Rational Points, Heights, and the Rank of Elliptic Curves

Salman Butt*

January 20, 2002

Mathematics Department
Princeton University
Princeton, NJ 08544

Abstract

Lutz-Nagell and Silverman provide an effective method of determining all torsion and integer points on the curve $E : x^3 + y^3 = m$, respectively. A standard lattice point counting argument asymptotically gives us the number of points with bounded height, both integral and non-integral. From Silverman, we know there is a finite number of integral points, but we are concerned with exactly how many integral points there are and how large they can be. We also investigate how, if at all, the number of rational solutions and their heights vary with m and with the rank of the curve.

*E-mail: `sbutt@math.princeton.edu`

1 Theory

1.1 Previous Work

The Mordell-Weil theorem is one of the most fundamental theorems concerning rational points on elliptic curves.

Theorem 1.1 *(Mordell-Weil) If E is an elliptic curve over $\mathbb{Q}$, then the abelian group $E(\mathbb{Q})$ is finitely generated.*

Proof: this proof can be found in any standard text on elliptic curves, including [1] and [3]

A straightforward application of the structure theorem for finitely generated abelian groups allows us to write $E(\mathbb{Q})$ as

$$\begin{aligned} E(\mathbb{Q}) &= \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus \mathbb{Z}_{/m_1\mathbb{Z}} \oplus \cdots \oplus \mathbb{Z}_{/m_s\mathbb{Z}} \\ &= \mathbb{Z}^{r_g} \oplus T \end{aligned} \tag{1.1}$$

where r_g is the **geometric rank** of the curve ($\mathbb{Z}$ occurs r_g times) and T is the torsion group, $T = \mathbb{Z}_{/m_1\mathbb{Z}} \oplus \cdots \oplus \mathbb{Z}_{/m_s\mathbb{Z}}$.

Note: $\mathbb{Z}^{r_g}$ is sometimes also referred to as $E(\mathbb{Q})_{ind}$ since its generators are linearly independent points.

The Lutz-Nagell theorem provides an algorithm for determining the torsion points in $E(\mathbb{Q})$.

Theorem 1.2 *(Lutz-Nagell) For $E : y^2 = x^3 + Ax + B$ over $\mathbb{Q}$, the finite abelian group F can be computed as follows:*
If $P = (x, y)$ is in F (i.e. $P \in E(\mathbb{Q})$), then
(1) $x, y \in \mathbb{Z}$
(2) $y = 0$ and P has order 2
***or** $y \neq 0$ and $y^2 \mid D$ where D is the discriminant, $D = -4A^3 - 27B^2$.*

Proof: this proof has been omitted for brevity, but can be found in [1] and [3]. $\square$

In fact, Lutz-Nagell holds if E is in the more general form $y^2 = x^3 + Ax^2 + Bx + C$. Silverman's theorem provides a bound on the number of integer points on the curve of interest to us.

Theorem 1.3 *(Silverman) Let $m \geq 1$ be an integer, and let C_m be the cubic curve*

$$C_m : x^3 + y^3 = m \tag{1.2}$$

There is a constant $\kappa > 1$, independent of m, so that

$$\#\{(x,y) \in C_m(\mathbb{Q}) : x, y \in \mathbb{Z},\ gcd(x,y) = 1\} \leq \kappa^{1+rank\ C_m(\mathbb{Q})} \tag{1.3}$$

where $\#(\cdot)$ refers to the number of elements in a set.

Proof: For a more detailed proof of this theorem, see [2]. Silverman first proves two important theorems:

Lemma 1.4 *Let $D \in \mathbb{Z}$ and $c, \gamma \in \mathbb{R}$ be given. Then there are absolute constants c_1, c_2, c_3 and a constant $m_0 = m_0(D, c, \gamma)$ so that for all sixth-power-free integers m satisfying $|m| > m_0$,*

$$\#\{P \in E_{mD}(\mathbb{Q}) : h(P) < c \log |m| + \gamma\} < c_1(c_2\sqrt{c + c_3} + 1)^{rank\ E_{mD}(\mathbb{Q})} \tag{1.4}$$

where $E_D : Y^2Z = X^3 + DZ^3$ is the elliptic curve in the projective plane $(D \neq 0)$ and h is the Mordell-Weil height

$$h(P) = \log \max\{|x|, |y|, |z|\} \tag{1.5}$$

for $P = (x, y, z)$.

Lemma 1.5 *Let $f(x,y) \in \mathbb{Z}[x,y]$ be a homogeneous form of degree n with at least 3 distinct roots in $\bar{\mathbb{Q}}$. Then there are effectively computable constants $c = c(n)$, $\gamma = \gamma(f)$, and $m_0 = m_0(f)$ so that for all $m \in \mathbb{Z}$ with $|m| > m_0$, the set*

$$\{(x,y) \in \mathbb{Z}^2 : f(x,y) = m \text{ and } \max(|x|, |y|) > \gamma |m|^c\} \tag{1.6}$$

contains at most n elements if n is odd, $2n$ elements if n is even.

Lemma 1.4 provides a bound on the number of rational points on $E_D : Y^2 = X^3 + D$ whose height is bounded by effectively computable constants. Lemma 1.5 gives an upper bound for the size of "almost all" of the integral solutions to any homogeneous form $f(x,y) = m$, specifically C_m. That is, except for n or $2n$ number of points, $\max\{|x|, |y|\} < \gamma |m|^c$ where γ, c, m_0 are effectively computable.

From here, C_m is mapped to its Jacobian, which has the Weierstrass form $Y^2 = X^3 + D$ required by Lemma 1.4. From Lemma 1.5, we have an upper bound for the height of almost all of the integer points on the curve C_m. This upper bound also provides an upper bound for the heights of the images of these integer solutions to the Jacobian. Applying Lemma 1.4 to the Jacobian then gives us the desired inequality. $\square$

The constant κ can be taken to be quite small. For all sufficiently large cube-free m,

$$\#\{(x,y) \in C_m(\mathbb{Q}) : x, y \in \mathbb{Z},\ gcd(x,y) = 1\} < 9(15^{rank\ C_m(\mathbb{Q})} + 1). \quad (1.7)$$

Thus we have for these curves two methods for determining $C_m(\mathbb{Q})_{tors}$ as well as an upper bound on the number of integer points on the curve. We are left with determining points in $C_m(\mathbb{Q})_{ind}$ which are not necessarily integer. Unlike Silverman's theorem which deals with the finite set of integer points, we cannot expect to find a similar bound on the number of rational points that only depends on a constant κ and the rank of the curve, since the set of rational points is infinite. Instead, we restrict the number of rational points under study by making use of height functions.

1.2 Heights

The height functions measure how complicated a rational point is from the view of number theory. The functions have many applications, including proving Mordell's Theorem (Silverman-Tate). Let us begin by defining the naive height h_0 for a general curve E:

Definition 1.6 *(Naive height) Let $P = (x,y)$, $P \in E(\mathbb{Q})$ so that $x = \frac{m}{n}$.*

$$h_0(P) = h_0(x) = \log \max\{|m|, |n|\} \quad (1.8)$$

Another height function of interest to us is the canonical height $\hat{h}$:

Definition 1.7 *(Canonical height) For any $P \in E(\mathbb{Q})$,*

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h_0(2^n P)}{4^n} \quad (1.9)$$

Note: A **point of low height** is one whose height is small relative to another specified quantity. Since we still have yet to collect data, defining this quantity is difficult since low height is a relative term. Constructing a scale for comparison is not obvious since heights could vary enormously in a family if one is not careful about which curves to observe.

Our working definition makes use of curves in the family with odd functional equation and with rank 1. The Mordell-Weil group is thus generated by a single point P_1 with height $\hat{h}(P_1)$. Now, if we find other curves in this family with odd functional equation whose rank is 3, we will have two more linearly independent generators. We can then compare their heights to the original point P_1, defining $\hat{h}(P_1)$ as the quantity used for comparison. Unfortunately, this definition only makes sense for a special series of points $P_1(m) = (x(m), y(m))$ such that for all m sufficiently large, $P_1(m)$ is on the elliptic curve C_m. Thus each curve has a point forced on it with height $\hat{h}(P_1(m))$, allowing us to compare the new generators.

Another possibility would be to take m in the interval $[N, 2N]$ for some large N. With such an m, the coefficients and conductors of the elliptic curves will be about the same. We can then observe how the heights vary between curves in the family, specifically how they change for curves of "extra" rank (i.e. those with more linearly independent points). But the final definition of points of low height will ultimately depend on our results.

There are three important properties of heights that will be especially useful to us.

Proposition 1.8 *Let $\hat{h}$ be the canonical height and $P, Q \in E(\mathbb{Q})$*
(1) The Parallelogram Law:

$$\hat{h}(P+Q) = 2\hat{h}(P) + 2\hat{h}(Q) - \hat{h}(P-Q). \tag{1.10}$$

(2) For any integer m,

$$\hat{h}(mP) = m^2\hat{h}(P). \tag{1.11}$$

(3) P is a point of finite order if and only if

$$\hat{h}(P) = 0 \tag{1.12}$$

Note: the parallelogram law holds for any quadratic form (or, equivalently, any bilinear form).

Proof: We will be proving (1) only — the proof of (2) and (3) can be found in [1] and [3]. We assume (2), i.e. $\hat{h}$ is a quadratic form. First note that any quadratic form corresponds to a unique bilinear form and vice versa. Given a quadratic form q, define a bilinear form b by $b(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y))$. There are two basic properties to check:

$$\begin{aligned}
b(\lambda x + y, z) &= \lambda b(x,z) + b(y,z) \\
b(x, \lambda y + z) &= \lambda b(x,y) + b(x,z)
\end{aligned} \tag{1.13}$$

Unfortunately, we were not able to verify these in time for this paper since a useful exposition of the properties of quadratic forms could not be found. But we were able to show that given a bilinear form b, one can define q by $q(x) = b(x,x)$ such that q is a quadratic form:

$$\begin{aligned}
q(ax) &= b(ax, ax) \\
&= ab(x, ax) \\
&= a^2 b(x,x) \\
&= a^2 q(x)
\end{aligned} \tag{1.14}$$

Assuming we are able to verify the properties of 1.13, we have good definitions of $q(x)$ and $b(x,y)$ in terms of the other. Now, assuming Proposition 1.8.2, we identify the bilinear form $b(P,Q)$ as $\langle P,Q\rangle$. So,

$$\begin{aligned}
\hat{h}(P+Q) &= \langle P+Q, P+Q\rangle \\
&= \langle P,P\rangle + 2\langle P,Q\rangle + \langle Q,Q\rangle \\
&= \hat{h}(P) + 2\langle P,Q\rangle + \hat{h}(Q)
\end{aligned} \tag{1.15}$$

$$\begin{aligned}
\hat{h}(P-Q) &= \langle P-Q, P-Q\rangle \\
&= \langle P,P\rangle - 2\langle P,Q\rangle + \langle Q,Q\rangle \\
&= \hat{h}(P) - 2\langle P,Q\rangle + \hat{h}(Q)
\end{aligned} \tag{1.16}$$

Combining these two results, we get

$$\begin{aligned}
\hat{h}(P+Q) + \hat{h}(P-Q) &= \hat{h}(P) + 2\langle P,Q\rangle + \hat{h}(Q) + \hat{h}(P) - 2\langle P,Q\rangle + \hat{h}(Q) \\
&= 2\hat{h}(P) + 2\hat{h}(Q).
\end{aligned} \tag{1.17}$$

This verifies the assertion. $\square$

1.3 Heights and Rank

At the core of our investigations we are attempting to find relations between properties of elliptic curves, specifically height and rank. In this section, we motivate the choice of these two propeties.

Proposition 1.9 *(Knapp) For $E : y^2 = x^3 + Ax + B$, the following formula is valid as $\tau \to \infty$:*

$$\begin{aligned} \#\{(x,y) \in E(\mathbb{Q}) : |x|_\infty \le \tau\} &= \#(T) & if\ r_g = 0 \quad (1.18) \\ \textbf{\textit{or}} &\approx \frac{\#(T)\Omega_{r_g}}{R_{E/\mathbb{Q}}^{1/2}} (\log \tau)^{r_g/2} & if\ r_g > 0 \quad (1.19) \end{aligned}$$

*where T is the torsion group, $x = \frac{m}{n}$, $|x|_\infty = \max\{|m|, |n|\}$, Ω_{r_g} is the volume of the unit ball in $\mathbb{R}^{r_g}$, and $R_{E/\mathbb{Q}}^{1/2}$ is the **elliptic regulator** of E over $\mathbb{Q}$, $R_{E/\mathbb{Q}} = det(\langle P_i, P_j \rangle)$.*

Proof: A more detailed and complete proof can be found in [1]. If $r > 0$, the result is immediate. Knapp's argument requires Euclidean Fourier analysis and counting lattice points in $\mathbb{Z}^{r_g}$. We need to know how many lattice points are in the unit r_g-sphere, which introduces the Ω_{r_g} factor. The square root of the determinant of the height matrix comes from the fact that the determinint measures the size of the fundamental parallelpiped. Basically for every volume equal to the determinant of the height matrix, you get one lattice point. Thus, the larger the determinant, the fewer lattice points you get. The number of torsion points enters in multiplicatively, since they do not affect the canonical height of a point $P \in E(\mathbb{Q})_{ind}$ by Proposition 1.8.1 and 1.8.3. So once we determine a relation for the number of points with canonical height less than τ, we can multiply by $\#(T)$, the number of torsion points we have. Then, since $\hat{h} - h_0$ is bounded and $r > 0$, the same estimate is valid for h_0. The $(\log T)^{r_g/2}$ factor is the result of further analysis. $\square$

Knapp's proof makes use of concepts beyond our knowledge. We therefore provide another theorem whose proof is simpler and which gives a lower bound of the same order of magnitude as Knapp's estimate.

Theorem 1.10 *Let $E : x^3 + y^3 = m$ (i.e. $E = C_m$) be an elliptic curve with geometric rank $r_g > 0$ and let α be a bound on the height of points in $E(\mathbb{Q})_{ind}$. There exists a constant K_{r_g} depending on r_g and on the maximum height of the generators of $\mathbb{Z}^{r_g}$ such that*

$$\#\{P \in E(\mathbb{Q}) : \hat{h}(P) \le \alpha\} \ge K_r \alpha^{\frac{r_g}{2}} \tag{1.20}$$

Proof: We want to take a point P on E that can be written as the linear combination of the generators of $E(\mathbb{Q})_{ind}$. Since we will only be looking for a lower bound on the number of points, we can ignore those points which are of the form $P+t$ where $P \in E(\mathbb{Q})_{ind}$ and $t \in T$ (T is the torsion group). In fact, since the addition of torsion points will not change the canonical height, we can add any torsion points we have to our point P without changing $\hat{h}(P)$. Supposing there are $\#(T)$ torsion points, we can simply multiply our lower bound by $\#(T)$ for the extra possible combinations to get a lower bound that includes torsion points, similar to Knapp's proof. Thus, we can restrict ourselves to points in $E(\mathbb{Q})_{ind}$.

$$P = \sum_{i=1}^{r_g} n_i Pi \tag{1.21}$$

where r_g is the geometric rank of E. Inductively using Proposition 1.8.1 and 1.8.2, we get for the height of P:

$$\begin{aligned}
\hat{h}(\sum_{i=1}^{r_g} n_i Pi) &= \hat{h}(n_1P_1 + n_2P_2 + \cdots + n_{r_g}P_{r_g}) \\
&\leq 2\hat{h}(n_1P_1) + 2\hat{h}(n_2P_2 + \cdots + n_{r_g}P_{r_g}) \\
&\leq 2\hat{h}(n_1P_1) + 2(2\hat{h}(n_2P_2) + 2\hat{h}(n_3P_3 + \cdots + n_{r_g}P_{r_g})) \\
&\vdots \\
&\leq 2\hat{h}(n_1P_1) + 2^2\hat{h}(n_2P_2) + \cdots + 2^{r_g}\hat{h}(n_{r_g}P_{r_g}) \\
&\leq 2^{r_g-1}\sum_{i=1}^{r_g}\hat{h}(n_iPi) \\
&\leq 2^{r_g-1}\sum_{i=1}^{r_g} n_i^2\hat{h}(P_i)
\end{aligned} \tag{1.22}$$

Now let $c = \max_i\{\hat{h}(P_i)\}$ and bound the n_i's by $\frac{N+1}{2}$, $|n_i| \leq \frac{N+1}{2}$:

$$\begin{aligned}
\hat{h}(\sum_{i=1}^{r_g} n_i Pi) &\leq 2^{r_g-1}\frac{(N+1)^2}{4}cr_g \\
&\leq 2^{r_g-3}(N+1)^2 cr_g
\end{aligned} \tag{1.23}$$

From the definition of P we have

$$\sum_{i=1}^{r_g} n_i P_i = n_1P_1 + n_2P_2 + \cdots + n_{r_g}P_{r_g} \tag{1.24}$$

There are $N+1$ choices for each n_i (including $n_i = 0$), which implies there are at least $(N+1)^{r_g}$ points whose height is less than $2^{r_g-3}(N+1)^2 cr_g$ (there may exist points whose n_i's are larger than $\frac{N+1}{2}$ but whose heights are bounded by $2^{r_g-3}(N+1)^2 cr_g$). Let $\alpha = 2^{r_g-3}(N+1)^2 cr_g$. So,

$$N+1 = (\frac{\alpha}{2^{r_g-3}cr_g})^{\frac{1}{2}} \tag{1.25}$$

$$\Rightarrow (N+1)^{r_g} = (\frac{\alpha}{2^{r_g-3}cr_g})^{\frac{r_g}{2}} \tag{1.26}$$

Thus,

$$\#\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq \alpha\} \geq K_{r_g} \alpha^{\frac{r_g}{2}} \tag{1.27}$$

where α is defined as above and $K_{r_g} = (\frac{1}{2^{r_g-3}cr_g})^{\frac{r_g}{2}}$. $\square$

Thus we arrive at a similar lower bound to Knapp's relation, except our factor K_{r_g} depends on the maximum height of the Mordell-Weil group generators in addition to the rank.

2 Implementation

2.1 Preliminaries

Let us first make the switch from $x^3 + y^3 = m$ to Weierstrass form.

Proposition 2.1

$$x^3 + y^3 = m \Leftrightarrow y^2 = x^3 + 2^4 \cdot (-3)^3 \cdot m^2 \tag{2.28}$$

Proof: First make the switch to the projective plane:

$$x^3 + y^3 = m \Rightarrow x^3 + y^3 = mz^3 \tag{2.29}$$

Now, in the projective plane, we identify two solutions if they differ by a multiple $r \in \mathbb{Q}$. Thus $(x_1, y_1, z_1) \approx (x_2, y_2, z_2)$ if $(x_1, y_1, z_1) = r(x_1, y_1, z_1)$. Further, if we have a solution (x_1, y_1, z_1) for which $z \neq 0$, then it is equivalent to a solution of the form $(x_2, y_2, 1)$ since $(x_1, y_1, z) = z(\frac{x_1}{z}, \frac{y_1}{z}, 1)$ for $z \neq 0$.

On the other hand, if $z = 0$, we have $(x, y, 0)$. If $y = 0$, then $x = 0$ necessarily and we get the point $(0, 0, 0)$ which is not counted since it is not in the projective plane. If $y \neq 0$, we can factor out y to get $y(\frac{x}{y}, 1, 0)$. This forces $\frac{x}{y} = 0$ and we get the point at infinity.

To then make the switch from $x^3 + y^3 = mz^3$ to Weierstrass form, we perform the following substitions:

$$\begin{array}{rcll}
3x(y^2+xy) & = & -x^3 - mz^3 & from \quad x \to x+y \\
3x(y+\frac{1}{2}x)^2 & = & -\frac{1}{4}x^3 - mz^3 & from \quad y \to y - \frac{1}{2}x \\
3xy^2 & = & -x^3 - 2^2mz^3 & from \quad y \to \frac{1}{2}y \\
3y^2z & = & -z^3 - 2^2mx^3 & from \quad x \to z,\ z \to x \\
y^2z & = & -2^2mx^3 - 3^3z^3 & from \quad y \to \frac{1}{9}y,\ x \to \frac{1}{3}x \\
y^2z & = & -x^3 - 2^4 \cdot 3^3 m^2 z^3 & from \quad y \to \frac{y}{2^2m^2}, x \to \frac{x}{2^2m} \\
y^2z & = & x^3 + 2^4 \cdot (-3)^3 \cdot m^2z^3 & from \quad x \to -x. \ \square
\end{array}$$

2.2 Algorithm

We now discuss the algorithm we developed with Ellen Eischen to determine ratonal points and their heights on the curve C_m.

We first make a change of variables: $Y^2 = X^3 + 2^4 \cdot (-3)^3 \cdot m^2$. If there are rational solutions to this curve, a simple algebraic computation shows they must be of the form $Y = \frac{y_1}{c^3}$ and $X = \frac{x_1}{c^2}$. We can multiply out giving us:

$$y_1 = \sqrt{x_1^3 - 432m^2c^6}. \tag{2.30}$$

Let $D = x_1^3 - 432m^2c^6$, so $y_1 = \sqrt{D}$. We want to iterate x_1 from $-\alpha$ to α (where α is the previously mentioned bound on height and which we want to take as large as possible) and c from 1 to $\sqrt{\alpha}$ (i.e. $c^2 \leq \alpha$), checking to make sure $gcd(x, c) = 1$ (if $gcd(x, c) \neq 1$, then we have already checked the point). If $D < 0$, we know immediately that this choice of x_1, c will not give us a rational solution. To determine candidate points on the curve for $D > 0$, we observe that if x_1 and c correspond to a rational solution, then D is a perfect square in $\mathbb{Z}$. Thus it must be a perfect square mod p for any prime p, in particular the first 10 primes. Conversely, if D is a square mod the first 10 primes, it is likely that it is a perfect square in $\mathbb{Z}$. On the other hand, if D is not a square mod the first 10 primes, then we know we cannot find a y_1 for this choice of x_1 and c. This test reduces to checking that $(\frac{x_1}{c^2})^3 + -432m^2$ is a square mod p (since c^6 is clearly the square of c^3). We note that

$$\frac{x_1}{c^2} \equiv xk \ (mod\ p) \tag{2.31}$$

where $k \equiv (c^2)^{-1}$. Using this fact, we rewrite D as $(x_1 k)^3 - 432m^2 \ (mod\ p)$. A look-up table was made with the first 10 primes and their squares. Using this table, we determined k and checked D. Computations were done $mod\ p$ in order to keep numbers small thus preventing overflow.

A noteworthy problem encountered was dealing with negative numbers. In the C programming language, the mod function is not defined for negative values. This resulted in frequent errors in our preliminary data. We corrected this by noting that we can add any multiple t of p to x_1 in order to make it positive. Then, when we reduce $mod\ p$, we get the correct solution. If we reduce x_1 first, we can take $t = 1$ since all positive t are equivalent. This gives us the following pseudocode:

```
INPUT t, p
if t≥0
   return (t % p)                where % is C's mod function
else
   t=-t
   temp=p-(t % p)
   return (temp % p)
```

Once it is verified that D was a square mod the first 10 primes, we then calculate $\sqrt{D} = \sqrt{x_1^3 - 432c^6m^2}$ for given x, c and m using C's `double` type since D could be larger than C's `long`. $\sqrt{D}$ must also be an integer in order for $Y \in \mathbb{Q}$, so we run a check to see that $d = \sqrt{D} - \lfloor\sqrt{D}\rfloor$ is close to 0 or 1. Specifically, if we take our accuracy to be 10^{-4}, we want $d < 0.001$ or $d > 0.999$. In the first case, $y_1 = \lfloor\sqrt{D}\rfloor$ while in the second case $y_1 = \lfloor\sqrt{D}\rfloor + 1$. Given these two possibilites, we have two candidate points which we send to the PARI function `oncurve()` in order to verify that the point is on the curve. If it is, we compute the canonical height using PARI's built-in height functions and determine which points belong to $C_m(\mathbb{Q})_{ind}$ and which belong to the torsion group T.

3 Results and Conclusion

Results have yet to come in, but we expect to be getting data soon.

4 Acknowledgements

I would like to thank Steve Miller, Professor Andrew Wiles, Ellen Eischen and Adam Durrett. Much thanks also to the rest of the Junior Seminar class and to my family and friends.

5 Bibliography

References

[1] A. W. Knapp. *Elliptic Curves.* Mathematical Notes 40. Princeton University Press, Princeton, N. J., 1992.

[2] J. H. Silverman. "Integer Points and the rank of Thue Elliptic Curves". *Invent. Math.* 66 (1982), 395-404.

[3] J. H. Silverman and J. Tate. *Rational Points on Elliptic Curves.* Springer-Verlag, New York, 1992.