MAD 4471: Introduction to Cryptography and Coding Theory **Fall 2022**

Lecture 17: Modular Polynomials

Lecturer: Jean-François Biasse *TA: William Youmans*

The goal of this lecture is to describe elements of $\mathbb{Z}_q[X]/(X^n+1)$.

17.1 Polynomials

Polynomials over a field are a well-known example of infinite-dimensional vector spaces. They have been studied by most calculus students in the case where the field of definition if $\mathbb{R}$. In this case, we are mostly interested in the variations of the *polynomial function* $p : \mathbb{R} \to \mathbb{R}$ defined by

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0.$$

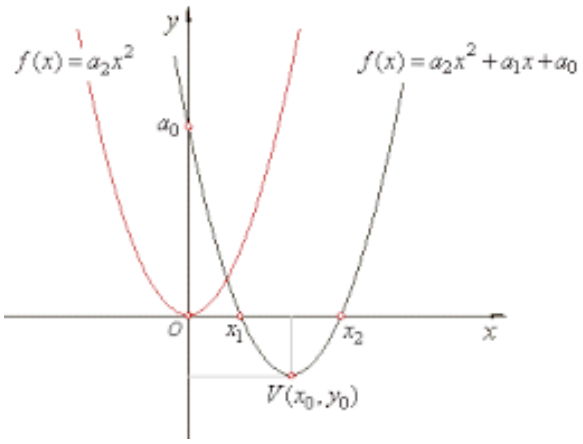

Figure 17.1: Some polynomial functions over $\mathbb{R}$

In algebraic terms, polynomials are elements, and we don't necessarily see them as functions. To properly define them, we need to use the notion of *ring*. In a nutshell, a ring is an additive group that has a multiplication. We focus our attention to rings with a multiplicative identity. The prototypical example of a ring is $(\mathbb{Z}, +, \times)$ where $+$ and $\times$ are the

Definition 17.1 (Ring) *A ring is a set R equipped with two binary operations: the addition $+$ and the multiplication $\times$ that satisfy the following properties:*

1. *$(R, +)$ is a commutative group*
   - $\forall a, b, c \in R$, $(a + b) + c = a + (b + c)$.

- $\forall a, b \in R$, $a + b = b + c$.
- *There is* $0 \in R$ *such that* $\forall a \in R$, $a + 0 = a$.
- $\forall a \in R$, $\exists - a \in R$ *such that* $a - a = 0$.

2. $(R, \times)$ *is a monoid*

- $\forall a, b, c \in R$, $(a \times b) \times c = a \times (b \times c)$.
- *There is* $1 \in R$ *such that* $\forall a \in R$, $a \times 1 = a$.

3. *Multiplication is distributive with respect to addition*

- $\forall a, b, c \in R$, $a \times (b + c) = (a \times b) + (a \times c)$.
- $\forall a, b, c \in R$, $(b + c) \times a = (b \times a) + (c \times a)$.

Example 1 *Given* $N > 1$, *one can easily verify that* $(\mathbb{Z}/N\mathbb{Z}, +, \times)$ *is a ring.*

With that in mind, we can define a polynomial over a ring R.

Definition 17.2 (Polynomial) *Let* R *be a ring. A polynomial* P *over* R *is an* n*-tuple of elements of elements* $(a_0, a_1, \ldots, a_{n-1})$ *in* R^n *for some* $n \geq 0$ *where* $a_{n-1} \neq 0$ *that is denote as*

$$P(X) = a_{n-1}X^{n-1} + \ldots + a_1 X + a_0.$$

The set of polynomials over R *is denoted* $R[X]$.

With the above notation, we implicitely assume that there will be no multivariate polynomials, or polynomials in another variable than X. Otherwise, one needs to specify a *transcendental* element X over R. We do not need any of that in this course. It turns out that $R[X]$ is itself a ring, where the addition is straighforward, and multiplication is the one we are used to for polynomial functions.

Definition 17.3 (Arithmetic of polynomials) *Let* R *be a ring. Let* $P(X) = \sum_{i=0}^{m} a_i X^i$, *and* $Q(X) = \sum_{j=0}^{n} b_j X^j \in R[X]$ *for* $m, n \geq 0$. *We define* $(P + Q)(X) = \sum_{i=0}^{\max m,n} c_i$ *and* $(P \times Q)(X) = \sum_{i=0}^{m+n} d_i$ *where* c_i, d_i *are defined as follows*

$$c_i = a_i + b_i$$
$$d_i = \sum_{k,l:k+l=i} a_k b_l$$

where $a_i = 0$ *for* $i > m$ *and* $b_j = 0$ *for* $j > n$.

Example 2 *Over* $\mathbb{Z}[X]$, *let us define* $P(X) = X^2 + 1$ *and* $Q(X) = X^3 + X + 2$. *Then*

$$P + Q = X^3 + X^2 + X + 3$$
$$P \times Q = X^5 + 2X^3 + 2X^2 + X + 2$$

Before moving on to to the division algorithm, we end this section by a few basic definitions.

Definition 17.4 *Let* R *be a ring.*

- *The degree of* $P(X) = \sum_{i=0}^{n} a_i X^i$ *is* $\deg(P) = n$.
- *If* $P(X) = 1 \cdot X^n + \ldots + a_1 X + a_0$, *we say that* P *is monic.*

17.2 Division by a monic polynomial

Similar to integers, one can define a polynomial division. First, given A and B in $R[X]$, it is possible that there is a Q in $R[X]$ such that $A = Q \times B$. In this case, we say that A is *divisible* by B. This is not the case in general. On the other hand, if B is monic, then there is always $Q, R \in R[X]$ with $\deg(R) < \deg(B)$ such that

$$A(X) = Q(X)B(X) + R(X).$$

We say that Q is the *quotient* and that R is the *remainder* of the polynomial division of A by B.

Remark 1 *In the case where R is a field, we can always divide by $B = \sum_{i \leq n} b_i X^i$ by first dividing $A' = \frac{1}{b_n} A$ by $B' = \frac{1}{b_n} B$ which is monic, thus getting an identity of the form $A'(X) = Q'(X)B'(X) + R'(X)$ with $\deg(R') < \deg(B') = \deg(B)$, and then multiply both sides of the equation by b_n to get $A(X) = Q'(X)B(X) + b_n R'(X)$.*

The proof of the existence of the polynomial division by a monic polynomial essentially derives from the description of the division algorithm itself. First, if $n \geq m$, then

$$A = 0 \times B + A,$$

i.e. $Q = B$ and $R = B$. This is the analogue of the integer division of a by $b > a$. Now we assume that $\deg(A) = m > \deg(B) = n$.

We start the procedure with $Q = 0$ and $k = m - n$. Then as long as $k \geq 0$, we repeat the operations:

1. $A \leftarrow A - a_{k+m} X^k B$.
2. $Q \leftarrow Q + a_{k+m} X^k$.
3. $k \leftarrow k - 1$.

At the end of the process, we set R to be A, which has degree less or equal to n.

Example 3 *$A = X^4 + 2X + 1$, and $B = X^2 + 1$. We start with $Q = 0$, and $k = 2$.*

1. *For $k = 2$:*
   - $A \leftarrow A - X^2 B = -X^2 + 2X + 1$.
   - $Q \leftarrow Q + X^2 = X^2$.
2. *For $k = 1$:*
   - $A \leftarrow A - (0X)B = -X^2 + 2X + 1$.
   - $Q \leftarrow Q + 0 = X^2$.
3. *For $k = 0$:*
   - $A \leftarrow A - (-1)B = +2X + 2$.
   - $Q \leftarrow Q + (-1) = X^2 - 1$.

At the end, $Q = X^2 - 1$, and $R = A = 2X + 2$. We can check that $QB + R = (X^2 + 1)(X^2 - 1) + 2X + 2 = X^4 - 1 + 2X + 2 = A$.

We can define congruence classes modulo a monic polynomial in $R[X]$ in the same way as for the integers.

Definition 17.5 (Congruence relation modulo a monic polynomial) *Let R be a ring and B be a monic polynomial of $R[X]$. We say that $A_1 \in R[X]$ is congurent to $A_2 \in R[X]$ if*

$$\exists Q \in R[X] \text{ such that } A_1 = QB + A_2.$$

We denote this properly by $A_1 \equiv A_2 \bmod B$.

The remainder of the division of A by B is denoted by $A \bmod B$, and it is the only element in the congruence class of A modulo B that has a degree strictly less than $\deg(B)$.

Definition 17.6 *Let R be a ring, and $B \in R[X]$ be a monic polynomial. We denote by $R[X]/B$ the congruence classes of elements of $R[X]$ modulo B. This space is equipped with an addition and a multiplication of element defined as follows*

$$[A_1] + [A_2] = [A_1 + A_2]$$
$$[A_1] \times [A_2] = [A_1 \times A_2],$$

where $[A]$ denotes the congruence class of A modulo B.

17.3 Circulant matrices

Our last lecture is about Module-LWE, a variant of LWE where operations happen in $\mathbb{Z}_q[X]/X^n+1$ instead of $\mathbb{Z}_q$. We can turn arithmetic in $\mathbb{Z}_q[X]/X^n+1$ into a linear algebra operation by using *circulant matrices*.

The multiplication of X^i by X^j gives the monomial X^{i+j}. If $i+j < n$, then $X^{i+j} \bmod X^n+1 = X^{i+j}$. On the other hand, if $i+j \geq n$, then

$$X^{i+j} = X^{i+j-n}(X^n+1) - X^{i+j-n},$$

hence $X^{i+j} \bmod X^n+1 = -X^{i+j-n}$. Next, we represent the congruence class of $P \in \mathbb{Z}_q[X]$ as the column vector in $\mathbb{Z}_q^n$ corresponding to the coefficients of $P \bmod X^n+1$. The map

$$[P] \in \mathbb{Z}_q[X]/X^n+1 \longmapsto [X^i] \times [P]$$

is linear. We can represent it as a matrix $A_i \in \mathbb{Z}_q^{n \times n}$ whose columns correspond to the image of $[X^j]$ for $j = 0, \ldots, n-1$.

$$A_i = \begin{pmatrix} & & & -1 & & (0) \\ & & & & \ddots & \\ & & & (0) & & -1 \\ 1 & & (0) & & & \\ & \ddots & & & & \\ (0) & & 1 & & & \end{pmatrix}$$

Example 4 *Assume $n = 3$, and $i = 1$, then*

$$A_1 = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

We can verify 1 by 1 all multiplications of X by $1, X, X^2$ modulo X^3+1:

- $X \times 1 \bmod X^3+1 = X$, *and* $A_1 \begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}0\\1\\0\end{pmatrix}$.
- $X \times X \bmod X^3+1 = X^2$, *and* $A_1 \begin{pmatrix}0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\end{pmatrix}$.
- $X \times X^2 \bmod X^3+1 = -1$, *and* $A_1 \begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}-1\\0\\0\end{pmatrix}$.

Multiplication by a given $[A]$ in $\mathbb{Z}_q[X]/X^n+1$ is obtained by linearity. Indeed, let $a_0, \ldots, a_{n-1}$ such that $[A] = a_0[1]+a_1[X]+\ldots, a_{n-1}[X^{n-1}]$, then the matrix of the multiplication-by-A linear map on $\mathbb{Z}_q[X]/X^n+1$ is

$$M_A = a_0A_0 + a_1A_1 + \ldots + a_{n-1}A_{n-1}.$$

Considering the shape of the A_i, we can easily give M_A with respect to the $(a_i)_{i<n}$:

$$M_A = \begin{pmatrix} a_0 & -a_{n-1} & \ldots & -a_1 \\ a_1 & a_0 & \ldots & -a_2 \\ \vdots & \vdots & & \vdots \\ a_{n-2} & a_{n-3} & \ldots & -a_{n-1} \\ a_{n-1} & a_{n-2} & \ldots & a_0 \end{pmatrix}$$

The fact that the coefficients of $[A]$ loop back to the lower indices is what gives these matrices their name: *circulant matrices.*

Example 5 *Assume $n = 3$ and $A = X^2 + 2X + 1$. Then*

$$M_A = \begin{pmatrix} 1 & -1 & -2 \\ 2 & 1 & -1 \\ 1 & 2 & 1 \end{pmatrix}$$

Assume that we want to know the image of $[P]$ for $P = X^2+1$ by the multiplication-by-$[A]$ map. The element $[P]$ corresponds to $\mathbf{x} = \begin{pmatrix}1\\0\\1\end{pmatrix}$, and

$$M_A\mathbf{x} = \begin{pmatrix}-1\\1\\2\end{pmatrix},$$

which tells us that $[P \times A] = [2X^2 + X - 1]$. We can verify this by direct calculation:

$$P \times A = X^4 + 2X^3 + 2X^2 + 2X + 1.$$

On the other hand, $(X^3+1)(X+2) + 2X^2 + X - 1 = X^4 + 2X^3 + 2X^2 + 2X + 1 = P \times A$. This shows that $P \times A \bmod X^3+1 = 2X^2 + X - 1$, as anticipated by the circulant matrix multiplication.