Lecture 5

Elliptic curves over $\mathbb{Q}$

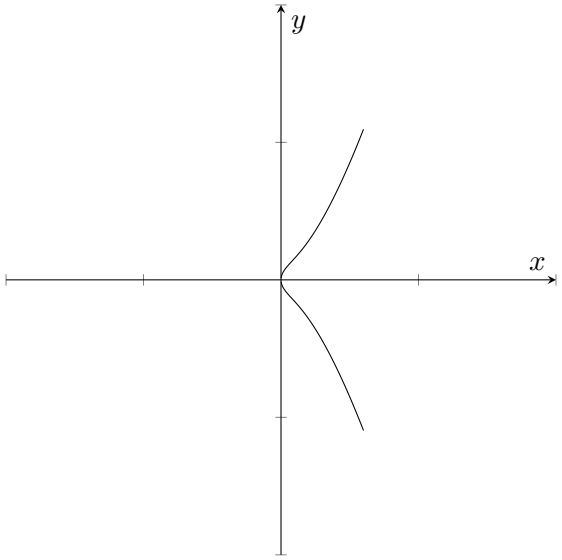
In this lecture, we turn our focus to elliptic curves and modular curves over $\mathbb{Q}$. As a reminder, if K is a subfield of $\mathbb{C}$ (or more generally, a field of characteristic not 2 or 3), then E/K can be described by an equation

$$y^2 = x^3 + Ax + B,$$

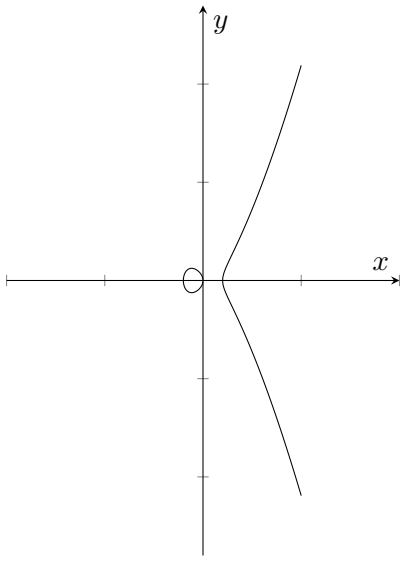
where $A, B \in K$ and $-16(4A^3 + 27B^2) \neq 0$.

Remark 1 *If $K = \mathbb{Q}$, by making the substitutions $X = d^2x$ and $Y = d^3y$, we obtain the equation $Y^2 = X^3 + d^4AX + d^6B$; in this way, we may clear denominators and assume that an elliptic curve $E/\mathbb{Q}$ is defined by an equation with $A, B \in \mathbb{Z}$.*

Over $\mathbb{C}$, two elliptic curves E and E' are isomorphic if and only if $j(E) = j(E')$. Over a non-algebraically closed field, this is not true. Consider for example the curves $E : y^3 = x^3 + x$ and $E' : y^2 = x^3 - x$. Over $\mathbb{R}$, E has only one connected component while E' has two; thus they are not isomorphic over $\mathbb{R}$, despite the fact that $j(E) = j(E') = 1728$.



$E : y^2 = x^3 + x$.



$E' : y^2 = x^3 - x$

Recall from the first lecture that if $E/\mathbb{R}$ is an elliptic curve, then given points $P, Q \in E(\mathbb{R})$ the line that contain P and Q will intersect E at a third point R. If $R = (x_0, y_0)$, we define $P + Q = (x_0, -y_0)$. Thus the points P, Q, and R satisfy $P + Q + R = \mathcal{O}$, where $\mathcal{O}$ (the point at infinity) serves as the identity for the group law. If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ with $x_i, y_i \in \mathbb{Q}$, then the third point of intersection $R = (x_3, y_3)$ will also have $x_3, y_3 \in \mathbb{Q}$, so this same process works to give $E(\mathbb{Q})$ the structure of an abelian group as well. (Indeed, if K is a field and E/K an elliptic curve, the points $E(K)$ form an abelian group; the group law can be described using explicit formulas.)

In 1908, Poincare conjectured (by way of tacit assumption) that $E(\mathbb{Q})$ was a finitely generated abelian group for any elliptic curve $E/\mathbb{Q}$. This conjecture was proved by Mordell in 1922 and vastly generalized by Weil in 1928.

Theorem 2 (Mordell-Weil) *Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is a finitely generated abelian group.*

This means that $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$, where $r \geq 0$ is an integer (known as the rank of the curve), and T is a finite abelian group. In other words, there is a finite set of points $P_1, P_2, \ldots, P_s$ such that every point $P \in E(\mathbb{Q})$ can be expressed as

$$P = n_1 P_1 + n_2 P_2 + \cdots + n_s P_s, \; n_i \in \mathbb{Z}$$

Remark 3 *Abelian varieties are higher dimensional analogues of elliptic curves. Weil's generalization states that for an abelian variety A defined over a number field K (a finite degree extension of $\mathbb{Q}$), $A(K)$ is a finitely generated abelian group.*

A natural question which presents itself is this: What groups can $E(\mathbb{Q})$ actually be? There are two parts to this question. First, what are the possibilities for the integer r? Second, what finite abelian groups T are possible? While there are many open questions about r (including whether there is some constant M such that the rank $r \leq M$ for every elliptic curve $E/\mathbb{Q}$), we have a complete classification for the possible torsion subgroups T.

Theorem 4 (Mazur) *Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup T of E is isomorphic to one of the following groups:*

$\mathbb{Z}/N\mathbb{Z}$ *with* $1 \leq N \leq 10$ *or* $N = 12$,

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ *with* $1 \leq N \leq 4$.

To prove this result, Mazur determined the $\mathbb{Q}$-rational points on $X_1(N)$ for all N ([3]).

Modular Curves over $\mathbb{Q}$

Our focus has been on the curves $Y(N), Y_1(N), Y_0(N)$ and their compactifications $X(N), X_1(N)$, and $X_0(N)$. We saw in the previous lecture that points of the curves $Y(N), Y_1(N)$, and $Y_0(N)$ correspond to isomorphism classes of elliptic curves $E/\mathbb{C}$ with torsion data. A point of $Y(N)$ corresponds to an isomorphism class of a triple $[E, P, Q]$ where P and Q are a basis for $E[N]$ and $e_N(P, Q) = e^{2\pi i/N}$, where e_N denotes the Weil. A point on $Y_1(N)$ corresponds to a pair $[E, P]$, where P is a point of E of order N. A point on $Y_0(N)$ corresponds to a pair $[E, C]$ where C is a cyclic subgroup of E of order N.

For each $N \in \mathbb{Z}^+$, we have $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N)$. This gives rise to natural surjections

$$Y(N) \to Y_1(N) \to Y_0(N)$$

$$\Gamma(N)\tau \mapsto \Gamma_1(N)\tau \mapsto \Gamma_0(N)\tau$$

These maps have an interpretation as "forgetful" maps:

$$[E, P, Q] \mapsto [E, Q] \mapsto [E, \langle Q \rangle]$$

(in the last map, $\langle Q \rangle$ is a cyclic subgroup of E of order N; the map "forgets" the torsion point Q, but "remembers" the cyclic subgroup it generates).

Each of the curves $X(N), X_1(N)$, and $X_0(N)$ can be defined over $\mathbb{Q}$. For $X_1(N)$ and $X_0(N)$, there are canonical models defined over $\mathbb{Q}$ (in the sense of [7, §6.7]), however the canonical model for $X(N)$ is defined over the field $\mathbb{Q}(\zeta_N)$, where ζ_N denotes a primitive N-th root of unity. When $N > 2$, this is a proper extension of $\mathbb{Q}$. The noncuspidal $\mathbb{Q}$-rational points of these curves still carry N-torsion data (when they exist), but the interpretations of points on $X(N)$ and $X_0(N)$ are not as straight-forward as they are over $\mathbb{C}$. While we will not give an interpretation for noncuspidal $\mathbb{Q}$-rational points on $X(N)$, we will however discuss what $\mathbb{Q}$-rational points of $Y_1(N)$ and $Y_0(N)$ represent.

Theorem 5 *A point $x \in Y_1(N)(\mathbb{Q})$ is represented by a pair $[E, P]$, where $E/\mathbb{Q}$ is an elliptic curve and $P \in E(\mathbb{Q})$ is a point of order N. A point $x \in Y_0(N)(\mathbb{Q})$ is represented by a pair $[E, C]$, where $E/\mathbb{Q}$ is an elliptic curve and C is a cyclic subgroup of E which is rational over $\mathbb{Q}$.*

Remark 6 *This theorem holds for fields other than $\mathbb{Q}$ ([6, Thm. 1]). If K is a field of characteristic not dividing N, then K-rational points of $Y_1(N)$ or $Y_0(N)$ are represented by $[E, P]$ or $[E, C]$ (respectively) where $P \in E(K)$ or E and C are defined over K (respectively).*

It is important to note that while C is a $\mathbb{Q}$-rational subgroup of E, this does not necessarily mean that $C \subseteq E(\mathbb{Q})$. Rather, it means that there is an isogeny $\phi : E \to E'$ defined over $\mathbb{Q}$ such that $C = \ker(\phi)$. Indeed, there is another way of understanding points of $Y_0(N)$: each point of $Y_0(N)$ corresponds to a triple $[E, E', \phi]$ where $\phi : E \to E'$ is an isogeny such that $\ker(\phi)$ is a cyclic group of order N.

Remark 7 *The curves $Y(N), Y_1(N)$ and $Y_0(N)$ are moduli spaces for moduli problems determining isomorphism classes of elliptic curves with certain N-torsion data. $Y_0(N)$ is always a coarse moduli space: its K-points classify elliptic curves with cyclic N-isogenies up to $\bar{K}$-isomorphism. The same is true for $Y(N)$ for $N \leq 2$ and for $Y_1(N)$ for $N \leq 3$.*

Mazur's theorem 4 was first proved in [3]; in [4], Mazur gave a second proof. In this case, the proof was a consequence of the following theorem ([4, Thm. 7.1]:

Theorem 8 (Mazur) *Let N be a prime number such that the genus of $X_0(N)$ is > 0 (i.e., $N = 11$ or $N \geq 17$). Then there are no elliptic curves over $\mathbb{Q}$ possessing $\mathbb{Q}$-rational N-isogenies except when $N = 11, 17, 19, 37, 43, 67,$ or 163. Equivalently, there are no noncuspidal $\mathbb{Q}$-rational points on $X_0(N)$ except for the above values of N.*

A (very) brief word about Fermat's Last Theorem

Modular curves feature in the proof of one of the most famous results in number theory, and we would be remiss if we said nothing of the connection. Fermat (some time around 1637) made the following claim:

Fermat's Last Theorem *Let $n \geq 3$. Then the are no solutions $x, y, z \in \mathbb{Z}$ to $x^n + y^n = z^n$ for which $xyz \neq 0$.*

In 1984, Frey suggested that Fermat's Last Theorem might follow from what would eventually be known as the modularity theorem. Serre gave a partial proof to link the two results, and Ribet (in proving the ϵ conjecture/ Ribet's Theorem) provided the final link. Wiles presented an argument to prove the modularity conjecture, but there was gap in the argument. Wiles and Taylor subsequently provided an alternative argument which completed the proof of the modularity theorm in the case needed to prove Fermat's Last Theorem. The modularity theorem was then proved in full by Breuil, Conrad, Harris, and Taylor.

We state the Modularity Theorem below, and refer the reader to [1] for a brief explanation of the history of the statement:

Theorem 9 (Modularity Theorem, Wiles et. al.) *If $E/\mathbb{Q}$ is an elliptic curve, then there is an integer N and a surjective morphism $\phi : X_0(N) \to E$ defined over $\mathbb{Q}$.*

Further Reading

This lecture series was intended to give an overview of modular curves; there were therefore many results which we did not prove in full and many ideas we did not explore. My hope is that you have encountered something new that you would like to learn more about. To that end, I include some references below that cover some of the material from this lecture series in more depth.

Complex Analysis and Riemann Surfaces

- *Complex Analysis.* Ahlfors
- *Riemann Surfaces and Algebraic Curves: A First Course in Hurwitz Theory.* Cavalieri and Miles.
- *Riemann Surfaces, Second Ed.* Farkas and Kra.

Modular Curves

- *A First Course in Modular Forms.* Diamond and Shurman.
- *Modular Functions and Modular Forms.* Milne.
- *Introduction to the Arithmetic Theory of Automorphic Forms.* Shimura.
- *18.783 Elliptic Curves. Spring 2019. Massachusetts Institute of Technology: MIT OpenCourseWare.* Sutherland

Elliptic Curves

- *The Arithmetic of Elliptic Curves.* Silverman.
- *Advanced Topics in the Arithmetic of Elliptic Curves.* Silverman.
- *18.783 Elliptic Curves. Spring 2019. Massachusetts Institute of Technology: MIT OpenCourseWare.* Sutherland

Thank you

I want to say thank you to everyone who took the time to watch the lectures, to read these notes, and to offer feedback. Thank you to the organizers, Alina, Bryden, Kiran, and DZB for organizing this Virtual School. Last - but by no means least - many thanks to Tyler Genao, Hyun Jong Kim, Zonia Menendez, and Sam Mundy for the considerable time, effort, planning, and thought you each put in to developing the problem sets, and thank you as well for your helpful suggestions.

References

[1] Clark, P.L., `http://alpha.math.uga.edu/~pete/modularandshimura.pdf`

[2] Diamond, F. and Shurman, J. *A First Course in Modular Forms.* Springer 2016, 4th. printing.

[3] Mazur, B. *Modular curves and the Eisenstein ideal.* Publ. Math. I.H.E.S. 47 (1977)

[4] Mazur, B. *Rational isogenies of prime degreel.* Invent. Math. 44, 129-162 (1978) 437–449.

[5] Milne, J.S., *Modular Functions and Modular Forms.* `https://www.jmilne.org/math/CourseNotes/mf.html`

[6] Ogg, A. *Diophantine equations and modular forms.* Bull. Soc. Math. France 102, 449-462 (1974)

[7] Shimura, G. *Introduction to the Arithmetic Theory of Automorphic Functions.* Kanô Memorial Lectures, no. 1, Publ. Math. Soc. Japan, no. 11, Princeton Univ. Press, 1971.

[8] Silverman, J. *The Arithmetic of Elliptic curves, second edition.* Springer 2009.