On relations for rings generated by algebraic numbers and their conjugates

Paulius Drungilas, Artūras Dubickas & Jonas Jankauskas

Annali di Matematica Pura ed Applicata (1923 -)

ISSN 0373-3114
Volume 194
Number 2

Annali di Matematica (2015)
194:369-385
DOI 10.1007/s10231-013-0380-4

Springer

Annali di Matematica (2015) 194:369–385
DOI 10.1007/s10231-013-0380-4

On relations for rings generated by algebraic numbers and their conjugates

Paulius Drungilas · Artūras Dubickas · Jonas Jankauskas

Received: 4 April 2013 / Accepted: 8 October 2013 / Published online: 29 October 2013

Abstract Let α be an algebraic number of degree d with minimal polynomial $F \in \mathbb{Z}[X]$, and let $\mathbb{Z}[\alpha]$ be the ring generated by α over $\mathbb{Z}$. We are interested whether a given number $\beta \in \mathbb{Q}(\alpha)$ belongs to the ring $\mathbb{Z}[\alpha]$ or not. We give a practical computational algorithm to answer this question. Furthermore, we prove that a rational number $r/t \in \mathbb{Q}$, where $r \in \mathbb{Z}$, $t \in \mathbb{N}$, $\gcd(r, t) = 1$, belongs to the ring $\mathbb{Z}[\alpha]$ if and only if the square-free part of its denominator t divides all the coefficients of the minimal polynomial $F \in \mathbb{Z}[X]$ except for the constant coefficient $F(0)$ that must be relatively prime to t, namely $\gcd(F(0), t) = 1$. We also study the question when the equality $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha']$ for algebraic numbers α, α' conjugates over $\mathbb{Q}$ holds. In particular, it is shown that for each $d \in \mathbb{N}$, there are conjugate algebraic numbers α, α' of degree d satisfying $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$ and $\mathbb{Z}[\alpha] \neq \mathbb{Z}[\alpha']$. The question concerning the equality $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha']$ is answered completely for conjugate quadratic pairs α, α' and also for conjugate pairs α, α' of cubic algebraic integers.

Keywords Rings of algebraic numbers · Conjugate algebraic numbers · Minimal polynomial · Polynomials in finite fields · Algorithms

Mathematical Subject Classification (2010) 11R04 · 11R09 · 11T06 · 11Y16

P. Drungilas · A. Dubickas · J. Jankauskas
Department of Mathematics and Informatics, Vilnius University,
Naugarduko 24, 03225 Vilnius, Lithuania
e-mail: pdrungilas@gmail.com

A. Dubickas
e-mail: arturas.dubickas@mif.vu.lt

J. Jankauskas (✉)
Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby,
British Columbia V5A 1S6, Canada
e-mail: jonas.jankauskas@gmail.com

1 Introduction

Recall that $\alpha \in \mathbb{C}$ is an *algebraic number* over the field of rationals $\mathbb{Q}$ if there exists a nonzero polynomial

$$F(X) = a_d X^d + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$$

such that α is a root of F. Among all polynomials $F \in \mathbb{Z}[X]$ vanishing at $X = \alpha$, there exists a polynomial of the least possible degree d, which is irreducible in the ring $\mathbb{Z}[X]$ and has positive leading coefficient $a_d > 0$. This polynomial is called the *minimal polynomial* of α. The degree of the algebraic number α is defined as the degree of its minimal polynomial F. Note that the irreducibility in $\mathbb{Z}[X]$ implies that the minimal polynomial F is *primitive*, namely $\gcd(a_d, \ldots, a_0) = 1$. In particular, if the minimal polynomial F is *monic* (i.e., its leading coefficient a_d is 1), then α is called an *algebraic integer*. The roots $\alpha_1, \alpha_2, \ldots, \alpha_d$ of the minimal polynomial F are called *algebraic conjugates* of α.

For an arbitrary number $\alpha \in \mathbb{C}$, the ring $\mathbb{Z}[\alpha]$ is defined as the subset of all complex numbers that can be written as integer polynomials in α, i.e., the number $\beta \in \mathbb{C}$ belongs to $\mathbb{Z}[\alpha]$ if and only if there exists a polynomial $G \in \mathbb{Z}[X]$ such that $\beta = G(\alpha)$ (in general, the polynomial G is not unique). A necessary (but not sufficient) condition for the number β to be in $\mathbb{Z}[\alpha]$ is $\beta \in \mathbb{Q}(\alpha)$ (which is a field of fractions of $\mathbb{Z}[\alpha]$).

In this paper, we study two problems related to the ring $\mathbb{Z}[\alpha]$ generated by an algebraic number α.

Problem 1 *Let α be an algebraic number. Given $\beta \in \mathbb{Q}(\alpha)$, find whether $\beta \in \mathbb{Z}[\alpha]$ or $\beta \notin \mathbb{Z}[\alpha]$.*

This problem is inspired by the study of the representations of the numbers in different non-integer bases. Two natural problems arising in this context are the following. Which numbers can be represented by such expansions? When the representation (expansion) is finite? For instance, if a non-integer rational fraction $r/t \in \mathbb{Q}$ can be expressed in base α, where $\alpha \in \mathbb{C}$, using only finitely many terms with integer coefficients (digits), then

$$r/t = b_0 + b_1\alpha + \cdots + b_n\alpha^n$$

for some integers $b_j \in \mathbb{Z}$, $j = 0, 1, \ldots, n$. This implies that α is a root of the polynomial $r - tG(X) \in \mathbb{Z}[x]$, where $G(X) = b_0 + b_1 X + \cdots + b_n X^n$. Hence, α is an algebraic number. It is easy to see that $\mathbb{Z}[\alpha] \cap \mathbb{Q} = \mathbb{Z}$ when α is a transcendental number or an algebraic integer, so the set $\mathbb{Z}[\alpha] \cap \mathbb{Q}$ can be non-trivial only if α is an algebraic number that is not an algebraic integer.

The first authors who investigated the representations of the real numbers $x \in [0, 1)$ obtained by the greedy expansion using the map $T_\alpha(x) = \alpha x \pmod 1$ were Rényi [20] and Parry [19]. Such representations, in general, are infinite. In [19], Parry asked which numbers have finite expansions and which have ultimately periodic expansions. Bertrand [5] proved that all numbers in $\mathbb{Q}(\alpha) \cap [0, 1)$ have ultimately periodic greedy expansions if α is a *Pisot number*, i.e., a real algebraic integer greater than 1 whose all the remaining conjugates (if any) lie strictly inside the unit disc. In addition, Schmidt [21] showed that if each number in $\mathbb{Q} \cap [0, 1)$ has ultimately periodic greedy expansion in base α, then α must be a Pisot number or a *Salem number* (i.e., real algebraic integer greater than 1 with all the other conjugates being of modulus at most 1 and with some conjugates of modulus equal to 1). It is still not known whether every number in $\mathbb{Q}(\alpha)$ has a periodic greedy expansion for a Salem number α; see a paper of Boyd [7] for a discussion on this subject, which is supported by substantial

computational evidence. See also [1,6,8–10,14] for other problems concerning so-called beta-expansions.

Closely related to the expansions in non-integer bases are the studies of the spectra of real numbers

$$\Lambda^{\mathcal{B}}(\alpha) = \{b_0 + b_1\alpha + \cdots + b_n\alpha^n : \ n \in \mathbb{N}, \ b_j \in \mathcal{B}\}, \quad \mathcal{B} \subset \mathbb{Z}, \ \ |\mathcal{B}| < \infty.$$

For instance, a recent paper on the accumulation points of $\Lambda^{\mathcal{B}}(\alpha)$ by Akiyama and Komornik [3] contains a comprehensive list of references on the subject, whereas [2] is devoted to the construction of the number systems in the rings $\mathbb{Z}[\alpha]$, where α is an algebraic integer with all conjugates of modulus > 1 (see also [4] for further research on this topic).

In all the above-mentioned problems of finite and periodic representations, the case of α being an algebraic integer is of the central importance, and the integer coefficients of the representation of the number β are restricted. Clearly, this is not the case for general representations in rings $\mathbb{Z}[\alpha]$ as the coefficients of an arbitrary element $\beta \notin \mathbb{Z}[\alpha]$ do not have to be bounded in any way, and moreover, α need not be an algebraic integer. However, the study of the rings $\mathbb{Z}[\alpha]$ for algebraic numbers α that are not algebraic integers have received surprisingly little attention so far. One of the main results of this paper concerning Problem 1 is an algorithm that determines whether a given element $\beta \in \mathbb{Q}(\alpha)$ belongs to $\mathbb{Z}[\alpha]$ or not (see Theorem 4 and Sect. 5 for all the details concerning the verification of the congruence (1)). In the case when β is a rational number, the set $\mathbb{Z}[\alpha] \cap \mathbb{Q}$ can be determined by using Theorem 5 below.

If the number β belongs to $\mathbb{Z}[\alpha]$, then $\mathbb{Z}[\beta] \subseteq \mathbb{Z}[\alpha]$. For which α and β the equality $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$ holds? For this equality, it is sufficient to check whether the inclusions $\beta \in \mathbb{Z}[\alpha]$ and $\alpha \in \mathbb{Z}[\beta]$ hold at the same time using the algorithm that verifies the congruence (1) below. However, if one assumes that α and β are conjugate algebraic numbers, then it is possible to prove some more explicit results. In particular, we will investigate the following problem:

Problem 2 *Let α and α' be two conjugate algebraic numbers generating the same field, namely $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$. Determine whether $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha']$ or $\mathbb{Z}[\alpha] \neq \mathbb{Z}[\alpha']$.*

We remark that Problem 2 is of some interest in the context of non-integer expansions and number systems. More precisely, our results show that the behavior of the ring $\mathbb{Z}[\alpha]$ as a subset of $\mathbb{C}$ under different embeddings is highly non-trivial. We shall demonstrate that it is possible for a number $\beta \in \mathbb{Q}(\alpha)$ to have a finite representation in $\mathbb{Z}[\alpha]$ but do not have one in $\mathbb{Z}[\alpha']$, even if $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$ and the respective rings $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\alpha']$ are isomorphic in the algebraic sense.

One can see that the results that are proved in this paper can be restated for a polynomial ring $R[\alpha]$ over any principal ideal domain R (instead of $\mathbb{Z}$) with the quotient field K (instead of $\mathbb{Q}$) of characteristic 0, provided that α is algebraic over K. However, we are not aware of any practical applications of such generalization, so in this paper we focus on the number field setting.

2 Main results

Let α be an algebraic number of degree d with minimal polynomial $F \in \mathbb{Z}[X]$, and let $\beta \in \mathbb{Q}(\alpha)$. We assume that the expression of the number $\beta \in \mathbb{Q}(\alpha)$ is known, that is, one knows some polynomial with rational coefficients $R \in \mathbb{Q}[X]$, which represents β in the form $\beta = R(\alpha)$. Expressing the powers of α^n, where $n \geqslant d$, by smaller powers of α, we may pick R of the degree at most $d - 1$ and write this polynomial in the form

$$R(X) = \frac{G(X)}{t},$$

where $t \in \mathbb{N}$, and the coefficients of the polynomial

$$G(X) = g_0 + g_1 X + \cdots + g_{d-1} X^{d-1} \in \mathbb{Z}[X]$$

satisfy

$$\gcd(g_0, g_1, \ldots, g_{d-1}, t) = 1.$$

We call the polynomial R the *canonical representative* of β, while G shall be called the *numerator polynomial*. Both the canonical representative and the numerator polynomial are unique, since $1, \alpha, \ldots, \alpha^{d-1}$ is the basis of $\mathbb{Q}(\alpha)$. In particular, if $\beta = \alpha'$ is conjugate to α over $\mathbb{Q}$, the polynomial R is called the *root polynomial* (see, e.g., [13,15]).

For an algebraic integer α, the answer to Problem 1 is trivial. We record it here only for the sake of completeness.

Lemma 3 *Suppose that α is an algebraic integer. Then, $\beta \in \mathbb{Q}(\alpha)$ belongs to $\mathbb{Z}[\alpha]$ if and only if the canonical representative $R \in \mathbb{Q}[X]$ of β has all integer coefficients, that is, $R \in \mathbb{Z}[X]$ (or, equivalently, $R = G, t = 1$).*

We shall write $U \equiv V \pmod{t}$ for polynomials $U, V \in \mathbb{Z}[X]$ and an integer $t \neq 0$, if all the coefficients of the polynomial $U - V$ are divisible by t.

Theorem 4 *Let α be an algebraic number with minimal polynomial $F \in \mathbb{Z}[X]$. Suppose that $\beta \in \mathbb{Q}(\alpha)$ is canonically represented in $\mathbb{Q}(\alpha)$ by*

$$\beta = R(\alpha) = \frac{G(\alpha)}{t}.$$

Then, $\beta \in \mathbb{Z}[\alpha]$ if and only if the congruence

$$F(X) \cdot H(X) \equiv G(X) \pmod{t} \tag{1}$$

has a solution $H \in \mathbb{Z}[X]$.

Theorem 4 is simple to state (and very simple to prove). Unfortunately, the condition (1) is sometimes very difficult to check. In Sect. 5, below we shall study the congruence (1) in detail and give an algorithm for its solution. This algorithm either gives some solution $H \in \mathbb{Z}[X]$ of (1) or shows that such H does not exist.

Theorem 5 gives a complete description of the set $\mathbb{Z}[\alpha] \cap \mathbb{Q}$. Obviously, $\mathbb{Z} \subseteq \mathbb{Z}[\alpha]$, so we shall only consider rational non-integer numbers.

Theorem 5 *Let*

$$F(X) = a_d X^d + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$$

be the minimal polynomial of an algebraic number α. A rational fraction r/t, where $r \in \mathbb{Z}$, $r \neq 0$, $t \in \mathbb{N}$, $t \geqslant 2$, $\gcd(r, t) = 1$, belongs to the ring $\mathbb{Z}[\alpha]$ if and only if the square-free part of t divides the coefficients a_j for each $j = 1, \ldots, d$ but does not divide a_0.

Recall that the square-free part of a positive integer $n \geqslant 2$ is the product of all distinct prime divisors of n and the square-free part of 1 is 1. Note that for $t \geqslant 2$, no prime divisor of t cannot divide all the coefficients of F in view of $\gcd(a_d, \ldots, a_0) = 1$. Hence, the condition concerning the divisibility of a_0 by the square-free part of t can be removed from Theorem 5 (it is given there only for the sake of clarity).

Note that Theorem 5 settles Problem 2 in the quadratic case:

Corollary 6 *Let*

$$F(X) = aX^2 + bX + c = a(X - \alpha)(X - \alpha'), \quad a \in \mathbb{N},\ b, c \in \mathbb{Z},$$

be irreducible in $\mathbb{Z}[X]$. *Then,* $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha']$ *if and only if the square-free part of a divides b.*

Let α be a cubic algebraic integer with conjugates $\alpha_1 = \alpha, \alpha_2, \alpha_3$. Any relation $\alpha_i \in \mathbb{Z}[\alpha_j]$, where the indices $i \neq j$ are in $\{1, 2, 3\}$, implies that all three rings $\mathbb{Z}[\alpha_1], \mathbb{Z}[\alpha_2], \mathbb{Z}[\alpha_3]$ coincide (see Theorem 11 below). This is possible only if α is a root of an irreducible cubic integer polynomial whose discriminant is a square $\Delta(F) = \ell^2$, $\ell \in \mathbb{Z}$, so that the splitting field of this polynomial has a cyclic Galois group.

In [13] (see also [12]), Girstmair investigated cyclic cubic equations and derived some explicit formulas for the root polynomials that represent α_2 and α_3 in $\mathbb{Q}(\alpha_1)$. More precisely, he showed that if the minimal polynomial of α is given by

$$F(X) = X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{Z}[X]$$

whose splitting field is cyclic, then the root polynomials $R_j \in \mathbb{Q}[X]$, $\alpha_j = R_j(\alpha)$, $j = 2, 3$, are given by

$$R_j(X) = c_{j2}X^2 + c_{j1}X + c_{j0}$$

with

$$\begin{aligned} c_{j2} &= (a_2^2 - 3a_1)/\ell_j, \\ c_{j1} &= (2a_2^3 - 7a_1a_2 + 9a_0)/2\ell_j - 1/2, \\ c_{j0} &= (a_2^2a_1 + 3a_2a_0 - 4a_1^2)/2\ell_j - a_2/2, \end{aligned} \tag{2}$$

where $j = 2, 3$ and $\{\ell_2, \ell_3\} = \{-\ell, \ell\}$, $\ell = \sqrt{\Delta(F)}$ (the choice of the sign depends on the enumeration of the roots α_2, α_3). Combining Lemma 3 with the formulas (2), we immediately obtain the answer to Problem 2 for cubic integer rings.

Corollary 7 *Let*

$$F(X) = X^3 + a_2X^2 + a_1X + a_0 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$$

be an irreducible cubic polynomial in $\mathbb{Z}[X]$ *with discriminant*

$$\Delta(F) = -4a_2^3a_0 + a_2^2a_1^2 + 18a_0a_1a_2 - 4a_1^3 - 27a_0^2.$$

Then,

$$\mathbb{Z}[\alpha_1] = \mathbb{Z}[\alpha_2] = \mathbb{Z}[\alpha_3]$$

if and only if the polynomial $F(X)$ *satisfies the following four conditions:*

1. $\Delta(F) = \ell^2$ *for some* $\ell \in \mathbb{N}$;
2. $\ell \mid a_2^2 - 3a_1$;
3. $2\ell \mid 2a_2^3 - 7a_1a_2 + 9a_0 - \ell$;
4. $2\ell \mid a_2^2a_1 + 3a_2a_0 - 4a_1^2 - a_2\ell$.

Below, we shall also prove the following:

Theorem 8 *Let* K *be a normal extension of* $\mathbb{Q}$ *degree* $d \geqslant 2$. *Then, there exist two algebraic numbers* $\alpha, \alpha' \in K$ *that are conjugate over* $\mathbb{Q}$ *such that* $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha') = K$ *and* $\mathbb{Z}[\alpha] \neq \mathbb{Z}[\alpha']$.

We shall give two independent proofs of Theorem 8. Our original proof is based on the observation that, by a simple linear transformation, every algebraic number can be modified

in such a way that the ring equality does not hold for all of its algebraic conjugates at the same time:

Theorem 9 *Let α be an algebraic number with conjugates $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$, where $d \geqslant 2$. Then, there exist an integer t and a prime number p such that*

$$\mathbb{Z}\left[\frac{\alpha_i + t}{p}\right] \neq \mathbb{Z}\left[\frac{\alpha_j + t}{p}\right]$$

for some indices $i < j$ from the set $\{1, \ldots, d\}$.

An alternative proof of Theorem 8 was supplied by the referee. It is shorter, but involves a bit more of algebraic number theory.

Here is a result in the opposite direction:

Theorem 10 *Let K be a normal extension of $\mathbb{Q}$ of degree $d \geqslant 2$. Then, there exists an algebraic number $\alpha \in K$ with conjugates $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ over $\mathbb{Q}$ such that $\mathbb{Q}(\alpha_j) = K$ for each $j = 1, 2, \ldots, d$ and*

$$\mathbb{Z}[\alpha_1] = \mathbb{Z}[\alpha_2] = \cdots = \mathbb{Z}[\alpha_d].$$

As a side note, we also record the next observation.

Theorem 11 *Let $\alpha_1, \alpha_2, \ldots, \alpha_d$ be distinct conjugate algebraic numbers of degree d. If d is a prime number, then the relation $\alpha_i \in \mathbb{Z}[\alpha_j]$ for some two conjugates α_i, α_j, $i \neq j$, implies*

$$\mathbb{Z}[\alpha_1] = \mathbb{Z}[\alpha_2] = \cdots = \mathbb{Z}[\alpha_d].$$

Furthermore, we show that any two algebraic numbers that generate the same number field can be modified in such a way that the rings that they generate over $\mathbb{Z}$ coincide. This fact will be used in the proof of Theorem 10.

Theorem 12 *Let α and β be two algebraic numbers satisfying $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Then, there exists a nonzero integer m for which the equality*

$$\mathbb{Z}\left[\frac{\alpha}{tm}\right] = \mathbb{Z}\left[\frac{\beta}{tm}\right]$$

holds for every $t \in \mathbb{Z} \setminus \{0\}$.

The proof of Theorem 9 is based on the next criterion.

Lemma 13 *Let $\alpha_1, \alpha_2, \ldots, \alpha_d$ be $d \geqslant 2$ conjugate algebraic numbers with minimal polynomial*

$$F(X) = a_d X^d + \cdots + a_1 X + a_0 \in \mathbb{Z}[X].$$

Suppose that there exists a prime number p such that $p \mid a_0$ and $p \nmid a_1$. Then, $\mathbb{Z}[\alpha_i/p] \neq \mathbb{Z}[\alpha_j/p]$ for some indices $i < j$.

The existence of the parameters p and t in Theorem 9 is guaranteed by the following lemma.

Lemma 14 *Suppose that $F(X) \in \mathbb{Z}[X]$ is non-constant and separable. Then, there exist a prime number p and an integer t such that $p \mid F(t)$, but $p \nmid F'(t)$. Moreover, the set of such pairs (p, t) is infinite.*

In Sect. 3, we shall give some motivating numerical examples. The proofs are given in Sect. 4. Note that in the proof of Theorem 8, we use Theorem 9; in the proof of Theorem 10, we use Theorem 12; and in the proof of Lemma 13, we use Theorem 5.

3 Some numerical examples

Example 15 Consider an algebraic number α with minimal polynomial

$$F(X) = 6X^3 - 6X^2 + 4X + 3.$$

The prime factorization of the leading coefficient is $a_3 = 2 \cdot 3$. The prime $p = 2$ divides a_1, a_2 and does not divide a_0. The prime $p = 3$ divides the coefficients a_2 and a_0, but not a_1. Hence, Theorem 5 implies

$$\mathbb{Z}[\alpha] \cap \mathbb{Q} = \{r/2^m \mid \quad r \in \mathbb{Z}, m \in \mathbb{N} \cup \{0\}\}.$$

Example 16 Let α be the root of

$$F(X) = 5X^4 + 4X^3 + 10X^2 + 5X + 3.$$

Since the greatest common divisor of the first four coefficients of F, namely 5, 4, 10, and 5 equals 1, by Theorem 5, we obtain $\mathbb{Z}[\alpha] \cap \mathbb{Q} = \mathbb{Z}$.

Example 17 Let

$$F(X) = 2X^2 + 2X + 3 = 2(X - \alpha_1)(X - \alpha_2),$$

where

$$\alpha_1 = \frac{-1 + i\sqrt{5}}{2}, \quad \alpha_2 = \frac{-1 - i\sqrt{5}}{2}.$$

Then, Corollary 6 gives $\mathbb{Z}[\alpha_1] = \mathbb{Z}[\alpha_2]$. Analogously, for

$$F(X) = 2X^2 + 3X + 2 = 2(X - \alpha_1)(X - \alpha_2),$$

where

$$\alpha_1 = \frac{-3 + i\sqrt{7}}{4}, \quad \alpha_2 = \frac{-3 - i\sqrt{7}}{4},$$

using Corollary 6 we find that $\mathbb{Z}[\alpha_1] \neq \mathbb{Z}[\alpha_2]$.

Example 18 Consider

$$F(X) = X^3 - 3X - 1 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3).$$

The discriminant of F is $\Delta(F) = 9^2$. Therefore, $K = \mathbb{Q}(\alpha_1)$ is a normal extension of $\mathbb{Q}$. In view of (2), the root polynomials of α_2, α_3 are

$$R_2(X) = X^2 - X - 2, \quad R_3(X) = -X^2 + 2.$$

Since they have integer coefficients, we obtain $\mathbb{Z}[\alpha_1] = \mathbb{Z}[\alpha_2] = \mathbb{Z}[\alpha_3]$.

Example 19 Let $\alpha = \alpha_1$ be a cubic with minimal polynomial

$$F(X) = X^3 + 9X^2 - X - 1 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3).$$

Then, $\Delta(F) = 56^2$; therefore, $\mathbb{Q}(\alpha_1)$ is a normal extension of $\mathbb{Q}$. Consequently, $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2) = \mathbb{Q}(\alpha_3)$. It is easy to see that the polynomial F does not satisfy the condition 2) of Corollary 7. Thus, $\alpha_i \notin \mathbb{Z}[\alpha_j]$, for all $i, j \in \{1, 2, 3\}, i \neq j$, according to Corollary 7 and Theorem 11.

Example 20 Consider a "random" irreducible quartic integer polynomial

$$F(X) = 6X^4 - 4X^2 + 19X + 2$$

with one of the roots α. Assume that three algebraic numbers $\beta, \gamma, \delta \in \mathbb{Q}(\alpha)$ are given by

$$\beta = \frac{40\alpha^3 - 152\alpha^2 + 353\alpha + 74}{36}, \quad \gamma = \frac{12\alpha^3 - 271\alpha^2 + 35\alpha + 2}{10},$$
$$\delta = \frac{6\alpha^3 - 3\alpha^2 + 229\alpha + 4}{12}.$$

We will determine which of the numbers β, γ, δ belong to the ring $\mathbb{Z}[\alpha]$ and which do not. Moreover, in case a number lies in $\mathbb{Z}[\alpha]$, we shall find its representation in the form $T(\alpha)$ with $T \in \mathbb{Z}[X]$. Let us start with β. Evidently, $\beta = G(\alpha)/t$, where

$$G(X) = 40X^3 - 152X^2 + 353X + 74 \quad \text{and} \quad t = 36.$$

Since $\gcd(40, -152, 353, 74, 36) = 1$, $G(X)$ is the numerator polynomial, and t is the denominator of the canonical representation of β. Note that the prime factorization of t is $t = 2^2 \cdot 3^2$. We next use the algorithm from Sect. 5 to check whether β is in $\mathbb{Z}[\alpha]$ or not. For this, by Theorem 4, it suffices either to find $H \in \mathbb{Z}[X]$ satisfying the congruence

$$F \cdot H \equiv G \pmod{36} \tag{3}$$

or to show that no such H as in (3) exists. Firstly, we run Algorithm 23 from Sect. 5 for $p = 2, m = 2$ on MAPLE computer algebra system. The program successfully computes the polynomials

$$H_0(X) = 1, \qquad H_1(X) = 1 + X^3,$$

and the partial sum of the 2-adic representation of $H(X)$

$$S_2(X) = H(0) + 2H_1(X) = 3 + 2X^3.$$

For $p = 3, m = 2$, Algorithm 23 outputs

$$H_0(X) = 1 + 2X, \qquad H_1(X) = X + X^3,$$

so the 3-adic partial sum of $H(X)$ is

$$S_2(X) = H(0) + 3H_1(X) = 1 + 5X + 3X^3.$$

It follows that the congruence (3) has solutions modulo 4 and modulo 9. Hence, by Proposition (21), there exists an integer solution modulo 36, so that $\beta \in \mathbb{Z}[\alpha]$.

One can recover the solution $H(X)$ using the formulas (12) from the proof of Proposition 21. Since $\delta_2(36) = 9$, $\delta_3(36) = 28$, we have

$$\begin{aligned} H(X) &\equiv 9(3 + 2X^3) + 28(1 + 5X + 3X^3) \\ &\equiv 30X^3 + 32X + 19 \pmod{36}. \end{aligned}$$

So the representation of β in $\mathbb{Z}[\alpha]$ is given by the polynomial

$$\begin{aligned} T(X) &= \frac{G(X) - F(X)H(X)}{36} \\ &= 1 - 2X - 19X^2 + 3X^3 - 19X^4 - 2X^5 - 5X^7. \end{aligned}$$

This representation $\beta = T(\alpha)$ is not unique. For instance, $\beta = 1 + \alpha^3 + \alpha^7$ gives another (more simple) representation.

We next prove that $\gamma \notin \mathbb{Z}[\alpha]$ and $\delta \notin \mathbb{Z}[\alpha]$. For this, one can also use the main algorithm. On the other hand, there exists a short proof using Proposition 24. Indeed, the prime $p = 5$ in the denominator of the number γ does not divide the leading coefficient $a_4 = 6$ of the minimal polynomial $F(X)$, so $\gamma \notin \mathbb{Z}[\alpha]$, by Proposition 24. For the number δ, this trick does not work, as all the prime divisors of 12 divide $a_d = 6$. However, the numerator polynomial $G(X) = 6X^3 - 3X^2 + 229X + 4$ reduced modulo 3 to $\overline{G}(X) = X + 1$ is of degree 1, whereas $\overline{F}(x) = 2X^2 + X + 2$ has degree 2, so $\overline{F} \nmid \overline{G}$ in $\mathbb{F}_3[X]$. Hence, $\delta \notin \mathbb{Z}[\alpha]$, according to Proposition 24.

4 Proofs of the main results

Proof of Lemma 3 The proof follows easily from the fact that the collection of powers $1, \alpha, \ldots, \alpha^{d-1}$ is a basis of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ and a basis of $\mathbb{Z}$-module $\mathbb{Z}[\alpha]$ over $\mathbb{Z}$ (see the conditions INT 1 and INT 2 on p. 334 in [16]); thus, the representation of the numbers $\beta \in \mathbb{Z}[\alpha] \cap \mathbb{Q}(\alpha)$ is unique.

Another proof of Lemma 3 can also be derived from Proposition 24 (see the discussion after the proof of Proposition 24). □

Proof of Theorem 4 *Necessity*: Suppose that $\beta \in \mathbb{Z}[\alpha]$. Then, there exists a polynomial $T \in \mathbb{Z}[X]$ such that $\beta = T(\alpha)$. Since $\beta = G(\alpha)/t$, by the representation of β in $\mathbb{Q}(\alpha)$, one has $G(\alpha) - tT(\alpha) = 0$. By the Gauss lemma, there exists $H \in \mathbb{Z}[X]$ such that $G(X) - tT(X) = F(X)H(X)$. Thus, $F(X)H(X) - G(X) = -tT(X)$, and hence, (1) holds with $H \in \mathbb{Z}[X]$.

Sufficiency: Let $H \in \mathbb{Z}[X]$ be a solution to the congruence (1). Then, there exists a polynomial $T \in \mathbb{Z}[X]$ for which $G(X) - F(X)H(X) = tT(X)$. Since $F(\alpha) = 0$, one obtains $G(\alpha) = tT(\alpha)$. Thus, $\beta = G(\alpha)/t = T(\alpha) \in \mathbb{Z}[\alpha]$. □

Proof of Theorem 5 *Necessity:* Suppose that $t \geqslant 2$ and $r \neq 0$ are relatively prime integers and $r/t \in \mathbb{Z}[\alpha]$. Then, there exists a polynomial $G(X) \in \mathbb{Z}[X]$ such that

$$\frac{r}{t} = G(\alpha).$$

Since $tG(\alpha) - r = 0$, the polynomial $tG(X) - r$ is divisible by the minimal polynomial of α, that is, $F(X)$. Thus, for some $H(X) \in \mathbb{Z}[X]$, we have

$$F(X)H(X) = tG(X) - r. \tag{4}$$

Now, fix any prime number p that divides t. Reduction in (4) modulo p gives

$$\overline{F}(X)\overline{H}(X) = -\overline{r},$$

where $\overline{F}, \overline{H} \in \mathbb{F}_p[X]$ and $-\overline{r} \in \mathbb{F}_p$. Hence, $\overline{F}$ and $\overline{H}$ must be constant polynomials. In particular, this implies that all the coefficients $a_1, a_2, \ldots, a_d$ of $F(X)$ are divisible by p. Of course, a_0 must be relatively prime to p, since F is a primitive polynomial.

Sufficiency: Let $r \in \mathbb{Z}$ and $t \in \mathbb{N}$ be as above. Assume that every prime divisor of t divides each coefficient $a_1, a_2, \ldots, a_d$ (clearly, none of them divides a_0). Then, there exists a positive (sufficiently large) integer n such that all the coefficients of the polynomial

$$V(X) = \big(-a_1X - a_2X^2 - \cdots - a_dX^d\big)^n$$

are divisible by t. Note that

$$a_0^n = (a_0 - F(\alpha))^n = V(\alpha). \tag{5}$$

Since $\gcd(a_0^n, t) = 1$, there exist integers $u, v \in \mathbb{Z}$ such that $a_0^n u + tv = 1$. Hence, according to (5),

$$\frac{1}{t} = \frac{a_0^n u + tv}{t} = \frac{u}{t} a_0^n + v = \frac{u}{t} V(\alpha) + v \in \mathbb{Z}[\alpha],$$

because all the coefficients of $V(X)$ are divisible by t. Finally, $1/t \in \mathbb{Z}[\alpha]$ implies $r/t \in \mathbb{Z}[\alpha]$ for every $r \in \mathbb{Z}$. □

Proof of Corollary 6 Observe that $\alpha + \alpha' = -b/a$. Hence, the relations $\alpha' \in \mathbb{Z}[\alpha]$ and $\alpha \in \mathbb{Z}[\alpha']$ both are equivalent to $b/a \in \mathbb{Z}[\alpha]$. There is nothing to prove for $a = 1$. For $a \geqslant 2$, write $a = gt$ and $b = gr$ with $g, t \in \mathbb{N}, r \in \mathbb{Z}$, $\gcd(r, t) = 1$. Note that $\gcd(g, c) = 1$, since F is irreducible in $\mathbb{Z}[X]$. To conclude, it remains to apply Theorem 5 to the fraction $r/t = b/a$ and the polynomial F. □

Proof of Theorem 8 According to the Primitive Element Theorem (see Theorem 4.6 on p. 243 in [16]), there exists a number $\beta \in K$ of degree $d \geqslant 2$ such that $K = \mathbb{Q}(\beta)$. Since K is normal, any algebraic conjugate β' of β also generates K, that is, $K = \mathbb{Q}(\beta')$. By Theorem 9 (whose proof is given below), there exist integers $p > 0$ and t such that

$$\mathbb{Z}\left[\frac{\beta' + t}{p}\right] \neq \mathbb{Z}\left[\frac{\beta'' + t}{p}\right]$$

for some two conjugates $\beta' \neq \beta''$ of β. Selecting $\alpha := (\beta' + t)/p$ and $\alpha' := (\beta'' + t)/p$ we see that α and α' are conjugate algebraic numbers of degree d satisfying $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha') = K$ and $\mathbb{Z}[\alpha] \neq \mathbb{Z}[\alpha']$. □

Alternative proof of Theorem 8 It is well known (see, e.g., Theorem 4.37 in [18]) that for any number field K of degree $d \geqslant 2$, there exist infinitely many primes $p \in \mathbb{Z}$ such that the ideal (p) splits completely in the ring of integers of K, namely

$$(p) = \wp_1 \wp_2 \dots \wp_d,$$

where $\wp_j$, $j = 1, \dots, d$, are d distinct prime ideals. So let p be a prime with such a property. By the Chinese Remainder Theorem, one can find an algebraic integer $\beta = \beta_1 \in \wp_1$ such that $\beta \notin \wp_j$ for $j = 2, \dots, d$. Since K is normal over $\mathbb{Q}$, the ideals $\wp_j$ are all conjugate. Therefore, β has at least d distinct conjugates $\beta_j \in \wp_j$ over $\mathbb{Q}$. It follows that β is of maximal degree in K and so $\mathbb{Q}(\beta) = K$.

Let $\beta' \neq \beta$ be one of these conjugates. Then, $\mathbb{Z}[1/\beta] \neq \mathbb{Z}[1/\beta']$ (in fact, none of these rings is a subring of the other). Indeed, assume that $1/\beta' \in \mathbb{Z}[\beta]$. Then, $1/\beta' = P(1/\beta)$ for some polynomial $P \in \mathbb{Z}[X]$ of degree $n \geqslant 1$, which implies $\beta^n = \beta' \cdot P^*(\beta)$, where $P^*(X) = X^n P(1/X)$. Consequently, β belongs to the same prime ideal $\wp_j$, $j \geqslant 2$, as β' does, in contradiction to the initial choice of p and β. To complete the proof, one takes $\alpha := 1/\beta$. □

Proof of Theorem 9 Let $F(X) = a_d X^d + \dots + a_0 \in \mathbb{Z}[X]$ be the minimal polynomial of α. By Lemma 14, there exists an integer t and a prime number p such that $p | F(-t)$, but $p \nmid F'(-t)$. The constant coefficient of the polynomial $F(X - t)$ (written as the polynomial in X) is $a_0 = F(-t)$ while the coefficient of X is $F'(-t)$. Note that $F(X - t)$ is the minimal polynomial of the number $\alpha + t$. In order to complete the proof, observe that, by Lemma 13, the d rings $\mathbb{Z}[(\alpha_j + t)/p]$, $j = 1, \dots, d$, generated by the algebraic conjugates of $(\alpha + t)/p$ cannot all be equal. □

Proof of Theorem 10 By the Primitive Element Theorem, there exists $\beta \in K$ such that $K = \mathbb{Q}(\beta)$. Let $\beta_1 = \beta, \beta_2, \ldots, \beta_d$ be all the conjugates of β over $\mathbb{Q}$. Since K is a normal extension of $\mathbb{Q}$, for each $j = 1, 2, \ldots, d$ we must have $K = \mathbb{Q}(\beta_j)$. On applying Theorem 12 (whose proof is given below) to β_1 and β_j, where $j = 2, 3, \ldots, d$, we get some nonzero integers $m_2, m_3, \ldots, m_d$ such that equality

$$\mathbb{Z}\left[\frac{\beta_1}{m_j t_j}\right] = \mathbb{Z}\left[\frac{\beta_j}{m_j t_j}\right] \tag{6}$$

holds for every $t_j \in \mathbb{Z} \setminus \{0\}$. Now fix $j \in \{2, 3, \ldots, d\}$. Choosing

$$t_j = \frac{m_2 \cdot m_3 \cdot \cdots \cdot m_d}{m_j} \in \mathbb{Z}$$

in (6), we obtain

$$\mathbb{Z}\left[\frac{\beta_1}{m}\right] = \mathbb{Z}\left[\frac{\beta_j}{m}\right]$$

for each $j = 2, \ldots, d$, where $m := m_2 \cdots \cdots m_d$. It is now evident that the algebraic conjugates of the number $\alpha := \beta_1/m$ have all required properties. □

Proof of Theorem 11 Set $\alpha := \alpha_i$ and $p := d$, where p is a prime. Let $\mathcal{G}$ be the Galois group of the normal closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Observe that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$; hence, p divides the order of $\mathcal{G}$. By Cauchy's theorem, $\mathcal{G}$ contains an element of order p, say τ. Now, consider $\mathcal{G}$ as the group of permutations of the set $\mathcal{S} := \{\alpha_1, \ldots, \alpha_d\}$. Since τ is of the order p, it must be a p-cycle. Hence, there exists $k \in \mathbb{N}$, where $1 \leqslant k \leqslant p-1$, such that $\tau^k \alpha_i = \alpha_j$. Put $\sigma := \tau^k$. Since k and p are relatively prime, σ is a p-cycle too. Note that $\alpha_i \in \mathbb{Z}[\alpha_j]$ implies that $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha_i] \subseteq \mathbb{Z}[\alpha_j] = \mathbb{Z}[\sigma\alpha]$. A repeated application of σ on the relation $\mathbb{Z}[\alpha] \subseteq \mathbb{Z}[\sigma\alpha]$ yields

$$\mathbb{Z}[\alpha] \subseteq \mathbb{Z}[\sigma\alpha] \subseteq \mathbb{Z}[\sigma^2\alpha] \subseteq \cdots \subseteq \mathbb{Z}[\sigma^{p-1}\alpha] \subseteq \mathbb{Z}[\sigma^p\alpha] = \mathbb{Z}[\alpha]. \tag{7}$$

Since σ is a p-cycle on $\mathcal{S}$, one has $\{\alpha, \sigma\alpha, \ldots, \sigma^{p-1}\alpha\} = \mathcal{S}$. Hence, by (7), we conclude that $\mathbb{Z}[\alpha_1] = \mathbb{Z}[\alpha_2] = \cdots = \mathbb{Z}[\alpha_d]$. □

Proof of Theorem 12 Let d be the degree of α over $\mathbb{Q}$. Since $\beta \in \mathbb{Q}(\alpha)$, we have $\beta/\alpha^2 \in \mathbb{Q}(\alpha)$. Hence, there exists a numerator polynomial $G(X) = g_0 + g_1 X + \cdots + g_{d-1}X^{d-1} \in \mathbb{Z}[X]$ such that

$$\frac{\beta}{\alpha^2} = \frac{g_0 + g_1\alpha + \cdots + g_{d-1}\alpha^{d-1}}{m_1}$$

for some denominator $m_1 \in \mathbb{N}$. Multiplying by both sides α^2, we get

$$\beta = \frac{g_0\alpha^2 + g_1\alpha^3 + \cdots + g_{d-1}\alpha^{d+1}}{m_1}.$$

Hence, for any $s \in \mathbb{Z} \setminus \{0\}$, the equality

$$\beta = g_0 m_1 s^2 \left(\frac{\alpha}{m_1 s}\right)^2 + g_1(m_1^2 s^3)\left(\frac{\alpha}{m_1 s}\right)^3 + \cdots + g_{d-1}(m_1^d s^{d+1})\left(\frac{\alpha}{m_1 s}\right)^{d+1}$$

holds. Writing the latter equality in the form

$$\frac{\beta}{m_1 s} = g_0 s \left(\frac{\alpha}{m_1 s}\right)^2 + g_1(m_1 s^2)\left(\frac{\alpha}{m_1 s}\right)^3 + \cdots + g_{d-1}(m_1^{d-1} s^d)\left(\frac{\alpha}{m_1 s}\right)^{d+1},$$

we obtain

$$\mathbb{Z}\left[\frac{\beta}{m_1 s}\right] \subseteq \mathbb{Z}\left[\frac{\alpha}{m_1 s}\right] \quad \text{for every } s \in \mathbb{Z} \setminus \{0\}. \tag{8}$$

Analogously, by interchanging α with β, there exists a nonzero integer m_2 such that

$$\mathbb{Z}\left[\frac{\alpha}{m_2 s}\right] \subseteq \mathbb{Z}\left[\frac{\beta}{m_2 s}\right] \quad \text{for every } s \in \mathbb{Z} \setminus \{0\}. \tag{9}$$

Substituting $s = m_2 t$ into (8) and $s = m_1 t$ into (9), we find that

$$\mathbb{Z}\left[\frac{\beta}{m_1 m_2 t}\right] \subseteq \mathbb{Z}\left[\frac{\alpha}{m_1 m_2 t}\right]$$

and

$$\mathbb{Z}\left[\frac{\alpha}{m_1 m_2 t}\right] \subseteq \mathbb{Z}\left[\frac{\beta}{m_1 m_2 t}\right]$$

for every $t \in \mathbb{Z} \setminus \{0\}$. Hence,

$$\mathbb{Z}\left[\frac{\alpha}{tm}\right] = \mathbb{Z}\left[\frac{\beta}{tm}\right]$$

for $m := m_1 m_2$ and every $t \in \mathbb{Z} \setminus \{0\}$. □

Proof of Lemma 13 Assume the contrary,

$$\mathbb{Z}\left[\frac{\alpha_1}{p}\right] = \mathbb{Z}\left[\frac{\alpha_2}{p}\right] = \cdots = \mathbb{Z}\left[\frac{\alpha_d}{p}\right],$$

where $\alpha_1 = \alpha$. Then,

$$\frac{a_0}{a_d p^{d-1}\alpha} = (-1)^d \frac{\alpha_2}{p} \cdot \frac{\alpha_3}{p} \cdot \cdots \cdot \frac{\alpha_d}{p} \in \mathbb{Z}\left[\frac{\alpha}{p}\right].$$

Similarly, $a_0/a_d p^{d-1}\alpha_j \in \mathbb{Z}[\alpha_j/p] = \mathbb{Z}[\alpha/p]$ for each $j = 1, \ldots, d$. Hence,

$$\text{Trace}\left(\frac{a_0}{a_d\, p^{d-1}\alpha}\right) = \frac{a_0}{a_d p^{d-1}} \text{Trace}\left(\frac{1}{\alpha}\right) = -\frac{a_1}{a_d\, p^{d-1}} \in \mathbb{Z}\left[\frac{\alpha}{p}\right],$$

since the minimal polynomial of $1/\alpha$ is $\pm X^d F(1/X)$ (the trace denotes the sum of the conjugates of an algebraic number). From $p \nmid a_1$, we see that p divides the denominator of the nonzero fraction $-a_1/a_d p^{d-1}$. By Theorem 5, the prime p must divide all the coefficients of the minimal polynomial of α/p except for the constant coefficient. Since $p|a_0$, α/p is the root of the irreducible polynomial

$$p^{d-1} a_d X^d + p^{d-2} a_{d-1} X^{d-1} + \cdots + a_1 X + \frac{a_0}{p} \in \mathbb{Z}[X]$$

whose coefficient a_1 is not divisible by p, a contradiction. □

Proof of Lemma 14 The greatest common divisor of $F(X)$ and $F'(X)$ in $\mathbb{Q}[X]$ is 1, because $F(X)$ is separable and has a positive degree. By the Euclidean algorithm, there exists polynomials $U, V \in \mathbb{Z}[X]$ and a nonzero integer a such that

$$U(X)F(X) + V(X)F'(X) = a. \tag{10}$$

Suppose that for some prime number $p > a$ and an integer t, we have $p \mid F(t)$. Substituting $x = t$ into (10), we obtain $U(t)F(t) + V(t)F'(t) = a$. Then, $p \nmid F'(t)$, since otherwise $p|a$ which contradicts to $p > a$. Since for any non-constant integer polynomial $F \in \mathbb{Z}[X]$, the set of distinct prime divisors of the integers $F(t), t \in \mathbb{Z}$, is infinite (see, e.g., Theorem 1 in [11] or Exercise 1.2.5 and its solution in [17]), there are infinitely many primes p and integers t such that $p \mid F(t)$ and $p \nmid F'(t)$. □

5 Main algorithm

For a given integer $t \neq 0$, let $v_p(t)$ be the power of the prime number p in the factorization of t, namely the largest integer m for which $p^m \mid t$ and $p^{m+1} \nmid t$. A finite field of integer residue classes modulo p is denoted by $\mathbb{F}_p$. Let $\overline{U}$ be a polynomial in $\mathbb{F}_p[X]$, obtained by reducing the coefficients of $U \in \mathbb{Z}[X]$ modulo p. We will also make some use of the p-adic representation of integers (one may consult, for instance, Chapter 13 of [22] as a reference).

A standard strategy of solving congruences modulo an integer is to factor this integer into prime powers and solve the congruence for those prime powers first. The solution is then recovered by using the Chinese remainder theorem. This is described in the next proposition.

Proposition 21 *Let $F, G \in \mathbb{Z}[X], t \in \mathbb{N}$ be the same as in Theorem 4. Then, the congruence (1) of Theorem 4 has a solution $H \in \mathbb{Z}[X]$ if and only if for each prime $p \mid t$, the congruence*

$$F(X) \cdot H(X) \equiv G(X) \pmod{p^{v_p(t)}} \tag{11}$$

has a solution $H = H_p \in \mathbb{Z}[X]$. (The solutions $H_p(X)$ do not need to be the same for different primes p).

Proof of Proposition 21 The necessity is trivial, so we only need to prove the sufficiency. By the Chinese remainder theorem, for each prime $p \mid t$, there exists an integer $\delta_p(t)$ such that

$$\begin{cases} \delta_p(t) \equiv 1 \pmod{p^{v_p(t)}}, \\ \delta_p(t) \equiv 0 \pmod{q^{v_q(t)}} \quad \text{if } q \mid t,\ q - \text{prime},\ q \neq p. \end{cases}$$

Define

$$H(X) := \sum_{p|t,\ p\ -prime} \delta_p(t) H_p(X). \tag{12}$$

Since $H \equiv H_p \pmod{p^{v_p(t)}}$ for each $p \mid t$, by (11), the coefficients of the polynomial $F \cdot H - G$ are all divisible by t. Hence, the polynomial H defined in (12) is a solution of the congruence (1).

In view of Proposition 21, one needs a practical algorithm for solving polynomial congruences modulo a fixed prime power p^m, where $m \in \mathbb{N}$. For $m = 1$, solving the congruence $F \cdot H \equiv G \pmod{p}$ is equivalent to checking if the polynomial G, reduced modulo p to the polynomial $\overline{G}$, is divisible by $\overline{F}$ in $\mathbb{F}_p[X]$, which is simply the polynomial F reduced modulo p. We record this observation as follows:

Proposition 22 *Let $t \in \mathbb{N}$ be square-free, and let α be an algebraic number with minimal polynomial $F \in \mathbb{Z}[X]$. Then, an element $\beta \in \mathbb{Q}(\alpha)$ canonically represented as $\beta = G(\alpha)/t$ belongs to $\mathbb{Z}[\alpha]$ if and only if for each prime $p \mid t$, the polynomial $\overline{F}$ divides the polynomial $\overline{G}$ in $\mathbb{F}_p[X]$.*

For higher prime powers p^m, $m \geqslant 2$, the p-adic notation is useful. Observe that one can write any polynomial $H \in \mathbb{Z}[X]$ in the p-adic form

$$H(X) = H_0(X) + pH_1(X) + \cdots + p^m H_m(X) + \cdots, \tag{13}$$

where the polynomials $H_k \in \mathbb{Z}[X]$ are of degree at most $\deg H$. The form (13) can be obtained by using the p-adic expansion for integer coefficients of H. To ensure that polynomials H_k in (13) are unique, we require that all polynomials H_k have coefficients in the set $\{0, 1, \ldots, p-1\}$. Observe that the expression (13) is infinite if some coefficients of the polynomial H are negative. This is because all negative integers have infinite p-adic expansions.

Next, for the polynomial $H \in \mathbb{Z}[X]$ in the form (13), we define its partial sums $S_k(X)$ by the formula

$$S_k(X) := \sum_{j=0}^{k-1} p^j H_j(X). \tag{14}$$

Observe that $H(X) \equiv S_k(X) \pmod{p^k}$. To solve (11), one can use the following algorithm.

Algorithm 23 *Solves the congruence* $F(X) \cdot H(X) \equiv G(X) \pmod{p^m}$.

Input: *Polynomials* $F, G \in \mathbb{Z}[X]$, *a prime number* p, *a positive integer* m.
Output: *A solution* $H \in \mathbb{Z}[X]$ *of* $F(X) \cdot H(X) \equiv G(X) \pmod{p^m}$ *or* $\varnothing$ *if such* H *does not exist.*
Variables: *Polynomials* $H_k \in \mathbb{Z}[X]$.
Partial sums $S_k \in \mathbb{Z}[X]$.
Auxiliary polynomials $W_k \in \mathbb{Z}[X]$.
Step number k.

Initialization: *set* $S_0 := 0$, $k := 0$,
calculate the reduction of $\overline{F} \in \mathbb{F}_p[X]$ *of* F *modulo* p.
Step $k \geqslant 0$*:* *while* $k \leqslant m$ *do*
calculate $W_k := (G - S_k \cdot F)/p^k$
reduce W_k *modulo* p *to a polynomial* $\overline{W}_k \in \mathbb{F}_p[X]$
check whether $\overline{W}_k$ *is divisible by* $\overline{F}$ *in* $\mathbb{F}_p[X]$
if $\overline{F} \mid \overline{W}_k$
then
calculate $\overline{H}_k := \overline{W}_k/\overline{F}$
define $H_k \in \mathbb{Z}[X]$ *to be the polynomial with coefficients in the set* $\{0, 1, \ldots p-1\}$ *whose reduction modulo* p *coincides with* $\overline{H}_k$
set $S_{k+1} := p^k H_k + S_k$
increase $k := k + 1$
else
end do.
end do.
Last step: *if* $k < m$, *then output* $\varnothing$
else output the solution $H := S_k$.

We will now prove the correctness of Algorithm 23.

Proposition 23 *If the congruence* $F(X)H(X) \equiv G(X) \pmod{p^m}$ *is solvable, then Algorithm 23 always finds one of its solutions* $H \in \mathbb{Z}[X]$. *If the congruence* $F(X)H(X) \equiv G(X) \pmod{p^m}$ *is insolvable, then Algorithm 23 will determine that there are no solutions.*

Proof of Proposition 24 First, suppose that the congruence has at least one solution $H \in \mathbb{Z}[X]$. Write H in the p-adic form (13) and consider the partial sums S_k defined in (14). We claim that Algorithm 23 calculates the partial sums S_{k+1} of the p-adic form (13). To see this, we use the induction on k. Indeed, for $k = 0$, the polynomial $S_1 = H_0$ coincides with the one calculated by Algorithm 23, since the solution to the congruence $F \cdot H \equiv G \pmod{p}$ is unique modulo p, and all the coefficients of the polynomial H_0 belong to the set $\{0, 1, \ldots, p-1\}$. Assume now that the claim is true for some $k \geqslant 0$. Since $H \equiv S_{k+1} \pmod{p^{k+1}}$ for $k = 0, 1, \ldots, m-1$, each partial sum S_{k+1} satisfies the congruence $F \cdot S_{k+1} \equiv G \pmod{p^{k+1}}$. Write

$$S_{k+1} = p^k H_k + S_k. \tag{15}$$

Then,

$$F \cdot \left(p^k H_k + S_k\right) \equiv G \pmod{p^{k+1}}, \tag{16}$$

which is equivalent to

$$p^k F H_k \equiv G - F \cdot S_k \pmod{p^{k+1}}. \tag{17}$$

Since S_k is a solution to $F \cdot S_k \equiv G \pmod{p^k}$, the polynomial

$$W_k = \frac{G - F S_k}{p^k} \tag{18}$$

has all integer coefficients. Therefore, the congruence (17) is equivalent to

$$F H_k \equiv W_k \pmod{p}. \tag{19}$$

Note that the congruence (19) is equivalent to the fact that the polynomial F, reduced modulo p, divides the polynomial W_k in $\mathbb{F}_p$. The polynomials H_k have all the coefficients in the set $\{0, 1, \ldots, p-1\}$. Therefore, by (19), the polynomial H_k, reduced modulo p, coincides with the polynomial $\overline{W}_k / \overline{F} \in \mathbb{F}_p[X]$. By the induction hypothesis, the partial sum S_k coincides with the polynomial computed by Algorithm 23. Thus, the polynomials W_k, H_k, and S_{k+1} also coincide with respective polynomials calculated by Algorithm 23. This concludes the induction step and proves the first statement of Proposition 23. To prove the second assertion, note that polynomials S_{k+1}, calculated at the k-th iteration of Algorithm 23, satisfy

$$F \cdot S_{k+1} \equiv G \pmod{p^{k+1}}. \tag{20}$$

This is easily proved by induction on k as in the first part of Proposition 23. Indeed, for $k = 0$, observe that the polynomial S_1 solves the congruence $F \cdot S_1 \equiv G \pmod{p}$. Suppose that this is true for some $k \geqslant 0$ and consider the polynomial S_{k+1} calculated by Algorithm 23. By the induction hypothesis, one has $F \cdot S_k \equiv G \pmod{p^k}$, so that the coefficients of the polynomial W_k in (18) are all integers. The condition $\overline{F} \mid \overline{W}_k$ in $\mathbb{F}_p[X]$ implies that (19) holds. Observe that (18) and (19) together imply (17). This proves $F \cdot S_{k+1} \equiv G \pmod{p^{k+1}}$ via (15), (16) and completes the induction. If the congruence $F \cdot H \equiv G \pmod{p^m}$ has no solutions, the above argument implies that Algorithm 23 will stop at some step $k < m - 1$, since the congruence (20) has no solutions. The proof of Proposition 23 is completed.

We finish Sect. 5 by recording an observation that has some practical applications to Problem 1.

Proposition 24 *Let α be an algebraic number of degree $d \geqslant 2$ with minimal polynomial $F \in \mathbb{Z}[X]$ whose leading coefficient is a_d. Suppose that $\beta \in \mathbb{Q}(\alpha)$ is canonically represented by $\beta = G(\alpha)/t$, and suppose that a prime number p divides t. Then, $\beta \in \mathbb{Z}[\alpha]$ implies $p|a_d$. Moreover, the degree of the polynomial $\overline{F}$ is smaller than or equal to the degree of $\overline{G}$ in $\mathbb{F}_p[X]$.*

Proof of Proposition 25 According to Theorem 4 and Proposition 21, $\beta \in \mathbb{Z}[\alpha]$ implies that $F \cdot H \equiv G \pmod{p}$ for some polynomial $H \in \mathbb{Z}[X]$. This occurs if $\overline{F} \mid \overline{G}$ in $\mathbb{F}_p[X]$. Hence, the degree of $\overline{F}$ is smaller than or equal to the degree of $\overline{G}$. Since G is the numerator polynomial of the canonical representation of β in $\mathbb{Q}(\alpha)$, the degree of G is at most $d-1$, so the degree of $\overline{F}$ cannot exceed $d-1$ too. This yields $p \mid a_d$. □

Proposition 24 can be used to give an alternative proof of Lemma 3. Indeed, if α is an algebraic integer, then the leading coefficient a_d of its minimal polynomial is 1, so $t = 1$ and the canonical representing polynomial of each $\beta \in \mathbb{Z}[\alpha]$ must have integer coefficients.

One can also derive Theorem 5 as a corollary of Proposition 22 and Proposition 24. The necessary condition for $r/t \in \mathbb{Z}[\alpha]$ follows easily from Proposition 24, by observing that $1/p \in \mathbb{Z}[\alpha]$ for each prime $p \mid t$ implies $r/t \in \mathbb{Z}[\alpha]$. To prove the sufficiency, note that every polynomial $\overline{F} \neq 0$ of degree zero in $\mathbb{F}_p[X]$ divides all polynomials in $\mathbb{F}_p[X]$ and then apply Proposition 22.

Acknowledgments We thank the anonymous referee for the alternative Proof of Theorem 8. This research was supported by the Research Council of Lithuania Grant No. MIP-068/2013/LSS-110000-740.

References

1. Akiyama, S., Barat, G., Berthé, V., Siegel, A.: Boundary for central tiles associated with Pisot beta-numeration and purely periodic expansions. Monatsh. Math. **155**, 377–419 (2008)
2. Akiyama, S., Drungilas, P., Jankauskas, J.: Height reducing problems on algebraic integers. Funct. Approx. Comment. Math. **47**, 105–119 (2012)
3. Akiyama, S., Komornik, V.: Discrete spectra and Pisot numbers. J. Number Theory **133**, 375–390 (2013)
4. Akiyama, S., Zaimi T.: Comments of the height reducing property. Centr. Eur. J. Math. **11**, 1616–1627 (2013)
5. Bertrand, A.: Développements en base de Pisot et répartition modulo 1. C.R. Acad. Sci. Paris Sér. A **285**, 419–421 (1977)
6. Brown, G., Yin, Q.: β-transformation, natural extension and invariant measure. Ergod. Theory Dyn. Syst. **20**, 1271–1285 (2000)
7. Boyd, D.W.: On the beta expansion for Salem numbers of degree 6. Math. Comp. **65**, 861–875 (1996)
8. Fan, Q., Wang, S., Zhang, L.: Recurrence in β-expansion over formal Laurent series. Monatsh. Math. **166**, 379–394 (2012)
9. Feng, D.-J., Sidorov, N.: Growth rate for beta-expansions. Monatsh. Math. **162**, 41–60 (2011)
10. Frougny, C., Solomyak, B.: Finite beta-expansions. Ergod. Theory Dyn. Syst. **12**, 713–723 (1992)
11. Gerst, I., Brillhart, J.: On the prime divisors of polynomials. Am. Math. Mon. **78**, 250–266 (1971)
12. Girstmair, K.: Über konstruktive Methoden der Galoistheorie. Manuscr. Math. **26**, 423–441 (1979)
13. Girstmair, K.: On root polynomials of cyclic cubic equations. Arch. Math. **36**, 313–326 (1981)
14. Hollander, M.: Linear numeration systems, finite beta expansions, and discrete spectrum of substitution dynamical systems. Ph.D. Thesis, University of Washington (1996)
15. Kleiman, H.: Methods for uniquely determining Galois polynomials and related theorems. Monatsh. Math. **73**, 63–68 (1969)
16. Lang, S.: Algebra, 3rd ed., Graduate Texts in Mathematics, vol. 211. Springer, New York (2002)
17. Murty, M.R., Esmonde, J.: Problems in Algebraic Number Theory, 2nd ed., Graduate Texts in Mathematics, vol. 190. Springer, New York (2005)

18. Narkiewicz, W.: Elementary and Analytic Theory of Algebraic Numbers, 3rd edn. Springer, Berlin (2004)
19. Parry, W.: On the β-expansions of real numbers. Acta Math. Acad. Sci. Hung. **11**, 401–416 (1960)
20. Rényi, A.: Representations for real numbers and their ergodic properties. Acta Math. Acad. Sci. Hung. **8**, 477–493 (1957)
21. Schmidt, K.: On periodic expansions of Pisot numbers and Salem numbers. Bull. Lond. Math. Soc. **12**, 269–278 (1980)
22. Steuding, J.: Diophantine Analysis, Discrete Mathematics and its Applications Series. Chapman & Hall, CRC Press, Boca Raton (2005)