Week 14

The DLP in $(G, \circ)$

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 α.

Objective: find the unique integer a s.t. $0 \leq a \leq |H|-1$ & $\alpha^a = \beta$, where the notation α^a means

$$\underbrace{\alpha \circ \alpha \circ \cdots \circ \alpha}_{a \text{ times}}$$

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 α.

$\mathcal{P} = G$, $\mathcal{C} = G \times G$, & define $\mathcal{K} = \{(G, \alpha, a, \beta) : \alpha^a = \beta\}$ (secret)

- G, α, β are public
- a is secret
- for $K = (G, \alpha, a, \beta)$, & for a (secret) random number $k \in \mathbb{Z}_{|H|}$ define

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

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

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

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

p prime

Z_p^*, Z_{p-1}.

$(Z_p^*, \cdot)$ cyclic of order $p-1$.

isomorphic to $(Z_{p-1}, +)$

$\phi : Z_p^* \longrightarrow Z_{p-1}$.

DLP in Z_p^* $\alpha, \beta = \alpha^a \rightarrow$ find a

DLP in Z_{p-1} $\phi(\alpha), \phi(\beta) = a\,\phi(\alpha) \rightarrow$ find a is feasible.

$\phi(xy \bmod p) = (\phi(x) + \phi(y)) \bmod (p-1)$ Extended Euclidean Algm.

If we can find an efficient algm. to compute isomorphism ϕ, ⓓ we can solve DLP in $(Z_p^*, \cdot)$. → No known general method to efficiently compute the isomorphism ϕ.

Careful about the choice of your group

G

$H = \langle \alpha \rangle$ $\phi : H \rightarrow Z_{|H|}$

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 where DLP seems to be intractable.
  - $GF(p^n)$
  - Elliptic curve group.

Polynomial Rings

- $R \to$ commutative ring.
- $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$, $a_i \in R$, $n \geq 0$.
  - a_i: coefficients
  - poly. of deg. n if n is the largest int. s.t. $a_n \neq 0$.
  - $n = \deg(f(x))$
  - $a_n \to$ leading co-efficient of $f(x)$.
- $f(x) = a_0$ (const. poly)
  - $a_0 \neq 0$, $\deg(f(x)) = 0$.
  - $a_0 = 0$
  - $f(x) \to$ zero poly.
  - $\deg(f(x)) = -\infty$.
- $f(x)$ is monic poly. if leading co-efficient of $f(x)$ is 1.

Defⁿ: $R \to$ commutative ring

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

$+, \cdot \to$ two operations with coefficient arithmetic performed in R.

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

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

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

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

&

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

Example:

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

$h(x) = x^2 + 2$ in $\mathbb{Z}_5[x]$.

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

x^2+2 | $x^4 + 3x + 2$ | $x^2 + 3$

$-x^4 \pm 2x^2$

$3x^2 + 3x + 2$

$-3x^2 \pm 1$

$3x - 1 \leftarrow \deg < 2$

$\downarrow$

$r(x)$

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

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

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

- F → arbitrary field.
- $F[x]$ → poly. ring

$F[x]$ has many properties in common with $\mathbb{Z}$.

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 Algm. for polynomials

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

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

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

$q(x)$ → quotient → $g(x)$ div $h(x)$.

$r(x)$ → remainder

↓

$g(x)$ mod $h(x)$

Example:

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

$$\begin{array}{r|l} x^4+x^3+1 & x^6+x^5+x^3+x^2+x+1 \;\Big|\; x^2 \\ & x^6+x^5 \quad +x^2 \\ \hline & x^3+x+1 \end{array}$$

$\therefore g(x) = x^2 h(x) + (x^3+x+1)$

$q(x) = x^2$

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

i.e. $g(x)$ mod $h(x) = x^3+x+1$, $g(x)$ div $h(x) = x^2$.

Def^n. If $g(x), h(x) \in F[x]$, then $h(x)$ divides $g(x)$, ~~written~~

$$h(x) \mid g(x)$$

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

Def^n. If $g(x), h(x) \in F[x]$, then $g(x)$ is said to be congruent to $h(x)$ modulo $f(x)$ if

$$f(x) \mid g(x) - h(x).$$

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

Fact (Properties of congruences)

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

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

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

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

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

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

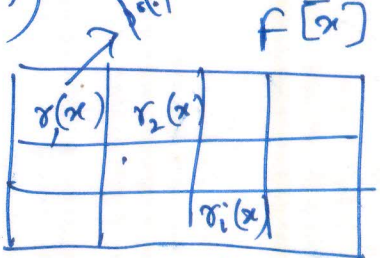
then $g(x) + h(x) \equiv g_1(x) + h_1(x) \pmod{f(x)}$ and

$g(x)\,h(x) \equiv g_1(x)\,h_1(x) \pmod{f(x)}$

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

$g(x) \in F[x]$ $\quad$ $g(x)$ modulo $f(x)$ $\quad$ $g_1(x)$

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



$F[x]/(f(x))$ → quotient ring

~~if~~ field if $f(x)$ is irreducible commutative.

Def^n: $F[x]/(f(x))$ 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

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

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

$\mathbb{Z}_p \to$ field when n is prime.

$GF(p^n)$.

$\exists$ prime p s.t. $|F| = p^n$, p prime for some $n \in \mathbb{Z}_+$

finite $F \to$ ← for all p, $\exists$ a finite F with $|F| = p^n$ & F is unique.

of finite fields.

Existence & Uniqueness theorem

(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 $GF(p^m)$.

$GF(p) = \mathbb{Z}_p$.

↓ Construction

$GF(p^n)$.

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

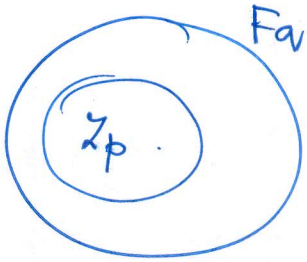
- Z_p is a field if p is prime, hence every field of order p is isomorphic to Z_p.

- $F_p \xrightarrow{\text{identified}} Z_p$.

- **Fact** If F_q is a finite field of order $q = p^m$, p a prime, then $p \to$ characteristic of F_q.

  Moreover, F_q contains a copy of Z_p as a subfield.

Hence, F_q can be viewed as an extension field of Z_p of degree m.



$F_q = F_{p^m}$.

↓

extension field of Z_p of deg. m.

↓

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

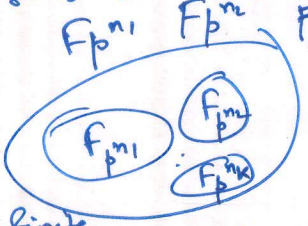
- **Fact** (Subfields of a finite field)

  $F_q \to$ a finite field of order $q = p^m$.

$m = n_1 n_2 \cdots n_k$, n_i +ve divisors of m.

exactly one subfield ↙ ↙ ↙

$F_{p^{n_1}}$ $F_{p^{n_2}}$ $\cdots$ F_{p^m} F_q.



$a \in F_q$ 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 +ve divisor n of m.

Conversely, if n is a +ve divisor of m, then $\exists$ exactly one subfield F_{p^n} of F_q of order p^n; an element $a \in F_q$ is in the subfield F_{p^n} iff $a^{p^n} = a$.

Defⁿ The non-zero elements of F_q form a group under multiplication called the multiplicative group of F_q, denoted by F_q^*.

Fact F_q^* is cyclic of order $q-1$. Hence $a^q = a \ \forall a \in F_q$.

Defⁿ A generator of the cyclic group F_q^* is called a primitive element or generator of F_q.

Fact If $a, b \in F_q$, a finite field of characteristic p, then $(a+b)^{p^t} = a^{p^t} + b^{p^t} \quad \forall t \geq 0$.

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

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

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

$$\left.\begin{array}{l}(x^5+4x^3+2)+(3x^3+2x) \\ (x^5+4x^3+2)\cdot(3x^3+2x)\end{array}\right\} \text{ in } \mathbb{Z}_5[x].$$

proposition

If p prime, $f, g \in \mathbb{Z}_p[x]$,

then $\deg(f\cdot g) = \deg(f) + \deg(g)$.

Vector Representation of Polynomials

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

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

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

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

$f+g \sim [c_N, c_{N-1}, \ldots, c_1, c_0]$, $c_i \equiv a_i + b_i \pmod p$ for $0 \le i \le N$.

$N = \max(n,m)$

$$f \cdot g = f \cdot \sum_{i=0}^{m} b_i x^i$$

$$= \sum_{i=0}^{m} f \cdot b_i x^i$$

$$= \sum_{i=0}^{m} b_i [a_n, a_{n-1}, \cdots a_0, \underbrace{0,0,\cdots 0}_{i \text{ zeros}}]$$

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

$$\sim [a_0, a_1, \cdots, a_n]$$

$$f(x) \cdot x^k = a_0 x^k + a_1 x^{k+1} + \cdots + a_n x^{k+n}$$

$$\sim [$$

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

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

$$f \cdot x^k = a_n x^{n+k} + a_{n-1} x^{n+k-1} + \cdots + a_1 x^{k+1} + a_0 x^k$$

$$\sim [a_n, a_{n-1}, \cdots, a_1, a_0, \underbrace{0,\cdots 0}_{k \text{ zeros}}]$$

$$b_k x^k \sim [b_k, \underbrace{0,0,\cdots,0}_{k \text{ zeros}}]$$

$$\therefore [a_n, a_{n-1}, \cdots, a_1, a_0] \cdot [b_k \underbrace{0 \cdots 0}_{k \text{ zeros}}]$$

$$= b_k [a_n, a_{n-1}, \cdots, a_1, a_0, \underbrace{0 \cdots 0}_{k \text{ zeros}}]$$

$$\to f \cdot b_k x^k$$

Ex Find $x^5 + x \pmod{x^3+x+1}$ in $Z_2[x]$.

Method 1 Go for long division (Division Algm.)

$$\begin{array}{r|l} x^3+x+1 & x^5+x \quad \Big| \; x^2+1 \\ \hline & \underline{x^5} \quad \underline{+x^3} \quad \underline{+x^2} \\ \hline & x^3+x^2+x \\ & \underline{x^3} \quad \underline{+x} \quad \underline{+1} \\ \hline & x^2+1 \to r(x) \end{array}$$

Ans $\to x^3+1$.

Method 2 (Reduction)

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

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

$$x^3 + x + 1 \equiv 0 \pmod{x^3+x+1}$$

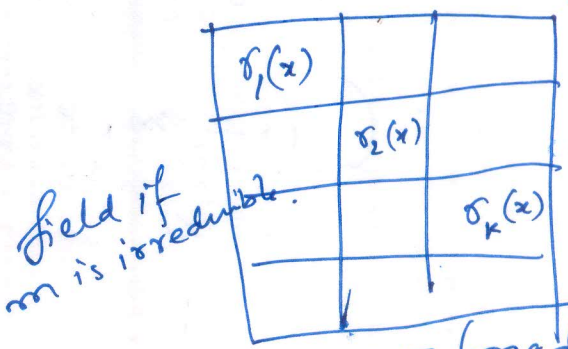
$$\therefore x^3 \equiv x + 1 \pmod{x^3+x+1}$$

Building finite fields from $Z_p[x]$

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

Parallels between construction of finite fields $GF(p)$ from Z and $GF(p^n)$ from $Z_p[x]$.

↓ $Z_p[x]$



↑ quotient ring. $Z_p[x] \pmod m$ or $Z_p[x] / (m)$.

mod x^2+x+1

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

$\otimes$	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

x^2+x
$x+1+x$
x^2+1
$= x+$

$GF(4) = GF(2^2) \simeq Z_2[x] \pmod{x^2+x+1}$.

poly.	Binary	Power
0	0 0	
1	0 1	$\longrightarrow x^0$
x	1 0	$\longrightarrow x$
$x+1$	1 1	$\longrightarrow x^2$

$GF(8) = GF(2^3) = Z_2[x] / (\text{mod } f(x))$

$f(x) \to$ irr. poly of deg. 3.

poly. in $Z_2[x]$ of degree 3

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

x^3+x+1 or x^3+x^2+1.

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

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

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

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

$\equiv 2x^2+1$

$x(x^2+x+1)$, $(x^2+1)(x+1)$, x^3+x+x^2+1

x^3+x^2, x^3+x

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

↓ to prove them are irreducible.

poly of deg < 3

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

Example. GF(2^2) construction.

$Z_2[x]$ → find an irreducible poly. of degree 2 ↓ m.

$Z_2[x]/(m)$ → GF(2^2).

polys in $Z_2[x]$ of degree 2

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

x^2 → $x \cdot x$; x^2+1 → $(x+1)(x+1)$; x^2+x → $x(x+1)$; x^2+x+1 ↓ to prove it is irreducible.

$f(x)\ g(x)$

deg 1 deg 1 → only deg 1 polys

$x, x+1$

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

$\equiv 1 \pmod{x}$

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

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

x^2+x+1 is irreducible.

$\Rightarrow$ GF(2^2) = GF(4) construction

$= Z_2[x]/(x^2+x+1)$.

$= \{0, 1, x, x+1\}$

+	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

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

We need to find a poly $f(x) \in Z_2[x]$ 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.

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

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

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

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

$x^2 \nmid f_2(x)$

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

$x^2+x \;\big|\; x^3+x+1 \;\big|\; x+1$

x^3+x^2

$x^2+x+1 \;\big|\; x^3+x+1 \;\big|\; x$

x^3+x^2+x

x^2+1

x^2+x+1

x^2+x

1

$x^2 \;\big|\; x^3+x+1 \;\big|\; x$

x^3

$x+1$

$GF(8) = GF(2^3) = Z_2[x] / (\text{mod } f(x))$

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

$\rightarrow$ deg 3 irreducible poly.

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

$x^6 = (x^3+1)^2$
$= x^2 + 1$

$x^3 \equiv x+1$

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

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

poly	Binary	Power
0	0 0 0	
1	0 0 1	x^0
x	0 1 0	x^1
$x+1$	0 1 1	x^3
x^2	1 0 0	x^2
x^2+1	1 0 1	x^6
x^2+x	1 1 0	x^4
x^2+x+1	1 1 1	x^5

cyclic group of order 7.

$\downarrow$

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

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

$x^7 = 1$

·	1	x	$x+1$ (x^3)	x^2	x^2+1 (x^6)	x^2+x (x^4)	x^2+x+1 (x^5)
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1

$x^3 \leftarrow x+1$	$x+1$
x^2	x^2
$x^6 \leftarrow x^2+1$	x^2+1
$x^4 \leftarrow x^2+x$	x^2+x
$x^5 \leftarrow x^2+x+1$	x^2+x+1

$x^7 = 1$

·	1 (001)	x (010)	x^3 ($x+1$) (011)	x^2 (100)	x^6 (x^2+1) (101)	x^4 (x^2+x) (110)	x^5 (x^2+x+1) (111)
1 (001)	001	010	011	100	101	110	111
x (010)	010	100	110	011	001	111	101
x^3 (011)	011	110	101	111	100	001	010
x^2 (100)	100	011	111	110	010	101	001
x^6 (101)	101	001	100	010	111	011	110
x^4 (110)	110	111	001	101	011	010	100
x^5 (111)	111	101	010	001	110	100	011

$GF(8) = \langle 010 \rangle = \langle x \rangle$