Congruent Numbers, Elliptic Curves, and the Passage from the Local to the Global

Chandan Singh Dalawat

The ancient unsolved problem of congruent numbers has been reduced to one of the major questions of contemporary arithmetic: the finiteness of the number of curves over Q which become isomorphic at every place to a given curve. We give an elementary introduction to congruent numbers and their conjectural characterisation, discuss local-to-global issues leading to the finiteness problem, and list a few results and conjectures in the arithmetic theory of elliptic curves.

Chandan Singh Dalawat was born in Bhitwara and now lives in Chhatnag. He would like to see more young people from diverse backgrounds take up mathematics and hopes that the world will make some place for them.

The area α of a right triangle with sides a, b, c (so that $a^2 + b^2 = c^2$) is given by $2\alpha = ab$. If a, b, c are rational, then so is α. Conversely, which rational numbers α arise as the area of a rational right triangle a, b, c ? This problem of characterising "congruent numbers" – areas of rational right triangles – is perhaps the oldest unsolved problem in all of Mathematics. It dates back to more than a thousand years and has been variously attributed to the Arabs, the Chinese, and the Indians.

Three excellent accounts of the problem are available on the Web : *Right triangles and elliptic curves* by Karl Rubin, *Le problème des nombres congruents* by Pierre Colmez, which also appears in the October 2006 issue of the *Gazette des mathématiciens*, and Franz Lemmermeyer's translation *Congruent numbers, elliptic curves, and modular forms* of an article in French by Guy Henniart. A more elementary introduction is provided by the notes of a lecture in Hong Kong by John Coates, which have appeared in the August 2005 issue of the *Quaterly journal of pure and applied mathematics*. A

Keywords
Congruent numbers, elliptic curves, Hasse principle, Birch and Swinnerton-Dyer conjecture, Shafarevich-Tate conjecture.

detailed account is to be found in *Introduction to elliptic curves and modular forms* (Springer, 1984) by Neal Koblitz. None of these sources goes beyond the theorems of John Coates and Andrew Wiles [1] (see Theorem 14) and of Jerrold Tunnell [2] (see Theorem 25).

In 1991, Rubin [3] (see Theorem 15) reduced the congruent number problem to a natural finiteness question in the arithmetic of elliptic curves (with "complex multiplications"). An excellent survey of such finiteness questions can be found in Barry Mazur's article [4].

This article consist of three parts of quite different nature. The first part is an elementary presentation of the problem of congruent numbers (§1) and its conjectural solution (§2); the material here is borrowed from the accounts which have been cited. The second part introduces local number fields (§3) and discusses the local-to-global principle – its validity in the case of conics (§4) and its failure in the case of cubics (§5) – in a language which can be understood by bright undergraduates. The last part, which requires greater mathematical maturity, is a catalogue of results – some old, some new – and conjectures in the arithmetic theory of elliptic curves in general (§6) and those without complex multiplications in particular (§7); it ends with a word about the role played by modular forms (§8).

1. Congruent Numbers

If a rational number α is the area of a right triangle with rational sides, then so is $\alpha\beta^2$ for every rational $\beta \in \mathbf{Q}^\times$. Indeed, if α is the area of a rational right triangle with sides a, b, c, then $\alpha\beta^2$ is the area of the rational right triangle with sides $a|\beta|, b|\beta|, c|\beta|$. So, up to replacing α by $\alpha\beta^2$ for a suitable β, we may assume that α is an integer, and moreover that α is not divisible by the square of any prime number. In other words, we assume that α is a positive squarefree integer.

Definition 1. *A squarefree integer $\alpha > 0$ is said to be a congruent number if there exist $a, b, c \in \mathbf{Q}$ such that $a^2 + b^2 = c^2$ and $ab = 2\alpha$.*

The terminology is classical and comes from the fact that α is congruent if and only if it is the common difference (*congruum*, in Latin) of a three-term arithmetic progression of rational squares. For if α is the area of a rational right triangle with sides $a < b < c$, then, putting $d = (c/2)^2$, the arithmetic progression $d - \alpha$, d, $d + \alpha$ consists of rational squares. Conversely, if there is a rational number d

such that $d - \alpha$, d, $d + \alpha$ are all three squares, then α is the area of the rational right triangle with sides $\sqrt{d+\alpha} - \sqrt{d-\alpha}$, $\sqrt{d+\alpha} + \sqrt{d-\alpha}$ and $2\sqrt{d}$.

The problem we address is that of deciding which numbers are congruent: we are asking for an easily-checked criterion which would tell us whether a given number is congruent or not.

Let us first study the single equation $a^2 + b^2 = c^2$ in strictly positive rational numbers; such a triple (a, b, c) wil be called a *rational solution* for short. Two rational solutions (a, b, c), (a', b', c') of this equation are called *equivalent* if $a = \lambda.a'$, $b = \lambda.b'$, $c = \lambda.c'$ for some $\lambda \in \mathbf{Q}^\times$ (necessarily positive). A rational solution is called *primitive* if $a, b, c \in \mathbf{Z}$, and if they have no common prime divisor. Every rational solution is equivalent to a primitive one, and no two primitive solutions are equivalent.

Reducing a primitive solution modulo 4, we see that precisely one of a, b is even.

Proposition 2. *Let (a, b, c) be a primitive solution of $a^2 + b^2 = c^2$, with $a = 2t$ even (and b, c odd). Then there exist integers $m > n > 0$, $\gcd(m, n) = 1$, $m \not\equiv n \pmod{2}$, such that*

$$a = 2mn, \quad b = m^2 - n^2, \quad c = m^2 + n^2. \tag{1}$$

Conversely, every such pair m, n of integers ($m > n > 0$, mutually prime, not of the same parity) gives rise via (1) to a primitive triangle a, b, c with a even (and b, c odd).

Proof : As b is odd, so is c. Hence $c + b$ and $c - b$ are even; write $c + b = 2u$ and $c - b = 2v$. If a number divides both u and v, it would divide their sum $u + v = c$ and their difference $u - v = b$. But $\gcd(b, c) = 1$, so we have $\gcd(u, v) = 1$. The relation $a^2 + b^2 = c^2$ implies that $t^2 = uv$, which shows that each of u, v must be a square. Let $m > n > 0$ be such that $u = m^2$, $v = n^2$; clearly, $\gcd(m, n) = 1$. Also, $m \not\equiv n \pmod{2}$ because $b = m^2 - n^2$ is odd.

Conversely, we have to show that the triangle a, b, c obtained from such a pair m, n is primitive. Now, 2 divides neither b nor c ; if a prime $p \neq 2$ divides both b and c, it would divide $c + b$ and $c - b$, hence u and v, and hence m and n.

Let C be a projective conic with a rational point O, for example the one defined by $a^2 + b^2 = c^2$, with $O = (1 : 0 : 1)$. Denoting by D the projective line of lines through O, the morphism f which sends a point $P \in C$ to the line $f(P) \in D$ passing through O and P – the tangent to C at O if $P = O$ – is an isomorphism.

This result allows us to generate a list which will eventually contain any given congruent number: it suffices to go through the list of all such pairs (m, n), compute the area $mn(m^2 - n^2)$ of the triangle (1), and take the 'squarefree part'. Thus the pair $(2, 1)$ shows that the number $6 = 2.1.(2^2 - 1^2)$ is congruent.

Retaining only the squarefree parts of the numbers produced by this procedure, the first few congruent numbers which show up are

$$5, 6, 7, 13, 14, 15, 21, 22, 23, 29, 30, 31, 34, 37, 38, 39, 41, \ldots \qquad (2)$$

Note that we have *not* proved that the numbers $1, 2, 3$ are not congruent; it may simply be that they haven't yet shown up on the list ! Indeed, Leonardo of Pisa (called Fibonacci) (1175–1240) was challenged to find a rational right triangle of area 5 (he succeeded) and he conjectured that 1 is not congruent; this was settled much later by Pierre Fermat (1601–1665).

How can we determine if a specific number such as 157 is congruent? The naïve approach, suggested by the discussion just after Definition 1, would be to go through a 'list' of squares d of rational numbers and to see if both $d - 157$ and $d + 157$ are squares. There is indeed such a 'list': first we go through the squares of the finitely many rational numbers whose numerator and denominator have just one digit, then through the squares of those – again finitely many – whose numerator and denominator have at most two digits, and so on. It turns out that the first square which works for 157, according to Don Zagier, is

$$d = \left(\frac{224403517704336969924557513090674863160948472041}{2 \times 8912332268928859588025535178967163570016480830}\right)^2 .$$

Clearly, this number could not have been found by the naïve approach; some theory is needed. Also, as before, this approach cannot prove that the given number, for example 1, is not congruent.

Theorem 3 (P Fermat $\sim$ 1640). *The number* 1 *is not congruent.*

Proof: We have to show that there is no rational right triangle whose area is a square. If there is such a triangle, we may assume, as before, that its sides are integers not all divisible divisible by any prime number. Fermat's idea of infinite descent consists in showing that if there were such a 'primitive' triangle whose area is a square, then there would be a smaller primitive triangle whose area is also a square. Clearly, this cannot go on for ever.

Let (a, b, c) be a primitive triangle whose area is a square. Assume that a is even (and b, c odd). Write $a = 2mn$, $b = m^2 - n^2$, $c = m^2 + n^2$, with $m > n > 0$, $\gcd(m, n) = 1$ and $m \not\equiv n \pmod{2}$ (Proposition 2). As the area $mn(m+n)(m-n)$ is a square, and as no two of the four factors have a common prime divisor, all four must be squares: $m = x^2$, $n = y^2$, $m + n = u^2$, $m - n = v^2$. Both u, v are odd because $m+n$, $m-n$ are odd, and $\gcd(u, v) = 1$. We also have $u^2 - v^2 = 2y^2$, which we rewrite as

$$2y^2 = (u + v)(u - v). \qquad (3)$$

As u, v are odd and $\gcd(u, v) = 1$, we have $\gcd(u + v, u - v) = 2$. So one of the two factors on the right in (3) must be of the form $2r^2$ and the other of the form $4s^2$. In any case, the sum of their squares is $16s^4 + 4r^4$. At the same time, $(u+v)^2 + (u-v)^2 = 2(u^2 + v^2) = 4m = 4x^2$. Comparing these two results, we get $4s^4 + r^4 = x^2$, which means that $(2s^2, r^2, x)$ is also an integral right triangle whose area $(rs)^2$ is a square. This triangle is smaller than our original triangle (a, b, c) because $x^4 = m^2 < m^2 + n^2 = c$; it may not be primitive, but the corresponding primitive triangle is even smaller.

The passage from the triple (a, b, c) to the triple $(2s^2, r^2, x)$ can be construed as *division* by ±2 on the elliptic curve $C_1 : y^2 = x^3 - x$; cf. the discussion before Exercise 7, and the beginning of § 6. The idea of the size of a triple leads to the notion of the *height* of a rational point on an elliptic curve.

Corollary 4. *The equation $x^4 - y^4 = z^2$ has no solutions in integers with $xyz \neq 0$.*

Proof: If there were a solution, the integral triangle $(2x^2y^2, x^4 - y^4, x^4 + y^4)$ would have square area $(xyz)^2$.

Corollary 5. *The equation $x^4 + y^4 = z^4$ has no solutions in integers with $xyz \neq 0$.*

Proof: If there were a solution, we would have $z^4 - y^4 = (x^2)^2$.

The system of equations ($a^2 + b^2 = c^2$; $ab = 2\alpha$) whose solvability in rational numbers characterises α as a congruent numbers can be changed into a single, more familiar, equation.

Proposition 6. *The integer α is congruent if and only if the equation*

$$C_\alpha : \alpha y^2 = x^3 - x \tag{4}$$

has a solution $x, y \in \mathbf{Q}$ with $y \neq 0$.

Proof: If (x, y) is such a solution, then the area of the rational right triangle $(2|x|, |x^2 - 1|, |x^2 + 1|)$ is α, up to a rational square (y^2). Conversely, let (a, b, c) be a rational right triangle and write

$$a = \lambda.2mn, \quad b = \lambda.(m^2 - n^2), \quad c = \lambda.(m^2 + n^2)$$

for some $\lambda \in \mathbf{Q}^\times$ and integers m, n as in Proposition 2. If the area of this triangle is α, we have $\alpha = \lambda^2.mn(m^2 - n^2)$, which means that (4) has the solution $x = m/n$ and $y = 1/\lambda n$.

From a given rational point $P = (x, y)$ $(y \neq 0)$ on C_α (4) we can generate infinitely many others : the tangent to C_α at the point P meets C_α at another rational point $P_1 = (x_1, y_1)$, and this process can be continued. It is not obvious, but it can be shown that this process does not terminate, essentially because it leads to points whose coordinates have more and more digits (cf. the discussion of torsion points on C_α, before Theorem 18).

Exercise 7. $(x_1, y_1) = \left(\dfrac{(x^2+1)^2}{4x(x^2-1)}, -\dfrac{x^6 - 5x^4 - 5x^2 + 1}{8\alpha^3 y^3} \right).$

This has an amusing consequence which is not at all obvious at the outset, and which goes back to Fermat:

Corollary 8. *If (a squarefree positive integer) α is congruent, then it is the area of infinitely many rational right triangles.*

Corollary 9. *A squarefree positive integer α is congruent if and only if the equation $\alpha y^2 = x^3 - x$ has infinitely many solutions $x, y \in \mathbf{Q}$.*

Here are the first few rational squares d such that both $d - 6$ and $d + 6$ are also squares:

$$\left(\frac{5}{2\times 1}\right)^2, \left(\frac{1201}{2\times 70}\right)^2, \left(\frac{7776485}{2\times 1319901}\right)^2, \left(\frac{2094350404801}{2\times 241717895860}\right)^2, \ldots$$

The morphism $y \mapsto \sqrt{\alpha}y$ shows that the curves C_1 and C_α become isomorphic over $\mathbf{Q}(\sqrt{\alpha})$; this is expressed by saying that C_α is a 'quadratic twist' of C_1. The problem of congruent numbers thus consists in characterising the quadratic twists of the fixed elliptic curve C_1 which have infinitely many rational points.

2. The Conjectural Solution

After these elementary observations, let us give the conjectural answer to the problem of characterising congruent numbers.

Recursively define the polynomial $g_r(T) = g_{r-1}(T)(1-T^{8r})(1-T^{16r})$, starting with $g_1(T) = T(1-T^8)(1-T^{16})$. Notice that $g_r(T) - g_{r-1}(T)$ is of degree $> 8r$, which means that the polynomials g_r and g_{r-1} have the same terms till degree $8r$. This implies that as $r \to +\infty$, the g_r tend to a formal series $g \in \mathbf{Z}[[T]]$.

Notation 10. *For $j = 1, 2$ and integer $n > 0$, define $c_j(n)$ as being the coefficient of T^n in the formal series $g(T)\theta_j(T)$, where*

$$g(T) = T\prod_{n=1}^{+\infty}(1-T^{8n})(1-T^{16n}) \quad \textit{and} \quad \theta_j(T) = 1 + 2\sum_{n=1}^{+\infty} T^{2jn^2}.$$

Notice that the numbers $c_j(n)$ are quite easy to compute. Here are the first few, for n odd and squarefree.

Table 11.

n	1	3	5	7	11	13	15	17	19	21	23	$\cdots$
$c_1(n)$	1	2	0	0	-2	0	0	-4	-2	0	0	$\cdots$
$c_2(n)$	1	0	2	0	0	-2	0	0	0	-4	0	$\cdots$

Exercise 12. *Let n be an odd squarefree integer. If $n \equiv 5, 7$ (mod. 8), then $c_1(n) = 0$. If $n \equiv 3$ (mod. 4), then $c_2(n) = 0$.*

For the remainder of this section, let α be a squarefree integer > 0, and write $\alpha = jn$, with $j = 1, 2$ and n odd.

Conjecture 13. *The number $\alpha = jn$ is congruent if and only if $c_j(n) = 0$.*

As we shall see, this conjecture is implied by Conjecture 24 (Birch and Swinnerton-Dyer), combined with Theorem 25 (Tunnell).

The reader should marvel at how unexpected the (conjectural) characterisation is, how far-removed from rational right triangles and their areas!

The physicist Richard Feynman claims in his *Surely you are joking* that he could guess whether a mathematical statement explained to him in elementary terms was true or false. It would have been interesting to have given him Definition 1 and Notation 10, and to have asked him if Conjecture 13 is true.

We do know one of the implications in Conjecture 13:

Theorem 14 (J Coates and A Wiles [1]). *If $c_j(n) \neq 0$, then $\alpha = jn$ is not congruent.*

It follows for example that the numbers $1, 2, 3, 10, 17, 19, 26$ and 42 (Table 11) are not congruent (cf. Theorem 3).

If the squarefree odd integer n is $\equiv 3 \pmod{4}$ (resp. $\equiv 5, 7 \pmod{8}$), then $2n$ (resp. n) should be congruent (Exercise 12, Conjecture 13), and the first few such n are indeed so (cf. (2)). In a paper which became influencial only when it was properly understood years after its publication, K Heegner proved that this is true if n is prime [5].

However, in general, the result is only conditional. It is conditional on the finiteness of a certain set S_α, which will be discussed in detail in later parts of this article (cf. Conjecture 16). Suffice it to say here that the finiteness of the set S_α is equivalent to the finiteness of the group $Ш(E_\alpha)$ which is more familiar to arithmeticians. We have chosen to formulate things in terms of the closely related set S_α because it can be defined in elementary terms.

Theorem 15 (K Rubin [3]). *If $c_j(n) = 0$ and if the set S_α is finite, then the number $\alpha = jn$ is congruent.*

Note that if $c_j(n) = 0$ and if S_α is finite, then Theorem 15 shows that α is congruent *without* exhibiting a rational right triangle of area α. However, in some cases ('rank 1'), the set S_α is known to be finite and there is a method ('Heegner points') for constructing such a triangle. Zagier's example showing that 157 is congruent, displayed before Theorem 3, is of this type. A method for explicitly constructing solutions in the 'higher rank' case would be a major advance.

3. Local Number Fields

We have seen (Theorem 15) that the problem of deciding whether a given (square-free) integer $\alpha > 0$ is congruent or not comes down to deciding if the set S_α – which we have mentioned but not yet defined – is finite or not. In order to define it, we first need to introduce K Hensel's local number fields.

The group $\mathbf{Q}^\times$, modulo its torsion subgroup $\{1, -1\}$, admits the set of prime numbers as a $\mathbf{Z}$-basis. For every prime number p, there is thus a unique homomorphism $v_p : \mathbf{Q}^\times \to \mathbf{Z}$ such that $v_p(p) = 1$ and $v_p(l) = 0$ for every prime number $l \neq p$; this defines a *discrete valuation* because, extending it to a map on the whole of $\mathbf{Q}$ by posing $v_p(0) = +\infty$, we have

$$v_p(x+y) \geq \inf(v_p(x), v_p(y)) \qquad \text{for all } x, y \in \mathbf{Q}.$$

Define $| \;|_p : \mathbf{Q} \to \mathbf{R}$ by $|x|_p = p^{-v_p(x)}$ (convention: $p^{-\infty} = 0$). Then $|x-y|_p$ is a *metric* on $\mathbf{Q}$ with respect to which it can be completed to obtain a field $\mathbf{Q}_p$ much in the same way as we obtain the field $\mathbf{R}$ from $\mathbf{Q}$ by completing it with respect to the usual metric $|x-y|_\infty = \sup(x-y, y-x)$. For this reason, the field of real numbers is sometimes denoted $\mathbf{Q}_\infty$.

It can be shown that the v_p (p prime) are the only discrete valuations, and $| \;|_\infty$ the only archimedean absolute value, on the field $\mathbf{Q}$ (A Ostrowski, 1918). Thus the absolute values $| \;|_p$ (p prime or $p = \infty$) determine all the *places* of $\mathbf{Q}$.

The fields $\mathbf{Q}_p$ (including $p = \infty$) play a fundamental role in arithmetic. It is always a good idea to first study 'global questions' – questions about rational numbers – everywhere 'locally' in the fields $\mathbf{Q}_p$, before trying to answer the original question. It is a good idea because questions become simpler over local number fields and can often be further reduced to questions over finite fields. Sometimes it suffices to consider just one local field, sometimes finitely many, sometimes all of them. In most cases, the local study is easy at almost all places. We discuss a basic example in the next section.

For p prime, the (locally compact) field $\mathbf{Q}_p$ comes equipped with a continuous discrete valuation extending v_p; elements of positive valuation form a (compact) subring $\mathbf{Z}_p$ ('the ring of integers') in which $p\mathbf{Z}_p$ is the unique maximal ideal; it consists of elements whose valuation is strictly positive. The quotient $\mathbf{Z}_p/p\mathbf{Z}_p$ ('the residue field') is the same as the finite field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ of p elements.

All books on Number Theory (Artin, Hasse, Weil, Serre, Kato–Kurokawa–Saito, ...) provide an introduction to the fields $\mathbf{Q}_p$ and their extensions.

4. The Local-to-Global Principle for Conics

To avoid speaking of curves, we use the equivalent language of a *function field* F over a field k: a finitely generated extension of k in which k is algebraically closed; we'll be mostly concerned with the case when F has transcendence degree 1 over k. Concretely, if $f \in k[x, y]$ is an absolutely irreducible polynomial – one which remains irreducible over every finite extension of k –, then the field of fractions F of the (integral) ring $k[x, y]/fk[x, y]$ is a function field over k; we write $F = k(x, y)$, with the relation $f = 0$. For every extension L of k, we then get a function field over L by 'extending the scalars' of F from k to L: the field of fractions of $L[x, y]/fL[x, y]$.

Let us fix an algebraic closure $\bar{\mathbf{Q}}$ of $\mathbf{Q}$. Clearly, the function field $\mathbf{Q}(x)$ becomes isomorphic to $\bar{\mathbf{Q}}(x)$ over $\bar{\mathbf{Q}}$. Are there any other function fields over $\mathbf{Q}$ which do? And, is there a way to classify them all?

Fix an algebraic closure $\bar{\mathbf{Q}}_p$ of $\mathbf{Q}_p$. The corresponding local question is: find all function fields over $\mathbf{Q}_p$ which become isomorphic over $\bar{\mathbf{Q}}_p$ to $\bar{\mathbf{Q}}_p(x)$. Such function fields will be called *solutions* to our problem.

The trivial solution to the problem is the rational function field $\mathbf{Q}_p(x)$. *It can be shown that there is precisely one other solution*; let us call it F_p. Thus the function field F_p is not the rational function field but becomes (isomorphic to) the rational function field over $\bar{\mathbf{Q}}_p$. For example, when $p = \infty$, the field F_∞ is $\mathbf{Q}_\infty(x, y)$ with the relation $x^2 + y^2 + 1 = 0$. When p is an odd prime, choosing an integer $u \notin p\mathbf{Z}$ which does not become a square in $\mathbf{F}_p^\times$, we may take F_p to be the function field over $\mathbf{Q}_p$ defined by the relation $ux^2 + py^2 - 1 = 0$. Over $\mathbf{Q}_2$, we may take F_2 to be the function field defined by $ux^2 + 2y^2 - 1 = 0$, where u is any odd integer such that $(u^2-1)/8$ is also odd. Moreover, for every place p, it is an easy matter to decide if a given 'local solution' is isomorphic to $\mathbf{Q}_p(x)$ or to F_p.

Now, if F is 'global solution' to our problem, then it is a 'local solution' everywhere. In other words, if F is a function field over $\mathbf{Q}$ which becomes the rational function field over $\bar{\mathbf{Q}}$, then F becomes isomorphic to one of $\mathbf{Q}_p(x)$, F_p over every completion $\mathbf{Q}_p$ of $\mathbf{Q}$, including $p=\infty$.

What can be shown is that every such F becomes isomorphic to $\mathbf{Q}_p(x)$ for almost every p, the places where it doesn't – there are thus only finitely many of them – are even in number, and, given any finite set Σ of places, even in number, there is a unique global solution which becomes isomorphic to F_p for all $p\in\Sigma$ and to $\mathbf{Q}_p(x)$ for all $p\notin\Sigma$.

There are many equivalent ways – curves of genus 0, quadratic forms in three variables, quaternion algebras – of expressing this principle.

It follows that if two global solutions F, F' are 'everywhere locally isomorphic' (become isomorphic to each other at every place p, including $p=\infty$), then they are $\mathbf{Q}$-isomorphic. This happy circumstance is expressed by saying that such function fields obey *the local-to-global principle.* (In fact, in the case at hand, it is sufficient to demand that F, F' be isomorphic at all places but one; they are then automatically isomorphic at the remaining place.)

The best accounts of this circle of ideas, in the equivalent language of quadratic forms, are to be found in Serre's *Course in arithmetic* and in *Number theory 1, Fermat's dream* by Kato, Kurokawa and Saito. A theorem of Adrien-Marie Legendre can be considered to be a precursor of local-to-global considerations, see Weil's *Number theory, an approach through history.*

I don't know of any classification of function fields over $\mathbf{Q}$ which become the 2-variable rational function field over every completion.

5. The Failure of the Local-to-Global Principle

In the last section we saw that the local-to-global principle holds for function fields over $\mathbf{Q}$ which become isomorphic over $\bar{\mathbf{Q}}$ to the rational function field. Such function fields are of the form $\mathbf{Q}(x,y)$, $ax^2+by^2=1$, for some $a,b\in\mathbf{Q}^\times$, and it is easy to decide when this field is isomorphic to the one defined by $a'x^2+b'y^2=1$ ($a',b'\in\mathbf{Q}^\times$), because it suffices to check that they are isomorphic everywhere locally. This is a finite amount of computation because for any odd prime p where all four numbers a, b, a', b' have valuation 0, the two function fields are automatically isomorphic to the rational function field $\mathbf{Q}_p(x)$.

In the early 1940s, Carl-Erik Lind and Hans Reichardt found the first examples of function fields which violate the local-to-global principle. Equivalently, Reichardt showed that $2y^2 = 1-17x^4$ has solutions in every completion of $\mathbf{Q}$ but no rational solutions – not even on the geometers' 'line at infinity in $\mathbf{P}_2$' (not to be confused with our 'place at infinity' ∞ of $\mathbf{Q}$).

Lind's thesis was reviewed by André Weil in the *Mathematical Reviews*, and it is amazing to note that he does not mention this discovery. Nor does the reviewer of Reichardt's paper, in spite of the explicit title: *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen.* It must be said that the first instance of the failure of a local-to-global principle, due to Hasse, was discovered by him after he had proved its validity for quadratic forms.

The most commonly cited example, originating with Ernst Selmer, is that of the function field $\mathbf{Q}(x, y)$, $3x^3 + 4y^3 + 5 = 0$. Cf. Example 27.

Let α be a squarefree integer > 0 and consider the function field $\mathbf{Q}(C_\alpha)$ defined by the equation $C_\alpha : \alpha y^2 = x^3 - x$. It may happen that there are many function fields F over $\mathbf{Q}$ which become isomorphic to $\mathbf{Q}(C_\alpha)$ at every place p of $\mathbf{Q}$. In other words, $\mathbf{Q}(C_\alpha)$ may have 'twisted forms' F which become isomorphic to it when we extend scalars of F and $\mathbf{Q}(C_\alpha)$ from $\mathbf{Q}$ to $\mathbf{Q}_p$. Let us denote the set of $\mathbf{Q}$-isomorphism classes of such F by S_α. This is the set which appears in Theorem 15.

Thus the problem of congruent numbers would be solved if we could settle the following conjecture, whose generalisation Conjecture 26 is a major open question in contemporary arithmetic.

Conjecture 16 (I Shafarevich and J Tate). *For every α, the set S_α – of $\mathbf{Q}$-isomorphism classes of function fields which become isomorphic to $\mathbf{Q}(C_\alpha)$ at every place – is finite.*

The more standard version of this conjecture asserts the finiteness of the *group* $Ш(E_\alpha)$, whose definition is more advanced. The reader who knows it should be able to prove that S_α is finite if and only if $Ш(E_\alpha)$ is finite [4]. The same remark applies to Conjecture 26.

We have seen that the congruent number problem amounts to the arithmetic study of the equation $\alpha y^2 = x^3 - x$, which can be rewritten as $y^2 = x^3 - \alpha^2 x$. The rest of this report is devoted to a rapid survey of the arithmetic of equations of the type $y^2 = f(x)$, where $f \in \mathbf{Q}[x]$ is a monic cubic polymonial with distinct roots (in $\bar{\mathbf{Q}}$).

6. Elliptic Curves: Results and Conjectures

In the next two sections, we enumerate some arithmetic properties of elliptic curves. For the sake of simplicity, we work over the field $\mathbf{Q}$; the only exceptions being a result over finite fields, one over $\mathbf{Q}_p$, and an example over $\mathbf{Q}(\sqrt{-1})$.

An *elliptic curve* E over a field k is a curve defined in the projective plane by (the homogenous version of) an equation of the type

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \quad (a_i \in k) \tag{5}$$

without singularities, a condition which says that the discriminant Δ – a certain polynomial in the a_i – is $\neq 0$, or equivalently that the corresponding function field is of 'genus 1', unlike the function fields which become isomorphic to $\bar{\mathbf{Q}}(x)$, which are of genus 0.

More precisely, the discriminant of f – the result of elliminating x, y from f, f'_x, f'_y – is

$$\Delta = -b_2^2b_8 - 2^3b_4^3 - 3^3b_6^2 + 3^2b_2b_4b_6,$$

where

$$b_2 = a_1^2 + 2^2a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 2^2a_6,$$

and

$$b_8 = b_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

The curve E has a 'point at infinity' O; for any extension L of k, there is a natural group law on the set $E(L)$ consisting of O and the solutions of (5) in L, uniquely determined by the requirement that O be the neutral element and that the sum of the three points (counted with multiplicity) in which E intersects a given line be O; the groups $E(L)$ are commutative. Associativity is not obvious, but follows from a classical result in plane projective geometry.

Elements of $E(L)$ can be identified with triples $(x, y, z) \neq (0, 0, 0)$ $(x, y, z \in L)$ satisfying the homogenised version of (5); two such triples being considered the same if each is a multiple of the other by an element of $L^{\times}$. The point O is the one with homogenous coordinates $(0 : 1 : 0)$. Two elliptic curves are said to be isomorphic if the corresponding function fields over k are k-isomorphic.

Let C be a smooth proper absolutely connected k-curve and let J be its jacobian – an abelian k-variety. If C has a k-rational point O, there is a unique k-morphism $C \to J$ sending a point P to the class of the divisor $P - O$. If moreover C has genus 1, then $C \to J$ is an isomorphism. Conversely, if (a smooth, proper, absolutely connected curve) k-curve C admits a group law, then C has genus 1 (and carries a rational point).

For surveys of arithmetic on elliptic curves, see Cassels [6] and Tate [7].

Theorem 17 (L Mordell, 1922). *For every elliptic curve E over $\mathbf{Q}$, the group $E(\mathbf{Q})$ is finitely generated.*

This result was conjectured by Henri Poincaré around 1900. Mordell's proof is a generalisation of Fermat's method of infinite descent – employed in the proof of Theorem 3 – ; its modern renditions consist of two parts.

The first part shows that the group $E(\mathbf{Q})/2E(\mathbf{Q})$ is finite. The second part studies a canonical real-valued 'height' function h on $E(\mathbf{Q})$, coming from the various absolute values of $\mathbf{Q}$, which measure how 'big' the coordinates of a point are. The method of infinite descent is distilled in the statement that a commutative group Γ, endowed with such a function h, for which $\Gamma/2\Gamma$ is finite, is necessarily finitely generated.

Accounts of the proof can be found in the books by Weil and Kato–Kurokawa–Saito cited above, as well as in Silverman–Tate, *Rational points on elliptic curves.*

Notice that the additive group $\mathbf{Q}$, the multiplicative group $\mathbf{Q}^{\times}$, and the 'elliptic' group $E(\mathbf{Q})$ differ from each other greatly in their structure. By contrast, the corresponding local result says that for an elliptic curve E over $\mathbf{R}$, the group $E(\mathbf{R})$ has a subgroup of index at most 2 isomorphic to $\mathbf{R}/\mathbf{Z}$, and, for an elliptic curve E over $\mathbf{Q}_p$ (p prime), $E(\mathbf{Q}_p)$ has a subgroup of finite index isomorphic to $\mathbf{Z}_p$. Thus, for an elliptic curve E over $\mathbf{Q}$, although the three groups $\mathbf{Q}$, $\mathbf{Q}^{\times}$, $E(\mathbf{Q})$ have very different structures, they are 'almost the same' everywhere locally.

For a given E over $\mathbf{Q}$, the torsion subgroup of $E(\mathbf{Q})$ is easy to determine (É Lutz); for example, the torsion subgroup of $C_\alpha(\mathbf{Q})$ consists of O and the three points $(-1,0)$, $(0,0)$, $(1,0)$ of order 2.

Theorem 18 (B Mazur [8]). *Let E be an elliptic curve over $\mathbf{Q}$. The torsion subgroup of $E(\mathbf{Q})$ is isomorphic to one of the fifteen groups*

$$\mathbf{Z}/m\mathbf{Z}\ (m = 1,2,\ldots,10,12), \quad \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\nu\mathbf{Z}\ (\nu = 1,2,3,4).$$

and each of these groups occurs as the tosrion subgroup of $E(\mathbf{Q})$ for infinitely many E.

No *uncondtional* method is known, however, for determining the rank of $E(\mathbf{Q})$ for a given E. The set of possible ranks for variable E (over $\mathbf{Q}$) is not known either, but N Elkies has recently produced examples where $\operatorname{rk} E(\mathbf{Q})$ is at least 28. We shall mostly concentrate on the question of deciding if the rank is 0 or > 0.

Let p be a prime number and let E be an elliptic curve over $\mathbf{Q}_p$, given by (5). We may assume by a change of variables that $a_i \in \mathbf{Z}_p$; the discriminant Δ is then in $\mathbf{Z}_p$. If the $a_i \in \mathbf{Z}_p$ can be so chosen that $\Delta \in \mathbf{Z}_p^\times$, we say that E has *good reduction* at p; if so, equation (5), read modulo p, defines an elliptic curve E_p – uniquely determined by E and p – over the finite field $\mathbf{F}_p$, and there is a homomorphism $E(\mathbf{Q}_p) \to E_p(\mathbf{F}_p)$ which sends a point to the reduction modulo p of any of its representatives $(x : y : z)$ with coordinates in $\mathbf{Z}_p$ and at least one coordinate in $\mathbf{Z}_p^\times$. Any given elliptic curve E over $\mathbf{Q}$ has good reduction at almost all primes because the defining equation (5) can be taken to have coefficients in $\mathbf{Z}$ and because the discriminant Δ has only finitely many prime factors.

There is a criterion for good reduction ('Néron-Ogg-Shafarevich'). Let $\bar{\mathbf{Q}}_p$ be an algebraic closure of $\mathbf{Q}_p$. There is a unique extension of v_p to a valuation $v_p : \bar{\mathbf{Q}}_p^\times \to \mathbf{Q}$ of which the residue field $\bar{\mathbf{F}}_p$ is an algebraic closure of $\mathbf{F}_p$. The *inertia group* is the kernel of the natural surjection $\operatorname{Gal}(\bar{\mathbf{Q}}_p|\mathbf{Q}_p) \to \operatorname{Gal}(\bar{\mathbf{F}}_p|\mathbf{F}_p)$; it acts on the m-torsion ${}_mE(\bar{\mathbf{Q}}_p)$ – the kernel of the multiplication by m – for every integer m.

Theorem 19 (J-P Serre and J Tate [9]). *An elliptic curve E over $\mathbf{Q}_p$ has good reduction if and only if the the action of the inertia group on ${}_mE(\bar{\mathbf{Q}}_p)$ is trivial for every m prime to p.*

One might ask to what extent E is determined by the the number $|E_p(\mathbf{F}_p)|$ of points modulo p for varying p. We say that two elliptic curves are *isogenous* if their function fields can be embedded into each other.

Theorem 20 (G Faltings [10]). *If E' is an elliptic curve over $\mathbf{Q}$ such that $|E'_p(\mathbf{F}_p)| = |E_p(\mathbf{F}_p)|$ for almost all primes p, then E' is isogenous to E.*

If two elliptic curves are isogenous, they have good reduction at the same primes (cf. Theorem 19). We might wish to fix a finite set T of primes and ask for a characterisation of all elliptic curves which have good reduction outside T – at every prime $p \notin T$. The first step is the following result:

Theorem 21 (I Shafarevich, 1962). *Given a finite set T of primes, there are only finitely many elliptic curves over $\mathbf{Q}$ having good reduction at every prime $p \notin T$.*

Another result of Shafarevich states that there are *no* elliptic curves over $\mathbf{Q}$ which have good reduction everywhere. This is an anlogue of Minkowski's theorem according to which there is no finite extension of $\mathbf{Q}$ (other than $\mathbf{Q}$ itself) which is everywhere unramified: the discriminant cannot be ± 1.

There is a sense in which the more fundamental quantity is not $|E_p(\mathbf{F}_p)|$ but $a_p(E)$, defined by $|E_p(\mathbf{F}_p)| = 1 - a_p(E) + p$, and there is sense in which the following theorem is the analogue, for function fields of elliptic curves over finite fields, of the famous Riemann Hypothesis: 'The zeros in the critical strip $0 < \mathrm{Re}(s) < 1$ of the zeta function ζ of $\mathbf{Q}$ have real part $\frac{1}{2}$'.

Theorem 22 (H Hasse, 1933). *Let A be an elliptic curve over a finite field k of q elements, and define a by $|A(k)| = 1 - a + q$. Then $|a| \leq 2\sqrt{q}$.*

Returing to our E over $\mathbf{Q}$, Birch and Swinnerton-Dyer argued that if $E(\mathbf{Q})$ is infinite, the groups $E_p(\mathbf{F}_p)$ (for p a prime of good reduction for E) should have more elements 'on the average' than if $E(\mathbf{Q})$ is finite. In view of Hasse's theorem, the product $\prod_p \frac{p}{|E_p(\mathbf{F}_p)|}$ should diverge to 0 if the rank is > 0, and converge to a limit $\neq 0$ if the rank is 0. This is made precise in terms of the L-function of E.

For a prime p of good reduction for E, we have the number $a_p(E)$; for 'cohomological' reasons, consider the infinite product (for $s \in \mathbf{C}$)

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

Theorem 22 implies that this converges for $\mathrm{Re}(s) > \frac{3}{2}$, but more is true:

Theorem 23 (A Wiles, R Taylor, F Diamond, B Conrad, C Breuil, 1995–2000). *The function $L(E,s)$ admits an analytic continuation to the whole of* $\mathbf{C}$.

For the congruent number elliptic curves C_α, this is due to André Weil. There is a way of introducing factors in $L(E,s)$ corresponding to the primes which divide Δ, and indeed to the place ∞. This 'completed' L-function $\Lambda(E,s)$ has a 'functional equation' for $s \mapsto 2-s$, just as the ζ-function, when 'completed', has a functional equation for $s \mapsto 1-s$.

Note that the product $\prod_p \frac{p}{|E_p(\mathbf{F}_p)|}$ is formally equal to $L(E,1)$. The above heuristic considerations and extensive calculations on one of the first electronic computers at Cambridge led to the following conjecture.

Conjecture 24 (B Birch and P Swinnerton-Dyer, 1965). *The group $E(\mathbf{Q})$ is infinite if and only if $L(E,1) = 0$. More precisely, its rank equals the order of vanishing of $L(E,s)$ at $s = 1$.*

The order of vanishing of the completed L-function $\Lambda(E,s)$ is the same as that of $L(E,s)$ at $s = 1$. There is a refined version of Conjecture 24 which gives the leading coefficient of $\Lambda(E,s)$ at $s = 1$ in terms of the local and global arithmetic invariants of the curve E; its formulation is subject to the truth of Conjecture 26.

Conjecture 13 follows from Conjecture 24, thanks to the following criterion:

Theorem 25 (J Tunnell [2]). *For a squarefree integer $\alpha = jn$ ($j = 1,2$ and n odd), one has $L(C_\alpha, 1) = 0$ if and only if $c_j(n) = 0$.*

The elliptic curve E has the function field $\mathbf{Q}_l(E)$ at the various places l of $\mathbf{Q}$. Just as we did in the case of the congruent number elliptic curves C_α, we now consider the set S_E of (isomorphism classes of) all function fields over $\mathbf{Q}$ which becomes isomorphic to $\mathbf{Q}_l(E)$ at every place l; of course, $\mathbf{Q}(E)$ belongs to S_E.

Conjecture 26 (I Shafarevich and J Tate). *For every elliptic curve E over $\mathbf{Q}$, the set S_E is finite.*

The original conjecture asserts the finiteness, for every E over $\mathbf{Q}$, of the *group* $Ш(E)$ of 'torsors' under E which are 'everywhere locally trivial'. This is equivalent to the finiteness of S_E.

Yuri Manin has introduced an 'obstruction' to explain the failure of the local-to-global principle for the function field $\mathbf{Q}(E)$ of an elliptic curve E over $\mathbf{Q}$. He shows that the finiteness of S_E is equivalent to his obstruction being the only one.

The equation $x^3+y^3+60=0$ can be put in the form (5) by a change of variables; it therefore defines an elliptic curve.

Example 27 (B Mazur [4]). *For E defined by $x^3+y^3+60=0$, the set S_E consists of $\mathbf{Q}(E)$ and the function fields defined by*

$$3x^3+4y^3+5, \quad 12x^3+y^3+5, \quad 15x^3+4y^3+1, \quad 3x^3+20y^3+1.$$

The best available result in the direction of Conjectures 24 and 26 to date, the fruit of a succession of papers by numerous mathematicians, is a theorem of Victor Kolyvagin, of which the theorem of Coates and Wiles (Theorem 14) is a particular case, and which subsumes some of the results of Benedict Gross and Don Zagier [11].

Theorem 28 (V Kolyvagin [12]). *If $L(E,1)\neq 0$, then $E(\mathbf{Q})$ is finite. If $L(E,s)$ has a simple zero at $s=1$, then $E(\mathbf{Q})$ has rank 1. In both these cases, the set S_E is finite.*

If the zero at $s=1$ has multiplicity >1, Conjecture 26 is needed (Cf. Theorem 15):

Theorem 29 (C Skinner and É Urban [13]). *Suppose that $L(E,1)=0$ and that the set S_E is finite. Then the group $E(\mathbf{Q})$ is infinite.*

There is a parallel theory of elliptic curves E over function fields F over finite fields. The analogue of Mordell's theorem (Theorem 17) is true: the group $E(F)$ is finitely generated. K Kato and F Trihan [14] have proved the analogue of (the refined version of) the Birch and Swinnerton-Dyer conjecture (Conjecture 24), subject to the truth of the analogue of the Shafarevich-Tate conjecture (Conjecture 26).

The study of 'special values' of L-functions, of which the refined conjecture of

Birch and Swinnerton-Dyer is the prototype, is one of the major themes of contemporary arithmetic. This is a very active area in which P Deligne, S Bloch, A Beilinson, K Kato, J-M Fontaine, B Perrin-Riou, among others, have made seminal contributions.

7. Complex Multiplications

Let E be an elliptic curve over $\bar{\mathbf{Q}}$, defined by an equation $f(x,y)=0$. Because E has a group law, there are many embeddings of the function field $\bar{\mathbf{Q}}(E)=\bar{\mathbf{Q}}(x,y)$ into itself: for every integer $n \neq 0$, there is an embedding $[n]_E$ which sends x,y to x_n, y_n, the coordinates of the multiple nP of the point $P=(x,y)$; the embedding $[n]_E$ is of degree n^2. For example, when E is the congruent number elliptic curve C_α (4) and $n=-1$, it is the automorphism $x \mapsto x$, $y \mapsto -y$ of the function field; when $n=-2$, it is the degree-4 embedding given in Exercise 7.

In a sense, for most elliptic curves, these are the only embeddings of the function field into itself. But there are some elliptic curves for which there are more embeddings, for example the automorphism $x \mapsto -x$, $y \mapsto iy$ (i being a chosen square root of -1) of $\bar{\mathbf{Q}}(C_\alpha)$ whose square is $[-1]_{C_\alpha}$. In such a case we say that the elliptic curve E has 'complex multiplications'; it then determines an imaginary quadratic field K, the field of fractions of the ring of $\bar{\mathbf{Q}}$-endomorphisms of E. In the case of the curves C_α, it is $\mathbf{Q}(i)$. We say that E has complex multiplications by K.

The arithmetic properties of elliptic curves differ vastly according as they have complex multiplications or not. For example, for elliptic curves having complex multiplications, the theorem '$L(E,1) \neq 0 \Rightarrow E(\mathbf{Q})$ is finite' was proved by Coates-Wiles (cf. Theorem 14) a good eleven years before Kolyvagin's general result (cf. Theorem 28); the analytic continuation of $L(E,s)$ was proved by Weil and Max Deuring in 1953–1957, much before the general result of Wiles and his school in 1995–2000 (Theorem 23); the implication '$L(E,1)=0$ and S_E finite $\Rightarrow$ $E(\mathbf{Q})$ infinite' was proved by Rubin (cf. Theorem 15) some fifteen years before the general result of Skinner–Urban (Theorem 29).

We illustrate the differences by three examples. For the first, recall that an elliptic curve A over $\mathbf{F}_p$ is called *supersingular* if the p-torsion ${}_pA(\bar{\mathbf{F}}_p)$ is reduced to $\{O\}$, or, equivalently for $p \neq 2,3$, if $|A(\mathbf{F}_p)| = 1+p$ (equivalently, $a=0$, in the notation of Theorem 22). Returning to our E over $\mathbf{Q}$, we ask: How often is

E_p supersingular? Deuring showed if E has complex multiplications, then this happens for half the primes p (cf. Example 33); if not, Serre proved that the set of supersingular primes has density 0. That it is infinite is a relatively recent result.

Theorem 30 (N Elkies [15]). *For every elliptic curve E over $\mathbf{Q}$, there are infinitely many primes p at which E_p is supersingular.*

For the second example, recall that for every prime p, if we adjoin the p-torsion of the multiplicative group $\bar{\mathbf{Q}}^\times$, which consists of pth roots of 1, to $\mathbf{Q}$, we get a galoisian extension $\mathbf{Q}({}_p\mu)$ whose group of automorphisms is $\mathrm{Gal}(\mathbf{Q}({}_p\mu)|\mathbf{Q}) = GL_1(\mathbf{F}_p)$. For an elliptic curve E over $\mathbf{Q}$, the p-torsion of $E(\bar{\mathbf{Q}})$ is a 2-dimensional vector $\mathbf{F}_p$-space; if we adjoin it to $\mathbf{Q}$, we get a galoisian extension $\mathbf{Q}({}_pE)$. What is $\mathrm{Gal}(\mathbf{Q}({}_pE)|\mathbf{Q})$?

Theorem 31 (J-P Serre [16]). *Suppose that E does not have complex multiplications. Then the group of automorphisms of $\mathbf{Q}({}_pE)$ is $GL_2(\mathbf{F}_p)$ for almost all – all but finitely many – primes p.*

The corresponding local result for E over $\mathbf{Q}_l$ says, at least in the case of good reduction, that $\mathrm{Gal}(\mathbf{Q}_l({}_pE)|\mathbf{Q}_l)$ is cyclic for $l \neq p$ (cf. Theorem 19).

If E (over $\mathbf{Q}$) has complex multiplications, the group of automorphisms is much smaller: if K – an imaginary quadratic field – is the field of complex multiplications, then $K({}_pE)$ is an abelian extension of K. However, such E serve a different, if related, purpose.

Recall that the theorem of Kronecker–Weber asserts that *if we adjoin the entire torsion subgroup of $\bar{\mathbf{Q}}^\times$ – all roots of 1 – to $\mathbf{Q}$, we get its maximal abelian extension.* Generating the maximal abelian extension of other number fields is a major open problem (Kronecker's *Jugendtraum*, Hilbert's Problem 12); the theory of complex multiplications provides the answer in the case of imaginary quadratic fields, as in the next example.

Example 32. *Let E be the elliptic curve $y^2 = x^3 + x$, which has complex multiplications by $\mathbf{Q}(i)$ ($i = \sqrt{-1}$). If we adjoin the entire torsion subgroup of $E(\bar{\mathbf{Q}})$ to $\mathbf{Q}(i)$, we get its maximal abelian extension.*

Our third example concerns a 'formula' for $a_p(E)$ for a fixed E and varying p.

There is indeed such a formula if E has complex multiplications, as illustrated by a theorem of Gauss about the curve $x^3 + y^3 + 1 = 0$ (which can be put in the canonical form (5), and has complex multiplications by $\mathbf{Q}(\zeta_3)$, where ζ_3 is a primitive cube root of 1). It uses the fact that for a prime $p \equiv 1 \pmod{3}$, there is a pair of integers (c_p, d_p), unique up to signs, such that $4p = c_p^2 + 27d_p^2$; to fix the sign of c_p, assume that $c_p \equiv -1 \pmod{3}$.

Exmaple 33 (C Gauss, 1801). *Let E be the elliptic curve $x^3+y^3+1 = 0$ and p a prime. If $p \equiv 1 \pmod{3}$, then $a_p(E) = c_p$. If $p \equiv -1 \pmod{3}$, then $a_p(E) = 0$.*

See Silverman–Tate for a proof. Note that this implies Theorem 22 for E.

By contrast, if E does not have complex multiplications, the behaviour of the $a_p(E)$ is entirely different. Mikio Sato and John Tate independently arrived at a conjectural distribution law for $\gamma_p(E) = a_p(E)/2\sqrt{p}$, which lies between -1 and $+1$ for every p (cf. Theorem 22). How often does it lie in $[\beta, \delta] \subset [-1, +1]$?

Conjecture 34 (M Sato and J Tate, 1960). *Suppose that E does not have complex multiplications, and let $[\beta, \delta] \subset [-1, +1]$ be an interval. Then the proportion of primes p for which $\gamma_p(E) \in [\beta, \delta]$ is given by*

$$\frac{2}{\pi}\int_\beta^\delta \sqrt{1 - x^2}\, \mathrm{d}x.$$

This conjecture has been proved, subject to a mild technical hypothesis on E, by Laurent Clozel, Michael Harris, Nicholas Shepherd-Barron and Richard Taylor in a series of three papers in early 2006. The technical hypothesis demands that E have 'multiplicative reduction' at some prime p, which means roughly that the best possible reduction at p is not an elliptic curve E_p as in the case of good reduction, but the multiplicative group (and not the additive group – the third possibility). An algorithm due to Tate allows one to determine the type of reduction at any given p in terms of the coefficients a_i (5) defining E. Concretely, although we cannot choose $a_i \in \mathbf{Z}_p$ with minimal $v_p(\Delta)$ so as to have $v_p(\Delta) = 0$, they can be so chosen as to have $v_p(c_4) = 0$, where $c_4 = b_2^2 - 2^3.3.b_4$, and the b_i are displayed after equation (5). It is only a matter of time before this hypothesis is removed.

Theorem 35 (L Clozel, M Harris, N Shepherd-Barron and R Taylor [17]). *Conjecture 34 is true if E has multiplicative reduction at some prime p.*

8. Modular Forms

We have not mentioned them, although they have appeared in these notes without being named. If we evoke them here, it is only to say that most of the spectacular recent results which we have enumerated would not have been possible without their help. Take the analytic continuation of $L(E, s)$ (Theorem 23): the crucial result (Wiles and others) is to show that the sequence $(a_p(E))_p$ defines a modular form.

Results of Gross–Zagier and of Kolyvagin (Theorem 28), which predate Wiles, were enunciated only for those elliptic curves whose L-functions have this modulariy property; thanks to Wiles and his successors, we now know that they all have.

Mazur's determination of the possible torsion subgroups (Theorem 18) involves the study of *modular curves*, which are intimately related to modular forms.

Tunnell's criterion (Theorem 25) is actually an expression for $L(C_\alpha, 1)$ in terms of (the 'real period' of C_1 and) the coefficients $c_j(n)$ of certain modular forms of half-integral weight (cf. Notation 10).

The role of *automorphic forms* – a generalisation of modular forms – is even greater in the results of Skinner–Urban (Theorem 29) and in the proof of the Sato–Tate conjecture (Theorem 34). It is unlikely to diminish in the future: more and more L-functions are going to become automorphic, fulfilling the prophetic vision of Robert Langlands [18].

For a first introduction, apart from Serre's *Course*, see the book by Koblitz and Knapp's *Elliptic curves.*

Acknowledgements

I thank Pete Clark for a very careful reading of the manuscript, and for his suggestions for improvement.

Suggested Reading

[1] John Coates and Andrew Wiles: On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.*, Vol. 39, No.3, pp.223–251, 1977.

[2] Jerrold Tunnell: A classical Diophantine problem and modular forms of weight 3/2, *Invent. Math.*, Vol.72, No.2, pp.323–334, 1983.

[3] Karl Rubin : The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Invent. Math.*, Vol.103, No.1, pp.25–68, 1991.

[4] Barry Mazur : On the passage from local to global in number theory, *Bull. Amer. Math. Soc*. (N.S.), Vol.29, No.1, pp.14–50, 1993.

[5] Kurt Heegner : Diophantische Analysis und Modulfunktionen, *Math. Z*. Vol.56, pp.227–253, 1952.

[6] John Cassels: Diophantine equations with special reference to elliptic curves, *J. London Math. Soc*., Vol.41, pp.193–291, 196

[7] John Tate : The arithmetic of elliptic curves, *Invent. Math*. Vol.23, pp.179–206, 1974.

[8] Barry Mazur : Modular curves and the Eisenstein ideal, *Inst. Hautes Études Sci. Publ. Math*., Vol.47, pp.33–186, 1978.

[9] Jean-Pierre Serre and John Tate : Good reduction of abelian varieties, *Ann. of Math*. (2) Vol.88, pp.492–517, 1968.

[10] Gerd Faltings : Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. math*., Vol.73, No.3, pp.349–366, 1983.

[11] Benedict Gross and Don Zagier : Heegner points and derivatives of L-series, *Invent. Math*., Vol.84, No. 2, pp.225–320, 1986.

[12] Victor Kolyvagin : The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves, (Russian) Izv. Akad. Nauk SSSR Ser., *Mat*. Vol.52, No.6, pp.1154–1180, 1327, 1988.

[13] Christopher Skinner and Éric Urban : Sur les déformations *p*-adiques de certaines représentations automorphes, *J. Inst. Math. Jussieu*, Vol.5, No.4, pp.629–698, 2006.

[14] Kazuya Kato and Fabien Trihan : On the conjectures of Birch and Swinnerton-Dyer in characteristic p>0, *Invent. Math*., Vol.153, No.3, pp.537–592, 2003.

[15] Noam Elkies : The existence of infinitely many supersingular primes for every elliptic curve over Q, *Invent. Math*. Vol.89, no.3, pp.561–567, 1987.

[16] Jean-Pierre Serre : Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math*., Vol.15, No.4, pp.259–331, 1972.

[17] Richard Taylor : Automorphy for some l-adic lifts of automorphic mod l representations. II, www.math.harvard.edu/~rtaylor/.

[18] Robert Langlands : Problems in the theory of automorphic forms, *Lecture Notes in Math*., Vol.170, Springer, Berlin, pp.18–61, 1970.

The site gdz.sub.uni-goettingen.de has the papers [2], [3], [4], [5], [6], [12], [13], [16 and [18]. The site www.numdam.org has the paper [10]. All papers by Langlands are available at his website.

***Address for Correspondence**:* Chandan Singh Dalawat, Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211 019, India. Email: dalawat@gmail.com