Hand in: until monday 27.11.2023, before the lecture starts

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

Exercise 1: Introspective numbers in the AKS-test

If p is prime, we call $m \in \mathbb{N}$ introspective for $f \in \mathbb{Z}_p[X]$ and $r \in \mathbb{N}$, if

$$f(X)^m \equiv f(X^m) \bmod (X^r - 1, p).$$

Let p be prime and $r \in \mathbb{N}$ be given, show the following assertions:

(a) For any $a \in \mathbb{Z}_p$, the number p is introspective for $f(X) = X + a \in \mathbb{Z}_p[X]$ and r.

(b) If $k, m \in \mathbb{N}$ are introspective for $f \in \mathbb{Z}_p[X]$ and r, then also km.

(c) If m is introspective for f, $g \in \mathbb{Z}_p[X]$ and r, then m is also introspective for fg and r.

Exercise 2: DL-problem with known power residues in factor base 2,3,5

Let p be the given prime $p = 2^{13} - 1$ with primitive root $g = 17$. We seek for ℓ with $g^\ell \equiv 5\ (p)$. For this, the following power residues are known: $g^{3513} \equiv 2^3 \cdot 3 \cdot 5^2\ (p)$, $g^{993} \equiv 2^4 \cdot 3 \cdot 5^2\ (p)$, $g^{1311} \equiv 2^2 \cdot 3 \cdot 5\ (p)$. Solve this DL-problem by linear algebra: determine integers a, b, c such that $g^{3513a+993b+1311c} \equiv 5\ (p)$ holds.

Exercise 3: DL-problem with known power residue collision

Let G be a group with generator g of order n. For $x \in G$ we seek for r with $g^r = x$ (DL). Suppose one could discover a pair $a, b \in \mathbb{Z}$ with $g^b = x^a$. Show that $r = (bu + kn)/d \bmod n$ is the discrete logarithm in question for some $k \in [0, d-1] \cap \mathbb{Z}$, where $d = (a, n)$ and u is Bézout's element in $ua + vn = d$.