Algebra: (Finite) Fields

- For prime p, $\mathbb{Z}/p$ affords addition, multiplication & division.
  → behaves like integers, reals, rationals & complex numbers.

- $(\mathbb{Z}/p)^*$: addition is absent, eg. $(p-1)+1 \notin (\mathbb{Z}/p)^*$.
  - multiplication is present.
  - division " " .

- $\mathbb{Z}/n$ for composite n : only division goes out.

Defn: A set $\mathbb{F}$, with two operations denoted by $+$ & $*$, is a <u>field</u>, if

- $\forall\, a, b \in \mathbb{F}$, $a+b \in \mathbb{F}$; $0 \in \mathbb{F}$; $-a \in \mathbb{F}$.

  (+ & * are assumed <u>associative</u>)

  unique sum

  $a+0=a$

  additive identity

  additive inverse

- $a*b \in \mathbb{F}$; $1 \in \mathbb{F}$; $(a \neq 0 \Rightarrow 1/a \in \mathbb{F})$

  unique product

  $a*1=a$

  multiplicative identity

  mult. inverse

- $*$ <u>distribute</u> on $+$: $a*(b+c) = ab + ac$.
- ($+$ & $*$ are <u>commutative</u> operations: $a+b=b+a$ & $a*b=b*a$.)

  (or <u>Abelian</u>)

~Egs. $\mathbb{F} = (\mathbb{Q}, +, *)$, $(\mathbb{R}, +, *)$, $(\mathbb{C}, +, *)$ are the <u>natural</u> fields.

▷ $\mathbb{F} = (\mathbb{Z}/p, +, *)$ is a field for <u>prime</u> p.

Pf: as seen before. $\square$

Ex: $(\mathbb{Z}/n, +, *)$ for <u>composite</u> n is <u>not</u> a field.

▷ In any field $\mathbb{F}^{\neq\{0\}}$, 0^{-1} doesn't exist.

Pf: • Suppose $\exists\, a \in \mathbb{F}$, $a * 0 = 1$

$\Rightarrow \underline{0 = 1} \Rightarrow \forall b \in \mathbb{F}$, $b * 0 = b * 1$

$\Rightarrow b = 0 \Rightarrow \mathbb{F} = \{0\} \Rightarrow$ ↯ $\square$

▷ $a*0 = a*(0+0) = a*0 + a*0$ (0 behaves like zero)

$\Rightarrow 0 = a*0, \quad \forall a \in \mathbb{F}$.

- Eg. $(\mathbb{Z}, +, *)$ is <u>not</u> a field.

▷ Only $\pm 1 \in \mathbb{Z}$ has mult. inverse.

(Cancellation)

▷ In field $\mathbb{F}$: $ab = 0 \iff a=0 \vee b=0$.

Pf: • $ab = 0$ & $a \neq 0 \Rightarrow (a^{-1}*a)b = a^{-1}*0$

$\qquad\qquad\qquad\qquad\qquad\qquad \overset{\shortparallel}{a^{-1}*(a*b)}$

$\Rightarrow b = 1*b = 0$.

- Eg. $((n \times n \text{ matrices on } \mathbb{R}), +, *)$: $\xrightarrow{\text{misses}}$ mult. inv.

$\quad\to$ non.comm.mult.

$\Rightarrow$ is <u>not</u> a field; but <u>ring</u>.

D Every field is a ring; but not conversely.

- $(\mathbb{Z}, +, *)$ is a ring.

  $(\mathbb{Z}/n, +, *)$ is a ring, $\forall n \in \mathbb{Z}$.

- <u>Defn</u>: <u>Characteristic</u> of a field $\mathbb{F}$, is smallest $n \in \mathbb{N}_{>0}$ s.t. $n \cdot 1 = 0$.
  - If it doesn't exist then define it to be <u>0</u>.
- eg. $char(\mathbb{Q}) = char(\mathbb{R}) = char(\mathbb{C}) = 0$.

  $char(\mathbb{Z}/p) = p$, for prime p.

D For finite field $\mathbb{F}$, $char(\mathbb{F}) > 0$.

Pf: • Consider the following sums:

$\{1, 2\cdot 1, 3\cdot 1, \ldots, |\mathbb{F}|\cdot 1, (|\mathbb{F}|+1)\cdot 1\}$ has a repeating element $\Rightarrow \exists\, a, b \in \mathbb{N}_{>0}$ $(a>b)$:

$$a\cdot 1 = b\cdot 1 \quad \text{in } \mathbb{F}$$

$$\Rightarrow \quad (a-b)\cdot 1 = 0 \Rightarrow n \text{ exists. } \square$$

<u>Lemma 1:</u> $\mathbb{F}$ is a field $\Rightarrow$ $\mathrm{char}(\mathbb{F}) = 0$ or prime.

Pf: • Suppose $\mathrm{char}(\mathbb{F}) > 0$:

$\Rightarrow \mathrm{char}(\mathbb{F}) =: n$. Say, $n = m_1 \cdot m_2$, where $n > m_1, m_2 > 1$.

$$\Rightarrow 0 = n\cdot 1 = m_1\cdot \underbrace{(m_2\cdot 1)}^{=:u} \Rightarrow m_2\cdot 1 = 0 \lor (m_2\cdot 1)^{-1} \in \mathbb{F}$$

$$\Rightarrow m_1\cdot u\cdot u^{-1} = 0\cdot u^{-1} = 0 \Rightarrow m_1\cdot 1 = 0 \Rightarrow \lightning. \quad \square$$

- $\mathbb{F} := (\{0\}, +, *)$ is also a <u>field</u> with $1 := 0$.

$\triangleright$ $\mathrm{char}(\mathbb{F}) = 1$.

<u>Lemma 2</u>: $\forall\, n \in \{0, 1, p \mid \text{prime } p\}$, $\exists$ field $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) = n$.

- <u>Defn</u>: The finite field of size p (prime) is denoted <u>$\mathbb{F}_p$</u> $:= (\mathbb{Z}/p, +, *)$.

(called <u>prime</u> field or <u>Galois</u> field)

$\triangleright$ $\mathbb{F}_p$ is the <u>unique</u> field of size $= p$.

- <u>Qn</u>: Are there other (finite) fields of char $= p$?

- eg. $\mathbb{F}_2 = (\mathbb{Z}/2, +, *)$; (XOR)

$0+0=0$, $0+1=1+0=1$, $1+1=0$.

$0*\_=0=\_*0$, $1*1=1$. (AND)

- Let's study <u>functions</u> over field $\mathbb{F}$.
- In particular, we study <u>polynomials</u> over $\mathbb{F}$.

Polynomials over fields

- Use a new (formal) variable $\underline{x}$: eg. $f(x) = 3x^2 + 2x - 1$.
- We can also use <u>multivariate</u>; $x_1, x_2, \dots, x_n$.

- Polynomial has coefficients, monomials & terms.

product of vars.

Defn: The set of polynomials in var. x over field $\mathbb{F}$ is called $\mathbb{F}[x]$ - polynomial ring.

- eg. $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{F}_p[x]$, ...
- eg. $\sum_{i \geq 0} x^i$ doesn't exist here.

▷ $\forall a, b \in \mathbb{F}[x]$; $a+b \in \mathbb{F}[x]$; $a * b \in \mathbb{F}[x]$.

eg. $a =: a_0 + a_1 x + a_2 x^2$; $b =: b_0 + b_1 x + b_2 x^2 + b_3 x^3$.

- eg. $a(x)+b(x) =: \sum_i \underbrace{(a_i+b_i)}_{\in \mathbb{F}} x^i \quad \in \mathbb{F}[x]$

$a(x) * b(x) =: \sum_i x^i \cdot \underbrace{\left(\sum_{j=0}^{i} a_j b_{i-j}\right)}_{\in \mathbb{F}} \quad \in$ "

convolution

- Sum requires linear-time.
- Qn: Product requires quadratic-time?

▷ $\mathbb{F}[x]$ is a ring. (not a field; $\nexists\, x^{-1}$.)

- Defn: • For $0 \neq a = a(x) \in \mathbb{F}[x]$, we can write
  $a =: a_0 + a_1 x + \dots + a_d x^d$, where $a_d \neq 0$.
  • $a_d x^d$ is the leading-term (lt) & a_d is leading-coeff (lc).

- d is the <u>degree</u> of $a(x)$. $d =: \underline{\deg(a)}$.
- $\deg(0) := -\infty$; $\forall a \neq 0$, $\deg(a) \geq 0$.

▷ $\forall a \in \mathbb{F}^*$, $\deg(a) = 0$. ▷ $\deg : \mathbb{F}[x] \to \mathbb{N} \cup \{-\infty\}$.

– eg. $\deg(x+1) = 1$; $\deg(x^2-1) = 2$;

▷ $\deg(a*b) = \deg(a) + \deg(b)$.

▷ $\deg(a+b) \leq \deg(a), \deg(b)$.

– eg. $\deg(1-1) = \deg(0) = -\infty < 0, 0$.

- $a(x)$ is <u>monic</u> if $lc(a) = 1$.

– eg. $x+1$ is monic, but $2x$ is <u>not</u>.

— Let's define division (gcd, ..., unique factors) for polynomials.

Theorem (Division): For $f, g \in \mathbb{F}[x]$, there's unique (q, r) s.t. $f = q \cdot g + r$, where $\deg f \geq \deg g$ & $\deg r < \deg g$.

$\deg q = \deg f - \deg g$

- eg. $x^2+1 / x-1$: $x^2+1 = (x+1)\underline{(x-1)} + 2$

by long-division

- eg. $1 = 1 \cdot 1 + 0$

Pf: • This is the base case; and use induction on $\deg(f)$.

- <u>Induction step:</u> $f =: f_n x^n + f_{n-1} x^{n-1} + \dots + f_0$ &
(m ≤ n) $\quad g =: g_m x^m + g_{m-1} x^{m-1} + \dots + g_0$.

- $f - g * (\overbrace{f_n g_m^{-1} * x^{n-m}}) =: f - g * u * x^{n-m}$

$$= (f_{n-1} - g_{m-1} * u)\, x^{n-1} + (f_{n-2} - g_{m-2} * u)\, x^{n-2} + \cdots$$
$$\cdots + (f_{n-m} - g_0 * u)\, x^{n-m} + f_{n-m-1} x^{n-m-1} + \dots + f_0 .$$

- Since it's $\deg < n = \deg f$; we can use the induction hypothesis to get <u>remainder</u> <u>$r(x)$</u> with $\deg r < \deg g = m$.
- This gives <u>quotient</u> $q(x) := f_n g_m^{-1} \cdot x^{n-m} + \dots$ of

degree $= n-m = \deg f - \deg g$.

$\Rightarrow \quad f = q \cdot g + r$.

(Uniqueness): Suppose not: $f = q_1 g + r_1 = q_2 g + r_2$

$\Rightarrow \quad \underbrace{(q_1 - q_2)\, g}_{\deg \ \geq \deg g} = (r_2 - r_1) \neq 0$ $\leftarrow \deg < \deg g$ $\quad \Rightarrow \lightning$

$\Rightarrow \quad r_1 = r_2 \quad \Rightarrow \quad q_1 = q_2$. $\quad \square$

▷ $x = 10$ recovers the integer-division algo.

$\Rightarrow$ Polynomials are the new integers!

- **Defn:** • For $f, g \in \mathbb{F}[x]$, $\underline{\gcd(f,g)}$ (or $\underline{(f,g)}$) is the largest degree monic polynomial $h(x)$ s.t. $h \mid f$ & $h \mid g$.

- Eg. $(1, x) = 1$; $(x, x^2+2x) = x$;
$(x+1, x^3+1) = x+1$ in $\mathbb{Q}[x]$.
$(2x, 4x) = x$.   **Note:** $3 = 2 * \underbrace{(3/2)}_{\in \mathbb{Q}[x]}$

▷ $f = q \cdot g + r \Rightarrow (f,g) = (g,r)$. [deg reduces]
- Let $\deg f \geq \deg g$, then $\deg r < \deg g \leq \deg f$.
- Continue this process to get (like Euclid):

$$f = q_1 \cdot g + r_1$$
$$g = q_2 \cdot r_1 + r_2$$
$$\vdots$$
$$r_{n-2} = q_n \cdot r_{n-1} + \underline{r_n} \in \mathbb{F}$$

▷ $r_n = 0 \Rightarrow (f,g) = r_{n-1}$

▷ $r_n \in \mathbb{F}^* \Rightarrow (f,g) = 1$.

▷ $\#\text{steps} = n \leq \deg f$.

Eg. $(x+1, x^3+1) = x+1$.

▷ [Bézout's identity] $a(x) \cdot f(x) + b(x) \cdot g(x) = \gcd(f,g)$.

Pf: (Exercise). □

▷ $\exists$ unique (a,b) s.t. $\deg a < \deg g$ & $\deg b < \deg f$.

Pf: $(a - u \cdot g) f + (b + uf) \cdot g = (f,g)$. □

- Defn: • $f \in \mathbb{F}[x]$ is reducible if $f = g_1 \cdot g_2$ s.t. $0 < \deg g_i < \deg f$.

• Else, f is called irreducible or prime in $\mathbb{F}[x]$.

- Eg. $x^2 = x \cdot x$; $x^2+1 = (x-\sqrt{-1})(x+\sqrt{-1})$

reducible over $\mathbb{C}$ irreducible over $\mathbb{R}, \mathbb{Q}$.

x^2-1 is (always) reducible; $x+1$ is irreducible over all $\mathbb{F}$.

▷ f is irreducible $\Rightarrow (f, g) = 1$ or f.

— Given polynomial $f \in \mathbb{F}[x]$.

- If f is reducible then $f =: g_1 \cdot g_2$ (nontrivial)
- If g_i " " " continue factoring.

⋮

$\Rightarrow f = c \cdot \prod_i g_i^{e_i}$, where g_i is irreducible (deg > 0) & monic in $\mathbb{F}[x]$. ($c \in \mathbb{F}$)

[Factorization]

Theorem (Unique factorization): Factorization of f into monic irreducible polynomials is <u>unique</u> (up to ordering of g_i's).

Pf: Suppose $f = c \cdot \prod g_i^{e_i} = c' \cdot \prod h_i^{e'_i}$.

$\Rightarrow lc(f) = c = c'$.

$\Rightarrow \prod_i g_i^{e_i} = \prod_i h_i^{e_i'}$ ---(1)

D $(g,h)=1$ & $g \mid h \cdot v \Rightarrow g \mid v$.

[Pf: $ag+bh=1 \Rightarrow agv+bhv=v \Rightarrow g \mid v$.]

• Apply this repeatedly in eqn.(1) for g_1:

$\Rightarrow \exists i_1, \; g_1 = h_{i_1} \Rightarrow e_1 = e'_{i_1}$

$\cdots\cdots \Rightarrow \exists \pi, \; g_1 = h_{\pi(1)}$ & $e_1 = e'_{\pi(1)}$, for <u>permutation</u> π. $\square$

$$D\,(f(x),\ x-a) = \begin{cases} x-a, & \text{if } f(a)=0 \\ 1, & \text{if } f(a)\neq 0. \end{cases}$$

- Defn: If $f(a)=0$, for $a\in\mathbb{F}$, then a is root of f. [$f(x) = q\cdot(x-a)+r \Rightarrow f(a)=r.$]

Corollary: $\#(\text{roots of } f \text{ in } \mathbb{F}) \leq \deg f.$

Pf: Let $\alpha_1,\dots,\alpha_r\in\mathbb{F}$ be distinct roots of $f(x)$.

$$\Rightarrow \quad f(x) = (x-\alpha_1)^{e_1}\cdots(x-\alpha_r)^{e_r}\cdot g(x)$$

no roots in $\mathbb{F}$

uniquely.

$$\Rightarrow \quad \deg f \geq r.$$

$\square$

Cyclic structure of $\mathbb{F}_p$

- $(\mathbb{F}_p, +) = \{1, 1+1, 1+1+1, \dots, p\cdot 1\}$

$\triangleright$ $\forall a \in \mathbb{F}_p^* := \mathbb{F}_p \setminus \{0\}$, a generates $\mathbb{F}$ under addition.

- Qn: What about $(\mathbb{F}_p^*, *)$, for prime p?
  $\exists a ? , \{a, a^2, a^3, \dots, a^{p-1}\} =? \mathbb{F}_p^*$?
- Defn: If powers of a generate $\mathbb{F}_p^*$, then we call it primitive element in $\mathbb{F}_p$.

- For $a \in \mathbb{F}_p^*$, $\underline{\mathrm{ord}(a)} =: e$ is the smallest in $\mathbb{N}_{>0}$ s.t. $a^e \equiv 1 \mod p$. ▷ $0 < e \leq p-1$.

– egs. $\mathrm{ord}(2) = 2$ in $\mathbb{F}_3$; $\mathrm{ord}(2) = 4$ in $\mathbb{F}_5$
$\mathrm{ord}(2) = 3$ in $\mathbb{F}_7$.

primitive

imprimitive

▷ If $\mathrm{ord}(a) = e$ in $\mathbb{F}_p$, then for any $n \in \mathbb{N}$,

$$a^n \equiv 1 \iff e \mid n.$$

Pf: • Let $n =: qe + r$, $0 \leq r < e$.

• $a^n \equiv 1 \Rightarrow a^{qe} \cdot a^r \equiv 1 \Rightarrow a^r \equiv 1 \Rightarrow r = 0$.

• $e \mid n \Rightarrow a^n = (a^e)^{n/e} \equiv 1^{n/e} \equiv 1$. $\square$

D $\operatorname{ord}(a) \mid (p-1)$.

Pf: $a^e \equiv 1$ & $a^{p-1} \equiv 1 \Rightarrow e \mid (p-1)$. D

D $e := \operatorname{ord}(a)$ in $\mathbb{F}_p$, and $k \in \mathbb{N}$. Then,
$\operatorname{ord}(a^k) = e/(e,k) =: e'$.

Pf: • $(a^k)^{e'} \equiv a^{ke/(e,k)} = (a^e)^{k/(e,k)} \equiv 1$.

• Suppose $(a^k)^t \equiv 1 \Rightarrow e \mid kt$

$\Longleftrightarrow e' \mid \frac{k}{(e,k)} \cdot t \quad \left[\left(e', \frac{k}{(e,k)}\right) = 1\right]$

$\Rightarrow e' \mid t \Rightarrow \operatorname{ord}(a^k) = e'$. $\square$

Theorem: For prime p, $\mathbb{F}_p$ has $\varphi(p-1)$ primitive elements.

Pf: • $\mathbb{F}_p^* := \mathbb{F}_p \setminus \{0\}$. $|\mathbb{F}_p^*| = p-1$.

• $x^{p-1} - 1 = 0$ has $(p-1)$ roots in $\mathbb{F}_p^*$.

(by Fermat's little thm.)

• $\forall a \in \mathbb{F}_p^*$, $d := \mathrm{ord}(a)$, a is root of $x^d - 1 = 0$.

(& $d \mid (p-1)$)

– Let's <u>count</u> roots of such eqns.

• Define <u>$e(d)$</u> $:= \#\{x \in \mathbb{F}_p^* \mid \mathrm{ord}(x) = d\}$.

<u>Claim</u>: $\displaystyle\sum_{d \mid (p-1)} e(d) = p-1 = |\mathbb{F}_p^*|$.

[Pf: $\forall a \in \mathbb{F}_p^*$, a contributes to $e(d)$, for <u>unique</u> d.]

Claim 2: $\sum_{d|n} \varphi(d) = n.$

[Pf: $\cdot$ $n =: \prod_i p_i^{e_i}$. LHS $= \sum_{e_i' \le e_i} \varphi\left(\prod_i p_i^{e_i'}\right)$

$= \prod_i \left(1 + \varphi(p_i) + \cdots + \varphi(p_i^{e_i})\right)$ [$\because \varphi$ is multiplicative]

$= \prod_i \left(1 + p_i - 1 + p_i^2 - p_i + \cdots\right) = \prod_i p_i^{e_i} = n.$ $\square$]

Claim 3: $\forall d | n$, $e(d) = \varphi(d)$ or 0.

[Pf: $\cdot$ Consider $a \in \mathbb{F}_p^*$, with $\mathrm{ord}(a) =: d$.

It's root of $0 \equiv x^d - 1 =: f(x)$.

$\cdot$ Also, $\{a, a^2, a^3, \cdots, a^d\}$ are all the roots of $f(x)$.

- Note that $\mathrm{ord}(a^k) = d/(k,d)$.

  So, # a^k's with ord $= d$ is: $=$

  # k's coprime to d is: $\varphi(d)$.

$\Rightarrow \quad e(d) = \varphi(d)$, if one '$a$' exists,

$\quad = 0$, else. $\square$

- Using Claims 1-3:

$$p-1 = \sum_{d|n} \varphi(d) \geq \sum_{d|n} e(d) = p-1.$$

$\Rightarrow \forall d|n,\ e(d) = \varphi(d)$.

$\Rightarrow e(p-1) = \varphi(p-1) \Rightarrow \exists$ many primitive elts. $\square$

- This idea can be generalized to more <u>abstract</u> constructions.

- Eg. $\mathbb{F}_p[x]/(x) = \mathbb{F}_p$; $\mathbb{F}_p[x]/(x^2+1) =: \{ax+b \mid a,b \in \mathbb{F}_p\}$

has addition & multiplication mod (x^2+1).

- Eg. $(x+1)x \equiv x^2+x \equiv x-1$.

- Division is also possible (sometimes?):

- eg. $x^{-1} \equiv -x$.

▷ $\mathbb{F}_p[x]/f$ is a <u>field</u> iff $f(x)$ is <u>irreducible</u> in $\mathbb{F}_p[x]$.

Pf: • Consider $a(x) \in \mathbb{F}_p[x]/f$ s.t.

$a(x) \not\equiv 0 \mod f(x)$. $\Rightarrow \gcd(a,f) = 1$.

• Extended Euclid gcd gives:

$$u \cdot a + v \cdot f = 1.$$

$\Rightarrow u \equiv a^{-1} \mod f$. $\square$

- Qn: How to find irreducible f of deg $= d$ in $\mathbb{F}_p[x]$?

▷ $\mathbb{F}_p[x]/f$ is a field of size $(p)^d$ of char. $= p$.

Denote this finite field by $\mathbb{F}_{p^d}$. [p^d-size field]

▷ Assuming $\mathbb{F}_{p^d}$ exists, $\mathbb{F}_{p^d}^*$ has $\varphi(p^d-1)$ primitive elements.

Pf: • $|\mathbb{F}_{p^d}^*| = p^d - 1$.

• Follow the pf. of $\mathbb{F}_p^*$ to get $\varphi(p^d-1)$. $\square$

▷ $\forall a \in \mathbb{F}_{p^d}^*$, $a^{p^d} \equiv a$. [Similar to $\mathbb{F}_p^*$ again.]

- Eg. $p=2$: $f := x^2+x+1 \in \mathbb{F}_2[x]$ is irred.

$\mathbb{F}_4 := \mathbb{F}_2[x]/(x^2+x+1)$ is finite field.

$= \{0, 1, x, x+1\}$; $x(x+1) = x^2+x = 1$

• $x^4 \equiv (x^2)^2 \equiv (x+1)^2 \equiv x$. $\quad$ $(x+1)^{-1}$ " $\quad$ " x^{-1} $\quad$ ▷ x & $x+1$ are primitive.

<u>Theorem:</u> $\forall$ prime p, $d \in \mathbb{N}_{>0}$, $\mathbb{F}_{p^d}$ exists.
[Or, deg-d $f(x)$ in $\mathbb{F}_p[x]$ exists.]

- <u>Defn:</u> $I(t) :=$ # irreducible deg-t monic polynomials in $\mathbb{F}_p[x]$.

▷ $g(x)$ is deg-t irreducible $\Rightarrow$ $x^{p^t} \equiv x \bmod g(x)$ & $p^t > 1$ is the <u>least</u> such power.

Pf: $x \in \mathbb{F}_p[x]/g$; which is a field of size p^t.
$\Rightarrow$ $(x)^{p^t} \equiv x$ in the field. $\square$

- $\underline{E_t(x)} := x^{p^t} - x$ "contains" deg-t irreducibles mod p.

-Pn: $x^{p^e} \equiv x \mod g(x)$ & $0 < e < t$?

$\Rightarrow v(x)^{p^e} \equiv v(x^{p^e}) \equiv v(x)$ in $\mathbb{F}_p[x]/(g(x))$, $\forall v$.

$\Rightarrow v(x)^{p^e-1} \equiv 1$ $\forall$ nonzero $v \in \mathbb{F}_p[x]/(g) =: \mathbb{F}_{p^t}$

$\Rightarrow \mathbb{F}_{p^t}^*$ has no primitive element.

$\Rightarrow$ ↯.

Lemma 1: [g as before] $x^{p^d} \equiv x \mod g(x)$

$\Longleftrightarrow t \mid d$. [i.e. $E_d(x)$ has irred. factors of deg $t \mid d$]

Pf: [$\Leftarrow$]: Let $d =: tk$.

$x^{p^t} \equiv x \Rightarrow (x^{p^t})^{p^t} \equiv x^{p^t} \equiv x$

$\Rightarrow x^{p^{3t}} \equiv x^{p^t} \equiv x \Rightarrow \cdots \Rightarrow x^{p^{tk}} \equiv x.$

[$\Rightarrow$]: Let $d =: k \cdot t + r^{<t}$ & $x^{p^{kt+r}} \equiv x$.

$\Rightarrow (x^{p^{kt}})^{p^r} \equiv x^{p^r} \equiv x \mod g(x)$.

$\Rightarrow r = 0$. $\square$

— Let's consider the factors of $x^{p^d} - x$ in $\mathbb{F}_p[x]$:

$\triangleright$ $\sum_{t|d} t \cdot I(t) = p^d$.

Pf: • Let factorization of $x^{p^d} - x$ be:

$= f_1(x) \cdot f_2(x) \cdots f_d(x)$, where

$f_t :=$ product of irreducibles of $\deg = t \mid d$.

$\Rightarrow \deg(f_t) = I(t) \cdot t \Rightarrow$ gives LHS! $\square$

Lemma 2: $\forall s \in \mathbb{N}$, $s \cdot I(s) = \sum_{d|s} \mu(s/d) \cdot p^d$.
(Möbius inversion formula)

Pf: • RHS $= \sum_{d|s} \mu(s/d) \cdot \left(\sum_{t|d} t \cdot I(t) \right)$

$= \sum_{t|s} t \cdot I(t) \cdot \left(\sum_{s' | \frac{s}{t}} \mu(s') \right)$ $= 0$, unless $\frac{s}{t} = 1$.

$s =: \underbrace{t \cdot t'}_{d} \cdot s'$

$= s \cdot I(s) = \text{LHS}$. $\square$

- eg. $2 \cdot I(2) = p^2 - p$; $4 \cdot I(4) = p^4 - p^2$;
$6 \cdot I(6) = p^6 - p^3 - p^2 + 1$. $\triangleright$ $\forall s$, $I(s) > 0$.

▷ $I(d) \approx p^d/d$, $\forall d > 1$.

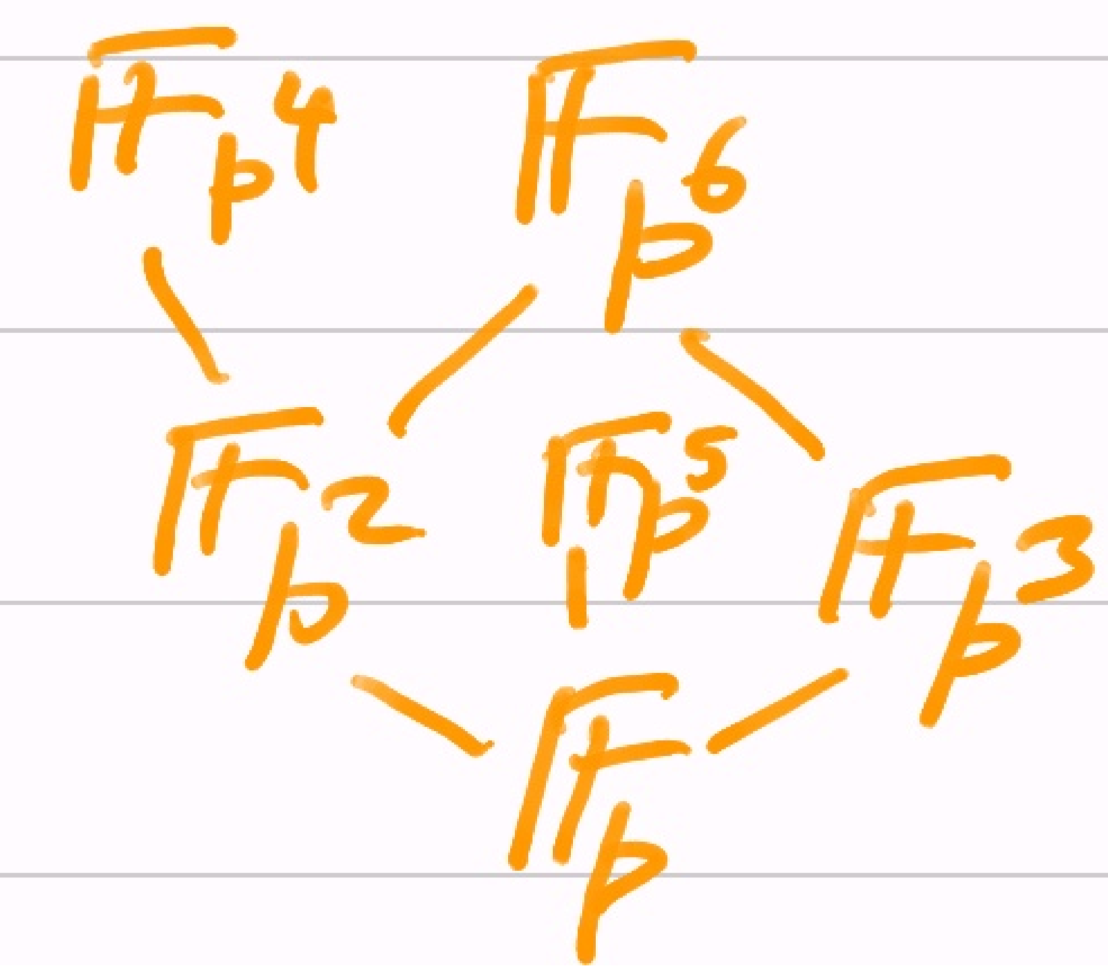
[Prime density estimate in $\mathbb{F}_p[x]$] $= \dfrac{\#(\text{deg-}d \text{ polynomials mod } p)}{d}$.

— This is like the prime-number density estimate $\pi(x)/x \approx 1/\log x$.

⤳ degree is the new #digits! □

— Defn: $\mathbb{F}_p \cup \mathbb{F}_{p^2} \cup \mathbb{F}_{p^3} \cup \dots =: \overline{\mathbb{F}_p}$ is the algebraic closure of $\mathbb{F}_p$.

infinite



Error-Correcting Codes

- We can outline this application of $\mathbb{F}_p^d$.

Qn: How can messages be sent on a corrupt channel? (assuming error-rate < 50%) We want efficiency.

$$A \xrightarrow{+e} B$$

$$m \qquad\qquad m+e$$

$$m \in \{0,1\}^k$$

- Eg. Channel makes $\leq \frac{1}{2}$ errors & A wants to send "god". god $\longrightarrow$ goo

- god $\xrightarrow{\varepsilon}$ ggoodd $\rightsquigarrow$ gdoodd
- $\xrightarrow{\varepsilon}$ gggoooddd $\rightsquigarrow$ ggdoooudde

↳ Repetition code: For #errors $\leq t$, it requires repeating a letter $(2t+1)$ times.

k length $\longrightarrow$ $n := k(2t+1)$ code

Qn: Can you make n closer to k? (eg. $n \approx k \cdot \log k$)

- We want to design better & fast, encoding algorithm; with a (fast) decoding algorithm. (for code + error)

- Think of <u>message</u> as a string in $\mathbb{F}_q^k$; where $q =$ p-power & prime p.
- <u>Encoding</u> $E : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$ $(n > k)$

$$(a_0, a_1, \dots, a_{k-1}) \longmapsto (b_0, b_1, \dots, b_{n-1})$$

- Consider polynomial $f_{\bar{a}}(X) := a_0 + a_1 X + \dots + a_{k-1} X^{k-1} + X^k$
- Let $\mathbb{F}_q \supseteq \{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\} \leftarrow$ elements.
- $b_0 := f(\alpha_0)$; $b_1 := f(\alpha_1)$; - - - ; $b_{n-1} = f(\alpha_{n-1})$.

$$E : \underset{\in \mathbb{F}_q^k}{\bar{a} := (a_0, a_1, \dots, a_{k-1})} \longmapsto \underset{\in \mathbb{F}_q^n}{(f_{\bar{a}}(\alpha_0), \dots, f_{\bar{a}}(\alpha_{n-1}))}.$$

$f_{\bar{a}}$!!

Claim: If messages $\bar{a} \neq \bar{a}'$ the $f_{\bar{a}}$ & $f_{\bar{a}'}$ differ in $n-k+1$ places.

Pf: • $f_{\bar{a}}$ & $f_{\bar{a}'}$ are the same at i-th place iff $f_{\bar{a}}(\alpha_i) = f_{\bar{a}'}(\alpha_i)$.

iff $(f_{\bar{a}} - f_{\bar{a}'})(\alpha_i) = 0$ [Let $g(X) := f_{\bar{a}}(X) - f_{\bar{a}'}(X)$.]

$\Rightarrow g(\alpha_i) = 0$.

$\Rightarrow$ #(equal-places) gives #(roots of g).

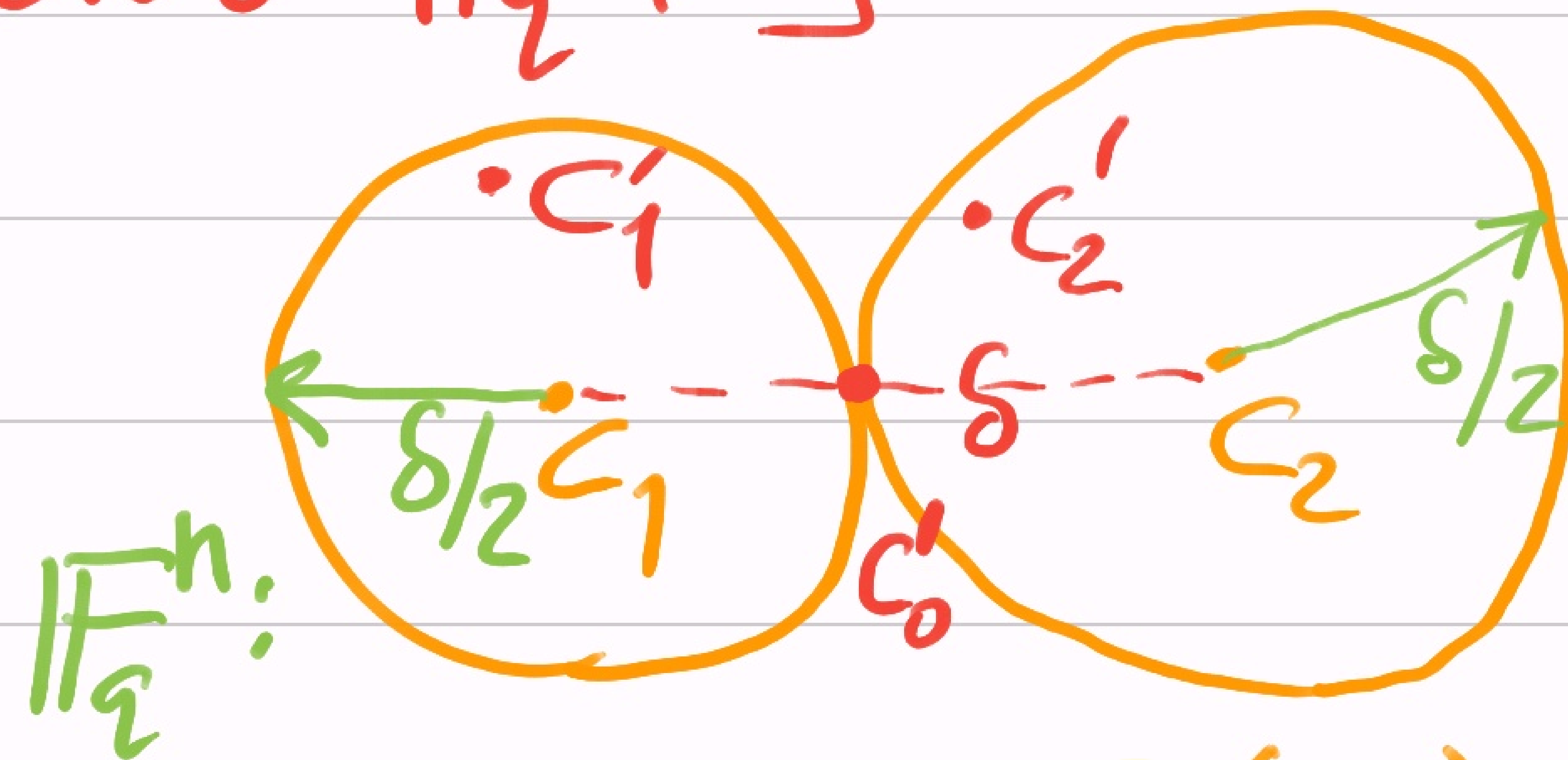
• Note: $\deg(g) \leq k-1$.

$\Rightarrow$ #(roots of g) $\leq k-1$.

$\Rightarrow f_{\bar{a}}, f_{\bar{a}'}$ differ in $n-k-1)$ places! $\square$

Theorem [Reed-Solomon, 1960]: RS-code has distance $n-k+1 =: \delta$.

[It's an (k,n,δ)-code over $\mathbb{F}_q$.]



$c_i := E(m_i)$

▷ Bob can (theoretically) deduce c_1 from c_1', & c_2 from c_2'.

But, cannot deduce information from c_0'.

▷ (k,n,δ)-code is good up to errors $< \delta/2$; so, $< (n-k+1)/2$ errors in length $= n$.

- Eg. For 49% errors: $0.49 = \dfrac{\left(\frac{n-k}{2}\right)}{n}$

$\Rightarrow \quad 0.98n = n-k$

$\Rightarrow \quad 0.02n = k \Rightarrow n = \dfrac{k}{0.02} = 50k.$

▷ RS-code has a fast decoding algorithm.
(Exercise: Read it for fun.)

Eg. $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$

$f(Y) := Y^2+Y+1$ in $\mathbb{F}_4[Y]$.

$\hookrightarrow$ has root x & x^2.

$= (Y-x).(Y-x^2)$ $\rightsquigarrow$ That's like $\mathbb{R}$ to $\mathbb{R}(\sqrt{-1}) = \mathbb{C}$