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

4. Übungsblatt für die Übungen vom 22.4.-26.4.2019

Primzahlen, Primfaktorzerlegung

N4.1 **Hausaufgabe (Nachbereitung) Abgabe vor Übungsbeginn**

(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. Machen Sie eine Probe!

Diese Aufgabe soll jedes Mitglied Ihrer Hausaufgabengruppe lösen.

(b) Für welche Primzahlen p ist $p^2 - 1 = (p-1)(p+1)$ durch 24 teilbar?

V4.2 **Hausaufgabe (Vorbereitung) Abgabe vor Übungsbeginn**

(a) Das *Sieb des Eratosthenes* ist eine Methode, um alle Primzahlen zwischen 1 und $n \in \mathbb{N}$ zu bestimmen: Dazu werden die Zahlen von 1 bis n in eine Liste geschrieben und für jede Primzahl $p \leq \sqrt{n}$ werden alle (echten) Vielfachen von p gestrichen. Alle nichtgestrichenen Zahlen sind dann prim.

(i) Bestimmen Sie mit diesem Verfahren alle Primzahlen zwischen 1 und 100.

(ii) Warum funktioniert das Verfahren? (Sie müssen also zeigen, dass jedes $n \in \mathbb{N} \setminus \mathbb{P}$ einen Primteiler $p \leq \sqrt{n}$ besitzt).

(b) Zeigen Sie, dass die Menge $\{p \in \mathbb{P} \mid p \equiv 3 \pmod 4\}$ unendlich ist. Dabei bezeichne $\mathbb{P}$ die Menge der Primzahlen.

Hinweis: Versuchen Sie den Beweis analog zu dem Beweis zu führen, dass es unendlich viele Primzahlen gibt.

Ü4.3 Zeigen Sie: Ist n keine Primzahl, dann ist auch $2^n - 1$ keine Primzahl.

Hinweis: Gilt $n = a \cdot b$, dann zeigen Sie $2^a - 1 | 2^n - 1$.

Um große Primzahlen zu finden, werden als Kandidaten Zahlen der Form $2^n - 1$ betrachtet. U.a. wegen obiger Eigenschaft lassen sich solche Zahlen besser auf Primalität untersuchen.

Ü4.4 Beweisen Sie mit dem „Prinzip des kleinsten Verbrechers“, dass es zu einer natürlichen Zahl $n \geq 1$ keine natürliche Zahl m gibt, so dass $2m^2 = n^2$ gilt. Schlussfolgern Sie, dass $\sqrt{2}$ keine rationale Zahl ist.

Ü4.5 (a) Wie viele Teiler hat die Zahl 360?

(b) Wie viele dieser Teiler sind durch 4 teilbar?

(c) Zeichnen Sie ein Teilerdiagramm der Menge der durch 4 teilbaren Teiler der Zahl 360, geordnet nach Teilbarkeit.

(d) Wie viele gerade natürliche Zahlen gibt es, die genau 5 Teiler haben?

Ü4.6 Beweisen Sie Satz 2.23(2) aus der Vorlesung:

Für alle $e, f \in \mathbb{N}^{\mathbb{P}}$ gilt:

(a) $\psi(e \vee f) = \mathrm{kgV}(\psi(e), \psi(f))$,

(b) $\psi(e \wedge f) = \mathrm{ggT}(\psi(e), \psi(f))$,

(c) $\psi(e + f) = \psi(e) \cdot \psi(f)$.

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

H4.7 Es sei $\underline{R} = (R, +, \cdot)$ ein kommutativer Ring mit 1. Überzeugen Sie sich von der Richtigkeit der folgenden Gleichungen für alle $a, b \in R$ und alle $n \in \mathbb{N}$:

(a) $\forall n \in \mathbb{N} : a^n - b^n = (a-b) \cdot \sum_{i=0}^{n-1} a^{n-1-i} b^i \qquad$ (d.h. $(a-b)|(a^n - b^n)$),

(b) $\forall n \in \mathbb{N} : 2 \not| n \implies a^n + b^n = (a+b) \cdot \sum_{i=0}^{n-1} (-1)^i a^{n-1-i} b^i \qquad$ (d.h. $(a+b)|(a^n + b^n)$),

(c) $\forall n \in \mathbb{N} : 2 | n \implies a^n - b^n = (a+b) \cdot \sum_{i=0}^{n-1} (-1)^i a^{n-1-i} b^i \qquad$ (d.h. $(a+b)|(a^n - b^n)$).

Hinweis: Falls Sie „Angst“ vor Ringen haben, stellen Sie sich einfach vor, Sie würden in $\mathbb{Z}$ rechnen - die Beweise sind völlig gleich.

H4.8 Finden Sie alle natürlichen Zahlen $x, y \in \mathbb{N}$, für die $y^3 - x^3 = 721$ gilt.

H4.9 Gegeben sei die Abbildung $f : \mathbb{N} \to \mathbb{N}, \quad n \mapsto n^2 - n + 41$. Bestimmen Sie $f(n)$ für alle $n \in \{0, 1, \ldots, 10\}$ und überzeugen Sie sich davon, dass $f(n)$ in jedem Fall eine Primzahl ist. Beweisen oder widerlegen Sie: Für jede natürliche Zahl n ist $n^2 - n + 41$ eine Primzahl.

H4.10 (a) Bestimmen Sie den größten gemeinsamen Teiler $\mathrm{ggT}(m, n)$ und das kleinste gemeinsame Vielfache $\mathrm{kgV}(m, n)$ der beiden Zahlen $m = 240 = 2^4 \cdot 3 \cdot 5$ und $n = 396 = 2^2 \cdot 3^2 \cdot 11$. Bilden Sie die Produkte $m \cdot n$ und $\mathrm{ggT}(m, n) \cdot \mathrm{kgV}(m, n)$. Was stellen Sie fest?

(b) Beweisen Sie: Für je zwei natürliche Zahlen m, n gilt $m \cdot n = \mathrm{ggT}(m, n) \cdot \mathrm{kgV}(m, n)$.

H4.11 (a) Finden Sie eine Wohlordnung auf $\mathbb{Z}$.

(b)* Finden Sie eine Wohlordnung auf $\mathbb{Q}$. (Wenn Sie auch nach einigem Überlegen auf keine Lösung kommen, dann suchen Sie nach „Cantors Diagonalargument“).