Introduction to Elliptic Curves

by

Seyyed Mohammad Reza Hashemi Moosavi

Elliptic curves are a special kind of algebraic curves which have a very rich arithmetical structure.

There are several fancy ways of defining them. but for our purposes we can just define them as the set of points satisfying a polynomial equation of a certain form. To be

specific, consider an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where the a_i are integers (There is a reason for the strange choice of indices on the a_i, but we won't go into it here). we want to consider the set of points (x, y) which satisfy

this equation.

To make things easier, let us focus on the special case in which the equation is of the form

$$y^2 = x^3 + Ax^2 + Bx + C = g(x) \quad (*)$$

with $g(x)$ a cubic polynomial (in other words, we're assuming $a_1 = a_3 = 0$). In this case (*), it's very easy to determine when there can be singular points, and even what

sort of singular points they will be. If we put

$$f(x, y) = y^2 - g(x),$$

Then we have

$$\frac{\partial f}{\partial x}(x, y) = -g'(x) \text{ and } \frac{\partial f}{\partial y}(x, y) = 2y,$$

we know, the curve will be smooth if there are no common solutions of the equations

$$f(x, y) = 0 \ , \ \frac{\partial f}{\partial x}(x, y) = 0 \ , \ \frac{\partial f}{\partial y}(x, y) = 0 \quad (**)$$

Attention. we know, from elementary analysis, that an equation $f(x, y) = 0$ defines a smooth curve exactly when there are no points on the curve at which both partial

derivatives of f vanish.

in other words, the curve will be smooth if there are no common solutions of the equations (**).

And the condition for a point to be "bad" be comes

$$y^2 = g(x)\ ,\ -g'(x) = 0\ ,\ 2y = 0$$

which boils down to $y = g(x) = g'(x) = 0$. In other words, a point will be "bad" exactly when its y - coordinate is Zero and its x - coordinate is a double root of the

polynomial $g(x)$. since $g(x)$ is of degree 3, this gives us only three possibilities:

- **$g(x)$ has no multiple roots, and the equation defines an elliptic curve (Three distinct roots), (For example, elliptic curve $y^2 = x^3 + x$ has three distinct roots).**
- **$g(x)$ has a double root (curve has a node), (For example, curve $y^2 = x^3 + x^2$ has a node).**
- **$g(x)$ has a triple root (curve has a cusp), (For example, curve $y^2 = x^3$ has a cusp).**

Attention. If x_1, x_2 and x_3 are the roots of the polynomial $g(x)$, the discriminant for the equation $y^2 = g(x)$ turns out to be $(g(x) = 0)$

$$\Delta = k(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$$

where k is a constant.

This does just what we want:

If two of the roots are equal, it is Zero, and if not, not. Further more, it is not too hard to see that Δ is actually a polynomial in the coefficients of $g(x)$, which is what we

claimed. In other words, all the discriminant do for us is giving a direct algebraic procedure for determining whether there are singular points.

while this analysis applies specifically to curves of the form $y^2 = g(x)$, it actually extends to all equations of the sort we are considering there is at most one singular point

and it is either a node or a cusp.

Attention. with some examples in hand, we can proceed to deeper waters. In order to understand the connection we are going to establish between elliptic curves and Fermat's

Last Theorem, we need to review quite a large portion of what is known about the rich arithmetic structure of these curves.

Conclusion. Elliptic curve of the form

$$y^2 = x^3 + Ax^2 + Bx + C = g(x)$$

is a elliptic curve of Non – Singular if $g(x)$ has not a double root or

a triple root. In fact below equation

$$g(x) = x^3 + Ax^2 + Bx + C = 0$$

has three distinct roots, if

$$\Delta_{HM} = (AB - 9C)^2 - 4(A^2 - 3B)(B^2 - 3AC) \neq 0$$

Attention. If $\Delta_{HM} \neq 0$ then $g(x)$ has no multiple roots, and $y^2 = g(x)$ is a

Non –Singular cubic elliptic curve.

✶✶✶3 New Proof of Fermat's last Theorem by HM Final Main Theorem✶✶✶

by

Seyyed Mohammad Reza Hashemi Moosavi

- **HM Final – Main Theorem**

For every odd number $P \geq 3$ Fermat's Last Theorem ($abc \neq 0$):

$$a^P + b^P = c^P$$

Special case is of an elliptic curve (Non – Singular Cubic Curve) HM:

$$H^2 = M^3 + (3S^P)M^2 + (3S^{2P})M + (S^{3P} + S^P) \quad (*)$$

- **Proof:**

It is enough in the below general elliptic curve:

$$y^2 = x^3 + Ax^2 + Bx + C \quad (**)$$

Or elliptic curve HM (*) we assume:

$$y = H = \left(ac^{\frac{3P-5}{2}}\right)^{P}$$
$$x = M = \left(ac^{P-2}\right)^{P} - \left(a^{2}bc^{3P-6}\right)^{P}$$
$$A = 3\ S^{P} = 3\left(a^{2}bc^{3P-6}\right)^{P}$$
$$B = 3\ S^{2P} = 3\left(a^{2}bc^{3P-6}\right)^{2P}$$
$$C = S^{3P} + S^{P} = \left(a^{2}bc^{3P-6}\right)^{3P} + \left(a^{2}bc^{3P-6}\right)^{P}$$

then after replacing in (*) or (**):

(odd numbers) $P \geq 3\ :\ a^{P} + b^{P} = c^{P}$

Attention:

- **Elliptic curve (*) is Non – Singular.**
- **First Fermat's equation is multiplied** λ_{HM}.
- **We assume** $R = M + S^{P}\ \left(R^{3} + S^{P} = H^{2}\right)$.
- **We know that Proofed** $x^{3} + y^{3} = z^{3}$ **is an elliptic curve.**

New Proof of Fermat's Last Theorem by HM Final – Main Theorem

Because: $y^{2} = x^{3} + Ax^{2} + Bx + C$;

$$H^{2} = M^{3} + \left(3S^{P}\right)M^{2} + \left(3S^{2P}\right)M + \left(S^{3P} + S^{P}\right);$$

$$H^{2} = \left(M^{3} + 3S^{P}M^{2} + 3S^{2P}M + S^{3P}\right) + S^{P};$$

$$H^{2} = \left(M + S^{P}\right)^{3} + S^{P};$$

$$\left|\begin{array}{l} H = \left(ac^{\frac{3P-5}{2}}\right)^{P} \\ M = \left(ac^{P-2}\right)^{P} - \left(a^{2}bc^{3P-6}\right)^{P} \\ S = \left(a^{2}bc^{3P-6}\right) \end{array}\right.$$

$$M + S^{P} = \left(ac^{P-2}\right)^{P} - \left(a^{2}bc^{3P-6}\right)^{P} + \left(a^{2}bc^{3P-6}\right)^{P} = \left(ac^{P-2}\right)^{P}$$

$$H^{2} = \left(ac^{P-2}\right)^{3P} + \left(a^{2}bc^{3P-6}\right)^{P} = \left(ac^{\frac{3P-5}{2}}\right)^{2P};$$

(odd numbers) $P \geq 3 : \left(ac^{P-2}\right)^{3P} + \left(a^{2}bc^{3P-6}\right)^{P} = \left(a^{2}c^{3P-5}\right)^{P};$

$$a^{3P}c^{3P^{2}-6P} + a^{2P}b^{P}c^{3P^{2}-6P} = a^{2P}c^{3P^{2}-5P};$$

$$a^{2P}c^{3P^{2}-6P}\left[a^{P} + b^{P} = c^{P}\right];$$

$$\left(\lambda_{HM} = a^{2P}c^{3P^{2}-6P}\right);$$

$$abc \neq 0 : a^{P} + b^{P} = c^{P}$$

Attention:

- **Elliptic curve HM (*) is non – Singular, because:**

$$M^{3} + \left(3S^{P}\right)M^{2} + \left(3S^{2P}\right)M + \left(S^{3P} + S^{P}\right) = 0 \;;$$

$M_{1} = -S^{P} - \sqrt[3]{S^{P}}\ ,\ M_{2,3} = \alpha \pm i\beta$ **(Three different roots)**

- **References**

[1] S. M. R. Hashemi Moosavi, The Discovery of Prime Numbers Formula & It's Results (2003). (ISBN: 978-600-94467-9-7).

[2] S. M. R. Hashemi Moosavi, Generalization of Fermat's Last Theorem and Solution of Beal's Equation by HM Theorems (2016). (ISBN: 978-600-94467-3-5).

[3] S. M. R. Hashemi Moosavi, 31 Methods for Solving Cubic Equations and Applications (2016). (ISBN: 978-600-94467-7-3).