THE BIRCH AND SWINNERTON-DYER CONJECTURE

ANDREW WILES

A polynomial relation $f(x, y) = 0$ in two variables defines a curve C_0. If the coefficients of the polynomial are rational numbers, then one can ask for solutions of the equation $f(x, y) = 0$ with $x, y \in \mathbb{Q}$, in other words for rational points on the curve. If we consider a non-singular projective model C of the curve, then topologically it is classified by its genus, and we call this the genus of C_0 also. Note that $C_0(\mathbb{Q})$ and $C(\mathbb{Q})$ are either both finite or both infinite. Mordell conjectured, and in 1983 Faltings proved, the following deep result.

Theorem ([9]). *If the genus of C_0 is greater than or equal to 2, then $C_0(\mathbb{Q})$ is finite.*

As yet the proof is not effective so that one does not possess an algorithm for finding the rational points. (There is an effective bound on the number of solutions but that does not help much with finding them.)

The case of genus zero curves is much easier and was treated in detail by Hilbert and Hurwitz [12]. They explicitly reduce to the cases of linear and quadratic equations. The former case is easy and the latter is resolved by the criterion of Legendre. In particular, for a non-singular projective model C we find that $C(\mathbb{Q})$ is non-empty if and only if C has p-adic points for all primes p, and this in turn is determined by a finite number of congruences. If $C(\mathbb{Q})$ is non-empty, then C is parametrized by rational functions and there are infinitely many rational points.

The most elusive case is that of genus 1. There may or may not be rational solutions and no method is known for determining which is the case for any given curve. Moreover when there are rational solutions there may or may not be infinitely many. If a non-singular projective model C has a rational point, then $C(\mathbb{Q})$ has a natural structure as an abelian group with this point as the identity element. In this case we call C an elliptic curve over $\mathbb{Q}$. (For a history of the development of this idea see [19].) In 1922 Mordell [15] proved that this group is finitely generated, thus fulfilling an implicit assumption of Poincaré.

Theorem. *If C is an elliptic curve over $\mathbb{Q}$, then*

$$C(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus C(\mathbb{Q})^{\text{tors}}$$

for some integer $r \geq 0$, where $C(\mathbb{Q})^{\text{tors}}$ is a finite abelian group.

The integer r is called the rank of C. It is zero if and only if $C(\mathbb{Q})$ is finite. We can find an affine model for the curve in Weierstrass form

$$C \colon y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Z}$. We let Δ denote the discriminant of the cubic and set

$$\begin{aligned} N_p &:= \#\{\text{solutions of } y^2 \equiv x^3 + ax + b \mod p\}, \\ a_p &:= \ p - N_p. \end{aligned}$$

Then we can define the incomplete L-series of C (incomplete because we omit the Euler factors for primes $p|2\Delta$) by

$$L(C, s) := \prod_{p \nmid 2\Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

We view this as a function of the complex variable s and this Euler product is then known to converge for $\mathrm{Re}(s) > 3/2$. A conjecture going back to Hasse (see the commentary on 1952(d) in [26]) predicted that $L(C, s)$ should have a holomorphic continuation as a function of s to the whole complex plane. This has now been proved ([25], [24], [1]). We can now state the millenium prize problem:

Conjecture (Birch and Swinnerton-Dyer)**.** *The Taylor expansion of $L(C, s)$ at $s = 1$ has the form*

$$L(C, s) = c(s - 1)^r + \textit{higher order terms}$$

with $c \neq 0$ and $r = \mathrm{rank}(C(\mathbb{Q}))$.

In particular this conjecture asserts that $L(C, 1) = 0 \Leftrightarrow C(\mathbb{Q})$ is infinite.

Remarks. 1. There is a refined version of this conjecture. In this version one has to define Euler factors at primes $p|2\Delta$ to obtain the completed L-series, $L^*(C, s)$. The conjecture then predicts that $L^*(C, s) \sim c^*(s - 1)^r$ with

$$c^* = |\text{Ш}_C| R_\infty w_\infty \prod_{p|2\Delta} w_p / |C(\mathbb{Q})^{\mathrm{tors}}|^2.$$

Here $|\text{Ш}_C|$ is the order of the Tate–Shafarevich group of the elliptic curve C, a group which is not known in general to be finite although it is conjectured to be so. It counts the number of equivalence classes of homogeneous spaces of C which have points in all local fields. The term R_∞ is an $r \times r$ determinant whose matrix entries are given by a height pairing applied to a system of generators of $C(\mathbb{Q})/C(\mathbb{Q})^{\mathrm{tors}}$. The w_p's are elementary local factors and w_∞ is a simple multiple of the real period of C. For a precise definition of these factors see [20] or [22]. It is hoped that a proof of the conjecture would also yield a proof of the finiteness of Ш_C.

2. The conjecture can also be stated over any number field as well as for abelian varieties, see [20]. Since the original conjecture was stated, much more elaborate conjectures concerning special values of L-functions have appeared, due to Tate, Lichtenbaum, Deligne, Bloch, Beilinson and others, see [21], [3] and [2]. In particular, these relate the ranks of groups of algebraic cycles to the order of vanishing (or the order of poles) of suitable L-functions.

3. There is an analogous conjecture for elliptic curves over function fields. It has been proved in this case by Artin and Tate [20] that the L-series has a zero of order at least r, but the conjecture itself remains unproved. In the function field case it is now known to be equivalent to the finiteness of the Tate–Shafarevich group, [20], [17, Corollary 9.7].

4. A proof of the conjecture in the stronger form would give an effective means of finding generators for the group of rational points. Actually, one only needs the integrality of the term Ш_C in the expression for $L^*(C, s)$ above, without any interpretation as the order of the Tate–Shafarevich group. This was shown by Manin [16] subject to the condition that the elliptic curves were modular, a property which is now known for all elliptic curves by [25], [24], [1]. (A modular elliptic curve is one that occurs as a factor of the Jacobian of a modular curve.)

1. Early History

Problems on curves of genus 1 feature prominently in Diophantus' *Arithmetica.* It is easy to see that a straight line meets an elliptic curve in three points (counting multiplicity) so that if two of the points are rational then so is the third.[1] In particular, if a tangent is taken at a rational point, then it meets the curve again in a rational point. Diophantus implicitly used this method to obtain a second solution from a first. He did not iterate this process, however, and it was Fermat who first realized that one can sometimes obtain infinitely many solutions in this way. Fermat also introduced a method of 'descent' that sometimes permits one to show that the number of solutions is finite or even zero.

One very old problem concerned with rational points on elliptic curves is the congruent number problem. One way of stating it is to ask which rational integers can occur as the areas of right-angled triangles with rational length sides. Such integers are called congruent numbers. For example, Fibonacci was challenged in the court of Frederic II with the problem for $n = 5$, and he succeeded in finding such a triangle. He claimed, moreover, that there was no such triangle for $n = 1$, but the proof was fallacious and the first correct proof was given by Fermat. The problem dates back to Arab manuscripts of the 10th century (for the history see [27, Chapter 1, §VII] and [7, Chapter XVI]). It is closely related to the problem of determining the rational points on the curve $C_n : y^2 = x^3 - n^2 x$. Indeed,

$$C_n(\mathbb{Q}) \text{ is infinite } \iff n \text{ is a congruent number.}$$

Assuming the Birch and Swinnerton-Dyer conjecture (or even the weaker statement that $C_n(\mathbb{Q})$ is infinite $\Leftrightarrow L(C_n, 1) = 0$) one can show that any $n \equiv 5, 6, 7 \mod 8$ is a congruent number, and, moreover, Tunnell has shown, again assuming the conjecture, that for n odd and square-free

$$n \text{ is a congruent number } \iff \begin{array}{l} \#\{x, y, z \in \mathbb{Z} \colon 2x^2 + y^2 + 8z^2 = n\} \\ = 2 \times \#\{x, y, z \in \mathbb{Z} \colon 2x^2 + y^2 + 32z^2 = n\}, \end{array}$$

with a similar criterion if n is even [23]. Tunnell proved the implication left to right unconditionally with the help of the main theorem of [5] described below.

2. Recent History

It was the 1901 paper of Poincaré that started the modern theory of rational points on curves and that first raised questions about the minimal number of generators of $C(\mathbb{Q})$. The conjecture itself was first stated in the form we have given in the early 1960s (see [4]). It was found experimentally using one of the early EDSAC computers at Cambridge. The first general result proved was for elliptic curves with complex multiplication. The curves with complex multiplication fall into a finite number of families including $\{y^2 = x^3 - Dx\}$ and $\{y^2 = x^3 - k\}$ for varying $D, k \neq 0$. This theorem was proved in 1976 and is due to Coates and Wiles [5]. It states that if C is a curve with complex multiplication and $L(C, 1) \neq 0$, then $C(\mathbb{Q})$ is finite. In 1983 Gross and Zagier showed that if C is a modular elliptic curve and $L(C, 1) = 0$ but $L'(C, 1) \neq 0$, then an earlier construction of Heegner actually gives a rational point of infinite order. Using new ideas together with this result, Kolyvagin showed in 1990 that for modular elliptic curves, if $L(C, 1) \neq 0$

[1] This was apparently first explicitly pointed out by Newton.

then $r = 0$ and if $L(C, 1) = 0$ but $L'(C, 1) \neq 0$ then $r = 1$. In the former case Kolyvagin needed an analytic hypothesis which was confirmed soon afterwards; see [6] for the history of this and for further references. Finally as noted in remark 4 above it is now known that all elliptic curves over $\mathbb{Q}$ are modular so that we now have the following result:

Theorem. *If $L(C, s) \sim c(s-1)^m$ with $c \neq 0$ and $m = 0$ or 1, then the conjecture holds.*

In the cases where $m = 0$ or 1 some more precise results on c (which of course depends on the curve) are known by work of Rubin and Kolyvagin.

3. Rational Points on Higher-Dimensional Varieties

We began by discussing the diophantine properties of curves, and we have seen that the problem of giving a criterion for whether $C(\mathbb{Q})$ is finite or not is only an issue for curves of genus 1. Moreover, according to the conjecture above, in the case of genus 1, $C(\mathbb{Q})$ is finite if and only if $L(C, 1) \neq 0$. In higher dimensions, if V is an algebraic variety, it is conjectured (see [14]) that if we remove from V (the closure of) all subvarieties that are images of $\mathbb{P}^1$ or of abelian varieties, then the remaining open variety W should have the property that $W(\mathbb{Q})$ is finite. This has been proved by Faltings in the case where V is itself a subvariety of an abelian variety [10].

This suggests that to find infinitely many points on V one should look for rational curves or abelian varieties in V. In the latter case we can hope to use methods related to the Birch and Swinnerton-Dyer conjecture to find rational points on the abelian variety. As an example of this, consider the conjecture of Euler from 1769 that $x^4 + y^4 + z^4 = t^4$ has no non-trivial solutions. By finding a curve of genus 1 on the surface and a point of infinite order on this curve, Elkies [8] found the solution

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

His argument shows that there are infinitely many solutions to Euler's equation.

In conclusion, although there has been some success in the last fifty years in limiting the number of rational points on varieties, there are still almost no methods for finding such points. It is to be hoped that a proof of the Birch and Swinnerton-Dyer conjecture will give some insight concerning this general problem.

References

[1] 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.
[2] A. Beilinson, *Notes on absolute Hodge cohomology* in Applications of algebraic K-theory to algebraic geometry and number theory, Contemp. Math. **55**, AMS, Providence, RI, 1986, 35–68.
[3] S. Bloch, *Height pairings for algebraic cycles*, J. Pure Appl. Algebra **34** (1984), 119–145.
[4] B. Birch and H. Swinnerton-Dyer, *Notes on elliptic curves* II, Journ. reine u. angewandte Math. **218** (1965), 79–108.
[5] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223–251.
[6] H. Darmon, *Wiles' theorem and the arithmetic of elliptic curves*, in Modular forms and Fermat's Last Theorem, Springer, Berlin, 1997, 549–569
[7] L. Dickson, *History of the Theory of Numbers*, vol. II, Carnegie Institute, Washington, 1919, reprinted AMS, Providence, RI, 1999.
[8] N. Elkies, *On $A^4 + B^4 + C^4 = D^4$*, Math. Comput. **51** (1988), 825–835.

[9] G. Faltings, *Endlichkeitsätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 549–576.

[10] G. Faltings, *The general case of S. Lang's conjecture*, in Barsotti Symposium in Algebraic Geometry, Perspec. Math., vol. 15, Academic Press, Boston, 1994, 175–182.

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

[12] D. Hilbert, A. Hurwitz, *Uber die diophantischen Gleichungen von Geschlect Null*, Acta Mathematica **14** (1890), 217–224.

[13] V. Kolyvagin, *Finiteness of* $E(\mathbb{Q})$ *and* $\text{Ш}(E, \mathbb{Q})$ *for a class of Weil curves*, Math. USSR, Izv. **32** (1989), 523–541.

[14] S. Lang, *Number Theory III*, Encyclopædia of Mathematical Sciences, vol. 60, Springer-Verlag, Heidelberg, 1991.

[15] L. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge Phil. Soc. **21** (1922-23), 179–192.

[16] Y. Manin, *Cyclotomic fields and modular curves*, Russian Mathematical Surveys **26**, no. 6 (1971), 7–78.

[17] J. Milne, *Arithmetic Duality Theorems*, Academic Press, Boston, 1986.

[18] H. Poincaré, *Sur les propriétés arithmétiques des courbes algébriques*, Jour. Math. Pures Appl. **7**, Ser. 5 (1901).

[19] N. Schappacher, *Développement de la loi de groupe sur une cubique*, in Seminaire de Théorie des Nombres, Paris 1988/89, Progress in Math., vol. 91, Birkhaüser, Basel, 1991, 159–184.

[20] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Seminaire Bourbaki 1965/66, no. 306.

[21] J. Tate, *Algebraic cycles and poles of zeta functions*, in Arithmetical Algebraic Geometry: Proceedings of a Conference at Purdue University, O.F.G. Schilling, ed., Harper and Row, New York, 1965, 93–110.

[22] J. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.

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

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

[25] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math. **142** (1995), 443–551.

[26] A. Weil, *Collected Papers*, Vol. II, Springer-Verlag, New York, 1979.

[27] A. Weil, *Basic Number Theory*, Birkhaüser, Boston, 1984.