MSG-Zirkel 9b | 13. März 2025

Kongruenzen in Verschlüsselungen

1. Der Diffie-Hellman-Algorithmus

Der *Diffie-Hellman-Algorithmus* zum Austauschen eines Schlüssels zwischen Alice und Bob funktioniert so:

1. Alice und Bob einigen sich öffentlich auf eine Primzahl p und eine natürliche Zahl $g < p$.
2. Alice wählt eine geheime natürliche Zahl $a < p$ und veröffentlicht $A := \text{Rest}(g^a : p)$. Bob wählt eine geheime natürliche Zahl $b < p$ und veröffentlicht $B := \text{Rest}(g^b : p)$.
3. Alice berechnet $K_1 := \text{Rest}(B^a : p)$ und Bob berechnet $K_2 := \text{Rest}(A^b : p)$.

Es ist zu zeigen, dass Alice und Bob dieselbe Zahl erhalten.

Die Modulo-Funktion

Durch die Division einer Zahl $a \in \mathbb{N}$ durch $m \in \mathbb{N}$ mit Rest erhält man eine Zahl $k \in \mathbb{N}$ und einen Rest $r \in \mathbb{N}$ mit

$$a = k \cdot m + r.$$

Die *Modulo-Funktion* $\mod m$ ordnet der Zahl a ihren Rest r bei der Division durch m zu. Wir schreiben dann

$$a \mod m = r.$$

(a) Sei $a \in \mathbb{N}$ und $m \in \mathbb{N}$ mit $a \mod m = r$, d. h. es existieren $k \in \mathbb{N}$ und $r \in \mathbb{N}$ mit $a = k \cdot m + r$. Begründe, dass dann auch

$$a + m \mod m = r \quad \text{bzw. allgemein} \quad a + l \cdot m \mod m = r$$

für alle ganzen Zahlen l gilt.

(b) Sei $a \mod m = r_1$ mit $a = k \cdot m + r_1$ für ein $k \in \mathbb{Z}$ und $b \mod m = r_2$ mit $b = l \cdot m + r_2$ für ein $l \in \mathbb{Z}$. Welche der folgenden Gleichungen sind korrekt? Gib Gegenbeispiele für die falschen an und beweise die korrekten.

(i) $(a \mod m) + (b \mod m) = (a + b) \mod m$

(ii) $[(a \mod m) + (b \mod m)] \mod m = (a + b) \mod m$

(iii) $(a \mod m) \cdot (b \mod m) = (a \cdot b) \mod m$

(iv) $[(a \mod m) \cdot (b \mod m)] \mod m = (a \cdot b) \mod m$

(c) Drücke K_1 und K_2 mithilfe der Modulo-Schreibweise aus und beweise, dass tatsächlich $K_1 = K_2$ gilt.

2. Modulo-Rechnung für Einsteiger

(a) Löse die folgenden drei Aufgaben:

(i) Welcher Wochentag ist in 142 Tagen?

(ii) Klaras Bus fährt immer zur vollen Stunde direkt vor ihrer Haustür. Im Moment ist es Viertel nach. Wie lange wird sie auf ihren Bus warten müssen, wenn sie zuerst noch eine DVD anschaut, die 202 Minuten dauert?

(iii) Um 14 Uhr sollte der Zug abfahren. Leider hat der Zug eintausend Stunden Verspätung. Wie viel Uhr wird es sein, wenn der Zug kommt?

Hinter solchen alltäglichen Rechnungen steckt ein mathematisches Konzept:

Kongruenz

Wenn zwei Zahlen $a, b \in \mathbb{N}$ bei der Division durch $m \in \mathbb{N}$ denselben Rest lassen, d. h. wenn es $k, l, r \in \mathbb{N}$ gibt mit

$$a = k \cdot m + r \quad \text{und} \quad b = l \cdot m + r,$$

gilt in der Modulo-Schreibweise

$$a \mod m = b \mod m = r.$$

In diesem Fall heißen a und b *kongruent modulo* m und wir schreiben

$$a \equiv b \mod m.$$

Beispielsweise ist $142 \equiv 2 \mod 7$, denn es gilt $142 = 20 \cdot 7 + 2$ und $2 = 0 \cdot 7 + 2$.

Damit können wir Aufgabe (i) geschickt lösen. Heute ist ein Donnerstag, also der 4. Tag der Woche. Es gilt nun

$$4 + 142 = 146 \equiv 6 \mod 7.$$

In 142 Tagen ist also der 6. Wochentag: ein Samstag.

(b) Löse die anderen Aufgaben aus (a) auch noch einmal mit der Modulo-Technik.

(c) Diskutiere mit deinen Nachbarn:

(i) Es gilt $7 \equiv 2 \mod 5$ und $12 \equiv 2 \mod 5$. Wieso folgt daraus *nicht* $7 = 12$?

(ii) Für jede natürliche Zahl a gilt entweder $a \equiv 0 \mod 2$ oder $a \equiv 1 \mod 2$. Warum?

(iii) Gibt es eine natürliche Zahl n mit $n \equiv 1 \mod 5$ und $n \equiv 2 \mod 2025$?

3. Modulo-Rechnung für Fortgeschrittene

Es gibt ein wichtiges Kriterium, mit dem sich die Kongruenz zweier Zahlen überprüfen lässt:

Differenzkriterium:

Zwei ganze Zahlen a und b sind kongruent modulo $m \in \mathbb{N}$ genau dann, wenn $a - b$ durch m teilbar ist.

Beispiel: Es gilt $142 \equiv 2 \mod 7$, denn $142 - 2 = 140$ ist durch 7 teilbar.

(a)* Beweise mithilfe des Differenzkriteriums: Sind $a, b, c, d \in \mathbb{N}$ und $m \in \mathbb{N}$ mit $a \equiv b \mod m$ und $c \equiv d \mod m$, so gilt:

(A) $a + c \equiv b + d \mod m$

(M) $ac \equiv bd \mod m$

(b) Welchen Rest lässt 102^{37} bei der Division durch 5?
*Tipp: Nutze die Aussage **(M)** aus (a).*