Kryptographie **Blatt 6**

hhu Düsseldorf
WiSe 2023/24

Abgabe: bis Montag 27.11.2023, vor der Vorlesung

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Aufgabe 1: Introspektive Zahlen beim AKS-Test

Ist p prim, so heißt $m \in \mathbb{N}$ introspektiv für $f \in \mathbb{Z}_p[X]$ und $r \in \mathbb{N}$, falls gilt: $f(X)^m \equiv f(X^m) \bmod (X^r - 1, p)$. Seien p prim und $r \in \mathbb{N}$ gegeben, zeigen Sie:

(a) Für jedes $a \in \mathbb{Z}_p$ ist p introspektiv für $f(X) = X + a \in \mathbb{Z}_p[X]$ und r.

(b) Sind $k, m \in \mathbb{N}$ introspektiv für $f \in \mathbb{Z}_p[X]$ und r, so auch km.

(c) Ist m introspektiv für f, $g \in \mathbb{Z}_p[X]$ und r, so ist m auch introspektiv für fg und r.

Aufgabe 2: DL-Problem bei bekannten Potenzresten der Faktorbasis 2,3,5

Gegeben sei die Primzahl $p = 2^{13} - 1$ und die Primitivwurzel $g = 17$. Gesucht sei ℓ mit $g^\ell \equiv 5\ (p)$. Es sind dafür die folgenden Potenzreste schon bekannt: $g^{3513} \equiv 2^3 \cdot 3 \cdot 5^2\ (p)$, $g^{993} \equiv 2^4 \cdot 3 \cdot 5^2\ (p)$, $g^{1311} \equiv 2^2 \cdot 3 \cdot 5\ (p)$. Lösen Sie dieses DL-Problem mittels linearer Algebra durch Bestimmung ganzer Zahlen a, b, c so, dass $g^{3513a+993b+1311c} \equiv 5\ (p)$ ist.

Aufgabe 3: DL-Problem bei Kollision von Potenzen

Sei G eine Gruppe mit Erzeuger g der Ordnung n. Für ein $x \in G$ sei r mit $g^r = x$ gesucht (DL). Angenommen, man entdeckt ein Paar $a, b \in \mathbb{Z}$ mit $g^b = x^a$. Zeigen Sie, dass dann $r = (bu + kn)/d \bmod n$ für ein $k \in [0, d-1] \cap \mathbb{Z}$ der gesuchte diskrete Logarithmus ist, wo $d = (a, n)$ und u das Bézout-Element in $ua + vn = d$ ist.