

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

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

Class Field Theory

Steven Charlton

29th February 2012

Introduction

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

- Motivating examples
- Definition of a binary quadratic form
- Fermat and the sum of two squares
- The Hilbert class field
- Primes of the form $x^2 + 23y^2$

Motivating Examples

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

- $p = x^2 + y^2 \Leftrightarrow p = 2, \text{ or } p \equiv 1 \pmod{4}$
- $p = x^2 + 2y^2 \Leftrightarrow p = 2, \text{ or } p \equiv 1, 3 \pmod{8}$
- $p = x^2 + 5y^2 \Leftrightarrow p = 5, \text{ or } p \equiv 1, 9 \pmod{20}$

Motivating Examples

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

- $p = x^2 + y^2 \Leftrightarrow p = 2, \text{ or } p \equiv 1 \pmod{4}$
- $p = x^2 + 2y^2 \Leftrightarrow p = 2, \text{ or } p \equiv 1, 3 \pmod{8}$
- $p = x^2 + 5y^2 \Leftrightarrow p = 5, \text{ or } p \equiv 1, 9 \pmod{20}$

- For $p \neq 2, 17$:

$$p = x^2 + 17y^2 \Leftrightarrow \begin{cases} \left(\frac{-17}{p}\right) = 1, \text{ and} \\ (2x^2 - 1)^2 \equiv 17 \pmod{p} \end{cases} \text{ has a solution}$$

Binary Quadratic Forms

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

- Binary quadratic form: $ax^2 + bxy + cy^2$
- Discriminant: $D = b^2 - 4ac$
- Notion of equivalence
- Ideals in a quadratic field correspond to quadratic forms

Binary Quadratic Forms

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

- Binary quadratic form: $ax^2 + bxy + cy^2$
- Discriminant: $D = b^2 - 4ac$
- Notion of equivalence
- Ideals in a quadratic field correspond to quadratic forms

Theorem

If $p \nmid n$ is an odd prime, then $\left(\frac{-n}{p}\right) = 1$ if and only if p is represented by some binary quadratic form of discriminant $D = -4n$.

Fermat and the Sum of Two Squares

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

When is $p = x^2 + y^2$?

Fermat and the Sum of Two Squares

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

When is $p = x^2 + y^2$?

For $p \nmid 1$ an odd prime:

- p is represented by a form with $D = -4$ if and only if $\left(\frac{-1}{p}\right) = 1$
- There is only one quadratic form with $D = -4$
- p is represented by $x^2 + y^2$ if and only if $\left(\frac{-1}{p}\right) = 1$

Fermat and the Sum of Two Squares

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

When is $p = x^2 + y^2$?

For $p \nmid 1$ an odd prime:

- p is represented by a form with $D = -4$ if and only if $\left(\frac{-1}{p}\right) = 1$
- There is only one quadratic form with $D = -4$
- p is represented by $x^2 + y^2$ if and only if $\left(\frac{-1}{p}\right) = 1$

Finding the condition:

- $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{4}$ by quadratic reciprocity
- $2 = 1^2 + 1^2$

So $p = x^2 + y^2 \Leftrightarrow p = 2$, or $p \equiv 1 \pmod{4}$.

The Hilbert Class Field

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

Definition

The **Hilbert class field** L is the maximal unramified abelian extension of a number field K .

The Hilbert Class Field

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

Definition

The **Hilbert class field** L is the maximal unramified abelian extension of a number field K .

Theorem

A prime ideal \mathfrak{p} of K is principal if and only if \mathfrak{p} splits completely in L .

Setting Up

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

Which primes are of the form $p = x^2 + 23y^2$?

- First look at $K = \mathbb{Q}(\sqrt{-23})$
- $Q_0 = x^2 + xy + 6y^2$ corresponds to principal ideals in K
- Q_0 represents p if and only if p splits into principal ideals in K

Hilbert Class Field of $K = \mathbb{Q}(\sqrt{-23})$

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

- The Hilbert class field of K is $L = K(\alpha)$, where $\alpha^3 - \alpha - 1 = 0$

Hilbert Class Field of $K = \mathbb{Q}(\sqrt{-23})$

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

Steven Charlton

Motivation

Binary Quadratic
Forms

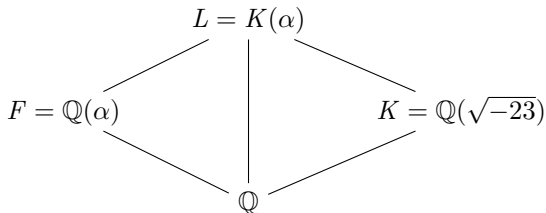
Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

- The Hilbert class field of K is $L = K(\alpha)$, where $\alpha^3 - \alpha - 1 = 0$



Hilbert Class Field of $K = \mathbb{Q}(\sqrt{-23})$

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

Steven Charlton

Motivation

Binary Quadratic
Forms

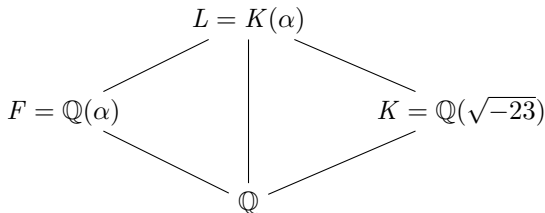
Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

- The Hilbert class field of K is $L = K(\alpha)$, where $\alpha^3 - \alpha - 1 = 0$



- $p = x^2 + xy + 6y^2$ if and only if p splits in F and in K

Hilbert Class Field of $K = \mathbb{Q}(\sqrt{-23})$

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

Steven Charlton

Motivation

Binary Quadratic
Forms

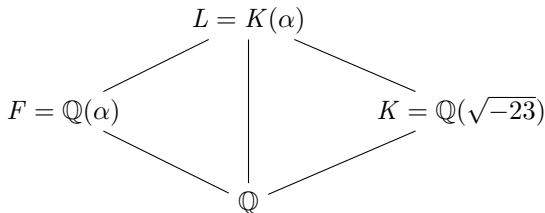
Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

- The Hilbert class field of K is $L = K(\alpha)$, where $\alpha^3 - \alpha - 1 = 0$



- $p = x^2 + xy + 6y^2$ if and only if p splits in F and in K
- For $p \neq 23$:

$$p = x^2 + xy + 6y^2 \Leftrightarrow \begin{cases} \left(\frac{-23}{p}\right) = 1, \text{ and} \\ x^3 - x - 1 \equiv 0 \pmod{p} \text{ has a solution} \end{cases}$$

Primes of the Form $x^2 + 23y^2$

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

- Identity: $x^2 + xy + 6y^2 = \left(x + \frac{y}{2}\right)^2 + 23\left(\frac{y}{2}\right)^2$
- If $p \neq 2$, then $p = x^2 + xy + 6y^2$ means y is even:

$$1 \equiv x^2 + xy \equiv x(x + y) \pmod{2}$$

Primes of the Form $x^2 + 23y^2$

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

- Identity: $x^2 + xy + 6y^2 = (x + \frac{y}{2})^2 + 23(\frac{y}{2})^2$
- If $p \neq 2$, then $p = x^2 + xy + 6y^2$ means y is even:

$$1 \equiv x^2 + xy \equiv x(x + y) \pmod{2}$$

- $p = x^2 + xy + 6y^2$ if and only if $p = x^2 + 23y^2$

For $p \neq 23$:

$$p = x^2 + 23y^2 \Leftrightarrow \begin{cases} \left(\frac{-23}{p}\right) = 1, \text{ and} \\ x^3 - x - 1 \equiv 0 \pmod{p} \text{ has a solution} \end{cases}$$

Conclusion

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

In summary:

- Defined binary quadratic forms
- Proved Fermat's two-squares theorem
- Used the Hilbert class field to find when $p = x^2 + 23y^2$

Conclusion

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

Steven Charlton

Motivation

Binary Quadratic
Forms

Sum of Two
Squares

The Hilbert Class
Field

$p = x^2 + 23y^2$

Conclusion

In summary:

- Defined binary quadratic forms
- Proved Fermat's two-squares theorem
- Used the Hilbert class field to find when $p = x^2 + 23y^2$

What else could we look at?

- Ring class fields to deal with **all** $x^2 + ny^2$, $n > 0$
- Narrow class fields to study **indefinite** forms