THE MORDELL-WEIL THEOREM FOR $\mathbb{Q}$

NICOLAS FORD

Abstract. An elliptic curve is a specific type of algebraic curve on which one may impose the structure of an abelian group with many desirable properties. The study of elliptic curves has far-reaching connections number theory, cryptography, analysis, and many other fields, and occupies a large area of current research. If an elliptic curve happens to be defined over the rationals, one may examine the subgroup of points with rational coordinates. The Mordell-Weil Theorem for $\mathbb{Q}$ states that this group is finitely generated.

Contents

1. Preliminaries

We assume some familiarity with the theory of algebraic curves and algebraic number theory. As such, many definitions will be stated quickly and under the assumption that the reader has seen them before, and results that come purely from one of these fields will be stated without proof.

Definition 1.1. Let K be an algebraically closed field. Recall that the *projective plane over* K is the set $\mathbb{P}^2(K)$ of equivalence classes of nonzero points in K^3 under the relation $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$ for each $\lambda \neq 0 \in K$. The equivalence class of the point (x, y, z) is denoted $[x : y : z]$.

Definition 1.2. For any homogeneous polynomial F in $K[X, Y, Z]$ we have a set $V(F)$ defined by

$$V(F) = \{[a : b : c] \in \mathbb{P}^2 : F(a, b, c) = 0\}.$$

Note that this definition does not depend on the choice of representative for the point $[a : b : c]$, because $F(\lambda a, \lambda b, \lambda c) = \lambda^{\deg F} F(a, b, c)$, since F is homogeneous. Such a set $V(F)$ is called the *locus of* F. If L is a subfield of K and the coefficients of F lie in L, we say $V(F)$ is *defined over* L.

In this paper, we will be concerned only with curves of a specific type, namely those specified by a cubic polynomial with only one point on the line $H_\infty = \{[x : y : 0] : x, y \in K\}$ at infinity. After a linear change of coordinates, we may assume

that the point in question is $[0:1:0]$. The curve may then be given by an equation of the following form, called a *Weierstrass equation*:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Given a Weierstrass equation, we define the following quantities [4, 46]:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned}$$

The quantity Δ above is called the *discriminant*. Note that if the characteristic of K is not 2, we may simplify the Weierstrass equation by completing the square. Replacing Y with $\frac{1}{2}(Y - a_1X - a_3Z)$, one can easily check that the Weierstrass equation becomes

$$Y^2Z = 4X^3 + b_2X^2Z + 2b_4XZ^2 + b_6.$$

Definition 1.3. Recall that a point $P \in V(F)$ is called a *singular point* if

$$\partial F/\partial X(P) = \partial F/\partial Y(P) = \partial F/\partial Z(P) = 0.$$

Suppose F is given by a Weierstrass equation. It takes a straightforward but tedious calculation, which we omit here, to verify that every point of $V(F)$ is nonsingular if and only if $\Delta \neq 0$. If this is the case, we call $V(F)$ an *elliptic curve*. The *basepoint* is the point $O = [0:1:0]$.

The points of an elliptic curve can be made into an abelian group in a relatively simple way, and it is this group that will be the object of study in this paper. Before defining the group operation, we recall some definitions that will help in defining our operation properly.

Definitions 1.4. Let E be an elliptic curve.

- The *divisor group* $\mathrm{Div}(E)$ of E is the free abelian group generated by the points of E. If $D = \sum_{i=1}^m n_iP_i \in \mathrm{Div}(E)$, we define $\deg(D) = \sum_{i=1}^m n_i$. We write $D \geq D'$ if each entry in D is greater than or equal to the corresponding entry in D'.
- Recall that if P is a nonsingular point on E, then the local ring $\mathscr{O}_P$ at P (the ring of rational functions on E which are defined at P) is a discrete valuation ring. Given a rational function $f \in K(E)$ (where $K(E)$ is the field of rational functions on E) we define $\mathrm{div}(f) = \sum_{P \in \mathbb{P}^2} \mathrm{ord}_P(f)$, where ord_P is the valuation on K induced by $\mathscr{O}_P$.
- The image of div forms a subgroup of $\mathrm{Div}^0(E) = \{D \in \mathrm{Div}(E) : \deg D = 0\}$. The quotient of $\mathrm{Div}^0(E)$ by this subgroup is called $\mathrm{Pic}^0(E)$, and if two elements D and D' of the divisor group differ by an element of the image of div, we write $D \sim D'$.
- For $D \in \mathrm{Div}(E)$, we write $L(D) = \{f \in K(E) : \mathrm{div}(f) \geq -D\}$. This is a vector space over K.

Proposition 1.5. *Let E be an elliptic curve and let $O \in E$ be the point $[0:1:0]$. Then for every $D \in \mathrm{Div}^0(E)$, there is a unique point P such that $D \sim P - O$.*

Proof. A nonsingular plane cubic has genus 1, so we may apply the Riemann-Roch Theorem [2, 108] to get that $\dim L(D+O) = 1$. Let f be a nonzero element of $L(D+O)$. Then $\operatorname{div}(f) \geq -D - O$ which, since $\deg(\operatorname{div}(f)) = \deg D = 0$, gives us that $\operatorname{div}(f) = P - D - O$ for some P. Then $D \sim P - O$ as desired. If $D \sim P' - O$ for some other P', then $P \sim P'$, so for some rational function f, $\operatorname{div}(f) = P - P' \in L(P')$. But by the same reasoning as above, $L(P')$ is one-dimensional, and it contains all the constant functions, so f must be constant, meaning $\operatorname{div}(f) = 0$, so $P = P'$. □

This gives a one-to-one correspondence between the elements of $\operatorname{Pic}^0(E)$ and the points on E, and since $\operatorname{Pic}^0(E)$ is already an abelian group, this gives us a group structure on E. If L is a subfield of K, we write $E(L)$ for the set of points $[x : y : z]$ of E for which, for some $\lambda \in K^\times$, $\lambda x, \lambda y, \lambda z \in L$. That is, $E(L)$ is the set of points of E for which there exists a choice of coordinates using only elements of L.

Remark 1.6. There is also a geometric way to think about the group law on an elliptic curve. Suppose P and Q are points on E. By Bézout's theorem [2, 57], the line going through P and Q intersects E in exactly one other point, say R. Write $R = P \oplus Q$. Then $P + Q = O \oplus (P \oplus Q)$. To see this, let L be the line going through P and Q (or tangent at P if $P = Q$), and let L' be the line going through $P \oplus Q$ and O. It is easy to see by inspecting the Weierstrass equation that $\operatorname{ord}_O(Z) = 3$ and $\operatorname{ord}_P(Z) = 0$ for $P \neq O$, so we get that

$$\operatorname{div}(L/Z) = P + Q + (P \oplus Q) - 3O,$$

$$\operatorname{div}(L'/Z) = (P \oplus Q) + (O \oplus (P \oplus Q)) - 2O.$$

Then

$$0 \sim \operatorname{div}(L/L') = P + Q - O - (O \oplus (P \oplus Q)),$$

so we get that $(P - O) + (Q - O) = (O \oplus (P \oplus Q)) - O$.

Thinking of the group law in terms of lines allows us to derive an explicit formula for computing the sum of two points on an elliptic curve. The verification of the formula is long and would take us too far off course, but we transcribe it here.

Proposition 1.7. [4, 58] *Let $P = [x_1 : y_1 : 1]$ and $Q = [x_2 : y_2 : 1]$ be two nonidentity points on an elliptic curve E. If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then $P = -Q$. Otherwise, if $x_1 \neq x_2$, define*

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1},$$

and if $x_1 = x_2$, define

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3},$$

$$\nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

The line $Y = \lambda X + \nu Z$ is the line L from the preceding discussion. Then if

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3,$$

then $[x_3 : y_3 : 1] = P + Q$.

2. Heights and the Descent Theorem

The goal of this paper is to prove that, if E is an elliptic curve, then the group $E(\mathbb{Q})$ is finitely generated. To do this, we will use a general result called the Descent Theorem, which relies on the existence of a function with certain properties which measures the "size" of an element of the group and uses information about the number of elements of small enough size to find a finite generating set.

Theorem 2.1 (Descent)**.** [4, 199] *Suppose A is an abelian group, and $h : A \to \mathbb{R}$ is a function with the following properties:*

- *For each $q \in A$ there is a constant c_1 depending on A and q such that $h(p+q) \leq 2h(p) + c_1$ for all p.*
- *For some integer $m \geq 2$ and some constant c_2 depending only on A, we have that $h(mp) \geq m^2 h(p) - c_2$ for all p.*
- *For every real number k, $\{p \in A : h(p) < k\}$ is finite.*

If, in addition, A/mA is finite for the m above, then A is finitely generated.

Proof. Pick representatives $q_1, \ldots, q_r \in A$ for each of the cosets of A/mA, and pick some $p \in A$. Write $p = mp_1 + q_{i_1}$ for some i_1. Continuing inductively in this way, writing $p_{n-1} = mp_n + q_{i_n}$. From the first two properties of the height function, we have that

$$\begin{aligned} h(p_n) &\leq \frac{1}{m^2}(h(mp_n) + c_2) \\ &= \frac{1}{m^2}(h(p_{n-1} - q_{i_n}) + c_2) \\ &\leq \frac{1}{m^2}(2h(p_{n-1} + c_1' + c_2) \end{aligned}$$

where c_1' is the maximum of the c_1's for all the $-q_i$'s.

Doing this repeatedly gives us that

$$\begin{aligned} h(p_n) &\leq \left(\frac{2}{m^2}\right)^n h(p) + (c_1' + c_2)\sum_{i=1}^{n} \frac{2^{n-1}}{m^{2n}} \\ &< \left(\frac{2}{m^2}\right)^n h(p) + \frac{c_1' + c_2}{m^2 - 2} \\ &\leq 2^{-n} h(p) + (c_1' + c_2)/2. \end{aligned}$$

So if n is big enough we can make $h(p_n) < 1 + (c_1' + c_2)/2$. Since p is a linear combination of p_n and the q_i's and there are only finitely many elements α of height less than $1 + (c_1' + c_2)/2$, those α's and the q_i's generate A. □

3. The Weak Mordell-Weil Theorem

In order to apply the Descent Theorem to the rational points on an elliptic curve, we need two things: a height function on $\mathbb{Q}$ satisfying the conditions of the theorem, and that $E(\mathbb{Q})/mE(\mathbb{Q})$ is finite where m is the number used in the Descent Theorem. The second of these is the focus of this section. In fact, we will prove something stronger [4, 190]:

Theorem 3.1 (Weak Mordell-Weil)**.** *If $K/\mathbb{Q}$ is a finite extension, and E is an elliptic curve in $\mathbb{P}^2(\bar{K})$ defined over K, then for each $m \geq 2$, $E(K)/mE(K)$ is finite.*

We first prove a series of reductions, and at the end we will take advantage of a finiteness result from algebraic number theory. (For a group G and a natural number m, we write $G[m]$ for the set of elements $g \in G$ with $mg = 0$.)

Lemma 3.2. *If L/K is a finite Galois extension and $E(L)/mE(L)$ is finite, then so is $E(K)/mE(K)$.*

Proof. Let Φ be the kernel of the obvious map from $E(K)/mE(K)$ to $E(L)/mE(L)$. For each $P \in \Phi$, pick a Q_P in $E(L)$ with $mQ_P = P$, and define $\lambda_P(\sigma) = \sigma(Q_P) - Q_P$ for each $\sigma \in \mathrm{Gal}(L/K)$. It is easy to check that λ_P lands in $E[m]$, that it is well-defined, and that if $\lambda_P = \lambda_{P'}$, then $P = P'$ in $E(K)/mE(K)$. So the map sending P to λ_P is injective, but there are only finitely many maps from $\mathrm{Gal}(L/K)$ to $E[m]$, so Φ is finite. ($E[m]$ is the kernel of the multiplication-by-m map, which is representable by a rational function, so it must be finite.) So both the image and kernel of the aforementioned map from $E(K)/mE(K)$ to $E(L)/mE(L)$ are finite, so $E(K)/mE(K)$ is finite. □

In light of this statement, it is enough to prove Weak Mordell-Weil under the assumption that $E[m]$ is contained in $E(K)$ (note that, as mentioned in the proof above, $E[m]$ is finite): according to the explicit formulas for the group operation on an elliptic curve given in 1.7, membership in the kernel may be specified by a polynomial in x and y, and adjoining the roots of that polynomial gives us a finite extension of K with the desired property, to which we may apply 3.2.

We now reduce the question of the finiteness of $E(K)/mE(K)$ to a question about the finiteness of a certain field extension:

Lemma 3.3. *Let L be the composite of all extensions $K(Q)$ over all Q with $mQ \in E(K)$. If L/K is a finite extension, then $E(K)/mE(K)$ is finite.*

Proof. Define the map $\kappa : E(K) \times \mathrm{Gal}(\bar{K}/K) \to E[m]$ as follows: for $P \in E(K)$, pick $Q \in E(\bar{K})$ with $mQ = P$; then $\kappa(P, \sigma) = \sigma(Q) - Q$. It is straightforward to check that this map is bilinear and independent of the choice of Q. The kernel of κ on the left is $mE(K)$, because if $\kappa(P, \sigma) = 0$ for all σ, then each σ fixes the Q with $mQ = P$, so the entries of Q are in the fixed field of $\mathrm{Gal}(\bar{K}/K)$, i.e., $Q \in E(K)$, so $P \in mE(K)$. The kernel on the right is $\mathrm{Gal}(\bar{K}/L)$: if σ fixes L, then the Q for each P is in L by definition, so $\kappa(\sigma, P) = O$ for each P, and if σ is in the kernel, then σ fixes every Q with $mQ \in E(K)$, so σ fixes L.

This gives a perfect bilinear pairing $E(K)/mE(K) \times \mathrm{Gal}(L/K) \to E[m]$, so $E(K)/mE(K) \cong \mathrm{Hom}(\mathrm{Gal}(L/K), E[m])$, but, as mentioned above, $E[m]$ is finite, so the lemma follows. □

Suppose v is a discrete valuation on K. Since E is an elliptic curve over K, we may consider it as an elliptic curve over the completion K_v of K with respect to v. Replacing X and Y by $u^{-2}X$ and $u^{-3}Y$ respectively, one can easily see that each coefficient a_i in the Weierstrass equation for E is replaced by $u^i a_i$. So by doing this with an appropriate u we can find a Weierstrass equation for E so that $v(a_i) \geq 0$ for each i and $v(\Delta)$ is as small as possible. This is called a minimal Weierstrass equation for E.

Given a minimal Weierstrass equation for E over K_v we may reduce the coefficients with respect to the maximal ideal of K_v to obtain a new elliptic curve $\tilde{E}_v$ in $\mathbb{P}^2(k_v)$, where k_v is the residue field of K_v.

Definition 3.4. We say E has *good reduction at* v if $\tilde{E}_v$ is nonsingular. Otherwise, we say E has *bad reduction at* v.

In order to proceed we will need the following fact, whose proof would unfortunately take took long to include here. For a proof, see [4, 176].

Lemma 3.5. *Suppose v is a discrete valuation over K, $v(m) = 0$, and E has good reduction at v. Then the map $E(K)[m] \to \tilde{E}_v(k_v)$ given by the reduction described above is injective.*

Definition 3.6. If v is a valuation on K, L is an algebraic extension of K, and v' is a place of L lying above v, then the *inertia group of v' over v* is the subgroup $I_{v'/v}$ of $\mathrm{Gal}(L_{v'}/K_v)$ which act trivially on the residue field $k_{v'}$ of $L_{v'}$. We say that the extension L/K is *unramified at v* if the action of the inertia group of v' over v is trivial for every v' lying above v.

Proposition 3.7. *Let L be the field defined in 3.3. Then* $\mathrm{Gal}(L/K)$ *is abelian of exponent m. Let S be the set of valuations v on K for which v is Archimedean, $v(m) \neq 0$, or E has bad reduction at v. Then if v is a valuation and $v \notin S$, L/K is unramified at v.*

Proof. From the proof of 3.3, there's an injective map from $\mathrm{Gal}(L/K)$ to $\mathrm{Hom}(E(K), E[m])$, which proves that the Galois group is abelian of exponent m.

Pick some $v \notin S$ and some Q with $mQ \in E(K)$. It's enough to show that $K(Q)/K$ is unramified at v, since L is the composite of all such extensions. Pick some place v' of $K(Q)$ lying above v. Since E has good reduction at v, it clearly also does at v'. Let r be the reduction map $E(K(Q)) \to \tilde{E}_{v'}(k_{v'})$.

Pick some σ in the inertia group of v'/v. By definition, $r(\sigma(Q)-Q) = \sigma(r(Q)) - r(Q) = r(O)$. But $m(\sigma(Q) - Q) = O$ as well, so $\sigma(Q) - Q \in E[m]$ and it's in the kernel of the reduction map, so by 3.5, σ fixes Q.

So, since $K(Q)$ is fixed by every element of the inertia group of v'/v for every v' lying above v, we see that $K(Q)/K$ is unramified at v. □

We have now established enough about the extension L/K to prove that it is finite. The proof will require a result from algebraic number theory, which we state here without proof:

Theorem 3.8 (Dirichlet's S-Unit Theorem)**.** *Let K be a finite extension of $\mathbb{Q}$, and let R be its ring of integers. If S is a finite set of valuations on R, define R_S to be the ring $\{a \in K : v(a) \geq 0$ for all $v \notin S\}$. Then the group of units $R_S^\times$ is finitely generated.*

Theorem 3.9. *If $K/\mathbb{Q}$ is a finite extension and S is a finite set of places on K containing all the non-Archimedean absolute values, and $m \geq 2$, let L/K be the maximal extension of K whose automorphism group over K is abelian of exponent m and which is unramified outside of S. Then L/K is a finite extension.*

Proof. First, note that if the theorem is true for some finite extension K' of K (replacing S with the set S' of places of K' lying above S), then we would have that LK'/K' finite, so L/K would be as well. Therefore, we may assume K contains the m'th roots of unity.

We can also make S bigger, since this will only make L bigger. Since the class number of K is finite (since K is a finite extension of $\mathbb{Q}$; this is a fundamental

fact of algebraic number theory, cf. [3, 34]), we may add finitely many places to S to make the ring R_S described above into a principal ideal domain. We may also throw in every v for which $v(m) \neq 0$.

By the primary theorem of Kummer theory (cf. [1, 626, 816]), because K contains the m'th roots of unity, abelian extensions of K of exponent m are obtained by adjoining m'th roots of elements of K. Pick some (normalized) valuation $v \notin S$. Since $v(m) = 0$, one may check that $K_v(\sqrt[m]{a})/K_v$ is unramified if and only if $m|v(a)$. So L is obtained by adjoining m'th roots of elements of T_S, where

$$T_S = \{a \in K^\times/(K^\times)^m : m|v(a) \text{ for all } v \notin S\}.$$

We just need to check that T_S is finite.

There is a natural map $R_S^\times \to T_S$. For any $a \in K^\times$ whose residue is in T_S, we know that aR_S is the m'th power of some ideal of R_S, since $v(a)$ is a multiple of m for each $v \notin S$. So for some unit u, we have $a = ub^m$ for some $b \in K^\times$, because R_S is a principal ideal domain. Now, $u \in R_S^\times$, but our map sends u to the residue of a, so our map is surjective. And the kernel obviously contains the m'th powers, so we have a surjection $R_S^\times/(R_S^\times)^m \to T_S$. By Dirichlet's S-Unit Theorem, $R_S^\times$ is finitely generated, so that quotient is finite, so T_S is finite, as desired. □

4. Height over $\mathbb{Q}$

Our next task should be to find a height function on $E(\mathbb{Q})$ with the properties we need. First we note that, since $\mathbb{Q}$ has characteristic 0, we may simplify our Weierstrass equation even further. It is left to the reader to check that in this case, with an appropriate change of coordinates, we may assume that the equation looks like

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

for some A and B. We define a height function as follows:

Definition 4.1. For any rational number p/q with $\gcd(p, q) = 1$, define $H(p/q) = \max\{|p|, |q|\}$. Then for any point in $E(\mathbb{Q})$, define $h_x([x : y : 1]) = \log H(x)$ and $h_x([0 : 1 : 0]) = 0$.

We now show that h_x satisfies the conditions of the Descent Theorem:

Proposition 4.2. [4, 202]

(a) If $P_0 \in E(\mathbb{Q})$ then there is a constant c_1 so that for all $P \in E(\mathbb{Q})$, we have

$$h_x(P + P_0) \leq 2h_x(P) + c_1$$

s.

(b) There is a constant c_2 so that for all $P \in E(\mathbb{Q})$, $h_x(2P) \geq 4h_x(P) - c_2$.

(c) For every k, the set $\{P \in E(\mathbb{Q}) : h_x(P) \leq k\}$ is constant.

Proof. With appropriate final adjustments to c_1, we may assume that $P, P_0 \neq O$ and $P \neq \pm P_0$. Let $P = [x : y : 1], P_0 = [x_0 : y_0 : 1]$ where $x = a/d^2$, $y = b/d^3$, $x_0 = a_0/d_0^2$, $y_0 = b_0/d_0^3$ in lowest terms. (It is easy to verify from the Weierstrass equation that they may be put into this form.)

Using the addition formula given in 1.7 and the Weierstrass equation, one may verify that the x coordinate of $P + P_0$ (after normalizing with $z = 1$) is

$$x(P + P_0) = \frac{(aa_0 + Ad^2d_0^2)(ad_0^2 + a_0d^2) + 2Bd^4d_0^4 - 2bdb_0d_0}{(ad_0^2 - a_0d^2)^2}.$$

Cancelling common factors would only make the height smaller, so we get that $H(x(P+P_0)) \leq c\max\{|a|^2, |d|^4, |bd|\}$. Now, $H(x(P)) = \max\{|a|, |d|^2\}$, so except for the $|bd|$ this is what we want.

But from the Weierstrass equation, we get that

$$b^2 = a^3 + Aad^4 + Bd^6,$$

so $|b| \leq c' \max\{|a|^{3/2}, |d|^3\}$, so $|bd|$ won't affect the maximum. This proves (a).

With appropriate final adjustments to c_2, we can force our height to be above those of the finitely many points of $E(\mathbb{Q})[2]$, allowing us to assume that $2P \neq O$. Set $P = [x : y : 1]$. Using the addition formula, we get that the x coordinate of $2P$ is

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}.$$

Let

$$F(X,Z) = X^4 - 2AX^2Z^2 - 8BXZ^3 + A^2Z^4,$$
$$G(X,Z) = 4X^3Z + 4AXZ^3 + 4BZ^4.$$

Then writing $x = a/b$ in lowest terms, it is clear that $x(2P) = F(a,b)/G(a,b)$.

Let $\Delta = 4A^3 + 27B^2$ be the discriminant of E. We leave it to the reader to check that there are cubic homogeneous polynomials f_1, g_1, f_2, g_2 so that

$$f_1F - g_1G = 4\delta Z^7,$$
$$f_2F + g_2G = 4\delta X^7.$$

(Check that F and G are relatively prime if $\Delta \neq 0$.) Let $\delta = \gcd(F(a,b), G(a,b))$. From the equations just proved, it is clear that δ divides 4Δ, so $H(x(2P)) \geq \max\{F(a,b), G(a,b)\}/|4\Delta|$. Using the homogeneity of the f_i's and the g_i's, the equations also tell us that

$$\max\{|4\Delta a^7|, |4\Delta b^7|\} \leq 2c\max\{|a|^3, |b|^3\}\max\{F(a,b), G(a,b)\},$$

and cancelling and making the appropriate substitutions gives us that $H(x(2P)) \geq (2c)^{-1}H(x(P))^4$, which implies (b).

The set $\{t \in \mathbb{Q} : H(t) \leq k\}$ is obviously finite, and for a given rational there are at most two points on the curve with that number as an x value, so (c) is clear. □

Remark 4.3. This, together with Weak Mordell-Weil and the Descent Theorem, shows that $E(\mathbb{Q})$ is finitely generated. Given the way Weak Mordell-Weil was stated and proved, it is natural to ask whether $E(K)$ is finitely generated for any finite extension K over $\mathbb{Q}$. The answer is yes, and one may construct a height function on such a K, though the construction and the proof that it satisfies the hypotheses of the Descent Theorem will be a bit more complicated than they were for $\mathbb{Q}$.

References

[1] David S. Dummit and Richard M. Foote. Abstract Algebra: Third Edition. John Wiley and Sons. 2004.
[2] William Fulton. Algebraic Curves. ⟨http://www.math.lsa.umich.edu/∼wfulton/CurveBook.pdf⟩. 2008.
[3] Jürgen Neurkirch. Algebraic Number Theory. Springer-Verlag. 1999.
[4] Joseph H. Silverman. The Arithmetic of Elliptic Curves. Springer-Verlag. 1986.