ЧЕБЫШЕВСКИЙ СБОРНИК
Том 11 Выпуск 1 (2010)

Труды VII Международной конференции
Алгебра и теория чисел: современные проблемы и приложения,
посвященной памяти профессора Анатолия Алексеевича Карацубы

УДК 511.6

АРИФМЕТИЧЕСКИЕ СВОЙСТВА ФУНКЦИОНАЛЬНЫХ КВАДРАТИЧНЫХ ПОЛЕЙ И КРУЧЕНИЕ В ЯКОБИАНАХ

В. П. Платонов (г. Москва)
platonov@niisi.ras.ru

Пусть K — поле алгебраических чисел, $[K:Q]<\infty$, V^K — множество всех попарно неэквивалентных нормирований поля K.

Пусть $f(x)=x^{2n}+a_{2n-1}x^{2n-1}+...+a_0\in K[x]$ и многочлен $f(x)$ является свободным от квадратов. Обозначим

$$D_f=K[x](\sqrt{f})=\{\alpha+\beta\sqrt{f}|\alpha,\beta\in K[x]\}$$

Элемент $u\in D_f$ называется единицей, если u обратим в D_f. Легко видеть, что $u=\alpha+\beta\sqrt{f}$ обратим в D_f тогда и только тогда, когда $N(u)=\alpha^2-\beta^2 f\in K^*$. Если $u\in K^*$, тогда u называется тривиальной единицей в D_f. Предположим, что D_f обладает нетривиальными единицами. Тогда мультипликативная группа $D_f^*=K^*\times\langle u_1\rangle$, где $\langle u_1\rangle$ - бесконечная циклическая группа. Элемент u_1 называется фундаментальной единицей в D_f.

Проблема существования нетривиальных единиц в D_f является трудной. Это подтверждается следующим простым наблюдением. Пусть J_f — якобиан (якобиево многообразие) кривой X_f, определяемой уравнением $y^2=f(x)$. Поле $L=K(x)(\sqrt{f})$ имеет два бесконечных нормирования $w_1(\infty),w_2(\infty)$. D_f имеет нетривиальную единицу тогда и только тогда, когда образ класса дивизора $w_1(\infty)-w_2(\infty)$ в $J_f(K)$ является элементом конечного порядка. Проблема о кручении в якобианах $J_f(K)$ для $n>2$ является пока неприступной в общем случае. Мы устанавливаем здесь локально-глобальный принцип для существования нетривиальных единиц.

Пусть $v\in V^K, O_v$ — кольцо нормирования для v, p_v — максимальный идеал в O_v, $K_v=O_v/p_v$ — поле вычетов, являющееся конечным полем, $\pi_v:O_v\to O_v/p_v$ — каноническая проекция. Для почти всех $v\in V^K$ все коэффициенты многочлена $f(x)$ принадлежат O_v. Мы можем рассмотреть многочлен $f_v(x)$, получающийся из $f(x)$ редукцией его коэффициентов по модулю p_v :$f_v(x)\in k_v[x]$.

Нетрудно показать, что для почти всех v многочлен $f_v(x)$ свободен от квадратов. Рассмотрим $D_{f_v} = \{\alpha_v + \beta_v\sqrt{f_v(x)}|\alpha_v, \beta_v \in k_v[x]\}$.

Хорошо известно, что D_{f_v} имеет нетривиальные единицы, так что $D_f^* = k_v^* \times \langle u_v \rangle$, где u_v — фундаментальная единица в D_{f_v}. Если $u_v = \alpha_v + \beta_v\sqrt{f_v(x)}$, то определим $\deg u_v = \deg \alpha_v$.

Теорема 1. *Если для некоторого бесконечного подмножества* $\mathrm{T} \in V^K$ *существует такая константа* m, *что для любого* $v \in \mathrm{T}$ $\deg u_v < m$, *то* D_f *обладает нетривиальной единицей.*

Так как для почти всех $v \in \mathrm{T}$ редуцированный многочлен $f_v(x)$ является бесквадратным, то, не ограничивая общности, можно предполагать, что это верно для любых $v \in \mathrm{T}$. Через $\Delta^\circ(L)$ мы будем обозначать группу классов дивизиров степени 0.

Лемма 1. *Пусть* $w_1^v(\infty), w_2^v(\infty)$ — *неэквивалентные бесконечные нормирования поля* $L_v = k_v(x)(\sqrt{f_v(x)})$. *Если* u_v — *фундаментальная единица в* D_{f_v}, *то степень* $\deg u_v$ *равна порядку класса дивизора* $w_1^v(\infty) - w_2^v(\infty)$ *в группе классов дивизоров* $\Delta^\circ(L_v)$ *поля* L_v.

Нам понадобятся некоторые свойства якобиана J_f и соответствующих якобианов J_{f_v}, функториальные относительно редукции по $\mathrm{mod} p_v$, которые следуют из конструкции и базовых свойств якобиевых многообразий кривой.
Существует естественное вложение группы классов дивизоров $\Delta^\circ(L)$ в $J_f(K)$ и соответствующие вложения групп $\Delta^\circ(L_v)$ в $J_{f_v}(k_v)$ (на самом деле, в нашей ситуации вложения являются изоморфизмами). Для почти всех $v \in V^K$ редукция абелева многообразия $J_f(K)$ по модулю p_v является хорошей и изоморфна $J_{f_v}(k_v)$. При этом для почти всех v из T редукция образа класса дивизора $w_1(\infty) - w_2(\infty)$ будет совпадать с образом класса дивизора $w_1^v(\infty) - w_2^v(\infty)$.

Доказательство. Теорема 1 следует из леммы и приведенных выше утверждений. Действительно, для почти всех $v \in \mathrm{T}$ класс дивизора $w_1^v(\infty) - w_2^v(\infty)$ аннулируется умножением на $m!$ в группах $\Delta^\circ(L_v)$. Так как T бесконечно, то отсюда следует что класс дивизора $w_1(\infty) - w_2(\infty)$ также аннулируется умножением на $m!$ из естественных аппроксимационных свойств якобиана J_f.

Теорема 1 позволяет получить следующий локально-глобальный принцип для существования нетривиальных единиц в D_f.

Теорема 2. D_f *обладает нетривиальной единицей тогда и только тогда, когда существует такая константа* C, *что для почти всех* $v \in V^K$ $\deg u_v < C$.

Действительно, если для почти всех v $\deg u_v < C$, то D_f обладает нетривиальной единицей по теореме 1.

Пусть теперь u - нетривиальная единица в D_f, $u = \alpha(x) + \beta(x)\sqrt{f(x)}$. Тогда для почти всех $v \in V^K$ определена редукция $u_v = \alpha(x)_v + \beta(x)_v\sqrt{f_v(x)}$, где u_v будет нетривиальной единицей в D_{f_v} и $\deg u_v = \deg u$. Для таких v $\deg u_v \leqslant \deg u$.

Теорема 3. *Нетривиальная единица u в D_f тогда и только тогда является фундаментальной, когда для почти всех $v \in V^K$ редуцированные единицы u_v являются фундаментальными в D_{f_v}.*

Рассмотрим теперь ситуацию для $n = 1, 2$.

Если $n = 1$ и $f(x) = x^2 + a_1x + a_0$, то очевидно, что $u = x + \frac{a_1}{2} + \sqrt{f}$ является фундаментальной единицей в D_f.

Случай $n = 2$ уже является сложным. Без ограничения общности, можно считать, что $f(x) = x^4 + a_2x^2 + a_1x + a_0$. Тогда существует эффективная процедура для описания якобина J_f, который в этом случае является эллиптической кривой .

А именно, для проективизации $\overline{X}_f$ кривой X_f существует бирационально эквивалентная эллиптическая кривая E, задаваемая уравнением $y^2 = x^3 + Ax + B$, где $A, B \in K$. Мы можем интерпретировать $w_1(\infty)$ и $w_2(\infty)$ как две различные точки на бесконечности для кривой $\overline{X}_f$. Тогда существует бирациональный морфизм $\varphi : \overline{X}_f \to E$ со свойством: $\varphi(w_2(\infty)) = 0_\infty$ (нулевой элемент в группе E), $\varphi(w_1(\infty)) = (x_0, y_0) \in E(K)$.

Кольцо D_f имеет нетривиальную единицу тогда и только тогда, когда (x_0, y_0) является элементом конечного порядка в абелевой группе $E(K)$. Так как подгруппа кручения $E_{tor}(K)$ в $E(K)$ конечна, и ее порядок ограничен некоторой константой, зависящей от K, но не от E (L. Merel), то существует формально эффективная процедура для проверки конечности порядка элемента (x_0, y_0) в $E(K)$. Но особенно эффективный алгоритм получается для $K = Q$, ибо в этом случае есть глубокий результат Мазура , утверждающий, что для эллиптической кривой E над Q порядок группы $E_{tor}(Q) \leqslant 12$.

Если $f(x) = x^4 + a_0$, $a_0 \in Q^*$, то очевидно, что D_f $u = x^2 + \sqrt{f}$ является фундаментальной единицей. Если $f(x) = x^4 + x$, то нетривиальные единицы в D_f существуют и $u = x^3 + \frac{1}{2} + x^2\sqrt{x^4 + x}$ будет фундаментальной единицей.

Но уже для следующего многочлена $f(x) = x^4 + x + 1$ ситуация будет совершенно иной. Следующее предложение дает ответ на вопрос, поставленный Ф. Груневальдом.

Предложение 1. *Для $f(x) = x^4 + x + 1$ кольцо $D_f = Q[x] + Q[x]\sqrt{f}$ не имеет нетривиальных единиц, т.е. $D_f^* = Q^*$.*

Доказательство. Вычислительная процедура позволяет определить якобиан J_f следующим образом: J_f будет эллиптической кривой E, задаваемой уравнением $s^2 = t^3 - 4t + 1$, причем образом класса дивизора $w_1(\infty) - w_2(\infty)$ в E будет точка $(0, 1)$. $(0, 1) \in E(Q) = \{(x, y) \in Q^2 | y^2 = x^3 - 4x + 1\} \bigcup \{0_\infty\}$.

Мы хотим доказать, что точка $(0, 1)$ имеет бесконечный порядок в $E(Q)$. Можно путем рутинных вычислений установить, что $(0, 1)$ не является точкой

порядка $m \leqslant 12$. Тогда из теоремы Мазура будет следовать, что $(0,1)$ является точкой бесконечного порядка. Более интересно здесь использовать редукцию по различным простым модулям. Дискриминант эллиптической кривой равен 229, поэтому редукции по $mod2$ и $mod3$ будут хорошими.

Через $\overline{E}$ будем обозначать редуцированную эллиптическую кривую по $mod2$ или $mod3$. Тогда $\left|\overline{E}\,(F_2\,)\right| = 3$, $\left|\overline{E}\,(F_3\,)\right| = 7$. Отсюда следует, что $|E_{tor}(Q\,)| = 1$, и точка $(0,1)$ имеет бесконечный порядок. В качестве следствия из предложения и теоремы 1 получаем следующее интересное утверждение.

Следствие 1. *Если $f = x^4 + x + 1$ и u_p обозначает фундаментальную единицу в кольце $D_{f_p} = F_p\,[x] + F_p\,[x]\sqrt{f_p(x)}$ для простого числа p, тогда $\sup\limits_{p\in T} \deg u_p = \infty$ для бесконечного множества T простых чисел, т.е. степени фундаментальных единиц u_p не являются в совокупности ограниченными.*

Теоремы 1-3 доказаны в статье автора [6].

Следующая теорема доказана автором совместно с В. Беняш-Кривецем (см. [8]).

Теорема 4. *Для многочлена $f(x) = x^4 + bx + c$ кольцо D_f обладает фундаментальной единицей и степени n при следующих значениях n, b и c:*

$$1) n = 2, b = 0, c \in \mathbb{Q}^*, u = x^2 + \sqrt{f};$$

$$2) n = 3, c = 0, b \in \mathbb{Q}^*, u = x^3 + \frac{b}{2} + x\sqrt{f};$$

3) $n = 4$, $b = t^3$, $c = \frac{t^4}{2}$, *где* $t \in \mathbb{Q}^*$, $u = x^4 - tx^3 + \frac{t^2}{2}x^2 + \frac{t^3}{2}x - \frac{t^4}{4} + \left(x^2 - tx + \frac{t^2}{2}\right)\sqrt{f}$.

Для $n = 3$ проблема существования нетривиальных единиц пока неприступна для произвольного многочлена f шестой степени. Одна из важных причин такого положения дел заключается в следующем. В этом случае якобиан J_f является двумерным абелевым многообразием и до сих пор мало известно о кручении в $J_f(K)$ даже для $K = Q$. До сих пор остается открытой известная гипотеза об ограниченности кручения в $J_f(Q)$ некоторой константой, зависящей только от Q.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[1] Серр Ж.-П. Алгебраические группы и поля классов, М.: Мир, 1968, с.278.

[2] Lang S. Abelian varieties, Interscience, N.Y., 1983, 272 p.

[3] Adams W.W., Razar M.J., Multiples of points on elliptic curves and continued fractions , Proc. London Math.Soc.,// 1980, v.41, №3, p. 481-498.

[4] Merel L.,Borne pour la torsion des courbes elliptiques sur les cops de nombres,// Invent. Math., 1996, v. 124, p. 437-449.

[5] Mazur B., Modular curves and the Eisenstein ideal,// Publ Math. IHES, 1978, v. 47, 33-186.

[6] Платонов В.П Арифметика квадратичных полей и кручение в якобианах,// Доклады РАН, 430(2010), №3.

[7] Беняш-Кривец В.В., Платонов В.П., Группы S-единиц в гиперэллиптических полях и непрерывные дроби, // Математический сборник, 200(2009), №11, 15-45.

[8] Беняш-Кривец В.В., Платонов В.П., О новом локально-глобальном принципе для квадратичных функциональных полей // Доклады РАН 433(2010) (в печати).

НИИСИ РАН
Поступило 15.05.2010