RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Enrico Thomae, Philipp Wagner, Vera Knüppels

Präsenzübungen zur Vorlesung

Zahlentheorie

Sommersemester 2012

Blatt 3

AUFGABE 1:
Zeigen Sie, dass $\mathrm{ggT}(a_0, a_1)$ in $\mathbb{Z}$ in der Zeit $\mathcal{O}(\log^3 a_0)$ mit Hilfe des euklidischen Algorithmus berechnet werden kann.

AUFGABE 2:
Berechnen Sie in $\mathbb{Z}[i]$ den $\mathrm{ggT}(a, b)$ für

a) $a = 208 + i, b = 509$,

b) $a = 1 + 3i, b = 5i - 1$.

AUFGABE 3:
Seien $a = 47 + 17\sqrt{3}$ und $b = 36 + 16\sqrt{3}$ aus $\mathbb{Z}[\sqrt{3}]$ gegeben. Bestimmen Sie $z := \mathrm{ggT}(a, b)$ in $\mathbb{Z}[\sqrt{3}]$ und geben Sie eine Linearkombination $z = ua + vb$ an. Benutzen Sie hierbei, dass $\mathbb{Z}[\sqrt{3}]$ euklidisch ist mit der Normfunktion $N(x + y\sqrt{3}) = |x^2 - 3y^2|$.

AUFGABE 4:
Berechnen Sie 123^{-1} mod 4567 mit Hilfe des erweiterten Euklidischen Algorithmus.