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

Kapitel: 3. Ideal and Symmetric Ideal Solutions

DOI: https://doi.org/10.5169/seals-61102

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. $\square$

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

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

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

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

and

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

In particular for each j

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

has exactly k solutions (counting multiplicity, in the sense that $\alpha_j \equiv \beta_i$ mod 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. $\square$

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 $\{\alpha_1, ..., \alpha_s\}$ 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 $\upsilon(k)$. Recall that the usual Waring problem requires al positive signs. For arbitrary k the best known bounds for $\upsilon(k)$ 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 $\{\alpha_1, ..., \alpha_n\} \overset{k-2}{=} \{\beta_1, ..., \beta_n\}$. 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

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