Algorithms for Calculating Cyclotomic Polynomials

Andrew Arnold (ada26@sfu.ca), **Michael Monagan** (mmonagan@cecm.sfu.ca)
Centre for Experimental and Constructive Mathematics (CECM), Simon Fraser University

What are cyclotomic polynomials?

Definition 1. *The n_{th} **cyclotomic polynomial**, $\Phi_n(z)$, is the monic polynomial in $\mathbb{Z}[z]$ whose roots are the $\phi(n)$ primitive roots of unity.*

$$\Phi_n(z) = \prod_{\substack{d=0 \\ \gcd(d,n)=1}}^{n-1} (1 - z^d)$$

Here are some basic properties of cyclotomic polynomials:

Lemma 1. *If $n > 1$, then the coefficients of $\Phi_n(z)$ are **palindromic**. That is, for $\Phi_n(z) = \sum_{k=0}^{\phi(n)} a_k z^k$, it holds that $a_j = a_{\phi(n)-j}$.*
Lemma 2. *If n is odd, then $\Phi_{2n}(z) = \Phi_n(-z)$.*
Lemma 3. *If p is a prime that divides n, then $\Phi_{np}(z) = \Phi_n(z^p)$.*

Here are the first nine cyclotomic polynomials:

$\Phi_1(z) = z - 1$ $\quad\Phi_2(z) = z + 1$ $\quad\Phi_3(z) = z^2 + z + 1$
$\Phi_4(z) = z^2 + 1$ $\quad\Phi_5(z) = z^4 + z^3 + z^2 + z + 1$ $\quad\Phi_6(z) = z^4 + z^2 + 1$
$\Phi_7(z) = z^6 + z^5 + z^4 + z^3 + z^2 + z + 1$ $\quad\Phi_8(z) = z^4 + 1$ $\quad\Phi_9(z) = z^6 + z^3 + 1$

Observe that the coefficients are all 1 or -1. This holds for the first 104 cyclotomic polynomials; however,

$$\Phi_{105}(z) = 1 + z + z^2 + z^4 - z^5 - z^6 - \mathbf{2}z^7 - z^8 - z^9 + z^{12} + z^{13} + z^{14} + z^{15} + z^{16} + z^{17} - z^{20} - z^{22} - z^{24} - z^{26} - z^{28} + z^{31} + z^{32} + z^{33} + z^{34} + z^{35} + z^{36} - z^{39} - z^{40} - \mathbf{2}z^{41} - z^{42} - z^{43} + z^{46} + z^{47} + z^{48}.$$

We say that $\Phi_{105}(z)$ has height 2.

Definition 2. *The **height** of $\Phi_n(z)$, $A(n)$, is the maximum of the absolute values of the coefficients of $\Phi(n)$. That is, for $\Phi_n(z) = \sum_{k=0}^{\phi(n)} a_k z^k$, $A(n) = \max_{1 \le k \le \phi(n)} |a_k|$.*

For cyclotomic polynomials $\Phi_n(z)$ that can be easily computed with most computer algebra systems, $A(n)$ is typically small. In fact, for $n < 10^6$, $A(n) \le 60000$. One might guess that $A(n)$ is bounded by n. Erdős, however, proved the following:

Theorem 1. ***(Erdős)*** *[3] For all $c > 0$, there exists n such that $A(n) > n^c$.*

We aim is to answer the question: **What is the smallest n such that $A(n)$ is greater than n? n^2? n^3? . . . .** As far as we know, no one has previously calculated $\Phi_n(z)$ with $n > A(n)$. Here is what we have computed to date:

c	min(n) for which $A(n) > n^c$	$A(n)$
1	1181895	14102773
2	43730115	31484567640915734941
3	416690995	80103182105128365570406901971
4	1880394945	64540997036010911566826446181523888971563

Table 1: Smallest n such that $A(n) > n^c$, for $1 \le c \le 4$.

To compute these results, we needed to develop faster algorithms to calculate $\Phi_n(z)$. We present two such algorithms in this poster.

By lemmas 2 and 3, we know that if we introduce repeated factors or powers of 2 into n, that it will not result in a cyclotomic polynomial $\Phi_n(z)$ of greater height; therefore, our algorithms are designed with squarefree, odd n in mind.

The sparse power series algorithm

The following identity is well-known:

Lemma 4. *[2] For $n > 1$, $\Phi_n(z) = \prod_{d|n}(1 - z^d)^{\mu(\frac{n}{d})} = \left(\prod_{\mu(\frac{n}{d})=1}(1 - z^d)\right) \div \left(\prod_{\mu(\frac{n}{d})=-1}(1 - z^d)\right)$,*
where μ is the mobius function. ($\mu(n) = 1$ for squarefree n with an even number of prime factors; $\mu(n) = -1$ for squarefree n with an odd number of prime factors; $\mu(n) = 0$ for n not squarefree.)

For instance,

$$\Phi_{3\cdot5\cdot7}(z) = \frac{(1 - z^{105})(1 - z^3)(1 - z^5)(1 - z^7)}{(1 - z^{35})(1 - z^{21})(1 - z^{15})(1 - z)}$$

Given a power series $f(z) = \sum_{k=0}^{\infty} a_k z^k, f \in \mathbb{Z}[[z]]$, we can retrieve the first m terms of the both the product $f(z) \cdot (1 - z^d)$ and quotient $\frac{f(z)}{1-z^d}$ in $\mathcal{O}(m)$ operations in $\mathbb{Z}$. This is seen in the algorithm described hereafter:

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 $\Phi_n(z)$
$M \leftarrow \frac{\phi(n)}{2} + 1$, $a(0) \leftarrow 1$, **for** $1 \le i \le M$ **do** $a(i) \longleftarrow 0$
for $d|n, d > 0$ **do**
  if $\frac{n}{d}$ *has an even number of prime factors* **then**
    for $k = 0$ **to** $M - d$ **do** $a_{M-k} \leftarrow a_{M-k} - a_{(M-k)-d}$ (divide by $1 - z^d$)
  else
    for $k = d$ **to** M **do** $a_k \leftarrow a_k + a_{k-d}$ (multiply by $1 - z^d$)

Algorithm 1: Computing $\Phi_n(z)$ as a quotient of sparse power series

We only need to calculate half the terms of $\Phi_n(z)$, as the coefficients are palindromic by lemma 1. The algorithm takes $\mathcal{O}(2^k n)$ arithmetic operations in $\mathbb{Z}$.

The "big prime" algorithm

Calculating cyclotomic polynomials of very large degree using algorithm 1 can bode problematic, as oftentimes $\Phi_n(z)$ will not fit in main memory. In such a case, there are a variety of approaches to calculate $\Phi_n(z)$.

One approach is to calculate $\Phi_n(z)$ modulo primes p_i sufficiently small that we can fit $\Phi_n(z)$ in memory and write the images to hard disk. We then use Chinese remaindering to reconstruct the coefficients of $\Phi_n(z)$ sequentially from the images of $\Phi_n(z) \mod p_i$. This minimizes the amount of computation we have to do on the hard disk.

For yet larger cyclotomic polynomials, we may not even be able to store the coefficients modulo a prime in memory. In which case we may be forced to write $\Phi_n(z)$ and our intermediate work to disk. This proves most costly, as the hard disk bottlenecks the algorithm. In such instances, we need a low-memory algorithm to calculate $\Phi_n(z)$. Our low-memory approach requires the following definition and lemma:

Definition 3. *For notational convenience, we define $\Psi_n(z) = \frac{1 - z^n}{\Phi_n(z)}$.*

Lemma 5. *Let p be a prime such that $p \nmid m$, then $\Phi_{mp}(z) = \frac{\Phi_m(z^p)}{\Phi_m(z)} = \Phi_m(z^p) \cdot \left(\Psi_m(z) \cdot \frac{1}{1 - z^m}\right)$.*

Given $n = mp$, our approach to compute $\Phi_n(z)$ is roughly as follows: We first calculate $\Phi_m(z)$ and $\Psi_m(z)$. We can very easily calculate $\Psi_m(z)$ in a manner similar to algorithm 1. We then multiply $\Phi_m(z^p)$ by the power series of $\frac{\Psi_m(z)}{1-z^m}$ in a "forgetful" manner.

If we write

$$\Phi_m(z) = b_0 + b_1 z + \ldots + b_{\phi(m)} z^{\phi(m)}, \quad \text{and} \quad \Psi_m(z) = c_0 + c_1 z + \ldots + c_{m-\phi(m)} z^{m-\phi(m)},$$

then it follows from lemma 5 that

$$\Phi_n(z) = \left(\sum_{l=ip+j} b_i c_j \cdot z^l\right)\left(1 + z^m + z^{2m} + z^{3m} + \ldots\right) = \sum_{l \equiv ip+j \mod m} b_i c_j \cdot z^l.$$

Thus, if we write $\Phi_n(z) = a_0 + a_1 z + \ldots + a_{\phi(n)} z^{\phi(n)}$, we get the recurrence:

$$a_l = a_{l-m} + \sum_{l=ip+j} b_i c_j.$$

Using this recursion we compute the coefficients of $\Phi_n(z)$ sequentially, while storing only m coefficients.

Input: $n = p_1 p_2 \cdots p_k$, a product of k distinct primes.
$\bar{a}_0, \bar{a}_1, \ldots, \bar{a}_m$, an array
Output: A, the height of $\Phi_n(z)$
$m \leftarrow p_1 p_2 \ldots p_{k-1}$, $A \leftarrow 0$
$b_0, b_1, \ldots, b_{\phi(m)} \leftarrow$ the coefficients of $\Phi_m(z)$, $c_0, c_1, \ldots, c_{m-\phi(m)} \leftarrow$ the coefficients of $\left(\frac{z^m - 1}{\Phi_m(z)}\right)$
$\bar{a}_0, \bar{a}_1 \ldots, \bar{a}_{m-1} \leftarrow 0, 0, \ldots, 0$
$i \leftarrow 0, l \leftarrow 0$
while $i \le \frac{\phi(n)}{2}$ **do**
  for $j = 0$ **to** $m - \phi(m)$ **do**
    $\bar{a}_{(i+j \mod m)} \leftarrow \bar{a}_{(i+j \mod m)} + b_l \cdot c_j$, **if** $j < p_k$ *and* $|\bar{a}_{(i+j \mod m)}| > A$ **then** $A \leftarrow |\bar{a}_{(i+j \mod m)}|$
  $l \leftarrow l + 1$, $i \leftarrow i + p_k$
return A

Algorithm 2: A low-memory algorithm to obtain the height of $\Phi_n(z)$

We temporarily store the i_{th} coefficient of $\Phi_n(z)$, a_i, in the $(i \mod m)_{th}$ location in our array, $\bar{a}_{i \mod m}$. Algorithm 2 takes $\mathcal{O}\left(\left(\frac{n}{p_k}\right)^2\right)$ arithmetic operations in $\mathbb{Z}$. The space complexity is $\mathcal{O}\left(\frac{n}{p_k}\right)$. Clearly, the algorithm works best for n with a large prime divisor p_k. As such, we call it the "big prime" algorithm.

Computational Results

Cyclotomic Polynomials of Large Height

We have computed a library of data on the heights and lengths of cyclotomic polynomials. This data is available at `http://www.cecm.sfu.ca/~ada26/cyclotomic/`. Table 2, below, shows $\Phi_n(z)$ of increasing height:

n	$A(n)$	n	$A(n)$	n	$A(n)$
1	1	20615	27	1181895	14102773
105	2	26565	59	1752465	14703509
385	3	40755	359	3949491	56938657
1365	4	106743	397	8070699	74989473
1785	5	171717	434	10163195	1376877780831
2805	6	255255	532	13441645	1475674234751
3135	7	279565	1182	15069565	1666495909761
6545	9	327845	31010	30489585	2201904353336
10465	14	707455	35111	37495115	2286541988726
11305	23	886445	44125	40324935	2699208408726
17255	25	983535	59815	43730115	862550638890874931

n	factorization of n	$A(n)$
169828113	(3)(7)(13)(17)(23)(37)(43)	31484567640915734941
185626077	(3)(7)(13)(17)(23)(37)(47)	42337944402802720258
416690995	(5)(7)(17)(19)(29)(31)(41)	80103182105128365570406901971
437017385	(5)(7)(17)(19)(29)(31)(43)	86711753206816303264095919005
712407185	(5)(7)(17)(19)(29)(41)(53)	111859370951526698803198257925
1250072985	(3)(5)(7)(17)(19)(29)(31)(41)	137565800042644454188531306886
1311052155	(3)(5)(7)(17)(19)(29)(31)(43)	192892314415997583551731009410
1880394945	(3)(5)(11)(13)(19)(29)(37)(43)	64540997036010911566826446181523888971563
2317696095	(3)(5)(11)(13)(19)(29)(37)(53)	67075962666923019823602030663153118803367

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

We are currently computing $\Phi_n(z)$, for $n = 99660932085 = 3 \cdot 5 \cdot 11 \cdot 13 \cdot 19 \cdot 29 \cdot 37 \cdot 43 \cdot 53$, to 192-bit precision using algorithm 1. We expect it to have a greater height than that of any previously computed cyclotomic polynomial.

Flat cyclotomic polynomials

Definition 4. *A polynomial is **flat** if it has height one.*
Definition 5. *The **order** of a cyclotomic polynomial $\Phi_n(z)$ is the number of distinct odd prime factors that divide n.*

A question we are currently researching is: **Are there flat cyclotomic polynomials of order five?** It holds that $A(p) = 1$ for all primes p and $A(pq) = 1$ for all primes p,q. There are also infinitely many flat cyclotomic polynomials of order three [1][4], and we have computed flat cyclotomic polynomials of order four ($\Phi_{3\cdot5\cdot29\cdot1741}(z)$, is the first such example). To our knowledge, however, no one has yet found a flat cyclotomic polynomial of order five. We are using a two-pronged search: calculation of select examples of $\Phi_n(z)$ of order five, for which we expect $A(n)$ to be small (typically for very large n), and an exhaustive computation of cyclotomic polynomials $\Phi_n(z)$ of order five, for small n. To date, we have calculated every cyclotomic polynomial $\Phi_n(z)$ of order five for squarefree, odd $n < 2 \cdot 10^8$. Here are the cyclotomic polynomials of smallest height that we have computed:

n	factorization of n	$A(n)$	n	factorization of n	$A(n)$
48713385	(3)(5)(7)(47)(9871)	5	146130285	(3)(5)(7)(47)(29611)	5
61944015	(3)(5)(7)(53)(11131)	5	151911165	(3)(5)(7)(83)(17431)	5
76762245	(3)(5)(7)(59)(12391)	4	153518295	(3)(5)(7)(59)(24781)	4
82041645	(3)(5)(7)(61)(12809)	5	164102505	(3)(5)(7)(61)(25621)	5
97411965	(3)(5)(7)(47)(19739)	5	185820915	(3)(5)(7)(53)(33391)	5
117496785	(3)(5)(7)(73)(15329)	5	746443728915	(3)(5)(31)(929)(1727939)	3
117512115	(3)(5)(7)(73)(15331)	5	1147113361785	(3)(5)(29)(1741)(1514671)	2
123871335	(3)(5)(7)(53)(22259)	5	2576062979535	(3)(5)(29)(2609)(2269829)	2

Table 3: Computed cyclotomic polynomials of order five with height ≤ 5.

Future work

Another unanswered problem we would like to investigate is:

Is $A(np) \ge A(n)$ for every integer $n > 0$ and for every prime p?

References

[1] Gennady Bachman. Flat cyclotomic polynomials of order three. *Bulletin of the London Mathematical Society*, 38(01):53–60, 2006.

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

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

[4] Nathan Kaplan. Flat cyclotomic polynomials of order three. *J. Number Theory*, 127(1):118–126, 2007.