Übungen zur Kryptologie

Blatt 7 SoS 2024 — H. Kiechle

Präsenzaufgaben

φ bezeichne die Eulersch Phi-Funktion.

20. In der Vorlesung wurde behauptet, dass $\varphi(pq) = (p-1)(q-1)$, wenn p, q verschiedene Primzahlen sind.

(a) Beweisen Sie diese Aussage.

(b) Was kommt heraus, wenn $p = q$?

Hausaufgaben

21. Bestimmen Sie $\varphi(p^2q)$, für verschiedene Primzahlen p, q. Gehen Sie direkt vor, wie bei den Beispielen in der Vorlesung; benutzen Sie insbesondere keine unbewiesenen Aussagen über φ.

22. Es sei $n = pq$, $p \neq q$, mit Primzahlen p und q.

(a) Zeigen Sie, dass p und q die Nullstellen des Polynoms $f(x) = x^2 - (n - \varphi(n) + 1)x + n$ sind.

(b) Es gelte $n = 166213$ und $\varphi(n) = 165388$. Bestimmen Sie p und q ohne n zu faktorisieren.

(c) Zählen Sie die Anzahl der Rechenoperationen, die Sie dafür durchführen mussten.