NUMBER THEORY

EXTC – BE – DATA COMPRESSION AND CRYPTOGRAPHY

Ms. Vandana Sawant

Assistant Professor

Dept. of Electronics & Telecommunication Engineering,

SIES Graduate School of Technology

QUESTIONS

- Define Fermat's little theorem .
- State Fermat's little theorem and Euler's theorem. Illustrate with an example how FLT can be used to find modular inverse.
- State Fermat's little theorem and Euler's theorem in modular arithmetic. What is Euler's totient function.
- State Fermat's theorem with their application in cryptography.
- State Euler's theorem with their application in cryptography.
- Write a short note on chines remainder theorem.
- State chines remainder theorem with their application in cryptography.
- Explain chines remainder theorem with example.
- Find the solution to the simultaneous equation x=2 mod 3, x=3 mod 5, x=2 mod 7

OBJECTIVES OF LECTURE

- Students should be able to

  - Know about number theory.

PRIME NUMBERS

- Prime Number – An integer whose only factors are 1 and itself.
- Factor – a number that can divide another number without a remainder.
- Prime Factors – an expression of numbers that divides another integer without a remainder where all the factors are prime.
- Let’s look at a number grid from 1 to 100 and see how they were discovered.

PRIME NUMBERS

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			

MODULAR ARITHMATIC

- The modular arithmetic deals with operations on integers specifically around remainders from division

dividend	divisor	quotient	Remainder(modulus)
15	5	3	0
15	4	3	3
15	3	5	0
15	2	7	1
15	1	15	0

- 15/2=7 remainder 1 can be written as 15mod2=1

MODULAR ARITHMATIC

- Congruence property: two numbers are said to be in congruence modulo, if they give out same mod
- For ex 15 mod 2=1
- 17 mod 2=1
- So 15 is congruence to 17 mod 2
- 15=17(mod2)

FERMAT'S THEOREM

- Fermat's theorem also known as Fermat's little theorem or fermat's primality test , states that for any prime number 'p' and any integer 'a' such that 'p' does not divide 'a'(the pair are relatively prime) 'p' divides exactly into $a^p - a$
- This can be expressed as
- $a^p \equiv a(mod\ p)$
- Another variant of thi theorem is when 'a' is not divisible by 'p'
- $a^{p-1} \equiv 1(mod\ p)$

FERMAT’S THEOREM

- Proof
- Let a= 2 and p=7
- a^7= $2^7 = 128$
- a^7-a=128-2=126
- 126=7$\div$ 18 $and\ no\ remainder$
- Second variant can be similarly proved
- $a^{7-1} \equiv a^6 = 2^6 = 64$
- Now $64(mod\ 7) = 1$

FERMAT'S THEOREM

- Find $2^{16} mod(17)$
- Solution :
- You can rewrite 2^{17-1} mod(17)
- According to Fermat's theorem
- $a^{p-1} \equiv 1(mod\ p)$
- 2^{17-1} $\equiv$1mod(17)
- Hence 2^{17-1} mod(17)=1

SIES Graduate School of Technology
RISE WITH EDUCATION

FERMAT'S THEOREM

- Find $2^{50} mod(17)$
- Solution :
- You can rewrite $2^{50} mod(17) \quad as \quad [(2^{16})^3 * 2^4] mod(17)$
- $=[(2^{17-1} \text{ mod}(17))^3 \; *4(\text{mod}17)]$
- $= 1^3 *4(\text{mod}17)$
- $=4$

FERMAT'S THEOREM

- Find the result using farmat's little theorem (i)$3^{12} mod(11)$ (ii)$3^{10} mod(11)$
- Solution :
- You can rewrite

EULER'S THEOREM

- EULER'S theorem is also known as the Fermat's Euler theorem or Euler's totient theorem states that if 'n' and 'a' are coprime positive integers then $a^{\Phi(n)} \equiv 1 \pmod{n}$ where $\phi(n)$ is Euler's totient function.
- Euler's totient function counts the positive integer 'n' that are relatively prime to 'n'. It is denoted by the Greek letter phi $\phi(n)$. These co prime number are also called as totative.
- Find $\phi(n)$where n=5
- Solution :
- Numbers greater than or equal to 1 and less than 5 are 1, 2,3 and 4
- Each pair is co prime with 5 because
- Gcd(1,5) =1
- Gcd(2,5)=1
- Gcd(3,5)=1
- Gcd(4,5)=1
- Hence $\phi(5)$=4(that is there are 4 co prime number with respect to 5)

EULER'S THEOREM

- Compute this using Euler's totient function $\phi(37)$, $\phi(35)$ and $\phi(75)$
- Solution
- Hence $\phi(37)=36$(that is there are 36 co prime numbers with respect to 37)
- Hence $\phi(35)=24$(that is there are 24 co prime numbers with respect to 35)
- Hence $\phi(75)=40$(that is there are 40 co prime numbers with respect to 75)

EULER'S THEOREM

- Compute this using Euler's totient function $\phi(37)$, $\phi(49)$ and $\phi(100)$
- Solution
- Hence $\phi(37)=36$(that is there are 36 co prime numbers with respect to 37)
- Hence $\phi(49)=42$(that is there are 42 co prime numbers with respect to 49)
- Hence $\phi(100)=40$(that is there are 40 co prime numbers with respect to 100)

CRT THEOREM

- The Chinese remainder theorem(CRT) helps to solve a system of simultaneous linear congruences
- Let m1,m2,……………..mr be the collection of pairwise relatively prime integers. Then the system of simultaneous congruences
- X ≡ a1(mod m1)
- X ≡ a2 (mod m2)
- .
- .
- X ≡ ar(mod mr)
- Has a unique solution modulo M=m1m2……..mr for any given integers a1,a2,…….ar

CRT THEOREM

- Find the value of x using Chinese remainder theorem(CRT) when $x \equiv 2 \bmod 7$, $x \equiv 3 \bmod 9$
- Here a1=2, a2=3
- m1=7, m2=9
- According to CRT
- x=(M1x1a1+M2x2a2)mod M
- M=m1*m2=7*9=63
- M1=M/m1=63/7
- M2 = M/m2=63/9
- Calculate inverse modulo for each congruence
- $M1x1 \equiv 2(\bmod 7)$
- $9x1 \equiv 2(\bmod 7)$

CRT THEOREM

Value of x1	operation	result
0	(9*0)mod7	0
1	(9*1)mod7	2
2	(9*2)mod7	4
3	(9*3)mod7	6
4	(9*4)mod7	1

- Hence modulo inverse of $9x1 \equiv 2 \pmod 7$ is 4. Hence x1=4
- Similarly
- $M2x2 \equiv 3 \pmod 9$
- $7x2 \equiv 3 \pmod 9$

CRT THEOREM

- Value of x2| operation | result
- 0 (7*0)mod9 0
- 1 (7*1)mod9 7
- 2 (7*2)mod9 5
- 3 (7*3)mod9 3
- 4 (7*4)mod9 1
- Hence modulo inverse of $7x2 \equiv 3$(mod9)is 4. Hence x2=4
- Putting this value in crt equation you get
- x=(M1x1a1+M2x2a2)mod M
- x=(9*4*2+7*4*3)mod 63
- X=30
- So $30 \equiv 2$(mod7)
- $30 \equiv 3$ (mod 9)

CRT THEOREM

- In school picnic
- 1. if children were arranged in group of 3 , 2 children were left out
- 2. if children were arranged in group of 4 , 3 children were left out
- 3. if children were arranged in group of 5 , 4 children were left out
- Find out minimum no of children could be in school picnic
- Assume that no of children's in the school picnic is x

CRT THEOREM

CRT THEOREM

CRT THEOREM

CRT THEOREM

CRT THEOREM

- Find the solution to simultaneous equation $x=2 \bmod 3$, $x=3 \bmod 5$, $x=2 \bmod 7$

CRT THEOREM

- Find the solution to simultaneous equation x=2mod3, x=3mod5, x=2mod7

CRT THEOREM

- Find the solution to simultaneous equation x=2mod3, x=3mod5, x=2mod7

CRT THEOREM

- Find the solution to simultaneous equation $x=2 \bmod 3$, $x=3 \bmod 5$, $x=2 \bmod 7$

Euler's Theorem

Euler's Theorem

Given integer $n > 1$, such that $\gcd(a, n) = 1$ then

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

Corollary of Theorem 7.14

Corollary

Given integer $n > 1$, such that $\gcd(a, n) = 1$ then

$a^{\Phi(n)-1} \bmod n$ is a multiplicative inverse of a mod n.

Corollary

Given integer $n > 1$, x, y, and a positive integers with $\gcd(a, n) = 1$. If $x \equiv y \pmod{\Phi(n)}$, then

$$a^x \equiv a^y \pmod{n}.$$

Consequence of Euler's Theorem

Principle of Modular Exponentiation

Given a, n, x, y with $n \geq 1$ and $\gcd(a,n)=1$,
if $x \equiv y \pmod{\phi(n)}$, then

$$a^x \equiv a^y \pmod{n}$$

Proof idea:

$a^x = a^{k\phi(n) + y} = a^y (a^{\phi(n)})^k$

by applying Euler's theorem we obtain

$a^x \equiv a^y \pmod{p}$

Chinese Reminder Theorem (CRT)

Theorem

Let $n_1, n_2, ,,, n_k$ be integers s.t. $\gcd(n_i, n_j) = 1$ for any $i \neq j$.

$$x \equiv a_1 \bmod n_1$$

$$x \equiv a_2 \bmod n_2$$

$$\ldots$$

$$x \equiv a_k \bmod n_k$$

There exists a unique solution modulo

$$n = n_1\, n_2 \ldots n_k$$

Proof of CRT

- Consider the function χ: $Z_n \rightarrow Z_{n1} \times Z_{n2} \times \ldots \times Z_{nk}$ $\chi(x) = (x \bmod n_1, \ldots, x \bmod n_k)$
- We need to prove that χ is a bijection.
- For $1 \leq i \leq k$, define $m_i = n / n_i$, then $\gcd(m_i, n_i) = 1$
- For $1 \leq i \leq k$, define $y_i = m_i^{-1} \bmod n_i$
- Define function $\rho(a1,a2,\ldots,ak) = \Sigma\ a_i m_i y_i \bmod n$, this function inverts χ
  - $a_i m_i y_i \equiv a_i \pmod{n_i}$
  - $a_i m_i y_i \equiv 0 \pmod{n_j}$ where $i \neq j$

An Example Illustrating Proof of CRT

- Example of the mappings:
  - $n_1=3$, $n_2=5$, $n=15$
  - $m_1=5$, $y_1=m_1^{-1} \bmod n_1=2$, $5 \cdot 2 \bmod 3 = 1$
  - $m_2=3$, $y_2=m_2^{-1} \bmod n_2=2$, $3 \cdot 2 \bmod 5 = 1$

  - $\rho(2,4) = (2 \cdot 5 \cdot 2 + 4 \cdot 3 \cdot 2) \bmod 15 = 44 \bmod 15 = 14$
  - $14 \bmod 3 = 2$, $14 \bmod 5 = 4$

Example of CRT:

$x \equiv 5 \pmod{7}$
$x \equiv 3 \pmod{11}$
$x \equiv 10 \pmod{13}$

- $n_1=7$, $n_2=11$, $n_3=13$, $n=1001$
- $m_1=143$, $m_2=91$, $m_3=77$
- $y_1=143^{-1} \bmod 7 = 3^{-1} \bmod 7 = 5$
- $y_2=91^{-1} \bmod 11 = 3^{-1} \bmod 11 = 4$
- $y_3=77^{-1} \bmod 13 = 12^{-1} \bmod 13 = 12$

- $x \quad =(5\times143\times5 + 3\times91\times4 + 10\times77\times12) \bmod 1001$
  $= 13907 \bmod 1001 = 894$

Fermat's Little Theorem

Fermat's Little Theorem

If *p* is a prime number and *a* is a natural number that is not a multiple of p, then

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

Proof idea: Corollary of Theorem 7.14

- $\gcd(a, p) = 1$, then the set $\{ i \cdot a \bmod p\}$ $0 < i < p$ is a permutation of the set $\{1, \ldots, p-1\}$.
  - otherwise we have $0<n<m<p$ s.t. $ma \bmod p = na \bmod p$, and thus $p \mid (ma - na) \Rightarrow p \mid (m-n)$, where $0<m-n < p$)
- $a \times 2a \times \ldots \times (p-1)a = (p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}$

Since $\gcd((p-1)!, p) = 1$, we obtain $a^{p-1} \equiv 1 \pmod{p}$

Euler's Theorem

Euler's Theorem

Given integer $n > 1$, such that $\gcd(a, n) = 1$ then

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

Corollary of Theorem 7.14

Corollary

Given integer $n > 1$, such that $\gcd(a, n) = 1$ then

$a^{\Phi(n)-1} \bmod n$ is a multiplicative inverse of $a \bmod n$.

Corollary

Given integer $n > 1$, x, y, and a positive integers with $\gcd(a, n) = 1$. If $x \equiv y \pmod{\Phi(n)}$, then

$$a^x \equiv a^y \pmod{n}.$$

Consequence of Euler's Theorem

Principle of Modular Exponentiation

Given a, n, x, y with $n \geq 1$ and $\gcd(a,n)=1$,
if $x \equiv y \pmod{\phi(n)}$, then

$$a^x \equiv a^y \pmod{n}$$

Proof idea:

$a^x = a^{k\phi(n) + y} = a^y (a^{\phi(n)})^k$

by applying Euler's theorem we obtain

$a^x \equiv a^y \pmod{p}$

Chinese Reminder Theorem (CRT)

Theorem

Let n_1, n_2, ,,, n_k be integers s.t. $\gcd(n_i, n_j) = 1$ for any $i \neq j$.

$$x \equiv a_1 \bmod n_1$$

$$x \equiv a_2 \bmod n_2$$

$$\ldots$$

$$x \equiv a_k \bmod n_k$$

There exists a unique solution modulo

$$n = n_1 n_2 \ldots n_k$$

Proof of CRT

- Consider the function χ: $Z_n \rightarrow Z_{n1} \times Z_{n2} \times \ldots \times Z_{nk}$ $\chi(x) = (x \bmod n_1, \ldots, x \bmod n_k)$
- We need to prove that χ is a bijection.
- For $1 \leq i \leq k$, define $m_i = n / n_i$, then $\gcd(m_i, n_i) = 1$
- For $1 \leq i \leq k$, define $y_i = m_i^{-1} \bmod n_i$
- Define function $\rho(a1,a2,\ldots,ak) = \Sigma\ a_i m_i y_i \bmod n$, this function inverts χ
  - $a_i m_i y_i \equiv a_i \pmod{n_i}$
  - $a_i m_i y_i \equiv 0 \pmod{n_j}$ where $i \neq j$

An Example Illustrating Proof of CRT

- Example of the mappings:
  - n_1=3, n_2=5, n=15
  - m_1=5, y_1=m_1^{-1} mod n_1=2,   5·2 mod 3 = 1
  - m_2=3, y_2=m_2^{-1} mod n_2=2,   3·2 mod 5 = 1

  - $\rho(2,4)$ = (2·5·2 + 4·3·2) mod 15 = 44 mod 15 = 14
  - 14 mod 3 = 2, 14 mod 5 = 4

Example of CRT:

$x \equiv 5 \pmod{7}$
$x \equiv 3 \pmod{11}$
$x \equiv 10 \pmod{13}$

- $n_1=7,\ \ n_2=11,\ \ n_3=13,\ \ n=1001$
- $m_1=143,\ \ m_2=91,\ \ m_3=77$
- $y_1=143^{-1} \bmod 7 = 3^{-1} \bmod 7 = 5$
- $y_2=91^{-1} \bmod 11 = 3^{-1} \bmod 11 = 4$
- $y_3=77^{-1} \bmod 13 = 12^{-1} \bmod 13 = 12$

- $x \quad =(5\times143\times5 + 3\times91\times4 + 10\times77\times12) \bmod 1001$
  $= 13907 \bmod 1001 = 894$

Thank You!

(vandanas@sies.edu.in)