TECHNISCHE UNIVERSITÄT DRESDEN

Bereich Mathematik und Naturwissenschaften Fakultat Mathematik, Institut fur Algebra

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

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

5. Übungsblatt für die Übungen vom 29.4.-3.5.2019

Rechnen in Restklassenringen

An Stelle der ausfallenden Übungen am 1. Mai besuchen Sie bitte eine der Ersatzübungen am 30.4., 6.DS, WIL/C204 oder am 2.5., 6.DS, WIL/C204.

N5.1 **Hausaufgabe (Nachbereitung) Abgabe vor Übungsbeginn**

(a) Schreiben Sie Ihre Matrikelnummer auf; die zweite, dritte, vierte und fünfte Ziffer bilden (als 4-stellige Dezimalzahl gelesen) die Zahl x.

Bestimmen Sie die Primfaktorzerlegung von x. Zeichnen Sie ein Teilerdiagramm aller Teiler von x und bestimmen Sie die Anzahl der Teiler.

Diese Teilaufgabe ist von jedem Mitglied Ihrer Gruppe zu lösen!

(b) Finden Sie alle natürlichen Zahlen n, die genau 6 Teiler haben und durch 6 teilbar sind.

(c) Zeigen Sie, dass folgende Gleichung für alle $a, b \in \mathbb{N}$ gilt:

$$\mathrm{ggT}(a, \mathrm{kgV}(a, b)) = a.$$

Hinweis: Wenn Sie den Beweis besonders elegant und kurz aufschreiben wollen, verwenden Sie 1.19 und 2.23 aus der Vorlesung.

V5.2 **Hausaufgabe (Vorbereitung) Abgabe vor Übungsbeginn**

(a) (i) Berechnen Sie $\varphi(120)$.

(ii) Wie viele Elemente $x \in \mathbb{Z}_{120}$ besitzen ein multiplikatives Inverses?

(iii) Berechnen Sie die multiplikativen Inversen zu $a = 43$ und $b = 87$ in $\mathbb{Z}_{120}$ (falls sie existieren) mit dem erweiterten Euklidischen Algorithmus.

(b) Zeigen Sie (mit 2.27) die folgenden Aussagen zum Modulo-Rechnen:

(i) $\forall a, b \in \mathbb{Z} \forall m, n \in \mathbb{N} : a \equiv b \pmod{m \cdot n} \implies a \equiv b \pmod{n}$

(ii) $\forall a, b \in \mathbb{Z} \forall m, n \in \mathbb{N} : ma \equiv mb \pmod{m \cdot n} \iff a \equiv b \pmod{n}$

Ü5.3 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!

Ü5.4 Lösen Sie folgende Systeme linearer Kongruenzen. Führen Sie jeweils eine Probe durch.

(a)
$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

(b)
$$\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 6 \pmod 7 \\ x &\equiv 9 \pmod{11} \end{aligned}$$

Ü5.5 Berechnen Sie mit der Methode *Square and Multiply* folgende Werte:

(a) $3^{205} \bmod 11$ (b) $36^{326} \bmod 17$

Ü5.6 Beweisen Sie, dass für jede Primzahl p gilt:

$$\forall i \in \{1, \ldots, p-1\} : p \mid \binom{p}{i}.$$

Schlussfolgern Sie, dass für jede Primzahl p gilt:

$$\forall a, b \in \mathbb{Z} : (a+b)^p \equiv a^p + b^p \pmod{p}.$$

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

H5.7 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: Eine Zahl mit der Ziffernfolge $\ldots a_2 a_1 a_0$ kann als $\ldots + 10^2 \cdot a_2 + 10^1 \cdot a_1 + 10^0 \cdot a_0$ geschrieben werden. Betrachten Sie diese Darstellung modulo 3, 9 bzw. 11.

H5.8 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.

H5.9 Es war einmal eine Bande von 17 Piraten, die stahl einen Sack mit Goldstücken. Als sie ihre Beute in gleiche Teile teilen wollten, blieben 3 Goldstücke übrig. Beim Streit darüber, wer ein Goldstück mehr verdient habe, wurde ein Pirat erschlagen. Wieder wurde gleichmäßig verteilt, doch nun blieben dabei 10 Goldstücke übrig. Erneut kam es zu Streit und wieder verlor ein Seeräuber sein Leben. Da aber ließ sich endlich die Beute gleichmäßig verteilen. Wie viele Goldstücke waren mindestens im Sack?

H5.10 Zum Schluss noch ein Rätsel, welches auf Modulrechnung (hier (mod 2)) beruht:

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

Übrigens kann dasselbe Rätsel auch mit n Hutfarben gestellt werden, dann muss entsprechend (mod n) gerechnet werden.