Cryptography
Introduction to Number Theory

Preview
• Integers
• Prime Numbers
• Modular Arithmetic
• Totient Function
• Euler's Theorem
• Fermat's Little Theorem
• Euclid's Algorithm

Introduction to Number Theory
• Integers
• Arithmetic
• Prime numbers
• Factoring
• GCD
• Modular arithmetic
Number Theory Essentials

- Prime Numbers
  - $a \in \mathbb{I}$ is prime iff
    - It's only factors are itself and 1
    - Equivalently, $\forall x \in \mathbb{I}, \gcd(x,a) = 1$
  - $a, b \in \mathbb{I}$ are relatively prime iff:
    - $\gcd(a,b) = 1$
- Fundamental theorem of arithmetic:
  - Every integer has a unique factorization that is a product of prime powers

Modular Arithmetic Systems

- Form: $(a \equiv b) \mod n$
- The Modulo partitions the integers into congruence classes
- The congruence class of an integer 'a' is the set of all integers congruent to 'a' modulo 'n'.
- $a \equiv b \mod n$ asserts that 'a' and 'b' are members of the same congruence class in modulo 'n'

Congruence Classes

- $(1 \equiv 6 \equiv 11) \mod 5$
- $\ldots \ldots 14 \ 9 \ 4 \ 1 \ 6 \ 11 \ \ldots \ldots$
- $\ldots \ldots 3 \ 2 \ 7 \ 12 \ \ldots \ldots$
Notation for Modular Arithmetic

- Form: \( a \equiv b \mod n \) congruent
  \( a = b \mod n \) equal

\( \equiv \) indicates that the integers \( a \) and \( b \) fall into the same congruence class modulo \( n \)

\( = \) means that integer \( a \) is the reminder of the division of integer \( b \) by integer \( n \), thus, \( a \) is the smallest (least) member of the congruence class.

The Integers Modulo \( n \)

- \( \forall a,b,n \in \mathbb{I}, a \equiv b \mod n \) iff \( n \cdot | (a-b) \)
  - \( 28 \equiv 6 \mod 11: (28-6)/11 = 2 \in \mathbb{I} \)
  - \( 219 \equiv 49 \mod 17: (219-49)/17 = 12 \in \mathbb{I} \)
  - If \( a \equiv b \mod n \) then \( b \equiv a \mod n \)
  - Transitivity holds

* \( N \) divides \( (a-b) \)

A Few Properties of Modular Arithmetic

- \( (a + b) \mod n = ((a \mod n) + (b \mod n)) \mod n \)
- \( ((a \mod n) + (b \mod n)) \mod n = ((b \mod n) + (a \mod n)) \mod n \)
- \( (a \times b) \mod n = ((a \mod n) \times (b \mod n)) \mod n \)
- \( (a \times (b + c)) \mod n = (((a \times b) \mod n) + ((a \times c) \mod n)) \mod n \)
- \( (a^{b^c}) \mod n = (a^{b \mod n})^{c \mod n} \mod n \)
- If \( a \equiv b \mod n \) then \( b \equiv a \mod n \)
  *
Prime Numbers and Modular Arithmetic
- Modular computations can be utilized to scramble data
- Cryptographic systems utilize large prime numbers to create the modulus

Fermat's Little Theorem
If for $p$, $a \in \mathbb{N}$, where $p$ is prime and $1 < a < p$
\[ a^p = a \pmod{p} \]
Equivalently, if $p$ is prime and $1 < a < p$
\[ a^{p-1} = 1 \pmod{p} \]

Fermat's Little Theorem
Proof by Example
\[ a^{p-1} = 1 \pmod{p} \]
- Let $p = 11$, pick a's
  - 3: $3^{10} = 59049 \pmod{11} = 1$
  - 5: $5^{10} = 9765625 \pmod{11} = 1$
  - 7: $7^{10} = 282475249 \pmod{11} = 1$
  - 8: $8^{10} = 1073741824 \pmod{11} = 1$
Using FLT to Compute Large Modular Computations

- Compute: $3^{12} \mod 11$
  
  $(3^{10} \times 3^2) \mod 11$
  
  $(3^{10}) \mod 11 \times (3^2) \mod 11$
  
  $= 1 \times (3^2) \mod 11$
  
  $= 9$

Compute: $249^{122} \mod 31$

- Compute: $249^{122} \mod 31$
  
  $(249^{120} \times 249^2) \mod 31$
  
  $(249^{120}) \mod 31 \times (249^2) \mod 31$
  
  $= 1 \times (249^2) \mod 31$
  
  $= 62001$

Prime Number Challenges

1. Finding large prime numbers
2. Recognizing large numbers as prime
How Do We Get BIG Prime Numbers?

- Buy them
- Look them up
- Compute them

Finding Big Primes

- The probability of a randomly chosen number being prime is $1/\ln n$
- For a 100 digit number, the chance is about $1/230$
- Guess and check, should take 230 tries on the average
- How do we check? Primality testing.

Primality Testing:

- FLT says that:
  - "If $p$ is prime, then $a^{p-1} \mod p = 1$
- If we don't know whether or not $n$ is prime, what does the fact that $(a^{n-1} \mod n = 1)$ say about $N$?
A Number P is Probably Prime if: \( a^{p-1} = 1 \mod p \)

1. Select \( p \), a large number
2. Select \( a < p \)
3. Compute \( x = a^{p-1} \mod p \)
   a. If \( x \neq 1 \), \( p \) is not prime
   b. If it is one, \( p \) is probably prime

If \( a^{p-1} = 1 \mod p \), the chance that \( p \) is not prime is \( 1/10^{13} \)

Large Exponents
- \( 381^{1502} \)
- Thank goodness:
  - That our computations are \( \mod n \)
  - When \( n \) is prime
  - For FLT
- \( 381^{1502} \mod 751 = 218 \)
Large Exponents & FLT

- $381^{1502}$ mod 751
  - $= 381^2 \times 381^{750} \times 381^{750}$
  - $= 381^2$ mod 751 $\times$ 1 mod 751
  - $= 145161$ mod 751
  - $= 218$

Exponentiation with FLT

- $a^{p-1} \equiv 1 \mod p$
- $7^{13} \equiv x \mod 11$
- $7^{10} \mod 11 \times 7^3 \mod 11 \equiv x \mod 11$
- $1 \mod 11 \times 7^3 \mod 11 \equiv x \mod 11$
- $7^3 \mod 11 \equiv x \mod 11$
- $343 \mod 11 \equiv 2 \mod 11$

$\mathbb{Z}_n^*$

- $\mathbb{Z} = $ set of all integers
- $\mathbb{Z}_n = $ set of all integers mod $n$
- $\mathbb{Z}_n^* = $ set of integers in $\mathbb{Z}_n$ (less than $n$) that are relatively prime to $n$ ($\gcd(m,n) = 1$)
- $\mathbb{Z}_n^* = $ closed under multiplication
\( \phi(n) \)

- \( \phi(n) \) is the # of #s less than \( n \) that are relatively prime to \( n \)
- The function \( \phi(n) \) returns the cardinality of \( \mathbb{Z}_n^* \)
- \( \forall \ p \in \text{Primes}, \ \phi(p) = p - 1 \)

Deriving \( \phi(n) \)

- For Primes:
  - Product of 2 relatively prime #s
  - Product of \( n \) relatively prime #s
  - Generally (i.e. for all integers \( x \))

Deriving \( \phi(n) \)

- Primes:
  - \( \forall \ p \in \text{Primes}, \ \phi(p) = p - 1 \).
- Product of 2 relatively prime #s
  - if \( \gcd(m,n) = 1 \), then
    - \( \phi(mn) = \phi(m) \ast \phi(n) \)
  - 15 = 3*5 and
  - \( \phi(15) = 2*4 = 8 \), \{1,2,4,7,8,11,13,14\}
**Deriving \( \phi(n) \)**

- Product of \( n \) relatively prime numbers
  - if gcd \( (a_1,a_2, \ldots a_n) = 1 \), then
  \[
  \phi(a_1a_2\ldots a_n)=\phi(a_1)*\phi(a_2)*\ldots\phi(a_n)
  \]
- \( 30 = 2*3*5 \) and
- \( \phi(30)=1*2*4=8 \)
  \[ Z_{30}^* = \{1,7,11,13,17,19,23,29\} \]

---

**Tuesday**

Modulo multiplication as an asymmetric key cipher

---

Modulo Multiplication as a Public Key Cipher

- a and b are inverses mod \( n \) iff:
  - \( a \times b \mod n = 1 \)
- Only numbers that are relatively prime to \( n \) have multiplicative inverses mod \( n \)
- Inverses mod \( n \) can be found using Euclid's algorithm.
- Can we use multiplicative inverses modulo \( n \) as public and private keys?
Modulo Multiplication as a Public Key Cipher

- $e, d$ are multiplicative inverses mod $n$ iff:
  - $ed \mod n = 1$
- If $e$ and $d$ are inverses then:
  - $m \times e \times d \mod n \equiv m \mod n$
- For example:
  - Select $e = 5$, $d = 6$, $n = 29$, so $ed = 1 \mod 29$
  - Encrypt 17: $17 \times 5 \mod 29 = 85 \mod 29 = 27$
  - Decrypt 27: $27 \times 6 \mod 29 = 162 \mod 29 = 17$

Exponentiation mod $n$ As Public/Private Key Scramble

- Find $e$ & $d$ such that $m^{ed} \equiv m \mod n$
  - That is, find $e$'s exponentive inverse
- $D[E[m,e], d] \equiv (m^e \mod n)^d \mod n \equiv m$
- Encryption: $E(m,e) \equiv m^e \mod n$
- Decryption: $D(c,d) \equiv c^d \mod n$
  - $\equiv (m^e \mod n)^d \mod n$
  - $\equiv m^{ed} \mod n$
  - $\equiv m \mod n$

RSA

- Rivest, Shamir, Adleman, 1978, MIT
- Variable key size, common to use 1024
- Generating RSA keys is based on finding multiplicative inverses of large numbers (modulo), which is not hard
- Generating RSA ciphertext is based on modulo exponentiation, which is not hard
- RSA's strength is based on difficulty of factoring large numbers, WHICH IS HARD
- There may be other trap doors in RSA, but none have been found yet.
The Foundation of RSA

- \( x^y \mod n = x \mod (y \mod \Phi(n)) \mod n \)
- If \( y \mod \Phi(n) = 1 \),
  - then for any \( x \), \( x^y \mod n = x \mod n \)
- If we can choose \( e \) and \( d \) such that
  - \( ed = y \mod \Phi(n) \)
- then we can encrypt by raising \( x \) to the \( e \)th power and decrypt by raising to the \( d \)th power.

RSA Example

1. Select two large primes, 2357 and 2551.
2. Multiply them to get \( n = 6012707 \)
3. Select \( e = 3674911 \), relatively prime to \( \Phi(n) = 600780 \)
4. \( d = 422191 \) is the multiplicative inverse of \( e \mod \Phi(n) \)
5. Encrypt \( m \) as, \( c = m^e \mod n \).
6. Decrypt \( c \) as, \( m = c^d \mod n \).

Why does finding \( d \) as the multiplicative inverse of \( e \mod \Phi(n) \), make \( d \) the exponent inverse of \( e \mod n \)?

The RSA Algorithm

1. Select two large primes, \( p, q \). Multiply them to get \( n \).
2. As your public key, select \( e \) relatively prime to \( \Phi(n) \).
3. As your private key, find \( d \) that is the multiplicative inverse of \( e \mod \Phi(n) \).
4. Encrypt \( m < n \) as, \( c = m^e \mod n \).
5. Decrypt \( c \) as, \( m = c^d \mod n \).

Why does finding \( d \) as the multiplicative inverse of \( e \mod \Phi(n) \), make \( d \) the exponent inverse of \( e \mod n \)?

*Multiplicative inverses can be found using Euclid's algorithm.*
Euler's Theorem
Test to see if two numbers are relatively prime

if \( \gcd(a,n) = 1, \ a^{\Phi(n)} \mod n = 1 \)

1. \((3,11)\): \(3^{10} \mod 11 = 59049 \mod 11 = 1\)
2. \((4,9)\): \(4^8 \mod 9 = 4096 \mod 9 = 1\)
3. \((5,18)\): \(5^8 \mod 18 = 15625 \mod 18 = 1\)
4. \((4,6)\): \(4^2 \mod 6 = 16 \mod 6 = 4\)

Finding a Multiplicative Inverse mod n
• Find \(y\) such that:
  – \(xy = 1 \mod n\)
• Why?
  – It is needed in RSA
• How?
  – Euclid's Algorithm

Integer Properties/Rules
• Denote the set of integers as \(I\)
• Division: For \(a,b,c \in I, a|b\) iff \(\exists c \ni b = a \cdot c\)
  • \(a|a\)
  • If \(a|b\) and \(b|c\), then \(a|c\)
  • If \(a|b\) and \(a|c\), then \(a|(bx+cy) \forall x, y \in I\)
  • If \(a|b\) and \(b|a\), then \(a = \pm b\)
  • \(c = \gcd(a,b)\) if \(c\) is the largest integer that divides both \(a\) and \(b\)
• Remainders: \(\forall a, b \in I, \exists q, r \in I: a = qb + r\) where \(r\) is the remainder of \(a/b\)
  • \(r = a \mod b\)
Finding a GCD

• If \((x \text{ divides } a)\) and \((x \text{ divides } b)\), then
  \(- x \text{ divides } a - b\)

• For example
  - \(x = 10, a = 90, b = 40\): 10 divides 50
  - \(x = 5, a = 35, b = 25\): 5 divides 10
  - \(x = 19, a = 95, b = 57\): 19 divides 38

Finding a GCD

For \(a > b\), \(\text{gcd}(a,b) = \text{gcd}\left(b, a \mod b\right)\)

\[\text{gcd}(95, 57) = \text{gcd}\left(57, 95 \mod 57\right)\]
\[= \text{gcd}(57, 38) = \text{gcd}\left(38, 57 \mod 38\right)\]
\[= \text{gcd}(38, 19) = \text{gcd}\left(19, 38 \mod 19\right)\]
\[= \text{gcd}(19, 0)\]
\[= \text{gcd}(95, 57) = 19\]

Relative Primality Test

• For \(a > b\), \(\text{gcd}(a,b) = \text{gcd}\left(b, a \mod b\right)\)

\[\text{gcd}(196, 87) = \text{gcd}\left(87, 196 \mod 87\right)\]
\[= \text{gcd}(87, 22) = \text{gcd}\left(22, 87 \mod 22\right)\]
\[= \text{gcd}(22, 21) = \text{gcd}\left(21, 22 \mod 21\right)\]
\[= \text{gcd}(21, 1)\]
\[= 196 \text{ and } 87 \text{ are relatively prime.}\]
Multiplicative Inverse mod n

- m must be relatively prime to n
- m is in \( Z_n \) iff there exists u, v such that:
  \[ um + vn = 1 \mod n \]
  
  \[ u7 + v17 = 1 \mod 17 \]
  
  by inspection, \( u = 5, v = -2 \)

Euclid's Algorithm

- Find the multiplicative inverse \( u \) of m mod n, where
  - \( u \) and m are relatively prime
    - i.e. find \( um = 1 \mod n \)
    - equivalently, \( um \) differs from a multiple of n by 1,
    - equivalently, there exists a \( v \) such that \( um + vn = 1 \)
    - \( \gcd(14,9) = 1, u = 2, v = -3: (2*14) + (-3*9) = 1 \)
    - \( \gcd(21,8) = 1, u = -3, v = 8: (-3*21) + (8*8) = 1 \)
    - computing \( \gcd(m,n) \) finds \( u \) and \( v \) provided \( \gcd(m,n) = 1 \)
    - Any \( x \) that divides m and n, also divides \( m - kn \) for \( kn < m \)
    - Repetitively replace \( <m,n> \) with \( <n,m \mod n> \)
    - When \( m \mod n = 0 \), n is the \( \gcd(M,N) \)

Facts for Finding a Multiplicative Inverse mod n

#1: \( \forall \ x,y \in I, \exists u,v \mid \gcd(x,y) = ux + vy \)

#2: \( \gcd(x,y) \mod n = (ux+vy) \mod n \)

#3: If \( x,y \) are relatively prime mod n, then \( \gcd(x,y) = 1 \mod n \)

#4: If \( x,y \) are relatively prime mod n, then \( \exists u,v \mid ux + vy = 1 \mod n \)
Multiplicative Inverse mod n

\[ \gcd(m, n) = um + vn \text{ for all } m \text{ and } n \]
- \( \gcd(35, 50) \)
  by inspection:
  \[ 35u + 50v = 35(3) + 50(-2) = 105 - 100 = 5 \]
- \( \gcd(42, 56) \)
  \[ um & vn \text{ differ by } 14 \text{ at a multiple of } 56 \]
  \[ -56, 112 \quad u=3, \ v=-2 \]
  \[ -42, 126 \]

Using Euclid to Find Inverses Mod N

find \( 7^{\cdot} \mod 51 \), or find \( ux + vy = 1 \) or \( ux = 1 - vy \) where \( x = 7 \) and \( y = 51 \)

Opportunities for \( 7u = 1 \mod 51 \) or \( 7u = 1 - 51v \), occur at \([v]\) (multiples of 51) + 1 (52, 103, 154, 205, etc.)

So we look for one of these that 7 divides evenly and recognize 154.
\( (7\cdot 22) + (-3 \cdot 51) = 1 \mod 51 \) or \( (7\cdot 22) = 1 - (-3 \cdot 51) - 1 + (3\cdot 51) \)
Thus \( 7 \cdot 22 = 154 = 1 \mod 51 \) and that \( 7^{-1} = 22 \mod 51 \)

\[ u = 8 \]
\[ v = -1 \]
\[ u = 15 \]
\[ v = -2 \]
\[ u = 22 \]

\[ u = 3 \]

Paydirt

<table>
<thead>
<tr>
<th>( n )</th>
<th>( q_n )</th>
<th>( r_n )</th>
<th>( u_n )</th>
<th>( v_n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>-2</td>
<td></td>
<td>323</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>-1</td>
<td>( u_n = u_{n-2} - (q_{n-1} \cdot u_{n-1}) )</td>
<td>18209</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>( v_n = v_{n-2} - (q_{n-1} \cdot v_{n-1}) )</td>
<td>323</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>56</td>
<td>121</td>
<td>-56</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>81</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1-(2\cdot -56)</td>
<td>113-2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
\[
\begin{align*}
\begin{array}{cccc}
n & q_n & r_n & u_n \\
-2 & 323 & 1 & 0 \\
-1 & u_n &=& u_{n-2} - (q_n \times u_{n-1}) \\
0 & v_n &=& v_{n-2} - (q_n \times v_{n-1}) \\
1 & 56 & 121 & -56 \\
2 & 2 & 81 & 113 \\
3 & 1 & 40 & 169 \\
4 & & & \\
\end{array}
\end{align*}
\]

\[
\text{Compute the inverse of } 17 \text{ mod 71}
\]

\[
\begin{array}{cccc}
n & q_n & r_n & u_n \\
-2 & 17 & 1 & 0 \\
-1 & 71 & 0 & 1 \\
0 & 17 & 1 & 0 \\
1 & 4 & 3 & -4 \\
2 & & & \\
3 & & & \\
4 & & & \\
5 & & & \\
\end{array}
\]

Recall that
\[
u_n = u_{n-2} - (q_n \times u_{n-1})
\]
and
\[
v_n = v_{n-2} - (q_n \times v_{n-1})
\]
Compute the inverse of $17 \mod 71$

<table>
<thead>
<tr>
<th>n</th>
<th>qn</th>
<th>r n</th>
<th>un</th>
<th>vn</th>
</tr>
</thead>
<tbody>
<tr>
<td>-2</td>
<td>17</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>-1</td>
<td>71</td>
<td>0</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>17</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>3</td>
<td>-4</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>2</td>
<td>21</td>
<td>-5</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td>-25</td>
<td>6</td>
</tr>
</tbody>
</table>

For $n = 1$: $(-4*17) + (1*71) = -68 + 71 = 3$ (which is $r_1$)
For $n = 2$: $(21*17) + (-5*71) = 357 + 355 = 2$ (which is $r_2$)
For $n = 3$: $(-25*17) + (6*71) = -425 + 426 = 1$ (which is $r_3$)

Recall that $u_n = u_{n-2} - (q_n * u_{n-1})$ and $v_n = v_{n-2} - (q_n * v_{n-1})$

Negative Inverses, Mod N

find $7^{-1} \mod 51$, or find $ux + vy = 1$ or $ux = 1 - vy$ where $x = 7$ and $y = 51$

We may also consider places where $vy = 1 - ux$

$(4 \times 51) = (1 - (7 \times -29))$

$204 = (1 - (-203)) = 204$

$v = 3$

$u = 15$

$u = -29$

$u = -15$

$u = -8$

$204$ 196 188 175 168 161 154 147 140 133 126 119 112 105 98 91 84 77 70 63 56 49 42 35 28 21 14 7 0

Negatives Modulo Numbers

- OK, so is -25 the answer?
- Yes but, $17^{-1} = -25 \mod 71$

$= (71 - 25) \mod 71$

$= 46 \mod 71$

which is a better answer
Questions?