Attribution Key

for more information see: http://open.umich.edu/wiki/AttributionPolicy

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

Public Domain – Government: Works that are produced by the U.S. Government. (17 USC § 105)

Public Domain – Expired: Works that are no longer protected due to an expired copyright term.

Public Domain – Self Dedicated: Works that a copyright holder has dedicated to the public domain.

Creative Commons – Zero Waiver

Creative Commons – Attribution License

Creative Commons – Attribution Share Alike License

Creative Commons – Attribution Noncommercial License

Creative Commons – Attribution Noncommercial Share Alike License

GNU – Free Documentation License

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

Public Domain – Ineligible: Works that are ineligible for copyright protection in the U.S. (17 USC § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

Fair Use: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (17 USC § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

Lecture 1: Overview

In the first lecture, I give an introduction to Mazurs theorem, including a sketch of the proof. The purpose of this course is to develop these ideas in more detail. I also talk a little about some related results: Serres uniformity theorem and Merels uniform boundedness theorem.

1 Mazur's theorem

Consider the following problem:

Problem 1. *Let $f \in \mathbf{Q}[x,y]$ be a polynomial. Describe the set of points $(x,y) \in \mathbf{Q}^2$ such that $f(x,y)=0$.*

This can be phrased (almost) equivalently as:

Problem 2. *Let $C/\mathbf{Q}$ be an algebraic curve (connected, smooth, projective). Describe the set $C(\mathbf{Q})$.*

This is an extremely fundamental problem, and cases of it have been considered for thousands of years. Much about this problem has been discovered in the last century. The first thing to mention, probably, is the fundamental trichotomy depending on the genus of C:

- Genus 0. There are two possibilities: either C has no rational points, or C is isomorphic to $\mathbf{P}^1$, in which case it has infinitely many rational points, and these points form a 1-parameter algebraic family.
- Genus 1. If C is non-empty then $C(\mathbf{Q})$ has the structure of a finitely generated commutative group. The hard part of this statement (the finite generation) is Mordell's theorem, from 1922. (According to that link, it was Poincaré who first suggested this result.)
- Genus ≥ 2. the set $C(\mathbf{Q})$ is finite. This is Faltings' theorem (MR0718935), proved in 1983 and first conjectured by Mordell in 1922.

Given these results, one can start to ask more quantitative questions. For example:

Question 3. *How many rational points can a genus 2 curve have?*

It is conjectured that there is an absolute bound, i.e., there exists a number N such that if $C/\mathbf{Q}$ is any genus 2 curve then $\#C(\mathbf{Q}) \leq N$. This has not been proved, however. So far, the record for number of rational points seems to be 642, found by Michael Stoll in 2008. It is worth mentioning here a recent result of Manjul Bhargava: most genus 2 curves have no rational points. The situation in higher genus is similar.

In genus 1, one should not simply ask "how many points" but "what is the structure of the group of points." Suppose C is a genus 1 curve with a point. Then, according to Mordell's theorem, we have a decomposition $C(\mathbf{Q}) = C(\mathbf{Q})_{\mathrm{tors}} \times \mathbf{Z}^r$, where $C(\mathbf{Q})_{\mathrm{tors}}$ is a finite abelian group (the torsion subgroup) and $r \geq 0$ is an integer, called the rank. So, one would like to know the possibilities for r and $C(\mathbf{Q})_{\mathrm{tors}}$.

Very little is known about the rank. For instance, it is unknown if it can be arbitrarily large. The current record is $r \geq 28$, found by Noam Elkies in 2006.

The situation is much better for the torsion subgroup; in fact, this is exactly what Mazur's theorem describes:

These are notes for Math 679, taught in the Fall 2013 semester at the University of Michigan by Andrew Snowden.

Theorem 4 (Mazur, 1977, MR488287)**.** *$C(\mathbf{Q})_{\text{tors}}$ is isomorphic to one of the following 15 groups:*

$$\begin{aligned} \mathbf{Z}/n\mathbf{Z} \quad & \text{with } 1 \leq n \leq 10 \text{ or } n = 12 \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \quad & \text{with } n = 2, 4, 6, 8. \end{aligned}$$

Furthermore, each of these groups does occur.

One can view this theorem as a first step to a quantitative answer to the original problem.

2 Overview of the proof

The goal of this course is to prove Mazur's theorem. I'll now give an overview of the proof, which I'll break into three steps. I must thank Jacob Tsimerman here, as he and I came to this organization while reading Mazur's paper together.

2.1 Step 1. A criterion for the non-existence of N-torsion

The hard part of the proof is to show that an elliptic curve over $\mathbf{Q}$ cannot have an N-torsion point, for N a prime > 7. Let $Y_1(N)$ be the set of isomorphism classes of pairs (E, P) where $E/\mathbf{C}$ is an elliptic curve and $P \in E$ is a point of exact order N. Then $Y_1(N)$ is actually (the set of complex points of) an algebraic curve defined over the rational numbers. Furthermore, the set of rational points on $Y_1(N)$ is exactly what you'd expect: it consists of those (E, P) for which E is defined over $\mathbf{Q}$ and $P \in E(\mathbf{Q})$. Thus Mazur's theorem essential amounts to showing that $Y_1(N)(\mathbf{Q})$ is empty for $N > 7$. The proof will appeal to the dual nature of $Y_1(N)$: it can be thought of as a single geometric object, or as a set of geometric objects.

We'll need some slight variants of $Y_1(N)$. Let $Y_0(N)$ be the set of pairs (E, G) where $E/\mathbf{C}$ is an elliptic curve and $G \subset E$ is a cyclic subgroup of order N. This is also an algebraic curve over $\mathbf{Q}$. There is a natural map $Y_1(N) \to Y_0(N)$ (take the subgroup generated by the point). The curve $Y_0(N)$ is affine: it's missing two points, which are labeled 0 and ∞, and called the cusps. The compactified curve is denoted $X_0(N)$. We can now state the criterion:

Theorem 5 (Theorem A)**.** *Suppose $N > 7$ and there exists an abelian variety $A/\mathbf{Q}$ and a map of varieties $f\colon X_0(N) \to A$ (defined over $\mathbf{Q}$) such that the following conditions hold:*

- *A has good reduction away from N.*
- *$f(0) \neq f(\infty)$.*
- *$A(\mathbf{Q})$ has rank 0.*

Then no elliptic curve defined over $\mathbf{Q}$ has a point of order N.

Sketch of proof. Suppose $E/\mathbf{Q}$ is an elliptic curve which has a point of order N. Let $x \in X_0(N)(\mathbf{Q})$ be the resulting rational point. We first remark that $X_0(N)$ naturally extends to a scheme over $\mathbf{Z}[1/N]$ (or even all of $\mathbf{Z}$) and x extends to a section over this base as well. By studying the reduction of E mod 3, and using the fact that 3 is small compared to N, one finds that E must have bad reduction at 3. This means that x must reduce to either 0 or ∞ mod 3, and in fact it must be ∞. To see this, one must be familiar with the modular interpretations of the two cusps, which we will cover later in the course.

Now for the key step: the difference $f(x) - f(\infty)$ is an element of $A(\mathbf{Z}[1/N])$ which reduces to 0 in $A(\mathbf{F}_3)$. However, $f(x) - f(\infty)$ is a torsion point (since A has rank 0), and the reduction map

is injective on torsion. We conclude that $f(x) = f(\infty)$. It follows from this, and the assumption that $f(\infty) \neq f(0)$, that if p is any prime of bad reduction for E then x reduces to ∞ mod p.

Now, consider $E[N]$ as a 2-dimensional representation of the absolute Galois group $G_{\mathbf{Q}}$ over the finite field $\mathbf{Z}/N\mathbf{Z}$. Since E has an N-torsion point, this representation contains the trivial representation $\mathbf{Z}/N\mathbf{Z}$ as a sub. The Weil pairing implies that the quotient is μ_N. The modular interpretation of the cusp ∞ shows that the resulting extension is actually split at all the bad primes. A number-theoretic argument then shows that the extension is split globally, i.e., $E[N]$ is isomorphic to $\mathbf{Z}/N\mathbf{Z} \oplus \mu_N$. One can apply the same argument to E/μ_N to see that its N-torsion is split; continuing in this way, one finds that the N-adic Tate module of E is reducible, which cannot happen. This contradiction completes the proof. □

2.2 Step 2. A criterion for rank 0

To apply Theorem A, we must find the abelian variety A and verify the conditions of the theorem. The hardest of these is the rank 0 condition. We now give a criterion for an abelian variety to have rank 0. This may look like a general criterion, but the hypotheses are actually very restrictive; it will apply to the case of interest, however.

Theorem 6 (Theorem B)**.** *Let $A/\mathbf{Q}$ be an abelian variety and let N and p be distinct prime numbers, with N odd. Suppose the following conditions hold:*

- *A has good reduction away from N.*
- *A has completely toric reduction at N.*
- *The Jordan–Holder constituents of $A[p](\overline{\mathbf{Q}})$ are 1-dimensional, and either trivial or cyclotomic.*

Then $A(\mathbf{Q})$ has rank 0.

Sketch of proof. Let $\mathcal{A}/\mathbf{Z}$ be the Néron model of A. One first shows that the group scheme $\mathcal{A}[p^n]$ is built of very simple pieces: it has a filtration such that the successive quotients are each one of four very specific group schemes. Computing explicitly with these specific group schemes, one shows that the order of $\mathrm{H}^1_{\mathrm{fppf}}(\mathrm{Spec}(\mathbf{Z}), \mathcal{A}[p^n])$ is bounded independent of n. This implies that the inverse limit over n of these cohomology groups is finite, which completes the proof, as $A(\mathbf{Q})$ injects into the inverse limit. This proof is closely related to the proof of the Mordell–Weil theorem, which I'll talk about some. □

2.3 Step 3. Completion of the proof

We now wish to prove Mazur's theorem by applying the above criteria. But first we must find the abelian variety A. Every curve has a Jacobian, a universal abelian variety to which it maps (given a point). Thus we are more or less forced to try to find A as a quotient of the Jacobian $J_0(N)$ of $X_0(N)$.

Using the modular interpretation of $X_0(N)$, one constructs certain Hecke operators T_p on $J_0(N)$. These generate a commutative ring of operators, called the Hecke algebra. We'll find A by defining an explicit ideal in the Hecke algebra (closely related to the Eisenstein ideal appearing in the title of Mazur's paper), and forming the corresponding quotient of $J_0(N)$. We'll then go through each of the hypotheses in the two criteria and verify that A satisfies them.

In fact, this argument will only end up working for $N > 13$, so auxiliary arguments are needed for $N = 11, 13$. For $N = 11$, the result was first established in 1939 by Billing–Mahler. For $N = 13$, it was established by Mazur–Tate in 1973.

3 Plan of the course

The course will be divided into three parts, corresponding to the three steps above (though out of order!).

Part I. Elliptic curves and abelian varieties

- Theory over fields. I will give very few proofs here. I'll assume you're either familiar with this, or can do outside reading to learn it.
- Group schemes. I won't assume you know much at all here, and I'll attempt to prove nearly everything we'll need.
- Theory in mixed characteristic, including Néron models (though not the proof of their existence). Jacobians.
- The culmination of Part I will be the proof of Theorem B.

Part II. Moduli of elliptic curves

- Modular curves, over $\mathbf{C}$, $\mathbf{Q}$, and $\mathbf{Z}$.
- Modular forms and Hecke operators.
- The Eichler–Shimura theorem, and the Galois representation attached to a modular form.
- The culmination of Part II will be the proof of Theorem A.

Part III. Proof of Mazur's theorem

- The Eisenstein ideal and the Eisenstein quotient of $J_0(N)$.
- The special fiber at N of $J_0(N)$.
- Ogg's theorem on the order of $[0] - [\infty]$ in $J_0(N)$.
- Application of Theorems A and B.
- Auxiliary results (Mazur–Tate, etc)

4 Related results

To end this lecture, I'll discuss two families of results that generalize Mazur's theorem. Unfortunately, we probably won't have time in this course to discuss these results further.

4.1 Merel's theorem

You might be wondering: does a version of Mazur's theorem exist over general number fields? The answer is yes! For an integer $d \geq 1$, let $S(d)$ be the set of prime numbers p for which there exists a number field $K/\mathbf{Q}$ of degree $\leq d$ and an elliptic curve E/K such that E has a K-point of order p. Mazur's theorem is that $S(1) = \{2, 3, 5, 7\}$. Kamienny proved (in 1992, MR1172689) that $S(2) = \{2, 3, 5, 7, 11, 13\}$. Mazur and Kamienny then conjectured that $S(d)$ is always finite (the Uniform Boundedness Conjecture, or UBC), which was proven by Merel:

Theorem 7 (Merel, 1996, MR1369424)**.** *The set $S(d)$ is finite. In fact, if $p \in S(d)$ then $p \leq d^{3d^2}$.*

In 2003, Parent computed $S(3)$ and found it to be the same as $S(2)$ (MR2142238, see also MR1779891). I don't know if any other $S(d)$'s have been explicitly computed.

The review of Merel's paper by Darmon, linked above, contains a thorough overview of the UBC.

4.2 Serre's uniformity theorem

Let $E/\mathbf{Q}$ be an elliptic curve, and let N be a prime. Then $E[N](\overline{\mathbf{Q}})$ is isomorphic to $(\mathbf{Z}/N\mathbf{Z})^2$, and carries an action of the absolute Galois group $G_{\mathbf{Q}}$. We can therefore regard it as a representation $\rho_{E,N} \colon G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$. Serre proved the following:

Theorem 8 (Serre, 1972, MR387283)**.** *Assume E does not have complex multiplication. Then there exists a number $N_0(E)$ such that $\rho_{E,N}$ is surjective for all $N > N_0(E)$.*

Serre posed the following question:

Question 9 (Serre's uniformity problem)**.** *Can $N_0(E)$ be taken independent of E? Precisely, does there exist a number N_0 such that $\rho_{E,N}$ is surjective whenever E is non-CM and $N > N_0$?*

It is thought that the answer to this question is yes, and that one can even take $N_0 = 37$.

If $\rho_{E,N}$ is not surjective, then its image is a proper subgroup of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$, and thus contained in a maximal proper subgroup. One can therefore attack Serre's question by proving, for each maximal proper subgroup G of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$, that the image of $\rho_{E,N}$ is not contained in G (for N large enough). It's not difficult to enumerate the maximal proper subgroups:

- The Borel subgroup (upper-triangular matrices).
- The normalizer of the split Cartan (monomial matrices).
- The normalizer of the non-split Cartan.
- Exceptional subgroups (those having projective image A_4, S_4, or A_5).

Serre himself dealt with the exceptional case: the image of $\rho_{E,N}$ is not contained in an exceptional subgroup if $N > 7$ (check this!). (In this and what follows, E is non-CM.)

Mazur's theorem that we have been discussing above is close to handling the Borel, but doesn't quite: it shows that the image of $\rho_{E,N}$ is not contained in the group of matrices of the form $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ for $N > 7$. However, Mazur extended his results (MR482230) and handled the Borel case: he showed that the image of $\rho_{E,N}$ is not contained in a Borel for $N > 37$.

In 2009, Bilu and Parent (MR2753610) handled the split Cartan case: the image of $\rho_{E,N}$ is not contained in the normalizer of the split Cartan for $N > N_0$, for some constant N_0. I took a very brief look at their paper and wasn't able to see if N_0 can be made explicit or not.

The non-split Cartan case is still open!