Jacobsthal identity for $\mathbb{Q}(\sqrt{-2})$

Yifan Yang (with Ki-Ichiro Hashimoto and Ling Long)

National Chiao Tung University, Taiwan

5 November 2010, NCKU Colloquium

Jacobsthal's identity

Theorem (Fermat)

An odd prime p is a sum of two integer squares if and only if $p \equiv 1 \mod 4$.

Theorem (Jacobsthal)

Let p be a prime congruent to 1 modulo 4 and n be a quadratic nonresidue modulo p. Set

$$A = \frac{1}{2}\sum_{x=0}^{p-1}\left(\frac{x^3-x}{p}\right), \qquad B = \frac{1}{2}\sum_{x=0}^{p-1}\left(\frac{x^3-nx}{p}\right).$$

Then $A, B \in \mathbb{Z}$ and satisfies $p = A^2 + B^2$.

Jacobsthal's identity

Theorem (Fermat)

An odd prime p is a sum of two integer squares if and only if $p \equiv 1 \mod 4$.

Theorem (Jacobsthal)

Let p be a prime congruent to 1 *modulo* 4 *and n be a quadratic nonresidue modulo p. Set*

$$A = \frac{1}{2}\sum_{x=0}^{p-1}\left(\frac{x^3 - x}{p}\right), \qquad B = \frac{1}{2}\sum_{x=0}^{p-1}\left(\frac{x^3 - nx}{p}\right).$$

Then $A, B \in \mathbb{Z}$ and satisfies $p = A^2 + B^2$.

Legendre symbols

Definition

Let p be an odd prime. An integer a relatively prime to p is a quadratic residue (resp. quadratic nonresidue) modulo p if the congruence equation

$$x^2 \equiv a \mod p$$

is solvable (resp. unsolvable) in integers.

Definition

Let p be an odd prime. Then the Legendre symbol $\left(\frac{\cdot}{p}\right)$ is defined by

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

Legendre symbols

Definition

Let p be an odd prime. An integer a relatively prime to p is a quadratic residue (resp. quadratic nonresidue) modulo p if the congruence equation

$$x^2 \equiv a \mod p$$

is solvable (resp. unsolvable) in integers.

Definition

Let p be an odd prime. Then the Legendre symbol $\left(\frac{\cdot}{p}\right)$ is defined by

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

Properties of Legendre symbols

Definition

If $f(x) \in \mathbb{Z}[x]$, then we call

$$J_f(p) := \sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right)$$

a **Jacobsthal sum**.

Proposition

We have

- $\left(\frac{ab}{p} \right) = \left(\frac{a}{p} \right) \left(\frac{b}{p} \right)$.
- $\left(\frac{a}{p} \right) \equiv a^{(p-1)/2} \mod p$.

Properties of Legendre symbols

Definition

If $f(x) \in \mathbb{Z}[x]$, then we call

$$J_f(p) := \sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right)$$

a Jacobsthal sum.

Proposition

We have

- $\left(\frac{ab}{p} \right) = \left(\frac{a}{p} \right) \left(\frac{b}{p} \right)$,
- $\left(\frac{a}{p} \right) = a^{(p-1)/2} \mod p$.

Properties of Legendre symbols

Definition

If $f(x) \in \mathbb{Z}[x]$, then we call

$$J_f(p) := \sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right)$$

a Jacobsthal sum.

Proposition

We have

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,
- $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$.

Gauss' proof of the Jacobsthal identity

- Set $S(n) = \sum_{x=0}^{p-1} \left(\frac{x^3 - nx}{p} \right)$.
- Pairing the term $x = a$ with the term $x = p - a$, we find $S(n)$ is always even.
- Replacing x by rx, we find $S(r^2 n) = \left(\frac{r}{p} \right) S(n)$.
- Let g be a primitive root modulo p. The above shows

$$S(g) = -S(g^3) = S(g^5) = -S(g^7) = \ldots,$$

$$S(g^2) = -S(g^4) = S(g^6) = -S(g^8) = \ldots.$$

Gauss' proof of the Jacobsthal identity

- Set $S(n) = \sum_{x=0}^{p-1} \left(\frac{x^3 - nx}{p} \right)$.
- Pairing the term $x = a$ with the term $x = p - a$, we find $S(n)$ is always even.
- Replacing x by rx, we find $S(r^2 n) = \left(\frac{r}{p} \right) S(n)$.
- Let g be a primitive root modulo p. The above shows

$$S(g) = -S(g^3) = S(g^5) = -S(g^7) = \ldots,$$

$$S(g^2) = -S(g^4) = S(g^6) = -S(g^8) = \ldots.$$

Gauss' proof of the Jacobsthal identity

- Set $S(n) = \sum_{x=0}^{p-1} \left(\frac{x^3 - nx}{p}\right)$.
- Pairing the term $x = a$ with the term $x = p - a$, we find $S(n)$ is always even.
- Replacing x by rx, we find $S(r^2 n) = \left(\frac{r}{p}\right) S(n)$.
- Let g be a primitive root modulo p. The above shows

$$S(g) = -S(g^3) = S(g^5) = -S(g^7) = \dots,$$

$$S(g^2) = -S(g^4) = S(g^6) = -S(g^8) = \dots.$$

Gauss' proof of the Jacobsthal identity

- Set $S(n) = \sum_{x=0}^{p-1} \left(\frac{x^3 - nx}{p}\right)$.
- Pairing the term $x = a$ with the term $x = p - a$, we find $S(n)$ is always even.
- Replacing x by rx, we find $S(r^2 n) = \left(\frac{r}{p}\right) S(n)$.
- Let g be a primitive root modulo p. The above shows

$$S(g) = -S(g^3) = S(g^5) = -S(g^7) = \dots,$$

$$S(g^2) = -S(g^4) = S(g^6) = -S(g^8) = \dots.$$

Gauss' proof of the Jacobsthal identity, continued

- Let $S(g) = 2A$ and $S(g^2) = 2B$. Then

$$2(p-1)(A^2+B^2) = \sum_{n,x,y=0}^{p-1} \left(\frac{x^3-nx}{p}\right)\left(\frac{y^3-ny}{p}\right)$$
$$= \sum_{x,y=0}^{p-1}\left(\frac{xy}{p}\right)\sum_{n=0}^{p-1}\left(\frac{(x^2-n)(y^2-n)}{p}\right).$$

- Using

$$\sum_{z=0}^{p-1}\left(\frac{z(z+r)}{p}\right) = \begin{cases} p-1, & \text{if } r \equiv 0 \mod p, \\ -1, & \text{if } r \not\equiv 0 \mod p, \end{cases}$$

we find

$$2(p-1)(A^2+B^2) = p\sum_{x,y=0}^{p-1}\delta_{x^2,y^2} = 2(p-1)p.$$

Gauss' proof of the Jacobsthal identity, continued

- Let $S(g) = 2A$ and $S(g^2) = 2B$. Then

$$2(p-1)(A^2+B^2) = \sum_{n,x,y=0}^{p-1} \left(\frac{x^3-nx}{p}\right)\left(\frac{y^3-ny}{p}\right)$$
$$= \sum_{x,y=0}^{p-1} \left(\frac{xy}{p}\right) \sum_{n=0}^{p-1} \left(\frac{(x^2-n)(y^2-n)}{p}\right).$$

- Using

$$\sum_{z=0}^{p-1} \left(\frac{z(z+r)}{p}\right) = \begin{cases} p-1, & \text{if } r \equiv 0 \mod p, \\ -1, & \text{if } r \not\equiv 0 \mod p, \end{cases}$$

we find

$$2(p-1)(A^2+B^2) = p \sum_{x,y=0}^{p-1} \delta_{x^2,y^2} = 2(p-1)p.$$

Idea.

Consider the elliptic curve $E_n : y^2 = x^3 - nx$. We have

$$\#E_n(\mathbb{F}_p) = 1 + \sum_{x=0}^{p-1}\left(1 + \left(\frac{x^3 - nx}{p}\right)\right) = p + 1 + \sum_{x=0}^{p-1}\left(\frac{x^3 - nx}{p}\right).$$

Thus,

$$L(E_n/\mathbb{Q}, s)^{-1} = \prod_p \left(1 + \sum_{x=0}^{p-1}\left(\frac{x^3 - nx}{p}\right)p^{-s} + p^{1-2s}\right).$$

Since E_1 and E_n are isomorphic over $\mathbb{Q}(\sqrt[4]{n})$, the two L-functions $L(E_1/\mathbb{Q}, s)$ and $L(E_n/\mathbb{Q}, s)$ must be related in some way, which give information about the Jacobsthal sums.

Arithmetic-geometric approach

Idea.

Consider the elliptic curve $E_n : y^2 = x^3 - nx$. We have

$$\#E_n(\mathbb{F}_p) = 1 + \sum_{x=0}^{p-1} \left(1 + \left(\frac{x^3 - nx}{p}\right)\right) = p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 - nx}{p}\right).$$

Thus,

$$L(E_n/\mathbb{Q}, s)^{-1} = \prod_p \left(1 + \sum_{x=0}^{p-1} \left(\frac{x^3 - nx}{p}\right) p^{-s} + p^{1-2s}\right).$$

Since E_1 and E_n are isomorphic over $\mathbb{Q}(\sqrt[4]{n})$, the two L-functions $L(E_1/\mathbb{Q}, s)$ and $L(E_n/\mathbb{Q}, s)$ must be related in some way, which give information about the Jacobsthal sums.

Arithmetic-geometric approach

Idea.

Consider the elliptic curve $E_n : y^2 = x^3 - nx$. We have

$$\#E_n(\mathbb{F}_p) = 1 + \sum_{x=0}^{p-1}\left(1 + \left(\frac{x^3 - nx}{p}\right)\right) = p + 1 + \sum_{x=0}^{p-1}\left(\frac{x^3 - nx}{p}\right).$$

Thus,

$$L(E_n/\mathbb{Q}, s)^{-1} = \prod_p \left(1 + \sum_{x=0}^{p-1}\left(\frac{x^3 - nx}{p}\right) p^{-s} + p^{1-2s}\right).$$

Since E_1 and E_n are isomorphic over $\mathbb{Q}(\sqrt[4]{n})$, the two L-functions $L(E_1/\mathbb{Q}, s)$ and $L(E_n/\mathbb{Q}, s)$ must be related in some way, which give information about the Jacobsthal sums.

Tate modules and Galois representations

Let ℓ be a prime. Let E be an elliptic curve over a number field K and $E[\ell^n]$ be the subgroup of ℓ^n-torsion points.

Consider the Tate module

$$T_\ell(E) = \varprojlim E[\ell^n].$$

The absolute Galois group $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ acts on $T_\ell(E)$, yielding a Galois representation

$$\rho_{E,\ell} : G_K \to \mathrm{GL}(2, \mathbb{Q}_\ell).$$

Then $L(\rho_{E,\ell}, s) = L(E/K, s)$.

Tate modules and Galois representations

Let ℓ be a prime. Let E be an elliptic curve over a number field K and $E[\ell^n]$ be the subgroup of ℓ^n-torsion points.

Consider the Tate module

$$T_\ell(E) = \varprojlim E[\ell^n].$$

The absolute Galois group $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ acts on $T_\ell(E)$, yielding a Galois representation

$$\rho_{E,\ell} : G_K \to \mathrm{GL}(2, \mathbb{Q}_\ell).$$

Then $L(\rho_{E,\ell}, s) = L(E/K, s)$.

Tate modules and Galois representations

Let ℓ be a prime. Let E be an elliptic curve over a number field K and $E[\ell^n]$ be the subgroup of ℓ^n-torsion points.

Consider the Tate module

$$T_\ell(E) = \varprojlim E[\ell^n].$$

The absolute Galois group $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ acts on $T_\ell(E)$, yielding a Galois representation

$$\rho_{E,\ell} : G_K \to \mathrm{GL}(2, \mathbb{Q}_\ell).$$

Then $L(\rho_{E,\ell}, s) = L(E/K, s)$.

Tate modules and Galois representations

Let ℓ be a prime. Let E be an elliptic curve over a number field K and $E[\ell^n]$ be the subgroup of ℓ^n-torsion points.

Consider the Tate module

$$T_\ell(E) = \varprojlim E[\ell^n].$$

The absolute Galois group $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ acts on $T_\ell(E)$, yielding a Galois representation

$$\rho_{E,\ell} : G_K \to \mathrm{GL}(2, \mathbb{Q}_\ell).$$

Then $L(\rho_{E,\ell}, s) = L(E/K, s)$.

A lemma

Lemma (Clifford)

(Under suitable conditions on G and ρ) Assume that $H \lhd G$ and G/H is cyclic of finite order.

Assume that $\rho_1 : G \to \mathrm{GL}(V_1)$ and $\rho_2 : G \to \mathrm{GL}(V_2)$ are irreducible representations over an algebraically closed of characteristic not dividing $|G/H|$ such that $\rho_1\big|_H$ and $\rho_2\big|_H$ have a common isomorphic irreducible subrepresentations of H.

Then

$$\rho_1 \simeq \rho_2 \otimes \chi$$

for some representation of G of degree 1 that is lifted from that of G/H.

A lemma

Lemma (Clifford)

(Under suitable conditions on G and ρ) Assume that $H \lhd G$ and G/H is cyclic of finite order.

Assume that $\rho_1 : G \to \mathrm{GL}(V_1)$ and $\rho_2 : G \to \mathrm{GL}(V_2)$ are irreducible representations over an algebraically closed of characteristic not dividing $|G/H|$ such that $\rho_1\big|_H$ and $\rho_2\big|_H$ have a common isomorphic irreducible subrepresentations of H.

Then

$$\rho_1 \simeq \rho_2 \otimes \chi$$

for some representation of G of degree 1 that is lifted from that of G/H.

A lemma

Lemma (Clifford)

(Under suitable conditions on G and ρ) Assume that $H \lhd G$ and G/H is cyclic of finite order.

Assume that $\rho_1 : G \to \mathrm{GL}(V_1)$ and $\rho_2 : G \to \mathrm{GL}(V_2)$ are irreducible representations over an algebraically closed of characteristic not dividing $|G/H|$ such that $\rho_1\big|_H$ and $\rho_2\big|_H$ have a common isomorphic irreducible subrepresentations of H.

Then

$$\rho_1 \simeq \rho_2 \otimes \chi$$

for some representation of G of degree 1 that is lifted from that of G/H.

Arithmetic-geometric approach

Let $E_n : y^2 = x^3 - nx$. It is isomorphic to E_1 over $\mathbb{Q}(\sqrt[4]{n})$, which is not abelian over $\mathbb{Q}$.

Extend the base field to $K = \mathbb{Q}(i)$. Then $L = \mathbb{Q}(\sqrt[4]{n}, i)$ is cyclic over $\mathbb{Q}$. Let $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $G_L = \mathrm{Gal}(\overline{\mathbb{Q}}/L)$.

The elliptic curves E_n have CM by $\mathbb{Z}[i]$, so

$$\rho_{E_n,\ell}\big|_{G_K} = \pi_n \oplus \overline{\pi}_n,$$

where π_n are representations of G_K of degree 1.

Arithmetic-geometric approach

Let $E_n : y^2 = x^3 - nx$. It is isomorphic to E_1 over $\mathbb{Q}(\sqrt[4]{n})$, which is not abelian over $\mathbb{Q}$.

Extend the base field to $K = \mathbb{Q}(i)$. Then $L = \mathbb{Q}(\sqrt[4]{n}, i)$ is cyclic over $\mathbb{Q}$. Let $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $G_L = \mathrm{Gal}(\overline{\mathbb{Q}}/L)$.

The elliptic curves E_n have CM by $\mathbb{Z}[i]$, so

$$\rho_{E_n,\ell}\big|_{G_K} = \pi_n \oplus \overline{\pi}_n,$$

where π_n are representations of G_K of degree 1.

Arithmetic-geometric approach

Let $E_n : y^2 = x^3 - nx$. It is isomorphic to E_1 over $\mathbb{Q}(\sqrt[4]{n})$, which is not abelian over $\mathbb{Q}$.

Extend the base field to $K = \mathbb{Q}(i)$. Then $L = \mathbb{Q}(\sqrt[4]{n}, i)$ is cyclic over $\mathbb{Q}$. Let $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $G_L = \mathrm{Gal}(\overline{\mathbb{Q}}/L)$.

The elliptic curves E_n have CM by $\mathbb{Z}[i]$, so

$$\rho_{E_n,\ell}\big|_{G_K} = \pi_n \oplus \overline{\pi}_n,$$

where π_n are representations of G_K of degree 1.

Arithmetic-geometric approach

E_1/K and E_n/K are isomorphic over L, so

$$\pi_1\big|_{G_L} \simeq \pi_n\big|_{G_L}.$$

By the lemma above,

$$\pi_n = \pi_1 \otimes \chi$$

for some linear character χ on G_K with $G_L \subset \ker\chi$, i.e., a character on $G_K/G_L \simeq \mathrm{Gal}(L/K)$.

Arithmetic-geometric approach

E_1/K and E_n/K are isomorphic over L, so

$$\pi_1\big|_{G_L} \simeq \pi_n\big|_{G_L}.$$

By the lemma above,

$$\pi_n = \pi_1 \otimes \chi$$

for some linear character χ on G_K with $G_L \subset \ker\chi$, i.e., a character on $G_K/G_L \simeq \mathrm{Gal}(L/K)$.

Arithmetic-geometric approach

A character on G_K with $G_L \subset \ker\chi$ has the following description. The Galois group $\mathrm{Gal}(L/K)$ is generated by

$$\sigma : \sqrt[4]{n} \longmapsto i\sqrt[4]{n}.$$

For each prime $\mathfrak{p}$ of K not dividing $2n$, the Frobenius $\mathrm{Frob}_\mathfrak{p}$ is the element $\sigma^j \in \mathrm{Gal}(L/K)$ such that

$$\sigma^j(\sqrt[4]{n}) \equiv (\sqrt[4]{n})^{N\mathfrak{p}} \mod \mathfrak{p},$$

where $N\mathfrak{p}$ denotes the norm of $\mathfrak{p}$.

Then there exists $k \in \{1, 3\}$ such that χ satisfies

$$\chi(\mathrm{Frob}_\mathfrak{p}) = i^{jk}$$

for all $\mathfrak{p}$.

Arithmetic-geometric approach

A character on G_K with $G_L \subset \ker\chi$ has the following description. The Galois group $\mathrm{Gal}(L/K)$ is generated by

$$\sigma : \sqrt[4]{n} \longmapsto i\sqrt[4]{n}.$$

For each prime $\mathfrak{p}$ of K not dividing $2n$, the Frobenius $\mathrm{Frob}_\mathfrak{p}$ is the element $\sigma^j \in \mathrm{Gal}(L/K)$ such that

$$\sigma^j(\sqrt[4]{n}) \equiv (\sqrt[4]{n})^{N\mathfrak{p}} \mod \mathfrak{p},$$

where $N\mathfrak{p}$ denotes the norm of $\mathfrak{p}$.

Then there exists $k \in \{1, 3\}$ such that χ satisfies

$$\chi(\mathrm{Frob}_\mathfrak{p}) = i^{jk}$$

for all $\mathfrak{p}$.

Arithmetic-geometric approach

A character on G_K with $G_L \subset \ker\chi$ has the following description. The Galois group $\mathrm{Gal}(L/K)$ is generated by

$$\sigma : \sqrt[4]{n} \longmapsto i\sqrt[4]{n}.$$

For each prime $\mathfrak{p}$ of K not dividing $2n$, the Frobenius $\mathrm{Frob}_{\mathfrak{p}}$ is the element $\sigma^j \in \mathrm{Gal}(L/K)$ such that

$$\sigma^j(\sqrt[4]{n}) \equiv (\sqrt[4]{n})^{N\mathfrak{p}} \mod \mathfrak{p},$$

where $N\mathfrak{p}$ denotes the norm of $\mathfrak{p}$.

Then there exists $k \in \{1, 3\}$ such that χ satisfies

$$\chi(\mathrm{Frob}_{\mathfrak{p}}) = i^{jk}$$

for all $\mathfrak{p}$.

Proof of Jacobsthal's identity

Now for a prime $p \equiv 1 \mod 4$, a prime of K lying over p has norm p.

If n is a quadratic nonresidue modulo p, then

$$n^{(p-1)/2} \equiv -1 \mod p,$$

which implies that

$$(\sqrt[4]{n})^{N\mathfrak{p}} \equiv \pm i\sqrt[4]{n} \mod \mathfrak{p}.$$

That is,

$$\chi(\mathrm{Frob}_{\mathfrak{p}}) = \pm i.$$

Proof of Jacobsthal's identity

Now for a prime $p \equiv 1 \mod 4$, a prime of K lying over p has norm p.

If n is a quadratic nonresidue modulo p, then

$$n^{(p-1)/2} \equiv -1 \mod p,$$

which implies that

$$(\sqrt[4]{n})^{N\mathfrak{p}} \equiv \pm i\sqrt[4]{n} \mod \mathfrak{p}.$$

That is,

$$\chi(\mathrm{Frob}_{\mathfrak{p}}) = \pm i.$$

Proof of Jacobsthal's identity

Now for a prime $p \equiv 1 \mod 4$, a prime of K lying over p has norm p. If n is a quadratic nonresidue modulo p, then

$$n^{(p-1)/2} \equiv -1 \mod p,$$

which implies that

$$(\sqrt[4]{n})^{N\mathfrak{p}} \equiv \pm i \sqrt[4]{n} \mod \mathfrak{p}.$$

That is,

$$\chi(\mathrm{Frob}_{\mathfrak{p}}) = \pm i.$$

Proof of Jacobsthal's identity

It is well-known that

$$L(E_1/\mathbb{Q}, s) = \prod_{p\equiv 1 \mod 4} \frac{1}{1 - 2\epsilon_p a_p p^{-s} + p^{1-2s}} \prod_{p\equiv 3 \mod 4} \frac{1}{1 + p^{1-2s}},$$

where for $p \equiv 1 \mod 4$, a_p and b_p are positive integers with a_p odd and b_p even such that $p = a_p^2 + b_p^2$, and

$$\epsilon_p = \left(\frac{-1}{a_p}\right) (-1)^{b_p/2}.$$

Thus, for a prime $\mathfrak{p}$ of $K = \mathbb{Q}(i)$ lying over $p \equiv 1 \mod 4$,

$$\pi_1(\mathfrak{p}) = \pm a_p \pm b_p i$$

Then

$$\pi_n(\mathfrak{p}) = \pi_1(\mathfrak{p})\chi(\mathfrak{p}) = \pm b_p \pm a_p i$$

Proof of Jacobsthal's identity

It is well-known that

$$L(E_1/\mathbb{Q}, s) = \prod_{p\equiv 1 \mod 4} \frac{1}{1 - 2\epsilon_p a_p p^{-s} + p^{1-2s}} \prod_{p\equiv 3 \mod 4} \frac{1}{1 + p^{1-2s}},$$

where for $p \equiv 1 \mod 4$, a_p and b_p are positive integers with a_p odd and b_p even such that $p = a_p^2 + b_p^2$, and

$$\epsilon_p = \left(\frac{-1}{a_p}\right)(-1)^{b_p/2}.$$

Thus, for a prime $\mathfrak{p}$ of $K = \mathbb{Q}(i)$ lying over $p \equiv 1 \mod 4$,

$$\pi_1(\mathfrak{p}) = \pm a_p \pm b_p i$$

Then

$$\pi_n(\mathfrak{p}) = \pi_1(\mathfrak{p})\chi(\mathfrak{p}) = \pm b_p \pm a_p i$$

Proof of Jacobsthal's identity

It is well-known that

$$L(E_1/\mathbb{Q},s)=\prod_{p\equiv 1 \mod 4}\frac{1}{1-2\epsilon_p a_p p^{-s}+p^{1-2s}}\prod_{p\equiv 3 \mod 4}\frac{1}{1+p^{1-2s}},$$

where for $p\equiv 1 \mod 4$, a_p and b_p are positive integers with a_p odd and b_p even such that $p=a_p^2+b_p^2$, and

$$\epsilon_p=\left(\frac{-1}{a_p}\right)(-1)^{b_p/2}.$$

Thus, for a prime $\mathfrak{p}$ of $K=\mathbb{Q}(i)$ lying over $p\equiv 1 \mod 4$,

$$\pi_1(\mathfrak{p})=\pm a_p\pm b_p i$$

Then

$$\pi_n(\mathfrak{p})=\pi_1(\mathfrak{p})\chi(\mathfrak{p})=\pm b_p\pm a_p i$$

Proof of Jacobsthal's identity

Therefore, the p-factor of $L(E_n, s)$ is

$$(1 \pm 2b_p p^{-s} + p^{1-2s})^{-1}.$$

That is,

$$\sum_{x=0}^{p-1} \left(\frac{x^3 - nx}{p} \right) = \pm 2b_p,$$

which gives us the Jacobsthal identity.

Proof of Jacobsthal's identity

Therefore, the p-factor of $L(E_n, s)$ is

$$(1 \pm 2b_p p^{-s} + p^{1-2s})^{-1}.$$

That is,

$$\sum_{x=0}^{p-1} \left(\frac{x^3 - nx}{p} \right) = \pm 2b_p,$$

which gives us the Jacobsthal identity.

Cubic analogue of the Jacobsthal identity

Theorem (Chan-Long-Y)

Let $p \equiv 1 \mod 6$*. Assume that* n *is an integer such that* $x^3 \equiv n \mod p$ *is not solvable in integers. Set*

$$A = \sum_{x=0}^{p-1} \left(\frac{x^3 - 1}{p} \right), \qquad B = \sum_{x=0}^{p-1} \left(\frac{x^3 - n}{p} \right).$$

Then

$$A^2 + AB + B^2 = 3p.$$

Cubic analogue of the Jacobsthal identity

Theorem (Chan-Long-Y)

Let $p \equiv 1 \mod 6$*. Assume that* n *is an integer such that* $x^3 \equiv n \mod p$ *is not solvable in integers. Set*

$$A = \sum_{x=0}^{p-1} \left(\frac{x^3 - 1}{p} \right), \qquad B = \sum_{x=0}^{p-1} \left(\frac{x^3 - n}{p} \right).$$

Then

$$A^2 + AB + B^2 = 3p.$$

Question

Let $-d$ be the discriminant of an imaginary quadratic number field such that $\mathbb{Q}(\sqrt{-d})$ has class number 1.

Let

$$f(x,y) = \begin{cases} x^2 + (d/4)y^2, & \text{if } d \equiv 0 \mod 4, \\ x^2 + xy + ((1+d)/4)y^2, & \text{if } d \equiv 3 \mod 4. \end{cases}$$

Then whether $p = f(x,y)$ is solvable depends only on $\left(\frac{-d}{p}\right)$.

Question. When $\left(\frac{-d}{p}\right) = 1$, can we express the integers A and B in $p = f(A,B)$ in terms of Jacobsthal sums in a uniform way?

Question

Let $-d$ be the discriminant of an imaginary quadratic number field such that $\mathbb{Q}(\sqrt{-d})$ has class number 1.

Let

$$f(x,y)=\begin{cases} x^2+(d/4)y^2, & \text{if } d\equiv 0 \mod 4,\\ x^2+xy+((1+d)/4)y^2, & \text{if } d\equiv 3 \mod 4.\end{cases}$$

Then whether $p=f(x,y)$ is solvable depends only on $\left(\frac{-d}{p}\right)$.

Question. When $\left(\frac{-d}{p}\right)=1$, can we express the integers A and B in $p=f(A,B)$ in terms of Jacobsthal sums in a uniform way?

Question

Let $-d$ be the discriminant of an imaginary quadratic number field such that $\mathbb{Q}(\sqrt{-d})$ has class number 1.

Let

$$f(x,y) = \begin{cases} x^2 + (d/4)y^2, & \text{if } d \equiv 0 \mod 4, \\ x^2 + xy + ((1+d)/4)y^2, & \text{if } d \equiv 3 \mod 4. \end{cases}$$

Then whether $p = f(x,y)$ is solvable depends only on $\left(\frac{-d}{p}\right)$.

Question. When $\left(\frac{-d}{p}\right) = 1$, can we express the integers A and B in $p = f(A,B)$ in terms of Jacobsthal sums in a uniform way?

Jacobsthal identity for $\mathbb{Q}(\sqrt{-2})$, Part I

Theorem (Hashimoto-Long-Y)

Assume that $p \equiv 1 \mod 8$ *and* n *is a quadratic nonresidue modulo* p. *Set*

$$A = \frac{1}{2}\sum_{x=0}^{p-1}\left(\frac{x^3+4x^2+2x}{p}\right), \qquad B = \frac{1}{4}\sum_{x=0}^{p-1}\left(\frac{x^5+nx}{p}\right).$$

Then A *and* B *are integers satisfying* $p = A^2 + 2B^2$.

Jacobsthal identity for $\mathbb{Q}(\sqrt{-d})$, Part II

Theorem (Hashimoto-Long-Y)

Assume that $p \equiv 3 \mod 8$. Set

$$A = \frac{1}{2}\sum_{x=0}^{p-1}\left(\frac{x^3+4x^2+2x}{p}\right),$$

$$B = \frac{1}{4}\left(1+\sum_{x=0}^{p-1}\left(\frac{x^6+4x^5+10x^4-20x^2-16x-8}{p}\right)\right).$$

Then A and B are integers satisfying $p = A^2 + 2B^2$.

The elliptic curve $y^2 = x^3 + 4x^2 + 2x$

Lemma

The elliptic curve $y^2 = x^3 + 4x^2 + 2x$ has CM by $\mathbb{Z}[\sqrt{-2}]$ and its L-function is

$$\prod_{p \equiv 1,3 \mod 8} \frac{1}{1 - 2\epsilon_p a_p p^{-s} + p^{1-2s}} \prod_{p \equiv 5,7 \mod 8} \frac{1}{1 + p^{1-2s}},$$

where a_p and b_p are positive integers such that $p = a_p^2 + 2b_p^2$ and

$$\epsilon_p = \begin{cases} 2(-1)^{b_p/2}\left(\frac{-2}{a_p}\right), & \text{if } p \equiv 1 \mod 8, \\ -2\left(\frac{-2}{a_p}\right), & \text{if } p \equiv 3 \mod 8. \end{cases}$$

The hyperelliptic curve $y^2 = x^5 + x$

Lemma

For $C : y^2 = x^5 + x$, we have

$$L(C/\mathbb{Q}, s) = L(E_1/\mathbb{Q}, s)L(E_2/\mathbb{Q}, s), \tag{1}$$

where $E_1 : y^2 = x^3 + 4x^2 + 2x$, $E_2 : y^2 = x^3 - 4x^2 + 2x$.

Proof.

There are 2-to-1 coverings

$$(x, y) \longmapsto (X, Y) = \left(\frac{(x \pm 1)^2}{x}, \frac{y(x \pm 1)}{x^2} \right)$$

from C to E_1 and E_2. Considering the associated Galois representations, we get (1). □

The hyperelliptic curve $y^2 = x^5 + x$

Lemma

For $C : y^2 = x^5 + x$, we have

$$L(C/\mathbb{Q}, s) = L(E_1/\mathbb{Q}, s)L(E_2/\mathbb{Q}, s), \tag{1}$$

where $E_1 : y^2 = x^3 + 4x^2 + 2x$, $E_2 : y^2 = x^3 - 4x^2 + 2x$.

Proof.

There are 2-to-1 coverings

$$(x, y) \longmapsto (X, Y) = \left(\frac{(x \pm 1)^2}{x}, \frac{y(x \pm 1)}{x^2} \right)$$

from C to E_1 and E_2. Considering the associated Galois representations, we get (1). □

L-function of $y^2 = x^5 + x$

Corollary

For $C : y^2 = x^5 + x$, let

$$\frac{1}{(1-\alpha_{p,1}p^{-s})\dots(1-\alpha_{p,4}p^{-s})}$$

be the p-factor of $L(C/\mathbb{Q}, s)$.

- If $p \equiv 1 \mod 8$, then

  $$\alpha_{p,j} = \left(\frac{-2}{a}\right)(-1)^{b/2}(a \pm b\sqrt{-2}),$$

  each with multiplicity 2, where a and b are the positive integers such that $p = a^2 + 2b^2$.

- If $p \equiv 3 \mod 8$, then $\alpha_{p,j} = \pm a \pm b\sqrt{-2}$, where a and b are integers such that $p = a^2 + 2b^2$.

L-function of $y^2 = x^5 + x$

Corollary

For $C : y^2 = x^5 + x$, let

$$\frac{1}{(1-\alpha_{p,1}p^{-s})\dots(1-\alpha_{p,4}p^{-s})}$$

be the p-factor of $L(C/\mathbb{Q}, s)$.

- If $p \equiv 1 \mod 8$, then

$$\alpha_{p,j} = \left(\frac{-2}{a}\right)(-1)^{b/2}(a \pm b\sqrt{-2}),$$

  each with multiplicity 2, where a and b are the positive integers such that $p = a^2 + 2b^2$.
- If $p \equiv 3 \mod 8$, then $\alpha_{p,j} = \pm a \pm b\sqrt{-2}$, where a and b are integers such that $p = a^2 + 2b^2$.

The curve $y^2 = x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8$

Lemma

The hyperelliptic curve $X_1 : y^2 = x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8$ is isomorphic to $X_2 : y^2 = x^5 + x$ over a field of degree 16 over $\mathbb{Q}$, which is cyclic of degree 4 over $\mathbb{Q}(\zeta_8)$.

Proof.

Setting

$$x = \frac{\sqrt{2}(x_1 + 1)}{x_1 - 1}, \qquad y = \frac{y_1}{(x_1 - 1)^3},$$

we get $y_1^2 = 128(2 + \sqrt{2})x_1(x_1^4 + 3 - 2\sqrt{2})$. □

The proof of the theorem follows the argument in the case of the classical Jacobsthal identity (although more complicated).

The curve $y^2 = x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8$

Lemma

The hyperelliptic curve $X_1 : y^2 = x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8$ is isomorphic to $X_2 : y^2 = x^5 + x$ over a field of degree 16 over $\mathbb{Q}$, which is cyclic of degree 4 over $\mathbb{Q}(\zeta_8)$.

Proof.

Setting

$$x = \frac{\sqrt{2}(x_1 + 1)}{x_1 - 1}, \qquad y = \frac{y_1}{(x_1 - 1)^3},$$

we get $y_1^2 = 128(2 + \sqrt{2})x_1(x_1^4 + 3 - 2\sqrt{2})$. □

The proof of the theorem follows the argument in the case of the classical Jacobsthal identity (although more complicated).

The curve $y^2 = x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8$

Lemma

The hyperelliptic curve $X_1 : y^2 = x^6 + 4x^5 + 10x^4 - 20x^2 - 16x - 8$ is isomorphic to $X_2 : y^2 = x^5 + x$ over a field of degree 16 over $\mathbb{Q}$, which is cyclic of degree 4 over $\mathbb{Q}(\zeta_8)$.

Proof.

Setting

$$x = \frac{\sqrt{2}(x_1 + 1)}{x_1 - 1}, \qquad y = \frac{y_1}{(x_1 - 1)^3},$$

we get $y_1^2 = 128(2 + \sqrt{2})x_1(x_1^4 + 3 - 2\sqrt{2})$. □

The proof of the theorem follows the argument in the case of the classical Jacobsthal identity (although more complicated).

How do we find the curves?

Assume $p \equiv 1, 3 \mod 8$ and $p = a^2 + 2b^2 = (a + b\sqrt{-2})(a - b\sqrt{-2})$.

If $C : y^2 = f(x)$ is a curve such that the p-factor of $L(C/\mathbb{Q}, s)$ is

$$\frac{1}{(1 \pm (a + b\sqrt{-2})p^{-s})(1 \pm (a - b\sqrt{-2})p^{-s})},$$

then

$$\sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right) = \pm 2a.$$

Thus, we are looking at elliptic curves with CM by $\mathbb{Z}[\sqrt{-2}]$.

How do we find the curves?

Assume $p \equiv 1, 3 \mod 8$ and $p = a^2 + 2b^2 = (a + b\sqrt{-2})(a - b\sqrt{-2})$.

If $C : y^2 = f(x)$ is a curve such that the p-factor of $L(C/\mathbb{Q}, s)$ is

$$\frac{1}{(1 \pm (a + b\sqrt{-2})p^{-s})(1 \pm (a - b\sqrt{-2})p^{-s})},$$

then

$$\sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right) = \pm 2a.$$

Thus, we are looking at elliptic curves with CM by $\mathbb{Z}[\sqrt{-2}]$.

How do we find the curves?

Assume $p \equiv 1, 3 \mod 8$ and $p = a^2 + 2b^2 = (a + b\sqrt{-2})(a - b\sqrt{-2})$.

If $C : y^2 = f(x)$ is a curve such that the p-factor of $L(C/\mathbb{Q}, s)$ is

$$\frac{1}{(1 \pm (a + b\sqrt{-2})p^{-s})(1 \pm (a - b\sqrt{-2})p^{-s})},$$

then

$$\sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right) = \pm 2a.$$

Thus, we are looking at elliptic curves with CM by $\mathbb{Z}[\sqrt{-2}]$.

How do we find the curves?

To get b, we observe that

$$(a+b\sqrt{-2})(\zeta_8+\zeta_8^3)+(a-b\sqrt{-2})(\zeta_8^5+\zeta_8^7)=-4b.$$

Thus, we are looking for curves $y^2=f(x)$ whose L-function has p-factor

$$\frac{1}{(1\pm\zeta_8(a+b\sqrt{-2})p^{-s})\dots(1\pm\zeta_8^7(a-b\sqrt{-2})p^{-s})},$$

i.e., a hyperelliptic curve of genus 2.

To find such a curve, we shall find "its L-function" first.

How do we find the curves?

To get b, we observe that

$$(a+b\sqrt{-2})(\zeta_8+\zeta_8^3)+(a-b\sqrt{-2})(\zeta_8^5+\zeta_8^7)=-4b.$$

Thus, we are looking for curves $y^2=f(x)$ whose L-function has p-factor

$$\frac{1}{(1\pm\zeta_8(a+b\sqrt{-2})p^{-s})\dots(1\pm\zeta_8^7(a-b\sqrt{-2})p^{-s})},$$

i.e., a hyperelliptic curve of genus 2.

To find such a curve, we shall find "its L-function" first.

How do we find the curves?

To get b, we observe that

$$(a+b\sqrt{-2})(\zeta_8+\zeta_8^3)+(a-b\sqrt{-2})(\zeta_8^5+\zeta_8^7)=-4b.$$

Thus, we are looking for curves $y^2=f(x)$ whose L-function has p-factor

$$\frac{1}{(1\pm\zeta_8(a+b\sqrt{-2})p^{-s})\dots(1\pm\zeta_8^7(a-b\sqrt{-2})p^{-s})},$$

i.e., a hyperelliptic curve of genus 2.

To find such a curve, we shall find "its L-function" first.

Hecke characters

Let K be a number field. For each place v, let K_v be the completion of K with respect to $|\cdot|_v$ and $\mathcal{O}_v$ be the valuation ring of K_v when v is a finite place.

Let

$$\mathbb{I}_K = \left\{ (x_v) \in \prod_v K_v^* : x_v \in \mathcal{O}_v^* \text{ for all but finitely many } v \right\}$$

be the idele group of K, equipped with the product topology.

Definition

A Hecke character (Grössencharakter) χ is a continuous group homomorphism from the idele class group $\mathbb{I}_K/K^*$ to $\mathbb{C}^*$.

Hecke characters

Let K be a number field. For each place v, let K_v be the completion of K with respect to $|\cdot|_v$ and $\mathcal{O}_v$ be the valuation ring of K_v when v is a finite place.

Let

$$\mathbb{I}_K = \left\{ (x_v) \in \prod_v K_v^* : x_v \in \mathcal{O}_v^* \text{ for all but finitely many } v \right\}$$

be the idele group of K, equipped with the product topology.

Definition

A Hecke character (Grössencharakter) χ is a continuous group homomorphism from the idele class group $\mathbb{I}_K/K^*$ to $\mathbb{C}^*$.

Hecke characters

Let K be a number field. For each place v, let K_v be the completion of K with respect to $|\cdot|_v$ and $\mathcal{O}_v$ be the valuation ring of K_v when v is a finite place.

Let

$$\mathbb{I}_K = \left\{ (x_v) \in \prod_v K_v^* : x_v \in \mathcal{O}_v^* \text{ for all but finitely many } v \right\}$$

be the idele group of K, equipped with the product topology.

Definition

A Hecke character (Grössencharakter) χ is a continuous group homomorphism from the idele class group $\mathbb{I}_K/K^*$ to $\mathbb{C}^*$.

Hecke L-functions and their functional equations

Definition

Let χ be a Hecke character. Write $\chi = \prod_v \chi_v$. The Hecke L-function is defined by

$$L(s,\chi) = \prod_{v \text{ finite},\ \chi_v(\mathcal{O}_v^*)=1} \frac{1}{1-\chi_v(\pi_v)Nv^{-s}},$$

where π_v is any uniformizer of K_v and Nv is the norm of the prime ideal corresponding to v.

Proposition

Let K be an imaginary quadratic number field. Suppose that k is the positive integer such that $|\chi(x)| = |x|^{k-1}$ for all $x \in \mathbb{I}_K/K^*$. Setting

$$\Lambda(s,\chi) = \left(\frac{2\pi}{\sqrt{d_K d_\chi}}\right)^{-s} \Gamma(s)L(s,\chi),$$

we have

$$\Lambda(s,\chi) = \epsilon\Lambda(k-s,\overline{\chi})$$

for some root of unity ϵ, where d_K is the discriminant of K and d_χ is the norm of the modulus of χ.

Remark

We get CM modular forms from Hecke characters on imaginary quadratic number field.

Hecke L-functions and their functional equations

Proposition

Let K be an imaginary quadratic number field. Suppose that k is the positive integer such that $|\chi(x)| = |x|^{k-1}$ for all $x \in \mathbb{I}_K/K^*$. Setting

$$\Lambda(s,\chi) = \left(\frac{2\pi}{\sqrt{d_K d_\chi}}\right)^{-s} \Gamma(s) L(s,\chi),$$

we have

$$\Lambda(s,\chi) = \epsilon\Lambda(k-s,\overline{\chi})$$

for some root of unity ϵ, where d_K is the discriminant of K and d_χ is the norm of the modulus of χ.

Remark

We get CM modular forms from Hecke characters on imaginary quadratic number field.

Finding curves

- Let $K = \mathbb{Q}(\sqrt{-2})$. We construct Hecke characters χ_1 and χ_2 of modulus 8 so that χ takes value $\zeta_8^j(a + b\sqrt{-2})$.
- We then look for a hyperelliptic curve whose L-function coincide with $L(s,\chi_1)L(s,\chi_2)$. Specifically, we look for such a curve among hyperelliptic curves with an automorphism defined over $\mathbb{Q}(\sqrt{-2})$.
- In practice, we consider curves

$$y^2 = x^6 + mx^5 + nx^4 - 2nx^2 - 4mx - 8,$$

which has an automorphism

$$(x, y) \longmapsto \left(\frac{2}{x}, \frac{\sqrt{-8}y}{x^3}\right),$$

and search for m and n such that the L-function is $L(s,\chi_1)L(s,\chi_2)$.

Finding curves

- Let $K = \mathbb{Q}(\sqrt{-2})$. We construct Hecke characters χ_1 and χ_2 of modulus 8 so that χ takes value $\zeta_8^j(a + b\sqrt{-2})$.
- We then look for a hyperelliptic curve whose L-function coincide with $L(s, \chi_1)L(s, \chi_2)$. Specifically, we look for such a curve among hyperelliptic curves with an automorphism defined over $\mathbb{Q}(\sqrt{-2})$.
- In practice, we consider curves

$$y^2 = x^6 + mx^5 + nx^4 - 2nx^2 - 4mx - 8,$$

which has an automorphism

$$(x, y) \longmapsto \left(\frac{2}{x}, \frac{\sqrt{-8}y}{x^3}\right),$$

and search for m and n such that the L-function is $L(s, \chi_1)L(s, \chi_2)$.

Finding curves

- Let $K = \mathbb{Q}(\sqrt{-2})$. We construct Hecke characters χ_1 and χ_2 of modulus 8 so that χ takes value $\zeta_8^j(a + b\sqrt{-2})$.
- We then look for a hyperelliptic curve whose L-function coincide with $L(s, \chi_1)L(s, \chi_2)$. Specifically, we look for such a curve among hyperelliptic curves with an automorphism defined over $\mathbb{Q}(\sqrt{-2})$.
- In practice, we consider curves

$$y^2 = x^6 + mx^5 + nx^4 - 2nx^2 - 4mx - 8,$$

which has an automorphism

$$(x, y) \longmapsto \left(\frac{2}{x}, \frac{\sqrt{-8}y}{x^3}\right),$$

and search for m and n such that the L-function is $L(s, \chi_1)L(s, \chi_2)$.

Problem

Problem. For each imaginary quadratic number field K with class number 1, find an analogous identity.