Finite Fields

Mike Reiter
reiter@cs.unc.edu


Groups

A group \( \langle G, \cdot \rangle \) is a set \( G \) of elements with a binary operation \( \cdot \) satisfying the following properties

- Closure: \( \forall a, b \in G : a \cdot b \in G \)
- Associativity: \( \forall a, b, c \in G : a \cdot (b \cdot c) = (a \cdot b) \cdot c \)
- Identity element: \( \exists e \in G : \forall a \in G : a \cdot e = e \cdot a = a \)
- Inverse element: \( \forall a \in G : \exists a' \in G : a \cdot a' = a' \cdot a = e \)

If \( G \) has a finite number of elements, then it is a finite group, and the order of the group is the size of \( G \).

A group \( \langle G, \cdot \rangle \) is abelian if it also satisfies the following

- Commutative: \( \forall a, b \in G : a \cdot b = b \cdot a \)
Examples of Groups

- The set of bijections on \( n \) elements, with

\[
(\pi \cdot \rho)(i) = \pi(\rho(i))
\]

- Closure: \( \pi \cdot \rho \) is still a bijection on \( n \) elements
- Associative: \( \pi(\rho \cdot \tau)(i) = (\pi \cdot \rho)(\tau(i)) \)
- Identity element: defined by \( \pi(i) = i \)
- Inverse element: If \( \pi(i) = j \) then \( \pi(j) = i \)

- Integers under addition an abelian group?
- Reals under multiplication an abelian group?
- Bijections on \( n \) elements with \( \cdot \) as above an abelian group?

Cyclic Groups

- Define exponentiation in a group as repeated application of the group operator

\[
a^3 = a \cdot a \cdot a, \text{ for example}
\]

\[
a^0 = e
\]

- A group \( \langle G, \cdot \rangle \) is cyclic if

\[
\exists a \in G : \forall b \in G : \exists k : b = a^k
\]

\[
a \text{ is said to generate } G, \text{ or to be a generator of } G
\]
Rings

A ring \( \langle R, +, \cdot \rangle \) is a set \( R \) of elements with two binary operators\n
+ (“addition”) and \( \cdot \) (“multiplication”) satisfying\n
\(< R, + > \) is an abelian group, with identity element denoted “0” and the\n
inverse of \( a \) denoted \(-a\)\n
\( \forall a, b \in R : a \cdot b \in R \)\n
\( \forall a, b, c \in R : a \cdot (b \cdot c) = (a \cdot b) \cdot c \)\n
\( \forall a, b, c \in R : a \cdot (b + c) = a \cdot b + a \cdot c \)\n
\( \forall a, b, c \in R : (a + b) \cdot c = a \cdot c + b \cdot c \)\n
A ring is commutative if it satisfies:\n
\( \forall a, b \in R : a \cdot b = b \cdot a \)

Examples of Rings

\( n \times n \) matrices over the reals\n
A ring w.r.t. addition and multiplication?\n
A commutative ring?\n
The even integers\n
A commutative ring w.r.t. addition and multiplication?
Integral Domains and Fields

- A commutative ring \( \langle R, +, \cdot \rangle \) is an integral domain if it obeys
  - Multiplicative identity: \( \exists 1 \in R : \forall a \in R : a \cdot 1 = 1 \cdot a = a \)
  - No zero divisors: \( \forall a, b \in R : a \cdot b = 0 \Rightarrow a = 0 \lor b = 0 \)

- Example: Integers under addition and multiplication?

- A integral domain \( \langle F, +, \cdot \rangle \) is a field if it obeys
  - Multiplicative inverse: \( \forall a \in F \setminus \{0\} : \exists a^{-1} \in F : a \cdot a^{-1} = a^{-1} \cdot a = 1 \)

- Example: Integers under addition and multiplication?
- Example: Rationals under addition and multiplication?
Modular Arithmetic

- Given a positive integer $n$ and any integer $a$, if we divide $a$ by $n$ we get an integer quotient $q$ and an integer remainder $r$

$$a = qn + r \quad \text{where} \quad 0 \leq r < n \quad \text{and} \quad q = \lfloor a/n \rfloor$$

- $\lfloor x \rfloor$ denotes the largest integer less than or equal to $x$
- $r$ is often called a residue

- Define $a \mod n$ to be the residue when $a$ is divided by $n$

- Integers $a$ and $b$ are congruent mod $n$ if $(a \mod n) = (b \mod n)$
  - This is written $a \equiv b \mod n$

Divisors

- Nonzero $b$ divides $a$ if $a = mb$ for some $m$, where $a$, $b$, $m$ are integers, i.e., if $a \equiv 0 \mod b$
  - Notation: $b|a$ means $b$ divides $a$

- The following relations hold
  - If $a|1$ then $a = \pm 1$
  - If $a|b$ and $b|a$ then $a = \pm b$
  - Any $b \not= 0$ divides 0
  - If $b|g$ and $b|h$ then $b|(mg+nh)$ for any integers $m$ and $n$
Properties of mod

- \( n \mid (a - b) \Rightarrow a \equiv b \mod n \)
- \( a \equiv b \mod n \Rightarrow b \equiv a \mod n \)
- \( a \equiv b \mod n \land b \equiv c \mod n \Rightarrow a \equiv c \mod n \)

- Properties of modular arithmetic
  - \((a \mod n) + (b \mod n) \equiv (a + b) \mod n\)
  - \((a \mod n) - (b \mod n) \equiv (a - b) \mod n\)
  - \((a \mod n) \cdot (b \mod n) \equiv (a \cdot b) \mod n\)

- If we let \( \mathbb{Z}_n = \{0, 1, 2, ..., n-1\} \), then \( \langle \mathbb{Z}_n, +, \cdot \rangle \) is a commutative ring

Greatest Common Divisors

- Positive integer \( c \) is the greatest common divisor of \( a \) and \( b \) if
  - \( c \) is a divisor of \( a \) and of \( b \)
  - Any divisor of \( a \) and \( b \) is a divisor of \( c \)
- We denote \( c \) by \( \gcd(a, b) \)

- Because we require \( \gcd(a, b) \) to be positive,
  \[ \gcd(a, b) = \gcd(a, -b) = \gcd(-a, -b) \]

- \( a \) and \( b \) are relatively prime if \( \gcd(a, b) = 1 \)
Euclid’s Algorithm for Computing gcd

Fact: If \( a \geq 0 \) and \( b > 0 \), then \( \gcd(a, b) = \gcd(b, a \mod b) \).

Proof: Note that \( a \mod b = a - kb \) for some integer \( k \).

Lemma 1: If \( d \mid a \) and \( d \mid b \), then \( d \mid (a \mod b) \).

Proof: Since \( d \mid a \) and \( d \mid b \), it is the case that \( d \mid (a - kb) \).

Lemma 2: If \( d \mid b \) and \( d \mid (a \mod b) \), then \( d \mid a \).

Proof: \( d \mid kb \) and \( d \mid (a - kb) \) and so \( d \mid (a - kb + kb) \).

Thus the set of common divisors for \( a \) and \( b \) is the same as the set of common divisors for \( b \) and \( a \mod b \).

Euclid’s Algorithm for Computing gcd

```c
/* Assumption: a, b > 0 */

int Euclid(a, b) {
    A ← a; B ← b;
    while (B > 0) {
        R ← A mod B;
        A ← B; B ← R;
    }
    return A;
}
```

For arbitrary integers \( a, b \), invoke as \( \text{Euclid}(\left|a\right|, \left|b\right|) \).
Computing Multiplicative Inverses

- Fact: If $\gcd(m, b) = 1$, then $b$ has a multiplicative inverse mod $m$.
  - Corollary: If $p$ is prime, then $(\mathbb{Z}_p, +, \cdot)$ satisfies "multiplicative inverse".

```c
int ExtendedEuclid(m, b) {
    (A1, A2, A3) ← (1, 0, m);
    (B1, B2, B3) ← (0, 1, b);
    while (B3 > 1) {
        Q ← \lfloor A3/B3 \rfloor;
        (T1, T2, T3) ← (A1−Q·B1, A2−Q·B2, A3−Q·B3);
        (A1, A2, A3) ← (B1, B2, B3);
        (B1, B2, B3) ← (T1, T2, T3);
    }
    if (B3 = 1) return B2; else return null;
}
```

Computing Multiplicative Inverses

- Why does the extended Euclidean algorithm work?
- First note that $A3$ and $B3$ in `ExtendedEuclid` are treated identically to $A$ and $B$ in `Euclid`
  - Except that exit condition from loop is weaker in `ExtendedEuclid`
- Loop invariants in `ExtendedEuclid`
  - $m·A1 + b·A2 = A3$
  - $m·B1 + b·B2 = B3$
Computing Multiplicative Inverses

- If $1 \leftrightarrow \text{Euclid}(m, b)$, then at start of its last loop iteration, $A = 0$ and $B = 1$

- Now consider the corresponding point in ExtendedEuclid, at which point the while loop terminates (since $B_3 = 1$)
  
  \[ m \cdot B_1 + b \cdot B_2 = B_3 \]
  
  \[ m \cdot B_1 + b \cdot B_2 = 1 \]
  
  \[ (m \cdot B_1 + b \cdot B_2) \mod m = 1 \mod m \]

- That is, $B_2$ is $b^{-1} \mod m$

Polynomial Arithmetic

- A polynomial of degree $n \geq 0$ is an expression of the form
  \[ f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i \]

- If
  \[ f(x) = \sum_{i=0}^{n} a_i x^i; \quad g(x) = \sum_{i=0}^{m} b_i x^i; \quad n \geq m \]
  
  then their addition is defined as
  \[ f(x) + g(x) = \sum_{i=0}^{m} (a_i + b_i) x^i + \sum_{i=n+1}^{n} a_i x^i \]
Polynomial Arithmetic

- Multiplication is defined as
  \[ f(x) \cdot g(x) = \sum_{i=0}^{n+m} c_i x^i \]
  where \( c_k = a_0 \cdot b_k + a_1 \cdot b_{k-1} + \ldots + a_{k-1} \cdot b_1 + a_k \cdot b_0 \) and \( a_i = 0 \) for \( i > n \) and \( b_i = 0 \) for \( i > m \)

- If coefficients are in a field \( F \), then we define division as
  \[ \frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)} \]
  i.e., \( f(x) = q(x) \cdot g(x) + r(x) \) where \( q(x) \) is of degree \( n-m \) and \( r(x) \) is of degree at most \( m-1 \)

Irreducible Polynomials and gcd

- A polynomial \( f(x) \) over a field \( F \) is irreducible iff \( f(x) \) cannot be expressed as a product of two polynomials, both over \( F \), and both of degree lower than \( f(x) \)
  - Also called a prime polynomial, by analogy to integers

- Polynomial \( c(x) \) is the greatest common divisor (“gcd”) of \( a(x) \) and \( b(x) \) if
  - \( c(x) \) divides both \( a(x) \) and \( b(x) \)
  - Any divisor of \( a(x) \) and \( b(x) \) is a divisor of \( c(x) \)

- Fact: \( \gcd(a(x), b(x)) = \gcd(b(x), a(x) \mod b(x)) \)
  - By analogy to the integers, we write \( f(x) \mod g(x) \) for the residue of \( f(x)/g(x) \)
Euclid’s Algorithm for Polynomials

```c
/* Assumption: deg(a(x)) > deg(b(x)) */
polynomial Euclid(a(x), b(x)) {
    A(x) ← a(x); B(x) ← b(x);
    while (B(x) ≠ 0) {
        R(x) ← A(x) mod B(x);
        A(x) ← B(x); B(x) ← R(x);
    }
    return A(x);
}
```

Computing Polynomial Inverses

- If gcd(m(x),b(x)) = 1, same extension computes \( b(x)^{-1} \mod m(x) \)

```c
polynomial ExtendedEuclid(m(x), b(x)) {
    (A1(x),A2(x),A3(x)) ← (1,0,m(x));
    (B1(x),B2(x),B3(x)) ← (0,1,b(x));
    while (B3(x) ∉ {0,1}) {
        Q(x) ← quotient of A3(x)/B3(x);
        (T1(x),T2(x),T3(x)) ← (A1(x)−Q(x)⋅B1(x),
                                A2(x)−Q(x)⋅B2(x),
                                A3(x)−Q(x)⋅B3(x));
        (A1(x),A2(x),A3(x)) ← (B1(x),B2(x),B3(x));
        (B1(x),B2(x),B3(x)) ← (T1(x),T2(x),T3(x));
    }
    if (B3(x)=1) return B2(x); else return null;
}
```
Finite Fields of Non-Prime Order

- Fact: The order of any finite field must be $p^n$ for some prime $p$ and positive integer $n$.
- Fact: $\langle \mathbb{Z}_p, +, \cdot \rangle$ is a field.
  - However, $\langle \mathbb{Z}_{p^n}, +, \cdot \rangle$ is generally not.
- What structure with $p^n$ elements is a field?

- Motivating example: Suppose we want to define a field with $2^n$ elements, so we can represent it with $n$ bits?
  - $\langle \mathbb{Z}_{2^n}, +, \cdot \rangle$ is not a field, and so we can’t do division in it

---

Finite Fields of Non-Prime Order

- Consider the set of all polynomials of degree $n - 1$ or less over the field $\mathbb{Z}_p$, with ordinary polynomial arithmetic where
  - Arithmetic on coefficients is performed in $\langle \mathbb{Z}_p, +, \cdot \rangle$
  - Multiplication is reduced modulo some irreducible polynomial $m(x)$ of degree $n$

- Fact: This is a finite field of order $p^n$.
  - We denote this by $\text{GF}(p^n)$

- Fact: All finite fields of a given order are isomorphic.
Finite Field \(GF(2^n)\)

- We will typically be most interested in polynomials with coefficients in the field \(GF(2) = \langle \mathbb{Z}_2, +, \cdot \rangle\).
- In \(GF(2)\),
  - Addition is equivalent to logical exclusive-OR (XOR)
  - Multiplication is equivalent to logical AND
  - Addition and subtraction are equivalent

- Represent an element of \(GF(2^n)\) by the \(n\)-bit vector of its coefficients
  - E.g., \(f(x) = x^6 + x^4 + x^2 + x + 1\) in \(GF(2^8)\) is represented by 01010111
- Then, addition of two elements in \(GF(2^n)\) is simply their XOR
  - Very, very efficient

Finite Field \(GF(2^n)\)

- Multiplication in \(GF(2^n)\) can be done efficiently using the fact that for a degree-\(n\) polynomial \(m(x) = x^n + \ldots\),
  \[ x^n \mod m(x) = m(x) - x^n \]
- Now consider multiplication \(x \cdot f(x) \mod m(x)\), where
  \[ m(x) = x^n + \sum_{i=0}^{n-1} a_i x^i \]
  is irreducible, and
  \[ f(x) = \sum_{i=0}^{n-1} b_i x^i \]
Finite Field $GF(2^n)$

\[ x \cdot f(x) \mod m(x) = \sum_{i=0}^{n-1} b_i x^{i+1} \mod m(x) \]
\[ = b_{n-1} x^n \mod m(x) + \sum_{i=0}^{n-2} b_i x^{i+1} \]
\[ = \begin{cases} 
\sum_{i=0}^{n-2} b_i x^{i+1} & \text{if } b_{n-1} = 0 \\
m(x) - x^n + \sum_{i=0}^{n-2} b_i x^{i+1} & \text{if } b_{n-1} = 1 
\end{cases} \]

Finite Field $GF(2^n)$

- So, to compute $x \cdot f(x) \mod m(x)$, compute it as

\[ x \cdot f(x) = \begin{cases} 
(b_{n-2} b_{n-3} \ldots b_0 0) & \text{if } b_{n-1} = 0 \\
(b_{n-2} b_{n-3} \ldots b_0 0) \oplus (a_{n-1} a_{n-2} \ldots a_0) & \text{if } b_{n-1} = 1 
\end{cases} \]

- Multiplication by a higher power of $x \cdot f(x)$ can be computed by repeated application