Diskrete Mathematik **FTB-INF**
Dr. Martin E. Müller **WS 24/25**

Übungsblatt 3 - ggT, Division in $\mathbb{Z}/n\mathbb{Z}$, und Anwendung endlicher Körper

1. Implementieren Sie in PYTHON eine „naive“ Funktion `ggT(a,b)`, welche den größten gemeinsamen Teiler von a und b berechnet, indem sie ausgehend von der kleineren der beiden Zahlen diese um eins reduziert und prüft, ob diese Zahl ggT von a und b ist.

2. Zeigen Sie anhand eines Zahlenbeispiels, dass wenn c Teiler von a und b ist, c auch deren Differenz teilt.

3. Inwiefern ist die Aussage „Ist c Teiler von a und b dann teilt c auch $\alpha \cdot a + \beta \cdot b$“ eine Veralgemeinerung der Aussage „Ist c Teiler von a und b dann teilt c auch $a + b$ sowie $a - b$“?

4. Berechnen Sie den größten gemeinsamen Teiler von 233 und 144 mit Bleistift und Papier, indem Sie Euklids Algorithmus anwenden. Wiederholen Sie das mit anderen Werten, bis Sie den Algorithmus verstanden haben. (Sie können die PYTHON-Funktion verwenden, um Ihre Ergebnisse zu überprüfen)

5. Verbessern Sie die Funktion `ggT(a,b)` aus der Vorlesung, in dem Sie nicht in jedem Durchlauf die kleinere von der größeren Zahl abziehen, sondern gleich den Rest bei n-fachem Abziehen berechnen.

6. Erklären Sie die in der Vorlesung gezeigte Erweiterung von Euklids Algorithmus, welche uns zusätzlich zum ggT die lineare Kombination der beiden Parameter a und b liefert, so dass $ggT = \alpha \cdot a + \beta \cdot b$.

7. Welche Gleichung lösen Sie, wenn sie das multiplikativ Inverse berechnen? Wie können Sie mithilfe der Berechnung des ggT's feststellen, ob ein multiplikativ inverses Element für eine Zahl a in einem Restklassenring $\mathbb{Z}/n\mathbb{Z}$ existiert?

8. Berechnen Sie von Hand das multiplikative Inverse von 3 in $\mathbb{Z}_7$ sowie von 8 in $\mathbb{Z}_{11}$.

9. Verwenden Sie den erweiterten Algorithmus von Euklid und berechnen Sie damit das multiplikativ Inverse (Kehrwerte) von 7 in $\mathbb{Z}/18\mathbb{Z}$. Prüfen Sie auch ihre Ergebnisse aus Aufgabe 8.

10. Schreiben Sie eine PYTHON-Funktion `checkISBN(digits)` welche bei Eingabe einer ISBN-Nummer als String (z.B. `"148421177"`) die Prüfziffer berechnet und zurückgibt. Hinweis: iterieren Sie durch jede Ziffer des Strings und konvertieren Sie diese mit `int(digit)` in einen Integer.

11. Zeigen Sie, dass das Prüfverfahren für ISBN-Nummern eine fehlerhafte Eingabe einer einzelnen Ziffer findet. (Hinweis: Gehen Sie gleich vor wie beim Beweis für das Vertauschen zweier Ziffern in der Vorlesung.)

Mögliche Theoriefragen:

- Was ist der größte gemeinsame Teiler zweier Zahlen?
- Beschreiben Sie den euklidischen Algorithmus.
- Was ist der erweiterte euklidische Algorithmus?
- Was ist das multiplikativ Inverse in einem Restklassenring?
- Was muss erfüllt sein, damit eine Zahl in einem Restklassenring ein multiplikatives Inverses hat?
- Was ist ein endlicher Körper? Warum existiert in einem endlichen Körper für jede Zahl ein multiplikatives Inverses?
- Warum sind endliche Körper für uns als Informatiker*innen so wichtig?