A Proof of the Quadratic Reciprocity Law

Math Dicker, Open University of the Netherlands

October 19, 2018

Abstract

A proof of the Quadratic reciprocity Law is presented using a Lemma of Gauss, the theory of finite fields and the Frobenius automorfism.

1 Introduction.

Let p, q be distinct odd prime numbers and let e denote the order of q in \mathbb{F}_p^* . The Frobenius automorphism $x \to x^q$ in the field \mathbb{F}_{q^e} is here denoted by φ_q . Because p divides $q^e - 1$, the cyclic group $\mathbb{F}_{q^e}^*$ contains a primitive p-th root of unity to which we refer by θ . If we specify $f(x) = 1 + x + x^2 \dots + x^{p-1}$ then $f(\theta^k) = 0$ for k with $\gcd(k,p)=1$, otherwise $f(\theta^k) = p$. We denote by $\delta(x_1, x_2, x_3, \dots, x_p)$ the determinant of the p-square matrix with the entry in the ith row and jth column equal to $(x_j)^i$.

2 The Quadratic Reciprocity Law.

In particular, $\delta(1, \vartheta, \vartheta^2, ..., \vartheta^{p-1})$ is the following determinant:

$$\delta(1, \vartheta, \vartheta^{2},, \vartheta^{p-1}) = \begin{vmatrix} 1 & \vartheta & \vartheta^{2} & \vartheta^{3} & \cdots & \vartheta^{p-1} \\ 1 & \vartheta^{2} & \vartheta^{4} & \vartheta^{6} & \cdots & \vartheta^{2(p-1)} \\ 1 & \vartheta^{3} & \vartheta^{6} & \vartheta^{9} & \cdots & \vartheta^{3(p-1)} \end{vmatrix}$$

$$\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \vartheta^{i} & \vartheta^{2i} & \vartheta^{3i} & \cdots & \vartheta^{i(p-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \cdots & 1 \end{vmatrix}$$

Let M be the matrix corresponding with this determinant.

Theorem

1]
$$\delta(1,\vartheta,\vartheta^2,....,\vartheta^{p-1})^2=p^*p^{p-1}$$
 with $p^*=(-1)^{\frac{p-1}{2}}p$

$$2]\ \varphi_q(\delta(1,\vartheta,\vartheta^2,....,\vartheta^{p-1}))=(\frac{q}{p})\delta(1,\vartheta,\vartheta^2,....,\vartheta^{p-1})$$

From 1], 2] and using $\varphi_q(x) = x \iff x \in \mathbb{F}_q$ and Euler's criterion, it follows:

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

Proof

ad 1] Consider the matrixproduct:

$$M^{T}M = \begin{vmatrix} p & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & p \\ 0 & 0 & 0 & \cdots & p & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & p & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & p & 0 & 0 & \cdots & 0 \end{vmatrix}$$

because $M^TM = (f(\vartheta^{(i+j-2)}))$ for row i = 1, 2, .., p and column j = 1, 2, .., p.

ad 2] Consider the residue classes of \mathbb{F}_p^* represented by the following half systems: $\mathbf{H}=1,2,3,...,\frac{(p-1)}{2}$ and $\mathbf{H}=-1,-2,-3,...,-\frac{(p-1)}{2}$. We introduce the function ϱ_q which is connected as we shall see in a moment, to the Frobenius automorfism; The function $\varrho_q:\mathbb{F}_p^*\longrightarrow\mathbb{F}_p^*$ is defined by $x\longrightarrow qx$; the result of ϱ_q is a permutation of \mathbb{F}_p^* . If we denote by μ the number of elements in the set S, with $S=\{x|x\in H,\varrho_q(x)\notin H\}$, then $(\frac{q}{p})=(-1)^{\mu}$ (lemma of Gauss)[1].

Important for us is that the permutation ϱ_q working on \mathbb{F}_p^* is the result of μ interchanges, leaving aside a multiple of 2. This can be grasped as follows: define the permutation π on \mathbb{F}_p^* :

 $\pi = [\Pi_{y \in S}(\varrho_q(y), -\varrho_q(y))] \varrho_q$; by (i,j) is denoted the permutation which interchanges i and j. The permutation ϱ_q and π originate from each other by μ interchanges.

The permutation π has the following properties: $\pi(x) = -\pi(-x)$; $\pi(H) = H$ and $\pi(-H) = -H$. Hence the identity permutation originates from π by an even number of paired interchanges on H and -H.

We have:
$$\delta(1, \vartheta, \vartheta^2, ..., \vartheta^{p-1}) = \delta(1, \vartheta, \vartheta^2, ..., \vartheta^{\frac{p-1}{2}}, \vartheta^{-\frac{(p-1)}{2}}, ..., \vartheta^{-2}, \vartheta^{-1}).$$

The application of the Frobenius automorfism and the consideration of the above mentioned properties of ϱ_q , results in:

$$\begin{split} &\varphi_q \ (\delta(1,\vartheta,\vartheta^2,..,\vartheta^{\frac{p-1}{2}},\vartheta^{-\frac{(p-1)}{2}},..,\vartheta^{-2},\vartheta^{-1})) = \\ &\delta(1,\vartheta^q,\vartheta^{2q},..,\vartheta^{\frac{p-1}{2}q},\vartheta^{-\frac{(p-1)}{2}q},..,\vartheta^{-2q},\vartheta^{-1q}) = \\ &(-1)^{\mu} \ \delta(1,\vartheta,\vartheta^2,..,\vartheta^{\frac{p-1}{2}},\vartheta^{-\frac{(p-1)}{2}},..,\vartheta^{-2},\vartheta^{-1}) = \\ &(\frac{q}{p}) \ \delta(1,\vartheta,\vartheta^2,..,\vartheta^{\frac{p-1}{2}},\vartheta^{-\frac{(p-1)}{2}},..,\vartheta^{-2},\vartheta^{-1}) \end{split}$$

3 An example of ϱ_q .

The crucial point of this proof is that the operation of φ_q on the determinant $\delta(1, \vartheta, \vartheta^2,, \vartheta^{p-1})$ results in μ interchanges of the columns, leaving aside a multiple of 2 interchanges. This is caused by the properties of the connected function ϱ_q .

To illustrate, we consider the case where p=13 and q=5. The residue classes of \mathbb{F}^*_{13} are represented by: 1,2,3,4,5,6,-6,-5,-4,-3,-2,-1. H contains the first six classes. The function ϱ_5 results in the following permutation: 5,-3,2,-6,-1,4,-4,1,6,-2,3,-5. μ is 3; hence $(\frac{5}{13})=-1$ [lemma of Gauss]; $S=\{2,4,5\}$. The permutation π is: 5,3,2,6,1,4,-4,-1,-6,-2,-3,-5. The permutation π can be transformed into the identity permutation by the following six paired interchanges (-2,-3) (2,3) (-4,-6) (4,6) (-5,-1) (5,1)

References

[1] C.F.Gauss, Untersuchungen über höhere Arithmetik, pp.458-459, Art.3

Math Dicker, Kerselarenstraat 36 3700 Tongeren, Belgium louis.dicker@telenet.be; math.dicker@ou.nl