Introduction to Number Theory

Acknowledgement & References

- “Cryptography & Network Security” by William Stallings, Pearson Education Asia.
- “Cryptography and Network Security” by Behrouz A. Forouzan, Mc Graw Hill.
- “Introduction to Cryptography with Coding Theory” by Wade Trappe & Lawrence C Washington, Pearson.

Objective

- To introduce prime numbers
- To introduce Congruence
- To introduce CRT
- To introduce Fermat's & Euler's Theorem
- To introduce finite fields
- To introduce discrete logarithms

Number system

N : Set of Natural Numbers $\{1, 2, \ldots\}$

Z : Set of Integers $\{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$

- Divisibility
- Def^n: a, b integers, $a \neq 0$, then a divides b if there is an integer k such that $b=ak$. If a divides b then a is called divisor of b and relation is expressed symbolically as $a|b$.
- *Example* : $3|48$ as $48=3\times 16$.
- If $a|b$ and $a|c$, then $a|(b+c)$

Primes

- Asymmetric-key cryptography uses primes extensively.
- **Def^{n}:** An integer $p \geq 2$ is called Prime if and only if it is divisible only by 1 and by itself (that is it has no proper factors) **(its only divisors/factors are ±1 and ±p).**
- **Example:** The smallest prime is 2, which is divisible by ±2 (itself) and **±1** .

- **Example:**
- List the primes smaller than 10.
- There are four primes less than 10: 2, 3, 5, and 7.

- Note: By convention, the number 1 is neither Prime nor Composite.

Fundamental Theorem of Arithmetic

- Every integer n >= 2 has a factorization as a product of primes:
- i.e. n = $p_1^{a1} p_2^{a2}$ _ _ _ p_k^{ak}
- where the p_i are distinct primes in increasing order, and the a_i positive integers.
- Example: 504= $2^3 * 3^2 * 7$

GCD

- Greatest Common Divisor (GCD) of n numbers $a_1, a_2, \ldots, a_n$ is the largest positive divisor of $a_1, a_2, \ldots, a_n$.
- Example: GCD of 12,30,72,120 is 6, symbolically GCD of 12,30,72,120 is written as gcd(12,30,72,120).
- Find gcd(28, 952) (Euclidean algorithm is used for finding the gcd of 2 large integers)

Properties of GCD:

1. gcd(a,0)= a
2. gcd(a,b)=gcd(b,a)
3. gcd(a,ka)= a

.....

Contd.

- Ex: gcd (6,4) = 2
- gcd (24,60) = 12
- Def^{n}: Two integers a and b are said to be relatively Prime (co-prime) if gcd (a,b)=1
- Ex: 9 & 28 are relatively prime.

Euclidean Algorithm

- The Euclidean Algorithm is a method developed by the Greek mathematician Euclid that finds the greatest common divisor of two positive integers. We begin with two numbers, say a and b, where a is greater than b. We divide a by b and get remainder r. We then divide b by r, to get new remainder t. **We continue in this manner until the remainder is either one or zero.** If the remainder is one, then the two numbers are relatively prime, so their greatest common divisor is one. However, if the remainder is zero, the greatest common divisor would be the remainder before the zero.

Euclidean Algorithm

- Use to compute GCD
- Based on following theorem:
  gcd(a, b) = gcd (b, a mod b)
- Example: Find gcd(19,8)

$$19 = \underline{2} * 8 + 3$$

$$8 = \underline{2}*3 + 2$$ (take the remainder 3 and divide it into 8)

$$3 = \underline{1}* 2 + 1 \rightarrow \text{gcd}(19,8)$$

$$2= 2*1+0$$

Answer: gcd(19,8)=1

Example GCD of 2740 and 1760 ?

Extended Euclidean Algorithm

- If a and b are positive integers, then there are always integers m and n so that the gcd of a and b equals ma+nb.

$$\mathbf{ma + nb = gcd(a, b)}$$

The extended Euclidean algorithm can calculate the gcd (a, b) and at the same time calculate the value of m and n.

Extended Euclidean Algorithm

- If gcd(a,b)=1 this solves the problem of computing modular inverses.
- **Observation : The extended Euclidean algorithm gcd*(a, b)= ma+ nb is* particularly useful when a and b are coprime, since then m is the multiplicative inverse of a modulo b, and n is the multiplicative inverse of b modulo a.**

Extended Euclidean Algorithm

- Find the inverse of 8 mod 19:

  19 = <u>2</u> * 8 + 3

  8 = <u>2</u>*3 + 2 (take the remainder 3 and divide it into 8)

  3 = <u>1</u>* 2 + 1→ gcd(19,8)

  2= 2*1+0

- (Last non-zero remainder is gcd(19,8)). The quotients are underlined.
- Steps for finding inverse : Start this with two rows:

  1 0 and, underneath it, **0 1**

Extended Euclidean Algorithm

- **0   1** (multiply the second row by our first quotient, two, and subtract it from the previous row to get next row)
- **Next row: 1   -2** (multiply this by our second quotient, two, and subtract it from the previous row to get next row)
- **Next row: -2   5** (multiply this by our third quotient, one, and subtract it from the previous row to get next row)
- **Next row: 3 -7**, this means that
- $3 * 19 + (-7) * 8 = 1$
- We take this mod 19, to obtain 0 – 7 * 8 = 1. Thus, the inverse of 8 is (-7) mod 19 = 12

Extended Euclidean Algorithm

- Find the inverse of 20(mod 97).

Solution: 97= 20*<u>4</u>+17

20=17*<u>1</u>+3

17=3*<u>5</u>+2

3=2*<u>1</u>+**1**→gcd(97, 20)

2=2*1+0

Last non-zero remainder (i.e., 1) is the gcd(97,20). Quotients of each step are underlined.

Extended Euclidean Algorithm

- Compute inverse as

1	0
0	1
1	-4
-1	5
6	-29
-7	34

Hence,

$(-7) \times 97 + 34 \times 20 = 1$

- Since there are 4 steps (quotients),
- 3^{rd} row = 2^{nd} row × first quotient - 1^{st} row.
- 4^{th} row= 3^{rd} row × second quotient – 2^{nd} row.
- Similarly…..
- 6^{th} row= 5^{th} row × fourth quotient – 4^{th} row.