Het Prouhet-Tarry-Escott probleem en ontleedbare polynomen

Kika Dimitrić

Bachelorscriptie Wiskunde

begeleider: prof. dr. G.L.M. Cornelissen

25/01/2023

Universiteit Utrecht

Inhoudsopgave

1 Introductie

Probleemstelling
Deze scriptie is (hoofdzakelijk) gebaseerd het artikel "The Prouhet–Tarry–Escott problem, indecomposability of polynomials and Diophantine equations" van L. Hajdu, Á. Papp en R. Tijdeman [7].

Bekijk de verzamelingen $\{0, 3, 5, 6\}$ en $\{1, 2, 4, 7\}$. De som over alle getallen uit de verzamelingen geeft:

$$0 + 3 + 5 + 6 = 14$$

en

$$1 + 2 + 4 + 7 = 14.$$

Deze zijn gelijk aan elkaar. Dan kwadrateren we elk getal uit de verzameling en nemen we de som:

$$0^2 + 3^2 + 5^2 + 6^2 = 70$$

en

$$1^2 + 2^2 + 4^2 + 7^2 = 70.$$

Deze zijn wederom gelijk aan elkaar. De verzamelingen $\{0, 3, 5, 6\}$ en $\{1, 2, 4, 7\}$ maken samen een oplossing voor het zogeheten Prouhet-Tarry-Escott probleem. Ofwel het PTE probleem.

Het Prouhet-Tarry-Escott (PTE) probleem vraagt, gegeven een natuurlijk getal $r \geq 1$, om het vinden van disjuncte verzamelingen van gehele getallen met dezelfde kardinaliteit zodat hun machtssommen gelijk zijn aan elkaar tot en met macht r. In het geval van twee verzamelingen $\{a_1, a_2, ..., a_n\}$ en $\{b_1, b_2, ..., b_n\}$, geldt dat

$$\begin{aligned}
&a_1 + a_2 + ... + a_n = b_1 + b_2 + ... + b_n \\
&a_1^2 + a_2^2 + ... + a_n^2 = b_1^2 + b_2^2 + ... + b_n^2 \\
&\vdots \\
&a_1^r + a_2^r + ... + a_n^r = b_1^r + b_2^r + ... + b_n^r.
\end{aligned}$$

Het bovenstaande wordt ook wel genoteerd als

$$\{a_1, a_2, ..., a_n\} =_r \{b_1, b_2, ..., b_n\}.$$

We noemen n de maat van de oplossing en r de graad.

Historie
Prouhet, Tarry en Escott waren wiskundigen in de 19e en 20e eeuw. Eugène Prouhet (1817 - 1867) was een Franse docent wiskunde aan de École Polytechnique in Parijs en redacteur van *Nouvelles Annales de Mathématiques*, een wiskundig tijdschrift [1]. Gaston Tarry (1843 - 1913) was een Franse amateur-wiskundige die vooral bekend staat om het bewijzen van het vermoeden van Euler van het zogenoemde "36 officieren probleem" [11]. Hij vond in het bijzonder een oplossing voor het PTE probleem van maat 14 en graad 10. Edward Brind Escott (1868 - 1946) was een Amerikaanse actuaris die gespecialiseerd was in getaltheorie [6]. Ook was hij docent wiskunde aan de universiteit van Michigan [8].

Voordat Prouhet, Tarry óf Escott zich bezig hielden met het probleem waren er al een aantal wiskundigen die oplossingen hadden gevonden [9]. Als eerst kwam Leonhard Euler met de oplossing

$$\{a, b, c, a+b+c\} =_2 \{a+b, b+c, a+c\}$$

met $a, b, c \in \mathbb{N}$. Dit kwam naar voren in briefverkeer dat Euler had met wiskundige Christian Goldbach in 1751. Merk op dat deze verzamelingen niet dezelfde maat hebben. Later schreef Goldbach terug met de oplossing

$$\{a+b+d, a+c+d, b+c+d, d\} =_2 \{a+d, b+d, c+d, a+b+c+d\}$$

met $a, b, c, d \in \mathbb{N}$, en wel beide dezelfde maat. In het bijzonder was Euler's oplossing een speciaal geval van deze, namelijk met $d = 0$.

Prouhet kwam in 1851 als eerste met een algemene oplossing met een grotere maat die een verhouding gaf tussen de maat en de graad. Hij stelde dat er een verzameling van n^{r+1} getallen bestaat die opgedeeld kan worden in n verzamelingen, elk van maat n^r, die een oplossing geeft voor wat we nu het PTE probleem noemen, van graad r.

Opmerkelijk is dat het PTE probleem voor een lange tijd het "Tarry-Escott probleem" heeft geheten, totdat Prouhet's bevindingen zijn herontdekt een eeuw later.

Overzicht
In deze scriptie wordt eerst gekeken naar voorbeelden en eigenschappen van het PTE probleem. Dan gaan we kijken naar hoe we oplossingen kunnen vinden met behulp van de Thue-Morse rij. Als laatste verdiepen we ons in ontleedbare polynomen en komen we bij de stelling die een verband geeft tussen een oplossing voor het PTE probleem en ontleedbaarheid van polynomen.

Conventies
Het getal 0 is in de natuurlijke getallen inbegrepen: $\mathbb{N} = \{0, 1, 2, 3, ...\}$.

We zullen het hebben over de maat van een verzameling. In dit geval gaat het om de telmaat. De verzamelingen waar we mee te maken zullen krijgen zijn eindige verzamelingen van natuurlijke getallen, dus de maat van een verzameling zal gelijk zijn aan de kardinaliteit ervan.

De polynomen die in deze scriptie voorkomen zijn polynomen in x over $\mathbb{Z}$ tenzij anders gespecificeerd, zoals de symmetrische polynomen over $a_1, ..., a_n$. Sommige stellingen gelden ook voor polynomen over een grotere verzameling dan $\mathbb{Z}$, zeg $\mathbb{R}$ of $\mathbb{C}$, maar ze worden allen op een manier toegepast op oplossingen van het PTE probleem, wat alleen getallen neemt uit $\mathbb{Z}$. Dus verzamelingen groter dan $\mathbb{Z}$ is voor ons niet relevant.

2 Het Prouhet-Tarry-Escott probleem

Het Prouhet-Tarry-Escott (PTE) probleem vraagt, gegeven een natuurlijk getal $r \geq 1$, om het vinden van disjuncte verzamelingen van gehele getallen met dezelfde kardinaliteit zodat hun machtssommen gelijk zijn aan elkaar tot en met macht r. Het kunnen meerdere verzamelingen zijn, maar wij kijken de komende hoofdstukken naar exact twee verzamelingen die voldoen aan het probleem. In het geval van twee verzamelingen $\{a_1, a_2, ..., a_n\}$ en $\{b_1, b_2, ..., b_n\}$, geldt dat

$$\begin{aligned}
&a_1 + a_2 + ... + a_n = b_1 + b_2 + ... + b_n \\
&a_1^2 + a_2^2 + ... + a_n^2 = b_1^2 + b_2^2 + ... + b_n^2 \\
&\vdots \\
&a_1^r + a_2^r + ... + a_n^r = b_1^r + b_2^r + ... + b_n^r.
\end{aligned}$$

Met $a_i, b_i \in \mathbb{Z}$ en $r, n \in \mathbb{N}$. Het bovenstaande wordt ook wel genoteerd als

$$\{a_1, a_2, ..., a_n\} =_r \{b_1, b_2, ..., b_n\}.$$

We noemen n de maat van de oplossing en r de graad.

De *machtssom* is gedefinieerd als

$$s_k(a_1, ..., a_n) = \sum_{i=1}^{n} a_i^k.$$

Als $\{a_1, a_2, ..., a_n\} =_r \{b_1, b_2, ..., b_n\}$, dan geldt dus dat

$$s_k(a_1, ..., a_n) = \sum_{i=1}^{n} a_i^k = \sum_{i=1}^{n} b_i^k = s_k(b_1, ..., b_n),$$

voor $0 \leq k \leq r$. Meer over machtssommmen volgt in hoofdstuk 5.

Voorbeelden van oplossingen van het PTE probleem zijn

Voorbeeld 2.1. 1. $\{2, 3, 7\} =_2 \{1, 5, 6\}$

2. $\{0, 3, 5, 6\} =_2 \{1, 2, 4, 7\}$

3. $\{0, 5, 6, 16, 17, 22\} =_5 \{1, 2, 10, 12, 20, 21\}$

4. $\{20, 26, 30, 32, 38, 40, 44, 50\} =_3 \{22, 24, 28, 3436, 42, 46, 48\}$

$\oslash$

2.1 Eigenschappen van oplossingen van het PTE probleem

Uit oplossingen van het PTE volgen onder andere twee eigenschappen die uitgedrukt zijn in onderstaande stellingen.

Stelling 2.2. *Als* $\{a_1, a_2, ..., a_n\} =_r \{b_1, b_2, ..., b_n\}$, *dan geldt ook*

$$\{a_1 + l, a_2 + l, ..., a_n + l\} =_r \{b_1 + l, b_2 + l, ..., b_n + l\}$$

voor een willekeurige $l \in \mathbb{Z}$.

Bewijs. Als $\{a_1, a_2, ..., a_n\} =_r \{b_1, b_2, ..., b_n\}$, dan geldt dus dat

$$\sum_{i=1}^{n} a_i^k = \sum_{i=1}^{n} b_i^k \tag{1}$$

voor $0 \leq k \leq r$. Volgens het *binomium van Newton* geldt

$$(a_i + l)^k = \sum_{j=0}^{k} \binom{k}{j} a_i^j l^{k-j}.$$

Dan krijgen we voor de som over $(a_i + l)^k$,

$$\begin{aligned}
\sum_{i=1}^{n} (a_i + l)^k &= \sum_{i=1}^{n} \left(\sum_{j=0}^{k} \binom{k}{j} a_i^j l^{k-j} \right) \\
&= \sum_{j=0}^{k} \binom{k}{j} \left(\sum_{i=1}^{n} a_i^j \right) l^{k-j} \\
&= \sum_{j=0}^{k} \binom{k}{j} \left(\sum_{i=1}^{n} b_i^j \right) l^{k-j} \\
&= \sum_{i=1}^{n} \sum_{j=0}^{k} \binom{k}{j} b_i^j l^{k-j} \\
&= \sum_{i=1}^{n} (b_i + l)^k.
\end{aligned}$$

□

Stelling 2.3. *Veronderstel dat* $\{a_1, a_2, ..., a_n\} =_r \{b_1, b_2, ..., b_n\}$. *Zij* f *een willekeurig polynoom van graad* $s \leq r$ *over* $\mathbb{Z}$. *Dan geldt dat*

$$\sum_{i=0}^{n} f(a_i) = \sum_{i=0}^{n} f(b_i). \tag{2}$$

Bewijs. We gaan dit bewijzen aan de hand van inductie. Voor $s = 0$ is f een constante. Het is duidelijk dat de gelijkheid hiervoor geldt. Dan nemen we aan dat de gelijkheid geldt voor $s = l$ voor een $l \in \mathbb{N}$ met $0 \leq l \leq r - 1$. Het polynoom f heeft graad $l + 1$ en is te schrijven als $f(x) = \sum_{j=0}^{l+1} c_j x^j$. Dan volgt de gelijkheid:

$$\begin{aligned}
\sum_{i=0}^{n} f(a_i) &= \sum_{i=0}^{n} \sum_{j=0}^{l+1} c_j a_i^j \\
&= \sum_{i=0}^{n} \left(c_{l+1} a_i^{l+1} + \sum_{j=0}^{l} c_j a_i^j \right) \\
&= \sum_{i=0}^{n} c_{l+1} a_i^{l+1} + \sum_{i=0}^{n} \sum_{j=0}^{l} c_j a_i^j \\
&= c_{l+1} \sum_{i=0}^{n} a_i^{l+1} + \sum_{i=0}^{n} \sum_{j=0}^{l} c_j a_i^j .
\end{aligned}$$

Gezien $l + 1 \leq r$ geldt dat $s_{l+1}(a_i) = s_{l+1}(b_i)$. Verder is $\sum_{j=0}^{l} c_j a_i^j$ een polynoom van graad l dus voldoet het aan de inductiehypothese. Dan krijgen we:

$$\begin{aligned}
\sum_{i=0}^{n} f(a_i) &= c_{l+1} \sum_{i=0}^{n} b_i^{l+1} + \sum_{i=0}^{n} \sum_{j=0}^{l} c_j b_i^j \\
&= \sum_{i=0}^{n} c_{l+1} b_i^{l+1} + \sum_{i=0}^{n} \sum_{j=0}^{l} c_j b_i^j \\
&= \sum_{i=0}^{n} \left(c_{l+1} b_i^{l+1} + \sum_{j=0}^{l} c_j b_i^j \right) \\
&= \sum_{i=0}^{n} \left(\sum_{j=0}^{l+1} c_j b_i^j \right) \\
&= \sum_{i=0}^{n} f(b_i).
\end{aligned}$$

We concluderen a.d.h.v. inductie dat $\sum_{i=0}^{n} f(a_i) = \sum_{i=0}^{n} f(b_i)$. $\square$

Opmerking. Er hoeft dus niet te gelden dat

$$\sum_{i=0}^{n} (f(a_i))^k = \sum_{i=0}^{n} (f(b_i))^k.$$

voor $1 < k \leq r$. Als f bijvoorbeeld graad r heeft, dan heeft f^2 graad $2r$ en gaat dit bewijs niet op. $\oslash$

3 Thue-Morse rij

De Thue-Morse rij bestaat uit de binaire getallen 0 en 1. In dit hoofdstuk gaan we deze rij definiëren en zien we hoe die gebruikt kan worden om oplossingen te vinden voor het PTE probleem. Daarna volgt het bewijs van de stelling hierover.

3.1 Binaire ontwikkeling van gehele getallen

Elk geheel getal is te ontwikkelen in een sommatie van machten van twee. Dit gaan wij gebruiken om de natuurlijke getallen op te delen.

Bekijk onderstaande voorbeelden

$$\begin{aligned}
0 &= 0 \cdot 2^0 \\
1 &= 1 \cdot 2^0 \\
2 &= 0 \cdot 2^0 + 1 \cdot 2^1 \\
3 &= 1 \cdot 2^0 + 1 \cdot 2^1 \\
4 &= 0 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 \\
5 &= 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 \\
&\vdots
\end{aligned}$$

De algemene formule voor deze ontwikkeling luidt

$$n = \sum_{i \geq 0} n_i 2^i \text{ met } \; n_i \in \{0, 1\}. \tag{3}$$

We beschouwen nu echter alleen het aantal machten van twee dat voorkomt per getal. Hiervoor definiëren we

$$S_2(n) = \sum_i n_i, \tag{4}$$

met n_i uit formule (3).

We bekijken $S_2(n)$ van de eerste acht natuurlijke getallen:

$$\begin{aligned}
S_2(0) &= 0 \\
S_2(1) &= 0 + 1 = 1 \\
S_2(2) &= 1 + 0 = 1 \\
S_2(3) &= 1 + 1 = 2 \\
S_2(4) &= 0 + 0 + 1 = 1 \\
S_2(5) &= 1 + 0 + 1 = 2 \\
S_2(6) &= 0 + 1 + 1 = 2 \\
S_2(7) &= 1 + 1 + 1 = 3.
\end{aligned}$$

Nemen we nu deze getallen modulo 2 dan krijgen we de rij

$$\{0, 1, 1, 0, 1, 0, 0, 1\}.$$

Dit is in feite de directe definitie van de Thue-Morse rij.

Definitie 3.1 (De Thue-Morse rij)**.** De *Thue-Morse rij* is gedefinieerd als

$$(S_2(n) \bmod 2)_{n \in \mathbf{N}},$$

met $S_2(n)$ uit (4). $\oslash$

Opmerking. Definieer het complement van een binaire expansie als de binaire expansie waar 0 en 1 verwisseld zijn. Dan is de Thue-Morse rij ook te construeren op de volgende manier: begin met 0 en voeg hier recursief het complement aan toe, dus

0	
01	(het complement van 0 is 1)
01 10	(het complement van 01 is 10)
0110 1001	(het complement van 0110 is 1001)
01101001 10010110	(het complement van 01101001 is 10010110)
etc.	

$\oslash$

3.2 Thue-Morse rij bij het PTE probleem

De Thue-Morse rij kan worden gebruikt om uit een rekenkundige rij een oplossing voor het PTE probleem te construeren. Neem $n = 2^r$ opeenvolgende elementen van een rekenkundige rij met $r \in \mathbb{N}$. Dan kan deze rij gesplitst worden aan de hand van de Thue-Morse reeks, waarbij er in de ene rij de getallen staan waar op de corresponderende plek in de Thue-Morse rij een 0 staat, en in de andere rij de getallen waar op de corresponderende plek in de Thue-Morse rij een 1 staat. Dan zijn deze twee rijen een oplossing voor het PTE-probleem voor de machten $0 \leq k < r$.

Voorbeeld 3.2. Bekijk de rij

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}.$$

Deze rij heeft lengte $n = 2^4$. Als deze gesplitst is zal het een oplossing zijn voor het PTE probleem voor de machten $0 \leq k < 4$. De eerste 2^4 termen van de Thue-Morse rij zijn:

$$\{0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0\}.$$

Dan is rij A de getallen waarbij op de corresponderende plek in de Thue-Morse rij een 0 staat en B de 1:

$$A = \{0, 3, 5, 6, 9, 10, 12, 15\} \qquad \text{en} \qquad B = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

Passen we de machtssommen toe op beide verzamelingen, krijgen we

$$\begin{aligned}
s_0(A) &= 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 \\
&= 8 \\
&= s_0(B) \\
s_1(A) &= 0 + 3 + 5 + 6 + 9 + 10 + 12 + 15 \\
&= 60 \\
&= 1 + 2 + 4 + 7 + 8 + 11 + 13 + 14 \\
&= s_1(B) \\
s_2(A) &= 0^2 + 3^2 + 5^2 + 6^2 + 9^2 + 10^2 + 12^2 + 15^2 \\
&= 620 \\
&= 1^2 + 2^2 + 4^2 + 7^2 + 8^2 + 11^2 + 13^2 + 14^2 \\
&= s_2(B) \\
s_3(A) &= 0^3 + 3^3 + 5^3 + 6^3 + 9^3 + 10^3 + 12^3 + 15^3 \\
&= 7200 \\
&= 1^3 + 2^3 + 4^3 + 7^3 + 8^3 + 11^3 + 13^3 + 14^3 \\
&= s_3(B).
\end{aligned}$$

We zien dat dit voorbeeld inderdaad geeft

$$\{0, 3, 5, 6, 9, 10, 12, 15\} =_3 \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

$\oslash$

Opmerking. Met behulp van de Thue-Morse rij kunnen we oplossingen vinden voor het PTE probleem bestaande uit twee deelverzamelingen van $\mathbb{N}$. Als $\{a_1, a_2, ..., a_n\} =_r \{b_1, b_2, ..., b_n\}$ zo'n oplossing is kunnen we ook alle elementen uit de verzamelingen vermenigvuldigen met -1. Zo krijgen we nog een oplossing voor het PTE probleem bestaande uit deelverzamelingen van $\mathbb{Z}^- \cup \{0\}$. Deze oplossing ziet eruit als

$$\{-a_1, -a_2, ..., -a_n\} =_r \{-b_1, -b_2, ..., -b_n\}.$$

$\oslash$

3.3 Opdeling van de natuurlijke getallen a.d.h.v. de Thue-Morse rij

De natuurlijke getallen zijn op te delen aan de hand van de Thue-Morse rij in twee verzamelingen $\mathbb{N}_0$ en $\mathbb{N}_1$. Deze opdeling hebben we nodig voor het bewijs van het verband tussen de Thue-Morse rij en het PTE probleem. Neem voor $\mathbb{N}_0$ alle getallen $n \in \mathbb{N}$ waarbij het $(n+1)$-de getal in de Thue-Morse rij gelijk is aan 0. Zodoende bestaat $\mathbb{N}_1$ uit alle $n \in \mathbb{N}$ zodanig dat het $(n+1)$-de getal in de Thue-Morse rij gelijk is aan 1.

$$\begin{aligned} \mathbb{N}_0 &= \{0, 3, 5, 6, 9, 10, 12, 15, ...\} \\ \mathbb{N}_1 &= \{1, 2, 4, 7, 8, 11, 13, 14, ...\}. \end{aligned}$$

Deze opdeling kunnen we ook uitdrukken in termen van de directe definitie van de Thue-Morse reeks,

$$\begin{aligned} \mathbb{N}_0 &= \{n \in \mathbb{N}, S_2(n) \equiv 0 \bmod 2\} \\ \mathbb{N}_1 &= \{n \in \mathbb{N}, S_2(n) \equiv 1 \bmod 2\}. \end{aligned}$$

En zodoende bestaat het complement $\mathbb{N}_0 = \mathbb{N} \setminus \mathbb{N}_1$.

3.4 Bewijs van het verband tussen de Thue-Morse rij en het PTE probleem

Hier volgt het bewijs van dat de Thue-Morse rij gebruikt kan worden om oplossingen te vinden voor het PTE probleem.

Stelling 3.3. *[N. Pytheas Fogg [5]] Voor elke natuurlijke getallen k en r zo dat $k < r$, hebben we*

$$\sum_{\substack{n\in\mathbb{N}_0\\ n<2^r}} n^k = \sum_{\substack{n\in\mathbb{N}_1\\ n<2^r}} n^k. \tag{5}$$

Voor het bewijs van stelling 3.3 introduceren we de polynoom

$$f_r(x) = \sum_{n<2^r} (-1)^{S_2(n)} x^n \tag{6}$$

en gebruiken we onderstaande lemma's.

Lemma 3.4. *Voor de polynoom f_r uit (6) geldt*

$$f_r(x) = \sum_{n<2^r} (-1)^{S_2(n)} x^n = \prod_{k<r} (1 - x^{2^k}).$$

Bewijs lemma 3.4. Allereerst merken we op dat $S_2(n)$ gelijk is aan het aantal machten van 2 dat in de binaire ontwikkeling van n voorkomt. Dan herschrijven we de de som

$$\sum_{n<2^r} (-1)^{S_2(n)} x^n = \sum_{0<k_1<\ldots<k_s<r} (-1)^s x^{2^{k_1}+\ldots+2^{k_s}}.$$

We splitsen de som in alle x die als macht een som heeft waar in ieder geval 2^{r-1} (de grootste 2^{k_i}) in voor komt en alle x die dat niet heeft:

$$\begin{aligned}
f_r(x) &= \sum_{0<k_1<\ldots<k_s<r} (-1)^s x^{2^{k_1}+\ldots+2^{k_s}} \\
&= \sum_{0<k_1<\ldots<k_s=r-1} (-1)^s x^{2^{k_1}+\ldots+2^{k_{s-1}}+2^{r-1}} + \sum_{0<k_1<\ldots<k_s<r-1} (-1)^s x^{2^{k_1}+\ldots+2^{k_s}} \\
&= \sum_{0<k_1<\ldots<k_s=r-1} (-1)^s x^{2^{k_1}+\ldots+2^{k_{s-1}}+2^{r-1}} + f_{r-1}(x) \\
&= -x^{2^{r-1}} \cdot \sum_{0<k_1<\ldots<k_{s-1}<r-1} (-1)^{s-1} x^{2^{k_1}+\ldots+2^{k_{s-1}}} + f_{r-1}(x) \\
&= (1 - x^{2^{r-1}}) f_{r-1}(x).
\end{aligned}$$

Inductief zien wij dan dat

$$f_r(x) = \prod_{k<r} (1 - x^{2^k}).$$

□

Lemma 3.5. *Er bestaat een polynoom $g_r(x)$ zodoende dat voor $f_r(x)$ uit (6) geldt*

$$f_r(x) = (1-x)^r g_r(x)$$

Bewijs lemma 3.5. Beschouw

$$\begin{aligned}(1+y+...+y^{r-1})(1-y) &= 1+y+...+y^{r-1}-(y+...+y^r)\\ &= 1-y^r.\end{aligned}$$

Dan zien we dat

$$1-x^{2^k} = (1-x)(1+x+...+x^{2^k-1}).$$

Daaruit volgt dat

$$\begin{aligned}f_r(x) &= \prod_{k<r}(1-x^{2^k})\\ &= \prod_{k<r}(1-x)(1+x+...+x^{2^k-1})\\ &= (1-x)^r\prod_{k<r}(1+x+...+x^{2^k-1}).\end{aligned}$$

En dus bestaat polynoom $g_r(x)$ zodat $f_r(x) = (1-x)^r g_r(x)$. □

Nu kunnen we de vergelijking van lemma 3.4 en de existentie van polynoom $g_r(x)$ uit lemma 3.5 gebruiken om stelling 3.3 te bewijzen.

Bewijs stelling 3.3. Door de definitie van $\mathbb{N}_0$ en $\mathbb{N}_1$ is vergelijking (5) equivalent met

$$\sum_{n<2^r}(-1)^{S_2(n)}n^k = 0.$$

Dan bekijken we de k-de afgeleide van f_r in $x=1$ voor $k<r$,

$$f_r^{(k)}(1) = ((1-x)^r g_r(x))^{(k)}|_{x=1} = 0.$$

Dit betekent ook dat

$$\begin{aligned}f_r^{(k)}(1) &= (\sum_{n<2^r}(-1)^{S_2(n)}x^n)^{(k)}|_{x=1}\\ &= \sum_{n<2^r}(-1)^{S_2(n)}n(n-1)\cdots(n-k+1) = 0.\end{aligned}$$

Als we naar de eerste afgeleide kijken, ofwel $k = 1$, dan hebben we

$$f^{(1)}(1) = (\sum_{n<2^r} (-1)^{S_2(n)} n x^{n-1})|_{x=1} = \sum_{n<2^r} (-1)^{S_2(n)} n = 0.$$

Vullen we dit in in de tweede afgeleide volgt uit

$$f^{(2)}(1) = \sum_{n<2^r} (-1)^{S_2(n)} n(n-1) = \sum_{n<2^r} (-1)^{S_2(n)} (n^2 - n) = 0$$

dat ook

$$\sum_{n<2^r} (-1)^{S_2(n)} n^2 = 0.$$

Dan zien we dus inductief dat uit

$$f^{(k)}(1) = \sum_{n<2^r} (-1)^{S_2(n)} n(n-1)\cdots(n-k+1) = 0$$

volgt dat

$$\sum_{n<2^r} (-1)^{S_2(n)} n^k = 0.$$

voor alle $k < r$. $\square$

Merk op dat de vergelijking in stelling 3.3 de eerste $2^r - 1$ elementen uit $\mathbb{N}$ nemen. Dit is in het bijzonder een rij beginnend bij 0 met stapgrootte 1. Er is eerder benoemd dat Thue-Morse toegepast op een *rekenkundige rij* een oplossing voor PTE geeft. Beschouw het volgende voorbeeld.

Voorbeeld 3.6. Neem de rekenkundige rij

$$\{3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48\}.$$

Aan de hand van de Thue-Morse rij wordt deze rij gesplitst en krijgen we de oplossing

$$\{3, 12, 18, 21, 30, 33, 39, 47\} =_3 \{6, 9, 15, 24, 27, 36, 42, 45\}.$$

Er valt zelf na te gaan dat dit inderdaad een oplossing is voor het PTE probleem voor van graad 3. Dit is ook te verklaren met stelling 2.3. Beschouw de polynoom $f(x) = 3x + 3$. We nemen als beginrij

$$R = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}.$$

Dan zegt stelling 2.3 dat de corresponderende splitsing van

$$R' = \{f(x) : x \in R\} = \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48\}$$

ook een oplossing is voor het PTE probleem. $\oslash$

4 Ontleding van polynomen

Er is een verband tussen bepaalde oplossingen voor het PTE probleem en de ontleedbaarheid van polynomen. In dit hoofdstuk bekijken we de definitie van ontleedbaarheid, wanneer polynomen ontleedbaar zijn en zien we een aantal voorbeelden. De polynomen waar we vanaf nu naar gaan kijken zijn monisch. Een polynoom wordt *monisch* genoemd als de kopcoëfficiënt gelijk is aan 1. Ofwel

$$p(x) = x^n + \alpha_{n-1}x^{n-1} + ... + \alpha_1 x + \alpha_0.$$

met $\alpha_n = 1$ en $a_i \in \mathbb{Z}$.

4.1 Ontleedbaarheid

Definitie 4.1 (Ontleedbaarheid [10])**.** Een polynoom f over $\mathbb{Z}$ is *ontleedbaar* als er twee polynomen g en h over $\mathbb{Z}$ van een graad strikt groter dan 1 bestaan, zodoende dat $f = g \circ h$. D.w.z. $f(x) = g(h(x))$. ⊘

Opmerking. Zij α een lineaire polynoom met inverse α^{-1}, waarvoor geldt

$$(\alpha \circ \alpha^{-1})(x) = (\alpha^{-1} \circ \alpha)(x) = x.$$

Als g', h' polynomen zijn met een graad groter dan 1 z.d.d. $g' = g \circ \alpha^{-1}$ en $h' = \alpha \circ h$, dan beschouwen we $g \circ h$ en $g' \circ h'$ als eenzelfde ontleding van f. Een ontleding is dus niet uniek. ⊘

We gaan bekijken wanneer polynomen wel en niet ontleedbaar zijn.

We merken als eerst op dat polynomen van graad n waarbij n priem is, niet ontleedbaar zijn. Was deze wel ontleedbaar geweest dan zouden er twee polynomen met graad m en l bestaan zodanig dat de compositie hiervan een polynoom is van graad $m \cdot l = n$. Dit is in tegenspraak met dat n priem is of dat m en l strikt groter zijn dan 1.

Voorbeeld 4.2. We beschouwen nu een polynoom van graad 4. Deze is van de vorm

$$f(x) = x^4 + Ax^3 + Bx^3 + Cx^4.$$

Voor deze polynoom om ontleedbaar te zijn moeten er twee tweedegraads polynomen

$$g(x) = x^2 + ax + b, \qquad h(x) = x^2 + cx + d$$

bestaan waarvoor $f = g \circ h$. Als we de compositie nemen van g en h zien we dat de coëfficiënten van polynoom f aan onderstaande eisen moeten voldoen:

$$\begin{cases} A = 2c \\ B = a + c^2 + 2d \\ C = 2cd + ac \\ D = ad + b + d^2. \end{cases}$$

Voorbeelden van een ontleedbare functies van graad 4 zijn

- $x^4 + 2x^3 + 8x^2 + 7x + 11 = (x^2 + x + 2)^2 + 3(x^2 + x + 2) + 1$ met $a = 3, b = 1, c = 1$ en $d = 2$.
- $x^4 + 4x^3 + 7x^2 + 6x + 5 = (x^2 + 2x + 1)^2 + (x^2 + 2x + 1) + 3$ met $a = 1, b = 3, c = 2$ en $d = 1$.

Andersom kunnen we onderzoeken of een willekeurige vierdegraads polynoom ontleedbaar is. We nemen als voorbeeld het polynoom

$$f(x) = x^4 + 3x^3 + 9x^2 + 12x + 20. \tag{7}$$

Dan proberen we volgend stelsel op te lossen

$$\begin{cases} 3 = 2c \\ 9 = a + c^2 + 2d \\ 12 = 2cd + ac \\ 20 = ad + b + d^2. \end{cases}$$

De eerste vergelijking geeft $c = \frac{3}{2}$. Vullen we deze waarde in in de tweede vergelijking krijgen we $9 = a + (\frac{3}{2})^2 + 2d$, ofwel $d = \frac{1}{8}(27 - 4a)$. Dan vullen we de gevonden waarden van c en d in in het linkerlid van de derde vergelijking:

$$\begin{aligned} 2cd + ac &= 2 \cdot \frac{3}{2} \cdot \frac{1}{8}(27 - 4a) + \frac{3}{2}a \\ &= \frac{3}{8} \cdot 27 - \frac{3}{8}4a + \frac{3}{2} \\ &= \frac{81}{8}. \end{aligned}$$

Dit is duidelijk ongelijk aan 12. We zien dat dit stelsel niet oplosbaar is. Hieruit concluderen we dat polynoom $f(x) = x^4 + 3x^3 + 9x^2 + 12x + 20$ niet ontleedbaar is. $\oslash$

4.2 Ontbindbaarheid

Definitie 4.3 (Ontbindbaarheid)**.** Een polynoom f is *ontbindbaar* over $\mathbb{Z}$ als er twee polynomen g en h over $\mathbb{Z}$ bestaan, zodoende dat $f = g \cdot h$. $\oslash$

Stelling 4.4. *Ontbindbaarheid impliceert geen ontleedbaarheid en ook niet andersom.*

Bewijs. We bewijzen deze stelling aan de hand van twee tegenvoorbeelden. We merken op dat f uit (7) te schrijven is als

$$f(x) = (x^2 + 3x + 5)(x^2 + 4)$$

en dus ontbindbaar is. Daaruit volgt dat ontbindbaarheid geen ontleedbaarheid impliceert.

Dan nemen we als voorbeeld het polynoom $x^4 + 1$. Als deze ontbindbaar zou zijn dan zou dat enkel in twee polynomen met een vorm van $g(x) = x^2 + a$ en $h(x) = x^2 + b$ zijn. We bekijken de factorisatie van hun product:

$$x^4 + 1 = (x^2 + a)(x^2 + b) = x^4 + (a + b)x^2 + ab.$$

Waaruit volgt dat $a + b = 0$ en $ab = 1$. Substitueren we $a = -b$ in de tweede vergelijking krijgen we $b = \sqrt{-1}$. Dit is alleen mogelijk in $\mathbb{C}$. Het polynoom $x^4 + 1$ dus niet ontbindbaar over $\mathbb{Z}$. Dit polynoom is wel te schrijven als

$$x^4 + 1 = (x^2)^2 + 1,$$

en is dus ontleedbaar. Dit laat zien dat ontleedbaarheid ook geen ontbindbaarheid impliceert. $\square$

5 Newton's identiteiten

Om de stelling over het verband tussen oplossingen van het PTE probleem en ontleedbare polynomen te bewijzen, hebben we identiteiten nodig dat twee verschillende symmetrische polynomen bevat, genaamd *Newton's identiteiten.*

5.1 Elementair symmetrische polynomen

Zij $p(x)$ een polynoom van graad n met nulpunten in $a_1, ..., a_n \in \mathbb{Z}$, dan is p te schrijven als

$$p(x) = (x - a_1)(x - a_2) \cdots (x - a_n). \tag{8}$$

Factoriseren we dit polynoom dan krijgen we een polynoom van de vorm

$$\begin{aligned} p(x) &= \sigma_0(a_1, ..., a_n)x^n - \sigma_1(a_1, ..., a_n)x^{n-1} + \sigma_2(a_1, ..., a_n)x^{n-2} - ... \\ &\quad + (-1)^n \sigma_n(a_1, ..., a_n) \\ &= \sum_{i=0}^{n} (-1)^i \sigma_i(a_1, ..., a_n)x^{n-i}. \end{aligned}$$

Met

$$\begin{aligned} &\sigma_0(a_1, ..., a_n) = 1 \\ &\sigma_1(a_1, ..., a_n) = a_1 + a_2 + ... + a_n \\ &\sigma_2(a_1, ..., a_n) = a_1a_2 + ... + a_1a_n + a_2a_3 + ... + a_2a_n + ... + a_{n-1}a_n \\ &\vdots \\ &\sigma_n(a_1, ..., a_n) = a_1 \cdots a_n. \end{aligned}$$

Hierin wordt σ_i een elementair symmetrisch polynoom in $a_1, ..., a_n$ genoemd.

Definitie 5.1 (Elementair symmetrische polynomen)**.** Zij $a_1, ..., a_n \in \mathbb{Z}$. Dan zijn de *elementair symmetrische polynomen* in $a_1, ..., a_n$ gegeven door

$$\sigma_k(a_1, ..., a_n) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} a_{i_1} \cdots a_{i_k}.$$

voor $k \in \mathbb{N}$. $\oslash$

Deze polynomen worden symmetrisch genoemd omdat ze dezelfde waarde geven voor alle permutaties van $\{a_1, ..., a_n\}$.

5.2 Machtssommen

Definitie 5.2 (Machtssommen)**.** Zij $a_1, ..., a_n \in \mathbb{Z}$. Dan zijn de *machtssommen* symmetische polynomen in $a_1, ..., a_n$ gegeven door:

$$s_k(a_1, ..., a_n) = \sum_{i=1}^{n} a_i^k,$$

voor $k \in \mathbb{N}$. ⊘

Voorbeeld 5.3. Voor $n = 3$ krijgen we de machtssommen:

$$\begin{aligned}
&s_1(a_1, a_2, a_3) = a_1 + a_2 + a_3 \\
&s_2(a_1, a_2, a_3) = a_1^2 + a_2^2 + a_3^2 \\
&s_3(a_1, a_2, a_3) = a_1^3 + a_2^3 + a_3^3 \\
&\vdots \\
&s_k(a_1, a_2, a_3) = a_1^k + a_2^k + a_3^k.
\end{aligned}$$

⊘

Met de volgende identiteiten is de relatie te zien tussen de elementair symmetrische polynomen en de machtssommen.

Stelling 5.4 (Newton's identiteiten)**.** *Newton's identiteiten geven de volgende relaties tussen de elementair symmetrische polynomen en de machtssommen in* $a_1, ..., a_n$*:*

- *Voor* $k \leq n$ *geldt:*

$$\begin{aligned}
&s_0 = n \\
&s_1 = \sigma_1 \\
&s_2 = \sigma_1 s_1 - 2\sigma_2 \\
&s_3 = \sigma_1 s_2 - \sigma_2 s_1 + 3\sigma_3 \\
&\vdots \\
&s_{n-1} = \sigma_1 s_{n-2} - \sigma_2 s_{n-3} + ... + (-1)^{n-3}\sigma_{n-2} s_1 + (-1)^{n-2}\sigma_{n-1} \cdot (n-1)
\end{aligned}$$

- *Voor* $k > n$ *geldt:*

$$s_k = \sum_{j=1}^{n} (-1)^{j+1} \sigma_j s_{k-j}.$$

Opmerking. Deze identiteiten zijn recursief te gebruiken om machtssommen uit te drukken in elementair symmetrische polynomen en andersom. Zoals bijvoorbeeld

$$
\begin{aligned}
&s_1 = \sigma_1 \\
&s_2 = \sigma_1^2 - 2\sigma_2 \\
&s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 \\
&\text{etc.}
\end{aligned}
$$

$\oslash$

Uit deze identiteiten volgt dat wanneer de machtssommen van twee verzamelingen gelijk zijn, zeg $s_k(A) = s_k(B)$ voor $0 \leq k \leq r$, dan ook de elementair symmetrische polynomen aan elkaar gelijk zijn voor dezelfde k: $\sigma_k(A) = \sigma_k(B)$. En andersom. Van deze eigenschap maken we gebruik in het volgende hoofdstuk.

6 Verband tussen oplossingen van het PTE probleem en ontleedbaarheid van polynomen

In dit hoofdstuk komen oplossingen van het PTE probleem en ontleedbaarheid van polynomen samen. Dit verband komt alleen voor onder ideale oplossingen van het PTE probleem.

Definitie 6.1 (Ideale oplossingen.)**.** Een oplossing voor het PTE probleem noemen we *ideaal* als het maat n en graad $n-1$ heeft. ⊘

Voorbeelden. Zie de oplossingen van voorbeeld 2.1.1 en 2.1.3.

Een ideale oplossing is het maximale geval van een oplossing voor het PTE probleem. Met een maat van n is een graad hoger dan $n-1$ niet mogelijk [3]. Het is lastig om ideale oplossingen te vinden. Tot nu toe zijn er ideale oplossingen gevonden tot en met graad 11. Dat is niet veel voor een probleem dat al twee eeuwen bekend is. De algemene formules die gebruikt zijn om de ideale oplossingen te vinden die nu bekend zijn staan beschreven in “Computational Excursions in Analysis and Number Theory” van P. Borwein [2] en “Ideal Solutions of the Tarry-Escott Problem” van J. Chernick [4]. Merk ook op dat de oplossingen die gevonden worden met behulp van de Thue-Morse rij niet ‘sterk’ zijn wat betreft de verhouding tussen de maat en de graad. Deze zijn over het algemeen niet ideaal, op graad 0 en 1 na.

Opmerking. Als $\{A\} =_{n-1} \{B\}$ een ideale oplossing is dan geldt dat $s_k(A) = s_k(B)$ voor $k \in \{1, ..., n-1\}$. Uit Newton's identiteiten volgt dat dan ook de elementair symmetrische polynomen $\sigma_1, ..., \sigma_{n-1}$ van A en B gelijk aan elkaar zijn. ⊘

We hebben tot nu toe gekeken naar oplossingen voor het PTE probleem in twee verzamelingen. Om de volgende stelling die we gaan introduceren te veralgemeniseren, bekijken we oplossingen in t verzamelingen.

We bekijken de partitie $A_0, ..., A_t$ met $t \geq 2$ van verzameling $N = \{1, ..., m\}$ met $m \in \mathbb{N}$, waarbij $A_1, ..., A_t$ ideale oplossingen geven voor het PTE probleem met

$$| A_1 | = | A_2 | = \ ... \ = | A_t | = \ n.$$

De overige getallen uit N zijn in A_0 bevat, of A_0 is leeg. Verder noemen we $A = \{1, ..., m\} \setminus A_0$.

Stelling 6.2. *[Hajdu, Papp en Tijdeman, pg. 1079-1080 [7]] Zij* $A_0, ..., A_t$ *een partitie als boven genoemd. Deze partitie bestaat d.e.s.d.a. het polynoom*

$$f_A(x) = \prod_{a \in A} (x - a)$$

ontleedbaar is in $\mathbb{Z}$. *In het bijzonder, als de partitie bestaat dan is* $f_A(x) = h_1(h_2(x))$ *met*

$$h_2(x) = \prod_{a \in A_1} (x - a) - \prod_{a \in A_1} (-a)$$

en

$$h_1(x) = \left(x + \prod_{a \in A_1} (-a) \right) \cdots \left(x + \prod_{a \in A_t} (-a) \right).$$

Opmerking. Het polynoom h_2 is gedefinieerd op elementen uit verzameling A_1. In het bewijs wordt duidelijk dat het niet uit maakt welke A_i ($i \in \{1, ..., t\}$) gebruikt wordt. $\oslash$

Bewijs stelling 6.2. Stel dat de partitie bestaat. Dat wil zeggen dat $\sigma_j(A_1) = \sigma_j(A_2) = ... = \sigma_j(A_t)$ voor $j \in \{1, ..., n-1\}$. We noemen de elementen uit de klassen $A_i = \{a_{i1}, ..., a_{in}\}$. Dan is

$$f_A(x) = (x - a_{11}) \cdots (x - a_{1n})(x - a_{21}) \cdots (x - a_{2n}) \cdots (x - a_{t1}) \cdots (x - a_{tn})$$

en

$$\begin{aligned} h_2(x) &= (x - a_{11}) \cdots (x - a_{1n}) - (-a_{11}) \cdots (-a_{1n}) \\ &= x^n - \sigma_1(A_1) x^{n-1} + \sigma_2(A_1) x^{n-2} - ... + (-1)^{n-1} \sigma_{n-1}(A_1) x. \end{aligned}$$

Merk op dat we hebben aangenomen dat de partitie bestaat dus σ_j voor $j \in \{1, ..., n-1\}$ is gelijk voor elke klasse. Zo zien we dus dat het niet uitmaakt welke A_i ($i \in \{1, ..., t\}$) gebruikt wordt in h_2. We schrijven h_2 als

$$h_2(x) = \sum_{j=0}^{n-1} (-1)^j \sigma_j x^{n-j}.$$

Dan zien we dat

$$\begin{aligned}
h_1(h_2(x)) &= \left(\sum_{j=0}^{n-1}(-1)^j\sigma_j x^{n-j} + \prod_{a\in A_1}(-a)\right)\cdots\left(\sum_{j=0}^{n-1}(-1)^j\sigma_j x^{n-j} + \prod_{a\in A_t}(-a)\right)\\
&= \left(\sum_{j=0}^{n-1}(-1)^j\sigma_j(A_1) x^{n-j} + \prod_{a\in A_1}(-a)\right)\cdots\left(\sum_{j=0}^{n-1}(-1)^j\sigma_j(A_t) x^{n-j} + \prod_{a\in A_t}(-a)\right)\\
&= \left(\prod_{a\in A_1}(x-a)\right)\cdots\left(\prod_{a\in A_t}(x-a)\right)\\
&= \prod_{a\in A}(x-a)\\
&= f_A(x).
\end{aligned}$$

We concluderen dat f_A ontleedbaar is in de gedefinieerde h_1 en h_2.

Dan veronderstellen we nu dat $h_1(h_2(x))$ een ongedefinieerde ontleding is van $f_A(x)$ en gaan we aantonen dat de partitie bestaat. Omdat polynoom f_A monisch is volgt dat polynomen h_1 en h_2 dat ook zijn. We definiëren h_1 als

$$h_1(x) = \prod_{i=1}^{t}(x-\alpha_i),$$

en A_i als de verzameling van de nulpunten van $h_2(x)-\alpha_i$. Dan hebben we

$$h_1(h_2(x)) = \prod_{i=1}^{t}(h_2(x)-\alpha_i) = f_A(x) = \prod_{i=1}^{t}\left(\prod_{a\in A_i}(x-a)\right).$$

Schrijven we nu $h_2(x) = x^n + b_{n-1}x^{n-1} + ... + b_1x + b_0$, dan hebben we

$$\begin{aligned}
x^n + b_{n-1}x^{n-1} + ... + b_1x + b_0 - \alpha_i &= h_2(x) - \alpha_i\\
&= \prod_{a\in A_i}(x-a)\\
&= \sum_{j=0}^{n}(-1)^j\sigma_j(A_i)x^{n-j}.
\end{aligned}$$

Met de gelijkheden

$$\begin{aligned}
&\sigma_0(A_i) = 1\\
&\sigma_1(A_i) = -b_{n-1}\\
&\sigma_2(A_i) = b_{n-2}\\
&\vdots\\
&\sigma_{n-1}(A_i) = (-1)^{n-1}b_1\\
&\sigma_n(A_i) = (-1)^n(b_0 - \alpha_i).
\end{aligned}$$

We zien dus dat b_j voor $j \in \{1, ..., n-1\}$ onafhankelijk is van i. Dat betekent dat voor deze j, $\sigma_j(A_i)$ gelijk is voor alle i. Hieruit volgt dat de partitie bestaat. $\square$

6.1 Voorbeelden

We bekijken voorbeelden van decomposities van functie f_A met gegeven oplossingen van het PTE probleem.

Voorbeeld 6.3. We nemen voorbeeld 2.1.1 uit hoofdstuk 2 met ideale oplossing: $A_1 = \{2, 3, 7\}, A_2 = \{1, 5, 6\}$ en $A = \{1, 2, 3, 5, 6, 7\}$. Dit is een oplossing voor de machten $0 \leq k \leq 2$ en dus geldt dat $\sigma_i(A_1) = \sigma_i(A_2)$ voor $0 \leq i \leq 2$. Herinner dat $\sigma_0(A) = 1$ voor elke willekeurige verzameling A. We construeren $h_2(x)$:

$$\begin{aligned}
h_2(x) &= (x-2)(x-3)(x-7) - (-2)(-3)(-7)\\
&= \sigma_0(2,3,7)x^3 - \sigma_1(2,3,7)x^2 + \sigma_2(2,3,7)x - \sigma_3(2,3,7) + \sigma_3(2,3,7)\\
&= x^3 - \sigma_1(2,3,7)x^2 + \sigma_2(2,3,7)x.
\end{aligned}$$

En $h_1(x)$:

$$\begin{aligned}
h_1(x) &= (x + (-2)(-3)(-7))\,(x + (-1)(-5)(-6))\\
&= (x - 2\cdot 3\cdot 7)\,(x - 1\cdot 5\cdot 6)\\
&= (x - \sigma_3(2,3,7))\,(x - \sigma_3(1,5,6))
\end{aligned}$$

Dan nemen we de compositie h_1 na h_2 en maken we gebruik van de gelijkheid van de elementair symmetrische polynomen:

$$\begin{aligned}
h_1(h_2(x)) &= \big((x^3 - \sigma_1(2,3,7)x^2 + \sigma_2(2,3,7)x) - \sigma_3(2,3,7)\big)\cdot\\
&\quad\ \big((x^3 - \sigma_1(2,3,7)x^2 + \sigma_2(2,3,7)x) - \sigma_3(1,5,6)\big)\\
&= \big(x^3 - \sigma_1(2,3,7)x^2 + \sigma_2(2,3,7)x - \sigma_3(2,3,7)\big)\cdot\\
&\quad\ \big(x^3 - \sigma_1(1,5,6)x^2 + \sigma_2(1,5,6)x - \sigma_3(1,5,6)\big)\\
&= ((x-2)(x-3)(x-7))\,((x-1)(x-5)(x-6))\\
&= (x-1)(x-2)(x-3)(x-5)(x-6)(x-7)\\
&= f_A(x).
\end{aligned}$$

$\oslash$

Voorbeeld 6.4. We nemen voorbeeld 2.1.3 uit hoofdstuk 2 met ideale oplossing: $A_1 = \{0, 5, 6, 16, 17, 22\}, A_2 = \{1, 2, 10, 12, 20, 21\}$ en $A = \{0, 1, 2, 5, 6, 10, 12, 16, 17, 20, 21, 22\}$. De compositie van h_1 en h_2 gaat op eenzelfde manier als bij het vorige voorbeeld beschreven. Omdat dit voorbeeld een ideale oplossing is geldt dat $\sigma_i(A_1) = \sigma_i(A_2)$ voor $0 \leq i \leq 5$.

$$
\begin{aligned}
h_1(h_2(x)) =&((x^6 - \sigma_1(0, 5, 6, 16, 17, 22) + ... - \sigma_5(0, 5, 6, 16, 17, 22)) \\
&+ \sigma_6(0, 5, 6, 16, 17, 22))\cdot \\
&((x^6 - \sigma_1(0, 5, 6, 16, 17, 22) + ... - \sigma_5(0, 5, 6, 16, 17, 22)) \\
&+ \sigma_6(1, 2, 10, 12, 20, 21)) \\
=&(x^6 - \sigma_1(0, 5, 6, 16, 17, 22) + ... - \sigma_5(0, 5, 6, 16, 17, 22) \\
&+ \sigma_6(0, 5, 6, 16, 17, 22))\cdot \\
&(x^6 - \sigma_1(1, 2, 10, 12, 20, 21) + ... - \sigma_5(1, 2, 10, 12, 20, 21) \\
&+ \sigma_6(1, 2, 10, 12, 20, 21)) \\
=&((x - 0)(x - 5)(x - 6)(x - 16)(x - 17)(x - 22))\cdot \\
&((x - 1)(x - 2)(x - 10)(x - 12)(x - 20)(x - 21)) \\
=&(x - 0)(x - 1)(x - 2)(x - 5)(x - 6)(x - 10)(x - 12)(x - 16)\cdot \\
&(x - 17)(x - 20)(x - 21)(x - 22) \\
=&f_A(x).
\end{aligned}
$$

$\oslash$

Opmerking. Uit bovenstaande voorbeelden komt naar voren dat het van belang is dat $\sigma_i(A_1) = \sigma_i(A_2)$ voor $i \in \{1, ..., r - 1\}$, zodat de te termen omgewisseld kunnen worden. Als dit niet het geval is werkt deze ontleding niet. Dit legt uit waarom de stelling is gedefinieerd op enkel ideale oplossingen. $\oslash$

7 Slot

Het Prouhet-Tarry-Escott probleem kent oplossingen met verschillende maten en graden. Een manier om oplossingen te vinden gebeurt met behulp van de Thue-Morse rij. We hebben gezien wanneer polynomen ontleedbaar zijn. Er bestaat een ideale oplossing voor het PTE probleem dan en slechts dan als het polynoom dat nulpunten heeft in alle getallen uit de oplossing ontleedbaar is.

De oplossingen die we krijgen met behulp van de Thue-Morse rij zijn niet heel sterk wat betreft de verhouding tussen de maat en de graad. Dan rest ons de vraag: hoe worden ideale oplossingen voor het PTE probleem systematisch gevonden?

Als laatste wil ik graag Gunther Cornelissen bedanken voor de fantastische begeleiding tijdens het schrijven van deze scriptie en het aandragen van het artikel waar het op gebaseerd is. Ik heb er met veel plezier aan gewerkt.

Referenties

[1] S. Altmann and E. L. Ortiz, *Mathematics and social utopias in France: Olinde Rodrigues and his times*, History of Mathematics, vol. 28, American Mathematical Soc., 2006, pagina 148.

[2] P. Borwein, *Computational excursions in analysis and number theory*, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, vol. 10, Springer-Verlag, New York, 2002. MR 1912495

[3] T. Caley, *The Prouhet-Tarry-Escott problem for Gaussian integers*, Math. Comp. **82** (2013), no. 282, 1121–1137. MR 3008852

[4] J. Chernick, *Ideal solutions of the tarry-escott problem*, The American Mathematical Monthly **44** (1937), no. 10, 626–633.

[5] N. Pytheas Fogg, *Substitutions in dynamics, arithmetics and combinatorics*, Lecture Notes in Mathematics, vol. 1794, Springer-Verlag, Berlin, 2002, Edited by V. Berthé, S. Ferenczi, C. Mauduit and A. Siegel. MR 1970385

[6] M. Gardner, *New mathematical diversions*, revised ed., MAA Spectrum, Mathematical Association of America, Washington, DC, 1995. MR 1335231

[7] L. Hajdu, Á. Papp, and R. Tijdeman, *The Prouhet-Tarry-Escott problem, indecomposability of polynomials and Diophantine equations*, Ramanujan J. **58** (2022), no. 4, 1075–1093.

[8] University of Michigan. Board of Regents., *Proceedings of the board of regents (1901-1906)*, The University, 2000.

[9] S. Raghavendran and V. Narayanan, *The prouhet tarry escott problem: A review*, Mathematics **7** (2019), no. 3, 227.

[10] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), no. 1, 51–66. MR 1501189

[11] A. Slavík, *Transformation of mathematics between world wars: the case of combinatorics*, The development of mathematics between the World Wars—case studies, examples and analyses, World Sci. Publ., Hackensack, NJ, [2021] ©2021, p. 550. MR 4450753