Text

Description automatically generatedText, letter

Description automatically generated

A point must satisfy both the equation and condition, then these points are said to be elliptic curve cryptography.

So(2,4) is said to be elliptic curve cryptography.

(x,y) 🡪 can be a real number, complex number or a finite field also.

A picture containing text, sky, white

Description automatically generatedAll the points plotted, will look like this curve.

# **Types of Elliptic Curve**

Diagram

Description automatically generated

A picture containing text

Description automatically generated

# **Elliptic Curve over Finite Field**

We are going to construct an elliptical curve where the values of x and y will be from a finite field.

Text

Description automatically generated with medium confidence

Text, letter

Description automatically generated

Set of all integers under mod 11.

Diagram, polygon

Description automatically generated

This is the modular arithmetic property.

# **Construct an Elliptic Curve over a Finite Field Z/11**

Text, letter

Description automatically generated

With this equation, we are going to find all our points that are used to construct a elliptic curve over a finite field Z/11.

## **Finding the points**

Table

Description automatically generated

Table

Description automatically generated with medium confidence

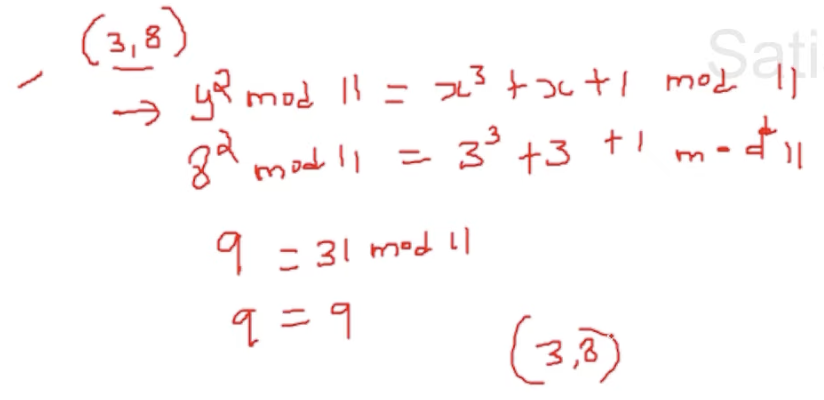
So we have successfully identified all our points to form an elliptic curve that was constructed over set of all integers mod 11.

## **Plotting the points**

Chart, scatter chart

Description automatically generated

## **Check if a point falls on the curve**



These are the points which fall on a elliptic curve.

## **Adding two points on a curve**

What is P+Q provided (P!=Q) ?

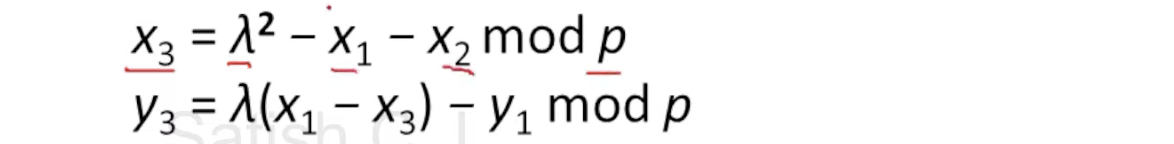
Chart, diagram

Description automatically generated

1. Draw a straight line joining P and Q.
2. The line intersects the curve at a point.
3. Opposite to that point on the X-axis is P+Q (i.e R).

### **Going to find R in a method**

Text

Description automatically generatedGoing to find R(x3,y3).  


What is lambda ??  
Text

Description automatically generated

Lets see an example, We can find the third point(R) by adding P and Q. [P!=Q and Q!= - P]

1. Find lambda
2. Find x3
3. Find y3

Text, whiteboard

Description automatically generated

Text, whiteboard

Description automatically generated

Now we found the point(x3, y3)

### **Checking R(x3, y3)**

Now (x3, y3) = (3,3).  
Lets check whether the points (3,3) lie on the elliptical curve or not ??  
Text, letter

Description automatically generated

How to add 2 points when both are same points ??

