RUHR
UNIVERSITÄT
BOCHUM

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

Hausübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 3 / 19. April 2013 / Abgabe bis spätestens 29. 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:

- Aufgabe 1 Kasten A
- Aufgaben 2,3 in Kasten B
- Aufgaben 4,5 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).

AUFGABE 1 (3 Punkte)**:**
Berechnen Sie mit Hilfe des Erweiterten Euklidischen Algorithmus
$d = \mathrm{ggT}(2X^3 - 2, 3X^3 + 3X^2 - 3X - 3)$ über $\mathbb{Q}[X]$ sowie Bezout-Koeffizienten $f, g \in \mathbb{Q}[X]$ mit $f \cdot (2X^3 - 2) + g \cdot (3X^3 + 3X^2 - 3X - 3) = d$.

AUFGABE 2 (3 Punkte)**:**
Sei R faktorieller Ring, bei dem jedes Ideal in R endlich erzeugt ist.
Weiterhin sollen für beliebige $a, b \in R$, nicht beide 0, stets $x, y \in R$ existieren mit $ax + by = \mathrm{ggT}(a, b)$ (bis auf Assoziiertheit).
Zeigen Sie, dass R ein Hauptidealring ist.

— bitte wenden —

AUFGABE 3 (5 Punkte)**:**
Es seien F_n die Fibnoacci-Zahlen mit $F_0 = 0, F_1 = 1$ und $F_n = F_{n-1} + F_{n-2}$ für $n \geq 2$.

n	0	1	2	3	4	5	6	7	8	9	10	11	...
F_n	0	1	1	2	3	5	8	13	21	34	55	89	...

(a) Berechnen Sie x, y mit $xF_5 + yF_4 = \mathrm{ggT}(F_5, F_4)$ mit dem erweiterten Euklidischen Algorithmus.

(b) Zeigen Sie allgemein, dass der Erweiterte Euklidische Algorithmus, angewendet auf $\mathrm{ggT}(F_{n+1}, F_n) = 1$ mit $n \geq 2$ als Bezout-Koeffizienten

$$1 = (-1)^{n+1} F_{n-2} F_{n+1} + (-1)^n F_{n-1} F_n$$

liefert. D.h. die Bezout-Koeffizienten sind $x = (-1)^{n+1} F_{n-2}$ und $y = (-1)^n F_{n-1}$

Bemerkung: $\mathrm{ggT}(F_{n+1}, F_n) = 1$ wurde in der Präsenzübung gezeigt und darf vorausgesetzt werden. Um Teil (b) zu zeigen, sollte man in (a) (oder notfalls durch Berechnen von $\mathrm{ggT}(F_n, F_{n+1})$ für andere konkrete Werte von n) Gesetzmässigkeiten für die auftretenden a_i, q_i, x_i und y_i (in der Notation der Vorlesung) sehen, die sich per Induktion leicht zeigen lassen.

AUFGABE 4 (4 Punkte)**:**
Wir betrachten den Ring $R = \mathbb{Z}[i]$ und die Normfunktion $N : R \to \mathbb{Z}$ mit $N(z) = z\overline{z}$.

(a) Zeigen Sie: Sind $a, b \in \mathbb{Z}[i]$, wobei $N(a), N(b)$ teilerfremd (in $\mathbb{Z}$) sind, so sind a, b teilerfremd (in $\mathbb{Z}[i]$).

(b) Geben Sie $a, b \in \mathbb{Z}[i]$ an mit a, b teilerfremd in $\mathbb{Z}[i]$, für die $N(a), N(b)$ *nicht* teilerfremd in $\mathbb{Z}$ sind.

AUFGABE 5 (5 Punkte)**:**
Sei $p \neq 2, 5$ eine Primzahl und $a > 0$ eine ganze Zahl. Wir betrachten die Dezimaldarstellung $a = \sum_i 10^i a_i$ und schreiben die Zahl im Dezimalsystem als $a = a_k a_{k-1} \ldots a_0$ für Ziffern $a_i \in \{0, \ldots, 9\}$. Wir fassen die Ziffern in Blöcken b_j von je $p-1$ Ziffern zusammen, wobei wir ggf. mit führenden 0en ergänzen, s.d. $p - 1 \mid k + 1$:

$$a = \underbrace{a_k \ldots a_{k-p+2}}_{b_{\frac{k+1}{p-1}-1}} \ldots \underbrace{a_{2p-1} a_{2p-2} \ldots a_{p-1}}_{b_1} \underbrace{a_{p-2} \ldots a_1 a_0}_{b_0}.$$

Wir interpretieren die b_j's als $p - 1$ stellige Dezimalzahlen und betrachten $b = \sum_j b_j$.
Zeigen Sie: $p \mid a$ genau dann wenn $p \mid b$.