Hochschule RheinMain

Ü B U N G E N

zur Veranstaltung ***Quantencomputing*** im Studiengang Angewandte Informatik

No. 6 Martin Rehberg

Präsenzaufgaben

Aufgabe 1: Bestimmen Sie $ggT(4081, 2585)$ und stellen Sie diesen anschließend als Linearkombination von 4081 und 2585 dar.

Aufgabe 2: Wir sagen eine ganze Zahl a *teilt* eine ganze Zahl b (in Zeichen $a|b$), wenn eine ganze Zahl c mit $ac = b$ existiert. Zeigen Sie

(i) Aus $a|b$ und $a|c$ folgt $a|(b + c)$ für ganze Zahlen a, b, c.

(ii) Aus $a|b$ folgt $a|bc$ für ganze Zahlen a, b, c.

Aufgabe 3: Zeigen Sie (unter Verwendung von Aufgabe 2): Es gilt $ggT(a + cb, b) = ggT(a, b)$ für ganze Zahlen a, b, c.

Übungsaufgaben

Aufgabe 1: Die *Eulersche φ-Funktion* ist definiert als $\varphi(n) = \#\{1 \leq k \leq n : ggT(k, n) = 1\}$. Zeigen Sie

(i) $\varphi(p) = p - 1$ gilt genau dann, wenn p eine Primzahl ist. Allgemein gilt $\varphi(n) \leq n - 1$ für $n > 1$.

(ii) $\varphi(p^r) = p^r - p^{r-1}$ für eine Primzahlpotenz p^r.

(iii) $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$, wobei das Produkt über alle Primteiler von n gebildet wird.
Hinweis: Verwenden Sie den *Hauptsatz der Elementaren Zahlentheorie* in Kombination damit, dass die φ-Funktion *multiplikativ* ist, d.h. $\varphi(n_1 ... n_k) = \varphi(n_1) ... \varphi(n_k)$ für paarweise teilerfremde $n_1, ..., n_k$.

Aufgabe 2 (RSA): Gegeben $p = 61, q = 97$ und $e = 47$. Verschlüsseln Sie die Nachricht $m = 348$ mit dem RSA-Verfahren.