

On the Bloch-Kato conjecture at $s = 2$ for certain elliptic curves

Joint work with Neil Dummigan, Vasily Golyshev and Matt Kerr
<http://arxiv.org/abs/2605.11100>

Rob de Jeu
r.m.h.de.jeu@vu.nl

Department of Mathematics
Vrije Universiteit Amsterdam
The Netherlands
<http://www.few.vu.nl/~jeu>

22nd May 2026, Amsterdam, The Netherlands

The ζ -function of a number field

For a number field F ,

$$\operatorname{Res}_{s=1} \zeta_F(s) = \frac{2^{r_1} (2\pi)^{r_2} R \# \operatorname{Cl}(\mathcal{O})}{w \sqrt{\Delta_F}}$$

- $\operatorname{Cl}(\mathcal{O})$ = the class group of $\mathcal{O}$
- w = the number of roots of unity in $F = \# \mathcal{O}^*_{\text{tor}}$
- Δ_F the absolute value of the discriminant of F .

This is a statement about algebraic K -theory:

$$K_0(\mathcal{O}) \cong \mathbb{Z} \amalg \operatorname{Cl}(\mathcal{O}) \text{ and } K_1(\mathcal{O}) \cong \mathcal{O}^*,$$

so

$$\# \operatorname{Cl}(\mathcal{O}) = \# K_0(\mathcal{O})_{\text{tor}} \text{ and } w = \# K_1(\mathcal{O})_{\text{tor}}.$$

If F is a field then $K_2(F)$ is an Abelian group **written additively**, with

generators $\{a, b\}$ for a, b in F^*

relations $\{a_1 a_2, b\} = \{a_1, b\} + \{a_2, b\}$

$\{a, b_1 b_2\} = \{a, b_1\} + \{a, b_2\}$

$\{a, 1 - a\} = 0$ if $a \neq 0, 1$

Then also $\{a, b\} = -\{b, a\}$ and $\{c, -c\} = 0$ for a, b, c in F^* .

Note that $K_2(F) \simeq F^* \otimes F^* / \langle x \otimes (1 - x) \rangle$ with $\{a, b\}$ corresponding to the class of $a \otimes b$.

An example: $K_2(\mathbb{Q})$

Proposition

$$K_2(\mathbb{Q}) \xrightarrow{\sim} \{\pm 1\} \times \prod_{p \text{ prime}} \mathbb{F}_p^*$$

with components

$$T_\infty : K_2(\mathbb{Q}) \rightarrow \{\pm 1\} \text{ with } T_\infty(\{a, b\}) = \begin{cases} -1 & \text{if } a, b < 0 \\ 1 & \text{otherwise} \end{cases}$$

$$T_p : K_2(\mathbb{Q}) \rightarrow \mathbb{F}_p^* \text{ with}$$

$$T_p(\{a, b\}) = (-1)^{\text{ord}_p(a)\text{ord}_p(b)} \frac{a^{\text{ord}_p(b)}}{b^{\text{ord}_p(a)}} \bmod p \text{ the tame symbol for } p$$

T_∞ gives an isomorphism $\{\pm 1\} \simeq K_2(\mathbb{Z}) = \langle \{-1, -1\} \rangle \subset K_2(\mathbb{Q})$

For the proof of the proposition, for q prime or -1 , let

$$F_q = \langle \{a, b\} \text{ with } a, b \in \{-1, 2, 3, 5, 7, 11, \dots, q\} \rangle \subseteq K_2(\mathbb{Q})$$

Then

$$F_q/F_{q'} \xrightarrow{\cong} \mathbb{F}_q^* \text{ via } T_q \quad (q \geq 2)$$

with q' the **subprime** of q (= one prime smaller) ($2' = -1$)

An example: $K_2(\mathbb{Q})$

For the proof of this isomorphism, let $q \geq 2$

- surjectivity: $\{a, q\} \mapsto \bar{a} \in \mathbb{F}_q^* \ (a = 1, \dots, q-1)$
- injectivity: the kernel of $F_q \xrightarrow{T_q} \mathbb{F}_q^*$ is $F_{q'}$: $F_{q'} \subseteq \ker(T_q)$: clear;
if $q = 2$ then $F_2 = F_{-1}$ as $\{2, 2\} = \{2, -1\} = \{-1, 2\} = 0$
if $q > 2$ then $F_q/F_{q'}$ is generated by the classes of $\{a, q\} - \{b, q\}$
with $a, b \in M_q \stackrel{\text{def}}{=} \{-1, 1, 2, 3, 4, 5, \dots, q-1\}$

If $a_1, a_2 \in M_q$ then $\{a_1, q\} + \{a_2, q\} \stackrel{F_{q'}}{=} \{a_3, q\}$ for $a_3 \in M_q$:
division with remainder gives $a_1 a_2 - a_3 = Aq$ with
 $a_3 = 1, 2, \dots, q-1 \in M_q$ and $A = -1, 0, 1, \dots, q-2$.

If $A = 0$: $a_1 a_2 = a_3$ so clear;

If $A \neq 0$: $0 = \{\frac{a_1 a_2}{Aq}, \frac{a_3}{-Aq}\} \stackrel{F_{q'}}{=} \{a_3, q\} - \{a_1, q\} - \{a_2, q\}$.

So $F_q/F_{q'} = \{\{a, q\} - \{b, q\} \text{ with } a, b \in M_q\}$

Finally, if $T_q(\{a, q\}) = T_q(\{b, q\})$ for $a, b \in M_q$ then
 $a - b = 0, \pm q$ and $\{a, q\} \equiv \{b, q\}$ modulo $F'_{q'}$ as before

Some results by Quillen and Soulé

Quillen defined Abelian groups $K_n(R)$ ($n \geq 0$) for rings R , as well as for algebraic varieties.

Let F be a number field, with r_1 real and $2r_2$ non-real embeddings, $d = r_1 + 2r_2$, and ring of algebraic integers $\mathcal{O}$, and let Δ_F be the absolute value of the discriminant of F

Then

- $K_0(\mathcal{O}) \cong \mathbb{Z} \amalg \text{Cl}(\mathcal{O})$
- $K_1(\mathcal{O}) \cong \mathcal{O}^*$ has rank $r_1 + r_2 - 1$

Theorem (Quillen) $K_n(\mathcal{O})$ is finitely generated for all $n \geq 0$.

Theorem (Soulé) The localisation map $K_n(\mathcal{O}) \rightarrow K_n(F)$ is injective for $n > 0$.

This implies that $K_n(\mathcal{O}) = K_n(F)$ for $n > 1$ odd because K_m of a finite field is 0 for $m > 0$ and even.

Borel's theorem

Theorem (Borel; with some results of Quillen and Soulé thrown in)

- (1) $K_{2n}(\mathcal{O})$ is a finite group if $n \geq 1$.
- (2) For $n \geq 2$, $K_{2n-1}(\mathcal{O})$ is finitely generated of rank

$$m_{2n-1} = \begin{cases} r_2, & \text{if } n \text{ is even} \\ r_1 + r_2, & \text{if } n \text{ is odd} \end{cases}$$

- (3) There exists a natural regulator map

$$K_{2n-1}(\mathcal{O}) \rightarrow \mathbb{R}^{m_{2n-1}} \quad (n \geq 2).$$

Its image is a lattice with (normalized) volume of a fundamental domain

$$R_n(F) = q \frac{\zeta_F(n)}{\pi^{n(d-m_{2n-1})} \sqrt{\Delta_F}}$$

with q in $\mathbb{Q}^*$.

Example: the K -theory of $\mathbb{Z}$

$\zeta_{\mathbb{Q}}$ is the Riemann zeta function. For $n \geq 2$:

$$K_{2n-1}(\mathbb{Z}) = K_{2n-1}(\mathbb{Q})$$

this is finite for n even;

it has rank 1 for n odd, and $R_n(F) = q_n \zeta(n)$ with $q_n \in \mathbb{Q}^*$.

n	2	3	4	5	6	7	...
m_{2n-1}	0	1	0	1	0	1	...
$\zeta(n)$	$\pi^2/6$	irrational	$\pi^4/90$	???	$\pi^6/945$	???	...

Bloch's construction and result

Let $E/\mathbb{Q}$ be an elliptic curve. There is a commutative diagram

$$\begin{array}{ccccccc}
 K_2(E) & \longrightarrow & K_2(\mathbb{Q}(E)) & \xrightarrow{T} & \coprod_{E(1)} \mathbb{Q}(P)^* & & \\
 \vdots \downarrow \text{reg} & & \downarrow \text{reg} & & \downarrow L & & \\
 0 \longrightarrow & H_{\text{dR}}^1(E(\mathbb{C}), \mathbb{R}) & \longrightarrow & H_{\text{dR}}^1(\mathbb{C}(E), \mathbb{R}) & \longrightarrow & \coprod_{Q \in E(\mathbb{C})} \mathbb{R} & \longrightarrow \dots
 \end{array}$$

with exact rows, and

- $T = \prod_P T_P$ the tame symbol; T_P uses $\text{ord}_P(\cdot) : \mathbb{Q}(E)^* \rightarrow \mathbb{Z}$
- $L(a|_P) = (\log |\sigma(a)|_{|\sigma(P)})_{\sigma: \mathbb{Q}(P) \rightarrow \mathbb{C}}$
- $\text{reg}(\{f, g\}) =$ the class of $\log |f| \, d \arg(g) - \log |g| \, d \arg(f)$ in $H_{\text{dR}}^1(\mathbb{C}(E), \mathbb{R}) \stackrel{\text{def}}{=} \lim_{\rightarrow U} H_{\text{dR}}^1(U, \mathbb{R})$ with $E(\mathbb{C}) \setminus U$ finite
- $\text{reg}(\{f, 1 - f\}) = df^*(D)$ with $D : \mathbb{C} \setminus \{0, 1\} \rightarrow \mathbb{R}$ the **Bloch-Wigner dilogarithm**

Bloch's construction and result

Theorem (Bloch) Let E be an elliptic curve defined over $\mathbb{Q}$, and ω a non-zero holomorphic form on $E(\mathbb{C})$ with $\int_{E(\mathbb{R})} \omega = 1$.

If $E(\mathbb{C})$ has complex multiplication, then there exists α in $K_2(E)$ with

$$L'(E, 0) = q \frac{1}{2\pi} \int_{E(\mathbb{C})} \text{reg}(\alpha) \wedge \omega$$

with q in $\mathbb{Q}^*$, or, using the functional equation for the L -function

$$\frac{1}{2\pi} L(E, 2) = q' \int_{E(\mathbb{C})} \text{reg}(\alpha) \wedge \omega$$

with q' in $\mathbb{Q}^*$.

The kernel of the tame symbol

Let C be a regular, projective curve over a field F . For P a closed point of C we have the tame symbol at P

$$T_P : K_2(F(C)) \rightarrow F(P)^*$$

$$\{f, g\} \mapsto (-1)^{\text{ord}_P(f)\text{ord}_P(g)} \frac{f^{\text{ord}_P(g)}}{g^{\text{ord}_P(f)}}(P)$$

For β in $K_2(F(C))$ we have $\prod_P \text{Nm}_{F(P)/F}(T_P(\beta)) = 1$ in F^*
product formula

We have an exact localisation sequence

$$\begin{aligned} \dots \rightarrow \coprod_P K_2(F(P)) \rightarrow K_2(C) \rightarrow K_2(F(C)) \xrightarrow{T} \coprod_P F(P)^* \\ \rightarrow K_1(C) \rightarrow F(C)^* \xrightarrow{\text{div}} \coprod_P \mathbb{Z} \rightarrow K_0(C) \rightarrow \mathbb{Z} \rightarrow 0 \end{aligned}$$

Set $K_2^T(C) = \ker(T)$, the image of $K_2(C)$ in $K_2(F(C))$ under localisation

Fact $K_2(F)$ of a number field F is an infinite torsion group.

The integrality condition

Now assume F is a number field, and $\mathcal{C}$ a regular, flat and proper model over $\mathcal{O}_F$ of C over F . For an irreducible curve $\mathcal{D} \subseteq \mathcal{C}$ with residue field $\mathbb{F}(\mathcal{D})$, we have the tame symbol at $\mathcal{D}$

$$T_{\mathcal{D}} : K_2(F(C)) \rightarrow \mathbb{F}(\mathcal{D})^*$$
$$\{f, g\} \mapsto (-1)^{v_{\mathcal{D}}(f)v_{\mathcal{D}}(g)} \frac{f^{v_{\mathcal{D}}(g)}}{g^{v_{\mathcal{D}}(f)}}(\mathcal{D})$$

Set $K_2(C; \mathbb{Z}) = \ker\left(\prod_{\mathcal{D}} T_{\mathcal{D}} : K_2(F(C)) \rightarrow \prod_{\mathcal{D}} \mathbb{F}(\mathcal{D})^*\right)$

Then $K_2(C; \mathbb{Z}) \subseteq K_2^T(C)$: 'horizontal' $\mathcal{D}$ correspond to P in C

Proposition (Liu-de Jeu (2015)) $K_2(C; \mathbb{Z})$ is independent of $\mathcal{C}$. It is the image of $K_2(C)$ in $K_2(F(C))$ under localisation (hence behaves functorially).

$K_2(C; \mathbb{Z}) =$ 'integral elements' of $K_2^T(C)$, coming from $K_2(C)$

Beilinson's conjecture for K_2 of curves

For notational simplicity, suppose C is defined over $\mathbb{Q}$.

Conjecture (Beilinson; with Bass for supposed finite generation)

(1) The group $K_2(C; \mathbb{Z})$ is a finitely generated Abelian group of rank the genus g of C .

(2) The pairing

$$H_1(C(\mathbb{C}); \mathbb{Z})^- \times K_2(C; \mathbb{Z})_{\text{tf}} \rightarrow \mathbb{R}$$
$$(\gamma, \alpha) = \frac{1}{2\pi} \int_{\gamma} \text{reg}(\alpha)$$

is non-degenerate. $H_1(C(\mathbb{C}); \mathbb{Z})^- \cong \mathbb{Z}^g$: anti-invariants under complex conjugation on $C(\mathbb{C})$; reg as in Bloch's construction

(3) Let the Beilinson regulator R be the absolute value of the determinant of $(\cdot, \cdot)$ with respect to $\mathbb{Z}$ -bases of $H_1(C(\mathbb{C}); \mathbb{Z})^-$ and $K_2(C; \mathbb{Z})_{\text{tf}}$. Then, for some q in $\mathbb{Q}^*$,

$$(2\pi)^{-2g} L(C, 2) = qR.$$

A philosophy with ramification(s)

$u \geq 5$ integer with $D = u^2 - 4$ squarefree. A fundamental unit for $\mathcal{O}_F$ in $F = \mathbb{Q}(\sqrt{D})$ is $v > 1$ with $v^2 - uv + 1 = 0$; it has regulator

$$\log(v) = F_1(u) = \log(u) - \sum_{n=1}^{\infty} \binom{2n}{n} \frac{u^{-2n}}{2n},$$

hence
$$-\frac{\zeta'_F(0)}{F_1(u)} = \frac{\#\text{Cl}(\mathcal{O}(F))}{2} = \frac{\#\text{Cl}^+(\mathcal{O}(F))}{4}.$$

$\text{Cl}^+(\mathcal{O}_F)[2] \simeq (\mathbb{Z}/2\mathbb{Z})^{r-1}$ if D has r factors. $r = 2$ is necessary for $\text{ord}_2(\#\text{Cl}(\mathcal{O})) = 0$ but not sufficient:

minimal 2-part in class group		
u	$u^2 - 4$	$\text{ord}_2(\#\text{Cl}(\mathcal{O}_F))$
5	$3 \cdot 7$	0
9	$7 \cdot 11$	0
21	$19 \cdot 23$	0
45	$43 \cdot 47$	0
69	$67 \cdot 71$	0
81	$79 \cdot 83$	0

minimal number of factors in $u^2 - 4$		
u	$u^2 - 4$	$\text{ord}_2(\#\text{Cl}(\mathcal{O}_F))$
15	$13 \cdot 17$	1
99	$97 \cdot 101$	2
2139	$2137 \cdot 2141$	3
195	$193 \cdot 197$	4
3531	$3529 \cdot 3533$	5
2859	$2857 \cdot 2861$	6

A family of elliptic curves E with an element in $K_2^T(E)$

On the elliptic curve

$$E_u : y^2 = x(x+1)(x+u^2) \quad (u \text{ in } \mathbb{Q} \text{ with } u^2 \neq 0, 1).$$

let

$$v = \frac{x+u^2}{y} \quad w = \frac{u(x+1)-y}{u(x+1)+y} \quad h = \frac{u(x+1)+y}{x+u}$$

All have divisors in $\langle (-1, 0), (u, u^2 - u) \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Proposition

- (1) $\alpha_u = \{v, w\} + \{-1, h\}$ is in $K_2^T(E_u) \subset K_2(\mathbb{Q}(E_u))$.
- (2) If $4u$ is an integer then $2\alpha_u$ is in $K_2(E_u; \mathbb{Z})$.

Idea the rational number q_u in the Beilinson conjecture using the regulator of α_u should behave similarly to the quadratic number field situation; in particular, limiting $\text{ord}_2(q_u)$ should limit the number of primes of bad reduction of E_u .

Some numerical data

Let $F(u) = \log(4u) - \sum_{n=1}^{\infty} \binom{2n}{n}^2 \frac{(4u)^{-2n}}{2n} > 0$ for $u \geq 1$.

Proposition For $u > 1$, the Beilinson regulator of α_u is $R(\alpha_u) = |(\gamma, \alpha_u)| = F(u)$, where γ generates $H_1(E_u(\mathbb{C}), \mathbb{Z})^-$.

Numerical examples N_u the conductor of E_u ; q_u in $\mathbb{Q}^*$ with

$$\pm N_u^{-1} L'(E_u, 0) = (2\pi i)^{-2} L(E_u, 2) = q_u R(\alpha_u)$$

u	N_u	$\text{reg}(\alpha_u)$	$L(E_u, 2)$	$-q_u N_u$
4	$3 \cdot 5$	2.76463477084577...	0.66147518792106...	11^{-1}
92	$3 \cdot 7 \cdot 13 \cdot 23 \cdot 31$	5.90806816924716...	0.57516744273982...	$2^5 \cdot 3 \cdot 5$
236	$3 \cdot 5 \cdot 47 \cdot 59 \cdot 79$	6.85012392180782...	0.69525456664861...	$2^8 \cdot 3 \cdot 11$
556	$3 \cdot 5 \cdot 37 \cdot 139 \cdot 557$	7.70706225101732...	0.69222426353636...	$2^5 \cdot 5 \cdot 13 \cdot 47$

Remark For $u = 4$ it is known that $q_u = -\frac{1}{165}$.

Some indivisibility results

Uniform assumption (for expository purposes) from now on:

$u > 0$ is integer congruent to 4 mod 8 and $\text{ord}_p(\frac{1}{4}u(u^2 - 1))$ for a prime p is 0 or odd.

Then E_u has

- conductor $N_u = \prod_{\substack{p|u(u^2-1)/4 \\ p \text{ prime}}} p$;
- ordinary good reduction at 2;
- multiplicative reduction at each prime divisor of $u(u^2 - 1)/4$, split unless $p \equiv 3$ modulo 4 and p divides $u^2 - 1$.

Theorem Let $m_u = 1$ if $u + 1$ has a prime factor congruent to 3 modulo 4, and 2 otherwise. Then:

- 1 the image of α_u in $H^1(\mathbb{Q}, H_{\text{ét}}^1(E_u, \overline{\mathbb{Q}}, \mathbb{Z}_2(2)))$ modulo torsion under the 2-adic regulator map is not divisible by 2^{m_u} ;
- 2 α_u is not in $2^{m_u} K_2^T(E_u) + K_2^T(E_u)_{\text{tor}}$;
- 3 $2\alpha_u$ is in $K_2(E_u; \mathbb{Z})$ but not in $2K_2(E_u; \mathbb{Z}) + K_2(E_u; \mathbb{Z})_{\text{tor}}$.

Observation $2\alpha_u$ always has 2-divisible image under the 2-adic regulator map but is not 2-divisible in $K_2(E_u; \mathbb{Z})$ modulo torsion.

ℓ -adic regulator maps

Let ℓ be a prime number.

Proposition (1) The structure map $E_u \rightarrow \mathbb{Q}$ gives an injective pullback $H_{\text{ét}}^2(\text{Spec}(\mathbb{Q}), \mathbb{Z}_\ell(2)) \rightarrow H_{\text{ét}}^2(E_u, \mathbb{Z}_\ell(2))$.

(2) There is a short exact sequence

$$0 \rightarrow H_{\text{ét}}^2(\text{Spec}(\mathbb{Q}), \mathbb{Z}_\ell(2)) \rightarrow H_{\text{ét}}^2(E_u, \mathbb{Z}_\ell(2)) \xrightarrow{\pi_\ell} HH_\ell \rightarrow 0$$

with $HH_\ell = H^1(\mathbb{Q}, H_{\text{ét}}^1(E_{u, \overline{\mathbb{Q}}}, \mathbb{Z}_\ell(2)))$ which can be split by pullback to any rational point of E_u .

Here $H^1(\mathbb{Q}, \cdot)$ is continuous Galois cohomology

(3) The ℓ -adic Chern class induces a map reg_ℓ that fits into a commutative diagram

$$\begin{array}{ccc} K_2(E_u) & \xrightarrow{\quad} & K_2^T(E_u) \\ \text{ch}_\ell \downarrow & & \downarrow \text{reg}_\ell \\ H_{\text{ét}}^2(E_u, \mathbb{Z}_\ell(2)) & \xrightarrow{\pi_\ell} & H^1(\mathbb{Q}, H_{\text{ét}}^1(E_{u, \overline{\mathbb{Q}}}, \mathbb{Z}_\ell(2)))_{\text{tf}}. \end{array}$$

Interpreting the powers of 2 in the rational number

The 2-Selmer subgroup $H_f^1(\mathbb{Q}, E_u[2^\infty](-1)) \subseteq H^1(\mathbb{Q}, E_u[2^\infty](-1))$ is defined using local conditions involving ramification groups at all odd primes and ∞ , and B_{cris} for the prime 2

Its 2-torsion is explicitly computable:

Theorem Let S be the set of prime divisors of $u^2 - 1$, and S' the set of prime divisors of u that are congruent to 1 modulo 4. Then the 2-torsion in $H_f^1(\mathbb{Q}, E_u[2^\infty](-1))$ is in bijection with pairs (D, D') of positive squarefree integers, where the prime factors of D are in S and those of D' in S' , and which satisfy

- D' is a square modulo p for every p in S ;
- $2^{\text{ord}_p(D')} D$ is a square modulo p for every p in S' ;
- $D \equiv 1$ modulo 8.

Remark It happens often ($u = 4, 12, 20, 28, 60, 68, 108, 140, \dots$) that the group has no 2-torsion, hence is trivial!

The prediction of the Bloch-Kato conjecture

For a positive integer n , let

- $\omega(n)$: the number of distinct prime divisors of n
- $\omega_1(n)$: the number of distinct prime divisors of n congruent to 1
- $\omega_3(n)$: the number of distinct prime divisors of n congruent to 3

Theorem Assume

- $K_2(E_u; \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is 1-dimensional,
- $\frac{L(E_u, 2)}{(2\pi i)^2 F(u)}$ is a non-zero rational number q_u ,
- $H_f^1(\mathbb{Q}, E_u[2^\infty](-1))$ is finite, of order 2^{s_u} ,

Then the Bloch-Kato conjecture predicts that

$$\text{ord}_2(q_u) + n_u + 2 = \omega_3(u) + 2\omega_1(u) + \omega(u^2 - 1) + s_u.$$

where n_u is such that $\text{reg}_2(\alpha_u)$ is divisible by 2^{n_u} but not by 2^{1+n_u} .

Remark We have $0 \leq n_u \leq m_u - 1$ with $m_u = 1$ or 2 by the earlier indivisibility result. We have no indication that $n_u = 1$ occurs.

Minimising the exponent of 2 in q_u

Remark The terms involving the ω come from *Tamagawa factors*.

Proposition Assume that $\frac{1}{4}u(u^2 - 1)$ is squarefree.

- The right-hand side in the prediction is at least 2,
- it equals 2 for $u = 4$ only,
- it equals 3 for $u = 12$ only,
- it equals 4 **if and only if** $u - 1$ and $u + 1$ are primes, and $u = 12p$ for a prime number p congruent to 3 modulo 4.

(The last case is for $\omega_1(u) = 0$, $\omega_3(u) = 2$, $\omega(u^2 - 1) = 2$, $s_u = 0$.)

Ramifications in the philosophy?

If $\text{ord}_2(q_u) = 2$ then N_u has a very short and specific factorisation (and conversely). But if we allow more prime factors then $\text{ord}_2(q_u)$ grows but the Selmer group can still be trivial or of small predicted order. **So this is different from the earlier situation of the class group, which has to grow as more primes ramify.**

Numerical data: small values of u

$2^{\hat{s}_u}$ is the predicted order of the 2-Selmer group

$2^{s'_u}$ is the order of its 2-torsion subgroup

0^* : $n_u = 0$ and $\hat{s}_u = s'_u$ (so Selmer group should be 2-torsion)

1^+ : $\hat{s}_u = s'_u$ if we assume $n_u = 0$ (it could be 1)

u	$u/4$	$u-1$	$u+1$	N_u	$-N_u q_u$	$\hat{s}_u - n_u$	s'_u	$m_u - 1$
4	1	3	5	$3 \cdot 5$	11^{-1}	0	0	1^+
12	3	11	13	$3 \cdot 11 \cdot 13$	2	0	0	1^+
20	5	19	$3 \cdot 7$	$3 \cdot 5 \cdot 7 \cdot 19$	2^3	0	0	0^*
28	7	3^3	29	$3 \cdot 7 \cdot 29$	2	0	0	1^+
52	13	$3 \cdot 17$	53	$3 \cdot 13 \cdot 17 \cdot 53$	$2^5 \cdot 3$	2	1	1
60	$3 \cdot 5$	59	61	$3 \cdot 5 \cdot 59 \cdot 61$	$2^3 \cdot 29$	0	0	1^+
68	17	67	$3 \cdot 23$	$3 \cdot 17 \cdot 23 \cdot 67$	$2^3 \cdot 3^3$	0	0	0^*
84	$3 \cdot 7$	83	$5 \cdot 17$	$3 \cdot 5 \cdot 7 \cdot 17 \cdot 83$	$2^5 \cdot 17$	2	1	1
92	23	$7 \cdot 13$	$3 \cdot 31$	$3 \cdot 7 \cdot 13 \cdot 23 \cdot 31$	$2^5 \cdot 3 \cdot 5$	2	2	0^*
108	3^3	107	109	$3 \cdot 107 \cdot 109$	$2 \cdot 3 \cdot 19$	0	0	1^+
124	31	$3 \cdot 41$	5^3	$3 \cdot 5 \cdot 31 \cdot 41$	$2^4 \cdot 3$	2	1	1
132	$3 \cdot 11$	131	$7 \cdot 19$	$3 \cdot 7 \cdot 11 \cdot 19 \cdot 131$	$2^6 \cdot 3^3$	3	1	0
140	$5 \cdot 7$	139	$3 \cdot 47$	$3 \cdot 5 \cdot 7 \cdot 47 \cdot 139$	$2^4 \cdot 113$	0	0	0^*
156	$3 \cdot 13$	$5 \cdot 31$	157	$3 \cdot 5 \cdot 13 \cdot 31 \cdot 157$	$2^4 \cdot 3^2 \cdot 23$	0	0	1^+
164	41	163	$3 \cdot 5 \cdot 11$	$3 \cdot 5 \cdot 11 \cdot 41 \cdot 163$	$2^{10} \cdot 3$	6	1	0
188	47	$11 \cdot 17$	$3^3 \cdot 7$	$3 \cdot 7 \cdot 11 \cdot 17 \cdot 47$	$2^5 \cdot 13$	2	2	0^*
204	$3 \cdot 17$	$7 \cdot 29$	$5 \cdot 41$	$3 \cdot 5 \cdot 7 \cdot 17 \cdot 29 \cdot 41$	$2^{10} \cdot 7$	5	1	1
212	53	211	$3 \cdot 71$	$3 \cdot 53 \cdot 71 \cdot 211$	$2^3 \cdot 3^2 \cdot 73$	0	0	0^*
220	$5 \cdot 11$	$3 \cdot 73$	$13 \cdot 17$	$3 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 73$	$2^9 \cdot 13$	4	1	1
228	$3 \cdot 19$	227	229	$3 \cdot 19 \cdot 227 \cdot 229$	$2^2 \cdot 3 \cdot 5^4$	0	0	1^+
236	59	$5 \cdot 47$	$3 \cdot 79$	$3 \cdot 5 \cdot 47 \cdot 59 \cdot 79$	$2^8 \cdot 3 \cdot 11$	0	0	0

Numerical data: some special cases ($244 \leq u \leq 24996$)

- $\text{ord}_2(q_u)$ minimal • $\text{ord}_2(q_u)$ maximal • few primes of bad reduction but $\text{ord}_2(q_u)$ large (the Tamagawa factors contribute little to it and s'_u is small, but $\hat{s}_u$ is large) • more primes of bad reduction (contributing to $\text{ord}_2(q_u)$ through the Tamagawa factors, but $s_u = 0$) • Selmer group supposedly cyclic of large order

u	$u/4$	$u-1$	$u+1$	$-N_u q_u$	$\hat{s}_u - n_u$	s'_u	$m_u - 1$
1668	$3 \cdot 139$	1667	1669	$2^2 \cdot 3^2 \cdot 68023$	0	0	1^+
3252	$3 \cdot 271$	3251	3253	$2^2 \cdot 3 \cdot 5 \cdot 29 \cdot 9067$	0	0	1^+
4548	$3 \cdot 379$	4547	4549	$2^2 \cdot 3^2 \cdot 1268759$	0	0	1^+
8292	$3 \cdot 691$	8291	8293	$2^2 \cdot 3 \cdot 61 \cdot 71 \cdot 5099$	0	0	1^+
15972	$3 \cdot 11^3$	15971	15973	$2^2 \cdot 859 \cdot 4357$	0	0	1^+
22660	$5 \cdot 11 \cdot 103$	$3 \cdot 7 \cdot 13 \cdot 83$	$17 \cdot 31 \cdot 43$	$2^{25} \cdot 3 \cdot 43$	16	4	0
2716	$7 \cdot 97$	$3 \cdot 5 \cdot 181$	$11 \cdot 13 \cdot 19$	$2^{20} \cdot 3^2$	13	3	0
11452	$7 \cdot 409$	$3 \cdot 11 \cdot 347$	$13 \cdot 881$	$2^{20} \cdot 3 \cdot 173$	14	2	1
20460	$3 \cdot 5 \cdot 11 \cdot 31$	$41 \cdot 499$	$7 \cdot 37 \cdot 79$	$2^{20} \cdot 3^3 \cdot 5 \cdot 29$	12	2	0
20596	$19 \cdot 271$	$3 \cdot 5 \cdot 1373$	$43 \cdot 479$	$2^{20} \cdot 3^2 \cdot 7 \cdot 47$	15	3	0
2308	577	$3 \cdot 769$	2309	$2^{10} \cdot 3^3 \cdot 5 \cdot 37$	7	2	1
19212	$3 \cdot 1601$	19211	19213	$2^7 \cdot 3^3 \cdot 7^2 \cdot 19 \cdot 977$	4	1	1
24572	6143	24571	$3 \cdot 8191$	$2^9 \cdot 3^3 \cdot 23 \cdot 15583$	7	1	0
340	$5 \cdot 17$	$3 \cdot 113$	$11 \cdot 31$	$2^6 \cdot 3 \cdot 7 \cdot 17$	0	0	0^*
1508	$13 \cdot 29$	$11 \cdot 137$	$3 \cdot 503$	$2^6 \cdot 3 \cdot 7517$	0	0	0^*
24492	$3 \cdot 13 \cdot 157$	$19 \cdot 1289$	$7 \cdot 3499$	$2^7 \cdot 47863201$	0	0	0^*
5612	$23 \cdot 61$	$31 \cdot 181$	$3 \cdot 1871$	$2^{16} \cdot 3 \cdot 349$	0	0	0

Sketch of proof of the indivisibility statements

From now on abbreviate $HH_2 = H^1(\mathbb{Q}, H_{\text{ét}}^1(E_{u, \overline{\mathbb{Q}}}, \mathbb{Z}_2(2)))$ to HH

Proposition $HH_{\text{tor}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

- Pullback to a point R in $E(\mathbb{Q})$ gives a map $i_R^* : K_2(E_u) \rightarrow K_2(\mathbb{Q})$
- $K_2^T(E_u) = H^0(E_u, \mathcal{K}_2)$, the global sections of the sheafified K_2 , and the pullback factorises through $K_2(E_u) \rightarrow K_2^T(E_u)$.
- The pullback $K_2^T(E_u) \rightarrow K_2(\mathbb{Q})$ is explicitly computable by rewriting elements in $K_2^T(E_u)$.

The pullbacks in $K_2(\mathbb{Q})$ of some elements in $K_2^T(E_u)$ at some points in $E(\mathbb{Q})$ are as follows.

	$P = (0, 0)$	$Q = (-u^2, 0)$
$\{-1, x\}$	0	$\{-1, -1\}$
$\{-1, x + 1\}$	0	$\{-1, 1 - u^2\}$
$\alpha_u = \{v, w\} + \{-1, h\}$	0	$\{-1, 1 + u\}$

Key ingredient: controlling the torsion

For P, Q in the table, and $m \geq 1$, we have a commutative diagram

$$\begin{array}{ccccc}
 K_2(E_u) & \xrightarrow{\text{ch}_2} & H_{\text{ét}}^2(E_u, \mathbb{Z}_2(2)) & \xrightarrow{\pi_2} & HH \\
 \downarrow & & \downarrow i_Q^* - i_P^* & \nearrow & \\
 K_2^T(E_u) & & & & \\
 \downarrow i_Q^* - i_P^* & & & & \\
 K_2(\mathbb{Q}) & \xrightarrow{\text{ch}_2} & H_{\text{ét}}^2(\text{Spec}(\mathbb{Q}), \mathbb{Z}_2(2)) & & \\
 \downarrow & & \downarrow & & \\
 K_2(\mathbb{Q})/2^m & \xrightarrow[\simeq]{\text{ch}_{2,m}} & H_{\text{ét}}^2(\text{Spec}(\mathbb{Q}), \mu_{2^m}^{\otimes 2}) & &
 \end{array}$$

$\text{ch}_{2,m}$ is an isomorphism
by Merkur'ev-Suslin

where $K_2(E_u) \rightarrow K_2^T(E_u)$ is surjective with torsion kernel. We get a map $\psi_m : HH \rightarrow K_2(\mathbb{Q})/2^m$.

The pullback table gives:

- lifting $\{-1, x\}$ and $\{-1, x+1\}$ from $K_2^T(E_u)$ to $K_2(E_u)$ and then applying $\pi_2 \circ \text{ch}_2$ produces an $\mathbb{F}_2$ -basis of HH_{tor} ;
- ψ_m is injective on HH_{tor}

Proof of the indivisibility statement for $\text{reg}_2(\alpha)$

reg_2 is induced by $\pi_2 \circ \text{ch}_2$, so

$\text{reg}_2(\alpha)$ is in $2^m HH_{\text{tf}}$ if and only if, for any lift $\tilde{\alpha}$ of α to $K_2(E_u)$,

$$\pi_2 \circ \text{ch}_2(\tilde{\alpha}) = 2^m s + t$$

in HH for s, t in HH with t torsion.

If this holds then applying ψ_m leads to

$$\{-1, 1 + u\} \in \langle \{-1, -1\}, \{-1, 1 - u^2\} \rangle + 2^m K_2(\mathbb{Q})$$

inside $K_2(\mathbb{Q})$.

- Applying T_∞ shows $\{-1, 1 + u\}$ or $\{-1, u - 1\}$ is in $2^m K_2(\mathbb{Q})$.
- Applying T_p to $\{-1, u - 1\}$ for a prime $p \equiv 3$ modulo 4 dividing $u - 1$ shows this is not in $2K_2(\mathbb{Q})$.
- Applying T_p to $\{-1, 1 + u\}$ for a prime $p \equiv 1 + 2^{m_u}$ modulo 4 dividing $u + 1$ with $m = m_u = 1$ or 2 shows it is not in $2^{m_u} K_2(\mathbb{Q})$.

Proof of the indivisibility statement for 2α

2α is in $2K_2(E_u; \mathbb{Z}) + K_2(E_u; \mathbb{Z})_{\text{tor}}$ if and only if $2\alpha = 2\beta + \gamma$ for β, γ in $K_2(E_u; \mathbb{Z})$ with γ torsion.

That is equivalent to, inside $K_2^T(E_u)$,

$$\alpha = \beta + \delta$$

with δ in $K_2^T(E_u)_{\text{tor}}$.

- β came from $K_2(\mathcal{E}_u)$ so $(i_P^* - i_Q^*)(\beta)$ is in $K_2(\mathbb{Z}) = \langle \{-1, -1\} \rangle$
- Lifting δ to $K_2(E_u)$ and going through HH in the diagram then gives, in $K_2(\mathbb{Q})$, for any $m \geq 1$, that

$$\{-1, 1 + u\} \in \langle \{-1, -1\}, \{-1, 1 - u^2\} \rangle + 2^m K_2(\mathbb{Q}).$$

Applying T_∞ shows that then either $\{-1, u + 1\}$ or $\{-1, u - 1\}$ must be in $2^m K_2(\mathbb{Q})$. Fix a prime p dividing $u + 1$, a prime q dividing $u - 1$, and m such that $2^{m+1} \nmid p - 1$ or $q - 1$.

Then $T_p(\{-1, u + 1\}) = -1$ is not a 2^m th power in $\mathbb{F}_p^*$, and $T_q(\{-1, u - 1\}) = -1$ is not a 2^m th power in $\mathbb{F}_q^*$; contradiction.

The Bloch-Kato conjecture

Conjecture For every prime number ℓ , with

- $T_\ell(E_u)$ the Tate module,
- $T = T_\ell(E_u)(-1)$
- $V = T \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$,

we have

$$n_{u,\ell} + \text{ord}_\ell(q_u) = \text{ord}_\ell \left(\frac{\#H_f^1(\mathbb{Q}, V/T) \cdot \prod_{p \leq \infty} \text{Tam}_{p, \omega_p}^0(T(2))}{\#H^0(\mathbb{Q}, (V/T)(2)) \cdot \#H^0(\mathbb{Q}, V/T)} \right)$$

where

- the $\text{Tam}_{p, \omega_p}^0(T(2))$ are *Tamagawa factors*
- $n_{u,\ell}$ is such that $\text{reg}_\ell(\alpha_u)$ is divisible by $\ell^{n_{u,\ell}}$ but not by $\ell^{1+n_{u,\ell}}$ (and is assumed to exist)

The definition of $H_f^1(\mathbb{Q}, V/T)$

- Let (also for $p = \infty$)

$$H_f^1(\mathbb{Q}_p, V) = \begin{cases} \ker(H^1(\mathbb{Q}_p, V) \rightarrow H^1(I_p, V)) & p \neq \ell; \\ \ker(H^1(\mathbb{Q}_p, V) \rightarrow H^1(\mathbb{Q}_p, V \otimes B_{\text{cris}})) & p = \ell, \end{cases}$$

where $I_p \subseteq G_{\mathbb{Q}_p}$ is the inertia subgroup.

- Let $H_f^1(\mathbb{Q}_p, V/T)$ be the image of $H_f^1(\mathbb{Q}_p, V)$ under the natural map from $H^1(\mathbb{Q}_p, V)$ to $H^1(\mathbb{Q}_p, V/T)$.
- $H_f^1(\mathbb{Q}, V/T) := \cap_p \text{res}_p^{-1}(H_f^1(\mathbb{Q}_p, V/T))$, where $\text{res}_p : H^1(\mathbb{Q}, V/T) \rightarrow H^1(\mathbb{Q}_p, V/T)$ is the restriction map.

The definition of $H_f^1(\mathbb{Q}, V/T)$

If $p \neq \ell, \infty$ then g in $H^1(\mathbb{Q}, V/T)$ has $\text{res}_p(g)$ in $H_f^1(\mathbb{Q}_p, V/T)$ if and only if the latter comes from $H_f^1(\mathbb{Q}_p, V)$ in the commutative inflation/restriction diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H_f^1(\mathbb{Q}_p, V) & \longrightarrow & H^1(\mathbb{Q}_p, V) & \longrightarrow & H^1(I_p, V) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & H^1(\mathbb{F}_p, (V/T)^{I_p}) & \longrightarrow & H^1(\mathbb{Q}_p, V/T) & \longrightarrow & H^1(I_p, V/T) \end{array}$$

with exact rows. Here $G_{\mathbb{Q}_p}/I_p \simeq G_{\mathbb{F}_p}$, $H_f^1(\mathbb{Q}_p, V) \simeq H^1(\mathbb{F}_p, V^{I_p})$.

The left-most vertical map is the composition of

- the surjection $H^1(\mathbb{F}_p, V^{I_p}) \rightarrow H^1(\mathbb{F}_p, V^{I_p}/T^{I_p})$
- the natural map $H^1(\mathbb{F}_p, V^{I_p}/T^{I_p}) \rightarrow H^1(\mathbb{F}_p, (V/T)^{I_p})$

So the condition is: $\text{res}_p(g)$ comes from an h in $H^1(\mathbb{F}_p, (V/T)^{I_p})$ that maps to 0 in $H^1(\mathbb{F}_p, C)$, with C the cokernel of the injection $V^{I_p}/T^{I_p} \rightarrow (V/T)^{I_p}$.