О. М. ВВЕДЕНСЬКИЙ

КРУЧЕННЯ ЕЛІПТИЧНИХ КРИВИХ НАД ЛОКАЛЬНИМ ПОЛЕМ

Нехай k — поле алгебраїчних чисел (тобто конечне розширення поля Q раціональних чисел), A — абелева многовидність, визначена над k, A_k — група точок A, раціональних над k.

Теорема Морделла—Вейля стверджує, що A_k має конечне число твірних.

Питання про рівномірну обмеженість числа твірних A_k (k — фіксоване) залишається відкритим. Існувала думка, що p — компонента абелевої многовидності над локальним полем $\mathfrak{P}$-адичних чисел ($\mathfrak{P}$ ділить p) рівномірно обмежена.

Тут будується контрприклад: A — еліптична крива над Q_p (поповнення Q по простому дивізору p, p — просте число, більше як три); A можна вибрати так, щоб кручення A_{Q_p} ділилось на будь-яке наперед задане число.

0. Нагадаємо деякі співвідношення з теорії еліптичних функцій Вейєрштраса $\mathfrak{P}(u)$ з періодами ω_1 і ω_2, де

$$\mathfrak{P}'(u)^2=4\mathfrak{P}(u)^3-g_2\mathfrak{P}(u)-g_3.$$

Розглянемо функцію

$$\mathfrak{P}(nu)-\mathfrak{P}(u). \tag{1}$$

Вона перетворюється в безмежність при $u=0$ і при всіх тих u^*, які мають вигляд:

$$u^*=\frac{\nu_1\omega_1+\nu_2\omega_2}{n}, \tag{2}$$

де ν_1 і ν_2 — довільні цілі числа.

Визначаємо (при $n>1$)

$$\psi_n(u)^2=n^2\prod^{\nu_1,\,\nu_2}\left[\mathfrak{P}(u)-\mathfrak{P}\left(\frac{\nu_1\omega_1+\nu_2\omega_2}{n}\right)\right], \tag{3}$$

де (ν_1, ν_2) пробігає повну систему лишків по $\bmod n$, за винятком $(0, 0)$ і $\psi_1=1$.

Звідси одержуємо

n непарне: $\psi_n=P_n$;

n парне: $\psi_n=\mathfrak{P}'(u)\,P_n$,

де P_n — ціла раціональна функція від $\mathfrak{P}(u)$ степеня $\frac{n^2-1}{2}$ при n непарному і степеня $\frac{n^2-4}{2}$ при n парному; тоді $P_1=1$; $P_2=-1$;

$$P_3=3\mathfrak{P}(u)^4-\frac{3}{2}g_2\mathfrak{P}(u)^2-3g_3\mathfrak{P}(u)-\frac{g_2^2}{16}; \tag{4}$$

$$P_4=-2\mathfrak{P}(u)^6+\frac{5}{2}g_2\mathfrak{P}(u)^4+10g_3\mathfrak{P}(u)^3+\frac{5}{2}g_2^2\mathfrak{P}(u)^2+$$
$$+\frac{1}{2}g_2g_3\mathfrak{P}(u)+g_3^2-\frac{g_2^3}{32}.$$

Для обчислення ψ_n і P_n існують рекурентні формули:

$$\psi_{m-n}(u)\psi_{m+n}(u)=\psi_{m+1}(u)\psi_{m-1}(u)\psi_n^2(u)-\psi_{n+1}(u)\psi_{n-1}(u)\psi_m^2(u); \tag{5}$$

$$\begin{aligned} P_{2n+1}&=\mathfrak{P}'(u)^4P_{n+2}P_n^3-P_{n+1}^3P_{n-1}, \quad n \text{ парне};\\ P_{2n+1}&=P_{n+2}P_n^3-\mathfrak{P}'(u)^4P_{n+1}^3P_{n-1}, \quad n \text{ непарне}; \end{aligned} \tag{6}$$

$$P_{2n}=-P_n(P_{n+2}P_{n-1}^2-P_{n+1}^2P_{n-2}). \tag{6'}$$

Звідси всі P_n раціонально виражаються через P_1, P_2, P_3 і P_4. З (5) виходить

$$\psi_{m-2}(u)\psi_{m+2}(u)=\psi_{m+1}(u)\psi_{m-1}(u)\psi_2^2(u)-\psi_3(u)\psi_m^2(u). \tag{7}$$

1. Розглянемо криву

$$y^2=(x-\varepsilon)^2(x+2\varepsilon) \tag{8}$$

і покажемо (позначаючи через $\overline{P_n}$ і $\overline{\psi_m}$ відповідні P_n, ψ_m з пункту 0 для цієї кривої), що

$$\begin{aligned} \overline{P}_{2k+1}&=a^{k(2k+1)}(b^k+r_1ab^{k-1}+\ldots+r_ka^k);\\ \overline{P}_{2k+2}&=a^{k(2k+3)}(-b^k+s_1ab^{k-1}+\ldots+s_ka^k), \end{aligned} \tag{9}$$

де $a=x-\varepsilon$, $b=12\varepsilon$; $r_1,\ldots,r_k$, $s_1,\ldots,s_k$ — цілі числа.

Зручніше доводити більш точний результат:
при параметризації

$$x=\varepsilon\left(1+\frac{12t}{(t-1)^2}\right), \quad y=3\varepsilon\sqrt{3\varepsilon}\,\frac{4t(t+1)}{(t-1)^3} \tag{10}$$

додаванню точок на кривій (за винятком особливої точки $x=\varepsilon$, $y=0$) відповідає множення параметрів (за винятком $t=0$ і $t=\infty$, які дають подвійну особливу точку (8)), тому має місце

Лема 1. Має місце при $k\geqslant 1$:

$$\begin{aligned} \overline{P}_{2k+1}&=\frac{b^{2k(k+1)}t^{k(2k+1)}}{(t-1)^{4k(k+1)}}\cdot\frac{t^{2k+1}-1}{t-1};\\ \overline{P}_{2k+2}&=-\frac{b^{2k(k+2)}t^{k(2k+3)}}{(t-1)^{4k(k+2)}}\cdot\frac{t^{2k+2}-1}{t^2-1}. \end{aligned} \tag{11}$$

Доведення. Доводимо по (7):

$$\overline{P}_{2k+3}\overline{P}_{2k-1}=\overline{P}_{2k+2}\overline{P}_{2k}\overline{\psi}_2^4-\overline{P}_3\overline{P}_{2k+1}^2; \tag{12}$$

$$\overline{P}_{2k+4}\overline{P}_{2k}=\overline{P}_{2k+3}\overline{P}_{2k+1}-\overline{P}_3\overline{P}_{2k+2}^2; \tag{13}$$

для $\overline{P}_3$, $\overline{P}_4$, $\overline{P}_5$, $\overline{P}_6$ ці формули дають вирази (11) при відповідних k.

Далі доведення проводимо за індукцією, тому що

$$\overline{\psi}_2^2 = \frac{b^3 t^2 (t+1)^2}{(t-1)^6}, \tag{14}$$

і вважаючи $\overline{P}_{2k-1}$, $\overline{P}_{2k}$, $\overline{P}_{2k+1}$, $\overline{P}_{2k+2}$ заданими по (11), одержуємо, поділивши праву частину співвідношення (12) на $\overline{P}_{2k-1}$, відповідний вираз для $\overline{P}_{2k+3}$, а потім, переходячи до співвідношення (13), одержуємо $\overline{P}_{2k+4}$.

2. Переходимо тепер до основної кривої:

$$y^2 = (x-\varepsilon)^2 (x+2\varepsilon) + \delta p^l. \tag{15}$$

Одержимо деякі відомості про многочлени P_n цієї кривої, використовуючи результати пункту 1. Оскільки (поклавши $\delta p^l = c$)

$$\begin{aligned} &\psi_2^2 = a^2 (b+4a) + 4c, \quad P_3 = a^3 (b+3a) + c(b+12a); \\ &P_4 = a^5 (-b-2a) + ac(-b^2-10ab-40a^2) + 16c^2, \end{aligned} \tag{16}$$

то при вазі a рівній вазі $b=1$, вазі $c=3$, одержуємо:

Лема 2. Всі одночлени, які входять в розклад многочлена P_n від невідомих a, b і c, мають при вазі a рівній вазі $b=1$, вазі $c=3$ одну і ту саму вагу:

$$\frac{n^2-1}{2} \text{ при } n \text{ непарному},$$

$$\frac{n^2-4}{2} \text{ при } n \text{ парному}.$$

Доведення йде за індукцією з використанням (6).

Лема 3. При $k \geqslant 1$

$$P_{2k+1} = \overline{P}_{2k+1} + a^{(k-1)(2k+1)} c (b^{3k-2} + a f_{2k+1}(a, b)) + c^2 g_{2k+1}(a, b, c);$$

$$P_{2k+2} = \overline{P}_{2k+2} + a^{2k^2+k-2} c (-b^{3k-1} + a f_{2k+2}(a, b)) + c^2 g_{2k+2}(a, b, c),$$

де $f_{2k+1}(a, b)$, $f_{2k+2}(a, b)$, $g_{2k+1}(a, b, c)$, $g_{2k+2}(a, b, c)$ — многочлени з цілими коефіцієнтами; всі одночлени в їх розкладах мають при вазі a рівній вазі $b=1$, вазі $c=3$ одну й ту саму вагу, відповідно рівну $3k-3$, $3k-2$, $2k^2+2k-6$, $2k^2+4k-6$.

Доведення. Фактично доведення вимагає лише твердження, що одночлен в розкладі P_n $(n \geqslant 3)$, який містить найменший степінь a серед всіх одночленів, що містять c в першому степені, має вигляд, вказаний в лемі 3. Доведення проводиться з використанням формули (6). Особливість доведення в тому, що одночлени з P_n можуть у формулах (6) частково знищуватися, але їх знищення ми можемо прослідкувати за лемою 1; навпаки, серед одночленів, які містять c в першому степені, знаходиться один, який містить найменший степінь a.

Можна іти далі в тому ж напрямі, розглядаючи одночлени, які містять найменший степінь a серед тих, які містять c^2, і т. д. Після досить складних обчислень за принципом пункту 2 ми приходимо до такого висновку: якщо покласти вагу $a=1$, вагу $c=n$, то всі одночлени, які містять c^2, мають вагу, більшу як $\frac{n^2-4}{2}$ при n парному, і $\frac{n^2-1}{2}$ при n непарному.

Теорема. Існують еліптичні криві, кручення яких ділиться на будь-яке задане наперед число.

Доведення. Візьмемо криву (15), де ε і δ — одиниці з Q_p. Покладемо $x-\varepsilon=up^{\frac{l}{n}}$, де u — невідома одиниця з Q_p (тут припускаємо, що l кратне n) і продовжуємо розв'язок по модулю зростаючих степенів p.

На закінчення висловлюю щиру подяку І. Р. Шафаревічу, під керівництвом якого виконана ця робота.

ЛІТЕРАТУРА

1. H. Weber. Lehrbuch der Algebra, Bd. III. Braunschweig, 1908.

О. Н. ВВЕДЕНСКИЙ

КРУЧЕНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ НАД ЛОКАЛЬНЫМ ПОЛЕМ

(резюме)

На основе исследования уравнений деления на эллиптических кривых, близких (в p-адической топологии) к кривым с особыми точками, доказано, что кручение эллиптических кривых над полем p-адических чисел может делиться на любое наперед заданное число.