

Datensicherheit und Kryptografie

1. Übung

Abgabe: Lösen Sie Aufgabe 3. Ihre Lösungen geben Sie bitte entweder

- bis zum 20.04.2022 um 20:00 Uhr per Mail
an `julian.pape-lange@informatik.tu-chemnitz.de`
mit *Betreff:* TI1 Hausaufgaben,
- nach der Vorlesung am 19.04.2022 oder
- bis zum 20.04.2022 um 20:00 Uhr im Briefkasten der Professur Theoretische Informatik (vor Raum A10.266.4)

ab.

1. Aufgabe:

Zeigen Sie, dass die Grundrechenarten $+$, $-$ und \cdot modulo M aus den entsprechenden Grundrechenarten aus den ganzen Zahlen folgen.

Also dass für $a \equiv c \pmod{M}$ und $b \equiv d \pmod{M}$ die folgenden Gleichungen folgen:

- $a + b \equiv c + d \pmod{M}$
- $a - b \equiv c - d \pmod{M}$
- $a \cdot b \equiv c \cdot d \pmod{M}$

2. Aufgabe:

Folgen Sie aus Aufgabe 1, dass die üblichen Kommutativgesetze, Assoziativgesetze und Distributivgesetze auch modulo M gelten.

Zeigen Sie auch dass in allen Restklassen a die beiden Gleichungen $a + 0 \equiv a \pmod{M}$ und $a \cdot 1 \equiv a \pmod{M}$ gelten.

3. Aufgabe: (3+4+3)P

- In Aufgabe 1 haben Sie gesehen, dass $+$, $-$ und \cdot modulo M aus den ganzen Zahlen folgen. Zeigen Sie, dass das für Potenzen nicht gilt. Finden Sie Zahlen a, b, c, d, M mit $a \equiv c \pmod{M}$ und $b \equiv d \pmod{M}$ aber $a^b \not\equiv c^d \pmod{M}$.
- In den ganzen Zahlen hat jede Zahl ungleich 0 entweder keine (Quadrat-)Wurzeln oder genau 2 Wurzeln (\sqrt{n} und $-\sqrt{n}$). Bei Restklassen kann es mehr Wurzeln geben. Finden Sie alle vier Restklassen r mit $r^2 \equiv 1 \pmod{15}$.
- Sei $V = 5$ und $M = 11$. Finden Sie E mit $E \cdot V \equiv 1 \pmod{M}$.

4. Aufgabe:

In der Vorlesung haben wir gesehen, dass wir Buchstaben Restklassen modulo 26 mit $\cdot 3$ verschlüsseln und dann mit $\cdot 9$ wieder entschlüsseln können.

Betrachten Sie die beiden Verschlüsselungen $\cdot 4$ und $\cdot 5$ modulo 25 und finden Sie, wenn möglich, die Schlüssel zum Entschlüsseln.

5. Aufgabe:

Seien $a = 11011100$ und $b = 110$ zwei Binärzahlen. Bestimmen Sie den Bruch $\frac{a}{b}$ und den Rest der Division

- (a) mit binärer Suche und einem Multiplikationsalgorithmus Ihrer Wahl und
- (b) mit der Schulmethode zur Division.

Geben Sie zu beiden Algorithmen die Laufzeitkomplexität an.