

Final Project

Stephen McKeown
Math 581b
Professor Stein, Instructor

December 13, 2010

The purpose of this paper is to present a substantial portion of the proof of Mordell's theorem, which states that the group $E(\mathbb{Q})$ of rational points on an elliptic curve E over \mathbb{Q} is finitely generated. Though the argument generalizes straightforwardly to number fields, and much less straightforwardly to abelian varieties (at which point it is known as the Mordell-Weil theorem), I will consider only, roughly speaking, the half of the rational case. All the material is drawn, rather directly, from Husemöller's *Elliptic Curves*, Lang's *Elliptic Curves: Diophantine Analysis*, and Silverman's *Arithmetic of Elliptic Curves*.

1 Background and Basic Results

An elliptic curve is a nonsingular curve of genus one with a specified point O . Any elliptic curve can be written as the solution set to the equation $y^2 = f(x)$, where $f(x)$ is some cubic of the form $f(x) = x^3 + ax + b$. (Husemöller, p. 28). We are typically interested in elliptic curves wherein $a, b \in \mathbb{Q}$ or some number field. In this paper we will restrict attention to \mathbb{Q} . A natural object of interest is then the set of rational points $(x, y) \in \mathbb{Q}^2$ such that $y^2 = f(x)$. This is referred to as $E(\mathbb{Q})$.

Several theorems are most easily proven in the context of projective space $P^2(\mathbb{Q})$. A point p in projective n -space can be represented as $0 \neq (p_0, \dots, p_n)$, under the equivalence relation $(p_0, \dots, p_n) \sim \lambda(p_0, \dots, p_n)$ for nonzero λ . It is clear that by appropriate choice of λ , any point can be written with all the p_i integers, and with a gcd of 1. (Call this reduced integer form.) In projective space, the equation of an elliptic curve is homogenized to $Y^2Z = X^3 + aXZ^2 + bZ^3$.

As Jacobi first realized, an abelian group structure can be put on $E(\mathbb{Q})$ using a geometric addition procedure: for two rational points P and Q on the curve, take the line through P and Q and consider the third point of intersection, $P * Q$. Then take the line through O and $P * Q$, and call the third point of intersection of *this* line with the curve $P + Q$. Then this yields an abelian group law. All properties are easy to prove except associativity. See either reference for a proof.

Mordell's theorem, proven in 1922, states that $E(\mathbb{Q})$ is a finitely generated abelian group. In the case of curves over \mathbb{Q} , much is now known about the torsion subgroup; indeed, Mazur¹ completely classified the possible torsion

¹Mazur, *Rational Isogenies of Prime Degree*, Invent. Math. 44, 2 (June 1978), p. 129

subgroups. Substantially less is known about the rank of the free part, and its study is one of the major themes in modern algebraic number theory.

I wanted to learn and present Mordell's theorem, because it is a foundational theorem of the field whose proof is somewhat accessible, yet slightly too complicated to be frequently taught. This paper will present half of its proof. I close this section with unproved statements of two background results that will prove useful.

Theorem 1 *Let (x, y) be a rational point on an elliptic curve $y^2 = x^3 + ax + b$, and let $n(x, y)$ be multiplication by n in $E(\mathbb{Q})$. Then $n(x, y) = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \dots \right)$, where $\phi_n(x) \in \mathbb{Z}[x]$ of degree n^2 , and $\psi_n^2(x) \in \mathbb{Z}[x]$ of degree $n^2 - 1$.*

This is proven in chapter 2 of Lang, using a complex analytic development of elliptic curves which – unfortunately – would take us far afield. For a more elementary treatment when $n = 2$, see Silverman and Tate, *Rational Points on Elliptic Curves*, chapter 1.

Next, we state part of the addition formula for a curve. Suppose $(x_1, y_1), (x_2, y_2)$ are distinct points. Then the ordinate of their sum will be

$$x_3 = -x_1 - x_2 + \frac{1}{4} \left(\frac{y_1 - y_2}{x_1 - x_2} \right)^2. \quad (1)$$

Again, see Lang or Silverman, e.g., for a proof.

2 An outline of the proof

We begin with a definition.

Definition Let G be an abelian group. A *height* on G is a function $h : G \rightarrow [0, \infty]$ satisfying the following axioms:

- a) For fixed $g \in G$, there is a constant c_g such that $h(g + x) \leq 2h(x) + c_g$.
- b) There is an integer $m \geq 2$ and a constant c_1 such that $h(mg) \geq m^2h(g) - c_1$.
- c) $|h^{-1}([0, c])| < \infty$ for any $c > 0$.

The proof of Mordell's theorem will ultimately follow from the following important result.

Theorem 2 Let G be an abelian group. Suppose that G/mG is finite for some m , and there exists a height function $h : G \rightarrow [0, \infty]$ on G . Then G is finitely generated.

Proof Let g_1, \dots, g_r be representatives of the cosets of mG in G . Let $p \in G$ and write $p = mq_1 + g_{n_1}$. Induct, writing $q_i = mq_{i+1} + g_{i_{n+1}}$. We have, from the axioms,

$$-c_1 + m^2 h(q_{n+1}) \leq h(mq_{n+1}) \leq 2h(q_n) + k,$$

where $k = \max_{1 \leq i \leq r} c_{g_i}$. Taking $\kappa = c_1 + k$, we have

$$\begin{aligned} h(q_{n+1}) &\leq \frac{2}{m^2} h(q_n) + \frac{\kappa}{m^2} \\ &\leq \frac{2^n}{m^{2n}} + \kappa \left(\sum_{j=1}^n \frac{2^j}{m^{2j}} \right). \end{aligned}$$

Therefore, for n large enough, we always get $h(q_n)$ bounded – say by 1. There are finitely many elements with height less than 1, so any element can be written as a sum of the r p_i and at most one additional element from the finite set $h^{-1}(\text{bounded})$. Therefore, G is finitely generated. ■

The proof of Mordell now proceeds in two steps: first, show that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, and then show that there is a height function. The first step will not be covered in this paper; there are various ways to prove it – for two of them, see Lang – including the construction of certain ~~of~~ homomorphisms on $E(\mathbb{Q})$ and the study of their properties. We will provide a proof of the existence of a height function.

3 Construction of the Height Function

We first create a height function on $P^n(\mathbb{Q})$, projective n -space. Define $H(p) = \max_i |p_i|$, where $||$ is the normal Euclidean absolute value, and define $h(p) = \log H(p)$.

Theorem 3 There is only a finite number of points of bounded height and bounded degree in $P^n(\mathbb{Q})$.

Proof This is completely obvious from the definition. ■

Definition Let f_0, \dots, f_m be homogenous polynomials in $n+1$ variables and of degree d (i.e., $f_i(tX_0, \dots, tX_n) = t^d f_i(X_0, \dots, X_n)$), and assume there is no common nontrivial zero. The map $f : P^n \rightarrow P^m$ defined by $f = (f_0, \dots, f_m)$ is a *morphism of degree d* . It is well-defined because it is never zero by hypothesis.

Lemma 1 Let φ be a homogenous polynomial of degree d , in $n+1$ variables. Then there is a positive constant $c(\varphi)$ such that for $y \in P^n(\mathbb{Q})$, represented as above by integers y_0, \dots, y_n , $|\varphi(y)| \leq c(\varphi)H(y)^d$.

Proof Write $\varphi(y) = \sum a_i m_i(y)$, where each m_i is a monomial. Then

$$|\varphi(y)| \leq \sum_i |a_i| |m_i(y)| \leq \left(\sum_i |a_i| \right) (\max_i |y_i|)^d \equiv c(\varphi) H(y)^d. \quad \blacksquare$$

We next state a major theorem of Hilbert:

Theorem 4 (*Hilbert's Nullstellensatz*) Let $\mathfrak{o} \subseteq K[x_1, \dots, x_n]$ be an ideal, and $V(\mathfrak{o}) = \{x \in \overline{K} : p(x) = 0 \forall p \in \mathfrak{o}\}$. Suppose $f \in K[x_1, \dots, x_n]$, and $f(x) = 0$ for all $x \in V(\mathfrak{o})$. Then for some $n \in \mathbb{N}$, $f^n \in V(\mathfrak{o})$.

The proof of this theorem is relatively brief, but would take us somewhat far afield, and so will not be given here. A proof can be found in Lang's *Algebra, Rev. 3rd Ed.*, at p. 378 ff.

Corollary 5 Let $f = (f_0, \dots, f_m) : P^n(\mathbb{Q}) \rightarrow P^m(\mathbb{Q})$ be a morphism. Then there exists an integer $s > 0$, an integer b , and homogenous polynomials $g_{ij} \in \mathbb{Z}[X_0, \dots, X_n]$ of degree s such that $bX_i^{s+d} = \sum_j g_{ij} f_j$.

Proof From the definition of morphism, the polynomials f_j have only zero as a common root. Hence, if \mathfrak{o} is the ideal generated by f_0, \dots, f_m , then $V(\mathfrak{o}) = \{0\}$. Since X^d shares this root, the Nullstellensatz implies that X^{d+m} is in the ideal \mathfrak{o} for some m , i.e., there exist $g_{ij} \in \mathbb{Q}[X_0, \dots, X_n]$ such that $X_i^{d+m} = \sum_j g_{ij} f_j$. By clearing the denominator of the g_{ij} (multiplying by d) and considering m as it ranges over i , we thus establish the result, except for homogeneity. If g_{ij} contains terms that are not degree- s , then clearly the terms are not (taken as a whole) necessary to the identity, but must rather cancel with other such terms; and we may therefore assume that they are degree s .

The following theorem is pivotal in proving Mordell:

Theorem 6 *Let h be the height on $P^n(\mathbb{Q})$ as defined above. Then for any \mathbb{Q} -morphism $f : P^n(\mathbb{Q}) \rightarrow P^n(\mathbb{Q})$, $hf - dh$ is bounded over $P^n(\mathbb{Q})$.*

Proof Let x be a point in P^n expressed in \mathbb{Z} -reduced form. Using lemma 1, we have $H(f(x)) = \max_i |f_i(y)| \leq H(y)^d \cdot \max_i c(f_i) \equiv CH(y)^d$.

Now corollary 5 implies that

$$|b||x_i|^{s+d} \leq \max_{i,j} c(g_{ij}) \max \{|x_0|^s, \dots, |x_n|^s\} \sum_j |f_j(x)|$$

(where we are using the homogeneity of the g_{ij}).

$$= \max_{ij} c(g_{ij}) \cdot H(x)^2 \cdot (m+1) \cdot \max_j |f_j(x)|$$

We then have $\max_j |f_j(x)| = |b|H(f(x))$, where b is as in the prior corollary (recall that H acts on points represented by integer coefficients). Hence

$$|b|H(x)^{2+d} \leq \max_{i,j} c(g_{ij}) \cdot (m+1)H(x)^2 |b|H(f(x)),$$

whence

$$cH(x)^d \leq H(f(x)),$$

for some c . Thus $cH(x)^d \leq H(f(x)) \leq CH(x)^d$, and

$$c \leq \frac{H(f(x))}{H(x)^d}.$$

Taking logarithms gives the result. ■

Recall from section one that if (x, y) is a point on an elliptic curve, then multiplication by n yields an x -coordinate given by $\frac{f}{g}$, where f is a polynomial of degree n^2 , and g is of degree $n^2 - 1$. Consider the homogenizations of f and g , of degree n^2 , calling them F and G : in this case, (G, F) will form a morphism on projective 1-space. This enables us finally to construct heights on elliptic curves.

Definition Let E be an elliptic curve, and (by abuse of notation) $x : E \rightarrow P^1$ be given by $x(x, y) = (1, x)$, i.e., if $P = (x, y)$, $x(P) = (1, x)$. Define $h_E : E \rightarrow [0, \infty]$ by

$$h_E(P) = h(x(P)).$$

Theorem 7 *Let h_E be as above. Then for $n \in \mathbb{Z}^+$, $h(nP) - n^2h(P)$ is bounded over E .*

Proof As in the above discussion, let $n : P^1 \rightarrow P^1 = (G, F)$. By theorem 6, $hn - n^2h$ is bounded over P^1 ; and $h_E(nP) = h(n \circ x(P))$. This suffices. ■

Theorem 8 *As defined above, h_E is a height function.*

Proof Property (a) follows from equation (1) (recalling that h is the *log* of H). Property (b) follows from theorem 7. Property (c) follows from theorem 3. ■

Assuming the absent result that $E_{\mathbb{Z}^+}$ is finitely generated, this proves Mordell's theorem, by theorem 2.