# Spins, Galois representations and a question of Ramakrishna

**Peter Koymans**
**Institute for Theoretical Studies**

*Cornell Number Theory Seminar*

Online, 15 March 2024

# A question about $a_p(E)$

**Question (Ramakrishna, 2003)**

*Let $E$ be the elliptic curve $E : y^2 = x^3 - x$, and define*

$$a_p(E) = p + 1 - |E(\mathbb{F}_p)|.$$

# A question about $a_p(E)$

**Question (Ramakrishna, 2003)**

*Let $E$ be the elliptic curve $E : y^2 = x^3 - x$, and define*

$$a_p(E) = p + 1 - |E(\mathbb{F}_p)|.$$

*Are there infinitely many primes $p \equiv 1 \bmod 12$ such that $a_p(E)$ is a cubic residue modulo $p$?*

# A question about $a_p(E)$

**Question (Ramakrishna, 2003)**

*Let $E$ be the elliptic curve $E : y^2 = x^3 - x$, and define*

$$a_p(E) = p + 1 - |E(\mathbb{F}_p)|.$$

*Are there infinitely many primes $p \equiv 1 \bmod 12$ such that $a_p(E)$ is a cubic residue modulo $p$?*

If $p \equiv 2 \bmod 3$, then all elements of $\mathbb{F}_p$ are cubes, because

$$|\mathbb{F}_p^*| = p - 1 \not\equiv 0 \bmod 3.$$

# A question about $a_p(E)$

**Question (Ramakrishna, 2003)**

*Let $E$ be the elliptic curve $E : y^2 = x^3 - x$, and define*

$$a_p(E) = p + 1 - |E(\mathbb{F}_p)|.$$

*Are there infinitely many primes $p \equiv 1 \bmod 12$ such that $a_p(E)$ is a cubic residue modulo $p$?*

If $p \equiv 2 \bmod 3$, then all elements of $\mathbb{F}_p$ are cubes, because

$$|\mathbb{F}_p^*| = p - 1 \not\equiv 0 \bmod 3.$$

If $p \equiv 3 \bmod 4$ and $p > 3$, then $E$ has supersingular reduction at $p$, so

$$a_p(E) = 0,$$

which is a cube modulo $p$.

# Rephrasing the question

**Theorem (Cox, Theorem 14.16)**

*Let $K$ be an imaginary quadratic field and let $\mathcal{O}$ be an order in $K$. Let $L$ be the ring class field of $\mathcal{O}$, and let $E$ be an elliptic curve over $L$ with $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$.*

# Rephrasing the question

**Theorem (Cox, Theorem 14.16)**

*Let $K$ be an imaginary quadratic field and let $\mathcal{O}$ be an order in $K$. Let $L$ be the ring class field of $\mathcal{O}$, and let $E$ be an elliptic curve over $L$ with $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$.*

*Let $p$ be a prime that splits completely in $L$ and $\mathfrak{p}$ be a prime in $K$ above $p$. Suppose $E$ has good reduction at $\mathfrak{p}$. Then there is $\kappa \in \mathcal{O}$ such that $p = \kappa\overline{\kappa}$ and*

$$a_p(E) = p + 1 - |E(\mathbb{F}_p)| = \kappa + \overline{\kappa}.$$

# Rephrasing the question

**Theorem (Cox, Theorem 14.16)**

*Let $K$ be an imaginary quadratic field and let $\mathcal{O}$ be an order in $K$. Let $L$ be the ring class field of $\mathcal{O}$, and let $E$ be an elliptic curve over $L$ with* $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$.

*Let $p$ be a prime that splits completely in $L$ and $\mathfrak{p}$ be a prime in $K$ above $p$. Suppose $E$ has good reduction at $\mathfrak{p}$. Then there is $\kappa \in \mathcal{O}$ such that $p = \kappa\overline{\kappa}$ and*

$$a_p(E) = p + 1 - |E(\mathbb{F}_p)| = \kappa + \overline{\kappa}.$$

In our situation, we have

$$E : y^2 = x^3 - x, \quad K = \mathbb{Q}(i), \quad \mathcal{O} = \mathbb{Z}[i], \quad L = \mathbb{Q}(i).$$

# Rephrasing the question

**Theorem (Cox, Theorem 14.16)**

*Let $K$ be an imaginary quadratic field and let $\mathcal{O}$ be an order in $K$. Let $L$ be the ring class field of $\mathcal{O}$, and let $E$ be an elliptic curve over $L$ with $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$.*

*Let $p$ be a prime that splits completely in $L$ and $\mathfrak{p}$ be a prime in $K$ above $p$. Suppose $E$ has good reduction at $\mathfrak{p}$. Then there is $\kappa \in \mathcal{O}$ such that $p = \kappa\overline{\kappa}$ and*

$$a_p(E) = p + 1 - |E(\mathbb{F}_p)| = \kappa + \overline{\kappa}.$$

In our situation, we have

$$E : y^2 = x^3 - x, \quad K = \mathbb{Q}(i), \quad \mathcal{O} = \mathbb{Z}[i], \quad L = \mathbb{Q}(i).$$

Since $\mathbb{Z}[i]$ is a PID, we can write $p = \pi\overline{\pi}$, and $\pi$ is unique up to multiplying by a power of $i$. Then, for some choice of $\pi$, we have

$$a_p(E) = \pi + \overline{\pi}.$$

# A criterion for $a_p(E)$ being a cube modulo $p$

Since we have $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[i]/\pi\mathbb{Z}[i]$, we have that $a_p(E) = \pi + \overline{\pi}$ is a cube modulo $p$ if and only if it is a cube modulo $\pi$.

# A criterion for $a_p(E)$ being a cube modulo $p$

Since we have $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[i]/\pi\mathbb{Z}[i]$, we have that $a_p(E) = \pi + \overline{\pi}$ is a cube modulo $p$ if and only if it is a cube modulo $\pi$.

However, observe that $a_p(E) \equiv \overline{\pi} \bmod \pi$. So the question is equivalent to $\overline{\pi}$ being a cube modulo $\pi$.

# A criterion for $a_p(E)$ being a cube modulo $p$

Since we have $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[i]/\pi\mathbb{Z}[i]$, we have that $a_p(E) = \pi + \overline{\pi}$ is a cube modulo $p$ if and only if it is a cube modulo $\pi$.

However, observe that $a_p(E) \equiv \overline{\pi} \bmod \pi$. So the question is equivalent to $\overline{\pi}$ being a cube modulo $\pi$.

**Lemma**

*If $p \equiv 1 \bmod 12$, then $\overline{\pi}$ is a cube modulo $\pi$ if and only if $\overline{i \cdot \pi}$ is a cube modulo $\pi$.*

# A criterion for $a_p(E)$ being a cube modulo $p$

Since we have $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[i]/\pi\mathbb{Z}[i]$, we have that $a_p(E) = \pi + \overline{\pi}$ is a cube modulo $p$ if and only if it is a cube modulo $\pi$.

However, observe that $a_p(E) \equiv \overline{\pi} \bmod \pi$. So the question is equivalent to $\overline{\pi}$ being a cube modulo $\pi$.

**Lemma**

*If $p \equiv 1 \bmod 12$, then $\overline{\pi}$ is a cube modulo $\pi$ if and only if $\overline{i \cdot \pi}$ is a cube modulo $\pi$.*

**Proof.**

Since $p \equiv 1 \bmod 12$, we know that there is a primitive 12-th root of unity $\zeta_{12}$ in $\mathbb{F}_p$. Thus $i = \zeta_4$ is a cube in $\mathbb{F}_p$. $\square$

# A criterion for $a_p(E)$ being a cube modulo $p$

Since we have $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[i]/\pi\mathbb{Z}[i]$, we have that $a_p(E) = \pi + \overline{\pi}$ is a cube modulo $p$ if and only if it is a cube modulo $\pi$.

However, observe that $a_p(E) \equiv \overline{\pi} \bmod \pi$. So the question is equivalent to $\overline{\pi}$ being a cube modulo $\pi$.

**Lemma**

*If $p \equiv 1 \bmod 12$, then $\overline{\pi}$ is a cube modulo $\pi$ if and only if $\overline{i \cdot \pi}$ is a cube modulo $\pi$.*

**Proof.**

Since $p \equiv 1 \bmod 12$, we know that there is a primitive 12-th root of unity $\zeta_{12}$ in $\mathbb{F}_p$. Thus $i = \zeta_4$ is a cube in $\mathbb{F}_p$. □

**Corollary**

*Let $p \equiv 1 \bmod 12$. Then $a_p(E)$ is a cube modulo $p$ if and only if $(\overline{\pi}/\pi)_3 = 1$, where $\pi$ is any element of $\mathbb{Z}[i]$ satisfying $\pi\overline{\pi} = p$.*

# Cubic residue symbols

Let $K$ be a number field with $\zeta_3 \in K$. For $\alpha \in O_K$ and $\mathfrak{p} \nmid 3O_K$ a prime, we define $(\alpha/\mathfrak{p})_{K,3}$ as the unique element in $\{1, \zeta_3, \zeta_3^2, 0\}$ with

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_{K,3} \equiv \alpha^{\frac{N_{K/\mathbb{Q}}(\mathfrak{p})-1}{3}} \bmod \mathfrak{p}.$$

# Cubic residue symbols

Let $K$ be a number field with $\zeta_3 \in K$. For $\alpha \in O_K$ and $\mathfrak{p} \nmid 3O_K$ a prime, we define $(\alpha/\mathfrak{p})_{K,3}$ as the unique element in $\{1, \zeta_3, \zeta_3^2, 0\}$ with

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_{K,3} \equiv \alpha^{\frac{N_{K/\mathbb{Q}}(\mathfrak{p})-1}{3}} \bmod \mathfrak{p}.$$

We multiplicatively extend this to all ideals coprime to 3.

# Cubic residue symbols

Let $K$ be a number field with $\zeta_3 \in K$. For $\alpha \in O_K$ and $\mathfrak{p} \nmid 3O_K$ a prime, we define $(\alpha/\mathfrak{p})_{K,3}$ as the unique element in $\{1, \zeta_3, \zeta_3^2, 0\}$ with

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_{K,3} \equiv \alpha^{\frac{N_{K/\mathbb{Q}}(\mathfrak{p})-1}{3}} \bmod \mathfrak{p}.$$

We multiplicatively extend this to all ideals coprime to 3.

This residue symbol has the same usual properties as the quadratic residue symbol, i.e. periodicity and reciprocity.

## The symbol encoding $a_p(E)$

Consider the field diagram

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_{12}) \arrow[dl, dash, "\langle\sigma\rangle"'] \arrow[d, dash, "\langle\tau\rangle"'] \arrow[dr, dash, "\langle\sigma\tau\rangle"] & \\
\mathbb{Q}(\zeta_3) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd} .$$

# The symbol encoding $a_p(E)$

Consider the field diagram

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_{12}) \arrow[dl, dash, "\langle\sigma\rangle"'] \arrow[d, dash, "\langle\tau\rangle"'] \arrow[dr, dash, "\langle\sigma\tau\rangle"] & \\
\mathbb{Q}(\zeta_3) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd} .$$

For an ideal $\mathfrak{a}$ of $\mathbb{Z}[\zeta_{12}]$, we define the symbol $[\mathfrak{a}]$

$$[\mathfrak{a}] := \begin{cases} \left(\frac{\sigma(\alpha)\sigma\tau(\alpha)}{\alpha}\right)_{\mathbb{Q}(\zeta_{12}),3} & \text{if } \gcd(\mathfrak{a},(3)) = 1 \\ 0 & \text{otherwise,} \end{cases}$$

where $\alpha$ is any generator of $\mathfrak{a}$.

# The symbol encoding $a_p(E)$

Consider the field diagram

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_{12}) \arrow[dl, dash, "\langle\sigma\rangle"'] \arrow[d, dash, "\langle\tau\rangle"'] \arrow[dr, dash, "\langle\sigma\tau\rangle"] & \\
\mathbb{Q}(\zeta_3) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd} .$$

For an ideal $\mathfrak{a}$ of $\mathbb{Z}[\zeta_{12}]$, we define the symbol $[\mathfrak{a}]$

$$[\mathfrak{a}] := \begin{cases} \left(\frac{\sigma(\alpha)\sigma\tau(\alpha)}{\alpha}\right)_{\mathbb{Q}(\zeta_{12}),3} & \text{if } \gcd(\mathfrak{a},(3)) = 1 \\ 0 & \text{otherwise,} \end{cases}$$

where $\alpha$ is any generator of $\mathfrak{a}$. The symbol is well-defined, and satisfies

$$\sum_{\rho \in \mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q})} [\rho(\mathfrak{p})] = \begin{cases} -2 & \text{if } a_p(E) \text{ is not a cube modulo } p \\ 4 & \text{if } a_p(E) \text{ is a cube modulo } p \end{cases}$$

for $\mathfrak{p}$ a split prime of degree 1 (i.e. $p = \mathfrak{p} \cap \mathbb{Z}$ satisfies $p \equiv 1 \bmod 12$).

# Our main results

**Theorem (K.–Uttenthal)**

*There exists $C > 0$ such that for all $X \geq 100$*

$$\left| \sum_{\substack{N_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}}(\mathfrak{p}) \leq X \\ \mathfrak{p} \text{ prime}}} [\mathfrak{p}] \right| \leq C X^{\frac{3199}{3200}}.$$

# Our main results

### Theorem (K.–Uttenthal)

*There exists $C > 0$ such that for all $X \geq 100$*

$$\left| \sum_{\substack{N_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}}(\mathfrak{p}) \leq X \\ \mathfrak{p} \text{ prime}}} [\mathfrak{p}] \right| \leq C X^{\frac{3199}{3200}}.$$

### Corollary (K.–Uttenthal)

*We have*

$$\frac{\#\{p \equiv 1 \bmod 12 : a_p(E) \text{ is a cube modulo } p\}}{\#\{p \equiv 1 \bmod 12\}} = \frac{1}{3} + O\left(\frac{\log X}{X^{1/3200}}\right).$$

# Our main results

**Theorem (K.–Uttenthal)**

*There exists $C > 0$ such that for all $X \geq 100$*

$$\left| \sum_{\substack{N_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}}(\mathfrak{p}) \leq X \\ \mathfrak{p} \text{ prime}}} [\mathfrak{p}] \right| \leq C X^{\frac{3199}{3200}}.$$

**Corollary (K.–Uttenthal)**

*We have*

$$\frac{\#\{p \equiv 1 \bmod 12 : a_p(E) \text{ is a cube modulo } p\}}{\#\{p \equiv 1 \bmod 12\}} = \frac{1}{3} + O\left(\frac{\log X}{X^{1/3200}}\right).$$

In fact, one can prove a similar result for any imaginary quadratic field, which has applications to a conjecture of Weston.

# Spin of prime ideals

**Definition**

*Let $K/\mathbb{Q}$ be a totally real Galois field and assume that all totally positive units (i.e. positive in every real embedding) are squares.*

# Spin of prime ideals

**Definition**

*Let $K/\mathbb{Q}$ be a totally real Galois field and assume that all totally positive units (i.e. positive in every real embedding) are squares.*

*Given $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and a principal prime $\mathfrak{p}$ of $K$ admitting a totally positive generator, FIMR define*

$$\mathrm{spin}(\sigma, \mathfrak{p}) = \left(\frac{\sigma(\pi)}{\mathfrak{p}}\right)_{K,2},$$

*where $(\cdot/\cdot)_{K,2}$ is the quadratic residue symbol in $K$ and where $\pi$ is any totally positive generator of $\mathfrak{p}$.*

# Spin of prime ideals

**Definition**

*Let $K/\mathbb{Q}$ be a totally real Galois field and assume that all totally positive units (i.e. positive in every real embedding) are squares.*

*Given $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and a principal prime $\mathfrak{p}$ of $K$ admitting a totally positive generator, FIMR define*

$$\mathrm{spin}(\sigma, \mathfrak{p}) = \left(\frac{\sigma(\pi)}{\mathfrak{p}}\right)_{K,2},$$

*where $(\cdot/\cdot)_{K,2}$ is the quadratic residue symbol in $K$ and where $\pi$ is any totally positive generator of $\mathfrak{p}$. This is well-defined, as changing the generator $\pi$ of $\mathfrak{p}$ changes $\pi$ by the square of a unit.*

# The main result of FIMR

**Theorem (FIMR)**

*Assume that $K/\mathbb{Q}$ is cyclic of degree $n$ and that $\sigma$ is a generator of* $\mathrm{Gal}(K/\mathbb{Q})$. *If $n \geq 4$, assume a short character sum conjecture. There exists $\delta > 0$ such that for all $X \geq 100$*

$$\left| \sum_{N_{K/\mathbb{Q}}(\mathfrak{p}) \leq X} \mathrm{spin}(\sigma, \mathfrak{p}) \right| \ll X^{1-\delta}.$$

*Here the sum is over prime ideals $\mathfrak{p}$ admitting a totally positive generator.*

# The main result of FIMR

**Theorem (FIMR)**

*Assume that $K/\mathbb{Q}$ is cyclic of degree $n$ and that $\sigma$ is a generator of $\mathrm{Gal}(K/\mathbb{Q})$. If $n \geq 4$, assume a short character sum conjecture. There exists $\delta > 0$ such that for all $X \geq 100$*

$$\left| \sum_{N_{K/\mathbb{Q}}(\mathfrak{p}) \leq X} \mathrm{spin}(\sigma, \mathfrak{p}) \right| \ll X^{1-\delta}.$$

*Here the sum is over prime ideals $\mathfrak{p}$ admitting a totally positive generator.*

We adapt their arguments to cubic residue symbols and the field $K = \mathbb{Q}(\zeta_{12})$, which is neither cyclic nor totally real, and has degree $\geq 4$.

# The main result of FIMR

**Theorem (FIMR)**

*Assume that $K/\mathbb{Q}$ is cyclic of degree $n$ and that $\sigma$ is a generator of $\mathrm{Gal}(K/\mathbb{Q})$. If $n \geq 4$, assume a short character sum conjecture. There exists $\delta > 0$ such that for all $X \geq 100$*

$$\left| \sum_{N_{K/\mathbb{Q}}(\mathfrak{p}) \leq X} \mathrm{spin}(\sigma, \mathfrak{p}) \right| \ll X^{1-\delta}.$$

*Here the sum is over prime ideals $\mathfrak{p}$ admitting a totally positive generator.*

We adapt their arguments to cubic residue symbols and the field $K = \mathbb{Q}(\zeta_{12})$, which is neither cyclic nor totally real, and has degree $\geq 4$.

Our main analytic achievement is in making their techniques unconditional in this case.

# Applications of spins

Spins have found numerous applications since their inception. They measure the splitting of $\pi$ in $K(\sqrt{\sigma(\pi)})$. Applications include

# Applications of spins

Spins have found numerous applications since their inception. They measure the splitting of $\pi$ in $K(\sqrt{\sigma(\pi)})$. Applications include

- 2-Selmer ranks of elliptic curves in quadratic twist families indexed by primes (FIMR),

# Applications of spins

Spins have found numerous applications since their inception. They measure the splitting of $\pi$ in $K(\sqrt{\sigma(\pi)})$. Applications include

- 2-Selmer ranks of elliptic curves in quadratic twist families indexed by primes (FIMR),
- 16-rank of the class group of $\mathbb{Q}(\sqrt{-2p})$ and $\mathbb{Q}(\sqrt{-p})$ (Milovic, K.-Milovic, K.),

# Applications of spins

Spins have found numerous applications since their inception. They measure the splitting of $\pi$ in $K(\sqrt{\sigma(\pi)})$. Applications include

- 2-Selmer ranks of elliptic curves in quadratic twist families indexed by primes (FIMR),
- 16-rank of the class group of $\mathbb{Q}(\sqrt{-2p})$ and $\mathbb{Q}(\sqrt{-p})$ (Milovic, K.-Milovic, K.),
- Ramakrishna's question, Weston's conjecture and Weston–Zaurova conjecture (Weston–Zaurova),

# Applications of spins

Spins have found numerous applications since their inception. They measure the splitting of $\pi$ in $K(\sqrt{\sigma(\pi)})$. Applications include

- 2-Selmer ranks of elliptic curves in quadratic twist families indexed by primes (FIMR),
- 16-rank of the class group of $\mathbb{Q}(\sqrt{-2p})$ and $\mathbb{Q}(\sqrt{-p})$ (Milovic, K.-Milovic, K.),
- Ramakrishna's question, Weston's conjecture and Weston–Zaurova conjecture (Weston–Zaurova),
- residue field degrees of primes $\mathfrak{p}$ in the ray class field of $K$ of conductor $p$,

# Applications of spins

Spins have found numerous applications since their inception. They measure the splitting of $\pi$ in $K(\sqrt{\sigma(\pi)})$. Applications include

- 2-Selmer ranks of elliptic curves in quadratic twist families indexed by primes (FIMR),
- 16-rank of the class group of $\mathbb{Q}(\sqrt{-2p})$ and $\mathbb{Q}(\sqrt{-p})$ (Milovic, K.-Milovic, K.),
- Ramakrishna's question, Weston's conjecture and Weston–Zaurova conjecture (Weston–Zaurova),
- residue field degrees of primes $\mathfrak{p}$ in the ray class field of $K$ of conductor $p$,
- lifting problems of Galois representations.

# Proving oscillation of spins: Vinogradov's sieve

Vinogradov's sieve is the only sieve at the moment that is able to catch primes. We will discuss it for simplicity over $\mathbb{Z}$.

# Proving oscillation of spins: Vinogradov's sieve

Vinogradov's sieve is the only sieve at the moment that is able to catch primes. We will discuss it for simplicity over $\mathbb{Z}$.

Let $a_p$ be a sequence indexed by primes. We wish to estimate $\sum_{p \leq X} a_p$.

# Proving oscillation of spins: Vinogradov's sieve

Vinogradov's sieve is the only sieve at the moment that is able to catch primes. We will discuss it for simplicity over $\mathbb{Z}$.

Let $a_p$ be a sequence indexed by primes. We wish to estimate $\sum_{p \leq X} a_p$.

**Theorem (Vinogradov's sieve)**

*Let $y_n$ be a sequence indexed by positive integers such that $y_p = a_p$ for all primes $p$. Assume that we have good estimates for*

$$\sum_{\substack{n \leq X \\ n \equiv 0 \bmod q}} y_n \qquad \text{(sums of type I, linear sums)}$$

*uniformly in $q$,*

# Proving oscillation of spins: Vinogradov's sieve

Vinogradov's sieve is the only sieve at the moment that is able to catch primes. We will discuss it for simplicity over $\mathbb{Z}$.

Let $a_p$ be a sequence indexed by primes. We wish to estimate $\sum_{p \leq X} a_p$.

**Theorem (Vinogradov's sieve)**

*Let $y_n$ be a sequence indexed by positive integers such that $y_p = a_p$ for all primes $p$. Assume that we have good estimates for*

$$\sum_{\substack{n \leq X \\ n \equiv 0 \bmod q}} y_n \qquad \text{(sums of type I, linear sums)}$$

*uniformly in $q$, and*

$$\sum_{n \leq X} \sum_{m \leq Y} \alpha_n \beta_m y_{nm} \qquad \text{(sums of type II, bilinear sums)}$$

*for all $\alpha_n, \beta_m \in \mathbb{C}$ bounded by 1.*

# Proving oscillation of spins: Vinogradov's sieve

Vinogradov's sieve is the only sieve at the moment that is able to catch primes. We will discuss it for simplicity over $\mathbb{Z}$.

Let $a_p$ be a sequence indexed by primes. We wish to estimate $\sum_{p \leq X} a_p$.

**Theorem (Vinogradov's sieve)**

*Let $y_n$ be a sequence indexed by positive integers such that $y_p = a_p$ for all primes $p$. Assume that we have good estimates for*

$$\sum_{\substack{n \leq X \\ n \equiv 0 \bmod q}} y_n \qquad \text{(sums of type I, linear sums)}$$

*uniformly in $q$, and*

$$\sum_{n \leq X} \sum_{m \leq Y} \alpha_n \beta_m y_{nm} \qquad \text{(sums of type II, bilinear sums)}$$

*for all $\alpha_n, \beta_m \in \mathbb{C}$ bounded by $1$.*

*Then we get an estimate for $\sum_{p \leq X} a_p$.*

# Extending the sequence

Note that the first goal of Vinogradov's sequence is to extend the original sequence $a_p$ to a new sequence $y_n$ that matches $a_p$ on the primes.

# Extending the sequence

Note that the first goal of Vinogradov's sequence is to extend the original sequence $a_p$ to a new sequence $y_n$ that matches $a_p$ on the primes.

There are natural candidates for this both in our problem, namely the symbol $[\mathfrak{a}]$, and also in FIMR, namely

$$\mathrm{spin}(\sigma, \mathfrak{a}) = \left(\frac{\sigma(\alpha)}{\mathfrak{a}}\right)_{K,2},$$

where $\alpha$ is a totally positive generator of $\mathfrak{a}$.

# Sums of type II

Let $\alpha_{\mathfrak{n}}, \beta_{\mathfrak{m}} \in \mathbb{C}$ be bounded by 1. The bilinear sums

$$\sum_{N_{K/\mathbb{Q}}(\mathfrak{n}) \leq X} \sum_{N_{K/\mathbb{Q}}(\mathfrak{m}) \leq Y} \alpha_{\mathfrak{n}} \beta_{\mathfrak{m}} \mathrm{spin}(\sigma, \mathfrak{n}\mathfrak{m})$$

are relatively easy.

# Sums of type II

Let $\alpha_{\mathfrak{n}}, \beta_{\mathfrak{m}} \in \mathbb{C}$ be bounded by 1. The bilinear sums

$$\sum_{N_{K/\mathbb{Q}}(\mathfrak{n}) \leq X} \sum_{N_{K/\mathbb{Q}}(\mathfrak{m}) \leq Y} \alpha_{\mathfrak{n}} \beta_{\mathfrak{m}} \mathrm{spin}(\sigma, \mathfrak{n}\mathfrak{m})$$

are relatively easy.

Indeed, the key point is the "twisted multiplicativity" of spin

$$\mathrm{spin}(\sigma, \mathfrak{n}\mathfrak{m}) = \mathrm{spin}(\sigma, \mathfrak{n})\mathrm{spin}(\sigma, \mathfrak{m})t(\mathfrak{n}, \mathfrak{m}).$$

# Sums of type II

Let $\alpha_{\mathfrak{n}}, \beta_{\mathfrak{m}} \in \mathbb{C}$ be bounded by 1. The bilinear sums

$$\sum_{N_{K/\mathbb{Q}}(\mathfrak{n}) \leq X} \sum_{N_{K/\mathbb{Q}}(\mathfrak{m}) \leq Y} \alpha_{\mathfrak{n}} \beta_{\mathfrak{m}} \mathrm{spin}(\sigma, \mathfrak{n}\mathfrak{m})$$

are relatively easy.

Indeed, the key point is the "twisted multiplicativity" of spin

$$\mathrm{spin}(\sigma, \mathfrak{n}\mathfrak{m}) = \mathrm{spin}(\sigma, \mathfrak{n})\mathrm{spin}(\sigma, \mathfrak{m}) t(\mathfrak{n}, \mathfrak{m}).$$

The twist factor $t(\mathfrak{n}, \mathfrak{m})$ can be computed explicitly and roughly looks like the Legendre symbol

$$\left(\frac{\eta}{\mu}\right)_{K,2} \qquad \mathfrak{n} = (\eta), \mathfrak{m} = (\mu).$$

# Sums of type II

Let $\alpha_{\mathfrak{n}}, \beta_{\mathfrak{m}} \in \mathbb{C}$ be bounded by 1. The bilinear sums

$$\sum_{N_{K/\mathbb{Q}}(\mathfrak{n})\leq X} \sum_{N_{K/\mathbb{Q}}(\mathfrak{m})\leq Y} \alpha_{\mathfrak{n}}\beta_{\mathfrak{m}}\mathrm{spin}(\sigma, \mathfrak{n}\mathfrak{m})$$

are relatively easy.

Indeed, the key point is the "twisted multiplicativity" of spin

$$\mathrm{spin}(\sigma, \mathfrak{n}\mathfrak{m}) = \mathrm{spin}(\sigma, \mathfrak{n})\mathrm{spin}(\sigma, \mathfrak{m})t(\mathfrak{n}, \mathfrak{m}).$$

The twist factor $t(\mathfrak{n}, \mathfrak{m})$ can be computed explicitly and roughly looks like the Legendre symbol

$$\left(\frac{\eta}{\mu}\right)_{K,2} \qquad \mathfrak{n} = (\eta), \mathfrak{m} = (\mu).$$

Absorbing $\mathrm{spin}(\sigma, \mathfrak{n})$ and $\mathrm{spin}(\sigma, \mathfrak{m})$ in the coefficients $\alpha_{\mathfrak{n}}$ and $\beta_{\mathfrak{m}}$, it suffices to estimate

$$\sum_{N_{K/\mathbb{Q}}(\mathfrak{n})\leq X, \mathfrak{n}=(\eta)} \sum_{N_{K/\mathbb{Q}}(\mathfrak{m})\leq Y, \mathfrak{m}=(\mu)} \alpha_{\mathfrak{n}}\beta_{\mathfrak{m}} \left(\frac{\eta}{\mu}\right)_{K,2}.$$

# Sums of type II

Let $\alpha_{\mathfrak{n}}, \beta_{\mathfrak{m}} \in \mathbb{C}$ be bounded by 1. The bilinear sums

$$\sum_{N_{K/\mathbb{Q}}(\mathfrak{n}) \leq X} \sum_{N_{K/\mathbb{Q}}(\mathfrak{m}) \leq Y} \alpha_{\mathfrak{n}} \beta_{\mathfrak{m}} \mathrm{spin}(\sigma, \mathfrak{n}\mathfrak{m})$$

are relatively easy.

Indeed, the key point is the "twisted multiplicativity" of spin

$$\mathrm{spin}(\sigma, \mathfrak{n}\mathfrak{m}) = \mathrm{spin}(\sigma, \mathfrak{n})\mathrm{spin}(\sigma, \mathfrak{m}) t(\mathfrak{n}, \mathfrak{m}).$$

The twist factor $t(\mathfrak{n}, \mathfrak{m})$ can be computed explicitly and roughly looks like the Legendre symbol

$$\left(\frac{\eta}{\mu}\right)_{K,2} \qquad \mathfrak{n} = (\eta), \mathfrak{m} = (\mu).$$

Absorbing $\mathrm{spin}(\sigma, \mathfrak{n})$ and $\mathrm{spin}(\sigma, \mathfrak{m})$ in the coefficients $\alpha_{\mathfrak{n}}$ and $\beta_{\mathfrak{m}}$, it suffices to estimate

$$\sum_{N_{K/\mathbb{Q}}(\mathfrak{n}) \leq X, \mathfrak{n} = (\eta)} \sum_{N_{K/\mathbb{Q}}(\mathfrak{m}) \leq Y, \mathfrak{m} = (\mu)} \alpha_{\mathfrak{n}} \beta_{\mathfrak{m}} \left(\frac{\eta}{\mu}\right)_{K,2}.$$

This can be handled using large sieve techniques.

# Sums of type I

The essential difficulty lies in the estimation of sums of type I. These are

$$\sum_{\substack{N_{K/\mathbb{Q}}(\mathfrak{a})\leq X \\ \mathfrak{a}=(\alpha),\alpha \text{ tot. pos.}}} \left(\frac{\sigma(\alpha)}{\alpha}\right)_{K,2},$$

where we have taken $q = 1$ for simplicity.

# Sums of type I

The essential difficulty lies in the estimation of sums of type I. These are

$$\sum_{\substack{N_{K/\mathbb{Q}}(\mathfrak{a})\leq X \\ \mathfrak{a}=(\alpha),\alpha \text{ tot. pos.}}} \left(\frac{\sigma(\alpha)}{\alpha}\right)_{K,2},$$

where we have taken $q = 1$ for simplicity.

The insight of FIMR is to approach this as follows: we split

$$O_K = \mathbb{Z} \oplus \mathbb{M},$$

so $\alpha = a + \beta$ with $a \in \mathbb{Z}$, $\beta \in \mathbb{M}$.

# Sums of type I

The essential difficulty lies in the estimation of sums of type I. These are

$$\sum_{\substack{N_{K/\mathbb{Q}}(\mathfrak{a})\leq X\\ \mathfrak{a}=(\alpha),\alpha \text{ tot. pos.}}} \left(\frac{\sigma(\alpha)}{\alpha}\right)_{K,2},$$

where we have taken $q = 1$ for simplicity.

The insight of FIMR is to approach this as follows: we split

$$O_K = \mathbb{Z} \oplus \mathbb{M},$$

so $\alpha = a + \beta$ with $a \in \mathbb{Z}$, $\beta \in \mathbb{M}$.

Then we have $\sigma(\alpha) = a + \sigma(\beta)$, hence

$$\left(\frac{\sigma(\alpha)}{\alpha}\right)_{K,2} = \left(\frac{a+\sigma(\beta)}{a+\beta}\right)_{K,2} = \left(\frac{\sigma(\beta)-\beta}{a+\beta}\right)_{K,2} \approx \left(\frac{a+\beta}{\sigma(\beta)-\beta}\right)_{K,2}.$$

# Sums of type I, continued

Recall that $O_K = \mathbb{Z} \oplus \mathbb{M}$, $\alpha = a + \beta$ and

$$\left(\frac{\sigma(\alpha)}{\alpha}\right)_{K,2} = \left(\frac{a+\beta}{\sigma(\beta)-\beta}\right)_{K,2}.$$

# Sums of type I, continued

Recall that $O_K = \mathbb{Z} \oplus \mathbb{M}$, $\alpha = a + \beta$ and

$$\left(\frac{\sigma(\alpha)}{\alpha}\right)_{K,2} = \left(\frac{a+\beta}{\sigma(\beta)-\beta}\right)_{K,2}.$$

Therefore we need to estimate

$$\sum_{\beta \in \mathbb{M}} \sum_{\substack{a \in \mathbb{Z} \\ N_{K/\mathbb{Q}}(a+\beta) \leq X}} \left(\frac{a+\beta}{\sigma(\beta)-\beta}\right)_{K,2}.$$

# Sums of type I, continued

Recall that $O_K = \mathbb{Z} \oplus \mathbb{M}$, $\alpha = a + \beta$ and

$$\left(\frac{\sigma(\alpha)}{\alpha}\right)_{K,2} = \left(\frac{a+\beta}{\sigma(\beta)-\beta}\right)_{K,2}.$$

Therefore we need to estimate

$$\sum_{\beta \in \mathbb{M}} \sum_{\substack{a \in \mathbb{Z} \\ N_{K/\mathbb{Q}}(a+\beta) \leq X}} \left(\frac{a+\beta}{\sigma(\beta)-\beta}\right)_{K,2}.$$

We now fix $\beta$, then $a$ runs over a sum of typical length $X^{1/n}$, while the conductor is $N_{K/\mathbb{Q}}(\sigma(\beta) - \beta)$ typically of size $X$. So our sum is "short". Here is where the short character sum conjecture comes in.

# Sums of type I, continued

Recall that $O_K = \mathbb{Z} \oplus \mathbb{M}$, $\alpha = a + \beta$ and

$$\left(\frac{\sigma(\alpha)}{\alpha}\right)_{K,2} = \left(\frac{a+\beta}{\sigma(\beta)-\beta}\right)_{K,2}.$$

Therefore we need to estimate

$$\sum_{\beta \in \mathbb{M}} \sum_{\substack{a \in \mathbb{Z} \\ N_{K/\mathbb{Q}}(a+\beta) \leq X}} \left(\frac{a+\beta}{\sigma(\beta)-\beta}\right)_{K,2}.$$

We now fix $\beta$, then $a$ runs over a sum of typical length $X^{1/n}$, while the conductor is $N_{K/\mathbb{Q}}(\sigma(\beta)-\beta)$ typically of size $X$. So our sum is "short". Here is where the short character sum conjecture comes in.

Technical warning: to make this precise, note that every ideal $\mathfrak{a}$ has infinitely many generators. So to avoid our sums running over infinitely many terms, we need to construct a fundamental domain and pick for each ideal $\mathfrak{a}$ the unique generator from the fundamental domain.

# Why does FIMR only allow cyclic Galois groups?

The character $\left(\frac{a+\beta}{\sigma(\beta)-\beta}\right)_{K,2}$ does not oscillate if $\sigma(\beta)-\beta$ is a square.

# Why does FIMR only allow cyclic Galois groups?

The character $\left(\frac{a+\beta}{\sigma(\beta)-\beta}\right)_{K,2}$ does not oscillate if $\sigma(\beta) - \beta$ is a square.

In fact, because of the way the short character sum conjecture works, we need to show that $\sigma(\beta) - \beta$ has not too large squarefull part if $\beta \in \mathbb{M}$.

# Why does FIMR only allow cyclic Galois groups?

The character $\left(\frac{a+\beta}{\sigma(\beta)-\beta}\right)_{K,2}$ does not oscillate if $\sigma(\beta)-\beta$ is a square.

In fact, because of the way the short character sum conjecture works, we need to show that $\sigma(\beta)-\beta$ has not too large squarefull part if $\beta \in \mathbb{M}$.

This gets increasingly difficult as $\mathbb{M}$ has smaller rank compared to $O_K$. In FIMR, the $\mathbb{Z}$-rank of $\mathbb{M}$ is $n-1$ exactly because $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic of degree $n$ and $\sigma$ is a generator.

# Why does FIMR only allow cyclic Galois groups?

The character $\left(\frac{a+\beta}{\sigma(\beta)-\beta}\right)_{K,2}$ does not oscillate if $\sigma(\beta)-\beta$ is a square.

In fact, because of the way the short character sum conjecture works, we need to show that $\sigma(\beta)-\beta$ has not too large squarefull part if $\beta \in \mathbb{M}$.

This gets increasingly difficult as $\mathbb{M}$ has smaller rank compared to $O_K$. In FIMR, the $\mathbb{Z}$-rank of $\mathbb{M}$ is $n-1$ exactly because $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic of degree $n$ and $\sigma$ is a generator.

This difficulty was overcome by K.-Milovic, who also obtained the joint distribution of spins

$$\prod_{\sigma \in S} \mathrm{spin}(\sigma, \mathfrak{p}),$$

for any subset $S$ of $\mathrm{Gal}(K/\mathbb{Q})$ satisfying $\sigma \in S \Rightarrow \sigma^{-1} \notin S$.

# Why does FIMR only allow cyclic Galois groups?

The character $\left(\frac{a+\beta}{\sigma(\beta)-\beta}\right)_{K,2}$ does not oscillate if $\sigma(\beta)-\beta$ is a square.

In fact, because of the way the short character sum conjecture works, we need to show that $\sigma(\beta)-\beta$ has not too large squarefull part if $\beta \in \mathbb{M}$.

This gets increasingly difficult as $\mathbb{M}$ has smaller rank compared to $O_K$. In FIMR, the $\mathbb{Z}$-rank of $\mathbb{M}$ is $n-1$ exactly because $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic of degree $n$ and $\sigma$ is a generator.

This difficulty was overcome by K.-Milovic, who also obtained the joint distribution of spins

$$\prod_{\sigma \in S} \mathrm{spin}(\sigma, \mathfrak{p}),$$

for any subset $S$ of $\mathrm{Gal}(K/\mathbb{Q})$ satisfying $\sigma \in S \Rightarrow \sigma^{-1} \notin S$. This assumption is important because

$$\mathrm{spin}(\sigma, \mathfrak{p}) = \left(\frac{\sigma(\pi)}{\pi}\right), \qquad \mathrm{spin}(\sigma^{-1}, \mathfrak{p}) = \left(\frac{\sigma^{-1}(\pi)}{\pi}\right)$$

are related by quadratic reciprocity. This was further studied by McMeekin, and Chan–McMeekin–Milovic.

# Back to our situation

Recall the field diagram

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_{12}) \arrow[dl, dash, "\langle\sigma\rangle"'] \arrow[d, dash, "\langle\tau\rangle"'] \arrow[dr, dash, "\langle\sigma\tau\rangle"] & \\
\mathbb{Q}(\zeta_3) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd},$$

# Back to our situation

Recall the field diagram

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_{12}) \arrow[dl, dash, "\langle\sigma\rangle"'] \arrow[d, dash, "\langle\tau\rangle"'] \arrow[dr, dash, "\langle\sigma\tau\rangle"] & \\
\mathbb{Q}(\zeta_3) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd},$$

so our aim is to estimate the type I sums

$$\sum_{\substack{\alpha\in\mathbb{Z}[\zeta_{12}] \\ N_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}}(\alpha)\le X}} \left(\frac{\sigma(\alpha)\sigma\tau(\alpha)}{\alpha}\right)_{\mathbb{Q}(\zeta_{12}),3}.$$

# Field lowering

It turns out that the symbol

$$\left(\frac{\sigma\tau(\alpha)}{\alpha}\right)_{\mathbb{Q}(\zeta_{12}),3}$$

is "almost" identically equal to 1, while the other symbol can be "lowered" to $\mathbb{Q}(\zeta_3)$.

# Field lowering

It turns out that the symbol

$$\left(\frac{\sigma\tau(\alpha)}{\alpha}\right)_{\mathbb{Q}(\zeta_{12}),3}$$

is "almost" identically equal to 1, while the other symbol can be "lowered" to $\mathbb{Q}(\zeta_3)$.

So the modulus of the character becomes $X^{1/2}$ instead of $X \cdot X = X^2$, while the sum over $a \in \mathbb{Z}$ is still of length $X^{1/4}$.

# Field lowering

It turns out that the symbol

$$\left(\frac{\sigma\tau(\alpha)}{\alpha}\right)_{\mathbb{Q}(\zeta_{12}),3}$$

is “almost” identically equal to 1, while the other symbol can be “lowered” to $\mathbb{Q}(\zeta_3)$.

So the modulus of the character becomes $X^{1/2}$ instead of $X \cdot X = X^2$, while the sum over $a \in \mathbb{Z}$ is still of length $X^{1/4}$.

Thus we can apply Burgess inequality in this range to get our savings.

# Field lowering

It turns out that the symbol

$$\left(\frac{\sigma\tau(\alpha)}{\alpha}\right)_{\mathbb{Q}(\zeta_{12}),3}$$

is "almost" identically equal to 1, while the other symbol can be "lowered" to $\mathbb{Q}(\zeta_3)$.

So the modulus of the character becomes $X^{1/2}$ instead of $X \cdot X = X^2$, while the sum over $a \in \mathbb{Z}$ is still of length $X^{1/4}$.

Thus we can apply Burgess inequality in this range to get our savings.

Let us now show how this "field lowering" mechanism happens.

# Field lowering in practice

We get from the FIMR method, writing $\alpha = a + \beta$

$$\left(\frac{\sigma\tau(\alpha)}{\alpha}\right)_{\mathbb{Q}(\zeta_{12}),3} \approx \left(\frac{a+\beta}{\sigma\tau(\beta)-\beta}\right)_{\mathbb{Q}(\zeta_{12}),3}.$$

# Field lowering in practice

We get from the FIMR method, writing $\alpha = a + \beta$

$$\left(\frac{\sigma\tau(\alpha)}{\alpha}\right)_{\mathbb{Q}(\zeta_{12}),3} \approx \left(\frac{a+\beta}{\sigma\tau(\beta)-\beta}\right)_{\mathbb{Q}(\zeta_{12}),3}.$$

The ideal $(\sigma\tau(\beta) - \beta)\mathbb{Z}[\zeta_{12}]$ is fixed by $\sigma\tau$.

# Field lowering in practice

We get from the FIMR method, writing $\alpha = a + \beta$

$$\left(\frac{\sigma\tau(\alpha)}{\alpha}\right)_{\mathbb{Q}(\zeta_{12}),3} \approx \left(\frac{a+\beta}{\sigma\tau(\beta)-\beta}\right)_{\mathbb{Q}(\zeta_{12}),3}.$$

The ideal $(\sigma\tau(\beta) - \beta)\mathbb{Z}[\zeta_{12}]$ is fixed by $\sigma\tau$.

This implies that, if $\sigma\tau(\beta) - \beta$ is coprime to the ramified primes in $\mathbb{Z}[\zeta_{12}]$, it is the extension of some ideal $\mathfrak{c}$ from $\mathbb{Q}(\sqrt{3})$.

# Field lowering in practice

We get from the FIMR method, writing $\alpha = a + \beta$

$$\left(\frac{\sigma\tau(\alpha)}{\alpha}\right)_{\mathbb{Q}(\zeta_{12}),3} \approx \left(\frac{a+\beta}{\sigma\tau(\beta)-\beta}\right)_{\mathbb{Q}(\zeta_{12}),3}.$$

The ideal $(\sigma\tau(\beta) - \beta)\mathbb{Z}[\zeta_{12}]$ is fixed by $\sigma\tau$.

This implies that, if $\sigma\tau(\beta) - \beta$ is coprime to the ramified primes in $\mathbb{Z}[\zeta_{12}]$, it is the extension of some ideal $\mathfrak{c}$ from $\mathbb{Q}(\sqrt{3})$.

Furthermore, $a + \beta$ is fixed by $\sigma\tau$ modulo $\sigma\tau(\beta) - \beta$. Thus there is some $\gamma \in \mathbb{Z}[\sqrt{3}]$ such that

$$a + \beta \equiv \gamma \bmod \sigma\tau(\beta) - \beta.$$

# Field lowering in practice

We get from the FIMR method, writing $\alpha = a + \beta$

$$\left(\frac{\sigma\tau(\alpha)}{\alpha}\right)_{\mathbb{Q}(\zeta_{12}),3} \approx \left(\frac{a+\beta}{\sigma\tau(\beta)-\beta}\right)_{\mathbb{Q}(\zeta_{12}),3}.$$

The ideal $(\sigma\tau(\beta)-\beta)\mathbb{Z}[\zeta_{12}]$ is fixed by $\sigma\tau$.

This implies that, if $\sigma\tau(\beta)-\beta$ is coprime to the ramified primes in $\mathbb{Z}[\zeta_{12}]$, it is the extension of some ideal $\mathfrak{c}$ from $\mathbb{Q}(\sqrt{3})$.

Furthermore, $a+\beta$ is fixed by $\sigma\tau$ modulo $\sigma\tau(\beta)-\beta$. Thus there is some $\gamma \in \mathbb{Z}[\sqrt{3}]$ such that

$$a+\beta \equiv \gamma \bmod \sigma\tau(\beta)-\beta.$$

We rewrite

$$\left(\frac{a+\beta}{\sigma\tau(\beta)-\beta}\right)_{\mathbb{Q}(\zeta_{12}),3} = \left(\frac{a+\beta}{\mathfrak{c}\mathbb{Z}[\zeta_{12}]}\right)_{\mathbb{Q}(\zeta_{12}),3} = \left(\frac{\gamma}{\mathfrak{c}\mathbb{Z}[\zeta_{12}]}\right)_{\mathbb{Q}(\zeta_{12}),3}.$$

# The field lowering lemmas

**Lemma (Field lowering for split primes)**

*Let $K$ be a number field and let $\mathfrak{p}$ be a prime of $K$ coprime to $3$. Assume that $L$ is a quadratic extension of $K$ such that $L$ contains $\zeta_3$ and $\mathfrak{p}$ splits in $L$. Write $\sigma$ for the non-trivial element of* $\mathrm{Gal}(L/K)$*. Then for $\alpha \in O_K$*

$$\left(\frac{\alpha}{\mathfrak{p}O_L}\right)_{L,3} = \begin{cases} \left(\frac{\alpha}{\mathfrak{p}O_K}\right)_{K,3}^2 & \text{if } \sigma \text{ fixes } \zeta_3 \\ \mathbf{1}_{\mathfrak{p}\nmid\alpha} & \text{if } \sigma \text{ does not fix } \zeta_3. \end{cases}$$

# The field lowering lemmas

**Lemma (Field lowering for split primes)**

*Let $K$ be a number field and let $\mathfrak{p}$ be a prime of $K$ coprime to 3. Assume that $L$ is a quadratic extension of $K$ such that $L$ contains $\zeta_3$ and $\mathfrak{p}$ splits in $L$. Write $\sigma$ for the non-trivial element of $\mathrm{Gal}(L/K)$. Then for $\alpha \in O_K$*

$$\left(\frac{\alpha}{\mathfrak{p}O_L}\right)_{L,3} = \begin{cases} \left(\frac{\alpha}{\mathfrak{p}O_K}\right)_{K,3}^2 & \text{if } \sigma \text{ fixes } \zeta_3 \\ \mathbf{1}_{\mathfrak{p}\nmid\alpha} & \text{if } \sigma \text{ does not fix } \zeta_3. \end{cases}$$

**Lemma (Field lowering for inert primes)**

*Let $K$ be a number field and let $\mathfrak{p}$ be a prime of $K$ coprime to 3. Assume that $L$ is a quadratic extension of $K$ such that $L$ contains $\zeta_3$ and assume that $\mathfrak{p}$ stays inert in $L$. Further assume that $\mathfrak{p}$ has degree 1 in $K$ and let $p$ be the prime of $\mathbb{Q}$ lying below $\mathfrak{p}$. Then we have for all $\alpha \in O_K$*

$$\left(\frac{\alpha}{\mathfrak{p}O_L}\right)_{L,3} = \left(\frac{\alpha}{\mathfrak{p}O_K}\right)_{K,3}^{p+1}.$$

# Questions?

Thank you for your attention!