The BSD Conjecture: Part II

Francesco Naccarato

19/12/2021

Definition 1. *The analytic rank of E is $r_{an}(E) = ord_{s=1}L(E,s)$.*

This does not make sense *a priori*, but, as we will see, $L(E,s)$ admits an entire analytic continuation. Suppose we could use the Euler product expression for $L(E,s)$ even for $s = 1$: then we would get

$$L(E,1)\text{“}=\text{”}\prod_p \frac{p}{N_p} \tag{1}$$

So, heuristically, if the curve has "a lot" of $\mathbb{F}_p$-rational points as $p \to \infty$, then we would expect that $L(E,1) = 0$.

Observation 1. Interestingly, if the above infinite product converges, say to α, then by a theorem of Goldfeld $L(E,s)$ satisfies the Riemann hypothesis and $L(E,1) = \sqrt{2}\alpha$.

Now, one could consider the following heuristics: suppose E has large rank r. Then we expect, on average over p, E_p to have "a lot" of rational points (still obeying Hasse-Weil!), and so we expect the product in (1) to diverge to 0 quite rapidly, that is, we expect $r_{an}(E)$ to be large.
Supported by a lot of numerical evidence, Birch and Swinnerton-Dyer came up with the following:

Conjecture 1. $r(E) = r_{an}(E)$

As we know, this turned out to be considered a very important problem: it constitutes one of the main examples of the usefulness of L-functions and their critical values in the study of algebro-geometric objects; in particular, the analytic rank can be studied via complex analytic techniques (usually effective if we assume the associated Riemann Hypothesis). There are also various formulas for the order 0 and 1 derivatives of $L(E,s)$ at $s = 1$ which, assuming BSD, shed some light on the arithmetic of "most" elliptic curves, other than being the main tool in the progress that we have towards BSD itself.
The latter class of formulas comes from "modularity", a deep and deeply surprising aspect of rational elliptic curves. In order to understand this aspect, we first need to define **modular forms**. Let $\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. For a proof of all the facts about modular forms that we will use, see [Zag08], unless another reference is mentioned.

Definition 2. *A modular form of weight k (for $\mathbb{SL}_2(\mathbb{Z})$) is a holomorphic function $f : \mathbb{H} \longrightarrow \mathbb{C}$ that stays bounded as $\mathrm{Im}(z) \to \infty$ and such that*

$$f(\gamma z) = (cz + d)^{-k} f(z) \tag{2}$$

for any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \gamma \in \mathbb{SL}_2(\mathbb{Z})$, where the action is $\gamma z = \frac{az+b}{cz+d}$.

This definition may at first seem quite arbitrary, but it turns out that modular forms are a very effective tool to encode arithmetical information and prove combinatorial identities. This is, in some sense, a consequence of the fact that modular forms of a given weight form a finite dimensional vector space, and that many power series whose coefficients are "arithmetical functions" turn out to be modular forms after a change of variables.

A very important corollary of the definition of modular form is its periodicity, for, using $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in (2) we get

$$f(z+1) = f(z).$$

As a consequence of this and holomorphy, we obtain that a modular form has a Fourier expansion $f(z) = a_0 + a_1 q + a_2 q^2 + ...$ with $q = \exp(2\pi i z)$, where the fact that only terms with $n \geq 0$ occur is equivalent to the boundedness condition. The modular forms related to elliptic curves famously have weight 2, but it can be seen that the only such function according to our definition is identically 0. We in fact need to relax (2) to some subgroup Γ of $\mathbb{SL}_2(\mathbb{Z})$.

Example 1. It is not hard to show that the function

$$f(z) = \sum_{x_1,...,x_4 \in \mathbb{Z}} q^{x_1^2+...+x_4^2} = (\sum_{n \in \mathbb{Z}} q^{n^2})^4 \tag{3}$$

is a modular form for the subgroup of $\mathbb{SL}_2(\mathbb{Z})$ such that $4|c$. Notice that the coefficient of q^n is $\#\{(x_1, ..., x_4) \in \mathbb{Z}^4 : x_1^2 + ...x_4^2 = n\}$: this fact can be used for a quick proof of Lagrange's Theorem that every natural number is the sum of 4 squares of integers.

The link between modular forms and elliptic curves, conjectured by Tanyiama, Shimura and Weil and proved by Wiles, Taylor et al., is: for any elliptic curve E over $\mathbb{Q}$, the power series $\sum_{n \geq 0} a_n q^n$ formed with the coefficients a_n of (the Euler product for) $L(E, s)$ is a modular form (under the broader definition) of weight 2. Analogously, given a modular form $f(z) = a_0 + a_1 q + a_2 q^2 + ...$, we can consider its L-function $L(f, s) = \sum_{n \geq 0} a_n n^{-s}$. Then we have:

Theorem 1 (Modularity of elliptic curves)**.** *For any rational elliptic curve E there is a modular form f of weight 2 such that for $\mathrm{Re}(s) > \frac{3}{2}$ we have $L(E, s) = L(f, s)$.*

Corollary 1. *For such curves, $L(E, s)$ analytically extends to the whole complex plane.*

Proof. It is well known that L-functions of modular forms are analytic, so we get the claim by the uniqueness of analytic continuation.

This being considered, let us go back to the Congruent Number Problem, before surveying the results we have for BSD. Let us start with an example, due to Zagier, that strongly suggests that this advanced machinery is actually needed to attack the problem.

Example 2. $n = 157$ is a congruent number: in particular, the "simplest" right triangle with rational sides of which it is the area has shorter sides

$$a = \frac{411340519227716149383203}{21666555693714761309610}, \; b = \frac{6803298487826435051217540}{411340519227716149383203}$$

So, any sort of characterization of congruent numbers has to account for this "arithmetic complexity" that is intrinsic to the problem. Even more, we can see how, even for incredibly small values of n, a brute force search is not a feasible way to attack the problem.

As we know, a squarefree positive integer n is congruent if and only if $r(E_n) > 0$. Assuming BSD, we could write $r_{an}(E_n) > 0$, that is, $L(E_n, 1) = 0$. The key fact here is that there are various formulas for critical values of (twisted) L-function of modular forms in terms of the coefficients of related modular forms. The one we need is due to Tunnell, adapting a general result of Kohnen and Zagier, which in turns builds on fundamental work of Shimura. See [Kob93] for the precise statements of these theorems.

Proposition 2. *There exist modular forms*[1] $f(z) = \sum_{n \geq 0} a_n q^n$, $g(z) = \sum_{n \geq 0} b_n q^n$ *such that, up to nonzero factors, we have:*

$$L(E_n, 1) = \begin{cases} a_n^2, & \text{if } n \text{ is odd} \\ b_{\frac{n}{2}}^2, & \text{if } n \text{ is even} \end{cases}$$

[1] These have actually *half-integer* weight 3/2. For an introduction to their theory, see [Kob93]

Tunnel computed the relevant modular forms, which, as in the example above, depend on the number of ways certain quadratic forms represent n, thus obtaining, under the assumption of BSD, a necessary and sufficient condition for n to be congruent. Moreover, it is a theorem of Coates and Wiles that if the rank of an elliptic curve over $\mathbb{Q}$ is nonzero, then so is its analytic rank, so the "necessary" part is unconditional. We can now state the full form of Tunnell's Theorem.

Theorem 3. *Let*

$$A(n) = \begin{cases} \{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 32z^2\}, & \text{if } n \text{ is odd} \\ \{(x,y,z) \in \mathbb{Z}^3 : \frac{n}{2} = 4x^2 + y^2 + 32z^2\}, & \text{if } n \text{ is even} \end{cases}$$

and

$$B(n) = \begin{cases} \{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 8z^2\}, & \text{if } n \text{ is odd} \\ \{(x,y,z) \in \mathbb{Z}^3 : \frac{n}{2} = 4x^2 + y^2 + 8z^2\}, & \text{if } n \text{ is even} \end{cases}$$

Then if n is congruent we have $\#A(n) = \frac{1}{2}\#B(n)$, and, assuming BSD, the converse holds.

Remark 3.1. Observe that Tunnell's condition is very easy to algorithmically verify. Take for example $n = 17$; any triple in $A(17)$ must have $z = 0$ and $|x| < 3$. We are left to check five cases of x to see which lead to $17 - x^2$ being a square: this gives the solutions $(\pm 2, \pm 3, 0)$ and so $\#A(n) = 4$. The same reasoning for $B(n)$, but considering also $z = \pm 1$, gives $B(n) = \{(\pm 2, \pm 3, 0), (0, \pm 3, \pm 1), (\pm 2, \pm 1, \pm 1)$, so $\frac{1}{2}\#B(n) = 8$ and so we know that 17 is not congruent.

Remark 3.2. Say that n is odd: looking (mod 8) at the two corresponding quadratic forms, we see that, since quadratic residues (mod 8) are $0, 1, 4$, the odd integers they can represent are congruent to 1 or 3 (mod 8). Analogously, if n is even, the corresponding forms can only represent integers congruent to 2 or 4 (mod 8), hence we obtain the following nice result:

Corollary 2. *If $n \equiv 5, 6, 7 \pmod 8$ is squarefree, then, assuming BSD, n is a congruent number.*

Proof: In this case, by the previous observation we must have $A(n) = B(n) = 0$, so the claim follows from Tunnell's Theorem.

Finally, let us go back to the partial progress towards BSD; the first significant step was the aforementioned result of Coates and Wiles (1977) that a positive rank implies a positive analytic rank. A few years later, Gross and Zagier made another breakthrough:

Theorem 4. *If $r_{an}(E) = 1$ then $r(E) \geq 1$*

Their proof is based on the construction of a special rational point, called *Heegner point*, on E that provably has infinite order if the analytic rank is 1. Unfortunately, this does not generalize to higher analytic rank, because in that case the Heegner point is torsion.
In the early 90s Kolyvagin built on Gross and Zagier's work to prove that if $r_{an}(E) = 1$ than the Mordell-Weil group of E is actually generated by its Heegner point, completing the proof of the following:

Theorem 5 (Gross, Zagier, Kolyvagin)**.** *If $r_{an}(E) \leq 1$ the the Birch and Swinnerton-Dyer conjecture holds.*

References

[Kob93] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms.* Springer, 1993.

[Zag08] D. Zagier. *The 1-2-3 of Modular Forms: Elliptic Modular Forms and their applications.* Springer, 2008.