Overview

1. The Euclidean Algorithm for GCD
2. Modular Arithmetic
3. Groups, Rings, and Fields
4. Galois Fields GF(p)
5. Polynomial Arithmetic

Euclid's Algorithm

- Goal: To find greatest common divisor
- Example: \( \text{gcd}(10, 25) = 5 \) using long division

10) 25 (2
  20
  --
5) 10 (2
  10
  --
  00

Test: What is GCD of 12 and 105?
**Euclid's Algorithm: Tabular Method**

<table>
<thead>
<tr>
<th>10</th>
<th>25</th>
</tr>
</thead>
<tbody>
<tr>
<td>$q_i$</td>
<td>$r_i$</td>
</tr>
<tr>
<td>0</td>
<td>25</td>
</tr>
<tr>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

- $r_i = u_i x + v_i y$
- $u_i = u_{i-2} - q_i u_{i-1}$
- $v_i = v_{i-2} - q_i v_{i-1}$

1. Write the first 2 rows. Set $i = 2$.
2. Divide $r_{i-1}$ by $r_i$, write quotient $q_{i+1}$ on the next row.
3. Fill out the remaining entries in the new bottom row:
   a. Multiply $r_i$ by $q_{i+1}$ and subtract from $r_{i-1}$
   b. Multiply $u_i$ by $q_{i+1}$ and subtract from $u_{i-1}$
   c. Multiply $v_i$ by $q_{i+1}$ and subtract from previous $v_{i-1}$

Finally, If $r_i = 0$, $\gcd(x, y) = r_{i-1}$

If $\gcd(x, y) = 1$, $u_i x + v_i y = 1 \Rightarrow x^{-1} \mod y = u_i$  
$\Rightarrow u_i$ is the inverse of $x$ in “mod $y$” arithmetic.
Euclid’s Algorithm Tabular Method (Cont)

Example 2: Fill in the blanks

<table>
<thead>
<tr>
<th>( q_i )</th>
<th>( r_i )</th>
<th>( u_i )</th>
<th>( v_i )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>15</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>8</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Homework 4A

- Find the multiplicative inverse of 5678 mod 8765
- Do it on your own. Do not submit.
- Answer: 2527
Modular Arithmetic

- $xy \mod m = (x \mod m)(y \mod m) \mod m$
- $(x+y) \mod m = ((x \mod m) + (y \mod m)) \mod m$
- $(x-y) \mod m = ((x \mod m) - (y \mod m)) \mod m$
- $x^4 \mod m = (x^2 \mod m)(x^2 \mod m) \mod m$
- $x^{ij} \mod m = (x^i \mod m)^j \mod m$
- $125 \mod 187 = 125$
- $(225+285) \mod 187 = (225 \mod 187) + (285 \mod 187) = 38 + 98 = 136$
- $125^2 \mod 187 = 15625 \mod 187 = 104$
- $125^4 \mod 187 = (125^2 \mod 187)^2 \mod 187$
  $= 104^2 \mod 187 = 10816 \mod 187 = 157$
- $125^6 \mod 187 = 125^{4+2} \mod 187 = (157 \times 104) \mod 187 = 59$
Modular Arithmetic Operations

- \( Z = \text{Set of all integers} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \)
- \( Z_n = \text{Set of all non-negative integers less than } n = \{0, 1, 2, \ldots, n-1\} \)
- \( Z_2 = \{0, 1\} \)
- \( Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\} \)
- Addition, Subtraction, Multiplication, and division can all be defined in \( Z_n \)
- For Example:
  - \((5+7) \mod 8 = 4\)
  - \((4-5) \mod 8 = 7\)
  - \((5 \times 7) \mod 8 = 3\)
  - \((3/7) \mod 8 = 5\)
  - \((5 \times 5) \mod 8 = 1\)
# Modular Arithmetic Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commutative laws</td>
<td>$(w + x) \mod n = (x + w) \mod n$</td>
</tr>
<tr>
<td></td>
<td>$(w \times x) \mod n = (x \times w) \mod n$</td>
</tr>
<tr>
<td>Associative laws</td>
<td>$[((w + x) + y) \mod n = [w + (x + y)] \mod n]$</td>
</tr>
<tr>
<td></td>
<td>$[((w \times x) \times y) \mod n = [w \times (x \times y)] \mod n$</td>
</tr>
<tr>
<td>Distributive law</td>
<td>$[w \times (x + y)] \mod n = [(w \times x) + (w \times y)] \mod n$</td>
</tr>
<tr>
<td>Identities</td>
<td>$(0 + w) \mod n = w \mod n$</td>
</tr>
<tr>
<td></td>
<td>$(1 \times w) \mod n = w \mod n$</td>
</tr>
<tr>
<td>Additive inverse $(-w)$</td>
<td>For each $w \in Z_n$, there exists a $z$ such that $w + z = 0 \mod n$</td>
</tr>
</tbody>
</table>
Homework 4B

- Determine $125^{107} \mod 187$
- Do it on your own. Do not submit.
- Answer: 5
Group

- **Group**: A set of elements that is closed with respect to some operation.
- **Closed** ⇒ The result of the operation is also in the set
- The operation obeys:
  - Obeys associative law: \((a \cdot b) \cdot c = a \cdot (b \cdot c)\)
  - Has identity \(e\): \(e \cdot a = a \cdot e = a\)
  - Has inverses \(a^{-1}\): \(a \cdot a^{-1} = e\)
- **Abelian Group**: The operation is commutative
  \(a \cdot b = b \cdot a\)
- **Example**: \(Z_8\), + modular addition, identity = 0
Cyclic Group

- **Exponentiation**: Repeated application of operator
  - example: \(a^3 = a \cdot a \cdot a\)

- **Cyclic Group**: Every element is a power of some fixed element, i.e.,
  \[b = a^k\] for some \(a\) and every \(b\) in group
  - \(a\) is said to be a generator of the group

- Example: \{0, 1, 2, 4, 8\} with **mod 12** multiplication,
  - the generator is 2.

- \(2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 4, 2^5 = 8\)
Ring

- **Ring:**
  1. A group with two operations: addition and multiplication
  2. The group is abelian with respect to addition: \( a + b = b + a \)
  3. Multiplication and additions are both associative:
     \[ a + (b + c) = (a + b) + c \]
     \[ a \cdot (b \cdot c) = (a \cdot b) \cdot c \]
  1. Multiplication distributes over addition
     \[ a \cdot (b + c) = a \cdot b + a \cdot c \]
     \[ (a + b) \cdot c = a \cdot c + b \cdot c \]

- **Commutative Ring:** Multiplication is commutative, i.e.,
  \[ a \cdot b = b \cdot a \]

- **Integral Domain:** Multiplication operation has an identity
  and no zero divisors

Consider the set $S = \{a, b, c\}$ with addition and multiplication defined by the following tables:

<table>
<thead>
<tr>
<th>+</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>a</td>
<td>c</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>c</td>
<td>a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\times$</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>b</td>
<td>c</td>
</tr>
</tbody>
</table>

Is $S$ a ring? Justify your answer.
Field

- **Field**: An integral domain in which each element has a multiplicative inverse.

### Properties of Fields

- **Field**
- **Integral domain**
- **Commutative ring**
- **Ring**
- **Abelian group**
- **Group**

#### Field Properties

- (A1) Closure under addition:
- (A2) Associativity of addition:
- (A3) Additive identity:
- (A4) Additive inverse:
- (A5) Commutativity of addition:
- (M1) Closure under multiplication:
- (M2) Associativity of multiplication:
- (M3) Distributive laws:
- (M4) Commutativity of multiplication:
- (M5) Multiplicative identity:
- (M6) No zero divisors:
- (M7) Multiplicative inverse:
Finite Fields or Galois Fields

- Finite Field: A field with finite number of elements
- Also known as Galois Field
- The number of elements is always a power of a prime number. Hence, denoted as $\text{GF}(p^n)$
- $\text{GF}(p)$ is the set of integers $\{0,1, \ldots, p-1\}$ with arithmetic operations modulo prime $p$
- Can do addition, subtraction, multiplication, and division without leaving the field $\text{GF}(p)$
- $\text{GF}(2) = \text{Mod } 2$ arithmetic
  $\text{GF}(8) = \text{Mod } 8$ arithmetic
- There is no $\text{GF}(6)$ since 6 is not a power of a prime.
**GF(7) Multiplication Example**

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Polynomial Arithmetic

\[ f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = \sum a_ix^i \]

1. Ordinary polynomial arithmetic:
   - Add, subtract, multiply, divide polynomials,
   - Find remainders, quotient.
   - Some polynomials have no factors and are prime.

2. Polynomial arithmetic with \text{mod } p coefficients

3. Polynomial arithmetic with \text{mod } p coefficients and mod \text{ } m(x) operations
Polynomial Arithmetic with Mod 2 Coefficients

- All coefficients are 0 or 1, e.g.,
  
  let \( f(x) = x^3 + x^2 \) and \( g(x) = x^2 + x + 1 \)
  
  \[ f(x) + g(x) = x^3 + x + 1 \]
  
  \[ f(x) \times g(x) = x^5 + x^2 \]

- **Polynomial Division**: \( f(x) = q(x) g(x) + r(x) \)
  
  - can interpret \( r(x) \) as being a remainder
  
  - \( r(x) = f(x) \mod g(x) \)
  
  - if no remainder, say \( g(x) \) divides \( f(x) \)
  
  - if \( g(x) \) has no divisors other than itself & 1 say it is **irreducible** (or prime) polynomial

- Arithmetic modulo an irreducible polynomial forms a finite field

- Can use Euclid’s algorithm to find gcd and inverses.
Example GF($2^3$)

### Table 4.7 Polynomial Arithmetic Modulo ($x^3 + x + 1$)

#### (a) Addition

<table>
<thead>
<tr>
<th></th>
<th>000</th>
<th>001</th>
<th>010</th>
<th>011</th>
<th>100</th>
<th>101</th>
<th>110</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>0</td>
<td>1</td>
<td>x</td>
<td>x+1</td>
<td>x^2</td>
<td>x^2+1</td>
<td>x^2+x</td>
<td>x^2+x+1</td>
</tr>
<tr>
<td>000</td>
<td>0</td>
<td>1</td>
<td>x</td>
<td>x+1</td>
<td>x^2</td>
<td>x^2+1</td>
<td>x^2+x</td>
<td>x^2+x+1</td>
</tr>
<tr>
<td>001</td>
<td>1</td>
<td>0</td>
<td>x+1</td>
<td>x</td>
<td>x^2+1</td>
<td>x^2</td>
<td>x^2+x+1</td>
<td>x^2+x</td>
</tr>
<tr>
<td>010</td>
<td>x</td>
<td>x+1</td>
<td>0</td>
<td>1</td>
<td>x^2+x</td>
<td>x^2+x+1</td>
<td>x^2</td>
<td>x^2+1</td>
</tr>
<tr>
<td>011</td>
<td>x+1</td>
<td>x</td>
<td>1</td>
<td>0</td>
<td>x^2+x+1</td>
<td>x^2+x</td>
<td>x^2+1</td>
<td>x^2</td>
</tr>
<tr>
<td>100</td>
<td>x^2</td>
<td>x^2+1</td>
<td>x^2+x</td>
<td>x^2+x+1</td>
<td>0</td>
<td>1</td>
<td>x</td>
<td>x+1</td>
</tr>
<tr>
<td>101</td>
<td>x^2+1</td>
<td>x^2</td>
<td>x^2+x+1</td>
<td>x^2+x</td>
<td>1</td>
<td>0</td>
<td>x+1</td>
<td>x</td>
</tr>
<tr>
<td>110</td>
<td>x^2+x</td>
<td>x^2+x+1</td>
<td>x^2</td>
<td>x^2+1</td>
<td>x</td>
<td>x+1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>111</td>
<td>x^2+x+1</td>
<td>x^2+x</td>
<td>x^2+1</td>
<td>x</td>
<td>x+1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

#### (b) Multiplication

<table>
<thead>
<tr>
<th></th>
<th>000</th>
<th>001</th>
<th>010</th>
<th>011</th>
<th>100</th>
<th>101</th>
<th>110</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>×</td>
<td>0</td>
<td>1</td>
<td>x</td>
<td>x+1</td>
<td>x^2</td>
<td>x^2+1</td>
<td>x^2+x</td>
<td>x^2+x+1</td>
</tr>
<tr>
<td>000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>001</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>x</td>
<td>x+1</td>
<td>x^2</td>
<td>x^2+1</td>
<td>x^2+x</td>
</tr>
<tr>
<td>010</td>
<td>x</td>
<td>x</td>
<td>x^2</td>
<td>x^2+x</td>
<td>x+1</td>
<td>x^2+1</td>
<td>x^2+x+1</td>
<td>x^2+x</td>
</tr>
<tr>
<td>011</td>
<td>x+1</td>
<td>0</td>
<td>x+1</td>
<td>x^2+x</td>
<td>x^2+1</td>
<td>x^2+x+1</td>
<td>x^2</td>
<td>x^2</td>
</tr>
<tr>
<td>100</td>
<td>x^2</td>
<td>0</td>
<td>x^2</td>
<td>x+1</td>
<td>x^2+x+1</td>
<td>x^2+x</td>
<td>x</td>
<td>x^2+1</td>
</tr>
<tr>
<td>101</td>
<td>x^2+1</td>
<td>0</td>
<td>x^2+1</td>
<td>1</td>
<td>x^2+1</td>
<td>x</td>
<td>x+1</td>
<td>x</td>
</tr>
<tr>
<td>110</td>
<td>x^2+x</td>
<td>0</td>
<td>x^2+x</td>
<td>1</td>
<td>x^2+1</td>
<td>x+1</td>
<td>x</td>
<td>x^2</td>
</tr>
<tr>
<td>111</td>
<td>x^2+x+1</td>
<td>0</td>
<td>x^2+x+1</td>
<td>1</td>
<td>x+1</td>
<td>x</td>
<td>x^2</td>
<td>x^2+1</td>
</tr>
</tbody>
</table>
Computational Example in GF($2^n$)

- Since coefficients are 0 or 1, any polynomial can be represented as a bit string.
- In GF($2^3$), $(x^2+1)$ is $101_2$ & $(x^2+x+1)$ is $111_2$.
- Addition:
  - $(x^2+1) + (x^2+x+1) = x$
  - $101 \text{ XOR } 111 = 010_2$
- Multiplication:
  - $(x+1).(x^2+1) = x.(x^2+1) + 1.(x^2+1) = x^3+x+x^2+1 = x^3+x^2+x+1$
  - $011.101 = (101)<<(1) \text{ XOR } (101)<<(0) = 1111_2$
- Polynomial modulo reduction (get $q(x)$ & $r(x)$) is
  - $(x^3+x^2+x+1) \mod (x^3+x+1) = 1.(x^3+x+1) + (x^2) = x^2$
  - $1111 \mod 1011 = 1111 \text{ XOR } 1011 = 0100_2$
Homework 4D

- Determine the gcd of the following pairs of polynomials over GF(11)
  
  \[ 5x^3 + 2x^2 - 5x - 2 \text{ and } 5x^5 + 2x^4 + 6x^2 + 9x \]
Using a Generator

- A generator $g$ is an element whose powers generate all non-zero elements
  - in $F$ have $0$, $g^0$, $g^1$, ..., $g^{q-2}$
- Can create generator from root of the irreducible polynomial then adding exponents of generator
1. Euclid’s tabular method allows finding gcd and inverses
2. Group is a set of elements and an operation that satisfies closure, associativity, identity, and inverses
3. Abelian group: Operation is commutative
4. Rings have two operations: addition and multiplication
5. Fields: Commutative rings that have multiplicative identity and inverses
6. Finite Fields or Galois Fields have $p^n$ elements where $p$ is prime
7. Polynomials with coefficients in GF($2^n$) also form a field.
Lab Homework 4

This lab consists of using the following tools:

1. Password dump, Pwdump6,

2. John the ripper, Brute force password attack,
   http://www.openwall.com/john/
Lab Homework 4 (Cont)

- If you have two computers, you can install these programs on one computer and conduct these exercises. *Your anti-virus programs may prevent you from doing so.*
- Alternately, you can remote desktop via VPN to CSE571XPS and conduct exercises.
- You need to reserve time in advance.
- Use your last name (with spaces removed) as your user name.
1. PWDump6

- Goal: Get the password hash from CSE571XPC
- On CSE571XPS, open a dos box
- CD to c:\pwdump6
- Run pwdump6 without parameters for help
- Run pwdump6 with parameters to get the hash file from client CSE571XPC
- You will need the common student account and password supplied in the class.
- Open the hash file obtained in notepad. Delete all lines except the one with your last name.
- Save the file as c:\john179\run\<your_last_name>.txt
- Delete the original full hash file that you downloaded
2. Find your password

- On CSE571XPS, use the command box
- CD to c:\john179\run
- Delete john.pot and john.log
- Run john without parameters to get help
- Run john with the file you created in step 1
- This will tell you your password. Note down the contents of john.pot file and submit.
- Delete your hash file, john.pot, and john.log
- logout
- Close your remote desktop session.
3. Change your password

- Now remote desktop to CSE571XPC
- Login using your last name as username and the password you obtained in step 2.
- **Change your password** to a strong password. Do this from your own account (not the common student account).
- Note the time and date you change the password. Submit the time as homework answer.
- Logout