On Powerful Integers Expressible as Sums of Two Coprime Fourth Powers

ANTS-XV, University of Bristol

Noam D. Elkies[1] and Gaurav Goel*[2]

Harvard University, Cambridge, MA, USA

August 2022

[1]Simons AGNTC Collaboration grant #550031
[2]Harvard College Research Program (HCRP) Summer 2020

Statement of Results

Definition

An integer N is said to be *powerful* if every prime factor $p \mid N$ satisfies $p^2 \mid N$.

A powerful $N \geq 1$ is $a^2 b^3$ for $a, b \in \mathbf{Z}$ with $a, b \geq 1$, uniquely if b is squarefree.

Theorem

The smallest powerful $N > 1$ expressible as a sum of two coprime fourth powers is

$$\begin{aligned} N_1 :&= 3088257489493360278725196965477359217 \\ &= 17^3 \cdot 73993169^2 \cdot 338837713^2 \\ &= 427511122^4 + 1322049209^4, \end{aligned}$$

and this is in fact the only such integer up to $3.6125 \cdot 10^{37}$.

Statement of Results (Cont'd)

Further:

(1) We propose a candidate $\approx 1.06 \cdot 10^{60}$ for the next smallest such number, namely

$$17^3 \cdot 38401618921^2 \cdot 382833034044850177^2$$
$$= 572132418369898^4 + 988478679472373^4.$$

(2) We give an algorithm using the arithmetic of elliptic curves to quickly list all such numbers with small b; use it to go up to $2^{-2/3}\exp(400) \approx 3.29 \cdot 10^{173}$.

(3) We use (2) to propose a candidate $\approx 7.51 \cdot 10^{161}$ with $b = 113$ for the smallest such number with $b \neq 17$.

Introduction and Motivation

- Reconsider classical Diophantine equations with ~~squares~~ powerful numbers.

- Powerful numbers contain the squares as a subset of positive density $\zeta(3)/\zeta(3/2) \approx 0.46$, so might expect solutions to be more numerous only by a constant factor, but...

- New behavior can arise, e.g.

  (1) consecutive powerful numbers, e.g. $3^2 - 2^3 = 17^2 - 2^5 3^2 = 1$ (Fermat-Pell), or

  (2) 3-powerful "counterexamples" to FLT3, e.g. $2^3 \cdot 3^5 \cdot 73^3 = 919^3 + (-271)^3$ (use the elliptic curve $x^3 + y^3 = bz^3$).

- We search for powerful "counterexamples" to Fermat's theorem on solutions to $z^2 = x^4 + y^4$, i.e. for powerful N solutions to $N = x^4 + y^4$ with coprime $x, y \in \mathbf{Z}$.

- Expect such numbers to be rare, i.e. that the number of such $N \leq N_{\max}$ is $N_{\max}^{o(1)}$.

Introduction and Motivation (Cont'd)

- Consider twists[3] of the genus 1 curve $C : x^4 + y^4 = z^2$ of the form $C_b : x^4 + y^4 = bz^2$ for $b \in \mathbf{Z}$, and seek coprime $(x, y, z) \in \mathbf{Z}^3$ on C_b s.t. $b \mid z$.
- We show that if $C_b(\mathbf{Q})$ is nontrivial, then it contains an *acceptable* point.
- The first twist that works is C_{17} of rank 2. The smallest soln. s.t. $17 \mid z$ is N_1.
- To check that N_1 is the smallest over all b seems hard: searching over (x, y) up to $N_1^{1/2}$ or over $b < N_1^{1/3}$ (and processing that many elliptic curves) is daunting!
- What to do?

[3] A *twist* of a smooth projective curve C defined over a perfect field K is a smooth projective curve C' defined over K that is isomorphic to C over $\overline{K}$.

Why do we care?

- Questions such as this one arise naturally.
- This question needs a combination of nontrivial theory and computation.
- It involves an application, not previously known, of a computation [1] of congruent number theta coefficients by Hart, Tornaria, and Watkins presented at ANTS-IX.
- It's fun!

Reducing from $1.46 \cdot 10^{12}$ to 66551915 Candidate b's

Let $N > 1$ be powerful and a sum of two coprime fourth powers. Then:

(1) Every $p \mid N$ is 1 mod 8.

Proof Sketch: $2 \nmid N$ and odd $p \mid N \Rightarrow \exists\, \alpha \in (\mathbf{Z}/p)^*$ s.t. $\alpha^4 = -1$.

(2) (Lucas) If $N = a^2 b^3$ and b squarefree, then $a, b \geq 17$.

Proof Sketch: We have $b > 1$ by Fermat. If $a = 1$, then $x^2 \pm iy^2 \in \mathbf{Z}[i]$ are cubes. Reduce to showing $y^2 = x^3 + \{12, 108\}x$ have rank 0.

Let b be a product of $k \geq 1$ distinct primes, each 1 mod 8, and $C_b : x^4 + y^4 = bz^2$.

(1) If $C_b(\mathbf{Q}) \neq \emptyset$, then C_b is $\mathbf{Q}$-isomorphic to its Jacobian $E_b : Y^2 = X^3 - 4b^2 X$.

(2) The rational torsion of E_b is $E_b(\mathbf{Q})_{\text{tors}} = E_b[2] = \{\infty, (0,0), (\pm 2b, 0)\}$.

(3) C_b has nontrivial rational point $\Leftrightarrow$ E_b has positive rank $\Leftrightarrow$ $2b$ is congruent,

(4) in which case, by Coates-Wiles [2], E_b has positive *analytic* rank, and this can be checked via Tunnell's criterion [3].

Reducing from $1.46 \cdot 10^{12}$ to 66551915 Candidate b's (Cont'd)

- Look at squarefree $b \geq 1$ with each factor 1 mod 8 such that $2b$ is congruent.
- Going up to $b \leq M$ can be used to find all solutions up to $17^2 M^3$.
- The list of all such numbers (more precisely, of all b such that E_b has even positive analytic rank) up to $M = 5 \cdot 10^{11}$ is included in the results of a recent comptuation [1] by Hart, Tornaria, and Watkins.[4]
- This leaves us with 66551915 "candidate b" values, and looking at these suffices to go up to $17^2(5 \cdot 10^{11})^3 = 3.6125 \cdot 10^{37} > N_1$.

[4] We thank Mark Watkins and William Hart for making this list available to us.

Principal Search Strategy

Let $b \geq 1$ be as above and look for coprime $x, y, z \in \mathbf{Z}$ s.t. $x^4 + y^4 = bz^2$.

(1) Factor $x^4 + y^4 = (x^2 + iy^2)(x^2 - iy^2)$. Then $x^2 \pm iy^2 \in \mathbf{Z}[i]$ are coprime.

(2) Write $x^2 + iy^2 = \beta\zeta^2$ for $\beta, \zeta \in \mathbf{Z}[i]$ primitive of norms b, z respectively.

(3) Let $\beta = \mu + i\nu$ and $\zeta = r + is$ for $\mu, \nu, r, s \in \mathbf{Z}$ with $\gcd(\mu, \nu) = \gcd(r, s) = 1$. We are reduced to the conics

$$x^2 = Q_1(r,s) := \mu(r^2 - s^2) - 2\nu rs,$$
$$y^2 = Q_2(r,s) := 2\mu rs + \nu(r^2 - s^2).$$

If b has k prime factors, then (up to units) there are 2^k primitive $\beta \in \mathbf{Z}[i]$ of norm b. For each β, look at the two conics.

(1) If either conic is locally obstructed, discard β.

(2) Else, parametrize $x^2 = Q_1(r,s)$ by $\mathbf{P}^1_{\mathbf{Q}}$ using $r, s, x \in \mathbf{Z}[m,n]_2$, BUT...

(3) Not sufficient. If $m, n \in \mathbf{Z}$, then $\gcd(m,n) = 1 \not\Rightarrow \gcd(r(m,n), s(m,n)) = 1$.

Interlude: Integer Parametrizations of Planar Integer Quadratic Forms

- Let $Q(r,s,x) \in \mathbf{Z}[r,s,x]_2$ s.t. the conic $C_Q = \mathbf{V}(Q) \subset \mathbf{P}^2$ is rational.
- Usually, a single parametrization $(r,s,x) \in \mathbf{Z}[m,n]_2^3$ does not suffice to list all coprime triples $(r,s,x) \in \mathbf{Z}^3$ on Q by using only coprime $m,n \in \mathbf{Z}^2$.
- For instance, let $Q = x^2 - r^2 - s^2$. This admits the parametrization $(r,s,x) = (m^2-n^2, 2mn, m^2+n^2)$, but can't get $(4,3,5) \in \mathbf{Z}^3$ on Q by $m,n \in \mathbf{Z}$.
- We show: there is a finite list $\{(r_i,s_i,x_i)\}_i \subset \mathbf{Z}[m,n]_2^3$ of parametrizations s.t. for every pairwise coprime triple $(r,s,x) \in \mathbf{Z}^3$ satisfying Q there is at least one i and some coprime $m,n \in \mathbf{Z}$ such that $(r,s,x) = (r_i(m,n), s_i(m,n), x_i(m,n))$.

  Proof Sketch: For each prime $\ell \mid \operatorname{disc} Q$, there is a finite set I_ℓ of parametrizations in $\mathbf{Z}_\ell[m,n]_2$ corresponding to the ℓ-adic components of Q. These parametrizations (r_i,s_i,x_i) are indexed by $i \in \prod_{\ell \mid \operatorname{disc} Q} I_\ell$.

Elkies has written a gp routine qsolve that given a quadratic form Q produces such a list (r_i,s_i,x_i) of parametrizations.

Principal Search Strategy (Cont'd)

(4) Produce a finite list $\{(r_i(m,n), s_i(m,n), x_i(m,n))\}_i$ of parametrizations of the plane conic $x^2 = Q_1(r,s)$ as above.

- ☐ In our case, $\operatorname{disc} Q_1 = 4(\mu^2 + \nu^2) = 4b$, so $|I_2| = 1$ and $|I_\ell| = 2$ for odd $\ell \mid b$, so 2^k parametrizations suffice.

(5) For each i, let $\Psi_i(m,n) = Q_2(r_i(m,n), s_i(m,n))$. A point (x,y,z) as above then gives us a point on the elliptic curve $Y^2 = \Psi_i(T,1)$ for some i.

(6) Have strategy: find all β, find all (r_i, s_i, x_i), and all points on $Y^2 = \Psi_i(T,1)$ using Stoll's hyperellratpoints up to a calculated height bound.

This strategy sufficed to prove the theorem.

Another Strategy for Small b's

- For a $b \geq 1$ as above, consider the 2-isogenous $E_b' : Y^2 = X^3 + b^2 X$ which admits a map $\rho_b : C_b \to E_b', (x:y:z) \mapsto (b(x/y)^2, b^2 xz/y^3)$.

- Algorithm: for each $b \geq 1$,
  (i) find all $P \in E_b'(\mathbf{Q})$ with $\hat{h}(P) \leq \frac{1}{2} \log N_{\max} + \frac{1}{3} \log 2$, and
  (ii) for each $P = (X,Y)$ check if $X/b \in (\mathbf{Q}^*)^2$. If not, discard P.
  (iii) Else, write $\sqrt{X/b} = x/y$ for coprime $x, y \in \mathbf{Z}$ and let $z := Yy^3/(b^2 x)$.
  (iv) For (x,y,z) as in (iii), check if $b \mid z$.

- We show: the set of acceptable points in $E_b'(\mathbf{Q})$ forms a coset of a subgroup of $E_b'(\mathbf{Q})$ of index dividing $2^k b$.

  Proof Sketch: $\rho_b(C_b(\mathbf{Q})) = w_2^{-1}[b]$ where $w_2 = [X] : E_b'(\mathbf{Q}) \to \mathbf{Q}^*/(\mathbf{Q}^*)^2$.
  For $p \mid b$, curve $E_b'(\mathbf{Q}_p)$ has Kodaira type I_0^* and Tamagawa number $c_p = 4$; using this, figure out when a point is p-acceptable.

- Given gens. $P_1, \ldots, P_r$ of $E_b'(\mathbf{Q})/\text{tors}$, a $P = \sum_{i=1}^r a_i P_i \in E_b'(\mathbf{Q})$ is acceptable iff the $a_i \in \mathbf{Z}$ satisfy a few linear congruences mod 2 and mod p for each $p \mid b$.

- Given generators of $E_b'(\mathbf{Q})$, can list all acceptable points up to any height.

Another Strategy for Small b's (Cont'd)

- The BSD conjecture and heuristics on $L(E,s)$ at $s=1$ suggest that the regulators of E_b, E'_b grow not faster than $b^{1/2+o(1)}$.
- Our curves have rank ≥ 2, so their MW groups would be typically generated by points of height at most $b^{1/4+o(1)}$.
- Can't find generators of $E'_b(\mathbf{Q})$ for a typical $b < 5 \cdot 10^{11}$, but a 2-descent in mwrank [4] sufficed to find the full MW group for most "small" b (i.e. $b < 10^4$).
- Since $(0,0) \in E'_b(\mathbf{Q})[2]$, mwrank easily found all principal homogenous spaces.
- For 67 of the 72 candidate $b < 10^4$ (all except $4721, 4777, 6497, 6577$, and 9881), mwrank found 2 independent points in $E'_b(\mathbf{Q})$ and proved that they together with torsion $(0,0)$ generate $E'_b(\mathbf{Q})$.
- This allowed us to go up to $2^{-2/3}\exp(400)$ for all but five $b < 10^4$ to find the other solutions mentioned on the results page.

Suggestions for Further Work

To take our analysis beyond $3.6125 \cdot 10^{37}$, we would need either

- ☐ an extension of the Hart-Tornaria-Watkins [1] computation to $2b > 10^{12}$, or
- ☐ an extension of Lucas's result on $x^4 + y^4 = a^2 b^3$ to $a = 17, 41, 73, \ldots$, or
- ☐ a complete parametrization of coprime (X, y, b) such that $X^2 + y^4 = a^2 b^3$ (as in Roberts [5] for $a = 1$) by homogenous polynomials of degree 12.

To take our second approach further, we would need

- ☐ to find a better way (say using higher descent) of finding generators of the MW group of $E'_b : Y^2 = X^3 + b^2 X$, at least in the fairly special case when $b > 1$ is a product of distinct primes, each 1 mod 8, with $2b$ congruent.

References

[1] W. B. Hart, G. Tornaria, and M. Watkins, "Congruent number theta coefficients to 10^{12}," *9th International Symposium on Algorithmic Number Theory, ANTS-IX 2010*, vol. 6197, pp. 186–200, 2010.

[2] J. H. Coates and A. Wiles, "On the conjecture of Birch and Swinnerton-Dyer," *Inventiones math.*, vol. 39, pp. 223–251, 1977.

[3] J. B. Tunnell, "A classical Diophantine problem and modular forms of weight $3/2$," *Inventiones math.*, vol. 72, no. 2, pp. 323–334, 1983.

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

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