ELLIPTIC CURVES AND RATIONAL DISTANCE SETS

W. D. PEEPLES, JR.

1. Introduction. Poincaré's paper of 1901 was perhaps the first step in the development of the arithmetic on an algebraic curve. Since his paper was published, there have been many articles on the subject. Mordell, in particular, has written a large number of papers on the topic. It was his celebrated result that the rank of any elliptic cubic is finite which was the second major step in the development of the theory. Just recently Mordell [5] published another paper on the subject. Hurwitz, Weil, Siegel, Mahler, Huff, Sansone, Nagell, and others have all added to the theory. Although these men have studied the fundamental properties of the configuration of rational points on an elliptic ternary cubic, there exist no general conditions sufficient to assure that a given curve will have an infinite number of rational points. In this paper the problem is studied from the point of view of valuation theory. It is the purpose of this paper to show that simple conditions do exist. The author became interested in this problem after reading a paper Professor Gerald B. Huff [1] at the University of Georgia published on the subject.

2. Sets of rational points on the elliptic cubic. Professor Huff showed that under the substitution

\[ s: Z_1: Z_2: Z_3 = b(a^2 w_3 + w_2): a(b^2 w_3 + w_2): w_1 \]

\[ s^{-1}: w_1: w_2: w_3 = a b (b^2 - a^2) Z_3: a b (b Z_1 - a Z_2): (-a Z_1 + b Z_2) \]

the elliptic cubic

\[ c(Z): a Z_1 (Z_2^2 - Z_3^2) - b Z_3 (Z_1^2 - Z_2^2) = 0 \]

may be put in the form

\[ c(w): w_1^2 w_3 = w_2 (w_2 + a^2 w_3) (w_2 + b^2 w_3). \]

The class of cubics \( c(Z) \) is then a subclass of the cubics given by Hurwitz, in his general and classical theorem. The theorems of this paper are for the nonhomogeneous form

\[ a x (y^2 - 1) - b y (x^2 - 1) = 0. \]

It is well known that a tangent drawn to this curve at a rational

Presented to the Society, April 21, 1951; received by the editors March 11, 1953 and, in revised form, May 16, 1953.

29
point cuts the curve in another rational point. This process of tangentialing is used to show that there are an infinite number of rational points on many curves of this type. By substituting in (1) the following theorem may be verified.

**Theorem 1.** If \((x, y)\) is a rational point on (1) and \(x \neq 0, y \neq 0\), then 
\[-x, -y, (\pm x, \mp 1/y), (\pm 1/x, \mp y)\] and 
\[(\pm 1/x, \pm 1/y)\] all are rational points on (1).

In his paper Professor Huff gives the following formula for the tangential \((x_t, y_t)\) of the point \((x, y)\).

\[
x_t = \frac{2x(y^2 + 1)}{(x^2 + 1)(y^2 - 1)},
\]
\[
y_t = \frac{2y(x^2 + 1)}{(y^2 + 1)(x^2 - 1)}.
\]

Throughout this paper \((m)\) shall be used to designate the field of rational numbers and \([m]\) the integral domain of whole numbers.

**Definition.** Let \(x\) be an element of \((m - 0)\). Then \(x = (r/s)^2\), \(s \neq 0\) where \((r, 2) = 1\) and \((s, 2) = 1\). \(v(x)\) is defined to be \(t\).

Under this definition \(v(x)\) is a valuation of \((m)\). Using formula (1.1), Theorem 2 may be shown to be true.

**Theorem 2.** The points \((x, y), (-x, 1/y), (1/x, -y), (-1/x, -1/y)\) all have the same tangential \((x_t, y_t)\).

The other four points of Theorem 1 have the same tangential which differs from \((x_t, y_t)\) only in sign. Thus the valuations of the coordinates of the tangentials of the points of Theorem 1 are all the same.

The next theorems give sufficient conditions for (1) to have an infinite number of rational points on it. Lemma 3 follows directly from the definition.

**Lemma 3.** If \(x, y \in (m - 0)\) and \(v(x) = v(y)\), then \(v(x + y) > v(x)\).

**Theorem 3.** If \((x, y)\) is a rational point on (1) and \(v(x) \neq 0, v(y) \neq 0\), then there are an infinite number of rational points on (1).

**Proof.** When \(v(x) \neq 0, v(y) \neq 0\), Theorem 1 and Theorem 2 immediately reduce the proof to the case \(v(x) > 0, v(y) > 0\). Formula (1.1) states

\[
x_t = \frac{2x(y^2 + 1)}{(x^2 + 1)(y^2 - 1)}.
\]

Applying the rules for operating with valuations gives

\[
v(x_t) = v(2) + v(x) + v(y^2 + 1) - v(x^2 + 1) - v(y^2 - 1)
\]

\[
= 1 + v(x) + 0 - 0 - 0.
\]
Thus $v(x_1) = 1 + v(x)$. Similarly $v(y_1) = 1 + v(y)$. Hence $(x_1, y_1) \neq (x, y)$. But $v(x_1) > 0, v(y_1) > 0$ so that the same argument may be made using $(x_1, y_1)$ in place of $(x, y)$. Since this process may be repeated over and over again, it gives an infinite number of rational points on (1).

The following lemmas permit the application of Theorem 4 in many cases.

**Lemma 4.1.** If $(x, y)$ is a rational point on (1) with $v(y) = 0$ and $v(x) = (2^n - 1) [v(y^2 - 1) - 2]^{*0}$, or $v(x) = 0$ and $v(y) = (2^n - 1) [v(x^2 - 1) - 2]^{*0}$, then $v(x_n) = v(y_n) = 0$ where $(x_n, y_n)$ is the $n$th tangential of $(x, y)$.

**Proof.** This proof is by induction. Let $\lambda = 2^n - 1$. Assuming that the valuations of the $n - 1$ tangentials of the $x$ coordinate are positive, it will be proved that

$$v(x_n) = (\lambda - 2^n + 1) [v(y^2 - 1) - 2].$$

For $n = 1$ this states $v(x_1) = (\lambda - 1) [v(y^2 - 1) - 2]$. It is easily seen that $v(y^2 + 1) = 1$ when $v(y) = 0$. Hence, using (3.1),

$$v(x_1) = 2 + v(x) - v(y^2 - 1).$$

Substituting $v(x) = \lambda [v(y^2 - 1) - 2]$ in the above equation and collecting terms gives

$$v(x_1) = (\lambda - 1) [v(y^2 - 1) - 2].$$

Now

$$v(y_1) = v(2) + v(y) + v(x^2 + 1) - v(y^2 + 1) - v(x^2 - 1)$$

(4.1)

$$= 1 + 0 + 0 - 1 - 0 = 0.$$

Assume

$$v(x_{n-1}) = (\lambda - 2^{n-1} + 1) [v(y^2 - 1) - 2],$$

$$v(y_{n-1}) = 0.$$

It has just been shown that under these conditions

(4.2)

$$v(x_n) = 2 + v(x_{n-1}) - v(x_{n-1}^2).$$

From (1) it is seen that

$$v(a/b) = -v(x) - v(y^2 - 1).$$

But since $(x_{n-1}, y_{n-1})$ is on (1),

$$v(a/b) = -v(x_{n-1}) - v(y_{n-1}^2 - 1).$$
Thus
\[-v(y_n^2 - 1) = v(x_n - 1) - v(x) - v(y^2 - 1).\]
Substituting this in (4.2), using the induction hypothesis, and collecting terms gives
\[v(x_n) = (\lambda - 2^n + 1)[v(y^2 - 1) - 2].\]
Thus since \(\lambda = 2^n - 1\), \(v(x_n) = 0\) and, by (4.1), \(v(y_n) = 0\). The proof for \(v(x) = 0\) and \(v(y) = (2^n - 1)[v(x^2 - 1) - 2]\) is similar.

In like manner Lemma 4.2 follows.

**Lemma 4.2.** If \((x, y)\) is a rational point on (1) with \(v(y) = 0\) and \((2^n - 1)v(x) = v(y^2 - 1) - 2\), or \(v(x) = 0\) and \((2^n - 1)v(y) = v(x^2 - 1) - 2\), then \(v(x_n) = v(y_n) = 0\).

**Theorem 4.** If \((x, y)\) is a rational point on (1) and \(v(x) = v(y) = 0\) and \((x, y) \neq (\pm 1, \pm 1)\), then there are an infinite number of rational points on (1).

**Proof.** Writing
\[x = 2k_1 + 1/2k_2 + 1,\]
\[y = 2k_3 + 1/2k_4 + 1,\]
where \(k_i \in [m]\), it is easily seen that \(v(x^2 + 1) = v(y^2 + 1) = 1\) and that \(v(x^2 - 1)\) and \(v(y^2 - 1)\) are \(\geq 2\). Therefore using (3.1)
\[v(x_1) = v(2) + v(x) + v(y^2 + 1) - v(x^2 + 1) - v(y^2 - 1)\]
\[= 1 + 0 + 1 - 1 - v(y^2 - 1) \leq -1.\]

Similarly \(v(y_1) \leq -1\). Now \((x_1, y_1)\) satisfy the conditions of Theorem 3 and hence there are an infinite number of rational points on (1).

**Theorem 5.** If the conditions of Lemma 4.1 or 4.2 are satisfied, there are an infinite number of rational points on (1) provided \((x_1, y_1) \neq (\pm 1, \pm 1)\) when \(n = 1\).

**Proof.** For \(n = 1\) it is necessary to add the restriction \((x_1, y_1) \neq (\pm 1, \pm 1)\) to obtain an infinite number of rational points on (1). Professor Huff [1] proved a theorem which allows one to state that if the first tangential is not one of the four points \((\pm 1, \pm 1)\), then none of the tangentials can be equal to one of these and hence by Theorem 4 there are an infinite number of rational points on (1).

This still leaves the question of whether or not \((1)\) has an infinite number of rational points on it unanswered for some cases where \(v(x) > 0\) and \(v(y) = 0\). Since it is known that there are curves of this
type with only a finite number of rational points on them, the process should surely be expected to fail in these cases. However, the preceding theorems do give simple conditions under which a person may write down a curve of the form (1) and be certain that there are an infinite number of rational points on it.

3. Rational distance sets. When \((x, y)\) is a rational point of (1), then the distances from \((2by/y^2 - 1, 0)\) to \((0, \pm a)\) and \((0, \pm b)\) are rational. Therefore, when (1) has an infinite number of rational points (e.g. when the hypotheses of Theorem 3, or 4, or 5 are fulfilled), then there are an infinite number of points \((u, 0)\) which, together with \((0, \pm a)\) and \((0, \pm b)\), form a configuration in which all distances are rational.

Bibliography