AN EFFECTIVE VERSION OF A THEOREM OF SHIODA ON THE
RANKS OF ELLIPTIC CURVES GIVEN BY \(y^2 = f(x) + m^2\)

P. G. Walsh
Department of Mathematics, University of Ottawa, Ottawa, Ontario, Canada
gwalsh@uottawa.ca

Received: 7/21/21, Accepted: 12/24/21, Published: 1/7/22

Abstract
In this short note, we extend results in several papers by proving effectively that for \(m\) sufficiently large, an elliptic curve given by \(y^2 = f(x) + m^2\), with \(f(x)\) a cubic polynomial that splits over \(\mathbb{Z}\), has rank at least 2. This also constitutes an effective version of a theorem of Shioda.

1. Introduction
In a well known paper on a family of elliptic curves, Brown and Myers [3] prove that the rank of any elliptic curve of the form
\[ y^2 = x^3 - x + m^2, \quad m \in \mathbb{Z} \]
is always at least 2 for \(m \geq 2\). Since then, a number of other papers have been written on families of curves extending the result of Brown and Myers. These include the work of Antoniewicz [1] on curves of the form \(y^2 = x^3 - m^2x + 1\), Tadić [10] on curves of the form \(y^2 = x^3 - x + m^2\), Fujita and Nara [4] and Juyal and Kumar [6] on curves of the form \(y^2 = x^3 - m^2x + n^2\), and most recently, Hatley and Stack [5] on curves of the form \(y^2 = x^3 - x + m^6\).

In this article, we consider the slightly more general family of curves given by
\[ E_{f,m} : y^2 = f(x) + m^2, \quad (1.1) \]
in which \(f(x)\) is a cubic polynomial with three distinct integer roots \(a, b, c\), and \(m \geq 0\) is an integer. Our goal is to prove that the rank of \(E_{f,m}\) is similarly bounded from below because of the existence of independent points on the curve provided that \(m\) is large enough with respect to \(a, b, c\). In fact, it is not difficult to construct examples with relatively small \(m\) for which the result is false. For example, Voutier [11] has found that the families of curves \(y^2 = x(x - a)(x - b) + m^2\), with \((a, b, m) = (1, 4k^2, 4k^3 - 4k)\) and \((a, b, m) = (3, 8k^2 + 6, 8k^3 + 6k)\), are very often curves of rank 1.
Proving a lower bound for the rank as discussed above was the topic of an earlier version of our work prior to learning of the much earlier work of Shioda in [7], wherein he proves a lower bound of 2 for the rank of
\[ E_f(t) : y^2 = f(x) + t^2 \]
regarded as an elliptic surface. Applying Silverman’s Specialization Theorem in [8] to Shioda’s result is already enough to effectively prove the result we present here. However, we feel the methods used here are somewhat more natural, using a combination of group theoretic and Diophantine methods, and provide perhaps more hope of getting a bound for \( m \) which is closer to the truth. Indeed, we are unable to find any curve of the form (1.1) of rank 1 for which \( m \geq \max(|a|, |b|, |c|)^2 \).

We first remark that if the curve in question is given by
\[ y^2 = (x - a)(x - b)(x - c) + m^2, \]
and we let \( X = x - c \), then the curve can be rewritten as
\[ y^2 = X(X + c - a)(X + c - b) + m^2, \]
and so there is no loss in generality by restricting our focus to the case that \( f(x) \) has a root at \( x = 0 \), i.e., that \( c = 0 \). However, we will state our result in full generality.

We now state the main result of this paper.

**Theorem 1.** Let \( a, b, c \) be distinct integers. Then there is a computable constant \( C = C(a, b, c) \), depending on \( a, b, c \), with the property that if \( m > C \), then the rank of the curve
\[ y^2 = (x - a)(x - b)(x - c) + m^2 \]
is at least 2.

We fall short of proving an effective result on the torsion subgroup. In particular, it appears that for fixed \( a, b, c \), the torsion subgroup is trivial for \( m \) sufficiently large, however we are unable to effectively deal with the possibility that it has order 5. In fact, a much stronger property appears to hold; if \( \phi_5(x) \) denotes the fifth division polynomial of the curve in (1.2), our computations show that this polynomial is actually irreducible for all \( m \) sufficiently large.

**2. An Independence Criterion**

In this section we prove a simple result which will provide our overall strategy to prove Theorem 1.1.
Lemma 1. Assume that $E(\mathbb{Q})$ is $2$-torsion free. If $P$ and $Q$ are points of infinite order such that all three of $P, Q, P+Q$ are not in $2E(\mathbb{Q})$, then $P$ and $Q$ are independent.

Proof. The order of the torsion subgroup $T$ is odd by hypothesis, which by Mazur’s theorem, implies that it is one of $3, 5,$ or $7$. Let $p$ denote this order, and notice that for any $P \in T$, $P = 2 \cdot ((p+1)/2) \cdot P$, so that $P \in 2E(\mathbb{Q})$. It is well-known that if for an arbitrary rational torsion point $T$, any linear combination of $P$, $Q$, $T$ (except for $T$ alone) is not in $2E(\mathbb{Q})$, then $P$ and $Q$ are independent. The assertion now immediately follows from the observation above that $T \in 2E(\mathbb{Q})$ for any rational torsion point $T$ of odd order.

3. Proof of Theorem 1.1

Proof. We now turn our attention to the proof of Theorem 1.1. By Lemma 2.1, it is enough to prove that if $m$ is large enough, then $E$ has no rational $2$-torsion; $(a,m)$ and $(b,m)$ are not points of order $3, 5$ or $7$; $(a,m)$, $(b,m)$ and $(a,m) + (b,m)$ (which equals $(0, -m)$) are not in $2E(\mathbb{Q})$.

In order to achieve these, it becomes significantly simpler to deal with a short Weierstrass equation, and a short computation shows that the curve in (1.1), with $c = 0$ (as remarked just prior to the statement of Theorem 1.1), can be written in the form

$$Y^2 = X^3 + AX + B,$$

(3.1)

where $A = -27(a^2 - ab + b^2)$ and $B = (27m)^2 + 3A(a + b) + 27(a + b)^3$.

We begin by considering the problem of eliminating $2$-torsion. If $(r, s)$ denotes a $2$-torsion point on the curve given in (3.1), then $s = 0$ and $r$ is an integer root of the cubic therein. This implies that there is an integer $t$ for which

$$X^3 + AX + B = (X - r)(X^2 + rX + t).$$

Therefore, $A = t - r^2$ and $B = -rt$, and by substituting $t = r^2 + A$ into $B = -rt$, we see that $B = -r^3 - Ar$. Using the expression above for $B$ shows that

$$(27m)^2 = (-r)^3 + A(-r) - 3A(a + b) - 27(a + b)^3.$$ 

Therefore, the pair $(-r, 27m)$ is an integral point on the curve

$$y^2 = x^3 + Ax - (3A(a + b) + 27(a + b)^3).$$

By the main result in [2], it follows that $m \leq C_1(a, b)$.

The next step is to show that for $m$ large, both $(a,m)$ and $(b,m)$ are not points of order $3, 5$ or $7$. This is achieved by computing the division polynomials of the
curve defined by (3.1), and evaluating at \( x = a \) and \( x = b \). This was achieved using MAGMA’s Evaluate function, and not surprisingly, the resulting values were found not to be identically zero. The division polynomials were of the form \( F_{a,b}(x,m) \), and thus \( m \) is bounded in terms of \( a \) and \( b \) by the height of \( F \) after making the substitution \( x = a \) and \( x = b \) respectively. As one would expect, the largest height arose from the 7-th division polynomial, which we do not display here. If we let \( C_2(a,b) \) denote this height, then for \( m \geq \max(C_1(a,b),C_2(a,b)) \), we deduce that both \((a,m)\) and \((b,m)\) are points of infinite order. To complete the proof of Theorem 2.1, we will show that for \( m \) large enough, none of \((a,m)\), \((b,m)\) or \((0,-m)\) are in \( 2E \). We will describe the case for \((0,-m)\), as the other two cases give similar bounds. We will use the doubling formula from p.58-59 of [9], which allows us to use the equation \( y^2 = x(x-a)(x-b) + m^2 \) for our curve. In this case, the basic quantities from [9] are
\[
\begin{align*}
&\quad a_1 = a_3 = 0, a_2 = -(a + b), a_4 = ab, a_6 = m^2,
\end{align*}
\]
from which we deduce that
\[
\begin{align*}
\lambda &= \frac{3x^2 - 2(a + b)x + ab}{2y}, \\
\nu &= \frac{-x^3 + abx + 2m^2}{2y},
\end{align*}
\]
from which it follows that \( 0 = \lambda^2 + (a + b) - 2x \) and \(-m = -\lambda \cdot 0 - \nu = -\nu \). The two expressions for \( \nu \) combine to give the equation
\[
x^4 - 2abx^2 - 8m^2x + (a^2b^2 + 4m^2(a + b)) = 0.
\]
This equation in \( x \) and \( m \) satisfies the condition of Runge’s theorem on Diophantine equations (see [12]), giving an upper bound \( C_3(a,b) \) for \( m \).

Acknowledgements. The author would like to thank Adam Logan, Paul Voutier and Joe Silverman for their valuable input into this work.

References


