Math 214 Fall 2022 Number Theory I

Quadratic Reciprocity

Sankar Sitaraman – nature-lover.net/math

Math Dept, Howard University

11-13-2022

Outline

Basic idea

Henceforth, $\mathbb{F}_p^*$ will denote $(\mathbb{Z}/p\mathbb{Z})^*$.

Basic questions:

How to find square roots modulo a prime?

In general, in the world of $\mathbb{F}_p^*$ how do you find roots of numbers?

More generally, how do you find roots modulo any number?

You can think of solving linear congruences as trying to divide numbers in $\mathbb{F}_p^*$.

For example, $ax \equiv b \pmod{p}$ means x is b/a in the world of $\mathbb{F}_p^*$.

Similarly, $x^2 \equiv a \pmod{p}$ means x is $\sqrt{a}$ in the world of $\mathbb{F}_p^*$.

Solving a quadratic equation depends on $\sqrt{D}$ where D is the discriminant.

Definition of quadratic residues and non-residues

We say a is a **quadratic residue** mod p is $x^2 \equiv a \pmod{p}$ has a solution.

In other words, quadratic residues are the numbers who have a square root in the world of $\mathbb{F}_p^*$.

We say a is a **quadratic non-residue** mod p is $x^2 \equiv a \pmod{p}$ has no solution.

In other words, quadratic non-residues are the numbers who don't have a square root in the world of $\mathbb{F}_p^*$.

The behavior of quadratic residues

The least quadratic non-residue

While we have many beautiful theorems that help us to compute the quadratic residue modulo a given prime, the distribution of the residues over different primes seems to be almost random.

We do have some estimates of things like where the smallest non-residue can be found, for all primes. Note that the smallest residues will be 1, 4, 9, etc., It still makes sense to ask for the least prime or the least non-square that is a residue.

Estimates for least quadratic non-residues

Estimates

1. (Burgess) The least quadratic non-residue is of the order $p^{\frac{1}{4\sqrt{e}}+\epsilon}$.
2. (Lamzouri et al) Assuming the generalized Riemann Hypothesis, for large primes p the least quadratic non-residue mod p is less than $2(\log p)^2$; The least prime quadratic residue is less than $4(\log p)^2$.

The Legendre symbol

Definition of the Legendre Symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if a is a residue mod } p \\ -1 & \text{a is a non-residue mod } p \end{cases}$$

Multipicativity of Legendre Symbol

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

This is useful in breaking down the problem of finding square-roots of big numbers into that of finding square-roots of smaller ones.

Proof: Now, the product of two squares is also a square.
On the other hand, if you multiply a square by a non-square, then the result cannot be a square, because other wise you can divide by the square to get a contradiction (see textbook for details).
In next page we will show that product of two non-squares is a square.

Multipicativity of Legendre Symbol – contd.

Proof that product of two non-squares is a square

First, we need to show that
Number of Squares = Number of Non-Squares

Main idea: $x^2 = (-x)^2$ or $x^2 \equiv (p-x)^2 \pmod{p}$. So the squares of $1, 2, 3, ..., (p-1)/2$ will equal the squares of their negatives. But the squares of any two numbers in $1, 2, 3, ..., (p-1)/2$ are different (see textbook for proof).

So there are $(p-1)/2$ squares and as many non-squares.

Multipicativity of Legendre Symbol – conclusion.

Proof that product of two non-squares is a square

Finally, the subgroup of squares in $S \leq \mathbb{F}_p^*$ (check that it is a subgroup!) is of index 2 because the order is $(p-1)/2$. So there are only two cosets, S itself and Sx where x is any non-square. Also the square of any coset gives you the subgroup! $(Sx)^2 = Sx^2 = S$ because $x^2 \in S$ for all $x \in \mathbb{F}_p^*$.

Now let x and y be non-squares. So $Sx \neq S, Sy \neq S$. But the index is 2 so $Sx = Sy$ because there is only one coset other than S itself. So $SxSy = (Sx)^2 = (Sy)^2 = S$. This means $xy \in S$.

Multipicativity of Legendre Symbol – remarks

Remarks on proof that product of two non-squares is a square

Alternate proof: If x and y be non-squares. So $Sx \neq S, Sy \neq S$. But the index is 2 so $Sxy = Sx$ *or* S because there is only one coset other than S itself. But $SxSy = Sx \implies Sy = S$, a contradiction. So $Sxy = S$. This means $xy \in S$. Here we used the fact that x, y are relatively prime to p.

NOTE: If $p|a$, then we will define that $\left(\frac{a}{p}\right) = 0$.

Multipicativity of Legendre Symbol – remarks – contd

Remarks on proof that product of two non-squares is a square

The proof in textbook doesn't use group theory but it is pretty much identical, because it looks at behavior of the set Sa for a given a.

Basically, if a is a non-residue, then Sa consists of only non-residues, and they are all different. Since there are $(p-1)/2$ of them, they exhaust all the non-residues. So if b is another non-residue, then ba has to be a residue because $ba \notin Sa$ and Sa already contains all non-residues

Legendre Symbol as a character

The multiplicativity of the Legendre symbol $\left(\frac{a}{p}\right)$ makes it possible to define a homomorphism

$$\phi : \mathbb{F}_p^* \to \{1, -1\} \; ; \; \phi(a) = \left(\frac{a}{p}\right).$$

Check that this is a homomorphism! Clearly, the kernel is S, the subgroup of quadratic residues.

Any map from a group to $\mathbb{C}^*$ is called a character. Characters play an important role in group theory and number theory. NOTE: Since $\mathbb{F}_p^*/S$ is a group of order 2, you get a homomorphism to $\{1, -1\}$ for free. This is another proof that ϕ is an isomorphism.

Formula for the Legendre symbol : Euler's criterion

Formula of the Legendre Symbol (EULER'S CRITERION)
As before we assume a is not divisible by p. If it is, then we say the value of the legendre symbol is 0.

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

Proof: If we assume that $\mathbb{F}_p^*$ is cyclic, and write $a = g^k$, then a is a square or non-square depending on whether k is odd or even.

$$\textit{Now } g^{p-1} \equiv 1 \pmod{p} \implies (g^{(p-1)/2})^2 \equiv 1 \pmod{p}$$

$$\implies g^{(p-1)/2} \equiv 1 \textit{ or } -1 \pmod{p}.$$

But it can't be 1 because then g won't generate all of $\mathbb{F}_p^*$.
contd:

Contd: Proof of Formula for Legendre symbol

We showed:

$$g^{(p-1)/2} \equiv -1 \pmod{p}.$$

If k is odd, say $2m+1$, then

$$a^{(p-1)/2} = (g^{2m+1})^{(p-1)/2} = g^{m(p-1)} g^{(p-1)/2} \equiv -1 \pmod{p}$$

if it is even, say $k = 2m$ then

$$a^{(p-1)/2} = (g^{2m})^{(p-1)/2} = g^{m(p-1)} \equiv 1 \pmod{p}$$

We have proved: $\left(\frac{a}{p}\right) = a^{(p-1)/2}$

Proof of Euler's criterion – without cyclicity –Proof 1

Let a be a non-residue. The product of $a_i a$ where a_i runs over residues gives a product over all non-residues (How?). Now $a_i \equiv x^2 \implies a_i^{-1} = (x^{-1})^2$ and so when a_i runs over residues so does a_i^{-1}. We get

$$\prod_{a_i \in S} (a_i a) = \prod_{b_i \in NR} b_i \implies a^{(p-1)/2} \equiv \prod_i b_i \prod_i a_i^{-1} \equiv (p-1)! \pmod{p}.$$

By Wilson's theorem $a^{(p-1)/2} \equiv -1 \pmod{p}$. On the other hand, when a is a residue, $a \equiv x^2 \implies a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$.

So we have proved: $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Proof of Euler's criterion – without cyclicity – Proof 2

The text book proves in an elementary way without assuming cyclicity of $\mathbb{F}_p^*$.
The steps are as follows:

1. If $a \equiv x^2 \pmod{p}$ then $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$.
2. To prove $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p} \implies a \equiv x^2 \pmod{p}$ use the polynomial $x^{(p-1)/2} - 1$. This has at most $(p-1)/2$ roots by the fundamental theorem analog for finite fields. But every quadratic residue is a root already and there are $(p-1)/2$ of them. So only the squares are roots of $x^{(p-1)/2} - 1$ and if $a^{(p-1)/2} \equiv 1 \pmod{p}$ then a is a square.

Additional remark: $x^{p-1} - 1 = (x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1)$ means $\left(\frac{a}{p}\right) = -1 \implies x^{(p-1)/2} + 1 \equiv 0 \pmod{p}$.

Proof of Euler's criterion – using group theory

We can try to prove Euler's criterion using only group theory.

As before, $\mathbb{F}_p^*/S$ is a group of order 2 and it is isomorphic to $\{1, -1\}$. The isomorphism ϕ can be explicitly given by

$$\phi : \mathbb{F}_p^* \to \{1, -1\} \; ; \phi(a) = a^{(p-1)/2}.$$

Check that this is a homomorphism. As before, $a^{p-1} \equiv 1$ means $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. Therefore the image has to be $\{1, -1\}$.

contd. next slide

Proof of Euler's criterion – using group theory – contd

On the other hand, the kernel contains S because as shown before, when a is a residue, $a \equiv x^2$ and $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$. So $\phi(S) = \{1\}$ but then in order to prove that the kernel is just S and *not all of* $\mathbb{F}_p^*$ we need at least one element a such that $a^{(p-1)/2} \equiv -1$.

But we don't have that unless we prove that using the fact that $\mathbb{F}_p^*$ is cyclic or some other way. If that is the case then kernel has to be just S and $\mathbb{F}_p^*/S$ is isomorphic to $\{1, -1\}$ and $\phi(Sa) = -1$ where a is any non-residue, and therefore ϕ maps all non-residues to -1.

Legendre symbol for -1

We have proved: $\left(\frac{a}{p}\right) = a^{(p-1)/2}$

Letting $a = -1$, we get

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

So -1 has a square root mod an odd prime p if the prime is 1 mod 4 and non-square otherwise.

Legendre symbol for -1 – constructive proof

We can actually find the square root of -1 when $p \equiv 1 \pmod 4$, using Wilson's theorem.

$$-1 \equiv (p-1)! = \left(\frac{p-1}{2}\right)! \times \left(\frac{p+1}{2}\right)\left(\frac{p+3}{2}\right)\ldots(p-2)(p-1)$$

$$\implies -1 \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 (-1)^{(p-1)/2} \pmod p.$$

When $p \equiv 1 \pmod 4$ we have $(p-1)/2$ even and this gives us that -1 has the square root $u = ((p-1)/2)!$ mod an odd prime p if the prime is 1 mod 4.

Application 1: Sums of squares and primes of form 1 mod 4

Suppose p divides $x^2 + y^2$ where x, y are integers.
Easy to see that x, y have to be prime to p and we get

$$x^2 + y^2 \equiv 0 \pmod{p} \implies (xy^{-1})^2 \equiv -1 \pmod{p}$$

But -1 is a square mod p implies $p \equiv 1 \pmod{4}$.

Later we will see that when $p \equiv 1 \pmod{4}$, we actually have $p = x^2 + y^2$ for some x, y.

Application 2: Infinite number of primes of form 1 mod 4

Idea of proof: Assume $p_1, p_2, p_3, ..., p_n$ are all the primes of form 1 mod 4.
Let $P = p_1 p_2 p_3 ... p_n$, their product. Then $4P^2 + 1$ is not divisible by any of them, but because it is bigger than all of them, it is either a prime or divisible by some prime q. But if a prime q divides it, then

$$q|(4P^2 + 1) \implies 4P^2 \equiv -1 \pmod{q}$$

$$\implies \left(\frac{-1}{q}\right) = -1 \implies q \equiv 1 \pmod{4}.$$

Thus either $4P^2 + 1$ is a prime or we have a prime q of form 1 mod 4 different from all the p_i that divides it, which contradicts the assumption that $p_1, p_2, ..., p_n$ are all the primes.

Legendre symbol for 2

We have proved: $\left(\frac{a}{p}\right) = a^{(p-1)/2}$

Letting $a = 2$, we have (proof to follow)

$$\left(\frac{2}{p}\right) = 2^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$$

So 2 has a square root mod an odd prime p if the prime is 1 or 7 mod 8 and non-square otherwise.

Proof: Formula for Legendre symbol for 2

[Based on classical proof. This proof demonstrates a general theme in number theory : To get information on integers, look in extensions of the integers in number fields, such as $\mathbb{Z}[i]$, the Gaussian integers which is the set of complex numbers with integer real and imaginary parts].

$$\left(\frac{2}{p}\right) = 2^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$$

Proof:

$$(1+i)^2 = 2i \implies (1+i)^{p-1} = 2^{(p-1)/2} i^{(p-1)/2}$$

$$\implies (1+i)^p = 2^{(p-1)/2} i^{(p-1)/2} (1+i)$$

Proof contd: Formula for Legendre symbol for 2

We had $1 + p(a + bi) + i^p = 2^{(p-1)/2} i^{(p-1)/2}(1 + i)$, with a, b integers. Using binomial formula, we get, after simplification,$1 + p(a + bi) + i^p = 2^{(p-1)/2} i^{(p-1)/2}(1 + i)$. Now we compare the imaginary parts. There are two cases.

Case 1: $p \equiv 1$ *or* $5 \pmod 8$
We have $(p-1)/2$ is even, $i^{(p-1)/2} = \pm 1$ is real, $i^p = i$.

When $p \equiv 1 \pmod 8$ we get the imaginary parts as
$pbi + i = 2^{(p-1)/2} i \implies 2^{(p-1)/2} \equiv 1 \pmod p$.

When $p \equiv 5 \pmod 8$ we get the imaginary parts as
$pbi + i = -2^{(p-1)/2} i \implies 2^{(p-1)/2} \equiv -1 \pmod p$.

case 2 of Proof of Formula for Legendre symbol for 2

We had $1 + p(a + bi) + i^p = 2^{(p-1)/2} i^{(p-1)/2}(1 + i)$, with a, b integers.

Case 2: $p \equiv 3$ *or* $7 \pmod 8$
Now $(p-1)/2$ is odd, $i^{(p-1)/2} = i^3$ *or* i hence imaginary, $i^p = i^3$.

When $p \equiv 7 \pmod 8$ we get the imaginary parts as
$pbi + i^3 = 2^{(p-1)/2} i^3 \implies 2^{(p-1)/2} \equiv 1 \pmod p$.

When $p \equiv 3 \pmod 8$ we get the imaginary parts as
$pbi + i^3 = 2^{(p-1)/2} i \implies 2^{(p-1)/2} \equiv -1 \pmod p$.

This concludes the calculation of the quadratic residue of 2.

Proof in textbook of Formula for Legendre symbol for 2

Main idea: Look at the set $T = \{2, 4, 6, ..., p-1\}$.

Let $P = (p-1)/2$. Then the product of the elements in T is $M = 2^{(p-1)/2} P!$.
On the other hand, any two of these elements are distinct and the ones bigger than P are negatives of the numbers from 1 to P.

So then M is nothing but $P!$ times $(-1)^k$ where k is the number of elements in T that are bigger than P.

Setting $2^{(p-1)/2} P! = P!(-1)^k$ we get $2^{(p-1)/2} = (-1)^k$ so it all comes down to counting k in the different cases of p modulo 8.
Proof in textbook / hw problem.

Application: A case where 2 is a primitive root

Application of quadratic residue to Artin' primitive roots conjecture:

When p is a prime and $(p-1)/4$ is also a prime, then 2 is a primitive root p.
Proof: We will prove that there is no prime ℓ dividing $p-1$ such that $2^{(p-1)/\ell} \equiv 1 \pmod{p}$. Since $p-1 = 4q$, with q a prime, the only possibilities are $\ell = 2$ or q.
Now from earlier theorem $2^{(p-1)/2} \equiv 1 \implies p \equiv \pm 1 \pmod{8}$.
Both are impossible if $p = 4q+1$.
$2^{(p-1)/q} = 2^4 \equiv 1 \pmod{p} \implies p = 3, 5$. In both cases $(p-1)/4$ is not a prime.

Problem: Not known if there are infinitely many primes of form $4q+1$ where q is prime.

Statement and purpose of Quadratic reciprocity law

Let p, q be primes. Quadratic reciprocity is basically about reducing the calculation of residue of q mod p to that of p mod q.
Once we do that we can easily calculate the residue of any integer mod any other, by factoring into primes and also reducing mod primes.
The law of quadratic reciprocity says

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

This means

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \text{ or } p \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv 3 \text{ AND } q \equiv 3 \pmod 4 \end{cases}$$

Formula for residue of any integer

We will give a sketch of the proof. Please refer to text for details.

.

Let $\mu(a, p)$ be the number of elements in the set $\{a, 2a, 3a, ..., Pa\}$ that are negatives of elements in $\{1, 2, ..., P\}$. Here $P = (p-1)/2$ as before.

$$\text{First show:} \quad \left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}$$

Proof similar to proof for the residue formula of 2.
First look at the residues of ka mod p and show that they are neither equal nor negatives of each other.
Then show that $a^{(p-1)/2} \equiv (-1)^{\mu(a,p)}$ by looking at the product of the ka mod p.

Formula for sum of sign changes

Let $\left\lfloor \frac{a}{b} \right\rfloor$ be largest integer smaller than a/b. Assume a is odd and relatively prime to p.

$$\text{Now show:} \quad \sum_{1}^{P} \left\lfloor \frac{ka}{p} \right\rfloor \equiv \mu(a,p) \pmod 2.$$

Notice that it is mod 2, because we are only concerned with powers of -1.

Idea of proof: divide $ka = pq_k + r_k$ by p. You get that $\left\lfloor \frac{ka}{p} \right\rfloor$ either is q_k or $q_k - 1$. Now sum over k. You get that $\sum \left\lfloor \frac{ka}{p} \right\rfloor \equiv \sum q_k - \mu(a,p) \bmod 2$. Show that $\sum q_k \equiv 0 \bmod 2$ and note that $\mu(a,p) \equiv -\mu(a,p) \bmod 2$. .

Conclusion of proof

Now we need to show that

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Use the formula $\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}$ with q, p instead of a, p and then p, q instead of a, p. Then all we need to show is that $\mu(p,q) + \mu(q,p) \equiv (p-1)/2 \times (q-1)/2 \bmod 2$. This follows from observing that $\sum \left\lfloor \frac{kq}{p} \right\rfloor$ equals the number of integer points inside the triangle with vertices $(0,0), (p/2,0), (p/2,q/2)$ and the sum $\sum \left\lfloor \frac{kp}{q} \right\rfloor$ equals the number of integer points inside the triangle with vertices $(0,0), (0,q/2), (p/2,q/2)$

Proof using Frobenius map in algebraic extensions - page 1

The Frobenius map $\phi : K \to K$ given by $\phi(x) = x^p$ is an automorphism for finite fields K of characteristic a prime p, namely extensions of $\mathbb{F}_p$.

Proof: Easy to see that it is a field homomorphism. Now every element in the finite field satisfies $x^{p^n} = x$, where n is the degree of K over F. But $\phi(x) = 1 \implies \phi^n(x) = x^{p^n} = 1$ by repeated application (composition of ϕ with itself). This means $x = 1$. So the kernel is trivial.

Incidentally, the proof above also shows that **the order of the Frobenius map equals the degree of the extension and also generates the Galois group.** (How?)

Proof using Frobenius map in algebraic extensions - page 2

Quadratic Residue of -1 mod p using Frobenius.

The idea : Look at $(-1)^{(p-1)/2} = i^{p-1} = i^p/i = \phi(i)/i$ in some finite extension of $\mathbb{F}_p$. (Because Frobenius map may not be an automorphism for extensions of other fields)

Quadratic Residue of -1 : $\mathbb{F}_p[i] \simeq \mathbb{F}_p[x]/(x^2+1)$ is a finite field extension of $\mathbb{F}_p$. In it, $\phi(i) = i^p$ and $i^p = i$ if $p \equiv 1 \pmod 4$ and $i^p = -i$ if $p \equiv 3 \pmod 4$.

So ϕ is the identity map if $p \equiv 1 \pmod 4$. Since ϕ generates $Gal[\mathbb{F}_p[i]/\mathbb{F}_p]$, the Galois group is $= \{id\}$ and so $p \equiv 1 \pmod 4 \implies \mathbb{F}_p[i] = \mathbb{F}_p \implies \sqrt{-1} \in \mathbb{F}_p$. Thus -1 is a square mod p if $p \equiv 1 \pmod 4$.

Proof using Frobenius map in algebraic extensions - page 3

Quadratic residue of 2:

Of course, this was a very heavy handed way to find residue of -1. The real power of the Frobenius map is revealed when looking at residues of other primes, starting with 2.

(Some of this based on Wikipedia page on proofs of quadratic reciprocity).

We saw in class that $\frac{1+i}{\sqrt{i}} = \pm\sqrt{2}$. (Use $(1+i)^2 = 2i$). Now i is the primitive 4th root of 1 (generates the other roots) and so $\sqrt{i} = \zeta_8$, the primitive 8th root of 1. So we get

$$\frac{1+i}{\sqrt{i}} = \frac{1}{\sqrt{i}} + \sqrt{i} = \zeta_8^{-1} + \zeta_8 = \tau, \ \textit{The Gauss Sum},$$

a crucial quantity in number theory.

Proof using Frobenius map in algebraic extensions - page 4

$\tau^2 = 2$ and $\tau = \pm\sqrt{2}$.
Now applying the Frobenius map to τ in $\mathbb{F}_p[\tau] \simeq \mathbb{F}_p[x]/(x^2 - 2)$ we get

$$\tau^p = \zeta_8^p + \zeta_8^{-p} = \begin{cases} \tau & \text{if } p \equiv \pm 1 \pmod 8 \\ -\tau & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

Similar to proof for -1 shown earlier, this implies $\tau \in \mathbb{F}_p$ if $p \equiv \pm 1 \pmod 8$ and not otherwise.
So 2 is a square mod p iff $p \equiv \pm 1 \pmod 8$.

Proof using Frobenius map in algebraic extensions - page 5

Also we have

$$\phi(\tau) = \tau^p \equiv \left(\frac{2}{p}\right)\tau \pmod{p}.$$

Explanation: The degree $[\mathbb{F}_p[\tau] : \mathbb{F}_p]$ is either 2 or 1, depending on whether the Frobenius automorphism $\phi = id$ or not, because the Frobenius automorphism ϕ generates the Galois group.
If it is *id*, then $\mathbb{F}_p[\tau] = \mathbb{F}_p$ and $\sqrt{2} \in \mathbb{F}_p$ namely $\pm\tau$.
If $\phi \neq id$, then $\phi(\tau)$ to $-\tau$ because an automorphism sends a root of $x^2 - 2$ (the irreducible polynomial of $\mathbb{F}_p[\tau]$) to the other root, and here the only roots are τ and $-\tau$. But there are two roots in the extension exactly when the roots are not in the base field $\mathbb{F}_p$. So $\phi(\tau) \equiv \left(\frac{2}{p}\right)\tau \pmod{p}$.

Proof using Frobenius map for general p - page 6

You can express this as

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \text{ and } \tau^p = (-1)^{\frac{p^2-1}{8}}\tau.$$

Note that we bypassed the Euler's criterion. If you use that, you don't need to use the Frobenius map. So the Frobenius map really explains where the Euler's criterion comes from.

Proof using Frobenius map for general p - page 1

In the general case, the Gauss sum τ_p is defined as $\sum_1^{p-1} \left(\frac{k}{p}\right) \zeta_p^k$ and similar to the case $p = 2$ we have $\tau_p^2 = \pm p$. In fact we have $\tau_p^2 = (-1)^{(p-1)/2} p$. Let q and p be odd primes. Now raise both sides to $(q-1)/2$.

$$\tau_p^2 = (-1)^{(p-1)/2} p \implies \tau_p^{q-1} = (-1)^{(p-1)(q-1)/2} p^{(q-1)/2}. \quad (1)$$

Proof using Frobenius for general p - page 2

Working in $\mathbb{F}_q[\tau_p]$ and denoting the Frobenius automorphism $x \to x^q$ by ϕ_q we get from (1):

$$\phi_q(\tau_p) \equiv (-1)^{(p-1)(q-1)/2} \left(\frac{p}{q}\right) \tau_p \pmod{q}.$$

On the other hand, it is true that (just algebra):

$$\phi_q(\tau_p) \equiv \left(\frac{q}{p}\right) \tau_p \pmod{q}. \tag{2}$$

Combining (1) and (2) we get the law of quadratic reciprocity:

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

Can prove (2) using only action of ϕ_q.