Hochschule RheinMain
Fachbereich Design Informatik Medien
Studiengang Angewandte Informatik / Informatik Technische Systeme
Prof. Dr. Bernhard Geib

Security

Sommersemester 2022
(LV 4120 und 7240)

5. Aufgabenblatt

Ganze Zahlen spielen eine fundamentale Rolle in der angewandten Kryptologie. Daher stellen wir in dieser Übungsserie grundlegende Eigenschaften der ganzen Zahlen heraus, die wir anschließend nutzen, um grundlegende kryptographische Basisalgorithmen effizient formulieren zu können. Ferner lösen wir Kongruenzgleichungen und beschäftigen uns mit einer Anwendung der Eulerschen Phi-Funktion.

Aufgabe 5.1

Es sei g := ggT(a, b) der größte gemeinsame Teiler der Zahlen a und b. Eine Vielfachsummendarstellung von g bei bekannten a und b ist gegeben durch die Form:

$$g = x \cdot a + y \cdot b$$

a) Ermitteln Sie zunächst mit Hilfe des Euklidischen Algorithmus den größten gemeinsamen Teiler der Zahlen a = 792 und b = 75.

b) Berechnen Sie anschließend durch sukzessives Einsetzen der Euklidischen Gleichungskette die ganzen Zahlen x und y mit der Eigenschaft:

$$ggT(792, 75) = 792 \cdot x + 75 \cdot y$$

Aufgabe 5.2

Es seien $a \in \mathbf{N}$ (Menge der natürlichen Zahlen) sowie $p, q \in \mathbf{P}$ (Primzahlen). Die Zahl a sei ferner kongruent 1 modulo p und kongruent 0 modulo q, d. h.

$$a \equiv 1 \pmod 5 \quad \text{und} \quad a \equiv 0 \pmod{17}$$

Wie lautet die Zahl a? (Bitte den Berechnungsweg vollständig angeben!)

Aufgabe 5.3

a) Berechnen Sie mit Hilfe eines Taschenrechners die Zahl $z = 257^{887} \bmod 31$.

b) Berechnen Sie die modulare Inverse der Zahl 15 im Ring $\mathbf{Z}_{1276}$!

Formal: $15^{-1} \bmod 1276 = ?$

Aufgabe 5.4

Bezüglich der Zahl 53461 seien zwei Dinge bekannt geworden:

i) Die Zahl 53461 ist das Produkt von genau zwei Primzahlen.

ii) $\phi(53461) = 52992$, wobei ϕ die Eulersche ϕ-Funktion bezeichne.

a) Können Sie mit Hilfe dieser Informationen die Zahl 53461 faktorisieren? Wenn ja, wie lauten die Primfaktoren?

b) Welche Konsequenzen hätte die Möglichkeit einer solchen Faktorisierung im Hinblick auf die Erzeugung kryptographischer Schlüssel?