Computing Cyclotomic Polynomials of Large and Small Height

Michael Monagan

Centre for Experimental and Constructive Mathematics
Simon Fraser University

Joint work with Andrew Arnold
The \( k \)'th cyclotomic polynomial \( \Phi_k(x) \) is the polynomial whose roots are the primitive \( k \)'th complex roots of unity. Example:

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

<table>
<thead>
<tr>
<th>$k$</th>
<th>$\Phi_k(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$x^2 + x + 1$</td>
</tr>
<tr>
<td>4</td>
<td>$x^2 + 1$</td>
</tr>
<tr>
<td>5</td>
<td>$x^4 + x^3 + x^2 + x + 1$</td>
</tr>
<tr>
<td>6</td>
<td>$x^2 - x + 1$</td>
</tr>
<tr>
<td>7</td>
<td>$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$</td>
</tr>
<tr>
<td>8</td>
<td>$x^4 + 1$</td>
</tr>
<tr>
<td>9</td>
<td>$x^6 + x^3 + 1$</td>
</tr>
<tr>
<td>10</td>
<td>$x^4 - x^3 + x^2 - x + 1$</td>
</tr>
</tbody>
</table>

cyclotomic polynomials of order 3–10
Bigger Cyclotomic Polynomials

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

\[ + \ldots + x^{14} + x^{13} + x^{12} - x^{9} - x^{8} - 2x^{7} - x^{6} - x^{5} + x^{2} + x + 1. \]
Bigger Cyclotomic Polynomials

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

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

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

\[ - 2x^{122} - 3x^{121} - 3x^{120} - 3x^{119} - 2x^{118} - 2x^{117} - x^{116} + x^{114} \]

\[ + \ldots - x^{12} - 2x^{11} - x^{10} - x^{9} - x^{8} - x^{7} + x^{4} + x^{3} + x^{2} + x + 1 \]
### Largest Heights up to $10^6$

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

\[ H_k = ||\Phi_k(x)||_\infty. \]
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
\[ k = 4, 849, 845 = (3)(5)(7)(11)(13)(17)(19), \quad H_k = 669, 606. \]

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 \( H_k > k^c \)?

<table>
<thead>
<tr>
<th>( c )</th>
<th>( \min(k) ) s.t. ( H_k &gt; k^c )</th>
<th>( H_k )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1,181,895 = (3)(5)(11)(13)(19)(29)</td>
<td>14,102,773</td>
</tr>
<tr>
<td>3</td>
<td>416,690,995 = (5)(7)(17)(19)(29)(31)(41)</td>
<td>80103182105128365570406901971</td>
</tr>
<tr>
<td>4</td>
<td>1,880,394,945 = 43730115 \times 43</td>
<td>A</td>
</tr>
<tr>
<td>5?</td>
<td>99,660,932,095 = 188394945 \times 53</td>
<td>???</td>
</tr>
<tr>
<td></td>
<td>(need about 0.5 TB)</td>
<td>(?? 192 bits??)</td>
</tr>
</tbody>
</table>

A = 6454099703601091156682646181523888971563 (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.

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

\[
\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1
\]

If \( k = p_1p_2 \) 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

<table>
<thead>
<tr>
<th>$k$</th>
<th>$H_k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>48713385 = (3)(5)(7)(47)(9871)</td>
<td>5</td>
</tr>
<tr>
<td>76762245 = (3)(5)(7)(59)(12391)</td>
<td>4</td>
</tr>
<tr>
<td>746443728915 = (3)(5)(31)(929)(1727939)</td>
<td>3</td>
</tr>
<tr>
<td>1147113361785 = (3)(5)(29)(1741)(1514671)</td>
<td>2</td>
</tr>
<tr>
<td>2576062979535 = (3)(5)(29)(2609)(2269829)</td>
<td>2</td>
</tr>
</tbody>
</table>
Algorithms.

- Maple and Magma
- Using the FFT and CRT
- Sparse Power Series Algorithm
- The Big Prime Algorithm.
If $p$ is prime then $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$.

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 classical $\div$ is $O(k^2/p)$ integer operations.
Using the discrete FFT

Do the division in

\[ \Phi_k(x) = \frac{\Phi_m(x^p)}{\Phi_m(x)} \quad (k = mp) \]

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

\[ \Phi_k(x) = \frac{\Phi_m(x^p)}{\Phi_m(x)} \quad (k = mp) \]

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.

\[
\Phi_{p_1p_2p_3}(x) = \frac{(1 - x^{p_1p_2p_3})(1 - x^{p_1})(1 - x^{p_2})(1 - x^{p_3})}{(1 - x^{p_1p_2})(1 - x^{p_1p_3})(1 - x^{p_2p_3})(1 - x^1)}
\]

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

<table>
<thead>
<tr>
<th>$k$</th>
<th>$d$</th>
<th>divide</th>
<th>modp1</th>
<th>dft10</th>
<th>adiv2</th>
</tr>
</thead>
<tbody>
<tr>
<td>105</td>
<td>48</td>
<td>0.001s</td>
<td>0.001</td>
<td>0.001</td>
<td></td>
</tr>
<tr>
<td>1155</td>
<td>480</td>
<td>0.002s</td>
<td>0.001</td>
<td>0.003</td>
<td></td>
</tr>
<tr>
<td>15015</td>
<td>5760</td>
<td>1.530s</td>
<td>0.104</td>
<td>0.044</td>
<td>0.0</td>
</tr>
<tr>
<td>255255</td>
<td>92160</td>
<td>751.5s</td>
<td>20.105</td>
<td>0.890</td>
<td>0.010</td>
</tr>
<tr>
<td>4849845</td>
<td>1658880</td>
<td>-</td>
<td>5995.36</td>
<td>17.543</td>
<td>0.558</td>
</tr>
<tr>
<td>111546435</td>
<td>36495360</td>
<td>-</td>
<td>-</td>
<td>692.550</td>
<td>27.39</td>
</tr>
</tbody>
</table>

\[ d = \deg \Phi_k(x) = \phi(k). \]
The Big Prime Algorithm

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

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.