**JP Journal of Algebra, Number Theory and Applications**

http://www.pphmj.com
http://dx.doi.org/10.17654/0972555522026
Volume 57, 2022, Pages 1-16 **P-ISSN: 0972-5555**

# ON THE MONOGENITY OF CERTAIN BINOMIAL COMPOSITIONS

**István Gaál**

Mathematical Institute
University of Debrecen
H-4002 Debrecen Pf. 400
Hungary
e-mail: gaal.istvan@unideb.hu

## Abstract

Recently, there are several results on the monogenity of certain classes of polynomials and the number fields generated by a root of them. In addition to the frequently investigated binomials of type $x^n - m$, trinomials of type $x^n + ax^m + b$, Harrington and Jones [8] considered binomial compositions of type $f(g(x))$, where $f(x) = x^n - a$, $g(x) = x^m - b$.

This is a completely new construction. In this paper, our purpose is to describe monogenity properties of a class of binomial compositions of degree six.

Received: April 28, 2022; Accepted: July 4, 2022
2020 Mathematics Subject Classification: Primary 11R04, 11R16; Secondary 11Y50.
Keywords and phrases: monogenity, power integral basis, binomial compositions, sextic fields, calculating the solutions.

How to cite this article: István Gaál, On the monogenity of certain binomial compositions, JP Journal of Algebra, Number Theory and Applications 57 (2022), 1-16.
http://dx.doi.org/10.17654/0972555522026

Published Online: July 9, 2022

## 1. Introduction

Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree $n$ with a root $\vartheta$. The polynomial $f(x)$ is called *monogenic* if $(1, \vartheta, ..., \vartheta^{n-1})$ is an integer basis in the number field $K = \mathbb{Q}(\vartheta)$. Such an integral basis is called *power integral basis*. A number field $K$ of degree $n$ is called *monogenic* if it admits a power integral basis, that is if there exists an algebraic integer $\vartheta \in \mathbb{Z}_K$ such that $(1, \vartheta, ..., \vartheta^{n-1})$ is an integer basis in $K$ (see [4]).

The monogenity of the polynomial $f(x)$ with a root $\vartheta$ implies the monogenity of the number field $K = \mathbb{Q}(\vartheta)$. On the other hand, $K$ can happen to be monogenic even if $f(x)$ is not monogenic.

The index of a primitive element $\vartheta \in \mathbb{Z}_K$ is defined as

$$I(\vartheta) = (\mathbb{Z}_K : \mathbb{Z}[\vartheta]).$$

$\vartheta$ generates a power integral basis (that is $(1, \vartheta, ..., \vartheta^{n-1})$ is an integer basis) if and only if $I(\vartheta) = 1$. If $\alpha, \beta \in \mathbb{Z}_K$ and $\beta \pm \alpha \in \mathbb{Z}$, then $\alpha$ and $\beta$ are called *equivalent*. Equivalent algebraic integers have the same indices.

A further important question is how many inequivalent generators of power integral bases exist? (As it is known, there are only finitely many algebraic integers in $K$ with a given index.)

Recently, there are several results on the monogenity of polynomials, just as examples, see [9-12]. A powerful method to consider this question is the Newton polygon method, cf. Guardia et al. [6, 7]. The results on monogenic polynomials usually derive as a consequence that the number field generated by a root of the polynomial is monogenic, but do not consider the monogenity of these number fields in detail. In case of a sextic family of monogenic polynomials, our main purpose is to decide *whether there exist only one or there are several inequivalent generators of power integral bases*.

To determine all inequivalent generators of power integral bases is a complicated problem, leading to the resolution of index form equations.

If $(1, \omega_2, ..., \omega_n)$ is an integral basis in $K$, then the discriminant of the linear form $L(\underline{x}) = x_1 + \omega_2 x_2 + \cdots + \omega_n x_n$ can be written as

$$D(L(\underline{x})) = I(x_2, ..., x_n)^2 \cdot D_K,$$

where $D_K$ is the discriminant of $K$ and $I(x_2, ..., x_n)$ is a homogeneous polynomial of degree $n(n-1)/2$ having the property that for any $\vartheta = x_1 + x_2\omega_2 + \cdots + x_n\omega_n \in \mathbb{Z}_K$, the equation $I(\vartheta) = |I(x_2, ..., x_n)|$ is satisfied. Therefore, determining generators of power integral bases leads to the Diophantine equation

$$I(x_2, ..., x_n) = \pm 1 \text{ in } x_2, ..., x_n \in \mathbb{Z},$$

see [4]. These *index form equations* usually only have "small" solutions, that is solutions, say, with $|x_i| < 100$. Therefore, besides the tedious algorithms determining all solutions of index form equations (or better to say, excluding extremely "large" solutions), it is certainly meaningful to use much faster algorithms, that do not exclude "large" solutions, but produce all solutions, e.g., with $|x_i| < 10^{100}$. These yield all solutions with a high probability. In all practical cases, these solutions are sufficient for further calculations. Moreover, such a fast algorithm enables us to consider a large number of number fields. Therefore, in this paper, we shall use such an algorithm.

There is an extensive literature of monogenity of binomials of type $x^n - m$, trinomials of type $x^n + ax^m + b$. Recently, Harrington and Jones [8] considered so-called *binomial compositions*. These are different from those composite fields of type $K = M \cdot L$ that we formerly considered, assuming that the discriminants of the fields $M$, $L$ are coprime [2, 5]. Harrington and Jones [8] considered binomial compositions of type $f(g(x))$, where $f(x) = x^n - a$ and $g(x) = x^m - b$.

To be able to consider a large number of polynomials of this type, and number fields generated by a root of polynomials of this type, in this paper, we consider the case $n = 2,\ m = 3,\ a = -1,$ that is our composed polynomials are of type

$$F(x) = (x^3 - b)^2 + 1. \tag{1}$$

Harrington and Jones [8] formulated statements on the monogenity of compositions of polynomials. *Our purpose is to investigate if there are further generators of power integer bases of number fields generated by a root of monogenic polynomial compositions*.

## 2. The Sextic Family

Under certain conditions, Harrington and Jones [8] gave a criterion for the monogenity of binomial compositions. In case $n = 2,$ their statement is as follows:

**Lemma 1** (Theorem 1.4 of [8])**.** *Let* $a, b, m \in \mathbb{Z}$ *with* $a \neq 0$ *and* $m \geq 2,$ *and let* $\hat{m} = m/\gcd(2a, m)$. *Let* $f(x) = x^2 - a,\ \ g(x) = x^m - b,$ $T(x) = f(g(x))$ *and suppose that* $\kappa(|\, am\,|) = \kappa(|\, b^2 - a\,|),$ *where* $\kappa(*)$ *denotes the squarefree kernel of the positive integer* $*$. *Then* $f(x)$ *and* $T(x)$ *are monogenic if and only if all of the following conditions hold*:

(1) *a is squarefree*,

(2) $a \not\equiv 1 \pmod 4,$

(3) $b^2 - a \not\equiv 0 \pmod{p^2}$ *for all primes p dividing* $\hat{m}$,

(4) $-(2b)^{p+1} + 3b^2 + a \not\equiv 0 \pmod{p^2}$ *for all primes p dividing* $\hat{m}$.

In case of our sextic polynomials, for $m = 3,\ \ a = -1,$ the condition $\kappa(|\, am\,|) = \kappa(|\, b^2 - a\,|)$ yields $\kappa(3) = \kappa(b^2 + 1).$ Since $b \equiv 0, \pm 1 \pmod 3$ hence $b^2 + 1 \equiv 1,\ 2 \not\equiv 0 \pmod 3,$ this condition can never be satisfied in our

case. Let us remark that even if the above lemma does not apply to our case, it covers a wide class of binomial compositions.

We were interested in describing the monogenity properties of the polynomials (1) and the number fields generated by a root of the monogenic polynomials. These number fields are certainly monogenic, our point was to find out if there exist only one or several inequivalent generators of power integral bases in these fields.

*For this purpose, we considered the polynomials* (1) *for* $1 \leq b \leq 500000$.

## 3. Discriminants and Indices

In this section, we give some statements for the discriminants of the polynomials $g(x) = (x^3 - b)^2 - a$ (these statements are valid for any $a \in \mathbb{Z}$). The following lemmas can be proved by direct Maple calculation, but they will be necessary in the sequel.

**Lemma 2.** *Assume* $a, b \in \mathbb{Z}$, $a \neq 0, 1$ *such that* $g(x) = (x^3 - b)^2 - a$ *is irreducible. Then*

$$D(g) = 2^6 3^6 (a - b^2)^2 a^3.$$

*If* $\alpha$ *is a root of* $g(x)$, *then the basis*

$$B = \{1, \alpha, \alpha^2, \sqrt{a}, \sqrt{a} \cdot \alpha, \sqrt{a} \cdot \alpha^2\}$$

*has discriminant*

$$D(B) = D(g).$$

Let $M = \mathbb{Q}(\sqrt{a})$, $K = \mathbb{Q}(\alpha)$. As it is known (see [13, p. 150]), the discriminant $D_K$ of $K$ can be expressed by the discriminant $D_M$ of $M$ and the relative discriminant $D_{K/M}$ of $K$ over $M$:

$$D_K = D_M^3 \cdot N_{M/\mathbb{Q}}(D_{K/M}).$$

Denote by $\alpha_{1,j}$ the cube roots of $b+\sqrt{a}$ and by $\alpha_{2,j}$ the cube roots of $b-\sqrt{a}$ $(j=1, 2, 3)$: these are the conjugates of $\alpha$. We have:

**Lemma 3.** *Assume* $a, b \in \mathbb{Z}$, $a \neq 0, 1$ *such that* $g(x) = (x^3-b)^2 - a$ *is irreducible. Then*

$$D(g) = D(\alpha) = D_1 \cdot D_2,$$

*where*

$$\sqrt{|D_1|} = \sqrt{|N_{M/\mathbb{Q}}(D_{K/M})|}$$

$$= \left| \prod_{1\le j_1<j_2\le 3} (\alpha_{1,j_1} - \alpha_{1,j_2}) \cdot \prod_{1\le j_1<j_2\le 3} (\alpha_{2,j_1} - \alpha_{2,j_2}) \right|$$

$$= 27|b^2 - a|,$$

$$\sqrt{|D_2|} = \sqrt{|D_M^3|} = \left| \prod_{1\le j_1\le 3} \prod_{1\le j_2\le 3} (\alpha_{1,j_1} - \alpha_{2,j_2}) \right| = 8(\sqrt{|a|})^3.$$

As above, let $\alpha$ be a root of the polynomial $g(x) = (x^3-b)^2 - a = x^6 - 2x^3b + b^2 - a$, and $K = \mathbb{Q}(\alpha)$ with ring of integers $\mathbb{Z}_K$. As it is shown in Lemma 2, if $g(x)$ is a monogenic polynomial, that is $(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5)$ is an integer basis, then $(1, \alpha, \alpha^2, \sqrt{a}, \sqrt{a}\cdot\alpha, \sqrt{a}\cdot\alpha^2)$ is also an integer basis. We shall represent the algebraic integers $\vartheta \in \mathbb{Z}_K$ in the form

$$\vartheta = x_1 + x_2\alpha + x_3\alpha^2 + y_1 i + y_2 i\alpha + y_3 i\alpha^2 = X_1 + \alpha X_2 + \alpha^2 X_3, \qquad (2)$$

with $X_j = x_j + iy_j$ $(j=1, 2, 3)$, where $x_j, y_j \in \mathbb{Z}$, $X_j \in \mathbb{Z}_M$ $(j=1, 2, 3)$.

According to the discriminant, the index of $\vartheta$ also has two factors (see [4]):

**Lemma 4.** *Using the above notation*,

$$I(\vartheta) = F_1(x_2,\ y_2,\ x_3,\ y_3) \cdot F_2(y_1,\ x_2,\ y_2,\ x_3,\ y_3),$$

*where*

$$F_1(x_2,\ y_2,\ x_3,\ y_3)$$

$$= \frac{\sqrt{|\ N_{M/\mathbb{Q}}(D_{K/M}(\vartheta))\ |}}{\sqrt{|\ N_{M/\mathbb{Q}}(D_{K/M})\ |}} = \prod_{k=1}^{2} \left| \prod_{1 \le j_1 < j_2 \le 3} \frac{(\vartheta_{k,\,j_1} - \vartheta_{k,\,j_2})}{(\alpha_{k,\,j_1} - \alpha_{k,\,j_2})} \right|$$

$$= \prod_{k=1}^{2} \left| \prod_{j=1}^{3} (X_2 - \alpha_{k,\,j} X_3) \right|$$

$$= |\ N_{M/\mathbb{Q}}(N_{K/M}(X_2 - \alpha X_3))\ | = |\ N_{M/\mathbb{Q}}(X_2^3 - (b + \sqrt{a})X_3^3)\ |$$

*and*

$$F_2(y_1,\ x_2,\ y_2,\ x_3,\ y_3) = \left| \prod_{1 \le j_1 \le 3} \prod_{1 \le j_2 \le 3} \frac{(\vartheta_{1,\,j_1} - \vartheta_{2,\,j_2})}{(\alpha_{1,\,j_1} - \alpha_{2,\,j_2})} \right|.$$

*Both polynomials* $F_1$ *and* $F_2$ *have integer coefficients*.

## 4. Monogenic Polynomials of Degree 6

Let us return to our polynomials $F(x) = (x^3 - b)^2 + 1$ setting $a = -1$ in the above $g(x)$. We were checking the monogenity of these polynomials for $1 \le b \le 500000$. We found that in each interval of 500 parameters, the number of monogenic polynomials was between 390 and 404. In the following table, we list the number # of monogenic polynomials for some indicated intervals of the parameter $b$:

| | # | | # | | # |
|---|---|---|---|---|---|
| $1 \le b \le 500$ | 401 | $250001 \le b \le 250500$ | 398 | $494001 \le b \le 494500$ | 398 |
| $501 \le b \le 1000$ | 396 | $250501 \le b \le 251000$ | 396 | $495501 \le b \le 496000$ | 397 |
| $1001 \le b \le 1500$ | 400 | $251001 \le b \le 251500$ | 398 | $496001 \le b \le 496500$ | 396 |
| $1501 \le b \le 2000$ | 397 | $251501 \le b \le 252000$ | 399 | $496501 \le b \le 497000$ | 397 |
| $2001 \le b \le 2500$ | 400 | $252001 \le b \le 252500$ | 399 | $497001 \le b \le 497500$ | 403 |
| $2501 \le b \le 3000$ | 395 | $252501 \le b \le 253000$ | 398 | $497501 \le b \le 498000$ | 394 |
| $3001 \le b \le 3500$ | 397 | $253001 \le b \le 253500$ | 395 | $498001 \le b \le 498500$ | 399 |
| $3501 \le b \le 4000$ | 398 | $253501 \le b \le 254000$ | 400 | $498501 \le b \le 499000$ | 402 |
| $4001 \le b \le 4500$ | 394 | $254001 \le b \le 254500$ | 401 | $499001 \le b \le 499500$ | 398 |
| $4501 \le b \le 5000$ | 400 | $254501 \le b \le 255000$ | 395 | $499501 \le b \le 500000$ | 400 |

In the interval $1 \le b \le 500000$, we found all together 397715 monogenic polynomials, that is the number of monogenic polynomials was 79.543%. The occurrence of monogenic polynomials seemed to be quite regular. This calculation took 125 minutes, using Maple.

## 5. The Relative Thue Equation

We were further interested in describing multi-monogenity of number fields, generated by a root of the above monogenic polynomials. If $F(x) = (x^3 - b)^2 + 1$ is a monogenic polynomial for certain parameter $1 \le b \le 500000$, we wondered if $\alpha$ is the only generator of a power integral basis of $K$ or there are other (inequivalent) generators of power integral bases.

To answer this question, we have to determine all $\vartheta \in \mathbb{Z}_K$ with $I(\vartheta) = 1$. In view of the above lemmas, this is equivalent to solving the system of equations:

$$F_1(x_2,\ y_2,\ x_3,\ y_3) = \pm 1, \tag{3}$$

$$F_2(y_1,\ x_2,\ y_2,\ x_3,\ y_3) = \pm 1. \tag{4}$$

For the parameters $1 \le b \le 500000$, we found 397715 monogenic polynomials. It is only possible to consider this large number of fields by

using some fast algorithm. Therefore, we determine all solutions of the above system of equations with

$$| x_j |, | y_j | \le 10^{100} \ (j = 1, 2, 3). \tag{5}$$

As the index form equations usually only have small solutions, the solutions with the above property yield all solutions with a very high probability.

**5.1. Elementary estimates**

Equation (3) is a relative Thue equation. We used the fast algorithm [3] to determine its solutions with (5). To enable that method to solve 397715 equations, we must prepare its application very accurately.

Let $\alpha = \alpha_{11} = \sqrt[3]{b + i}$ be a root of $F(x) = (x^3 - b)^2 + 1$. Set $\alpha_{12} = \left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i\right)\alpha$ and $\alpha_{13} = \left(-\frac{1}{2} - \frac{\sqrt{3}}{2} i\right)\alpha$. Similarly, let $\alpha_{2j}$ $(j = 1, 2, 3)$ be the three values of $\sqrt[3]{b - i}$.

Assume that $x_2, y_2, x_3, y_3 \in \mathbb{Z}$ is a solution of equation (3). Then, in view of Lemma 4, we have

$$\prod_{j=1}^{3} | X_2 - \alpha_{1j} X_3 | = 1. \tag{6}$$

Denote by $j_0$ the index with $| X_2 - \alpha_{1j_0} X_3 | = \min_j | X_2 - \alpha_{1j} X_3 |$. Obviously,

$$| X_2 - \alpha_{1j_0} X_3 | \le 1. \tag{7}$$

Then, using $| \alpha_{1j} - \alpha_{1j_0} | = \sqrt{3} | \alpha |$, for $j \ne j_0$, we have

$$\begin{aligned} | X_2 - \alpha_{1j} X_3 | &= | (\alpha_{1j} - \alpha_{1j_0}) X_3 - (X_2 - \alpha_{1j_0} X_3) | \\ &\ge \sqrt{3} \cdot | \alpha | \cdot | X_3 | - 1 \ge (\sqrt{3} \cdot | \alpha | - \varepsilon) | X_3 |, \end{aligned}$$

assumed $\varepsilon|X_3| \geq 1$, that is $|X_3| \geq 1/\varepsilon$. This implies in turn by (6) that

$$|X_2 - \alpha_{1j_0} X_3| \leq \frac{1}{(\sqrt{3}|\alpha| - \varepsilon)^2} \cdot \frac{1}{|X_3^2|}. \tag{8}$$

Finally,

$$|X_2| \leq |X_2 - \alpha_{1j_0} X_3| + |\alpha| \cdot |X_3| \leq \frac{\varepsilon^2}{(\sqrt{3}|\alpha| - \varepsilon)^2} + |\alpha| \cdot |X_3|$$

$$\leq (\delta + |\alpha|)|X_3|,$$

assuming $\delta \geq \varepsilon^2/(|X_3| \cdot (\sqrt{3}|\alpha| - \varepsilon)^2)$. This implies by (8),

$$A = \max(|x_2|, |y_2|, |x_3|, |y_3|) \leq \max(|X_2|, |X_3|) \leq (\delta + |\alpha|) \cdot |X_3|,$$

whence

$$|X_2 - \alpha_{1j_0} X_3| \leq c \cdot \frac{1}{A^2}, \tag{9}$$

with

$$c = \frac{(\delta + |\alpha|)^2}{(\sqrt{3}|\alpha| - \varepsilon)^2}.$$

We were using this inequality with $\varepsilon = 1/30$ and $\delta = 30^{-3} = 0.000037$. We had $c \leq 0.3426$: according to the value of $b$, we calculated it separately for each $b$.

**5.2. Reduction**

In view of (9), if $x_2$, $y_2$, $x_3$, $y_3$ is a solution of (6), then for some $j_0$ $(1 \leq j_0 \leq 3)$, we have

$$|x_2 + i \cdot y_2 - \alpha_{1j_0} x_3 - \alpha_{1j_0} i \cdot y_3| \leq \frac{c}{A^2}. \tag{10}$$

The following procedure must be performed for all possible values of $j_0$.

Let $H$ be a large integer and consider the lattice generated by the columns of the following matrix:

$$\mathcal{L} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ H & 0 & -H \cdot Re(\alpha_{1j_0}) & -H \cdot Re(i\alpha_{1j_0}) \\ 0 & H & -H \cdot Im(\alpha_{1j_0}) & -H \cdot Im(i\alpha_{1j_0}) \end{pmatrix}.$$

Denote by $b_1$ the first vector of the LLL reduced basis of $\mathcal{L}$.

According to Theorem 3 of [3] (see also Lemma 5.3 of [4]), we have:

**Lemma 5.** *If* $(x_2, y_2, x_3, y_3) \in \mathbb{Z}^4$ *is a solution of* (9),

$$A = \max(|x_2|, |x_3|, |y_2|, |y_3|) \leq A_0$$

*and H is so large that*

$$|b_1| \geq \sqrt{40} A_0,$$

*then*

$$A \leq \left(\frac{c_1 H}{A_0}\right)^{1/2}.$$

Applying this lemma, we obtain that $H$ is of magnitude $A_0^2$, therefore $A$ will be about $\sqrt{A_0}$. To find the solutions with $\max(|x_2|, |y_2|, |x_3|, |y_3|) \leq 10^{100}$ of the relative Thue equation (6), we applied the above lemma first with $A_0 = 10^{100}$, then, in several subsequent steps with the previous reduced bound for $A$, obtained by the lemma. In the first reduction steps, we took $H = 10^3 A_0^2$, in the last steps, we took $H$ as small as possible. The following table displays the values of $H$ and as the reduced bound "new $A_0$", the maximum of the reduced bounds obtained for all considered parameters. The CPU time refers to the total CPU time for all possible

parameters together. Also, as we had to use multiple precision arithmetics, we also include the number of digits used in that reduction step.

| Step | $A_0$ | $H$ | $\|\| b_1 \|\| \geq$ | Digits | New $A_0$ | CPU time |
|---|---|---|---|---|---|---|
| 1. | $10^{100}$ | $10^{203}$ | $6.324555 \cdot 10^{100}$ | 250 | $1.8509 \cdot 10^{51}$ | 3000 sec |
| 2. | $1.8509 \cdot 10^{51}$ | $3.42583 \cdot 10^{105}$ | $1.1706 \cdot 10^{52}$ | 150 | $7.9632 \cdot 10^{26}$ | 2500 sec |
| 3. | $7.963 \cdot 10^{26}$ | $6.3409 \cdot 10^{56}$ | $5.0362 \cdot 10^{27}$ | 100 | $5.2232 \cdot 10^{14}$ | 500 sec |
| 4. | $5.2232 \cdot 10^{14}$ | $2.7281 \cdot 10^{32}$ | $3.3034 \cdot 10^{15}$ | 50 | $4.2302 \cdot 10^{8}$ | 400 sec |
| 5. | $4.2302 \cdot 10^{8}$ | $1.7894 \cdot 10^{20}$ | $2.6754 \cdot 10^{9}$ | 30 | $3.8069 \cdot 10^{5}$ | 190 sec |
| 6. | $3.8069 \cdot 10^{5}$ | $1.4492 \cdot 10^{14}$ | $2.4076 \cdot 10^{6}$ | 20 | 11420 | 170 sec |
| 7. | 11420 | $1.3041 \cdot 10^{11}$ | 72226.4217 | 20 | 1978 | 167 sec |
| 8. | 1978 | $2.3474 \cdot 10^{9}$ | 12509.9704 | 20 | 637 | 132 sec |
| 9. | 637 | $1.6230 \cdot 10^{8}$ | 4028.7417 | 20 | 295 | 113 sec |
| 10. | 295 | $2.6107 \cdot 10^{7}$ | 1865.7438 | 20 | 174 | 110 sec |
| 11. | 174 | $9.0828 \cdot 10^{6}$ | 1100.4726 | 20 | 133 | 110 sec |
| 12. | 133 | $5.3067 \cdot 10^{6}$ | 841.1658 | 20 | 116 | 110 sec |
| 13. | 116 | $2.6912 \cdot 10^{6}$ | 733.6484 | 20 | 89 | 110 sec |
| 14. | 89 | $1.4257 \cdot 10^{6}$ | 562.8854 | 20 | 74 | 110 sec |
| 15. | 74 | $7.6664 \cdot 10^{5}$ | 468.0170 | 20 | 59 | 110 sec |
| 16. | 59 | $3.4810 \cdot 10^{5}$ | 373.1487 | 20 | 44 | 110 sec |
| 17. | 44 | $1.9360 \cdot 10^{5}$ | 278.2804 | 20 | 38 | 110 sec |

As mentioned above, in the last reduction steps, we took $H$ as small as possible. As a consequence, we had several exceptional parameters, for which we had to perform the reduction procedure separately. The final reduced bounds were found different from the value 38 obtained for all other parameters. These exceptional parameters and the corresponding reduced bound are stated below:

| $b$ | Bound |
|---|---|
| 11 | 44 |
| 75 | 44 |
| 272 | 50 |
| 283 | 51 |
| 422 | 73 |
| 862 | 56 |
| 899 | 116 |
| 1123 | 44 |

| $b$ | Bound |
|---|---|
| 1516 | 116 |
| 1781 | 204 |
| 2278 | 46 |
| 3160 | 44 |
| 3261 | 44 |
| 4096 | 44 |
| 4564 | 88 |
| 4913 | 44 |

We dealt with these parameters separately.

**5.3. Enumerating solutions under the bound**

Except for the above few parameters, for all $b$ in question we had to test if equation (3) has solutions with $|x_2|, |y_2|, |x_3|, |y_3| \leq 38$. This bound is in accordance with our assumption $|X_3| > 1/\varepsilon = 30$. In [3], the basic proposed method is to enumerate the $x_3, y_3$ with absolute values $\leq 38$, calculate $X_2$ from

$$X_2^3 - (b+i)X_3^3 = \pm 1, \pm i \tag{11}$$

and test if the real and imaginary parts of $X_3$ are integers.

This works fast for some fixed equations, but not for a huge number of parameters. Therefore, we used a different strategy which can be useful also in similar cases.

We let $x_2$ run through $[0, 38]$, $y_2$, $x_3$, $y_3$ run through $[-38, 38]$. Substituting $x_2, y_2, x_3, y_3$ into (11), we tested if the corresponding value of $b$ is an integer (for some of the possible right hand sides). We also had to check if the possible values of $b$ correspond to monogenic polynomials.

If $(x_2, y_2, x_3, y_3)$ is a solution of (3), corresponding to $X_2, X_3 \in \mathbb{Z}_M$, then $(-y_2, x_2, -y_3, x_3)$ is also a solution, corresponding to $iX_2, iX_3 \in \mathbb{Z}_M$. Moreover, the negatives of these solutions are also solutions, but we list the solutions only up to sign.

The solutions of the relative Thue equation (3) we substituted into equation (4) to check if there exists a $y_1$ corresponding to $(x_2, y_2, x_3, y_3, b)$.

We found two tuples that are solutions for any values of $b$ but there exists a corresponding $y_1$ only for one of them:

| $b$ | $x_2$ | $y_2$ | $x_3$ | $y_3$ | $y_1$ |
|---|---|---|---|---|---|
| *any b* | 0 | 1 | 0 | 0 | −− |
| *any b* | 1 | 0 | 0 | 0 | 0 |

Since we consider monogenic polynomials, $\vartheta = \alpha$ indeed generates a power integral basis, as it was known.

There are some sporadic solutions:

| $b$ | $x_2$ | $y_2$ | $x_3$ | $y_3$ | $y_1$ |
|---|---|---|---|---|---|
| 1 | 0 | −1 | 1 | 0 | −− |
| 1 | 1 | 0 | 0 | 1 | −1 |
| 2 | 1 | −1 | −1 | 0 | −− |
| 2 | 1 | 1 | 0 | −1 | −− |
| 11 | 1 | 2 | −1 | 0 | −− |
| 11 | −2 | 1 | 0 | −1 | −− |
| 25 | 1 | 4 | 1 | −1 | −− |
| 25 | −4 | 1 | 1 | 1 | −− |

The above parameters correspond to monogenic polynomials. We obtain that there exists an additional generator of power integral basis only for $b = 1$, namely $\vartheta = \alpha - i + i\alpha^2$.

In cases $b = k^3$ is a cube, our data allowed us to conjecture and formally prove by Maple that the following tuples are solutions of (3) for any such $b$. There exists a corresponding solution $y_1$ of (4) only in one of the cases:

| $b$ | $x_2$ | $y_2$ | $x_3$ | $y_3$ | $y_1$ |
|---|---|---|---|---|---|
| $k^3$ | 0 | $k$ | 0 | 1 | $k^2$ |
| $k^3$ | $k$ | 0 | 1 | 0 | −− |

This implies that for $b = k^3$, the integer $\vartheta = ik^3 + ik\alpha + i\alpha^2$ may also generate a power integral basis. However, the parameters $b = k^3$ do not always give monogenic polynomials. It will be monogenic, e.g., for $k = 1$, 2, 4, 5, 8, 10, 11 etc, but not for $k =$ 3, 6, 7, 9, 12 etc.

The complete calculation described in this section took about 10.5 CPU hours.

## 6. Summary

We summarize our results as follows:

**Theorem 6.** *For* $1 \le b \le 500000$, *the polynomial* $F(x) = (x^3 - b)^2 + 1$ *is monogenic for* 397715 *parameters. If* $F(x)$ *is monogenic,* $\alpha$ *is a root of* $F(x)$ *and* $K = \mathbb{Q}(\alpha)$, *then for the above parameters, up to equivalence* $\vartheta = \alpha$ *is the only generator of power integral bases of K, represented in the form* (2), *with the property* (5), *except*

$\vartheta = \alpha - i + i\alpha^2$ *for* $b = 1$, *and*

$\vartheta = ik^3 + ik\alpha + i\alpha^2$, *if b is a cube.*

We conjecture that $F(x)$ is monogenic for infinitely many parameters of the form $b = k^3$ and in all such cases, the above $\vartheta = \alpha$ and $\vartheta = ik^3 + ik\alpha + i\alpha^2$ yield all inequivalent generators of power integral bases. Moreover, we guess that all other number fields generated by a root of a monogenic polynomial $F(x)$ has up to equivalence only $\vartheta = \alpha$ as a generator of power integral bases.

## 7. Computational Remarks

All our algorithms were coded in Maple and were executed on a laptop with Core i7 processors.

## References

[1] B. W. Char, K. O. Geddes, G. H. Gonnet, M. B. Monagan and S. M. Watt, eds., MAPLE, Reference Manual, Watcom Publications, Waterloo, Canada, 1988.

[2] I. Gaál, Power integral bases in composita of number fields, Canad. Math. Bull. 41 (1998), 158-165.

[3] I. Gaál, Calculating “small” solutions of relative Thue equations, Exp. Math. 24(2) (2015), 142-149.

[4] I. Gaál, Diophantine equations and power integral bases, Theory and Algorithms, 2nd ed., Birkhäuser, Boston, 2019.

[5] I. Gaál and L. Remete, Integral bases and monogenity of composite fields, Exp. Math. 28(2) (2019), 209-222.

[6] J. Guardia, J. Montes and E. Nart, Newton polygons of higher order in algebraic number theory, Trans. Amer. Math. Soc. 364(1) (2012), 361-416.

[7] J. Guardia and E. Nart, Genetics of polynomials over local fields, Contemp. Math. 637 (2015), 207-241.

[8] J. Harrington and L. Jones, Monogenic binomial compositions, Taiwanese J. Math. 24(5) (2020), 1073-1090.

[9] R. Ibarra, H. Lembeck, M. Ozaslan, H. Smith and K. E. Stange, Monogenic fields arising from trinomials, arXiv:1908.09793.

[10] A. Jakhar, S. K. Khanduja and N. Sangwan, Characterization of primes dividing the index of a trinomial, Int. J. Number Theory 13(10) (2017), 2505-2514.

[11] L. Jones and T. Phillips, Infinite families of monogenic trinomials and their Galois groups, Internat. J. Math. 29(5) (2018), Article ID 1850039, 11 pp.

[12] L. Jones and D. White, Monogenic trinomials with non-squarefree discriminant, Internat. J. Math. 32(13) (2021), Paper no. 2150089, 21 pp.

[13] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, 3rd ed., Springer, 2004.