Prime bodies

equivalence class modulo p:

$$[a]_p := \{ b \in \mathbb{Z} \mid a \equiv b \pmod p \} \qquad \text{e.g.} \quad [2]_4 = \{2, 6, 10, 14 \dots\}$$

we can just write a instead of $[a]$ if it's clear

then we define the ring of the remainder classes modulo p:

$$\mathbb{Z}_p := \{ [a]_p \mid a \in \mathbb{Z} \}$$

← otherwise we can get 0 from multiplication

$\mathbb{Z}_p$ is a field iff p is prime, in that case we use the notation $\mathbb{F}_p$

e.g. $\mathbb{F}_3 = \{0,1,2\} = \{[0]_3, [1]_3, [2]_3\}$

simplify notation

Polynomial rings

the polynomial ring over a field $\mathbb{F}$ is:

$$\mathbb{F}[x] := \left\{ \sum_{i=0}^{n} a_i x^i \mid 0 \le n < \infty,\ a_i \in \mathbb{F} \right\} \quad \text{degree } n$$

e.g. $\mathbb{F}_2 \qquad 1+1=0$

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

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

this is not a field because we don't have the inverse, but from this we can derive all possible finite fields.

As with $\mathbb{Z}$ we can define prime terms (irreducible pol.)
like pol.s that don't have non-trivial divisors.
As with $\mathbb{N}$ we can factor any pol. in its prime components

Quotient ring

Suppose $G(x)$ is a fixed polynomial of degree n in $\mathbb{F}_p[x]$

Two poly. $a(x)$ and $b(x)$ are equivalent modulo $g(x)$ if they have the same remainder when divided by $g(x)$ (same as $g(x) \mid a(x)-b(x)$).

We construct a new ring by reconsidering the polynomials except for equivalence modulo $g(x)$.

new ring $\mathbb{F}_2/g$ which consists of the remainder classes:

$$[a(x)]_g := \{ b(x) \in \mathbb{F}_2[x] \mid a(x) \equiv b(x) \mod g(x) \}$$

since the remainders are always gonna have a lower degree than g, each polynomial is equivalent to a pol. with degree $< n$.

Therefore there are p^n elements in this ring that correspond to possible remainders

The easiest way to work with this ring is to calculate with remainders when you multiply and then take the rest dividing by $g(x)$

We can have $\emptyset$ as a result of a multiplication (if we get a multiple of $g(x)$)

eg. $[x^2]_{x^4} \cdot [x^3]_{x^4} = [x^5]_{x^4} = [0]_{x^4}$

this is only possible when $g(x)$ is not irreducible

because if $g(x)$ is irreducible and $g(x) \mid a(x)b(x)$ then $a(x)$ or $b(x)$ must be $g(x)$ in its prime factorization and so $a(x)$ or $b(x) \equiv 0 \mod g(x)$.

We can therefore use Euclide's algorithm for finding inverses

for simplification we'll use the notation $[a(x)]_g := a(\xi)$

(ξ: greek letter x_i)

all the pols with remainder $a(x)$

example ①

$g(x) := x^2 + x + 1$ then $\mathbb{F}_2[x]/g(x)$ consists of 4 elements: $0, 1, \xi, \xi+1$

these are the possible operations:

+	0	1	ξ	$\xi+1$
0	0	1	ξ	$\xi+1$
1	1	0	$\xi+1$	ξ
ξ	ξ	$\xi+1$	0	1
$\xi+1$	$\xi+1$	ξ	1	0

·	1	ξ	$\xi+1$
1	1	ξ	$\xi+1$
ξ	ξ	$\xi+1$	1
$\xi+1$	$\xi+1$	1	ξ

$(x+1)(x+1) = x^2+2x+1 = x^2+1$ $\quad g(x) = 1(x^2+1) + x$ (remainder)

example ②

$g(x) := x^2+1$, then $\mathbb{F}_2[x]/g(x)$ is no longer a field because

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

we have 4 elements $0, 1, \xi, \xi+1$

$\xi+1$ is not reversible because $(\xi+1)^2 = 0$

·	1	ξ	$\xi+1$
1	1	ξ	$\xi+1$
ξ	ξ	$\xi+1$	1
$\xi+1$	$\xi+1$	1	0

if we choose whatever irreducible polynomial of degree n $\mathbb{F}_p[X]/_{g(X)}$ and $\mathbb{F}_p[X]/_{g'(X)}$ are isomorf

this means we can identify their elements between each other
To make this cleared with an example
$\xi := [X]_{X^3+X+1}$, $\eta := [X]_{X^3+X^2+1}$ we have that:

$$(\xi+1)^3 + (\xi+1)^2 + 1 = \xi^3 + \xi^2 + \xi + 1\ \xi^2 + 1 + 1 = \xi^3 + \xi + 1 = 0$$

then ξ satisfies the same equation in the first field as η in the second.
Via this method we can find an association between their elements

$0 \longleftrightarrow 0$	$\xi^2 \longleftrightarrow \eta^2+1$
$1 \longleftrightarrow 1$	$\xi^2+1 \longleftrightarrow \eta^2$
$\xi \longleftrightarrow \eta+1$	$\xi^2+\xi \longleftrightarrow \eta^2+\eta$
$\xi+1 \longleftrightarrow \eta$	$\xi^2+\xi+1 \longleftrightarrow \eta^2+\eta+1$

theorem
for every power of prime $q := p^n$ there exist a unique finite field with q elements.
That field is called Galois field with q elements and we denote it with $\mathbb{F}_q$.

Galois fields

from now on $q = p^n$

> **theorem**
> for a finite field $\mathbb{F}_q$, $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ is a cyclic group with $q-1$ elements

This means there is an $a \in \mathbb{F}_q^* \mid \forall b \in \mathbb{F}_q^*, b = a^i \; i \in \mathbb{N}$

e.g. $\mathbb{F}_8^*$ $p=2$ $n=3$
we can take ξ itself

$$0 = 0 \qquad \xi^2 = \xi^2$$
$$1 = \xi^0 \qquad \xi^2 + 1 = \xi^6$$
$$\xi = \xi^1 \qquad \xi^2 + \xi = \xi^4$$
$$\xi + 1 = \xi^3 \qquad \xi^2 + \xi + 1 = \xi^5$$

if we now calculate the 7-th power we get 1 (it's cyclic)
In this way every element can be written as a power of ξ

$$\xi + 1 = \xi^3 = \xi^{10} = \xi^{17} \dots$$

naturally we can also consider η considering $\xi^3 = \eta$ so $\xi = \xi^{15} = \eta^5$
and we have

$$\xi^2 + \xi + 1 = \xi^5 = \eta^{25} = \eta^4$$

now consider an element $\alpha \in \mathbb{F}_q$ with $q = 2^n$. A polynomial $a(x) \in \mathbb{F}_2[X]$ for which $a(\alpha) = 0$, we call it a charatteristic polynomial for α.
The caratteristic polynomial with the lowest degree is called the minimum polynomial of α.
It can be proven that the minimum polynomial is a divisor of all the other char. pol. and it is irreducible.

example:

in $\mathbb{F}_4$ $S(x) = x^3+1$ is a charatteristic pol. for ξ because $\xi^3 = (\xi+1)\xi = \xi+1+\xi = 1$

but it's not the minimum because:

$\xi^3+1 = (x+1)(x^2+x+1)$ and $\xi^2+\xi+1 = 0$

The degree of an element of a finite field is defined as the degree of its min. pol.
Not all the el. of a finite field have the same degree.

in $\mathbb{F}_{16} = \mathbb{F}_2[X]/(x^4+x+1)$ ξ is of degree 4, but for ξ^5 we have that:

$$\xi^{10} = \xi^2(\xi+1)^2 = \xi^4+\xi^2 = \xi+1+\xi^2 = \xi(\xi+1)+1 = \xi^5+1$$

so ξ^5 is of degree 2 (with min. pol. x^2+x+1).
It follows that $\mathbb{F}_{16}$ is a subfield generated by ξ^5.
this field has 4 elements $0, 1, \xi^5, \xi^5+1$ and is isomorf with $\mathbb{F}_4$
Although $\mathbb{F}_{16}$ contains $\mathbb{F}_4$, it doesn't contain $\mathbb{F}_8$.
If so there would exist an element $\alpha \in \mathbb{F}_{16}$ such that $\alpha^7 = 1$
let's write that element as ξ^j, then $\xi^{7j} = 1 = \xi^{15}$ so 15 must be a divisor of $7j$
and therefore $15 | j$, therefore $\alpha = 1$, contradiction.

theorem

In general we can embed $\mathbb{F}_{p^m}$ in $\mathbb{F}_{p^n}$ if and only if $m | n$.
Moreover, there is only 1 subfield of $\mathbb{F}_{p^n}$ isomorf with $\mathbb{F}_{p^m}$. $\frac{p^n-1}{p^m-1}$
If ξ is a producer of $\mathbb{F}_{p^n}^*$ then $\mathbb{F}_{p^m}^*$ is generated by $\xi^{\frac{p^n-1}{p^m-1}}$

- Some elements have the same min. pol.

- it can be proven that every pol. of an el. in a finite field has many roots as its degree if α is a root then α^p, α^{p^2}, etc... are also roots. Some roots overlap

Since $\mathbb{F}_q^*$ is a cyclic group with $q-1$ elements we have that $\alpha \in \mathbb{F}_q^*$

$\forall \alpha \in \mathbb{F}_q^* : \alpha^{q-1} = 1$

this means that every element of $\mathbb{F}_q$ (including 0) is a root of $x^q - x$.
So all of the minimum polynomials of the elements of $\mathbb{F}_q$ divide $x^q - x$, $x^q - x$ is the product of all minimum pols. of the elements of $\mathbb{F}_q$

$$x^8 - x = \underbrace{x}_{0} \underbrace{(x+1)}_{1} \underbrace{(x^3+x+1)}_{\xi, \xi^2, \xi^4} \underbrace{(x^3+x^2+1)}_{\xi^3, \xi^5, \xi^6}$$

We can consider polynomials over the field $\mathbb{F}_q$, same properties as $\mathbb{F}_p[X]$.
We can use the division algo. again to define irreducible poly.

example:

calculate the quotient of $f(x) := x^4 + \xi x^3 + x^2 + (\xi+1)x + \xi$ divided by $x - \xi$ over $\mathbb{F}_4$

coeff. $f(x)$	1	ξ	1	$\xi+1$	ξ
$+$		ξ	0	ξ	ξ
$=$	1	0	1	1	0

the third line is the sum of the first 2 (over $\mathbb{F}_4$)

the coeff. of the quotient are the elements of the third line except the last

so: $x^3 + x + 1$

Working in $\mathbb{F}_{16}$

we always work in modulo 2 (therefore $-=+$)

there are several ways to look at $\mathbb{F}_{16}$

- we can represent it through the primitive poly

  $\pi(x) = x^4+x+1$

  and name α a root of $\pi(x)$. The elements of the body can then be represented with multiplicative or additive notation.

  $\mathbb{F}_{16} = \{0, 1, \alpha, \alpha^2 \dots \alpha^{14}\} = \{a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0 \mid a_i \in \mathbb{F}_2\}$

  recall: $\mathbb{F}_{15}=1$

  the relation between the elements follow the table

$0 = 0$	$\alpha^7 = \alpha^3 + \alpha + 1$
$1 = 1$	$\alpha^8 = \alpha^2 + 1$
$\alpha = \alpha$	$\alpha^9 = \alpha^3 + \alpha$
$\alpha^2 = \alpha^2$	$\alpha^{10} = \alpha^2 + \alpha + 1$
$\alpha^3 = \alpha^3$	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$
$\alpha^4 = \alpha + 1$	$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^5 = \alpha^2 + \alpha$	$\alpha^{13} = \alpha^3 + \alpha^2 + 1$
$\alpha^6 = \alpha^3 + \alpha^2$	$\alpha^{14} = \alpha^3 + 1$

- view $\mathbb{F}_{16}$ as the zero of $X^{16}-X$, which breaks down into irreducible components

  $X^{16-X} = X(X-1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1)$

  the 16 elements are the zeroes of these polynomials

- $X \to 1$
- $X^2+X+1 \to \alpha^5, \alpha^{10}$
- $X^4+X+1 \to \alpha, \alpha^2, \alpha^4+\alpha^8$
- $X^4+X^3+1 \to \alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$
- $X^4+X^3+X^2+X+1 \to \alpha^3, \alpha^6, \alpha^9, \alpha^{12}$

we call the poly. from this list of which α^k is a zero of the minimum polynomial of α^k and we annotate it $m_{\alpha^k}(X)$ eg.

$m_{\alpha^k}(X) = X^4+X^3+X^2+X+1$