TECHNISCHE UNIVERSITÄT DRESDEN

Bereich Mathematik und Naturwissenschaften Fakultät Mathematik, Institut für Algebra

Jun.-Prof. Martin Schneider, Dr. C. Zschalig

Algebra und Zahlentheorie für Lehramt (Modul ALGZTH), Sommersemester 2019

13. Übungsblatt für die Übungen vom 1.7.-5.7.2019

Wiederholung, Anwendung

N13.1 **Hausaufgabe (Nachbereitung) Abgabe vor Übungsbeginn**

Es seien a_4, a_5, a_6, a_7 die letzten 4 Ziffern ihrer Matrikelnummer und $b_i = (a_i \mod 2)$ für $i \in \{4,5,6,7\}$. Weiter seien $p(X) = 1 \cdot X^4 + b_4 \cdot X^3 + b_5 \cdot X^2 + b_6 \cdot X^1 + b_7 \cdot X^0$ und $q(X) = X^3 + X^2 + X$ Elemente des Polynomrings $\mathbb{Z}_2[X]$.

Bestimmen Sie mit dem erweiterten Euklidischen Algorithmus $\mathrm{ggT}(p(X), q(X))$ und stellen Sie ihn als Linearkombination von $p(X)$ und $q(X)$ dar, d.h. finden Sie Polynome $r(X), s(X) \in \mathbb{Z}_2[X]$ mit

$$\mathrm{ggT}(p(X), q(X)) = r(X)p(X) + s(X)q(X).$$

Machen Sie eine Probe! Ist $q(X)$ invertierbar im Faktorring $\mathbb{Z}_2[X]/p(X)$?

V13.2 **Hausaufgabe (Vorbereitung) Abgabe vor Übungsbeginn**

(a) Eine natürliche Zahl n ist genau dann durch 3 teilbar, wenn ihre Quersumme (in Dezimaldarstellung) durch 3 teilbar ist. Beweisen Sie diese Aussage.

Finden Sie ähnliche Teilbarkeitsregeln für die Division durch 9 und durch 11.

Hinweis: Für eine Dezimalzahl n mit der Ziffernfolge $\ldots a_2 a_1 a_0$ ist $\ldots + 10^2 \cdot a_2 + 10^1 \cdot a_1 + 10^0 \cdot a_0 = n$. Betrachten Sie diese Darstellung modulo 3, 9 bzw. 11.

(b) Beweisen Sie die Teilbarkeitsregeln für 2, 4, 5 und 8.

Ü13.3 Im *Babylonischen Talmud* findet sich die folgende Teilbarkeitsregel (für im Dezimalsystem vorliegende Zahlen) für 7:
Spalte von einer natürlichen Zahl n die beiden letzten Ziffern ab. Die beiden letzten Ziffern bilden die Zahl a, alle anderen Ziffern die Zahl b. Dann ist n genau dann durch 7 teilbar, wenn $2b + a$ durch 7 teilbar ist.
Diese Regel kann rekursiv fortgesetzt werden, bis eine höchstens zweistellige Zahl n' vorliegt, von der die Teilbarkeit durch 7 bekannt ist.

(a) Bestimmen Sie mit der beschriebenen Methode, ob die Zahl $n = 26534$ durch 7 teilbar ist. Führen Sie das Verfahren rekursiv durch, bis Sie eine Zahl $n' < 100$ gefunden haben.

(b) Zeigen Sie, dass das Verfahren richtig ist und dass sogar $n \equiv 2b + a \pmod 7$ gilt.

(c) Finden Sie eine ähnliche Teilbarkeitsregel für die Zahl 17.

Begründen Sie Ihre Argumentation!

Ü13.4 Der ISBN13-Code bzw. EAN-Code wird folgendermaßen berechnet: (siehe Wikipedia): Sind $x_1, \ldots, x_{13}$ die Ziffern des Codes (x_{13} ist die *Prüfziffer*), dann muss gelten

$$3 \cdot \sum_{i=1}^{6} x_{2i} + \sum_{i=0}^{6} x_{2i+1} \equiv 0 \pmod{10}.$$

(a) Bestimmen Sie ein Verfahren, mit dem Sie zu gegebenen $x_1, \ldots, x_{12}$ die Prüfziffer x_{13} berechnen können.

(b) Zeigen Sie: Der Code erkennt einzelne Tippfehler (d.h. wird eine einzige Ziffer falsch geschrieben, dann ist die Prüfsumme falsch).

(c) Welche Zahlendreher erkennt der Code nicht?

Ü13.5 Zum Verschlüsseln eines Textes verwenden wir das RSA-Verfahren. Wir codieren die Buchstaben $\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Z}$ durch die Zahlen $0, 1, \ldots, 25$. Verschlüsseln Sie den Klartext `GEHEIM` mit dem öffentlichen Schlüssel

$$\text{(i) } (n, e) = (33, 3), \qquad \text{(ii) } (n, e) = (15, 5)$$

Das *RSA-Verfahren* verwendet einen öffentlichen Schlüssel (n, e) und einen privaten Schlüssel d. Dabei sind $n, e, d \in \mathbb{N}$ und $n = p \cdot q$ für zwei Primzahlen p, q. Weiter gilt $de \equiv 1 \pmod{\varphi(n)}$. Die Verschlüsselung eines Klartextbuchstaben $m \in \mathbb{Z}_n$ erfolgt durch die Abbildung $m \mapsto m^e =: c \pmod{n}$ und die Entschlüsselung durch $c \mapsto c^d = m \pmod{n}$.

Die folgenden Selbststudiumsaufgaben dienen der Festigung und Vertiefung des Stoffes in der Nachbereitung der Lehrveranstaltung. Sie müssen nicht abgegeben werden.

H13.6 In der Schule werden Teilbarkeitsregeln anhand bestimmter Klassen von Zahlen behandelt. Sie führen 5-stellige Zahlenpalindrome der Form *ababa* (d.h. natürliche Zahlen n in Dezimaldarstellung: $n = 10^4a + 10^3b + 10^2a + 10^1b + 10^0a$ mit $a, b \in \{0, \ldots, 9\}$ sein) ein.

Hinweis: Sie dürfen die üblichen Teilbarkeitsregeln für 3 und 11 als bekannt voraussetzen, d.h. Sie müssen sie nicht beweisen.

(a) Weisen Sie nach, dass die Zahl *ababa* genau dann durch 3 teilbar ist, wenn $b \in \{0, 3, 6, 9\}$ gilt.

(b) Ein Schüler vermutet, dass eine solche Zahl nie durch 13 teilbar ist. Widerlegen Sie das! Welche Bedingung muss an a und/oder an b gestellt werden, dass *ababa* durch 13 teilbar ist?

(c) Schließlich untersuchen wir die Teilbarkeit durch 11: Finden Sie eine Formel, mit der Sie für eine vorgegebene Ziffer $b \neq 4$ eine Ziffer a finden, so dass *ababa* durch 11 teilbar ist.

H13.7 Informieren Sie sich z.B. hier:

https://de.wikipedia.org/wiki/Internationale_Bankkontonummer#Validierung

wie die Prüfsumme in der Internationalen Bankkontonummer (IBAN) berechnet wird.

(a) Verifizieren Sie, dass die IBAN zu Ihrem Bankkonto korrekt ist.

(b) Bestimmen Sie ein Verfahren, mit dem Sie die Prüfziffer für gegebenen Ländercode, Bankleitzahl und Kontonummer berechnen können.

(c) Zeigen Sie: Der Code erkennt einzelne Tippfehler (d.h. wird eine einzige Ziffer falsch geschrieben, dann ist die Prüfsumme falsch).

(d) Zeigen Sie: Der Code erkennt Zahlendreher (d.h. werden zwei benachbarte Ziffern in falscher Reihenfolge, d.h. *ba* an Stelle von *ab*, geschrieben, dann ist die Prüfsumme falsch).

(e) Finden Sie ein Beispiel, so dass ein dreistelliger Zahlendreher nicht vom Code erkannt wird.

H13.8 Zum Verschlüsseln eines Textes wurde das RSA-Verfahren mit $(n, e) = (671, 113)$ verwendet. Bestimmen Sie d und entschlüsseln Sie den Text KC EW OS WK UK.

Hinweis: Die Buchstaben $A_1, \ldots, A_{10}$ des Klartextes wurden durch Zahlen $a_1, \ldots, a_{10}$ ersetzt ($A \to 0, B \to 1, \ldots, Z \to 25$). Je zwei aufeinanderfolgende Zahlen a_i und a_{i+1} ($i \in \{1, 3, 5, 7, 9\}$) wurden zu der neuen Zahl $m_i := 26 \cdot a_i + a_{i+1}$ zusammengefasst und durch $c_i = m_i^{113} \pmod{671}$ verschlüsselt. Die c_i wurden schließlich wieder in die Form $c_i = 26 \cdot b_i + b_{i+1}$ zerlegt und den Zahlen $b_1, \ldots, b_{10}$ Buchstaben $B_1, \ldots, B_{10}$ zugeordnet.