Primes of the Form $x^2 + ny^2$

With an introduction to class field theory

Andrew J. Kobin

ak5ah@virginia.edu

October 2, 2015

Master's thesis work with Dr. Frank Moore
at Wake Forest University

Introduction

Introduction

For the first half of the talk, three main ideas:

Introduction

For the first half of the talk, three main ideas:

- Dirichlet's Theorem

Introduction

For the first half of the talk, three main ideas:

- Dirichlet's Theorem
- Polynomial factorization

Introduction

For the first half of the talk, three main ideas:

- Dirichlet's Theorem
- Polynomial factorization
  - Galois Theory

Introduction

For the first half of the talk, three main ideas:

- Dirichlet's Theorem
- Polynomial factorization
  - Galois Theory
- Density Theorems

Introduction

For the second half of the talk:

Introduction

For the second half of the talk:

- Class field theory

Introduction

For the second half of the talk:

- Class field theory
- Primes of the form $x^2 + ny^2$

Introduction

For the second half of the talk:

- Class field theory
- Primes of the form $x^2 + ny^2$
- Symmetric n-Fermat primes

Introduction

Question to think about:

Introduction

Question to think about:

For a given $n \in \mathbb{N}$, when is $x^2 + ny^2$ prime? And when is $y^2 + nx^2$ also prime?

Dirichlet's Theorem

Recall:

Dirichlet's Theorem

Recall:

Theorem (Dirichlet)

For every pair of relatively prime integers a and m, there are infinitely many primes of the form $km + a$.

Dirichlet's Theorem

Recall:

Theorem (Dirichlet)

For every pair of relatively prime integers a and m, there are infinitely many primes of the form $km + a$.

In other words, the set

$$S = \{p \text{ prime} \mid p \equiv a \pmod{m}\}$$

is infinite.

Another view of Dirichlet's Theorem

Another view of Dirichlet's Theorem

Definition

A set S of prime numbers has **Dirichlet density** δ if

Another view of Dirichlet's Theorem

Definition

A set S of prime numbers has **Dirichlet density** δ if

$$\sum_{p \in S} \frac{1}{p^s} \sim -\delta \log(s-1).$$

Another view of Dirichlet's Theorem

Definition

A set S of prime numbers has **Dirichlet density** δ if

$$\sum_{p \in S} \frac{1}{p^s} \sim -\delta \log(s-1).$$

This is equal to the *natural density*

$$\lim_{x \to \infty} \frac{\#\{p \in S : p \leq x\}}{\#\{p \text{ prime} : p \leq x\}}$$

if both exist*.

Another view of Dirichlet's Theorem

Definition

A set S of prime numbers has **Dirichlet density** δ if

$$\sum_{p \in S} \frac{1}{p^s} \sim -\delta \log(s-1).$$

This is equal to the *natural density*

$$\lim_{x \to \infty} \frac{\#\{p \in S : p \leq x\}}{\#\{p \text{ prime} : p \leq x\}}$$

if both exist*.

*If S has a natural density, then $\delta(S)$ exists. The converse is false.

Another view of Dirichlet's Theorem

Definition

A set S of prime numbers has **Dirichlet density** δ if

$$\sum_{p \in S} \frac{1}{p^s} \sim -\delta \log(s-1).$$

Fact: If $\delta(S) > 0$ then S is an infinite set.

Another view of Dirichlet's Theorem

Dirichlet's Theorem (1837)

Let a and m be positive integers so that $\gcd(a, m) = 1$. Then the set

$$S = \{p \text{ prime} \mid p \equiv a \pmod m\}$$

has density $\delta(S) = \frac{1}{\phi(m)}$ and in particular S is infinite.

Another view of Dirichlet's Theorem

Dirichlet's Theorem (1837)

Let a and m be positive integers so that $\gcd(a, m) = 1$. Then the set

$$S = \{p \text{ prime} \mid p \equiv a \pmod{m}\}$$

has density $\delta(S) = \frac{1}{\phi(m)}$ and in particular S is infinite.

- Dirichlet originally proved this using L-series.

Another view of Dirichlet's Theorem

Dirichlet's Theorem (1837)

Let a and m be positive integers so that $\gcd(a, m) = 1$. Then the set

$$S = \{p \text{ prime} \mid p \equiv a \pmod{m}\}$$

has density $\delta(S) = \frac{1}{\phi(m)}$ and in particular S is infinite.

- Dirichlet originally proved this using L-series.
- We will use the Čebotarev density theorem.

Polynomial Factorization

Switching gears...

Polynomial Factorization

Question

Given a polynomial $f(x)$ with integer coefficients, how does f factor modulo different primes p?

Question

How does f factor mod p?

Example

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

Some decomposition patterns of f mod p for different primes:

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

Some decomposition patterns of f mod p for different primes:

- $f \equiv (x^3 + 3x^2 + 2x + 5)(x + 4) \pmod 7$

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

Some decomposition patterns of f mod p for different primes:

- $f \equiv (x^3 + 3x^2 + 2x + 5)(x + 4) \pmod 7$ (3,1)

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

Some decomposition patterns of f mod p for different primes:

- $f \equiv (x^3 + 3x^2 + 2x + 5)(x + 4) \pmod 7$ (3,1)
- $f \equiv x^4 - x - 1 \pmod{47}$

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

Some decomposition patterns of f mod p for different primes:

- $f \equiv (x^3 + 3x^2 + 2x + 5)(x + 4) \pmod 7$ (3,1)
- $f \equiv x^4 - x - 1 \pmod{47}$ (4)

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

Some decomposition patterns of f mod p for different primes:

- $f \equiv (x^3 + 3x^2 + 2x + 5)(x + 4) \pmod 7$ (3,1)
- $f \equiv x^4 - x - 1 \pmod{47}$ (4)
- $f \equiv (x^2 + 34x + 24)(x^2 + 67x + 21) \pmod{101}$

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

Some decomposition patterns of f mod p for different primes:

- $f \equiv (x^3 + 3x^2 + 2x + 5)(x + 4) \pmod{7}$ (3,1)
- $f \equiv x^4 - x - 1 \pmod{47}$ (4)
- $f \equiv (x^2 + 34x + 24)(x^2 + 67x + 21) \pmod{101}$ (2,2)

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

Some decomposition patterns of f mod p for different primes:

- $f \equiv (x^3 + 3x^2 + 2x + 5)(x + 4) \pmod 7$ (3,1)
- $\boxed{f \equiv x^4 - x - 1 \pmod{47} \quad (4)}$
- $f \equiv (x^2 + 34x + 24)(x^2 + 67x + 21) \pmod{101}$ (2,2)

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$. $\quad \ldots f$ is irreducible!

Some decomposition patterns of f mod p for different primes:

- $f \equiv (x^3 + 3x^2 + 2x + 5)(x + 4) \pmod 7$ (3,1)
- $\boxed{f \equiv x^4 - x - 1 \pmod{47}}$ (4)
- $f \equiv (x^2 + 34x + 24)(x^2 + 67x + 21) \pmod{101}$ (2,2)

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

f factors into the partitions of $n = 4$ with the following frequencies:

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

f factors into the partitions of $n = 4$ with the following frequencies:

decomposition	proportion of primes
4	

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

f factors into the partitions of $n = 4$ with the following frequencies:

decomposition	proportion of primes
4	1/4

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

f factors into the partitions of $n = 4$ with the following frequencies:

decomposition	proportion of primes
4	1/4
3,1	

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

f factors into the partitions of $n = 4$ with the following frequencies:

decomposition	proportion of primes
4	1/4
3,1	1/3

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

f factors into the partitions of $n = 4$ with the following frequencies:

decomposition	proportion of primes
4	1/4
3,1	1/3
2,2	

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

f factors into the partitions of $n = 4$ with the following frequencies:

decomposition	proportion of primes
4	1/4
3,1	1/3
2,2	1/8

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

f factors into the partitions of $n = 4$ with the following frequencies:

decomposition	proportion of primes
4	1/4
3,1	1/3
2,2	1/8
2,1,1	

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

f factors into the partitions of $n = 4$ with the following frequencies:

decomposition	proportion of primes
4	1/4
3,1	1/3
2,2	1/8
2,1,1	1/4

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

f factors into the partitions of $n = 4$ with the following frequencies:

decomposition	proportion of primes
4	1/4
3,1	1/3
2,2	1/8
2,1,1	1/4
1,1,1,1	

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

f factors into the partitions of $n = 4$ with the following frequencies:

decomposition	proportion of primes
4	1/4
3,1	1/3
2,2	1/8
2,1,1	1/4
1,1,1,1	1/24

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

Recall:

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

Recall:

- $f \equiv (x^3 + 3x^2 + 2x + 5)(x + 4) \pmod{7}$ (3,1)
- $f \equiv x^4 - x - 1 \pmod{47}$ (4)
- $f \equiv (x^2 + 34x + 24)(x^2 + 67x + 21) \pmod{101}$ (2,2)

Question

How does f factor mod p?

Example

Let $f(x) = x^4 - x - 1$.

Recall:

- $f \equiv (x^3 + 3x^2 + 2x + 5)(x + 4) \pmod 7$ (3,1)
- $f \equiv x^4 - x - 1 \pmod{47}$ (4)
- $f \equiv (x^2 + 34x + 24)(x^2 + 67x + 21) \pmod{101}$ (2,2)

There's a group acting on the roots of f ...

Galois Theory

Switching gears again...

Galois Theory

- Let $f(x)$ be an irreducible polynomial with coefficients in $\mathbb{Z}$.

Galois Theory

- Let $f(x)$ be an irreducible polynomial with coefficients in $\mathbb{Z}$.
- Let $\{\alpha_1, \ldots, \alpha_n\}$ be the distinct complex roots of f.

Galois Theory

- Let $f(x)$ be an irreducible polynomial with coefficients in $\mathbb{Z}$.
- Let $\{\alpha_1, \ldots, \alpha_n\}$ be the distinct complex roots of f.
- There is a group $\mathrm{Gal}(f)$ called the *Galois group of* f that acts on f by permuting the α_i in some fashion.

Galois Theory

- Let $f(x)$ be an irreducible polynomial with coefficients in $\mathbb{Z}$.
- Let $\{\alpha_1, \ldots, \alpha_n\}$ be the distinct complex roots of f.
- There is a group $\mathrm{Gal}(f)$ called the *Galois group of f* that acts on f by permuting the α_i in some fashion.

This is best understood in the context of field extensions.

Galois Theory

Galois Theory

Definition

If K is a field, a **field extension** of K is a field L containing K.

Galois Theory

Definition

If K is a field, a **field extension** of K is a field L containing K. This is denoted L/K.

Galois Theory

Definition

If K is a field, a **field extension** of K is a field L containing K. This is denoted L/K.

Definition

The **Galois group** $\mathrm{Gal}(L/K)$ is the group of automorphisms of L that fix K. *****

Galois Theory

Definition

If K is a field, a **field extension** of K is a field L containing K. This is denoted L/K.

Definition

The **Galois group** $\mathrm{Gal}(L/K)$ is the group of automorphisms of L that fix K. *****

Galois Theory

Galois Theory

Definition

Let $f(x) \in \mathbb{Z}[x]$.

Galois Theory

Definition

Let $f(x) \in \mathbb{Z}[x]$. A **splitting field** for f is a field extension $K/\mathbb{Q}$ such that f can be written as a product of linear factors in $K[x]$:

Galois Theory

Definition

Let $f(x) \in \mathbb{Z}[x]$. A **splitting field** for f is a field extension $K/\mathbb{Q}$ such that f can be written as a product of linear factors in $K[x]$:

$$f(x) = \prod (x - \beta_i), \quad \beta_i \in K.$$

Galois Theory

Definition

Let $f(x) \in \mathbb{Z}[x]$. A **splitting field** for f is a field extension $K/\mathbb{Q}$ such that f can be written as a product of linear factors in $K[x]$:

$$f(x) = \prod (x - \beta_i), \quad \beta_i \in K.$$

Definition

The **Galois group of a polynomial** $f(x) \in \mathbb{Z}[x]$ is $\mathrm{Gal}(K/\mathbb{Q})$ where K is a splitting field for f.

Galois Theory

Galois Theory

Congratulations!

Galois Theory

Congratulations!

Back to polynomials

- Recall the question: how does $f(x)$ factor mod p?

- Recall the question: how does $f(x)$ factor mod p?
- $f(x) \equiv f_1(x)f_2(x)\cdots f_r(x) \pmod{p}$ where $f_i \in \mathbb{Z}[x]$ are distinct, irreducible.

- Recall the question: how does $f(x)$ factor mod p?
- $f(x) \equiv f_1(x)f_2(x)\cdots f_r(x) \pmod{p}$ where $f_i \in \mathbb{Z}[x]$ are distinct, irreducible.
- Let $d_i = \deg f_i$ for each i.

- Recall the question: how does $f(x)$ factor mod p?
- $f(x) \equiv f_1(x)f_2(x)\cdots f_r(x) \pmod{p}$ where $f_i \in \mathbb{Z}[x]$ are distinct, irreducible.
- Let $d_i = \deg f_i$ for each i.
- We say f has decomposition type $(d_1, d_2, \ldots, d_r)$ mod p.

- Recall the question: how does $f(x)$ factor mod p?
- $f(x) \equiv f_1(x) f_2(x) \cdots f_r(x) \pmod{p}$ where $f_i \in \mathbb{Z}[x]$ are distinct, irreducible.
- Let $d_i = \deg f_i$ for each i.
- We say f has decomposition type $(d_1, d_2, \ldots, d_r)$ mod p.

- Recall the question: how does $f(x)$ factor mod p?
- $f(x) \equiv f_1(x)f_2(x)\cdots f_r(x) \pmod{p}$ where $f_i \in \mathbb{Z}[x]$ are distinct, irreducible.
- Let $d_i = \deg f_i$ for each i.
- We say f has decomposition type $(d_1, d_2, \ldots, d_r)$ mod p.

Question

For a given prime p, is there a permutation $\sigma_p \in \mathrm{Gal}(f)$ that has the same cycle type as f's decomposition mod p?

- Recall the question: how does $f(x)$ factor mod p?
- $f(x) \equiv f_1(x) f_2(x) \cdots f_r(x) \pmod{p}$ where $f_i \in \mathbb{Z}[x]$ are distinct, irreducible.
- Let $d_i = \deg f_i$ for each i.
- We say f has decomposition type $(d_1, d_2, \ldots, d_r)$ mod p.

Question

For a given prime p, is there a permutation $\sigma_p \in \mathrm{Gal}(f)$ that has the same cycle type as f's decomposition mod p?

Definition

If $\sigma \in \mathrm{Gal}(f)$ has the same cycle type as the decomposition of f mod p, σ is called a **Frobenius element** of p.

Question

For a given prime p, can we find a permutation $\sigma \in \mathrm{Gal}(f)$ that has the same cycle type as f's decomposition mod p?

Example (Stevenhagen, Lenstra)

Consider $f(x) = x^m - 1$ and a prime $p \nmid m$.

Question

For a given prime p, can we find a permutation $\sigma \in \mathrm{Gal}(f)$ that has the same cycle type as f's decomposition mod p?

Example (Stevenhagen, Lenstra)

Consider $f(x) = x^m - 1$ and a prime $p \nmid m$. For $m = 12$, the primes and decomposition types look like:

Question

For a given prime p, can we find a permutation $\sigma \in \mathrm{Gal}(f)$ that has the same cycle type as f's decomposition mod p?

Example (Stevenhagen, Lenstra)

Consider $f(x) = x^m - 1$ and a prime $p \nmid m$. For $m = 12$, the primes and decomposition types look like:

- $p \equiv 1 \pmod{12} \longleftrightarrow$ (1,1,1,1,1,1,1,1,1,1,1,1)
- $p \equiv 5 \pmod{12} \longleftrightarrow$ (1,1,1,1,2,2,2,2)
- $p \equiv 7 \pmod{12} \longleftrightarrow$ (1,1,1,1,1,1,2,2,2)
- $p \equiv 11 \pmod{12} \longleftrightarrow$ (1,1,2,2,2,2,2)

Question

For a given prime p, can we find a permutation $\sigma \in \mathrm{Gal}(f)$ that has the same cycle type as f's decomposition mod p?

Example (Stevenhagen, Lenstra)

Consider $f(x) = x^m - 1$ and a prime $p \nmid m$. For $m = 12$, the primes and decomposition types look like:

- $p \equiv 1 \pmod{12} \longleftrightarrow$ (1,1,1,1,1,1,1,1,1,1,1,1)
- $p \equiv 5 \pmod{12} \longleftrightarrow$ (1,1,1,1,2,2,2,2)
- $p \equiv 7 \pmod{12} \longleftrightarrow$ (1,1,1,1,1,1,2,2,2)
- $p \equiv 11 \pmod{12} \longleftrightarrow$ (1,1,2,2,2,2,2)

So according to Dirichlet's Theorem, there are infinitely many primes corresponding to each cycle type.

Frobenius' Density Theorem

Frobenius' Density Theorem

Theorem (Frobenius)

Let $f \in \mathbb{Z}[x]$ with Galois group $G = \mathrm{Gal}(f)$.

Frobenius' Density Theorem

Theorem (Frobenius)

Let $f \in \mathbb{Z}[x]$ with Galois group $G = \mathrm{Gal}(f)$. Suppose S is the set of primes p that have Frobenius elements $\mathrm{Frob}(p)$ of some given cycle type r.

Frobenius' Density Theorem

Theorem (Frobenius)

Let $f \in \mathbb{Z}[x]$ with Galois group $G = \mathrm{Gal}(f)$. Suppose S is the set of primes p that have Frobenius elements $\mathrm{Frob}(p)$ of some given cycle type r. Then the Dirichlet density of S is

$$\delta(S) = \frac{T}{|G|}$$

where $T = \#\{\sigma \in G : \sigma \text{ has cycle type } r\}$.

Frobenius' Density Theorem

Theorem (Frobenius)

Let $f \in \mathbb{Z}[x]$ *with Galois group* $G = \mathrm{Gal}(f)$. *Suppose* S *is the set of primes* p *that have Frobenius elements* $\mathrm{Frob}(p)$ *of some given cycle type* r. *Then the Dirichlet density of* S *is*

$$\delta(S) = \frac{T}{|G|}$$

where $T = \#\{\sigma \in G : \sigma \text{ has cycle type } r\}$.

So if there exists a permutation $\sigma \in G$ with a given cycle type, then f has that particular decomposition mod p for *infinitely many primes* p.

Questions you should be asking:

Questions you should be asking:

- Can this be generalized?

Questions you should be asking:

- Can this be generalized?
- i.e. is there a canonical choice of σ for each prime?

Questions you should be asking:

- Can this be generalized?
- i.e. is there a canonical choice of σ for each prime?
- Why in the world should I care?

Čebotarev's Density Theorem

Theorem (Čebotarev)

Let $f \in \mathbb{Z}[x]$ *with Galois group* $G = \mathrm{Gal}(f)$*.*

Čebotarev's Density Theorem

Theorem (Čebotarev)

Let $f \in \mathbb{Z}[x]$ *with Galois group* $G = \mathrm{Gal}(f)$*. Take an element* $\sigma \in G$ *and denote its conjugacy class by* C*.*

Čebotarev's Density Theorem

Theorem (Čebotarev)

Let $f \in \mathbb{Z}[x]$ with Galois group $G = \mathrm{Gal}(f)$. Take an element $\sigma \in G$ and denote its conjugacy class by C. Then the set S of all primes p such that $\mathrm{Frob}(p) \in C$ has density

$$\delta(S) = \frac{|C|}{|G|}.$$

Čebotarev's Density Theorem

Theorem (Čebotarev)

Let $f \in \mathbb{Z}[x]$ with Galois group $G = \mathrm{Gal}(f)$. Take an element $\sigma \in G$ and denote its conjugacy class by C. Then the set S of all primes p such that $\mathrm{Frob}(p) \in C$ has density

$$\delta(S) = \frac{|C|}{|G|}.$$

This is pretty much the best we could hope for.

Čebotarev's Density Theorem

Theorem (Čebotarev)

Let $f \in \mathbb{Z}[x]$ with Galois group $G = \mathrm{Gal}(f)$. Take an element $\sigma \in G$ and denote its conjugacy class by C. Then the set S of all primes p such that $\mathrm{Frob}(p) \in C$ has density

$$\delta(S) = \frac{|C|}{|G|}.$$

This is pretty much the best we could hope for.

Notice that when G is abelian, this says each prime has a *unique Frobenius element* in G.

Consequences

Consequences

Corollary

Given a field extension $K/\mathbb{Q}$ whose Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, fix an element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Then the set S of primes p such that $\mathrm{Frob}(p) = \sigma$ has density

$$\delta(S) = \frac{1}{|G|}$$

and in particular G is infinite.

Consequences

Corollary

Given a field extension $K/\mathbb{Q}$ whose Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, fix an element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Then the set S of primes p such that $\mathrm{Frob}(p) = \sigma$ has density

$$\delta(S) = \frac{1}{|G|}$$

and in particular G is infinite.

Corollary

For a polynomial $f(x) \in \mathbb{Z}[x]$, there are infinitely many primes p such that f splits completely into a product of linear factors mod p.

Consequences

Example

Let
$f(x) = x^9 + 3x^8 - 18x^7 - 38x^6 + 93x^5 + 147x^4 - 161x^3 - 201x^2 + 57x + 53.$

Consequences

Example

Let
$f(x) = x^9 + 3x^8 - 18x^7 - 38x^6 + 93x^5 + 147x^4 - 161x^3 - 201x^2 + 57x + 53$.

Oh god, why??

Consequences

Example

Let
$f(x) = x^9 + 3x^8 - 18x^7 - 38x^6 + 93x^5 + 147x^4 - 161x^3 - 201x^2 + 57x + 53$.

Oh god, why??

Well, it turns out that $\mathrm{Gal}(f) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Consequences

Example

Let
$f(x) = x^9 + 3x^8 - 18x^7 - 38x^6 + 93x^5 + 147x^4 - 161x^3 - 201x^2 + 57x + 53$.

Oh god, why??

Well, it turns out that $\mathrm{Gal}(f) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

You didn't answer my question...

Consequences

Example

Let
$f(x) = x^9 + 3x^8 - 18x^7 - 38x^6 + 93x^5 + 147x^4 - 161x^3 - 201x^2 + 57x + 53$.

Oh god, why??

Well, it turns out that $\mathrm{Gal}(f) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

You didn't answer my question...

I'll tell you! If you want to know *how* this polynomial corresponds to the group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, ask me later.

Consequences

Example

Let
$f(x) = x^9 + 3x^8 - 18x^7 - 38x^6 + 93x^5 + 147x^4 - 161x^3 - 201x^2 + 57x + 53.$

Consequences

Example

Let
$f(x) = x^9 + 3x^8 - 18x^7 - 38x^6 + 93x^5 + 147x^4 - 161x^3 - 201x^2 + 57x + 53.$

$G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ has:

- Nine conjugacy classes (it's abelian!)
- Five divisions*
- Two cycle types

Consequences

Example

Let
$f(x) = x^9 + 3x^8 - 18x^7 - 38x^6 + 93x^5 + 147x^4 - 161x^3 - 201x^2 + 57x + 53$.

$G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ has:

- Nine conjugacy classes (it's abelian!)
- Five divisions*
- Two cycle types

So it's useful to illustrate the difference between Frobenius' density theorem and Čebotarev's density theorem.

Consequences

Example

Let
$f(x) = x^9 + 3x^8 - 18x^7 - 38x^6 + 93x^5 + 147x^4 - 161x^3 - 201x^2 + 57x + 53.$

Consequences

Example

Let
$f(x) = x^9 + 3x^8 - 18x^7 - 38x^6 + 93x^5 + 147x^4 - 161x^3 - 201x^2 + 57x + 53$.

The distribution of primes among the cycle types:

(1)	1/9
(3,3,3)	8/9

Consequences

Example

Let
$f(x) = x^9 + 3x^8 - 18x^7 - 38x^6 + 93x^5 + 147x^4 - 161x^3 - 201x^2 + 57x + 53$.

The distribution of primes among the divisions:

D_1	1/9
D_2	2/9
D_3	2/9
D_4	2/9
D_5	2/9

Consequences

Example

Let
$f(x) = x^9 + 3x^8 - 18x^7 - 38x^6 + 93x^5 + 147x^4 - 161x^3 - 201x^2 + 57x + 53$.

The distribution of primes among the conjugacy classes:

id	1/9
σ_1	1/9
σ_2	1/9
σ_3	1/9
σ_4	1/9
σ_5	1/9
σ_6	1/9
σ_7	1/9
σ_8	1/9

Consequences

Example

Let $K = \mathbb{Q}(i)$. (These are all complex numbers of the form $a + bi$, where $a, b \in \mathbb{Q}$.) The ring of integers for K is called the *Gaussian integers*, $\mathbb{Z}[i]$.

Consequences

Example

Let $K = \mathbb{Q}(i)$. (These are all complex numbers of the form $a + bi$, where $a, b \in \mathbb{Q}$.) The ring of integers for K is called the *Gaussian integers*, $\mathbb{Z}[i]$. Here $[K : \mathbb{Q}] = 2$ so $|\operatorname{Gal}(K/\mathbb{Q})| = 2$ and consequently $K/\mathbb{Q}$ is abelian. So $\operatorname{Frob}(p)$ is unique for each prime p.

Consequences

Example

Let $K = \mathbb{Q}(i)$. (These are all complex numbers of the form $a + bi$, where $a, b \in \mathbb{Q}$.) The ring of integers for K is called the *Gaussian integers*, $\mathbb{Z}[i]$. Here $[K : \mathbb{Q}] = 2$ so $|\operatorname{Gal}(K/\mathbb{Q})| = 2$ and consequently $K/\mathbb{Q}$ is abelian. So $\operatorname{Frob}(p)$ is unique for each prime p. By studying the residue fields of the extension, $\ell = \mathbb{Z}[i]/p\mathbb{Z}[i] = \mathbb{F}_{p^2}$ and $k = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, we can prove that

$$\operatorname{Frob}(p) = \begin{cases} \tau & \text{if } p \equiv 3 \pmod 4 \\ 1 & \text{if } p \equiv 1 \pmod 4, \end{cases}$$

where $\tau \in \operatorname{Gal}(K/\mathbb{Q})$ is complex conjugation.

Consequences

Example

This is part of a more extensive classification of primes in the extension $\mathbb{Q}(i)/\mathbb{Q}$. For a prime $p \in \mathbb{Z}$, the following are equivalent:

(a) $p \equiv 1 \pmod{4}$.

(b) (p) splits completely in $\mathbb{Z}[i]$.

(c) -1 is a quadratic residue mod p.

(d) $\mathrm{Frob}(p) = 1$ in $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$.

(e) (Fermat) $p = x^2 + y^2$ for some integers x and y.

Consequences

Example

This is part of a more extensive classification of primes in the extension $\mathbb{Q}(i)/\mathbb{Q}$. For a prime $p \in \mathbb{Z}$, the following are equivalent:

(a) $p \equiv 1 \pmod 4$.

(b) (p) splits completely in $\mathbb{Z}[i]$.

(c) -1 is a quadratic residue mod p.

(d) $\mathrm{Frob}(p) = 1$ in $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$.

(e) (Fermat) $p = x^2 + y^2$ for some integers x and y.

In fact, (c) is part of Gauss's theory of quadratic reciprocity. The Frobenius element is a direct generalization of the Legendre symbol $\left(\frac{\cdot}{p}\right)$ and consequently we sometimes write $\mathrm{Frob}(p) = \left(\frac{K/\mathbb{Q}}{p}\right)$.

Consequences

We can prove Dirichlet's Theorem using Čebotarev's density theorem.

Consequences

We can prove Dirichlet's Theorem using Čebotarev's density theorem.

Proof.

- Consider $f(x) = x^m - 1$ again.

Consequences

We can prove Dirichlet's Theorem using Čebotarev's density theorem.

Proof.

- Consider $f(x) = x^m - 1$ again.
- A splitting field for f is $K = \mathbb{Q}(\zeta_m)$ where $\zeta_m = e^{2\pi i/m}$, a primitive mth root of unity.

Consequences

We can prove Dirichlet's Theorem using Čebotarev's density theorem.

Proof.

- Consider $f(x) = x^m - 1$ again.
- A splitting field for f is $K = \mathbb{Q}(\zeta_m)$ where $\zeta_m = e^{2\pi i/m}$, a primitive mth root of unity.
- There is a canonical isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

Consequences

We can prove Dirichlet's Theorem using Čebotarev's density theorem.

Proof.

- Consider $f(x) = x^m - 1$ again.
- A splitting field for f is $K = \mathbb{Q}(\zeta_m)$ where $\zeta_m = e^{2\pi i/m}$, a primitive mth root of unity.
- There is a canonical isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.
- Notice: $|\,\mathrm{Gal}(K/\mathbb{Q})| = \phi(m)$.

Consequences

We can prove Dirichlet's Theorem using Čebotarev's density theorem.

Proof.

- Consider $f(x) = x^m - 1$ again.
- A splitting field for f is $K = \mathbb{Q}(\zeta_m)$ where $\zeta_m = e^{2\pi i/m}$, a primitive mth root of unity.
- There is a canonical isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.
- Notice: $|\,\mathrm{Gal}(K/\mathbb{Q})| = \phi(m)$.
- Under the isomorphism, $(\zeta_m \mapsto \zeta_m^a) \longleftrightarrow a \pmod{m}$.

Consequences

We can prove Dirichlet's Theorem using Čebotarev's density theorem.

Proof.

- Consider $f(x) = x^m - 1$ again.
- A splitting field for f is $K = \mathbb{Q}(\zeta_m)$ where $\zeta_m = e^{2\pi i/m}$, a primitive mth root of unity.
- There is a canonical isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.
- Notice: $|\,\mathrm{Gal}(K/\mathbb{Q})| = \phi(m)$.
- Under the isomorphism, $(\zeta_m \mapsto \zeta_m^a) \longleftrightarrow a \pmod{m}$.
- For a prime p, $\mathrm{Frob}(p) = (\zeta_m \mapsto \zeta_m^p)$.

Consequences

We can prove Dirichlet's Theorem using Čebotarev's density theorem.

Proof.

- Consider $f(x) = x^m - 1$ again.
- A splitting field for f is $K = \mathbb{Q}(\zeta_m)$ where $\zeta_m = e^{2\pi i/m}$, a primitive mth root of unity.
- There is a canonical isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.
- Notice: $|\,\mathrm{Gal}(K/\mathbb{Q})| = \phi(m)$.
- Under the isomorphism, $(\zeta_m \mapsto \zeta_m^a) \longleftrightarrow a \pmod{m}$.
- For a prime p, $\mathrm{Frob}(p) = (\zeta_m \mapsto \zeta_m^p)$.
- By Čebotarev, the set of primes p for which $\mathrm{Frob}(p) = \sigma$ is infinite for each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Consequences

We can prove Dirichlet's Theorem using Čebotarev's density theorem.

Proof.

- Consider $f(x) = x^m - 1$ again.
- A splitting field for f is $K = \mathbb{Q}(\zeta_m)$ where $\zeta_m = e^{2\pi i/m}$, a primitive mth root of unity.
- There is a canonical isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.
- Notice: $|\,\mathrm{Gal}(K/\mathbb{Q})| = \phi(m)$.
- Under the isomorphism, $(\zeta_m \mapsto \zeta_m^a) \longleftrightarrow a \pmod{m}$.
- For a prime p, $\mathrm{Frob}(p) = (\zeta_m \mapsto \zeta_m^p)$.
- By Čebotarev, the set of primes p for which $\mathrm{Frob}(p) = \sigma$ is infinite for each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.
- Therefore there are infinitely many primes $p \equiv a \pmod{m}$.

Consequences

We can prove Dirichlet's Theorem using Čebotarev's density theorem.

Proof.

- Consider $f(x) = x^m - 1$ again.
- A splitting field for f is $K = \mathbb{Q}(\zeta_m)$ where $\zeta_m = e^{2\pi i/m}$, a primitive mth root of unity.
- There is a canonical isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.
- Notice: $|\,\mathrm{Gal}(K/\mathbb{Q})| = \phi(m)$.
- Under the isomorphism, $(\zeta_m \mapsto \zeta_m^a) \longleftrightarrow a \pmod m$.
- For a prime p, $\mathrm{Frob}(p) = (\zeta_m \mapsto \zeta_m^p)$.
- By Čebotarev, the set of primes p for which $\mathrm{Frob}(p) = \sigma$ is infinite for each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.
- Therefore there are infinitely many primes $p \equiv a \pmod m$.

Q.E.D.

Class Field Theory (in 2 slides)

Class Field Theory (in 2 slides)

Fix a number field K

Class Field Theory (in 2 slides)

Fix a number field K (a finite-dimensional field extension $K \supset \mathbb{Q}$)

Class Field Theory (in 2 slides)

Fix a number field K (a finite-dimensional field extension $K \supset \mathbb{Q}$)

Definition

The set $\mathcal{O}_K$ of all algebraic integers of K, i.e. elements $\alpha \in K$ that are the root of some monic polynomial in $\mathbb{Z}[x]$, is called the **ring of integers** of K.

Class Field Theory (in 2 slides)

Fix a number field K (a finite-dimensional field extension $K \supset \mathbb{Q}$)

Definition

The set $\mathcal{O}_K$ of all algebraic integers of K, i.e. elements $\alpha \in K$ that are the root of some monic polynomial in $\mathbb{Z}[x]$, is called the **ring of integers** of K.

Proposition

The set $I_K^{\mathfrak{m}}$ of fractional ideals in the ring of integers $\mathcal{O}_K$ relatively prime to a modulus $\mathfrak{m}$ is a free abelian group on the prime ideals of $\mathcal{O}_K$ that are relatively prime to $\mathfrak{m}$.

Class Field Theory (in 2 slides)

Fix a number field K (a finite-dimensional field extension $K \supset \mathbb{Q}$)

Definition

The set $\mathcal{O}_K$ of all algebraic integers of K, i.e. elements $\alpha \in K$ that are the root of some monic polynomial in $\mathbb{Z}[x]$, is called the **ring of integers** of K.

Proposition

The set $I_K^{\mathfrak{m}}$ of fractional ideals in the ring of integers $\mathcal{O}_K$ relatively prime to a modulus $\mathfrak{m}$ is a free abelian group on the prime ideals of $\mathcal{O}_K$ that are relatively prime to $\mathfrak{m}$.

Denote the subgroup of $I_K^{\mathfrak{m}}$ generated by principal prime ideals by $P_K(\mathfrak{m}, 1)$.

Class Field Theory (in 2 slides)

Definition

A subgroup $H \leq I_K^{\mathfrak{m}}$ is a **congruence subgroup** for K if $P_K(\mathfrak{m}, 1) \leq H \leq I_K^{\mathfrak{m}}$. For such a subgroup H, the quotient $I_K^{\mathfrak{m}}/H$ is called a **generalized ideal class group** for K.

Class Field Theory (in 2 slides)

Definition

A subgroup $H \leq I_K^{\mathfrak{m}}$ is a **congruence subgroup** for K if $P_K(\mathfrak{m}, 1) \leq H \leq I_K^{\mathfrak{m}}$. For such a subgroup H, the quotient $I_K^{\mathfrak{m}}/H$ is called a **generalized ideal class group** for K.

The goal of class field theory is to classify all abelian extensions of K via class groups.

Class Field Theory (in 2 slides)

Definition

A subgroup $H \leq I_K^{\mathfrak{m}}$ is a **congruence subgroup** for K if $P_K(\mathfrak{m}, 1) \leq H \leq I_K^{\mathfrak{m}}$. For such a subgroup H, the quotient $I_K^{\mathfrak{m}}/H$ is called a **generalized ideal class group** for K.

The goal of class field theory is to classify all abelian extensions of K via class groups. This is accomplished by proving

Theorem (The Classification Theorem)

For a number field K, there is a one-to-one, inclusion-reversing correspondence

$$\left\{ \begin{array}{c} \textit{finite abelian} \\ \textit{extensions } L/K \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{generalized ideal} \\ \textit{class groups of } K \end{array} \right\}.$$

Take a deep breath

Ok, I lied...

Ok, I lied...

- Just consider I_K (free abelian group on prime ideals of $\mathcal{O}_K$)

Ok, I lied...

- Just consider I_K (free abelian group on prime ideals of $\mathcal{O}_K$)
- $P_K =$ the subgroup of principal ideals

Ok, I lied...

- Just consider I_K (free abelian group on prime ideals of $\mathcal{O}_K$)
- $P_K =$ the subgroup of principal ideals
- So P_K is a congruence subgroup

Ok, I lied...

- Just consider I_K (free abelian group on prime ideals of $\mathcal{O}_K$)
- $P_K =$ the subgroup of principal ideals
- So P_K is a congruence subgroup

Ok, I lied...

- Just consider I_K (free abelian group on prime ideals of $\mathcal{O}_K$)
- $P_K =$ the subgroup of principal ideals
- So P_K is a congruence subgroup

Definition

The quotient I_K/P_K is called the **class group** of K, denoted $C(\mathcal{O}_K)$.

Ok, I lied...

- Just consider I_K (free abelian group on prime ideals of $\mathcal{O}_K$)
- $P_K =$ the subgroup of principal ideals
- So P_K is a congruence subgroup

Definition

The quotient I_K/P_K is called the **class group** of K, denoted $C(\mathcal{O}_K)$.

By the Classification Theorem, there's an abelian extension...

The Hilbert Class Field

Definition

For a number field K, the unique abelian extension H/K with $\mathrm{Gal}(H/K) \cong C(\mathcal{O}_K)$ is called the **Hilbert class field** of K.

The Hilbert Class Field

Definition

For a number field K, the unique abelian extension H/K with $\mathrm{Gal}(H/K) \cong C(\mathcal{O}_K)$ is called the **Hilbert class field** of K.

Theorem

The Hilbert class field of K is the unique maximal unramified abelian extension of K.

The Hilbert Class Field

So what is it good for?

The Hilbert Class Field

So what is it good for?

Recall the motivating question:

For $n \in \mathbb{N}$, when is $x^2 + ny^2$ prime?

The Hilbert Class Field

So what is it good for?

Recall the motivating question:

For $n \in \mathbb{N}$, when is $x^2 + ny^2$ prime?

Class field theory (on the HCF) gives an answer...

The Hilbert Class Field

Theorem (Cox)

Let n a squarefree positive integer such that $n \not\equiv 3 \pmod 4$ and set $K = \mathbb{Q}(\sqrt{-n})$.

The Hilbert Class Field

Theorem (Cox)

Let n a squarefree positive integer such that $n \not\equiv 3 \pmod 4$ and set $K = \mathbb{Q}(\sqrt{-n})$. Let H be the Hilbert class field of K and suppose $f(x)$ is the minimal polynomial of some primitive element of H over K.

The Hilbert Class Field

Theorem (Cox)

Let n a squarefree positive integer such that $n \not\equiv 3 \pmod 4$ and set $K = \mathbb{Q}(\sqrt{-n})$. Let H be the Hilbert class field of K and suppose $f(x)$ is the minimal polynomial of some primitive element of H over K. Then for an odd prime p that doesn't divide the discriminant of f,

The Hilbert Class Field

Theorem (Cox)

Let n a squarefree positive integer such that $n \not\equiv 3 \pmod 4$ and set $K = \mathbb{Q}(\sqrt{-n})$. Let H be the Hilbert class field of K and suppose $f(x)$ is the minimal polynomial of some primitive element of H over K. Then for an odd prime p that doesn't divide the discriminant of f,

$$p = x^2 + ny^2 \iff \left(\frac{-n}{p}\right) = 1 \text{ and } f(x) \equiv 0 \pmod p \text{ for some } x \in \mathbb{Z}.$$

The Hilbert Class Field

Theorem (Cox)

Let n a squarefree positive integer such that $n \not\equiv 3 \pmod 4$ and set $K = \mathbb{Q}(\sqrt{-n})$. Let H be the Hilbert class field of K and suppose $f(x)$ is the minimal polynomial of some primitive element of H over K. Then for an odd prime p that doesn't divide the discriminant of f,

$$p = x^2 + ny^2 \iff \left(\frac{-n}{p}\right) = 1 \text{ and } f(x) \equiv 0 \pmod p \text{ for some } x \in \mathbb{Z}.$$

There is also a generalization for all n, but it uses even more class field theory (orders, ring class fields).

n-Fermat Primes

Definition

For an integer $n \geq 1$, a prime p is an n**-Fermat prime** if $p = x^2 + ny^2$ for some $x, y \in \mathbb{Z}$.

n-Fermat Primes

Definition

For an integer $n \geq 1$, a prime p is an n**-Fermat prime** if $p = x^2 + ny^2$ for some $x, y \in \mathbb{Z}$.

Cox's Theorem fully characterizes n-Fermat primes with congruence conditions and polynomial solvability conditions.

Symmetric n-Fermat Primes

Symmetric n-Fermat Primes

A related (and much harder) question is:

If $x^2 + ny^2$ is prime, when is $y^2 + nx^2$ also prime?

Symmetric n-Fermat Primes

A related (and much harder) question is:

If $x^2 + ny^2$ is prime, when is $y^2 + nx^2$ also prime?

Definition

An n-Fermat prime $p = x^2 + ny^2$ is a **symmetric n-Fermat prime** provided $q = y^2 + nx^2$ is also prime.

Symmetric n-Fermat Primes

A related (and much harder) question is:

If $x^2 + ny^2$ is prime, when is $y^2 + nx^2$ also prime?

Definition

An n-Fermat prime $p = x^2 + ny^2$ is a **symmetric n-Fermat prime** provided $q = y^2 + nx^2$ is also prime.

Question

Are there conditions similar to Cox's Theorem that determine when an n-Fermat prime is symmetric?

Symmetric n-Fermat Primes

- There are infinitely many n-Fermat primes for each $n \geq 1$. (Cox)

Symmetric n-Fermat Primes

- There are infinitely many n-Fermat primes for each $n \geq 1$. (Cox)
- Are there infinitely many symmetric n-Fermat primes?

Symmetric n-Fermat Primes

- There are infinitely many n-Fermat primes for each $n \geq 1$. (Cox)
- Are there infinitely many symmetric n-Fermat primes?
- Easy case: $n = 1$ (think about it)

Symmetric n-Fermat Primes

- There are infinitely many n-Fermat primes for each $n \geq 1$. (Cox)
- Are there infinitely many symmetric n-Fermat primes?
- Easy case: $n = 1$ (think about it)
- Even for $n = 2$, the answer is not known (as far as we can tell)

Symmetric n-Fermat Primes

Example

Let $n = 2$.

Symmetric n-Fermat Primes

Example

Let $n = 2$.

First few symmetric 2-Fermat primes: 3, 11, 19, 43, 59, 67, 83, 107, 139, 163, 179 $\ldots$

Symmetric n-Fermat Primes

Example

Let $n = 2$.

First few symmetric 2-Fermat primes: 3, 11, 19, 43, 59, 67, 83, 107, 139, 163, 179 $\ldots$

It appears that p is a symmetric 2-Fermat prime $\iff p \equiv 3 \pmod 8$.

Symmetric n-Fermat Primes

Example

Let $n = 2$.

First few symmetric 2-Fermat primes: 3, 11, 19, 43, 59, 67, 83, 107, 139, 163, 179 ...

It appears that p is a symmetric 2-Fermat prime $\iff p \equiv 3 \pmod 8$.

But this breaks early for 131:

$$131 = 9^2 + 2 \cdot 5^2 \quad \text{but} \quad 5^2 + 2 \cdot 9^2 = 187 = 11 \cdot 17.$$

Symmetric n-Fermat Primes

Example

Let $n = 2$.

Empirical results:

- About 14% of 2-Fermat primes are symmetric.

Symmetric n-Fermat Primes

Example

Let $n = 2$.

Empirical results:

- About 14% of 2-Fermat primes are symmetric.
- Using the Prime Number Theorem as an estimate, the ratio of observed symmetric 2-Fermat primes to expected symmetric 2-Fermat primes is about 0.94.

Symmetric n-Fermat Primes

Example

Let $n = 2$.

Empirical results:

- About 14% of 2-Fermat primes are symmetric.
- Using the Prime Number Theorem as an estimate, the ratio of observed symmetric 2-Fermat primes to expected symmetric 2-Fermat primes is about 0.94.
- That is, *there are slightly less* symmetric 2-Fermat primes than we expect!

Symmetric n-Fermat Primes

Example

Let $n = 2$.

Empirical results:

- About 14% of 2-Fermat primes are symmetric.
- Using the Prime Number Theorem as an estimate, the ratio of observed symmetric 2-Fermat primes to expected symmetric 2-Fermat primes is about 0.94.
- That is, *there are slightly less* symmetric 2-Fermat primes than we expect!
- Something interesting is going on here...

Symmetric n-Fermat Primes

- For a positive number M, let $\pi_{sym,n}(M)$ denote the number of primes $y^2 + nx^2$ such that $x^2 + ny^2$ is prime and $x, y \leq M$.

Symmetric n-Fermat Primes

- For a positive number M, let $\pi_{sym,n}(M)$ denote the number of primes $y^2 + nx^2$ such that $x^2 + ny^2$ is prime and $x, y \leq M$.
- This is like the prime counting function $\pi(x)$ or Dirichlet's generalization $\pi_{a,m}(x)$ for $p \equiv a \pmod{m}$.

Symmetric n-Fermat Primes

- For a positive number M, let $\pi_{sym,n}(M)$ denote the number of primes $y^2 + nx^2$ such that $x^2 + ny^2$ is prime and $x, y \leq M$.
- This is like the prime counting function $\pi(x)$ or Dirichlet's generalization $\pi_{a,m}(x)$ for $p \equiv a \pmod{m}$.
- By the PNT, there is a nonnegative real number α_n so that

$$\pi_{sym,n}(M) \sim 2\alpha_n \sum_{q \leq M} \frac{1}{\log q}$$

where the sum is over numbers $q = y^2 + nx^2$ for which $x, y \leq M$, x and y are relatively prime and $x^2 + ny^2$ is prime.

Symmetric n-Fermat Primes

- For a positive number M, let $\pi_{sym,n}(M)$ denote the number of primes $y^2 + nx^2$ such that $x^2 + ny^2$ is prime and $x, y \leq M$.
- This is like the prime counting function $\pi(x)$ or Dirichlet's generalization $\pi_{a,m}(x)$ for $p \equiv a \pmod{m}$.
- By the PNT, there is a nonnegative real number α_n so that

$$\pi_{sym,n}(M) \sim 2\alpha_n \sum_{q \leq M} \frac{1}{\log q}$$

  where the sum is over numbers $q = y^2 + nx^2$ for which $x, y \leq M$, x and y are relatively prime and $x^2 + ny^2$ is prime.
- For example, when $n = 2$, $\alpha_2 \approx 0.94$.

Conjectures and Further Research

$$\pi_{sym,n}(M) \sim 2\alpha_n \sum_{q \leq M} \frac{1}{\log q}$$

Conjectures and Further Research

$$\pi_{sym,n}(M) \sim 2\alpha_n \sum_{q \leq M} \frac{1}{\log q}$$

Conjecture

$\alpha_n > 0$ for all $n \geq 1$.

Conjectures and Further Research

$$\pi_{sym,n}(M) \sim 2\alpha_n \sum_{q \leq M} \frac{1}{\log q}$$

Conjecture

$\alpha_n > 0$ for all $n \geq 1$.

Holds for $n \leq 100,000$ and $x, y \leq 2,000$.

Conjectures and Further Research

$$\pi_{sym,n}(M) \sim 2\alpha_n \sum_{q \leq M} \frac{1}{\log q}$$

Conjecture

$\alpha_n > 0$ for all $n \geq 1$.

Holds for $n \leq 100,000$ and $x, y \leq 2,000$.

Conjecture

The average value of α_n over all $n \geq 1$ is equal to 1.

Conjectures and Further Research

$$\pi_{sym,n}(M) \sim 2\alpha_n \sum_{q \leq M} \frac{1}{\log q}$$

Conjecture

$\alpha_n > 0$ for all $n \geq 1$.

Holds for $n \leq 100,000$ and $x, y \leq 2,000$.

Conjecture

The average value of α_n over all $n \geq 1$ is equal to 1.

Some n have $\alpha_n > 2$ and others $< \frac{1}{2}$, but for $n \leq 100,000$, $0.4 \leq \alpha_n \leq 2.1$ within the search space $x, y \leq 2,000$.

Conjectures and Further Research

$$\pi_{sym,n}(M) \sim 2\alpha_n \sum_{q \leq M} \frac{1}{\log q}$$

Conjecture

$\alpha_n > 0$ for all $n \geq 1$.

Holds for $n \leq 100,000$ and $x, y \leq 2,000$.

Conjecture

The average value of α_n over all $n \geq 1$ is equal to 1.

Some n have $\alpha_n > 2$ and others $< \frac{1}{2}$, but for $n \leq 100,000$, $0.4 \leq \alpha_n \leq 2.1$ within the search space $x, y \leq 2,000$.

Conjecture

The set of α_n is bounded.

Conjectures and Further Research

Conjecture

There exists an extension L of $K = \mathbb{Q}(\sqrt{-n})$ such that if $f(x)$ is the minimal polynomial of a primitive element of L over K and p is an odd prime not dividing the discriminant of f, then p is a symmetric n-Fermat prime if and only if $\left(\frac{-n}{p}\right) = 1$ and $f(x) \equiv 0 \pmod{p}$ is solvable over $\mathbb{Z}$.

Conjectures and Further Research

Conjecture

There exists an extension L of $K = \mathbb{Q}(\sqrt{-n})$ such that if $f(x)$ is the minimal polynomial of a primitive element of L over K and p is an odd prime not dividing the discriminant of f, then p is a symmetric n-Fermat prime if and only if $\left(\frac{-n}{p}\right) = 1$ and $f(x) \equiv 0 \pmod{p}$ is solvable over $\mathbb{Z}$.

Question

If p is an n-Fermat prime, is there an algorithm for finding all or even any solutions $x, y \in \mathbb{Z}$ to $p = x^2 + ny^2$?

Conjectures and Further Research

Conjecture

There exists an extension L of $K = \mathbb{Q}(\sqrt{-n})$ such that if $f(x)$ is the minimal polynomial of a primitive element of L over K and p is an odd prime not dividing the discriminant of f, then p is a symmetric n-Fermat prime if and only if $\left(\frac{-n}{p}\right) = 1$ and $f(x) \equiv 0 \pmod{p}$ is solvable over $\mathbb{Z}$.

Question

If p is an n-Fermat prime, is there an algorithm for finding all or even any solutions $x, y \in \mathbb{Z}$ to $p = x^2 + ny^2$?

And if so, how many solutions are there?

An Application (Finally!)

An Application (Finally!)

Let p be an odd prime.

An Application (Finally!)

Let p be an odd prime. Fermat was able to prove:

$$p = x^2 + y^2 \iff p \equiv 1 \pmod 4.$$

$$p = x^2 + 2y^2 \iff p \equiv 1 \text{ or } 3 \pmod 8.$$

$$p = x^2 + 3y^2 \iff p = 3 \text{ or } p \equiv 1 \pmod 3.$$

An Application (Finally!)

Let p be an odd prime. Fermat was able to prove:

$$p = x^2 + y^2 \iff p \equiv 1 \pmod 4.$$
$$p = x^2 + 2y^2 \iff p \equiv 1 \text{ or } 3 \pmod 8.$$
$$p = x^2 + 3y^2 \iff p = 3 \text{ or } p \equiv 1 \pmod 3.$$

- Euler discovered primality tests for these, e.g. $m = x^2 + y^2$ has a single solution (x, y) in positive integers when m is prime.

An Application (Finally!)

Let p be an odd prime. Fermat was able to prove:

$$p = x^2 + y^2 \iff p \equiv 1 \pmod 4.$$
$$p = x^2 + 2y^2 \iff p \equiv 1 \text{ or } 3 \pmod 8.$$
$$p = x^2 + 3y^2 \iff p = 3 \text{ or } p \equiv 1 \pmod 3.$$

- Euler discovered primality tests for these, e.g. $m = x^2 + y^2$ has a single solution (x, y) in positive integers when m is prime.
- There are similar tests for $n = 2, 3$.

An Application (Finally!)

Let p be an odd prime. Fermat was able to prove:

$$p = x^2 + y^2 \iff p \equiv 1 \pmod 4.$$
$$p = x^2 + 2y^2 \iff p \equiv 1 \text{ or } 3 \pmod 8.$$
$$p = x^2 + 3y^2 \iff p = 3 \text{ or } p \equiv 1 \pmod 3.$$

- Euler discovered primality tests for these, e.g. $m = x^2 + y^2$ has a single solution (x, y) in positive integers when m is prime.
- There are similar tests for $n = 2, 3$.
- These are useful for codebreaking algorithms and, more importantly, for writing secure cryptosystems.

An Application (Finally!)

Let p be an odd prime. Fermat was able to prove:

$$p = x^2 + y^2 \iff p \equiv 1 \pmod 4.$$
$$p = x^2 + 2y^2 \iff p \equiv 1 \text{ or } 3 \pmod 8.$$
$$p = x^2 + 3y^2 \iff p = 3 \text{ or } p \equiv 1 \pmod 3.$$

- Euler discovered primality tests for these, e.g. $m = x^2 + y^2$ has a single solution (x, y) in positive integers when m is prime.
- There are similar tests for $n = 2, 3$.
- These are useful for codebreaking algorithms and, more importantly, for writing secure cryptosystems.
- The complexity of n-Fermat primes and symmetric n-Fermat primes may soon contribute to greater cryptographic security.

Thank you!

Selected References

(1) Artin, Emil and Tate, John. *Class Field Theory*. W.A. Benjamin, New York (1968).

(2) Cox, David A. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, 2^{nd} ed. John Wiley & Sons, Hoboken (2013).

(3) Dirichlet, Peter Gustav Lejeune. There are infinitely many prime numbers in all arithmetic progressions with first term and difference coprime. Translated from German. `arXiv:0808.1408v1 [math.HO]` (2008).

(4) Janusz, Gerald J. *Algebraic Number Fields*. Academic Press, New York (1973).

(5) Stevenhagen, P. and Lenstra, H.W., Jr. Chebotarëv and his Density Theorem. *The Mathematical Intelligencer*, vol. 18, no. 2 (1996). pp. 26-37.

Questions?