Calculating cyclotomic polynomials of very large height

Andrew Arnold (ada26@sfu.ca)
Michael Monagan (mmonagan@cecm.sfu.ca)

October 10, 2008

Abstract

We present two algorithms to calculate $\Phi_n(z)$, the n_{th} cyclotomic polynomial. The first algorithm calculates $\Phi_n(z)$ by a series of polynomial divisions, which we do using the discrete Fourier transform. The second algorithm calculates $\Phi_n(z)$ as a quotients of products of sparse power series. These algorithms, described in detail in the paper, were used to calculate cyclotomic polynomials of large height and length. In particular, we have found cyclotomic polynomials $\Phi_n(z)$ of minimal order n whose height is greater than n, n^2, n^3, and n^4, respectively. We include these results as well as other examples of cyclotomic polynomials of unusually large height, and bounds on the k_{th} coefficient for all cyclotomic polynomials.

1 Introduction

The n_{th} **cyclotomic polynomial**, $\Phi_n(z)$, is the monic polynomial whose $\phi(n)$ distinct roots are exactly the n_{th} primitive roots of unity.

$$\Phi_n(z) = \prod_{\substack{k=1 \\ gcd(k,n)=1}}^{n} \left(z - e^{2\pi i \frac{k}{n}}\right).$$

It is an irreducible polynomial over $\mathbb{Z}$ with degree $\phi(n)$, where $\phi(n)$ is Euler's function. We write

$$\Phi_n(z) = \sum_{k=0}^{\phi(n)} a_n(k) z^k,$$

It is well known that for $n < 105$, the coefficients of $\Phi_n(z)$ are either $-1, 0$, or 1 and that both 2 and -2 appear as coefficients in $\Phi_{105}(z)$. Denote by $A(n)$

2000 *Mathematics Subject Classification.* Primary 11Y16, Secondary 12-04

and $S(n)$ the height and length, respectively, of the n_{th} cyclotomic polynomial. That is,

$$A(n) = \|\Phi_n(z)\|_\infty = \max_{0 \le k \le \phi(n)} |a_n(k)|, \quad \text{and} \quad S(n) = \|\Phi_n(z)\|_1 = \sum_{k=0}^{\phi(n)} |a_n(k)|.$$

Paul Erdos [5] proved that $A(n)$ is not bounded above by any polynomial in n, that is, for any constant $c > 0$, there exist n such that $A(n) > n^c$. There is a wealth of material on the behaviour of $A(n)$ and the size of cyclotomic polynomial coefficients [3], [2], [10], [11]; however, comparatively little work has gone into actually calculating these values. Koshiba calculated $A(4849845) = 669606$ [8] and found the coefficients of $\Phi_n(z)$ with degree less than $\phi(n)/10$ for $n = 111546345 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$ [9]. Bosma in [4] found the least value of k for which a occurs as $a_n(k)$ for some n, for $|a| < 50$.

But as far as we know, no one has found an n with $A(n) > n$. It was when we found $A(1181895) = 14102773$, which is greater than n, that we got excited about computing $A(n)$. We then developed the asymptotically fast algorithms presented in this paper to allow us to search systematically for larger $A(n)$ for n over one billion. Our algorithms are implemented entirely in C because our computer algebra systems that we use, Maple and Magma, are just not fast enough to let us search at n greater than one million.

1.1 Organization of paper.

We present two algorithms to calculate cyclotomic polynomials. Our first algorithm calculates $\Phi_n(z)$ for squarefree n via a series of polynomial divisions. We use the discrete Fourier transform to do these divisions quickly. The second algorithm calculates $\Phi_n(z)$ as a quotient of products of sparse power series.

Using these two algorithms, we have produced a wealth of data on the heights and lengths of cyclotomic polynomials. Amongst our results, we have found:

1. $A(n)$ and $S(n)$ for all odd, squarefree $n < 5 \cdot 10^6$.
2. $A(n)$ and $S(n)$ for squarefree $n < 10^8$ with five or more prime factors.
3. $A(n)$ and $S(n)$ for squarefree $n < 6.0 \cdot 10^8$ with six or more prime factors.
4. $A(n)$ and $S(n)$ for squarefree $n < 1.89 \cdot 10^9$ with seven or more prime factors.
5. $A(n)$ and $S(n)$ for squarefree $n < 2.6 \cdot 10^9$ with eight or more prime factors.
6. $A(n)$ and $S(n)$ for squarefree $n < 8 \cdot 10^9$ with nine or more prime factors.
7. The smallest values of n for which $A(n) > n, n^2, n^3$, and n^4 respectively.
8. The smallest n such that $A(n) > 2^{64}$ (machine precision).
9. $\max_n(a_n(k))$, $\min_n(a_n(k))$, $\max_n(|a_n(k)|)$ for fixed k, for $k < 162$.

10. The smallest instance of k for which $a_n(k) = a$ for some n, for $-575 \leq a \leq 585$.

We include in this paper items 7, 8, the smallest k for which $|a_n(k)| = a$ for $a < 250$, and the values $\max_n(|a_n(k)|)$ for $k \leq 162$. All of the data listed above is available on the web at

`http://www.cecm.sfu.ca/~ada26/cyclotomic/`

1.2 Preliminaries

We are interested in computing cyclotomic polynomials of high degree. The following two identities are useful:

Lemma 1. *Let $n > 1$ be odd. Then $\Phi_{2n}(z) = \Phi_n(-z)$.*

Lemma 2. *Let p be a prime that divides n. Then $\Phi_{np}(z) = \Phi_n(z^p)$*

Lemma 1 tells us $A(2n) = A(n)$ and $S(2n) = S(n)$ for odd n. Lemma 2 says that $A(np) = A(n)$ and $S(np) = S(n)$ for p dividing n. For the remainder of the paper, we will be strictly concerned with the calculation of cyclotomic polynomials of squarefree, odd order. Lemmas 1 and 2 provide an easy means of calculating $\Phi_n(z)$ for n even or nonsquarefree, provided we can calculate $\Phi_m(z)$, where m is the product of the odd prime factors of n.

2 Using the discrete Fourier transform

Our first algorithm calculates $\Phi_n(z)$ by a series of polynomial divisions. Our algorithm uses the following identity [12].

Lemma 3. *Let p be prime that does not divide m. Then $\Phi_{mp}(z) = \dfrac{\Phi_m(z^p)}{\Phi_m(z)}$.*

We thus are able to calculate $\Phi_n(z)$ by repeated polynomial division, as detailed in algorithm 1.

Input: $n = p_1 p_2 \cdots p_k$, a product of k distinct primes.
Output: $\Phi_n(z)$, the n_{th} cyclotomic polynomial.
$m \longleftarrow 1$
$\Phi_m(z) \longleftarrow z - 1$
for $j = 1$ **to** k **do**
  $m^* \longleftarrow m p_j$
  $\Phi_{m^*}(z) \longleftarrow \dfrac{\Phi_m(z^{p_j})}{\Phi_m(z)}$
  $m \longleftarrow m^*$

Algorithm 1: calculating $\Phi_n(z)$ by repeated division

This algorithm (see [12]) is well-known. It is used in many computer algebra systems. For example, in Maple, it is the `numtheory[cyclotomic]` command. Using classical, quadratic polynomial division, however, is much too slow to do any extensive search on cyclotomic polynomials of order greater than roughly one million. Maple, which uses classical, quadratic-time polynomial division and multi-precision integers to calculate $\Phi_n(z)$, takes over five minutes to find $\Phi_{255255}(z)$. Using the same algorithm with machine-precision integers takes under 15 seconds. We implemented algorithm 1 with machine-precision arithmetic and optimized the polynomial division in algorithm 1 by way of the Fast Fourier Transform (FFT)[6, 12]. Our implementation of algorithm 1 can calculate $\Phi_{255255}(z)$ modulo two 32-bit primes in under one second (see table 3.1 for timings). Algorithm 2 gives a high-level description of the division calculation via the FFT. Using the Fast Fourier transform, we can calculate $\frac{\Phi_m(z^p)}{\Phi_m(z)}$ in $\mathcal{O}(N \log(N))$ arithmetic operations, where N is the smallest power of 2 greater than $\phi(m) \cdot p$, the degree of the numerator.

Input:

- m, an odd, squarefree, positive integer greater than 1
- $\Phi_m(z)$
- p, an odd prime not dividing m
- $N = 2^s$, a power of 2 greater than $\phi(m) \cdot p$
- q, a prime of the form $q = r \cdot N + 1$
- ω, a primitive N_{th} root of unity modulo q

Output: $\Phi_{mp}(z) \mod q$

Calculate $A_i = \Phi_m(\omega^{ip}) \bmod q$ and $B_i = \Phi_m(\omega^i) \bmod q$ for $i = 0, 1, \ldots, N-1$ using the FFT.

$C_i \longleftarrow \dfrac{A_i}{B_i} \mod q$ for $i = 0, 1, \ldots, N-1$ `/* C_i = Φ_mp(ω^i) */`

Interpolate $C(z) = \Phi_{mp}(z) \mod q$ by the inverse FFT.

Algorithm 2: Polynomial division via the Fast Fourier transform

Observe that algorithm 2 requires that B_i is nonzero for ω^i, $0 \leq i < N$. This does not pose a problem for odd orders m, however, by the following lemma.

Lemma 4. *Let $m > 1$ be an odd, squarefree integer, and let p, N, q, and ω be as defined in algorithm 2. Then $\Phi_m(\omega^i)$ is nonzero*

Proof. Every power of ω is a $2^k th$ root of unity modulo q for some $k \leq s$. For $m > 1$ it holds that $\Phi_m(z)$ divides

$$\frac{z^m - 1}{z - 1} = z^{m-1} + z^{m-1} + \cdots + z + 1. \tag{1}$$

Thus if q does not divide m, any root of $\Phi_m(z) \bmod q$ is necessarily an m_{th} root of unity not equal to 1. Given m is odd for our purposes, the only m_{th} root of

unity that is also a $2^k th$ root of unity modulo q for some k is exactly 1, and so $\Phi_m(\omega^i) \neq 0 \bmod q$ for $0 \leq i < N$. □

2.1 Implementation Details

The Fast Fourier Transform, as described in 2, requries that N is a power of two greater than $\phi(m) \cdot p$, the degree of the numerator of $\Phi_m(z^p)$. For primes $q < 2^{32}$ of the form $q = r \cdot N + 1$, N cannot be greater than 2^{27}. Thus for cyclotomic polynomials of large degree, we require primes larger than 2^{32}. Choosing unnecessarily large primes for the DFT, however, would require multiprecision arithmetic. Using 64-bit arithmetic, we are able to multiply modulo prime numbers as large as 42-bits (algorithm 3); however, multiplication modulo a 42-bit prime is roughly twice as slow as multiplication modulo a 32-bit prime.

Input: $a = a_{41}a_{40}\cdots a_1a_0, b = b_{41}b_{40}\cdots b_1b_0$, two 42-bit primes modulo a 42-bit prime q (i.e. $q < 2^{42}$)
Output: $c = ab \mod q$
A_0 and B_0 are obtained via bitmask operations; A_1 and B_1 are obtained by bitshifts:

$A_0 \longleftarrow a_{20}a_{19}\cdots a_0$ /* $A_0 = a \mod 2^{21}$ */
$A_1 \longleftarrow a_{41}a_{40}\cdots a_{21}$ /* $A_1 = (a - A_0)/2^{21}$ */
$B_0 \longleftarrow b_{20}b_{19}\cdots b_0$ /* $B_0 = b \mod 2^{21}$ */
$B_1 \longleftarrow b_{41}b_{40}\cdots b_{21}$ /* $B_1 = (b - B_0)/2^{21}$ */
$c \longleftarrow A_1B_1 2^{21} \mod q$
$c \longleftarrow c + A_1B_0$
if $c > q$ **then**
  $c \longleftarrow c - q$
$c \longleftarrow c + A_0B_1$
if $c > q$ **then**
  $c \longleftarrow c - q$
$c \longleftarrow c \cdot 2^{21} \mod q$
$c \longleftarrow c + A_0B_0$
if $c > q$ **then**
  $c \longleftarrow c - q$

Algorithm 3: multiplication modulo a 42-bit prime

The FFT only gives us the coefficients of $\Phi_n(z)$ modulo a prime q_1. Our resulting polynomial, call it $H_n(z)$, will not equal $\Phi_n(z)$ if $A(n) > \frac{q_1}{2}$. We calculate $\Phi_n(z)$ modulo another prime q_2. We then reconstruct $H_n(z) \equiv \Phi_n(z) \bmod q_1q_2$ by Chinese remaindering. We do this with primes $q_1, q_2 \ldots q_l$ until $\|H_n(z)\|_\infty \cdot 2^{20} < \frac{q_1q_2\ldots q_l}{2}$. We then take our solution $H_n(z)$ and use the FFT to test that

$$H_n(\omega^j) \cdot \Phi_{n/p_k}(\omega^j) - \Phi_{n/p_k}(\omega^{jp_k}) \equiv 0 \mod q_{l+1}, \tag{2}$$

for some new prime q_{l+1} with N_{th} primitive root ω. If equation (2) holds for all j, $H_n(z) \equiv \Phi_n(z) \pmod{Q = q_1q_2\cdots q_l \cdot q_{l+1}}$. For $q_{l+1} > 2^{40}$, it follows

that all of the coefficients of $\Phi_n(z)$, modulo Q, lie in the interval $(\frac{-Q}{2^{60}}, \frac{Q}{2^{60}})$. We consider 60 redundant bits sufficient. As we know the cyclotomic coefficients have a flat-bell distribution, it is very improbable that the height of $\Phi_n(z)$ were greater than $\frac{Q}{2}$ with all the coefficients strictly in the range $(\frac{-Q}{2^{60}}, \frac{Q}{2^{60}})$ modulo Q. Indeed, all our results obtained by this method thus far have been consistent with results we have obtained by non-modular algorithms. Table 1 lists the primes and the primitive roots we used in our computations.

	q	=	$r \cdot N + 1$	size of q	ω
q_1	2748779069441	=	$5 \cdot 2^{39} + 1$	42 bits	243
q_2	4123168604161	=	$15 \cdot 2^{38} + 1$	42 bits	624392905782
q_3	2061584302081	=	$15 \cdot 2^{37} + 1$	41 bits	624392905781
q_4	206158430209	=	$3 \cdot 2^{36} + 1$	38 bits	10648
q_5	2027224563713	=	$59 \cdot 2^{35} + 1$	41 bits	1609812002788

Table 1: primes and the primitive roots used in our FFT calculations

The brunt of the computation in our implementation of 1 takes place in the last division, as each successive division effectively increases the degree of the resulting intermediate polynomial by another factor. For squarefree n with largest prime divisor p, where N is the smallest power of two greater than $\phi(\frac{n}{p})p$, we can compute $\Phi_n(z)$ in $\mathcal{O}(N \cdot \log(N))$ arithmetic operations.

3 Calculating $\Phi_n(z)$ as a quotient of sparse polynomials

It is well known that

$$\Phi_n(z) = \prod_{d|n} \left(1 - z^d\right)^{\mu(\frac{n}{d})}, \tag{3}$$

where μ is the Mőbius function. For instance, for $n = 105 = 3 \cdot 5 \cdot 7$,

$$\Phi_{105}(z) = \frac{(1-z^3)(1-z^5)(1-z^7)(1-z^{105})}{(1-z)(1-z^{15})(1-z^{21})(1-z^{35})}$$

The sparseness of each term in this quotient lends itself to fast polynomial arithmetic. For the purposes of our algorithm, we treat $\Phi_n(z)$ as a power series. Multiplying a power series $A(z) = \sum_{i=0}^{\infty} a(i)z^i$ by $1 - z^d$ is easy:

$$\left(\sum_{i=0}^{\infty} a(i)z^i\right)\left(1 - z^d\right) = \sum_{i=0}^{d-1} a(i)z^i + \sum_{i=d}^{\infty}(a(i) - a(i-d))z^i \tag{4}$$

To divide by $1 - z^d$ we merely multiply by the power series for $\frac{1}{1-z^d}$:

$$\left(\sum_{i=0}^{\infty} a(i)z^i\right)\left(1 + z^d + z^{2d} + \cdots\right) = \sum_{i=0}^{\infty}\left(a(i) + a(i-d) + a(i-2d) + \cdots\right)z^i \tag{5}$$

Observe that the coefficients of $A(z)(1+z^d)$ and $a(n)(1+z^d)^{-1}$ depend strictly on coefficients of lesser degree in $A(z)$. In addition, we know that the $\phi(n)+1$ coefficients of $\Phi_n(z)$, $\{a_n(0), a_n(1), \ldots a_n(\phi(n))\}$, are palindromic, that is, $a_n(k) = a_n(\phi(n)-k)$. So, to calculate the $\Phi_n(z)$ as a power series, we only need compute the first $\frac{\phi(n)}{2}+1$ terms.

Input: $n = p_1 p_2 \cdots p_k$, a product of k distinct primes.
Output: $a(0), a(1), \cdots, a(\frac{\phi(n)}{2}+1)$, the first half of the coefficients of $\Phi_n(z)$

$M \longleftarrow \dfrac{\phi(n)}{2} + 1$
$a(0) \longleftarrow 1$
for $1 \leq i \leq M$ **do**
  $a(i) \longleftarrow 0$
for $d|n, d > 0$ **do**
  if $\frac{n}{d}$ *has an even number of prime factors* **then**
    $i \longleftarrow M$
    multiplying by $(1 - z^d)$:
    while $i \geq d$ **do**
      $a(i) \longleftarrow a(i) - a(i-d)$
      $i \longleftarrow i - 1$
  else
    $i \longleftarrow d$
    dividing by $(1 - z^d)$
    while $i \leq M$ **do**
      $a(i) \longleftarrow a(i) + a(i-d)$
      $i \longleftarrow i + 1$

Algorithm 4: solving $\Phi_n(z)$ as a quotient of sparse power series

Division by $(1-z^d)$ done naively could potentially be quadratic-time, ruining the efficiency of the algorithm. We avoid this by the following trick: Suppose we have the coefficients $a(0)$, $a(1)$, ... $a(\frac{\phi(n)}{2})$ of some power series $A(z)$ up to degree $D = \frac{\phi(n)}{2}$, and we want to calculate the coefficients $b(0), b(1), \cdots b(D)$ of the power series $A(z) \cdot (1-z^d)^{-1}$ up to degree D. We can calculate all the $b(i)$ in linear time, without using additional memory to store intermediate results. By equation 5, $b(i) = a(i)$ for $0 \leq i < d$. For $i > d$, where $i = qd + r$ and $0 \leq r < i$,

$$b(i) = a(i) + a(i-d) + \cdots a(i-qd). \tag{6}$$

Observing that $b(i-d) = a(i-d) + a(i-2d) + \cdots a(i-qd)$, we have that

$$b(i) = b(i-d) + a(i). \tag{7}$$

If we solve $b(i) = b(i-d) + a(i)$ for $i = d, d+1, \cdots, D$, we will have calculated all the $b(i)$ using at most one addition operation. Notice that after we use

Table 2: A comparison of running times of cyclotomic polynomial algorithms on a 3 GHz Intel Xeon system

Algorithm	Running time (seconds)		
	$n = 255255$	$n = 1181895$	$n = 43730115$
Maple `cyclotomic` command	429.14	-	-
Maple using machine precision integers	13.78	197.37	-
FFT algorithm using two 42-bit primes, plus an additional check prime	1.12	4.52	371.93
FFT algorithm using two 32-bit primes, plus one check prime	0.47	2.07	163.68
Power series algorithm with 64-bit precision	0.01	0.08	6.04

$a(i)$ to calculate $b(i)$, we never use $a(i)$ again. Thus, if we have an array in memory containing all our values $a(i)$, we can write all our values $b(i)$ into that array. We implement multiplication by $(1 - z^d)$ in a similar fashion that follows immediately from equation 4. Algorithm 4 details how we calculate $\Phi_n(z)$ using these techniques.

We have implemented a 64-bit and 128-bit version of this algorithm. We do not use the GNU Multi-Precision library for multiprecision arithmetic. We hand-coded our own 64 and 128-bit integer arithmetic that checks for overflow. This can be done without using redundant bits. We also have a modular implementation of the algorithm that calculates $\Phi_n(z)$ modulo many 16 or 32-bit primes, and reconstructs $\Phi_n(z)$ by Chinese remaindering. This version is particularly useful for calculating cyclotomic polynomials that we cannot completely store in main memory with large precision.

3.1 A comparison of the two algorithms.

Calculating $\Phi_n(z)$ by algorithm 4 for n, a product of k distinct primes takes $\mathcal{O}(2^k\phi(n))$ arithmetic operations and $4 \cdot \phi(n)$ bytes of memory to store the terms with 64-bit precision. We expect that our second approach is slower for n a product of many distinct small primes; however, we currently cannot calculate $\Phi_n(z)$ for odd n with more than 9 distinct prime factors. Calculating $\Phi_n(z)$ where $n = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$, the product of the smallest ten odd primes, would require $\frac{\phi(n)}{2} = 122624409600$ bytes (approximately 114 GB) of memory merely to store the polynomial coefficients up to 64-bit precision. In practice, the power series method is appreciably faster than the FFT approach.

Our implementation of algorithm 4 has several advantages. First, we can perform the calculations in memory; aside from a small overhead, all the memory

used in the power series algorithm is to store the coefficients. The power series algorithm makes better use of the memory used to store terms. Using 64-bits of storage for one term gives us exactly 64-bit precision using algorithm 4, whereas algorithm 1 uses 64-bits to store a 42-bit terms. In addition, the arithmetic operations used in algorithm 4 are strictly additions and subtractions, which take fewer CPU cycles than multiplication and division operations. In practice, algorithm 4 is more than an order of magnitude faster than algorithm 1 (see table 3.1).

4 Results

All of our numerical results can be found in the appendix.

4.1 Heights and Lengths of cyclotomic polynomials

To find cyclotomic polynomials with large heights, we considered some useful bounds on $A(n)$. Bang showed that for $n = pqr$, a product of three primes with $p < q < r$, that $A(n) < p$ and for n, a product of two primes, $A(n) = 1$ [1]. Bloom later proved for $n = pqrs$, a product of four primes with $p < q < r < s$, that $A(n) < p(p-1)(pq-1)$ [3]. Bateman, Pomerance, and Vaughan proved a more general albeit slightly weaker result [2]: for $n = p_1 p_2 \cdots p_k$, a product of k distinct primes with $p_1 < p_2 < \cdots p_k$,

$$A(n) \leq A(p_1 p_2 \cdots p_{k-1}) \prod_{j=0}^{k-2} S(p_1 p_2 \cdots p_j) \tag{8}$$

Using that $S(p_1 p_2 \cdots p_j) \leq A(p_1 p_2 \cdots p_j) \cdot p_1 p_2 \cdots p_j$ and Bang's results, they inductively obtain that

$$A(p_1 p_2 \cdots p_k) \leq \prod_{i=1}^{k-2} (p_i - 1)^{2^{k-i-1}-1} \tag{9}$$

For example, $A(p_1 p_2 p_3 p_4 p_5 p_6) \leq p_1^{15} p_2^7 p_3^3 p_4^4$. We use this bound to narrow our search for large values of $A(n)$, more specifically, $A(n)$ for which $A(n) > A(m)$ for $n < m$. Consider, for instance, $n = p_1 p_2 p_3 p_4 p_5$, a product of five primes where $p_1 < p_2 < p_3 < p_4 < p_5$. We have that $A(n) < p_1^7 p_2^3 p_3 < n^{2.2}$. Given that $\max_{1 \leq k \leq n} A(k)$ exceeds $n^{2.2}$ for $n > 43730115$, we skip products of five primes greater than 43730115.

Using the two methods detailed in this paper, we have created a library of data on $A(n)$ and $S(n)$. We include here our more noteworthy results. Table 3 shows those cyclotomic polynomials we have found whose height is greater than all those of smaller order. Excluding orders n less than roughly 10000, those orders n for which we obtain the largest heights also typically yield the largest lengths. Table 3 also shows the growth of $\log_n(A(n))$, which we found of interest. Our results include the first instances of n such that $A(n) > n$,

$A(n) > n^2$ and $A(n) > n^3$. Table 4 shows $A(n)$ for n, a product of the s smallest odd primes, for $1 \leq s \leq 9$. Table 5 shows $A(n)$ for various multiples of 43037115. $A(43037115)$ is the first instance of $A(n)$ such that $A(n) > n^2$. Equation 8 suggests that if order n produces a large height, that multiplying n by another prime may give an order of a cyclotomic polynomial of large height as well. This appears the case in table 5, which shows the four instances we have found such that $A(n) > n^4$.

4.2 Extreme values for the k_{th} cyclotomic polynomial coefficient $a_n(k)$

Table 6 gives the the maximum absolute value of $|a_n(k)|$ for fixed $k \leq 162$, and the smallest order n for which we obtain those extrema. Algorithm 4 tells us that $a_n(k)$ depends strictly on the divisors of n that are less than or equal to k. To find the extreme values of $a_n(k)$ for fixed k, we calculate $a_n(k)$ for all squarefree n whose prime divisors are not greater than k. It is easy to check by inspection whether a non-squarefree order will produce a larger coefficient. By lemma 2, if p divides n, then $a_{np}(k) = a_n(\frac{k}{p})$ if $p|k$, and 0 otherwise. Thus to prove that some non-squarefree order m will not produce a larger k_{th} coefficient $a_m(k)$ than every squarefree order, it suffices to show that for every positive divisor d of k, that

$$\max_{\text{squarefree } n} a_n(d) < \max_{\text{squarefree } n} a_n(k), \tag{10}$$

and similarly for the minimum values. Using this brute-force approach to find the minimum and maximum values of $a_n(k)$ for $0 \leq k \leq K$, where there are P primes less than or equal to K, we need to calculate the the first $K+1$ terms of some 2^P cyclotomic polynomials. We calculated the first 163 coefficients of some 2^{37} cyclotomic polynomials to produce these results. We find that $k = 119$ is the smallest $k > 0$ such that $a_n(k) > k$ for some n, as $\min_n a_n(119) = -136$.

Tables 7 shows, for $a \leq 250$, the smallest k such that $|a_n(k)| = a$, and for that a and k, the smallest order n. We extend results by Bosma [4], and by Grytczuk and Tropak[7]. Grytczuk and Tropak found results for $|a| \leq 10$. Bosma calculated results for $|a| \leq 50$. We have in fact calculated the smallest k such that $a_n(k) = a$ for $-575 \leq a \leq 585$. All of these results can be found at

`http://www.cecm.sfu.ca/~ada26/cyclotomic/`

4.3 Computing heights of larger order.

We are presently trying to compute the cyclotomic polynomials for

$$n = 99660932085 = (3)(5)(11)(13)(19)(29)(37)(43)(53),$$

which should have a very large height, and $n = 100280245065$, the product of the first 10 odd primes. These are too big to fit in main memory but perhaps they can be computed using algorithm 4 and disk storage.

References

[1] A. S. Bang. Om ligningen $\phi_n(x) = 0$. *Nyt Tidsskrift for Mathematik*, (6):6–12, 1895.

[2] P. T. Bateman, C. Pomerance, and R. C. Vaughan. On the size of the coefficients of the cyclotomic polynomial. In *Topics in classical number theory, Vol. I, II (Budapest, 1981)*, volume 34 of *Colloq. Math. Soc. János Bolyai*, pages 171–202. North-Holland, Amsterdam, 1984.

[3] D. M. Bloom. On the coefficients of the cyclotomic polynomials. *Amer. Math. Monthly*, 75:372–377, 1968.

[4] Wieb Bosma. Computation of cyclotomic polynomials with Magma. In *Computational algebra and number theory (Sydney, 1992)*, volume 325 of *Math. Appl.*, pages 213–225. Kluwer Acad. Publ., Dordrecht, 1995.

[5] Paul Erdős and R.C. Vaughn. On the coefficients of the cyclotomic polynomial. *Bull. Amer. Math. Soc.*, 52:179–184, 1946.

[6] Keith O. Geddes, Stephen R. Czapor, and George Labahn. *Algorithms for Computer Algebra*. Kluwer Academic Publishers, Boston, 1992.

[7] A. Grytczuk and B. Tropak. A numerical method for the determination of the cyclotomic polynomial coefficients. In *Computational number theory (Debrecen, 1989)*, pages 15–19. de Gruyter, Berlin, 1991.

[8] Yôichi Koshiba. On the calculations of the coefficients of the cyclotomic polynomials. *Rep. Fac. Sci. Kagoshima Univ.*, (31):31–44, 1998.

[9] Yôichi Koshiba. On the calculations of the coefficients of the cyclotomic polynomials. II. *Rep. Fac. Sci. Kagoshima Univ.*, (33):55–59, 2000.

[10] Helmut Maier. The size of the coefficients of cyclotomic polynomials. In *Analytic number theory, Vol. 2 (Allerton Park, IL, 1995)*, volume 139 of *Progr. Math.*, pages 633–639. Birkhäuser Boston, Boston, MA, 1996.

[11] R. Thangadurai. On the coefficients of cyclotomic polynomials. In *Cyclotomic fields and related topics (Pune, 1999)*, pages 311–322. Bhaskaracharya Pratishthana, Pune, 2000.

[12] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.

5 Appendix

Table 3: n such that $A(n) > A(m)$ for $m < n$

n	$A(n)$	$\log_n A(n)$
1	1	-
105	2	0.15
385	3	0.18
1365	4	0.19
1785	5	0.21
2805	6	0.23
3135	7	0.24
6545	9	0.25
10465	14	0.29
11305	23	0.34
17255	25	0.33
20615	27	0.33
26565	59	0.40
40755	359	0.55
106743	397	0.52
171717	434	0.50
255255	532	0.50
279565	1182	0.56
327845	31010	0.81
707455	35111	0.77
886445	44125	0.78
983535	59815	0.80
1181895	14102773	1.18
1752465	14703509	1.15
3949491	56938657	1.18
8070699	74989473	1.14
10163195	1376877780831	1.73
13441645	1475674234751	1.71
15069565	1666495909761	1.70
30489585	2201904353336	1.65
37495115	2286541988726	1.63
40324935	2699208408726	1.63
43730115	862550638890874931	2.35
169828113	**31484567640915734941	2.37
185626077	42337944402802720258	2.37
416690995	80103182105128365570406901971	3.35
437017385	86711753206816303264095919005	3.35
712407185	11185937095152669880319825792 5	3.28
1250072985	13756580004264445418853130688 6	3.20
1311052155	19289231441599758355173100941 0	3.22
1880394945	64540997036010911566826446181523888971563	4.40
2317696095	67075962666923019823602030663153118803367	4.36

****First instance such that $A(n) > 2^{64}$**

Table 4: $A(n)$ for n a product of the smallest odd primes

n	factorization of n	$A(n)$	$\log_n(A(n))$
105	$3 \cdot 5 \cdot 7$	2	0.15
1155	$3 \cdot 5 \cdot 7 \cdot 11$	3	0.16
15015	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	23	0.33
255255	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	532	0.50
4849845	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	**669606	0.87
111546435	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	8161018310	1.23
3234846615	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$	2888582082500892851	1.94

**(Koshiba,2002).

Table 5: $A(n)$ for n a multiple of $m = 43730115$

n	$A(n)$	$\log_n A(n)$
$7m = 306110805$	4722828832054556497	2.20
$17m = 743411955$	6456302257306534821	2.12
$23m = 1005792645$	1265789099436496061273	2.34
$31m = 1355633565$	234024136058399564071	2.23
$41m = 1792934715$	35986559322549038756	2.11
$43m = 1880394945$	64540997036010911566826446181523888971563	4.40
$47m = 2055315405$	440380022701792944369	2.22
$53m = 2317696095$	67075962666923019823602030663153118803367	4.36
$59m = 2580076785$	44175422396168003849853052788119894299323	4.32
$61m = 2667537015$	50961134639969020986073186655691393930064	4.32

Table 6: The maximum values of $|a_n(k)|$ for fixed k, $0 \le k \le 162$

k	$\max_n \lvert a_n(k)\rvert$	n
0	1	1
1	1	1
2	1	3
3	1	5
4	1	5
5	1	7
6	1	7
7	2	210
8	1	11
9	1	11
10	1	11
11	2	770
12	1	13
13	2	858
14	1	17
15	2	1430
16	2	165
17	3	646646
18	3	15015
19	3	646646
20	2	3927
21	3	2124694
22	3	373065
23	4	2124694
24	3	11305
25	3	2124694
26	3	2028117
27	3	2124694
28	4	37182145
29	4	3095547
30	5	37182145
31	4	10214438
32	4	40755
33	4	40755
34	5	275147873
35	5	10015005
36	6	215656441
37	5	13498485
38	5	103488385
39	6	170255085
40	6	17596892049

Continued on Next Page...

Table 6 – Continued

k	$\max_n \lvert a_n(k)\rvert$	n
41	6	63171570
42	6	955049953
43	7	131104243270
44	6	955049953
45	7	131104243270
46	8	845904650955
47	9	150290230090
48	9	17917712785
49	7	4925015277
50	8	1872852957833
51	8	14849835
52	10	30704573184285
53	13	291583831193655
54	12	25725453208455
55	10	14591862285
56	12	397428761916951765
57	9	18455277027
58	11	728792550255
59	15	442420697228304795
60	13	57927965433905
61	13	127091154560370
62	12	498899935172343705
63	15	378943703223140055
64	12	887324910800312985
65	16	2848916332815
66	15	993969333554296364265
67	15	63625798099535
68	14	3783331790535
69	16	1891748086442047919085
70	24	1091736808985866498455
71	17	25725453208455
72	21	63625798099535
73	21	1189504284417436632645
74	16	111495150862095
75	22	8259588898970029005
76	28	4982833447424642054149905
77	26	1256527270719582196335
78	21	4281025919618354440889355
79	28	1852415459294912176665
80	24	4728312119717787804808605
81	25	1587395172801733690395
82	35	1615936890023221260495
83	34	2380678513899766945785703155

Continued on Next Page...

Table 6 – Continued

k	$\max_n \lvert a_n(k)\rvert$	n
84	33	22038662790004608958212907905
85	28	1247748737866031606205
86	34	23806785138997669045785703155
87	36	4163737538258947469906085
88	37	6520570107084766792494435
89	49	167385506312292611060919278882805
90	43	203648402996245120753106611735
91	33	1106494163767990292295
92	44	1673855063122926110609192788828805
93	48	231545444502580068801477386885
94	49	248283669406381037630499848555
95	55	22659470192539950055627356015
96	53	133532257844637925677812008996395
97	53	33481178119721655445849732005
98	48	143185192146659944401509262658785
99	60	19482575324873402271025030820785
100	70	16395732925227694671832613762848 5
101	66	162491060750703981848903769983565
102	65	11527839819727592123765510736658780 35
103	70	16570870551804465475680285453769 5
104	65	162491060750703981848903769983565
105	68	17737867086825037888545177314446 5
106	91	17413114221667800328667432582178204 15
107	86	13859313041694970306100108413735837 05
108	78	12240902076617958646885026864699529 65
109	87	20500022683190892815326068986770 5
110	86	13859313041694970306100108413735837 05
111	86	15949477010855983623292008005514202 95
112	109	139993492552224470112239096122544194612 65
113	110	13417252766180944472850677946397154449365
114	98	12690998857538106169053450769987651287315
115	104	12003214657654503139178521488685946 55
116	108	13417252766180944472850677946397154449365
117	116	16257518586949770074583567079612611 15
118	124	16341725979698299454544252147247132 05
119	136	12942305765608167677351538904046812698945
120	136	13986749840892746808913808093603390483749861 5
121	118	143185192146659944401509262658785
122	132	12942305765608167677351538904046812698945
123	153	14500025064411746691809727656671404813428755 5
124	147	12458136493179608808153387453107143924245
125	162	12942305765608167677351538904046812698945
126	174	200723846966651809454722059951302256832294262386 5

Continued on Next Page...

Table 6 – Continued

k	$\max_n \lvert a_n(k)\rvert$	n
127	150	171127673492893481906389227422130158220 15
128	156	171239647584761666539038211239443378819741295
129	187	145000250644117466918097276566714048134287555
130	191	241236916996618229711638439024042161810142052535
131	196	171239647584761666539038211239443378819741295
132	201	200723846966651809454722059951302256832294262 3865
133	194	139867498408927468089138080936033904837498615
134	198	232697557102932628659899025253279607478146445 7755
135	213	162938425981534060763635083977029188109663335
136	237	207045857894735331012351101209610989330949199 7845
137	248	243355460481692901728291347020605391026763840 2385
138	229	153446867186493241690025273259920691714925665
139	243	276243710181827737764419468645851620788999034 3735
140	254	452645625918859120029573077462892895914235
141	251	633167761145979605542358107674651343519722323 5
142	294	281285173139005843509181852060685030308144796 4255
143	301	200723846966651809454722059951302256832294262 3865
144	291	116892483724340991053402819194270607854965738184285
145	301	452645625918859120029573077462892895914235
146	316	685755327805529852730955783837679993558095
147	330	674544779709846147504033218370947314887637 4015
148	337	207045857894735331012351101209610989330949199 7845
149	368	831438318905265125123349716730284208250729293657360 30
150	375	461608905640024647158871554244336319595705
151	384	242845163109929017909716028617535776293554299955190
152	393	478027623633935332367679979002868198488865
153	425	175298826350875913590457265690803970966870322484210
154	434	107542674229140771296568016004880130412536030921145
155	444	212530435487345134176041109731328708163373753808290
156	476	209245310257825056489376345377121525743100205570435 6755
157	495	216707997929822979792927485932726168833060162441110
158	501	820256580118655062857920788412942566687679186 5
159	534	391648911007684860907841400686572458936373717408625 8610
160	554	876494131754379567952286328454019854834351612421 05
161	575	384786677923785674349591400223699986936976216955029 3630
162	585	108353998964911489896463742966363084416530081220555

Table 7: Least k for which a occurs as $|a_n(k)|$, $0 < a \leq 250$

a	k	n
0	1	4
1	0	1
2	7	210
3	17	646646
4	23	2124694
5	30	37182145
6	36	215656441
7	43	131104243270
8	46	845904650955
9	47	150290230090
10	52	30704573184285
11	53	127943760945
12	53	2848916332815
13	53	291583831193655
14	59	159545869898415
15	59	442420697228304795
16	65	2848916332815
17	70	2848916332815
18	70	159545869898415
19	70	176794072049595
20	70	152125131763605
21	70	385941459284265885
22	70	307444891294245705
23	70	961380175077106319535
24	70	1091736808985866498455
25	76	397428761916951765
26	76	961380175077106319535
27	76	1664829083670110943585
28	76	49828334474246420541499905
29	82	397428761916951765
30	82	307444891294245705
31	82	385941459284265885
32	82	993969333554296364265
33	82	346693175289255795
34	82	961380175077106319535
35	82	1615936890023221260495
36	87	4163737538258947469906085
37	88	6520570107084766792494435
38	89	97970304029884898115
39	89	1156915125940246587915
40	89	1352450076803386856295
41	89	961380175077106319535

Continued on Next Page...

Table 7 – Continued

a	k	n
42	89	1189504284417436632645
43	89	1091736808985866498455
44	89	4281025919618354440889355
45	89	3929160775540133527939545
46	89	4702110436302127008845685
47	89	2380678513899766904578570315
48	89	2265947019253995005562735601
49	89	1673855063122926110609192788828
50	95	392916077554013352793954
51	95	4632891063696575353839165
52	95	428102591961835444088935
53	95	2036484029962451207531066173
54	95	2401227438313935005894839219
55	95	2265947019253995005562735601
56	99	4573285492841794762027995
57	99	5346235153603788242934135
58	99	2971263584699314056889588351
59	99	2770953680112843446312762170
60	99	1948257532487340227102503082078
61	100	4573285492841794762027995
62	100	5151743055811918055985495
63	100	4281025919618354440889355
64	100	3929160775540133527939545
65	100	4163737538258947469906085
66	100	2203866279000460895821290790
67	100	2482836694063810376304998485
68	100	2036484029962451207531066173
69	100	1504350752933262707003198582364
70	100	1639573292522769467183261376284
71	106	1189504284417436632645
72	106	5856673608823972617117435
73	106	993969333554296364265
74	106	961380175077106319535
75	106	1091736808985866498455
76	106	4982833447424642054149905
77	106	5544279469669672144758345
78	106	4163737538258947469906085
79	106	4632891063696575353839165
80	106	428102591961835444088935
81	106	4861504010414063517620115
82	106	4702110436302127008845685
83	106	2637413743721863039261544716
84	106	392916077554013352793954

Continued on Next Page...

Table 7 – Continued

a	k	n
85	106	22038662790004608958212907905
86	106	20364840299624512075310661735
87	106	22659470192539950055627356015
88	106	133532257844637925677812008996395
89	106	16738550631229261106091927888 2805
90	106	120032146576545031391785214886 8594655
91	106	17413114221667800328667432582178 20415
92	112	47021104363021270088456 85
93	112	42810259196183544408893 55
94	112	27060130261144899606919646415
95	112	28176011921398297528854477195
96	112	24828366940638103763049984855
97	112	22038662790004608958212907905
98	112	23154544450258006880147738685
99	112	22659470192539950055627356015
100	112	23806785138997669045785703155
101	112	20364840299624512075310661735
102	112	15605577121602263603310560087 5305
103	112	16249106075070398184890376998 3565
104	112	14318519214665994440150926265 8785
105	112	15043507529332627070031985823 6445
106	112	133532257844637925677812008996395
107	112	120032146576545031391785214886 8594655
108	112	12716276914544869662298037616726 69585
109	112	13999349255222447011223909612254419461265
110	113	13417252766180944472850677946397154449365
111	117	133532257844637925677812008996395
112	117	16395732925227694671832613762 8485
113	117	15043507529332627070031985823 6445
114	117	17071845623175228472732927732 4505
115	117	14738124326487174740510336511424 51665
116	117	16257518586949770074583567079612 61115
117	118	16738550631229261106091927888 2805
118	118	15605577121602263603310560087 5305
119	118	133532257844637925677812008996395
120	118	16249106075070398184890376998 3565
121	118	11527839819727592123765510736658 78035
122	118	14318519214665994440150926265 8785
123	118	120032146576545031391785214886 8594655
124	118	16341725979698299454544252147247 13205
125	119	16570870551804465475680285453 7695
126	119	15605577121602263603310560087 5305
127	119	18086014670096529174083398686 8535

Continued on Next Page...

Table 7 – Continued

a	k	n
128	119	150435075293326270700319858236445
129	119	133532257844637925677812008996395
130	119	16395732925227694671832613762848 5
131	119	129539643335083251700045429927402 7895
132	119	122409020766179586468850268646995 2965
133	119	115278398197275921237655107366587 8035
134	119	133412078812577751544701978188298 2445
135	119	127048322653217792796019693828716418 23735
136	119	129423057656081676773515389040468126 98945
137	123	22659470192539950055627356015
138	123	25527757558684247531023223865
139	123	20364840299624512075310661735
140	123	18243139452013913789785584327 6765
141	123	16570870551804465475680285453 7695
142	123	15605577121602263603310560087 5305
143	123	133532257844637925677812008996395
144	123	14318519214665994440150926265 8785
145	123	18305954945332473904496753833 5915
146	123	122409020766179586468850268646995 2965
147	123	115278398197275921237655107366587 8035
148	123	12716276914544869662298037616726695 85
149	123	12003214657654503139178521488685946 55
150	123	11992411764462614086353260819346129 198105
151	123	13156723586255100890853577403748666 013455
152	123	12458136493179608808153387453107143 924245
153	123	14500025064411746691809727656671404 8134287555
154	125	133412078812577751544701978188298 2445
155	125	12716276914544869662298037616726695 85
156	125	12003214657654503139178521488685946 55
157	125	115278398197275921237655107366587 8035
158	125	129539643335083251700045429927402 7895
159	125	122409020766179586468850268646995 2965
160	125	11992411764462614086353260819346129 198105
161	125	13476009096148710674355726075347712 191685
162	125	129423057656081676773515389040468126 98945
163	126	17214399505272600057260102364595 5
164	126	133532257844637925677812008996395
165	126	15093151104179424739363091376862526 85
166	126	12003214657654503139178521488685946 55
167	126	12716276914544869662298037616726695 85
168	126	115278398197275921237655107366587 8035
169	126	13859313041694970306100108413735837 05
170	126	11992411764462614086353260819346129 198105

Continued on Next Page...

Table 7 – Continued

a	k	n
171	126	1245813649317960880815338745310714392424 5
172	126	14771053570288601770161311351188627333305928 5
173	126	139867498408927468089138080936033904837498615
174	126	200723846966651809454722059951302256832294262386 5
175	129	14027853274608274753015862462681166 45
176	129	15613656464694333635986198086360626 55
177	129	13353225784463792567781200899639 5
178	129	14118365621913567881915063711188843 35
179	129	12953964333508325170004542992740278 95
180	129	11527839819727592123765510736658780 35
181	129	13429339171435236185417553744767445 15
182	129	12716276914544869662298037616726695 85
183	129	13156723586255100890853577403748666013455
184	129	1245813649317960880815338745310714392424 5
185	129	13938311126032631636844879031694131321185
186	129	15344686718649324169002527325992069171492566 5
187	129	14500025064411746691809727656671404813428755 5
188	130	11992411764462614086353260819346129198105
189	130	16809763570247246164841365690477469296983778 5
190	130	14500025064411746691809727656671404813428755 5
191	130	24123691699661822971163843902404216188101420525 35
192	131	11992411764462614086353260819346129198105
193	131	13444919581748290693947715172165135522205
194	131	12690998857538106169053450769987651287315
195	131	139867498408927468089138080936033904837498615
196	131	17123964758476166653903821123944337881974129 5
197	132	13228742874201027909688648532680781692755
198	132	13970541540044076203689881160681573189545
199	132	14500025064411746691809727656671404813428755 5
200	132	16293842598153406076363508397702918810966333 5
201	132	200723846966651809454722059951302256832294262386 5
202	135	13891360783577683408262783295894971 85
203	135	11527839819727592123765510736658780 35
204	135	14895555539017034016089008594393403 55
205	135	12240902076617958646885026864699529 65
206	135	16341725979698299454544252147247132 05
207	135	12003214657654503139178521488685946 55
208	135	15701405093677855556359423959350086682055
209	135	13156723586255100890853577403748666013455
210	135	17225813355199977455035096188413201893905
211	135	13970541540044076203689881160681573189545
212	135	18984568898765895153194179509250189807272700 5
213	135	16293842598153406076363508397702918810966333 5

Continued on Next Page...

Table 7 – Continued

a	k	n
214	136	1740990197214899537318308471725 15
215	136	1808601467009652917408339868685 35
216	136	1402785327460827475301586246268116645
217	136	1504350752933262707003198582364 45
218	136	1335322578446379256778120089963 95
219	136	1470056626611618923787032407041312555
220	136	1389136078357768340826278329589497185
221	136	1443083110527002062800114381224040765
222	136	1557386723242012127180321460924954885
223	136	1200321465765450313917852148868594655
224	136	1295396433350832517000454299274027895
225	136	1224090207661795864688502686469952965
226	136	1271627691454486966229803761672669585
227	136	1385931304169497030610010841373583705
228	136	1322874287420102790968864853268078169 2755
229	136	1152783981972759212376551073665878035
230	136	1269099885753810616905345076998765128 7315
231	136	1199241176446261408635326081934612919 8105
232	136	1245813649317960880815338745310714392 4245
233	136	1344491958174829069394771517216513552 2205
234	136	1270483226532177927960196938287164182 3735
235	136	1398674984089274680891380809360339048374986 15
236	136	1564854190119683553868574568888300123429439 95
237	136	2070458578947353310123511012096109893309491997845
238	137	1341725276618094447285067794639715444936 5
239	137	1200321465765450313917852148868594655
240	137	1451308684257005974558075033197017797360 5
241	137	1315672358625510089085357740374866601345 5
242	137	1245813649317960880815338745310714392 4245
243	137	1322874287420102790968864853268078169 2755
244	137	1199241176446261408635326081934612919 8105
245	137	1450002506441174669180972765667140481342875 55
246	137	1398674984089274680891380809360339048374986 15
247	137	2007238469666518094547220599513022568322942623865
248	137	2433554604816929017282913470206053910267638402385
249	140	4361167992281136140568196140889227246 5
250	140	3957891671439806629159492019586181253 5