V.1 From Quadratic Reciprocity to Class Field Theory

Kiran S. Kedlaya

The law of quadratic reciprocity, discovered by EULER (X.X) and first proved by GAUSS (X.X) (who dubbed it his *theorema aureum*, or golden theorem), is considered a crown jewel of number theory, and with good cause. Whereas its statement could be rediscovered by a sufficiently ingenious student (indeed, it actually has been rediscovered on a regular basis at the Arnold Ross mathematics summer program for several decades), rare is the student who comes up with a proof unassisted.

The law is most conveniently stated in LEGENDRE's (X.X) formulation. For n an integer not divisible by the prime p, write $(\frac{n}{p}) = 1$ if n is congruent to some perfect square modulo p, and $(\frac{n}{p}) = -1$ if it is not. Then quadratic reciprocity states the following. (The prime 2 must be treated separately.)

Theorem (quadratic reciprocity). *Suppose that p and q are two different primes, neither equal to 2. Then $(\frac{p}{q})(\frac{q}{p}) = -1$ if p and q are both congruent to 3 modulo 4, and $(\frac{p}{q})(\frac{q}{p}) = 1$ otherwise.*

For instance, if $p = 13$ and $q = 29$, then $(\frac{p}{q})(\frac{q}{p}) = 1$. Since 29 is congruent modulo 13 to the perfect square 16, it must be that 13 is congruent to some perfect square modulo 29, and in fact $100 = 3 \cdot 29 + 13$.

This statement is simple but also mysterious, because it violates our intuition that congruences modulo different primes should act independently. For instance, the Chinese remainder theorem asserts that (in a suitably precise sense) knowing that a random integer is odd or even does not prejudice it toward having any particular remainder modulo 3. Number theorists are fond of using geometric language to describe this situation, referring to phenomena associated with congruences modulo a single prime (or a power of a single prime) as *local* phenomena. The Chinese remainder theorem can be interpreted as saying that local phenomena at one point really are local, in that they do not influence local phenomena at another point. However, just as a particle physicist cannot explain the behavior of the universe by analyzing individual particles in isolation, one cannot hope to understand the behavior of integers by looking at individual primes in isolation. Quadratic reciprocity thus emerges as one of the first known examples of a *global* phenomenon, proving to be a "fundamental force" that binds together two different primes. The interplay between local and global is built thoroughly into our modern understanding of number theory, but the phenomenon of quadratic reciprocity was where it first came to light.

Another indication of the fundamental nature of quadratic reciprocity is that it admits proofs using many different techniques. Gauss himself devised eight proofs in his lifetime, and nowadays dozens of proofs are available. These suggest numerous directions of generalization; here we will focus on the direction that led historically to class field theory. Among the many fascinating sidelights that this will force us to omit is the theory of Gauss sums and its surprisingly diverse range of applications, such as Kolyvagin's work on THE CONJECTURE OF BIRCH AND SWINNERTON-DYER (X.X), and the use of number theory in CRYPTOGRAPHY (X.X) and other areas of computer science.

Euler had sought reciprocity laws for perfect third and fourth powers, but had had limited success. Gauss succeeded in formulating such laws (but not proving them; that fell to Eisenstein later) by realizing that one could only properly understand them by stepping out of the ring of integers.

Let us see this explicitly for fourth powers. Let p and q be primes that are both congruent to 1 modulo 4. The reciprocity between p being congruent to a fourth power modulo q and vice versa cannot be easily stated in terms of p and q. Instead, we must recall a result of Fermat: we can write $p = a^2 + b^2$ and $q = c^2 + d^2$, where each of the pairs (a, b) and (c, d) is unique up to changing signs and ordering. In other words, in the ring of complex numbers whose real and imaginary parts are integers (now called the *Gaussian integers*), we have $p = (a + b\mathrm{i})(a - b\mathrm{i})$ and $q = (c + d\mathrm{i})(c - d\mathrm{i})$.

Gauss defined an analogue of the Legendre symbol as follows. It was already known to Euler that

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

to see that the right-hand side is either 1 or -1, note that it squares to 1 by FERMAT'S LITTLE THEOREM (X.X), and the equation $x^2 = 1$ has just these two roots. Gauss similarly defined

$$\left(\frac{c + d\mathrm{i}}{a + b\mathrm{i}}\right)_4$$

to be i^k, for the unique choice of k modulo 4 for which

$$\mathrm{i}^k \equiv (c + d\mathrm{i})^{(a^2+b^2-1)/4} = (c + d\mathrm{i})^{(p-1)/4} \pmod{a + b\mathrm{i}}.$$

Here we say that two integers are congruent mod $a+b\mathrm{i}$ if their difference is a multiple of $a+b\mathrm{i}$ by a Gaussian integer. The existence of such k again follows from Fermat's little theorem: if you expand $(c+d\mathrm{i})^p$, then all the binomial coefficients are multiples of p apart from the first and the last, so you obtain $c^p+(d\mathrm{i})^p$, which equals $c+d\mathrm{i}$ by Fermat's theorem and the assumption that p is congruent to 1 mod 4; it follows that $(c+d\mathrm{i})^{p-1}\equiv 1$. (Alternatively, one can prove this by showing that the Gaussian integers mod $a+b\mathrm{i}$ form a group of order $p-1$ and applying Lagrange's theorem.)

Before stating the reciprocity law, we must stamp out the ambiguity in the choice of a, b, c, and d. We require that a and c must be odd, and that $a+b-1$ and $c+d-1$ must be divisible by 4. (Note that we can still flip the signs of b and d.)

Theorem (quartic reciprocity). *With p, q, a, b, c, and d as above, we have*

$$\left(\frac{a+b\mathrm{i}}{c+d\mathrm{i}}\right)\left(\frac{c+d\mathrm{i}}{a+b\mathrm{i}}\right)=-1$$

if p and q are both congruent to 5 modulo 8, and

$$\left(\frac{a+b\mathrm{i}}{c+d\mathrm{i}}\right)\left(\frac{c+d\mathrm{i}}{a+b\mathrm{i}}\right)=+1$$

otherwise.

One might expect to find an nth power reciprocity law that looks like this by working with the ring generated by a primitive nth root of 1. What complicates matters is that this ring does not enjoy the property of UNIQUE FACTORIZATION (X.X) (whereas the usual integers and the Gaussian integers both do). This was remedied only by KUMMER's (X.X) theory of IDEALS (X.X) (short for "ideal numbers"). An ideal is a set that has the typical properties of the set of all multiples of a given number, but it can be more general. (Even if an ideal *is* the set of all multiples of some number, that number is not unique, since one can multiply it by a unit. For instance, both 2 and -2 generate the ideal of all even numbers.) Using Kummer's theory, Kummer and Eisenstein managed to formulate broad generalizations of quadratic reciprocity for higher powers.

HILBERT (X.X) then realized that these should fit together as part of some sort of maximally general reciprocity law. He also gave a candidate for this law, inspired by a reformulation of quadratic reciprocity itself in terms of the *norm residue symbol*. For a prime p, and any nonzero integers m and n, the norm residue symbol $(\frac{m,n}{p})$ equals $+1$ if, for all sufficiently large k, the equations $mx^2+ny^2\equiv z^2 \pmod{p^k}$ have solutions where x, y, and z are not all divisible by p^k; otherwise the symbol equals -1. In other words, the symbol equals $+1$ if the equation $mx^2+ny^2=z^2$ has a solution in the p-ADIC NUMBERS (X.X).

Hilbert's formulation of quadratic reciprocity is that, for any nonzero m and n,

$$\prod_p\left(\frac{m,n}{p}\right)=1,$$

where the product is taken over all primes p *and the prime* $p=\infty$. The latter requires some explanation: we write $(\frac{m,n}{\infty})=+1$ if and only if m and n are not both negative, i.e., if the equation $mx^2+ny^2=z^2$ has a solution in the *real* numbers. This fits into a general pattern, that conditions quantified over "all prime numbers" must also account for the so-called infinite prime.

It should also be clarified that Hilbert's product only makes sense by virtue of the fact that, for fixed m and n, $(\frac{m,n}{p})=1$ for all but finitely many p. This is because in general, since approximately half the integers mod p^k are quadratic residues, it is easy to solve the equation $mx^2+ny^2=z^2$: difficulties arise only when multiplication by m or n identifies many of these quadratic residues. For instance, if m and n are (positive) prime numbers, then only those two primes contribute to the product; the two resulting factors can be related to $(\frac{m}{n})$ and $(\frac{n}{m})$, leading back to quadratic reciprocity.

Using this formulation, Hilbert was able to state and prove a form of quadratic reciprocity over any number field, in which the corresponding product of symbols is quantified over the prime ideals of the number field (together with some "infinite primes"). Hilbert also conjectured a higher-power reciprocity law over any number field. That conjecture was tackled by Hasse, Takagi, and finally ARTIN (X.X), who stated a general reciprocity law. Its statement is a bit too technical to include here; we limit ourselves to observing that Artin's reciprocity law, when applied to a number field K, describes certain norm residue symbols in terms of *Abelian* extensions of K, i.e., number fields containing K whose groups of symmetries (GALOIS GROUPS (X.X)) are commutative.

The Abelian extensions of $\mathbb{Q}$ are easy to describe: the Kronecker–Weber theorem asserts that they are all contained in fields generated by roots of 1. This explains the role of the roots of 1 in the classical reciprocity laws. However, describing the Abelian extensions of an arbitrary number field K is somewhat harder. They can

at least be classified in terms of the structure of the field K itself; this is what is commonly referred to as *class field theory*.

However, explicitly specifying generators of the Abelian extensions of K (Hilbert's twelfth problem) remains mostly unsolved, except in some special cases. For instance, the theory of ELLIPTIC FUNCTIONS (X.X) solves this problem for fields of the form $\mathbb{Q}(\sqrt{-d})$ with $d > 0$ via the theory of *complex multiplication*. Some additional examples emerged from the work of Shimura on modular forms, leading to the *Shimura reciprocity law*.

This last example shows that the story of reciprocity laws is not yet complete. Any new instance of explicit class field theory would reveal another reciprocity law that had previously been hidden from view. Some exciting new conjectures in this direction have been advanced by Bertolini, Darmon, and Dasgupta, who have proposed some new constructions of Abelian extensions using p-adic analysis. These are analogous to the aforementioned constructions using elliptic functions, in which one evaluates a transcendental function at a special value. At first, there seems to be no reason to expect the resulting complex number to have any special properties, but in fact it turns out to be an algebraic number that generates an appropriate Abelian extension of the base field. While one can check in individual examples, using computer calculations, that the construction seems to be converging p-adically to a particular generator of the right field, a proof seems out of reach at present.

Further Reading

Ireland, K., and M. Rosen. 1990. *A Classical Introduction to Modern Number Theory*, 2nd edn. New York: Springer.

Lemmermeyer, F. 2000. *Reciprocity Laws, from Euler to Eisenstein*. Berlin: Springer.