ON POWERFUL INTEGERS EXPRESSIBLE AS SUMS OF TWO COPRIME FOURTH POWERS

NOAM D. ELKIES AND GAURAV GOEL

Abstract. We confirm the conjecture made in [5] that the smallest powerful integer expressible as a sum of two coprime fourth powers is

$$308825748949336027872519696547735921 7 = 17^3 \cdot 73993169^2 \cdot 338837713^2 = 427511122^4 + 1322049209^4,$$

and that in fact this is the only solution up to $3.6125 \cdot 10^{37}$. We also conjecture that

$$106185359534837079852858458570799339559762493431196127017785 7 = 17^3 \cdot 38401618921^2 \cdot 382833034044850177^2 = 5721324183698984^4 + 9884786794723734^4$$

is the second-smallest solution. Finally, we suggest one approach that might allow our result to be extended past $3.6125 \cdot 10^{37}$.

1. Introduction and motivation

An integer N is said to be "powerful" if every prime factor $p \mid N$ satisfies $p^2 \mid N$ (so N is a multiple of some power of p higher than p^1). More generally, N is "k-powerful" for some $k \geq 2$ if $p^k \mid N$ for every prime factor $p \mid N$.

Several classical Diophantine equations have been reconsidered with one or more squares (or k-th powers) replaced by powerful (or k-powerful) numbers. Since the k-powerful numbers contain the k-th powers as a subset of positive density,[1] one might expect that replacing a k-th power by a k-powerful number would make the solutions more numerous but only by a constant factor; but new behavior can arise. For example, while there are clearly no consecutive squares other than $0, 1$, one can use Fermat–Pell equations to get infinite sequences of powerful numbers $x^2 \pm 1$, such as $3^2 - 1, 17^2 - 1, \ldots$ (from powers of $(1 + \sqrt{2})^2$) and $682^2 + 1 = 5^3 61^2, 930249^2 - 1 = 5^3 83204^2, \ldots$ (from powers of $(2 + \sqrt{5})^5$). In each such sequence the number of terms up to x is asymptotically proportional to $\log x$, as one expects from the density of powerful numbers. Likewise, while there are no nonzero integer solutions of $x^3 + y^3 = z^3$, one can get infinite families of powerful $N = x^3 + y^3$ with x, y coprime (as we must assume, here and later, to avoid trivial constructions such as $(x, y, N) = (m(m^3 + n^3), n(m^3 + n^3), (m^3 + n^3)^4)$. For example, the elliptic curve $x^3 + y^3 = 9z^3$ yields infinitely many examples starting with $919^3 + (-271)^3 = 2^3 3^5 73^3$. In general an elliptic curve of rank r yields a sequence with $\sim c \log^{r/2} x$

Date: December 2021.

Simons AGNTC Collaboration grant #550031; Harvard College Research Program (HCRP) Summer 2020.

[1] For each k there exists α_k with $1 < \alpha_k < \infty$ such that the number of k-powerful $N \in [1, x]$ is asymptotic to $\alpha_k x^{1/k}$ as $x \to \infty$. For example, $\alpha_2 = \zeta(3/2)/\zeta(3) = 2.173+$. See [8, pp.407ff.].

terms up to x. The curve $x^3+y^3=9z^3$ has rank 1, but there is at least one known curve $x^3+y^3=Az^3$ of rank 11 (see [6]), giving $\sim c\log^{11/2}x$; this exceeds the probabilistic estimate, which again grows only as a multiple of $\log x$.[2]

In the present paper we study the similar equation $x^4+y^4=N$ with x,y coprime and N powerful. There are no nontrivial solutions with $N=z^2$, but again we can find infinite families of solutions by replacing the rank-zero elliptic curve $x^4+y^4=z^2$ by suitable twists, which here are curves $C_b: x^4+y^4=bz^2$. The first twist that works is C_{17}, which is an elliptic curve of rank 2; and the highest rank known is 6,[3] for $b=695946499681=17\cdot 16481\cdot 2483953$, so the number of solutions up to x grows at least as a multiple of $\log^3 x$.

For this equation, though, already the first C_b that works requires $N=bz^2$ to be quite large when we impose the condition $b\mid z$ that makes N powerful: even with a rank-2 group of rational points, the smallest N coming from C_{17} is

$$N_1 := 427511122^4+1322049209^4 = 17^3\,73993169^2\,338837713^2 > 3\cdot 10^{36}. \tag{1}$$

Further C_b produced more solutions, but all were larger than N_1 and even larger than the second example

$$N_2 := 572132418369898^4+988478679472373^4 > 1.06\cdot 10^{60} \tag{2}$$

coming from C_{17}. This led the first-named author to guess that N_1 may be the smallest solution. But this seemed quite hard to check: searching either over pairs (x,y) or over powerful $N<N_1$ would take computational work on the order of $N_1^{1/2}$, quite exorbitant when $N_1>3\cdot 10^{36}$. Searching over $b<N_1^{1/3}$ may seem more promising, but processing that many elliptic curves is still daunting. A MathOverflow question [5] generated interest and discussion but no solution or improved strategy.

Not long after posting, the first-named author noticed that this problem has some special features that made it possible to build on previous theoretical and computational work to reduce the number of candidate b's to a tiny fraction of $N_1^{1/3}$. In particular, $2b$ would have to be one of the rare even "congruent numbers" that are congruent to 2 mod 8. Such numbers had already been computed up to 10^{12} [7], so we could use the resulting list to exclude $b<5\cdot 10^{11}$. This might not seem large enough because $(5\cdot 10^{11})^3<N_1$, leaving us short by a factor of almost 25. Fortunately it is a classical result[4] that $x^4+y^4=b^3$ has no solution in positive integers with $\gcd(x,y)=1$. It soon follows that if $N=x^4+y^4$ is powerful then $N\ge 17^2b^3$, and now a list of candidate $b<5\cdot 10^{11}$ would suffice to reach N_1 and even further, to $17^2(5\cdot 10^{11})^3=3.6125\cdot 10^{37}$.

The list of candidate b would still be substantial, and it was not clear how efficiently each one might be processed. Some years later, he suggested this problem

[2] A Fermat–Pell equation leads to the unit group in $\mathbb{Z}[\sqrt{D}]$, which has rank 1; but in that setting the logarithmic height grows linearly, not quadratically, so rank 1 suffices to get $c\log x$. The special case $x^2-1=y^2$ leads to the ring "$\mathbb{Z}[\sqrt{1}]$" $\cong\{(m,n)\in\mathbb{Z}^2 : m\equiv n \bmod 2\}$, which has zero divisors and a finite unit group $(m,n)=(\pm1,\pm1)$.

[3] While there are known curves C_b whose Jacobians E_b (see (4) below) have rank 7, none of them has a rational point. Indeed it was not easy even to find one of the known rank-6 curves E_b (see [13]) for which C_b has a rational point. For $b=695946499681$, such a point is $(x,y,z)=(1470038250,2196674399,6337763194489)$.

[4] Attributed to Lucas in [4, p.83]. They refer to page 630 of Dickson's *History of the Theory of Numbers*, which in turn cites papers published in 1873 and 1877. These papers are not easy to locate, so we later give a self-contained proof.

to the second-named author for an undergraduate research project. After some work and further refinements, the second-named author found and implemented a strategy that was efficient enough to complete search up to $3.6125 \cdot 10^{37}$ in a few days on a laptop CPU. Since no new examples turned up, this proved that indeed N_1 is the smallest powerful sum of two coprime positive fourth powers, and the unique one up to $3.6125 \cdot 10^{37}$.

The rest of this paper is organized as follows. In the next section we show that b must satisfy several conditions that, taken together, leave only 66551915 possible candidates with $b < 5 \cdot 10^{11}$. In the following two sections, we treat 67 "small" candidate b's (all but 5 of those with $b < 10^4$) using the arithmetic of elliptic curves, and then the remaining "large" b's using unique factorization in $\mathbb{Z}[i]$ and the arithmetic of conic curves. Finally we suggest how our techniques might be extended to go beyond $3.6125 \cdot 10^{37}$.

2. The 66551915 candidate b's

We seek solutions to the Diophantine equation $N = x^4 + y^4$ where $1 \le x < y$ with $(x, y) = 1$ and N powerful. Every powerful number $N > 0$ can be written as $N = a^2b^3$ for integers $a, b > 0$, and this representation is unique if we require b to be squarefree. Given such b, we consider the genus-1 curve

$$C_b : x^4 + y^4 = bz^2, \tag{3}$$

and then find all positive integer solutions of (3) satisfying $b \mid z$ with z up to some bound. By a classical theorem of Fermat, $b > 1$. If N is sum of two coprime fourth powers, then every odd prime factor $p \mid N$ is congruent to 1 mod 8, because $x/y \bmod p$ has order 8 in the group $(\mathbb{Z}/p\mathbb{Z})^*$. Moreover, if N is even then $N \equiv 2 \bmod 16$, so in particular N cannot be powerful. Therefore we need only consider values of b that are products of distinct primes, each congruent to 1 mod 8.

In fact, we have a further restriction on b, which dramatically reduces the computational resources required. If the curve C_b has a rational point then it is isomorphic over $\mathbb{Q}$ with its Jacobian, which we can identify with

$$E_b : Y^2 = X^3 - 4b^2X \tag{4}$$

using classical invariant theory.[5] It is well-known that the rational torsion group of such a curve E_b is exactly $E_b[2] = \{\infty, (0,0), (2b,0), (-2b,0)\}$ (see [10, X.6.1(a)]). Hence if E_b is to have a finite rational point with $y \neq 0$ then E_b must have positive rank.

Now the curve E_b has positive rank iff $2b$ is a congruent number. For b odd, the L-function of E_b has sign ± 1 according as $b \equiv 1 \bmod 4$. Fortunately for us, all our b are $+1 \bmod 4$, so all our E_b should have even rank, and the vast majority should have rank zero: it is expected that among all $b < M$ with $b \equiv +1 \bmod 4$, only $M^{3/4 \pm o(1)}$ have E_b of positive rank as $M \to \infty$. We are also fortunate that the

[5] See for instance [3, p. 89]. We could tell *a priori* that E_b must have $j = 1728$, because C_b has an automorphism $(x : y : z) \mapsto (x : iy : z)$ that multiplies a holomorphic differential ω by i; also E_b must have all 2-torsion rational: a 2-torsion point on the Jacobian of C_b corresponds to an involution of C_b that fixes ω, and here the involutions $(x : y : z) \mapsto (x : -y : -z)$ and $(x : y : z) \mapsto (y : x : -z)$ are defined over $\mathbb{Q}$. Thus E_b must be $Y^2 = X^3 - \beta^2 X$ for some β. We can pin down β by noting that β^2 is quadratic in the coefficients of $b(x^4 + y^4)$, so β must be proportional to b. Then it is enough to compute (or cite) a single example such as $b = 1$ to recover $\beta = 2b$.

list of such b with $2M = 10^{12}$ (which is more than enough for us to verify that the proposed solution is smallest) was computed in 2010 [7]. More precisely, that paper reports on a computation that determines which E_b have positive *analytic* rank (via Tunnell's criterion [12]); but by Kolyvagin — or indeed Coates–Wiles [1], since E_b has complex multiplication — if E_b has positive arithmetic rank then it must have positive analytic rank. Hence we need only consider those b such that $2b$ appears in the list computed by [7]. This reduces by nearly two orders of magnitude the list of possible b values: there are about $5 \cdot 10^{11}/\pi^2 > 5 \cdot 10^{10}$ squarefree $b < 5 \cdot 10^{11}$ such that $b \equiv 1 \bmod 8$, and about $6 \cdot 10^9$ of those are the product of primes congruent to 1 mod 8, but only 66551915 of those satisfy Tunnell's criterion. We call these the "candidate b" values. We thank Mark Watkins and William Hart for finding and making available to us their list of 561217401 squarefree $2b < 10^{12}$ such that $b \equiv 1 \bmod 8$ and E_b has positive analytic rank.

3. Small b

Even when the curve $C_b : x^4 + y^4 = bz^2$ has a rational point, and is thus birational with its Jacobian E_b, we find it easier to use instead the 2-isogenous curve $E'_b : Y^2 = X^3 + b^2X$, which admits a map

$$C_b \to E'_b, \quad (x : y : z) \mapsto \big(b(x/y)^2, b^2xz/y^3\big) \tag{5}$$

that does not depend on a choice of rational point on C_b, or even on the existence of such a point.

The conjecture of Birch and Swinnerton-Dyer, together with the heuristic that the leading term of $L(E, s)$ at $s = 1$ should not grow faster than $N_E^{o(1)}$, suggests that the regulators of E_b and E'_b grow no faster than $b^{1/2+o(1)}$. In our setting these curves have rank at least 2, so their Mordell–Weil groups would typically be generated by points of canonical height at most $b^{1/4+o(1)}$. This is large enough that we cannot hope to find generators for typical $b < 5 \cdot 10^{11}$, but small enough that a 2-descent sufficed to determine the full Mordell–Weil group for most candidate $b < 10^4$. Each curve E'_b has a rational 2-torsion point $(0, 0)$, so Cremona's mwrank [2] easily found all the relevant principal homogeneous spaces. For 67 of the 72 candidate $b < 10^4$, mwrank found two independent points on E'_b and proved that they together with the 2-torsion point $(0, 0)$ generate $E'_b(\mathbb{Q})$. For such b we can then use small combinations of these generators to quickly list all points in $E'_b(\mathbb{Q})$ up to a given height, and check whether any of those pull back under (5) to points on C_b with $b \mid z$. The exceptional b were

$$4721,\ 4777,\ 6497,\ 6577,\ 9881; \tag{6}$$

we treat those b using the methods of the next section.[6]

To know how far we must search in the Mordell–Weil group of each E'_b, we must bound the difference between the canonical height $\widehat{h}$ and the logarithmic ℓ^2 height h. We shall define the logarithmic ℓ^2 height so that the image of a point (x, y, z) on C_b has height $\frac{1}{2}\log(x^4 + y^4)$, whence a bound on h corresponds directly to a

[6]Two of these b, namely 4721 and 6577, are prime; in each case mwrank found only one generator. The remaining three factor: $4777 = 17 \cdot 281$, $6497 = 73 \cdot 89$, $9881 = 41 \cdot 241$; for each of those b, mwrank found two independent points but could not prove that the rank is only 2. We later checked this by running mwrank on the curves E_b, each of which has 3 choices of 2-isogeny descent; in each case at least one of these descents yielded an upper bound of 2 on the rank.

bound on $N = e^{2h}$. To make this work we scale the coordinates of E'_b to obtain the model $E : bY^2 = X^3 + X$, so that (x, y, z) maps to $\big((x/y)^2, xz/y^2\big)$. This has the additional advantage of making the duplication formula, and thus the bounds on $\widehat{h} - h$, independent of b. Explicitly, for P on E we have $X([2]P) = f(X(P))$ where

$$f(X) := \frac{(X^2-1)^2}{4X(X^2+1)}\,. \tag{7}$$

We define the ℓ^2 height as follows.

Definition 1. For a rational number m/n in lowest terms, we define its ℓ^2 *height* and *logarithmic* ℓ^2 *height* by

$$H(m/n) := \sqrt{m^2+n^2} \text{ and } h(m/n) := \log H(m/n)$$

respectively. For a rational point $P = (X, Y) \neq \infty$ on the elliptic curve $bY^2 = X^3 + X$, we define its *logarithmic* ℓ^2 *height* by $h(P) := h(X)$.

We shall need the following lemma adapted from [11] §3.3.

Lemma 1. Let $\phi(X), \psi(X) \in \mathbb{Z}[X]$ be relatively prime polynomials with leading coefficients c_ϕ and c_ψ respectively. Define $d := \max\{\deg\phi, \deg\psi\}$, and for a rational number m/n in lowest terms, define

$$\Phi(m,n) := n^d\phi(m/n) \text{ and } \Psi(m,n) := n^d\psi(m/n).$$

Let $F(X), G(X) \in \mathbb{Q}[X]$ be any polynomials such that $F(X)\phi(X) + G(X)\psi(X) \equiv 1$. Let R the smallest positive integer such that $RF(X), RG(X) \in \mathbb{Z}[X]$, and let $D := \max\{\deg F, \deg G\}$. Then

$$\gcd(\Phi(m,n), \Psi(m,n)) \mid R\gcd(c_\phi, c_\psi)^{d+D}. \tag{8}$$

In particular, if either ϕ or ψ is monic then $\gcd(\Phi(m,n), \Psi(m,n)) \mid R$.

Proof. Without loss of generality, assume that $\deg\phi = d$ and $\deg\psi = e \leq d$, and write $\phi(x) = \sum_{j=0}^{d} a_j x^{d-j}$ and $\psi(x) = \sum_{j=0}^{e} b_j x^{e-j}$ for integers a_j, b_j, where $a_0 = c_\phi$ and $b_0 = c_\psi$. Fix a rational number m/n in lowest terms, and define $\gamma = \gamma(m,n) := \gcd(\Phi(m,n), \Psi(m,n))$; it suffices to show that $\gamma \mid Ra_0^{d+D}$. Substituting $X = m/n$ in the identity $F(X)\phi(X) + G(X)\psi(X) \equiv 1$ and multiplying throughout by Rn^{d+D} gives

$$n^D RF\left(\frac{m}{n}\right)\Phi(m,n) + n^D RG\left(\frac{m}{n}\right)\Psi(m,n) = Rn^{d+D},$$

so certainly $\gamma \mid Rn^{d+D}$. But expanding

$$\begin{aligned} Rn^{d+D-1}\Phi(m,n) &= Rn^{d+D-1}(a_0m^d + a_1m^{d-1}n + \cdots + a_dn^d) \\ &= Rn^{d+D-1}m^da_0 + Rn^{d+D}C \end{aligned}$$

for some integer C, we conclude that

$$\gamma \mid \gcd(Rn^{d+D-1}m^da_0, Rn^{d+D}) = Rn^{d+D-1}\gcd(m^da_0, n) \mid Rn^{d+D-1}a_0,$$

where in the last step we have used that $\gcd(m,n) = 1$. Similarly, we can expand $Rn^{d+D-k}\Phi(m,n)$ for $1 \leq k \leq d+D$ to inductively show that $\gamma \mid Rn^{d+D-k}a_0^k$. At the last stage, we get $\gamma | Ra_0^{d+D}$. □

Note that R here divides the resultant $\mathrm{res}(\phi, \psi)$, but in general can be smaller. We prove:

Proposition 1. For all rational points $P \neq \infty$ on $bY^2 = X^3 + X$, the difference between the canonical and logarithmic ℓ^2 height is bounded by

$$-\frac{4}{3}\log 2 \leq \hat{h}(P) - h(P) \leq \frac{1}{3}\log 2. \tag{9}$$

Proof. We use Tate's formula $\hat{h}(P) = \lim_{n\to\infty} 4^{-n} h([2^n]P)$. (The height h that appears in this formula is the logarithmic ℓ^∞ height associated to the Weierstrass model $Y^2 = X^3 + b^2X$, and thus differs from our logarithmic ℓ^2 height by at most $\log b + O(1)$; since this difference is divided by 4^n, it does not affect the limit as $n \to \infty$.) Now apply Lemma 1 to the numerator and denominator of the duplication formula (7); that is, take $\phi(X) = (X^2-1)^2$ and $\psi(X) = 4X^2(X^2+1)$. Then $d = 4$, and we find the identity

$$\left(\frac{3X^2+4}{4}\right)\phi(X) + \left(\frac{-3X^3+5X}{16}\right)\psi(X) = 1,$$

so that $R = 16$ works. This bounds the possible cancellation between numerator and denominator of $f(m/n) = (m^2-n^2)^2/(4m(m^2+n^2)$, and we conclude that

$$\frac{H(f(X))}{H(X)^4} \geq \frac{1}{16}\frac{\sqrt{\Phi(m,n)^2+\Psi(m,n)^2}}{(m^2+n^2)^2} = \frac{1}{16} + \frac{1}{4}\left(\frac{X}{X^2+1}\right)^2 \geq \frac{1}{16}.$$

for all $X = m/n \in \mathbb{Q}^*$ with $\gcd(m,n) = 1$.

Thus $h([2]P) - 4h(P) \geq -4\log 2$ for all P. For the inequality in the other direction, we use

$$H(f(X)) \leq \sqrt{\Phi(m,n)^2+\Psi(m,n)^2} = H(X)^4 + 4m^2n^2 \leq 2H(X)^4$$

(in the last step $H(X)^4 = (m^2+n^2)^2 \geq 4m^2n^2$ by the AM-GM inequality). Thus $h([2]P) - 4h(P) \leq \log 2$. Therefore,

$$h([2]P) - 4h(P) \in [-4\log 2, \log 2].$$

The telescoping sum

$$4^{-n}h([2^n]P) - h(P) = \sum_{k=1}^{n} 4^{-k}(h([2^k]P) - 4h([2^{k-1}]P))$$

shows that since $\sum_{k=1}^{\infty} 4^{-k} = 1/3$, we have

$$\hat{h}(P) - h(P) \in= \left[-\frac{4}{3}\log 2, \frac{1}{3}\log 2\right],$$

which is equivalent to the claimed inequality (9). □

Suppose then that (x,y,z) is a primitive point on $C_b : x^4 + y^4 = bz^2$ with $x^4+y^4 \leq N_{\max}$. Then its image $P : (X,Y) = (x^2/y^2, xz/y^2)$ on $E : bY^2 = X^3 + X$ satisfies

$$h(P) = \frac{1}{2}\log(x^4+y^4) \leq \frac{1}{2}\log N_{\max} \implies \hat{h}(P) \leq \frac{1}{2}\log N_1 + \frac{1}{3}\log 2. \tag{10}$$

Since the canonical height is independent of the model, the bound (10) applies also on the minimal Weierstrass model E'_b of E on which we computed Mordell–Weil generators. We thus have the following strategy:

Strategy 1 (small b). Given a squarefree positive integer b, to find all the solutions to $x^4 + y^4 = bz^2$ with $x^4 + y^4 \leq N_{\max}$:

(1) first find all points P on $E'_b : Y^2 = X^3 + b^2X$ with $\hat{h}(P) \le h_0 := \frac{1}{2}\log N_{\max} + \frac{1}{3}\log 2$, and then
(2) for each $P = (X, Y)$, check if X/b is a rational square. If not, discard P. If it is, write $\sqrt{X/b} = x/y$ with $(x, y) = 1$, and let $z = Yy^3/(b^2x)$. This (x, y, z) is a solution, and every solution in this range arises in this way.

In our example, if $N_{\max} = N_1$ then this bound becomes $h_0 = \frac{1}{2}\log N_1 + \frac{1}{3}\log 2 < 42.25$, while $N_{\max} = N_2$ makes $h_0 \approx 70$. This algorithm relies on our ability to efficiently find all points up to that height on the curve E'_b. For each of the candidate $b < 10^4$ other than the five exceptions (6), we used Cremona's mwrank to find generators, and gp-pari's qfminim to find all vectors of norm at most 42.25 in the Mordell–Weil lattice. (Actually qfminim lists only nonzero vectors, and only one of each pair $\{P, -P\}$; but the origin and the 2-torsion point $T = (0, 0)$ give trivial solutions, while P and $-P$ give the same solution, and solutions associated to $P = (X, Y)$ and $P + T = (1/X, -Y/X^2)$ are related by swapping x with y.) Doing this with $h_0 = 70$ and each of our 67 small b, we obtained:

Theorem 1. Suppose $x^4 + y^4 = bz^2$ for positive integers b, x, y, z such that $b \mid z$, $\gcd(x, y) = 1$, and $x^4 + y^4 \le 2^{2/3}e^{140} \approx 1.0044 \cdot 10^{61}$. If $b \le 10^4$ and b is not one of the five values listed in (6) then $b = 17$ and $\{x, y\} = \{427511122, 1322049209\}$ or $\{572132418369898, 988478679472373\}$.

This is also why we conjecture that N_2 is the second-smallest powerful integer that can be expressed as the sum of two coprime fourth powers.

4. Large b

For $b > 10^4$, or b among the few values of $b < 10^4$ for which mwrank did not find the full Mordell–Weil group of E'_b, we use another approach, starting from the factorization $x^4 + y^4 = (x^2 + iy^2)(x^2 - iy^2)$ in $\mathbb{Z}[i]$. In effect this is a further descent step; even if we cannot find enough points to generate $E'_b(\mathbb{Q})$, we will still efficiently find all points in the range corresponding to $x^4 + y^4 \le N_{\max} = 3.6125 \cdot 10^{37}$.

Recall that, for fixed b that is a product of distinct primes congruent to 1 mod 8, we seek positive integer solutions (x_0, y_0, z_0) to $x^4 + y^4 = bz^2$ with $(x_0, y_0) = 1$ and $b \mid z_0$. Since b is odd, x_0 and y_0 have opposite parity, so $x_0^2 + iy_0^2$ and $x_0^2 - iy_0^2 \in \mathbb{Z}[i]$ are coprime. Therefore, $x_0^2 + iy_0^2 = \beta\zeta^2$ with $\beta, \zeta \in \mathbb{Z}[i]$ some primitive Gaussian integers with norms b and z respectively. (If b is a product of $k > 0$ distinct primes, then there are 2^{k-1} such β up to units and conjugation.) For fixed $\beta = \mu + i\nu$, we write $\zeta = r + is$ and obtain a solution to the system of equations

$$x^2 = Q_1(r, s), \quad y^2 = Q_2(r, s) \tag{11}$$

where

$$Q_1(r, s) := \mu(r^2 - s^2) - 2\nu rs, \quad Q_2(r, s) := 2\mu rs + \nu(r^2 - s^2). \tag{12}$$

Note also that in this case $(x_0, y_0) = 1$ implies that $(r, s) = 1$ as well. Each of the equations in (11) is a plane conic. If either of them is locally obstructed at some place then $\beta = \mu + i\nu$ is impossible. Assume then that both conics are unobstructed, so that each conic is rational, and thus admits a rational parametrization by the Hasse–Minkowski theorem.

Say we parametrize $x^2 = Q_1(r, s)$ by homogeneous quadratic polynomials $r = r(t_1, t_2)$, $s = s(t_1, t_2)$, $x = x(t_1, t_2)$ with integer coefficients on the projective line

with coordinates $(t_1 : t_2)$. Then $Q_2(r, s)$ is a homogeneous quartic in t_1, t_2, and we seek coprime t_1, t_2 that make it a square.

We can efficiently find all such (t_1, t_2) up to some height bound B using Stoll's program ratpoints, recently ported into gp as hyperellratpoints. (This still takes time essentially quadratic in B, but with a very small constant.) This is not sufficient because $r(t_1, t_2)$ and $s(t_1, t_2)$ may have common factors even when $\gcd(t_1, t_2) = 1$. To avoid this difficulty we replace the single parametrization $(r(t_1, t_2), s(t_1, t_2), x(t_1, t_2))$ by a finite list of parametrizations $(r_i(t_1, t_2), s_i(t_1, t_2), x_i(t_1, t_2))$ such that for every solution (x_0, r_0, s_0) of $x^2 = Q_1(r, s)$ with $\gcd(r_0, s_0) = 1$ there is at least one i and some $t_1, t_2 \in \mathbb{Z}$ such that

$$(r_0, s_0) = \pm\big(r_i(t_1, t_2), s_i(t_1, t_2)\big).$$

[For each prime factor ℓ of $\operatorname{disc} Q_1$ there is a finite set I_ℓ of such $(r, s) \in \mathbb{Z}_\ell[t_1, t_2]$, corresponding to ℓ-adic components of $x^2 = Q_1(r, s)$; the (r_i, s_i) are indexed by $\prod_{\ell | \operatorname{disc} Q_1} I_\ell$. In our setting, $\operatorname{disc} Q_1 = 4(\mu^2 + \nu^2) = 4b$ is squarefree but for the factor 2^2, and we find $|I_\ell| = 2$ for each odd ℓ while $|I_2| = 1$. For example, if $b = 17$ and $(\mu, \nu) = (1, 4)$ we can take $(r_1, s_1) = (2t_1t_2 + 5t_2^2, 2t_1^2 + 2t_1t_2 + t_2^2)$ and $(r_2, s_2) = (2t_1t_2 + 8t_2^2, t_1^2 + t_2^2)$. Documentation of the code that computes (r_i, s_i, x_i) is in preparation and will appear elsewhere.] For each i, let

$$\Phi_i := x_i(t_1, t_2)^2 \text{ and } \Psi_i(t_1, t_2) := Q_2\big(r_i(t_1, t_2), s_i(t_1, t_2)\big).$$

It follows from $x_i^2 \equiv Q_1(r_i, s_i)$ that

$$\Phi_i(t_1, t_2)^2 + \Psi_i(t_1, t_2)^2 = b\,\Xi_i(t_1, t_2)^2 \text{ where } \Xi_(t_1, t_2) := r_i(t_1, t_2)^2 + s_i(t_1, t_2)^2.$$

From a solution (x_0, y_0, z_0) as above, we get a point

$$(x_0, r_0, s_0) = (x(m, n), r(m, n), s(m, n))$$

by the procedure explained above, and hence a point $(Y, T) = (y_0/n^2, m/n)$ on the elliptic curve $Y^2 = \Psi(T, 1)$. Conversely, this point lets us recover (x_0, y_0, z_0) by taking $x_0 = x(m, n)$ and $y_0 = n^2 Y$. Note that in this case $x_0^2 = \Phi_i(m, n)$ and $y_0^2 = \Psi_i(m, n)$ are coprime, whence

$$H\left(\frac{x_0^2}{y_0^2}\right) = \sqrt{x_0^4 + y_0^4} = \sqrt{\Phi_i^2(m, n) + \Psi_i^2(m, n)} = \sqrt{b}\,\Xi_i(m, n).$$

Therefore,

$$\frac{H(x_0^2/y_0^2)}{H(m/n)^4} = b^{1/2}\frac{\Xi_i(m, n)}{(m^2 + n^2)^2} = b^{1/2}\left[\frac{\xi_i(z)}{(z^2 + 1)^2}\right]_{z=m/n} \geq b^{1/2}C_i,$$

where $\xi_i(z) := \Xi_i(z, 1)$ is a quartic with integer coefficients and

$$C_i := \inf_{z \in \mathbb{R}} \frac{\xi_i(z)}{(z^2 + 1)^2}$$

is a positive real number because $r(z, 1)$ and $s(z, 1)$ share no common complex roots: any common root would also be a root of $x(z, 1)$, and then (r, s, x) would be proportional to a degree-1 parametrization, which is not possible for a conic. It follows that

$$H\left(\frac{m}{n}\right)^4 \leq \frac{1}{b^{1/2}C_i} H\left(\frac{x_0^2}{y_0^2}\right) \leq \frac{(N_1/b)^{1/2}}{C_i},$$

and so it suffices to search for all points on the elliptic curve $Y^2 = \Psi_i(T, 1)$ of height at most

$$\max\{|m|, |n|\} \leq H\left(\frac{m}{n}\right) \leq N_1^{1/8} b^{-1/8} C_i^{-1/4}.$$

We can estimate C_i quickly to high numerical precision, and so we have the following strategy:

Strategy 2 (large b). Given a squarefree positive integer b, to find all the solutions to $x^4 + y^4 = bz^2$ with $x^4 + y^4 \leq N_{\max}$:

(1) Find all[7] $\mu, \nu \in \mathbb{Z}$ such that $0 \leq \mu \leq \nu \in \mathbb{Z}$ and $\mu^2 + \nu^2 = b$.
(2) For each of these (μ, ν), define $Q_1(r, s)$ and $Q_2(r, s)$ by (12). Check whether either of the plane conics $x^2 = Q_1(r, s)$ and $y^2 = Q_2(r, s)$ is locally obstructed at some place; if so, discard this choice of (μ, ν).
(3) If neither is locally obstructed, use qsolve to produce a finite list of parametrizations $(x(t_1, t_2), r(t_1, t_2), s(t_1, t_2))$ of $x^2 = Q_1(r, s)$ of the form explained above.
(4) For each parametrization on this list, define $\xi_i(z) := r_i(z, 1)^2 + s_i(z, 1)^2$ and calculate C_i to sufficient precision that $N_{\max}^{1/8} b^{-1/8} C_i^{-1/4}$ can be estimated to within an integer.
(5) Use hyperellratpoints to find all points (Y, T) on the elliptic curve $Y^2 = \Psi_i(T, 1) := Q_2(r_i(T, 1), s_i(T, 1))$ of ℓ^∞ height at most the upper bound on $N_1^{1/8} b^{-1/8} C_i^{-1/4}$ from (4). Given a point (Y, T), write $T = m/n$ in lowest terms and define $x_0 := x(m, n)$ and $y_0 = n^2 Y$. Then $(x_0, y_0, b^{-1/2}\sqrt{x_0^4 + y_0^4})$ is a solution of the required form. Conversely, every such solution arises in this way.

It is easy to write a one-line algorithm in gp that uses LLL lattice reduction to efficiently find all such pairs (μ, ν). Checking local obstructions are easy in gp, and both qsolve and hyperellratpoints are efficient enough to allow us to go to $N_{\max} = N_1$ to prove the claim asserted in the abstract.

To keep this proof self-contained, we conclude by showing the result, attributed to Lucas, that $x^4 + y^4 = b^3$ has no solution in positive coprime integers; recall that we need this to ensure that $a \geq 17$ in $x^4 + y^4 = a^2 b^3$.

Proposition 2. There are no positive integers x, y, b such that $\gcd(x, y) = 1$ and $x^4 + y^4 = b^3$.

Proof. Assume on the contrary that such x, y, b exist. Necessarily b is odd because if $2 \mid b$ then $8 \mid b^3 = x^4 + y^4$, so x, y are both even, contradicting $\gcd(x, y) = 1$. As before we factor over $\mathbb{Z}[i]$, finding $(x^2 + iy^2)(x^2 - iy^2) = b^3$, with the factors $x^2 \pm iy^2$ relatively prime because b is odd. Hence each of $x^2 \pm iy^2$ is a cube in $\mathbb{Z}[i]$, say

$$x^2 \pm iy^2 = (m \pm in)^3, \tag{13}$$

because $\mathbb{Z}[i]$ has unique factorization and all its units are cubes. Expanding (13) gives

$$x^2 = m(m^2 - 3n^2), \quad y^2 = n(3m^2 - n^2). \tag{14}$$

In particular m and n are relatively prime because any common factor would be inherited by x^2 and y^2. It follows that each of $m, n, m^2 - 3n^2, 3m^2 - n^2$ is a square

[7] As observed before, if b is a product of k distinct primes congruent to 1 mod 8 then there are 2^{k-1} such pairs (μ, ν).

multiplied by ± 1 or ± 3. Moreover m, n are of opposite parity (else x, y are both even); switching x with y if necessary we may assume that m is odd and that n is even, and thus divisible by 4 because $4 \mid x^2$. This in turn makes $m^2 - 3n^2 \equiv 1 \bmod 8$ while $3m^2 - n^2 \equiv 3 \bmod 8$, so $m^2 - 3n^2$ and thus also m is a square, while $3m^2 - n^2$ and thus also n is 3 times a square. Writing $(m, n) = (M^2, 3N^2)$, we deduce that $M^4 - 27N^4$ and $M^4 - 3N^4$ are both squares. We claim that neither of these can be a square unless $N = 0$, which would also make $y = 0$. Indeed each of $M^4 - 27N^4 = z^2$ and $M^4 - 3N^4 = z^2$ is an elliptic curve with 2 rational points at infinity that differ by a 2-torsion point; Weierstrass models are respectively $y^2 = x^3 + 108x$ and $y^2 = x^3 + 12x$. In each case a 2-descent proves[8] that there are no other rational points. □

To take our analysis past $N \le 3.6125 \cdot 10^{37} = 17^2(5 \cdot 10^{11})^3$, we would need either an extension of the Hart–Tornaría–Watkins computation [7] to $2b > 10^{12}$ or an analogue of Proposition 2 for $x^4 + y^4 = a^2b^3$ for $a = 17, 41, 73, 89, 97, \ldots$. The former approach would require extensive computation, though the result would be of independent interest and could find other uses. The latter approach runs into a new theoretical difficulty: we still obtain formulas for x^2, y^2 analogous to (14), but these cubics no longer factor. It may be possible to instead give complete parametrizations of coprime (X, y, b) such that $X^2 + y^4 = a^2b^3$, analogous to those of [9, p.234, B.1.1] for $a = 1$. Such a parametrization yields a short list of homogeneous polynomials $X(m, n)$ of degree 12, for each of which one could use hyperellratpoints to find all solutions of $x^2 = X(m, n)$ with $x < N_{\max}^{1/4}$ in time about $N_{\max}^{1/12}$.

References

[1] John H. Coates and Andrew Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Inventiones math.*, 39:223–251, 1977.

[2] J. E. Cremona. mwrank. http://homepages.warwick.ac.uk/staff/J.E.Cremona/mwrank/index.html.

[3] J. E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, second edition, 1997. URL: https://johncremona.github.io/book/fulltext/index.html.

[4] Henri Darmon and Loïc Merel. Winding quotients and some variants of Fermat's Last Theorem. *J. f.d. reine und angew. Math.*, 490:81–100, 1997.

[5] Noam D. Elkies. $x^4 + y^4$ powerful for relatively prime x, y. MathOverflow Question 191889. URL: https://mathoverflow.net/q/191889 (version: 2017-04-13).

[6] Noam D. Elkies and Nicholas F. Rogers. Elliptic Curves $x^3 + y^3 = k$ of High Rank. In *Proceedings of ANTS-6, 2004; D. Buell, ed.*, volume 3067 of *Lecture Notes in Computer Science*, pages 184–193, 2004.

[7] William B. Hart, Gonzalo Tornaría, and Mark Watkins. Congruent number theta coefficients to 10^{12}. *9th International Symposium on Algorithmic Number Theory, ANTS-IX 2010*, 6197:186–200, 2010.

[8] Aleksandar Ivić. *The Riemann Zeta Function*. John Wiley & Sons, New York, 1985.

[9] Johnny Roberts. A complete solution to $x^2 + y^3 + z^5 = 0$. *J. f.d. reine und angew. Math.*, 571:213–236, 2004.

[10] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 106, Graduate Texts in Mathematics. Springer, second edition, 2008.

[11] Joseph H. Silverman and John H. Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer, second edition, 2015.

[12] Jerrold B. Tunnell. A classical Diophantine problem and modular forms of weight 3/2. *Inventiones math.*, 72(2):323–334, 1983.

[8] We did this in mwrank, and checked against published and online tables (both curves have conductor $576 = 2^4 3^2$). According to Dickson's *History*, $x^4 - 27y^4 = z^2$ and $x^4 - 3y^4 = z^2$ are among the Diophantine equations $ax^4 + by^4 = cz^2$ that Lucas proved have no nonzero integer solutions.

[13] Mark Watkins, Stephen Donnelly, Noam D. Elkies, Tom Fisher, Andrew Granville, and Nicholas F. Rogers. Ranks of quadratic twists of elliptic curves. *Publ. math. de Besançon, Alg. et Théor. nr.*, 2014/2:63–98, 2014. URL: http://www.numdam.org/item/10.5802/pmb.9.pdf.

Department of Mathematics, Harvard University, Cambridge MA 02138 USA
E-mail address: elkies@math.harvard.edu

Harvard University
E-mail address: gauravgoel@college.harvard.edu