Lecture 27: Torsion Points on Elliptic Curves and Mazur's Big Theorem

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2001**

1 Mordell's Theorem

Venerable Problem: *Find an algorithm that, given an elliptic curve E over $\mathbb{Q}$, outputs a complete description of the set of rational points (x_0, y_0) on E.*

This problem is difficult. In fact, so far it has stumped everyone! There is a *conjectural algorithm*, but nobody has succeeded in proving that it is really an algorithm, in the sense that it terminates for any input curve E. Several of your profs at Harvard, including Barry Mazur, myself, and Christophe Cornut (who will teach Math 129 next semester) have spent, or might spend, a huge chunk of their life thinking about variants of this problem.

How could one possible "describe" the group $E(\mathbb{Q})$, since it can be infinite? In 1923, Mordell proved that there is always a reasonable way to describe $E(\mathbb{Q})$.

Theorem 1.1 (Mordell). *The group $E(\mathbb{Q})$ is finitely generated.*

This means that there are points $P_1, \ldots, P_s \in E(\mathbb{Q})$ such that every element of $E(\mathbb{Q})$ is of the form $n_1P_1 + \cdots + n_sP_s$ for some $n_1, \ldots n_s \in \mathbb{Z}$. I will not prove Mordell's theorem in this course. See §1.3 of [Kato et al.] for a proof in the special case when E is given by an equation of the form $y^2 = (x-a)(x-b)(x-c)$.

Example 1.2. Consider the elliptic curve E given by $y^2 = x^3 - 6x - 4$. Then $E(\mathbb{Q}) \approx (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$ with generators $(-2, 0)$ and $(-1, 1)$. We have

$$5(-1,1) = \left(-\frac{131432401}{121462441}, -\frac{1481891884199}{1338637562261}\right).$$

Trying finding that point without knowing about the group law!

2 Exploring the Possibilities

As E varies over all elliptic curves over $\mathbb{Q}$, what are the possibilities for $E(\mathbb{Q})$? What finitely generated abelian groups occur? Mordell's theorem implies that

$$E(\mathbb{Q}) \approx \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{tor}},$$

where $E(\mathbb{Q})_{\text{tor}}$ is the set of points of finite order in $E(\mathbb{Q})$ and $\mathbb{Z}^r \approx E(\mathbb{Q})/E(\mathbb{Q})_{\text{tor}}$. The number r is called the *rank* of E.

2.1 The Torsion Subgroup

Theorem 2.1 (Mazur, April 16, 1976). *Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})_{\text{tor}}$ is isomorphic to one of the following 15 groups:*

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} \qquad & \textit{for } n \le 10 \textit{ or } n = 12, \\ (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2n\mathbb{Z}) \qquad & \textit{for } n \le 4. \end{aligned}$$

As we will see in the next section, all of these torsion subgroups really do occur. Mazur's theorem is very deep, and I can barely begin to hint at how he proved it. The basic idea is to define, for each positive integer N, a curve $Y_1(N)$ with the magnificient property that the points of $Y_1(N)$ with complex coordinates are in natural bijection with the (isomorphism classes of) pairs (E, P), where E is an elliptic curve and P is a point of E of order N. Moreover, $Y_1(N)$ is amazing in that it has a rational point if and only if there is an elliptic curve over $\mathbb{Q}$ with a rational point of order N. I won't define $Y_1(N)$, but here it is for the first few N:

N	A curve that contains $Y_1(N)$
$1 - 10$, 12	a straight line; these have lots of points!
11	$y^2 + y = x^3 - x^2$
13	$y^2 = x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1$
14	$y^2 + xy + y = x^3 - x$
15	$y^2 + xy + y = x^3 + x^2$
16	$y^2 = (x-1)(x+1)(x^2 - 2x - 1)(x^2 + 1)$
17	The intersection of the hypersurfaces in $\mathbb{P}^4$ defined by: $ac - b^2 + 5bd - 3be - c^2 - 4cd + 2ce - 4d^2 + 7de - 2e^2$, $ad - bc + bd - be + c^2 - 2cd - 2d^2 + 4de - e^2$, and $ae - be - cd + 2d^2 - 2de + e^2$.
18	$y^2 = x^6 + 4x^5 + 10x^4 + 10x^3 + 5x^2 + 2x + 1$

(Some of the curves in the right hand column have a few obvious rational points, but these points "don't count".)

Mazur proved that if $N = 11$ or $N \ge 13$, then $Y_1(N)$ has no rational points. This result, together with the theory surrounding $Y_1(N)$, yields his theorem.

2.2 The Rank

Conjecture 2.2. *There exist elliptic curves over $\mathbb{Q}$ of arbitrarily large rank.*

As far as I know, nobody has any real clue as to how to prove Conjecture 2.2 (Doug Ulmer recently wrote a paper which gives theoretical evidence). The current "world record" is a curve of rank ≥ 24. It was discovered in January 2000 by Roland Martin and William McMillen of the **National Security Agency**. For security reasons, I won't tell you anything about how they found it.

Theorem 2.3. *The elliptic curve*

$$y^2 + xy + y = x^3 - 120039822036992245303534619191166796374x + 504224992484910670010801799168082726759443756222911415116$$

over $\mathbb{Q}$ has rank at least 24. The following points $P_1, \ldots, P_{24}$ are independent points on the curve:

$$
\begin{aligned}
P_1 &= (2005024558054813068, -16480371588343085108234888252)\\
P_2 &= (-4690836759490453344, -31049883525785801514744524804)\\
P_3 &= (4700156326649806635, -6622116250158424945781859743)\\
P_4 &= (6785546256295273860, -14561809288309785211075204730)\\
P_5 &= (6823803569166584943, -16859507354771759473517748170)\\
P_6 &= (7788809602110240789, -6462981622972389783453855713)\\
P_7 &= (27385442304350994620556, 4531892554281655472841805111276996)\\
P_8 &= (5428468206028525371 9/4, -29660878815798901619218209042 7/8)\\
P_9 &= (-94200235260395075139/25, -3756324603619419619213452459781/125)\\
P_{10} &= (-3463661055331841724647/576, -43903354139186769004111404728779 3/13824)\\
P_{11} &= (-6684065934033506970637/676, -473072253066190669804172657192457/17576)\\
P_{12} &= (-956077386192640344198/2209, -2448326762443096987265907469107661/103823)\\
P_{13} &= (-27067471797013364392578/2809, -4120976168445115434193886851218259/148877)\\
P_{14} &= (-25538866857137199063309/3721, -7194962289937471269967128729589169/226981)\\
P_{15} &= (-102632501176025905189 4331/108241, -10008952940674898577361109630032677 73/35611289)\\
P_{16} &= (9351361230729481250627334/1366561, -28697496057486357774753723393062048 32/1597509809)\\
P_{17} &= (10100878635879432897339615/1423249, -5304965776276966451066900941489387801/1697936057)\\
P_{18} &= (11499655868211022625340735/17522596, -1513435763341541188265230241426826478043/73349586856)\\
P_{19} &= (110352253665081002517811734/21353641, -461706833308406671405570254542647784288/98675175061)\\
P_{20} &= (414280096426033094143668538257/285204544, 266642138924791310663963499787603019833872421/4816534339072)\\
P_{21} &= (36101712290699828042930087436/4098432361, -2995258855766764520463389153587111670142292/262377541318859)\\
P_{22} &= (45442463408503524215460183165/5424617104, -371604158147014410872159069555467015638886 9/399533898943808)\\
P_{23} &= (983886013344700707678587482584/141566320009, -1266158183877179304491616259603976057419409 53/53264752602346277)\\
P_{24} &= (1124614335716851053281176544216033/152487126016, -37714203831317877163580088877209977295481388540127/59545612760743936)
\end{aligned}
$$

Proof. See

`http://listserv.nodak.edu/scripts/wa.exe?A2=ind0005&L=nmbrthry&P=R182`

□

3 How to Compute $E(\mathbb{Q})_{\text{tor}}$

The following theorem yields an algorithm to compute $E(\mathbb{Q})_{\text{tor}}$.

Theorem 3.1 (Nagell-Lutz). *Suppose that $y^2 = x^3 + ax + b$ (with $a, b \in \mathbb{Z}$) defines an elliptic curve E over $\mathbb{Q}$, let $\Delta = -16(4a^3 + 27b^2)$ be the discriminant, and suppose that $P = (x, y) \in E(\mathbb{Q})_{\text{tor}}$. Then x and y are integers and either $y = 0$, in which case P has order 2, or $y^2 \mid \Delta$.*

Non-proof. I will not prove this theorem. However, you can find a readable proof in Chapter II of Silverman and Tate's *Rational Points on Elliptic Curves.* □

Warning: Nagell-Lutz is NOT an if and only if statement. There are points of infinite order that satisfy the conclusion of Theorem 3.1. For example, the point $(1, 3)$ on $y^2 = x^3 + 8$ has integer coordinates and $y^2 = 9 \mid \Delta = -16 \cdot 27 \cdot 3^2$. However,

$$(1, 3) + (1, 3) = \left(-\frac{7}{4}, -\frac{13}{8}\right).$$

Since the coordinates of $(1,3)+(1,3)$ are not integers, it follows from the contrapositive (not converse!) of Nagell-Lutz that $(1,3)$ must be a point of infinite order.

Example 3.2. The following is a list of elliptic curves with each possible torsion subgroup. Tom Womack (a graduate student in Nottingham, where Robin Hood lives) has a web page, `http://www.tom.womack.net/maths/torsion.htm`, which contains PARI code that lists infinitely many elliptic curve with each torsion subgroup.

Curve	$E(\mathbb{Q})_{\mathrm{tor}}$
$y^2 = x^3 - 2$	$\{0\}$
$y^2 = x^3 + 8$	$\mathbb{Z}/2\mathbb{Z}$
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$
$y^2 - y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$
$y^2 = x^3 - 43x + 166$	$\mathbb{Z}/7\mathbb{Z}$
$y^2 + 7xy = x^3 + 16x$	$\mathbb{Z}/8\mathbb{Z}$
$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9\mathbb{Z}$
$y^2 + xy = x^3 - 45x + 81$	$\mathbb{Z}/10\mathbb{Z}$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$
$y^2 = x^3 - 4x$	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$
$y^2 = x^3 + 2x^2 - 3x$	$(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$(\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$
$y^2 + 17xy - 120y = x^3 - 60x^2$	$(\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$

The `elltors` function in PARI computes torsion subgroups:

```
? ?elltors
elltors(e,{flag=0}): torsion subgroup of elliptic curve e: order, structure,
generators. If flag = 0, use Doud's algorithm; if flag = 1, use Lutz-Nagell.
? e=ellinit([17,-60,-120,0,0]);
? elltors(e)
%4 = [16, [8, 2], [[30, -90], [-40, 400]]]
? e.disc
%5 = 51438240000
? e.disc % 90^2        \\ verify Nagell-Lutz
%6 = 0
? e.disc % 400^2       \\ verify Nagell-Lutz
%7 = 0
```