Национальная академия наук Беларуси
Труды Института математики. 2008. Том 16. № 2. С. 57–62

УДК 511.36

О МАЛЫХ ЗНАЧЕНИЯХ ДИСКРИМИНАНТОВ ПОЛИНОМОВ n-Й СТЕПЕНИ, ЯВЛЯЮЩИХСЯ ПРОИЗВЕДЕНИЕМ ЛИНЕЙНЫХ ПОЛИНОМОВ С ЦЕЛЫМИ КОЭФФИЦИЕНТАМИ

О. С. Куксо, В. И. Берник, Е. В. Зорин

Институт математики НАН Беларуси
e-mail: olga_kukso@tut.by, bernik@im.bas-net.by, evgeniyzorin@yandex.ru
Поступила 06.09.2007

В распределении значений дискриминантов целочисленных многочленов $P_n(x)$ степени $\deg P \geq 4$ должны быть лакуны. В работе оценивается мера таких пропусков для специальных многочленов, указанных в заглавии.

Дискриминантом многочлена

$$P_n(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

где $a_n \neq 0$, называют определитель

$$D(P) = (-1)^{n(n-1)/2} \begin{vmatrix} 1 & a_{n-1} & a_{n-2} & \ldots & a_0 & 0 & \ldots \\ 0 & a_n & a_{n-1} & \ldots & a_1 & a_0 & \ldots \\ \multicolumn{7}{c}{\dotfill} \\ 0 & \ldots & 0 & a_n & \ldots & a_1 & a_0 \\ n & (n-1)a_{n-1} & (n-2)a_{n-2} & \ldots & a_1 & 0 & \ldots \\ 0 & na_n & (n-1)a_{n-1} & \ldots & 2a_2 & a_1 & \ldots \\ \multicolumn{7}{c}{\dotfill} \\ 0 & \ldots & 0 & na_n & \ldots & 2a_2 & a_1 \end{vmatrix}. \tag{1}$$

Можно заметить, что $D(P) = |\mathrm{Res}(P, P')/a_n|$, где $\mathrm{Res}(P, Q)$ — результант многочленов $P(x)$ и $Q(x)$.

Утверждение. *Пусть $\alpha_1, \ldots, \alpha_n$ — все корни многочлена P в некотором алгебраически замкнутом поле, которому принадлежат все коэффициенты многочлена P. Тогда*

$$D(P) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2. \tag{2}$$

Доказательство данного утверждения можно найти, например, в [1, § 35]. Представление $D(P)$ в виде (2) часто принимают в качестве определения дискриминанта. В работах [2, 3] можно ознакомиться с более общим понятием дискриминанта расширения модулей, которое в частном случае, когда расширение целых (или рациональных) чисел определяется одним многочленом, совпадает с дискриминантом многочлена в только что определенном смысле.

В этой работе мы будем называть высотой многочлена $P_n(x)$ степени n максимум значения модулей его коэффициентов

$$H = H(P) = \max_{0 \le j \le n} |a_j|.$$

Далее будем рассматривать только многочлены с целыми рациональными коэффициентами и обозначать через $c_1(n), c_2(n), \ldots$ величины, зависящие от n и не зависящие от H. Из (1) нетрудно получить, что

$$|D(P)| < c_1(n) H^{2n-2}. \tag{3}$$

Известно, что $D(P) = 0$ если и только если многочлен P имеет кратные корни, поэтому, в силу (1), если многочлен P не имеет кратных корней, то

$$|D(P)| \ge 1. \tag{4}$$

О распределении значений дискриминантов к настоящему времени известно мало, хотя диофантовы уравнения с дискриминантами в настоящее время интенсивно исследуются [4]. Это связано в первую очередь со сложной нелинейной зависимостью $D(P)$ от коэффициентов $P_n(x)$. Интересным является следующий вопрос: верно ли, что для полиномов $|D(P)|$ стремится к бесконечности вместе с ростом n? В настоящей работе мы даем частичный ответ на поставленный вопрос для специальных полиномов. Пусть даны n пар $(q_1, p_1), \ldots, (q_n, p_n)$ целых чисел, $(q_i, p_i) = 1$, причем все q_i не равны 0 и $\frac{p_i}{q_i} \ne \frac{p_j}{q_j}$ при $i \ne j$. Рассмотрим полиномы n-й степени вида

$$T_n(x) = \prod_{i=1}^{n} (q_i x - p_i). \tag{5}$$

Такие полиномы имеют корни $\alpha_1 = \frac{p_1}{q_1}, \ \ldots, \ \alpha_n = \frac{p_n}{q_n}$.

Теорема 1. *Существуют полиномы вида (5) степени 2 и 3 с дискриминантом, равным единице. Для любого полинома вида (5) степени* $n \ge 4$ *имеет место оценка* $D(P) \ge 4$.

Теорема 2. *Существует такой многочлен* $P_n(x)$ *вида (5), что*

$$|D(T)| < \exp(n^2 \ln n). \tag{6}$$

Теорема 3. *Пусть* $n \ge 4$. *Тогда существует постоянная* c_1 *такая, что для любого полинома вида (5) верна оценка*

$$D(P) \ge \max(4, \exp(c_1 n^2 \ln n)). \tag{7}$$

Константу c_1 *можно указать явно. Если* $n \ge 25$, *то подходит* $c_1 = \frac{1}{126}$. *Для любого значения* $n \ge 4$ *можно взять* $c_1 = \frac{\ln 2}{625 \ln 5}$.

Для нас будет важно следующее представление $D(P)$, когда все корни полинома P рациональны — это представление вытекает непосредственно из формулы (2). Пусть степень полинома P равна n и его корни являются рациональными числами $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$. Тогда дискриминант P представляет собой модуль произведения всех возможных определителей

$$\Delta_{ij} = \begin{vmatrix} p_i & q_i \\ p_j & q_j \end{vmatrix} = p_i q_j - p_j q_i, \quad i \ne j, \tag{8}$$

а именно
$$D(P) = \left|\prod_{i\neq j} \Delta_{ij}\right|. \tag{9}$$

Для доказательства приведенных теорем удобно представлять рациональные числа в следующем виде. Пусть (Oxy) — координатная плоскость. Произвольное рациональное число представим в виде несократимой дроби $\dfrac{p}{q}$, где $p \in \mathbb{Z}$, $q \in \mathbb{N}$. Этому рациональному числу сопоставим точку на координатной плоскости с координатами (q, p). В дальнейшем будем иногда говорить, что "точка плоскости (Oxy) с целыми координатами является корнем многочлена такого-то" или "некое рациональное число совпадает с такой-то точкой плоскости (Oxy)", всегда подразумевая именно такое представление рациональных чисел.

При данном представлении рациональных чисел точками на плоскости дискриминант можно интерпретировать как произведение площадей всех возможных треугольников с одной из вершин в начале координат и двумя другими вершинами в различных корнях многочлена. В лемме 3, которая доказывается ниже, показано, что если на плоскости выбрано достаточно много точек, скажем n, то найдется достаточно много треугольников, по крайней мере $\dfrac{1}{4}n$, с достаточно большой площадью, не меньше $\dfrac{1}{4}\sqrt{n}$. Из этого непосредственно получается оценка снизу дискриминанта в теореме 3.

Доказательство теоремы 1. В случае $n = 2$ можно взять полином
$$P_2(x) = x^2 - (2k+1)x + k(k+1)$$
(при любом натуральном k). Непосредственно вычисляя дискриминант, получаем $D(P_2) = 1$. В случае $n = 3$ можно взять полином, рациональные корни которого представляются точками $(1, 1)$, $(1, 2)$, $(2, 3)$. Легко проверить, что все определители Δ_{ij} при таком выборе трех рациональных корней равны 1 и, значит, дискриминант такого многочлена равен 1. Второе утверждение теоремы 1 доказывается в лемме 4.

Доказательство теоремы 2. Возьмем точки с координатами $(1; 1), (1; 2), \ldots, (1; n)$. Явная запись такого многочлена:
$$P(x) = \prod_{i=1}^{n}(x - i).$$
Пусть P_j обозначает произведение площадей треугольников, у которых одна вершина — это начало координат, вторая — вершина $(1; j)$ при некотором фиксированном j и третья — любая другая точка из нашего набора. Тогда $P_j < n^n$, поскольку в любом треугольнике с вершинами в точках $(0, 0)$, $(1, i)$ и $(1, j)$ длина стороны $((1, i)(1, j))$ не превосходит n и длина высоты, опущенной из вершины $(0, 0)$ на эту сторону, равна 1. Поэтому дискриминант соответствующего многочлена (т.е. многочлена, множество корней которого совпадает с множеством выбранных нами точек) оценивается как
$$\prod_{j=1}^{n} P_j < (n^n)^n = e^{n^2 \ln n}.$$

Для доказательства теоремы 3 нам понадобится несколько вспомогательных утверждений.

Лемма 1. *Пусть* $(a; b) \in \mathbb{Z}^2$. *Существует матрица с целыми коэффициентами*
$$M \in \mathcal{S}L_2(\mathbb{Z})$$
такая, что $M(a; b)^{\mathrm{T}} = (1; 0)^{\mathrm{T}}$.

Доказательство. Существует такая пара $(c;d) \in \mathbb{Z}^2$, что $ac-bd=1$, причем можно считать, что $d>0$. Существование следует, например, из алгоритма Евклида, положительность d можно получить, что если пара (c,d) удовлетворяет условию, то и пары $(c+b,d+a)$ и $(c-b,d-a)$ тоже ему удовлетворяют. Матрица $\begin{pmatrix} a & d \\ b & c \end{pmatrix}$ принадлежит $\mathcal{S}L_2(\mathbb{Z})$ и переводит векторы $(1;0)^{\text{т}}$ и $(0;1)^{\text{т}}$ соответственно в $(a;b)^{\text{т}}$ и $(d;c)^{\text{т}}$. Обратная к ней матрица также принадлежит $\mathcal{S}L_2(\mathbb{Z})$ и переводит векторы $(a;b)^{\text{т}}$ и $(d;c)^{\text{т}}$ соответственно в $(1;0)^{\text{т}}$ и $(0;1)^{\text{т}}$.

Замечание 1. Обозначим $\mathcal{S}L_2'(\mathbb{Z})$ группу матриц 2×2 с целыми коэффициентами и определителем ± 1. Эта группа порождается элементами $\mathcal{S}L_2(\mathbb{Z})$ и симметрией относительно оси Ox. Понятно, что симметрия относительно оси Ox сохраняет целочисленность координат точек и площади всех фигур, в частности площади треугольников. То же справедливо относительно элементов $\mathcal{S}L_2(\mathbb{Z})$, а потому и $\mathcal{S}L_2'(\mathbb{Z})$.

Лемма 2. *Пусть* $(a;b),(c;d)\in\mathbb{Z}^2$. *Обозначим площадь треугольника* $((0;0),(a,b),(c,d))$ *через* S. *Существует элемент* $M\in\mathcal{S}L_2'(\mathbb{Z})$, *который переводит* $(a;b)^{\text{т}}$ *в* $(1;0)$ *и* $(c;d)^{\text{т}}$ *в* $(t;S)^{\text{т}}$, *где* $t\in[0,S)$.

Доказательство. Согласно лемме 1, существует матрица $M_1\in\mathbb{Z}$ такая, что

$$m_1(a;b)^{\text{т}} = (1;0)^{\text{т}}.$$

Поскольку действие M_1, как действие всякой матрицы с определителем по модулю равным 1, сохраняет площадь, то $(c;d)$ перейдет в точку $(x;\pm S)$ при некотором x. Используем симметрию s относительно оси Ox, т.е. можно заменить M_1 на sM_1 и считать, что $M_1(c;d)^{\text{т}} = (x;S)^{\text{т}}$. Возьмем матрицу $M_2 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$. Она переводит вектор $(1;0)^{\text{т}}$ в себя, а вектор $(x;S)$ в $(x-S;S)$. Соответственно обратная матрица M_2^{-1} переводит вектор $(1;0)^{\text{т}}$ в себя, а вектор $(x;S)$ в $(x+S;S)$. Для подходящего целого числа n получаем, что матрица $M_2^nM_1$ подходит в качестве $M\in\mathcal{S}L_2'(\mathbb{Z})$, существование которой мы и доказываем.

Лемма 3. *Пусть на плоскости выделено n различных, отличных от* $(0;0)$, *точек с целыми координатами. Выберем и зафиксируем две точки из этого набора, допустим A и B. Тогда существует по крайней мере* $\frac{1}{4}n$ *треугольников с одной вершиной в* $(0;0)$, *двумя другими вершинами в выделенных точках, причем хотя бы одна из этих двух вершин совпадает с A или B и площади треугольников не менее* $\frac{1}{4}\sqrt{n}$.

Доказательство. По точкам A и B построим матрицу M как в лемме 2. Действуя этой матрицей на исходную картинку с выделенными точками, получим новую картинку, в которой точки с целочисленными координатами взаимно-однозначно соответствуют точкам с целочисленными координатами исходной картинки, и все площади треугольников с вершинами в выделенных точках остаются прежними. Нам достаточно доказать утверждение для новой картинки. Это позволяет считать, что точка A является точкой $(1;0)$, а B представляет собой точку $(t;S)$ для $t\in[0,S)$, $S>0$.

Выделим прямоугольник с центром в $(0;0)$, сторонами, параллельными координатным осям, половиной высоты $\frac{1}{4}\sqrt{n}$ и половиной ширины $\frac{3}{4}\sqrt{n}$. Любая точка вне этого прямоугольника образует вместе с O, A (для точек, лежащих выше прямой $y=\frac{1}{4}\sqrt{n}$ или ниже прямой $y=-\frac{1}{4}\sqrt{n}$) или O, B (для точек, лежащих правее $x=\frac{3}{4}\sqrt{n}$ или левее $x=-\frac{3}{4}\sqrt{n}$) треугольник площади не менее $\frac{1}{4}\sqrt{n}$.

Доказательство теоремы 3. Пусть на плоскости расположено n точек $X_1,X_2,\ldots,X_n$. Будем называть треугольник *выделенным,* если одна из его вершин является точкой $(0;0)$, а две другие являются точками X_i и X_j ($i \neq j$). Согласно лемме 3, существует по крайней мере $\frac{1}{4}n$ выделенных треугольников площади по крайней мере $\frac{1}{4}\sqrt{n}$, и одной из вершин которых является одна из точек X_1 или X_2. Применим затем лемму 3 к набору $X_3, \ldots, X_n$. Это даст существование не менее $\frac{1}{4}(n-2)$ треугольников каждый площади по крайней мере $\frac{1}{4}\sqrt{n-2}$ с одной из вершин X_3 или X_4. Все эти треугольники будут отличны от треугольников, полученных в результате предыдущего применения леммы 3, поскольку все те имели в качестве одной из своих вершин X_1 или X_2, а полученные на текущем этапе — точки из набора $X_3, \ldots, X_n$. Теперь применим лемму 3 несколько раз: сначала к точкам $X_5, \ldots, X_n$, затем к наборам $X_i, \ldots, X_n$, до тех пор, пока $i+1 \geq n/3$.

Предположим пока $n \geq 25$ (так проще излагать доказательство, выделение первых нескольких значений n не имеет существенного значения). Тогда в результате описанных выше применений леммы 3 получим не менее $n/6$ наборов, каждый содержащий по крайней мере $\frac{1}{4}n/2$ треугольников с площадью $\frac{1}{4}\sqrt{n/2}$. Все полученные треугольники различны между собой в силу описанной выше причины. Произведение их площадей не меньше

$$\left(\frac{1}{4}\sqrt{n/2}\right)^{n/6\times\frac{1}{4}n/2} > e^{\frac{1}{48}n^2\left(\frac{1}{2}\ln n-\frac{1}{2}\ln 2-2\ln 2\right)\ln n} > e^{\frac{1}{126}n^2\ln n}.$$

Для первых нескольких значений n, т.е. для $4 \leq n \leq 24$, можно просто уменьшить константу $\frac{1}{126}$ до подходящего значения (простые геометрические соображения (см. лемму 4 ниже) показывают, что при $n \geq 4$ дискриминант полинома степени n не меньше 4, поэтому по крайней мере константа $\frac{\ln 4}{25^2\ln 25}\left(<\frac{1}{126}\right)$ подойдет для всех значений n).

Лемма 4. *Для любого полинома вида (5) степени $n \geq 4$ имеет место оценка $D(T) \geq 4$.*

Доказательство. Согласно лемме 2, в предположении противного мы можем считать, что два корня нашего многочлена после преобразования некоторой матрицей из $\mathcal{S}L_2'(\mathbb{Z})$ представляются точками $(1,0)$ и $(0,1)$. Существует только четыре точки, в которых может находиться третий корень так, чтобы площади всех возможных треугольников с одной вершиной в начале координат и двумя другими в наших трех выбранных точках-корнях многочлена были равны 1, а именно: $(\pm1,\pm1)$ — если первая (горизонтальная) координата четвертого корня A строго меньше -1 или строго больше 1, то треугольник $(0,0)A(0,1)$ имеет площадь по крайней мере 2; если вторая (вертикальная) координата четвертого корня строго больше 1 или строго меньше -1, то площадь треугольника $(0,0)A(1,0)$ не меньше 2). Все остальные случаи, если учесть еще требование различности всех корней полинома, сводятся к точке $(1,1)$ или $(-1,-1)$ в качестве одной вершины, назовем ее B, и двум точкам $(-1,1)$ или $(1,-1)$ в качестве второй, назовем ее A. В обоих случаях треугольник $(0,0)AB$ имеет площадь 2.

Таким образом, если полином имеет степень 4 или более, то найдется по крайней мере один треугольник с одной вершиной в начале координат и двумя остальными вершинами в отмеченных точках, скажем X_k и X_m, и с площадью по крайней мере 2. В произведении

$$D(P) = \left|\prod_{i\neq j}\Delta_{ij}\right|,$$

таким образом, встретится по крайней мере два члена по модулю не меньше $2:$ Δ_{km} и Δ_{mk}. Значит, дискриминант $D(P)$ не меньше 4.

Литература

1. *Ван дер Ваден Б.Л.* Алгебра. М.: Наука, 1979.
2. *Касселс Дж., Фрелих А.* Алгебраическая теория чисел. М.: Мир, 1969.
3. *Milne J.S.* Algebraic Number Theory // www.jmilne.org/math/CourseNotes/math676.pdf
4. *Gyory K.* Polynomials and binary forms with given discriminant // Publ. Math. Debrecen. 2006. V. 69. № 4. P. 473–499.

O. S. Kukso, V. I. Bernik, E. V. Zorin

On small values of discriminats of polynomials, the product of linear integer polynomials of n-th degree

Summary

The distribution of discriminants of integer polynomials $P_n(x)$ with degree $\deg P \geq 4$ have to have lacunaes. The paper is devoted to the research of the lacunaes measures for special polynomials, that are specified in the title.