The Prouhet–Tarry–Escott Problem

Timothy Caley

Department of Pure Mathematics, University of Waterloo

September 23, 2009

The Prouhet–Tarry–Escott Problem

Given positive integers n and k, with $k \leq n-1$, the Prouhet–Tarry–Escott (PTE) problem asks for two distinct subsets of $\mathbb{Z}$, say $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_n\}$, such that

$$\begin{aligned}
x_1 + x_2 + \ldots + x_n &= y_1 + y_2 + \ldots + y_n \\
x_1^2 + x_2^2 + \ldots + x_n^2 &= y_1^2 + y_2^2 + \ldots + y_n^2 \\
&\vdots \\
x_1^k + x_2^k + \ldots + x_n^k &= y_1^k + y_2^k + \ldots + y_n^k
\end{aligned}$$

for some integer $k \leq n-1$. A solution is written $X =_k Y$, and n is its *size* and k is its *degree*.

Two examples are: $\{1, 3, 3, 3\} =_2 = \{2, 2, 2, 4\}$ since

$$\begin{aligned} 1 + 3 + 3 + 3 &= 10 = 2 + 2 + 2 + 4 \\ 1^2 + 3^2 + 3^2 + 3^2 &= 28 = 2^2 + 2^2 + 2^2 + 4^2 \end{aligned}$$

and $\{0, 3, 5, 11, 13, 16\} =_5 \{1, 1, 8, 8, 15, 15\}$ since

$$\begin{aligned} 0 + 3 + 5 + 11 + 13 + 16 &= 48 = 1 + 1 + 8 + 8 + 15 + 15 \\ 0^2 + 3^2 + 5^2 + 11^2 + 13^2 + 16^2 &= 580 = 1^2 + 1^2 + 8^2 + 8^2 + 15^2 + 15^2 \\ 0^3 + 3^3 + 5^3 + 11^3 + 13^3 + 16^3 &= 7776 = 1^3 + 1^3 + 8^3 + 8^3 + 15^3 + 15^3 \\ 0^4 + 3^4 + 5^4 + 11^4 + 13^4 + 16^4 &= 109444 = 1^4 + 1^4 + 8^4 + 8^4 + 15^4 + 15^4 \\ 0^5 + 3^5 + 5^5 + 11^5 + 13^5 + 16^5 &= 1584288 = 1^5 + 1^5 + 8^5 + 8^5 + 15^5 + 15^5. \end{aligned}$$

Note that requiring "distinct" subsets excludes trivial solutions. That is, $\{0, 3, 5, 11, 13, 16, 20\} =_5 \{1, 1, 8, 8, 15, 15, 20\}$ is trivial.

Two examples are: $\{1, 3, 3, 3\} =_2= \{2, 2, 2, 4\}$ since

$$1 + 3 + 3 + 3 = 10 = 2 + 2 + 2 + 4$$
$$1^2 + 3^2 + 3^2 + 3^2 = 28 = 2^2 + 2^2 + 2^2 + 4^2$$

and $\{0, 3, 5, 11, 13, 16\} =_5 \{1, 1, 8, 8, 15, 15\}$ since

$$0 + 3 + 5 + 11 + 13 + 16 = 48 = 1 + 1 + 8 + 8 + 15 + 15$$
$$0^2 + 3^2 + 5^2 + 11^2 + 13^2 + 16^2 = 580 = 1^2 + 1^2 + 8^2 + 8^2 + 15^2 + 15^2$$
$$0^3 + 3^3 + 5^3 + 11^3 + 13^3 + 16^3 = 7776 = 1^3 + 1^3 + 8^3 + 8^3 + 15^3 + 15^3$$
$$0^4 + 3^4 + 5^4 + 11^4 + 13^4 + 16^4 = 109444 = 1^4 + 1^4 + 8^4 + 8^4 + 15^4 + 15^4$$
$$0^5 + 3^5 + 5^5 + 11^5 + 13^5 + 16^5 = 1584288 = 1^5 + 1^5 + 8^5 + 8^5 + 15^5 + 15^5.$$

Note that requiring “distinct” subsets excludes trivial solutions. That is, $\{0, 3, 5, 11, 13, 16, 20\} =_5 \{1, 1, 8, 8, 15, 15, 20\}$ is trivial.

Two examples are: $\{1, 3, 3, 3\} =_2= \{2, 2, 2, 4\}$ since

$$1 + 3 + 3 + 3 = 10 = 2 + 2 + 2 + 4$$
$$1^2 + 3^2 + 3^2 + 3^2 = 28 = 2^2 + 2^2 + 2^2 + 4^2$$

and $\{0, 3, 5, 11, 13, 16\} =_5 \{1, 1, 8, 8, 15, 15\}$ since

$$0 + 3 + 5 + 11 + 13 + 16 = 48 = 1 + 1 + 8 + 8 + 15 + 15$$
$$0^2 + 3^2 + 5^2 + 11^2 + 13^2 + 16^2 = 580 = 1^2 + 1^2 + 8^2 + 8^2 + 15^2 + 15^2$$
$$0^3 + 3^3 + 5^3 + 11^3 + 13^3 + 16^3 = 7776 = 1^3 + 1^3 + 8^3 + 8^3 + 15^3 + 15^3$$
$$0^4 + 3^4 + 5^4 + 11^4 + 13^4 + 16^4 = 109444 = 1^4 + 1^4 + 8^4 + 8^4 + 15^4 + 15^4$$
$$0^5 + 3^5 + 5^5 + 11^5 + 13^5 + 16^5 = 1584288 = 1^5 + 1^5 + 8^5 + 8^5 + 15^5 + 15^5.$$

Note that requiring “distinct” subsets excludes trivial solutions. That is, $\{0, 3, 5, 11, 13, 16, 20\} =_5 \{1, 1, 8, 8, 15, 15, 20\}$ is trivial.

PTE – Other formulations and facts

Suppose $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_n\}$ are subsets of $\mathbb{Z}$, and $k \in \mathbb{N}$ with $k \leq n-1$. Then the following are equivalent:

$$(i) \quad \sum_{i=1}^{n} x_i^j = \sum_{i=1}^{n} y_i^j \quad \text{for } j = 1, 2, \ldots, k$$

$$(ii) \quad \deg\left(\prod_{i=1}^{n}(x - x_i) - \prod_{i=1}^{n}(x - y_i)\right) \leq n - k - 1$$

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

The maximal interesting case occurs when $k = n - 1$. A solution in this case, say $X =_{n-1} Y$, is called *ideal*.

PTE – Other formulations and facts

Suppose $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_n\}$ are subsets of $\mathbb{Z}$, and $k \in \mathbb{N}$ with $k \leq n - 1$. Then the following are equivalent:

$$(i) \quad \sum_{i=1}^{n} x_i^j = \sum_{i=1}^{n} y_i^j \quad \text{for } j = 1, 2, \ldots, k$$

$$(ii) \quad \deg\left(\prod_{i=1}^{n}(x - x_i) - \prod_{i=1}^{n}(x - y_i)\right) \leq n - k - 1$$

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

The maximal interesting case occurs when $k = n - 1$. A solution in this case, say $X =_{n-1} Y$, is called *ideal*.

PTE – Other formulations and facts (cont'd)

In the above examples,

$$(x-1)(x-3)(x-3)(x-3)-(x-2)(x-2)(x-2)(x-4)=2x-5$$

$$(x-0)(x-3)(x-5)(x-11)(x-13)(x-16)$$
$$-(x-1)(x-1)(x-8)(x-8)(x-15)(x-15)=-14400.$$

Assuming

$$\{x_1,\ldots,x_n\}=_k\{y_1,\ldots,y_n\},$$

then for any $M,K\in\mathbb{Z}$ we have

$$\{Mx_1+K,\ldots,Mx_n+K\}=_k\{My_1+K,\ldots,My_n+K\}.$$

Solutions arising this way are *equivalent*, and otherwise, they are *inequivalent.*

PTE – Other formulations and facts (cont'd)

In the above examples,

$$(x-1)(x-3)(x-3)(x-3)-(x-2)(x-2)(x-2)(x-4)=2x-5$$

$$(x-0)(x-3)(x-5)(x-11)(x-13)(x-16)$$
$$-(x-1)(x-1)(x-8)(x-8)(x-15)(x-15)=-14400.$$

Assuming

$$\{x_1,\ldots,x_n\}=_k\{y_1,\ldots,y_n\},$$

then for any $M, K \in \mathbb{Z}$ we have

$$\{Mx_1+K,\ldots,Mx_n+K\}=_k\{My_1+K,\ldots,My_n+K\}.$$

Solutions arising this way are *equivalent*, and otherwise, they are *inequivalent*.

PTE – Other formulations and facts (cont'd)

In the above examples,

$$(x-1)(x-3)(x-3)(x-3)-(x-2)(x-2)(x-2)(x-4)=2x-5$$

$$\begin{aligned}&(x-0)(x-3)(x-5)(x-11)(x-13)(x-16)\\&\qquad -(x-1)(x-1)(x-8)(x-8)(x-15)(x-15)=-14400.\end{aligned}$$

Assuming

$$\{x_1,\ldots,x_n\}=_k\{y_1,\ldots,y_n\},$$

then for any $M, K \in \mathbb{Z}$ we have

$$\{Mx_1+K,\ldots,Mx_n+K\}=_k\{My_1+K,\ldots,My_n+K\}.$$

Solutions arising this way are *equivalent*, and otherwise, they are *inequivalent.*

PTE – Other formulations and facts (cont'd)

In the above examples,

$$(x-1)(x-3)(x-3)(x-3)-(x-2)(x-2)(x-2)(x-4)=2x-5$$

$$\begin{aligned}&(x-0)(x-3)(x-5)(x-11)(x-13)(x-16)\\&\qquad -(x-1)(x-1)(x-8)(x-8)(x-15)(x-15)=-14400.\end{aligned}$$

Assuming

$$\{x_1,\dots,x_n\}=_k\{y_1,\dots,y_n\},$$

then for any $M,K\in\mathbb{Z}$ we have

$$\{Mx_1+K,\dots,Mx_n+K\}=_k\{My_1+K,\dots,My_n+K\}.$$

Solutions arising this way are *equivalent*, and otherwise, they are *inequivalent*.

Connections to other problems

Given an integer k, the "Easier" Waring problem asks for the smallest n, denoted $v(k)$, such that for all m there exists integers $x_1, \ldots, x_n$ such that

$$\pm x_1^k \pm \ldots \pm x_n^k = m.$$

- The best bound for arbitrary k is $v(k) << k \log(k)$, but $v(k)$ is conjectured to be $O(k)$.
- For small values of k, the best bounds for $v(k)$ derive from ideal solutions of the PTE problem. In fact, these are much better than those which derive from the usual Waring problem.

Connections to other problems

Given an integer k, the "Easier" Waring problem asks for the smallest n, denoted $v(k)$, such that for all m there exists integers $x_1, \ldots, x_n$ such that

$$\pm x_1^k \pm \ldots \pm x_n^k = m.$$

- The best bound for arbitrary k is $v(k) << k \log(k)$, but $v(k)$ is conjectured to be $O(k)$.
- For small values of k, the best bounds for $v(k)$ derive from ideal solutions of the PTE problem. In fact, these are much better than those which derive from the usual Waring problem.

Connections to other problems

Given an integer k, the "Easier" Waring problem asks for the smallest n, denoted $v(k)$, such that for all m there exists integers $x_1, \ldots, x_n$ such that

$$\pm x_1^k \pm \ldots \pm x_n^k = m.$$

- The best bound for arbitrary k is $v(k) << k \log(k)$, but $v(k)$ is conjectured to be $O(k)$.
- For small values of k, the best bounds for $v(k)$ derive from ideal solutions of the PTE problem. In fact, these are much better than those which derive from the usual Waring problem.

Connections to other problems (cont'd)

Given N, the goal of the Erdös–Szekeres problem is to find positive integers $\alpha_1, \ldots, \alpha_N$ that minimize

$$\|(1 - z^{\alpha_1})(1 - z_2^{\alpha})\cdots(1 - z^{\alpha_N})\|_\infty.$$

In particular, show that these minima grow faster than N^β for any positive constant β.

- For $N = 1, 2, 3, 4, 5, 6, 8$, the minimizing sets $\{\alpha_1, \ldots, \alpha_N\}$ give an ideal solution to the PTE problem of size N.
- However, it has been shown that the minimizing sets for $N = 7, 9, 10, 11$ cannot lead to PTE solutions.
- For larger cases, nothing is known.

Connections to other problems (cont'd)

Given N, the goal of the Erdös–Szekeres problem is to find positive integers $\alpha_1, \ldots, \alpha_N$ that minimize

$$\|(1 - z^{\alpha_1})(1 - z_2^{\alpha}) \cdots (1 - z^{\alpha_N})\|_\infty.$$

In particular, show that these minima grow faster than N^β for any positive constant β.

- For $N = 1, 2, 3, 4, 5, 6, 8$, the minimizing sets $\{\alpha_1, \ldots, \alpha_N\}$ give an ideal solution to the PTE problem of size N.
- However, it has been shown that the minimizing sets for $N = 7, 9, 10, 11$ cannot lead to PTE solutions.
- For larger cases, nothing is known.

Connections to other problems (cont'd)

Given N, the goal of the Erdös–Szekeres problem is to find positive integers $\alpha_1, \ldots, \alpha_N$ that minimize

$$\|(1 - z^{\alpha_1})(1 - z_2^{\alpha})\cdots(1 - z^{\alpha_N})\|_\infty.$$

In particular, show that these minima grow faster than N^β for any positive constant β.

- For $N = 1, 2, 3, 4, 5, 6, 8$, the minimizing sets $\{\alpha_1, \ldots, \alpha_N\}$ give an ideal solution to the PTE problem of size N.
- However, it has been shown that the minimizing sets for $N = 7, 9, 10, 11$ cannot lead to PTE solutions.
- For larger cases, nothing is known.

Connections to other problems (cont'd)

Given N, the goal of the Erdös–Szekeres problem is to find positive integers $\alpha_1, \ldots, \alpha_N$ that minimize

$$\|(1 - z^{\alpha_1})(1 - z_2^{\alpha})\cdots(1 - z^{\alpha_N})\|_\infty.$$

In particular, show that these minima grow faster than N^β for any positive constant β.

- For $N = 1, 2, 3, 4, 5, 6, 8$, the minimizing sets $\{\alpha_1, \ldots, \alpha_N\}$ give an ideal solution to the PTE problem of size N.
- However, it has been shown that the minimizing sets for $N = 7, 9, 10, 11$ cannot lead to PTE solutions.
- For larger cases, nothing is known.

Ideal solutions to the PTE problem

In 1934, Wright conjectured that it is always possible to find ideal solutions.

- For $n = 2, 3, 4, 5$, complete parametric ideal solutions are known.
- For $n = 6, 7, 8$, only incomplete parametric solutions are known.
- For $n = 10, 11$ infinite inequivalent families of solutions are known (albeit incomplete), due to Smyth (1991) and Choudhry and Wróblewski (2008) respectively. In both cases, the solutions arise from rational points on elliptic curves.
- For both $n = 9, 12$ only two inequivalent solutions are konwn. All were found computationally, due to P. Borwein, Lisonek and Percival and Kuosa, Myrignac and Shuwen, and Broadhurst, respectively.
- For $n > 12$, no ideal solutions are known.

Ideal solutions to the PTE problem

In 1934, Wright conjectured that it is always possible to find ideal solutions.

- For $n = 2, 3, 4, 5$, complete parametric ideal solutions are known.
- For $n = 6, 7, 8$, only incomplete parametric solutions are known.
- For $n = 10, 11$ infinite inequivalent families of solutions are known (albeit incomplete), due to Smyth (1991) and Choudhry and Wróblewski (2008) respectively. In both cases, the solutions arise from rational points on elliptic curves.
- For both $n = 9, 12$ only two inequivalent solutions are konwn. All were found computationally, due to P. Borwein, Lisonek and Percival and Kuosa, Myrignac and Shuwen, and Broadhurst, respectively.
- For $n > 12$, no ideal solutions are known.

Ideal solutions to the PTE problem

In 1934, Wright conjectured that it is always possible to find ideal solutions.

- For $n = 2, 3, 4, 5$, complete parametric ideal solutions are known.
- For $n = 6, 7, 8$, only incomplete parametric solutions are known.
- For $n = 10, 11$ infinite inequivalent families of solutions are known (albeit incomplete), due to Smyth (1991) and Choudhry and Wróblewski (2008) respectively. In both cases, the solutions arise from rational points on elliptic curves.
- For both $n = 9, 12$ only two inequivalent solutions are konwn. All were found computationally, due to P. Borwein, Lisonek and Percival and Kuosa, Myrignac and Shuwen, and Broadhurst, respectively.
- For $n > 12$, no ideal solutions are known.

Ideal solutions to the PTE problem

In 1934, Wright conjectured that it is always possible to find ideal solutions.

- For $n = 2, 3, 4, 5$, complete parametric ideal solutions are known.
- For $n = 6, 7, 8$, only incomplete parametric solutions are known.
- For $n = 10, 11$ infinite inequivalent families of solutions are known (albeit incomplete), due to Smyth (1991) and Choudhry and Wróblewski (2008) respectively. In both cases, the solutions arise from rational points on elliptic curves.
- For both $n = 9, 12$ only two inequivalent solutions are konwn. All were found computationally, due to P. Borwein, Lisonek and Percival and Kuosa, Myrignac and Shuwen, and Broadhurst, respectively.
- For $n > 12$, no ideal solutions are known.

Ideal solutions to the PTE problem

In 1934, Wright conjectured that it is always possible to find ideal solutions.

- For $n = 2, 3, 4, 5$, complete parametric ideal solutions are known.
- For $n = 6, 7, 8$, only incomplete parametric solutions are known.
- For $n = 10, 11$ infinite inequivalent families of solutions are known (albeit incomplete), due to Smyth (1991) and Choudhry and Wróblewski (2008) respectively. In both cases, the solutions arise from rational points on elliptic curves.
- For both $n = 9, 12$ only two inequivalent solutions are konwn. All were found computationally, due to P. Borwein, Lisonek and Percival and Kuosa, Myrignac and Shuwen, and Broadhurst, respectively.
- For $n > 12$, no ideal solutions are known.

Ideal solutions to the PTE problem

In 1934, Wright conjectured that it is always possible to find ideal solutions.

- For $n = 2, 3, 4, 5$, complete parametric ideal solutions are known.
- For $n = 6, 7, 8$, only incomplete parametric solutions are known.
- For $n = 10, 11$ infinite inequivalent families of solutions are known (albeit incomplete), due to Smyth (1991) and Choudhry and Wróblewski (2008) respectively. In both cases, the solutions arise from rational points on elliptic curves.
- For both $n = 9, 12$ only two inequivalent solutions are konwn. All were found computationally, due to P. Borwein, Lisonek and Percival and Kuosa, Myrignac and Shuwen, and Broadhurst, respectively.
- For $n > 12$, no ideal solutions are known.

The PTE problem over other rings

In 2007, Alpers and Tijdeman addressed the PTE problem over $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z}[i]$, the Gaussian integers.

- Ideal solutions should be "easier" to find over the Gaussian integers.
- In fact, all the basic facts hold, not only over $\mathbb{Z}[i]$, but over any ring of integers, $\mathcal{O}$, of a number field, but we will stick to the case where $\mathcal{O}$ is a UFD.
- The next step is to examine the PTE problem over the Gaussian integers for $n \geq 9$, using the computational methods of Borwein et al.

The PTE problem over other rings

In 2007, Alpers and Tijdeman addressed the PTE problem over $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z}[i]$, the Gaussian integers.

- Ideal solutions should be "easier" to find over the Gaussian integers.
- In fact, all the basic facts hold, not only over $\mathbb{Z}[i]$, but over any ring of integers, $\mathcal{O}$, of a number field, but we will stick to the case where $\mathcal{O}$ is a UFD.
- The next step is to examine the PTE problem over the Gaussian integers for $n \geq 9$, using the computational methods of Borwein et al.

The PTE problem over other rings

In 2007, Alpers and Tijdeman addressed the PTE problem over $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z}[i]$, the Gaussian integers.

- Ideal solutions should be "easier" to find over the Gaussian integers.
- In fact, all the basic facts hold, not only over $\mathbb{Z}[i]$, but over any ring of integers, $\mathcal{O}$, of a number field, but we will stick to the case where $\mathcal{O}$ is a UFD.
- The next step is to examine the PTE problem over the Gaussian integers for $n \geq 9$, using the computational methods of Borwein et al.

The PTE problem over other rings

In 2007, Alpers and Tijdeman addressed the PTE problem over $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z}[i]$, the Gaussian integers.

- Ideal solutions should be "easier" to find over the Gaussian integers.
- In fact, all the basic facts hold, not only over $\mathbb{Z}[i]$, but over any ring of integers, $\mathcal{O}$, of a number field, but we will stick to the case where $\mathcal{O}$ is a UFD.
- The next step is to examine the PTE problem over the Gaussian integers for $n \geq 9$, using the computational methods of Borwein et al.

Finding Ideal Solutions

Suppose our search space is $0 \le x_i, y_i \le S$. We can assume $x_1 = 0$. Then select the remaining integers so that $0 \le x_2 \le x_3 \le \ldots \le x_n$ and $1 \le y_1 \le \ldots \le y_{n-1}$, with $y_n = x_1 + \ldots + x_n - (y_1 + \ldots + y_{n-1})$. Now check whether or not

$$x_1^k + \ldots + x_n^k = y_1^k + \ldots + y_n^k$$

for each $k = 1, \ldots, n-1$. However, we can do better. Recall that:

$$(x - x_1)(x - x_2) \cdots (x - x_n) = (x - y_1)(x - y_2) \cdots (x - y_n) + C.$$

Substituting $x = y_j$ for $j = 1, \ldots, n$ we get

$$(y_j - x_1) \cdots (y_j - x_n) = C.$$

Finding Ideal Solutions

Suppose our search space is $0 \le x_i, y_i \le S$. We can assume $x_1 = 0$. Then select the remaining integers so that $0 \le x_2 \le x_3 \le \ldots \le x_n$ and $1 \le y_1 \le \ldots \le y_{n-1}$, with $y_n = x_1 + \ldots + x_n - (y_1 + \ldots + y_{n-1})$. Now check whether or not

$$x_1^k + \ldots + x_n^k = y_1^k + \ldots + y_n^k$$

for each $k = 1, \ldots, n-1$. However, we can do better. Recall that:

$$(x - x_1)(x - x_2) \cdots (x - x_n) = (x - y_1)(x - y_2) \cdots (x - y_n) + C.$$

Substituting $x = y_j$ for $j = 1, \ldots, n$ we get

$$(y_j - x_1) \cdots (y_j - x_n) = C.$$

Finding Ideal Solutions

Suppose our search space is $0 \leq x_i, y_i \leq S$. We can assume $x_1 = 0$. Then select the remaining integers so that $0 \leq x_2 \leq x_3 \leq \ldots \leq x_n$ and $1 \leq y_1 \leq \ldots \leq y_{n-1}$, with $y_n = x_1 + \ldots + x_n - (y_1 + \ldots + y_{n-1})$. Now check whether or not

$$x_1^k + \ldots + x_n^k = y_1^k + \ldots + y_n^k$$

for each $k = 1, \ldots, n-1$. However, we can do better. Recall that:

$$(x - x_1)(x - x_2) \cdots (x - x_n) = (x - y_1)(x - y_2) \cdots (x - y_n) + C.$$

Substituting $x = y_j$ for $j = 1, \ldots, n$ we get

$$(y_j - x_1) \cdots (y_j - x_n) = C.$$

Finding Ideal Solutions (cont'd)

For any $k \in \{1, \ldots, n\}$, we can rearrange this equation to

$$f(y_j) = \frac{1}{C}(y_j - x_{n-k+2}) \cdots (y_j - x_n) = (y_j - x_1)^{-1} \cdots (y_j - x_{n-k+1})^{-1}$$

for $j = 1, \ldots, k$. So if we have $x_1, \ldots, x_{n-k+1}$ and $y_1, \ldots, y_k$, then we can interpolate to find $f(x)$, using the ordered pairs $(y_j, f(y_j))$ for $j = 1, \ldots, k$.

Thus, $f(x)$ is a polynomial of degree $k - 1$, and its roots are $x_{n-k+2}, \ldots, x_n$, which we find by solving $f(x) = 0$.

We repeat this process to find the remaining $y_{k+1}, \ldots, y_n$.

Thus, instead of searching in $2n - 2$ variables, we need only search in $n + 1$ variables.

Finding Ideal Solutions (cont'd)

For any $k \in \{1, \ldots, n\}$, we can rearrange this equation to

$$f(y_j) = \frac{1}{C}(y_j - x_{n-k+2}) \cdots (y_j - x_n) = (y_j - x_1)^{-1} \cdots (y_j - x_{n-k+1})^{-1}$$

for $j = 1, \ldots, k$. So if we have $x_1, \ldots, x_{n-k+1}$ and $y_1, \ldots, y_k$, then we can interpolate to find $f(x)$, using the ordered pairs $(y_j, f(y_j))$ for $j = 1, \ldots, k$.

Thus, $f(x)$ is a polynomial of degree $k - 1$, and its roots are $x_{n-k+2}, \ldots, x_n$, which we find by solving $f(x) = 0$.

We repeat this process to find the remaining $y_{k+1}, \ldots, y_n$.

Thus, instead of searching in $2n - 2$ variables, we need only search in $n + 1$ variables.

Finding Ideal Solutions (cont'd)

For any $k \in \{1, \ldots, n\}$, we can rearrange this equation to

$$f(y_j) = \frac{1}{C}(y_j - x_{n-k+2}) \cdots (y_j - x_n) = (y_j - x_1)^{-1} \cdots (y_j - x_{n-k+1})^{-1}$$

for $j = 1, \ldots, k$. So if we have $x_1, \ldots, x_{n-k+1}$ and $y_1, \ldots, y_k$, then we can interpolate to find $f(x)$, using the ordered pairs $(y_j, f(y_j))$ for $j = 1, \ldots, k$.

Thus, $f(x)$ is a polynomial of degree $k - 1$, and its roots are $x_{n-k+2}, \ldots, x_n$, which we find by solving $f(x) = 0$.

We repeat this process to find the remaining $y_{k+1}, \ldots, y_n$.

Thus, instead of searching in $2n - 2$ variables, we need only search in $n + 1$ variables.

Finding Ideal Solutions (cont'd)

For any $k \in \{1, \ldots, n\}$, we can rearrange this equation to

$$f(y_j) = \frac{1}{C}(y_j - x_{n-k+2}) \cdots (y_j - x_n) = (y_j - x_1)^{-1} \cdots (y_j - x_{n-k+1})^{-1}$$

for $j = 1, \ldots, k$. So if we have $x_1, \ldots, x_{n-k+1}$ and $y_1, \ldots, y_k$, then we can interpolate to find $f(x)$, using the ordered pairs $(y_j, f(y_j))$ for $j = 1, \ldots, k$.

Thus, $f(x)$ is a polynomial of degree $k - 1$, and its roots are $x_{n-k+2}, \ldots, x_n$, which we find by solving $f(x) = 0$.

We repeat this process to find the remaining $y_{k+1}, \ldots, y_n$.

Thus, instead of searching in $2n - 2$ variables, we need only search in $n + 1$ variables.

Making the Search More Efficient

Definition

Let $\mathcal{S}_n := \{(X, Y) \subset \mathcal{O}^n \times \mathcal{O}^n | X =_{n-1} Y\}$. *Then let*

$$C_n := \gcd\{C_{n,X,Y} | (X, Y) \in \mathcal{S}\}.$$

We say that C_n *is the constant associated with the* $\mathcal{O}$-PTE *problem of size* n.

Theorem (Borwein et al)

Suppose $\mathcal{O}$ *is a UFD. Let* $\{x_1, \ldots, x_n\} =_{n-1} \{y_1, \ldots, y_n\}$ *be subsets of* $\mathcal{O}$ *that are an ideal* $\mathcal{O}$-PTE *solution. Suppose that* $q \in \mathcal{O}$ *is a prime such that* $q \mid C_n$. *Then we can reorder the* y_i *such that*

$$x_i \equiv y_i \pmod{q} \qquad \text{for } i = 1, \ldots, n.$$

Making the Search More Efficient

Definition

Let $\mathcal{S}_n := \{(X, Y) \subset \mathcal{O}^n \times \mathcal{O}^n | X =_{n-1} Y\}$. *Then let*

$$C_n := \gcd\{C_{n,X,Y} | (X, Y) \in \mathcal{S}\}.$$

We say that C_n *is the constant associated with the* $\mathcal{O}$-PTE *problem of size* n.

Theorem (Borwein et al)

Suppose $\mathcal{O}$ *is a UFD. Let* $\{x_1, \ldots, x_n\} =_{n-1} \{y_1, \ldots, y_n\}$ *be subsets of* $\mathcal{O}$ *that are an ideal* $\mathcal{O}$-PTE *solution. Suppose that* $q \in \mathcal{O}$ *is a prime such that* $q \mid C_n$. *Then we can reorder the* y_i *such that*

$$x_i \equiv y_i \pmod{q} \qquad \text{for } i = 1, \ldots, n.$$

Making the Search More Efficient (cont'd)

Hence, we can reorder the solutions modulo q, and so we can search in the following way:

- Suppose q_1, q_2 are the two largest primes (in $\mathcal{O}$) dividing C_n.
- Assume $x_1 = 0$, and pick the rest so that for $i = 1, \ldots, n$

$$x_i \equiv y_i \pmod{q_1}$$

$$(x_{i+1} - y_i) \cdot \sum_{j=1}^{i} (x_j - y_j) \equiv 0 \pmod{q_2}.$$

- Thus, every prime q that divides the constant reduces the search space in each variable by $1/q$.

Making the Search More Efficient (cont'd)

Hence, we can reorder the solutions modulo q, and so we can search in the following way:

- Suppose q_1, q_2 are the two largest primes (in $\mathcal{O}$) dividing C_n.
- Assume $x_1 = 0$, and pick the rest so that for $i = 1, \ldots, n$

$$x_i \equiv y_i \pmod{q_1}$$

$$(x_{i+1} - y_i) \cdot \sum_{j=1}^{i} (x_j - y_j) \equiv 0 \pmod{q_2}.$$

- Thus, every prime q that divides the constant reduces the search space in each variable by $1/q$.

Making the Search More Efficient (cont'd)

Hence, we can reorder the solutions modulo q, and so we can search in the following way:

- Suppose q_1, q_2 are the two largest primes (in $\mathcal{O}$) dividing C_n.
- Assume $x_1 = 0$, and pick the rest so that for $i = 1, \ldots, n$

$$x_i \equiv y_i \pmod{q_1}$$

$$(x_{i+1} - y_i) \cdot \sum_{j=1}^{i} (x_j - y_j) \equiv 0 \pmod{q_2}.$$

- Thus, every prime q that divides the constant reduces the search space in each variable by $1/q$.

Making the Search More Efficient (cont'd)

Hence, we can reorder the solutions modulo q, and so we can search in the following way:

- Suppose q_1, q_2 are the two largest primes (in $\mathcal{O}$) dividing C_n.
- Assume $x_1 = 0$, and pick the rest so that for $i = 1, \dots, n$

$$x_i \equiv y_i \pmod{q_1}$$

$$(x_{i+1} - y_i) \cdot \sum_{j=1}^{i} (x_j - y_j) \equiv 0 \pmod{q_2}.$$

- Thus, every prime q that divides the constant reduces the search space in each variable by $1/q$.

Divisibility Results for C_n

Thus, we have the following divisibility results for C_n:

- C_n is divisible by $(n-1)!$.
- If $p > 3$ is a prime and $p = n$, then $p \mid C_n$.
- If p is a prime with $n + 2 \leq p < n + 2 + \frac{n-3}{6}$, then $p \mid C_n$.

n	Lower bound for $C_n/n!$	Upper bound for $C_n/n!$
2	1	1
3	2	2
4	$2 \cdot 3$	$2 \cdot 3$
5	$2 \cdot 3 \cdot 5$	$2 \cdot 3 \cdot 5$
6	$2^2 \cdot 3 \cdot 5$	$2^3 \cdot 3 \cdot 5$
7	$3 \cdot 5 \cdot 7 \cdot 11$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
8	$3 \cdot 5 \cdot 7 \cdot 11$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
9	$3 \cdot 5 \cdot 7 \cdot 11$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
10	$5 \cdot 7 \cdot 13$	$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 37 \cdot 53 \cdot 61 \cdot 79 \cdot 83$ $\cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 191$
11	$5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	none known
12	$5 \cdot 7 \cdot 11$	$2^4 \cdot 3^5 \cdot 5 \cdot 7 \cdot 11 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$

Divisibility Results for C_n

Thus, we have the following divisibility results for C_n:

- C_n is divisible by $(n-1)!$.
- If $p > 3$ is a prime and $p = n$, then $p \mid C_n$.
- If p is a prime with $n + 2 \le p < n + 2 + \frac{n-3}{6}$, then $p \mid C_n$.

n	Lower bound for $C_n/n!$	Upper bound for $C_n/n!$
2	1	1
3	2	2
4	$2 \cdot 3$	$2 \cdot 3$
5	$2 \cdot 3 \cdot 5$	$2 \cdot 3 \cdot 5$
6	$2^2 \cdot 3 \cdot 5$	$2^3 \cdot 3 \cdot 5$
7	$3 \cdot 5 \cdot 7 \cdot 11$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
8	$3 \cdot 5 \cdot 7 \cdot 11$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
9	$3 \cdot 5 \cdot 7 \cdot 11$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
10	$5 \cdot 7 \cdot 13$	$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 37 \cdot 53 \cdot 61 \cdot 79 \cdot 83$ $\cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 191$
11	$5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	none known
12	$5 \cdot 7 \cdot 11$	$2^4 \cdot 3^5 \cdot 5 \cdot 7 \cdot 11 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$

Divisibility Results for C_n

Thus, we have the following divisibility results for C_n:

- C_n is divisible by $(n-1)!$.
- If $p > 3$ is a prime and $p = n$, then $p \mid C_n$.
- If p is a prime with $n + 2 \le p < n + 2 + \frac{n-3}{6}$, then $p \mid C_n$.

n	Lower bound for $C_n/n!$	Upper bound for $C_n/n!$
2	1	1
3	2	2
4	$2 \cdot 3$	$2 \cdot 3$
5	$2 \cdot 3 \cdot 5$	$2 \cdot 3 \cdot 5$
6	$2^2 \cdot 3 \cdot 5$	$2^3 \cdot 3 \cdot 5$
7	$3 \cdot 5 \cdot 7 \cdot 11$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
8	$3 \cdot 5 \cdot 7 \cdot 11$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
9	$3 \cdot 5 \cdot 7 \cdot 11$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
10	$5 \cdot 7 \cdot 13$	$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 37 \cdot 53 \cdot 61 \cdot 79 \cdot 83$ $\cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 191$
11	$5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	none known
12	$5 \cdot 7 \cdot 11$	$2^4 \cdot 3^5 \cdot 5 \cdot 7 \cdot 11 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$

Divisibility Results for C_n for general $\mathcal{O}$

The last two results generalize to $\mathcal{O}$ exactly:

- If $q \in \mathcal{O}$ is a prime with $N(q) > 3$, then $q \mid C_{N(q)}$.
- If $q \in \mathcal{O}$ is a prime such that $n + 2 \leq N(q) < n + 2 + \frac{n-3}{6}$, then $q \mid C_n$.
- If $q \in \mathcal{O}$ is a prime, with $q \mid C_n$, then $q^{\left\lceil \frac{n}{N(q)} \right\rceil} \mid C_n$.

Unfortunately, the fact that $(n-1)! \mid C_n$ does not generalize easily.

Divisibility Results for C_n for general $\mathcal{O}$

The last two results generalize to $\mathcal{O}$ exactly:

- If $q \in \mathcal{O}$ is a prime with $N(q) > 3$, then $q \mid C_{N(q)}$.
- If $q \in \mathcal{O}$ is a prime such that $n + 2 \le N(q) < n + 2 + \frac{n-3}{6}$, then $q \mid C_n$.
- If $q \in \mathcal{O}$ is a prime, with $q \mid C_n$, then $q^{\left\lceil \frac{n}{N(q)} \right\rceil} \mid C_n$.

Unfortunately, the fact that $(n-1)! \mid C_n$ does not generalize easily.

Divisibility Results for C_n for general $\mathcal{O}$

The last two results generalize to $\mathcal{O}$ exactly:

- If $q \in \mathcal{O}$ is a prime with $N(q) > 3$, then $q \mid C_{N(q)}$.
- If $q \in \mathcal{O}$ is a prime such that $n + 2 \leq N(q) < n + 2 + \frac{n-3}{6}$, then $q \mid C_n$.
- If $q \in \mathcal{O}$ is a prime, with $q \mid C_n$, then $q^{\left\lceil \frac{n}{N(q)} \right\rceil} \mid C_n$.

Unfortunately, the fact that $(n-1)! \mid C_n$ does not generalize easily.

Divisibility Results for C_n for $\mathbb{Z}[i]$

Theorem (Gaussian Primes Theorem)

Suppose $q \in \mathbb{Z}[i]$. Then q is a Gaussian prime if and only if q is equal to a unit (± 1 or $\pm i$) multiplied by exactly one of the following:

(i) $1 + i$.
(ii) any rational prime $p \in \mathbb{Z}$ with $p \equiv 3 \pmod 4$.
(iii) any Gaussian integer $u + iv$ where $p = u^2 + v^2$ is a rational prime with $p \equiv 1 \pmod 4$.

Theorem

Suppose q is a Gaussian prime of type (i) or (iii), with $sN(q) < n + 1$ for some $s \in \mathbb{N}$. Let $0 \leq \ell \leq s$ be the highest power of q dividing n. Then $q^{s-\ell} \mid C_n$.

Divisibility Results for C_n for $\mathbb{Z}[i]$

Theorem (Gaussian Primes Theorem)

Suppose $q \in \mathbb{Z}[i]$. Then q is a Gaussian prime if and only if q is equal to a unit (± 1 or $\pm i$) multiplied by exactly one of the following:

(i) $1 + i$.
(ii) any rational prime $p \in \mathbb{Z}$ with $p \equiv 3 \pmod 4$.
(iii) any Gaussian integer $u + iv$ where $p = u^2 + v^2$ is a rational prime with $p \equiv 1 \pmod 4$.

Theorem

Suppose q is a Gaussian prime of type (i) or (iii), with $sN(q) < n + 1$ for some $s \in \mathbb{N}$. Let $0 \leq \ell \leq s$ be the highest power of q dividing n. Then $q^{s-\ell} \mid C_n$.

Divisibility Results for the $\mathbb{Z}[i]$-PTE Problem	
n	lower bound
2	1
3	$(1+i)^2$
4	1
5	$(1+i)^4(2+i)(2-i)$
6	$(1+i)^3(2+i)(2-i)$
7	$(1+i)^4(2+i)(2-i)\cdot 3$
8	$(1+i)^4(2+i)(2-i)$
9	$(1+i)^5(2+i)(2-i)\cdot 3^2\cdot(3+2i)(3-2i)$
10	$(1+i)^5(2+i)(2-i)(3+2i)(3-2i)$
11	$(1+i)^6(2+i)^2(2-i)^2$
12	$(1+i)^6(2+i)^2(2-i)^2$
13	$(1+i)^7(2+i)^2(2-i)^2(3+2i)(3-2i)(4+i)(4-i)$
14	$(1+i)^7(2+i)^2(2-i)^2(3+2i)(3-2i)(4+i)(4-i)$
15	$(1+i)^8(2+i)(2-i)(3+2i)(3-2i)$

Implementation and Results

- An algorithm that selects Gaussian integers, manipulates them, computes the interpolation polynomial and tests to see if it has an integer root has been written in Maple.
- To increase speed, this has since been coded in C++, using the Class Library for Numbers (CLN).
- Crucially, this problem is trivially parallelizeable. One divides the search space into intervals and assigns each processor an interval. No communication between the processors is necessary.
- Currently, these computations are running on a cluster with 16 nodes, each with 4 cores.
- Unfortunately, as of September 21, these computations are still in progress, although preliminary results agree with what has been done so far.

Implementation and Results

- An algorithm that selects Gaussian integers, manipulates them, computes the interpolation polynomial and tests to see if it has an integer root has been written in Maple.
- To increase speed, this has since been coded in C++, using the Class Library for Numbers (CLN).
- Crucially, this problem is trivially parallelizeable. One divides the search space into intervals and assigns each processor an interval. No communication between the processors is necessary.
- Currently, these computations are running on a cluster with 16 nodes, each with 4 cores.
- Unfortunately, as of September 21, these computations are still in progress, although preliminary results agree with what has been done so far.

Implementation and Results

- An algorithm that selects Gaussian integers, manipulates them, computes the interpolation polynomial and tests to see if it has an integer root has been written in Maple.
- To increase speed, this has since been coded in C++, using the Class Library for Numbers (CLN).
- Crucially, this problem is trivially parallelizeable. One divides the search space into intervals and assigns each processor an interval. No communication between the processors is necessary.
- Currently, these computations are running on a cluster with 16 nodes, each with 4 cores.
- Unfortunately, as of September 21, these computations are still in progress, although preliminary results agree with what has been done so far.

Implementation and Results

- An algorithm that selects Gaussian integers, manipulates them, computes the interpolation polynomial and tests to see if it has an integer root has been written in Maple.
- To increase speed, this has since been coded in C++, using the Class Library for Numbers (CLN).
- Crucially, this problem is trivially parallelizeable. One divides the search space into intervals and assigns each processor an interval. No communication between the processors is necessary.
- Currently, these computations are running on a cluster with 16 nodes, each with 4 cores.
- Unfortunately, as of September 21, these computations are still in progress, although preliminary results agree with what has been done so far.

Implementation and Results

- An algorithm that selects Gaussian integers, manipulates them, computes the interpolation polynomial and tests to see if it has an integer root has been written in Maple.
- To increase speed, this has since been coded in C++, using the Class Library for Numbers (CLN).
- Crucially, this problem is trivially parallelizeable. One divides the search space into intervals and assigns each processor an interval. No communication between the processors is necessary.
- Currently, these computations are running on a cluster with 16 nodes, each with 4 cores.
- Unfortunately, as of September 21, these computations are still in progress, although preliminary results agree with what has been done so far.

References

- P. Borwein, P. Lisoněk and C. Percival, *Computational investigations of the Prouhet-Tarry-Escott problem,* Math. Comp. **72** (2003), 2063–2070.
- P. Borwein, C. Ingalls, *The Prouhey-Tarry-Escott Problem revisited,* Enseign. Math. **40** (1994), 3–27.
- L. E. Dickson, *History of the Theory of Numbers Vol. II*, Chelsea Publ. Co., New York, 1971.
- E. Rees and C. Smyth, *On the Constant in the Tarry-Escott Problem*, Lecture Notes in Mathematics 1415, Springer, Berlin, 1990, 196–208.
- Chen Shuwen, The Prouhet-Tarry-Escott Problem. `http://euler.free.fr/eslp/TarryPrb.htm`
- E. M. Wright, *Prouhet's 1851 solution of the Tarry-Escott problem*, Amer. Math. Monthly **66** (1959) 199–201.