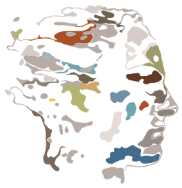


From quadratic reciprocity to Langlands' program

A major task in mathematics is to solve equations. Early sources, like the Rhind Papyrus, written around 1650 BCE by Ahmes, contains methods for solving linear equations. Rational numbers and complex numbers were created to solve certain equations. And still today, equations and their solutions in various number systems, continue to be an excellent source of new knowledge, in mathematics as well as in other scientific disciplins.

Finding integer solutions of equations is of particular interest to mathematicians. This problem is closely related to the many attempts at understanding the most basic mathematical object, the natural numbers; $\mathbb{N} = \{1, 2, 3, \dots\}$. The additive structure of the natural numbers is easily accessible; every positive integer is obtained from 1 by repeated addition. The multiplicative structure is more subtle. The prime numbers 2, 3, 5, , 7, . . . , which are the multiplicative basis for the natural numbers, are still hiding a lot of secrets; e.g. how to efficiently decide whether a given number is a prime or not.

A first attempt to decide whether a polynomial equation $P(x_1, \dots, x_n) = 0$ has an integer solution is to reduce the problem modulo m, i.e. look for solutions in the ring $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$ for various positive integers m. By using the **Chinese Remainder Theorem** this is equivalent to the problem of finding solutions modulo powers p^k, where p is a prime and $k \geq 1$. Solving the **congruence** (this is the technical term for an equation when we work modulo an integer)

$$P(x_1, \dots, x_n) \equiv 0 \pmod{p^k}$$

is called a "local" problem since we focus on one prime or "place" $p \in \mathbb{Z}$ at a time. The counterpart is a "global" problem, where we solve the equation over the integers $\mathbb{Z}$.

Kurt Hensel (1861-1941) reformulated the local problem i 1897 by introducing the **p-adic integers**;

$$\hat{\mathbb{Z}}_p = \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}$$

a construction which embraces all powers p^k, for $k \geq 1$. Hensel's reformulation says that solving the equation for any integer m is equivalent to solving the equation in the p-adic integers for all primes p. In addition to the prime solutions the existence of a solution over the real numbers $\mathbb{R}$ is of course a necessary condition in order to have a solution over $\mathbb{Z}$.

The p-adic integers is defined as an inverse limit, and has the corresponding "completion" topology. The topology can be defined via the **p-adic metric**;

Definition 1. *For a rational number*

$$q = \frac{p^\alpha m}{n}$$

where n and m are not divisible by p, the p-adic metric of q is given by

$$|q|_p = p^{-\alpha}$$

It follows that two natural numbers are p-close (i.e., with respect to the p-adic metric) if their difference is divisible by a high power of p. In this way 14 and 15 are not so 2-close since their difference is not divisible by any positive power of 2, while 31 and 63 with difference $63 - 31 = 32 = 2^5$ are much 2-closer.

We can localize $\hat{\mathbb{Z}}_p$ in the multiplicative set of non-zero elements to obtain the **p-adic numbers** $\hat{\mathbb{Q}}_p$. The real numbers $\mathbb{R}$ is the completion of the rational numbers $\mathbb{Q}$ with respect to the ordinary norm. We use the notation $|q|_\infty$ for this norm, and call $\mathbb{R}$ the completion of $\mathbb{Q}$ at the "infinite" prime, i.e. $\mathbb{R} = \hat{\mathbb{Q}}_\infty$.

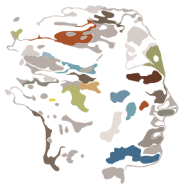
Each $\hat{\mathbb{Q}}_p$, $p \leq \infty$, is called a "local field", and $\mathbb{Q}$ itself a "global" field. The Hasse-Minkowski Theorem gives a positive example of the **local-global principle**: *A statement is valid over $\mathbb{Q}$ if and only if it is valid over all local fields $\hat{\mathbb{Q}}_p$ for $p \leq \infty$.*

Theorem 2 (Hasse-Minkowski)**.** *Let Q be a non-degenerate quadratic form. Then*

$$Q(x_1, \dots, x_n) = 0$$

has a non-trivial integer solution if and only if it has a real solution and a p-adic solution for every prime p.

Notice that the Hasse-Minkowski Theorem tells us something about quadratic polynomials. The result is not true for polynomials of higher degree. It was already known in 1909 that the Fermat equation $x^n +$



$y^n = z^n$ has p-adic solutions for all p. But as we now know, there are no non-trivial integer solutions.

Another example of an equation which is solvable locally, but not globally was found by **Ernst Selmer** (1920-2006) in 1951. It is given by the formula

$$3x^3 + 4y^3 + 5z^3 = 0$$

and Selmer showed that this equation can be solved modulo p for any prime p, as well as over $\mathbb{R}$, but there are still no solutions in $\mathbb{Z}$.

An innocent looking equation which has drawn a lot of attention throughout history is the quadratic equation

$$x^2 = d,$$

where d is a positive integer. The equation has an integer solution if and only if d is a perfect square.

Assume d is not a perfect square. Then by the Hasse-Minkowski Theorem we know that for some prime p the congruence

$$x^2 \equiv d \pmod{p^k}$$

fails to have a solution, i.e., for some prime power p^k the number d fails to be a **quadratic residue**. **Adrien-Marie Legendre** (1752-1833) reformulated this statement in a symbolic way:

Definition 3. *Let p be an odd prime and d an integer. The **Legendre symbol** $\left(\frac{d}{p}\right)$ is defined as*

$$\left(\frac{d}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv d \pmod{p} \text{ is solvable} \\ -1 & \text{if } x^2 \equiv d \pmod{p} \text{ is } \textbf{not} \text{ solvable} \\ 0 & \text{if } p \text{ divides } d \end{cases}$$

The Legendre symbol is multiplicative and p-periodic in the top argument. It can be shown that the symbols satisfy the **quadratic reciprocity law**:

Theorem 4. *Let p and q be two odd primes. Then*

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

The special value for the prime $p = 2$ is given by

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

The Legendre symbol can be computed by Euler's formula, introduced by **Leonhard Euler** (1707-1783) in 1748:

Theorem 5. *Let p be an odd prime and d an integer. Then we have*

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

An immediate and useful consequence of Euler's formula is the fact that

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Euler's criterion is easily proved using Fermat's little theorem,

$$d^{p-1} \equiv 1 \pmod{p}$$

Rewriting this as

$$(d^{\frac{p-1}{2}} - 1)(d^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$$

and using the fact that p is prime, we deduce that one of the factors has to be congruent to 0 (mod p). If d is a quadratic residue, i.e., $x^2 \equiv d \pmod{p}$ for some x, then

$$d^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$$

which makes the first factor equal to 0. Since the polynomial $x^2 - d$ has degree 2, it can have at most two roots, x and $-x$. Thus there are at least $\frac{p-1}{2}$ non-zero quadratic residues. On the other hand the polynomial

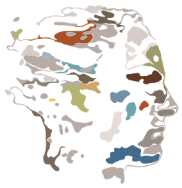
$$x^{\frac{p-1}{2}} - 1$$

can have at most $\frac{p-1}{2}$ non-zero roots. It follows that the remaining $\frac{p-1}{2}$ non-quadratic residue classes must be roots of the second factor, i.e., satisfying

$$d^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Thus we have $d^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$, depending on whether d is a quadratic residue modulo p or not.

A general framework for describing solutions of polynomial equations was introduced by **Évariste Galois** (1811-1832) in 1832, a few days before he



died from wounds suffered in a duel, only 20 years of age. Given a polynomial with integer coefficients, we can extend the rational numbers by the the solutions of the equation (found among complex numbers) to form a **field extension** E of the rational numbers $\mathbb{Q}$. Galois' idea was to consider automorphisms of the extended field fixing the rational numbers, and thereby fixing the polynomial itself. The set of such automorphisms forms a **group**, the so-called **Galois group** $G(E/\mathbb{Q})$ of the field extension. The Galois groups have a rich structure which reflects a lot of properties of the original polynomial equation; e.g., the Galois group is trivial if and only if the polynomial splits completely in linear factors with integer coefficients.

The equation $x^2 - d = 0$ has at most two roots, and the only possible non-trivial automorphism of $E = \mathbb{Q}(\sqrt{d})$ fixing $\mathbb{Q}$ is the conjugation map $\sigma : \sqrt{d} \mapsto -\sqrt{d}$. Thus the Galois group in this case is the unique group of two elements, $\mathbb{Z}_2 = \{Id, \sigma\}$ where $\sigma^2 = Id$.

The group $\mathbb{Z}_2$ also appears in an arithmetic context, namly as the multiplictaive group $(\mathbb{Z}_4)^* = \{1, 3\}$ of units in $\mathbb{Z}_4$. In this group 1 acts as the identity element, and 3 satisfies $3^2 \equiv 1 \pmod 4$. We define a map

$$\phi : (\mathbb{Z}_4)^* \to G(E/\mathbb{Q})$$

by $(p \pmod 4) \mapsto \left(\frac{d}{p}\right)$. The map is well-defined by Euler's criterion for all odd primes. It is in fact also a group homomorphism.

The map ϕ is called the **Artin map**, and the image $\phi_p := \phi(p)$ of a prime number p is called the **Frobenius element** of the Galois group $G(E/\mathbb{Q})$. The Frobenius element corresponds to the so-called **Frobenius map** of a finite field. Let E_p be an extension of the unique field $\mathbb{F}_p$ of order p. The Frobenius map is a map of E_p into itself. It is defined by $x \mapsto x^p$. Since E_p is an extension of $\mathbb{F}_p$ the Frobenius map defines a ring homomorphism. This follows from the fact that $p = 0$ in $\mathbb{F}_p$. For a so-called **unramified** field extension the Frobenius map can be lifted in a unique way from $G(E_p/\mathbb{F}_p)$ to $G(E/\mathbb{Q})$. The result of this lifting is the Frobenius element.

In $\mathbb{F}_p$, the Frobenius map is the identity map, by Fermat's little theorem. In the quadratic example, as treated above, we can compute $x \mapsto x^p$ for an element $v + w\sqrt{d} \in \mathbb{F}_p[\sqrt{d}]$. We have

$$\begin{aligned}(v + w\sqrt{d})^p &= v^p + w^p(\sqrt{d})^p \\ &= v + wd^{\frac{p-1}{2}}\sqrt{d}\end{aligned}$$

Thus we are interested in the value of $d^{\frac{p-1}{2}} \pmod p$. From Fermat's little theorem we have

$$0 = d^p - d = d \cdot (d^{\frac{p-1}{2}} - 1)(d^{\frac{p-1}{2}} + 1)$$

and since $\mathbb{F}_p$ is a field, one of the three factors must vanish. Our assumption that p does not divide $2d$ excludes the first factor, and we are left with the other two. For

$$d^{\frac{p-1}{2}} = 1,$$

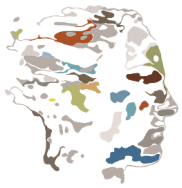
the Frobenius map is the identity, while for

$$d^{\frac{p-1}{2}} = -1,$$

the Frobenius map corresponds to the conjugation automorphism $\sigma : \sqrt{d} \mapsto -\sqrt{d}$. But we also have that the first case corresponds to d being a quadratic residue, the other one not. Also notice that when d is a quadratic residue, the polynomial $x^2 - d$ splits completely into linear factors.

Even if the Artin map in this example looks rather innocent, it reflects a deep connection between two objects of rather different origin; The Galois group of the equation on one side, and the arithmetic of $\mathbb{F}_p$ on the other.

In 1923 the Austrian mathematician **Emil Artin** (1898-1962) formulated what is now known as the *Artin's reciprocity law*. At first a conjecture, but a few years later he was able to give a proof. Artin's reciprocity law can be viewed as a generalization of the quadratic reciprocity law. In this generalization we consider more general field extensions of $\mathbb{Q}$, but limit ourselves to extensions E such that the Galois group $G(E/\mathbb{Q})$ is abelian. The corresponding generalization of the left hand side of the Artin map is the **adele ring**, introduced by **Claude Chevalley** (1909-1984) in the early 1950s. The adele ring is the so-called **restricted product** of all the completions $\hat{\mathbb{Q}}_p$, $p \leq \infty$, of the rational numbers. We can consider the adele ring as the collection of all local properties of the global field $\mathbb{Q}$.



Artin's reciprocity law gives a precise correspondence between an abelian field extension, i.e., a field extension such that the corresponding Galois group is abelian, and the adele ring. We may think of this correspondence as an example of the local-global principle, where Galois theory represents the global part and the adele ring the local part. In the above example the Galois group is cyclic of order 2 and $(\mathbb{Z}_4)^*$ is the corresponding quotient of the **idele class group**, which again is the group of units in the adele ring.

Artin's reciprocity law was further generalized by Robert P. Langlands, starting with the letter to **André Weil** in 1967. With Artin's treatment of the abelian case, it was natural to ask whether it was possible to extend the Artin map to non-abelian Galois groups. The question was far from irrelevant, just notice that already the splitting field of the polynomial $x^3 - 2$ has non-abelian Galois group over $\mathbb{Q}$. The answer to this problem was to introduce some sort of non-commutativity also on the "adele side" of the correspondence.

As a preparation for such an extension to a non-commutative setting, we can change our point of view of Artin's reciprocity law as a purely commutative theory. The key point is representation theory for groups, and the important fact that an abelian group is completely described by its 1-dimensional representations. Thus, instead of studying the group itself we consider the set of 1-dimensional representations $\rho : G \to \mathbb{C}^* = GL_1(\mathbb{C})$ of the group and nothing is lost. On the other hand, we replace the adele ring $\mathbb{A}$ by an appropriate quotient of $GL_1(\mathbb{A})$; the multiplicative group of units of $\mathbb{A}$.

Langlands' suggestion was to find a similar description of higher dimensional representations $\rho : G \to GL_n(\mathbb{C})$ of the non-abelian Galois groups. Such representations should correspond to representations of the group $GL_n(\mathbb{A})$ on an appropriate quotient of itself; the so-called **automorphic forms**. The described correspondence is now known as **Langlands' correspondence**.