Theorema Aureum – 1

Shivam Kumar

Are there perfect squares which on division by 7 leave remainder 3? Are there perfect squares which on division by 3 leave remainder 7? (A "remainder of 7" on division by 3 is the same as a remainder of 1.) The answers: 'NO' and 'YES', respectively. These facts are stated by number theorists as follows: *3 is a quadratic non-residue modulo 7; 7 is a quadratic residue modulo 3.* The notion of quadratic residue is far reaching, and the key theorem here is the Law of Quadratic Reciprocity, first stated by Euler in 1783, but without proof, and first proved by Gauss, in 1796. The theorem is easy to state but is mysterious, as it reveals a connection between two questions that appear unconnected. Let p, q be distinct odd primes; then the questions are: "Is p a quadratic residue modulo q?" and "Is q a quadratic residue modulo p?" Gauss had a high regard for this result and called it *Theorema Aureum*, the Golden Theorem. Though it has been proved in many different ways, it retains its mystery. In this two part article we give three proofs of the theorem. The first one, described in this part, is based on group theory.

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.

1. Historical Setting

Historically, one of the important reasons for studying algebra has been to find good ways of solving polynomial equations. Linear and quadratic equations were mastered long back, and attempts to solve the cubic equation brought mathematicians into contact for the first time with the strange world of complex numbers. By the seventeenth century, cubic equations and quartic

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

equations had been mastered, and attention then turned to the quintic (degree 5) equation. The resolution of this problem (in the negative[1], as it turned out) is an extremely important stage in the development of algebra, for it brought forth group theory, the theory of finite fields, Galois theory, and most importantly, the **axiomatic approach** in algebra.

In the last decade of the eighteenth century, Carl Gauss opened the field wide by expanding the domain over which we may seek solutions to equations. He introduced the notion of a **congruence** among integers, denoted by the symbol '$\equiv$'. Let a, b and m be integers, with $m \neq 0$; we call m the **modulus**, and say that *a and b are congruent modulo m* if they leave the same remainder on division by m; we write this compactly as $a \equiv b \pmod{m}$; e.g., $17 \equiv 12 \pmod 5$ and $37 \equiv 13 \pmod 8$. The word 'congruence' is used here in much the same way as it is in geometry, where we say that two shapes are congruent to each other if they 'look the same'. The idea is that when the modulus is m, then the universe of available numbers is (in effect) the finite set $\{0, 1, 2, \ldots, m-1\}$, and the numbers 1, $m+1$, $2m+1$, $3m+1, \ldots$ 'look' the same in this world, as do the numbers 2, $m+2$, $2m+2$, $3m+2, \ldots$ (we may picture the numbers as 'cycling back' to 0 after reaching $m-1$). The algebra of congruences is easy to construct, as the congruence symbol '$\equiv$' obeys practically all the rules of the more familiar equality symbol, '$=$'. Only division can pose some difficulty, and even this is not the case if the modulus is a prime number; e.g., if $m = 7$, then $2 \times 4 \equiv 1$, so 2 and 4 may be called reciprocals of each other, and this shows how division can be done; e.g., $3/4 \equiv 3 \times 2 \equiv 6 \pmod 7$.

Once this idea has been conceived, the possibility of *solving equations* over these finite domains immediately suggests itself. For example, the linear equation $2x + 3 \equiv 4 \pmod 7$ has the unique solution $x \equiv 4 \pmod 7$, and

[1] Ruffini, Abel and Galois showed, independently, that equations of degree 5 and higher cannot be solved in the same way that we solve equations of degree less than 5, i.e., using methods of school algebra such as 'completing the square' and so on.

the quadratic equation $x^2 + 2x \equiv 3 \pmod 7$ has two solutions $x \equiv 1 \pmod 7$ and $x \equiv 4 \pmod 7$. On the other hand, the equation $x^2 + 2x \equiv 4 \pmod 7$ has no solutions. The intricacy of algebra in this finite domain soon emerges, posing numerous questions of great appeal to a mathematician.

For studying further the algebra of congruences, the reader may consult any book on number theory; e.g., the well-known one by Hardy and Wright [1].

2. Quadratic Reciprocity

Quadratic reciprocity concerns congruences of the kind $x^2 \equiv a \pmod p$, where a is an integer and p is a prime number, and x is an integer to be found. Depending on the values of a and p, this congruence may or may not have any solutions. For example, the congruences $x^2 \equiv 2 \pmod 3$ and $x^2 \equiv 5 \pmod 7$ have no solutions, as may be verified by simply computing the squares of the first few positive integers and checking their residues modulo 3 and modulo 7, respectively. On the other hand, the congruences $x^2 \equiv 1 \pmod 3$ and $x^2 \equiv 2 \pmod 7$ do possess solutions; the former congruence has solutions $x \equiv \pm 1 \pmod 3$, the latter one $x \equiv \pm 3 \pmod 7$.

The more general quadratic congruence $ax^2 + bx + c \equiv 0 \pmod m$, where a, b, c, m are integers and x is an integer to be found, may always be reduced to a finite set of congruences of the type $x^2 \equiv a \pmod p$. But this simple looking congruence possesses vast depths! So the study of these congruences takes care of all quadratic congruences.

Let p denote an odd prime number, and let a be any integer not divisible by p. If the congruence $x^2 \equiv a \pmod p$ possesses a solution, then a is called a Quadratic Residue modulo p; if not, it is a Quadratic Non-Residue modulo p. For example, in the set $\{1, 2, 3, \ldots, 10\}$, the quadratic residues modulo 11 are 1, 3, 4, 5, 9 and the quadratic

Box 1. Quadratic Residues, Cryptography, Coin Tossing, Primality Testing

Studying quadratic residues modulo a prime is not only a natural problem in number theory, it also proves extremely useful in several other places like cryptography. Here is one way of seeing the connection. We stated in the article that the quadratic residues modulo 11 are 1, 3, 4, 5, 9 and the quadratic non-residues are 2, 6, $7, 8$, 10. So the numbers from 1 to 10 have been placed in two sets, but they give the impression of being randomly distributed. This fact may be made use of in devising codes and in "tossing a coin over a telephone" (i.e., tossing a coin electronically) and conveying the result in a believable and verifiable way.

In primality testing, there is an efficient test called the Miller–Rabin primality test which is not known to be deterministic, but it can be proved to be deterministic if one could guarantee the existence of 'small' quadratic non-residues modulo any prime. Such a guarantee can be given if one assumes one of the deepest open problems of mathematics – the Generalized Riemann Hypothesis. We describe the Miller–Rabin test in *Box* 2.

non-residues are 2, 6, $7, 8$, 10. Among the many attractive properties of these sets of numbers are the following: (I) There are as many quadratic residues modulo p as non-residues modulo p. (II) The product of two quadratic residues or two non-residues modulo p is a quadratic residue modulo p; e.g., $4 \times 5 \equiv 9$ or $6 \times 8 \equiv 4$ for the case $p = 11$. (III) The product of a quadratic residue and a non-residue modulo p is a quadratic non-residue modulo p; e.g., $3 \times 7 \equiv 10$.

Properties (II), (III) remind us of the arithmetical relations 'plus × plus = plus', 'minus × minus = plus' and 'plus × minus = minus'; and indeed, there *is* a group theoretic connection.

A convenient way of denoting the quadratic character of a modulo p is through the use of the following symbol first introduced by Legendre:

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

For example, $\left(\frac{2}{7}\right) = +1$, whereas $\left(\frac{2}{5}\right) = -1$. If a is a multiple of p, we write $\left(\frac{a}{p}\right) = 0$.

An easily proved (and most convenient) property of the Legendre symbol is its *multiplicativity*: we have $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ for all integers a, b, and all primes p. (This is another way of expressing properties (II), (III) given above.)

Is there a quick way of computing $\left(\frac{a}{p}\right)$ for a given integer a and a prime number p? Following the remark made above, we may restrict our attention to the cases when the numerator a is prime; e.g., one may ask for the value of $\left(\frac{29}{641}\right)$ or $\left(\frac{101}{1999}\right)$. In the resolution of this question lies a startling fact connecting the values of $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ for pairs of distinct odd primes p and q. This connection was first found empirically by Euler and Legendre, and proved rigorously by Gauss, but the seeds of its discovery lie in discoveries made much earlier by Fermat. Today this connection is called Quadratic Reciprocity. The famous law of quadratic reciprocity may thus be said to have had more than one birth!

3. First Movement: Fermat, *circa* 1640; Euler, *circa* 1749

Fermat's discovery is the following, which he expressed in a letter to Mersenne in 1540:

> *Every prime number which surpasses by one*
> *a multiple of four is composed of two*
> *squares . . . .*

That is, a prime number $p \equiv 1 \pmod 4$ is a sum of two squares. In a letter to Pascal in 1654, he also wrote[2] that a prime number $p \equiv 1 \pmod 3$ is of the form $x^2 + 3y^2$, and that a prime number $p \equiv 1$ or $3 \pmod 8$ is of the form $x^2 + 2y^2$.

The prolific Leonhard Euler learnt of many of Fermat's assertions through his correspondence with Goldbach,

[2] Fermat often mentioned results without proof, in his letters and other writings. Considering the story behind Fermat's Last Theorem, we should be thankful for this habit of his!

and it became a life-long passion for him to prove these assertions. (And, being Euler, he succeeded most of the time.)

Euler's proof of Fermat's statement that a prime number $p \equiv 1 \pmod 4$ is a sum of two squares had two steps:

- A *descent step* to show that if p is a prime number which divides a number of the form $x^2 + y^2$ with x, y coprime, then p is itself a sum of two squares;
- A *reciprocity step* to show that a prime number of the form $p \equiv 1 \pmod 4$ does divide a number of the form $x^2 + y^2$ with x, y coprime.

Using the same method, Euler also proved the other two assertions of Fermat (given above). He spent a number of years in proving the reciprocity steps. Indeed, the reason we have called it the 'reciprocity' step is because, in modern terminology, the two reciprocity statements:

- *A prime p divides $x^2 + y^2$ for some $(x, y) = 1$ if and only if $p \equiv 1$ mod 4,*
- *A prime p divides $x^2 + 2y^2$ for some $(x, y) = 1$ if and only if $p \equiv 1$ or 3 mod 8,*

are equivalent, respectively, to the assertions

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

After discovering several similar such results, for example, that

$$\left(\frac{7}{p}\right) = 1 \text{ if and only if } p \equiv \pm 1, \pm 3, \pm 9 \pmod{28},$$

Euler finally made the following conjecture around 1749:

Euler's Conjecture. *Let p, q denote distinct odd primes; then $\left(\frac{q}{p}\right) = 1$ if and only if $p \equiv \pm\alpha^2 \pmod{4q}$ for some odd integer α.*

It is easy to see that this conjecture is equivalent to the usual formulation of the

Law of Quadratic Reciprocity (QRL). *Let p, q denote distinct odd primes; then*

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

Equivalently: if one or both of p, q are of the form $1 \pmod 4$*, then* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$*; and if p, q are both of the form* $3 \pmod 4$*, then* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

4. Second Movement: Gauss, *circa* 1795

The second independent birth of the reciprocity law occurred in Gauss's work in March 1795; he was not yet 18 then! In April 1796 Gauss found the first complete proof of the quadratic reciprocity law[3]. Apparently, he became aware of Euler's and Legendre's work only later. Following his first proof, Gauss found a number of other proofs. The second proof involves the deep genus theory of binary quadratic forms which he himself pioneered. One reason he gave many proofs may be that he considered it a very fundamental result — he called it the *theorema aureum* (the golden theorem). Several people have given proofs subsequently, and a tongue-in-cheek title of a paper by Gerstenhaber suggests his proof to be the 152nd! However, many of these proofs are similar to others. In this two-part article I single out three proofs which use different ideas and which I enjoyed learning about. They are all pretty and not too well known; none of them appears in any textbook.

We resisted the temptation to include the elegant geometric proof given by Gauss's phenomenal but tragically short-lived student G Eisenstein[4], as it appears in one form in the famous book by Hardy and Wright [1]. It must be remarked that not all the beautiful features of Eisenstein's proof seem to have been well understood as

[3] Later Gauss wrote, "For a whole year this theorem tormented me and absorbed my greatest efforts ...".

[4] Eisenstein was very pleased with his own proof and wrote, "How lucky good Euler would have considered himself, had he possessed these lines about seventy years ago."

pointed out by Laubenbacher and Pengelley [2] in their engaging article in *Mathematical Intelligencer.*

Remark. There have been various generalizations of quadratic reciprocity; we have cubic reciprocity (Gauss and Eisenstein), quartic reciprocity (Gauss), general p-adic reciprocity (Eisenstein), Artin's general abelian reciprocity law, the Hilbert–Takagi class field theory, and its nonabelian generalizations (in the 'Langlands program'), and so on. We shall not go into any of these in this article.

4.1 *Notation*

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.

4.2 *Euler's Criterion*

Before proceeding with the proofs, we recall an important criterion used to check quadratic reciprocity. First note that the congruence

$$\left(x^{(p-1)/2}\right)^2 \equiv 1 \pmod{p}$$

implies that $x^{(p-1)/2} = \pm 1$ for any $x \in \mathbb{Z}/p\mathbb{Z}$. But if $x = y^2$, then

$$x^{(p-1)/2} = y^{p-1} \equiv 1 \pmod{p},$$

so the quadratic residues are all roots of the polynomial $t^{(p-1)/2} - 1$. Since this polynomial cannot have more than $\frac{1}{2}(p - 1)$ roots in the field $\mathbb{Z}/p\mathbb{Z}$, we conclude that its roots are exactly the quadratic residues. This yields

Box 2. The Miller–Rabin Primality test

This is in wide usage especially for the RSA cryptosystem.

Let n be an odd prime; write $n-1 = r\cdot 2^s$ with r odd. For $(a,n)=1$, we have $a^{2^{s-1}r} \equiv \pm 1$ mod n. Thus, a satisfies at least one of the following conditions:

- $a^r \equiv 1 \bmod n$;
- $a^{2^i r} \equiv -1$ for some $0 \leq i < s$.

A *composite* n which satisfies this last-mentioned property is called a *strong pseudoprime to the base* a. One also calls such a base *a strong liar* for n. When n is *not* a strong pseudoprime to some base a (that is, if each of the $s+1$ congruences fails), then evidently n is composite, and a is known as a *strong witness* to the compositeness of n.

For example, the Carmichael number 561 has 2 as a strong witness. This is so because $560 = 16 \times 35$ and $2^{35} \equiv 263, 2^{2\times 35} \equiv 166$, and $2^{4\times 35} \equiv 67$ mod 561. Also $2^{8\times 35} \equiv 1$ mod 561.

The Miller–Rabin test starts by picking a random $a < n-1$ and checking whether a^r (mod n) is ± 1. If it is, then n "passes the test" and we conclude that n is a "probable prime"; we then move to the next a. If it is not ± 1, we keep squaring (up to $s-1$ times) and checking until we reach -1. If it does, then again n passes the test and is a probable prime; we move to the next a. If -1 is never reached, then n must be composite.

It turns out that at the most $\frac{1}{4}$ of the numbers 1, 2, ... , $n-1$ can be strong liars for a composite n. Thus, after d iterations, the probability that the Miller–Rabin test concludes primality of a composite n is at the most $\frac{1}{4^d}$; this is the probability of a wrong conclusion. It may be shown that the Miller–Rabin test is deterministic if we assume the Generalized Riemann hypothesis or GRH.

A consequence of GRH is that for any prime $p \geq 3$, the least quadratic nonresidue is strictly less than $2(\log p)^2$. So if the Miller–Rabin test is performed for all a less than $2(\log n)^2$, then it finds a strong witness for n. This makes it a deterministic test.

the criterion due to Euler:

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

Here is an example of the usage of the criterion: we shall compute $\left(\frac{3}{29}\right)$. The criterion tells us that $\left(\frac{3}{29}\right) \equiv 3^{14}$ (mod 29). Now, modulo 29 we have:

$$3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^3 \equiv 27 \equiv -2, \quad 3^4 \equiv 81 \equiv -6,$$

$$3^7 \equiv (-2) \times (-6) \equiv 12, \quad 3^{14} \equiv 12^2 \equiv 144 \equiv -1.$$

Therefore, 3 is a quadratic non-residue modulo 29.

4.3 *Two Illustrations of QRL*

We give two examples of the law in action.

- $p = 5, q = 19$

  Here $p \equiv 1$ and $q \equiv 3 \pmod 4$, so QRL predicts that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, that is, $\left(\frac{5}{19}\right) = \left(\frac{19}{5}\right)$.

  This is true, as both sides are equal to 1. For we have: $9^2 = 81 \equiv 5 \pmod{19}$, showing that $\left(\frac{5}{19}\right) = 1$; and $2^2 = 4 \equiv 19 \pmod 5$, showing that $\left(\frac{19}{5}\right) = 1$.

- $p = 7, q = 23$

  Here both $p \equiv 3$ and $q \equiv 3 \pmod 4$, so QRL predicts that $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, that is, $\left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right)$.

  This is true; we can verify by calculation that 7 is a quadratic non-residue modulo 23, so $\left(\frac{7}{23}\right) = 1$; but 23 is a quadratic residue modulo 7, for we have $3^2 = 9 \equiv 2 \equiv 23 \pmod 7$, so $\left(\frac{23}{7}\right) = -1$.

5. First Proof of QRL – by Counting Cosets

We begin with a computation-based group theoretic proof due to G Rousseau. Throughout, p, q represent an arbitrary but given pair of distinct, odd primes.

In the language of abstract algebra, CRT[5] gives a ring isomorphism of $\mathbb{Z}/pq\mathbb{Z}$ with $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, the map being $c \mapsto (a, b)$ with $c \equiv a \pmod p$, $c \equiv b \pmod q$.

In particular, the groups of *units* (i.e., the invertible elements) on both sides are isomorphic to each other. Since the units in a direct product of rings are the elements

[5] Recall the Chinese Remainder Theorem (CRT): Given any two integers a,b, an integer x may be found such that $x \equiv a \pmod p$ and $x \equiv b \pmod q$. In the interval $[1, pq]$, there is just one such x.

Isomorphism of rings

$\mathbb{Z}/15\mathbb{Z}$	0	1	2	3	4	5	6	7
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$	$(0,0)$	$(1,1)$	$(2,2)$	$(0,3)$	$(1,4)$	$(2,0)$	$(0,1)$	$(1,2)$

$\mathbb{Z}/15\mathbb{Z}$	8	9	10	11	12	13	14
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$	$(2,3)$	$(0,4)$	$(1,0)$	$(2,1)$	$(0,2)$	$(1,3)$	$(2,4)$

Isomorphism of groups of units

$(\mathbb{Z}/15\mathbb{Z})^*$	1	2	4	7	8	11	13	14
$(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$	$(1,1)$	$(2,2)$	$(1,4)$	$(1,2)$	$(2,3)$	$(2,1)$	$(1,3)$	$(2,4)$

- $\{1,14\}$ is a subgroup of $(\mathbb{Z}/15\mathbb{Z})^*$, of order 2. It may also be written as $\{1,-1\}$.
- The corresponding subgroup of $(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$ is $H = \{(1,1),(2,4)\}$. It may also be written as $H = \{1,1),(-1,-1)\}$.

Table 1. Shows the correspondences for the case p = 3, q = 5.

that have units in each coordinate, we have a group isomorphism τ of $(\mathbb{Z}/pq\mathbb{Z})^*$ with $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$.

*T*able 1 shows the ring and group isomorphisms for the case $p = 3, q = 5$.

Now consider the subgroup $K = \{1,-1\}$ of $(\mathbb{Z}/pq\mathbb{Z})^*$, generated by -1; it has order 2. The isomorphism maps it to a subgroup of order 2 of $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$; namely, $\tau K = H = \{(1,1),(-1,-1)\}$. If we evaluate and compare the products of the coset representatives of K and H, we find to our surprise that we get the reciprocity law!

To motivate the analysis of the general case, it is worth taking a careful look at the case $p = 3, q = 5$. Let $\tau : (\mathbb{Z}/15\mathbb{Z})^* \to (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$ denote the group isomorphism shown in *Table* 1. Then τ maps the subgroup $K = \{1,14\}$ of $(\mathbb{Z}/15\mathbb{Z})^*$ to the subgroup $\tau K = \{(1,1),(2,4)\}$ of $(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$.

In the group $(\mathbb{Z}/15\mathbb{Z})^*$, the cosets of $K = \{1, 14\}$ are

$$\{1, 14\}, \quad \{2, 13\}, \quad \{4, 11\}, \quad \{7, 8\}.$$

The quotient group here, $(\mathbb{Z}/15\mathbb{Z})^*/K$, is isomorphic to the cyclic group of order 4, and the product of the cosets is the coset $\{4, 11\}$. (This is the element in the quotient group that has order 2.)

In the group $(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$, the cosets of $\tau K = \{(1, 1), (2, 4)\}$ are

$$\{(1, 1), (2, 4)\},\ \{(2, 2), (1, 3)\},\ \{(1, 4), (2, 1)\},\ \{(1, 2), (2, 3)\}.$$

The product of the cosets is the coset $\{(1, 4), (2, 1)\}$. Observe that τ maps the product of the cosets of K to the product of the cosets of τK. This was to be expected.

The same correspondence must hold in the general case. On probing further, we get the reciprocity law. The details are as follows.

We consider the group $G_1 = (\mathbb{Z}/pq\mathbb{Z})^*$, its subgroup $K = \{1, -1\}$ of order 2, and the quotient group G_1/K which has $\frac{1}{2}(p - 1)(q - 1)$ elements.

Under τ, this translates into the group $G_2 = (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$, its subgroup $H = \tau K = \{(1, 1), (-1, -1)\}$ of order 2, and the quotient group G_2/H which has $\frac{1}{2}(p - 1)(q - 1)$ elements.

The cosets of K in G_1 have the form $\{i, pq - i\}$ where i is coprime to pq. Since $\min\{i, pq - i\} < \frac{1}{2}pq$, we can always select a representative from each coset which is less than $\frac{1}{2}pq$. It follows that the set T given by

$$T \ = \ \{i \ : \ 1 \leq i \leq \frac{1}{2}(pq - 1),\ \gcd(i, pq) = 1\}$$

is a set of distinct coset representatives of K in $G_1 = (\mathbb{Z}/pq\mathbb{Z})^*$.

The cosets of H in G_2 have the form $\{(i,j),(p-i, q-j)\}$. Since $\min\{j, q-j\} < \frac{1}{2}q$, we can always select a representative from each coset whose second coordinate is less than $\frac{1}{2}q$. It follows that the set S given by

$$S \;=\; \{(i,j) \;:\; 1 \le i \le p-1,\; 1 \le j \le \frac{1}{2}(q-1)\}$$

is a set of distinct coset representatives of H in $G_2 = (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$.

Note that $\#T = \#S = \frac{1}{2}(p-1)(q-1) = \#G_1/K = \#G_2/H$.

Next, we calculate the products of the elements of the coset representatives S and T in the respective groups. For the group $G_2 = (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$, we get the product

$$\prod_{s\in S} s \;=\; \left((p-1)!^{(q-1)/2},\; \left(\left(\frac{q-1}{2}\right)!\right)^{p-1}\right) H. \quad (1)$$

For the group $G_1 = (\mathbb{Z}/pq\mathbb{Z})^*$, we have, modulo p:

$$\begin{aligned}\prod_{t\in T} t \;&\equiv\; \frac{\left(\prod_{i=1}^{p-1} i\right)\cdot\left(\prod_{i=1}^{p-1}(p+i)\right)\cdot\left(\prod_{i=1}^{p-1}(2p+i)\right)\cdots\prod_{i=1}^{(p-1)/2}\left((\frac{1}{2}(q-1)p+i\right)}{q\cdot 2q\cdot\;\cdots\;\cdot\frac{1}{2}(p-1)q}\\ &\equiv\; \frac{(p-1)!^{(q-1)/2}\cdot(\frac{1}{2}(p-1))!}{q^{(p-1)/2}\cdot(\frac{1}{2}(p-1))!} \;\equiv\; \frac{(p-1)!^{(q-1)/2}}{\left(\frac{q}{p}\right)} \qquad \text{(Euler's criterion!)}\\ &\equiv\; (p-1)!^{(q-1)/2}\cdot\left(\frac{q}{p}\right) \pmod p \;\equiv\; (-1)^{(q-1)/2}\cdot\left(\frac{q}{p}\right) \pmod p,\end{aligned}$$

where Wilson's theorem (the statement that $(r-1)! \equiv -1 \pmod r$ for all primes r) is needed in the last step. In the same way, we get, working modulo q:

$$\prod_{t\in T} t \;\equiv\; (-1)^{(p-1)/2}\cdot\left(\frac{p}{q}\right) \pmod q.$$

Therefore, by the CRT, τ maps $\prod_{t \in T} t$ to

$$\left((-1)^{(q-1)/2} \cdot \left(\frac{q}{p}\right), \;\; (-1)^{(p-1)/2} \cdot \left(\frac{p}{q}\right)\right) H \;\in\; G_2/H. \tag{2}$$

Since $i \equiv -(q-i) \pmod{q}$, we have:

$$(q-1)! \;\equiv\; \left(\left(\frac{q-1}{2}\right)!\right)^2 \times (-1)^{(q-1)/2} \pmod{q}.$$

Raising both sides to the $\frac{1}{2}(p-1)$-th power and using Wilson's theorem again, we get:

$$\left(\left(\frac{q-1}{2}\right)!\right)^{p-1} \;\equiv\; (-1)^{(p-1)/2} \cdot (-1)^{(p-1)(q-1)/4} \pmod{q}. \tag{3}$$

Expression (1) for $\prod_{s \in S} s$ may therefore be simplified (after reducing the first coordinate modulo p, and the second coordinate modulo q) to

$$\left((-1)^{(q-1)/2}, \;\; (-1)^{(p-1)/2} \cdot (-1)^{(p-1)(q-1)/4}\right) H. \tag{4}$$

Since expressions (2) and (4) represent the same element in G_2/H, comparing them we get

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

which is nothing but the Law of Quadratic Reciprocity!

5.1 *Illustration: The Case $p = 3$, $q = 5$*

Let us work through the case $p = 3$, $q = 5$. We know that 3 is not a square in $\mathbb{Z}/5\mathbb{Z}$, nor is 5 a square in $\mathbb{Z}/3\mathbb{Z}$. So, $\left(\frac{3}{5}\right) = -1$, $\left(\frac{5}{3}\right) = -1$, $\left(\frac{3}{5}\right) \cdot \left(\frac{5}{3}\right) = 1$.

Let us check this against the above computations. Using the same symbols, we have: $G = (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$,

$S = \{(1,1),(1,2),(2,1),(2,2)\}$, $T = \{1,2,4,7\}$, and:

$$\prod_{s\in S} s \;\equiv\; (4,4)H \equiv (1,-1)\,H,$$

$$\prod_{t\in T} t \;\equiv\; (-1)^2\left(\frac{5}{3}\right) \pmod 3 \;\equiv\; \left(\frac{5}{3}\right) \pmod 3,$$

$$\prod_{t\in T} t \;\equiv\; (-1)^1\left(\frac{3}{5}\right) \pmod 5 \;\equiv\; -\left(\frac{3}{5}\right) \pmod 5.$$

Comparing the two results we see that

$$-\left(\frac{5}{3}\right)\cdot\left(\frac{3}{5}\right) \;=\; 1\cdot(-1),$$

that is, $\left(\frac{5}{3}\right)\cdot\left(\frac{3}{5}\right) = 1$, in agreement with what was stated at the beginning.

More to come ... In Part 2 we present two more proofs of the QRL – one based on linear algebra, and the other on the notion of field extensions. The latter proof is rather more advanced than the first two.

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