УДК 513.6:511.7

М. В. Піменов

Про коливання знака залишка в формулі для числа точок алгебраїчної кривої

Нехай X — незвідна проективна крива роду g, визначена над полем F_q, яке складається з $q = p^f$ елементів (p — просте число), і $Z = Z(t, X)$ — дзета-функція многовиду X над полем F_q. Тоді

$$\frac{d}{dt}(\log Z) = \sum_{s=1}^{\infty} N_s t^{s-1},$$

де через N_s позначено кількість точок многовиду X, раціональних над розширенням степеня s поля F_q. Відомо (див. [1]), що має місце

$$Z(t, X) = \frac{(1-\omega_1 t)(1-\tilde{\omega}_1 t)\ldots(1-\omega_g t)(1-\bar{\omega}_g t)}{(1-t)(1-qt)},$$

де $\omega_1, \ldots, \omega_g$ цілі алгебраїчні числа, модуль яких дорівнює $q^{1/2}$, $\bar{\omega}_1, \ldots, \bar{\omega}_g$ — їх комплексно спряжені.

Для кількості точок N_s справедлива формула

$$N_s = 1 + q^s - \omega_1^s - \ldots - \omega_g^s - \bar{\omega}_1^s - \ldots - \bar{\omega}_g^s.$$

Кількість точок проективної прямої в розширенні степеня s поля F_q дорівнює $1+q^s$. Тоді величину $\Theta_s = -\omega_1^s - \ldots - \omega_g^s - \bar{\omega}_1^s - \ldots - \bar{\omega}_g^s$ можна розглядати як відхилення числа точок кривої X в розширенні степеня s поля F_q від числа точок проективної прямої.

Розглянемо Θ_s в такому вигляді:

$$\Theta_s = -2q^{s/2}(\cos 2\pi s\varphi_1 + \ldots + \cos 2\pi s\varphi_g);$$
$$\omega_k = q^{1/2}\exp i2\pi\varphi_k,\ k=\overline{1,g},\ 0 \leqslant \varphi_k < 1. \quad (1)$$

Виникає запитання, чи змінює свій знак залишок Θ_s при змінюванні s, чи може з деякого значення s_0 величина Θ_s стає знакосталою. Первісно така задача виникла в роботі О. Н. Введенського [2] при доведенні мономорфності гомоморфізма Тейта—Шафаревича для еліптичних кривих з ненульовим інваріантом Хассе, в якій було використано існування такого розширення степеня s поля F_q, в якому еліптична крива має більше $1+q^s$ точок. Те, що еліптична крива має точок більше $1+q^s$, еквівалентно тому, що $\Theta_s = -2q^{s/2}\cos 2\pi s\varphi_1 > 0$ в деякому розширенні степеня s поля F_q. В цій роботі буде доведено коливання знака Θ_s для деякого класу гіпереліптичних кривих. Результат роботи можна сформулювати в такій теоремі.

Теорема 1. *Нехай $\varphi_1, \ldots, \varphi_g$ відмінні від 0. Тоді величина Θ_s змінює свій знак, коли s приймає значення* $1, 2, 3, \ldots$.

Розглянемо випадок, коли в формулі (1) величини $\varphi_1, \ldots, \varphi_g$ ірраціональні, множина $\{1, \varphi_1, \ldots, \varphi_g\}$ лінійно незалежна над полем Q раціональних чисел. Тоді можна використати такий результат (див. [3, 4]) з теорії діофантових наближень: послідовність $(\{s\varphi_1\}, \ldots, \{s\varphi_g\})_{s=1,2,\ldots}$ при вказаних вище умовах рівномірно розподілена в g-вимірному торі T^g (тут $\{x\}$ позначає дробову частину числа x), і тим більше ця послідовність всюди щільна в T^g. Через те що функція $\Sigma(x_1, \ldots, x_g) = \cos 2\pi x_1 + \ldots + \cos 2\pi x_g$ приймає значення різних знаків і в кожному околі точки $(x_1, \ldots, x_g) \in T^g$ є нескінченно багато точок послідовності $(\{s\varphi_1\}, \ldots, \{s\varphi_g\})_{s=1,2,\ldots}$, випливає коливання знака. Однак в загальному випадку серед кутів $\varphi_1, \ldots, \varphi_g$ можуть бути як ірраціональні числа з деякою лінійною залежністю над полем Q раціональних чисел, так і раціональні числа. Тому для доведення коливання знака в послідовності Θ_s буде використано прийом, який описується в наведених нижче твердженнях і основується на використанні рівномірного розподілу послідовності чисел $(\{s\alpha_1\}, \ldots, \{s\alpha_l\})_{s=1,2,\ldots}$ в l-вимірному торі T^l (коли величини $\alpha_1, \ldots, \alpha_l$ ірраціональні і незалежні) і на використанні специфічних властивостей ряду $\sum\limits_{s=1}^{\infty} \frac{\cos s\alpha}{s}$.

Цей прийом включає і той випадок, коли всі значення $\varphi_1 \ldots, \varphi_g$ раціональні, тобто коли неможливо застосувати результати рівномірного розподілу з діофантових наближень.

Запровадимо таке означення. Нехай задані $(a_s)_{s=1,2,\ldots}$, $a_s \in R$, послідовність дійсних чисел, довільне число $\varepsilon \in R$. Позначимо $N(x, \varepsilon)$ — число чисел $s \leqslant x$ таких, що $a_s < \varepsilon$. Якщо для всяко о ε існує границя

$$F(\varepsilon) = \lim_{x\to\infty} \frac{N(x, \varepsilon)}{x},$$

то функцію $F(\varepsilon)$ назвемо функцією розподілу послідовності $(a_s)_{s=1,2,3,\ldots}$.

Нехай $\rho(\varepsilon) = F(\varepsilon) - F(0)$ — густина розподілу послідовності $(a_s)_{s=1,2,\ldots}$ на інтервалі $[0, \varepsilon)$. Коливання знака залишку Θ_s, як це видно з формули (1), випливає з коливання знака величини $\Sigma_s = \cos 2\pi s\varphi_1 + \ldots + \cos 2\pi s\varphi_g$.

Коливання знака Σ_s, в свою чергу, випливає з таких тверджень.

Твердження 1. *Нехай маємо ряд вигляду*

$$\sum_{s=1}^{\infty} \frac{a_s}{s}, \tag{2}$$

де всі a_s, за виключенням скінченного числа, задовольняють умову $a_s \geqslant 0$, і нехай для послідовності $(a_s)_{s=1,2,\ldots}$ існує функція розподілу $F(\varepsilon)$. Тоді необхідною умовою збіжності ряду (2) є $\rho(\varepsilon) = 1$ для всякого $\varepsilon > 0$.

Твердження 2. *Розглянемо послідовність* $(\Sigma_s)_{s=1,2,\ldots}$. *Для цієї послідовності існує функція розподілу* $F(\varepsilon)$ *і таке* $\varepsilon = \varepsilon_0 > 0$, *для якого* $\rho(\varepsilon) = F(\varepsilon) - F(0) < 1$.

Доведемо коливання знака Θ_s з тверджень 1,2 від супротивного: нехай $\Sigma_s \geqslant 0$ (або $\Sigma_s \leqslant 0$) для всіх досить великих s. Розглянемо ряд (2) з коефіцієнтами $a_s = \Sigma_s$, коли $\Sigma_s \geqslant 0$ при всіх досить великих s (випадок $\Sigma_s \leqslant 0$ розглядається з $a_s = -\Sigma_s$). Цей ряд збігається за ознакою Діріхле. З другого боку, з тверджень 1,2 випливає його розбіжність. Отримана суперечність доводить неможливість сталості знака Θ_s. Теорему 1 доведено.

Доведення твердження 1. Доведення ведемо від супротивного: нехай для деякого $\varepsilon > 0$ густина $\rho(\varepsilon) < 1$, а ряд (2) збігається. Зрозуміло що скінченне число початкових від'ємних a_s не впливають на збіжність (2) і тому всі $a_s \geqslant 0$. Розглянемо відрізок ряду (2):

$$R^1_{n_1} = \frac{a_1}{1} + \frac{a_2}{2} + \ldots + \frac{a_{n_1}}{n_1}.$$

За визначенням густини ρ серед чисел $a_1, \ldots, a_{n_1}$ є $(1 - \rho(\varepsilon))\, n_1 + o(n_1$ чисел, які більші або дорівнюють ε. Підставимо в $R^1_{n_1}$ число ε, замість тих значень a_m $(m = 1, 2, \ldots, n_1)$, які більші або дорівнюють ε. Решта a_m $(m = 1, 2, \ldots, n_1)$ покладемо рівними 0. Тоді дістанемо оцінку $R^1_{n_1}$ знизу

$$R^1_n \geqslant \varepsilon\left(\frac{1}{n_1} + \frac{1}{n_1 - 1} + \ldots + \frac{1}{\rho(\varepsilon)\, n_1 + o(n_1)}\right). \tag{3}$$

Застосуємо до (3) формулу Ейлера, за якою $1 + \frac{1}{2} + \ldots + \frac{1}{n} = \log n + C + o(1)$, C — стала Ейлера. При виборі досить великого n_1 дістанемо

$$R^1_{n_1} \geqslant \varepsilon\,(\log n_1 - \log(\rho(\varepsilon)\, n_1 + o(n_1)) + o(1)) =$$
$$= \varepsilon\left(\log\left(\frac{1}{\rho(\varepsilon) + o(1)}\right) + o(1)\right) \geqslant \mu > 0,$$

μ — стала, $0 < \mu < \varepsilon \log \frac{1}{\rho(\varepsilon)}$.

Розглянемо такий відрізок ряду (2):

$$R^2_{n_2} = \frac{a_{n_1+1}}{n_1 + 1} + \ldots + \frac{a_{n_1+n_2}}{n_1 + n_2} \geqslant$$
$$\geqslant \varepsilon\left(\frac{1}{n_1 + n_2} + \ldots + \frac{1}{\rho(\varepsilon)(n_1 + n_2) + o(n_2)}\right).$$

Застосуємо знову формулу Ейлера і виберемо досить велике n_2. Тоді дістанемо

$$R^2_{n_2} \geqslant \varepsilon\,(\log(n_1 + n_2) - \log(\rho(\varepsilon)(n_1 + n_2) + o(n_2)) + o(n_2)) =$$
$$= \varepsilon\left(\log \frac{1 + o(1)}{\rho(\varepsilon) + o(1)}\right) \geqslant \mu > 0.$$

Оскільки процес можна продовжити далі, то дістаємо, що ряд (2) розбігається.

Доведення твердження 2. Припустимо спочатку, що серед $\varphi_1, \ldots, \varphi_g$ є хоча б одне ірраціональне число. Виділимо з $\varphi_1, \ldots, \varphi_g$ максимальну систему ірраціональних чисел S таких, що множина $\{1, S\}$ лінійно незалежна над полем Q раціональних чисел. Нехай $S = \{\varphi_1, \ldots, \varphi_l\}$. Тоді зобразимо Σ_s в такому вигляді:

$$\sum_s = \sum_{\varphi \in S} \cos 2\pi s\varphi + \sum_{\varphi \in Q} \cos 2\pi s\varphi + \sum_{\varphi \in S_1} \cos 2\pi s\varphi. \tag{4}$$

Перший доданок в формулі (4) являє собою суму по тих φ, які належать множині S. Другий доданок — суму по раціональних φ з $\varphi_1, \ldots, \varphi_g$. Третій доданок — це сума по тих ірраціональних φ, які лінійно залежать від $1, \varphi_1, \ldots, \varphi_l$ (S_1 — множина таких φ).

Мета дальших перетворень полягає в тому, щоб використати рівномірний розподіл в T^l послідовності $(\{s\varphi_1\}, \ldots, \{s\varphi_l\})_{s=1,2,\ldots}$. Зобразимо ірраціональне $\varphi \in S_1$ комбінацією

$$\varphi = \frac{1}{b_\varphi} (a_l\varphi_l + \ldots + a_1\varphi_1 + a_0), \tag{5}$$

де $b_\varphi, a_l, \ldots, a_0$ цілі раціональні.

Нехай d — найменше кратне всіх знаменників раціональних φ, і всіх b_φ для залежних $\varphi \in S_1$. Виділимо в послідовності $(\Sigma_s)_{s=1,2,\ldots}$ підпослідовності виду $(\Sigma_{r+dt})_{t=0,1,2,\ldots}$ при $0 < r \leqslant d-1$, та підпослідовність $(\Sigma_{dt})_{t=1,2,\ldots}$ при $r = 0$. Доповнимо послідовність $(\Sigma_s)_{s=1,2,3,\ldots}$ елементом Σ_0, що відповідає $s = 0$ (це не впливає на існування функції розподілу та її вигляд), тоді при $0 \leqslant r \leqslant d-1$

$$\sum_{r+dt} = \sum_{\varphi \in S} \cos(2\pi r\varphi + 2\pi d\varphi t) + \sum_{\varphi \in Q} \cos(2\pi r\varphi + 2\pi d\varphi t) + \\ + \sum_{\varphi \in S_1} \cos(2\pi r\varphi + 2\pi d\varphi t).$$

Підставимо в (6) для залежних $\varphi \in S_1$ лінійні комбінації вигляду (5). Зробивши очевидне перетворення, дістанемо

$$\sum_{r+dt} = \sum_{\varphi \in S} \cos(2\pi r\varphi + 2\pi d \cdot \{t\varphi\}) + \sum_{\varphi \in Q} \cos(2\pi r\varphi) + \\ + \sum_{\varphi \in S_1} \cos\left(2\pi r \frac{1}{b_\varphi} (a_l\varphi_l + \ldots + a_0) + 2\pi \frac{d}{b_\varphi} (a_l \{\varphi_l t\} + \ldots + a_1 \{\varphi_1 t\})^1\right). \tag{7}$$

Розглянемо неперервну функцію на l-вимірному торі T^l вигляду

$$\sum\nolimits^r (x_{\varphi_1}, \ldots, x_{\varphi_l}) = \sum_{\varphi \in S} \cos(2\pi r\varphi + 2\pi d x_\varphi) + \sum_{\varphi \in Q} \cos(2\pi r\varphi) + \\ + \sum_{\varphi \in S_1} \cos\left(2\pi r \frac{1}{b_\varphi} (a_l\varphi_l + \ldots + a_0) + 2\pi \frac{d}{b_\varphi} (a_l x_{\varphi_l} + \ldots + a_1 x_{\varphi_1})\right).$$

Тоді побудувавши функцію Σ^r, маємо

$$\Sigma^r (\{t\varphi_1\}, \ldots, \{t\varphi_l\}) = \Sigma_{r+dt}.$$

Зауваження. З останнього видно, що якби вдалось показати, що функції Σ^r приймають значення різних знаків (нехай навіть при різних r), то коливання знака послідовності $(\Sigma_s)_{s=1,2,3,\ldots}$ випливає з рівномірного розподілу $(\{t\varphi_1\}, \ldots, \{t\varphi_l\})$.

Функція розподілу послідовності $(\Sigma_{r+dt})_{t=0,1,2,\ldots}$ має вигляд

$$F_r(x) = \overbrace{\int\int\ldots\int}^{l}_{(\Sigma^r)^{-1}(-\infty,x)} dz_1 \ldots dz_l$$

$((\Sigma^r)^{-1}(-\infty, x)$ — повний прообраз інтервалу $(-\infty, x))$ і являє собою об'єм множини $(\Sigma^r)^{-1}(-\infty, x) \in T^l$.

Функція розподілу всієї послідовності $(\Sigma_s)_{s=1,2,3\ldots}$ має вигляд

$$F(x) = \frac{1}{d}(F_0(x) + \ldots + F_{d-1}(x)).$$

Покажемо тепер, що існує таке $\varepsilon > 0$, для якого $\rho(\varepsilon) < 1$. Існує така точка $(x_1, \ldots, x_l) \in T^l$, що для деякого r $\Sigma^r(x_1, \ldots, x_l) \neq 0$. Візьмемо довільний відкритий окіл $O = (a, b)$ точки $\Sigma^r(x_1, \ldots, x_l)$ такий, що $0 \notin O$. Тоді густина розподілу послідовності $(\Sigma_s)_{s=1,2,3,\ldots}$ на (a, b) дорівнює:

$$F(b) - F(a) = \frac{1}{d}(F_0(b) - F_0(a) + \ldots + F_{d-1}(b) - F_{d-1}(a)) \geqslant$$

$$\geqslant \frac{1}{d}(F_r(b) - F_r(a)) > 0,$$

тому що $F_r(b) - F_r(a)$ — об'єм $(\Sigma^r)^{-1}(O)$ непорожньої відкритої множини. Тепер візьмемо ε таким, щоб перетин інтервалу $[0, \varepsilon)$ з інтервалом (a, b) був порожнім, і тоді $p(\varepsilon) = F(\varepsilon) - F(0) < 1$. Твердження 2 доведено для випадку, коли серед $\varphi_1, \ldots, \varphi_g$ є хоч одне ірраціональне число.

Якщо $\varphi_1, \ldots, \varphi_g$ раціональні, то існування $\varepsilon > 0$ з властивістю $\rho(\varepsilon) < 1$ випливає з скінченності множини різних значень, які приймає послідовність $(\Sigma_s)_{s=1,2,3,\ldots}$

Автор висловлює глибоку подяку О. Н. Введенському за постановку задачі і увагу до роботи.

ЛІТЕРАТУРА

1. A. Weil, Variétés abéliennes et courbes algébriques. Hermann, Paris, 1948.
2. О. Н. Введенский, Эллиптические кривые.— Изв. АН СССР, сер. матем., 1973, т. 37, № 1.
3. Дж. Касселс, Введение в теорию диофантовых приближений, ИЛ, М., 1961.
4. С. Ленг, Введение в теорию диофантовых приближений. «Мир», М., 1970.

Завод «Львівприлад»

Надійшла до редакції
27.VIII 1974 р.