Arithmetic triple linking numbers

YRANT V - Cambridge

Yan Yau Cheng

University of Edinburgh

8 September 2023

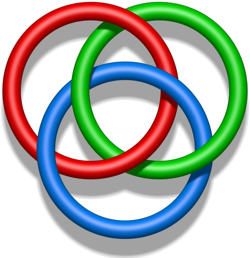
The Knots and Primes analogy

In the 1960s, Barry Mazur noticed an analogy between knots in a three manifold and primes in a number field.

Topology	Arithmetic
3-Manifold M e.g. S^3	Number Ring $\operatorname{Spec}\mathcal{O}_K$ e.g. $\operatorname{Spec}\mathbb{Z}$
Knot $K : S^1 \hookrightarrow M$	Prime ideal $\mathfrak{p} \triangleleft \mathcal{O}_k$ $\operatorname{Spec}\mathbb{F}_{\mathfrak{p}} \hookrightarrow \operatorname{Spec}\mathcal{O}_K$
Tubular ngbd $V(K)$ of K Torus $\partial V(K)$	p-adic integers $\operatorname{Spec}\mathcal{O}_{K_{\mathfrak{p}}}$ p-adic field $\operatorname{Spec} K_{\mathfrak{p}}$
Linking Number $\mathrm{lk}(L, K)$	Power Residue Symbol $\left(\frac{\mathfrak{p}}{\mathfrak{q}}\right)_n$

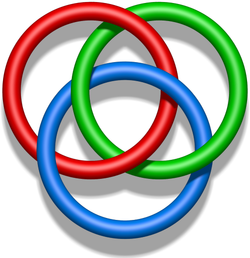
Borromean Rings

The Borromean Rings is a set of three rings that are pairwise unlinked, but altogether linked.



Borromean Rings

The Borromean Rings is a set of three rings that are pairwise unlinked, but altogether linked.



The Borromean Rings cannot be detected by linking numbers, but the *Milnor invariants* can be defined for multiple knots and can detect phenomena such as the Borromean Rings.

Arithmetic Milnor Invariants

We wish to define multiple linking numbers mod l. Fix a prime number l, and suppose $S = \{p_1, p_2, p_3\}$ is a set of primes of $\mathcal{O}_K$ with $p_i \equiv 1 \pmod{l}$.

Arithmetic Milnor Invariants

We wish to define multiple linking numbers mod l. Fix a prime number l, and suppose $S = \{p_1, p_2, p_3\}$ is a set of primes of $\mathcal{O}_K$ with $p_i \equiv 1 \pmod{l}$.

Let τ_i be a monodromy over p_i and σ_i be a lift of the p_i Frobenius. These are elements of $G_S = \mathrm{Gal}(K_S/K)$ which satisfy the following:

$$\tau_i(\zeta_{l^n}) = \zeta_{l^n}; \quad \tau_i(\sqrt[l^n]{p_i}) = \zeta_{l_n} \sqrt[l^n]{p_i}$$
$$\sigma_i(\zeta_{l^n}) = \zeta_{l^n}^{p_i}; \quad \sigma_i(\sqrt[l^n]{p_i}) = \sqrt[l^n]{p_i}$$

Arithmetic Milnor Invariants

We wish to define multiple linking numbers mod l. Fix a prime number l, and suppose $S = \{p_1, p_2, p_3\}$ is a set of primes of $\mathcal{O}_K$ with $p_i \equiv 1 \pmod{l}$.

Let τ_i be a monodromy over p_i and σ_i be a lift of the p_i Frobenius. These are elements of $G_S = \mathrm{Gal}(K_S/K)$ which satisfy the following:

$$\tau_i(\zeta_{l^n}) = \zeta_{l^n}; \quad \tau_i(\sqrt[l^n]{p_i}) = \zeta_{l_n} \sqrt[l^n]{p_i}$$
$$\sigma_i(\zeta_{l^n}) = \zeta_{l^n}^{p_i}; \quad \sigma_i(\sqrt[l^n]{p_i}) = \sqrt[l^n]{p_i}$$

If $K = \mathbb{Q}$ there is a theorem of Koch ([KGR70]) where the maximal pro-l quotient of the Galois Group G_S has the following presentation:

$$G_S(l) \cong \left\langle x_1, \ldots x_r | x_1^{p_1 - 1}[x_1, y_1] = \cdots = x_r^{p_r - 1}[x_r, y_r] = 1 \right\rangle$$

Where x_i represents the monodromy τ_i, and y_i are words that represent σ_i.

Arithmetic Milnor Invariants

Suppose these primes are pairwise unlinked mod l. i.e. $\left(\frac{p_i}{p_j}\right)_l = 1$

There is a surjective homomorphism ψ from G_S to the Heisenberg Group with entries in $\mathbb{Z}/l\mathbb{Z}$ such that:

$$\tau_1 \mapsto \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} ; \tau_2 \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Arithmetic Milnor Invariants

Suppose these primes are pairwise unlinked mod l. i.e. $\left(\frac{p_i}{p_j}\right)_l = 1$

There is a surjective homomorphism ψ from G_S to the Heisenberg Group with entries in $\mathbb{Z}/l\mathbb{Z}$ such that:

$$\tau_1 \mapsto \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \tau_2 \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Moreover, the Frobenius σ_3 of p_3 will be mapped to a matrix of the form:

$$\begin{pmatrix} 1 & 0 & \mu \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Arithmetic Triple Linking Numbers

Let L/K be the extension of K corresponding to the kernel $\ker\psi$. Then $\mathrm{Gal}(L/K) \cong H_3(\mathbb{Z}/l\mathbb{Z})$ is ramified only at the primes p_1, p_2, and also dependent only on p_1, p_2.

Arithmetic Triple Linking Numbers

Let L/K be the extension of K corresponding to the kernel $\ker\psi$. Then $\mathrm{Gal}(L/K) \cong H_3(\mathbb{Z}/l\mathbb{Z})$ is ramified only at the primes p_1, p_2, and also dependent only on p_1, p_2.

If K contains a primitive lth root of unity ζ_l, then we define the mod l linking number of p_1, p_2, p_3 to be:

$$[p_1, p_2, p_3]_l = \zeta_l^{\mu}$$

The triple linking number measures whether p_3 splits or is inert in L/K.

Rédei Triple Symbols

In the case of $l = 2$, Rédei (1939) gave an explicit construction of the extension $L/\mathbb{Q}$ and interprets the Rédei Triple Symbol $[p_1, p_2, p_3]$ as a generalisation of the Legendre Symbol. [Réd39]

[1] Amano-Kodani-Morishita-Sakamoto-Ogasawara-Yoshida

Rédei Triple Symbols

In the case of $l = 2$, Rédei (1939) gave an explicit construction of the extension $L/\mathbb{Q}$ and interprets the Rédei Triple Symbol $[p_1, p_2, p_3]$ as a generalisation of the Legendre Symbol. [Réd39]

In 2013, a paper by Amano et al.[1] gives a way to calculate Rédei Triple Symbols through counting lattice points on quadratic forms, and can also be expressed as a Fourier coefficient of a modular form of weight one, gives an explicit and constructive example of the theorem by Weil-Langlands and Deligne-Serre. [AKMOSY13]

[1] Amano-Kodani-Morishita-Sakamoto-Ogasawara-Yoshida

Outline of Proof

1. Construct a $\mathbb{C}$-representation $\rho : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ of the Rédei extension $L/\mathbb{Q}$ such that

$$[-p_1, p_2, p_3] = \frac{1}{2} \operatorname{tr} \rho(\sigma_{p_3})$$

Then the triple symbols are encoded in the coefficients of the Artin L-function:

$$L(\rho, s) = \prod_p L_p(\rho, s)$$

$$L_p(\rho, s) = \det_{V^{I_p}} \left(I - t\rho(\sigma_p)\right)^{-1}$$

Outline of Proof

2. Construct a 1-dimensional character $\chi : \mathrm{Gal}(L/M) \to \mathbb{C}^\times$ of a sub-extension L/M such that $\mathrm{Ind}\,\chi$ is equivalent to ρ. Then we have an equality of L-functions:

$$L(\chi, s) = L(\rho, s)$$

In particular L/M is abelian so we can factor χ through the class group H_M to get a Hecke character and Hecke L-function that is also equal.

$$\boldsymbol{\chi} = \chi \circ \left(\frac{L/M}{\cdot}\right) : H_M \to \mathbb{C}^\times$$

$$L(\boldsymbol{\chi}, s) = L(\chi, s) = L(\rho, s)$$

Outline of Proof

3. $M = \mathbb{Q}(\sqrt{-p_1p_2})$ is a quadratic extension over $\mathbb{Q}$. Since there is a bijection between the class group H_M and quadratic forms with the same discriminant, let Q_i be the quadratic form associated to ideal class C_i.

Lemma

Let:

$$a(C_i, n) := \#\{(x, y) \in \mathbb{Z}^2 | Q_i(x, y) = n\}$$

$$b(C_i, n) := \#\{\mathfrak{a} \in C_i^{-1} : N\mathfrak{a} = n\}$$

Then

$$a(C_i, n) = 2b(C_i, n)$$

Outline of Proof

4. We can now rewrite the L function as follows

$$\begin{aligned} L(\chi, s) &= \sum_{\mathfrak{a} \triangleleft \mathcal{O}_M} \chi([\mathfrak{a}]) N\mathfrak{a}^{-s} \\ &= \sum_{i=0}^{h_M - 1} \chi(C_i^{-1}) \sum_{\mathfrak{a} \in C_i^{-1}} N\mathfrak{a}^{-s} \\ &= \sum_{i=0}^{h_M - 1} \chi(C_i^{-1}) \sum_{n=1}^{\infty} b(C_i, n) n^{-s} \\ &= \frac{1}{2} \sum_{i=0}^{h_M - 1} \chi(C_i^{-1}) \sum_{n=1}^{\infty} a(C_i, n) n^{-s} \end{aligned}$$

So we can recover the values of the Rédei triple symbols by counting lattice points on Quadratic forms Q_i.

Outline of Proof

5. If we define:

$$\begin{cases} \theta(C_i, z) & := \dfrac{1}{2}\displaystyle\sum_{n=0}^{\infty} a(C_i, n) q^n = \dfrac{1}{2} \sum_{(x,y)\in\mathbb{Z}^2} q^{Q_i(x,y)} \\ \Theta(z) & := \displaystyle\sum_{i=0}^{h_M - 1} \boldsymbol{\chi}(C_i)\theta(C_i, z) \end{cases}$$

Then θ is a modular form, and Θ is a cuspidal eigenform. Moreover

$$L(\Theta, s) = L(\boldsymbol{\chi}, s) = L(\rho, s)$$

Giving an explicit and constructive example of the Langlands correspondence.

Question

The Rédei Triple Symbol is the mod 2 triple linking number of primes. Is it possible to extend this result to mod 3 triple linking numbers?

Question

The Rédei Triple Symbol is the mod 2 triple linking number of primes. Is it possible to extend this result to mod 3 triple linking numbers?

Since our base field K will need to contain the cubic roots of unity, we will have to work over $K = \mathbb{Q}(\sqrt{-3})$

A paper by Amano, Mizusawa, and Morishita [AMM18] gives an explicit construction of the extension L/K in this case.

Progress so far

Managed to construct analogues for ρ and χ in the mod 3 linking number case.

$$\rho : \mathrm{Gal}(L/K) \cong H_3(\mathbb{Z}/3\mathbb{Z}) \to \mathrm{GL}_3(\mathbb{C})$$

$$\begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta & 0 \\ 0 & 0 & \zeta^2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Progress so far

Managed to construct analogues for ρ and χ in the mod 3 linking number case.

$$\rho : \mathrm{Gal}(L/K) \cong H_3(\mathbb{Z}/3\mathbb{Z}) \to \mathrm{GL}_3(\mathbb{C})$$
$$\begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta & 0 \\ 0 & 0 & \zeta^2 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

This map sends $\begin{pmatrix} 1 & 0 & 1 \\ & 1 & 0 \\ & & 1 \end{pmatrix}$ to $\begin{pmatrix} \zeta & 0 & 0 \\ 0 & \zeta & 0 \\ 0 & 0 & \zeta \end{pmatrix}$, and so it satisfies:

$$[\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3]_3 = \frac{1}{3} \operatorname{tr} \rho(\sigma_{\mathfrak{p}_3})$$

Progress so far

Considering $M = L^H$ to be the intermediate field fixed by the subgroup

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ & 1 & a \\ & & 1 \end{pmatrix}; \quad a, b \in \mathbb{F}_3 \right\}$$

Progress so far

Considering $M = L^H$ to be the intermediate field fixed by the subgroup

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ & 1 & a \\ & & 1 \end{pmatrix} ; \quad a, b \in \mathbb{F}_3 \right\}$$

The character χ given by $\chi \begin{pmatrix} 1 & a & b \\ & 1 & a \\ & & 1 \end{pmatrix} = \zeta^b$ satisfies $\rho = \operatorname{Ind} \chi$.

Progress so far

Considering $M = L^H$ to be the intermediate field fixed by the subgroup

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ & 1 & a \\ & & 1 \end{pmatrix}; \quad a, b \in \mathbb{F}_3 \right\}$$

The character χ given by $\chi \begin{pmatrix} 1 & a & b \\ & 1 & a \\ & & 1 \end{pmatrix} = \zeta^b$ satisfies $\rho = \operatorname{Ind} \chi$.

Thus defining $\boldsymbol{\chi} = \chi \circ \left(\frac{L/M}{\cdot} \right) : H_M \to \mathbb{C}^\times$ we once again have the following equalities of L-functions:

$$L(\boldsymbol{\chi}, s) = L(\chi, s) = L(\rho, s)$$

Difficulties

- The intermediate field M is a degree 3 extension of $K = \mathbb{Q}(\sqrt{-3})$ rather than a degree 2 extension of $\mathbb{Q}$, so there isn't any well documented bijection between ideal classes of H_M and binary cubic forms.

Difficulties

- The intermediate field M is a degree 3 extension of $K = \mathbb{Q}(\sqrt{-3})$ rather than a degree 2 extension of $\mathbb{Q}$, so there isn't any well documented bijection between ideal classes of H_M and binary cubic forms.
- The proof of the lemma $a(C_i, n) = 2b(C_i, n)$ requires the fact that $\mathcal{O}_M^\times = \{\pm 1\}$, since the $\mathcal{O}_M^\times$ will be infinite in our case, we would have to count equivalence classes of lattice points rather than lattice points.

Thank you!

References

Ladislaus von Rédei. "Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. I.". In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 1939 (1939), pp. 1 –43 (cit. on pp. 12, 13).

Helmut Koch, Wolfgang Gröbner, and Holger Reichardt. "Galoissche Theorie der p-Erweiterungen". In: 1970 (cit. on pp. 5–7).

Fumiya Amano, Hisatoshi Kodani, Masanori Morishita, Takeshi Ogasawara, Takayuki Sakamoto, and Takafumi Yoshida. "Rédei's Triple Symbols and Modular Forms". In: *Tokyo Journal of Mathematics* 36.2 (2013), pp. 405 –427. DOI: 10.3836/tjm/1391177979. URL: https://doi.org/10.3836/tjm/1391177979 (cit. on pp. 12, 13).

Fumiya Amano, Yasushi Mizusawa, and Masanori Morishita. "On mod 3 triple Milnor invariants and triple cubic residue symbols in the Eisenstein number field". In: *Research in Number Theory* 4.1 (Feb. 2018), p. 7. ISSN: 2363-9555. DOI: 10.1007/s40993-018-0100-7. URL: https://doi.org/10.1007/s40993-018-0100-7 (cit. on pp. 19, 20).