Diskrete Mathematik WS 09\10
Lösungsblatt 5

1

Wir rechnen in $(\mathbb{Z}_{35}, +, \cdot)$.

(a) Welche Elemente haben ein Inverses?

(b) Man berechne das multiplicative Inverse von 8.

Lösung:
a) $n = 35 = 5 \cdot 7$
x hat ein Inverses $\iff ggT(x, n) = 1$.
x hat ein Inverses $\leftrightarrow x$ heißt Einheit.
Die Elemente die keine Einheiten sind, sind Nullteiler.
Einheiten: $\{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34\}$
Nullteiler: $\{5, 7, 10, 14, 15, 20, 21, 25, 28, 30\}$

b) Mit erweiterten euklidischen Algorithmus
Berechne $ggT(35, 8)$

$$\begin{aligned} 35 &= 4 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot \mathbf{1} + \underline{0} \end{aligned}$$

$ggT(35, 8) = 1 = 3 - (8 - 2 \cdot 3) = 3 \cdot 3 - 8 = 3 \cdot (35 - 4 \cdot 8) - 8 =$
$= 3 \cdot 35 - 13 \cdot 8 = 1\surd$

$$\begin{aligned} &\implies 3 \cdot 35 + (-13) \cdot 8 = 1 \\ &(-13) \cdot 8 = 1 - 3 \cdot 35 \implies \\ &(-13) \cdot 8 \equiv 1 \mod 35 \end{aligned}$$

$\implies$ Das Inverse von 8 ist -13
$-13 = -13 + 35 = 22$
$\implies 8^{-1} = 22$
Test: $22 \cdot 8 = 176 \equiv 1 \mod 35\surd$

2

Man löse im Körper $\mathbb{Z}_7$ das lineare Gleichungssystem:

(a) $x + 3y = 1$

(b) $3x + y = 4$

Lösung:

$$x + 3y = 1 \implies 3x + 9y = 3 \implies 3x + 2y = 3 \quad (1)$$
$$3x + y = 4 \quad (2)$$

2 in 1':

$$\begin{aligned} y - 2y &= 4 - 3 \\ (-1) \cdot y &= 1 \\ y &= -1 \\ \implies \underline{y &= 6} \end{aligned}$$

in 1:

$$\begin{aligned} x + 3 \cdot 6 &= 1 \\ x &= -17 \\ \implies \underline{x &= 4} \end{aligned}$$

3

Wir rechnen in $(\mathbb{Z}_p, +, \cdot)$, wobei p eine Primzahl größer 2 ist. Wir haben also einen Zahlenkörper. Man zeige:

(a) $x \neq 0 \implies x \neq -x$

(b) 1 hat genau 2 Wurzeln, nämlich 1 und –1

(c) Wenn eine Zahl $a \neq 0$ eine Wurzel x hat, dann haz sie genau 2 Wurzeln, nämlich x und $-x$

(d) Man finde in $(\mathbb{Z}_7, +, \cdot)$ alle Zahlen, die eine Wurzel haben.

Lösung:
a)
$x \neq 0$
Angenommen $x = -x \implies x + x = 0 \implies 2 \cdot x = 0 \implies x = 0$ (Widerspruch)
b)
$1 \cdot 1 = 1$
$(-1) \cdot (-1) = 1$
Also sind 1 und -1 Wurzeln von 1.

Sei $(1+x)$ eine Wurzel von 1 $\implies$

$$\begin{aligned}(1+x)\cdot(1+x) &= 1 \implies\\ 1+x+x+x^2 &= 1 \implies\\ 2x+x^2 &= 0 \implies\\ x(2+x) &= 0\\ \underbrace{\implies}_{\text{x kein Nullteiler}} \quad x &= 0 \vee x = -2\end{aligned}$$

$1+x = 1 \vee -1 \implies$ 1 und -1 sind die einzigen Wurzeln von 1

c)
Sei x eine Wurzel von $a (a \neq 0)$
$(-x)^2 = [(-1)\cdot x]^2 = 1 \cdot x^2 = a$
Also ist auch $-x$ eine Wurzel von a.

Sei y eine weiter Wurzel von a

$$\begin{aligned}y^2 = a &= x^2\\ y^2 - x^2 &= 0\\ (y-x)\cdot(y+x) &= 0 \implies\\ y-x = 0 \vee y+x &= 0 \implies\\ y = x \vee y &= -x \implies\end{aligned}$$

x und $-x$ sind die einzigen Wurzeln von a.

d)

$$\begin{aligned}1^2 &= 1\\ 2^2 &= 4\\ 3^2 &= 9 = 2\\ 4^2 &= 16 = 2\\ 5^2 &= 25 = 4\\ 6^2 &= 36 = 1\end{aligned}$$

Die Quadratzahlen sind also: 1,2,4

4 Druck einer Broschüre

Wir wollen eine Broschüre aus Blättern erstellen, die wir in der Mitte falten. Ein Blatt wird vorne und hinten mit je zwei Seiten Text bedruckt. Die Reihenfolge beim Ausdruck kann deshalb nicht Seite 1, 2, 3, ... sein. Unsere Aufgabe

ist es, ein Programm zu entwickeln, das als Eingabe die Anzahl der Seiten einer Broschüre erwartet und die richtige Verteilung der Seiten auf die Blätter ausgibt. Eingabe: In der Datei broschuere.in befinden sich mehrere natürliche Zahlen n aus dem Intervall [1, 220], die die Anzahl der Seiten darstellen. Ausgabe: In broschuere.out werden die Informationen für den Ausdruck geschrieben.

Lösung:
Siehe Buch[2], Seiten 97-99.

5 Korrekte Nachrichten

Um während einer Informationsübetragung in der EDV Fehler zu erkennen, wird meist das CRC-Verfahren (Cyclic Redundancy Check) eingesetzt. Die Daten werden in kleinen Paketen gesendet, und am Ende jedes Pakets fügt man zusätzliche Informationen (Prüfsummen) ein, die helfen sollen, Übertra- gungs- fehler aufzuspüren.
Die Nachricht (das Paket) ist als eine lange binäre Zahl gegeben. Das erste Byte der Nachricht ist das Byte mit dem höchsten Stellenwert der binären Zahl. Das zweite Nachrichtenbyte hat den zweithöchsten Stellenwert usw. Wenn wir die Nachricht mit m bezeichnen, dann müssen wir nun m2 anstatt m übertragen, wobei m2 die Nachricht m und zwei Bytes für die Prüfsumme beinhaltet.
Der CRC-Wert ist so gewählt, dass die Division von m2 durch einen bestimmten 16-Bit-Wert g (Generatorwert) den Rest 0 ergibt. Dadurch kann der Empfangsprozess prüfen, ob die Nachricht fehlerfrei übertragen wurde. Er dividiert einfach die empfangenen Daten durch g. Wenn der Rest 0 ist, nimmt er an, dass die Übetragung korrekt erfolgt ist.
Unsere Aufgabe ist es ein Programm zu implementieren, das den CRC- Wert einer zu sendenden Nachricht berechnet. Wir nehmen als Generatorwert g=34943. Das Programm wird die Zeilen aus der Eingabedatei lesen und für jede von ihnen den zwei Byte langen CRC- Wert berechnen und ihn danach, repräsentiert durch zwei Hexadezimalzahlen, in die Ausgabedatei schreiben. Jede Eingabezeile beinhaltet maximal 1024 ASCII-Zeichen. Bemerkung: Jeder ausgegebene CRC-Wert liegt zwischen 0 und 34942 (dezimal). Eingabe: In der Eingabedatei crc.in finden sich mehrere String-Nachrichten, eine auf jeder Zeile. Ausgabe: Schreiben Sie in die Datei crc.out für jede Eingabezeile eine Zeile mit den hexadezimal dargestellten Prüfsummen- Bytes.

Lösung:
Siehe Buch[2], Seiten 114-117.

References

[1] Albrecht Beutelspacher, Marc-Alexander Zschiegner, Diskrete Mathematik für Einsteiger. Mit Anwendungen in Technik und Informatik, 3. Auflage, Vieweg Verlag, 2007.

[2] Doina Logofătu, Algorithmen und Problemlösungen mit C++, Vieweg+Tebuner Verlag, 2010.