Lineare Algebra - Übungen zur Prädikatenlogik & Moduloarithmetik

Leopold Karl

2. Oktober, 2023

1 Moduloarithmetik: Tricks zum Lösen von Gleichungen

1.1 Finden eines multiplikativen Inversen in $\mathbb{F}_p$

Mit dem erweiterten euklidischen Algorthmus lässt sich algorithmisch das Inverse von $x \in \mathbb{F} \setminus \{0\}$ finden: Führe den erweiterten euklidischen Algorithmus für p und x durch, wobei wir x im Repräsentantensystem $\{1, 2, \ldots, p-1\}$ von $\mathbb{F} \setminus \{0\}$ wählen. Dann erhalten wir $a, b \in \mathbb{Z} : a \cdot p + b \cdot x = \text{ggt}(p, x) = 1$, da p prim und $b < p$ ist und wobei ggt als Abkürzung für „größten gemeinsamen Teiler“steht. Betrachten wir diese Gleichung modulo p, so erhalten wir gerade $b \cdot x \equiv_p 1$, da ja $a \cdot p \equiv_p 0$. Somit ist das so gefunden b gerade das Inverse von x in $\mathbb{F}_p$.
Wer den verallgemeinten Euklidischen Algorithmus nicht kennt, kann unter anderem folgende Quellen zu Rate ziehen:

1. Skript zur Vorlesung „Grundstrukturen“ für das zweite Semester in Mathematik von Lorenz Halbeisen, Kapitel 8, Seite 48ff. (https://metaphor.ethz.ch/x/2022/fs/401-1032-00L/sc/script.pdf)
2. Wikipedia. (https://de.wikipedia.org/wiki/Erweiterter_euklidischer_Algorithmus)

1.2 Gleichungen mit höheren Potenzen

Wenn wir Moduloarithmetik bzgl. einer Primzahl durchführen, gibt es häufig nur einige wenige Werte, die Potenzen annehmen können. Zum Beispiel kann $x^2 modulo 7$ nur die Werte $0, 1, 2, 4$ annehmen, wie man durch direktes Ausrechnen von $x^2 modulo 7$ für $x \in \{0, 1, 2, 3, 4, 5, 6\}$ einsieht. Für kleine Beispiele ist es oft nützlich dies konkret zu Berechnen, um vielleicht zu bemerken, dass sich gewisse Zahlen gar nicht als Potenz (zB als Quadrat eines Elements von $\mathbb{F}_p$) schreiben lassen und eine Gleichung somit potenziell gar keine Lösung besitzt.

2 Übungen zur Prädikatenlogik

Da das letzte Quiz beschaulich ausgefallen ist, hier noch ein paar Aufgaben zur Prädikatenlogik. Die Lösungen zur jeweils ersten Teilaufgabe findet ihr am Ende dieses Dokuments. Die Lösung der restlichen Teilaufgaben ist eine ähnliche. Bei Fragen könnt ihr euch natürlich jederzeit gerne an mich wenden!

Aufgabe 1 *Schreibe die folgenden Aussagen in Prädikatenlogik und negiere sie anschließend.*

(a) *„Alle Studenten arbeiten fleißig und interessieren sich für Lineare Algebra.“*

(b) *„Es gibt Studenten, die an der ETH studieren wollen, dies aber nicht tun.“*

(c) *„Alle Mensa-Sitzplätze sind besetzt oder reserviert.“*

Aufgabe 2 *Gib den folgenden mathematischen Aussagen einen Kontext. Negiere außerdem die mathematische Aussage. Dabei bezeichnen kleine Buchstaben Elemente von Mengen, A,B,C Aussagen (zB. A(x) = x hat eine Glatze) mit A(x) wahr, falls x die verlangte Eigenschaft besitzt, und falsch, falls nicht. Die restlichen Buchstaben bezeichnen Mengen.*

(a) $\forall x \in X : A(x) \implies B(x)$.

(b) $\exists y \in Y : y \in M \vee (y \in L \wedge y \in N)$.

(c) $\forall z \in Z\ \exists!\ w \in Z : z \cdot w = 1$.

Aufgabe 3 *Denke dir selbst ähnliche Aufgaben aus und stelle sie deinen Kollegen!*

3 Übungen zur Moduloarithmetik

Aufgabe 4 *Berechne die multiplikativen Inversen von:*

(a) $x \equiv_{101} 20$

(b) $x \equiv_{43} 4$

(c) $x \equiv_{73} 27$

Aufgabe 5 *Berechne die quadratischen Reste ...*

(a) *... modulo 5*

(b) *... modulo 11*

(c) *... modulo 4*

Aufgabe 6 *Hat die folgende Gleichung Lösungen? Falls ja, gib diese an!*

(a) $x^2 \equiv_5 2$

(b) $x^2 \equiv_7 4$

(c) $x^3 - x^2 \equiv_4 3$

(d) $x^3 + 2x^2 \equiv_4 1$

Die Lösungen findet ihr auf der nächsten Seite.

4 Lösungen zu den Aufgaben

Lösung 1

(a) *Sei $S :=$ Menge der Studenten, $F :=$ Menge der fleißig arbeitenden Menschen, $L :=$ Menge der Menschen, die sich für Lineare Algebra interessieren. Dann lautet die Aussage aus Aufgabe 1(a): $\forall s \in S : s \in F \wedge s \in L$ und ihre Negation: $\exists s \in S : s \notin F \vee s \notin L$.*

Lösung 2

(a) *Für alle Studenten der ETH gilt, wer fleißig arbeitet, erreicht sein Ziel. (Etwas näher an der mathematischen (Symbol-)Sprache: Für jeden Studenten der ETH gilt: Wenn der Student fleißig arbeit, impliziert dies, dass er seine Ziele erreicht.)*

Lösung 3 *Die muss wohl jeder selbst notieren. ;)*

Lösung 4 *(a)* $x^{-1} \equiv_{101} 96$

(b) $x^{-1} \equiv_4 311$

(c) $x^{-1} \equiv_7 346$

Lösung 5

(a) $x^2 \ mod\ 5 \in \{0, 1, 4\}$

(b) $x^2 \ mod\ 11 \in \{0, 1, 3, 4, 5, 9\}$

(c) $x^2 \ mod\ 4 \in \{0, 1\}$

Lösung 6

(a) *Es gibt keine Lösung (vgl. A5(a)).*

(b) $x \in \{2, 5\}$

(c) *Es gibt keine Lösung.*

(d) $x \equiv_4 3$.

Anmerkung A6(b),(c),(d) wurden hier durch konkrete Berechnung gelöst.

Kontakt:
Website: www.leopoldkarl.com
Mail: lekarl@student.ethz.ch
LinkedIn: Leopold Karl