RUHR UNIVERSITÄT BOCHUM

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Hausübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 1 / 5. April 2013 / Abgabe bis spätestens 15. April 2013, 12:00 Uhr in dem Kasten auf NA 02 oder am Anfang der Vorlesung

Geben Sie bitte die Aufgaben zur Vereinfachung der Korrektur folgendermassen nach Aufgaben getrennt ab:

- Aufgaben 1 und 4 in Kasten A
- Aufgaben 2 und 3 in Kasten B
- Aufgaben 5 und 6 in Kasten C

Die Kästen auf NA 02 sind entsprechend beschriftet. Wenn Sie in der Vorlesung abgeben, machen sie einfach 3 getrennte Stapel. Schreiben Sie auf alle 3 Abgaben jeweils Ihre(n) Namen und/oder Matrikelnummer(n). Falls Sie diese Bitte zu spät lesen, ignorieren Sie sie.

AUFGABE 1 (2 Punkte)**:**
Seien $A \in \mathbb{R}_{>0}$ und $B \in \mathbb{R}$ beliebig. Betrachten Sie die Funktion $f : \mathbb{N} \to \mathbb{R}$, $f(n) = An + B$. Zeigen Sie, dass $f(n) = \Theta(n)$.

AUFGABE 2 (2 Punkte)**:**
Sei $\varepsilon > 0$ beliebig. Zeigen Sie, dass $\log_2(n) = \mathcal{O}(n^\varepsilon)$.

AUFGABE 3 (4 Punkte)**:**
Seien $f, g, h, f_1, f_2, g_2, g_2 : \mathbb{N} \to \mathbb{N}$ Funktionen. Zeigen Sie:

(a) Wenn $f_1 = \mathcal{O}(g_1)$ und $f_2 = \mathcal{O}(g_2)$ ist, so ist auch $f_1 \cdot f_2 = \mathcal{O}(g_1 \cdot g_2)$.

(b) Wenn $f = \mathcal{O}(g)$ und $g = \mathcal{O}(h)$ gilt, so gilt auch $f = \mathcal{O}(h)$.

(c) Es gilt stets $(f + g)(n) = \Theta(\max\{f(n), g(n)\})$.

AUFGABE 4 (4 Punkte)**:**
Für $n \geq 0$ sei $F_n = 2^{(2^n)} + 1$ die n-te Fermatzahl. Zeigen Sie:

(a) $F_n = 2 + \Pi_{i=0}^{n-1} F_i$.

(b) Wenn $k \mid F_i$ ein Teiler der i-ten Fermatzahl ist, so gilt $k \nmid F_j$ für alle $j > i$. (D.h. die Fermatzahlen sind teilerfremd.)

— bitte wenden —

AUFGABE 5 (4 Punkte)**:**
Sei R ein Integritätring und $a, b, b_1, b_2, d, d_1, d_2 \in R$ beliebig mit $d \neq 0$. Zeigen Sie:

(a) $a \mid b_1$ und $a \mid b_2 \implies a \mid b_1 d_1 + b_2 d_2$

(b) $a \mid b \Leftrightarrow ad \mid bd$

(c) $a \mid b$ und $b \mid a \Leftrightarrow a$ und b sind assoziiert.

AUFGABE 6 (4 Punkte)**:**
In dieser Aufgabe sei die Eindeutigkeit der Primfaktorzerlegung vorausgesetzt.
Für $n \in \mathbb{N}$ sei $f(n)$ die Anzahl der Primfaktoren von n, gezählt mit Vielfachheit.

n	1	2	3	4	5	6	7	8	9	10	11	12	...
$f(n)$	0	1	1	2	1	2	1	3	2	2	1	3	...

Zeigen Sie, dass $f(n) = \mathcal{O}(\log n)$ gilt.
Spiel die Basis des Logarithmus dabei eine Rolle?
Gilt auch $f(n) = \Theta(\log n)$?