Weierstrass Normal Form

Sayak Chakrabarti
sayak@iitk.ac.in

Recap

Notation 1

The operation $P * Q$

Recap (Contd.)

Notation 2

The **group** operation $P + Q = O * (P * Q)$

Weierstrass Normal Form

Objective:

- Simplify the equation

Weierstrass Normal Form

Objective:

- Simplify the equation

Weierstrass Normal Form

$y^2 = 4x^3 - g_1 x - g_2$

Weierstrass Normal Form

Objective:

- Simplify the equation

Weierstrass Normal Form

$y^2 = 4x^3 - g_1 x - g_2$

Note: Equivalent to $y^2 = ax^3 + bx^2 + cx + d$

Steps of Construction

1 Given Homogeneous Equation
$ax^3 + by^3 + cz^3 + dx^2y + exy^2 + fx^2z + gy^2z + hxz^2 + iyz^2 = 0$

- Use $x \leftarrow \frac{x}{z}, y \leftarrow \frac{y}{z}$

Steps of Construction

1 Given Homogeneous Equation
$ax^3 + by^3 + cz^3 + dx^2y + exy^2 + fx^2z + gy^2z + hxz^2 + iyz^2 = 0$

- Use $x \leftarrow \frac{x}{z}, y \leftarrow \frac{y}{z}$
- Equation:

$$ax^3 + by^3 + dx^y + exy^2 + fx^2 + gy^2 + hx + iy + c = 0$$

Steps of Construction

2 Transformation of Coordinates

Steps of Construction

2 Transformation of Coordinates

- Takes the form $xy^2 + (ax + b)y = cx^2 + dx + e$

Steps of Construction

3 Multiplying by x and substituting $y \leftarrow xy$ we get
$y^2 + (ax + b)y = cx^3 + dx^2 + ex$

Example

- Start with cubic form $u^3 + v^3 = \alpha$; $\alpha \in \mathbb{Q}$

Example

- Start with cubic form $u^3 + v^3 = \alpha$; $\alpha \in \mathbb{Q}$
- Substitute $u \leftarrow \frac{36\alpha+y}{6x}$; $y \leftarrow \frac{36\alpha-y}{6x}$
- New equation $y^2 = x^3 - 432\alpha^2$

But is " $+$ " a group after transformation?

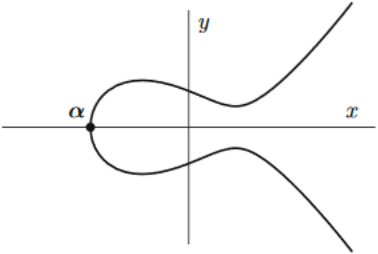
Cubic Curves

Elliptic Curves

Equation of curve: $y^2 = x^3 + ax^2 + bx + c$ such that $f(x) = x^3 + ax^2 + bx + c$ has complex roots as distinct

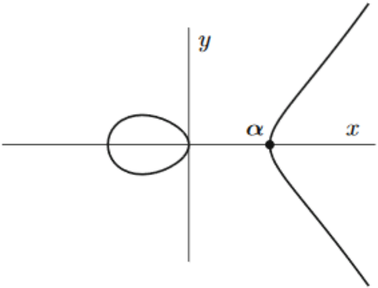
Cubic Curves: Elliptic Curves

- $f(x)$ has only one real root



Cubic Curves: Elliptic Curves

- $f(x)$ has 3 real roots



Cubic Curves: Singular Curves

- $g(x, y) = y^2 - x^3 + ax^2 + bx + c$

Cubic Curves: Singular Curves

- $g(x, y) = y^2 - x^3 + ax^2 + bx + c$
- Singular Point: $\frac{\partial g}{\partial y} = 0$ and $\frac{\partial g}{\partial x} = 0$
  $\implies f(x_0) = 0$ and $f'(x_0) = 0$

Cubic Curves: Singular Curves

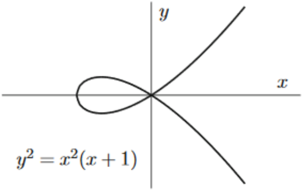
- $g(x, y) = y^2 - x^3 + ax^2 + bx + c$
- Singular Point: $\frac{\partial g}{\partial y} = 0$ and $\frac{\partial g}{\partial x} = 0$
  $\implies f(x_0) = 0$ and $f'(x_0) = 0$

Repeating Root!

Cubic Curves: Singular Curves

Example:

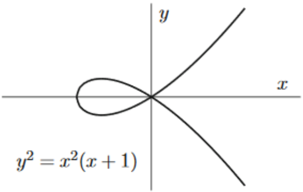
- $y^2 = x^2(x+1)$



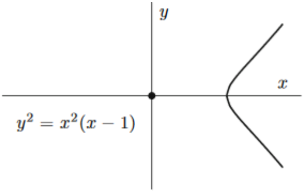
Cubic Curves: Singular Curves

Example:

- $y^2 = x^2(x+1)$



- $y^2 = x^2(x-1)$



Why Singular Curves?

Cubic Curves: Singularity

- Singular Curves: Easy like conics
  - From singular point $\rightarrow$ line, only one point of intersection
  - One-one

Cubic Curves: Singularity

- Singular Curves: Easy like conics
  - From singular point $\rightarrow$ line, only one point of intersection
  - One-one
  - Example: $y^2 = x^2(x+1)$
    Let $r = \frac{y}{x}$, we get $x = r^2 - 1$, $y = r^2 - 1$

Conclusion

- Motivation for studying cubic curves

Conclusion

- Motivation for studying cubic curves
- Group Law for Elliptic Curves

Acknowledgements

Most of the content has been taken from ”Rational Points on Elliptic Curves” by Silverman and Tate.