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: 2. Elementary Properties
DOI: https://doi.org/10.5169/seals-61102

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:*

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

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

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

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. $\square$

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* $\{\alpha_1, \ldots, \alpha_n\} \stackrel{k}{=} \{\beta_1, \ldots, \beta_n\}$ *then*

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

for any integer M.

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

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. $\square$

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. $\square$

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.