

# Calculating cyclotomic polynomials

Andrew Arnold (ada26@sfu.ca)

Michael Monagan (mmonagan@cecm.sfu.ca)

July 16, 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, optimized using the discrete Fourier transform. The second algorithm calculates  $\Phi_n(z)$  as a quotient of sparse power series. These algorithms were used to calculate cyclotomic polynomials of large height and length. In particular we find cyclotomic polynomials  $\Phi_n(z)$  of minimal order  $n$  whose height is greater than  $n$ ,  $n^2$ ,  $n^3$ , and  $n^4$ , respectively.

## 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 in  $\mathbb{Z}$  of degree  $\phi(n)$  where  $\phi(n)$  is Euler's function. We write

$$\Phi_n(z) = \sum_{k=1}^{\phi(n)} a_n(k) z^k,$$

It is well known that for  $n < 105$ , the coefficients of  $\Phi_n(z)$  are strictly  $-1, 0$ , or  $1$  and that both  $2$  and  $-2$  appear as coefficients in  $\Phi_{105}(z)$ . Denote by  $A(n)$  and  $S(n)$  the height and length, respectively, of the  $n$ th cyclotomic polynomial. That is,

$$A(n) = \max_{0 \leq k \leq \phi(n)} |a_n(k)|, \quad S(n) = \sum_{k=0}^{\phi(n)} |a_n(k)|.$$

Paul Erdos [5] proved that  $A(n)$  is not bounded above by any polynomial of  $n$ , 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. Koshiya 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  $n$  over 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 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  $n < 6 \cdot 10^8$  with six or more prime factors
4.  $A(n)$  and  $S(n)$  for squarefree  $n < 1.3 \cdot 10^9$  with seven or more prime factors
5.  $A(n)$  and  $S(n)$  for squarefree  $n < 2 \cdot 10^9$  with eight or more prime factors
6. the smallest values of  $n$  for which  $A(n) > n, n^2$  and  $n^3$  respectively
7. an order  $n$  for which  $A(n) > n^4$
8. the smallest  $n$  such that  $A(n) > 2^{64}$  (machine precision)
9. the maximum and minimum values of  $a_n(k)$  for fixed  $k$ , for  $k < 148$
10. the smallest instance of  $k$  for which  $a_n(k) = a$  for some  $n$ , for  $|a| < 248$

We include in this paper items 6,7, as well as the maximum values for  $|a_n(k)|$ , for fixed  $k \leq 148$ , and the smallest instance of  $k$  for which  $|a_n(k)| = a$ , for  $|a| < 248$ . All of the data listed above is available on the web at

<http://www.cecm.sfu.ca/~mmonagan/research/Heights.html>

## 1.2 Preliminaries

We are interested in finding cyclotomic polynomials with large coefficients for  $n = 105$ , etc. 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 squarefree, 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 to calculate $\Phi_n(z)$

Our first algorithm calculates  $\Phi_n(z)$  by a series of polynomial divisions. For primes  $p \nmid m$ ,

$$\Phi_{mp}(z) = \frac{\Phi_m(z^p)}{\Phi_m(z)}. \quad (1)$$

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.  
 $m \leftarrow 1$   
 $\Phi_m(z) \leftarrow z - 1$   
**for**  $j = 1$  **to**  $k$  **do**  
     $m^* \leftarrow m p_j$   
     $\Phi_{m^*}(z) \leftarrow \frac{\Phi_m(z^{p_j})}{\Phi_m(z)}$   
     $m \leftarrow m^*$

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

Our key optimization was to perform the polynomial division in algorithm 1 by way of the discrete Fourier transform (DFT)[6]. Algorithm 2 gives a high-level description of the division calculation. Using the discrete 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.

Observe that algorithm 2 requires that  $B_i$  is nonzero for  $\omega^i$ ,  $0 \leq i < N$ . This is not a problem for odd orders  $m$ , however, so long as our modulus  $q$  does not

**Input:**

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

**Output:**  $\Phi_{mp}(z)$ 

Calculate  $A_i$  and  $B_i$  by the DFT:

$$A_i \leftarrow \Phi_n(\omega^{ip}) \bmod q \text{ for } i = 0, 1, \dots, N - 1$$

$$B_i \leftarrow \Phi_n(\omega^i) \bmod q \text{ for } i = 0, 1, \dots, N - 1$$

$$C_i \leftarrow \frac{A_i}{B_i} \text{ for } i = 0, 1, \dots, N - 1 \quad /* C_i = \Phi_{mp}(\omega^i) */$$

Interpolate  $C$  by the inverse discrete fast Fourier transform to get the coefficients of  $\Phi_{mp}(z)$ .

**Algorithm 2:** A brief description of polynomial division via the discrete fast Fourier transform

divide the order  $m$ . Every power of  $\omega$  is a  $2^k$ th root of unity modulo  $q$  for some  $k < s$ . For  $m > 1$  it holds that  $\Phi_m(z)$  divides

$$\frac{z^m - 1}{z - 1} = z^{m-1} + z^{m-2} + \dots + z + 1. \quad (2)$$

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 always 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

Our implementation of the DFT modulo a 42-bit prime  $q$  requires  $12N$  bytes of storage:  $8N$  to store the input polynomial and the result of the DFT, and another  $4N$  bytes in which we use for the DFT computation. We require that  $N$  is a power of two greater than  $\phi(n/p_k)p_k$ , the degree of the numerator  $\Phi_{n/p_k}(z^{p_k})$ . For 32-bit primes  $q$ ,  $N$  is no greater than  $2^{27}$ . For cyclotomic polynomials of larger degree, we require larger primes. Choosing unnecessarily large primes for the DFT, however, would require multiprecision arithmetic. Using 64-bit arithmetic, we are able to do multiplication modulo prime numbers as large as 42-bits (see algorithm 3); however, the multiplication is roughly four times slower than multiplying two integers. We typically use a 32-bit prime unless a 42-bit prime is necessary. Our implementation of algorithm 2 requires  $20N$  bytes of storage:  $16N$  bytes to store the intermediate results  $A_i$  and  $B_i$  for  $0 \leq i < N$ , and additional  $4N$  bytes of memory for the DFT computation.

The DFT 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  $A(n) > \frac{q_1}{2}$ . If the

<b>Input:</b> $a = a_{41}a_{40} \cdots a_1a_0, b = b_{41}b_{40} \cdots b_1b_0$ , two 42-bit primes modulo a 42-bit prime $q$	
<b>Output:</b> $c = ab \pmod q$	
$A_0 \leftarrow a_{20}a_{19} \cdots a_0$	$/* A_0 = a \pmod{2^{21}} */$
$A_1 \leftarrow a_{41}a_{40} \cdots a_{21}$	$/* A_1 = (a - A_0)/2^{21} */$
$B_0 \leftarrow b_{20}b_{19} \cdots b_0$	$/* B_0 = b \pmod{2^{21}} */$
$B_1 \leftarrow b_{41}b_{40} \cdots b_{21}$	$/* B_1 = (b - B_0)/2^{21} */$
$c \leftarrow (A_1)(B_1)(2^{21}) + (A_1)(B_0) + (A_0)(B_1)$	
$c \leftarrow c \pmod q$	
$c \leftarrow (c)(2^{21}) + (A_0)(B_0) \pmod q$	

**Algorithm 3:** multiplication modulo a 42-bit prime

height of  $H_n(z)$  is close to  $\frac{q_1}{2}$ , we calculate  $\Phi_n(z)$  modulo another prime  $q_2$ . We then reconstruct  $H_n(z) \equiv \Phi_n(z) \pmod{q_1q_2}$  by Chinese remaindering. We do this process with primes  $q_1, q_2 \dots q_l$  until the height of  $H_n(z)$  is less than  $\frac{q_1q_2 \cdots q_l}{2}$  by a factor of  $2^{20}$  or more. We then take our solution  $H_n(z)$  and use the DFT to test that

$$H_n(\omega^j) \cdot \Phi_{n/p_k}(\omega^j) - \Phi_{n/p_k}(\omega^{jp_k}) \equiv 0 \pmod{q_{l+1}}, \quad (3)$$

for some new prime  $q_{l+1}$  with  $N_{th}$  primitive root  $\omega$ . If equation (3) 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. All our results obtained by this method have been consistent with results we have obtained by non-modular algorithms. It is very unlikely that  $\Phi_n(z)$  would have coefficients strictly in such a small range mod  $Q$  provided its height  $A(n)$  were greater than  $\frac{Q}{2}$ . Table 1 lists the primes and the primitive roots we used in our computations.

	$q =$	$r \cdot N + 1$	size of $q$	$\omega$
$q_1$	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 DFT calculations

The brunt of the computation takes place in the last division step, as each successive division step involves polynomials of greater degree, which requires us to use larger  $N$  for the DFT. For squarefree  $n$  with largest prime divisor  $p$ , we can compute  $\Phi_n(z)$  in  $\mathcal{O}(\phi(\frac{n}{p})p \cdot \log(\frac{n}{p}p))$  arithmetic operations. Our implementation of algorithm 2 modulo one 42-bit prime  $q$  requires  $20N$  bytes of storage:  $8N$  bytes are used to store the numerator and the final result; an additional  $4N$  bytes are used in the DFT computation.

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

It is well known that

$$\Phi_n(z) = \prod_{d|n} (1 - z^d)^{\mu(\frac{n}{d})}, \quad (4)$$

where  $\mu$  is the Möbius 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  $C(z) = \sum_{i=0}^{\infty} c_n z^n$  by  $1 - z^d$  is easy:

$$\left( \sum_{i=0}^{\infty} c_n z^n \right) (1 - z^d) = \sum_{i=0}^{d-1} c_n z^i + \sum_{i=d}^{\infty} (c_i - c_{i-d}) z^i \quad (5)$$

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

$$\left( \sum_{i=0}^{\infty} c_n z^n \right) (1 + z^d + z^{2d} + \dots) = \sum_{i=0}^{\infty} (c_i + c_{i-d} + c_{i-2d} + \dots) z^i \quad (6)$$

Observe that the coefficients of  $C(z)(1+z^d)$  and  $C(z)(1+z^d)^{-1}$  depend strictly on coefficients of lesser degree in  $C(z)$ . In addition, we know that the  $\phi(n) + 1$  coefficients of  $\Phi_n(z)$ ,  $\{a_n(0), a_n(1), \dots, a_n(\phi(n))\}$ , 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.

#### 3.1 A comparison of the two algorithms.

Calculating  $\Phi_n(z)$  for  $n$ , a product of  $k$  distinct primes takes  $\mathcal{O}(2^k \phi(n))$  arithmetic operations and  $4\phi(n)$  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 practise, the power series method is appreciably faster than the DFT 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

```

Input:  $n = p_1 p_2 \cdots p_k$ , a product of  $k$  distinct primes.
Output:  $a_n(0), a_n(1), \dots, a_n(\frac{\phi(n)}{2} + 1)$ , the first half of the coefficients
of  $\Phi_n(z)$ 
 $M \leftarrow \frac{\phi(n)}{2} + 1$ 
 $a_n(0) \leftarrow 1$ 
for  $1 \leq i \leq M$  do
   $a_n(i) \leftarrow 0$ 
for  $d|n, d > 0$  do
  if  $\frac{n}{d}$  has an even number of prime factors then
     $i \leftarrow M$ 
    while  $i \geq d$  do
       $c_i \leftarrow a_n(i) - a_n(i - d)$ 
       $i \leftarrow i - 1$ 
    else
       $i \leftarrow d$ 
      while  $i \leq M$  do
         $a_n(i) \leftarrow a_n(i) + a_n(i - d)$ 
         $i \leftarrow i + 1$ 

```

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

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 practise, algorithm 4 is approximately 30 times faster than algorithm 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 strictly looked at cyclotomic polynomials of squarefree, odd order. For odd  $n > 1$ , it holds that

$$\Phi_{2n}(z) = \Phi_n(-z), \quad (7)$$

and so  $A(2n) = A(n)$ ; moreover, for any prime  $p$  dividing some integer  $n$ ,

$$\Phi_{np}(z) = \Phi_n(z^p), \quad (8)$$

thus  $A(np) = A(n)$ . We also considered the number of prime factors of  $n$ . Bang showed that for  $n = pqr$ , a product of three primes with  $p < q < r$ , that  $A(n) < p$ . 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 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  $p_1 < p_2 < \cdots < p_k$ , exceeding  $n^4$ .

$$A(n) \leq \prod_{k=1}^{j-2} p_k^{2^{j-k-1}-1}. \quad (9)$$

For instance, for  $n = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5$ ,  $A(n) < p_1^7 \cdot p_2^3 \cdot p_3^1 < n^2$ .

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 2 shows those cyclotomic polynomials we have found whose height is greater than all those of smaller order. We include the lengths as well. Excluding orders  $n$  less than roughly 10000, those orders  $n$  for which we obtain the largest heights also typically yield the largest lengths. Table 2 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 3 shows  $A(n)$  for  $n$ , a product of the  $s$  smallest odd primes, for  $1 \leq s \leq 9$ . Table 4 shows  $A(n)$  for various multiples of 43037115.  $A(43037115)$  was is first instance of  $A(n)$  such that  $A(n) > n^2$ . We expected that if order  $n$  produced a large height, that multiplying  $n$  by another prime would result in large heights as well. Table 4 shows how we found the biggest values for  $A(n)$  we have obtained so far – four values with  $A(n) > n^4$ . Indeed, given for primes  $p$  such that  $p \nmid n$

$$\Phi_{np}(z) = \frac{\Phi_n(z^p)}{\Phi_n(z)}, \quad (10)$$

it holds that  $A(np) \leq A(n)S(n)$ . This follows by inspection of long division. Table 4 notably has the first four  $n$  we have found for which  $A(n) > n^4$ .

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

Table 5 gives the the maximum absolute value of  $|a_n(k)|$  for fixed  $k \leq 148$ , 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  $n$  will not produce a larger coefficient  $a_n(k)$ , it suffices to show that for every positive divisor  $d$  of  $k$ , that

$$\max_n a_n(d) < \max_n a_n(k), \quad (11)$$

and similarly for the minimum values. 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. Tentatively we have results for  $K = 138$ . We find the  $k = 119$  is the smallest  $k > 0$  such that  $a_n(k) > k$  for some  $n$ , as  $\min_n a_n(119) = -136$ .

Tables 6 shows, for  $-248 \leq a \leq 248$ , 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 Tropicak[7].

## References

- [1] A. S. Bang. Om ligningen  $\phi_n(x) = 0$ . *Nyt Tidsskrift for Matematik*, (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, 101 Philip Drive, Assinippi Park, Norwell, Massachusetts 02061 USA, 1992.
- [7] A. Grytczuk and B. Tropicak. 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 Koshihira. On the calculations of the coefficients of the cyclotomic polynomials. *Rep. Fac. Sci. Kagoshima Univ.*, (31):31–44, 1998.
- [9] Yôichi Koshihira. 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.

## 5 Appendix

Table 2:  $n$  such that  $A(n) > A(m)$  for  $m < n$

$n$	$A(n)$	$S(n)$	$\log_n A(n)$
1	1	1	-
105	2	35	0.15
385	3	219	0.18
1365	4	639	0.19
1785	5	987	0.21
2805	6	2231	0.23
3135	7	2853	0.24
6545	9	6563	0.25
10465	14	20747	0.29
11305	23	48893	0.34
17255	25	81517	0.33
20615	27	98157	0.33
26565	59	152149	0.40
40755	359	1896745	0.55
106743	397	6362025	0.52
171717	434	10258345	0.50
255255	532	8784659	0.50
279565	1182	27024801	0.56
327845	31010	1967355537	0.81
707455	35111	4976000157	0.77
886445	44125	6564013961	0.78
983535	59815	6689950767	0.80
1181895	14102773	2189485343213	1.18
1752465	14703509	3180720401669	1.15
3949491	56938657	32085727023085	1.18
8070699	74989473	89647642675785	1.14
10163195	1376877780831	2537194394168988549	1.73
13441645	1475674234751	3701817831306521717	1.71
15069565	1666495909761	4321747364216785297	1.70
30489585	2201904353336	10666361061590540191	1.65
37495115	2286541988726	13915523932865067641	1.63
40324935	2699208408726	14360210245699163747	1.63
43730115	862550638890874931	4324164200335279163572713	2.35
169828113	31484567640915734941	729226462343060056562590557	2.37
185626077	42337944402802720258	1022825486031084909139839773	2.37
416690995	80103182105128365570406901971	5501746104401532041904501220254174393	3.35
437017385	86711753206816303264095919005	5897388783148538992443295292389679821	3.35
712407185	111859370951526698803198257925	1192111113823611743144623717383264530	3.28
1250072985	137565800042644454188531306886	24089889001907097594773048678814820831	3.20
1311052155	192892314415997583551731009410	26625004087406986183656170071582476711	3.22

Table 3:  $A(n)$  for  $n$  a product of the smallest odd primes

$n$	factorization of $n$	$A(n)$
105	$3 \cdot 5 \cdot 7$	3
1155	$3 \cdot 5 \cdot 7 \cdot 11$	3
15015	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	23
255255	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	532
4849845	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	669606*
111546435	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	8161018310
3234846615	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$	2888582082500892851

\*(Koshiba,2002).

Table 4:  $A(n)$  for  $n$  a multiple of  $m = 43730115$

$n$		$A(n)$
$7m =$	306110805	4722828832054556497
$17m =$	743411955	6456302257306534821
$23m =$	1005792645	1265789099436496061273
$31m =$	1355633565	234024136058399564071
$41m =$	1792934715	35986559322549038756
$43m =$	1880394945	64540997036010911566826446181523888971563
$47m =$	2055315405	440380022701792944369
$53m =$	2317696095	67075962666923019823602030663153118803367
$59m =$	2580076785	44175422396168003849853052788119894299323
$61m =$	2667537015	50961134639969020986073186655691393930064

Table 5: The maximum values of  $|a_n(k)|$  for fixed  $k$ ,  $0 \leq k \leq 148$

$k$	$\max_n  a_n(k) $	$n$
0	1	1
1	1	2
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 5 – Continued

$k$	$\max_n  a_n(k) $	$n$
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	23806785138997669045785703155

Continued on Next Page...

Table 5 – Continued

$k$	$\max_n  a_n(k) $	$n$
84	33	22038662790004608958212907905
85	28	1247748737866031606205
86	34	23806785138997669045785703155
87	36	4163737538258947469906085
88	37	6520570107084766792494435
89	49	167385506312292611060919278882805
90	43	20364840299624512075310661735
91	33	1106494163767990292295
92	44	167385506312292611060919278882805
93	48	23154544450258006880147738685
94	49	24828366940638103763049984855
95	55	22659470192539950055627356015
96	53	133532257844637925677812008996395
97	53	33481178119721655445849732005
98	48	143185192146659944401509262658785
99	60	194825753248734022710250308207855
100	70	163957329252276946718326137628485
101	66	162491060750703981848903769983565
102	65	1152783981972759212376551073665878035
103	70	165708705518044654756802854537695
104	65	162491060750703981848903769983565
105	68	177378670868250378885451773144465
106	91	1741311422166780032866743258217820415
107	86	1385931304169497030610010841373583705
108	78	1224090207661795864688502686469952965
109	87	205000226831908928153260689867705
110	86	1385931304169497030610010841373583705
111	86	1594947701085598362329200800551420295
112	109	13999349255222447011223909612254419461265
113	110	13417252766180944472850677946397154449365
114	98	12690998857538106169053450769987651287315
115	104	1200321465765450313917852148868594655
116	108	13417252766180944472850677946397154449365
117	116	1625751858694977007458356707961261115
118	124	1634172597969829945454425214724713205
119	136	12942305765608167677351538904046812698945
120	136	139867498408927468089138080936033904837498615
121	118	143185192146659944401509262658785
122	132	12942305765608167677351538904046812698945
123	153	145000250644117466918097276566714048134287555
124	147	12458136493179608808153387453107143924245
125	162	12942305765608167677351538904046812698945
126	174	2007238469666518094547220599513022568322942623865

Continued on Next Page...

Table 5 – Continued

$k$	$\max_n  a_n(k) $	$n$
127	150	17112767349289348190638922742213015822015
128	156	171239647584761666539038211239443378819741295
129	187	145000250644117466918097276566714048134287555
130	191	2412369169966182297116384390240421618810142052535
131	196	171239647584761666539038211239443378819741295
132	201	2007238469666518094547220599513022568322942623865
133	194	139867498408927468089138080936033904837498615
134	198	2326975571029326286598990252532796074781464457755
135	213	162938425981534060763635083977029188109663335
136	237	2070458578947353310123511012096109893309491997845
137	248	2433554604816929017282913470206053910267638402385
138	229	153446867186493241690025273259920691714925665
139	243	2762437101818277377644194686458516207889990343735
140	254	452645625918859120029573077462892895914235
141	251	6331677611459796055423581076746513435197223235
142	294	2812851731390058435091818520606850303081447964255
143	301	2007238469666518094547220599513022568322942623865
144	291	116892483724340991053402819194270607854965738184285
145	301	452645625918859120029573077462892895914235
146	316	685755327805529852730955783837679993558095
147	330	6745447797098461475040332183709473148876374015
148	337	2070458578947353310123511012096109893309491997845

Table 6: Least  $k$  for which  $a$  occurs as  $|a_n(k)|$ ,  $0 < a \leq 248$

$a$	$k$	$n$
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	4982833447424642054149905
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 6 – Continued

<i>a</i>	<i>k</i>	<i>n</i>
42	89	1189504284417436632645
43	89	1091736808985866498455
44	89	4281025919618354440889355
45	89	3929160775540133527939545
46	89	4702110436302127008845685
47	89	23806785138997669045785703155
48	89	22659470192539950055627356015
49	89	167385506312292611060919278882805
50	95	3929160775540133527939545
51	95	4632891063696575353839165
52	95	4281025919618354440889355
53	95	20364840299624512075310661735
54	95	24012274383139350058948392195
55	95	22659470192539950055627356015
56	99	4573285492841794762027995
57	99	5346235153603788242934135
58	99	29712635846993140568895883515
59	99	27709536801128434463127621705
60	99	194825753248734022710250308207855
61	100	4573285492841794762027995
62	100	5151743055811918055985495
63	100	4281025919618354440889355
64	100	3929160775540133527939545
65	100	4163737538258947469906085
66	100	22038662790004608958212907905
67	100	24828366940638103763049984855
68	100	20364840299624512075310661735
69	100	150435075293326270700319858236445
70	100	163957329252276946718326137628485
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	4281025919618354440889355
81	106	4861504010414063517620115
82	106	4702110436302127008845685
83	106	26374137437218630392615447165
84	106	3929160775540133527939545

Continued on Next Page...

Table 6 – Continued

<i>a</i>	<i>k</i>	<i>n</i>
85	106	22038662790004608958212907905
86	106	20364840299624512075310661735
87	106	22659470192539950055627356015
88	106	133532257844637925677812008996395
89	106	167385506312292611060919278882805
90	106	1200321465765450313917852148868594655
91	106	1741311422166780032866743258217820415
92	112	4702110436302127008845685
93	112	4281025919618354440889355
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	156055771216022636033105600875305
103	112	162491060750703981848903769983565
104	112	143185192146659944401509262658785
105	112	150435075293326270700319858236445
106	112	133532257844637925677812008996395
107	112	1200321465765450313917852148868594655
108	112	1271627691454486966229803761672669585
109	112	1399934925522447011223909612254419461265
110	113	13417252766180944472850677946397154449365
111	117	133532257844637925677812008996395
112	117	163957329252276946718326137628485
113	117	150435075293326270700319858236445
114	117	170718456231752284727329277324505
115	117	1473812432648717474051033651142451665
116	117	1625751858694977007458356707961261115
117	118	167385506312292611060919278882805
118	118	156055771216022636033105600875305
119	118	133532257844637925677812008996395
120	118	162491060750703981848903769983565
121	118	1152783981972759212376551073665878035
122	118	143185192146659944401509262658785
123	118	1200321465765450313917852148868594655
124	118	1634172597969829945454425214724713205
125	119	165708705518044654756802854537695
126	119	156055771216022636033105600875305
127	119	180860146700965291740833986868535

Continued on Next Page...

Table 6 – Continued

<i>a</i>	<i>k</i>	<i>n</i>
128	119	150435075293326270700319858236445
129	119	133532257844637925677812008996395
130	119	163957329252276946718326137628485
131	119	1295396433350832517000454299274027895
132	119	1224090207661795864688502686469952965
133	119	1152783981972759212376551073665878035
134	119	1334120788125777515447019781882982445
135	119	12704832265321779279601969382871641823735
136	119	12942305765608167677351538904046812698945
137	123	22659470192539950055627356015
138	123	25527757558684247531023223865
139	123	20364840299624512075310661735
140	123	182431394520139137897855843276765
141	123	165708705518044654756802854537695
142	123	156055771216022636033105600875305
143	123	133532257844637925677812008996395
144	123	143185192146659944401509262658785
145	123	183059549453324739044967538335915
146	123	1224090207661795864688502686469952965
147	123	1152783981972759212376551073665878035
148	123	1271627691454486966229803761672669585
149	123	1200321465765450313917852148868594655
150	123	11992411764462614086353260819346129198105
151	123	13156723586255100890853577403748666013455
152	123	12458136493179608808153387453107143924245
153	123	145000250644117466918097276566714048134287555
154	125	1334120788125777515447019781882982445
155	125	1271627691454486966229803761672669585
156	125	1200321465765450313917852148868594655
157	125	1152783981972759212376551073665878035
158	125	1295396433350832517000454299274027895
159	125	1224090207661795864688502686469952965
160	125	11992411764462614086353260819346129198105
161	125	13476009096148710674355726075347712191685
162	125	12942305765608167677351538904046812698945
163	126	172143995052726000572601023645955
164	126	133532257844637925677812008996395
165	126	1509315110417942473936309137686252685
166	126	1200321465765450313917852148868594655
167	126	1271627691454486966229803761672669585
168	126	1152783981972759212376551073665878035
169	126	1385931304169497030610010841373583705
170	126	11992411764462614086353260819346129198105

Continued on Next Page...

Table 6 – Continued

$a$	$k$	$n$
171	126	12458136493179608808153387453107143924245
172	126	147710535702886017701613113511886273333059285
173	126	139867498408927468089138080936033904837498615
174	126	2007238469666518094547220599513022568322942623865
175	129	1402785327460827475301586246268116645
176	129	1561365646469433363598619808636062655
177	129	133532257844637925677812008996395
178	129	1411836562191356788191506371118884335
179	129	1295396433350832517000454299274027895
180	129	1152783981972759212376551073665878035
181	129	1342933917143523618541755374476744515
182	129	1271627691454486966229803761672669585
183	129	13156723586255100890853577403748666013455
184	129	12458136493179608808153387453107143924245
185	129	13938311126032631636844879031694131321185
186	129	153446867186493241690025273259920691714925665
187	129	145000250644117466918097276566714048134287555
188	130	11992411764462614086353260819346129198105
189	130	168097635702472461648413656904774692969837785
190	130	145000250644117466918097276566714048134287555
191	130	2412369169966182297116384390240421618810142052535
192	131	11992411764462614086353260819346129198105
193	131	13444919581748290693947715172165135522205
194	131	12690998857538106169053450769987651287315
195	131	139867498408927468089138080936033904837498615
196	131	171239647584761666539038211239443378819741295
197	132	13228742874201027909688648532680781692755
198	132	13970541540044076203689881160681573189545
199	132	145000250644117466918097276566714048134287555
200	132	162938425981534060763635083977029188109663335
201	132	2007238469666518094547220599513022568322942623865
202	135	1389136078357768340826278329589497185
203	135	1152783981972759212376551073665878035
204	135	148955553901703401608900859439340355
205	135	1224090207661795864688502686469952965
206	135	1634172597969829945454425214724713205
207	135	1200321465765450313917852148868594655
208	135	15701405093677855556359423959350086682055
209	135	13156723586255100890853577403748666013455
210	135	17225813355199977455035096188413201893905
211	135	13970541540044076203689881160681573189545
212	135	189845688987658951531941795092501898072727005
213	135	162938425981534060763635083977029188109663335

Continued on Next Page...

Table 6 – Continued

$a$	$k$	$n$
214	136	174099019721489953731830847172515
215	136	180860146700965291740833986868535
216	136	1402785327460827475301586246268116645
217	136	150435075293326270700319858236445
218	136	133532257844637925677812008996395
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	13228742874201027909688648532680781692755
229	136	1152783981972759212376551073665878035
230	136	12690998857538106169053450769987651287315
231	136	11992411764462614086353260819346129198105
232	136	12458136493179608808153387453107143924245
233	136	13444919581748290693947715172165135522205
234	136	12704832265321779279601969382871641823735
235	136	139867498408927468089138080936033904837498615
236	136	156485419011968355386857456888830012342943995
237	136	2070458578947353310123511012096109893309491997845
238	137	13417252766180944472850677946397154449365
239	137	1200321465765450313917852148868594655
240	137	14513086842570059745580750331970177973605
241	137	13156723586255100890853577403748666013455
242	137	12458136493179608808153387453107143924245
243	137	13228742874201027909688648532680781692755
244	137	11992411764462614086353260819346129198105
245	137	145000250644117466918097276566714048134287555
246	137	139867498408927468089138080936033904837498615
247	137	2007238469666518094547220599513022568322942623865
248	137	2433554604816929017282913470206053910267638402385