Number theory in cryptography

– Exercise set 6 –

The exercises P6.1, P6.2 have to be handed in on Tuesday, 2nd April 2024, 8:30 at latest.

Theoretical questions

T 6.1 Let $f(X) \in \mathbb{F}_q[X]$ be a polynomial of degree n over the finite field $\mathbb{F}_q$. For $i = 0, ..., n-1$ consider the remainders

$$X^{iq} \mod f(X) = q_{i,0} + q_{i,1}X + \cdots + q_{i,n-1}X^{n-1}.$$

Write the coefficients $\{q_{i,j}\}_{0 \le i,j \le n-1}$ as a matrix

$$Q = \begin{bmatrix} q_{0,0} & q_{1,0} & \cdots & q_{n-1,0} \\ q_{0,1} & q_{1,1} & \cdots & q_{n-1,1} \\ \vdots & \vdots & \ddots & \vdots \\ q_{0,n-1} & q_{1,n-1} & \cdots & q_{n-1,n-1} \end{bmatrix} \in \mathrm{Mat}_{n\times n}(\mathbb{F}_q).$$

For a polynomial $g(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1} \in \mathbb{F}_q[X]/(f(X)) =: R$, show that

$$g(X)^q = g(X) \text{ holds in } R \quad \text{if and only if} \quad v_g := \begin{bmatrix} c_0 \\ \vdots \\ c_{n-1} \end{bmatrix} \in \ker(Q - I_n).$$

T 6.2 (Rabin's irreducibility test) Prove the following criterion for a polynomial $f \in \mathbb{F}_q[x]$ of degree n: f is irreducible if and only if

a) $f(x) \mid (x^{q^n} - x)$,

b) $\gcd(f(x), x^{q^{n/\ell}} - x) = 1$ for every prime divisor $\ell \mid n$.

Programming exercises

P 6.1 In this exercise, you will implement a function `Berlekamp(f, q)` performing a Berlekamp factorization. It should take as an argument a square-free polynomial $f(X) \in \mathbb{F}_q[X]$ over some finite field $\mathbb{F}_q$. Return the list of non-trivial factors of f that you find using Berlekamp's algorithm if f is reducible (so it should just return f if your algorithm detects that f is irreducible), without using the built-in function `factor` for polynomials.

P 6.2 Use the above function to implement the function `Berlekamp_factor(f, q)`, that, given a polynomial $f(X) \in \mathbb{F}_q[X]$ returns a list with all irreducible factors of $f(X)$, together with their multiplicities. Don't forget to work with the square-free part[1] of f before using the `Berlekamp` function from above. Hint: you may want to consult https://doc.sagemath.org/html/en/reference/matrices/index.html to find information about the base class for matrices in SAGE.

P 6.3 (optional) Implement a function `factor_fixed_degree(f)` that takes a polynomial $f \in \mathbb{F}_q[X]$ of degree n and returns the list of all pairs (g_d, d) where g_d is a non-constant monic polynomial that is the product of all irreducible factors of f of degree d. Hint: think first about an *efficient* way to compute $\gcd(f, t^{q^r} - t)$ for a polynomial $f \in \mathbb{F}_q[t]$ and $r > 0$.

[1] You may want to use your function `remove_repeated_factors` from last week, or use the SAGE method `f.radical()`.