Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 40 (1994)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: THE PROUHET-TARRY-ESCOTT PROBLEM REVISITED
Autor: Borwein, Peter / Ingalls, Colin
DOI: https://doi.org/10.5169/seals-61102

L'Enseignement Mathématique, t. 40 (1994), p. 3-27

THE PROUHET-TARRY-ESCOTT PROBLEM REVISITED

by Peter BORWEIN and Colin INGALLS

ABSTRACT. The old problem of Prouhet, Tarry, Escott and others asks one to find two distinct sets of integers $\{\alpha_1, \ldots, \alpha_n\}$, and $\{\beta_1, \ldots, \beta_n\}$ with

$$\alpha_1^m + \cdots + \alpha_n^m = \beta_1^m + \cdots + \beta_n^m$$

for $m = 1, \ldots, k$ (with the most interesting case being $k = n - 1$). We review some elementary properties of solutions and examine the fine structure of 'ideal' and 'symmetric ideal' solutions. The relationship of this problem to the 'easier' Waring problem and a problem of Erdős and Szekeres of minimizing the norm of a product of cyclotomic polynomials on the unit disk is then discussed. We present some new bounds for this problem and for the Prouhet-Tarry-Escott problem of small size. We also present an algorithm for calculating symmetric ideal p-adic solutions of the the Prouhet-Tarry-Escott problem.

1. INTRODUCTION

A classic problem in Diophantine Analysis that occurs in many guises is the Prouhet-Tarry-Escott problem. This is the problem of finding two distinct sets of integers $\{\alpha_1, \ldots, \alpha_n\}$, $\{\beta_1, \ldots, \beta_n\}$ such that

$$\begin{aligned}
\alpha_1 + \cdots + \alpha_n &= \beta_1 + \cdots + \beta_n \\
\alpha_1^2 + \cdots + \alpha_n^2 &= \beta_1^2 + \cdots + \beta_n^2 \\
&\vdots \quad \vdots \quad \vdots \\
\alpha_1^k + \cdots + \alpha_n^k &= \beta_1^k + \cdots + \beta_n^k .
\end{aligned}$$

Classification Numbers: 11-04, 11D41. Key Words: Diophantine Equations, Tarry, Escott, Prouhet, Waring Problem.

This we will call the Prouhet-Tarry-Escott Problem. We call n the size of the solution and k the degree. We abbreviate the above system by writing $\{\alpha_i\} \overset{k}{=} \{\beta_i\}$ and reserve α_i and β_i as integer variables.

This problem has a long history and is, in some form, over 200 years old. In 1750-51 Euler and Goldbach noted that

$$\{a, b, c, a + b + c\} \overset{2}{=} \{a + b, a + c, b + c\} .$$

A general solution of the problem for all degrees, but large sizes, came a century later in 1851 when Prouhet found that there are n^{k+1} numbers separable into n sets so that each pair of sets forms a solution of degree k and size n^k. Over the next 60 years some more parametric and specific solutions of degrees two, three, four and five were found. In the 1910's Tarry and Escott looked more closely at the problem and subsequently their names were attached to it. They found many specific solutions and provided a number of elementary general results. Prouhet's result, while the first general solution of the problem, was not properly noticed until 1959 when Wright [23] took exception to the problem being called the Tarry-Escott problem and drew attention to Prouhet's contribution in a paper called *Prouhet's 1851 Solution of the Tarry-Escott Problem of 1910.* More of the early history of the problem can be found in Dickson [5], where he refers to it as the problem of 'equal sums of like powers'.

The problem is called the problem of Prouhet and Tarry by Hua in his text [11], which is a good source of some of the elementary material. It has also been referred to as the Tarry problem. A good introductory paper [7] by Dorwart and Brown calls it the Tarry-Escott problem. Solutions are often called 'multigrades' as in Smyth [19].

While the Prouhet-Tarry-Escott problem is old it appears to have received only a little serious computational attention. So one particular aim is to provide some numerical insights and report the results of various computations. We computed extensively on the size 7 and size 11 cases of the problem. Eleven is of particular interest because it is the first unresolved case and we found that "no symmetric ideal" solutions exist with all $\{\alpha_i\}$ and $\{\beta_i\}$ of relatively small size ($\leqslant 363$). This is discussed in Section 5 and an algorithm is presented.

We also computed extensively on an old and related problem of Erdős and Szekeres that concerns the norms of products of cyclotomic polynomials. This is discussed and many new bounds for small sizes are given in section 4.2.

Section 2 of this paper collects together some of the elementary theory.

Section 3 then focuses on the most interesting minimal case of $n = k + 1$. The known solutions are presented and Smyth's attractive recent treatment of the largest known case ($n = 10$) is discussed. In these minimal cases a solution must have considerable additional structure.

Two related problems are discussed in Section 4. One is due to Erdős and Szekeres the other due to Wright. Both have been open for decades.

Section 6 presents some of the many open problems directly related to these matters.

2. Elementary Properties

The problem can be stated in three equivalent ways. This is an old result as are most of the results of this section in some form or another. (See for example [7], [11].) In various contexts it is easier to use different forms of the problem.

PROPOSITION 1. *The following are equivalent:*

$$\sum_{i=1}^{n} \alpha_i^j = \sum_{i=1}^{n} \beta_i^j \quad \text{for} \quad j = 1, \ldots, k \tag{1}$$

$$\deg\left(\prod_{i=1}^{n} (x - \alpha_i) - \prod_{i=1}^{n} (x - \beta_i)\right) \leqslant n - (k+1) \tag{2}$$

$$(x-1)^{k+1} \mid \sum_{i=1}^{n} x^{\alpha_i} - \sum_{i=1}^{n} x^{\beta_i}. \tag{3}$$

Proof. An application of Newton's symmetric polynomial identities shows the equivalence of (1) and (2). To prove the equivalence of (1) and (3) apply xd/dx to equation (3) and evaluate at one $k + 1$ times. □

A solution of the Prouhet-Tarry-Escott problem generates a family of solutions by the following lemma. Any solutions that can be derived from each other in this manner are said to be equivalent.

LEMMA 1. *If* $\{\alpha_1, \ldots, \alpha_n\}, \{\beta_1, \ldots, \beta_n\}$ *is a solution of degree* k, *then so is* $\{M\alpha_1 + K, \ldots, M\alpha_n + K\}, \{M\beta_1 + K, \ldots, M\beta_n + K\}$ *for arbitrary integers* M, K.

Proof. The second form of the problem is clearly preserved when the polynomials $\prod_{i=1}^{n}(x - \alpha_i)$ and $\prod_{i=1}^{n}(x - \beta_i)$ are scaled and translated by integer constants. □

We are particularly interested in the solutions of small size and we define $N(k)$ to be the least integer n such that there is a solution of size n and degree k. We immediately get the following proposition.

PROPOSITION 2.

$$N(k) \geqslant k + 1 .$$

Proof. This follows from the second form of the problem since monic polynomials with identical coefficients have identical roots. □

Solutions of degree k and size $k + 1$ are called **ideal**. Ideal solutions are of particular interest since they are minimal solutions to the problem. We may use the following lemma to obtain an upper bound for $N(k)$, and to construct solutions of high degree.

LEMMA 2. *If* $\{\alpha_1, \ldots, \alpha_n\} \overset{k}{=} \{\beta_1, \ldots, \beta_n\}$ *then*

$$\{\alpha_1, \ldots, \alpha_n, \beta_1 + M, \ldots, \beta_n + M\} \overset{k+1}{=} \{\alpha_1 + M, \ldots, \alpha_n + M, \beta_1, \ldots, \beta_n\}$$

for any integer M.

Proof. This follows upon multiplying (3) by $(x^M - 1)$. □

COROLLARY 1.

$$N(k) \leqslant C2^k .$$

Proof. Simply use Lemma 2 and choose M so large that there are no common elements in the two sets. □

As will be shown later $N(k) = k + 1$ for $k = 1, \ldots, 9$ so we can choose C to be $10/2^9$ for $k \geqslant 9$, but this is unnecessary in light of the next proposition.

PROPOSITION 3.

$$N(k) \leqslant \frac{1}{2} k(k + 1) + 1 .$$

Proof. Let $n > s^k s!$ and

$$A = \{(\alpha_1, \ldots, \alpha_s) : 1 \leqslant \alpha_i \leqslant n \quad \text{for } i = 1, \ldots, s\} .$$

There are n^s members of A. Consider the relation $\sim$ defined on A by $(\alpha_i) \sim (\beta_i)$ iff $(\alpha_i) := (\alpha_1, \ldots, \alpha_s)$ is a permutation of $(\beta_i) := (\beta_1, \ldots, \beta_s)$.

There are at least $n^s/s!$ distinct equivalence classes in $A/\sim$ since each $(\alpha_1, \ldots, \alpha_s)$ has at most $s!$ different permutations. Let

$$s_j((\alpha_i)) = \alpha_1^j + \cdots + \alpha_s^j \quad \text{for } j = 1, \ldots, k .$$

Note that

$$s \leqslant s_j((\alpha_i)) \leqslant sn^j$$

so there are at most

$$\prod_{j=1}^{k} (sn^j - s + 1) < s^k n^{\frac{k(k+1)}{2}}$$

distinct sets $(s_1((\alpha_i)), \ldots, s_k((\alpha_i)))$. We may now choose $s = \frac{1}{2}k(k+1) + 1$ and we have

$$s^k n^{\frac{k(k+1)}{2}} = s^k n^{s-1} < \frac{n^s}{s!}$$

since $n > s^k s!$. So the number of possible $(s_1((\alpha_i)), \ldots, s_k((\alpha_i)))$ is less than the number of distinct (α_i) and we may conclude that two distinct sets $\{\alpha_1, \ldots, \alpha_s\}$ and $\{\beta_1, \ldots, \beta_s\}$ form a solution of degree k. □

Slightly stronger upper bounds are discussed in [22] and [15], but they are much more difficult to establish and only improve the estimates to

$$N(k) \leqslant \begin{cases} \frac{1}{2}(k^2 - 3) & k \text{ odd} \\ \frac{1}{2}(k^2 - 4) & k \text{ even} . \end{cases}$$

We can also define $M(k)$ to be the least s such that there is a solution of size s and degree exactly k and no higher. Hua in [11] shows

$$M(k) \leqslant (k+1)\left(\frac{\log \frac{1}{2}(k+2)}{\log(1 + \frac{1}{k})} + 1\right) \sim k^2 \log k .$$

This is also a considerably harder argument than the above bound for $N(k)$.

3. Ideal and Symmetric Ideal Solutions

We explore some of the properties of ideal solutions. On occasion we add still more structure by requiring symmetric solutions. The notion of symmetry depends on the parity of the degree of the solution. Only ideal symmetric solutions are defined below, but one may easily define symmetric solutions for arbitrary degree.

An **even ideal symmetric solution** of size $k+1$ and odd degree k is of the form $\{\pm\alpha_1, \ldots, \pm\alpha_{(k+1)/2}\}, \{\pm\beta_1, \ldots, \pm\beta_{(k+1)/2}\}$ and satisfies any of the following equivalent statements:

$$\sum_{i=1}^{(k+1)/2} \alpha_i^{2j} = \sum_{i=1}^{(k+1)/2} \beta_i^{2j} \quad \text{for} \quad j = 1, \ldots, \frac{k-1}{2}$$

$$\prod_{i=1}^{(k+1)/2} (x^2 - \alpha_i^2) - \prod_{i=1}^{(k+1)/2} (x^2 - \beta_i^2) = C \quad \text{for some constant } C$$

$$(1-x)^{k+1} \Big| \sum_{i=1}^{(k+1)/2} (x^{\alpha_i} + x^{-\alpha_i}) - \sum_{i=1}^{(k+1)/2} (x^{\beta_i} + x^{-\beta_i}) .$$

An **odd ideal symmetric solution** of size $k+1$ and even degree k is of the form $\{\alpha_1, \ldots, \alpha_{k+1}\}, \{-\alpha_1, \ldots, -\alpha_{k+1}\}$ and satisfies any of the following equivalent statements:

$$\sum_{i=1}^{k+1} \alpha_i^j = 0 \quad \text{for} \quad j = 1, 3, 5, .., k-1$$

$$\prod_{i=1}^{k+1} (x - \alpha_i) - \prod_{i=1}^{k+1} (x + \alpha_i) = C \quad \text{for some constant } C$$

$$(1-x)^{k+1} \Big| \sum_{i=1}^{k+1} x^{\alpha_i} - \sum_{i=1}^{k+1} x^{-\alpha_i} .$$

For non-ideal symmetric solutions the parity of the solution is named after the parity of the degree plus one.

COROLLARY 2. *If* $\{\alpha_1, \ldots, \alpha_n\}, \{\beta_1, \ldots, \beta_n\}$ *is an ideal solution and is ordered so that*

$$\alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_n \quad \textit{and} \quad \beta_1 \leqslant \beta_2 \leqslant \cdots \leqslant \beta_n$$

then

$$\alpha_1 \neq \beta_j \quad \textit{for any} \quad j$$

and

$$\alpha_1 < \beta_1 \leqslant \beta_2 < \alpha_2 \leqslant \alpha_3 < \beta_3 \leqslant \beta_4 < \alpha_4 \cdots$$

(where without loss we assume that $\alpha_1 < \beta_1$*).*

Proof. This is all known, and easily deduced in the following fashion. Consider the second form of the ideal solution in Proposition 1. This gives, for some constant C

$$\prod_{i=1}^{n} (x - \alpha_i) - \prod_{i=1}^{n} (x - \beta_i) = C .$$

So the polynomial $p(x) := \prod_{i=1}^{n} (x - \alpha_i)$ is just a shift of the polynomial $q(x) := \prod_{i=1}^{n} (x - \beta_i)$. The result is now most easily seen by considering the graph of $p(x)$ and the graph of $q(x) = p(x) - C$. Note that p and q have the same critical points and these critical points separate the zeros of both p and q. Note also that p and q never intersect. □

Symmetric ideal solutions are only known for sizes $n \leqslant 10$. Throughout this paper we call an odd symmetric ideal solution **perfect** if it forms a complete set of residues modulo n. Listed below are ideal symmetric solutions for sizes $2 \leqslant n \leqslant 10$, the odd symmetric solutions (with even degrees) are all perfect. These solutions are listed in abbreviated symmetric form. For example the solution for size 6 is

$$\{\pm 4, \pm 9, \pm 13\}, \{\pm 1, \pm 11, \pm 12\}$$

and the solution for size 5 is

$$\{-8, -7, 1, 5, 9\}, \{8, 7, -1, -5, -9\} .$$

2 $\{3\}, \{1\}$

3 $\{-2, -1, 3\}$

4 $\{3, 11\}, \{7, 9\}$

5 $\{-8, -7, 1, 5, 9\}$

6 $\{4, 9, 13\}, \{1, 11, 12\}$

7 $\{-51, -33, -24, 7, 13, 38, 50\}$

8 $\{2, 16, 21, 25\}, \{5, 14, 23, 24\}$

9 $\{-98, -82, -58, -34, 13, 16, 69, 75, 99\}$ and
$\{-169, -161, -119, -63, 8, 50, 132, 148, 174\}$

10 $\{436, 11857, 20449, 20667, 23750\}, \{12, 11881, 20231, 20885, 23738\}$ and
$\{133225698289, 189880696822, 338027122801, 432967471212, 529393533005\}$,
$\{87647378809, 243086774390, 308520455907, 441746154196, 527907819623\}$

Chernick discusses symmetric solutions up to size 8 in [4]. Sinha discusses some parametric ideal symmetric solutions in [18]. There are two solutions of

size 9 and two of size 10 listed; three of these were found in the 1940's by Letac and Gloden (see [10]). The last solution was found by Smyth who has shown in [19] that one can generate infinitely many solutions of size 10. There are no known ideal solutions, symmetric or otherwise, of size 11 or higher. It has been conjectured for a long time that such solutions exist for all n, although the only evidence appears to be the existence of solutions up to size 10.

Smyth's elegant treatment of size ten solutions follows as the next proposition.

PROPOSITION 4. *If* x, y *are rational solutions of* $x^2y^2 - 13x^2 - 13y^2 + 121 = 0$ *then*

$$\{\pm(4x+4y), \pm(xy+x+y-11), \pm(xy-x-y-11), \pm(xy+3x-3y+11), \pm(xy-3x+3y+11)\},$$

$$\{\pm(4x-4y), \pm(xy-x+y+11), \pm(xy+x-y+11), \pm(xy-3x-3y-11), \pm(xy+3x+3y-11)\}$$

gives rise to an ideal symmetric solution of size 10.

Proof. This is simply a calculation. After finding the coefficients of the difference of the polynomials in the second form of the problem, one sees that all but the constant coefficient are either zero or have $x^2y^2 - 13x^2 - 13y^2 + 121$ as a factor. This is easily done using a symbolic computation package. It is clear that rational solutions give rise to integer solutions on clearing denominators using Lemma 1. □

Smyth shows in [19] that there are infinitely many rational solutions to the biquadratic $x^2y^2 - 13x^2 - 13y^2 + 121 = 0$ which give rise to distinct symmetric ideal solutions of size 10. The two we have included in the preceding list correspond to

$$(x, y) = (153/61, 191/79)$$

and

$$(x, y) = (-296313/249661, -1264969/424999).$$

It is interesting to note that any such solution is also a non-symmetric ideal solution of size 5 with α_i, β_i all squares.

There are various results concerning the divisibility of

$$C_n := \prod_{i=1}^{n} (x - \alpha_i) - \prod_{i=1}^{n} (x - \beta_i)$$

where $\{\alpha_i\}, \{\beta_i\}$ is an ideal solution.

LEMMA 3. *If* $\{\alpha_i\}, \{\beta_i\}$ *is an ideal solution with* C_n *defined as above, then*

$$|C_n| = \left|\prod_{i=1}^{n} (\beta_j - \alpha_i)\right| = \left|\prod_{i=1}^{n} (\alpha_j - \beta_i)\right| = \left|\frac{\sum_{i=1}^{n} \alpha_i^n - \sum_{i=1}^{n} \beta_i^n}{n}\right|$$

$$= \left|\prod_{i=1}^{n} \alpha_i - \prod_{i=1}^{n} \beta_i\right|$$

for all j.

Proof. This is an easy calculation. □

PROPOSITION 5. *Suppose*

$$f(x) := \sum_{i=1}^{n} x^{\alpha_i} - \sum_{i=1}^{n} x^{\beta_i}$$

is divisible by

$$\prod_{i=1}^{k} (1 - x^{n_i}) .$$

Then

$$k! \prod_{i=1}^{k} n_i \Big| \sum_{i=1}^{n} \alpha_i^k - \sum_{i=1}^{n} \beta_i^k .$$

Proof. Let

$$G(x) = \frac{\sum_{i=1}^{n} x^{\alpha_i} - \sum_{i=1}^{n} x^{\beta_i}}{\prod_{i=1}^{k} (1 - x^{n_i})}$$

By assumption, the numerator and denominator of the above both have zeros of order k at 1. Thus we compute that

$$\lim_{x \to 1} G(x) = \frac{\sum_{i=1}^{n} \alpha_i^k - \sum_{i=1}^{n} \beta_i^k}{k! \prod_{i=1}^{k} n_i}$$

by repeated application of Hôpital's rule (applied to $xG(x)$). But $G(x)$ is a polynomial with integer coefficients so the result is proved. □

COROLLARY 3. *Suppose that* $\{\alpha_1, \ldots, \alpha_n\}, \{\beta_1, \ldots, \beta_n\}$ *is an ideal solution, then* $(n-1)! \mid C_n$.

Proof. This follows from the third form of the problem and the above Proposition, on observing that $(1 - x)^n \mid f(x)$. □

This corollary is due to Kleiman [12] and Wright [24].

PROPOSITION 6. *Let* $\{\alpha_i\}, \{\beta_i\}$ *be an ideal solution of size* n. *Let*

$$C_n := \prod_{i=1}^{n} (x - \alpha_i) - \prod_{i=1}^{n} (x - \beta_i)$$

as before. If p *is prime then*

$$p \mid C_n \quad \textit{iff} \quad (1 - x^p) \mid \sum_{i=1}^{n} x^{\alpha_i} - \sum_{i=1}^{n} x^{\beta_i}$$

Proof. Suppose $p^k \mid C_n$ but $p^{k+1} \nmid C_n$. Then

$$p^k \mid \prod_{i=1}^{n} (\beta_j - \alpha_i) \qquad j = 1, \ldots, n$$

and

$$p^k \mid \prod_{i=1}^{n} (\alpha_j - \beta_i) \qquad j = 1, \ldots, n\ .$$

In particular for each j

$$\alpha_j \equiv \beta_i \bmod p$$

has exactly k solutions (counting multiplicity, in the sense that $\alpha_j \equiv \beta_i \bmod p^s$ (but not mod p^{s+1}) counts as multiplicity s). Likewise, for each j

$$\beta_j \equiv \alpha_i \bmod p$$

has exactly k solutions. Now, suppose ζ is a primitive p^{th} root of unity then

$$\zeta^{\alpha_j} - \zeta^{\beta_i} = 0 \quad \text{if} \quad \alpha_j \equiv \beta_i \bmod p^s\ .$$

Thus since $\{\alpha_i\}$ and $\{\beta_i\}$ partition, by their congruences mod p, into sets of multiplicity k, we deduce that ζ is a root of

$$\sum_{i=1}^{n} x^{\alpha_i} - \sum_{i=1}^{n} x^{\beta_i}$$

and hence

$$(1 - x^p) \mid \sum_{i=1}^{n} x^{\alpha_i} - \sum_{i=1}^{n} x^{\beta_i}\ .$$

This, with Proposition 5, proves the statement. □

Rees and Smyth have proved many results on the divisibility in [17]. We state a few of their more interesting results and their summary of results in the form of a table.

PROPOSITION 7.

1. *If* p *is prime and* $pk < n$ *for* $k \geqslant 1$ *then* $p^{k+1} \mid C_n$.
2. *If* $p > 3$ *is prime and* $p = n$ *then* $p \mid C_n$.
3. *If* p *is prime and*

$$n + 2 \leqslant p < n + 2 + \frac{n-3}{6}$$

then $p \mid C_n$.

Proof. See [17]. □

We define

$$r_n := \gcd\{(C_n)/n!\}$$

where C_n ranges over all ideal solutions of size n. The following table demonstrates what is known about r_n.

n	r_n
2	1
3	2
4	$2 \cdot 3$
5	$2 \cdot 3 \cdot 5 \cdot 7$
6	$2^2 \cdot 3 \cdot 5 \mid r_6 \mid 2^3 \cdot 3 \cdot 5$
7	$3 \cdot 5 \cdot 7 \cdot 11 \mid r_7 \mid 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
8	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \mid r_8 \mid 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
9	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \mid r_9 \mid 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
10	$5 \cdot 7 \cdot 13 \mid r_{10} \mid 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 37 \cdot 53 \cdot 61 \cdot 79 \cdot 83 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 191$
11	$5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \mid r_{11}$

This table is in [17]. We have improved the upper bound for r_{10} by using Smyth's solution in [19].

If we restrict our attention to symmetric solutions we can obtain more divisors of r_n.

PROPOSITION 8. *For symmetric solutions we have*

$$19 \mid r_7, \quad 19 \mid r_{11}, \quad 17 \cdot 19 \mid r_{13}$$

Proof. This is a result of performing the calculation mod p and observing that $C_n \equiv 0 \bmod p$. □

It is interesting to observe that an ideal solution in its third form has a large factor

$$\prod (1 - x^{p_i}) .$$

This follows from Propositions 6 and 7. Hence the degree of this polynomial grows at least like $n^2/(2 \log n)$.

4. RELATED PROBLEMS

There are several related problems. We mention two.

4.1. THE 'EASIER' WARING PROBLEM

In [21] Wright stated, and probably misnamed, the following variation of the well known Waring problem. The problem is to find the least s so that for all n there are natural numbers $\{\alpha_1, \ldots, \alpha_s\}$ so that

$$\pm \alpha_1^k \pm \cdots \pm \alpha_s^k = n$$

for some choice of signs. We denote the least such s by $v(k)$. Recall that the usual Waring problem requires al positive signs. For arbitrary k the best known bounds for $v(k)$ derive from the bounds for the usual Waring problem. So to date, the "easier" Waring problem is not easier than the Waring problem. However, the best bounds for small k are derived in an elementary manner from solutions to the Prouhet-Tarry-Escott problem.

Suppose $\{\alpha_1, \ldots, \alpha_n\} \overset{k-2}{=} \{\beta_1, \ldots, \beta_n\}$. We see that

$$\sum_{i=1}^{n} (x + \alpha_i)^k - \sum_{i=1}^{n} (x + \beta_i)^k = Cx + D$$

where

$$C = k \left(\sum_{i=1}^{n} \alpha_i^{k-1} - \sum_{i=1}^{n} \beta_i^{k-1} \right)$$

and

$$D = \sum_{i=1}^{n} \alpha_i^k - \sum_{i=1}^{n} \beta_i^k .$$

We define $\Delta(k, C)$ to be the smallest s such that every residue mod C is represented by s positive and negative k^{th} powers. We also define $\Delta(k) = \max_C \Delta(k, C)$. Wright shows how to calculate $\Delta(k, C)$ and $\Delta(k)$ in [9].

LEMMA 4. *If*

$$\sum_{i=1}^{n} (x + \alpha_i)^k - \sum_{i=1}^{n} (x + \beta_i)^k = Cx + D$$

then

$$v(k) \leqslant 2n + \Delta(k, C) \leqslant 2n + \Delta(k) .$$

Proof. This follows directly from the above definitions. □

PROPOSITION 9.

$$v(k) \leqslant 2M(k-2) + \Delta(k) \leqslant 2(k-1)\left(\frac{\log \frac{1}{2}(k)}{\log\left(1 + \frac{1}{k-2}\right)} + 1\right) + \begin{cases} \frac{1}{2}(3k-1) & k \text{ odd} \\ 2k & k \text{ even} . \end{cases}$$

Proof. This follows from the fact that

$$\Delta(k) \leqslant \begin{cases} \frac{1}{2}(3k-1) & k \text{ odd} \\ 2k & k \text{ even} \end{cases}$$

which is established in [22], and Lemma 4, and Hua's bound for $M(k)$ in [11]. Note that we must use $M(k)$ and not $N(k)$ since we require exact solutions so that $C \neq 0$. □

The best bounds for small k are derived from the above lemma using specific solutions of the Prouhet-Tarry-Escott problem and careful computation of $\Delta(k, C)$. In the following table we represent solutions as in the third form of the problem, and we define

$$[n_1, \ldots, n_k] := \prod_{i=1}^{k} (1 - x^{n_i})$$

$$g := 1 - x + x^3 + x^5 - x^4 + x^{10} + x^{27} + x^{17} - x^{26} - x^{23} + x^{22} + x^{24}$$

$$h := x + x^{25} + x^{31} + x^{84} + x^{87} + x^{134} + x^{158} + x^{182} + x^{198} - x^2 - x^{18} - x^{42} - x^{66} - x^{113} - x^{116} - x^{169} - x^{175} - x^{199}$$

k	bound for $v(k)$	solution
7	14	[1, 1, 2, 3, 4, 5]
8	30	$[3, 5, 7, 11, 13, 17, 19] \cdot g$
9	29	[1, 2, 3, 5, 7, 8, 11, 13]
10	30	h
11	28	[1, 2, 3, 4, 5, 7, 9, 11, 13, 17]
12	37	[1, 2, 3, 5, 7, 8, 9, 11, 13, 17, 19]
13	39	[1, 2, 3, 5, 6, 7, 8, 9, 11, 13, 17, 19]
14	53	[1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 13, 17, 19]
15	69	[1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 13, 15, 17, 19]
16	92	[1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 15, 16, 17, 19]
17	72	[1, 1, 2, 3, 4, 5, 6, 7, 7, 8, 9, 10, 11, 13, 17, 19]
18	86	[1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, 16, 17, 19, 23, 29]
19	88	[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 14, 16, 17, 19, 22, 23]
20	120	[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 15, 17, 19, 21, 23, 25, 29]

This table is from [9] and [24] as are most of the results of this section. Some of the bounds are improved by using Wright's calculation of $\Delta(k)$ and our solutions of smaller size.

4.2. A Problem of Erdős and Szekeres

We call a solution $\{\alpha_1, \ldots, \alpha_n\}, \{\beta_1, \ldots, \beta_n\}$ of the Prouhet-Tarry-Escott problem a **pure product** if

$$\sum_{i=1}^{n} z^{\alpha_i} - \sum_{i=1}^{n} z^{\beta_i} = \prod_{i=1}^{k} (1 - z^{n_i})$$

for some $n_1, \ldots, n_k$. Note that pure products are obtained from ideal solutions of degree zero by applying Lemma 2 repeatedly. These are a very restricted class of solutions of the Prouhet-Tarry-Escott Problem.

Proposition 10. *If*

$$\sum_{i=1}^{n} z^{\alpha_i} - \sum_{i=1}^{n} z^{\beta_i} = \prod_{i=1}^{k} (1 - z^{n_i})$$

then $\{\alpha_i\}, \{\beta_i\}$ *is equivalent to a symmetric solution of degree* k *and size* n.

Proof. Note that symmetry in the third form of the problem requires

$$f(z) = \sum_{i=1}^{n} z^{\alpha_i} - \sum_{i=1}^{n} z^{\beta_i} = (-1)^k f(1/z) .$$

The appropriate equivalent solution can be shown to satisfy this condition. □

For $f(z) = \prod_{i=1}^{k}(1 - z^{n_i}) = \sum_{i=0}^{n} \alpha_i z^i$, where $n = \deg f$, we define the norms

$$\| f \|_1 = \sum_{i=0}^{n} | \alpha_i |$$

$$\| f \|_2 = \left(\sum_{i=0}^{n} \alpha_i^2 \right)^{1/2} = \left(\frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta})^2 d\theta \right)^{1/2}$$

$$\| f \|_\infty = \sup_{|z|=1} | f(z) | .$$

We observe that $\| f \|_1$ is twice the size of the solution $\{\alpha_i\}, \{\beta_i\}$ of the Prouhet-Tarry-Escott problem.

LEMMA 5.

$$\frac{\| f \|_1}{\sqrt{\deg f + 1}} \leqslant \| f \|_2 \leqslant \| f \|_\infty \leqslant \| f \|_1 \leqslant \| f \|_2^2 .$$

Proof. This is all easily established. It all follows from well known inequalities and the fact that the coefficients of f are integers. □

In 1958 [8] Erdős and Szekeres formulated the problem of finding

$$A(k) = \min_{n_1, \ldots, n_k} \left\| \prod_{i=1}^{k} (1 - z^{n_i}) \right\|_\infty$$

They have conjectured that $A(k) \geqslant k^C$ for any C. There has been very little progress in this pretty old problem. Though an interesting and possibly related problem is solved in [2]. See Section 6.

We can use pure product solutions of the Prouhet-Tarry-Escott problem to find upper bounds for $A(k)$. These are not good general bounds, but we do find good upper bounds for small values of k using specific solutions. The following table was derived using various greedy algorithms to find the $\{n_i\}$.

k	$\|f\|_1$	$\{n_1, \ldots, n_k\}$
1	2	$\{1\}$
2	4	$\{1, 2\}$
3	6	$\{1, 2, 3\}$
4	8	$\{1, 2, 3, 4\}$
5	10	$\{1, 2, 3, 5, 7\}$
6	12	$\{1, 1, 2, 3, 4, 5\}$
7	16	$\{1, 2, 3, 4, 5, 7, 11\}$
8	16	$\{1, 2, 3, 5, 7, 8, 11, 13\}$
9	20	$\{1, 2, 3, 4, 5, 7, 9, 11, 13\}$
10	24	$\{1, 2, 3, 4, 5, 7, 9, 11, 13, 17\}$
11	28	$\{1, 2, 3, 5, 7, 8, 9, 11, 13, 17, 19\}$
12	36	$\{1, \ldots, 9, 11, 13, 17\}$
13	48	$\{1, \ldots, 9, 11, 13, 17, 19\}$
14	56	$\{1, \ldots, 7, 9, 10, 11, 13, 15, 16, 17\}$
15	60	$\{1, \ldots, 7, 9, 10, 11, 13, 15, 16, 17, 19\}$
16	60	$\{1, \ldots, 11, 13, 15, 17, 19, 23\}$
17	68	$\{1, \ldots, 7, 9, 10, 11, 13, 14, 16, 17, 19, 23, 29\}$
18	84	$\{1, \ldots, 11, 13, 14, 16, 17, 19, 22, 23\}$
19	100	$\{1, \ldots, 11, 13, 15, 17, 19, 21, 23, 25, 29\}$
20	116	$\{1, \ldots, 11, 13, 15, 17, 19, 21, 23, 25, 27, 31\}$
21	130	$\{1, \ldots, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}$
22	140	$\{1, \ldots, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 37\}$
23	156	$\{1, \ldots, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 37\}$
24	204	$\{1, \ldots, 7, 9, 10, 11, 13, 15, 16, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37\}$
25	188	$\{1, \ldots, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 41\}$
26	228	$\{1, \ldots, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41\}$
27	276	$\{1, \ldots, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41\}$
28	336	$\{1, \ldots, 13, 15, 17, 18, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41\}$
29	392	$\{1, 1, 2, 2, \ldots, 27\}$
30	432	$\{1, 1, 1, 2, \ldots, 28\}$

k	$\|f\|_1$	$\{n_1, \ldots, n_k\}$
40	1900	{1, 2, 2, ..., 17, 19, ..., 29, 31, ..., 37, 43, 47, 49, 49}
41	1348	{1, 2, 2, ..., 17, 19, ..., 29, 31, ..., 38, 40, 43, 49, 53}
42	1936	{1, 2, 2, ..., 17, 19, ..., 29, 31, ..., 38, 40, 43, 47, 52, 53}
43	2396	{1, 2, 2, ..., 17, 19, ..., 29, 31, ..., 38, 40, 43, 46, 52, 53, 60}
44	2492	{1, 2, 2, ..., 29, 31, ..., 38, 40, 43, 46, 52, 53, 60}
45	2684	{1, 2, 2, ..., 29, 31, ..., 38, 40, 43, 44, 46, 52, 53, 60}
46	2336	{1, 2, 2, ..., 29, 31, ..., 38, 40, 43, 44, 46, 48, 52, 53, 60}
47	3196	{1, 2, 2, ..., 29, 31, ..., 38, 40, 40, 43, 44, 46, 48, 52, 53, 60}
48	4080	{1, 2, 2, ..., 29, 31, ..., 38, 40, 40, 43, 44, 46, 48, 50, 52, 53, 60}
49	4086	{1, 2, 2, ..., 29, 31, ..., 38, 40, 40, 43, 44, 46, 48, 50, 52, 53, 55, 60}
50	5088	{1, 2, 2, ..., 29, 31, ..., 38, 40, 40, 43, 44, 46, 48, 49, 50, 52, 53, 55, 60}
51	5480	{1, 2, 2, ..., 29, 31, ..., 38, 40, 40, 43, 44, 46, 48, 49, 50, 52, 53, 55, 56, 60}
52	5296	{1, ..., 11, 13, 16, 17, 24, 52, ..., 56, ..., 58, 80, 82, 83, 84, 86, 88, 89, 92, 95, 100}
53	6000	{1, ..., 11, 13, 16, 17, 24, 52, 53, 54, 56, 58, ..., 80, 82, 83, 84, 86, 88, 89, 90, 92, 95, 100, 142}
54	7352	{1, 1, 2, 2, ..., 29, 31, ..., 38, 40, 42, 43, 44, 46, 48, ..., 53, 55, 56, 60}
55	5044	{1, 1, 2, 2, ..., 29, 31, ..., 38, 40, 42, 43, 44, 46, ..., 56, 60}
56	7536	{1, 1, ..., 11, 13, 16, 17, 24, 52, 53, 54, 56, 58, ..., 80, 82, ..., 92, 95, 100}
57	7156	{1, 1, ..., 11, 13, 16, 17, 24, 52, ..., 56, 58, ..., 80, 82, ..., 92, 95, 100}
58	6268	{1, 1, 2, 2, ..., 29, 31, ..., 38, 41, ..., 44, 46, ..., 60}
59	7572	{1, 1, ..., 11, 13, ..., 17, 24, 52, ..., 52, 58, ..., 80, 82, ..., 92, 95, 100}
60	10848	{1, 1, ..., 11, 13, ..., 17, 24, 52, ..., 56, 58, ..., 80, 82, ..., 92, 95, 100, 100}
80	1629900	{1, ..., 73, 90, ..., 95, 97}
100	41947220	{1, ..., 89, 107, ..., 117}

For $k = 1, 2, 3, 4, 5, 6$, and 8 these products are ideal solutions and therefore also optimal. These may well be the only k for which pure products give ideal solutions. We computed extensively on degree 6 ($k = 7$) and could not find a degree 6 product with $\|f\|_1 = 14$. Since $\|f\|_1$ is always an even integer we therefore conjecture that the minimum attainable is 16 (as above). For larger k there is no reason to believe that we have found minimal examples. This table also provides some good bounds for $N(k)$. For example $N(29) \leqslant 216$ which is much better than the bound of 419 that derives from the discussion following Proposition 3. There are many partial results on the Erdős-Szekeres problem

to be found in [8], [1], [6], [14], [3], [20], [2], [16] and [13]. We give one such new result here.

We now construct an easy example to show that we cannot in general expect exponential growth of the norms of the partial products of $\prod_{i=1}^{\infty}(1-z^{\beta_i})$ on the unit disk. From this point on, $\|f\|$ without a subscript will denote $\|f\|_\infty$.

LEMMA 6. *Let* $1 \leqslant \beta_1 < \beta_2 < \ldots$ *and let*

$$W_n(z) = \prod_{1 \leqslant i < j \leqslant n} (1 - z^{\beta_j - \beta_i})$$

then

$$\| W_n(z) \| \leqslant n^{\frac{n}{2}}.$$

Proof. We can explicitly evaluate the Vandermonde determinant

$$D_n := \prod_{1 \leqslant i < j \leqslant n} (z^{\beta_j} - z^{\beta_i}) = \begin{vmatrix} 1 & z^{\beta_1} & \cdots & z^{(n-1)\beta_1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & z^{\beta_n} & \cdots & z^{(n-1)\beta_n} \end{vmatrix}$$

and by Hadamard's inequality, since each entry of the matrix has modulus at most one in the unit disk,

$$\| D_n \| \leqslant n^{n/2}.$$

Thus

$$\left\| \prod_{1 \leqslant i < j \leqslant n} (1 - z^{\beta_j - \beta_i}) \right\| = \left\| \prod_{1 \leqslant i < j \leqslant n} (z^{\beta_j} - z^{\beta_i}) \right\| \leqslant n^{n/2}. \qquad \square$$

Observe, as Dobrowolski did in [6], that if we take $\beta_i = i$, we deduce that

$$\left\| \prod_{i=1}^{n} (1 - z^i)^{n-i-1} \right\| \leqslant n^{n/2},$$

a result originally obtained by Atkinson in [1].

PROPOSITION 11. *Let* β_i *be the sequence formed by taking the set* $\{2^n - 2^m : n > m \geqslant 0\}$ *in increasing order. Then for all* n,

$$\| \prod_{i=1}^{n} (1 - z^{\beta_i}) \| \leqslant (32n)^{\sqrt{n/8}}.$$

Proof. Note that $2^n - 2^m \geqslant 2^m$ if $n > m$ and that $2^{n_1} - 2^{m_1} = 2^{n_2} - 2^{m_2}$ if and only if $(n_1, m_1) = (n_2, m_2)$. So whenever $n = \frac{k(k-1)}{2}$ for some k we have

$$\left\| \prod_{i=1}^{n} (1 - z^{\beta_i}) \right\| = \left\| \prod_{1 \leqslant i < j \leqslant k} (z^{2^{j-1}} - z^{2^{i-1}}) \right\| \leqslant k^{k/2} \leqslant \sqrt{2n}^{\sqrt{n/2}} .$$

While if $\frac{k(k-1)}{2} < n < \frac{(k+1)k}{2}$ then

$$\left\| \prod_{i=1}^{n} (1 - z^{\beta_i}) \right\| \leqslant \left\| \prod_{1 \leqslant i < j \leqslant k} (z^{2^{j-1}} - z^{2^{i-1}}) \right\| \left\| \prod_{i=\frac{k(k-1)}{2}+1}^{n} (1 - z^{\beta_i}) \right\|$$

$$\leqslant \sqrt{2n}^{\sqrt{n/2}} 2^{n - \frac{k(k-1)}{2} - 1} \leqslant \sqrt{2n}^{\sqrt{n/2}} 2^{k-1}$$

$$\leqslant \sqrt{2n}^{\sqrt{n/2}} 2^{\sqrt{2n}} = (32n)^{\sqrt{n/8}} . \qquad \square$$

This is not as good an estimate as Odlyzko's in [16] (see also [13]) which has exponent roughly $n^{1/3}$. What distinguishes it is that it holds for all the partial products of a single infinite product (with distinct increasing exponents). Also, clearly any $\alpha > 2$ could play the role of 2 in the construction of the β_i with the exact same conclusion.

THEOREM 1. *Let* $\{\delta_i\}$ *be any sequence of integers and let* $\{\beta_i\}$ *be the sequence of differences in the following order*

$$\{\delta_1 - \delta_0, \delta_2 - \delta_0, \delta_2 - \delta_1, \ldots, \delta_n - \delta_0, \ldots, \delta_n - \delta_{n-1}, \ldots\}$$

then

$$\left\| \prod_{i=1}^{n} (1 - z^{\beta_i}) \right\| \leqslant (32n)^{\sqrt{n/8}} .$$

5. PERFECT SOLUTIONS OF PRIME SIZE

The first unresolved case of the Prouhet-Tarry-Escott problem is the eleven case. The previous ideal solutions were all found without computer assistance; indeed the cases 1, ..., 10 were all resolved prior to 1950. It therefore seems appropriate to discuss an algorithm for searching for such solutions. We wish to perform a computer search for perfect symmetric ideal solutions

of size 11. To this end we produce a method of finding all such solutions mod 11^n for any n. As this method applies to any odd prime p we present it in the general situation. (A similar method for solving the ideal Prouhet-Tarry-Escott problem mod p^n is suggested in [17] for all primes p greater or equal to the size.) We will be using symmetric residues throughout, as they facilitate checking for solutions in ranges of the form $[-l, l]$.

LEMMA 7. *If* $\{\beta_0, \ldots, \beta_{p-1}\}$ *is a perfect solution mod* p^{n+1} *then*

$$\beta_i = m_i p^n + \alpha_i \quad \text{for } i = 0, \ldots, p-1$$

and $\{\alpha_0, \ldots, \alpha_{p-1}\}$ *is a perfect solution mod* p^n.

Proof. This is done by expanding $\{\beta_0, \ldots, \beta_{p-1}\}$ to the base p. □

This simple lemma allows us to create solutions mod p^n for any n inductively. We only need to find the $\{m_0, \ldots, m_{p-1}\}$ given $\{\alpha_0, \ldots, \alpha_{p-1}\}$. This is provided by the theorem below.

Now suppose that $\{\alpha_0, \ldots, \alpha_{p-1}\}$ is a perfect solution mod p^n. We define

$$s_k = -\frac{\sum_{i=0}^{p-1} \alpha_i^{2k-1}}{p^n} \quad \text{for } k = 1, \ldots, \tfrac{p-1}{2}.$$

We also suppose without loss of generality that $\alpha_i \equiv i \pmod p$ for $i = 0, \ldots, p-1$.

THEOREM 2. *Given* $\{\alpha_0, \ldots, \alpha_{p-1}\}$, *a perfect solution mod* p^n, *all* $p^{\frac{p+1}{2}}$ *perfect solutions mod* p^{n+1} *of the form*

$$\{m_0 p^n + \alpha_0, \ldots, m_{p-1} p^n + \alpha_{p-1}\}$$

are given by

$$(m_0, \ldots, m_{p-1}) = (a_0, \ldots, a_{p-1}) + (h_0, \ldots, h_{p-1}),$$

where

$$a_0 = 0$$

$$a_i = \sum_{j=1}^{p-1} \frac{-i^{2-2j}}{2j-1} s_j \pmod p \quad \text{for } i = 1, \ldots, \tfrac{p-1}{2}$$

$$a_i = a_{p-i} \quad \text{for } i = \tfrac{p+1}{2}, \ldots, p-1$$

and $(h_0, \ldots, h_{\frac{p-1}{2}})$ *are arbitrary residues mod* p *and*

$$h_i = 2h_0 - h_{p-i} \quad \text{for } i = \frac{p+1}{2}, \ldots, p-1 .$$

So there are exactly $p^{n\frac{p+1}{2}}$ *perfect solutions mod* p^{n+1}.

Proof. Suppose $\{m_i p^n + \alpha_i\}$ is a perfect solution mod p^{n+1} and $\{\alpha_i\}$ is a perfect solution mod p^n. For $k = 1, \ldots, \frac{p-1}{2}$

$$\sum_{i=0}^{p-1} (m_i p^n + \alpha_i)^{2k-1} \equiv 0 \pmod{p^{n+1}} .$$

On expanding we get

$$\sum_{i=0}^{p-1} ((2k-1)\alpha_i^{2k-2} m_i p^n + \alpha_i^{2k-1}) \equiv 0 \pmod{p^{n+1}}$$

$$\sum_{i=0}^{p-1} (2k-1)\alpha_i^{2k-2} m_i p^n \equiv -\sum_{i=0}^{p-1} \alpha_i^{2k-1} \pmod{p^{n+1}} .$$

Division by p^n gives us

$$\sum_{i=0}^{p-1} (2k-1)\alpha_i^{2k-2} m_i \equiv -\frac{\sum_{i=0}^{p-1} \alpha_i^{2k-1}}{p^n} \pmod{p} ,$$

and since $\alpha_i \equiv i \pmod{p}$ we have

$$\sum_{i=0}^{p-1} (2k-1) i^{2k-2} m_i \equiv -\frac{\sum_{i=0}^{p-1} \alpha_i^{2k-1}}{p^n} \pmod{p} .$$

So we define A, a $\left(\frac{p-1}{2} \times p\right)$ matrix, by

$$A_{k,i} \equiv (2k-1)(i-1)^{2k-2} \pmod{p} .$$

We now have, with $s := (s_0, \ldots, s_{(p-1)/2})$ and $m := (m_0, \ldots, m_{(p-1)})$,

$$Am \equiv s \pmod{p} .$$

For example with $p = 7$ we get

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 3 & -2 & -1 & -1 & -2 & 3 \\ 0 & -2 & 3 & -1 & -1 & 3 & -2 \end{pmatrix} \begin{pmatrix} m_0 \\ m_1 \\ \vdots \\ m_6 \end{pmatrix} = \begin{pmatrix} \sum \alpha_i \\ \sum \alpha_i^3 \\ \sum \alpha_i^5 \end{pmatrix} .$$

In general the rank of A is always $\frac{p-1}{2}$, as the next argument makes clear, so there are $p^{\frac{p+1}{2}}$ solutions of this underdetermined linear system.

We first derive a particular solution $a := (a_0, \ldots, a_{p-1})$ of the system. We set $a_0 = 0$ and $\bar{A}$ to be A without its first column. We also define $\bar{a}$ to be a without a_0. We solve the reduced system

$$\bar{A}\bar{a} \equiv s \pmod{p}$$

by the standard method. So

$$\bar{a} \equiv \bar{A}^T(\bar{A}\bar{A}^T)^{-1}s \pmod{p}.$$

$\bar{A}\bar{A}^T$ is a particularly simple symmetric matrix given by

$$\begin{pmatrix} \sum i^0 & \sum 3i^2 & \sum 5i^4 & \ldots & \sum (p-2)i^{p-3} \\ \vdots & \sum 9i^4 & \sum 15i^6 & \ldots & \sum 3(p-2)i^{p-1} \\ \vdots & \vdots & \sum 25i^8 & \ldots & \sum 5(p-2)i^{p+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \sum (p-2)^2 i^{2p-6} \end{pmatrix}$$

where each sum ranges over $i = 1, \ldots, p-1$. Since $\sum_{i=1}^{p-1} i^k \equiv 0 \pmod{p}$ when $k \not\equiv 0 \pmod{p-1}$ almost all the elements of the matrix vanish and we are left with a very simple matrix. In fact we get the product of a diagonal and a permutation matrix. Note that this shows that A has full rank modulo p. For example when $p = 11$ we get

$$\bar{A}\bar{A}^T = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -5 \\ 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & -2 & 0 & 0 \\ 0 & -5 & 0 & 0 & 0 \end{pmatrix}.$$

So it is a simple matter to find $B = \bar{A}^T(\bar{A}\bar{A}^T)^{-1}$. For $i = 1, \ldots, p-1$ $j = 1, \ldots, \frac{p-1}{2}$

$$B_{i,j} \equiv \frac{-i^{2-2j}}{2j-1} \pmod{p}.$$

For example B, when $p = 7$, is

$$\begin{pmatrix} -1 & 2 & -3 \\ -1 & -3 & 2 \\ -1 & 1 & 1 \\ -1 & 1 & 1 \\ -1 & -3 & 2 \\ -1 & 2 & -3 \end{pmatrix}.$$

So our particular solution a is given by $a_0 = 0$ and $\bar{a} = Bs$.

To find the solution h of the homogeneous system

$$Ah \equiv 0 \pmod{p}$$

consider the reduced system

$$\bar{A}\bar{h} \equiv \begin{pmatrix} -h_0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \pmod{p} .$$

Note that if $h_i + h_{p-i} \equiv 2h_0$ for $i = 1, \ldots, \frac{p-1}{2}$ we have a solution since

$$\sum_{i=1}^{p-1} i^k \equiv 0 \pmod{p} \quad \text{if} \quad k \not\equiv 0 \pmod{p-1} .$$

Finally setting $(h_0, h_1, \ldots, h_{\frac{p-1}{2}})$ arbitrary we get the solution as in the statement of the theorem. □

This theorem allows one to calculate all $p^{(n-1)\frac{p+1}{2}}$ perfect solutions mod p^n for any odd prime p and any n. This is essentially calculating solutions in the ring of p-adic integers. We were hoping to find a perfect solution of size 11 using this method, but we were only able to show that there is no such solution with coefficients in the range $[-363, 363]$. This is because there are 11^6 solutions mod 11^2, and 11^{12} solutions mod 11^3. So checking for solutions in the relatively small range $[-665, 665]$, would require checking more than a billion cases. Even checking in the range $[-363, 363]$ was a substantial computation. We were able to compute all 7^8 solutions mod 7^3 to find that all perfect solutions of size 7 with coefficients in the range $[-171, 171]$ are

$$\{-51, -33, -24, 7, 13, 38, 50\}$$
$$\{-90, -86, -39, -5, 48, 77, 95\}$$
$$\{-116, -104, -36, -19, 75, 77, 123\}$$
$$\{-120, -110, -23, -13, 38, 105, 123\}$$
$$\{-134, -75, -66, 8, 47, 87, 133\} .$$

We hope that this technique in combination with others may yield a viable computer search for a perfect solution of size 11.

6. Open Problems

There are many open questions and unproven conjectures about the Prouhet-Tarry-Escott problem. We conclude by listing a few.

1. Find an ideal solution for any size higher than 10 or find some degree for which an ideal solution does not exist. (Even a heuristic argument would be of interest.)
2. Find another class of solutions of size 9 or 10.
3. Prove $N(k) \leqslant o(k^2)$.
4. Prove $M(k) \leqslant O(k^2)$.
5. Show that there is no 7 factor (degree 6) pure product of norm 14.
6. Find a non-trivial lower bound for $A(k)$. Almost equivalently prove

$$\min_{n_1, \ldots, n_k} \left\| \prod_{i=1}^{k} (1 - x^{n_k}) \right\|_1 > 2k$$

for some k. (Problem 5 is the $k = 7$ case of this.)

7. Find a true algorithm, even an impractical one, that determines if there is an ideal solution of size 11.
8. Find a true algorithm, even an impractical one, that determines if there is a degree 6 ($k = 7$) pure product of norm 14.
9. Solve the ideal problem mod p^n for all primes p smaller than the size of the solution and all n.

The big prize is to find ideal solutions of all degrees, if indeed they exist. Question 1 above is, of course, the first step. No progress on questions 3 and 4 has been made for many years. Questions 5, 6, and 8 all relate to the Erdős-Szekeres Problem. The issue in Questions 7 and 8 is that it is not known how to bound solutions so as to make the problems finite. Question 9 is raised in [17] and would show that no local obstructions exist to solutions.

REFERENCES

[1] Atkinson, F.V. On a Problem of Erdős and Szekeres. *Canad. Math. Bull. 1* (1961), 7-12.

[2] Beck, J. The Modulus of Polynomials with Zeros on the Unit Circle: A Problem of Erdös. *Annals of Math. 134* (1991), 609-651.

[3] Borwein, P. Some Restricted Partition Functions. *J. Number Theory 45* (1993), 228-240.

[4] CHERNICK, J. Ideal Solutions of the Tarry-Escott Problem. *M.A.A. Monthly 44* (1937), 627-633.
[5] DICKSON, L.E. *History of the Theory of Numbers, Vol. 2.* Chelsea Publishing Comp., New York, 1952.
[6] DOBROWOLSKI, E. On a Question of Lehmer and the Number of Irreducible Factors of a Polynomial. *Acta Arithmetica 34* (1979), 341-401.
[7] DORWART, H.L. and O.E. BROWN. The Tarry-Escott Problem. *M.A.A. Monthly 44* (1937), 613-626.
[8] ERDŐS, P. and G. SZEKERES. On the Product $\prod_{k=1}^{n}(1 - z^{a_k})$. *Acad. Serbe Sci. Publ. Institut Math. 12* (1958), 29-34.
[9] FUCHS, W.H.J. and E.M. WRIGHT. The 'Easier' Waring Problem. *Quart. J. Math. 10* (1939), 190-209.
[10] GLODEN, A. *Mehrgradige Gleichungen.* Noordhoff, Groningen, 1944.
[11] HUA, L.K. *Introduction to Number Theory.* Springer-Verlag, Berlin, Heidelberg, New York, 1982.
[12] KLEIMAN, H. A Note on the Tarry-Escott Problem. *J. Reine Angew. Math. 278/279* (1975), 48-51.
[13] KOLOUNTZAKIS, M.N. On Non-Negative Cosine Polynomials with Non-Negative, Integral Coefficients. *Proc. Amer. Math. Soc. 120* (1994), 157-168.
[14] LINDEN, C.N. The Modulus of Polynomials with Zeros on the Unit Circle. *Bull. London Math. Soc. 9* (1977), 65-69.
[15] MELZAK, Z.A. A Note on the Tarry-Escott Problem. *Canad. Math. Bull. vol. 4, no. 3* (1961), 233-237.
[16] ODLYZKO, A.M. Minima of Cosine Sums and Maxima of Polynomials on the Unit Circle. *J. London Math. Soc. (2), 26* (1982), 412-420.
[17] REES, E. and C.J. SMYTH. On the Constant in the Tarry-Escott Problem. In *Cinquante Ans de Polynômes, Fifty Years of Polynomials.* Springer-Verlag, Berlin, Heidelberg, New York, 1988.
[18] SINHA, T.N. On The Tarry-Escott Problem. *M.A.A. Monthly 73* (1966), 280-285.
[19] SMYTH, C.J. Ideal 9th-order Multigrades and Letac's Elliptic Curve. *Math. Comp. 57* (1991), 817-823.
[20] SUDLER, C., Jr. An Estimate for a Restricted Partition Function. *Quart. J. Math. Oxford (2), 15* (1964), 1-10.
[21] WRIGHT, E.M. An Easier Waring's Problem. *J.L.M.S. 9* (1934), 267-272.
[22] —— On Tarry's Problem (I). *Quart. J. Math., Oxford Ser. 6* (1935), 261-267.
[23] —— Prouhet's 1851 Solution of the Tarry-Escott Problem of 1910. *M.A.A. Monthly 66* (1959), 199-201.
[24] —— The Tarry-Escott and the "Easier" Waring Problem. *J. Reine Angew. Math. 311/312* (1972), 170-173.

(Reçu le 13 octobre 1992)

Peter Borwein and Colin Ingalls

Department of Mathematics and Statistics
Simon Fraser University
Burnaby, British Columbia
Canada V5A 1S6

vide-leer-empty