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

Steven Charlton

28 November 2012
Outline

1 Motivating Examples
2 Quadratic Forms
3 Class Field Theory
4 Hilbert Class Field
5 Narrow Class Field
6 Cubic Forms
7 Modular Forms and Counting Solutions
Fermat’s Claims

\[ p = x^2 + y^2 \iff p = 2 \text{ or } p \equiv 1 \pmod{4} \]
Fermat’s Claims

\[ p = x^2 + y^2 \iff p = 2 \text{ or } p \equiv 1 \pmod{4} \]

\[ p = x^2 + 2y^2 \iff p = 2 \text{ or } p \equiv 1, 3 \pmod{8} \]

\[ p = x^2 + 3y^2 \iff p = 3 \text{ or } p \equiv 1 \pmod{3} \]
Other Examples

\[ p = x^2 + 5y^2 \iff p = 5 \text{ or } p \equiv 1, 9 \pmod{20} \]
\[ p = x^2 - 2y^2 \iff p = 2 \text{ or } p \equiv 1, 7 \pmod{8} \]
For $p \neq 2, 17$

$$p = x^2 + 17y^2 \iff \begin{cases} 
    t^8 + 5t^6 + 4t^4 + 5t^2 + 1 \equiv 0 \pmod{p} \\
    \text{has a solution}
\end{cases}$$

$$\iff \begin{cases} 
    \frac{-17}{p} = 1 \quad \text{and} \\
    t^4 + t^2 - 2t + 1 \equiv 0 \pmod{p} \\
    \text{has a solution}
\end{cases}$$
Other Examples

For \( p \neq 2, 5, 71, 241 \)

\[ p = x^2 - 142y^2 \iff \begin{cases} 
  t^{12} - 14t^{10} + 109t^8 - 356t^6 + 452t^4 \\
  - 352t^2 + 1024 \equiv 0 \pmod{p} \text{ has a solution}
\end{cases} \]

\[ \iff \begin{cases} 
  (142/p) = 1 \text{ and} \\
  t^6 - 2t^5 + t^4 + 2t^2 - 8t + 8 \equiv 0 \pmod{p} \text{ has a solution}
\end{cases} \]
Binary Quadratic Forms

Definition

A binary quadratic form is a polynomial $f(x, y) = ax^2 + bxy + cy^2$

Discriminant $D = b^2 - 4ac$

- Positive definite if $D < 0$
- Indefinite if $D > 0$

Which primes does $f(x, y)$ represent?
Act on quadratic forms by $\text{SL}(2, \mathbb{Z})$:

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \cdot f(x, y) = f(px + ry, qx + sy)$$

- Preserves discriminant
- Represents same integers
- Finite number of equivalence classes
- Algorithmic way of listing classes
Ideals in Quadratic Fields

\(D\) a fundamental discriminant, \(K = \mathbb{Q}(\sqrt{D})\)

Map:

\[\{\text{narrow ideal classes in } K\} \longrightarrow \{\text{quadratic forms of discriminant } D\}\]

\[a = [\alpha, \beta] \mapsto Q(x, y) = \frac{1}{N(a)} N(\alpha x + \beta y)\]
Ideals in Quadratic Fields

$D$ a fundamental discriminant, $K = \mathbb{Q}(\sqrt{D})$

Map:

\[ \{ \text{narrow ideal classes in } K \} \longrightarrow \{ \text{quadratic forms of discriminant } D \} \]

\[ \alpha = [\alpha, \beta] \longmapsto Q(x, y) = \frac{1}{N(\alpha)} N(\alpha x + \beta y) \]

**Theorem**

*This map is a bijective correspondence.*
Representing Integers

**Lemma**

\( m \) is represented by \( f(x, y) \) if and only if there is an ideal of norm \( m \) in the same narrow class as \( \alpha \).

**Theorem**

An odd prime \( p \nmid D \) is represented by some quadratic form of discriminant \( D \) if and only if \( (D/p) = 1 \).
Class Number One

Problem solved for class number one:

- All quadratic forms are equivalent
- $(D/p) = 1$ if and only if some form represents $p$
- if and only if any form represents $p$
Problem solved for class number one:

- All quadratic forms are equivalent
- \((D/p) = 1\) if and only if some form represents \(p\)
- if and only if any form represents \(p\)

What if the class number isn’t one?

- Need to determine the ideal classes \((p)\) splits into.
- For \(p = x^2 + ny^2\), need \((p)\) to split as principal ideals.
- How to check if an ideal is principal?
Generalised Ideal Class Groups

Definition

A modulus $m$ is a product of primes and distinct real embeddings

$$\mathcal{I}_K(m) = \{ \text{fractional ideals prime to } m_0 \}$$
$$\mathcal{P}_{1,K}(m) = \{ \text{principal ideals } (\alpha) \mid \alpha \equiv 1 \pmod{m_0} \text{ and } \sigma(\alpha) > 0 \}$$

Definition

- $H \leq \mathcal{I}_K(m)$ is a congruence subgroup if
  $$\mathcal{P}_{1,K}(m) \leq H \leq \mathcal{I}_K(m)$$
- Then $\mathcal{I}_K(m)/H$ is a generalised ideal class group
Artin Map

$L/K$ Galois, $\mathfrak{P}$ prime above unramified $p$.

$$\tilde{G} := \text{Gal} \left( \frac{\mathcal{O}_L/\mathfrak{P}}{\mathcal{O}_K/p} \right) \cong D_\mathfrak{P} \leq \text{Gal}(L/K)$$

Definition

Artin symbol is $$((L/K)/\mathfrak{P}) := \text{Frob} (\tilde{G}) \in \text{Gal}(L/K)$$

- If $L/K$ is Abelian the Artin symbol depends only on $p$
- Prime $p$ splits completely if and only if $$((L/K)/p) = 1$$

Definition

Let $m$ be divisible by all ramified primes. Extend $$((L/K)/\cdot)$$ to the Artin map:

$$\Phi: \mathcal{I}_K(m) \longrightarrow \text{Gal}(L/K)$$
Theorems of Class Field Theory

Theorem (Artin Reciprocity)

Let $L/K$ be Abelian, and $\mathfrak{m}$ divisible by all ramified primes. If the exponents of $\mathfrak{m}$ are sufficiently large:

- The Artin map is surjective
- Its kernel is a congruence subgroup
- $\text{Gal}(L/K)$ is a generalised ideal class group

Theorem (Existence)

Given $\mathfrak{m}$, and $H$, there is a unique Abelian extension $L/K$, whose ramified primes divide $\mathfrak{m}$, such that the Artin map has kernel $H$. 
**Hilbert Class Field**

**Definition**

The Hilbert Class Field $L$ arises from $m = 1$, and $H = \mathcal{P}(K)$

**Theorem**

*The Hilbert class field is the maximal unramified Abelian extension.*

**Theorem**

*A prime $\mathfrak{p}$ is principal if and only if it splits completely in $L$.***
Positive-Definite Forms

- $D$ a fundamental discriminant
- $Q(x, y) \leftarrow \mathcal{O}_K$ in $K = \mathbb{Q}(\sqrt{-d})$
- $L = K(\alpha)$ the Hilbert class field generated by $f(t)$ over $\mathbb{Q}$
- $\mathbb{Q}(\alpha)/\mathbb{Q}$ generated by $g(t)$

**Theorem**

- For odd $p \nmid D$, $p$ is represented by $Q(x, y)$ if and only if $(p)$ splits completely in $L/\mathbb{Q}$
- If $p \nmid \text{disc } f(t)$, then if and only if $f(t)$ has a root modulo $p$
- If $p \nmid \text{disc } g(t)$, then if and only if $(-D/p) = 1$ and $g(t)$ has a root modulo $p$
Narrow Class Field

**Definition**

The **Narrow Class Field** $L$ arises from $m = \sigma_1\sigma_2$, and $H = \mathcal{P}^+(K)$

**Theorem**

The Narrow class field is the maximal Abelian extension, unramified at all finite primes.

**Theorem**

A prime $\mathfrak{p}$ is totally positive principal if and only if it splits completely in $L$. 
Indefinite Forms

- $D$ a fundamental discriminant
- $Q(x, y) \leftarrow \mathcal{O}_K^+ \text{ in } K = \mathbb{Q}(\sqrt{d})$
- $L = K(\alpha)$ the Narrow class field generated by $f(t)$ over $\mathbb{Q}$
- $\mathbb{Q}(\alpha)/\mathbb{Q}$ generated by $g(t)$

Theorem

- For odd $p \nmid D$, $p$ is represented by $Q(x, y)$ if and only if $(p)$ splits completely in $L/\mathbb{Q}$
- If $p \nmid \text{disc } f(t)$, then if and only if $f(t)$ has a root modulo $p$
- If $p \nmid \text{disc } g(t)$, then if and only if $(-D/p) = 1$ and $g(t)$ has a root modulo $p$
When is $p = a^3 + 11b^3 + 121c^3 - 33abc$?
Cubic Forms

When is \( p = a^3 + 11b^3 + 121c^3 - 33abc \)?

Plan of attack:

1. Recognize this as a norm form
2. Phrase it in terms of number fields
3. Throw some class field theory at it
4. ?
5. Profit
For $p \neq 2, 3, 11$

$$p = a^3 + 11b^3 + 121c^3 - 33abc \iff \begin{cases} t^6 - 15t^4 + 9t^2 - 4 \equiv 0 \pmod{p} \\ \text{has a solution} \end{cases}$$
Representation Numbers and Theta Series

- How many solutions?

**Definition**

The **Theta series** of $Q(x, y)$ is:

$$\Theta_Q := \sum_{(x, y) \in \mathbb{Z}^2} q^{Q(x, y)} = \sum_{n=0}^{\infty} r_n(Q) q^n$$

- This is a modular form (for some group, weight, character...)

Take characters $\chi$ of the class group
Look at linear combinations of the Theta series
How many solutions?

**Definition**

The Theta series of \( Q(x, y) \) is:

\[
\Theta_Q := \sum_{(x, y) \in \mathbb{Z}^2} q^{Q(x, y)} = \sum_{n=0}^{\infty} r_n(Q) q^n
\]

This is a modular form (for some group, weight, character…)

Take characters \( \chi \) of the class group

Look at linear combinations of the Theta series
\textbf{Definition}

\textit{L}-series of $f = \sum_n a_n q^n$ is $L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$
$L$-Series

Definition

$L$-series of $f = \sum_n a_n q^n$ is $L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$

The linear combinations here have an Euler product:

$L(f, s) = \prod_{p \text{ prime}} \frac{1}{1 - a_p p^{-s} + (D/p)p^{-2s}}$
Formulae for Representation Numbers

\[
r_{x^2+5y^2}(n) = \sum_{d|n} \left( \frac{-20}{d} \right) + \left( \frac{-4}{d} \right) \left( \frac{5}{n/d} \right)
\]

\[
r_{2x^2+2xy+3y^2}(n) = \sum_{d|n} \left( \frac{-20}{d} \right) - \left( \frac{-4}{d} \right) \left( \frac{5}{n/d} \right)
\]
Epilogue

Still plenty to be done...

- Non-fundamental discriminants
- Separating all forms of discriminant $D$
  - Class field theory struggles
  - Modular forms work better
- Finding other representation numbers
- More general polynomial equations
  - Non-abelian class field theory
  - Langlands program