RUHR UNIVERSITÄT BOCHUM

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

Präsenzübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 3 / 22.–24. April 2013

AUFGABE 1:
Berechnen Sie $d = \text{ggT}(58, 17)$ mit Hilfe des Erweiterten Euklischen Algorithmus und geben sie Bezout-Koeffizienten x, y mit $d = 58x + 17y$ an.

AUFGABE 2:
Wir betrachten die Fibonacci-Zahlen F_i, gegeben durch die Rekursionsgleichung
$F_1 := 1, F_2 := 2$ und $F_n := F_{n-1} + F_{n-2}$ für $n \geq 3$.
D.h. $F_1 = 1, F_2 = 2, F_3 = 3, F_4 = 5, F_5 = 8, F_6 = 13, F_7 = 21, F_9 = 34, F_{10} = 55 \ldots$.
Zeigen Sie, dass für alle n gilt: $\text{ggT}(F_n, F_{n+1}) = 1$.

Bemerkung: In der Literatur (und Hausübung) betrachten man die Folge meist mit leicht verschobenen Indizes. Die Wahl hier ist für Aufgabe 3 optimiert. Man kann zeigen, dass $F_n = \Theta(\phi^n)$ gilt, wobei $\phi = \frac{1+\sqrt{5}}{2}$ der goldene Schnitt ist. Insbesondere wächst F_n exponentiell.

AUFGABE 3:
Seien $a_0 > a_1 > 0$ ganze Zahlen. Wir betrachten a_i und q_i, gegeben durch den Euklidischen Algorithmus wie in der Vorlesung:

$$a_{i-2} = q_{i-1}a_{i-1} + a_i$$

für $a_i \geq 2$ und $0 \leq a_i < a_{i-1}$, solange $a_{i-1} \neq 0$.
Sei k so, dass $a_k = 0$ ist (d.h. der Euklische Algorithmus berechnet dann $k - 1$ Divisionen mit Rest).
Zeigen Sie, dass für $a_0 < F_n$ stets $k < n$ gilt.

Hinweis: Rechnen Sie den euklidischen Algorithmus „rückwärts“. Zeigen Sie, dass $a_i \geq F_{k-i}$ gilt und somit $a_0 \geq F_k$.
Was folgt hieraus für die Laufzeit des euklidischen Algorithmus?

AUFGABE 4:

- Gilt $\mathrm{kgv}(a,b,c) \cdot \mathrm{ggT}(a,b,c) = abc$ für $a,b,c \in \mathbb{N}$?
- Geben Sie $a,b,c \in \mathbb{Z}$ an mit $\mathrm{ggT}(a,b,c) = 1$,
  aber $\mathrm{ggT}(a,b) \neq 1, \mathrm{ggT}(a,c) \neq 1, \mathrm{ggT}(b,c) \neq 1$.

Dabei seien alle ggT's stets ≥ 0 gewählt.

AUFGABE 5:
Berechnen Sie $d = \mathrm{ggT}(7-11i, 4-7i)$ in $\mathbb{Z}[i]$ sowie Bezout-Koeffizienten mit Hilfe des Erweiterten Euklidischen Algorithmus.

AUFGABE 6:
Überlegen Sie sich, warum der Euklidische Algorithmus in $\mathbb{Z}[i]$ mit Bewertungsfunktion $N(z) = z\overline{z}$ bei Eingabe a_0, a_1 mit $N(a_0) \geq N(a_1)$ höchstens $\mathcal{O}(\log N(a_0))$ Iterationen benötigt.