

Week 14

## The DLP in $(G, \circ)$

①

Problem Instance:  $I = (G, \alpha, \beta)$ , where  $G$  is a finite group with group operation  $\circ$ ,  $\alpha \in G$  and  $\beta \in H$ , where  $H = \{\alpha^i : i \geq 0\}$  is the subgroup of  $G$  generated by  $\alpha$ .

Objective: find the unique integer  $a$  s.t.  $0 \leq a \leq |H| - 1$  &  $\alpha^a = \beta$ , where the notation  $\alpha^a$  means  $\underbrace{\alpha \circ \alpha \circ \dots \circ \alpha}_{a \text{ times}}$

We will denote this integer  $a$  by  $\log_{\alpha} \beta$ .

## Generalized ElGamal Public-Key Cryptosystem

Let  $G$  be a finite group with group operation  $\circ$ , and let  $\alpha \in G$  be an element s.t. the DLP in  $H$  is intractable, where  $H = \{\alpha^i : i \geq 0\}$  is the subgroup generated by  $\alpha$ .

$\beta \in G$ ,  $G = \alpha \times \alpha$ , & define  $X = \{(a, \alpha^a, \beta) : \alpha^a = \beta\}$

$\alpha, \alpha, \beta$  are public

$a$  is secret

for  $K = (G, \alpha, a, \beta)$ , & for a (secret) random number  $k \in \mathbb{Z}_{1/M}$

define  $e_K(x, k) = (y_1, y_2)$

where  $y_1 = \alpha^k$ ,  $y_2 = \alpha^k \beta^k$

for a cipher-text  $y = (y_1, y_2)$ , define

$d_K(y) = y_2 \circ (y_1)^{-1}$

$p$  prime

$$\mathbb{Z}_p^*, \mathbb{Z}_{p-1}.$$

(2)

$(\mathbb{Z}_p^*)$  cyclic of order  $p-1$ .  
isomorphic to  $(\mathbb{Z}_{p-1}, +)$

$$\phi: \mathbb{Z}_p^* \rightarrow \mathbb{Z}_{p-1}.$$

DLP in  $\mathbb{Z}_p^*$

$$\alpha, \beta = \alpha^a \rightarrow \text{find } a$$

DLP in  $\mathbb{Z}_{p-1}$

$$\phi(\alpha), \phi(\beta) = a \phi(\alpha) \rightarrow \text{find } a \text{ is feasible.}$$

$$\begin{aligned} & \phi(x) \equiv \phi(y \pmod p) \\ & \Rightarrow (\phi(x) + \phi(y)) \pmod{p-1} \end{aligned} \quad \text{Extended Euclidean Algm.}$$

If we can find an efficient algm. to compute isomorphism  $\phi$ , we can solve DLP in

$(\mathbb{Z}_p^*) \rightarrow$  No known general method to efficiently compute the isomorph  $\phi$ .

Careful about the choice of your group.

A ~~is~~

$\downarrow$

$$H = \langle \alpha \rangle \quad \phi: H \rightarrow \mathbb{Z}_{|H|}$$

DLP in  $H$  can be solved efficiently

- DLP may be easy or difficult depending on the representation of the cyclic group that is used.
- Study other groups
  - $G_F(p^n)$  when DLP seems to be intractable.
  - Elliptic curve group.

(3)

## Polynomial Rings

- $R \rightarrow$  commutative ring

- $f(x) = a_n x^n + \dots + a_2 x^2 + a_1 x + a_0, \quad a_i \in R, \quad n > 0$

$\downarrow$   
poly. of deg.  $m$  if  $m$  is the  
largest int. s.t.  $a_m \neq 0$ .

$m = \deg(f(x))$   
 $a_m \rightarrow$  leading co-efficient of  $f(x)$ .

- $f(x) = a_0$  (const. poly)

$a_0 \neq 0, \quad \deg(f(x)) = 0.$

$a_0 = 0$

- $f(x) \rightarrow$  zero poly.

$\deg(f(x)) = -\infty$ .

- $f(x)$  is monic poly. if leading co-efficient of  $f(x)$  is 1.

Def'n:  $R \rightarrow$  commutative ring

$R[x] \rightarrow$  polynomial ring formed by the set of all polynomials in  $x$  having coefficients from  $R$ .

$+ , \cdot \rightarrow$  two operations with coefficient arithmetic

performed in  $R$ .

Example:  $\mathbb{Z}, \mathbb{Z}_n (n > 1)$  rings;  $\mathbb{Z}_p[x] \rightarrow$  poly. ring when  $p$  is prime

Example:  $f(x) = x^3 + x + 1, \quad g(x) = x^2 + x \in \mathbb{Z}_2[x]$

Working in  $\mathbb{Z}_2[x]$ ,

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

$\ell \quad f(x) \cdot g(x) = x^5 + x^4 + x^3 + x$

Example:

④

$$g(x) = x^4 + 3x + 2$$
$$h(x) = x^2 + 2 \quad \text{in}$$

$\mathbb{Z}_5[x]$ .

$$\begin{array}{c} h(x) \qquad g(x) \qquad r(x) \\ x^2+2 \mid x^4+3x+2 \qquad \qquad \qquad | x^2+3 \\ \underline{-x^4 \cancel{-2x^2}} \qquad \qquad \qquad \pm 2x^2 \\ \hline 3x^2+3x+2 \\ \underline{-3x^2} \qquad \qquad \qquad +1 \\ \hline 3x-1 \leftarrow \deg < 2 \end{array}$$

$r(x)$

$$g(x) = h(x)q(x) + r(x), \quad \deg r(x) < \deg h(x).$$

$$g(x) \bmod h(x) = 3x - 1$$

$$g(x) \div h(x) = x^2 + 3.$$

- $\cdot F \rightarrow$  arbitrary field. (5)  $| F[x]$  has many properties in common with  $\mathbb{Z}$ .
- $\cdot F[x] \rightarrow$  poly. ring

Defn: Let  $f(x) \in F[x]$  be a poly. of degree at least 1. Then  $f(x)$  is said to be irreducible over  $F$  if it cannot be written as the product of two polynomials in  $F[x]$ , each of positive degree.

### Division Algo. for polynomials

If  $g(x), h(x) \in F[x]$ , with  $h(x) \neq 0$ , then ordinary long poly. long division of  $g(x)$  by  $h(x)$  yields poly's  $q(x) + r(x) \in F[x]$  p.t.

$$g(x) = q(x)h(x) + r(x), \text{ where } \deg(r(x)) < \deg(h(x))$$

Moreover  $q(x), r(x)$  are unique.

$q(x) \rightarrow$  quotient  $\rightarrow g(x) \text{ div } h(x)$ .

$r(x) \rightarrow$  remainder

$\downarrow$   
 $g(x) \text{ mod } h(x)$

### Example:

$$\begin{aligned} g(x) &= x^6 + x^5 + x^3 + x^2 + x + 1 \\ h(x) &= x^4 + x^3 + 1 \end{aligned} \quad \text{in } \mathbb{Z}_2[x].$$

$$\begin{array}{r} x^4 + x^3 + 1 \mid x^6 + x^5 + x^3 + x^2 + x + 1 \\ \hline x^6 + x^5 + x^2 \\ \hline x^3 + x + 1 \end{array}$$

i.e.  $g(x) \text{ mod } h(x) = x^3 + x + 1$ ,

$$\begin{aligned} \therefore g(x) &= x^2 h(x) + (x^3 + x + 1) \\ q(x) &= x^2 \\ r(x) &= x^3 + x + 1 \\ g(x) \text{ div } h(x) &= x^2. \end{aligned}$$

Defn: If  $g(x), h(x) \in F[x]$ , then  $\textcircled{6}$   $h(x)$  divides  $g(x)$ , ~~if~~

$$h(x) | g(x)$$

if  $g(x) \bmod h(x) = 0$ .

Defn: If  $g(x), h(x) \in F[x]$ , then  $g(x)$  is said to be congruent to  $h(x)$  modulo  $f(x)$  if

$$f(x) | g(x) - h(x).$$

$$g(x) \equiv h(x) \pmod{f(x)}.$$

Fact (Properties of congruence)

$$\forall g(x), h(x), g_1(x), h_1(x), p(x) \in F[x]$$

(i)  $g(x) \equiv h(x) \pmod{f(x)}$  iff  $g(x) \neq h(x)$  leave the same remainder upon division by  $f(x)$ .

$$(ii) (\text{reflexivity}) \quad g(x) \equiv g(x) \pmod{f(x)}$$

$$(iii) (\text{symmetry}) \quad \text{if } g(x) \equiv h(x) \pmod{f(x)} \text{ then } h(x) \equiv g(x) \pmod{f(x)}$$

$$(iv) (\text{transitivity}) \quad \text{if } g(x) \equiv h(x) \pmod{f(x)} \text{ and } h(x) \equiv p(x) \pmod{f(x)},$$

$$(v) \quad \text{If } g(x) \equiv g_1(x) \pmod{f(x)} \text{ and } h(x) \equiv h_1(x) \pmod{f(x)},$$

$$\text{then } g(x) + h(x) \equiv g_1(x) + h_1(x) \pmod{f(x)} \text{ and } g(x)h(x) \equiv g_1(x)h_1(x) \pmod{f(x)}$$

$f(x) \in F[x] \rightarrow$  a fixed poly.,

$g(x) \bmod f(x)$

$$g_1(x)$$

$$g(x) \in F[x]$$

~~$f(x)$  is irreducible~~

$F[x]/(f(x)) \rightarrow$  quotient ring  
if  $f(x)$  is irreducible.

$x_1(x)$	$r_2(x)$	
.	.	
		$r_i(x)$

Defn.  $F[x]/(f(x))$  denotes the set of (equivalence classes of) polynomials in  $F[x]$  of degree less than  $n = \deg(f(x))$ . Addition & multiplications are performed modulo  $f(x)$ .

fact:  $F[x]/(f(x))$  is a commutative ring

Fact: If  $f(x)$  is irreducible over  $F$ , then  $F[x]/(f(x))$  is a field.

## finite fields

$F \rightarrow$  field with finite no. of elements

$\mathbb{Z} \rightarrow$  not field, a ring as  $2 \cdot k = 1$  for no  $k \in \mathbb{Z}$

$\mathbb{Z}_p \rightarrow$  field when  $p$  is prime.

$\text{GF}(p^n)$

finite  $F \rightarrow |F| = p^n$ ,  $p$  prime  
 $\leftarrow$  for some  $n \in \mathbb{Z}_+$   
 of finite fields.  
 Existence & Uniqueness theorem  
 with  $|F| = p^n$  if  $F$  is unique.

(i) If  $F$  is a finite field, then  $F$  contains  $p^m$  elements for some prime  $p$  & integer  $m \geq 1$

(ii) for every prime power  $p^m$  there is a unique (up to isomorphism) finite field of order  $p^m$ . This field is denoted by  $F_{p^m}$  or sometimes by  $\text{GF}(p^m)$ .

$\text{GF}(p) = \mathbb{Z}_p$   
 ↓ Construction

$\text{GF}(p^n)$

$\text{GF}(p^m)$

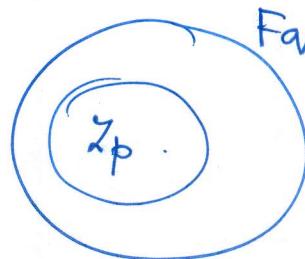
Two fields are isomorphic if they are structurally the same, although the representation of their field elements may be different.

- $\mathbb{Z}_p$  is a field if  $p$  is prime, hence every field of order  $p$  is isomorphic to  $\mathbb{Z}_p$ .
- $F_p \xrightarrow{\text{identified}} \mathbb{Z}_p$ .

Fact If  $F_q$  is a finite field of order  $q = p^m$ ,  $p$  prime, then  $p \rightarrow \text{characteristic of } F_q$ .

Moreover,  $F_q$  contains a copy of  $\mathbb{Z}_p$  as a subfield.

Hence,  $F_q$  can be viewed as an extension field of  $\mathbb{Z}_p$  of degree  $m$ .

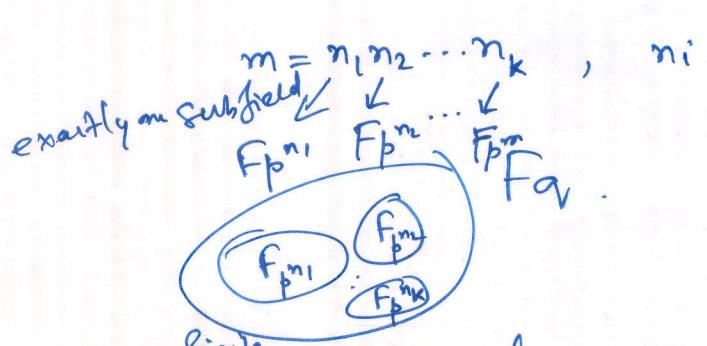


$F_q = F_{p^m}$ .  
 ↓  
 extension field of  
 $Z_p$  of deg.  $m$ .

Fact (subfields of a finite field)

$F_q \rightarrow$  a finite field of order  $n = p^m$ .

↓  
 every element in  
 $F_q$  is expressible  
 as a poly of deg  
 $< m$ .



$a \in F_q$  is in  $F_{p^{n_i}}$   
 iff  $a^{p^{n_i}} = a$ .

Let  $F_q$  be a finite field of order  $q = p^m$ . Then every subfield of  $F_q$  has order  $p^n$ , for some tve divisor  $n$  of  $m$ .  
Conversely, if  $n$  is a tve divisor of  $m$ , then  $\exists$  exactly one subfield of  $F_q$  of order  $p^n$ ; an element  $a \in F_q$  is in the one subfield  $F_{p^n}$  iff  $a^{p^n} = a$ .

Def<sup>n</sup> The non-zero elements of  $\text{F}_q$  form a group under multiplication called the multiplicative group of  $\text{F}_q$ , denoted by  $\text{F}_q^*$ .

fact  $\text{F}_q^*$  is cyclic of order  $q-1$ . Hence  $a^{q-1} = a \neq 0$  in  $\text{F}_q$ .

Def<sup>n</sup> A generator of the cyclic group  $\text{F}_q^*$  is called a primitive element or generator of  $\text{F}_q$ .

fact If  $a, b \in \text{F}_q$ , a finite field of characteristic  $p$ , then  $(a+b)^p = a^p + b^p \quad \forall p \geq 0$ .

## Addition & Multiplication in $\mathbb{Z}_p[x]$

(10)

$$f(x) = \sum_{i=0}^n a_i x^i, \quad g(x) = \sum_{i=0}^m b_i x^i$$

i)  $f(x) + g(x) = \sum_{i=0}^N c_i x^i$  with  $N = \max(n, m)$   
 $c_i \equiv a_i + b_i \pmod{p}$ .

ii)  $f(x)g(x) = \sum_{i=0}^{n+m} d_i x^i$  with  $d_i \equiv \sum_{j=0}^i a_j b_{i-j} \pmod{p}$

Exercise find  

$$\left( x^5 + 4x^3 + 2 \right) + \left( 3x^3 + 2x \right) \quad \left\{ \text{in } \mathbb{Z}_5[x] \right.$$

$$\left. \left( x^5 + 4x^3 + 2 \right) \cdot \left( 3x^3 + 2x \right) \right\}$$

## Proposition

If  $p$  prime,  $f, g \in \mathbb{Z}_p[x]$ ,  
then  $\deg(f \cdot g) = \deg(f) + \deg(g)$ .

## Vector Representation of Polynomials

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}_p[x]$$

$$\sim [a_n, a_{n-1}, \dots, a_1, a_0]$$

$$g = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0 \in \mathbb{Z}_p[x]$$

$$\sim [b_m, b_{m-1}, \dots, b_1, b_0]$$

$$f+g \sim [c_N, c_{N-1}, \dots, c_1, c_0], \quad c_i \equiv a_i + b_i \pmod{p}$$

$$N = \max(n, m) \quad \text{for } 0 \leq i \leq N.$$

$$\begin{aligned}
 f \cdot g &= f \cdot \sum_{i=0}^m b_i x^i \\
 &= \bigoplus_{i=0}^m \bigoplus_{j=0}^m f \cdot b_i x^i \\
 &= \sum_{i=0}^m b_i [a_n, a_{n-1}, \dots, a_0, \underbrace{0, 0, \dots, 0}_{k \text{ zeros.}}]
 \end{aligned}$$

(11)

$$\begin{aligned}
 f(x) &= a_0 + a_1 x + \dots + a_n x^n \\
 &\sim [a_0, a_1, \dots, a_n] \\
 f(x) \cdot x^k &= a_0 x^k + a_1 x^{k+1} + \dots + a_n x^{k+n} \\
 &\sim [a_0, a_1, \dots, a_n] \\
 f(x^k) &= a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \\
 &\sim [a_n, a_{n-1}, \dots, a_1, a_0] \\
 f \cdot x^k &= a_n x^{n+k} + a_{n-1} x^{n+k-1} + \dots + a_1 x^{k+1} + a_0 x^k \\
 &\sim [a_n, a_{n-1}, \dots, a_1, a_0, \underbrace{0, 0, \dots, 0}_{k \text{ zeros.}}]
 \end{aligned}$$

Ex Find  $x^5 + x \pmod{x^3 + x + 1}$   
in  $\mathbb{Z}_2[x]$ .

Method 1 Go for long division  
(Division Alg.)

$$\begin{array}{r|rr}
 & x^5 + x & x^2 + 1 \\
 \hline
 x^3 + x + 1 & \underline{-} & \\
 & x^5 & + x^3 + x^2 \\
 & \underline{-} & \\
 & x^3 + x^2 + x & \\
 & \underline{-} & \\
 & x^3 & + x + 1 \\
 & \underline{-} & \\
 & x^2 + 1 & \rightarrow r(x)
 \end{array}$$

$$\begin{aligned}
 b_k x^k &\sim [b_k, \underbrace{0, 0, \dots, 0}_{k \text{ zeros.}}] \\
 \therefore [a_n, a_{n-1}, \dots, a_1, a_0] \cdot [b_k, \underbrace{0, 0, \dots, 0}_{k \text{ zeros.}}] \\
 &= b_k [a_n, a_{n-1}, \dots, a_1, a_0, \underbrace{0, 0, \dots, 0}_{k \text{ zeros.}}] \\
 \rightarrow f \cdot b_k x^k
 \end{aligned}$$

$$\text{Ans} \rightarrow x^3 + 1$$

Method 2 (Reduction)

$$x^5 + x \equiv x^2 \cdot (x+1) + x$$

$$\equiv x^3 + x^2 + x \equiv x+1 + x^2 + x \equiv x+1 \pmod{x^3 + x + 1}$$

$$\begin{aligned}
 x^3 + x + 1 &\equiv x^3 + x + 1 \pmod{0} \quad (\text{mod } x^3 + x + 1) \\
 \therefore x^3 &\equiv x + 1 \pmod{x^3 + x + 1} \\
 &\equiv x+1 \pmod{\frac{x^3 + x + 1}{x-1}}
 \end{aligned}$$

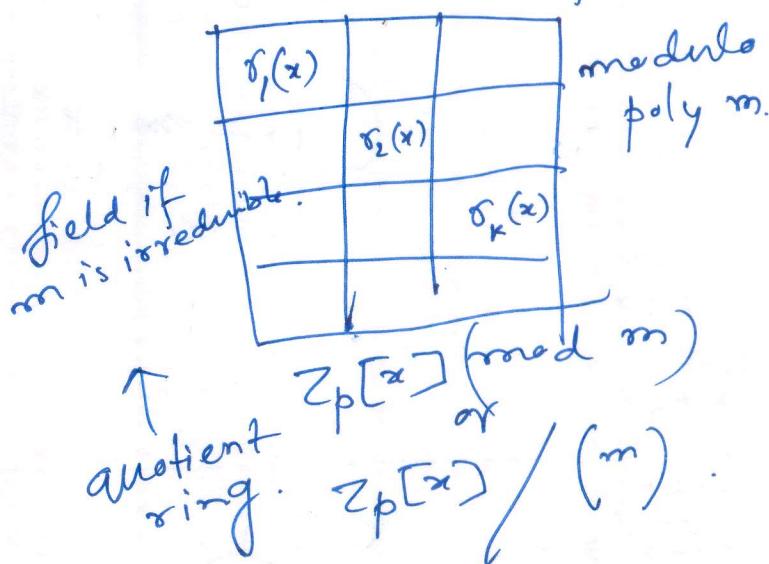
# Building finite fields from $\mathbb{Z}_p[x]$

(12)

	Integers	Polynomials
infinite ring	$\mathbb{Z}$	$\mathbb{Z}_p[x]$
fixed ring element	$m$ (integer $> 1$ )	$m$ (poly of deg $> 0$ )
finite modular ring	$\mathbb{Z}_m$ (has $m$ elmts)	$\mathbb{Z}_p[x] \pmod{m}$ (has $p^{\deg(m)}$ elements)
When is finite modular ring a field?	$\mathbb{Z}_m$ is a field iff $m = \text{a prime } p$	$\mathbb{Z}_p[x] \pmod{m}$ is a field iff $m$ is an irreducible poly.
	↓ this field is $\mathbb{Z}_p$ or $GF(p)$ from $\mathbb{Z}$	↓ this field is $GF(p^n)$ from $\mathbb{Z}_p[x]$ when $n = \deg(m)$ .

↓

Parallels between construction of finite fields  $GF(p)$  from  $\mathbb{Z}$ ,  $GF(p^n)$  and  $GF(p^n)$  from  $\mathbb{Z}_p[x]$ .



$\otimes$	0	1	$x$	$x+1$
0	0	0	0	0
1	0	1	$x$	$x+1$
$x$	0	$x$	$x+1$	1
$x+1$	0	$x+1$	1	$x$

$GF(4) = GF(2^2) = \mathbb{Z}_2[x] / (x^2 + x + 1)$ .

Power

Binary

Poly.

0

1

$x$

$x+1$

00

01

10

11

$x^0$

$x$

$x^2$

$$GF(8) = GF(2^3) = \mathbb{Z}_2[x] / (\text{irred } f(x))$$

$f(x) \rightarrow$  irr. poly of

deg. 3.

poly. in  $\mathbb{Z}_2[x]$  of degree 3

$$\begin{array}{l} x^3, x^3+1, \\ (x+1)(x^2+x+1) \end{array}$$

$$\begin{array}{l} x^3+x^2+x+1 \\ x^3+x^2+x \\ x^3+x^2 \\ x^3+x^2+x+1 \\ x^3+x^2+x \\ x^3+x^2+x+1 \\ x^3+x^2+x+1 \end{array}$$

$$\begin{array}{l} x^3+x^2+x+1 \\ x^3+x^2+x+1 \\ x^3+x^2+x+1 \\ x^3+x^2+x+1 \\ x^3+x^2+x+1 \end{array}$$

$$\begin{array}{l} x^3+x^2+x+1 \\ x^3+x^2+x+1 \\ x^3+x^2+x+1 \\ x^3+x^2+x+1 \\ x^3+x^2+x+1 \end{array}$$

$$x^3+x^2+x+1$$

$$x^3+x^2+x+1$$
</div

Example.  $\text{GF}(2^2)$  construction. (17)  
 $\mathbb{Z}_2[x] \rightarrow$  find an irreducible poly. of degree 2  
 $\perp_m$ .

$$\mathbb{Z}_2[x]/(m) \rightarrow \text{GF}(2^2).$$

polys in  $\mathbb{Z}_2[x]$  of degree 2

$$x^2, x^2+1, x^2+x, x^2+x+1.$$

$\downarrow$        $\downarrow$        $\downarrow$        $\downarrow$   
 $x \cdot x$      $(x+1)(x+1)$      $x(x+1)$     to prove it is  
irreducible.

$$f(x) g(x)$$

$$\begin{matrix} \leftarrow & \downarrow \\ \deg 1 & \deg 1 \end{matrix} \Rightarrow \text{only deg 1 polys}$$

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

$$\equiv 1 \pmod{x}$$

$$\equiv 1 \pmod{x+1}.$$

$$\therefore x \nmid x^2+x+1, \text{ also } x+1 \nmid x^2+x+1.$$

$x^2+x+1$  is irreducible.

$\Rightarrow$   $x^2+x+1$  is irreducible.

$$\begin{aligned} \text{GF}(2^2) &= \text{GF}(4) \text{ construction} \\ &= \mathbb{Z}_2[x]/(x^2+x+1). \\ &= \{0, 1, x, x+1\} \end{aligned}$$

$+ \backslash$	0	1	$x$	$x+1$
0	0	1	$x$	$x+1$
1	1	0	$x+1$	$x$
$x$	$x$	$x+1$	0	1
$x+1$	$x+1$	$x$	1	0

Example

(15)

$GF(2^3) = GF(8)$  Construction

We need to find a poly  $f(x) \in \mathbb{Z}_2[x]$  of degree 3, which is irreducible.

Such poly must have const. term 1.

$$f_1(x) = x^3 + 1 = (x+1)(x^2+x+1)$$

$$f_2(x) = x^3 + x + 1$$

$$f_3(x) = x^3 + x^2 + 1$$

$$f_4(x) = x^3 + x^2 + x + 1 = (x^2+1)(x+1).$$

both are irreducible.

check

$x, x+1, x^2, x^2+1, x^2+x$ ,  $x^2+x+1$   
not factors of  $f_2(x)$  or  $f_3(x)$ .

↓  
apply division algm/reduction method.

$$f_2(x) = x^3 + x + 1 \\ = x(x^2+1) + 1 \Rightarrow x, x^2+1 \nmid f_2(x)$$

$$= x(x+1)^2 + 1 \Rightarrow x+1 \nmid f_2(x)$$

$$= x^2 \cdot x + x + 1 = x^3 + x + 1 = 1 \Rightarrow x^2 \nmid f_2(x)$$

$$x^2 \nmid x^2+1 \nmid f_2(x)$$

$$\begin{array}{r} x^2+x | x^3+x^2+x+1 \\ \underline{x^3+x^2} \\ x^2+x+1 \end{array}$$

$$\begin{array}{r} x^2+x+1 | x^3+x^2+x+1 \\ \underline{x^3+x^2} \\ x^2+x+1 \end{array}$$

$$\begin{array}{r} x^2 | x^3+x^2+x+1 \\ \underline{x^3+x^2} \\ x^2+x+1 \end{array}$$

$$GF(8) = GF(2^3) = \mathbb{Z}_2[x] / (\text{mod } f(x))$$

(16)

$$f(x) = x^3 + x + 1 \text{ or } x^3 + x^2 + 1$$

$\rightarrow$  deg 3 irreducible poly.

$$= \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}.$$

$$x^6 = \frac{(x^2+1)}{x+1}$$

$$x^3 = x+1$$

<u>poly</u>	<u>Binary</u>	<u>Power</u>
0	00 0	$x^0$
1	00 1	
$x$	01 0	$x^1$
$x+1$	01 1	$x^3$
$x^2$	10 0	$x^2$
$x^2+1$	10 1	$x^6$
$x^2+x$	11 0	$x^4$
$x^2+x+1$	11 1	$x^5$

~~$$x^4 = x^2 + x$$~~

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

$$x^5 = x^3 + x^2 \\ = x+1 + x^2$$

cyclic group of order 7.



$$(GF(8) \setminus \{0\}; \cdot)$$

Multiplicative group of non-zero poly in  $GF(8)$

$\rightarrow$  cyclic gr. of order 7.

as 7 is prime, any non-zero element is a generator of this multiplication gr.

i.e. a primitive element of the field.

$x \rightarrow$  primitive element  
every other non-zero element is represented as  $x^i$  for some  $i$ .

	1	$x$	$x+1$	$x^2$	$x^2+1$	$x^2+x$	$x^2+x+1$	$x^7=1$
1	1	$x$	$x+1$	$x^2$	$x^2+1$	$x^2+x$	$x^2+x+1$	
$x$		$x$	$x^2$	$x^2+x$	$x+1$		$x^2+x+1$	$x^2+1$
$x^2-x+1$			$x+1$					
$x^3$				$x^2$				
$x^6$				$x^2+1$				
$x^4-x+x^2$				$x^2+x$				
$x^9-x+x+1$				$x^2+x+1$				
	1	$x$	$x+1$	$x^2$	$x^2+1$	$x^2+x$	$x^2+x+1$	$x^7=1$
	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$
.	001	010	011	100	101	110	111	
1	001	<u>001</u>	010	011	100	101	110	
$x$	010	010	100	110	011	<u>001</u>	111	101
$x^3$	011	011	110	101	111	100	<u>001</u>	010
$x^2$	100	100	011	111	110	010	101	<u>001</u>
$x^6$	101	101	<u>001</u>	<del>100</del>	010	111	011	110
$x^4$	110	110	111	<u>001</u>	101	011	010	100
$x^5$	111	111	101	010	<u>001</u>	110	100	011

$$GF(8) = \langle x^10 \rangle = \langle x \rangle$$