Gedächnisprotokoll der Klausur vom 2024-02-01 — mit autoge-TEX'en Lösungen!

# ELEMENTARE ZAHLENTHEORIE

*Wie immer:* Keine Garantie auf Richtigkeit. Angaben sollten mehr oder weniger passen. Fehler und Verbesserungen an die FSI-Informatik Melden: `fsi@cs.fau.de`. Der Quelltext sollte im PDF-Anhang sein.

*Allgemeine Informationen:* Die meisten Taschenrechner "Teilen mit Rest" (÷R), Primfaktorzerlegung (`FACT`, auf Casio-Geräten), und ggT (`GCD`) berechnen können, auf wenn nicht programmierbar. Gegebenenfalls ist es notwendig sein eigenes Papier in die Klausur zu nehmen. **Alle Antworten sollten in Form eines Antwortsatzes sein.** Die Klausur dauert 60 Minuten, und sollte in Nürnberg stattfinden.

---

**Aufgabe 1**

Berechnen Sie den größten gemeinsamem Teiler der Zahlen 47753 und 89787 mit Hilfe des Euklidischen Algorithmus.

Die Rechenschritte sind:

- $47753 \div 89787$ ist $0\ R\ 47753$.
- $89787 \div 47753$ ist $1\ R\ 42034$.
- $47753 \div 42034$ ist $1\ R\ 5719$.
- $42034 \div 5719$ ist $7\ R\ 2001$.
- $5719 \div 2001$ ist $2\ R\ 1717$.
- $2001 \div 1717$ ist $1\ R\ 284$.
- $1717 \div 284$ ist $6\ R\ 13$.
- $284 \div 13$ ist $21\ R\ 11$.
- $13 \div 11$ ist $1\ R\ 2$.
- $11 \div 2$ ist $5\ R\ 1$.
- $2 \div 1$ ist $2\ R\ 0$.
- $1 \div 0$ terminiert.

Lösung ist das Letzte $a_i$ wo $b_i = 0$, d.h. $\underline{1}$.

**Aufgabe 2**

Bestimmen Sie den Repräsentanten $1 \leq x < 356$ des Inversen $\overline{47}^{-1} \in \mathbb{Z}/356\mathbb{Z}$.

Man benutzt den Erweiterten Euklidischen Algorithmus (iterativ) auf $(a, b) = (356, 47)$ um die Parameter $x$ und $y$ zu finden, mit denen $xa + yb = \mathrm{ggT}(a, b)$ gilt:

- $r = 47$, $r' = 356$, $s = 0$, $s' = 1$, $t = 1$, $t' = 0$
- $r = 27$, $r' = 47$, $s = 1$, $s' = 0$, $t = -7$, $t' = 1$
- $r = 20$, $r' = 27$, $s = -1$, $s' = 1$, $t = 8$, $t' = -7$
- $r = 7$, $r' = 20$, $s = 2$, $s' = -1$, $t = -15$, $t' = 8$
- $r = 6$, $r' = 7$, $s = -5$, $s' = 2$, $t = 38$, $t' = -15$
- $r = 1$, $r' = 6$, $s = 7$, $s' = -5$, $t = -53$, $t' = 38$
- $r = 0$, $r' = 1$, $s = -47$, $s' = 7$, $t = 356$, $t' = -53$

Wir müssen sicherstellen, dass das Ergebnis im gefordertem Intervall liegt

$$-53 \equiv 303 \mod 356.$$

Die Inverse von $\overline{47}^{-1}$ in $\mathbb{Z}/356\mathbb{Z}$ ist demnach $\underline{\underline{303}}$. Mit dem Taschenrechner kann man überprüfen ob

$$303 \cdot 47 = 14241 \equiv 1 \mod 356.$$

**Aufgabe 3**
Welchen Rest hat $9^{322}$ bei Division durch 11?

Die Aufgabe kann mit dem Euler-Theorem und der Euler'schen $\varphi$-Funktion gelöst werden, oder mit dem "Square and Multiply" Algorithmus,

$$\begin{aligned} c_0 &= 1, \\ c_{n+1} &= \textbf{if } e_n \text{ ungerade } \textbf{then } (c_n b_n) \bmod m \textbf{ else } c_n, \\ e_{n+1} &= \left\lfloor \frac{e_n}{2} \right\rfloor, \\ b_{n+1} &= b_n^2 \bmod m, \end{aligned}$$

wo $e_0 = 322$, $b_0 = 9$ und $m = 11$.

Dieses wird iteriert, bis ein $i$ erreicht wird, wo $e_i = 0$ gilt:

- $c_0 = 1, e_0 = 322, b_0 = 9$
- $c_1 = 1, e_1 = 161, b_1 = 4$
- $c_2 = 4, e_2 = 80, b_2 = 5$
- $c_3 = 4, e_3 = 40, b_3 = 3$
- $c_4 = 4, e_4 = 20, b_4 = 9$
- $c_5 = 4, e_5 = 10, b_5 = 4$
- $c_6 = 4, e_6 = 5, b_6 = 5$
- $c_7 = 9, e_7 = 2, b_7 = 3$
- $c_8 = 9, e_8 = 1, b_8 = 9$
- $c_9 = 4, e_9 = 0, b_9 = 4$

Das Endergebnis ist demnach das $c_i$ der letzten Iteration $\underline{4}$.

**Aufgabe 4**
Bestimmen Sie die Lösungsmenge des Gleichungssystem

$$x \equiv 2 \mod 13 \qquad x \equiv 3 \mod 11 \qquad x \equiv 3 \mod 7.$$

Gegeben sind die Parameter $(a_1, a_2, a_3) = (2, 3, 3)$ und $(m_1, m_2, m_3) = (13, 11, 7)$. Wir müssen zunächst die Zwischenparameter des Chinesischen Restsatzes berechnen:

- $q_1 = \frac{\prod_{i=1}^{3} m_i}{m_1} = 11 \cdot 7 = 77$
- $q_1^{-1} = 12$ bezüglich $\mathbb{Z}/13\mathbb{Z}$
- $q_2 = \frac{\prod_{i=1}^{3} m_i}{m_2} = 13 \cdot 7 = 91$
- $q_2^{-1} = 4$ bezüglich $\mathbb{Z}/11\mathbb{Z}$
- $q_3 = \frac{\prod_{i=1}^{3} m_i}{m_3} = 13 \cdot 11 = 143$
- $q_3^{-1} = 5$ bezüglich $\mathbb{Z}/7\mathbb{Z}$

Es ist zu prüfen ob jedes $(q_i, m_i)$ paarweise Teilerfremd sind (trivial wenn alle $m_i$ Primzahlen sind).

Eine Lösung berechnet sich aus

$$x = \sum_{i=1}^{3} a_i q_i q_i^{-1} = 5085 \equiv 80 \mod 1001$$

und daraus kann man die Lösungsmenge

$$\mathbb{L} = \left\{ x \mid x \equiv \underline{\underline{80}} \mod 1001 \right\}$$

bestimmen.

**Aufgabe 5**
Begründen Sie, warum der Bruch $\frac{1980}{3315}$ eine endliche, reinperiodische oder gemischtperiodische Dezimalbruchentwicklung hat.

Es ist als erstes notwendig den Bruch zu kürzen, indem man

$$\mathrm{ggT}(1980, 3315) = 15$$

berechnet, und damit dann

$$\frac{1980}{3315} = \frac{1980/15}{3315/15} = \frac{132}{221}$$

vereinfachen kann (das kann alles auch der Taschenrechner direkt für einen machen).

Man betrachte den Nenner, und prüft ob dieser dargestellt werden kann durch die spezifische Primzahlendekomposition $221 = 2^i 5^j$, für $i, j \in \mathbb{N}$?

Nein, der Nenner ist darstellbar durch die Primzahlendekomposition. Als nächstes berechnen wir

$$\mathrm{ggT}(221, 10) = 1$$

Da der ggT gleich 1 ist, können wir daraus schließen, der Bruch eine rein-periodische BDE hat.

**Aufgabe 6**
Bestimmen Sie die Darstellung der Zahl 423 zur Basis 5.

Um die Darstellung der Zahl zur Basis 5 zu bestimmen, teilen wir 423 iterativ bis nichts mehr übrig bleibt und merken uns die Restwerte:

- $423 \div 5$ ist $84\ R\ 3$.
- $84 \div 5$ ist $16\ R\ 4$.
- $16 \div 5$ ist $3\ R\ 1$.
- $3 \div 5$ ist $0\ R\ 3$.

In dem man die Reste von unten nach oben durchließt, können wir das Endergebnis $\underline{\underline{3143_{(5)}}}$ bestimmen.