296.3:Algorithms in the Real World

Finite Fields review

Finite Fields Outline

Groups
- Definitions, Examples, Properties
- Multiplicative group modulo n

Fields
- Definition, Examples
- Polynomials
- Galois Fields

Why review finite fields?

Groups

A **Group** (*G*,*,I) is a set *G* with operator * such that:

1. **Closure**. For all $a,b \in G$, $a * b \in G$
2. **Associativity**. For all $a,b,c \in G$, $a*(b*c) = (a*b)*c$
3. **Identity**. There exists $I \in G$, such that for all $a \in G$, $a*I=I*a=a$
4. **Inverse**. For every $a \in G$, there exist a unique element $b \in G$, such that $a*b=b*a=I$

An **Abelian or Commutative Group** is a Group with the additional condition

5. **Commutativity**. For all $a,b \in G$, $a*b=b*a$

Examples of groups

- Integers, Reals or Rationals with Addition
- The nonzero Reals or Rationals with Multiplication
- Non-singular n x n real matrices with Matrix Multiplication
- Permutations over n elements with composition
  $[0\to1, 1\to2, 2\to0] \circ [0\to1, 1\to0, 2\to2] = [0\to0, 1\to2, 2\to1]$

We will only be concerned with **finite groups**, I.e., ones with a finite number of elements.

Key properties of finite groups

Notation: $a^j \equiv a * a * a * \ldots$ j times

Theorem (Fermat's little): for any finite group $(G,*,I)$ and $g \in G$, $g^{|G|} = I$

Definition: the **order** of $g \in G$ is the smallest positive integer m such that $g^m = I$

Definition: a group G is **cyclic** if there is a $g \in G$ such that order(g) = |G|

Definition: an element $g \in G$ of order |G| is called a **generator** or **primitive element** of G.

Groups based on modular arithmetic

The group of positive integers modulo a prime p

$Z_p^* \equiv \{1, 2, 3, \ldots, p-1\}$

$*_p \equiv$ multiplication modulo p

Denoted as: $(Z_p^*, *_p)$

Required properties

1. Closure. Yes.
2. Associativity. Yes.
3. Identity. 1.
4. Inverse. Yes.

Example: $Z_7^* = \{1,2,3,4,5,6\}$

$1^{-1} = 1,\ 2^{-1} = 4,\ 3^{-1} = 5,\ 6^{-1} = 6$

Other properties

$|Z_p^*| = (p-1)$

By Fermat's little theorem: $a^{(p-1)} = 1 \pmod p$

Example of Z_7^*

	x	x^2	x^3	x^4	x^5	x^6
	1	1	1	1	1	1
	2	4	1	2	4	1
Generators	**3**	**2**	**6**	**4**	**5**	**1**
	4	2	1	4	2	1
Generators	**5**	**4**	**6**	**2**	**3**	**1**
	6	1	6	1	6	1

For all p the group is cyclic.

Fields

A **Field** is a set of elements F with binary operators * and + such that

1. (F, +) is an **abelian group**
2. $(F \setminus I_+, *)$ is an **abelian group** the "multiplicative group"
3. **Distribution**: $a*(b+c) = a*b + a*c$
4. **Cancellation**: $a*I_+ = I_+$

The **order** of a field is the number of elements.

A field of finite order is a **finite field**.

The reals and rationals with + and * are fields.

Finite Fields

Z_p (p prime) with + and * mod p, is a **finite** field.

1. (Z_p, +) is an **abelian group** (0 is identity)
2. (Z_p \ 0, *) is an **abelian group** (1 is identity)
3. **Distribution**: a*(b+c) = a*b + a*c
4. **Cancellation**: a*0 = 0

Are there other finite fields?

What about ones that fit nicely into bits, bytes and words (i.e., with 2^k elements)?

Polynomials over Z_p

$Z_p[x]$ = polynomials on x with coefficients in Z_p.

- Example of $Z_5[x]$: $f(x) = 3x^4 + 1x^3 + 4x^2 + 3$
- deg(f(x)) = 4 (the **degree** of the polynomial)

Operations: (examples over $Z_5[x]$)

- Addition: $(x^3 + 4x^2 + 3) + (3x^2 + 1) = (x^3 + 2x^2 + 4)$
- Multiplication: $(x^3 + 3) * (3x^2 + 1) = 3x^5 + x^3 + 4x^2 + 3$
- $I_+ = 0$, $I_* = 1$
- + and * are associative and commutative
- Multiplication distributes and 0 cancels

Do these polynomials form a field?

Division and Modulus

Long division on polynomials ($Z_5[x]$):

$$
\begin{array}{r|r}
 & \boxed{x+4} \\
x^2+1 & x^3+4x^2+0x+3 \\
 & \underline{x^3+0x^2+1x+0} \\
 & 4x^2+4x+3 \\
 & \underline{4x^2+0x+4} \\
 & \boxed{4x+4}
\end{array}
$$

$(x^3+4x^2+3)/(x^2+1) = (x+4)$ with remainder $4x+4$

$(x^3+4x^2+3) \bmod (x^2+1) = (4x+4)$

$(x^2+1)(x+4)+(4x+4) = (x^3+4x^2+3)$

Polynomials modulo Polynomials

How about making a field of polynomials modulo another polynomial? This is analogous to Z_p (i.e., integers modulo another integer).

e.g., $Z_5[x]$ mod (x^2+2x+1)

Does this work? Problem: (x+1)(x+1) = 0

Multiplication not closed over non-zero polynomials!

Definition: An **irreducible polynomial** is one that is not a product of two other polynomials both of degree greater than 0.

e.g., $(x^2 + 2)$ for $Z_5[x]$

Analogous to a prime number.

Galois Fields

The polynomials

$Z_p[x] \bmod p(x)$

where

$p(x) \in Z_p[x]$,

$p(x)$ is irreducible,

and $\deg(p(x)) = n$ (i.e., n+1 coefficients)

form a finite field. Such a field has p^n elements.

These fields are called **Galois Fields** or **GF(p^n).**

The special case n = 1 reduces to the fields Z_p

The multiplicative group of GF(p^n)/{0} is cyclic (this will be important later).

GF(2^n)

Hugely practical!

The coefficients are **bits** {0,1}.

For example, the elements of GF(2^8) can be represented as **a byte**, one bit for each term, and GF(2^{64}) as **a 64-bit word**.

- *e.g.*, $x^6 + x^4 + x + 1 = 01010011$

How do we do addition?

Addition over Z_2 corresponds to xor.

- Just take the xor of the bit-strings (bytes or words in practice). This is dirt cheap

Multiplication over GF(2^n)

If n is small enough can use a table of all combinations.

The size will be $2^n \times 2^n$ (e.g. 64K for GF(2^8)).

Otherwise, use standard shift and add (xor)

Note: dividing through by the irreducible polynomial on an overflow by 1 term is simply a test and an xor.

e.g. 0111 / 1001 = 0111

1011 / 1001 = 1011 xor 1001 = 0010

^ just look at this bit for GF(2^3)

Multiplication over GF(2^8)

```
typedef unsigned char uc;

uc mult(uc a, uc b) {
  int p = a;
  uc r = 0;
  while(b) {
    if (b & 1) r = r ^ p;
    b = b >> 1;
    p = p << 1;
    if (p & 0x100) p = p ^ 0x11B;
  }
  return r;
}
```

Finding inverses over $GF(2^n)$

Again, if n is small just store in a table.

- Table size is just 2^n.

For larger n, use Euclid's algorithm.

- This is again easy to do with shift and xors.

Polynomials with coefficients in $GF(p^n)$

Recall that $GF(p^n)$ were defined in terms of coefficients that were themselves fields (*i.e.*, Z_p).

We can apply this **recursively** and define:

$GF(p^n)[x]$ = polynomials on x with coefficients in $GF(p^n)$.

- Example of $GF(2^3)[x]$: $f(x) = 001x^2 + 101x + 010$
  Where 101 is shorthand for x^2+1.

Polynomials with coefficients in $GF(p^n)$

We can make a finite field by using an irreducible polynomial $M(x)$ selected from $GF(p^n)[x]$.

For an order m polynomial and by abuse of notation we write: **$GF(GF(p^n)^m)$**, which has p^{nm} elements.

Used in **Reed-Solomon codes** and **Rijndael**.

- In Rijndael p=2, n=8, m=4, i.e. each coefficient is a byte, and each element is a 4 byte word (32 bits).

Note: all finite fields are isomorphic to $GF(p^n)$, so this is really just another representation of $GF(2^{32})$. This representation, however, has practical advantages.