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

– Primes, Quadratic Forms, and Hilbert Class Field Theory

수리과학부 19학번
조영훈

2023 Winter Math Seminar

March 1, 2023

Overview

Fermat's Marginal Notes

Every prime number which surpasses by one a multiple of four is composed of two squares. ($p \equiv 1 \pmod 4 \implies p = x^2 + y^2$)

Every prime number which surpasses by one or three a multiple of eight is composed of a square and the double of another square. ($p \equiv 1, 3 \pmod 8 \implies p = x^2 + 2y^2$)

Every prime number which surpasses by one a multiple of three is composed of a square and the triple of another square. ($p \equiv 1 \pmod 3 \implies p = x^2 + 3y^2$)

- Pierre de Fermat, 1658.

... But where are the proofs?

Euler's Two-Step Strategy

Fermat's $4k+1$ Theorem

An odd prime p can be written as x^2+y^2 if and only if $p \equiv 1 \pmod 4$.

Proof. ($\Rightarrow$) is obvious. We prove ($\Leftarrow$) part.

- **Reciprocity Step**: $p \equiv 1 \pmod 4 \implies p \mid a^2+b^2, \gcd(a,b)=1$.
- **Descent Step**: $p \mid a^2+b^2, \gcd(a,b)=1 \implies p = x^2+y^2$.

The Reciprocity Step

- **Reciprocity Step**: $p \equiv 1 \pmod 4 \implies p \mid a^2 + b^2$, $\gcd(a, b) = 1$.

In modern language, it is essentially

$$p \equiv 1 \pmod 4 \implies \left(\frac{-1}{p}\right) = 1,$$

and it is easy to show:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1.$$

The Method of Infinite Descent

- **Descent Step**: $p \mid a^2 + b^2$, $\gcd(a, b) = 1 \implies p = x^2 + y^2$.

We begin with the classical identity

$$(x^2 + y^2)(z^2 + w^2) = (xz \pm yw)^2 + (xw \mp yz)^2.$$

Lemma

$q = x^2 + y^2 \mid N = a^2 + b^2$, $\gcd(a, b) = 1$, then $N/q = c^2 + d^2$.

WLOG, assume that $|a|, |b| < \frac{p}{2}$.

Then, all prime divisors $q \neq p$ of $N = a^2 + b^2$ are less than p.

If all such q's were $x^2 + y^2$, then we are done by the above Lemma.

Otherwise, apply the method of infinite descent. □

(Analogous proofs can be applied to the cases $n = 2, 3$.)

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

The $x^2 + ny^2$ Problem

Given $n \in \mathbb{N}$, a prime p can be written as $x^2 + ny^2$ if and only if ...

What can be the analogous of **Reciprocity Step** and **Descent Step**?

Theory of Quadratic Residues

Reciprocity Step is quite accessible:

$$p \mid a^2 + nb^2, \gcd(a, b) = 1 \iff \left(\frac{-n}{p}\right) = 1.$$

Given N, how can we determine if $\left(\frac{N}{p}\right) = 1$?

- $(-3/p) = 1 \iff p \equiv 1, 7 \pmod{12}$
- $(5/p) = 1 \iff p \equiv \pm 1, \pm 11 \pmod{20}$
- $(6/p) = 1 \iff p \equiv \pm 1, \pm 5 \pmod{24}$

Guess. $(N/p) = 1 \iff p \equiv \alpha \pmod{4N}$ for certain α's?

Theory of Quadratic Residues

Theorem

$D \equiv 0, 1 \pmod 4$ is a nonzero integer. Then there is a unique homomorphism $\chi : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ such that $\chi([p]) = (D/p)$ for odd primes $p \nmid D$.

Corollary

Let $D = -4n$, then

$$\left(\frac{-n}{p}\right) = 1 \iff [p] \in \ker \chi \subset (\mathbb{Z}/D\mathbb{Z})^\times.$$

Theory of Quadratic Residues

Its proof heavily relies on the quadratic reciprocity:

Quadratic Reciprocity for Jacobi Symbols

- $(-1/m) = (-1)^{(m-1)/2}$
- $(2/m) = (-1)^{(m^2-1)/8}$
- $(M/m) = (-1)^{(M-1)(m-1)/4}(m/M)$

Corollary

If $m \equiv n \pmod{D}$ are positive odds, $D \equiv 0, 1 \pmod{4}$, then $(D/m) = (D/n)$.

Hence, $\chi([p]) = (D/p)$ for odd primes $p \nmid D$ gives a well-defined homomorphism $\chi : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$.

Failure of Descent Step

But, **Descent Step** seems quite complicated...

Hopefully, we still have the analogous identity

$$(x^2 + ny^2)(z^2 + nw^2) = (xz \pm nyw)^2 + n(xw \mp yz)^2.$$

Q. Possible Generalization of Descent Step

$p \mid N = a^2 + nb^2$, then $p = x^2 + ny^2$?

But this fails even for $n = 5$:

$$3 \mid 21 = 1^2 + 5 \cdot 2^2, \qquad 3 \neq x^2 + 5y^2.$$

More Conjectures from Euler

Euler stated more conjectures on primes of the form $x^2 + ny^2$:

(1) $$p = x^2 + 5y^2 \iff p \equiv 1, 9 \pmod{20}$$

(Note that $(-5/p) = 1 \iff p \equiv 1, 3, 7, 9 \pmod{20}$.)

(2) $$p = \begin{cases} x^2 + 14y^2 \\ 2x^2 + 7y^2 \end{cases} \iff p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}$$

(Note that $(-7/p) = 1 \iff p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \pmod{56}$.)

More Conjectures from Euler

(3) $$p = x^2 + 27y^2 \iff \begin{cases} \left(\frac{-27}{p}\right) = 1, \\ 2 \text{ is a cubic residue } \bmod p \end{cases}$$

(4) $$p = x^2 + 64y^2 \iff \begin{cases} \left(\frac{-64}{p}\right) = 1, \\ 2 \text{ is a quartic residue } \bmod p \end{cases}$$

Lagrange's Theory of Quadratic Forms

Q. Which integer m can be represented as $m = x^2 + ny^2$?

Definition

- An integral quadratic form

$$f(x,y) = ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \quad a, b, c \in \mathbb{Z}$$

  is *primitive* if $\gcd(a,b,c) = 1$. (We will deal exclusively with primitive forms.)
- An integer m is *represented* by a form $f(x,y)$ if $m = f(x,y)$ for some x, y.
- Moreover, m is *properly represented* if such x, y are relatively prime.

Q. Given a primitive form $f(x,y)$, which integer m is properly represented by f?

Lagrange's Theory of Quadratic Forms

Definition

- Two forms $f(x,y), g(x,y)$ are *equivalent* if

$$f(x,y) = g(px+qy, rx+sy)$$

  for some $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{Z})$.
- Moreover, $f(x,y), g(x,y)$ are *properly equivalent* if $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$, and *improperly equivalent* otherwise.

Note that equivalent forms (properly) represent the same numbers.

Lagrange's Theory of Quadratic Forms

Also note that the equivalence relation preserves discriminant:

Definition

- The *discriminant* of a form $f(x,y) = ax^2 + bxy + cy^2$ is

$$\operatorname{disc} f = b^2 - 4ac = -4\det\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

- The *(form) class group* $C(D)$ is the collection of proper equivalence classes of the forms of discriminant D.
- The *class number* $h(D)$ is the cardinality of $C(D)$.

FACT

For every integer $D \equiv 0, 1 \pmod 4$, $h(D)$ is finite.

Quadratic Form and Quadratic Residue

However, we have the following consequence:

Lemma

A form $f(x,y)$ properly represents m if and only if $f(x,y)$ is properly equivalent to $mx^2+Bxy+Cy^2$ for some B,C.

Proposition

Let $D \equiv 0,1 \pmod 4$ and m be an odd integer relatively prime to D. Then, m is properly represented by a primitive form of discriminant D if and only if D is a quadratic residue $\bmod m$.

Proof.

($\Rightarrow$) WLOG $f(x,y)=mx^2+bxy+cy^2$. Then, $D=b^2-4mc\equiv b^2 \pmod m$.

($\Leftarrow$) $D\equiv b^2 \pmod m$, so WLOG $D\equiv b^2 \pmod{4m}$.

Write $D=b^2-4mc$, then for $f(x,y)=mx^2+bxy+cy^2$, $m=f(1,0)$. □

Quadratic Form and Quadratic Residue

Proposition

Let $D \equiv 0, 1 \pmod 4$ and m be an odd integer relatively prime to D. Then, m is properly represented by a primitive form of discriminant D if and only if D is a quadratic residue $\bmod\ m$.

Corollary

$(-n/p) = 1$ if and only if p is represented by a primitive form of discriminant $-4n$.

- Recall that we already got $(-n/p) = 1$ condition in **Reciprocity Step**.
- If $h(-4n) = 1$, then we are done!

Quadratic Form and Quadratic Residue

- Recall that we already got $(-n/p) = 1$ condition in **Reciprocity Step**.
- If $h(-4n) = 1$, then we are done!

FACT

$h(-4n) = 1 \iff n = 1, 2, 3, 4, 7.$

(Uniqueness problem for $D > 0$ is much more complicated.)

Corollary

If $n = 1, 2, 3, 4, 7$, then

$$p = x^2 + ny^2 \iff \left(\frac{-n}{p}\right) = 1 \iff [p] \in \ker\chi \subset (\mathbb{Z}/4n\mathbb{Z})^\times .$$

... We need to refine our theory further.

The Failure of Quadratic Residue Condition

The first failure is the case when $n = 5$:

$$C(-20) = \{[x^2 + 5y^2], [2x^2 + 2xy + 3y^2]\}.$$

Also recall Euler's conjecture:

$$(1) \qquad \begin{cases} p = x^2 + 5y^2 & \iff p \equiv 1, 9 \pmod{20} \\ 2p = x^2 + 5y^2 & \iff p \equiv 3, 7 \pmod{20} \end{cases}$$

However, we can observe that

$$x^2 + 5y^2 \text{ represents } m \implies m \equiv 1, 9 \pmod{20}$$
$$2x^2 + 2xy + 3y^2 \text{ represents } m \implies m \equiv 3, 7 \pmod{20}$$

Genus Theory

Definition

Given $D < 0$.

- Two forms of discriminant D are in the same *genus* if they represent the same values in $\ker\chi \subset (\mathbb{Z}/D\mathbb{Z})^\times$.
- The *principal form* of discriminant D is

$$\begin{cases} x^2 - \frac{D}{4}y^2 & \text{if } D \equiv 0 \pmod 4 \\ \left(x + \frac{y}{2}\right)^2 - \frac{D}{4}y^2 & \text{if } D \equiv 1 \pmod 4 \end{cases}$$

- Let $H \subset \ker\chi \subset (\mathbb{Z}/D\mathbb{Z})^\times$ be the values represented by the principal genus.

Genus Theory

Theorem

Given $D < 0$.

(a) H forms a subgroup of $\ker\chi \subset (\mathbb{Z}/D\mathbb{Z})^\times$.

(b) The values $H' \subset \ker\chi$ represented by a genus forms a coset of H.

(c) If $D = -4n$, then $H = \{k^2, k^2 + n \pmod{D}\}$.

(d) If $D = 1 - 4n$, then $H = \{k^2 \pmod{D}\}$.

Proof.

(a) $(x^2 + ny^2)(z^2 + nw^2) = (xz \pm nyw)^2 + n(xw \mp yz)^2$.

(b) $af(x, y) = (ax + \frac{b}{2}y)^2 - \frac{D}{4}y^2 \implies H' = [a]^{-1}H$.

(c) $x^2 + ny^2 \equiv x^2$ or $x^2 + n \pmod{4n}$. □

Genus Theory

Corollary

- p is represented by the principal genus of discriminant $-4n$ if and only if

$$p \equiv k^2, k^2 + n \pmod{4n}.$$

- Especially, if the principal genus consists of only one class, then it implies that p is of the form $x^2 + ny^2$.
  (Example: $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, \ldots$)

For $n = 14$, the principal genus consists of two classes:

(2) $$p = \begin{cases} x^2 + 14y^2 \\ 2x^2 + 7y^2 \end{cases} \iff p \equiv 1^2, 3^2, 5^2, 1^2 + 14, 3^2 + 14, 5^2 + 14 \pmod{56}$$

Multiplication between Classes

- The genera of forms has a group structure as $\ker\chi/H$.
- Recall the identity

$$(x^2+ny^2)(z^2+nw^2)=(xz\pm nyw)^2+n(xw\mp yz)^2.$$

- Also, we can observe that

$$(2x^2+2xy+3y^2)(2z^2+2zw+3w^2)=(2xz+xw+yz+3yw)^2+5(xw-yz)^2.$$

These suggests that the class group $C(D)$ is *indeed* a group.

Multiplication between Classes

The *composition* $[F(x,y)]$ of two classes $[f(x,y)],[g(x,y)]$ is the class satisfying

$$f(x,y)g(z,w) = F(B_1(x,y;z,w), B_2(x,y;z,w))$$

where

$$B_i(x,y;z,w) = a_i xz + b_i xw + c_i yz + d_i yw.$$

... But is it well-defined?

Actually, it results in a multi-valued operation, so we have to define it more carefully.

Composition of Forms

A variety of definitions of composition has been given. (e.g. Gauss, Bhargava) We present Dirichlet's definition here.

Definition

Assume that $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = a'x^2 + b'xy + c'y^2$ have discriminant $D < 0$, satisfy $\gcd(a, a', \frac{b+b'}{2}) = 1$. Then, there exists an integer B, unique up to $\bmod 2aa'$, such that

$$B \equiv b \pmod{2a}, \quad B \equiv b' \pmod{2a'}, \quad B^2 \equiv D \pmod{4aa'}.$$

The *composition* of $f(x,y)$ and $g(x,y)$ is the form

$$F(x,y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2.$$

The Class *Group*

Theorem

Given $D < 0$.

- The composition induces a well-defined binary operation on $C(D)$, which makes $C(D)$ into a finite abelian group of order $h(D)$.
- The principal class is the identity element of $C(D)$.
- The inverse of the class $[ax^2 + bxy + cy^2]$ is the class $[ax^2 - bxy + cy^2]$.

Genus Theory Revisited

Sending a class to the coset of $H \subset \ker \chi$ it represents defines a group homomorphism

$$\Phi : C(D) \to \ker \chi / H.$$

Since H contains all squares in $(\mathbb{Z}/D\mathbb{Z})^\times$, we can see that

- $\ker \chi / H \cong \{\pm 1\}^m$ for some m;
- the number of genera of discriminant D is a power of 2;
- $C(D)^2 \subset \ker \Phi$, i.e., $C(D)^2$ is contained in the principal genus.

Genus Theory Revisited

However, we can say something more.

Definition

Given $D < 0$. Let $p_1, \ldots, p_r$ be the odd primes dividing D. Consider

$$\chi_i(a) = (a/p_i), \quad \delta(a) = (-1)^{(a-1)/2}, \quad \epsilon(a) = (-1)^{(a^2-1)/8}.$$

Then the *assigned characters* for D are:

$D \equiv 1 \pmod 4$	$\chi_1, \ldots, \chi_r$
$D = 4n,\ n \equiv 3 \pmod 4$	$\chi_1, \ldots, \chi_r$
$D = 4n,\ n \equiv 1 \pmod 4$	$\chi_1, \ldots, \chi_r, \delta$
$D = 4n,\ n \equiv 4 \pmod 8$	$\chi_1, \ldots, \chi_r, \delta$
$D = 4n,\ n \equiv 6 \pmod 8$	$\chi_1, \ldots, \chi_r, \epsilon$
$D = 4n,\ n \equiv 2 \pmod 8$	$\chi_1, \ldots, \chi_r, \delta\epsilon$
$D = 4n,\ n \equiv 0 \pmod 8$	$\chi_1, \ldots, \chi_r, \delta, \epsilon$

The number of assigned characters is denoted by μ.

Genus Theory Revisited

- The assigned characters give a homomorphism

$$\Psi : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}^\mu,$$

  and its kernel is H.
- $|(\mathbb{Z}/D\mathbb{Z})^\times : \ker \chi| = 2$, so $\ker \chi/H \cong \{\pm 1\}^{\mu-1}$.
- We can check that $C(D)$ has exactly $2^{\mu-1}$ elements of order ≤ 2.

Thus, $\ker \Phi = C(D)^2$, and we get an induced isomorphism

$$C(D)/C(D)^2 \xrightarrow{\sim} \ker \chi/H \cong \{\pm 1\}^{\mu-1}.$$

Euler's Conjectures Revisited

(3) $$p = x^2 + 27y^2 \iff \begin{cases} \left(\frac{-27}{p}\right) = 1, \\ 2 \text{ is a cubic residue } \bmod p \end{cases}$$

Note that with the genus theory, only a partial result can be achieved:

$$p = \begin{cases} x^2 + 27y^2 \\ 4x^2 + 2xy + 7y^2 \end{cases} \iff \left(\frac{-27}{p}\right) = 1.$$

Euler's Conjectures Revisited

(3) $$p = x^2 + 27y^2 \iff \begin{cases} \left(\frac{-27}{p}\right) = 1, \\ 2 \text{ is a cubic residue} \bmod p \end{cases}$$

(4) $$p = x^2 + 64y^2 \iff \begin{cases} \left(\frac{-64}{p}\right) = 1, \\ 2 \text{ is a quartic residue} \bmod p \end{cases}$$

Where do the cubic and quartic residues emerge?

Recall: Modern Algebra I

The ring $\mathbb{Z}[\omega]$

- $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ where $\omega = e^{2\pi i/3} = (-1 + \sqrt{3})/2$.
- The *norm* of $\alpha \in \mathbb{Z}[\omega]$ is $N(\alpha) = \alpha\bar{\alpha}$.
- $\mathbb{Z}[\omega]$ is a ED, so is a PID and a UFD.
- $\alpha \in \mathbb{Z}[\omega]^\times \iff N(\alpha) = 1 \iff \alpha \in \{\pm 1, \pm\omega, \pm\omega^2\}$.
- Let p be a prime in $\mathbb{Z}$.
  - (a) If $p = 3$, then $1 - \omega$ is prime in $\mathbb{Z}[\omega]$ and $3 = -\omega^2(1 - \omega)^2$. ($3$ ramifies.)
  - (b) If $p \equiv 1 \pmod 3$, then there is a prime $\pi \in \mathbb{Z}[\omega]$ such that p decomposes into $p = \pi\bar{\pi}$, and $\pi, \bar{\pi}$ are nonassociate in $\mathbb{Z}[\omega]$. (p splits completely.)
  - (c) If $p \equiv 2 \pmod 3$, then p remains prime in $\mathbb{Z}[\omega]$. (p inerts.)

Theory of Cubic Residues

Fix a prime $\pi \in \mathbb{Z}[\omega]$ nonassociate to $1-\omega$.

Then $\pi\mathbb{Z}[\omega]$ is a maximal ideal, so $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is a field of $N(\pi)$ elements.

Hence, $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^\times$ is a finite group of order $N(\pi)-1$.

Fermat's Little Theorem

If $\alpha \in \mathbb{Z}[\omega]$ is not a multiple of π, then

$$\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}.$$

Legendre Symbol for Cubic Residues

The *Legendre symbol* $(\alpha/\pi)_3$ is the unique cubic root of unity such that

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{(N(\pi)-1)/3} \pmod{\pi}.$$

Cubic Reciprocity

A prime $\pi \in \mathbb{Z}[\omega]$ is *primary* if $\pi \equiv \pm 1 \pmod 3$.

The Law of Cubic Reciprocity

If π and θ are primary primes in $\mathbb{Z}[\omega]$ of unequal norms, then

$$\left(\frac{\theta}{\pi}\right)_3 = \left(\frac{\pi}{\theta}\right)_3.$$

Supplementary Laws

If $\pi \equiv -1 \pmod 3$ is a prime in $\mathbb{Z}[\omega]$, $\pi = -1 + 3m + 3n\omega$, then

$$\left(\frac{\omega}{\pi}\right)_3 = \omega^{m+n}, \qquad \left(\frac{1-\omega}{\pi}\right)_3 = \omega^{2m}.$$

Primes of the form $x^2 + 27y^2$

$$(3) \qquad p = x^2 + 27y^2 \iff \begin{cases} \left(\dfrac{-27}{p}\right) = 1, \\ 2 \text{ is a cubic residue } \bmod p \end{cases}$$

Proof.

($\Rightarrow$) $p = x^2 + 27y^2 \implies (-27/p) = 1 \implies p \equiv 1 \pmod 3$.
Let $\pi = x + 3\sqrt{-3}y$ so that $p = \pi\bar{\pi}$, then π is a prime in $\mathbb{Z}[\omega]$.
Since there is a natural isomorphism $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$,

$$2 \text{ is a cubic residue } \bmod p \iff \left(\frac{2}{\pi}\right)_3 = 1.$$

However, $(2/\pi)_3 = (\pi/2)_3 \equiv \pi^{(N(2)-1)/3} \equiv \pi \equiv 1 \pmod 2$. (check)

Primes of the form $x^2 + 27y^2$

(3) $$p = x^2 + 27y^2 \iff \begin{cases} \left(\frac{-27}{p}\right) = 1, \\ 2 \text{ is a cubic residue } \bmod p \end{cases}$$

Proof.

($\Leftarrow$) Write $p = \pi\bar{\pi}$ for a primary prime $\pi = a + 3b\omega \in \mathbb{Z}[\omega]$.

Then we have

$$4p = 4\pi\bar{\pi} = 4(a^2 - 3ab + 9b^2) = (2a - 3b)^2 + 27b^2.$$

However, $(\pi/2)_3 = (2/\pi)_3 = 1$ implies that $\pi \equiv 1 \pmod 2$, so a is odd, b is even. Hence, $p = x^2 + 27y^2$. □

Recall: Modern Algebra I

The ring $\mathbb{Z}[i]$

- $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.
- The *norm* of $\alpha \in \mathbb{Z}[i]$ is $N(\alpha) = \alpha\bar{\alpha}$.
- $\mathbb{Z}[i]$ is a ED, so is a PID and a UFD.
- $\alpha \in \mathbb{Z}[i]^\times \iff N(\alpha) = 1 \iff \alpha \in \{\pm 1, \pm i\}$.
- Let p be a prime in $\mathbb{Z}$.
  - (a) If $p = 2$, then $1 + i$ is prime in $\mathbb{Z}[i]$ and $2 = i^3(1 + i)^2$. (2 ramifies.)
  - (b) If $p \equiv 1 \pmod 4$, then there is a prime $\pi \in \mathbb{Z}[i]$ such that p decomposes into $p = \pi\bar{\pi}$, and $\pi, \bar{\pi}$ are nonassociate in $\mathbb{Z}[i]$. (p splits completely.)
  - (c) If $p \equiv 3 \pmod 4$, then p remains prime in $\mathbb{Z}[i]$. (p inerts.)

Theory of Quartic Residues

Fix a prime $\pi \in \mathbb{Z}[i]$ nonassociate to $1+i$.

Then $\pi\mathbb{Z}[i]$ is a maximal ideal, so $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ is a field of $N(\pi)$ elements.

Hence, $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^\times$ is a finite group of order $N(\pi)-1$.

Fermat's Little Theorem

If $\alpha \in \mathbb{Z}[i]$ is not a multiple of π, then

$$\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}.$$

Legendre Symbol for Quartic Residues

The *Legendre symbol* $(\alpha/\pi)_4$ is the unique quartic root of unity such that

$$\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{(N(\pi)-1)/4} \pmod{\pi}.$$

Quartic Reciprocity

A prime $\pi \in \mathbb{Z}[i]$ is *primary* if $\pi \equiv \pm 1 \pmod{2(1+i)}$.

The Law of Quartic Reciprocity

If π and θ are distinct primary primes in $\mathbb{Z}[i]$, then

$$\left(\frac{\theta}{\pi}\right)_4 = (-1)^{(N(\theta)-1)(N(\pi)-1)/16} \left(\frac{\pi}{\theta}\right)_4.$$

Supplementary Laws

If $\pi = a + bi$ is a primary prime in $\mathbb{Z}[i]$, then

$$\left(\frac{i}{\pi}\right)_4 = i^{-(a-1)/2}, \qquad \left(\frac{1+i}{\pi}\right)_4 = i^{(a-b-1-b^2)/4}.$$

Primes of the form $x^2 + 64y^2$

(4) $$p = x^2 + 64y^2 \iff \begin{cases} \left(\dfrac{-64}{p}\right) = 1, \\ 2 \text{ is a quartic residue } \bmod p \end{cases}$$

Proof.

($\Rightarrow$) $p = x^2 + 64y^2 \implies (-64/p) = 1 \implies p \equiv 1 \pmod 4$.

Let $\pi = x + 8iy$ so that $p = \pi\bar{\pi}$, then π is a prime in $\mathbb{Z}[i]$.

Since there is a natural isomorphism $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[i]/\pi\mathbb{Z}[i]$,

$$2 \text{ is a quartic residue } \bmod p \iff \left(\frac{2}{\pi}\right)_4 = 1.$$

However, $(2/\pi)_4 = i^{a \cdot 8b/2} = 1$. (check)

Primes of the form $x^2 + 64y^2$

(4) $$p = x^2 + 64y^2 \iff \begin{cases} \left(\frac{-64}{p}\right) = 1, \\ 2 \text{ is a quartic residue } \bmod p \end{cases}$$

Proof.

($\Leftarrow$) Write $p = \pi\bar{\pi}$ for a primary prime $\pi = a + bi \in \mathbb{Z}[i]$.

Then we have

$$p = \pi\bar{\pi} = a^2 + b^2.$$

However, $(2/\pi)_4 = i^{ab/2} = 1$ implies that b is divisible by 8. Hence, $p = x^2 + 64y^2$. □

Peeking at Further Generalization

The cubic and quartic residual conditions can be interpreted as:

$$x^3 - 2 \equiv 0 \pmod p, \quad x^4 - 2 \equiv 0 \pmod p \quad \text{has an integer solution.}$$

Guess

Given $n > 0$, there is a polynomial $f_n(x) \in \mathbb{Z}[x]$ such that

$$p = x^2 + ny^2 \iff \begin{cases} \left(\dfrac{-n}{p}\right) = 1, \\ f_n(x) \equiv 0 \pmod p \text{ has an integer solution.} \end{cases}$$

The Class Field Theory will enable us to establish such a theorem.

Number Fields

Definition

- A *number field* K is a finite extension of $\mathbb{Q}$.
- The *ring of integers* $\mathcal{O}_K$ of K is the set of algebraic integers of K, i.e., the set of all $\alpha \in K$ which are roots of a monic integer polynomial.
- Given a nonzero ideal $\mathfrak{a} \subset \mathcal{O}_K$, its *norm* is $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$.

FACT

- $\mathcal{O}_K$ is a subring of $\mathbb{C}$ whose field of fractions is K.
- $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Prime Factorization

In general, $\mathcal{O}_K$ is not a UFD. (e.g. $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$)

However, we have something similar.

FACT

$\mathcal{O}_K$ is a *Dedekind domain*, that is,

- $\mathcal{O}_K$ is integrally closed, i.e., if $\alpha \in K$ is a root of a monic polynomial with coefficients in $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$;
- $\mathcal{O}_K$ is Noetherian;
- Every nonzero prime ideal of $\mathcal{O}_K$ is maximal.

Corollary: Prime Factorization

Every nonzero ideal $\mathfrak{a} \subset \mathcal{O}_K$ can be uniquely written as a product of prime ideals. Furthermore, such ideals are exactly the prime ideals containing $\mathfrak{a}$.

Ramification of Primes

Consider number fields $L/K/\mathbb{Q}$, then $\mathcal{O}_K$ is a subring of $\mathcal{O}_L$.

For a prime $\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{p}\mathcal{O}_L \subset \mathcal{O}_L$ has a prime factorization

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}.$$

Definition

- The *ramification index* of $\mathfrak{p}$ in $\mathfrak{P}_i$ is $e_{\mathfrak{P}_i|\mathfrak{p}} = e_i$.
- The *inertial degree* of $\mathfrak{p}$ in $\mathfrak{P}_i$ is the degree $f_{\mathfrak{P}_i|\mathfrak{p}} = f_i$ of the residue field extension $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}_i$.

Theorem

$$\sum_{i=1}^{g} e_i f_i = [\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L : \mathcal{O}_K/\mathfrak{p}] = [L : K].$$

Ramification of Primes

Now we assume that L/K is Galois.

Theorem

- $\mathrm{Gal}(L/K)$ acts transitively on the primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$.
- $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ all have the same ramification index e and the same inertia degree f, so

$$efg = [L : K].$$

Definition

- $\mathfrak{p}$ *ramifies* if $e > 1$, and is *unramified* if $e = 1$.
- $\mathfrak{p}$ *splits completely* if $e = f = 1$.
- $\mathfrak{p}$ *inerts* (i.e., remains prime) if $e = g = 1$, $f > 1$.

Ideal Class Group

Definition

- A *fractional ideal* $\mathfrak{a} \subset K$ is a nonzero finitely generated $\mathcal{O}_K$-module, or equivalently, $\mathfrak{a} = \alpha\mathfrak{b}$ for $\alpha \in K$ and an ideal $\mathfrak{b} \subset \mathcal{O}_K$.
- The set of fractional ideals is denoted by I_K, and the set of principal fractional ideals is denoted by P_K.
- The *(ideal) class group* is $C(\mathcal{O}_K) = I_K/P_K$.
- The *class number* $h(\mathcal{O}_K)$ is the cardinality of $C(\mathcal{O}_K)$.

FACT

$C(\mathcal{O}_K)$ is a finite abelian group.

Remark

$h(\mathcal{O}_K) = 1$ if and only if $\mathcal{O}_K$ is a PID.

Quadratic Number Fields

Here, we consider the number field $K = \mathbb{Q}(\sqrt{N})$ where $N \neq 0, 1$ is squarefree.

Ring of Integer

- The *discriminant* of K is $d_K = \begin{cases} N & \text{if } N \equiv 1 \pmod 4, \\ 4N & \text{otw.} \end{cases}$
- The ring of integers is given by

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{d_K + \sqrt{d_K}}{2}\right] = \begin{cases} \mathbb{Z}[\sqrt{N}] & \text{if } N \not\equiv 1 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right] & \text{if } N \equiv 1 \pmod 4. \end{cases}$$

Note that for $K = \mathbb{Q}(\sqrt{-n})$,

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}] \iff n \text{ is squarefree, } n \not\equiv 3 \pmod 4.$$

Quadratic Number Fields

Units of $\mathbb{Q}(\sqrt{N})$

- For real quadratic fields ($d_K > 0$), $\mathcal{O}_K^\times$ is infinite. (Pell's equation)
- $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$, $\mathcal{O}_{\mathbb{Q}(i)}^\times = \{\pm 1, \pm i\}$.
- For other imaginary quadratic fields ($d_K < 0$), $\mathcal{O}_K = \{\pm 1\}$.

Primes of $\mathbb{Q}(\sqrt{N})$

Let p be a prime in $\mathbb{Z}$.

- If $(d_K/p) = 0$, then $p\mathcal{O}_K = \mathfrak{p}^2$ for a prime $\mathfrak{p} \subset \mathcal{O}_K$. ($p\mathbb{Z}$ ramifies.)
- If $(d_K/p) = 1$, then $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ where $\mathfrak{p} \neq \mathfrak{p}'$ are prime in $\mathcal{O}_K$. ($p\mathbb{Z}$ splits completely.)
- If $(d_K/p) = -1$, then $p\mathcal{O}_K \subset \mathcal{O}_K$ is a prime. ($p\mathbb{Z}$ inerts.)

Quadratic Number Fields

Class Group of $\mathbb{Q}(\sqrt{N})$

Let K be an imaginary quadratic field of discriminant $d_K < 0$.

- If $f(x,y) = ax^2 + bxy + cy^2$ is a primitive form of discriminant d_K, then

$$\left\langle a, \frac{-b+\sqrt{d_K}}{2} \right\rangle = \left\{ ma + n\frac{-b+\sqrt{d_K}}{2} : m, n \in \mathbb{Z} \right\}$$

  is an ideal of $\mathcal{O}_K$.

- The map $f(x,y) \mapsto \langle a, (-b+\sqrt{d_K})/2 \rangle$ induces an isomorphism between the form class group $C(d_K)$ and the ideal class group $C(\mathcal{O}_K)$.

The Artin Symbol

The Artin Symbol

Let L/K be a Galois extension, and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime unramified in L. If $\mathfrak{P} \subset \mathcal{O}_L$ contains $\mathfrak{p}\mathcal{O}_L$, then there is a unique element $\left(\frac{L/K}{\mathfrak{P}}\right) \in \mathrm{Gal}(L/K)$, called the *Artin symbol*, such that for all $\alpha \in \mathcal{O}_L$,

$$\left(\frac{L/K}{\mathfrak{P}}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}}.$$

FACT

- If $\sigma \in \mathrm{Gal}(L/K)$, then $\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}$.
- The order of $\left(\frac{L/K}{\mathfrak{P}}\right)$ is the inertial degree $f = f_{\mathfrak{P}|\mathfrak{p}}$.
- $\mathfrak{p}$ splits completely in L if and only if $\left(\frac{L/K}{\mathfrak{P}}\right) = 1$.

The Artin Map

Notes

- If L/K is abelian, then $\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1} = \left(\frac{L/K}{\mathfrak{P}}\right)$,
  so the Artin symbol only depends on the underlying prime $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{P}$.
  Hence, $\left(\frac{L/K}{\mathfrak{p}}\right) = \left(\frac{L/K}{\mathfrak{P}}\right)$ is well-defined.
- If L/K is unramified, then the Artin symbol can be defined with all $\mathfrak{p} \subset \mathcal{O}_K$.

The Artin Map

If L/K is an unramified abelian extension, then the Artin symbol defines the homomorphism, called the *Artin map*,

$$\left(\frac{L/K}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K).$$

The Hilbert Class Field

The Hilbert Class Field

Given a number field K, there exists the maximal unramified abelian extension $L = \mathrm{HCF}(K)$ of K, which is called the *Hilbert class field* of K.

The Artin Reciprocity Theorem

- If $L = \mathrm{HCF}(K)$, then the Artin map $\left(\frac{L/K}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K)$ is surjective, and its kernel is exactly the subgroup P_K of principal fractional ideals.
- Thus the Artin map induces an isomorphism $C(\mathcal{O}_K) \xrightarrow{\sim} \mathrm{Gal}(L/K)$.

Corollary

$\mathfrak{p}$ splits completely in $L \iff \left(\frac{L/K}{\mathfrak{p}}\right) = 1 \iff \mathfrak{p}$ is principal.

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

Let $K = \mathbb{Q}(\sqrt{-n})$ and $L = \mathrm{HCF}(K)$.

Assume that n is squarefree and $n \not\equiv 3 \pmod 4$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$.

Theorem

If $p \nmid n$ is an odd prime, then

$$p = x^2 + ny^2 \iff p \text{ splits completely in } L.$$

Proof.

$p = x^2 + ny^2$

$\iff p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, $\mathfrak{p} \neq \bar{\mathfrak{p}}$ and $\mathfrak{p}$ is principal in $\mathcal{O}_K$.

$\iff p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, $\mathfrak{p} \neq \bar{\mathfrak{p}}$ and $\mathfrak{p}$ splits completely in L.

$\iff p$ splits completely in L. ($\because L/\mathbb{Q}$ is Galois.) □

$$\begin{array}{ccccc} L & \supset & \mathcal{O}_L & \supset & \mathfrak{P}, \bar{\mathfrak{P}} \\ | & & | & & | \\ K & \supset & \mathcal{O}_K & \supset & \mathfrak{p}, \bar{\mathfrak{p}} \\ | & & | & & | \\ \mathbb{Q} & \supset & \mathbb{Z} & \supset & p\mathbb{Z} \end{array}$$

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

Theorem

Let K be an imaginary quadratic field, and let L be a finite extension of K which is Galois over $\mathbb{Q}$. Then:

- There is a real algebraic integer α such that $L = K(\alpha)$.
- Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α. If $p \nmid \operatorname{disc} f$ is a prime, then

$$p \text{ splits completely in } L \iff \begin{cases} \left(\dfrac{d_K}{p}\right) = 1, \\ f(x) \equiv 0 \pmod{p} \text{ has an integer solution.} \end{cases}$$

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

The Main Theorem

Let $n > 0$ be a squarefree integer, $n \not\equiv 3 \pmod 4$.

Then, there is a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree $h(-4n)$ such that if an odd prime p divides neither n nor $\operatorname{disc} f_n$, then

$$p = x^2 + ny^2 \iff \begin{cases} \left(\dfrac{-n}{p}\right) = 1, \\ f_n(x) \equiv 0 \pmod p \text{ has an integer solution.} \end{cases}$$

Furthermore, $f_n(x)$ may be taken to be the minimal polynomial of a real algebraic integer α for which $L = K(\alpha)$ is the Hilbert class field of $K = \mathbb{Q}(\sqrt{-n})$.

The Primes of the Form $x^2 + 14y^2$

Recall:

(5) $$p = \begin{cases} x^2 + 14y^2 \\ 2x^2 + 7y^2 \end{cases} \iff p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}$$

Let $K = \mathbb{Q}(\sqrt{-14})$ and $L = K(\alpha)$ where $\alpha = \sqrt{2\sqrt{2} - 1}$.
Since $h(-56) = 4$ and L is an unramified abelian extension of K of degree 4, L is the Hilbert class field of K. Note that α is a real integral primitive element of L over K, and its minimal polynomial is $f_{14}(x) = (x^2 + 1)^2 - 8$. Thus,

$$p = x^2 + 14y^2 \iff \begin{cases} \left(\frac{-14}{p}\right) = 1, \\ (x^2 + 1)^2 \equiv 8 \pmod{p} \text{ has an integer solution.} \end{cases}$$

Further Remarks

- Knowing $f_n(x)$ is equivalent to knowing the Hilbert class field.
- Actually, our main theorem is not applicable for $n = 27, 64$ since these are not squarefree.

  However, we can further generalize the main theorem for every $n > 0$, by using the *ring class field* of the order $\mathbb{Z}[\sqrt{-n}]$ in $\mathbb{Q}(\sqrt{-n})$ in place of the Hilbert class field.
- Our main theorem is not constructive. The constructive solution of $p = x^2 + ny^2$ is much more complicated.

References

- D. Cox, *Primes of the Form* $x^2 + ny^2$, Second Edition, Wiley, 2013.
- K. Ireland & M. Rosen, *A Classical Introduction to Modern Number Theory*, Second Edition, Springer, 1990.