Generalized Modular Congruence over Algebraic Numbers

Mohammad Asfaque, Dr. Wagner

July 2025

Introduction

Modular arithmetic has played a foundational role in number theory [1], particularly in understanding congruences over the integers. In this paper, we propose a novel theory of *generalized modular congruence* for algebraic numbers, grounded in the use of primitive polynomials over $\mathbb{Z}[x]$. We define modular solution sets as the roots of the reduced primitive polynomial modulo an integer $k > 1$, and classify algebraic numbers into two types (A and B) based on the nature of these roots.

Using this framework, we construct *modular obstruction theorems* to show when certain exponential Diophantine equations cannot be satisfied. We also develop an algebraic generalization of the classical digital root function, by interpreting it as a modular reduction of the number's defining primitive polynomial modulo 9. This leads to a unified way to compute digital roots of integers, terminating fractions, and even certain irrational algebraic numbers, all within the same modular structure.

Throughout, we provide concrete examples, congruence classifications modulo both prime and composite integers, and connections to classical theorems, identities and digit-based number properties.

1 Generalized Modular Congruence

Definition 1 (Primitive Polynomial)**.** *Let α be an algebraic number. The* primitive polynomial *$f_\alpha(x) \in \mathbb{Z}[x]$ is the unique irreducible polynomial with integer coefficients such that $f_\alpha(\alpha) = 0$, the greatest common divisor of its coefficients is 1, and the leading coefficient is positive. We are choosing the leading coefficients to be positive because it ensures that the primitive polynomial is uniquely defined (not just up to sign). See [2] for a thorough treatment of primitive and irreducible polynomials over integer rings.*

Definition 2 (Modular Solution Set)**.** *Given an integer $k > 1$, define the solution set of α modulo k as:*

$$Sol_k(\alpha) := \{a \in \mathbb{Z}_k : f_\alpha(a) \equiv 0 \mod k\}.$$

If no such $a \in \mathbb{Z}_k$ satisfies this condition, then the solution set is defined to be the empty set.

Definition 3 (Generalized Modular Congruence)**.** *Let α and β be algebraic numbers with primitive polynomials f_α and f_β. We define:*

$$\alpha \equiv^* \beta \mod k \quad \textit{if} \quad \mathit{Sol}_k(\alpha) = \mathit{Sol}_k(\beta).$$

This defines an equivalence relation on algebraic numbers modulo k.

Remark 1. *We classify algebraic numbers modulo k into:*

- ***Type A:*** *Numbers whose $\mathit{Sol}_k(\alpha)$ is nonempty and whose solution set contains no element $a \in \mathbb{Z}_k$ such that $a = 0$ or $\gcd(a, k) > 1$.*
- ***Type B:*** *All others.*

Type A numbers are suitable for modular obstruction arguments, which we will discuss later in the paper.

2 Well-Definedness of Generalized Modular Congruence

We show that if two algebraic numbers share the same primitive polynomial, then their modular solution set is uniquely determined by reducing the polynomial modulo k.

Theorem 1 (Well-Definedness)**.** *The equivalence $\alpha \equiv^* \beta \mod k$ is well defined: if $\alpha = \beta$, then $\mathit{Sol}_k(\alpha) = \mathit{Sol}_k(\beta)$.*

Proof. Assume, for contradiction, that $\alpha = \beta$ but $\mathrm{Sol}_k(\alpha) \neq \mathrm{Sol}_k(\beta)$. Since $\alpha = \beta$, we consider their primitive polynomials. Although a primitive polynomial is only unique up to sign, we have fixed the convention that the leading coefficient must be positive, which ensures that $f_\alpha(x) = f_\beta(x) \in \mathbb{Z}[x]$. Let $f(x) := f_\alpha(x)$.

By definition, the modular solution set $\mathrm{Sol}_k(\alpha)$ consists of all elements $a \in \mathbb{Z}_k$ such that $f(a) \equiv 0 \mod k$. Similarly, $\mathrm{Sol}_k(\beta)$ is the same set because it is defined using the same polynomial $f(x)$. The reduction of a fixed integer polynomial modulo an integer k yields a unique polynomial in $\mathbb{Z}_k[x]$, and the set of roots of that polynomial in $\mathbb{Z}_k$ is uniquely determined [2].

Therefore, $\mathrm{Sol}_k(\alpha) = \mathrm{Sol}_k(\beta)$, contradicting our assumption. Hence, the equivalence $\alpha \equiv^* \beta \mod k$ is well defined when $\alpha = \beta$. $\square$

Example 1. *Let $\alpha = \sqrt{7}$. Then $f_\alpha(x) = x^2 - 7$. Modulo 9, we solve:*

$$x^2 - 7 \equiv 0 \mod 9 \Rightarrow x^2 \equiv 7 \mod 9.$$

The solutions are $x \equiv 4, 5 \mod 9$. So $\mathit{Sol}_9(\sqrt{7}) = \{4, 5\}$.

Example 2. *Let* $\beta = \sqrt{34}$*. Then* $f_\beta(x) = x^2 - 34$*. Modulo 9, we solve:*

$$x^2 \equiv 34 \equiv 7 \mod 9 \Rightarrow x^2 \equiv 7 \mod 9.$$

Again, solutions are 4 and 5, so $Sol_9(\sqrt{34}) = \{4, 5\}$*. Thus,*

$$\sqrt{7} \equiv^* \sqrt{34} \mod 9.$$

We will next explore some concrete and non-trivial examples of algebraic numbers categorized by their generalized modular solution sets.

3 Congruence Classes Mod 3

We will look at a few examples of Type A numbers for modulo 3. Type A because we will use them in modular obstruction theorems later. The possible congruence classes over $\mathbb{Z}_3$ are the subsets:

$$\{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}, \varnothing$$

Among these, the sets $\{1\}, \{2\}, \{1,2\}$ are classified as type A, as they are nonempty and do not include 0.

Examples from Congruence Class {1}

Example: $\alpha = \sqrt[7]{2 + \sqrt[5]{2}}$

Let:

$$x^7 = 2 + \sqrt[5]{2} \Rightarrow (x^7 - 2)^5 = \sqrt[5]{2}^5 = 2$$
$$\Rightarrow (x^7 - 2)^5 - 2 = 0$$

Expanding the left-hand side using the binomial theorem:

$$(x^7 - 2)^5 = x^{35} - 10x^{28} \cdot 2 + 40x^{21} \cdot 4 - 80x^{14} \cdot 8 + 80x^7 \cdot 16 - 32$$
$$= x^{35} - 20x^{28} + 160x^{21} - 640x^{14} + 1280x^7 - 32$$
$$\Rightarrow f(x) = x^{35} - 20x^{28} + 160x^{21} - 640x^{14} + 1280x^7 - 34$$

Reduce modulo 3:

$$f(x) \equiv x^{35} + x^{28} + 1x^{21} + 2x^{14} + 2x^7 + 2 \mod 3$$

Check values in $\mathbb{Z}_3$:

$$f(0) \equiv 2 \mod 3$$
$$f(1) \equiv 1 + 1 + 1 + 2 + 2 + 2 = 9 \equiv 0 \mod 3$$
$$f(2) \equiv 2 + 1 + 2 + 2 + 1 + 2 = 10 \equiv 1 \mod 3$$

Thus, $\mathrm{Sol}_3(\alpha) = \{1\}$, placing this algebraic number in class $\{1\}$.

Example: $\beta = \sqrt[7]{2 + \sqrt[3]{5}}$

To find its primitive polynomial, define:

$$x^7 = 2 + \sqrt[3]{5} \Rightarrow (x^7 - 2)^3 = \sqrt[3]{5}^3 = 5$$
$$\Rightarrow (x^7 - 2)^3 - 5 = 0$$

Expanding the left-hand side:

$$(x^7 - 2)^3 = x^{21} - 6x^{14} + 12x^7 - 8 \Rightarrow f(x) = x^{21} - 6x^{14} + 12x^7 - 13$$

Reduce modulo 3:

$$f(x) \equiv x^{21} + 0x^{14} + 0x^7 + 2 = x^{21} + 2 \mod 3$$

Check values in $\mathbb{Z}_3$:

$$f(0) \equiv 2 \mod 3$$
$$f(1) \equiv 1 + 2 = 3 \equiv 0 \mod 3$$
$$f(2) \equiv 2 + 2 = 4 \equiv 1 \mod 3$$

So $\mathrm{Sol}_3(\beta) = \{1\}$, placing this algebraic number in class $\{1\}$.

Examples from Congruence Class {2}

Example: $\gamma = \sqrt[5]{1 + \sqrt[3]{7}}$

Let:

$$x^5 = 1 + \sqrt[3]{7} \Rightarrow (x^5 - 1)^3 = \sqrt[3]{7}^3 = 7$$
$$\Rightarrow (x^5 - 1)^3 - 7 = 0$$

Expanding:

$$(x^5 - 1)^3 = x^{15} - 3x^{10} + 3x^5 - 1 \Rightarrow f(x) = x^{15} - 3x^{10} + 3x^5 - 8$$

Reduce modulo 3:

$$f(x) \equiv x^{15} + 0x^{10} + 0x^5 + 1 = x^{15} + 1 \mod 3$$

Check values:

$$f(0) \equiv 1 \mod 3$$
$$f(1) \equiv 1 + 1 = 2 \mod 3$$
$$f(2) \equiv 2 + 1 = 3 \equiv 0 \mod 3$$

So $\mathrm{Sol}_3(\gamma) = \{2\}$, so this belongs to class $\{2\}$.

Example: $\delta = \sqrt[7]{6 + \sqrt[3]{5}}$

Let:

$$x^7 = 6 + \sqrt[3]{5} \Rightarrow (x^7 - 6)^3 = 5 \Rightarrow (x^7 - 6)^3 - 5 = 0$$

Expand:

$$(x^7 - 6)^3 = x^{21} - 18x^{14} + 108x^7 - 216 \Rightarrow f(x) = x^{21} - 18x^{14} + 108x^7 - 221$$

Reduce modulo 3:

$$f(x) \equiv x^{21} + 0x^{14} + 0x^7 + 2 = x^{21} + 1 \mod 3$$

Test:

$$\begin{aligned} f(0) &\equiv 1 \mod 3 \\ f(1) &\equiv 1 + 1 = 2 \equiv 2 \mod 3 \\ f(2) &\equiv 2 + 1 = 3 \equiv 0 \mod 3 \end{aligned}$$

So $\mathrm{Sol}_3(\delta) = \{2\}$, so this belongs to class $\{2\}$.

Examples from Congruence Class {1,2}

Example: $\epsilon = 1 + \sqrt[3]{8 - \sqrt{19}}$

We use its primitive polynomial:

$$f(x) = x^6 - 6x^5 + 21x^4 - 60x^3 + 117x^2 - 162x + 62$$

Reduce modulo 3:

$$f(x) \equiv x^6 + 0x^5 + 0x^4 + 0x^3 + 0x^2 + 0x + 2 = x^6 + 2 \mod 3$$

Test:

$$\begin{aligned} f(0) &\equiv 2 \mod 3 \\ f(1) &\equiv 1 + 2 = 3 \equiv 0 \mod 3 \\ f(2) &\equiv 1 + 2 = 3 \equiv 0 \mod 3 \end{aligned}$$

So $\mathrm{Sol}_3(\epsilon) = \{1, 2\}$, which fits class {1,2}.

Example: $\zeta = \frac{1}{\sqrt{7-\sqrt{15}}}$

The primitive polynomial is:

$$f(x) = 34x^4 - 14x^2 + 1$$

Reduce modulo 3:

$$f(x) \equiv x^4 + x^2 + 1 \mod 3$$

Test:

$$\begin{aligned} f(0) &\equiv 1 \mod 3 \\ f(1) &\equiv 1 + 1 + 1 = 3 \equiv 0 \mod 3 \\ f(2) &\equiv 1 + 1 + 1 = 3 \equiv 0 \mod 3 \end{aligned}$$

So $\mathrm{Sol}_3(\zeta) = \{1, 2\}$, confirming it belongs to class {1,2}.

4 Congruence Classes Mod 4

We will now pick a non-prime integer 4 and explore some non-trivial examples of algebraic numbers categorized by their generalized modular solution sets modulo 4. The possible congruence classes over $\mathbb{Z}_4$ are the subsets:

$$\{0\}, \{1\}, \{2\}, \{3\}, \{0,1\}, \{0,2\}, \{0,3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{0,1,2\}, \{0,1,3\},$$

$$\{0,2,3\}, \{1,2,3\}, \{0,1,2,3\}, \phi$$

Among these, the sets $\{1\}, \{3\}, \{1,3\}$ are classified as Type A, as they are nonempty and do not contain any element $a \in \mathbb{Z}_4$ such that $a = 0$ or $\gcd(a, 4) > 1$.

Examples from Congruence Class {1}

Example: $\alpha = \sqrt[5]{2 + \sqrt[3]{7}}$

Let:

$$\begin{aligned} &y = \sqrt[3]{7} \Rightarrow y^3 = 7 \\ &z = 2 + y \Rightarrow x^5 = z = 2 + \sqrt[3]{7} \Rightarrow x^5 - 2 = y \\ &(x^5 - 2)^3 = y^3 = 7 \Rightarrow (x^5 - 2)^3 - 7 = 0 \end{aligned}$$

This gives:

$$\begin{aligned} f(x) &= (x^5 - 2)^3 - 7 = x^{15} - 6x^{10} + 12x^5 - 8 - 7 \\ &= x^{15} - 6x^{10} + 12x^5 - 15 \end{aligned}$$

Reduce modulo 4:

$$f(x) \equiv x^{15} + 2x^{10} + 0x^5 + 1 \mod 4$$

Test:

$$\begin{aligned} f(0) &\equiv 1 \mod 4 \\ f(1) &\equiv 1+2+0+1=4 \equiv 0 \mod 4 \\ f(2) &\equiv 0+0+0+1=1 \mod 4 \\ f(3) &\equiv 3+2+0+1=6 \equiv 2 \mod 4 \end{aligned}$$

So $\mathrm{Sol}_4(\alpha) = \{1\}$.

Example: $\beta = \sqrt[3]{8+\sqrt[7]{5}}$

Let:

$$\begin{aligned} &y = \sqrt[7]{5} \Rightarrow y^7 = 5 \\ &x^3 = 8 + y \Rightarrow (x^3-8)^7 = y^7 = 5 \Rightarrow (x^3-8)^7 - 5 = 0 \end{aligned}$$

Reduce modulo 4:

$$\begin{aligned} f(0) &\equiv (-8)^7 - 5 \equiv 0 - 1 = 3 \mod 4 \\ f(1) &\equiv (-7)^7 - 5 \equiv 1 - 1 = 0 \mod 4 \\ f(2) &\equiv 0 - 1 = 3 \mod 4 \\ f(3) &\equiv 19^7 - 5 \equiv 3 - 1 = 2 \mod 4 \end{aligned}$$

So $\mathrm{Sol}_4(\beta) = \{1\}$.

Examples from Congruence Class {3}

Example: $\gamma = \sqrt[3]{2+\sqrt[5]{9}}$

Let:

$$\begin{aligned} &y = \sqrt[5]{9} \Rightarrow y^5 = 9 \\ &x^3 = 2 + y \Rightarrow x^3 - 2 = y \Rightarrow (x^3-2)^5 = 9 \Rightarrow (x^3-2)^5 - 9 = 0 \end{aligned}$$

Expand:

$$f(x) = x^{15} - 10x^{12} + 40x^9 - 80x^6 + 80x^3 - 32 - 9 = x^{15} - 10x^{12} + 40x^9 - 80x^6 + 80x^3 - 41$$

Reduce mod 4:

$$f(x) \equiv x^{15} + 2x^{12} + 0 + 0 + 0 + 3 \mod 4$$

Test:

$$\begin{aligned} f(0) &\equiv 3 \mod 4 \\ f(1) &\equiv 1+2+3=6 \equiv 2 \mod 4 \\ f(2) &\equiv 0+0+3=3 \mod 4 \\ f(3) &\equiv 3+2+3=8 \equiv 0 \mod 4 \end{aligned}$$

So $\mathrm{Sol}_4(\gamma) = \{3\}$.

Example: $\delta = \sqrt[5]{6 + \sqrt[7]{5}}$

Let:

$$x^5 = 6 + \sqrt[7]{5} \Rightarrow (x^5 - 6)^7 = 5 \Rightarrow (x^5 - 6)^7 - 5 = 0$$

Mod 4:

$$\begin{aligned} f(0) &\equiv 2 - 1 = 1 \mod 4 \\ f(1) &\equiv 3 - 1 = 2 \mod 4 \\ f(2) &\equiv 0 - 1 = 3 \mod 4 \\ f(3) &\equiv 1 - 1 = 0 \mod 4 \end{aligned}$$

So $\mathrm{Sol}_4(\delta) = \{3\}$.

Examples from Congruence Class {1,3}

Example: $\epsilon = \sqrt[5]{1 + \sqrt[7]{12}}$

$$x^5 = 1 + \sqrt[7]{12} \Rightarrow (x^5 - 1)^7 = 12 \Rightarrow (x^5 - 1)^7 - 12 = 0$$

Test modulo 4:

$$\begin{aligned} f(0) &\equiv 3 \mod 4 \\ f(1) &\equiv 0 \mod 4 \\ f(2) &\equiv 3 \mod 4 \\ f(3) &\equiv 0 \mod 4 \end{aligned}$$

So $\mathrm{Sol}_4(\epsilon) = \{1, 3\}$.

Example: $\zeta = \sqrt{8 + \sqrt[3]{9}}$

$$x^2 = 8 + \sqrt[3]{9} \Rightarrow (x^2 - 8)^3 = 9 \Rightarrow (x^2 - 8)^3 - 9 = 0$$

Mod 4:

$$\begin{aligned} f(0) &\equiv 3 \mod 4 \\ f(1) &\equiv 0 \mod 4 \\ f(2) &\equiv 3 \mod 4 \\ f(3) &\equiv 0 \mod 4 \end{aligned}$$

So $\mathrm{Sol}_4(\zeta) = \{1, 3\}$.

5 Modular Obstruction Theorems over Type A algebraic numbers

Theorem 2 (Modular Obstruction for mod 2)**.** *Let a, b, c be algebraic numbers such that all three are Type A modulo 2. Then the equation*

$$a^n + b^n = c^n$$

does not hold.

Proof. Since all three are Type A modulo 2. Then their modular solution sets are non-empty and do not include 0. So for any solution $a', b', c' \in \mathbb{Z}_2$ from $\mathrm{Sol}_2(a), \mathrm{Sol}_2(b), \mathrm{Sol}_2(c)$ respectively, we must have:

$$a'^n + b'^n \equiv 1 + 1 \equiv 0 \not\equiv 1 \equiv c'^n \mod 2.$$

This is a contradiction. Hence, at least one of a, b, c must be Type B. □

Example 3. ***(i) Pythagorean Triples:*** *Let $a = 3, b = 4, c = 5$, which satisfy $a^2 + b^2 = c^2$ [1]. Modulo 2, these numbers reduce to $a \equiv 1, b \equiv 0, c \equiv 1$. Since $b \equiv 0$, it violates the condition for being a Type A number. This validates the Modular Obstruction Theorem for Mod 2.*
This tells us that the Pythagorean triples will always have an even integer.

(ii) Trigonometric Identity: *Consider the identity $\sin^2(\theta) + \cos^2(\theta) = 1$. At specific angles, such as $\theta = 30°$ or $\theta = 45°$, we have algebraic values like $\sin(30°) = \frac{1}{2}$ and $\sin(45°) = \frac{\sqrt{2}}{2}$. These are not in $\mathbb{Z}$, and their primitive polynomials do not admit roots in $\mathbb{Z}_2$, hence their solution sets modulo 2 are empty. Thus, these values are Type B numbers, again validating the Modular Obstruction Theorem.*
This shows that trigonometric identities of the form $a^n + b^n = c^n$ will always have at least one Type B number modulo 2 if they involve algebraic numbers.

We can extend this to other moduli and get unique patterns, but we will mention only a few nice ones in this paper.

Theorem 3 (Modular Obstruction for Even Moduli)**.** *Let $k \geq 2$ be any even integer, and let a, b, c be algebraic numbers such that all three are Type A modulo k. Then the equation*

$$a^n + b^n = c^n$$

does not hold for any integer $n \geq 1$.

Proof. Since a, b, c are Type A modulo k, their modular solution sets contain only odd integers in $\mathbb{Z}_k$ (since even integers share a nontrivial gcd with k).

Let $a', b', c' \in \mathbb{Z}_k$ be representatives from their solution sets. Because they are odd, any power $(a')^n, (b')^n, (c')^n$ remains odd. Adding two odd numbers yields an even number, and reducing an even number modulo an even modulus yields an even residue. But c'^n, being odd, yields an odd residue.

Thus, we have:

$$\text{odd} + \text{odd} \equiv \text{even} \not\equiv \text{odd} \mod k$$

This contradiction shows the equation does not hold when all three terms are Type A modulo even k. □

Theorem 4 (Modular Obstruction for Prime Moduli). *Let p be a prime number and let a, b, c be algebraic numbers such that all three are Type A modulo p. Then the equation*

$$a^{p-1} + b^{p-1} = c^{p-1}$$

does not hold.

Proof. Since a, b, c are Type A modulo p, their modular solution sets do not contain 0, and all elements $a', b', c' \in \mathbb{Z}_p$ that satisfy the respective primitive polynomials satisfy $\gcd(a', p) = 1$. Therefore, each of them is a unit modulo p.

By Fermat's Little Theorem [1], we know:

$$(a')^{p-1} \equiv 1 \mod p, \quad (b')^{p-1} \equiv 1 \mod p, \quad (c')^{p-1} \equiv 1 \mod p$$

Substituting into the original equation:

$$1 + 1 \equiv 2 \not\equiv 1 \mod p$$

Hence, the equation $a^{p-1} + b^{p-1} = c^{p-1} \mod p$ does not hold. Therefore, it is impossible for all three numbers to be Type A modulo p while satisfying this equation. □

6 Digital Root Function for Algebraic Numbers

In classical number theory, the digital root of a natural number is the repeated sum of its digits until a single-digit number is obtained. It is closely related to the residue of the number modulo 9, with one key distinction: if the number is divisible by 9, the digital root is defined to be 9, not 0. In this section, we generalize the concept of digital roots to all algebraic numbers using the framework of Generalized Modular Congruence.

Definition 4 (Digital Root Function $\mathrm{dr}(\alpha)$). *Let α be an algebraic number with primitive polynomial $f_\alpha(x) \in \mathbb{Z}[x]$. Define the digital root set $\mathrm{dr}(\alpha) \subseteq \mathbb{Z}$ as follows:*

1. *Compute $Sol_9(\alpha) = \{a \in \mathbb{Z}_9 : f_\alpha(a) \equiv 0 \mod 9\}$.*
2. *Replace every occurrence of 0 in $Sol_9(\alpha)$ with 9.*

Formally,

$$\mathrm{dr}(\alpha) := \{a \in Sol_9(\alpha) \mid a \neq 0\} \cup \{9 \mid 0 \in Sol_9(\alpha)\}.$$

We now discuss how this definition behaves in various cases.

Natural Numbers

For a natural number n, the classical digital root corresponds to the unique element $r \in \mathbb{Z}_9$ such that $n \equiv r \mod 9$, with $r = 0$ interpreted as 9.

Example 4. *$dr(86) = 5$ because $8 + 6 = 14, 1 + 4 = 5$ and $86 \equiv 5 \mod 9$.*

$dr(99) = 9$ because $9 + 9 = 18, 1 + 8 = 9$, and although $99 \equiv 0 \mod 9$, the digital root is defined to be 9.

Terminating Fractions

For rational algebraic numbers with terminating decimal expansions (i.e., denominators relatively prime to 3), modular inverses exist modulo 9, and $\mathrm{Sol}_9(\alpha)$ contains a unique value. The digital root coincides with the sum-of-digits interpretation.

Example 5. *$\alpha = \frac{1}{2} = 0.5 \Rightarrow$ primitive polynomial: $2x - 1 \Rightarrow x \equiv 5 \mod 9$, so $dr(1/2) = 5$. Sum of digits: $5 \Rightarrow dr = 5$.*

$\alpha = \frac{2}{5} = 0.4 \Rightarrow$ primitive polynomial: $5x - 2 \Rightarrow x \equiv 4 \mod 9$, so $dr(2/5) = 4$. Sum of digits: $4 \Rightarrow dr = 4$.

$\alpha = \frac{7}{8} = 0.875 \Rightarrow$ primitive polynomial: $8x - 7 \Rightarrow x \equiv 2 \mod 9$, so $dr(7/8) = 2$. Sum of digits: $8 + 7 + 5 = 20, \quad 2 + 0 = 2 \Rightarrow dr = 2$.

Non-Terminating Fractions

For repeating decimals like $\frac{1}{7} = 0.142857142857\ldots$, we still define their digital root using generalized mod 9.

Example 6. *$\alpha = \frac{1}{7} \Rightarrow 7x - 1 = 0 \Rightarrow x \equiv 4 \mod 9$. So $dr(1/7) = 4$.*

This raises the question: Does the sum of the digits in the repeating decimal expansion of $\frac{1}{7}$, i.e., 0.142857..., equal $9m + 4$ for some integer m?

Irrational Algebraic Numbers

For irrational algebraic numbers, primitive polynomials often have multiple roots modulo 9. Hence, $\mathrm{Sol}_9(\alpha)$ may contain more than one value, making the digital root multivalued in this sense.

Example 7. *$\alpha = \sqrt{7} \Rightarrow$ polynomial : $x^2 - 7 \Rightarrow x^2 \equiv 7 \mod 9$. The roots are $x \equiv 4, 5 \mod 9$, so $Sol_9(\alpha) = \{4, 5\}$.*

This prompts the question: If we could meaningfully sum the digits of $\sqrt{7}$, would the result be congruent to $9m + 4$ or $9m + 5$?

Conclusion

We have introduced a generalized modular congruence framework for algebraic numbers based on their primitive polynomials. By defining modular solution sets and classifying algebraic numbers into Type A and Type B, we obtained a powerful lens to examine the behavior of algebraic equations under modular constraints. Our framework allowed us to establish several *Modular Obstruction Theorems*, demonstrating that equations such as $a^n + b^n = c^n$ cannot hold under specific modular conditions when all involved numbers are Type A.

In addition, we proposed a novel modular definition of the digital root function. By reducing the primitive polynomial modulo 9 and analyzing its roots, we extended the digital root operation to rational and algebraic numbers. For integers and terminating decimals, our method recovers the classical digit-sum behavior, while offering a consistent generalization to irrational algebraic numbers where classical digit sums are ambiguous or undefined.

We are currently exploring further questions within this framework, such as: will every algebraic number be a Type A number for at least one prime? Is there any algebraic number that's type B except zero for infinite number of primes? What is the density of Type A and Type B numbers modulo a given prime? How often is a number Type A across the primes? These directions are under active investigation and will be reported in forthcoming work.

References

[1] Joseph H. Silverman, *A Friendly Introduction to Number Theory*, 4th ed., Pearson, 2012.

[2] David S. Dummit and Richard M. Foote, *Abstract Algebra*, 3rd ed., Wiley, 2004.