Important Results from Number Theory

Moduler Arithmetic

let $m > 1$, $m \in \mathbb{Z}$ be the modulus

If $a, b \in \mathbb{Z}$, and $m \mid (b-a)$ then

$$a \equiv b \pmod{m}$$

This is called "congruence"

Properties of "Congruence"

Let $a, b, c, d, x, y \in \mathbb{Z}$, $m > 1 \in \mathbb{Z}$

- If $a \equiv b \pmod{m}$ & $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$
- If $a \equiv b$ & $c \equiv d$ then $ac \equiv bd$ (drop (mod m))
- If $a \equiv b$ & $c \equiv d$ then $ax + cy \equiv bx + dy$

Call $I_m = \{0, 1, \dots, m-1\}$, using $\equiv$ can map $x \in \mathbb{Z}$ to unique $r \in I_m$

r is the residue of x modulo m; $|x|_m$

Then if $a, b \in \mathbb{Z}$, $m > 1 \in \mathbb{Z}$

- $|a|_m$ is unique
- $|a|_m = |b|_m \iff a \equiv b \pmod{m}$
- $|km|_m = 0 \quad \forall k \in \mathbb{Z}$
- $|a+b|_m = ||a|_m + |b|_m|_m$

  $= ||a|_m + b\,|_m$

  $= |\,a + |b|_m|_m$
- $|ab|_m = ||a|_m |b|_m|_m$

  $= ||a|_m b\,|_m$

  $= |\,a\,|b|_m|_m$

reduce as often as you wish!

Theorem: $(I_m, \underbrace{+}_{\text{addition mod n}}, \underbrace{*}_{\text{mult. mod m}})$ is a commutative ring with identity

Theorem: $(I_m, +, *)$ isomorphic to a finite field w/ m elements, $GF(m)$ $\iff$ m is prime

if m not prime there are elements in I_m w/o mult. inverses

Let $a \in \mathbb{Z}$, $\exists!\ b \in I_m \ni$

$$|ab|_m = |ba|_m = 1 \iff$$

$$|a|_m \neq 0 \text{ and } \gcd(a,m) = 1$$

(think of LCGs)

Chinese Remainder Theorem:

Let $m_1, \dots, m_j$ be pairwise coprime & let $a_1, \dots, a_j \in \mathbb{Z}$ then

$$x \equiv a_i \pmod{m_i} \quad i = 1, \dots, j \iff$$

$$x \equiv a_1 M_{-1} M_1 + \dots + a_j M_{-j} M_j \pmod{M}$$

with $M = \prod_{i=1}^{j} m_i$

$$M_i = M / m_i$$

$$M_{-i} \ni M_{-i} M_i \equiv 1 \ (m_i)$$

This is used to compute large modular results (M) with many small moduli (m_i)

$$x \sim (a_1, a_2, \dots, a_j)$$

this is because

- Let $x \equiv a_i \pmod{m_i}$ $i = 1, \dots, j$
  $y \equiv b_i \pmod{m_i}$ $i = 1, \dots, j$

Then
$$\left.\begin{aligned} x \pm y &\equiv a_i \pm b_i \pmod{m_i} \\ xy &\equiv a_i b_i \pmod{m_i} \end{aligned}\right)$$
$i = 1, 2, \dots, j$

<u>Period Length</u>

Let $a, m \in \mathbb{Z}$, $\gcd(a, m) = 1$
The multiplicative order of a modulo m is smallest $e \geq 1 \in \mathbb{Z} \ni$
$$a^e \equiv 1 \pmod{m}$$

Theorem (Fermat's Little):
Let m be prime and $a \in \mathbb{Z} \ni$
$m \nmid a$, then
$$a^{m-1} \equiv 1 \pmod{m}$$
This implies that $e \mid m-1$.

Euler Toticent Function: $\phi(m)$

For $m > 0 \in \mathbb{Z}$ $\phi(m)$ is # of $r > 0$ with $r < m$ & $\gcd(r, m) = 1$, $\phi(1) = 1$.

Note: p, prime $\rightarrow \phi(p) = p - 1$

$$\phi(p^k) = p^k - p^{k-1} \quad k \geq 1$$
$$= p^k\left(1 - \frac{1}{p}\right)$$

Also $\phi(\cdot)$ is multiplicative and so is uniquely defined by it values on the prime powers (more later)

Theorem: Let $a, m \in \mathbb{Z} \ni \gcd(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

when m is prime, it's the Farmat.

Let m be a prime, the a is a primitive root modulo m if $e = m - 1$.

Theorem: m, prime, $\exists$ $\phi(m-1)$ distinct primitive roots modulo m.

$\phi(\phi(m)) = \phi(m-1)$

Let g be a prim. root modulo m & $\gcd(k, m) = 1$, then the index of k modulo m (w.r.t. p.r. g) is the smallest positive integer, t, ∋

$$g^t \equiv k \pmod{m}$$

$t = \mathrm{ind}_g^{(m)}(k)$, this is the famous discrete logarithm problem.

Note: $\mathrm{ind}_g^{(m)}(a) = \mathrm{ing}_g^{(m)}(b) \iff a \equiv b$

<u>Theorem</u>: m prime, e is order of a modulo m, and g is a prim. root modulo m, then $e = \frac{m-1}{d}$ where $d = \gcd(\mathrm{ind}_g^{(m)}(a), m-1)$, and the # of $r \in I_m$ with order e is $\phi(e)$.

If m is <u>not</u> prime $\Rightarrow (I_m, +, *)$ is not a field, so some do not have mult.$^{-1}$ But $\forall a \in I_m$ where $a^e \equiv 1 \pmod{m}$ for $e \geq 1$, $a^{-1} = a^{e-1}$, so only if $\gcd(a, m) = 1$ does a have nozero order.

Knuth: Let $m > 1 \in \mathbb{Z}$ then a is a primitive element mod m if the order of a is maximal

Theorem: Let $\lambda(m)$: maximal order mod m, $\lambda(2) = 1$, $\lambda(4) = 2$, $\lambda(2^e) = 2^{e-2}$, $e \geq 3$ $\lambda(p^e) = p^{e-1}(p-1)$, p prime, and for $M = p_1^{e_1} \cdots p_k^{e_k}$ $\lambda(M) = \mathrm{lcm}(\lambda(p_1^{e_1}), \dots, \lambda(p_k^{e_k}))$

Continued Fractions: Arise in diophantine approximation, modular arithmetic, certain gcd algorithms. A continued fraction expansion of a rational number

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}} \qquad \overset{\text{"real integer"}}{\downarrow} \quad \underbrace{[a_0; a_1, a_2, \dots]}_{\text{positive } \mathbb{Z}}$$

$P_j / Q_j = [a_0; a_1, \dots, a_j]$ a convergent of order j or approximating fraction, $\gcd(P_j, Q_j) = 1$:

$$P_j = a_j P_{j-1} + P_{j-2}, \quad P_0 = a_0, \quad P_{-1} = 1$$

$$Q_j = a_j Q_{j-1} + Q_{j-2}, \quad Q_0 = 1, \quad Q_{-1} = 0$$

If $a_j \neq 1$ then P_j / Q_j is uniquely represented by $[a_0; a_1, \dots, a_j]$, why $\neq 1$?

$\frac{1}{2} = [0; 2]$ and $[0; 1, 1]$

Also $P_j Q_{j-1} - P_{j-1} Q_j = (-1)^{j+1} \Rightarrow$ convergents approach alternatively from above and below.

Examples: $\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, \cdots]$

Naperian base $\longrightarrow$ $e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \cdots]$

$\sqrt{2} = [1; \bar{2}]$ — repeating digit

$\frac{1+\sqrt{5}}{2} = [1; \bar{1}]$

Recall Fibonacci numbers

$$\underbrace{F_i = F_{i-1} + F_{i-2}}_{\text{same as } P/Q \text{ recurrence}}, \quad F_0 = 0, \; F_1 = 1$$

$$\frac{F_{i+1}}{F_i} = [1; \overbrace{1, \cdots, 1}^{i-1}] \xrightarrow[i \to \infty]{} \frac{1+\sqrt{5}}{2}$$

Famous Arithmetical Functions:

d: divisor function
μ: Möbius function
ϕ: Euler function

all are multiplicative

Let $n = \prod_{i=1}^{k} p_i^{e_i}$ (FT of arithmetic),

$$d(n) = \prod_{i=1}^{k} (e_i + 1)$$

otherwise empty sum ambiguous

$d(1) = 1$

We have $d(mn) = d(m)\,d(n)$

when $\gcd(m,n) = 1$

$$d(n) = \sum_{d \backslash n} 1 \quad (\text{why?})$$

Möbius Function, μ:

i) $\mu(1) = 1$

ii) $\mu(n) = 0$ if n has square factor

iii) $\mu(n) = (-1)^k$ if product of k distinct primes

$$\mu(n): \quad \sum_{d \backslash n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

- $\mu(m,n) = \mu(m)\mu(n)$ with $\gcd(m,n) = 1$
- $\mu(m,n) = 0$ if $\gcd(m,n) > 1$
- $\sum_{d \backslash n} \mu(d) = 0$ if $n > 1$

$\mu(\cdot)$ is used in the Möbius transformation / inversion formula

Theorem: If int. valued function f, F:

$$F(n) = \sum_{d \mid n} f(d) \quad \text{then}$$

$$f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) F(d) = \sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right)$$

Note on multiplicative functions:

$m(n)$ is multiplicative if

a) $m(1) = 1$

b) $m(ab) = m(a)\,m(b)$ $\forall \gcd(a,b) = 1$

ϕ, μ, d are multiplicative & the Möbius inversion formula holds for such functions.

Theorem: $\displaystyle\sum_{i=1}^{d(n)} \phi\left(\frac{n}{d_i}\right) = n \iff$

$$n = \sum_{d \mid n} \phi\left(\frac{n}{d}\right) = \sum_{d \mid n} \phi(d)$$

So $F(n) \equiv n$ when $f(n) = \phi(n)$

So by Möbius inversion:

$$\phi(n) = \sum_{d \backslash n} \mu\left(\frac{n}{d}\right) d = n \sum_{d \backslash n} \frac{\mu(d)}{d}$$

Polynomial Arithmetic:

Let $q = p^k$ (prime power)

$GF[q, z]$ is the ring of polynomials with coefficients in $GF(q)$, $GF(2)$ is particularly of interest.

Def: Let $f(z) \in GF[q, z]$ have degree $r > 0$, let $GF(q')$ be a field that contains $GF(q)$ as a subfield, then $f(z)$ splits $GF(q')$ if can write

$$f(z) = a(z - \alpha_1) \ldots (z - \alpha_r)$$

$$a\ \alpha_1, \alpha_2, \ldots, \alpha_r \in GF(q')$$

$GF(q')$ is a splitting field of $f(z)$ over $GF(q)$ if $f(z)$ splits in $GF(q')$ and no proper subfield of $GF(q')$ contains the α_j

Def: Let $\alpha \neq 0 \in GF(q)$, the mult. order of α in $GF(q)$ is the smallest $e > 0 \ni \alpha^e = 1$.

Consider factoring $z^N - 1$ over $GF(q)$:

- The roots are N^{th} roots of unity, $K^{(N)}$, over the splitting field
- $K^{(N)}$ is a primitive N^{th} root of unity over $GF(q)$ if its order is N.
- If W_N is a primitive root of $z^N - 1$, W_N^n, $n = 0, 1, \cdots, N-1$ are distinct, and

$$z^N - 1 = \prod_{n=0}^{N-1} (z - W_N^n)$$

- This factorization is unique, W_N^n are <u>all</u> the primitive roots with $\gcd(n, N) = 1$

Def: Let W_n be a primitive n^{th} root of unity over $GF(q)$ and that n is not divisible by (*). Then the <u>polynomial</u>:

$$C_n(z) = \prod_{\substack{1 \leq d \leq n \\ \gcd(d,n)=1}} (z - W_n^d) \quad \Big\} \sim d \nmid n$$

is the n^{th} cyclotomic polynomial over $GF(q)$.

(*) The characteristic of $GF(q)$ is the smallest $p > 0 \in \mathbb{Z} \ni p\alpha = 0 \ \forall \alpha \in GF(q)$.

Let p be the characteristic of $GF(q)$ and $n > 0 \in \mathbb{Z}$, $p \nmid n$, then

$$z^n - 1 = \prod_{d \setminus n} C_d(z)$$ by inversion with products

$$C_n(z) = \prod_{d \setminus n} (z^d - 1)^{\mu(n/d)} = \prod_{d \setminus n} (z^{n/d} - 1)^{\mu(d)}$$

$$\deg(C_n(z)) = \sum_{d \setminus n} d\,\mu\left(\frac{n}{d}\right) = \phi(n)$$

<u>Def:</u> Polynomial $f(z) \in GF[q, z]$ is "irreducible over $GF(q)$" if $\deg(f(z)) > 0$ and when $f(z) = b(z)\,c(z)$ with $b(z), c(z) \in GF[q, z]$ either $b(z)$ or $c(z)$ is constant.

- "Irreducible" polynomials have no nontrivial factorization
- Serve the function of primes on $GF[q, z]$

<u>Theorem</u>: If $f(z) \in GF[q, z]$ is irreducible with degree r, then $f(z)$ has a root $\alpha \in GF(q^r)$, and all the roots of $f(z)$ are simple and are given by $\alpha, \alpha^q, \alpha^{q^2}, \dots \alpha^{q^{r-1}} \in GF(q^r)$.

$\Rightarrow$ With $f(z)$ as above $GF(q^r)$ is the splitting field

<u>Theorem</u>: $\forall\, GF(q)$, $r \in \mathbb{Z}$ the product of all monic irreducible polynomials $\in GF[q, z]$ whose degree divides r is equal to $z^{q^r} - z$

Cor: Let $N_q(d) = \#$ monic irred. w/degree $d \in GF[q,z]$

$$q^r = \sum_{d \backslash r} d\, N_q(d) \quad \forall\, r>0 \in \mathbb{Z}$$

Mōbius

$$N_q(r) = \frac{1}{r} \sum_{d \backslash r} \mu\left(\frac{r}{d}\right) q^d = \frac{1}{r} \sum_{d \backslash r} \mu(d)\, q^{r/d}$$

$I(q,r;z)$ = product of all monic irred./degree $r \in GF[q,z]$

Theorem: For $r>1$ $\quad I(q,r;z) = \prod_d C_d(z)$

$d \backslash q^r-1$ and r is the multiplicative order of q modulo d

Def: $f(z) \neq 0 \in GF[q,z]$, if $f(0) \neq 0$, the smallest positive e for which $f(z) \backslash z^e - 1$ is the order of $f(z)$, $e = \mathrm{ord}(f)$. If $f(0)=0$, then $f(z) = z^h g(z)$ with $h>0 \in \mathbb{Z}$, $g(0) \neq 0 \in GF[q,z]$ and then $\mathrm{ord}(f) = \mathrm{ord}(g)$.

- $f(z) = c \neq 0 \Rightarrow \mathrm{ord}(f) = 1$ because $c \backslash z-1$
- $f(z) = z \in GF[2,z]$ has $\mathrm{ord}(f)=1$

Theorem: If $f(z)$ is irred., has degree $r \in GF[q,z]$ then $r \backslash q^r - 1$.

Theorem: Let $m_1(z), \ldots, m_j(z)$ be pairwise co-prime, then

$$\mathrm{ord}(m_1(z) \cdot m_2(z) \cdots m_j(z)) = \mathrm{lcm}(\mathrm{ord}(m_1), \mathrm{ord}(m_2), \ldots, \mathrm{ord}(m_j))$$

Primitive Polynomial Definition: $f(z)$, monic $\in GF[q,z]$ with $f(0) \neq 0$ with degree r is primitive if its order is $q^r - 1$, note $f(0)=0$ for $f(z)=z$ in $GF(2)$ is not primitive

Theorem: # primitive of degree r in $GF[q,z]$ = $\dfrac{\phi(q^r-1)}{r}$

Modular Arithmetic on $GF[q, z]$:

$\forall f(z), M(z) \in GF[q, z]$ we have (quotient/remainder)

$f(z) = q(z) M(z) + g(z)$, where

$q(z), g(z) \in GF[q, z]$ and are unique

$f(z) \equiv g(z) \pmod{M(z)}$ where we have $\deg(g) < \deg(M)$

<u>Theorem</u>: $M(z) \in GF[q, z]$, $\deg(M) = r$, then the residue class $GF[q, z]/(M)$ is a field isomorphic to $GF(q^r) \Leftrightarrow M(z)$ is irred.

Note: $GF[q, z]/(M)$ is the ideal generated by $M(z)$, which is the polynomial / modulus while q is the arithmetic modulus.

<u>Theorem</u>: Let $M(z) \in GF[q, z]$ have $\deg(M) = r$, then if $M(\alpha) = 0$, then $\{1, \alpha, \dots, \alpha^{r-1}\}$ is a basis for $GF(q^r)$ over $GF(q)$. With this all elements in $GF[q^r]$ can be represented as $f(\alpha)$, a polynomial with $\deg(f) < \deg(M)$.

<u>Theorem</u>: Let $M(z)$ be irred., $\deg(M) = r$, $M(0) \neq 0$, $M(\alpha) = 0$. Then $\mathrm{Ord}(M) =$ mult. order of α in $GF(q^r)$.

Chinese Remainder Theorem:

Given polynomials $y_1(z), \dots, y_I(z)$

$\exists!\; y(z) \ni y(z) = y_j(z) \pmod{m_j(z)}\; j=1,\dots,J$
$\ni \; 0 \le \deg(y(z)) < \sum_j \deg(m_j(z))$ when the monic $m_j(z)$'s are pairwise co-prime.

And write $M(z) = \prod_j m_j(z)$

$$M_j(z) = M(z)/m_j(z)$$

$$M_{-j}(z)\, M_j(z) \equiv 1 \pmod{m_j(z)}$$

$$y(z) \equiv \sum_{j=1}^{J} M_{-j}(z)\, M_j(z)\, y_j(z) \pmod{M(z)}$$

What is the analog of $\phi(\cdot)$?

Def: For $M(z) \in GF[g,z]$, $\Phi_g(M)$ is # of polynomials in $GF[g,z]$ are of smaller degree than and co-prime to $M(z)$.
$\Phi_g(M) = 1$ if $\deg(M) = 0$.

Theorem: Let $m_j(z)$, $j=1,\dots,J$ be distinct monic irred. polys $\in GF[g,z]$ and c_j, $j=1,\dots,J$ be distinct $\in \mathbb{Z}^+$. Let $v_j = \deg(m_j)$, $a \ne 0 \in GF(g)$. If $M(z) = a\prod_{j=1}^{J} m_j(z)^{c_j}$ and $\deg(M) \ge 1$ then

$$\Phi_g(M) = g^{r}(1-g^{-v_1})(1-g^{-v_2})\dots(1-g^{-v_J})$$

$r = \sum c_j v_j$

This is just the computational analog where the $m_j(z)$'s operate like primes.

<u>Theorem</u>: Let $g(z), M(z) \in GF[q, z]$ with $\gcd(g, M) = 1 \Rightarrow g(z)^{\Phi_q(M)} \equiv 1 \pmod{M(z)}$

<u>Formal Laurent Series</u>: q is a prime power, let $GF\{q, z\}$ be the field of formal Laurent Series

$$S(z) = \sum_{j \ge w} x_j z^{-j} \quad \text{in } z^{-1}$$
$$x_j \in GF(q)$$

<u>Def</u>: v is the discrete exponential valuation on $GF\{q, z\}$: If $S(z)$, $v(S) = -w$ where w is the smallest index of a nonzero x_w

If $S(z) = 0$, $v(S) = -\infty$

Note: $GF\{q, z\}$ contains the field of rational functions on $GF(q)$ as a subfield.

Note: $\forall S_1(z), S_2(z) \in GF\{q, z\}$ (exponents!)

- $v(S_1 S_2) = v(S_1) + v(S_2)$
- $v(S_1 + S_2) = \max(v(S_1), v(S_2))$

$\forall P(z), Q(z) \in GF[q, z]$ with $Q(z) \neq 0$

$$v(P/Q) = \deg(P) - \deg(Q)$$

$\forall S(z) \in GF\{q, z\}$ has the following unique continued fraction expansion

$$S(z) = A_0(z) + \cfrac{1}{A_1(z) + \cfrac{1}{A_2(z) + \cdots}}$$

$$= [A_0(z); A_1(z), \ldots]$$

with $A_i(z) \in GF[q,z]$ & $\deg(A_j(z)) \geq 1$, $j \geq 1$.

$S(z)$ rational $\Rightarrow$ finite or repeating expansion
" irrational $\Rightarrow$ infinite / nonrepeating expansion

Def: $[S(z)]$ is the polynomial part of $S(z)$

Recurrence Relations:

$$A_0(z) = [S(z)],$$

$$B_0(z) = S(z) - [S(z)],$$

$$A_{j+1}(z) = [1/B_j(z)]$$

$$B_{j+1}(z) = 1/B_j(z) - A_{j+1}(z), \quad j \geq 0$$

Note: If $B_j(z) = 0$ for some j, the exp. terms.

$P_j(z)/Q_j(z)$ is the jth convergent, and the satisfy:

$$P_{-1}(z) = 1, \quad P_0(z) = A_0(z)$$

$$P_j(z) = A_j(z) P_{j-1}(z) + P_{j-2}(z), \quad j \geq 1$$

$$Q_{-1}(z) = 0, \quad Q_0 = 1$$

$$Q_j(z) = A_j(z) Q_{j-1}(z) + Q_{j-2}(z), \quad j \geq 1$$

$$\deg(Q_j(z)) = \sum_{1 \le m \le j} \deg(A_m(z)) \quad j \ge 1$$

with $S(z)$ rational, $\deg(A_j(z)) = +\infty$

whenever $A_j(\cdot)$ & $Q_j(\cdot)$ do not exist. $\deg(Q_j(z)) = \infty$

Theorem: For $j \ge 0$

$$P_j(z)\,Q_{j-1}(z) - Q_j(z)\,P_{j-1}(z) = (-1)^{j+1}$$

where $P_j(z)/Q_j(z)$ is the j^{th} convergent of $S(z) \in GF\{q, z\}$

Theorem: For $j \ge 0$

$$v\left(S(z) - \frac{P_j(z)}{Q_j(z)}\right) = -\deg(Q_j(z)) - \deg(Q_{j+1}(z))$$

Theorem: $\forall\, n \ge 1$, $S \in GF\{q, z\}$, let $S_n(z)$ be in $GF\{q, z\} \ni v(S_n(z) - S(z)) = -n-1$, $\exists!\, j \ge 0$ determined by

$$\deg(Q_{j-1}(z)) + \deg(Q_j(z)) \le n < \deg(Q_j(z)) + \deg(Q_{j+1}(z))$$

A Summary of Facts for Linear Recurring Sequences:

Def: For $\alpha \in GF(q^r) = F$, $K = GF(q)$, $Tr_{F/K}(\alpha)$, trace of α over K

$$Tr_{K/F}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{r-1}}$$

If q is prime then this is the "absolute trace of α" and is written $Tr_F(\alpha)$.

From a previous theorem: $M(z) \in GF[q,z]$, $\deg(M) = r$ & M is irred. (monic), then its roots are $\alpha, \alpha^q, \dots, \alpha^{q^{r-1}}$,

$$M(z) = (z-\alpha)(z-\alpha^q)\cdots(z-\alpha^{q^{r-1}})$$
$$= z^r - a_{r-1}z^{r-1} - \cdots - a_0$$
$$Tr_{F/K}(\alpha) = a_{r-1}$$

- $Tr_{F/K}(\alpha+\beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta) \quad \forall \alpha,\beta \in F$
- $Tr_{F/K}(c\alpha) = c\,Tr_{F/K}(\alpha) \quad \forall c \in K, \alpha \in F$
- $Tr_{F/K}$ is a linear transformation of F onto K, where both are viewed as vector spaces over K
- $Tr_{F/K}(a) = ra \quad \forall a \in K$
- $Tr_{F/K}(\alpha^q) = Tr_{F/K}(\alpha), \ \forall \alpha \in F$

$\left(\begin{array}{l} F = GF(q^r) \\ K = GF(q) \end{array} \right.$

Def: $x_1, x_2, \ldots \in GF(q)$ is an rth-order linear recurring sequence if it satisfies

$$x_{n+r} = a_{r-1}x_{n+r-1} + a_{r-2}x_{n+r-2} + \cdots + a_0 x_n$$
$$n = 1, 2, \ldots$$

$a_0, a_1, \ldots, a_{r-1} \in GF(q)$

$x_1, \ldots, x_r$ are initial values & they uniquely determine the sequence, which is purely periodic if $a_0 \neq 0$ (why)

Def: The polynomial $M(z) = z^r - a_{r-1}z^{r-1} - \cdots - a_0$ is the characteristic polynomial of the recurrence relation and the linear recurring sequence.

If $M(z)$ is primitive $\Rightarrow$ maximal period $= q^r - 1$ as long as $x_1, \ldots, x_r$ are not all zero.

<u>Theorem</u>. x_n, $n = 1, 2, \ldots$ be an $r^{\underline{th}}$-order linear recurring sequence in $K \in GF(q)$ with $M(z)$ irred. over K. Let α be a root of $M(z)$ in $F = GF(q^r)$, $\exists!\, \gamma \in F \ni$

$$x_n = Tr_{F/K}(\gamma \alpha^n), \quad n = 1, 2, \ldots$$

The characteristic polynomial $M(z) = z^r - a_{r-1} z^{r-1} - \ldots - a_1 z - a_0$ has the $r \times r$ companion matrix

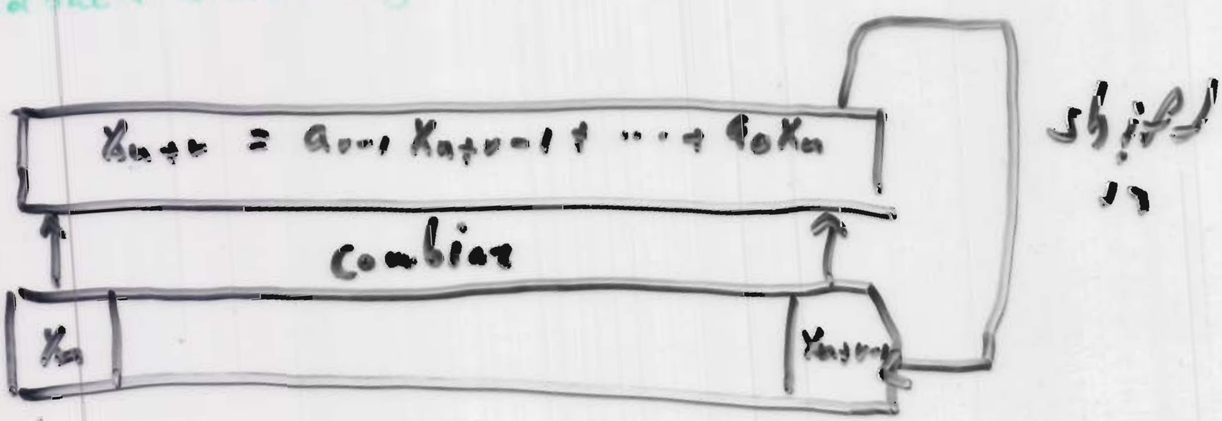
$$C = \begin{pmatrix} 0 & 0 & \cdots & & a_0 \\ 1 & 0 & \cdots & & a_1 \\ & \ddots & 0 & & \vdots \\ & 0 & \ddots & \ddots & \vdots \\ & & & 1 & a_{r-1} \end{pmatrix}$$

$\bar{x}_1 = (x_1, \ldots, x_r)$

$\bar{x}_n = (x_n, \ldots, x_{n+r-1})$, $n = 1, 2, \ldots$

$$\bar{x}_1, \bar{x}_1 C, \bar{x}_1 C^2, \ldots, \bar{x}_1 C^n$$

Linear Feedback Shift Register (LFSR):



Note: best implemented with fixed array and moving taps via pointers