NUMERICAL EXPLORATIONS OF ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

RAYA BAYOR; IBRAHIMA DIEDHIOU
MENTOR: PROF. JORGE PINEIRO

1. Presentation of the problem

The present project constitutes a numerical exploration of elliptic curves. An elliptic curve E over $\mathbb{Z}$ is given by an equation of the sort

$$E : y^2 = x^3 + px + q,$$

where the coefficients $p, q \in \mathbb{Z}$, and the polynomial $x^3 + px + q$ has no repeated roots, plus a point o at infinity. For example curves given by equations $y^2 = x^3 + 16$ or $y^2 = x^3 + x$, represent elliptic curves.
It is a natural operation to reduce the coefficients p, q module a prime l and study all possible solutions of the reduced curve over the field $\mathbb{Z}/l$. A deep theorem of Number Theory states that the amount of solutions should "be close to" l. For example the elliptic curve $y^2 = x^2 + 16$ when you reduce mod 2, takes the shape $y^2 = x^3$ and has only two solutions $(0, 0)$ and $(1, 1)$. Another example could be seen with the curve $y^2 = x^3 + x$ and the prime $l = 3$. The curve stays the same $y^2 = x^3 + x$ module 3 and we find the solutions $(0, 0); (1, 1); (2, 1)$. The examples above were carefully chosen and we should not expect the number of solutions to be exactly l in many cases, but on the contrary attached to very special types of elliptic curves. Of course we need a precise definition for the words "be close to". The mathematical statement says:

Theorem 1.1. *If E is an elliptic curve and N_l is the number of solutions of E module the prime l, then*

$$\|N_l - l\| \leq 2\sqrt{l}.$$

The term $a_l = N_l - l$ is called the l-defect of E. It plays an important role in relation to the analytic theory of the curve.

Definition 1.2. *A prime $l \neq 2, 3$ is called supersingular for the elliptic curve E if $a_l = 0$.*

FIGURE 1. Addition Law on Elliptic Curve $y^2 = x^3 - x$

2. Addition law and self-maps

Let $E : y^2 = x^3 + px + q$ be an elliptic curve. We can define an operation $\oplus$ on E, such that if we take $o = \infty = (0 : 1 : 0) \in E$, will satisfy the following properties:

(i) $\forall P, Q \in E,\ P \oplus Q = Q \oplus P$.
(ii) $\forall P \in E,\ P \oplus o = o \oplus P$.
(iii) $\forall P \in E$, there exist $-P$ such that $P \oplus -P = -P \oplus P = o$.
(iv) $\forall P, Q, R \in E,\ (P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

In the language of group theory we say that $(E, \oplus, o)$ is an Abelian group with neutral element o. As a consequence, an elliptic curve E comes always equipped with self-maps $[n] : E \to E$, representing multiplication by the different integers. For example the map $[2]P = P \oplus P$. For the elliptic curve $y^2 = G(x) = x^3 + px + q$ and a point $P = (x, y) \in E$ with $y \neq 0$, this map is expressed as

$$[2](x,y) = \Big(\frac{G'(x)^2 - 8xG(x)}{4G(x)}, \frac{G'(x)^3 - 12xG(x)G'(x) + 2G(x)}{8G(x)y}\Big).$$

The map $[n] : E \to E$ has degree n^2 for each n. All this maps commute, that is, $[n] \circ [m] = [m] \circ [n] = [n.m]$ and $[n](x, y)_x$ depends only on the x coordinate, not on y.

Question 2.1. *Does E has other self-maps, different from the $[n] : E \to E$ maps?*

Answer 2.2. *Sometimes Yes!!! For example the elliptic curve $E_1 : y^2 = x^3 + x$ has the automorphism $f(x, y) = (-x, iy)$ over the complex numbers. The ring of endomorphism in this case is $\mathbb{Z} + \mathbb{Z}i$.*

Definition 2.3. *An elliptic curve with at least one map $f : E \to E$, not equal to $[n] : E \to E$ for any n is called an elliptic curve with complex multiplication.*

In general we should expect that most elliptic curves do not have complex multiplication. The following result relate the concept of complex multiplication with the l-defects of the curve.

Proposition 2.4. *(Serre [?]) If E has no complex multiplication then the set of supersingular primes has density zero.*

This is a surprising result relating the theory of complex multiplication to the reduction of the curve module a prime.

3. Examples

In the following table we try to identify candidates with complex multiplication based on the theorem of Serre. We look for numerical evidences of the existence of a set of supersingular primes with positive density.

E	$N_l = l/l < 100$	$N_l = l/l < 1000$
$y^2 = x^3 + x$	.52	.518
$y^2 = x^3 - 4x^2 + 16$	.08	.03
$y^2 = x^3 + 2x - 7$	.08	.03
$y^2 = x^3 + 1$	.52	.518
$y^2 = x^3 + 4x^2 + 2x$	.48	.512
$y^2 + y = x^3 - x^2 - 7x + 10$	.48	.50
$y^2 = x^3 + 6x^2 + 74x + 72$	.04	.006
$y^2 = x^3 + 23x^2 + 75x - 92$	.12	.05
$y^2 = x^3 - 40x^2 + 42x - 50$	.08	.041
$y^2 + y = x^3 - 38x + 90$	.56	.50
$y^2 + y = x^3 - 860x + 9707$	.44	.49

The results show how that the elliptic curves with affine Weierstrass equations

$$\begin{gathered} y^2 + y = x^3 - 860x + 9707, \\ y^2 + y = x^3 - 38x + 90, \\ y^2 + y = x^3 - x^2 - 7x + 10, \\ y^2 = x^3 + 4x^2 + 2x, \\ y^2 = x^3 + 1, \end{gathered}$$

are also likely to have complex multiplication.

4. Modular forms

Modular forms are very important analytic objects which are at the center of the modern number theory.

Definition 4.1. *Let's denote by $\mathcal{H}$ the upper half-plane $\mathcal{H} = \{z = x + iy \in \mathbb{C} : y > 0\}$. A holomorphic function $f : \mathcal{H} \to \mathbb{C}$ is a modular form of weight k and level $N \geq 1$ if it satisfies a relationship*

$$f\Big(\frac{Az+B}{CNz+D}\Big) = \frac{1}{(CNz+D)^k} f(z)$$

for some integers A, B, C, D with $AD - BCN = 1$ and all $z \in \mathcal{H}$.

For example suppose that we take $q = \exp(2\pi i\tau)$, then the Delta function $\Delta(\tau) = \prod_{r=1}^{\infty}(1-q^r)^{24}$ is a modular form of weight $k = 12$ and level $N = 1$. The Δ function is essentially the first object that we find when study the level $N = 1$. The Fourier expansion of Δ is

$$\Delta = (2\pi)^{12} \sum_n \tau(n) q^n,$$

and there are many interesting properties of the numbers $\tau(n)$. For example a conjecture of Lehmer states that $\tau(n) \neq 0$ for all n.

Definition 4.2. *Let's put $q = \exp(2\pi iz)$. A series $\sum_i b_i q^i$ is said to exhibit a modularity pattern if there exist a modular eigenform $\sum_i c_i q^i = f(z)$ of weight 2 and level N such that for all primes $l, l \nmid N$, we have $b_l = c_l$.*

The term "eigenform" in the definition refers to the fact that $f(z)$ is a special kind of modular form, namely, eigenvector for a system of operators called the Hecke Operators on modular forms.

4.1. Modular forms and Elliptic curves.

Suppose that we have an elliptic curve E. We can build a series, called the L-function $L(q, E) = \sum_i a_i q^i$ attached to E, having $a_l = l$-defect of E for all primes l.

Theorem 4.3. *(Modularity Theorem) Suppose that E is an elliptic curve defined over $\mathbb{Q}$ and with conductor N, then the L-function $L(q, E) = \sum_i a_i q^i$, associated to E, exhibit a modularity pattern.*

We can look at Lehmer question in the context of elliptic curves. For elliptic curves with complex multiplication approximately half the a_l are zero, on the other hand a Theorem of Noam Elkies states that there are infinitely many l with $a_l = 0$, even for elliptic curves without complex multiplication.

$E : y^2 = x^3 + x$	
a_5	1
a_7	0
a_{11}	5
a_{13}	2
a_{17}	-6
a_{19}	-2
a_{23}	3
a_{29}	-10
a_{31}	-7
a_{37}	-4
a_{41}	7
a_{43}	9
a_{47}	0
a_{53}	-2
a_{59}	-8
a_{61}	-1
a_{67}	-10
a_{71}	-12
a_{73}	-11
a_{79}	8
a_{83}	2
a_{89}	3
a_{97}	7

$E : y^2 = x^3 + 7x - 1$	
a_5	-1
a_7	4
a_{11}	3
a_{13}	-2
a_{17}	-6
a_{19}	1
a_{23}	8
a_{29}	-3
a_{31}	-6
a_{37}	-6
a_{41}	5
a_{43}	8
a_{47}	0
a_{53}	2
a_{59}	-12
a_{61}	6
a_{67}	8
a_{71}	8
a_{73}	-3
a_{79}	1
a_{83}	9
a_{89}	7
a_{97}	-8

$E : y^2 = x^3 + 4x^2 + 2x$	
a_5	0
a_7	0
a_{11}	-6
a_{13}	0
a_{17}	-6
a_{19}	-2
a_{23}	0
a_{29}	0
a_{31}	0
a_{37}	0
a_{41}	6
a_{43}	10
a_{47}	0
a_{53}	0
a_{59}	-6
a_{61}	0
a_{67}	14
a_{71}	0
a_{73}	-2
a_{79}	0
a_{83}	-18
a_{89}	-18
a_{97}	10

References

[1] J. P. Serre, *Groupes de Lie l-Adiques attachés aux courbes elliptiques*, Colloque de Clermont-Ferrand, IHES, 1964.

[2] M. Hindry and J. Silverman, *Diophantine Geometry: an introduction*, Graduate Texts in Mathematics 201, 2000.

[3] J. Silverman, *A friendly introduction to Number Theory*, Third edition, Pearson Prentice Hall, 2006.

[4] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, 1986.

BCC.University Ave. and West 181 Street. Bronx, NY 10453