

Flat Cyclotomic Polynomials

Sam Elder

Colorado Math Circle

Saturday, January 2, 2010

A Factoring Challenge

Can you factor the following ten polynomials completely?

A Factoring Challenge

Can you factor the following ten polynomials completely?

① $x - 1 = \dots$

② $x^2 - 1 = \dots$

③ $x^3 - 1 = \dots$

④ $x^4 - 1 = \dots$

⑤ $x^5 - 1 = \dots$

⑥ $x^6 - 1 = \dots$

⑦ $x^7 - 1 = \dots$

⑧ $x^8 - 1 = \dots$

⑨ $x^9 - 1 = \dots$

⑩ $x^{10} - 1 = \dots$

Only use polynomials with integer coefficients.

A Factoring Challenge

Can you factor the following ten polynomials completely?

① $x - 1 = (x - 1)$

A Factoring Challenge

Can you factor the following ten polynomials completely?

① $x - 1 = (x - 1)$

② $x^2 - 1 = (x - 1)(x + 1)$

A Factoring Challenge

Can you factor the following ten polynomials completely?

① $x - 1 = (x - 1)$

② $x^2 - 1 = (x - 1)(x + 1)$

③ $x^3 - 1 = (x - 1)(x^2 + x + 1)$

A Factoring Challenge

Can you factor the following ten polynomials completely?

① $x - 1 = (x - 1)$

② $x^2 - 1 = (x - 1)(x + 1)$

③ $x^3 - 1 = (x - 1)(x^2 + x + 1)$

④ $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$

A Factoring Challenge

Can you factor the following ten polynomials completely?

$$① \quad x - 1 = (x - 1)$$

$$② \quad x^2 - 1 = (x - 1)(x + 1)$$

$$③ \quad x^3 - 1 = (x - 1)(x^2 + x + 1)$$

$$④ \quad x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$$

$$⑤ \quad x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$

A Factoring Challenge

Can you factor the following ten polynomials completely?

$$① \quad x - 1 = (x - 1)$$

$$② \quad x^2 - 1 = (x - 1)(x + 1)$$

$$③ \quad x^3 - 1 = (x - 1)(x^2 + x + 1)$$

$$④ \quad x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$$

$$⑤ \quad x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$

$$⑥ \quad x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$$

A Factoring Challenge

Can you factor the following ten polynomials completely?

$$\textcircled{1} \quad x - 1 = (x - 1)$$

$$\textcircled{2} \quad x^2 - 1 = (x - 1)(x + 1)$$

$$\textcircled{3} \quad x^3 - 1 = (x - 1)(x^2 + x + 1)$$

$$\textcircled{4} \quad x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$$

$$\textcircled{5} \quad x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$

$$\textcircled{6} \quad x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$$

$$\textcircled{7} \quad x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

A Factoring Challenge

Can you factor the following ten polynomials completely?

$$① \quad x - 1 = (x - 1)$$

$$② \quad x^2 - 1 = (x - 1)(x + 1)$$

$$③ \quad x^3 - 1 = (x - 1)(x^2 + x + 1)$$

$$④ \quad x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$$

$$⑤ \quad x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$

$$⑥ \quad x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$$

$$⑦ \quad x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

$$⑧ \quad x^8 - 1 = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$$

A Factoring Challenge

Can you factor the following ten polynomials completely?

① $x - 1 = (x - 1)$

② $x^2 - 1 = (x - 1)(x + 1)$

③ $x^3 - 1 = (x - 1)(x^2 + x + 1)$

④ $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$

⑤ $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$

⑥ $x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$

⑦ $x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$

⑧ $x^8 - 1 = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$

⑨ $x^9 - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$

A Factoring Challenge

Can you factor the following ten polynomials completely?

1 $x - 1 = (x - 1)$

2 $x^2 - 1 = (x - 1)(x + 1)$

3 $x^3 - 1 = (x - 1)(x^2 + x + 1)$

4 $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$

5 $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$

6 $x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$

7 $x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$

8 $x^8 - 1 = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$

9 $x^9 - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$

10 $x^{10} - 1 = (x - 1)(x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1)$

A Factoring Challenge

Can you factor the following ten polynomials completely?

$$① \quad x - 1 = (x - 1)$$

$$② \quad x^2 - 1 = (x - 1)(x + 1)$$

$$③ \quad x^3 - 1 = (x - 1)(x^2 + x + 1)$$

$$④ \quad x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$$

$$⑤ \quad x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$

$$⑥ \quad x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$$

$$⑦ \quad x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

$$⑧ \quad x^8 - 1 = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$$

$$⑨ \quad x^9 - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$$

$$⑩ \quad x^{10} - 1 = (x - 1)(x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1)$$

Anyone notice any patterns?

Cyclotomic Polynomials

These factors are known as *cyclotomic polynomials*.

$$① \quad x - 1 = (x - 1)$$

$$② \quad x^2 - 1 = (x - 1)(x + 1)$$

$$③ \quad x^3 - 1 = (x - 1)(x^2 + x + 1)$$

$$④ \quad x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$$

$$⑤ \quad x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$

$$⑥ \quad x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$$

$$⑦ \quad x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

$$⑧ \quad x^8 - 1 = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$$

$$⑨ \quad x^9 - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$$

$$⑩ \quad x^{10} - 1 = (x - 1)(x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1)$$

Cyclotomic Polynomials

These factors are known as *cyclotomic polynomials*.

$$① \quad x - 1 = (x - 1)$$

$$② \quad x^2 - 1 = (x - 1)(x + 1)$$

$$③ \quad x^3 - 1 = (x - 1)(x^2 + x + 1)$$

$$④ \quad x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$$

$$⑤ \quad x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$

$$⑥ \quad x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$$

$$⑦ \quad x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

$$⑧ \quad x^8 - 1 = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$$

$$⑨ \quad x^9 - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$$

$$⑩ \quad x^{10} - 1 = (x - 1)(x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1)$$

Notice how each $x^n - 1$ adds another factor. What else is there?

Cyclotomic Polynomials

We write the n th cyclotomic polynomial as $\Phi_n(x)$. Thus, we have

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

Cyclotomic Polynomials

We write the n th cyclotomic polynomial as $\Phi_n(x)$. Thus, we have

Facts:

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

Cyclotomic Polynomials

We write the n th cyclotomic polynomial as $\Phi_n(x)$. Thus, we have

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

Facts:

- $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Cyclotomic Polynomials

We write the n th cyclotomic polynomial as $\Phi_n(x)$. Thus, we have

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

Facts:

- $x^n - 1 = \prod_{d|n} \Phi_d(x)$.
- $\deg \Phi_n(x) = \varphi(n)$ (Euler totient).

Cyclotomic Polynomials

We write the n th cyclotomic polynomial as $\Phi_n(x)$. Thus, we have

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

Facts:

- $x^n - 1 = \prod_{d|n} \Phi_d(x)$.
- $\deg \Phi_n(x) = \varphi(n)$ (Euler totient).
- $\Phi_n(x)$ is *irreducible* (over \mathbb{Z}).

Cyclotomic Polynomials

We write the n th cyclotomic polynomial as $\Phi_n(x)$. Thus, we have

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

Facts:

- $x^n - 1 = \prod_{d|n} \Phi_d(x)$.
- $\deg \Phi_n(x) = \varphi(n)$ (Euler totient).
- $\Phi_n(x)$ is *irreducible* (over \mathbb{Z}).
- $\Phi_n(x)$ is *reciprocal*.

Cyclotomic Polynomials

We write the n th cyclotomic polynomial as $\Phi_n(x)$. Thus, we have

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

Facts:

- $x^n - 1 = \prod_{d|n} \Phi_d(x)$.
- $\deg \Phi_n(x) = \varphi(n)$ (Euler totient).
- $\Phi_n(x)$ is *irreducible* (over \mathbb{Z}).
- $\Phi_n(x)$ is *reciprocal*.
- The roots of $\Phi_n(x)$ are the *primitive n th roots of unity*.

Cyclotomic Polynomials

We write the n th cyclotomic polynomial as $\Phi_n(x)$. Thus, we have

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

Facts:

- $x^n - 1 = \prod_{d|n} \Phi_d(x)$.
- $\deg \Phi_n(x) = \varphi(n)$ (Euler totient).
- $\Phi_n(x)$ is *irreducible* (over \mathbb{Z}).
- $\Phi_n(x)$ is *reciprocal*.
- The roots of $\Phi_n(x)$ are the *primitive n th roots of unity*.
- For prime p ,

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

Cyclotomic Polynomials

We write the n th cyclotomic polynomial as $\Phi_n(x)$. Thus, we have

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

Facts:

- $x^n - 1 = \prod_{d|n} \Phi_d(x)$.
- $\deg \Phi_n(x) = \varphi(n)$ (Euler totient).
- $\Phi_n(x)$ is *irreducible* (over \mathbb{Z}).
- $\Phi_n(x)$ is *reciprocal*.
- The roots of $\Phi_n(x)$ are the *primitive n th roots of unity*.
- For prime p ,
 $\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$.
- The coefficients of cyclotomic polynomials tend to be small.

Cyclotomic Polynomials

We write the n th cyclotomic polynomial as $\Phi_n(x)$. Thus, we have

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

Facts:

- For $n < 105$, $\Phi_n(x)$ only has coefficients of ± 1 (or 0). It's *flat*.

Cyclotomic Polynomials

We write the n th cyclotomic polynomial as $\Phi_n(x)$. Thus, we have

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

Facts:

- For $n < 105$, $\Phi_n(x)$ only has coefficients of ± 1 (or 0). It's *flat*.
- If a prime p divides n , then $\Phi_{np}(x) = \Phi_n(x^p)$.

Cyclotomic Polynomials

We write the n th cyclotomic polynomial as $\Phi_n(x)$. Thus, we have

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

Facts:

- For $n < 105$, $\Phi_n(x)$ only has coefficients of ± 1 (or 0). It's *flat*.
- If a prime p divides n , then $\Phi_{np}(x) = \Phi_n(x^p)$.
- Therefore, if m is the product of the prime divisors of n , then $\Phi_n(x) = \Phi_m(x^{n/m})$.

Cyclotomic Polynomials

We write the n th cyclotomic polynomial as $\Phi_n(x)$. Thus, we have

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

Facts:

- For $n < 105$, $\Phi_n(x)$ only has coefficients of ± 1 (or 0). It's *flat*.
- If a prime p divides n , then $\Phi_{np}(x) = \Phi_n(x^p)$.
- Therefore, if m is the product of the prime divisors of n , then $\Phi_n(x) = \Phi_m(x^{n/m})$.
- So we only need *squarefree* n .

Cyclotomic Polynomials

We write the n th cyclotomic polynomial as $\Phi_n(x)$. Thus, we have

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

Facts:

- For $n < 105$, $\Phi_n(x)$ only has coefficients of ± 1 (or 0). It's *flat*.
- If a prime p divides n , then $\Phi_{np}(x) = \Phi_n(x^p)$.
- Therefore, if m is the product of the prime divisors of n , then $\Phi_n(x) = \Phi_m(x^{n/m})$.
- So we only need *squarefree* n .
- If n is odd, $\Phi_{2n}(x) = \Phi_n(-x)$.

Cyclotomic Polynomials

We write the n th cyclotomic polynomial as $\Phi_n(x)$. Thus, we have

- $\Phi_1(x) = x - 1$
- $\Phi_2(x) = x + 1$
- $\Phi_3(x) = x^2 + x + 1$
-
- $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$
-
- $\Phi_7(x) = x^6 + x^5 + \dots + x + 1$
-
-
-

Facts:

- For $n < 105$, $\Phi_n(x)$ only has coefficients of ± 1 (or 0). It's *flat*.
- If a prime p divides n , then $\Phi_{np}(x) = \Phi_n(x^p)$.
- Therefore, if m is the product of the prime divisors of n , then $\Phi_n(x) = \Phi_m(x^{n/m})$.
- So we only need *squarefree* n .
- If n is odd, $\Phi_{2n}(x) = \Phi_n(-x)$.
- So we only need odd n .

Order

So we've reduced everything to squarefree odd numbers, which are the products of distinct odd primes.

The *order* of a cyclotomic polynomial $\Phi_n(x)$ is the number of odd primes dividing it.

Order

So we've reduced everything to squarefree odd numbers, which are the products of distinct odd primes.

The *order* of a cyclotomic polynomial $\Phi_n(x)$ is the number of odd primes dividing it.

We already know what cyclotomic polynomials of order 1 look like:

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

Order

So we've reduced everything to squarefree odd numbers, which are the products of distinct odd primes.

The *order* of a cyclotomic polynomial $\Phi_n(x)$ is the number of odd primes dividing it.

We already know what cyclotomic polynomials of order 1 look like:

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

We call cyclotomic polynomials of order 1 *prime*, order 2 *binary*, order 3 *ternary*, order 4 *quaternary*, and order 5 *quinary*, respectively.

Order

So we've reduced everything to squarefree odd numbers, which are the products of distinct odd primes.

The *order* of a cyclotomic polynomial $\Phi_n(x)$ is the number of odd primes dividing it.

We already know what cyclotomic polynomials of order 1 look like:

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

We call cyclotomic polynomials of order 1 *prime*, order 2 *binary*, order 3 *ternary*, order 4 *quaternary*, and order 5 *quinary*, respectively.

Basically, the cyclotomic polynomials get more complicated as the order increases.

Möbius inversion and a formula for $\Phi_n(x)$

Recall that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. We can apply a technique known as Möbius inversion to rewrite this as

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)},$$

where $\mu(m)$ is the Möbius function, which is 0 if m is not squarefree, 1 if it is and has an even number of prime factors, and -1 if it is squarefree with an odd number of prime factors.

Möbius inversion and a formula for $\Phi_n(x)$

Recall that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. We can apply a technique known as Möbius inversion to rewrite this as

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)},$$

where $\mu(m)$ is the Möbius function, which is 0 if m is not squarefree, 1 if it is and has an even number of prime factors, and -1 if it is squarefree with an odd number of prime factors.

In other words, if p, q, r are primes,

$$\begin{aligned} \Phi_p(x) &= \frac{x^p - 1}{x - 1}, & \Phi_{pq}(x) &= \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}, \\ \Phi_{pqr}(x) &= \frac{(x^{pqr} - 1)(x^p - 1)(x^q - 1)(x^r - 1)}{(x^{pq} - 1)(x^{pr} - 1)(x^{qr} - 1)(x - 1)}, & \dots \end{aligned}$$

Möbius inversion and a formula for $\Phi_n(x)$

Recall that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. We can apply a technique known as Möbius inversion to rewrite this as

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)},$$

where $\mu(m)$ is the Möbius function, which is 0 if m is not squarefree, 1 if it is and has an even number of prime factors, and -1 if it is squarefree with an odd number of prime factors.

In other words, if p, q, r are primes,

$$\begin{aligned} \Phi_p(x) &= \frac{x^p - 1}{x - 1}, & \Phi_{pq}(x) &= \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}, \\ \Phi_{pqr}(x) &= \frac{(x^{pqr} - 1)(x^p - 1)(x^q - 1)(x^r - 1)}{(x^{pq} - 1)(x^{pr} - 1)(x^{qr} - 1)(x - 1)}, & \dots \end{aligned}$$

We can easily see why increasing the order complicates things.

$$\Phi_{pq}(x)$$

Recall that $\Phi_n(x)$ was flat for all $n < 105$. Why 105?

$\Phi_{pq}(x)$

Recall that $\Phi_n(x)$ was flat for all $n < 105$. Why 105?

Notice that $105 = 3 \cdot 5 \cdot 7$, so this is the first cyclotomic polynomial of order 3. One reason this is the first non-flat cyclotomic polynomial is because all of those of order 2, $\Phi_{pq}(x)$, are flat.

$\Phi_{pq}(x)$

Recall that $\Phi_n(x)$ was flat for all $n < 105$. Why 105?

Notice that $105 = 3 \cdot 5 \cdot 7$, so this is the first cyclotomic polynomial of order 3. One reason this is the first non-flat cyclotomic polynomial is because all of those of order 2, $\Phi_{pq}(x)$, are flat.

There is a nice formula for $\Phi_{pq}(x)$ for primes p and q , which we will demonstrate for $p = 5$ and $q = 7$.

$\Phi_{pq}(x)$

Recall that $\Phi_n(x)$ was flat for all $n < 105$. Why 105?

Notice that $105 = 3 \cdot 5 \cdot 7$, so this is the first cyclotomic polynomial of order 3. One reason this is the first non-flat cyclotomic polynomial is because all of those of order 2, $\Phi_{pq}(x)$, are flat.

There is a nice formula for $\Phi_{pq}(x)$ for primes p and q , which we will demonstrate for $p = 5$ and $q = 7$. First, make this table:

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

$\Phi_{pq}(x)$

Recall that $\Phi_n(x)$ was flat for all $n < 105$. Why 105?

Notice that $105 = 3 \cdot 5 \cdot 7$, so this is the first cyclotomic polynomial of order 3. One reason this is the first non-flat cyclotomic polynomial is because all of those of order 2, $\Phi_{pq}(x)$, are flat.

There is a nice formula for $\Phi_{pq}(x)$ for primes p and q , which we will demonstrate for $p = 5$ and $q = 7$. First, make this table:

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

We start with 0 in the lower left and add p for every move to the right and q for every move upwards. Reduce modulo pq . This contains all the numbers from 0 to $pq - 1$, the residues modulo pq .

$$\Phi_{pq}(x)$$

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

Draw lines to the left and below 1.

$$\Phi_{pq}(x)$$

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

Draw lines to the left and below 1.

The numbers in the lower left corner are the exponents of the terms with coefficient 1.

$$\Phi_{pq}(x)$$

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

Draw lines to the left and below 1.

The numbers in the lower left corner are the exponents of the terms with coefficient 1.

The numbers in the upper right corner are the exponents of the terms with coefficient -1 .

$\Phi_{pq}(x)$

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

Draw lines to the left and below 1.

The numbers in the lower left corner are the exponents of the terms with coefficient 1.

The numbers in the upper right corner are the exponents of the terms with coefficient -1 .

Therefore,

$$\Phi_{35}(x) = x^{24} - x^{23} + x^{19} - x^{18} + x^{17} - x^{16} + x^{14} - x^{13} + x^{12} - x^{11} + x^{10} - x^8 + x^7 - x^6 + x^5 - x + 1.$$

Along the way, I discovered that you can plot similar polynomials on the same diagram. In particular, the multiples of $\Phi_{pq}(x)$ of the form $(1 + x + \cdots + x^{\ell-1})\Phi_{pq}(x)$ can be found in the same form by doing to ℓ what we did to 1 in the case of $\Phi_{pq}(x)$.

Along the way, I discovered that you can plot similar polynomials on the same diagram. In particular, the multiples of $\Phi_{pq}(x)$ of the form $(1 + x + \dots + x^{\ell-1})\Phi_{pq}(x)$ can be found in the same form by doing to ℓ what we did to 1 in the case of $\Phi_{pq}(x)$.

$$\Phi_{pq}(x)$$

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

Along the way, I discovered that you can plot similar polynomials on the same diagram. In particular, the multiples of $\Phi_{pq}(x)$ of the form $(1 + x + \dots + x^{\ell-1})\Phi_{pq}(x)$ can be found in the same form by doing to ℓ what we did to 1 in the case of $\Phi_{pq}(x)$.

$\Phi_{pq}(x)$

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

$(1 + x)\Phi_{pq}(x)$

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

Along the way, I discovered that you can plot similar polynomials on the same diagram. In particular, the multiples of $\Phi_{pq}(x)$ of the form $(1 + x + \dots + x^{\ell-1})\Phi_{pq}(x)$ can be found in the same form by doing to ℓ what we did to 1 in the case of $\Phi_{pq}(x)$.

$\Phi_{pq}(x)$							$(1 + x + x^2)\Phi_{pq}(x)$						
28	33	3	8	13	18	23	28	33	3	8	13	18	23
21	26	31	1	6	11	16	21	26	31	1	6	11	16
14	19	24	29	34	4	9	14	19	24	29	34	4	9
7	12	17	22	27	32	2	7	12	17	22	27	32	2
0	5	10	15	20	25	30	0	5	10	15	20	25	30
$(1 + x)\Phi_{pq}(x)$							$(1 + x + x^2 + x^3)\Phi_{pq}(x)$						
28	33	3	8	13	18	23	28	33	3	8	13	18	23
21	26	31	1	6	11	16	21	26	31	1	6	11	16
14	19	24	29	34	4	9	14	19	24	29	34	4	9
7	12	17	22	27	32	2	7	12	17	22	27	32	2
0	5	10	15	20	25	30	0	5	10	15	20	25	30

Coefficient Notation

Before we go any further, let's establish some notation for denoting the coefficients of a polynomial.

Coefficient Notation

Before we go any further, let's establish some notation for denoting the coefficients of a polynomial.

- $[x^k]p(x)$ is the coefficient of x^k in $p(x)$.

Coefficient Notation

Before we go any further, let's establish some notation for denoting the coefficients of a polynomial.

- $[x^k]p(x)$ is the coefficient of x^k in $p(x)$.
- $V(p(x)) := \{[x^k]p(x) \mid k \geq 0\}$ is the set of all coefficients, including leading zeros.

Coefficient Notation

Before we go any further, let's establish some notation for denoting the coefficients of a polynomial.

- $[x^k]p(x)$ is the coefficient of x^k in $p(x)$.
- $V(p(x)) := \{[x^k]p(x) \mid k \geq 0\}$ is the set of all coefficients, including leading zeros.
- Abbreviate $V(\Phi_n(x)) =: V_n$.

Coefficient Notation

Before we go any further, let's establish some notation for denoting the coefficients of a polynomial.

- $[x^k]p(x)$ is the coefficient of x^k in $p(x)$.
- $V(p(x)) := \{[x^k]p(x) \mid k \geq 0\}$ is the set of all coefficients, including leading zeros.
- Abbreviate $V(\Phi_n(x)) =: V_n$.
- The *height* of $\Phi_n(x)$ is $A(n) := \max(V_n \cup -V_n)$, the largest coefficient in absolute value.

Coefficient Notation

Before we go any further, let's establish some notation for denoting the coefficients of a polynomial.

- $[x^k]p(x)$ is the coefficient of x^k in $p(x)$.
- $V(p(x)) := \{[x^k]p(x) \mid k \geq 0\}$ is the set of all coefficients, including leading zeros.
- Abbreviate $V(\Phi_n(x)) =: V_n$.
- The *height* of $\Phi_n(x)$ is $A(n) := \max(V_n \cup -V_n)$, the largest coefficient in absolute value.
- Recall that height 1 polynomials are said to be *flat*.

Approaching $\Phi_{pqr}(x)$

As we have seen, both $\Phi_p(x)$ and $\Phi_{pq}(x)$ are completely characterized. The next problem, of course, is $\Phi_{pqr}(x)$.

Approaching $\Phi_{pqr}(x)$

As we have seen, both $\Phi_p(x)$ and $\Phi_{pq}(x)$ are completely characterized. The next problem, of course, is $\Phi_{pqr}(x)$. Recall that

$$\Phi_{pqr}(x) = \frac{(x^{pqr} - 1)(x^p - 1)(x^q - 1)(x^r - 1)}{(x^{pq} - 1)(x^{qr} - 1)(x^{pr} - 1)(x - 1)}.$$

Approaching $\Phi_{pqr}(x)$

As we have seen, both $\Phi_p(x)$ and $\Phi_{pq}(x)$ are completely characterized. The next problem, of course, is $\Phi_{pqr}(x)$. Recall that

$$\Phi_{pqr}(x) = \frac{(x^{pqr} - 1)(x^p - 1)(x^q - 1)(x^r - 1)}{(x^{pq} - 1)(x^{qr} - 1)(x^{pr} - 1)(x - 1)}.$$

One tempting method would be to write the denominators as power series: $(1 - x)^{-1} = 1 + x + x^2 + \dots$, for instance. Several previous researchers used this method along with complicated counting arguments to estimate various coefficients.

Approaching $\Phi_{pqr}(x)$

As we have seen, both $\Phi_p(x)$ and $\Phi_{pq}(x)$ are completely characterized. The next problem, of course, is $\Phi_{pqr}(x)$. Recall that

$$\Phi_{pqr}(x) = \frac{(x^{pqr} - 1)(x^p - 1)(x^q - 1)(x^r - 1)}{(x^{pq} - 1)(x^{qr} - 1)(x^{pr} - 1)(x - 1)}.$$

One tempting method would be to write the denominators as power series: $(1 - x)^{-1} = 1 + x + x^2 + \dots$, for instance. Several previous researchers used this method along with complicated counting arguments to estimate various coefficients.

Another method is to write

$$\Phi_{pqr}(x) = \frac{\Phi_{pq}(x^r)}{\Phi_{pq}(x)} = \Phi_{pq}(x^r)\Phi_1(x)\Phi_p(x)\Phi_q(x)(1 + x^{pq} + x^{2pq} + \dots).$$

Approaching $\Phi_{pqr}(x)$

As we have seen, both $\Phi_p(x)$ and $\Phi_{pq}(x)$ are completely characterized. The next problem, of course, is $\Phi_{pqr}(x)$. Recall that

$$\Phi_{pqr}(x) = \frac{(x^{pqr} - 1)(x^p - 1)(x^q - 1)(x^r - 1)}{(x^{pq} - 1)(x^{qr} - 1)(x^{pr} - 1)(x - 1)}.$$

One tempting method would be to write the denominators as power series: $(1 - x)^{-1} = 1 + x + x^2 + \dots$, for instance. Several previous researchers used this method along with complicated counting arguments to estimate various coefficients.

Another method is to write

$$\Phi_{pqr}(x) = \frac{\Phi_{pq}(x^r)}{\Phi_{pq}(x)} = \Phi_{pq}(x^r)\Phi_1(x)\Phi_p(x)\Phi_q(x)(1 + x^{pq} + x^{2pq} + \dots).$$

This is a bit neater, but still relies on those complicated counting arguments.

Bounding $A(pqr)$ in terms of p

Most previous results focused on the $\Phi_{pqr}(x)$ which had the largest height, in terms of p . In particular, most focused on the following long-standing conjecture:

Conjecture (Beiter, 1968)

Let $p < q < r$ be primes. Then $A(pqr) \leq \frac{p+1}{2}$.

Bounding $A(pqr)$ in terms of p

Most previous results focused on the $\Phi_{pqr}(x)$ which had the largest height, in terms of p . In particular, most focused on the following long-standing conjecture:

Conjecture (Beiter, 1968)

Let $p < q < r$ be primes. Then $A(pqr) \leq \frac{p+1}{2}$.

This conjecture turned out to be false. The first counterexample is $(p, q, r) = (17, 29, 41)$. A better bound comes at $2p/3$:

Theorem (Moree and Gallot, 2007)

Given any $\epsilon > 0$, there exist infinitely many triples (p_j, q_j, r_j) with $p_1 < p_2 < \dots$ consecutive primes such that $A(p_j q_j r_j) > (2/3 - \epsilon)p_j$.

Resolving Beiter's Conjecture

Very recently (in October), Zhao and Zhang claim to have proven the corrected conjecture:

Theorem (Zhao and Zhang, 2009)

Let $p < q < r$ be primes. Then $A(pqr) \leq \frac{2p}{3}$.

This would completely resolve Beiter's conjecture, since Moree and Gallot showed that $2p/3$ was the best upper bound.

Flat Ternary Cyclotomic Polynomials

What about those of small height? In 2006, my advisor, Nathan Kaplan, at the same REU in Duluth, found this flat family:

Theorem (Kaplan, 2006)

Let $p < q < r$ be primes such that $r \equiv \pm 1 \pmod{pq}$. Then $A(pqr) = 1$.

Flat Ternary Cyclotomic Polynomials

What about those of small height? In 2006, my advisor, Nathan Kaplan, at the same REU in Duluth, found this flat family:

Theorem (Kaplan, 2006)

Let $p < q < r$ be primes such that $r \equiv \pm 1 \pmod{pq}$. Then $A(pqr) = 1$.

He also proved a result known as *periodicity*. Later he used his method to generalize to the following:

Theorem (Kaplan, 2009)

Let n be a positive integer. Let s, t be primes satisfying $n < s < t$ and $s \equiv t \pmod{n}$. Then $V_{ns} = V_{nt}$.

$\Phi_{pq}(x)$ as a GCD

I started by reexamining $\Phi_{pq}(x)$. Recall our table:

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

$\Phi_{pq}(x)$ as a GCD

I started by reexamining $\Phi_{pq}(x)$. Recall our table:

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

I noticed that we could also write this as the left columns

$\Phi_{pq}(x)$ as a GCD

I started by reexamining $\Phi_{pq}(x)$. Recall our table:

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

I noticed that we could also write this as the left columns minus the top rows.

$\Phi_{pq}(x)$ as a GCD

I started by reexamining $\Phi_{pq}(x)$. Recall our table:

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

I noticed that we could also write this as the left columns minus the top rows.

Now, the left columns are a multiple of $1 + x^7 + x^{14} + x^{21} + x^{28}$,

$\Phi_{pq}(x)$ as a GCD

I started by reexamining $\Phi_{pq}(x)$. Recall our table:

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

I noticed that we could also write this as the left columns minus the top rows.

Now, the left columns are a multiple of $1 + x^7 + x^{14} + x^{21} + x^{28}$, while the right columns are a multiple of $1 + x^5 + x^{10} + x^{15} + x^{20} + x^{25} + x^{30}$.

$\Phi_{pq}(x)$ as a GCD

I started by reexamining $\Phi_{pq}(x)$. Recall our table:

28	33	3	8	13	18	23
21	26	31	1	6	11	16
14	19	24	29	34	4	9
7	12	17	22	27	32	2
0	5	10	15	20	25	30

I noticed that we could also write this as the left columns minus the top rows.

Now, the left columns are a multiple of $1 + x^7 + x^{14} + x^{21} + x^{28}$, while the right columns are a multiple of $1 + x^5 + x^{10} + x^{15} + x^{20} + x^{25} + x^{30}$.

Notice that these are just $\Phi_5(x^7)$ and $\Phi_7(x^5)$. Any ideas for how this might generalize?

$\Phi_{np}(x)$ as a GCD

This can be generalized as follows:

Theorem

Let n be a positive integer and p a prime not dividing n . Then

$$\Phi_{np}(x) = \gcd\{1 + x^n + \cdots + x^{n(p-1)}, \Phi_n(x^p)\}.$$

$\Phi_{np}(x)$ as a GCD

This can be generalized as follows:

Theorem

Let n be a positive integer and p a prime not dividing n . Then

$$\Phi_{np}(x) = \gcd\{1 + x^n + \dots + x^{n(p-1)}, \Phi_n(x^p)\}.$$

A series of definitions:

- $f(x) := \Phi_{np}(x)$
- $g(x) := 1 + x^n + \dots + x^{n(p-1)}$
- $h(x) := \Phi_n(x^p)$

$\Phi_{np}(x)$ as a GCD

This can be generalized as follows:

Theorem

Let n be a positive integer and p a prime not dividing n . Then

$$\Phi_{np}(x) = \gcd\{1 + x^n + \dots + x^{n(p-1)}, \Phi_n(x^p)\}.$$

A series of definitions:

- $f(x) := \Phi_{np}(x)$
- $g(x) := 1 + x^n + \dots + x^{n(p-1)}$
- $h(x) := \Phi_n(x^p)$
- $a(x), b(x) \in \mathbb{Z}[x]$ such that $f(x) = a(x)g(x) + b(x)h(x)$

Divide and Conquer

Divide up the coefficients of $f(x)$ into family of polynomials $\{F_j(x)\}_{j=0}^{p-1}$ according to the residue of the exponents modulo p .

Divide and Conquer

Divide up the coefficients of $f(x)$ into family of polynomials $\{F_j(x)\}_{j=0}^{p-1}$ according to the residue of the exponents modulo p .

For example, consider $n = 10$ and $p = 3$:

$$f(x) = 1 + x - x^3 - x^4 - x^5 + x^7 + x^8.$$

Divide and Conquer

Divide up the coefficients of $f(x)$ into family of polynomials $\{F_j(x)\}_{j=0}^{p-1}$ according to the residue of the exponents modulo p .

For example, consider $n = 10$ and $p = 3$:

$$f(x) = 1 + x - x^3 - x^4 - x^5 + x^7 + x^8.$$

$$F_0(x) = 1 - x$$

Divide and Conquer

Divide up the coefficients of $f(x)$ into family of polynomials $\{F_j(x)\}_{j=0}^{p-1}$ according to the residue of the exponents modulo p .

For example, consider $n = 10$ and $p = 3$:

$$f(x) = 1 + x - x^3 - x^4 - x^5 + x^7 + x^8.$$

$$F_0(x) = 1 - x$$

$$F_1(x) = 1 - x + x^2$$

Divide and Conquer

Divide up the coefficients of $f(x)$ into family of polynomials $\{F_j(x)\}_{j=0}^{p-1}$ according to the residue of the exponents modulo p .

For example, consider $n = 10$ and $p = 3$:

$$f(x) = 1 + x - x^3 - x^4 - x^5 + x^7 + x^8.$$

$$F_0(x) = 1 - x$$

$$F_1(x) = 1 - x + x^2$$

$$F_2(x) = -x + x^2$$

Divide and Conquer

Divide up the coefficients of $f(x)$ into family of polynomials $\{F_j(x)\}_{j=0}^{p-1}$ according to the residue of the exponents modulo p .

For example, consider $n = 10$ and $p = 3$:

$$f(x) = 1 + x - x^3 - x^4 - x^5 + x^7 + x^8.$$

$$F_0(x) = 1 - x$$

$$F_1(x) = 1 - x + x^2$$

$$F_2(x) = -x + x^2$$

In general, we define

$$F_j(x) := \sum_{i \geq 0} x^i [x^{j+ip}] f(x), \text{ so } f(x) = \sum_{j=0}^{p-1} x^j F_j(x^p).$$

Divide and Conquer

Divide up the coefficients of $f(x)$ into family of polynomials $\{F_j(x)\}_{j=0}^{p-1}$ according to the residue of the exponents modulo p .

For example, consider $n = 10$ and $p = 3$:

$$f(x) = 1 + x - x^3 - x^4 - x^5 + x^7 + x^8.$$

$$F_0(x) = 1 - x$$

$$F_1(x) = 1 - x + x^2$$

$$F_2(x) = -x + x^2$$

In general, we define

$$F_j(x) := \sum_{i \geq 0} x^i [x^{j+ip}] f(x), \text{ so } f(x) = \sum_{j=0}^{p-1} x^j F_j(x^p).$$

$$V_{np} = V(f(x)) = \bigcup_{j=0}^{p-1} V(F_j(x^p)).$$

Divide and Conquer

Divide up the coefficients of $f(x)$ into family of polynomials $\{F_j(x)\}_{j=0}^{p-1}$ according to the residue of the exponents modulo p .

For example, consider $n = 10$ and $p = 3$:

$$f(x) = 1 + x - x^3 - x^4 - x^5 + x^7 + x^8.$$

$$F_0(x) = 1 - x$$

$$F_1(x) = 1 - x + x^2$$

$$F_2(x) = -x + x^2$$

In general, we define

$$F_j(x) := \sum_{i \geq 0} x^i [x^{j+ip}] f(x), \text{ so } f(x) = \sum_{j=0}^{p-1} x^j F_j(x^p).$$

$$V_{np} = V(f(x)) = \bigcup_{j=0}^{p-1} V(F_j(x^p)).$$

The $F_j(x)$ have quite a bit of structure. Moreover, this structure uniquely determines the $F_j(x)$!

Improving Previous Results

First, I used this method to improve Kaplan's periodicity result:

Theorem (Kaplan, 2009)

Let n be a positive integer. Let s, t be primes satisfying $n < s < t$ and $s \equiv t \pmod{n}$. Then $V_{ns} = V_{nt}$.

Improving Previous Results

First, I used this method to improve Kaplan's periodicity result:

Theorem (Kaplan, 2009)

Let n be a positive integer. Let s, t be primes satisfying $n < s < t$ and $s \equiv t \pmod{n}$. Then $V_{ns} = V_{nt}$.

Here's my version:

Theorem

Let n be a positive integer. Let s, t be primes satisfying $n - \varphi(n) < s < t$ and $s \equiv \pm t \pmod{n}$. Then $V_{ns} = \pm V_{nt}$, with the same signs taken in both \pm .

Improving Previous Results

I also reproved Kaplan's family of flat polynomials, and found more:

Theorem (Kaplan, 2006)

Let $p < q < r$ be primes such that $r \equiv \pm 1 \pmod{pq}$. Then $A(pqr) = 1$.

Improving Previous Results

I also reproved Kaplan's family of flat polynomials, and found more:

Theorem (Kaplan, 2006)

Let $p < q < r$ be primes such that $r \equiv \pm 1 \pmod{pq}$. Then $A(pqr) = 1$.

Theorem

Let $p < q < r$ be primes such that $r \equiv \pm 2 \pmod{pq}$. Then $A(pqr) = 1$ if and only if $q \equiv 1 \pmod{p}$.

Improving Previous Results

I also reproved Kaplan's family of flat polynomials, and found more:

Theorem (Kaplan, 2006)

Let $p < q < r$ be primes such that $r \equiv \pm 1 \pmod{pq}$. Then $A(pqr) = 1$.

Theorem

Let $p < q < r$ be primes such that $r \equiv \pm 2 \pmod{pq}$. Then $A(pqr) = 1$ if and only if $q \equiv 1 \pmod{p}$.

Theorem

Let $p < q < r$ be primes and w the minimal positive integer such that $r \equiv \pm w \pmod{pq}$. Then $A(pqr) \leq w$.

Broadhurst's Conjecture

During the summer, my advisor came across a discussion about flat cyclotomic polynomials on a Yahoo! primenumbers message board. Many of the comments centered on computing the heights of cyclotomic polynomials. One of the contributors, a mathematician named David Broadhurst, used his computations to generate some conjectures. I proved one of these:

Broadhurst's Conjecture

During the summer, my advisor came across a discussion about flat cyclotomic polynomials on a Yahoo! primenumbers message board. Many of the comments centered on computing the heights of cyclotomic polynomials. One of the contributors, a mathematician named David Broadhurst, used his computations to generate some conjectures. I proved one of these:

Theorem

Let $p < q < r$ be primes and let w be the minimal positive integer such that $r \equiv \pm w \pmod{pq}$. If $p \equiv 1 \pmod{w}$ and $q \equiv 1 \pmod{wp}$, then $A(pqr) = 1$.

Broadhurst's Conjecture

During the summer, my advisor came across a discussion about flat cyclotomic polynomials on a Yahoo! primenumbers message board. Many of the comments centered on computing the heights of cyclotomic polynomials. One of the contributors, a mathematician named David Broadhurst, used his computations to generate some conjectures. I proved one of these:

Theorem

Let $p < q < r$ be primes and let w be the minimal positive integer such that $r \equiv \pm w \pmod{pq}$. If $p \equiv 1 \pmod{w}$ and $q \equiv 1 \pmod{wp}$, then $A(pqr) = 1$.

Note that this gives us flat $\Phi_{pqr}(x)$ with r arbitrarily far from a multiple of pq , while Kaplan's family was always 1 away from a multiple of pq .

$\Phi_{pqrs}(x)$

Not much at all was known about these. In 2009, Kaplan took the smallest flat quaternary cyclotomic polynomial, $\Phi_{3 \cdot 5 \cdot 31 \cdot 929}(x)$, and used his new periodicity result to produce an infinite family of flat quaternary cyclotomic polynomials. For any prime $s \equiv 929 \equiv -1 \pmod{3 \cdot 5 \cdot 31}$, $A(3 \cdot 5 \cdot 31 \cdot s) = 1$.

$\Phi_{pqrs}(x)$

Not much at all was known about these. In 2009, Kaplan took the smallest flat quaternary cyclotomic polynomial, $\Phi_{3 \cdot 5 \cdot 31 \cdot 929}(x)$, and used his new periodicity result to produce an infinite family of flat quaternary cyclotomic polynomials. For any prime $s \equiv 929 \equiv -1 \pmod{3 \cdot 5 \cdot 31}$, $A(3 \cdot 5 \cdot 31 \cdot s) = 1$.

In this special case, notice that $q \equiv -1 \pmod{p}$ and $r \equiv 1 \pmod{pq}$. I massively generalized this family:

Theorem

Let $p < q < r < s$ be primes such that $r \equiv \pm 1 \pmod{pq}$ and $s \equiv \pm 1 \pmod{pqr}$. Then $A(pqrs) = 1$ if and only if $q \equiv -1 \pmod{p}$.

$\Phi_{pqrst}(x)$

For primes p, q, r, s, t , $\Phi_{pqrst}(x)$ is a *quinary cyclotomic polynomial*. I got to figure this name out, since no one had investigated these before!

$\Phi_{pqrst}(x)$

For primes p, q, r, s, t , $\Phi_{pqrst}(x)$ is a *quinary cyclotomic polynomial*. I got to figure this name out, since no one had investigated these before!

No known examples are flat. I showed that the natural candidates are indeed not flat:

$\Phi_{pqrst}(x)$

For primes p, q, r, s, t , $\Phi_{pqrst}(x)$ is a *quinary cyclotomic polynomial*. I got to figure this name out, since no one had investigated these before!

No known examples are flat. I showed that the natural candidates are indeed not flat:

Theorem

Let $p < q < r < s < t$ be odd primes such that $r \equiv \pm 1 \pmod{pq}$, $s \equiv \pm 1 \pmod{pqr}$ and $t \equiv \pm 1 \pmod{pqrs}$. Then $A(pqrst) > 1$.

Weird Cases

Normally, multiplying by an additional prime p increases the height of the cyclotomic polynomial (for $p > 2$, of course).

Weird Cases

Normally, multiplying by an additional prime p increases the height of the cyclotomic polynomial (for $p > 2$, of course).
 However, I found a few counterexamples for $p = 3$:

n	$3n$	$A(n)$	$A(3n)$
$4745 = 5 \cdot 13 \cdot 73$	14235	3	2
$7469 = 7 \cdot 11 \cdot 97$	22407	4	3
$10439 = 11 \cdot 13 \cdot 73$	31317	6	4
$14231 = 7 \cdot 19 \cdot 107$	42693	4	3
$14443 = 11 \cdot 13 \cdot 101$	43329	5	4
$14707 = 7 \cdot 11 \cdot 191$	44121	4	3

Weird Cases

Normally, multiplying by an additional prime p increases the height of the cyclotomic polynomial (for $p > 2$, of course). However, I found a few counterexamples for $p = 3$:

n	$3n$	$A(n)$	$A(3n)$
$4745 = 5 \cdot 13 \cdot 73$	14235	3	2
$7469 = 7 \cdot 11 \cdot 97$	22407	4	3
$10439 = 11 \cdot 13 \cdot 73$	31317	6	4
$14231 = 7 \cdot 19 \cdot 107$	42693	4	3
$14443 = 11 \cdot 13 \cdot 101$	43329	5	4
$14707 = 7 \cdot 11 \cdot 191$	44121	4	3

There are no examples where $A(5n) < A(n)$ for $n < 20000$. This leads to the question: For which primes p do there exist n such that $A(np) < A(n)$?

Pseudocyclotomic Polynomials

There's also a natural extension of the cyclotomic polynomials: the *pseudocyclotomic polynomials*. Basically, we take our expression for $\Phi_{pq}(x)$, for instance, $\frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)}$, and plug in values of p and q that aren't (necessarily) prime.

Pseudocyclotomic Polynomials

There's also a natural extension of the cyclotomic polynomials: the *pseudocyclotomic polynomials*. Basically, we take our expression for $\Phi_{pq}(x)$, for instance, $\frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)}$, and plug in values of p and q that aren't (necessarily) prime.

In order for this to cancel, we do need to require that p and q are relatively prime. You can see how to generalize this easily.

Pseudocyclotomic Polynomials

There's also a natural extension of the cyclotomic polynomials: the *pseudocyclotomic polynomials*. Basically, we take our expression for $\Phi_{pq}(x)$, for instance, $\frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)}$, and plug in values of p and q that aren't (necessarily) prime.

In order for this to cancel, we do need to require that p and q are relatively prime. You can see how to generalize this easily.

In fact, everything I proved about cyclotomic polynomials carries over to the pseudocyclotomic polynomials, since I never used that p , q and r were prime.

Pseudocyclotomic Polynomials

There's also a natural extension of the cyclotomic polynomials: the *pseudocyclotomic polynomials*. Basically, we take our expression for $\Phi_{pq}(x)$, for instance, $\frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)}$, and plug in values of p and q that aren't (necessarily) prime.

In order for this to cancel, we do need to require that p and q are relatively prime. You can see how to generalize this easily.

In fact, everything I proved about cyclotomic polynomials carries over to the pseudocyclotomic polynomials, since I never used that p , q and r were prime.

There are also some outstanding questions regarding the pseudocyclotomic polynomials:

- Does the revised Beiter conjecture hold for pseudocyclotomic polynomials?
- Are there any patterns in the pseudocyclotomic polynomials?

Open Questions and Conjectures

There are still many open questions and conjectures regarding cyclotomic polynomials of small height.

Open Questions and Conjectures

There are still many open questions and conjectures regarding cyclotomic polynomials of small height.

- Let $p < q < r$ be primes. If $q \not\equiv \pm 1 \pmod{p}$ and $r \not\equiv \pm 1 \pmod{pq}$, then $A(pqr) > 1$.

Open Questions and Conjectures

There are still many open questions and conjectures regarding cyclotomic polynomials of small height.

- Let $p < q < r$ be primes. If $q \not\equiv \pm 1 \pmod{p}$ and $r \not\equiv \pm 1 \pmod{pq}$, then $A(pqr) > 1$.
- There are no flat quinary cyclotomic polynomials.

Open Questions and Conjectures

There are still many open questions and conjectures regarding cyclotomic polynomials of small height.

- Let $p < q < r$ be primes. If $q \not\equiv \pm 1 \pmod{p}$ and $r \not\equiv \pm 1 \pmod{pq}$, then $A(pqr) > 1$.
- There are no flat quinary cyclotomic polynomials.
- For any prime p and positive integer n , if $A(n) > 1$, then $A(np) > 1$. (This holds even for our $A(np) < A(n)$ examples.)

Open Questions and Conjectures

There are still many open questions and conjectures regarding cyclotomic polynomials of small height.

- Let $p < q < r$ be primes. If $q \not\equiv \pm 1 \pmod{p}$ and $r \not\equiv \pm 1 \pmod{pq}$, then $A(pqr) > 1$.
- There are no flat quinary cyclotomic polynomials.
- For any prime p and positive integer n , if $A(n) > 1$, then $A(np) > 1$. (This holds even for our $A(np) < A(n)$ examples.)
- Classify all flat cyclotomic polynomials.

Open Questions and Conjectures

There are still many open questions and conjectures regarding cyclotomic polynomials of small height.

- Let $p < q < r$ be primes. If $q \not\equiv \pm 1 \pmod{p}$ and $r \not\equiv \pm 1 \pmod{pq}$, then $A(pqr) > 1$.
- There are no flat quinary cyclotomic polynomials.
- For any prime p and positive integer n , if $A(n) > 1$, then $A(np) > 1$. (This holds even for our $A(np) < A(n)$ examples.)
- Classify all flat cyclotomic polynomials.
- Which conjectures hold for pseudocyclotomic polynomials?

Open Questions and Conjectures

There are still many open questions and conjectures regarding cyclotomic polynomials of small height.

- Let $p < q < r$ be primes. If $q \not\equiv \pm 1 \pmod{p}$ and $r \not\equiv \pm 1 \pmod{pq}$, then $A(pqr) > 1$.
- There are no flat quinary cyclotomic polynomials.
- For any prime p and positive integer n , if $A(n) > 1$, then $A(np) > 1$. (This holds even for our $A(np) < A(n)$ examples.)
- Classify all flat cyclotomic polynomials.
- Which conjectures hold for pseudocyclotomic polynomials?

That's all! I hope you enjoyed listening to me talk about what I did for a summer, and got a feel for what research is like from me. Maybe if you go to Duluth some day you'll work on cyclotomic polynomials, too...