ACTA ARITHMETICA
Online First version

# Newton polygons and the constant associated with the Prouhet–Tarry–Escott problem

by

Ranjan Bera (Bangalore) and Saranya G. Nair (Zuarinagar)

**Abstract.** In a 2017 article Filaseta and Markovich obtained new information on the lower bounds of 2-adic valuation of certain constants $\overline{C_n}$ associated with the Prouhet–Tarry–Escott (PTE) problem for the cases $n = 8$ and $n = 9$ by using the classical theory of Newton polygons, and also pointed out that it would be of interest to obtain improved lower bounds in the cases when $10 \leq n \leq 12$. In the present article, we obtain new 2-adic information on the lower bounds of $\overline{C_n}$ for the cases $n = 10$ and $n = 12$.

**1. Introduction.** Given natural numbers $n$ and $k$, with $n > k$, the *Prouhet–Tarry–Escott* (henceforth abbreviated PTE) *problem* asks about distinct sets of integers, say $X = [x_1, \dots, x_n]$ and $Y = [y_1, \dots, y_n]$, such that

$$\sum_{i=1}^{n} x_i^j = \sum_{i=1}^{n} y_i^j \quad \text{for } j = 1, \dots, k. \tag{1}$$

If $X$ and $Y$ satisfy (1), then the pair $(X, Y)$ is called a *PTE solution* and is written as $X =_k Y$. We call $n$ the *size* of the solution and $k$ the *degree*. For example,

$$[3, 6, 6, 7] =_2 [4, 5, 5, 8]$$

is a PTE solution of size 4 and degree 2. Dating back to 1750s, a special case of this problem appeared in the works of Goldbach and Euler. For any integers $a, b, c, d$,

$$[a + b + d, a + c + d, b + c + d, d] =_2 [a + d, b + d, c + d, a + b + c + d]$$

is a family of PTE solutions of size 4 and degree 2 due to Goldbach. In fact, this example was also found by Euler when $d = 0$. Prouhet's work in 1851 established that for any given $k$ there is a solution with sufficiently large $n$.

2020 *Mathematics Subject Classification*: Primary 11D72; Secondary 11B75, 11D41, 11P05.
*Key words and phrases*: primes, Prouhet–Tarry–Escott problem, $p$-adic, Newton polygons.
Received 10 August 2023; revised 15 December 2023.
Published online 11 April 2024.

DOI: 10.4064/aa230810-29-12  

Prouhet's contribution to this problem was pointed out by Wright [18]. Tarry and Escott studied the more general problem in the 1910s and hence, nowadays, this problem is referred to as the Prouhet–Tarry–Escott problem. Volume II of L. E. Dickson's "History of the Theory of Numbers" [8] provides an extensive historical account of this problem, encompassing numerous early references.

The maximal non-trivial case of the PTE problem occurs when $k = n-1$. A solution of size $n$ and degree $n-1$ is called an *ideal solution.* An important open problem in the area is a conjecture of Wright [17] that states that an ideal solution exists for every $n \geq 3$. Wright's conjecture is verified for $3 \leq n \leq 10$ and $n = 12$. Even though the problem has been investigated for a long time, ideal solutions for $n = 11$ and $n \geq 13$ are hitherto unknown. Ideal solutions are particularly interesting due to their connections with problems in theoretical computer science and graph theory. The following question from graph theory is one such instance. Given any integer $m \geq 4$, does there exist a graph $G$ such that $G$ has a chordless cycle of order $m$ and all roots of the chromatic polynomial of $G$ are integers? In [12], Hernández and Luca established that ideal solutions of the PTE problem of size $n$ can be used to construct such graphs of order $n+1$, thus answering the aforementioned question on graphs affirmatively for $m = 8, 9, 10, 11$ and 13.

Some of the recent developments in the PTE problem are documented in [4, 5, 10, 13, 15]. Interesting works on generalizations of the PTE problem can be found in [1, 6]. For more applications stemming from the PTE problem, we refer to [2, 11, 12, 14, 16].

The following lemma and its corollary related to elementary symmetric functions will help in our further discussion of the PTE problem (see [3, 4]).

LEMMA 1.1. *Let $n$ and $k$ be integers with $1 \leq k < n$. Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ denote arbitrary integers. The following are equivalent:*

(i) $\sum_{i=1}^{n} x_i^l = \sum_{i=1}^{n} y_i^l$ *for* $l \in \{1, \ldots, k\}$,

(ii) $\deg\Big(\prod_{i=1}^{n}(z - x_i) - \prod_{i=1}^{n}(z - y_i)\Big) \leq n - k - 1$,

(iii) $(z-1)^{k+1} \,\Big|\, \Big(\sum_{i=1}^{n} z^{x_i} - \sum_{i=1}^{n} z^{y_i}\Big)$.

COROLLARY 1.2. *The lists $X = [x_1, \ldots, x_n]$ and $Y = [y_1, \ldots, y_n]$ give an ideal PTE solution if and only if*

$$\prod_{i=1}^{n}(z - x_i) - \prod_{i=1}^{n}(z - y_i) = C \tag{2}$$

*for some integer $C$.*

From now on, we will consider ideal PTE solutions as being lists $X = [x_1, \ldots, x_n]$ and $Y = [y_1, \ldots, y_n]$ satisfying (2). It has been shown in [4, 5, 7, 15] that the information about $C$, particularly on the representation of $C$ given in (2), is very useful in deriving examples of ideal PTE solutions. Since $C$ depends on $n$, $X$ and $Y$, we define for $X =_{n-1} Y$ the constant

$$C_n = C_n(X,Y) = \prod_{i=1}^{n}(z - x_i) - \prod_{i=1}^{n}(z - y_i).$$

Since $C_n$ is the constant term of the polynomial on the right hand side of the above equation, we can alternatively write

$$C_n = (-1)^n\Big(\prod_{i=1}^{n} x_i - \prod_{i=1}^{n} y_i\Big).$$

An important divisibility result for $C_n$ is that $n! \mid C_{n+1}$ (see [13]). Next, we state a result that follows from Corollary 1.2 and is used throughout this paper.

COROLLARY 1.3. *Let $a \in \mathbb{Z}$. The lists $X = [x_1, \ldots, x_n]$ and $Y = [y_1, \ldots, y_n]$ form an ideal PTE solution if and only if the lists $X' = [x_1 + a, \ldots, x_n + a]$ and $Y' = [y_1 + a, \ldots, y_n + a]$ form an ideal PTE solution. Furthermore, if these are ideal solutions, then $C_n(X,Y) = C_n(X',Y')$.*

Define

$$\overline{C}_n = \prod_{j=1}^{\infty} p_j^{e_j},$$

where

$$e_j = \min\{e : p_j^e \,\|\, C_n(X,Y) \text{ for some } X \text{ and } Y \text{ as above with } X =_{n-1} Y\}.$$

Thus, $\overline{C}_n$ can be viewed as the greatest common divisor over all constants $C_n(X,Y)$ where $X$ and $Y$ vary over distinct ordered lists of $n$ integers satisfying $X =_{n-1} Y$.

For $3 \le n \le 7$, the possible values of $\overline{C}_n$ were proved in [5]. For example, $\overline{C}_7 = 2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11$. It was also proved in [5] that

$$\begin{aligned} \overline{C}_8 &= 2^{e_0} \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13, \\ \overline{C}_9 &= 2^{e_1} \cdot 3^{e_2} \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17^{e_3} \cdot 23^{e_4} \cdot 29^{e_5}, \end{aligned} \tag{3}$$

where $4 \le e_0 \le 8$, $7 \le e_1 \le 9$, $3 \le e_2 \le 4$, and $0 \le e_j \le 1$ for $j \in \{3,4,5\}$.

For a prime $p$ and a positive integer $r$, we let $\nu_p(r)$ be the maximal power of $p$ dividing $r$ and we define $\nu_p(0) = +\infty$. Further we write $\nu(r) = \nu_p(r)$ if the prime is clear from the context. Obviously, $\nu_p(r) = k$ is equivalent to $p^k \,\|\, r$. We will also use the standard floor and ceiling notation.

Thus it follows from (3) that

$$4 \le \nu_2(\overline{C}_8) \le 8 \quad \text{and} \quad 7 \le \nu_2(\overline{C}_9) \le 9. \tag{4}$$

Similar divisibility results on $C_n$ for $n = 10$ and 12 were also proved in [5], and in particular,

$$7 \le \nu_2(\overline{C}_{10}) \le 11 \quad \text{and} \quad 8 \le \nu_2(\overline{C}_{12}) \le 12. \tag{5}$$

Using the theory of classical Newton polygons, Filaseta and Markovich [10] improved the existing lower bounds of $\nu_2(\overline{C}_8)$ and $\nu_2(\overline{C}_9)$, as given in (4), to $6 \le \nu_2(\overline{C}_8) \le 8$ and $\nu_2(\overline{C}_9) = 9$. Their results motivated us to investigate whether we can improve the lower bounds for 2-adic values of $\overline{C}_{10}$ and $\overline{C}_{12}$ as given by (5).

The following result is the main contribution of this article:

THEOREM 1. *With the notations as above,*

$$9 \le \nu_2(\overline{C}_{10}) \le 11 \quad \textit{and} \quad 11 \le \nu_2(\overline{C}_{12}) \le 12.$$

REMARK 1.4. The case $n = 10$ has been discussed in Section 3. There we show that in all but one cases (see Case 2.3(ii)) of conditions on $X = [x_1, \dots, x_{10}]$ and $Y = [y_1, \dots, y_{10}]$ that we consider, one has $2^{10} \mid C_{10}$. More specifically, only when exactly five $x_j$'s and five $y_j$'s are odd, and exactly one $x_j$ and one $y_j$ are of the form 2 (mod 4), we obtain $2^9 \parallel C_{10}$. Further analysis using this information on $C_{10}$ helped us to deduce 2-adic information on the remaining $x_j$'s and $y_j$'s. For instance, all the remaining $x_j$'s and $y_j$'s must be of the form 4 (mod 8) and 0 (mod 8) respectively. Observe that by analyzing this information, if it is possible to find an example of an ideal solution in this special case, then $\nu_2(\overline{C}_{10}) = 9$ in Theorem 1. On the other hand, if one proves that an ideal solution with these divisibility properties does not exist, then the lower bound for $\nu_2(\overline{C}_{10})$ would be $\ge 10$ in Theorem 1.

We introduce Newton polygons, and state further results based on the Newton polygons required in the proof of Theorem 1, in Section 2. We prove Theorem 1 for $n = 10$ in Section 3 and $n = 12$ in Section 4.

**2. Preliminaries.** We write

$$f(z) = \prod_{j=1}^{n}(z - x_j) = \sum_{j=0}^{n} a_j z^j \quad \text{and} \quad g(z) = \prod_{j=1}^{n}(z - y_j) = \sum_{j=0}^{n} b_j z^j, \tag{6}$$

where $x_j$ and $y_j$ are chosen so that

$$f(z) - g(z) = C_n \tag{7}$$

and that the exact power of 2 dividing $C_n$ is equal to the exact power of 2 in $\overline{C}_n$. From Corollary 1.2, we see that $X = [x_1, \dots, x_n]$ and $Y = [y_1, \dots, y_n]$ is an ideal solution. We will write $C = C_n$ if $n$ is clear from the context.

**Newton polygons.** We introduce the definition of a Newton polygon for a polynomial with respect to a prime. Let $h(x) = \sum_{j=0}^{n} c_j x^j \in \mathbb{Z}[x]$ with $c_0 c_n \neq 0$ and let $p$ be a prime. Let $S$ be the following set of points in the extended plane:

$$S = \{(0, \nu(c_n)), (1, \nu(c_{n-1})), (2, \nu(c_{n-2})), \ldots, (n, \nu(c_0))\}.$$

Consider the lower edges along the convex hull of these points. The leftmost endpoint is $(0, \nu(c_n))$ and the rightmost endpoint is $(n, \nu(c_0))$. The endpoints of each edge belong to $S$ and the slopes of the edges increase from left to right. When referring to the edges of a Newton polygon, we shall not allow two different edges to have the same slope. The polygonal path formed by these edges is called the *Newton polygon* of $h(x)$ with respect to the prime $p$ and denoted by $\mathrm{NP}_p(h)$. We write $\mathrm{NP}(h) = \mathrm{NP}_p(h)$ if $p$ is clear from the context. The endpoints of the edges of $\mathrm{NP}_p(h)$ are called the *vertices* of $\mathrm{NP}_p(h)$. Next we state a lemma of Dumas [9] that relates the Newton polygon of the product polynomial $h_1(x)h_2(x)$ to those of $h_1(x)$ and $h_2(x)$.

LEMMA 2.1. *Let $h_1(x), h_2(x) \in \mathbb{Z}[x]$ with $h_1(0)h_2(0) \neq 0$ and let $p$ be a prime. Let $k$ be a non-negative integer such that $p^k$ divides the leading coefficient of $h_1(x)h_2(x)$ but $p^{k+1}$ does not. Then the edges of the Newton polygon for $h_1(x)h_2(x)$ with respect to $p$ can be formed by constructing a polygonal path beginning at $(0, k)$ and using translates of the edges in the Newton polygons for $h_1(x)$ and $h_2(x)$ with respect to the prime $p$, using exactly one translate for each edge of the Newton polygons for $h_1(x)$ and $h_2(x)$. Necessarily, the edges are translated so as to form a polygonal path with increasing slopes.*

Let us consider the Newton polygons for the polynomials $f(z)$ and $g(z)$ defined in (6) with respect to the prime $p = 2$. We will denote them as $\mathrm{NP}(f)$ and $\mathrm{NP}(g)$ as the prime is fixed. For a fixed $n$, consider the two sets of points

$$S_1 = \{(j, \nu_2(a_{n-j})) : 0 \leq j \leq n\} \quad \text{and} \quad S_2 = \{(j, \nu_2(b_{n-j})) : 0 \leq j \leq n\}.$$

Since $f(z) - g(z) = C$, a constant, we see that $a_{n-j} = b_{n-j}$ for $0 \leq j \leq n-1$. Thus, $S_1$ and $S_2$ have at least $n$ of $n+1$ points in common. Using Corollary 1.2 we may assume that $a_0 \neq 0$ and $b_0 \neq 0$, thus ensuring $\nu_2(a_0) \neq +\infty$ and $\nu_2(b_0) \neq +\infty$. This in turn ensures that the rightmost points in $\mathrm{NP}(f)$ and $\mathrm{NP}(g)$ are in the finite plane. Observe that (7) still holds after this translation. We will be frequently using Corollary 1.2 to reduce the different cases in Sections 3 and 4.

The following lemma derived using Lemma 2.1 is crucial in applying Newton polygons in the study of the PTE problem as given by [10]. It uses the fact that $f(z)$ and $g(z)$ are products of $n$ linear factors.

Lemma 2.2. *The Newton polygons of $f(z)$ and $g(z)$ each pass through $n+1$ lattice points (including the endpoints), which we denote respectively as*

$$T_1 = \{(j, t_j) : 0 \le j \le n\} \quad \textit{and} \quad T_2 = \{(j, t'_j) : 0 \le j \le n\}.$$

*After possibly rearranging the $x_j$ and $y_j$, we find that $2^{t_j - t_{j-1}}$ exactly divides $x_j$ and $2^{t'_j - t'_{j-1}}$ exactly divides $y_j$ for each $j \in \{1, \dots, n\}$.*

We explain the importance of rearranging. The values of $\nu_2(x_j)$ and $\nu_2(y_j)$ are increasing as $j$ ranges from 1 to $n$. We will keep such an ordering throughout the paper. In particular, the values of the $x_j$ and the values of the $y_j$ are not necessarily increasing. Since the slopes of the edges of the Newton polygons increase from left to right, even though the points in $S_1$ and $S_2$ are the same except for $(n, \nu_2(a_0))$ and $(n, \nu_2(b_0))$, the vertices of the Newton polygons for $S_1$ and $S_2$, i.e. the points in $T_1$ and $T_2$ may not always be the same. We will see that a point in $T_1$ may be the same as a point in $T_2$. For example, consider $n = 10$ and let

$$X = \{9, 17, 25, 33, 41, 66, 68, 76, 92, 108\},$$
$$Y = \{101, 123, 127, 135, 145, 146, 162, 168, 184, 216\}.$$

In this case, consider $f(z) = \prod_{i=1}^{10}(z - x_i)$ and $g(z) = \prod_{i=1}^{10}(z - y_i)$; the respective sets $S_1$ and $S_2$ with respect to the prime $p = 2$ are

$$S_1 = \{(0,0), (1,0), (2,0), (3,0), (4,0), (5,0), (6,1), (7,4), (8,7), (9,10), (10,9)\},$$
$$S_2 = \{(0,0), (1,0), (2,0), (3,0), (4,0), (5,0), (6,1), (7,4), (8,7), (9,10), (10,14)\}.$$

The corresponding vertex sets for the Newton polygons $T_1$ and $T_2$ with respect to $p = 2$ are

$$T_1 = \{(0,0), (1,0), (2,0), (3,0), (4,0), (5,0), (6,1), (7,3), (8,5), (9,7), (10,9)\},$$
$$T_2 = \{(0,0), (1,0), (2,0), (3,0), (4,0), (5,0), (6,1), (7,4), (8,7), (9,10), (10,14)\}.$$

This is an example of $f(z)$ and $g(z)$ where $S_1$ and $S_2$ are the same except for the last point, but $T_1$ and $T_2$ are different.

Notations. Let us introduce some notations that will be useful in subsequent sections. Let $k_1$ be the number of odd $x_j$ and $k'_1$ be the number of odd $y_j$. Therefore $\nu_2(x_j) = \nu_2(y_j) = 0$ for such $x_j$ and $y_j$. Let $k_2$ be the number of $x_j$ that are congruent to 2 (mod 4) and $k'_2$ be the number of $y_j$ that are congruent to 2 (mod 4). Thus, $\nu_2(x_j) = \nu_2(y_j) = 1$ for such $x_j$ and $y_j$.

REMARK 2.3. By Corollary 1.3, translating $x_j$ and $y_j$ by 1 or any odd number if necessary, we may suppose $k_1' \leq \lfloor n/2 \rfloor$, and $a_0$ and $b_0$ are not 0. Furthermore, we may translate by 2 (or some other number congruent to 2 (mod 4)) to obtain $k_2' \geq \lceil (n-k_1')/2 \rceil$. This will help us reduce the number of cases to be dealt with, but sometimes we may consider a further translation to get more information about $C$. Cases that can be obtained through translation will be termed *equivalent*.

Using the following lemma from [4], we deduce that if $C$ is even, then $k_1 = k_1'$.

LEMMA 2.4. *Let* $[x_1, \ldots, x_n] =_{n-1} [y_1, \ldots, y_n]$ *be two lists of integers that constitute an ideal PTE solution, and suppose that a prime* $p$ *divides the constant* $C$ *associated with this solution. Then we can reorder the integers* $y_i$ *so that*

$$x_j \equiv y_j \pmod{p} \quad \text{for } j \in \{1, \ldots, n\}.$$

From the above lemma, we deduce that the number of odd $x_j$ must equal the number of odd $y_j$, i.e., $k_1 = k_1'$. Also, we can interchange the roles of $f(z)$ and $g(z)$, if necessary, so that $k_2' \geq k_2$. Since there are $n$ elements in each of the lists $X$ and $Y$, it must be the case that $k_1 + k_2 \leq n$ and $k_1' + k_2' \leq n$. Further, we state the following two lemmas and a corollary from [10].

LEMMA 2.5. *Let* $n \geq 8$ *and* $[x_1, \ldots, x_n] =_{n-1} [y_1, \ldots, y_n]$. *Let* $t$ *be such that* $x_1, \ldots, x_t$ *and* $y_1 \ldots, y_t$ *are odd and the other* $x_j$ *and* $y_j$ *are even. Then*

$$x_1^k + \cdots + x_t^k \equiv y_1^k + \cdots + y_t^k \pmod{16} \quad \text{for } k \geq 1,$$

*and*

$$x_{t+1}^k + \cdots + x_n^k \equiv y_{t+1}^k + \cdots + y_n^k \pmod{16} \quad \text{for } k \geq 1.$$

COROLLARY 2.6. *Let* $n \geq 8$ *and* $[x_1, \ldots, x_n] =_{n-1} [y_1, \ldots, y_n]$. *Let* $k_1, k_2$ *and* $k_1', k_2'$ *be as above. Then* $k_2 \equiv k_2' \pmod{4}$.

LEMMA 2.7. *If the points* $(n, \nu_2(a_0))$ *in* $S_1$ *and* $(n, \nu_2(b_0))$ *in* $S_2$ *are distinct and*

$$k = \min\{\nu_2(a_0), \nu_2(b_0)\},$$

*then* $2^k \parallel C$.

Let $n \geq 4$ be an integer. For integers $x_1, \ldots, x_n$, define

$$T(x_1, \ldots, x_n) = \sum_{i=1}^{n} \Big( \prod_{i<j<k<l\leq n} x_i x_j x_k x_l \Big) \quad \text{if } n \geq 4,$$

$$H(x_1, \ldots, x_n) = \sum_{i=1}^{n} \Big( \prod_{i<j\leq n} x_i x_j \Big) \qquad\quad \text{if } n \geq 2.$$

The following simple lemma discusses the divisibility of $T(x_1, \dots, x_n)$ and $H(x_1, \dots, x_n)$ by 2 and 4 when all the $x_i$'s are odd, and will be useful in later calculations. The easy proof is omitted.

LEMMA 2.8. *With the notations as above, assume that all the $x_i$'s are odd. Let $n \geq 8$ be an integer.*

(i) *If all the $x_i$'s, $1 \leq i \leq n$, are of the form $4k+1$ (or $4k+3$), then*

$$T(x_1, \dots, x_n) \equiv \binom{n}{4} \pmod{4}.$$

*In particular, when $n = 8$, $T(x_1, \dots, x_8)$ is exactly divisible by 2.*

(ii) *If exactly two $x_i$'s $(1 \leq i \leq n)$ are of the form $4k+3$, then*

$$T(x_1, \dots, x_n) \equiv \binom{n-2}{2} + 2\binom{n-2}{3} + \binom{n-2}{4} \pmod{4}.$$

*In particular, for $n = 8$ we have $2 \,\|\, T(x_1, \dots, x_8)$.*

(iii) *If exactly four $x_i$'s $(1 \leq i \leq n)$ are of the form $4k+3$, then*

$$T(x_1, \dots, x_n) \equiv 1 + 2\binom{n-4}{2} + \binom{n-4}{4} \pmod{4}.$$

*In particular, for $n = 8$ we have $2 \,\|\, T(x_1, \dots, x_8)$.*

(iv) *If exactly one $x_i$ is of the form $4k+3$, then*

$$H(x_1, \dots, x_n) \equiv 3(n-1) + \binom{n-1}{2} \pmod{4}.$$

*In particular, for $n = 8$ we have $2 \,\|\, H(x_1, \dots, x_8)$.*

(v) *If exactly three $x_i$ are of the form $4k+3$, then*

$$H(x_1, \dots, x_n) \equiv n + \binom{n-3}{2} \pmod{4}.$$

*In particular, for $n = 8$ we have $2 \,\|\, H(x_1, \dots, x_8)$.*

**3. Lower bound for $\nu_2(\overline{C}_{10})$.** Recall from (5) that

$$7 \leq \nu_2(\overline{C}_{10}) \leq 11.$$

Using the results discussed in Section 2, we will increase the lower bound by proving that $9 \leq \nu_2(\overline{C}_{10}) \leq 11$. To facilitate potential future analysis, we show that in all but one cases of conditions on $X = [x_1, \dots, x_{10}]$ and $Y = [y_1, \dots, y_{10}]$ that we consider, one has $2^{10} \mid \overline{C}_{10}$ (see Case 2.3(ii) where we prove $2^9 \,\|\, C$).

Throughout this section, we write $C$ for $\overline{C}_{10}$. It follows from Remark 2.3 with $n = 10$ that $k_1' + k_2' \leq 10$, $k_1 = k_1' \leq 5$ and $k_2 \leq k_2'$.

**3.1. Case 1: $k_1'+k_2'=10$.** In this case, no element $y_j$ is divisible by 4. Since $k_1=k_1'\le 5$, we get $k_2'\ge 5$. Further, $k_2\le k_2'$ implies the list $X$ contains at most $k_2'$ elements that are of the form 2 (mod 4). Therefore, every point $(j,\nu_2(a_{10-j}))$ in $S_1$ is at or above the corresponding point $(j,\nu_2(b_{10-j}))$ in $S_2$. Let us consider the following subcases.

Case 1.1: $k_2=k_2'$. We have $k_1=k_1'\le 5$, and $k_2=k_2'\ge 5$. Putting $z=2$ in (6), we obtain

$$\prod_{j=1}^{10}(2-x_j)-\prod_{j=1}^{10}(2-y_j)=f(2)-g(2)=C.$$

This implies $2^{2k_2}\,|\,C$. If $k_2\ge 6$, this leads to $2^{12}\,|\,C$, which contradicts $\nu_2(C)\le 11$. Therefore, $k_2=5$, and thus $2^{10}\,|\,C$.

Case 1.2: $k_2<k_2'$. In this case, $X$ must contain at least one $x_j$ that is divisible by 4, but we know that no $y_j$ is divisible by 4. We consider the cases $k_2=0$ and $k_2\ne 0$ separately.

Case 1.2(i): $k_2=0$. Since $k_2'\ge 5$ and $k_2\equiv k_2' \pmod 4$, we have $k_2'=8$, and hence $k_1=k_1'=2$. In this case, eight $x_j$'s are of the form 0 (mod 4) and eight $y_j$'s are of the form 2 (mod 4). Now consider the Newton polygons of $f(z)$ and $g(z)$. Since $k_2=0$, the edges of NP$(f)$ with positive slope have slope $\ge 2$. In particular, this implies

$$\nu_2(a_{10-j})\ge 2(j-2)\quad \text{for } 3\le j\le 10.$$

As the points $(j,\nu_2(a_{10-j}))\in S_1$ and $(j,\nu_2(b_{10-j}))\in S_2$ agree for $0\le j\le 9$, we deduce

$$\nu_2(b_{10-j})\ge 2(j-2)\quad \text{for } 3\le j\le 9. \tag{8}$$

Now we define $\tilde u_j\in\mathbb{Z}$ by the equation

$$(z-y_3)(z-y_4)\cdots(z-y_{10})=\sum_{j=0}^{8}\tilde u_j z^j. \tag{9}$$

We consider the 2-adic valuation of the $\tilde u_j$'s. Since $y_j\equiv 2 \pmod 4$ for $3\le j\le 10$, we derive $\nu_2(\tilde u_0)=8$. As $(z-y_1)(z-y_2)\equiv z^2+1 \pmod 2$, we have

$$\begin{aligned} b_1&=\tilde u_1\times(\text{odd number})+\tilde u_0\times(\text{even number}),\\ b_j&=\tilde u_j\times(\text{odd number})+\tilde u_{j-1}\times(\text{even number})+\tilde u_{j-2}\end{aligned} \tag{10}$$

for $2\le j\le 7$. We deduce from (8) with $j=9$ that $\nu_2(b_1)\ge 14$. Now using the facts $\nu_2(b_1)\ge 14$ and $\nu_2(\tilde u_0)=8$, it follows easily from the first equation of (10) that $\nu_2(\tilde u_1)\ge 9$. Using this along with $\nu_2(b_2)\ge 12$ (from (8)) and $\nu_2(\tilde u_0)=8$, it follows from the expression for $b_2$ as given by (10) with $j=2$

that $\nu_2(\tilde{u}_2) = 8$. Continuing, we obtain

(11) $\nu_2(\tilde{u}_3) \geq 9, \quad \nu_2(\tilde{u}_4) \geq 8, \quad \nu_2(\tilde{u}_5) \geq 6, \quad \nu_2(\tilde{u}_6) \geq 4, \quad \nu_2(\tilde{u}_7) \geq 2.$

Since $y_j \equiv 2 \pmod 4$ for $3 \leq j \leq 10$, we can write

$$y_j = 2y_j' \quad \text{for } 3 \leq j \leq 10, \qquad \text{where } y_j' \text{ is odd.}$$

Then the $y_j'$'s are of the form either $4k+1$ or $4k+3$. Observe that if $y_j'$ is of the form $4k+1$, then $y_j + 4 = 2y_j' + 4 = 2y_j''$, where $y_j''$ is of the form $4k+3$. Therefore, translating $z$ by $z-4$ in the definition of $C_n$ given by (7) we need to consider only the following equivalent subcases.

(i) If all the $y_j'$'s, $3 \leq j \leq 10$, are congruent modulo 4, then it follows from (9) that

$$\begin{aligned}\tilde{u}_4 &= \text{coefficient of } z^4 \text{ in } (z-y_3)\cdots(z-y_{10}) \\ &= \sum_{3\leq i<j<k<l\leq 10} y_i y_j y_k y_l = 2^4 \sum_{3\leq i<j<k<l\leq 10} y_i' y_j' y_k' y_l' \\ &= 2^4 T(y_3', \ldots, y_{10}').\end{aligned}$$

Therefore, by Lemma 2.8(i) we have $\nu_2(\tilde{u}_4) = 5$, which contradicts $\nu_2(\tilde{u}_4) \geq 8$ (see (11)).

(ii) If exactly two (or four) $y_j'$'s are of the form $4k+3$, then a similar argument, together with an appeal to Lemma 2.8(ii) (or Lemma 2.8(iii)), yields $\nu_2(\tilde{u}_4) = 5$, which is a contradiction.

(iii) Assume that exactly one $y_j'$ is of the form $4k+3$. Consider $u_2$, the coefficient of $z^2$ in $(z-y_3)\cdots(z-y_{10})$ (see (9)). Proceeding along the same lines as before, we obtain

$$\begin{aligned}\tilde{u}_6 &= \sum_{3\leq i<j\leq 10} y_i y_j \\ &= 2^2 H(y_3', \ldots, y_{10}') \qquad \text{(see Section 2 for notation).}\end{aligned}$$

By Lemma 2.8(iv), we have $2 \,\|\, H(y_3', \ldots, y_{10}')$, and hence $\nu_2(\tilde{u}_2) = 3$, which contradicts the fact that $\nu_2(\tilde{u}_2) = 8$.

(iv) If exactly three $y_j'$'s are of the form $4k+3$, then a similar argument together with an appeal to Lemma 2.8(v) shows that $\nu_2(\tilde{u}_2) = 3$, leading to a contradiction.

Thus, if $k_1' + k_2' = 10$ and $k_2 < k_2'$, then $k_2$ can never be zero.

Case 1.2(ii): $k_2 \neq 0$. Then there is at least one $x_j$ of the form $4k+2$, and hence, by taking $z = x_j$ in (7), we see that $2^{2k_2'} \mid C$. Similar arguments to Case 1.1 establish that $k_2' = 5$, and consequently $2^{10} \mid C$.

**3.2. Case 2:** $k_1' + k_2' < 10$**.** Since $k_1' \leq 5$ and $k_2' \geq \lceil (n - k_1')/2 \rceil$, we have $k_2' \geq 3$. Further $k_2' < 10 - k_1'$. Hence $(k_1', 0)$ and $(k_1' + k_2', k_2')$ are points in $S_2$ with $x$ coordinate $< 10$. Therefore $(k_1', 0)$ and $(k_1' + k_2', k_2')$ are points in $S_1$. Since there are exactly $k_1 = k_1'$ odd $x_j$ and $\mathrm{NP}(f)$ has integer slopes, the segment joining $(k_1', 0)$ and $(k_1' + k_2', k_2')$ is part of $\mathrm{NP}(f)$. This implies $k_2 \geq k_2'$, and by our initial assumption we also have $k_2 \leq k_2'$. Thus $k_2 = k_2'$. Further $k_1' \leq 5$, $k_1' + k_2' < 10$ and $k_2' \geq 3$ give the following subcases.

CASE 2.1: $k_2 = k_2' \geq 5$. We have $k_1 = k_1' \leq 4$. Thus, at least five $x_j$'s and five $y_j$'s are exactly divisible by 2 and at least one $x_j$ and one $y_j$ are divisible by 4. By taking $z = 2$ in (7), we get $2^{12} \mid C$, which is a contradiction. Thus, this case does not arise.

CASE 2.2: $k_2 = k_2' = 3$. Let us consider the following subcases.

CASE 2.2(i): $k_1' \leq 3$. Taking $z = 4$ in (7), we see that $2^{11} \mid C$.

CASE 2.2(ii): $k_1' = 5$. We translate $z$ by $z-2$ in the definition of $C_n$ given by (7). As this translation will not affect the value of $C$ (Corollary 1.3), let us consider the equivalent case when $k_1 = k_1' = 5$ and $k_2 = k_2' = 2$. Without loss of generality, assume that $x_i, y_i$ for $i \in \{6, 7\}$ are of the form 2 (mod 4).

For each of $\mathrm{NP}(f)$ and $\mathrm{NP}(g)$, the edge with slope 1 ends at $(7, 2)$. Thus the remaining edges to the right have slope at least 2, and we deduce that the rightmost points on each of the Newton polygons must be at or above $(10, 8)$.

Suppose the rightmost points of both $\mathrm{NP}(f)$ and $\mathrm{NP}(g)$ are at $(10, 8)$. Thus

$$T_1 = T_2 = \{(0,0), (1,0), (2,0), (3,0), (4,0), (5,0), \\ (6,1), (7,2), (8,4), (9,6), (10,8)\}.$$

Then Lemma 2.2 shows that the remaining $x_i$ and $y_i$ for $i \in \{8, 9, 10\}$ must be of the form 4 (mod 8). Substituting $z = y_8$ in (7) yields $2^{11} \mid C$.

Now let the rightmost point of $\mathrm{NP}(f)$ be $(10, 8)$ and that of $\mathrm{NP}(g)$ be above $(10, 8)$. By Lemma 2.8, we have $2^8 \parallel C$. Hence, we deduce that for $i \in \{6, 7\}$, $x_i, y_i$ are either of the form 2 (mod 8) or 6 (mod 8), and for $i \in \{8, 9, 10\}$, $x_i$'s are of the form 4 (mod 8) and $y_i$'s are of the form 0 or 4 (mod 8). If at least one of the $y_i$'s, say $y_8$, is of the form 4 (mod 8), then by putting $z = y_8$ in (7), we obtain $2^{11} \mid C$, a contradiction to $2^8 \parallel C$. Thus, we can assume that the $y_i$'s for $i \in \{8, 9, 10\}$ are of the form 0 (mod 8). By Lemma 2.5, we have $\sum_{i=6}^{10} x_i \equiv \sum_{i=6}^{10} y_i \pmod 8$. This implies that if both $x_6$ and $x_7$ are in the same congruence class (mod 8), then $y_6$ and $y_7$ cannot be. Similarly, if both $y_6$ and $y_7$ are in the same congruence class (mod 8), then $x_6$ and $x_7$ cannot be. Thus, without loss of generality, we have the following possibilities.

(i) Let $y_6$ be of the form 2 (mod 8) and $y_7$ be of the form 6 (mod 8). If both $x_6$ and $x_7$ are of the form 6 (mod 8), by putting $z = y_7$ in (7), we see that $2^9 \mid C$. If both $x_6$ and $x_7$ are of the form 2 (mod 8), putting $z = y_6$ in (7) yields $2^9 \mid C$, which contradicts $2^8 \parallel C$.

(ii) Let $x_6$ be of the form 2 (mod 8) and $x_7$ be of the form 6 (mod 8). If both $y_6$ and $y_7$ are of the form 2 (mod 8), by putting $z = x_6$ in (7) we get $2^9 \mid C$. If both $y_6$ and $y_7$ are of the form 6 (mod 8), by putting $z = x_7$ in (7), we obtain $2^9 \mid C$, which is a contradiction to $2^8 \parallel C$.

We now know that the rightmost points of NP$(f)$ and NP$(g)$ are at or above $(10, 9)$. If both rightmost points are at $(10, 9)$ or both are above $(10, 9)$, then by putting $z = 0$ in (7), we get $2^{10} \mid C$. Thus, we can assume that NP$(f)$ has the rightmost point $(10, 9)$, and NP$(g)$ has the rightmost point above $(10, 9)$. Thus

$$T_1 = \{(0,0), (1,0), (2,0), (3,0), (4,0), (5,0), (6,1), (7,2), (8,4), (9,6), (10,9)\}.$$

For each of NP$(f)$ and NP$(g)$, the edge with slope 1 ends at the point $(7, 2)$. Recall that the two points $(j, \nu_2(a_{10-j}))$ and $(j, \nu_2(b_{10-j}))$ agree for $j \in \{0, 1, \ldots, 9\}$. Since there is an edge of slope 2 joining the vertices $(7, 2)$ and $(9, 6)$ in $T_1$, we deduce that $(9, 6)$ is in $S_1$ and hence also in $S_2$. Since the slope of the line joining $(5, 0)$ and $(7, 2)$ in $T_2$ is 1 and $k'_2 = 2$, we have $(9, 6) \in T_2$ as well. Thus, we deduce that $x_6, x_7, y_6, y_7$ are of the form 2 (mod 4), $x_8, x_9, y_8, y_9$ are of the form 4 (mod 8), $x_{10}$ is of the form 8 (mod 16) and $y_{10}$ is of the form 0 (mod 16). Putting $z = y_8$ in (7), we get $2^{10} \mid C$ as desired.

Case 2.2(iii): $k'_1 = 4$. For each of NP$(f)$ and NP$(g)$, the edge with slope 1 ends at $(7, 3)$. Thus, the remaining edge(s) to the right have slope at least 2, and therefore the rightmost point on each of the Newton polygons must be at or above $(10, 9)$. Therefore, we have the following possibilities.

Let the rightmost points of both NP$(f)$ and NP$(g)$ be $(10, 9)$. Then exactly three $x_j$'s and three $y_j$'s are of the form 4 (mod 8) and so setting $z = 4$ in (7) we derive $2^{12} \mid C$, which is a contradiction.

Let NP$(f)$ have the rightmost point $(10, 9)$ and NP$(g)$ have the rightmost point above $(10, 9)$. Thus

$$T_1 = \{(0,0), (1,0), (2,0), (3,0), (4,0), (5,1), (6,2), (7,3), (8,5), (9,7), (10,9)\}.$$

Then there are three $x_j$'s, say $x_8, x_9, x_{10}$, of the form 4 (mod 8). Recall that $a_1 = \sum_{j=1}^{10} X_j$, where $X_i = \prod_{j=1,\, j\neq i}^{10} x_j$, which implies

$$a_1 = 2^9 \times (\text{even}) + 2^8 \times (\text{odd}) + 2^7 \times (\text{odd}).$$

Therefore, $\nu_2(a_1) = 7$ and hence $(9, 7) \in S_1 \cap S_2$. Since $(7, 3) \in T_1 \cap T_2$ and the edge with slope 1 ends at $(7, 3)$, we deduce that also $(9, 7) \in T_2$. Thus the line segment joining $(7, 3)$ to $(9, 7)$ is common to both the Newton polygons of $f(z)$ and $g(z)$. Therefore, at least two $y_j$'s are of the form 4 (mod 8), say $y_8$ and $y_9$. By setting $z = y_8$ in (7), we get $2^{12} \mid C$, which is a contradiction.

If the rightmost endpoints of the Newton polygons of $f(z)$ and $g(z)$ are at or above $(10, 10)$, then by taking $z = 0$ in (7), we have $2^{10} \mid C$, as desired.

CASE 2.3: $k_2 = k_2' = 4$. Let us consider the following subcases based on $k_1$.

CASE 2.3(i): $k_1 \leq 4$. By taking $z = 2$ in (7), we have $2^{10} \mid C$.

CASE 2.3(ii): $k_1 = 5$. We translate $z$ to $z-2$ in (7), and further consider the equivalent case $k_1 = k_1' = 5$ and $k_2 = k_2' = 1$.

For each of $\mathrm{NP}(f)$ and $\mathrm{NP}(g)$, the edge with slope 1 ends at $(6, 1)$. Thus, the remaining edge(s) to the right have slope at least 2, and therefore the rightmost points on each of the Newton polygons must be at or above $(10, 9)$. If the rightmost points of both $\mathrm{NP}(f)$ and $\mathrm{NP}(g)$ are $(10, 9)$ or both are above $(10, 9)$, then by taking $z = 0$ in (7), we have $2^{10} \mid C$. Therefore, we can assume that the rightmost point of $\mathrm{NP}(f)$ is $(10, 9)$ and the one of $\mathrm{NP}(g)$ is above $(10, 9)$. By Lemma 2.8, this implies

$$2^9 \parallel C. \tag{12}$$

Thus we have established that $9 \leq \nu_2(\overline{C}_{10}) \leq 11$ as stated in Theorem 1.

We are interested in finding more information about the divisibility properties of $x_j$ and $y_j$ when there is a possible ideal solution with $2^9 \parallel C$. These divisibility properties can be helpful in finding such an ideal solution, if one exists. Recall from Remark 1.4 that finding such an example will imply in Theorem 1 that $\nu_2(\overline{C}_{10}) = 9$.

If there is at least one $y_j$ that is exactly divisible by 4, then by taking $z = y_j$ in (7), we get $2^{13} \mid C$, a contradiction. Thus, $x_i$ and $y_i$ are odd for $1 \leq i \leq 5$ and

$$2 \parallel x_6, \quad 2^2 \parallel x_7, x_8, x_9, x_{10} \quad \text{and} \quad 2 \parallel y_6, \quad 8 \mid y_7, y_8, y_9, y_{10}. \tag{13}$$

Let us take $z = x_6$ in (7). Then using (12) and (13), we derive $x_6 \equiv y_6 \pmod{32}$. Further, using the vertices of $\mathrm{NP}(g)$, we derive

$$\begin{aligned} \nu_2(b_{10-j}) &\geq 3(j-6)+1 \quad && \text{for } 7 \leq j \leq 10, \\ \nu_2(a_{10-j}) &= \nu_2(b_{10-j}) && \text{for } 7 \leq j \leq 9. \end{aligned} \tag{14}$$

Define $u_j$ and $v_j \in \mathbb{Z}$ by the equations

$$\prod_{i=7}^{10}(z - x_i) = \sum_{j=0}^{4} u_j z^j \quad \text{and} \quad \prod_{i=7}^{10}(z - y_i) = \sum_{j=0}^{4} v_j z^j.$$

Also, $\prod_{i=1}^{5}(z-x_i) \equiv \prod_{i=1}^{5}(z-y_i) \equiv (z-1)^5 \pmod 2$. Then

$$\sum_{j=0}^{10} a_j z^j = (z-x_6)\prod_{i=1}^{5}(z-x_i)\sum_{j=0}^{4} u_j z^j,$$
$$\sum_{j=0}^{10} b_j z^j = (z-y_6)\prod_{i=1}^{5}(z-y_i)\sum_{j=0}^{4} v_j z^j.$$

Further, we have $\nu_2(a_0) = 9$ and $\nu_2(b_0) \geq 13$. Therefore,

$$\prod_{i=1}^{6}(z-x_i) = z^6 + \cdots + z^3 \times (\text{even}) + z^2 \times (\text{odd}) + z \times (\text{odd}) + x_6 \times (\text{odd}).$$

Using these equations, we deduce for $1 \leq j \leq 3$ that

$$a_j = u_j \times x_6 \times (\text{odd}) + u_{j-1} \times (\text{odd}) + u_{j-2} \times (\text{odd}) + u_{j-3} \times (\text{even}), \tag{15}$$

$$b_j = v_j \times x_6 \times (\text{odd}) + v_{j-1} \times (\text{odd}) + v_{j-2} \times (\text{odd}) + v_{j-3} \times (\text{even}). \tag{16}$$

Until the end of this subsection, let us assume that $j \in \{7, 8, 9, 10\}$. Since $4 \parallel x_j$, we write $x_j = 4x_j'$, where $x_j'$ is of the form $4k+1$ or $4k+3$. Observe that if $x_j'$ is of the form $4k+1$, then $x_j + 8 = 4(x_j' + 2) = 4x_j''$, where $x_j''$ is of the form $4k+3$. Therefore, we need to consider only the following subcases.

(i) Assume that there are exactly an even number of $x_j'$ of the form $4k+1$. We derive $\nu_2(u_1) \geq 8$ and $\nu_2(u_2) = 5$ and hence $\nu_2(a_2) = 6$ by (15) for $j = 2$ whereas from (14) we get $\nu_2(b_2) \geq 7$. Thus, this case does not arise.

(ii) Assume that there are exactly an odd number of $x_j'$ of the form $4k+1$. Note that if exactly three $x_j'$'s are of the form $4k+1$, then after translating $z$ to $z-8$ in (7), we can reduce it to the case when exactly one $x_j'$ is of the form $4k+1$. Let us further look at the divisibility of $y_j$ in this case. Recall from (13) that $8 \mid y_j$.

(a) If there are exactly an even number of $y_j$ of the form $8 \pmod{16}$, then using (16) for $b_3$, we have $\nu_2(b_3) \geq 5$. On the other hand, using (15) for $a_3$, we derive $\nu_2(a_3) = 4$, which is a contradiction.

(b) Assume that there are exactly an odd number of $y_j$ of the form $8 \pmod{16}$. If exactly three $y_j$'s are of the form $8 \pmod{16}$, then we get

$$\nu_2(v_0) \geq 13,\ \nu_2(v_1) = 9,\ \nu_2(v_2) = 6 \implies \nu_2(b_2) = 7 \quad \text{by (16).} \tag{17}$$

If exactly one $y_j$ is of the form $8 \pmod{16}$, then we get

$$\nu_2(v_0) \geq 15,\ \nu_2(v_1) = 11,\ \nu_2(v_2) \geq 7 \implies \nu_2(b_2) \geq 8 \quad \text{by (16).} \tag{18}$$

Depending on these conditions on $b_2$, we further derive the possible congruence classes of $x_j' \pmod 8$. Recall that we are in the case where one $x'_j$ is of the form $4k+1$ and the other three $x'_j$'s are of the form $4k+3$. Now $4k+1$ can be written as $8k+1$ or $8k+5$, and $4k+3$ can be written as $8k+3$ or $8k+7$. Observe that if $x'_j$ is of the form $8k+1$, then $x_j+16=4(x'_j+4)=4x''_j$, where $x''_j$ is of the form $8k+5$. If $x'_j$ is of the form $8k+3$, then $x_j+16=4(x'_j+4)=4x''_j$, where $x''_j$ is of the form $8k+7$. Therefore, without loss of generality, we consider the following subcases. Let exactly one $x'_j$ be of the form $8k+1$.

(I) Assume that exactly two $x'_j$'s are of the form $8k+3$ and one $x'_j$ is of the form $8k+7$ or all three remaining $x'_j$'s are of the form $8k+7$. In both cases, we deduce that $\nu_2(u_1)=7$, $\nu_2(u_2)\geq 7$, and hence $\nu_2(a_2)=7$. Therefore, using (14) and (17) we conclude that in both cases there must be exactly three $y_j$'s such that $8 \,\|\, y_j$.

(II) Assume that exactly two $x'_j$'s are of the form $8k+7$ and one $x'_j$ is of the form $8k+3$ or all three remaining $x'_j$'s are of the form $8k+3$. In both cases, we get $\nu_2(u_1)=7$ and $\nu_2(u_2)=6$ and therefore $\nu_2(a_2)\geq 8$. Using (14) and (18) we conclude that in both cases there must be exactly one $y_j$ such that $8 \,\|\, y_j$.

**4. Lower bound for $\nu_2(\overline{C}_{12})$.** Recall that we already have

$$8 \leq \nu_2(\overline{C}_{12}) \leq 12. \tag{19}$$

In this section we will increase the lower bound by proving that $11 \leq \nu_2(\overline{C}_{12}) \leq 12$.

As before, we consider (6); we set $n=12$ and we will be using $C$ for $\overline{C}_{12}$. The earlier notations $k_1, k'_1, k_2, k'_2$ will be followed in this section with $n=12$ and we consider multiple subcases depending on the possible values of $k'_1$ and $k'_2$. Using Remark 2.3 with $n=12$, we get $k'_1+k'_2\leq 12$, $k_1=k'_1\leq 6$, $k_2\leq k'_2$, $k'_2\geq 3$ and $k_2\equiv k'_2 \pmod 4$.

**4.1. Case 1: $k'_1+k'_2=12$.** As in Subsection 3.1, no element $y_j$ from $Y$ is divisible by 4, and since $k_2\leq k'_2$ we know that each point $(j,\nu_2(a_{10-j}))$ in $S_1$ is at or above the corresponding point $(j,\nu_2(b_{10-j}))$ in $S_2$. Further, $k'_1\leq 6$ will imply $k'_2=12-k'_1\geq 6$. Consider the following subcases.

Case 1.1: $k_2=k'_2$. Since $k_2=k'_2\geq 6$, by putting $z=2$ in (7) we get $2^{12}\mid C$.

Case 1.2: $k_2<k'_2$. In this case, $X$ must contain at least one $x_j$ that is divisible by 4, but we know that no $y_j$ is divisible by 4. We consider the cases $k_2=0$ and $k_2\neq 0$ separately.

Case 1.2(i): $k_2 \neq 0$. Then at least one $x_j$ is of the form $4k+2$, and hence, by taking $z = x_j$ in (7), we see that $2^{2k_2'} \mid C$. Since $k_2' \geq 6$, we get $2^{12} \mid C$.

Case 1.2(ii): $k_2 = 0$. Since $k_2' \geq 6$ and $k_2 \equiv k_2' \pmod 4$, we get $k_2' \in \{8, 12\}$. When $k_2' = 12$, we have $k_1' = k_1 = 0$. Thus, all $y_j$'s are divisible by 2 and all $x_j$'s are divisible by 4. By putting $z = 0$ in (7), we get $2^{12} \mid C$, as desired. Thus, it remains to consider $k_2 = 0$, $k_2' = 8$ and $k_1 = k_1' = 4$. In this case, the edges of the Newton polygon of $f(z)$ with positive slope have slope $\geq 2$. In particular, this implies

$$\begin{aligned} \nu_2(a_{12-j}) &\geq 2(j-4) \quad \text{for } 5 \leq j \leq 12, \\ \nu_2(b_{12-j}) &\geq 2(j-4) \quad \text{for } 5 \leq j \leq 11. \end{aligned} \tag{20}$$

We define $u_j \in \mathbb{Z}$ by the equation

$$\prod_{i=5}^{12}(z - y_i) = \sum_{j=0}^{8} u_j z^j. \tag{21}$$

Since $(z-y_1)(z-y_2)(z-y_3)(z-y_4) \equiv z^4 + 1 \pmod 2$, we have

$$\begin{aligned} b_j = u_j \times (\text{odd}) + u_{j-1} \times (\text{even}) + u_{j-2} \times (\text{even}) \\ + u_{j-3} \times (\text{even}) + u_{j-4} \times (\text{odd}) \quad \text{for } 1 \leq j \leq 7. \end{aligned} \tag{22}$$

Since $\nu_2(b_1) \geq 14$ from (20) and $\nu_2(u_0) = 8$, using (22) we get $\nu_2(u_1) \geq 9$. Using (20) and (22) successively, we get

$$\nu_2(u_2) \geq 9,\ \nu_2(u_3) \geq 9,\ \nu_2(u_4) \geq 8,\ \nu_2(u_5) \geq 6,\ \nu_2(u_6) \geq 4,\ \nu_2(u_7) \geq 2. \tag{23}$$

For $5 \leq j \leq 12$ we write $y_j = 2y_j'$, where $y_j'$ is odd. Consider the set $\{y_j' : 5 \leq j \leq 12\}$. Then $y_j'$ is of the form $4k+1$ or $4k+3$. Without loss of generality, we consider the following subcases.

(i) If all $y_j'$'s are of the form $4k+3$, then it follows from the definition of $u_4$ that $u_4 = 2^4 T(y_5', \ldots, y_{10}')$. Thus, by Lemma 2.8(i) we have $\nu_2(u_4) = 5$, which contradicts $\nu_2(u_4) \geq 8$ (see (23)).

(ii) If exactly two (or four) of $y_j'$'s are of the form $4k+3$, then by Lemma 2.8 we have $\nu_2(u_4) = 5$, an impossibility because of (23).

(iii) Assume that exactly one $y_j'$ is of the form $4k+3$. Then $u_6$, the coefficient of $z^6$ in (21), equals

$$u_6 = 2^2 \sum_{5 \leq i < j < k < l \leq 12} y_i' y_j' = 2^2 H(y_5', \ldots, y_{10}').$$

Using Lemma 2.8(iv), we have $\nu_2(u_6) = 3$, which contradicts the fact that $\nu_2(u_6) \geq 4$ by (23).

(iv) If exactly three $y'_j$'s are of the form $4k+3$, then a similar argument using Lemma 2.8(v) shows that $\nu_2(u_6) = 3$, again a contradiction to (23).

**4.2. Case 2: $k'_1+k'_2 < 12$.** In this case, at least one $y_j$ is of the form $y_j \equiv 0 \pmod 4$. Similarly to the arguments given in the introductory paragraph of Section 3.2, we derive $k_2 = k'_2$. Taking into account $k'_2 \geq 3$ we have $k_2 = k'_2 \geq 3$. Further, we consider subcases based on the values of $k'_1$.

CASE 2.1: $k'_1 \leq 5$. As $k'_1+k'_2 < 12$, at least one $x_j$ and at least one $y_j$ are divisible by 4. Furthermore, if $k_1 = k'_1 \leq 4$, then $k_2 = k'_2 \geq \lceil (n-k'_1)/2 \rceil = 4$. Thus, in this case, at least four $x_j$ and four $y_j$ are exactly divisible by 2. Hence taking $z = 2$ in (7) we see that $2^{12} \mid C$. If $k_1 = k'_1 = 5$, then $k_2 = k'_2 \geq \lceil (n-k'_1)/2 \rceil = 4$. Again taking $z = 2$ in (7) we get $2^{11} \mid C$. So we are left with the case when $k'_1 = 6$.

CASE 2.2: $k'_1 = 6$. We see that $3 \leq k'_2 \leq 5$.

CASE 2.2(i): $k'_2 = 5$. By putting $z = 2$ in (7) we get $2^{11} \mid C$.

CASE 2.2(ii): $k'_2 = 4$. We translate $z$ to $z-2$ in (7) and consider the equivalent case when $k_2 = k'_2 = 2$. Thus, we can assume that the $x_i, y_i$ are of the form $2 \pmod 4$ for $i \in \{7, 8\}$ and the $x_i, y_i$ are of the form $4 \pmod 8$ for $9 \leq i \leq 12$. Thus, we deduce that the rightmost points of $\mathrm{NP}(f)$ and of $\mathrm{NP}(g)$ must be at or above $(12, 10)$. If both rightmost points are at $(12, 10)$ or both are above $(12, 10)$, by putting $z = 0$ we get $2^{11} \mid C$. Thus, we can assume that $\mathrm{NP}(f)$ has the rightmost point $(12, 10)$, and $\mathrm{NP}(g)$ has the rightmost point above $(12, 10)$. Hence, $x_j$'s for $9 \leq j \leq 12$ are of the form $4 \pmod 8$. If some $y_j$ is of the form $4 \pmod 8$, then taking $z = y_j$, we get $2^{14} \mid C$, a contradiction by (19). Thus, we can assume that the $y_j$'s for $9 \leq j \leq 12$ are of the form $8 \pmod{16}$. This gives

$$\nu_2(b_{12-j}) \geq 3(j-8)+2 \quad \text{for } 9 \leq j \leq 12$$

and thus

$$\nu_2(a_{12-j}) \geq 3(j-8)+2 \quad \text{for } 9 \leq j \leq 11. \tag{24}$$

Since $x_j$'s for $1 \leq j \leq 6$ are odd, we obtain

$$\prod_{j=1}^{6}(z-x_j) = z^6 + \cdots + z^2 \times (\text{odd}) + z \times (\text{even}) + (\text{odd}).$$

As in Case 1.2, similarly to (21), we define $\tilde{u}_j \in \mathbb{Z}$ by the equation

$$\prod_{j=7}^{12}(z-x_j) = \sum_{j=0}^{6} \tilde{u}_j z^j$$

and thus

$$f(z) = \sum_{j=0}^{12} a_j z^j = \prod_{j=1}^{6}(z - x_j) \sum_{j=0}^{6} \tilde{u}_j z^j.$$

Hence $\nu_2(\tilde{u}_0) = 10$ and

$$a_1 = \tilde{u}_0 \times (\text{even}) + \tilde{u}_1 \times (\text{odd}),$$
$$a_2 = \tilde{u}_0 \times (\text{odd}) + \tilde{u}_1 \times (\text{even}) + \tilde{u}_2 \times (\text{odd}).$$

As earlier, we write $x_j = 2x'_j$ for $j \in \{7, 8\}$ and $x_j = 4x'_j$ for $9 \leq j \leq 12$, where the $x'_j$'s are odd. Consider the set $\{x'_j : 7 \leq j \leq 12\}$. Then the $x'_j$'s are of the form $4k+1$ or $4k+3$ where $k$ is an integer. Without loss of generality, we consider the following subcases.

(i) If all the $x'_j$'s are of the form $4k+1$, then $\nu_2(\tilde{u}_1) \geq 10$ and $\nu_2(\tilde{u}_2) = 7$, which implies $\nu_2(a_2) = 7$, contradicting (24).

(ii) Suppose exactly one $x'_j$ is of the form $4k+1$. If either $x'_7$ or $x'_8$ is of the form $4k+1$, we deduce that $\nu_2(\tilde{u}_2) = 7$, $\nu_2(\tilde{u}_1) \geq 10$ and hence $\nu_2(a_2) = 7$, contradicting (24). For $9 \leq j \leq 12$, if exactly one $x'_j$ is of the form $4k+1$, we deduce that $\nu_2(\tilde{u}_1) = 9$ and hence $\nu_2(a_1) = 9$, contradicting (24).

(iii) Assume that exactly two $x'_j$'s are of the form $4k+1$. If $x'_7$ and $x'_8$ are of the form $4k+1$, then $\nu_2(\tilde{u}_2) = 7$ and $\nu_2(\tilde{u}_1) \geq 10$, implying $\nu_2(a_2) = 7$, an impossibility by (24). For $9 \leq j \leq 12$, if exactly two $x'_j$'s are of the form $4k+1$, then $\nu_2(\tilde{u}_1) \geq 10$ and $\nu_2(\tilde{u}_2) = 7$. Therefore $\nu_2(a_2) = 7$, again a contradiction by (24). If either $x'_7$ or $x'_8$, and exactly one of the $x'_j$'s $(9 \leq j \leq 12)$ are of the form $4k+1$, then $\nu_2(\tilde{u}_1) = 9$. This implies that $\nu_2(a_1) = 9$, which contradicts (24).

(iv) Assume that exactly three $x'_j$'s are of the form $4k+1$. Let $x'_7, x'_8$ and exactly one of the $x'_j$'s $(9 \leq j \leq 12)$ be of the form $4k+1$. Then $\nu_2(\tilde{u}_1) = 9$ and hence $\nu_2(a_1) = 9$, contradicting (24). If exactly one of $x'_7$ and $x'_8$, and exactly two $x'_j$'s $(9 \leq j \leq 12)$ are of the form $4k+1$, then $\nu_2(\tilde{u}_1) \geq 10$ and $\nu_2(\tilde{u}_2) = 7$. Thus $\nu_2(a_2) = 7$, contradicting (24). If exactly three of $x'_j$'s $(9 \leq j \leq 12)$ are of the form $4k+1$, then $\nu_2(\tilde{u}_1) = 9$, which implies $\nu_2(a_1) = 9$, a contradiction to (24).

(v) Suppose exactly four $x'_j$'s are of the form $4k+1$. Let $x'_7, x'_8$, and exactly two $x'_j$'s $(9 \leq j \leq 12)$ be of the form $4k+1$. Then $\nu_2(\tilde{u}_1) \geq 10$ and $\nu_2(\tilde{u}_2) = 7$. Hence $\nu_2(a_2) = 7$, contradicting Equation (24). If exactly one of $x'_7$ and $x'_8$ and exactly three $x'_j$'s $(9 \leq j \leq 12)$ are of the form $4k+1$, then $\nu_2(\tilde{u}_1) = 9$, which implies that $\nu_2(a_1) = 9$, contradicting (24). If all $x'_j$'s $(9 \leq j \leq 12)$ are of the form $4k+1$, then $\nu_2(\tilde{u}_1) \geq 10$ and $\nu_2(\tilde{u}_2) = 7$, implying $\nu_2(a_2) = 7$, which contradicts (24).

(vi) Suppose exactly five $x'_j$'s are of the form $4k+1$. If both $x'_7$ and $x'_8$, and exactly three $x'_j$'s $(9 \leq j \leq 12)$ are of the form $4k+1$, then using

$\nu_2(\tilde{u}_1) = 9$ we derive $\nu_2(a_1) = 9$. This contradicts (24). If exactly one of $x'_7$ and $x'_8$ and exactly four $x'_j$'s $(9 \leq j \leq 12)$ are of the form $4k+1$, we see that $\nu_2(\tilde{u}_1) \geq 10$ and $\nu_2(\tilde{u}_2) = 7$. Thus, $\nu_2(a_2) = 7$, a contradiction.

Case 2.2(iii): $k'_2 = 3$. Then for each of $\mathrm{NP}(f)$ and $\mathrm{NP}(g)$, the edge with slope 1 ends at $(9,3)$ and the remaining edge(s) to the right have slope at least 2. Therefore, the rightmost point on each of the Newton polygons must be at or above $(12,9)$.

Suppose the rightmost endpoint of $\mathrm{NP}(f)$ is on $(12,9)$. Thus

$$\{(0,0),(1,0),(2,0),(3,0),(4,0),(5,0),(6,0),\\ (7,1),(8,2),(9,3),(10,5),(11,7),(12,9)\}$$

is the set of vertices of $\mathrm{NP}(f)$. Consider $a_1$, the coefficient of $z$ in $f(z)$. As the $x_i$ for $1 \leq i \leq 6$ are odd, $x_i \equiv 2 \pmod 4$ for $7 \leq i \leq 9$ and $x_i \equiv 4 \pmod 8$ for $10 \leq i \leq 12$, we derive

$$a_1 = 2^9 \times (\text{even}) + 2^8 \times (\text{odd}) + 2^7 \times (\text{odd})$$

and thus $\nu_2(a_1) = 7$. This implies $(11,7)$ belongs to $S_1$ and hence also to $S_2$. Since $k_2 = k'_2 = 3$, we know that $(9,3)$ is a point of $S_2$. Further, we know the slopes of $\mathrm{NP}(g)$ coming from edges joining with vertices $(9,3)$ onwards will have slope at least 2. Since the edges of the Newton polygon are joined in increasing order of slope, we deduce that $\mathrm{NP}(g)$ must contain an edge joining $(9,3)$ and $(11,7)$. This implies $4 \parallel y_{10}$ and $4 \parallel y_{11}$. Now, by substituting $z = y_{10}$ in (7), we get $2^{12} \mid C$.

Let the rightmost endpoint of $\mathrm{NP}(f)$ be $(12,10)$. The only possible vertices for $\mathrm{NP}(f)$ are

$$\{(0,0),(1,0),(2,0),(3,0),(4,0),(5,0),(6,0),\\ (7,1),(8,2),(9,3),(10,5),(11,7),(12,10)\}.$$

Since $(11,7) \in S_1 \cap S_2$ and $(9,3)$ is in $T_2$, we deduce that $(11,7) \in T_2$. Thus the possibilities for $\mathrm{NP}(g)$ are

$$\{(0,0),(1,0),(2,0),(3,0),(4,0),(5,0),(6,0),\\ (7,1),(8,2),(9,3),(10,5),(11,7),(12,r)\}$$

where $r \geq 10$.

Let the rightmost endpoint of $\mathrm{NP}(g)$ be $(12,r)$ where $r \geq 11$. Thus $2 \parallel x_i, y_i$ for $7 \leq i \leq 9$, $2^2 \parallel x_i, y_i$ for $i = 10, 11$, $2^3 \parallel x_{12}$ and $2^4 \mid y_{12}$. By substituting $z = x_{10}$ in (7), we get $2^{11} \mid C$, but from Lemma 2.7 we derive $2^{10} \parallel C$, a contradiction. Thus, the rightmost endpoint of $\mathrm{NP}(g)$ is $(12,10)$. Now, translating $z$ to $z-4$ in (7), we can further reduce this possibility to the case where the rightmost endpoints of $\mathrm{NP}(f)$ and $\mathrm{NP}(g)$ lie at or above $(12,11)$. In that case, if we take $z = 0$ in (7), we get $2^{11} \mid C$.

If the rightmost point of $\mathrm{NP}(f)$ is $(12, 11)$, then without loss of generality we can assume that the rightmost point of $\mathrm{NP}(g)$ is at or above $(12, 11)$. By taking $z = 0$ in (7) we conclude that $2^{11} \mid C$.

**Acknowledgements.** This work was initiated when the second author was visiting the Stat-Math Unit, Indian Statistical Institute, Bangalore, in July 2022. Both authors are grateful to Professor B. Sury for arranging the visit. The first and second authors express their gratitude to NBHM and SERB MATRICS Grant MTR/2022/000864, respectively, for the financial support of this work.

## References

[1] A. Alpers and R. Tijdeman, *The two-dimensional Prouhet–Tarry–Escott problem*, J. Number Theory 123 (2007), 403–412.

[2] B. Borchert, P. McKenzie, and K. Reinhardt, *Few product gates but many zeros*, in: Mathematical Foundations of Computer Science 2009, Lecture Notes in Computer Sci. 5734, Springer, Berlin, 2009, 162–174.

[3] P. Borwein, *Computational Excursions in Analysis and Number Theory*, CMS Books Math./Ouvrages Math. SMC 10, Springer, New York, 2002.

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

[5] T. Caley, *The Prouhet–Tarry–Escott problem*, Ph.D. thesis, Waterloo, ON, 2012.

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

[7] D. Coppersmith, M. J. Mossinghoff, D. Scheinerman, and J. M. VanderKam, *Ideal solutions in the Prouhet–Tarry–Escott problem*, Math. Comp. (online, 2023).

[8] L. E. Dickson, *History of the Theory of Numbers. Vol. II. Diophantine Analysis*, Chelsea, New York, 1971.

[9] G. Dumas, *Sur quelques cas d'irréductibilité des polynomes à coefficients rationnels*, J. Math. Pures Appl. 2 (1906), 191–258.

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

[11] K. Győry, L. Hajdu and R. Tijdeman, *Irreducibility criteria of Schur-type and Pólya-type*, Monatsh. Math. 163 (2011), 415–443.

[12] S. Hernández and F. Luca, *Integer roots chromatic polynomials of non-chordal graphs and the Prouhet–Tarry–Escott problem*, Graphs Combin. 21 (2005), 319–323.

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

[14] R. Maltby, *Pure product polynomials and the Prouhet–Tarry–Escott Problem*, Math. Comp. 66 (1997), 1323–1340.

[15] E. Rees and C. Smyth, *On the constant in the Tarry–Escott Problem*, in: Cinquante Ans de Polynômes (Paris, 1988), Lecture Notes in Math. 1415, Springer, Berlin, 1990, 196–208.

[16] A. Salomaa, *Subword balance, position indices and power sums*, J. Comput. System Sci. 76 (2010), 861–871.

[17] E. M. Wright, *On Tarry's problem (I)*, Quart. J. Math. 6 (1935), 261–267.

[18] E. M. Wright, *Prouhet's 1851 solution of the Tarry–Escott problem of 1910*, Amer. Math. Monthly 66 (1959), 199–201.

Ranjan Bera
Stat-Math Unit
ISI Bangalore
Bangalore, Karnataka, 560059, India
E-mail: ranjan.math.rb@gmail.com

Saranya G. Nair
Department of Mathematics
BITS Pilani
Zuarinagar, Goa, 403726, India
E-mail: saranyan@goa.bits-pilani.ac.in