Recitation: Finite fields

Groups

A **Group** (G,*,I) is a set *G* with operator * such that:

1. **Closure**. For all $a,b \in G$, $a * b \in G$
2. **Associativity.** For all $a,b,c \in G$, $a*(b*c) = (a*b)*c$
3. **Identity.** There exists $I \in G$, such that for all $a \in G$, $a*I=I*a=a$
4. **Inverse.** For every $a \in G$, there exist a unique element $b \in G$, such that $a*b=b*a=I$

An **Abelian or Commutative Group** is a Group with the additional condition

5. **Commutativity.** For all $a,b \in G$, $a*b=b*a$

Examples of groups

Q: Examples?

- Integers, Reals or Rationals with Addition
- The nonzero Reals or Rationals with Multiplication
- Invertible square real matrices with Matrix Multiplication
- Permutations over n elements with composition

  [0→1, 1→2, 2→0] o [0→1, 1→0, 2→2] = [0→0, 1→2, 2→1]

Often we will be concerned with **finite groups**, i.e., ones with a finite number of elements.

Groups based on modular arithmetic

The group of positive integers modulo a prime *p*

$Z_p^* \equiv \{1, 2, 3, \ldots, p\text{-}1\}$ $*_p \equiv$ multiplication modulo p

Denoted as: $(Z_p^*, *_p)$

Required properties

1. Closure. Yes.
2. Associativity. Yes.
3. Identity. 1.
4. Inverse. Yes. (try to prove this yourself)

Example: $Z_7^* = \{1,2,3,4,5,6\}$

$1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 5$, $6^{-1} = 6$

Fields

A **Field** is a set of elements F with **two** binary operators * and + such that

1. (F, +) is an **abelian group**
2. (F \ I_+, *) is an **abelian group**
   the "multiplicative group"
3. **Distribution**: a*(b+c) = a*b + a*c
4. **Cancellation**: $a*I_+ = I_+$

Example: The reals and rationals with + and * are fields.

The **order (or size)** of a field is the number of elements.

A field of finite order is a **finite field**.

Finite Fields

$\mathbb{Z}_p$ (p prime) with + and * mod p, is a **finite** field.

1. ($\mathbb{Z}_p$, +) is an **abelian group** (0 is identity)
2. ($\mathbb{Z}_p \setminus 0$, $*$) is an **abelian group** (1 is identity)
3. **Distribution**: a*(b+c) = a*b + a*c
4. **Cancellation**: a*0 = 0

We denote this by $\mathbb{F}_p$ or GF(p)

Are there other finite fields?

What about ones that fit nicely into bits, bytes and words (i.e with 2^k elements)?

Polynomials over $\mathbb{F}_p$

$\mathbb{F}_p[x]$ = polynomials on x with coefficients in $\mathbb{F}_p$.

- Example of $\mathbb{F}_5[x]$: f(x) = $3x^4 + 1x^3 + 4x^2 + 3$
- deg(f(x)) = 4 (the **degree** of the polynomial)

Operations: (examples over $\mathbb{F}_5[x]$)

•Addition: $(x^3 + 4x^2 + 3) + (3x^2 + 1) = (x^3 + 2x^2 + 4)$

•Multiplication: $(x^3 + 3) * (3x^2 + 1) = 3x^5 + x^3 + 4x^2 + 3$

•$I_+ = 0$, $I_* = 1$

•+ and * are associative and commutative

•Multiplication distributes and 0 cancels

Do these polynomials form a field?

Division and Modulus

Long division on polynomials ($\mathbb{F}_5[x]$):

$$
\begin{array}{r}
1x+4 \\
x^2+1 \overline{\big) x^3+4x^2+0x+3} \\
\underline{x^3+0x^2+1x+0} \\
4x^2+4x+3 \\
\underline{4x^2+0x+4} \\
4x+4
\end{array}
$$

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

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

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

Polynomials modulo Polynomials

How about making a field of polynomials modulo another polynomial?

This is analogous to $\mathbb{F}_p$ (i.e., integers modulo another integer).

Need a polynomial analogous to a prime number…

Definition: An **irreducible polynomial** is one that is not a product of two other polynomials both of degree greater than 0.

e.g. (x^2 + 2) for $\mathbb{F}_5[x]$

Galois Fields

The polynomials $\mathbb{F}_p[x] \bmod p(x)$ where

1. $p(x) \in \ \in \ \mathbb{F}_p\,[x]$, p(x) is irreducible and

2. deg(p(x)) = n

form a finite field.

Q: How many elements?

Such a field has p^n elements.

These fields are called **Galois Fields** or **GF(p^n)** or $\mathbb{F}_{p^n}$

The special case n = 1 reduces to the fields $\mathbb{F}_p$.

The special case p = 2 is especially useful for us.

GF(2^n)

$\mathbb{F}_{2^n}$ = set of polynomials in $\mathbb{F}_2[x]$ modulo irreducible polynomial $\mathrm{p}(x) \in \mathbb{F}_2[x]$ of degree n.

Elements are all polynomials in $\mathbb{F}_2[x]$ of degree $\leq n - 1$.

Has 2^n elements.

Natural correspondence with bits in $\{0,1\}^n$.

Elements of $\mathbb{F}_{2^8}$ can be represented as **a byte**, one bit for each term.

E.g., $x^6 + x^4 + x + 1 = 01010011$

GF(2^n)

$\mathbb{F}_{2^n}$ = set of polynomials in $\mathbb{F}_2[x]$ modulo
irreducible polynomial $\mathrm{p}(x) \in \mathbb{F}_2[x]$ of degree n.

Elements are all polynomials in $\mathbb{F}_2[x]$ of degree $\leq n-1$.
Has 2^n elements.
Natural correspondence with bits in $\{0,1\}^n$.

Addition over $\mathbb{F}_2$ corresponds to xor.

- Just take the xor of the bit-strings (bytes or words in practice). This is dirt cheap.

Multiplication over GF(2^n)

If n is small enough can use a table of all combinations.

The size will be 2^n x 2^n (e.g. 64K for $\mathbb{F}_{2^8}$)

Otherwise, use standard shift and add (xor)

Note: dividing through by the irreducible polynomial on an overflow by 1 term is simply a test and an xor.

e.g. 0111 mod 1001 = 0111

1011 mod 1001 = 1011 xor 1001 = 0010

^ just look at this bit for $\mathbb{F}_{2^3}$

Finding inverses over GF(2^n)

Again, if n is small just store in a table.

- Table size is just 2^n.

For larger n, use Euclid's algorithm.

- This is again easy to do with shift and xors.

Euclid's Algorithm

Euclid's Algorithm:

gcd(a,b) = gcd(b,a mod b)

gcd(a,0) = a

"Extended" Euclid's algorithm:

- Find **x** and **y** such that **ax + by = gcd(a,b)**
- Can be calculated as a side-effect of Euclid's algorithm.
- Note that **x** and **y** can be zero or negative.

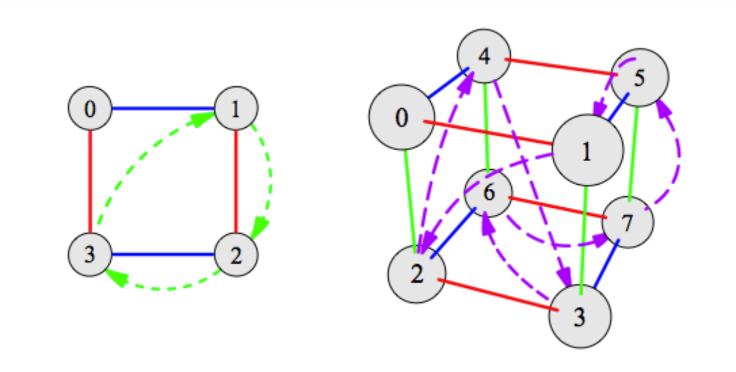
This allows us to find **a^{-1} mod p**, for **a** $\in Z_p^*$

Q: Any idea how?

In particular return **x** in **ax + py = 1**.

Similarly can apply to over polynomials

The structure of $\mathbb{F}_{2^2}$ and $\mathbb{F}_{2^3}$



Source: *Visual Group Theory*, Nathan C. Carter.

Polynomials

Lemma
Let $p \in \mathbb{F}[x]$ and let $\alpha \in \mathbb{F}$. Then $p(\alpha) = 0$ iff $(x - \alpha)$ divides $p(x)$.

Corollary
If a polynomial is irreducible over $\mathbb{F}$, then it does not have a root in $\mathbb{F}$.

Notice that the converse is not true. E.g. $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ with field $\mathbb{F}_2$.

Theorem
A polynomial $p \in \mathbb{F}[x]$ of degree n has at most n roots in $\mathbb{F}$.

Polynomials

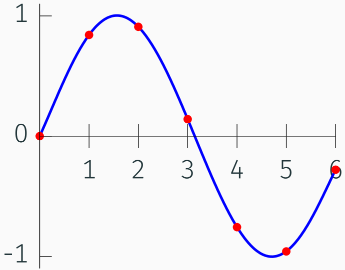
Lemma
Let $p \in \mathbb{F}[x]$ and let $\alpha \in \mathbb{F}$. Then $p(\alpha) = 0$ iff $(x - \alpha)$ divides $p(x)$.

Corollary
If a polynomial is irreducible over $\mathbb{F}$, then it does not have a root in $\mathbb{F}$.

Notice that the converse is not true. E.g. $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ with field $\mathbb{F}_2$.

Theorem
A polynomial $p \in \mathbb{F}[x]$ of degree n has at most n roots in $\mathbb{F}$.

Lagrange interpolation



Consider a set of k points:

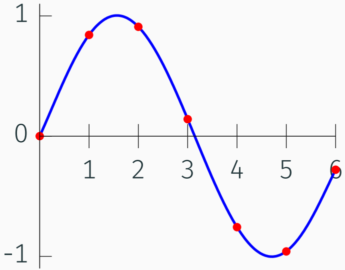
$$(x_0, y_0), \ldots, (x_j, y_j), \ldots, (x_k, y_k)$$

with distinct x_j.

We want a degree $k-1$ polynomial p such that:

$$p(x_j) = y_j, \text{ for } j \in \{0, \ldots, k\}$$

Lagrange interpolation



Consider a set of k points:

$$(x_0, y_0), \dots, (x_j, y_j), \dots, (x_k, y_k)$$

with distinct x_j.

We want a degree $k-1$ polynomial p such that:

$$p(x_j) = y_j, \text{ for } j \in \{0, \dots, k\}$$

Lagrange interpolation

$$(x_0, y_0), \ldots, (x_j, y_j), \ldots, (x_k, y_k)$$

We can solve this as a system of linear equations:

$$\begin{bmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^k \\ 1 & x_1 & x_1^2 & \cdots & x_1^k \\ 1 & x_2 & x_2^2 & \cdots & x_2^k \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_k & x_k^2 & \cdots & x_k^k \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_k \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_k \end{bmatrix}$$

Another “simpler” solution is obtained by representing polynomials in a different basis.

Lagrange interpolation

$$(x_0, y_0), \ldots, (x_j, y_j), \ldots, (x_k, y_k)$$

Consider the polynomial:

$$\ell_j(x) = \prod_{\substack{0 \le m \le k \\ m \ne j}} \frac{x - x_m}{x_j - x_m}$$

$$= \frac{(x - x_0)}{(x_j - x_0)} \cdots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \cdots \frac{(x - x_k)}{(x_j - x_k)}$$

Notice that:

$$\ell_j(x_j) = 1 \quad \text{and} \quad \ell_j(x_{i \ne j}) = 0.$$

Therefore the polynomial we want is:

$$L(x) = \sum_{j=0}^{k} y_j \ell_j(x)$$

Lagrange interpolation

$$(x_0, y_0), \ldots, (x_j, y_j), \ldots, (x_k, y_k)$$

Consider the polynomial:

$$\ell_j(x) = \prod_{\substack{0 \le m \le k \\ m \ne j}} \frac{x - x_m}{x_j - x_m}$$

$$= \frac{(x - x_0)}{(x_j - x_0)} \cdots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \cdots \frac{(x - x_k)}{(x_j - x_k)}$$

Notice that:

$$\ell_j(x_j) = 1 \quad \text{and} \quad \ell_j(x_{i \ne j}) = 0.$$

Therefore the polynomial we want is:

$$L(x) = \sum_{j=0}^{k} y_j \ell_j(x)$$

Lagrange interpolation

$$(x_0, y_0), \ldots, (x_j, y_j), \ldots, (x_k, y_k)$$

Consider the polynomial:

$$\ell_j(x) = \prod_{\substack{0 \le m \le k \\ m \ne j}} \frac{x - x_m}{x_j - x_m}$$

$$= \frac{(x - x_0)}{(x_j - x_0)} \cdots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \cdots \frac{(x - x_k)}{(x_j - x_k)}$$

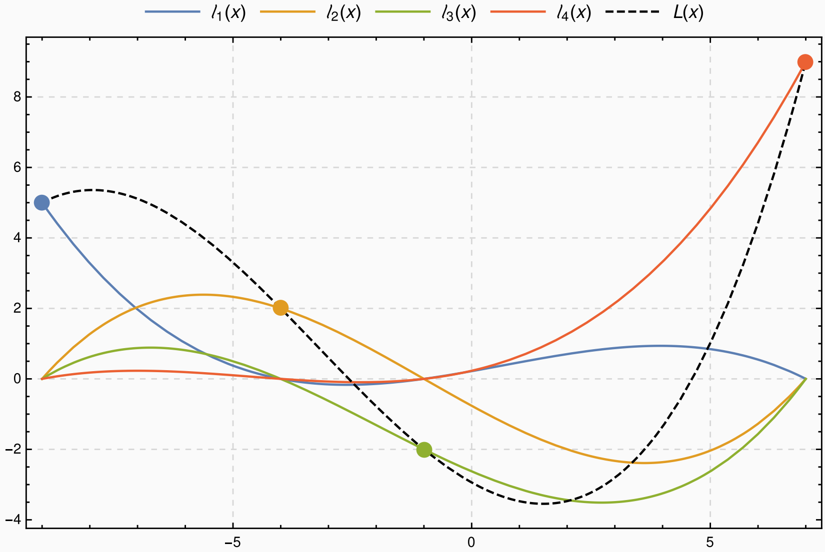
Notice that:

$$\ell_j(x_j) = 1 \quad \text{and} \quad \ell_j(x_{i \ne j}) = 0.$$

Therefore the polynomial we want is:

$$L(x) = \sum_{j=0}^{k} y_j \ell_j(x)$$

Lagrange interpolation



Source: `https://en.wikipedia.org/wiki/Lagrange_polynomial`

Linear algebra

- All the things you learnt in linear algebra also hold when elements come from a finite field
- A *vector space* over $\mathbb{F}$ is a set V with: *vector addition* and *scalar multiplication*, and closed under both operations.
- A *subspace* $W \subseteq V$ is a set of vectors closed under vector addition and scalar multiplication
- A *linear combination* of U is:

$$\sum_{\mathbf{v}_i \in U} \alpha_i \mathbf{v}_i \quad \text{for } \alpha_i \in \mathbb{F}$$

- U is *linearly independent* if no (non-trivial) linear combination is zero

Linear algebra

- The *span* of U is the set generated by all linear combinations of U
- A *basis* B of a subspace W is a linearly independent set of vectors that spans W
- The *dimension* of a subspace W is the number of vectors in any basis
- Let $A \in \mathbb{F}^{m \times n}$ be a matrix.
  - $\mathsf{col}(A) = \{A\mathbf{x} \mid \mathbf{x} \in \mathbb{F}^n\}$
  - $\mathsf{rank}(A) = \mathsf{dim}(\mathsf{col}(A))$
  - $\mathsf{null}(A) = \{\mathbf{x} \mid A\mathbf{x} = 0\}$.
  - $\mathsf{nullity}(A) = \mathsf{dim}(\mathsf{null}(A))$
  - $\mathsf{rank}(A) + \mathsf{nullity}(A) = n$
  - A is invertible iff $\mathsf{rank}(A) = n$