Bollettino Unione Matematica Italiana

Sezione A – La Matematica nella Società e nella Cultura

Stefano Vigni

Una formula di tipo Gross-Zagier per una certa funzione L p-adica anticiclotomica

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **9-A**—*La Matematica nella Società e nella Cultura* (2006), n.2 (Fascicolo dedicato alle tesi di dottorato), p. 307–310.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2006_8_9A_2_307_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2006.

Bollettino U. M. I.
La Matematica nella Società e nella Cultura
Serie VIII, Vol. IX-A, Agosto 2006, 307-310

Una formula di tipo Gross-Zagier per una certa funzione L p-adica anticiclotomica

STEFANO VIGNI

Sia E/F una curva ellittica definita sul campo di numeri F e sia $L(E/F, s)$ la funzione L complessa associata ad E/F. Se $E(F)$ è il gruppo abeliano dei punti F-razionali di E (detto *gruppo di Mordell-Weil*), il ben noto Teorema di Mordell-Weil assicura che $E(F)$ è finitamente generato, e lo studio del rango di $E(F)$ costituisce il problema centrale nella teoria aritmetica delle curve ellittiche. A tal proposito, la Congettura di Birch e Swinnerton-Dyer (per comodità citata nel seguito come "congettura BSD") afferma, nella sua forma più semplice, che

$$\mathrm{rk}_{\mathbb{Z}} E(F) = \mathrm{ord}_{s=1} L(E/F, s). \tag{1}$$

In questa direzione, un risultato fondamentale di Gross e Zagier ([3]) stabilisce che se E è definita su $\mathbb{Q}$ e K è un opportuno campo quadratico immaginario allora

$$L'(E/K, 1) = c \cdot \hat{h}(a_K), \tag{2}$$

dove c è una costante non nulla, $\hat{h}$ è l'altezza di Néron-Tate su $E(\bar{\mathbb{Q}})$ e a_K è un certo *punto di Heegner* in $E(K)$. In particolare, $L'(E/K, 1) \neq 0$ se e soltanto se a_K ha periodo infinito in $E(K)$. Combinando la 2 con i risultati ottenuti da Kolyvagin (teoria coomologica dei sistemi di Eulero) e con la modularità delle curve ellittiche razionali (provata da Wiles in [5] e dalla sua scuola), si riesce a dimostrare la BSD nella forma 1 per tutte le curve ellittiche $E/\mathbb{Q}$ tali che $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) \leq 1$.

Mentre la congettura BSD originale è formulata a partire da funzioni analitiche in senso classico (ossia su $\mathbb{C}$), il punto di partenza del nostro lavoro di tesi è invece la teoria di Bertolini e Darmon dei cosiddetti analoghi p-adici anticiclotomici della BSD, esposta in [1]. In questo importante lavoro, Bertolini e Darmon sfruttano le proprietà aritmetiche di particolari sistemi di punti di Heegner (e di Gross) su curve di Shimura per definire funzioni L p-adiche associate a una curva ellittica $E/\mathbb{Q}$, a un primo p e a un opportuno campo quadratico immaginario K. Il passo successivo è la formulazione di una serie dettagliata di congetture di tipo BSD, che rappresentano la naturale controparte "anticiclotomica" delle congetture di BSD p-adiche di Mazur, Tate e Teitelbaum ([4]). Il risultato principale della nostra tesi è un analogo della relazione 2 per una certa funzione L p-adica costruita secondo la proposta di Bertolini e Darmon.

Descriviamo adesso brevemente il lavoro svolto. Sia $E/\mathbb{Q}$ una curva ellittica di conduttore N e sia $p > 2$ un primo di riduzione moltiplicativa *spezzata* per E. Questa condizione assicura l'esistenza di una successione esatta di moduli di Galois

$$0 \longrightarrow q^{\mathbb{Z}} \longrightarrow \bar{\mathbb{Q}}_p^{\times} \longrightarrow E(\bar{\mathbb{Q}}_p) \longrightarrow 0,$$

che esprime l'uniformizzazione p-adica di Tate dei punti locali di E. Tale uniformizzazione è definita sopra $\mathbb{Q}_p$, e $q \in p\mathbb{Z}_p - \{0\}$ è il periodo moltiplicativo di Tate di E in p. Sia poi K un campo quadratico immaginario (con anello degli interi algebrici $\mathcal{O}_K$) tale che $(\mathrm{disc}(K), N) = 1$, il primo p *si decompone* in K e le seguenti condizioni sono soddisfatte:

1. se un primo ℓ è inerte in K allora $\ell^2 \not| N$;
2. il numero dei fattori primi di N che sono inerti in K è *pari*.

Siano quindi N^- il prodotto dei fattori primi di N inerti in K e $N^+ := N/N^-$, sicché ogni primo che divide N^+ si decompone in K. Si noti che $p \| N^+$. Indichiamo con B l'algebra di quaternioni su $\mathbb{Q}$ di discriminante N^-, che è unica a meno di isomorfismo. La condizione 2 implica che B è *indefinita*, i.e. $B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R})$: fissiamo un isomorfismo fra queste due algebre, che implicitamente identifichiamo. Nella terminologia adottata in [1] siamo nel caso "split indefinite".

Come illustrato in [1, §1.3], alla fattorizzazione $N = N^+N^-$ è associata una superficie di Riemann compatta X_{N^+,N^-}, detta *curva di Shimura* di discriminante N^- e livello N^+. Se $\mathcal{R} = \mathcal{R}_{N^+,N^-}$ è l'ordine di Eichler di livello N^+ in B definito come in [1, §1.1], $\mathcal{R}^1$ è il gruppo delle unità di norma 1 in $\mathcal{R}$ e $\mathcal{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ è il semipiano complesso superiore, si ha che $X_{N^+,N^-} \cong \mathcal{R}^1 \backslash \mathcal{H}$, con l'azione di $\mathcal{R}^1$ su $\mathcal{H}$ indotta dall'azione di $SL_2(\mathbb{R})$ per trasformazioni di Möbius. La curva proiettiva X_{N^+,N^-} (che coincide con la curva modulare $X_0(N)$ se $N^- = 1$) è naturalmente definita su $\mathbb{Q}$, ed ammette un'interpretazione come spazio di moduli di opportune superficie abeliane a moltiplicazione quaternionica con struttura di livello. Infine, la corrispondenza di Jacquet-Langlands per forme automorfe e la modularità di E assicurano l'esistenza di una "parametrizzazione modulare"

$$\pi_E : \mathrm{Pic}\,(X_{N^+,N^-}) \twoheadrightarrow E$$

definita su $\mathbb{Q}$, che supporremo fissata una volta per tutte.

Sia ora K_∞/K la $\mathbb{Z}_p$-estensione anticiclotomica di K: si tratta dell'unica estensione galoisiana di K diedrale su $\mathbb{Q}$ tale che $G_\infty := \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. Scriviamo $K_\infty = \bigcup_{n \geq 1} K_n$ con $G_n := \mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$. Nella definizione della nostra "funzione" L p-adica un ruolo fondamentale è giocato da particolari punti di Heegner su X_{N^+,N^-} (e su E). Vediamone rapidamente la definizione. Per cominciare, se $n \in \mathbb{N}$ sia $\mathcal{O}_{p^n} := \mathbb{Z} + p^n\mathcal{O}_K$ l'ordine di $\mathcal{O}_K$ di conduttore p^n. Per ogni $n \geq 0$ esistono immersioni $f : K \hookrightarrow B$ tali che $f^{-1}(\mathcal{R}) = \mathcal{O}_{p^n}$, dette immersioni ottimali di $\mathcal{O}_{p^n}$ in $\mathcal{R}$, e a meno di coniugazione per elementi di $\mathcal{R}^\times$ vi è un numero finito di immersioni di questo tipo. Per f come sopra, indichiamo con la stessa lettera anche l'estensione $\mathbb{C} = K \otimes_{\mathbb{Q}} \mathbb{R} \hookrightarrow B_\infty = M_2(\mathbb{R})$. Allora $f(\mathbb{C}^\times) \subset GL_2^+(\mathbb{R})$ agisce su $\mathcal{H}$, e la sua azione ha un unico punto fisso τ_f su $\mathcal{H}$; inoltre l'immagine $[\tau_f]$ di τ_f sulla curva di Shimura $X_{N^+,N^-} = \mathcal{R}^1\backslash\mathcal{H}$ dipende solo dalla classe di coniugazione di f modulo $\mathcal{R}^\times$. Diremo che $[\tau_f]$ è un *punto di Heegner* di conduttore p^n su X_{N^+,N^-} associato a K. La teoria della moltiplicazione complessa permette di concludere che il punto $[\tau_f]$ è definito sopra il ring class field H_n di K di conduttore p^n. Come sottolineato in [1, §2.4], è possibile selezionare un sistema compatibile $\{x_n\}$ di punti di Heegner su X_{N^+,N^-}; in questo caso, l'aggettivo "compatibile" indica che i punti x_n soddisfano particolari relazioni nel gruppo $\mathrm{Div}(X_{N^+,N^-})$ esprimibili in termini di traccia galoisiana e azione di operatori di Hecke. Poniamo quindi $y_n := \pi_E(x_n) \in E(H_n)$ per ogni $n \geq 0$, e infine $a_n := \mathrm{Tr}_{H_{d(n)}/K_n}(y_{d(n)}) \in E(K_n)$ per ogni $n \geq 1$, ove $d(n) := \min\{m \in \mathbb{N} \mid \mathbb{K}_\mathrm{n} \subset \mathbb{H}_\mathrm{m}\}$.

Seguendo [1], introduciamo la nostra funzione L p-adica $\mathscr{L}_p(E/K)$ come segue. Conservando la notazione adottata in precedenza, sia

$$\theta_n := \sum_{\sigma \in G_n} a_n^\sigma \otimes \sigma^{-1} \in E(K_n) \otimes_\mathbb{Z} \mathbb{Z}[G_n] \subset E(K_\infty) \otimes_\mathbb{Z} \mathbb{Z}[G_n]$$

per ogni $n \geq 1$. Poiché gli elementi θ_n sono compatibili rispetto alle proiezioni naturali, possiamo dare la seguente

DEFINIZIONE 1. – *L'elemento*

$$\mathscr{L}_p(E/K) := \varprojlim \theta_n \in E(K_\infty) \otimes \mathbb{Z}[\![G_\infty]\!]$$

è la funzione L p-adica anticiclotomica *associata a* E/K.

Sia I_n l'ideale di aumentazione in $\mathbb{Z}[G_n]$, i.e. il nucleo della mappa di aumentazione $\mathbb{Z}[G_n]\mathbb{Z}$ tale che $\gamma_n \mapsto 1$. Se $\rho \in \mathbb{N}$, diciamo che l'elemento θ_n *si annulla di ordine almeno* ρ se $\theta_n \in E(K_\infty) \otimes I_n^\rho$, e diciamo che $\mathscr{L}_p(E/K)$ *si annulla di ordine almeno* ρ se θ_n si annulla di ordine almeno ρ per ogni $n \geq 1$. L'*ordine di annullamento* di $\mathscr{L}_p(E/K)$ è il più grande ρ tale che $\mathscr{L}_p(E/K)$ si annulla di ordine almeno ρ. Come conseguenza formale delle definizioni si prova innanzitutto la

PROPOSITION 1. – $\mathrm{ord}\,\mathscr{L}_p(E/K) \geq 1$.

Motivati dalla Proposizione 2, concentriamo la nostra attenzione sulla "derivata prima" di $\mathscr{L}_p(E/K)$, che definiamo come la sua proiezione $\mathscr{L}'_p(E/K)$ sul quoziente $E(K_\infty) \otimes I/I^2$, ove $I := \varprojlim I_n$ è l'ideale di aumentazione in $\mathbb{Z}[\![G_\infty]\!]$.

Sia $a_K := \mathrm{Tr}_{H_0/K}(y_0) \in E(K)$ il "punto di Heegner elementare" su E, e definiamo l'*invariante* $\mathfrak{L}$ associato a E come

$$\mathfrak{L}_p(E) := \frac{\mathrm{rec}_p(q)}{\mathrm{ord}_p(q)},$$

dove q è il periodo di Tate di E in p, $\mathrm{rec}_p : \mathbb{Q}_p^\times \to \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ è (essenzialmente) la mappa di reciprocità in p della teoria locale dei campi di classe, e ord_p è l'usuale valutazione p-adica. Enunciamo adesso il risultato principale della tesi.

TEOREMA 1. – *A meno di un fattore non nullo esplicitamente calcolabile, l'uguaglianza*

$$\mathscr{L}'_p(E/K) = \mathfrak{L}_p(E) \cdot a_K \tag{3}$$

è valida in $E(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p$.

È evidente che la relazione 3, che esprime la derivata $\mathscr{L}'_p(E/K)$ in termini del punto di Heegner a_K, rappresenta effettivamente un analogo della formula di Gross e Zagier per la funzione $\mathscr{L}_p(E/K)$. Si osservi che $\mathfrak{L}_p(E)$ è un invariante non nullo della classe di $\mathbb{Q}_p$-isogenia di E, e ricorda da vicino l'invariante $\mathscr{L}_p(\mathscr{E})$ definito da Mazur, Tate e Teitelbaum in [4]. Ancora, $\mathscr{L}'_p(E/K) = 0$ se a_K è di torsione.

La dimostrazione del Teorema 2 distingue due casi: a_K non di torsione e a_K di torsione. Nel primo caso, sfruttando risultati ormai classici di Kolyvagin sul gruppo di Mordell-Weil e sul gruppo di Shafarevich-Tate di E/K si prova che il pro-p-gruppo di Selmer $S_p(E/K)$ di E/K, limite proiettivo rispetto alla moltiplicazione per p dei p^n-gruppi di Selmer di E/K, è uno $\mathbb{Z}_p$-modulo libero di rango uno. Tale modulo si identifica con $E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_p$. D'altra parte, argomenti di tipo coomologico e geometrico (buona riduzione in caratteristica p dei punti di Heegner a_n) mostrano che la derivata prima $\mathscr{L}'_p(E/K)$ vive naturalmente in $S_p(E/K)$, da cui si deduce l'esistenza di una costante p-adica κ tale che $\mathscr{L}'_p(E/K) = \kappa \cdot a_K$ in $E(K) \otimes \mathbb{Q}_p$. Infine, si "forza" la costante κ ad avere la forma richiesta applicando opportunamente la teoria di Jochnowitz delle congruenze fra valori speciali di funzioni L, e più precisamente i recenti risultati di Bertolini e Darmon sulla congettura principale di Iwasawa per curve ellittiche su $\mathbb{Z}_p$-estensioni anticiclotomiche (cf. [2]).

Concludiamo osservando che l'annullamento di $\mathscr{L}'_p(E/K)$ quando a_K è di torsione è equivalente all'annullamento di certe classi di coomologia di Galois definite in termini di "derivate di Kolyvagin" dei punti di Heegner a_n, la cui dimostrazione si affronta con tecniche algebriche dovute sostanzialmente a Kolyvagin.

BIBLIOGRAFIA

[1] BERTOLINI M. e DARMON H., *Heegner points on Mumford-Tate curves*, Invent. Math. **126** (1996), 413-456.

[2] BERTOLINI M. e DARMON H., *Iwasawa's Main Conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions*, Ann. of Math. (2) **162** (2005), 1-64.

[3] GROSS B. H. e ZAGIER D. B., *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225-320.

[4] MAZUR B., TATE J. e TEITELBAUM J., *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1-48.

[5] WILES A., *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), 443-551.

Dipartimento di Matematica, Università di Milano
e-mail: stevigni@mat.unimi.it
Dottorato in Matematica (sede amministrativa: Milano Università) - Ciclo XVI
Direttore di ricerca: Prof. Massimo Bertolini, Università di Milano