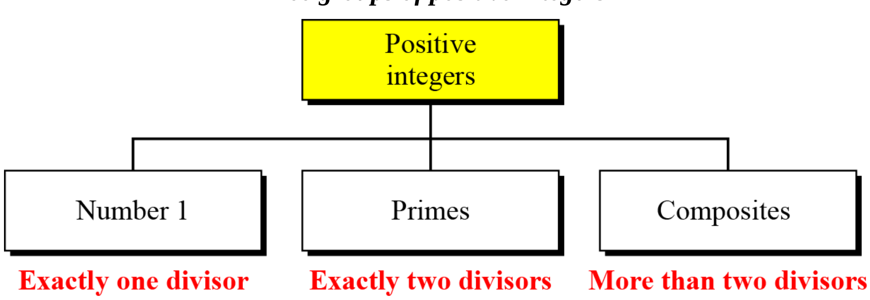
MATHEMATICS OF CRYPTOGRAPHY PART III

Primes and Related Congruence Equations

Primes

Three groups of positive integers



A prime is divisible only by itself and 1.

Euler's Phi-Function

- *Euler's phi-function*, ϕ (n), which is sometimes called the *Euler's totient function* plays a very important role in cryptography.
- The function finds the number of integers that are both smaller than n and relatively prime to n

1. $\phi(1) = 0$.
2. $\phi(p) = p - 1$ if p is a prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime.
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

Euler's Phi-Function(cont.)

- We can combine the above four rules to find the value of ϕ(n). For example, if n can be factored as

$$n = p_1^{e1} \times p_2^{e2} \times \ldots \times p_k^{ek}$$

- Then we combine the third and the fourth rule to find

$$\phi(n) = (p_1^{e_1} - p_1^{e_1 - 1}) \times (p_2^{e_2} - p_2^{e_2 - 1}) \times \cdots \times (p_k^{e_k} - p_k^{e_k - 1})$$

The difficulty of finding ϕ(n) depends on the difficulty of finding the factorization of n.

Euler’s Phi-Function(cont.)

- Example 1
  - What is the value of $\phi(13)$?
- Solution
  - Because 13 is a prime, $\phi(13) = (13 - 1) = 12$.
- Example 2
  - What is the value of $\phi(10)$?
- Solution
  - We can use the third rule: $\phi(10) = \phi(2) \times \phi(5) = 1 \times 4 = 4$, because 2 and 5 are primes.

Euler’s Phi-Function(cont.)

- Example 3
  - What is the value of $\phi(240)$?
- Solution
  - We can write $240 = 2^4 \times 3^1 \times 5^1$. Then

    $$\phi(240) = (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0) = 64$$
- Example 4
  - Can we say that $\phi(49) = \phi(7) \times \phi(7) = 6 \times 6 = 36$????

Euler's Phi-Function(cont.)

- Example 3
  - What is the value of $\phi(240)$?
- Solution
  - We can write $240 = 2^4 \times 3^1 \times 5^1$. Then

$$\phi(240) = (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0) = 64$$

- Example 4
  - Can we say that $\phi(49) = \phi(7) \times \phi(7) = 6 \times 6 = 36$????
- Solution
  - No. The third rule applies when *m* and *n* are relatively prime. Here $49 = 7^2$. We need to use the fourth rule: $\phi(49) = 7^2 - 7^1 = 42$.

Euler's Phi-Function(cont.)

- Example 5
  - What is the number of elements in $Z_{14}*$?
- Solution
  - The answer is $\phi(14) = \phi(7) \times \phi(2) = 6 \times 1 = 6$. The members are 1, 3, 5, 9, 11, and 13.

Interesting point: If n > 2, the value of $\phi(n)$ is even.

Fermat's Little Theorem

- First Version
  - If p is a prime and a is an integer such that p does not divide a,

$$a^{p-1} \equiv 1 \bmod p$$

- Second Version
  - Removes the condition on a
  - If p is prime and a is an integer,

$$a^{p} \equiv a \bmod p$$

Fermat's Little Theorem(cont.)

- Example 1
  - Find the result of 6^{10} mod 11.
- Solution
  - We have 6^{10} mod 11 = 1. This is the first version of Fermat's little theorem where $p = 11$.
- Example 2
  - Find the result of 3^{12} mod 11.
- Solution

Fermat's Little Theorem(cont.)

- Example 1
  - Find the result of 6^{10} mod 11.
- Solution
  - We have 6^{10} mod 11 = 1. This is the first version of Fermat's little theorem where p = 11.
- Example 2
  - Find the result of 3^{12} mod 11.
- Solution
  - Here the exponent (12) and the modulus (11) are not the same. With substitution this can be solved using Fermat's little theorem.

$$3^{12} \bmod 11 = (3^{11} \times 3) \bmod 11 = (3^{11} \bmod 11)\,(3 \bmod 11) = (3 \times 3) \bmod 11 = 9$$

Fermat's Little Theorem(cont.)

- Multiplicative Inverses

$$a^{-1} \bmod p = a^{p-2} \bmod p$$

- The answers to multiplicative inverses modulo a prime can be found without using the extended Euclidean algorithm:

a. $8^{-1} \bmod 17 = 8^{17-2} \bmod 17 = 8^{15} \bmod 17 = 15 \bmod 17$

b. $5^{-1} \bmod 23 = 5^{23-2} \bmod 23 = 5^{21} \bmod 23 = 14 \bmod 23$

c. $60^{-1} \bmod 101 = 60^{101-2} \bmod 101 = 60^{99} \bmod 101 = 32 \bmod 101$

d. $22^{-1} \bmod 211 = 22^{211-2} \bmod 211 = 22^{209} \bmod 211 = 48 \bmod 211$

Euler's Theorem

- First Version
  - If a and n are coprime,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

- Second Version
  - Removes the condition that a and n should be coprime

$$a^{k \times \phi(n) + 1} \equiv a \pmod{n}$$

The second version of Euler's theorem is used in the RSA cryptosystem

Euler's Theorem(cont.)

- Example 1
  - Find the result of 6^{24} mod 35.
- Solution
  - We have 6^{24} mod 35 = $6^{\phi(35)}$ mod 35 = 1.
- Example 2
  - Find the result of 20^{62} mod 77???

Euler's Theorem(cont.)

- Example 1
  - Find the result of 6^{24} mod 35.
- Solution
  - We have 6^{24} mod 35 = $6^{\phi(35)}$ mod 35 = 1.
- Example 2
  - Find the result of 20^{62} mod 77.
- Solution

If we let k = 1 on the second version, we have
20^{62} mod 77 = (20 mod 77) ($20^{\phi(77)+1}$ mod 77) mod 77
= (20)(20) mod 77 = 15.

Euler's Theorem(cont.)

- Multiplicative Inverses
  - Euler's theorem can be used to find multiplicative inverses modulo a composite.

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

Euler's Theorem(cont.)

- Example
  - The answers to multiplicative inverses modulo a composite can be found without using the extended Euclidean algorithm if we know the factorization of the composite:

a. $8^{-1} \bmod 77 = 8^{\phi(77)-1} \bmod 77 = 8^{59} \bmod 77 = 29 \bmod 77$

b. $7^{-1} \bmod 15 = 7^{\phi(15)-1} \bmod 15 = 7^{7} \bmod 15 = 13 \bmod 15$

c. $60^{-1} \bmod 187 = 60^{\phi(187)-1} \bmod 187 = 60^{159} \bmod 187 = 53 \bmod 187$

d. $71^{-1} \bmod 100 = 71^{\phi(100)-1} \bmod 100 = 71^{39} \bmod 100 = 31 \bmod 100$

CHINESE REMAINDER THEOREM

- Used to solve a set of congruent equations with one variable but different moduli, which are relatively prime

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\cdots \\
x &\equiv a_k \pmod{m_k}
\end{aligned}
$$

Continued…

- Example
  - The following is an example of a set of equations with different moduli:

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

  - The solution to this set of equations is given in the next section; for the moment, note that the answer to this set of equations is x = 23. This value satisfies all equations: 23 ≡ 2 (mod 3), 23 ≡ 3 (mod 5), and 23 ≡ 2 (mod 7).

Continued…

- Solution To Chinese Remainder Theorem
  - Find $M = m_1 \times m_2 \times \ldots \times m_k$. This is the common modulus.
  - Find $M_1 = M/m_1$, $M_2 = M/m_2$, …, $M_k = M/m_k$.
  - Find the multiplicative inverse of M_1, M_2, …, M_k using the corresponding moduli (m_1, m_2, …, m_k). Call the inverses M_1^{-1}, M_2^{-1}, …, M_k^{-1}.
  - The solution to the simultaneous equations is

$$\boxed{x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}) \bmod M}$$

Continued…

- Example
  - Find the solution to the simultaneous equations:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

- Solution: We follow the four steps.
  1. $M = 3 \times 5 \times 7 = 105$
  2. $M_1 = 105 / 3 = 35$, $M_2 = 105 / 5 = 21$, $M_3 = 105 / 7 = 15$
  3. The inverses are $M_1^{-1} = 2$, $M_2^{-1} = 1$, $M_3^{-1} = 1$
  4. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105 = 23 \bmod 105$

Continued…

- Example
  - Find an integer that has a remainder of 3 when divided by 7 and 13, but is divisible by 12.
- Solution ????

Continued…

- Example
  - Find an integer that has a remainder of 3 when divided by 7 and 13, but is divisible by 12.
- Solution
  - This is a CRT problem. We can form three equations and solve them to find the value of x.

$$x = 3 \bmod 7$$
$$x = 3 \bmod 13$$
$$x = 0 \bmod 12$$

  - If we follow the four steps, we find x = 276. We can check that
    276 = 3 mod 7, 276 = 3 mod 13 and 276 is divisible by 12 (the quotient is 23 and the remainder is zero).

Continued…

- Assume we need to calculate z = x + y where x = 123 and y = 334, but our system accepts only numbers less than 100. These numbers can be represented as follows:

$$\begin{array}{ll} x \equiv 24 \pmod{99} & y \equiv 37 \pmod{99} \\ x \equiv 25 \pmod{98} & y \equiv 40 \pmod{98} \\ x \equiv 26 \pmod{97} & y \equiv 43 \pmod{97} \end{array}$$

- Adding each congruence in x with the corresponding congruence in y gives

$$\begin{array}{lll} x + y \equiv 61 \pmod{99} & \rightarrow & z \equiv 61 \pmod{99} \\ x + y \equiv 65 \pmod{98} & \rightarrow & z \equiv 65 \pmod{98} \\ x + y \equiv 69 \pmod{97} & \rightarrow & z \equiv 69 \pmod{97} \end{array}$$

- Now three equations can be solved using the Chinese remainder theorem to find z. One of the acceptable answers is z = 457.

Continued…

Secret Sharing scheme in cryptography aims to distribute and later recover secret S among n parties. Secret S is distributed in form of shares which are generated from secret. Without cooperation of k no. of parties, the secret cannot be reconstructed from shares directly. Consider the following example:

Say our secret is S. The shares for n=4 no. of parties are generated taking modulus 11,13,17 and 19. They are respectively 1,12,2 and 3 and given by following equations:

Now, from four possible sets of k=3 shares (as k shares are necessary to reconstruct the secret), consider one possible set {1, 12, 2} and recover the secret S from it.

Continued…

Secret Sharing scheme in cryptography aims to distribute and later recover secret S among n parties. Secret S is distributed in form of shares which are generated from secret. Without cooperation of k no. of parties, the secret cannot be reconstructed from shares directly. Consider the following example:

Say our secret is S. The shares for n=4 no. of parties are generated taking modulus 11,13,17 and 19. They are respectively 1,12,2 and 3 and given by following equations:

S Ξ 1 mod 11,

S Ξ 12 mod 13,

S Ξ 2 mod 17,

S Ξ 3 mod 19.

Now, from four possible sets of k=3 shares (as k shares are necessary to reconstruct the secret), consider one possible set {1, 12, 2} and recover the secret S from it.

Continued…

Solution: The problem can be solved by Chinese remainder theorem.

For the set {1,12,2}, the equations available are,

$S \equiv 1 \bmod 11$,

$S \equiv 12 \bmod 13$,

$S \equiv 2 \bmod 17$,

Now solving this equation using CRT, M=11 *13*17 = 2431,

M1 = 2431/11=221,

M2 = 2431/13=187,

M3=2431/17=143

$M1^{-1}$, $M2^{-1}$ and $M3^{-1}$ can be calculated using Extended Euclidean Algorithm.

$M1^{-1} = 1$

$M2^{-1} = 8$

$M3^{-1} = 5$

Now, secret S= ((1*221*1) + (12*187*8) + (2*143*5)) mod 2431

S = 155 mod 2431