# Cyclotomic statistics

Lola Thompson

*For Helmut Maier on the occasion of his seventieth birthday*

**Abstract** Cyclotomic polynomials are a family of irreducible polynomials with integer coefficients whose roots lie on the unit circle. They have been studied since at least the time of Gauss. A number of papers from the last 150 years have focused on the coefficients of cyclotomic polynomials. In this survey article, we discuss what is currently known about the maximal coefficients (in absolute value) of cyclotomic polynomials.

## 1 Introduction

Cyclotomic polynomials are a seemingly simple family of polynomials that arise in many areas of mathematics. The name *cyclotomic* is derived from the Greek words κύκλος, meaning "circle," and τόμος, a "part which is cut." One obtains the roots of cyclotomic polynomials by cutting the unit circle into equal parts. This results in roots of the form

$$\zeta^k = e^{2\pi ik/n} = \cos\left(\frac{2\pi ik}{n}\right) + i\sin\left(\frac{2\pi ik}{n}\right),$$

for $k = 0, \ldots, n-1$. A root is called *primitive* if it generates all of the other roots, i.e., if $\gcd(n,k) = 1$. We define the $n^{th}$ *cyclotomic polynomial* by taking the product of all of the $n^{th}$ primitive roots of unity:

L. Thompson
Mathematisch Instituut, Universiteit Utrecht
e-mail: L.Thompson@uu.nl

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(n,k)=1}} (x - e^{2\pi ik/n}).$$

By taking the product over *all* of the $n^{th}$ roots (including the non-primitive roots), we obtain the following useful identity:

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Although the cyclotomic polynomials are formed by taking products of complex roots, it turns out that cyclotomic polynomials all have integer coefficients. It follows immediately from the definition of the Euler totient function, and the definition of the $n^{th}$ cyclotomic polynomial, that $\Phi_n(x)$ has degree $\varphi(n)$. Moreover, the cyclotomic polynomials are all irreducible in $\mathbb{Z}[x]$.

The fact that the cyclotomic polynomials are irreducible is nontrivial to show, and has a long history. It was proven in the case where $n$ is prime by Gauss (1801), Kronecker (1845), Schönemann (1846), and Eisenstein (1850). General proofs for composite $n$ were later given by Dedekind (1857), Landau (1929), and Schur (1929). These proofs have been collected by Weintraub in [57]. We may therefore conclude that the irreducible divisors of $x^n - 1$ in $\mathbb{Z}[x]$ are precisely the $d^{th}$ cyclotomic polynomials, for values of $d$ dividing $n$. As a result, every divisor of $x^n - 1$ in $\mathbb{Z}[x]$ is a product of distinct cyclotomic polynomials. Moreover, every product of distinct cyclotomic polynomials is a divisor of $x^n - 1$ for some positive integer $n$.

Cyclotomic polynomials have been a subject of study since at least 1798. In that year, Carl Friedrich Gauss wrote his *Disquisitiones Arithmeticae*, in which the final chapter discusses cyclotomic polynomials in the context of determining which regular polygons can be constructed using a compass and straightedge [23]. Since then, we have seen the cyclotomic polynomials appear in many other contexts.

In the 19th century, cyclotomic polynomials turned out to be important objects in Galois theory. This is perhaps unsurprising, since Galois theory is often used to prove that certain geometric objects are not constructible using a straightedge and compass. Due to their central role in Galois theory, cyclotomic polynomials now feature prominently in the mathematics curriculum for bachelor's students. The $n^{th}$ cyclotomic polynomial is the minimal polynomial for $e^{2\pi i/n}$. The cyclotomic polynomials provide a simple illustration of Galois theory: the automorphisms sending a fixed primitive $n^{th}$ root of unity to other primitive $n^{th}$ roots of unity are in bijection with the elements of $(\mathbb{Z}/n\mathbb{Z})^\times$.

In the 20th century, we saw that cyclotomic polynomials and their products form an infinite family of polynomials with trivial Mahler measure [48]. In the 21st century, cyclotomic polynomials have even arisen in lattice-based cryptography (see, for example, [18], [37], [44], [25]).

The focus of this survey article will be on the coefficients of cyclotomic polynomials. Let us first examine some concrete examples of cyclotomic polynomials.

$$\begin{aligned}
\Phi_1(x) &= x-1\\
\Phi_2(x) &= x+1\\
\Phi_3(x) &= x^2+x+1\\
\Phi_4(x) &= x^2+1\\
\Phi_5(x) &= x^4+x^3+x^2+x+1\\
\Phi_6(x) &= x^2-x+1\\
\Phi_7(x) &= x^6+x^5+x^4+x^3+x^2+x+1\\
\Phi_8(x) &= x^4+1\\
\Phi_9(x) &= x^6+x^3+1\\
\Phi_{10}(x) &= x^4-x^3+x^2-x+1\\
\Phi_{11}(x) &= x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1\\
\Phi_{12}(x) &= x^4-x^2+1
\end{aligned}$$

At first glance, it appears that all coefficients of cyclotomic polynomials belong to the set $\{-1,0,1\}$. Indeed, the first 104 cyclotomic polynomials all have this property. In 1883, Migotti [42] showed that $\Phi_{105}(x)$ is the first cyclotomic polynomial to have a new coefficient:

$$\begin{aligned}
\Phi_{105}(x) = x^{48}+x^{47}+x^{46}-x^{43}-x^{42}-\mathbf{2}x^{41}-x^{40}-x^{39}+x^{36}+x^{35}\\
+x^{34}+x^{32}+x^{31}-x^{28}-x^{26}-x^{24}-x^{22}-x^{20}+x^{17}+x^{16}+x^{15}\\
+x^{14}+x^{13}+x^{12}-x^9-x^8-\mathbf{2}x^7-x^6-x^5+x^2+x+1.
\end{aligned}$$

The fact that the new coefficient appearing in $\Phi_{105}(x)$ has absolute value 2 leads to the natural question, "How do the coefficients grow (in absolute value) as $n$ increases?" At the same time, the wealth of examples of cyclotomic polynomials with only $\pm 1,0$ as coefficients leads to a different natural question: "Are there infinite families of cyclotomic polynomials with coefficients only coming from the set $\{-1,0,1\}$?" It is easy to see that $\Phi_p(x) = \sum_{i=0}^{p-1} x^i$ for every prime $p$, so all of its coefficients are $+1$. We will exclude these trivial cases from our discussion. Instead, we will look at those $\Phi_n(x)$ where $n$ has at least two prime factors.

The fact that $\Phi_{105}(x)$ is the first cyclotomic polynomial with nontrivial coefficients is not a lucky accident: $105 = 3\cdot 5\cdot 7$, a product of three distinct odd primes. In the same paper in which Migotti described his observation about the coefficients of $\Phi_{105}(x)$, he also proved that, if $n = pq$ with $p$ and $q$ distinct odd primes, then all of the coefficients of $\Phi_n(x)$ lie in the set $\{-1,0,1\}$. In fact, the values of the coefficients of $\Phi_{pq}(x)$ can be described completely explicitly for any pair of primes $p$ and $q$ (see, for example, Theorem 2.3 in [52]). As we saw in the examples above, the height of a cyclotomic polynomial $\Phi_n(x)$ does not increase if we multiply $n$ by powers of 2. Similarly, the height is not impacted by multiplying $n$ by extra copies of primes that already appear in its factorization. As a result, studying heights of

cyclotomic polynomials amounts to studying heights of those $\Phi_n(x)$ for which $n$ is odd and squarefree. Once we restrict our view to only the cyclotomic polynomials $\Phi_n(x)$ where $n$ is a product of at least three distinct odd primes, it is clear that $\Phi_{105}(x)$ was the first cyclotomic polynomial that ever had any chance of having a nontrivial height.

With our motivating questions in mind, we will now formally define our main objects of study.

**Definition 1.** The *height* of $\Phi_n(x)$ is the largest coefficient in absolute value.

We shall denote the height of $\Phi_n(x)$ by $A(n)$ or $H(\Phi_n(x))$, depending on the context. As we saw above, the complexity of the coefficient behaviour is a function of the number of distinct odd prime factors of $n$. As a result, it makes sense to measure the height in terms of $\omega(n)$, the number of distinct prime factors of $n$, rather than comparing it directly with $n$.

Since the maximal coefficient in absolute value of $\Phi_n(x)$ is called its height, it seems logical to call a cyclotomic polynomial without any height "flat." In other words:

**Definition 2.** A cyclotomic polynomial is *flat* if it has height 1.

In Section 2, we will discuss what is known about flat cyclotomic polynomials. In Section 3, we will look at extreme behaviour versus typical behaviour of the cyclotomic polynomial height function. In Section 4, we will examine a related function, $B(n)$, which looks at the maximal height over all divisors of $x^n - 1$. In Section 5, we conclude by considering the question of whether every positive integer appears as a height of some cyclotomic polynomial. This question is currently open. Nevertheless, some progress has been made in this direction, and we will discuss the current state-of-affairs.

## 2 Flat cyclotomic polynomials

When discussing flat cyclotomic polynomials $\Phi_n(x)$, it often makes sense to categorize them in terms of the factorization of $n$. When $n$ has two distinct odd prime factors, we will refer to $\Phi_n(x)$ as a *binary cyclotomic polynomial*, or a *cyclotomic polynomial of order 2*. Likewise, when $p,q,r$ are distinct odd primes, we will call $\Phi_{pqr}(x)$ a *ternary cyclotomic polynomial*, or a *cyclotomic polynomial of order three*. Of course, these notions can be generalized to cyclotomic polynomials with higher orders. However, as we will see, much less is known about cyclotomic polynomials with orders greater than three.

As noted in Section 1, Migotti showed in 1883 that all cyclotomic polynomials of order two are flat. The situation already becomes substantially trickier for cyclotomic polynomials of order 3. While a number of infinite families of flat cyclotomic polynomials of order three have been constructed, there is still no complete classification of all flat cyclotomic polynomials of order three. The first to confirm the

existence of infinite families of flat ternary cyclotomic polynomials was Beiter [13], who showed that there are infinitely many primes $3 < p < q$ such that $\Phi_{3pq}(x)$ is flat. Bachman [2] constructed additional infinite families of flat cyclotomic polynomials of order three in 2006. He proved that, for any prime $p > 5$, there exist infinitely many pairs of primes $(q,r)$ such that $\Phi_{pqr}(x)$ is flat. Kaplan [29] later improved this by proving that for any odd primes $p$ and $q$, there are infinitely many primes $r$ such that $\Phi_{pqr}(x)$ is flat. In particular, he showed that $\Phi_{pqr}(x)$ is flat for all primes $p < q < r$ with $r \equiv \pm 1 \pmod{pq}$.

Kaplan [30] was also the first to prove that there are infinitely many flat cyclotomic polynomials of order four. Flat cyclotomic polynomials seem to get sparser as their order increases. As an example, computations of Arnold and Monagan [1] show that there are only 1389 squarefree integers $n$ with four distinct odd prime divisors that generate flat $\Phi_n(x)$ for $n < 3 \cdot 10^8$. A quick computation in Sage shows that the number of squarefree integers with four distinct odd prime divisors up to $3 \cdot 10^8$ is 18561166, so only about 0.007% of these integers generate flat cyclotomic polynomials.

No flat cyclotomic polynomials of order five have been found at this point, and it has been conjectured that none exist.

## 3 Cyclotomic polynomials with nontrivial heights

In contrast to flat cyclotomic polynomials, there are cyclotomic polynomials that can have arbitrarily large heights. This was already known to Schur, who mentioned it in an unpublished letter to Landau in 1931 (see [34]). Let us begin by examining some data on the first instances of each positive integer as a height of a cyclotomic polynomial:

| $A$ | First $n$ with $H(\Phi_n(x)) = A$ | $\omega(n)$ |
|---|---|---|
| 2 | 105 | 3 |
| 3 | 385 | 3 |
| 4 | 1365 | 4 |
| 5 | 1785 | 4 |
| 6 | 2805 | 4 |
| 7 | 3135 | 4 |
| 8 | 6545 | 4 |
| 9 | 10465 | 4 |
| 10 | 11305 | 4 |
| 11 | 17255 | 4 |
| 12 | 20615 | 4 |
| 13 | 26565 | 5 |
| 14 | 40755 | 5 |
| 15 | 106743 | 5 |
| 16 | 171717 | 5 |
| 17 | 255255 | 6 |
| 18 | 279565 | 5 |
| 19 | 327845 | 5 |
| 20 | 707455 | 5 |

Here, $H(\Phi_n(x))$ denotes the height of the $n^{th}$ cyclotomic polynomial, and $\omega(n)$ denotes the number of distinct prime factors of $n$. The data in the middle column comes from OEIS Entry A160340 (see [60]). This table illustrates the relationship between cyclotomic polynomial heights $A(n)$ and the number of prime factors of the corresponding integers $n$. In our discussion of $A(n)$, we will distinguish between several settings: cyclotomic polynomials $\Phi_n(x)$ where $n$ has a specific structure (e.g., $n$ is a product of three distinct odd primes) versus general results that hold for any cyclotomic polynomials. We will also look at the extreme behaviour of $A(n)$ (i.e., bounds that hold for any $n$) versus the typical behaviour of $A(n)$ (i.e., bounds that hold for almost all $n$).

## *3.1 Ternary cyclotomic polynomials*

There has been a great deal of literature on bounding the magnitude of the largest coefficient of ternary cyclotomic polynomials. The earliest work in this area is due to Bang [6], who proved in 1895 that the height of $\Phi_{pqr}(x)$ is at most $p-1$. This bound was subsequently improved independently by Beiter [11] and Bloom [14] in 1968, who obtained an upper bound of $(p+1)/2$ in the special case where $q$ or $r$ is congruent to $\pm 1 \pmod{p}$. Beiter, who was a Catholic nun teaching mathematics at a high school, also conjectured in [12] that this is the best possible upper bound that holds in general. This became known as the Sister Beiter Conjecture.

Subsequent work by Beiter [12], Möller [43] and Bachman [2] provided a great deal of evidence towards Beiter's conjecture. In 2003, Bachman [2] provided a second infinite family of examples that support Beiter's conjecture, namely the cyclotomic polynomials $\Phi_{pqr}(x)$ with $q$ or $r$ congruent to $\pm 2 \pmod{p}$. In 2009, Kaplan [31] obtained a periodicity result; he showed that, if $s > q$ is a prime with $s \equiv \pm r \pmod{pq}$, then $A(pqr) = A(pqs)$. In the same paper, he proved a technical lemma that explicitly relates the coefficients of $\Phi_{pqr}(x)$ to those of $\Phi_{pq}(x)$.

Gallott and Moree [20] used Kaplan's lemma in order to construct an infinite family of counterexamples to Beiter's conjecture. They showed that

$$A(pqr) > (p+1)/2$$

holds for each $p \geq 11$ and for infinitely many values of $q$ and $r$. In the same paper, they devised a "corrected" version of Beiter's conjecture.

*Conjecture 1 (Corrected Sister Beiter Conjecture).* Let $p < q < r$ be distinct odd primes. Then $A(pqr) \leq \frac{2}{3}p$.

Gallot and Moree [20] showed that there exist triples $p < q < r$ with $p$ arbitrarily large for which $A(pqr) > (\frac{2}{3} - \varepsilon)p$ for $\varepsilon > 0$, which means that the conjectured upper bound is optimal if it is true. In 2010, Bzdęga [9] obtained density results on polynomials $\Phi_{pqr}(x)$ with $A(pqr) \leq cp$. In particular, with $p$ fixed, he showed that at least $\frac{25}{27} + O(\frac{1}{p})$ of the polynomials $\Phi_{pqr}(x)$ satisfy the conjectured bound of Gallot and Moree. More recently, Luca, Moree, Osburn, Saad Eddin, and Sedunova [36] showed in 2019 that the corrected version of Beiter's conjecture holds for at least $25/27$ of the ternary integers. In 2023, Juran, Moree, Riekert, Schmitz, and Völlmecke [27] gave a proof of the Corrected Sister Beiter Conjecture. Their proof fleshes out an approach that Zhao and Zhang [59] gave back in 2009 that turned out to be correct. Unfortunately, the paper of Zhao and Zhang was never accepted for publication, likely because some of the arguments were difficult to follow. With the new details provided by Juran et al in [27], it is finally clear that the Corrected Sister Beiter Conjecture can now be called the Corrected Sister Beiter Theorem.

For cyclotomic polynomials with orders larger than three, not much is currently known. Felsch and Schmidt [19] and Justin [28] independently showed in 1967/8 that for $p_1 < \cdots < p_s$ odd primes, $A(p_1, ..., p_s)$ has an upper bound that does not depend on $p_{s-1}$ or $p_s$ (in other words, the two largest prime factors of $n$ do not affect the upper bound for $A(n)$). Bloom [14] showed in 1968 that

$$A(pqrs) \leq p(p-1)(pq-1),$$

for odd primes $p < q < r < s$. This was improved by Bzdęga in 2012, who showed that

$$A(pqrs) \leq \frac{3}{4}p^3 q.$$

He was also able to obtain upper bounds for fifth- and sixth-order cyclotomic polynomials, where $n$ factors into odd primes $p < q < r < s < t < u$. He showed

$$A(pqrst) \leq \frac{135}{512} p^7 q^3 r, \qquad A(pqrstu) \leq \frac{18225}{262144} p^{15} q^7 r^3 s.$$

It is unclear whether these bounds are anywhere close to being sharp.

### 3.2 Cyclotomic polynomials without restrictions on $n$

Instead of restricting ourselves to heights of ternary (or quaternary) cyclotomic polynomials, we can consider heights of $\Phi_n(x)$ for integers $n$ with an arbitrary but fixed number of prime factors. Erdős [17] showed that the height function, $A(n)$, is not bounded above by any polynomial function of $n$. In other words, for any constant $c > 0$, there exists an integer $n$ such that $A(n) > n^c$.

Bateman [7] was the first to obtain a bound for $\Phi_n(x)$ with $n$ having $k$ distinct odd prime factors, where $k$ ranges over all positive integers. He gave a simple argument in 1949 which showed that the height of $\Phi_n(x)$ is at most $n^{2^{k-1}}$. There were a number of improvements on Bateman's result in papers of Vaughan [54] and Bateman, Pomerance, and Vaughan [8], the latter of which gives an upper bound of $n^{\frac{2^{k-1}}{k}-1}$. In the same paper, Bateman, Pomerance and Vaughan show that $A(n) \geq n^{\frac{2^{k-1}}{k}-1}/(5\log n)^{2^{k-1}}$ holds for infinitely many $n$ with exactly $k$ distinct odd prime factors. Moreover, under the assumption of the prime $k$-tuples conjecture, they show that for each $k$ there exists a constant $c_k$ such that $A(n) \geq c_k n^{\frac{2^{k-1}}{k}-1}$ holds for infinitely many $n$ with exactly $k$ distinct odd prime factors. We can re-state these results without the dependence on $k$ by using the fact that the maximal order of $\omega(n)$ is $\frac{\log n}{\log\log n}$. This yields an upper bound of

$$A(n) \leq e^{n^{(\log 2 + o(1))/\log\log n}}$$

that holds for all positive integers $n$, as well as a lower bound of

$$A(n) \geq e^{n^{(\log 2 + o(1))/\log\log n}}$$

that holds for infinitely many values of $n$. In other words, if the prime $k$-tuples conjecture is true, their result is best possible.

### 3.3 Extreme versus typical heights

Maier showed in a pair of papers [38] and [40] that stronger results can be obtained for "typical" $n$; that is, for all $n$ except for an exceptional set with asymptotic density 0. In particular, let $\psi(n), \varepsilon(n)$ be functions defined for all positive integers such that $\psi(n) \to \infty$ and $\varepsilon(n) \to 0$ as $n \to \infty$. Maier proved that the inequalities

$$n^{\varepsilon(n)} \leq A(n) \leq n^{\psi(n)}$$

hold for almost all $n$. This settled a longstanding question of Erdős [52].

Maier's upper bound was published in 1990, while the lower bound came only in 1996. In the intervening time, Maier showed that his upper bound was best possible in [39]. Namely, he showed that for any positive constant $C$, it is the case that

$$A(n) \geq n^C$$

on a set of positive lower density. Maier's lower bound was improved several times over the next decade, first by Maier himself. Recall that $A(n)$ is actually a function of $\omega(n)$, and that $\omega(n)$ has average order $\log\log n$. Maier showed in [41] that for every constant $C > 2/\log 2$, if $\mathscr{E}_C$ is the set of squarefree integers $n$ with $\omega(n) \geq C\log\log n$, then for every $\varepsilon > 0$, the inequality

$$A(n) > \exp((\log n)^{(C\log 2)/2-\varepsilon})$$

holds for almost all $n \in \mathscr{E}_C$. This result was improved in 2004 by Konyagin, Maier, and Wirsing [32], who showed that the result holds, in fact, for all $n$ with $\omega(n) \geq C\log\log n$. In other words, $A(n)$ is large when $n$ has more than the average number of distinct prime factors.

## 4 A generalization: from $A(n)$ to $B(n)$

So far, we have only been considering heights of cyclotomic polynomials, but we can broaden our gaze to other families of (related) polynomials. If $f(x)$ is any polynomial with integer coefficients, let $H(f)$ denote its maximum coefficient in absolute value. We can then define $B(n) = \max\{H(f) : f(x) \mid x^n - 1, f(x) \in \mathbb{Z}[x]\}$. In particular, $A(n) \leq B(n)$ since $\Phi_n(x)$ divides $x^n - 1$ and $B(n)$ is the maximum height over all divisors of $x^n - 1$. In general, much less is known about $B(n)$ than $A(n)$. The first result concerning $B(n)$ is due to Justin [28], who showed in 1969 that $B(n)$ has an upper bound that does not depend on the size of the largest prime factor of $n$. In 2005, Pomerance and Ryan [45] proved that as $n \to \infty$,

$$\log B(n) \leq n^{(\log 3+o(1))/\log\log n}.$$

They also showed that this inequality can be reversed for infinitely many $n$. In 2009, Kaplan [31] gave a formula for $B(n)$ when $n = p^2q$, showing that $B(p^2q) = \min\{p^2, q\}$. He also gave upper and lower bounds for $B(pqr)$, showing that

$$\frac{1}{3}(3p^2q - p^3 + 7p - 6) \leq B(pqr) \leq p^2q^2.$$

Decker and Moree [15] took Kaplan's work a step further in 2013, determining which coefficients occur for each divisor of $x^n - 1$ when $n = p^2q$. In 2010, Ryan,

Ward, and Ward [46] did some computations for $B(n)$ and derived a number of conjectures about $B(n)$ for $n$ with certain specific shapes (e.g., $n = pq^b$) based on the data that they generated. Some of their conjectures were subsequently proven by Wang [56] in 2015.

As in the previous section, we can also step away from integers $n$ with specific forms, and instead consider $B(n)$ for any positive integer $n$. In 2009, Kaplan [31] showed that if $n = p_1^{e_1} \cdots p_k^{e_k}$ where $p_1 < \cdots < p_k$ and $e_1, ..., e_k \geq 1$ then, for $k \geq 2$, we have

$$B(n) < \prod_{i=1}^{k-1} p_i^{4 \cdot 3^{k-2} \cdot E - e_i},$$

where $E := \prod_{j=1}^{k} e_j$. Kaplan's upper bound was later improved by Zhang [58] in 2019, who showed that

$$B(n) < (2/5)^{\prod_{i=2}^{k} e_i} \prod_{i=1}^{k-1} p_i^{4 \cdot 3^{k-2} E - e_i}.$$

A less-precise but perhaps more palatable upper bound was given by Bzdęga [10] in 2012, who showed that

$$B(n) < (C + o(1))^{3^k} n^{(3^k-1)/(2k)-1}$$

as $k \to \infty$, where $C$ is an effectively computable constant less than 1. On the other hand, lower bounds were given by Ryan, Ward, and Ward [46], who showed that

$$B(n) \geq \min\{p_1^{e_1}, ..., p_k^{e_k}\}.$$

One can also ask about the "typical" behaviour of $B(n)$, as Maier did with $A(n)$. In that direction, we have the following theorem of Thompson [53]. Let $\tau(n)$ denote the count of divisors function, and let $\psi(n)$ be a function defined for all positive integers such that $\psi(n) \to \infty$ as $n \to \infty$. Then $B(n) \leq n^{\tau(n)\psi(n)}$ for almost all $n$, i.e., for all $n$ except for a set with asymptotic density 0. It is not yet known whether this upper bound for $B(n)$ is best possible.

## 5 Open questions

In spite of the preponderance of research on heights of cyclotomic polynomials, there is a great deal that is still not known. For example, it is natural to ask whether every positive integer can be a height of a cyclotomic polynomial. In other words, for any positive integer $h$, is there a positive integer $n$ such that $A(n) = h$? We still do not know the answer to this question, although there is a great deal of evidence that suggests that the answer is "yes."

What we do know is that every positive integer is a coefficient of some cyclotomic polynomial, thanks to a 1987 paper of Suzuki [51]. This property even holds

if we restrict ourselves to the set of ternary cyclotomic polynomials, as Bachman showed in [3]. Moreover, we know that, if there are any exceptions, these exceptions live in a subset of the integers with asymptotic density zero. In particular, Kosyak, Moree, Sofos and Zhang [33] showed in 2021 that as $x$ goes to infinity, the number of "bad" $h \leq x$ is $O_\varepsilon(x^{3/5+\varepsilon})$. Their work uses deep recent results about the distribution of primes. Using a more elementary approach, Bachman, Bao, and Wu [5] showed in 2023 that, for any positive integer $h$, either $h$ or $h+1$ is a height of some ternary cyclotomic polynomial.

A number of open questions are also alluded to in previous sections of this survey. We summarize them here for convenience. We saw in Section 2 that we still do not have a complete classification of flat ternary cyclotomic polynomials. Even less is known about cyclotomic polynomials of order four and higher. In particular, we still do not know whether there are any flat cyclotomic polynomials of order five. We also (likely) do not have good upper bounds for $A(n)$ when $\Phi_n(x)$ has order four, five, six, etc. The function $B(n)$, which is the maximal height over all products of cyclotomic polynomials dividing $x^n - 1$, remains mysterious, in part because it becomes difficult to compute rather quickly.

There are many other directions that can be taken with cyclotomic polynomials that were not discussed in this survey. For example, one can also study the values that cyclotomic polynomials take at different inputs. On the other hand, there are a number of papers that look at inverse cyclotomic polynomials, where the $n^{th}$ inverse cyclotomic polynomial is obtained by taking $x^n - 1$ and dividing it by $\Phi_n(x)$. Inverse cyclotomic polynomials have also given rise to cryptographic applications (see, for example, [26], [16]). In addition, there are papers that focus on the values that the $k^{th}$ coefficient of $\Phi_n(x)$ can assume as $n$ ranges over the positive integers, or on cyclotomic polynomials with neighbouring terms that jump by at most one (the so-called "jump one" property). See, for example, [22], [24], [21]. For other surveys on cyclotomic polynomials, see the 1979 survey by Lenstra [35], the 1989 survey by Vaughan [55], the 2000 survey by Thangadurai [52], and the 2022 survey by Sanna [47].

## Acknowledgements

I would like to thank the Ross Mathematics Program for sparking my interest in cyclotomic polynomials and my Ph.D. supervisor, Carl Pomerance, for nurturing that interest. I am extremely grateful to Pieter Moree, Harald Helfgott, and Alexandre Kosyak for carefully reading a draft of this manuscript and offering lots of valuable feedback. Lastly, I would like to thank Helmut Maier for providing the impetus for writing this expository article.

## References


1. A. Arnold and M. Monagan, *Calculating cyclotomic polynomials*. Math. Comp. **80** (2011), no. 276, 2359 – 2379.
2. G. Bachman, *On the coefficients of ternary cyclotomic polynomials*. J. Number Theory **100** (2003), 104 – 116.
3. G. Bachman, *Ternary cyclotomic polynomials with an optimally large set of coefficients*, Proc. Amer. Math. Soc. **132** (2004), no. 7, 1943 – 1950.
4. G. Bachman, *Flat cyclotomic polynomials of order three*. Bull. London Math. Soc. **38** (2006), 53 – 60.
5. G. Bachman, C. Bao, S. Wu, *A note on heights of cyclotomic polynomials*. arXiv:2309.03422 [math.NT].
6. A. S. Bang, *Om Ligningen* $\Phi_n(x) = 0$. Nyt Tidsskrift for Mathematik (B) **6** (1895), 6 – 12.
7. P. T. Bateman, *Note on the coefficients of the cyclotomic polynomials*. Bull. Amer. Math. Soc. **55** (1949), 1180 – 1181.
8. P. T. Bateman, C. Pomerance, and R. C. Vaughan, *On the size of the coefficients of the cyclotomic polynomial*. Colloq. Math. Soc. Janos Bolyai **34** (1984), 171 – 202.
9. B. Bzdęga, *Bounds on ternary cyclotomic coefficients*. Acta Arith. **144** (2010), no. 1, 5 –16.
10. B. Bzdęga, On the height of cyclotomic polynomials, Acta Arith. **152** (2012), no. 4, 349 – 359.
11. M. Beiter, *Magnitude of the coefficients of the cyclotomic polynomial* $F_{pqr}(x)$. Amer. Math. Monthly **75** (1968), 370 – 372.
12. M. Beiter, *Magnitude of the coefficients of the cyclotomic polynomial* $F_{pqr}(x)$. *II*. Duke Math. J. **38** (1971), 591 – 594.
13. M. Beiter, *Coefficients of the cyclotomic polynomial* $F_{3qr}(x)$, Fibonacci Quart. **16** (1978), no. 4, 302 – 306.
14. D. M. Bloom, *On the coefficients of the cyclotomic polynomials*. Amer. Math. Monthly **75** (1968), 372 – 377.
15. A. Decker and P. Moree, *Coefficient convexity of divisors of* $x^n - 1$, Sarajevo J. Math. **9** (2013), no. 21, 3 – 28.
16. C. Dunand, *On modular inverses of cyclotomic polynomials and the magnitude of their coefficients*. LMS J. Comput. Math. **15** (2012), 44 – 58.
17. P. Erdős, *On the coefficients of the cyclotomic polynomial*. Bull. Amer. Math. Soc. **52** (1946), 179 – 184.
18. J. Fan, F. Vercauteren, *Somewhat Practical Fully Homomorphic Encryption*. IACR Cryptol. ePrint Arch. 2012: 144 (2012).
19. V. Felsch and E. Schmidt, Über Perioden in den Koeffizienten der Kreisteilungspolynome $F_{np}(x)$, Math. Z. **106** (1968), 267 – 272.
20. Y. Gallot and P. Moree, *Ternary cyclotomic polynomials having a large coefficient*. J. Reine Angew. Math. **632** (2009), 105 – 125.
21. Y. Gallot and P. Moree, *Neighboring ternary cyclotomic coefficients differ by at most one.* J. Ramanujan Math. Soc. **24** (2009), no. 3, 235 – 248.
22. Y. Gallot, P. Moree, and H. Hommersom, *Value distribution of cyclotomic polynomial coefficients*. Unif. Distrib. Theory **6** (2011), no. 2, 177 – 206.
23. C. F. Gauss, *Disqvisitiones Arithmeticae*. Lipsiae, in commission apvd G. Fleischer, jun, 1801. Pdf. Retrieved from the Library of Congress, <www.loc.gov/item/36021572/>.
24. S. Gong, *On a problem regarding coefficients of cyclotomic polynomials*. J. Number Theory **129** (2009), no. 12, 2924 – 2932.
25. S. Halevi, Y. Polyakov, V. Shoup, *An Improved RNS Variant of the BFV Homomorphic Encryption Scheme*. Matsui, M. (eds) Topics in Cryptology – CT-RSA 2019. Lecture Notes in Computer Science, vol **11405**. Springer (2019).
26. H. Hong, E. Lee, H.-S. Lee, C.-M. Park, *Simple and exact formula for minimum loop length in Atei pairing based on Brezing-Weng curves*. Des. Codes Cryptogr. **67** (2013), no. 2, 271 – 292.

27. B. Juran, P. Moree, A. Riekert, D. Schmitz, J. Völlmecke, *A proof of the corrected Sister Beiter cyclotomic coefficient conjecture inspired by Zhao and Zhang* (2023), arXiv:2304.09250 [math.NT].
28. J. Justin, *Bornes des coefficients du polynome cyclotomique et de certains autres polynomes*, C. R. Acad. Sci. Paris Ser. A-B **268** (1969), A995 – A997.
29. N. Kaplan. *Flat cyclotomic polynomials of order three*. J. Number Theory **127** (2007), 118 – 126.
30. N. Kaplan. *Flat Cyclotomic Polynomials of order four and higher*. Integers **10** (2010), 357 – 363.
31. N. Kaplan, *Bounds for the maximal height of divisors of $x^n - 1$*. J. Number Theory **129** (2009), 2673 – 2688.
32. S. Konyagin, H. Maier, and E. Wirsing, *Cyclotomic polynomials with many primes dividing their oders*, Period. Math. Hungar. **49** (2004), no. 2, 99 – 106.
33. A. Kosyak, P. Moree, E. Sofos and B. Zhang, *Cyclotomic polynomials with prescribed height and prime number theory*. Mathematika **67** (2021), 214 – 234.
34. E. Lehmer, *On the magnitude of the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc. **42** (1936), no. 6, 389 – 392.
35. H. W. Lenstra, Jr., *Vanishing sums of roots of unity*, Proceedings, Bicentennial Congress Wiskundig Genootschap (Vrije Univ., Amsterdam, 1978), Part II, Math. Centre Tracts **101**, Math. Centrum, Amsterdam, 1979, pp. 249 – 268.
36. F. Luca, P. Moree, R. Osburn, S. Saad Eddin, and A. Sedunova, *Constrained ternary integers*, Int. J. Number Theory **15** (2019), no. 2, 407 – 431.
37. V. Lyubashevsky, C. Peikert, O. Regev, *On Ideal Lattices and Learning with Errors over Rings*. Gilbert, H. (eds), Advances in Cryptology – EUROCRYPT 2010. Lecture Notes in Computer Science, vol **6110**. Springer, Berlin, Heidelberg.
38. H. Maier, *The coefficients of cyclotomic polynomials*. Proc. Conf. in Honor of Paul T. Bateman, Progr. Math. **85** (1990), 349 – 366.
39. H. Maier, *Cyclotomic polynomials with large coefficients*. Acta Arith. **64** (1993), 227 – 235.
40. H. Maier, *The size of the coefficients of cyclotomic polynomials*, Analytic number theory, Vol. 2 (Allerton Park, IL, 1995), Progr. Math., vol. **139**, Birkhäuser Boston, Boston, MA, 1996, pp. 633 – 639.
41. H. Maier, *Cyclotomic polynomials whose orders contain many prime factors*, Period. Math. Hungar. **43** (2001), no. 1-2, 155 – 164.
42. A. Migotti, *Aur Theorie der Kreisteilungsgleichung*. Z. B. der Math.-Naturwiss, Classe der Kaiserlichen Akademie der Wissenschaften, Wien, **87** (1883), 7 – 14.
43. H. Möller, *Über die Koeffizienten des n-ten Kreisteilungspolynoms*. Math. Z. **119** (1971), 33 – 40.
44. T. Mukherjee, *Cyclotomic polynomials in Ring-LWE homomorphic encryption schemes*. Master's thesis, Rochester Institute of Technology, New York, 2016.
45. C. Pomerance and N. Ryan, *Maximal height of divisors of $x^n - 1$*. Illinois J. Math. **51** no. 2 (2007), 597 – 604 (electronic).
46. N. Ryan, B. Ward, R. Ward, *Some conjectures on the maximal height of divisors of $x^n - 1$*. Involve **3**(4): 451 – 457 (2010).
47. C. Sanna, *A survey on coefficients of cyclotomic polynomials*, Expositiones Mathematicae **40**, no. 3 (2022), 469 – 494.
48. C. Smyth, *The Mahler measure of algebraic numbers: a survey*. McKee J, Smyth C, eds. Number Theory and Polynomials. London Mathematical Society Lecture Note Series. Cambridge University Press (2008), 322 – 349.
49. S. T. Somu, *On the coefficients of divisors of $x^n - 1$*, J. Number Theory **167** (2016), 284 – 293.
50. S. T. Somu, *On the distribution of numbers related to the divisors of $x^n - 1$*, J. Number Theory **170** (2017), 3 – 9.
51. J. Suzuki, *On coefficients of cyclotomic polynomials*. Proc. Japan Acad. Ser. A Math. Sci. **63** (1987), 279 – 280.
52. R. Thangadurai, *On the coefficients of cyclotomic polynomials*. Cyclotomic Fields and Related Topics, Pune, 1999, Bhaskaracharya Pratishthana, Pune (2000), 311 – 322.

53. L. Thompson, *Heights of divisors of* $x^n - 1$. Integers **11A**. Proceedings of the Integers Conference 2009 (2011). Article 20, 1 – 9.
54. R. C. Vaughan, *Bounds for the coefficients of cyclotomic polynomials*, Michigan Math. J. **21** (1974), 289 – 295.
55. R. C. Vaughan, *Coefficients of cyclotomic polynomials and related topics*, Proceedings of the Congress on Number Theory (Spanish) (Zarauz, 1984), Univ. País Vasco-Euskal Herriko Unib., Bilbao, 1989, pp. 43 – 68.
56. S. Wang, *Maximal height of divisors of* $x^{pqb} - 1$, Int. J. Number Theory **11** (2015), no. 1, 67 – 79.
57. S. H. Weintraub, *Several proofs of the irreducibility of the cyclotomic polynomials*, Am. Math. Mon., **120**:6 (2013), 537 – 545.
58. B. Zhang, *A remark on bounds for the maximal height of divisors of* $x^n - 1$, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **62** (110) (2019), no. 2, 209 – 214.
59. J. Zhao and X. Zhang, *A proof of the Corrected Beiter conjecture* (2009), arXiv:0910.2770 [math.NT].
60. OEIS Foundation Inc. (2024), Entry A160340 in The On-Line Encyclopedia of Integer Sequences, https://oeis.org/A160340