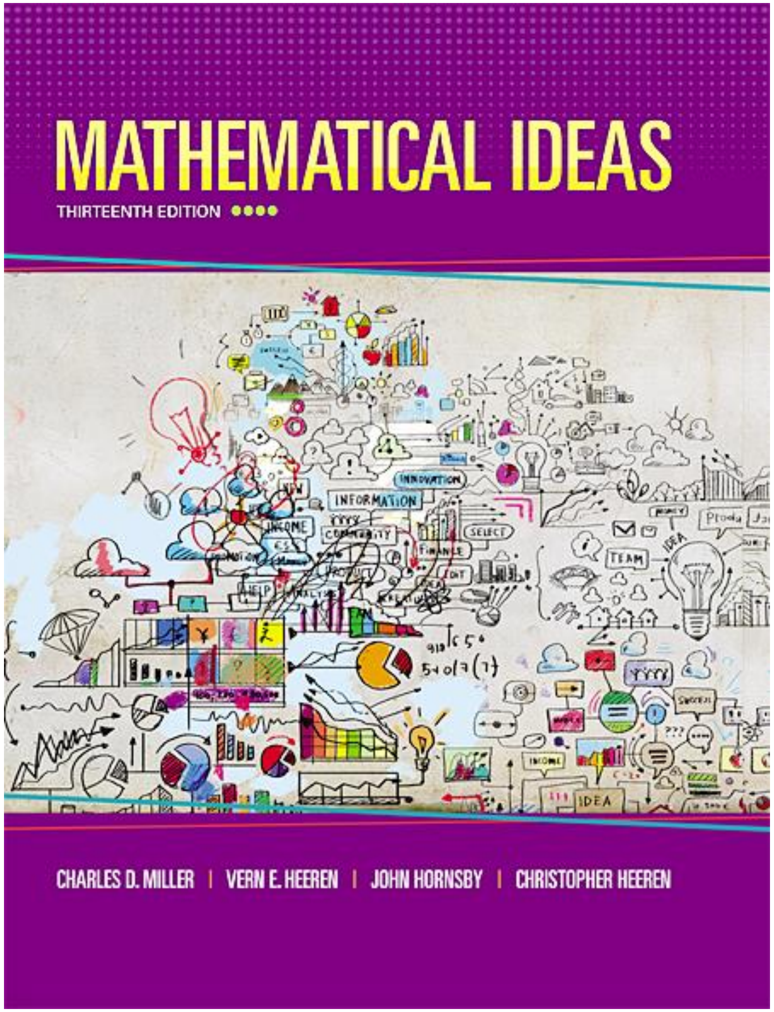
Chapter 10

Number Theory



Chapter 10: Number Theory

10.1 Prime and Composite Numbers

10.2 Selected Topics From Number Theory

10.3 Greatest Common Factor and Least Common Multiple

10.4 The Fibonacci Sequence and the Golden Ratio

10.X Modular Arithmetic and Cryptography

Section 10-Extension

Modular Arithmetic

&

Cryptography

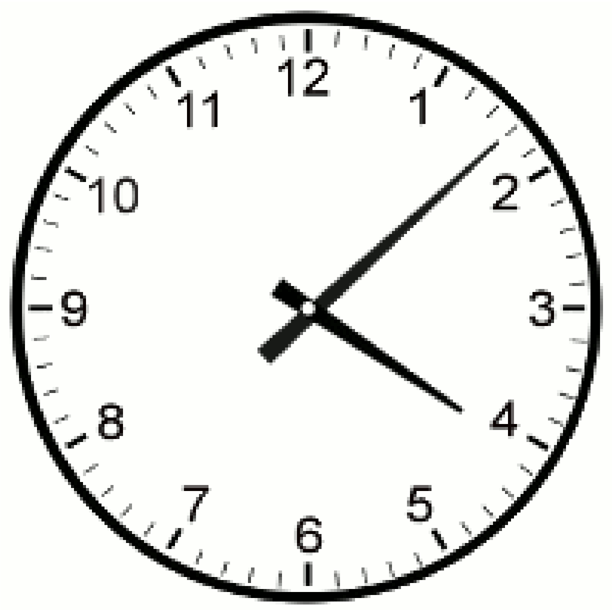
Objectives

- Clock Arithmetic
- Modular Systems
- Residues of Large Numbers
- Basics of Cryptography
- Key Exchange
- Public Key Cryptography

Clock Arithmetic

It’s 8 PM, what time will it be 33 hours from now?

One way to solve is to count using a clock. Set the hour hand to 8:00 and rotate the hour hand through 33 hours.



Clock Arithmetic

As we go through the hours we notice that we count through the set {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}.

NOTE: It is easier if we replace 12 with 0 and our set becomes {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}.

We can use a calculator to compute:

8+33=41 and 41/12 = 3.416666667

Clock Arithmetic

Since we don’t care about the number of revolutions (3) we then use 12*0.416666667 =5

Therefore 8+33=(3*12)+5 , but since 12=0

8+33=(3*0)+5=5

Thus we deal with the remainder when 8+33 or 41 is divided by 12.

Clock Arithmetic

Example: Using clock arithmetic, compute:

$$547 * 11873 = 649453$$

$$\frac{6494531}{12} = 12541210.9167$$

12*0.9167=11

Or

$$547 * 11873 = \left((12 * 45) + 7\right) * ((12 * 989) + 5)$$

$$(0 + 7) * (0 + 5) = 7 * 5 = 35 = 2 * 12 + 11\text{=11}$$

Modular Systems

True or False:

a) $16 \equiv 10 \bmod 2$ b) $49 \equiv 32 \bmod 5$ c) $30 \equiv 345 \bmod 7$

a) 16-10=6 is divisible by 2 so strictly this is a ***true*** statement.

b) 49-32=17 which is not divisible by 5 so this is a ***false*** statement.

c) 30-345=-315 which is divisible by 7.

Congruence Modulo *n*

$a \equiv b \pmod{n}$ if and only if the same remainder is obtained when a and b are divided by n

Residues of Large Numbers

The basic concern of a modular system is, given a number *n*, no matter how large *b* find *a* such that a is in the set {0, 1, 2, … ,n-1}. This number *a* is called the remainder or ***residue.***

Examples:

x=846238527 mod 23
*x=(23*36792979)+10*
x=10

Rule: **The residue of a product is the product of residues**

Example:

458687*931056 mod 18
(458687 mod 18)*(931056 mod 18)
11*6=66 mod 18 = 12

Basics of Cryptography

Cryptography involves secret codes, a way of disguising information such that only the sender and receiver know the information.

Basic Requirements of a Cryptography System:

- A *secret* algorithm for encrypting and decrpting data.
- A *secret* key that provides additional information for a receiver to decrypt.

Basics of Cryptography

Difficulty is that until the 1970's all encryption functions were two-way functions. An adversary could decrypt with the algorithm.

In the 1970's researchers discovered how to construct a one way function that overcame this problem. It is an *exponential function* given by:

$$C = M^k (mod\ n)$$

Where M and n are known to the parties and k computed.

Key Exchange

Alice's actions	Bob's Actions
1) Choose secret value of *a.*	1) Choose secret value of *b.*
2) Compute $\alpha = M^a (\text{mod } n)$	2) Compute $\beta = M^b$ (mod n)
3) Send the value of α to Bob.	3) Send the value of β to Alice
4) Receive β	4) Receive α
5) Compute the key: $K = \beta^a$ (mod n)	5) Compute the key: $K = \alpha^b$ (mod n)

Key Exchange

Alice and Bob will determine a key to encrypt and decrypt using the following procedure: (they agree M=7, n=13 note use of primes)

Alice's actions	Bob's Actions
1) Choose secret value of *a.* *(Alice selects 5)*	1) Choose secret value of *b.* *(Bob chooses 8)*
2) Compute $\alpha=M^a$ (mod n) 7^5(mod 13) 16807 mod 13 $\alpha=11$	2) Compute $\beta=M^b$ (mod n) 7^8 (mod 13) 5764801 (mod 13) $\beta=3$
3) Send the value of α to Bob.	3) Send the value of β to Alice
4) Receive β	4) Receive α
5) Compute the key: $K=\beta^a$ (mod n) $K=3^5$ mod 13 243 mod 13 9	5) Compute the key: $K=\alpha^b$ (mod n) $K=11^8$ mod 13 214358881 mod 13 9

Public Key Exchange (RSA Basics)

Alice (the receiver) completes the following steps:

1) Choose two prime numbers, p and q which are kept secret
2) Compute the modulus $n = p * q$
3) Compute $\ell=(p-1)(q-1)$
4) Chose e to be relatively prime between 1 and ℓ
5) Find the decryption exponent d such that

$$e*d=1 \text{ mod } (\text{mod } \ell)$$

6) Provide Bob with a public Key (n and e)

Public Key Exchange (RSA Basics)

Bob (the sender) completes the following to send Alice a secure message:

7) Convert the message to Alice into a number M (called a plaintext message)

8) Encrypt M using Alice's public key

$$C=M^e \ (mod\ n)$$

9) Transmit C to Alice

When Alice receives C, she completes the final step:

10) Decrypt C using the private key

$$M=C^d \ (mod\ n)$$

Public Key Exchange (Example)

Alice (the receiver) completes the following steps:

1) Choose two prime numbers, $p=7$ and $q=13$ which are secret
2) Compute the modulus $n = p * q = 7 * 13 = 91$
3) Compute $\ell=(p-1)(q-1)=(7 – 1)(13 – 1) = 72$
4) Chose $e=11$ to be relatively prime between 1 and ℓ
5) Find the decryption exponent d such that

$$11*d=1 \text{ mod } (\text{mod } 7)$$

$$d=59$$

6) Provide Bob with a public Key ($n=91$ and $e=11$, *p & q are secret*)

Public Key Exchange (Example)

Bob (the sender) completes the following to send Alice a secure message ("HI", H is letter 8 and I is letter 9) :

7) Convert the message to Alice into a number M ("HI" = 89)

8) Encrypt M using Alice's public key

$$C=M^{e} \pmod{n}$$

$$C=89^{11}$$

$$C=89^{1+2+8}$$

$$C=(89^{1} \bmod 91)(89^{2} \bmod 91)(89^{4} \bmod 91)$$

$$C=(89 \bmod 91)(7921 \bmod 91)(3.936588806E15 \bmod 91)$$

$$C=89*4*74 \bmod 91$$

$$C=26344 \bmod 91$$

$$C=45$$

9) Transmit C to Alice

Public Key Exchange (Example)

When Alice receives C, she completes the final step:

10) Decrypt C using the private key

$$M=C^{d}\ (mod\ n)$$
$$M=45^{59}\ mod\ 91$$
$$M=45^{1+2+8+16+32}\ mod\ 91$$
$$M=(45^{1}*45^{2}*45^{8}*45^{16}*45^{32})mod\ 91$$
$$M=45*23*16*74*16\ mod\ 91$$
$$M=19607040\ mod\ 91$$
$$M=89=\text{"HI" (our original message)}$$