Bereich Mathematik und Naturwissenschaften Fakultat Mathematik, Institut fur Algebra

Dr. E. Lehtonen, Dr. C. Zschalig

Algebra und Zahlentheorie für Lehramt (Modul ALGZTH), Sommersemester 2018

6. Übungsblatt für die Übungen vom 14.5.-18.5.2018

Modulrechnung

Ein wesentliches Kriterium bei der Präsentation der folgenden Themen ist die Interaktion. Ziel ist es, die Probleme gemeinsam mit dem Auditorium zu erarbeiten und nicht frontal zu vermitteln. Setzen Sie dabei - falls die limitierte Zeit dazu ausreicht - Lerntechniken ein, die Sie im Studium kennengelernt haben. Die Vortragsdauer ist strikt auf 12 Minuten beschränkt.

T6.1 **Themenaufgabe: Fibonacci-Zahlen**

Die Folge der *Fibonacci-Zahlen* (f_n) ist rekursiv definiert durch

$$f_1 = f_2 = 1 \quad \text{und} \quad f_{n+2} = f_{n+1} + f_n \text{ für alle } n > 0.$$

(a) Erläutern Sie kurz geschichtliche Entwicklung der Zahlen; wo kommen Fibonacci-Zahlen vor?

(b) Berechnen Sie die Elemente der Folge bis f_{10}.

(c) Stellen Sie den ggT von f_9 und f_{10} sowie von f_{10} und f_{11} als Linearkombination von f_9 und f_{10} bzw. von f_{10} und f_{11} dar.

(d) Zeigen Sie (z.B. durch Induktion), dass zwei aufeinanderfolgende Fibonacci-Zahlen f_n und f_{n+1} teilerfremd sind und insbesondere die Beziehung $(-1)^n = f_{n-1} \cdot f_n - f_{n-2} \cdot f_{n+1}$ (für alle $n > 2$) für ihre Linearkombination gilt.

T6.2 **Themenaufgabe: Modulrechnung - Kürzungsregeln & das Inverse.**

Diskutieren Sie die Gültigkeit von Kürzungsregeln beim Rechnen mit Kongruenzen.
Wie kommt der euklidische Algorithmus bei der Berechnung des Inversen ins Spiel? Wenden Sie dies auf lineare Kongruenzen:

$$\text{Finde alle } x \in \mathbb{Z}, \text{für die gilt:} \quad a \cdot x \equiv b \pmod{n}$$

an und besprechen Sie die drei grundlegenden Fälle für die Lösungsmenge an Beispielen.

Ü6.3 (a) Beweisen Sie die Teilbarkeitsregeln für 2, 4, 5 und 8.

(b) Beweisen Sie die Teilbarkeitsregeln durch 3, 9 und 11.

Ü6.4 Besitzen die folgenden Elemente x ein Inverses in $\mathbb{Z}_n$? Berechnen Sie ggf. das Inverse $x^{-1} \pmod{n}$.

(i) $x = 18, n = 31$, (ii) $x = 60, n = 257$, (iii) $x = 511, n = 1001$, (iv) $x = 512, n = 1001$.

Ü6.5 Es sei $n \in \mathbb{N}$ und $\mathbb{Z}_n$ der Restklassenring bezüglich n.

(a) Für welche n ist jedes Element $a \in \mathbb{Z}_n \setminus \{0\}$ eine Einheit?

(b) Beweisen oder widerlegen Sie: Das Produkt von zwei Einheiten ist wieder eine Einheit.

(c) Beweisen oder widerlegen Sie: Die Summe von zwei Einheiten ist wieder eine Einheit.

(d) Beweisen oder widerlegen Sie: Ist a eine Einheit, dann ist auch $n - a$ eine Einheit.

A6.6 **Hausaufgabe, Abgabe (mit Name und Matrikelnr.) bis 18.5.2018, 12:00 Uhr**

(a) Schreiben Sie Ihre Matrikelnummer (7-stellig) auf. Die letzten drei Ziffern bilden (als dreistellige Zahl gelesen) die Zahl z. Die Zahl y erhalten Sie nach der Vorschrift:

$$y := \begin{cases} z, & z > 99 \\ z + 100, & z \leq 99 \end{cases}$$

Bestimmen Sie mit dem Euklidischen Algorithmus den ggT von 1009 und y und stellen Sie ihn als Linearkombination von 1009 und y dar. Finden Sie das Inverse von y in $(\mathbb{Z}_{1009}, \cdot)$ oder begründen Sie, warum das Inverse nicht existiert. Machen Sie eine Probe!

(b) Verifizieren Sie, dass die folgende Teilbarkeitsregel für 7 richtig ist. Rechnen Sie ggf. vorher einige Beispiele:
Es sei n eine natürliche Zahl. Wir zerlegen die (bzgl. Dezimalsystem gegebenen) Ziffern von n in zwei Teile: Die letzte Ziffer bildet die Zahl a und die vor der letzten Stelle liegenden Ziffern bilden die Zahl b. Dann ist n genau dann durch 7 teilbar, wenn $b - 2a$ durch 7 teilbar ist. Das Verfahren kann rekursiv fortgesetzt werden.
Finden Sie eine ähnliche Teilbarkeitsregel für die Zahl 17.

Die folgenden Selbststudiumsaufgaben dienen der Festigung und Vertiefung des Stoffes in der Nachbereitung der Lehrveranstaltung.

H6.7 Geben Sie die Lösungsmengen der folgenden Gleichungen an!

(i) $5x \equiv 1 \pmod 7$ (ii) $10x \equiv 9 \pmod{25}$ (iii) $32x \equiv 14 \pmod{82}$

Hinweis zu (iii): Es gibt eine Regel zur Modulo-Rechnung, mit deren Hilfe die Gleichung geeignet umgeformt werden kann!

H6.8 Auf einer Insel leben 13 rote, 15 grüne und 17 blaue Chamäleons. Treffen sich zwei verschiedenfarbige Chamäleons, ändern sie beide ihre Farbe in die dritte Farbe. Begegnen sich gleichfarbige Chamäleons, ändern sie ihre Farbe nicht. Ist es durch eine bestimmte Folge von Begegnungen möglich, dass alle Chamäleons die gleiche Farbe annehmen?

Hinweis: Codieren Sie die drei Farben als Reste $\pmod 3$. Ändert sich die „Summe“ der Farben, wenn sich 2 Chamäleons treffen? Was folgt daraus?

H6.9 Beweisen Sie

(a) Proposition 1.72 ($\equiv_n$ ist für alle $n \in \mathbb{N}$ eine Äquivalenzrelation auf $\mathbb{Z}$)
Beschreiben Sie die Äquivalenzklassen im Fall $n = 1$ und $n = 0$.

(b) Propostion 1.75 ($\forall n \in \mathbb{N}, \forall a, b \in \mathbb{Z} : [a] = [b] \iff n | b - a$)

(c) Proposition 1.80 (siehe Skript).

H6.10 Zum Schluss noch ein Rätsel, welches auf Modulrechnung (hier $\pmod 2$) beruht:

https://ed.ted.com/lessons/can-you-solve-the-prisoner-hat-riddle-alex-gendler

Übrigens kann das selbe Rätsel auch mit n Hutfarben gestellt werden, dann muss entsprechend $\pmod n$ gerechnet werden.