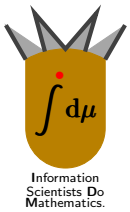

Vorlesung **Mathematik für Informatiker I** 14. Dezember 2018
(an der Universität Heidelberg)
Dozent: *Dr. Martin Rheinländer*
Tutoren: *Adrian Danisch, Armand Rousselot, Denise Becker, Vasil Manev, Christian Moses*

Aufgabenserie 7
Kongruenzklassen - Modulares Rechnen

Aufgabe 7.1: Rechnen mit Restklassen (5+5+5=15P)

a) Geben Sie die Multiplikationstafel von $\mathbb{Z}_9, \mathbb{Z}_{10}$ und $\mathbb{Z}_{11}$ an. Um Schreibarbeit zu sparen, kann man die Multiplikation mit 0 unberücksichtigt lassen. Wie lauten die jeweiligen Inversen sofern existent zu $3, 5$ und 7 in den drei Restklassenmengen?

b) Welche Reste ergeben sich, wenn man 3^{15} und 15^{83} durch 13 dividiert?

c) Seien $a, b, c \in \mathbb{Z}$ und $n \in \mathbb{N}$. Generell gilt dann folgende Implikation (Erweiterungsregel)

$$a \equiv b \mod n \quad \Rightarrow \quad ac \equiv bc \mod n.$$

Zeigen Sie anhand von zwei Beispielen, daß die umgekehrte Implikation im allgemeinen nicht stimmt. Unter welcher Voraussetzung an c läßt sich die Implikation umkehren, d.h. welche Eigenschaft muß der rechts wie links vorhandene Faktor c aufweisen, damit er formal herausgekürzt werden kann? Die Antwort ist zu begründen.

Aufgabe 7.2: Teilbarkeitsregeln (5+5+5=15P)

a) Rechnen Sie die Teilbarkeitsregeln für 3 und 9 nach: Eine natürliche Zahl n mit der Dezimaldarstellung $s_k s_{k-1} ... s_0$ (bestehend aus den Ziffern $s_i \in \{0, 1, ..., 9\}$ für $i \in \{0, 1, ..., k\}$) ist genau dann durch 3 bzw. 9 teilbar, wenn ihre Quersumme $q = \sum_{i=0}^{k} s_i$ durch 3 respektive 9 teilbar ist.

Zusatzfrage: Für welche Zahlen erwarten Sie analoge Teilbarkeitsregeln, wenn statt des Dezimalssytems das Stellewertsystem zur Basis 17 verwendet wird?

b) Geben Sie für dreistellige Dezimalzahlen $n = s_2 s_1 s_0$ eine Teilbarkeitsregel bezüglich 7 an unter Verwendung einer *gewichteten Quersumme* $w_2 s_2 + w_1 s_1 + w_0 s_0$ mit geeigneten ganzzahligen Gewichten w_0, w_1, w_2. Demonstrieren Sie Ihre Teilbarkeitsregel an einem Beispiel.

c) Können die Ziffern $x, y, z \in \{0, 1, 2, ..., 9\}$ paarweise verschieden gewählt werden, so daß für die dreistellige Zahl xxy und die vierstellige Zahl $zy5y$ die Gleichung

$$xxy \cdot y = zy5y$$

besteht? Wenn ja, wie sind die Ziffern zu wählen? Kommen mehrere Möglichkeiten in Betracht?

Anmerkung: Wer nicht überlegen möchte, kann seinen Computer sämtliche Möglichkeiten ausprobieren lassen und so vielleicht fündig werden. Das entspräche zwar nicht dem eigentlichen Zweck der Aufgabe, wäre aber dennoch eine nette kleine Programmierübung.

Aufgabe 7.3: Anwendung des Euklidischen Algorithmus (5+5+5+5=20P)

a) Erproben Sie den Euklidischen Algorithmus zunächst, indem Sie damit $\mathrm{ggT}(44, 12)$ bestimmen und eine zugehörige Vielfachsummendarstellung des ggT's. Warum heißt es eigentlich *eine* und nicht *die* zugehörige Vielfachsummendarstellung?

b) Hat $82 \in \mathbb{Z}_{239}$ (als Element der Restklassenmenge zu 239) ein multiplikativ Inverses? Geben Sie dieses ggf. an.

c) Existiert $x \in \mathbb{Z}_{119}$, so daß in $\mathbb{Z}_{119}$ gilt $x \cdot 21 = 35$? Wenn ja, geben Sie eine Lösung an.

d) (diophantische Gleichungen) Gesucht sind alle Paare ganzer Zahlen, welche eine Lösung (aus $\mathbb{Z} \times \mathbb{Z}$) zu jeweils einer der beiden folgenden Gleichungen darstellen:

$$\text{i)} \quad 42u + 15v = 153,$$
$$\text{ii)} \quad 35x + 21y = 116.$$

Es ist möglich, daß eine Gleichung mehrere oder keine Lösung hat. Die Antwort zu i) und ii) ist jeweils zu begründen.

Bonusaufgaben

Die folgenden Bonusaufgaben dienen der (freiwilligen) Wiederholung und Ergänzung der Vorlesung und sind unbepunktet. Ihr Tutor wird Sie aber sicher nicht ganz leer ausgehen lassen, wenn Sie sich damit in schriftlicher Form sinnvoll auseinandergesetzt haben und eine Berabeitung einreichen.

Aufgabe 7.4: Zum Verständnis des Euklidischen Algorithmus

a) **Grundlegende Idee**: Die Idee des Euklidischen Algorithmus beruht auf der Erkenntnis, daß der *größte gemeinsame Teiler*[1] zweier ganzer Zahlen a und b gleich dem größten gemeinsamen Teiler von b und der Differenz von $a - b$ ist (entsprechend könnte man auch a und $a - b$ bzw. $b - a$ betrachten).

Zeigen Sie nun *en détail*: Es gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a - b)$ und sogar $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a - kb)$ mit $k \in \mathbb{Z}$, wobei aus der letzteren Gleichung auch $\mathrm{ggT}(a, b) = \mathrm{ggT}\big(b, \mathrm{mod}(a, b)\big)$ folgt.

Hinweis: $a = (a - b) + b$.

b) **Algorithmische Formulierung:** Wie in der Vorlesung besprochen, kann der Euklidische Algorithmus wahlweise als einstufige Iteration

$$\begin{cases} a_i = b_{i-1} \\ b_i = r_{i-1} \\ q_i = a_i \operatorname{div} b_i \\ r_i = a_i \bmod b_i \end{cases}$$

mit der Initialisierung $b_0 = a \in \mathbb{N}_0$ und $r_0 = b \in \mathbb{N}_0$ oder als zweistufige Iteration

$$z_k = z_{k-2} - q_k z_{k-1} \qquad \text{mit} \quad q_k = z_{k-2} \operatorname{div} z_{k-1}$$

mit der Initialisierung $z_{-1} = a, z_0 = b$ geschrieben werden. Wie hängen die beiden Iterationen miteinander zusammen, d.h. welche Größen sind genau mit welchen zu identifizieren? Wie lauten die Abbruchbedingungen für die Iterationen?

Erklären Sie kurz das Verhalten des Algorithmus, falls dieser ungünstig mit $a < b$ (statt $a \geqq b$) initialisiert wird.

c) **Laufzeit-Analyse:** Warum gilt in jedem Iterationsschritt $b_{i+1} \leqq b_i - 1$? Begründen Sie zunächst die generelle Ungleichung

$$b \bmod (b - k) \; < \; b/2$$

[1] $d \in \mathbb{N}$ heißt größter gemeinsamer Teiler von $a, b \in \mathbb{Z}$, wenn d ein Teiler von a und b ist mit der Eigenschaft, daß jeder weitere gemeinsamer Teiler $t \in \mathbb{N}$ von a und b auch ein Teiler von d ist.

für $b \in \mathbb{N}$ und $k \in \{0, 1, ..., b-1\}$. Benutzen Sie diese, um zu erklären, warum der Euklidische-Algorithmus spätestens nach

$$2\lceil \log_2 b \rceil + 1$$

Schritten terminieren muß, wenn $b := \min\{a, b\}$ der kleineren der beiden Zahlen entspricht, deren größter gemeinsamer Teiler $\mathrm{ggT}(a, b)$ mit dem Euklidischen Algorithmus zu ermitteln ist.

d) **Anwendung:** Berechnen Sie mit dem erweiterten Euklidischen Algorithmus die multiplikativ Inverse zu $91 \in \mathbb{Z}_{264}$.

Aufgabe 7.5: Alternativ-Algorithmus gesucht!

Dividieren ist bekanntlich die aufwendigste der vier arithmetischen Grundoperationen. Dies gilt auch für Computer, allerdings mit einer Ausnahme. Da dem Computer die Zahlen in Binärdarstellung vorliegen, vermag er mit sehr geringem Aufwand durch 2 zu teilen, falls dies möglich ist.

Entwerfen Sie daher einen Algorithmus, der wie der Euklidische Algorithmus zu zwei gegebenen natürlichen Zahlen a, b den größten gemeinsamen Teiler bestimmt, dabei einerseits Divisionen mit einem Divisor ungleich 2 vermeidet, andererseits aber Divisionen durch 2 ausführt, wann immer dies möglich ist, um einen möglichst schnellen Abstieg zu erreichen.

Aufgabe 7.6: Nachtrag zum Thema Kardinalitäten und natürliche Zahlen

a) Es seien A und B zwei Mengen. Man zeige:

$$|A| \leqq |B| \quad \wedge \quad |B| \leqq |A| \qquad \Rightarrow \qquad |A| = |B|$$

Hinweis: Die Aussage von Aufgabe 6.6 kann verwendet werden.

b) Es sei $M \subset \mathbb{N}$ und es gelte $\forall n \in \mathbb{N} : |M| \neq n$ (d.h. $|M| \neq |A_n|$). Dann folgt: $|M| = |\mathbb{N}|$.

In Worten: Jede unendliche Teilmenge von $\mathbb{N}$ ist ebenso mächtig wie $\mathbb{N}$ selbst.

c) Erklären Sie, wie ein *Induktionsbeweis* basierend auf dem *Induktionsprinzip* formal in einen *Widerspruchsbeweis* umgewandelt werden kann, welchem das *Wohlordnungsprinzip* zugrunde liegt.

Bitte die Abgaben im Moodle hochladen bis zum 21.12.2018, 14:00 Uhr.