Computing Cyclotomic Polynomials of Large and Small Height

Michael Monagan

Centre for Experimental and Constructive Mathematics

Simon Fraser University

Joint work with Andrew Arnold

Cyclotomic Polynomials

The k'th cyclotomic polynomial $\Phi_k(x)$ is the polynomial whose roots are the primitive k'th complex roots of unity.

Example:

$$\Phi_4(x) = (x - i)(x + i) = x^2 + 1.$$

Cyclotomic Polynomials

The k'th cyclotomic polynomial $\Phi_k(x)$ is the polynomial whose roots are the primitive k'th complex roots of unity.

Example:

$$\Phi_4(x) = (x - i)(x + i) = x^2 + 1.$$

Definition: Let H_k be the height of $\Phi_k(x)$.

Example: $H_4 = 1$.

Some Cyclotomic Polynomials

k	$\Phi_k(x)$
3	$x^2 + x + 1$
4	$x^2 + 1$
5	$x^4 + x^3 + x^2 + x + 1$
6	$x^2 - x + 1$
7	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
8	$x^4 + 1$
9	$x^6 + x^3 + 1$
10	$x^4 - x^3 + x^2 - x + 1$

cyclotomic polynomials of order 3–10

Bigger Cyclotomic Polynomials

$$\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - \mathbf{2}x^{41} - x^{40} - x^{39} + x^{36}$$

$$+ \ldots + x^{14} + x^{13} + x^{12} - x^{9} - x^{8} - \mathbf{2}x^{7} - x^{6} - x^{5} + x^{2} + x + 1.$$

Bigger Cyclotomic Polynomials

$$\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - \mathbf{2}x^{41} - x^{40} - x^{39} + x^{36}$$

$$+ \ldots + x^{14} + x^{13} + x^{12} - x^{9} - x^{8} - \mathbf{2}x^{7} - x^{6} - x^{5} + x^{2} + x + 1.$$

$$\Phi_{385}(x) = x^{240} + x^{239} + x^{238} + x^{237} + x^{236} - x^{233} - x^{232} - x^{231} - x^{230} - 2\,x^{229} - \ldots$$

$$-2\,x^{122} - 3\,x^{121} - \mathbf{3}\,x^{120} - \mathbf{3}\,x^{119} - 2\,x^{118} - 2\,x^{117} - x^{116} + x^{114}$$

$$+ \ldots - x^{12} - 2\,x^{11} - x^{10} - x^{9} - x^{8} - x^{7} + x^{4} + x^{3} + x^{2} + x + 1$$

Largest Heights up to 10^6

k	H_k	k	H_k
105	2	26565	59
385	3	40755	359
1365	4	106743	397
1785	5	171717	434
2805	6	255255	532
3135	7	279565	585
6545	9	285285	1182
10465	14	327845	31010
11305	23	707455	35111
17255	25	886445	44125
20615	27	983535	59518

$$H_k = ||\Phi_k(x)||_\infty.$$

Larger heights.

Yoichi Koshiba (1998) For
$k = 4,849,845 = (3)(5)(7)(11)(13)(17)(19)$, $H_k = 669,606$.

Larger heights.

Yoichi Koshiba (1998) For
$k = 4,849,845 = (3)(5)(7)(11)(13)(17)(19)$, $H_k = 669,606$.

Paul Erdos
For any $c > 0$ there exists k such that $H_k > k^c$.
So what is the smallest k for which $H_k > k$??

Larger heights.

Yoichi Koshiba (1998) For
$k = 4,849,845 = (3)(5)(7)(11)(13)(17)(19)$, $H_k = 669,606$.

Paul Erdos
For any $c > 0$ there exists k such that $H_k > k^c$.
So what is the smallest k for which $H_k > k$??

c	min(k) s.t. $H_k > k^c$	H_k
1	1,181,895 = (3)(5)(11)(13)(19)(29)	14,102,773
2	43,730,115 = (3)(5)(11)(13)(19)(29)(37)	862,550,638,890,874,931
3	416,690,995 = (5)(7)(17)(19)(29)(31)(41)	80103182105128365570406901971
4	1,880,394,945 = 43730115×43	A
5?	99,660,932,095 = 188394945×53	???
	(need about 0.5 TB)	(?? 192 bits??)

A = 64540997036010911566826446181523888971563 (135.56 bits).

Flat Cyclotomic Polynomials

Definition: $\Phi_k(x)$ is flat if it has height $H_k = 1$.

Example: If p is prime then $\Phi_p(x)$ is flat.

$$\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + ... + x + 1$$

Flat Cyclotomic Polynomials

Definition: $\Phi_k(x)$ is flat if it has height $H_k = 1$.

Example: If p is prime then $\Phi_p(x)$ is flat.

$$\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + ... + x + 1$$

If $k = p_1 p_2$ then $\Phi_p(x)$ is flat.
For $k = (3)(7)(11)$, $\Phi_k(x)$ is flat.
For $k = (3)(5)(29)(1741)$, $\Phi_k(x)$ is flat.

Flat Cyclotomic Polynomials

Definition: $\Phi_k(x)$ is flat if it has height $H_k = 1$.

Example: If p is prime then $\Phi_p(x)$ is flat.

$$\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + ... + x + 1$$

If $k = p_1 p_2$ then $\Phi_p(x)$ is flat.
For $k = (3)(7)(11)$, $\Phi_k(x)$ is flat.
For $k = (3)(5)(29)(1741)$, $\Phi_k(x)$ is flat.

Are there any flat $\Phi_k(x)$ with k a product of five distinct odd primes?

Nathan Kaplan (2009): $k = 2,576,062,979,535$?

Almost Flat Cyclotomic Polynomials

k	H_k
48713385 = (3)(5)(7)(47)(9871)	5
76762245 = (3)(5)(7)(59)(12391)	4
746443728915 = (3)(5)(31)(929)(1727939)	3
1147113361785 = (3)(5)(29)(1741)(1514671)	2
2576062979535 = (3)(5)(29)(2609)(2269829)	2

Algorithms.

- Maple and Magma
- Using the FFT and CRT
- Sparse Power Series Algorithm
- The Big Prime Algorithm.

Computing $\Phi_k(x)$ in Maple and Magma

If p is prime then $\Phi_p(x) = x^{p-1} + x^{p-2} + ... + x + 1$.
If p is prime and $k = mp$ is square-free then

$$\Phi_k(x) = \frac{\Phi_m(x^p)}{\Phi_m(x)}.$$

Example:

$$\Phi_{15} = \frac{\Phi_3(x^5)}{\Phi_3(x)} = \frac{x^{10} + x^5 + 1}{x^2 + x + 1} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.$$

Cost using clasical $\div$ is $O(k^2/p)$ integer operations.

Using the discrete FFT

Do the division in

$$\Phi_k(x) = \frac{\Phi_m(x^p)}{\Phi_m(x)} \qquad\qquad (k = mp)$$

using the FFT modulo primes $q_1, q_2, \ldots$ and apply the CRT.
Cost: $O(k \log k)$ per prime.

Using the discrete FFT

Do the division in

$$\Phi_k(x) = \frac{\Phi_m(x^p)}{\Phi_m(x)} \qquad\qquad (k = mp)$$

using the FFT modulo primes $q_1, q_2, \ldots$ and apply the CRT.
Cost: $O(k \log k)$ per prime.

Let $d = \deg(\Phi_m(x^p))$.
Need primes of the form $q = 2^n r + 1$ with $2^n > d$.

For large k we used $q_1 = 10 \cdot 2^{38} + 1$ and $q_2 = 15 \cdot 2^{38} + 1.$
Coded 42 bit arithmetic in $\mathbb{Z}_q$ using 64 bit arithmetic.

Sparse Power Series Method

Let p_1, p_2, p_3 be distinct primes.

$$\Phi_{p_1 p_2 p_3}(x) = \frac{(1 - x^{p_1 p_2 p_3})(1 - x^{p_1})(1 - x^{p_2})(1 - x^{p_3})}{(1 - x^{p_1 p_2})(1 - x^{p_1 p_3})(1 - x^{p_2 p_3})(1 - x^1)}$$

Example

$$\Phi_{15}(x) = \frac{(1 - x^{15})(1 - x)}{(1 - x^3)(1 - x^5)} = 1 - x + x^3 - x^4 + x^5 - x^7 + x^8.$$

As a series, the multiplications and divisions are sparse.

For k a product of n primes, the cost is $O(2^n k)$ integer additions and subtractions.

Timings

k	d	divide	modp1	dft10	adiv2
105	48	0.001s	0.001	0.001	
1155	480	0.002s	0.001	0.003	
15015	5760	1.530s	0.104	0.044	0.0
255255	92160	751.5s	20.105	0.890	0.010
4849845	1658880	-	5995.36	17.543	0.558
111546435	36495360	-	-	692.550	27.39

$$d = \deg \Phi_k(x) = \phi(k).$$

The Big Prime Algorithm

Define $\Psi_k(z) = \dfrac{1 - z^k}{\Phi_k(z)}$.

Lemma: Let $k = mp$ such that p is prime and $p \nmid m$. 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 $k = mp$, first calculate $\Phi_m(z)$ and $\Psi_m(z)$ (at the same time). Then multiply $\Phi_m(z^p)$ by the power series of $\frac{\Psi_m(z)}{1-z^m}$ in a “forgetful” manner, in $O(m)$ space and $O(m^2)$ time.

For $p \in O(\sqrt{k})$, we have $O(\sqrt{k})$ space and $O(k)$ time.

Thank You.