Lecture-1

Introduction to Cryptography and Classical Ciphers

Chapter 1

1.1 Introduction:

In today's digital age the topmost priority of a human being is to communicate securely. But it is not easy to have secure communication over any channel. It has been always a topic of interest "how to communicate securely". In past, people used to communicate through handwritten letters, and letters were sent via hands. It was a tough challenge to maintain the secrecy of information. For secure communication, they were use riddles, puzzles, some special characters in place of the original message such a way that only the receiver could decode.
The practice and study of hiding information is known as Cryptography. Cryptography is a Mathematical science that comes up with a way for secure communication between two or more parties by converting the confidential information into a scrambled form so that only authorized users can remove scrambles and read information. For instance a sender Alice wants to send secret information to a receiver Bob over an insecure communication channel i.e via the internet or telephone. Then it is possible that Eavesdropper can intercept and read the information.

1.2 Security Services of Cryptography

The main goal of cryptography is to provide the following four fundamental information security services.

- **Confidentiality:** Confidentiality is the fundamental security service provided by cryptography. Confidentiality means protecting information from unauthorized users. It provides a surety to a user that his

information is not to be shared with anyone. It is sometimes referred to as privacy or secrecy.

- **Data Integrity:** It deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidentally. Data integrity cannot prevent the alteration of data, but provides a means for detecting whether data has been manipulated.

- **Authentication:** Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender. Apart from the originator, authentication may also provide assurance about other parameters related to data such as the date and time of creation/transmission.

- **Non-repudiation:** It ensures that an entity cannot refuse the ownership of a previous commitment or an action. Non-repudiation is a property that is most desirable in situations where there are chances of a dispute over the exchange of data.

1.3 Basic Terminology:

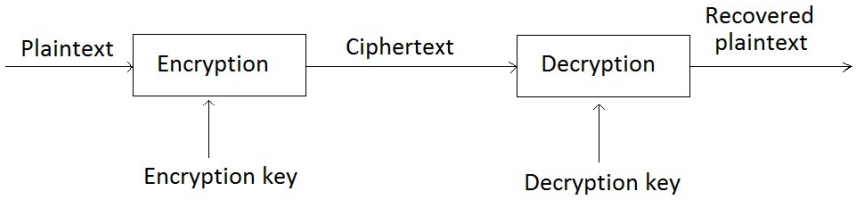


Figure 1.1: Block-diagram

- **Plaintext ($\mathcal{P}$):** It is the message to be protected during transmission.

- **Ciphertext ($\mathcal{C}$):** It is the scrambled version of the plaintext produced by the encryption.
- **Encryption ($\mathcal{E}$):** It is a process of converting plain text to cipher text i.e.

$$\begin{aligned}\mathcal{E} :&\mathcal{P} \mapsto \mathcal{C}\\ &m \mapsto \mathcal{E}(m) = c\end{aligned}$$

- **Decryption ($\mathcal{D}$):** It is a process of reconverting cipher text to plain text i.e.

$$\begin{aligned}\mathcal{D} :&\mathcal{C} \mapsto \mathcal{P}\\ &c \mapsto \mathcal{D}(c) = m\end{aligned}$$

- **Encryption Key:** It is a value that is known to the sender and used for encryption.
- **Decryption Key:** It is a value that is known to the receiver and used for decryption.
- **Cryptanalysis:** It is the study of deciphering ciphertext without knowing key.

Note:- The plaintext and ciphertext are written in some symbols (usually, but not always, they are written in the same symbols) consisting of a certain number n of letters. The term "letter" (or "character") can refer not only to the familiar A-Z, but also to numerals, blanks, punctuation marks, or any other symbols that we allow ourselves to use when writing the messages.

Let Plain text space is $\mathcal{P} = \{A, B, \ldots, Z\}$ and Cipher text space is $\mathcal{C} = \{A, B, \ldots, Z\}$.
Then Encryption function is defined by

$$\mathcal{E} : \mathcal{P} \to \mathcal{C}$$

And Decryption function is defined by

$$\mathcal{D} : \mathcal{C} \to \mathcal{P}$$

Such that

$$\mathcal{D}\mathcal{E} = \mathcal{E}\mathcal{D} = I$$

$\mathcal{E}_0$:	A	B	C	...	X	Y	Z	(No shift)
$\mathcal{E}_1$:	B	C	D	...	Y	Z	A	(Shift by 1)
$\mathcal{E}_2$:	C	D	E	...	Z	A	B	(Shift by 2)
$\mathcal{E}_3$:	D	E	F	...	A	B	C	(Shift by 3)

$\mathcal{D}_0$:	A	B	C	...	X	Y	Z
$\mathcal{D}_1$:	Z	A	B	...	W	X	Y
$\mathcal{D}_2$:	Y	Z	A	...	V	W	X
$\mathcal{D}_3$:	X	Y	Z	...	U	V	W

Decrypt "RK!LZLVKLNQRZ"

$\mathcal{D}_1$(RK)=QJ (make no sense i.e no english word)

$\mathcal{D}_2$(RK)=PI (possibility of english words like PIN,PING etc)

$\mathcal{D}_2$(LZL)=JXJ

Combining two decryptions we have "PI JXJ" (make no sense i.e no english word)

$\mathcal{D}_3$(RK)=OH (make sense)

$\mathcal{D}_3$(LZL)=IWI (make sense i.e OH I WI)

$\mathcal{D}_3$(VKL)=SHI (make sense i.e OH I WISH I)

$\mathcal{D}_3$(NQHZ)=KNOW (make sense)

So Cipher text is decrypted by $\mathcal{D}_3$ and decrypted message is "OH! I WISH I KNOW".

Numerical equivalent of Symbols (Alphabets, other text symbols):- To perform mathematical operations on plain texts and cipher texts we need some numeric value corresponding to alphabets.

- **Monograph:** Monograph means single symbol at a time for encryption and decryption.
  Numerical equivalent of monographs (Single symbol):

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	26	27

  i.e $\{A,B,\ldots,Y,Z,?,!,\ldots\hat{b}\}=\{0,1,\ldots,24,25,\ldots,n\text{-}1\}$ for n symbols and mathematical operations are same as $\mathbb{Z}_n$ with addition and multiplication modulo n(=no of symbols).

- **Digraphs:** Digraphs means two symbols at a time for encryption and decryption. There is two ways for numerical equivalent of digraphs:

1. Numerical equivalent of symbols are as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
00	01	02	03	04	05	06	07	08	09	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	26	27

Numerical equivalent of digraph XY is equal to
XY= Numerical equivalent of X.Numerical equivalent of Y (each having two digits).
e.g. NO=1314, AN=0013, NI=1308 O!=1427 etc.

2. Numerical equivalent of digraphs XY to base n can be written as

$$XY = n \times N(X) + N(Y)$$

N(X)= Numerical equivalent to X
N(Y)= Numerical equivalent to Y

E.g. AN=$0 \times n + 13$
NO=$13 \times n + 14$
O!= $14 \times n + 27$

In particular, let english alphabets be set of symbols (n=26) then we have
AN=A$\times$26+N=$0 \times 26 + 13$
NO=$13 \times 26 + 14$
NI= $13 \times 26 + 8$

- Similarly for trigraphs (3 alphabets at a time for encryption and decryption)

$$XYZ = n^2 \times N(X) + n \times N(Y) + N(Z)$$

Remark: In general, we can label blocks of k letters in an N-letter alphabet by integers between 0 and $N^k - 1$ by regarding each such block as a k-digit integer to the base N.

Assumption(Kirchoff's law):- The attacker knows all the details(of the cryptosystem) except the keys (excepts) the cryptosystem is still secure.
No cryptosystem is secure only time matters.

1.4 Classical Cipher:

Classical ciphers are ciphers that were used upto 1970s that is in the pre computer era. But since then thay have fallen out of use. This is due to the fact that most of them can be solved by hand or using modern cryptographic algorithms.
There are two type of classical ciphers.

Substitution Cipher: In substitution ciphers each symbol of the plaintext message is substituted by other symbol in a systematic form. Substitution of symbols can be done mono alphabetically or poly alphabetically.

Transposition cipher: In transposition cipher symbols of the plaintext message remain same but ordering of these symbols are changed in a specific form.

1.5 Substitution Ciphers

1.5.1 Shift Cipher:

Suppose we are using an n-letter symbols(alphabets) with numerical equivalents $0, 1, ..., n-1$, i.e. $|\mathcal{P}| = n$. Let b be a fixed integer with $0 \leq b \leq n-1$. In shift cipher we do encryption by shift transformation.

- **Encryption:** The encryption function is defined by

$$\mathcal{E} : \mathcal{P} \to \mathcal{C}$$
$$m \mapsto c = \mathcal{E}(m) \equiv m + b \pmod{n}$$

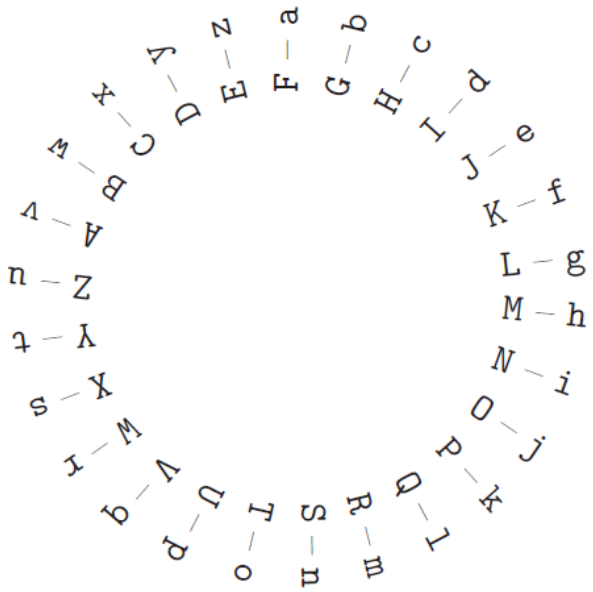


Figure 1.2: Cyclic Shift by 5 latter

where 'm' is numerical equivalent of symbol (alphabet) to be encrypted.

- **Decryption:** The decryption function is defined by

$$\mathcal{D}\colon \mathcal{C} \to \mathcal{P}$$
$$c \mapsto m = \mathcal{D}(c) \equiv c - b \pmod{n}$$

Note1: Here, $\mathcal{P}$ and $\mathcal{C}$ are equivalent to $\mathbb{Z}_n$.

Note2: In particular, when $b = 3$ shift cipher is known as **Caesar cipher**.

Example:

Let $\mathcal{P}$={A=0,B=1,...,Y=24,Z=25} be set of symbols (alphabets), then encryption function is given by
Encryption: Let $b = 2$

$$\mathcal{E}\colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$m \mapsto c = \mathcal{E}(m) \equiv m + 2 \pmod{26}$$

To encrypt "HELLO"

$$\begin{aligned}
&\mathcal{E}(m_1 = H) = \mathcal{E}(7) = 7 + 2 \equiv 9 \pmod{26} = \mathbf{J}\\
&\mathcal{E}(m_2 = E) = \mathcal{E}(4) = 4 + 2 \equiv 6 \pmod{26} = \mathbf{G}\\
&\mathcal{E}(m_3 = L) = \mathcal{E}(11) = 11 + 2 \equiv 13 \pmod{26} = \mathbf{N}\\
&\mathcal{E}(m_4 = L) = \mathcal{E}(11) = 11 + 2 \equiv 13 \pmod{26} = \mathbf{N}\\
&\mathcal{E}(m_5 = O) = \mathcal{E}(14) = 14 + 2 \equiv 16 \pmod{26} = \mathbf{Q}
\end{aligned}$$

So encryption of 'HELLO' is 'JGNNQ'.

Decryption: Decryption function is given by

$$\begin{aligned}
\mathcal{D}\colon &\mathbb{Z}_{26} \to \mathbb{Z}_{26}\\
&c \mapsto m = \mathcal{D}(c) \equiv c - 2 \pmod{26}
\end{aligned}$$

To decrypt "JGNNQ"

$$\begin{aligned}
&\mathcal{D}(C_1 = J) = \mathcal{D}(9) = 9 - 2 \equiv 7 \pmod{26} = \mathbf{H}\\
&\mathcal{D}(C_2 = G) = \mathcal{D}(6) = 6 - 2 \equiv 4 \pmod{26} = \mathbf{E}\\
&\mathcal{D}(C_3 = N) = \mathcal{D}(13) = 13 - 2 \equiv 11 \pmod{26} = \mathbf{L}\\
&\mathcal{D}(C_4 = N) = \mathcal{D}(13) = 13 - 2 \equiv 11 \pmod{26} = \mathbf{L}\\
&\mathcal{D}(C_5 = Q) = \mathcal{D}(16) = 16 - 2 \equiv 14 \pmod{26} = \mathbf{O}
\end{aligned}$$

So decryption of 'JGNNQ' is 'HELLO'.

1.5.2 Hill Cipher:

Let $\mathcal{P}$ and $\mathcal{C}$ be a plain text space and cipher text space on $\mathbb{Z}_n$.

- **Encryption:** The encryption function is defined by

$$\begin{aligned}
\mathcal{E}\colon &\mathbb{Z}_n \to \mathbb{Z}_n\\
&m \mapsto \mathcal{E}(m) = c \equiv am \pmod{n}
\end{aligned}$$

  where $a \in \mathbb{Z}_n$ is a fixed integer.

- **Decryption:** The decryption function is defined by

$$\begin{aligned}\mathcal{D} :&\mathbb{Z}_n \to \mathbb{Z}_n \\ &c \mapsto \mathcal{D}(c) \equiv a^{-1}c \pmod{n}\end{aligned}$$

(Provided a^{-1} exist) it exist when $(a, n) = 1$ and can be computed by Euclidean algorithm.

Example:

Let $\mathcal{P} = \{A, B, \ldots, Z, \}$ and $n = 26$
Plain text- "SPARKY"

Encryption: Let $a = 3$

$$\mathcal{E}(m) = c \equiv 3m \pmod{26}$$

$$\begin{aligned}\mathcal{E}(S) = \mathcal{E}(18) &\equiv 3 \cdot 18 \pmod{26} = 2 = \mathbf{C} \\ \mathcal{E}(P) = \mathcal{E}(15) &\equiv 3 \cdot 15 \pmod{26} = 9 = \mathbf{J} \\ \mathcal{E}(A) = \mathcal{E}(0) &\equiv 3 \cdot 0 \pmod{26} = 0 = \mathbf{A} \\ \mathcal{E}(R) = \mathcal{E}(17) &\equiv 3 \cdot 17 \pmod{26} = 25 = \mathbf{Z} \\ \mathcal{E}(K) = \mathcal{E}(10) &\equiv 3 \cdot 10 \pmod{26} = 4 = \mathbf{E} \\ \mathcal{E}(Y) = \mathcal{E}(24) &\equiv 3 \cdot 24 \pmod{26} = 20 = \mathbf{U}\end{aligned}$$

Encrypted message is "CJAZEU"

Decryption:

$$\mathcal{D}(c) \equiv 3^{-1}c \pmod{26}$$

Since $(3, 26) = 1$, hence 3^{-1} exist in $mod\ \ 26$. By Euclidean algorithm we can find inverse of 3 in $mod\ \ 26$.

i.e $3^{-1} \equiv 9 \pmod{26}$

$$\begin{aligned}
\mathcal{D}(C) = \mathcal{D}(2) &\equiv 9 \cdot 2 \pmod{26} = 18 = \mathbf{S} \\
\mathcal{D}(J) = \mathcal{D}(9) &\equiv 9 \cdot 9 \pmod{26} = 15 = \mathbf{P} \\
\mathcal{D}(A) = \mathcal{D}(0) &\equiv 9 \cdot 0 \pmod{26} = 0 = \mathbf{A} \\
\mathcal{D}(Z) = \mathcal{D}(25) &\equiv 9 \cdot 25 \pmod{26} = 17 = \mathbf{R} \\
\mathcal{D}(E) = \mathcal{D}(4) &\equiv 9 \cdot 4 \pmod{26} = 10 = \mathbf{K} \\
\mathcal{D}(U) = \mathcal{D}(20) &\equiv 9 \cdot 20 \pmod{26} = 24 = \mathbf{Y}
\end{aligned}$$

Decrypted message is "SPARKY"

1.5.3 Affine Cipher: (Shift as well as multiplication)

Let $\mathcal{P}$ and $\mathcal{C}$ be a plain text space and cipher text space on $\mathbb{Z}_n$.

- **Encryption:** The encryption function is defined by

$$\begin{aligned}
\mathcal{E} :&\mathbb{Z}_n \to \mathbb{Z}_n \\
&m \mapsto \mathcal{E}(m) = c \equiv am + b \pmod{n}
\end{aligned}$$

  where $a, b \in \mathbb{Z}_n$ are fixed integer.

- **Decryption:** The decryption function is defined by

$$\begin{aligned}
\mathcal{D} :&\mathbb{Z}_n \to \mathbb{Z}_n \\
&c \mapsto \mathcal{D}(c) \equiv a'c + b' \pmod{n}
\end{aligned}$$

  where $a' \equiv a^{-1} \pmod{n}$ and $b' \equiv -a^{-1}b \pmod{n}$ (Provided a^{-1} exist)

$$\begin{aligned}
c - b = am &\implies a^{-1}(c - b) = m \\
&\implies a^{-1}c - a^{-1}b = m \\
&\implies a'c + b' = m = \mathcal{D}(c)
\end{aligned}$$

Example:

Let $\mathcal{P} = \{A, B, \ldots, Z, \_\}$ and $n = 27$
Plain text- "HELP ME".

Encryption: Let $a = 13, b = 9$

$$\mathcal{E}(m) = c \equiv 13m + 7 \pmod{27}$$

$$\begin{aligned}
\mathcal{E}(H) = \mathcal{E}(7) &\equiv 13 \cdot 7 + 7 \pmod{27} = 17 = \mathbf{R} \\
\mathcal{E}(E) = \mathcal{E}(4) &\equiv 13 \cdot 4 + 7 \pmod{27} = 5 = \mathbf{F} \\
\mathcal{E}(L) = \mathcal{E}(11) &\equiv 13 \cdot 11 + 7 \pmod{27} = 15 = \mathbf{P} \\
\mathcal{E}(P) = \mathcal{E}(15) &\equiv 13 \cdot 15 + 7 \pmod{27} = 13 = \mathbf{N} \\
\mathcal{E}(_) = \mathcal{E}(26) &\equiv 13 \cdot 26 + 7 \pmod{27} = 21 = \mathbf{V} \\
\mathcal{E}(M) = \mathcal{E}(12) &\equiv 13 \cdot 12 + 7 \pmod{27} = 1 = \mathbf{B}
\end{aligned}$$

Encrypted message is "RFPNVBF"

Decryption:

$$\mathcal{D}(c) = \equiv a'c + b' \pmod{27}$$

where $a' \equiv 13^{-1} \pmod{27}$ and $b' \equiv -13^{-1}7 \pmod{27}$
Since $(13, 27) = 1$, hence 13^{-1} exist in $mod\ 27$. By using Euclidean algorithm we can find inverse of 13 in $mod\ 27$.
Hence $a' \equiv 25 \pmod{27}$ and $b' \equiv -25 \cdot 7 \pmod{27} \equiv 14 \pmod{27}$

$$\begin{aligned}
\mathcal{D}(R) = \mathcal{D}(17) &\equiv 25 \cdot 17 + 14 \pmod{27} = 7 = \mathbf{H} \\
\mathcal{D}(F) = \mathcal{D}(5) &\equiv 25 \cdot 5 + 14 \pmod{27} = 4 = \mathbf{E} \\
\mathcal{D}(P) = \mathcal{D}(15) &\equiv 25 \cdot 15 + 14 \pmod{27} = 11 = \mathbf{L} \\
\mathcal{D}(N) = \mathcal{D}(13) &\equiv 25 \cdot 13 + 14 \pmod{27} = 15 = \mathbf{p} \\
\mathcal{D}(V) = \mathcal{D}(21) &\equiv 25 \cdot 21 + 14 \pmod{27} = 26 = _ \\
\mathcal{D}(B) = \mathcal{D}(1) &\equiv 25 \cdot 1 + 14 \pmod{27} = 12 = \mathbf{M}
\end{aligned}$$

Decrypted message is "HELP ME"

Activity: Read a 500 words article in English. Count how many times each English alphabet letter appears in that article.

Lecture-2

Frequency Analysis and Vigenère Cipher

Practically, Code breakers always try their best to break cipher text with their best strategy. So encrypted text is secure only when it is secure from best known methods presently. As new improved methods are developed, the old encryption system can be less secure only, never become better .
In previous lecture we have studied about monoalphabetic substitution ciphers which are not more secure. In monoalphabetic cipher, each symbol is replaced by a unique symbol every time on encryption due to this fact we can apply frequency analysis to break such ciphers. In this lecture we will discuss cryptanalysis of some ciphers.

1 Frequency Analysis

From the activity given in last lecture, you would have observed that the letter **q** is always followed by letter **u**. The fact is that many letters appear, such as **e**, **t** and **a**, more frequently than others letters such as **f**, **h**, and **z**. Here we have frequency analysis of english alphabets:

By decreasing frequency			
E	13.11%	M	2.54%
T	10.47%	U	2.46%
A	8.15%	G	1.99%
O	8.00 %	Y	1.98%
N	7.10%	P	1.98%
R	6.83%	W	1.54%
I	6.35%	B	1.44%
S	6.10%	V	0.92%
H	5.26%	K	0.42%
D	3.79%	X	0.17%
L	3.39%	J	0.13%
F	2.92%	Q	0.12%
C	2.76%	Z	0.08%

Table 1: Frequency Analysis of English Alphabets

Example: Decrypt the following cipher text over the set of symbols $\mathcal{A}$={A=0,B=1,. . . ,Y=24,Z=25} , $|\mathcal{A}| = 26$ decrypted by substitution cipher.

DGMNM XNM TXUQ ODEUDO RU DGRO AWXOO MXAG ODEUD FUYJO GRO UXTM MZMNQYUM GXZM DGNMM HMU

First we observe frequency of letters in cipher text

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Count	2	0	0	7	2	0	6	1	0	1	0	0	12

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Count	4	8	0	2	3	0	2	7	0	1	6	2	2

(Verify !)

• M is most frequent and appears 12 times in cipher text, So M corresponds to E.
• O is second most frequent and appears 8 times in cipher text, So O corresponds to T.
• D, U appears 7 times each in cipher text, So D, U corresponds to A or O, first we take D corresponds to A and U corresponds to O.
• G, X appears 6 times each in cipher text, So G, X corresponds to R or N, first we take G corresponds to R and X corresponds to N.

i.e $\mathcal{D}$(M)=E, $\mathcal{D}$(O)=T, $\mathcal{D}$(D)=A, $\mathcal{D}$(U)=O, $\mathcal{D}$(X)=N, $\mathcal{D}$(G)=R and so on.

Cipher text	DGMNM	XNM	TXUQ	ODEUDO	RU	DGRO	AWXOO	MXAG
Plain text	ARE-E	N-E	-NO-	TA–AT	-O	AR-T	–NTT	EN-R

Obtained plain text is not meaningful.

So we will change the decrytions to nearby frequencies like $\mathcal{D}$(D)=T,$\mathcal{D}$(X)=A.

We have decryptions:

$\mathcal{D}$(M)=E, $\mathcal{D}$(O)=S, $\mathcal{D}$(D)=T, $\mathcal{D}$(U)=N, $\mathcal{D}$(X)=A, $\mathcal{D}$(G)=H $\mathcal{D}$(N)=R,$\mathcal{D}$(R)=I,$\mathcal{D}$(N)=R
$\mathcal{D}$(M)=U, $\mathcal{D}$(Q)=Y,$\mathcal{D}$(A)=C,$\mathcal{D}$(W)=L and so on.

Cipher text	DGMNM	XNM	TXUQ	ODEUDO	RU	DGRO	AWXOO	MXAG
Plain text	THERE	ARE	MANY	STUDENTS	IN	THIS	CLASS	EACH

In the same way, we can decrypt remaining cipher text.

Frequency Analysis attack: When attacker (unauthorized person) decrypt the cipher text using frequency analysis of symbols, called frequency analysis attack.

Note 1. In practice we do frequency analysis over large text for accuracy. In above example we have taken very small text (70 words only).

Similarly frequency analysis of digraphs and trigraphs over English alphabets are:
Decreasing order of digraphs

Order	Digraph	Order	Digraph
1	TH	20	HI
2	HE	21	IS
3	IN	22	OR
4	ER	23	TI
5	AN	24	AS
6	RE	25	TE
7	ND	26	ET
8	AT	27	NG
9	ON	28	OF
10	NT	29	AL
11	HA	30	DE
12	ES	31	SE
13	ST	32	LE
14	EN	33	SA
15	ED	34	SI
16	TO	35	AR
17	IT	36	VE
18	OU	37	RA
19	EA	38	LD

Order	Trigraph	Order	Trigraph
1	THE	16	ATI
2	AND	17	HAT
3	ING	18	ATE
4	ENT	19	ALL
5	ION	20	ETH
6	HER	21	HES
7	FOR	22	VER
8	THA	23	HIS
9	NTH	24	OFT
10	INT	25	ITH
11	ERE	26	FTH
12	TIO	27	STH
13	TER	28	OTH
14	EST	29	RES
15	ERS	30	ONT

2 Vigenère cipher

Vigenère Cipher is a polyalphabetic cipher. It is named after Blaise de Vigenere (1523–1596), whose 1586 book *Traicte des Chiffres* describes the known ciphers of his time.
In Vigenère cipher, encryption of different symbols is done by different shift ciphers. To decide how far to shift each symbol, sender (Bob) and receiver

(Alice) share on a common keyword (common knowledge).
Now, Bob wants to send a secret message to Alice. Bob will divide the plain text (message) into blocks of length l (l=length of the keyword). Then Bob will shift the symbols of each block corresponding to the keyword, i.e., Bob will shift the first symbols of the block by the first symbol of the keyword, the second symbol of the block by the second symbol of keyword, and so on, Bob will do this for each block to encrypt the whole message.
To decrypt the ciphertext, Alice will divide ciphertext into the blocks of length l, (l=length of the keyword). After that, Alice will perform a backward shift of each cipher symbol of each block corresponding to the keyword, i.e., first cipher symbols backward shift by the first symbol of keyword, second cipher symbols backward shift by the second symbol of keyword, and so on, to get the plaintext.

To understand above process of encryption and decryption,
suppose keyword

$$K = k_1k_2k_3 \dots k_l, \quad k_i \in \mathbb{Z}_n$$

message block is therefore

$$x = x_1x_2 \dots x_l, \quad x_i \in \mathbb{Z}_n$$

then encryption function is given by

$$\mathcal{E}(x) = y = y_1y_2 \dots y_l \quad \text{where} \quad y_i \equiv x_i + k_i \pmod{n}$$

decryption funtion is given by

$$\mathcal{D}(y) = x = x_1x_2 \dots x_l \ \text{ such that } \ x_i \equiv y_i - k_i \pmod{n}$$

where $n = |\mathcal{A}|$=number of symbols written in their numerical equivalent.

We can treat

$$x = (x_1, x_2, \dots, x_l) \in \underbrace{\mathbb{Z}_n \times \mathbb{Z}_n \times \cdots \mathbb{Z}_n}_{l \text{ times}} = \mathbb{Z}_n^l$$

Now consider plaintext space $\mathcal{P} = \mathbb{Z}_n^l$ and cipher text space $\mathcal{C} = \mathbb{Z}_n^l$ Then encryption is defined as

$$\mathcal{E} : \mathcal{P} \to \mathcal{C}$$

$$\mathcal{E}(x) = y = (y_1, y_2, \dots, y_l) \text{ where each } y_i \in \mathbb{Z}_n$$

Example: Let $\mathcal{A}$={A=0,B=1,... Y=24,Z=25,?=26} i.e $|\mathcal{A}| = 27$
Encrypt the following plain text with keyword "EGYPT"

"HELLO HOW ARE YOU?"

Solution:
Keyword: EGYPT, Keylength=5
Encrypt: HELLO HOW ARE YOU?
First divide the message into blocks of length 5 i.e.

b_1=HELLO b_2=HOWAR b_3=EYOU?

Encryption of block b_1=HELLO=$x = x_1x_2x_3x_4x_5 = [7\ 4\ 11\ 11\ 14]$

K=EGYPT=$k_1k_2k_3k_4k_5 = [4\ 6\ 24\ 15\ 19]$

$\mathcal{E}(x) = y = y_1y_2y_3y_4y_5$ where $y_i \equiv x_i + k_i \pmod{27}$

$$\begin{aligned}
y_1 &= x_1 + k_1 = 7 + 4 \equiv 11 \pmod{27} \\
y_2 &= x_2 + k_2 = 4 + 6 \equiv 10 \pmod{27} \\
y_3 &= x_3 + k_3 = 11 + 24 = 35 \equiv 8 \pmod{27} \\
y_4 &= x_4 + k_4 = 11 + 15 \equiv 26 \pmod{27} \\
y_5 &= x_5 + k_5 = 14 + 19 = 33 \equiv 6 \pmod{27}
\end{aligned}$$

$\mathcal{E}(x) = y = y_1y_2y_3y_4y_5$=[11 10 8 26 6]=LKI?G
So encryption of 'HELLO' is LKI?G

Similarly for block b_2=HOWAR=[7 14 22 0 17] =$x = x_1x_2x_3x_4x_5$
$\mathcal{E}(x) = y = y_1y_2y_3y_4y_5$ where $y_i \equiv x_i + k_i \pmod{27}$

$$\begin{aligned}
y_1 &= x_1 + k_1 = 7 + 4 \equiv 11 \pmod{27} \\
y_2 &= x_2 + k_2 = 14 + 6 \equiv 20 \pmod{27} \\
y_3 &= x_3 + k_3 = 22 + 24 = 46 \equiv 19 \pmod{27} \\
y_4 &= x_4 + k_4 = 0 + 15 \equiv 15 \pmod{27} \\
y_5 &= x_5 + k_5 = 17 + 19 = 33 \equiv 9 \pmod{27}
\end{aligned}$$

$\mathcal{E}(x) = y = y_1y_2y_3y_4y_5$=[11 20 19 15 9]=LUTPJ
So encryption of 'HOWAR' is LUTPJ.

Similarly do for block block b_3.

Decryption: y=LKI?G=$y_1y_2y_3y_4y_5$=[11 10 8 26 6]
$\mathcal{D}$(y)=x=$x_1x_2x_3x_4x_5$ such that $x_i \equiv y_i - k_i \pmod{27}$

$$
\begin{aligned}
x_1 &= y_1 - k_1 = 11 - 4 \equiv 7 \pmod{27} \\
x_2 &= y_2 - k_2 = 10 - 6 \equiv 4 \pmod{27} \\
x_3 &= y_3 - k_3 = 8 - 24 = -16 \equiv 11 \pmod{27} \\
x_4 &= y_4 - k_4 = 26 - 15 \equiv 11 \pmod{27} \\
x_5 &= y_5 - k_5 = 6 - 19 = -13 \equiv 14 \pmod{27}
\end{aligned}
$$

$\mathcal{D}$(y)=x=[7 4 11 11 14]=HELLO
So decryption of 'LKI?G' is 'HELLO'.
In the same way we can decrypt any Vigenère ciphers when keyword is known.

Autokey Cipher: Autokey cipher is similar to Vigenèner cipher. For encryption, shift few letters with the help of keyword after that shift the remaining plaintext by plaintext itself, that is key=keyword+plaintext.

Example: Encryption of "DO NOT WASTE THE TIME"
by keyword "CAT"

Plain Text:	D O N O T W A S T E T H E T I M E
Key:	C A T D O N O T W A S T E T H E T
Cipher Text:	F O G R H J O L P E L A I M P Q X

3 Techniques of decrypting Vigenère Cipher

- **When key length l is known**

Suppose the key length of the chosen keyword is l. Then lines up all ciphertext in l columns. So one can consider that 1st column is shifted by the first symbol of the keyword and 2nd column is shifted by 2nd symbol of the keyword and so on. That is each column can be seen as a monoalphabetic substitution cipher. Therefore, for each column, we can use frequency

analysis to guess the plaintext.

$$\begin{array}{lcccc} C_1 & = & y_1^1 & y_2^1 & \dots & y_l^1 \\ C_2 & = & y_1^2 & y_2^2 & \dots & y_l^2 \\ C_3 & = & y_1^3 & y_2^3 & \dots & y_l^3 \\ \vdots & & & & & \\ C_m & = & y_1^m & y_2^m & \dots & y_l^m \end{array}$$

Hence we can write

$$(y_1^1, y_1^2, y_1^3, \dots, y_1^m)(y_2^1, y_2^2, y_2^3, \dots, y_2^m) \dots (y_l^1, y_l^2, y_l^3, \dots y_l^m)$$

We now do the frequency analysis on each subset and get the plaintext.

Example: Decrypt the following ciphertext using Vigenère Cipher for keylength $l = 7$.

XHUEHXZHRIUHTIHGEUZSWEIATUMEZXHTVYXAAHKJLNX ECSBMIXONQDPVWKEKAIEEMGJAIELIMRVAVKWAPKGIXET GZEGHWIVPZVWIVGSSGFINVHLVETKVRXBZEUHRZGHIXPH LTPTJLOEHALGKKVTRDURMCEWTQDSIDAIVOZZKXUG

Step-1: At first divide ciphertext into blocks of length 7 i.e

XHUEHXZ HRIUHTI HGEUZSW EIATUME ZXHTVYX AAHKJLN XECSBMI XONQDPV WKEKAIE EMGJAIE LIMRVAV KWAPKGI XETGZEG HWIVPZV WIVGSSG FINVLHL VETKVRX BZEUHRZ GHIXPHL TPTJLOE HALGKKV TRDURMC EWTQDSI DAIVOZZ KXUG.

Step-2: Now lines up all ciphertext in 7 column

X	H	U	E	H	X	Z
H	R	I	U	H	T	I
H	G	E	U	Z	S	W
E	I	A	T	U	M	E
Z	X	H	T	V	Y	X
A	A	H	K	J	L	N
X	E	C	S	B	M	I
X	O	N	Q	D	P	V
W	K	E	K	A	I	E
E	M	G	J	A	I	E
L	I	M	R	V	A	V
K	W	A	P	K	G	I
X	E	T	G	Z	E	G
H	W	I	V	P	Z	V
W	I	V	G	S	S	G
F	I	N	V	L	H	L
V	E	T	K	V	R	X
B	Z	E	U	H	R	Z
G	H	I	X	P	H	L
T	P	T	J	L	O	E
H	A	L	G	K	K	V
T	R	D	U	R	M	C
E	W	T	Q	D	S	I
D	A	I	V	O	Z	Z
K	X	U	G			

Step-3: Now each column can be written as

$$(XHHEZAXXWELKXHWFVBGTHTEDK)$$
$$(HRGIXAEOKMIWEWIIEZHPARWAX)$$
$$(UIEAHHCNEGMATIVNTEITLDTIU)$$
$$(EUUTTKSQKJRPGVGVKUXJGUQVG)$$
$$(HHZUVJBDAAVKZPSLVHPLKRDO)$$
$$(XTSMYLMPIIAGEZSHRRHOKMSZ)$$
$$(ZIWEXNIVEEVIGVGLXZLEVCIZ)$$

Step-4: Now use frequency analysis on each column

On first column - X occurs 4 times which is the highest frequency in first column hence E may be encrypted to X i.e

$$\mathcal{E}(4) = 4 + b_1 = 23 \pmod{26}$$

$$\implies b_1 = 19 = \mathbf{T}$$

On second column- I occurs 4 times which is the highest frequency in second column hence E may be encrypted to I i.e

$$\mathcal{E}(4) = 4 + b_2 = 8 \pmod{26}$$

$$\implies b_2 = 4 = \mathbf{E}$$

On third column- T occurs 4 times which is the highest frequency in third column hence E may be encrypted to T i.e

$$\mathcal{E}(4) = 4 + b_3 = 19 \pmod{26}$$

$$\implies b_3 = 15 = P$$

(When we decrypt our cipher text taking third letter of keyword as P then plaintext does not make sense (Verify))
Now take second more frequent English alphabet i.e T hence T (second more frequent in English alphabet) may be encrypted to T (most frequent symbol in third column of cipher)

$$\mathcal{E}(19) = 19 + b_3 \pmod{26}$$

$$\implies b_3 = 0 = \mathbf{A}$$

On fourth column- G occurs 4 times which is the highest frequency in fourth column hence E may be encrypted to G i.e

$$\mathcal{E}(4) = 4 + b_4 = 6 \pmod{26}$$

$$\implies b_4 = 2 = \mathbf{C}$$

On fifth column- H and V occur more frequent but if we consider encryption of E either H or V then plaintext does not make sense (Verify). Similarly if we take encryption of T is either H or V then also plain text does not make sense. Now if we consider the 3rd more frequent letter in English alphabet i.e A may be encrypted to H then

$$\mathcal{E}(0) = 0 + b_5 = 7 \pmod{6}$$

$$\implies b_5 = 7 = \mathbf{H}$$

Similarly we can do frequency analysis on 6th and 7th column. After doing this we find that our key word is **TEACHER**.
Now we know keyword hence we can decrypt the cipher text easily and we get plaintext as follows.

"Education is a process of learning through which we acquire knowledge. It enlightens, empowers, and creates a positive development. Education gives an individual the knowledge and skills to work with virtue."

- **When key length is unknown**

If the key length of the keyword is not known then first we find the key length by Kasiski Method. Kasiski method utilizes the fact of repetition of words in the ciphertext. In this method, it is consider that repeated substring in plaintext is encrypted by the same substring in the keyword. That's why in the ciphertext, we get repeated substring, and the distance between the occurrence of repetition is multiple of the key lengths. Hence we can calculate key length by taking gcd of the distances between repetitions. After finding the key length, we apply the above method of frequency analysis for decrypting the ciphertext.

Note: Not every repetition occur in the above way but the probability of not occuring the repetition as above is very small.
A long ciphertext probably has more repetition and additionally, long repeated substrings are not likely to be by chance but short repetition may appear more often.

Example: Find the keylength and keyword for following cipher text

LIBVQSTNEZLQMEDLIVMAMPAKUFAVATLJVDAYYVN
FJQLNPLJVHKVTRNFLJVCMLKETALJVHUYJVSFKRF
TTWEFUXVHZNP
Solution: From the cipher text, we can see that

LJVH occurs 2 times
LJV occurs 4 times
JVH occurs 2 times
JV occurs 5 times
LJ occurs 4 times
VH occurs 3 times
LI, NF, NP occurs 2 times

Now the distance (number of symbols between two consecutive repetition) between two 4-graphs LJVH is $20 = 5 \times 2^2$
distance between trigraphs LJV is $15 = 5 \times 3$ and $10 = 5 \times 2$

So keylength = gcd of distances between repetitions

$$gcd(15, 10, 20) = 5$$

So keylength=5
Now we know the keylength, find keyword by above discussed method.

In next lecture, we will study application of matrices in substitution ciphers and other types of classical ciphers.

Lecture-3

Substitution Ciphers with matrices and Transposition Ciphers

1 Introduction

We have studied many encryption methods in previous lectures like Substitution/shift cipher, Hill cipher and affine ciphers. In this lecture we will discuss some of previous discussed encryption methods with the help of matrices with usual matrix addition and multiplication.

2 Hill Cipher

Let $\mathcal{A}$ be the set of symbols (like english alphabets A,B ...Z, ? , !, _ (blank space) and $\mathcal{P}$ be plain text.

Encryption: First divide the plain text into n-length message units
Choose a $n \times n$ matrix A, then encryption function $\mathcal{E}$ is defined by

$$\begin{aligned} \mathcal{E}&: \mathcal{P} \to \mathcal{A}^n \\ & X \longmapsto C = \mathcal{E}(X) = AX \end{aligned}$$

where $X = [x_1, x_2, ..., x_n]^T$ is message unit.

Decryption: Suppose $C = \mathcal{E}(X) = AX$, then decryption function $\mathcal{D}$ is defined by

$$\begin{aligned} \mathcal{D}&: \mathcal{A}^n \to \mathcal{P} \\ & C \longmapsto X = \mathcal{D}(C) = A^{-1}C \end{aligned}$$

provided A^{-1} exists.

Example: Let $\mathcal{A}$={A=0,B=1,C=2,...,Y=24,Z=25} be set of symbols(english alphabets).
$|\mathcal{A}| = 26$
Plain text: "NO I DO NOT KNOW"
First We divide plain text into 2-length (n=2) message units
i.e NO ID ON OT KN OW

Encryption: X_1=NO, X_2=ID, X_3=ON, X_4=OT, X_5=KN, X_6=OW
Now encryption of X_1=NO=$[13 \;\; 14]^T = \begin{bmatrix}13\\14\end{bmatrix}$
Let A=$\begin{bmatrix}2 & 3\\7 & 8\end{bmatrix}$, Fixed matrix for encryption in $\mathbb{Z}_{26} = |\mathcal{A}|$

Now encryption $\mathcal{E}(X_1) = AX_1$

$$\mathcal{E}(NO) = \begin{bmatrix}2 & 3\\7 & 8\end{bmatrix}\begin{bmatrix}13\\14\end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix}16\\21\end{bmatrix} \pmod{26} = \begin{bmatrix}Q\\V\end{bmatrix}$$

The Encryptionof 'NO' is 'QV'.

Decryption: For $C_1 = \begin{bmatrix}Q\\V\end{bmatrix} = \begin{bmatrix}16\\21\end{bmatrix}$

$\mathcal{D}(C_1) = A^{-1}C_1$, So first we calculate A^{-1} (if exists)

$$A = \begin{bmatrix}2 & 3\\7 & 8\end{bmatrix}$$

det(A)=$16 - 21 = -5 = 21 \pmod{26} \neq 0 \pmod{26}$
So, $A^{-1} \pmod{26}$ exists.

$A^{-1} = \frac{1}{det(A)} cofactor(A)$

$$
\begin{aligned}
A^{-1} &= -\frac{1}{5}\begin{bmatrix} 8 & -3 \\ -7 & 2 \end{bmatrix} \pmod{26} \\
&= -21\begin{bmatrix} 8 & -3 \\ -7 & 2 \end{bmatrix} \pmod{26} \quad (\text{since } \ 5^{-1} = 21 \pmod{26}) \\
&= 5\begin{bmatrix} 8 & -3 \\ -7 & 2 \end{bmatrix} \pmod{26} \\
&= \begin{bmatrix} 14 & 11 \\ 17 & 10 \end{bmatrix} \pmod{26}
\end{aligned}
$$

Now

$$
\begin{aligned}
\mathcal{D}(C_1) = \mathcal{D}\left(\begin{bmatrix} Q \\ V \end{bmatrix}\right) = \mathcal{D}\left(\begin{bmatrix} 16 \\ 21 \end{bmatrix}\right) &= A^{-1}C_1 \\
&= \begin{bmatrix} 14 & 11 \\ 17 & 10 \end{bmatrix}\begin{bmatrix} 16 \\ 21 \end{bmatrix} \pmod{26} \\
&= \begin{bmatrix} 224 + 231 \\ 272 + 210 \end{bmatrix} \pmod{26} \\
&= \begin{bmatrix} 455 \\ 482 \end{bmatrix} \pmod{26} \\
&= \begin{bmatrix} 13 \\ 14 \end{bmatrix} \pmod{26} \\
&= \begin{bmatrix} N \\ O \end{bmatrix}
\end{aligned}
$$

So decryption of 'QV' is 'NO'.

In the same way we can do encryption and decryption for X_2=ID, X_3=ON, X_4=OT, X_5=KN, X_6=OW .

3 Affine Cipher

Let $\mathcal{A}$ be the set of symbols (like english alphabtes, ? , !, _) and $\mathcal{P}$ be plain text.

Encryption: First divide plain text into n-length message units. Let A be $n \times n$ matrix and B be $n \times 1$ vector.
Encryption function $\mathcal{E}$, is defined by

$$\begin{aligned} \mathcal{E}&: \mathcal{P} \to \mathcal{A}^n \\ &X \mapsto C = \mathcal{E}(X) = AX + B \end{aligned}$$

where $X = [x_1, x_2, ..., x_n]^T$ is message unit.

Decryption: Supose $C = \mathcal{E}(X) = AX + B$, Decryption function $\mathcal{D}$ is defined by

$$\begin{aligned} \mathcal{D}&: \mathcal{A}^n \to \mathcal{P} \\ &C \mapsto X = \mathcal{D}(C) = A^{-1}(C - B) \end{aligned}$$

i.e $\mathcal{D}(C) = A'C + B'$ where $A' = A^{-1}$ and $B' = -A^{-1}B$, provided A^{-1} exists.

Example: Let $\mathcal{A}$ ={A=0,B=1,C=2,...,Y=24,Z=25} be set of alphabets.
$|\mathcal{A}| = 26$
Plain text $\mathcal{P}$: NO ANSWER

We first divide plain text into 2-length message unit (n=2) i.e X_1=NO, X_2=AN, X_3=SW, X_4=ER

Let A=$\begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix}$, Fixed matrix for encryption in $\mathbb{Z}_{26} = |\mathcal{A}|$, B=$\begin{bmatrix} 4 \\ 2 \end{bmatrix}$

Encryption:X_1=NO=$[13 \;\; 14]^T = \begin{bmatrix} 13 \\ 14 \end{bmatrix}$

$$\begin{aligned}
\mathcal{E}(X_1) = C_1 &= AX_1 + B \\
&= \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} \begin{bmatrix} 13 \\ 14 \end{bmatrix} + \begin{bmatrix} 4 \\ 2 \end{bmatrix} \pmod{26} \\
&= \begin{bmatrix} 16 \\ 21 \end{bmatrix} + \begin{bmatrix} 4 \\ 2 \end{bmatrix} \pmod{26} \\
&= \begin{bmatrix} 20 \\ 23 \end{bmatrix} \pmod{26} \\
&= \begin{bmatrix} U \\ X \end{bmatrix}
\end{aligned}$$

So encryption of 'NO' is 'UX'.

Decryption: C_1=UX

$$\mathcal{D}(C_1) = A'C_1 + B' = A^{-1}C_1 - A^{-1}B = A^{-1}(C_1 - B)$$

From previous example we have

$$\begin{aligned}
A^{-1} &= \begin{bmatrix} 14 & 11 \\ 17 & 10 \end{bmatrix} \pmod{26} \\
\mathcal{D}(C_1) &= \begin{bmatrix} 14 & 11 \\ 17 & 10 \end{bmatrix} \left(\begin{bmatrix} 20 \\ 23 \end{bmatrix} - \begin{bmatrix} 4 \\ 2 \end{bmatrix} \right) \pmod{26} \\
&= \begin{bmatrix} 14 & 11 \\ 17 & 10 \end{bmatrix} \begin{bmatrix} 16 \\ 21 \end{bmatrix} \pmod{26} \\
&= \begin{bmatrix} 13 \\ 14 \end{bmatrix} \pmod{26} \\
&= \begin{bmatrix} N \\ O \end{bmatrix}
\end{aligned}$$

So decryption of 'UX' is 'NO'.

In the the same way we can do encryption and decryption for X_2=AN, X_3=SW, X_4=ER.

Question: Decrypt the message

$$WKNCMSLRTQ$$

obtained by digraph encryption on English alphabets (A=0 to 25=Z) with "."(dot=26),","(comma=27),"?"(question mark=28) (29 letters) using Hill Cipher. Message started with 'GIVE'.

Solution: Digraph encryption means n=2, $|\mathcal{A}| = 29$

We know in Hill cipher encryption function is given by

$$\mathcal{E}(X) = AX$$

where A is 2×2 matrix in $\mathbb{Z}_{29}$ and X is 2-length message unit.

Decryption function is given by $\mathcal{D}(C) = A^{-1}C$

So, to decrypt the given cipher we have to calculate A^{-1} in $\mathbb{Z}_{29}$ i.e we have to find matrix A in $\mathbb{Z}_{29}$.
Let matrix A=$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Message started with 'GIVE' means $\mathcal{E}(GI) = WK$ and $\mathcal{E}(VE) = NC$
Let X_1=GI, C_1=WK, X_2=VE,C_2=NC
by encryption function we have $\mathcal{E}(X_1) = AX_1 = C_1$, $\mathcal{E}(X_2) = AX_2 = C_2$
i.e $AX_1 = C_1$, $AX_2 = C_2$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 6 \\ 8 \end{bmatrix} = \begin{bmatrix} 22 \\ 10 \end{bmatrix} \text{ and } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 21 \\ 4 \end{bmatrix} = \begin{bmatrix} 13 \\ 2 \end{bmatrix}$$

from above, we have system of 4 linear equations in a, b, c, d

$$\begin{aligned} 6a + 8b &= 22 \\ 6c + 8d &= 10 \\ 21a + 4b &= 13 \\ 21c + 4d &= 2 \end{aligned}$$

Solve the above system of equation for a, b, c, d
We have

$$a = \frac{1}{9} = 1 \times 9^{-1} = 1 \times 13 = 13 \pmod{29},$$
$$b = \frac{8}{3} = 8 \times 3^{-1} = 8 \times 10 = 22 \pmod{29},$$
$$c = \frac{-1}{6} = -1 \times 6^{-1} = -1 \times 5 = 24 \pmod{29},$$
$$d = \frac{11}{8} = 11 \times 8^{-1} = 11 \times 11 = 5 \pmod{29}$$

So we have matrix A=$\begin{bmatrix} 13 & 22 \\ 24 & 5 \end{bmatrix}$,
det(A)= $13 \times 5 - 22 \times 24 = 65 - 528 = -463 = 1 \pmod{29}$

and $A^{-1} = \begin{bmatrix} 5 & -22 \\ -24 & 13 \end{bmatrix} \pmod{29} = \begin{bmatrix} 5 & 7 \\ 5 & 13 \end{bmatrix} \pmod{29}$

$$C_3 = MS = \begin{bmatrix} 12 \\ 18 \end{bmatrix}$$
$$C_4 = LR = \begin{bmatrix} 11 \\ 17 \end{bmatrix}$$
$$C_5 = TQ = \begin{bmatrix} 19 \\ 16 \end{bmatrix}$$

Now

$$X_3 = A^{-1}C_3 = \begin{bmatrix} 5 & 7 \\ 5 & 13 \end{bmatrix} \begin{bmatrix} 12 \\ 18 \end{bmatrix} = \begin{bmatrix} 12 \\ 4 \end{bmatrix} \pmod{29} = \begin{bmatrix} M \\ E \end{bmatrix}$$
$$X_4 = A^{-1}C_4 = \begin{bmatrix} 5 & 7 \\ 5 & 13 \end{bmatrix} \begin{bmatrix} 11 \\ 17 \end{bmatrix} = \begin{bmatrix} 0 \\ 15 \end{bmatrix} \pmod{29} = \begin{bmatrix} A \\ P \end{bmatrix}$$
$$X_5 = A^{-1}C_5 = \begin{bmatrix} 5 & 7 \\ 5 & 13 \end{bmatrix} \begin{bmatrix} 19 \\ 16 \end{bmatrix} = \begin{bmatrix} 4 \\ 13 \end{bmatrix} \pmod{29} = \begin{bmatrix} E \\ N \end{bmatrix}$$

So decrypted mesaage is “GIVEMEAPEN" i.e. “GIVE ME A PEN"

4 Vigenèner Cipher

Recall Vigenère Cipher: Suppose keyword

$$K = k_1k_2k_3 \dots k_l, \quad k_i \in \mathbb{Z}_n$$

message block is therefore

$$x = x_1x_2 \dots x_l, \quad x_i \in \mathbb{Z}_n$$

then encryption function is given by

$$\mathcal{E}(x) = y = y_1y_2 \dots y_l \quad \text{where} \quad y_i \equiv x_i + k_i \pmod{n}$$

decryption funtion is given by

$$\mathcal{D}(y) = x = x_1x_2 \dots x_l \ \text{ such that } \ x_i \equiv y_i - k_i \pmod{n}$$

where $n = |\mathcal{A}|$=number of symbols written in their numerical equivalent.

We can write keyword K, message block x in matrix of order $l \times 1$ where l =keylength

$$K = \begin{bmatrix} k_1 \\ k_2 \\ . \\ . \\ . \\ k_l \end{bmatrix}, \quad x = \begin{bmatrix} x_1 \\ x_2 \\ . \\ . \\ . \\ x_l \end{bmatrix}$$

then encryption function is defined by

$\mathcal{E}\colon M_{l\times 1} \to M_{l\times 1}$

$$\mathcal{E}(x) = y = \mathcal{E}\left(\begin{bmatrix} x_1 \\ x_2 \\ . \\ . \\ . \\ x_l \end{bmatrix}\right) = \begin{bmatrix} x_1 \\ x_2 \\ . \\ . \\ . \\ x_l \end{bmatrix} + \begin{bmatrix} k_1 \\ k_2 \\ . \\ . \\ . \\ k_l \end{bmatrix} = \begin{bmatrix} x_1 + k_1 \\ x_2 + k_2 \\ . \\ . \\ . \\ x_l + k_l \end{bmatrix} \pmod{n} = \begin{bmatrix} y_1 \\ y_2 \\ . \\ . \\ . \\ y_l \end{bmatrix}$$

and decryption function is defined by

$\mathcal{D}$: $M_{l\times 1} \to M_{l\times 1}$

$$\mathcal{D}(y) = x = \mathcal{D}\left(\begin{bmatrix} y_1 \\ y_2 \\ . \\ . \\ . \\ y_l \end{bmatrix}\right) = \begin{bmatrix} y_1 \\ y_2 \\ . \\ . \\ . \\ y_l \end{bmatrix} - \begin{bmatrix} k_1 \\ k_2 \\ . \\ . \\ . \\ k_l \end{bmatrix} = \begin{bmatrix} y_1 - k_1 \\ y_2 - k_2 \\ . \\ . \\ . \\ y_l - k_l \end{bmatrix} \pmod{n} = \begin{bmatrix} x_1 \\ x_2 \\ . \\ . \\ . \\ x_l \end{bmatrix}$$

example: Let $\mathcal{A}$={A=0,B=1,... Y=24,Z=25,?=26} i.e $|\mathcal{A}| = 27$
Encrypt the following plain text with keyword "EGYPT"

"HELLO HOW ARE YOU?"

Solution: We have already done this example, here we do encryption and decryption by matrices
Keyword: EGYPT, Keylength=5
Encrypt: HELLO HOW ARE YOU?
First divide the message into blocks of length 5 i.e.

b_1=HELLO b_2=HOWAR b_3=EYOU?

$$\text{Encryption of block } b_1 = \begin{bmatrix} H \\ E \\ L \\ L \\ O \end{bmatrix} = x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \\ 11 \\ 11 \\ 14 \end{bmatrix}$$

$$\text{K=EGYPT=} \begin{bmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \\ k_5 \end{bmatrix} = \begin{bmatrix} 4 \\ 6 \\ 24 \\ 15 \\ 19 \end{bmatrix}$$

$\mathcal{E}\colon M_{5\times1} \to M_{5\times1}$

$$\mathcal{E}(x) = y = \mathcal{E}\left(\begin{bmatrix}7\\4\\11\\11\\14\end{bmatrix}\right) = \begin{bmatrix}7\\4\\11\\11\\14\end{bmatrix} + \begin{bmatrix}4\\6\\24\\15\\19\end{bmatrix} = \begin{bmatrix}7+4\\4+6\\11+24\\11+15\\14+19\end{bmatrix} \pmod{27} = \begin{bmatrix}11\\10\\8\\26\\6\end{bmatrix} \pmod{27} = \begin{bmatrix}L\\K\\I\\?\\G\end{bmatrix}$$

So encryption of 'HELLO' is 'LKI?G'

Decryption: y$= \begin{bmatrix}L\\K\\I\\?\\G\end{bmatrix} = \begin{bmatrix}y_1\\y_2\\y_3\\y_4\\y_5\end{bmatrix} = \begin{bmatrix}11\\10\\8\\26\\6\end{bmatrix}$

$\mathcal{D}\colon M_{5\times1} \to M_{5\times1}$

$$\mathcal{D}(y) = x = \mathcal{D}\left(\begin{bmatrix}11\\10\\8\\26\\6\end{bmatrix}\right) = \begin{bmatrix}11\\10\\8\\26\\6\end{bmatrix} - \begin{bmatrix}4\\6\\24\\15\\19\end{bmatrix} = \begin{bmatrix}11-4\\10-6\\8-24\\26-15\\6-19\end{bmatrix} \pmod{27} = \begin{bmatrix}7\\4\\11\\11\\14\end{bmatrix} \pmod{27} = \begin{bmatrix}H\\E\\L\\L\\O\end{bmatrix}$$

So decryption of 'LKI?G' is 'HELLO'
In the same way do encryption and decryption for other blocks.

5 Transposition Ciphers

In transposition cipher, symbols of the cipher text remain the same as plain-text, but the ordering of these symbols are changed in a specific form. Transposition Ciphers are not very secure as the cipher is the rearrangement of plain text. With modern computers, one can check all possible rearrangements of cipher text and get the plain text. But before the computer era, transposition ciphers were used and considered to be a secure cipher.

5.1 Columnar Transposition Cipher

5.1.1 Simple Columnar Transposition Cipher

In simple columnar transposition cipher, sender (Alice) and receiver (Bob) fix a number k. Alice will write the plain text in k columns to encrypt the message. Encrypted cipher text is obtained by writing column array from left to right, i.e., first, write symbols of the first column, then write the symbols of the second column and so on.

Example: To encrypt **"MATHEMATICS IS A LANGUAGE"**. Suppose fix number is $k = 4$ (known to both sender and receiver).

Now write the plain text into 4 columns as follows:

Column-1	Column-2	Column-3	Column-4
M	A	T	H
E	M	A	T
I	C	S	I
S	A	L	A
N	G	U	A
G	E		

The encryption of plain text is

"[Column-1][Column-2][Column-3][Column-4]"

i.e.

Cipher Text: "**MEISNGAMCAGETASLUHTIAA**"

For decryption, Count the numbers of symbols in cipher text say n. The receiver (Bob) knows the number of columns, which is k. Now Bob will perform the following calculations to know the number of symbols in each column.
By division algorithm $n = k \times q + r$, where q is quotient and r is remainder on dividing number of symbols in cipher text n by number of columns k.
If $r = 0$ then each column have q symbols.
If $r \neq 0$ then first r columns have $q + 1$ symbols and other columns (i.e. last $(k - r)$ columns) have q symbols. Plain text is obtained by writing symbols row-wise.

Example: Decrypt the following transposition cipher when the number of columns is 4.

Cipher Text: "**MEISNGAMCAGETASLUHTIAA**"

Solution:
Number of symbols in cipher text =22
Number of columns =4
By division algorithm $22 = 4 \times 5 + 2$, i.e $q = 5$ and $r = 2$
This implies first two columns have $q + 1 = 6$ symbols and last 2 columns have $q = 5$ symbols. So divide the cipher text into blocks of length 6, 6, 5 and 5, each block corresponds to column array.
So we have column array :

Column-1	Column-2	Column-3	Column-4
M	A	T	H
E	M	A	T
I	C	S	I
S	A	L	A
N	G	U	A
G	E		

Now plain text is "[row-1][row-2][row-3][row-4][row-5][row-6]" i.e.

"**MATHEMATICSISALANGUAGE**"

i.e.

"**MATHEMATICS IS A LANGUAGE**"

5.1.2 Keyword Columnar Transposition Cipher

In keyword columnar transposition ciphers, the sender (Alice) and receiver (Bob) choose a common keyword. To encrypt the plain text, sender will write the plain text into l columns (l = number of symbols in keyword). Cipher text is obtained by writing column array in alphabetical order of the keyword.

Example: Encrypt the following plain text using keyword columnar transposition ciphers with key **"WORLD"**

"**MATHEMATICS IS A LANGUAGE**"

Solution: Keyword is WORLD that has 5 symbols, so write the plaintext in five columns namely

Column-W	Column-O	Column-R	Column-L	Column-D
M	A	T	H	E
M	A	T	I	C
S	I	S	A	L
A	N	G	U	A
G	E			

alphabetical order of keyword is 'DLORW', thus ciphertext is

"[Column-D][Column-L][Column-O][Column-R][Column-W]"

i.e.

"ECLAHIAUAAINETTSGMMSAG"

Decryption: Since receiver knows the keyword, suppose keyword has k symbols (i.e. keylength=k). Perform the following calculations to know the number of symbols in each column according to keyword.
By division algorithm $n = k \times q + r$, where q is quotient and r is remainder on dividing number of symbols in cipher text n by number of columns k.
If $r = 0$ then each column have q symbols.
If $r \neq 0$ then first r columns of keyword have $q+1$ symbols and other columns of keyword (i.e. last $(k - r)$ columns) have q symbols. Now arrange the k columns in alphabetical order of keyword. Plain text is obtained by writing symbols row-wise.

Example: Decrypt the following keyword columnar transposition cipher using keyword **'WORLD'**

"ECLAHIAUAAINETTSGMMSAG"

Solution: No. of symbols in ciphertext =22
keylength is 5, so no. of columns is 5 By division algorithm $22 = 5 \times 4 + 2$, i.e $q = 4$ and $r = 2$
this implies first two columns, column-W and column-O have $q + 1 = 5$ symbols and last 3 columns column-R, column-L and column-D have $q = 4$ symbols. Now write columns in alphabetical order of keyword i.e.

Column-D Column-L Column-O Column-R Column-W

Now put first 4 cipher symbols in column-D,next 4 cipher symbols in column-L,next 5 cipher symbols in column-O, next 4 cipher symbols in column-R, next 5 cipher symbols in column-W i.e.

Column-D	Column-L	Column-O	Column-R	Column-W
E	H	A	T	M
C	I	A	T	M
L	A	I	S	S
A	U	N	G	A
		E		G

Now rearrange above array in keyword order i.e 'WORLD'

Column-W	Column-O	Column-R	Column-L	Column-D
M	A	T	H	E
M	A	T	I	C
S	I	S	A	L
A	N	G	U	A
G	E			

Plain text is obtained by writing symbols row-wise from above array

"MATHEMATICSISALANGUAGE"

i.e

"MATHEMATICS IS A LANGUAGE"

5.2 Double Transposition

In double transposition, we apply columnar transposition twice. First apply columnar transposition on plain text. Again apply columnar transposition on obtained cipher text.

Example: Encrypt the following plain text using double transposition with fix number (number of columns) is eqaul to 4

"MATHEMATICS IS A LANGUAGE"

Solution: First, apply columnar transposition on given plain text we obtained cipher text (from above example done in columnar transposition)

Cipher Text: "MEISNGAMCAGETASLUHTIAA"

again apply columnar transposition on the above cipher text

Column-1	Column-2	Column-3	Column-4
M	E	I	S
N	G	A	M
C	A	G	E
T	A	S	L
U	H	T	I
A	A		

The encryption of plain text is

"[Column-1][Column-2][Column-3][Column-4]"

i.e.

Cipher Text: "**MNCTUAEGAAHAIAGSTSMELI**"

So encryption of "MATHEMATICS IS A LANGUAGE" is "MNCTUAEGAAHAIAGSTSMELI" by double transposition.

Decryption: To decrypt double transposition cipher apply decryption of columnar transposition twice.

Example: Decrypt the following double transposition cipher

Cipher Text: "**MNCTUAEGAAHAIAGSTSMELI**"

Given, number of columns=4

Solution: Number of symbols in cipher text =22
number of columns=4
By division algorithm $22 = 4 \times 5 + 2$, i.e $q = 5$ and $r = 2$
this implies first two columns have $q + 1 = 6$ symbols and last 2 columns have $q = 5$ symbols. So divide the cipher text into blocks of length 6,6,5 and 5, each block corresponds to columns of transposition cipher.
So we have columns :

Column-1	Column-2	Column-3	Column-4
M	E	I	S
N	G	A	M
C	A	G	E
T	A	S	L
U	H	T	I
A	A		

After applying columnar transposition decryption one time we get

"MEISNGAMCAGETASLUHTIAA"

Again apply columnar transposition decryption on

"MEISNGAMCAGETASLUHTIAA"

(Similar to example of columnar transposition)
Number of symbols =22
number of columns=4
By division algorithm $22 = 4 \times 5 + 2$, i.e $q = 5$ and $r = 2$
this implies first two columns have $q + 1 = 6$ symbols and last 2 columns have $q = 5$ symbols. So divide the cipher text into blocks of length 6,6,5 and 5, each block corresponds to columns of transposition cipher.

So we have columns :

Column-1	Column-2	Column-3	Column-4
M	A	T	H
E	M	A	T
I	C	S	I
S	A	L	A
N	G	U	A
G	E		

Now, plain text is obtained by writing symbols row-wise

"**MATHEMATICSISALANGUAGE**"

i.e.

"**MATHEMATICS IS A LANGUAGE**"

Similarly, We can do double transposition with two different number of columns or keywords for two steps of columnar transposition.

Lecture-4

Some more classical Ciphers

1 ADFGX Cipher

ADFGX ciphers were used by the German military in March 1918 for the first time. This cipher is the combination of substitution cipher and transposition cipher. This cipher is named ADFGX because in the ciphertext only five symbols (A, D, F, G, X) can appear. It involves two steps.

In the first step, it uses the substitution cipher to encrypt the plaintext. To apply the substitution cipher, users (Sender and Receiver) agree upon a 5×5 array of the English alphabet. In the 5×5 array, there are 25 places at which 26 symbols are placed by considering I and J at the same place. The rows and columns of this ADFGX array are each labeled with the symbols A, D, F, G, and X in order as follows.

	A	D	F	G	X
A					
D					
F					
G					
X					

Now each symbol of plaintext is mapped to a pair of corresponding row and column symbol label. Therefore we get twice no. of the symbols in the ciphertext as compare to plaintext and it contains only five symbols A, D, F, G, and X.

In the 2nd step, it performs the transposition cipher's technique i.e keyword columnar transposition cipher on the obtained ciphertext in the first step.

Example: Consider the following 5×5 array of symbols

	A	D	F	G	X
A	T	F	I/J	K	E
D	H	N	C	S	Z
F	D	A	X	M	G
G	O	V	R	U	Y
X	L	B	Q	W	P

Take keyword 'WATER' and encrypt the following message using ADFGX cipher

"PEACOCK IS A NATIONAL BIRD OF INDIA"

Solution:
Encryption: To encrypt "PEACOCK IS A NATIONAL BIRD OF INDIA" we map each letter of plain text to a pair of corresponding row and column symbol label in 5×5 array of symbols i.e to encrypt P we write XX , For E we write AX and so on. And we get a first cipher text as follows.

Plain text	P	E	A	C	O	C	K	I	S	A	N
Cipher text	XX	AX	FD	DF	GA	DF	AG	AF	DG	FD	DD
Plain text	A	T	I	O	N	A	L	B	I	R	D
Cipher text	FD	AA	AF	GA	DD	FD	XA	XD	AF	GF	FA
Plain text	O	F	I	N	D	I	A				
Cipher text	GA	AD	AF	DD	FA	AF	FD				

Hence cipher text obtained from the first step of ADFGX cipher is

XXAXFDDFGADFAGAFDGFDDDFDAAAFGADDFDXAXDAFG FFAGAADAFDDFAAFFD

Now we apply key columner transposition cipher using key word 'WATER' on the ciphet text obtained from the first step to get final ciphertext.

Column array of key columnar transposition cipher:

Column-W	Column-A	Column-T	Column-E	Column-R
X	X	A	X	F
D	D	F	G	A
D	F	A	G	A
F	D	G	F	D
D	D	F	D	A
A	A	F	G	A
D	D	F	D	X
A	X	D	A	F
G	F	F	A	G
A	A	D	A	F
D	D	F	A	A
F	F	D		

Therefore, final cipher text is obtained by wrtining column arrays in alphabetical order of keyword i.e.

XDFDDADXFADFXGGFDGDAAAAFAADAAXFGFAAFAGFF FDFDFDXDDFDADAGADF

Decryption: To decrypt the cipher text we go in the reverse order of encryption i.e. first, we apply decrytpion of keyword columnar transposition cipher follwed by decryption of substituion cipher.
When we apply decrytpion of keyword columnar transposition cipher, we get

XXAXFDDFGADFAGAFDGFDDDFDAAAFGADDFDXAXDAFG FFAGAADAFDDFAAFFD
Now, decrypt the above text with the help of 5×5 array to get the plain text
To do so, divide the text in blocks of length 2. In each block, first symbol corresponds to row label and second symbol corresponds to column label. After dividing text in blocks of length 2 we have
XX AX FD DF GA DF AG AF DG FD DD FD AA AF GA DD FD XA XD AF GF FA GA AD AF DD FA AF FD

And 5×5 array is

	A	D	F	G	X
A	T	F	I/J	K	E
D	H	N	C	S	Z
F	D	A	X	M	G
G	O	V	R	U	Y
X	L	B	Q	W	P

So,
XX corresponds to P (row-X, column-X)
AX corresponds to E (row-A, column-X)
FD corresponds to A (row-F, column-D)
and so on.
Finally, we get plain text

"PEACOCK IS A NATIONAL BIRD OF INDIA"

2 ADFGVX Cipher:

In June 1918, Germans built this cipher from ADFGX, by increasing the size of the array to 6×6. They added the digit 0-9 in the plaintext. Therefore they had to increase the size of the array from 5×5 to 6×6. This array takes the values 0-9 and the English alphabet, by considering I and J are placed at a different position in the array. Now to label this array there was a requirement of an extra letter and this additional letter was 'V'.
Therefore the rows and columns of this ADFGVX array are each labeled with the symbols A, D, F, G, V and X in order as follows.

	A	D	F	G	V	X
A						
D						
F						
G						
V						
X						

Encryption and Decryption technique is similar to ADFGX cipher.

Example: Using ADFGVX cipher encrypt the plaintext **"EARTH IS ESTIMATED TO BE 4540 MILLION YEARS OLD"**. Keyword is **"STAR"**

	A	D	F	G	V	X
A	1	9	A	J	M	R
D	C	B	I	2	Q	Y
F	E	0	Z	3	D	V
G	7	8	O	F	G	S
V	6	H	4	X	T	W
X	P	5	N	K	L	U

Solution: We map each letter of plain text to a pair of corresponding row and column symbol label in 6×6 array of symbols i.e to encrypt E we write FA , For A we write AF and so on. And we get a first cipher text as follows.

Plaint text	E	A	R	T	H	I	S	E	S	T	I
Cipher text	FA	AF	AX	VV	VD	DF	GX	FA	GX	VV	DF
Plaint text	M	A	T	E	D	T	O	B	E	4	5
Cipher text	AV	AF	VV	FA	FV	VV	GF	DD	FA	VF	XD
Plain text	4	0	M	I	L	L	I	O	N	Y	E
Cipher text	VF	FD	AV	DF	XV	XV	DF	GF	XF	DX	FA
Plain text	A	R	S	O	L	D					
Cipher text	AF	AX	GX	GF	XV	FV					

Encrypted cipher text
"FAAFAXVVVDDFGXFAGXVVDFAVAFVVFAFVVVGFDDFA VFXDVFFDAVDFXVXVDFGFXFDXFAAFAXGXGFXVFV"

Now we apply key columner transposition cipher using key word 'STAR' on the ciphet text obtained from the first step to get final ciphertext.

Column-S	Column-T	Column-A	Column-R
F	A	A	F
A	X	V	V
V	D	D	F
G	X	F	A
G	X	V	V
D	F	A	V
A	F	V	V
F	A	F	A
V	V	G	F
D	D	F	A
V	F	X	D
V	F	F	D
A	V	D	F
X	V	X	V
D	F	G	F
X	F	D	X
F	A	A	F
A	X	G	X
G	F	X	V
F	V		

Final cipher text is :
"AVDFVAVFGFXFDXGDAGXFVFAVVVAFADDFVFXFXVF AVGGDAFVDVVAXDXFAGFAXDXXFFAVDFFVVFFAXFV"

3 Permutation cipher:

Let S_n be the symmetric group on n symbols where n is cardinality of Alphabets. The plaintext and ciphertext space is $X = \{m_1, m_2, \ldots, m_n\}$.
Then for plaintext $m = (m_1, m_2, \ldots, m_k)$ and a permutation $\sigma \in S_n$

- **Encrption:** The encryption function is defined by

$$\mathcal{E}: X \longrightarrow X$$
$$m \longmapsto (m)\sigma = (m_1, m_2, \ldots, m_k)\sigma = (m_{(1)\sigma}, m_{(2)\sigma}, \ldots, m_{(k)\sigma})$$

- **Decryption:** Denote σ^{-1} to be the inverse of σ in S_n. Let $m' = (m'_1, m'_2, \ldots, m'_k)$ is a ciphertext, encrypted with permutation cipher by using permutation σ, then decryption function is defined by

  $\mathcal{D}\colon X \longrightarrow X$
  $m' \longmapsto (m')\sigma^{-1} = (m'_1, m'_2, \ldots, m'_k)\sigma^{-1} = (m'_{(1)\sigma^{-1}}, m'_{(2)\sigma^{-1}}, \ldots, m'_{(k)\sigma^{-1}})$

Example: Consider the english alphabets as plaintext and ciphertext space $X = \{A = 1, B = 2, \ldots, Y = 25, Z = 26\}$.
Let $\sigma \in S_{26}$ and $\sigma = (1\ \ 3)(4\ \ 5)(16\ \ 17\ \ 18)(20\ \ 21\ \ 22)$

Plain text-**"NEVER GIVE UP "**

	N	E	V	E	R	G	I	V	E	U	P
	14	5	22	5	18	7	9	22	5	21	16
Encryption:-	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
	14	4	20	4	16	7	9	20	4	22	17
	N	D	T	D	P	G	I	T	D	V	Q

Encrypted Message is: **"NDTDP GITD VQ"**

$\sigma^{-1} = (1\ \ 3)(4\ \ 5)(17\ \ 16\ \ 18)(21\ \ 20\ \ 22)$

	N	D	T	D	P	G	I	T	D	V	Q
	14	4	20	4	16	7	9	20	4	22	17
Decryption:-	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
	14	5	22	5	18	7	9	22	5	21	16
	N	E	V	E	R	G	I	V	E	U	P

Decrypted message is: **"NEVER GIVE UP "**

Encryption in english alphabet by using key:

$X = \{A = 1, B = 2, \ldots, X = 24, Y = 25, Z = 26\}$.
Plain text:- **"LET US GO FOR PLAYING CRICKET"**
Keyword: **"SHARMA"**
Arrange it in alphabetic order and drop the duplicates i.e AHMRS

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
A	H	M	R	S	B	C	D	E	F	G	I	J	K	L	N	O	P	Q	T
1	8	13	18	19	2	3	4	5	6	7	9	10	11	12	14	15	16	17	20

21	22	23	24	25	26
U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓
U	V	W	X	Y	Z
21	22	23	24	25	26

Now $\sigma = (1)(2\ 8\ 4\ 18\ 16\ 14\ 11\ 7\ 3\ 13\ 10\ 6)(5\ 19\ 17\ 15\ 12\ 9)(20)(21)(22)(23)(24)(25)(26)$

i.e. $\sigma = (2\ \ 8\ \ 4\ \ 18\ \ 16\ \ 14\ \ 11\ \ 7\ \ 3\ \ 13\ \ 10\ \ 6)(5\ \ 19\ \ 17\ \ 15\ \ 12\ \ 9)$
Cipher text is :- **"IST UQ CL BLP NIAYEKC MPEMGST"**

For Decryption we use
$\sigma^{-1} = (1)(6\ 10\ 13\ 3\ 7\ 11\ 14\ 16\ 18\ 4\ 8\ 2)(9\ 12\ 15\ 17\ 19\ 5)(20)(21)(22)(23)(24)(25)(26)$
i.e. $\sigma^{-1} = (6\ \ 10\ \ 13\ \ 3\ \ 7\ \ 11\ \ 14\ \ 16\ \ 18\ \ 4\ \ 8\ \ 2)(9\ \ 12\ \ 15\ \ 17\ \ 19\ \ 5)$
Hence decrypted message is **"LET US GO FOR PLAYING CRICKET"**

4 Playfair Cipher:

The playfair cipher was the first practical digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone. But it was named after Lord Playfair because he started the use of this cipher.
We have a grid of 5×5 cipher. There are 25 spaces but we have 26 letters, by convention we put I,J together.

A	B	C	D	E
F	G	H	I,J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Encryption: There are four rules for encryption using playfair cipher. Suppose P,Q represent the plain text symbols and C,D represent cipher symbols.

1. If P,Q are in different rows and columns then they form a rectangle of which they are opposite diagonal entries, then the encryption of digraph PQ is given by CD where C is in the same column as of P and D is also in same column as of Q.
   Eg: $\mathcal{E}(CT) = SD,\ \mathcal{E}(WA) = BV$

2. If P,Q are different and lie in the same row then the encryption of digraph PQ is given by CD where C is just right from P and D is just right from Q. If needed wrap it.
   Eg: $\mathcal{E}(CE) = DA,\ \mathcal{E}(FK) = GF$

3. If P,Q are different and lie in the same column then the encryption of digraph PQ is given by CD where C is just below of P and D is just below Q. If needed wrap it.
   Eg: $\mathcal{E}(NH) = SN,\ \mathcal{E}(AQ) = FV$

4. If P,Q are same then by convention put letter X in between them and then do encryption by using rules 1,2,3.

Decryption: Decryption is reverse process of encryption. Decryption rules for playfair cipher are :

1. If C,D are in different rows and columns then they form a rectangle of which they are opposite diagonal entries, then the decryption of digraph CD is given by PQ where P is in the same column as of C and Q is also in same column as of D.
   Eg: $\mathcal{D}(NI) = HO,\ \mathcal{D}(BV) = WA$

2. If C,D are different and lie in the same row then the decryption of digraph CD is given by PQ where P is just left from C and Q is just left from D. If needed wrap it.
   Eg: $\mathcal{D}(DA) = CE,\ \mathcal{D}(GF) = FK$

3. If C,D are different and lie in the same column then the decryption of digraph CD is given by PQ where P is just above of C and Q is just above D. If needed wrap it.
   Eg: $\mathcal{D}(SN) = NH,\ \mathcal{D}(FV) = AQ$

Example: Key: RULE
Plaintext: INSTRUMENTS

Arrange key in alphabetical order i.e ELRU
In 5×5 grid, first we write row-wise alphabets of keyword in alphabetical order then remaining English alphabet in order.

E	L	R	U	A
B	C	D	F	G
H	I,J	K	M	N
O	P	Q	S	T
V	W	X	Y	Z

Plaintext: "INSTRUMENTS"
After split: 'IN' 'ST' 'RU' 'ME' 'NT' 'SZ'

$$\mathcal{E}(IN) = KH$$
$$\mathcal{E}(ST) = TO$$
$$\mathcal{E}(RU) = UA$$
$$\mathcal{E}(ME) = UH$$
$$\mathcal{E}(NT) = TZ$$
$$\mathcal{E}(SZ) = YT$$

Encrpted message is: "KHTOUAUHTZYT"
After split: 'MK' 'TL' 'VO' 'IA' ÙZ' 'XT'

$$\mathcal{D}(KH) = IN$$
$$\mathcal{D}(TO) = ST$$
$$\mathcal{D}(UA) = RU$$
$$\mathcal{D}(UH) = ME$$
$$\mathcal{D}(TZ) = NT$$
$$\mathcal{D}(YT) = SZ$$

Message is "INSTRUMENTS"

Note- When we perform encryption without keyword then we write 5×5 grid in English alphabets order i.e. A, B,... Y,Z

A	B	C	D	E
F	G	H	I,J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Lecture-5

Introduction to Number Theory

Greatest Common Divisor: Greatest Common Divisor (gcd) of integers a_1, a_2 (atleast one of them is not 0) is the largest positive integer that divides a_1, a_2.

Note :

1. If more than one integer is 0, then gcd does not exist.
2. $\gcd(a_1, a_2) = \gcd(a_2, a_1)$
3. $\gcd(a, 0) = |a|$ where a is non zero integer.
4. $\gcd(a_1, a_2, ..., a_n) = \gcd(a_1, a_2, ..., \gcd(a_i, a_j), ..., a_n) \ \ \forall\, i, j \ \in \ \{1, 2, ..., n\}$.

Relatively Prime Integers: Integers a and b and said to be relatively prime (or coprime) if the greatest common divisor of a and b is equal to 1.

Division Algorithm: If $a, b \in \mathbb{Z},\ b > 0$, then there exist integers q and r such that $a = bq + r$, where $0 \leq r < b$.

Lemma: If $a = bq + r$ then $\gcd(a, b)$=$\gcd(b, r)$
Proof: If d =$\gcd(a, b) \Rightarrow d|a$ and $d|b \Rightarrow d|(a - bq)$ *i.e* $d|r$
Thus, d is a common divisor of b and r. Now claim is that d is greatest divisor. Let c be another divisor of b and r then $c|b$ and $c|r \Rightarrow c|bq + r \Rightarrow c|a$. Since $c|a$ and $c|b \Rightarrow c|d$. This implies that d is a greatest common divisor of b and r i.e $\gcd(a, b)$=$\gcd(b, r)$.

Theorem: If $a, b \in \mathbb{Z}$, (atleast one of them is not 0) then $\gcd(a, b)$ exists.

Proof: Case 1 : $b > 0$

Applying division algorithm on a, b $(b > 0)$, $\exists\ q_1, r_1 \in \mathbb{Z}$ such that

$$a = bq_1 + r_1, \quad \text{where} \quad 0 \leq r_1 < b$$

.

If $r_1 = 0$, then $a = bq_1 \Rightarrow b|a$ also $b|b \Rightarrow b|\gcd(a, b)$.

Since, $\gcd(a, b)|a$ and $\gcd(a, b)|b \quad \Rightarrow \gcd(a, b) = b$

If $r_1 > 0$, then $0 < r_1 < b$ and thus we can apply division algorithm on b and r_1.

Therefore, $\exists\ q_2, r_2 \in \mathbb{Z}$ such that

$$b = r_1q_2 + r_2, \text{ where } 0 \leq r_2 < r_1$$

If $r_2 = 0$, then $b = r_1q_2 \Rightarrow r_1|b$ also $r_1|r_1 \Rightarrow \gcd(b, r_1) = r_1$.

If $r_2 \neq 0$, we can apply division algorithm on r_1 and r_2.

Thus $\exists\ q_3, r_3 \in \mathbb{Z}$ such that

$$r_1 = r_2q_3 + r_3 \text{ where } 0 \leq r_3 < r_2$$

Now proceed till we get n such that $r_n \neq 0$, $r_{n+1} = 0$ and $\gcd(r_{n-1}, r_n) = r_n$.

We get following system of equation:

$$\begin{aligned}
a &= bq_1 + r_1 && \text{where } 0 \leq r_1 < b \\
b &= r_1q_2 + r_2 && \text{where } 0 \leq r_2 < r_1 \\
r_1 &= r_2q_3 + r_3 && \text{where } 0 \leq r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n && \text{where } 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1} + r_{n+1}(= 0)
\end{aligned}$$

Note that

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = r_n.$$

Case 2 : $b < 0$
Take $b' = -b$, then $b' > 0$. Apply division algorithm on a and b' and solve.
Note that $\gcd(a, b) = \gcd(a, b')$

Euclidean Algorithm provides a way to find the gcd of any two integers and thus proves the existance of greatest common divisor.

Theorem (Extended Euclidean Algorithm): If $a, b \in \mathbb{Z}$, then $\gcd(a, b)$ exists. Let $\gcd(a, b) = d$ then, $\exists$ integers x, y such that $d = ax + by$.
Proof: Let us suppose a set S of all linear combinations of a and b

$$S = \{ax + by |\ ax + by > 0;\ x, y \in \mathbb{Z}\}$$

One of a, b is not zero. Without loss of generality, suppose $a \neq 0$ and if $a > 0$ then $0 < a = a \cdot 1 + b \cdot 0 \in S$, if $a < 0$ then $0 < -a = a \cdot (-1) + b \cdot 0 \in S$ therefore, S is non empty set of natural numbers.

Well Ordering Principle: Any non empty subset of natural numbers has a least element.

By Well Ordering Principle, S have a least element d (say). So by definition of set S , there exists integers x and y such that $d = a \cdot x + b \cdot y$
Claim: $d = \gcd(a, b)$
Apply division algorithm on a and d, there exists integers q and r such that $a = qd + r$, where $0 \leq r < d$. We can write $r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy)$. If $r > 0$ then $r \in S$ (as r is linear combination of a and b) and $r < d$ which is a contradiction to d is the least element in S. Therefore, $r = 0$ this implies $a = qd$ i.e. $d|a$.
Similarly, apply division algorithm on b and d, there exists integers q_1 and r_1 such that $b = q_1 d + r_1$, where $0 \leq r_1 < d$.
We can write $r_1 = b - q_1 d = b - q_1(ax + by) = a(-q_1 x) + b(1 - q_1 y)$
If $r_1 > 0$ then $r_1 \in S$ (as r_1 is linear combination of a and b) and $r_1 < d$ which is again a contradiction to d is the least element in S. Therefore, $r_1 = 0$ this implies $b = q_1 d$ i.e. $d|b$
So, d is common divisor of a and b.
If c is an arbitrary positive common divisor of a and b then c divides $a \cdot u + b \cdot v$ for all $u, v \in \mathbb{Z}$. In particular, c divides $ax + by = d$ this implies $c \leq d$
So d is greatest common divisor of a and b i.e. $\gcd(a, b)$=d.

Example: Let $a = 612$, $b = 2017$, then Find $\gcd(612, 2017)$ using Euclidean Algorithm.

Solution: To compute gcd, we apply Division Algorithm on $(2017, 612)$ as :

$$2017 = 612 \cdot 3 + 181$$

Note that $\gcd(2017, 612) = \gcd(612, 181)$, we apply Division Algorithm on $(612, 181)$ as :

$$612 = 181 \cdot 3 + 69$$

Similarly $\gcd(612, 181) = \gcd(181, 69)$, we apply Division Algorithm on $(181, 69)$ as :

$$181 = 69 \cdot 2 + 43$$

Similarly $\gcd(181, 69) = \gcd(69, 43)$, we apply Division Algorithm on $(69, 43)$ as :

$$69 = 43 \cdot 1 + 26$$

Proceeding the same way

$$43 = 26 \cdot 1 + 17$$

$$26 = 17 \cdot 1 + 9$$

$$17 = 9 \cdot 1 + 8$$

$$9 = 8 \cdot 1 + 1$$

$$8 = 1 \cdot 8 + 0$$

Thus $\gcd(612, 2017) = 1$

Example: Find the greatest common divisor d of 218 and 66, and find integers x and y solving the equation $218x + 66y = d$.

Solution: To compute $\gcd(218, 66)$, we apply Division Algorithm on $(218, 66)$ as :

$$218 = 66 \cdot 3 + 20$$

Note that $\gcd(218, 66) = \gcd(66, 20)$, we apply Division Algorithm on $(66, 20)$ as :

$$66 = 20 \cdot 3 + 6$$

Similarly $\gcd(66, 20) = \gcd(20, 6)$, we apply Division Algorithm on $(20, 6)$ as :

$$20 = 6 \cdot 3 + 2$$

Similarly $\gcd(20, 6) = \gcd(6, 2)$, we apply Division Algorithm on $(6, 2)$ as :

$$6 = 2 \cdot 3 + 0$$

Thus $\gcd(218, 66) = d = 2$. To find to integers x, y such that $d = 218x + 66y$, we do the back substitution of the above steps as follows:

$$\begin{aligned} 2 &= 20 - (6 \cdot 3) \\ &= 20 - (66 - (20 \cdot 3)) \cdot 3 \\ &= 20 - (66 \cdot 3 - 20 \cdot 3 \cdot 3) \\ &= 20 \cdot (1 + 9) - 66 \cdot 3 \\ &= 20 \cdot 10 - 66 \cdot 3 \\ &= (218 - (66 \cdot 3)) \cdot 10 - 66 \cdot 3 \\ &= 218 \cdot 10 - 66 \cdot (3 \cdot 10 + 3) \\ &= 218 \cdot 10 + 66 \cdot (-33) \end{aligned}$$

Thus, $(10, -33)$ satisfies the equation $218x + 66y = d$.
We can find the other solutions.

Modular Arithmetic: Modular Arithmetic is a system of arithmetic for integers, where numbers "wrap around" when reaching a certain value, called the modulus.

Congruence: Let a and b be two integers and $n > 1$ be a positive integer. Then a and b is said to be congruent in modulo n if n divides $a - b$ and it is denoted as $a \equiv b \ (mod\ n)$.

Properties of Congruence modulo n :

1. The congruence relation is an equivalence relation.
2. $a \equiv b \ (mod\ n) \Leftrightarrow a + k \equiv b + k \ (mod\ n) \quad \forall\ k \in \mathbb{Z}$
3. $a \equiv b \ (mod\ n) \Rightarrow ka \equiv kb \ (mod\ n) \quad \forall\ k \in \mathbb{Z}$

4. $a \equiv b \ (mod\ n) \Rightarrow a^k \equiv b^k \ (mod\ n) \quad \forall\ k \in \mathbb{Z}^+ \cup \{0\}$
5. $a \equiv b \ (mod\ n) \Rightarrow p(a) \equiv p(b) \ (mod\ n) \quad \forall$ polynomials $p(x)$ with integer coefficients.
6. $a_1 \equiv b_1 \ (mod\ n)$ and $a_2 \equiv b_2 \ (mod\ n) \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \ (mod\ n)$
7. $a_1 \equiv b_1 \ (mod\ n)$ and $a_2 \equiv b_2 \ (mod\ n) \Rightarrow a_1 a_2 \equiv b_1 b_2 \ (mod\ n)$
8. $ka \equiv kb \ (mod\ n)$ such that k is coprime to $n \Rightarrow a \equiv b \ (mod\ n)$
9. $ka \equiv kb \ (mod\ kn) \Rightarrow a \equiv b \ (mod\ n)$
10. $c \equiv d \ (mod\ \phi(n))$, where ϕ is Euler's totient function $\Rightarrow a^c \equiv a^d \ (mod\ n)$, where a is coprime to n

Modular Multiplicative Inverse: Let a be an integer. Then inverse of a in modulo n exists if $\gcd(a, n) = 1$. Inverse of a in modulo n is denoted by a^{-1} and satifies $a^{-1}a \equiv 1 \ (mod\ n)$.

Fermat's Little Theorem: Let p be a prime and a be an integer, then $a^p \equiv a \ (mod\ p)$.

Proof:
Case 1 : $\gcd(p, a) \neq 1$, then $p|a$ and $a \equiv 0 \ (mod\ p)$. Hence, Fermat's Little Theorem holds.

Case 2 : $\gcd(p, a) = 1$, then p does not divide a.
Consider the set $\{a,\ 2a,\ 3a, \ldots, (p-1)a\}$.
Since p does not divide $a \Rightarrow p$ does not divide $ia \quad \forall\ 1 \leqslant i \leqslant (p-1)$.
Since $a^{-1} \ (mod\ p)$ exists , thus $ia = ja \Rightarrow i = j \quad \forall\ 1 \leqslant i, j \leqslant (p-1)$.
Thus the set $\{a,\ 2a,\ 3a,\ \ldots, (p-1)a\}$ is eqvivalent to the set $\{1,\ 2,\ 3,\ \ldots, (p-1)\}$ in $mod\ p$
Hence,

$$a(2a)(3a)\cdots((p-1)a) \equiv 1 \cdot 2 \cdot 3 \cdots p - 1 \quad (mod\ p)$$

$$\Rightarrow \quad a^{p-1}\ (p-1)! \equiv (p-1)! \quad (mod\ p)$$

Since $\gcd(i, p) = 1 \ \forall\ 1 \leqslant i \leqslant (p-1) \Rightarrow a^{p-1} \equiv 1 \quad (mod\ p)$

Euler totient function:- Let n be a positive integer. The Euler totient function $\phi(n)$ is defined to be the number of non-negative integers b less than n which are prime to n:

$$\phi(n) = |\{0 \leq b < n | (b, n) = 1\}|$$

It is easy to see that $\phi(1) = 1$ and that $\phi(p) = p - 1$ for any prime p. We can also see that for any prime power

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right)$$

The Euler totient function is "multiplicative", meaning that

$$\phi(mn) = \phi(m)\phi(n) \text{ whenever } (m, n) = 1.$$

Since every n can be written as a product of prime powers, i.e
$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$

$$\phi(n) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \dots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right) = n \prod_{p|n}\left(1 - \frac{1}{p}\right)$$

Euler's Theorem: Let a and n be positive integer such that $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \ (mod\ n)$, where $\phi(n)$ is Euler's totient function.

Proof: Consider the set $U(n) = \{x \in \mathbb{Z} |\ gcd(x, n) = 1\ and\ 1 \leqslant x \leqslant n - 1\}$. Note that $U(n)$ is a commutative group with respect to with multiplication modulo n. and order of $U(n)$ is $\phi(n)$. Also $a \in \mathbb{Z}$. Thus, by Lagrange's theorem order of a divides $\phi(n)$.
So, $\exists\ k$ such that $a^k \equiv 1 \ (mod\ n)$ and k divides $\phi(n) \Rightarrow a^{\phi(n)} \equiv 1 \ (mod\ n)$.

Note : Case 2 of Fermat's Little Theorem is a particular case of Euler's Theorem

Example: Let $p = 11$

Let $a = 2$, then $\gcd(2, 11) = 1 \quad \Rightarrow \quad 2^{(11-1)} \equiv 1 \ (mod\ 11)$

Let $a = 3$, then $\gcd(3, 11) = 1 \quad \Rightarrow \quad 3^{(11-1)} \equiv 1 \ (mod\ 11)$

Let $a = 4$, then $\gcd(4, 11) = 1 \quad \Rightarrow \quad 4^{(11-1)} \equiv 1 \ (mod\ 11)$

Let $a = 5$, then $\gcd(5, 11) = 1 \quad \Rightarrow \quad 5^{(11-1)} \equiv 1 \ (mod\ 11)$

Let $a = 6$, then $\gcd(6, 11) = 1 \quad \Rightarrow \quad 6^{(11-1)} \equiv 1 \ (mod\ 11)$

Let $a = 7$, then $\gcd(7, 11) = 1 \quad \Rightarrow \quad 7^{(11-1)} \equiv 1 \ (mod\ 11)$

Let $a = 8$, then $\gcd(8, 11) = 1 \quad \Rightarrow \quad 8^{(11-1)} \equiv 1 \ (mod\ 11)$

Let $a = 9$, then $\gcd(9, 11) = 1 \quad \Rightarrow \quad 9^{(11-1)} \equiv 1 \ (mod\ 11)$

Let $a = 10$, then $\gcd(10, 11) = 1 \quad \Rightarrow \quad 10^{(11-1)} \equiv 1 \ (mod\ 11)$

Example: Let $n = 15$, then $\phi(15) = \phi(3)\phi(5) = 2 \cdot 4 = 8$

Let $a = 2$, then $\gcd(2, 15) = 1 \quad \Rightarrow \quad 2^8 \equiv 1 \ (mod\ 15)$

Let $a = 3$, then $\gcd(3, 15) \neq 1 \quad \Rightarrow \quad 3^8 \equiv 6 \ (mod\ 15)$

Let $a = 4$, then $\gcd(4, 15) = 1 \quad \Rightarrow \quad 4^8 \equiv 1 \ (mod\ 15)$

Let $a = 5$, then $\gcd(5, 15) \neq 1 \quad \Rightarrow \quad 5^8 \equiv 10 \ (mod\ 15)$

Let $a = 6$, then $\gcd(6, 15) \neq 1 \quad \Rightarrow \quad 6^8 \equiv 6 \ (mod\ 15)$

Let $a = 7$, then $\gcd(7, 15) = 1 \quad \Rightarrow \quad 7^8 \equiv 1 \ (mod\ 15)$

Let $a = 8$, then $\gcd(8, 15) = 1 \quad \Rightarrow \quad 8^8 \equiv 1 \ (mod\ 15)$

Let $a = 9$, then $\gcd(9, 15) \neq 1 \quad \Rightarrow \quad 9^8 \equiv 6 \ (mod\ 15)$

Let $a = 10$, then $\gcd(10, 15) \neq 1 \quad \Rightarrow \quad 10^8 \equiv 10 \ (mod\ 15)$

Let $a = 11$, then $\gcd(11, 15) = 1 \quad \Rightarrow \quad 11^8 \equiv 1 \ (mod\ 15)$

Let $a = 12$, then $\gcd(12, 15) \neq 1 \quad \Rightarrow \quad 12^8 \equiv 6 \ (mod\ 15)$

Let $a = 13$, then $\gcd(13, 15) = 1 \quad \Rightarrow \quad 13^8 \equiv 1 \ (mod\ 15)$

Let $a = 14$, then $\gcd(14, 15) = 1 \quad \Rightarrow \quad 14^8 \equiv 1 \ (mod\ 15)$

Note that $U(15) = \{1,\ 2,\ 4,\ 7,\ 8,\ 11,\ 13,\ 14\}$

Example: Reduce 50^{250} $(mod\ 83)$ to a number in the range $\{0,\ 1,\ \ldots,\ 82\}$.
(Note: 83 is prime.
If you multiply out 50^{250}, here's what you get:

52714787526044456024726519219225572551424023323922008641517022
09078987540239533171017648022222644649987502681255357847020768

633259724458839379224173171678557991981506347656250000000000000
000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000

But we can simply compute it using Fermat's Theorem.
Thus, by using Fermat's Theorem, we have

$$50^{250} \equiv 50^{82\cdot 3\ +\ 4} \equiv 50^4 \equiv 2500^2 \equiv 10^2 \equiv 17\ (mod\ 83)$$

Example: Let $n = 1001$, then $\phi(1001) = \phi(7)\phi(11)\phi(13) = 6\cdot 10\cdot 12 = 720$
Let $a \in U(1001)$, then $\gcd(a, 1001) = 1$
$\Rightarrow \quad a^{\phi(1001)} \equiv a^{720} \equiv 1\ (mod\ 1001)$

Compute 9^{2883}
$9^{2883} \equiv 9^{720\cdot 4+3} \equiv (9^{720})^4 \cdot 9^3 \equiv 1^4 \cdot 9^3 \equiv 9^3 \equiv 729\ (mod\ 1001)$

Compute 2^{4400}
$2^{4400} \equiv 2^{720\cdot 6+80} \equiv (2^{720})^6 \cdot 2^{80} \equiv (2^{10})^8 \equiv 1024^8 \equiv 23^8 \equiv 562^2 \equiv 529\ (mod\ 1001)$

Linear Diophantine equation: The simplest linear diophantine equation takes the form $ax + by = c$, where a, b and c are given integers.

- The diophantine equation $ax+by = c$ has a solution (where x and y are integers) if and only if c is a multiple of the greatest common divisor of a and b.
- Moreover, if (x, y) is a solution, then the other solutions have the form $(x + \frac{bt}{d}, y - \frac{at}{d})$, where t is an arbitrary integer, and $d =\gcd(a, b)$.

Linear Congruences

Theorem: The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if d divides b, where d=gcd(a, n). If $d|b$, the it has d mutually incongruent solutions modulo n.

Corollary:

1. If gcd(a, n)= 1, then the linear congruence $ax \equiv b \pmod{n}$ has a unique solution.
2. If gcd(a, n)= d, then d incongruent solution of the equation $ax \equiv b \pmod{n}$ is given by

$$x_0,\ x_0 + \left(\frac{n}{d}\right), x_0 + 2\left(\frac{n}{d}\right), \ldots, x_0 + (d-1)\left(\frac{n}{d}\right)$$

where x_0 is the solution of $\left(\frac{a}{d}\right) x \equiv \left(\frac{b}{d}\right) \pmod{\frac{n}{d}}$.

Example 1: Solve $3x \equiv 15 \pmod{20}$
Solution: First we calculate gcd(3,20) by Euclidean Algorithm

$$\begin{aligned} 20 &= 3 \cdot 6 + 2 & q_1 = 6,\ & r_1 = 2 \\ 3 &= 2 \cdot 1 + 1 & q_2 = 1,\ & r_2 = 1 \\ 2 &= 1 \cdot 2 + 0 & q_3 = 2,\ & r_3 = 0 \end{aligned}$$

$\Longrightarrow$ gcd(3,20)=1, hence given equtaion unique solution
Therefore 3^{-1} exists in modulo 20.
apply Extended Euclidean Algorithm as follows

$$\begin{aligned} 1 &= 3 - 1(2) \\ 1 &= 3 - 1(20 - (3 \cdot 6)) \\ 1 &= 7 \cdot 3 - 20 \\ \Longrightarrow\ 3^{-1} &\equiv 7 \pmod{20} \end{aligned}$$

Now,

$$\begin{aligned} 3x &\equiv 15 \pmod{20} \\ x &\equiv 3^{-1} \cdot 15 \pmod{20} \\ x &\equiv 5 \pmod{20} \end{aligned}$$

Example 2: Solve $20x \equiv 12 \pmod{36}$
Solution: Since gcd(20,36)=4 (verify by Euclidean Algorithm)
This implies given equation has 4 solutions under modulo 36.
To calculate all the solutions of the equation $20x \equiv 12 \pmod{36}$, we will find the solution of the equation

$$\frac{20}{4}x \equiv \frac{12}{4} \left(\text{mod } \frac{36}{4}\right)$$

$$\implies 5x \equiv 3 \pmod{9}$$

Since $\gcd(5, 9) = 1$, hence 5^{-1} exist in modulo 9. And

$$5^{-1} \equiv 2 \pmod{9}$$

Now,

$$\begin{aligned} 5x &\equiv 3 \pmod{9} \\ \implies x &\equiv 5^{-1} \cdot 3 \pmod{9} \\ \implies x &\equiv 6 \pmod{9} \end{aligned}$$

Therefore $x_0 = 6$ and other solutions are given by

$$6 + \left(\frac{36}{4}\right),\ 6 + 2\left(\frac{36}{4}\right),\ 6 + 3\left(\frac{36}{4}\right)$$

i.e solutions of the linear congruence $20x \equiv 12 \pmod{36}$ are

$$x_0 = 6,\ x_1 = 15,\ x_2 = 24,\ x_3 = 33$$

Example 3: Decrypt the following ciphertext which is encrypted by Hill cipher $\mathcal{E}(m) = am \pmod{26}$ over the set of symbols $\mathcal{A} = \{A = 0, B = 1, \ldots, Z = 25\}$. $|\mathcal{A}| = 26$

"KAFVMKAFYGC YC FVM HANSIASM QP FVM INYLMZCM"

where 'a' is the solution of following congruence equation

$$2x \equiv 6 \pmod{26}$$

Solution: To decrypt the message we will find the solutions of the given linear equation $2x \equiv 6 \pmod{26}$
Since $\gcd(2, 26) = 2$ and $2|6$, hence linear congruence has 2 solution.
To find the solutions, first we will find the solution of the following equation

$$\frac{2}{2}x \equiv \frac{6}{2} \left(\mod \frac{26}{2}\right)$$
$$\implies x \equiv 3 \pmod{13}$$

Hence solutions of $2x \equiv 6 \pmod{26}$ are given by
$x_0 = 3, x_1 = 3 + \left(\frac{26}{2}\right) = 16$
So we have two values of a=3 and a=16
First we decrypt the cipher by taking a=16
To decrypt the Hill cipher we have to find a^{-1} under modulo 26.
Note that $\gcd(16, 26) \neq 1$, therefore inverse of 16 does not exist in modulo 26. So a=16 will not work for decryption.

Now take a=3
Since $\gcd(3, 26) = 1$, 3^{-1} exist in modulo 26 and $3^{-1} \equiv 9 \pmod{26}$
Decryption function is $\mathcal{D}(c) = a^{-1}c \equiv 9c \pmod{26}$

$$\mathcal{D}(K) = \mathcal{D}(10) = 9 \cdot 10 = 90 \equiv 12 \pmod{26} = \mathbf{M}$$
$$\mathcal{D}(A) = \mathcal{D}(0) = 9 \cdot 0 \equiv 0 \pmod{26} = \mathbf{A}$$
$$\mathcal{D}(F) = \mathcal{D}(5) = 9 \cdot 5 = 45 \equiv 19 \pmod{26} = \mathbf{T}$$

and so on.
We have plaintext
MATHEMATICS IS THE LANGUAGE OF THE UNIVERSE

System of Linear Congruence

Theorem: The system of linear congruence

$$ax + by \equiv r \pmod{n} \tag{1}$$
$$cx + dy \equiv s \pmod{n} \tag{2}$$

has unique solution modulo n whenever $\gcd(ad - bc, n) = 1$.

How to find solution of above system of congruence
Multiply by d in equation(1) and multiply by b in equation(2), we have

$$adx + bdy \equiv dr \pmod{n}$$
$$bcx + bdy \equiv bs \pmod{n}$$

Subtract the above equations, we have

$$(ad - bc)x \equiv (dr - bs) \pmod{n}$$

Suppose $a' = (ad - bc)$ and $b' = (dr - bs)$ then

$$a'x \equiv b' \pmod{n}$$

If $d|b'$ then $a'x \equiv b' \pmod{n}$ has d solutions modulo n where $\gcd(a', n) = d$
To calculate y , put the values of x in given linear congruences equation(1) and equation(2), we get values of y.
So, solution of system of linear congruences is given by order pair (x, y) which satisfies each congruence.

Example: Solve the system of linear equations

$$5x + 3y \equiv 10 \pmod{12} \tag{3}$$
$$2x + 7y \equiv 6 \pmod{12} \tag{4}$$

Solution: Note that $\gcd(5 \cdot 7 - 3 \cdot 2, 12) = \gcd(29, 12) = 1$, so solution exists.
Multiply equation(3) by 7 and equation(4) by 3 , we have

$$35x + 21y \equiv 70 \pmod{12}$$
$$6x + 21y \equiv 18 \pmod{12}$$

Subtract the above equations we have

$$\begin{aligned}(35-6)x+(21-21)y &\equiv (70-18) \pmod{12}\\ 29x &\equiv 52 \pmod{12}\\ 5x &\equiv 4 \pmod{12}\end{aligned}$$

since $\gcd(5,12)=1 \implies 5^{-1} \pmod{12}$ exists and $5^{-1}=5 \pmod{12}$
So,

$$x \equiv 5^{-1}\cdot 4 \equiv 5\cdot 4 \equiv 20 \equiv 8 \pmod{12}$$

Now put the value of x in equation(3) we have

$$\begin{aligned}5\cdot 8+3y &\equiv 10 \pmod{12}\\ 40+3y &\equiv 10 \pmod{12}\\ 3y &\equiv (10-40) \equiv -30 \pmod{12}\\ 3y &\equiv 6 \pmod{12}\end{aligned}$$

Note that gcd(3,12)=3 and 3|6, So above linear congruence has 3 solutions
To find all solutions fist we solve follwing linear congruence

$$\begin{aligned}\left(\frac{3y}{3}\right) &\equiv \left(\frac{6}{3}\right) \left(\text{mod } \frac{12}{3}\right)\\ y &\equiv 2 \pmod{4}\end{aligned}$$

Hence all 3 solutions are 2, $2+\left(\frac{12}{3}\right)$, $2+2\cdot\left(\frac{12}{3}\right)$ i.e. 2, 6, 10 modulo 12.
Solutions (x,y) for equation(3) are (8, 2), (8, 6) and (8, 10).
Now put value of $x \equiv 8 \pmod{12}$ in equation(4), we have

$$\begin{aligned}2\cdot 8+7y &\equiv 6 \pmod{12}\\ 16+7y &\equiv 6 \pmod{12}\\ 7y &\equiv (6-16) \equiv -10 \pmod{12}\\ 7y &\equiv 2 \pmod{12}\end{aligned}$$

Also, gcd(7,12)=1 and $7^{-1}=7 \pmod{12}$
So

$$y \equiv 7^{-1}\cdot 2 \equiv 7\cdot 2 \equiv 14 \pmod{12}$$

$$y \equiv 2 \pmod{12}$$

Alternate way to calculate y, Multiply equation(3) by 2 and equation(4) by 5, we have

$$\begin{aligned} 10x + 6y &\equiv 20 \pmod{12} \\ 10x + 35y &\equiv 30 \pmod{12} \end{aligned}$$

Subtract the above equations we have

$$\begin{aligned} (10-10)x + (35-6)y &\equiv (30-20) \pmod{12} \\ 29y &\equiv 10 \pmod{12} \\ 5y &\equiv 10 \pmod{12} \\ y &\equiv 5^{-1} \cdot 10 \pmod{12} \quad (\because 5^{-1} = 5 \pmod{12}) \\ y &\equiv 5 \cdot 10 \pmod{12} \\ y &\equiv 50 \equiv 2 \pmod{12} \end{aligned}$$

Hence Solution for equation(4) is (8, 2).
Note that only the pair $(x, y) = (8, 2)$ is solution for both linear congruences. Therefore solution of given system of linear congruence is (8,2) i.e $x \equiv 8 \pmod{12}$, $y \equiv 2 \pmod{12}$.

Question: Decrypt the following cipher encrypted by affine cipher

$$NDXBHO$$

Let $\mathcal{A} = \{A = 0, B = 1 \ldots, Y = 24, Z = 25, \text{blank space}(\_) = 26\}$ be set of symbols. Suppose that frequency analysis is applied on digraphs, frequency analysis on cipher text tells that the most occurring digraphs (in decreasing order) : 'ZA', 'IA', 'IW'.
Also, suppose ' E_', 'S_' , '_T' appear maximum number of time (in the descending order) in the plain text.

Solution: Divide the cipher text into digraphs
c_1=ND, c_2=XB, c_3=HO
From given Frequency analysis of Plain text and cipher text, most occurring digraph in cipher text corresponds to most occurring digraph in plain text (in dcreasing order) i.e.
$\mathcal{D}$(ZA)=E_, $\mathcal{D}$(IA)=S_ and $\mathcal{D}$(IW)=_T

$|\mathcal{A}| = 27$, we are working on digraphs so $n = 27 \times 27 = 729$
Numerical equivalents of digraphs

$$\begin{aligned}
ZA =& 25 \cdot 27^1 + 0 \cdot 27^0 = 675 \pmod{729} \\
IA =& 8 \cdot 27^1 + 0 \cdot 27^0 = 216 \pmod{729} \\
IW =& 8 \cdot 27^1 + 22 \cdot 27^0 = 238 \pmod{729} \\
E_ =& 4 \cdot 27^1 + 26 \cdot 27^0 = 134 \pmod{729} \\
S_ =& 18 \cdot 27^1 + 26 \cdot 27^0 = 512 \pmod{729} \\
_T =& 26 \cdot 27^1 + 19 \cdot 27^0 = 721 \pmod{729}
\end{aligned}$$

Decryption function of affine cipher is defined by

$$\mathcal{D}(c) = ca' + b' \pmod{n}$$

by given information we have follwing 3 equations

$$\begin{aligned}
\mathcal{D}(\text{ZA})=\text{E_} &\implies \mathcal{D}(675) = 134 \pmod{729} \ i.e. \ 675a' + b' \equiv 134 \pmod{729} - (1) \\
\mathcal{D}(\text{IA})=\text{S_} &\implies \mathcal{D}(216) = 512 \pmod{729} \ i.e. \ 216a' + b' \equiv 512 \pmod{729} - (2) \\
\mathcal{D}(\text{IW})=\text{_}T &\implies \mathcal{D}(238) = 721 \pmod{729} \ i.e. \ 238a' + b' \equiv 721 \pmod{729} - (3)
\end{aligned}$$

Subtract, equation(1) and equation(2), we have

$$\begin{aligned}
(675 - 216)a' \equiv& (134 - 512) \equiv -378 \pmod{729} \\
i.e\ 459a' \equiv& 351 \pmod{729}
\end{aligned}$$

We calculate gcd(459,729):

$$\begin{aligned}
729 =& 1 \times 459 + 270 & q_1 = 1,\ r_1 = 270 \\
459 =& 1 \times 270 + 189 & q_2 = 1,\ r_2 = 189 \\
270 =& 1 \times 189 + 81 & q_3 = 1,\ r_3 = 81 \\
189 =& 2 \times 81 + 27 & q_4 = 2,\ r_4 = 27 \\
81 =& 3 \times 27 + 0 & q_5 = 3,\ r_5 = 0
\end{aligned}$$

gcd(459,729)=27, So 459^{-1} does not exists modulo 729.
So $459a' \equiv 351 \pmod{729}$ has 27 solutions modulo 729 obtained by solution

of equation

$$\left(\frac{459a'}{27}\right) \equiv \frac{351}{27} \pmod{\frac{729}{27}} \text{ i.e. } 17a' \equiv 13 \pmod{27}$$

Note that by Extended Euclidean Algorithm $17^{-1} \equiv 8 \pmod{27}$
So

$$a' \equiv 17^{-1} \cdot 13 \pmod{27} \equiv 8 \cdot 13 \equiv 23 \pmod{27}$$

.
Hence solutions of $459a' \equiv 351 \pmod{729}$ are

$$a' \equiv 23 + 27k \pmod{729} \text{ for } k = 0, 1, 2, \ldots 26$$

In particular for $k = 13$ $a' = 374$

Now subtract equation (1) and equation(3), we have

$$\begin{aligned}(675 - 238)a' &\equiv (134 - 721) \pmod{729} \\ 437a' &\equiv -587 \pmod{729} \\ 437a' &\equiv 142 \pmod{729} \\ a' &\equiv 437^{-1} \cdot 142 \pmod{729} \quad (\text{if } 437^{-1} \pmod{729} \text{ exists})\end{aligned}$$

Apply Euclidean algorithm to calculate gcd(437,729)

$$\begin{aligned}729 &= 1 \times 437 + 292 & q_1 = 1 \quad r_1 = 292 \\ 437 &= 1 \times 292 + 145 & q_2 = 1 \quad r_2 = 145 \\ 292 &= 2 \times 145 + 2 & q_3 = 2 \quad r_3 = 2 \\ 145 &= 72 \times 2 + 1 & q_4 = 72 \quad r_4 = 1 \\ 2 &= 2 \times 1 + 0 & q_5 = 2 \quad r_5 = 0\end{aligned}$$

gcd(437,729)=1, hence $437^{-1} \pmod{729}$ exists
and

$$437^{-1} = 362 \pmod{729} \text{ (by Extended Euclidean Algorithm)}$$

$437a' \equiv 142 \pmod{729}$ has unique solution.

$$a' \equiv 437^{-1} \cdot 142 \equiv 362 \cdot 142 \equiv 51404 \equiv 374 \pmod{729}$$

Now put the value of $a' = 374 \pmod{729}$ in equation(1),(2),(3)

$$\begin{aligned} b' \equiv & 134 - (675 \cdot 374) \equiv 647 \pmod{729} \quad \text{From equation (1)} \\ b' \equiv & 512 - (216 \cdot 374) \equiv 647 \pmod{729} \quad \text{From equation (2)} \\ b' \equiv & 721 - (238 \cdot 374) \equiv 647 \pmod{729} \quad \text{From equation (3)} \end{aligned}$$

So solution of system of linear equation (1),(2) and (3) is

$$a' = 374 \pmod{729} \quad b' = 647 \pmod{729}$$

We have cipher text c_1=ND, c_2=XB, c_3=HO, Decryption key is $(a',\ b')$=(374, 647) and decryption function is $\mathcal{D}(c) = a'c + b' \equiv 374 \cdot c + 647 \pmod{729}$

$$\begin{aligned} c_1 = ND = & 13 \cdot 27^1 + 3 \cdot 27^0 = 354 \pmod{729} \\ c_2 = XB = & 23 \cdot 27^1 + 1 \cdot 27^0 = 622 \pmod{729} \\ c_3 = HO = & 7 \cdot 27^1 + 14 \cdot 27^0 = 203 \pmod{729} \end{aligned}$$

decryptions are

$$\begin{aligned} \mathcal{D}(c_1) = & \mathcal{D}(354) = 374 \cdot 354 + 647 \equiv 365 \pmod{729} = 13 \cdot 27^1 + 14 \cdot 27^0 = \text{NO} \\ \mathcal{D}(c_2) = & \mathcal{D}(622) = 374 \cdot 622 + 647 \equiv 724 \pmod{729} = 26 \cdot 27^1 + 22 \cdot 27^0 = \_\text{W} \\ \mathcal{D}(c_3) = & \mathcal{D}(203) = 374 \cdot 203 + 647 \equiv 24 \pmod{729} = 0 \cdot 27^1 + 24 \cdot 27^0 = \text{AY} \end{aligned}$$

Therefore decrypted text is **"NO_WAY"** i.e **"NO WAY"**

Chinese Remainder Theorem:

Statement: Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ and $m_1, m_2, \ldots, m_n \in \mathbb{Z}$ such that

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

and $m_1, m_2, \ldots, m_n$ are pairwise relatively prime, then there exist a unique solution *modulo* m where $m = m_1 m_2 \cdots m_n$.

Proof: Write $m = \prod_{i=1}^{n} m_i$ and $M_i = \frac{m}{m_i}$
Observe that $(M_i, m_i) = 1 \ \forall i = 1, 2, \ldots, n$.
So $y_i \equiv M_i^{-1} \pmod{m_i}$ exist $\forall i = 1, 2, \ldots, n$ i.e $y_i M_i \equiv 1 \pmod{m_i} \ \forall i = 1, 2, \ldots, n$.
Let $x = \sum_{i=1}^{n} a_i y_i M_i \pmod{m}$.
We claim that x is a solution of the system of congruence, $x \equiv a_i \pmod{m_i} \ \forall i = 1, 2, \ldots, n$.

For $x = \sum_{i=1}^{n} a_i y_i M_i \pmod{m}$

$$\implies x = mk + \sum_{i=1}^{n} a_i y_i M_i \quad \text{for some } k \in \mathbb{Z}$$

$$\implies x \equiv \sum_{i=1}^{n} a_i y_i M_i \pmod{m_i} \quad \forall i = 1, 2, \ldots, n \quad (\text{Since } m_i | mk)$$

$$\implies x \equiv a_i y_i M_i \pmod{m_i} \quad \forall i = 1, 2, \ldots, n \quad (\text{Since } m_i | M_j \text{ for } i \neq j)$$

$$\implies x \equiv a_i \pmod{m_i} \quad \forall i = 1, 2, \ldots, n \quad (\text{Since } y_i M_i \equiv 1 \pmod{m_i})$$

Example:

Solve the simultaneous congruences

$$x \equiv 3 \pmod{5},$$
$$x \equiv 1 \pmod{7},$$
$$x \equiv 6 \pmod{8}$$

Solution: Since $5, 7, 8$ are pairwise relatively prime, the Chinese Remainder Theorem tells us that there is a unique solution modulo m, where $m = 5 \cdot 7 \cdot 8 = 280$.
Let $a_1 = 3, m_1 = 5, a_2 = 1, m_2 = 7, a_3 = 6, m_3 = 8$.
Now

$$M_1 = \frac{m}{m_1} = \frac{280}{5} = 56$$

$$M_2 = \frac{m}{m_2} = \frac{280}{7} = 40$$

$$M_3 = \frac{m}{m_3} = \frac{280}{8} = 35$$

$$\begin{aligned}
y_1 &\equiv M_1^{-1} \pmod{m_1} \equiv 56^{-1} \pmod 5 \equiv 1^{-1} \pmod 5 \equiv 1 \pmod 5 \\
y_2 &\equiv M_2^{-1} \pmod{m_2} \equiv 40^{-1} \pmod 7 \equiv 5^{-1} \pmod 7 \equiv 3 \pmod 7 \\
y_3 &\equiv M_3^{-1} \pmod{m_3} \equiv 35^{-1} \pmod 8 \equiv 3^{-1} \pmod 8 \equiv 3 \pmod 8
\end{aligned}$$

The solution, which is unique modulo 280, is

$$\begin{aligned}
x &\equiv a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3 \pmod m \\
x &\equiv 3 \cdot 1 \cdot 56 + 1 \cdot 3 \cdot 40 + 6 \cdot 3 \cdot 35 \pmod{280} \\
x &\equiv 78 \pmod{280}
\end{aligned}$$

Lecture-6

Modern Cryptography and Quadratic Residue

So far, we have studied some classical cipher. There are many other classical ciphers we have not learned. Classical ciphers are not secure with present advanced technologies. Now a days, Classical ciphers are not in use. Cryptographers have developed modern encryption techniques that are secure with modern technology, especially Public Key Cryptosystem. In classical ciphers, encryption and decryption keys are the same and known to sender and receiver both and no one else for secure communication.

Public Key Cryptosystem: In Public Key Cryptosystem, two keys are used, one public key and a second private key. The public key is used for encryption, and the private key is used for decryption.
Suppose Alice needs some information from Bob, then Alice will make two keys, one public and one private. The public key will be known to all, but the private key will not be known to anyone (not even to Bob) except Alice. Now anyone can send an encrypted message (encryption using Alice's public key) to Alice, and encrypted messages are public. But only Alice can decrypt the message with her private key.

In this lecture, we will study some modern cryptography, especially public-key cryptography.

Silver Pohlig - Hellman Exponentiation Cipher

Let p be a prime and e (called exponent) an integer such that $0 < e < p$ and $\gcd(e, p-1) = 1$.

Encryption: The encryption function is defined by

$$\begin{aligned} \mathcal{E} \colon \mathbb{Z}_p &\longrightarrow \mathbb{Z}_p \\ m &\longmapsto c = \mathcal{E}(m) \equiv m^e \pmod{p} \end{aligned}$$

Decryption: The decryption function is defined by

$$\begin{aligned} \mathcal{D} \colon \mathbb{Z}_p &\longrightarrow \mathbb{Z}_p \\ c &\longmapsto \mathcal{D}(c) \equiv c^d \pmod{p} \end{aligned}$$

Where $d \equiv e^{-1} \pmod{(p-1)}$, such d exists since $\gcd(e, p-1) = 1$ and can be determined by using Extended Euclidean Algorithm.

Now observe that, If $c = \mathcal{E}(m)$ then $c \equiv m^e \pmod{p}$.
Therefore $\mathcal{D}(c) \equiv c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{1+k(p-1)} \equiv m(m^{p-1})^k \pmod{p}$
for some $k \in \mathbb{Z}$, since $ed \equiv 1 \pmod{(p-1)}$.
This gives that $\mathcal{D}(c) \equiv c^d \equiv m \pmod{p}$ as $m^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem.

Example: Discuss Encryption and Decryption of the plain text.

HELLO HOW ARE YOU?

Solution:
Encrption: To encrypt this message take
$\mathcal{A} = \{\ A = 0, B = 1, \ldots, Z = 25, \_ = 26, ? = 27,\ . = 28\}$
So $p = 29 = |\mathcal{A}|$ and take $e = 3$.

Observe that $\gcd(e, p-1) = 1$ i.e $(3, 28) = 1$.

$$\begin{aligned}\mathcal{E}(H) = \mathcal{E}(7) &= 7^3 \pmod{29} \\ &= 343 \pmod{29} \\ &= 24 \pmod{29} = \mathbf{Y}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(E) = \mathcal{E}(4) &\equiv 4^3 \pmod{29} \\ &\equiv 64 \pmod{29} \\ &\equiv 6 \pmod{29} = \mathbf{G}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(L) = \mathcal{E}(11) &\equiv 11^3 \pmod{29} \\ &\equiv 1331 \pmod{29} \\ &\equiv 26 \pmod{29} = \_\end{aligned}$$

$$\begin{aligned}\mathcal{E}(O) = \mathcal{E}(14) &\equiv 14^3 \pmod{29} \\ &\equiv 2744 \pmod{29} \\ &\equiv 18 \pmod{29} = \mathbf{S}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(\_) = \mathcal{E}(26) &\equiv 26^3 \pmod{29} \\ &\equiv (-3)^3 \pmod{29} \\ &\equiv 2 \pmod{29} = \mathbf{C}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(W) = \mathcal{E}(22) &= 22^3 \pmod{29} \\ &\equiv (-7)^3 \pmod{29} \\ &\equiv 5 \pmod{29} = \mathbf{F}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(A) = \mathcal{E}(0) &\equiv 0^3 \pmod{29} \\ &\equiv 0 \pmod{29} = \mathbf{A}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(R) = \mathcal{E}(17) &\equiv 17^3 \pmod{29} \\ &\equiv 4913 \pmod{29} \\ &\equiv 12 \pmod{29} = \mathbf{M}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(Y) = \mathcal{E}(24) &\equiv 24^3 \pmod{29} \\ &\equiv (-5)^3 \pmod{29} \\ &\equiv 20 \pmod{29} = \mathbf{U}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(U) = \mathcal{E}(20) &\equiv 20^3 \pmod{29} \\ &\equiv (-9)^3 \pmod{29} \\ &\equiv 25 \pmod{29} = \mathbf{Z}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(?) = \mathcal{E}(27) &\equiv 27^3 \pmod{29} \\ &\equiv (-2)^3 \pmod{29} \\ &\equiv 21 \pmod{29} = \mathbf{V}\end{aligned}$$

Encrypted message is **YG_ _SCYSFCAMGCUSZV**

Decryption: For decryption we have to find d.
We know that $d \equiv e^{-1} \pmod{(p-1)}$. Here $e = 3, p = 29$.

$$\begin{aligned}d &\equiv 3^{-1} \pmod{28} \\ d &\equiv 19 \pmod{28}\end{aligned}$$

$$
\begin{aligned}
\mathcal{D}(Y) = \mathcal{D}(Y) &\equiv 24^{19} \pmod{29} \\
24 &\equiv (-5) \pmod{29} \\
24^2 &\equiv 25 \equiv (-4) \pmod{29} \\
24^4 &\equiv 16 \pmod{29} \\
24^6 &\equiv (-64) \equiv (-6) \pmod{29} \\
24^7 &\equiv 1 \pmod{29} \\
24^{14} &\equiv 1 \pmod{29} \\
24^{18} &\equiv 16 \pmod{29} \\
24^{19} &\equiv (-80) \equiv 7 \pmod{29} = \mathbf{H}
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{D}(G) = \mathcal{D}(G) &\equiv 6^{19} \pmod{29} \\
6^2 &\equiv 7 \pmod{29} \\
6^3 &\equiv 13 \pmod{29} \\
6^4 &\equiv 20 \pmod{29} \\
6^7 &\equiv 1 \pmod{29} \\
6^{14} &\equiv 1 \pmod{29} \\
6^{19} &\equiv 4 \pmod{29} = \mathbf{E}
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{D}(\_) = \mathcal{D}(\_) &\equiv 26^{19} \pmod{29} \\
26 &\equiv (-3) \pmod{29} \\
26^3 &\equiv (-27) \equiv 2 \pmod{29} \\
26^{18} &\equiv 6 \pmod{29} \\
26^{19} &\equiv 11 \pmod{29} = \mathbf{L}
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{D}(S) = \mathcal{D}(S) &\equiv 18^{19} \pmod{29} \\
18 &\equiv (-11) \pmod{29} \\
18^2 &\equiv 5 \pmod{29} \\
18^4 &\equiv (-4) \pmod{29} \\
18^7 &\equiv (-12) \pmod{29} \\
18^{14} &\equiv (-1) \pmod{29} \\
18^{18} &\equiv 4 \pmod{29} \\
18^{19} &\equiv 14 \pmod{29} = \mathbf{O}
\end{aligned}
$$

$$\begin{aligned}
\mathcal{D}(C) = \mathcal{D}(C) &\equiv 2^{19} \pmod{29} \\
2^7 &\equiv 12 \pmod{29} \\
2^{14} &\equiv (-1) \pmod{29} \\
2^{19} &\equiv 26 \pmod{29} = _
\end{aligned}$$

$$\begin{aligned}
\mathcal{D}(F) = \mathcal{D}(F) &\equiv 5^{19} \pmod{29} \\
5^2 &\equiv (-4) \pmod{29} \\
5^4 &\equiv 16 \pmod{29} \\
5^7 &\equiv (-1) \pmod{29} \\
5^{14} &\equiv 1 \pmod{29} \\
5^{19} &\equiv 22 \pmod{29} = \mathbf{W}
\end{aligned}$$

$$\mathcal{D}(A) = \mathcal{D}(A) = 0^{19} \pmod{29} = \mathbf{A}$$

$$\begin{aligned}
\mathcal{D}(M) = \mathcal{D}(M) &\equiv 12^{19} \pmod{29} \\
12^2 &\equiv (-1) \pmod{29} \\
12^{18} &\equiv (-1) \pmod{29} \\
12^{19} &\equiv 17 \pmod{29} = \mathbf{R}
\end{aligned}$$

$$\begin{aligned}
\mathcal{D}(U) = \mathcal{D}(U) &\equiv 20^{19} \pmod{29} \\
20 &\equiv (-9) \pmod{29} \\
20^2 &\equiv (-6) \pmod{29} \\
20^4 &\equiv 7 \pmod{29} \\
20^7 &\equiv 1 \pmod{29} \\
20^{14} &\equiv 1 \pmod{29} \\
20^{19} &\equiv 24 \pmod{29} = \mathbf{Y}
\end{aligned}$$

$$\begin{aligned}
\mathcal{D}(Z) = \mathcal{D}(Z) &\equiv 25^{19} \pmod{29} \\
25 &\equiv (-4) \pmod{29} \\
25^2 &\equiv 16 \pmod{29} \\
25^4 &\equiv (-5) \pmod{29} \\
25^7 &\equiv 1 \pmod{29} \\
25^{14} &\equiv 1 \pmod{29} \\
25^{19} &\equiv 20 \pmod{29} = \mathbf{U}
\end{aligned}$$

$$\begin{aligned}
\mathcal{D}(V) = \mathcal{D}(V) &\equiv 21^{19} \pmod{29} \\
21 &\equiv (-8) \pmod{29} \\
21^2 &\equiv 6 \pmod{29} \\
21^4 &\equiv 7 \pmod{29} \\
21^7 &\equiv 12 \pmod{29} \\
21^{14} &\equiv (-1) \pmod{29} \\
21^{19} &\equiv 27 \pmod{29} = \mathbf{?}
\end{aligned}$$

Decryption of cipher text is **HELLO HOW ARE YOU?**

Silver Pohlig - Hellman Exponentiation Cipher was developed in 1976. This is not considered to be a public-key cryptosystem because the public key and private key are the same, which is $(p,\ e)$.
From the idea of Silver Pohlig - Hellman Exponentiation, RSA cryptosystem was developed, which is the most secure public-key cryptosystem till today.

RSA Cryptosystem

RSA cryptosystem (from the last names of the inventors' Rivest, Shamir, and Adleman) was developed after one year of Silver Pohlig - Hellman Exponentiation Cipher in 1977, which is one of the most popular public-key cryptosystems, is based on the tremendous difficulty of factorization of integers.

Encryption and Decryption Techniques : Let p and q be two distinct large prime numbers and the product $n = pq$. Also let e such that $0 < e < n$ and $\gcd(e, \phi(n)) = 1$ i.e $\gcd(e, (p-1)(q-1)) = 1$.
Now (p, q) is private key and make (n, e) public key.
Encryption: The encryption function is defined by

$$\begin{aligned} \mathcal{E} &: \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \\ & m \longmapsto c = \mathcal{E}(m) \equiv m^e \pmod{n} \end{aligned}$$

Decryption: The decryption function is defined by

$$\begin{aligned} \mathcal{D} &: \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \\ & c \longmapsto m = \mathcal{D}(c) \equiv c^d \pmod{n} \end{aligned}$$

where $d \equiv e^{-1} \pmod{(p-1)(q-1)}$ exists, since $\gcd(e, (p-1)(q-1)) = 1$

Recall

1. **Euler totient function:-** Let n be a positive integer. The Euler totient function $\phi(n)$ is defined to be the number of non-negative integers b less than n which are prime to n:

$$\phi(n) = |\{0 \leq b < n |\ gcd(b, n) = 1\}|$$

2. **Euler's Theorem:-** It states that if a and n is a positive integer such that $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Validation of Encryption and Decryption
If $\mathcal{E}(m) = c \equiv m^e \pmod{n}$
Case-1 If $\gcd(m, n) = 1$ then By Eular's theorem

$$\begin{aligned} m^{\phi(n)} &\equiv 1 \pmod{n} \\ m^{(p-1)(q-1)} &\equiv 1 \pmod{n} \qquad \text{since } n = pq \end{aligned}$$

Note that $d \equiv e^{-1} \pmod{(p-1)(q-1)} \implies ed = 1 + k(p-1)(q-1)$ for some integer k.

$$\begin{aligned} \text{So,} \qquad \mathcal{D}(c) &\equiv c^d \pmod{n} \\ &\equiv (m^e)^d \pmod{n} \\ &\equiv m^{ed} \pmod{n} \equiv m^{1+k(p-1)(q-1)} \equiv m \left(m^{(p-1)(q-1)}\right)^k \equiv m \pmod{n} \end{aligned}$$

Case-2 If $\gcd(m,n) \neq 1$ then $\gcd(m,n)$ can be either p or q. So we can assume WLOG $\gcd(m,n) = q$ then $q|m$ and

$$m^r \equiv m \equiv 0 \pmod{q} \text{ for any } r > 0$$

$$\Rightarrow m^{(p-1)(q-1)} \equiv m \pmod{q}$$

Also observe that $p \nmid m$ i.e $\gcd(m,p) = 1 \Rightarrow m^{(p-1)} \equiv 1 \pmod{p}$.
Now,

$$c^d \equiv m^{ed} \equiv m^{1+k(p-1)(q-1)} \equiv m\left(m^{(q-1)}\right)^{k(p-1)} \equiv m \pmod{q}$$

$$c^d \equiv m^{ed} \equiv m^{1+k(p-1)(q-1)} \equiv m\left(m^{(p-1)}\right)^{k(q-1)} \equiv m \pmod{p}$$

So we get,

$$c^d \equiv m \pmod{q}$$

$$c^d \equiv m \pmod{p}$$

Let $c^d = x$ then we have

$$x \equiv m \pmod{q}$$

$$x \equiv m \pmod{p}$$

Since p and q are distinct primes. By chinese remainder theorem, we have

$$x \equiv m \pmod{pq}$$

i.e.

$$c^d \equiv m \pmod{pq}$$

i.e $\mathcal{D}(c) \equiv m \pmod{n}$

Example: Plain Text:- "CRYPTOGRAPHY"
$\mathcal{A} = \{A = 0, B = 1, \ldots, Z = 25, \_ = 26, ? = 27, \ . = 28, @ = 29, ! = 30, \chi = 31, \setminus = 32\}$
Let $p = 3, q = 11$ and $e = 3$, observe that $0 < e < n = 33$, $\phi(n = 3 \cdot 11) = 20$ and $\gcd(e, \phi(n)) = 1$ i.e $\gcd(3,20) = 1$

Encryption:

$$\begin{aligned}\mathcal{E}(C) = \mathcal{E}(2) &= 2^3 \pmod{33} \\ &= 8 \pmod{33} = \mathbf{I}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(R) = \mathcal{E}(17) &= 17^3 \pmod{33} \\ &= 29 \pmod{33} = \mathbf{@}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(Y) = \mathcal{E}(24) &= 24^3 \pmod{33} \\ &= 30 \pmod{33} = \mathbf{!}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(P) = \mathcal{E}(15) &= 15^3 \pmod{33} \\ &= 9 \pmod{33} = \mathbf{J}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(T) = \mathcal{E}(19) &= 19^3 \pmod{33} \\ &= 28 \pmod{33} = \mathbf{.}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(O) = \mathcal{E}(14) &= 14^3 \pmod{33} \\ &= 5 \pmod{33} = \mathbf{F}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(G) = \mathcal{E}(6) &= 6^3 \pmod{33} \\ &= 18 \pmod{33} = \mathbf{S}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(A) = \mathcal{E}(0) &= 0^3 \pmod{33} \\ &= 0 \pmod{33} = \mathbf{A}\end{aligned}$$

$$\begin{aligned}\mathcal{E}(H) = \mathcal{E}(7) &= 7^3 \pmod{33} \\ &= 13 \pmod{33} = \mathbf{N}\end{aligned}$$

Encrypted message is "I@!J.FS@AJN!"

Decryption:

$$\begin{aligned}\mathcal{D}(I) = \mathcal{D}(8) &\equiv 8^7 \pmod{33} \\ &\equiv 2 \pmod{33} = \mathbf{C}\end{aligned}$$

$$\begin{aligned}\mathcal{D}(@) = \mathcal{D}(29) &\equiv 29^7 \pmod{33} \\ &\equiv 17 \pmod{33} = \mathbf{R}\end{aligned}$$

$$\begin{aligned}\mathcal{D}(!) = \mathcal{D}(30) &\equiv 30^7 \pmod{33} \\ &\equiv 24 \pmod{33} = \mathbf{Y}\end{aligned}$$

$$\begin{aligned}\mathcal{D}(J) = \mathcal{D}(9) &\equiv 9^7 \pmod{33} \\ &\equiv 15 \pmod{33} = \mathbf{P}\end{aligned}$$

$$\begin{aligned}\mathcal{D}(.) = \mathcal{D}(28) &\equiv 28^7 \pmod{33} \\ &\equiv 19 \pmod{33} = \mathbf{T}\end{aligned}$$

$$\begin{aligned}\mathcal{D}(F) = \mathcal{D}(5) &\equiv 5^7 \pmod{33} \\ &\equiv 14 \pmod{33} = \mathbf{O}\end{aligned}$$

$$\begin{aligned}\mathcal{D}(S) = \mathcal{D}(18) &\equiv 18^7 \pmod{33} \\ &\equiv 6 \pmod{33} = \mathbf{G}\end{aligned}$$

$$\begin{aligned}\mathcal{D}(A) = \mathcal{D}(0) &\equiv 0^7 \pmod{33} \\ &\equiv 0 \pmod{33} = \mathbf{A}\end{aligned}$$

$$\begin{aligned}\mathcal{D}(N) = \mathcal{D}(13) &\equiv 13^7 \pmod{33} \\ &\equiv 7 \pmod{33} = \mathbf{H}\end{aligned}$$

Decrpted message is “CRYPTOGRAPHY”

Cryptanalysis: RSA is a Public key cryptosystem.

	Alice
Public	(n, e)
Private	(p, q)

and $n = pq$
To send a message to Alice, say the message $m \in \mathbb{Z}_n$
send her $c = m^e \pmod{n}$.
She decrypts the message $D(c) = c^d \pmod{n}$
She compute the decryption key d as

$$d = e^{-1} \pmod{(\phi(n))} = e^{-1} \pmod{(p-1)(q-1)}$$

To know d, one need to know $(p-1)(q-1) = \phi(n)$

When p and q are known then $\phi(n) = (p-1)(q-1)$ can be easily calculated.
Conversely when n and $\phi(n)$ are known then p and q can be calculated as follows

p, q are the roots of the equation

$$x^2 - (p+q)x + pq = 0$$

or that

$$x^2 - (p+q)x + n = 0$$

since $n = pq$ or

$$x^2 + (\phi(n) - n - 1)x + n = 0$$

Since $\phi(n) = pq - p - q + 1 = n - (p+q) + 1$

That is, when n and $\phi(n)$ is known then p and q are roots of the equation $x^2 + (\phi(n) - n - 1)x + n = 0$ such that $n = pq$.

Quadratic Cipher

Suppose $\mathcal{A}$ has n symbols (letters) then plain text space and cipher text space is treated as $\mathbb{Z}_n$.
Encryption: Encryption function is defined by

$$\begin{aligned}\mathcal{E}&\colon \mathbb{Z}_n \to \mathbb{Z}_n\\ &\quad m \mapsto c = \mathcal{E}(m) \equiv m^2 \pmod{n}\end{aligned}$$

Decryption: Decryption function is defined by

$$\begin{aligned}\mathcal{D}&\colon \mathbb{Z}_n \to \mathbb{Z}_n\\ &\quad c \mapsto m = \mathcal{D}(c) \equiv \sqrt{c} \pmod{n}\end{aligned}$$

provided $\sqrt{c}$ exists in $\mathbb{Z}_n$ i.e congruence equation $x^2 \equiv c \pmod{n}$ has solution in $\mathbb{Z}_n$

Example: Suppose $\mathcal{A} = \{A = 0, B = 1, \ldots Z = 25\}$, $|\mathcal{A}| = n = 26$
To encrypt : **HELLO**
Encryption :

$$\begin{aligned}\mathcal{E}(H) =& \mathcal{E}(7) = 7^2 = 49 \equiv 23 \pmod{26} = \mathbf{X}\\ \mathcal{E}(E) =& \mathcal{E}(4) = 4^2 = 16 \equiv 16 \pmod{26} = \mathbf{Q}\\ \mathcal{E}(L) =& \mathcal{E}(11) = 11^2 = 121 \equiv 17 \pmod{26} = \mathbf{R}\\ \mathcal{E}(O) =& \mathcal{E}(14) = 14^2 = 196 \equiv 14 \pmod{26} = \mathbf{O}\end{aligned}$$

So encryption of 'HELLO' is **'XQRRO'**

For decryption we have to know square root of elements of $\mathbb{Z}_n$. For that we calculate following table

a	$a^2 \pmod{26}$	a	$a^2 \pmod{26}$
0	0	13	13
1	1	14	14
2	4	15	17
3	9	16	22
4	16	17	3
5	25	18	12
6	10	19	23
7	23	20	10
8	12	21	25
9	3	22	16
10	22	23	9
11	17	24	4
12	14	25	1

Decryption function is $\mathcal{D}(c) = \sqrt{c} \pmod{26}$ i.e $\sqrt{c} = x \iff c = x^2 \pmod{26}$
To decrypt **'XQRRO'**

$$\begin{aligned}\mathcal{D}(X) = \mathcal{D}(23) =& \sqrt{23} \pmod{26} \equiv a \pmod{26}\ (say)\\ &\implies a^2 = 23 \pmod{26}\\ &\implies a = 7 \text{ or } 19 \ \text{ (from above table)}\\ \text{i.e. } \mathcal{D}(X) &= \textbf{H or T}\end{aligned}$$

$$\begin{aligned}\mathcal{D}(Q) = \mathcal{D}(16) =& \sqrt{16} \pmod{26} \equiv a \pmod{26}\ (say)\\ &\implies a^2 = 16 \pmod{26}\\ &\implies a = 4 \text{ or } 22 \ \text{ (from above table)}\\ \text{i.e. } \mathcal{D}(Q) &= \textbf{E or W}\end{aligned}$$

$$\begin{aligned}\mathcal{D}(R) = \mathcal{D}(17) =& \sqrt{17} \pmod{26} \equiv a \pmod{26}\ (say)\\ &\implies a^2 = 17 \pmod{26}\\ &\implies a = 11 \text{ or } 15 \ \text{ (from above table)}\\ \text{i.e. } \mathcal{D}(R) &= \textbf{L or P}\end{aligned}$$

$$\begin{aligned}\mathcal{D}(O) = \mathcal{D}(14) = &\sqrt{14} \pmod{26} \equiv a \pmod{26} \ (say)\\ &\implies a^2 = 14 \pmod{26}\\ &\implies a = 14 \text{ or } 12 \ \text{ (from above table)}\\ \text{i.e. } \mathcal{D}(O) = &\textbf{ O or M}\end{aligned}$$

Possible decryption of **'XQRRO'** is **"HELLO, TWPPM, HWPPM, HEPPM, HELLM, ..."**
"HELLO" is meaningful, so decryption of **'XQRRO'** is **'HELLO'**.

Note: It is possible that for some $a \in \mathbb{Z}_n$, $\sqrt{a} \pmod{n}$ does not exist.
E.g. Take $\mathbb{Z}_{26} = \{0, 1, \ldots, 25\}$
$5 \in \mathbb{Z}_{26}$, from above table we can verify that there is no $a \in \mathbb{Z}_{26}$ such that $a^2 \equiv 5 \pmod{26}$. Therefore $\sqrt{5} \pmod{26}$ does not exist.

Also, It is possible $\sqrt{a} \pmod{n}$ has more than 2 values in modulo n i.e. congruence $x^2 \equiv a \pmod{n}$ may have more than 2 solutions in modulo n.
E.g. Take $\mathbb{Z}_n = \mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$
Observe that

$$\begin{aligned}1^2 &\equiv 1 \pmod{8}\\ 3^2 &\equiv 1 \pmod{8}\\ 5^2 &\equiv 1 \pmod{8}\\ 7^2 &\equiv 1 \pmod{8}\end{aligned}$$

So congruence $x^2 \equiv 1 \pmod{8}$ has four solutions.
Therefore, $\sqrt{1} \pmod{8} = 1,\ 3,\ 5,\ 7 \pmod{8}$

Now we will see , when square root of elements exist modulo n

Quadratic Residue

An integer $a \in \mathbb{Z}$ is said to be a quadratic residue *mod* n (where n is a fixed positive integer such that $\gcd(a, n) = 1$). If the quadratic congruence

$x^2 \equiv a \pmod{n}$ has a solution. That is, if there exists $x \in \mathbb{Z}$ such that $x^2 \equiv a \pmod{n}$. If no such $x \in \mathbb{Z}$ exist, a is said to be a non-quadratic residue *mod* n.

Example: 1. 0 is quadratic residue modulo 4 since $x^2 \equiv 0 \pmod{4}$ has two solutions i.e. $x = 0,\ 2$.
2. 3 is non-quadratic residue modulo 4 since $x^2 \equiv 3 \pmod{4}$ has no solution.
3. 0 is quadratic residue modulo 9 since $x^2 \equiv 0 \pmod{9}$ has three solutions i.e. $x = 0,\ 3,\ 6$.

Recall: Fermat's little theorem: If a is positive integer such that $\gcd(a, n) = 1$ where p is prime then $a^{p-1} \equiv 1 \pmod{p}$.

Euler's Criteria: Let p be an odd prime. An integer $a \in \mathbb{Z}$ is a quadratic residue modulo p iff $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
Proof: Suppose a is quadratic residue *mod* p. So there exists $y \in \mathbb{Z}$ such that $y^2 \equiv a \pmod{p}$.
Since $\gcd(a, p) = 1 \implies p \nmid a \implies p \nmid y^2 \implies p \nmid y \implies (p, y) = 1$
Again by Fermat's little theorem

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

$$(y^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Conversely, suppose $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. We want to show that a is a quadratic residue *mod* p. That is $\gcd(a, p) = 1$ and $x^2 \equiv a \pmod{p}$ has an integer solution. Obviously $\gcd(a, p) = 1$ otherwise $p|a$

$$\implies a \equiv 0 \pmod{p} \implies a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$$

which is a contradiction.

If h is the least positive integer such that $a^h \equiv 1 \pmod{n}$ then we say that a has exponent h *modulo* n.
If g is an integer belonging to the exponent $\phi(n)$ then g is called a primitive root *modulo* n. i.e $g^{\phi(n)} \equiv 1 \pmod{n}$ and $g^k \not\equiv 1 \pmod{n}$ $\forall 1 \leq k < \phi(n)$.
In this case g become generator of $U(\mathbb{Z}_n)$, hence $g, g^2, \ldots, g^{\phi(n)-1}$ are all incongruent *modulo* n.

Now let g be a primitive root *mod* p. So $g^{\phi(p)} \equiv 1 \pmod{p}$ and $g^k \not\equiv 1 \pmod{p}$ $\forall 1 \leq k < p-1$.
(Since $U(\mathbb{Z}_r)$ is cyclic if r is prime).
Hence $U(\mathbb{Z}_p)$ is cycllic $\implies \langle g \mid g^{p-1} = 1\rangle = U(\mathbb{Z}_p)$.
Since $a \in U(\mathbb{Z}_p)$

$$\implies a \equiv g^r \pmod{p} \text{ for some } r \in \mathbb{Z}$$

Now,

$$\begin{aligned} 1 \equiv\ & a^{\frac{p-1}{2}} \equiv (g^r)^{\frac{p-1}{2}} \pmod{p} \\ \implies & g^{\frac{r\cdot(p-1)}{2}} \equiv 1 \pmod{p} \\ \implies & (p-1) \mid \frac{r}{2} \cdot (p-1) \qquad \because \mid U(\mathbb{Z}_p) \mid = p-1 \\ \implies & \frac{r}{2} \in \mathbb{Z} \end{aligned}$$

Take $y = g^s$ where $s = \frac{r}{2}$ this gives $y^2 = g^{2s} = g^r \equiv a \pmod{p}$.

Since $y \in \mathbb{Z}$ such that $y^2 \equiv a \pmod{p}$. We get a is a quadratic residue *mod* p.

Note: Recall that if $p = 2$ and $\gcd(a, p) = 1$ then $a \equiv 1 \pmod{2}$ i.e a is an odd integer. The congruence will be $x^2 \equiv 1 \pmod{2}$, and also has a solution $x \equiv 1 \mod 2$.

Theorem: Let p be a prime of the form $p = 4k+3$ for some $k \in \{0\} \cup \mathbb{N}$. If $a \in \mathbb{Z}$ such that $p \nmid a$ i.e $\gcd(a, p) = 1$ and if $x^2 \equiv a \pmod{p}$ has a solution $x \in \mathbb{Z}$, then all the solutions are $x = \pm a^{\frac{p+1}{4}}$.

Proof: Since x is a solution of $x^2 \equiv a \pmod{p}$ and $\gcd(a, p) = 1$, we get 'a' to be quadratic residue *mod* p.
By Euler's Criteria, therefore

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Since $p = 4k+3$

$$\implies \frac{p+1}{4} = \frac{4k+3+1}{4} = k+1 \in \mathbb{Z}$$

Now

$$\begin{aligned}\left(\pm a^{\frac{p+1}{4}}\right)^2 &\equiv a^{\frac{p+1}{2}} \pmod p \\ &\equiv a^{\frac{p+1}{2}} \cdot 1 \pmod p \\ &\equiv a^{\frac{p+1}{2}} \cdot a^{\frac{p-1}{2}} \pmod p \\ &\equiv a^p \pmod p \\ &\equiv a \cdot a^{p-1} \pmod p \\ &\equiv a \pmod p \qquad \text{(By Fermat's little theorem)}\end{aligned}$$

Hence $x \equiv \pm a^{\frac{p+1}{4}} \pmod p$ are solutions.
Then two solution namely $x \equiv a^{\frac{p+1}{4}} \pmod p$ and $x \equiv -a^{\frac{p+1}{4}} \pmod p$ are incongruent *mod p*.
Since $x^2 \equiv a \pmod p$ is a quadratic congruence. It can not have more than two incongruent solutions and therefore if the congruence $x^2 \equiv a \pmod p$ has a solution then $x \equiv \pm a^{\frac{p+1}{4}} \pmod p$ are all the solutions.

$**END**$

Lecture-7

Euler's Criteria: Let p be an odd prime. An integer $a \in \mathbb{Z}$ is a quadratic residue modulo p iff $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
Proof: Suppose a is quadratic residue *mod* p. So there exists $y \in \mathbb{Z}$ such that $y^2 \equiv a \pmod{p}$.
Since $\gcd(a,p) = 1 \implies p \nmid a \implies p \nmid y^2 \implies p \nmid y \implies \gcd(p,y) = 1$
Again by Fermat's little theorem

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

$$(y^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Conversely, suppose $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. We want to show that a is a quadratic residue *mod* p. That is $\gcd(a,p) = 1$ and $x^2 \equiv a \pmod{p}$ has an integer solution. Obviously $\gcd(a,p) = 1$ otherwise $p|a$

$$\implies a \equiv 0 \pmod{p} \implies a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$$

which is a contradiction. Hence $\gcd(a,p) = 1$. Now we will show that $x^2 \equiv a \pmod{p}$ has an integer solution.

Recall: If h is the least positive integer such that $a^h \equiv 1 \pmod{n}$ then we say that a has exponent h *modulo* n.
If g is an integer belonging to the exponent $\phi(n)$ then g is called a primitive root *modulo* n. i.e $g^{\phi(n)} \equiv 1 \pmod{n}$ and $g^k \not\equiv 1 \pmod{n}$ $\forall 1 \leq k < \phi(n)$.
In this case g becomes generator of $U(\mathbb{Z}_n)$, hence $g, g^2, \ldots, g^{\phi(n)-1}$ are all incongruent *modulo* n.

Now let g be a primitive root *mod* p. So $g^{\phi(p)} \equiv 1 \pmod{p}$ and $g^k \not\equiv$

$1 \pmod p$ $\forall 1 \leq k < p-1$.
Let us assume that $1 \leq a \leq p-1$.
(Since $U(\mathbb{Z}_r)$ is cyclic if r is prime).
Hence $U(\mathbb{Z}_p)$ is cyclic $\implies \langle g \mid g^{p-1} = 1 \rangle = U(\mathbb{Z}_p)$.
Since $a \in U(\mathbb{Z}_p)$

$$\implies a \equiv g^r \pmod p \text{ for some } r \in \mathbb{Z}$$

Now,

$$\begin{aligned} 1 \equiv\ & a^{\frac{p-1}{2}} \equiv (g^r)^{\frac{p-1}{2}} \pmod p \\ \implies & g^{\frac{r\cdot(p-1)}{2}} \equiv 1 \pmod p \\ \implies & (p-1) \mid \frac{r}{2} \cdot (p-1) \qquad \because \mid U(\mathbb{Z}_p) \mid = p-1 \\ \implies & \frac{r}{2} \in \mathbb{Z} \end{aligned}$$

Take $y = g^s$ where $s = \frac{r}{2}$ this gives $y^2 = g^{2s} = g^r \equiv a \pmod p$.

Since $y \in \mathbb{Z}$ such that $y^2 \equiv a \pmod p$. We get a is a quadratic residue *mod p*.

Note: Recall that if $p = 2$ and $\gcd(a, p) = 1$ then $a \equiv 1 \pmod 2$ i.e a is an odd integer. The congruence will be $x^2 \equiv 1 \pmod 2$, and also has a solution $x \equiv 1 \mod 2$.

Theorem 1: Let p be a prime of the form $p = 4k+3$ for some $k \in \{0\} \cup \mathbb{N}$. If $a \in \mathbb{Z}$ such that $p \nmid a$ i.e $\gcd(a, p) = 1$ and if $x^2 \equiv a \pmod p$ has a solution $x \in \mathbb{Z}$, then all the solutions are $x = \pm a^{\frac{p+1}{4}}$.

Proof: Since x is a solution of $x^2 \equiv a \pmod p$ and $\gcd(a, p) = 1$, we get 'a' to be quadratic residue *mod p*.
By Euler's Criteria, therefore

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

Since $p = 4k+3$

$$\implies \frac{p+1}{4} = \frac{4k+3+1}{4} = k+1 \in \mathbb{Z}$$

Now

$$\begin{aligned}\left(\pm a^{\frac{p+1}{4}}\right)^2 &\equiv a^{\frac{p+1}{2}} \pmod p \\ &\equiv a^{\frac{p+1}{2}} \cdot 1 \pmod p \\ &\equiv a^{\frac{p+1}{2}} \cdot a^{\frac{p-1}{2}} \pmod p \\ &\equiv a^p \pmod p \\ &\equiv a \cdot a^{p-1} \pmod p \\ &\equiv a \pmod p \qquad \text{(By Fermat's little theorem)}\end{aligned}$$

Hence $x \equiv \pm a^{\frac{p+1}{4}} \pmod p$ are solutions.
Then two solution namely $x \equiv a^{\frac{p+1}{4}} \pmod p$ and $x \equiv -a^{\frac{p+1}{4}} \pmod p$ are incongruent *mod p*.
Since $x^2 \equiv a \pmod p$ is a quadratic congruence under modulo p(prime). It can not have more than two incongruent solutions and therefore if the congruence $x^2 \equiv a \pmod p$ has a solution then $x \equiv \pm a^{\frac{p+1}{4}} \pmod p$ are all the solutions.

Theorem 2: If $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ $(a_n \not\equiv 0 \pmod p)$ has a solution, then the number of mutually incongruent *modulo p* solution is at most n.
Proof: By induction on n (the degree of $f(x)$).
If $n = 0$, then $f(x) = a_0 \not\equiv 0 \pmod p$. But then $f(x) \equiv 0 \pmod p$ has no solution.
If $n = 1$ then $f(x) = a_1 x + a_0,\ a_1 \not\equiv 0 \pmod p$. But $f(x) \equiv 0 \pmod p$ becomes $a_1 x + a_0 \equiv 0 \pmod p$

$$\begin{aligned}\implies a_1 x &\equiv -\, a_0 \pmod p \\ \implies x &\equiv -{a_1}^{-1} a_0 \pmod p\end{aligned}$$

Since $-{a_1}^{-1}$ is unique. We get $f(x) \equiv 0 \pmod p$ has at most 1 solution.

We assume that theorem holds for all polynomial of degree less than k(say).

Now let $f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$ $(a_k \not\equiv 0 \pmod p)$ be such that $f(x) \equiv 0 \pmod p$ has $k+1$ incongruent *modulo p* solution say

$$x = \omega_1, \omega_2, \ldots, \omega_{k+1} \pmod p$$

Let

$$g(x) = f(x) - a_k(x-\omega_1)(x-\omega_2)\cdots(x-\omega_k)$$

Then $g(x)$ is a polynomial of degree less than k.
By induction hypothesis $g(x) \equiv 0 \pmod{p}$ can have at most $(k-1)$ (incongruent *modulo* p) solution. But $g(x)$ has k incongruent *modulo* p solution $\omega_1, \omega_2, \ldots, \omega_k$. So $g(x) \equiv 0, \pmod{p}\ \forall x \in \mathbb{Z}$.
But then for $x = \omega_{k+1}$

$$\begin{aligned}
&\implies g(\omega_{k+1}) = 0 \pmod{p} \\
&\implies 0 = g(\omega_{k+1}) = f(\omega_{k+1}) - a_k(\omega_{k+1}-\omega_1)(\omega_{k+1}-\omega_2)\ldots(\omega_{k+1}-\omega_k) \pmod{p} \\
&\implies g(\omega_{k+1}) \equiv -a_k(\omega_{k+1}-\omega_1)(\omega_{k+1}-\omega_2)\ldots(\omega_{k+1}-\omega_k) \pmod{p} \\
&\qquad\qquad (\because f(\omega_{k+1}) \equiv 0 \pmod{p}) \\
&\implies g(\omega_{k+1}) \not\equiv 0 \pmod{p} \\
&\quad \text{(Since } p \nmid a_k \text{ and } \omega_i, i = 1, 2, \ldots, k+1 \text{ are incongruent)}
\end{aligned}$$

Hence we get a contradiction since $g(x) = 0\ \forall x \in \mathbb{Z}$.
Hence $f(x) \equiv 0$ has at most k incongruent solution. This proves the theorem for $n = k$, and this completes the induction.
Hence the theorem holds for all $n \geq 0$.

Legendre Symbol

Let p be odd prime and let gcd$(a,\ p)$=1. The Legendre Symbol $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \text{ i.e. } p \text{ divides } a \\ 1 & \text{if } p \nmid a \text{ and } a \text{ is a quadractic residue modulo } p \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is a non-quadractic residue modulo } p \end{cases}$$

Example: 1. $\left(\frac{2}{3}\right) = -1$ since $x^2 \equiv 2 \pmod{3}$ has no solution i.e. 2 is non-quadratic residue modulo 3 and $3 \nmid 2$

2. $\left(\frac{0}{p}\right) = 0$

3. $\left(\frac{3}{13}\right) = 1$ since $x^2 \equiv 3 \pmod{13}$ has solutions $x = 4, 9$ i.e. 3 is quadratic residue modulo 13

Note: Legendre symbol can be defined in general for any $'n'$ instead of prime p.

Properties of Legendre Symbol
Let p be an odd prime and let a and b be integers that are relatively prime to p. Then the Legendre symbol has the following properties:
(a) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(b) $\left(\frac{a^2}{p}\right) = 1$

(c) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

(d) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(e) If p (is an odd prime), then $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ (**Eular's Criteria**)

Theorem : If p is an odd prime, then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p = 4k+1, \quad k \in \mathbb{N} \cup \{0\} \\ -1 & \text{if } p = 4k+3, \quad k \in \mathbb{N} \cup \{0\} \end{cases}$$

and

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p = 8k+1, 8k-1, \quad k \in \mathbb{N} \cup \{0\} \\ -1 & \text{if } p = 8k+3, 8k-3, \quad k \in \mathbb{N} \cup \{0\} \end{cases}$$

Gauss Law of Quadratic Reciprocity:
Let p and q be distinct odd primes

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

equivalently

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{if } p = 4k_1+3, q = 4k_2+3 \\ & \qquad k_1,\ k_2 \in \mathbb{N} \cup \{0\} \\ \left(\frac{q}{p}\right) & \text{if } p = 4k_1+1, q = 4k_2+1, \\ & \quad p = 4k_1+1, q = 4k_2+3, \\ & \quad p = 4k_1+3, q = 4k_2+1 \\ & \qquad k_1,\ k_2 \in \mathbb{N} \cup \{0\} \end{cases}$$

Example: Check whether the congruence $x^2 \equiv -46 \pmod{17}$ has solutions.
Solution: We will use Legendre symbol to find solution exist or not.
Note that $17 \nmid -46$
By definition of Legendre symbol
If $\left(\frac{-46}{17}\right) = 1$ then -46 is a quadratic residue modulo 17 i.e. it has solution.
If $\left(\frac{-46}{17}\right) = -1$ then -46 is a non-quadratic residue modulo 17 i.e. it has no solution.
So we have to find

$$\left(\frac{-46}{17}\right) = ?$$

By property (d) we have

$$\begin{aligned} \left(\frac{-46}{17}\right) &= \left(\frac{-1}{17}\right)\left(\frac{46}{17}\right) \\ &= (1)\left(\frac{46}{17}\right) = \left(\frac{46}{17}\right) \quad (\text{ by above theorem }) \end{aligned}$$

Also

$$46 \equiv 12 \pmod{17} \implies \left(\frac{46}{17}\right) = \left(\frac{12}{17}\right) \quad (\text{by property (a)})$$

$$\begin{aligned} \left(\frac{12}{17}\right) &= \left(\frac{2^2 \cdot 3}{17}\right) \\ &= \left(\frac{2^2}{17}\right)\left(\frac{3}{17}\right) = \left(\frac{3}{17}\right) \end{aligned}$$

since $\left(\frac{2^2}{17}\right) = 1$ by property (b)

Now by property (c) we have

$$\begin{aligned}\left(\frac{3}{17}\right) \equiv & 3^{\frac{17-1}{2}} \pmod{17} \equiv 3^8 \equiv (3^4)^2 \pmod{17} \\ \equiv & 81^2 \pmod{17} \equiv (-4)^2 \pmod{17} \\ \equiv & 16 \pmod{17} \\ \equiv & -1 \pmod{17}\end{aligned}$$

So

$$\left(\frac{-46}{17}\right) = -1$$

Therefore congruence $x^2 = -46 \pmod{17}$ has no solution.

Theorem 3: There are infinitely many primes of the form $4k + 1$ for $k \in \mathbb{N}$.

Proof: Let there are only finitely many primes of the form $4k + 1$ namely $p_1, p_2, \ldots, p_n$.

To prove the theorem it is sufficient to show that there is a prime p of the form $4k + 1$ and $p \neq p_i$ for $i = 1, 2, \ldots, n$.

Let

$$N = (2p_1p_2 \cdots p_n)^2 + 1$$

Observe that N is odd and greater than 1. Therefore N has an odd prime divisor p (say).

If $p = p_i$ for some $i = 1, 2, \ldots, n$ then $p_i \mid N$ and $p_i \mid (2p_1p_2 \cdots p_n)^2$ this implies $p_i \mid N - (2p_1p_2 \cdots p_n)^2 = 1$ which is not possible since p_i is prime.

Therefore $p \neq p_i$ for any $i = 1, 2, \ldots, n$.

Since $p \mid N$ therefore

$$(2p_1p_2 \cdots p_n)^2 \equiv -1 \pmod{p} \qquad (1)$$

Also $\gcd((2p_1p_2 \cdots p_n), p) = 1$, by Fermat's Little Theorem

$$(2p_1p_2 \cdots p_n)^{p-1} \equiv 1 \pmod{p}$$

$$\left((2p_1p_2 \cdots p_n)^2\right)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

From (1), we have

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \qquad (2)$$

Since p is prime so it can be of the form $4k+1$ or $4k+3$.

If p is of the form $4k+3$ then $\frac{p-1}{2} = 2k+1$ is odd and therefore from (2) we have

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

which is not possible since p is odd.
Therefore p must be of the form $4k+1$.
So we have a prime p of the form $4k+1$ and $p \neq p_i$ for $i = 1, 2, \ldots, n$. Hence there are infinitely many primes of the form $4k+1$.

Remark: If p, q are primes of the form $4k+1$, then pq is also of the same form.

$$\begin{aligned}(4k_1+1)(4k_2+1) &= 4\{k_1(4k_2+1)\} + (4k_2+1) \\ &= 4\{k_1(4k_2+1)\} + 4k_2 + 1 \\ &= 4\{k_1(4k_2+1) + k_2\} + 1 \\ &= 4k_3 + 1\end{aligned}$$

Theorem 4: There are infinitely many primes of the form $4k+3$ for $k \in \mathbb{N}$.
Proof: Let the primes of the form $4k+3$ are finitely many namely $p_1, p_2, \ldots, p_n$.
WLOG, we may assume that $p_1 = 3, p_2 = 7, \ldots$ and that $p_1 < p_2 < \cdots < p_n$.
Each $p_2, p_3, \ldots, p_n$ is greater then 3.
Let

$$N = 4(p_2 \cdot p_3 \cdots p_n) + 3$$

N is either a prime of the form $4k+3$, which it can not be as $N > p_n$ and p_n is the largest such prime, or a prime of the form $4k+1$ which is not possible.
So N is composite and it must contain a prime factor of the form $4k+3$.
Otherwise if all prime factors of N are of the form $4k+1$ then N will also be of the form $4k+1 \implies N \equiv 1 \pmod{4}$ which is not true.
So N contains either all prime factors of the form $4k+3$ or both $4k+1$ & $4k+3$ i.e N must contain at least one prime factor of the form $4k+3$.
If no. of factor is 1 then N itself a prime of the form $4k+3$ (Not possible

since $N >$ all $4k+3$ primes). So N has more than 1 factor of the form $4k+3$.
Now if $3|N$ then $3|N-3$

$$\begin{aligned}
&\implies 3|4(p_2 \cdot p_3 \cdots p_n) \\
&\implies 3|p_2 \cdot p_3 \cdots p_n \\
&\implies 3|p_j \text{ some } j = 2, 3, \ldots, n \quad \text{(Not possible)} \\
&\implies 3 \nmid N
\end{aligned}$$

Now if $p_j|N$ for some $j > 2$ then $p_j|N - 4(p_2 \cdot p_3 \cdots p_n)$

$$\begin{aligned}
&\implies p_j|3 \quad \text{but } p_j > 3 \\
&\implies p_j \nmid 3 \\
&\implies p_j \nmid N \ \forall j = 2, 3, \ldots, n
\end{aligned}$$

Since N has a factor p of the form $4k+3$ type. But none of $p_1, p_2, \ldots, p_n$ divides N this implies that $p \neq p_i \quad i = 1, 2, \ldots, n$. Which is a contradiction.

So there are infinitely many primes of the form $4k+3$.

Lecture-8

Rabin Cipher

Let p, q be distinct primes of the form $4k + 3$ and take $n = pq$

Encryption function is defined by

$$\begin{aligned} \mathcal{E} &: \mathbb{Z}_n \to \mathbb{Z}_n \\ & m \mapsto c = \mathcal{E}(m) \equiv m^2 \pmod{n} \end{aligned}$$

Decryption function is defined by

$$\begin{aligned} \mathcal{D} &: \mathbb{Z}_n \to \mathbb{Z}_n \\ & c \mapsto m = \mathcal{D}(c) \equiv \sqrt{c} \pmod{n} \end{aligned}$$

provided c is quadratic residue modulo n.

Example: Let $p = 11, q = 3$ be primes of the form $4k + 3$,
$n = pq = 11 \cdot 3 = 33$
Suppose $\mathcal{A} = \{A = 0, B = 1, \ldots, Z = 25, \_ = 26, ? = 27, \ . = 28, @ = 29, ! = 30, \chi = 31, \backslash = 32\}$
To encrypt: "STUDENT"

$$\begin{aligned}
\mathcal{E}(S) =& \mathcal{E}(18) = 18^2 \equiv 324 \pmod{33} \equiv 27 \pmod{33} = \textbf{?} \\
\mathcal{E}(T) =& \mathcal{E}(19) = 19^2 \equiv 361 \pmod{33} \equiv 31 \pmod{33} = \chi \\
\mathcal{E}(U) =& \mathcal{E}(20) = 20^2 \equiv 400 \pmod{33} \equiv 4 \pmod{33} = \textbf{E} \\
\mathcal{E}(D) =& \mathcal{E}(3) = 3^2 \equiv 9 \pmod{33} = \textbf{J} \\
\mathcal{E}(E) =& \mathcal{E}(4) = 4^2 \equiv 16 \pmod{33} = \textbf{Q} \\
\mathcal{E}(N) =& \mathcal{E}(13) = 13^2 \equiv 169 \pmod{33} \equiv 4 \pmod{33} = \textbf{E} \\
\mathcal{E}(T) =& \mathcal{E}(19) = 19^2 \equiv 361 \pmod{33} \equiv 31 \pmod{33} = \chi
\end{aligned}$$

So encryption of "STUDENT" is **"?χEJQEχ"**

To decrypt: "?χEJQEχ"

$$\mathcal{D}(?) = \mathcal{D}(27) \equiv \sqrt{27} \pmod{33} \equiv x \pmod{33} \text{ i.e. } x^2 \equiv 27 \pmod{33}$$

To calculate: $x^2 \equiv 27 \pmod{33}$

By **Theorem 1:** Let p be a prime of the form $p = 4k+3$ for some $k \in \{0\} \cup \mathbb{N}$. If $a \in \mathbb{Z}$ such that $p \nmid a$ i.e $\gcd(a, p) = 1$ and if $x^2 \equiv a \pmod{p}$ has a solution $x \in \mathbb{Z}$, then all the solutions are $x = \pm a^{\frac{p+1}{4}}$

Here $a = 27$ for $p = 11 = 4 \times 2 + 3$ and $\gcd(27, 11) = 1$, we have

$$x \equiv \pm 27^{\frac{11+1}{4}} \pmod{11} \equiv \pm 27^3 \pmod{11} \equiv \pm 5^3 \equiv \pm 4 \pmod{11}$$

For $a = 27$ and $p = 3 = 0 \times 4 + 3$

$$a \equiv 27 \pmod{3} \equiv 0 \pmod{3}$$

$$x^2 \equiv a \equiv 0 \pmod{3} \text{ has solution } x \equiv 0 \pmod{3}$$

Now we have

$$x \equiv 4 \pmod{11} \tag{1}$$
$$x \equiv -4 \equiv 7 \pmod{11} \tag{2}$$
$$x \equiv 0 \pmod{3} \tag{3}$$

Recall: Chinese Remainder Theorem

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

m_1 and m_2 are relatively prime then solution of above system is given by

$$x \equiv a_1 y_1 M_1 + a_2 y_2 M_2 \pmod{m_1 m_2}$$

where

$$M_1 = \frac{m_1 \cdot m_2}{m_1} = m_2, \quad M_2 = \frac{m_1 \cdot m_2}{m_2} = m_1$$

$$y_1 \equiv M_1^{-1} \pmod{m_1}, \quad y_2 \equiv M_2^{-1} \pmod{m_2}$$

Now solve (1) and (3) using Chinese Remainder Theorem, we have
$a_1 = 4,\ a_2 = 0,\ m_1 = 11,\ m_2 = 3$

$$M_1 = \frac{11 \cdot 3}{11} = 3, \quad M_2 = \frac{11 \cdot 3}{3} = 11$$

$$y_1 \equiv 3^{-1} \pmod{11} \equiv 4 \pmod{11}, \quad y_2 \equiv 11^{-1} \pmod{3} \equiv 2 \pmod{3}$$

and

$$x \equiv (4 \cdot 4 \cdot 3) + (0 \cdot 2 \cdot 11) \equiv 48 \equiv 15 \pmod{33}$$

Similarly, solve (2) and (3) using Chinese Remainder Theorem, we get

$$x \equiv 18 \pmod{33}$$

Therefore $\sqrt{27} \equiv 15, 18 \pmod{33}$

$$\mathcal{D}(?) = \mathcal{D}(27) \equiv \sqrt{27} \pmod{33} \equiv 15, 18 \pmod{33} = \textbf{P or S}$$

Now

$$\mathcal{D}(\chi) = \mathcal{D}(31) \equiv \sqrt{31} \pmod{33} \equiv x \pmod{33} \text{ i.e. } x^2 \equiv 31 \pmod{33}$$

To calculate $x^2 \equiv 31 \pmod{33}$
For $a = 31$, $p = 11$ and $\gcd(31, 11) = 1$. By Theorem 1

we have

$$x \equiv \pm 31^{\frac{11+1}{4}} \pmod{11} \equiv \pm 31^3 \pmod{11} \equiv \pm 9^3 \equiv \pm 3 \pmod{11}$$

For $a = 31$, $p = 3$ and $\gcd(31, 3) = 1$. By Theorem 1
we have

$$x \equiv \pm 31^{\frac{3+1}{4}} \pmod{3} \equiv \pm 31^1 \pmod{3} \equiv \pm 1 \pmod{3}$$

Now we have

$$x \equiv 3 \pmod{11} \tag{4}$$
$$x \equiv -3 \equiv 8 \pmod{11} \tag{5}$$
$$x \equiv 1 \pmod{3} \tag{6}$$
$$x \equiv -1 \equiv 2 \pmod{3} \tag{7}$$

Solve (4) and (6) using Chinese Remainder Theorem, we have
$a_1 = 3,\ a_2 = 1,\ m_1 = 11,\ m_2 = 3$

$$M_1 = \frac{11 \cdot 3}{11} = 3, \quad M_2 = \frac{11 \cdot 3}{3} = 11$$

$$y_1 \equiv 3^{-1} \pmod{11} \equiv 4 \pmod{11}, \quad y_2 \equiv 11^{-1} \pmod{3} \equiv 2 \pmod{3}$$

and

$$x \equiv (3 \cdot 4 \cdot 3) + (1 \cdot 2 \cdot 11) \equiv 58 \equiv 25 \pmod{33}$$

Solve (4) and (7) using Chinese Remainder Theorem, we have
$a_1 = 3,\ a_2 = 2,\ m_1 = 11,\ m_2 = 3$

$$M_1 = \frac{11 \cdot 3}{11} = 3, \quad M_2 = \frac{11 \cdot 3}{3} = 11$$

$$y_1 \equiv 3^{-1} \pmod{11} \equiv 4 \pmod{11}, \quad y_2 \equiv 11^{-1} \pmod{3} \equiv 2 \pmod{3}$$

and

$$x \equiv (3 \cdot 4 \cdot 3) + (2 \cdot 2 \cdot 11) \equiv 80 \equiv 14 \pmod{33}$$

Solve (5) and (6) using Chinese Remainder Theorem, we have
$a_1 = 8,\ a_2 = 1,\ m_1 = 11,\ m_2 = 3$

$$M_1 = \frac{11 \cdot 3}{11} = 3, \quad M_2 = \frac{11 \cdot 3}{3} = 11$$

$$y_1 \equiv 3^{-1} \pmod{11} \equiv 4 \pmod{11}, \quad y_2 \equiv 11^{-1} \pmod{3} \equiv 2 \pmod{3}$$

and

$$x \equiv (8 \cdot 4 \cdot 3) + (1 \cdot 2 \cdot 11) \equiv 118 \equiv 19 \pmod{33}$$

$$x \equiv 19 \pmod{33}$$

Similarly, Solve (5) and (7) using Chinese Remainder Theorem, we get

$$x \equiv 8 \pmod{33}$$

Hence $\sqrt{31} \equiv 8, 14, 19, 25 \pmod{33}$

$$\mathcal{D}(\chi) = \mathcal{D}(31) \equiv \sqrt{31} \pmod{33} \equiv 8, 14, 19, 25 \pmod{33} = \textbf{I, O, T or Z}$$

In the same way we can do other decryptions, we get finitely many possible plain text. We shall choose meaningful plain texts.

Attacks on RSA

In RSA cryptosystem, we use two keys one for encryption which is public and another for decryption which is private. Attacks on RSA , we mean that without knowing private key how can someone decrypt the cipher text. There are many attacks on RSA, we will study few of them.

Low exponent attack

In RSA cryptosystem, when small value of exponent is used for encryption then it becomes easy to attack as follows
Suppose Alice wants to send same message m to Bob, Christopher and David with low exponent value $e = 3$ for this Bob, Christopher and David announce

their public key say $(n_B, 3)$, $(n_C, 3)$ and $(n_D, 3)$ respectively
Alice will send

$$c_B = m^3 \pmod{n_B} \textbf{ to Bob}$$
$$c_C = m^3 \pmod{n_C} \textbf{ to Christopher}$$
$$c_D = m^3 \pmod{n_D} \textbf{ to David}$$

Attacker perform the following computations to get message without knowing the private key.
write

$$x = c_B = m^3 \pmod{n_B}$$
$$x = c_C = m^3 \pmod{n_C}$$
$$x = c_D = m^3 \pmod{n_D}$$

Case 1: If n_B, n_C and n_D are relatively prime then by Chinese Remainder Theorem there exist a number x such that

$$x = m^3 \pmod{n_B n_C n_D}$$

Since $m < n_B, n_C$ and n_D implies that $m^3 < n_B n_C n_D$
Thus message m can be obtained by computing cubic root of x over the integers.

Case 2: If n_B, n_C and n_D are not relatively prime then we have divisors of n_B, n_C and n_D and we can decrypt the cipher easily.

Common modulus attack

In such type of attack it is considered that message is encrypted by taking n common for all receivers but exponents are different and relatively prime i.e. Public key for Bob, Christopher and David will be (n, e_1), (n, e_2) and (n, e_3) respectively and $\gcd(e_1, e_2, e_3) = 1$.

Alice will send

$$c_B = m^{e_1} \pmod{n} \textbf{ to Bob}$$
$$c_C = m^{e_2} \pmod{n} \textbf{ to Christopher}$$
$$c_D = m^{e_3} \pmod{n} \textbf{ to David}$$

Since $\gcd(e_1, e_2, e_3) = 1$ so by Extended Euclidean Algorithm, there exists integers x, y, z such that

$$x \cdot e_1 + y \cdot e_2 + z \cdot e_3 = 1$$

Now the following computation will give the message

$$\begin{aligned} c_B^x \cdot c_C^y \cdot c_D^z =& m^{e_1 \cdot x} m^{e_2 \cdot y} m^{e_3 \cdot z} \pmod{n} \\ =& m^{x \cdot e_1 + y \cdot e_2 + z \cdot e_3} \pmod{n} \\ =& m \pmod{n} \end{aligned}$$

Choosen Ciphertext Attack

Suppose public key is (n, e) , message is 'm' and cipher is 'c'
Attacker will perform following steps to get message without knowing private key i.e. $d \equiv e^{-1} \pmod{\phi(n)}$

- The attacker will choose a random integer s less than n.
- The attacker will construct a cipher text from the obtained cipher 'c' (to be decrypted)
$$c' \equiv s^e \cdot c \pmod{n}$$
- The attacker will manage somehow that receiver must decrypt c' with the help of private key d.
- Suppose receiver decrypts c' to m' i.e.

  $m' = (c')^d \pmod{n} \equiv (s^e \cdot c)^d \pmod{n} \equiv s^{e \cdot d} \cdot c^d \pmod{n} \equiv s \cdot m \pmod{n}$

  since $e \cdot d = 1 \pmod{\phi(n)}$ i.e. $e \cdot d = 1 + k\phi(n)$ for some $k \in \mathbb{Z}$.

- Since the attacker has choosen s himself, so attacker knows $s^{-1} \pmod{n}$, therefore message is obtained by

$$m \equiv s^{-1} \cdot m' \pmod{n}$$

Strong Prime

Let p be a large prime, then p is said to be a strong prime if,
• $p-1$ has a large prime factor say r
• $r-1$ has a large prime factor say t
• $p+1$ has a large prime factor say s

Observe that
Since $p-1$ has a lage prime factor r i.e. $p = kr+1$ for some k. If k is odd then p will be even which is not possible. Therefore k must be even.
Since $r-1$ has a lage prime factor t i.e. $r = k't+1$ for some k'. If k' is odd then r will be even which is not possible. Therefore k' must be even.
Also, Since $p+1$ has a lage prime factor s i.e. $p = k''s-1$ for some k''. If k'' is odd then p will be even which is not possible. Therefore k'' must be even.
So we can write
• $p = 2jr+1$
• $p = 2ms-1$
• $r = 2lt+1$
for some integres j, l, m where r, s and t are primes.
To construct strong primes, we take large primes r, s and t as above and compute p for different choices for j, l and m. Check whether p is prime or not. If p is prime then it will be strong prime.

Note: Large prime does not imply strong prime.
For e.g. **(1.)** $p = 3628273133$ is a 10-digits large prime but $p-1 = 3628273132$ has prime factor $r = 28211$ which is not large prime. So p is not strong prime.
(2.) $p = 10888869450418352160768000001$ is a 29 digits prime no.
Is p a strong prime? "YES" (Verfy!)
(3) $p = 2^{82589933} - 1$ is a large prime $(24,862,048$- digits) but not a strong prime since $p+1$ does not have a large prime factor ($p+1$ has only 2 as prime factor).

Question is given a positive integer n, to decide if it is a prime or not.

Recall: Fermat's little theorem: If a is positive integer such that $\gcd(a, p) = 1$ where p is prime then $a^{p-1} \equiv 1 \pmod{p}$.

What about converse of Fermat's little theorem ? i.e. If n and b is a positive integer such that $\gcd(b, n) = 1$ and $b^{n-1} \equiv 1 \pmod{n}$, is then n a prime ?

Converse of the Fermat's little theorem is **NOT** true i.e if n and b is a positive integer such that $\gcd(b, n) = 1$ and $b^{n-1} \equiv 1 \pmod{n}$ then n need not be prime.
For example: Let $b = 2$ and $n = 341$. Observe that n is not a prime since $n = 341 = 11 \times 31$.
But

$$2^{11-1} = 2^{10} \equiv 1 \pmod{11}$$

and

$$2^{31-1} = 2^{30} \equiv 1 \pmod{31}$$

$$2^{340} = (2^{10})^{34} \equiv 1 \pmod{11} \text{ and } 2^{340} = (2^{30})^{11} \cdot 2^{10} \equiv 1 \pmod{31}$$

Now

$$2^{340} \equiv 1 \pmod{11}$$

$$2^{340} \equiv 1 \pmod{31}$$

Then by CRT(Chinese Remainder Theorem), gives that

$$2^{340} \equiv 1 \pmod{11 \times 31} \text{ i.e. } 2^{340} \equiv 1 \pmod{341}.$$

Here $2^{341-1} \equiv 1 \pmod{341}$ but 341 is not a prime.

Some Definition:

- **Prime:** A positive integer $n > 1$ is said to be prime if its positive divisors are only 1 and n itself.

- **Pseudoprime:** A composite number n is said to be pseudoprime to the base b if b is a positive integer such that $\gcd(b, n) = 1$ and $b^{(n-1)} \equiv 1 \pmod{n}$.
  From above example, 341 is a pseudoprime to the base 2.

- **Carmichael number:** A composite number n is said to be Carmichael number if n is a pseudoprime to every base b. For eg:- 561,1105.
  For $n = 561 = 3 \cdot 11 \cdot 17$, for any $b \in \mathbb{Z}$
  Note that $\gcd(b, 3) = 1$, $\gcd(b, 11) = 1$ and $\gcd(b, 17) = 1$ then by Fermat's Little theorem, we have

$$b^2 \equiv 1 \pmod{3}$$
$$b^{10} \equiv 1 \pmod{11}$$
$$b^{16} \equiv 1 \pmod{17}$$

  Also,

$$b^{560} \equiv \left(b^2\right)^{280} \equiv 1 \pmod{3}$$
$$b^{560} \equiv \left(b^{10}\right)^{56} \equiv 1 \pmod{11}$$
$$b^{560} \equiv \left(b^{16}\right)^{35} \equiv 1 \pmod{17}$$

  Now by Chinese Remainder Theorem, we have

$$b^{560} \equiv 1 \pmod{561}$$

  So for all base $b \in \mathbb{Z}$, $b^{561-1} \equiv 1 \pmod{561}$.
  Hence 561 is Carmichael number. In fact 561 is smallest Carmichael number.

Fermat's Primality Test

Let n be a positive integer. If there exist a positive integer b such that $\gcd(b, n) = 1$ and $b^{n-1} \not\equiv 1 \pmod{n}$ then n is not prime.

Example 1: If $n = 341$ then $b = 3$ is such that $\gcd(3, 341) = 1$

$$3^5 \equiv 243 \pmod{341},$$

$$3^{10} \equiv 56 \pmod{341},$$
$$3^{20} \equiv 67 \pmod{341},$$
$$3^{30} \equiv 1 \pmod{341},$$
$$(3^{30})^{11} = 3^{330} \equiv 1 \pmod{341},$$
$$3^{340} = 3^{330} \cdot 3^{10} \equiv 56 \pmod{341},$$

$\Rightarrow 3^{341-1} \equiv 56 \not\equiv 1 \pmod{341}$.
Hence 341 is not prime and we can observe that $341 = 11 \times 31$.

Miller-Rabin test:

Let n be a postive integer and $n - 1 = 2^s t, s \geq 0$ and t odd positive integer. We say that n passes the Miller's test for the base b if either $b^t \equiv 1 \pmod{n}$ or $b^{2^k t} \equiv -1 \pmod{n}$ for some $k : 0 \leq k \leq s - 1$.

This test uses the simple fact: If p is prime then $x^2 \equiv 1 \pmod{p} \Rightarrow x \equiv \pm 1 \pmod{p}$.

Let b be a base, then $b^{n-1} \equiv 1 \pmod{n}$. (if not, then by Fermat's primality test, n is composite.)
WLOG, we may assume that $s > 0$ otherwise $n - 1$ will be odd and n will be even i.e n is composite.
So $n - 1$ is an even integer
$\Rightarrow \frac{n-1}{2} \in \mathbb{N}$
$\Rightarrow \left(b^{\frac{n-1}{2}}\right)^2 \equiv 1 \pmod{n}$
for $x = b^{\frac{n-1}{2}}, x^2 \equiv 1 \pmod{n}$, suppose $y = \frac{n-1}{2}$

1. If $x \not\equiv \pm 1 \pmod{n}$ then n is composite.
2. If $x \equiv -1 \pmod{n}$ then n may be a prime and may not be a prime and also we can not proceed further.
3. If $x \equiv 1 \pmod{n}$ then n may be a prime and may not be a prime and we can proceed further.

(a) If $2|y$ i.e. y is even, assign $y = y/2 \in \mathbb{Z}$ and evaluate

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

consider the three cases earlier.

(b) If $2 \nmid y$ then the last value for x is $x \equiv 1 \pmod{n}$. We can not go further and n passes the test for the base b.

If n passes the test for base b then we choose another base b' and apply Miller-Rabin test for base b'.

Example 1: Let $n = 29, b = 5$

$$5^{28} \equiv 1 \pmod{29}$$

$n - 1 = 28 = 2^2 \cdot 7$ where $t = 7, \text{and } s = 2$
$\left(\frac{n-1}{2}\right) = 14$

$$5^2 \equiv -4 \pmod{29},$$
$$5^4 \equiv 16 \pmod{29},$$
$$5^6 \equiv -6 \pmod{29},$$
$$5^7 \equiv -1 \pmod{29},$$
$$5^{14} \equiv 1 \pmod{29},$$

For $x = 5^{14} \equiv 1 \pmod{29}$
$x \equiv 1 \pmod{29}$ so 29 may be prime we can proceed further.
Since $2|14$ and $5^7 \equiv -1 \pmod{29}$. It may be a prime and may not be a prime and we can not proceed also further i.e 29 passes the test for the base 5.

Example 2:

Let $n = 1387, b = 2$

$$2^{10} \equiv 1024 \pmod{1387},$$
$$2^{12} \equiv -65 \pmod{1387},$$
$$2^{18} \equiv 1 \pmod{1387},$$

$$(2^{18})^{77} = 2^{1386} \equiv 1 \pmod{1387},$$

$$2^{1386} \equiv 1 \pmod{1387}$$

$n - 1 = 1386 = 2 \cdot 693$ where $t = 693, \text{and } s = 1$
$\left(\frac{n-1}{2}\right) = 693$

$$(2^{18})^{38} = 2^{684} \equiv 1 \pmod{1387},$$

$$2^{684} \cdot 2^9 = 2^{693} \equiv 512 \not\equiv \pm 1 \pmod{1387}$$

Since $x^2 = (2^{693})^2 = 2^{1386} \equiv 1 \pmod{1387}$ but $x = 2^{693} \equiv 512 \not\equiv \pm 1 \pmod{1387}$. Hence 1387 fails the test. Therefore 1387 is composite number and $1378 = 19 \cdot 73$.

Remark: Observe that a prime passes the test , but a composite may also. So if n passes the test we can not conclude that n is 'prime'. However if n fails the test then n is 'composite'.

Wilson's theorem:

Statement: Let p be a positive integer then p is a prime iff $(p-1)! \equiv -1 \pmod{p}$.

Proof:
$\Rightarrow$: Let p be a prime. If $p = 2$ then $(2-1)! = 1!$ and $1 \equiv -1 \pmod{2}$. So theorem holds for $p = 2$.
If $p = 3$ then $(3-1)! = 2!$ and $2 \equiv -1 \pmod{3}$. Theorem also true for $p = 3$.
Now consider $p > 3$

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1)$$

Since $1, 2, \ldots, (p-1) \in \mathbb{Z}_p^*$ and $\mathbb{Z}_p^*$ is group under multiplication modulo p. So every integer $1, 2, \ldots, (p-1) \in \mathbb{Z}_p^*$ has a unique inverse.

$$2 \cdot 3 \cdots (p-1) = \prod (x x^{-1})$$

writing have the factor x alongwith its inverse x^{-1} $\forall x \in \{2, 3, \ldots, (p-1)\}$ being then odd no. there should be some $x \in \{2, 3, \ldots, (p-1)\}$ such that

$x \equiv x^{-1} \pmod{p}$ i.e $x^2 \equiv 1 \pmod{p}$.

$$\Rightarrow (p-1)! \equiv x \pmod{p} \text{ for some } x \in \{2, 3, \ldots, (p-1)\}$$

such that $x \equiv x^{-1} \pmod{p} \Rightarrow x \equiv \pm 1 \pmod{p}$ since $1 \notin \{2, 3, \ldots, (p-1)\}$ we get $x \equiv -1 \pmod{p}$ that is $(p-1)! \equiv -1 \pmod{p}$.

$\Leftarrow$: For if p is not prime, then p has a divisor d with $1 < d < p$. Furthermore, because $d \leq (p-1), d$ occurs as one of the factors in $(p-1)!$, whence $d|(p-1)!$. Now we are assuming that $p|(p-1)! + 1$, and so $d|(n-1)! + 1$, too. The conclusion is that $d|1$, which is nonsense.
Hence If p is composite then $(p-1)! \not\equiv -1 \pmod{p}$ i.e if $(p-1)! \equiv -1 \pmod{p}$ then p is prime.

Example: For $p = 9$, $(9-1)! = 8! = 40320 \equiv 0 \pmod{9} \not\equiv -1 \pmod{9}$

AKS Primality Test

In 2002 Agrawal, Kayal, and Saxena (IIT Kanpur) introduced the deterministic primality test known as AKS algorithm named after them.
The following steps involve in AKS algorithm to check a given integer $n > 1$ is prime or not:

1. Check $n^{\frac{1}{k}}$ is an integer for $2 \leq k \leq \log_2(n)$. If $n^{\frac{1}{k}}$ is the integer i.e. n is perfect power, then n is composite.
2. Find the smallest integer r such that $\text{ord}_r(n) > (\log_2(n))^2$ where $\text{ord}_r(n)$ is multiplicative order of n modulo r.
3. Calculate $\gcd(a, n)$ for $2 \leq a \leq r$. If $\gcd(a, n) \neq 1, n$ for some a, then n composite.
4. If n has passed step (3) and $n \leq r$, then n is prime (because n is relatively prime to all $a < n$).
5. If n has passed all above steps then check that

$$(X + b)^n \equiv X^n + b \pmod{X^r - 1, n}$$

For all b such that $1 \leq b \leq \sqrt{\phi r}\log_2(n)$. If this the case n is prime i.e.

$$(X+b)^n \not\equiv X^n + b \pmod{X^r - 1, n}$$

For some b such that $1 \leq b \leq \sqrt{\phi(r)}\log_2(n)$, then n is composite.

Where $(X+b)^n \equiv X^n + b \pmod{X^r - 1, n}$ means that when we take the difference $(X+b)^n - (X^n + b)$ and divide by $X^r - 1$, the remainder has all of its coefficients divisible by n.

Example: We check whether $n = 37$ is pime or not by AKS Algorithm
$\log_2(n) = \log_2(37) \approx 5.2094$
For $2 \leq k \leq 5.2094$, we calculate $37^{\frac{1}{k}}$ (if $37^{\frac{1}{k}}$ is integer then 37 is composite).

$$37^{\frac{1}{2}} = 6.0827$$
$$37^{\frac{1}{3}} = 3.3322$$
$$37^{\frac{1}{4}} = 2.4663$$
$$37^{\frac{1}{5}} = 2.0589$$

Hence 37 is not perfect power of any integer.
Now we find smallest integer r such that

$$\text{ord}_r(n = 37) \geq (\log_2(n = 37))^2 \approx 27.1384$$

where $\text{ord}_r(n)$ is multiplicative order of n modulo r.

$$\text{ord}_2(37) = 1$$
$$\text{ord}_3(37) = 1$$
$$\text{ord}_4(37) = 1$$
$$\text{ord}_5(37) = 4$$
$$\text{ord}_6(37) = 1$$

and so on, We get

$$\text{ord}_{29}(37) = 28 > 27.1384$$

So we have $r = 29$
and $\gcd(a, 37) = 1$ for $2 \leq a \leq 27$
Since $n \geq r$ So it passes step (4), now we check step(5) i.e.

$$(X + b)^n \equiv X^n + b \pmod{X^r - 1, n}$$

for $n = 37$, $r = 29$ and $1 \leq b \leq \sqrt{\phi r}\log_2(n)$. and $\sqrt{\phi(29)}\log_2(37) = \sqrt{28}\log_2(37) = 27.6$ i.e $1 \leq b \leq 27.6$
For $b = 1$
$(X + 1)^{37} - (X^{37} + 1) = (X^{29} - 1)q(x) + r(x) \equiv r(x) \pmod{X^{29} - 1}$
where

$$q(x) = 37X^7+666X^6+7770X^5+66045X^4+435897X^3+2324784X^2+10295472X+38608020$$

and

$$\begin{aligned} r(x) =& 124403620X^{28} + 348330136X^{27} + 854992152X^{26} + 1852482996X^{25} + 3562467300X^{24} \\ &+ 6107086800X^{23} + 9364199760X^{22} + 12875774670X^{21} + 15905368710X^{20} \\ &+ 17672631900X^{19} + 17672631900X^{18} + 15905368710X^{17} + 12875774670X^{16} \\ &+ 9364199760X^{15} + 6107086800X^{14} + 3562467300X^{13} + 1852482996X^{12} \\ &+ 854992152X^{11} + 348330136X^{10} + 124403620X^9 + 38608020X^8 \\ &+ 10295435X^7 + 2324118X^6 + 428127X^5 - 428127X^3 \\ &- 2324118X^2 - 10295435X - 38608020 \end{aligned}$$

Observe that each coefficient of $r(x)$ is divisible 37, So we have

$$(X + 1)^{37} \equiv X^{37} + 1 \pmod{X^{29} - 1, 37}$$

Similarly, we can do for all b and we get

$$(X + b)^{37} \equiv X^{37} + b \pmod{X^{29} - 1, 37}$$

for $1 \leq b \leq 27.6$
Therefore 37 is prime.

Lecture-9

Factorization of Integers

Fermat's Factorization

Fermat's method for factoring a composite number n tries to write it as the difference of two squares $n = x^2 - y^2$, yielding the factorization $n = (x+y)(x-y)$. Indeed, for a composite odd number $n = ab$ such a representation always exists:

$$(a+b)^2 - (a-b)^2 = a^2 + b^2 + 2ab - (a^2 + b^2 - 2ab) = 4ab$$

$$\Rightarrow ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

$$\Rightarrow n = x^2 - y^2 \text{ where } x = \frac{a+b}{2}, y = \frac{a-b}{2}$$

If $n = x^2 - y^2$ is a positive odd integer then $x^2 - n = y^2$ i.e $x^2 - n$ is a perfect square.
Let m be the positive integer such that $m \geq \sqrt{n}$. Now look for perfect squares in the sequence $m^2 - n, (m+1)^2 - n, (m+2)^2 - n, \ldots$. The search will end into a perfect square for $m \leq \frac{n+1}{2}$.
Since
$m^2 - n,$ for $m = \frac{n+1}{2}$ is

$$m^2 - n = \frac{n^2 + 1 + 2n - 4n}{4} = \left(\frac{n-1}{2}\right)^2 \in \mathbb{Z}$$

Of course the value of m, gives trivial factor.

Remark: To have an initial guess for $m \geq \sqrt{n}, m \in \mathbb{N}$, apply Newton's method for function $f(x) = x^2 - n$, observe that $f'(x) = 2x$. Say r_0 and subsequent guesses by the sequence $r_k = r_{k-1} - \frac{f(r_{k-1})}{f'(r_{k-1})}$ for $k \geq 1$.

Example 1: Let $n = 3811$ and $m \geq \sqrt{3811}$.
Since $62 > \sqrt{3811} > 61$. Choose $m = 62$.
Now look for perfect square

$$62^2 - 3811 = 33$$
$$63^2 - 3811 = 158$$
$$64^2 - 3811 = 285$$
$$65^2 - 3811 = 414$$
$$66^2 - 3811 = 545$$
$$67^2 - 3811 = 678$$
$$68^2 - 3811 = 813$$
$$69^2 - 3811 = 950$$
$$70^2 - 3811 = 1089 = 33^2$$

$\Rightarrow 3811 = 70^2 - 33^2$
$\Rightarrow 3811 = (70 - 33)(70 + 33)$
$\Rightarrow 3811 = 37 \times 103$
Factosr of 3811 are 37 and 103.

Example 2: Let $n = 2183$ and $m \geq \sqrt{2183}$.
Since $47 > \sqrt{2183} > 46$. Choose $m = 47$.
Now look for perfect square

$$47^2 - 2183 = 26$$
$$48^2 - 2183 = 121 = 11^2$$

$\Rightarrow 2183 = 48^2 - 11^2$
$\Rightarrow 2183 = (48 - 11)(48 + 11)$
$\Rightarrow 2183 = 37 \times 59$
Factors of 2183 are 37 and 59.

Pollard's (p-1) Factorization

Pollard's (p-1) Algorithm is based on :
Suppose a large positive integer n is to be factored, if p is a prime such that

$p|n$ and $(p-1)|k!$ for some $k \in \mathbb{Z}^+$
WLOG, assume p is an odd prime i.e. $p > 2$. Let a be a positive integer such that $\gcd(a, n) = 1$ this implies that $\gcd(a, p) = 1$ then by Fermat's Little Theorem $a^{(p-1)} \equiv 1 \pmod{p}$
Since

$$\begin{aligned}(p-1)|k! &\implies a^{k!} \equiv 1 \pmod{p} \\ &\implies p|a^{k!} - 1 \\ \text{Let } a^{k!} - 1 &\equiv z \pmod{n} \\ &\implies a^{k!} - 1 = z + mn \quad \text{for some } m \in \mathbb{Z} \\ &\implies a^{k!} - 1 - mn = z\end{aligned}$$

Since $p|mn$ and $p|a^{k!} - 1$ this implies that $p|z$ and $p|n$ i.e $p|\gcd(z, n)$
Note: Since n is odd, we can choose $a = 2$.

Algorithm:
Suppose n is given integer which is to be factored.
Choose a base a such that $\gcd(a, n) = 1$. Let z be the least non-negative residue in modulo n of $a^{k!} - 1$ i.e.

$$a^{k!} - 1 \equiv z \pmod{n} \quad \text{for} \quad k = 1, 2, \ldots$$

Case 1: $z \neq 0$
Calculate $\gcd(z, n)$
If $\gcd(z, n) \neq 1$ then we get a non trivial factor on n.

Case 2: If $z = 0$ then test fails and we try it for another a.

Example: $n = 61937$, now take $a = 2$
Note that $\gcd(a, n) = \gcd(2, 61937) = 1$
We calculate $2^{k!} - 1 \equiv z \pmod{n}$ for $k \in \mathbb{Z}^+$ and $\gcd(z, n)$

For $k = 1$, $2^{1!} - 1 \equiv 1 \pmod{61937}$ and $\gcd(1, 61937) = 1$

For $k = 2$, $2^{2!} - 1 \equiv 3 \pmod{61937}$ and

$$61937 = 3 \cdot 20645 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2 + 0$$

Hence $\gcd(3, 61937) = 1$

For $k = 3$, $2^{3!} - 1 \equiv 63 \pmod{61937}$ and

$$61937 = 63 \cdot 983 + 8$$
$$63 = 8 \cdot 7 + 7$$
$$8 = 7 \cdot 1 + 1$$
$$7 = 1 \cdot 7 + 0$$

Hence $\gcd(63, 61937) = 1$

For $k = 4$, $2^{4!} - 1 \equiv 54225 \pmod{61937}$ and

$$61937 = 54225 \cdot 1 + 7712$$
$$54225 = 7712 \cdot 7 + 241$$
$$7712 = 241 \cdot 32 + 0$$

Hence $\gcd(54225, 61937) = 241$
Therefore 241 divides $n = 61937$ and $61937 = 241 \times 257$

Monte Carlo factorization

Monte Carlo factorization Algorithm (also known as Pollard's Rho Algorithm) is an algorithm for integer factorization. It was invented by John Pollard in 1975.

Setup

1. Let n be a positive composite integer.
2. Let p be a small prime factor of n.
3. Let k be an integer such that k is much larger than $\sqrt{p}$ and much smaller than $\sqrt{n}$, that is

$$\sqrt{p} << k << \sqrt{n}$$

4. Go to Algorithm.

Algorithm (When a small prime factor p is known)

1. Choose a sequence of positive integers

$$m_0,\ m_1,\ m_2,\ m_3, \ldots, m_k$$

such that their least non-negative residue are distint in modulo n but not all distint in modulo p,
that is,

$$m_i \not\equiv m_j\ (mod\ n)\ \ \forall i \neq j, \qquad i, j \in \{0, 1, 2, 3, ..., k\}$$

and

$$m_q \equiv m_r\ (mod\ p)\ \ for\ some\ q \neq r, \qquad q, r \in \{0, 1, 2, 3, ..., k\}$$

2. Observe the sequence

$$m_0,\ m_1,\ m_2,\ m_3, \ldots,\ m_k$$

Note that

$$p \text{ divides } n \text{ and } p \text{ divides } (m_q - m_r)$$

Now compute

$$\gcd((m_q - m_r), n)$$

If gcd is greater than p, then we have a factor of n other than p.

Algorithm (When a prime factor p is not known)

1. Start with a ramdomly generated integer m_0.
2. Choose a sequence of positive integers

   $$m_1,\ m_2,\ m_3, \ldots$$

   such that

   $$m_i \ = \ m_{i-1}^2 + 1 \pmod{n} \qquad \forall\ i \ \in \ 1, 2, 3, ...$$

3. Compute

   $$\gcd(m_{2i} - m_i, n)$$

4. If gcd is greater than 1 and less than n for some i, then we get a non trivial factor of n.
5. Proceed in similar way or go to the above algorithm (since we have a non trivial factor now and we can compute a prime factor of n also).

Note

1. Here, the function is choosen as $f(x_i) = x_{i-1}^2 + 1$.
2. We can take any other recursive function also.
3. If $n = pq$ where p and q are primes of the same size (that is, of same length), then Pollard's Rho Algorithm can find a non trivial factor of n in $O(\sqrt[4]{n})$.

Example 1: For $n = 8051$. Let $m_0 = 2$, and $f(x_i) = x_{i-1}^2 + 1$, then for each i, $\quad m_i = m_{i-1}^2 + 1$

then,

$$
\begin{aligned}
m_1 &= 2^2 + 1 = 5 \\
m_2 &= 5^2 + 1 = 26 \\
m_3 &= 26^2 + 1 = 677 \\
m_4 &= 677^2 + 1 = 458330 \equiv 7474 \ (mod\ 8051) \\
m_5 &= 7474^2 + 1 \equiv 2839 \ (mod\ 8051) \\
m_6 &= 2839^2 + 1 \equiv 871 \ (mod\ 8051)
\end{aligned}
$$

and so on
Now compute

$$\gcd(m_{2i} - m_i, n)$$

that is,

$$
\begin{aligned}
\gcd(m_2 - m_1, n) &= \gcd(21\ ,\ 8051) \ = \ 1 \\
\gcd(m_4 - m_2, n) &= \gcd(7448\ ,\ 8051) \ = \ 1 \\
\gcd(m_6 - m_3, n) &= \gcd(194\ ,\ 8051) \ = \ 97
\end{aligned}
$$

Thus 97 is a factor of $n = 8051$.
Other non trivial factor of n is 83.

Example 2: Let $n = 3293$
Let $m_0 = 3$, and $f(x_i) = x_{i-1}^2 + 1$, then
for each i, $\quad m_i = m_{i-1}^2 + 1$
then,

$$
\begin{aligned}
m_1 &= 3^2 + 1 = 10 \\
m_2 &= 10^2 + 1 = 101 \\
m_3 &= 101^2 + 1 = 10202 \equiv 323 \ (mod\ 3293) \\
m_4 &= 323^2 + 1 \equiv 2247 \ (mod\ 3293)
\end{aligned}
$$

and so on.
Compute

$$\gcd(m_{2i} - m_i, n)$$

that is,

$$\gcd(m_2 - m_1, n) \ = \ \gcd(91\ ,\ 3293) \ = \ 1$$

$$\gcd(m_4 - m_2, n) \;=\; \gcd(2146\ ,\ 3293) \;=\; 37$$

Thus 37 is a factor of $n = 3293$.
Other non trivial factor of n is 89.

Example 3: Let $n = 4087$
Let $m_0 = 2$, and $f(x_i) = x_{i-1}^2 + 3$, then
for each i, $\quad m_i = m_{i-1}^2 + 3$
then,

$$\begin{aligned}
m_1 &= 2^2 + 3 = 7 \\
m_2 &= 7^2 + 3 = 52 \\
m_3 &= 52^2 + 3 = 2707 \\
m_4 &= 2707^2 + 3 = 3948 \\
m_5 &= 3948^2 + 3 \equiv 2976 \ (mod\ 4087) \\
m_6 &= 2976^2 + 3 \equiv 50 \ (mod\ 4087) \\
m_7 &= 50^2 + 3 \equiv 2503 \ (mod\ 4087) \\
m_8 &= 2503^2 + 3 \equiv 3728 \ (mod\ 4087) \\
m_9 &= 3728^2 + 3 \equiv 2187 \ (mod\ 4087) \\
m_{10} &= 2187^2 + 3 \equiv 1182 \ (mod\ 4087) \\
m_{11} &= 1182^2 + 3 \equiv 3460 \ (mod\ 4087) \\
m_{12} &= 3460^2 + 3 \equiv 780 \ (mod\ 4087) \\
m_{13} &= 780^2 + 3 \equiv 3527 \ (mod\ 4087) \\
m_{14} &= 3527^2 + 3 \equiv 2991 \ (mod\ 4087)
\end{aligned}$$

and so on.

Compute

$$\gcd(m_{2i} - m_i, n)$$

that is,

$$\begin{aligned}
\gcd(m_2 - m_1, n) &= \gcd(45\ ,\ 4087) \ =\ 1 \\
\gcd(m_4 - m_2, n) &= \gcd(3896\ ,\ 4087) \ =\ 1 \\
\gcd(m_6 - m_3, n) &= \gcd(-2657\ ,\ 4087) \ =\ \gcd(2657\ ,\ 4087) \ =\ 1 \\
\gcd(m_8 - m_4, n) &= \gcd(-220\ ,\ 4087)\ \ \gcd(220\ ,\ 4087) \ =\ 1 \\
\gcd(m_{10} - m_5, n) &= \gcd(-1794\ ,\ 4087)\ \ \gcd(1794\ ,\ 4087) \ =\ 1 \\
\gcd(m_{12} - m_6, n) &= \gcd(730\ ,\ 4087) \ =\ 1 \\
\gcd(m_{14} - m_7, n) &= \gcd(488\ ,\ 4087) \ =\ 61
\end{aligned}$$

Thus 61 is a factor of $n = 4087$.
Other non trivial factor of n is 67.

Factor Base Factorization

Factor Base: Let $\mathcal{B} = \{p_1, p_2, \ldots, p_h\}$ where $p_1 = -1$ and $p_2, p_3 \ldots p_k$ are distinct primes then b^2 is said to be $\mathcal{B}-$smooth or $\mathcal{B}-$number modulo n if

$$b^2 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_h^{\alpha_k} \pmod{n}, \quad \alpha_i \geq 0$$

Example: for $n = 4633$ and $\mathcal{B} = \{-1, 2, 3\}$

$$\begin{aligned}
67^2 &\equiv 4489 \pmod{4633} \\
67^2 &\equiv -144 \pmod{4633} \\
67^2 &\equiv (-1)(2)^4(3)^2 \pmod{4633}
\end{aligned}$$

So $(67)^2$ is $\mathcal{B}-$smooth in modulo 4633. Similarly we have,

$$\begin{aligned}
(68)^2 &\equiv (-1)(2)^0(3)^2 \pmod{4633} \\
(69)^2 &\equiv (-1)^0(2)^7(3)^0 \pmod{4633}
\end{aligned}$$

• If b^2 is a $\mathcal{B}-$number for a given positive integer n

$$b^2 \pmod{n} = \prod_{j=1}^{h} p_j^{\alpha_j}, \quad p_j \in \mathcal{B}$$

Denote $\epsilon_j^b \equiv \alpha_j \pmod 2$ i.e. powers of primes modulo 2 and $\epsilon_b = \{\epsilon_1^b, \epsilon_2^b, \ldots, \epsilon_h^b\}$

From above example we have

$$\epsilon_{67} = \{1, 0, 0\}$$
$$\epsilon_{68} = \{1, 0, 0\}$$
$$\epsilon_{69} = \{0, 1, 0\}$$

Given a positive integer n to be factored, Suppose we have k $\mathcal{B}$-smooth numbers b_i^2 where $\mathcal{B}$ is a factor base and

$$\epsilon_i = \{\epsilon_{i1}, \epsilon_{i2}, \ldots, \epsilon_{ih}\}$$

corresponding to b_i^2's for $i = 1, 2 \ldots, k$ such that $\sum_{i=1}^k \epsilon_i = \{0, 0, \ldots, 0\} \pmod n$. Let a_i is least absolute residue modulo n for b_i^2 , $i = 1, 2, \ldots k$ then

$$b_i^2 \equiv a_i \equiv \prod_{j=1}^{h} p_j^{\alpha_j} \pmod n \quad p_j \in \mathcal{B}, \quad i = 1, 2, \ldots k$$

So

$$\prod_{i=1}^{k} a_i = \prod_{i=1}^{k} \left(\prod_{j=1}^{h} p_j^{\alpha_j} \right) \pmod n$$

$$= \prod_{j=1}^{h} p_j^{\sum_{i=1}^k \alpha_{ij}} \pmod n$$

$$\prod_{i=1}^{k} b_i^2 = \prod_{i=1}^{k} a_i = \prod_{j=1}^{h} p_j^{\sum_{i=1}^k \alpha_{ij}} \pmod n$$

Now if $\sum_{i=1}^k \epsilon_i = (0, 0, \ldots, 0)$ i.e. sum of powers modulo 2 is 0, i.e. even, then right side become a perfect square,

$$\textbf{RHS} = \prod_{j=1}^{h} p_j^{\sum_{i=1}^k \alpha_{ij}} = l^2 \quad \textbf{(say)}$$

and

$$b^2 = \left(\prod_{i=1}^{k} b_i \right)^2 \quad \text{(say)}$$

then we have

$$b^2 = l^2 \pmod{n}$$

i.e. $n \mid b^2 - l^2$ i.e. $n \mid (b-l)(b+l)$
and factors of n is obtained by computing $\gcd(n, b-l)$ and $\gcd(n, b+l)$
Example: From above we have, for $n = 4633$
$\epsilon_{67} = (1, 0, 0)$ and $\epsilon_{68} = (1, 0, 0)$
$\epsilon_{67} + \epsilon_{68} = (0, 0, 0)$

$$\begin{aligned}(67)^2 \cdot (68)^2 \equiv & (-1)^2(2)^4(3)^4 \pmod{n} \\ & \implies (67 \cdot 68)^2 \equiv 2^4 \cdot 3^4 \pmod{n} \\ & \implies n \mid (67 \cdot 68)^2 - 2^4 \cdot 3^4 \\ & \implies n \mid (67 \cdot 68)^2 - (36)^2 \\ & \implies n \mid (67 \cdot 68 - 36)(67 \cdot 68 + 36) \\ & \implies n \mid (4520)(4592)\end{aligned}$$

$$\gcd(n, 4520) = \gcd(4633, 4520) = 113$$

$$\gcd(n, 4592) = \gcd(4633, 4592) = 41$$

So factors of $n = 4633$ are 113 and 41.

Quadratic Sieve Factorization

Suppose n is the given positive integer which is to be factorized.
Let m is least positive integer such that $m \geq \sqrt{n}$
Take the polynomial $f(x) = (x+m)^2 - n$
Now we calculate $f(j) = (j+m)^2 - n \pmod{n}$ for different values of $j \in \mathbb{Z}$
Choose a factor base $\mathcal{B} = \{p_1, p_2, \ldots, p_n\}$ such that we can factor $f(j) \pmod{n}$ using primes in $\mathcal{B}$.
Find some $f(j)$'s such that product of $f(j) \pmod{n}$ is even power of primes in $\mathcal{B}$ (as in Factor Base Factorization).
Say

$$f(j_1) \cdot f(j_2) \cdots f(j_k) \equiv p_1^{e_1} \cdot {}_2^{e_2} \cdots p_n^{e_n} \pmod{n}$$

where e_i's are even i.e right hand side is perfect square .
Suppose $p_1^{e_1} \cdot_2^{e_2} \cdots p_n^{e_n} = l^2$ then we have

$$f(j_1) \cdot f(j_2) \cdots f(j_k) \equiv l^2 \pmod{n}$$

i.e.

$$(j_1 + m)^2 \cdot (j_2 + m)^2 \cdots (j_k + m)^2 \equiv l^2 \pmod{n}$$

Supoose $(j_1 + m)^2 \cdot (j_2 + m)^2 \cdots (j_k + m)^2 = r^2$ So we have

$$n \mid r^2 - l^2$$

i.e

$$n \mid (r - l)(r + l)$$

Factors of n is given by

$$\gcd(r - l, n)$$

and

$$\gcd(r + l, n)$$

Example: For $n = 7429$, $\sqrt{n} \approx 86.20$, so $m = 87$
take $f(x) = (87 + x)^2 - 7429$

$$\begin{aligned} f(0) &= 87^2 - 7429 \equiv 140 \pmod{7429} \equiv 2^2 \cdot 5 \cdot 7 \pmod{7429} \\ f(1) &= 88^2 - 7429 \equiv 315 \pmod{7429} \equiv 3^2 \cdot 5 \cdot 7 \pmod{7429} \\ f(-2) &= 85^2 - 7429 \equiv -204 \pmod{7429} \equiv (-1) \cdot 2^2 \cdot 3 \cdot 17 \pmod{7429} \end{aligned}$$

Note that $f(0)f(1) = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2 \pmod{7429}$

$$\begin{aligned} (87^2 - 7429)(88^2 - 7429) &\equiv 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2 \pmod{7429} \\ (87 \cdot 88)^2 &\equiv (210)^2 \pmod{7429} \\ \implies n &\mid (87 \cdot 88)^2 - (210)^2 \\ \implies n &\mid (87 \cdot 88 - 210)(87 \cdot 88 + 210) \\ \text{i.e. } n &\mid (7446)(7866) \end{aligned}$$

$$\gcd(n, 7446) = 17$$
$$\gcd(n, 7866) = 1$$

Factors of $n = 7429$ are 17 and 437.

Continued Fraction Factorization

For a give real number x, we define continued fraction

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\ddots}}}}}$$

In compact form $x = [a_0; a_1, a_2, \ldots, a_n, \ldots]$
where $a_0, a_1, \ldots, a_n$ are real numbers and all are positive except $a_0 \geq 0$. Continued Fractions can be finite or infinte.
k^{th} **convergent of continued fraction is**

$$c_k = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_k}}}}}$$

Example:

$$\frac{19}{35} = 0 + \frac{1}{\frac{35}{19}}$$

$$= 0 + \frac{1}{1 + \frac{16}{19}}$$

$$= 0 + \frac{1}{1 + \frac{1}{\frac{19}{16}}}$$

$$= 0 + \frac{1}{1 + \frac{1}{1 + \frac{3}{16}}}$$

$$= 0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{5 + \frac{1}{3}}}}$$

$$\frac{19}{35} = [0; 1, 1, 5, 3]$$

$$c_0 = 0$$

$$c_1 = 0 + \frac{1}{1} = 1$$

$$c_2 = 0 + \frac{1}{1 + \frac{1}{1}} = \frac{1}{2}$$

$$c_3 = 0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{5}}} = \frac{6}{11}$$

$$c_4 = 0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{5 + \frac{1}{3}}}} = \frac{19}{35}$$

Now define A_k and B_k for $k = 0, 1, 2, \ldots$
$A_0 = a_0$ and $B_0 = 1$
$A_1 = a_1 a_0 + 1$ and $B_1 = a_1$
$A_k = a_k A_{k-1} + A_{k-2}$ and $B_k = a_k B_{k-1} + B_{k-2}$

then we have

$$\begin{aligned} c_0 &= \frac{A_0}{B_0} \\ c_1 &= \frac{A_1}{B_1} \\ c_2 &= \frac{A_2}{B_2} \\ &\vdots \\ c_k &= \frac{A_k}{B_k} \end{aligned}$$

Algorithm for factorization

Suppose n is given positive integer which is to be factorized.

• Write $\sqrt{n}$ in continued fraction.

• Let $\frac{A_k}{B_k}$ be the k^{th} convergent of continued fraction.

• Write $A_k^2 \equiv r_k \pmod{n}$

• Choose set $\{r_1, r_2, \ldots, r_m\}$ such that $\prod_{i=1}^{m} r_i = X^2 \pmod{n}$ (say) is perfect square.

• Let $\prod_{i=1}^{m} A_i \equiv Y \pmod{n}$

then we have

$$\begin{aligned} X^2 \equiv \prod_{i=1}^{m} r_i = \prod_{i=1}^{m} A_i^2 \equiv Y^2 \pmod{n} \\ \implies X^2 \equiv Y^2 \pmod{n} \end{aligned}$$

If $X \neq \pm Y$ then factors of n is given by

$$\gcd((X - Y), n)$$

and

$$\gcd((X + Y), n)$$

Algorithm for wrting Continued fraction of $\sqrt{n}$
Initialization:

$$\begin{aligned} a_0 &= 2\left\lfloor \sqrt{n} \right\rfloor \\ y_0 &= \left\lfloor \sqrt{n} \right\rfloor \\ z_0 &= 1 \end{aligned}$$

Iteration process for $k \geq 1$

$$\begin{aligned} y_k &= a_{k-1} \cdot z_{k-1} - y_{k-1} \\ z_k &= \left\lfloor \frac{n - y_k^2}{z_{k-1}} \right\rfloor \\ a_k &= \left\lfloor \frac{\lfloor \sqrt{n} \rfloor + y_k}{z_k} \right\rfloor \end{aligned}$$

Then continued fraction for $\sqrt{n} = [\lfloor \sqrt{n} \rfloor ; a_1, a_2 \dots]$

$$\sqrt{n} = \lfloor \sqrt{n} \rfloor + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\ddots}}}}}$$

Example: For $n = 33$, we write $\sqrt{33}$ in continued fraction
$\sqrt{n} = \sqrt{33} \approx 5.744$ i.e. $\left\lfloor \sqrt{33} \right\rfloor = 5$

$$\begin{aligned} a_0 &= 2 \cdot \left\lfloor \sqrt{33} \right\rfloor = 2 \cdot 5 = 10 \\ y_0 &= \left\lfloor \sqrt{33} \right\rfloor = 5 \\ z_0 &= 1 \end{aligned}$$

$$y_1 = a_0 z_0 - y_0 = 10 \cdot 1 - 5 = 5$$
$$z_1 = \left\lfloor \frac{33 - 25}{1} \right\rfloor = 8$$
$$a_1 = \left\lfloor \frac{\lfloor \sqrt{33} \rfloor + y_1}{z_1} \right\rfloor = \left\lfloor \frac{5+5}{8} \right\rfloor = 1$$

$$y_2 = a_1 z_1 - y_1 = 1 \cdot 8 - 5 = 3$$
$$z_2 = \left\lfloor \frac{33 - 9}{8} \right\rfloor = 3$$
$$a_2 = \left\lfloor \frac{\lfloor \sqrt{33} \rfloor + y_2}{z_2} \right\rfloor = \left\lfloor \frac{5+3}{3} \right\rfloor = 2$$

$$y_3 = a_2 z_2 - y_2 = 2 \cdot 3 - 3 = 3$$
$$z_3 = \left\lfloor \frac{33 - 9}{3} \right\rfloor = 8$$
$$a_3 = \left\lfloor \frac{\lfloor \sqrt{33} \rfloor + y_3}{z_3} \right\rfloor = \left\lfloor \frac{5+3}{8} \right\rfloor = 1$$

$$\sqrt{33} = 5 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \ddots}}}$$

$$\sqrt{33} = [5; 1, 2, 1 \ldots] = [a_0; a_1, a_2, a_3 \ldots]$$

k-th convergent $c_k = \frac{A_k}{B_k}$

$$A_0 = a_0 \qquad B_0 = 1$$
$$A_1 = a_1 a_0 + 1 \qquad B_1 = a_1$$
$$A_k = a_k A_{k-1} + A_{k-2} \qquad B_k = a_k B_{k-1} + B_{k-2}$$

$$A_0 = a_0 = 5 \qquad B_0 = 1$$
$$A_1 = a_1 a_0 + 1 = 5 + 1 = 6 \qquad B_1 = a_1 = 1$$
$$A_2 = a_2 A_1 + A_0 = 17 \qquad B_2 = a_2 B_1 + B_0 = 3$$
$$A_3 = a_3 A_2 + A_1 = 23 \qquad B_3 = a_3 B_2 + B_1 = 4$$

$$c_0 = 5$$
$$c_1 = 6$$
$$c_2 = \frac{17}{3}$$
$$c_3 = \frac{23}{4}$$

So, $A_0 = 5, \quad A_1 = 6, \quad A_2 = 17, \quad , A_3 = 23$

$$A_0^2 \equiv 25 \pmod{33} = r_0$$
$$A_1^2 = 36 \equiv 3 \pmod{33} = r_1$$
$$A_2^2 = 17^2 \equiv 25 \pmod{33} = r_2$$
$$A_3^2 = 23^2 \equiv 1 \pmod{33} = r_3$$

Note that $r_2 = 25 = 5^2 = X^2$ and $A_2 = 17 \pmod{33} = Y$
Also

$$X^2 \equiv r_2 = A_2^2 \equiv Y^2 \pmod{33}$$

And $X \neq \pm Y$. Therefore factors of 33 is given by

$$\gcd(Y - X, n) = \gcd(17 - 5, 33) = 3$$

$$\gcd(Y + X, n) = \gcd(17 + 5, 33) = 11$$

Hence $33 = 3 \times 11$

Lecture-10

Key Exchange Protocols and Discrete Logarithm

Diffe-Hellman Key Excange Protocol

Let $G = \langle g | g^n = 1 \rangle$ be a cyclic group generated by g and be public. Alice (sender) and Bob (receiver) exchange the key as follows:

	Alice		Bob
Private	a		$b \in \mathbb{Z}_n$
Public	g^a	$\longrightarrow$	$g^a \in G$
Public	g^b	$\longleftarrow$	$g^b \in G$

Now Alice calculate $(g^b)^a = g^{ab}$ and Bob calculate $(g^a)^b = g^{ab}$.
Hence $K = g^{ab}$ which becomes their common knowledge.

Example: Let Alice and Bob be using shift transformation

$$\mathcal{E} : \mathcal{A} \to \mathcal{A} = \{A = 0, B = 1, \ldots, Z = 25\}$$
$$m \to \mathcal{E}(m) = m + k \pmod{26}$$

To exchange the encryption key k an integer modulo 26 they use Diffe-Hellman key exchange protocol as follows.
Let $G = \mathbb{F}_{53} = \mathbb{Z}_{53}^*$
Let $g = 2 \in G$. Note that $O(g) = 52$ hence g is the generator of $G = \langle g = 2 | g^{52} = 1 \pmod{53} \rangle$. Alice and Bob make public the group G.

	Alice		Bob
Private	$a = 29$		$b = 19 \in \mathbb{Z}_n$
Public	g^a	$\longrightarrow$	$g^a = 2^{29} \equiv 45 \pmod{53} \in G$
Public	$g^b = 12$	$\longleftarrow$	$g^b = 2^{19} \equiv 12 \pmod{53} \in G$

Now, Alice will calculate

$$(g^b)^a = (12)^{29} \pmod{53}$$
$$12^2 = 144 \equiv 38 \pmod{53}$$
$$12^4 = 1444 \equiv 13 \pmod{53}$$
$$12^8 = 169 \equiv 10 \pmod{53}$$
$$12^{16} = 100 \equiv -6 \pmod{53}$$
$$12^{24} = 12^{16} \cdot 12^8 \equiv -60 \equiv -7 \pmod{53}$$
$$12^{29} = 12^{24} \cdot 12^4 \cdot 12^1 = -7 \cdot 13 \cdot 12 = -1092 \equiv 21 \pmod{53}$$

Since $g^b = 12 \implies b = 19$ (as the least non-negative integer x such that $g^x = y$, for $y = 12, g = 2 \in G$)
$g^a = 45 \quad b = 19$
Now, Bob will calculate

$$\begin{aligned}(g^a)^b = (45)^{19} &\equiv (-8)^{19} \pmod{53} \\ &\equiv (-2^3)^{19} \pmod{53} \\ &\equiv (-1)^3 2^{57} \pmod{53} \\ &\equiv (-1)^3 2^{52} \cdot 2^5 \pmod{53} \\ &\equiv -32 \pmod{53} \\ &\equiv 21 \pmod{53}\end{aligned}$$

Alice choose $a = 29$, Bob choose $b = 19$ and kept as a secret. Made public $g^a = 2^{29} \equiv 45 \pmod{53}$ and $g^b = 2^{19} \equiv 12 \pmod{53}$. Then common shared key $k = 21$.

Massey-Omura Cryptosystem

Let $G = \langle g | g^n = 1 \rangle$ be a cyclic group generated by g and be public. Suppose a message $M \in G$ is sent by Alice and Bob. They choose integer in $\mathbb{Z}_n$ a and b respectively and keep secret. Then Alice and Bob exchange the key as follows.

	Alice		Bob
Private	a		$b \in \mathbb{Z}_n$
	M^a	$\longrightarrow$	$M^a \in G$
	$M^{ab} = (M^a)^b$	$\longleftarrow$	$(M^a)^b \in G$
	$(M^{ba})^{a^{-1}}$	$\longrightarrow$	$(M^{ba})^{a^{-1}} = M^b$

Hence Bob receives the message M by computing $(M^b)^{b^{-1}} = M$. Provided a^{-1} and b^{-1} exist in Modulo $\phi(n)$.

Example: Let $\mathcal{A} = \{A = 0, B = 1, \ldots, Z = 25, ? = 26, ! = 27, @ = 28\}$, $n = 29, \quad \phi(29) = 28$
Alice wants to send message **"CARTOON"**.
Alice: private key $a = 5$
Bob : Private key $b = 3$
To send M='C'=2 Alice will send to Bob

$$M^a = 2^5 \equiv 3 \pmod{29}$$

Now Bob will send to Alice

$$(M^a)^b = 3^3 \equiv 27 \pmod{29}$$

Alice will send to Bob

$$(M^{ab})^{a^{-1}} = 27^{5^{-1}} \equiv 27^{17} \equiv 8 \pmod{29} \quad (\text{since } 5^{-1} \equiv 17 \pmod{28})$$

Bob get the message by computing $(M^b)^{b^{-1}} = 8^{3^{-1}} \equiv 8^{19} \equiv 2 \pmod{29}$ ='C' (since $3^{-1} \equiv 19 \pmod{28}$).

ElGamal Cryptosystem

Let $G =< g|g^n = 1 >$ be public. All users, say Alice and Bob ... . They choose random integers $a,\ b,\ \ldots$ respectively and keep it secret and make $g^a, g^b, \cdots \in G$ public.
Now, if Bob wants to send message $\mathcal{M}$ to Alice. He choose a random integer k and create a mask by doing $(g^a)^k \in G$. Bob then sends to Alice $(g^k, \mathcal{M}g^{ak}) \in G \times G$.
Alice will receive $(g^k, \mathcal{M}g^{ak}) \in G \times G$, to recover $\mathcal{M}$ from order pair $(g^k, \mathcal{M}g^{ak})$, Alice will recreate the mask by doing $(g^k)^a = g^{ka} = g^{ak} \in G$, as Alice know a (secret) and g^k is first element of order pair $(g^k, \mathcal{M}g^{ak})$ received from Bob.
To recover the message, Alice will compute

$$(\mathcal{M}g^{ak})(g^{ak})^{-1} = \mathcal{M} \in G$$

Example: Let $G = \mathbb{Z}^*_{29} =< 2 \mid 2^{28} = 1 >= \{2^0, 2^1, 2^3, \ldots 2^{27}\} = \{1, 2, 4, 8, 16, , 6, 12, 24 \ldots\}, \quad |G| = 28$
suppose $\mathcal{A} = \{A = 1, B = 2, C = 4, D = 8, E = 16, F = 3, G = 6, H = 12, I = 24 \ldots\}$, $|\mathcal{A}| = 28$
Alice: Private key $a = 3$, Public key: $g^a = 2^3 = 8$
Bob wants to send message "HELLO"
To send $\mathcal{M}$=H= $12 = 2^7 \in G$,
Bob choose $k = 5$,
create mask:

$$(g^a)^k = (2^3)^5 = 2^{15} \equiv 27 \pmod{29}$$

Bob knows: $k,\ g^a = 8,$ and $\mathcal{M}$,
Bob will send to Alice $(g^k, \mathcal{M}g^{ak})$ i.e.

$$(2^5, 12 \cdot 27) = (3, 5) \in G \times G$$

Alice knows : a and $(g^k, \mathcal{M}g^{ak}) = (3, 5) \in G \times G$
Now, to recover the message Alice recreate the mask

$$(g^k)^a = 3^3 \equiv 27 \pmod{29} \in G$$

and compute

$$\mathcal{M}(g^{ak}) \cdot [g^{ak}]^{-1} = 5 \cdot 27^{-1} \equiv 5 \cdot 14 \equiv 12 \pmod{29}$$

(since $27^{-1} \equiv 14 \pmod{29}$)
So, Alice will get $\mathcal{M}$ =H (as 12 correspond to H)

Discrete Logarithm

Definition: Let G be a group and $g, h \in G$, then x is called the **discrete logarithm for h in G to the base g** (denoted as $x = dlog_g h$) if x is the least non negative integer satisfying $g^x = h$.

Note :

1. Discrete Logarithm may or may not exists.
   If discrete loagrithm for h in G to the base g exists, then we say $dlog_g h$ exists.
   If discrete loagrithm for h in G to the base g does not exist, then we say $dlog_g h$ does not exist.

2. If G is a finite cyclic group of order n with generator g
   that is, $G = < g |\ g^n = I_G >$, then $\forall\ h \in G,\ \exists\ x$ such that $g^x = h$

Examples :

1. Let $G = \mathbb{Z}_p$, where p is prime, then G **is cyclic**. Generators of G are all those integers elements of G whose g.c.d. with p is 1. Let $a \in G$ such that g.c.d.$(a, p) = 1$, then $\forall\ b \in G,\ \exists\ x$ such that $a^x = b$.

2. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$, then G **is abelian but not cyclic**.
   Note that $(0,1)^2 = (0,1) + (0,1) = (0,0)$, $(1,0)^2 = (1,0) + (1,0) = (0,0)$, $(1,1)^2 = (1,1) + (1,1) = (0,0)$.
   In this case discrete logarithm for any element of G to any base will not exists except $(0,0)$.

3. Let $G = S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ be the set of permutations on symbols $\{1, 2, 3\}$ then G **is neither abelian nor cyclic**.

   Note that
   $(1\ 2)(1\ 2) = I$
   $(1\ 3)(1\ 3) = I$
   $(2\ 3)(2\ 3) = I$
   $(1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2)$
   $(1\ 2\ 3)(1\ 2\ 3)(1\ 2\ 3) = I$
   $(1\ 3\ 2)(1\ 3\ 2) = (1\ 2\ 3)$
   $(1\ 3\ 2)(1\ 3\ 2)(1\ 3\ 2) = I$

   Observe that $dlog_{(1\ 2\ 3)}(1\ 3\ 2) = 2$
   Similarly $dlog_{(1\ 3\ 2)}(1\ 2\ 3) = 2$
   But $dlog_{(1\ 2\ 3)}(1\ 2)$ does not exists.

   Similarly check for others elements with different bases.

4. Let $G = D_8 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\} =< a, b | a^4 = 1,\ b^2 = 1,\ ab = ba^3 >$, where D_8 is the dihedral group of order 8 and a be the rotation and b be the reflction, then G **is neither abelian nor cyclic**. Generators of G are a and b.

   (a) Check for each elements with base = a.

   (b) Check for each elements with base = b.

The computation of discrete logarithm whenever exists is called Discrete Logarithm Problem (DLP).

The discrete logarithm problem is solvable in a cyclic group to the base g, where g is a generator of G. We shall discuss some algorithms to compute the discrete logarithm in a finite cyclic group of order n, say $G = < g : g^n = 1 >$:

1. By enumeration : The DLP is solvable. Hence, to compute $x = dlog_g h$ for an element h of G, simply by raising powers of g, till it becomes h. This is the simplest way. It always works. It needs only to store $x,\ g,\ g^x$. The problem is computation of g powers in a large finite cyclic group, as enumeration requires $x - 1$ multiplications and x number of comparisons in G. The method is not suitable for practical purposes, as x is usually desired to be large. Thus we need to look for other algorithms.

2. Some more algorithms are given as:

   (a) Shank Baby-Step Giant-Step Algorithm (given by Donald Shanks).

   (b) Pollard's Rho Algorithm (given by JH Pollard).

   (c) Pohlig-Hellman Algorithm

   (d) Index Calculus Algorithm (in its most basis setup). This is the fastest known algorithm.

Shank Baby-Step Giant-Step Algorithm

- This algorithm is given by Daniel Shanks in his paper "Class number, a theory of factorization and genera" in 1971.
- The baby-step giant-step algorithm is a generic algorithm. It works for every finite cyclic group.
- The algorithm is based on a space–time tradeoff. It is a fairly simple modification of trial multiplication, the naive method of finding discrete logarithms.
- The algorithm requires $O(m)$ memory where $m = \sqrt{n}$, and n is equal to the order of group.(that we will see later).
- As the name suggests, this method is divided into two parts. We call them as Baby Steps and Giant Steps.

Set up
Let G be a finite cyclic group.
$G = < g |\ g^n = 1 >$
Then, $\forall\ a \in G,\ dlog_g a$ exists.
Let, m be the least positive integer greater than or equal to $\sqrt{n}$.
Let $x = dlog_g a \quad \Rightarrow \quad g^x = a$
$\Rightarrow\ \exists\ q, r\ \in \mathbb{Z},\ 0 \leq r < m$ such that $x = mq + r$.
$\Rightarrow\ g^x = g^{mq\ +\ r} = a$
$\Rightarrow\ g^{mq} = ag^{-r}$

Algorithm :

Baby Steps
To compute baby steps, we compute a set

$$B \;=\; \{(ag^{-r}, r) | 0 \leq r \leq m-1\}$$

that is,

$$B \;=\; \{(a,0),\ (ag^{-1},1),\ (ag^{-1},1),\ (ag^{-2},2),\ (ag^{-3},3),\ \ldots,\ (ag^{-(m-1)},m-1)\}$$

If $\exists\ s,\ 0 \leq s \leq m-1$ such that $(ag^{-s}, s) \;=\; (1,s) \;\in\; B$,
then, $ag^{-s} \;=\; 1 \quad \Rightarrow \quad a \;=\; g^s \quad \Rightarrow \quad s \;=\; dlog_g a$
If such s does not exists, we go the Giant Steps.

Giant Steps:
If such s does not exists, that is, there dose not any $t,\ 0 \leq t \leq m-1$ such that $(ag^{-t}, t) \;=\; (1,t) \;\in\; B$, we go the Giant Steps.
To compute giant steps, we compute :

$$g^m,\ (g^m)^2,\ (g^m)^3,\ (g^m)^4,\ \ldots$$

that is,

$$(g^m)^i\ ,\quad i \;=\; 1,2,3,...$$

till we get some q such that $(g^m)^q \;=\; ag^{-r}$ for some $0 \leq r \leq m-1$.
In that case $(g^m)^q \;=\; ag^{-r} \quad \Rightarrow \quad g^{mq\,+\,r} \;=\; a$
and hence $dlog_g a \;=\; mq \;+\; r \;=\; x$.

Examples :

1. Determine, if exists, $dlog_5 3$ in $\mathbb{Z}_{53}^*$.

   Let, m be the least positive integer greater than or equal to $\sqrt{53} \;=\; 7.2\ approx.$
   $\Rightarrow \quad m \;=\; 8$
   Let $x \;=\; dlog_5 3 \quad \Rightarrow \quad 5^x \;=\; 3.$
   $\Rightarrow\ \exists\ q, r \;\in \mathbb{Z},\ 0 \leq r < 8$ such that $x \;=\; 8q \;+\; r$.

   Baby Steps :
   To compute baby steps, we compute a set

   $$B \;=\; \{(ag^{-r}, r)/0 \leq r \leq 7\}$$

   that is,

   $$B \;=\; \{(a,0),\ (ag^{-1},1)\ (ag^{-2},2),\ (ag^{-3},3),\ (ag^{-4},4),\ (ag^{-5},5),\ (ag^{-6},6),\ (ag^{-7},7)\}$$

   Note that $g^{-1} \;\equiv\; 5^{-1} \;\equiv\; 32\ (mod\ 53)$

$$\Rightarrow B = \{(3,0),\ (3\cdot 32,1),\ (3\cdot(32)^2,2),\ (3\cdot(32)^3,3),\ (3\cdot(32)^4,4),\ (3\cdot(32)^5,5),\ (3\cdot(32)^6,6),\ (3\cdot(32)^7,7)\}$$

$$\Rightarrow B = \{(3,0),\ (43,1),\ (51,2),\ (42,3),\ (19,4),\ (25,5),\ (5,6),\ (1,7)\}$$

Since $\exists\ s = 7$, such that $(ag^{-s}, s) = (1,s) = (1,7) \in B$,
then, $3 * 5^{-7} \equiv 1\ (mod\ 53) \quad \Rightarrow \quad 3 = 5^7 \quad \Rightarrow \quad 7 = dlog_5 3$

2. Determine, if exists, $dlog_5 15$ in $\mathbb{Z}_{37}^*$.

   Let, m be the least positive integer greater than or equal to $\sqrt{37} = 6.08\ approx.$
   $\Rightarrow \quad m = 7$
   Let $x = dlog_5 15 \quad \Rightarrow \quad 5^x = 15.$
   $\Rightarrow\ \exists\ q, r\ \in \mathbb{Z},\ 0 \le r < 7$ such that $x = 7q + r$.

   Baby Steps :

   To compute baby steps, we compute a set

   $$B = \{(ag^{-r}, r) | 0 \le r \le 6\}$$

   that is,

   $$B = \{(a,0),\ (ag^{-1},1)\ (ag^{-2},2),\ (ag^{-3},3),\ (ag^{-4},4),\ (ag^{-5},5),\ (ag^{-6},6)\}$$

   Note that $g^{-1} \equiv 5^{-1} \equiv 15\ (mod\ 37)$

   $$\Rightarrow B = \{(15,0),\ (15\cdot 15,1),\ (15\cdot(15)^2,2),\ (15\cdot(15)^3,3),\ (15\cdot(15)^4,4),\ (15\cdot(15)^5,5),\ (15\cdot(15)^6,6),\ (15\cdot(15)^7,7)\}$$

   $$\Rightarrow B = \{(15,0),\ (3,1),\ (8,2),\ (9,3),\ (24,4),\ (27,5),\ (35,6)\}$$

   Since there does not exists s, such that $(ag^{-s}, s) = (1,s) \in B$,
   thus we go to giant step.

   Giant Steps :

   To compute giant steps, we compute :

   $$g^m,\ (g^m)^2,\ (g^m)^3,\ (g^m)^4,\ \ldots$$

   that is,

   $$(5^7)^i\ ,\quad i = 1,2,3,...$$

   Note that

   $$(5^7)^1 = 18$$
   $$(5^7)^2 = 28$$

$$(5^7)^3 \;=\; 23$$

$$(5^7)^4 \;=\; 7$$

$$(5^7)^5 \;=\; 15$$

Here we get $q \;=\; 5$ such that $(g^m)^q \;=\; (5^7)^5 \;=\; 15 \;=\; ag^{-r}$ for $r \;=\; 0$.
Hence $(5^7)^5 \;=\; 15 \quad \Rightarrow \quad dlog_5 15 \;=\; 7 \cdot 5 \;+\; 0 \;=\; 35$.

Lecture-11

Discrete Logarithm Algorithm

Pollard's ρ algorithm for discrete logarithm

Let G be a finite multiplicative cyclic group generated by g of order n , i.e.

$$G =< g|g^n = 1 >$$

To find : $dlog_g a$ (it exists as G is cyclic)
Let G_1, G_2, G_3 be pairwise disjoint subsets of G such that $G = G_1 \cup G_2 \cup G_3$.
Define a function f
$f : G \to G$ where $G = G_1 \cup G_2 \cup G_3$
such that for $b \in G$

$$b \to f(b) = \begin{cases} gb & \text{if } b \in G_1 \\ b^2 & \text{if } b \in G_2 \\ ab & \text{if } b \in G_3 \end{cases}$$

Then we choose a random integer $x_0 \in \{1, 2, 3, ..., n\}$ and define $b_0 = g^{x_0} \in G$, and a sequence of elements $\{b_0, b_1, ...\}$ of G by

$$b_{i+1} = f(b_i) \quad \forall i \geq 0$$

for example :

$$b_1 = f(b_0) = \begin{cases} gb_0 & \text{if } b_0 \in G_1 \\ {b_0}^2 & \text{if } b_0 \in G_2 \\ ab_0 & \text{if } b_0 \in G_3 \end{cases} = \begin{cases} gg^{x_0} & \text{if } b_0 \in G_1 \\ (g^{x_0})^2 & \text{if } b_0 \in G_2 \\ ag^{x_0} & \text{if } b_0 \in G_3 \end{cases} = \begin{cases} g^{x_0+1} & \text{if } b_0 \in G_1 \\ g^{2x_0} & \text{if } b_0 \in G_2 \\ ag^{x_0} & \text{if } b_0 \in G_3 \end{cases}$$

as $b_0 = g^{x_0}$
similarly

$$b_2 = f(b_1) = \begin{cases} gb_1 & \text{if } b_1 \in G_1 \\ {b_1}^2 & \text{if } b_1 \in G_2 \\ ab_1 & \text{if } b_1 \in G_3 \end{cases}$$

NOTE 1 : $b_i \in G$ and b_i is of the form $b_i = g^{x_i}a^{y_i} \quad (i \geq 0)$
thus $b_{i+1} = f(b_i) = g^{x_{i+1}}a^{y_{i+1}}$

So,

$$b_1 = g^{x_1}a^{y_1} = \begin{cases} g^{x_0+1} & \text{if } b_0 \in G_1 \\ g^{2x_0} & \text{if } b_0 \in G_2 \\ ag^{x_0} & \text{if } b_0 \in G_3 \end{cases} = \begin{cases} g^{x_0+1}a^0 & \text{if } b_0 \in G_1 \\ g^{2x_0}a^0 & \text{if } b_0 \in G_2 \\ g^{x_0}a^1 & \text{if } b_0 \in G_3 \end{cases}$$

thus,

$$x_1 = \begin{cases} x_0 + 1 & \text{if } b_0 \in G_1 \\ 2x_0 & \text{if } b_0 \in G_2 \\ x_0 & \text{if } b_0 \in G_3 \end{cases}$$

and

$$y_1 = \begin{cases} y_0 & \text{if } b_0 \in G_1 \\ 2y_0 & \text{if } b_0 \in G_2 \\ y_0 + 1 & \text{if } b_0 \in G_3 \end{cases}$$

Iterating till i times, we get

$$x_{i+1} = \begin{cases} x_i + 1 \pmod n & \text{if } b_i \in G_1 \\ 2x_i \pmod n & \text{if } b_i \in G_2 \\ x_i \pmod n & \text{if } b_i \in G_3 \end{cases}$$

and

$$y_{i+1} = \begin{cases} y_i \pmod n & \text{if } b_i \in G_1 \\ 2y_i \pmod n & \text{if } b_i \in G_2 \\ y_i + 1 \pmod n & \text{if } b_i \in G_3 \end{cases}$$

NOTE 2 :

- we can prove it by induction
- we won't write $\pmod n$ again and again.

The sequence $\{b_m\}_{m=0}$ must be a finite sequence (as G is finite) and thus it terminates at some finite step. Suppose

$$\begin{aligned} b_{i+k} &= b_i \text{ for some } i, k \\ g^{x_{i+k}}\ a^{y_{i+k}} &= g^{x_i}\ a^{y_i} \\ g^{x_{i+k}-x_i} &= a^{y_i-y_{i+k}} \text{ in } \ G =< g|g^n = 1 > \end{aligned}$$

If $x = dlog_g a$, then $g^x = a$ Thus,

$$x_{i+k} - x_i \equiv x\ (y_i - y_{i+k}) \pmod{\phi(n)}$$
$$x \equiv (y_i - y_{i+k})^{-1}\ (x_{i+k} - x_i) \pmod{\phi(n)}$$

- If $(y_i - y_{i+k})^{-1} \pmod{\phi(n)}$ exists, then $dlog_g a = x$ is uniquely determined.
- If $(y_i - y_{i+k})^{-1} \pmod{\phi(n)}$ does not exist, the congruence

  $$x_{i+k} - x_i \equiv x\ (y_i - y_{i+k}) \pmod{\phi(n)}$$

  can still be solved and x can be determined from various possible solutions (by putting $g^x = a$ for least possible x).

EXAMPLE 1 : Determine if exists $dlog_5 18$ in $\mathbb{Z}_{23}^* = G$ where $|G| = 22$.
Assume $G_1 = \{1, 2, ..., 7\}$, $G_2 = \{8, 9, ..., 14\}$, $G_3 = \{15, 16, ..., 22\}$

(we have divided the group in this way but it can be divided in any way by choice)
Let $x_0 = 2$,
$b_0 = g^{x_0} = 5^2 \equiv 25 \equiv 2 \pmod{23}$

$b_0 = g^{x_0} a^{y_0} = (5^2)(18^0) \equiv 2 \pmod{23}$ and $2 \in G_1$

$b_1 = g^{x_1} a^{y_1} = g^{x_0+1} a^{y_0} = (5^3)(18^0) \equiv 10 \pmod{23}$ and $10 \in G_2$

$b_2 = g^{x_2} a^{y_2} = g^{2x_1} a^{2y_1} = (5^6)(18^0) \equiv 8 \pmod{23}$ and $8 \in G_2$

$b_3 = g^{x_3} a^{y_3} = g^{2x_2} a^{y_2} = (5^{12})(18^0) \equiv 18 \pmod{23}$ and $18 \in G_3$

$b_4 = g^{x_4} a^{y_4} = g^{x_3} a^{y_3+1} = (5^{12})(18^1) \equiv 2 \pmod{23}$ and $2 \in G_1$

Note that

$$\begin{aligned} b_4 &= b_0 \\ \implies g^{x_4} a^{y_4} &= g^{x_0} a^{y_0} \\ \implies g^{x_4 - x_0} &= a^{y_0 - y_4} \\ \implies x_4 - x_0 &\equiv x(y_0 - y_4) \pmod{22} \\ \implies 12 - 2 &\equiv x(0 - 1) \pmod{22} \\ \implies x &\equiv -10 \equiv 12 \pmod{22} \end{aligned}$$

Thus $dlog_5 18 = 12$

Index Calculus Algorithm in $\mathbb{Z}_p$:

Let $G = \mathbb{Z}_p^* = \langle g |\ g^{p-1} = 1 \rangle$. and $x = dlog_g a$ where $a \in G$. So $g^x \equiv a \pmod{p}$.
We choose a bound $\mathcal{B}$ and determine factor base $\mathcal{F}(\mathcal{B}) = \{q \in \mathbb{P} | q \leq \mathcal{B}\}$ where $\mathbb{P}$ is set of all prime numbers.
An integer b is said to be $\mathcal{B}$-smooth number if all prime divisors of b lie in $\mathcal{F}(\mathcal{B})$. That is if p is a prime such that $p|b$ and $p \leq \mathcal{B}$.

Example: If $\mathcal{B} = 15$ then $\mathcal{F}(\mathcal{B}) = \{2, 3, 5, 7, 11, 13\}$. The integer 990 is 15-smooth, since $990 = 2 \times 3^2 \times 5 \times 11$ and $2, 3, 5, 11 \in \mathcal{F}(\mathcal{B})$.

Step-1: Computing the discrete logarithm of the factor base elements.
That is solve for

$$x = x(q) \quad \forall q \in \mathcal{F}(\mathcal{B})$$

such that

$$g^{x(q)} \equiv q \pmod{p}$$

Step-2: Determine an exponent $y \in \{1, 2, \ldots, p-1\}$ such that $ag^y \pmod{p}$ is $\mathcal{B}$-smooth.
That is

$$ag^y \equiv \prod_{q \in \mathcal{F}(\mathcal{B})} q^{e(q)} \pmod{p}$$

where $e(q) \geq 0$ and $q \in \mathcal{F}(\mathcal{B})$.
Now

$$\begin{aligned} ag^y &\equiv \prod_{q \in \mathcal{F}(\mathcal{B})} q^{e(q)} \pmod{p} \\ &\equiv \prod_{q \in \mathcal{F}(\mathcal{B})} [g^{x(q)}]^{e(q)} \pmod{p} \\ &\equiv \prod_{q \in \mathcal{F}(\mathcal{B})} g^{x(q)e(q)} \pmod{p} \\ &\equiv g^{\sum_{q \in \mathcal{F}(\mathcal{B})} x(q)e(q)} \pmod{p} \end{aligned}$$

Hence

$$a \equiv g^{\left\{\left(\sum_{q \in \mathcal{F}(\mathcal{B})} x(q)e(q)\right) - y\right\}} \pmod{p}$$

This implies

$$g^x \equiv g^{\left\{\left(\sum_{q\in\mathcal{F}(\mathcal{B})} x(q)e(q)\right)-y\right\}} \pmod{p}$$
$$\implies x \equiv \left\{\left(\sum_{q\in\mathcal{F}(\mathcal{B})} x(q)e(q)\right) - y\right\} \pmod{p-1}$$

This gives the discrete log x of a to the base g.

Now for step-1, to determine of $x(q)$ the discrete log of the element $q \in \mathcal{F}(\mathcal{B})$.

For this we choose random integer $z \in \{1, 2, \ldots, p-1\}$ and compute $g^z \pmod{p}$, and check if these are $\mathcal{B}$-smmoth. If yes then compute the decomoposition:

$$g^z \pmod{p} = \prod_{q\in\mathcal{F}(\mathcal{B})} q^{f(q,z)}$$

Each exponent vector $f(q, z)$ (for $q \in \mathcal{F}(\mathcal{B})$) is called a relation.

Example: Let $p = 2027$, $g = 2$ and determine relations for the factor base $\mathcal{F}(\mathcal{B}) = \mathcal{F}(12) = \{2, 3, 5, 7, 11\}$.
Let $z = 1593$, then $g^z = 2^{1593} \equiv 33 \pmod{2027}$. Since $33 = 3 \times 11$ hence it is $\mathcal{B}$-smooth .
Similarly $2^{10} = 1024$ and $2^{11} = 2048 \equiv 21 = 3 \times 7 \pmod{2027}$ are $\mathcal{B}$-smooth number. If we have found as many relations as there are factor base elements, then we try to find the discrete logrithic by solving a system of linear congurences:

$$\begin{aligned}
3 \times 11 = 33 &\equiv 2^{1593} \pmod{2027} \\
5 \times 7 \times 11 = 385 &\equiv 2^{983} \pmod{2027} \\
2^7 \times 11 = 1408 &\equiv 2^{1318} \pmod{2027} \\
3^2 \times 7 = 63 &\equiv 2^{293} \pmod{2027} \\
2^6 \times 5^2 = 1600 &\equiv 2^{1918} \pmod{2027} \\
3 \times 7 = 21 &\equiv 2^{11} \pmod{2027}
\end{aligned}$$

Thus,

$$\begin{aligned} g^z &\equiv \prod_{q\in\mathcal{F}(\mathcal{B})} q^{f(q,z)} \pmod p \\ &\equiv \prod_{q\in\mathcal{F}(\mathcal{B})} [g^{x(q)}]^{f(q,z)} \pmod p \\ &\equiv g^{\left(\sum_{q\in\mathcal{F}(\mathcal{B})} x(q)f(q,z)\right)} \pmod p \end{aligned}$$

This implies that

$$g^{\left(z-\sum_{q\in\mathcal{F}(\mathcal{B})} x(q)f(q,z)\right)} \equiv 1 \pmod p$$

Implies that

$$z \equiv \sum_{q\in\mathcal{F}(\mathcal{B})} x(q)f(q,z) \pmod{p-1} \quad \forall z : g^z \pmod p \text{ is } \mathcal{B}-\text{smooth}$$

Hence we have a system of linear congruence in variables $x(q)$ for all $q \in \mathcal{F}(\mathcal{B})$

Example: Lep $p = 2027$ and $g = 2$
Factor base $\mathcal{F}(\mathcal{B}) = \{2, 3, 5, 7, 11\}$

Step-1 To find $dlog_g q \ \forall q \in \mathcal{F}(\mathcal{B})$ i.e. $dlog_g 2$, $dlog_g 3$, $dlog_g 5$, $dlog_g 7$, and $dlog_g 11$
For $q = 2$ $\quad dlog_2 2 = 1$(since $2^1 \equiv 2 \pmod p$)
So we have $x(2) = 1$.
Suppose $g^{x(q)} = q \quad \forall q \in \mathcal{F}(\mathcal{B})$ i.e.

$$g^{x(3)} = 3,\ g^{x(5)} = 5,\ g^{x(7)} = 7,\ g^{x(11)} = 11,$$

$z = 1593$ $\quad g^z = 2^{1593} \equiv 33 \equiv 11 \times 3 \pmod{2027}$ which is $\mathcal{B} - smooth$.
i.e.

$$g^z = 2^{1593} \equiv 33 \equiv 11 \times 3 \pmod{2027} \equiv g^{x(3)} \cdot g^{x(11)} \pmod p$$

i.e.

$$\begin{aligned} & g^{x(3)+x(11)-z} \equiv 1 \pmod{2027} \\ \implies & x(3) + x(11) - z \equiv 0 \pmod{2026} \\ \implies & x(3) + x(11) \equiv 1593 \pmod{2026} \end{aligned} \tag{1}$$

(since $(p-1) \mid (x(3)+x(11)-z)$ and $z = 1593$, $p = 2027$)

Next, $z = 983 \implies g^z = 2^{983} \equiv 385 \equiv 5 \times 7 \times 11 \pmod{2027}$ which is $\mathcal{B} - smooth$.
i.e.

$$g^z = 2^{983} \equiv g^{x(5)} \cdot g^{x(7)} \cdot g^{x(11)} \pmod{p}$$

i.e.

$$\begin{aligned} & g^{x(5)+x(7)+x(11)-z} \equiv 1 \pmod{2027} \\ \implies & x(5)+x(7)+x(11)-z \equiv 0 \pmod{2026} \\ \implies & x(5)+x(7)+x(11) \equiv 983 \pmod{2026} \end{aligned} \tag{2}$$

Similarly,
$z = 1318 \implies g^z = 2^{1318} \equiv 1408 \equiv 2^7 \times 11 \pmod{2027}$ which is $\mathcal{B} - smooth$.
i.e.

$$g^z = 2^{1318} \equiv g^{7x(2)} \cdot g^{x(11)} \pmod{p}$$

i.e.

$$\begin{aligned} & g^{7x(2)+x(11)-z} \equiv 1 \pmod{2027} \\ \implies & 7x(2)+x(11)-z \equiv 0 \pmod{2026} \\ \implies & 7x(2)+x(11) \equiv 1318 \pmod{2026} \end{aligned} \tag{3}$$

Similarly, $z = 293 \implies g^z = 2^{293} \equiv 3^2 \times 7 \pmod{2027}$ which is $\mathcal{B} - smooth$.
i.e.

$$g^z = 2^{293} \equiv g^{2x(3)} \cdot g^{x(7)} \pmod{p}$$

i.e.

$$\begin{aligned} & g^{2x(3)+x(7)-z} \equiv 1 \pmod{2027} \\ \implies & 2x(3)+x(7)-z \equiv 0 \pmod{2026} \\ \implies & 2x(3)+x(7) \equiv 293 \pmod{2026} \end{aligned} \tag{4}$$

Similarly, we have
for $z = 1918$

$$\implies 6x(2) + 2x(5) \equiv 1918 \pmod{2026} \tag{5}$$

and for $z = 11$

$$\implies x(3) + x(7) \equiv 11 \pmod{2026} \tag{6}$$

Finally we have six equations (1)-(6) to calculate $x(3),\ x(5),\ x(7),\ x(11)$ and we already know $x(2) = 1$.

Note- In fact we need only four equations to calculate four unknowns.

Now we have to solve system of equations (1)-(6) for $x(3),\ x(5),\ x(7),\ x(11)$ Note that $2026 = 2 \times 1013$. So we solve system of equations Modulo 2 and Modulo 1013.

$$x(3) + x(11) \equiv 1593 \equiv 1 \pmod{2} \tag{7}$$
$$x(5) + x(7) + x(11) \equiv 983 \equiv 1 \pmod{2} \tag{8}$$
$$7x(2) + x(11) \equiv 1318 \equiv 0 \pmod{2} \tag{9}$$
$$2x(3) + x(7) \equiv x(7) \equiv 293 \equiv 1 \pmod{2} \tag{10}$$
$$6x(2) + 2x(5) \equiv 1918 \pmod{2} \textbf{(This is of form 0=0)} \tag{11}$$
$$x(3) + x(7) \equiv 11 \equiv 1 \pmod{2} \tag{12}$$

we know $x(2) = 1 \pmod{2026} \implies x(2) = 1 \pmod{2}$ also.
On solving above system of equation, we get

$$x(3) \equiv 0 \pmod{2}$$
$$x(5) \equiv 1 \pmod{2}$$
$$x(7) \equiv 1 \pmod{2}$$
$$x(11) \equiv 1 \pmod{2}$$

and system of equation Modulo 1013

$$x(3) + x(11) \equiv 1593 \equiv 580 \pmod{1013} \tag{13}$$
$$x(5) + x(7) + x(11) \equiv 983 \pmod{1013} \tag{14}$$
$$7x(2) + x(11) \equiv 1318 \equiv 305 \pmod{1013} \tag{15}$$
$$2x(3) + x(7) \equiv 293 \pmod{1013} \tag{16}$$
$$6x(2) + 2x(5) \equiv 1918 \equiv 905 \pmod{1013} \tag{17}$$
$$x(3) + x(7) \equiv 11 \pmod{1013} \tag{18}$$

On solving above system , we get

$$\begin{aligned} x(3) &\equiv 282 \pmod{1013} \\ x(5) &\equiv 956 \pmod{1013} \\ x(7) &\equiv 742 \pmod{1013} \\ x(11) &\equiv 298 \pmod{1013} \end{aligned}$$

Now we have solutions in Modulo 2 and Modulo 1013, we can easily calculate solution Modulo 2026, using Chinese Remainder Theorem

$x(3) \equiv 0 \pmod{2}$
$x(3) \equiv 282 \pmod{1013}$
$x(3) \equiv 282 \pmod{2026}$ (by applying Chinese Remainder Theorem)

$x(5) \equiv 1 \pmod{2}$
$x(5) \equiv 956 \pmod{1013}$
$x(5) \equiv 1969 \pmod{2026}$ (by applying Chinese Remainder Theorem)

$x(7) \equiv 1 \pmod{2}$
$x(7) \equiv 742 \pmod{1013}$
$x(7) \equiv 1755 \pmod{2026}$ (by applying Chinese Remainder Theorem)

$x(11) \equiv 1 \pmod 2$
$x(11) \equiv 298 \pmod{1013}$
$x(11) \equiv 1311 \pmod{2026}$ (by applying Chinese Remainder Theorem)

Now to calculate $dlog_g a$ for g=2 and for given a
Factor base $\mathcal{F}(\mathcal{B}) = \{2, 3, 5, 7, 11\}$

(1). For $a = 12$
$a = 12 = 2^2 \cdot 3$ i.e a is $\mathcal{B}$-smooth and we have $g^{x(2)} = 2^1 = 2$ and $g^{x(3)} = 2^{282} = 3$ Then

$$a = 12 = 2^2 \cdot 3 = (2^1)^2 \cdot 2^{282} = 2^{2+282} = 2^{284}$$

Therefore $dlog_g a = dlog_2 12 = 284$

(2.) For $a = 65$
$a = 65 = 5 \times 13$ is not $\mathcal{B}$-smooth.
Now we find $y \in \{1, 2, \ldots p-1\}$ such that $ag^y \pmod p$ is $\mathcal{B}$-smooth.

$$ag \equiv 65 \cdot 2 \pmod{2027} \equiv 13 \cdot 5 \cdot 2 \pmod{2027}$$
$$ag^2 \equiv 65 \cdot 2^2 \pmod{2027} \equiv 13 \cdot 5 \cdot 2^2 \pmod{2027}$$
$$ag^3 \equiv 65 \cdot 2^3 \pmod{2027} \equiv 13 \cdot 5 \cdot 2^3 \pmod{2027}$$

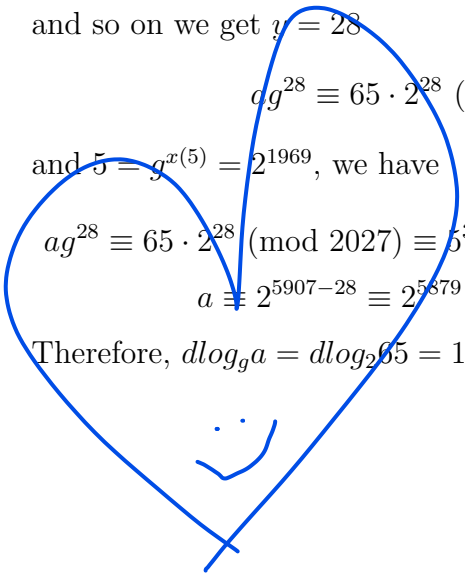
and so on we get $y = 28$

$$ag^{28} \equiv 65 \cdot 2^{28} \pmod{2027} \equiv 5^3 \pmod{2027}$$

and $5 = g^{x(5)} = 2^{1969}$, we have

$$ag^{28} \equiv 65 \cdot 2^{28} \pmod{2027} \equiv 5^3 \pmod{2027} \equiv (2^{1969})^3 \pmod{2027} \equiv 2^{5907}$$
$$a \equiv 2^{5907-28} \equiv 2^{5879} \pmod{2027} \equiv 2^{1827} \pmod{2027}$$

Therefore, $dlog_g a = dlog_2 65 = 1827$



Lecture-12

Discrete Logarithm Algorithm

Pohlig - Hellman Algorithm for discrete logarithm

Pohlig - Hellman Algorithm for a finite group of order n
About :

1. The Pohlig–Hellman algorithm, sometimes called as the Silver–Pohlig–Hellman algorithm, is a special-purpose algorithm for computing discrete logarithms in a finite abelian group whose order is a smooth integer.

2. The algorithm was introduced by Roland Silver, but first published by Stephen Pohlig and Martin Hellman.

3. The worst-case input for the Pohlig–Hellman algorithm is a group of prime order: In that case, it degrades to the baby-step giant-step algorithm, hence the worst-case time complexity is $\mathcal{O}(\sqrt{n})$. However, it is much more efficient if the order is smooth: Specifically, if $\prod_i p_i^{e_i}$ is the prime factorization of n, then the algorithm's complexity is

$$\mathcal{O}\left(\sum_i e_i(\log n + \sqrt{p_i})\right)$$

Algorithm :
Let G' be a finite abelian group of order k.
We need to compute $dlog_\gamma \alpha$, where $\alpha,\ \gamma\ \in\ G'$.
Assuming that $dlog_\gamma \alpha$ exists, we are considering a subgroup G of G' of order n such that

$$G\ = < \gamma | \gamma^n\ =\ 1 >$$

.
Thus G be a finite cyclic group of order n where $n = \prod_{p|n} p^{e(p)}$.

Then $\gamma \in G$, $O(\gamma) = n$, and, $dlog_\gamma \alpha$ exists.

Let $dlog_\gamma \alpha = x \implies \gamma^x = \alpha$.
For each prime p, $p|n$, denote

$$n_p = \frac{n}{p^{e(p)}}$$

Let, $\gamma_p = \gamma^{n_p} \in G$. Note that, $O(\gamma_p) = p^{e(p)}$

To check $O(\gamma_p) = p^{e(p)}$

Consider $(\gamma_p)^{p^{e(p)}} = (\gamma^{n_p})^{p^{e(p)}} = \gamma^{n_p p^{e(p)}} = \gamma^n = 1$.

$$\implies O(\gamma_p) | p^{e(p)}$$

To show $p^{e(p)} | O(\gamma_p)$, we prove it by contradiction.
Consider,

$$O(\gamma_p) = p^{\epsilon(p)}, \quad \text{where} \quad \epsilon(p) < e(p)$$

then $(\gamma_p)^{p^{\epsilon(p)}} = (\gamma^{n_p})^{p^{\epsilon(p)}} = \gamma^{\frac{n}{p^{e(p)-\epsilon(p)}}} = 1$
$\implies$ $O(\gamma) < n$, which is a contradiction.
Hence, $O(\gamma_p) = p^{e(p)}$

Since, $dlog_\gamma \alpha = x$, we assume $\alpha \neq 1$ [$\alpha = 1, \implies x = 0$]

Reduction to prime power order cyclic group :
Consider $\alpha_p = \alpha^{n_p}$, then

$$\gamma_p^x = (\gamma^{n_p})^x = \gamma^{n_p x} = (\gamma^x)^{n_p} = \alpha^{n_p} = \alpha_p$$

$$\implies \gamma_p^x = \alpha_p$$

Let $x(p) = dlog_{\gamma_p} \alpha_p$
Then $\gamma_P^{x(p)} = \alpha_p$ ($x(p)$ is the least non negative integer satisfying this relation.)

Let $H = < \gamma_p | \gamma_p^{p^{e(p)}} = 1 >$
Observe that

$$(\gamma^{-x}\alpha)^{n_p} = \gamma_p^{-x}\alpha_p = \alpha_p^{-1}\alpha_p = 1$$
$$\implies O(\gamma^{-x}\ \alpha)|n_p \quad \forall p|n$$
$$\implies O(\gamma^{-x}\ \alpha)|g.c.d.(n_p) \ \ \forall \text{ prime } p|n$$

and

$$g.c.d.(n_p) = 1 \ \ \forall \text{ prime } p|n$$
$$\implies O(\gamma^{-x}\ \alpha) = 1$$
$$\implies \gamma^{-x}\ \alpha = 1_G$$
$$\implies x = dlog_\gamma \alpha$$

Now,

$$H = < \gamma_p | \gamma_p^{p^{e(p)}} = 1 >$$

Then, note that $\alpha_p \in H$, which implies

$$\implies \gamma_p^{x-x(p)} = 1 \in H \ (\text{ since } \gamma_p^{-x}\alpha_p = 1 \implies \alpha_p = \gamma_p^x)$$

Since, $O(\gamma_p) = p^{e(p)}$ implies that

$$(x - x(p))|p^{e(p)}$$
$$\implies x \equiv x(p) \pmod{p^{e(p)}}$$

Since this relation holds for all prime divisors of n, thus the problem now reduces to the computation of $x(p)$ only. Once, we compute $x(p)$ for every prime (p) divisor of n, we can apply chinese remainder theorem to compute x.

Note that the problem now reduces to cyclic group of prime power order and computation of $x(p)$.

Now we further reduce the problem to a cyclic group of prime (p) order, where $p|n$.

Reduction to prime order group :

Let $H = < \gamma_p | \gamma_p^{p^{e(p)}} = 1 > \leq G \qquad \forall p|n$

Fix p as a prime divisor of n, then, $O(H) = p^{e(p)}$.

Notations :

Denote $e(p) = e$, $x(p) = x$, $\alpha_p = a$, $\gamma_p = g$.

Since we have to compute $x(p) = dlog_{\gamma_p}\alpha_p$, that is, we have to compute $x = dlog_g a$ in the set $H = < g | g^{p^e} = 1 >$

Since $x = dlog_g a \quad \Rightarrow \quad g^x = a$,

where $x = x_0 + x_1 p + x_2 p^2 + ... + x_{e-1} p^{e-1}, \quad 0 \leq x_i < p, \ \forall\ 0 \leq i \leq e-1$ be the p-nary representation of x can be obtained by division algorithm.

For example :
if $x = 9$ and $p = 3, e = 3$ then $O(H) = 3^3 = 27$ and $x = 0{+}0{\cdot}3{+}1{\cdot}3^2$,
if $x = 13$ and $p = 3, e = 3$ then $O(H) = 3^3 = 27$ and $x = 1{+}1{*}3{+}1{*}3^2$,
if $x = 26$ and $p = 3, e = 3$ then $O(H) = 3^3 = 27$ and $x = 2{+}2{*}3{+}2{*}3^2$.
Now,

$$
\begin{aligned}
& g^x = a \\
& \implies (g^x)^{p^{e-1}} = a^{p^{e-1}} \\
& \implies (g^{p^{e-1}})^x = a^{p^{e-1}} \\
& \implies g^{p^{e-1}x} = a^{p^{e-1}} \\
& \implies g^{p^{e-1}(x_0 + x_1 p + x_2 p^2 + \cdots + x_{e-1} p^{e-1})} = a^{p^{e-1}} \\
& \implies g^{(x_0 p^{e-1} + x_1 p^e + x_2 p^{e+1} + \cdots + x_{e-1} p^{2e-2})} = a^{p^{e-1}} \\
& \implies g^{x_0 p^{e-1}} \cdot g^{x_1 p^e} \cdot g^{x_2 p^{e+1}} \cdots g^{x_{e-1} p^{2e-2}} = a^{p^{e-1}}
\end{aligned}
$$

Note that $g^{p^e} = 1$, implies

$$g^{x_0 p^{e-1}} = a^{p^{e-1}}$$

$$\implies (g^{p^{e-1}})^{x_0} = a^{p^{e-1}}$$

Since $O(g) = p^e \implies g^{p^{e-1}} \neq 1 \implies x_0 = dlog_{g^{p^{e-1}}} a^{p^{e-1}}$ [Use same argument that we have used before to prove $x(p) = dlog_{\gamma_p}\alpha_p$]
Also, note that $O(g^{p^{e-1}}) = p$
Let $H_0 = \langle g^{p^{e-1}} | (g^{p^{e-1}})^p = 1 \rangle$ be a subgroup of H of order p,
then, $x_0 = dlog_{g^{p^{e-1}}} a^{p^{e-1}}$ in H_0.
Note that the problem now reduces to cyclic group of prime (p) order, namely

H_0 and computation of x_0.
To determine x_i for all i, we first calculate x_0 and then apply induction on x_i.
Suppose $x_0,\ x_1,\ x_2,\ \ldots\ x_{i-1}$ are determined, we need to determine x_i.
Now consider

$$\begin{aligned} g^{\left(x_i p^i + x_{i+1}p^{i+1} + \cdots + x_{e-1}p^{e-1}\right)} &= g^{\left(-x_0 - x_1 p - \cdots - x_{i-1}p^{i-1} \ + \ \sum_{j=0}^{e-1} x_j p^j\right)} \\ &= g^{-x_0 - x_1 p - \cdots - x_{i-1}p^{i-1}} \cdot g^x \\ &= g^{-x_0 - x_1 p - \cdots - x_{i-1}p^{i-1}} \cdot a \\ &= a_i \ \ (say) \end{aligned}$$

Thus, we have

$$g^{\left(x_i p^i + x_{i+1}p^{i+1} + \cdots + x_{e-1}p^{e-1}\right)} \ = \ a_i$$

Raising the power p^{e-i-1}, we get

$$\begin{aligned} & \left(g^{\left(x_i p^i + x_{i+1}p^{i+1} + \cdots + x_{e-1}p^{e-1}\right)}\right)^{p^{e-i-1}} = (a_i)^{p^{e-i-1}} \\ \Longrightarrow \quad & g^{\left(p^{e-i-1}(x_i p^i + x_{i+1}p^{i+1} + \cdots + x_{e-1}p^{e-1})\right)} = (a_i)^{p^{e-i-1}} \\ \Longrightarrow \quad & g^{\left(p^{e-1}\cdot p^{-i}(x_i p^i + x_{i+1}p^{i+1} + \cdots + x_{e-1}p^{e-1})\right)} = (a_i)^{p^{e-i-1}} \\ \Longrightarrow \quad & g^{\left(p^{e-1}\cdot(x_i + x_{i+1}p + \cdots + x_{e-1}p^{e-i-1})\right)} = (a_i)^{p^{e-i-1}} \\ \Longrightarrow \quad & g^{\left(p^{e-1}\cdot x_i\right)} \cdot g^{\left(p^{e-1}\cdot p(x_{i+1} + \cdots + x_{e-1}p^{e-i-2})\right)} = (a_i)^{p^{e-i-1}} \\ \Longrightarrow \quad & g^{\left(p^{e-1}\cdot x_i\right)} \cdot g^{p^e\cdot(x_{i+1} + \cdots + x_{e-1}p^{e-i-2})} = (a_i)^{p^{e-i-1}} \\ \Longrightarrow \quad & g^{\left(p^{e-1}\cdot x_i\right)} = (a_i)^{p^{e-i-1}} \quad \text{since} \ \ g^{p^e} = 1 \end{aligned}$$

Let $g^{p^{e-1}} = \bar{g}$
Then

$$(\bar{g})^{x_i} \ = \ (a_i)^{p^{e-i-1}} \quad \text{in some group } K \ = <\bar{g} \mid \bar{g}^p \ = \ 1>.$$

$$\Longrightarrow \ x_i \ = \ dlog_{\bar{g}}(a_i)^{p^{e-i-1}} \ \ \forall i$$

Examples :

1. Determine, if exists, $dlog_5 3$ in $\mathbb{Z}_{53}^*$.
   Let $x = dlog_5 3$, then $5^x = 3 \pmod{53}$

   Note that $G =< 5 |\ 5^{52} = 1 >$, thus $\gamma = 5$ and $\alpha = 3$

   Also, note that $O(\mathbb{Z}_{53}^*) = 52 = 2^2 \cdot 13$

   Let $p_1 = 2,\ p_2 = 13,\ e(2) = 2,\ e(13) = 1$

   Then, $n_2 = 13,\ n_{13} = 4$

   Let $\gamma_2 = \gamma^{n_2} = 5^{13} = 23 \pmod{53}$

   Let $H_1 =< \gamma_2 |\ {\gamma_2}^4 = 1 > =< 23 |\ 23^4 = 1 >$

   Note that $O(H_1) = 4$

   Let $\alpha_2 = \alpha^{n_2} = \alpha^{13} = 3^{13} = 30 \pmod{53}$,

   then, ${\gamma_2}^x = \alpha_2 \quad \Rightarrow \quad 23^x = 30 \pmod{53}$.

   We need to compute $x(2) = dlog_{\gamma_2} \alpha_2 = dlog_{23} 30$,

   such that $23^{x(2)} = 30$ and $x \equiv x(2) \pmod 4$).

   Since, here, ${p_1}^{e(2)} = 4$, a small integer, we can either compute $x(2)$ directly or we can reduce the prime power group to a cyclic group of order 2.

   One Possible way is we compute $x(2)$ as:

$$23^2 \equiv -1 \pmod{53}$$

$$23^3 \equiv 30 \pmod{53}$$

   thus, $x \equiv 3\ (mod\ 4)$
   Similarly, Let $\gamma_{13} = \gamma^4 = 5^4 = 42 \pmod{53}$

   Let $H_2 =< \gamma_{13} |\ {\gamma_{13}}^{13} = 1 > =< 42 |\ 42^{13} = 1 >$

   Note that $O(H_2) = 13$, which is prime, thus we don not require to reduce it further.

   Let $\alpha_{13} = \alpha^{n_{13}} = \alpha^4 = 3^4 = 28 \pmod{53}$,

   then, ${\gamma_{13}}^x = \alpha_{13} \quad \Rightarrow \quad 42^x = 28 \pmod{53}$.

   We need to compute $x(13) = dlog_{\gamma_{13}} \alpha_{13} = dlog_{42} 28$,

   such that $42^{x(13)} = 28$ and $x \equiv x(13) \pmod{13}$.

Solving $42^{x(13)} = 28$ in H_2, we get that $x(13) \equiv 7 \pmod{13}$, hence $x \equiv 7 \pmod{13}$.

Now we have two equations as :

$$x \equiv 3 \pmod{4}$$

$$x \equiv 7 \pmod{13}$$

Use Chinese remainder theorem to solve these two equation.
On solving, we get that

$$x \equiv 7 \pmod{52}$$

Thus, $dlog_5 3 = 7$ in $\mathbb{Z}^*_{53}$.

2. Determine, if exists, $dlog_6 7531$ in $\mathbb{Z}^*_{8101}$.

Let $x = dlog_6 7531$, then $6^x = 7531 \ (mod\ 8101)$

Note that $G =< 6 |\ 6^{8100} = 1 >$, thus $\gamma = 6$ and $\alpha = 7531$

Also, note that $|\mathbb{Z}^*_{8101}| = 8100 = 2^2 \cdot 3^4 \cdot 5^2$

Let $p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ e(2) = 2,\ e(3) = 4,\ e(5) = 2$

Then, $n_2 = 2025,\ n_3 = 100,\ n_5 = 324$

Let $\gamma_2 = \gamma^{2025} = 6^{2025}$

Let $H_1 =< \gamma_2 |\ {\gamma_2}^4 = 1 > =< 6^{2025} |\ (6^{2025})^4 = 1 >$

Note that $O(H_1) = 4$

Let $\alpha_2 = \alpha^{n_2} = \alpha^{2025} = 7531^{2025}$,

then, ${\gamma_2}^x = \alpha_2 \quad \Rightarrow \quad (6^{2025})^x = 7531^{2025}$.

We need to compute $x(2) = dlog_{\gamma_2} \alpha_2$,

such that $(6^{2025})^{x(2)} = 7531^{2025}$ and $x \equiv x(2) \ (mod\ 4)$.

Note that computation of 6^{2025} and 7531^{2025} is not easy and hence we reduce the problem to prime order group.

Since, $x(2)$ is in modulo 4, thus $x(2) = x_0 + x_1 * p$, where x_0 and x_1

is either 0 or 1.

Then

$$(\gamma_p{}^{p^{e-1}})^{x_0} \;=\; \alpha_p{}^{p^{e-1}} \;\in\; H_1$$

$$\Longrightarrow$$

$$(\gamma_2{}^2)^{x_0} \;=\; \alpha_2{}^2 \;\in\; H_1$$

$$\Longrightarrow$$

$$((6^{2025})^2)^{x_0} \;=\; (7531^{2025})^2 \;\in\; H_1$$

$$\Longrightarrow$$

$$(6^{4050})^{x_0} \;=\; 7531^{4050} \;\equiv\; -1 \;(mod\ 8101)$$

$$\Longrightarrow$$

$$(-1)^{x_0} \;\equiv\; -1 \;(mod\ 8101)$$

$$\Longrightarrow$$

$$x_0 \;=\; 1$$

Thus we need to compute x_1 now.
Note that $x_1 \;=\; dlog_{g^{p^{e-1}}} a_1{}^{p^{e-1-1}}$, where $a_1 \;=\; g^{-x_0}.\alpha_p$ and $g \;=\; \gamma_p \;=\; 6^{2025}$,

$$\Longrightarrow\; a_1 \;=\; g^{-x_0}.\alpha_2 \;=\; (6^{2025})^{(-1)}.7531^{2025}$$

$$\Longrightarrow$$

$$x_1 \;=\; dlog_{(6^{2025})^2} a_1{}^{2^{(2-1-1)}}$$

$$\Longrightarrow$$

$$x_1 \;=\; dlog_{(6^{2025})^2}.a_1$$

$$\Longrightarrow$$

$$(6^{2025})^{(-1)}.7531^{2025} \;=\; ((6^{2025})^2)^{x_1}$$

$$\Longrightarrow$$

$$(6^{-1})^{(2025)}.7531^{2025} \;=\; (-1)^{x_1}$$

Since, $6^{-1} \;\equiv\; 6751 \;(mod\ 8081)$, we have

$$(6751)^{2025}.7531^{2025} \;=\; (-1)^{x_1}$$

$$\Longrightarrow$$

$$(6751 * 7531)^{2025} \;=\; (-1)^{x_1}$$

$\Longrightarrow$

$$8006^{2025} \ = \ (-1)^{x_1}$$

Note that

$$8006^{2025} \ \equiv \ 1 \ (mod \ 4) \quad \Rightarrow \quad x_1 \ = \ 0$$

Thus

$$x(2) \ = \ x_0 + x_1 * 2 \ = \ 1$$

and the congruence relation is

$$x \ \equiv \ 1 \ (mod \ 4)$$

Similarly, Let $\gamma_3 \ = \ \gamma^{100} = \ 6^{100}$

Let $H_2 \ =< \gamma_3 | \ {\gamma_3}^{81} \ = \ 1 > =< 6^{100} | \ (6^{100})^{81} \ = \ 1 >$

Note that $O(H_2) \ = \ 8$

Let $\alpha_3 \ = \ \alpha^{n_3} \ = \alpha^{100} \ = \ 7531^{100}$,

then, ${\gamma_3}^x \ = \ \alpha_3 \quad \Rightarrow \quad (6^{100})^x \ = \ 7531^{100}$.

We need to compute $x(3) \ = \ dlog_{\gamma_3} \alpha_3$,

such that $(6^{100})^{x(3)} \ = \ 7531^{100}$ and $x \ \equiv \ x(3) \ (mod \ 81)$.

Note that computation of 6^{100} and 7531^{100} is not easy and hence we reduce the problem to prime order group.

Since, $x(3)$ is in modulo 81, thus $x(3) \ = \ x_0 + x_1 * p + x_2 * p^2 + x_3 * p^3$, where $x_0, \ x_1, \ x_2$, and x_3 is either 0 or 1 or 2.

Then

$$({\gamma_p}^{p^{e-1}})^{x_0} \ = \ {\alpha_p}^{p^{e-1}} \quad \in \quad H_2$$

$\Longrightarrow$

$$({\gamma_3}^{3^3})^{x_0} \ = \ {\alpha_3}^{3^3} \quad \in \quad H_2$$

$\Longrightarrow$

$$((6^{100})^{27})^{x_0} \ = \ (7531^{100})^{27} \quad \in \quad H_2$$

$\Longrightarrow$

$$(6^{2700})^{x_0} \ = \ 7531^{2700} \ \equiv \ 2217 \ (mod \ 8101)$$

$\Longrightarrow$

$$(5883)^{x_0} \ \equiv \ 2217 \ (mod \ 8101)$$

Since, $x_0 canbe 0, 1, 2$ only, thus after putting x_0 as $0, 1, 2$ in the above relation, we get

$$x_0 \;=\; 2$$

Thus we need to compute x_1 now.

Note that $x_1 \;=\; dlog_{g^{p^{e-1}}} {a_1}^{p^{e-1-1}}$, where $a_1 \;=\; g^{-x_0}.\alpha_p$ and $g \;=\; \gamma_p \;=\; 6^{100}$,

$\Longrightarrow \;\; a_1 \;=\; g^{-x_0}.\alpha_3 \;=\; (6^{100})^{(-2)}.7531^{100}$

$\Longrightarrow$

$$x_1 \;=\; dlog_{(6^{100})^{27}} {a_1}^{3^{(4-1-1)}}$$

$\Longrightarrow$

$$x_1 \;=\; dlog_{(6^{2700})} .{a_1}^9$$

$\Longrightarrow$

$$(6^{2700})^{x_1} \;=\; ((6^{100})^{(-2)}.7531^{100})^9$$

$\Longrightarrow$

$$(6^{2700})^{x_1} \;=\; (7531 \cdot 6^{-2})^{900}$$

Since, $6^{-2} \;\equiv\; 7876 \pmod{8081}$, we have

$$(6^{2700})^{x_1} \;=\; (7531 \cdot 7876)^{900}$$

$\Longrightarrow$

$$(6^{2700})^{x_1} \;=\; (6735)^{900}$$

$\Longrightarrow$

$$5883^{x_1} \;=\; 6735^{900} \;=\; 1$$

Note that

$$6735^{900} \;\equiv\; 1 \pmod{81} \quad \Rightarrow \quad x_1 \;=\; 0$$

Thus

$$x(2) \;=\; 2 + 0 \cdot 3 + x_2 \cdot 9 + x_3 \cdot 27$$

Similarly solve for x_2 and x_3.

On, solving, we get that $x_2 \;=\; 2$ and $x_3 \;=\; 1, \;\Longrightarrow$

$$x(2) \;=\; 2 + 0 \cdot 3 + 2 \cdot 9 + 1 \cdot 27 \;=\; 47$$

and the congruence relation is

$$x \equiv 47 \pmod{81}$$

Similarly solve for prime $p = 5$, and the congruence relation obtained will be

$$x \equiv 14 \pmod{25}$$

Thus, the problem now reduces to :

$$x \equiv 1 \pmod{4}$$
$$x \equiv 47 \pmod{81}$$
$$x \equiv 14 \pmod{25}$$

Use Chinese remainder theorem to compute the value of x.

3. Determine, if exists, $dlog_5 15$ in $\mathbb{Z}_{37}^*$. [Try it yourself]

Leture-13

Introduction to Finite Field

Some Definitions and Results

Group : A non empty set G is said to be a group if $\exists \ \ * : G \times G \to G$ defined as $(x, y) \to x * y \quad \forall \ \ x, y \in G$ such that :

1. Closure : $\forall \ \ x, y \in G, x * y \in G$
2. Associative : $(x * y) * z = x * (y * z) \quad \forall \ \ x, y, z \in G$
3. Existence of identity : $\exists\, e \in G$ such that $e * x = x * e = x$ (the element $e \in G$ is unique)
4. Existence of inverse : for $x \in G$, $\exists\ y \in G$ such that $x * y = y * x = e$ (the element $y \in G$ is unique)

It is denoted by $(G, *)$.

Commutative or abelian Group : A group $(G, *)$ is said to be commutative or abelian if $*$ is commutative over G, i.e. $x * y = y * x \quad \forall \ \ x, y, \in G$.

Cyclic Group : A group $(G, *)$ is said to be a cyclic group if there exist an element $x \in \ G$ such that every element $y \in G$ can be written as power of x.

Note : Every cyclic group is abelian but converse need not be true.
Proof : Let G be a cyclic group with a generator $g \in G$ i.e. $G = \langle g \rangle$ (every element in G is some power of g.) Let a and b be arbitrary elements in G. Then there exists $n, m \in \mathbb{Z}$ such that $a = g^n$ and $b = g^m$. It follows that $ab = g^n g^m = g^{n+m} = g^m g^n = ba$. Hence we obtain $ab = ba$ for arbitrary $a, b \in G$. Thus G is an abelian group.
Converse need not be true.

Let $G = \{e, a, b, ab\}$ such that $order\ of\ e = 1,$, $order\ of\ a = order\ of\ b = order\ of\ ab = 2$ and $ab = ba$, thus G is abelian. But G is not a cyclic.

Ring : A non empty set $(R, +, \cdot)$ is said to be a ring if :

1. $(R, +)$ is an abelian group.
2. R is closed w.r.t. multiplication, i.e. $\forall r, s \in R,\ r \cdot s = s \cdot r \in R$
3. The multiplication distributes over addition, i.e. $x(y + z) = xy + xz$ and $(x + y)z = xz + yz \quad \forall x, y, z \in R$

Note : We write $x \cdot y$ as xy.

Associative ring : A ring R is said to be an associative ring if multiplication is associative over R, i.e. $(xy)z = x(yz) \in R \qquad \forall\ x, y, z \in R$

Commutative ring : A ring R is s.t.b. a commutative or abelian ring if it is abelian w.r.t. multiplication over R, i.e. $x \cdot y = y \cdot x \quad \forall\ x, y \in R$

Ring with unity : A ring R is said to be a ring with unity if $\exists\ 1 \in R$ such that $x \cdot 1 = 1 \cdot x = x \quad \forall\ x \in R$. 1 is called multiplicative unity or (simply) unity of R.

Unit of ring : An element $x \in R$ is said to be a unit or an invertible element if there exists $y \in R$ such that $xy = yx = 1$ in a ring with unity 1. Such an element y is called multiplicative inverse or (simply) inverse of x and denoted by x^{-1}.

Ideal: For an arbitrary ring $(R, +, \cdot)$, a subset I is called a left ideal of R if:

1. $(I, +)$ is a subgroup of $(R, +)$
2. $\forall r \in R, \forall x \in I$, the product $rx \in I$

Similarly, we define right ideal. A two-sided ideal is a left ideal that is also a right ideal, and is sometimes simply called an ideal.

Maximal Ideal : A maximal ideal is an ideal that is maximal (with respect to set inclusion) amongst all proper ideals. In other words, I is a maximal ideal of a ring R if there are no other ideals contained between I and R, i.e.

For any ideal J with $I \subseteq J \subseteq R$, either $J = I$ or $J = R$.

Principal Ideal : A principal ideal is an ideal I in a ring R that is generated by a single element a of R through multiplication by every element of R i.e. $I = \{ar : r \in R\}$

Field : A non empty set $(\mathbb{F}, +, \cdot)$ is said to be a field if $(\mathbb{F}, +)$ is an abelian group and $(\mathbb{F} \setminus \{0\}, \cdot)$ is also an abelian group and multiplication distributes over addition.

Division ring or Skew field : $(D, +, \cdot)$ is said to be a division ring or a skew field if $(D, +)$ is an abelian group and $(D \setminus \{0\}, \cdot)$ form a group and multiplication distributed over addition.
($(D \setminus \{0\}, \cdot)$ need not be commutative.)

Zero Divisor : In a ring R, elements, if they exists, $a, b \in R$ such that $a \neq 0$, $b \neq 0$ but $ab = 0$, then a, b are called zero divisors in R.
Example : 2,3,4 are zero divisors of ring $(\mathbb{Z}_6, +_6, \cdot_6)$, since $3 \cdot_6 4 = 12 = 0 \in \mathbb{Z}_6$.

Integral Domain (ID) : A commutative ring without zero divisors is called an integral domain.

Principal Ideal Domain : A principal ideal domain (PID) is an integral domain in which every ideal is principal, i.e., can be generated by a single element.
Results :

1. **A field has no zero divisors.**
   Proof: Let $x, y \in \mathbb{F}$ and $xy = 0$. We will show either $x = 0$ or $y = 0$.
   If $x \neq 0$ then x^{-1} exists and $x^{-1}xy = x^{-1} \cdot 0 \implies 1 \cdot y = 0 \implies y = 0$.
   If $y \neq 0$ then y^{-1} exists and $xyy^{-1} = 0 \cdot y^{-1} \implies x \cdot 1 = 0 \implies x = 0$
   .

2. **A finite Integral Domain is a field.**

   Proof: We shall show that every non zero element in finite integral domain R is unit. Let r be a non zero element in R. To show that r is a unit. Define a map $f : R \to R$ as $x \to rx$.
   Claim: f is injective map.

Suppose $f(x) = f(y) \implies rx = ry \implies rx - ry = 0 \implies r(x-y) = 0$ since R is integral domain $r \neq 0 \implies (x-y) = 0 \implies x = y$
Hence f is injective. Since R finite therefore f is sujective. $1 \in R$ and f is surjective, so there exist $s \in R$ such that $f(s) = 1$ i.e. $rs = 1$ implies that r in unit in R.

3. **If R is an infinte ID, then R can be embedded into a field.**

4. **Every finite Division ring is a field.**

Proof of above results : try yourself

Theorem: Let R be a commutative ring with unity. Then, an ideal M of R is maximal if and only if quotient ring R/M is a field.

Characteristics of Ring : Let R be a ring. The Characteristic of R denoted char(R) or ch(R) is the least non negative integer n such that $n.1 = 0$. If no such n exists then we define the char(R)= 0.

Example : Consider the fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. It is easy to see that the characteristic of each of these fields is 0, for clearly $n.1 = n = 0$ if and only if $n = 0$.

Theorem: Let $\mathbb{F}$ be a field. Then char($\mathbb{F}$)= p for some prime p or char($\mathbb{F}$)= 0.
proof: If char($\mathbb{F}$)= 0, then we are done.
Otherwise, suppose that char($\mathbb{F}$)= n for some $n \in \mathbb{N}$, then $n.1 = 0$. Suppose that n is a composite number, say $n = rs$, then

$$rs.1 = 0$$

$$(r.1)(s.1) = 0$$

Since $\mathbb{F}$ is a field, $\mathbb{F}$ has no zero divisors. So $r.1 = 0$ or $s.1 = 0$. But this contradicts n being the least such non negative integer with this property. So $n = p$ for some prime p.

Euclidean Ring : An Integral Domain R is called an Euclidean Domain if $\forall\ 0 \neq a \in\ R,\ \ \exists$ a function $d : R \setminus \{0\} \to \mathbb{Z}^+ \cup \{0\}$ such that

1. $d(a) \leq d(ab)\ \ \forall\ a, b \in\ R\ \ (b \neq 0)$
2. $a = qb + r\ \ \forall\ a, b \in\ R\ \ (b \neq 0)$ and for some $q \in\ R$ and $r \in\ R$ such that $r = 0$ or $d(r) < d(b)$

Moreover, for $\forall a, b \in\ R,\ \ \exists\ \ gcd(a, b) = d \in\ R$ such that $d = \alpha a + \beta b$ for some $\alpha, \beta \in\ R$ and d is unique upto units.

Polynomial Ring : It is denoted by $\mathbb{F}[x]$ and defined as

$$\mathbb{F}[x] = \{f(x) = a_0 + a_1 x + ... + a_n x^n | a_0, a_1, ...a_n \in\ \mathbb{F}\}$$

Note : $a_0, a_1, ...a_n \in\ \mathbb{F}$ are called coefficients of polynomial $f(x) = a_0 + a_1 x + ... + a_n x^n$

Result : If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a Euclidean Ring.

Content of a polynomial : The content of a polynomial with integer coefficients is the greatest common divisor of its coefficients.
The primitive part of a polynomial with integer coefficient is the quotient of the polynomial by its content. Thus a polynomial is the product of its primitive part and its content.

Factorization of polynomials

Irreducible polynomial: Let D be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be irreducible over D if, whenever $f(x)$ is expressed, as a product $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$.

Reducible Polynomial: A nonzero, nonunit element of $D[x]$ that is not irreducible over D is called reducible over D.

Note: In the case that an integral domain is a field $\mathbb{F}$, it is equivalent and more convenient to define a nonconstant $f(x) \in \mathbb{F}[x]$ to be irreducible if $f(x)$ cannot be expressed as a product of two polynomials of lower degree.

Examples

1. The polynomial $f(x) = 2x^2 + 4$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{Z}$, since $2x^2 + 4 = 2(x^2 + 2)$ and neither 2 nor $x^2 + 2$ is a unit in $\mathbb{Z}[x]$.
2. The polynomial $f(x) = 2x^2 + 4$ is irreducible over $\mathbb{R}$ but reducible over $\mathbb{C}$.
3. The polynomial $f(x) = x^2 - 2$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$.
4. The polynomial $f(x) = x^2 + 1$ is irreducible over $\mathbb{Z}_3$ but reducible over $\mathbb{Z}_5$

Reducibility Test for Degree 2 and 3
Let $\mathbb{F}$ be a field. If $f(x) \in \mathbb{F}[x]$ and $deg f(x)$ is 2 or 3, then $f(x)$ is reducible over $\mathbb{F}$ if and only if $f(x)$ has a zero in F.

Theorem: Reducibility over Q Implies Reducibility Over Z
Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

Note :

- Converse of above theorem need not true .(See example 1).
- Condition $f(x) \in \mathbb{Z}[x]$ in above theorem is important.

Irreducibility Tests

Theorem: Mod p Irreducibility Test
Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $deg f(x) \geq 1$. Let $\overline{f(x)}$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $\overline{f(x)}$ is irreducible over $\mathbb{Z}_p$ and $deg\overline{f(x)} = deg f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Example : Let $f(x) = 21x^3 - 3x^2 + 2x + 9$. Then, over $\mathbb{Z}_2$,we have $\overline{f(x)} = x^3 + x^2 + 1$ and, since $\overline{f(0)} = 1$ and $\overline{f(1)} = 1$, we see that $f(x)$ is irreducible over $\mathbb{Z}_2$. Thus $f(x)$ is irreducible over $\mathbb{Q}$. Notice that over $\mathbb{Z}_3$, $\overline{f(x)} = 2x$ is irreducible, but we can not apply above theorem to conclude that $f(x)$ is irreducible over $\mathbb{Q}$ since $deg\overline{f(x)} \neq degf(x)$.

Note : Be careful not to use the converse of Theorem (Mod p Irreducibility Test). If $f(x) \in \mathbb{Z}[x]$ and $\overline{f(x)}$ is reducible over $\mathbb{Z}_p$ for some p, $f(x)$ need not be irreducible over $\mathbb{Q}$.

For example, consider $f(x) = 21x^3 - 3x^2 + 2x + 8$. Then, over $\mathbb{Z}_2$, $\overline{f(x)} = x^3 + x^2 = x^2(x + 1)$. But over $\mathbb{Z}_5$, has no zeros and therefore is irreducible over $\mathbb{Z}_5$. So, $f(x)$ is irreducible over $\mathbb{Q}$.

Note that this example shows that the Mod p Irreducibility Test may fail for some p and work for others. To conclude that a particular $f(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$, all we need to do is find a single p for which the corresponding polynomial in $\overline{f(x)} \in \mathbb{Z}_p$ is irreducible. However, this is not always possible, since $f(x) = x^4 + 1$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{Z}_p$ for every prime p.
The Mod p Irreducibility Test can also be helpful in checking for irreducibility of polynomials of degree greater than 3 and polynomials with rational coefficients.

Theorem: Eisenstein's Irreducibility Criterion :
Let $f(x) = a_n x^n + ... + a_1 x + a_0$ be a polynomial with integer coefficients. Suppose that there exists a prime p, such that

- $p \nmid a_n$
- $p \mid a_{n-1}, a_{n-2}, ..., a_1, a_0$
- $p^2 \nmid a_0$

Then $f(x)$ is irreducible over the integers.

Note : If $f(x) \in \mathbb{Z}[x]$, and it satisfies all 3 conditions, then $f(x)$ is irreducible over the $\mathbb{Q}$ and hence over $\mathbb{Z}$. But in general $f(x)$ need not be in $\mathbb{Z}[x]$.

Corollary: (Irreducibility of *pth* Cyclotomic Polynomial)
For any prime p, the *pth* cyclotomic polynomial

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + ... + x + 1$$

is irreducible over $\mathbb{Q}$.

Theorem Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$. Then $\langle f(x) \rangle$ is maximal in $\mathbb{F}[x]$ if and only if $f(x)$ is irreducible over $\mathbb{F}$.

Theorem: Let $\mathbb{F}$ be a field and let $f(x)$ be an irreducible polynomial over $\mathbb{F}$. Then $\frac{\mathbb{F}[x]}{\langle f(x) \rangle}$ is a field.

Leture-14

Introduction to Finite Field

Finite field

Theorem: If $\mathbb{F}$ is a finite field, then $\mid \mathbb{F} \mid = q = p^n$ for some prime p and some positive integer n.

Theorem: For every prime p and every positive integer n, there exist a field having p^n elements.

Theorem: If $\mathbb{F}$ is a finite field, then $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ is a cyclic group with respect to multiplication.

Splitting field : Let K be a field and let $f(x) \in K[x]$ be a polynomial. The splitting field of f is the smallest field extension L of K so that f splits into linear factors in $L[x]$.

Result : Let K be a field and let $f(x) \in K[x]$ be a polynomial. The splitting field of f exists and is unique up to isomorphism.

Example :

- The splitting field of $f(x) = x + 1 \in \mathbb{F}_2[x]$ is $\mathbb{F}_2$ itself since f is linear.
- The splitting field of $g(x) = x^2 + x + 1$ is $\mathbb{F}_4$ – by constructing the class of x in $L = \mathbb{F}_2[x]/g\mathbb{F}_2[x]$ is a root of g. To see this consider $g(y) = y^2 + y + 1$ as polynomial in $L[y]$ and note that we compute modulo $x^2 + x + 1$ in L

  $$(y + x)(y + x + 1) = y^2 + (x + x + 1)y + x^2 + x = y^2 + y + 1 = g(y)$$

  .

- Put $h(x) = (x^3 + x + 1) \in \mathbb{F}_2[x]$. This polynomial is irreducible over $\mathbb{F}_2$ and it thus allows to define a field with 8 elements as $\mathbb{F}_8$ is isomorphic to $\mathbb{F}_2[x]/h\mathbb{F}_2[x]$. By the same considerations as above the splitting field of h is $\mathbb{F}_8$.

Result : Let $f(x) = (x^p)^n - x \in \mathbb{F}_p[x]$ for some integer n. The splitting field of f is a finite field K with $\mid K \mid = p^n$ elements and f splits as

$$(x^p)^n - x = \prod_{a \in K} (x - a)$$

Theorem: Existence and uniqueness of finite fields
For any prime p and any natural number n there exists a finite field with p^n elements. Every field with p^n elements is isomorphic to the splitting field of $f(x) = (x^p)^n - x$ over $\mathbb{F}_p$.

Construction of a finite field

Points to remember :

1. We write $\mathbb{Z}/\langle p \rangle$ and $\mathbb{F}_p$ interchangeably for the field of size p.
2. Every finite field has prime power order.
3. For every prime power, there is a finite field of that order.
4. For a prime p and positive integer n, there is an irreducible $f(x)$ of degree n in $\mathbb{F}_p[x]$, and $\frac{\mathbb{F}_p[x]}{\langle f(x) \rangle}$ is a field of order p^n.
5. Any two finite fields of the same size are isomorphic.

Theorem: For a prime p and a monic irreducible $f(x) \in \mathbb{F}_p[x]$ of degree n, the ring $\mathbb{F}_p[x]/\langle f(x) \rangle$ is a field of order p^n.

Construction

We will explain the construction by an example.
$\mathbb{Z}_2[x]$ is a commutative ring with identity 1. Since for every field $\mathbb{F}$, the polynomial ring $\mathbb{F}[x]$ is a PID (also UFD -unique factorization domain) and every ideal is of the form $\langle f(x) \rangle$ and $\langle f(x) \rangle$ is maximal in $\mathbb{F}[x]$ if and only if $\langle f(x) \rangle$

is irreducible over $\mathbb{F}$.
Therefore $\mathbb{Z}_2[x]/\langle f(x)\rangle$ is a field, if $f(x)$ is irreducible over $\mathbb{Z}_2$.
If degree of $f(x)$ is n then $\mathbb{Z}_2[x]/\langle f(x)\rangle$ has finitely many elements and

$$\left|\frac{\mathbb{Z}_2[x]}{\langle f(x)\rangle}\right| = p^n = 2^n$$

If

$$f(x) = a_0 + a_1x + a_{n-1}x^{n-1} + a_nx^n, \quad a_n \neq 0$$

then

$$\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle} = \{g(x) + \langle f(x)\rangle : \ g(x) \in \mathbb{Z}_p[x]\}$$

implies

$$\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle} = \{f(x)q(x)+r(x)+\langle f(x)\rangle : \ q(x), r(x) \in \mathbb{Z}_p[x], \ \ r(x) = 0 \, or \, deg\, r(x) < deg\, f(x)\}$$

(by Euclidean Algorithm)
implies

$$\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle} = \{r(x)+\langle f(x)\rangle : \ r(x) \in \mathbb{Z}_p[x], \ \ r(x) = 0 \, or \, deg\, r(x) < deg\, f(x) = n\}$$

implies

$$\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle} = \{\alpha_0 + \alpha_1x + ... + \alpha_{n-1}x^{n-1} + \langle f(x)\rangle : \ \alpha_i \in \mathbb{Z}_p\}$$

$$\sim \{(\alpha_0, \alpha_1, ...\alpha_{n-1}) : \ \alpha_i \in \mathbb{Z}_p\}$$

Example 1 : $p = 2, n = 2$
The quadratic polynomial of degree 2 in $\mathbb{Z}_2[x]$ are :

$x^2 = x \cdot x$	**reducible**
$x^2 + 1 = (x + 1)(x + 1)$	**reducible**
$x^2 + x + 1$ **irreducible**	**verify!**
$x^2 + x = x(x + 1)$	**reducible**

Only one of these namely $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$
So,

$$\begin{aligned}\frac{\mathbb{Z}_2[x]}{\langle f(x)\rangle} &= \{\alpha_0 + \alpha_1 x + \langle x^2 + x + 1\rangle : \ \alpha_0, \alpha_1 \in \mathbb{Z}_2\} \\ &= \{0 + \langle x^2 + x + 1\rangle, 1 + \langle x^2 + x + 1\rangle, x + 1 + \langle x^2 + x + 1\rangle, x + \langle x^2 + x + 1\rangle\} \\ &\sim \{0, 1, x, x + 1\}\end{aligned}$$

Cayley's Table:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$.$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Note that $x^2 + x + 1 = 0 \implies x^2 = -x - 1 = x + 1 \mod 2$
Thus, it is closed with respect to addition and multiplication.
Verify that $\{0, 1, x, x + 1\}$ is a field of order 4 with above defined addition amd multiplication.

Example 2: Polynomials of degree 4 in $\mathbb{Z}_2$:

x^4	$x^4 + 1$	$x^4 + x$	$x^4 + x + 1$
$x^4 + x^3$	$x^4 + x^3 + x^2$	$x^4 + x^3 + x$	$x^4 + x^3 + 1$
$x^4 + x^2 + x + 1$	$x^4 + x^3 + x^2 + x$	$x^4 + x^3 + x^2 + x + 1$	$x^4 + x^2 + 1$
$x^4 + x^2 + x$	$x^4 + x^2$	$x^4 + x^3 + x + 1$	$x^4 + x^3 + x + 1$

1.	x^4	**reducible since x is a factor**
2.	x^4+1	**reducible since $x+1$ is a factor**
3.	x^4+x	**reducible since x is a factor**
4.	x^4+x+1	-
5.	x^4+x^3	**reducible since x is a factor**
6.	$x^4+x^3+x^2$	**reducible since x is a factor**
7.	x^4+x^3+x	**reducible since x is a factor**
8.	x^4+x^3+1	-
9.	x^4+x^2+x+1	**reducible since $x+1$ is a factor**
10.	$x^4+x^3+x^2+x$	**reducible since x is a factor**
11.	$x^4+x^3+x^2+x+1$	-
12.	x^4+x^2+1	**reducible since x^2+x+1 is a factor**
13.	x^4+x^2+x	**reducible since x is a factor**
14.	x^4+x^2	**reducible since x is a factor**
15.	x^4+x^3+x+1	**reducible since $x+1$ is a factor**
16.	x^4+x^3+x+1	**reducible since $x+1$ is a factor**

Now we check the reducibility of remaining polynomial

$$f(x)=x^4+x+1,\ g(x)=x^4+x^3+1,\ h(x)=x^4+x^3+x^2+x+1$$

None of them is divisible by a polynomial of degree 1. So they can be reducible if and only if divisible by an irreducible polynomial of degree 2 in $\mathbb{Z}_2[x]$ i.e. $x^2,\ x^2+x,\ x^2+1,\ x^2+x+1$.

There is only one irreducible polynomial of degree 2 over $\mathbb{Z}_2$, namely $k(x) = x^2 + x + 1$.
By division, Observe that $k(x) \nmid f(x)$, $k(x) \nmid g(x)$ and $k(x) \nmid h(x)$.
Therefore $f(x),\ g(x)$ and $h(x)$ are the only irreducible polynomial of degree 4 over $\mathbb{Z}_2$ and quotient over $\mathbb{Z}_2$ will become field of order $2^4 = 16$.

$$\frac{\mathbb{Z}_2[x]}{\langle f(x)\rangle} \cong \frac{\mathbb{Z}_2[x]}{\langle g(x)\rangle} \cong \frac{\mathbb{Z}_2[x]}{\langle h(x)\rangle}$$

Example 3: Two finite fields of order 8 are $\frac{\mathbb{F}_2[x]}{\langle x^3+x+1\rangle}$ and $\frac{\mathbb{F}_2[x]}{\langle x^3+x^2+1\rangle}$.

Example 4: Two finite fields of order 9 are $\frac{\mathbb{F}_3[x]}{\langle x^2+1\rangle}$ and $\frac{\mathbb{F}_3[x]}{\langle x^2+x+2\rangle}$.

Example 5: The polynomial $x^3 - 2$ is irreducible in $\mathbb{F}_7[x]$, so $\frac{\mathbb{F}_7[x]}{\langle x^3-2\rangle}$ is a field of order $7^3 = 343$.

Primitive Polynomial

If $\mathbb{F}$ is a finite field, then $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ is a cyclic group with respect to multiplication. Let $q = p^n$, then $\mathbb{F}_q^*$ is cyclic and thus, $\exists\ \alpha \in\ \mathbb{F}_q^*$ such that

$$\mathbb{F}_q^* = \langle\alpha\rangle = \langle\alpha^i :\ 0 \le i \le q-1\rangle$$

and $|\alpha| = q - 1$ with respect to multiplication.
Thus α is a primitive root of unity in $\mathbb{F}_q^*$.

Corollary : Every finite field contains at least one primitive element. More precisely there are exactly $\phi(q-1)$ primitive elements.

Primitive Polynomial : A polynomial $f(x)$ such that α is a root of $f(x)$ and α is a primitive element of $\mathbb{F}_q$ is called a primitive polynomial.

Example : From above example we have $\frac{\mathbb{Z}_2[x]}{\langle x^4+x^3+x^2+x+1\rangle}$ is a field of order 2^4 as $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$.

If α is a root of $f(x)$, then $f(\alpha) = 0$, implies,

$$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$$

multiplying both daides by $\alpha - 1$, we have

$$\alpha^5 - 1 = 0$$

implies

$$\alpha^5 = 1$$

Hence $|\alpha| = 5 \neq 15 = |\mathbb{Z}_{2^4}^*|$
So α cannot be primitive element and so $f(x)$ is not a primitive polynomial though $f(x)$ is irreducible over $\mathbb{Z}_2$.

Result : If $\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}$ and $\frac{\mathbb{Z}_p[x]}{\angle g(x)\rangle}$ are fields of order p^n, then they are isomorphic. But if $g(x)$ is a primitive polynomial, then $f(x)$ need not be primitive polynomial.

In above example $f(x)$ is not a primitive polynomial but $g(x) = x^4 + x + 1$ is a primitive polynomial.
$g(x)$ **is irreducible over** $\mathbb{Z}_2$**.**
If α is a root of $g(x)$, then $g(\alpha) = 0$, implies,

$$\alpha^4 + \alpha + 1 = 0 \implies \alpha^4 = \alpha + 1 \ (\ as\ 1 \equiv -1\ (mod\ 2))$$

The set
$\{\alpha^i :\ 0 \leq i \leq q - 1\}$

$= \{\alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4 = \alpha{+}1,\ \alpha^5 = \alpha^2{+}\alpha,\ \alpha^6 = \alpha^3{+}\alpha^2,\ \alpha^7 = \alpha^3{+}\alpha{+}1,\ \alpha^8 = \alpha^2{+}1,\ \alpha^9 = \alpha^3{+}\alpha^1,$

$\alpha^{10} = \alpha^2{+}\alpha{+}1,\ \alpha^{11} = \alpha^3{+}\alpha^2{+}\alpha,\ \alpha^{12} = \alpha^3{+}\alpha^2{+}\alpha{+}1,\ \alpha^{13} = \alpha^3{+}\alpha^2{+}1,\ \alpha^{14} = \alpha^3{+}1,\ \alpha^{15} = 1\}$

Hence α **is a primitive root of** $g(x)$**.**

Result : A polynomial $g(x) \in \mathbb{Z}_p[x]$ of degree k is said to be a primitive polynomial of degree k if $g(x) \mid x^m - 1$, $m = p^k - 1$ and for no smaller values of m.

Verify : $g(x) = x^4 + x + 1$ is a primitive ploynomial of degree 4 in $\mathbb{Z}_2[x]$ using above rsgult.

Example of Application of Primitive Polynomial
Whenever we need cyclic group with generator, we can take multiplicative group of finite field with primitive element. For example:

Recall the El-Gamal Cryptosystem, all users agree on a finite cyclic group, say $\mathbb{F}_q^* = \langle \alpha : \ \alpha^{q-1} = 1 \rangle$ where $\mathbb{F}_q = \mathbb{F}_q^* \cup \{0\}$ is a finite field of order $q = p^n$ for some prime p and some positive integer n.

Every user, say Alice, Bob,..., will choose and keep secret positive integer $a, b, ...$ and make public $\alpha^a, \alpha^b, ...$ respectively.

To send a message $M \in \ \mathbb{F}_q^*$, to Alice, we create a mask by choosing a random integer k and doing α^{ak} and hide the message $M(\alpha^a)^k \in \ \mathbb{F}_q^*$.

Now send Alice the ordered pair : $(\alpha^k, M(\alpha^a)^k) \ \in \ \mathbb{F}_q^* \times \mathbb{F}_q^*$

So, She retrives the message by doing $M(\alpha^a)^k \cdot [(\alpha^k)^a]^{-1} \ = \ M \ \in \ \mathbb{F}_q^*$

Exercise : Find a primitive polynomial of degree 6 and 7 over $\mathbb{Z}_2$.

Cryptography Over Finite Field

Let $\mathbb{F}_q$ be a finite field. Then order $|\mathbb{F}_q| = q = p^n$ for some prime p and some positive integer n.
We know that $G = \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is cyclic group with respect to multiplication of order $q - 1$. So

$$\mathbb{F}_q^* = \langle \alpha : \ \alpha^{q-1} \equiv 1(\mod p) \rangle$$

and $\mathbb{F}_q = \mathbb{F}_q^* \cup \{0\}$
Hence all the cryptographic applications done on finite cyclic groups are applicable on $G = \mathbb{F}_q$. For example

1. Diffie-Hellman Key Exchange Protocol

2. Massy-Omura Cryptosystem

3. ElGamal Cryptosystem

4. Discrete Logarithm Problem and Algorithm to calculate the Discrete Logarithm

Question: Decrypt the following ElGamal cipher text

(H,K) (X,P) (K,N) (R,H) (F,T) (Y,V) (H,E) (A,F) (W,T) (D,J) (J,U)

Take field $\frac{\mathbb{Z}_3[x]}{\langle x^3+2x^2+1\rangle}$

A	1	N	x^2+x+1
B	2	O	x^2+2x
C	x	P	x^2+2x+1
D	$x+1$	Q	x^2+2x+2
E	$x+2$	R	$2x^2$
F	$2x$	S	$2x^2+1$
G	$2x+1$	T	$2x^2+2$
H	$2x+2$	U	$2x^2+x$
I	x^2	V	$2x^2+x+1$
J	x^2+1	W	$2x^2+x+2$
K	x^2+2	X	$2x^2+2x$
L	x^2+x	Y	$2x^2+2x+1$
M	x^2+x+1	Z	$2x^2+2x+2$

The correspondence of the normal English alphabet letters with field elements

A	x^{26}	1
B	x^{13}	2
C	x	x
D	x^{18}	$x+1$
E	x^{11}	$x+2$
F	x^{14}	$2x$
G	x^{24}	$2x+1$
H	x^{5}	$2x+2$
I	x^{2}	x^2
J	x^{7}	x^2+1
K	x^{3}	x^2+2
L	x^{19}	x^2+x
M	x^{22}	x^2+x+1
N	x^{8}	x^2+x+1
O	x^{12}	x^2+2x
P	x^{10}	x^2+2x+1
Q	x^{4}	x^2+2x+2
R	x^{15}	$2x^2$
S	x^{16}	$2x^2+1$
T	x^{20}	$2x^2+2$
U	x^{25}	$2x^2+x$
V	x^{17}	$2x^2+x+1$
W	x^{23}	$2x^2+x+2$
X	x^{6}	$2x^2+2x$
Y	x^{21}	$2x^2+2x+1$
Z	x^{9}	$2x^2+2x+2$

Correspondence of the field elements to the normal text letters

C	x	F	x^{14}
I	x^2	R	x^{15}
K	x^3	S	x^{16}
Q	x^4	V	x^{17}
H	x^5	D	x^{18}
X	x^6	L	x^{19}
J	x^7	T	x^{20}
N	x^8	Y	x^{21}
Z	x^9	M	x^{22}
P	x^{10}	W	x^{23}
E	x^{11}	G	x^{24}
O	x^{12}	U	x^{25}
B	x^{13}	A	x^{26}

ElGamal Cipher text (H,K)= (x^5, x^3)
(X,P)=(x^6, x^{10})
(K,N)=(x^3, x^8)
(R,H)=(x^{15}, x^5)
(F,T)=(x^{14}, x^{20})
(Y,V)=(x^{21}, x^{17})
(H,E)=(x^5, x^{11})
(A,F)=(x^{26}, x^{14})
(W,T)=(x^{23}, x^3)
(D,J=(x^{18}, x^3)
(J,U)=(x^7, x^{25})

Recall: ElGamal Cryptosystem Let $G =< g|g^n = 1 >$ be public. All users, say Alice and Bob ... . They choose random integers a, b, ... respectively and keep it secret and make $g^a, g^b, \cdots \in G$ public.
Now, if Bob wants to send message $\mathcal{M}$ to Alice. He choose a random integer k and create a mask by doing $(g^a)^k \in G$. Bob then sends to Alice $(g^k, \mathcal{M}g^{ak}) \in G \times G$.
Alice will receive $(g^k, \mathcal{M}g^{ak}) \in G \times G$, to recover $\mathcal{M}$ from order pair $(g^k, \mathcal{M}g^{ak})$, Alice will recreate the mask by doing $(g^k)^a = g^{ka} = g^{ak} \in G$, as Alice know a (secret) and g^k is first element of order pair $(g^k, \mathcal{M}g^{ak})$ received from Bob. To recover the message, Alice will compute

$$(\mathcal{M}g^{ak})(g^{ak})^{-1} = \mathcal{M} \in G$$

Decryption: suppose secret $a = 11$, public encryption key $g^{11} = x^{11} = x + 2 = \text{E}$
The first cipher message unit (H,K) or (x^5, x^3)
The message lies masked in the first coordinate i.e. H or x^5
Recreate the mask from the second coordinate i.e. K or x^3 by doing $(x^3)^{11} = x^{33} = x^7$. Remove the mask from the first coordinate

$$x^5(x^7)^{-1} = x^5(x^{19}) = x^{24} \quad \text{Corresponds English alphabet G}$$

So the plain text corresponding to the first cipher (H,K) is G.
Similarly for others.

Leture-15

Introduction to Elliptic Curves

In 1985, Neal Koblitz and Victor S. Miller suggested independently the use of elliptic curves in cryptography. Elliptic curve cryptography algorithms entered wide use in 2004 to 2005. Elliptic curve cryptography is used in public key cryptosystems. The key size in Elliptic curve cryptosystems are much smaller in comparison to RSA to get the same level of security as in RSA. Elliptic curve cryptography is based on the algebraic structure of elliptic curves over finite fields. We shall study integer factorization, primality test and discrete logarithm problems with the help of elliptic curves. First, we shall discuss the basics of elliptic curves after that define an algebraic structure on the elliptic curves.

Elliptic Equation

The most general elliptic equation is the Weierstrass Equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

where the coefficient come from a ring or a field. Just for the time being consider the real Weierstrass equation, i.e. the coefficients a_i's are real numbers.

Conversion of Weierstrass Equation to a Normal Form:

With a suitable change of variables, Weierstrass equation i.e. (1) can be converted to a simpler form known as its normal form:

$$y^2 = x^3 + ax + b \tag{2}$$

for some real numbers a, b.
There are several methods to do this . We take the simplest way.
In equation(1), put

$$y = \frac{v - a_1x - a_3}{2}.$$

The LHS of equation becomes:

$$\begin{aligned} y^2 + a_1xy + a_3y &= y(y + a_1x + a_3) \\ &= \left(\frac{v - a_1x - a_3}{2}\right)\left(\frac{v - a_1x - a_3}{2} + a_1x + a_3\right) \\ &= \left(\frac{v - a_1x - a_3}{2}\right)\left(\frac{v + a_1x + a_3}{2}\right) \\ &= \frac{v^2 - (a_1x + a_3)^2}{4} \\ &= \frac{v^2 - (a_1^2x^2 + 2a_1a_3x + a_3^2)}{4} \end{aligned}$$

Hence equation(1) becomes:

$$\begin{aligned} &\frac{v^2 - (a_1^2x^2 + 2a_1a_3x + a_3^2)}{4} = x^3 + a_2x^2 + a_4x + a_6 \\ &v^2 = 4x^3 + 4a_2x^2 + 4a_4x + 4a_6 + a_1^2x^2 + 2a_1a_3x + a_3^2 \\ &v^2 = 4x^3 + (a_1^2 + 4a_2)x^2 + 2(a_1a_3 + 2a_4)x + (a_3^2 + 4a_6) \end{aligned} \tag{3}$$

In equation(3) put $x = \frac{X - 3(a_1^2 + 4a_2)}{36}$, then RHS of equation (3) becomes:

$$\begin{aligned} 4\left(\frac{X - 3(a_1^2 + 4a_2)}{36}\right)^3 &+ (a_1^2 + 4a_2)\left(\frac{X - 3(a_1^2 + 4a_2)}{36}\right)^2 \\ &+ 2(a_1a_3 + 2a_4)\left(\frac{X - 3(a_1^2 + 4a_2)}{36}\right) + (a_3^2 + 4a_6) \end{aligned}$$

And equation(3) becomes:

$$v^2 = \frac{4}{36^3}\{X - 3(a_1^2 + 4a_2)\}^3 + \frac{(a_1^2 + 4a_2)}{36^2}\{X - 3(a_1^2 + 4a_2)\}^2 + \frac{2}{36}(a_1a_3 + 2a_4)\{X - 3(a_1^2 + 4a_2)\} + ({a_3}^2 + 4a_6)$$

Now put $v = \frac{Y}{108}$, in this equation we get:

$$\left(\frac{Y}{108}\right)^2 = \frac{4}{36^3}\{X - 3(a_1^2 + 4a_2)\}^3 + \frac{(a_1^2 + 4a_2)}{36^2}\{X - 3(a_1^2 + 4a_2)\}^2 + \frac{2}{36}(a_1a_3 + 2a_4)\{X - 3(a_1^2 + 4a_2)\} + ({a_3}^2 + 4a_6)$$

Multiplying both sides by $(108)^2$, and $108 = 3 \times 36$; and

$$(108)^2.\frac{4}{(36)^3} = 4\frac{3^2.36^2}{36^3} = \frac{3^2.4}{36} = 1$$

$$\frac{108^2}{36^2} = \frac{3^2.36^2}{36} = 9$$

$$108^2.\ \frac{2}{36} = \frac{3^2\ .\ 36^2\ .\ 2}{36} = 3^2\ .\ 36\ .\ 2 = 3\ .\ 3\ .\ 2\ .36 = 6\ .\ 108$$

We get

$$Y^2 = \{X - 3(a_1^2 + 4a_2)\}^3 + 9(a_1^2 + 4a_2)\{X - 3(a_1^2 + 4a_2)\}^2 + 6\ .\ 108(a_1a_3 + 2a_4)\{X - 3(a_1^2 + 4a_2)\} + 108^2(a_3^2 + 4a_6)$$

On expanding each bracket term we get

$$\begin{aligned}Y^2 =&[\{X^3+3X^2\{-3(a_1^2+4a_2)\}+3X\{-3(a_1^2+4a_2)\}^2+\{-3(a_1^2+4a_2)\}^3]\\&+[9(a_1^2+4a_2)\{X^2-6(a_1^2+4a_2)X+9(a_1^2+4a_2)^2\}]\\&+[6.\ 108(a_1a_3+2a_4)X-18\ .108(a_1.\ a_3+2a_4)(a_1^2+4a_2)]\\&+[(108)^2(a_3^2+4a_6)]\end{aligned}$$

Writing the RHS as polynomial in X, the equation becomes:

$$\begin{aligned}Y^2 = X^3&+\{-9(a_1^2+4a_2)+9(a_1^2+4a_2)\}X^2\\&+\{27(a_1^2+4a_2)^2-54(a_1^2+4a_2)^2+6\ .\ 108\ (a_1a_3+2a_4)\}X\\&+\{-27(a_1^2+4a_2)^3+81(a_1^2+4a_2)^3-18\ .108(a_1a_3+2a_4)(a_1^2+4a_2)+108^2(a_3^2+4a_6)\}\end{aligned}$$

Or

$$\begin{aligned}Y^2 = X^3&+\{-27(a_1^2+4a_2)^2+6\ .108(a_1a_3+2a_4)\}X\\&+\{54(a_1^2+4a_2)^3-18\ .108(a_1a_3+2a_4)(a_1^2+4a_2)+108^2(a_3^2+4a_6)\}\end{aligned}$$

Or

$$Y^2 = X^3 + AX + B$$

Where $A = \{-27(a_1^2+4a_2)^2+6\ .108(a_1a_3+2a_4)\}$

$B = \{54(a_1^2+4a_2)^3-18\ .108(a_1a_3+2a_4)(a_1^2+4a_2)+108^2(a_3^2+4a_6)\}$

Note: In the process of transforming an elliptic curve to normal form we, have used division by 2 and 3. Hence if the coefficients are come from a field with, $Char(K) \neq 2, 3$, then the above equation is the normal form of Weierstrass equation over K. That is $y^2 = x^3 + ax + b$; $a, b \in K$, where $Char(K) \neq 2, 3$.

Normal Forms Of Weierstrass Equation Over Fields

Let K be a field of characteristic p. Then $p = 0$ or p is a prime.
Recall the Weierstrass equation in general form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Also recall that if $p \neq 2, 3$ then the equation can be transformed into simpler equation called normal form

$$Y^2 = X^3 + AX + B; \qquad A, B \in K$$

Similarly, the normal form in case $p = 2$,
either

$$Y^2 + XY = X^3 + AX^2 + B$$

or

$$Y^2 + CY = X^3 + AX + B; \qquad A, B, C \ \in \ K.$$

And in case $p = 3$, the normal form is

$$Y^2 = X^3 + AX^2 + BX + C \qquad A, B, C \ \in \ K.$$

This can be split into following two equivalent forms, $Y^2 = X^3 + CX^2 + D$ or $Y^2 = X^3 + AX + B, \quad A, B, C, D \in K$.

Real Elliptic Curves

The normal form of a real elliptic curve is

$$E = E_{\mathbb{R}} = \{(x, y) \ \in \ \mathbb{R} \times \mathbb{R} \ : \ y^2 = x^3 + ax + b, \ a, \ b \ \in \ \mathbb{R}\} \cup \{\infty\}.$$

Or

$$E = \{(x, y) \ \in \ \mathbb{R}\times\mathbb{R} \ : F(x, y) = 0 \ \textit{where} \ F(x, y) = y^2 - x^3 - ax - b, \ a, \ b \ \in \ \mathbb{R}\} \cup \{\infty\}.$$

The representation of E_K for a field of $Char(K) \neq 2, 3$, is same as above. However considering $K = \mathbb{R}$ have the advantage of knowledge of calculus and plane geometry. We shall move to other field as and when convenient. For the moment, let K be an algebraically closed field. Best is the field $\mathbb{C}$ of complex numbers.

Elliptic Curves

Let K be a field, and

$$E = E_K = \{(x, y) \in K \times K | y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\infty\},$$

or

$$E_K = \{(x, y) \in K \times K | F(x, y) = 0\} \cup \{\infty\},$$

where $F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$

Then E_k is said to be an elliptic curve over K. That is E consists of all points $(x, y) \in K \times K$, satisfying the Weierstrass equation (W.E.), together with the point at infinity denoted by ∞. We shall talk about the 'point of infinity' later on, where develop some basics of algebraic geometry. Till that let it be there. We shall set up some properties on E.

Singular and Non-Singular Curves

$$\begin{aligned} \text{Let } E = E_{\mathbb{R}} =& \{(x, y) \in \mathbb{R} \times \mathbb{R} | y^2 = x^3 + ax + b; a, b \in \mathbb{R}\} \cup \{\infty\} \\ =& \{(x, y) \in \mathbb{R} \times \mathbb{R} | 0 = F(x, y) = y^2 - x^3 - ax - b; a, b \in \mathbb{R}\} \cup \{\infty\} \end{aligned}$$

Then E can be traced by mapping a point $P(x, y) \in E$, with (x, y) as coordinates of P in $\mathbb{R}^2$ and ∞ as the point on the end of every ordinate.
Observe that E is symmetric, the graph $\{(x, y) \in \mathbb{R} \times \mathbb{R} | y^2 = x^3 + ax + b; a, b \in \mathbb{R}\}$ about x-axis. Many more properties can be seen easily. First of all:

Singular Point: A point $P(x, y)$ on a curve $F(x, y) = 0$, is said to be a singular point if

$$\left(\frac{\partial f}{\partial x}\right)_P = 0 \text{ and } \left(\frac{\partial f}{\partial y}\right)_P = 0.$$

Recall an ordinary point or a smooth point on the curve $f(x, y) = 0$, where the curve has a definite tangent.
Let $f(x, y) = 0$ be the curve. If both $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ exist, then we get

$$\frac{\partial f}{\partial x} + \frac{\partial f}{\partial y} \cdot \frac{dy}{dx} = 0$$

and so the slope of the tangent at $P(x, y)$:

$$\frac{dy}{dx} = -\frac{\left(\frac{\partial f}{\partial x}\right)_P}{\left(\frac{\partial f}{\partial y}\right)_P}$$

Now, if at least one of the partial derivative does not vanish, one of $\frac{dy}{dx}$ or $\frac{dx}{dy}$, can be determined (at P). The point then has surely a tangent and the point P is called an ordinary point. However, if both the partial derivative $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ at P vanish, the point P is called a singular point.
Further, a curve given by $f(x, y) = 0$ is said to be singular, if it has at least one singular point.
We shall discuss general real curves first, and then Elliptic curves in particular.

Example 1 Let the curve be given by $C : f(x, y) = 0$, where $f(x, y) = x^2 + y^2 - 1$, i.e. unit circle with origin as its centre. Then

$$\frac{\partial f}{\partial x} = 2x = 0 \implies x = 0$$

$$\frac{\partial f}{\partial y} = 2y = 0 \implies y = 0$$

Both $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ is zero only at $(0, 0)$ i.e. origin. But this does not lie on C. Hence, the curve C has no singular points.

Example 2 Let the curve be given by $C : f(x, y) = (x-1)^2-(y-1)(y-2)^2$, then

$$\frac{\partial f}{\partial x} = 0 \implies x = 1$$

$$\begin{aligned}
\frac{\partial f}{\partial y} = 0 &\implies -(y-1)\cdot 2(y-2) - (y-2)^2 = 0 \\
&\implies (y-2)\{2y - 2 + (y-2)\} = 0 \\
&\implies (y-2)(3y-4) = 0 \\
&\implies y = 2, \frac{4}{3}
\end{aligned}$$

Possible singular points are : $(1, 2)$ and $(1, \frac{4}{3})$.
However $(1, \frac{4}{3})$ does not lie on C. The point $(1, 2)$ is the only singular point of C.

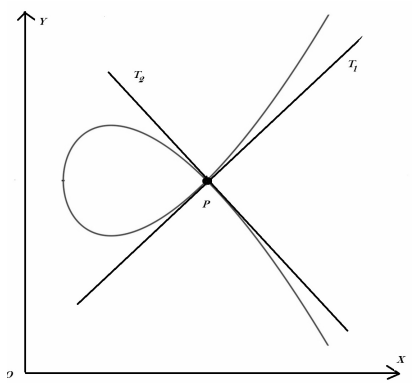
Double, Triple, Multiple Point: A point $P(x, y)$ on a curve C given by $f(x, y) = 0$ is said to be a multiple point of C, if more than one branch of C pass through P. In particular, if two branches pass through $P \in C$, P is called a double point of C. Like wise, if three branches pass through $P \in C$, P is called a triple point of C. A multiple point $P \in C$ is said to be of order m if m branches of C pass through P.

We shall discuss double point in more detail.

Types of Double Point: Let $P(x, y)$ be a double point of a curve C given by $f(x, y) = 0$. So there are two branches pass through P, and thus two tangent at P to C. These may be real and distinct, real and coincident, or imaginary. Accordingly, P is said to be

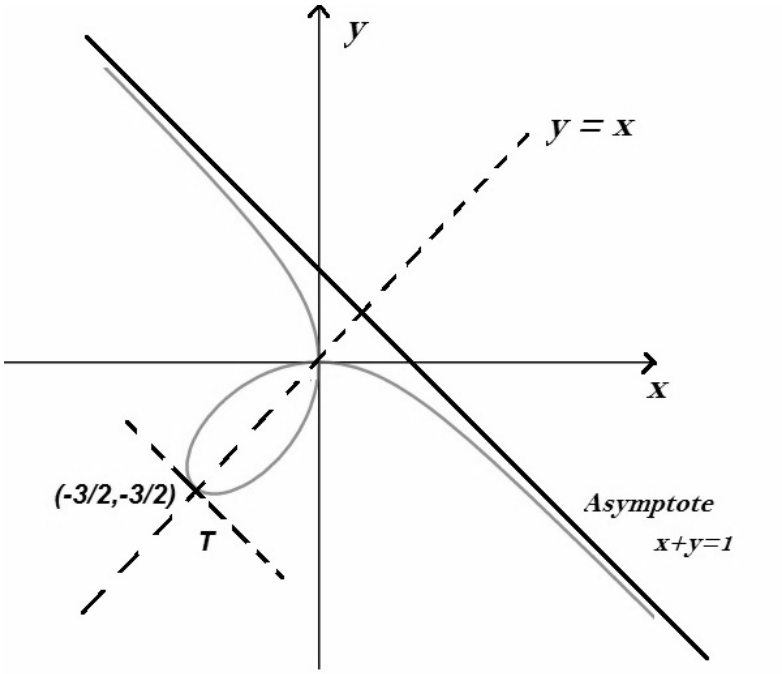
1. Node
2. Cusp
3. Conjugate or isolated point of C

More details on double points
Node: If $P(x, y)$ is a node of the curve C: $f(x, y) = 0$, then there exist two real, distinct tangent. The shape will be of the type



The curve crosses itself.

Example 3 Let C be given by : $f(x, y) = 0$, where $f(x, y) = x^3 + y^3 + 3xy$ or $x^3 + y^3 = -3xy$.
Let us trace the curve:



Observe that

1. The curve is symmetric about the line $y = x$. The point of intersection of line $y = x$ with C are given by substituting $y = x$ in the equation of C. That is:

$$2x^3 + 3x^2 = 0 \implies x^2(2x + 3) = 0 \implies x = 0, -\frac{3}{2}$$

Points of intersection are $(0, 0), (-\frac{3}{2}, -\frac{3}{2})$.
You may verify that:

2. The curve passes through origin but does not meet any of the coordinate axis at any other point.

3. There is no curve in the first quadrant.

4. Slope of the tangent at $(-\frac{3}{2}, -\frac{3}{2})$ is

$$\left(\frac{dy}{dx}\right)_{(-\frac{3}{2},-\frac{3}{2})} = -\frac{\left(\frac{\partial f}{\partial x}\right)_{(-\frac{3}{2},-\frac{3}{2})}}{\left(\frac{\partial f}{\partial y}\right)_{(-\frac{3}{2},-\frac{3}{2})}} = -\left(\frac{3x^2+3y}{3y^2+3x}\right)_{(-\frac{3}{2},-\frac{3}{2})} = -1$$

   Hence the equation of the tangent T at $(-\frac{3}{2}, -\frac{3}{2})$:

$$y + \frac{3}{2} = -\left(x + \frac{3}{2}\right) \implies T : x + y + 3 = 0$$

5. The line $A : x + y = 1$ is the only asymptote to the curve.

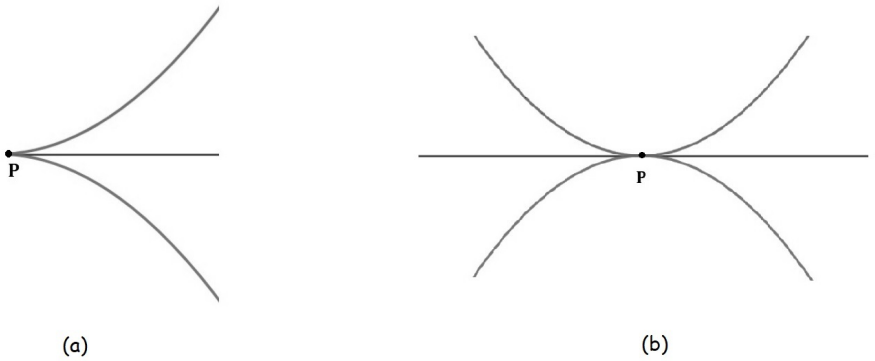
6. The curve lies between the tangent $T : x+y+3 = 0$ and the asymptote $A : x + y = 1$.

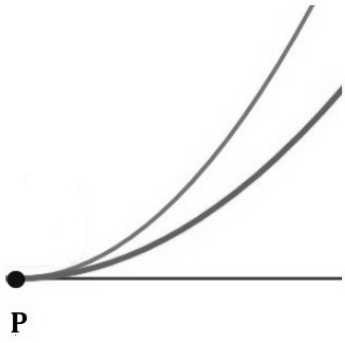
7. All points of C except origin are ordinary.

8. Origin is a point, where two coordinate axis namely $y = 0$, and $x = 0$ are two distinct and real tangents.

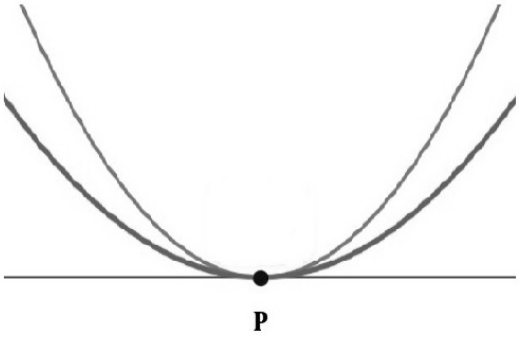
9. Origin is a node for the curve $C : f(x, y) = 0$, where $f(x, y) = x^3 + y^3 + 3xy$

Cusp: If the two tangent at a double point P on a curve C are real but coincident, P is called its cusp.
Depending of the two branches of the curve and the tangent at P, the curve at P may look like any of the following:

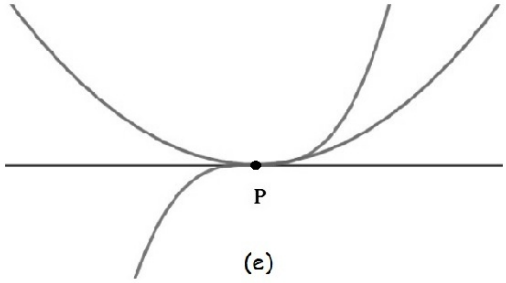




(c)



(d)



(e)

Accordingly, P is called.
Single Cusp: Figure (a) and (c), when the branches do not extend on both sides of the normal at P.

Double Cusp: Figures (d) and (e), when the branches extend on the both sides of the normal at P.

First Species: Figures (a) and (b), when two branches are on the opposite sides of the tangent at P.

Second Species: Figures (c) and (d), when the two branches of the curve are on the same side of the tangent at P.

Point of Oscul-inflexion: A double cusp if it is a mix of the two species e.g. Figure (e), then it is called a point of oscul-inflexion.

Example 5: Let C be given by $f(x,y)=0$, where $f(x,y)=x^3-y^3+x^2$
Observe that

$$\frac{\partial f}{\partial x}=3x^2+2x=0 \implies x=0,\ -\frac{2}{3}$$

and

$$\frac{\partial f}{\partial y}=-3y^2=0 \implies y=0.$$

Hence possible singular points are $(0,0)$ and $(-\frac{2}{3},0)$. Since $(0,0)$ lies on C, and $(-\frac{2}{3},0)$ does not lie on C. We get that $(0,0)$ is the only singular point on C.
Further, to know more about the nature of the point $(0,0)$, note that the tangent(s) at origin are given by $x^2=0$. The two tangents are real but coincident. In fact, it is a cusp of first species. (Prove it).

Example 6: Let C be given by $f(x,y)=x^2+y^2-x^3=0$
For $P(x,y)\in C$ to be singular point of C, $\left(\frac{\partial f}{\partial x}\right)_P=0$ and $\left(\frac{\partial f}{\partial y}\right)_P=0$
i.e.

$$2x-3x^2=0 \implies x(2-3x)=0 \implies x=0,\frac{2}{3},$$

$$2y=0 \implies y=0$$

Possible singular points are : $(0,0)$ and $(\frac{2}{3},0)$. The point $(0,0)$ lies on C, but $(\frac{2}{3},0)$ does not lie on C. Hence $(0,0)$ is the only singular point of C. Note that at $(0,0)$, the tangents are given by $x^2+y^2=0$, which means the tangents are imaginary. Thus $(0,0)$ is a double point, in fact only one. It is a conjugate point.

Necessary Condition For Double Points A necessary condition for the existence of a singular point P on a curve C is that at P, the values of $\frac{\partial f}{\partial x}=0$ and $\frac{\partial f}{\partial y}=0$. And, therefore a necessary condition for a double point or a multiple point is same i.e. $\left(\frac{\partial f}{\partial x}\right)_P=0$, $\left(\frac{\partial f}{\partial y}\right)_P=0$.
Further, a double point P on a curve $C: f(x,y)=0$ can be classified as:

1. **Node:** if $\left(\frac{\partial^2 f}{\partial x\partial y}\right)_P^2-\left(\frac{\partial^2 f}{\partial x^2}\right)_P\left(\frac{\partial^2 f}{\partial y^2}\right)_P>0$

2. **Cusp:** if $\left(\frac{\partial^2 f}{\partial x \partial y}\right)_P^2 - \left(\frac{\partial^2 f}{\partial x^2}\right)_P \left(\frac{\partial^2 f}{\partial y^2}\right)_P = 0$

3. **Conjugate Point:** if $\left(\frac{\partial^2 f}{\partial x \partial y}\right)_P^2 - \left(\frac{\partial^2 f}{\partial x^2}\right)_P \left(\frac{\partial^2 f}{\partial y^2}\right)_P < 0$

4. If $\left(\frac{\partial^2 f}{\partial x^2}\right)_P = 0, \left(\frac{\partial^2 f}{\partial y^2}\right)_P = 0$ and $\left(\frac{\partial^2 f}{\partial x \partial y}\right)_P = 0$

then the singular point $P \in C$ is called triple point.

Execise: Prove above statements.

Example 7: Let the curve C be given by : $f(x, y) = 0$, where

$$f(x, y) = x^2(x - y) + y^2 = x^3 - x^2 y + y^2$$

For singular points :

$$\frac{\partial f}{\partial x} = 0, \ \frac{\partial f}{\partial y} = 0$$

$$\frac{\partial f}{\partial x} = 3x^2 - 2xy = 0 \implies x(3x - 2y) = 0 \implies x = 0, y = \frac{3}{2}x$$

$$\frac{\partial f}{\partial y} = -x^2 + 2y = 0 \implies -x^2 + (3x) = 0 \implies x(-x + 3) = 0 \implies x = 0, 3$$

Possible singular points :$(0, 0), \ (3, \frac{9}{2})$.
Out of these $(3, \frac{9}{2})$ does not lie on C as

$$3^2(3 - \frac{9}{2}) + \left(\frac{9}{2}\right)^2 = 3^2\left(-\frac{3}{2}\right) + \frac{9^2}{4} = \frac{81}{4} - \frac{27}{2} \neq 0$$

However, $(0, 0)$ lies on C. So $(0, 0)$ is the only singular point. We discuss further, the nature of the singular point. We shall use the second derivative test.

$$\frac{\partial f}{\partial x} = 3x^2 - 2xy \implies \frac{\partial^2 f}{\partial x^2} = 6x - 2y$$
$$\frac{\partial f}{\partial y} = -x^2 + 2y \implies \frac{\partial^2 f}{\partial y^2} = 2$$
$$\frac{\partial^2 f}{\partial x \partial y} = -2x$$
$$\left(\frac{\partial^2 f}{\partial x \partial y}\right)^2 - \left(\frac{\partial^2 f}{\partial x^2}\right)\left(\frac{\partial^2 f}{\partial y^2}\right) = (-2x^2) - (6x - 2y)(2) = 4x^2 - 12x + 4y$$

At $(0, 0)$, this value is 0. Hence $(0, 0)$ is a cusp.

Discuss the nature of the cusp at $(0, 0)$ as follows:

1. Prove that $y = 0$ i.e. $x-$axis is a tangent at origin.
2. Note that $f(0, y) = y^2$ implies that in the neighborhood of origin, the curve is symmetric about $x-$axis i.e. the common tangent. Hence, origin is a cusp of first species.

Leture-16

Singular and Non singular Elliptic Curve

Let $E = E_{\mathbb{R}} = \{(x, y) \in \mathbb{R} \times \mathbb{R} | y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{R}\} \cup \{\infty\}$ be a real Elliptic Curve. The curve is singular if $\left(\frac{\partial f}{\partial x}\right)_P = 0$ and $\left(\frac{\partial f}{\partial y}\right)_P = 0$ at some point $P(x, y) \in E$ such a point is called a singular point.

For example: If $E = E_{\mathbb{R}} = \{(x, y) \in \mathbb{R} \times \mathbb{R} | f(x, y) = y^2 - x^3 + x^2 = 0\} \cup \{\infty\}$, then $(0, 0) \in E$ is such that

$$\left(\frac{\partial f}{\partial x}\right)_{(0,0)} = (-3x^2 + 2x)_{(0,0)} = 0 \text{ and } \left(\frac{\partial f}{\partial y}\right)_{(0,0)} = (2y)_{(0,0)} = 0$$

Hence $(0, 0)$ is a singular point of E, and E is a singular curve.
The point $P(x, y) \in E_{\mathbb{R}}$ is a non singular, if at least one of $\left(\frac{\partial f}{\partial x}\right)$ and $\left(\frac{\partial f}{\partial y}\right)$ is non zero at P. The curve E is non singular curve if every point of E is non singular point.

Theorem: Let $E = E_{\mathbb{R}} = \{(x, y) \in \mathbb{R} \times \mathbb{R} | y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{R}\} \cup \{\infty\}$. The following statement are equivalent.

1. E is a non singular curve.
2. The polynomial $f(x) = x^3 + Ax + B = 0$ has no repeated root.
3. $4A^3 + 27B^2 \neq 0$

Proof: (1) and (2) are equivalent is obvious.
For (2) and (3) are equivalent, we prove that $f(x) = x^3 + Ax + B = 0$ has repeated root if and only if $4A^3 + 27B^2 = 0$

Suppose, $f(x) = 0$ has a repeated root α. Two cases arises.
(a) α is repeated thrice
(b) α is repeated twice
In case (a): $f(x) = x^3 + Ax + B = (x - \alpha)^3 = x^3 - 3\alpha x^2 + 3\alpha x - \alpha^3$
On comparing the coefficient we get

$$-3\alpha = 0 \implies \alpha = 0$$

$$A = 3\alpha = 0; \quad B = -\alpha^3 = 0 \implies A = 0, B = 0$$
$$\implies 4A^3 + 27B^2 = 0$$

In case (b): $f(x) = x^3 + Ax + B = (x - \alpha)^2(x - \beta)$, for some $\beta \neq \alpha$.
Again, this implies that

$$x^3 + Ax + B = x^3 - (\beta + 2\alpha)x^2 + (\alpha^2 + 2\alpha\beta)x - \alpha^2\beta$$

On comparing the coefficient we get

$$\beta + 2\alpha = 0; \quad \alpha^2 + 2\alpha\beta = A; \quad -\alpha^2\beta = B$$
$$\implies \beta = -2\alpha; \quad \alpha^2 + 2\alpha(-2\alpha) = A; \quad -\alpha^2(-2\alpha) = B$$
$$\implies \beta = -2\alpha; \quad -3\alpha^2 = A; \quad 2\alpha^3 = B$$
$$\alpha = \left(-\frac{A}{3}\right)^{\frac{1}{2}}$$

and

$$\alpha = \left(\frac{B}{2}\right)^{\frac{1}{3}} \implies \left(-\frac{A}{3}\right)^{\frac{1}{2}} = \left(\frac{B}{2}\right)^{\frac{1}{3}}$$

Raising 6-th power on both side, we have

$$\left(-\frac{A}{3}\right)^3 = \left(\frac{B}{2}\right)^2$$
$$\implies -\frac{A^3}{27} = \frac{B^2}{4}$$
$$\implies 4A^3 + 27B^2 = 0$$

Conversely, suppose $4A^3 + 27B^2 = 0$
This gives that

$$\begin{aligned} -\frac{A^3}{27} = \frac{B^2}{4} &\implies \left(-\frac{A}{3}\right)^3 = \left(-\frac{B}{2}\right)^2 \\ &\implies \left(-\frac{A}{3}\right)^{\frac{1}{2}} = \left(-\frac{B}{2}\right)^{\frac{1}{3}} = \alpha \text{ (say)} \\ &\implies \alpha^2 = -\frac{A}{3} \text{ and } \alpha^3 = \frac{B}{2} \end{aligned}$$

Now

$$(x-\alpha)^2(x+2\alpha) = x^3 - 3\alpha^2 x + 2\alpha^3 = x^3 + Ax + B$$

This proves the equivalence of (2) and (3).

More On Roots Of A Polynomial

Recall, an element $b \in F$ said to be a root or a zero of a polynomial $f(x) \in F[x]$, if $f(b) = 0$. Obviously, $b \in F$ is a root of $f(x)$ if and only if $(x - b)$ divides $f(x)$. Further, $b \in F$ is said to be a root of $f(x)$ of multiplicity k, if $(x - b)^k$ divides $f(x)$, but $(x - b)^{k+1}$ does not divide $f(x)$.
In case $k = 1$, the root is called a simple root, if $k \geq 2$, then it is called a multiple root or repeated root. It is easy to see that $b \in F$ is a multiple root of $f(x)$ if and only if $f(x)$ and its derivative $f'(x)$ has b as a common root.
A polynomial $f(x) \in K[x]$ is said to split in F, (an extension F of K) if

$$f(x) = a(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$$

where a is the coefficient of the highest power of x in $f(x)$. The field F is called the splitting field of $f(x)$, if F is the smallest such extension of K. In that case $F = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.
Splitting fields can be useful in knowing if a polynomial has a multiple root. For this we need:

Discriminant $D(f)$ of a polynomial $f(x) \in K[x]$

Let $f(x) \in K[x]$ be a polynomial of degree n split into linear factor in $F[x]$, where F is the splitting field of K, as :

$$f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

then the discriminate $D(f)$ of $f(x)$ is defined as

$$D(f) = a^{2n-2} \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)^2; \quad \alpha_i \in F \quad \forall i = 1, 2, \ldots, n$$

Obviously $f(x)$ has a multiple root if and only if its discriminate $D(f) = 0$.
Although α_i's $\in F$, but $D(f) \in K$ (Prove)
For example, if $f(x) = ax^2 + bx + c = a(x-\alpha_1)(x-\alpha_2)$, then

$$\begin{aligned} D(f) &= a^2(\alpha_1 - \alpha_2)^2 \\ &= a^2\{(\alpha_1+\alpha_2)^2 - 4\alpha_1\alpha_2\} \\ &= a^2\left\{\left(-\frac{b}{a}\right)^2 - 4\cdot\frac{c}{a}\right\} \\ &= b^2 - 4ac \end{aligned}$$

Thus $D(ax^2+bx+c) = b^2 - 4ac$
And the two roots are equal if and only if $b^2 = 4ac$.

Exercise: Prove that:
$D(ax^3+bx^2+cx+d) = b^2c^2 - 4b^3d - 4ac^3 - 27a^2d^2 + 18abcd$

Corollary 1 $D(x^3+ax+b) = -(4a^3+27b^2)$.

Corollary 2 x^3+ax+b has a repeated root if and only if $4a^3+27b^2 = 0$.

For cryptographic applications, we mainly consider non-singular Elliptic Curves.
Henceforth, take K to be a field of $Char(K) = p$

1. **When $\mathbf{p \neq 2, 3}$**

$$E_K = \{(x,y) \in K \times K |\ y^2 = x^3 + ax + b; \quad a, b \in K\} \cup \{\infty\}$$
where $x^3 + ax + b = 0$ has no repeated root

$$E_K = \{(x,y) \in K \times K | y^2 = x^3 + ax + b; \quad 4a^3 + 27b^2 \neq 0\} \cup \{\infty\}$$

2. **When p = 2**

   (a)

   $$E_K = \{(x,y) \in K \times K | y^2 + cy = x^3 + ax + b; \quad a,b,c \in K \quad \} \cup \{\infty\}$$
   $$\text{such that } x^3 + ax + b = 0 \text{ has no repeated root.}$$

   (b)

   $$E_K = \{(x,y) \in K \times K | y^2 + xy = x^3 + ax^2 + b; \quad a,b \in K \quad \} \cup \{\infty\}$$
   $$\text{such that } x^3 + ax^2 + b = 0 \text{ has no repeated root.}$$

3. **When p = 3**

   (a)

   $$E_K = \{(x,y) \in K \times K | y^2 = x^3 + ax + b; \quad a,b \in K \quad \} \cup \{\infty\}$$
   $$\text{such that } x^3 + ax + b = 0 \text{ has no repeated root.}$$

   (b)

   $$E_K = \{(x,y) \in K \times K | y^2 = x^3 + ax^2 + b; \quad a,b \in K \quad \} \cup \{\infty\}$$
   $$\text{such that } x^3 + ax^2 + b = 0 \text{ has no repeated root.}$$

   Or combining the two cases:

   $$E_K = \{(x,y) \in K \times K | y^2 = x^3 + ax^2 + bx + c; \quad a,b,c \in K \quad \} \cup \{\infty\}$$
   $$\text{such that } x^3 + ax^2 + bx + c = 0 \text{ has no repeated root.}$$

Graph of an Elliptic Curve over $\mathbb{R}$

Let $E = E_{\mathbb{R}} = \{(x,y) \in \mathbb{R} \times \mathbb{R} : \ y^2 = x^3 + ax + b; \ a,b \in \mathbb{R}$ be such that $x^3 + ax + b = 0$ has no repeated roots$\} \cup \{\infty\}$.
We had seen this is equivalent to $4a^3 + 27b^2 \neq 0$ or $D(x^3 + ax + b) = -(4a^3 + 27b^2)$ the discriminant of $x^3 + ax + b$ is non zero. In the context of elliptic curves, the discriminant is denoted by

$$\Delta(E) = -16(4a^3 + 27b^2).$$

Thus $4a^3 + 27b^2 \neq$ iff $\Delta(E) \neq 0$.
Further, if $x^3 + ax + b = 0$ has no repeated root, then it has either one real root, or all the three real roots. This happens (Prove that) depending on $\Delta(E)$ is negative or positive.

Consider, the following Examples:
Example 1: $E_1 = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y^2 = x^3 + 2x - 3\} \cup \{\infty\}$

Example 2: $E_2 = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y^2 = x^3 - 7x + 6\} \cup \{\infty\}$.

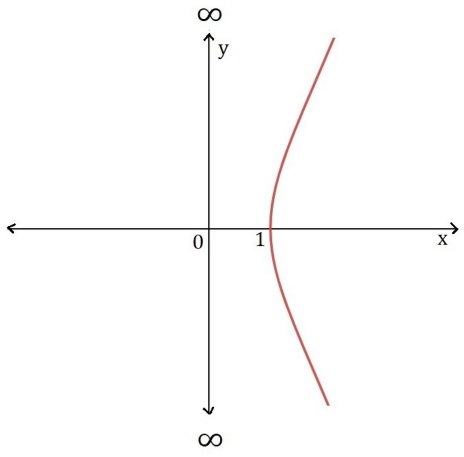
Observe that $\Delta(E_1) = -16(4 \cdot 2^3 + 27(-3)^2) < 0$. So, $x^3 + 2x - 3$ has exactly one real root. This is evident as

$$x^3 + 2x - 3 = (x - 1)(x^2 + x + 3)$$

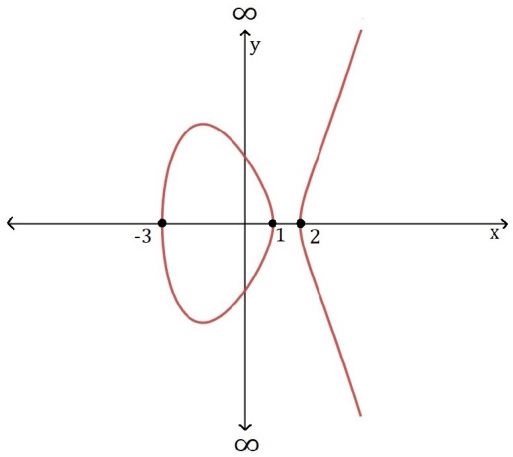
has only one real root namely $x = 1$, as $x^2 + x + 3$ has no real root.
Similarly,

$$\begin{aligned} \Delta(E_2) &= -16(4 \cdot (-7)^3 + 27 \cdot 6^2) \\ &= -64\{(-7)^3 + 27 \cdot 9\} \\ &= -64(-347 + 243) = 6400 > 0 \end{aligned}$$

Hence $x^3 - 7x + 6 = 0$ has all the three roots to be real. This too is clear that the roots are $x = 1, 2, -3$ as $x^3 - 7x + 6 = (x - 1)(x - 2)(x + 3)$.
We can now draw these graphs.



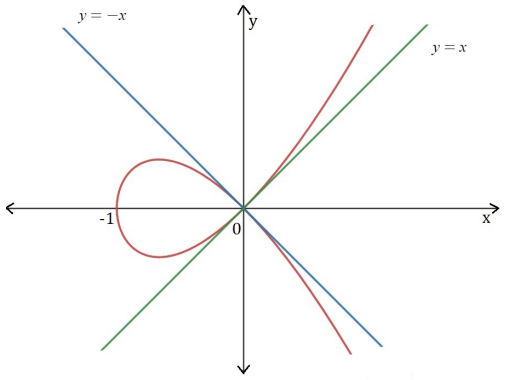
$E_1 = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y^2 = x^3 + 2x - 3\} \cup \{\infty\}$



$E_2 = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y^2 = x^3 - 7x + 6\} \cup \{\infty\}$

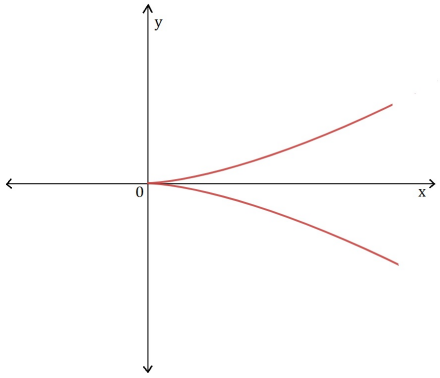
Examples of singular real Elliptic Curve:

Example 3: $E_1 = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y^2 = x^3 + x^2\} \cup \{\infty\}$.
Note that the $x^3 + x^2 = x^2(x + 1)$. The only singular point of E is $(0, 0)$. This is a node as $y = \pm x$ are two real tangents to the curve at this point. The graph is like:



$E_1 = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y^2 = x^3 + x^2\} \cup \{\infty\}$

Example 4: $E = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y^2 = x^3\} \cup \{\infty\}$. Note that the curve has only one singular point, namely $(0, 0)$, as $x^3 = 0$, has root $x = 0$, repeated thrice. The graph of the curve:



$E = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y^2 = x^3\} \cup \{\infty\}$

Analyzing the nature of the double point $(0,0)$ of E, we find that $(0,0)$ is a cusp of the first species as $y=0$ is the common tangent , and the branches of the curve lie on both sides of the tangent.

Examples Of An Elliptic Curve Over A Finite Field

Example 5: Le the the curve E is give by

$$E = \{(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p : \ y^2 = x^3 + ax + b; \ a,b \in \mathbb{Z}_p\} \cup \{\infty\}$$

For $p = 11, \ a = 3, \ b = 1$, this is

$$E = \{(x,y) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11} : \ y^2 = x^3 + 3x + 1; \ a,b \in \mathbb{Z}_p\} \cup \{\infty\}$$

The discriminant

$$\begin{aligned} \Delta(E) &= -16(4a^3 + 27b^2) = -16(4 \cdot 3^3 + 27 \cdot 1^2) \\ &= -16 \cdot 5 \cdot 27 = -2160 \\ &= 7 - 2167 = 7 - (197 \cdot 11) \equiv 7 \not\equiv 0 \mod 11 \end{aligned}$$

Hence the curve is non-singular.
As x, y both come from $\mathbb{Z}_p = \mathbb{Z}_{11}$, the curve has finitely many points. The number of points on E, except the point at infinity, is at most $11^2 = 121$. That is total number of points is at most 122. This number, however can be brought down to 20, using Hasse's Theorem. The point in E may be further less.
We calculate the points as follows:

x	0	1	2	3	4	5	6	7	8	9	10
y^2	1	5	15	37	77	141	235	365	537	757	100031
$y^2 \pmod{11}$	1	5	4	4	0	9	4	2	9	9	10

y	0	1	2	3	4	5	6	7	8	9	10
$y^2 \pmod{11}$	0	1	4	9	5	3	3	5	9	4	1

$y^2 \pmod{11}$	0	1	3	4	5	9
$y \pmod{11}$	0	1,10	5,6	2,9	4,7	3,8

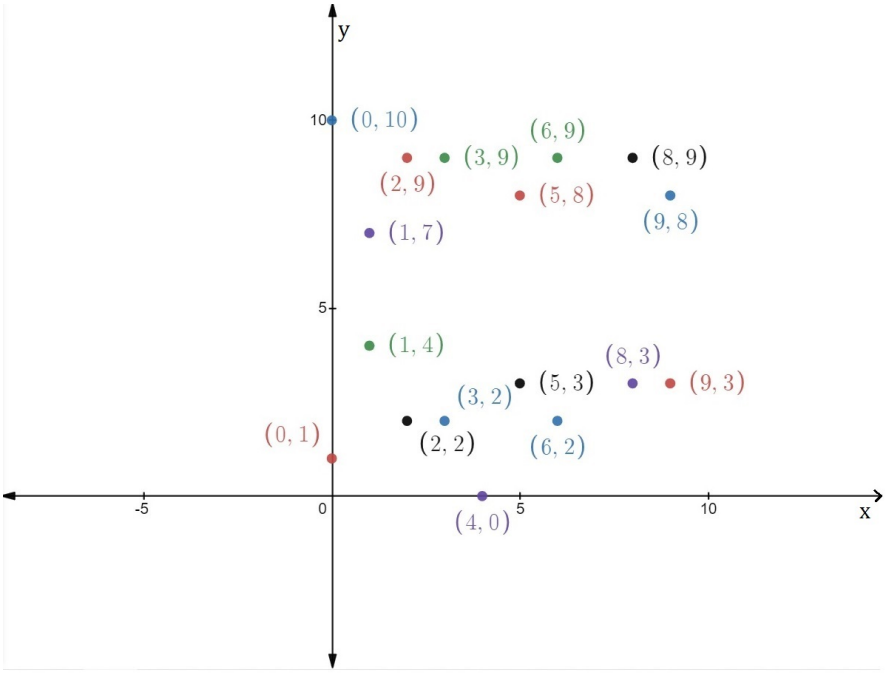
this gives the correspondence :

x	0	0	1	1	2	2	3	3	4	5	5	6	6	8	8	9	9
y	1	10	4	7	2	9	2	9	0	3	8	2	3	3	9	3	8

Hence the curve E is:

$$E := \{(0,1),(0,10),(1,4),(1,7),(2,2),(2,9),(3,2),(3,9),(4,0),(5,3),(5,8),$$

$$,(6,2),(6,9),(8,3),(8,9),(9,3),(9,8)\} \cup \{\infty\}$$



$$E = \{(x,y) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11} : \ y^2 = x^3 + x + 1; \ a,b \in \mathbb{Z}_{11}\} \cup \{\infty\}$$

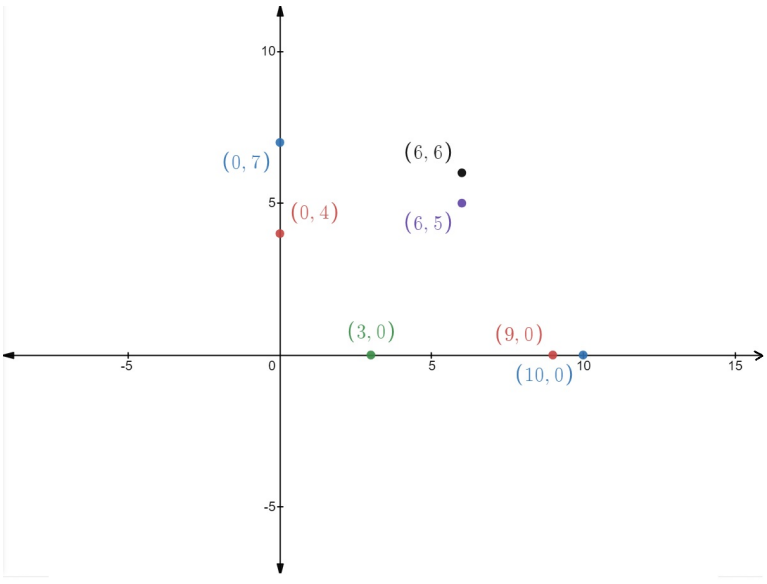
Example 6: Let the curve be defined by

$$E = E(\mathbb{Z}_{11}) = \{(x,y) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11} : \ y^2 = x^3 + 4x + 5\} \cup \{\infty\}$$

Its discriminant

$$\begin{aligned}\Delta(E) &= -16(4a^3 + 27b^2) \\ &\equiv 6(4a^3 + 5b^2) \pmod{11} \\ &\equiv 6(4 \cdot 4^3 + 5 \cdot 5^2) \pmod{11} \\ &\equiv 6(4 \cdot 64 + 5 \cdot 25) \pmod{11} \\ &\equiv 6(4(-2) + 5 \cdot 3) \pmod{11} \\ &\equiv 6(15 - 8) \equiv 6 \cdot 7 \pmod{11} \\ &\equiv 42 \pmod{11} \\ &\equiv -4 \equiv 7 \pmod{11} \not\equiv 0 \pmod{11}\end{aligned}$$

Hence the curve is non-singular. The number of points on E, using Hasse's Theorem, can not exceed 20. In fact, they are much less. Since $\mathbb{Z}_{11}$ is a small field, you can find all points of E by taking every $(x, y) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11}$ and checking if $P(x, y) \in E$, that is by observing $y^2 = x^3 + 4x + 5$ or not. And list all:
Points of $E : (0, 4),\ (0, 7),\ (3, 0),\ (6, 5),\ (6, 6),\ (9, 0),\ (10, 0), \infty$
Hence $E = \{(0, 4),\ (0, 7),\ (3, 0),\ (6, 5),\ (6, 6),\ (9, 0),\ (10, 0)\} \cup \{\infty\}$
Note that E has just eight points, including the point at infinity.



$E = E(\mathbb{Z}_{11}) = \{(x, y) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11} :\ y^2 = x^3 + 4x + 5\} \cup \{\infty\}$

Examples of Curves Over Field of Characteristic 2

Example 7: Let $E = \{(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_2 | y^2 + y = x^3 + x\} \cup \{\infty\}$.
Recall that the Elliptic Curve over finite fields K of characteristic 2 are of the form

1.

$$E_1 = \{(x, y) \in K \times K | y^2 + cy = x^3 + ax + b; \quad a, b, c \in K \quad \} \cup \{\infty\}$$
$$\text{such that } x^3 + ax + b = 0 \text{ has no repeated root.}$$

2.

$$E_2 = \{(x, y) \in K \times K | y^2 + xy = x^3 + ax^2 + b; \quad a, b \in K \quad \} \cup \{\infty\}$$
$$\text{such that } x^3 + ax^2 + b = 0 \text{ has no repeated root.}$$

The above example is an example of the form of E_1. We calculate point of E as follows:

x	$y^2 + y = x^3 + x$	y
0	0	0,1
1	0	0,1

Points: $(x, y) = (0, 0), (0, 1), (1, 0), (1, 1)$
Hence $E = \{(0, 0), (0, 1), (1, 0), (1, 1)\} \cup \{\infty\}$.
Number of points $\#(E) = 5$

Example 8: Let $E = \{(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_2 | y^2 + xy = x^3 + 1\} \cup \{\infty\}$.
This is an example of the form of E_2. We calculate points as follows:

x	$y^2 + xy = x^3 + 1$	y
0	$y^2 = 1$	1
1	$y^2 + y = 0$	0,1

Hence $E = \{(0, 1), (1, 0), (1, 1)\} \cup \{\infty\}$
The number of points $\#(E) = 4$

Example 9: Let $E = \{(x, y) \in F_4 \times F_4 | y^2 + y = x^3 + x\} \cup \{\infty\}$, where F_4 is a finite field of order 4.
Observe that $f(x) = x^2+x+1 \in \mathbb{Z}_2[x]$ is an irreducible quadratic polynomial over $\mathbb{Z}_2$. Let ω be a root of $f(x) = 0$. Then $\omega \neq 1, \omega^2+\omega+1 = 0$ and $\omega^3 = 1$.
We can take $F_4 = \{0, 1, \omega, \omega^2 | \omega^2 + \omega + 1 = 0\}$
We calculate points of E as follows:

x	$y^2 + y = x^3 + x$	y
0	0	0,1
1	0	0,1
ω	$1 + \omega = \omega^2$	-
$\omega^2 = 1 + \omega$	$1 + \omega^2 = \omega = \omega^4$	-

Hence the curve $E = \{(0, 0), (0, 1), (1, 0), (1, 1)\} \cup \{\infty\}$.
Number of points of E is $\#(E) = 5$.

Example 10: $E = \{(x, y) \in F_4 \times F_4 | y^2 + xy = x^3 + 1\} \cup \{\infty\}$, where F_4 is a finite field of order 4.
Recall

$$F_4 \cong \frac{\mathbb{Z}_2[x]}{\langle f(x) = x^2 + x + 1\rangle}$$

If ω is the primitive root of $f(x)$, then $\omega \neq 1, \omega^2 + \omega + 1 = 0$.
We can take $F_4 = \{0, 1, \omega, \omega^2 | \omega^2 + \omega + 1 = 0\}$
We calculate points of E as follows:

x	$y^2 + xy = x^3 + 1$	y
0	$y^2 = 1$	1
1	$y^2 + y = 0$	0,1
ω	$y^2 + \omega y = 0$	0,ω
ω^2	$y^2 + \omega^2 y = 0$	0,ω^2

Hence $E = \{(0, 1), (1, 0), (1, 1), (\omega, 0), (\omega, \omega), (\omega^2, 0), (\omega^2, \omega^2)\} \cup \{\infty\}$
Number of points of E is $\#(E) = 8$.

Example of Elliptic Curves Over Fields of Characteristic 3

Example 11: Let $E = \{(x, y) \in \mathbb{Z}_3 \times \mathbb{Z}_3 | y^2 = x^3 - x + 2\} \cup \{\infty\}$
Recall the Elliptic Curves defined over finite field of characteristic 3 are of the form:

$$E_K = \{(x, y) \in K \times K | y^2 = x^3 + ax^2 + bx + c; \quad a, b, c \in K \quad \} \cup \{\infty\}$$
$$\text{such that } x^3 + ax^2 + bx + c = 0 \text{ has no repeated root.}$$

These can be further divided into the following two types:

1.
$$E_1 = \{(x, y) \in K \times K | y^2 = x^3 + ax + b; \quad a, b \in K \quad \} \cup \{\infty\}$$
$$\text{such that } x^3 + ax + b = 0 \text{ has no repeated root.}$$

2.
$$E_2 = \{(x, y) \in K \times K | y^2 = x^3 + ax^2 + b; \quad a, b \in K \quad \} \cup \{\infty\}$$
$$\text{such that } x^3 + ax^2 + b = 0 \text{ has no repeated root.}$$

The given example curve is of the form E_1.
We calculate points of E as follows:

x	$y^2 = x^3 - x + 2$	y
0	2	-
1	2	-
2	2	-

Recall the Legendre Symbol $\left(\frac{2}{3}\right) = -1$
That is 2 is a quadratic non residue mod 3 i.e. $y^2 = 2 \pmod 3$ has no solution.
Hence $E = \{\infty\}$ and $\#(E) = 1$
Further, the curve is non singular as $\frac{\partial f}{\partial x} = 3x^2 - 1 = 2 \in \mathbb{Z}_3[x]$ is non zero for all $P(x, y) \in E$

Example 12: Let

$$E = \{(x, y) \in \mathbb{Z}_3 \times \mathbb{Z}_3 : \ y^2 = x^3 - x^2 + 2\} \cup \{\infty\}$$

$$= \{(x,y) \in \mathbb{Z}_3 \times \mathbb{Z}_3 : \ F(x,y) = 0\} \cup \{\infty\}$$

where $F(x,y) = y^2 - x^3 + x^2 - 2$

$$\frac{\partial f}{\partial x} = -3x^2 + 2x \equiv 2x \text{ over } \mathbb{Z}_3$$

Also

$$\frac{\partial f}{\partial x} = 0 \implies x = 0$$

$$\frac{\partial f}{\partial y} = 2y = 0 \implies y = 0$$

Hence, possible singular point is $(0,0)$. But $(0,0)$ does not lie on E. So the curve is non singular. We calcuate points of E as follows:

x	0	1	2
$y^2 = x^3 - x^2 + 2$	2	2	0
y	-	-	0

Points of E : $(0,2),\ \infty$; Hence $E = \{(2,0), \infty\}$, $\#(E) = 2 \cong C_2$

Example 13: Let $E = \{(x,y) \in \mathbb{F}_9 \times \mathbb{F}_9 : \ y^2 = x^3 - x + 2\} \cup \{\infty\}$, and

$$\mathbb{F}_9 \cong \frac{\mathbb{Z}_3[x]}{\langle g(x) = x^2 + x + 2 \rangle}$$

If ξ is a root of $x^2 + x + 2 = 0$, then ξ is a primitive $8th$ root of unity over $\mathbb{Z}_3$, and we can take

$$\mathbb{F}_9 = \{0, \xi^i : \ 1 \le i \le 8; \ \xi^2 + \xi + 2 = 0\}$$
$$= \{0, \xi, \ \xi^2 = 1 + 2\xi, \ \xi^3 = 2 + 2\xi, \ \xi^4 = -1 = 2, \ \xi^5 = 2\xi, \ \xi^6 = 1 + \xi, \ \xi^7 = 1 + \xi, \ \xi^8 = 1\}$$

We compute points of E as follows:

x	0	ξ	ξ^2	ξ^3	$\xi^4 = -1 = 2$
$y^2 = x^3 - x + 2$	2	$\xi^3 - \xi + 2$	$\xi^6 - \xi^2 + 2$	$\xi^9 - \xi^3 + 2$	$\xi^{12} - \xi^4 + 2$
y^2	2	$1 + \xi$	2ξ	2ξ	2
y^2	ξ^4	ξ^7	ξ^5	ξ^5	ξ^4
y	$\xi^2,\ 2\xi^2$	-	-	-	$\xi^2,\ 2\xi^2$

x	ξ^5	ξ^6	ξ^7	$\xi^8 = 1$
$y^2 = x^3 - x + 2$	$\xi^{15} - \xi^5 + 2$	$\xi^{18} - \xi^6 + 2$	$\xi^{21} - \xi^7 + 2$	$\xi^{24} - \xi^8 + 2$
y^2	2ξ	$1 + \xi$	$1 + \xi$	2
y^2	ξ^5	ξ^7	ξ^7	ξ^4
y	-	-	-	$\xi^2,\ 2\xi^2$

Point of E are :

$$(0, \xi^2), (0, 2\xi^2), (\xi^4, \xi^2), (\xi^4, 2\xi^2), (\xi^8, \xi^2), (\xi^8, 2\xi^2)$$

or

$$(0, 1 + 2\xi), (0, 2 + \xi), (2, 1 + 2\xi), (2, 2 + \xi), (1, 1 + 2\xi), (1, 2 + \xi)$$

and the point at infinity $'\infty'$

Hence $E := \{(0, 1+2\xi), (0, 2+\xi), (2, 1+2\xi), (2, 2+\xi), (1, 1+2\xi), (1, 2+\xi), \infty\}$.
And $\#(E) = 7$

Example 14: Let $E = \{(x, y) \in \mathbb{F}_9 \times \mathbb{F}_9 :\ y^2 = x^3 - x^2 + 2\} \cup \{\infty\}$
This is an example of type (ii) case curve, when $char(\mathbb{F}) = 3$.
Let

$$\mathbb{F}_9 \cong \frac{\mathbb{Z}_3[x]}{\langle g(x) = x^2 + x + 2\rangle}$$

If ξ is a root of $x^2 + x + 2 = 0$, then ξ is a primitive $8th$ root of unity over $\mathbb{Z}_3$, and we can take

$$\begin{aligned}\mathbb{F}_9 &= \{0, \xi^i :\ 1 \le i \le 8;\ \xi^2 + \xi + 2 = 0\} \\ &= \{0, \xi,\ \xi^2 = 1 + 2\xi,\ \xi^3 = 2 + 2\xi,\ \xi^4 = -1 = 2,\ \xi^5 = 2\xi,\ \xi^6 = 1 + \xi,\ \xi^7 = 1 + \xi,\ \xi^8 = 1\}\end{aligned}$$

We compute points of E as follows:

x	0	ξ	$\xi^2 = 1 + 2\xi$
$y^2 = x^3 - x^2 + 2$	2	$\xi^3 - \xi^2 + 2$	$\xi^6 - \xi^4 + 2$
y^2	ξ^4	$(2 + 2\xi) - (1 + 2\xi) + 2$	$(2 + \xi) - 2 + 2$
y^2	ξ^4	0	$2 + \xi = \xi^6$
y	$\xi^2,\ 2\xi^2$	0	$\xi^3,\ 2\xi^3$
y	$1 + 2\xi,\ 2 + \xi$	0	$2 + 2\xi,\ 1 + \xi$

x	$\xi^3 = 2 + 2\xi$	$\xi^4 = 2 = -1$	$\xi^5 = 2\xi$
$y^2 = x^3 - x^2 + 2$	$\xi^9 - \xi^6 + 2$	$\xi^{12} - \xi^8 + 2$	$\xi^{15} - \xi^{10} + 2$
y^2	$\xi - (2 + \xi) + 2$	$\xi^4 - 1 - 1$	$\xi^7 - \xi^2 + 2$
y^2	0	0	$(1 + \xi) - (1 + 2\xi) + 2 = 2 - \xi$ $= 2 + 2\xi = \xi^3$
y	0	0	-
y	0	0	-

x	$\xi^6 = 2 + \xi$	$\xi^7 = 1 + \xi$	$\xi^8 = 1$
$y^2 = x^3 - x^2 + 2$	$\xi^{18} - \xi^{12} + 2$	$\xi^{21} - \xi^{14} + 2$	$\xi^{24} - \xi^{16} + 2$
y^2	$\xi^2 - \xi^4 + 2$	$\xi^5 - \xi^6 + 2$	$1 - 1 + 2$
y^2	$(1 + 2\xi) - 2 + 2$	$(2\xi) - (2 + \xi) + 2$	2
y^2	$(1 + 2\xi) = \xi^2$	ξ	ξ^4
y	$\xi,\ 2\xi$	-	$\xi^2,\ 2\xi^2$
y	$\xi,\ 2\xi$	-	$1 + 2\xi,\ 2 + \xi$

This gives us the curve

$$E = \{(0, 1 + 2\xi), (0, 2 + \xi), (\xi, 0), (1 + 2\xi, 2 + 2\xi), (1 + 2\xi, 1 + \xi), (2 + 2\xi, 0), (2, 0), (2 + \xi, \xi), (2 + \xi, 2\xi), (1, 1 + 2\xi), (1, 2 + \xi)\} \cup \{\infty\}$$

Number of points of E : $\#(E) = 12$

Algebraic Structure on Elliptic Curve E

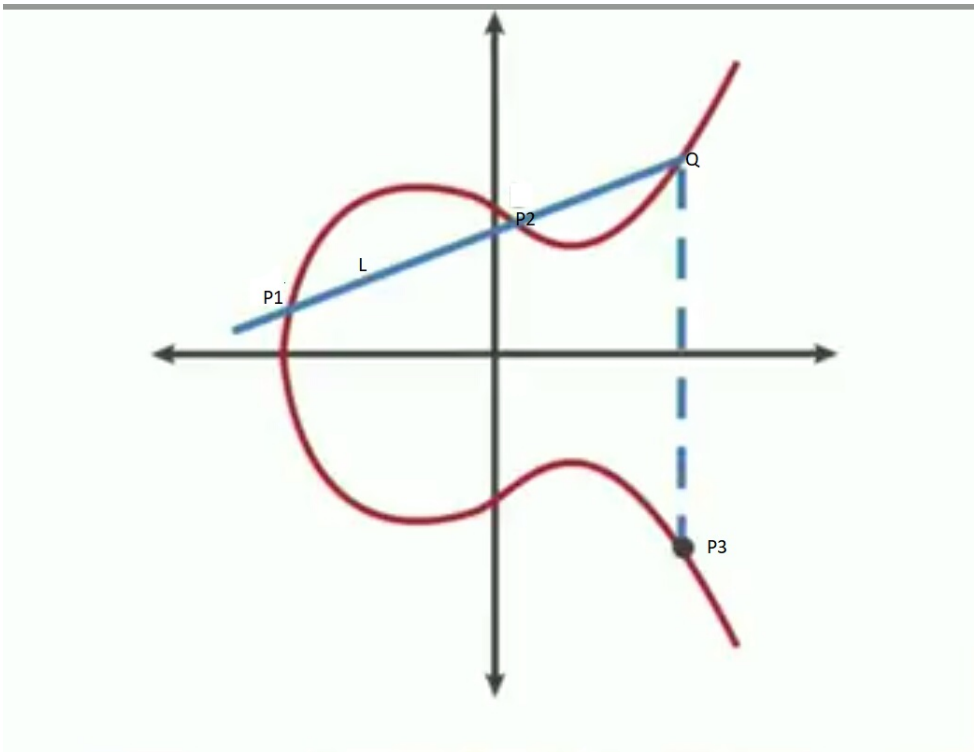
Let $\mathbb{F}$ be a field of characteristic 0 or a prime p, $p \neq 2$ *and* $p \neq 3$. Define the set

$$E_{\mathbb{F}} = \{(x, y) \in \mathbb{F} \times \mathbb{F} : \ y^2 = x^3 + ax + b\} \cup \{\infty\} \qquad \textit{where } a, b \in \mathbb{F}.$$

Define a **Relation** on $E_{\mathbb{F}}$:
If $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ be two points in $E_{\mathbb{F}}$ ($P_(x_1, y_1)$ is the point (x_1, y_1) represented by P_1), then define

$$P_3(x_3, y_3) = P_1(x_1, y_1) + P_2(x_2, y_2)$$

as follows :
Take L to be the the line P_1P_2 joining the points P_1 and P_2. Extend the same.
Let the line L meet the curve at Q. Define P_3 to be the reflection about $x-$ axis of Q on the curve $E_{\mathbb{F}}$. For example, see the curve in the bfollowing figure :



Properties desired by the relation (addition of points of Elliptic Curves $E_{\mathbb{F}}$

We desire the following Rules for addition:

1. *Closure property:* For every $P_1, P_2 \in E_{\mathbb{F}}$ their sum $P_1 + P_2 \in E_{\mathbb{F}}$
2. *Existence of (additive) identity property:*$P(x, y)+\infty = \infty+P(x, y) = P$ *including:* $\infty + \infty = \infty$ (We shall see the meaning of ∞ by example and figure given below)

3. *Existence of (additive) inverse:* If $P(x,y) = P \in E_{\mathbb{F}}$, then $P(x,-y) = -P(x,y) = -P \in E_{\mathbb{F}}$. That is $P(x,y) + P(x,-y) = P + (-P) = \infty$

4. *Commutative property:* $P_1(x_1,y_1) + P_2(x_2,y_2) = P_2(x_2,y_2) + P_1(x_1,y_1)$ for all $P_1, P_2 \in E_{\mathbb{F}}$

5. *Associative property:*$(P_1(x_1,y_1) + P_2(x_2,y_2)) + P_3(x_3,y_3) = P_1(x_1,y_1) + (P_2(x_2,y_2) + P_3(x_3,y_3))$ $\forall P_1, P_2, P_3 \in E_{\mathbb{F}}$

Note: Assuming above rules and $'\infty'$ as additive identity, the set $E_{\mathbb{F}}$ becomes an (additive) Abelian group.

Verify for $E_{\mathbb{F}}$: The properties listed above, using the geometry for addition of points. You will see thal The Associative Property (5th property) is the most difficult to prove, although it appears to be trivial.

Meaning of point at infinity ∞ and geometry of point addition on an elliptic curve

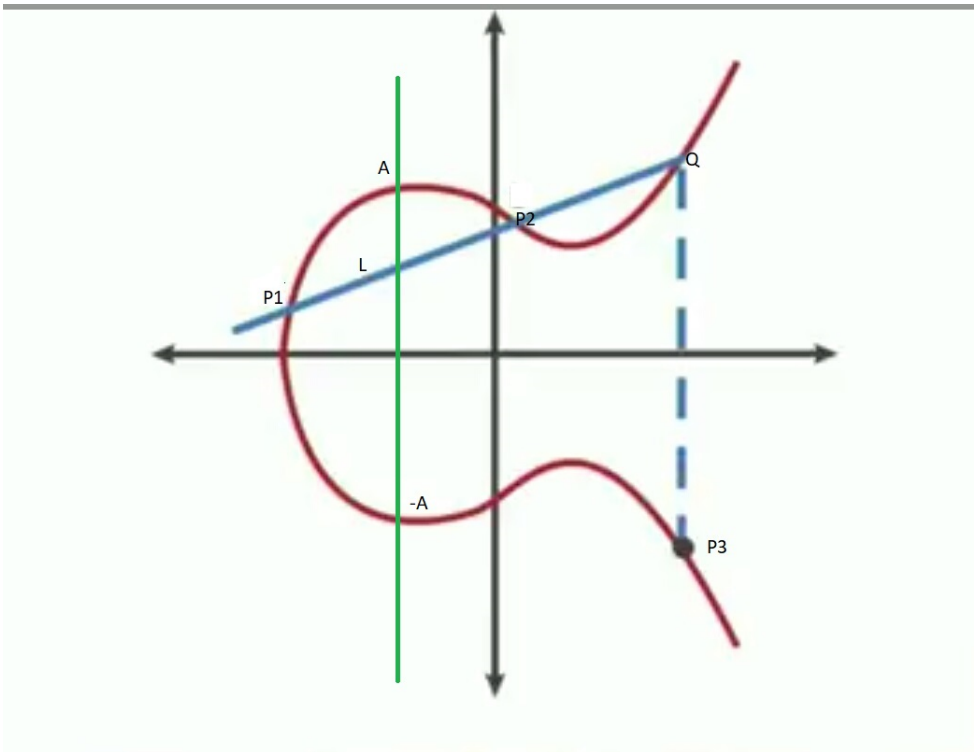
Although, things can be best explaind using algebraic geometry(projective space P^2_K over a field K), we define the point at infinity $'\infty'$ to be a point and a member of $E_{\mathbb{F}}$ defined to be geometrically sitting at the end point of every ordinate. We defer the algebraic geometric treatment of the concept for the timebeing.

Recall : If $P_1(x_1,y_1)$ and $P_2(x_2,y_2)$ are two distinct points (none of them point at infinity $'\infty'$) on $E_{\mathbb{F}}$, then the points $P_(x_1,y_1)$ can be represented as the points $(x_1,y_1),(x_2,y_2)$ represented by P_1 and P_2 respectively, in the figure. Recall, how their addition is defined.

$$P_3(x_3,y_3) = P_1(x_1,y_1) + P_2(x_2,y_2)$$

This was done in case $x_1 \neq x_2$ by : Take the line $L = P_1P_2$ joining P_1 and P_2 and extend the same. If the line L meet the curve at Q, then define P_3 to be the reflection of Q on $E_{\mathbb{F}}$.

Similarly, if we join (i.e. add) A and $-A$, case of two distinct points (none of them point at infinity $'\infty'$) on $E_{\mathbb{F}}$ having same $x-$ coordinate (as shown in the figure by green line), the line we get is a straight line parallel



to $y-$ axis, and thus it will not intersect the curve further (except at A and $-A$).

Since the line joining A and $-A$ goes to ∞ without intersecting the curve at any other point except A and $-A$, thus we assume

$$A + (-A) = \ Image\ of\ \infty = \infty.$$

If the points P_1, P_2 are identical (except the point at infinity, $'\infty'$), the line $l = P_1P_2$ becomes tangent to the curvge at P_1, Q is the point on the curve, whwre $'l'$ meets the curve, and the sum $P_1 + P_2 = P_3$ is the reflection on the curve about $x-$ axis olf the point Q. Similary, other rules too can be explained.

We need to develop algebraic formula for the coordinates of the point addition.

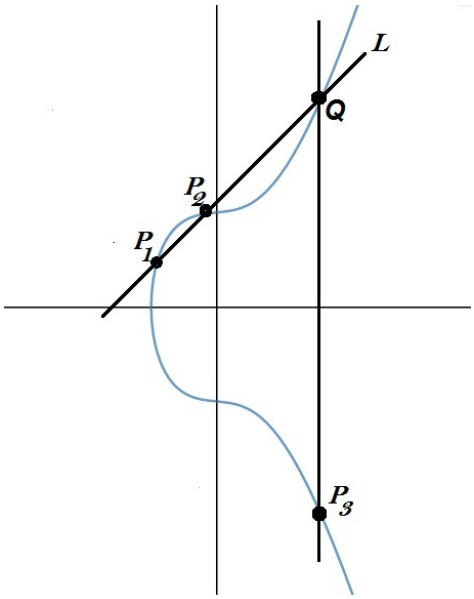
Algebraic Formula For Point Addition

Recall from geometry, discussed as earlier, the following rules hold for adding points $P_1(x_1, y_1), P_2(x_2, y_2), P_3(x_3, y_3)$ on an Elliptic Curve

$$E_{\mathbb{R}} = \{(x, y) \in \mathbb{R} \times \mathbb{R} | y^2 = x^3 + ax + b; \quad a, b \in \mathbb{R}\} \cup \{\infty\}$$

1. If $P_2 = \infty$, the point at infinity, then $P_1 + \infty = P_1 \quad \forall P_1 \in E$
2. If $x_1 = x_2$ but $y_1 \neq y_2$, then $P_1 + P_2 = \infty$.
3. If $P_1 = P_2$, and $y_1 = 0$, then $P_1 + P_2 = 2P_1 = \infty$.
4. (a) $P_1 \neq P_2$ with $x_1 \neq x_2$, and
   (b) $P_1 = P_2$ with $y_1 \neq 0$

Case(a)



Let L be the line joining P_1 to P_2. Suppose on extending it meets at Q, the curve E, and suppose P_3 is the reflection of Q, about $x-$axis on E. Then $P_1 + P_2 = P_3$

To determine coefficient (x_3, y_3) of P_3 in terms of the coordinates (x_1, y_1) of P_1 and (x_2, y_2) of P_2. Since $P_3(x_3, y_3) \in E$ is the point reflected by Q, we get the coordinates of Q as $(x_3, -y_3)$.
Now equation of $L : y = mx + c$, where $m = \frac{y_2 - y_1}{x_2 - x_1}$, since it passes through P_1 and P_2, we get :

$$y_2 = mx_2 + c, \quad y_1 = mx_1 + c.$$

$$\implies y_2 - y_1 = m(x_2 - x_1)$$

since $x_2 \neq x_1 \implies m = \frac{y_2 - y_1}{x_2 - x_1}$
Further,

$$y_1 = mx_1 + c \implies c = y_1 - mx_1$$

Hence equation of L: $y = mx + y_1 - mx_1$ or L: $y - y_1 = m(x - x_1)$, where $m = \frac{y_2 - y_1}{x_2 - x_1}$ or L: $y = m(x - x_1) + y_1$
Since L meets E at Q, we get:

$$\begin{aligned}
y^2 =& x^3 + ax + b \\
\implies & \{m(x - x_1) + y_1\}^2 = x^3 + ax + b \\
\implies & m^2(x - x_1)^2 + y_1^2 + 2m(x - x_1)y_1 = x^3 + ax + b \\
\implies & m^2(x^2 - 2xx_1 + x_1^2) + y_1^2 + 2m(xy_1 - x_1y_1) = x^3 + ax + b \\
\implies & x^3 - m^2x^2 + (a + 2m^2x_1 - 2my_1)x + (b - m^2x_1^2 - y_1^2 + 2mx_1y_1 = 0)
\end{aligned}$$

This is a cubic equation with roots x_1, x_2, x_3 as $P_1(x_1, y_1), P_2(x_2, y_2)$ and $Q_3(x_3, -y_3) \in E$
We observe that $x_1 + x_2 + x_3 = m^2$

$$\implies x_3 = m^2 - x_1 - x_2$$

Also L: $y = m(x - x_1) + y_1$, as $Q_3(x_3, -y_3)$ lies on this line L, we get:

$$\begin{aligned}
-y_3 =& m(x_3 - x_1) + y_1 \\
\text{or } -y_3 =& -m(x_1 - x_3) + y_1 \\
\implies y_3 =& m(x_1 - x_3) - y_1
\end{aligned}$$

Hence $P_3(x_3, y_3)$ can be given by:

$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = m(x_1 - x_3) - y_1,$$

where $m = \frac{y_2 - y_1}{x_2 - x_1}$.

Case(b) $P_1 = P_2$, and $y_1 \neq 0$. The line L become tangent to the curve E at $P_1(x, y)$. The slope of L, can be obtained as $\left(\frac{dy}{dx}\right)_{P_1(x_1, y_1)}$ on differentiation of $y^2 = x^3 + ax + b$ i.e.

$$2y\frac{dy}{dx} = 3x^2 + a \implies m = \left(\frac{dy}{dx}\right)_{P_1} = \frac{3x_1^2 + a}{2y_1}$$

This gives $P_1 + P_2 = 2P_1 = P_3(x_3, y_3)$,
where

$$\begin{aligned} x_3 &= m^2 - 2x_1 \\ y_3 &= m(x_1 - x_3) - y_1 \\ m &= \frac{3x_1^2 + a}{2y_1} \end{aligned}$$

We now summarize the definition of point addition on an Elliptic Curve over $\mathbb{R}$ given by:

$$E_{\mathbb{F}} := \{(x, y) \in \mathbb{F} \times \mathbb{F} : \ y^2 = x^3 + ax + b; \ a, b \in \mathbb{F}\} \cup \{\infty\}$$

where $\Delta(E) \neq 0$,
as follows : for $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, and $P_3 = (x_3, y_3)$

1. If $P_1, P_2 \neq \infty$ then $P_1 + P_2 = P_3$
   (a) When $x_1 \neq x_2$,

   $$x_3 = m^2 - x_1 - x_2, \ y_3 = m(x_1 - x_3) - y_1$$

   where $m = \frac{y_2 - y_1}{x_2 - x_1}$
   (b) When $x_1 = x_2$ but $y_1 \neq y_2$, $P_3 = \infty$
   (c) When $P_1 = P_2$ but $y_1 \neq 0$ then

   $$x_3 = m^2 - 2x_1, \ y_3 = m(x_1 - x_3) - y_1$$

   where $m = \frac{3x_1^2 + a}{2y_1}$

(d) When $P_1 = P_2$ and $y_1 = 0$ then $P_1 + P_2 = \infty$

2. $P + \infty = P \ \ \forall P \in E$
   (So $\infty + \infty = \infty$ is included)

These rules are defined for a field $\mathbb{F}$ of characteristic $char(\mathbb{F}) > 3$. In case $char(\mathbb{F}) = 2$ or 3, the rules are different.

It is easy to see that $P_1 + P_2 \in E \ \ \forall P_1, P_2 \in E$ and that:

1. The point addition is commutative.
   That is $P_1 + P_2 = P_2 + P_1 \ \ \forall P_1, P_2 \in E$

2. The point at infinity ∞ serves as the identity of the this addition, since $P + \infty = P = \infty + P \ \ \forall P \in E$

3. If $P(x, y) \in E$, then there is a point Q on E, such that

$$P + Q = \infty = Q + P$$

   This point Q is the additive inverse of P, and is usually denoted by $-P$. So for $P(x, y) \in E, \ -P(x, y) = (x, -y)$

4. The point addition is associative. That is

$$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3) \ \forall P_1, P_2, P_3 \in E.$$

   Although, it appears to be trivial. But this is the most difficult of all to prove as it requires to consider all cases for each P_1, P_2 and P_3.

Once all the properties of point addition are verified, we get that E becomes an Abelian group with respect to addition (of points on E).
In case $\mathbb{F}$ is a finite field, $E_{\mathbb{F}}$ or $E(\mathbb{F})$ becomes a finite Abelian group. By the fundamental theorem for finite Abelian gropus, E is isomorphic onto a finite direct sum of finite cyclic groups. In fact more can be said. We shall discuss that later on.
First, we shall discuss various examples of Elliptic curves over the filed $\mathbb{F} = \mathbb{R}$, finite fields $\mathbb{F}$ of characteristic $p > 3$, of characteristic $p = 2$, as well as over characteristic $p = 3$, fields.

Leture-17

Computations of integer multiples of a point on a curve E and the group E

We compute kP, for an integer k, using the laws of addition and duplication of points on E.

Example 1: Let $E := \{(x, y) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11} : \ y^2 = x^3 + 3x + 1\} \cup \{\infty\}$
If $P(x_1, y_1) \in E$, and if $P \neq \infty$, then $2P(x_3, y_3)$, where

$$\begin{aligned} x_3 =& m^2 - 2x_1 \\ y_3 =& m(x_1 - x_3) - y_1 \\ m =& \frac{3x^2 + a}{2y_1} \end{aligned}$$

For $x_1 = 4, y = 0$ i.e. for $P(4, 0)$,
we calculate $m = \frac{3 \cdot 4^2 + 3}{0} = \infty, \ 2P = \infty$ (point at infinity). Order of P is 2.

For $P(5, 8)$ i.e. $x_1 = 5, y_1 = 8$,

$$\begin{aligned} m =& \frac{3 \cdot 5^2 + 3}{2 \cdot 8} = \frac{78}{16} \\ =& \frac{1}{5} \equiv 5^{-1} \pmod{11} \\ \equiv& 9 \pmod{11} \end{aligned}$$

$$x_3 = 9^2 - 2 \cdot 5 = 81 - 10 = 71 \equiv 5 \pmod{11};$$

$$y_3 = 9 \cdot (5 - 5) - 8 \equiv -8 \equiv 3 \pmod{11}$$

Hence $2P = (5, 3)$. It is easy to see that $3P = P + 2P = (5, 8) + (5, 3) = \infty$. This gives order of $(5, 8)$ to be 3.
If $P(0, 1)$, then it can be seen that

$$2P = (5, 8),\ 3P = (4, 0),\ 4P = (5, 3),\ 5P = (0, 10),\ 6P = \infty$$

Finally, for $P(1, 4) \in E$ verify that

$$\begin{array}{cccc} 2P = (2, 9) & 3P = (0, 1) & 4P = (8, 8) & 5P = (3, 9) \\ 6P = (5, 8) & 7P = (6, 2) & 8P = (9, 8) & 9P = (4, 0) \\ 10P = (9, 3) & 11P = (6, 9) & 12P = (5, 3) & 13P = (3, 2) \\ 14P = (8, 3) & 15P = (0, 10) & 16P = (2, 2) & 17P = (1, 7) \\ & 18P = \infty & & \end{array}$$

Computation of order of a point $P(x, y)$ on an Elliptic Curve E.

Let $P(x, y)$ be point of the Elliptic Curve E, then the least non-negative integer k is said to be the order of P in E if $kP = \infty$ (point at infinity). Recall the curve

$$E := \{(x, y) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11} :\ y^2 = x^3 + 3x + 1\} \cup \{\infty\}$$

We have calculated all the points of E. They are 18 in all. To be specific:

$$\begin{aligned} E :=& \{(0, 1), (0, 10), (1, 4), (1, 7), (2, 2), (2, 9), (3, 2), (3, 9), (4, 0), (5, 3), (5, 8), \\ & (6, 2), (6, 9), (8, 3), (8, 9), (9, 3), (9, 8)\} \cup \{\infty\} \end{aligned}$$

Compute and observe that if $P = (4, 0)$, then $2P = \infty$.
Hence order of P is 2.
If $P = (5, 8)$, then $3P = \infty$. Hence order of $P(5, 8)$ is 3.
If $P = (0, 1)$, then $6P = \infty$. Hence order of $P(0, 1)$ is 6.
If $P = (2, 2)$, then $9P = \infty$. Hence order of $P(2, 2)$ is 9.
If $P = (1, 4)$, then $18P = \infty$. Hence order of $P(1, 4)$ is 18.
This also proves that E is a cyclic group C_{18} of order 18. The point $P(1, 4)$ is a generator of this group (with respect to point addition). Find all other generators. We can write E as:

$$E := \langle P(1, 4) :\ 18P = \infty \rangle = \{kP(1, 4) :\ 1 \leq k \leq 18\} \cong C_{18}$$

Recall the Elliptic Curve

Example 2:

$$E := E(\mathbb{Z}_{11}) = \{(x, y) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11} : \ y^2 = x^3 + 4x + 5\} \cup \{\infty\}$$

$$= \{(0, 4), (0, 7), (3, 0), (6, 5), (6, 6), (9, 0), (10, 0)\} \cup \{\infty\}$$

Note that : $\#(E) = 8$
Every element has order 2 or 4, as follows:
Points of order 2 are: $(3, 0), (9, 0), (10, 0)$
Points of order 4 are: $(0, 4), (0, 7), (6, 5), (6, 6)$

For $P(0, 4) = (x_1, y_1),\ x_1 = 0, y_1 = 4, 2P = (x_3, y_3)$, where

$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = m(x_1 - x_3) - y_1,$$

and

$$\begin{aligned} m =& \frac{y_2 - y_1}{x_2 - x_1} \text{ if } x_1 \neq x_2 \\ =& \frac{3x_1^2 + a}{2y_1} \text{ if } P_1 = P_2 \ \& \ y_1 \neq 0 \end{aligned}$$

Here

$$\begin{aligned} m =& \frac{3 \cdot 0^2 + 4}{2 \cdot 4} = \frac{4}{8} \quad \text{as } a = 4,\ b = 5, \\ \equiv& \frac{1}{2} \\ \equiv& 6 \quad \because 2 \times 6 \equiv 12 \equiv 1 \pmod{11} \end{aligned}$$

$$\begin{aligned} &\implies x_3 \equiv 6^2 - 0 - 0 = 36 \equiv 3 \pmod{11} \text{ and} \\ &\implies y_3 = 6(0 - 3) - 4 = -18 - 4 = -22 \equiv 0 \pmod{11} \end{aligned}$$

Hence $2P(x_3, y_3) = (3, 0)$.
Clearly $4P(0, 4) = 2P + 2P = (3, 0) + (3, 0) = \infty$. It is easy to see that

$3P = P + 2P = (0,4) + (3,0) = (0,7)$, using the addition of points formula. Since, there is no element of order 8, and the Elliptic curve E has 8 points in all, the group of points E is an Abelian group which can not be cyclic. Therefore, by the fundamental theorem of finite abelian group, E is isomorphic to $C_2 \times C_2 \times C_2$ or $C_2 \times C_4$. It can not be isomorphic to $C_2 \times C_2 \times C_2$ as it has points of order 4, e.g. if $P(0,4)$, then $2P = (3,0)$ and $4P = \infty$. This leaves, $E \cong C_2 \times C_4$. In fact, this is the case.
Observe that, subgroup of E of order 2: are the subgroups generated by $\langle(3,0)\rangle, \langle(9,0)\rangle, \langle(10,0)\rangle$. These are $\{(3,0),\infty\}, \{(9,0),\infty\}, \{(10,0),\infty\}$.
Similarly, subgroup of order 4:

$$\langle(0,4) : 4(0,4) = \infty\rangle = \{(0,4), 2(0,4) = (3,0), 3(0,4) = (0,7), 4(0,4) = \infty\}$$
$$\langle(6,5) : 4(6,5) = \infty\rangle = \{(6,5), 2(6,5) = (3,0), 3(6,5) = (6,6), 4(6,5) = \infty\}$$

You can prove that $E = \langle(9,0)\rangle \oplus \langle(0,4)\rangle$
For, $\langle(9,0)\rangle \oplus \langle(0,4)\rangle \subseteq E$ as $\langle(9,0)\rangle$ and $\langle(0,4)\rangle$ are subgroups of E.
Conversely

$$\begin{aligned}
(0,4) &= \infty + (0,4), \quad (0,7) = \infty + 3(0,4),\\
(3,0) &= \infty + 2(0,4), \quad (6,5) = (9,0) + (0,7) = (9,0) + 3(0,4),\\
(6,6) &= (9,0) + (0,4), \quad (9,0) = (9,0) + \infty,\\
(10,0) &= (9,0) + (3,0) = (9,0) + 2(0,4), \quad \infty = \infty + \infty.
\end{aligned}$$

This gives that $E \subseteq \langle(9,0)\rangle \oplus \langle(0,4)\rangle$ or that $E = \langle(9,0)\rangle \oplus \langle(0,4)\rangle \cong C_2 \times C_4$.

Example 3: Consider $E = \{(x,y) \in \mathbb{Z}_{29} \times \mathbb{Z}_{29} : \ y^2 = x^3 + 4x + 7\} \cup \{\infty\}$
Observe that $(6,0) \notin E$, since

$$6^3 + 4 \cdot 6 + 7 = 36 \cdot 6 + 31 \equiv 7.6 + 2 \equiv 42 + 2 = 44 \equiv 15 \not\equiv 0 \pmod{29}$$

However,

$$(0,6) \in E, \text{ since } x^3 + 4x + 7 = 0 + 7 = 7 \equiv 29 + 7 \equiv 36 \equiv 6^2 \pmod{29}$$

$\implies (0,-6)$ i.e. $(0,23)$ also is a point on E.
Since 29 is not a big number, all points on E can be calculated simply taking $(x,y) \in \mathbb{Z}_{29} \times \mathbb{Z}_{29}$ and verifying if $P(x,y) \in E$.
The order of E, $\#(E)$ can not exceed $29^2 = 841$. The order, however can not exceed, by Hasse's Theorem:

$$p + 1 + 2\sqrt{p} \text{ i.e. } 29 + 1 + 2\sqrt{29} = 30 + 11 = 41.$$

The order infact is much less. It is $\#(E) = 32$ You may verify that:

$$\begin{aligned} E = &\{(0,6),(0,23),(2,9),(2,20),(4,0),(5,6),(5,23),(7,1),(7,28),\\ &(8,0),(13,9),(13,20),(14,9),(14,20),(15,7),(15,22),(16,7),\\ &(16,22),(17,0),(18,13),(18,16),(20,5),(20,24),(22,10),(22,19),\\ &(23,12),(23,17),(24,6),(24,23),(27,7),(27,22)\} \cup \{\infty\} \end{aligned}$$

Next to determine the structure of the group of point E with respect to point addition, observe the following:
If P is $(0,6)$, the $P(0,6) \in E$, and multiples of P as:

$$P = (0,6),\ 2P = (13,9),\ 3P = (20,5), 4P = (4,0),$$
$$5P = (20,24), 6P = (13,20), 7P = (0,23), 8P = \infty.$$

Hence $H = \langle P \rangle = \{kP :\ 1 \leq k \leq 8\}$ is a subgroup of E of order 8.
And if, $Q = (22,10)$, then $Q(22,10) \in E$, as

$$\begin{aligned} 22^3 + 4 \cdot 22 + 7 \equiv &(-7)^3 + 4(-7) + 7 \pmod{29}\\ \equiv &-7^3 - 4 \cdot 7 + 7 \pmod{29}\\ \equiv &-7^3 - 3 \cdot 7 \equiv -7(7^2 + 3) \pmod{29}\\ \equiv &-7 \cdot 52 \equiv -7(-6) \pmod{29}\\ \equiv &42 \equiv 13 \equiv 13 + 3 \cdot 29 \pmod{29}\\ \equiv &13 + 87 = 100 = (\pm 10)^2 \pmod{29} \end{aligned}$$

and $-Q(22,10) = (22,-10) = (22,19) \in E$.
Also, observe that

$$Q = (22,10),\ 2Q = (8,0),\ 3Q = (22,19),\ 4Q = \infty$$

So, if $K = \langle Q \rangle = \{jQ :\ 1 \leq j \leq 4\}$, then K is a subgroup of order 4.
Further $K \cap H = \{\infty\}$. $H \oplus K \leq E$ and $E \leq H \oplus K$, as

$$(2,20) = P + Q, \quad (18,13) = 2P + Q$$

and so on (verify for remaining elements).
Hence $E = H + K$ and $H \cap K = \{\infty\}$.
This gives that $E = H \oplus K \implies E \cong C_8 \times C_4 \cong C_4 \times C_8$

Point Addition In Elliptic Curves Over Fields Of Characteristic 3

Recall the Elliptic curve $E(F)$ over a field F of Characteristics 3:

$$E_K = \{(x,y) \in F \times F | y^2 = x^3 + ax^2 + bx + c; \quad a,b,c \in F \quad \} \cup \{\infty\}$$

Let $P(x,y), P_1(x_1,y_1), P_2(x_2,y_2), P_3(x_3,y_3)$ be points on E. We define the sum of two points $P_1 + P_2 = P_3$ as follows (if $P_1, P_2 \neq \infty$):

1. $P + \infty = P \quad \forall P \in E$ (including $\infty + \infty = \infty$).
2. If $P_1 \neq P_2$ with $x_1 \neq x_2$, then $P_1 + P_2 = P_3(x_3, y_3)$, where
$$\begin{aligned} x_3 =& m^2 - a - x_1 - x_2 \\ y_3 =& m(x_1 - x_3) - y_1 \\ m =& \frac{y_2 - y_1}{x_2 - x_1} \end{aligned}$$
3. $P_1 \neq P_2$ with $x_1 = x_2$ but $y_1 \neq y_2$, then $P_1 + P_2 = \infty$
4. If $P_1 = P_2$ with $y_1 \neq 0$, then $2P_1 = P_1 + P_2 = P_3(x_3, y_3)$, where
$$\begin{aligned} x_3 =& m^2 - a - 2x_1, \\ y_3 =& m(x_1 - x_3) - y_1 \\ m =& \frac{3x_1^2 + 2ax_1 + b}{2y_1} \\ =& \frac{2ax_1 + b}{2y_1} \quad \text{since } Char(F) = 3 \end{aligned}$$
5. If $P_1 = P_2$ and $y_1 = 0$, then $2P_1 = P_1 + P_2 = \infty$

Note that the curve E can be represented as:

$$E = \{(x,y) \in F \times F | g(x,y) = 0, \text{ where } g(x,y) = y^2 - x^3 - ax^2 - bx - c; a,b,c \in F\} \cup \{\infty\}$$

And at a non singular point P, the slope of the line (tangent in case $P_1 = P_2$) is m which can be computed using:

$$\begin{aligned} m =& \frac{\left(\frac{\partial g}{\partial x}\right)_{P=P_1=P_2}}{\left(\frac{\partial g}{\partial y}\right)_{P=P_1=P_2}} \\ m =& -\left(\frac{-3x^2 - 2ax - b}{2y}\right)_{P(x_1,y_1)} \\ m =& \left(\frac{3x_1^2 + 2ax_1 + b}{2y_1}\right) \\ m^2 =& \left(\frac{3x_1^2 + 2ax_1 + b}{2y_1}\right)^2 \end{aligned}$$

Equation of tangent at $P_1(x_1, y_1)$:

$$\begin{aligned} y - y_1 &= m(x - x_1) \\ \implies T : y &= m(x - x_1) + y_1 \end{aligned}$$

$Q(x_3, -y_3)$ lies on T : this implies that $-y_3 = m(x_3 - x_1) + y_1$
Since Q is reflection of $P_3(x_3, y_3)$ about $x-$axis on E, hence

$$\begin{aligned} y_3 &= -m(x_3 - x_1) - y_1 \\ \text{Or } y_3 &= m(x_1 - x_3) - y_1 \end{aligned}$$

Particular Case (1): If the curve $E = E(F)$, where $Char(F) = 3$ is given by:

$$E_K = \{(x, y) \in F \times F | y^2 = x^3 + ax + b; \quad a, b \in F \quad \} \cup \{\infty\}$$

We define the sum of two points $P_1 + P_2 = P_3$ as follows :

1. $P + \infty = P \quad \forall P \in E$ (including $\infty + \infty = \infty$).
2. If $P_1 \neq P_2$ with $x_1 \neq x_2$, then $P_1 + P_2 = P_3(x_3, y_3)$, where

$$\begin{aligned} x_3 =& m^2 - x_1 - x_2, \\ y_3 =& m(x_1 - x_3) - y_1 \\ m =& \frac{y_2 - y_1}{x_2 - x_1} \end{aligned}$$

3. $P_1 \neq P_2$ with $x_1 = x_2$ but $y_1 \neq y_2$, then $P_1 + P_2 = \infty$

4. If $P_1 = P_2$ with $y_1 \neq 0$, then $2P_1 = P_1 + P_2 = P_3(x_3, y_3)$, where

$$\begin{aligned} x_3 =& m^2 - 2x_1, \\ y_3 =& m(x_1 - x_3) - y_1 \\ m =& \frac{3x_1^2 + a}{2y_1} \\ =& \frac{a}{2y_1} \quad \text{since } Char(F) = 3 \end{aligned}$$

5. If $P_1 = P_2$ and $y_1 = 0$, then $2P_1 = P_1 + P_2 = \infty$

Particular Case (2): If the curve $E = E(F)$, where $Char(F) = 3$ is given by:

$$E_K = \{(x, y) \in F \times F | y^2 = x^3 + ax^2 + b; \quad a, b \in F \quad \} \cup \{\infty\}$$

then for $P_1(x_1, y_1), P_2(x_2, y_2) \neq \infty$, and $P(x, y) \in E$, we define the sum of two points $P_1 + P_2 = P_3$ as follows:

1. $P + \infty = P \quad \forall P \in E$ (including $\infty + \infty = \infty$).

2. If $P_1 \neq P_2$ with $x_1 \neq x_2$, then $P_1 + P_2 = P_3(x_3, y_3)$, where

$$\begin{aligned} x_3 =& m^2 - a - x_1 - x_2 \\ y_3 =& m(x_1 - x_3) - y_1 \\ m =& \frac{y_2 - y_1}{x_2 - x_1} \end{aligned}$$

3. $P_1 \neq P_2$ with $x_1 = x_2$ but $y_1 \neq y_2$, then $P_1 + P_2 = \infty$

4. If $P_1 = P_2$ with $y_1 \neq 0$, then $2P_1 = P_1 + P_2 = P_3(x_3, y_3)$, where

$$\begin{aligned} x_3 =& m^2 - a - 2x_1 \\ y_3 =& m(x_1 - x_3) - y_1 \\ m =& \frac{3x_1^2 + 2ax_1}{2y_1} \\ =& \frac{2ax_1}{2y_1} \quad \text{since } Char(F) = 3 \end{aligned}$$

5. If $P_1 = P_2$ and $y_1 = 0$, then $2P_1 = P_1 + P_2 = \infty$

The Group Of Points On An Elliptic Curve Over Fields Of Characteristic 3:

Example 4:. Let $E = \{(x, y) \in \mathbb{Z}_3 \times \mathbb{Z}_3 | y^2 = x^3 - x + 2\} \cup \{\infty\}$
We have seen that E has only one point, namely the point at infinity ∞. Hence $E = \{\infty\}$, and therefore $E \cong C_1$

Example 5: Let $E = \{(x, y) \in \mathbb{Z}_3 \times \mathbb{Z}_3 | y^2 = x^3 - x^2 + 2\} \cup \{\infty\}$
We have computed all points of E, and found that $E\{(2, 0), \infty\}$. Also, note that if $P_1(x_1, y_1) = (2, 0)$, then $2P_1 = \infty$. Hence $E \cong C_2$.

Example 6: Let $E = \{(x, y) \in \mathbb{F}_9 \times \mathbb{F}_9 : \ y^2 = x^3 - x + 2\} \cup \{\infty\}$, where

$$\begin{aligned}\mathbb{F}_9 &= \{0, \xi^i : \ 1 \leq i \leq 8; \ \xi^2 + \xi + 2 = 0\} \\ &= \{0, \xi, \ \xi^2 = 1 + 2\xi, \ \xi^3 = 2 + 2\xi, \ \xi^4 = -1 = 2, \ \xi^5 = 2\xi, \ \xi^6 = 2 + \xi, \ \xi^7 = 1 + \xi, \ \xi^8 = 1\}\end{aligned}$$

We have computed all the points of the points of the curve E, we have seen that:

$$E := \{(0, 1 + 2\xi), (0, 2 + \xi), (2, 1 + 2\xi), (2, 2 + \xi), (1, 1 + 2\xi), (1, 2 + \xi), \infty\}.$$

Let $P(0, 1 + 2\xi)$ and $x_1 = 0$, $y_1 = 1 + 2\xi$ then $2P(x_1, y_1) = P_3(x_3, y_3)$, where

$$\begin{aligned}x_3 =& m^2 - 2x_1, \\ y_3 =& m(x_1 - x_3) - y_1 \\ m =& \frac{3x_1^2 + a}{2y_1} = \frac{a}{2y_1}\end{aligned}$$

Here $a = -1 = 2 \in F$, Also $a = \xi^4$, as ξ is a primitive 8-th root of unity over $\mathbb{F}_3 \cong \mathbb{Z}_3$. Now

$$\begin{aligned}& m = \frac{2}{2 \cdot (1 + 2\xi)} = \frac{1}{1 + 2\xi} = \frac{1}{\xi^2} = \xi^{-1} = \xi^6 \\ \implies \quad & m = 2 + \xi\end{aligned}$$

$$\begin{aligned} x_3 =& m^2 - 2x_1 = (2+\xi)^2 - 2 \cdot 0 = (2+\xi)^2 \\ =& (\xi - 1)^2 = \xi^2 - 2\xi + 1 = \xi^2 + \xi + 1 \\ =& (1 + 2\xi) + \xi + 1 = 2 + 3\xi = 2 = -1 = \xi^4 \end{aligned}$$

$$\begin{aligned} y_3 =& m(x_1 - x_3) - y_1 \\ =& (2+\xi)(0-2) - (1+2\xi) \\ =& (2+\xi) \cdot 1 - 1 - 2\xi \\ =& 2 + \xi - 1 + \xi = 1 + 2\xi = 1 - \xi = \xi^2 \end{aligned}$$

Hence $2P_1 = 2(0, 1+2\xi) = (2, 1+2\xi)$
Next, we calculate $3P_1$ as $P_1 + 2P_1$.
Let $P_2(x_2, y_2) = 2P_1$, have the coordinates $x_2 = 2, y_2 = 1 + 2\xi$. Also recall $x_1 = 0$, $y_1 = 1 + 2\xi$.
Suppose $P_3(x_3', y_3') = P_1 + P_2$, then

$$\begin{aligned} x_3' =& m^2 - x_1 - x_2, \\ y_3' =& m(x_1 - x_3') - y_1 \\ m =& \frac{y_2 - y_1}{x_2 - x_1} \end{aligned}$$

$$\begin{aligned} m =& \frac{y_2 - y_1}{x_2 - x_1} = \frac{(1+2\xi) - ()1+2\xi)}{2-0} = 0 \\ x_3' =& m^2 - x_1 - x_2 = 0^2 - 0 - 2 = -2 = 1 \\ y_3' =& m(x_1 - x_3') - y_1 = -y_1 = -(1+2\xi) = (2+\xi) \end{aligned}$$

Hence $3P_1 = (x_3', y_3') = (1, 2+\xi)$
We now calculate $4P_1$ as $(2P_1) + (2P_1)$.
Recall $2P_1 = (2, 1+2\xi) = (x_1'', y_1'')$(say) then $4P_1 = (x_3'', y_3'')$,
where

$$\begin{aligned} x_3'' =& m^2 - 2x_1'', \\ y_3'' =& m(x_1'' - x_3'') - y_1'' \\ m =& \frac{3(x_1'')^2 + a}{2y_1''} = \frac{a}{2y_1''} \end{aligned}$$

Thus

$$m = \frac{-1}{2 \cdot (1+2\xi)} = 2 + \xi$$

and

$$m^2 = -1 = 2$$

Now

$$x_3'' = m^2 - 2x_1'' = 2 - 2 \cdot 2 = 2 - 4 = -2 = 1$$

$$\begin{aligned} y_3'' =& m(x_1'' - x_3'') - y_1'' \\ =& (2+\xi)(2-1) - (1+2\xi) \\ =& (2+\xi) - (1+2\xi) \\ =& 1 - \xi = 1 + 2\xi \end{aligned}$$

Hence $4P_1 = (1, 1+2\xi)$
Similarly calculate $5P_1, 6P_1, 7P_1$. You may also note that

$$7P_1 = 3P_1 + 4P_1 = (1, 2+\xi) + (1, 1+2\xi) = \infty$$

Since $\#(E) = 7$. Therefore

$$E = \langle P_1 | 7P_1 = \infty \rangle \cong C_7$$

Example 7: Let $E = \{(x, y) \in \mathbb{F}_9 \times \mathbb{F}_9 : \ y^2 = x^3 - x^2 + 2\} \cup \{\infty\}$

$$\begin{aligned} \mathbb{F}_9 &= \{0, \xi^i : \ 1 \leq i \leq 8; \ \xi^2 + \xi + 2 = 0\} \\ &= \{0, \xi, \ \xi^2 = 1 + 2\xi, \ \xi^3 = 2 + 2\xi, \ \xi^4 = -1 = 2, \ \xi^5 = 2\xi, \ \xi^6 = 1 + \xi, \ \xi^7 = 1 + \xi, \ \xi^8 = 1\} \end{aligned}$$

We compute points of E as follows:

$$\begin{aligned} E =& \{(0, 1+2\xi), (0, 2+\xi), (\xi, 0), (1+2\xi, 2+2\xi), (1+2\xi, 1+\xi), (2+2\xi, 0), (2, 0), \\ & (2+\xi, \xi), (2+\xi, 2\xi), (1, 1+2\xi), (1, 2+\xi)\} \cup \{\infty\} \end{aligned}$$

Now calculate integer multiplication of the point $P_1(0, 1+2\xi)$ as follows:
Let $x_1 = 0, \ y_1 = 1 + 2\xi$ then $2P_1 = P_3(x_3, y_3)$
where

$$\begin{aligned} x_3 &= m^2 - a - 2x_1, \\ y_3 &= m(x_1 - x_3) - y_1 \\ m &= \frac{3x_1^2 + 2ax_1}{2y_1} = \frac{2ax_1}{2y_1} \end{aligned}$$

Observing $a = -1 = 2 \pmod 3$, $x_1 = 0,\ y_1 = 1 + 2\xi$, we get

$$m = \frac{2 \cdot 2 \cdot 0}{2 \cdot (1 + 2\xi)} = 0$$

$$x_3 = -a - 2x_1 = 1 + x_1 = 1$$

$$y_3 = m(x_1 - x_3) - y_1 = -y_1 = -(1 + 2\xi) = 2 + \xi$$

Hence $(2P_1)(x_1, y_3) = (1, 2 + \xi)$
next, we compute $3P_1$ by doing $P_1 + 2P_1$
Let $P_1 = (x_1, y_1), 2P_1 = (x_2, y_2)$ where $x_1 = 0, y_1 = 1 + 2\xi, x_2 = 1, y_2 = 2 + \xi$ then

$$\begin{aligned} x_3' =& m^2 - a - x_1 - x_2, \\ y_3' =& m'(x_1 - x_3') - y_1 \\ m' =& \frac{y_2 - y_1}{x_2 - x_1} = \frac{(2 + \xi) - (1 + 2\xi)}{1 - 0} = 1 - \xi = 1 + 2\xi = \xi^2 \\ (m')^2 =& \xi^4 = -1 = 2 \end{aligned}$$

This gives

$$\begin{aligned} x_3' =& 2 - 2 - 0 - 1 = 2 \\ y_3' =& m'(x_1 - x_3) - y_1 \\ =& (1 + 2\xi)(0 - 2) - (1 + 2\xi) \\ =& (1 + 2\xi) - (1 + 2\xi) = 0 \end{aligned}$$

Hence we get $3P_1 = (2, 0)$ this implies that $6P_1 = \infty$
Therefore $K = \langle P_1 | 6P_1 = \infty \rangle \leq E$ of order 6.
Compute $4P_1$ and $5P_1$ also and write all elements of K.
Let $(\xi, 0) = Q_1$. Then $H = \langle Q_1 | 2Q_1 = \infty \rangle \leq E$ is a subgroup of order 2.
Is $E \cong H \oplus K$?
Is $E = \langle (2 + 2\xi, 0) \rangle \oplus \langle (0, 2 + \xi) \rangle$?
Is $E \cong C_2 \times C_6$?
Write all possible combinations?

Example 8: Let

$$\begin{aligned} E &= \{(x, y) \in \mathbb{F}_9 \times \mathbb{F}_9 | y^2 = x^3 + x^2 + x + 1\} \cup \{\infty\} \\ &= \{(x, y) \in \mathbb{F}_9 \times \mathbb{F}_9 | g(x, y) = 0 \quad \text{where } g(x, y) = y^2 - x^3 - x^2 - x - 2\} \cup \{\infty\} \end{aligned}$$

$\mathbb{F}_9 = \{0, \xi^i : \ 1 \leq i \leq 8; \ \xi^2 + \xi + 2 = 0\}$
$= \{0, \xi, \ \xi^2 = 1 + 2\xi, \ \xi^3 = 2 + 2\xi, \ \xi^4 = -1 = 2, \ \xi^5 = 2\xi, \ \xi^6 = 1 + \xi, \ \xi^7 = 1 + \xi, \ \xi^8 = 1\}$

$$\frac{\partial g}{\partial x} = 3x^2 + 2x + 1 = 0 \implies x = 1$$
$$\frac{\partial g}{\partial y} = 2y = 0 \implies y = 0$$

So, possible singular point is $(1, 0)$. But $(1, 0)$ is not a point on the curve E.
Hence, the curve is non-singular. Now we compute points on E.
Some points are easily noticeable on E.
For example
$(0, 1) \in E$. Hence $(0, -1) = (0, 2) \in E$
$(1, 1) \in E$. Hence $(1, 2) \in E$. Also $(2, 0) \in E$
It is better to calculate all the points of E by taking $x, y \in F_9$ and verifying g if $(x, y) \in E$.

x	$y^2 = x^3 + x^2 + x + 1$	y^2	y^2	y
0	1	1	1	1,2
ξ	$\xi^3 + \xi^2 + \xi + 1$	$\xi^3 - 1 = 1 + 2\xi$	ξ^2	$\xi, 2\xi$
$\xi^2 = 1 + 2\xi$	$\xi^6 + \xi^4 + \xi^2 + 1$	$\xi^6 + \xi^2$	0	0
$\xi^3 = 2 + 2\xi$	$\xi^9 + \xi^6 + \xi^3 + 1$	$2 + \xi$	ξ^6	$2 + 2\xi, 1 + \xi$
$\xi^4 = -1 = 2$	$(-1)^3 + (-1)^2 + (-1) + 1$	0	0	0
$\xi^5 = 2\xi$	$(2\xi)^3 + (2\xi)^2 + (2\xi) + 1$	(2ξ)	ξ^5	-
$\xi^6 = 2 + \xi$	$\xi^{18} + \xi^{12} + \xi^6 + 1$	$\xi^2 + \xi^4 + \xi^6 + 1$	0	0
$\xi^7 = 1 + \xi$	$\xi^{21} + \xi^{14} + \xi^7 + 1$	$\xi^5 + \xi^6 + \xi^7 + 1$	$1 + \xi = \xi^7$	-
$\xi^8 = 1$	1	1	1	1,2

We can see that E has 12 points in all.
Points of E are

$$\begin{aligned} E =&\{(0,1),(0,2),(\xi,\xi),(\xi,2\xi),(1+2\xi,0),(2+2\xi,2+2\xi),(2+2\xi,1+\xi),\\ &(2,0),(2+\xi,0),(1,1),(1,2),\infty\} \end{aligned}$$

Points of order 2 are $(1+2\xi,0),(2,0),(2+\xi,0)$. We now compute the subgroup generated by $P_1=(0,1)$.
Observe that $2P_1=(0,2)$
For let $P_1=(0,1), x_1=0, y_1=1$ and $2P_1=(x_3,y_3)$ then

$$\begin{aligned} x_3 =& m^2-a-2x_1,\\ y_3 =& m(x_1-x_3)-y_1\\ m =& \frac{3x_1^2+2ax_1+b}{2y_1}=\frac{2ax_1+b}{2y_1} \end{aligned}$$

using $a=b=1,\quad x_1=0, y_1=1$, we get

$$m=\frac{2\cdot 1\cdot 0+1}{2\cdot 1}=\frac{1}{2}=2 \implies m^2=1$$

$$x_3=1-1-2\cdot 0=0$$

$$y_3=1\cdot(0-0)-1=-1=2$$

Hence $2P_1=(x_3,y_3)=(0,2)=(0,-1)$.
Next we compute $3P_1$ as follows, by doing P_1+2P_1.
Let $3P_1=(x_3',y_3')$. Suppose $2P_1=(x_2,y_2)=(0,2)$ and $P_1=(x_1,y_1)=(0,1)$
Since $x_1=x_2=0$ this implies that $3P_1=\infty$.
Hence $(0,1)$ is a point of order 3 on E.
Let $Q_1=(1,1)=(x_1,y_1)$, and $2Q_1=(x_3,y_3)$, then

$$\begin{aligned} x_3 =& m^2-a-2x_1,\\ y_3 =& m(x_1-x_3)-y_1\\ m =& \frac{3x_1^2+2ax_1+b}{2y_1}=\frac{2ax_1+b}{2y_1} \end{aligned}$$

Using $a=1, x_1=1, y_1=1$, we get

$$m=\frac{2\cdot 1\cdot 1+1}{2\cdot 1}=\frac{3}{2}=0$$

$$x_3 = 0^2 - 1 - 2 \cdot 1 = -3 = 0$$

$$y_3 = 0 \cdot (1 - 0) - 1 = 0 - 1 = 2$$

This implies that $2Q_1 = (x_3, y_3) = (0, 2)$
Note that $2P_1 = 2Q_1 = (0, 2)$
We compute $3Q_1 = (x_3'', y_3'') = Q_1 + 2Q_1 = (1, 1) + (0, 2)$. Then

$$\begin{aligned} x_3'' &= m^2 - a - x_1 - x_2, \\ y_3'' &= m(x_1 - x_3'') - y_1 \\ m &= \frac{y_2 - y_1}{x_2 - x_1} \end{aligned}$$

Using $a = 1, x_1 = 1, y_1 = 1, x_2 = 0, y_2 = 2$, we get

$$m = \frac{2-1}{0-1} = \frac{1}{-1} = \frac{1}{1} = 2 \implies m^2 = 1$$

$$x_3'' = 1 - 1 - 1 - 0 = -1 = 2$$

$$y_3'' = 1 \cdot (1 - 0) - 1 = 0$$

Hence $3Q_1 = (2, 0)$ this implies that $6Q_1 = \infty$.
Therefore $K = \langle Q_1 | 6Q_1 = \infty \rangle$.
Compute all elements of K.
If $H = \langle (1 + 2\xi, 0) \rangle$, then $H \leq E$ is a subgroup of order 2.
Is $E = H \oplus K$?
Write E as a direct sum of all possible subgroups of E. Is $E \cong C_2 \times C_6$.

Groups Of Elliptic Curve over fields of characteristic 2

Rules of point addition and duplication
There are two normal forms of Elliptic curves over fields of characteristic 2 as follows :

1. $E_1 = \{(x, y) \in \mathbb{F} \times \mathbb{F} | y^2 + cy = x^3 + ax + b; \quad a, b, c \in \mathbb{F} \quad \} \cup \{\infty\}$
2. $E_2 = \{(x, y) \in \mathbb{F} \times \mathbb{F} | y^2 + xy = x^3 + ax^2 + b; \quad a, b \in \mathbb{F} \quad \} \cup \{\infty\}$

We now state rules of addition of points on these curves
First for E_1:

1. $P + \infty = \infty + P = P \quad \forall P \in E_1$ (including $\infty + \infty = \infty$).
2. If $P_1(x_1, y_1), P_2(x_2, y_2) \neq \infty$ and $P_1 \neq P_2$ with $x_1 \neq x_2$, then $P_1 + P_2 = P_3(x_3, y_3)$ Where

$$x_3 = m^2 - x_1 - x_2 = m^2 + x_1 + x_2,$$

$$y_3 = m(x_1 - x_3) - y_1 - c = m(x_1 + x_3) + y_1 + c$$

   where $m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{y_2 + y_1}{x_2 + x_1}$ since $char(\mathbb{F}) = 2$
3. If $P_1(x_1, y_1), P_2(x_2, y_2) \neq \infty$ and $P_1 \neq P_2$ with $x_1 = x_2$, but $y_1 \neq y_2$ then $P_1 + P_2 = \infty$
4. If $P_1(x_1, y_1), P_2(x_2, y_2) \neq \infty$ and $P_1 = P_2$ then $2P_1 = P_1 + P_2 = P_3(x_3, y_3)$ Where

$$x_3 = m^2 - 2x_1 = m^2, \quad \because char(\mathbb{F}) = 2$$

$$y_3 = m(x_1 - x_3) - y_1 - c = m(x_1 + x_3) + y_1 + c$$

   as $char(\mathbb{F}) = 2$ where $m = \frac{x^2 + a}{c}$ [If $c = 0$ then $2P_1 = \infty$]

Theorem: E_1 is an additive Abelian group with respect to (point) addition (defined as above).

Rules of point addition on the curve $E_2(\mathbb{F}); Char(\mathbb{F}) = 2$:

$$E_2 = \{(x, y) \in \mathbb{F} \times \mathbb{F} | y^2 + xy = x^3 + ax^2 + b; \quad a, b \in \mathbb{F} \quad \} \cup \{\infty\}$$

1. $P + \infty = \infty + P = P \quad \forall P \in E_2$ (including $\infty + \infty = \infty$).
2. If $P_1(x_1, y_1), P_2(x_2, y_2) \neq \infty$ and $P_1 \neq P_2$ with $x_1 \neq x_2$, then $P_1 + P_2 = P_3(x_3, y_3)$ Where

$$x_3 = m^2 + m + a + x_1 + x_2,$$

$$y_3 = m(x_1 + x_3) + y_1 + x_3$$

   where $m = \frac{y_2 + y_1}{x_2 + x_1}$ $[\because char(\mathbb{F}) = 2]$

3. If $P_1(x_1, y_1), P_2(x_2, y_2) \neq \infty$ and $P_1 \neq P_2$ with $x_1 = x_2$, but $y_1 \neq y_2$ then $P_1 + P_2 = \infty$

4. If $P_1(x_1, y_1), P_2(x_2, y_2) \neq \infty$ and $P_1 = P_2$ with $x_1 \neq 0$ then $2P_1 = P_1 + P_2 = P_3(x_3, y_3)$ Where

$$x_3 = x_1^2 + \frac{b}{x_1^2},\ y_3 = \frac{x_1^2 + y_1}{x_1} x_3 + x_1^2 + x_3$$

[If $x_1 = 0$ then $2P_1 = \infty$]

Theorem: The points on the curve E_2 form an additive Abelian group.

Example 9: Let $E = \{(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_2 :\ y^2 + y = x^3 + x\} \cup \{\infty\}$.
We have seen that :

$$E = \{(0,0), (0,1), (1,0), (1,1), \infty\}$$

$\#(E) = 5$
Let $P = (0,0) = (x_1, y_1) \implies x_1 = 0, y_1 = 0$, suppose $2P = (x_3, y_3)$, where

$$x_3 = m^2, \quad y_3 = m(x_1 + x_3) + y_1 + c \text{ where } m = \frac{x_1^2 + a}{c}$$

i.e.

$$x_3 = \left(\frac{x_1^2 + a}{c}\right)^2, \quad y_3 = \frac{x_1^2 + a}{c}(x_1 + x_3) + y_1 + c$$

For this curve $y^2 + y = x^3 + x$, $c = 1, a = 1, b = 0$ and $x_1 = 0, y_1 = 0$ we get:

$$x_3 = \left(\frac{0^2 + 1}{1}\right)^2 = 1, \quad y_3 = \frac{0^2 + 1}{1}(0 + 1) + 0 + 1 = 1 \cdot 1 + 1 = 2 = 0$$

$\implies (x_3, y_3) = (1, 0)$. Hence $2P = (1, 0)$
We next, compute $3P = P + 2P = (0, 0) + (1, 0)$
Let $x_1 = 0, y_1 = 0, x_2 = 1, y_2 = 0$ then $3P = (x_3', y_3')$ where

$$x_3' = m^2 + x_1 + x_2, \quad y_3' = m(x_1 + x_3) + y_1 + c \text{ where } m = \frac{y_1 + y_2}{x_1 + x_2}$$

Here

$$m = \frac{0 + 0}{0 + 1} = 0 \implies x_3' = x_1 + x_2 = 0 + 1 = 1$$

and

$$y_3' = y_1 + c = 0 + c = c = 1$$

Hence $3P = (x_3', y_3') = (1, 1)$.
We now compute $4P$ as $2P + 2P$ i.e. $4P = (x_2, y_2) + (x_2, y_2), x_2 = 1, y_2 = 0$
Let $4P = (x_2, y_2) + (x_2, y_2) = (x_3'', y_3'')$,
then

$$x_3'' = \left(\frac{x_2^2 + a}{c}\right)^2 = \left(\frac{1^2 + 1}{1}\right)^2 = \frac{2^2}{1} = 0$$

$$y_3'' = \frac{x_2^2 + a}{c}(x_2 + x_3) + y_2 + c = 0(1 + 0) + 0 + c = c = 1$$

$\implies 4P = (x_3'', y_3'') = (0, 1)$
Finally, we compute $6P$ as $6P = 3P + 3P$.
Let $3P = (1, 1) = (u, v)$ with $u = 1, v = 1$
If $6P = (x_5, y_5)$ then

$$x_5 = \left(\frac{u^2 + a}{c}\right)^2 = \left(\frac{1^2 + 1}{1}\right)^2 = \left(\frac{2}{1}\right)^2 = 0$$

$$y_5 = \frac{u^2 + a}{c}(u + x_5) + v + c = 0(u + x_5) + v + c = v + c = 1 + 1 = 0$$

$\implies 6P = (x_5, y_5) = (0, 0) = P \implies 5P = \infty$
This can be obtained by observing that

$$2P + 3P = (1, 0) + (1, 1) = \infty$$

Hence

$$\begin{aligned} E =& \langle P : \ 5P = \infty \rangle \\ =& \{P = (0, 0), 2P = (1, 0), 3P = (1, 1), 4P = (0, 1), 5P = \infty\} \\ \cong& C_5 \end{aligned}$$

Example 10: Let $E = \{(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_2 : \ y^2 + xy = x^3 + 1\} \cup \{\infty\}$.
We have computed all the points on E, and observe that

$$E = \{(0, 1), (1, 0), (1, 1), \infty\}$$

$\#(E) = 4$
Now let $P = (0, 1)$, then $2P = \infty$.
Next if $Q = (1, 0)$, then $2Q = (x_3, y_3)$, where

$$x_3 = x_1^2 + \frac{b}{x_1^2}, \quad y_3 = \frac{x_1^2 + y_1}{x_1} x_3 + x_1^2 + x_3$$

where $x_1 = 1, y_1 = 0, a = 0, b = 1$ implies that

$$x_3 = 1^2 + \frac{1}{1} = 1 + 1 = 0,$$

$$y_3 = \frac{1^2 + 0}{1} \cdot 0 + 1^2 + 0 = 1$$

$$\implies 2Q = (0, 1) = P \implies 4Q = 2Q + 2Q = P + P = 2P = \infty.$$

Hence $E = \langle Q : \ 4Q = \infty \rangle = \langle (1, 0) : \ 4(1, 0) = \infty \rangle \cong C_4$

Example 11: Let $E = \{(x, y) \in \mathbb{F}_4 \times \mathbb{F}_4 |\ y^2 + y = x^3 + 3\} \cup \{\infty\}$, where

$$\begin{aligned} \mathbb{F}_4 =& \{0, \omega^i |\ 1 \leq i \leq 3;\ \omega^3 = 1, \omega \neq 1\} \\ =& \{0, 1, \omega, \omega^2 |\ w^2 + w + 1 = 0\} \\ =& \{0, 1, \omega, 1 + \omega\} \end{aligned}$$

We have computed all the points of E, and observe that:

$$E = \{(0, 0), (0, 1), (1, 0), (1, 1)\} \cup \{\infty\}$$

$\#(E) = 5$. We determine the subgroup generated by the point $P(0, 0) \in E$, as follows.
Let $x_1 = 0, y_1 = 0 \implies P(0, 0) = (x_1, y_1)$
$2P = (x_2, y_2)$, then

$$x_2 = \left(\frac{x_1^2 + a}{c} \right)^2, \quad y_2 = \frac{x_1^2 + a}{c} (x_1 + x_2) + y_1 + c$$

Here $a = 1, c = 1$.
We get $x_2 = \left(\frac{0^2 + 1}{1} \right)^2 = 1^2 = 1, \quad y_2 = 1(0 + 1) + 0 + 1 = 2 + 0 = 0$
$\implies (x_2, y_2) = 2P = (1, 0)$

Let $3P = (x_3, y_3) = P + 2P = (x_1, y_1) + (x_2, y_2)$ where
$x_1 = 0, y_1 = 0, x_2 = 1, y_2 = 0$, We have

$$x_3 = m^2 + x_1 + x_2, \quad y_3 = m(x_1 + x_3) + y_1 + c$$

where

$$m = \frac{y_1 + y_2}{x_1 + x_2} = \frac{0+0}{0+1} = \frac{0}{1} = 0$$

This gives $x_3 = 0^2 + 0 + 1 = 1$ and $y_3 = 0 \cdot (0+1) + 0 + 1 = 1 \ \ [\because c = 1]$
Hence $3P = (x_3, y_3) = (1, 1)$.

Next, let $4P = 2P + 2P = (1,0) + (1,0) = (x_2, y_2) + (x_2, y_2)$ have coordinates $4P = (x_4, y_4)$. Then

$$x_4 = \left(\frac{x_2^2 + a}{c}\right)^2 = m^2 = \left(\frac{1^2+1}{1}\right)^2 = \frac{2^2}{1} = 0 \ \ [\text{ as } a = 1, \ c = 1]$$

$$y_4 = m \cdot (x_2 + x_4) + y_2 + c = 0(1+0) + 0 + 1 = 1$$

Hence $4P = (x_4, y_4) = (0, 1)$.

We now calculate $6P = 3P + 3P = (1,1) + (1,1)$
Let $6P = (x_6, y_6) = (x_3, y_3) + (x_3, y_3)$ where $x_3 = 1, y_3 = 1$

$$x_6 = \left(\frac{x_3^2 + a}{c}\right)^2 = m^2 = \left(\frac{1^2+1}{1}\right)^2 = \frac{2^2}{1} = 0 \text{ i.e. } \ m = 0$$

$$y_6 = m \cdot (x_3 + x_6) + y_3 + c = 0(1+0) + 1 + 1 = 0$$

$\implies 6P = (0,0) = P \implies 5P = \infty$
Hence

$$\begin{aligned} E =& \langle P \rangle = \langle P : \ 5P = \infty \rangle \\ =& \{P = (0,0), 2P = (1,0), 3P = (1,1), 4P = (0,1), 5P = \infty\} \\ \cong& C_5 \end{aligned}$$

Example 12: Let $E = \{(x, y) \in \mathbb{F}_4 \times \mathbb{F}_4 |\ y^2 + xy = x^3 + 1\} \cup \{\infty\}$, where

$$\begin{aligned} \mathbb{F}_4 =& \{0, \omega^i |\ 1 \le i \le 3; \ \omega^3 = 1, \omega \neq 1\} \\ =& \{0, 1, \omega, \omega^2 |\ w^2 + w + 1 = 0\} \\ =& \{0, 1, \omega, 1 + \omega\} \end{aligned}$$

We have computed all the points of E. We found that E has eight points in all.

$$E = \{(0,1),(1,0),(1,1),(\omega,0),(\omega,\omega),(\omega^2,0),(\omega^2,\omega^2),\infty\}$$

or

$$E = \{(0,1),(1,0),(1,1),(\omega,0),(\omega,\omega),(1+\omega,0),(1+\omega,1+\omega),\infty\}$$

Prove that $Q = (0,1)$ is a point in E of order 2.
We compute multiples of $P = (\omega, 0) = (x, y)$ as follows:
Let $2P = (x_2, y_2)$, then

$$x_2 = x_1^2 + \frac{c}{x_1^2} = \omega^2 + \frac{1}{\omega^2} = \omega^2 + \omega = 1$$

$$y_2 = \frac{x_1^2 + y_1}{x_1} x_2 + x_1^2 + x_2 = \frac{\omega^2 + 0}{\omega} \cdot 1 + \omega^2 + 1$$

$$\implies y_2 = \omega + \omega^2 + 1 = 0$$

$\implies 2P = (x_2, y_2) = (1, 0)$
We next compute $4P = 2P + 2P = (x_2, y_2) + (x_2, y_2) = (1, 0) + (1, 0)$.
Let $4P = (x_4, y_4)$. Then

$$x_4 = x_2^2 + \frac{a}{x_2^2} = 1^2 + \frac{1}{1^2} = 1 + 1 = 0$$

$$y_4 = \frac{x_2^2 + y_2}{x_2} x_4 + x_2^2 + x_4 = \frac{1^2 + 0}{1} \cdot 0 + 1^2 + 0 = 1$$

$$\implies (x_4, y_4) = (0, 1) \text{ or } 4P = (0, 1) = Q$$

But Q is of order 2. Hence $8P = 2Q = \infty$
Hence $E = \langle P \rangle = \langle P : \ 8P = \infty \rangle \cong C_8$

Write all multiples kP $(k = 1, 2, 3, 4, 5, 6, 7, 8)$. In fact, you have to compute $3P, 5P$ and $7P$ only.

Leture-18

Application Of Elliptic Curves: Factorization Of Integers

We have studied several algorithm for integer factorization, earlier. We now see how Elliptic Curves can be used for this purpose. We begin with an example.

Example 1. Let $n = 589$, and

$$E := \{(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n | y^2 = x^3 + 4x + 9\} \cup \{\infty\}$$

If $P_1 = (x_1, y_1) = (2, 5)$, then $2^3 + 4 \times 2 + 9 = 25 = (\pm 5)^2$ implies that $P_1 \in E$ (and also $(2, -5)$ *i.e.* $(2, 584) \in E$.)
We compute integer multiples of P_1 as follows:
Let $2P_1 = P_2(x_2, y_2)$. Then

$$\begin{aligned} x_2 =& m^2 - 2x_1 \\ y_2 =& m(x_1 - x_2) - y_1 \\ m =& \frac{3x_1^2 + a}{2y_1} \end{aligned}$$

Since $x_1 = 2,\ y_1 = 5$ and $a = 4$, we get

$$m = \frac{3 \cdot 2^2 + 4}{2 \cdot 5} = \frac{16}{10} \implies m = 16 \times 10^{-1} \pmod{589}$$

As 10 and 589 are relatively prime, 10^{-1} can be computed, using division algorithm. we find that

$$10^{-1} \equiv 59 \implies m \equiv 16 \times 59 \equiv 944 \equiv 355 \pmod{589}.$$

Hence

$$x_2 = m^2 - 2x_1 = (355)^2 - 2 \cdot 2 = 126025 - 4 = 126021 \equiv 564 \pmod{589}$$

$$y_2 = m(x_1 - x_2) - y_1 = 355(2 - 564) - 5 = -199515 \equiv 156 \pmod{589}$$

This gives that

$$2P_1 = P_2(x_2, y_2) = (564, 156)$$

Let $3P_1 = P_3(x_3, y_3)$ then

$$\begin{aligned} x_3 =& m^2 - x_1 - x_2 \\ y_3 =& m(x_1 - x_3) - y_1 \\ m =& \frac{y_2 - y_1}{x_2 - x_1} \end{aligned}$$

Since $x_1 = 2, y_1 = 5, x_2 = 564, y_2 = 156$, we get

$$\begin{aligned} m =& \frac{156 - 5}{564 - 2} = \frac{151}{562} = 151 \times 562^{-1} \equiv 151 \times 349 \equiv 52699 \equiv 278 \pmod{589} \\ x_3 =& m^2 - x_1 - x_2 = 278^2 - 2 - 564 = 76718 = 148 \pmod{589} \\ y_3 =& m(x_1 - x_3) - y_1 = 278(2 - 148) - 5 = -40593 \equiv 48 \pmod{589} \end{aligned}$$

This gives $P_3 = 3P_1(x_3, y_3) = (148, 48)$
Next, let $P_4(x_4, y_4) = P_2 + P_2 = (564, 156) + (564, 156)$ then

$$\begin{aligned} x_4 =& m^2 - 2x_2 \\ y_4 =& m(x_2 - x_4) - y_2 \\ m =& \frac{3x_2^2 + a}{2y_2} \end{aligned}$$

Since $x_2 = 564, y_2 = 156, a = 4$, we get

$$\begin{aligned} & m = \frac{3 \cdot 564^2 + 4}{2 \cdot 156} = \frac{954292}{312} \\ \implies & m = \frac{112}{312} \equiv 112 \times 312^{-1} \equiv 112 \times 202 \equiv 22624 \equiv 242 \pmod{589} \\ & x_4 = m^2 - 2x_2 = 242^2 - 2 \times 564 = 57436 = 303 \pmod{589} \\ & y_4 = m(x_2 - x_4) - y_2 = 242(564 - 303) - 156 = 63006 \equiv 572 \pmod{589} \end{aligned}$$

Hence $P_4(x_4, y_4) = (303, 572)$.
We now compute $7P$.
Let $P_7 = (x_7, y_7) = 7P = 3P + 4P = (148, 48) + (303, 572)$

$$\begin{aligned} x_7 =& m^2 - x_3 - x_4 \\ y_7 =& m(x_3 - x_7) - y_3 \\ m =& \frac{y_4 - y_3}{x_4 - x_3} \end{aligned}$$

Since $x_3 = 148, y_3 = 48, x_4 = 303, y_4 = 572$, we get

$$m = \frac{572 - 48}{303 - 148} = \frac{524}{155} = 524 \times 155^{-1} \pmod{589}$$

We compute the gcd, the greatest common divisor of 155 and 589. Using Euclidean Algorithm as follows:

$$\begin{aligned} 589 =& 3 \times 155 + 124 \\ 155 =& 1 \times 124 + 31 \\ 124 =& 4 \times 31 + 0 \end{aligned}$$

We get $\gcd(155, 589) = 31$ (as the least non zero divisor).
Since $d = \gcd(155, 589) > 1$, this implies that $155^{-1} \pmod{589}$, does not exist.
In fact $d|589$. We get 31 as a factor of 589. The other factor can be easily seen to be 19. Hence $589 = 31 \times 19$.

The Algorithm by Hendrik Lenstra using Elliptic Curves for integer factorization is based on the J. M. Pollard's $p - 1$, factorization algorithm. We recall the $(p - 1)$- algorithm.
First, the idea of Pollard's $(p - 1)$- algorithm:
Let m be a positive odd integer greater than 1 (to be factored). Define

$$d_n = \gcd(2^{n!} - 1, m),$$

the gcd of $2^{n!} - 1$ and m for every positive integer n.
Since

$$d_{n+1} = \gcd(2^{(n+1)!} - 1, m),$$

and

$$2^{(n+1)!} - 1 = (2^{n!})^{n+1} - 1 = k^{n+1} - 1 = (k - 1)(k^n + k^{n-1} + \cdots + k + 1),$$

where $k = 2^{n!}$, gives that $2^{n!} - 1 = k - 1$ is a factor of $2^{(n+1)!} - 1$.
Hence

$$d_n|(2^{n!} - 1) \implies d_n|(2^{(n+1)!} - 1) \implies d_n|d_{n+1}, \text{ as } d_n|m.$$

Thus $d_n|d_{n+1} \quad \forall n = 1, 2, \ldots$

Further, observed that if p is a prime which divides m, and is such that $p - 1$ divides $n!$, then $d_n > 1 \quad \forall n = 1, 2 \ldots$. We in this process get a proper divisor of m.
We apply this idea to $m = 403$. We compute the sequence d_n as follows:

$$\begin{aligned}
d_1 &= \gcd(2^{1!} - 1, 403) = \gcd(1, 403) = 1, \\
d_2 &= \gcd(2^{2!} - 1, 403) = \gcd(3, 403) = 1, \\
d_3 &= \gcd(2^{3!} - 1, 403) = \gcd(2^6 - 1, 403) = \gcd(63, 403) = 1, \\
d_4 &= \gcd(2^{4!} - 1, 403) = \gcd(2^{24} - 1, 403) = \gcd(16777215, 403) = 13 > 1
\end{aligned}$$

We get 13 as a proper divisor of 403. The other divisor of 403 is 31. We also observe that $n = 4$ is the least positive integer such that d_n gives a proper factor of 403.
We also compute/conclude that $n = 5$ is the least n such that $d_n = d_5 = 403$
Next, we apply this idea on $m = 589$. We compute the sequence d_n as follows:

$$\begin{aligned}
d_1 &= \gcd(2^{1!} - 1, 589) = \gcd(1, 589) = 1, \\
d_2 &= \gcd(2^{2!} - 1, 589) = \gcd(3, 589) = 1, \\
d_3 &= \gcd(2^{3!} - 1, 589) = \gcd(2^6 - 1, 589) = \gcd(63, 589) = 1, \\
d_4 &= \gcd(2^{4!} - 1, 589) = \gcd(2^{24} - 1, 589) = \gcd(16777215, 589) = 1
\end{aligned}$$

What is d_5?
What is the least n for which 589 gives a proper divisor?
What is the least n such that $d_n = 589$?

Observe that one of the major difficulty in the idea discussed is the growing size of $d_n = \gcd(2^{n!} - 1, m)$, as n increase. This can be overcome by observing that $\gcd(a, b) = \gcd(a + bx, b) \; \forall a, b, x \in \mathbb{Z}$. So if $2^{n!} - 1 \equiv b \pmod{m}$ i.e. $2^{n!} - 1 = qm + b \; (0 \leq b < m)$, then $\gcd(2^{n!} - 1, m) = \gcd(b + mq, m) = \gcd(b, m) \implies d_m = \gcd(b, m)$. Therefore, we need not calculate exact value

of $2^{n!}-1$ but need to know $b \equiv (2^{n!}-1) \pmod{m}$. Since $0 \leq b < m$, it reduces computations a lot. For example d_5 for $m = 403$, can be obtained as:

$$d_4 = \gcd(2^{4!}-1, 403) = \gcd(16677215, 403) = \gcd(325, 403) = 13$$

Next observe that

$$2^{5!}-1 = (2^{4!})^5 - 1 = (2^{4!}-1)\{1 + 2^{4!} + (2^{4!})^2 + (2^{4!})^3 + (2^{4!})^4\}$$

$$\begin{aligned} k = 2^{4!} = 2^{24} &= 16677216 \equiv 326 \pmod{403} \\ k^2 = 326^2 &\equiv 106276 \equiv 287 \pmod{403} \\ k^3 = 287 \times 326 &\equiv 93562 \equiv 66 \pmod{403} \\ k^4 = 66 \times 326 &= 21516 \equiv 157 \pmod{403} \end{aligned}$$

Hence

$$2^{5!}-1 \equiv (k-1)(k^4+k^3+k^2+k+1) \pmod{403}$$

where $k = 2^{4!} \equiv 326 \pmod{403}$, We get

$$2^{5!}-1 \equiv (326-1)(157+66+287+326+1) \equiv 0 \pmod{403}$$

This implies that $d_5 = \gcd(2^{5!}-1, 403) = \gcd(0, 403) = 403$

Remark. If $a = 3$, then $a^{3!} = 3^6 = 729 = 326 \pmod{403}$. Hence in this case $d_3 = \gcd(a^{3!}-1, 403) = \gcd(326, 403) = 13$ and $d_4 = 403$.

We generalize the idea little further. In d_n, instead of taking integer $2^{n!}-1$, we take $a^{n!}-1$, where a is an arbitrary positive integer greater then 1. Define the sequence $\{g_n\}$ as follows:

$$g_n = \gcd(a_n - 1, m)$$

where m is the positive integer asked to be factored, and the $a_n's$ are define as

$$a_n = a_{n-1}^{r_{n-1}}, \text{ with } a_1 = a \ \ \forall n \geq 2,$$

where $\{r_k\}$ is a sequence of positive integer greater than 1. Thus

$$\begin{aligned}
g_1 =& \gcd(a_1 - 1, m) = \gcd(a - 1, m),\\
g_2 =& \gcd(a_2 - 1, m) = \gcd(a_1^{r_1} - 1, m) = \gcd(a^{r_1} - 1, m),\\
g_3 =& \gcd(a_3 - 1, m) = \gcd(a_2^{r_2} - 1, m) = \gcd((a_1^{r_1})^{r_2} - 1, m) = \gcd(a^{r_1 r_2} - 1, m),\\
&\vdots\\
g_n =& \gcd(a_n - 1, m) = \gcd(a^{r_1 r_2 \cdots r_{n-1}} - 1, m) \quad \forall n \geq 2\\
g_{n+1} =& \gcd(a_{n+1} - 1, m) = \gcd(a_n^{r_n} - 1, m)
\end{aligned}$$

Now

$$\begin{aligned}
g_n = gcd(a_n - 1, m) &\implies g_n \mid a_n - 1 \text{ and}\\
g_n \mid m &\implies g_n \mid (a_n^{r_n} - 1) \quad \because (a_n - 1) \mid (a_n^{r_n} - 1)\\
&\implies g_n \mid g_{n+1} \quad \forall n \geq 1\\
&\text{That is} \quad g_1 \mid g_2,\ g_2 \mid g_3, \ldots
\end{aligned}$$

Thus, we wish to determine one n (least positive integer in fact) such that $1 \lneq g_n \lneq m$, as this makes g_n to be a proper factor of m.
For $r_n = n\ \forall n \in \mathbb{N}$ and $a = 2$,

$$\begin{aligned}
g_n =& gcd(a^{r_1 r_2 \cdots r_{n-1}} - 1, m)\\
=& gcd(2^{1 \cdot 2 \cdot 3 \cdots (n-1)} - 1, m)\\
=& gcd(2^{(n-1)!} - 1, m) = d_{n-1}
\end{aligned}$$

in our earlier discussion.
Next, suppose p is a prime such that $p \mid m$, and $(p-1) \mid r_1 r_2 \cdots r_{n-1}$ then

$$a_n = a^{r_1 r_2 \cdots r_{n-1}} = \left[a^{(p-1)}\right]^t \equiv 1 \pmod{p},$$

where $(p-1)t = r_1 r_2 \cdots r_{n-1} \implies p \mid a_n - 1$. Since $p \mid m$, we get $p \mid g_n$ and we get a proper factor of m.

Can there be a better choice for r_n other than n?

Let $\{q_n\}$ be a sequence of all the positive powers of all the primes arranged in the increasing manner. Suppose $\{r_n\}$ is the sequence of positive integers such that $r_n \mid q_n$ and r_n is a prime $\forall n \in \mathbb{N}$.

For example: Consider positive integers 1 to 100. The terms of the sequence $\{q_n\}$ are:

$$q_1 = 2^1, q_2 = 3^1, q_3 = 2^2, q_4 = 5^1, q_5 = 7^1, q_6 = 2^3, q_7 = 3^2, q_8 = 11^1, q_9 = 13^1, q_{10} = 17$$

The terms of the sequence r_n are:

$$r_1 = 2, r_2 = 3, r_3 = 2, r_4 = 5, r_5 = 7, r_6 = 2, r_7 = 3, r_8 = 11, r_9 = 13, r_{10} = 17$$

Observe that: lcm, the least common multiple of the numbers 1 to 100, i.e

$$[1, 2, 3, \ldots, 10] = lcm[q_1, q_2, \ldots q_7] = r_1, r_2, \cdots r_7.$$

Prove in general that: $lcm\,[1, 2, 3, \ldots q_n] = lcm\,[q_1, q_2, \ldots q_n] = r_1, r_2, \cdots r_n\ \forall n \in \mathbb{N}$.
Since $r_1 r_2 \cdots r_n \leq n!$, we expect less number of calculations. Obviously, Pollard's $(p-1)$- algorithm is most efficient, when $p-1$ has a large number of small prime factors.
We summarize the algorithm as follows:
Input: The integer m (to be factored)

1. Set a positive integer grater than 1. It can be 2 itself.
2. Loop $j = 2, 3, 4, \cdots$, up to specific bound $\mathcal{B}$
3. Set $a = a^j \pmod m$
4. Compute $d = gcd(a - 1, m)$
5. If $1 \lneq d \lneq m$, then return d as a prper factor of m.
6. If not increment j and loop again at step 2.

Note 1. Hopping can be done to increase efficiency by computing (in step 4) gcd only for every $k - th$ position, for some suitable k.
Thus

$$\begin{aligned} 2^{5!} - 1 =& 325(157 + 66 + 287 + 326 + 1) \\ =& 325 \times 837 = 272025 \\ \equiv& 0 \pmod{403} \quad \text{as } 272025 = 675 \times 403 \end{aligned}$$

$$\implies d_5 = gcd(2^{5!-1}, 403) = gcd(0, 403) = 403$$

Of course, you could also have argued as follows:
Since $d_4 < d_5, d_4 \mid d_5, d_5 \leq 403$, and $d_4 = 13$, we get $d_5 = 403$.
Do this for $m = 589$.
Compute d_{120} for $m = 3870573781$.

Remark 1: In calculating $2^{n!} - 1 \pmod m$, we can use that

$$a \equiv b \pmod m \implies a + c \equiv b + c \pmod m.$$

Thus if $2^{n!} \equiv r \pmod m$, then $2^{n!} - 1 \equiv r - 1 \pmod m$. Apply this in proving that

$$2^{4!} \equiv 326 \pmod{403} \implies 2^{4!} - 1 \equiv 326 - 1 \equiv 325 \pmod{403}.$$

To do this use the method of repeated squaring and multiplying if required. observe that

$$2^{4!} = \left(2^{3!}\right)^4 = (2^6)^4$$
$$\text{and that } 2^6 = 64 \implies (2^6)^2 = 64^2 = 4096 \equiv 66 \pmod{403}$$
$$\implies (2^6)^4 \equiv 66^2 \equiv 4356 \equiv 326 \pmod{403}$$

Similarly $2^{5!} = (2^{4!})^5 = \left((2^{4!})^2\right)^2 (2^{4!})$

Lenstra's Elliptic Curve Factorizaton Algorithm

Recall the Pollard's $(p-1)$ factorization algorithm of a positive integer $m > 1$. The crux of algorithm was a prime factor p of m such that $p - 1$, has small prime factors and $(p-1) \mid (a^{r_1 r_2 \cdots r_{n-1}})$ where r_i's are primes not exceeding a bound, at most the primes occurring in $n!$ $\forall n \in \mathbb{N}$. The condition $(p-1) \mid (a^{r_1 r_2 \cdots r_{n-1}})$ implies $a^{p-1} \equiv 1 \pmod p$. This happens in the multiplicative group $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$, that $\alpha^{p-1} \equiv 1 \pmod p$, for every $0 \neq \alpha \in \mathbb{F}_p$. Lenstra replaced the multiplicative group by the additive Abelian group of an Elliptic Curve modulo n, where n is the composite number to be factored.

Thus an Elliptic Curve $E := \{(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n |\ y^2 = x^3 + Ax + B;\ A, B \in \mathbb{Z}_n\} \cup \{\infty\}$ is searched and a point $P(a, b)$ on E is found. Multiples of P are computed till the computation fails. In that case, a proper factor is found.

otherwise, start with a new curve E and a new point P on E.

How to choose a curve E?
Start with a point $P(a, b)$, compute $B \equiv b^2 - a^3 - Aa \pmod{n}$ for randomly chosen A, a, b so that $B + Aa + a^3$ is a quadratic residue $\pmod{n}$.

The Algorithm (Lenstra):
Input: Integer n to be factored.

1. Choose random values A, a and $b \pmod{n}$
2. Set $P = (a, b)$ and $B \equiv b^2 - a^3 - Aa \pmod{n}$.
3. Loop $j = 2, 3, \ldots$ up to a specified bound
4. Compute $Q = jP \pmod{n}$ and set $P = Q$.
5. If computation in step 4 fails, there exist a proper factor d of n.
6. If $d < n$, then success, return d.
7. If $d = n$, go to step 1 and choose a new curve and a new point P on E.
8. Increment j and loop again at step 2.

Example: Factorize $n = 589$ using Lenstra's Elliptic Curve Algorithm.
Let $P = (2, 5)$ i.e. $a = 2, b = 5$ and $A = 4$ then

$$B = b^2 - a^3 - Aa \pmod{589} \equiv 5^2 - 2^3 - 4 \cdot 2 = 25 - 8 - 8 = 9 = 3^2 \pmod{589}.$$

Hence choose the curve

$$E := \{(x, y) \in \mathbb{Z}_{589} \times \mathbb{Z}_{589} |\, y^2 = x^3 + Ax + B;\ A, B \in \mathbb{Z}_{589}\} \cup \{\infty\};\ \ A = 4, B = 9$$

Then clearly $P(2, 5) \in E$. let $P = (x_1, y_1),\ x_1 = 2, y_1 = 5$
Recall:

$$\begin{aligned} 2P &= (x_2, y_2) = (564, 156), \quad \text{so} \\ (2!)P &= P_2 = (x_2, y_2) = (564, 156) \\ 3(2P) &= (3!)P = 6P = P_6(x_6, y_6) = 2P + 4P = (564, 156) + (303, 572) \end{aligned}$$

We have calculated $4P = (x_4, y_4) = 2P_2 = (303, 572)$

$$\begin{aligned}
x_6 =& m_6^2 - x_2 - x_4 \\
y_6 =& m_6(x_2 - x_6) - y_2 \text{ where} \\
m_6 =& \frac{y_4 - y_2}{x_4 - x_2} \\
=& \frac{572 - 156}{303 - 564} = \frac{416}{-261} \\
\implies m_6 =& \frac{416}{328} \equiv 416 \times 328^{-1} \pmod{589} \\
\equiv& 416 \times 422 \equiv 30 \pmod{589} \\
\implies m_6^2 \equiv& 900 \equiv 311 \pmod{589}. \\
\implies x_6 =& 900 - 564 - 303 \equiv 311 - 564 - 303 \\
\equiv& -556 \equiv 33 \pmod{589} \\
y_6 =& 311(564 - 33) - 572 = 311 \times 531 - 572 \\
=& 165141 - 572 = 164569 \equiv 238 \pmod{589}
\end{aligned}$$

Hence $(3!)P = 6P = P_6 = (x_6, y_6) = (33, 238)$.
Now $(4!)P = 4(3!)P = 4Q$ where $Q = P_6 = (33, 238)$
Now $Q_1 = (u_1, v_1) = (33, 238)$.
Let $2Q = Q_2 = (u_2, v_2)$. Then

$$u_2 = m_2^2 - u_1 - u_2, \ v_2 = m_2(u_1 - u_2) - v_1$$

where

$$\begin{aligned}
m_2 =& \frac{3u_1^2 + A}{2u_1} = \frac{3 \cdot 33^2 + 4}{2 \cdot 238} \\
=& \frac{3271}{476} \equiv 3271 \times 476^{-1} \pmod{589} \\
\implies m_2 =& 3271 \times 172 \equiv 562612 \equiv 117 \pmod{589} \\
\implies m_2^2 \equiv& 117^2 \equiv 13689 \equiv 142 \pmod{589} \\
\implies u_2 \equiv& 142 - 33 - 33 \equiv 142 - 66 \pmod{589} \equiv 76 \pmod{589} \\
v_2 \equiv& 117(33 - 76) - 238 \equiv 117 \times (-43) - 238 \pmod{589} \\
\equiv& -5269 \equiv 32 \pmod{589} \\
\implies 2Q =& Q_2 = (u_2, v_2) = (76, 32)
\end{aligned}$$

$$
\begin{aligned}
\implies 4Q =& Q_4 = 2Q + 2Q = Q_2 + Q_2 = (76, 32) + (76, 32) \\
\implies u_4 =& m_4^2 - 2u_2, \quad v_4 = m_4(u_2 - u_4) - v_2, \\
m_4 =& \frac{3 \cdot u_2^2 + 4}{2 \cdot v_2} = \frac{3 \cdot 76^2 + 4}{2 \cdot 32} \\
m_4 =& \frac{17332}{64} = \frac{251}{64} \equiv 251 \times 64^{-1} \pmod{589} \\
\equiv& 251 \times 543 \equiv 234 \equiv 234 \pmod{589} \\
m_4^2 \equiv& 234^2 \equiv 568 \pmod{589} \\
\implies u_4 =& m_4^2 - 2u_2 = 568 - 2 \times 76 = 568 - 152 \equiv 396 \pmod{589} \\
v_4 \equiv& 568(76 - 396) - 32 = -181792 \equiv 209 \pmod{589}
\end{aligned}
$$

Hence $(4!)P = 4Q = (396, 209)$
So far, we have been able to compute $P, (2!)P, (3!)P, (4!)P$. Continue as per the Lenstra's Algorithm and determine non trivial factor of 589, if there is any.

Elliptic Curve Primality Test

Most of the Elliptic Curve methods are based on classical methods. For example, Lenstra's Elliptic Curve in factorization is based on the Pollard's(p-1) factorization method. Likewise, the Elliptic Curve primality test (Pocklington or Pocklington- Lehmar Primality Test is the basis due to Goldwasser, Kilian and Alkin). We shall therefore first discuss the Pocklington-Lehmar Primality test. Usually, it is lot more easier to prove that a given positive integer is not a prime (also called a composite number) rather than prime. For example $a(1 < a \in \mathbb{N})$ is a composite number then there exist positive integer b, c such that $1 < b < a$, $1 < c < a$ and $a = bc$. Let $b \leq c$. Then $1 < b \leq \sqrt{a}$, and by the fundamental theorem of arithmetic, that every positive integer greater than 1 is a product of primes, there exists a prime p such that $p|b$. Thus p is a prime such that $1 < p \leq b \leq \sqrt{a}$; $p|b,\ b|a \implies p|a$.

Conclusion: If $1 < a \in \mathbb{N}$ is composite, then a has a prime factor not exceeding $\sqrt{a}$.
Hence if $a \in \mathbb{N}$ does not have a prime factor p $(\leq \sqrt{a},)$ then a is a prime.
For example $a = 5179$ is a prime, since none of the primes up to $\sqrt{a}$, that is 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 71 (as

$\sqrt{a} \leq 72$), divide a. Of course, the availability of primes up to $\sqrt{a}$, when a is large could be a problem.

Proposition 1: Let $n > 1$ be a positive integer such that there exist a prime $q > \sqrt{n} - 1$ and $q|(n-1)$. If there exists an integer a such that

1. $a^{n-1} \equiv 1 \pmod{n}$
2. $\gcd(a^{\frac{n-1}{q}} - 1, n) = 1$

then n is prime.
Proof: Suppose contrary, that n is composite, then as discussed above there exists a prime $p \leq \sqrt{n}$ such that $p|n$. Now $q > \sqrt{n} - 1 \geq p - 1 \implies q > p - 1 \implies \gcd(q, p-1) = 1 \implies u, v \in \mathbb{Z}$ such that $uq + v(p-1) = 1$ this implies that

$$\begin{aligned} a^{\frac{n-1}{q}} =& a^{1 \cdot \frac{n-1}{q}} = a^{[uq+v(p-1)]\frac{n-1}{q}} \\ =& a^{uq \cdot \frac{n-1}{q}} \cdot a^{v(p-1)\frac{n-1}{q}} \\ \equiv& a^{uq \cdot \frac{n-1}{q}} \pmod{p} \end{aligned}$$

since $a^{v(p-1)\frac{n-1}{q}} = (a^{p-1})^{v \cdot \frac{n-1}{q}} \equiv 1 \pmod{p}$ (using Fermat's little Theorem , aslo $\frac{n-1}{q} \in \mathbb{N}$ as $q|(n-1)$).

$$\begin{aligned} \implies a^{\frac{n-1}{q}} &\equiv a^{uq \cdot \frac{n-1}{q}} \pmod{p} \\ &\equiv a^{u(n-1)} \pmod{p} \\ &\equiv \left(a^{n-1}\right)^u \pmod{p} \\ &\equiv 1 \pmod{p} \quad \text{Since } p|n \text{ and } a^{n-1} \equiv 1 \pmod{n} \\ \implies & p|a^{\frac{n-1}{q}} - 1 \\ \implies & \gcd(a^{\frac{n-1}{q}} - 1, n) \geq p > 1 \text{ as } p|n \end{aligned}$$

This is a contradiction to the second condition, Hence, n is a prime.

The Pocklington-Lehmar Test, stated above, is certain to return n as a prime, unlike the probabilistic primality test such as Miller-Rabin and many others.

The Elliptic Curve Primality Test due to Golawasser and Kilian is based

on the following proposition, which is analogous to the Pocklington-Lehmar primality test.

Proposition 2: Let n be a positive integer, and let

$$E := \{(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n |\ y^2 = x^3 + Ax + B;\ A, B \in \mathbb{Z}_n\} \cup \{\infty\}$$

Also let $m \in \mathbb{Z}$ be an integer. Further, let there exist a prime q such that $q|m$ and $q > (n^{\frac{1}{4}} + 1)^2$. If there exists a point $P \in E$ such that

1. $mP = \infty$
2. $\left(\frac{m}{q}\right) P \neq \infty$

is defined, then n is a prime.

Proof: Again assume n is composite, then there exists a prime p such that $p|n$ and $p \leq \sqrt{n}$. Let E_p be the Elliptic Curve E, defined mod p. That is:

$$E_p := \{(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p |\ y^2 = x^3 + A_p x + B_p;\ A_p, B_p \in \mathbb{Z}_p\} \cup \{\infty\}$$

Same A, B but now mod p. That is

$$A \equiv A_p \pmod{p}$$
$$B \equiv B_p \pmod{p}$$

Let $\#(E_p) = m_p$ (order of the group E_p). By Hasse's Theorem:

$$|p + 1 - m_p)| \leq 2\sqrt{p}$$

$$\begin{aligned}
&\implies m_p \leq p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2 \\
&\implies m_p \leq (\sqrt{p} + 1)^2 \leq \left(n^{\frac{1}{4}} + 1\right)^2 < q \ \text{ since } p \leq \sqrt{n} \\
&\implies 1 \leq m_p < q \\
&\implies \gcd(q, m_p) = 1 \\
&\implies 1 = uq + vm_p \quad \text{for some integer } u, v \in \mathbb{Z} \\
&\implies uq \equiv 1 \pmod{m_p}, \quad \text{for some } u \in \mathbb{Z}_p
\end{aligned}$$

Since $P = P(x, y) \in E$, we get $Q(x', y') \in E_p$, where $x, y \in \mathbb{Z}_n, x', y' \in \mathbb{Z}_p$ are such that $x \equiv x' \pmod{p}$, $y \equiv y' \pmod{p}$.
Now

$$q|m \implies \frac{m}{q} \in \mathbb{Z} \implies \left(\frac{m}{q}\right) Q = uq \left(\frac{m}{q} Q\right) = (um)Q = u(mQ) = \infty$$

Since $mP = \infty$ on E and Q is the same point considered mod p, instead mod n. Thus $\left(\frac{m}{q}\right) Q = \infty$ on E_p.
But this is a contradiction on to the condition 2. As this will lead to $\left(\frac{m}{q}\right) P = \infty$. Because, if $\left(\frac{m}{q}\right) P$ is defined and not ∞ on E, then as earlier $\left(\frac{m}{q}\right) Q \neq \infty$. The proposition is proved.

Remark: Even without knowing n(prime or composite), an Elliptic Curve E and a point P on E can be found, point addition (that includes doubling of a point) may lead to the factorization of n, and thus confirming n to be a composite.

Discrete Logarithm Problem on an Elliptic Curve

Let $E_{\mathbb{F}}$ be an elliptic curve on a field $\mathbb{F}$. If P, Q are two points on E such that $Q = xP = P + P + \cdots + P$ (x- copies) for some non-negative integer x, and x is such least value, then it is called the discrete logarithm of Q to the base (point) P, and written as $x = dlog_P Q$ (in E).
If no such x- exists, then it is said that $dlog_P Q$ in E, does not exist. The discrete logarithm problem is said to be solvable in an elliptic curve E with respect to the base point P on E, if for every $Q \in E$, $dlog_P Q$ exists. This of course is the case if E is an additive (or multiplicative) cyclic group and P is a generator with respect to addition (or multiplication). But this may not be the case if the group is not cyclic, even if it is Abelian.

Example: Let $E := \{(x, y) \in \mathbb{F}_{11} \times \mathbb{F}_{11} |\ y^2 = x^3 + 3x + 1\} \cup \{\infty\}$.
If $P(1, 4)$, then $P \in E$ as

$$1^3 + 3 \times 1 + 1 = 5 \equiv 16 \equiv (\pm 4)^2$$

$$\implies (1, 4) \text{ and } (1, -4) = (1, 7) \in E.$$

And $-(1, 4) = (1, -4)$. Also $2(1, 4) = (2, 9) \in E$ as can be seen by the addition of point formula.
So $dlog_P Q = 2$ where $Q = (2, 9), P = (1, 4)$. This can be verified that the DLP in E with respect to $P(1, 4)$ is solvable, as $dlog_P Q$ in E exits for every $Q \in E$, since E is an additive cyclic group and P is a generator of this group.

Determine $dlog$ of $(6,9)$ in E with respect to the base $(1,4)$.
Does $dlog_{(2,9)}(6,2)$ in E exist ? If yes, then what is it?

Eample: Let $E := \{(x,y) \in \mathbb{F}_{11} \times \mathbb{F}_{11} |\ y^2 = x^3 + 4x + 5\} \cup \{\infty\}$.
If $Q = (0,7), R = (3,0)$, then it can be verified that $Q, R \in E$
Further, if $P = (0,4)$, then $P \in E$.
Verify that $3P = (0,7) = Q$. hence $dlog_P Q = 3$, also $2P = (3,0) = R \implies dlog_P R = 2$. Also, verify that if $B = (9,0)$, then also $B \in E$, and $2B = \infty$. Hence $dlog_B Q$ as well as $dlog_B R$ does not exist.

Write all pairs P, Q of points on E, for which $dlog_P Q$ exists, as well as the pairs for which it does not exist in above two examples.

Algorithms to Compute Discrete Logarithm in Elliptic Curves

All the algorithms (except the index calculus method) to compute discrete logarithm in a multiplicative cyclic group can be applied to the additive Abelian group E (of elliptic curve) by suitably changing the multiplicative operation to the additive operation. We shall therefore, first recall the multiplicative cyclic group $G = \langle g | g^n = 1 \rangle$ and algorithms to compute $dlog_g h$ in G and then restate its Elliptic Curve group additive analogue, if required.

1. **Enumeration:** Let $E_{\mathbb{F}}$ be an elliptic curve $P, Q \in E_{\mathbb{F}}$. To compute $dlog_P Q$ in E, simply compute $kP,\ k = 1, 2, 3 \ldots$ if there exists such a k and is least with the property $kP = Q$, then $x = k = dlog_P Q$ in E. If no such k exists, then $dlog_P Q$ in E does not exist. This method always works, and is quite satisfactory of small order elliptic curves.
   For example, $dlog_{(1,4)}(2,9) = 2$ in

   $$E := \{(x,y) \in \mathbb{F}_{11} \times \mathbb{F}_{11} |\ y^2 = x^3 + 3x + 3\} \cup \{\infty\}.$$

   The problem is quite time consuming if the order of the group E is large. Compute the order of the group (of points)

   $$E := \{(x,y) \in \mathbb{F}_{97} \times \mathbb{F}_{97} |\ y^2 = x^3 + 14x + 19\} \cup \{\infty\}$$

   Let $P = (57,58)$ and $Q = (56,48)$

(a) Is $P \in E$?

(b) Is $Q \in E$?

(c) Does $dlog_P Q$ exist? If yes, then compute it.

(d) Does $dlog_Q P$ exist? If yes, then compute it.

(e) What is the group structure E?

Shanks Baby Step Giant Step Algorithm for Elliptic Curves

First, recall the algorithm in a multiplicative cyclic group $G = \langle g |\ g^n = 1 \rangle$ to compute $x = dlog_g h$ in G. Set m to be the least positive integer greater or equal to $\sqrt{n}$.
By division algorithm/Euclidean algorithm there exists integers q and r such that

$$\begin{aligned} & x = qm + r \quad (0 \leq r < m) \\ \implies & h = g^x = g^{qm+r} = g^{qm} \times g^r = (g^m)^q \times g^r \\ \implies & (g^m)^q = hg^{-r} \end{aligned}$$

Compute the Baby steps $B = \{(hg^{-r}, r) |\ 0 \leq r < m\}$ i.e.

$$B = \{(h, 0), (hg^{-1}, 1), (hg^{-2}, 2), \ldots (hg^{-(m-1)}, m-1)\}$$

There are m-Baby steps. If $(1_G, s) \in B$ for some $0 \leq s < m$, then

$$hg^{-s} = 1_G \implies h = g^s \implies s = dlog_g h$$

and we are done.
If $(1_G, s) \notin B$ for any $s = 0, 1, \ldots, m-1$ then compute the Giant steps,

$$g^m, (g^m)^2 = g^{2m}, (g^m)^3, \ldots$$

If $g^{(m)^q} = g^{mq}$, is the first component in some Baby step with second component r, then

$$(g^{mq}, r) \in B \implies g^{mq} = hg^{-r} \implies g^{mq+r} = h \implies x = dlog_g h$$

Algorithm:

We can now state the analogue of Shanks Baby step-Giant step algorithm for elliptic curves.
Let E be an elliptic curve of order $n = \#(E)$. Suppose $P, Q \in E$ are such that $Q = kP$ and k is the least non negative integer with this property. Then $dlog_P Q = k$.
So, we set m =the least integer greater or equal to $\frac{n}{2}$. Then $k = mq + r$, for some integer q, r such that $0 \leq r \lneq m$
We get

$$Q = kP = (mq + r)P = (mq)P + rP = q(mP) + rP \implies Q - rP = q(mP)$$

Baby steps $B := \{(Q - rP, r) |\ 0 \leq r \lneq m\}$ that is

$$B = \{(Q, 0), (Q - P, 1), (Q - 2P, 2), \ldots (Q - (m-1)P, m-1)\} \subseteq E \times \mathbb{Z}$$

m-Baby steps.
Now, if there is a Baby step $(\infty, j) \in B$ for some $j (0 \leq j \leq m - 1)$, then

$$Q - jP = \infty \implies Q = jP + \infty = jP \text{ and } j = dlog_P Q.$$

If there is no such Baby step then compute Giant steps:

$$mP, 2(mP), 3(mP), \ldots$$

The moment the Giant step $q(mP)$ is a point in the first component of a Baby step $(q(mP), r) \in B$ then

$$\begin{aligned} q(mP) = Q - rP &\implies Q = q(mP) + rP = (qm + r)P \\ &\implies k = qm + r = dlog_P Q \in E. \end{aligned}$$

Since $dlog_P Q$ exists, therefore, such integers q and r exist.

Example: Let $E := \{(x, y) \in \mathbb{F}_{11} \times \mathbb{F}_{11} |\ y^2 = x^3 + 3x + 1\} \cup \{\infty\}$
Suppose $P(1, 4)$ and $Q = (3, 2)$. Then $P, Q \in E$.
Recall $n =$ order of E is 18 and $E \cong C_{18} = \langle P = (1, 4) \rangle$. Then $dlog_P Q$ exists.
Let $k = dlog_P Q$. Then $Q = kP$.
We compute k using the Shanks Baby step Giant step algorithm as follows:

Set $m = \frac{18}{2} = 9$.
Now $k = qm + r$ for some integers q, r, $k = 9q + r$ $(0 \leq r < m)$ Baby step

$$B := \{(Q, 0), (Q - P, 1), (Q - 2P, 2), \ldots (Q - 8P, 8)\}$$

Observe that $P = (1, 4) \implies -P = (1, -4) = (1, 7) = R$(say)

$$B := \{(Q, 0), (Q + R, 1), (Q + 2R, 2) \ldots (Q + 8R, 8)\}$$

where $Q = (3, 2)$ and $R = (1, 7)$
The Baby steps:

$$\begin{aligned} B := \{&((3,2),0), ((3,2)+(1,7),1), ((3,2)+2(1,7),2), ((3,2)+3(1,7),3), ((3,2)+4(1,7),4), \\ &((3,2)+5(1,7),5), ((3,2)+6(1,7),6), ((3,2)+7(1,7),7), ((3,2)+8(1,7),8)\} \end{aligned}$$

$$\begin{aligned} = \{&((3,2),0), ((3,2)+(1,7),1), ((3,2)+(2,2),2), ((3,2)+(0,10),3), ((3,2)+(8,3),4), \\ &((3,2)+(3,2),5), ((3,2)+(5,3),6), ((3,2)+(6,9),7), ((3,2)+(9,3),8), ((3,2),0), \\ &((5,3),1), ((6,9),2), ((9,3),3), ((4,0),4), ((9,8),5), ((6,2),6), ((5,8),7), ((3,9),8)\} \end{aligned}$$

We observe that the point at infinity ∞ is not not appearing as the first coordinate in any of the Baby step.
Hence, we need to compute the Giant steps as follows:

$$mP, 2(mP), 3(mP), \ldots \text{ i.e. } 9P, 2(9P), 3(9P), \ldots$$
$$P = (1, 4) \implies 9P = (4, 0)$$

So the Giant-steps are:

$$(4, 0), 2(4, 0,), 3(4, 0), \ldots \text{ i.e. } (4, 0), \infty, (4, 0), \ldots$$

since order of $(4, 0)$ is 2.
We also observe that $((4, 0), 4)$ is a Baby-step.
Hence $q = 1, r = 4, m = 9$

$$\implies k = qm + r = 1 \times 9 + 4 = 13 \implies dlog_P Q = 13$$

This can be directly too verified as

$$P = (1, 4), 2P = (2, 9), 4P = (8, 8), 8P = (9, 8).$$

We calculate using doubling repeatedly and adding if required.
Hence $13P = 8P + 4P + P = (9, 8) + (8, 8) + (1, 4) = (5, 3) + (1, 4) = (3, 2) = Q$

Lecture-19

Pollard's Rho Algorithm For Discrete Logarithm

Recall the Pollard's ρ algorithm for computing discrete logarithm in a finite cyclic group of an element w.r.t its generator. We give here its analogue for the group E (the additive group of an elliptic curve E) as follows:
Let E be an Elliptic Curve, P, Q be points on E. Then $dlog_P Q$ exists if $Q \in \langle P \rangle \leq E$ where $G = \langle P \rangle$, denotes the subgroup of E (w.r.t. point addition in E).
So suppose, $|G| = n$, and $Q \in G = \langle P | nP = \infty \rangle$. Then $dlog_P Q$ exists. That is there is exist an integer $k \geq 0$, such that $kP = Q$ $(0 \lneq k < n)$, and k is least with this property. That means $k = dlog_P Q$ in G and thus in E. Now divide G into three pairwise disjoint subsets, G_1, G_2, G_3 such that G is their union. That is

$$G = G_1 \cup G_2 \cup G_3 \quad (G_i \cap G_j = \phi \quad \text{for } i \neq j)$$

Define a function

$$f : G = G_1 \cup G_2 \cup G_3 \to G$$
$$R \to f(R) = \begin{cases} P + R, & \text{if } R \in G_1 \\ 2R, & \text{if } R \in G_2 \\ Q + R, & \text{if } R \in G_3 \end{cases}$$

Choose a random integer $m_0 \in \{1, 2, \ldots, n\}$. Let $R_0 = m_0 P,\ R_1 = f(P_0),\ R_{i+1} = f(R_i)\ \ \forall i \geq 0$. This suggest that $R_i = m_i P + n_i Q\ \ i \geq 0,\ n_0 = 0$

$$\implies R_1 = f(R_0) = \begin{cases} P + m_0 P = (m_0 + 1)P & \text{if } R_0 \in G_1 \\ 2m_0 P & \text{if } R_0 \in G_2 \\ m_0 P + Q & \text{if } R_0 \in G_3 \end{cases}$$

By induction, prove that (assuming $R_i = m_iP + n_iQ$)

$$R_{i+1} = f(R_i) = f(m_iP + n_iQ) = m_{i+1}P + n_{i+1}Q \quad \forall i \geq 0, n_0 = 0$$

$$R_{i+1} = \begin{cases} m_{i+1}P + n_iQ & \text{if } R_i \in G_1 \\ 2m_{i+1}P + 2n_{i+1}Q & \text{if } R_i \in G_2 \\ m_iP + n_{i+1}Q & \text{if } R_i \in G_3 \end{cases}$$

Thus,

$$R_{i+1} = m_{i+1}P + n_{i+1}Q,$$

where

$$m_{i+1} = \begin{cases} m_i + 1, & \text{if } R_i \in G_1 \\ 2m_i, & \text{if } R_i \in G_2 \\ m_i, & \text{if } R_i \in G_3 \end{cases}$$

and

$$n_{i+1} = \begin{cases} n_i, & \text{if } R_i \in G_1 \\ 2n_i, & \text{if } R_i \in G_2 \\ n_i + 1, & \text{if } R_i \in G_3 \end{cases}$$

Since, $P, Q \in G$ and each $R_i = m_iP + n_iQ$ is an integer linear combination of P and Q, we get each $R_i \in G$.
Now $\#(E)$ is finite this implies $\#(G)$ is also finite, this gives that the points $R_0, R_1, R_2, \ldots$ thus constructed in G can not be distinct. So for some integer $j \geq 0$, $R_i = R_{i+j}$. But then

$$m_iP + n_iQ = m_{i+j}P + n_{i+j}Q$$

$$\implies (m_i - m_{i+j})P = (n_{i+j} - n_i)Q$$

If $k = dlog_P Q$ in G, then $Q = kP$, and we get

$$(m_i - m_{i+j})P = (n_{i+j} - n_i)kP$$

$$\implies k = (n_{i+j} - n_i)^{-1}(m_i - m_{i+j}) \text{ (if gcd } (n_{i+j} - n_i) \text{ and } n \text{ is 1).}$$

If $\gcd((n_{i+j} - n_i), n) = d > 1$, then $\gcd((n_{i+j} - n_i), \frac{n}{d}) = 1$, and $(n_{i+j} - n_i)^{-1}$ exists $\left(\text{mod } \frac{n}{d}\right)$. In that case

$$k \equiv (n_{i+j} - n_i)^{-1}(m_i - m_{i+j}) \ \left(\text{mod } \frac{n}{d}\right)$$

will give d number of choices for $k = dlog_P Q$, namely

$$k, k + \frac{n}{d}, k + \frac{2n}{d}, \ldots k + \frac{(d-1)n}{d},$$

i.e. $k + \frac{sn}{d}, \quad 0 \leq s \leq d-1$

Example. Compute if it exists $dlog_P Q$ in the curve

$$E = \{(x, y) \in F_{11} \times F_{11} | y^2 = x^3 + 3x + 1\} \cup \{\infty\}$$

where $P = (1, 4)$, and $Q = (3, 2)$. It can be easily verified that $P, Q \in E$ (and $dlog_P Q = k$ exists, as we know, but otherwise, we can assume that it exists and proceed). Since $\#(E)$ is small, in fact we have already computed all points on E, and saw that $\#(G) = \#(E) = 18$, where $G = \langle P \rangle$.
The group G can be written as the disjoint union.

$$\begin{aligned} E = G = &\{(0,1), (0,10), (1,4), (1,7), (2,2), (2,9)\} \\ &\cup \{(3,2), (3,9), (4,0), (5,3), (5,8), (6,2)\} \\ &\cup \{(6,9), (8,3), (8,8), (9,3), (9,8), \infty\} \\ &= G_1 \cup G_2 \cup G_3 \end{aligned}$$

where

$$\begin{aligned} G_1 &= \{(0,1), (0,10), (1,4), (1,7), (2,2), (2,9)\} \\ G_2 &= \{(3,2), (3,9), (4,0), (5,3), (5,8), (6,2)\} \\ G_3 &= \{(6,9), (8,3), (8,8), (9,3), (9,8), \infty\} \end{aligned}$$

Let $m_0 = 2, \quad n_0 = 0, \quad R_0 = m_0 P + n_0 Q \implies R_0 = 2P = 2(1,4) = (2,9)$
Define

$$f : G \to G$$

$$R \to f(R) = \begin{cases} P + R, & \text{if } R \in G_1 \\ 2R, & \text{if } R \in G_2 \\ Q + R, & \text{if } R \in G_3 \end{cases}$$

Then $R_{i+1} = f(R_i) \quad \forall i \geq 0 \implies R_1 = f(R_0) = P + R_0$ as $R_0 \in G_1$ This gives $R_1 = (1,4) + (2,9) = (0,1)$
Since $R_1 \in G_1$, we get

$$R_2 = f(R_1) = P + R_1 \quad i.e. \quad R_2 = (1,4) + (0,1) = (8,8)$$

As $R_2 = (8, 8) \in G_3$, we get

$$R_3 = f(R_2) = Q + R_2 = (3, 2) + (8, 8) = (1, 7)$$

Since $R_3 = (1, 7) \in G_1$, we get

$$R_4 = f(R_3) = P + R_3 = (1, 4) + (1, 7) \implies R_4 = \infty$$

Observe that $R_4 = \infty \in G_3$, we get

$$R_5 = f(R_4) = Q + R_4 = (3, 2) + \infty \implies R_5 = (3, 2)$$

Since $R_5 = (3, 2) \in G_2$, we get

$$R_6 = f(R_5) = 2R_5 = 2(3, 2) \implies R_6 = (9, 8)$$

We see that $R_6 = (9, 8) \in G_3$ this implies

$$R_7 = f(R_6) = Q + R_6 = (3, 2) + (9, 8) \implies R_7 = (0, 1)$$

We note that $R_1 = R_7 = (0, 1)$
We also know that

$$R_i = m_i P + n_i Q \quad \forall i \geq 0 \quad \text{with } m_0 = 2, n_0 = 0$$

This implies that

$R_1 = m_1 P + n_1 Q = R_7 = m_7 P + n_7 Q$
$\implies (m_1 - m_7)P = (n_7 - n_1)Q$
$\implies Q = (n_7 - n_1)^{-1}(m_1 - m_7)P$
$\implies k = (n_7 - n_1)^{-1}(m_1 - m_7) = dlog_P Q$. Provided $(n_7 - n_1)^{-1} \pmod{\#(G)}$ exist.

The integer $m_i's$ and n_i's are calculated using the recurrence relations:

$$m_{i+1} = \begin{cases} m_i + 1, & \text{if } R_i \in G_1 \\ 2m_i, & \text{if } R_i \in G_2 \\ m_i, & \text{if } R_i \in G_3 \end{cases} \quad \text{and } n_{i+1} = \begin{cases} n_i, & \text{if } R_i \in G_1 \\ 2n_i, & \text{if } R_i \in G_2 \\ n_i + 1, & \text{if } R_i \in G_3 \end{cases} \quad \forall i \geq 0 \, (m_0 = 2, n_0 = 0)$$

This gives :

$$\begin{aligned} m_1 =& m_0 + 1 = 2 + 1 = 3 \\ n_1 =& n_0 = 0 \quad \text{since } R_0 \in G_1 \end{aligned}$$

$$\begin{aligned} \implies m_2 =& m_1 + 1 = 3 + 1 = 4 \\ n_2 =& n_1 = 0 \quad \text{since } R_1 \in G_1 \end{aligned}$$

$$\begin{aligned} \implies m_3 =& m_2 = 4 \\ n_3 =& n_2 + 1 = 0 + 1 = 1 \quad \text{since } R_2 \in G_3 \end{aligned}$$

$$\begin{aligned} \implies m_4 =& m_3 + 1 = 4 + 1 = 5 \\ n_4 =& n_3 = 1 \quad \text{since } R_3 \in G_1 \end{aligned}$$

$$\begin{aligned} \implies m_5 =& m_4 = 5 \\ n_5 =& n_4 + 1 = 1 + 1 = 2 \quad \text{since } R_4 \in G_3 \end{aligned}$$

$$\begin{aligned} \implies m_6 =& 2m_5 = 2 \times 5 = 10 \\ n_6 =& 2n_5 = 2 \times 2 = 4 \quad \text{since } R_5 \in G_2 \end{aligned}$$

$$\begin{aligned} \implies m_7 =& m_6 = 10 \\ n_7 =& n_6 + 1 = 4 + 1 = 5 \quad \text{since } R_6 \in G_3 \end{aligned}$$

This gives $m_1 = 3, n_1 = 0, m_7 = 10, n_7 = 5$ and therefore

$$\begin{aligned} (m_1 - m_7)P &= (n_7 - n_1)Q \\ (3 - 10)P &= (5 - 0)Q \\ \text{or } -7P &= 5Q \\ \text{or } Q &= (-5^{-1} \times 7 \pmod{18})P \end{aligned}$$

Since $(5, 18) = 1$, we get using the Euclidean /Division Algorithm,
$5^{-1} \pmod{18}$ to be 11 as $11 \times 5 = 55 \equiv 1 \pmod{18}$
Hence $Q = (-11 \times 7)P = -77P = -5P = 13P \implies Q = 13P$
Hence $k = dlog_P Q = 13$
This can be directly verified by repeatedly doubling and adding that $13P = Q$

Silver-Pohlig-Hellman Algorithm For Computing Logarithm In Elliptic Curves

Recall the idea of the Silver-Pohlig Hellman Algorithm for computing discrete logarithm in a cyclic group $G = \langle g | g^n = 1 \rangle$ of order n for an element h to the base g the generator of G. The idea was first to reduce the DLP to cyclic groups of prime power order p^e, where $p^e | n$ but $p^{e+1} \nmid n$, and p is a prime, and then reduce the problem of prime order cyclic groups, evaluating g discrete logarithm in these groups and then computing discrete logarithm g, by applying Chinese Remainder Theorem.
So, we shall reiterate the algorithm but with changes according to the group $G = \langle P | nP = \infty \rangle \leq E$, where E is an elliptic curve and $Q,\ P \in G$ to compute $dlog_P Q$ in G and thus in E.

Writing prime factorization of n as :

$$n = \prod_{(p|n)} p^{e(p)} \implies nP = \infty \text{ as } O(P) = n$$

For each prime $p|n$, let $n_p = \frac{n}{p^{e(p)}}$, and

$$P_p = n_p P \in G$$

Then

$$p^{e(p)}[P_p] = p^{e(p)}[n_p P] = (p^{e(p)} \cdot n_p)P = nP = \infty \implies O(P_p) | p^{e(p)}$$

$P_p \neq \infty$ as this will imply that order of G is less than n.
Further, if $O(P_p) = p^{\epsilon(p)}$, then $\epsilon(p) < n$

$$\begin{aligned} &\implies p^{\epsilon(p)}(P_p) = \infty \\ &\implies p^{\epsilon(p)}(n_p P) = \infty \\ &\implies (p^{\epsilon(p)} \cdot n_p)P = \infty \\ &\implies n | (p^{\epsilon(p)} \cdot n_p) \end{aligned}$$

which is not possible as $n > (p^{\epsilon(p)} \cdot n_p)$. Hence $O(P_p) = p^{e(p)} \ \ \forall p | n$

Reduction of DLP to prime power order additive cyclic groups in Elliptic Curves

Let $G = \langle P | nP = \infty \rangle$, and $n = \prod_{(p|n)} p^{e(p)}$ be the prime factorization of n. If $n_p = \frac{n}{p^{e(p)}}$, then $p \nmid n_p$, and if $P_p = n_p P$ then $P_p \in G \leq E$ (the group of the Elliptic Curve), we have observed that order $O(P_p) = p^{e(p)}$. Let

$$H = \left\langle P_p |\ p^{e(p)} P_p = \infty \right\rangle \leq G \leq E$$

Suppose $k = dlog_P Q \in G$. Then

$$\begin{gathered} kP = Q \\ \implies k(P_p) = k(n_p P) = (kn_p)P = (n_p k)P = n_p(kP) = n_p Q = Q_p \ \ \text{(say)} \\ \implies Q_p \in H = \left\langle P_p |\ p^{e(p)} P_p = \infty \right\rangle \end{gathered}$$

Let $k(p) = dlog_{P_p} Q_p$. Then $k(p)[P_p] = Q_p \ \ \forall p|n$.
Observe that

$$\begin{aligned} n_p(-kP + Q) &= -k(n_p P) + n_p Q \\ &= -k(P_p) + Q_p = -Q_p + Q_p = \infty \\ &\implies O(-kp + Q) | n_p \ \ \forall p|n \\ &\implies O(-kp + Q) |\ \gcd(n_p) \ \ \forall p|n \\ &\implies O(-kp + Q) | 1 \\ &\implies O(-kp + Q) = 1 \\ &\implies -kp + Q = \infty \\ &\implies kP = Q \\ &\implies k = dlog_P Q \in E \end{aligned}$$

Recall, $Q_p = n_p Q \in H = \left\langle P_p = n_p P |\ p^{e(p)} P_p = \infty \right\rangle$ Also,

$$k(p) = dlog_{P_p} Q_p \implies k(p) P_p = Q_p \text{ and } k(P_p) = Q_p$$

Hence $k(P_p) = k(p) P_p$ in H, $|H| = p^{e(P)}$
$\implies (k - k(p)) P_p = \infty$ in H
$\implies k \equiv k(p) \pmod{p^{e(P)}}$
Thus k can be computed using Chinese Remainder Theorem.

Reduction of DLP to prime order cyclic group of an Elliptic Curve

Let $H = \langle P |\ p^{e(p)}P = \infty \rangle \leq E$ for an Elliptic Curve E.
Let $R \in H$, then $k = dlog_P R$ exists. If $A = \infty$, then $k = 0$.
Let $A \neq \infty$. Then $0 < k < m = p^e$.
Write

$$k = k_0 + k_1 p + k_2 p^2 + \cdots + k_{e-1} p^{e-1}$$

[This can be done (prove) that every positive integer a can be written an integer polynomial in the powers of an another integer b.]

Now $\quad kP = R \quad \because k = dlog_P R$ in H

$$\begin{aligned}
&\implies p^{e-1}(kP) = p^{e-1}R \\
&\implies (p^{e-1}k)P = p^{e-1}R \\
&\implies p^{e-1}(k_0 + k_1 p + k_2 p^2 + \cdots + k_{e-1}p^{e-1})P = p^{e-1}R \\
&\implies (k_0 p^{e-1})P + (k_1 p^e + k_2 p^{e+1} + \cdots + k_{e-1}p^{2e-2})P = p^{e-1}R \\
&\implies (k_0 p^{e-1})P + (k_1 + k_2 p + \cdots + k_{e-1}p^{e-2})p^e P = p^{e-1}R \\
&\implies (k_0 p^{e-1})P = p^{e-1}R
\end{aligned}$$

$\because (k_1 + k_2 p + \cdots + k_{e-1}p^{e-2})p^e P = \infty$ as $p^e P = \infty$ in H.
Thus

$$\begin{aligned}
&(k_0 p^{e-1})P = p^{e-1}R \quad \text{or} \quad k_0(p^{e-1}P) = p^{e-1}R \in H \\
\implies\ &k_0 = dlog_{(p^{e-1}P)}(p^{e-1}R) \in H \quad \text{or} \quad k_0 = dlog_{\bar{P}}\bar{R}
\end{aligned}$$

where

$$\bar{P} = p^{e-1}P \text{ and } \bar{R} = p^{e-1}R \in H$$

Further

$$p(\bar{P}) = p(p^{e-1}P) = p^e P = \infty$$

Let $K = \langle \bar{P} | p\bar{P} = \infty \rangle$, then $\bar{R} \in K$, and the problem of computing k_0 is to compute logarithm in K, a cyclic prime order group in E.

Computing other coefficients $\mathbf{k_1, k_2, \ldots, k_{e-1}}$

The other coefficient $k_1, k_2, \ldots, k_{e-1}$, are computed recursively as follows:
Suppose $k_1, k_2, \ldots, k_{i-1}$ have been computed then

$$\begin{aligned}(k_ip^i + k_{i+1}p^{i+1} + \cdots + k_{e-1}p^{e-1})P &= \left\{(-k_0 - k_1p - k_2p^2 - \cdots - k_{i-1}p^{i-1}) + \sum_{i=0}^{e-1} k_ip^i\right\}P \\ &= (-k_0 - k_1p - k_2p^2 - \cdots - k_{i-1}p^{i-1} + k)P \\ &= (-k_0 - k_1p - k_2p^2 - \cdots - k_{i-1}p^{i-1})P + kP \\ &= (-k_0 - k_1p - k_2p^2 - \cdots - k_{i-1}p^{i-1})P + R \\ &= R_i \quad \text{(say), as} \quad kP = R\end{aligned}$$

Thus

$$\begin{aligned}(k_ip^i + k_{i+1}p^{i+1} + \cdots + k_{e-1}p^{e-1})P =& R_i \\ =& (-k_0 - k_1p - k_2p^2 - \cdots - k_{i-1}p^{i-1})P + R, \\ & \forall i \geq 1 \quad \text{and} \quad R_0 = R\end{aligned}$$

$(k_ip^i + k_{i+1}p^{i+1} + \cdots + k_{e-1}p^{e-1})P = R_i$
Adding both sides p^{e-i-1} times. we get:

$$\begin{aligned}& \{p^{e-i-1}(k_ip^i + k_{i+1}p^{i+1} + \cdots + k_{e-1}p^{e-1})\}P = p^{e-i-1}R_i \\ \Longrightarrow\ & p^{e-1}p^{-i}(k_ip^i + k_{i+1}p^{i+1} + \cdots + k_{e-1}p^{e-1})P = p^{e-i-1}R_i \\ \Longrightarrow\ & p^{e-1}(k_i + k_{i+1}p + \cdots + k_{e-1}p^{e-i-1})P = p^{e-i-1}R_i \\ \Longrightarrow\ & \{p^{e-1}k_i + p^{e-1}p(k_{i+1} + k_{i+2}p + \cdots + k_{e-1}p^{e-i-2})\}P = p^{e-i-1}R_i \\ \Longrightarrow\ & (p^{e-1}k_i)P + p^e(k_{i+1} + k_{i+2}p + \cdots + k_{e-1}p^{e-i-2})P = p^{e-i-1}R_i \\ \Longrightarrow\ & (p^{e-1}k_i)P = p^{e-i-1}R_i \quad \forall i \geq 1\end{aligned}$$

Since $\quad p^e(k_{i+1} + k_{i+2}p + \cdots + k_{e-1}p^{e-i-2})P$
$= (k_{i+1} + k_{i+2}p + \cdots + k_{e-1}p^{e-i-2})[p^eP]$
$= \infty$

as $p^e P = \infty$, since $P \in H$, and $|H| = p^e$.
Hence

$$\begin{aligned} &\implies (p^{e-1}k_i)P = p^{e-i-1}R_i \quad \forall i \geq 1 \\ \textbf{Or} \quad &k_i(p^{e-1}P) = p^{e-i-1}R_i \\ &k_i\bar{P} = p^{e-i-1}R_i \implies p^{e-i-1}R_i \in K = \left\langle \bar{P} | p\bar{P} = \infty \right\rangle \end{aligned}$$

Hence solutions k_i's are the discrete logs of some element in K. in particular, we get

$$k_i = dlog_{(p^{e-1}P)}(p^{e-i-1}R_i) \ \ \forall i$$

Or

$$k_i = dlog_{\bar{P}}(p^{e-i-1}R_i) \ \text{ where } \bar{P} = p^{e-1}P$$

Since $\bar{P}$ is an element of $K \leq E$, so $\bar{P}$ is a point of order p, the prime $p|n$. Thus the problem is now completely reduced to finding discrete logarithm in a cyclic group of order a prime p.
Recall

$$\begin{aligned} R_i =&(-k_0 - k_1 p - k_2 p^2 - \cdots - k_{i-1}p^{i-1})P + R \\ =&(k_i p^i + k_{i+1}p^{i+1} + \cdots + k_{e-1}p^{e-1})P \end{aligned}$$

In particular,

$$R_0 = (k_0 + k_1 p + \cdots + k_{e-1}p^{e-1})P = kP = R \quad \text{Or} \quad R_0 = R$$

Hence, $k_0 = dlog_{\bar{P}}(p^{e-1}R_0) = dlog_{(p^{e-1}P)}(p^{e-1}R)$ as $R_0 = R$

$$\implies k_0 = dlog_{(p^{e-1}P)}(p^{e-1}R)$$

Next,

$$\begin{aligned} R_1 =&(k_1 p + k_2 p^2 + \cdots + k_{e-1}p^{e-1})P \\ =&(k_0 + k_1 p + \cdots + k_{e-1}p^{e-1} - k_0)P \\ =&(k - k_0)P \\ =&kP - k_0 P \\ \text{Or} \quad R_1 =&R - k_0 P \\ \text{and so,} \quad k_1 =&dlog_{\bar{P}}(p^{e-2}R_1) \end{aligned}$$

Since k_0 has already been determined, R_i is determined and hence k_1 can be determined,
Similarly,

$$\begin{aligned} R_2 =&(k_2p^2 + k_3p^3 + \cdots + k_{e-1}p^{e-1})P \\ =&(k_0 + k_1p + \cdots + k_{e-1}p^{e-1} - k_0 - k_1p)P \\ =&(k - k_0 - k_1p)P \\ =&kP + (-k_0 - k_1p)P \\ \implies R_2 =&kP - k_0P - (k_1p)P \\ k_2 =&dlog_{\bar{P}}(p^{e-3})R_2 \text{ where } \bar{P} = pP \end{aligned}$$

can be determined as k_0, k_1 have been determined, then k_i (and hence k) can be determined.

Example: Let $E = \{(x, y) \in F_{11} \times F_{11} |\ y^2 = x^3 + 3x + 1\} \cup \{\infty\}$ using Silver-Pohlig-Hellman Algorithm determined $dlog_{(1,4)}(3, 2)$ in E, if it exists.
Suppose $k = dlog_P Q$ exists.
Let $P = (1, 4),\ Q = (3, 2)$. Then it can be verified that P has order 18 in E.
Also note that $Q \in G = \langle P = (1, 4) |\ 18P = \infty \rangle \leq E$,
Recall, the notations, explained in the Algorithm order of G is

$$n = 18 = 2 \times 3^2 = \prod_{p|n} p^{e(p)} \implies e(p) = 1 \text{ for } p = 2, e(p) = 2 \text{ for } p = 3.$$

Since

$$n_p = \frac{n}{p^{e(p)}}$$

$$\implies n_2 = \frac{18}{2} = 9, \text{ So } n_2 = 9 \text{ for } p = 2$$

$$\implies n_3 = \frac{18}{3^2} = 2, \text{ So } n_3 = 2 \text{ for } p = 3$$

$$P_{p=2} = n_pP = n_2P = 9P = 9(1, 4) = (4, 0)$$
$$P_{p=3} = n_pP = n_3P = 2P = 2(1, 4) = (2, 9)$$

Since $Q_p = n_pQ$ this implies that

$$\begin{aligned} Q_{p=2} =&n_2Q = 9(3, 2) = (4, 0) \\ Q_{p=3} =&n_3Q = 2(3, 2) = (9, 8) \end{aligned}$$

Corresponding subgroup H of G

$$\begin{aligned} H_{p=2} &= \left\langle P_{(p=2)} = (4,0) | 2P_{p=2} = \infty \right\rangle \\ H_{p=3} &= \left\langle P_{(p=3)} = (2,9) | 9P_{p=3} = \infty \right\rangle \\ \implies |H_{p=2}| &= p^{e(p)} = 2^1 = 2 \text{ and } |H_{p=3}| = p^{e(p)} = 3^2 = 9 \end{aligned}$$

We know that $Q_{p=2} \in H_{p=2}$ and $Q_{p=3} \in H_{p=3}$ and the problem is now reduced to determine discrete logarithm in these subgroups of order $p^{e(p)}$ for $p = 2, 3$ respectively i.e.

$$\begin{aligned} k(2) &= dlog_{(P_{p=2})} Q_{p=2} = dlog_{(4,0)}(4,0) \in H_{p=2} \\ k(3) &= dlog_{(P_{p=3})} Q_{p=3} = dlog_{(2,9)}(9,8) \in H_{p=3} \end{aligned}$$

Obviously $k(2) = 1$. We determine $k(3)$ by reducing the DLP further to the prime order cyclic group for $p = 3$ i.e. C_3. Since $e(p) = 2$ for $p = 3$, we can assume for some integers $k_0(3)$ and $k_1(3)$, that

$$k(3) = k_0(3) + 3k_1(3)$$

The integer $k_0(3)$ and $k_1(3)$ are determined as follows: $R_{p=3} = (9,8)$ [follows the notations]. Recall

$$\bar{P}_{p=3} = p^{e(p)-1} P_{p=3} = 3^{2-1}(2,9) = 3(2,9) = (5,8)$$

and

$$\bar{R}_{p=3} = p^{e(p)-1} R_{p=3} \implies \bar{R}_{p=3} = 3^{2-1}(9,8) = 3(9,8) = (5,8)$$

Hence $k_0(3) = dlog_{(\bar{P}_{p=3})} \bar{R}_{p=3} = dlog_{(5,8)}(5,8) = 1$. We next determine $k_1(3) = dlog_{(\bar{P}_{p=3})} \bar{R}_{1(p=3)}$ where

$$\begin{aligned} \bar{R}_{1(p=3)} &= p^{e(p)-2} R_1 \text{ for } p = 3 \\ &= 3^{2-2} R_{1(p=3)} = R_{1(p=3)} \\ \text{where } R_{1(p=3)} &= R - k_0(p) P_{p=3} = R_{p=3} - k_0(3) P_{p=3} \\ &= (9,8) - 1 \cdot (2,9) = (9,8) - (2,9) \\ &= (9,8) + (2,-9) = (9,8) + (2,2) \\ &= (5,8) \end{aligned}$$

This gives $\bar{R}_{1(p=3)} = \bar{R}_{(p=3)} = (5, 8)$. And therefore $k_1(3) = dlog_{(\bar{P}_{p=3})}\bar{R}_{1(p=3)} = dlog_{(5,8)}(5, 8) = 1$. Hence

$$k(3) = k_0(3) + 3k_1(3) = 1 + 3 \cdot 1 = 1 + 3 = 4$$

These values, $k(2) = 1$ and $k(3) = 4$, give value $k = dlog_P Q$, since

$$\begin{aligned} & k \equiv k(2) \pmod 2 \\ & k \equiv k(3) \pmod 9 \\ \Longrightarrow\ & k \equiv 1 \pmod 2 \\ & k \equiv 4 \pmod 9 \end{aligned}$$

Apply now the Chinese Remainder Theorem to get $k \equiv 13 \pmod{18}$. Hence

$$dlog_{(1,4)}(3, 2) = 13 \in E$$

This can be verified directly by computing $13P$ for $P = (1, 4)$ using the method of repeatedly doubling and adding if required.

Elliptic Curve Cryptography

We shall see how elliptic curves can be used in communication. Both the plain text space as well as the cipher text space is the group $E = E(\mathbb{F})$ of points of an elliptic curve E over a field $\mathbb{F}$. The group E is an additive Abelian group.
We present here analogues of various cryptosystem already discussed on cyclic groups. We begin with:

Diffie-Hellman Key Exchange Protocol

Let $\mathbb{F}_q$ be a finite field of order q (here q is prime or prime power). Then $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is a multiplicative cyclic group of order $q - 1$. And we know how to set up Diffie-Hellman Key Exchange Protocol on $\mathbb{F}_q^*$. The corresponding analogue for $E = E(\mathbb{F}_q)$ is as follows:
Let $E = E(\mathbb{F}_q)$ be an elliptic curve over a finite field $\mathbb{F}_q$. Suppose Alice and Bob wants to have a common knowledge (a point on E). For this, Alice chooses a positive integer 'a' and keeps it secret. Similarly, Bob chooses a

positive integer 'b' and keeps it secret.
Suppose E and a point P on E are known to them. Alice computes the point aP (by adding P repeatedly a-times) and sends it to Bob. Bob computes the point bP and sends it to Alice.
Alice, who received bP from Bob, computes $a(bP)$, adding bP (repeatedly a-times) and get $(ab)P$. Similarly, Bob has received aP from Alice. He computes $b(aP)$. Now Alice has the point $a(bP)$ while Bob has the point $b(aP)$ of E. Both of them in fact have the same point namely $(ab)P$ as $a(bP) = (ab)P = (ba)P = b(aP)$ in E. This point becomes their common knowledge.

Example: Let $E := \{(x, y) \in \mathbb{F}_{11} \times \mathbb{F}_{11} |\ y^2 = x^3 + 3x + 1\} \cup \{\infty\}$ be public. Also let the point $P(3, 2)$ be also public.
Suppose Alice chooses integer $a = 3$ and Bob chooses the integer $b = 5$. They keep these integers secret. Alice computes $aP = 3P = (0, 1)$ and sends it to Bob. Bob Computes $bP = 5P = (6, 9)$. Alice computes

$$a(bP) = 3(6, 9) = (0, 10).$$

Similarly Bob computes

$$b(aP) = 5(0, 1) = (0, 10).$$

Now Alice and Bob both have their common knowledge the point $(0, 10) \in E$. They can use it in various applications of Diffie-Hellman key exchange protocol.
Verify all the calculations.

The Diffie-Hellman Problem and The Diffie-Hellman Assumption

Let $E = E(\mathbb{F}_q)$ be an elliptic curve P, aP, bP are points on E, where a, b are some integers. Suppose E, P, aP, bP are public. Then the Diffie-Hellman Problem (DHP) is to compute (from this knowledge) the point $(ab)P$ (of E). The Diffie-Hellman Assumption (DHA) is that it is difficult to do that. Of course the Diffie-Hellman Problem is solvable if the discrete logarithm can be computed of the point(s) aP, bP to the base point P in E. There may be some other ways as well to do the same. There is another related problem:

Decision Diffie-Hellman Problem and The Diffie-Hellman Assumption

If $P, aP, bP \in E(\mathbb{F}_q)$ are known is then possible to decide for a given point $Q \in E(\mathbb{F}_q)$, that $Q = (ab)P$ or not. Accordingly, the DDH Assumption is that it is not easy to do that.

Massey-Omura Cryptosystem

Alice and Bob setup the Massey-Omura cryptosystem for communication as follows:

1. They both agree on a Elliptic Curve $E = E(\mathbb{F}_q)$.
2. They also agree that the plain text space as well as cipher text space are the points of E i.e. the group E.

   Now suppose Alice wants to send a message (a point $M \in E$) to Bob.

   (a) She chooses and keeps it secret a positive integer a, computes the point $aM \in E$ and sens it to Bob

   (b) Bob also chooses and keeps secret a positive integer b. He received aM from Alice. He computes $b(aM) = baM = abM \in E$ and sends it to Alice.

   (c) Alice received $(ab)M$ from Bob, she computes $a^{-1}(ab)M = bM$ and sends it to Bob.

   (d) Bob received bM from Alice, he computes $b^{-1}(bM) = M$ and thus gets the message M from Alice.

Note: Alice computes a^{-1} from a and Bob computes b^{-1} from b. This, therefore, requires $gcd(a, N) = 1$ as well as $gcd(b, N) = 1$, where N is the order of the group. Hence, while choosing integers a, b, they have to be careful. The $a^{-1} \pmod N$ and $b^{-1} \pmod N$ can be computed using Division Algorithm/Euclidean Algorithm.

Example: Let Alice and Bob want to communicate using Massey-Omura cryptosystem.

1. They agree on the Elliptic curve:

$$E = E(\mathbb{F}_{11}) = \{(x, y) \in \mathbb{F}_{11} \times \mathbb{F}_{11} | y^2 = x^3 + 3x + 1\} \cup \{\infty\}$$

   Verify N=order of E is 18.

2. Alice chooses and keeps it secret the integer $a = 7$. She computes $7^{-1} \pmod{18}$. This is 13 (as $13 \times 7 = 91 = 1 + 5 \times 18 \equiv 1 \pmod{18}$).

3. Bob chooses and keeps it secret the integer $b = 11$. He computes $11^{-1} \pmod{18}$. This is 5 since $11 \times 5 = 1 + 3 \times 18 \equiv 1 \pmod{18}$.

   Now suppose Alice wants to send the message the point $M(6, 2) \in E$ to Bob.

   (a) She computes $aM = 7M = 7(6, 2) = (3, 2)$ and sends to Bob.

   (b) Bob received $aM = (3, 2)$ from Alice.
   He computes $b(aM) = 11(3, 2) = (1, 7)$ and sends to her.

   (c) Alice received $b(aM) = (ba)M = (ab)M = a(bM) = (1, 7)$ from Bob.
   She computes $a^{-1}(ab)M = 7^{-1}(1, 7) = 13(1, 7) = (3, 9)$.
   She sends $(3, 9)$ to Bob.

   (d) Bob received the point $(3, 9)$ from Alice. this is $a^{-1}(ab)M = bM$.
   He retrieves the message M by doing $b^{-1}(bM)$ i.e.
   $11^{-1}(3, 9) = 5(3, 9) = (6, 2)$.

Verify all the computations.

Elliptic Curve ElGamal Cryptosystem

1. All user, Alice, Bob, ... agree upon an Elliptic Curve $E = E(\mathbb{F}_q)$, and a point P (called a Base point) on E.

2. To send a message $M \in E$ to a user say Alice, use her public (encrypting) key aP (a is a secretly chosen positive integer by her) as follows:

   (a) Choose a positive integer k. Create a mask by computing the point $k(aP) \in E$.

(b) Hide the message as the point $Q_2 = M + k(aP) \in E$.

(c) Send to Alice the ordered pair of points $(Q_1, Q_2) \in E \times E$ where $Q_1 = kP$.

(d) Alice receives the pair of points (Q_1, Q_2) from Bob. She knows that the message is hidden in the second coordinate point Q_2. She recreates the mask by doing

$$aQ_1 = a(kP) = (ak)P = (ka)P = k(aP) \in E$$

.

(e) Alice retrieves the message from Q_2 by doing

$$\begin{aligned} Q_2 - aQ_1 =& \{M + k(aP)\} - a(kP) \\ =& M + \{k(aP) - a(kP)\} \\ =& M \in E \end{aligned}$$

Example:

1. Let the publicly agreed elliptic curve be

$$E = E(\mathbb{F}_{11}) = \{(x, y) \in \mathbb{F}_{11} \times \mathbb{F}_{11} |\ y^2 = x^3 + 3x + 1\} \cup \{\infty\}$$

and the public base point $P(1, 4) \in E$.

2. Let Alice choose the integer $a = 11$, keep it secret and publish her public (encrypting) key $aP = 11(1, 4) = (6, 9)$.

(a) Choose a positive integer $k = 13$. Create a mask

$$k(aP) = 13(6, 9) = (1, 7).$$

(b) Suppose the message to be sent to Alice is the point $M = (3, 2) \in E$. Hide the message in

$$Q_2 = M + k(aP) = (3, 2) + (1, 7) = (5, 3).$$

(c) Send Alice the ordered pair of points (Q_1, Q_2). Here

$$Q_1 = kP = 13P = 13(1, 4) = (3, 2)$$

and $Q_2 = (5, 3)$. That is the pair $((3, 2), (5, 3)) \in E \times E$ of points $(3, 2)$ and $(5, 3)$ is sent to Alice.

(d) Alice received $(Q_1, Q_2) = ((3,2),(5,3))$. She knows the message M is hidden in the (second coordinate) point $Q_2 = (5,3)$. She recreates the mask. She computes $aQ_1 = 1(3,2) = (1,7)$. This point $aQ_1 = a(kP)$.

(e) Alice retrieves the message by doing

$$Q_2 - aQ_1 = (5,3) - (1,7) = (5,3) + (1,-7) = (5,3) + (1,4) = (3,2)$$

Remark 1: In the Elliptic Curve ElGamal Cryptosystem the creation of mask by Bob $k(aP)$, as well as the recreation of mask by Alice $a(kP)$ uses the Diffie-Hellman Key Exchange.
Remark 2: In the Elliptic Curve Diffie-hellman Key Exchange Protocol (ECDHKEP) on an elliptic curve $\pmod p$ for $p > 3$, say

$$E := \{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p |\ y^2 = x^3 + Ax + B;\ A, B \in \mathbb{F}_p\} \cup \{\infty\}$$

the common knowledge is a point say $K = a(bP) = b(aP) = abP$, where a, b are positive integers, secretly chosen by Alice and Bob. So, if $K = (x,y) \in E$ is the common knowledge, then $x, y \in E$ such that $y^2 = x^3 + Ax + B;\ A, B \in \mathbb{F}_p$. Because x, y satisfy an (elliptic) equation, they are not independent. If an eavesdropper Eve know the x-coordinate of K, then he can compute $y^2 = x_K^3 + Ax_K + B$, since the curve E is a public knowledge. As $\mod p$, half are quadratic residues and half are quadratic non residues. In case of a quadratic residue only two values of y (other $-y$) congruent $\mod p$ are possible and not very difficult to calculate. Thus Eve gets $K = (x_K, y_K)$ or in the worst case $(x_K, -y_k) = -K$. But it hardly makes big difference as K or $-K$ are only two cases of the common knowledge, Eve posses. Therefore, in practical situation, it is enough to send their common knowledge, the x-coordinate only. In that case, they get either (in case of Alice) $\pm a(bP)$ or (in case of Bob) $\pm b(aP)$ i.e. $\pm K$. But in both cases x-coordinate (of K) is same.

Example: recall the curve

$$E = E(\mathbb{F}_{11}) = \{(x,y) \in \mathbb{F}_{11} \times \mathbb{F}_{11} |\ y^2 = x^3 + 3x + 1\} \cup \{\infty\}$$

and the point $P(3,2)$. Suppose Alice and Bob have agreed on these publicly. Let Alice choose and keep it secret the integer $a = 3$, and Bob $b = 5$.
Alice computes $aP = 3P = (0,1)$, and Bob computes $bP = 5P = (6,9)$. Suppose Alice sends to Bob instead the point $(0,1)$, just its x-coordinate i.e.

0, and like wise Bob sends to Alice only the x-coordinate of bP i.e. 6. Alice received from Bob only the x-coordinate say $x_B = 6$. The corresponding y_B satisfies

$$\begin{aligned} y_B^2 + x_B^3 + 3x_b + 1 \pmod{11} &\implies y_B^2 = 6^3 + 3\dot{6} + 1 \\ &\equiv 235 \equiv 4 \pmod{11} \\ &\implies y_B = \pm 2 \pmod{11} \\ &\implies y_B = 2 \text{ or } -2 \end{aligned}$$

Hence the point, she may assume sent by Bob to be

$$B(6, 2) \text{ or } B(6, -2) = (6, 9)$$

Similarly, Bob may assume the point sent by Alice $A(0, 1)$ or $(0, 10)$ This happened in their first exchange i.e. the points (bP) and (aP) as sent by Bob to Alice and by Alice to Bob respectively.
In the next and final round, Alice computes aB (or $-aB$ as the other possibility) i.e. $3(6, 2)$ or $-3(6, 2)$ [and 5(0,1) or 5(0,10) by Bob].
Observe that

$$3(6, 2) = (0, 1);\ -3(6, 2) = 3(6, -2) = 3(6, 9) = (0, 10)$$

Hence common knowledge by Alice calculation is $(0, 1)$ or (0,10).
Similarly, the common knowledge by Bob calculation is

$$5(0, 1) = (0, 10) \text{ or } -5(0, 1) = 5(0, 10) = (0, 1).$$

So their common point is $(0, 1)$ or (0,10). They are additive inverse of each other, make no difference as long as their common knowledge which is x-coordinate is concerned.

Message mapping on an Elliptic Curve

Since the plain text space as well as the cipher text space is the group E of the points of an elliptic curve, it requires a method by which normal message units are mapped onto a point in E, and vice versa while decryption. This can be done b several ways.

(1). Pre-arranged table between message units and points on E. For example consider the elliptic curve

$$E = E(\mathbb{F}_{11}) = \{(x, y) \in \mathbb{F}_{11} \times \mathbb{F}_{11} |\ y^2 = x^3 + 3x + 1\} \cup \{\infty\}$$

We know that $\#(E) = 18$. So we can map 18-message units to 18 points of E and vice versa.
For example, the English Language letters 'A,B,C,D,E,F,G,,I,J,K,L,M,N,O,P,Q,R' can be put into one-one correspondence with points of E.
The problem is that the one-one correspondence putting message units with points on an elliptic curve has to be shared by the users.

Exercises (1). set up Diffie-Hellman Key Exchange Protocol on the elliptic curve E of discussed above and use to communicate letters 'A' to 'R' only.
(2). Explain Massey-Omura cryptosystem by an example using letters, 'A' to 'R' only.
(3). Discuss ElGamal cryptosystem to encrypt and decrypt a message using letters 'A' to 'R' by mapping them on the elliptic curve E, of the above discussion.

(2). Koblitz Method
In Koblitz method message units are already represented by an integer $m \pmod p$, where $p > 3$ is a prime. To map the integer m on to a point P on the elliptic curve $E := \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p |\ y^2 = x^3 + Ax + B;\ A, B \in \mathbb{F}_p\} \cup \{\infty\}$, look for a point$P(x, y) \in E$ if there is any such that $x = m$. If there is no such point, look for the points $(m + 1, y), (m + 2, y), \ldots$ (a value of y) such that $(m + j, y) \in E$. The integer m is represented by that corresponding point on E.
If the probability of failure acceptable is $\frac{1}{2^k}$, then for the message (represented by the integers) $m : 0 \leq m < \frac{p}{k}$, let $x_j = j = j + mk$ $(0 \leq j < k)$. For these values of $j = 0, 1, 2, \ldots k - 1$ compute

$$\beta_j = x_j^3 + Ax_j + B.$$

If $\beta_j^{\frac{p-1}{2}} \equiv 1 \pmod p$, then β_j is a square $\pmod p$. In that we have got a corresponding point on E. Recall how the square roots modulo a prime are calculated. For example, in case $p \equiv 3 \pmod 4$, a square root $\pmod p$ is

given by $y_j = \beta_j^{\frac{p+1}{4}}$. The point $P_m(x_j, y_j)$ lies on E, and thus can represent m on E. The process is reversible. To retrieve m from $P_m(x_j, y_j)$ is to compute $\left[\frac{x_j}{k}\right]$, the greatest integer less or equal to $\frac{x_j}{k}$. This is m since

$$\begin{aligned} \frac{x_j}{k} =& \frac{mk+j}{k} = m + \frac{j}{k} \ (0 \leq j < k) \\ \implies & \left[\frac{x_j}{k}\right] = m \text{ since } 0 \leq \frac{j}{k} < 1 \end{aligned}$$

Exercise: Let $E = E(\mathbb{F}_{271}) = \{(x, y) \in \mathbb{F}_{271} \times \mathbb{F}_{271} | y^2 = x^3 + 3x + 1\} \cup \{\infty\}$. If it is acceptable that the probability of failure in representing an integer modulo 271 to a point on E can be $\frac{1}{2^{10}}$, then represent English Language letters A to Z, first by representing them by integers $1, 2, \ldots 26$ and then by points on the elliptic curve E.

The Group E of an Elliptic Curve: Order and Structure of E(Some Basic Theorems)

Let $E(\mathbb{F})$ be an elliptic curve defined over a field $\mathbb{F}$. Then an operation, called point addition can be defined with respect to which E becomes an (additive) Abelian group. Further, if $\mathbb{F} = \mathbb{F}_q$ is a finite field, then $E(\mathbb{F}_q)$ is a finite Abelian group, and therefore by the Fundamental Theorem fo Finite Abelian groups, E is isomorphic to a direct product of finitely many cyclic groups of finite order [Prove the theorem].
can there be more information on the structure of E, since E is a particular finite Abelian group?
Yes, indeed. The answer is the following.

Theorem: Let $\mathbb{F}_q$ be a finite field and $E = E(\mathbb{F}_q)$ be the group of points on E. Then either $E \cong C_n$ or $E \cong C_{n_1} \times C_{n_2}$ for some integer $n \geq 1$ or for some integers $n_1, n_2 \geq 1$ and $n_1 \mid n_2$.
since E is an additive Abelian group some authors prefer to write above results as either $E \cong \mathbb{Z}_n$ or $E \cong \mathbb{Z}_{n_1} \bigoplus \mathbb{Z}_{n_2}$, $n, n_1, n_2 \in \mathbb{N}$ and $n_1 \mid n_2$.
We have discussed examples of Elliptic curves of each type.
The next question is about the integers n, n_1, n_2. Can they be precisely determined? or estimated? At least a bound on the order of the E?
Let $\mathbb{F}_q$ be a finite field and $E = E(\mathbb{F}_q)$ be the group of points on elliptic

curve$E$ over the finite field $\mathbb{F}_q$ (So q is a prime or a power of prime). Then the order N =(also denoted by $\#(E)$) of E, satisfies :

$$\#(E) = q + 1 - t_q \text{ where } |t_q| \leq 2\sqrt{q}.$$

Hence $q + 1 - 2\sqrt{q} \leq \#(E) \leq q + 1 + 2\sqrt{q}$. We have used this theorem in some examples to compute the order $\#(E)$.
Can the order be computed precisely? Is there any algorithm? Schoof's algorithm is the answer to count points on E.