Lecture 26: The Elliptic Curve Group Law

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2001**

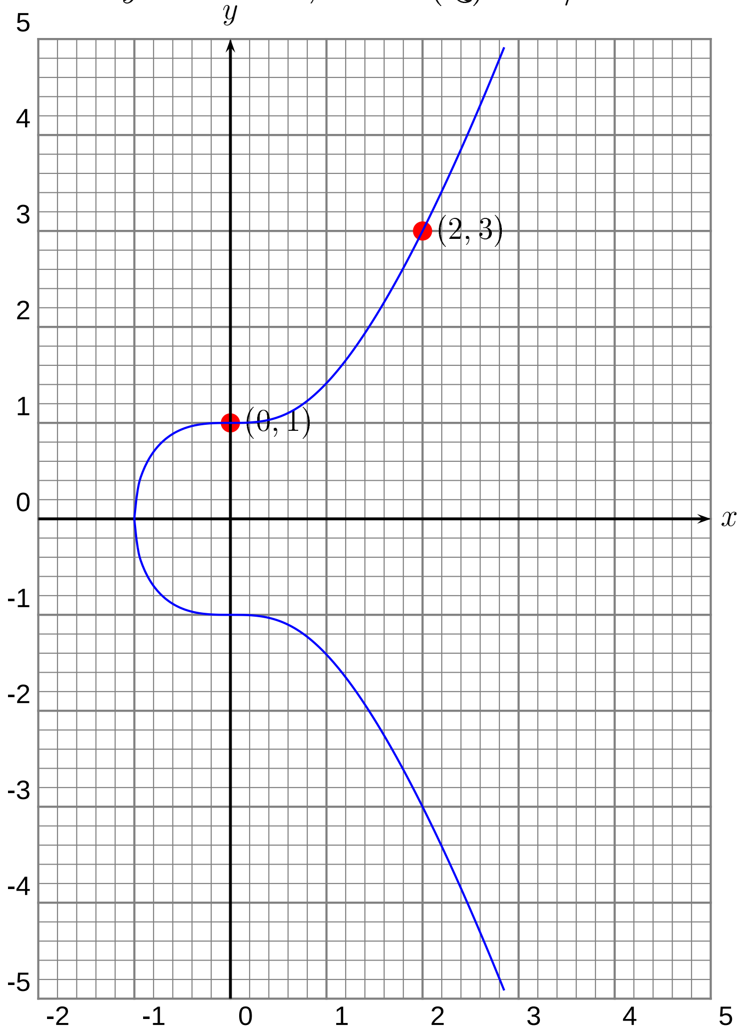
1 Some Graphs

Recall that an elliptic curve over a field K (in which 2 and 3 are invertible) can be defined by an equation

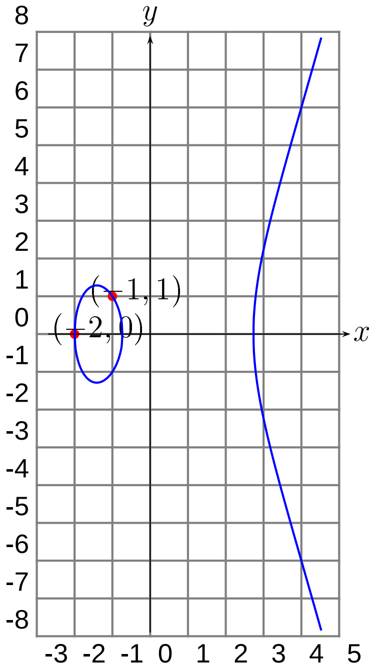
$$y^2 = x^3 + ax + b$$

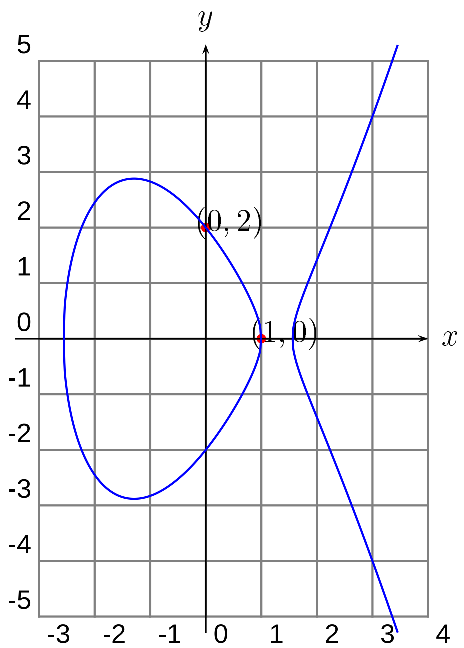
with $a, b \in K$. Here are some examples over $\mathbb{Q}$.

$$y^2 = x^3 + 1, \qquad E(\mathbb{Q}) \approx \mathbb{Z}/6\mathbb{Z}$$



$$y^2 = x^3 - 6x - 4 \qquad \text{and} \qquad y^2 = x^3 - 5x + 4$$
$$E(\mathbb{Q}) \approx (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z} \quad \text{(for both curves)}$$





(Exercise: Add the indicated points.)

2 The Point $\mathcal{O}$ at Infinity

The graphs of the previous section are each missing a point at infinity. They are graphs in the plane $\mathbb{R}^2$. The plane is a subset of the projective plane $\mathbb{P}^2$. The "closure" of the graph of $y^2 = x^3 + ax + b$ in $\mathbb{P}^2$ has exactly one extra point $\mathcal{O}$, which has rational coordinates, and which we sometimes call "the point at infinity".

Definition 2.1. The *projective plane* $\mathbb{P}^2$ is the set of triples (a, b, c), with a, b, c not all 0, modulo the equivalence relation

$$(a, b, c) \sim (\lambda a, \lambda b, \lambda c)$$

for any nonzero λ. We denote by $(a:b:c)$ the equivalence class of (a, b, c).

The "closure" in $\mathbb{P}^2$ of the graph of $y^2 = x^3 + ax + b$ is the graph of

$$y^2 z = x^3 + axz^2 + bz^3$$

and the extra point is $\mathcal{O} = (0:1:0)$. All finite points are of the form $(a:b:1)$.

For more about the projective plane, see page 28 of [Kato et al.].

3 The Group Law is a Group Law

Let E be an elliptic curve of the form $y^2 = x^3 + ax + b$ over a field K. Consider the set

$$E(K) = \{\mathcal{O}\} \cup \left\{(x, y) \in K \times K \,:\, y^2 = x^3 + ax + b\right\}.$$

Recall from the last lecture that there is a natural way to endow the set $E(K)$ with a *group* structure. Here's how it works. First, the element $\mathcal{O} \in E(K)$ is the zero element of the group. Next, suppose P and Q are elements of $E(K)$. Just like we did earlier, let $R = (x_3, y_3)$ be the third point of intersection of E and the line determined by P and Q (try this with the graphs on pages 1 and 2). Define

$$P + Q = (x_3, -y_3).$$

(For what goes wrong if you try to define $P + Q = (x_3, y_3)$, see your homework assignment.) There are various special cases to consider, such as when $P = Q$ or the third point of intersection is $\mathcal{O}$, but I will let you read about them in [Kato et al.].

It is not surprising that this binary operation on $E(K)$ satisfies $P + Q = Q + P$. Also, the inverse of $P = (x_1, y_1)$ is $-P = (x_1, -y_1)$. The only other axiom to check in order to verify that $+$ gives $E(K)$ an abelian group structure is the associative law. This is simple but *tedious* to check using only elementary methods. The right way to prove that the associate law holds is to develop the theory of algebraic curves and define the group law in terms of divisor classes, but this is outside the scope of this course. For fun, we can coerce the amazingly cool (but complicated) computer algebra system MAGMA into verifying the associative law (over $\mathbb{Q}$) for us:

```
// Define the field K = Q(a,b,x0,x1,x2)
K<a,b,x0,x1,x2> := FieldOfFractions(PolynomialRing(Rationals(),5));
// Define the polynomial ring R = K[y0,y1,y2]
R<y0,y1,y2> := PolynomialRing(K,3);
// Define a maximal ideal of R:
I := ideal<R | y0^2 - (x0^3+a*x0+b),
               y1^2 - (x1^3+a*x1+b),
               y2^2 - (x2^3+a*x2+b)>;
// The quotient L = R/I is a field that contains three
// distinct "generic" points on E.
L  := quo<R|I>;
// Define the elliptic curve y^2 = x^3 + a*x + b over L.
E  := EllipticCurve([L| a,b]);
// Let P0, P1, and P2 be three distinct "generic" points on E.
P0 := E![L|x0,y0]; P1 := E![L|x1,y1]; P2 := E![L|x2,y2];
// The algebraic formulas for the group law are built into MAGMA.
lhs := (P0 + P1) + P2;  rhs := P0 + (P1 + P2);
// Verify the associative law.
lhs eq rhs;
true     // Yeah, it works!
```

4 An Example Over a Finite Field

Let E be the elliptic curve $y^2 = x^3 + 3x + 3$ over the finite field

$$K = \mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}.$$

First, we find all points on E using PARI:

```
? for(x=0,4, for(y=0,4, if((y^2-(x^3+3*x+3))%5==0, print1([x,y],"  "))))
[3, 2]  [3, 3]  [4, 2]  [4, 3]
```

Thus $E(K) = \{\mathcal{O}, (3,2), (3,3), (4,2), (4,3)\}$, so $E(K)$ must be a cyclic abelian group of order 5. Let's verify that $E(K)$ is generated by $(3,2)$.

```
? e = ellinit([0,0,0,Mod(3,5),Mod(3,5)])
? ?ellpow    \\ type ?5 for a complete list of elliptic-curve functions
ellpow(e,x,n): n times the point x on elliptic curve e (n in Z).
? x = [3,2];
? for(n=1,5,print(n,"*[3,2] =  ",lift(ellpow(e,x,n))))
1*[3,2] =  [3, 2]
2*[3,2] =  [4, 3]
3*[3,2] =  [4, 2]
4*[3,2] =  [3, 3]
5*[3,2] =  [0]
```

5 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 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 5.1 (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, but see §1.3 of [Kato et al.].

Example 5.2. 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!