2016

On a Constant Associated with the Prouhet-Tarry-Escott Problem

Maria E. Markovich
University of South Carolina

On a Constant Associated with the Prouhet-Tarry-Escott Problem

by

Maria E. Markovich

Bachelor of Science

Shippensburg University, 2014

Submitted in Partial Fulfillment of the Requirements

For the Degree of Master of Arts in

Mathematics

College of Arts and Sciences

University of South Carolina

2016

Accepted by:

Michael Filaseta, Director of Thesis

Ognian Trifonov, Reader

Lacy Ford, Senior Vice Provost and Dean of Graduate Studies

Abstract

For n a positive integer, the Prouhet-Tarry-Escott Problem asks for two different sets of n positive integers for which the sum of the k^{th} powers of the elements of one set is equal to the sum of the k^{th} powers of the elements of the second set for each positive integer $k < n$. For $n > 12$, it is not known whether such sets exist. I will give some background on this problem and then show how Newton polygons can be used to determine information on the size of the 2-adic value of a certain constant associated with the problem.

Table of Contents

List of Figures

Chapter 1

Introduction

We discuss a result about a classical problem in Diophantine number theory, namely the Prouhet-Tarry-Escott problem (the PTE problem). The PTE problem asks for two distinct multisets of integers $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_n\}$ such that

$$\sum_{i=1}^{n} x_i^e = \sum_{i=1}^{n} y_i^e \qquad \text{for } e = 1, 2, \ldots, k \tag{1.1}$$

for some integer $k \leq n-1$. If X, Y satisfy (1.1) then the pair is called a *s*olution of the PTE problem, denoted as $X =_k Y$. A solution is *ideal* if $k = n-1$. We call n the size of the solution and k the degree. The largest known ideal solution is of size $n = 12$ [1]. However, there is no known ideal solution of size $n = 11$ [1].

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be n variables. Then,

$$\begin{aligned}
\sigma_1 &= \alpha_1 + \alpha_2 + \cdots \alpha_n \\
\sigma_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n \\
\sigma_3 &= \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \cdots + \alpha_{n-2}\alpha_{n-1}\alpha_n \\
&\vdots \quad \vdots \\
\sigma_n &= \alpha_1\alpha_2 \cdots \alpha_n
\end{aligned}$$

are the elementary symmetric functions in $\alpha_1, \alpha_2, \ldots, \alpha_n$. We recall the following result about symmetric polynomials.

Lemma 1. *Let R be a commutative ring with an identity. Then every symmetric polynomial in $\alpha_1, \ldots, \alpha_n$ with coefficients in R is expressible as a polynomial in $\sigma_1, \ldots, \sigma_n$ with coefficients in R.*

Proof. For a symmetric $h(\alpha_1, \ldots, \alpha_n) \in R[\alpha_1, \ldots, \alpha_n]$, we set $T = T_h$ to be the set of n-tuples $(\ell_1, \ldots, \ell_n)$ with the coefficient of $\alpha_1^{\ell_1} \cdots \alpha_n^{\ell_n}$ in $h(\alpha_1, \ldots, \alpha_n)$ non-zero. We define the *size* of h to be $(k_1, \ldots, k_n)$ where $(k_1, \ldots, k_n)$ is the element of T with k_1 as large as possible, k_2 as large as possible given k_1, etc. Since $h(\alpha_1, \ldots, \alpha_n)$ is symmetric, it follows that $(\ell_1, \ldots, \ell_n) \in T$ if and only if each permutation of $(\ell_1, \ldots, \ell_n)$ is in T. This implies that $k_1 \geq k_2 \geq \cdots \geq k_n$. Observe that we can use the notion of size to form an ordering on the elements of $R[\alpha_1, \ldots, \alpha_n]$ in the sense that if h_1 has size $(k_1, \ldots, k_n)$ and h_2 has size $(k'_1, \ldots, k'_n)$, then $h_1 > h_2$ if there is an $i \in \{0, 1, \ldots, n-1\}$ such that $k_1 = k'_1, \ldots, k_i = k'_i$, and $k_{i+1} > k'_{i+1}$. Note that the elements of $R[\alpha_1, \ldots, \alpha_n]$ which have size $(0, 0, \ldots, 0)$ are precisely the constants (the elements of R).

Suppose now that $(k_1, \ldots, k_n)$ is the size of some symmetric $g \in R[\alpha_1, \ldots, \alpha_n]$ with $g \notin R$. For non-negative integers $d_1, \ldots, d_n$, the size of $h = \sigma_1^{d_1} \sigma_2^{d_2} \cdots \sigma_n^{d_n}$ is $(d_1 + d_2 + \cdots + d_n, d_2 + \cdots + d_n, \ldots, d_{n-1} + d_n, d_n)$. Taking $d_1 = k_1 - k_2, d_2 = k_2 - k_3, \ldots, d_{n-1} = k_{n-1} - k_n$, and $d_n = k_n$, we get the size of h is $(k_1, \ldots, k_n)$. The coefficient of $\alpha_1^{k_1} \cdots \alpha_n^{k_n}$ in h is 1. It follows that there is an $a \in R$ such that $g - ah$ is of smaller size than g.

The above implies that for any symmetric element $f \in R[\alpha_1, \ldots, \alpha_n]$, there exist $a_1, \ldots, a_m \in R$ and $h_1, \ldots, h_m \in R[\sigma_1, \ldots, \sigma_n]$ such that $f - a_1 h_1 - \cdots - a_m h_m$ has size $(0, 0, \ldots, 0)$. This implies the lemma. □

Taking R to be the ring on integers, we use Lemma 1 to prove the following lemma [1].

Lemma 2. *Let n and k be integers with $1 \leq k < n$. Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ denote arbitrary integers. The following are equivalent:*

$$\sum_{i=1}^{n} x_i^e = \sum_{i=1}^{n} y_i^e \qquad \text{for } e = 1, 2, \ldots, k, \tag{1.2}$$

$$\deg\left(\prod_{i=1}^{n}(z - x_i) - \prod_{i=1}^{n}(z - y_i)\right) \leq n - (k+1) = n - k - 1 \tag{1.3}$$

$$(z-1)^{k+1} \Big| \left(\sum_{i=1}^{n} z^{x_i} - \sum_{i=1}^{n} z^{y_i}\right) \tag{1.4}$$

Proof. We begin by proving (1.2) $\implies$ (1.3). Let

$$\sum_{i=1}^{n} x_i^e = \sum_{i=1}^{n} y_i^e \qquad \text{for } e = 1, 2, \ldots, k.$$

Further, we define,

$$f(z) = \prod_{i=1}^{n}(z - x_i) \quad \text{and} \quad g(z) = \prod_{i=1}^{n}(z - y_i).$$

Upon expanding, we have,

$$f(z) = z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \cdots + (-1)^n \sigma_n$$
$$g(z) = z^n - \sigma_1' z^{n-1} + \sigma_2' z^{n-2} - \cdots + (-1)^n \sigma_n',$$

where σ_j signifies the sum of each product of j of the x_i (with distinct subscripts), and the σ_j' are similarly defined using the y_j. Thus,

$$\sigma_1 = \sum_{i=1}^{n} x_i$$
$$\sigma_2 = \sum_{1 \leq i < j \leq n} x_i x_j$$
$$\vdots$$

Note that

$$\sigma_1 = \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} y_i = \sigma_1'$$

by assumption. Further,

$$\begin{aligned}\sum_{i=1}^{n} x_i^2 &= (x_1 + \cdots + x_n)(x_1 + \cdots + x_n) - 2(x_1x_2 + \cdots + x_nx_{n-1}) \\ &= \sigma_1^2 - 2\sigma_2\end{aligned}$$

and

$$\begin{aligned}\sum_{i=1}^{n} y_i^2 &= (y_1 + \cdots + y_n)(y_1 + \cdots + y_n) - 2(y_1y_2 + \cdots + y_ny_{n-1}) \\ &= (\sigma_1')^2 - 2\sigma_2'.\end{aligned}$$

For $k \geq 2$, we have

$$\sum_{i=1}^{n} x_i^2 = \sum_{i=1}^{n} y_i^2,$$

so that

$$\begin{aligned}\sigma_1^2 - 2\sigma_2 &= (\sigma_1')^2 - 2\sigma_2' \\ &= \sigma_1^2 - 2\sigma_2'.\end{aligned}$$

Hence $\sigma_2 = \sigma_2'$. This trend continues until we deduce that $\sigma_j = \sigma_j'$, for all $j \leq k$. We lastly consider the difference

$$\begin{aligned}f(z) - g(z) &= \prod_{i=1}^{n}(z - x_i) - \prod_{i=1}^{n}(z - y_i) \\ &= (z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \cdots + (-1)^n\sigma_n) \\ &\quad - (z^n - \sigma_1' z^{n-1} + \sigma_2' z^{n-2} - \cdots + (-1)^n\sigma_n').\end{aligned}$$

Since $\sigma_i = \sigma_i'$ for $1 \leq i \leq k$, we have

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

This completes the proof of (1.2) $\implies$ (1.3).

Next, we establish (1.3) $\implies$ (1.2). For $k=1$, from (1.3), we deduce that the coefficient of z^{n-1} must be the same in both $f(z)$ and $g(z)$. That is, based off of the notation above, $\sigma_1 = \sigma_1'$. This establishes that (1.3) $\implies$ (1.2) for $k=1$. We suppose that (1.3) $\implies$ (1.2) for $k \leq k_0$ for some $1 \leq k_0 < n-1$ and prove by way of induction that (1.3) $\implies$ (1.2) for $k = k_0+1$.

For $1 \leq e \leq n-1$, define $S_e = \sum\limits_{i=1}^{n} x_i^e$ and $S_e' = \sum\limits_{i=1}^{n} y_i^e$. Newton's Identities imply

$$\sum_{i=1}^{n} x_i^e = \sigma_1 S_{e-1} - \sigma_2 S_{e-2} + \cdots \pm \sigma_{e-1} S_1 \mp e\sigma_e$$

and

$$\sum_{i=1}^{n} y_i^e = \sigma_1' S_{e-1}' - \sigma_2' S_{e-2}' + \cdots \pm \sigma_{e-1}' S_1' \mp e\sigma_e'.$$

Given (1.3) holds for $k = k_0+1$, we deduce that $\sigma_i = \sigma_i'$ for $1 \leq i \leq k_0+1$. Also, (1.3) will hold for $k=k_0$, so that by the induction hypothesis $S_e = S_e'$ for $e \leq k_0$. Taking $e = k_0+1$ above, we deduce that

$$\begin{aligned}\sum_{i=1}^{n} x_i^{k_0+1} &= \sigma_1 S_{k_0} - \sigma_2 S_{k_0-1} + \cdots \pm \sigma_{k_0} S_1 \mp (k_0+1)\sigma_{k_0+1} \\ &= \sigma_1' S_{k_0}' - \sigma_2' S_{k_0-1}' + \cdots \pm \sigma_{k_0}' S_1' \mp (k_0+1)\sigma_{k_0+1}' = \sum_{i=1}^{n} y_i^{k_0+1}.\end{aligned}$$

Thus, (1.2) holds for $k = k_0+1$, completing the proof that (1.3) $\implies$ (1.2).

Next, we show that (1.2) $\implies$ (1.4). We consider the function

$$F(w) = \sum_{i=1}^{n} w^{x_i} - \sum_{i=1}^{n} w^{y_i},$$

so that

$$\begin{aligned} F'(w) &= \sum_{i=1}^{n} x_i w^{x_i-1} - \sum_{i=1}^{n} y_i w^{y_i-1} \\ &\vdots \\ F^{(k)}(w) &= \sum_{i=1}^{n} x_i \cdots (x_i-(k-1)) w^{x_i-k} - \sum_{i=1}^{n} y_i \cdots (y_i-(k-1)) w^{y_i-k}. \end{aligned}$$

Observe that $F(1) = 0$ and (1.2) implies $F'(1) = \sum_{i=1}^{n} x_i - \sum_{i=1}^{n} y_i = 0$. For $k \geq 2$, we also deduce from (1.2) that

$$\begin{aligned} F''(1) &= \sum_{i=1}^{n} x_i(x_i-1) - \sum_{i=1}^{n} y_i(y_i-1) \\ &= \left(\sum_{i=1}^{n} x_i^2 - \sum_{i=1}^{n} y_i^2 \right) - \left(\sum_{i=1}^{n} x_i - \sum_{i=1}^{n} y_i \right) = 0. \end{aligned}$$

Continuing in this manner, we deduce that (1.2) implies

$$F(1) = F'(1) = F''(1) = \cdots = F^{(k)}(1) = 0.$$

Hence, $F(w)$ has a root at $w = 1$ with multiplicity $k+1$. Therefore,

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

establishing (1.4).

Lastly, we prove (1.4) $\implies$ (1.2). Let

$$h(z) = \sum_{i=1}^{n} z^{x_i} - \sum_{i=1}^{n} z^{y_i}.$$

Thus, (1.4) is the same as $(z-1)^{k+1} | h(z)$. In other words, $h(z)$ has a zero at $z = 1$ of order $k+1$. It follows that $h^{(j)}(1) = 0$ for $0 \leq j \leq k$. Since

$$h'(z) = \sum_{i=1}^{n} x_i z^{x_i-1} - \sum_{i=1}^{n} y_i z^{y_i-1},$$

we obtain

$$h'(1) = \sum_{i=1}^{n} x_i - \sum_{i=1}^{n} y_i = 0 \implies \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} y_i.$$

Since

$$\begin{aligned} z \cdot h'(z) &= z \left(\sum_{i=1}^{n} x_i z^{x_i - 1} - \sum_{i=1}^{n} y_i z^{y_i - 1} \right) \\ &= \sum_{i=1}^{n} x_i z^{x_i} - \sum_{i=1}^{n} y_i z^{y_i}, \end{aligned}$$

we obtain by taking a derivative that

$$h'(z) + z \cdot h''(z) = \sum_{i=1}^{n} x_i^2 z^{x_i - 1} - \sum_{i=1}^{n} y_i^2 z^{y_i - 1}. \tag{1.5}$$

Setting $z = 1$ into (1.5), for $k \geq 2$, we have

$$0 = h'(1) + 1 \cdot h''(1) = \sum_{i=1}^{n} x_i^2 - \sum_{i=1}^{n} y_i^2 \implies \sum_{i=1}^{n} x_i^2 = \sum_{i=1}^{n} y_i^2.$$

Continuing in this manner, by successfully multiplying by x, taking a derivative, and setting $x = 1$, we obtain

$$\sum_{i=1}^{n} x_i^e = \sum_{i=1}^{n} y_i^e \quad \text{for } e = 1, 2, \ldots, k.$$

This completes the proof that (1.4) $\implies$ (1.2) and, hence, the proof of Lemma 2. □

Corollary 3. *The pair of multisets* $\{x_1, \ldots, x_n\}$, $\{y_1, \ldots, y_n\}$ *is an ideal PTE solution if and only if*

$$\prod_{i=1}^{n} (z - x_i) - \prod_{i=1}^{n} (z - y_i) = C \tag{1.6}$$

for some real constant C*.*

Proof. This follows immediately from the fact that $k = n - 1$ is the degree of an ideal solution. Using Lemma 2 and $k = n - 1$, we see that (1.3) is equivalent to

$$\deg \left(\prod_{i=1}^{n} (z - x_i) - \prod_{i=1}^{n} (z - y_i) \right) \leq 0.$$

Thus, the corollary follows from the equivalence of (1.2) and (1.3). □

Corollary 4. *Let $a \in \mathbb{Z}$. The pair of multisets $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_n\}$ is an ideal PTE solution if and only if the pair of multisets $\{x_1 + a, \ldots, x_n + a\}$ and $\{y_1 + a, \ldots, y_n + a\}$ is an ideal PTE solution*

Proof. From Corollary 3, it is sufficient to observe that (1.6) holds if and only if

$$\prod_{i=1}^{n}(z - a - x_i) - \prod_{i=1}^{n}(z - a - y_i) = C \tag{1.7}$$

holds. Indeed, it is clear that the difference of the left and right side of (1.6) has infinitely many zeroes if and only if the difference of the left and right side of (1.7) has infinitely many zeroes, from which the result follows. □

As a consequence, we can translate ideal solutions as in Corollary 4 to obtain new ideal solutions. We will use this at various stages of our arguments.

Definition 5. *Let $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_n\}$, where $X =_{n-1} Y$ is an ideal solution. We define*

$$C_n(X, Y) = \prod_{i=1}^{n}(z - x_i) - \prod_{i=1}^{n}(z - y_i).$$

Further, we define

$$\overline{C}_n = \prod_{j=1}^{\infty} p_j^{e_j},$$

where

$$e_j = \min\{e : p_j^e \| C_n(X, Y) \text{ for some } X \text{ and } Y \text{ with } X =_{n-1} Y\}.$$

There has been some interest in determining the exact values of $\overline{C}_n$ (cf. [1] and

[2]). The values of $\overline{C}_n$ for $2 \leq n \leq 7$ are known:

$$\overline{C}_2 = 1$$

$$\overline{C}_3 = 2^2$$

$$\overline{C}_4 = 2^2 \cdot 3^2$$

$$\overline{C}_5 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$$

$$\overline{C}_6 = 2^5 \cdot 3^2 \cdot 5^2$$

$$\overline{C}_7 = 2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11.$$

In this thesis, we pay particular attention to ideal solutions of sizes 8 and 9. For these, according to [2], it is known that

$$\overline{C}_8 = 2^{e_1} \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13, \quad \text{where } 4 \leq e_1 \leq 8$$

$$\overline{C}_9 = 2^{e_2} \cdot 3^{e_3} \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17^{e_4} \cdot 23^{e_5} \cdot 29^{e_6}, \quad \text{where } 7 \leq e_2 \leq 9,\ 3 \leq e_3 \leq 4,\ 0 \leq e_j \leq 1, \text{ for } j \in \{4,5,6\}.$$

After discussing further preliminary material in Chapter II, we show in Chapter III that $2^9 \| \overline{C}_9$ (so $e_2 = 9$). Further, in Chapter IV, we show that $2^6 | \overline{C}_8$ (so $6 \leq e_1 \leq 8$). We do not know if $2^8 | \overline{C}_8$. In particular, our arguments are based on working modulo small powers of 2 (taking advantage of information from Newton polygons) and on obtaining contradictions to (1.6) by considering the largest power of 2 that divides the left-hand side of (1.6) for different choices of $z \in \mathbb{Z}$. The example

$$X = \{221, 259, 274, 278, 292, 320, 375, 473\}$$

and

$$Y = \{42, 606, 652, 699, 721, 1413, 2424, 4127\}$$

has the property that

$$\prod_{i=1}^{8}(z-x_i)-\prod_{i=1}^{8}(z-y_i)\equiv 128 \pmod{2^{12}}.$$

In particular, for any value of $z\in\mathbb{Z}$, the left-hand side is exactly divisible by 2^7, and arguments showing (1.6) cannot hold with $2^7\|\overline{C}_8$ modulo a power of 2 less than 2^{12} are not possible. Thus, it is unlikely our same methods can provide a proof that $2^8|\overline{C}_8$. Similarly, the example

$$X=\{24,135,152,153,170,199,345,426\}$$

and

$$Y=\{21,22,525,611,622,772,1979,2172\}$$

has the property that

$$\prod_{i=1}^{8}(z-x_i)-\prod_{i=1}^{8}(z-y_i)\equiv 64 \pmod{2^{10}}.$$

In the way of a slightly different example, we note that

$$\begin{aligned}X=\{&31914804930538,392011859134314,414199788923609,\\&550721232905543,563570240533272,870589495146520,\\&1039460985683225,1113937730497799\}\end{aligned}$$

and

$$\begin{aligned}Y=\{&226375709153429,382003430459158,502458387218286,\\&690280771238587,750383096702563,764464731978500,\\&790357673966989,870082337037308\}\end{aligned}$$

has the property that

$$\prod_{i=1}^{8}(z-x_i)-\prod_{i=1}^{8}(z-y_i)\equiv 954668492881984 \pmod{2^{50}}.$$

Of interest here is that the number 954668492881984 is exactly divisible by 2^6. Perhaps these examples exist for the obvious reason that $2^6\|\overline{C}_8$, but we cannot show this.

The examples above raise the following natural question.

Question: Let p be a prime. Is it possible to have a p-adic solution to

$$\prod_{i=1}^{n}(z-x_i)-\prod_{i=1}^{n}(z-y_i)=C,$$

for which $\nu_p(C)<\nu_p\Big(\overline{C}_n\Big)$, where ν_p is the usual p-adic valuation?

Chapter 2

Further preliminaries

We write

$$f(z) = \prod_{j=1}^{n}(z - x_j) = \sum_{j=0}^{n} a_j z^j \quad \text{and} \quad g(z) = \prod_{j=1}^{n}(z - y_j) = \sum_{j=0}^{n} b_j z^j$$

where $x_j, y_j \in \mathbb{Z}$ are chosen so that

$$f(z) - g(z) = C_n \tag{2.1}$$

and so that the exact power of 2 dividing C_n is equal to the exact power of 2 dividing $\overline{C}_n$. Thus, by Corollary 3, we have that $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_n\}$ is an ideal solution. Recall that we write this as $X =_{n-1} Y$. We write $C = C_n$, where n should be clear from the context.

Definition 6. *For $m \in \mathbb{Z} - \{0\}$ and p a prime, $\nu_p(m)$ denotes the nonnegative integer k such that $p^k \| m$. We further define $\nu_p(0) = +\infty$.*

For fixed n, we consider the two sets of points in the extended plane

$$S_1 = \{(j, \nu_2(a_{n-j})) : 0 \le j \le n\} \quad \text{and} \quad S_2 = \{(j, \nu_2(b_{n-j})) : 0 \le j \le n\}.$$

Since $f(z) - g(z) = C$, a constant, we see that $a_{n-j} = b_{n-j}$ for $0 \le j \le n-1$. Otherwise, we would have that $f(z) - g(z)$ is a polynomial with degree at least 1. Thus, S_1 and S_2 have at least n of $n+1$ points in common.

We translate $f(z)$ and $g(z)$ by the same translation, if necessary, so that $a_0 \neq 0$ and $b_0 \neq 0$. Thus, $\nu_2(a_0) \neq +\infty$ and $\nu_2(b_0) \neq +\infty$. Note that (2.1) still holds. This ensures that the remaining points $(n, \nu_2(a_0))$ and $(n, \nu_2(b_0))$, which may differ in S_1 and S_2, are in the finite plane.

We will be interested in Newton polygons, and in particular to a result that goes back to work of Dumas [3].

Definition 7 (Newton Polygon)**.** *Let $F(z) = \sum_{j=0}^{n} c_j z^j \in \mathbb{Z}[z]$ with $c_0 c_n \neq 0$. Let p be a prime. For $j \in \{0, \cdots, n\}$, we define $x_j = j$ and define $y_j = \nu_p(c_{n-j})$. We consider the lower edges along the convex hull of the points in $S = \{(x_0, y_0), \cdots, (x_n, y_n)\}$. The polygonal path formed by these edges is called the Newton polygon associated with $F(z)$ with respect to p.*

Thus, the Newton polygon of $f(z)$ with respect to the prime 2 is exactly the lower convex hull of the points in S_1. Similarly, the Newton polygon of $g(z)$ with respect to 2 is the lower convex hull of the points in S_2. Note that the slopes of the edges of the Newton polygons increase from left to right. The following is an important property of Newton polygons applicable to our current situation.

Lemma 8. *The Newton polygons of $f(z)$ and $g(z)$ will each pass through $n+1$ lattice points (including the endpoints), which we denote respectively as*

$$T_1 = \{(j, t_j) : 0 \leq j \leq n\} \quad \text{and} \quad T_2 = \{(j, t'_j) : 0 \leq j \leq n\}$$

After possibly rearranging the x_j and y_j, we have $2^{t_j - t_{j-1}}$ exactly divides x_j and $2^{t'_j - t'_{j-1}}$ exactly divides y_j for each $j \in \{1, 2, \cdots, n\}$.

This lemma follows directly from a theorem of Dumas [3] which asserts that the Newton polygon of a product of two polynomials with respect to a prime p can

be obtained by translating the edges of the Newton polygons for each polynomial with respect to p. Since $f(z)$ and $g(z)$ are a product of n linear factors, we have that the Newton polygons associated with $f(z)$ and $g(z)$ each have ten lattice points (including endpoints) along its edges.

As a consequence of Lemma 8, the slope of each edge of the Newton polygon of $f(z)$ and $g(z)$ is an integer. In the last statement of Lemma 8, we observe that this implies that the values $\nu_2(x_j)$ and $\nu_2(y_j)$ are increasing as j ranges from 1 to n.

We consider the following figures as potential Newton polygons for $f(z)$ in Figure 2.1 and $g(z)$ in Figure 2.2, where $n = 9$.

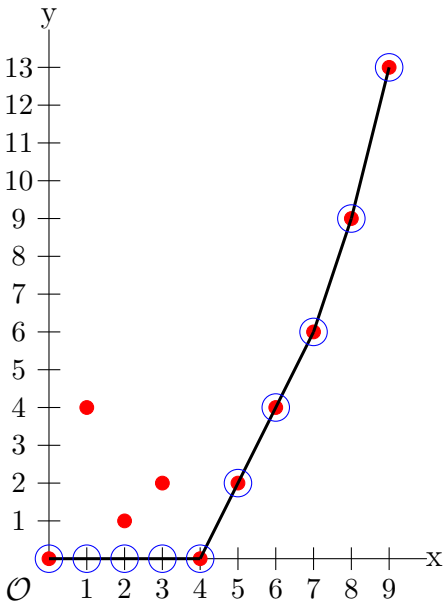

Figure 2.1: NP 1

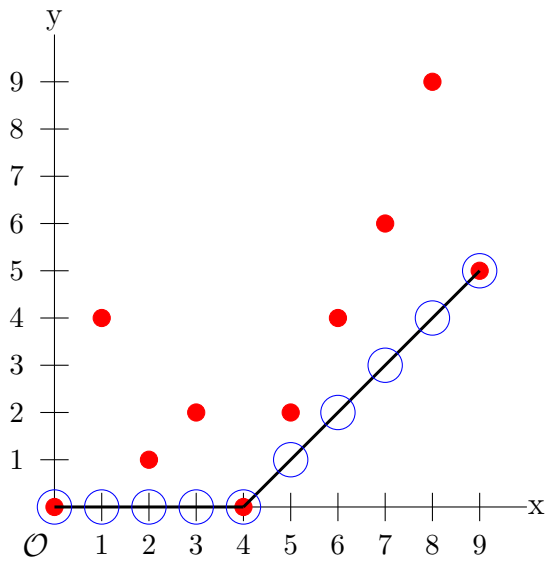

Figure 2.2: NP 2

Note that the solid circles represent the points of S_1 and S_2 with the bottom left-hand endpoint equal to $(0, 0)$ in each case (since the polynomials are monic). Further, the open circles refer to the lattice points in T_1 and T_2 as mentioned in Lemma 8. In these figures, the 9 points in S_1 that are identical to points in S_2 correspond to the x-coordinates in $[0, 8]$. Following Lemma 8, the lattice points associated with

Figures 2.1 and 2.2 are as follows:

$$T_1 = \{(0,0),(1,0),(2,0),(3,0),(4,0),(5,2),(6,4),(7,6),(8,9),(9,13)\},$$

and

$$T_2 = \{(0,0),(1,0),(2,0),(3,0),(4,0),(5,1),(6,2),(7,3),(8,4),(9,5)\}.$$

We note that in general, unlike S_1 and S_2, the points other than $(0,0)$ belonging to T_1 and T_2 can be different. Looking at the height differences between two consecutive lattice points in T_1, referring to Lemma 8, we note that there are exactly four odd x_j's, three x_j's that are exactly divisible by 4, one x_j exactly divisible by 8, and one x_j that is exactly divisible by 16. Similarly for T_2, there are exactly four y_j's that are odd and five y_j's that are exactly divisible by 2. By considering the following lemma, we can immediately see that Figure 2.1 and Figure 2.2 cannot be the Newton polygons for $f(z)$ and $g(z)$.

Lemma 9. *If the points $(n, \nu_2(a_0))$ in S_1 and $(n, \nu_2(b_0))$ in S_2 are distinct and*

$$k = \min\{\nu_2(a_0), \nu_2(b_0)\},$$

then $2^k \| C$.

Proof. By hypothesis, we assume that a_0 and b_0 are distinct. Since $C = a_0 - b_0$, we see that

$$\nu_2(C) = \nu_2(a_0 - b_0) = \min\{\nu_2(a_0), \nu_2(b_0)\} = k;$$

thus, $2^k \| C$. □

We note that $2^{\nu_2(a_0)}$ exactly divides the constant term of $f(z)$ and $2^{\nu_2(b_0)}$ exactly divides the constant term of $g(z)$. Hence according to Figure 2.1 and Figure 2.2, we

see that $2^{\nu_2(b_0)} = 2^5 \| C$, which is a contradiction since it is known that 2^7 divides C [2].

We develop some notation that we will be using in the subsequent chapters. Let k_1 be the number of odd x_j and k_1' be the number of odd y_j; thus, the 2-valuation of each of these x_j and y_j is equal to 0. Further, we let k_2 be the number of x_j which are congruent to 2 (mod 4) and k_2' be the number of y_j that are congruent to 2 (mod 4); thus, the 2-valuation of each of these x_j and y_j is equal to 1.

By translating $f(z)$ and $g(z)$ by 1 (or some odd number to guarantee that a_0 and b_0 are not equal to 0), we may suppose $k_1' \leq \lfloor n/2 \rfloor$. Furthermore, we may now translate by 2 (or some other number that is congruent to 2 (mod 4)) if needed to obtain that $k_2' \geq \lceil (n - k_1')/2 \rceil$ of the y_j are congruent to 2 (mod 4). To make this concept explicit, after translating as above, we note that Figure 2.2 could be the Newton polygon of $g(z)$ since in this case $k_1' = 4 = \lfloor 9/2 \rfloor$ and $k_2' = 5 \geq 3 = \lceil (9 - k_1')/2 \rceil$. However, after our translations, Figure 2.1 could not be the Newton polygon of $g(z)$ since in this case $k_1' = 4$ but $k_2' = 0 < 3 = \lceil (9 - k_1')/2 \rceil$.

Using the following proposition from Caley [2], we deduce that if C is even, then $k_1 = k_1'$.

Lemma 10. *Let $\{x_1, \ldots, x_n\} =_{n-1} \{y_1, \ldots, y_n\}$ be two multisets of integers that constitute an ideal PTE solution, and suppose that a prime p divides the constant C associated with this solution. Then we can reorder the integers y_i so that*

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

Proof. Let p be a prime dividing C; thus, $C \equiv 0 \pmod{p}$. We consider the field of p elements, $\mathbb{F}_p$. Since $\prod_{j=1}^{n}(z - x_j) - \prod_{j=1}^{n}(z - y_j) = C \equiv 0 \pmod{p}$, we have

$$\prod_{j=1}^{n}(z - x_j) \equiv \prod_{j=1}^{n}(z - y_j) \pmod{p},$$

in $\mathbb{F}_p[x]$. Since $\mathbb{F}_p$ is a field, we have that the polynomial ring $\mathbb{F}_p[x]$ is a unique factorization domain. Since each factor $z - x_i$ and $z - y_i$ is irreducible, we have that the multisets $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_n\}$ are equal as subsets of $\mathbb{F}_p$. That is to say, after reordering, $x_i \equiv y_i \pmod{p}$ for $i = 1, \ldots, n$. □

Taking $p = 2$ in Lemma 10, we obtain the fact that the number of odd x_j must equal the number of odd y_j, that is, $k_1 = k_1'$. Further, we can interchange the roles of $f(z)$ and $g(z)$, if necessary, so that $k_2' \geq k_2$. Since there are n elements in the multisets X and Y, it must be the case that $k_1 + k_2 \leq n$ and $k_1' + k_2' \leq n$.

Before ending this chapter, we establish the following.

Lemma 11. *Let $n \geq 8$. Suppose $\{x_1, \ldots, x_n\} =_{n-1} \{y_1, \ldots, y_n\}$. For $1 \leq j \leq n$, let x_j and y_j be such that $x_1, \ldots, x_t$ and $y_1, \ldots, y_t$ are odd and otherwise x_j and y_j are even. Then*

$$x_1^k + \cdots + x_t^k \equiv y_1^k + \cdots + y_t^k \pmod{16}, \quad \textit{for } k \geq 1.$$

and

$$x_{t+1}^k + \cdots + x_n^k \equiv y_{t+1}^k + \cdots + y_n^k \pmod{16}, \quad \textit{for } k \geq 1. \tag{2.2}$$

Proof. Since $x_1, \ldots, x_t$ and $y_1, \ldots, y_t$ are odd, we obtain

$$x_j^4 \equiv y_j^4 \equiv 1 \pmod{16}, \quad \text{for } 1 \leq j \leq t.$$

Thus,

$$x_1^k + \cdots + x_t^k \equiv x_1^{k+4} + \cdots + x_t^{k+4} \pmod{16}$$

and

$$y_1^k + \cdots + y_t^k \equiv y_1^{k+4} + \cdots + y_t^{k+4} \pmod{16}.$$

As $x_j^{k+4} \equiv y_j^{k+4} \equiv 0 \pmod{16}$ for $t+1 \le j \le n$, we deduce that

$$\begin{aligned} x_1^k + \cdots + x_t^k &\equiv x_1^{k+4} + \cdots + x_t^{k+4} \equiv x_1^{k+4} + \cdots + x_n^{k+4} \\ &\equiv y_1^{k+4} + \cdots + y_n^{k+4} \equiv y_1^{k+4} + \cdots + y_t^{k+4} \equiv y_1^k + \cdots + y_t^k \pmod{16}, \end{aligned}$$

provided $1 \le k+4 \le n-1$. Since $n \ge 8$, the above holds for $1 \le k \le 3$. On the other hand,

$$x_1^k + \cdots + x_n^k = y_1^k + \cdots + y_n^k, \quad \text{for } 1 \le k \le 3.$$

Hence,

$$x_{t+1}^k + \cdots + x_n^k \equiv y_{t+1}^k + \cdots + y_n^k \pmod{16}, \quad \text{for } 1 \le k \le 3.$$

The lemma follows since for $k \ge 4$, both sides of the congruence in (2.2) are divisible by 16. □

Chapter 3

The 2-adic value of $\overline{C}_9$

It is known that $2^7|\overline{C}_9$ and $2^{10} \nmid \overline{C}_9$ [2]. Our goal in this chapter is to increase the lower bound of the valuation of 2 in $\overline{C}_9$. Using Newton polygons in the PTE problem, we establish $2^9|\overline{C}_9$ from which we can deduce that $2^9\|\overline{C}_9$.

We make use of the notation in the previous chapter with $n = 9$ and deal with two cases, each involving multiple subcases, depending on the values of k_1' and k_2'.

Case 1. $k_1' + k_2' = 9$

In this case, we are assuming that there are no elements in the multiset Y that are congruent to 0 (mod 4). We consider possibilities for the Newton polygon of $f(z)$. From Lemma 10, we know that $k_1 = k_1'$ odd x_j's are in the multiset X. Additionally, the slopes of the Newton polygon of $f(z)$ are integers. We recall that $k_2 \leq k_2'$, which implies that X contains at most k_2' elements that are divisible by 2 exactly once. Combining these facts, we have that each point $(j, \nu_2(a_{9-j}))$ in S_1 is on or above the corresponding point $(j, \nu_2(b_{9-j}))$ in S_2.

Case 1.1. $k_2 = k_2'$

By construction, we supposed $k_1' \leq 4$. Therefore, in this subcase, k_2 and k_2' are both greater than or equal to 5. We consider what happens when $z = 2$ in (2.1). That is,

we consider

$$f(2) - g(2) = \prod_{j=1}^{9}(2 - x_j) - \prod_{j=1}^{9}(2 - y_j),$$

where at least five of the x_j's and at least five of the y_j's are 2 modulo 4. Thus, 2^{10} divides each product, and therefore, their difference. This implies a contradiction, since $2^{10} \nmid C$.

Case 1.2. $k_2 < k_2'$

In this subcase, X must contain some elements that are congruent to 0 (mod 4) but Y cannot. We deduce that the right-most point of the Newton polygon of $f(z)$ is above the point $(9, \nu_2(b_0))$. Since these endpoints are distinct, by Lemma 9 we have $2^{\nu_2(b_0)} \| C$. Since all of the even elements in Y are congruent to 2 (mod 4) (thus have valuation equal to 1 with respect to the prime 2), we have that $\nu_2(b_0) = k_2'$. In the case under consideration, $\nu_2(b_0) = k_2' = 9 - k_1'$. By assumption $2^7 \mid C$; thus, $k_2' \geq 7$ and $k_1' \leq 2$.

Figure 3.1 and Figure 3.2 are possible Newton polygons for $f(z)$ and $g(z)$.

Case 1.2.1. $k_1' = 2$

Letting $k_1' = 2$ as in Figure 3.2, we arrive at a contradiction as follows. Consider the constant term in the expansion of the product

$$(z - y_3)(z - y_4)(z - y_5)(z - y_6)(z - y_7)(z - y_8)(z - y_9). \tag{3.1}$$

We note that in this case, $y_j \equiv 2 \pmod 4$ for $3 \leq j \leq 9$. Hence, we see that the constant term is divisible by 2^7. Further, the coefficient on z in the above product is given by

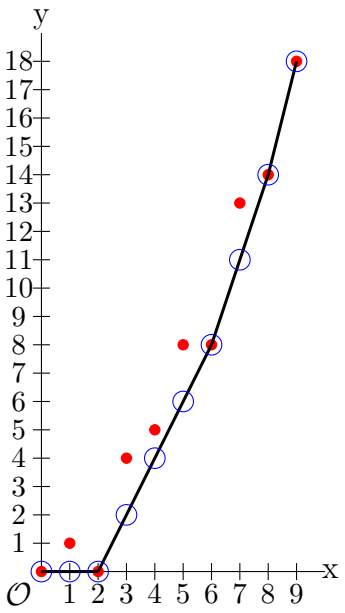

Figure 3.1: NP 3

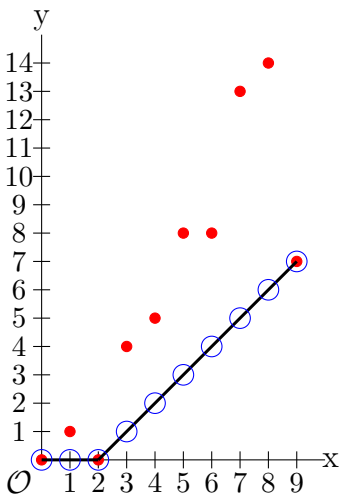

Figure 3.2: NP 4

$$y_3y_4y_5y_6y_7y_8 + y_3y_4y_5y_6y_7y_9 + y_3y_4y_5y_6y_8y_9 + \cdots + y_4y_5y_6y_7y_8y_9, \tag{3.2}$$

the sum of the product of combinations of 6 roots taken at a time. Thus, in total, there are seven terms in the summation, each of which is 2^6 times an odd number. Hence, the coefficient on z in the product above is exactly divisible by 2^6. Next, we consider $(z - y_1)(z - y_2) = z^2 - (y_1 + y_2)z + y_1y_2$. Recall y_1 and y_2 are both odd. Thus, the constant term y_1y_2 is also odd. Further, the coefficient on z is even, since it is the sum of two odd numbers. Multiplying the two products above gives us the expression for $g(z)$. We now consider the coefficient of z in $g(z)$, given by the sum of

$$\Big(\text{the product of the constant term in (3.1) and } -(y_1 + y_2)\Big) + \Big(\text{the product of (3.2) and } y_1y_2\Big).$$

Note that this sum is exactly divisible by 2^6. Hence, $(8, 6)$ must be a point in S_2. Since the points in S_1 and S_2 agree for $0 \leq j \leq 8$, we have that $(8, 6)$ is also a point

in S_1. Recall $k_1 = k_1' = 2$ and the slopes of the edges of the Newton polygon of $f(z)$ are integers. Hence, the line segment joining $(2, 0)$ and $(8, 6)$ must be on the Newton polygon of $f(z)$. By Lemma 8, we see that $k_2 \geq 6$. We again consider when $z = 2$ in (2.1). Notice, there are at least six factors $2 - x_j$ in $f(2)$ and at least six factors of $2 - y_j$ in $g(2)$ each divisible by 2^2. Hence $2^{12} \mid C$ in this case. However, we are given $2^{10} \nmid C$, giving us a contradiction.

Case 1.2.2. $k_1' = 1$

In this subcase, we consider the following polynomial

$$w(z) = (z - y_2)(z - y_3) \cdots (z - y_9) = \sum_{j=0}^{8} u_j z^j. \tag{3.3}$$

We study the 2-adic valuations in the coefficients of $w(z)$ to gain insight into $g(z)$. Note, $(z - y_1)w(z) = g(z)$, with $g(z)$ monic. Thus, $u_8 = 1$. Further, u_0 is exactly divisible by 2^8, since $y_j \equiv 2 \pmod 4$ for $2 \leq j \leq 9$.

We claim that $2^8 \| u_1$. Otherwise, considering the coefficient of z in $g(z)$, we deduce

$$\nu_2(a_1) = \nu_2(b_1) = \nu_2(u_0 - y_1 u_1) = \min\{\nu_2(u_0), \nu_2(u_1)\} \leq 8.$$

The first equality holds since $a_1 = b_1$. The second equality holds by expanding $(z - y_1)w(z)$ and comparing the coefficient of z with that of $g(z)$. The third equality follows from the rules of valuations and the fact that y_1 is odd and thus does not contribute a factor of 2. The last inequality holds since $\nu_2(u_0) = 8$. Since $(8, \nu_2(a_1)) \in S_1$, there is an edge of the Newton polygon of $f(z)$ that lies on or below the segment joining $(1, 0)$ and $(8, 8)$. Since the slopes of the edges of the Newton polygon must be integers, we deduce that the segment joining $(1, 0)$ and $(8, 7)$ is on

the Newton polygon of $f(z)$. Setting $z = 2$ in (2.1) as before gives $2^{15} \mid C$, implying a contradiction. Thus, $2^8 \| u_1$.

Similarly, we argue $2^8 \| u_2$. Otherwise, we have

$$\nu_2(a_2) = \nu_2(b_2) = \nu_2(u_1 - y_1 u_2) = \min\{\nu_2(u_1), \nu_2(u_2)\} \leq 8.$$

This would imply that there is a point on or below $(7, 8)$ in S_1. We again recall that the edges of the Newton polygon of $f(z)$ have integer slopes, and therefore the segment joining $(1, 0)$ and $(7, 6)$ is on the Newton polygon of $f(z)$. Setting $z = 2$ in (2.1) would imply $2^{14} | C$, a contradiction. Thus, $2^8 \| u_2$.

Next, we show $2^2 \| u_7$. In this subcase, recall that there are eight elements of Y that are congruent to $2 \pmod 4$. Writing $y_j = 4y'_j + 2$ for $j \in \{2, 3, \ldots, 9\}$ in (3.3), we see that

$$u_1 = -2^7 \left(\prod_{j=2}^{9} (2y'_j + 1) \right) \left(\frac{1}{2y'_2 + 1} + \frac{1}{2y'_3 + 1} + \cdots + \frac{1}{2y'_9 + 1} \right).$$

We note that every odd square is $1 \pmod 8$. In particular, $(2y'_k + 1)^2 \equiv 1 \pmod 8$. Therefore, for each $k \in \{2, 3, \ldots, 9\}$, we have

$$\begin{aligned} \left(\prod_{j=2}^{9} (2y'_j + 1) \right) \frac{1}{2y'_k + 1} &\equiv \left(\prod_{j=2}^{9} (2y'_j + 1) \right) \frac{1}{2y'_k + 1} \cdot (2y'_k + 1)^2 \\ &\equiv \left(\prod_{j=2}^{9} (2y'_j + 1) \right) (2y'_k + 1) \pmod 8. \end{aligned}$$

Thus,

$$-\frac{u_1}{2^7} \equiv \prod_{j=2}^{9} (2y'_j + 1) \cdot \sum_{k=2}^{9} \frac{1}{2y'_k + 1} \equiv \prod_{j=2}^{9} (2y'_j + 1) \cdot \sum_{k=2}^{9} (2y'_k + 1) \pmod 8.$$

Recall, we proved $2^8 \| u_1$. Thus $\nu_2(\frac{u_1}{2^7}) = 1$. We deduce that $\sum_{k=2}^{9} (2y'_k + 1)$ is exactly divisible by 2 (since a product of odd numbers does not contribute any factors of 2). Multiplying $\sum_{k=2}^{9} (2y'_k + 1)$ by 2, we deduce that

$$\nu_2(y_2 + y_3 + \cdots + y_9) = 2.$$

In other words, $2^2 \| u_7$.

The last bit of information we need for this case is that $2^4 \| u_6$. We continue along the same lines as the argument given for $2^2 \| u_7$. Here, we let k and l be in $\{2, 3, \cdots, 9\}$ with $k \neq l$. We have,

$$\begin{aligned}\left(\prod_{j=2}^{9}(2y_j'+1)\right)\frac{1}{(2y_k'+1)(2y_l'+1)} &\equiv \left(\prod_{j=2}^{9}(2y_j'+1)\right)\frac{(2y_k'+1)^2(2y_l'+1)^2}{(2y_k'+1)(2y_l'+1)} \\ &\equiv \left(\prod_{j=2}^{9}(2y_j'+1)\right)(2y_k'+1)(2y_l'+1) \pmod 8.\end{aligned}$$

Note that u_2 is the sum of the product of six roots of $w(z)$ at a time. Thus, u_2 is 2^6 times the sum of all expressions of the form above. That is,

$$u_2 = 2^6\left(\prod_{j=2}^{9}(2y_j'+1)\right)\left(\sum_{2\leq k<l\leq 9}\frac{1}{(2y_k'+1)(2y_l'+1)}\right).$$

Therefore,

$$\begin{aligned}\frac{u_2}{2^6} &\equiv \left(\prod_{j=2}^{9}(2y_j'+1)\right)\sum_{2\leq k<l\leq 9}\frac{1}{(2y_k'+1)(2y_l'+1)} \\ &\equiv \left(\prod_{j=2}^{9}(2y_j'+1)\right)\sum_{2\leq k<l\leq 9}(2y_k'+1)(2y_l'+1) \pmod 8.\end{aligned}$$

Since $2^8 \| u_2$, we deduce that 2^2 exactly divides $\sum_{2\leq k<l\leq 9}(2y_k'+1)(2y_l'+1)$. Multiplying by 2^2, we deduce that

$$\nu_2\left(\sum_{2\leq k<l\leq 9} y_k y_l\right) = 4.$$

In other words, $2^4 \| u_6$.

Recall $y_j = 4y_j' + 2$. Thus, for each $j \in \{2, 3, \cdots, 9\}$, we have that

$$y_j^2 = (4y_j'+2)^2 = 4 \cdot (2y_j'+1)^2$$

is 4 times an odd square. We consider

$$y_2^2 + y_3^2 + \cdots + y_9^2 = 4 \cdot \sum_{j=2}^{9}(2y_j'+1)^2.$$

Since $(2y_j'+1)^2 \equiv 1 \pmod 8$, we deduce

$$\sum_{j=2}^{9}(2y_j'+1)^2 \equiv 0 \pmod 8.$$

Therefore, $y_2^2+y_3^2+\cdots+y_9^2$ is 4 times a number that is divisible by 8. Thus, $y_2^2+y_3^2+\cdots+y_9^2$ is divisible by 2^5. We make use of the identity

$$(y_2+y_3+\cdots+y_9)^2 = y_2^2+y_3^2+\cdots+y_9^2+2\sum_{2\le k<l\le 9} y_k y_l.$$

The last sum in the identity above is u_6. We established before that u_6 is exactly divisible by 2^4. Thus, the right-hand side of the identity is divisible by 2^5. However, on the left-hand side we have u_7^2. We have shown that $2^2 \| u_7$; thus $2^4 \| u_7^2$. Hence, we have a contradiction since the 2-adic valuations do not agree on the left and right sides of the equation above. This completes the case for $k_1'=1$.

Case 1.2.3. $k_1'=0$

From (2.1),

$$C_9 = f(0)-g(0) = -\prod_{j=1}^{9} x_j + \prod_{j=1}^{9} y_j$$

is divisible by 2^9. This is what we set out to show, so we are done in this case. (Alternatively, one can use that the 18 x_j's and y_j's cannot all have a common prime divisor p in (2.1) if $\nu_p(C_9)$ is minimal. From this point of view, this subcase cannot occur.)

Case 2. $k_1'+k_2'<9$

Recall that we chose $k_1' \le 4$ and

$$k_2' \ge \left\lceil \frac{9-k_1'}{2} \right\rceil \ge 3.$$

We also have $k_2' \geq k_2$. We note the importance of the condition $k_1' + k_2' < 9$. This implies $k_2' < 9 - k_1'$. We consider the coefficient $b_{9-k_1'}$. This coefficient is equal to plus or minus the sum of the product of y_j's taken k_1' at a time. Since there are k_1' odd elements of Y, exactly one of the summands mentioned in the previous sentence is a product of odd numbers. Thus, $\nu_2(b_{9-k_1'}) = 0$. Hence, $(k_1', 0)$ and $(k_1' + k_2', k_2')$ are points in S_2 and, hence, points in S_1. Since there are exactly $k_1 = k_1'$ odd x_j and the Newton polygon of $f(z)$ has integer slopes, we deduce that the segment joining $(k_1', 0)$ and $(k_1' + k_2', k_2')$ is part of the Newton polygon of $f(z)$. In particular, $k_2 \geq k_2' \geq 3$. Since $k_2' \geq k_2$, we deduce $k_2 = k_2' \geq 3$.

Case 2.1. $k_1' \leq 3$

If $k_1' \leq 3$, then there are at least six even x_j and six even y_j. Out of the six even x_j's and the six even y_j's, at least three x_j's and three y_j's are $2 \pmod 4$. Thus, setting $z = 2$ in (2.1), we obtain $2^9 | C$, as desired.

Case 2.2. $k_1' = 4$

We lastly consider $k_1' = k_1 = 4$ and $k_2 = k_2' \geq 3$. Since we are in the case where $k_1' + k_2' < 9$ and $k_1' = 4$, we have $k_2' < 5$. Thus, either $k_2' = 4$ or $k_2' = 3$.

Case 2.2.1. $k_2' = 4$

If $k_2' = 4$, then $k_2 = k_2' = 4$ implies that there are five even x_j's and five even y_j's. Out of the five even x_j's and the five even y_j's, there are four x_j's and four y_j's that are $2 \pmod 4$. Setting $z = 2$ in (2.1), we obtain $2^9 | C$ and are done as before.

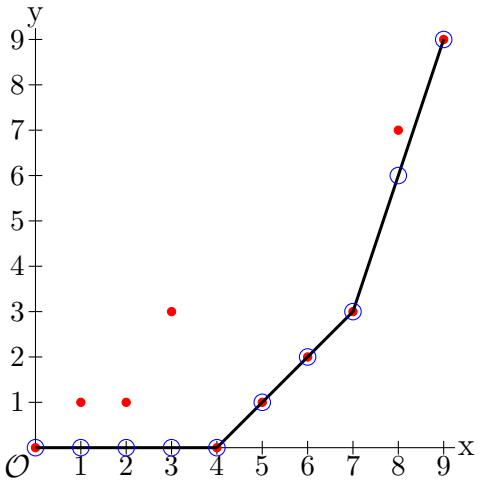

Figure 3.3: NP 5

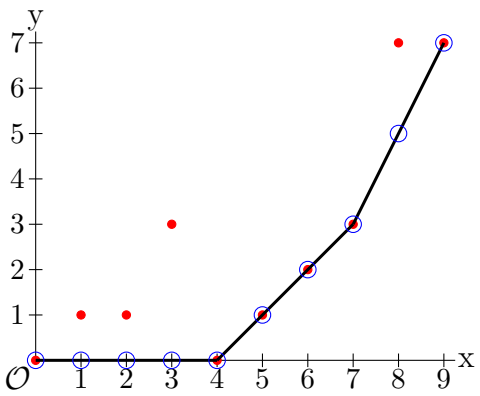

Figure 3.4: NP 6

Case 2.2.2. $k_2' = 3$

One possibility for the Newton polygons for $f(z)$ and $g(z)$ is given by Figure 3.3 and Figure 3.4. We quickly rule out the possibility that these could be the Newton polygons for $f(z)$ and $g(z)$. By Lemma 9, assuming Figure 3.3 and 3.4 are the Newton polygons of $f(z)$ and $g(z)$, we have $2^7 \| C$. However, setting $z = 2$ in (2.1), we obtain $2^8 | C$, a contradiction.

If the right-most points on the Newton polygons, $(9, \nu_2(a_0))$ and $(9, \nu_2(b_0))$, are on or above $(9, 9)$, then we take $z = 0$ in (2.1) to see that $2^9 | C$. This finishes the argument in this case.

Further, we recall the slopes of the Newton polygons of $f(z)$ and $g(z)$ are integers, where the slopes increase from left to right. For each of these Newton polygons, the edge with slope 1 ends at the point $(k_1 + k_2, k_2) = (7, 3)$. Thus, the remaining edge(s) have slope at least 2, and therefore, the right most point must be on or above $(9, 7)$.

If exactly one of the Newton polygons has the right-most point $(9, 7)$, then we proceed as above, setting $z = 2$ in (2.1) to get $2^8 | C$. However, Lemma 9 implies that

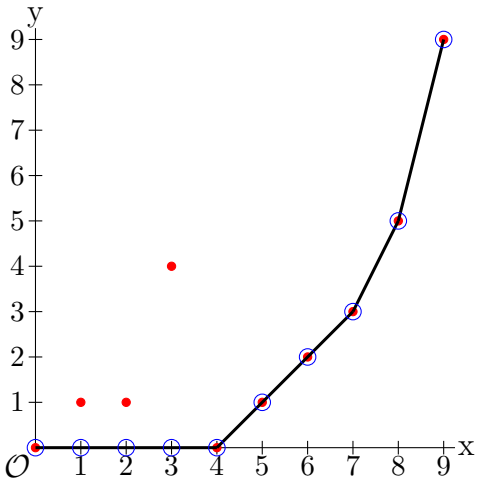

Figure 3.5: NP 7

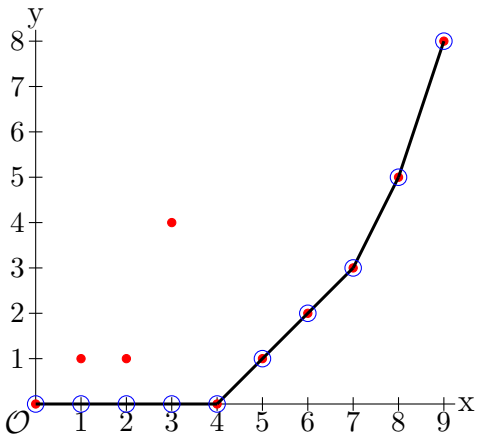

Figure 3.6: NP 8

$2^7 \| C$, a contradiction. If both of the Newton polygons have right-most endpoint $(9, 7)$, as in Figure 3.4, then by setting $z = 4$ in (2.1), we see that $2^9 | C$, giving us the conclusion we want.

We now have that both of the Newton polygons have right-most point on or above $(9, 8)$. We have already handled the case where both of the right-most points are on or above $(9, 9)$. Thus, we consider the case that at least one of the Newton polygons has right-most point $(9, 8)$. We consider if the Newton polygons for $f(z)$ and $g(z)$ both look like Figure 3.6. If this is the case, we take $z = 8$ in (2.1). Doing so yields that $2^9 | C$, as desired.

Now, we assume one of the Newton polygons looks like Figure 3.6 and the other has right-most point above $(9, 8)$ as in Figure 3.5. We observe that $(8, 5)$ is a point in either S_1 or S_2, and thus both, since they agree for all $j \leq 8$. Since there are four odd x_j's and y_j's and three x_j's and y_j's congruent to 2 (mod 4) we have $(7, 3)$ as a point in both S_1 and S_2. Hence the edge joining $(7, 3)$ and $(8, 5)$ is common to both Newton polygons. Thus, the Newton polygons look like those of Figure 3.5 and Figure 3.6 with the exception that the right-most point of Figure 3.5 may be

above $(9, 9)$ and the associated edge modified accordingly. Observe that each of x_5, x_6, x_7, y_5, y_6, and y_7 is 2 modulo 4. Thus, they are either 2 or 6 modulo 8. If one of these x_j is congruent to one of the y_j modulo 8, then by setting $z = 2$ or $z = 6$ in (2.1), we see that $2^9|C$, and we are done. Hence, we only need to consider the case that each of x_5, x_6, and x_7 is congruent modulo 8, each of y_5, y_6, and y_7 is congruent modulo 8, and $x_5 \not\equiv y_5 \pmod 8$. As a consequence, one of the sums $x_5 + x_6 + x_7$ or $y_5 + y_6 + y_7$ is equivalent to $2 + 2 + 2 \equiv 6 \pmod 8$ and the other is $6 + 6 + 6 \equiv 2 \pmod 8$. Further, since $(7, 3)$ and $(8, 5)$ are points on the Newton polygon of $f(z)$ and on the Newton polygon of $g(z)$, we obtain from Lemma 8 that

$$x_8 \equiv y_8 \equiv 4 \pmod 8.$$

Further, since the right-most points of the Newton polygons are on or above $(9, 8)$, by Lemma 8 we have

$$x_9 \equiv y_9 \equiv 0 \pmod 8.$$

Since $x_5 + x_6 + x_7 \not\equiv y_5 + y_6 + y_7 \pmod 8$, $x_8 \equiv y_8 \pmod 8$, and $x_9 \equiv y_9 \pmod 8$, we obtain that

$$x_5 + x_6 + x_7 + x_8 + x_9 \not\equiv y_5 + y_6 + y_7 + y_8 + y_9 \pmod 8.$$

This contradicts (2.2) in Lemma 11 with $t = 4$, $n = 9$ and $k = 1$. Thus, we are done in this case.

Chapter 4

Lower bound for $\nu_2\left(\overline{C}_8\right)$

In this chapter, we investigate $\overline{C}_8$. It is known (see [2]) that $2^4|\overline{C}_8$ and $2^9 \nmid \overline{C}_8$. In this chapter, we increase the lower bound on the 2-adic valuation of $\overline{C}_8$. We show that $2^6|\overline{C}_8$. For possible future analysis, we show in all but one case of conditions on $X = \{x_1, \ldots, x_8\}$ and $Y = \{y_1, \ldots, y_8\}$ that we consider, one has $2^8|\overline{C}_8$.

Our set-up in this chapter is that

$$f(z) = \prod_{j=1}^{8}(z - x_j) = \sum_{j=0}^{8} a_j z^j \quad \text{and} \quad g(z) = \prod_{j=1}^{8}(z - y_j) = \sum_{j=0}^{8} b_j z^j$$

where $x_j, y_j \in \mathbb{Z}$ are chosen so that

$$f(z) - g(z) = C_8, \tag{4.1}$$

with the largest power of 2 dividing C_8 equal to the largest power of 2 dividing $\overline{C}_8$. Thus, by Corollary 3, we have that $X = \{x_1, \ldots, x_8\}$ and $Y = \{y_1, \ldots, y_8\}$ give an ideal solution or $X =_7 Y$. For the remainder of this chapter, we have $C = C_8$.

Recall $f(z)$ and $g(z)$ have been translated, if necessary, so that $a_0 \neq 0$, $b_0 \neq 0$ and k_1, k_1', k_2, and k_2' are as before. Thus, $k_1' = k_1 \leq 4$, $k_2' \geq \lceil (8 - k_1')/2 \rceil \geq 2$ and $k_2' \geq k_2$. Since here the multisets X and Y have eight elements, $k_1 + k_2 \leq 8$ and $k_1' + k_2' \leq 8$.

CASE 1. $k_1' = 4$ AND $k_2' = 4$

From Lemma 11, we have

$$x_5^2 + x_6^2 + x_7^2 + x_8^2 \equiv y_5^2 + y_6^2 + y_7^2 + y_8^2 \pmod{16}.$$

As an even integer m squared is 4 modulo 16 if $m \equiv 2 \pmod 4$ and otherwise is 0 modulo 16, the above congruence can be rewritten as

$$4k_2 \equiv 4k_2' \pmod{16} \iff k_2 \equiv k_2' \pmod 4.$$

Thus, either $k_2 = 0$ or $k_2 = 4$. In the second case, letting $z = 2$ in (4.1) shows $2^8 | C$, as we want. So suppose $k_2 = 0$. In this case, the edges of the Newton polygon of $f(z)$ with positive slope have slope ≥ 2. In particular, this implies

$$\nu_2(a_{8-j}) \geq 2(j-4) \quad \text{for } 5 \leq j \leq 8.$$

As the points $\big(j, \nu_2(a_{8-j})\big)$ on S_1 and $\big(j, \nu_2(b_{8-j})\big)$ on S_2 agree for $0 \leq j \leq 7$, we deduce

$$\nu_2(b_{8-j}) \geq 2(j-4) \quad \text{for } 5 \leq j \leq 7. \tag{4.2}$$

Define $u_j \in \mathbb{Z}$ by the equation

$$(z-y_5)(z-y_6)(z-y_7)(z-y_8) = \sum_{j=0}^{4} u_j z^j.$$

Next, we obtain information on the 2-adic values of the u_j. As $y_j \equiv 2 \pmod 4$ for $5 \leq j \leq 8$, we have

$$u_0 = y_5 y_6 y_7 y_8 \implies \nu_2(u_0) = 4.$$

Also, u_1 is the sum of 4 terms that are exactly divisible by 8, so $\nu_2(u_1) \geq 4$. Assume $\nu_2(u_1) = 4$. We make use of the congruence

$$(z-y_1)(z-y_2)(z-y_3)(z-y_4) \equiv (z+1)^4 \equiv z^4 + 1 \pmod 2. \tag{4.3}$$

Thus, the product on the left when expanded is a quartic with odd constant term and an odd coefficient for z^4 but otherwise has even coefficients. Thus, there are integers r and s satisfying

$$b_1 = u_1(2r+1) + u_0(2s).$$

Since $\nu_2(u_0) = \nu_2(u_1) = 4$, we deduce $\nu_2(b_1) = 4$. This contradicts (4.2) with $j = 7$. Thus,

$$\nu_2(u_1) \geq 5.$$

Writing $y_j = 2(2y'_j + 1)$ for $5 \leq j \leq 8$, we see that

$$u_1 = -2^3(2y'_5+1)(2y'_6+1)(2y'_7+1)(2y'_8+1)\left(\frac{1}{2y'_5+1}+\frac{1}{2y'_6+1}+\frac{1}{2y'_7+1}+\frac{1}{2y'_8+1}\right).$$

We deduce that

$$-\frac{u_1}{2^3} \equiv (2y'_5+1)(2y'_6+1)(2y'_7+1)(2y'_8+1)\sum_{j=5}^{8}(2y'_j+1) \pmod 8.$$

Since $\nu_2(u_1) \geq 5$, we deduce that the last sum above must be divisible by 4. Hence,

$$u_3 = -y_5 - y_6 - y_7 - y_8 = -2\sum_{j=5}^{8}(2y'_j+1) \implies \nu_2(u_3) \geq 3.$$

Observe that

$$u_3^2 = 2^2\sum_{j=5}^{8}(2y'_j+1)^2 - 2u_2. \tag{4.4}$$

Since

$$\sum_{j=5}^{8}(2y'_j+1)^2 \equiv 4 \pmod 8,$$

we see that $2^2\sum_{j=5}^{8}(2y'_j+1)^2$ is exactly divisible by 2^4. On the other hand, $\nu_2(u_3) \geq 3$ implies u_3^2 is divisible by 2^6. Hence, (4.4) implies

$$\nu_2(u_2) = 3.$$

From (4.3), there exist integers r, s and t such that

$$b_2 = u_2(2r+1) + u_1(2s) + u_0(2t).$$

The values and estimates obtained above on $\nu_2(u_j)$, with $j \in \{0,1,2\}$, imply now that $\nu_2(b_2) = 3$. This contradicts (4.2) with $j = 6$, completing this case.

Case 2. $k_1' \leq 3$

We can suppose $k_1' \geq 1$ (see Case 1.2.3 of the previous chapter). Since $k_1' \leq 3$, we obtain $k_2' \geq \lceil (8-3)/2 \rceil = 3$. Suppose first that $k_2' < 8 - k_1'$. Since the points $\left(j, \nu_2(a_{8-j})\right)$ on S_1 and $\left(j, \nu_2(b_{8-j})\right)$ on S_2 agree for $0 \leq j \leq 7$, we deduce that $k_2 = k_2'$. In this case, letting $z = 2$ in (4.1), we see that $2^8 | C$, as we want. Now, suppose $k_2' = 8 - k_1'$. As in Case 1, we obtain $k_2 \equiv k_2' \pmod 4$. Hence, $k_2 \geq 1$ and, in particular, $x_{k_1'+1} \equiv 2 \pmod 4$. Let $z = x_{k_1'+1}$ in (4.1). As $f(z) = 0$ and $g(z)$ is divisible by 2^{10}, we get $2^{10} | C$, contradicting that $2^9 \nmid C$.

Case 3. $k_1' = 4$ and $k_2' < 4$

Given that $k_1' + k_2' < 8$ in addition to knowing $k_1 = k_1'$ and $k_2' \geq k_2$, we deduce

$$k_1 + k_2 \leq k_1 + k_2' = k_1' + k_2' < 8.$$

Therefore, $k_1 + k_2 < 8$. Since the points $\left(j, \nu_2(a_{8-j})\right)$ on S_1 and $\left(j, \nu_2(b_{8-j})\right)$ on S_2 agree for $0 \leq j \leq 7$, we conclude that $k_2 = k_2'$ in this case. Note that $k_2' \geq \lceil (8-4)/2 \rceil = 2$ is true. Setting $z = 2$, one checks in this case that $2^{8+k_2'-k_1'}$ divides C. As $8 + k_2' - k_1' \geq 8 + 2 - 4 = 6$, we obtain $2^6 | C$ in this case.

Bibliography

[1] Peter Borwein, Petr Lisoněk, and Colin Percival. Computational investigations of the Prouhet-Tarry-Escott problem. *Mathematics of Computation*, 72(244):2063–2070, 2003.

[2] Timothy Caley. The Prouhet-Tarry-Escott problem for Gaussian integers. *Mathematics of Computation*, 82(282):1121–1137, 2013.

[3] Gustave Dumas. Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels. *Journal de Math. Pure et Appl*, 2:191–258, 1906.