I. Bouw
F. Kiraly

24.04.2008
SS 2008

Übungen zur elementaren Zahlentheorie - Blatt 3

Abgabe im Briefkasten vor H3 spätestens am 08.05.2008 um 10 Uhr

Durch die Verschiebung der Übungen der IST-Studenten auf den Donnerstag Vormittag haben sich die Abgabemodalitäten verändert. Um einen unguten Informationsgradienten zu vermeiden, wurde der Abgabetermin auf Donnerstag früh verlegt (vor die IST-Übungen). Um die dadurch verkürzte Bearbeitungszeit zu kompensieren, erfolgt die Ausgabe des Übungsblattes bereits am Dienstag eine Woche davor in der Vorlesung. Durch die Verlegung ist insgesamt weniger Zeit, um Blatt 2 und 3 zu bearbeiten, sodass Blatt 3 nur die Hälfte der ansonsten üblichen Aufgabenzahl beinhaltet. Blatt 2 wird wie gewohnt vor den Übungen am 05.05. abgegeben, die neue Regelung beginnt ab Blatt 3.

Aufgabe 11: ISBN (1+2+2 = 5 P)

Zur eindeutigen Nummerierung von Büchern wird heute die sogenannte ISBN-13 (internationale Standard-Buchnummerierung) verwendet. Im Jahre 2006 löste sie die ISBN-10 als Standard ab, nachdem es mit dar Anzahl englischer Bücher Probleme gab.
Die ISBN-10 ist eine 10 -stellige Folge von 9 Dezimalziffern und einer Undezimalziffer (d.h. $x_{10} \in \{0, 1, \ldots, 10\}$, wobei $10 = X$), die ISBN-13 ist eine 13 -stellige Folge von Dezimalziffern. Die letzte Zahl jeder ISBN-Nummer ist die sogenannte Prüfziffer, sie ist Linearkombination der anderen Ziffern modulo einer Zahl. Die anderen Zahlen kodieren Verlags- und Landesinformationen.
Seien x_i , $1 \leq i \leq n$ mit $n = 10$ oder $n = 13$ nun die einzelnen Ziffern der ISBN. Für die Prüfziffer x_{10} der ISBN-10 gilt:

$$x_{10} \equiv \sum_{i=1}^{9} i x_i \bmod 11$$

Geschrieben wird dabei der Repräsentant des kanonischen Restsystems. Für die Prüfziffer x_{13} der ISBN-13 gilt:

$$x_{13} \equiv -\sum_{i=1}^{12} (2 + (-1)^i) x_i \bmod 10$$

Zur Umwandlung von ISBN-10 in ISBN-13 wird der ISBN-10 die Ziffernfolge 978 voran gestellt. Die Prüfziffer wird dabei entfernt und neu berechnet.

(a) Berechnen Sie die Prüfziffer x_{10} der ISBN-10 $345386143x_{10}$.
Berechnen Sie auch die ISBN-13 des Buches.

(b) Der Sinn der Prüfziffer ist, beim Eingeben z.B. an der Kasse mögliche Fehler entdecken und korrigieren zu können. Zeigen Sie, dass das Vertauschen von zwei voneinander verschiedenen Ziffern x_i und x_j , $i \neq j$ in einer ISBN-10 festgestellt werden kann (der häufigste Fehler).

(c) Nehmen Sie an, beim Einlesen einer ISBN-10 erhalten Sie folgende Ziffernfolge, wobei das ? für einen Lesefehler steht.

3540?02449

Welche Möglichkeiten gibt es? Welche für die folgende ISBN-13?

978 – 3540?02447

Unter der Annahme, dass beide ISBN dasselbe Buch bezeichnen (d.h. durch Umwandlung auseinander hervorgingen) , um welches Buch handelt es sich (Angabe der ISBN reicht)?

Aufgabe 12: Die multiplikative Gruppe der Restklassen (1+2+2 = 5 P)

Im Folgenden betrachten wir das kanonische Restesystem R modulo 17. Aus der Vorlesung wissen wir: R kann kanonisch mit der Menge $\{0, 1, 2, \ldots, 16\}$ identifiziert werden. Auf dieser Menge ist die Multiplikation $R \cdot R \to R$ wohldefiniert: Man setzt einfach $a \cdot b = c$, wenn c die Restklasse des Produktes belibiger Repräsentanten aus a und b ist. Beispielsweise ist $5 \cdot 5 = 8$ (oft wird das Restesystem auch mit $\overline{\text{Oberstrichen}}$ versehen, wenn man auf R eine Multiplikation definiert).

(a) Zeigen Sie: $R^\times := R - \{0\}$ enthält ein Element g mit $\operatorname{ord} g = 16 = \varphi(17)$. Außerdem lässt sich jedes Element in $R^\times$ als Potenz von g darstellen.

Ein Element mit den Eigenschaften in (a) heißt Erzeuger von $R^\times$.

(b) Sei g ein Element mit $\operatorname{ord} g = 16$ (also ein Erzeuger). Sei $a \in R^\times$ beliebig. Zeigen Sie: $\operatorname{ord} a | \operatorname{ord} g$ und falls $a = g^n$ die eindeutige Darstellung von a mit $n \leq 16$ ist, so ist $\operatorname{ord} a = \frac{16}{\mathrm{ggT}(n,16)}$.

(c) Berechnen Sie für jedes Element die Ordnung.