Übungen zur Vorlesung **Blatt 1**
Elliptische Kurven und Kryptographie 20.04.2015

PD Dr. K. Halupczok
Dipl.–Math. A. Juhas SoSe 2015

Abgabetermin: Montag, 27. April 2015, bis 12:15 Uhr in die Briefkästen

---

Aufgabe 1:

Lösen Sie die folgenden Kongruenzen–Systeme:

(a) $x \equiv 1 \bmod 2$, $x \equiv 1 \bmod 3$;

(b) $2x \equiv 1 \bmod 5$, $3x \equiv 1 \bmod 7$, $4x \equiv 1 \bmod 11$;

(c) $x \equiv 31 \bmod 41$, $x \equiv 59 \bmod 26$.

Aufgabe 2:

(a) Berechnen Sie $\mathrm{ggT}(4144, 7696)$ und finden Sie $x, y \in \mathbb{Z}$ mit $4144x + 7696y = 592$.

(b) Die Fibonacci–Zahlen F_n sind rekursiv definiert durch

$$F_0 := 0,\ F_1 := 1,\ F_n := F_{n-1} + F_{n-2},\ \text{für } n \geq 2$$

und man hat die explizite Formel

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

Zeigen Sie, dass der Eukl. Algorithmus bei Eingabe (a, b) mit $a \geq b$, $a, b \in \mathbb{N}$, eine Laufzeit von $O(\log(b + 1))$ Schritten besitzt.
Hinweis: Betrachten Sie den Fall, dass a, b zwei aufeinander folgende Fibonacci–Zahlen sind.

Aufgabe 3:

(a) Zeigen Sie $\mathrm{ggT}(a, a + n) \mid n$ für alle $a \in \mathbb{Z}$, $n \in \mathbb{N}$.

(b) Seien $a, b, c \in \mathbb{Z}$ mit $a^2 + b^2 \neq 0$, $\mathrm{ggT}(a, b) = 1$ und $c \mid (a + b)$. Zeigen oder widerlegen Sie $\mathrm{ggT}(a + b, ab) = 1$ und $\mathrm{ggT}(a, c) = \mathrm{ggT}(b, c) = 1$.

Aufgabe 4:

Zeigen Sie:

(a) $3^n + 3^m + 1$ ist keine Quadratzahl, wobei $n, m \in \mathbb{N}$.

(b) Seien $a, b, c \in \mathbb{Z}$ mit $7 \mid a^3 + b^3 + c^3$. Dann gilt $7 \mid abc$.