Матняк С.В.
м. Хмельницький, Україна

ДОВЕДЕННЯ СПРАВЕДЛИВОСТІ ГІПОТЕЗИ БЕРЧА І СУІННЕРТОНА-ДАЙЄРА

УДК 511.3

В статті дається доведення справедливості гіпотези Берча і Суіннертона-Дайєра. Для доведення справедливості цієї гіпотези використовується доведена раніше в роботі [3] гіпотеза Рімана, а також теорія комплексної змінної і теорія групи Галуа.

Ключові слова: гіпотеза Берча і Суіннертона– Дайєра, функція Хассе-Вейля, гіпотеза Рімана, група Галуа, комплексний степеневий ряд.

Вступ

Берч і Суіннертон-Дайєр, на початку 1960-х років, запропонували, що ранг r групи еліптичної кривої E над Q рівний порядку нуля дзета-функції Хассе-Вейля $L(E,s)$ в точці $s=1$. Більш детально гіпотеза твердить, що існує ненульова границя $B_E = \lim\limits_{s\to 1} \dfrac{L(E,s)}{(s-1)^r}$, де значення B_E залежить від тонких арифметичних інваріантів кривих.

Найбільш важливим частковим результатом станом на 2011 рік залишається доведена в 1977 році Джоном Коутсом і Ендрю Уайлсом твердження, справедливе для великого класу елліптичних кривих про те, що коли крива F містить нескінченно багато раціональных точок, то $L(E,s)=0$.

Гіпотеза є єдиним відносно простим загальним методом обчислення рангу еліптичних кривих.

1. Постановка задачі (гіпотеза)

Вважаємо, що E – деяка еліптична крива, визначена над Q. Тоді ранг групи E, r_E рівний порядку нуля L – функції $L(E,s)$ в точці $s=1$.

Рішення. Нехай E – еліптична крива, визначена над Q рівнянням:

$$x_0 x_2^2 = x_1^2 - A\cdot x_0^2 \cdot x_1 - B\cdot x_0^2,\ \ A,B\in Q. \tag{1}$$

Аффіне рівняння одержимо, поклавши $x=\dfrac{x_1}{x_0}$ і $y=\dfrac{x_2}{x_0}$:

$$y^2 = x^3 - A\cdot x - B. \tag{2}$$

Перетворення $(x,y)\to(c^2x, c^2y)$ переводе це рівняння в:

$$y^2 = x^3 - c^4 Ax - c^6 B. \tag{3}$$

Таким чином, з самого початку можна вважати,що $A,B\in Z$. Число $\Delta = 16\left(4\cdot A^2 - 27B^2\right)$ називається дискримінантом кривої E. Як ми бачимо, $\Delta\neq 0$.

Нехай $p\in Z$ деяке просте число, і розглянемо порівняння:

$$y^2 = x^3 - Ax - B(p),$$

або, що еквівалєнтно, рівнянню:

$$y^2 = x^3 - \overline{A}x - \overline{B},\ \ \overline{A},\overline{B}\in Z/pZ = F_p. \tag{4}$$

Це рівняння визначає еліптичну криву E_p над F_p, тільки тоді коли $(p,\Delta)=1$. В дальнійшому будуть розглядатися тільки такі прості числа, коли явно не обувмовлене протилежне. Крива E_p називається редукцією кривої E по модулю p.

Нехай N_{p^m} позначає число точок в $E_p\left(F_{p^m}\right)$. Тоді ми можемо розглянути дзета-функцію:

$$Z\left(E_p,u\right) = \exp\left(\sum_{m=1}^{\infty} N_{pm}\frac{u^m}{m}\right). \tag{5}$$

Використовуючи теорему Рімана–Роха, можно записати:

$$Z(E_p,u)=\frac{1-a_p u+pu^m}{(1-u)\cdot(1-pu)},\quad a_p\in Z. \tag{6}$$

Для $a_p^2\le 4p$, запишемо:

$$1-a_p u+pu^2=(1-\pi\cdot u)(1-\overline{\pi}\cdot u), \tag{7}$$

Де $\overline{\pi}$ – комплексно спряжене с π. Видно, що $\pi\cdot\overline{\pi}=p$, $a_p=\pi+\overline{\pi}$.

Крім того, $|\pi|=|\overline{\pi}|=\sqrt{p}$. Це є << гіпотеза Рімана>> для еліптичної кривої над F_p.

Логарифмічно дифференціюємо (5) і (6), і враховуючи (7) і прирівнюючи коефіцієнти, одержимо:

$$N_{pm}=p^m+1-\pi^m-\overline{\pi}^m. \tag{8}$$

Зокрема, $N_p=p+1-a_p$. Таким чином,шляхом розрахунку N_p, ми визначаємо a_p. Оскільки π і $\overline{\pi}$ є корені рівняння $T^2-a_p\cdot T+p=0$, то рівняння (8) визначає N_{pm} для всіх $m\ge 1$.

Замінимо змінну u на p^{-s} і одержимо:

$$\varsigma(E_p,s)=\frac{1-a_p\cdot p^{-s}+p^{1-s}}{(1-p^{-s})\cdot(1-p^{1-s})}, \tag{9}$$

Ми визначили $\varsigma(E_p,s)$ для простих чисел $(p,\Delta)=1$. Коли p/Δ, то ми вважаємо:

$$\varsigma(E_p,s)=\frac{1}{(1-p^{-s})\cdot(1-p^{1-s})}.$$

Тепер, ввівши локальну дзета-функцію для всіх простих чисел p, ми визначимо глобальну дзота-функцію просто, як добуток локальних дзета-функцій:

$$\varsigma(E,s)=\prod_{з}\varsigma(E_p,s). \tag{10}$$

Із визначення ми бачимо, що

$$L(E,s)=\frac{\varsigma(s)\cdot\varsigma(1-s)}{\varsigma(E,s)}. \tag{11}$$

Запишемо функцію (11) у вигляді:

$$L(E,s)=\frac{\varsigma(s)\cdot\varsigma(1-s)}{\varsigma(E,s)}=\frac{-0{,}5\cdot k_1\cdot\prod_p(1-p^{-s})\cdot(1-p^{-1-s})}{\prod_p(1-a_p p^{-s}+p^{1-2s})}, \tag{12}$$

де k_1 значення функції $\frac{1}{\varsigma(1)}$. Функція $\varsigma(1)$ збігається – теорема 5 [3, ст.9].

Теорема 1. Функція $L(E,s)$ при $s=1$ буде дорівнювати нулю $(L(E,s)=0)$ при всіх значеннях p.

Доведення. Визначимо:

$$k_1=\frac{1}{\varsigma(1)}=\sum_{n=1}^{\infty}M(n)\cdot\left(\frac{1}{n+1}-\frac{1}{n}\right)=\sum_{n=1}^{\infty}2{,}25\cdot\sqrt{N}\cdot\left(\frac{n-1-n}{(n+1)n}\right)=-2{,}25\cdot\sum_{n=1}^{\infty}\frac{\sqrt{N}}{n^2+n}\le -2{,}25\int_{n=1}^{\infty}\frac{dn}{n^{\frac{3}{2}}}=4{,}5.$$

Значення функції $\varsigma(1)=\frac{1}{k_1}$ знаходиться в границях $\frac{1}{4{,}5}<\varsigma(1)<1$ $\frac{1}{4{,}5}<\varsigma(1)<1$.

Тоді запишемо, що при $s=1$:

$$L(E,s)=\frac{\varsigma(s)\cdot\varsigma(1-s)}{\varsigma(E,s)}=\frac{-0{,}5\cdot\prod_p(1-p^{-s})\cdot(1-p^{-1-s})}{\prod_p(1-a_p p^{-s}+p^{1-2s})}, \tag{13}$$

а при $s=1+\varepsilon$ і при $1<k_1<4{,}5$ будемо мати:

$$L(E,s)=-0{,}5\cdot \underset{з}{П}\frac{\left(pp^{\varepsilon}-1\right)\cdot\left(p^{\varepsilon}-1\right)}{\left(pp^{\varepsilon}-a_p p^{\varepsilon}+1\right)};$$

тому що з леми 1 [9, ст.33].

"При $\operatorname{Re}s>0$, $N>>1:\varsigma(s)=\sum_{n=1}^{N}\frac{1}{n^s}+\frac{N^{1-s}}{s-1}-\frac{1}{2}\cdot N^{-3}+s\cdot\int_{N}^{\infty}\frac{\frac{1}{2}-\{u\}}{u^{s+1}}du$" одержимо, що $\varsigma(0)=-0{,}5$; при $\varepsilon\to 0$ одержимо:

$$L(E,s)=-0{,}5\cdot\lim_{\varepsilon\to 0}\underset{p}{П}\left(\frac{pp^{\varepsilon}-1}{pp^{\varepsilon}+1-a_p\cdot p^{\varepsilon}}\right)\cdot\left(p^{\varepsilon}-1\right)=-0{,}5\cdot\underset{p}{П}\left(\frac{p-1}{p+1-a_p}\right)\cdot\lim_{\varepsilon\to 0}\left(p^{\varepsilon}-1\right)=0.\cdot$$

Тому що, при $\varepsilon\to 0$ $\left(p^{e}-1\right)\to 0$, а $\left(\frac{p-1}{p+1-a_p}\right)>1$ і при $p\to\infty$ $\lim_{p\to\infty}\frac{p-1}{p+1-a_p}=1.$

Теорема доведена.

2. Порядок нуля

Коли функція $L(E.s)$, яка тотожно не дорівнює нудю , голоморфна в області D, і рівна нулю в точці a цієї області, то разклад її для деякого околу точки a має вигляд:

$$L(E,s)=c_1\cdot(s-1)+c_2\cdot(s-1)^2+\ldots+c_n\cdot(s-1)^n+\ldots, \tag{14}$$

оскільки $c_0=L(E,1)=0$.

Очевидно, всі коефіцієнти c_n розкладу (14) не можуть дорівнювати нулю, оскільки в цьому випадку функція $L(E,s)$, дорівнює нулю всюду в деякому околі точки a, була би за теоремою єдинного розв'язку тотожним нулем в області D. Таким чином, серед коефіцієнтів c_n $(n=1,2,3,\ldots)$ є відмінні від нуля; позначимо через n, де $n>>1$ □ найменший номер таких коефіцієнтів.

Тоді будемо мати:

$$c_1=c_2=\ldots=c_{n-1}=0,\ c_n\neq 0.$$

Отже, розкладання (14) приймає вигляд:

$$L(E,s)=c_n\cdot(s-1)^n+c_{n+1}(s-1)^{n+1}+\ldots, \tag{15}$$

де $c_n\neq 0$.

В цьому випадку точка a є нуль порядку m для функції $L(E,s)$ в точці $s=1$.

3. Побудова групи Галуа еліптичної кривої

Нехай еліптична крива E визначена над полем K і нехай L □ розширення поля K. І нехай далі, σ є ізоморфізмом поля L, не обов'язково тотожним на K [4, ст. 27]. Він визначає криву E^{σ}, одержану застосуванням σ до коефіцієнтів рівняння, яке задає криву E. Наприклад, коли крива E задана рівнянням:

$$y^2=x^3-Ax-B,$$

,

то E^{σ} визначається рівнянням:

$$y^2=x^3-A^{\sigma}x-B^{\sigma}.$$

Коли P, Q є точками кривої E в полі L, то має місце формула:

$$(P+Q)^{\sigma}=P^{\sigma}+Q^{\sigma}.$$

Сума в лівій частині відноситься до довання на E, а сума в правій частині відноситьсядо додавання на E^{σ}. Рівність очевидним чином випливає з того, що алгебраїчна формула додавання задається

раціональними функціями від координат з коефіцієнтами з поля K. До того ж, коли $P=(x,y)$, то $P^{\sigma}=(x^{\sigma},y^{\sigma})$ отримується застосуванням σ до координат.

Зокрема, припустимо, що P є точкою скінченного порядку, тому що $NP=0$. Оскільки точка O раціональна над K, то для будь якого ізоморфізма σ поля L над K маємо $NP^{\sigma}=0$ і, отже, P^{σ} також є точкою порядку N. Далі оскільки число точок порядку N скінченно, звідси випливає, що всі вони є алгебраїчні над K (тобто їх координати алгебраїчні над K).

Коли $P=(x,y)$, то позначимо $K(P)=K(x,y)$ розширення поля K, одержане приєднанням координат точки P. Аналогично $k(E_N)$ позначимо композит полів $K(P)$ для всіх $P\in E_n$. Підкреслимо, що ми розглядаємо всі точки скінченного порядку як точки з координаиами з фіксованного алгебраїчного замикання поля K, яке позначимо ${}^{a}K$ або K_a.

Зроблене вище заувпаження показує, що група Галуа Gal (K_s/K) діє як група елементів множини E_N. Отже, $K(E_N)$ є нормальне розширення поля K і є розширенням Галуа, коли N не ділиться на характеристику поля K. Назвемо $K(E_N)$ полем точок порядку N кривої A над полем K.

Крім того, коли σ є автоморфізм поля $K(E_N)$ над K і коли $\{t_1\}$, $\{t_1,t_2\}$,..., $\{t_1,t_2,...,t_r\}$ □ бази E_N над Z/nZ, то σ можна представити матрицями:

$$(a),\ \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix},\ ...,\ \begin{pmatrix} a_{1,1} & ... & a_{1,r} \\ & & \\ a_{r,1} & ... & a_{r,r} \end{pmatrix} \quad \text{такими, що}$$

$$(\sigma\cdot t_1),\quad \begin{pmatrix} \sigma\cdot t_1 \\ \sigma\cdot t_2 \end{pmatrix}=\begin{pmatrix} a_{11}t_1+a_{1,2}t_2 \\ a_{2,1}t_1+a_{2,2}t_2 \end{pmatrix}\cdot\begin{pmatrix} t_1 \\ t_2 \end{pmatrix} \quad \text{т.д.}$$

Таким чином, ми одержали інъєктивний гоморфізм:

$$Gal(K(E_N)/K)\to GL(n,Q).$$

Теорема 2 (Морделла) [1, ст. 367]. Нехай E – деяка еліптична крива, визначена над Q. Тоді $E(Q)$ – скінченно породжена абелева група.

Теорема 3 [1, ст. 368]. Нехай E – деяка еліптична крива, визначена над Q. Тоді $E(Q)$. ізоморфна одній із наступних груп Z/mZ при $m\le 10$ або $m=12$, $Z/2Z\oplus Z/2mZ$ при $m\le 4$.

4. Теорема 4 (Відповідності між рангом групи і порядком нуля)

Нехай L/K скінченне розширення Галуа степені n і $\sigma_1,\sigma_2,...,\sigma_n$ □ елементи його групи G, де $\sigma_1=(s-1)$, $\sigma_2=(s-1)^2$,..., $\sigma_n=(s-1)^n$. Тоді існує елемент $\omega\in L$, такий, що $\sigma_1\cdot\omega,\sigma_2\cdot\omega,...,\sigma_n\cdot\omega$ утворюють базис L над K, тоді елементи групи Галуа переводять $(n-1)$ перших коефіцієнтів ряду (14) в нулі ряду (15). І отже ранг групи Галуа буде дорівнювати порядку нулів ряду $L(E,.s)$.

Доведення. Для будь-якого $\sigma\in G$ нехай X_{σ} □ змінна і $t_{\sigma,\tau}=X_{\sigma^{-1}\tau}$. Покладемо $X_i=X_{\sigma_i}$. Де $X_i=(s-1)_{\sigma_i}$, а $t_{\sigma\tau}=(s-1)_{\sigma^{-1}\tau}$.

Нехай $f(x_1,x_2,...,x_n)=\det(t\sigma_i,\sigma_j)$.

Тоді f не є тотожним нулем, що видно, то по теоремі 19 [2, ст. 259] визначник не може бути рівним нулю при всіх $x\in L$, коли ми в f підставим $\sigma_i(x)$ замість X_i . Тому, існує елемент $\omega\in L$, для якого

$$\det(\sigma_i^{-1}\cdot\sigma_j(\omega))\neq 0.$$

Позначимо коефіцієнти степеневого ряду (14) через $c_1, c_2, ..., c_{n-1}$. І вважатимемо, що елементи (коефіцієнти степеневого ряду) $c_1, c_2, ..., c_{n-1} \in K$ такі, що:

$$c_1 \cdot \sigma_1(\omega) + c_2 \cdot \sigma_2(\omega) + ... + c_{n-1} \cdot \sigma_n(\omega) = 0.$$

Застосуємо σ_i^{-1} до цього виразу відповідно для кожного $i = 1,2,...,n-1$. Оскільки $c_{i,j} \in K$, ми одержимо систему лінійних рівнянь відносно невідомих c_j і одержимо, що $c_j = 0$ для $i = 1,2,...,n-1$.

І, отже, ω буде шуканим елементів, в данному випадку $\omega = \frac{1}{s-1}$.

Відповідно до наслідку леми 2.3 [10, ст.144] :"Нехай $L-$ скінченне розширення поля K з абелевою групою Галуа G степені, яка ділить n. Тоді група G є прямий добуток циклічних підгруп $G_1, G_{2,}..., G_r$. Нехай для кожного i через L_i буде позначено підполе, нерухоме для підгрупи $G_1 \times G_2 \times ... \times G_r$; тоді $G(L_i / K) = G_i$, $L_i = K(\alpha_i)$, де $\alpha_i^n = a_i \in K$ і $L = K(\alpha_1, ..., \alpha_n)$".

І леми 2.4 [10, ст.144]. Коли $L-$ нормальне алгебраїчне розширення K з групою Галуа G, то:

$$H^1(G, L^*) = 0.$$

Тоді використовуючи теорему 1 і лему 2.4 можна записати, що при нормальному розширенні група Галуа перетворює ряд (14) в ряд:

$$L(E,1) = c_n(s-1)^n + c_{n+1}(s-1)^{n+1} + ... \quad (16)$$

Використовуючи співвідношення (16) будемо мати, при $n = r_E$:

$$C_{n,E} = \lim_{s \to 1+0} \frac{L(E,1)}{(s-1)^{r_E}} = \lim_{s \to 1+0} \frac{c_n(s-1)^n + c_{n+1}(s-1)^{n+1}}{(s-1)^{r_E}} = c_n.$$

Відповідно до леми 1 і наслідку [9, ст. 33] функція $L(E,s)$ аналітична на всій області $s \in (0,\infty)$, то її можна розкласти в ряд Тейлора по степеням $(s-1)$ і з коефіцієнтами $C_{n,E} = \frac{L^{(n)}(E,1)}{k!} = \frac{B_{n,E}}{k!}$, де $L^{(n)}(E,s)$ –похідна $n-$ го порядку з функції Хассе-Вейля $L(E,s)$. Отже, ранг групи Галуа рівний порядку нулів функції Хассе–Вейля.

Теорема доведена.
Тому гіпотеза Берча і Суіннертона–Дайєра справедлива.

Література

1. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. – М.: Мир, 1987. – 415 с.
2. Ленг С. Алгебра. – М.: Мир, 1968. – 564 с.
3. Матняк С.В. Доведення справидливості гіпотези Рімана // Проблеми трибології. – 2013. – № 2. – С. 43-49.
4. Ленг С. Эллиптические функции. – М.: Наука, 1987. – 311 с.
5. Коблиц Н. Введение в эллиптические кривые и модулярные формы. – М.: Мир, 1988. – 318с.
6. Привалов И.И. Введение в теорию функций комплексного переменного. – М.: Наука, 1984. – 432 с.
7. Коблиц Н. р-адические числа, р-адический анализ и дзета-функции. – М.: Мир, 1982. – 192 с.
8. Ван-дер-Варден Б.Л. Алгебра. – М.:Москва, 1976. – 648 с.
9. Карацуба А.А.. Основы аналитической теории чисел. – М.: УРСС, 2004. – 182 с.
10. Алгебраическая теория чисел. Под ред. Дж. Касселса и А. Фрелиха. □ М.: Мир, 1969. – 483 с.

Поступила в редакцію 09.09.2013

Matnyak S.V. **The proof of the correctness of the conjecture of the Birch and Swinnerton-Dyer.**

The proof of the conjecture of the Birch and Swinnerton-Dyer *presents* in the *paper*. The Riemann's hypothesis on the distribution of non-trivial zeros of the zeta function of Riemann, previously proven, using to prove this hypothesis. The theorem proved about the behavior of the L-function curve E for $s \to 1$. It is shown that the L-function of the curve E tends to zero for any prime unpaired integers. It is shown that the function can be expanded in a power series of the holomorphic field. The theorem proved on conformity of the basis of the Galois group and the number of zero coefficients of the power series. The result proved the conjecture of Birch and Swinnerton-Dyer.

Key words: the hypothesis of Birch and Swinnerton-Dyer, function of Hasse-Weil, Riemann's hypothesis, the Galois group, the complex power series.

References

1. Ajerljend K., Rouzen M. Klassicheskoe vvedenie v sovremennuju teoriju chisel. M.: Mir, 1987. 415 s.
2. Leng S. Algebra. M.: Mir, 1968. 564 s.
3. Matnjak S.V. Dovedennja spravidlivosti gipotezi Rimana. Problemi tribologiї. 2013. № 2. S. 43-49.
4. Leng S. Jellipticheskie funkcii. M.: Nauka, 1987. 311 s.
5. Koblic N. Vvedenie v jellipticheskie krivye i moduljarnye formy. M.: Mir, 1988. 318s.
6. Privalov I.I. Vvedenie v teoriju funkcij kompleksnogo peremennogo. M.: Nauka, 1984. 432 s.
7. Koblic N. r-adicheskie chisla, p-adicheskij analiz i dzeta-funkcii. M.: Mir, 1982. 192 s.
8. Van-der-Varden B.L. Algebra. M.:Moskva, 1976. 648 s.
9. Karacuba A.A.. Osnovy analiticheskoj teorii chisel. M.: URSS, 2004. 182 s.
10. Algebraicheskaja teorija chisel. Pod red. Dzh. Kasselsa i A. Freliha. M.: Mir, 1969. 483 s.