MSG-Zirkel 9b

RSA I: Modulares Invertieren

1. Teiler und Teilbarkeit

Seien a und t ganze Zahlen. Man sagt, t *teilt* a, in Zeichen $t \mid a$, wenn es eine Zahl $k \in \mathbb{Z}$ gibt, sodass $a = k \cdot t$. Wir nennen t dann einen *Teiler* von a.

(a) Seien $a, b, t \in \mathbb{Z}$. Beweise mithilfe der Definition:

(i) $t \mid a \quad \text{und} \quad t \mid b \quad \Rightarrow \quad t \mid (a + b)$

(ii) $t \mid a \quad \text{und} \quad t \mid b \quad \Rightarrow \quad t \mid (a - b)$

(b) Nutze die Rechenregeln aus (a), um zu beweisen:
Jeder gemeinsamen Teiler von a und b ist auch ein gemeinsamen Teiler von $a - b$ und b und umgekehrt.

2. Der euklidische Algorithmus

> *„Nimmt man abwechselnd immer das Kleinere vom Größeren weg, dann muss der Rest schließlich alle vorhergehenden Größe messen.“*
>
> – Euklid, Die Elemente, Zehntes Buch §3

(a) Führe diese Methode zeichnerisch und rechnerisch für zwei Strecken mit den Längen 22 und 16 durch. Was meint Euklid mit „messen“?

Der **euklidische Algorithmus** führt in jedem Schritt eine Division mit Rest aus, um den größten gemeinsamen Teiler zweier Zahlen a und b (hier: $a \geq b$) zu finden. Im ersten Schritt dividieren wir a durch b und erhalten das Ergebnis q_1 mit Rest r_1:

$$a = q_1 \cdot b + r_1$$

In jedem weiteren Schritt wird mit dem Divisor und dem Rest des vorhergehenden Schritts eine erneute Division mit Rest durchgeführt, und zwar so lange, bis eine Division aufgeht, d. h. der Rest Null ist.

$$\begin{aligned} b &= q_2 \cdot r_1 + r_2 \\ r_1 &= q_3 \cdot r_2 + r_3 \\ r_2 &= q_4 \cdot r_3 + r_4 \\ &\vdots \\ r_{n-1} &= q_{n+1} \cdot r_n + 0 \end{aligned}$$

Der Divisor der letzten Division ist der *größte gemeinsame Teiler* $\mathrm{ggT}(a, b) = r_n$.

(b) Bestimme mithilfe des euklidischen Algorithmus $\mathrm{ggT}(15, 99)$ und $\mathrm{ggT}(972, 864, 189)$.

(c)* Erkläre mithilfe von 1 (b), *warum* der euklidische Algorithmus am Ende den größten gemeinsamen Teiler zweier Zahlen liefert.

3. Modulares Invertieren

„Zu jeder Zahl $x \in \mathbb{R}$ gibt es eine (multiplikativ) *inverse* Zahl $x^{-1} \in \mathbb{R}$ mit $x \cdot x^{-1} = 1$.“

(a) Überprüfe die Aussage. Wie sehen diese inversen Zahlen aus? Sind sie eindeutig? Gibt es Ausnahmen?

Modulares Inverses

Zu einer Zahl $a \in \mathbb{N}$ ist $b \in \mathbb{N}$ ein *modulares Inverses modulo* n, wenn gilt:

$$a \cdot b \equiv 1 \mod m.$$

(b) Gib zu $a = 7$ ein modulares Inverses b modulo 10 an. Gibt es weitere?

Wenn a und m teilerfremd sind, d. h. wenn $\mathrm{ggT}(a, m) = 1$ gilt, lässt sich ein modulares Inverses zu a modulo m leicht berechnen.

Beispiel: Für $a = 20$ ist ein modulares Inverses modulo $m = 31$ gesucht. Der euklidische Algorithmus liefert

$$\begin{aligned} 31 &= 1 \cdot 20 + 11 \\ 20 &= 1 \cdot 11 + 9 \\ 11 &= 1 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Der letzte echte Rest ist der größte gemeinsame Teiler $\mathrm{ggT}(31, 20) = 1$.

(c) Stelle den größten gemeinsamen Teiler $\mathrm{ggT}(31, 20) = 1$ als Produktsumme der Anfangszahlen $a = 31$ und $m = 20$ dar, also bestimme ganze Zahlen t und s mit

$$t \cdot 31 + s \cdot 20 = 1.$$

Stelle dafür die Gleichungen des euklidischen Algorithmus jeweils nach dem Rest um und setze die Ergebnisse geschickt ineinander ein.
Hinweis: Dieses Verfahren wird erweiterter euklidischer Algorithmus genannt.

(d) Erkläre, wie das Ergebnis aus (c) nun ein modulares Inverses für $a = 20$ modulo $m = 31$ liefert.

(e) Bestimme mithilfe des erweiterten euklidischen Algorithmus ein Inverses zu

(i) $17 \mod 101$,

(ii) $31 \mod 141$.
Hinweis: Das modulare Inverse ist eine positive ganze Zahl.