

Remark k

$$x \in \overline{F_p} \subseteq F_{p^2!} \subseteq \dots \subseteq \overline{F_{p^n!}}$$

~~$F_{p^{2!}}$~~

$$q = p^k$$

$$y \in \overline{F_q} \subseteq F_{q^{2!}} \subseteq \dots \subseteq \overline{F_{q^{n!}}}$$

$$\overline{F_q} = \bigcup_{n \in N} F_{q^{n!}}$$

Note:

$$\overline{F_p} = \overline{F_q}$$

could also define

$$\overline{F_p} = F_p \subseteq F_{p^2} \subseteq F_{p^4}$$

$$\subseteq \dots \subseteq F_{p^{2^n}} \subseteq$$

$$F_p \subseteq F_q$$

$$r_p^s - r_p^t$$

$$\Leftrightarrow s \mid \underline{t}$$

Recall

$$0 := \emptyset$$

$$1 = \{\emptyset\}$$

$$2 := \{\emptyset, \{\emptyset\}\}$$

⋮

$$\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \dots$$

Def: A relation on a set X
is a subset $R \subseteq X \times X$.

When $(x, y) \in R$ we

denote $x R y$ or $x \sim_R y$

Ex: a function $f: X \rightarrow X$

gives rise to a relation:

$$x \sim_R y \Leftrightarrow f(x) = y.$$

Def: A relation R on X
is called an equivalence relation
if

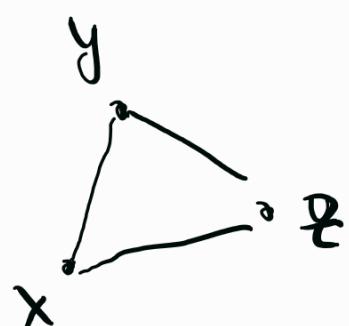
1) Reflexive: $\forall x \in X, x \sim_R x$.

2) Symmetric: $\forall x, y \in X, x \sim_R y$
 $\Leftrightarrow y \sim_R x$.

3) Transitive: $\forall x, y, z \in X$

$$x \sim_R y \wedge y \sim_R z$$

$$\Rightarrow x \sim_R z$$



Ex: if $f: X \rightarrow X$, f is id_X

ie $\exists x_0 \in X$ s.t. $f(x_0) \neq x_0$

Then the relation $x \sim_R y$

(\supset) $f(x) = y$ is not
reflexive.

Ex $X = \mathbb{Z}$, $n \in \mathbb{N}$

$$R = \equiv \pmod{n}$$

ie for $x, y \in \mathbb{Z}$

$$x \sim_R y \Leftrightarrow x \equiv y \pmod{n}.$$

1) $\forall x \in \mathbb{Z} \quad x \equiv x \pmod{n}$

2) $\forall x, y \in \mathbb{Z} \quad x \equiv y \pmod{n}$

$$\Leftrightarrow y \equiv x \pmod{n}$$

3) $\forall x, y, z \text{ if } x \equiv y \pmod{n}$

and $y \equiv z \pmod{n}$

then $x \equiv z \pmod{n}$.

Construction Let \sim be

an equivalence relation on a set X . For $x \in X$, denote

$$[x] = \{y \in X \mid x \sim y\} \subseteq X$$

and call it equivalence class

of $\underline{\underline{X}}$

eg $X = \mathbb{Z}$, \sim is $\underline{\underline{\text{mod } n}}$

$$[n+1] = [1] = \{1, n+1, 2n+1, \dots, 1-n, 1-n^2, \dots\}$$

Note : 1) if $a, b \in [x]$ then

$$a \sim x \wedge b \sim x \\ \stackrel{\text{sym}}{\Rightarrow} x \sim b \stackrel{\text{Trans.}}{\Rightarrow} a \sim b$$

2) If $x, y \in X$ are s.t h

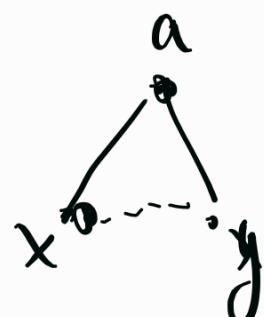
$$\underline{\underline{[x] \neq [y]}}. \text{ If } \underline{\underline{a \in [x] \cap [y]}}$$

Then $a \sim x \wedge a \sim y$

$$\Rightarrow x \sim a \wedge a \sim y$$

Tr.

$$\Rightarrow x \sim y$$



$$\Rightarrow [x] = [y]$$

(bcs if $t \in [x]$ $t \sim x$

then since $x \sim y$ it

follows that $t \sim y$ i.e

$$t \in [y]$$

$$\text{So } [x] = [y] \iff x \sim y$$

and if $[x] \neq [y]$

as subsets of X then

$$[x] \cap [y] = \emptyset.$$

Thus, the collection (of sets)

$$\underline{\mathcal{Q}} = \{ [x] \subseteq X \mid x \in X \}$$

$$(\text{recall } \{0, 1\} = \{0, 1, 1\})$$

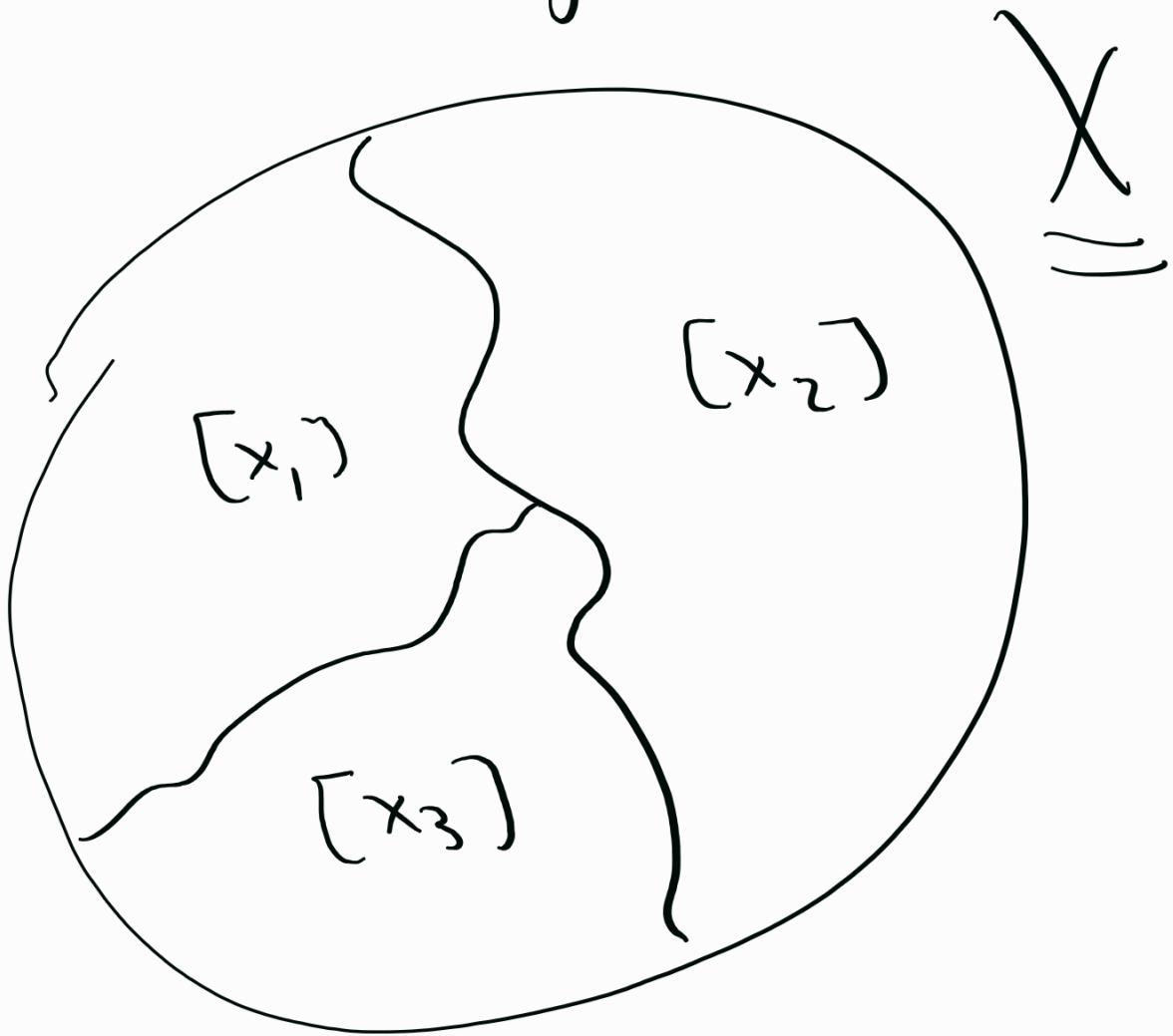
is a partition of X

$$\text{in that } \bigcup_{x \in X} [x] = X$$

and $x, y \in X$, either

$$[x] = [y] \quad \text{or}$$

$$[x] \cap [y] = \emptyset$$



Ex: $X = \mathbb{Z}$, w/ $\equiv \pmod{n}$

$$\mathbb{Q} = \{ [x] \mid x \in \mathbb{Z} \}$$

$$= \{ \dots, (-1), (0), (1), (2), \dots \}$$

remove repetitions.

$$= \{ [0], [1], \dots, [n-1] \}$$

\mathbb{Z}_n

$$= \{ [n], [n+1], \dots, [2n-1] \}$$

= - - - -

Notation: Given a set X

w/ an equivalence rel. \sim

We denote

$$X/\sim := Q = \left\{ [x] \mid x \in X \right\}$$

and call it the quotient

set

Ex: $X = \{1, \dots, 7\}$



$$\begin{aligned}X/\sim &= \{ [1], [2], [5] \} \\&= \{ [4], [3], [6] \}.\end{aligned}$$

Note if \mathcal{P} is a partition

of a set X , ie

$$\mathcal{P} = \{V_i\}_{i \in I}$$

and $\forall i, j \in I \text{ if } i \neq j$

then $U_i \cap U_j = \emptyset$

$$+ \underbrace{\bigcup_{i \in I} U_i}_{} = X$$

We can define an equivalence rel. on X by

for $x, y \in X$, $x \sim y$

$\Leftrightarrow \exists i \in I$ s.t.

$x, y \in U_i$



$\Rightarrow 1-1$ correspondence

equivalence rel's
on X

bijection \longleftrightarrow Partitions of X

Recall: If (G, \cdot) is an abelian gp and $H \leq G$.

for $x \in G$, the H coset of x is

$$(x+H) \underset{\equiv}{=} x \cdot H = \{ \underset{\equiv}{\underline{x \cdot h}} \mid h \in H \}.$$

We defined

$$G/H = \{ \underset{\equiv}{\underline{xH}} \}_{x \in G}$$

Lemma $x \cdot H = yH \iff x \cdot y^{-1} \in H$

G/H

has an abelian gp
structure, given by

$$\text{unit} = e \cdot H = H$$

$$\begin{aligned} \text{mult} \quad (xH) \cdot (yH) &= (xy)H \\ &= \{ (xy)h \mid h \in H \} \\ &= \{ x(yh) \mid h \in H \} \dots \end{aligned}$$

inverse of xH is $x^{-1}H$

Claim: The collection $\{ xH \mid x \in G \}$

is a partition of G .

$$\cup xH \subseteq G \subseteq xH \subseteq G$$

Proof: 1) Want: $\bigcup_{x \in G} xH = G$

to indeed, if $x \in G$
 then $x = x \cdot e \in xH$ ($e \in H$)

2) if $x, y \in G$ and

$xH \neq yH$, want: $xH \cap yH = \emptyset$

Suppose (towards contradiction)

that $a \in xH \cap yH$.

Then $\exists h, h' \in H$ s.th

$$x \cdot h = a = y \cdot h'$$

Thus $x = y(h'h)^{-1} \in yH$

$$y = x(h(h')^{-1}) \in xH$$

Finally : if $\alpha = xh_1 \in xH$

Then $\alpha = y(h^{-1}h_1) \cdot h_1 \in yH$

and similarly if $\beta = yh_2 \in yH$

then $\beta = x(h(h^{-1})) \cdot h_2 \in xH$

so $xH \subseteq yH \Rightarrow$

$yH \subseteq xH$

$xH = yH \cdot 1 //$

$n \in \mathbb{N}$ Ex: $G = \mathbb{Z}$, $H = n\mathbb{Z}$

$G/H = \left\{ \frac{0+n\mathbb{Z}}{n\mathbb{Z}}, \frac{1+n\mathbb{Z}}{n\mathbb{Z}}, \dots, \frac{(n-1)+n\mathbb{Z}}{n\mathbb{Z}} \right\}$

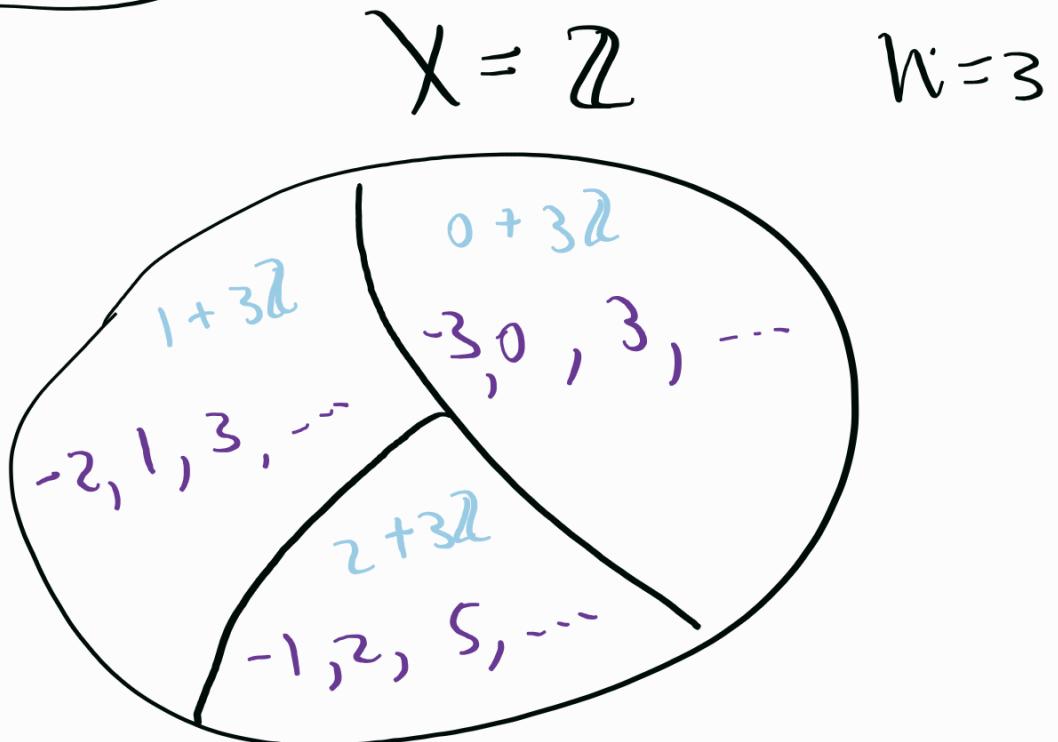
By the above

$\mathbb{Z}/n\mathbb{Z}$ is a partition

/H

of \mathbb{Z} hence gives
 rise to an equivalence
relation:

eg



$$a, b \in \mathbb{Z} \quad a \sim b$$

$$(\Rightarrow) \quad a \equiv b \pmod{3}$$

Example: \mathbb{F} a field

$$\phi(x) \in \mathbb{F}[x] \quad \deg \phi = n$$

$$\mathbb{F}[x]/(\phi) \stackrel{\text{as set}}{=} \quad$$

$$\left\{ r(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \middle| \begin{matrix} a_i \\ \in \mathbb{F} \end{matrix} \right\}$$

if ϕ is prime then

mod- ϕ arithmetic defines

a field structure on

$$K = \rightarrow \mathbb{F}[x]/(\phi)$$

$$\phi(X) = (X-a) \psi(X)$$

We could set: for

$$f(x), g(x) \in \mathbb{F}[x]$$

$$f \approx g \iff f \equiv g \pmod{\phi}$$

Exercise: \sim_{ϕ} is an equivalence relation

$$\boxed{F[x]} / \sim_{\phi} = \left\{ [f] \mid f \in F[x] \right\}$$

\equiv

$$= \left\{ [r] \mid \deg r < n = \deg \phi \right\}$$

$$[f] = [g] \Leftrightarrow$$

$$f \sim_{\phi} g$$

$$\Leftrightarrow f \equiv g \pmod{\phi}$$

$$f = q_1 \phi + r_1 \quad \deg r_1 < n$$

$$g = q_2 \phi + r_2 \quad \deg r_2 < n$$

$$f = r_2' \quad \text{mod } \phi$$

$$f \equiv g \pmod{\phi}$$

$$(=) \quad r_1 = r_2$$

$$\text{if } r_1 \neq r_2$$

$$\text{then } [r_1] \neq [r_2]$$

i.e.

$$\mathbb{F}[x]/\sim_{\phi}$$

$\deg \phi = n$

$$= \left\{ [r] \mid \deg r < n \right\}$$



W₀ ⁴ ₁ ₂ ₃ ₄ ₅ ₆ ₇ ₈ ₉ ₁₀ ₁₁ ₁₂ ₁₃ ₁₄ ₁₅ ₁₆ ₁₇ ₁₈ ₁₉ ₂₀ ₂₁ ₂₂ ₂₃ ₂₄ ₂₅ ₂₆ ₂₇ ₂₈ ₂₉ ₃₀ ₃₁ ₃₂ ₃₃ ₃₄ ₃₅ ₃₆ ₃₇ ₃₈ ₃₉ ₄₀ ₄₁ ₄₂ ₄₃ ₄₄ ₄₅ ₄₆ ₄₇ ₄₈ ₄₉ ₅₀ ₅₁ ₅₂ ₅₃ ₅₄ ₅₅ ₅₆ ₅₇ ₅₈ ₅₉ ₆₀ ₆₁ ₆₂ ₆₃ ₆₄ ₆₅ ₆₆ ₆₇ ₆₈ ₆₉ ₇₀ ₇₁ ₇₂ ₇₃ ₇₄ ₇₅ ₇₆ ₇₇ ₇₈ ₇₉ ₈₀ ₈₁ ₈₂ ₈₃ ₈₄ ₈₅ ₈₆ ₈₇ ₈₈ ₈₉ ₉₀ ₉₁ ₉₂ ₉₃ ₉₄ ₉₅ ₉₆ ₉₇ ₉₈ ₉₉ ₁₀₀ ₁₀₁ ₁₀₂ ₁₀₃ ₁₀₄ ₁₀₅ ₁₀₆ ₁₀₇ ₁₀₈ ₁₀₉ ₁₁₀ ₁₁₁ ₁₁₂ ₁₁₃ ₁₁₄ ₁₁₅ ₁₁₆ ₁₁₇ ₁₁₈ ₁₁₉ ₁₂₀ ₁₂₁ ₁₂₂ ₁₂₃ ₁₂₄ ₁₂₅ ₁₂₆ ₁₂₇ ₁₂₈ ₁₂₉ ₁₃₀ ₁₃₁ ₁₃₂ ₁₃₃ ₁₃₄ ₁₃₅ ₁₃₆ ₁₃₇ ₁₃₈ ₁₃₉ ₁₄₀ ₁₄₁ ₁₄₂ ₁₄₃ ₁₄₄ ₁₄₅ ₁₄₆ ₁₄₇ ₁₄₈ ₁₄₉ ₁₅₀ ₁₅₁ ₁₅₂ ₁₅₃ ₁₅₄ ₁₅₅ ₁₅₆ ₁₅₇ ₁₅₈ ₁₅₉ ₁₆₀ ₁₆₁ ₁₆₂ ₁₆₃ ₁₆₄ ₁₆₅ ₁₆₆ ₁₆₇ ₁₆₈ ₁₆₉ ₁₇₀ ₁₇₁ ₁₇₂ ₁₇₃ ₁₇₄ ₁₇₅ ₁₇₆ ₁₇₇ ₁₇₈ ₁₇₉ ₁₈₀ ₁₈₁ ₁₈₂ ₁₈₃ ₁₈₄ ₁₈₅ ₁₈₆ ₁₈₇ ₁₈₈ ₁₈₉ ₁₉₀ ₁₉₁ ₁₉₂ ₁₉₃ ₁₉₄ ₁₉₅ ₁₉₆ ₁₉₇ ₁₉₈ ₁₉₉ ₂₀₀ ₂₀₁ ₂₀₂ ₂₀₃ ₂₀₄ ₂₀₅ ₂₀₆ ₂₀₇ ₂₀₈ ₂₀₉ ₂₁₀ ₂₁₁ ₂₁₂ ₂₁₃ ₂₁₄ ₂₁₅ ₂₁₆ ₂₁₇ ₂₁₈ ₂₁₉ ₂₂₀ ₂₂₁ ₂₂₂ ₂₂₃ ₂₂₄ ₂₂₅ ₂₂₆ ₂₂₇ ₂₂₈ ₂₂₉ ₂₃₀ ₂₃₁ ₂₃₂ ₂₃₃ ₂₃₄ ₂₃₅ ₂₃₆ ₂₃₇ ₂₃₈ ₂₃₉ ₂₄₀ ₂₄₁ ₂₄₂ ₂₄₃ ₂₄₄ ₂₄₅ ₂₄₆ ₂₄₇ ₂₄₈ ₂₄₉ ₂₅₀ ₂₅₁ ₂₅₂ ₂₅₃ ₂₅₄ ₂₅₅ ₂₅₆ ₂₅₇ ₂₅₈ ₂₅₉ ₂₆₀ ₂₆₁ ₂₆₂ ₂₆₃ ₂₆₄ ₂₆₅ ₂₆₆ ₂₆₇ ₂₆₈ ₂₆₉ ₂₇₀ ₂₇₁ ₂₇₂ ₂₇₃ ₂₇₄ ₂₇₅ ₂₇₆ ₂₇₇ ₂₇₈ ₂₇₉ ₂₈₀ ₂₈₁ ₂₈₂ ₂₈₃ ₂₈₄ ₂₈₅ ₂₈₆ ₂₈₇ ₂₈₈ ₂₈₉ ₂₉₀ ₂₉₁ ₂₉₂ ₂₉₃ ₂₉₄ ₂₉₅ ₂₉₆ ₂₉₇ ₂₉₈ ₂₉₉ ₃₀₀ ₃₀₁ ₃₀₂ ₃₀₃ ₃₀₄ ₃₀₅ ₃₀₆ ₃₀₇ ₃₀₈ ₃₀₉ ₃₁₀ ₃₁₁ ₃₁₂ ₃₁₃ ₃₁₄ ₃₁₅ ₃₁₆ ₃₁₇ ₃₁₈ ₃₁₉ ₃₂₀ ₃₂₁ ₃₂₂ ₃₂₃ ₃₂₄ ₃₂₅ ₃₂₆ ₃₂₇ ₃₂₈ ₃₂₉ ₃₃₀ ₃₃₁ ₃₃₂ ₃₃₃ ₃₃₄ ₃₃₅ ₃₃₆ ₃₃₇ ₃₃₈ ₃₃₉ ₃₄₀ ₃₄₁ ₃₄₂ ₃₄₃ ₃₄₄ ₃₄₅ ₃₄₆ ₃₄₇ ₃₄₈ ₃₄₉ ₃₅₀ ₃₅₁ ₃₅₂ ₃₅₃ ₃₅₄ ₃₅₅ ₃₅₆ ₃₅₇ ₃₅₈ ₃₅₉ ₃₆₀ ₃₆₁ ₃₆₂ ₃₆₃ ₃₆₄ ₃₆₅ ₃₆₆ ₃₆₇ ₃₆₈ ₃₆₉ ₃₇₀ ₃₇₁ ₃₇₂ ₃₇₃ ₃₇₄ ₃₇₅ ₃₇₆ ₃₇₇ ₃₇₈ ₃₇₉ ₃₈₀ ₃₈₁ ₃₈₂ ₃₈₃ ₃₈₄ ₃₈₅ ₃₈₆ ₃₈₇ ₃₈₈ ₃₈₉ ₃₉₀ ₃₉₁ ₃₉₂ ₃₉₃ ₃₉₄ ₃₉₅ ₃₉₆ ₃₉₇ ₃₉₈ ₃₉₉ ₄₀₀ ₄₀₁ ₄₀₂ ₄₀₃ ₄₀₄ ₄₀₅ ₄₀₆ ₄₀₇ ₄₀₈ ₄₀₉ ₄₁₀ ₄₁₁ ₄₁₂ ₄₁₃ ₄₁₄ ₄₁₅ ₄₁₆ ₄₁₇ ₄₁₈ ₄₁₉ ₄₂₀ ₄₂₁ ₄₂₂ ₄₂₃ ₄₂₄ ₄₂₅ ₄₂₆ ₄₂₇ ₄₂₈ ₄₂₉ ₄₃₀ ₄₃₁ ₄₃₂ ₄₃₃ ₄₃₄ ₄₃₅ ₄₃₆ ₄₃₇ ₄₃₈ ₄₃₉ ₄₄₀ ₄₄₁ ₄₄₂ ₄₄₃ ₄₄₄ ₄₄₅ ₄₄₆ ₄₄₇ ₄₄₈ ₄₄₉ ₄₅₀ ₄₅₁ ₄₅₂ ₄₅₃ ₄₅₄ ₄₅₅ ₄₅₆ ₄₅₇ ₄₅₈ ₄₅₉ ₄₆₀ ₄₆₁ ₄₆₂ ₄₆₃ ₄₆₄ ₄₆₅ ₄₆₆ ₄₆₇ ₄₆₈ ₄₆₉ ₄₇₀ ₄₇₁ ₄₇₂ ₄₇₃ ₄₇₄ ₄₇₅ ₄₇₆ ₄₇₇ ₄₇₈ ₄₇₉ ₄₈₀ ₄₈₁ ₄₈₂ ₄₈₃ ₄₈₄ ₄₈₅ ₄₈₆ ₄₈₇ ₄₈₈ ₄₈₉ ₄₉₀ ₄₉₁ ₄₉₂ ₄₉₃ ₄₉₄ ₄₉₅ ₄₉₆ ₄₉₇ ₄₉₈ ₄₉₉ ₅₀₀ ₅₀₁ ₅₀₂ ₅₀₃ ₅₀₄ ₅₀₅ ₅₀₆ ₅₀₇ ₅₀₈ ₅₀₉ ₅₁₀ ₅₁₁ ₅₁₂ ₅₁₃ ₅₁₄ ₅₁₅ ₅₁₆ ₅₁₇ ₅₁₈ ₅₁₉ ₅₂₀ ₅₂₁ ₅₂₂ ₅₂₃ ₅₂₄ ₅₂₅ ₅₂₆ ₅₂₇ ₅₂₈ ₅₂₉ ₅₃₀ ₅₃₁ ₅₃₂ ₅₃₃ ₅₃₄ ₅₃₅ ₅₃₆ ₅₃₇ ₅₃₈ ₅₃₉ ₅₄₀ ₅₄₁ ₅₄₂ ₅₄₃ ₅₄₄ ₅₄₅ ₅₄₆ ₅₄₇ ₅₄₈ ₅₄₉ ₅₅₀ ₅₅₁ ₅₅₂ ₅₅₃ ₅₅₄ ₅₅₅ ₅₅₆ ₅₅₇ ₅₅₈ ₅₅₉ ₅₆₀ ₅₆₁ ₅₆₂ ₅₆₃ ₅₆₄ ₅₆₅ ₅₆₆ ₅₆₇ ₅₆₈ ₅₆₉ ₅₇₀ ₅₇₁ ₅₇₂ ₅₇₃ ₅₇₄ ₅₇₅ ₅₇₆ ₅₇₇ ₅₇₈ ₅₇₉ ₅₈₀ ₅₈₁ ₅₈₂ ₅₈₃ ₅₈₄ ₅₈₅ ₅₈₆ ₅₈₇ ₅₈₈ ₅₈₉ ₅₉₀ ₅₉₁ ₅₉₂ ₅₉₃ ₅₉₄ ₅₉₅ ₅₉₆ ₅₉₇ ₅₉₈ ₅₉₉ ₆₀₀ ₆₀₁ ₆₀₂ ₆₀₃ ₆₀₄ ₆₀₅ ₆₀₆ ₆₀₇ ₆₀₈ ₆₀₉ ₆₁₀ ₆₁₁ ₆₁₂ ₆₁₃ ₆₁₄ ₆₁₅ ₆₁₆ ₆₁₇ ₆₁₈ ₆₁₉ ₆₂₀ ₆₂₁ ₆₂₂ ₆₂₃ ₆₂₄ ₆₂₅ ₆₂₆ ₆₂₇ ₆₂₈ ₆₂₉ ₆₃₀ ₆₃₁ ₆₃₂ ₆₃₃ ₆₃₄ ₆₃₅ ₆₃₆ ₆₃₇ ₆₃₈ ₆₃₉ ₆₄₀ ₆₄₁ ₆₄₂ ₆₄₃ ₆₄₄ ₆₄₅ ₆₄₆ ₆₄₇ ₆₄₈ ₆₄₉ ₆₅₀ ₆₅₁ ₆₅₂ ₆₅₃ ₆₅₄ ₆₅₅ ₆₅₆ ₆₅₇ ₆₅₈ ₆₅₉ ₆₆₀ ₆₆₁ ₆₆₂ ₆₆₃ ₆₆₄ ₆₆₅ ₆₆₆ ₆₆₇ ₆₆₈ ₆₆₉ ₆₇₀ ₆₇₁ ₆₇₂ ₆₇₃ ₆₇₄ ₆₇₅ ₆₇₆ ₆₇₇ ₆₇₈ ₆₇₉ ₆₈₀ ₆₈₁ ₆₈₂ ₆₈₃ ₆₈₄ ₆₈₅ ₆₈₆ ₆₈₇ ₆₈₈ ₆₈₉ ₆₉₀ ₆₉₁ ₆₉₂ ₆₉₃ ₆₉₄ ₆₉₅ ₆₉₆ ₆₉₇ ₆₉₈ ₆₉₉ ₇₀₀ ₇₀₁ ₇₀₂ ₇₀₃ ₇₀₄ ₇₀₅ ₇₀₆ ₇₀₇ ₇₀₈ ₇₀₉ ₇₁₀ ₇₁₁ ₇₁₂ ₇₁₃ ₇₁₄ ₇₁₅ ₇₁₆ ₇₁₇ ₇₁₈ ₇₁₉ ₇₂₀ ₇₂₁ ₇₂₂ ₇₂₃ ₇₂₄ ₇₂₅ ₇₂₆ ₇₂₇ ₇₂₈ ₇₂₉ ₇₃₀ ₇₃₁ ₇₃₂ ₇₃₃ ₇₃₄ ₇₃₅ ₇₃₆ ₇₃₇ ₇₃₈ ₇₃₉ ₇₄₀ ₇₄₁ ₇₄₂ ₇₄₃ ₇₄₄ ₇₄₅ ₇₄₆ ₇₄₇ ₇₄₈ ₇₄₉ ₇₅₀ ₇₅₁ ₇₅₂ ₇₅₃ ₇₅₄ ₇₅₅ ₇₅₆ ₇₅₇ ₇₅₈ ₇₅₉ ₇₆₀ ₇₆₁ ₇₆₂ ₇₆₃ ₇₆₄ ₇₆₅ ₇₆₆ ₇₆₇ ₇₆₈ ₇₆₉ ₇₇₀ ₇₇₁ ₇₇₂ ₇₇₃ ₇₇₄ ₇₇₅ ₇₇₆ ₇₇₇ ₇₇₈ ₇₇₉ ₇₈₀ ₇₈₁ ₇₈₂ ₇₈₃ ₇₈₄ ₇₈₅ ₇₈₆ ₇₈₇ ₇₈₈ ₇₈₉ ₇₉₀ ₇₉₁ ₇₉₂ ₇₉₃ ₇₉₄ ₇₉₅ ₇₉₆ ₇₉₇ ₇₉₈ ₇₉₉ ₈₀₀ ₈₀₁ ₈₀₂ ₈₀₃ ₈₀₄ ₈₀₅ ₈₀₆ ₈₀₇ ₈₀₈ ₈₀₉ ₈₁₀ ₈₁₁ ₈₁₂ ₈₁₃ ₈₁₄ ₈₁₅ ₈₁₆ ₈₁₇ ₈₁₈ ₈₁₉ ₈₂₀ ₈₂₁ ₈₂₂ ₈₂₃ ₈₂₄ ₈₂₅ ₈₂₆ ₈₂₇ ₈₂₈ ₈₂₉ ₈₃₀ ₈₃₁ ₈₃₂ ₈₃₃ ₈₃₄ ₈₃₅ ₈₃₆ ₈₃₇ ₈₃₈ ₈₃₉ ₈₄₀ ₈₄₁ ₈₄₂ ₈₄₃ ₈₄₄ ₈₄₅ ₈₄₆ ₈₄₇ ₈₄₈ ₈₄₉ ₈₅₀ ₈₅₁ ₈₅₂ ₈₅₃ ₈₅₄ ₈₅₅ ₈₅₆ ₈₅₇ ₈₅₈ ₈₅₉ ₈₆₀ ₈₆₁ ₈₆₂ ₈₆₃ ₈₆₄ ₈₆₅ ₈₆₆ ₈₆₇ ₈₆₈ ₈₆₉ ₈₇₀ ₈₇₁ ₈₇₂ ₈₇₃ ₈₇₄ ₈₇₅ ₈₇₆ ₈₇₇ ₈₇₈ ₈₇₉ ₈₈₀ ₈₈₁ ₈₈₂ ₈₈₃ ₈₈₄ ₈₈₅ ₈₈₆ ₈₈₇ ₈₈₈ ₈₈₉ ₈₉₀ ₈₉₁ ₈₉₂ ₈₉₃ ₈₉₄ ₈₉₅ ₈₉₆ ₈₉₇ ₈₉₈ ₈₉₉ ₉₀₀ ₉₀₁ ₉₀₂ ₉₀₃ ₉₀₄ ₉₀₅ ₉₀₆ ₉₀₇ ₉₀₈ ₉₀₉ ₉₁₀ ₉₁₁ ₉₁₂ ₉₁₃ ₉₁₄ ₉₁₅ ₉₁₆ ₉₁₇ ₉₁₈ ₉₁₉ ₉₂₀ ₉₂₁ ₉₂₂ ₉₂₃ ₉₂₄ ₉₂₅ ₉₂₆ ₉₂₇ ₉₂₈ ₉₂₉ ₉₃₀ ₉₃₁ ₉₃₂ ₉₃₃ ₉₃₄ ₉₃₅ ₉₃₆ ₉₃₇ ₉₃₈ ₉₃₉ ₉₄₀ ₉₄₁ ₉₄₂ ₉₄₃ ₉₄₄ ₉₄₅ ₉₄₆ ₉₄₇ ₉₄₈ ₉₄₉ ₉₅₀ ₉₅₁ ₉₅₂ ₉₅₃ ₉₅₄ ₉₅₅ ₉₅₆ ₉₅₇ ₉₅₈ ₉₅₉ ₉₆₀ ₉₆₁ ₉₆₂ ₉₆₃ ₉₆₄ ₉₆₅ ₉₆₆ ₉₆₇ ₉₆₈ ₉₆₉ ₉₇₀ ₉₇₁ ₉₇₂ ₉₇₃ ₉₇₄ ₉₇₅ ₉₇₆ ₉₇₇ ₉₇₈ ₉₇₉ ₉₈₀ ₉₈₁ ₉₈₂ ₉₈₃ ₉₈₄ ₉₈₅ ₉₈₆ ₉₈₇ ₉₈₈ ₉₈₉ ₉₉₀ ₉₉₁ ₉₉₂ ₉₉₃ ₉₉₄ ₉₉₅ ₉₉₆ ₉₉₇ ₉₉₈ ₉₉₉ ₁₀₀₀

repetitions.

$$\mathbb{Z}_n = \{ 0, \dots, n-1 \}$$

+ mod n

$$\mathbb{Z} / \sim_{\text{mod } n} = \{ [0], \dots, [n-1] \}$$

+

$$[a] + [b]$$

$$= [a + b]$$

$$= [a + b \text{ mod } n]$$

$$\mathbb{F}[x] / (\phi)$$

$$= \{ r \mid \text{remainder of poly's} \}$$

↑
mod ϕ

$$\mathbb{F}[x] / \sim_{\phi}$$

$$= \{ [r] \mid \text{remainder poly's} \}$$

Mod ϕ

$$[r_1] + [r_2] := [r_1 + r_2]$$

$$[r_1] \cdot [r_2] = [r_1 \cdot r_2]$$

↑

