Reciprocity Laws and Density Theorems

Richard Taylor [*]
Department of Mathematics,
Harvard University,
Cambridge,
MA 02138,
U.S.A.

August 29, 2007

1 Introduction

This article is a written version of my 2007 Shaw Lecture. It is meant to explain the related ideas of reciprocity laws (such as quadratic reciprocity and the Shimura-Taniyama conjecture) and of density theorems (such as Dirichlet's theorem and the Sato-Tate conjecture) to a general audience. I discuss these in the context of Diophantine equations, which have provided much of the historical motivation for reciprocity conjectures. There was significant overlap between my Shaw lecture and a talk I gave at the Akademie der Wissenschaften zu Göttingen in 2005 and hence this article is a somewhat extended version of [Tay1]. I see no point in writing something different just for the sake of it.

I was both surprised and extremely honoured to be awarded the 2007 Shaw Prize in Mathematics. It was a particular honour to share it with Bob Langlands, whose mathematics I so admire. I would like to take this opportunity to express my great gratitude to Sir Run Run Shaw and the Shaw Foundation.

Gauss called number theory the "queen of mathematics". Today it has become an extremely technical subject drawing on techniques from all over mathematics. Nonetheless it retains a particular beauty from the amazing interconnections that lie at the heart of the subject. In a short article I can

[*] Partially supported by NSF Grant DMS-0600716

only hope to illustrate some of this beauty through very specific examples. I can not explain the general setting we see for the subject.

Number theory can be thought of as having its roots in the study of Diophantine equations, that is polynomial equations with rational (or 'fractional') coefficients which we seek to solve while we insist that the solutions should again be rational numbers. Numbers like 1, $-1/2$, $3/17$, 6 are rational numbers, whereas numbers like $\sqrt{2}$, π and e are not.

The question of whether a given equation has solutions which are rational numbers turns out to be very subtle. It is a famous theorem, probably known to the Greeks by about 400BC, that $X^2 - 2 = 0$ has no solution in rational numbers. The parabola $Y = X^2 - 2$ cuts the X-axis in two points, which one can approximate as closely as one likes: $X = \pm 1.414213.....$ But how ever closely we approximate it, this will not tell us whether or not it is a rational number. Moreover if we displace the parabola a little, and considers, for instance, $Y = X^2 - 1.9881$, then the intercepts with the X-axis suddenly become the rational numbers: $X = \pm 141/100$.

In a similar vein the circle $X^2 + Y^2 = 1$ has infinitely many points with rational coordinates (for example $(X, Y) = (1, 0)$, $(3/5, 4/5)$, $(5/13, 12/13)$, $(9/41, 40/41)$,...). In fact the points with rational coordinates are everywhere dense on the circle. This was known to the Greeks, although a famous Babylonian tablet from before 1600BC contains a list of several rational points on this circle. On the other hand if one shrinks the circle a little bit, say to $X^2 + Y^2 = 0.999999$ then there are no rational points on this new circle!

Both these examples indicate that the existence of rational solutions to Diophantine equations is a subtle question certainly depending on much more than the size of the coefficients.

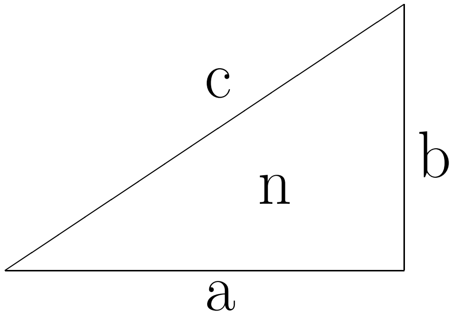
Let me consider one further example, to which I will return at the end of this article (see [Kob]). An Arab manuscript from before 972AD asks (a problem equivalent to): for which integers ('whole numbers') n is there a right angled triangle with area n whose sides have rational lengths? (See chapter XVI of [D].) Algebraically we are asked to solve the simultaneous equations:

$$a^2 + b^2 = c^2$$

and

$$ab = 2n$$

in positive rational numbers a, b, c. It is very hard to spot a pattern in the values of n for which such a triangle exists. No such triangle exists for $n = 1, 2, 3$ or 4. They do exist for $n = 5, 6$ and 7. The reader might like to try to find one for $n = 6$ and perhaps also $n = 5$ before coming to the end of this article.



It is convenient to reformulate this problem as one Diophantine equation in two unknowns. Some elementary algebra shows that the original problem about right angled triangles with area n is equivalent to solving the equation

$$Y^2 = X^3 - n^2 X$$

in non-zero rational numbers X, Y. (If (x, y) is a rational solution to this equation with $y \neq 0$, one can take $a = |n^2 - x^2|/|y|$, $b = |2nx|/|y|$ and $c = |n^2 + x^2|/|y|$.) It is harder, but still not very deep, to see that the equation $Y^2 = X^3 - n^2 X$ either has exactly three rational solutions (namely $(0, 0)$, $(n, 0)$ and $(-n, 0)$) or it has infinitely many. (Once you find one rational solution with $X \neq 0$, you can use it to generate infinitely many others.) Thus n is the area of a right angled triangle with rational sides if and only if the equation

$$Y^2 = X^3 - n^2 X$$

has infinitely many solutions in rational numbers.

Let me digress for a moment to remind the reader about prime numbers. A *prime* number is an integer greater than 1 which is divisible only by 1 and itself. Thus $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$ are prime numbers while $9 = 3 \times 3$ and $15 = 3 \times 5$ are not. It was already known to the Greeks that there are infinitely many prime numbers. Primes play a key role in number theory. They are the building blocks of all integers. Any positive integer can be written as a product of prime numbers, and this expression is unique in the sense that the number of times any prime occurs in this product is uniquely determined. For instance

$$1000000 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 5 \times 5 \times 5 \times 5 \times 5 \times 5$$

and

$$999999 = 3 \times 3 \times 3 \times 7 \times 11 \times 13 \times 37.$$

Unique factorisation into primes can be used to show that $X^2 = 2$ has no rational solutions. Indeed, if x were a rational solution we could write

$$x = \frac{p_1^{a_1}...p_r^{a_r}}{q_1^{b_1}...q_s^{b_s}},$$

where $p_1, ..., p_r, q_1, ..., q_s$ are distinct prime numbers and $a_1, ..., a_r, b_1, ..., b_s$ are positive integers. Then we would have

$$p_1^{2a_1}...p_r^{2a_r} = 2q_1^{2b_1}...q_s^{2b_s}.$$

The power of two on the left hand side is even, while the power on the right hand side is odd. This contradicts the unique factorisation into primes. (This proof can be simplified - one does not really require unique factorisation, only the distinction between odd and even numbers.)

2 Reciprocity Laws

We have many techniques for trying to solve Diophantine equations, or for trying to show no such solutions exist. One of the most elementary, but also one of the most powerful is the theory of congruences. Let me quickly review what we mean by congruences. Suppose that m is a non-zero integer. We call two integers a and b *congruent modulo* m if m divides the difference $a - b$. We write

$$a \equiv b \pmod{m}.$$

By a congruence class $[a]$ modulo m we mean the collection of all integers which are congruent to a modulo m. Thus there are m congruence classes modulo m, namely $[0]$, $[1]$, $[2]$, ..., $[m-1]$. (We have for instance that $[m] = [0]$ and $[m+1] = [1]$.) We denote by $\mathbb{Z}/m\mathbb{Z}$ the set of these congruence classes. The basic observation is that we can do arithmetic with congruence classes as well as we can with integers or rational numbers. For example we set

$$[a] + [b] = [a + b]$$

and

$$[a] - [b] = [a - b]$$

and

$$[a] \times [b] = [a \times b].$$

One has to check that these definitions make sense, i.e. that $[a+b]$, $[a-b]$, $[a \times b]$ do not depend on the choice of a and b in their respective congruence classes. But this is straightforward to do. Thus for example

$$5 + 6 \equiv 4 \pmod{7}$$

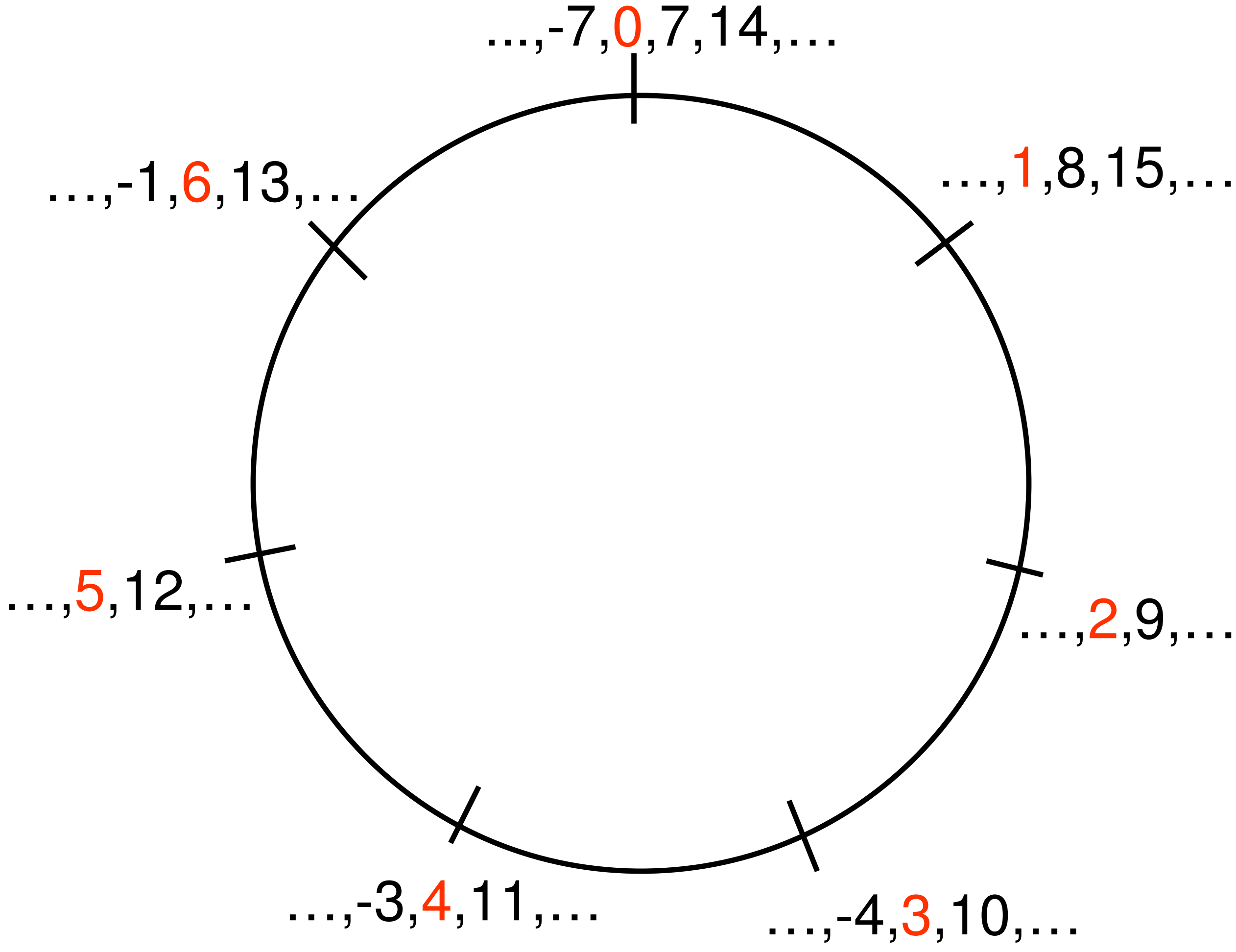
and

$$3 - 5 \equiv 5 \pmod{7}$$

and

$$3 \times 3 \equiv 2 \pmod{7}.$$

This is sometimes called 'clock arithmetic' as one can imagine the residue classes modulo m around the face of a clock with m hours. As you count you cycle back to zero when you get to m, just as after twelve o'clock you move back to one o'clock. Here is the 'clock' for arithmetic modulo 7:



You can also consider equations modulo m. For instance the equation

$$X^2 - 2 \equiv 0 \pmod{7}$$

has two solutions $X = 3$ or 4, while the equation

$$X^2 - 6 \equiv 0 \pmod{7}$$

has no solutions. You may like to quickly verify these facts. The latter fact also implies that $X^2 - 6 = 0$ has no solution in integers, for any solution in integers would give a solution modulo 7, and we have just checked there is no solution modulo 7. Of course there are other ways to see this (for example using unique factorisation into primes), but arguments along these lines are one of the basic ways that congruences can be applied to the study of Diophantine equations.

There is no reason to limit oneself to equations of one variable. The equation

$$Y^2 + Y \equiv X^3 - X^2 \pmod{7}$$

has exactly nine solutions:

$$(0,0), (0,6), (1,0), (1,6), (4,2), (4,4), (5,1), (5,5), (6,3).$$

You may like to compute the solutions modulo 2, 3, 5, 11 and 13. (You should find 4, 4, 4, 10 and 9 solutions respectively. Because of special symmetries in this equation the number you get is always congruent to -1 modulo 5 unless $p = 11$. This is not the sort of behaviour one would usually expect.)

You can easily verify that the equation

$$X^2 + Y^2 \equiv 3Z^2 \pmod{4}$$

has no solutions modulo 4 unless X, Y and Z are all even. This can be used to explain why

$$a^2 + b^2 = 0.999999$$

has no solutions in rational numbers a, b. If it did we can write $a = \alpha/\gamma$ and $b = \beta/\gamma$ where α, β, γ are integers with no common factor. They satisfy

$$1000000(\alpha^2 + \beta^2) = 999999\gamma^2.$$

Hence $\gamma = 1000\delta$ for some integer δ satisfying

$$\alpha^2 + \beta^2 = 999999\delta^2.$$

In particular

$$\alpha^2 + \beta^2 \equiv 3\delta^2 \pmod{4},$$

which as we have seen is impossible. Thus no such rational numbers a and b can exist.

Reciprocity laws concern the question:

If we fix an equation $f(X, Y, ..., Z)$ with integer coefficients, how does the number of solutions to

$$f(X, Y, ..., Z) \equiv 0 \pmod{p}$$

vary with the prime number p?

The prototype reciprocity law is Gauss' law of quadratic reciprocity, which concerns quadratic equations in one variable. This was first observed by Euler in 1783, but the first correct proof was found by Gauss in 1796. It is supposed to have been Gauss' favourite theorem ('theorema aureum'), and he liked it so much he found eight different proofs of it during his lifetime.

Let us first consider an example, the equation

$$X^2 + 7 \equiv 0 \pmod{p}.$$

Below I tabulate the solutions for the first twenty prime numbers, excluding 2 and 7 which behave a bit differently.

p	solutions
3	none
5	none
11	2,9
13	none
17	none
19	none
23	4,19
29	14,15
31	none
37	17,20

p	solutions
41	none
43	6, 37
47	none
53	24,29
59	none
61	none
67	23, 44
71	8,63
73	none
79	25,54

Can you see the pattern? If not perhaps the following table gives a hint?

p	$p \pmod 7$	# of solutions
3	3	0
5	5	0
11	4	2
13	6	0
17	3	0
19	5	0
23	2	2
29	1	2
31	3	0
37	2	2
41	6	0
43	1	2
47	5	0
53	4	2
59	3	0
61	5	0
67	4	2
71	1	2
73	3	0
79	2	2

It appears that there are no solutions if $p \equiv 3$, 5 or 6 modulo 7, while there are exactly two solutions if $p \equiv 1$, 2 or 4 modulo 7. Indeed this is true. It is a special case of Gauss' law of quadratic reciprocity.

Gauss' law of quadratic reciprocity: For any integer n and prime number p the number of solutions to

$$X^2 \equiv n \pmod p$$

depends only on p modulo $4n$.

It is not hard to see that the number of solutions is either 0, 1 or 2; and that 1 only occurs for the finite number of primes p which divide $4n$.

I would like to stress how surprising this theorem is to me. Why should the number of solutions to a congruence modulo p, have anything to do with which congruence class p lies in modulo something else? What have these two questions to do with each other? On the face of it, absolutely nothing.

I would also like to stress the power of this theorem. If you were asked how many solutions the congruence

$$X^2 \equiv -7 \pmod{32452843}$$

has, it would take a very long time to run through all the possibilities! (The number 32452843 is a prime.) However $32452843 = 1159030 \times 28 + 3$, so the law of quadratic reciprocity tells us that the number of solutions is the same as the number of solutions to

$$X^2 \equiv -7 \equiv 2 \pmod 3.$$

It is easy to check that this latter congruence has no solutions and hence $X^2 \equiv -7 \pmod{32452843}$ also has no solutions.

In the last two centuries Gauss' law has seen many generalisations. One of the great achievements of mathematics in the first half of the twentieth was the development of class field theory. Central to this is Artin's reciprocity law (1927), which can be seen as a generalisation of quadratic reciprocity to certain special ('abelian') higher order equations (in one variable). More recently attention has focused on other equations of one variable and on equations of several variables. Langlands has proposed very precise but complicated conjectures which would cover all equations in any number of variables, but we still seem to be a very long way from proving these.

For these questions the simplest non-trivial case of equations in more than one variable is the case of plane cubic equations, which (with little loss of generality) we can arrange to be in the form:

$$E : Y^2 + aY = X^3 + bX^2 + cX + d.$$

I will assume that this equation defines a smooth curve, i.e. that $64(b^2-3c)^3 \neq (27a^2 + 8b^3 - 36bc + 108d)^2$. So for fixed integers a, b, c, d and for a variable prime number p we want to consider the number of solutions to the congruence

$$Y^2 + aY \equiv X^3 + bX^2 + cX + d \pmod{p}.$$

I will write $N_p(E)$ for the number of such solutions. Hasse proved in 1933 that $N_p(E)$ was of the same order of magnitude as p. This is what one might guess if one supposed that for approximately half the p possible values for X there are two possibilities for Y, and that for approximately half there are no possibilities for Y. More precisely Hasse proved [H] that

$$|p - N_p(E)| \leq 2\sqrt{p}$$

(for all but the finitely many primes p, where E has bad reduction).

The Shimura-Taniyama conjecture, which has a complicated history, but evolved during the late 1950's and early 1960's, proposed a pattern to the ('error terms') $p - N_p(E)$ which amounts to a rule for efficiently computing them without checking lots of cases. It would be beyond the scope of this article to describe this algorithm precisely, but I will illustrate it, with a simple, although somewhat atypical, example. It is more complicated than quadratic reciprocity. It is *not* true that the number of points only depends on the congruence class of p modulo some number.

Consider the equation

$$Y^2 + Y = X^3 - X^2$$

and write N_p for the number of solutions to

$$Y^2 + Y \equiv X^3 - X^2 \pmod{p}.$$

I asked you to compute N_2, N_3, N_5, N_7, N_{11} and N_{13} above. I have tabulated a few values of p and $p - N_p$.

p	2	3	5	7	11	13	17	19	...
$p - N_p$	-2	-1	1	-2	1	4	-2	0	...

The Shimura-Taniyama conjecture suggests another way to compute these numbers: multiply out the following infinite product in an indeterminate q.

$$\begin{aligned} q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = q - \mathbf{2q^2} - \mathbf{q^3} + 2q^4 + \mathbf{q^5} + 2q^6 - \mathbf{2q^7} - 2q^9 - 2q^{10} \\ + \mathbf{q^{11}} - 2q^{12} + \mathbf{4q^{13}} + 4q^{14} - q^{15} - 4q^{16} - \mathbf{2q^{17}} + 4q^{18} + 2q^{20} + \ldots \end{aligned}$$

The number $p - N_p$ is just the coefficient of q^p in this expansion. Another apparently amazing coincidence.

In greater generality the values of $p - N_p(E)$ are not related to product expansions. Rather they arise from a study of subgroups of finite index in $SL_2(\mathbb{Z})$ and their action on the hyperbolic plane. $SL_2(\mathbb{Z})$ denotes the group of 2×2 integer matrices with determinant 1. These groups act as isometries on the hyperbolic plane, a non-standard geometry in which there are many lines through a given point parallel to a given line. This geometry provided the basis of Escher's 'circle limit' woodcuts.

This instance of the Shimura-Taniyama conjecture was known to Eichler [E], before the general conjecture was even formulated. Indeed it may have provided much of the motivation for the general conjecture. The full conjecture was finally proved in 2001 by Christophe Breuil, Brian Conrad, Fred Diamond and the author [BCDT], following on from key breakthroughs by Wiles [W] and by the author and Wiles [TW] in the early 1990s.

3 Density Theorems

Reciprocity theorems give us methods for efficiently calculating the number of solutions to a given equation modulo a variable prime number p. As well as asking for a method of calculation, one could ask about the distribution of the number of solutions as p varies. This is related to reciprocity, but not equivalent to it.

For instance given a whole number n, which is not the negative of a perfect square, one could ask for what proportion of prime numbers p does

$$X^2 + n \equiv 0 \bmod p$$

have no solutions, and for what proportion does it have two solutions? In 1837 Dirichlet showed that each of the two possibilities occurs for about half the primes. Dirichlet gave a slightly technical meaning to the phrase 'for about half the primes'. In 1896 de la Vallée-Poussin proved the more natural form of the theorem, which asserts that the ratios

$$\frac{\#\{p \leq t: \ X^2 + n \equiv 0 \bmod p \text{ has no solutions}\}}{\#\{p \leq t\}}$$

and

$$\frac{\#\{p \leq t: \ X^2 + n \equiv 0 \bmod p \text{ has two solutions}\}}{\#\{p \leq t\}}$$

(where p denotes a variable *prime* number) both tend to 1/2 as t tends to infinity. Both Dirichlet and de la Vallée-Poussin used Gauss' law of quadratic reciprocity, but they required additional analytic arguments.

Similar results are known for any equation involving just one variable. Let

$$f(X) = X^n + a_1 X^{n-1} + ... + a_{n-1}X + a_n$$

be a polynomial whose coefficients $a_1, ..., a_n$ are whole numbers. We say that f has degree n. For simplicity I will assume that f is *irreducible.* By this we mean that we can not write it as a product of two polynomials of smaller degree also having coefficients which are whole numbers. By an 1806 theorem of Argand we can write

$$f(X) = (X - \alpha_1)(X - \alpha_2)...(X - \alpha_n)$$

for some complex numbers $\alpha_1, ..., \alpha_n$. We need to consider the collection G of permutations (re-orderings)

$$\begin{array}{ccc} \alpha_1 & \longrightarrow & \alpha_{\sigma 1} \\ \alpha_2 & \longrightarrow & \alpha_{\sigma 2} \\ & \vdots & \\ \alpha_n & \longrightarrow & \alpha_{\sigma n} \end{array}$$

which preserve the algebraic relations between the α_i's, i.e. such that for any polynomial $F(X_1, ..., X_n)$ in n-variables with whole number coefficients with

$$F(\alpha_1, ..., \alpha_n) = 0$$

we also have

$$F(\alpha_{\sigma 1}, ..., \alpha_{\sigma n}) = 0.$$

The collection G plays a central role in modern number theory. It is called the Galois group of f, named for its inventor Evariste Galois (1811-1832). In 1880 Frobenius proved that the fraction of prime numbers p for which

$$f(X) \equiv 0 \bmod p$$

has exactly r solution modulo p is equal to the fraction of elements of G which fix exactly r of the $\alpha_1, ..., \alpha_n$. Frobenius used the same technical definition of 'fraction' that Dirichlet did, but de la Vallée-Poussin's methods allow one to restate the result more naturally:

$$\frac{\#\{p \leq t : \ f(X) \equiv 0 \bmod p \text{ has } r \text{ solutions}\}}{\#\{p \leq t\}}$$

(where p denotes a variable *prime* number) tends to

$$\frac{\text{number of elements of } G \text{ fixing exactly } r \text{ of the } \alpha_1, ..., \alpha_n}{\#G}$$

as t tends to infinity. It is striking that this goes beyond the reciprocity laws available even today, which are only known in the 'abelian case' (plus a few other isolated examples), and also predates them. In 1922 Cebotarev proved a significantly tighter version of Frobenius' theorem, which seems to be the last word in density theorems in the one variable case.

For example, consider the equation

$$X^4 - 2 = 0.$$

If $\sqrt[4]{2}$ denotes the positive real fourth root of 2 and if i denotes a square root of -1 then

$$X^4 - 2 = (X - \sqrt[4]{2})(X - i\sqrt[4]{2})(X + \sqrt[4]{2})(X + i\sqrt[4]{2}).$$

In this case it turns out that the collection G consists of all permutations of the set

$$\{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\}$$

which take the pair $\{\sqrt[4]{2}, -\sqrt[4]{2}\}$ either to itself or to the pair $\{i\sqrt[4]{2}, -i\sqrt[4]{2}\}$. (Note that the relation $\sqrt[4]{2} + (-\sqrt[4]{2}) = 0$ has to be preserved.) There are 8 such permutations. Of these 4 take $\{\sqrt[4]{2}, -\sqrt[4]{2}\}$ to $\{i\sqrt[4]{2}, -i\sqrt[4]{2}\}$ and fix no element of $\{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\}$. The other four take $\{\sqrt[4]{2}, -\sqrt[4]{2}\}$ to itself. Of these, one fixes all four elements of $\{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\}$; two fix two elements of this set; and one fixes none. Thus

$$\frac{\#\{p \leq t : \ X^4 - 2 \equiv 0 \bmod p \text{ has } 0 \text{ solutions}\}}{\#\{p \leq t\}} \longrightarrow 5/8$$

$$\frac{\#\{p \le t:\ X^4 - 2 \equiv 0 \bmod p \text{ has 1 solution}\}}{\#\{p \le t\}} \longrightarrow 0$$
$$\frac{\#\{p \le t:\ X^4 - 2 \equiv 0 \bmod p \text{ has 2 solutions}\}}{\#\{p \le t\}} \longrightarrow 1/4$$
$$\frac{\#\{p \le t:\ X^4 - 2 \equiv 0 \bmod p \text{ has 3 solutions}\}}{\#\{p \le t\}} \longrightarrow 0$$
$$\frac{\#\{p \le t:\ X^4 - 2 \equiv 0 \bmod p \text{ has 4 solutions}\}}{\#\{p \le t\}} \longrightarrow 1/8$$

as t goes to infinity.

Let us now turn to equations in several variables. Again the simplest case seems to be a (smooth) cubic equation in two variables of the form:

$$E : Y^2 + aY = X^3 + bX^2 + cX + d.$$

Both the number of solutions modulo p, which we are denoting $N_p(E)$, and the difference $p - N_p(E)$ are hard to compare as p varies. However by Hasse's theorem the ratio

$$\frac{p - N_p(E)}{2\sqrt{p}}$$

is always a real number between -1 and 1. One can ask how these normalised errors terms $(p - N_p(E))/2\sqrt{p}$ are distributed between -1 and 1 as p varies. There are a few special cases (the CM cases) with extra symmetries, for which there is a special answer. These special cases are rather rare and are much easier to understand. Thus, for the rest of this section, I will suppose that E is not CM. In this non-CM case Sato and Tate [Tat] independently conjectured in 1963 that the $(p - N_p)/2\sqrt{p}$ are distributed between -1 and 1 like

$$(2/\pi)\sqrt{1 - u^2}.$$

(One way to make this precise is to require that for any continuous function f on $[-1, 1]$, the average

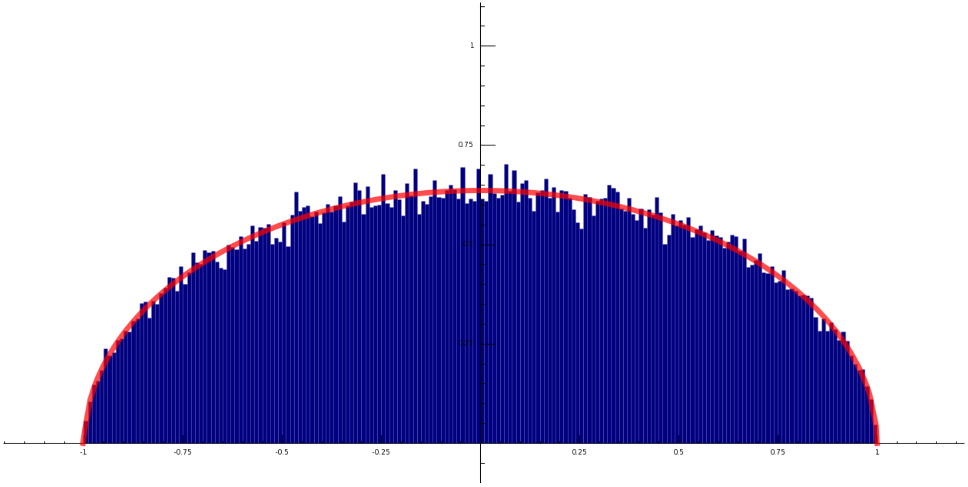
$$\#\{p \le t\}^{-1} \sum_{p \le t} f((p - N_p(E))/2\sqrt{p})$$

tends to

$$(2/\pi) \int_{-1}^{1} f(u)\sqrt{4 - u^2}du$$

as t tends to infinity.)

Below is a graph drawn by William Stein. It shows the distribution of the normalised errors for the modular form Δ with$p < 1,000,000$, as well as the the function $(2/\pi)\sqrt{1-u^2}$ for comparison. (Although Δ is not an elliptic curve, one expects exactly similar behaviour. I wasn't able to find a similarly nicely presented graph for an elliptic curve.)



Sato was led to the conjecture via numerical experiments, while Tate had heuristic reasons to believe it true. In 2006 Laurent Clozel, Michael Harris, Nick Shepherd-Barron and I [CHT], [HSBT], [Tay2] were able to verify the Sato-Tate conjecture in the case that the j-invariant

$$\frac{16^3(b^2-3c)^3}{16c^2(b^2-4c)+8b(a^2+4d)(9c-2b^2)-27(a^2+4d)^2}$$

is not an integer. (It should be possible to treat the general case in the same way, the only problems seem to be technical.)

Perhaps surprisingly reciprocity law for E (i.e. the Shimura-Taniyama conjecture) does not suffice to prove the Sato-Tate conjecture. Rather, as Tate had realised, it depends on knowing the reciprocity law for all the (infinitely many) self-products $E \times ... \times E$. Once one has these reciprocity laws the argument is much the same as that of Dirichlet and de la Vallée-Poussin. This seems to be a general phenomenon: density theorems follow from reciprocity theorems for arbitrary self products. (See the appendix to chapter I of [S].)

4 The Birch-Swinnerton-Dyer Conjecture

I will finish this article by considering a Diophantine application of the Shimura-Taniyama conjecture. Consider again the equation

$$E : Y^2 + aY = X^3 + bX^2 + cX + d.$$

Consider also the infinite product

$$L_0(E) = \sqrt{2}\omega_E^{-1} \prod_p \frac{p}{1 + N_p(E)},$$

where the product runs over all prime numbers p and where

$$\omega_E = \int_{x_0}^{\infty} dX/|2Y + a|$$

with x_0 is the largest real number such that $(X, Y) = (x_0, -a/2)$ satisfies the equation E. It is not known whether this product converges but it is presumed that it does. It follows from Hasse's theorem that at least $p/(1+N_p(E))$ tends to 1 as p tends to infinity. Note also that if $N_p(E)$ is large for lots of prime numbers p then $L_0(E)$ would tend to be small. One reason that $p/(1+N_p(E))$ might often be small could be that E has lots of solutions in rational numbers. In fact in 1965, Birch and Swinnerton-Dyer made the following remarkable conjecture [BSD]. (The first sentence of this conjecture is not in [BSD], but follows from conjectures in [BSD] in view of [G].)

Birch-Swinnerton-Dyer Conjecture (preliminary form): The product defining $L_0(E)$ converges to a rational number whose denominator can be explicitly bounded. The equation E has infinitely many solutions in rational numbers if and only if $L_0(E) = 0$.

It seems to be problematic to prove the convergence of the product defining $L_0(E)$, for reasons that have little bearing on the number theory of E. Thus it is conventional to 'regularise' the definition. More precisely for a complex number s consider the product

$$L(E, s) = \prod_p (1 - (p - N_p(E))p^{-s} + p^{1-2s})^{-1}.$$

This product converges for s a complex number with $\operatorname{Re} s > 3/2$ and defines a holomorphic function in this region. It is a consequence of the Shimura-Taniyama conjecture that this function has a unique analytic continuation to the whole complex plane. We define our regularised version of $L_0(E)$ by

$$L(E) = \omega_E^{-1} L(E, 1).$$

Because of the Shimura-Taniyama conjecture, this always makes sense. Moreover if $L_0(E)$ converges then $L(E) = L_0(E)$. (See [G]. Note that if we formally put $s = 1$ into the product defining $L(E, s)$ we would get

$$\prod_p \frac{p}{1 + N_p}.$$

However we actually believe that

$$L(E, 1) = \sqrt{2} \prod_p \frac{p}{1 + N_p}.\Bigg)$$

The Shimura-Taniyama conjecture, combined with a theorem of Faltings [F], in fact allows one to show that $L(E)$ is a rational number. We get the following alternative form of the Birch-Swinnerton-Dyer conjecture [BSD]:

Birch-Swinnerton-Dyer Conjecture: The equation E has infinitely many solutions in rational numbers if and only if $L(E) = 0$.

The only known method to get a handle on $L(E)$, indeed the only known method to show that it is well defined, is via the Shimura-Taniyama conjecture. This is typical in number theory. In general it seems that the only way to control expressions involving the number of points satisfying a given equation modulo all prime numbers is via reciprocity laws. Moreover those partial results we do have towards the Birch-Swinnerton-Dyer conjecture all depend on the Shimura-Taniyama conjecture combined with Faltings' proof of the Tate conjecture for elliptic curves [F]. For instance we have the following theorem of Gross and Zagier and of Kolyvagin [GZ], [Kol], [Ko2].

Theorem If $L(E) \neq 0$ then E has only finitely many rational solutions. If $L(E, s)$ has a simple zero at $s = 1$ then E has infinitely many rational solutions.

Now let us return to the congruence number problem. Recall that this asked: for which positive integers n is there a right angle triangle of area n and with rational side lengths? I have told you that it is not hard to see that such a triangle exists if and only if

$$E_n : \;\; Y^2 = X^3 - n^2 X$$

has infinitely many solutions in rational numbers. The Shimura-Taniyama conjecture has long been known for E_n. Tunnell [Tu] realised that one can use this to give a simple combinatorial formula for $L(E_n)$. For simplicity I will explain this in the case that n is odd. A similar formula exists for n even.

Define A_n^+ to be the number of integers α, β, γ such that

$$n = \alpha^2 + 2\beta^2 + 8\gamma^2$$

and γ is even. Similarly define A_n^- to be the number of integers α, β, γ such that

$$n = \alpha^2 + 2\beta^2 + 8\gamma^2$$

and γ is odd. Note that it is very easy to calculate $A_n^\pm$ because we only have to try a small number of possibilities for α, β and γ. For instance we must have $\gamma \leq \sqrt{n/8}$. You may like to calculate the following values of $A_n^\pm$ for yourself.

n	A_n^+	A_n^-
1	2	0
3	4	0
5	0	0
157	0	0

Tunnell showed that for n odd

$$L(E_n) = (A_n^+ - A_n^-)^2/8n^2.$$

Thus we have the following theorem and conjecture, which provide a (conjectural) answer to the congruent number problem.

Theorem If n is odd and $A_n^+ \neq A_n^-$ then there is no right angled triangle with area n and rational side lengths.

Conjecture If n is odd and $A_n^+ = A_n^-$ then there is a right angled triangle with area n and rational side lengths.

Thus there is no right angled triangle with rational side lengths and area 1 or 3. On the other hand we expect there are with area 5 or 157. Indeed this is the case. The simplest examples being, for $n = 5$, a triangle with sides

$$9/6, \;\; 40/6, \;\; 41/6;$$

and for $n = 157$ a triangle with sides

$$\frac{411340519227716149383203}{21666555693714761309610},$$

and

$$\frac{6803298487826435051217540}{411340519227716149383203},$$

and

$$\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}.$$

(This is due to Zagier, see [Kob].) I hope this latter example indicates that brute computational force is often insufficient for even simple Diophantine problems. A little theory, including suitable reciprocity laws, can be a great help.

References

[B] C. Boyer, *A history of mathematics*, Wiley 1968.

[BCDT] C. Breuil, B. Conrad, F. Diamond and R.Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), 843–939.

[BSD] B. Birch and P. Swinnerton-Dyer, *Notes on elliptic curves II*, J. Reine Angew. Math. 218 (1965), 79–108.

[CHT] L. Clozel, M. Harris and R. Taylor, *Automorphy for some l-adic lifts of automorphic mod l representations.*, submitted to Pub. Math. I.H.E.S. and available at `www.math.harvard.edu/~rtaylor`.

[D] L. Dickson, *History of the theory of numbers, II*, Chelsea Publ. Co. 1966.

[E] M. Eichler, *Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunction*, Arch. Math. 5 (1954), 355-366.

[F] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), no. 3, 349–366.

[G] D. Goldfeld, *Sur les produits partiels eulériens attachés aux courbes elliptiques*, C. R. Acad. Sci. Paris 294 (1982), 471–474.

[GZ] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. 84 (1986), 225-320.

[H] H. Hasse, *Beweis des Analogues der Riemannschen Vermutung für die Artinschen und F.K.Schmidtschen Kongruenzzetafunktionen in gewissen zyklisschen Fällen. Vorläufige Mitteilung.*, Nachr. Ges. Wiss. Göttingen I. Math.-Phys. Kl. Fachr. I Math. 42 (1933), 253-262.

[HSBT] M. Harris, N. Shepherd-Barron and R. Taylor, *A family of Calabi-Yau varieties and potential automorphy*, submitted to the Annals of Math. and available at `www.math.harvard.edu/~rtaylor`.

[Kob] N. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate Texts in Mathematics 97, Springer-Verlag, 1984.

[Kol] V.Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and Sha$(E, \mathbb{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), 522–540, 670–671.

[Ko2] V. Kolyvagin, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves*, in "Proceedings of the ICM (Kyoto, 1990)", Math. Soc. Japan, 1991.

[S] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, W.A.Benjamin 1968.

[Tat] J. Tate, *Algebraic cycles and poles of zeta functions*, in 'Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ. 1963)', Harper and Row 1965.

[Tay1] R. Taylor, *Reciprocity laws from Gauss to Langlands*, Jahrbuch der Akademie Wissenschaften zu Göttingen (2005), 152-165.

[Tay2] R. Taylor, *Automorphy for some l-adic lifts of automorphic mod l representations. II*, submitted to Pub. Math. I.H.E.S. and available at `www.math.harvard.edu/~rtaylor`.

[Tu] J. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. 72 (1983), 323-334.

[TW] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. 141 (1995), 553–572.

[W] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. 141 (1995), 443–551.