Polynomials

Definition: A *polynomial* of degree n in variable x over a field $\mathbb{K}$ is an expression $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$, where $a_n \neq 0$ and $a_n, \ldots, a_0 \in \mathbb{K}$. We write $p \in \mathbb{K}(x)$.

Operations on polynomials $p(x) = \sum_{i=0}^{n} a_i x^i, q(x) = \sum_{i=0}^{m} b_i x^i$:

- addition, subtraction: $(p \pm q)(x) = \sum_{i=0}^{\max n,m} (a_i \pm b_i)x^i$
- scalar multiple: $(\alpha p)(x) = \sum_{i=0}^{n} (\alpha a_i)x^i$
- product $(pq)(x) = \sum_{i=0}^{n+m} c_i x^i$, where $c_i = \sum_{j=0}^{i} a_j b_{i-j}$
- division with a remainder — there are unique polynomials $r, t \in \mathbb{K}(x)$ such that $p = qt + r$, where the degree of r is less than m, the degree of q.

Example — operations on polynomials over $\mathbb{Z}_5$

Addition:

$$(3x^3 + 2x + 1) + (2x^2 + 3x + 1) = 3x^3 + 2x^2 + 2$$

the degree may decrease:

$$(3x^3 + 2x + 1) + (2x^3 + 3x + 1) = 2$$

Multiple:

$$2 \cdot (3x^3 + 2x + 1) = x^3 + 4x + 2$$

Product:

$$(3x^3 + 2x + 1)(2x^2 + 3x + 1) = x^5 + 4x^4 + 2x^3 + 3x^2 + 1$$

Example — operations on polynomials over $\mathbb{Z}_5$

Division with the remainder:

$$
\begin{array}{rrrrrrl}
4x^5 & +2x^4 & & +3x^2 & & +3 & : \ 3x^2+4x+2 \ = \ 3x^3+3x+2 \\
-4x^5 & -2x^4 & -\ x^3 & & & & \\
\cline{1-3}
 & & 4x^3 & +3x^2 & & & \\
 & & -4x^3 & -2x^2 & -\ x & & \\
\cline{3-5}
 & & & x^2 & +4x & +3 & \\
 & & & -\ x^2 & -3x & -4 & \\
\cline{4-6}
 & & & & x & +4 &
\end{array}
$$

Correctness check $p = qt + r$:

$$4x^5 + 2x^4 + 3x^2 + 3 \ = \ (3x^2 + 4x + 2)(3x^3 + 3x + 2) \ + \ (x + 4)$$

Fermat's little theorem

Theorem: For any $x \in \mathbb{Z}_p \setminus \{0\} : x^{p-1} = 1$.

Proof: The map $i \to xi$ is a bijection on $\{1, \ldots, p-1\}$ in $\mathbb{Z}_p$.
In $\prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} xi = x^{p-1} \prod_{i=1}^{p-1} i$ cancel the nonzero term $\prod_{i=1}^{p-1} i$.

Corollary: For any $x \in \mathbb{Z}_p : x^p - x = 0$.

Corollary: For any $q \in \mathbb{Z}_p(x)$ there is $r \in \mathbb{Z}_p(x)$ of degree at most $p-1$, such that $\forall x \in \mathbb{Z}_p : q(x) = r(x)$.

Example:

$$4x^5 + 2x^4 + 3x^2 + 3 \;=\; 4(x^5 - x) \;+\; 2x^4 + 3x^2 + 4x + 3$$

i.e. the polynomial $q(x) = 4x^5 + 2x^4 + 3x^2 + 3$ yields on $\mathbb{Z}_5$ the same values as $r(x) = 2x^4 + 3x^2 + 4x + 3$.

Roots

Definition: The *root* of a polynomial $p \in \mathbb{K}(x)$
is $r \in \mathbb{K}$ such that $p(r) = 0$.

Observation: The element $r \in \mathbb{K}$ is a root of a polynomial p if and only if the linear polynomial $x - r$ divides p without a remainder.

Definition: The *multiplicity* of the root r of $p \in \mathbb{K}(x)$ is the maximum positive integer k such that $(x - r)^k$ divides p.

Theorem: (The fundamental theorem of algebra)
Every polynomial $p \in \mathbb{C}(x)$ has at least one root.

Corollary: Every polynomial $p \in \mathbb{C}(x)$ can be factorized into linear factors, i.e polynomials of degree one.

Definition: If every $p \in \mathbb{K}(x)$ of degree at least 1 has a root, then the field $\mathbb{K}$ is *algebraically closed*.

Representations of polynomials of degree n

- by the coefficients $a_0, \dots, a_n$
- in algebraically closed fields by a_n and the n roots $r_1, \dots, r_n$
- by the values of the polynomial in $n+1$ distinct points

Problem: Given $n+1$ pairs (x_i, y_i) for $i = 0, \dots, n$, determine $p \in \mathbb{K}(x)$ of degree at most n such that $p(x_i) = y_i$ for all i.

Observation: Coefficients $a_0, \dots, a_n$ of p are solution of the system:

$$\begin{pmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{pmatrix}$$

Definition: The matrix of this system is the *Vandermonde matrix* $\boldsymbol{V}_{n+1}(x_0, \dots, x_n)$

Theorem: The Vandermonde matrix $\boldsymbol{V}_{n+1}(x_0, \dots, x_n)$ is regular if an only if $x_0, \dots, x_n$ are distinct.

Proof of the regularity of the Vandermonde matrix

$$\boldsymbol{V}_{n+1}(x_0, \ldots, x_n) = \begin{pmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^n \\ 1 & x_1 & x_1^2 & \ldots & x_1^n \\ 1 & x_2 & x_2^2 & \ldots & x_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^n \end{pmatrix}$$

Deduct the first row from others. Then factor out $x_i - x_0$ from the i-th row for each $i = 1, \ldots, n$. In the first column are n zeros so we can expand: $\det(\boldsymbol{V}_{n+1}) =$

$$= \prod_{i=1}^{n}(x_i - x_0) \cdot \begin{vmatrix} 1 & x_1 + x_0 & x_1^2 + x_1x_0 + x_0^2 & \ldots & x_1^{n-1} + x_1^{n-2}x_0 + \cdots + x_0^{n-1} \\ 1 & x_2 + x_0 & x_2^2 + x_2x_0 + x_0^2 & \ldots & x_2^{n-1} + x_2^{n-2}x_0 + \cdots + x_0^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n + x_0 & x_n^2 + x_nx_0 + x_0^2 & \ldots & x_n^{n-1} + x_n^{n-2}x_0 + \cdots + x_0^{n-1} \end{vmatrix}$$

Now *backward* subtract from every column the x_0-multiple of the previous one. By this we eliminate all terms containing x_0.

Consequently, we get a recurrence that could be expanded as follows:

$$\begin{aligned} \det(\boldsymbol{V}_{n+1}(x_0, \ldots, x_n)) &= \left(\prod_{i=1}^{n}(x_i - x_0)\right) \det(\boldsymbol{V}_n(x_1, \ldots, x_n)) \\ &= \prod_{i<j}(x_j - x_i) \end{aligned}$$

Example for $n = 3$

$$\det(\boldsymbol{V}_4(x_0, \dots, x_3)) =$$

$$= \begin{vmatrix} 1 & x_0 & x_0^2 & x_0^3 \\ 1 & x_1 & x_1^2 & x_1^3 \\ 1 & x_2 & x_2^2 & x_2^3 \\ 1 & x_3 & x_3^2 & x_3^3 \end{vmatrix} \begin{array}{c} \mathrm{I} \\ \mathrm{II} \\ \mathrm{III} \\ \mathrm{IV} \end{array} = \begin{vmatrix} 1 & x_0 & x_0^2 & x_0^3 \\ 0 & x_1 - x_0 & x_1^2 - x_0^2 & x_1^3 - x_0^3 \\ 0 & x_2 - x_0 & x_2^2 - x_0^2 & x_2^3 - x_0^3 \\ 0 & x_3 - x_0 & x_3^2 - x_0^2 & x_3^3 - x_0^3 \end{vmatrix} \begin{array}{c} \mathrm{I} \\ \mathrm{II} - \mathrm{I} \\ \mathrm{III} - \mathrm{I} \\ \mathrm{IV} - \mathrm{I} \end{array}$$

$$= \begin{vmatrix} x_1 - x_0 & x_1^2 - x_0^2 & x_1^3 - x_0^3 \\ x_2 - x_0 & x_2^2 - x_0^2 & x_2^3 - x_0^3 \\ x_3 - x_0 & x_3^2 - x_0^2 & x_3^3 - x_0^3 \end{vmatrix} \begin{array}{l} : (x_1 - x_0) \\ : (x_2 - x_0) \\ : (x_3 - x_0) \end{array}$$

$$= (x_1 - x_0)(x_2 - x_0)(x_3 - x_0) \begin{array}{c} \begin{vmatrix} 1 & x_1 + x_0 & x_1^2 + x_1 x_0 + x_0^2 \\ 1 & x_2 + x_0 & x_2^2 + x_2 x_0 + x_0^2 \\ 1 & x_3 + x_0 & x_3^2 + x_3 x_0 + x_0^2 \end{vmatrix} \\ \begin{array}{ccc} \mathrm{I} & \mathrm{II} & \mathrm{III} \end{array} \end{array}$$

$$= \prod_{i=1}^{3} (x_i - x_0) \begin{array}{c} \begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{vmatrix} \\ \begin{array}{ccc} \mathrm{I} & \mathrm{II} - x_0 \mathrm{I} & \mathrm{III} - x_0 \mathrm{II} \end{array} \end{array} = \left(\prod_{i=1}^{3} (x_i - x_0) \right) \det(\boldsymbol{V}_3(x_1, x_2, x_3))$$

Lagrange interpolation

... an alternative way to interpolate a polynomial $p \in \mathbb{K}(x)$ of degree n through $n+1$ points (x_i, y_i) for $i = 1, \ldots, n+1$.

1. determine $n+1$ auxiliary polynomials of degree n

$$p_i(x) = \frac{\prod\limits_{j \neq i} (x - x_j)}{\prod\limits_{j \neq i} (x_i - x_j)} =$$

$$= \frac{(x-x_1)\ldots(x-x_{i-1})(x-x_{i+1})\ldots(x-x_{n+1})}{(x_i-x_1)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_{n+1})}$$

Observe that $p_i(x_i) = 1$ and $p_i(x_j) = 0$ for $i \neq j$.

2. compose $p(x)$ as the linear combination $p(x) = \sum\limits_{i=1}^{n+1} y_i p_i(x)$.

Then $p(x_i) = y_i p_i(x_i) = y_i$ as in all the other terms $p_j(x_i) = 0$.

Example of Lagrange interpolation

Goal: interpolate a polynomial $p(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ over $\mathbb{Z}_{11}$ through points $(1, 5)$, $(2, 1)$, $(3, 3)$, $(4, 4)$, $(5, 3)$, $(6, 5)$ and $(7, 10)$.

We seek a_4, a_3, a_2, a_1 and a_0, that satisfy (over $\mathbb{Z}_{11}$!!)

$$
\begin{array}{rcrcrcrcrcr}
a_4 & + & a_3 & + & a_2 & + & a_1 & + & a_0 & = & 5 \\
5a_4 & + & 8a_3 & + & 4a_2 & + & 2a_1 & + & a_0 & = & 1 \\
4a_4 & + & 5a_3 & + & 9a_2 & + & 3a_1 & + & a_0 & = & 3 \\
3a_4 & + & 9a_3 & + & 5a_2 & + & 4a_1 & + & a_0 & = & 4 \\
9a_4 & + & 4a_3 & + & 3a_2 & + & 5a_1 & + & a_0 & = & 3 \\
9a_4 & + & 7a_3 & + & 3a_2 & + & 6a_1 & + & a_0 & = & 5 \\
3a_4 & + & 2a_3 & + & 5a_2 & + & 7a_1 & + & a_0 & = & 10
\end{array}
$$

In fact, 5 points suffices. We may restrict ourselves to the first 5 equations (and the first 5 points).

We first calculate partial polynomials $p_1, \ldots, p_5$.
These polynomials satisfy: $p_i(x_i) = 1$ and also $j \neq i : p_i(x_j) = 0$.

$$p_1(x) = \frac{(x-2)(x-3)(x-4)(x-5)}{(1-2)(1-3)(1-4)(1-5)} = \frac{x^4+8x^3+5x^2+10}{2} = 6x^4+4x^3+8x^2+5$$
$$p_2(x) = \frac{(x-1)(x-3)(x-4)(x-5)}{(2-1)(2-3)(2-4)(2-5)} = \frac{x^4+9x^3+4x^2+3x+5}{5} = 9x^4+4x^3+3x^2+5x+1$$
$$p_3(x) = \frac{(x-1)(x-2)(x-4)(x-5)}{(3-1)(3-2)(3-4)(3-5)} = \frac{x^4+10x^3+5x^2+10x+7}{4} = 3x^4+8x^3+4x^2+8x+10$$
$$p_4(x) = \frac{(x-1)(x-2)(x-3)(x-5)}{(4-1)(4-2)(4-3)(4-5)} = \frac{x^4+8x^2+5x+8}{5} = 9x^4+6x^2+x+6$$
$$p_5(x) = \frac{(x-1)(x-2)(x-3)(x-4)}{(5-1)(5-2)(5-3)(5-4)} = \frac{x^4+x^3+2x^2+5x+2}{2} = 6x^4+6x^3+x^2+8x+1$$

The desired polynomial is combined from the partial polynomials and from the values in the given points $(i, p(i))$ as:

$$\begin{aligned} p(x) &= \sum_{i=1}^{5} y_i p_i(x) = 5p_1(x) + p_2(x) + 3p_3(x) + 4p_4(x) + 3p_5(x) \\ &= 3x^4 + 5x^2 + 2x + 6 \end{aligned}$$

We may check, whether the other points $(6, 5)$, $(7, 10)$ lie on $p(x)$

$$p(6) = 3 \cdot 6^4 + 5 \cdot 6^2 + 2 \cdot 6 + 6 = 3 \cdot 9 + 5 \cdot 3 + 2 \cdot 6 + 6 = 5$$
$$p(7) = 3 \cdot 7^4 + 5 \cdot 7^2 + 2 \cdot 7 + 6 = 3 \cdot 3 + 5 \cdot 5 + 2 \cdot 7 + 6 = 10$$

Applications

Problem: Given numbers m and n, design m keys so that:

- It is possible to reconstruct a given secret from any combination of n keys, but
- it is impossible to reconstruct a given secret from any combination of less than n keys.

Assume that the way the keys are constructed is publicly known.

Solution: Construct a polynomial of degree $n-1$ and distribute m distinct pairs $(x_i, p(x_i))$ as keys. The secret is the polynomial. The field could be e.g. $\mathbb{R}$ or $\mathbb{Z}_p$ with $p > m$.

Problem: Can two integers of n digits be multiplied in $o(n^2)$ time?

Solution:

- Interpret these integers as polynomials p, q of degree $n-1$,
- choose $2n$ pairs $(i, p(i)), (i, q(i))$ and compute $(i, p(i)q(i))$,
- then find the coefficients of the product pq in time $O(n \log n)$.

The choice of a suitable field and the recurrence behind is the principle of the so called *fast Fourier transform*.