RUHR UNIVERSITÄT BOCHUM

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

Präsenzübungen zur Vorlesung

Zahlentheorie

Sommersemester 2012

Blatt 1

AUFGABE 1:
Beweisen Sie $n + \log n = \Theta(n)$.

FRAGE 2:
Warum ist die Teilbarkeitslehre in Körpern trivial?

AUFGABE 3:
Sei R ein Integritätsbereich und $a, b, b_1, b_2, d, d_1, d_2 \in R$. Beweisen Sie folgende Aussagen.

(a) $a \,|\, b \Rightarrow a \,|\, db$

(b) $a \,|\, b_1$ und $a \,|\, b_2 \Rightarrow a \,|\, (d_1 b_1 + d_2 b_2)$

(c) $a \,|\, b \Rightarrow da \,|\, db$

(d) $a \,|\, b$ und $b \,|\, d \Rightarrow a \,|\, d$

(e) $a \,|\, b$ und $b \,|\, a \Leftrightarrow a, b$ sind assoziiert.

AUFGABE 4:
Zeigen Sie: Ist $n \geq 1$, so sind die Zahlen $(n+1)! + k$ mit $2 \leq k \leq n+1$ alle keine Primzahlen. Es gibt also beliebig große Lücken in den Primzahlen.

AUFGABE 5:
Zeigen Sie, dass der Polynomring $\mathbb{F}[X]$ über einem Körper $\mathbb{F}$ euklidisch ist.

AUFGABE 6:
Zeigen sie mit Hilfe der Normfunktion $N(\cdot)$, das für die Einheiten der Gaußschen Zahlen gilt

$$\mathbb{Z}[i]^* = \{\pm 1, \pm i\}.$$