Theorema Aureum – 2

Shivam Kumar

In the first part[1] of this article, we had introduced the notion of *quadratic reciprocity* and dwelt briefly on its history, which goes back all the way to the work of Fermat. Then we discussed the Law of Quadratic Reciprocity ('QRL'), which Gauss named *Theorema Aureum*. Following this, we gave a not too well known proof of the QRL, due to G Rousseau. Now we give two more proofs of the QRL, drawing respectively from ideas in *linear algebra* and *field extensions*; they too are not very well known.

Shivam Kumar graduated from Indian Statistical Institute, Bangalore and is joining the London School of Economics for MSc in applicable mathematics. His interest lies in expanding the existing applied paradigm of mathematics from stock market to unchartered subjects such as sociometrics.

Preamble

Throughout, p, q denote distinct odd primes; x, y denote integers; m denotes an arbitrary modulus, not necessarily prime; $\mathbb{Z}/m\mathbb{Z}$ denotes the set $\{0, 1, 2, \ldots, m-1\}$, which forms a ring under addition and multiplication modulo m; $(\mathbb{Z}/p\mathbb{Z})^*$ denotes the set of non-zero elements in $\mathbb{Z}/p\mathbb{Z}$, i.e., the set $\{1, 2, \ldots, p-1\}$. Note that $\mathbb{Z}/p\mathbb{Z}$ forms a field under addition and multiplication modulo p, and $(\mathbb{Z}/p\mathbb{Z})^*$ forms a group under multiplication modulo p. For any integer a which is not a multiple of a prime p, we define the symbol $\left(\frac{a}{p}\right)$ is defined thus: $\left(\frac{a}{p}\right) = 1$ if a is a quadratic residue modulo p; $\left(\frac{a}{p}\right) = -1$ if a is a quadratic non-residue modulo p. The QRL states that

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

Keywords
Congruence, modulus, quadratic residue, quadratic reciprocity, group theory, cosets.

1. Proof Using Linear Algebra

The proof we now give is due to F Keune. It uses linear algebra and the following two results; the first one

[1] Part 1. *Resonance*, Vol.12, No.9, pp.25–39, 2007.

concerns *the nature of the multiplicative group of a finite field*, while the second one concerns *the existence of elements of a given order in a finite cyclic group.*

1. *The multiplicative group formed by the non-zero elements of any finite field is cyclic.* (This theorem is due to Galois.)

2. *Let G be a cyclic group of order n, and let k be any divisor of n. Then there exists an element of G with order k.*

1. The multiplicative group formed by the non-zero elements of any finite field is cyclic. (This theorem is due to Galois.)

2. Let G be a cyclic group of order *n*, and let *k* be any divisor of *n*. Then there exists an element of *G* with order *k*.

Let p be any prime number, and let r be any positive integer; then the theorem tells us that the multiplicative group of non-zero elements of the field $\mathbb{F}_{p^r}$ is cyclic, i.e., it has an element of order $p^r - 1$. (In the particular case of the field $\mathbb{Z}/p\mathbb{Z}$, this amounts to stating that a primitive root modulo p exists; this is a known result in number theory.) The proofs of these theorems may be found in any text on algebra.

1.1 *Keune's Proof*

Let p, q be distinct odd primes, and let n be the order of p modulo q; then $p^n \equiv 1 \pmod{q}$, so $q \mid (p^n - 1)$, i.e., $q \mid \#\left(\mathbb{F}^*_{p^n}\right)$. Since the group $\mathbb{F}^*_{p^n}$ is cyclic, this implies that there exists an element $\rho \in \mathbb{F}^*_{p^n}$ with order q.

We now work with the $q \times q$ matrix $\mathbf{A} \in M_q\left(\mathbb{F}_{p^n}\right)$ with entries $a_{i,j} = \rho^{(i-1)(j-1)}$, and with the $q \times q$ matrix $\mathbf{B} = \mathbf{A}^2$. The two matrices have the following appearance:

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \rho & \rho^2 & \cdots & \rho^{q-1} \\ 1 & \rho^2 & \rho^4 & \cdots & \rho^{2(q-1)} \\ 1 & \rho^3 & \rho^6 & \cdots & \rho^{3(q-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \rho^{q-1} & \rho^{2(q-1)} & \cdots & \rho^{(q-1)^2} \end{bmatrix},$$

The multiplicative group of non-zero elements of the field $\mathbb{F}_{p^r}$ is cyclic, i.e., it has an element of order p^r–1.

$$\mathrm{B} \ = \begin{bmatrix} q & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & q & 0 \\ 0 & 0 & 0 & \cdots & q & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & q & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}.$$

To see why **B** has the form shown, note that $b_{i,j} = \sum_{k=1}^{q} a_{i,k}\, a_{k,j} = \sum_{k=1}^{q} \rho^{(i+j-2)(k-1)}$. So if $q \mid (i+j-2)$ then $b_{i,j} = \sum_{k=1}^{q} 1 = q$, since $\rho^q = 1$. For other pairs i, j, we get $b_{i,j} = 0$, because the expression for $b_{i,j}$ simplifies to $1 + \rho + \rho^2 + \cdot + \rho^{q-1} = 0$.

From the above we get:

$$\det \mathbf{B} = q^q(-1)^{(q-1)/2}, \qquad \therefore (\det \mathbf{A})^2 = q^q(-1)^{(q-1)/2}. \tag{1}$$

Write d for $\det \mathbf{A}$. We see that $d^2 \in \mathbb{F}_p$. However, d may not be an element of $\mathbb{F}_p$. We shall now prove the following:

$$d^{p-1} = \left(\frac{q}{p}\right) \cdot (-1)^{(p-1)(q-1)/4}, \tag{2}$$

$$d^{p-1} = \left(\frac{p}{q}\right); \text{ that is, } d^{p-1} \ = \ (-1)^{(q-1)/n}. \tag{3}$$

The QRL will then readily follow from the equality $\left(\frac{q}{p}\right) \cdot (-1)^{(p-1)(q-1)/4} = \left(\frac{p}{q}\right)$.

In (3) we use the equality $\left(\frac{p}{q}\right) = (-1)^{(q-1)/n}$. We may justify this as follows. If $\frac{q-1}{n}$ is even, then $\frac{q-1}{2}$ is a multiple of n, so $p^{(q-1)/2} \equiv 1 \pmod{q}$, and therefore, $\left(\frac{p}{q}\right) = 1$. If $\frac{q-1}{n}$ is odd, then $\frac{q-1}{2}$ is equal to n times half an odd integer; therefore, $p^{(q-1)/2} \equiv -1 \pmod{q}$, and therefore, $\left(\frac{p}{q}\right) = -1$.

To prove (2) we use Euler's criterion. Since $d^2 = q^q(-1)^{(q-1)/2}$ we have:

$$d^{p-1} = \left(d^2\right)^{(p-1)/2} = q^{q(p-1)/2} \cdot (-1)^{(p-1)(q-1)/4},$$

and as $q^{(p-1)/2} \equiv \left(\frac{q}{p}\right)$ in $\mathbb{F}_p$, and q is odd, we get $d^{p-1} = \left(\frac{q}{p}\right) \cdot (-1)^{(p-1)(q-1)/4}$.

To prove (3), we write it in the form $d^p = \left(\frac{p}{q}\right) d$. By definition we have:

$$d \;=\; \sum_{\sigma \in S_q} (\text{sgn } \sigma)\, a_{1,\sigma(1)}\, a_{2,\sigma(2)} \cdots\, a_{q,\sigma(q)}.$$

Since $\mathbb{F}_p$ has characteristic p, taking p-th powers of both sides is easy to do:

$$d^p \;=\; \sum_{\sigma \in S_q} (\text{sgn } \sigma)\, a^p_{1,\sigma(1)}\, a^p_{2,\sigma(2)} \cdots a^p_{q,\sigma(q)}. \qquad (4)$$

We see from (4) that d^p is the determinant of the matrix $\mathbf{C}$ whose entries are the p-th powers of the corresponding entries of $\mathbf{A}$. That is,

$$d^p \;=\; \det \mathbf{C}, \text{ where}$$

$$\mathbf{C} \;=\; \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \rho^p & \rho^{2p} & \cdots & \rho^{p(q-1)} \\ 1 & \rho^{2p} & \rho^{4p} & \cdots & \rho^{2p(q-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \rho^{p(q-1)} & \rho^{2p(q-1)} & \cdots & \rho^{p(q-1)^2} \end{bmatrix}. \qquad (5)$$

Since $\rho^q = 1$, we may reduce the exponents modulo q, so that they lie between 0 and $q-1$; we find then that the columns of $\mathbf{C}$ are a permutation of the columns of $\mathbf{A}$, i.e., $\mathbf{C} = \mathbf{A} \times$ (a permutation matrix). This tells us that $\det \mathbf{C} = \pm \det \mathbf{A}$, i.e., $d^p = \pm d$; we only need to find which is the correct sign.

To make progress we examine the case $p = 5, q = 3$ in some detail, and see what understanding it brings.

1.2. *The Case $p = 5$, $q = 3$*

The order of 5 modulo 3 is 2, so $n = 2$. We must now construct a field $\mathbb{F}_{5^2}$ of order 5^2, and find an element $\rho \in \mathbb{F}^*_{5^2}$ with order $q = 3$. To construct a field of order 5^2, we use the polynomial $x^2 + 2$ which is irreducible over $\mathbb{F}_5$, since $-2 \equiv 3$ is a quadratic non-residue modulo 5. So $\mathbb{F}_{5^2}$ can be realized as

$$\frac{\mathbb{F}_5[x]}{(x^2+2)} \equiv \mathbb{F}_5(\alpha)$$

where α satisfies the relation $\alpha^2+2 = 0$. After searching through the elements of the field, we find that a generator of the cyclic group $\mathbb{F}^*_{5^2}$ is $\alpha + 1$. So one element with order 3 is $(\alpha+1)^8$, which simplifies to $\alpha+2$. Accordingly, we let $\rho = \alpha + 2$.

Now we construct the 3×3 matrices $\mathbf{A}$, $\mathbf{B}$ $(= \mathbf{A}^2)$, and $\mathbf{C}$ (remember that $\rho^3 = 1$):

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \rho^1 & \rho^2 \\ 1 & \rho^2 & \rho^4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \rho^1 & \rho^2 \\ 1 & \rho^2 & \rho^1 \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha+2 & -\alpha+2 \\ 1 & -\alpha+2 & \alpha+2 \end{bmatrix},$$

with $\det \mathbf{A} = 3(\rho^2 - \rho) = -\alpha$; and

$$\mathbf{B} = \mathbf{A}^2 = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 0 & 3 \\ 0 & 3 & 0 \end{bmatrix}, \qquad \mathbf{C} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \rho^2 & \rho^1 \\ 1 & \rho^1 & \rho^2 \end{bmatrix},$$

with $\det \mathbf{C} = 3(\rho - \rho^2) = \alpha$. Note that the 2nd column of $\mathbf{C}$ is the same as the 3rd column of $\mathbf{A}$, and the 3rd column of $\mathbf{C}$ is the same as the 2nd column of $\mathbf{A}$. Indeed,

$\mathbf{C} = \mathbf{AD}$, where $\mathbf{D}$ is a permutation matrix:

$$\mathbf{D} \;=\; \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \qquad \det \mathbf{D} \;=\; -1.$$

1.3. *The General Case*

In general, the columns of $\mathbf{C}$ will be some permutation of the columns of $\mathbf{A}$. If we number the columns as $0, 1, 2, \ldots, q-1$, then this permutation corresponds to some permutation θ of $\{0, 1, 2, \ldots, q-1\}$, with $\theta(0) = 0$.

It is not hard to identify θ. Since we are multiplying the exponents by p and reducing modulo q, it is simply the permutation map $\theta : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ defined by $\theta(x) = px$. Since the order of p in $\mathbb{Z}_q^*$ is n, it follows that θ is a product of the singleton cycle (0) and one or more disjoint cycles of the form $(i, pi, \cdots, p^{n-1}i)$. If the number of such cycles is t, then $tn = q - 1$. Therefore,

Since the order of p in $\mathbb{Z}_q^*$ is n, it follows that θ is a product of the singleton cycle (0) and one or more disjoint cycles of the form (i, pi, ..., p^{n-1} i).

$$\operatorname{sgn}\,(\theta) = ((-1)^{n-1})^t = (-1)^{t(n-1)} = (-1)^{q-1-t} =$$

$$\frac{(-1)^{q-1}}{(-1)^t} = (-1)^t,$$

and so $\det \mathbf{D} = (-1)^t = (-1)^{(q-1)/n}$.

It follows that $d^p = (-1)^{(q-1)/n}\, d$, and so $d^{p-1} = (-1)^{(q-1)/n}$, as claimed.

With (2) and (3) proved, our task is done. Equating the quantities on the right sides, and multiplying both quantities by $\left(\frac{q}{p}\right)$, we get the QRL:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) \;=\; (-1)^{(p-1)(q-1)/4}. \qquad (6)$$

2. Proof Using Norms from a Field Extension

Now we present a proof due to R Swan which is rather more sophisticated than the earlier proofs. It is based on calculations of *norms* of certain field extensions and rests on finding a certain 'natural' element in a cyclotomic field whose norm is $\left(\frac{p}{q}\right)$. The norm of this element turns out to be expressible in terms of sine values, and the very same expression appears in another proof of the quadratic reciprocity law (as given in J-P Serre's *A Course in Arithmetic*). Before going into the details, we first recall the basic notions of field extension and norm.

It is based on calculations of *norms* of certain field extensions and rests on finding a certain 'natural' element in a cyclotomic field whose norm is $\left(\frac{p}{q}\right)$.

We start with a familiar example, that of *Gaussian Integers*, first introduced by Gauss in 1829–1831 while studying generalizations of quadratic reciprocity law. A *Gaussian integer* is a complex number $a+bi$ where $a, b \in \mathbb{Z}$. The Gaussian integers are members of the imaginary quadratic field $\mathbb{Q}(i)$ and form a ring denoted by $\mathbb{Z}[i]$. The norm of a Gaussian integer $a+bi$ is $(a+ib)(a-ib) = a^2+b^2$, i.e., the square of its magnitude. The norm of an element may be thought of as giving an indication of its 'size'. A similar result holds true for arbitrary quadratic extensions $\mathbb{Q}(\sqrt{d})$ where d is a squarefree integer. The field $\mathbb{Q}(\sqrt{d})$ can be realized as the quotient

$$\frac{\mathbb{Q}[x]}{(x^2-d)},$$

where (x^2-d) denotes the *ideal* generated by the monic polynomial x^2-d in the ring $\mathbb{Q}[x]$. (The ideal generated by a polynomial $g(x) \in \mathbb{Q}[x]$ is the set of all multiples of $g(x)$, i.e, all elements of the form $f(x)\,g(x)$ with $f(x) \in \mathbb{Q}[x]$.) The elements of this field can also be represented by the remainders of polynomials in $\mathbb{Q}[x]$ when divided by x^2-d. For example, in $\mathbb{Q}(\sqrt{2})$, x represents $\sqrt{2}$. The norm of an arbitrary element $a+b\sqrt{d}$ is $\left(a+b\sqrt{d}\right)\left(a-b\sqrt{d}\right) = a^2-db^2$.

The field $\mathbb{Q}(\sqrt{d})$ can be realized as the quotient

$$\frac{\mathbb{Q}[x]}{(x^2-d)},$$

where (x^2–d) denotes the *ideal* generated by the monic polynomial x^2–d in the ring $\mathbb{Q}[x]$. The elements of this field can also be represented by the remainders of polynomials in $\mathbb{Q}[x]$ when divided by x^2–d.

The concept of norm is useful in algebraic number the-

$\mathbb{Q}(i)$	$= \{x + yi \ : \ x, y \in \mathbb{Q}\}$	(dimension = 2),
$\mathbb{Q}(2^{1/2})$	$= \left\{x + y\, 2^{1/2} \ : \ x, y \in \mathbb{Q}\right\}$	(dimension = 2),
$\mathbb{Q}(2^{1/3})$	$= \left\{x + y\, 2^{1/3} + z\, 2^{2/3} \ : \ x, y, z \in \mathbb{Q}\right\}$	(dimension = 3).

Table 1. Some examples of finite field extensions.

ory. *Algebraic numbers* are the roots of non-zero polynomials with integer coefficients. An *algebraic integer* is an algebraic number which is a root of a polynomial with integer coefficients and with leading coefficient 1. An *algebraic number field* is obtained by taking an algebraic number $\alpha \notin \mathbb{Q}$ and forming all the numbers that can be produced from α and the rational numbers using the operations $+$, $-$, $\times$ and $\div$ (by non-zero numbers); the field is denoted by $\mathbb{Q}(\alpha)$, and it is called a *finite dimensional field extension* of $\mathbb{Q}$, its dimension being the degree of the polynomial with integer coefficients and least degree of which α is a root. Examples are given in *Table* 1.

If $\mathbf{K}$ is an algebraic number field, we denote by $\mathbf{R}_K$ the subring containing all the algebraic integers of $\mathbf{K}$. By an abuse of notation we say that a 'unit of $\mathbf{R}_K$' is a 'unit element of $\mathbf{K}$'. The norm of an algebraic integer α is now defined to be *the product of all the roots of its monic minimal polynomial* $p(x)$. (Considering the examples mentioned above, this is a natural definition; e.g., the norm of $a + bi$ is $(a + bi)(a - bi)$; the norm of $a + b\sqrt{d}$ is $\left(a + b\sqrt{d}\right)\left(a - b\sqrt{d}\right)$.) The absolute value of the norm is also equal to the number of elements in the finite quotient ring $\frac{\mathbf{R}_K}{(\alpha)}$.

The above discussion can be generalized for any extension $\mathbf{L}/\mathbf{K}$ of number fields, as we now show. Let $\mathbf{K}$ be a field of *characteristic zero*; that is, $n \times 1 \neq 0$ for all $n \in \mathbb{N}$. Let $\mathbf{E}$ be a finite extension of $\mathbf{K}$. Let $\{\sigma_i\}_{1 \leq i \leq r}$ be the distinct embeddings (that is, injective homomorphisms) of $\mathbf{E}$ in $\mathbf{K}^a$ (the algebraic closure of $\mathbf{K}$) over

Algebraic numbers are the roots of non-zero polynomials with integer coefficients. An *algebraic integer* is an algebraic number which is a root of a polynomial with integer coefficients and with leading coefficient 1.

An element α in $\mathbf{R}_K$ is a unit if and only if $\mathbf{N}^{\mathbf{K}}_{\mathbb{Q}}(\alpha) = \pm 1.$

$\mathbf{K}$ (that is, the restriction of the above injective map is the identity map on $\mathbf{K}$). For any $\alpha \in \mathbf{E}$, we define the norm of α in $\mathbf{K}$ by

$$\mathbf{N}^E_K(\alpha) \;=\; \prod_{i=1}^{k} \sigma_i(\alpha);$$

then $\mathbf{N}^E_K(\alpha) \in \mathbf{K}^*$. The norm function is a multiplicative map, and if $\mathbf{K} \subset \mathbf{E} \subset \mathbf{F}$, then one has the transitivity property $\mathbf{N}^F_K = \mathbf{N}^E_K \circ\, \mathbf{N}^F_E$, where embeddings of $\mathbf{E}$ over $\mathbf{K}$ are extended to maps from $\mathbf{K}^a$ to $\mathbf{K}^a$ (which is possible since all extensions under consideration are algebraic) and then $\mathbf{N}^E_K$ is considered. Also, if $\mathbf{E} = \mathbf{K}(\alpha)$, and the least degree polynomial over $\mathbf{K}$ of which α is a root is $x^n + a_{n-1}x^{n-1} + \cdots + a_0$, then $\mathbf{N}^E_K(\alpha) = (-1)^n a_0$.

The following is true: *An element $\alpha \in \mathbf{R}_K$ is a unit if and only if* $\mathbf{N}^{\mathbf{K}}_{\mathbb{Q}}(\alpha) = \pm 1$.

To see why, let α be a unit; then by definition there exists $\beta \in \mathbf{R}_{\mathbf{K}}$ such that $\alpha\beta = 1$. Then, $1 = \mathbf{N}^{\mathbf{K}}_{\mathbb{Q}}(1) = \mathbf{N}^{\mathbf{K}}_{\mathbb{Q}}(\alpha\beta) = \mathbf{N}^{\mathbf{K}}_{\mathbb{Q}}(\alpha)\,\mathbf{N}^{\mathbf{K}}_{\mathbb{Q}}(\beta) \in \mathbb{Z}$. But, as the only units of $\mathbb{Z}$ are ± 1, we get $\mathbf{N}^{\mathbf{K}}_{\mathbb{Q}}(\alpha) = \pm 1$.

Next, suppose for some $\alpha \in \mathbf{R}_{\mathbf{K}}$, we have $\mathbf{N}^{\mathbf{K}}_{\mathbb{Q}}(\alpha) = \pm 1$. We know that there exists $\beta \in \mathbf{K}^*$ such that $\alpha\beta = 1$. Now α satisfies a monic integer polynomial of the form $x^n + a_{n-1}x^{n-1} + \cdots + a_0,$ where $a_i \in \mathbb{Z}$, $0 \leq i \leq n-1$. Also, $a_0 = \pm 1$. Therefore, β satisfies the monic polynomial $\pm x^n + a_1 x^{n-1} + \cdots + 1$. So, $\beta \in \mathbf{R}_{\mathbf{K}}$. Therefore, α is a unit in $\mathbf{R}_{\mathbf{K}}$. Thus this characterization of units is proved.

2.1 *Swan's Song*

With these preliminaries covered, we now give Swan's proof. Let p be an odd prime and let ς_p be a primitive p^{th} root of unity in $\mathbb{Q}^a$. The minimal polynomial of ς_p over $\mathbb{Q}$ is the cyclotomic polynomial

$$\Phi_p(x) \;=\; \prod_{r=1}^{p-1}\left(x-\varsigma_p^r\right) \;=\; 1+x+x^2+\cdots+x^{p-1}.$$

The $p-1$ embeddings of $\mathbb{Q}(\varsigma_p)$ over $\mathbb{Q}$ are those which send ς_p to ς_p^r as r varies from 1 to $p-1$. So the norm $\mathbf{N}_{\mathbb{Q}}^{\mathbb{Q}(\varsigma_p)}(1-\varsigma_p)=\Phi_p(1)=p$.

Now consider the field $\mathbf{K}_p=\mathbb{R}\cap\mathbb{Q}(\varsigma_p)=\mathbb{Q}(\varsigma_p+\varsigma_p^{-1})$. Let π_p be defined as follows:

$$\pi_p \;=\; \mathbf{N}_{\mathbf{K}_p}^{\mathbb{Q}(\varsigma_p)}(1-\varsigma_p) \;=\; (1-\varsigma_p)\left(1-\varsigma_p^{-1}\right).$$

Note that π_p is a real number, and $\mathbf{N}_{\mathbb{Q}}^{\mathbf{K}_p}(\pi_p)=\mathbf{N}_{\mathbb{Q}}^{\mathbf{K}_p}\circ\mathbf{N}_{\mathbf{K}_p}^{\mathbb{Q}(\varsigma_p)}(1-\varsigma_p)=p$ by virtue of transitivity of the norm.

Let q be another odd prime. We similarly consider the field $\mathbf{K}_q$ and the element π_q. Finally, we look at the field $\mathbf{L}=\mathbf{K}_p\mathbf{K}_q$ and the element

$$\eta=\pi_p-\pi_q=\varsigma_q+\varsigma_q^{-1}-\varsigma_p-\varsigma_p^{-1}=\varsigma_q^{-1}\left(1-\varsigma_p\varsigma_q\right)\left(1-\varsigma_p^{-1}\varsigma_q\right).$$

This element is going to be our candidate for a unit whose norm is equal to $\left(\frac{p}{q}\right)$*; we claim that* η *is a unit in* $\mathbf{R}_L$.

To prove this, we need to show only that η is a unit in $\mathbf{R}_{\mathbb{Q}(\varsigma_{pq})}$ where we have written ς_{pq} for $\varsigma_p\varsigma_q$; this is a primitive pq^{th} root of unity. We have:

$$\mathbf{N}_{\mathbb{Q}}^{\mathbb{Q}(\varsigma_{pq})}(\eta) \;=\; \mathbf{N}_{\mathbb{Q}}^{\mathbb{Q}(\varsigma_{pq})}\left(\varsigma_q^{-1}\right)\mathbf{N}_{\mathbb{Q}}^{\mathbb{Q}(\varsigma_{pq})}\left(1-\varsigma_p\varsigma_q\right)\mathbf{N}_{\mathbb{Q}}^{\mathbb{Q}(\varsigma_{pq})}\left(1-\varsigma_p^{-1}\varsigma_q\right).$$

Now, $\mathbf{N}_{\mathbb{Q}}^{\mathbb{Q}(\varsigma_{pq})}\left(\varsigma_q^{-1}\right)=\prod_{i=1}^r\sigma_i\left(\varsigma_q^{-1}\right)=\prod_{i=1}^r\varsigma_q^i=1$ (since ς_q^{-1} is also a primitive q^{th} root of unity). Next,

$$\mathbf{N}_{\mathbb{Q}}^{\mathbb{Q}(\varsigma_{pq})}\left(1-\varsigma_p\varsigma_q\right) \;=\; \frac{\prod_{i=1}^{pq-1}\left(1-\varsigma_{pq}^i\right)}{\prod_{i=1}^{q-1}\left(1-\varsigma_q^i\right)\prod_{i=1}^{p-1}\left(1-\varsigma_p^i\right)} \;=\; \frac{pq}{p\times q} \;=\; 1.$$

Similarly, we get $\mathbf{N}_{\mathbb{Q}}^{\mathbb{Q}(\varsigma_{pq})}\left(1-\varsigma_p^{-1}\varsigma_q\right)=1$. It follows that $\mathbf{N}_{\mathbb{Q}}^{\mathbb{Q}(\varsigma_{pq})}(\eta)=1$, and so η is a unit in $\mathbb{Q}(\varsigma_{pq})$. Since $\eta \in \mathbb{R}$ (the set of real numbers), it follows that $\eta^{-1} \in \mathbf{R}_{\mathbb{Q}(\varsigma_{pq})} \cap \mathbb{R}$ and hence to $\mathbf{R}_L$. Therefore, η is a unit in $\mathbf{R}_L$.

We now claim that $\mathbf{N}_{\mathbb{Q}}^{\mathbf{L}}(\eta)=\left(\frac{p}{q}\right)$.

For, $\eta \equiv \pi_p \pmod{\pi_q}$, and any embedding of $\mathbf{L}$ over $\mathbb{Q}$ must take π_p to π_p times a unit in $\mathbf{R}_L$. This is because any conjugate of ζ_p is ζ_p^r for some $1 \le r \le p-1$, and the element $1-\zeta_p^r$ is $1-\zeta_p$ times a unit in $\mathbb{Q}(\zeta_p)$. In other words, both π_p and π_q are moved by an embedding of $\mathbf{L}$ to themselves times units in $\mathbf{R}_L$. Hence, we have

$$\mathbf{N}_{\mathbb{Q}}^{\mathbf{L}}(\eta) \;=\; \prod_{\sigma}(\sigma(\pi_p)-\sigma(\pi_q)) \;\equiv\; \mathbf{N}_{\mathbb{Q}}^{\mathbf{L}}(\pi_p) \pmod{\pi_q}\mathbf{R}_L.$$

But then $\mathbf{N}_{\mathbb{Q}}^{\mathbf{L}}(\eta)-\mathbf{N}_{\mathbb{Q}}^{\mathbf{L}}(\pi_p) \in \pi_q\mathbf{R}_L \cap \mathbb{Z}$.

Now, as $q=\mathbf{N}_{\mathbb{Q}}^{\mathbf{K}_q}(\pi_q) \in \pi_q\mathbf{R}_{\mathbf{K}_q} \subset \pi_q\mathbf{R}_L$, and as $q\mathbb{Z}$ is a maximal ideal, it follows that $q\mathbb{Z}=\pi_q\mathbf{R}_L \cap \mathbb{Z}$. Hence, $\mathbf{N}_{\mathbb{Q}}^{\mathbf{L}}(\eta)-\mathbf{N}_{\mathbb{Q}}^{\mathbf{L}}(\pi_p) \in q\mathbb{Z}$.

On the other hand, $\mathbf{N}_{\mathbb{Q}}^{\mathbf{L}}(\pi_p)=\mathbf{N}_{\mathbb{Q}}^{\mathbf{K}_p} \circ \mathbf{N}_{\mathbf{K}_p}^{\mathbf{L}}(\pi_p)=\mathbf{N}_{\mathbb{Q}}^{\mathbf{K}_p}(\pi_p)^{(q-1)/2}=p^{(q-1)/2}$, because $[\mathbf{L}:\mathbf{K}_p]=\frac{1}{2}(q-1)$.

So $\mathbf{N}_{\mathbb{Q}}^{\mathbf{L}}(\eta) \equiv p^{(q-1)/2} \equiv \left(\frac{p}{q}\right) \pmod{q}$. As the left side is ± 1, and so is $(\frac{p}{q})$, they must be equal, and the claim follows.

Interchanging p and q, we get $(-1)^{[\mathbf{L}:\mathbb{Q}]}\mathbf{N}_{\mathbb{Q}}^{\mathbf{L}}(\eta)=\left(\frac{q}{p}\right)$. Therefore,

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

This is equivalent to the QRL.

Remarks

It is interesting to note that η can be rewritten as follows. Writing $\varsigma_p=e^{2\pi i r/p}$ for some $1 \le r \le p-1$, we get

$$\pi_p \;=\; 4\sin^2\left(\frac{\pi r}{p}\right).$$

Thus, the norm

$$\mathbf{N}^{\mathbf{L}}_{\mathbb{Q}}(\eta) \;=\; 4^{[\mathbf{L}:\mathbb{Q}]}\prod_{s,t}\left(\sin^2\frac{\pi s}{p} - \sin^2\frac{\pi t}{q}\right).$$

This is exactly the expression in the trigonometric proof given in Serre's book. So this in some sense provides a conceptual way of viewing the trigonometric proof, which is otherwise quite mysterious and scarcely believable.

Acknowledgments: I would like to thank B Sury under whose supervision I did this work during the summer break of 2006. I would also like to thank Shailesh Shirali for reading through earlier versions and making key suggestions to make the exposition readable.

Suggested Reading

[1] G H Hardy and E M Wright, *Introduction to the Theory of Numbers*, Oxford University Press.

[2] F Keune, Quadratic reciprocity and finite fields, *Nieuw Archief voor Wiskunde*, Vol.4, No.9, pp.263–266, 1991.

[3] S Lang, *Algebra*, Springer Verlag, 2002.

[4] R C Laubenbacher and D J Pengelley, Eisenstein's misunderstood geometric proof of the quadratic reciprocity theorem, *College Mathematics Journal,* Vol.25, pp.29–34, 1994.

[5] R C Laubenbacher and D J Pengelley, Gauss, Eisenstein, and the third proof of the quadratic reciprocity theorem, Ein kleines Schauspiel, *Mathematical Intelligencer*, Vol.16, No.2, pp.67–72, 1994.

[6] J-P Serre, *A Course in Arithmetic*, Springer Verlag, 1973.

[7] B Sury, *Group Theory – Selected Problems*, Universities Press, 2004.

[8] R G Swan, Another proof of the quadratic reciprocity law?, *American Mathematical Monthly*, Vol.97, pp.138–139, 1990.

Address for Correspondence
Shivam Kumar
S/o Mr Harishankar Prasad Singh
Coal Mines Provident Fund Office
Dhanbad 2 Region
Dhanbad 826 001.
Jharkhand, India.
Email:shivam.isi@gmail.com