PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 48, Number 2, April 1975

ON THE NUMBER OF COPRIME SOLUTIONS OF $y^2 = x^3 + k$

N. M. STEPHENS

ABSTRACT. Let $N'(k)$ denote the number of coprime integer solutions x, y of $y^2 = x^3 + k$. It is shown that $\limsup_{k\to\infty} N'(k) \geq 8$ and that $\limsup_{k\to-\infty} N'(k) \geq 12$.

1. Let $N'(k)$ denote the number of coprime integer solutions x, y of the equation

$$y^2 = x^3 + k. \tag{1}$$

Mohanty [2] has proved that $\limsup_{k\to\infty} N'(k) \geq 6$ by showing that the equation

$$y^2 = x^3 + (t^6 - 6t^3 + 1) \tag{2}$$

has six solutions $x, y \in Z[t]$ (Z denotes the ring of integers). These are the three solutions P_1, P_2, P_3 where

$$P_1 : x = 2, \quad y = t^3 - 3,$$
$$P_2 : x = 2t, \quad y = t^3 + 1,$$
$$P_3 : x = 2t^2, \quad y = 3t^3 - 1,$$

and $-P_1, -P_2, -P_3$ where $-P_i = (x, -y)$. If t is even integer, each pair x, y is coprime and hence $N'(t^6 - 6t^3 + 1) \geq 6$.

2. We can consider (2) as an elliptic curve E over the function field $Q(t)$ (Q is the field of rational numbers) on which there is an additive law. If (x_1, y_1) and (x_2, y_2) are two distinct points on E, their sum (x', y') is given by

$$x' = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \qquad -y' = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x' - x_1) + y_1.$$

The x, y coordinates for $P_i \pm P_j$, $1 \leq i < j \leq 3$, are given below:

Received by the editors December 18, 1973.
AMS (MOS) subject classifications (1970). Primary 10B10.

$P_1 + P_2$	$(-2t^3 + 2t^2 + 2t + 2)/(t-1)^2$	$-(t^6 - 3t^5 + 3t^4 - 8t^3 + 9t^2 + 3t + 3)/(t-1)^3$
$P_1 - P_2$	$t^4 + 2t^3 + 3t^2 - 1$	$-(t^6 + 3t^5 + 6t^4 + 4t^3 - 3t)$
$P_1 + P_3$	$(-t^4 + 2t^3 - t^2 + 2t - 1)/(t-1)^2$	$(3t^4 - 7t^3 + 3t^2)/(t-1)^3$
$P_1 - P_3$	$(2t^4 + 4t^3 + 8t^2 + 4t + 2)/(t+1)^2$	$(3t^6 + 9t^5 + 21t^4 + 22t^3 + 21t^2 + 9t + 3)/(t+1)^3$
$P_2 + P_3$	$(-t^4 + 3t^2 + 2t + 1)/t^2$	$(3t^5 - 4t^3 - 6t^2 - 3t - 1)/t^3$
$P_2 - P_3$	$(2t^4 + 2t^3 + 2t^2 - 2t)/(t-1)^2$	$-(3t^6 + 3t^5 + 9t^4 - 8t^3 + 3t^2 - 3t + 1)/(t-1)^3$

If t is an integer, the x, y coordinates of $P_1 - P_2$ are coprime. Hence, for general even values of t, there are at least eight distinct coprime solutions of (2) and so

Lemma 1. $\limsup_{k\to\infty} N'(k) \geq 8$.

Let $k(t) = t^6 - 6t^3 + 1$. From above it follows that

$$y(t)^2 = x(t)^3 + k(t) \tag{3}$$

has six solutions $(\pm P_1, \pm P_2, \pm P_3)$ with $\deg(x) \leq 2$ and $\deg(y) \leq 3$; and that

$$Y(t)^2 = X(t)^3 + (t-1)^6 k(t) \tag{4}$$

has six solutions (corresponding to $\pm(P_1 + P_2)$, $\pm(P_1 + P_3)$, $\pm(P_2 - P_3)$) with $\deg(X) \leq 4$ and $\deg(Y) \leq 6$. Consider now the effect of replacing t by $1 + 1/t$. From (3), if $x'(t) = t^2 x(1 + 1/t)$ and $y'(t) = t^3 y(1 + 1/t)$, then

$$y'(t)^2 = x'(t)^3 + k'(t)$$

where $k'(t) = t^6 k(1 + 1/t)$. From (4), if $X'(t) = t^4 X(1 + 1/t)$, $Y'(t) = t^6 Y(1 + 1/t)$ and for the same $k'(t)$

$$Y'(t)^2 = X'(t)^3 + k'(t).$$

It follows that we have 12 solutions $x(t), y(t) \in Z[t]$ of the equation

$$y^2 = x^3 + (-4t^6 - 12t^5 - 3t^4 + 14t^3 + 15t^2 + 6t + 1).$$

These are:

Q_1	$2t^2$	$-2t^3 + 3t^2 + 3t + 1$
Q_2	$2t^2 + 2t$	$2t^3 + 3t^2 + 3t + 1$
Q_3	$2t^2 + 4t + 2$	$2t^3 + 9t^2 + 9t + 3$
$Q_1 + Q_2$	$4t^4 - 4t^2 - 2t$	$-(8t^6 - 12t^4 - 6t^3 + 3t^2 + 3t + 1)$
$Q_1 + Q_3$	$t^4 + 2t^3 - t^2 - 2t - 1$	$-(t^6 + 3t^5 - 5t^3 - 3t^2)$
$Q_2 - Q_3$	$4t^4 + 16t^3 + 20t^2 + 10t + 2$	$-(8t^6 + 48t^5 + 108t^4 + 118t^3 + 69t^2 + 21t + 3)$

To check that the solutions $x(t)$, $y(t)$ are coprime for all integers t, Euclid's algorithm may be applied. For example, for $Q_1 + Q_2$:

$$8t^6 - 12t^4 - 6t^3 + 3t^2 + 3t + 1 = (2t^2 - 1)(4t^4 - 4t^2 - 2t) + (-2t^3 - t^2 + t + 1),$$

$$4t^4 - 4t^2 - 2t = (-2t + 1)(-2t^3 - t^2 + t + 1) + (-t^2 - t - 1),$$

$$-2t^3 - t^2 + t + 1 = (2t - 1)(-t^2 - t - 1) + 2t.$$

Thus, if, for some integer t, $d \mid x(t)$ and $d \mid y(t)$, then $d \mid 2t$. But $y(t)$ is odd and coprime to t, so $d = 1$. The other cases may be checked in a similar fashion.

Hence, for an infinite family of k there are 12 coprime solutions of (1). Since all but a finite number of these k are negative, it follows that:

Lemma 2. $\limsup_{k \to -\infty} N'(k) \geq 12$.

3. If $k(t)$ is a real sextic polynomial with distinct roots, then, by [1], there are at most eight real solutions $x(t)$, $y(t)$ of equation (1) with $\deg(x) \leq 2$ and $\deg(y) \leq 3$. Mohanty's solutions illustrate that six of these real solutions can lie in $Z[t]$, but it remains an open question whether there exists such a k for which there are eight solutions in $Z[t]$. Of the author's 12 solutions for Lemma 2, only six have the required restrictions on the degree.

The author expresses his thanks to the referee for the information in [1].

REFERENCES

1. D. Johnson, unpublished.

2. S. P. Mohanty, *A note on Mordell's equation* $y^2 = x^3 + k$, Proc. Amer. Math. Soc. 39 (1973), 645–646. MR 47 #4924.

MATHEMATICS INSTITUTE, UNIVERSITY COLLEGE, CARDIFF, WALES