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 $\mathbb{Z}_2[x]$?

Solution. $\mathbb{Z}_2[x]$ is a ring. ○

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.

Solution. There are exactly 8 different polynomials: 0, 1, x, $x + 1$, x^2, $x^2 + 1$, $x^2 + x$, and $x^2 + x + 1$. Using the shorthand bit-string notation, those elements are 000, 001, 010, 011, 100, 101, 110, and 111. ○

(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.

Solution. Addition over $\mathbb{Z}_2[x]_{\leq 2}$ is just a coefficient-wise exclusive-OR of the coefficients: $r_i = p_i \oplus q_i$, for $0 \leq i \leq 2$.

+	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

(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 $\mathbb{Z}_2[x]_{\leq 2}$?

Solution. The degree of $R(x)$ is at most 4. Therefore, $R(x)$ may fall outside of $\mathbb{Z}_2[x]_{\leq 2}$. ◯

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

Solution. We can compute the multiplication modulo a fixed polynomial $M(x)$ of degree 3. Or simply truncate the polynomial $R(x)$ to keep only its 3 least significant coefficients (which is actually equivalent to considering it modulo the polynomial $M(x) = x^3$). ◯

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.

Solution. As $M(x)$ has degree 3, $\mathbb{Z}_2[x]/(M(x))$ contains all the binary polynomials of degree at most 2. And so does $\mathbb{Z}_2[x]_{\leq 2}$, by definition. ◯

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

Solution.

$\times$	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	100	110	011	001	111	101
011	000	011	110	101	111	100	001	010
100	000	100	011	111	110	010	101	001
101	000	101	001	100	010	111	011	110
110	000	110	111	001	101	011	010	100
111	000	111	101	010	001	110	100	011

◯

(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?

Solution. Suppose we have $P(x) \in \mathbb{Z}_2[x]/(M(x))$, $P(x) \neq 0$, such that $P(x)$ doesn't have a multiplicative inverse. $\mathbb{Z}_2[x]/(M(x))$ being finite, it actually means that $P(x)$ divides 0: there exists another polynomial $Q(x) \in \mathbb{Z}_2[x]/(M(x))$, $Q(x) \neq 0$, such that $P(x) \cdot Q(x) \equiv 0 \pmod{M(x)}$. Hence, factoring $P(x)$ as a product of irreducible polynomials, at least one of these factors has to divide $M(x)$, which contradicts the hypothesis that $M(x)$ is irreducible. ○

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

Solution. $\mathbb{Z}_2[x]/(M(x))$ is a field. ○

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 $N(y) = y^3 + y^2 + 1 = 0$.

Solution. $y^2(x) = x^2 + 1$ and $y^3(x) = x^2$. Hence $y^3 + y^2 + 1 = 0$. ○

(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.

Solution.

$\mathbb{Z}_2[y]/(N(y))$	0	1	y	$y+1$	y^2	y^2+1	y^2+y	y^2+y+1
$\mathbb{Z}_2[x]/(M(x))$	0	1	$x+1$	x	x^2+1	x^2	x^2+x	x^2+x+1

○

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 $\mathbb{Z}_2[x]/(M(x))$.

Solution. With $P(y) = p_2y^2 + p_1y + p_0$ and $Q(y) = q_2y^2 + q_1y + q_0$, we have

$$(P + Q)(y) = (p_2 + q_2)y^2 + (p_1 + q_1)y + (p_0 + q_0).$$

Hence

$$\begin{aligned}
\varphi(P + Q)(x) &= (p_2 + q_2)(x + 1)^2 + (p_1 + q_1)(x + 1) + (p_0 + q_0) \\
&= (p_2(x + 1)^2 + p_1(x + 1) + p_0) + \\
&\quad (q_2(x + 1)^2 + q_1(x + 1) + q_0) \\
&= \varphi(P)(x) + \varphi(Q)(x).
\end{aligned}$$

○

(xiii) Same question for the multiplication.

Solution. With $P(y) = p_2y^2 + p_1y + p_0$ and $Q(y) = q_2y^2 + q_1y + q_0$, we have

$$\begin{aligned}(P \cdot Q)(y) &= p_2q_2y^4 + (p_2q_1 + p_1q_2)y^3 + \\ &\quad (p_2q_0 + p_1q_1 + p_0q_2)y^2 + (p_1q_0 + p_0q_1)y + p_0q_0.\end{aligned}$$

Verifying that

$$\varphi(y^4)(x) = \varphi(y^2+y+1)(x) = (x+1)^2+(x+1)+1 = x^2+x+1 = (x+1)^4$$

and

$$\varphi(y^3)(x) = \varphi(y^2+1)(x) = (x+1)^2+1 = x^2 = (x+1)^3,$$

we get

$$\begin{aligned}&\varphi(P \cdot Q)(x) \\ &\quad = p_2q_2(x+1)^4 + (p_2q_1 + p_1q_2)(x+1)^3 + \\ &\qquad (p_2q_0 + p_1q_1 + p_0q_2)(x+1)^2 + (p_1q_0 + p_0q_1)(x+1) + p_0q_0 \\ &\quad = (p_2(x+1)^2 + p_1(x+1) + p_0) \cdot \\ &\qquad (q_2(x+1)^2 + q_1(x+1) + q_0) \\ &\quad = \varphi(P)(x) \cdot \varphi(Q)(x).\end{aligned}$$

○

(xiv) Conclude.

Solution. Proving that φ is a homomorphism, along with φ^{-1}, we show that φ is in fact an isomorphism between $\mathbb{Z}_2[y]/(N(y))$ and $\mathbb{Z}_2[x]/(M(x))$.

○

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.

Solution.

i	$rem[i]$	$quo[i]$	$aux[i]$
0	$x^8 + x^4 + x^3 + x + 1$	–	0
1	$x^6 + x^4 + x^2 + x + 1$	–	1
2	x^4	$x^2 + 1$	$x^2 + 1$
3	$x^2 + x + 1$	$x^2 + 1$	x^4
4	x	$x^2 + x$	$x^6 + x^5 + x^2 + 1$
5	1	$x + 1$	$x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$

We can then check that $(x^6+x^4+x^2+x+1)\cdot(x^7+x^5+x^4+x^3+x^2+x+1) \equiv 1 \pmod{M(x)}$. ○

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

Solution. $x^6 + x^4 + x^2 + x + 1$ is 01010111, which gives the byte `57`. Similarly, $x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$ is `BF`. ○

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 $\mathbb{F}_2$?

Solution. No, since $N(x) = x^8 + 1 = (x + 1)^8$. ○

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

Solution. $\mathbb{F}_2[x]/(N(x))$ is only a ring, since elements such as $x+1$ don't have a multiplicative inverse modulo $N(x)$. ○

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 $P(x)$.

Solution. From question (i), we have $Q(x) = x^7+x^5+x^4+x^3+x^2+x+1 =$ BF. We then compute 1F$\cdot$BF $=$ 34 and finally 1F$\cdot$BF$+$63 $=$ 34$+$63 $=$ 5B. Hence S-box(57) $=$ 5B.

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

Solution. Computing modulo $N(x)$, $x^8 = 1$, which means that the multiplication of a polynomial by x^i is equivalent to a rotation of its coefficients by i places to the left:

$$x^i \cdot (p_7 x^7 + \cdots + p_1 x + p_0) = p_{7-i} x^7 + \cdots + p_0 x^i + p_7 x^{i-1} + \cdots + p_{7-i+1}.$$

The multiplication by $x^4 + x^3 + x^2 + x + 1$ can actually be seen as the following matrix multiplication:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} p_0 \\ p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \\ p_6 \\ p_7 \end{bmatrix}.$$

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.

Solution. We use once again the extended Euclidean algorithm:

i	$rem[i]$	$quo[i]$	$aux[i]$
0	$x^8 + 1$	–	0
1	$x^4 + x^3 + x^2 + x + 1$	–	1
2	$x^3 + 1$	$x^4 + x^3$	$x^4 + x^3$
3	x^2	$x + 1$	$x^5 + x^3 + 1$
4	1	x	$x^6 + x^3 + x$

The multiplicative inverse of `1F` is then `4A`. ◯

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

Solution. We start by subtracting (or adding, equivalently) `63` from the input polynomial $P(x)$. We then multiply it by `4A`, modulo $N(x)$. We finally compute the multiplicative inverse of the resulting polynomial modulo $M(x)$. ◯