Quadratic twists of genus one curves and Diophantine quintuples

Representation Theory XVIII, Dubrovnik
June 23, 2023

Matija Kazalicki

University of Zagreb

A problem

Quadratic twists of genus one curves

Consider the genus one quartic

$$H: \quad y^2 = f(x),$$

where $f(x) \in \mathbb{Z}[x]$ is a monic polynomial of degree 4 with the nonzero discriminant.

Quadratic twists of genus one curves

Consider the genus one quartic

$$H: \quad y^2 = f(x),$$

where $f(x) \in \mathbb{Z}[x]$ is a monic polynomial of degree 4 with the nonzero discriminant.

For a square-free integer d, we denote by $H^d : dy^2 = f(x)$ the quadratic twist of H with respect to $\mathbb{Q}(\sqrt{d})$.

Two questions

Consider

$$S = \{d \in \mathbb{Z} : H^d(\mathbb{Q}) \neq \emptyset \text{ and } |d| \text{ is a prime}\}.$$

Two questions

Consider

$$S = \{d \in \mathbb{Z} : H^d(\mathbb{Q}) \neq \emptyset \text{ and } |d| \text{ is a prime}\}.$$

Question

$$H^d(\mathbb{Q}) \neq \emptyset?$$

Two questions

Consider

$$S = \{d \in \mathbb{Z} : H^d(\mathbb{Q}) \neq \emptyset \text{ and } |d| \text{ is a prime}\}.$$

Question

$$H^d(\mathbb{Q}) \neq \emptyset?$$

Question
What is asymptotically the size of $S(X) = \{d \in S : |d| < X\}$ *as* $X \to \infty$*?*

Two questions

Consider

$$S = \{d \in \mathbb{Z} : H^d(\mathbb{Q}) \neq \emptyset \text{ and } |d| \text{ is a prime}\}.$$

Question

$$H^d(\mathbb{Q}) \neq \emptyset?$$

Question
What is asymptotically the size of $S(X) = \{d \in S : |d| < X\}$ as $X \to \infty$?

In this talk we address these questions in case when

$$H : \quad y^2 = (x^2 - x - 3)(x^2 + 2x - 12).$$

Known results

Çiperiani, Ozman: a criterion for $H^d(\mathbb{Q}) \neq \emptyset$ in terms of the image of the global trace map $tr_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}$ on E.

No estimates for the size of set $S(X)$ are known.

Connection with Diophantine quintuples

$D(q)$-m-tuples

For a rational number q, we say that the set of m **rational** numbers is a rational $D(q) - m$-tuple if the product of any two its distinct elements is q less then a square.

$D(q)$-m-tuples

For a rational number q, we say that the set of m **rational** numbers is a rational $D(q) - m$-tuple if the product of any two its distinct elements is q less then a square.

Diophantus of Alexandria

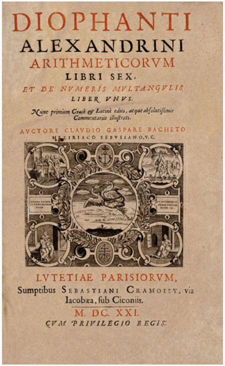
DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque abſolutiſſimis
Commentariis illuſtrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via
Iacobæa, ſub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Figure 1: Cover of the 1621 edition

Diophantus of Alexandria

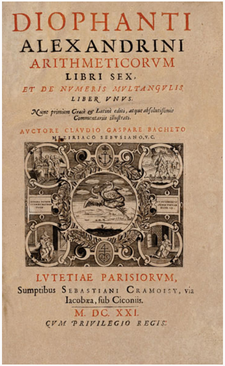

Figure 1: Cover of the 1621 edition

Diophantus - rational $D(1)$ quadruple:
$\{1/16, 33/16, 17/4, 105/16\}$

Fermat

Figure 2: Pierre de Fermat

Fermat

Figure 2: Pierre de Fermat

Fermat - $D(1)$ quadruples: $\{1, 3, 8, 120\}$

Fermat

Figure 2: Pierre de Fermat

Fermat - $D(1)$ quadruples: $\{1, 3, 8, 120\}$

$$1 \cdot 3 + 1 = 2^2 \quad 1 \cdot 8 + 1 = 3^2 \quad 1 \cdot 120 + 1 = 11^2$$
$$3 \cdot 8 + 1 = 5^2 \quad 3 \cdot 120 + 1 = 19^2 \quad 8 \cdot 120 + 1 = 31^2.$$

Euler

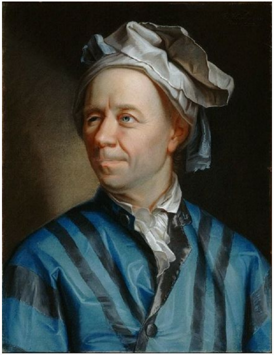

Figure 3: Leonhard Euler

Euler

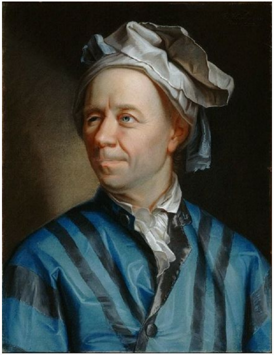

Figure 3: Leonhard Euler

Euler - $D(1)$-quintuple:
$\{1, 3, 8, 120, 777480/8288641\}$

Lots of interesting questions...

For more information: A. Dujella, What is... a Diophantine m-tuple?, Notices of AMS, August 2016

Lots of interesting questions...

For more information: A. Dujella, What is... a Diophantine m-tuple?, Notices of AMS, August 2016

Question
Does there exist a rational $D(q)$-quintuple for every q?

Lots of interesting questions...

For more information: A. Dujella, What is... a Diophantine m-tuple?, Notices of AMS, August 2016

Question
Does there exist a rational $D(q)$-quintuple for every q?

Dražić (continuing the work of Dujella and Fuchs):
Assuming the parity conjecture, for at least 99.5% squarefree integers q there are infinitely many $D(q)$-quintuples

Connection with quadratic twists of genus one curves

Dujella:

$$\left\{\tfrac{1}{3}(x^2+6x-18)(-x^2+2x+2), \tfrac{1}{3}x^2(x+5)(-x+3), (x-2)(5x+6), \tfrac{1}{3}(x^2+4x-6)(-x^2+4x+6), 4x^2\right\}$$

is $D(\frac{16}{9}x^2(x^2-x-3)(x^2+2x-12))$-quintuple.

Connection with quadratic twists of genus one curves

Dujella:

$$\left\{\tfrac{1}{3}(x^2+6x-18)(-x^2+2x+2), \tfrac{1}{3}x^2(x+5)(-x+3), (x-2)(5x+6), \tfrac{1}{3}(x^2+4x-6)(-x^2+4x+6), 4x^2\right\}$$

is $D(\frac{16}{9}x^2(x^2-x-3)(x^2+2x-12))$-quintuple.

For squarefree integer d, if

$$H^d : dy^2 = (x^2 - x - 3)(x^2 + 2x - 12)$$

for some rational (x, y) then by dividing the elements of quintuple above with $\frac{4}{3}xy$ we obtain $D(d)$-quintuple.

Question

Describe primes d for which H^d has infinitely many rational points.

Question
Describe primes d for which H^d has infinitely many rational points.

Proposition
If $d \in \mathbb{Z}$ is square free integer such that $H^d(\mathbb{Q}) \neq \emptyset$, then $H^d(\mathbb{Q})$ is infinite.

Results

Elliptic curve

Since quartic H has rational point at infinity, it is birationally equivalent to the elliptic curve

$$E : y^2 = (x - 9)(x - 8)(x + 18).$$

Denote by E^d its quadratic twist.

Density result

Theorem
Assuming the parity conjecture for curves E^d and that 100% of quadratic twists E^d have rank 0 or 1 (where $|d|$ is prime), we have that as $X \to \infty$

$$C_1 + o(1) \leq \frac{\#S(X)}{2\pi(X)} \leq C_2 + o(1),$$

where $C_1 = \frac{43}{256}$ and $C_2 = \frac{46}{256}$.

Some sets and fields

Let $T = T^+ \cup T^-$ where

$$T^+ = \{d > 0 : |d| \text{ is prime}, \left(\frac{d}{13}\right) = 1, \left(\frac{d}{3}\right) = 1, d \equiv 1 \pmod 8\},$$

$$T^- = \{d < 0 : |d| \text{ is prime}, \left(\frac{d}{13}\right) = 1, \left(\frac{d}{2}\right) \cdot \left(\frac{d}{3}\right) = -1, d \equiv 5, 7 \pmod 8\}.$$

Some sets and fields

Let $T = T^+ \cup T^-$ where

$$T^+ = \{d > 0 : |d| \text{ is prime}, \left(\tfrac{d}{13}\right) = 1, \left(\tfrac{d}{3}\right) = 1, d \equiv 1 \pmod 8\},$$

$$T^- = \{d < 0 : |d| \text{ is prime}, \left(\tfrac{d}{13}\right) = 1, \left(\tfrac{d}{2}\right) \cdot \left(\tfrac{d}{3}\right) = -1, d \equiv 5, 7 \pmod 8\}.$$

Define

$$L_{H_1,H_2} = \mathbb{Q}(\sqrt{3}, \sqrt{-1}, \sqrt{2})\sqrt{8(1+\sqrt{3})(4+2\sqrt{3})},$$

$$L_{H,H_1} = \mathbb{Q}(\sqrt{3}, \sqrt{13})(\sqrt{4+\sqrt{13}}),$$

$$L_{H,H_2} = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{13})(\sqrt{4+2\sqrt{13}}),$$

$$L_{H^{-1},F_2} = \mathbb{Q}(\sqrt{13}, \sqrt{-1}, \sqrt{-3})(\sqrt{3(1+\sqrt{13})(3+\sqrt{13})}).$$

Main result

Corollary

Let $d \in T$. *Assuming the parity conjecture for* E^d, *if* d *does not split completely in* $L_{H_1,H_2} = L_{F_1,F_2}$ *and*

a) $d = -p < 0$ *with* $p \equiv 1 \bmod 4$ *and* p *splits completely in* L_{H^{-1},F_2}, *or*
b) $d = p > 0$ *and* p *splits completely in* L_{H,H_1} *and* L_{H,H_2},

then $H^d(\mathbb{Q}) \neq \emptyset$. *Hence, for such* d *there exists infinitely many* $D(d)$*-quintuples.*

Example

Example

The set of $d \in T$, $|d| < 3000$, for which Corollary implies that $H^d(\mathbb{Q}) \neq \emptyset$ is equal to

$$\{-2857, -2833, -1993, -601, -337, -313, 1993, 2833, 2857\}.$$

For $d = -313$, we find a point

$$(-2107/1202, 389073/1444804) \in H^{-313}(\mathbb{Q})$$

which produces a $D(-313)$-quintuple

$$\left\{\frac{81062614477261}{1313828969096}, \frac{15660515591}{623554328}, \frac{9009021853}{546517874}, \frac{28246175292437}{1313828969096}, \frac{2532614}{129691}\right\}.$$

Example

The set of $d \in T$, $|d| < 3000$, for which Corollary implies that $H^d(\mathbb{Q}) \neq \emptyset$ is equal to

$$\{-2857, -2833, -1993, -601, -337, -313, 1993, 2833, 2857\}.$$

For $d = -313$, we find a point

$$(-2107/1202, 389073/1444804) \in H^{-313}(\mathbb{Q})$$

which produces a $D(-313)$-quintuple

$$\left\{\frac{81062614477261}{1313828969096}, \frac{15660515591}{623554328}, \frac{9009021853}{546517874}, \frac{28246175292437}{1313828969096}, \frac{2532614}{129691}\right\}.$$

Remark

Results about infinite number of $D(d)$-quintuples obtained as above from $d \in T$ where $d < 0$ are new.

More details

Local solvability

Proposition
For a square-free $d \in \mathbb{Z}$, the quartic H^d is everywhere locally solvable (ELS) if and only if for all primes $p|d$ we have $\left(\frac{p}{13}\right) = 1$ or $p = 13$.

Selmer group

Starting observation: if H^d is ELS, then H^d represents na element in $\mathrm{Sel}^{(2)}(E^d/\mathbb{Q})$.

Reformulation

If H^d is ELS then $H^d(\mathbb{Q}) = \emptyset$ if and only if H^d represents a nontrivial element in $Ш(E^d)[2]$ (where $Ш(E^d)$ denotes the Tate-Shafarevich group of E^d), or more precisely, if and only if the image of H^d under the map $\iota : \mathrm{Sel}^{(2)}(E^d) \to Ш(E^d)[2]$ from the exact sequence

$$0 \longrightarrow E^d(\mathbb{Q})/2E^d(\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(2)}(E^d) \xrightarrow{\iota} Ш(E^d)[2] \longrightarrow 0 \qquad (1)$$

is nonzero. In this case we say that H^d represents the element of order two in $Ш(E^d)$.

Definition of T - root number of E^d

If $\text{rank}(E^d(\mathbb{Q})) = 0$, then $H^d(\mathbb{Q}) = \emptyset$, hence, assuming the parity conjecture and standard rank conjectures, the main contribution to $\#S(X)$ comes from the d's for which the root number $w(E^d)$ is -1.

Definition of T - root number of E^d

If $\text{rank}(E^d(\mathbb{Q})) = 0$, then $H^d(\mathbb{Q}) = \emptyset$, hence, assuming the parity conjecture and standard rank conjectures, the main contribution to $\#S(X)$ comes from the d's for which the root number $w(E^d)$ is -1.

Proposition
For $d = \pm p$ where $p \neq 2, 3, 13$ is a prime, the root number $w(E^d)$ is equal to -1 if and only if

$$\left(\frac{p}{2}\right) \cdot \left(\frac{p}{3}\right) \cdot \left(\frac{p}{13}\right) = 1.$$

Here $\left(\frac{\cdot}{2}\right)$ is the Kronecker symbol for odd d defined by

$$\left(\frac{d}{2}\right) = \begin{cases} 1, & \textit{if } |d| \equiv 1, 7 \bmod (8) \\ -1, & \textit{if } |d| \equiv 3, 5 \bmod (8). \end{cases}$$

Definition of T - nontrivial $Ш(E)[2]$

Moreover, if $Ш(E^d)[2]$ is trivial, then H^d automatically has a rational point, thus we furthermore focus on d's for which, besides $w(E^d) = -1$, we have that generically $\mathrm{rank}_{\mathbb{F}_2} Ш(E^d)[2] > 0$.

Definition of T - nontrivial $Ш(E)[2]$

Moreover, if $Ш(E^d)[2]$ is trivial, then H^d automatically has a rational point, thus we furthermore focus on d's for which, besides $w(E^d) = -1$, we have that generically $\mathrm{rank}_{\mathbb{F}_2} Ш(E^d)[2] > 0$.

Since $E^d : dy^2 = (x-8)(x-9)(x+18)$ has full rational 2-torsion, for such d's generically we will have $\mathrm{rank}_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(E^d) = 5$ since (again assuming the parity conjecture) we have that $\mathrm{rank}_{\mathbb{F}_2} Ш(E^d)[2]$ is even (hence at least 2 if non-trivial).

Definition of T - nontrivial $\text{Ш}(E)[2]$

Moreover, if $\text{Ш}(E^d)[2]$ is trivial, then H^d automatically has a rational point, thus we furthermore focus on d's for which, besides $w(E^d) = -1$, we have that generically $\operatorname{rank}_{\mathbb{F}_2} \text{Ш}(E^d)[2] > 0$.

Since $E^d : dy^2 = (x-8)(x-9)(x+18)$ has full rational 2-torsion, for such d's generically we will have $\operatorname{rank}_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(E^d) = 5$ since (again assuming the parity conjecture) we have that $\operatorname{rank}_{\mathbb{F}_2} \text{Ш}(E^d)[2]$ is even (hence at least 2 if non-trivial).

These conditions altogether define set T.

Size of 2-Selmer group

Proposition (without using the parity conjecture)
For prime $p > 3$, let $d = \pm p$ be such that $\left(\frac{d}{13}\right) = 1$ and $w(E^d) = -1$. We have that $\mathrm{rank}_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(E^d) = 3$ *or* 5. *More precisely,* $\mathrm{rank}_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(E^d) = 5$ *if and only if $d \equiv 1 \pmod 8$ if $d > 0$ or $d \equiv 5, 7 \pmod 8$ if $d < 0$.*

Size of 2-Selmer group

Proposition (without using the parity conjecture)
For prime $p > 3$, let $d = \pm p$ be such that $\left(\frac{d}{13}\right) = 1$ and $w(E^d) = -1$. We have that $\operatorname{rank}_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(E^d) = 3$ or 5. More precisely, $\operatorname{rank}_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(E^d) = 5$ if and only if $d \equiv 1 \pmod 8$ if $d > 0$ or $d \equiv 5, 7 \pmod 8$ if $d < 0$.

Proof: Mazur-Rubin method

Cassels-Tate pairing

Our main tool for studying image of H^d in $Ш(E^d)[2]$ is the Cassels-Tate pairing on $Ш(E^d)$ with values in $\mathbb{Q}/\mathbb{Z}$, or more precisely, its extension to a pairing of Selmer group by (1)

$$\langle \cdot, \cdot \rangle_{CT} : \mathrm{Sel}^{(2)}(E^d)[2] \times \mathrm{Sel}^{(2)}(E^d)[2] \to \mathbb{Z}/2\mathbb{Z} = \{0, 1\}.$$

Cassels-Tate pairing

Our main tool for studying image of H^d in $\text{Ш}(E^d)[2]$ is the Cassels-Tate pairing on $\text{Ш}(E^d)$ with values in $\mathbb{Q}/\mathbb{Z}$, or more precisely, its extension to a pairing of Selmer group by (1)

$$\langle \cdot, \cdot \rangle_{CT} : \mathrm{Sel}^{(2)}(E^d)[2] \times \mathrm{Sel}^{(2)}(E^d)[2] \to \mathbb{Z}/2\mathbb{Z} = \{0, 1\}.$$

This pairing is bilinear, alternating, and non-degenerate on $\text{Ш}(E^d)[2]/2\text{Ш}(E^d)[4]$, or equivalently, on $\mathrm{Sel}^{(2)}(E^d)/2\,\mathrm{Sel}^{(4)}(E^d)$.

Cassels-Tate pairing

Our main tool for studying image of H^d in $\text{Ш}(E^d)[2]$ is the Cassels-Tate pairing on $\text{Ш}(E^d)$ with values in $\mathbb{Q}/\mathbb{Z}$, or more precisely, its extension to a pairing of Selmer group by (1)

$$\langle \cdot, \cdot \rangle_{CT} : \mathrm{Sel}^{(2)}(E^d)[2] \times \mathrm{Sel}^{(2)}(E^d)[2] \to \mathbb{Z}/2\mathbb{Z} = \{0, 1\}.$$

This pairing is bilinear, alternating, and non-degenerate on $\text{Ш}(E^d)[2]/2\text{Ш}(E^d)[4]$, or equivalently, on $\mathrm{Sel}^{(2)}(E^d)/2\,\mathrm{Sel}^{(4)}(E^d)$.

Thus, if we find a class $L \in \mathrm{Sel}^{(2)}(E^d)$ such that $\langle H^d, L \rangle_{CT} = 1$, we can conclude that $\iota(H^d) \neq 0$, and, hence, that H^d represents the element of order two in $\text{Ш}(E^d)$.

Cassels-Tate pairing

Our main tool for studying image of H^d in $\text{Ш}(E^d)[2]$ is the Cassels-Tate pairing on $\text{Ш}(E^d)$ with values in $\mathbb{Q}/\mathbb{Z}$, or more precisely, its extension to a pairing of Selmer group by (1)

$$\langle \cdot, \cdot \rangle_{CT} : \mathrm{Sel}^{(2)}(E^d)[2] \times \mathrm{Sel}^{(2)}(E^d)[2] \to \mathbb{Z}/2\mathbb{Z} = \{0, 1\}.$$

This pairing is bilinear, alternating, and non-degenerate on $\text{Ш}(E^d)[2]/2\text{Ш}(E^d)[4]$, or equivalently, on $\mathrm{Sel}^{(2)}(E^d)/2\,\mathrm{Sel}^{(4)}(E^d)$.

Thus, if we find a class $L \in \mathrm{Sel}^{(2)}(E^d)$ such that $\langle H^d, L\rangle_{CT} = 1$, we can conclude that $\iota(H^d) \neq 0$, and, hence, that H^d represents the element of order two in $\text{Ш}(E^d)$.

Note that in the situation when $\text{Ш}(E^d)[2] = 2\text{Ш}(E^d)[4]$, we can not obtain any information about H^d using Cassels-Tate pairing.

More quartics

Define

$$\begin{aligned} H_1 &: y^2 = 4x^4 - 56x^2 + 169 \in \mathrm{Sel}^{(2)}(E), \\ H_2 &: y^2 = 18x^4 - 24x^3 - 32x^2 + 40x + 34 \in \mathrm{Sel}^{(2)}(E), \\ F_1 &: y^2 = 11x^4 + 12x^3 + 56x^2 + 24x + 68 \in \mathrm{Sel}^{(2)}(E^{-1}), \\ F_2 &: y^2 = x^4 + 56x^2 + 676 \in \mathrm{Sel}^{(2)}(E^{-1}). \end{aligned} \tag{2}$$

More quartics

Define

$$\begin{aligned} H_1 &: y^2 = 4x^4 - 56x^2 + 169 \in \mathrm{Sel}^{(2)}(E), \\ H_2 &: y^2 = 18x^4 - 24x^3 - 32x^2 + 40x + 34 \in \mathrm{Sel}^{(2)}(E), \\ F_1 &: y^2 = 11x^4 + 12x^3 + 56x^2 + 24x + 68 \in \mathrm{Sel}^{(2)}(E^{-1}), \\ F_2 &: y^2 = x^4 + 56x^2 + 676 \in \mathrm{Sel}^{(2)}(E^{-1}). \end{aligned} \tag{2}$$

The pairings between the twists of these classes and H^d determine whether $\iota(H^d) = 0$.

When is $\iota(H^d) \neq 0$?

Theorem

Let $d \in T$ such that $\text{Ш}(E^d)[2] \neq 2\text{Ш}(E^d)[4]$. Assuming the parity conjecture for E^d, the following is true.

a) *If $d < 0$ and $d \equiv 1 \pmod 4$ then $\langle H^d, F_1^{-d} \rangle_{CT} = 1$. In particular, $\iota(H^d) \neq 0 \in \text{Ш}(E^d)[2]$.*

b) *If $d < 0$ and $d \equiv 3 \pmod 4$ then $\iota(H^d) \neq 0$ if and only if $\langle H^d, F_2^{-d} \rangle_{CT} = 1$.*

c) *If $d > 0$ then $\iota(H^d) \neq 0$ if and only if $\langle H^d, H_1^d \rangle_{CT} = 1$ or $\langle H^d, H_2^d \rangle_{CT} = 1$.*

How to compute Cassels-Tate pairing?

Theorem (Smith)

Let $\tilde{E}$ be an elliptic curve over $\mathbb{Q}$ with full 2-torsion over $\mathbb{Q}$. Let

$$F, F' \in H^1(\mathbb{Q}, \tilde{E}[2]),$$

and let K be the minimal field over which F and F' are trivial. Next, let S be any set of places of $\mathbb{Q}$ which contains all places of bad reduction of $\tilde{E}$, the archimedean place and 2. Take $\mathcal{D}$ to be the set of pairs (d_1, d_2) of elements in $\mathbb{Q}^\times$ such that d_1/d_2 is square at all places of S, and F^{d_1} and F'^{d_2} are elements of 2-Selmer group of $\tilde{E}^{d_1}$ and $\tilde{E}^{d_2}$ respectively.

If $F \cup F'$ is alternating, then $\langle F^{d_1}, F'^{d_1} \rangle_{CT} = \langle F^{d_2}, F'^{d_2} \rangle_{CT}$ for all $(d_1, d_2) \in \mathcal{D}$. Otherwise, there is a quadratic extension L of K that is ramified only at primes in S such that

$$\langle F^{d_1}, F'^{d_1} \rangle_{CT} = \langle F^{d_2}, F'^{d_2} \rangle_{CT} + \left[\frac{L/K}{\mathfrak{d}} \right],$$

for all $(d_1, d_2) \in \mathcal{D}$, where the Galois group $\mathrm{Gal}(L/K)$ is identified with $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$. Here $\mathfrak{d}$ is any ideal of K coprime to the conductor of L/K that has norm in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ equal to (d_1/d_2). Such $\mathfrak{d}$ exists for all $(d_1, d_2) \in \mathcal{D}$. We denote by $\left[\frac{\cdot}{\cdot} \right]$ the Artin symbol.

Remark

We will call field L from the statement of Theorem above a governing field of F and F'. It needs not to be unique.

Example of a governing field

Example

$$L_{H^{-1},F_2} = \mathbb{Q}(\sqrt{13}, \sqrt{-1}, \sqrt{-3})(\sqrt{3(1+\sqrt{13})(3+\sqrt{13})})$$

Example of a governing field

Example

$$L_{H^{-1},F_2} = \mathbb{Q}(\sqrt{13}, \sqrt{-1}, \sqrt{-3})(\sqrt{3(1+\sqrt{13})(3+\sqrt{13})})$$

Essentially, field of a governing field is a field of definition of suitable choosen 1-cochain $\Gamma : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mu_2$ with the property that $d\Gamma = H^{-1} \cup F_2$.

Lemma
For integers a and b such that ab is not a perfect square let $L_{a,b}/\mathbb{Q}(\sqrt{a},\sqrt{b})$ be quadratic extension such that $L_{a,b}/\mathbb{Q}$ is Galois with Galois group isomorphic to dihedral group D_4. There exist a map

$$\gamma_{a,b} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{res} \mathrm{Gal}(L_{a,b}/\mathbb{Q}) \to \mu_2$$

which satisfies $d\gamma_{a,b} = \chi_a \cup \chi_b \in H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mu_2)$. Here $\mu_2 = \{\pm 1\}$ and the cup product $\chi_a \cup \chi_b$ is induced by the natural bilinear map $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ (hence for $\sigma, \tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we have that $(\chi_a \cup \chi_b)(\sigma, \tau) = -1$ if and only if $\sqrt{a}^{\sigma} = -\sqrt{a}$ and $\sqrt{b}^{\tau} = -\sqrt{b}$).

When is $Ш(E^d)[2] = 2Ш(E^d)[4]$?

Proposition
Let $d \in T$ and (thus $\operatorname{rank}_{\mathbb{F}_2} \operatorname{Sel}^{(2)}(E^d) = 5$*). We have that* $Ш(E^d)[2] = 2Ш(E^d)[4]$ *(which include the case when* $\operatorname{rank}(E(\mathbb{Q})) = 3$*) if and only if*

a) $\langle H^d, H_i^d \rangle_{CT} = 0$ *and* $\langle H_1^d, H_2^d \rangle_{CT} = 0$ *for* $i = 1, 2$ *if* $d > 0$,

b) $\langle H^d, F_i^{-d} \rangle_{CT} = 0$ *and* $\langle F_1^{-d}, F_2^{-d} \rangle_{CT} = 0$ *for* $i = 1, 2$ *if* $d < 0$.

Putting everything together - Chebotarev density theorem

Density result now follows from the description of Cassels-Tate pairing (the splitting condition in governing fields) and Chebotarev density theorem.

Thank you for your attention!