

Factorising the ℓ^{th} Cyclotomic Polynomial over \mathbb{F}_p

Andrew Potter

May 12, 2009

Introduction

Efficiency
Background

The Problem

Statement
Motivation
Prerequisites

Results

Examples
Results

Future Directions

The Problem of Efficiency

The Problem of Efficiency

We seek *efficient* algorithms.

The Problem of Efficiency

We seek *efficient* algorithms. What do we mean by *efficient*?

The Problem of Efficiency

We seek *efficient* algorithms. What do we mean by *efficient*?

Practical Version

It can actually be done in
reasonable time!

The Problem of Efficiency

We seek *efficient* algorithms. What do we mean by *efficient*?

Practical Version

It can actually be done in reasonable time!

Theoretical Version

It can be done in polynomial time.

The Problem of Efficiency

We seek *efficient* algorithms. What do we mean by *efficient*?

Practical Version

It can actually be done in reasonable time!

Is time $O(n^{1000})$ *efficient*?

Theoretical Version

It can be done in polynomial time.

The Problem of Efficiency

We seek *efficient* algorithms. What do we mean by *efficient*?

Practical Version

It can actually be done in reasonable time!

Is time $O(n^{1000})$ *efficient*?

Is time $O(2^{n/1000})$ *efficient*?

Theoretical Version

It can be done in polynomial time.

The Problem of Efficiency

We seek *efficient* algorithms. What do we mean by *efficient*?

Practical Version

It can actually be done in reasonable time!

Is time $O(n^{1000})$ *efficient*?

Is time $O(2^{n/1000})$ *efficient*?

Theoretical Version

It can be done in polynomial time.

I seek **polynomial-time** algorithms for **polynomial factorisation**.

Polynomial Factorisation

Issues to Consider

Polynomial Factorisation

Issues to Consider

- ▶ Deterministic or Probabilistic?

Polynomial Factorisation

Issues to Consider

- ▶ Deterministic or Probabilistic?
- ▶ Univariate or Multivariate?

Polynomial Factorisation

Issues to Consider

- ▶ Deterministic or Probabilistic?
- ▶ Univariate or Multivariate?
- ▶ Over which field?

Polynomial Factorisation

Issues to Consider

- ▶ Deterministic or Probabilistic?
- ▶ Univariate or Multivariate?
- ▶ Over which field?

Examples

Polynomial Factorisation

Issues to Consider

- ▶ Deterministic or Probabilistic?
- ▶ Univariate or Multivariate?
- ▶ Over which field?

Examples

- ▶ LLL algorithm: deterministic, univariate, over \mathbb{Q}

Polynomial Factorisation

Issues to Consider

- ▶ Deterministic or Probabilistic?
- ▶ Univariate or Multivariate?
- ▶ Over which field?

Examples

- ▶ LLL algorithm: deterministic, univariate, over \mathbb{Q}
- ▶ Berlekamp and Cantor-Zassenhaus: probabilistic, univariate, over \mathbb{F}_q

My Research

My Research

- ▶ Fix an odd prime ℓ . The ℓ^{th} cyclotomic polynomial ψ is defined by

$$\psi(x) = 1 + x + x^2 + \dots + x^{\ell-1}.$$

My Research

- ▶ Fix an odd prime ℓ . The ℓ^{th} cyclotomic polynomial ψ is defined by

$$\psi(x) = 1 + x + x^2 + \dots + x^{\ell-1}.$$

- ▶ For odd prime $p \neq \ell$, factor ψ over \mathbb{F}_p .

My Research

- ▶ Fix an odd prime ℓ . The ℓ^{th} cyclotomic polynomial ψ is defined by

$$\psi(x) = 1 + x + x^2 + \dots + x^{\ell-1}.$$

- ▶ For odd prime $p \neq \ell$, factor ψ over \mathbb{F}_p .
- ▶ Algorithm should be **deterministic** in time **polynomial** in $\log p$.

History

History

- ▶ **Schoof** (1985): Counting points on an elliptic curve over \mathbb{F}_p

History

- ▶ **Schoof** (1985): Counting points on an elliptic curve over \mathbb{F}_p
 \rightsquigarrow **Application**: Square roots mod p

History

- ▶ **Schoof** (1985): Counting points on an elliptic curve over \mathbb{F}_p
 \rightsquigarrow **Application**: Square roots mod p
 Fix $a \in \mathbb{Z}$. Factor $x^2 - a \pmod{p}$.

History

- ▶ **Schoof** (1985): Counting points on an elliptic curve over \mathbb{F}_p
 \rightsquigarrow **Application**: Square roots mod p
 Fix $a \in \mathbb{Z}$. Factor $x^2 - a \pmod{p}$.
- ▶ **Pila** (1990): Generalised Schoof's work to abelian varieties

History

- ▶ **Schoof** (1985): Counting points on an elliptic curve over \mathbb{F}_p
 \rightsquigarrow **Application**: Square roots mod p
 Fix $a \in \mathbb{Z}$. Factor $x^2 - a \pmod{p}$.
- ▶ **Pila** (1990): Generalised Schoof's work to abelian varieties
 \rightsquigarrow **Application**: ℓ^{th} roots of unity mod p

History

- ▶ **Schoof** (1985): Counting points on an elliptic curve over \mathbb{F}_p
 \rightsquigarrow **Application:** Square roots mod p
 Fix $a \in \mathbb{Z}$. Factor $x^2 - a \pmod{p}$.
- ▶ **Pila** (1990): Generalised Schoof's work to abelian varieties
 \rightsquigarrow **Application:** ℓ^{th} roots of unity mod p
 Factor $\psi \pmod{p}$ when $p \equiv 1 \pmod{\ell}$.

History

- ▶ **Schoof (1985)**: Counting points on an elliptic curve over \mathbb{F}_p
 \rightsquigarrow **Application**: Square roots mod p
 Fix $a \in \mathbb{Z}$. Factor $x^2 - a \pmod{p}$.
- ▶ **Pila (1990)**: Generalised Schoof's work to abelian varieties
 \rightsquigarrow **Application**: ℓ^{th} roots of unity mod p
 Factor $\psi \pmod{p}$ when $p \equiv 1 \pmod{\ell}$.
 \rightsquigarrow *linear factors*

History

- ▶ **Schoof (1985)**: Counting points on an elliptic curve over \mathbb{F}_p
 \rightsquigarrow **Application**: Square roots mod p
 Fix $a \in \mathbb{Z}$. Factor $x^2 - a \pmod{p}$.
- ▶ **Pila (1990)**: Generalised Schoof's work to abelian varieties
 \rightsquigarrow **Application**: ℓ^{th} roots of unity mod p
 Factor $\psi \pmod{p}$ when $p \equiv 1 \pmod{\ell}$.
 \rightsquigarrow *linear factors*
- ▶ $p \not\equiv 1 \pmod{\ell}$?

The Idea

The Idea

- ▶ Let f be the smallest positive integer such that $p^f \equiv 1 \pmod{\ell}$.

The Idea

- ▶ Let f be the smallest positive integer such that $p^f \equiv 1 \pmod{\ell}$.
- ▶ Let $g = (\ell - 1)/f$.

The Idea

- ▶ Let f be the smallest positive integer such that $p^f \equiv 1 \pmod{\ell}$.
- ▶ Let $g = (\ell - 1)/f$.
- ▶ ψ splits into g factors, each of degree f .

The Idea

- ▶ Let f be the smallest positive integer such that $p^f \equiv 1 \pmod{\ell}$.
- ▶ Let $g = (\ell - 1)/f$.
- ▶ ψ splits into g factors, each of degree f .

- ▶ The g factors of ψ

The Idea

- ▶ Let f be the smallest positive integer such that $p^f \equiv 1 \pmod{\ell}$.
- ▶ Let $g = (\ell - 1)/f$.
- ▶ ψ splits into g factors, each of degree f .

- ▶ The g factors of $\psi \leftrightarrow$ the g **prime ideals** lying over p in $\mathbb{Z}[\zeta]$.

Algebraic Number Theory

Algebraic Number Theory

- ▶ \mathbb{Z} admits *unique factorisation*.

Algebraic Number Theory

- ▶ \mathbb{Z} admits *unique factorisation*.
Every element in \mathbb{Z} factorises uniquely into a product of primes.

Algebraic Number Theory

- ▶ \mathbb{Z} admits *unique factorisation*.
Every element in \mathbb{Z} factorises uniquely into a product of primes.
- ▶ Let $\zeta = e^{2\pi i/\ell}$ be a primitive ℓ^{th} root of unity.

Algebraic Number Theory

- ▶ \mathbb{Z} admits *unique factorisation*.
Every element in \mathbb{Z} factorises uniquely into a product of primes.
- ▶ Let $\zeta = e^{2\pi i/\ell}$ be a primitive ℓ^{th} root of unity.
Define the ring
$$\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \dots + a_{\ell-1}\zeta^{\ell-1} \mid a_0, \dots, a_{\ell-1} \in \mathbb{Z}\}.$$

Algebraic Number Theory

- ▶ \mathbb{Z} admits *unique factorisation*.
Every element in \mathbb{Z} factorises uniquely into a product of primes.
- ▶ Let $\zeta = e^{2\pi i/\ell}$ be a primitive ℓ^{th} root of unity.
Define the ring
$$\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \dots + a_{\ell-1}\zeta^{\ell-1} \mid a_0, \dots, a_{\ell-1} \in \mathbb{Z}\}.$$
- ▶ $\mathbb{Z}[\zeta]$ does **not** admit unique factorisation, but it does admit *unique factorisation of ideals*.

Algebraic Number Theory

- ▶ \mathbb{Z} admits *unique factorisation*.
Every element in \mathbb{Z} factorises uniquely into a product of primes.
- ▶ Let $\zeta = e^{2\pi i/\ell}$ be a primitive ℓ^{th} root of unity.
Define the ring
$$\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \dots + a_{\ell-1}\zeta^{\ell-1} \mid a_0, \dots, a_{\ell-1} \in \mathbb{Z}\}.$$
- ▶ $\mathbb{Z}[\zeta]$ does **not** admit unique factorisation, but it does admit *unique factorisation of ideals*.
Every ideal $I \subset \mathbb{Z}[\zeta]$ factorises uniquely as a product of *prime ideals*.

Algebraic Number Theory

- ▶ \mathbb{Z} admits *unique factorisation*.
Every element in \mathbb{Z} factorises uniquely into a product of primes.
- ▶ Let $\zeta = e^{2\pi i/\ell}$ be a primitive ℓ^{th} root of unity.
Define the ring
$$\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \dots + a_{\ell-1}\zeta^{\ell-1} \mid a_0, \dots, a_{\ell-1} \in \mathbb{Z}\}.$$
- ▶ $\mathbb{Z}[\zeta]$ does **not** admit unique factorisation, but it does admit *unique factorisation of ideals*.
Every ideal $I \subset \mathbb{Z}[\zeta]$ factorises uniquely as a product of *prime ideals*.
- ▶ How does (p) factorise in $\mathbb{Z}[\zeta]$?

Algebraic Number Theory

- ▶ \mathbb{Z} admits *unique factorisation*.
Every element in \mathbb{Z} factorises uniquely into a product of primes.
- ▶ Let $\zeta = e^{2\pi i/\ell}$ be a primitive ℓ^{th} root of unity.
Define the ring
$$\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \dots + a_{\ell-1}\zeta^{\ell-1} \mid a_0, \dots, a_{\ell-1} \in \mathbb{Z}\}.$$
- ▶ $\mathbb{Z}[\zeta]$ does **not** admit unique factorisation, but it does admit *unique factorisation of ideals*.
Every ideal $I \subset \mathbb{Z}[\zeta]$ factorises uniquely as a product of *prime ideals*.
- ▶ How does (p) factorise in $\mathbb{Z}[\zeta]$?
 $(p) = \mathfrak{P}_1 \mathfrak{P}_2 \dots \mathfrak{P}_g.$

Jacobi Sums

Jacobi Sums

- ▶ We obtain the prime ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ from *Jacobi sums*.

Jacobi Sums

- ▶ We obtain the prime ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ from *Jacobi sums*.
- ▶ Each Jacobi sum J satisfies

$$(J) = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}.$$

Jacobi Sums

- ▶ We obtain the prime ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ from *Jacobi sums*.
- ▶ Each Jacobi sum J satisfies

$$(J) = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}.$$

- ▶ Can we isolate each \mathfrak{P}_i by some GCD calculation of Jacobi sums?

Jacobi Sums

- ▶ We obtain the prime ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ from *Jacobi sums*.
- ▶ Each Jacobi sum J satisfies

$$(J) = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}.$$

- ▶ Can we isolate each \mathfrak{P}_i by some GCD calculation of Jacobi sums?
- ▶ We can get our hands on all the Jacobi sums in deterministic polynomial time (using Pila's generalisation of Schoof's algorithm and LLL).

Example 1

$$\ell = 7, p = 23$$

$p^3 \equiv 1 \pmod{\ell}$, so $f = 3$ and $g = 2$.

Example 1

$$\ell = 7, p = 23$$

$p^3 \equiv 1 \pmod{\ell}$, so $f = 3$ and $g = 2$.

a, b	1	2	3	4	5	6
1	$\mathfrak{P}_1 \mathfrak{P}_2^2$	\mathfrak{P}_2^3	$\mathfrak{P}_1^2 \mathfrak{P}_2$	\mathfrak{P}_2^3	$\mathfrak{P}_1 \mathfrak{P}_2^2$	
2	\mathfrak{P}_2^3	$\mathfrak{P}_1 \mathfrak{P}_2^2$	$\mathfrak{P}_1 \mathfrak{P}_2^2$	\mathfrak{P}_2^3		$\mathfrak{P}_1^2 \mathfrak{P}_2$
3	$\mathfrak{P}_1^2 \mathfrak{P}_2$	$\mathfrak{P}_1 \mathfrak{P}_2^2$	$\mathfrak{P}_1^2 \mathfrak{P}_2$		\mathfrak{P}_1^3	\mathfrak{P}_1^3
4	\mathfrak{P}_2^3	\mathfrak{P}_2^3		$\mathfrak{P}_1 \mathfrak{P}_2^2$	$\mathfrak{P}_1^2 \mathfrak{P}_2$	$\mathfrak{P}_1 \mathfrak{P}_2^2$
5	$\mathfrak{P}_1 \mathfrak{P}_2^2$		\mathfrak{P}_1^3	$\mathfrak{P}_1^2 \mathfrak{P}_2$	$\mathfrak{P}_1^2 \mathfrak{P}_2$	\mathfrak{P}_1^3
6		$\mathfrak{P}_1^2 \mathfrak{P}_2$	\mathfrak{P}_1^3	$\mathfrak{P}_1 \mathfrak{P}_2^2$	\mathfrak{P}_1^3	$\mathfrak{P}_1^2 \mathfrak{P}_2$

Example 1

$$\ell = 7, p = 23$$

$p^3 \equiv 1 \pmod{\ell}$, so $f = 3$ and $g = 2$.

a, b	1	2	3	4	5	6
1	$\mathfrak{P}_1 \mathfrak{P}_2^2$	\mathfrak{P}_2^3	$\mathfrak{P}_1^2 \mathfrak{P}_2$	\mathfrak{P}_2^3	$\mathfrak{P}_1 \mathfrak{P}_2^2$	
2	\mathfrak{P}_2^3	$\mathfrak{P}_1 \mathfrak{P}_2^2$	$\mathfrak{P}_1 \mathfrak{P}_2^2$	\mathfrak{P}_2^3		$\mathfrak{P}_1^2 \mathfrak{P}_2$
3	$\mathfrak{P}_1^2 \mathfrak{P}_2$	$\mathfrak{P}_1 \mathfrak{P}_2^2$	$\mathfrak{P}_1^2 \mathfrak{P}_2$		\mathfrak{P}_1^3	\mathfrak{P}_1^3
4	\mathfrak{P}_2^3	\mathfrak{P}_2^3		$\mathfrak{P}_1 \mathfrak{P}_2^2$	$\mathfrak{P}_1^2 \mathfrak{P}_2$	$\mathfrak{P}_1 \mathfrak{P}_2^2$
5	$\mathfrak{P}_1 \mathfrak{P}_2^2$		\mathfrak{P}_1^3	$\mathfrak{P}_1^2 \mathfrak{P}_2$	$\mathfrak{P}_1^2 \mathfrak{P}_2$	\mathfrak{P}_1^3
6		$\mathfrak{P}_1^2 \mathfrak{P}_2$	\mathfrak{P}_1^3	$\mathfrak{P}_1 \mathfrak{P}_2^2$	\mathfrak{P}_1^3	$\mathfrak{P}_1^2 \mathfrak{P}_2$

$$\gcd(\mathfrak{P}_1^3, \mathfrak{P}_1 \mathfrak{P}_2^2) = \mathfrak{P}_1.$$

Example 2

$$\ell = 7, p = 13$$

$p^2 \equiv 1 \pmod{\ell}$, so $f = 2$ and $g = 3$.

Example 2

$$\ell = 7, p = 13$$

$p^2 \equiv 1 \pmod{\ell}$, so $f = 2$ and $g = 3$.

a, b	1	2	3	4	5	6
1	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	
2	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$		$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$
3	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$		$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$
4	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$		$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$
5	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$		$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$
6		$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$

Example 2

$$\ell = 7, p = 13$$

$p^2 \equiv 1 \pmod{\ell}$, so $f = 2$ and $g = 3$.

a, b	1	2	3	4	5	6
1	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	
2	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$		$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$
3	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$		$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$
4	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$		$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$
5	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$		$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$
6		$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$	$\mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$

There is **no way** to get the prime ideals via a GCD calculation.

Results

Results

- ▶ When f is even, each Jacobi sum J factorises as

$$(J) = \mathfrak{P}_1^{f/2} \dots \mathfrak{P}_g^{f/2}.$$

Results

- ▶ When f is even, each Jacobi sum J factorises as

$$(J) = \mathfrak{P}_1^{f/2} \dots \mathfrak{P}_g^{f/2}.$$

Thus the method fails.

Results

- ▶ When f is even, each Jacobi sum J factorises as

$$(J) = \mathfrak{P}_1^{f/2} \dots \mathfrak{P}_g^{f/2}.$$

Thus the method fails.

- ▶ When f is odd, the method always works!

Future Directions

Future Directions

- ▶ Find a similar method which works for f even?

Future Directions

- ▶ Find a similar method which works for f even?
- ▶ Factorise the n^{th} cyclotomic polynomial, where n is any integer?

Future Directions

- ▶ Find a similar method which works for f even?
- ▶ Factorise the n^{th} cyclotomic polynomial, where n is any integer?
- ▶ Factorise ψ over \mathbb{F}_q , where q is any prime power?

Future Directions

- ▶ Find a similar method which works for f even?
- ▶ Factorise the n^{th} cyclotomic polynomial, where n is any integer?
- ▶ Factorise ψ over \mathbb{F}_q , where q is any prime power?
- ▶ What other polynomials can be factored using a similar method?