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/cse571-14/

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

These slides are partly based on Lawrie Brown's slides supplied with William Stallings's book "Cryptography and Network Security: Principles and Practice," 6th Ed, 2013.

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 ø(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 ø(n)**
- In general need prime factorization, but
  - for p (p prime) ø(p)=p-1
  - for p.q (p,q prime) ø(p.q)=(p-1)x(q-1)
- Examples: ø(37) = 36

  ø(21) = (3-1)x(7-1) = 2x6 = 12

Euler's Theorem

- A generalisation of Fermat's Theorem
- $a^{ø(n)} = 1 \pmod{n}$
  - for any a, n where $\gcd(a,n)=1$
- Example:

  $a=3$; $n=10$; $ø(10)=4$;

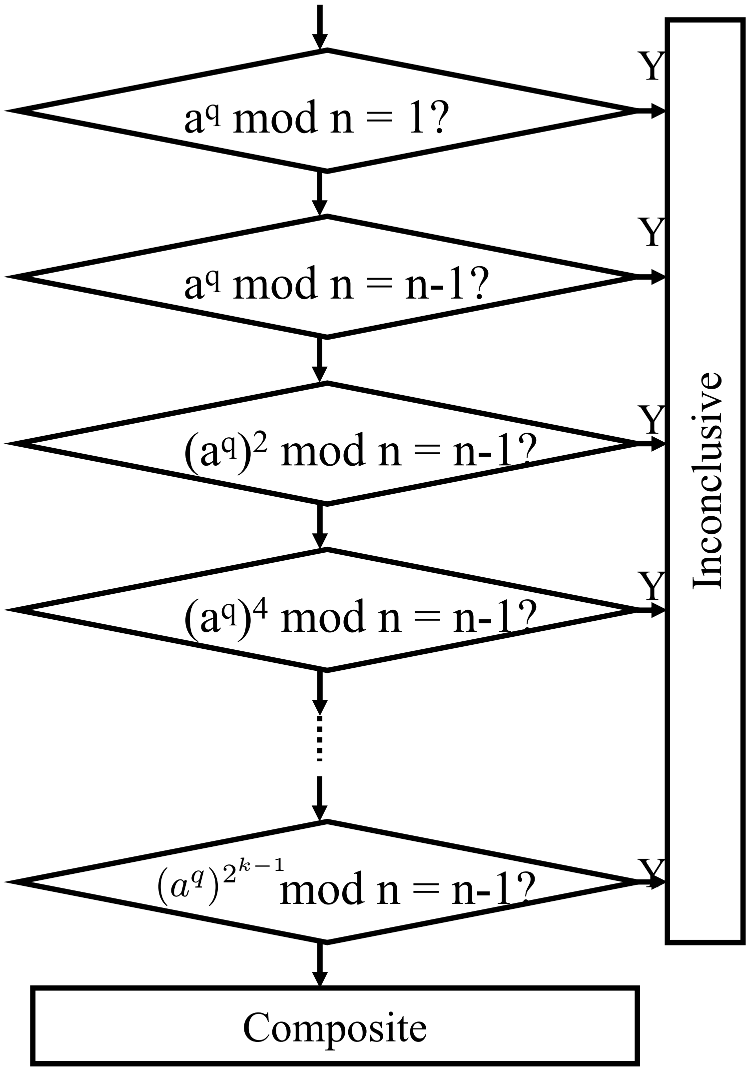
  hence $3^4 = 81 = 1 \bmod 10$

  $a=2$; $n=11$; $ø(11)=10$;

  hence $2^{10} = 1024 = 1 \bmod 11$
- Also have: $a^{ø(n)+1} = a \pmod{n}$

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** $a^q \bmod n = 1$ **then** return ("inconclusive");
  4. **for** $j = 0$ **to** $k - 1$ **do**
     5. **if** $(a^{2^j q} \bmod n = n-1)$ **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
    - $10^7 \bmod 29 = 17$
    - $17^2 \bmod 29 = 28 \Rightarrow$ Inconclusive
- Test 221 for primality
  - $221-1=220=2^2 \times 55$
  - Let a=5
    - $5^{55} \bmod 221 = 112$
    - $112^2 \bmod 221 = 168 \Rightarrow$ 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 $M = m_1 m_2 .. m_k$
- Chinese Remainder theorem lets us work in each moduli m_i separately
- Since computational cost is proportional to size, this is faster

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

- 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) +2x21$\times(21^{-1}$ 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

$35^{-1} = x \bmod 3$
$35x = 1 \bmod 3 \Rightarrow x = 2$
$21x = 1 \bmod 5 \Rightarrow x = 1$
$15x = 1 \bmod 7 \Rightarrow x = 1$

Chinese Remainder Theorem

- Alternately, the solution to the following equations:

  $x = a_1 \bmod m_1$

  $x = a_2 \bmod m_2$

  $x = a_k \bmod m_k$

  where $m_1, m_2, \ldots, m_k$ are relatively prime is found as follows:

  $M = m_1 m_2 \ldots M_k$ then

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

Chinese Remainder Theorem Example

- 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?

$$
\begin{aligned}
x &= 1 \bmod 7 \\
x &= 2 \bmod 8 \\
x &= 3 \bmod 9 \\
N &= 7 \times 8 \times 9 = 504 \\
x &= \left(1 \times \frac{504}{7} \times \left[\frac{504}{7}\right]_7^{-1} + 2 \times \frac{504}{8} \times \left[\frac{504}{8}\right]_8^{-1} \right. \\
&\quad \left. +3 \times \frac{504}{9} \times \left[\frac{504}{9}\right]_9^{-1}\right) \bmod 7 \times 8 \times 9 \\
&= (1 \times 72 \times (72^{-1} \bmod 7) + 2 \times 63 \times (63^{-1} \bmod 8) \\
&\quad +3 \times 56 \times (56^{-1} \bmod 9)) \bmod 504 \\
&= (1 \times 72 \times 4 + 2 \times 63 \times 7 + 3 \times 56 \times 5) \bmod 504 \\
&= (288 + 882 + 840) \bmod 504 \\
&= 2010 \bmod 504 \\
&= 498
\end{aligned}
$$

Ref: http://demonstrations.wolfram.com/ChineseRemainderTheorem/

Primitive Roots

- From Euler's theorem have $a^{ø(n)}$mod n=1
- Consider $a^m = 1$ (mod n), GCD(a,n)=1
  - For some a's, m can smaller than ø(n)
- If the smallest m is ø(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

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

- 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 $i = \mathrm{dlog}_a\, b \pmod{p}$
- If `a` is a primitive root then it always exists, otherwise it may not, e.g.,

  $x = \log_3 4 \bmod 13$ has no answer

  $x = \log_2 3 \bmod 13 = 4$ 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

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

(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

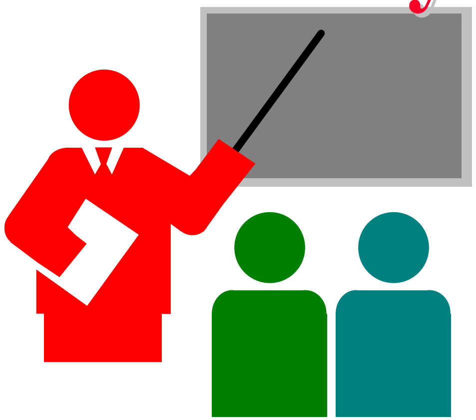
(e) Discrete logarithms to the base 14, modulo 19

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

Summary



1. Fermat's little theorem: $a^{p-1}=1 \bmod p$
2. Euler's Totient Function $ø(p)$ = # of $a<p$ relative prime to p
3. Euler's Theorem: $a^{ø(p)}=1 \bmod p$
4. Primality Testing: $n-1=2^k q$, $a^q=1$, $a^{2q}=n-1$, …, $(a^q)^{2^{k-1}}=n-1$
5. Chinese Remainder Theorem: $x=a_i \bmod m_i$, $i=1,\ldots,k$, then you can calculate x by computing inverse of $M_i \bmod m_i$
6. Primitive Roots: Minimum m such that $a^m=1 \bmod p$ is $m=p-1$
7. Discrete Logarithms: $a^i=b \bmod p \Rightarrow i=\mathrm{dlog}_{b,p}(a)$

Homework 8

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 bruteforce 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