Prof. Dr. M. Lesch
P. Holy

Abgabe bis 07.01., vor 09:15 morgens
oder wie mit Ihren Tutoren vereinbart

Übungen zur Vorlesung Elemente der Mathematik

ÜBUNGSBLATT 9

Aufgabe 1: (3 Punkte) Simulieren Sie eine Chiffrierung und Dechiffrierung mit dem RSA-Verfahren. Der Empfänger E wählt die (nicht besonders) großen Primzahlen $p = 11$ und $q = 13$, damit ist also $n = p \cdot q = 143$. Wählen Sie ein $d > 1$ mit $(d, \phi(n)) = 1$ und berechnen Sie ein e mit $d \cdot e \equiv 1\ (\phi(n))$. Wenden Sie das Chiffrierverfahren mit den gewählten Parametern auf die Zahl $x = 10$ an, Geben Sie das Ergebnis der Chiffrierung an und dechiffrieren Sie dies durch eine entsprechende Berechnung wieder.

Wir nennen das Stellenwertsystem zur Basis $b \in \mathbb{N}$ im Folgenden auch das b-*System* und wir notieren eine natürliche Zahl im b-System durch $[r_m, \ldots, r_0]_b$, wobei für $0 \leq i \leq m$ gilt dass $0 \leq r_i < b$.

Aufgabe 2: (6 Punkte)

(a) Sei $[2, 2, 3, 4]_5$ die Darstellung einer natürlichen Zahl im 5er-System. Stellen Sie die Zahl im 3er-System dar.

(b) Sei $[1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1]_2$ die Darstellung einer natürlichen Zahl im 2er-System. Stellen Sie die Zahl im 8er-System dar. Überlegen Sie, warum sich diese Aufgabe mit Hilfe der Tatsache dass $2^3 = 8$ gilt schnell und einfach lösen lässt.

(c) Bestimmen Sie $a \geq 5$ und $b \geq 4$ in $\mathbb{N}$ so dass $[4, 0, 3]_a = [2, 3, 0, 2]_b$ gilt (es genügt eine Lösung für a und b zu finden, Sie müssen nicht *alle* möglichen Lösungen suchen).

(d) Sei eine natürliche Zahl $[1, 0, 1, 2, 2, 0, 1, 3, a, b]_{10}$ gegeben, von der wir die letzten beiden Ziffern a und b nicht kennen. Jedoch wissen wir, dass die Darstellung dieser Zahl im 4er, 5er und 9er-System jeweils mit einer 1 endet. Bestimmen Sie a und b.

Aufgabe 3: (6 Punkte) Ähnlich wie das übliche Zehnersystem, das Hexadezimalsystem zur Basis 16 oder das Binärsystem zur Basis 2 wollen wir in dieser Aufgabe das Faktoriellensystem einführen - zur Erinnerung: ist $n \in \mathbb{N}$, so ist $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$, insbesondere ist $1! = 1$.

Für Zahlen $a_1, \ldots, a_n \in \mathbb{N}$ mit $n \in \mathbb{N}$ sei

$$[a_n, \ldots, a_1]_! := a_n \cdot n! + a_{n-1} \cdot (n-1)! + \ldots + a_2 \cdot 2! + a_1 \cdot 1!.$$

Ist nun $a \in \mathbb{N}$, so sagen wir dass a im !-System darstellbar ist, wenn es $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in \mathbb{N}$ gibt so dass $a_i \leq i$ für alle $i \leq n$ gilt, so dass $a_n \neq 0$ falls $n > 1$ und so dass $a = [a_n, \ldots, a_1]_!$ gilt.

(a) Berechnen Sie:

$$[10, 7, 3, 8, 2, 5, 3, 5, 3, 2, 2, 2, 1]_! + [2, 7, 7, 6, 8, 7, 4, 3, 4, 2, 2, 0]_!$$

und stellen Sie das Ergebnis im !-System dar.

(b) Zeigen Sie für $k \in \mathbb{N}$: $\sum_{i=0}^{k} i \cdot i! < (k+1)!$ mit vollständiger Induktion.

(c) Zeigen Sie: Jede natürliche Zahl ist eindeutig im !-System darstellbar.

(d) Versuchen Sie zu überlegen, welche Vor- und/oder Nachteile das !-System im Gegensatz zu den in der Vorlesung vorgestellten Systemen hat (also den b-Systemen für $b \in \mathbb{N}$).

Aufgabe 4: (6 Punkte) Seien $a, b \in \mathbb{N}$ mit $0 < \frac{a}{b} < 1$. Zeigen Sie:

(a) Wenn wir $n \in \mathbb{N}$ kleinstmöglich wählen so dass $\frac{a}{b} \geq \frac{1}{n}$ und das Ergebnis der Subtraktion $\frac{a}{b} - \frac{1}{n}$ als gekürzten Bruch (mit nichtnegativem Zähler und Nenner) darstellen, so ist der Zähler dieses gekürzten Bruchs kleiner als a.

(b) Zeigen Sie mit Hilfe von (a): Ist $0 \leq \frac{a}{b} \leq 1$, so können wir $\frac{a}{b}$ als (endliche) Summe von jeweils verschiedenen Stammbrüchen schreiben (Ein *Stammbruch* ist ein Bruch der Form $\frac{1}{n}$ für $n \in \mathbb{N}$). Die *leere Summe* soll dabei Wert 0 haben. *Bemerkung:* Ohne der Voraussetzung der Verschiedenheit ist das trivial, denn z.B. ist $\frac{7}{8} = \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}$. Aber es ist etwa auch $\frac{7}{8} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8}$.

(c) Überlegen Sie, wie (c) eine Art Zahlendarstellung für Brüche zwischen 0 und 1 ermöglicht. Stellen Sie $\frac{n}{7}$ für $n = 0, 1, 2, \ldots, 7$ entsprechend dar.

(d) Zeigen Sie, dass diese Darstellung nicht eindeutig ist, finden Sie also einen Bruch $\frac{a}{b}$ zwischen 0 und 1, der auf zwei verschiedene Arten (die sich nicht nur durch die Reihenfolge der Summanden unterscheiden) als Summe von Stammbrüchen geschrieben werden kann.