# Vorlesung „Kryptographie II“ (Sommersemester 2025)

# Übungsblatt 6 (30.5.2025)

**Aufgabe 26:** Katharina schickt an ihre Freundin Petra folgende ABC-verschlüsselte Nachricht:

```
FCVITSFKNUTNTGRIUVWFNALGLIPUJGNJTSFTGVKHVTFAGDEPGSEKDJGWFCMXJRFCBICRFPBFPSJCAVHT
JCUXGEJJWIDHUINLREPGMBTHEUEOVSFCLXFNJODDPTJEIFKNAUPWFHRFUEBGLFKAEMPUBOGHWCJFVTWR
```

Bei der im 1. Weltkrieg verwendeten ABC-Chiffrierung wird zuerst eine VIGENERE-Verschlüsselung mit dem Schlüsselwort ABC ausgeführt, anschließend folgt eine TRANSSPA-Verschlüsselung.
Worum geht es in der Nachricht?
(Hinweis: `FCNYGRAMNUYMRUA`)

**Aufgabe 27:** Gegeben seien $P, Q \in \mathbb{Z}$. Beweise folgende Formeln für die Lucas-Folgen, wobei $D = P^2 - 4Q$ und $U_i = U_i(P,Q)$, $V_i = V_i(P,Q)$ ist:

(1) $V_i = U_{i+1} - QU_{i-1}$ für $i \geq 1$.
(2) $DU_i = V_{i+1} - QV_{i-1}$ für $i \geq 1$.
(3) $2U_{i+j} = U_iV_j + U_jV_i$ für $i, j \geq 0$.
(4) $V_i^2 - DU_i^2 = 4Q^i$ für $i \geq 0$.

**Aufgabe 28:** Untersuche das Periodizitätsverhalten (Periodenlänge, explizite Periode) der Folge $(f_i \bmod n)_{i\geq 0}$, wobei $f_i = U_i(1,-1)$ die $i$-te Fibonacci-Zahl ist, in folgenden Fällen:

(1) $n = 8$. Warum gibt es keine Fibonacci-Zahl, in der 2 genau 2-mal aufgeht?
(2) $n = 26$. Bestimme die zugehörige Häufigkeitsverteilung der Zahlen $0, \ldots, 25$.

**Aufgabe 29:** Seien $P, Q \in \mathbb{Z}$ mit $P \neq 0$ und $D = P^2 - 4Q > 0$. Seien $\alpha$ und $\beta$ die Nullstellen des Polynoms $x^2 - Px + Q$ und o.E. $|\alpha| \geq |\beta|$. Zeige:

(1) Es gilt $|\alpha| > |\beta|$.
(2) Die Folge
$$\left(\frac{U_n(P,Q)}{\alpha^n}\right)_{n\geq 0}$$
konvergiert. (Was ist der Grenzwert?)
(3) Im Fall $(P,Q) \neq (\pm 1, 0)$ gilt
$$\lim_{n\to\infty} |U_n(P,Q)| = \infty.$$

**Aufgabe 30:**

(1) Berechne $U_{340}(1,-1) \bmod 341$ mit einer in der Vorlesung vorgestellten Methode.
(2) Zeige, dass $n$ den Fermat-Test zur Basis 2 besteht, nicht jedoch den Lucas-Test zum Parameterpaar $(1,-1)$.

(Bemerkung: Es ist keine zusammengesetzte natürliche Zahl bekannt, deren letzte Ziffer eine 3 oder 7 ist, und die den Fermat-Test zur Basis 2 und den Lucas-Test zum Parameterpaar $(1,-1)$ besteht.)

---

Datei: kii_u6.tex. Version vom 29.5.2025