Canad. Math. Bull.Vol. **34** (3), 1991 pp. 375–384

ELLIPTIC CURVES AND MODULAR FORMS

M. RAM MURTY

ABSTRACT. This is a survey of some recent developments in the theory of elliptic curves. After an informal discussion of the main theorems of the arithmetic side of the theory and the open problems confronting the subject, we describe the recent work of K. Rubin, V. Kolyvagin, K. Murty and the author which establishes the finiteness of the Shafarevic-Tate group for modular elliptic curves of rank zero and one.

Consider the problem of finding all the rational points on the curve

$$C: \qquad x^2 + y^2 = 1.$$

We will denote the set of rational points on C by $C(\mathbb{Q})$. If $(x, y) \in C(\mathbb{Q})$, then the slope t of the line through $(-1, 0)$ is rational. Conversely, the line $y = t(x+1)$ with t rational intersects C in a rational point. This establishes a one-one correspondence between rational points and lines with rational slope

$$y = t(x+1).$$

Therefore, t parametrizes all rational points. Indeed, if we solve for t fixed,

$$\begin{aligned} 1 &= x^2 + y^2 \\ y &= t(x+1) \end{aligned}$$

we obtain after some simplification

$$x = \frac{1-t^2}{1+t^2}, \quad y = \frac{2t}{1+t^2}.$$

If we let $t = m/n$, where $m, n \in \mathbb{Z}$, by the above formulas, we can generate all the primitive Pythagorean triples. These are solutions of

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

with $a, b, c, \in \mathbb{Z}$ which are pairwise coprime. This is an ancient theorem known to at least three early civilizations: the Hindus, the Egyptians and the Babylonians. Pythagoras alluded to it in the 6th century B.C. and Diophantus wrote down a proof, in the modern mathematical sense, in 250 A.D. Thus, we obtain:

This is the substance of the Coxeter-James Lecture delivered in December 1988 at the Canadian Mathematical Society Winter meeting in Toronto, Canada.

Received by the editors April 2, 1990 .

AMS subject classification: Primary: 11G05; secondary: 11G40.

THEOREM. *All primitive solutions of*

$$a^2 + b^2 = c^2, \quad a, b, c \in \mathbb{Z}$$

are given by

$$\begin{aligned} a &= n^2 - m^2 \\ b &= 2mn \\ c &= n^2 + m^2 \\ (m,n) = 1 \qquad m &\not\equiv n \pmod 2. \end{aligned}$$

The same idea works for any rational conic.

Using this theorem, for instance, Fermat showed that the equation

$$x^4 + y^4 = z^2, \quad x, y, z, \in \mathbb{Z}$$

has no non-trivial integral solutions. His method is the origin of the method of descent and is very instructive. As the above equation is classical and is treated in many books, I will illustrate the method by another example. Consider instead the equation

$$x^4 + 4y^4 = z^2.$$

Suppose the equation has a non-trivial solution. Of all the solutions, we will choose the one with $|y|$ minimal and > 0 as the solution is non-trivial. By our ancient theorem, we can parametrise a hypothetical solution by

$$\begin{aligned} x^2 &= r^2 - s^2 \\ 2y^2 &= 2rs \\ z &= r^2 + s^2 \end{aligned}$$

and we notice that the equation above

$$x^2 + s^2 = r^2$$

can in turn be parametrised by

$$\begin{aligned} x &= \alpha^2 - \beta^2 \\ s &= 2\alpha\beta \\ r &= \alpha^2 + \beta^2. \end{aligned}$$

But now, if we combine these parametrizations, namely

$$2y^2 = 2rs, \quad s = 2\alpha\beta, \quad r = \alpha^2 + \beta^2$$

we obtain

$$y^2 = 2\alpha\beta(\alpha^2 + \beta^2).$$

Because α and β are relatively prime, 2α, β and $\alpha^2+\beta^2$ must all be perfect squares. Therefore,

$$\begin{aligned}\alpha &= 2u^2\\ \beta &= v^2\\ \alpha^2+\beta^2 &= w^2\end{aligned}$$

from which we deduce that

$$v^4+4u^4 = w^2.$$

But now, $0 < |u| < |\alpha|^{1/2} < |y|$, which contradicts the minimality of the solution. Hence, there are no non-trivial solutions.

Now consider rational cubics of the following form.

$$E: \qquad y^2 = x^3+ax+b, \qquad a,b \in \mathbb{Q}$$

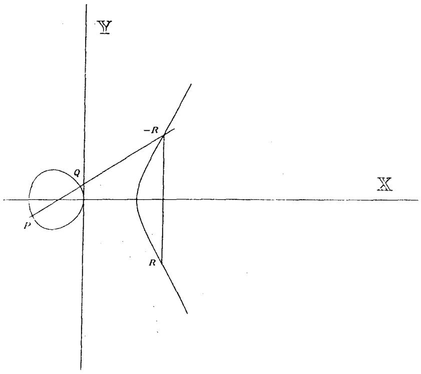

FIGURE 1

A line passing through two rational points intersects the curve in another rational point. This defines a group law on $E(\mathbb{Q})$, first noticed by Poincaré. Suppose that

$$P = (x_1,y_1), \quad Q = (x_2,y_2)$$

are two rational points on the curve. The line through them is

$$Y = mX+B, \quad m = \frac{y_2-y_1}{x_2-x_1}.$$

To find the third point of intersection, we solve

$$\begin{aligned}y^2 &= x^3+ax+b\\ y &= mx+B\end{aligned}$$

to obtain

$$(mx+B)^2 = x^3+ax+b.$$

We already know two roots of this cubic equation, namely $x = x_1$, $x = x_2$. Therefore, the third root satisfies

$$x_1 + x_2 + x_3 = m^2$$

and we obtain

$$x_3 = -x_1 - x_2 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2$$
$$y_3 = mx_3 + B$$

and this gives the addition formula for two distinct points. If $x_1 = x_2$, the tangent line at (x_1, y_1) determines (x_3, y_3). Define

$$(x_1, y_1) \oplus (x_2, y_2) = (x_3, -y_3)$$

and formally add the point at infinity to play the role of the identity element. This makes $E(\mathbb{Q})$ into a group. If $R = (x_3, y_3)$, then the group law is illustrated by Figure 1. Poincaré conjectured that $E(\mathbb{Q})$ is finitely generated. In 1922, Mordell proved this for elliptic curves over $\mathbb{Q}$:

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r.$$

$r = r_{\mathbb{Q}}$ is called the rank of E over $\mathbb{Q}$. In 1928, A. Weil proved in his doctoral thesis the same theorem for global fields (that is, either an algebraic number field or an algebraic function field over a finite field of transcendence degree one). If k is a global field, then

$$E(k) \simeq E(k)_{\text{tors}} \oplus \mathbb{Z}^{r_k}$$

and r_k is called the rank of E over k. More generally, the same holds for abelian varieties. (A good reference for the arithmetic theory of elliptic curves is [7]. Many of the classical results that will be referred to in the subsequent discussion can be found there and the original source is cited there.)

Therefore, in order to know $E(\mathbb{Q})$, we first must know $E(\mathbb{Q})_{\text{tors}}$ and r. The knowledge of torsion is supplied by the classical Lutz-Nagell theorem of 1935. This says:

THEOREM (LUTZ-NAGELL, 1935). *Let*

$$y^2 = x^3 + ax + b, \quad a, b, \in \mathbb{Z}.$$

If $(x,y) \in E(\mathbb{Q})_{\text{tors}}$, *then* $(x,y) \in \mathbb{Z}$ *and either* $y = 0$ *or* $y^2 | 4a^3 + 27b^2$.

EXAMPLE. Let

$$E: \qquad y^2 = x^3 + 3, \qquad \Delta = -3^5.$$

Now, $(1,2) \in E(\mathbb{Q})$. If $(1,2) \in E(\mathbb{Q})_{\text{tors}}$ then $y = 2$ divides 3^5, which is a contradiction. Therefore, (1,2) is point of infinite order. In fact, $E(\mathbb{Q})_{\text{tors}} = 1$.

How does one compute torsion? That this can be done effectively for curves over $\mathbb{Q}$ is a theorem of Mazur:

THEOREM (MAZUR). *$E(\mathbb{Q})_{\text{tors}}$ is one of*

$$\mathbb{Z}/N\mathbb{Z}, \qquad 1 \le N \le 10, \quad N = 12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, \qquad 1 \le N \le 4$$

and each group occurs for some curve $E/\mathbb{Q}$. For arbitrary number fields, such a result is unknown and it is conjectured that:

CONJECTURE. $|E(K)_{\text{tors}}| \le C_K$ for some constant C_K depending only on the number field K.

Recent work in progress by S. Kamienny determines the finite list of primes that can divide the order of the torsion subgroup when K is a quadratic extension of $\mathbb{Q}$.

EXERCISE. If E is defined over $\mathbb{Q}$, then

$$|E(K)_{\text{tors}}| \le 16[K:Q]!$$

Another way to guess the size of torsion is noting

$$E(\mathbb{Q})_{\text{tors}} \hookrightarrow E(\mathbb{F}_p)$$

for p not dividing $4a^3 + 27b^2$. We know from a classical result of Hasse that

$$\#E(\mathbb{F}_p) = p + 1 - a_p$$

where $|a_p| \le 2\sqrt{p}$.

EXAMPLE. Consider $y^2 = x^3 - 2$. The discriminant of the curve is 108. A direct computation shows that $\#E(\mathbb{F}_5) = 6$ and $\#E(\mathbb{F}_7) = 7$. As these two cardinalities are relatively prime $E(\mathbb{Q})_{\text{tors}} = 1$.

It is not difficult to see that the ring of endomorphisms of E is either an order in an imaginary quadratic field or $\mathbb{Z}$. In the former case, we say that E has complex multiplication (CM).

If E has CM and p is inert in k, then $a_p = 0$. Therefore, if $m = \#E(\mathbb{Q})_{\text{tors}}$, then as the torsion group imbeds into the group of points mod p for p not dividing the discriminant, we can conclude that

$$m | p + 1 - a_p.$$

But $a_p = 0$ if p is inert in k. Thus,

$$p + 1 \equiv 0 (\operatorname{mod} m)$$

for at least *half* of the primes. Hence,

$$\frac{1}{\phi(m)} \ge \frac{1}{2}$$

by Dirichlet's theorem on primes in arithmetic progressions. We conclude that $\phi(m) \le 2$ so that $m = 1, 2, 3, 4$, or 6 in the CM case.

What about the rank r? This is more difficult. For the sake of simplicity, let us suppose that our cubic has a rational root. After a suitable transformation, we can write the curve as

$$y^2 = x^3 + ax^2 + bx.$$

For each b, let $b = b_1 b_2$ be a factorisation modulo squares. Look at

$$C_{b_1,b_2}: \qquad N^2 = b_1 M^4 + aM^2e^2 + b_2 e^4.$$

If C_{b_1,b_2} has a non-trivial integral solution (N, M, e), call the factorisation *good*. Let $g(b)$ be the number of *good* factorisations. Now let

$$E': \qquad y^2 = x^3 + a'x^2 + b'x$$

where

$$a' = -2a$$
$$b' = a^2 - 4b.$$

For $b' = b'_1 b'_2$ define $g'(b')$ analogously. Then

THEOREM (TATE'S ALGORITHM).

$$2^r = \frac{g(b)g'(b')}{4}.$$

EXAMPLE. For

$$E: \qquad y^2 = x^3 - x$$

$g(-1) = 2$. The curve

$$E': \qquad y^2 = x^3 + 4x$$

leads to

$$N^2 = M^4 + 4e^4$$

which has no solutions by our first example. Therefore $g'(4) = 2$ as $N^2 = 2M^4 + 2e^4$ has (2,1,1) as solution. Therefore, $2^r = 1$ so that $r = 0$.

Potentially, this algorithm can run into the difficulty of an intractible diophantine problem. This would make the calculation of r difficult. To circumvent this difficulty, Birch and Swinnerton-Dyer were led to make the following considerations about L-series.

Define

$$L_E(s) = \prod_{p|\Delta}\left(1 - \frac{t_p}{p^s}\right)^{-1} \prod_{p\nmid\Delta} L_p(s)$$

where $t_p = 0, 1, -1$ depending on the type of reduction of E mod p, and

$$L_p(s) = \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}.$$

By virtue of Hasse's inequality on a_p, this series converges for $\Re(s) > 3/2$.

CONJECTURE (BIRCH AND SWINNERTON-DYER). $L_E(s)$ has an analytic continuation for all complex values of s and satisfies the functional equation

$$\begin{aligned}\Lambda(s) &= \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s) L_E(s)\\ &= w\Lambda(2-s), \qquad w = \pm 1.\end{aligned}$$

Moreover,

$$\operatorname{ord}_{s=1} L_E(s) = \text{rank } E(\mathbb{Q}).$$

If E has CM, Deuring showed $L_E(s)$ has an analytic continuation and satisfies the functional equation. Coates and Wiles (1977) showed that if rank $E(\mathbb{Q}) \geq 1$ then $L_E(1) = 0$ for CM elliptic curves. In 1982, Rajiv Gupta and H. Stark used the theory of Eisenstein series to establish the same result. Recently, Rubin [6] proved that for CM elliptic curves, $r_{\mathbb{Q}} \geq 2$ implies $\operatorname{ord}_{s=1} L_E(s) \geq 2$.

What about non-CM curves? There is a central conjecture of Taniyama that shows the way for non-CM curves.

CONJECTURE (TANIYAMA, 1955). There is a normalised cusp form of weight 2 on $\Gamma_0(N)$ such that if

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$$

is the Fourier expansion at $i\infty$ then

$$L_E(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Such a conjecture would establish the functional equation and the analytic continuation of the L-series of E.

Shimura proved that every CM elliptic curve over $\mathbb{Q}$ is *modular,* that is satisfies Taniyama's conjecture.

Recently, the Soviet mathematician V. Kolyvagin [3] made significant progress towards the Birch-Swinnerton-Dyer conjecture. Combined with a result of Gross-Zagier [2] his result may be stated in the following form:

THEOREM (KOLYVAGIN, PART 1). *If E is a modular elliptic curve over $\mathbb{Q}$ and rank $E(\mathbb{Q}) \geq 1$, then $L_E(1) = 0$, provided the following hypothesis holds:*

HYPOTHESIS. There is a quadratic character χ_D and $D < 0$, such that all $p|N$ split completely in $Q(\sqrt{D})$ and

$$\sum_{n=1}^{\infty} \frac{a_n}{n} \left(\frac{D}{n}\right) \log n \neq 0.$$

In joint work with V. Kumar Murty [5], it was shown that the hypothesis is always true. Independently, Bump, Hoffstein and Friedberg [1] using the automorphic theory of

GSp(4), also established the truth of the hypothesis. Thus, Kolyvagin's theorem can be stated unconditionally by putting together the work of eight mathematicians!

Knowing the rank still leaves the problem of finding primitive generators.

This problem is approached in the following way. Consider the surjective map

$$E(\bar{\mathbf{Q}})\xrightarrow{n}E(\bar{\mathbf{Q}})$$

with kernel

$$E[n] = \{P \in E(\bar{\mathbf{Q}}) : nP = 0\}.$$

Therefore, we have the exact sequence

$$0 \longrightarrow E[n] \longrightarrow E(\bar{\mathbf{Q}})\xrightarrow{n}E(\bar{\mathbf{Q}}) \longrightarrow 0.$$

Now the Galois group $G = \mathrm{Gal}(\bar{\mathbf{Q}} / \mathbf{Q})$ acts on $E(\bar{\mathbf{Q}})$ and the G-fixed points of $E(\bar{\mathbf{Q}})$ are the $\mathbf{Q}$ rational points of E. In general, whenever we have an exact sequence of G-modules, we have a long exact sequence of cohomology groups obtained by taking the G-fixed points: thus,

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

leads to

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow H^1(G,A) \longrightarrow H^1(G,B) \longrightarrow H^1(G,,C) \longrightarrow H^2(G,A) \longrightarrow \cdots$$

For the sake of completeness, we give the definition of the first cohomology group (the higher cohomology groups not being used in the later part of the exposition). Let G be a group and A an abelian group on which G acts. Define

$$Z^1(G,A) = \{f\colon G \longrightarrow A \mid f(\sigma\tau) = \sigma f(\tau) + f(\sigma)\}.$$

Let

$$B^1(G,A) = \{f\colon G \longrightarrow A \mid \exists a : f(\sigma) = \sigma a - a\}.$$

It is easily seen that $B^1(G,A)$ and $Z^1(G,A)$ are abelian groups and $B^1(G,A)$ is a subgroup of $Z^1(G,A)$. The quotient group

$$H^1(G,A) = Z^1(G,A)/B^1(G,A)$$

is called the first cohomology group and its elements are called 1-cocycles.

In our case therefore, we obtain

$$0 \longrightarrow E[n](\mathbf{Q}) \longrightarrow E(\mathbf{Q})\xrightarrow{n}E(\mathbf{Q}) \longrightarrow H^1(\mathbf{Q},E[n]) \longrightarrow H^1(\mathbf{Q},E(\bar{\mathbf{Q}}))\xrightarrow{n}H^1(\mathbf{Q},E(\bar{\mathbf{Q}}))\ldots.$$

We can shorten this exact sequence by noting that the image of the penultimate map surjects to the kernel of

$$H^1(\mathbf{Q},E(\bar{\mathbf{Q}})\xrightarrow{n}H^1(\mathbf{Q},E(\bar{\mathbf{Q}})).$$

Thus, we get the short sequence

$$0 \longrightarrow E(\mathbf{Q})/nE(\mathbf{Q}) \longrightarrow H^1(\mathbf{Q}, E[n]) \longrightarrow H^1(\mathbf{Q}, E)[n] \longrightarrow 0.$$

However, the groups above are infinite groups and the sequence is not amenable to calculation. We therefore study the sequence over the p-adic number field $\mathbf{Q}_p$. We get:

$$0 \longrightarrow E(\mathbf{Q}_p)/nE(\mathbf{Q}_p) \longrightarrow H^1(\mathbf{Q}_p, E[n]) \longrightarrow H^1(\mathbf{Q}_p, E)[n] \longrightarrow 0.$$

Define the n-Selmer group as

$$S^{(n)} = \ker\{H^1(\mathbf{Q}, E[n]) \longrightarrow \prod_p H^1(\mathbf{Q}_p, E)\}$$

and the Tate-Shafarevic group by

$$\text{Ш} = \ker\{H^1(\mathbf{Q}, E) \longrightarrow \prod_p H^1(\mathbf{Q}_p, E)\}$$

Our sequence becomes

$$0 \longrightarrow E(Q)/nE(Q) \longrightarrow S^{(n)} \longrightarrow \text{Ш}[n] \longrightarrow 0$$

where now these groups are finite.

We have

CONJECTURE. **Ш** is finite.

Rubin showed that if E has CM and $L_E(1) \neq 0$, then **Ш** is finite. Recently, Kolyvagin (1987, 1988) showed that if E is a modular elliptic curve and $L_E(1) \neq 0$, then **Ш** is finite provided the above analytic hypothesis holds. Since this hypothesis is now a theorem, again Kolyvagin's results can be stated unconditionally.

Our proof [5] of the analytic hypothesis establishes the following asymptotic formula. Let

$$L_E(s, D) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \left(\frac{D}{n}\right),$$

and set

$$C = \frac{1}{2N} \sum_{n_1, n_2} \frac{\phi(n_2)}{n_2} \frac{a_{n_1 n_2^2}}{n_1 n_2^2},$$

where n_1 ranges over positive integers with the property that $p|n_1$ implies $p|4N$ and n_2 ranges over all integers satisfying $(n_2, 4N) = 1$.

THEOREM. *Suppose $L_E(1) \neq 0$. Then, $C \neq 0$ and*

$$\sum_{\substack{0 < -D \leq Y \\ D \equiv 1 \pmod{4N}}} L'_E(1, D) = CY \log Y + o(Y \log Y)$$

as $Y \longrightarrow \infty$.

On the other hand, Bump, Friedberg and Hoffstein [1] realise the values of these quadratic twists as Fourier coefficients of metaplectic forms on GSp(4) and show that the form is not identically zero.

It is possible to prove more. If r_D is the order of the zero of

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}\left(\frac{D}{n}\right)$$

at $s = 1$ then the author [4] has shown that the generalised Riemann hypothesis implies

$$\sum_{0<-D\leq X} r_D \leq 2.5X$$

as $X \longrightarrow \infty$. This shows that $r_D = 1$ for a positive proportion of quadratic twists. It is conjectured that $r_D \geq 2$ occurs rarely. More precisely,

$$\#\{D \leq X : r_D \geq 2\} = o(X)$$

as $X \longrightarrow \infty$.

It is believed that there are elliptic curves of unbounded rank. This is true for elliptic curves over function fields over finite fields by a result of Shafarevic and Tate. In view of the Birch-Swinnerton-Dyer conjectures, this leads to the following question. Are there L-series of modular forms with a large order zero at the center of the criticial strip? This is not known.

The algorithm of Tate however yields the following curious result. Let $f(n)$ denotes the number of ways of writing $n = ab$ with $a + b$ a perfect square. If

$$\lim \sup_{n \text{ squarefree}} f(n) = \infty$$

then there are curves over Q of arbitrarily large rank. D. Clark in his McGill M.Sc. thesis showed that

$$\lim \sup f(n) = \infty$$

without the squarefree assumption.

References

1. D. Bump, S. Friedberg and J. Hoffstein, *Non-vanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102**(1990), 543–618.

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

3. V. A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $\text{III}_{E/\mathbb{Q}}$ for a subclass of Weil curves*, Izv. Akad. Nauk. SSSR Ser. Math. **52**(1988), 522–540; English transl. in Math. USSR Izv. **32**(1989).

4. M. Ram Murty, *On simple zeroes of certain L-series*, in Number Theory, Proceedings of the Banff conference, (ed. R. Mollin), 1990, 427–439, Walter de Gruyter.

5. M. Ram Murty, and V. Kumar Murty, *Mean values of derivatives of modular L-series*, Annals of Mathematics, **133**(1991), 447–475.

6. K. Rubin, *Tate-Shafarevic groups and L-functions of elliptic curves with complex multiplication*, Inv. Math. (3)**89**(1987), 527–559.

7. J. Silverman, *The arithmetic of elliptic curves*. Springer-Verlag, New York, 1986.

McGill University
Montréal, Québec