Calculating Really Big Cyclotomic Polynomials

Andrew Arnold, Michael Monagan

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

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

The first ten cyclotomic polynomials are as follows:

$\Phi_1(z) = z - 1$ $\qquad$ $\Phi_6(z) = z^2 - z + 1$

$\Phi_2(z) = z + 1$ $\qquad$ $\Phi_7(z) = z^6 + z^5 + z^4 + z^3 + z^2 + z + 1$

$\Phi_3(z) = z^2 + z + 1$ $\qquad$ $\Phi_8(z) = z^4 + 1$

$\Phi_4(z) = z^2 + 1$ $\qquad$ $\Phi_9(z) = z^6 + z^3 + 1$

$\Phi_5(z) = z^4 + z^3 + z^2 + z + 1$ $\qquad$ $\Phi_{10}(z) = z^4 - z^3 + z^2 - z + 1$

Observe that all the coefficients in the polynomials above are either -1, 0, or 1. In fact, the first cyclotomic polynomial with a coefficient that is not -1, 0, or 1 is $\Phi_{105}(z)$. If we write $\Phi_n(z) = \sum_{j=1}^{\phi(x)} a_n(m) z^m$, then we let $A_n = \max_{1 \le m \le \phi(n)} |a_n(m)|$ and $S_n = \sum_{m=1}^{\phi(n)} |a_n(m)|$ be the height and length of $\Phi_n(z)$, respectively. The aim of our research is to study A_n and S_n. In particular, we are looking for cyclotomic polynomials with large heights.

We present two algorithms to calculate cyclotomic polynomials. Our first algorithm uses that for primes $p \nmid n$, $\Phi_{np}(z) = \Phi_n(z^p) \div \Phi_n(z)$. We perform fast polynomial division via the discrete fast Fourier transform.

For our second algorithm, we use the identity:

$$\Phi_n(z) = \prod_{\substack{1 \le k \le n \\ k | n}} (z^k - 1)^{\mu(\frac{k}{n})}$$

We construct $\Phi_n(z)$ as a quotient of sparse power series. This method allows us to calculate cyclotomic polynomials in an integer array completely in memory, thereby minimizing memory requirements.

Using the latter approach we are able to quickly calculate cyclotomic polynomials of order upwards of one billion. Amongst our findings we have found the cyclotomic polynomial of smallest order whose height exceeds its order; the first cyclotomic polynomial whose height exceeds its order squared; the first whose height exceeds machine precision (2^{64}); a cyclotomic polynomial whose height exceeds its order raised to the fourth power; and all cyclotomic polynomials of squarefree order with six or more distinct factors up to order $6 \cdot 10^8$, and all with squarefree order with seven or more distinct factors up to 10^9.