Introduction to Cryptography

by

Dr. Deep Singh

Department of Mathematics,
Central University of Jammu, Jammu

Outline

- Introduction to Number Theory
- Classification of Numbers
- Various results
- Introduction to Cryptography
- Private key cryptosystems

What is Number Theory?

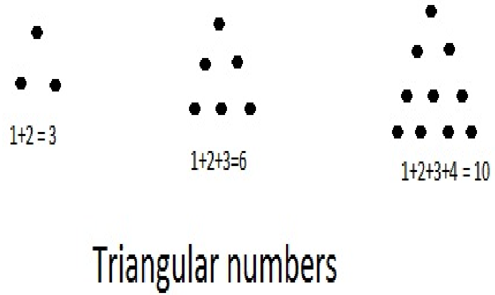
- Study of the behavior of positive integers $1, 2, 3, 4, 5, \ldots$ and their various combinations
- God made the numbers and rest all the work of man.

  \- L. Kronecker.
- Classification of natural numbers

odd	1, 3, 5, 7, 9, 11, ...
even	2, 4, 6, 8, 10, ...
square	1, 4, 9, 16, 25, 36, ...
cube	1, 8, 27, 64, 125, ...
prime	2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...
composite	4, 6, 8, 9, 10, 12, 14, 15, 16, ...
1 (modulo 4)	1, 5, 9, 13, 17, 21, 25, ...
3 (modulo 4)	3, 7, 11, 15, 19, 23, 27, ...
perfect	6, 28, 496, ...(sum of proper divisors = number)
triangular	1, 3, 6, 10, 15, 21, ...

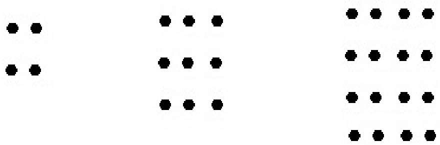
Triangular numbers

- can be arranged in the shape of triangles



Square numbers

- Square numbers are the numbers $1, 4, 9, 16, \ldots$ that can be arranged in the shape of square.



$2^2 = 4$ $3^2 = 9$ $4^2 = 16$

Square numbers

Obvious queries

- Can the sum of two squares be a square?
  Yes. (Pythagorean Triples)
  Examples: $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$ etc.
- Can the sum of two cubes be a cube ? Can the sum of two fourth powers be a fourth power ?
- In general, can the sum of two n^{th} powers be an n^{th} power?

- No.
- **Fermat's Last Theorem:** $a^n + b^n \neq c^n, \; n > 2$.
  After 358 years in 1994 Andrew Wiles has given the first successful proof of the problem and formally published in 1995.
- Proof is about 100 page long.

Ramanujan number

- A natural number that can be expressed as the sum of cubes of positive numbers in two different ways.
  Example: 1729 (Ramanujan number)
  $1729 = 1^3 + 12^3 = 9^3 + 10^3$
- Divisors of 1729 are
  1, 7, 13, 19, 91, 133, 247. (not a perfect number)

Taxicab numbers

- can be expressed as a sum of two positive cubes in n distinct ways.
- $T(1) = 2 = 1^3 + 1^3$
- $$\begin{aligned} T(2) = 1729 = & \ 1^3 + 12^3 \\ & \ 9^3 + 10^3 \end{aligned}$$
- $$\begin{aligned} T(3) = 87539319 = & \ 167^3 + 436^3 \\ & \ 228^3 + 423^3 \\ & \ 255^3 + 414^3 \end{aligned}$$
- $$\begin{aligned} T(4) = 6963472309248 = & \ 2421^3 + 19083^3 \\ & \ 5436^3 + 18948^3 \\ & \ 10200^3 + 18072^3 \\ & \ 13322^3 + 16630^3 \end{aligned}$$

- **Modular Arithmetic :** Let n be a $+$ve integer. Then any two integers a and b are said to be congruent modulo n i.e., $a \equiv b \mod n$ if $n/(a-b)$.

For Example;

1. $50 \equiv 14 \mod 12$
2. $2 \equiv -3 \mod 5$

Euclid's division algorithm

- For every integer m and $+$ve integer n, there exist unique integers q and r such that
  $m = nq + r$, $0 \leq r < n$. Further, $r = m \mod n$.

Example

compute $10 \mod 7$ and $-10 \mod 7$. What are q and r in each case? Does $(-m) \mod n = -(m \mod n)$?

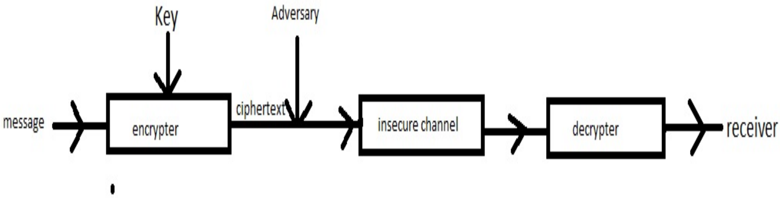
Cryptography

- Cryptography is a key technology in providing secure transmission of information.
- It is a branch of science which mainly deals with constructing and analyzing protocols which are related to various aspects of secure communication.
- Nowdays cryptography is at the heart of many techniques used for secure transfer of data,
- such as web based applications, online government services, online banking, mobile phones, wireless local area networks, ATM etc.

Cryptosystem

- Cryptography is associated with the security of the piece of the information being transmitted over the insecure channel.
- Cryptosystem is an algorithm required to implement special types of encryptions and decryptions.
- There are mainly two types of cryptosystems: symmetric key (private key) and asymmetric key (public key) cryptosystems.

Encryption and decryption process



The communication channel

Caesar Cipher (Private key cryptography)

- One can encrypt the original message by just shifting each symbol to some certain places.
- To encrypt the message symbols for n places, the encryption function is

$$E_n(x) = (x + n) \mod 26$$

Decryption function is

$$D_n(y = x + n) = (y - n) \mod 26$$

G UGJJ KCCR WMS YR KGBLGEFR

- A Caeser cipher is especially easy to implement on a computer using a scheme known as arithmetic mod 26.
- English alphabets and residue modulo 26

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

- Numbers corresponds to alphabets

G	U	G	J	J	K	C	C	R	W	M	S	Y	R
6	20	6	9	9	10	2	2	17	22	12	18	24	17

K	G	B	L	G	E	F	R
10	6	1	11	6	4	5	17

guess

G can corresponds to I or A only

$\Rightarrow$ Key = 2 or 20

- Right shift by 2 (Key $= 2$)

8	22	8	11	11	12	4	4	19	24	14	20	26	19
I	W	I	L	L	M	E	E	T	Y	O	U	A	T

12	8	3	13	8	6	7	19
M	I	D	N	I	G	H	T

I WILL MEET YOU AT MIDNIGHT

BQXOSNFQZOGX LDZMR GHCCDM VQJSHMF

- Right shift by 1 (Key $= 1$)

CRYPTOGRAPHY MEANS HIDDEN WRITING

QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

- Right shift by 3 (Key $= 3$)

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Refrences

- Hoffstein J., Pipher J., Silverman J. H.: An Introduction to Mathematical cryptography. Springer 2008.
- Moon T. K., Error Correction Coding: Mathematical methods and Algorithms, John wiley & Sons 2009.
- Stinson D. R.: Cryptography Theory and Practice, Chapman & Hall/CRC, Taylor & Francis Group 2006.
- Shannon C., Communication theory of secrecy systems, Bell System Technical Journal Vol.28, pp. 656-715, 1949.

Thank You