Algorithmic Number Theory and Cryptography
(CS 303)

Modular Arithmetic

Jeremy R. Johnson
Introduction

• Objective: To become familiar with modular arithmetic and some key algorithmic constructions that are important for computer algebra algorithms.
  - Modular Arithmetic
  - Modular inverses and the extended Euclidean algorithm
  - Fermat’s theorem
  - Euler’s Identity
  - Chinese Remainder Theorem

References: Rivest, Shamir, Adelman.
**Modular Arithmetic (\(Z_n\))**

Definition: \(a \equiv b \pmod{n} \iff n \mid (b - a)\)

Alternatively, \(a = qn + b\)

**Properties (equivalence relation)**

- \(a \equiv a \pmod{n}\) \ [Reflexive]
- \(a \equiv b \pmod{n} \implies b \equiv a \pmod{n}\) \ [Symmetric]
- \(a \equiv b \pmod{n} \text{ and } b \equiv c \pmod{n} \implies a \equiv c \pmod{n}\) \ [Transitive]

Definition: An equivalence class mod n

\[
[a] = \{ x : x \equiv a \pmod{n}\} = \{ a + qn \mid q \in \mathbb{Z}\}
\]
Modular Arithmetic \((\mathbb{Z}_n)\)

It is possible to perform arithmetic with equivalence classes mod \(n\).

- \([a] + [b] = [a+b]\)
- \([a] * [b] = [a*b]\)

In order for this to make sense, you must get the same answer (equivalence) class independent of the choice of \(a\) and \(b\). In other words, if you replace \(a\) and \(b\) by numbers equivalent to \(a\) or \(b\) mod \(n\) you end up with the sum/product being in the same equivalence class.

\[
\begin{align*}
a_1 &\equiv a_2 \pmod{n} \quad \text{and} \quad b_1 &\equiv b_2 \pmod{n} \quad \Rightarrow \quad a_1 + b_1 &\equiv a_2 + b_2 \pmod{n} \\
a_1 \cdot b_1 &\equiv a_2 \cdot b_2 \pmod{n}
\end{align*}
\]

\[
\begin{align*}
(a + q_1n) + (b + q_2n) &= a + b + (q_1 + q_2)n \\
(a + q_1n) \cdot (b + q_2n) &= a \cdot b + (b*q_1 + a*q_2 + q_1 \cdot q_2)n
\end{align*}
\]
Representation of $\mathbb{Z}_n$

The equivalence classes $[a] \mod n$, are typically represented by the representatives $a$.

- **Positive Representation:** Choose the smallest positive integer in the class $[a]$ then the representation is $\{0, 1, \ldots, n-1\}$.

- **Symmetric Representation:** Choose the integer with the smallest absolute value in the class $[a]$. The representation is $\{-\lfloor (n-1)/2 \rfloor, \ldots, \lfloor n/2 \rfloor \}$. When $n$ is even, choose the positive representative with absolute value $n/2$.

- **E.G.** $\mathbb{Z}_6 = \{-2, -1, 0, 1, 2, 3\}$, $\mathbb{Z}_5 = \{-2, -1, 0, 1, 2\}$
Modular Inverses

Definition:  x is the inverse of a mod n, if \( ax \equiv 1 \pmod{n} \)

The equation \( ax \equiv 1 \pmod{n} \) has a solution iff \( \gcd(a,n) = 1 \).

By the Extended Euclidean Algorithm, there exist x and y such that \( ax + ny = \gcd(a,n) \). When \( \gcd(a,n) = 1 \), we get \( ax + ny = 1 \). Taking this equation mod n, we see that \( ax \equiv 1 \pmod{n} \)

By taking the equation mod n, we mean applying the mod n homomorphism: \( \phi_m \mathbb{Z} \to \mathbb{Z}_m \), which maps the integer a to the equivalence class \([a]\). This mapping preserves sums and products. I.E.

\[
\phi_m(a+b) = \phi_m(a) + \phi_m(b), \quad \phi_m(a*b) = \phi_m(a) * \phi_m(b)
\]
Fermat’s Theorem

Theorem: If \( a \neq 0 \in \mathbb{Z}_p \), then \( a^{p-1} \equiv 1 \pmod{p} \). More generally, if \( a \in \mathbb{Z}_p \), then \( a^p \equiv a \pmod{p} \).

Proof: Assume that \( a \neq 0 \in \mathbb{Z}_p \). Then
\[
a \cdot 2a \cdot \ldots \cdot (p-1)a = (p-1)! \cdot a^{p-1}
\]
Also, since \( a^i \equiv a^j \pmod{p} \implies i \equiv j \pmod{p} \), the numbers \( a, 2a, \ldots, (p-1)a \) are distinct elements of \( \mathbb{Z}_p \). Therefore they are equal to \( 1, 2, \ldots, (p-1) \) and their product is equal to \( (p-1)! \pmod{p} \). This implies that
\[
(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod{p} \implies a^{p-1} \equiv 1 \pmod{p}.
\]
Euler phi function

• Definition: \( \phi(n) = \# \{ a: 0 < a < n \text{ and } \gcd(a,n) = 1 \} \)

• Properties:
  – \( \phi(p) = p-1 \), for prime \( p \).
  – \( \phi(p^e) = (p-1)p^{e-1} \)
  – \( \phi(mn) = \phi(m)\phi(n) \) for \( \gcd(m,n) = 1 \).
  – \( \phi(pq) = (p-1)(q-1) \)

• Examples:
  
  – \( \phi(15) = \phi(3)\phi(5) = 2\times4 = 8 \) = \( \# \{1,2,4,7,8,11,13,14\} \)
  – \( \phi(9) = (3-1)3^{(2-1)} = 2\times3 = 6 \) = \( \# \{1,2,4,5,7,8\} \)
Euler’s Identity

1. The number of elements in $\mathbb{Z}_n$ that have multiplicative inverses is equal to $\phi(n)$.

2. Theorem: Let $(\mathbb{Z}_n)^*$ be the elements of $\mathbb{Z}_n$ with inverses (called units). If $a \in (\mathbb{Z}_n)^*$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. The same proof presented for Fermat’s theorem can be used to prove this theorem.
Chinese Remainder Theorem

Theorem: If gcd(m,n) = 1, then given a and b there exist an integer solution to the system:
\[ x \equiv a \pmod{m} \text{ and } x = b \pmod{n}. \]

Proof:
Consider the map \( x \mapsto (x \mod m, x \mod n) \).
This map is a 1-1 map from \( \mathbb{Z}_{mn} \) to \( \mathbb{Z}_m \times \mathbb{Z}_n \), since if \( x \) and \( y \) map to the same pair, then \( x \equiv y \pmod{m} \) and \( x \equiv y \pmod{n} \).
Since gcd(m,n) = 1, this implies that \( x \equiv y \pmod{mn} \).
Since there are \( mn \) elements in both \( \mathbb{Z}_{mn} \) and \( \mathbb{Z}_m \times \mathbb{Z}_n \), the map is also onto. This means that for every pair \((a,b)\) we can find the desired \( x \).
Alternative Interpretation of CRT

• Let $Z_m \times Z_n$ denote the set of pairs $(a,b)$ where $a \in Z_m$ and $b \in Z_n$. We can perform arithmetic on $Z_m \times Z_n$ by performing componentwise modular arithmetic.

  - $(a,b) + (c,d) = (a+b, c+d)$
  - $(a,b) \cdot (c,d) = (a\cdot c, b\cdot d)$

• Theorem: $Z_{mn} \approx Z_m \times Z_n$. I.E. There is a 1-1 mapping from $Z_{mn}$ onto $Z_m \times Z_n$ that preserves arithmetic.

  - $(a\cdot c \mod m, b\cdot d \mod n) = (a \mod m, b \mod n) \cdot (c \mod m, d \mod n)$
  - $(a+c \mod m, b+d \mod n) = (a \mod m, b \mod n) + (c \mod m, d \mod n)$
  - The CRT implies that the map is onto. I.E. for every pair $(a,b)$ there is an integer $x$ such that $(x \mod m, x \mod n) = (a,b)$. 
Constructive Chinese Remainder Theorem

Theorem: If \( \gcd(m,n) = 1 \), then there exist \( e_m \) and \( e_n \) (orthogonal idempotents)
- \( e_m \equiv 1 \pmod{m} \)
- \( e_m \equiv 0 \pmod{n} \)
- \( e_n \equiv 0 \pmod{m} \)
- \( e_n \equiv 1 \pmod{n} \)

It follows that \( a*e_m + b*e_n \equiv a \pmod{m} \) and \( \equiv b \pmod{n} \).  

Proof.

Since \( \gcd(m,n) = 1 \), by the Extended Euclidean Algorithm, there exist \( x \) and \( y \) with \( m*x + n*y = 1 \). Set \( e_m = n*y \) and \( e_n = m*x \)