

[Descent and](#page-2-0)

[The Hilbert](#page-16-0) Class Field

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

Advaith Mopuri

July 2023

K ロ ▶ K 個 ▶ K 할 ▶ K 할 ▶ 이 할 → 9 Q Q →

[Primes of the](#page-0-0) Form
 $x^2 + ny^2$ [Descent and](#page-2-0) [The Hilbert](#page-16-0) Class Field Table of Contents 1 [Descent and Reciprocity](#page-2-0) 2 [Reciprocity](#page-9-0)

K ロ ▶ K 個 ▶ K 할 ▶ K 할 ▶ 이 할 → 9 Q Q →

3 [The Hilbert Class Field](#page-16-0)

A Classic Theorem of Fermat

[Descent and](#page-2-0) Reciprocity

[The Hilbert](#page-16-0) Class Field

It is well known that for $x, y \in \mathbb{Z}$ and an odd prime p,

$$
p = x^2 + y^2 \Longleftrightarrow p \equiv 1 \bmod 4. \tag{1}
$$

¹Here we are only considering odd primes p, as they make up the actually interesting parts of this problemK ロ ▶ K 個 ▶ K 할 ▶ K 할 ▶ 이 할 → 9 Q Q →

A Classic Theorem of Fermat

[Descent and](#page-2-0) **Reciprocity**

[The Hilbert](#page-16-0) Class Field

It is well known that for $x, y \in \mathbb{Z}$ and an odd prime p,

$$
p = x^2 + y^2 \Longleftrightarrow p \equiv 1 \text{ mod } 4. \tag{1}
$$

This begs the question $-$ is there a similar way that we can classify which primes 1 can be expressed in the form $x^2 + ny^2$?

¹Here we are only considering odd primes p, as they make up the actually interesting parts of this problemK ロ ▶ K 個 ▶ K 결 ▶ K 결 ▶ │ 결 │ K 9 Q Q

Brief History

[Descent and](#page-2-0) **Reciprocity**

[The Hilbert](#page-16-0) Class Field

Mathematicians like Fermat, Euler, Legendre, Lagrange, and Gauss all contributed to the creation of such a classification, and developed techniques such as quadratic forms, reciprocity, and genus theory in the process.

Proving Fermat's Theorem

[Descent and](#page-2-0) Reciprocity

[The Hilbert](#page-16-0) Class Field

Recall equation [1](#page-2-1)

$$
p = x^2 + y^2 \Longleftrightarrow p \equiv 1 \text{ mod } 4.
$$

K ロ ▶ K 레 ▶ K 코 ▶ K 코 ▶ 『코 │ ◆ 9 Q Q ↓

Proving Fermat's Theorem

[Descent and](#page-2-0) Reciprocity

[The Hilbert](#page-16-0) Class Field

Recall equation [1](#page-2-1)

$$
p = x^2 + y^2 \Longleftrightarrow p \equiv 1 \text{ mod } 4.
$$

In order to prove this theorem, Euler used an approached based off of two steps, descent and reciprocity.

Descent and Reciprocity

[Primes of the](#page-0-0) Form
 $x^2 + ny^2$

[Descent and](#page-2-0) Reciprocity

[The Hilbert](#page-16-0) Class Field

Descent and Reciprocity

Descent:

If
$$
p|x^2 + y^2
$$
, $gcd(x, y) = 1$, then p can be written as $x^2 + y^2$

for some possibly different x, y .

Descent and Reciprocity

[Primes of the](#page-0-0) Form
 $x^2 + ny^2$

Mopuri

[Descent and](#page-2-0) **Reciprocity**

[The Hilbert](#page-16-0) Class Field

Descent and Reciprocity

Descent:

If
$$
p|x^2 + y^2
$$
, $gcd(x, y) = 1$, then p can be written as $x^2 + y^2$

for some possibly different x, y .

Reciprocity:

If $p \equiv 1 \text{ mod } 4$, then $p|x^2 + y^2$, $gcd(x, y) = 1$.

KORKARYKERKER POLO

Note: $p = x^2 + y^2 \implies p \equiv 0, 1, 2 \text{ mod } 4$ since $x^2\equiv 0,1$ mod 4. But, for odd primes p the first and third options are clearly impossible.

Why Reciprocity?

[Descent and](#page-2-0)

[Reciprocity](#page-9-0)

[The Hilbert](#page-16-0) Class Field

As Euler continued using the descent and reciprocity steps for different values of n , he found that the reciprocity step became increasingly difficult to prove.

Why Reciprocity?

[Reciprocity](#page-9-0)

[The Hilbert](#page-16-0) Class Field

As Euler continued using the descent and reciprocity steps for different values of n , he found that the reciprocity step became increasingly difficult to prove.

KORKARYKERKER POLO

Three main types of reciprocity are:

- **1** Quadratic Reciprocity
- 2 Cubic Reciprocity $(\mathbb{Z}[\omega])$
- **3** Biquadratic Reciprocity $(\mathbb{Z}[i])$.

Quadratic Reciprocity

[Primes of the](#page-0-0) Form
 $x^2 + ny^2$

Define

[Descent and](#page-2-0)

[Reciprocity](#page-9-0)

[The Hilbert](#page-16-0) Class Field

\int a p $=$ $\sqrt{ }$ \int $\overline{\mathcal{L}}$ 0 $p|a$ 1 p $\nmid a, a$ is a quadratic residue mod p -1 p $\nmid a, a$ is a quadratic nonresidue mod p

K ロ ▶ K 個 ▶ K 할 ▶ K 할 ▶ 이 할 → 이익(연

Quadratic Reciprocity

[Primes of the](#page-0-0) Form
 $x^2 + ny^2$

[Descent and](#page-2-0)

[Reciprocity](#page-9-0)

[The Hilbert](#page-16-0) Class Field

$$
\left(\frac{a}{p}\right) = \begin{cases} 0 & p|a \\ 1 & p \nmid a, a \text{ is a quadratic residue mod } p \\ -1 & p \nmid a, a \text{ is a quadratic nonresidue mod } p \end{cases}
$$

We then have

Define

$$
p|x^2 + ny^2, \gcd(x, y) = 1 \iff \left(\frac{-n}{p}\right) = 1
$$

K ロ ▶ K 레 ▶ K 코 ▶ K 코 ▶ 『코 │ ◆ 9 Q Q ↓

Cubic Reciprocity

[Primes of the](#page-0-0) Form
 $x^2 + ny^2$

[Descent and](#page-2-0)

[Reciprocity](#page-9-0)

[The Hilbert](#page-16-0) Class Field

Define

$$
\alpha^{\frac{N(\pi)-1}{3}}=\left(\frac{a}{\pi}\right)_3 \text{ mod } \pi
$$

KORK ERKER ADAM ADA

for a prime π not dividing 3, and norm $N(\pi) = \pi \bar{\pi}$.

This can take on the values $1, \omega$, and ω^2 .

Cubic Reciprocity

[Primes of the](#page-0-0) Form
 $x^2 + ny^2$

[Descent and](#page-2-0)

[Reciprocity](#page-9-0)

[The Hilbert](#page-16-0) Class Field

Define

$$
\alpha^{\frac{N(\pi)-1}{3}}=\left(\frac{a}{\pi}\right)_3 \text{ mod } \pi
$$

for a prime π not dividing 3, and norm $N(\pi) = \pi \bar{\pi}$.

This can take on the values $1, \omega$, and ω^2 . Similar to before, we have

$$
\left(\frac{a}{\pi}\right)_3 = 1 \iff x^3 \equiv \alpha \text{ mod } \pi \text{ has a solution.}
$$

KORKARYKERKER POLO

Cubic Reciprocity

[Descent and](#page-2-0)

[Reciprocity](#page-9-0)

[The Hilbert](#page-16-0) Class Field

This definition of cubic reciprocity can be used to prove the following:

$$
x^3 \equiv a \bmod p \text{ is solvable in } \mathbb{Z} \iff \left(\frac{a}{\pi}\right) = 1, p = \pi \bar{\pi}
$$

 $p = x^2 + 27y^2 \iff p \equiv 1$ mod 3, 2 is a cubic residue modulo p

KORK STRAIN A STRAIN A COMP

[Primes of the](#page-0-0) Form
 $x^2 + ny^2$

[The Hilbert](#page-16-0) Class Field

The *ramification index* of a prime in a field L is a property defined by the exponent of that prime in the product of the factorization of the ring of integers of L with a prime ideal p.

[Primes of the](#page-0-0) Form
 $x^2 + ny^2$

[The Hilbert](#page-16-0) Class Field

The *ramification index* of a prime in a field L is a property defined by the exponent of that prime in the product of the factorization of the ring of integers of L with a prime ideal p. The inertial degree of p is the degree of the residue field extension of the ring of integers of L over said prime.

KORKARYKERKER POLO

[Primes of the](#page-0-0) Form
 $x^2 + ny^2$

[The Hilbert](#page-16-0) Class Field

The *ramification index* of a prime in a field L is a property defined by the exponent of that prime in the product of the factorization of the ring of integers of L with a prime ideal p. The inertial degree of p is the degree of the residue field extension of the ring of integers of L over said prime.

If the ramification index and the inertial degree of a prime are both equal to 1, then we say that the prime *splits completely* in L.

KORKARYKERKER POLO

[Primes of the](#page-0-0) Form
 $x^2 + ny^2$

[The Hilbert](#page-16-0) Class Field

The *ramification index* of a prime in a field L is a property defined by the exponent of that prime in the product of the factorization of the ring of integers of L with a prime ideal p. The inertial degree of p is the degree of the residue field extension of the ring of integers of L over said prime.

If the ramification index and the inertial degree of a prime are both equal to 1, then we say that the prime *splits completely* in L.

In fact, in the case of a Galois extension, the inertial degree and ramification indices of all primes in the factorization are equal, so we say that $\mathfrak p$ splits completely in L .

The Hilbert Class Field

[Descent and](#page-2-0)

[The Hilbert](#page-16-0) Class Field

Using some group theory and the Hilbert class field, it turns out that we can derive the following theorem:

 $p = x^2 + n y^2 \iff p$ splits completely in L .

KORKARYKERKER POLO