FINITE FIELDS

DR. ODELU VANGA

COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY SRI CITY

CHITTOOR, INDIA

Recap:
Groups, Sub-groups, Cyclic Groups

$\exists\, a \in G,\ G = \langle a \rangle$
$= \{a^n \mid n \in N\}$

$Z_{10} = \{0, 1, \underline{2}, 3, 4, 5, 6, 7, 8, 9\}$

$+_{10}$.
1) closure
2) Associative
3) Existence of identity
4). Existance of inverse.
5). commutative

$H = \langle 2 \rangle$
$= \{2, 4, 6, 8, 0\}$

$\times_{10}$

$H \subseteq G$, $(G, +)$ is group.

if $(H, +)$ is group

$\Rightarrow$ subgroup of G.

permutation group

S_n.

1) 2) 3) 4)

$\times$ (5).

$f, g \in S_n$

$(f \circ g)(x) = f(g(x))$.

$(S_n, \circ)$ - group

Rings

Definition: A set F with two binary operations + (addition) and $\cdot$ (multiplication) is called a commutative *ring* with identity if

1 $\forall\, a,b \in F,\ a+b \in F$

2 $\forall\, a,b,c \in F,\ (a+b)+c = a+(b+c)$

3 $\forall\, a,b \in F,\ a+b = b+a$

4 $\exists\, 0 \in F,\ \forall\, a \in F,\ a+0 = a$

5 $\forall\, a \in F,\ \exists\, -a \in F,\ a+(-a) = 0$

6 $\forall\, a,b \in F,\ a\cdot b \in F$ – closure

7 $\forall\, a,b,c \in F,\ (a\cdot b)\cdot c = a\cdot(b\cdot c)$ – Associ

8 $\forall\, a,b \in F,\ a\cdot b = b\cdot a$ – commutative

9 $\exists\, 1 \in F,\ \forall\, a \in F,\ a\cdot 1 = a$ – identity

10 $\forall\, a,b,c \in F,\ a\cdot(b+c) = a\cdot b + a\cdot c$

$(b+c)\cdot a = b\cdot a + c\cdot a$

$(F, +)$

$(F, +, \cdot)$

$0 \quad 1$

$(F, \cdot)$

$2 \times (3+4) = 2\times 3 + 2\times 4$

Examples: Z_{24}, $+_{24}$, $\times_{24}$

$(\mathbb{Z}_{24}, +_{24})$ $(\mathbb{Z}_m, +_m)$

↳ Commutative.

$a, b \in \mathbb{Z}_{24}$

$a +_{24} b \in \mathbb{Z}_{24}$

$0 +_{24} b = b$

$a +_{24} (-a) = 0$

$a +_{24} b = b +_{24} a$.

$(\mathbb{Z}_{24}, \times_{24})$

6) closure: $a, b \in \mathbb{Z}_{24}$

$a \times_{24} b = (a \times b) \bmod 24$

$7 \times_{24} 5 = 35 \bmod 24$

$= 11 \in \mathbb{Z}_{24}$

7). Associative.

8). $1 \times_{24} a = a, \ \forall a \in \mathbb{Z}_{24}$.

$1 \in \mathbb{Z}_{24}$

9). $(a \times_{24} b) = (b \times_{24} a)$.

Fields

Def (field): A set F with two binary operations + (addition) and · (multiplication) is called a *field* if

1 $\forall$ a,b$\in$F, a+b$\in$F

2 $\forall$ a,b,c$\in$F, (a+b)+c=a+(b+c)

3 $\forall$ a,b$\in$F, a+b=b+a

4 $\exists$ 0$\in$F, $\forall$ a$\in$F, a+0=a

5 $\forall$ a$\in$F, $\exists$ -a$\in$F, a+(-a)=0

6 $\forall$ a,b$\in$F, a·b$\in$F

7 $\forall$ a,b,c$\in$F, (a·b)·c=a·(b·c)

8 $\forall$ a,b$\in$F, a·b=b·a

9 $\exists$ 1$\in$F, $\forall$ a$\in$F, a·1=a

10 $\forall$ a,b,c$\in$F,a·(b+c)=a·b+a·c

zero-divisors

$2 \neq 0$

$12 \neq 0$

$2 \times 12 = 24 \bmod 24 = 0$

11) $\forall$ a$\neq$0$\in$F, $\exists$ $a^{-1}\in$F, $a \cdot a^{-1}=1$

$(\mathbb{Z}_{24}, +_{24})$ field ?

$(2, 24) \neq 1$

$\boxed{a^{-1} \bmod m \text{ exists} \iff (a, m) = 1.}$

Fields

A field is a commutative ring with identity where each non-zero element has a multiplicative inverse

$$\forall\, a \neq 0 \in F,\ \exists\, a^{-1} \in F,\ a \cdot a^{-1} = 1$$

$\{(\mathbb{R}, +, \times), (\mathbb{C}, +, \times)\}$

Equivalently, (F,+) is a commutative (additive) group, and (F \ {0}, ·) is a commutative (multiplicative) group

$F = \mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

$(a, 7) = 1$.

$(F, +)$ – abelian group

$a \in \mathbb{Z}_7^*$

$(F \setminus \{0\}, \times)$ – abelian group.

a^{-1} exists in $\mathbb{Z}_7$

$\mathbb{Z}_p$, p - prime $\Longleftrightarrow$ $(\mathbb{Z}_p, +_p, \times_p)$ field.

Polynomials over Fields

$\mathbb{R}$, $\mathbb{C}$

$\mathbb{Z}_p$

Let $f(x)= a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \ldots + a_1 \cdot x + a_0$ be a polynomial of degree n in one variable x over a field F (namely $a_n, a_{n-1}, \ldots, a_1, a_0 \in F$).

Theorem: The equation $\boxed{f(x)=0}$ has at most n solutions in F.

Remark: The theorem does not hold over rings with identity.

For example, in Z_{24} the equation $\boxed{6 \cdot x = 0}$ has six solutions (0,4,8,12,16,20).

$f(x) = 6x$

$f(4) = 6 \times 4 = 24 \bmod 24 = 0$

Polynomial Remainders

Let $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \ldots + a_1 \cdot x + a_0$

$g(x) = b_m \cdot x^m + b_{m-1} \cdot x^{m-1} + b_{m-2} \cdot x^{m-2} + \ldots + b_1 \cdot x + b_0$

be two polynomials over F such that $m < n$ (or $m = n$).

Theorem: There is a unique polynomial $r(x)$ of degree $< m$ over F such that $f(x) = h(x) \cdot g(x) + r(x)$.

Remark: $r(x)$ is called the remainder of $f(x)$ modulo $g(x)$.

Finite Fields

$(a,m) \neq 1$

Z_m $\quad m = a \times b$ mod $m = 0$

$a, b \in Z_m$

Finite Field: A field $(F,+,\cdot)$ is called a finite field if the set F is finite.

Example: Z_p denotes $\{0,1,\ldots,p-1\}$. We define $+$ and $\cdot$ as addition and multiplication modulo p, respectively.

One can prove that $(Z_p,+,\cdot)$ is a field iff p is prime.

Q.: Are there any finite fields except $(Z_p,+,\cdot)$?

The Characteristic of Finite Fields

Let $(F,+,\cdot)$ be a finite field.

There is a positive integer n such that

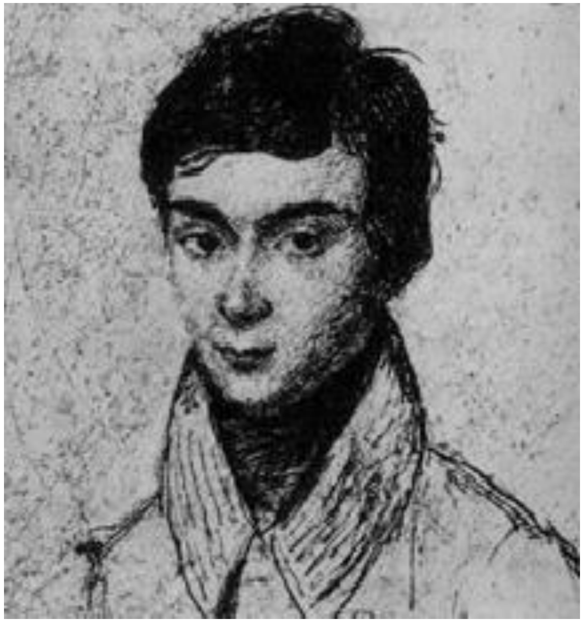
$$\underbrace{1+\ldots+1}_{\text{(n times)}} = 0$$

The minimal such ***n*** is called the characteristic of F, char(F).

Theorem: For any finite field F, char(F) is a prime number.

Galois Fields GF(p^k)

Theorem: For every prime power p^k (k=1,2,…) there is a unique finite field containing p^k elements. These fields are denoted by GF(p^k). There are no finite fields with other cardinalities.



Évariste Galois (1811-1832)

Remarks:

1. For F=GF(p^k), char(F)=p
2. GF(p^k) and Z_{pk} are not the same!

Polynomials over Finite Fields

Polynomial equations and factorizations in finite fields can be different than over the rationals.

Examples

```
factor(x^6-1);  # over the rationals
```

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

```
Factor(x^6-1) mod 7; # over Z7
```

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

```
factor(x^4+x^2+x+1); # over the rationals
```

$$x^4+x^2+x+1$$

```
Factor(x^4+x^2+x+1) mod 2; # over Z2
```

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

Irreducible Polynomials

A polynomial is irreducible in GF(p) if it does not factor over GF(p). Otherwise it is reducible.

Examples:

```
Factor(x^5+x^4+x^3+x+1) mod 5;
```

over Z_5

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

```
Factor(x^5+x^4+x^3+x+1) mod 2;
```

Z_2

$$x^5+x^4+x^3+x+1$$

The same polynomial is reducible in $\mathbf{Z_5}$
but irreducible in $\mathbf{Z_2}$.

Implementing GF(p^k) arithmetic

Theorem: Let $f(x)$ be an irreducible polynomial of degree k over Z_p.

The finite field $GF(p^k)$ can be realized as the set of degree k-1 polynomials over Z_p, with addition and multiplication done modulo $f(x)$.

mod p

Z_p

$p = 2$

2^k

Example: Implementing GF(2^k)

By the theorem, the finite field $GF(2^5)$ can be realized as the set of degree 4 polynomials over Z_2, with addition and multiplication done modulo the irreducible polynomial $f(x)=x^5+x^4+x^3+x+1$.

$ax=0$

The coefficients of polynomials over Z_2 are 0 or 1.
So, a degree k polynomial can be written down by k+1 bits.
For example, with k=4:

$x^3+x+1 \longleftrightarrow (0,1,0,1,1)$

$x^4+x^3+x+1 \longleftrightarrow (1,1,0,1,1)$

Implementing GF(2^k)

Addition: bit-wise XOR (since 1+1=0)

$\mathbb{Z}_2 = \{0,1\}$

XOR.

	x^3+x+1	(0,1,0,1,1)
+	x^4+x^3+x	(1,1,0,1,0)
	x^4+1	(1,0,0,0,1)

x^4

Implementing GF(2^k)

Multiplication: Polynomial multiplication, and then remainder modulo the defining polynomial f(x):

```
> g(x):=(x^4+x^3+x+1)*(x^3+x+1);
```

$$g(x) := (x^4+x^3+x+1)(x^3+x+1)$$

(1,1,0,1,1) *(0,1,0,1,1)

```
> f(x):=x^5+x^4+x^3+x+1;
```

$$f(x) := x^5+x^4+x^3+x+1$$

= (1,1,0,0,1)

$$1+3x^4+x^3+2x$$

```
> % mod 2;
```

$$1+x^4+x^3$$

How to find inverse modulo an irreducible polynomial ? Using Extended Euclidean Algorithm

Extended Euclidean Algorithm

	Remainder	Quotient		Auxiliary	
m(x)	$2^8 + 2^6 + 2^5 + 2^1 + 2^0$		Q1	0	A1
f(x)	$2^6 + 2^4 + 2^2$		Q2	1	A2
m(x)/f(x)	$2^5 + 2^4 + 2^1 + 2^0$	2^2	Q3	2^2	A3
	2^0	$2^1 + 2^0$	Q4	$2^3 + 2^2 + 1$	A4

A3 = A1 + A2*Q3

A4 = A2 + A3*Q4

Thank you