hexagon:2611.00058v1

Two improved lower bounds for the 2-adic valuation of the constant of the Prouhet–Tarry–Escott problem

David Niedbala Giraudin
ORCID 0009-0009-1526-1178

3 November 2026

Abstract

For an ideal solution of the Prouhet–Tarry–Escott problem of size n the associated constant C is divisible by a large power of 2. Restricting to symmetric solutions, we prove two new lower bounds for $v_2(C)$: $v_2(C) \geq 14$ at $n = 15$, improving 12, and $v_2(C) \geq 19$ at $n = 20$, improving 18; both earlier bounds are those of the companion article hexagon:2611.00057. The first rests on two identities satisfied by every symmetric solution of odd size, one relating $v_2(C)$ to a difference of two products and one turning the index relation into an equality, together with an arithmetic criterion for a block of entries of equal valuation. The second rests on an identity internal to each of the two sides, from which we deduce that the vanishing of the cross invariant R forces $k_0 \equiv 0 \pmod 4$ when $k_0 \geq 4$. Two self-contained verifiers accompany the note.

1 Setting and statements

Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$ be multisets forming an ideal solution of the Prouhet–Tarry–Escott problem, that is $\sum_i a_i^k = \sum_i b_i^k$ for $1 \leq k \leq n-1$ while the two multisets differ. The associated constant is

$$C = \prod_i a_i - \prod_i b_i.$$

A solution is *symmetric* when $B = -A$ (after a translation) for n odd, and when $A = \{\pm a_1, \ldots, \pm a_m\}$, $B = \{\pm b_1, \ldots, \pm b_m\}$ with $n = 2m$ for n even. As in [6], solutions of odd size are taken with entries in $\mathbb{Z}_2$ and solutions of even size with entries in $\mathbb{Z}$. Throughout, v_2 denotes the 2-adic valuation and all statements are about symmetric solutions.

Kleiman's bound gives $v_2(C) \geq v_2((n-1)!)$ [5]. In [6] the symmetric case is treated at every size up to 20: the values $4, 6, 9, 11$ at $n = 5, 7, 9, 11$ are attained (at $n = 11$ over $\mathbb{Z}_2$), the bound $v_2(C) \geq 12$ is proved at $n = 13$ and at $n = 15$, and the bounds $8, 11, 12, 12, 16, 18, 18$ are proved at $n = 8, 10, 12, 14, 16, 18, 20$. The present note improves two of these.

Theorem 1. *Every symmetric ideal solution of size* 15 *over* $\mathbb{Z}_2$ *satisfies* $v_2(C) \geq 14$.

Theorem 2. *Every symmetric ideal solution of size* 20 *with entries in* $\mathbb{Z}$ *satisfies* $v_2(C) \geq 19$.

Sections 2 and 3 develop the tools and prove these. Section 5 records what is proved, what is verified by computation, and what remains open.

2 Odd sizes

Let n be odd and $B = -A$. The ideal conditions read $p_k(A) = 0$ for every odd $k \le n-2$, where p_k is the k-th power sum. Equivalently, by Newton's identities, $e_j(A) = 0$ for every odd $j \le n-2$; the only surviving odd index is $j = n$. Writing $m = (n-1)/2$ we therefore obtain the following normal form.

Lemma 3. *Let $F(x) = \prod_{i=1}^{n}(x - a_i)$. Then there are a monic $H \in \mathbb{Z}_2[y]$ of degree m and $c \in \mathbb{Z}_2$ with*

$$F(x) = x\,H(x^2) - c, \qquad c = \prod_i a_i,$$

and $C = 2c$, so that $v_2(C) = 1 + \sum_i v_2(a_i)$.

We write $t = \sum_i v_2(a_i)$, so $v_2(C) = 1 + t$, and call the multiset of the nonzero $v_2(a_i)$ the *profile*; w denotes the number of odd entries, so that $n = w + u$ with u the number of even entries. Reducing $p_1(A) = 0$ modulo 2 shows that w is even.

2.1 Two identities

Lemma 4 (two products)**.** *With the notation of Lemma 3,*

$$\prod_i (1 + a_i) = H(1) + c, \qquad \prod_i (1 - a_i) = H(1) - c,$$

hence $2c = \prod_i(1 + a_i) - \prod_i(1 - a_i)$ and $v_2(C) = v_2\big(\prod_i(1 + a_i) - \prod_i(1 - a_i)\big)$.

Proof. $F(1) = \prod_i(1 - a_i)$ and $F(1) = H(1) - c$ give the second identity. Since n is odd, $F(-1) = \prod_i(-1 - a_i) = -\prod_i(1 + a_i)$, while $F(-1) = -H(1) - c$; this gives the first. Subtracting yields $2c$, and $C = 2c$. □

Lemma 5 (index identity)**.** *For every index j,*

$$\prod_i (a_j + a_i) = 2c, \qquad \textit{hence} \qquad \sum_i v_2(a_j + a_i) = v_2(C).$$

Proof. By Lemma 3, $F(x) + F(-x) = -2c$ identically. Taking $x = a_j$ and using $F(a_j) = 0$ gives $F(-a_j) = -2c$; and $F(-a_j) = \prod_i(-a_j - a_i) = -\prod_i(a_j + a_i)$. □

Lemma 5 is an equality for every single index, not merely an inequality for the best index. Written out, it determines the internal structure of each block of entries of equal valuation. Let f be a valuation occurring with multiplicity m_f in the profile and write those entries as $2^f b_i$ with b_i odd. Separating the contributions in Lemma 5 according to the valuation of the partner gives, for each i in the block,

$$\sum_{\substack{k \ne i \\ v_2(a_k) = f}} v_2(b_i + b_k) = R_f, \qquad R_f = v_2(C) - (1 + f) - \sum_{v \ne f} m_v \min(f, v) - (m_f - 1)f, \quad (1)$$

a quantity depending only on $v_2(C)$ and the profile (here $m_0 = w$). The same computation applied to an odd entry gives $\sum_{k \ne j} v_2(a_j + a_k) = t$, the sum running over the w odd entries.

2.2 An arithmetic criterion for a block

Lemma 6. *For b, b' odd, $\min\big(v_2(b-b'), v_2(b+b')\big) = 1$, and $v_2(b+b') = 1$ if and only if $b \equiv b' \pmod 4$.*

Proof. $(b+b') + (b-b') = 2b$ has valuation 1, so the minimum of the two valuations is 1. Both $b \pm b'$ are even; $b + b' \equiv 0 \pmod 4$ holds exactly when $b' \equiv -b \pmod 4$, that is exactly when b and b' lie in different classes modulo 4. □

Proposition 7 (block criterion)**.** *Let $b_1, \dots, b_m$ be odd with $\sum_{k \neq i} v_2(b_i + b_k) = R$ for every i. Then*

$$R = m - 1, \qquad \text{or} \qquad m \text{ is even and } R \geq \tfrac{3m}{2} - 1.$$

In particular $R = m$ is impossible as soon as $m \geq 3$, and for m odd the value $R = m - 1$ is forced.

Proof. By Lemma 6 the indices split into $P = \{i : b_i \equiv 1 \ (4)\}$ and $Q = \{i : b_i \equiv 3 \ (4)\}$, with $v_2(b_i + b_k) = 1$ inside a part and ≥ 2 across. Put $p = |P|$, $q = |Q| = m - p$. For $i \in P$ the row sum is $(p-1) + \sum_{k \in Q} v_2(b_i + b_k) = R$, so the total of the cross entries, counted from the P side, equals $p(R - p + 1)$; counted from the Q side it equals $q(R - q + 1)$. Equating and writing $s = R + 1$ gives $s(p - q) = (p - q)(p + q)$, hence $p = q$ or $s = m$, that is $R = m - 1$. If $p = q = m/2$ then each row carries $m/2 - 1$ entries equal to 1 and $m/2$ entries at least 2, whence $R \geq 3m/2 - 1$. If one part is empty all entries equal 1 and $R = m - 1$. □

2.3 Finite differences

Let $E_j = \sum_i c_i^{2j+1}$, the sum running over the even entries c_i, and let Δ be the forward difference in j. Since Δ^m applied to $j \mapsto x^j$ equals $(x-1)^m$ at $j = 0$,

$$\Delta^m E = \sum_i c_i \, (c_i^2 - 1)^m. \tag{2}$$

On the other hand, for an odd entry a write $a^2 = 1 + 8k_a$ with $k_a \in \mathbb{Z}_2$; then $a^{2j+1} = a(1 + 8k_a)^j$, and Δ^m of that sequence equals $a(8k_a)^m$ at $j = 0$. Since $E_j = -\sum_{a \text{ odd}} a^{2j+1}$ for $0 \leq j \leq M$ with $M = (n-3)/2$, we obtain

$$\Delta^m E = -8^m \sum_{a \text{ odd}} a \, k_a^m, \qquad \text{in particular} \qquad 2^{3m} \mid \Delta^m E \quad (0 \leq m \leq M). \tag{3}$$

This is the finite-difference lemma of [6].

Lemma 8. *Let $c_1, \dots, c_u$ be even elements of $\mathbb{Z}_2$ satisfying the conditions $2^{3m} \mid \Delta^m E$ for $0 \leq m \leq M$, and let λ be a unit of $\mathbb{Z}_2$. Then $\lambda c_1, \dots, \lambda c_u$ satisfy the same conditions. Consequently, when these conditions are imposed, the odd part of one even entry may be normalised to 1.*

Proof. Write $\lambda^2 = 1 + 8\kappa$. For each c,

$$(\lambda^2 c^2 - 1)^m = \big((c^2 - 1) + 8\kappa c^2\big)^m = \sum_{k=0}^{m} \binom{m}{k} (8\kappa)^k c^{2k} (c^2 - 1)^{m-k},$$

and $c^{2k} = \big(1 + (c^2 - 1)\big)^k = \sum_{l=0}^{k} \binom{k}{l} (c^2 - 1)^l$. Summing over the even entries,

$$\sum_i \lambda c_i (\lambda^2 c_i^2 - 1)^m = \lambda \sum_{k=0}^{m} \sum_{l=0}^{k} \binom{m}{k} \binom{k}{l} (8\kappa)^k \, \Delta^{m-k+l} E.$$

Since $m-k+l \le m \le M$, each $\Delta^{m-k+l}E$ is divisible by $2^{3(m-k+l)} \ge 2^{3(m-k)}$, so each term is divisible by $2^{3k} \cdot 2^{3(m-k)} = 2^{3m}$. For the normalisation take $\lambda = b^{-1}$, b the odd part of the chosen entry; the block conditions (1) involve only valuations of sums and are unchanged by the scaling. □

2.4 Proof of Theorem 1

The admissible pairs (profile, w) at a given n and t are those passing the necessary conditions of [6, Sections 6–9]. At $n = 15$ they leave none at $t \le 10$, none at $t = 12$, and four candidates at $t = 11$. We eliminate the four.

The candidate $w = 8$, profile $(3, 2, 2, 1, 1, 1, 1)$. Here $v_2(C) = 12$ and the block of valuation 1 has multiplicity $m_1 = 4$; formula (1) gives $R_1 = 12 - 2 - 3 - 3 = 4$. By Proposition 7 the value $R = m$ is impossible for $m \ge 3$, so this candidate does not occur.

The candidates $w = 12$, profiles $(9, 1, 1)$, $(7, 2, 2)$, $(5, 3, 3)$. Each has three even entries, and (1) pins the single value $v_2(b_1+b_2)$ of the repeated block to 8, 5 and 2 respectively. The odd parts of the three even entries are then lifted one 2-adic digit at a time; by Lemma 8 one of them is fixed to 1. At level L the odd parts are known modulo 2^L, and a residue class is discarded only when the constraint of (1) or one of the divisibilities (3), evaluated to the precision then available, already fails for every lift of it. In each of the three cases the set of surviving residue classes becomes empty, at levels 11, 10 and 9 respectively, the largest intermediate set having 512, 256 and 128 elements. Hence none of the three occurs.

Consequently $t \ge 13$, and $v_2(C) = 1 + t \ge 14$. □

Remark 9. At $n = 13$ the same analysis, applied to the four candidates at $t = 11$ left by the conditions used in the lower-bound proofs of [6], removes two of them, namely $w = 6$ with profile $(3, 2, 2, 1, 1, 1, 1)$, by Proposition 7, and $w = 8$ with profile $(4, 3, 2, 1, 1)$, because (1) returns $R_3 = 1$ for a block of multiplicity 1, where the left-hand side is an empty sum (it is also excluded by [6, Theorem 8.3]). Two candidates remain, $w = 8$ with profiles $(7, 1, 1, 1, 1)$ and $(5, 2, 2, 1, 1)$, and the bound at $n = 13$ stays at 12.

3 Even sizes

Let $n = 2m$ and put $u_i = a_i^2$, $v_j = b_j^2$. The odd power sums vanish by symmetry, and the even ones agreeing up to degree $2(m-1)$ say exactly that

$$P(y) = \prod_{i=1}^{m}(y - u_i) \qquad \text{and} \qquad Q(y) = \prod_{j=1}^{m}(y - v_j)$$

share every coefficient but the constant one. Write $Q = P + d$; then $d = \prod_j (u_i - v_j)$ for every i, $d = \pm C$ and $v_2(d) = v_2(C)$. Evaluating Q at u_i recovers the index identity in this setting,

$$\sum_j v_2(u_i - v_j) = v_2(C) \text{ for each } i, \qquad \sum_i v_2(u_i - v_j) = v_2(C) \text{ for each } j. \tag{4}$$

Let k_0 be the number of odd entries on each side (it is the same on both sides [6, Prop. 3.2]); for odd entries write $a^2 = 1 + 8\xi$ and $b^2 = 1 + 8\eta$. Separating (4) at an odd index gives $v_2(C) = 3k_0 + R$ with

$$R = \sum_{j \text{ odd}} v_2(\xi_i - \eta_j) \quad \text{independent of } i, \tag{5}$$

and symmetrically along columns.

3.1 An identity internal to each side

Lemma 10. *$P' = Q'$, and therefore for each i*

$$\prod_{k\neq i}(u_i - u_k) = \sum_j \prod_{l\neq j}(u_i - v_l) = d\sum_j (u_i - v_j)^{-1},$$

with the symmetric statement along the other side.

Proof. P and Q differ by a constant, so their derivatives agree. The left member is $P'(u_i)$; the right one is $Q'(u_i)$, and $\prod_{l\neq j}(u_i - v_l) = d/(u_i - v_j)$ because $\prod_l (u_i - v_l) = Q(u_i) = d$. □

Corollary 11. *For each i,*

$$\sum_{k\neq i} v_2(a_i^2 - a_k^2) \;\geq\; v_2(C) - \max_j v_2(a_i^2 - b_j^2),$$

with equality whenever that maximum is attained at a single j.

Proof. By Lemma 10, the left-hand side equals $v_2(C) + v_2\big(\sum_j (u_i - v_j)^{-1}\big)$. Each term of the sum has valuation $-v_2(u_i - v_j) \geq -\max_j v_2(u_i - v_j)$, with equality for a single term when the maximum is attained once; the ultrametric inequality gives the claim. □

3.2 The vanishing of R

Theorem 12. *Let a symmetric ideal solution of even size satisfy $R = 0$, so that $v_2(C) = 3k_0$, and assume $k_0 \geq 4$. Then $k_0 \equiv 0 \pmod 4$.*

Proof. By (5) every $\xi_i - \eta_j$ is odd, so the family (ξ_i) and the family (η_j) have opposite parities; in particular $\xi_i - \xi_k$ is even for all $i \neq k$. Separating the terms of $D_i = \sum_{k\neq i} v_2(u_i - u_k)$ at an odd index i, the even entries contribute 0 and each other odd entry contributes $3 + v_2(\xi_i - \xi_k) \geq 4$, so

$$D_i \;\geq\; 4(k_0 - 1) \;\geq\; 3k_0 = v_2(C) \qquad (k_0 \geq 4).$$

By Lemma 10, $D_i = v_2(C) + v_2\big(\sum_j (u_i - v_j)^{-1}\big)$, whence $v_2\big(\sum_j (u_i - v_j)^{-1}\big) \geq 0$. In that sum the k_0 odd indices j contribute $\big(8(\xi_i - \eta_j)\big)^{-1}$ and the remaining ones contribute units of $\mathbb{Z}_2$; writing $S_i = \sum_{j\ \mathrm{odd}} (\xi_i - \eta_j)^{-1}$, the sum equals $\frac{1}{8}S_i$ plus an element of $\mathbb{Z}_2$, so $v_2(S_i) \geq 3$. The same argument along columns gives $v_2(S'_j) \geq 3$ with $S'_j = \sum_{i\ \mathrm{odd}} (\eta_j - \xi_i)^{-1}$.

Every odd element of $\mathbb{Z}_2$ is its own inverse modulo 8, so

$$S_i \equiv k_0\xi_i - \sum_j \eta_j, \qquad S'_j \equiv k_0\eta_j - \sum_i \xi_i \pmod 8.$$

Suppose $k_0 \equiv 2 \pmod 4$ and, first, that the ξ_i are even and the η_j odd. Writing $k_0 = 2\kappa$ with κ odd and $\xi_i = 2x_i$ we get $k_0\xi_i = 4\kappa x_i \equiv 4x_i \pmod 8$, so the row conditions force $\sum_j \eta_j \equiv 0 \pmod 4$. The column conditions force all $k_0\eta_j$ equal modulo 8; as $k_0 = 2\kappa$ with κ odd, all η_j are congruent modulo 4, say to $c \in \{1, 3\}$, whence $\sum_j \eta_j \equiv k_0 c \equiv 2c \equiv 2 \pmod 4$. This contradicts $\sum_j \eta_j \equiv 0 \pmod 4$. If instead the ξ_i are odd and the η_j even, the same computation with the roles of the two families exchanged gives the same contradiction. Hence $k_0 \not\equiv 2 \pmod 4$.

For k_0 odd the row conditions give $k_0\xi_i \equiv \sum_j \eta_j \pmod 8$ for every i and the column conditions $k_0\eta_j \equiv \sum_i \xi_i \pmod 8$ for every j; as k_0 is invertible modulo 8, all η_j are congruent to one η modulo 8, so $\sum_j \eta_j \equiv k_0\eta$ and the rows give $\xi_i \equiv \eta \pmod 8$, contradicting the opposite parities. Hence $k_0 \equiv 0 \pmod 4$. □

For k_0 odd the conclusion $R \geq 1$ was already known on both branches of [6], by [6, Lemma 3.4] when $\sigma = \sigma'$ and by parity when the sums differ; the new content of Theorem 12 is the case $k_0 \equiv 2 \pmod 4$.

3.3 Proof of Theorem 2

The lower bound of [6, Theorem 5.1] at a given even n is the smallest value compatible with the necessary conditions listed there, minimised over the profiles with $\sigma = \sigma'$ and over the pairs with $\sigma \neq \sigma'$, the latter enumerated exhaustively thanks to the saturation lemma [6, Lemma 5.2]. Theorem 12 adds one condition: $R \geq 1$ whenever $k_0 \geq 4$ and $k_0 \equiv 2 \pmod 4$. Replaying the minimisation with this condition leaves $n = 8, 10, 12, 14, 16, 18$ unchanged at $8, 11, 12, 12, 16, 18$ and raises $n = 20$ from 18 to 19: at that size every configuration compatible with the value 18, on either branch, has $k_0 = 6$ and $R = 0$, and is now excluded (on the branch $\sigma = \sigma'$ these five profiles move to 21, since $R = 1$ and $R = 2$ are not realisable for $k_0 = 6$). The next compatible value on the branch $\sigma = \sigma'$ is 19, reached by the profile $(0, 0, 0, 0, 0, 1, 1, 1, 2, 3)$ with $k_0 = 5$ and $R = 4$, while the branch with distinct profiles does not descend below 20. □

4 Tables

n	Kleiman	[6]	this note
5	3	4	4
7	4	6	6
9	7	9	9
11	8	11	11
13	10	12	12
15	11	12	**14**

n	Kleiman	[6]	this note
8	4	8	8
10	7	11	11
12	8	12	12
14	10	12	12
16	11	16	16
18	15	18	18
20	16	18	**19**

5 Status and verification

Proved. Lemmas 3, 4, 5, 6, 8 and 10, formulas (1)–(5), Proposition 7, Corollary 11 and Theorem 12.

Verified. Theorems 1 and 2 rest, besides the statements above, on finite computations: an exhaustive digit-by-digit lifting for the three candidates at $n = 15$, and a replay of the bound minimisation of [6] for the even sizes. Both are carried out in the ancillary files, which are pure Python 3, with no dependency, and take no argument. The file `VERIF_PTE2ADIC_N15.py` replays the odd-size assertions and reports 36 PASS and 0 FAIL in about ten seconds; the file `VERIF_PTE2ADIC_N20.py` replays the even-size ones and reports 51 PASS and 0 FAIL in about twenty minutes, the case of distinct profiles being enumerated exhaustively, with all entries of the larger profile up to $s' + m + 3$. The identities of Sections 2 and 3 are checked on the known symmetric odd solutions of sizes $5, 7, 9, 11, 13$ and on the six symmetric even solutions of sizes $8, 10, 12$; the block criterion of Proposition 7 is checked against exhaustive enumeration of odd residues modulo a power of 2 for $m = 2, 3, 4, 5$; the congruences in the proof of Theorem 12 are checked by exhaustive enumeration modulo 8 for $k_0 = 2, \ldots, 6$; and the bound engine for the even sizes is checked to return the values of [6] before the new condition is added.

Open. At $n = 13$ two candidate profiles remain at $t = 11$, namely $w = 8$ with profiles $(7, 1, 1, 1, 1)$ and $(5, 2, 2, 1, 1)$, so the bound there stays $v_2(C) \geq 12$; the smallest valuation

realised by a known 2-adic witness at that size is 17 [6]. Whether $R = 0$ can occur at all for $k_0 \equiv 0 \pmod 4$ is not settled here.

Credits

The germ of the finite-difference lemma for the odd sizes is a congruence modulo 16 of Filaseta and Markovich [3]. The construction of 2-adic ideal solutions by successive lifting, for $3 \leq n \leq 8$, is due to Joseph Foster, in his 2021 dissertation [4]. The near-solutions of size 11 used as 2-adic witnesses in [6] are those of Coppersmith, Mossinghoff, Scheinerman and VanderKam [2]. The sizes 10 and 12 were treated by Bera and Nair [1]. The bound $v_2(C) \geq v_2((n-1)!)$ is Kleiman's [5]. A first version of this note is dated 19 October 2026. Technical assistance: Claude (Anthropic).

References

[1] R. Bera and S. G. Nair, *Newton polygons and the constant associated with the Prouhet–Tarry–Escott problem*, Acta Arith. **213** (2024), 75–95.

[2] D. Coppersmith, M. J. Mossinghoff, D. Scheinerman and J. M. VanderKam, *Ideal solutions in the Prouhet–Tarry–Escott problem*, preprint, arXiv:2304.11254.

[3] M. Filaseta and M. Markovich, *Newton polygons and the Prouhet–Tarry–Escott problem*, J. Number Theory **174** (2017), 384–400.

[4] J. C. Foster, *Polynomials, primes and the PTE problem*, Ph.D. thesis, University of South Carolina, 2021.

[5] H. Kleiman, *A note on the Tarry–Escott problem*, J. Reine Angew. Math. **278/279** (1975), 48–51.

[6] D. Niedbala Giraudin, *The 2-adic valuation of the constant for symmetric ideal Prouhet–Tarry–Escott solutions*, preprint, hexagon:2611.00057 (2026).