2^k-Selmer groups and Goldfeld's conjecture

Alexander Smith

23 July 2019

Congruent numbers

Definition

A positive integer d is called a *congruent number* if it is the area of a right triangle with rational side lengths.

Alternatively, a positive integer d is a congruent number if and only if the elliptic curve

$$E_{CN}^{d} : y^2 = x^3 - d^2 x$$

has positive rank.

Theorem (S. 2017)

Among the positive integers equal to 1, 2, *or* 3 *mod* 8, *the congruent numbers have zero natural density.*

Goldfeld's conjecture

Definition

Given an elliptic curve

$$E : y^2 = x^3 + ax + b$$

defined over $\mathbb{Q}$, and given a positive integer d, the quadratic twist E^d is defined to be the curve

$$E^d : y^2 = x^3 + d^2ax + d^3b.$$

Conjecture (Goldfeld 1979)

Given any elliptic curve $E/\mathbb{Q}$,

- *50% of the quadratic twists of E have rank zero,*
- *50% of the quadratic twists of E have rank one, and*
- *0% have any higher rank.*

Selmer groups

Given an elliptic curve $E/\mathbb{Q}$ and a positive integer n, we have an exact sequence

$$0 \to E[n] \to E \to E \to 0$$

of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ modules. The long exact sequence for group cohomology then gives an isomorphism

$$E(\mathbb{Q})\big/nE(\mathbb{Q}) \cong \ker\Big(H^1(G_{\mathbb{Q}}, E[n]) \longrightarrow H^1(G_{\mathbb{Q}}, E)\Big)$$

$$\subseteq \mathrm{Sel}^n E := \ker\Big(H^1(G_{\mathbb{Q}}, E[n]) \longrightarrow \prod_v H^1(G_{\mathbb{Q}_v}, E)\Big).$$

Define

$$\mathrm{Sel}^{2^\infty} E := \bigcup_{k \geq 1} \mathrm{im}\left(\mathrm{Sel}^{2^k} E \to H^1\left(G_{\mathbb{Q}}, E[2^\infty]\right)\right).$$

Selmer ranks

Given an elliptic curve $E/\mathbb{Q}$, we can write the abelian group $\mathrm{Sel}^{2^\infty} E$ in the form

$$(\mathbb{Z}/2\mathbb{Z})^{r_2(E)-r_4(E)} \oplus (\mathbb{Z}/4\mathbb{Z})^{r_4(E)-r_8(E)} \oplus \cdots \oplus (\mathbb{Q}_2/\mathbb{Z}_2)^{r_{2^\infty}(E)},$$

with the Selmer ranks $r_k(E)$ determined from E.

Facts

- We have $r_2(E) \geq r_4(E) \geq \cdots \geq r_{2^\infty}(E) \geq \mathrm{rank}(E) \geq 0$.
- (Conjectured) $r_{2^\infty}(E) = \mathrm{rank}(E)$.
- The integers $r_2(E), r_4(E), \ldots, r_{2^\infty}(E)$ all have the same parity.
- The analytic rank of E has this same parity.

The Cassels-Tate pairing is an alternating pairing on $\mathrm{Sel}^{2^\infty} E$ whose kernel is the maximal 2-divisible subgroup of $\mathrm{Sel}^{2^\infty} E$.

Heath-Brown's Result

Given $n \geq j \geq 0$, take $P^{\mathrm{Alt}}(j \big| n)$ to be the probability that a uniformly selected $n \times n$ alternating matrix with coefficients in $\mathbb{F}_2$ has kernel of rank exactly j. Take

$$P^{\mathrm{Alt}}(j \big| \infty) = \frac{1}{2} \lim_{n \to \infty} P^{\mathrm{Alt}}(j \big| 2n + j).$$

Theorem (Heath-Brown, '94)

For $r_2 \geq 0$,

$$\lim_{N \to \infty} \frac{\#\left\{0 < d < N \,:\, r_2(E^d_{CN}) = r_2\right\}}{N} \;=\; P^{\mathrm{Alt}}(r_2 \big| \infty)$$

This was extended to elliptic curves with full rational 2-torsion and no rational cyclic 4-isogeny by Kane.

(WIP) It also holds for elliptic curves with no rational 2-torsion.

Main result

Given $n \geq j \geq 0$, take $P^{\text{Alt}}(j \big| n)$ to be the probability that a uniformly selected $n \times n$ alternating matrix with coefficients in $\mathbb{F}_2$ has kernel of rank exactly j.
Take
$$P^{\text{Alt}}(j \big| \infty) = \frac{1}{2} \lim_{n \to \infty} P^{\text{Alt}}(j \big| 2n + j).$$

Theorem (S.)

Suppose the elliptic curve $E/\mathbb{Q}$ obeys certain technical conditions. Choose $k > 1$, and choose a sequence $r_2 \geq r_4 \geq \cdots \geq r_{2^k} \geq 0$ of integers. Then

$$\lim_{N \to \infty} \frac{\#\{0 < d < N \,:\, r_2(E^d) = r_2, \ldots, r_{2^k}(E^d) = r_{2^k}\}}{N}$$
$$= P^{\text{Alt}}(r_{2^k} \big| r_{2^{k-1}}) \cdot P^{\text{Alt}}(r_{2^{k-1}} \big| r_{2^{k-2}}) \cdot \cdots \cdot P^{\text{Alt}}(r_4 \big| r_2) \cdot P^{\text{Alt}}(r_2 \big| \infty)$$

The sequence r_2, r_4, …, r_{2^k} behaves like a Markov process.

Selmer ranks as a Markov chain

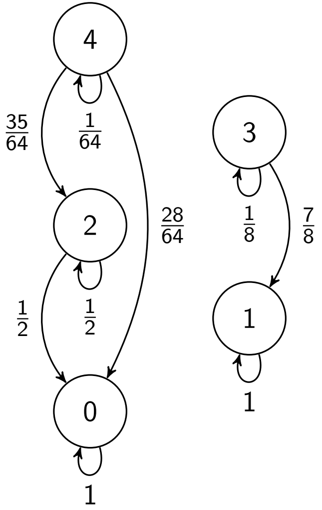


Table: Probability that $r_{2^k}(E^d)$ equals r.

		r = 0	1	2	3	4	5
k	1	.21	.42	.28	.08	.01	.00
	2	.35	.49	.15	.01	.00	
	3	.43	.50	.07	.00		
	4	.46	.50	.04			
	5	.48	.50	.02			
	$\vdots$	$\vdots$	$\vdots$	$\vdots$			
	∞	$\frac{1}{2}$	$\frac{1}{2}$	0	0	0	0

Main consequence

Theorem

Suppose the elliptic curve $E/\mathbb{Q}$ obeys the aforementioned technical conditions. Then, among the quadratic twists E^d of E,

- *50% have r_{2^∞} equal to zero,*
- *50% have r_{2^∞} equal to one, and*
- *0% have higher r_{2^∞}.*

In particular, at least 50% of the twists of E have rank zero, and 100% have rank at most one.

If we assume either the Birch and Swinnerton-Dyer conjecture or the Shafarevich-Tate conjecture, we get Goldfeld's conjecture for curves satisfying the conditions.

Twisting

Given a Galois module M over $G_{\mathbb{Q}}$ and a character

$$\chi \in \mathrm{Hom}(G_{\mathbb{Q}}, \pm 1),$$

we can define a Galois module M^{χ} and a (non-equivariant) isomoprhism $\beta_{\chi} : M^{\chi} \to M$ so,for σ in $G_{\mathbb{Q}}$ and m in M, we have

$$\beta_{\chi}(\sigma m) = \chi(\sigma)\,(\sigma\beta_{\chi}(m))\,.$$

Because $1 = -1$ in characteristic two, the map β_{χ} restricts to an isomorphism

$$M^{\chi}[2] = M[2]$$

of $G_{\mathbb{Q}}$ modules.

Two is special

Because of the isomorphism

$$E[2] \cong E^d[2],$$

there is an isomomrphism

$$H^1(G_{\mathbb{Q}}, E[2]) \cong H^1(G_{\mathbb{Q}}, E^d[2]).$$

We can then think of the 2-Selmer groups of the twists of E as lying in the same ambient space.
This property makes Sel^2 uniquely approachable. After Sel^2, Sel^4 is second best because of the diagram

$$\begin{tikzcd}
0 \arrow[r] & E[2] \arrow[r] \arrow[d, equal] & E[4] \arrow[r, "\cdot 2"] \arrow[d, phantom, "\not\parallel"] & E[2] \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & E^d[2] \arrow[r] & E^d[4] \arrow[r, "\cdot 2"] & E^d[2] \arrow[r] & 0.
\end{tikzcd}$$

In cubic twist families, the special Selmer group is the 3-Selmer group.

Class groups

Take $d > 1$ and consider $K = \mathbb{Q}(\sqrt{-d})$. Write Δ for the discriminant of K, and define

$$\mathrm{Cl}^{\vee} K = \mathrm{Hom}\left(\mathrm{Cl}\, K,\, \mathbb{Q}/\mathbb{Z}\right).$$

We can write

$$\mathrm{Cl}^{\vee} K[2^{\infty}] = \ker\left(H^1(G_K, \mathbb{Q}_2/\mathbb{Z}_2) \to \prod_{\mathfrak{p} \text{ of } K} H^1(I_{K_{\mathfrak{p}}}, \mathbb{Q}_2/\mathbb{Z}_2)\right).$$

If a divides Δ, the quadratic character for $K(\sqrt{a})/K$ is in this kernel. Because of these elements, the 2-class torsion tends to grow with d.

Class groups as Selmer groups

Take χ to be the quadratic character associated to $K = \mathbb{Q}(\sqrt{-d})$. With some technical assumptions on Δ, we can write

$$\begin{aligned} &2\mathrm{Cl}^\vee K[2^\infty] \\ &= \ker\left(H^1(G_{\mathbb{Q}}, (\mathbb{Q}_2/\mathbb{Z}_2)^\chi) \to \begin{array}{l} \prod_{p \mid \Delta} H^1(G_{\mathbb{Q}_p}, (\mathbb{Q}_2/\mathbb{Z}_2)^\chi) \\ \times \prod_{p \nmid \Delta} H^1(I_{\mathbb{Q}_p}, (\mathbb{Q}_2/\mathbb{Z}_2)^\chi) \end{array} \right) \end{aligned}$$

We can write $2\mathrm{Cl}\, K[2^\infty]$ as a subquotient of $H^1\left(G_{\mathbb{Q}}, (\mu_{2^\infty})^\chi\right)$. With these identifications, the natural nondegenerate pairing

$$2\mathrm{Cl}\, K[2^\infty] \times 2\mathrm{Cl}^\vee K[2^\infty] \to \mathbb{Q}/\mathbb{Z}$$

takes the form of Flach's generalization of the Cassels-Tate pairing. This pairing is non-alternating.

Fouvry and Klüners' result

Given $n \geq j \geq 0$, take $P^{\mathrm{Mat}}(j \big| n)$ to be the probability that a uniformly selected $n \times n$ matrix with coefficients in $\mathbb{F}_2$ has kernel of rank exactly j. Take

$$P^{\mathrm{Mat}}(j \big| \infty) = \lim_{n \to \infty} P^{\mathrm{Mat}}(j \big| n).$$

Write $r_{2^k}(K)$ for the 2^k class rank of the field K.

Theorem (Fouvry and Klüners', '07)

For $r_4 \geq 0$,

$$\lim_{N \to \infty} \frac{\#\left\{0 < d < N \;:\; r_4\left(\mathbb{Q}(\sqrt{-d})\right) = r_4\right\}}{N} \;=\; P^{\mathrm{Mat}}(r_4 \big| \infty)$$

Main result for class groups

Given $n \geq j \geq 0$, take $P^{\mathrm{Mat}}(j \middle| n)$ to be the probability that a uniformly selected $n \times n$ matrix with coefficients in $\mathbb{F}_2$ has kernel of rank exactly j.

Take

$$P^{\mathrm{Mat}}(j|\infty) = \lim_{n\to\infty} P^{\mathrm{Mat}}(j|n).$$

Write $r_{2^k}(K)$ for the 2^k class rank of the field K.

Theorem (S.)

Given a sequence of integers $r_4 \geq r_8 \geq \cdots \geq r_{2^k} \geq 0$, we have

$$\lim_{N\to\infty} \frac{\#\left\{0 < d < N \;:\; r_4\left(\mathbb{Q}(\sqrt{-d})\right) = r_4,\ \dots,\ r_{2^k}(\mathbb{Q}(\sqrt{-d})) = r_{2^k}\right\}}{N}$$
$$= P^{\mathrm{Mat}}(r_{2^k}|r_{2^{k-1}}) \cdot P^{\mathrm{Mat}}(r_{2^{k-1}}|r_{2^{k-2}}) \cdot \dots \cdot P^{\mathrm{Mat}}(r_8|r_4) \cdot P^{\mathrm{Mat}}(r_4|\infty).$$

Class ranks as a Markov chain

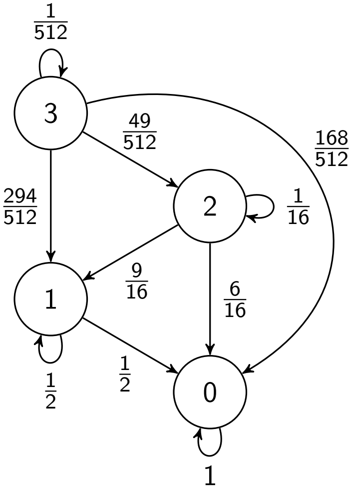


Table: Probability that $r_{2^k}(\mathbb{Q}(\sqrt{-d}))$ equals r

		r 0	1	2	3	4
k	2	.29	.58	.13	.01	.00
	3	.63	.36	.01	.00	
	4	.81	.19	.00		
	5	.91	.09			
	6	.95	.05			
	$\vdots$	$\vdots$	$\vdots$			
	∞	1	0	0	0	0

Our first goal will be to give the method for calculating 8-class ranks in some detail.

4-class groups

With $K = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{-d})$, we have isomorphisms

$$2\mathrm{Cl}^{\vee} K[4] \cong \frac{\{a|\Delta \,:\, (a, -\Delta)_v = +1 \text{ for all } v\} \cdot (\mathbb{Q}^{\times})^2}{\{1, \Delta\} \cdot (\mathbb{Q}^{\times})^2}$$

$$2\mathrm{Cl}\, K[4] \cong \frac{\{b|\Delta \,:\, (b, \Delta)_v = +1 \text{ for all } v\} \cdot (\mathbb{Q}^{\times})^2}{\{1, -\Delta\} \cdot (\mathbb{Q}^{\times})^2}$$

The pairing

$$2\mathrm{Cl}^{\vee} K[4] \times 2\mathrm{Cl}\, K[4] \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$$

is given by

$$(a, b) \mapsto [a, \Delta/a, b],$$

where [, ,] denotes a Rédei symbol.

Rédei symbols

Suppose a, b, c are nonzero integers satisfying

$$(a, b)_{\mathbb{Q},p} = +1 \quad (b, c)_{\mathbb{Q},p} = +1 \quad (a, c)_{\mathbb{Q},p} = +1$$

for all places p of $\mathbb{Q}$. We also assume c is squarefree and positive. Choose a primitive integer triple (x, y, z) so $x^2 - by^2 = az^2$, and take

$$L_{a,b} = \mathbb{Q}\left(\sqrt{a}, \sqrt{b}, \sqrt{x + y\sqrt{b}}\right).$$

For a rational prime p, define

$$\left(\frac{L_{a,b}/\mathbb{Q}}{p}\right) = \begin{cases} 1/2 & \text{if } L_{a,b} \,/\, \mathbb{Q}(\sqrt{a}, \sqrt{b}) \text{ is inert over } p \\ 0 & \text{otherwise.} \end{cases}$$

We then define $[a, b, c]$ in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ by

$$[a, b, c] \quad = \quad \sum_{p \mid c} \left(\frac{L_{a,b}/\mathbb{Q}}{p}\right) \; + \; p = 2 \text{ correction.}$$

An 8-class computation

$$2\mathrm{Cl}^\vee K[4] \cong \frac{\{a|\Delta\ : \forall v\ (a, -\Delta)_v = +1\}}{\{1, \Delta\}}$$
$$2\mathrm{Cl}\, K[4] \cong \frac{\{b|\Delta\ : \forall v\ (b, \Delta)_v = +1\}}{\{1, -\Delta\}}.$$

The pairing

$$2\mathrm{Cl}^\vee K[4] \times 2\mathrm{Cl}\, K[4] \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$$

sends (a, b) to $[a, \Delta/a, b]$.

Fix integers a_0, b_0, d_0 so $a_0, b_0 \big| d_0$ and $b_0, d_0 > 0$.
Take I to be some interval of primes disjoint from those dividing $2d_0$. For every p in I, we assume that

$$2\mathrm{Cl}^\vee \mathbb{Q}(\sqrt{-d_0 p})[4] \cong \langle a_0 p\rangle \quad \text{and} \quad 2\mathrm{Cl}\, \mathbb{Q}(\sqrt{-d_0 p})[4] \cong \langle b_0\rangle$$

$\mathbb{Q}(\sqrt{-d_0 p})$ has 8-class rank zero or one, depending on the value of

$$[a, \Delta/a, b] = [a_0 p,\ -d_0/a_0,\ b_0] = \left(\frac{L_{a_0 p, -d_0/a_0}/\mathbb{Q}}{b_0}\right).$$

Rédei reciprocity

We have the identities

$$[aa', b, c] = [a, b, c] + [a', b, c] \quad \text{and} \quad [a, b, c] = [b, a, c].$$

We also have

$$[a, b, c] = [c, b, a];$$

this can be proved as a consequence of Hilbert reciprocity.
We want to control $[a_0 p, -d_0/a_0, b_0]$ as p varies over an interval.

$$[a_0 p, -d_0/a_0, b_0] = [b_0, -d_0/a_0, a_0 p] = C + \left(\frac{L_{b_0, -d_0/a_0}/\mathbb{Q}}{p}\right).$$

The splitting of p in $L_{a,b}$ determines the 8-class rank of $\mathbb{Q}(\sqrt{-d_0 p})$. Because of this, $L_{a,b}$ is sometimes called a *governing field*.

Limitations of governing fields

- In general, governing fields can be constructed that control the 8-class rank in typical families of fields $\mathbb{Q}(\sqrt{-d_0 p})$.
- Similarly, governing fields can usually be constructed to control the 4-Selmer rank in families of twists $E^{d_0 p}$.
- *(Little problem)* Effective Chebotarev only suffices if we either assume GRH or focus on families where the family of p is much larger than d_0.
- *(Big problem)* Governing fields conjecturally do not exist for 16-class ranks or 8-Selmer groups.

Avoiding GRH

If we want to use effective Chebotarev, we need to use a governing field that gives less information.
We will just need the identities

$$[aa', b, c] = [a, b, c] + [a', b, c] \quad \text{and}$$
$$[a, bb', c] = [a, b, c] + [a, b', c]$$

Another 8-class computation

Fix integers a_0, b_0, d_0 so $a_0, b_0 \,\big|\, d_0$ and $b_0, d_0 > 0$.
Choose *three* disjoint sets of primes X_1, X_a, X_b. Choosing $p_a \in X_a$ and $p_b \in X_b$, we assume

$$\left(\frac{c}{p_1}\right) = \left(\frac{c}{p_1'}\right) \quad \text{for } c \,\big|\, 2d_0 p_a p_b, \;\; p_1, p_1' \in X_1.$$

We also make the similar assumption for X_a and X_b.
Under these assumptions, the 4-class rank of $K_{(p_1, p_a, p_b)} = \mathbb{Q}(\sqrt{-d_0 p_1 p_a p_b})$ does not depend on the choice of (p_1, p_a, p_b). We assume that we have, for every such tuple,

$$2\mathrm{Cl}^\vee K_{(p_1,p_a,p_b)}[4] \cong \langle a_0 p_a \rangle \quad \text{and} \quad 2\mathrm{Cl}\, K_{(p_1,p_a,p_b)}[4] \cong \langle b_0 p_b \rangle.$$

Another 8-class computation

$$K_{(p_1,p_a,p_b)} = \mathbb{Q}(\sqrt{-d_0 p_1 p_a p_b}), \quad (p_1, p_a, p_b) \in X_1 \times X_a \times X_b.$$

$$2\mathrm{Cl}^\vee K_{(p_1,p_a,p_b)}[4] \cong \langle a_0 p_a \rangle \quad \text{and} \quad 2\mathrm{Cl}\, K_{(p_1,p_a,p_b)}[4] \cong \langle b_0 p_b \rangle.$$

$$r_8(K_{(p_1,p_a,p_b)}) = \begin{cases} 0 & \text{if } [a_0 p_a,\ -d_0 p_1 p_b,\ b_0 p_b] = 1/2 \\ 1 & \text{otherwise.} \end{cases}$$

Choose p_a, p_a' in X_a, p_1, p_1' in X_1.

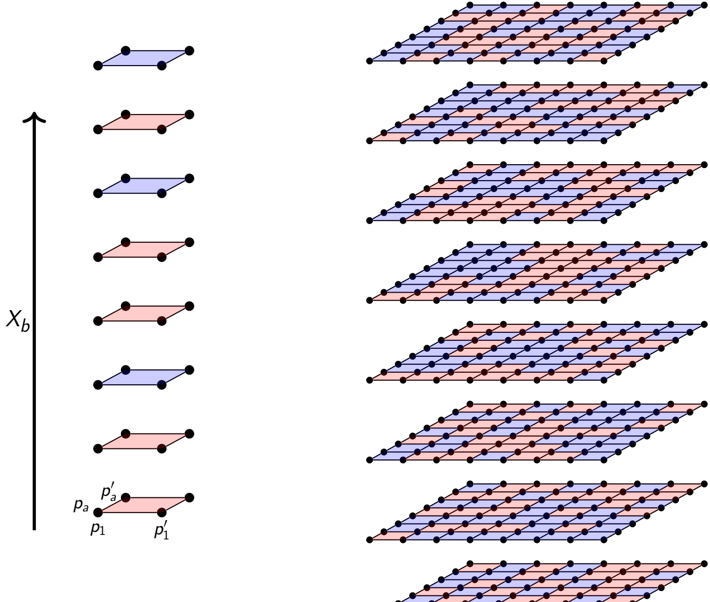
$$\begin{aligned} [a_0 p_a,\ -d_0 p_1 p_b,\ b_0 p_b] + [a_0 p_a,\ -d_0 p_1' p_b,\ b_0 p_b] &= [a_0 p_a,\ p_1 p_1',\ b_0 p_b] \\ [a_0 p_a,\ p_1 p_1',\ b_0 p_b] + [a_0 p_a',\ p_1 p_1',\ b_0 p_b] &= [p_a p_a',\ p_1 p_1', b_0 p_b]. \end{aligned}$$

So the parity of

$$r_8(K_{(p_1,p_a,p_b)}) + r_8(K_{(p_1',p_a,p_b)}) + r_8(K_{(p_1,p_a',p_b)}) + r_8(K_{(p_1',p_a',p_b)})$$

is determined from the splitting of p_b in $L_{p_a p_a', p_1 p_1'}$.

Relative governing fields



Controling higher class groups

Consider the family

$$\mathbb{Q}(\sqrt{-d_0 p_1 p_2 p_a p_b}), \quad (p_1, p_2, p_a, p_b) \in X_1 \times X_2 \times X_a \times X_b$$

$$2\mathrm{Cl}^\vee K_{(p_1,p_a,p_b)}[4] \cong \langle a_0 p_a \rangle \quad \text{and} \quad 2\mathrm{Cl}\, K_{(p_1,p_a,p_b)}[4] \cong \langle b_0 p_b \rangle.$$

If various (quite delicate) hypotheses are satisfied, the parity of

$$\begin{aligned} & r_{16}(K_{(p_1,p_2,p_a,p_b)}) + r_{16}(K_{(p_1',p_2,p_a,p_b)}) \\ +& r_{16}(K_{(p_1,p_2,p_a',p_b)}) + r_{16}(K_{(p_1',p_2,p_a',p_b)}) \\ +& r_{16}(K_{(p_1,p_2',p_a,p_b)}) + r_{16}(K_{(p_1',p_2',p_a,p_b)}) \\ +& r_{16}(K_{(p_1,p_2',p_a',p_b)}) + r_{16}(K_{(p_1',p_2',p_a',p_b)}) \end{aligned}$$

is determined by the splitting of p_b in a field $L_{p_a p_a' : p_1 p_1', p_2 p_2'}$. Etc.

Trilinearity equivalent for elliptic curves

Write

$$H^1(G_{\mathbb{Q}}, E[2^k]) = C^1(G_{\mathbb{Q}}, E[2^k])\big/B^1(G_{\mathbb{Q}}, E[2^k])$$

Choose nonzero integers d_1, d_2, and take

$$\phi_1 \in C^1(G_{\mathbb{Q}}, E^{d_1}[4]), \quad \phi_2 \in C^1(G_{\mathbb{Q}}, E^{d_2}[4]), \text{ and}$$
$$\phi_{12} \in C^1(G_{\mathbb{Q}}, E^{d_1 d_2}[4]).$$

Suppose

$$2\phi_1 = 2\phi_2 = 2\phi_{12}.$$

Then

$$-\phi_1 - \phi_2 - \phi_{12} \in C^1(G_{\mathbb{Q}}, E[4]).$$

Generating 8-Selmer elements

Choose nonzero integers d_1, d_2, d_3, and take

$$\begin{aligned}
&\phi_1 \in C^1(E^{d_1}[8]), \qquad \phi_2 \in C^1(E^{d_2}[8]), \qquad \phi_3 \in C^1(E^{d_3}[8]),\\
&\phi_{12} \in C^1(E^{d_1 d_2}[8]), \quad \phi_{13} \in C^1(E^{d_1 d_3}[8]), \quad \phi_{23} \in C^1(E^{d_2 d_3}[8]),\\
&\phi_{123} \in C^1(E^{d_1 d_2 d_3}[8]).
\end{aligned}$$

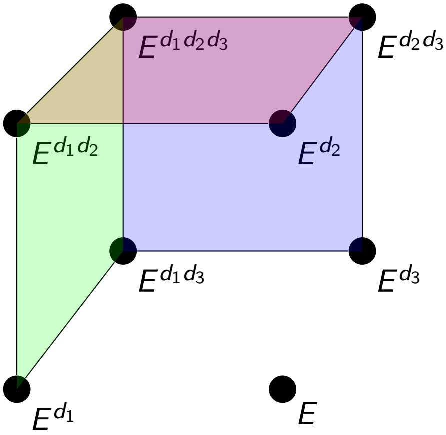
Suppose $4\phi_1 = 4\phi_2 = 4\phi_3 = 4\phi_{12} = 4\phi_{13} = 4\phi_{23} = 4\phi_{123}$ and

$$\begin{aligned}
&\ 2\phi_1 + 2\phi_{12} + 2\phi_{13} + 2\phi_{123}\\
&= 2\phi_2 + 2\phi_{12} + 2\phi_{23} + 2\phi_{123}\\
&= 2\phi_3 + 2\phi_{13} + 2\phi_{23} + 2\phi_{123} \ = \ 0.
\end{aligned}$$

Then

$$-\phi_1 - \phi_2 - \phi_3 - \phi_{12} - \phi_{13} - \phi_{23} - \phi_{123} \ \in \ C^1(E[8]).$$

Generating 8-Selmer elements



Thank you!