ist dann und nur dann injektiv, wenn es eine Funktion $g\colon B \to A$ gibt, so dass $g \circ f = \mathrm{id}_A$. ($g$ heißt ein Linksinverses zu f.)

3. Seien $A \subseteq \mathbb{N}$ und B Mengen. Eine Funktion $f\colon A \to B$ ist dann und nur dann surjektiv, wenn es eine Funktion $g\colon B \to A$ gibt, so dass $f \circ g = \mathrm{id}_B$. ($g$ heißt ein Rechtsinverses zu f.) Warum haben wir hier $A \subseteq \mathbb{N}$ vorausgesetzt?