KNOTS AND LEGENDRE SYMBOLS

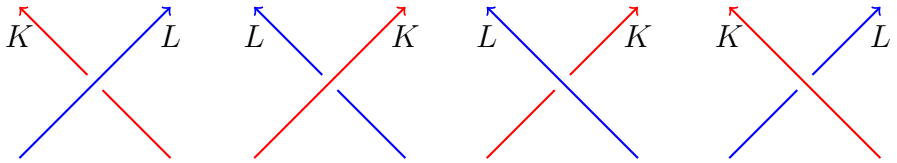
ALLEN LIN

1. Introduction

Number theory and knot theory may seem like disjoint fields of mathematics, with number theory concerned with the properties of integers and integer-valued functions and knot theory the classification and invariants of knots and links. However, over the past half-century, mathematicians have discovered many surprising analogies and connections between the two fields that became the basis of a new field of mathematics known as *arithmetic topology*. This paper focuses on the connection between the Legendre symbol and the linking number of two knots.

Recall that a subset $K \subset S^3$ is a *knot* if it is homeomorphic to S^1, and K is a *link* if K is homeomorphic to a finite disjoint union of copies of S^1. Each of these copies of S^1 is a knot that forms a *component* of the link K, and the components are possibly linked together. To determine how components interact with each other, knot theorists use the linking number $\mathrm{lk}(L, K)$, an invariant that intuitively measures how intertwined knots L and K are to each other. There are many equivalent definitions, but we discuss the definition given by the notion of positive and negative crossings. We refer the reader to Rolfsen [8] for this and other equivalent definitions.

We briefly review the definition. Let L and K be two disjoint oriented knots with n crossings. Label each crossing as *positive* or *negative* according to Figure 1.



(A) Positive crossings. (B) Negative crossings.

FIGURE 1. Positive and negative crossings.

For each crossing P_i of L and K, let

$$\varepsilon(P_i) := \begin{cases} 1 & \text{if } P_i \text{ is a positive crossing,} \\ -1 & \text{if } P_i \text{ is a negative crossing.} \end{cases}$$

Then the *linking number of L and K* is defined by

$$\mathrm{lk}(L, K) := \frac{1}{2} \sum_{\text{crossings } P_i} \varepsilon(P_i).$$

By definition, $\mathrm{lk}(L,K) = \mathrm{lk}(K,L)$, so the linking number is symmetric. We define $\mathrm{lk}_2(L,K)$ as the image of $\mathrm{lk}(L,K)$ under the surjection $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

Example 1. The 4_1^2 link has linking number ± 2 depending on orientation.

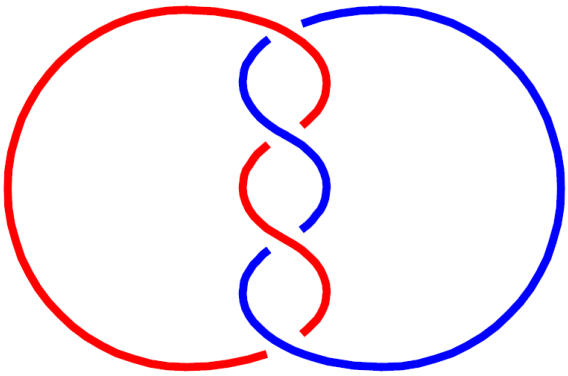


FIGURE 2. The 4_1^2 link.

The linking number of two knots has a surprising connection to the Legendre symbol. The Legendre symbol is an integer-valued function $\mathbb{F}_p \to \{\pm 1\}$ that, for any $a \in \mathbb{F}_p$, denotes whether a solution $x \in \mathbb{F}_p$ exists such that $x^2 \equiv a \pmod{p}$. Such elements $a \in \left(\mathbb{F}_p^\times\right)^2 \coloneqq \left\{x^2 \mid x \in \mathbb{F}_p^\times\right\}$ form the set of quadratic residues modulo p. Then the Legendre symbol is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a nonquadratic residue modulo } p. \end{cases}$$

The particular relation between the linking number and the Legendre symbol arises when considering the decomposition of knots and prime numbers when viewed in larger spaces. For a knot L, this larger space is a covering space of the knot complement $X_L \coloneqq S^3 \setminus L$. In particular, this covering space, denoted by X_2, is known as the 2-fold cover. Associated with X_2 is a covering map $p_2 \colon X_2 \to X_L$ that decomposes a knot K as follows.

Theorem 1. *If* $\mathrm{lk}_2(L,K) = 1$*, then there exists a knot* $\mathfrak{K} \subset X_2$ *such that* $p_2^{-1}(K) = \mathfrak{K}$*. If* $\mathrm{lk}_2(L,K) = 0$*, then there exist two knots* $K_1, K_2 \subset X_2$ *such that* $p_2^{-1}(K) = K_1 \cup K_2$*. In other words,*

$$p_2^{-1}(K) = \begin{cases} K_1 \cup K_2 & \textit{if } \mathrm{lk}_2(L,K) = 0, \\ \mathfrak{K} & \textit{if } \mathrm{lk}_2(L,K) = 1. \end{cases}$$

On the other hand, for an odd prime q with $q^* \coloneqq (-1)^{(q-1)/2} q$, the larger space is the quadratic field extension $\mathbb{Q}\left(\sqrt{q^*}\right)$ with ring of integers $\mathcal{O}_{\mathbb{Q}\left(\sqrt{q^*}\right)}$. A prime ideal (p) of $\mathbb{Z}$ may not remain prime in $\mathcal{O}_{\mathbb{Q}\left(\sqrt{q^*}\right)}$. We describe this decomposition exactly.

Theorem 2. *Let $p \neq q$ be odd primes. If q^* is a nonquadratic residue modulo p, then $\mathfrak{p} = (p)$ is a prime ideal of $\mathcal{O}_{\mathbb{Q}[\sqrt{q^*}]}$. If q^* is a quadratic residue modulo p, then there exist prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$ of $\mathcal{O}_{\mathbb{Q}[\sqrt{q^*}]}$ such that $(p) = \mathfrak{p}_1\mathfrak{p}_2$. In other words*

$$(p) = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2 & \text{if } \left(\dfrac{q^*}{p}\right) = 1, \\ \mathfrak{p} & \text{if } \left(\dfrac{q^*}{p}\right) = -1. \end{cases}$$

From Theorem 1, one sees that a knot decomposes into two components precisely when $\mathrm{lk}_2(L, K) = 0$. On the other hand, Theorem 2 asserts that a prime splits when q^* is a quadratic residue modulo p. Although there appears to be no immediate connection between the linking number and the Legendre symbol at first glance, the similarity between the two theorems follows from the analogous constructions of both objects in their respective fields.

The breakdown of the paper is as follows. In Section 2, we give a brief discussion on covering spaces and other topological objects, followed by a proof of Theorem 1. In Section 3, we review number-theoretical preliminaries, including quadratic residues and the ring of integers of a field extension, and then prove Theorem 2.

Acknowledgements. The author thanks Jonathan Zung for introducing this topic and providing references. Moreover, the author thanks Susan Ruff for her invaluable feedback and Ben Osborn for his comments that greatly improved the paper's quality.

2. Linking Numbers and Covering Spaces

In this section, we give a brief overview of covering spaces and linking numbers. For proofs and further details, we refer the reader to Munkres [6] and Hatcher [3].

2.1. Covering Spaces.

Let X and Y be topological spaces.

Definition 1. A continuous map $p\colon Y \to X$ is a *covering* of X if for every $x \in X$, there exists an open neighborhood U_x such that

$$p^{-1}(U_x) = \bigsqcup_{\alpha} U_\alpha$$

is a disjoint union of open sets U_α and $p|_{U_\alpha}\colon U_\alpha \to U_x$ is a homeomorphism for all α.

We call (Y, p) a *cover* of the *base space* X, Y a *covering space*, and each U_α a *sheet*. We now give examples of coverings of S^1.

Example 2. The $\mathrm{id}_X\colon X \to X$ is the *trivial cover* of X.

Example 3. Fix $n \in \mathbb{N}$. The map $\mathbb{C} \to \mathbb{C}$ given by $z \mapsto z^n$ induces $p_n\colon S^1 \to S^1$. One can show p_n is a covering of S^1.

Example 4. The exponential map $p\colon \mathbb{R} \to S^1$ given by $t \mapsto e^{2\pi i t}$ is the *universal cover* of S^1.

The choice of the cover (Y, p) gives rise to a group of automorphisms of Y.

Definition 2. Let (Y, p) be a cover of X. The set of automorphisms $\{h\colon Y \to Y\}$ over X forms the *Deck transformation group of* p under composition, denoted $\mathrm{Aut}(Y/X)$.

We restrict to a particular type of coverings known as Galois coverings.

Definition 3. A covering $p\colon Y \to X$ is *Galois* if for each $x \in X$ and a pair of distinct lifts $y, y' \in p^{-1}(x)$, there exists a $h \in \mathrm{Aut}(Y/X)$ such that $h(y) = y'$. If p is Galois, we denote the Deck transformation group of p by $\mathrm{Gal}(Y/X)$.

The notation $\mathrm{Gal}(Y/X)$ suggests some connection to Galois theory. In fact, the theory of covering spaces allows us to associate a well-defined topological space X_H to each subgroup H of the fundamental group $\pi_1(X)$, similar to the bijection between intermediate field extensions and subgroups of the Galois group given by the main theorem of Galois theory. Specifically, we have the following.

Theorem 3 (Galois correspondence)**.** *The covering $p\colon Y \to X$ induces the injective group homomorphism $p_*\colon \pi_1(Y, y) \to \pi_1(X, x)$, and there is a bijection*

$$\{\textit{coverings } p\colon Y \to X\}/\textit{isomorphism} \to \{\textit{subgroups of } \pi_1(X, x)\}/\textit{conjugation},$$
$$(p\colon Y \to X) \mapsto p_*(\pi_1(Y, y)) \quad \textit{for} \quad y \in p^{-1}(x).$$

Moreover, p is Galois if and only if $p_*(\pi_1(Y, y))$ is a normal subgroup of $\pi_1(X, x)$. In this case, $\mathrm{Gal}(Y/X) \cong \pi_1(X, x)/p_*(\pi_1(Y, y))$.

With the above bijection, the *universal cover* of X is the map $h\colon Y \to X$ (up to isomorphism) that corresponds to the identity subgroup 1 of $\pi_1(X, x)$. As such, the universal cover is a covering of every covering space of X.

Example 5. From Example 4, the exponential map $p\colon \mathbb{R} \to S^1$ is the universal cover since $p_*(\pi_1(\mathbb{R})) = 1$. This cover is also Galois, and $\mathrm{Gal}\left(\mathbb{R}/S^1\right) \cong \pi_1\left(S^1\right)/1 \cong \mathbb{Z}$. The only quotient groups of $\mathbb{Z}$ are the finite cyclic groups $\mathbb{Z}/n\mathbb{Z}$, which corresponds to the coverings p_n given by Example 3 by Theorem 3.

2.2. **Monodromy Permutation Representations.** The theory of covering spaces also allows us to lift homotopies from the base to its covering space. Once again, let X, Y, and Z be topological spaces.

Theorem 4 (Homotopy lifting)**.** *Let (Y, p) be a cover of X, $H\colon Z \times [0, 1] \to X$ be a homotopy between Z and X, and $\widetilde{H}_0\colon Z \times \{0\} \to Y$ be a lift of H_0. Then there exists a unique homotopy $\widetilde{H}\colon Z \times Y$ such that $\widetilde{H} = p \circ H$.*

In particular, if we take Z to be a point, we obtain the path-lifting property.

Corollary 1 (Path lifting)**.** *Let (Y, p) be a cover of X, and let $\gamma\colon [0, 1] \to X$ be a path in X with basepoint $x := \gamma(0)$. For any point $y \in p^{-1}(x)$, there exists a unique path $\widetilde{\gamma}_y\colon [0, 1] \to Y$ such that $\gamma_y = p \circ \widetilde{\gamma}_y$ and $\widetilde{\gamma}_y(0) = y$.*

Using the path-lifting property (Corollary 1), we can define an action of $\pi_1(X, x)$ acting on a fiber $p^{-1}(x)$. This action is known as the monodromy permutation representation.

Definition 4. Let $\gamma\colon [0,1] \to X$ be a loop in X with basepoint $x \coloneqq \gamma(0)$. The *monodromy action of* $\pi_1(X,x)$ *on* $p^{-1}(x)$ is defined by

$$[\gamma] \cdot y \coloneqq \widetilde{\gamma}_y(1).$$

The induced representation $\rho_x\colon \pi_1(X,x) \to \operatorname{Aut}(p^{-1}(x))$ is called the *monodromy permutation representation of* $\pi_1(X,x)$.

2.3. **Infinite and Finite Cyclic Covers.** Let K be a knot and $X_K = S^3 \setminus K$ be its *knot complement*. Its *knot group* is $G_K = \pi_1(X_K)$ whose *Wirtinger presentation* comprises finitely many generators that are mutually conjugate (see Rolfsen [8]). As such, its abelianization $G_K^{\mathrm{ab}} \coloneqq G_K/[G_K,G_K] \cong \mathbb{Z}$ is generated by the class of a meridian α of K. Using the Galois correspondence (Theorem 3), we construct two classes of coverings of X_K. Let $\psi_\infty\colon G_K \to \mathbb{Z}$ be defined by $\alpha \mapsto 1$ and ψ_n be the composition of ψ_∞ with the surjection $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

Definition 5. The *infinite cyclic cover* of X_K is (X_∞, p_∞), where $p_\infty\colon X_\infty \to X_K$ uniquely corresponds to the subgroup $\ker\psi_\infty = [G_K,G_K]$ of G_K guaranteed by Theorem 3. Hence

$$\operatorname{Gal}(X_\infty/X_K) \cong G_K^{\mathrm{ab}} \cong \mathbb{Z}.$$

Definition 6. The *n-fold cyclic cover* of X_K is (X_n, p_n), where $p_n\colon X_n \to X_K$ uniquely corresponds to the subgroup $\ker\psi_n$ of G_K guaranteed by Theorem 3. Hence

$$\operatorname{Gal}(X_n/X_K) = \mathbb{Z}/n\mathbb{Z}.$$

One can construct the infinite and n-fold cyclic covers using Seifert surfaces. We omit the details and refer the reader to Rolfsen [8] and Li and Sia [5].

2.4. **Linking Numbers and Covering Spaces.** We defined linking numbers previously in Section 1. We now show how the linking number relates to the infinite cyclic cover. To this end, let L and K form a two component link. Let (X_∞, p_∞) be the infinite cyclic cover of X_L. Consider K as a loop in X_L with basepoint x, and let $\rho_\infty\colon G_L \to \operatorname{Gal}(X_\infty/X_L)$ be the induced monodromy permutation representation. Since $\operatorname{Gal}(X_\infty/X_L) = \mathbb{Z}$, let τ denote the generator.

Theorem 5. *We have* $\rho_\infty([K]) = \tau^{\operatorname{lk}(L,K)}$.

Proof. Let Σ_L be the Seifert surface of L, and let Y be the space obtained by cutting X_L along Σ_L. Then X_∞ is constructed by gluing copies Y_i ($i \in \mathbb{Z}$) of Y. Let $\widetilde{K}$ be a lift of K to X_∞. When K crosses Σ_L such that $\operatorname{lk}(L,K) = 1$ (resp. $\operatorname{lk}(L,K) = -1$), $\tilde{K}$ crosses from Y_i to Y_{i+1} (resp. Y_{i+1} to Y_i) for some $i \in \mathbb{Z}$. Therefore, if $\widetilde{K}$ starts at $y_0 \in Y_0$, then its endpoint is in Y_ℓ, where $\ell = \operatorname{lk}(L,K)$. Thus, $\rho_\infty([K])(y_0) \in Y_\ell$. Since τ maps Y_i onto Y_{i+1}, we have $\rho_\infty([K]) = \tau^{\operatorname{lk}(L,K)}$. □

Now let (X_2, p_2) be the 2-fold cyclic cover of X_L. Consider K as a loop in X_2 with basepoint x, and let $\rho_2\colon G_L \to \operatorname{Gal}(X_2/X_L)$ be the induced monodromy permutation representation. Define the mod 2 *linking number* $\operatorname{lk}_2(L,K)$ by the image of $\operatorname{lk}(L,K)$ under the surjection $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. We now prove Theorem 1.

Theorem 1. *If* $\mathrm{lk}_2(L,K)=1$*, then there exists a knot* $\mathfrak{K}\subset X_2$ *such that* $p_2^{-1}(K)=\mathfrak{K}$*. If* $\mathrm{lk}_2(L,K)=0$*, then there exist two knots* $K_1,K_2\subset X_2$ *such that* $p_2^{-1}(K)=K_1\cup K_2$*. In other words,*

$$p_2^{-1}(K)=\begin{cases}K_1\cup K_2 & \text{if } \mathrm{lk}_2(L,K)=0,\\ \mathfrak{K} & \text{if } \mathrm{lk}_2(L,K)=1.\end{cases}$$

Proof. Suppose that $p_2^{-1}(x)=\{y_1,y_2\}$ in X_2, and let $\widetilde{K}$ be a lift of K to X_2. Then $\rho_2([K])(y_i)=y_i\cdot[K]$, the endpoint of $\widetilde{K}$ with starting point y_i. We consider y_1.

Case 1 Suppose that $\rho_2([K])(y_1)=y_1$ (i.e., the endpoint of $\widetilde{K}$ with starting point y_1 is y_1). Denote this lift by K_1. Then K_1 is a knot in X_2. Similarly, suppose $\rho_2([K])(y_2)=y_2$ (i.e., the endpoint of $\widetilde{K}$ with starting point y_2 is y_2). Denote this lift by K_2. Then K_2 is a knot in X_2 as well, and hence K decomposes into a 2-component link $K_1\cup K_2$.
Conversely, suppose K decomposes into two separate knots $K_1\ni y_1$ and $K_2\ni y_2$. Then K_1 has the same starting point and endpoint (as does K_2), so $\rho_2([K])=\mathrm{id}_{X_2}$.

Case 2 Suppose that $\rho_2([K])(y_1)=y_2$ (i.e., the endpoint of $\widetilde{K}$ with starting point y_1 is y_2). Then $\rho_2([K])(y_2)=y_1$, so $\widetilde{K}$ forms a knot $\mathfrak{K}$ in X_2.
Suppose $p_2^{-1}(K)=\mathfrak{K}$ is a knot in X_2. We must have $\rho_2([K])(y_1)=y_2$ (and similarly $\rho_2([K])(y_2)=y_1$) since otherwise $p_2^{-1}(K)=K_1\cup K_2$. Thus $\rho_2([K])=\tau$.

This immediately implies that

$$\begin{aligned}\rho_2([K])=\mathrm{id}_{X_2} &\iff p_2^{-1}(K)=K_1\cup K_2 \text{ is a two-component link in } X_2,\\ \rho_2([K])=\tau &\iff p_2^{-1}(K)=\mathfrak{K} \text{ is a knot in } X_2.\end{aligned}$$

But $\rho_2\colon G_L\to\mathrm{Gal}(X_2/X_L)\cong\mathbb{Z}/2\mathbb{Z}$ takes $[K]\mapsto\mathrm{lk}_2(L,K)$. This gives the result. □

3. Quadratic Reciprocity and Primes

3.1. **Quadratic Reciprocity.** Quadratic reciprocity is one of the most remarkable theorems in number theory. It is one of the fundamental results in the theory of quadratic residues, i.e., determining solutions to quadratic congruences. In the sequel, let p be an odd prime unless otherwise stated.

Definition 7. Let $a\in\mathbb{Z}$. We say that a is a *quadratic residue* modulo p if there exists some $x\in\mathbb{F}_p$ such that $x^2\equiv a\pmod p$. If a is not a quadratic residue modulo p, we say a is a *quadratic nonresidue* modulo p.

This motivates the definition of the Legendre symbol.

Definition 8. Let p be an odd prime and let $a\in\mathbb{F}_p^\times$. Then the *Legendre symbol* is a map $\mathbb{F}_p^\times\to\{\pm1\}$ given by

$$\left(\frac{a}{p}\right)\coloneqq\begin{cases}1 & \text{if } a \text{ is a quadratic residue modulo } p,\\ -1 & \text{if } a \text{ is a nonquadratic residue modulo } p.\end{cases}$$

Remark 1. We can extend Legendre symbols to $\mathbb{Z}$. If $a = 0$, then put

$$\left(\frac{0}{p}\right) = 0.$$

Otherwise, for any $a \in \mathbb{Z}$, take the image $a' \in \mathbb{F}_p$ and by abuse of notation put

$$\left(\frac{a}{p}\right) \coloneqq \left(\frac{a'}{p}\right).$$

Example 6. Note $\left(\mathbb{F}_{11}^{\times}\right)^2 = \{1, 3, 4, 5, 9\}$. Hence, 3 is a quadratic residue modulo 11, while 7 is a nonquadratic residue modulo 11. Thus we write

$$\left(\frac{3}{11}\right) = 1 \quad \text{and} \quad \left(\frac{7}{11}\right) = -1.$$

We now justify this definition of the Legendre symbol. Consider the inclusion map $\left(\mathbb{F}_p^{\times}\right)^2 \hookrightarrow \mathbb{F}_p$. The subgroup $\left(\mathbb{F}_p^{\times}\right)^2$ of quadratic residues modulo p has index 2 because $\mathbb{F}_p^{\times}$ is a cyclic group of order $p - 1$. This gives the exact sequence

$$1 \to \left(\mathbb{F}_p^{\times}\right)^2 \to \mathbb{F}_p^{\times} \to \{\pm 1\} \to 1,$$

so the Legendre symbol is the quotient map $\mathbb{F}_p^{\times} \to \{\pm 1\}$ (see Serre [9] for further details). Specifically, the map is a group homomorphism, which implies the following.

Proposition 1. *The Legendre symbol is* multiplicative*: for any $a, b \in \mathbb{F}_p^{\times}$, we have*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

The following proposition gives a computation that determines the Legendre symbol without enumerating $\left(\mathbb{F}_p^{\times}\right)^2$. When we write $a = b$ in $\mathbb{F}_p$, we mean $a \equiv b \pmod{p}$.

Proposition 2 (Euler's criterion)**.** *For any $a \in \mathbb{F}_p^{\times}$, we have in $\mathbb{F}_p$*

$$\left(\frac{a}{p}\right) = a^{(p-1)/2}.$$

Example 7. Using Proposition 2, we confirm Example 6: we get (in $\mathbb{F}_p$)

$$\left(\frac{3}{11}\right) = 3^5 = 1.$$

One can use Euler's criterion (Proposition 2), multiplicativity (Proposition 1), and the following quadratic reciprocity law to simply computations of Legendre symbols.

Theorem 6 (Quadratic reciprocity)**.** *Let p and q be odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Hundreds of proofs of the quadratic reciprocity law exist, six of them due to Gauss [5]. We refer the reader to Apostol [1] for one of Gauss's proof and Lia and Sia [5] for Rousseau's proof. For more advanced proofs, we refer the reader to Gerstenhaber [2] and Lemmermeyer [4].

Example 8. To determine if 219 is a quadratic residue modulo 383, we compute

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right)\left(\frac{73}{383}\right)$$

by multiplicativity. We use quadratic reciprocity (Theorem 6) and Euler's criterion (Proposition 2) to obtain

$$\begin{aligned}\left(\frac{3}{383}\right) &= \left(\frac{383}{3}\right)(-1)^{(383-1)(3-1)/4} \\ &= \underbrace{-\left(\frac{2}{3}\right) = -2^{(3-1)/2} = -2 = 1}_{\text{in } \mathbb{F}_3}, \\ \left(\frac{73}{383}\right) &= \left(\frac{383}{73}\right)(-1)^{(383-1)(73-1)/4} \\ &= \left(\frac{18}{383}\right) = \left(\frac{3^2}{383}\right)\left(\frac{2}{383}\right) = \underbrace{\left(\frac{2}{383}\right) = 2^{(383-1)/2} = 1}_{\text{in } \mathbb{F}_{383}},\end{aligned}$$

which implies 219 is indeed a quadratic residue modulo 383.

3.2. **Ramified and Unramified Primes.** In the previous section, we restricted our attention to quadratic residues modulo p. One might naturally extend this question to quadratic residues modulo n, where n is any composite integer.

Number theorists primarily study prime numbers because of their fundamental atomicity: all integers $n > 1$ can be uniquely factored into a product of prime numbers (up to order). As such, many properties about integers and integer-valued functions can be deduced from analyzing prime numbers. This notion can be extended to any number field F; in particular, modern number theory research involves studying the primes in the ring of integers $\mathcal{O}_F$ in F. We refer the reader to Neukirch [7] for details.

Definition 9. A *number field* F is a finite field extension of $\mathbb{Q}$. The *ring of integers* $\mathcal{O}_F$ *of* F is the integral closure of $\mathbb{Z}$ in F (i.e., roots of monic polynomials in $\mathbb{Z}[X]$).

Example 9. The degree two field extension $F = \mathbb{Q}(i)$ has ring of integers $\mathcal{O}_F = \mathbb{Z}[i]$, known as the *ring of Gaussian integers*.

Example 10. For any $n \in \mathbb{N}$, let ζ_n be a primitive nth root of unity. Then the field extension $F = \mathbb{Q}(\zeta_n)$ is a *cyclotomic field* with ring of integers $\mathcal{O}_F = \mathbb{Z}[\zeta_n]$.

A number field $F = \mathbb{Q}(\alpha)$ need not have $\mathcal{O}_F = \mathbb{Z}[\alpha]$ as its ring of integers, as the next example shows.

Example 11. Let $d \neq 0$ be a squarefree integer, and consider $F = \mathbb{Q}\left(\sqrt{d}\right)$. Then $\mathcal{O}_F = \mathbb{Z}\left[\sqrt{d}\right]$ if $d \equiv 2, 3 \pmod 4$, and $\mathcal{O}_F = \mathbb{Z}\left[\left(1+\sqrt{d}\right)/2\right]$ if $d \equiv 1 \pmod 4$.

In much the same way that integers $\mathbb{Z}$ have unique prime factorization, ideals over the ring of integers $\mathcal{O}_F$ have a unique factorization into prime ideals.

Theorem 7. *Let $\mathcal{O}_F$ be the ring of integers of some number field F. Any nontrivial ideal $\mathfrak{a}$ of $\mathcal{O}_F$ has a unique decomposition into a product of prime ideals up to order*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}.$$

Example 12. The number field $F = \mathbb{Q}\left(\sqrt{-5}\right)$ has ring of integers $\mathcal{O}_F = \mathbb{Z}\left[\sqrt{-5}\right]$. The ideal (6) of $\mathcal{O}_F$ has the prime decomposition

$$(6) = \left(2, 1+\sqrt{-5}\right)\left(2, 1-\sqrt{-5}\right)\left(3, 1+\sqrt{-5}\right)\left(3, 1-\sqrt{-5}\right).$$

In particular, in the finite field extension $F/\mathbb{Q}$, prime ideals (p) of $\mathbb{Z}$ may decompose into a product of prime ideals of $\mathcal{O}_F$.

Definition 10. Let F be some number field. Let $p \in \mathbb{Z}$ be prime, and suppose the ideal (p) has the prime factorization

$$(p) = \prod_{i=1}^{m} \mathfrak{p}_i^{e_i}$$

of prime ideals $\mathfrak{p}_i$ in $\mathcal{O}_F$. Then p is *unramified* in $\mathcal{O}_F$ if $e_i = 1$ for all $i \in \{1, \ldots, m\}$, in which case e_i is the *ramification index* of $\mathfrak{p}_i$. Otherwise, p is *ramified*.

Example 13. The prime ideals of the ring of Gaussian integers have a concise classification. The only prime in $\mathbb{Z}$ that ramifies in $\mathbb{Z}[i]$ is 2; one writes $(2) = (1+i)^2$. If $p \equiv 1 \pmod 4$, then (p) splits into two primes $\mathfrak{p}_1\mathfrak{p}_2$ in $\mathbb{Z}[i]$. If $p \equiv 3 \pmod 4$, then $(p) = \mathfrak{p}$ remains prime in $\mathbb{Z}[i]$.

The ramification behavior of primes is connected to a numerical invariant of number fields known as the discriminant.

Definition 11. Let K be a number field of degree n and let $\{\alpha_j\}_{j=1}^n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. The *discriminant* d_K of K is the number $d_K = (\det(\sigma_i(a_j))_{ij})^2$, where σ_i run over the embeddings $K \hookrightarrow \mathbb{C}$.

Example 14. Let $d \neq 0$ be a squarefree integer, and consider $F = \mathbb{Q}\left(\sqrt{d}\right)$. There are two embeddings $F \hookrightarrow \mathbb{C}$, given by $\sigma_1 = \mathrm{id}$ and conjugation σ_2. Example 11 gives a $\mathbb{Z}$-basis for $d \equiv 2, 3 \pmod 4$ and $d \equiv 1 \pmod 4$, which implies the discriminants

$$d_K = \begin{cases} d & \text{if } d \equiv 1 \pmod 4, \\ 4d & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

With the discriminant, we can completely determine which primes ramify in $\mathcal{O}_K$. We refer the reader to Neukirch [7].

Proposition 3. *A prime p is ramified in $\mathcal{O}_K$ if and only if $p \mid d_K$.*

Note that Proposition 3 immediately implies that there are only a finite number of primes that ramify in K, since d_K is finite and thus has finitely many divisors.

Proposition 4. *The maximal abelian extension of $\mathbb{Q}$ unramified outside p is*

$$\mathbb{Q}(\zeta_{p^\infty}) \coloneqq \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{p^n}).$$

3.3. **Algebraic Structures.** We define more algebraic structures necessary to prove Theorem 2. We start with the prime spectrum of a commutative ring R.

Definition 12. Let R be a commutative ring. The *prime spectrum* of R, denote by $\operatorname{Spec} R$, is the set of prime ideals of R.

Example 15. We have $\operatorname{Spec} \mathbb{Z} = \{(0), (2), (3), (5), \ldots\}$ and $\operatorname{Spec} \mathbb{Q} = \{(0)\}$.

Let $\mathfrak{p}$ be a prime ideal of B. For any ring homomorphism $\phi\colon A \to B$, the ideal $\phi^{-1}(\mathfrak{p})$ is a prime ideal of A. Thus, any ring homomorphism $A \to B$ induces a map $\operatorname{Spec} B \to \operatorname{Spec} A$.

The p-adic integers form another algebraic object commonly found in number theory. First, we define an inverse system and an inverse limit.

Definition 13. An *inverse system* is a sequence of rings A_n with a sequence of morphisms $\phi_n\colon A_{n+1} \to A_n$. The *inverse limit* $A = \varprojlim A_n$ of the inverse system is the set of all sequences $a = (a_n)$ for which $\phi_n(a_{n+1}) = a_n$ for all $n \geq 1$.

Definition 14. Let p be a prime. Let $A_n = \mathbb{Z}/p^n\mathbb{Z}$ and let $\phi_n\colon \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ be reduction modulo p^n. The *set of p-adic integers* is $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

The units of $\mathbb{Z}_p$ has structure $\mathbb{Z}_p^\times \cong \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p)$.

3.4. **The** mod 2 **Linking Numbers for Primes.** Theorems 1 and 5 have number-theoretic analogues. In the same way that knots K are subsets of S^3, we view prime ideals (p) as points of the simply connected "3-manifold" $\operatorname{Spec} \mathbb{Z}$. Similarly, knot complements $X_K = S^3 \setminus K$ and the knot group $\pi_1(X_K)$ have the analogous constructions $X_{\{p\}} = \operatorname{Spec} \mathbb{Z} \setminus \{p\} = \operatorname{Spec} \mathbb{Z}[1/p]$ and the prime group $G_{\{p\}} = \pi_1\left(X_{\{p\}}\right)$.

In Section 2.3, we constructed the 2-fold cyclic cover (X_2, p_2) of X_K. The analogous number-theoretic construction is as follows.

Let q be an odd prime, and let $q^* \coloneqq (-1)^{(q-1)/2}q$. Consider $K = \mathbb{Q}\left(\sqrt{q^*}\right)$. Note that $q^* \equiv 1 \pmod 4$, so Example 11 implies $\mathcal{O}_K = \mathbb{Z}\left[\left(1 + \sqrt{q^*}\right)/2\right]$ and Example 14 implies $d_K = q^*$. By Proposition 3, only q is ramified. Define

$$\begin{aligned} X_{\{q\}} &= \operatorname{Spec} \mathbb{Z}[1/q], \\ G_{\{q\}} &= \pi_1(X_{\{q\}}), \\ X_2 &= \operatorname{Spec} \mathbb{Z}[1/q, \left(1 + \sqrt{q}\right)/2]. \end{aligned}$$

The embedding $\mathbb{Z}[1/q] \to \mathbb{Z}\left[1/q, \left(1+\sqrt{q}\right)/2\right]$ induces $h_2 \colon X_2 \to X_{\{q\}}$, known as the *double étale covering*. It follows from class field theory that

$$G_{\{q\}}^{\mathrm{ab}} \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{q^\infty})/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/q^n\mathbb{Z})^\times = \mathbb{Z}_q^\times,$$

where $\mathbb{Q}(\zeta_{q^\infty})$ is the maximal abelian extension of $\mathbb{Q}$ unramified outside of q by Proposition 4. Then the structure $\mathbb{Z}_q^\times \cong \mathbb{F}_q^\times \times (1+q\mathbb{Z}_q)$ gives rise to the natural quotient map

$$\rho_2 \colon G_{\{q\}} \to G_{\{q\}}^{\mathrm{ab}} \to \mathbb{F}_q^\times \to \mathbb{Z}/2\mathbb{Z}.$$

We now define the mod 2 linking number for primes.

Definition 15. For two primes p and q, define the mod 2 *linking number of p and q* to be $\mathrm{lk}_2(p,q) \coloneqq \rho_2(\sigma_p)$, where $\sigma_p \in \mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{q}\right)/\mathbb{Q}\right)$ is the Frobenius automorphism associated to p.

The Legendre symbol and the mod 2 linking number for primes are related by the following theorem.

Theorem 8. *Let p and q be distinct odd primes. Then*

$$\left(\frac{q^*}{p}\right) = (-1)^{\mathrm{lk}_2(q,p)}.$$

Proof. Note that $\mathrm{lk}_2(q,p) = 0$ if and only if $\rho_2(\sigma_p) = \mathrm{id}_{X_2}$. This happens if and only if $\sigma_p\left(\sqrt{q^*}\right) = \sqrt{q^*}$. But this is equivalent to $\sqrt{q^*} \in \mathbb{F}_p^\times$ (i.e., q^* is a quadratic residue modulo p), as required. □

We now prove Theorem 2.

Theorem 2. *Let $p \neq q$ be odd primes. If q^* is a nonquadratic residue modulo p, then $\mathfrak{p} = (p)$ is a prime ideal of $\mathcal{O}_{\mathbb{Q}\left[\sqrt{q^*}\right]}$. If q^* is a quadratic residue modulo p, then there exist prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$ of $\mathcal{O}_{\mathbb{Q}\left[\sqrt{q^*}\right]}$ such that $(p) = \mathfrak{p}_1\mathfrak{p}_2$. In other words*

$$(p) = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2 & \text{if } \left(\dfrac{q^*}{p}\right) = 1, \\ \mathfrak{p} & \text{if } \left(\dfrac{q^*}{p}\right) = -1. \end{cases}$$

Proof. For brevity, let $K = \mathbb{Q}\left[\sqrt{q^*}\right]$. We have the ring isomorphism

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_p[X]/\left(X^2 - q^*\right).$$

Because p is not ramified in $\mathcal{O}_K$, either p remains prime or splits. We use the fact that $\mathcal{O}_K/p\mathcal{O}_K$ is a domain if and only if $p\mathcal{O}_K$ is prime.

If q^* is a quadratic residue modulo p, then there exists some $x \in \mathbb{F}_p$ such that $x^2 \equiv q^* \pmod{p}$. This means that $\mathbb{F}_p[X]/\left(X^2 - q^*\right)$ (and hence $\mathcal{O}_K/p\mathcal{O}_K$) is not a domain, which means that $p\mathcal{O}_K$ is not prime.

On the other hand, if q^* is a nonquadratic residue modulo p, then $x^2 \not\equiv q^* \pmod{p}$ for all $x \in \mathbb{F}_p$. This means that $\mathbb{F}_p[X]/\left(X^2 - q^*\right)$ (and hence $\mathcal{O}_K/p\mathcal{O}_K$) is a domain. This implies that $p\mathcal{O}_K$ is prime. □

Note that Theorem 8 allows us to write Theorem 2 in a different form. Specifically,

$$(p) = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2 & \text{if } \left(\frac{q^*}{p}\right) = 1, \\ \mathfrak{p} & \text{if } \left(\frac{q^*}{p}\right) = -1, \end{cases}$$
$$= \begin{cases} \mathfrak{p}_1\mathfrak{p}_2 & \text{if } \mathrm{lk}_2(q,p) = 0, \\ \mathfrak{p} & \text{if } \mathrm{lk}_2(q,p) = 1. \end{cases}$$

One can directly compare this to the statement of Theorem 1 that

$$p_2^{-1}(K) = \begin{cases} K_1 \cup K_2 & \text{if } \mathrm{lk}_2(L,K) = 0, \\ \mathfrak{K} & \text{if } \mathrm{lk}_2(L,K) = 1. \end{cases}$$

References

[1] Tom Apostol, *Introduction to Analytical Number Theory*, Springer-Verlag New York, 1976.
[2] Murray Gerstenhaber, *The 152nd Proof of the Law of Quadratic Reciprocity*, Amer. Math. Monthly **70** (1963), no. 4, 397–398.
[3] Allen Hatcher, *Algebraic Topology*, Cambridge University Press, 2002.
[4] Franz Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*, Springer-Verlag Berlin Heidelberg, 2000.
[5] Chao Li and Charmaine Sia, *Knots and Primes: Summer 2012 Tutorial*, 2012. `https://www.julianlyczak.nl/seminar/knots2016-files/knots_and_primes.pdf`.
[6] James Munkres, *Topology*, Pearson Education Unlimited, 2014.
[7] Jürgen Neukirch, *Algebraic Number Theory*, Springer-Verlag Berlin Heidelberg, 1999.
[8] Dale Rolfsen, *Knots and Links*, Publish or Perish, 1976.
[9] Jean-Pierre Serre, *A Course in Arithmetic*, Springer-Verlag New York, 1973.

Massachusetts Institute of Technology, 77 Massachusetts Ave, Cambridge, MA 02139-4301

Email address: `allenees@mit.edu`