Canad. Math. Bull. Vol. 65 (3), 2022, pp. 806–814
http://dx.doi.org/10.4153/S0008439521000874

A dynamical characterization for monogenity at every level of some infinite 2-towers

Marianela Castillo

Abstract. We consider a concrete family of 2-towers $(\mathbb{Q}(x_n))_n$ of totally real algebraic numbers for which we prove that, for each n, $\mathbb{Z}[x_n]$ is the ring of integers of $\mathbb{Q}(x_n)$ if and only if the constant term of the minimal polynomial of x_n is square-free. We apply our characterization to produce new examples of monogenic number fields, which can be of arbitrary large degree under the ABC-Conjecture.

1 Introduction

Let

$$\mathbb{Z}^{(v,x_0)} = \bigcup_{n\geq 0} R_n,$$

where $R_0 = \mathbb{Z}$ and $R_n = R_{n-1}[x_n]$, for some fixed rational integers $v \geq 2$ and $x_0 \geq 0$ such that $v + x_0$ is not a square and x_n is the positive square root of $v + x_{n-1}$. Note that $R_n = \mathbb{Z}[x_n]$. Let $\mathbb{Q}^{(v,x_0)}$ be the fraction field of $\mathbb{Z}^{(v,x_0)}$.

In this paper, we give a characterization for the ring $\mathbb{Z}^{(v,x_0)}$ to be the ring of integers of $\mathbb{Q}^{(v,x_0)}$, answering partially a question raised by Vidaux and Videla in [10, Question 1.1, and the paragraph above Question 1.5]. The original motivation comes from a question in mathematical logic raised by Julia Robinson (see [10]).

For each n, let P_n denote the minimal polynomial of x_n over $\mathbb{Q}$. In Section 3 we prove the following result.

Theorem 1.1 *Assume that $v + x_0$ is congruent to 2 or 3 modulo 4 and is square-free. The ring $\mathbb{Z}^{(v,x_0)}$ is the ring of integers of $\mathbb{Q}^{(v,x_0)}$ if and only if $P_n(0)$ is square-free for all $n \geq 1$.*

Received by the editors June 16, 2021; revised July 13, 2021, accepted September 15, 2021.
Published online on Cambridge Core October 20, 2021.
The work is part of my PhD thesis [1] under the supervision of X. Vidaux and C. R. Videla, to whom I am grateful for support and encouragement. It has been supported by the Conicyt fellowship "Beca Doctorado Nacional," by the Universidad de Concepción (Chile), and by the Fondecyt research project 1130134 (Chile) of X. Vidaux. Part of this work was done while visiting Carlos R. Videla at Mount Royal University, Calgary, Canada. I am grateful to the referees for their careful reading of this paper, which helped improving the presentation and simplify some proofs.
AMS subject classification: **11N32**, 11R04, 11R80.
Keywords: Totally real fields, 2-towers, monogenic fields, square-free integers, iteration of polynomials.

Table 1: Values of n such that $P_k(0)$ is square-free for k up to n.

v	$n = 1$	$n = 2$	$n = 6$	v	$n = 1$	$n = 2$	$n = 6$
3			X	47			X
6			X	51	X		
7			X	55	X		
10	X			58			X
11			X	59		X	
14			X	62			X
15			X	66			X
19	X			67			X
21	X			70			X
22			X	71			X
23			X	74			X
26	X			78			X
30			X	79			X
31			X	82	X		
34		X		83			X
35			X	86			X
38			X	87			X
39			X	91	X		
42			X	94			X
43			X	95		X	
46	X						

The only pairs for which we know that our theorem applies are $(2, 0)$ and $(2, 1)$, which corresponds to known cases (see Liang [4]). To determine any other pair for which the above result applies appears to be a very difficult problem. However, numerically we have established that for many pairs (v, x_0) and values of n, $P_n(0)$ is square-free, and therefore we are able to produce new examples of monogenic number fields. It should be noted that the problem of determining whether or not a number field is monogenic goes back to Dedekind, who showed that cyclotomic number fields are monogenic (see [2] for a modern presentation of the subject).

For our proof to work, we need that the tower increases at each step, meaning that for every n, $\mathbb{Q}(x_n)$ has degree 2 over $\mathbb{Q}(x_{n-1})$ (in particular, this implies that P_n has degree 2^n). In [10, Proposition 2.15], it is shown that this happens whenever $v + x_0$ is congruent to 2 or 3 modulo 4. We observe that if $x_0 = 0$ and v is not a square, the tower also increases at each step (apply [8, Corollary 1.3] to the iterated of $f(t) = t^2 - v$.

Assuming $x_0 = 0$, we computed $P_n(0)$ for n from 1 to 6 and for v up to 100. Considering only the relevant values of v, in the Table 1 an X in the cell (v, n) means that $P_k(0)$ is square-free for k up to n. It is remarkable that there is no X for $n = 3, 4, 5$. From this, we obtain new monogenic number fields up to degree 2^6. One can go further for some given value of v. Could it be true that for $v = 3$, $P_n(0)$ is always square-free?

https://doi.org/10.4153/S0008439521000874 Published online by Cambridge University Press

In Section 4, we give some more evidence for the existence of pairs $(\nu, 0) \neq (2, 0)$ for which Theorem 1.1 applies. In particular, under the ABC-Conjecture, and assuming that $x_0 = 0$, we prove that for each n, there exist infinitely many values of ν for which $P_n(0)$ is square-free. We will also prove that, for $\nu \geq 3$, the largest prime divisor of $P_n(0)$ tends to infinity as n tends to infinity.

We finish this introduction by a remark. Indeed, in order to prove Theorem 1.1, we will prove that for each $n \geq 1$, $P_n(0)$ is square-free if and only if $\mathbb{Z}[x_n]$ is the ring of integers of $\mathbb{Q}(x_n)$. Because of the latter, the condition that $\nu + x_0$ is congruent to 2 or 3 modulo 4 cannot be dropped, because

(1) if $\mathbb{Z}[x_n] = \mathcal{O}_{\mathbb{Q}(x_n)}$ for some $n \geq 2$, then also $\mathbb{Z}[x_{n-1}] = \mathcal{O}_{\mathbb{Q}(x_{n-1})}$; and
(2) for square-free $\nu + x_0$, the ring $\mathbb{Z}[x_1]$ is equal to the ring of integers $\mathcal{O}_{\mathbb{Q}(x_1)}$ of $\mathbb{Q}(x_1)$ if and only if $\nu + x_0$ is congruent to 2 or 3 modulo 4.

To see why item 1 is true, let $\alpha \in \mathcal{O}_{\mathbb{Q}(x_{n-1})}$. If $\mathbb{Z}[x_n] = \mathcal{O}_{\mathbb{Q}(x_n)}$, then we have

$$\alpha = a_0 + a_1 x_n + a_2 x_n^2 + \cdots + a_{2^n-1} x_n^{2^n-1},$$

for some $a_i \in \mathbb{Z}$. Separating even and odd powers of x_n, since $x_n^2 = \nu + x_{n-1}$, we have

$$\alpha = a + b x_n,$$

for some $a, b \in \mathbb{Z}[x_{n-1}]$. Since the tower increases at each step, we have $x_n \notin \mathbb{Q}(x_{n-1})$, and we deduce that b is 0. Hence, $\alpha \in \mathbb{Z}[x_{n-1}]$.

2 Discriminant of x_n

In this section we assume that the integer $\nu + x_0$ is square-free and congruent to 2 or 3 modulo 4. We will prove the following result.

Proposition 2.1 *Assume that $\mathbb{Q}(x_n)$ has degree 2^n over $\mathbb{Q}$. We have*

$$\operatorname{disc}(x_0) = 1 \text{ and } \operatorname{disc}(x_1) = 2^2(\nu + x_0),$$

and for $n \geq 2$ we have

$$\operatorname{disc}(x_n) = (\operatorname{disc}(x_{n-1}))^2 \cdot 2^{2^n} P_n(0).$$

In our situation, the assumption that $\mathbb{Q}(x_n)$ has degree 2^n over $\mathbb{Q}$ is fulfilled because $\nu + x_0$ is congruent to 2 or 3 modulo 4 (see [10, Proposition 2.15]). Under this assumption, $\mathbb{Q}(x_n)$ has basis

$$B_n := \{1, x_n, x_n^2, \ldots, x_n^{2^n-1}\}$$

over $\mathbb{Q}$. Note that the field extension $\mathbb{Q}(x_n)/\mathbb{Q}(x_m)$ has degree 2^{n-m}. We will denote by $\operatorname{disc}_{n/n-1}(x_n)$ the discriminant of x_n from $\mathbb{Q}(x_n)$ to $\mathbb{Q}(x_{n-1})$. Hence, for $n \geq 1$, we have

$$\operatorname{disc}_{n/n-1}(x_n) = \begin{vmatrix} 1 & x_n \\ 1 & -x_n \end{vmatrix}^2 = 4(x_n)^2 = 4(\nu + x_{n-1}).$$

https://doi.org/10.4153/S0008439521000874 Published online by Cambridge University Press

Notation 2.2 For $n \geq 1$, we denote by N_n the norm from $\mathbb{Q}(x_n)$ to $\mathbb{Q}$ of $\mathrm{disc}_{n+1/n}(x_{n+1})$, and by N_0 the discriminant of x_1 from $\mathbb{Q}(x_1)$ to $\mathbb{Q}$.

Proposition 2.3 *We have*

(1) $N_0 = 2^2(\nu + x_0)$, *and*

(2) $N_n = 2^{2^{n+1}} P_{n+1}(0)$ *for any* $n \geq 1$.

Proof Item 1 is immediate from our above computation, so we prove item 2. Let $n \geq 1$. We have

$$\begin{aligned} N_n &= \mathrm{Norm}_{\mathbb{Q}(x_n)/\mathbb{Q}}\left(\mathrm{disc}_{n+1/n}(x_{n+1})\right) \\ &= \mathrm{Norm}_{\mathbb{Q}(x_n)/\mathbb{Q}}(4(\nu + x_n)) \\ &= 2^{2^{n+1}} \mathrm{Norm}_{\mathbb{Q}(x_n)/\mathbb{Q}}(\nu + x_n) \\ &= 2^{2^{n+1}} \mathrm{Norm}_{\mathbb{Q}(x_n)/\mathbb{Q}}(-\mathrm{Norm}_{\mathbb{Q}(x_{n+1})/\mathbb{Q}(x_n)}(x_{n+1})) \\ &= 2^{2^{n+1}} \mathrm{Norm}_{\mathbb{Q}(x_{n+1})/\mathbb{Q}}(x_{n+1}) \\ &= 2^{2^{n+1}} P_{n+1}(0) \end{aligned}$$

■

We need the following proposition (see [5, Chapter 2, Exercise 23, p. 43]).

Proposition 2.4 *Let* $K \subset L \subset M$ *be number fields,* $[L{:}K] = n$, $[M{:}L] = m$, *and let* $\{\alpha_1, \ldots, \alpha_n\}$ *and* $\{\beta_1, \ldots, \beta_m\}$ *be bases for* L *over* K *and* M *over* L, *respectively. We have*

$$\mathrm{disc}_{M/K}(\alpha_1\beta_1, \ldots, \alpha_n\beta_m) = \left(\mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n)\right)^m \cdot \mathrm{Norm}_{L/K}\left(\mathrm{disc}_{M/L}(\beta_1, \ldots, \beta_m)\right).$$

Proposition 2.1 follows from Propositions 2.3 and 2.4 in the following way. Take

$$K = \mathbb{Q}, \quad L = \mathbb{Q}(x_{n-1}), \quad \text{and} \quad M = \mathbb{Q}(x_n).$$

The degree of L over K is 2^{n-1} and L has basis

$$\left\{1, x_{n-1}, x_{n-1}^2, \ldots, x_{n-1}^{2^{n-1}-1}\right\}$$

over K, while the degree of M over L is 2 and M has basis $\{1, x_n\}$ over L. The set $\{\alpha_1\beta_1, \ldots, \alpha_n\beta_m\}$ in Proposition 2.4 corresponds to the set

$$B' = \left\{1, x_{n-1}, x_{n-1}^2, \ldots, x_{n-1}^{2^{n-1}-1}, x_n, x_{n-1}x_n, x_{n-1}^2 x_n, \ldots, x_{n-1}^{2^{n-1}-1} x_n\right\}.$$

This set B' is a basis for M over K. Indeed, we have

$$|B'| = 2\left(2^{n-1} - 1\right) + 2 = 2^n = |B_n|,$$

and since $x_n^2 = \nu + x_{n-1}$, each element of B_n can be written as a $\mathbb{Z}$-linear combination of elements of B'. Similarly, each element of B' is a $\mathbb{Z}$-linear combination of elements

https://doi.org/10.4153/S0008439521000874 Published online by Cambridge University Press

of B_n. Since the base change matrices from B_n to B' and from B' to B_n have an integral determinant and because the discriminants are also integers, we deduce

$$\mathrm{disc}_{M/K}(B') = \mathrm{disc}_{M/K}(B_n) = \mathrm{disc}_{M/K}(x_n).$$

One obtains the formula in Proposition 2.1 by using in Proposition 2.4 the formulas from Proposition 2.3.

3 Proof of Theorem 1.1

In this section we assume that the integer $\nu + x_0$ is square-free and congruent to 2 or 3 modulo 4.

We start by a lemma that we will need at the end of the section in order to finish the proof of Theorem 1.1.

Lemma 3.1 *If $\mathbb{Z}^{(\nu,x_0)}$ is the ring of integers of its fraction field, then $\mathbb{Z}[x_n] = \mathcal{O}_{\mathbb{Q}(x_n)}$ for every $n \geq 1$.*

Proof For n fixed, let $\alpha \in \mathcal{O}_{\mathbb{Q}(x_n)}$, hence α can be written as $a + bx_n$, for some $a, b \in \mathbb{Q}(x_{n-1})$. Since $\alpha \in \mathbb{Z}^{(\nu,x_0)}$, there exists $m \geq 0$ such that $\alpha \in \mathbb{Z}[x_m]$. If $m = 0$, then $\alpha \in \mathbb{Z}$, so we assume $m > 0$. Choose $m > 0$ minimal such that $\alpha \in \mathbb{Z}[x_m]$. Note that there exist $c, d \in \mathbb{Z}[x_{m-1}]$ such that $\alpha = c + dx_m$ and $d \neq 0$ (by minimality of m). Therefore, we have

$$a + bx_n = c + dx_m,$$

hence $x_m \in \mathbb{Q}(x_n)$, so $m \leq n$ and $\alpha \in \mathbb{Z}[x_n]$. ∎

We will also use the following result from [9].

Theorem 3.2 [9] *Let R be a Dedeking ring. Let θ be an element of some integral domain which contains R and let θ be integral over R. Then $R[\theta]$ is a Dedekind ring if and only if the defining polynomial $f(t)$ of θ is not contained in $\mathfrak{m}^2$ for any maximal ideal $\mathfrak{m}$ of the polynomial ring $R[t]$.*

Before we go to the proof of the theorem, we need to recall a few facts.

Proposition 3.3 [6, Proposition 2.13] *Let θ be an algebraic integer. We have*

$$\mathrm{disc}(\theta) = m^2 \mathrm{disc}(\mathbb{Q}(\theta)),$$

where m is the index in $\mathcal{O}_{\mathbb{Q}(\theta)}$ of the $\mathbb{Z}$-module $\mathbb{Z}[\theta]$.

Definition 3.1 We say that a monic polynomial

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with coefficients in $\mathbb{Z}$ is *p-Eisenstein* with respect to the prime number p, if $a_0, a_1, \ldots, a_{n-1}$ are divisible by p, and p^2 does not divide a_0.

https://doi.org/10.4153/S0008439521000874 Published online by Cambridge University Press

Lemma 3.4 [6, Lemma 2.17] *Let θ be an algebraic integer and p be a prime number. If the minimal polynomial of θ over $\mathbb{Q}$ is p-Eisenstein, then the index of θ in $\mathbb{Q}(\theta)$ is not divisible by p.*

In the proof of Proposition 2.15 in [10], Vidaux and Videla proved the following result.

Proposition 3.5 [10] *For each $n \geq 1$, let P_n be the minimal polynomial of x_n. Suppose that $\nu + x_0$ is congruent to 2 or 3 modulo 4. We have*

(1) *if n is odd, then $P_n(t+a)$ is 2-Eisenstein, where*

$$a = \begin{cases} 0 \text{ if } \nu + x_0 \equiv 2 \mod 4, \\ 1 \text{ if } \nu + x_0 \equiv 3 \mod 4, \end{cases}$$

and

(2) *if n is even, then $P_n(t+x_0)$ is 2-Eisenstein.*

Moreover, writing $f(t) = t^2 - \nu$, we have $P_n(t) = f^{\circ n}(t) - x_0$, hence in particular P_n has no monomial of odd degree (here, $f^{\circ n}$ stands for the composition of f with itself n times).

Proposition 3.6 *For all $n \geq 1$, if $\nu + x_0$ is congruent to 2 or 3 modulo 4, then the index in $\mathcal{O}_{\mathbb{Q}(x_n)}$ of the $\mathbb{Z}$ module $\mathbb{Z}[x_n]$ is not divisible by 2.*

Proof It is an immediate consequence of Proposition 3.5 and Lemma 3.4, since for any rational integer c, $P_n(t+c)$ is the minimal polynomial of $x_n - c$, $\mathbb{Z}[x_n - c] = \mathbb{Z}[x_n]$, and $\mathbb{Q}(x_n - c) = \mathbb{Q}(x_n)$. ∎

3.1 Proof of Theorem 1.1

Assume first that there exists $n \geq 1$ such that $P_n(0)$ is not square-free. Let p be a prime such that p^2 divides $P_n(0)$ and write $P_n(0) = p^2 s$, where $s \in \mathbb{Z} - \{0\}$. Since P_n has only monomials of even degree, we have

$$P_n(t) = p^2 s + pt \cdot 0 + t^2 g(t),$$

for some $g(t) \in \mathbb{Z}[t]$. Hence $P_n(t) \in (p,t)^2 \subseteq \mathbb{Z}[t]$. Since the ideal (p,t) is a maximal ideal of $\mathbb{Z}[x_n]$ (the quotient ring is the field $\mathbb{F}_p$), $\mathbb{Z}[x_n]$ is not the ring of integers of $\mathbb{Q}(x_n)$ by Theorem 3.2. We deduce from Lemma 3.1 that $\mathbb{Z}^{\nu,x_0}$ is not the ring of integers of its fraction field.

We will show by induction on n that if $P_n(0)$ is square-free, then $\mathbb{Z}[x_n] = \mathcal{O}_{\mathbb{Q}(x_n)}$. This is enough to prove the other direction in Theorem 1.1. Indeed, if $\alpha \in \mathcal{O}_{\mathbb{Q}(\nu,x_0)}$, then there exists $n \geq 0$ such that $\alpha \in \mathcal{O}_{\mathbb{Q}(x_n)} = \mathbb{Z}[x_n]$.

Let m_n be the index in $\mathcal{O}_{\mathbb{Q}(x_n)}$ of the $\mathbb{Z}$-module $\mathbb{Z}[x_n]$, so that

$$\operatorname{disc}(x_n) = m_n^2 \operatorname{disc} \mathbb{Q}(x_n)$$

by Proposition 3.3. We prove that $m_n = 1$.

https://doi.org/10.4153/S0008439521000874 Published online by Cambridge University Press

For $n = 1$, we have $\operatorname{disc}(x_1) = 4(\nu + x_0) = \operatorname{disc}\mathbb{Q}(x_1)$, because $\nu + x_0 \equiv 2, 3 \pmod 4$.

For $n \geq 2$, suppose that $m_{n-1} = 1$, that is $\operatorname{disc}(x_{n-1}) = \operatorname{disc}\mathbb{Q}(x_{n-1})$. By Proposition 2.1 and by induction hypothesis we have

$$2^{2^n} P_n(0) = \frac{\operatorname{disc}(x_n)}{(\operatorname{disc}(x_{n-1}))^2} = \frac{m_n^2 \operatorname{disc}\mathbb{Q}(x_n)}{(\operatorname{disc}\mathbb{Q}(x_{n-1}))^2}.$$

On the one hand, by Proposition 3.6 we have that 2 does not divide m_n, and on the other hand, by [6, Corollary 1 of Proposition 4.15], the discriminant of $\mathbb{Q}(x_n)$ is divisible by

$$(\operatorname{disc}\mathbb{Q}(x_{n-1}))^{[\mathbb{Q}(x_n):\mathbb{Q}(x_{n-1})]} = (\operatorname{disc}\mathbb{Q}(x_{n-1}))^2.$$

Hence, $P_n(0) = m_n^2 \ell$ for some $\ell \in \mathbb{Z}$. We deduce that $m_n = 1$ because $P_n(0)$ is assumed to be square-free.

4 Monogenity up to any level assuming ABC

In all this section, we assume $x_0 = 0$.

Given an integer $r \geq 2$ and a polynomial $h \in \mathbb{Z}[X]$ of degree r, we consider

$$N_h(x) = \#\{n \leq x : h(n) \text{ is square-free}\},$$

and

$$G_h = \gcd\{h(n) : n \geq 1\}.$$

Theorem 4.1 [3, Theorem 1] *Assume the ABC-Conjecture. Let $h \in \mathbb{Z}[t]$ be a polynomial with integer coefficients, of degree at least 2, without repeated factors. If G_h is square-free, then*

$$N_h(x) \sim c_h x,$$

for some $c_h > 0$.

Recall that since $x_0 = 0$, we have $P_n(t) = f^{\circ n}(t)$, where $f(t) = t^2 - \nu$. We define the polynomials $g_n(t) \in \mathbb{Z}[t]$ by induction on n:

- $g_1(t) = -t$, and
- $g_{n+1}(t) = (g_n(t))^2 - t$, for each $n \geq 2$.

So in particular we have $P_1(0) = -\nu = g_1(\nu)$, and if $P_n(0) = g_n(\nu)$, then

$$P_{n+1}(0) = (f \circ f^{\circ n})(0) = (f^{\circ n}(0))^2 - \nu = P_n(0)^2 - \nu = g_n(\nu)^2 - \nu = g_{n+1}(\nu).$$

Therefore, for each $n \geq 1$, we have

$$P_n(0) = g_n(\nu).$$

Given $\ell \geq 1$, we consider

$$h_\ell(t) = \operatorname{lcm}\{g_n(t) : 1 \leq n \leq \ell\}.$$

Lemma 4.2 *For every $\ell \geq 1$, G_{h_ℓ} is square-free.*

Proof Since $2^2 - 2 = 2$, for all $n \geq 1$ we have $g_n(2) = \pm 2$. Also, it is immediate from the definition of g that there exists a polynomial $q_n(t)$ in $\mathbb{Z}[t]$ such that $g_n(t) = tq_n(t)$. Hence for each $n \geq 1$ we have $q_n(2) = \pm 1$, and for each polynomial $p(t)$ in $\mathbb{Z}[t]$ which divides $q_n(t)$, we have $p(2) = \pm 1$. Hence for each $\ell \geq 1$, we have $h_\ell(2) = \pm 2$. Since $g_2(t) = t(t-1)$, the product $t(t-1)$ divides $h_\ell(t)$ for each $\ell \geq 2$, so 2 divides $h_\ell(t)$ for any $t \geq 2$ and for each $\ell \geq 2$, hence for each $\ell \geq 1$. We have $h_\ell(1) = -1$ for odd ℓ, in which case $G_{h_\ell} = 1$, and $h_\ell(1) = 0$ for even ℓ, in which case $G_{h_\ell} = \pm 2$. ∎

Lemma 4.3 *For every $\ell \geq 1$, the polynomial $h_\ell \in \mathbb{Z}[t]$ has degree ≥ 2 and no repeated factors.*

Proof The fact that h_ℓ has degree ≥ 2 is immediate from its definition. It is enough to show that each g_n has no repeated factor. The derivative of $g_n(t)$ is

$$g_n'(t) = 2(g_{n-1}(t)) \cdot ((g_{n-1})'(t)) - 1.$$

Hence the reduction modulo 2 of $g_n'(t)$ is equal to 1. If there were a root α in common between $g_n(t)$ and $g_n'(t)$, then $g_n'(t)$ would have the form $A(t)B(t)$, with $A(t)$ the minimal polynomial of α. Since $g_n(t)$ is monic with integer coefficients, α would be an algebraic integer, hence $A(t)$ also would be a monic polynomial with integer coefficients. By Gauss' Lemma, $B(t)$ also has integer coefficients. Reducing modulo 2, we get $A(t)B(t) \equiv 1$, hence in particular $A(t) \equiv 1$, which contradicts the fact that it is monic and non-constant. ∎

Corollary 4.4 *Assume $x_0 = 0$ and fix an integer $\ell \geq 2$. Under the ABC Conjecture, there exist infinitely many values of v such that, for all $1 \leq n \leq \ell$, $P_n(0)$ is square-free. Moreover, all these v are congruent to 2 or 3 modulo 4.*

Proof By Theorem 4.1 and Lemmas 4.2 and 4.3, we know that $h_\ell(v)$ infinitely many v. For each of those v, given $1 \leq n \leq \ell$, since g_n divides h_ℓ in $\mathbb{Z}[t]$, also $g_n(v) = P_n(0)$ is square-free. Let v be such that $P_n(0)$ each $1 \leq n \leq \ell$. In particular, $P_1(0) = -v$ and $P_2(0) = v^2 - v$ are square-free, so v cannot be congruent to 0 or 1 modulo 4. ∎

We finish with a simple remark.

Assume $v \geq 3$. Note that under this condition, the sequence $(P_n(0))_n$ is strictly increasing. We prove that the largest prime of $P_n(0)$ tends to infinity as n tends to infinity. If this were not true, then there would be no hope for $P_n(0)$ to be square-free for every n.

We adapt an argument that we saw in [7, Section 7.6, p. 105]. For the sake of contradiction, assume that there exists a sequence $(n_i)_i$ tending to infinity and there exists M such that $P_{n_i}(0) = p_1^{h_1}, \ldots, p_j^{h_j}$, with the $h_k \geq 1$ and the p_k primes less than M. Let θ_k be the remainder of the division of h_k by 3, so that $P_{n_i}(0) = p_1^{\theta_1}, \ldots, p_j^{\theta_j} y^3$, so $f(P_{n_i-1}(0)) = p_1^{\theta_1}, \ldots, p_j^{\theta_j} x^3$. The curve $f(Y) = Y^2 - v = p_1^{\theta_1}, \ldots, p_j^{\theta_j} X^3$ is an elliptic curve, so by Siegel's Theorem it has finitely many integral points. Since there are

https://doi.org/10.4153/S0008439521000874 Published online by Cambridge University Press

finitely many choices for the θ_k and for the primes, there are finitely many such curves, hence finitely many possible values for $P_{n_i}(0)$.

References

[1] M. Castillo, *On the Julia Robinson number of rings of totally real algebraic integers in some towers of nested square roots*. Ph.D. thesis, Universidad de Concepción, Chile, 2018. http://dmat.cfm.cl/dmat/doctorado/tesis/

[2] I. Gaál, *Diophantine equations and power integral bases: theory and algorithms*, Birkhäuser, Boston, 2002.

[3] A. Granville, *ABC allows us to count squarefrees*, Int. Math. Res. Not. IMRN **1998**(1998), no. 19, 991–1009.

[4] J. J. Liang, *On the integral basis of the maximal real subfield of a cyclotomic field*. J. Reine Angew. Math. **286**–**287**(1976), 223–226.

[5] D. Marcus, *Number fields*, Springer-Verlag, New York, 1977.

[6] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 3rd ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004, xii+708 p.

[7] J.-P. Serre, *Lectures on the Mordell–Weil theorem*, Aspects of Mathematics, E15, Friedr. Vieweg and Sohn, Braunschweig, 1989, x+218 p. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt.

[8] M. Stoll, *Galois group over* $\mathbb{Q}$ *of some iterated polynomials*. Arch. Math. **59**(1992), 239–244.

[9] K. Uchida, *When is* $Z[\alpha]$ *the ring of the integers?* Osaka J. Math. **14**(1977), no. 1, 155–157.

[10] X. Vidaux and C. R. Videla, *Definability of the natural numbers in totally real towers of nested square roots*. Proc. Amer. Math. Soc. **143**(2015), 4463–4477.

Departamento de Ciencias Básicas, Universidad de Concepción, Campus Los Ángeles,
Juan Antonio Coloma 201, Los Ángeles 4430000, Chile
e-mail: mcastillo@udec.cl

https://doi.org/10.4153/S0008439521000874 Published online by Cambridge University Press