Unit III Asymetric Ciphers
Some More Number Theory

Presented by: Er. Kobid Karkee
Himalaya College of Engineering

Number Theory

- Number theory deals with the theory of numbers and is probably one of the oldest branches of mathematics.
- It is divided into several areas including elementary, analytic and algebraic number theory.
- These are distinguished more by the methods used in each than the type of problems posed.
- Relevant ideas discussed here and include:
  - Prime numbers
  - Primality testing
  - Euler's Theorem and Fermat's little Theorem
  - Chinese Remainder Theorem

Prime Numbers

- A positive integer p is prime if the only positive factors of p are 1 and p
  - If there are other factors, it is composite
  - Note that 1 is not prime!
    - It's not composite either – it's in its own class

- An integer n is composite if and only if there exists an integer a such that $a \mid n$ and $1 < a < n$
- Prime numbers are of the utmost importance to certain cryptographic algorithms and most of the techniques used will not work without them.

Fundamental Theorem of Arithmetic

Fundamental Theorem of Arithmetic:

- Every positive integer greater than 1 can be uniquely written as a prime or as the product of two or more primes where the prime factors are written in order of increasing size.

- Examples
  - 100 = 2 * 2 * 5 * 5
  - 182 = 2 * 7 * 13
  - 29820 = 2 * 2 * 3 * 5 * 7 * 71

- In a fundamental sense, primes are the *building blocks* of the natural numbers.

Composite Factors

Theorem:

- If n is a composite integer, then n has a prime divisor less than or equal to the square root of n.
- Proof
  - Since n is composite, it has a factor a such that $1<a<n$
  - Thus, $n = ab$, where a and b are positive integers greater than 1
  - Either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ (Otherwise, assume a > $\sqrt{n}$ and b > $\sqrt{n}$, then $ab > \sqrt{n}*\sqrt{n} > n$. Contradiction.)
  - Thus, n has a divisor not exceeding $\sqrt{n}$
  - This divisor is either prime or a composite
    - If the latter, then it has a prime factor (by the Fundamental Theorem of Arithmetics)
  - In either case, n has a prime factor less than $\sqrt{n}$

Showing a number is a prime or composite

Show that 113 is prime.

- Solution
  - The only prime factors less than $\sqrt{113} = 10.63$ are 2, 3, 5, and 7
  - None of these divide 113 evenly
  - Thus, by the fundamental theorem of arithmetic, 113 must be prime

Show that 899 is composite.

- Solution
  - Divide 899 by successively larger primes, starting with 2
  - We find that 29 and 31 divide 899

Some random numbers factored

- 12304: 2 2 2 2 769
- 12304038495: 3 5 7 3109 37691
- 29485404038495: 5 5897080807699
- 294854040334945723: 67 2472061 1780217629
- 2948540403420344: 2 2 2 1109 3323422456427
- 294854043485472: 2 2 2 2 2 3 151 173 117574409
- 2948540420348 4: 2 2 3 101 103 229 1031411
- 9348492404203484: 2 2 7 23 145162925531 11
- 928439237492742742: 2 13 89 10453 12821 2993831
- 92843923293 78472: 2 2 2 31321 37053384029
- 928439232937847232 3: 3 3 3 307 1120085936708707

Apparent pattern of a several small prime factors ending with one or two very large primes.

Still many mysteries in prime number patterns…

Mersenne Numbers

- Mersenne number: any number of the form 2^n-1
- Mersenne prime: any prime of the form 2^p-1, where p is also a prime
  - Example: $2^5-1 = 31$ is a Mersenne prime
  - But $2^{11}-1 = 2047$ is not a prime (23*89)
- If M is a Mersenne prime, then M(M+1)/2 is a perfect number
  - A perfect number equals the sum of its divisors
  - Example: $2^3-1 = 7$ is a Mersenne prime, thus 7*8/2 = 28 is a perfect number
    - 28 = 1+2+4+7+14
  - Example: $2^5-1 = 31$ is a Mersenne prime, thus 31*32/2 = 496 is a perfect number
- The largest primes found are Mersenne primes.

Prime Factorisation

- to **factor** a number `n` is to write it as a product of other numbers: `n=a × b × c`
- note that factoring a number is relatively hard compared to multiplying the factors together to generate the number
- the **prime factorisation** of a number `n` is when its written as a product of primes
  - **eg.** $91=7\times13$; $3600=2^4\times3^2\times5^2$
- If P is the set of all prime numbers, then any positive integer can be written uniquely in the following form:

$$a = \prod_{p \in P} p^{a_p} \qquad \text{where each } a_p \geq 0$$

Relative Primes/Co-primes

- Two numbers are *relatively prime or co-primes* if they don't have any common factors (other than 1)
  - Rephrased: *a* and *b* are relatively prime if gcd (a,b) = 1

- gcd (25, 16) = 1, so 25 and 16 are relatively prime

Pairwise relatively prime

- A set of integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if, for all pairs of numbers, they are relatively prime
  - Formally: The integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

- Example: are 10, 17, and 21 pairwise relatively prime?
  - gcd(10,17) = 1, gcd (17, 21) = 1, and gcd (21, 10) = 1
  - Thus, they are pairwise relatively prime
- Example: are 10, 19, and 24 pairwise relatively prime?
  - Since gcd(10,24) ≠ 1, they are not

Fermat's Theorem

- Ancient Chinese mathematicians noticed that whenever n is prime, $2^{n-1} \equiv 1 \pmod{n}$.
  - Some also claimed that the converse was true.
- However, it turns out that the converse is not true!
  - If $2^{n-1} \equiv 1 \pmod{n}$, it doesn't follow that n is prime.
- Fermat generalized the ancient observation that $2^{p-1} \equiv 1 \pmod{p}$ for primes p to the following more general theorem:
- **Theorem:** (Fermat's Little Theorem.)
  - If p is prime and a is an integer not divisible by p (i.e. a and p are coprimes), then

    $a^{p-1} \equiv 1 \pmod{p}$ where gcd(a,p)=1
  - Furthermore, for every integer a

    $a^p \equiv a \pmod{p}$.

Euler Totient Function ø(n)

- when doing arithmetic modulo n
- **complete set of residues** is: `0..n-1`
- **reduced set of residues** is those numbers (residues) which are relatively prime to n
  - eg 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)**

Euler Totient Function ø(n)

- **Euler's totient function** (also called the Phi function) counts the number of positive integers less than *n* that are coprime to *n*. That is, $\phi(n)$ is the number of $m \in \mathbb{N}$ such that $1 \le m < n$ and $\gcd(m,n)=1$.
- to compute ø(n) need to count number of elements to be excluded
- 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)(q-1)
- eg.
  - ø(37) = 36
  - ø(21) = (3-1)×(7-1) = 2×6 = 12

Euler's Theorem

- Euler's theorem is a generalization of Fermat's little theorem dealing with powers of integers modulo positive integers.

Theorem:

- Let '*n*' be a positive integer, and let '*a*' be an integer that is relatively prime to *n*. Then

$$a^{\phi(n)} \bmod N = 1$$

where $\gcd(a,N)=1$

- eg.
  - $a=3; n=10; \phi(10)=4;$
  - hence $3^4 = 81 = 1 \bmod 10$
  - $a=2; n=11; \phi(11)=10;$
  - hence $2^{10} = 1024 = 1 \bmod 11$

Primality Testing

- often need to find large prime numbers
- traditionally **sieve** using **trial division**
  - ie. divide by all numbers (primes) in turn less than the square root of the number
  - only works for small numbers
- alternatively can use statistical primality tests based on properties of primes
  - for which all primes numbers satisfy property
  - but some composite numbers, called pseudo-primes, also satisfy the property

Miller Rabin Algorithm

- a test based on Fermat's Theorem
- algorithm is:

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**
   if $(a^{2^j q} \bmod n = n-1)$
   then return(" inconclusive ")
6. return ("composite")

Probabilistic Considerations

- if Miller-Rabin returns "composite" the number is definitely not prime
- otherwise is a prime or a pseudo-prime
- chance it detects a pseudo-prime is < ¼
- hence if repeat test with different random 'a' then chance n is prime after t tests is:
  - Pr(n prime after t tests) = $1-4^{-t}$
  - eg. for t=10 this probability is > 0.99999

Prime Distribution

- prime number theorem states that primes occur roughly every (`ln n`) integers
- since can immediately ignore evens and multiples of 5, in practice only need test `0.4 ln(n)` numbers of size n before locate a prime
  - note this is only the "average" sometimes primes are close together, at other times are quite far apart

Primes under 2000

Table 8.1 Primes Under 2000

2	101	211	307	401	503	601	701	809	907	1009	1103	1201	1301	1409	1511	1601	1709	1801	1901
3	103	223	311	409	509	607	709	811	911	1013	1109	1213	1303	1423	1523	1607	1721	1811	1907
5	107	227	313	419	521	613	719	821	919	1019	1117	1217	1307	1427	1531	1609	1723	1823	1913
7	109	229	317	421	523	617	727	823	929	1021	1123	1223	1319	1429	1543	1613	1733	1831	1931
11	113	233	331	431	541	619	733	827	937	1031	1129	1229	1321	1433	1549	1619	1741	1847	1933
13	127	239	337	433	547	631	739	829	941	1033	1151	1231	1327	1439	1553	1621	1747	1861	1949
17	131	241	347	439	557	641	743	839	947	1039	1153	1237	1361	1447	1559	1627	1753	1867	1951
19	137	251	349	443	563	643	751	853	953	1049	1163	1249	1367	1451	1567	1637	1759	1871	1973
23	139	257	353	449	569	647	757	857	967	1051	1171	1259	1373	1453	1571	1657	1777	1873	1979
29	149	263	359	457	571	653	761	859	971	1061	1181	1277	1381	1459	1579	1663	1783	1877	1987
31	151	269	367	461	577	659	769	863	977	1063	1187	1279	1399	1471	1583	1667	1787	1879	1993
37	157	271	373	463	587	661	773	877	983	1069	1193	1283		1481	1597	1669	1789	1889	1997
41	163	277	379	467	593	673	787	881	991	1087		1289		1483		1693			1999
43	167	281	383	479	599	677	797	883	997	1091		1291		1487		1697			
47	173	283	389	487		683		887		1093		1297		1489		1699			
53	179	293	397	491		691				1097				1493					
59	181			499										1499					
61	191																		
67	193																		
71	197																		
73	199																		
79																			
83																			
89																			
97																			

Chinese Remainder Theorem

- **Theorem:** (Chinese remainder theorem.) Let $m_1,\ldots,m_n > 0$ be relatively prime. Then the system of equations

  $x \equiv a_i \pmod{m_i}$ (for i=1 to n) has a unique solution modulo $m = m_1 \cdot \ldots \cdot m_n$.

- It is used to speed up modulo computations
- Chinese Remainder theorem lets us work in each moduli m_i separately
- since computational cost is proportional to size, this is faster than working in the full modulus m

Chinese Remainder Theorem Example

- What's x such that:

  $x \equiv 2 \pmod 3$

  $x \equiv 3 \pmod 5$

  $x \equiv 2 \pmod 7$?

- Using the Chinese Remainder theorem let:
- $m = 3 \times 5 \times 7 = 105$
- $M_1 = m/3 = 105/3 = 35$; 2 is an inverse of $M_1 = 35 \pmod 3$ (since $35 \times 2 \equiv 1 \pmod 3$)
- $M_2 = m/5 = 105/5 = 21$; 1 is an inverse of $M_2 = 21 \pmod 5$ (since $21 \times 1 \equiv 1 \pmod 5$)
- $M_3 = m/7 = 105/7 = 15$; 1 is an inverse of $M_3 = 15 \pmod 7$ (since $15 \times 1 \equiv 1 \pmod 7$)

- So $x \equiv 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 233 \equiv 23 \pmod{105}$
- So answer: 23

- So, we're solving equations in modular arithmetic.

Chinese Remainder Theorem Example

- By Chinese Remainder Theorem, an integer a where

  $0 \le a < m = \prod m_i$, $\gcd(m_i, m_{j \neq i}) = 1$, can be

  represented by a's residues mod m_i:

  $(a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_n)$

- Implicitly, consider the set of equations $x \equiv a_i \pmod{m_i}$, with $a_i = a \bmod m_i$. By the CRT, unique $x \equiv a \bmod m$, with $m = \prod m_i$ is a solution.

Primitive Roots

- Let *n* be a positive integer. A primitive root mod n is an integer *g* such that every integer relatively prime to *n* is congruent to a power of g mod n.
- That is, the integer *g* is a primitive root *(mod n)* if for every number *a* relatively prime to *n* there is an integer z such that $a \equiv (g^z (\mathrm{mod} n))$.
- these are useful but relatively hard to find

Primitive Roots

EXAMPLE

2 is a primitive root mod 5, because for every number a relatively prime to 5, there is an integer z such that $2^z \equiv a$. All the numbers relatively prime to 5 are 1, 2, 3, 4, and each of these (mod 5) is itself (for instance 2 (mod 5) = 2) :

- $2^0 = 1,\ 1 \pmod 5 = 1$, so $2^0 \equiv 1$
- $2^1 = 2,\ 2 \pmod 5 = 2$, so $2^1 \equiv 2$
- $2^3 = 8,\ 8 \pmod 5 = 3$, so $2^3 \equiv 3$
- $2^2 = 4,\ 4 \pmod 5 = 4$, so $2^2 \equiv 4$.

For every integer relatively prime to 5, there is a power of 2 that is congruent.

The number 3 is a primitive root modulo 7[1] because

$$
\begin{aligned}
3^1 &= 3^0 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod 7 \\
3^2 &= 3^1 \times 3 \equiv 3 \times 3 = 9 \equiv 2 \pmod 7 \\
3^3 &= 3^2 \times 3 \equiv 2 \times 3 = 6 \equiv 6 \pmod 7 \\
3^4 &= 3^3 \times 3 \equiv 6 \times 3 = 18 \equiv 4 \pmod 7 \\
3^5 &= 3^4 \times 3 \equiv 4 \times 3 = 12 \equiv 5 \pmod 7 \\
3^6 &= 3^5 \times 3 \equiv 5 \times 3 = 15 \equiv 1 \pmod 7 \\
3^7 &= 3^6 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod 7
\end{aligned}
$$

Primitive Roots

- 4 is not a primitive root mod 5, because for every number relatively prime to 5 (again, 1, 2, 3, 4) there is not a power of 4 that is congruent. Powers of 4 (mod 5) are only congruent to 1 or 4. There is no power of 4 that is congruent to 2 or 3:

  - $4^0 = 1,\ 1 \pmod 5 = 1$
  - $4^1 = 4,\ 4 \pmod 5 = 4$
  - $4^2 = 16,\ 16 \pmod 5 = 1$
  - $4^3 = 64,\ 64 \pmod 5 = 4$

  and the pattern continues...

Discrete Logarithms or Indices

- the inverse problem to exponentiation is to find the **discrete logarithm** of a number modulo p
- that is to find x where $a^x = b \bmod p$
- written as $x=\log_a b \bmod p$ **or** $x=\text{ind}_{a,p}(b)$
- if a is a primitive root then always exists, otherwise may not
  - x = $\log_3 4 \bmod 13$ (x st $3^x = 4 \bmod 13$) has no answer
  - x = $\log_2 3 \bmod 13 = 4$ by trying successive powers
- whilst exponentiation is relatively easy, finding discrete logarithms is generally a **hard** problem