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: 5. Perfect Solutions of Prime Size
DOI: https://doi.org/10.5169/seals-61102

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*

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

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

$$a_0 = 0$$

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

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

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

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

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

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 $a := (a_0, \dots, a_{p-1})$ 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

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

where each sum ranges over $i = 1, \dots, p-1$. 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 $i = 1, \dots, p-1$ $j = 1, \dots, \frac{p-1}{2}$

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

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 $i = 1, \dots, \frac{p-1}{2}$ 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 $(h_0, h_1, \dots, h_{\frac{p-1}{2}})$ 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.