# Kryptologie
## Übungsblatt 2

### Aufgabe 2.1

Seien $x$ und $y$ natürliche Zahlen mit Bitlänge $m$ und $n$ mit $m \geq n$. Sei $k = \lceil \log_2(q) \rceil$ die Bitlänge des Quotienten $q$ der Division von $x$ durch $y$.
Zeige: Die Laufzeit der Division von $x$ durch $y$ mit Rest beträgt $\mathcal{O}(kn)$.

### Aufgabe 2.2

Berechnen Sie das Inverse von 47 modulo 263 mit dem erweiterten Euklidischen Algorithmus. Geben Sie wie in der Vorlesung alle Zwischenergebnisse an.

### Aufgabe 2.3

Geben Sie die Multiplikationstabelle für $\mathbb{Z}_{14}^*$ an und bestimmen Sie für jedes $x \in \mathbb{Z}_{14}^*$ das Inverse.
Geben Sie die Ordnung von 3 und 11 in $\mathbb{Z}_{14}^*$ an. Was können Sie über die Ordnung der anderen Elemente sagen, ohne diese explizit zu berechnen?

### Aufgabe 2.4

Neun Piraten haben einen Schatz von Goldmünzen erobert. Es sind weniger als 500 Münzen. Da die Piraten nicht rechnen bzw. zählen können, verteilen sie den Schatz Münze für Münze reihum. Es geht leider nicht auf: 4 Münzen bleiben übrig. Darüber geraten sie so in Streit, dass am Ende einer der Piraten sein Leben verliert. Nun wird diesmal erneut der Schatz Münze für Münze zwischen 8 Piraten aufgeteilt. Erneut bleiben diesmal 3 Münzen übrig. Erneuter Streit endet mit 7 überlebenden Piraten. Beim diesmaligen Aufteilungsvorgang geht es auf. Jeder Pirat erhät 1/7 des Goldschatzes.
Wie viele Münzen sind es?

### Aufgabe 2.5

Die Zahlen $n_1 = 5$ und $n_2 = 8$ sind teilerfremd. Der Chinesische Restsatz liefert eine bijektive Abbildung zwischen $\mathbb{Z}_5 \times \mathbb{Z}_8$ und $\mathbb{Z}_{40}$. Ermitteln Sie daraus eine Bijektion zwischen $\mathbb{Z}_5^* \times \mathbb{Z}_8^*$ und $\mathbb{Z}_{40}^*$, die Sie in einer passend gewählten Tabelle angeben.

### Aufgabe 2.6

(a) Berechnen Sie $\varphi\left(2^5 \cdot 3^2 \cdot 5^4 \cdot 11^3 \cdot 17\right)$.

(b) Sei $n \in \mathbb{N}$ mit $n > 2$. Zeigen Sie, dass $\varphi(n)$ gerade ist.

(c) Berechnen Sie $27^{101} \mod 101$.

## Aufgabe 2.7

Wir betrachten die rekursive Formulierung des Euklidischen Algorithmus aus der Vorlesung mit Eingaben $(a, b)$, wobei wir $a > b \geq 0$ voraussetzen. Es sei

$$H_k := \{(a, b) | \, \text{ggT}(a, b) \text{ benötigt } k \text{ Modulo-Rechnungen}\}$$

Es seien $F_0 := 0$, $F_1 := 1$, $F_{k+2} := F_k + F_{k+1}$ (für $k \in \mathbb{N}_0$) die *Fibonacci-Zahlen*. Beweisen Sie:
Für $k \geq 1$ ist $(F_{k+2}, F_{k+1})$ die kleinste Eingabe aus $H_k$; genauer sollten Sie dafür folgende Punkte zeigen:

- $(F_{k+2}, F_{k+1}) \in H_k$,
- $F_{k+2} = \min\{a \in \mathbb{N} | \exists b < a : (a, b) \in H_k\}$ und
- $F_{k+1} = \min\{b \in \mathbb{N} | \exists a > b : (a, b) \in H_k\}$.