hexagon:2611.00057v1

The 2-adic valuation of the constant for symmetric ideal Prouhet–Tarry–Escott solutions

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, let C denote the associated constant, and let $\overline{C_n}$ be the greatest common divisor of these constants. Filaseta and Markovich obtained $v_2(\overline{C_8}) \geq 6$ and determined $v_2(\overline{C_9}) = 9$, and asked for improved lower bounds in the range $10 \leq n \leq 12$; Bera and Nair gave bounds for $n = 10$ and $n = 12$. We treat the symmetric case at every size, even and odd, by 2-adic arguments throughout. A single identity, the row law, governs both parities. For n even, over $\mathbb{Z}$, it splits into two regular systems and yields $v_2(C) \geq 6, 8, 11, 12, 12, 16, 18, 18$ for $n = 6, 8, 10, \ldots, 20$. The values at $n = 6, 8, 10, 12$ are attained and hence exact for the symmetric constant: in the symmetric case this closes both brackets of Bera–Nair, and gives $v_2(C'_8) = 8$, for which the published information was $v_2(\overline{C_8}) \geq 6$. We also record that the two lower bounds of Bera–Nair, 9 at $n = 10$ and 11 at $n = 12$, are attained by 2-adic solutions symmetric about $-1/2$, so that no argument using 2-adic information alone can raise them. For n odd, over $\mathbb{Z}_2$, it combines with a finite-difference lemma refining a congruence of Filaseta–Markovich to give $v_2(C) \geq 11, 12, 12$ for $n = 11, 13, 15$, against 8, 10 and 11 from Kleiman's bound $(n-1)! \mid C$; the chain also reproduces the known values $4, 6, 9$ at $n = 5, 7, 9$. At $n = 11$ the bound is sharp: the two quadratic near-solutions of Coppersmith, Mossinghoff, Scheinerman and VanderKam are symmetric ideal solutions over $\mathbb{Z}_2$ with $v_2(C) = 11$, since in both of the real quadratic fields involved the prime 2 splits. This answers, for $n = 11$ and $p = 2$, two questions of Filaseta–Markovich, and exhibits for those sizes the case $p \leq n$ of the question closing Rees–Smyth, who construct p-adic ideal solutions only for $p > n$: at the prime 2 there is no local obstruction at these sizes. At $n = 13$ we exhibit a symmetric ideal solution over $\mathbb{Z}_2$, obtained from a second object of the same authors, although its constant has valuation 17.

1 Introduction

For a positive integer n, the Prouhet–Tarry–Escott problem asks for two distinct multisets A, B of n integers with $\sum_{a \in A} a^k = \sum_{b \in B} b^k$ for $1 \leq k \leq n-1$. Such a pair is called an *ideal* solution, and

$$\prod_{a \in A} (X - a) \; - \; \prod_{b \in B} (X - b) \; = \; C$$

is then a nonzero constant. Writing $\overline{C_n}$ for the greatest common divisor of the constants C over all ideal solutions of size n, Kleiman [11] showed $(n-1)! \mid \overline{C_n}$, and Rees and Smyth [15], Caley [4, 5], and others added further prime divisors. Filaseta and Markovich [8], developing the master's thesis [14], used Newton polygons to obtain $v_2(\overline{C_8}) \geq 6$ and $v_2(\overline{C_9}) = 9$, and remarked that improved lower bounds for $10 \leq n \leq 12$ would be of interest. Bera and Nair [1] treated $n = 10$ and $n = 12$.

A solution is *symmetric* when $A = -A$ and $B = -B$ for n even, and when $B = -A$ after translation for n odd. We write C'_n for the greatest common divisor of the constants over the symmetric ideal solutions of size n, so that $\overline{C_n} \mid C'_n$.

All the arguments below are 2-adic, but the two parities are not stated over the same ring, and it is worth saying at once why. For n odd everything is carried out over $\mathbb{Z}_2$ itself, so the results there bound the valuation for 2-adic solutions and a fortiori for integer ones. For n even the solutions are taken with entries in $\mathbb{Z}$. The arguments are again purely 2-adic, but one step — the equality of the numbers of odd entries on the two sides, in Proposition 3.2 — needs to know that C is even, which over $\mathbb{Z}$ is given by Kleiman's bound and which a 2-adic solution of even size need not satisfy. The even-size results therefore extend verbatim to any symmetric ideal solution over $\mathbb{Z}_2$ of even size whose constant is even, but not beyond. Throughout, $v = v_2$ denotes the 2-adic valuation.

The prime 2 is the one the classical local theory does not reach. Rees and Smyth lift a solution modulo p^k to one modulo p^{k+1}, and so obtain a p-adic ideal solution with $C \neq 0$ for every $p > n$ [15, Prop. 5.3 and Corollary]; their lifting requires the solution multiset to contain n distinct residues modulo p, of which there are only two when $p = 2$. Nothing in that direction constrains $v_2(C)$, which is why the 2-adic case has to be treated by hand. Their paper closes by asking whether the corollary also holds for $p \leq n$, so that there would be no local obstruction at any prime; the 2-adic solutions of Sections 10 and 11 answer that for $p = 2$ at the sizes 11 and 13, where no integer solution is known.

The two parities are governed by one identity, the row law of Section 2: if $f - g$ is a nonzero constant and β is a root of g, then $f(\beta)$ is that constant, so the valuations of the differences between β and the roots of f sum to $v(C)$ — and this holds for each root separately, not merely on average. What the two parities do with it differs, and the paper is organised accordingly: Sections 3–5 treat n even, Sections 6–11 treat n odd.

Theorem 1.1. *Let A be a symmetric ideal solution of size n with constant C, with entries in $\mathbb{Z}$ if n is even and in $\mathbb{Z}_2$ if n is odd. Then*

n	6	8	10	12	14	16	18	20
$v(C) \geq$	6	8	11	12	12	16	18	18

n	5	7	9	11	13	15
$v(C) \geq$	4	6	9	11	12	12

The bounds at $n = 5, 6, 7, 8, 9, 10, 11, 12$ are attained, and those at $n = 5, 7, 9$ are the known values of $v_2(\overline{C_n})$ [15, 4, 8].

At $n = 10$ and $n = 12$ the bounds are attained by integer solutions, so $v_2(C'_{10}) = 11$ and $v_2(C'_{12}) = 12$ exactly; these close the two brackets of Bera–Nair in the symmetric case. At $n = 11$ the bound is attained only over $\mathbb{Z}_2$, by objects already in the literature:

Theorem 1.2. *For $n = 11$ the bound is attained. Consequently*

$$\min\{v(C) : A \text{ a symmetric ideal solution over } \mathbb{Z}_2 \text{ of size } 11\} = 11.$$

The witnesses are not new objects: they are the two near-solutions of size 11 exhibited by Coppersmith, Mossinghoff, Scheinerman and VanderKam, each consisting of nine rational integers together with a conjugate pair of quadratic irrationalities. What is observed here is that both lie in $\mathbb{Z}_2$ (Section 10).

2 The row law

Proposition 2.1 (row law)**.** *Let $f = \prod_{i=1}^{N}(X - \alpha_i)$ and $g = \prod_{j=1}^{N}(X - \beta_j)$ be monic of the same degree over $\mathbb{Z}_2$, with $f - g = C$ a nonzero constant. Then for every j,*

$$\prod_{i=1}^{N}(\beta_j - \alpha_i) = C, \qquad \text{hence} \qquad \sum_{i=1}^{N} v(\beta_j - \alpha_i) = v(C),$$

and symmetrically $\prod_j(\alpha_i - \beta_j) = -C$ for every i.

Proof. Evaluating $f - g = C$ at $X = \beta_j$ gives $f(\beta_j) - 0 = C$, and $f(\beta_j) = \prod_i(\beta_j - \alpha_i)$. Evaluating at $X = \alpha_i$ gives $0 - g(\alpha_i) = C$, and $g(\alpha_i) = \prod_j(\alpha_i - \beta_j)$. □

This evaluation is the one used by Rees–Smyth [15] and by Coppersmith–Mossinghoff–Scheinerman–VanderKam [7]; what is used below is its refinement at the level of valuations, namely that the N sums $\sum_i v(\beta_j - \alpha_i)$ are all equal, and likewise the N sums taken the other way.

3 Even sizes: reduction to squares and the two regular systems

Let $n = 2r$ be even and let $A = \pm\{a_1, \dots, a_r\}$, $B = \pm\{b_1, \dots, b_r\}$ be a symmetric ideal solution with entries in $\mathbb{Z}$.

Proposition 3.1. *Put $\alpha_i = a_i^2$ and $\beta_j = b_j^2$. Then $\{\alpha_i\}$ and $\{\beta_j\}$ form an ideal solution of size r, all of whose entries are squares, and*

$$C = (-1)^r\Big(\prod_{i=1}^{r}\alpha_i - \prod_{j=1}^{r}\beta_j\Big), \qquad \text{so} \qquad v(C) = v\Big(\prod_i \alpha_i - \prod_j \beta_j\Big).$$

Proof. The odd power sums of A and of B vanish by symmetry. For $1 \le k \le r-1$ the power sums of order $2k$ agree, and $\sum_i a_i^{2k} = \frac{1}{2}\sum_{a\in A} a^{2k}$, so the families of squares have equal power sums up to order $r-1$. Finally $\prod_{a\in A}(X - a) = \prod_i(X^2 - \alpha_i)$ and likewise for B, and the constant is read at $X = 0$. □

We write σ and σ' for the multisets $\{v(a_i)\}$ and $\{v(b_j)\}$, so that $v(\alpha_i) = 2v(a_i)$ and $v(\beta_j) = 2v(b_j)$. In the ancillary verifier these two profiles are printed σ and τ; the letter τ is reserved here for a scalar attached to the odd case (Section 7).

Proposition 3.2. *Let k_0 be the number of odd entries among $a_1, \dots, a_r$ and k_0' the number among $b_1, \dots, b_r$. Then $k_0 = k_0'$, and the row law splits into two independent systems: a $k_0 \times k_0$ matrix on the odd parts and an $(r - k_0) \times (r - k_0)$ matrix on the even parts, each with all row sums and all column sums equal to $v(C)$.*

Proof. If α_i is odd and β_j even, or the reverse, then $\beta_j - \alpha_i$ is odd and contributes 0. So for β_j odd the row law reads $\sum_{\alpha_i \text{ odd}} v(\beta_j - \alpha_i) = v(C)$, and symmetrically. Let M be the matrix of these valuations, with k_0' rows and k_0 columns. Summing its entries in the two possible orders gives $k_0'\, v(C) = k_0\, v(C)$, and $v(C) \neq 0$ because $(n-1)!$ divides C by Kleiman's theorem and $n \ge 4$; hence $k_0 = k_0'$. The same argument applies to the even parts. □

Corollary 3.3. *$v(C) = 3k_0 + R$ with $R \geq 0$. In particular $v(C) \geq 3k_0$, and if every entry is odd then $v(C) \geq 3r$.*

Proof. Odd squares are congruent to 1 modulo 8, so each of the k_0 entries of a row of the odd system is at least 3; write R for the total excess of that row over $3k_0$. □

Not every value of R occurs. For a given k_0 the realisable values form a set with gaps, determined by the possible valuations of differences of odd squares; it is computed by a finite check in the ancillary verifier, which also confirms directly, modulo 8, that $R = 1$ cannot occur for $k_0 = 3$, and that $R = 2$ can, consistently with the second solution of Borwein, Lisoněk and Percival.

Lemma 3.4. *Suppose $\sigma = \sigma'$. Then $v(C) \geq 2\sum\sigma + 3$; and if moreover k_0 is odd, then $R \geq 1$.*

Proof. Write $\alpha_i = 2^{2\sigma_i}u_i$ and $\beta_j = 2^{2\sigma'_j}u'_j$ with u_i, u'_j odd squares (an entry 0 cannot occur on both sides, since then C would vanish by Proposition 2.1, and with $\sigma = \sigma'$ it occurs on neither). Then $\prod_i \alpha_i - \prod_j \beta_j = 2^{2\sum\sigma}\bigl(\prod_i u_i - \prod_j u'_j\bigr)$, and both products are congruent to 1 modulo 8; this gives the first claim.

For the second, suppose $R = 0$. Then every entry of the odd system equals 3, that is $\beta_j - \alpha_i \equiv 8 \pmod{16}$ for all odd α_i, β_j. Hence all the odd α_i are congruent to one residue X modulo 16 and all the odd β_j to $X + 8$. Since $r \geq 2$, the first power sums of the two families agree (Proposition 3.1). Modulo 16, an even α_i is $\equiv 4$ if $\sigma_i = 1$ and $\equiv 0$ if $\sigma_i \geq 2$, and likewise for the β_j; as $\sigma = \sigma'$, the even entries contribute the same amount on both sides. The odd entries contribute k_0X and $k_0(X + 8)$, which differ by $8k_0 \equiv 8 \pmod{16}$ for k_0 odd, a contradiction. □

Finally, if $k_0 = 0$ then every entry is even, and $A/2$, $B/2$ is again a symmetric ideal solution with entries in $\mathbb{Z}$, whose constant is $C/2^n$. Iterating, every lower bound below that holds when $k_0 \geq 1$ holds a fortiori when $k_0 = 0$, since it then holds for $C/2^n$ and $v(C) = n + v(C/2^n)$. We may and do assume $k_0 \geq 1$, that is $\min\sigma = \min\sigma' = 0$.

4 Even sizes: three instruments

4.1 The index bound

For integers $s, t \geq 0$ put $\psi(s, t) = 2\min(s, t)$ if $s \neq t$, and $\psi(s, s) = 2s + 3$.

Lemma 4.1. *If $v(a) = s$ and $v(b) = t$ then $v(a^2 - b^2) \geq \psi(s, t)$, with equality when $s \neq t$.*

Proof. If $s \neq t$ then $v(a^2) = 2s \neq 2t = v(b^2)$ and the valuation of the difference is the smaller of the two. If $s = t$, write $a = 2^s x$ and $b = 2^s y$ with x, y odd; then $a^2 - b^2 = 2^{2s}(x - y)(x + y)$, and of the two factors $x \mp y$ one is congruent to 2 modulo 4 and the other divisible by 4, so the valuation is at least $2s + 3$. □

Theorem 4.2. *$v(C) \geq \max_j \sum_{i=1}^{r} \psi(\sigma_i, \sigma'_j)$, and symmetrically with the roles of the two families exchanged.*

Proof. Immediate from Proposition 2.1 applied at β_j and Lemma 4.1. □

On the five symmetric ideal solutions of sizes 10 and 12 considered here this bound is tight in exactly three cases: it returns 14 for the first solution of Borwein, Lisoněk and Percival [2], 12 for that of Kuosa, Meyrignac and Shuwen [12], and 12 for that of Choudhry and Wróblewski [6], which are their exact values; on the second solution of Borwein, Lisoněk and Percival it returns 9 against the true value 11, and on that of Broadhurst [3] 13 against 14.

4.2 Rigidity of the Newton polygon

Theorem 4.3. *In a symmetric ideal solution of even size, either $\sigma = \sigma'$ as multisets, or $v(C) = 2\min\big(\sum\sigma, \sum\sigma'\big)$.*

Proof. The elementary symmetric functions of order at most $r-1$ of $\{\alpha_i\}$ and of $\{\beta_j\}$ coincide, by Proposition 3.1; only the constant terms may differ. Hence the Newton polygons of the two monic polynomials are lower convex hulls of the same points, except the point of abscissa 0. If the two constant terms have the same valuation, the polygons coincide, and so do the multisets of valuations of the roots, that is $2\sigma = 2\sigma'$. Otherwise the valuation of the difference is the smaller of the two constant-term valuations, namely $2\min(\sum\sigma, \sum\sigma')$. □

4.3 The predictor

Proposition 4.4. *For a half-family of profile σ, let $T_j(\sigma)$ be the sum of the j smallest entries of σ and $N_j(\sigma)$ the number of j-element sub-multisets realising that minimum. Then*

$$v(e_j) = 2\,T_j(\sigma) + v\big(N_j(\sigma)\big),$$

where e_j is the j-th elementary symmetric function of the squares, provided $N_j(\sigma)$ is not divisible by 8 and $v(N_j(\sigma))$ is smaller than twice the gap between T_j and the next attainable weight.

Proof. Write $\alpha_i = 2^{2\sigma_i}u_i$ with u_i an odd square, so that each j-element sub-multiset contributes $2^{2W}\prod u_i$ with W its weight, and $\prod u_i \equiv 1 \pmod 8$ as a product of odd squares. The N_j sub-multisets of minimal weight therefore contribute $2^{2T_j}(N_j + 8k)$ for some k, of valuation $2T_j + v(N_j)$ as soon as $8 \nmid N_j$. Every other sub-multiset has weight at least $T_j + g$, where g is the gap to the next attainable weight, hence valuation at least $2T_j + 2g$, which exceeds $2T_j + v(N_j)$ under the second proviso. □

This predictor is exact, at every order j, on the twelve half-solutions of the six even solutions of sizes 8, 10 and 12 checked in the first ancillary file.

5 Even sizes: the main theorem and the extremal configurations

Theorem 5.1. *For every symmetric ideal solution of even size n with entries in $\mathbb{Z}$, the valuation of the constant satisfies the bounds below. At $n = 6, 8, 10, 12$ the bounds are*

attained, hence exact for C'_n.

n	*Kleiman*	*previously*	*here*	*gain*	*status*
6	3	—	6	+3	*exact*
8	4	≥ 6 *(Filaseta–Markovich)*	8	+4	*exact*
10	7	9 *to* 11 *(Bera–Nair)*	11	+4	*exact*
12	8	11 *to* 12 *(Bera–Nair)*	12	+4	*exact*
14	10	—	12	+2	*lower bound*
16	11	—	16	+5	*lower bound*
18	15	—	18	+3	*lower bound*
20	16	—	18	+2	*lower bound*

Proof. By the reduction following Lemma 3.4 we may assume $\min\sigma = \min\sigma' = 0$, and by Theorem 4.3 there are two cases.

Case $\sigma = \sigma'$. Then $v(C)$ is at least the bound of Theorem 4.2, at least $2\sum\sigma + 3$, and of the form $3k_0 + R$ with R in the set of values realisable for k_0 (Corollary 3.3), with $R \geq 1$ when k_0 is odd (Lemma 3.4). An entry equal to 9 or more gives $v(C) \geq \psi(9,9) = 21$ by Theorem 4.2, beyond every bound of the table, so it suffices to enumerate the profiles with entries at most 8 and to take, for each, the least value of $v(C)$ compatible with these conditions.

Case $\sigma \neq \sigma'$. Let σ' denote the profile of smaller sum and put $s' = \sum\sigma'$, so that $v(C) = 2s'$. Since $v(C) = 3k_0 + R$ is then even, $R = 0$ is impossible for k_0 odd. The pair must satisfy the following necessary conditions:

(a) Theorem 4.2, with the roles of the two families in both orders;

(b) $v(C) = 3k_0 + R$ with R realisable for k_0;

(c) compatibility of the predictor: since e_j is the same for the two families for $1 \leq j \leq r-1$, whenever Proposition 4.4 determines $v(e_j)$ for both profiles the two values agree, and whenever it determines it for one profile but not for the other, that value is at least $2T_j + \min(3, 2g)$ computed for the other profile, which by the proof of Proposition 4.4 is a lower bound for $v(e_j)$ whenever the predictor does not determine it.

For a value B of the table, $2s' \leq B$ bounds the entries of σ'. The entries of σ are not bounded a priori (an entry $a_i = 0$ counts as an infinite entry), but by Lemma 5.2 below it suffices to enumerate the profiles σ whose entries are at most $s' + r + 3$.

Both enumerations are finite; they are carried out in the ancillary files for the eight sizes $6 \leq n \leq 20$, and the minimum over the two cases is the bound of the table. □

Lemma 5.2. *Let* $\sigma \neq \sigma'$ *with* $s' = \sum\sigma' < \sum\sigma$. *There is an integer* c *with* $s'+1 \leq c \leq s'+r+1$ *such that no entry of* σ *equals* $c+1$. *Let* σ^* *be obtained from* σ *by replacing every entry larger than* c *by* $c+2$. *Then* σ^* *has entries at most* $s'+r+3$, *and the pair* (σ^*, σ') *satisfies each of the conditions* (a), (b), (c) *if and only if* (σ, σ') *does.*

Proof. The $r+1$ values $s'+2, \ldots, s'+r+2$ cannot all be entries of σ, which has r entries; this gives c. Call the entries larger than c *large*; they are at least $c+2$, and the other entries are at most c. Every entry of σ' is at most $s' < c$.

(a) For $x > \max\sigma'$ one has $\psi(x,t) = 2t$ for every entry t of σ', so the row and column sums of Theorem 4.2 do not depend on the value of a large entry.

(b) The number k_0 of zero entries and the value $v(C) = 2s'$ are unchanged.

(c) Let p be the number of entries at most c. For $j \le p$, the j smallest entries, T_j and N_j do not involve the large entries. The next attainable weight is either reached without large entries, which does not depend on them, or by exchanging a chosen entry, at most c, for a large one, which raises the weight by at least 2. As the predictor depends on the gap g only through $\min(3, 2g)$ and through the comparison of $v(N_j) \le 2$ with $2g$ (when $8 \nmid N_j$), its output is the same for σ and σ^*. For $j > p$, every j-element sub-multiset of σ or of σ^* contains a large entry, so $T_j \ge c + 2 \ge s' + 3$ and the value or lower bound given by the predictor is at least $2s' + 6$; for σ' it is at most $2T_j(\sigma') + 3 \le 2s' + 3$. Hence, for both σ and σ^*, the order j is incompatible exactly when the predictor determines $v(e_j)$ for σ', a condition that does not involve σ. □

The two smallest even sizes are not new, and serve as a calibration. At $n = 6$ the bound returned is 6, and it is attained by $\pm\{0, 7, 7\}$ against $\pm\{3, 5, 8\}$, whose constant is $14400 = 2^6 \cdot 225$. At $n = 8$ the bound is 8, and it is attained by equation (4.7) of [15], so that $v_2(C'_8) = 8$; we have not found this exact value stated, the published information being $v_2(\overline{C_8}) \ge 6$ from [8].

The value 11 at $n = 10$ is attained already by the solution recorded as equation (4.9) of [15], which goes back to Letac and is recorded by Gloden [10], and again by the second solution of Borwein, Lisoněk and Percival; the value 12 at $n = 12$ by that of Kuosa, Meyrignac and Shuwen [12] as well as by that of Choudhry and Wróblewski. Both brackets of Bera–Nair therefore close in the symmetric case. Since every ideal solution known at these two sizes is symmetric, a smaller value for $\overline{C_n}$ would require a *non-symmetric* ideal solution of size 10 or 12, and none is known.

In the case $\sigma \ne \sigma'$, the enumeration shows that every pair compatible with the bound has its two profiles equal in every entry but the largest, the largest entry of σ taking every value from some threshold on. This is an observation from the computation, not a consequence of Theorem 4.3. We call such a one-parameter family a *form*.

Theorem 5.3. *The enumeration yields more than a lower bound: the exhaustive list of the profiles that the necessary conditions above do not exclude at the bound. Any symmetric ideal solution attaining the bound has one of these profiles.*

n	*profiles $\sigma = \sigma'$ compatible with the bound*	*forms with $\sigma \ne \sigma'$*
10	$(0,0,0,1,1)$, $(0,0,0,1,2)$, $(0,0,0,1,3)$	0
12	$(0,0,0,0,1,1)$, $(0,0,0,0,1,2)$, $(0,0,0,0,1,3)$, $(0,0,0,1,1,2)$	3
14	$(0,0,0,0,1,1,2)$	1
16	*none*	1
18	*fourteen profiles*	6
20	*five profiles*	2

Three consequences deserve to be recorded. At size 10 the case of distinct profiles produces nothing at or below the bound, so any symmetric ideal solution of size 10 attaining 11 has two half-families of the *same* profile, which the solution of Borwein, Lisoněk and Percival confirms. At size 16 no profile with $\sigma = \sigma'$ descends below 17: if the two half-families have the same profile then $v(C) \ge 17$, and the value 16 can only be attained in the single form

$$\sigma' = (0,0,0,0,1,1,2,4), \qquad \sigma = (0,0,0,0,1,1,2,\Lambda), \qquad \Lambda \ge 5.$$

At size 14 the profile is *unique* in the case $\sigma = \sigma'$, namely $(0,0,0,0,1,1,2)$, and the one form with distinct profiles is $\sigma' = (0,0,0,0,1,1,4)$ against $\sigma = (0,0,0,0,1,1,\Lambda)$ with $\Lambda \ge 5$; at a size where no solution is known, this is a completely explicit search criterion.

6 Odd sizes: a finite-difference lemma

Definition 6.1. Let $n \geq 5$ be odd. A *symmetric ideal solution over $\mathbb{Z}_2$ of size n* is a tuple $A = (a_1, \ldots, a_n) \in \mathbb{Z}_2^n$ such that

$$p_k(A) := \sum_{i=1}^{n} a_i^k = 0 \qquad \text{for every odd } k \text{ with } 1 \leq k \leq n-2,$$

and such that $C(A) := -2\prod_{i=1}^{n} a_i$ is nonzero.

Equivalently, with $f(X) = \prod_i (X - a_i)$ one has $f(X) + f(-X) = C(A)$. Indeed $\prod_i (X + a_i) = -f(-X)$ because n is odd, so $\prod_i (X - a_i) - \prod_i (X + a_i) = f(X) + f(-X)$, which is twice the sum of the terms of f of even degree. As n is odd those are the terms $(-1)^k e_k(A) X^{n-k}$ with k odd, and they reduce to the single term $-e_n(A)$ precisely when $e_1 = e_3 = \cdots = e_{n-2} = 0$. If $(A, -A)$ is a symmetric ideal PTE solution over $\mathbb{Z}$, then A is a symmetric ideal solution over $\mathbb{Z}_2$ in the above sense, with the same constant.

We write

$$t(A) := \sum_{i=1}^{n} v(a_i),$$

let O and E be the sets of indices with a_i odd, respectively even, and put

$$w := |O|, \qquad u := |E| = n - w, \qquad c_i := v(a_i)\ (i \in E), \qquad m_1 := \#\{i \in E :\ c_i = 1\}.$$

Proposition 6.2. $v(C) = 1 + t(A)$.

Proof. Immediate from $C = -2\prod a_i$. □

Corollary 6.3. *For every j, $\sum_{i=1}^{n} v(a_j + a_i) = v(C)$.*

Proof. Apply Proposition 2.1 with $f = \prod_i (X - a_i)$ and $g = \prod_i (X + a_i)$, whose roots are the $-a_i$. □

Lemma 6.4. *Let A be as in Definition 6.1 and let $0 \leq m \leq (n-3)/2$. Then*

$$\sum_{i=1}^{n} a_i \, (a_i^2 - 1)^m = 0,$$

and consequently

$$8^m \;\Big|\; \sum_{i \in E} a_i \, (a_i^2 - 1)^m \qquad \text{in } \mathbb{Z}_2.$$

Proof. Expanding, $a(a^2-1)^m = \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} a^{2j+1}$, so

$$\sum_i a_i (a_i^2 - 1)^m = \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} p_{2j+1}(A) = 0,$$

every exponent $2j+1$ being odd and at most $2m+1 \leq n-2$. For a odd one has $8 \mid a^2 - 1$, so each term with $i \in O$ is divisible by 8^m; the displayed divisibility follows. □

Remark 6.5. The corresponding statement of Filaseta–Markovich [8] is recorded there in the form of a congruence modulo 16 between the power sums of the odd parts, respectively of the even parts, of the two sides of a general ideal solution. Lemma 6.4 is a strengthening: instead of one fixed modulus it produces a tower of conditions modulo $8, 64, 512, 4096, \ldots$, indexed by m, and these are conditions on the even part alone.

Corollary 6.6. *w is even and u is odd.*

Proof. $p_1(A) = 0$; reducing modulo 2 gives $w \equiv 0$. □

Corollary 6.7. *Let $c_{\min} = \min\{c_i : i \in E\}$ and let μ denote its multiplicity. If μ is odd then $c_{\min} \geq 3 \cdot \frac{n-3}{2}$.*

Proof. In $\sum_{i\in E} a_i(a_i^2-1)^m$ each term has valuation exactly c_i, since a_i is even and a_i^2-1 is odd. The μ terms with $c_i = c_{\min}$ are each $2^{c_{\min}}$ times an odd number, so, μ being odd, their sum is again $2^{c_{\min}}$ times an odd number, while every other term has valuation greater than $c_{\min}$. Hence the whole sum has valuation exactly $c_{\min}$, and Lemma 6.4 with $m = (n-3)/2$ gives $3m \leq c_{\min}$. □

Corollary 6.8. *The number m_1 is even; and if $u = 1$ then $t \geq 3 \cdot \frac{n-3}{2}$.*

Proof. If $m_1 \geq 1$ then $c_{\min} = 1$, and $1 < 3(n-3)/2$ for $n \geq 5$, so $\mu = m_1$ is even by Corollary 6.7; if $m_1 = 0$ there is nothing to prove. If $u = 1$ then $\mu = 1$ is odd and $t = c_{\min}$. □

Lemma 6.9. *Put $s := \max\{\min(2 + v(k-1),\, k) \;:\; k \text{ odd},\ 3 \leq k \leq n-2\}$. Then*

$$\sum_{i\in O} a_i \equiv 0 \pmod{2^s}.$$

One has $s \geq 3$ for $n \geq 5$, $s \geq 4$ for $n \geq 7$ and $s \geq 5$ for $n \geq 11$.

Proof. Fix such a k. For a odd and $M = k-1$ even, the lifting-the-exponent formula gives $v(a^M - 1) = v(a-1) + v(a+1) + v(M) - 1 \geq 2 + v(M)$, since one of $a \mp 1$ is divisible by 4. Hence $a^k \equiv a \pmod{2^{2+v(k-1)}}$ for a odd, while $v(a^k) \geq k$ for a even. Reducing $p_k(A) = 0$ modulo $2^{\min(2+v(k-1),k)}$ leaves $\sum_{i\in O} a_i$. Taking the largest such modulus over the admissible k gives the claim; the stated values come from $k = 3, 5, 9$. □

7 Odd sizes: the odd part

Proposition 7.1. *For every $j \in O$,*

$$\sum_{i\in O,\ i\neq j} v(a_j + a_i) = t.$$

In particular $t \geq w - 1$, and $\tau := t - (w-1) \geq 0$ does not depend on j.

Proof. Apply Corollary 6.3 at $j \in O$. For $i \in E$ the sum $a_j + a_i$ is odd, so those terms vanish; the term $i = j$ equals $v(2a_j) = 1$. By Proposition 6.2 the total is $1 + t$. □

If $a_i \equiv a_j \pmod 4$ with both odd then $a_i + a_j \equiv 2 \pmod 4$, so $v(a_i + a_j) = 1$ exactly; if $a_i \not\equiv a_j \pmod 4$ then $v(a_i + a_j) \geq 2$. Let $A_{(1)}$ and $A_{(3)}$ denote the elements of O congruent to 1, respectively 3, modulo 4. Then for $j \in A_{(1)}$,

$$\tau = \sum_{i\in A_{(3)}} \big(v(a_i + a_j) - 1\big),$$

and symmetrically for $j \in A_{(3)}$.

Proposition 7.2. *Assume $w \geq 2$, let $h := w/2$ and let s be as in Lemma 6.9, so $s \geq 3$. Exactly one of the following holds.*

(i) $\tau = 0$; *then* O *lies in a single class modulo* 4 *and* $w \equiv 0 \pmod 4$.

(ii) $\tau = h$; *then* h *is even, hence again* $w \equiv 0 \pmod 4$.

(iii) $\tau \geq h + \lceil h/2 \rceil$.

Moreover if $w = 2$ *then* (i) *and* (ii) *are impossible and* $\tau \geq s - 1$.

Proof. Suppose first $\tau = 0$. Then no pair of elements of O lies in distinct classes modulo 4, so one of $A_{(1)}, A_{(3)}$ is empty and O is contained in a single class, say $\varepsilon \in \{1, 3\}$. Then $\sum_{i \in O} a_i \equiv w\varepsilon \pmod 4$, and Lemma 6.9 forces $4 \mid w\varepsilon$, i.e. $4 \mid w$.

Now suppose $\tau > 0$, so both classes are nonempty; write $p = |A_{(1)}|$, $q = |A_{(3)}|$ and let $M = (M_{ab})$ be the $p \times q$ matrix with entries $M_{ab} = v(a + b) - 1 \geq 1$ for $a \in A_{(1)}$, $b \in A_{(3)}$. By the displayed formula all row sums and all column sums of M equal τ. Counting the total two ways gives $p\tau = q\tau$, hence $p = q = h$. Since all entries are at least 1, $\tau \geq h$.

Assume $\tau = h$. Then every entry of M equals 1, i.e. $v(a + b) = 2$ for every cross pair, i.e. $a + b \not\equiv 0 \pmod 8$. Elements of $A_{(1)}$ are $\equiv 1$ or 5 modulo 8 and elements of $A_{(3)}$ are $\equiv 3$ or 7; the forbidden sums modulo 8 are exactly $(1, 7)$ and $(5, 3)$. If $A_{(1)}$ met both classes modulo 8, then $A_{(3)}$ could contain neither a 3 nor a 7, which is absurd. So $A_{(1)}$ is homogeneous modulo 8 and then so is $A_{(3)}$, the two possibilities being $(1, 3)$ and $(5, 7)$. In both cases $\sum_{i \in O} a_i \equiv 4h \pmod 8$, and Lemma 6.9 with $s \geq 3$ forces h even.

Finally assume $\tau > h$ and put $N = M - J$, where J is the all-ones matrix, so $N \geq 0$ with all line sums $\rho = \tau - h \geq 1$. One has $N_{ab} \geq 1$ exactly when $a + b \equiv 0 \pmod 8$, that is on the set $(A^1_{(1)} \times A^7_{(3)}) \cup (A^5_{(1)} \times A^3_{(3)})$, where the superscript records the class modulo 8. Write $\kappa = |A^1_{(1)}|$ and $\lambda = |A^3_{(3)}|$. A row of N indexed by an element of $A^1_{(1)}$ has at least $h - \lambda$ entries ≥ 1, whence $\rho \geq h - \lambda$ whenever $A^1_{(1)} \neq \emptyset$; similarly $\rho \geq \lambda$ if $A^5_{(1)} \neq \emptyset$, $\rho \geq h - \kappa$ if $A^3_{(3)} \neq \emptyset$, and $\rho \geq \kappa$ if $A^7_{(3)} \neq \emptyset$. If $0 < \kappa < h$ then $\rho \geq \max(h - \lambda, \lambda) \geq \lceil h/2 \rceil$. If $\kappa = h$ then $A^7_{(3)} \neq \emptyset$ (otherwise the support of N is empty and $\rho = 0$), so $\rho \geq h$; the case $\kappa = 0$ is symmetric. In all cases $\rho \geq \lceil h/2 \rceil$.

For $w = 2$ one has $h = 1$, so (i) fails because $2 \not\equiv 0 \pmod 4$ and (ii) fails because h is odd. Here $\sum_{i \in O} a_i = a_1 + a_2$ has valuation $\tau + 1$ by Proposition 7.1, so Lemma 6.9 gives $\tau + 1 \geq s$. □

8 Odd sizes: the even part

Proposition 8.1. *For every* $j \in E$,

$$\sum_{i \in E} v(a_i + a_j) = 1 + t.$$

Consequently, for every $j \in E$,

$$(c_j + 1) \; + \sum_{\substack{i \in E,\ i \neq j \\ c_i \neq c_j}} \min(c_i, c_j) \; + \sum_{\substack{i \in E,\ i \neq j \\ c_i = c_j}} (c_j + 1) \; \leq \; 1 + t, \tag{1}$$

and $t \geq u$ *when* $u \geq 2$.

Proof. Apply Corollary 6.3 at $j \in E$; the terms with $i \in O$ vanish. For $i \neq j$ one has $v(a_i + a_j) = \min(c_i, c_j)$ if $c_i \neq c_j$ and $v(a_i + a_j) \geq c_j + 1$ if $c_i = c_j$, while the term $i = j$ equals $c_j + 1$; this gives (1). Keeping only the bound $v(a_i + a_j) \geq 1$ for $i \neq j$ gives $1 + t \geq (c_j + 1) + (u - 1)$, i.e. $t \geq c_j + u - 1$; summing over $j \in E$ yields $ut \geq t + u(u - 1)$, hence $t \geq u$ for $u \geq 2$. □

Corollary 8.2. *Suppose $u \geq 3$ and $m_1 \geq 1$. Then $t \geq \max(m_1 + u - 1,\ 2u - m_1)$. If $m_1 = 0$ then $t \geq 2u$.*

Proof. Apply (1) to an index j with $c_j = 1$: the left-hand side equals $2 + 2(m_1 - 1) + (u - m_1) = m_1 + u$, giving $t \geq m_1 + u - 1$. On the other hand $t = \sum_i c_i \geq m_1 + 2(u - m_1) = 2u - m_1$. If $m_1 = 0$ then every $c_i \geq 2$. □

In particular, since m_1 is even by Corollary 6.8,

$$u = 5 \Rightarrow t \geq 8, \qquad u = 7 \Rightarrow t \geq 10, \qquad u = 9 \Rightarrow t \geq 14, \qquad u = 11 \Rightarrow t \geq 16.$$

We record one further structural statement, which is not used in the lower bounds below but sharpens the picture and subsumes Corollary 6.6.

Theorem 8.3. *In a symmetric ideal solution over $\mathbb{Z}_2$ of odd size n: the maximal valuation among $v(a_1), \ldots, v(a_n)$ is attained exactly once, and every other value is attained an even number of times.*

Proof. Let $M = \max_i v(a_i)$ and let i_0 be an index attaining it. Apply Corollary 6.3 at i_0. The term $i = i_0$ equals $v(2a_{i_0}) = 1 + M$, and for $i \neq i_0$ one has $v(a_{i_0} + a_i) \geq \min(M, v(a_i)) = v(a_i)$. Summing,

$$v(C) = \sum_i v(a_{i_0} + a_i) \ \geq \ 1 + M + \sum_{i \neq i_0} v(a_i) = 1 + t = v(C)$$

by Proposition 6.2, so every inequality is an equality: $v(a_{i_0} + a_i) = v(a_i)$ for all $i \neq i_0$. If some $k \neq i_0$ had $v(a_k) = M$, then $a_{i_0} + a_k$ would be the sum of two elements of the same valuation, whence $v(a_{i_0} + a_k) \geq M + 1 > v(a_k)$, a contradiction. So the maximum is attained exactly once.

For the second assertion, write $f(X) = XH(X^2) + c_0$ with H monic of degree $(n-1)/2$ and $C = 2c_0$, as in Definition 6.1. From $f(a_i) = 0$ one gets $a_i H(a_i^2) = -c_0$ and hence $a_i^2 H(a_i^2)^2 = c_0^2$, so each a_i^2 is a root of the monic polynomial $R(Y) = YH(Y)^2 - c_0^2$ of degree n. In fact $R(X^2) = -f(X)f(-X) = \prod_i (X^2 - a_i^2)$, since $f(-X) = -XH(X^2) + c_0$ and n is odd, so the roots of R are exactly the a_i^2 with multiplicity. Now R and $YH(Y)^2$ have the same coefficients in every degree from 1 to n and differ only in degree 0, so their Newton polygons share every vertex of abscissa at least 1. By the first assertion the largest valuation among the a_i^2, namely $2M$, is attained once, so the initial segment of the Newton polygon of R has length 1; the remaining $n - 1$ slopes are those of $YH(Y)^2$, that is the valuations of the roots of H, each occurring twice. Halving, every value other than M occurs an even number of times among the $v(a_i)$. □

Remark 8.4. Theorem 8.3 holds on the odd witnesses used in this paper: Letac's two solutions of size 9 [13] have full valuation profiles $(4, 1, 1, 1, 1, 0, 0, 0, 0)$ and $(3, 2, 2, 1, 1, 0, 0, 0, 0)$, the two quadratic objects of Section 10 have $(4, 2, 2, 1, 1, 0^6)$, and the solution of Section 11 has $(6, 3, 3, 1, 1, 1, 1, 0^6)$. In each case the maximum occurs once and every other value an even number of times. Taking the value 0, whose multiplicity is w, recovers Corollary 6.6.

9 Odd sizes: lower bounds

Lemma 9.1 (reduction)**.** *If A is a symmetric ideal solution over $\mathbb{Z}_2$ of size n with $w = 0$, then $A/2$ is one as well, and $t(A/2) = t(A) - n$. Consequently, in order to bound t from below it suffices to treat the case $w \geq 2$.*

Proof. If every a_i is even then $p_k(A/2) = 2^{-k}p_k(A) = 0$ and $C(A/2) = 2^{-n}C(A) \neq 0$. Given an arbitrary A, halving it repeatedly produces A' with $w(A') \geq 1$ and $t(A') \leq t(A)$; by Corollary 6.6, $w(A')$ is even, hence ≥ 2. □

9.1 The sizes $n = 5$ and $n = 7$

Proposition 9.2. *For $n = 5$ one has $t \geq 3$, and for $n = 7$ one has $t \geq 5$; hence $v(C) \geq 4$ and $v(C) \geq 6$ respectively. Both bounds are attained.*

Proof. Let $n = 5$, so $s = 3$ and $w \in \{2, 4\}$. If $w = 2$ then $u = 3$ and Corollary 8.2 with m_1 even gives $t \geq 4$. If $w = 4$ then $u = 1$ and Corollary 6.8 gives $t \geq 3 \cdot 1 = 3$.

Let $n = 7$, so $s = 4$ and $w \in \{2, 4, 6\}$. If $w = 2$ then $u = 5$ and Corollary 8.2 gives $t \geq 8$. If $w = 6$ then $u = 1$ and Corollary 6.8 gives $t \geq 6$. If $w = 4$ then $u = 3$, $h = 2$, and Corollary 8.2 gives $t \geq 4$; by Proposition 7.2 the possible values of τ are 0, 2 and $\tau \geq 3$, giving $t = 3 + \tau \in \{3, 5\} \cup [6, \infty)$, and $t = 3$ is excluded. Hence $t \geq 5$.

The tuples $(9, 5, 1, -7, -8)$ and $(-50, -38, -13, -7, 24, 33, 51)$ are symmetric ideal solutions over $\mathbb{Z}$ with $t = 3$ and $t = 5$, so $v(C) = 4$ and $v(C) = 6$. These are the known values of $v_2(\overline{C_5})$ [15, Prop. 2.4] and of $v_2(\overline{C_7})$, for which Caley proved $2^6 \mid \overline{C_7}$ [4]; see [7, §2.1]. □

9.2 The size $n = 9$

Theorem 9.3. *Let A be a symmetric ideal solution over $\mathbb{Z}_2$ of size 9. Then $t \geq 8$, hence $v(C) \geq 9$. The bound is attained.*

Proof. Here $s = 4$ and $(n - 3)/2 = 3$; by Lemma 9.1, $w \in \{2, 4, 6, 8\}$.

- $w = 2$, $u = 7$: Corollary 8.2 gives $t \geq 10$.
- $w = 4$, $u = 5$: Corollary 8.2 gives $t \geq 8$.
- $w = 6$, $u = 3$, $h = 3$: case (i) of Proposition 7.2 requires $4 \mid w$ and case (ii) requires h even, so (iii) holds and $\tau \geq 3 + 2 = 5$, whence $t = 5 + \tau \geq 10$.
- $w = 8$, $u = 1$: Corollary 6.8 gives $t \geq 3 \cdot 3 = 9$.

Thus $t \geq 8$. The first solution of Letac of size 9, namely

$$(-98, -82, -58, -34, 13, 16, 69, 75, 99),$$

has $w = 4$, $u = 5$ and even valuations $(4, 1, 1, 1, 1)$, so $t = 8$ and $v(C) = 9$. □

Theorem 9.3 recovers, for symmetric solutions, the value $v_2(\overline{C_9}) = 9$ obtained by Filaseta and Markovich by a different route, and shows in addition that the value cannot be improved by any 2-adic argument, since it is attained already over $\mathbb{Z}$.

9.3 The size $n = 11$

Proposition 9.4. *Let A be a symmetric ideal solution over $\mathbb{Z}_2$ of size 11 with $t \leq 9$. Then $w = 8$, $u = 3$, $\tau = 0$, $t = 7$, and the multiset of even valuations is $(5, 1, 1)$ or $(3, 2, 2)$. Writing a_2, a_3 for the two entries of equal valuation, one has $v(a_2 + a_3) = 5$ in the first case and $v(a_2 + a_3) = 3$ in the second.*

Proof. Here $s = 5$ and, by Lemma 9.1, $w \in \{2, 4, 6, 8, 10\}$.

- $w = 2$, $u = 9$: Corollary 8.2 gives $t \geq 14$.
- $w = 4$, $u = 7$: Corollary 8.2 gives $t \geq 10$.
- $w = 6$, $u = 5$, $h = 3$: cases (i) and (ii) of Proposition 7.2 are excluded ($4 \nmid 6$; h odd), so $\tau \geq 3 + 2 = 5$ and $t = 5 + \tau \geq 10$.
- $w = 10$, $u = 1$: Corollary 6.8 gives $t \geq 3 \cdot 4 = 12$.
- $w = 8$, $u = 3$, $h = 4$: Proposition 7.2 leaves $\tau = 0$, $\tau = 4$ or $\tau \geq 6$, that is $t = 7 + \tau \in \{7\} \cup \{11\} \cup [13, \infty)$.

So $t \leq 9$ forces $w = 8$, $u = 3$, $\tau = 0$ and $t = 7$. The multiset (c_1, c_2, c_3) is a partition of 7 into three positive parts: $(5,1,1)$, $(4,2,1)$, $(3,3,1)$ or $(3,2,2)$. In $(4,2,1)$ and $(3,3,1)$, $c_{\min} = 1$ has multiplicity 1, so Corollary 6.7 would force $c_{\min} \geq 12$, which fails. For $(5,1,1)$, Proposition 8.1 at an index of valuation 1 reads $2 + \min(5,1) + v(a_2 + a_3) = 1 + t = 8$, so $v(a_2+a_3) = 5$. For $(3,2,2)$, at an index of valuation 2 it reads $3+\min(3,2)+v(a_2+a_3) = 8$, so $v(a_2 + a_3) = 3$. □

Proposition 9.5. *Neither configuration of Proposition 9.4 occurs.*

Proof. The profile $(5,1,1)$. Write $E_k = \sum_{i \in E} a_i^k$ and $\Delta^m E = \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} E_{2j+1} = \sum_{i \in E} a_i (a_i^2 - 1)^m$, so that $8^m \mid \Delta^m E$ for $m \leq 4$ by Lemma 6.4. Write $a_1 = 32b_1$, $a_2 = 2b_2$, $a_3 = 2b_3$ with b_i odd. For k odd, $b_2^k + b_3^k = (b_2 + b_3) q_k$ with q_k odd, being a sum of k odd terms. The condition $v(a_2 + a_3) = 5$ gives $v(b_2 + b_3) = 4$, say $b_2 + b_3 = 16c$ with c odd; put $z := b_1 + c$, an even integer. Then

$$E_1 = 32z, \qquad E_3 = 2^{15} b_1^3 + 2^7 c q_3, \qquad E_5 = 2^{25} b_1^5 + 2^9 c q_5,$$

$$E_7 = 2^{35} b_1^7 + 2^{11} c q_7, \qquad E_9 = 2^{45} b_1^9 + 2^{13} c q_9.$$

Modulo 2^9 the only surviving terms of $\Delta^3 E = E_7 - 3E_5 + 3E_3 - E_1$ are $3E_3$ and $-E_1$, so $384\, cq_3 - 32z \equiv 0 \pmod{2^9}$, that is $z \equiv 12\, cq_3 \pmod{16}$. As cq_3 is odd, $12\, cq_3 \equiv 4$ or $12 \pmod{16}$, whence $z \equiv 4 \pmod 8$. Modulo 2^{12} the only surviving terms of $\Delta^4 E = E_9 - 4E_7 + 6E_5 - 4E_3 + E_1$ are $6E_5$, $-4E_3$ and E_1, so $3072\, cq_5 - 512\, cq_3 + 32z \equiv 0 \pmod{2^{12}}$, that is $96\, cq_5 - 16\, cq_3 + z \equiv 0 \pmod{128}$; reducing modulo 16 gives $z \equiv 0 \pmod{16}$, hence $z \equiv 0 \pmod 8$. This contradicts the previous congruence.

The profile $(3,2,2)$. Write $a_1 = 8b_1$, $a_2 = 4b_2$, $a_3 = 4b_3$ with b_i odd. Now $v(a_2+a_3) = 3$ gives $b_2 + b_3 = 2c$ with c odd, and as before $b_2^k + b_3^k = 2cq_k$ with q_k odd for k odd. Put $z := b_1 + c$. Then

$$E_1 = 8z, \qquad E_3 = 2^9 b_1^3 + 2^7 c q_3, \qquad E_5 = 2^{15} b_1^5 + 2^{11} c q_5,$$

$$E_7 = 2^{21} b_1^7 + 2^{15} c q_7, \qquad E_9 = 2^{27} b_1^9 + 2^{19} c q_9.$$

Modulo 2^9, $\Delta^3 E \equiv 3E_3 - E_1 \equiv 384\, cq_3 - 8z$, so $z \equiv 48\, cq_3 \pmod{64}$ and $v(z) = 4$. Modulo 2^{12}, the terms E_9, $4E_7$ and $6E_5$ vanish (note $6 \cdot 2^{11} = 3 \cdot 2^{12}$), so $\Delta^4 E \equiv -4E_3 + E_1 \equiv -2^{11} b_1^3 - 2^9 cq_3 + 8z$, whence $z \equiv 64\, cq_3 + 256\, b_1^3 \pmod{512}$ and $v(z) = 6$. The two values of $v(z)$ are incompatible. □

Remark 9.6. Proposition 9.5 has been confirmed independently by exhaustive computation, for both profiles, in the second ancillary file: no even triple of either profile satisfies the two conditions at $m = 3$ and $m = 4$ simultaneously.

Theorem 9.7. *Let A be a symmetric ideal solution over $\mathbb{Z}_2$ of size 11. Then $t \geq 10$, hence*

$$v(C) \;\geq\; 11.$$

Proof. Immediate from Propositions 9.4 and 9.5. □

For comparison, Kleiman's bound $(n-1)! \mid \overline{C_n}$ gives $v_2 \geq v_2(10!) = 8$.

9.4 The sizes $n = 13$ and $n = 15$

Theorem 9.8. *Let A be a symmetric ideal solution over $\mathbb{Z}_2$ of size 13. Then $t \geq 11$, hence $v(C) \geq 12$.*

Proof. Here $s = 5$ and $(n-3)/2 = 5$; by Lemma 9.1, $w \in \{2, 4, 6, 8, 10, 12\}$.

- $w = 2$, $u = 11$: Corollary 8.2 gives $t \geq 16$.
- $w = 4$, $u = 9$: Corollary 8.2 gives $t \geq 14$.
- $w = 10$, $u = 3$, $h = 5$: cases (i) and (ii) of Proposition 7.2 are excluded, so $\tau \geq 5 + 3 = 8$ and $t = 9 + \tau \geq 17$.
- $w = 12$, $u = 1$: Corollary 6.8 gives $t \geq 3 \cdot 5 = 15$.
- $w = 8$, $u = 5$, $h = 4$: $\tau \in \{0, 4\} \cup [6, \infty)$, so $t = 7 + \tau \in \{7, 11\} \cup [13, \infty)$; and $t \geq 8$ by Corollary 8.2, so $t \geq 11$.
- $w = 6$, $u = 7$, $h = 3$: as at $n = 11$, $\tau \geq 5$ and $t = 5 + \tau \geq 10$. Suppose $t = 10$. Corollary 8.2 forces $\max(m_1 + 6,\, 14 - m_1) \leq 10$, so $m_1 = 4$ and the profile is $(2, 2, 2, 1, 1, 1, 1)$. Applying Proposition 8.1 at an index of valuation 2 gives a row sum at least $3 + 3 + 3 + 1 + 1 + 1 + 1 = 13 > 1 + t = 11$, a contradiction. Hence $t \geq 11$.

□

Theorem 9.9. *Let A be a symmetric ideal solution over $\mathbb{Z}_2$ of size 15. Then $t \geq 11$, hence $v(C) \geq 12$.*

Proof. Here $s = 5$ and $(n-3)/2 = 6$; by Lemma 9.1, w is even with $2 \leq w \leq 14$. Corollary 8.2 gives $t \geq 20$, 16 and 14 for $u = 13$, 11 and 9, that is for $w = 2$, 4 and 6. For $w = 10$ one has $u = 5$ and $h = 5$, and cases (i) and (ii) of Proposition 7.2 are excluded, so $\tau \geq 5 + 3 = 8$ and $t = 9 + \tau \geq 17$. For $w = 14$ one has $u = 1$, and Corollary 6.8 gives $t \geq 3 \cdot 6 = 18$. For $w = 8$ one has $u = 7$ and $h = 4$, so $\tau \in \{0, 4\} \cup [6, \infty)$ and $t = 7 + \tau \in \{7, 11\} \cup [13, \infty)$, while Corollary 8.2 gives $t \geq 10$; hence $t \geq 11$. Finally for $w = 12$ one has $u = 3$ and $h = 6$, so $\tau \in \{0, 6\} \cup [9, \infty)$ and $t = 11 + \tau \geq 11$. □

Corollary 9.10. *Let $(A, -A)$ be a symmetric ideal Prouhet–Tarry–Escott solution with entries in $\mathbb{Z}$ and constant C. Then $2^9 \mid C$ if A has size 9, $2^{11} \mid C$ if it has size 11, and $2^{12} \mid C$ if it has size 13 or 15.*

Proof. Such a solution is a symmetric ideal solution over $\mathbb{Z}_2$ in the sense of Definition 6.1; apply Theorems 9.3, 9.7, 9.8 and 9.9. □

10 Sharpness at $n = 11$

Coppersmith, Mossinghoff, Scheinerman and VanderKam exhibit two multisets of size 11, each consisting of nine rational integers together with a conjugate pair of quadratic irrationalities, whose odd power sums p_1, p_3, p_5, p_7, p_9 all vanish:

$$A_1 = \{-95,\ -68-\alpha,\ -52,\ -48,\ -13,\ -9,\ 30,\ 34,\ 61,\ 65,\ 95+\alpha\},$$

$$A_2 = \{-589,\ -546+\beta,\ -363,\ -185,\ -170,\ 41,\ 87-\beta,\ 234,\ 355,\ 548,\ 588\},$$

where $\alpha^2 + 163\alpha - 8 = 0$ and $\beta^2 - 633\beta + 30 = 0$.

Theorem 10.1. *Each root α of $X^2 + 163X - 8$ and each root β of $X^2 - 633X + 30$ lies in $\mathbb{Z}_2$, and the corresponding tuples A_1, A_2 are symmetric ideal solutions over $\mathbb{Z}_2$ of size 11 with $v(C) = 11$. Consequently the bound of Theorem 9.7 is attained and*

$$\min\{v(C)\} = 11.$$

Proof. The discriminants are $163^2 + 32 = 26601$ and $633^2 - 120 = 400569$, both congruent to 1 modulo 8, hence squares in $\mathbb{Z}_2$; their square roots are odd, so $-163 \pm \sqrt{26601}$ and $633 \pm \sqrt{400569}$ are even and the four roots lie in $\mathbb{Z}_2$. The identities $p_1 = p_3 = p_5 = p_7 = p_9 = 0$ hold identically in $\mathbb{Z}[\alpha]$ and in $\mathbb{Z}[\beta]$, as a direct expansion confirms, hence in $\mathbb{Z}_2$. Finally $C = -2\prod a_i$ is a rational integer in both cases, of 2-adic valuation 11. □

Remark 10.2. The structure of these two witnesses matches the case analysis exactly: in all four embeddings one finds $w = 6$, $u = 5$, $\tau = 5$ and even valuations $(4, 2, 2, 1, 1)$, the six odd row sums of Proposition 7.1 all equal 10 and the five even row sums of Proposition 8.1 all equal 11.

Remark 10.3. Since 2 splits in both fields, the same argument applies to every prime p that splits in $\mathbb{Q}(\sqrt{26601})$ or in $\mathbb{Q}(\sqrt{400569})$: for such p there exists a p-adic ideal solution of size 11, necessarily not rational. Among the 30 primes below 120, exactly 21 are of this kind, namely

2, 5, 7, 11, 13, 17, 19, 23, 31, 37, 41, 43, 59, 61, 71, 73, 83, 89, 103, 109, 113,

the remaining nine being $3, 29, 47, 53, 67, 79, 97, 101, 107$. Filaseta and Markovich ask whether a 2-adic ideal solution exists for every $n \geq 3$, and whether a p-adic ideal solution necessarily exists at $n = 11$; both questions are repeated by Foster [9]. The first is vacuous for $n \leq 10$ and $n = 12$, where ideal solutions exist over $\mathbb{Z}$, so its content lies at $n = 11$ and at $n \geq 13$; Theorem 10.1 settles $n = 11$ and Proposition 11.1 settles $n = 13$, the first two open cases, and in both the solution is irrational. For the second question the present section gives an affirmative answer for every p that splits in one of the two fields, and says nothing for the nine primes below 120 that are inert or ramified in both.

Remark 10.4. It may be worth recording that $C(A_1)$ satisfies every divisibility known to be required of the constant of a symmetric ideal solution of size 11 over $\mathbb{Z}$ except one: its valuations at $2, 3, 5, 7, 11, 13, 17, 19$ are $11, 5, 3, 2, 1, 3, 1, 1$, all at or above the required values $8, 4, 3, 2, 1, 1, 1, 1$, while $31 \nmid C(A_1)$. The exception is accounted for by the fact that 31 is inert in $\mathbb{Q}(\sqrt{26601})$, since $26601 \equiv 3 \pmod{31}$ is not a square, so that the local argument producing the factor 31 does not apply. In $\mathbb{Q}(\sqrt{400569})$ the prime 31 splits, and indeed $31 \mid C(A_2)$.

11 A 2-adic solution at $n = 13$

No ideal solution of size 13 is known over $\mathbb{Z}$. Over $\mathbb{Z}_2$ one exists, and it too is obtained from an object already in the literature: among the configurations reported by Coppersmith, Mossinghoff, Scheinerman and VanderKam at size 13, consisting of eight rational integers together with the roots of a totally real quintic, the second one splits 2-adically.

Proposition 11.1. *Let* $f(x) = x^5 - 4278125x^3 + 3664306448884x - 975527373189600$. *Then* f *splits completely over* $\mathbb{Q}_2$*, and the multiset*

$$\{-1827,\ -989,\ -715,\ -405,\ 64,\ 902,\ 1330,\ 1640\} \ \cup\ \{\alpha : f(\alpha) = 0\}$$

is a symmetric ideal solution over $\mathbb{Z}_2$ *of size* 13*, with* $v(C) = 17$.

Proof. The six identities $p_1 = p_3 = \cdots = p_{11} = 0$ hold exactly: the power sums of the roots of f are computed from its coefficients by Newton's identities, and added to those of the eight integers they vanish. The Newton polygon of f at 2 has vertices $(0, 5)$, $(1, 2)$, $(3, 0)$, $(5, 0)$, hence segments of slopes -3, -1, 0 and lengths 1, 2, 2; a 2-adic lifting shows that each segment splits, so f has five roots in $\mathbb{Z}_2$, of valuations $3, 1, 1, 0, 0$. The eight rational integers have valuations $0, 0, 0, 0, 1, 1, 3, 6$. Hence $t = 16$ and $v(C) = 1 + t = 17$ by Proposition 6.2. □

Remark 11.2 (certificate)**.** The splitting of f over $\mathbb{Q}_2$ is checked as follows. Each of the five residues r below satisfies $v(f(r)) > 2\,v(f'(r))$, so by Hensel's lemma there is a unique $\alpha \in \mathbb{Z}_2$ with $f(\alpha) = 0$ and $v(\alpha - r) \geq v(f(r)) - v(f'(r)) \geq 32$; the five residues being pairwise distinct modulo 2^{32}, the five roots are distinct, and $v(\alpha) = v(r)$.

$r \bmod 2^{32}$	$v(f(r))$	$v(f'(r))$	$v(r)$
2723974027	33	1	0
1263895509	34	1	0
3276945658	35	3	1
3386758734	36	3	1
2233327960	34	2	3

Corollary 11.3. *At* $n = 13$ *one has* $12 \leq \min\{v(C)\} \leq 17$. *In particular a symmetric ideal solution over* $\mathbb{Z}_2$ *of size* 13 *exists, no ideal solution of that size being known over* $\mathbb{Z}$.

Remark 11.4. The structure of this witness is $w = 6$, $u = 7$, $\tau = 11$ and even valuations $(6, 3, 3, 1, 1, 1, 1)$; the six odd row sums of Proposition 7.1 all equal 16 and the seven even row sums of Proposition 8.1 all equal 17. Whether the lower bound 12 of Theorem 9.8 is attained remains open.

Remark 11.5. The first configuration reported at size 13 in the same place consists of the eight integers $-1026, -532, -248, -245, 207, 286, 533, 1025$ together with the roots of a quintic printed, in the arXiv version of [7], as $x^5 - 1215245x^3 + 170781322924x + 931022099280$. With that constant term the required identities fail: one finds $p_5 = -10 \cdot 931022099280 \neq 0$. With the constant term -931022099280 all six identities $p_1 = p_3 = \cdots = p_{11} = 0$ hold exactly, so the sign appears to be a misprint. With that sign, however, its Newton polygon at 2 has segments of slopes $-2, -1, 0$ and lengths $1, 2, 2$, and only three of the five roots lie in $\mathbb{Q}_2$; the configuration therefore lives in a quadratic extension and is not a symmetric ideal solution over $\mathbb{Z}_2$. For the second configuration, the arXiv version of [7] prints the coefficient of x as 366430644884; with that value p_9 and p_{11} do not vanish, whereas the value 3664306448884 used in Proposition 11.1 makes all six identities hold exactly.

12 Summary, scope and credits

All entries in the second and third columns are bounds on $v_2(C)$; at $n = 5, 7, 9$ the value in the third column is the known exact value of $v_2(\overline{C_n})$. The value at $n = 5$ is Proposition 2.4 of [15], the divisibility $2^6 \mid \overline{C_7}$ is due to Caley [4], and the value at $n = 9$ is due to Filaseta and Markovich [8].

n	here	previously	attained by
5	≥ 4	$= 4$	$(9, 5, 1, -7, -8)$
6	≥ 6	≥ 3 (Kleiman)	$\pm\{0, 7, 7\}$ against $\pm\{3, 5, 8\}$
7	≥ 6	$= 6$ (Caley)	$(-50, -38, -13, -7, 24, 33, 51)$
8	≥ 8	≥ 6 (Filaseta–Markovich)	$\pm\{5, 14, 23, 24\}$ against $\pm\{2, 16, 21, 25\}$
9	≥ 9	$= 9$	Letac
10	≥ 11	9 to 11 (Bera–Nair)	Gloden; Borwein–Lisoněk–Percival
11	≥ 11	≥ 8 (Kleiman)	A_1, A_2 over $\mathbb{Z}_2$
12	≥ 12	11 to 12 (Bera–Nair)	Kuosa–Meyrignac–Shuwen
13	≥ 12	≥ 10 (Kleiman)	— (but 17 occurs)
14	≥ 12	≥ 10 (Kleiman)	—
15	≥ 12	≥ 11 (Kleiman)	—
16	≥ 16	≥ 11 (Kleiman)	—
18	≥ 18	≥ 15 (Kleiman)	—
20	≥ 18	≥ 16 (Kleiman)	—

Scope. All the statements above concern *symmetric* solutions, hence C'_n and not $\overline{C_n}$; for n even they concern solutions with entries in $\mathbb{Z}$, for n odd solutions over $\mathbb{Z}_2$, for the reason given in the introduction. At $n = 5, 7, 9$ the two agree, the minimum being already attained by a symmetric solution over $\mathbb{Z}$. At $n = 10$ and $n = 12$ the equalities hold for C'_n; a smaller value for $\overline{C_n}$ would require a non-symmetric ideal solution of that size, and whether one exists is open.

The restriction to symmetry about 0 is not vacuous, and at these two sizes one can say exactly how much is lost. Over $\mathbb{Z}_2$ there exist ideal solutions of size 10 and of size 12, symmetric about $-1/2$ rather than about 0, whose constants have valuation exactly 9 and exactly 11; they are exhibited with Hensel certificates in the third ancillary file. The lower bounds of Bera and Nair at those two sizes are therefore attained 2-adically, so no argument using 2-adic information alone can raise them, and deciding the exact values of $v_2(\overline{C_{10}})$ and $v_2(\overline{C_{12}})$ requires global input. The equalities proved here for C'_{10} and C'_{12} and this limitation on $\overline{C_{10}}$ and $\overline{C_{12}}$ are consistent: they bear on different classes of solutions.

The lower bounds at $n = 13, \ldots, 20$ are not asserted to be optimal. For n odd the same case analysis applies at every size, but beyond $n = 15$ it is weaker than Kleiman's bound: at $n = 17$, 19 and 21 it gives $v(C) \geq 12$, 12 and 16, against $v_2((n-1)!) = 15$, 16 and 18.

Verification. Three self-contained verifiers are attached, written in Python with no dependencies. The even-size verifier replays sixty-seven checks: ideality and valuations of the six even solutions of sizes 8, 10 and 12, regularity of the two systems, validity and tightness of the index bound, exactness of the predictor on the twelve half-solutions, slopes of the Newton polygons, the minimum of the bound for each of the eight sizes $6 \leq n \leq 20$ in both cases of the dichotomy (in the case $\sigma \neq \sigma'$ with all entries of the larger profile up to $s' + r + 3$, as allowed by Lemma 5.2), the counts and the explicit lists of Theorem 5.3 together with the one-parameter shape of every form, and structural statements on the odd witnesses; it runs in about ten minutes. The odd-size verifier replays twenty-five checks: the witnesses of Sections 10 and 11, the Hensel certificate, the congruences of Proposition 9.5 for both profiles, exhaustively, and the chain of Section 9 at every odd size up to 21. The third file replays twenty-eight checks on the two 2-adic witnesses of the scope paragraph

above: Hensel certificates for every root of the four polynomials involved, a calibration at size 8 against the bound of Filaseta and Markovich, and the position of the size-10 witness within the case analysis of Bera and Nair.

Credits. The reference lower bound is due to Kleiman (1975). The use of Newton polygons on this constant is due to Filaseta and Markovich (2017), who also raised the question of the sizes 10 to 12; the germ of Lemma 6.4 is their congruence modulo 16 between power sums of odd and even parts, and the parameters w and m_1 used here are their k_1 and k_2. The published lower bounds at sizes 10 and 12, which the present work closes, are due to Bera and Nair (2024). The construction of 2-adic ideal solutions by successive lifting, which is the counterpart of the obstruction developed above, is due to Foster, in his 2021 thesis, who carries it out for $3 \leq n \leq 8$. The explicit ideal solutions used as witnesses are catalogued by Coppersmith, Mossinghoff, Scheinerman and VanderKam, and are due to Letac (1942) at size 9, to Smyth (1991) [16] for the infinite family at size 10 and to Borwein, Lisoněk and Percival (2003) for the two smaller solutions of that size, and at size 12 to Kuosa, Meyrignac and Shuwen (1999), to Broadhurst (2007) and to Choudhry and Wróblewski (2008). The two quadratic objects of Section 10 and the quintic configuration of Section 11 are those of Coppersmith, Mossinghoff, Scheinerman and VanderKam; what is added here is the observation that they are 2-adic. Technical assistance: Claude (Anthropic).

Remark 12.1 (on Bera–Nair)**.** The paper of Bera and Nair treats the sizes $n = 10$ and $n = 12$ only, as their abstract states. Their results at those two sizes are the brackets recorded in Theorem 5.1, which the present work closes in the symmetric case; they give nothing at $n = 11$ or $n = 13$, so the statements of Sections 9–11 do not overlap with theirs.

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] P. Borwein, P. Lisoněk and C. Percival, *Computational investigations of the Prouhet–Tarry–Escott problem*, Math. Comp. **72** (2003), 2063–2070.

[3] D. Broadhurst, *A new Prouhet–Tarry–Escott solution*, NMBRTHRY mailing list, 26 September 2007.

[4] T. Caley, *The Prouhet–Tarry–Escott problem*, Ph.D. thesis, University of Waterloo, 2012.

[5] T. Caley, *The Prouhet–Tarry–Escott problem for Gaussian integers*, Math. Comp. **82** (2013), 1121–1137.

[6] A. Choudhry and J. Wróblewski, *Ideal solutions of the Tarry–Escott problem of degree eleven with applications to sums of thirteenth powers*, Hardy–Ramanujan J. **31** (2008), paper no. 1.

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

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

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

[10] A. Gloden, *Mehrgradige Gleichungen*, 2nd ed., Noordhoff, Groningen, 1944.

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

[12] P. Kuosa, J.-C. Meyrignac and C. Shuwen, ideal solution of size 12 announced in 1999 on J.-C. Meyrignac's website on equal sums of like powers; see [7].

[13] A. Letac, Gazeta Matematică **48** (1942), 68–69.

[14] M. E. Markovich, *On a constant associated with the Prouhet–Tarry–Escott problem*, Master's thesis, University of South Carolina, 2016.

[15] E. Rees and C. J. Smyth, *On the constant in the Tarry–Escott problem*, Lecture Notes in Math. **1415**, Springer, 1990, 196–208.

[16] C. J. Smyth, *Ideal 9th-order multigrades and Letac's elliptic curve*, Math. Comp. **57** (1991), no. 196, 817–823.