Number Theory Review

Groups

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

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

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

5. **Commutativity.** For all \(a, b \in G\), \(a \ast b = b \ast a\)

Examples of groups

- Integers, Reals or Rationals with Addition
- The nonzero Reals or Rationals with Multiplication
- Non-singular \(n \times n\) real matrices with Matrix Multiplication
- Permutations over \(n\) elements with composition

\[
\begin{bmatrix}
0 \rightarrow 1, 1 \rightarrow 2, 2 \rightarrow 0
\end{bmatrix} \circ \begin{bmatrix}
0 \rightarrow 1, 1 \rightarrow 0, 2 \rightarrow 2
\end{bmatrix} = \begin{bmatrix}
0 \rightarrow 0, 1 \rightarrow 2, 2 \rightarrow 1
\end{bmatrix}
\]

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

Number Theory Outline

- **Groups**
  - Definitions, Examples, Properties
  - Multiplicative group modulo \(n\)
  - The Euler-phi function

- **Fields**
  - Definition, Examples
  - Polynomials
  - Galois Fields

Why does number theory play such an important role?

It is the mathematics of finite sets of values.
Key properties of finite groups

Notation: \( a^j = a \ast a \ast a \ast \ldots \ast j \) times

Theorem (Fermat's little): for any finite group \((G, \ast, I)\) 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 \( \text{order}(g) = |G| \)

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 \( p \)
\( Z_p^* = \{1, 2, 3, \ldots, p-1\} \)
\( \ast_p = \) multiplication modulo \( p \)
Denoted as: \((Z_p^*, \ast_p)\)

Required properties
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: \( a^{(p-1)} = 1 \) (mod \( p \))
Example of \( Z_7^* \)

<table>
<thead>
<tr>
<th></th>
<th>x1</th>
<th>x2</th>
<th>x3</th>
<th>x4</th>
<th>x5</th>
<th>x6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>6</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>6</td>
</tr>
</tbody>
</table>

Generators

For all \( p \) the group is cyclic.

Fields

A Field is a set of elements \( F \) with binary operators \( \ast \) and \( + \) such that
1. \((F, +)\) is an abelian group
2. \((F \setminus I, \ast)\) is an abelian group
   the "multiplicative group"
3. Distribution: \( a \ast (b + c) = a \ast b + a \ast c \)
4. Cancellation: \( a \ast I_+ = I_+ \)

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 \( \ast \) are fields.
Finite Fields

$\mathbb{Z}_p$ (p prime) with + and * mod p, is a finite field.
1. $(\mathbb{Z}_p, +)$ is an abelian group (0 is identity)
2. $(\mathbb{Z}_p \setminus 0, *)$ 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 $\mathbb{Z}_p$

$\mathbb{Z}_p[x] = \text{polynomials on } x \text{ with coefficients in } \mathbb{Z}_p$.
- Example of $\mathbb{Z}_5[x]$: $f(x) = 3x^4 + 1x^3 + 4x^2 + 3$
- $\deg(f(x)) = 4$ (the degree of the polynomial)

Operations: (examples over $\mathbb{Z}_5[x]$)
• Addition: $(x^3 + 4x^2 + 3) + (3x^2 + 1) = (x^3 + 2x^2 + 4)$
• Multiplication: $(x^3 + 3) * (3x^2 + 1) = 3x^5 + x^3 + 4x^2 + 3$
• $I_+, I_* = 0, 1$
• + and * are associative and commutative
• Multiplication distributes and 0 cancels
Do these polynomials form a field?

Division and Modulus

Long division on polynomials ($\mathbb{Z}_5[x]$):

\[
x^2 + 1 \quad \overline{\begin{align*}
x^3 &+ 4x^2 + 0x + 3 \\
x^3 &+ 0x^2 + 1x + 0 \\
&- \hline \\
&4x^2 + 4x + 3 \\
&4x^2 + 0x + 4 \\
&\hline \\
&(x^3 + 4x^2 + 3)/(x^2 + 1) = (x + 4) \\
&(x^3 + 4x^2 + 3) \mod(x^2 + 1) = (4x + 4) \\
&(x^2 + 1)(x + 4) + (4x + 4) = (x^3 + 4x^2 + 3)
\end{align*}}
\]

Polynomials modulo Polynomials

How about making a field of polynomials modulo another polynomial? This is analogous to $\mathbb{Z}_p$ (i.e., integers modulo another integer).

e.g. $\mathbb{Z}_5[x] \mod (x^2+2x+1)$
Does this work?
Does $(x + 1)$ have an inverse?

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 $\mathbb{Z}_5[x]$
Analogous to a prime number.
Galois Fields

The polynomials
\[ \mathbb{Z}_p[x] \mod p(x) \]
where
\[ p(x) \in \mathbb{Z}_p[x], \]
\[ p(x) \text{ is irreducible,} \]
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 \textbf{Galois Fields} or \( \mathbf{GF}(p^n) \).
The special case \( n = 1 \) reduces to the fields \( \mathbb{Z}_p \).
The multiplicative group of \( \mathbf{GF}(p^n)/\{0\} \) is cyclic (this will be important later).

\( \text{GF}(2^n) \)

Hugely practical!
The coefficients are bits \( \{0,1\} \).
For example, the elements of \( \mathbf{GF}(2^8) \) can be represented as a byte, one bit for each term, and \( \mathbf{GF}(2^{64}) \) as a 64-bit word.
- \( \text{e.g.} \ x^6 + x^4 + x + 1 = 01010011 \)

How do we do addition?
Addition over \( \mathbb{Z}_2 \) corresponds to xor.
- Just take the xor of the bit-strings (bytes or words in practice). This is dirt cheap

Multiplication over \( \mathbf{GF}(2^n) \)

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 \( \mathbf{GF}(2^8) \)).
Otherwise, use standard shift and add (xor)

\textbf{Note}: dividing through by the irreducible polynomial on an overflow by 1 term is simply a test and an xor.
\text{e.g.} \ 0111 / 1001 = 0111
1011 / 1001 = 1011 xor 1001 = 0010
\^ just look at this bit for \( \mathbf{GF}(2^3) \)

\textbf{Typedef} unsigned char uc;

\textbf{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 \( \text{GF}(2^n) \)

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

Recall that \( \text{GF}(p^n) \) were defined in terms of coefficients that were themselves fields (i.e., \( \mathbb{Z}_p \)).
We can apply this recursively and define:

\[
\text{GF}(p^n)[x] = \text{polynomials on } x \text{ with coefficients in } \text{GF}(p^n).
\]
- Example of \( \text{GF}(2^3)[x] \): \( f(x) = 001x^2 + 101x + 010 \)
  Where 101 is shorthand for \( x^2+1 \).

Polynomials with coefficients in \( \text{GF}(p^n) \)

We can make a finite field by using an irreducible polynomial \( M(x) \) selected from \( \text{GF}(p^n)[x] \).
For an order \( m \) polynomial and by abuse of notation we write: \( \text{GF}(\text{GF}(p^n)^m) \), 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 \( \text{GF}(p^n) \), so this is really just another representation of \( \text{GF}(2^{32}) \).
This representation, however, has practical advantages.