Motivating the Gauss sum proof of the quadratic reciprocity

Pierre-Yves Gaillard

1 Introduction

As the title indicates we try to motivate the Gauss sum proof of the quadratic reciprocity.

First recall the definition of the **Legendre symbol**. Let p be a prime, a an integer and $n(a,p)$ the number of distinct solutions of the equation $x^2 = a$ in the field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Then the Legendre symbol $\left(\frac{a}{p}\right)$ is equal to $n(a,p) - 1$. Equivalently $\left(\frac{a}{p}\right)$ is characterized by the conditions: $\left(\frac{a}{p}\right) \in \{-1, 0, 1\}$ and $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$. A proof of this equivalence is given in Proposition 6 p. 5. Note that it implies $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for all a, b.

Consider the question:

Question 1. *Given an odd prime q, is there an integer q^* such that*

$$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right) \tag{1}$$

for all odd prime p not equal to q?

An answer will be given by the **quadratic reciprocity law**: see Theorem 3 p. 4 below.

2 The main argument

Let p and q be distinct odd primes.

Convention 2. Let ℓ be a prime number. In this section and the next two ones, unless otherwise indicated, an equality between integers (or between an integer and an element of $\mathbb{F}_\ell$) will be regarded as an equality in $\mathbb{F}_\ell$, where ℓ is clear from the context. We have $\ell = p$ in this section and the next one, and $\ell = q$ in Section 4.

Clearly (1) can be stated as

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

(equality in $\mathbb{F}_p$). To handle this equation it will be convenient to embed $\mathbb{F}_p$ in a larger ring A. Then A will be a nonzero $\mathbb{F}_p$-algebra[1]. One of the main features of an $\mathbb{F}_p$-algebra is a canonical endomorphism, called the *Frobenius endomorphism*, defined by $a \mapsto a^p$.

The first item on our agenda is to express Equality (2) in terms of the Frobenius endomorphism of some $\mathbb{F}_p$-algebra A.

Suppose we have an integer q^* and an $\mathbb{F}_p$-algebra A with an element $a \in A$ such that the equality

$$a^2 = q^* \tag{3}$$

holds in $\mathbb{F}_p$ (see Convention 2). If q^* is prime to p then a is invertible and we can rewrite (2) as

$$a^p = \left(\frac{p}{q}\right) a, \tag{4}$$

an equality which does involve the Frobenius endomorphism of A.

In view of (2), this shows that, to answer our question, it suffices to find an integer q^* prime to p and a nonzero $\mathbb{F}_p$-algebra A with an element $a \in A$ satisfying the quadratic equation (3) and the **linear** equation (4).

Our strategy will be as follows:

Step 1: Find an $\mathbb{F}_p$-algebra A and a nonzero solution $a \in A$ of (4).

Step 2: Find an integer q^* prime to p and a scalar $\lambda \in \mathbb{F}_p$ such that $\lambda^2 a^2 - q^*$ is *not* invertible in A.

Then the quotient of A by the ideal generated by $\lambda^2 a^2 - q^*$ will be a nonzero $\mathbb{F}_p$-algebra in which (3) and (4) hold (for the image of λa in this quotient).

3 Step 1

Let A be an $\mathbb{F}_p$-algebra. We will make some assumptions to make Equation (4) in A as simple as possible.

Our first simplifying assumption is that A is *finite dimensional* over $\mathbb{F}_p$. Let $(b(x))_{x \in X}$ be an $\mathbb{F}_p$-basis of A. We can express an arbitrary element $a \in A$ as $a = \sum_x f(x)\, b(x)$ with $f(x) \in \mathbb{F}_p$, and (4) becomes

$$\sum_x f(x)\, b(x)^p = \sum_y \left(\frac{p}{q}\right) f(y)\, b(y).$$

[1]Recall that an $\mathbb{F}_p$**-algebra** is a ring A equipped with a morphism $\mathbb{F}_p \to A$. (In this text all rings and all algebras are associative, commutative and have an element 1.)

Of course in general $b(x)^p$ will be a linear combination of the $b(y)$, but our second simplifying assumption is that each $b(x)^p$ is just "another" basis vector, which we denote by $b(p*x)$. To make things even simpler we suppose that the map $x \mapsto p*x$, $X \to X$, is *bijective*. The above display becomes

$$\sum_x f(x)\, b(p*x) = \sum_y \left(\frac{p}{q}\right) f(y)\, b(y),$$

that is

$$f(p*x) = \left(\frac{p}{q}\right) f(x)$$

for all x.

This suggests the following attempt: $X = \mathbb{F}_q$, $p*x = px$ (where the second p is viewed as an element of $\mathbb{F}_q$, see Convention 2 p. 1), $f(x) = \left(\frac{x}{q}\right)$. (Recall that we want a *nonzero* solution of (4).)

So far A is only an $\mathbb{F}_p$-vector space with a basis indexed by $\mathbb{F}_q$, and our problem becomes: Can we find an $\mathbb{F}_p$-algebra multiplication on A such that $b(x)^p = b(xp)$ for all x?

It suffices to define the products $b(x)\, b(y)$, and we see immediately that the formula $b(x)\, b(y) = b(x+y)$ does the job.

We prefer the notation b^x to $b(x)$, so that we get

$$b^x b^y = b^{x+y}, \quad (b^x)^p = b^{xp}, \quad b^0 = 1$$

and

$$a = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) b^x.$$

(The $\mathbb{F}_p$-algebra A is called *the $\mathbb{F}_p$-algebra of the additive group $\mathbb{F}_q$*.)

4 Step 2

We must compute a^2. In the lines below the subscripts x, y, z run over $\mathbb{F}_q$; for instance $\sum_{x \neq 0}$ means that x runs over $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$. We have

$$a^2 = \sum_{x,y} \left(\frac{xy}{q}\right) b^{x+y} = \sum_{x \neq 0} \sum_y \left(\frac{xy}{q}\right) b^{x+y}.$$

Setting $z := x^{-1}y \in \mathbb{F}_q^*$ we get $y = xz$ and thus

$$a^2 = \sum_{x \neq 0} \sum_z \left(\frac{z}{q}\right) b^{x+xz} = \sum_z \left(\frac{z}{q}\right) \sum_{x \neq 0} b^{(1+z)x} = \sum_z \left(\frac{z}{q}\right) \left(\sum_x b^{(1+z)x} - 1\right)$$

$$= \sum_z \left(\frac{z}{q}\right) \sum_x b^{(1+z)x} - \sum_z \left(\frac{z}{q}\right) = \sum_z \left(\frac{z}{q}\right) \sum_x b^{(1+z)x}.$$

If we set $s = \sum_{x \in \mathbb{F}_q} b^x$ we can continue the above chain of equalities as follows (see Convention 2 p. 1):

$$\sum_z \left(\frac{z}{q}\right) \sum_x b^{(1+z)x} = \left(\frac{-1}{q}\right) q + s \sum_{z \neq -1} \left(\frac{z}{q}\right)$$

$$= (-1)^{(q-1)/2}\, q + s \left(\sum_z \left(\frac{z}{q}\right) - \left(\frac{-1}{q}\right) \right) = (-1)^{(q-1)/2}\, q - (-1)^{(q-1)/2}\, s,$$

so that at the end we get

$$a^2 = (-1)^{(q-1)/2}\, q - (-1)^{(q-1)/2}\, s,$$

which suggests to set

$$q^* := (-1)^{(q-1)/2}\, q.$$

To make sure that this answers Question 1, it suffices to check that $q^* - a^2$, or equivalently that s, is not invertible in A. But the obvious equality $b^x s = s$ for all x implies $cs \in \mathbb{F}_q\, s$ for all $c \in A$. (The scalar $\lambda \in \mathbb{F}_p$ mentioned in the description of Step 2 given at the end of Section 2 is equal to 1.)

We have proved the **quadratic reciprocity law**:

Theorem 3 (Quadratic Reciprocity)**.** *If p and q are distinct odd primes, then we have*

$$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)$$

with $q^* := (-1)^{(q-1)/2}\, q$, or equivalently

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

5 Additional proofs

To make this short text more self-contained we add a couple of proofs.

For any positive integer n let C_n be the group $\mathbb{Z}/n\mathbb{Z}$, for any group G let $G(n)$ be the cardinality of the set of elements of order n in G, and set $\phi(n) = C_n(n)$. (Usually ϕ is called Euler's totient function.)

Proposition 4. *In the above setting we have for any group G of finite order n:*

(a) $G(k) = 0$ *if k does not divide n,*

(b) $\sum_d G(d) = n$ *where the sum runs either over the divisors of n or over all positive integers,*

(c) $C_n(d) = \phi(d)$ *if d divides n,*

(d) $\sum_d \phi(d) = n$ *where the sum runs over the divisors of n.*

Proof. Part (c) follows from the fact that C_n contains a unique group of order d whenever d divides n. The proof of the other statements is straightforward. □

Theorem 5. *Let G be a finite subgroup of the multiplicative group K^* of a field K. Then G is cyclic.*

Proof. Let n be the order of G and let the above notation be in force. We claim $G(d) = \phi(d)$ for every divisor d of n. This will imply that $G(n) = \phi(n) \geq 1$, and thus that G is cyclic. Let d be a divisor of n. In view of Parts (b) and (d) of Proposition 4 it suffices to prove $G(d) \leq \phi(d)$. We can assume $G(d) \geq 1$. Let $g \in G$ be of order d, let $g^{\mathbb{Z}}$ be the subgroup of G generated by g, and let H be the subgroup of K^* (the multiplicative group of K) consisting of all the solutions of the equation $x^d = 1$. We claim

$$G(d) \leq K^*(d) = H(d) = g^{\mathbb{Z}}(d) = \phi(d).$$

To prove $H(d) = g^{\mathbb{Z}}(d)$ note that we have $g^{\mathbb{Z}} \subset H$, that $g^{\mathbb{Z}}$ has order d, and that H has order at most d (because the polynomial $X^d - 1$ cannot have more than d roots in K). This implies $g^{\mathbb{Z}} = H$. The other statements are clear. □

Proposition 6. *Let p be an odd prime and a a nonzero element of the field $\mathbb{F}_p$. Then a is a square in $\mathbb{F}_p$ if and only if $a^{(p-1)/2} = 1$.*

Proof. Let g be a generator of the multiplicative group $\mathbb{F}_p^*$ of $\mathbb{F}_p$ (see Theorem 5) and set $n = (p-1)/2$. Note that $g^n = -1$ because $(g^n)^2 = 1$ and $g^n \neq 1$. If $a = g^{2k}$ for some integer k, then $a^n = g^{(p-1)k} = 1$. If $a = g^{2k+1}$ for some integer k, then $a^n = g^{(p-1)k+n} = g^n = -1$. □