Number theory in cryptography

– Exercise set 4 –

The exercises T4.3 and P4.1 have to be handed in on Tuesday, 19th March 2024, 8:30 at latest. As usual, theoretical exercises have to be uploaded on **Moodle**, as a PDF file (e.g., a scan of a handwritten version or a PDF obtained from a LaTeX file). Programming exercises have to be done in the relevant file in the `CoCalc` project.

Theoretical questions

T 4.1 Let p be an odd prime and let q be a prime such that p (viewed as an element mod q and hence, of $\mathbb{F}_q$) is a primitive element of $\mathbb{F}_q^\times$ (i.e., that p generates the cyclic group $\mathbb{F}_q^\times$). Consider the polynomial

$$f(X) = \frac{X^q - 1}{X - 1} = X^{q-1} + \cdots + X + 1 \in \mathbb{F}_p[X].$$

Let α be a root of $f(X)$ and $\mathbb{F}_p(\alpha)$ be the finite field extension of $\mathbb{F}_p$ generated by α.

a) If $\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^d}$, show that $q \mid (p^d - 1)$.

b) Show that $d = q - 1$ and deduce that f is irreducible.

c) Show that $f(\alpha^{p^i}) = 0$ for all $i \in \{0, 1, \ldots, q-2\}$.

d) Let α be as above. Show that the set of elements $\{\alpha, \ldots, \alpha^{q-1}\}$ is the same as the set of elements $\left\{\alpha^{p^0}, \alpha^{p^1}, \ldots, \alpha^{p^{q-2}}\right\}$.

e) Deduce that $\{\alpha^{p^1}, \ldots, \alpha^{p^{q-1}}\}$ is a normal basis for $\mathbb{F}_{p^{q-1}}$ over $\mathbb{F}_p$. In fact, one calls this basis an *optimal normal basis.*

T 4.2 Prove that if g is a primitive element (= multiplicative generator) of $\mathbb{F}_{p^n}^\times$ and if $d \mid n$ then $g^{(p^n-1)/(p^d-1)}$ is a primitive element of $\mathbb{F}_{p^d}^\times$.

T 4.3 We have seen in class that we can construct $\mathbb{F}_9$ by adjoining to $\mathbb{F}_3$ the roots of an irreducible monic polynomial of degree 2.

a) Check that $f(X) = X^2 - X - 1 \in \mathbb{F}_3[X]$ is an irreducible polynomial and call α a root of this polynomial (in some algebraic closure of $\mathbb{F}_3$). All the elements of $\mathbb{F}_9$ can be written as $a + b\alpha$ for some $a, b \in \mathbb{F}_3$ (you don't need to prove this). Show that α is a generator of the multiplicative group $\mathbb{F}_9^\times$ (explain in detail your computations).

b) Find the discrete logarithm of $\alpha - 2$ to the base $\alpha - 1$, if it exists. That is, find an integer $n \in \mathbb{Z}$ such that $(\alpha - 1)^n = \alpha - 2 \in \mathbb{F}_9$.

Programming exercises

P 4.1 Implement `Montgomery_mult` and `Montgomery_exp` corresponding to the Montgomery multiplication and exponentiation respectively. Test the correctness of your functions using the `%` operator and compare the timing.

P 4.2 Construct with Sage the finite fields $\mathbb{F}_p$, $\mathbb{F}_{p^n}$ and $\mathbb{F}_p[X]/(P(X))$ for some irreducible polynomial $P(X)$ over $\mathbb{F}_p[X]$.

For various values of prime numbers p and integers $n > 1$ (e.g. $p = 23, n = 10$), find what irreducible polynomial $f(X) \in \mathbb{F}_p[X]$ is used in SAGE to construct the finite field $\mathbb{F}_{p^n}$.

P 4.3 We say that $x \in \mathbb{F}_p^\times$ is a square (or *a quadratic residue*) if there exists $y \in \mathbb{F}_p^\times$ such that $x = y^2$. Write a program counting how many squares there are in $\mathbb{F}_p^*$. Compute this number for all $p < 100$ and give a formula for this number. Prove this formula. Prove that $x \neq 0$ is a square if and only if $x^{\frac{p-1}{2}} = 1$ in $\mathbb{F}_p^*$.

P 4.4 Write a function computing the euclidean division between two polynomials in $\mathbb{F}_p[X]$.