Number Theory

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:
http://www.cse.wustl.edu/~jain/cse571-17/
Overview

1. Prime numbers
2. Fermat’s and Euler’s Theorems
3. Testing for primality
4. The Chinese Remainder Theorem
5. Discrete Logarithms

Fermat's Little Theorem

- Given a prime number \( p \):
  \[ a^{p-1} = 1 \pmod{p} \]
  For all integers \( a \neq p \)

- Or
  \[ a^p = a \pmod{p} \]

- Example:
  - \( 1^4 \mod 5 = 1 \)
  - \( 2^4 \mod 5 = 1 \)
  - \( 3^4 \mod 5 = 1 \)
  - \( 4^4 \mod 5 = 1 \)
Euler Totient Function \( \varphi(n) \)

- When doing arithmetic modulo \( n \) **complete set of residues** is: \( 0..n-1 \)

- **Reduced set of residues** is those residues which are relatively prime to \( n \), e.g., for \( n=10 \), complete set of residues is \( \{0,1,2,3,4,5,6,7,8,9\} \) reduced set of residues is \( \{1,3,7,9\} \)

- Number of elements in reduced set of residues is called the **Euler Totient Function** \( \varphi(n) \)

- In general need prime factorization, but
  - for \( p \) (\( p \) prime) \( \varphi(p) = p-1 \)
  - for \( p.q \) (\( p,q \) prime) \( \varphi(p.q) = (p-1) \times (q-1) \)

- Examples: \( \varphi(37) = 36 \)
  \[ \varphi(21) = (3-1) \times (7-1) = 2 \times 6 = 12 \]

Washington University in St. Louis  http://www.cse.wustl.edu/~jain/cse571-17/ ©2017 Raj Jain
Euler's Theorem

- A generalisation of Fermat's Theorem
- \( a^{\varphi(n)} = 1 \pmod{n} \)
  - for any \( a, n \) where gcd\((a,n)\)=1
- Example:
  - \( a=3; n=10; \varphi(10)=4; \)
    - hence \( 3^4 = 81 = 1 \pmod{10} \)
  - \( a=2; n=11; \varphi(11)=10; \)
    - hence \( 2^{10} = 1024 = 1 \pmod{11} \)
- Also have: \( a^{\varphi(n)+1} = a \pmod{n} \)
Miller Rabin Algorithm for Primality

- A test for large primes based on Fermat’s Theorem

- TEST \((n)\) is:
  1. Find integers \(k, q, k > 0, q\) odd, so that \((n-1) = 2^k q\)
  2. Select a random integer \(a\), \(1 < a < n-1\)
  3. if \(a^q \mod n = 1\) then return (“inconclusive”)
  4. for \(j = 0\) to \(k - 1\) do
  5. if \((a^{2^j q} \mod n = n-1)\) then return(“inconclusive"")
  6. return (“composite”)

- If inconclusive after \(t\) tests with different \(a\)’s:
  Probability \((n\) is Prime after \(t\) tests) = \(1 - 4^{-t}\)

- E.g., for \(t=10\) this probability is \(> 0.99999\)
Miller Rabin Algorithm Example

- Test 29 for primality
  - \(29-1 = 28 = 2^2 \times 7 = 2^k q \Rightarrow k=2, q=7\)
  - Let \(a = 10\)
    - \(10^7 \mod 29 = 17\)
    - \(10^{2 \times 7} \mod 29 = 17^2 \mod 29 = 28 \Rightarrow \text{Inconclusive}\)

- Test 221 for primality
  - \(221-1 = 220 = 2^2 \times 55\)
  - Let \(a = 5\)
    - \(5^{55} \mod 221 = 112\)
    - \(5^{2 \times 55} \mod 221 = 112^2 \mod 221 = 168 \Rightarrow \text{Composite}\)
Prime Distribution

- Prime numbers: 1 2 3 5 7 11 13 17 19 23 29 31
- Prime number theorem states that primes occur roughly every \((\ln n)\) integers
- But can immediately ignore even numbers
- So in practice need only test \(0.5 \ln(n)\) numbers of size \(n\) to locate a prime
  - Note this is only the “average”
  - Sometimes primes are close together
  - Other times are quite far apart
Chinese Remainder Theorem

- If working modulo a product of numbers
  - E.g., mod $M = m_1 m_2 \ldots m_k$
- Chinese Remainder theorem lets us work in each moduli $m_i$ separately
- Since computational cost is proportional to size, this is faster

$$A \mod M = \sum_{i=1}^{k} \left( A \mod m_i \right) \frac{M}{m_i} \left( \left[ \frac{M}{m_i} \right]^{-1} \mod m_i \right)$$

- Example: $452 \mod 105$
  
  $$= (452 \mod 3)(105/3)\{(105/3)^{-1} \mod 3\} + (452 \mod 5)(105/5)\{(105/5)^{-1} \mod 5\} + (452 \mod 7)(105/7)\{(105/7)^{-1} \mod 7\}$$
  $$= 2 \times 35 \times (35^{-1} \mod 3) + 2 \times 21 \times (21^{-1} \mod 5) + 4 \times 15 \times (15^{-1} \mod 7)$$
  $$= 2 \times 35 \times 2 + 2 \times 21 \times 1 + 4 \times 15 \times 1$$
  $$= (140 + 42 + 60) \mod 105 = 242 \mod 105 = 32$$

- $35^{-1} = x \mod 3$
  - $35x = 1 \mod 3 \Rightarrow x = 2$
- $21x = 1 \mod 5 \Rightarrow x = 1$
- $15x = 1 \mod 7 \Rightarrow x = 1$
Chinese Remainder Theorem

- Alternately, the solution to the following equations:
  \[ x = a_1 \mod m_1 \]
  \[ x = a_2 \mod m_2 \]
  \[ x = a_k \mod m_k \]
  where \( m_1, m_2, \ldots, m_k \) are relatively prime is found as follows:

  \[ M = m_1 \cdot m_2 \cdots m_k \]
  then

  \[ x = \sum_{i=1}^{k} a_i \frac{M}{m_i} \left( \left[ \frac{M}{m_i} \right]^{-1} \mod m_i \right) \]
For a parade, marchers are arranged in columns of seven, but one person is left out. In columns of eight, two people are left out. With columns of nine, three people are left out. How many marchers are there?

\[ x \equiv 1 \mod 7 \]
\[ x \equiv 2 \mod 8 \]
\[ x \equiv 3 \mod 9 \]

\[ N = 7 \times 8 \times 9 = 504 \]

\[ x = \left( 1 \times \frac{504}{7} \times \left[ \frac{504}{7} \right]^{-1} + 2 \times \frac{504}{8} \times \left[ \frac{504}{8} \right]^{-1} + 3 \times \frac{504}{9} \times \left[ \frac{504}{9} \right]^{-1} \right) \mod 7 \times 8 \times 9 \]

\[ = (1 \times 72 \times (72^{-1} \mod 7) + 2 \times 63 \times (63^{-1} \mod 8) + 3 \times 56 \times (56^{-1} \mod 9)) \mod 504 \]

\[ = (1 \times 72 \times 4 + 2 \times 63 \times 7 + 3 \times 56 \times 5) \mod 504 \]

\[ = (288 + 882 + 840) \mod 504 \]

\[ = 2010 \mod 504 \]

\[ = 498 \]

Primitive Roots

- From Euler’s theorem have $a^\phi(n) \mod n = 1$
- Consider $a^m = 1 \pmod{n}$, $\gcd(a, n) = 1$
  - For some $a$’s, $m$ can smaller than $\phi(n)$
- If the smallest $m$ is $\phi(n)$ then $a$ is called a primitive root
- If $n$ is prime, then successive powers of $a$ "generate" the group $\mod n$
- These are useful but relatively hard to find
Powers mod 19

<table>
<thead>
<tr>
<th>a</th>
<th>a²</th>
<th>a³</th>
<th>a⁴</th>
<th>a⁵</th>
<th>a⁶</th>
<th>a⁷</th>
<th>a⁸</th>
<th>a⁹</th>
<th>a¹⁰</th>
<th>a¹¹</th>
<th>a¹²</th>
<th>a¹³</th>
<th>a¹⁴</th>
<th>a¹⁵</th>
<th>a¹⁶</th>
<th>a¹⁷</th>
<th>a¹⁸</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>13</td>
<td>7</td>
<td>14</td>
<td>9</td>
<td>18</td>
<td>17</td>
<td>15</td>
<td>11</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>5</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>8</td>
<td>5</td>
<td>15</td>
<td>7</td>
<td>2</td>
<td>6</td>
<td>18</td>
<td>16</td>
<td>10</td>
<td>11</td>
<td>4</td>
<td>12</td>
<td>17</td>
<td>13</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>7</td>
<td>9</td>
<td>17</td>
<td>11</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>16</td>
<td>7</td>
<td>9</td>
<td>17</td>
<td>11</td>
<td>6</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>11</td>
<td>17</td>
<td>9</td>
<td>7</td>
<td>16</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>6</td>
<td>11</td>
<td>17</td>
<td>9</td>
<td>7</td>
<td>16</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>17</td>
<td>7</td>
<td>4</td>
<td>5</td>
<td>11</td>
<td>9</td>
<td>16</td>
<td>1</td>
<td>6</td>
<td>17</td>
<td>7</td>
<td>4</td>
<td>5</td>
<td>11</td>
<td>9</td>
<td>16</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>7</td>
<td>18</td>
<td>11</td>
<td>12</td>
<td>1</td>
<td>8</td>
<td>18</td>
<td>11</td>
<td>12</td>
<td>1</td>
<td>8</td>
<td>18</td>
<td>11</td>
<td>12</td>
<td>1</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>7</td>
<td>6</td>
<td>16</td>
<td>11</td>
<td>4</td>
<td>17</td>
<td>1</td>
<td>9</td>
<td>5</td>
<td>7</td>
<td>6</td>
<td>16</td>
<td>11</td>
<td>4</td>
<td>17</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>5</td>
<td>12</td>
<td>6</td>
<td>3</td>
<td>11</td>
<td>15</td>
<td>17</td>
<td>18</td>
<td>9</td>
<td>14</td>
<td>7</td>
<td>13</td>
<td>16</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>7</td>
<td>1</td>
<td>11</td>
<td>7</td>
<td>1</td>
<td>11</td>
<td>7</td>
<td>1</td>
<td>11</td>
<td>7</td>
<td>1</td>
<td>11</td>
<td>7</td>
<td>1</td>
<td>11</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>11</td>
<td>18</td>
<td>7</td>
<td>8</td>
<td>1</td>
<td>12</td>
<td>11</td>
<td>18</td>
<td>7</td>
<td>8</td>
<td>1</td>
<td>12</td>
<td>11</td>
<td>18</td>
<td>7</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>17</td>
<td>12</td>
<td>4</td>
<td>14</td>
<td>11</td>
<td>10</td>
<td>16</td>
<td>18</td>
<td>6</td>
<td>2</td>
<td>7</td>
<td>15</td>
<td>5</td>
<td>8</td>
<td>9</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>6</td>
<td>8</td>
<td>17</td>
<td>10</td>
<td>7</td>
<td>3</td>
<td>4</td>
<td>18</td>
<td>5</td>
<td>13</td>
<td>11</td>
<td>2</td>
<td>9</td>
<td>12</td>
<td>16</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>15</td>
<td>16</td>
<td>12</td>
<td>9</td>
<td>2</td>
<td>11</td>
<td>13</td>
<td>5</td>
<td>18</td>
<td>4</td>
<td>3</td>
<td>7</td>
<td>10</td>
<td>17</td>
<td>8</td>
<td>6</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>9</td>
<td>11</td>
<td>5</td>
<td>4</td>
<td>7</td>
<td>17</td>
<td>6</td>
<td>1</td>
<td>16</td>
<td>9</td>
<td>11</td>
<td>5</td>
<td>4</td>
<td>7</td>
<td>17</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>17</td>
<td>4</td>
<td>11</td>
<td>16</td>
<td>6</td>
<td>7</td>
<td>5</td>
<td>9</td>
<td>1</td>
<td>17</td>
<td>4</td>
<td>11</td>
<td>16</td>
<td>6</td>
<td>7</td>
<td>5</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>1</td>
<td>18</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
<td>1</td>
<td>18</td>
</tr>
</tbody>
</table>

- 2, 3, 10, 13, 14, 15 are primitive roots of 19
Discrete Logarithms

- The inverse problem to exponentiation is to find the **discrete logarithm** of a number modulo $p$
- That is to find $i$ such that $b = a^i \pmod{p}$
- This is written as $i = d\log_a b \pmod{p}$
- If $a$ is a primitive root then it always exists, otherwise it may not, e.g.,
  - $x = \log_3 4 \pmod{13}$ has no answer
  - $x = \log_2 3 \pmod{13} = 4$ by trying successive powers
- While exponentiation is relatively easy, finding discrete logarithms is generally a **hard** problem
Discrete Logarithms mod 19

(a) Discrete logarithms to the base 2, modulo 19

<table>
<thead>
<tr>
<th>$a$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\log_{2,19}(a)$</td>
<td>18</td>
<td>1</td>
<td>13</td>
<td>14</td>
<td>6</td>
<td>3</td>
<td>8</td>
<td>17</td>
<td>12</td>
<td>15</td>
<td>5</td>
<td>7</td>
<td>11</td>
<td>14</td>
<td>10</td>
<td>9</td>
<td>18</td>
<td></td>
</tr>
</tbody>
</table>

(b) Discrete logarithms to the base 3, modulo 19

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|-----|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|
| $\log_{3,19}(a)$ | 18 | 7 | 1 | 14 | 4 | 8 | 6 | 3 | 2 | 11 | 12 | 15 | 17 | 13 | 5 | 10 | 16 | 9 |

(c) Discrete logarithms to the base 10, modulo 19

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|-----|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|
| $\log_{10,19}(a)$ | 18 | 17 | 5 | 16 | 2 | 4 | 12 | 15 | 10 | 1 | 6 | 3 | 13 | 11 | 7 | 14 | 8 | 9 |

(d) Discrete logarithms to the base 13, modulo 19

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|-----|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|
| $\log_{13,19}(a)$ | 18 | 11 | 17 | 4 | 14 | 10 | 12 | 15 | 16 | 7 | 6 | 3 | 1 | 5 | 13 | 8 | 2 | 9 |

(e) Discrete logarithms to the base 14, modulo 19

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|-----|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|
| $\log_{14,19}(a)$ | 18 | 13 | 7 | 8 | 10 | 2 | 6 | 3 | 14 | 5 | 12 | 15 | 11 | 1 | 17 | 16 | 4 | 9 |

(f) Discrete logarithms to the base 15, modulo 19

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|-----|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|
| $\log_{15,19}(a)$ | 18 | 5 | 11 | 10 | 8 | 16 | 12 | 15 | 4 | 13 | 6 | 3 | 7 | 17 | 1 | 2 | 14 | 9 |
1. Fermat’s little theorem: \( a^{p-1} \equiv 1 \mod p \)
2. Euler’s Totient Function \( \varphi(p) = \# \text{ of } a < p \text{ relative prime to } p \)
3. Euler’s Theorem: \( a^{\varphi(p)} \equiv 1 \mod p \)
4. Primality Testing: \( n-1 = 2^k q, \ a^q \equiv 1, \ a^{2q} \equiv n-1, \ldots, (a^q)^{2^{k-1}} \equiv n-1 \)
5. Chinese Remainder Theorem: \( x \equiv a_i \mod m_i, \ i=1,\ldots,k, \) then you can calculate \( x \) by computing inverse of \( M_i \mod m_i \)
6. Primitive Roots: Minimum \( m \) such that \( a^m \equiv 1 \mod p \) is \( m=p-1 \)
7. Discrete Logarithms: \( a^i = b \mod p \Rightarrow i = \text{dlog}_{b,p}(a) \)
Homework 3

a. Use Fermat’s theorem to find a number $x$ between 0 and 22, such that $x^{111}$ is congruent to 8 modulo 23. Do not use brute force searching.

b. Use Miller Rabin test to test 19 for primality

c. $X = 2 \mod 3 = 3 \mod 5 = 5 \mod 7$, what is $x$?

d. Find all primitive roots of 11

e. Find discrete log of 17 base 2 mod 29
Acronyms

- AD  Anno Domini (Latin for "The Year of the Lord")
- CRT  Chinese Remainder Theorem
- DSA  Digital signature algorithm
- GCD  Greatest Common Divisor
- RSA  Rivest, Samir, and Adleman
Related Modules

CSE571S: Network Security (Spring 2017),
http://www.cse.wustl.edu/~jain/cse571-17/index.html

CSE473S: Introduction to Computer Networks (Fall 2016),
http://www.cse.wustl.edu/~jain/cse473-16/index.html

Wireless and Mobile Networking (Spring 2016),
http://www.cse.wustl.edu/~jain/cse574-16/index.html

CSE571S: Network Security (Fall 2014),
http://www.cse.wustl.edu/~jain/cse571-14/index.html

Audio/Video Recordings and Podcasts of Professor Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw