Canad. Math. Bull. Vol. **66** (1), 2023, pp. 166–177
http://dx.doi.org/10.4153/S0008439522000157

Integers that are sums of two rational sixth powers

Alexis Newton and Jeremy Rouse

Abstract. We prove that 164 634 913 is the smallest positive integer that is a sum of two rational sixth powers, but not a sum of two integer sixth powers. If C_k is the curve $x^6 + y^6 = k$, we use the existence of morphisms from C_k to elliptic curves, together with the Mordell–Weil sieve, to rule out the existence of rational points on C_k for various k.

1 Introduction and statement of results

Fermat's classification of which integers are the sum of two integer squares allows one to prove that if k is a positive integer and there are $a, b \in \mathbb{Q}$ with $a^2 + b^2 = k$, then there are $c, d \in \mathbb{Z}$ with $c^2 + d^2 = k$. (For more detail, see Proposition 5.4.9 of [5].)

However, when considering higher powers, the analogous result is no longer true. In particular, $6 = \left(\frac{17}{21}\right)^3 + \left(\frac{37}{21}\right)^3$ despite the fact that there are no integers x and y so that $x^3 + y^3 = 6$. In [3], Bremner and Morton prove that $5\,906 = \left(\frac{25}{17}\right)^4 + \left(\frac{149}{17}\right)^4$ is the smallest positive integer which is a sum of two rational fourth powers, but not a sum of two integer fourth powers. Their proof involves a number of explicit calculations involving class numbers and units in rings of integers of number fields.

It is natural to ask what can be said about values of $n > 4$. In particular, is there always an integer k that is a sum of two rational nth powers, but not a sum of two integer nth powers? In John Byrum's unpublished undergraduate thesis (conducted under the direction of the second author), he proves that if there is a prime $p \equiv 1 \pmod{2n}$ with $p \leq 2n^2 - n + 1$, then there is a positive integer k that is a sum of two rational nth powers, but not a sum of two integer nth powers. It is not known that one can find such a prime p. Even assuming the generalized Riemann hypothesis (GRH), the strongest known result at this time is that the smallest prime $p \equiv 1 \pmod{2n}$ is less than or equal to $(\phi(2n)\log(2n))^2$ (by Corollary 1.2 of [15]), which is not sufficiently small unless $n = 3$. It is conjectured that the smallest prime $p \equiv a \pmod{q}$ satisfies $p \ll q^{1+\varepsilon}$, which would be sufficient.

The goal of the present paper is to handle the case $n = 6$ and prove an analogous result to that of Bremner and Morton. Our main result is the following.

Received by the editors February 2, 2021; revised January 25, 2022, accepted February 18, 2022.
Published online on Cambridge Core March 7, 2022.
AMS subject classification: **11G05**, 14H45, 11Y50.
Keywords: Elliptic curve, Mordell–Weil sieve, Fermat curve, sixth power.

Theorem 1 *The smallest positive integer which is a sum of two rational sixth powers but not a sum of two integer sixth powers is*

$$164\,634\,913 = \left(\frac{44}{5}\right)^6 + \left(\frac{117}{5}\right)^6.$$

To prove the main result, we must show that if an integer $k < 164\,634\,913$ is sixth-power free and is not a sum of two integer sixth powers, then it is not a sum of two rational sixth powers either. We proceed by studying when $C_k : x^6 + y^6 = kz^6$ has a solution in $\mathbb{Q}_p$ for all primes p, which reduces the number of necessary k to consider to 111 625. To handle these, we decompose the Jacobian of C_k (up to isogeny) as a product of 10 elliptic curves, each with j-invariant zero. If $k \notin \{1, 2\}$ is sixth-power free and one of these elliptic curves has rank zero, it follows that $C_k(\mathbb{Q})$ is empty (via Theorem 6). If we are able to determine a finite-index subgroup of the Mordell–Weil group of one of the elliptic curves, we use the Mordell–Weil sieve to prove that $C_k(\mathbb{Q})$ is empty.

We note that there are infinitely many integers that are sums of two rational sixth powers, but not sums of two integer sixth powers.

Theorem 2 *Let t be an integer and $f_1 = (2\,863 + 10\,764t)/13$ and $f_2 = (1\,207 + 26\,455t)/13$. Then $f_1^6 + f_2^6$ is an integer that is a sum of two rational sixth powers, but not a sum of two integer sixth powers.*

The polynomial $f_1^6 + f_2^6$ is constructed so that the coefficients of $t, t^2, \ldots, t^6$ are all multiples of 13, whereas the constant coefficient is equivalent to 5 (mod 13). Since it is impossible to have an integer equivalent to 5 (mod 13) be a sum of two integer sixth powers, we have our result.

Remark It seems likely that no positive integer can be written as a sum of two rational sixth powers in more than one way. In [9], Ekl searched for integer solutions to $a^6 + b^6 = c^6 + d^6$ with $a \neq c$ and $a \neq d$ and found none for which $a^6 + b^6 < 7.25 \times 10^{24}$. The surface $X : a^6 + b^6 = c^6 + d^6$ is a surface of general type, and the Bombieri–Lang conjecture predicts that there are only finitely many rational points on X that do not lie on a genus 0 or 1 curve.

2 Background

We let $\mathbb{Q}_p$ denote the field of p-adic numbers. We say a curve C is locally solvable if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p.

For our purposes, an elliptic curve is a smooth cubic curve of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

There is a natural abelian group structure on $E(\mathbb{Q})$, the set of rational points on E.

Theorem 3 [17, Theorem VIII.4.1] *The group $E(\mathbb{Q})$ is finitely generated. That is, there is a finite group $E(\mathbb{Q})_{tors}$ so that $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$ for some nonnegative integer r.*

https://doi.org/10.4153/S0008439522000157 Published online by Cambridge University Press

The nonnegative integer r is called the rank of $E(\mathbb{Q})$. The Birch and Swinnerton-Dyer conjecture predicts that if $L(E,s)$ is the L-function of E, the $\mathrm{ord}_{s=1}L(E,s) = r$. This is proved in the case that $r = 0$ or 1 by Gross and Zagier [13] and Kolyvagin [14].

For $k \neq 0$, the curve $C_k : x^6 + y^6 = kz^6$ is a curve of genus 10. For $k = 1$, the decomposition of the Jacobian is worked out in [1], and it follows that each factor of $J(C_1)$ is an elliptic curve with j-invariant zero. We will show in Section 5 that there are nonconstant morphisms from C_k to six different elliptic curves of the form $E_a : y^2 = x^3 + a$. The torsion subgroup of an elliptic curve of the form E_a has been known for some time.

Theorem 4 [11] *If $E_a : y^2 = x^3 + a$, then*

$$E_a(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/6\mathbb{Z} & \text{if } a \text{ is a sixth power,} \\ \mathbb{Z}/3\mathbb{Z} & \text{if } a \text{ is a square but not a sixth power or} \\ & \quad a \text{ is } -432 \text{ times a sixth power,} \\ \mathbb{Z}/2\mathbb{Z} & \text{if } a \text{ is a cube but not a sixth power,} \\ \mathbb{Z}/1\mathbb{Z} & \text{otherwise.} \end{cases}$$

There is a torsion point on $y^2 = x^3 + a$ for which x and y are both nonzero only when $a = -432k^6$ (namely $(12k^2 : \pm 36k^3 : 1)$) or $a = k^6$ (namely $(2k^2 : \pm 3k^3 : 1)$).

The Mordell–Weil sieve is a technique for proving that a curve C has no rational points. For a thorough treatment of this subject, see the paper of Bruin and Stoll [4].

Let J be the Jacobian of C, and assume that we have in hand a $\mathbb{Q}$-rational divisor D of degree 1 on C. Let $\iota : C \to J$ be the map $\iota(P) = P - D$. Fix a positive integer N and a finite set S of primes. We then have the following commutative diagram:

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\quad\iota\quad} & J(\mathbb{Q})/NJ(\mathbb{Q}) \\ \downarrow & & \downarrow{\scriptstyle\alpha} \\ \prod_{p\in S} C(\mathbb{F}_p) & \xrightarrow{\quad\beta\quad} & \prod_{p\in S} J(\mathbb{F}_p)/NJ(\mathbb{F}_p) \end{array}$$

If $C(\mathbb{Q})$ is nonempty, then there will be an element in $\prod_{p\in S} J(\mathbb{F}_p)/NJ(\mathbb{F}_p)$ that is in the image of both α and β. Therefore, if we can find an N and a finite set S for which the image of α and the image of β are disjoint, then $C(\mathbb{Q})$ is empty.

The curve C_k has maps to six different elliptic curves: E_k, E_{4k}, E_{-k^2}, E_{16k^2}, E_{k^3}, and E_{-4k^4}. As a consequence, we will replace J with one of these six curves in our applications. Computing the Mordell–Weil group (or a finite index subgroup thereof) for one of these six elliptic curves allows us to apply the Mordell–Weil sieve to C_k.

3 Finding an integer that is a sum of two rational sixth powers

We will describe briefly how the representation of $164\,634\,913 = (44/5)^6 + (117/5)^6$ was generated by the authors. We seek integers x, y, and m for which $x^6 + y^6 \equiv 0 \pmod{m^6}$ with $\gcd(x,m) = \gcd(y,m) = 1$. This equation implies that xy^{-1} must have order 4 or 12 in $(\mathbb{Z}/m^6\mathbb{Z})^\times$, which implies that all the prime factors of m must be $\equiv 1 \pmod 4$. The smallest such m is $m = 5$.

https://doi.org/10.4153/S0008439522000157 Published online by Cambridge University Press

We let $q = 1\,068$ be an element of order 4 in $(\mathbb{Z}/5^6\mathbb{Z})^\times$. Then $1^6 + q^6 \equiv 0 \pmod{5^6}$. We wish to find an integer a so that $\pm a \bmod 5^6$ and $\pm aq \bmod 5^6$ are both small. We consider the lattice $L \subseteq \mathbb{R}^2$ consisting of all vectors $\left\{\begin{bmatrix} x \\ y \end{bmatrix} : y \equiv qx \pmod{5^6}\right\}$. We find that an LLL-reduced basis for this lattice consists of $\begin{bmatrix} 117 \\ 44 \end{bmatrix}$ and $\begin{bmatrix} 44 \\ -117 \end{bmatrix}$ from which we obtain $164\,634\,913 = \left(\frac{44}{5}\right)^6 + \left(\frac{117}{5}\right)^6$.

We wish to note that this representation was found at least twice previouoeisly. First, it is given by Gandhi on page 1 001 of [12]. Second, it was noted by John W. Layman on October 20, 2005 in connection with Online Encyclopedia of Integer Sequences (OEIS) sequence A111152 (the smallest integers that are a sum of two rational nth powers, but not a sum of two integer nth powers).

For integers of the form $x^n + y^n$ with n odd, there are no local restrictions, and setting $x = \frac{2^{n-1}-1}{2}$ and $y = \frac{2^{n-1}+1}{2}$ leads to a fairly small integer that is a sum of two rational nth powers. For $n = 5$, this leads to $68\,101 = \left(\frac{15}{2}\right)^5 + \left(\frac{17}{2}\right)^5$. At present, it is not known if 68 101 is the smallest positive integer that is a sum of two rational fifth powers, but not a sum of two integer fifth powers.

4 Local solvability

In this section, we study the question of when $C_k : x^6 + y^6 = k$ is locally solvable.

Theorem 5 *Let k be a positive integer which is sixth-power free. Then C_k is locally solvable if and only if C_k has points over $\mathbb{Q}_p$ for all primes $p < 400$ and all odd prime factors $p \mid k$ have $p \equiv 1 \pmod 4$.*

Proof The curve C_k is smooth over $\mathbb{F}_p$ for all primes p other than 2, 3 and those dividing k. Since C_k has genus 10, Hasse's theorem gives that $|C_k(\mathbb{F}_p)| > p + 1 - 20\sqrt{p}$ provided $C_k/\mathbb{F}_p$ is smooth. The latter quantity is positive if $p > 400$. Furthermore, Hensel's lemma implies that if $C_k(\mathbb{F}_p)$ has a nonsingular point, then it lifts to a nonsingular point of $C_k(\mathbb{Q}_p)$ and hence $C_k(\mathbb{Q}_p) \neq \emptyset$.

If $p \mid k$ and $p \equiv 1 \pmod 4$, then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. Since $a^2 + b^2 \mid a^6 + b^6$, we have that $(a : b : 1)$ is a smooth point on $C_k/\mathbb{F}_p$ and therefore $C_k(\mathbb{Q}_p) \neq \emptyset$.

Suppose that $p \mid k$, $p \equiv 3 \pmod 4$ and $(x_0 : y_0 : z_0) \in C_k(\mathbb{Q}_p)$ with $x_0, y_0, z_0 \in \mathbb{Z}_p$, not all of which are multiples of p. It follows that p divides one of $x_0^2 + y_0^2$ or $x_0^4 - x_0^2 y_0^2 + y_0^4$, and both of these imply that $x_0 \equiv y_0 \equiv 0 \pmod p$. It follows that $x_0^6 + y_0^6 = kz_0^6$ is a multiple of p^6. Since k is sixth-power free, it follows that $p \mid z_0$, which is a contradiction. Thus, $C_k(\mathbb{Q}_p) = \emptyset$. ∎

We note that the smallest positive integer k that is not a sum of two integer sixth powers for which C_k is locally solvable is $k = 2\,017$.

To enumerate the $k < 164\,634\,913$ for which C_k is locally solvable, we note that if C_k is locally solvable, then $k \equiv 1, 2 \pmod 7$, $k \equiv 1, 2 \pmod 8$, and $k \equiv 1, 2 \pmod 9$. Moreover, for each $p \equiv 1 \pmod 6$ with $13 \leq p \leq 400$, we enumerate and cache the integers which are sums of two sixth powers modulo p. Now, we test integers less than

https://doi.org/10.4153/S0008439522000157 Published online by Cambridge University Press

or equal to 164 634 913 in each of the eight residue classes modulo $504 = 7 \times 8 \times 9$. We remove the values of k that are not sixth-power free, that are divisible by a prime $\equiv 3 \pmod 4$, that are sums of two integer sixth powers, and that reduce modulo some $p \equiv 1 \pmod 6$ to an element of $\mathbb{F}_p$ that is not a sum of two sixth powers. The result is a list of 111 625 values of $k < 164\,634\,913$ which are not sums of two integer sixth powers and for which C_k is locally solvable. The computation runs in 46.29 seconds, and the code can be found in the script `step1-localtest.txt`.

5 Maps from C_k to elliptic curves

The curve $C_k : x^6 + y^6 = kz^6$ has at least 72 automorphisms defined over $\mathbb{Q}(\zeta_6)$, generated by the maps $\mu_1(x : y : z) = (\zeta_6 x : y : z)$, $\mu_2(x : y : z) = (x : \zeta_6 y : z)$, and $\mu_3(x : y : z) = (y : x : z)$. Magma can work out the action of each of these maps on the 10-dimensional space of holomorphic 1-forms on C_k. We find eight subgroups H of $\mathrm{Aut}(C_k)$ for which the quotient curve C_k/H has genus 1 and the corresponding one-dimensional subspaces of holomorphic 1-forms are distinct. From these, it is not difficult to compute the corresponding map to an elliptic curve.

For example, one such subgroup is $\langle \mu_1^5\mu_2, \mu_2^3\mu_3 \rangle$. The monomials x^3y^3, xyz^4, and $x^6 - y^6$ are all fixed by $\mu_1^5\mu_2$, and each is sent to their negative by $\mu_2^3\mu_3$. If $\phi : C_k \to \mathbb{P}^2$ is given by $\phi((x : y : z)) = (x^3y^3 : xyz^4 : x^6 - y^6)$, then we have $\phi(P) = \phi(\alpha(P))$ for all points P on C_k and all $\alpha \in \langle \mu_1^5\mu_2, \mu_2^3\mu_3 \rangle$. Letting $a = x^3y^3$, $b = xyz^4$, and $c = x^6 - y^6$, the image of ϕ is the curve

$$a^3 - \frac{k^2}{4}b^3 + \frac{1}{4}ac^2 = 0.$$

This curve has genus 1, and thus is the quotient curve $C_k/\langle \mu_1^5\mu_2, \mu_2^3\mu_3 \rangle$. This curve has the point $(0 : 0 : 1)$ on it, and a change of variables turns this into the elliptic curve E_{-4k^4}. Composing these maps gives the map $\phi : C_k \to E_{-4k^4}$ given by $\phi(x : y : z) = (k^2xyz^4 : -k^2x^6 + k^2y^6 : x^3y^3)$.

The table below lists all 10 independent maps from C_k to elliptic curves.

Subgroup of $\mathrm{Aut}(C_k)$	Codomain	Map
$\langle \mu_1^2\mu_2^3 \rangle$	E_k	$(x, y) \mapsto (-y^2, x^3)$
$\langle \mu_1^3\mu_2^2 \rangle$	E_k	$(x, y) \mapsto (-x^2, y^3)$
$\langle \mu_1\mu_2^2 \rangle$	E_{4k}	$(x, y) \mapsto \left(\frac{x^4}{y^2}, \frac{x^6+2y^6}{y^3}\right)$
$\langle \mu_1^2\mu_2 \rangle$	E_{4k}	$(x, y) \mapsto \left(\frac{y^4}{x^2}, \frac{2x^6+y^6}{x^3}\right)$
$\langle \mu_1\mu_2^3 \rangle$	E_{-k^2}	$(x, y) \mapsto \left(\frac{k}{y^2}, \frac{kx^3}{y^3}\right)$
$\langle \mu_1^3\mu_2 \rangle$	E_{-k^2}	$(x, y) \mapsto \left(\frac{k}{x^2}, \frac{ky^3}{x^3}\right)$
$\langle \mu_1\mu_2^5, \mu_1^2\mu_2 \rangle$	E_{16k^2}	$(x, y) \mapsto \left(-4x^2y^2, -8x^6 + 4k\right)$
$\langle \mu_1\mu_2^4 \rangle$	E_{k^3}	$(x, y) \mapsto \left(\frac{kx^2}{y^2}, \frac{k^2}{y^3}\right)$
$\langle \mu_1^4\mu_2 \rangle$	E_{k^3}	$(x, y) \mapsto \left(\frac{ky^2}{x^2}, \frac{k^2}{x^3}\right)$
$\langle \mu_1^5\mu_2, \mu_2^3\mu_3 \rangle$	E_{-4k^4}	$(x, y) \mapsto \left(\frac{k^2}{x^2y^2}, \frac{-k^2x^6+k^2y^6}{x^3y^3}\right)$

https://doi.org/10.4153/S0008439522000157 Published online by Cambridge University Press

We wish to note that for the maps from $C_k \to E_{4k}$, the quotient curve by the subgroup indicated (either $\langle \mu_1 \mu_2^2 \rangle$ or $\langle \mu_1^2 \mu_2 \rangle$) is the genus two hyperelliptic curve given by $D_k : y^2 = \frac{1}{k}x^6 + \frac{1}{4k^2}$. This equation may be rewritten as

$$\left(\frac{2ky}{x^3}\right)^2 = \left(\frac{1}{x^2}\right)^3 + 4k.$$

As a consequence, we have the map $\phi(x, y) = \left(\frac{1}{x^2}, \frac{2ky}{x^3}\right)$ from $D_k \to E_{4k}$. (The authors did not find a subgroup of $\mathrm{Aut}(C_k)$ that fixed a one-dimensional space of differentials corresponding to these maps.)

Theorem 6 *Suppose that k is a sixth-power-free integer and $P = (x, y)$ is a rational point on C_k, and the image of P under one of the 10 maps given above is a torsion point. Then $k = 1$ or $k = 2$.*

Proof Apart from the cases of E_{a^6} and E_{-432a^6}, every torsion point on E_a has the x or y coordinate zero. Inspecting the 10 maps above, we find that if $P \in C_k(\mathbb{Q})$ and its image on E_a has the x or y coordinate zero, then $x = 0$ or $y = 0$ or (for the 7th or 10th maps) that $x^6 = y^6 = k/2$. This implies that $k/2$ is a sixth power, but since k is sixth-power free, $k = 2$.

Now, we consider the case that $E_a = E_{\alpha^6}$ or $E_a = E_{-432\alpha^6}$ for $a \in \{k, 4k, -k^2, 16k^2, k^3, -4k^4\}$. If α is a rational number and $k = \alpha^6$ is a sixth power, this forces $k = 1$. If $4k = \alpha^6$ and k is sixth-power free, then $k = 16$, but $x^6 + y^6 = 16$ has no points in $\mathbb{Q}_2$. The cases $-k^2 = -432\alpha^6$ and $-4k^4 = -432\alpha^6$ never occur. If $16k^2 = \alpha^6$, then $k = 2$. Finally, if $k^3 = \alpha^6$, then k is a perfect square. In this case, E_{k^3} has the torsion points $(2\alpha^2, \pm 3\alpha^3)$. However, we have that $2\alpha^2 = \frac{\alpha^2 x^2}{y^2}$ or $\frac{\alpha^2 y^2}{x^2}$, which implies that $2 = \frac{x^2}{y^2}$ or $\frac{y^2}{x^2}$, contradicting the irrationality of $\sqrt{2}$. ∎

As a consequence of the above result, if $k \notin \{1, 2\}$ is sixth-power free and the rank of one of the six elliptic curves E_k, E_{4k}, E_{-k^2}, E_{16k^2}, E_{k^3}, or E_{-4k^4} is zero, then k is not a sum of two rational sixth powers. For each of the 111 625 values of k found in the previous section, we need to determine the Mordell–Weil group (or a finite index subgroup thereof) of one of these six curves. The most straightforward approach to this problem is to conduct a 2-descent. However, a 2-descent on E_k requires computing the class group of $\mathbb{Q}(\sqrt[3]{-k})$, and this is time-consuming to do unconditionally if k is large. We proceed to apply a number of other techniques specific to our situation and resort to an unconditional 2-descent only when absolutely necessary.

6 Checking if $L(E_{k^3}, 1) = 0$

The elliptic curve $E_{k^3} : y^2 = x^3 + k^3$ is a quadratic twist of $E_1 : y^2 = x^3 + 1$. If $k \equiv 1 \pmod 8$, the sign of the functional equation for E_{k^3} is 1, whereas if $k \equiv 2 \pmod 8$, the sign of the functional equation is -1. We are able to rule out most odd values of k by showing that $L(E_{k^3}, 1) \neq 0$.

https://doi.org/10.4153/S0008439522000157 Published online by Cambridge University Press

Waldspurger's theorem [18] says, very roughly speaking, that

$$\sum_k k^{1/4}\sqrt{L(E_{k^3},1)}q^k$$

is a weight $3/2$ modular form of a particular level. In Theorem 11 of [16], Purkait works out the predictions of Waldspurger's theorem, showing that there is a modular form $f = \sum b(k)q^k$ of level 576 and trivial character whose Fourier coefficients encode the L-values of $L(E_{k^3},1)$ under the assumption that $3 \nmid k$. In Example 2 of [16], Purkait gives a complicated formula for this modular form f in terms of ternary theta series. We are able to find a formula more amenable to computation using the theta series for the six ternary quadratic forms:

$$\begin{aligned}
Q_1 &= x^2 + 4y^2 + 144z^2,\\
Q_2 &= 4x^2 - 4xy + 5y^2 + 36z^2,\\
Q_3 &= 4x^2 + 9y^2 + 16z^2,\\
Q_4 &= x^2 + 16y^2 + 36z^2,\\
Q_5 &= 4x^2 + 13y^2 + 10yz + 13z^2, \text{ and}\\
Q_6 &= 4x^2 + 4y^2 + 4yz + 37z^2.
\end{aligned}$$

These six quadratic forms constitute a single genus. Let

$$h = \frac{5}{16}\theta_{Q_1} - \frac{3}{16}\theta_{Q_2} - \frac{7}{16}\theta_{Q_3} + \frac{5}{16}\theta_{Q_4} + \frac{9}{16}\theta_{Q_5} - \frac{3}{16}\theta_{Q_6} = \sum c(n)q^n.$$

Then, for $k \equiv 1 \pmod{24}$, we have $c(k) = b(k)$, and if $k \equiv 17 \pmod{24}$, we have $c(k) = 6b(k)$. It follows that if $k \equiv 1 \pmod 8$ is a fundamental discriminant and $c(k) \neq 0$, then $L(E_{k^3},1) \neq 0$. Hence, E_{k^3} has rank zero, and if $k > 1$, this implies that k is not the sum of two rational sixth powers. (If k is not square-free, we can simply replace k with k/m^2 in the above calculation.)

Each theta series above can be computed by multiplying a binary theta series by a unary theta series. In this way, it is possible to compute the first 165 million coefficients of h and among these determine the odd values of k for which $L(E_{k^3},1) \neq 0$. Of the 111 625 values of k for which C_k is locally solvable, 55 284 are odd, whereas 56 341 are even. The computation just described rules out all but 2 753 odd values of k. The computation takes 559.20 seconds, and the code run can be found in the script `step2-wald.txt`.

7 Computing Mordell–Weil groups

Here and elsewhere, we rely on the procedure for explicit n-descent developed by Cremona et al. in [6–8] and implemented in Magma with much of the code written by Michael Stoll, Tom Fisher, and Steve Donnelly.

First, we use that each elliptic curve E_a has a cyclic 3-isogeny. We take the remaining 59 094 values of k and compute the 3-isogeny Selmer groups to bound the rank for the elliptic curves in the set $\{E_k, E_{4k}, E_{-k^2}, E_{16k^2}, E_{-4k^4}\}$. We hope to rule out k's for which one of these curves has rank zero and so we only test elliptic curves

https://doi.org/10.4153/S0008439522000157 Published online by Cambridge University Press

with root number equal to 1. This test is run in `step3-3isog.txt` and takes a bit under 6 hours (namely 20 551.4 seconds). This step rules out 39 586 values of k, and 19 508 values remain.

Second, for each of the 19 508 remaining k's, we perform a full 3-descent by doing a first and second 3-isogeny descent (via the Magma command `ThreeDescentByIsogeny`) on E_k, E_{4k}, and E_{k^3}. For these curves, this command requires class group computations of low-discriminant quadratic and cubic fields. We search for points on the resulting 3-covers in the hope that we can provably compute the rank of E_k, E_{4k}, or E_{k^3}. This test is run in `step4-findMW.txt`. Once the 3-covers are found, we sort the curves in increasing order of the upper bound on the rank and search for points on the associated 3-covers with a height bound of 10 000. If we are not successful, we double the height bound and search again. If we are not successful at a height bound of 320 000, we give up. This is the most time-consuming step of the process, taking about 26 hours. This step finds 864 additional values of k for which one of E_k, E_{4k}, or E_{k^3} has rank zero. In the end, we succeed in computing the Mordell–Weil groups of one of E_k, E_{4k}, or E_{k^3} for all but 196 values of k. There are also 34 cases where the elliptic curve in question has rank 5, and one case (k = 123 975 217) for which the rank of E_k is 6. For these k's, we seek to find the Mordell–Weil group of a different elliptic curve.

Third, for each of the 196 + 35 = 231 remaining k's, we obtain as much unconditional information as possible about the ranks of the six elliptic curves using descent by 3-isogeny, as well as a 2-descent on E_{k^3} (combined with the Cassels–Tate pairing to identify 2-covers as corresponding to a nontrivial element of the Shafarevich–Tate group of E_{k^3}). Once these unconditional upper bounds on ranks have been obtained, we search for points on these curves by assuming GRH and performing 2-descents and 4-descents on all six curves and searching for points on the 2-covers and 4-covers to see if enough independent points are found to match the unconditional rank upper bound. This takes about 22 minutes (1 292.52 seconds). The code that runs these computations is available in the scripts `step5-24descent.txt` and `step5-highrank.txt`. Of the 196k's for which generators were not found, this step is unsuccessful for 26, and of the 35k's for which one of E_k, E_{4k}, or E_{k^3} has rank 5 or 6, this is unsuccessful for four values of k.

Fourth, for each of the 30 remaining values of k, we use the method of Fisher [10] to search for points using 12-descent. For each of the remaining k's, there is at least one elliptic curve E_a for which we have an unconditional upper bound on the rank of 1, and for which the root number is −1. For each such k, we choose a minimal subject to these conditions and perform a conditional 12-descent and search for points. We succeed in finding a generator in 23 cases. We fail to find a generator for the following seven values of k: 49 897 450; 117 092 530; 120 813 050; 128 327 978; 130 187 450; 149 477 050; and 160 631 290. (For k = 128 327 978, E_{k^3} has rank 5 with easily found generators.) This is performed with the script `step6-12desc.txt`, and the running time is just over 3 hours (11 180.99 seconds).

So far, we have avoided doing an unconditional 2-descent on any elliptic curve other than E_{k^3} because of the cost of computing the class group of a (potentially high discriminant) cubic field. We now do this for the remaining seven values of k. For each k, we choose the elliptic curve for which the corresponding Minkowski

https://doi.org/10.4153/S0008439522000157 Published online by Cambridge University Press

bound is the smallest. For $k = 49\,897\,450$ and $k = 149\,477\,050$, this shows that E_k has rank zero. For $k = 120\,813\,050$ and $k = 130\,187\,450$ this shows that E_{4k} has rank zero. For $k = 128\,327\,978$, the computation shows that E_{16k^2} has rank zero (using both a 2-descent and the Cassels–Tate pairing). For $k = 117\,092\,530$ and $k = 160\,631\,290$, a 2-descent shows that E_k has rank 1 (whereas previously our unconditional bound on the rank had been 3). This is performed with the script `step7-2descents.txt`, and the running time is just under 2 hours (7 153.69 seconds). For $k = 117\,092\,530$, the Minkowski bound for $\mathbb{Q}(\sqrt[3]{-k})$ is 57 383 551, and the time needed for the proof phase of the class group computation is 3 327.08 seconds.

Of the 19 508 values of k that remained after Step 3 864 were removed in Step 4 and 5 more were removed in Step 7. For each of the remaining 18 639 values of k, we know a finite-index subgroup of the Mordell–Weil group of one of the six corresponding elliptic curves, and moreover that curve has rank less than or equal to 4. In fact, of the 18 639 values of k, the chosen elliptic curve has rank 1 in 16 032 cases, rank 2 in 1 172 cases, rank 3 in 1 371 cases, and rank 4 in only 64 cases.

8 Using the Mordell–Weil sieve

As indicated in Section 2, the goal of the Mordell–Weil sieve is to choose an integer N and a finite set S of primes p of good reduction for E and consider the diagram:

$$\begin{array}{ccc} C_k(\mathbb{Q}) & \xrightarrow{\quad\iota\quad} & E(\mathbb{Q})/NE(\mathbb{Q}) \\ \downarrow & & \downarrow \alpha \\ \prod_{p\in S} C_k(\mathbb{F}_p) & \xrightarrow{\quad\beta\quad} & \prod_{p\in S} E(\mathbb{F}_p)/NE(\mathbb{F}_p) \end{array}$$

If one finds that $\operatorname{im}\alpha \cap \operatorname{im}\beta = \emptyset$, then $C_k(\mathbb{Q})$ must be empty. Here, E can be any of the six elliptic curves E_k, E_{4k}, E_{-k^2}, E_{16k^2}, E_{k^3}, or E_{-4k^4}. In practice, we are not always able to provably find $E(\mathbb{Q})$. Instead, we have used the `Saturation` command in Magma to compute a finite index subgroup $A \subseteq E(\mathbb{Q})$ with the property that $[E(\mathbb{Q}) : A]$ is not divisible by any primes $p \le 100$. It follows that if there is no prime $\ell > 100$ for which $\ell \mid N$, then $A/NA \cong E(\mathbb{Q})/NE(\mathbb{Q})$, and we may use A in place of $E(\mathbb{Q})$ in the diagram above. In practice, the largest N we need to use is $N = 84$.

Before discussing the method and the results, we begin with a simple example. Let $k = 138\,826$. We have $E_{4k}(\mathbb{Q}) \cong \mathbb{Z}$, and a generator is

$$P = \left(\frac{605\,879\,737}{2\,358^2}, \frac{-17\,828\,809\,046\,227}{2\,358^3}\right).$$

We use the map $\phi : C_k \to E_{4k}$ given by $\phi(x, y) = \left(\frac{x^4}{y^2}, \frac{x^6+2y^6}{y^3}\right)$. We find that $C_k(\mathbb{F}_5)$ contains six points, $E_{4k}(\mathbb{F}_5) \cong \mathbb{Z}/6\mathbb{Z}$, but that the image of $C_k(\mathbb{F}_5) \to E_{4k}(\mathbb{F}_5)$ consists of three points. The reduction $\tilde{P} \in E_{4k}(\mathbb{F}_5)$ has order 6, and if n is an integer, then nP reduces to a point in $E_{4k}(\mathbb{F}_5)$ that is in the image of $C_k(\mathbb{F}_5) \to E_{4k}(\mathbb{F}_5)$ if and only if n is even. It follows that if $Q \in C_k(\mathbb{Q})$, then $\phi(Q) = nP$ for some even n.

https://doi.org/10.4153/S0008439522000157 Published online by Cambridge University Press

Now, we consider reduction modulo 7. In this case, $C_k(\mathbb{F}_7)$ has 36 points and the image of $C_k(\mathbb{F}_7) \to E_{4k}(\mathbb{F}_7)$ consists of 6 points. We have $E_{4k}(\mathbb{F}_7) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, and the reduction $\tilde{P} \in E_{4k}(\mathbb{F}_7)$ again has order 6. This time, we find that nP reduces to a point in $E_{4k}(\mathbb{F}_7)$ that is in the image of $C_k(\mathbb{F}_7) \to E_{4k}(\mathbb{F}_7)$ if and only if $n \equiv 1$ or $5 \pmod 6$. It follows that if $Q \in C_k(\mathbb{Q})$, then $\phi(Q) = nP$ for some odd n, and this contradicts the previous paragraph. Thus, $C_k(\mathbb{Q}) = \emptyset$.

As explained in Section 3.2 of [4], the sets A/NA can be very large if N is large or if the rank of E is high. For this reason, we follow their suggestion of successively raising N one prime factor at a time. Suppose that we have already computed the admissible elements of A/NA (i.e., those that could possibly occur as the image of a point from $C_k(\mathbb{Q})$) by sieving using a collection of small primes S. We then choose a small prime r and set $N' = rN$. Then we find the full preimage of the admissible elements in $A/N'A$, retest their admissibility for primes in S, and possibly test a further set of primes. Unlike the case of [4], the maximum N needed to prove that $C_k(\mathbb{Q})$ is empty is never more than 84 (whereas Bruin and Stoll report occasionally needing to have N as large as 10^{100}).

As an example, consider the case of $k = 3\,506\,050$. The elliptic curve E_k has rank 4 and trivial torsion subgroup. First, we let $N = 2$ and test the primes p of good reduction less than or equal to 311. We find that of the 16 elements of $A/2A$, 9 are admissible. We then increase N to 4 and begin with $9 \times 16 = 144$ elements of $A/4A$. We retest their admissibility for primes less than or equal to 311 and find that all of them are admissible. We then increase N from 4 to 12 and test primes $p \le 479$. Initially, we had 11 664 elements of $A/12A$, but this is reduced to 1 296. Next, we increase N from 12 to 84 and start with 3 111 696 elements of $A/84A$. Testing for $p \le 229$ reduces this to 1 204 elements, and by the time we test $p = 1021$, no admissible elements remain. Hence, $C_{3\,506\,050}(\mathbb{Q}) = \emptyset$. The total time required for this k was 508 seconds, and this is the most time-consuming of all the k's we test.

Compared with the previous steps, the Mordell–Weil sieve step is comparatively fast, taking about 35 minutes (2 107.69 seconds) to show that $C_k(\mathbb{Q}) = \emptyset$ for all 18 639 remaining k's with $k < 164\,634\,913$. This computation is performed by the script `step8-MWsieve.txt`. This concludes the proof of Theorem 1. Below is a table summarizing the steps in the computation and the time required for each.

Step	Task	Run time (seconds)	k's eliminated
1	Local solvability	46.29	164 523 287
2	$L(E_{k^3}, 1) \neq 0$	559.20	52 531
3	3-isogeny descent	20 551.40	39 586
4	Full 3-descent	119 076	864
5	Conditional descent	1 292.52	0
6	12-descent	11 180.99	0
7	Unconditional 2-descent	7 153.69	5
8	Mordell–Weil sieve	2 107.69	18 639
Total		161 968	164 634 912

https://doi.org/10.4153/S0008439522000157 Published online by Cambridge University Press

9 Concluding remarks

As mentioned in the introduction, it is natural to consider the problem of finding the smallest positive integer which is a sum of two rational nth powers but not a sum of two integer nth powers. If $n = 5$, the curve $D_k : x^5 + y^5 = k$ admits no map to an elliptic curve, and the projective closure of D_k always has a rational point (namely $(-1 : 1 : 0)$). This precludes the possibility of ruling out rational points on D_k using local methods or the Mordell–Weil sieve. For these reasons, the $n = 5$ case appears to be more challenging than the $n = 4$ or $n = 6$ cases.

Similar techniques should allow one to approach the cases of $n = 8$ and $n = 12$ where there are maps from $x^n + y^n = k$ to elliptic curves, but the smallest known values of k for which these curves are known to have rational noninteger points are 8 000 587 738 704 025 541 501 346 146 and 873 135 263 681 497 645 296 811 652 793 869 145 886 016 236 198 018 083 488 332 176 234 017, respectively. The size of these numbers would make an exhaustive search prohibitively time-consuming.

Acknowledgment This work represents joint work done when the first author was a master's student at Wake Forest University. Computations were done in Magma [2] version 2.26-9 on a desktop with an Intel i9-11900K CPU and 128 GB of RAM. The authors thank the referees for the detailed suggestions including the decomposition of the Jacobian of $x^6 + y^6 = kz^6$ and computational suggestions that led to an unconditional main result.

References

[1] N. Aoki, *Simple factors of the Jacobian of a Fermat curve and the Picard number of a product of Fermat curves*. Amer. J. Math. **113**(1991), no. 5, 779–833.
[2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*. J. Symbolic Comput. **24**(1997), 235–265. Computational algebra and number theory (London, 1993).
[3] A. Bremner and P. Morton, *A new characterization of the integer* 5906. Manuscripta Math. **44**(1983), nos. 1–3, 187–229.
[4] N. Bruin and M. Stoll, *The Mordell–Weil sieve: proving non-existence of rational points on curves*. LMS J. Comput. Math. **13**(2010), 272–306.
[5] H. Cohen, *Number theory. Volume I. Tools and Diophantine equations*, Graduate Texts in Mathematics, 239, Springer, New York, 2007.
[6] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves. I. Algebra*. J. Reine Angew. Math. **615**(2008), 121–155.
[7] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves. II. Geometry*. J. Reine Angew. Math. **632**(2009), 63–84.
[8] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves. III. Algorithms*. Math. Comp. **84**(2015), no. 292, 895–922.
[9] R. L. Ekl, *Equal sums of four seventh powers*. Math. Comp. **65**(1996), no. 216, 1755–1756.
[10] T. Fisher, *Finding rational points on elliptic curves using 6-descent and 12-descent*. J. Algebra **320**(2008), no. 2, 853–884.
[11] R. Fueter, *Ueber kubische diophantische Gleichungen*. Comment. Math. Helv. **2**(1930), no. 1, 69–89.
[12] J. M. Gandhi, *On Fermat's last theorem*. Amer. Math. Monthly **71**(1964), 998–1006.
[13] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*. Invent. Math. **84**(1986), no. 2, 225–320.
[14] V. A. Kolyvagin, *Finiteness of $E(Q)$ and $Ш(E, Q)$ for a subclass of Weil curves*. Izv. Akad. Nauk SSSR Ser. Mat. **52**(1988), no. 3, 522–540, 670–671.

https://doi.org/10.4153/S0008439522000157 Published online by Cambridge University Press

[15] Y. Lamzouri, X. Li, and K. Soundararajan, *Conditional bounds for the least quadratic non-residue and related problems*. Math. Comp. **84**(2015), no. 295, 2391–2412.
[16] S. Purkait, *Explicit application of Waldspurger's theorem*. LMS J. Comput. Math. **16**(2013), 216–245.
[17] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, 106, Springer, New York, 1992. Corrected reprint of the 1986 original.
[18] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*. J. Math. Pures Appl. (9) **60**(1981), no. 4, 375–484.

Department of Mathematics, Emory University, Atlanta, GA 30307, USA

Department of Mathematics and Statistics, Wake Forest University, Winston-Salem, NC 27106, USA
e-mail: rouseja@wfu.edu

https://doi.org/10.4153/S0008439522000157 Published online by Cambridge University Press