Modular Arithmetic
(Read Sections 4.1 thro 4.4)

- Set of all integers $Z = \{-\infty, \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots, \infty\}$
- Set of positive integers less than $m$
  $Z_m = \{0, 1, 2, 3, \ldots, m-1\}$
- We want to perform arithmetic in $Z_m$
- Equivalence Classes $a \equiv b \mod m \Rightarrow a = b + cm; \ a, b, c, m \in Z$
- Say $m = 5$
- EC of 0 \{-15, -10, -5, 0, 5, 10, \ldots\}$
  $-15 \equiv -10 \equiv -5 \ldots \equiv 0 \equiv 5 \ldots \mod m$
- EC 0f 1 \{-14, -9, -4, 1, 6, 11, \ldots\}
- EC 0f 2 \{-13, -8, -3, 2, 7, 12, \ldots\}
- EC 0f 3 \{-12, -7, -2, 3, 8, 13, \ldots\}
- EC 0f 4 \{-11, -6, -1, 4, 9, 14, \ldots\}
Addition mod m

\[ a \equiv b \mod m \Rightarrow a = b + k \cdot m \]

\[ c \equiv d \mod m \Rightarrow c = d + l \cdot m \]

\[(a + c) \equiv (c + a) \mod m \]

\[(a + c) \equiv (b + d) \equiv (a + d) \equiv (b + c) \mod m \]

\[(a + c) = b + d + (k + l) \cdot m = (b + d) + j \cdot m \]
Multiplication mod m

\[ a \equiv b \mod m \Rightarrow a = b + k \cdot m \]
\[ c \equiv d \mod m \Rightarrow c = d + l \cdot m \]
\[ ac = (b + k \cdot m)(d + l \cdot m) = bd + (bl + kd + kl \cdot m) \cdot m \]
\[ ac \equiv bd \mod m \]
Multiplicative Inverse

- Is division possible in $\mathbb{Z}$?
- Group, Abelian Group, Ring and Field
  - Group
    - Addition is closed, associative
    - Existence of additive identity, additive inverse
  - Abelian group – addition is also commutative
  - Ring
    - Multiplication is closed, associative, commutative, multiplicative identity, distributive
  - Field – every element except “additive identity” has multiplicative inverse
Multiplicative Inverse

- Additive identity is 0
- Multiplicative identity is 1

Consider \( m = 5 \)
- \( 2 \to \) multiplicative inverse is 3 as \( 2*3 \equiv 1 \mod 5 \)
- \( 3 \to 2 \)
- \( 4 \to 4 \quad 4*4 \equiv 1 \mod 5 \)
  - Obviously 1 is its own inverse

Now \( m = 6 \)
- \( 5 \to \) inverse is 5 as \( 5*5 \equiv 1 \mod 6 \)
- What about 2, 3 and 4? No inverses - why?
Basic Theorems of Arithmetic

- Let $p_i$ represent the $i^{th}$ prime

\[
 n = \prod_{i=1}^{\infty} p_i^{e_i}, \quad e_i > 0
\]

\[
 n = \prod_{i=1}^{\infty} p_i^{n_i}
\]

\[
 m = \prod_{i=1}^{\infty} p_i^{m_i}
\]

\[
 l c m( m, n) = \prod_{i=1}^{\infty} p_i^{\max(n_i, m_i)}
\]

\[
 g c d( m, n) = \prod_{i=1}^{\infty} p_i^{\min(n_i, m_i)}
\]
Preliminaries

- $\text{gcd}(m,n)$ is usually represented as $(m,n)$
- If $n = km$, (and $k$ is an integer) we say $m \mid n$ ($m$ divides $n$)
- The number $s = (m,n)$ is the largest positive integer such that $s \mid m$ and $s \mid n$
- If $(m,n)=1$, and if $m \mid a$ and $n \mid a$ then $mn \mid a$
Algorithm for GCD

- Basic idea - if \( a = qb + c \) then \( (a,b) = (b,c) \)
  - Let \( s = (a,b) \) and \( t = (b,c) \)
  - \( s|a, s|b, t|b, t|c \)
  - \( c = a – qb = s(a_1 - qb_1) \) or \( s|c \)
    - As \( s|b \) and \( s|c \) and \( t \) is the largest integer that divides both \( b \) and \( c \), \( s \leq t \)
  - \( a = qb+c = t(qb_2 +c_2) \) or \( t|a \)
    - As \( t|b \) and \( t|a \) and \( s \) is the largest integer that divides both \( a \) and \( b \),
      \[ t \leq s \]
      \[ t = s \] or \((a, b) = (b, c)\) if \( a = qb + c \)
Euclidean Algorithm

\[
(a_0, a_1), \ a_0 > a_1
\]

\[
a_0 = q_1 a_1 + a_2 \Rightarrow (a_0, a_1) = (a_1, a_2)
\]

\[
a_1 = q_2 a_2 + a_3 \Rightarrow (a_1, a_2) = (a_2, a_3)
\]

\[\vdots\]

\[
a_{i-1} = q_i a_i + a_{i+1} \Rightarrow (a_{i-1}, a_i) = (a_i, a_{i+1})
\]

\[\vdots\]

\[
a_{r-2} = q_{r-1} a_{r-1} + a_r
\]

\[
a_{r-1} = q_r a_r + 0 \Rightarrow (a_{r-1}, a_r) = a_r = (a_{r-2}, a_{r-1}) = \cdots = (a_0, a_1)
\]
Euclidean Algorithm

- (457, 283)
Euclidean Algorithm

- \((457, 283)\)
- \(457 = 1 \times 283 + 174\)
Euclidean Algorithm

- \((457, 283)\)
- \(457 = 1 \times 283 + 174\)
- \(283 = 1 \times 174 + 109\)
- \(174 = 1 \times 109 + 65\)
- \(109 = 1 \times 65 + 44\)
- \(65 = 1 \times 44 + 21\)
- \(44 = 2 \times 21 + 2\)
- \(21 = 10 \times 2 + 1\)
Euclidean Algorithm

- $(457, 283)$
- $457 = 1 \cdot 283 + 174$
- $283 = 1 \cdot 174 + 109$
- $174 = 1 \cdot 109 + 65$
- $109 = 1 \cdot 65 + 44$
- $65 = 1 \cdot 44 + 21$
- $44 = 2 \cdot 21 + 2$
- $21 = 10 \cdot 2 + 1$
- $2 = 2 \cdot 1 + 0$  or $(457, 283) = (2, 1) = 1$
Euclidean Algorithm

- \((457, 283)\)
- \(457 = 1 \times 283 + 174\)
- \(283 = 1 \times 174 + 109\)
- \(174 = 1 \times 109 + 65\)
- \(109 = 1 \times 65 + 44\)
- \(65 = 1 \times 44 + 21\)
- \(44 = 2 \times 21 + 2\)
- \(21 = 10 \times 2 + 1\) \quad \text{or} \quad 1 = 21 - 10 \times 2\)
- \(2 = 2 \times 1 + 0\) \quad \text{or} \quad (457, 283) = (2, 1) = 1
Euclidean Algorithm

- \((457, 283)\)
- \(457 = 1 \times 283 + 174\)
- \(283 = 1 \times 174 + 109\)
- \(174 = 1 \times 109 + 65\)
- \(109 = 1 \times 65 + 44\)
- \(65 = 1 \times 44 + 21\)
- \(44 = 2 \times 21 + 2\)
- \(21 = 10 \times 2 + 1\)
- \(2 = 2 \times 1 + 0\)  \(\text{or } (457, 283) = (2, 1) = 1\)
Euclidean Algorithm (Extended)

- \((457, 283)\)
- \(457 = 1 \times 283 + 174\) \(1 = 135 \times 457 + (-218) \times 283\)
- \(283 = 1 \times 174 + 109\)
- \(174 = 1 \times 109 + 65\)
- \(109 = 1 \times 65 + 44\)
- \(65 = 1 \times 44 + 21\)
- \(44 = 2 \times 21 + 2\) \(1 = 21 - 10 \times (44 - 2 \times 21)\)
- \(21 = 10 \times 2 + 1\) \(1 = 21 - 10 \times 2\)
- \(2 = 2 \times 1 + 0\) or \((457, 283) = (2, 1) = 1\)
Bezout's Representation

- $s = (a, b) = ia + jb$
- $s$ is the *smallest strictly positive integer* that can be written *as a combination of* $a$ and $b$
- If coins are minted in only two denominations $a$ and $b$ can we accomplish *any* transaction?
- How can you mark 1 foot with two scales – one 9 feet long and the other 7 feet long?
Modular Inverse

Does inverse of \( a \mod m \) exist?

\[ a a^{-1} \equiv 1 \mod m \]

Let \( b = a^{-1} \)

\[ a b \equiv 1 \mod m \Rightarrow a b = 1 + k m \Rightarrow 1 = (-b) a + k m \]

\( (a, m) = 1 \)

Inverse exists only if \((a, m) = 1\)

If \((a, m) = 1\) then \(a\) is “relatively prime” to \(m\)

No wonder we couldn't find inverses for 2, 3 and 4 in \( \mod 6 \)

Note that \((5, 6) = 1\) (so 5 has an inverse in \( \mod 6 \))
Euclidean Algorithm (Extended)

- \((457, 283)\)
- \(457 = 1 \times 283 + 174\) \quad 1 = 135 \times 457 + (-218) \times 283
- \(283 = 1 \times 174 + 109\)
- \(174 = 1 \times 109 + 65\)
- \(109 = 1 \times 65 + 44\)
- \(65 = 1 \times 44 + 21\)
- \(44 = 2 \times 21 + 2\) \quad 1 = 21 - 10 \times (44 - 2 \times 21)
- \(21 = 10 \times 2 + 1\) \quad 1 = 21 - 10 \times 2
- \(2 = 2 \times 1 + 0\) \quad \text{or} \ (457, 283) = (2, 1) = 1
Euclidean Algorithm (Extended)

- $(457, 283)$
- $457 = 1*283 + 174 \quad 1 = 135*457 + (-218)*283$
- $283 = 1*174 + 109 \quad (-218*283) = 1 + (-135)*457$
- $174 = 1*109 + 65 \quad (-218*283) \equiv 1 \mod 457$
- $109 = 1*65 + 44 \quad -218 \equiv 239 \mod 457$
- $65 = 1*44 + 21 \quad (239*283) \equiv 1 \mod 457$
- $44 = 2*21 + 2$
- $21 = 10*2 + 1 \quad 1 = 21 - 10*2$
- $2 = 2*1 + 0 \quad \text{or } (457, 283) = (2, 1) = 1$
Euclidean Algorithm (Extended)

- \((457, 283)\)
- \(457 = 1 \cdot 283 + 174\) \hspace{1cm} 1 = 135 \cdot 457 + (-218) \cdot 283
- \(283 = 1 \cdot 174 + 109\) \hspace{1cm} (-218 \cdot 283) = 1 + (-135) \cdot 457
- \(174 = 1 \cdot 109 + 65\) \hspace{1cm} (-218 \cdot 283) \equiv 1 \mod 457
- \(109 = 1 \cdot 65 + 44\) \hspace{1cm} -218 \equiv 239 \mod 457
- \(65 = 1 \cdot 44 + 21\) \hspace{1cm} (239 \cdot 283) \equiv 1 \mod 457
- **239 is the inverse of 283 (mod 457)**
- \(239 \cdot 283 = 67637 = 1 + 148 \cdot 457\)
Prime Modulus

- What if $m$ is prime?
- We have $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$
- Every number is relatively prime to a prime number!
- So every number $1 \ldots m - 1$ has an inverse!
- $\mathbb{Z}_m$ forms a FIELD
- Normally referred to as prime field $\mathbb{Z}_p$
Why prime modulus?

- It is a field
  - Almost all mathematical operations are supported.
  - Crunch away!
- Cannot decipher “patterns”
  - Deterministic mathematical functions – yet the results seem random!
  - Good for cryptography!
How about Exponentiation?

- Just repeated multiplication!
- Lets choose a large prime $p$ and a generator $g$ – both are public
- Choose some number $a$, and calculate
  - $A \equiv g^a \mod p$
  - There is a simple algorithm for exponentiation involving repeated squaring - complexity $O(\log(a))$
  - No algorithm for determining $a$ from $A$! (complexity $O(p)$!)  
  - Why is this feature useful?
Diffie-Helman Key Exchange!
(Sneak Peak)

- Alice and Bob agree on a large prime $p$ and a generator $g$
- Alice chooses a secret $a$, and calculates
  $A \equiv g^a \mod p$ – $A$ is Alice's public key
- Bob chooses a secret $b$, and calculates
  $B \equiv g^b \mod p$ – $B$ is Bob's public key
- Alice and Bob exchange $A$ and $B$ in public
  - Alice calculates $S \equiv B^a \mod p \equiv g^{ba} \mod p$
  - Bob calculates $S \equiv A^b \mod p \equiv g^{ab} \mod p$
- Nobody else can calculate $S$
  - even if they know $A,B,g$ and $p$!
  - only $g^{a+b} \mod p$ (or $g^{a-b}$)– not very useful!
RECAP

- $Z_m = \{0,1,2,...,m-1\}$
  - $Z_m$ is a ring – addition, multiplication...
  - Multiplicative inverse of $a$ in $Z_m$ exists only if
    - $(a,m)=1$
    - GCD – Euclidean algo
    - Multiplicative Inverse – Extended Euclidean Algorithm

- If $m = p$ (a prime) then $Z_p$ is a field
  - Supports all regular operations – addition, subtraction, multiplication and multiplicative inverses
  - All elements of the field (except additive identity) has a multiplicative inverse.