The Height of the 3,234,846,615th Cyclotomic Polynomial is Big (2,888,582,082,500,892,851)

Andrew Arnold, Michael Monagan
ada26@sfu.ca, mmonagan@cecm.sfu.ca

Cyclotomic Polynomials

Definition 1. *The n_{th} **cyclotomic polynomial**, $\Phi_n(z)$ is defined as follows:*

$$\Phi_n(z) = \prod_{\substack{k=0 \\ gcd(k,n)=1}}^{n-1} (z - e^{2\pi i \frac{k}{n}}).$$

It is the monic polynomial whose distinct $\phi(n)$ zeros are the n_{th} complex primitive roots of unity. Its coefficients are all integer-valued. For $n > 1$, the coefficients of $\Phi_n(z)$ are palindromic about $\phi(n)$. That is, the coefficients read the same backwards as they do forwards. Here are the first ten cyclotomic polynomials:

$\Phi_1(z) = z - 1$
$\Phi_2(z) = z + 1$
$\Phi_3(z) = z^2 + z + 1$
$\Phi_4(z) = z^2 + 1$
$\Phi_5(z) = z^4 + z^3 + z^2 + z + 1$
$\Phi_6(z) = z^2 - z + 1$
$\Phi_7(z) = z^6 + z^5 + z^4 + z^3 + z^2 + z + 1$
$\Phi_8(z) = z^4 + 1$
$\Phi_9(z) = z^6 + z^3 + 1$
$\Phi_{10}(z) = z^4 - z^3 + z^2 - z + 1$

Observe that the coefficients are all -1, 0, or 1. This is true for orders up to $n = 104$. For $n = 105$, however, we have:

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

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

It is known that $A(n)$ can get arbitrarily large. In fact, Paul Erdos proved the following result:

Theorem 1. *For any constant $c > 0$ there exists n such that $A(n) > n^c$.*

The question is, how large does n have to be before $A(n) > n$? Can we find n such that $A(n) > n^2$? In this poster we describe two algorithms for computing $\Phi_n(z)$ and we list some results of our search for large $A(n)$ including the first n such that $A(n) > n$ and one n for which $A(n) > n^2$.

fasg

Constructing $\Phi_n(z)$

Here are some properties of cyclotomic polynomials that are useful in their computation.

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

Lemma 2. *Let p be a prime. Then $\Phi_p(z) = \sum_{k=0}^{p-1} z^p = \frac{z^p-1}{z-1}$*

Lemma 3. *Let $n \in \mathbb{N}$ and p be a prime. Then $\Phi_{np^2}(z) = \Phi_{np}(z^p)$*

Lemma 4. *Let $n \in \mathbb{N}$ and p be a prime that does not divide n. Then $\Phi_{np}(z) = \frac{\Phi_n(z^p)}{\Phi_n(z)}$*

The reader should check these lemmas against the examples above.

Lemma 3 provides an easy means of generating $\Phi_n(z)$ for arbitrary n, assuming we already have the cyclotomic polynomials of square-free order. We present the following two algorithms to generate $\Phi_n(z)$ for odd, square-free integers n:

Algorithm 1. Let $n = p_1 p_2 ... p_j$, for distinct odd primes $p_1, p_2, ..., p_j$, where $p_1 < p_2 < ... < p_j$.
Let $n_k = \prod_{h=1}^{k} p_h$. Then n_j is then simply n.
We know from lemma 2 that $\Phi_{p_1}(z) = \sum_{h=0}^{p_1-1} z^h$. We can then solve for $\Phi_n(z)$ recursively using lemma 4. This algorithm does a sequence of polynomial divisions.
For k from 2 to j: $\Phi_{n_k}(z) = \frac{\Phi_{n_{k-1}}(z^p)}{\Phi_{n_{k-1}}(z)}$
Number of operations: $O(\frac{n^2}{p_j})$

Algorithm 2. (Bloom)
We'll illustrate this algorithm with an example. Consider primes p, q, r with $p < q < r$
By lemma 4, $\Phi_{pqr}(z) = \frac{\Phi_{pq}(z^r)}{\Phi_{pq}(z)}$.
We can apply lemma 4 repeatedly:

$$\Phi_{pqr}(z) = \frac{\left[\frac{\Phi_p((z^r)^q)}{\Phi_p(z^r)}\right]}{\left[\frac{\Phi_p(z^q)}{\Phi_p(z)}\right]} = \frac{\Phi_p(z^{qr}) \cdot \Phi_p(z)}{\Phi_p(z^q) \cdot \Phi_p(z^r)} = \frac{\left[\left(\frac{\Phi_1((z^{qr})^p)}{\Phi_1(z^{qr})}\right)\left(\frac{\Phi_1(z^p)}{\Phi_1(z)}\right)\right]}{\left[\left(\frac{\Phi_1((z^q)^p)}{\Phi_1(z^q)}\right)\left(\frac{\Phi_1((z^r)^p)}{\Phi_1(z^r)}\right)\right]}$$

$$= \frac{\Phi_1(z^{pqr}) \cdot \Phi_1(z^p) \cdot \Phi_1(z^q) \cdot \Phi_1(z^r)}{\Phi_1(z^{pq}) \cdot \Phi_1(z^{pr}) \cdot \Phi_1(z^{qp}) \cdot \Phi_1(z)}$$

$$= \frac{(z^{pqr} - 1) \cdot (z^p - 1) \cdot (z^q - 1) \cdot (z^r - 1)}{(z^{pq} - 1) \cdot (z^{pr} - 1) \cdot (z^{qr} - 1) \cdot (z - 1)}$$

In general, we can express $\Phi_n(z)$ for arbitrary $n = p_1 p_2 ... p_j$ in this fashion.

$$\Phi_n(z) = \prod_{m, \frac{m}{n} \in \mathbb{N}} (z^m - 1)^{\mu(\frac{m}{n})} = \left(\prod_{\mu(\frac{m}{n})=1} (z^m - 1) \right) \div \left(\prod_{\mu(\frac{m}{n})=-1} (z^m - 1) \right)$$

where $\mu(k)$ is the **Moebius function** ($\mu : \mathbb{N} \rightarrow \{-1, 0, 1\}$. $\mu(1) = 0$ and $\mu(k) = 0$ if k isn't square-free, otherwise $\mu(k) = 1$ if k has an even number of prime factors, and $\mu(k) = -1$ if k has an odd number of prime factors).

We can then solve for $\Phi_n(z)$ as a power series evaluated up to degree $\frac{\phi(n)}{2}$, half the degree $\Phi_n(z)$. Using the reciprocity of cyclotomic polynomial coefficients, we effectively know all the coefficients for a cycltomic polynomial if we've determined the first half. We multiply the terms in the numerator and then divide by the terms in the denominator, all individually, so as to preserve the sparseness of each of the terms. A product of j distinct primes $p_1, p_2, ..., p_j$ has 2^j positive divisors. In total, both the numerator and denominator in the equation above have 2^{j-1} terms of the form $z^m - 1$.
Number of operations: $O(2^j n)$

Theoretical Bounds on the Height of $\Phi_n(z)$

Theorem 2. *(A.S.Bang, 1895) Let p, q, r be odd primes satisfying $p < q < r$. Then $A(n) \le p - 1$.*

Theorem 3. *(Bloom, 1968) Let p, q, r, s be odd primes such that $p < q < r < s$.
Then $A(pqrs) \le p(pq - 1)(q - 1)$.*

Theorem 4. *(P.T. Bateman, 1982) Let $n = p_1 p_2 ... p_j$, for primes $p_k, 1 \le k \le j$, such that $2 < p_1 < p_2 < ... < p_j$. Then,*

$$A(n) \le \prod_{k=1}^{j-2} (p_k^{2^{j-k-1}-1})$$

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

Computed Heights of Cyclotomic Polynomials

Using algorithm 1, we were able to compute the heights of cyclotomic polynomials. Here are some results we computed:

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

We have verified that $\Phi_{1,181,895}(z)$ is the first cyclotomic polynomial whose height exceeds its order. $\Phi_{43,730,115}(z)$ is the first cyclotomic polynomial we've discovered to have a height greater than its order squared; however, we have yet to verify whether the same holds for any cyclotomic polynomials of smaller order. Below are the heights of cyclotomic polynomials whose orders are products of the first k odd prime numbers.

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**

$*(Koshiba, 2002). **(Monagan, 2007).$

To compute large cyclotomic polynomials, we implemented algorithm 1 using the **fast Fourier transform** (FFT). To compute $\Phi_n(z) = \frac{\Phi_{n/p}(z^p)}{\Phi_{n/p}(z)}$, we first find the smallest power of two, N, such that $N > \phi(n/p) \cdot p$, the degree of the numerator. We then find a prime, q, of the form $aN + 1$, and ω, an N_{th} root of unity modulo q. Given these parameters, we use the FFT to find $\Phi_{n/p}((\omega^k)^p)$ mod q and $\Phi_{n/p}(\omega^k)$ mod q, for $0 \le k \le N$ in ***O(nlg(n))* operations**. We then compute for $\Phi_n(\omega^k) = \Phi_{n/p}((\omega^k)^p) \div \Phi_{n/p}(\omega^k)$ mod q, for $0 \le k \le n$. We then apply the inverse FFT to interpolate $\Phi_n(z)$ mod q.

Often the theoretical bound for $A(n)$ exceeds our choice of prime q. In such case we solve $\Phi_n(z)$ mod q for two primes, q_1 and q_2. We then solve for $\Phi_n(z)$ with the **Chinese remainder Theorem**. After we have obtained a result by Chinese remaindering (call it $H_n(z)$), we can check that $H_n(z)$ is infact the correct solution by solving $H_n(z)\Phi_{\frac{n}{p}}(z) - \Phi_{\frac{n}{p}}(z^p)$ mod a third prime, q_3, where $\Phi_{\frac{n}{p}}(z)$ is the polynomial that resulted from the second last division step of the algorithm. We know $\Phi_n(z)\Phi_{\frac{n}{p}}(z) - \Phi_{\frac{n}{p}}(z^p) = 0$, so if we obtain that $H_n(z)\Phi_{\frac{n}{p}}(z) - \Phi_{\frac{n}{p}}(z^p) = 0$ mod q_3, then we can assume with confidence that $H_n(z)$ is infact $\Phi_n(z)$.

For polynomials of degree less than 2^{27}, we used primes $q_1 = 15 \cdot 2^{27}$ and $q_2 = 17 \cdot 2^{27}$. For degree greater than 2^{27}, we used $q_1 = 10 \cdot 2^{38}$ and $q_2 = 15 \cdot 2^{38}$. To use the FFT for a prime q greater than 32 bits, we needed to encode multiplication over $\mathbb{Z}_q$ so as to avoid integer overflow while running on a 64-bit computer. By breaking integers into their upper and lower bits, we were able to perform arithmetic in $\mathbb{Z}_q$ for primes q as large as 42 bits. Our 42-bit multiplication requires two division operations.

$\Phi_{3,234,846,615}(z)$ was particularly difficult to compute. It took 12 hours to solve, requiring 40 gigabytes of memory! As far as we know, its height is the **greatest height ever computed** for a cyclotomic polynomial.