Cryptography

PROF. DR. JOACHIM VON ZUR GATHEN, JÉRÉMIE DETREY

2. Tutorial: Finite fields – Cultivating polynomials

(when agriculture meets cryptography)

Exercise 2.1 (Bonsai polynomials).

Let's first familiarise ourselves with finite fields with a toy example.

We consider here the set of binary polynomials $\mathbb{Z}_2[x]$, where $\mathbb{Z}_2 = \{0, 1\}$ is the set of integers modulo 2.

(i) What is the algebraic structure of $\mathbb{Z}_2[x]$?

In order to control the number of elements in this set, we restrict ourselves to polynomials of degree at most 2. We note this set as $\mathbb{Z}_2[x]_{\leq 2}$. We transparently represent each polynomial $P(x) = p_2x^2 + p_1x + p_0$ as the bit-string $p_2p_1p_0$.

(ii) How many elements are there in this set? List them.

(iii) Describe how to compute the sum $R(x)$ of two polynomials $P(x)$ and $Q(x) \in \mathbb{Z}_2[x]_{\leq 2}$. Give the corresponding addition table.

(iv) We now consider multiplication over this set. What is the degree of the product $R(x)$ of two polynomials $P(x)$ and $Q(x) \in \mathbb{Z}_2[x]_{\leq 2}$? Does $R(x)$ still lies in $\mathbb{Z}_2[x]_{\leq 2}$?

(v) Describe a way of "trimming" $R(x)$ so that the result of a multiplication actually remains in $\mathbb{Z}_2[x]_{\leq 2}$.

Taking $M(x) = x^3 + x + 1$, which can be shown to be irreducible over $\mathbb{Z}_2$, we consider $\mathbb{Z}_2[x]/(M(x))$, that is the set of binary polynomials modulo $M(x)$.

(vi) Show that $\mathbb{Z}_2[x]/(M(x))$ and $\mathbb{Z}_2[x]_{\leq 2}$ contain exactly the same elements.

(vii) Give the multiplication table over $\mathbb{Z}_2[x]/(M(x))$.

(viii) Verify from that table that every element $P(x) \in \mathbb{Z}_2[x]/(M(x))$, $P(x) \neq 0$, has a multiplicative inverse $P^{-1}(x)$. Could we have expected that?

(ix) What is the algebraic structure of $\mathbb{Z}_2[x]/(M(x))$?

Now let's see what happens if we choose another irreducible polynomial of degree 3. Namely, we take $N(x) = x^3 + x^2 + 1$.

(x) Verify that the element $y(x) = x + 1 \in \mathbb{Z}_2[x]/(M(x))$ is a solution of the equation $N(y) = y^3 + y^2 + 1 = 0$.

(xi) Consider the set of binary polynomials in the variable y, modulo $N(y)$, noted $\mathbb{Z}_2[y]/(N(y))$. Express all the elements of this set in function of x.

Remark that each element $P(y)$ of $\mathbb{Z}_2[y]/(N(y))$ can be mapped to an element $Q(x) = P(x + 1)$ of $\mathbb{Z}_2[x]/(M(x))$. We note φ this mapping.

(xii) Given two polynomials $P(y)$ and $Q(y) \in \mathbb{Z}_2[y]/(N(y))$, verify that $\varphi(P + Q) = \varphi(P)+\varphi(Q)$, where the first addition is performed over $\mathbb{Z}_2[y]/(N(y))$ whereas the second one is performed over $\mathbb{Z}_2[x]/(M(x))$.

(xiii) Same question for the multiplication.

(xiv) Conclude.

Actually, one can show that finite fields like $\mathbb{Z}_2[x]/(M(x))$ are unique up to isomorphism. The choice of the irreducible polynomial only impacts on the representation of the elements, but not the intrinsic algebraic structure of the set. This is why we will usually note it simply $\mathbb{F}_{2^3}$. It is an extension of degree 3 of $\mathbb{Z}_2$, which is itself the finite field $\mathbb{F}_2$.

Exercise 2.2 (Agricultural Encryption Standard).

We now consider the finite field used in the S-boxes during the `SubBytes` step of the AES cipher.

Each byte of the current state is first seen as an element of the finite field $\mathbb{F}_{2^8}$, represented using the irreducible polynomial $M(x) = x^8 + x^4 + x^3 + x + 1$.

(i) Compute the multiplicative inverse of the polynomial $P(x) = x^6 + x^4 + x^2 + x + 1$ in $\mathbb{F}_2[x]/(M(x))$ using the extended Euclidean algorithm.

(ii) Using hexadecimal byte notation, what are $x^6 + x^4 + x^2 + x + 1$ and its inverse?

After this first step, we cease seeing our 8-bit words as elements of $\mathbb{F}_2[x]/(M(x))$, but we now consider them modulo the polynomial $N(x) = x^8 + 1$.

(iii) Is $N(x)$ irreducible over $\mathbb{F}_2$?

(iv) What can you say about the algebraic structure of $\mathbb{F}_2[x]/(N(x))$?

The remaining operations performed by the S-box are described as follows: if $P(x)$ was the initial input byte, and $Q(x)$ its multiplicative inverse modulo $M(x)$, the S-box then computes its result as

$$(x^4 + x^3 + x^2 + x + 1) \cdot Q(x) + (x^6 + x^5 + x + 1),$$

where the product is performed modulo $N(x)$. Using the hexadecimal notation, this becomes `1F` $\cdot\, Q(x) +$ `63`.

(v) Given $P(x) = x^6 + x^4 + x^2 + x + 1$ and its multiplicative inverse which you have computed above, complete the computation of the full S-box applied to $P(x)$.

(vi) Discuss the choice of $N(x)$ for those final operations.

We are now interested in the inverse transformation S-box^{-1}, used in the `InvSubBytes` step of the decryption process of AES.

(vii) Is the polynomial `1F` invertible modulo $N(x)$? If so, compute its inverse.

(viii) What is the inverse transformation of the S-box?