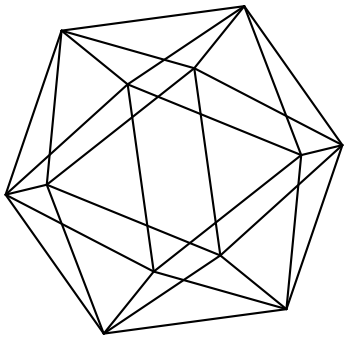
Max-Planck-Institut für Mathematik Bonn

Prime gaps and cyclotomic polynomials

by

Pieter Moree



Max-Planck-Institut für Mathematik
Preprint Series 2021 (50)

Date of submission: November 9, 2021

Prime gaps and cyclotomic polynomials

by

Pieter Moree

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

MPIM 21-50

PRIME GAPS AND CYCLOTOMIC POLYNOMIALS

PIETER MOREE

Abstract. This is the write-up of a talk I gave at the Winter Symposium of the Royal Dutch Mathematical Society on January 9, 2021, which is to appear in the Dutch journal Nieuw Archief voor Wiskunde. It discusses my recent research paper [26] with Kosyak, Sofos and Zhang on finding cyclotomic polynomials with prescribed maximum coefficient and its connections with prime number theory.

1. Cyclotomic polynomials: basics

It is clear that $X^2-1=(X-1)(X+1), X^3-1=(X-1)(X^2+X+1)$ and $X^4-1=(X-1)(X+1)(X^2+1)$. Over the rationals none of the factors can be factorized further and the expressions give the factorization into *irreducibles*. However, it is not so obvious how to factorize X^n-1 for an *arbitrary* integer $n\geq 1$ into *irreducibles* over the rationals in a systematic way.

Over the *complex numbers* the answer is easy:

$$X^n-1=\prod_{m=1}^{n}(X-e^{\frac{2\pi i m}{n}}). \tag{1.1}$$

The roots are the n-th roots of unity and these divide the circle into equal parts. The word *cyclotomy* comes from ancient Greek and literally means circle-cutting. A root of unity ζ is said to be a *primitive* n-th root of unity if it satisfies $\zeta^n=1$, but not $\zeta^d=1$ for any $1\leq d<n$. For any two integers n and d by the Euclidean algorithm we can find integers a and b such that $an+bd=\gcd(n,d)$, where gcd is a shorthand for *greatest common divisor*. Thus if $\zeta^n=1$ and $\zeta^d=1$, it follows that $\zeta^{\gcd(n,d)}=1$. Therefore, in order to check that ζ is a primitive n-th root of unity, it suffices to check that $\zeta^n=1$ and $\zeta^d\neq 1$ for every proper divisor d of n. By a similar argument one deduces that if ζ is a primitive n-th root of unity, then ζ^j is of order $n/\gcd(j,n)$. It follows that all the primitive n-th roots of unity are of the form ζ^j, with $1\leq j\leq n$ and $\gcd(j,n)=1$. There are precisely $\varphi(n)$ primitive n-th roots of unity, where φ is the *Euler totient function*, which is defined as

$$\varphi(n)=\sum_{\substack{j=1\\(j,n)=1}}^{n}1.$$

An obvious primitive n-th root of unity is $e^{2\pi i/n}$.

The n-th *cyclotomic polynomial* can be defined as

$$\Phi_n(X)=\prod_{\substack{j=1\\(j,n)=1}}^{n}(X-e^{\frac{2\pi i j}{n}}). \tag{1.2}$$

Date: September 2021.

n	$\Phi_n(x)$
5	$x^4+x^3+x^2+x+1$
12	x^4-x^2+1
15	$x^8-x^7+x^5-x^4+x^3-x+1$
16	x^8+1
60	$x^{16}+x^{14}-x^{10}-x^8-x^6+x^2+1$
105	$x^{48}+x^{47}+x^{46}-x^{43}-x^{42}-2x^{41}-x^{40}-x^{39}+\ldots+1$
210	$x^{48}-x^{47}+x^{46}+x^{43}-x^{42}+2x^{41}-x^{40}+x^{39}+\ldots+1$
240	$x^{64}+x^{56}-x^{40}-x^{32}-x^{24}+x^8+1$

TABLE 1. Some cyclotomic polynomials

It thus has precisely the n-th order primitive roots of unity as its simple roots. (Note that of all Greek letters Φ looks the most like a cut circle.) The degree of $\Phi_n(X)$ is $\varphi(n)$ and we have $\Phi_n(x) = X^{\varphi(n)} + \ldots$.

By reducing the fractions m/n in (1.1) (e.g., $4/6 = 2/3$), we see that for each divisor d of n there are $\varphi(d)$ reduced fractions with denominator d. These correspond to roots of unity of order d. We thus infer from (1.1) and (1.2) that

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{1.3}$$

Setting $n = 1$ we get $\Phi_1(X) = X - 1$. In case $n = p$ is a prime, we obtain

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \ldots + X + 1.$$

It can be shown that all cyclotomic polynomials have integer coefficients and are irreducible, and so (1.3) gives the factorization of $X^n - 1$ into irreducibles over the rationals. Indeed, many famous mathematicians gave proofs of the irreducibility of the cyclotomic polynomials (Gauss, Kronecker, Eisenstein, Dedekind, Landau, Schur, ...). For some of these proofs, see Weintraub [46]. The (very short) proof of Schur was even set to rhyme! (Cremer [14, p. 39-41]).

Write

$$\Phi_n(x) = \sum_{j=0}^{\varphi(n)} a_n(j) x^j. \tag{1.4}$$

For $j > \varphi(n)$ we put $a_n(j) = 0$. We define

$$A(n) = \max_{k \geq 0} |a_n(k)|, \quad A\{n\} = \{a_n(k) : k \geq 0\},$$

and call $A(n)$ the *height* of Φ_n. Note that, for example, $A\{105\} = \{-2, -1, 0, 1\}$, see Table 1. Our interest is in the possible heights $A(n)$ and extrema of $A\{n\}$ as n runs over the integers.

The cyclotomic coefficients $a_n(j)$ are usually very small. Indeed, in the 19-th century mathematicians even thought that they are always 0 or ± 1. The first counterexample to this claim occurs at $n = 105$; we have $a_{105}(41) = a_{105}(7) = -2$. Issai Schur in a letter to Edmund Landau proved that every negative even number occurs as a coefficient of some cyclotomic polynomial. Emma Lehmer [29] reproduced Schur's argument, which is easily adapted to show that *every* integer is assumed as value of a cyclotomic coefficient [44]. For the best result to date in this direction see Fintzen [17] (found during her Max Planck Insitut für Mathematik (MPIM) internship).

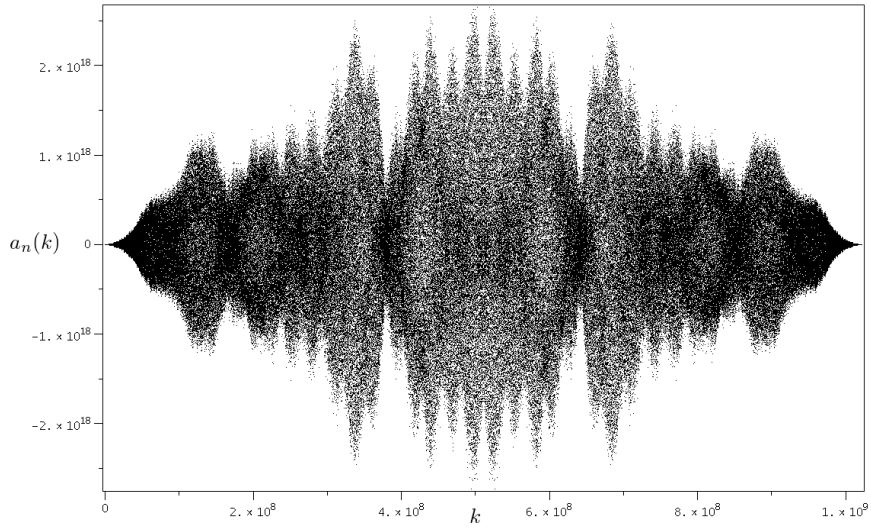


FIGURE 1. Coefficients of the n-th cyclotomic polynomial for $n = 3234846615 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$, cf. [2].

Nowadays computations can be extended enormously far beyond $n = 105$, cf. Figure 1. These and analytic number theoretical considerations show clearly that the complexity of the coefficients is a function of the number of distinct odd prime factors of n, much rather than the size of n. Complex patterns arise (see Figure 1) and a lot of mysteries remain.

2. Which maximum coefficients of cyclotomic polynomials do occur?

The very innocent looking question we consider here is the following.

Question 2.1. *Which integers occur as a maximum coefficient of some cyclotomic polynomial?*

For example, Φ_{210} has 2 as a maximum coefficient. We propose the following conjecture.

Conjecture 2.2. *Every natural number occurs as the maximum coefficient of some cyclotomic polynomial.*

The rest of the paper discusses the progress we made on establishing this conjecture. Surprisingly, a big role in this is played by deep work done by many number theorists on the distribution of gaps between primes. Last but not least, everything hinges on a construction found by Eugenia Roşu [38] during a 2010 MPIM internship, improving on an earlier construction due to Yves Gallot and myself [21].

3. Prime gaps

3.1. **Elementary material, generalities.** For millenia now (some!) humans have been fascinated by prime numbers and their distribution. Recall that *prime numbers* are numbers > 1 only divisible by themselves and 1 (it turns out that it is much better to consider 1 itself not as a prime number). It is usually attributed to Euclid (circa 300 BCE) that he proved there are infinitely many primes. Several formulas producing infinitely many primes are known, but they turn out to be practically useless. A famous example is a result of Mills, which asserts the existence of a real number $A > 1$ with the property that A^{3^n} rounded down to the nearest integer is prime for each natural number n. This first "defeat" forces us to take a step back and

ask less precise questions such as to estimate the *prime counting function* $\pi(x)$, which counts the number of primes p not exceeding x; that is $\pi(x) = \sum_{p \le x} 1$. In the course of answering this, the *stochastic* nature of the prime numbers will become apparent. The notion of an error term will also be involved. If $|f(x)| \le Bg(x)$, for some positive constant B and all values of $x \ge 1$, we write this compactly as $f(x) = O(g(x))$. This notation was introduced by Bachmann in 1894 and popularized by Landau and is generally named *Landau's Big O notation*. Edmund Landau (1877–1938) was the first to put prime number theory as a separate field on the mathematical map and wrote a bulky standard work [28] on it. Two non-Germans mathematicians, who studied the original German version, were surprised to learn about a very strong mathematician called Verfasser they had never heard of (Verfasser means author...).

The first mathematicians to investigate the growth of $\pi(x)$ had of course to start with collecting data to get some intuition for what is going on. They did this by painfully setting up tables of consecutive prime numbers. The most famous of these computers was Carl-Friedrich Gauss. In 1791, when he was 14 years old, he noticed that as one gets to larger and larger numbers the primes thin out, but that locally their distribution appears to be quite erratic. He based himself on a prime number table contained in a booklet with tables of logarithms he had received as a prize, and went on to conjecture that the "probability that an arbitrary integer n is actually a prime number should equal $1/\log n$". Thus Gauss conjectured the following approximations:

$$\pi(x) \approx \sum_{2 \le n \le x} \frac{1}{\log n} \approx \mathrm{Li}(x),$$

where

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t},$$

denotes the *logarithmic integral*. By partial integration one sees that $\mathrm{Li}(x) \sim x/\log x$, where by $A(x) \sim B(x)$ we mean that $\lim_{x\to\infty} A(x)/B(x) = 1$. Thus Gauss's heuristic leads to the conjecture that

$$\pi(x) \sim \frac{x}{\log x}.$$

This was proved much later, in 1896, by Hadamard and independently by de la Vallée-Poussin and is now called the *Prime Number Theorem* (PNT). Both of them were divinely rewarded for doing so and became immortal. Well, almost – they lived to be near centenarians...

If the *Riemann Hypothesis* (RH) were true, it would imply that

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x). \tag{3.1}$$

The RH is one of the Millenium Problems and will not be discussed further here. Its intimate connection with the distribution of prime numbers is discussed in an introductory way in [37].

Prime number questions fall into two main categories: *global problems* and *local problems*. The former concerns asymptotic formulae, sums, estimations and the like of $\pi(x)$ and related functions (of which the PNT is an example), while local problems involve questions dealing with the individual primes. Our focus here will be on large differences between primes (a local property) and their applications.

We let p_n denote the n-th prime number and put $d_n := p_{n+1} - p_n$. For example, the first few prime numbers are $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$, which means that the first few prime gaps are $d_1 = 1$, $d_2 = 2$, and $d_3 = 2$. Note that $\sum_{k=1}^{n}(p_{k+1} - p_k) = p_{n+1} - 2$. By an equivalent form of the PNT the n-th prime number p_n asymptotically grows as $n \log n$. (This is plausible as by the PNT the number of primes not exceeding $n \log n$ is asymptotically equal

to $n \log n/(\log(n \log n)$, that is to n.) Thus on average the prime gap is $\log n$, which behaves as $\log p_n$. A natural question is then how often d_n is behaving far from average. E.g., looking at the d_n one might suspect that infinitely often $d_n = 2$. This happens when both p_n and p_{n+1} are primes (they then form a *twin prime pair*) and the Twin Prime Conjecture states that there are infinitely many twin prime pairs. Similarly it is suspected that, given any even number $2k$, infinitely often $d_n = 2k$. Proving results in this direction is extremely hard. If one focuses on rather bigger gaps, life is a bit easier. For example, Helmut Maier [31] showed that $p_{n+1} - p_n \leq (\log p_n)/4$ for infinitely many n. There are a lot of interesting things to say further on small gaps and some spectacular recent developments to report on, see, e.g., the recent book by Broughan [10]. However, our focus will be on large prime gaps. One does not need the PNT to see that there are arbitrarily large prime gaps, i.e. arbitrarily large stretches of composite integers. Namely, for every $N > 1$ there exists a string of at least N consecutive composite integers. An example is given by the string $(N+1)!+2, (N+1)!+3, \ldots, (N+1)!+N+1$. Experimentally gaps of size N have been found between numbers much smaller than $(N+1)!+N+1$. Rankin [40] proved in 1938 that there exists a positive constant c such that, for infinitely many n, we have

$$p_{n+1} - p_n \geq c \log p_n \frac{(\log\log p_n)(\log\log\log\log p_n)}{(\log\log\log p_n)^2}.$$

This improved on work of Westzynthius (1931) who showed that the sequence $(p_{n+1}-p_n)/\log p_n$ is unbounded. In his final paper on this topic Rankin showed that one can take c to be any number smaller than e^γ, where $\gamma = 0,5772156649\ldots$ is *Euler's constant*. This had been shown already in 1935 by Pál Erdős [16]. Indeed, Erdős who had the habit of offering prizes for solving various open problems, offered 10.000 dollar to anyone who could prove that c can be replaced by any arbitrarily large constant. In 2016, twenty years after Erdős passed away, this conjecture was independently established by Ford, Green, Konyagin and Tao [18] and Maynard [33]. The group of four authors and Maynard received each 5.000 dollar from Ron Graham, a close friend of Erdős.

The function $\log\log x$ walks off to infinity in such a gentle way that one does not notice it. For example, the reciprocal prime sum $\sum_{p \leq x} 1/p$ behaves in that way. It comes perhaps to as a surprise (or shock!) to the reader that if we sum the reciprocals of all different primes any human eye has ever looked at, the number comes to be out less than ... 4! The fact that making conjectures in analytic prime number theory is a notoriously dangerous endeavour is related to this. The danger lies in the fact that computers can barely spot $\log\log$ terms and are certainly blind to the $\log\log\log$ terms that frequently occur. It is there that the log log log devil is in his element. The presence of such terms can result in the conjecture being false on very thin subsequences. A famous example is the conjecture that $\pi(x) < \mathrm{Li}(x)$. It is false, but true up to gigantic values of x. Littlewood proved that $\pi(x)$ and $\mathrm{Li}(x)$ carry out an eternal dance around each other. This is now a classic result, but falls a bit short of proving RH (on the suggestion of his tutor Littlewood tried to prove RH during his postdoctoral studies!). Further examples of log log log devil teases are discussed in my article [36].

3.2. **Large prime gaps.** There is a whole range of conjectures on gaps between consecutive primes; from more careful to high-risk. The most famous one is Legendre's and claims that there is a prime in $(m^2, (m+1)^2)$ for every natural number m. This is a conjecture that is on the safer side, but for example Firoozbakht's conjecture that $p_n^{1/n}$ is a strictly decreasing function of n is "trés risqué". It implies that $d_n < (\log p_n)^2 - \log p_n + 1$ for all n sufficiently large (see Sun [43]), contradicting a heuristic model suggesting that, given any $\epsilon > 0$, there

exponent	author	year
0.9666	D. Wolke	1975
0.8674	R.J. Cook	1979
0.8243	M.N. Huxley	1980
0.8083	A. Ivić	1981
0.8055	R.J. Cook	1981
0.7501	D.R. Heath-Brown	1979
0.6944	A.S. Peck	1998
0.6666	K. Matomäki	2007
0.6001	D.R. Heath-Brown	2019

TABLE 2. Record exponents α in (3.2) over time

are infinitely many n such that $d_n > (2e^{-\gamma} - \epsilon)(\log p_n)^2$; see Banks, Ford and Tao [4]. Cramér in 1936 conjectured that $d_n = O\left((\log p_n)^2\right)$. Piltz in 1884 conjectured more modestly that $d_n = O(p_n^\epsilon)$ for every $\epsilon > 0$. The first to *prove* that $d_n = O(p_n^\theta)$ for some $\theta < 1$ was Hoheisel in 1930. He took $\theta = 1 - \frac{1}{33000} + \epsilon$. Well-known to number theorists is Huxley's [24] result from 1972 showing that one can take $\theta = 7/12 + \epsilon$. Baker et al. [3] showed that $d_n = O(p_n^{0.525})$, which is not much weaker than what one can prove assuming RH. Under RH it is an easy consequence of (3.1) that $d_n = O(\sqrt{p_n}(\log p_n)^2)$. Cramér [13] improved on this by showing in 1920 that $d_n = O(\sqrt{p_n}\log p_n)$ under RH. More explicitly, Carneiro et al. [11] established under RH that $d_n \leq \frac{22}{25}\sqrt{p_n}\log p_n$ for every $p_n > 3$.

We will be especially interested in the following conjecture, which is in the same league as Legendre's conjecture.

Conjecture 3.1 (Andrica's conjecture)**.** *For $n \geq 1$, $p_{n+1} - p_n < \sqrt{p_n} + \sqrt{p_{n+1}}$, or equivalently $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$, or equivalently $p_{n+1} - p_n < 2\sqrt{p_n} + 1$.*

Andrica's Conjecture is currently out of reach as we have just seen (even under RH). The next best thing one can then hope for is to prove that there are not too many n for which the inequality fails (more on that later).

Many mathematicians take it that an unproven assertion can only be called conjecture if there are overwhelming reasons for its truth. From this perspective it seems fair to say that this does not apply to any of the conjectures in this section. Some log log log devil (or any of its kin) might well be lurking somewhere...

3.3. **The size of large prime gaps.** Estimating the size of large prime gaps by establishing a small exponent α in

$$\sum_{\substack{p_n \leq x \\ p_{n+1} - p_n \geq \sqrt{p_n}}} (p_{n+1} - p_n) = O(x^\alpha) \tag{3.2}$$

is a sport. The current record is due to Heath-Brown [23], who established $\alpha = 3/5 + \epsilon$, with ϵ any positive number. This result is very relevant for us, as we will see in the sequel. I include the table with "exponent hunters", as it strongly suggests how much effort it often takes in prime number theory to achieve seemingly small improvements.

4. More on cyclotomic polynomials

From (1.3) it can be deduced by so-called Möbius inversion that

$$\Phi_n(X) = \prod_{d\,|n} (X^d - 1)^{\mu(n/d)}, \tag{4.1}$$

where the product is over all positive divisors d of n and μ is the *Möbius function* defined by $\mu(n) = (-1)^t$ if n is a square-free positive integer having t prime factors, and $\mu(n) = 0$ if n has a repeated prime factor.

Let p be a prime and n a positive integer. Then from (4.1) the following properties are easily deduced

a) $\Phi_{pn}(X) = \Phi_n(X^p)$ if p divides n;
b) $\Phi_{2n}(X) = (-1)^{\varphi(n)}\Phi_n(-X)$ if n is odd;
c) $\Phi_n(X) = X^{\varphi(n)}\Phi_n(1/X)$, that is, Φ_n is *self-reciprocal* if $n > 1$.

For example, using the first property we infer that $\Phi_{16}(X) = \Phi_2(X^8) = X^8 + 1$.

It is a classical result that if n has at most two distinct odd prime factors, then $A(n) = 1$, cf. Lam and Leung [27]. The first non-trivial case arises where n has precisely three distinct odd prime divisors and thus is of the form $n = p^e q^f r^g$, with $2 < p < q < r$ prime numbers. By repeatedly invoking the first property above we have $A\{p^e q^f r^g\} = A\{pqr\}$, and hence it suffices to consider only the case where $e = f = g = 1$ and so $n = pqr$. This motivates the following definition.

Definition 4.1. A cyclotomic polynomial Φ_n is said to be *ternary* if $n = pqr$, with $2 < p < q < r$ primes. In this case we call the integer n *ternary*.

An important subclass of these polynomials where we have even more control are the *optimal* ternary cyclotomic polynomials.

Definition 4.2. A ternary cyclotomic polynomial Φ_{pqr} is said to be *optimal* if its coefficients assume $p + 1$ different values, that is $A\{pqr\}$ has cardinality $p + 1$.

The usage of the word optimal comes from the fact that $p + 1$ is the maximum number of distinct coefficients that can occur.

A special property of ternary cyclotomic polynomials is that consecutive coefficients differ by at most one (proven in [20]). Here an example:

$$\Phi_{11\cdot 13\cdot 17}(X) = ... - X^{672} - 2X^{673} - 2X^{674} - 2X^{675} - 3X^{676} - 4X^{677} - 3X^{678} \ldots$$

It follows that $A\{n\}$ consists of consecutive integers if n is ternary (this is not true in general!). For example, $A\{11 \cdot 13 \cdot 17\} = \{-4, -3, \ldots, 1, 2, 3\}$, as can be read off from Table 5. In the ternary case the behaviour of the coefficients is both non-trivial, but also understood so well, that we can use this to our benefit. This is not the case if n has four or more distinct odd prime factors. For optimal ternary cyclotomic polynomials the situation is even more under control, since if we know that $a_{pqr}(k_1) = b$ and $a_{pqr}(k_2) = a$, with $b - a = p$, then b must be the maximal coefficient and a the minimal one.

4.1. The family Φ_{pqr} with p fixed.

In this subsection we briefly discuss other research on ternary coefficients.

The height $A(n)$ is unbounded if n ranges over the ternary integers. However, if we restrict to ternary n having a prescribed smallest prime factor $P(n) = p$, we get a bounded quantity $M(p)$. The definition of $M(p)$ can be stated more explicitly as

$$M(p) = \max\{A(pqr) : 2 < p < q < r\},$$

p	3	5	7	11	13	17	19	23	29	31	37	41
$(p+1)/2$	2	3	4	6	7	9	10	12	15	16	18	21
$M(p) \geq$	2	3	4	7	8	10	12	14	18	19	22	26
$\lfloor 2p/3 \rfloor$	2	3	4	7	8	11	12	15	19	20	24	27

TABLE 3. Some numerical evidence for the corrected Sister Beiter conjecture

where p is a fixed odd prime and q, r range over the primes satisfying $r > q > p$. As the definition of $M(p)$ involves infinitely many cyclotomic polynomials, it is not clear whether there exists a finite procedure to determine it. Duda [15], during his internship at MPIM, provided such a procedure. It reduces the computation of $M(p)$ to the determination of the maximum value of $A(n)$, with n running through a *finite* set of ternary integers pqr. As the n involved are huge, the procedure is unfortunately not practical. It is a major open problem to find a *practical* procedure leading to explicit values of $M(p)$.

In 1971, Möller [35] gave a construction showing that $M(p) \geq (p+1)/2$ for $p > 5$. On the other hand, in 1968, Sister Marion Beiter [5] had conjectured that $M(p) \leq (p+1)/2$ and shown that $M(3) = 2$ [7], which on combining leads to the conjecture that $M(p) = (p+1)/2$ for $p > 2$. The bound of Möller together with Beiter's [6] bound $M(5) \leq 3$ shows that $M(5) = 3$. Zhao and Zhang [47] showed that $M(7) = 4$. Thus Beiter's conjecture holds true for $p \leq 7$. Gallot and Moree [21] showed that Beiter's conjecture is false for every $p \geq 11$. Moreover, they showed that for every $\epsilon > 0$ we have $M(p) \geq (2/3 - \epsilon)p$ and conjectured that always $M(p) \leq 2p/3$, dubbing this conjecture the "corrected Sister Beiter conjecture".

The true behavior of $M(p)$ is much more complicated than suggested by Beiter's conjecture. For one, it is related to the distribution of inverses modulo primes p. Given any integer a coprime to p, any integer b with $ab \equiv 1 (\mathrm{mod}\ p)$ is its *modular inverse*. The collection of points (a, b) with $0 < a, b < p$ is called the *modular hyperbola*; for a survey see Shparlinski [42]. The distribution of points on the modular hyperbola is traditionally investigated using the *Kloosterman sum* $K(a, b; p)$, which is defined as

$$K(a, b; p) = \sum_{1 \leq x \leq p-1} e^{2\pi i (ax + b\overline{x})/p},$$

with $\overline{x}$ any modular inverse of x modulo p. (As an aside we note that the Dutch word kloosterman means "cloister man" and thus the cloister man sums can be used to investigate a conjecture of a nun. Honi soit qui mal y pense! Reader beware: too intense study of these sums and their applications can lead to "Kloostermania" [34].) By a fundamental result of Weil we have $|K(a, b; p)| \leq 2\sqrt{p}$, which can be used to show that $M(p) > 2p/3 - 3\, p^{3/4} \log p$ (see Cobeli et al. [12]).

In Figure 2 we display part of the modular hyperbola mod 241 that is relevant in constructing a sharp lower bound for $M(241)$ in the work of Gallot and myself. It gives integer pairs (a, b) with $1 \leq a, b \leq 240$ in certain triangles with $ab \equiv 1 (\mathrm{mod}\ 241)$. For a detailed analysis of this construction, see Cobeli et al. [12].

5. Our results on the possible maximum coefficient

In this section I finally return to Question 2.1 and discuss the recent progress made on it in my paper with Kosyak, Sofos and Zhang [26]. It relies on a construction found by my former intern Eugenia Roşu (using only paper!). For certain primes p it improves on an

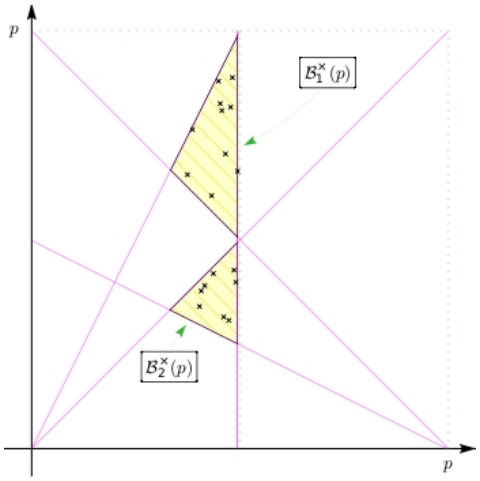


FIGURE 2. $M(241)$ estimation relevant part of modular hyperbola mod 241.

earlier construction by Gallot and myself (found using paper... and computer). The original formulation is quite lengthy, however for us the following watered down version will do.

Theorem 5.1. (Moree and Roşu [38]). *Let $m \geq 0$ be an arbitrary integer and $p \geq 4m^2+2m+3$ be any prime. Then there exist primes q_1, r_1, q_2, r_2 such that $\Phi_{pq_1r_1}$ and $\Phi_{pq_1r_1}$ have maximum coefficient $(p-1)/2-m$, respectively $(p+1)/2+m$.*

This shows that the set of cyclotomic maximum coefficients we can obtain certainly contains

$$\begin{aligned}\mathcal{R} : \;=\; & \Big\{\frac{p-1}{2} - m : p \text{ is a prime, } m \geq 0,\, 4m^2+2m+3 \leq p\Big\} \\ & \cup \Big\{\frac{p-1}{2} + m : p \text{ is a prime, } m \geq 0,\, 4m^2+2m+3 \leq p\Big\}.\end{aligned}$$

We conjecture that this set equals the set of all natural numbers, thus implying that each natural number can arise as maximum coefficient of some cyclotomic polynomial. Roughly speaking $\mathcal{R}$ is a union of integers in intervals of the form $((p-1)/2-\sqrt{p}/2, (p-1)/2+\sqrt{p}/2)$, and thus if the gaps between successive primes are *always* sufficiently small, all natural integers will be covered. Working out the technicalities one arrives at the following result.

Theorem 5.2. *If $p_{n+1}-p_n < \sqrt{p_n}+\sqrt{p_{n+1}}$ holds for $p_n \leq 2h$, then the integers $1, 2, \ldots, h$ are in $\mathcal{R}$. Andrica's conjecture, Conjecture 3.1, implies that every natural number occurs as the maximum coefficient of some ternary cyclotomic polynomial.*

A lot of numerical work on large gaps has been done (see the website [39]). This can be used to infer that the inequality in Theorem 5.2 holds for $p_n \leq 2 \cdot 2^{63} \approx 1.8 \cdot 10^{19}$, leading to the following corollary.

Corollary 5.3. *Every integer up to $9 \cdot 10^{18}$ occurs as the maximal coefficient of some ternary cyclotomic polynomial.*

If holes in the set $\mathcal{R}$ appear, it is when $p_{n+1}-p_n \geq \sqrt{p_n}+\sqrt{p_{n+1}}$. The number of natural numbers up to x that are not in $\mathcal{R}$ (if any), is close to

$$\sum_{\substack{p_n \leq 2x \\ d_n \geq \sqrt{p_n}+\sqrt{p_{n+1}}}} (d_n - \sqrt{p_n} - \sqrt{p_{n+1}}) \leq \sum_{\substack{p_n \leq 2x \\ d_n \geq \sqrt{p_n}+\sqrt{p_{n+1}}}} d_n \leq \sum_{\substack{p_n \leq 2x \\ d_n \geq \sqrt{p_n}}} d_n.$$

h	p	q
3	5	11
5	13	53
55	139	7507
117	263	30509
219	449	97883

TABLE 4. Smallest choice of $p \geq 2h-1$ with $q := 1+(h-1)p$ prime

Now the reader might be reminded of (3.2). An easy climb on the shoulders of giants in analytic number theory then leads to the following result.

Theorem 5.4. *For any fixed $\epsilon > 0$, there exists a constant C_ϵ such that the number of positive integers $\leq x$ that do not occur as a height of a ternary cyclotomic polynomial is at most $C_\epsilon x^{3/5+\epsilon}$. Under the Riemann Hypothesis this number is at most $C_\epsilon x^{1/2+\epsilon}$.*

5.1. **A different approach.** Let $h > 1$ be odd. If there exists a prime $p \geq 2h-1$ such that $q := 1+(h-1)p$ is a prime too, then for some prime $r > q$ it can be shown that Φ_{pqr} has maximum coefficient h. This is a consequence of work of Gallot, Moree and Wilms [22] and involves ternary cyclotomic polynomials that are not optimal.

For some choices of h, p and q see Table 4.

Conjecture 5.5. *Let $h > 1$ be any odd integer. There exists a prime $p \geq 2h-1$, such that $1+(h-1)p$ is a prime too.*

This conjecture is a consequence of the widely believed Bateman–Horn conjecture [1], which implies that, given an arbitrary odd integer $h > 1$, there are *infinitely* many primes p such that $1+(h-1)p$ is a prime too.

Theorem 5.6. *If Conjecture 5.5 holds true, then every positive odd natural number occurs as maximal coefficient of some ternary cyclotomic polynomial. Unconditionally a positive fraction of all odd natural numbers occur as maxima.*

Our proof of the second assertion makes use of deep work of Bombieri, Friedlander and Iwaniec [8] on the level of distribution of primes in arithmetic progressions with fixed residue and varying moduli. Although the unconditional statement in Theorem 5.6 is surpassed by the unconditional statement in Theorem 5.4, the proof of Theorem 5.6 is, in a way, 'orthogonal' to the one of Theorem 5.4; it thus has the potential of working for variations of the problem where the method behind Theorem 5.4 would fail. Interestingly, like our prime gap criterion, it rests on a variation of a certain very well studied problem involving prime numbers. Both prime number questions are, however, quite different.

6. Concluding remarks

In [26] we also obtain the same type of results as described in the previous section for the minimum coefficient and for the height. In case of the height a conjecture slightly stronger than Andrica's enters the game.

Conjecture 6.1. *Every natural number occurs as the height of some cyclotomic polynomial.*

height	p	q	r	k	sign	diff.
1	3	7	11	0	+	2
2	3	5	7	7	−	**3**
3	5	7	11	119	−	**5**
4	11	13	17	677	−	7
5	11	13	19	1008	−	9
6	13	23	29	2499	−	10
7	17	19	53	6013	+	14
8	17	31	37	5596	−	14
9	17	47	53	14538	−	**17**
10	17	29	41	4801	−	**17**

TABLE 5. Minimal ternary examples with prescribed height

We demonstrate this in Table 5, which gives the minimum ternary integer $n = pqr$ with $p < q < r$ such that Φ_n has height m for the numbers $m = 1, \ldots, 10$. The integer k has the property that $a_{pqr}(k) = \pm m$, with the sign coming from the sixth column. The seventh column records the difference between the largest and smallest coefficient and is in bold if this is optimal, that is, if the difference equals p (compare Definition 4.2). See [26] for the continuation of the table up to $m = 40$.

Prime differences make their appearance since in our approach we work with ternary cyclotomic polynomials. One would want to work with Φ_n with n having at least four prime factors; however, this leads to a loss of control over the behaviour of the coefficients in general and the maximum, minimum and height in particular. Prime number properties play a true role if one asks for the possible heights $A(n)$ and extrema of $A\{n\}$ with n restricted to ternary integers.

7. Further reading

Ribenboim's book [41] gives a wealth of results on prime numbers and their distribution. It can be thought of as a number-theoretical version of the Guinness Book of Records. Also some of the underlying mathematics is explained. For a computational history of prime numbers and Riemann zeros see [37]. The truly courageous might have a go at the monumental book of Landau [28].

8. Acknowledgment

I would like to thank Alexandru Ciolan, Kate Kattegat, Alexandre Kosyak and Lola Thompson for proofreading earlier versions, and Igor Shparlinski for a mathematical comment. Figure 2 was provided by Cristian Cobeli. The part of the Table 2 up to 1981 is taken from Ivić [25, p. 350], who also gives a proof of the 1979 result of Heath-Brown. Table 3 was computed by Yves Gallot, and Table 5 by Bin Zhang.

Since 2005 I have regularly guided budding mathematicians for one month internships. I dedicate this article to them for their youthful enthusiasm, energy, fresh outlook at life and mathematical creativity.

FIGURE 3. With Bogdan Petrenko and MPIM interns Oana-Maria Camburu, Jessica Fintzen and Eugenia Roşu (from left to right).

REFERENCES

[1] S.L. Aletheia-Zomlefer, L. Fukshansky and S.R. Garcia, The Bateman-Horn conjecture: heuristics, history and applications, *Expos. Math.* **38** (2020), 430–479.

[2] A. Arnold and M. Monagan, `http://www.cecm.sfu.ca/~ada26/cyclotomic/`.

[3] R.C. Baker, G. Harman and J. Pintz, The difference between consecutive primes. II, *Proc. London Math. Soc.* (3) **83** (2001), 532–562.

[4] W. Banks, K. Ford and T. Tao, Large prime gaps and probabilistic models, arXiv:1908.08613.

[5] M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial $F_{pqr}(x)$, *Amer. Math. Monthly* **75** (1968), 370–372.

[6] M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial F_{pqr}. II, *Duke Math. J.* **38** (1971), 591–594.

[7] M. Beiter, Coefficients of the cyclotomic polynomial $F_{3qr}(x)$, *Fibonacci Quart.* **16** (1978), 302–306.

[8] E. Bombieri, J.B. Friedlander and H. Iwaniec, Primes in arithmetic progressions to large moduli. II, *J. Math. Ann.* **277** (1987), 361–393.

[9] K. Broughan, *Equivalents of the Riemann Hypothesis*. Vol. 2. Analytic equivalents, Encyclopedia of Mathematics and its Applications **165**, Cambridge University Press, Cambridge, 2017.

[10] K. Broughan, *Bounded gaps between primes: the epic breakthroughs of the early* 21*st century*, Cambridge University Press, Cambridge, 2021.

[11] E. Carneiro, M.B. Milinovich and K. Soundararajan, Fourier optimization and prime gaps, *Comment. Math. Helv.* **94** (2019), 533–568.

[12] C. Cobeli, Y. Gallot, P. Moree and A. Zaharescu, Sister Beiter and Kloosterman: a tale of cyclotomic coefficients and modular inverses, *Indag. Math.* **24** (2013), 915–929.

[13] H. Cramér, Some theorems concerning prime numbers, *Arkiv f. Math. Astr. Fys.* **15** (1920), 1–33. [Collected Works **1**, 85–91, Springer, Berlin-Heidelberg, 1994.]

[14] H. Cremer, *Carmina mathematica und andere poetische Jugendsünden*, 7. Aufl., Aachen: Verlag J. A. Mayer, 1982.

[15] D. Duda, The maximal coefficient of ternary cyclotomic polynomials with one free prime, *Int. J. Number Theory* **10** (2014), 1067–1080.

[16] P. Erdős, On the difference of consecutive primes, *Quart. Journ. of Math.* **6** (1935), 124–128.

[17] J. Fintzen, Cyclotomic polynomial coefficients $a(n, k)$ with n and k in prescribed residue classes, *J. Number Theory* **131** (2011), 1852–1863.

[18] K. Ford, B. Green, S. Konyagin and T. Tao, Large gaps between consecutive prime numbers, *Ann. of Math.* (2) **183** (2016), 935–974.
[19] K. Ford, B. Green, S. Konyagin, J. Maynard and T. Tao, Long gaps between primes, *J. Amer. Math. Soc.* **31** (2018), 65–105.
[20] Y. Gallot and P. Moree, Neighboring ternary cyclotomic coefficients differ by at most one, *J. Ramanujan Math. Soc.* **24** (2009), 235–248.
[21] Y. Gallot and P. Moree, Ternary cyclotomic polynomials having a large coefficient, *J. Reine Angew. Math.* **632** (2009), 105–125.
[22] Y. Gallot, P. Moree and R. Wilms, The family of ternary cyclotomic polynomials with one free prime, *Involve* **4** (2011), 317–341.
[23] D.R. Heath-Brown, The differences between consecutive primes. V, *Int. Math. Res. Not. IMRN*, to appear, `https://academic.oup.com/imrn/article-abstract/doi/10.1093/imrn/rnz295/5676434`.
[24] M.N. Huxley, On the difference between consecutive primes, *Invent. Math.* **15** (1972), 164–170.
[25] A. Ivić, *The Riemann zeta-function*, John Wiley & Sons, Inc., New York, 1985.
[26] A. Kosyak, P. Moree, E. Sofos and B. Zhang, Cyclotomic polynomials with prescribed height and prime number theory, *Mathematika* **67** (2021), 214–234.
[27] T.Y. Lam and K.H. Leung, On the cyclotomic polynomial $\Phi_{pq}(X)$, *Amer. Math. Monthly* **103** (1996), 562–564.
[28] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, 2 Bände, second ed. With an appendix by P.T. Bateman, Chelsea Publishing Co., New York, 1953.
[29] E. Lehmer, On the magnitude of the coefficients of the cyclotomic polynomials, *Bull. Amer. Math. Soc.* **42** (1936), 389–392.
[30] H. Maier, Primes in short intervals, *Michigan Math. J.* **32** (1985), 221–225.
[31] H. Maier, Small differences between prime numbers, *Michigan Math. J.* **35** (1988), 323–344.
[32] J. Maynard, Small gaps between primes, *Ann. of Math.* **181** (2015), 1–31.
[33] J. Maynard, Large gaps between primes, *Ann. of Math.* **183** (2016), 915–933.
[34] P. Michel, Some recent applications of Kloostermania, *Physics and number theory*, IRMA Lect. Math. Theor. Phys. **10**, Eur. Math. Soc., Zürich (2006), 225–251.
[35] H. Möller, Über die Koeffizienten des $n$ten Kreisteilungspolynoms, *Math. Z.* **119** (1971), 33–40.
[36] P. Moree, Irregular behaviour of class numbers and Euler-Kronecker constants of cyclotomic fields: the log log log devil at play, in *'Irregularities in the Distribution of Prime Numbers - Research Inspired by Maier's Matrix Method'*, Eds. J. Pintz and M.Th. Rassias, Springer, 2018, 143–163.
[37] P. Moree, I. Petrykiewicz and A. Sedunova, A computational history of prime numbers and Riemann zeros, `https://arxiv.org/abs/1810.05244`.
[38] P. Moree and E. Roşu, Non-Beiter ternary cyclotomic polynomials with an optimally large set of coefficients, *Int. J. Number Theory* **8** (2012), 1883–1902.
[39] T.R. Nicely, First occurrence prime gaps, web page `http://www.trnicely.net/gaps/gaplist.html`.
[40] R.A. Rankin, The difference between consecutive prime numbers, *J. London Math. Soc.* **11** (1936), 242–245.
[41] P. Ribenboim, *The book of prime number records*, second edition, Springer-Verlag, New York, 1989.
[42] I. Shparlinski, Modular hyperbolas, *Jpn. J. Math.* **7** (2012), 235–294.
[43] Z.-W. Sun, On a sequence involving sums of primes, *Bull. Aust. Math. Soc.* **88** (2013), 197–205.
[44] J. Suzuki, On coefficients of cyclotomic polynomials, *Proc. Japan Acad. Ser. A Math. Sci.* **63** (1987), 279–280.
[45] R. Thangadurai, On the coefficients of cyclotomic polynomials, *Cyclotomic fields and related topics* (Pune, 1999), 311–322.
[46] S. Weintraub, Several proofs of the irreducibility of the cyclotomic polynomials, *Amer. Math. Monthly* **120** (2013), 537–545.
[47] J. Zhao and X. Zhang, Coefficients of ternary cyclotomic polynomials, *J. Number Theory* **130** (2010), 2223–2237.