Übungsaufgaben — Mathematik für Informatik III

SERIE 5 — Termin: 17.12.19/07.01.20

5.1 Sei $M := \mathbb{Q} \times \mathbb{Q}$. Auf M definieren wir

$$\begin{aligned}(a_1, a_2) \oplus (b_1, b_2) &:= (a_1 + b_1, a_2 + b_2)\\ (a_1, a_2) \odot (b_1, b_2) &:= (a_1 b_1, a_1 b_2 + a_2 b_1)\end{aligned}$$

Man beweise, dass $(M, \oplus, \odot)$ ein kommutativer Ring mit Einselement ist und bestimme die Nullteiler dieses Ringes!
Zu welchen Elementen von M gibt es bezüglich $\odot$ inverse Elemente?

5.2

(a) Ist das Polynom $p = x^2 + 1$ über $\mathbb{Z}/_3[x]$ irreduzibel?

(b) Stellen Sie die Verknüpfungstafeln für Addition und Multiplikation im Körper aus 9 Elementen auf.

5.3 Berechnen Sie alle Lösungen $(x_1, x_2, x_3)^T \in \mathbb{Z}_5^3$ des folgenden Gleichungssystems mit Koeffizenten aus $\mathbb{Z}_5$.

$$\begin{array}{rcrcrcl} 2x_1 & + & x_2 & & & = & 2\\ x_1 & & & + & 2x_3 & = & 4\\ 2x_1 & + & 2x_2 & + & x_3 & = & 1\end{array}$$

5.4 Ein zukünftiger Empfänger einer Nachricht wählt die beiden Primzahlen $p = 11, q = 17$ und als privaten Schlüssel den Exponenten $g = 97$. Was muss der Empfänger dem Absender mitteilen und wie muss der Absender seine Nachricht $a = 20$ verschlüsseln? Wie kann der Empfänger die übertragene Nachricht wieder entschlüsseln?

5.5 Die zweistellige Prüfsumme s für den IBAN wird so berechnet, dass $s \in \{2, 3, \ldots, 98\}$ und $s + k \equiv 1 \pmod{97}$ ist, wobei k die Kontoidentifikation ist. Die Kontoidentifikation ist eine 24-stellige Zahl, die sich aus der BLZ, der Kontonummer, dem Landescode sowie durch Auffüllung mit Nullen ergibt. Kann es passieren, dass 2 benachbarte Ziffern der Kontoidentifikation verändert werden, ohne dass sich die Prüfsumme ändert, dass man also 2 Fehler nicht erkennt? Wenn die Antwort "ja" lautet, geben Sie auch alle Möglichkeiten für die ursprünglichen benachbarten Ziffern an.