IRREDUCIBILITY OF POLYNOMIALS WITH COEFFICIENTS IN A POSITIVE ARITHMETIC PROGRESSION

Hiroaki Kakuma
Department of Mathematics, Kaichi Nihonbashi Junior and Senior High School, Tokyo, Japan
kakumah@kng.ed.jp

Received: 3/1/26, Accepted: 7/5/26, Published: 7/29/26

Abstract

Let a and d be coprime positive integers, and let $m \geq 2$ be an integer. We consider the polynomial $A_m(x) = ax^m + (a+d)x^{m-1} + \cdots + (a+(m-1)d)x + (a+md)$. We prove that $A_m(x)$ is irreducible in $\mathbb{Z}[x]$ whenever $8a > m^2d^2$. Our proof is based on zero localization: we show that, in this range, the zeros of $A_m(x)$ have nearly equal moduli, and that this is incompatible with the arithmetic constraints imposed by a nontrivial factorization over $\mathbb{Z}[x]$. We also study the cases $m = 2, 3, 4$ in detail, including a complete characterization of reducibility for $m = 2$.

1. Introduction

Determining irreducibility in $\mathbb{Z}[x]$ is a classical problem in algebraic number theory. Many standard criteria are arithmetic in nature, relying on divisibility properties of the coefficients, as in Eisenstein's criterion [2]. There are also criteria based on the sizes of coefficients or on arithmetic properties of values of the polynomial [7, 5]. Among the size-based approaches, Perron's criterion is a representative result linking coefficient size to the distribution of zeros: for a monic polynomial, irreducibility follows when the coefficient of x^{n-1} dominates the remaining coefficients.

Theorem 1 (Perron's irreducibility criterion [6])**.** *Let*

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 \in \mathbb{Z}[x],\ a_0 \neq 0.$$

If $|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|$*, then* $f(x)$ *is irreducible in* $\mathbb{Z}[x]$*.*

In this paper, we study irreducibility from the viewpoint of coefficient size, but in a setting different from Perron's criterion. We consider polynomials whose coefficients are positive integers forming an arithmetic progression, and we focus on the regime in which the ratios of consecutive coefficients are nearly constant.

DOI: 10.5281/zenodo.21678152

For coprime positive integers a and d and an integer $m \geq 2$, define

$$A_m(x) = ax^m + (a+d)x^{m-1} + \cdots + (a+(m-1)d)x + (a+md) \in \mathbb{Z}[x].$$

This family has been studied in special cases. In particular, Borisov et al. [1] proved that for $a = d = 1$ the polynomial $A_m(x)$ is irreducible for almost all degrees m, although a complete classification is still unknown. Our work may be viewed as a complementary direction: we treat general a and d, and give explicit size conditions ensuring irreducibility.

Theorem 2 (Main Theorem)**.** *Let $m \geq 2$ be an integer, and a and d be coprime positive integers with*

$$a > \frac{m^2 d^2}{8}. \tag{1}$$

Then, the polynomial

$$ax^m + (a+d)x^{m-1} + \cdots + (a+(m-1)d)x + (a+md)$$

is irreducible over $\mathbb{Z}[x]$.

The proof has a geometric component: when a is sufficiently large relative to d and m, we show that the zeros of $A_m(x)$ have nearly equal moduli. We then combine this zero localization with constraints on the coefficients of a reducible polynomial in $\mathbb{Z}[x]$ to rule out nontrivial factorizations.

We also analyze small degrees, where reducibility can occur even for moderate a. For $m = 2$, we give a complete characterization: there exists an a for which $A_2(x)$ is reducible if and only if every prime divisor of d is congruent to 1 modulo 3. For $m = 3$, computational data indicate that reducible examples occur frequently when d has prime divisors congruent to 1 modulo 4, although we do not yet have a necessary and sufficient condition. For $m = 4$, we prove that $A_4(x)$ does not factor as a product of two quadratic polynomials. Extensive numerical evidence further suggests the following conjecture: $A_m(x)$ is reducible only when it has a rational zero.

This paper is a continuation of the author's previous work [3], in which irreducibility results for polynomials with Fibonacci coefficients were established via the geometry of their zeros. The present paper applies the same viewpoint to arithmetic-progression coefficients, whose structure is simpler, with the aim of clarifying how zero distribution controls irreducibility.

2. Irreducibility Criteria for Polynomials with Arithmetic Progression Coefficients

Throughout this section, we put

$$a_n = a + (n-1)d \quad (n \geq 0).$$

for positive integers a and d. With this notation, the polynomial $A_m(x)$ is given by

$$A_m(x) = a_1x^m + a_2x^{m-1} + \cdots + a_mx + a_{m+1}.$$

Lemma 1. *Let a, d and m are positive integers. The following identity holds.*

$$A_m(x)(x-1)^2 = a_1x^{m+2} - a_0x^{m+1} - a_{m+2}x + a_{m+1}.$$

Furthermore, if z is a zero of $A_m(x)$ or if $z = 1$, then

$$z^{m+1} = \frac{a_{m+2}z - a_{m+1}}{a_1z - a_0}. \tag{2}$$

Proof. Since $\{a_n\}$ is an arithmetic progression, the relation $2a_n = a_{n+1} + a_{n-1}$ holds. Therefore,

$$\begin{aligned} A_m(x)(x-1)^2 &= a_1x^{m+2} + (a_2 - 2a_1)x^{m+1} + \sum_{j=2}^{m}(a_{j-1} - 2a_j + a_{j+1})x^j \\ &\quad + (a_m - 2a_{m+1})x + a_{m+1} \\ &= a_1x^{m+2} - a_0x^{m+1} - a_{m+2}x + a_{m+1}. \end{aligned}$$

This establishes the identity. □

We use this relationship to investigate the distribution of the zeros.

Proposition 1. *Let $m \geq 2$ be an integer and let a and d be positive integers with $a \geq d$. The equation*

$$a_1x^{m+2} + a_0x^{m+1} - a_{m+2}x - a_{m+1} = 0 \tag{3}$$

has exactly one positive real solution larger than 1.

Proof. Let $G(x)$ denote the left-hand side of the equation. Then,

$$\begin{aligned} G'(x) &= (m+2)a_1x^{m+1} + (m+1)a_0x^m - a_{m+2}, \\ G''(x) &= (m+1)\{(m+2)a_1x + ma_0\}x^{m-1}. \end{aligned}$$

Thus, $G''(x) > 0$ for all $x > 0$, implying that $G'(x)$ is monotonically increasing for $x > 0$. Since

$$G'(1) = 2(m+1)(a-d) \geq 0,$$

$G(x)$ is monotonically increasing for $x > 1$. For simplicity, we shall write $t = d/a$

in what follows. Then we have

$$\begin{aligned}
G\left(\frac{a_2}{a_1}\right) &= (a_2+a_0)\left(\frac{a_2}{a_1}\right)^{m+1} - \frac{a_{m+2}a_2 + a_{m+1}a_1}{a_1} \\
&= 2a(1+t)^{m+1} - \frac{\{a+(m+1)d\}(a+d)+(a+md)a}{a} \\
&\geq 2a\left\{1+(m+1)t+\frac{m(m+1)}{2}t^2\right\} - 2a\left\{1+(m+1)t+\frac{m+1}{2}t^2\right\} \\
&= a(m^2-1)t^2 > 0, \\
G(1) &= a_1+a_0-a_{m+2}-a_{m+1} = -2(m+1)d < 0.
\end{aligned}$$

Therefore, the equation $G(x)=0$ has a real solution in the interval $(1, a_2/a_1)$. □

Hereafter, we denote this unique positive solution by λ.

Proposition 2. *Let $m \geq 2$ be an integer and let a and d be positive integers with $a \geq d$. Let λ denote the only positive solution of (3). For every zero z of the polynomial $A_m(x)$, one has $|z| \leq \lambda$. Moreover, equality $|z| = \lambda$ can occur only at the real point $z = -\lambda$.*

Proof. We proceed by contradiction. Assume that $|z| > \lambda$. From Equation (2), if we define the Möbius transformation $g : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$ by

$$g(x) = \frac{a_{m+2}x - a_{m+1}}{a_1 x - a_0},$$

then $z^{m+1} = g(z)$ holds. The transformation g maps the exterior of the circle $|x| = \lambda$ to the interior of a circle whose diameter has endpoints $g(\lambda)$ and $g(-\lambda)$. Since

$$g(z) = \frac{a_{m+2}}{a_1} - \frac{a_{m+1}a_1 - a_{m+2}a_0}{a_1(a_1 z - a_0)} = \frac{a_{m+2}}{a_1} - \frac{(m+1)d^2}{a_1(a_1 z - a_0)},$$

it follows that $g(-\lambda) > g(\lambda)$. Furthermore, since

$$g(-\lambda) = \frac{a_{m+2}\lambda + a_{m+1}}{a_1\lambda + a_0} = \lambda^{m+1}, \tag{4}$$

any complex number x satisfying $|x| > \lambda$ must satisfy $|g(x)| < \lambda^{m+1}$. However, if z is a zero of $A_m(x)$, we must have $g(z) = z^{m+1}$, which implies $|g(z)| = |z|^{m+1}$. The assumption $|z| > \lambda$ leads to $|z|^{m+1} > \lambda^{m+1}$, while the mapping property of g implies $|g(z)| < \lambda^{m+1}$, a contradiction. Therefore, $|z| \leq \lambda$ holds for any zero z of $A_m(x)$. Furthermore, suppose that z is a zero of $A_m(x)$ satisfying $|z| = \lambda$. Then $z^{m+1} = g(z)$, and hence

$$|g(z)| = \left|z^{m+1}\right| = |z|^{m+1} = \lambda^{m+1}.$$

As shown above, g maps the circle $|z| = \lambda$ onto the circle whose diameter has endpoints $g(\lambda)$ and $g(-\lambda)$. On this image circle, $|w|$ attains its maximum value λ^{m+1} only at the endpoint $w = g(-\lambda) = \lambda^{m+1}$. Therefore, we must have $g(z) = g(-\lambda)$. Since g is injective, it follows that $z = -\lambda$. □

Lemma 2. *Let $m \geq 2$ be an integer and let a and d be positive integers with $a \geq d$. Let λ denote the only positive solution of (3). Then the following inequality holds.*

$$a\lambda^m - a_{m+1} > 0.$$

Proof. Let $z_1, z_2, \ldots, z_m$ be zeros of $A_m(x)$. From the relation between roots and coefficients, we have

$$a_{m+1} = a \prod_{j=1}^{m} |z_j|.$$

By Proposition 2, we have $|z_j| \leq \lambda$ for all j. Moreover, not all zeros of $A_m(x)$ are equal to $-\lambda$. Hence

$$a_{m+1} < a\lambda^m.$$

□

Putting $t = d/a$, this inequality can be rewritten as

$$\lambda > (1 + mt)^{\frac{1}{m}}. \tag{5}$$

Lemma 3. *Let $x > 0$ be a real number, and let $m \geq 2$ be an integer. Then the following inequality holds.*

$$(1 + mx)^{\frac{1}{m}} > \frac{2 + (m+1)x}{2 + (m-1)x}.$$

Proof. Let

$$f(x) = \frac{1}{m} \log(1 + mx) - \log\left(2 + (m+1)x\right) + \log\left(2 + (m-1)x\right).$$

We aim to show that $f(x) > 0$ for $x > 0$. The derivative is given by

$$\begin{aligned} f'(x) &= \frac{1}{1 + mx} - \frac{m+1}{2 + (m+1)x} + \frac{m-1}{2 + (m-1)x} \\ &= \frac{(m^2 - 1)x^2}{(1 + mx)\{2 + (m+1)x\}\{2 + (m-1)x\}}. \end{aligned}$$

Since $f'(x) > 0$ for $x > 0$, $f(x)$ is monotonically increasing in this range. Therefore, for $x > 0$,

$$f(x) > f(0) = 0.$$

□

From Equation (5) and Lemma 3, we observe that

$$\lambda > \frac{2+(m+1)t}{2+(m-1)t}. \tag{6}$$

Proposition 3. *Let $m \geq 2$ be an integer and let a and d be positive integers with $2a > \sqrt{m^2-1}\, d^{\frac{3}{2}}$. Let λ denote the only positive solution of (3). Then we have the following equation:*

$$\lfloor a\lambda^m \rfloor = a_{m+1}.$$

Proof. Note that the condition $2a > \sqrt{m^2-1}\, d^{3/2}$ implies $a \geq d$. From Equation (4), we have

$$\lambda^m = \frac{a_{m+2}\lambda + a_{m+1}}{\lambda(a_1\lambda + a_0)} = \frac{\{1+(m+1)t\}\lambda + 1 + mt}{\lambda^2 + (1-t)\lambda}.$$

At this point, we again put $t = d/a$. For $x > 1$, define

$$F(x) = \frac{\{1+(m+1)t\}x + 1 + mt}{x^2 + (1-t)x}.$$

Then the derivative is

$$F'(x) = -\frac{\{1+(m+1)t\}x^2 + 2(1+mt)x + (1-t)(1+mt)}{\{x^2+(1-t)x\}^2} < 0,$$

so $F(x)$ is monotonically decreasing for $x > 1$. Using Equation (6), we obtain

$$\begin{aligned}\lambda^m = F(\lambda) &< F\left(\frac{2+(m+1)t}{2+(m-1)t}\right) \\ &= \frac{\{1+(m+1)t\}\{2+(m+1)t\}\{2+(m-1)t\} + (1+mt)\{2+(m-1)t\}^2}{\{2+(m+1)t\}^2 + (1-t)\{2+(m+1)t\}\{2+(m-1)t\}}.\end{aligned}$$

This leads to the inequality

$$\lambda^m - (1+mt) < \frac{(mt+2)(m^2-1)t^3}{\{(m+1)t+2\}\{m+3-(m-1)(t-1)^2\}}.$$

Since $0 < t \leq 1$, we have $m+3-(m-1)(t-1)^2 = 4+(m-1)t(2-t) > 4$, and thus

$$a\lambda^m - a_{m+1} < \frac{(m^2-1)}{4}at^3 = \frac{(m^2-1)d^3}{4a^2}.$$

Given that $4a^2 > (m^2-1)d^3$, we have

$$a\lambda^m - a_{m+1} < 1.$$

Therefore, combined with Lemma 2 which ensures $a\lambda^m - a_{m+1} > 0$, we conclude that $\lfloor a\lambda^m \rfloor = a_{m+1}$.

□

Proposition 4. *Let $m \geq 2$ be an integer, and a and d be positive integers with $2a > (m+1)d$. Let λ denote the only positive solution of (3). Then the following inequality holds for every integer p with $1 \leq p \leq m-1$:*

$$\lfloor a\lambda^p \rfloor < a_{p+1}.$$

Proof. To establish the desired inequality, it suffices to prove that

$$a\lambda^p < a_{p+1} = a + pd,$$

or equivalently,

$$\lambda < (1+pt)^{\frac{1}{p}}.$$

We use the notation $t = d/a$ again. Since the right-hand side is monotonically decreasing in p, it is enough to verify the case $p = m-1$, namely,

$$a\lambda^{m-1} < a_m.$$

The assumption $2a > (m+1)d$ is equivalent to $0 < t < 2/(m+1)$. From Equation (5) and Lemma 3, we have

$$\lambda > \frac{2+(m+1)t}{2+(m-1)t} > 1.$$

Set

$$N(x) = a_1a_mx^3 + a_0a_mx^2 - a_1a_{m+2}x - a_1a_{m+1}.$$

Then we have

$$\lambda^2(a_m - a\lambda^{m-1}) = \frac{N(\lambda)}{a_1\lambda + a_0}.$$

Since $a_1\lambda + a_0 > 0$, it suffices to show $N(\lambda) > 0$. We have

$$N''(x) = 6a_1a_mx + 2a_0a_m > 0 \qquad (x > 0),$$

so $N'(x)$ is increasing for $x > 0$. Moreover,

$$\frac{N'(1)}{a^2} = 4 + 4(m-2)t - 2(m-1)t^2.$$

The right-hand side is a concave quadratic in t, denote it by $h(t)$, and

$$h(0) = 4 > 0, \quad h\left(\frac{2}{m+1}\right) = \frac{4(3m+1)(m-1)}{(m+1)^2} > 0,$$

hence $N'(1) > 0$ for $0 < t < 2/(m+1)$. Therefore $N'(x) > 0$ for all $x > 1$, and N is increasing for $x > 1$. Consequently,

$$N(\lambda) > N\left(\frac{2+(m+1)t}{2+(m-1)t}\right).$$

A direct computation gives

$$a^{-2}N\left(\frac{2+(m+1)t}{2+(m-1)t}\right)=\frac{(m-1)t^2}{(2+(m-1)t)^3}\,f(t),$$

where

$$f(t)=8+4(m-1)t-2(m^2+2m-1)t^2-(m-1)(m+1)^2t^3.$$

Since

$$f''(t)=-4(m^2+2m-1)-6(m-1)(m+1)^2t<0\quad(t>0),$$

f is concave on $[0,2/(m+1)]$, hence

$$f(t)>\min\Big\{f(0),\,f\Big(\frac{2}{m+1}\Big)\Big\}=\min\Big\{8,\,\frac{16}{(m+1)^2}\Big\}>0.$$

Thus $N(\lambda)>0$, which implies $a\lambda^{m-1}<a_m$ and completes the proof. □

Proposition 5. *Let $m\geq 2$ be an integer, let a and d be positive integers, and let p be an integer with $1\leq p\leq m-1$. Let λ denote the only positive solution of (3). If $2a>p(m-p)d^2$, then the following equation holds:*

$$\lfloor a\lambda^p\rfloor=a_{p+1}-1.$$

In particular, if $8a>m^2d^2$, then, for every integer p with $1\leq p\leq m-1$, we have

$$\lfloor a\lambda^p\rfloor=a_{p+1}-1.$$

Proof. From Equation (5), we have

$$a_{p+1}-a\lambda^p<a+pd-a(1+mt)^{\frac{p}{m}}.$$

Let

$$E(x)=\frac{p(m-p)}{2}x^2-\{1+px-(1+mx)^{\frac{p}{m}}\}.$$

For $x>0$, the derivatives are

$$E'(x)=p(m-p)x-p+p(1+mx)^{\frac{p}{m}-1},$$
$$E''(x)=p(m-p)\{1-(1+mx)^{\frac{p}{m}-2}\}>0.$$

Thus, $E'(x)$ is monotonically increasing for $x>0$. Since $E'(x)>E'(0)=0$, $E(x)$ is also monotonically increasing for $x>0$. Given $E(0)=0$, we have $E(t)>0$. Therefore,

$$a_{p+1}-a\lambda^p<\frac{p(m-p)}{2}at^2=\frac{p(m-p)d^2}{2a}.$$

Consequently, if $2a > p(m-p)d^2$, then

$$a_{p+1} - a\lambda^p < 1.$$

Furthermore, since

$$p(m-p) = \frac{m^2}{4} - \left(\frac{m}{2} - p\right)^2 \leq \frac{m^2}{4},$$

for any $1 \leq p \leq m-1$, we have

$$a_{p+1} - a\lambda^p < \frac{m^2 d^2}{8a}.$$

Therefore, if $8a > m^2 d^2$, then

$$a_{p+1} - a\lambda^p < 1$$

holds. □

Using the results above, we now prove the paper's main Theorem.

Proof of Theorem 2. Assume that there exist non-constant polynomials $P(x), Q(x) \in \mathbb{Z}[x]$ such that

$$A_m(x) = P(x)Q(x).$$

Let p and q be the degrees of $P(x)$ and $Q(x)$, α and β be the absolute values of their leading coefficients, and γ and δ be the absolute values of their constant terms, respectively. Then,

$$m = p + q, \quad a_1 = \alpha\beta, \quad a_{m+1} = \gamma\delta.$$

Let $z_1, z_2, \ldots, z_p$ be the zeros of $P(x)$ and $z_{p+1}, z_{p+2}, \ldots, z_m$ be the zeros of $Q(x)$. From the relation between roots and coefficients,

$$\alpha \prod_{j=1}^{p} |z_j| = \gamma, \quad \beta \prod_{j=1}^{q} |z_{p+j}| = \delta.$$

By Proposition 2, we have $|z_k| \leq \lambda$ $(k = 1, 2, \ldots, m)$. Hence

$$\alpha\lambda^p - \gamma \geq 0, \quad \beta\lambda^q - \delta \geq 0.$$

On the other hand,

$$\begin{aligned} a\lambda^m - a_{m+1} &= a\Big(\lambda^m - \prod_{j=1}^{m} |z_j|\Big) \\ &= a\lambda^q\Big(\lambda^p - \prod_{j=1}^{p} |z_j|\Big) + a\prod_{j=1}^{p} |z_j|\Big(\lambda^q - \prod_{j=1}^{q} |z_{p+j}|\Big) \\ &= \beta\lambda^q\Big(\alpha\lambda^p - \alpha\prod_{j=1}^{p} |z_j|\Big) + \gamma\Big(\beta\lambda^q - \beta\prod_{j=1}^{q} |z_{p+j}|\Big) \\ &= \beta\lambda^q\big(\alpha\lambda^p - \gamma\big) + \gamma\big(\beta\lambda^q - \delta\big). \end{aligned}$$

The only triples of positive integers (m, a, d) satisfying

$$\frac{(m+1)d}{2} \geq a > \frac{m^2d^2}{8}$$

are

$$(m, a, d) = (2, 1, 1),\ (2, 3, 2),\ (3, 2, 1).$$

The corresponding polynomials are

$$x^2 + 2x + 3, \quad 3x^2 + 5x + 7, \quad 2x^3 + 3x^2 + 4x + 5,$$

respectively, and all of them are irreducible over $\mathbb{Z}[x]$. Therefore, in what follows, we may assume that

$$a > \frac{m^2d^2}{8} \quad \text{and} \quad a > \frac{(m+1)d}{2}.$$

Then

$$a^2 > \frac{(m+1)d}{2} \cdot \frac{m^2d^2}{8} = \frac{m^2}{4(m-1)} \cdot \frac{(m^2-1)d^3}{4} \geq \frac{(m^2-1)d^3}{4},$$

and hence $2a > \sqrt{m^2-1}\, d^{\frac{3}{2}}$. By Propositions 3, 4, and 5, we have

$$a\lambda^m - a_{m+1} < 1,\ \lfloor a\lambda^p \rfloor = a_{p+1} - 1\ (p = 1, 2, \ldots, m-1).$$

Thus,

$$0 \leq \alpha\lambda^p - \gamma < \frac{1}{\beta\lambda^q}(a\lambda^m - a_{m+1}) < \frac{1}{\beta\lambda^q} < 1.$$

Also, since

$$0 \leq \alpha\beta\lambda^p - \beta\gamma = a\lambda^p - \beta\gamma < \frac{1}{\lambda^q} < 1,$$

we have

$$\gamma = \lfloor \alpha\lambda^p \rfloor, \quad \beta\gamma = \lfloor a\lambda^p \rfloor.$$

Similarly, we can show

$$0 \le \beta\lambda^q - \delta < \frac{1}{\alpha\lambda^p},$$

which implies

$$\delta = \lfloor \beta\lambda^q \rfloor, \quad \alpha\delta = \lfloor a\lambda^q \rfloor.$$

From $\gamma\delta = a_{m+1}$, we obtain

$$\begin{aligned} a_{m+1} &= \frac{\alpha\delta \cdot \beta\gamma}{\alpha\beta} = \frac{\lfloor a\lambda^p \rfloor \lfloor a\lambda^q \rfloor}{a} = \frac{(a_{p+1}-1)(a_{q+1}-1)}{a} \\ &= \frac{(a+pd-1)(a+qd-1)}{a} \\ &= \frac{a^2 + a(p+q)d + pqd^2 - 2a - (p+q)d + 1}{a} \\ &= a + md + \frac{p(m-p)d^2 - 2a - md + 1}{a}. \end{aligned}$$

This implies

$$a = \frac{1}{2}p(m-p)d^2 - \frac{1}{2}(md-1) < \frac{m^2d^2}{8},$$

contradicting Equation (1). Therefore, $A_m(x)$ is irreducible over $\mathbb{Z}[x]$. □

3. Irreducibility Criteria for Low-Degree Polynomials

Regarding the irreducibility of the polynomial $A_m(x)$, we can consider the following simple sufficient condition.

Proposition 6. *Assume that $m+1$ is a prime number. If d has a prime divisor p such that $p \not\equiv 0 \pmod{m+1}$, and p is a primitive root modulo $m+1$, then the polynomial*

$$A_m(x) = ax^m + (a+d)x^{m-1} + \cdots + (a+md)$$

is irreducible over $\mathbb{Z}[x]$.

Proof. Let p be a prime factor of d that satisfies the hypothesis. Then $a \not\equiv 0 \pmod{p}$, and

$$A_m(x) \equiv a(x^m + x^{m-1} + \cdots + x + 1) \pmod{p}.$$

Since $x^m + x^{m-1} + \cdots + x + 1$ is irreducible over $\mathbb{F}_p[x]$, it follows that $A_m(x)$ is irreducible over $\mathbb{F}_p[x]$, and hence over $\mathbb{Z}[x]$. □

For small values of m, we can establish stronger results than the general theory suggests. For $A_2(x)$, we have the following necessary and sufficient condition.

Theorem 3. *Fix a positive integer d. There exists an positive integer a such that*

$$A_2(x) = ax^2 + (a+d)x + (a+2d)$$

is reducible over $\mathbb{Z}[x]$ if and only if every prime divisor p of d satisfies $p \equiv 1 \pmod 3$. Moreover, if d has n distinct prime divisors, then there are exactly 2^{n-1} such integers a.

Proof. The polynomial $A_2(x)$ is reducible over $\mathbb{Z}[x]$ if and only if its discriminant

$$\Delta = (a+d)^2 - 4a(a+2d) = 4d^2 - 3(a+d)^2$$

is a square.

Assume that there exists an integer a such that Δ is a square. If $2 \mid d$, then $\gcd(a,d) = 1$ forces a to be odd, hence $a+d$ is odd and

$$\Delta \equiv -3 \equiv 5 \pmod 8,$$

which is impossible. Thus $2 \nmid d$. If $3 \mid d$, then $3 \nmid (a+d)$ and hence $(a+d)^2 \equiv 1, 4, 7 \pmod 9$, so

$$\Delta \equiv -3(a+d)^2 \equiv 6 \pmod 9,$$

also impossible. Therefore $3 \nmid d$. Now let p be any prime divisor of d. Then $p \neq 3$ and $d \equiv 0 \pmod p$, so

$$\Delta \equiv -3(a+d)^2 \equiv -3a^2 \pmod p,$$

where we used $\gcd(a,p) = 1$. Hence -3 is a quadratic residue modulo p, and for $p \neq 3$ this is equivalent to $p \equiv 1 \pmod 3$. Thus every prime divisor of d satisfies $p \equiv 1 \pmod 3$.

Assume conversely that every prime divisor p of d satisfies $p \equiv 1 \pmod 3$. Let $\omega = \frac{-1+\sqrt{-3}}{2}$, so that $\mathbb{Z}[\omega]$ is the ring of Eisenstein integers and

$$N(x+y\omega) = (x+y\omega)(x+y\overline{\omega}) = x^2 - xy + y^2$$

is its norm. We claim that there exist integers s and t such that

$$N(s+t\omega) = s^2 - st + t^2 = d^2, \qquad t > d, \qquad \gcd(s,t) = 1. \tag{7}$$

Write

$$d = \prod_{k=1}^{n} p_k^{e_k},$$

where the p_k are distinct primes with $p_k \equiv 1 \pmod 3$. In $\mathbb{Z}[\omega]$ each p_k splits as $p_k = \pi_k \overline{\pi_k}$ with $\gcd(\pi_k, \overline{\pi_k}) = 1$. For each k, choose one of π_k and $\overline{\pi_k}$, and define

$$\alpha := \prod_{k=1}^{n} \eta_k^{2e_k} \in \mathbb{Z}[\omega], \text{ where } \eta_k \in \{\pi_k, \overline{\pi_k}\}.$$

Then $N(\alpha) = \prod_{k=1}^{n} N(\eta_k)^{2e_k} = d^2$, so writing $\alpha = s + t\omega$ gives $N(s + t\omega) = d^2$. Moreover, $\gcd(s, t) = 1$. Indeed, if a prime r divides both s and t, then $r \mid (s+t\omega) = \alpha$, so $r \mid N(\alpha) = d^2$, hence $r = p_k$ for some k. But then both π_k and $\overline{\pi_k}$ divide α, contradicting the construction of α. Up to multiplication by a unit, there are 2^n possibilities for α. Complex conjugation interchanges the complementary choices $\pi_k^{2e_k} \leftrightarrow \overline{\pi_k}^{2e_k}$, so these 2^n possibilities split into 2^{n-1} conjugate pairs $\{\alpha, \overline{\alpha}\}$ up to units. For each conjugate pair, choose a unit $\varepsilon \in \{\pm 1, \pm\omega, \pm\omega^2\}$ such that

$$\beta := \varepsilon\alpha \quad \text{satisfies} \quad \frac{\pi}{3} < \arg(\beta) < \frac{2\pi}{3}.$$

This is possible because α is not on a boundary ray $\arg \in \{0, \pm\pi/3, \pm 2\pi/3, \pi\}$. Write again $\beta = s + t\omega \in \mathbb{Z}[\omega]$. Then we have

$$\beta = \left(s - \frac{t}{2}\right) + i\frac{\sqrt{3}t}{2}.$$

The condition $\frac{\pi}{3} < \arg(\beta) < \frac{2\pi}{3}$ implies $y > 0$ and $\sqrt{3}|x| < y$ for $\beta = x + iy$. Hence

$$\frac{\sqrt{3}t}{2} > 0, \quad \left|s - \frac{t}{2}\right| < \frac{t}{2},$$

so $0 < s < t$. Using $N(\beta) = N(\alpha) = d^2$, we obtain

$$t^2 - d^2 = t^2 - (s^2 - st + t^2) = s(t - s) > 0,$$

and therefore $t > d$. This proves (7).

Finally, different conjugate pairs yield different values of t: for fixed t, the equation $s^2 - st + t^2 = d^2$ is quadratic in s, so s can take only the two values s and $t - s$, which correspond to $\beta = s + t\omega$ and $(t - s) + t\omega = -\overline{\beta}$, i.e. the same conjugate pair. Hence there are exactly 2^{n-1} possible values of $t > d$. Moreover, for each such t, set $a = t - d$. Then

$$\Delta = 4d^2 - 3t^2 = 4(s^2 - st + t^2) - 3t^2 = (2s - t)^2,$$

so Δ is a square.

□

Remark 1. Consider the case $d = 1729 = 7 \cdot 13 \cdot 19$. The prime factors decompose in $\mathbb{Z}[\omega]$ as:

$$7 = (3 + \omega)(3 + \overline{\omega}), \quad 13 = (4 + \omega)(4 + \overline{\omega}), \quad 19 = (5 + 2\omega)(5 + 2\overline{\omega}).$$

For instance, consider the divisor of d^2:

$$(3 + \omega)^2(4 + \omega)^2(5 + 2\omega)^2 = 249 + 1840\omega.$$

Setting $a = t - d = 1840 - 1729 = 111$, the resulting quadratic polynomial factors as:

$$111x^2 + 1840x + 3569 = (3x + 43)(37x + 83).$$

Similarly, taking the divisors

$$\begin{aligned}
-\omega^2(3+\overline{\omega})^2(4+\omega)^2(5+2\omega)^2 &= 799 + 1984\omega,\\
-\omega^2(3+\omega)^2(4+\overline{\omega})^2(5+2\omega)^2 &= 96 + 1775\omega,\\
-\omega^2(3+\omega)^2(4+\omega)^2(5+2\overline{\omega})^2 &= 1305 + 1961\omega,
\end{aligned}$$

yields $a = 255, 46$, and 232, respectively. The corresponding quadratic polynomials factor as follows:

$$\begin{aligned}
255x^2 + 1984x + 3713 &= (15x + 47)(17x + 79),\\
46x^2 + 1775x + 3504 &= (2x + 73)(23x + 48),\\
232x^2 + 1961x + 3690 &= (8x + 45)(29x + 82).
\end{aligned}$$

For the polynomial

$$A_3(x) = ax^3 + (a + d)x^2 + (a + 2d)x + (a + 3d),$$

we have not obtained such a clear condition. However, if it is reducible, it must have a linear factor $ux + v$, where where u and v are coprime integers. Since

$$A_3\left(-\frac{v}{u}\right) = \frac{-a(v^3 - uv^2 + u^2v - u^3) + du(v^2 - 2uv + 3u^2)}{u^3} = 0,$$

and given that $\gcd(a, d) = 1$, let

$$\begin{aligned}
g &= \gcd\big(v^3 - uv^2 + u^2v - u^3,\ u(v^2 - 2uv + 3u^2)\big)\\
&= \begin{cases} 2 & \text{if } u \text{ and } v \text{ are both odd,}\\ 1 & \text{if } u \text{ and } v \text{ have different parity.}\end{cases}
\end{aligned}$$

Then the following relations hold:

$$ga = u(v^2 - 2uv + 3u^2), \quad gd = v^3 - uv^2 + u^2v - u^3.$$

If a and d can be represented in this form, then $A_3(x)$ is reducible.

As in the case of $A_2(x)$, there are instances where multiple values of a exist for a single d such that $A_3(x)$ is reducible, but the general law governing this is unknown. For example, when $d = 265, 365, 3445$, there are two values for a. These values of d share the property that their prime factors are all congruent to 1 modulo 4. However, the condition that all prime factors are congruent to 1 modulo 4 does not guarantee the existence of such an a. Furthermore, multiple values of a can

appear even when d contains prime factors like 2 or 3 (or others not congruent to 1 modulo 4), as seen in $d = 14794$ or $d = 241995$. The smallest d for which three values of a exist is $d = 32045$. At present, the largest number of such values of a observed is four; one example is $d = 235855985$. In this case, reducibility occurs as shown by the following factorizations:

$$(292x + 701)(337809x^2 + 334562x + 1150083) \quad (a = 98640228)$$
$$(649x + 854)(884427x^2 + 84050x + 1500657) \quad (a = 573993123)$$
$$(2002x + 2031)(8016849x^2 + 1682x + 8250763) \quad (a = 16049731698)$$
$$(4854x + 4859)(47122657x^2 + 50x + 47219787) \quad (a = 228733377078)$$

It is not yet known whether $d = 235855985$ is minimal or not among those admitting four. To date, no d has been found for which five or more values of a exist.

For $m = 4$, we prove the following result.

Theorem 4. *Let a and d be coprime positive integers with $a \geq d$. The polynomial*

$$A_4(x) = ax^4 + (a + d)x^3 + (a + 2d)x + (a + 3d)x + (a + 4d)$$

cannot be factored as a product of two quadratic polynomials over $\mathbb{Z}[x]$.

Proof. Suppose, for contradiction, that there exist rational numbers p, q, r, s such that

$$A_4(x) = a(x^2 + px + q)(x^2 + rx + s).$$

Setting $t = d/a$, we obtain

$$\begin{cases} p + r = 1 + t, \\ pr + q + s = 1 + 2t, \\ ps + qr = 1 + 3t, \\ qs = 1 + 4t. \end{cases}$$

If $q = s$, then the system reduces to

$$p + r = 1 + t, \quad pr + 2q = 1 + 2t, \quad q(p + r) = 1 + 3t, \quad q^2 = 1 + 4t,$$

so that

$$q^2 = \left(\frac{1 + 3t}{1 + t}\right)^2 = 1 + 4t.$$

Expanding yields

$$1 + 6t + 9t^2 = 1 + 6t + 9t^2 + 4t^3,$$

which is impossible since $t > 0$. Hence $q \neq s$. Solving the first and third equations for p and r gives

$$p = -\frac{q - 1 + (q - 3)t}{s - q}, \quad r = \frac{s - 1 + (s - 3)t}{s - q},$$

and from the fourth equation we have $t = \frac{qs-1}{4}$. Substituting these into the second equation yields

$$\begin{aligned} q^3s^3 - 3q^3s^2 + 8q^3s - 16q^3 - 3q^2s^3 - q^2s^2 + 6q^2s + 8q^2 \\ + \ 8qs^3 + 6qs^2 - qs - 3q - 16s^3 + 8s^2 - 3s + 1 = 0. \end{aligned}$$

Let $u = q + s$ and $v = qs$. Then the above equation becomes

$$v^3 - 3uv^2 - 17v^2 + 8u^2v + 54uv - 17v - 16u^3 + 8u^2 - 3u + 1 = 0.$$

Now set $w = u - 2$ and $z = v - u + 1$. This transforms the equation into

$$-10w^3 + 5w^2z - 20w^2 + 40wz + z^3 - 20z^2 + 80z = 0.$$

If $z = 0$, then $w = 0$ or $w = -2$. Since $q \neq s$, we must have $w = -2$, and hence

$$t = \frac{v-1}{4} = \frac{u-2}{4} = \frac{w}{4} = -\frac{1}{2},$$

contradicting $t > 0$. Thus $z \neq 0$. Define

$$X = \frac{w}{z}, \qquad Y = \frac{1}{z}.$$

Dividing the previous equation by z^3 yields

$$80Y^2 - 20(X-1)^2Y - (10X^3 - 5X^2 - 1) = 0.$$

Since $p, q, r, s \in \mathbb{Q}$, we have $X, Y \in \mathbb{Q}$. Viewing this as a quadratic equation in Y, let $\mathcal{D}$ denote its discriminant. Then

$$\mathcal{D} = 80(5X^4 + 20X^3 + 10X^2 - 20X + 1) = 80\{5(X^2 + 2X - 1)^2 - 4\}$$

must be a square in $\mathbb{Q}$. Hence there exists $Z \in \mathbb{Q}$ such that

$$5(X^2 + 2X - 1)^2 - 4 = 5Z^2.$$

Write $X + 1 = A/B$ and $Z = C/D$ with coprime integers A, B and C, D. Clearing denominators gives

$$5D^2(A^2 - 2B^2)^2 - 5B^4C^2 = 4B^4D^2.$$

In particular, $5 \mid B$ or $5 \mid D$. If $5 \mid B$, write $B = 5B_1$. Then

$$D^2(A^2 - 50B_1^2)^2 - 625B_1^4C^2 = 500B_1^4D^2.$$

Reducing modulo 5 gives $A^4D^2 \equiv 0 \pmod 5$. Since $\gcd(A, B) = 1$, we have $5 \nmid A$, hence $5 \mid D$.

Conversely, if $5 \mid D$, write $D = 5D_1$. Then

$$25D_1^2(A^2 - 2B^2)^2 - B^4C^2 = 20B^4D_1^2.$$

Reducing modulo 5 yields $B^4C^2 \equiv 0 \pmod 5$. Since $\gcd(C, D) = 1$, we have $5 \nmid C$, hence $5 \mid B$. Therefore $5 \mid B$ and $5 \mid D$. In particular, $5 \nmid A$ and $5 \nmid C$. Write $B = 5B_1$ and $D = 5D_1$; substituting into the cleared equation gives

$$D_1^2(A^2 - 50B_1^2)^2 - 25B_1^4C^2 = 500B_1^4D_1^2.$$

Reducing modulo 5 shows $5 \mid D_1$, so write $D_1 = 5D_2$. Then

$$B_1^4C^2 = A^4D_2^2 - 100A^2B_1^2D_2^2 + 2000B_1^4D_2^2.$$

Set

$$\mathcal{X} = \frac{A}{B_1}, \quad \mathcal{Y} = \frac{C}{D_2}.$$

Dividing by $B_1^4D_2^2$ yields

$$\mathcal{Y}^2 = \mathcal{X}^4 - 100\mathcal{X}^2 + 2000.$$

Letting $x = \mathcal{X}^2$ and $y = \mathcal{X}\mathcal{Y}$, we obtain the elliptic curve

$$y^2 = x^3 - 100x^2 + 2000x.$$

According to the L-functions and Modular Forms Database (LMFDB) [4], this curve has rank 0 and its only rational point is $(0, 0)$. However, $(x, y) = (0, 0)$ implies $\mathcal{X} = 0$, and then $\mathcal{Y}^2 = 2000$, contradicting $\mathcal{Y} \in \mathbb{Q}$. □

References

[1] A. Borisov, M. Filaseta, T. Y. Lam, and O. Trifonov, Classes of polynomials having only one non-cyclotomic irreducible factor, *Acta Arith.* **90(2)** (1999), 121–153.

[2] G. Eisenstein, Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt, *J. Reine Angew. Math.* **39** (1850), 160–179.

[3] H. Kakuma, The location of zeros and irreducibility of Fibonacci-coefficient polynomials, *Fibonacci Quart.* **63** (2025), 570–587.

[4] LMFDB Collaboration, Elliptic curve with LMFDB label 200.d2 (Cremona label 200d1) [Internet], 2025, `https://www.lmfdb.org/EllipticCurve/Q/200/d/2` (cited 2025 Oct 21).

[5] M. R. Murty, Prime numbers and irreducible polynomials, *Amer. Math. Monthly* **109** (2002), 452–458.

[6] O. Perron, Neue Kriterien für die Irreduzibilität algebraischer Gleichungen, *J. Reine Angew. Math.* **132** (1907), 288–307.

[7] G. Pólya, Verschiedene Bemerkungen zur Zahlentheorie, *Jahresber. Dtsch. Math.-Ver.* **28** (1919), 31–40.