УДК 511.36

О.С. КУКСО, Н.В. САКОВИЧ, Н.В. ШАМУКОВА

О МНОГОЧЛЕНАХ ЗАДАННОГО ДИСКРИМИНАНТА, БОЛЬШОЙ ВЫСОТЫ И С КОРНЯМИ, ОГРАНИЧЕННЫМИ ВО ВСЕХ МЕТРИКАХ

Работа посвящена исследованию влияния преобразований сдвига и инверсии на взаимное расположение корней целочисленных многочленов. Хорошо известно, что приведенные преобразования не меняют дискриминантов многочленов. Основная идея доказательства состоит в том, что все значения многочлена степени n на арифметической прогрессии длины n+1 не могут быть значительно меньше высоты многочлена. В работе сконструирована специальная последовательность арифметических прогрессий, в каждой из которых удается найти такой член, в котором p_1-адическая норма многочлена достаточно велика для любых заранее выбранных простых чисел $p_1, p_2, \ldots, p_k$. Затем в следующей арифметической прогрессии находится член, в котором велика и архимедова метрика многочлена.

Введение

Во многих задачах теории чисел нужно по величине коэффициентов многочленов получить информацию о величине корней в поле комплексных чисел или об их p-адической норме. С ростом $H(P)$ корни многочлена остаются ограниченными. Получено условие, обеспечивающее ограниченность корней $P_n(x)$ в разных метриках. Исследованы связи величин коэффициентов и корней целочисленных многочленов и влияния преобразований сдвига и инверсии на взаимное расположение корней целочисленных многочленов в поле p-адических чисел. Многие результаты этой статьи верны для многочленов с действительными и комплексными коэффициентами. Однако в приложениях чаще речь идет о целочисленных многочленах, поэтому в дальнейшем мы рассматриваем многочлены с целыми коэффициентами.

Основная часть

Пусть $P_n(x) = a_n x^n + \ldots + a_1 x + a_0,\ a_j \in \mathbf{Z},\ 0 \le j \le n$ − (1)

многочлен с целыми коэффициентами и $H = H(P) = \max\limits_{0 \le j \le n} |a_j|$ − высота многочлена, $|\ldots|$ и $|\ldots|_p$ − архимедова и неархимедова нормы, << − символ Виноградова, обозначающий в записи $A << B$ существование величины $c > 0$ такой, что $A < cB$.

Обозначим через $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbf{C}$ корни многочлена $P_n(x)$, а через $\gamma_1, \gamma_2, \ldots, \gamma_n \in \mathbf{C}$ − корни многочлена $P_n(w)$, лежащие в $\mathbf{Q}_p$ или некотором алгебраическом расширении $\mathbf{Q}_p$. Во многих задачах теории чисел удобно, когда с ростом $H(P)$ корни многочлена остаются ограниченными. Впервые на это обратил внимание В.Г. Спринджук [1]. Есть простое достаточное условие, обеспечивающее ограниченность корней $P_n(x)$ в разных метриках.

Лемма 1. *Если при некотором* c_1 *имеем* $|a_n| \ge c_1 H$, *то*

$$\max_{1 \le j \le m} |\alpha_j| \le c_1^{-1} + 1. \tag{2}$$

Доказательство. Пусть максимум в левой части неравенства (2) достигается при $j = j_0$. Тогда если $|\alpha_{j_0}| \le d = c_1^{-1} + 1$, то (2) доказано. Пусть $|\alpha_{j_0}| > d$. Ясно, что $d \ge 2$. Тогда из равенства $P(\alpha_j) = 0$ имеем

$$a_n \alpha_{j_0}^n = -a_{n-1}\alpha_{j_0}^{n-1} - a_{n-2}\alpha_{j_0}^{n-2} - \ldots - a_1\alpha_{j_0} - a_0$$

$$|\alpha_{j_0}| = \left|\frac{a_{n-1}}{a_n}\alpha_{j_0}^{-1}\right| + \left|\frac{a_{n-2}}{a_n}\alpha_{j_0}^{-2}\right| + \ldots + \left|\frac{a_0}{a_n}\alpha_{j_0}^{-n+1}\right| <$$

$$< c_1^{-1}\left(|\alpha_{j_0}|^{-1} + \ldots + |\alpha_{j_0}^{n-1}|^{-1} + \ldots\right) \le c_1^{-1}\frac{|\alpha_{j_0}|^{-1}}{1 - |\alpha_{j_0}|^{-1}}. \tag{3}$$

Максимальное значение величины $|\alpha_{j_0}|^{-1}\left(1 - |\alpha_{j_0}|^{-1}\right)^{-1}$ не превосходит $|\alpha_{j_0}|^{-1}\left(1 - \frac{1}{2}\right)^{-1} = 2d^{-1}$. Поэтому левая часть неравенства (3) больше $c_1^{-1} + 1$, а правая меньше 1. Получили противоречие.

Лемма 2. *Если при некотором* $c_2 > 0$ *имеем* $|a_n|_p \ge c_2$, *то*

$$\max_{1 \le i \le n} |\gamma_i|_p < c_2^{-\frac{1}{n}}. \tag{4}$$

Доказательство. Пользуясь свойством неархимедовости нормы, аналогично (3) получим

$$|\gamma_k|_p = \left|\frac{a_{n-1}}{a_n} + \frac{a_0}{a_n}\gamma_k^{-n+1}\right|_p \le \max_{0\le i\le n-1}\left|\frac{a_i}{a_n}\gamma_k^{-n+i+1}\right|_p \le c_2^{-1}\max_{0\le i\le n-1}|\gamma_k|_p^{-n+i+1} \le c_2^{-1}|\gamma_k|_p^{-n+1},$$

откуда $|\gamma_k|_p^n < c_2^{-1}$, что доказывает (4).

Однако приведенные достаточные условия выполняются не всегда. Тогда в зависимости от поставленной задачи с многочленом можно произвести преобразования аргумента, не меняющие важнейших характеристик изучаемых множеств. Такими преобразованиями являются сдвиг аргумента и инверсия. В [1] показано, как это можно сделать отдельно в случае архимедовой и не архимедовой норм. Мы приведем новые доказательства утверждений из [1], а затем покажем, как их можно совместить, т.е. добиться одновременного выполнения неравенств

$$|a_n| > c_1 H, \ |a_n|_p > c_2. \tag{5}$$

Частные случаи приведенных ниже теорем доказаны в [2].

Теорема 1. *Пусть* $P(x) \in \mathbf{Z}[x]$. *Тогда сдвигом аргумента и инверсией многочлен* $P(x)$ *можно привести к многочлену, для которого выполняется первое неравенство* (5).

Доказательство. Вначале докажем, что для любого целого числа l найдется целое число m, $1 \le m \le 1+n$, при котором

$$|P(m)| > c_3 H. \tag{6}$$

Установим, что при подходящем c_3 система из $n+1$ неравенства

$$\max_{1\le m\le 1+n} |P(m)| \le c_3 H \tag{7}$$

противоречива. Перепишем (7) в виде системы уравнений

$$\begin{cases} |P(l)| = |a_n l^n + a_{n-1} l^{n-1} + \ldots + a_1 l + a_0| = \theta_0 c_3 H, \\ |P(l+1)| = |a_n (l+1)^n + a_{n-1}(l+1)^{n-1} + \ldots + a_1(l+1) + a_0| = \theta_1 c_3 H, \\ \ldots \\ |P(l+n)| = |a_n (l+n)^n + a_{n-1}(l+n)^{n-1} + \ldots + a_1(l+n) + a_0| = \theta_n c_3 H, \end{cases} \tag{8}$$

где $|\theta_k| \le 1$, для любого k, $0 \le k \le n$. Один из коэффициентов многочлена $P(x)$ равен H. Пусть это a_j. Решим систему уравнений (8) относительно a_j. Получим

$$H = a_j = \frac{\Delta_j}{\Delta}. \tag{9}$$

Определитель Δ в (9) – это определитель системы неравенств (8), а Δ_j – определитель, в котором j-ый столбец в Δ заменен на столбец свободных коэффициентов. Ясно, что при подходящем c_3 правая часть в (9) меньше H и равенство (9) противоречиво. От произвольного полинома $P(x) \in \mathbf{Z}[x]$ перейдем к полиному $P_1(x) = P(x + m)$. Свободный коэффициент $P_1(x)$ равен $P(m)$ и $\left|P(m)\right| > c_3 H$. Затем рассмотрим полином $P_2(x) = x^n P_1\left(\frac{1}{x}\right)$. Старший коэффициент у многочлена $P_2(x)$ равен $P(m)$, что доказывает теорему 1.

Теорема 2. *Пусть $P(x) \in \mathbf{Z}[x]$ и $P(x)$ – примитивный полином. Тогда для любого простого числа p путем сдвига аргумента и инверсии можно получить полином $T(x)$, для которого выполняется второе неравенство* (5).

Доказательство. Вначале покажем, что для любого $l \in \mathbf{Z}$ существует такое $m \in \mathbf{Z}$, $l \le m \le l + n$, что

$$\left|P(m)\right|_p > c_4(n, p).$$

Не умаляя общности, положим $l = 1$. Предположим, что

$$\max_{1 \le m \le n+1} \left|P(m)\right|_p \le c_4. \tag{10}$$

Из примитивности $P(x)$ следует, что для некоторого его коэффициента a_j имеем $\left|a_j\right|_p = 1$. Заменим (10) на систему уравнений и решим ее относительно a_j. Получим

$$\begin{cases} \left|a_n + a_{n-1} + \ldots + a_1 + a_0\right|_p = \theta_1 c_4, \\ \left|a_n 2^n + a_{n-1} 2^{n-1} + \ldots + a_1 2 + a_0\right|_p = \theta_2 c_4, \\ \ldots \\ \left|a_n (n+1)^n + a_{n-1}(n+1)^{n-1} + \ldots + a_1(n+1) + a_0\right|_p = \theta_{n+1} c_4, \\ \theta_i = p^{-d_i},\ d_i \ge 1,\ 1 \le i \le n+1. \end{cases}$$

$$a_{j_0} = \frac{\Delta_{j_0}}{\Delta}. \tag{11}$$

Определитель Δ из (11) – определитель Ван дер Монда.

$$\Delta = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ 1 & 2 & \ldots & n+1 \\ & & \ldots & \\ 1 & 2^n & \ldots & (n+1)^n \end{vmatrix} = \prod_{k=0}^{n} k\ !\ (n-k)\ ! \tag{12}$$

Простое число p входит в $k!$ в степени, не большей

$$\left[\frac{k}{p}\right]+\left[\frac{k}{p^2}\right]+\ldots\leq k\sum_{j=1}^{\infty}p^{-j}\leq k,$$

и Δ содержит степень p, не большую, чем n^2.

Для определителя Δ_j равенство $\Delta_{j_0}=a_j\Delta$, $\left|\Delta_{j_0}\right|\leq 1$, и поэтому $\left|\Delta_{j_0}\right|_p\leq p^{-d}$. Если $\left|\Delta_{j_0}\right|_p=1$, равенство (11) не выполняется при $d>n^2$.

Снова, как в теореме 1, произведем преобразование произвольного полинома $P(w)$ к полиномам $P_1(w)=P(w+m)$ и $P_2(w)=w^nP_1\left(\frac{1}{w}\right)$. У полинома $P_2(w)$ старший коэффициент равен $P(m)$ и $\left|P(m)\right|_p>c_4$. Возьмем другое простое число q и достаточно большое $l_1\in\mathbf{N}$. Из теоремы 1 следует, что существует такое натуральное число m, при котором $\left|P\left(m+sp^{l_1}\right)\right|_p=\left|P(m)\right|_p$. Как и при доказательстве теоремы 1, можно для любого $t_1\in\mathbf{Z}$ найти такое s_1, $t_1\leq s_1\leq t_1+n$, что свободный член многочлена $P_1(w)=P\left(w+m+s_1p^{l_1}\right)$ будет иметь q-адическую норму, большую некоторой величины c_5. Применим инверсию и вновь получим полином с нужными свойствами. Далее можно взять третье простое число r, отличное от p и q, и найти такое число s_2, $t_2\leq s_2\leq t_2+n$, при котором свободный коэффициент многочлена $P_1\left(w+m+s_1p^{l_1}+s_2p^{l_1}q^{l_2}\right)$ будет иметь r-адическую норму, большую c_6. В результате мы придем к следующей теореме.

Теорема 3. *Пусть $P(x)\in\mathbf{Z}[x]$ и $p_1,p_2,\ldots,p_k$ – различные простые числа. Тогда путем сдвига и инверсии можно получить многочлен такой, что*

$$\min_{1\leq i\leq k}\left|u_n\right|_{p_i}>c_7. \qquad (13)$$

Объединяя теоремы 1 и 3, можно получить следующее утверждение:

Теорема 4. *Пусть $p_1,p_2,\ldots,p_k$ – различные простые числа и $P(x)\in\mathbf{Z}[x]$. Тогда существует многочлен $Q_1(x)=b_nx^n+\ldots b_1x+b_0$, полученный из $P(x)$ сдвигом и инверсией, для которого справедлива система неравенств*

$$\min_{1\leq i\leq k}\left|b_n\right|_{p_i}>c_7,\ \left|b_n\right|>c_8H. \qquad (14)$$

Для доказательства теоремы 4 мы вначале найдем такие целые числа $m,s_1,\ldots,s_{k-1}$, при которых многочлен $P(w)$ путем сдвига на целое число

$$m+s_1p_1^{l_1}+\ldots+s_{k-1}p_1^{l_1}\cdot\ldots\cdot p_{k-1}^{l_{k-1}}$$

и последующей инверсии перейдет в многочлен $Q(w)$, для которого выполняется неравенство (13). Сдвиг аргумента, при котором свободный коэффициент будет иметь значение, по модулю превосходящее $c_8 H$, при достаточно большом l_k будем искать в виде

$$m + s_1 p_1^{l_1} + \ldots + s_{k-1} p_1^{l_1} \cdot \ldots \cdot p_{k-1}^{l_{k-1}} + s p_1^{l_1} \cdot \ldots \cdot p_{k-1}^{l_{k-1}} p_k^{l_k}.$$

Как и при доказательстве теоремы 1, среди любых подряд идущих $n + 1$ целых чисел s мы найдем такое s_k, при котором выполняется второе неравенство (14).

Покажем, как указанные преобразования можно использовать при построении многочленов большой высоты с малыми дискриминантами и заданной структурой корней. Построить многочлен с относительно небольшим дискриминантом просто. Для этого достаточно взять целочисленный многочлен небольшой высоты. Например, многочлен степени n

$$P(x) = (x-1)\ldots(x-n)$$

имеет дискриминант $D(P) = \prod_{k=1}^{n-1} k!^2$. Нетрудно проверить, что дискриминант многочлена не меняется при сдвиге, $D(P(x)) = D(P(x-m))$ и при преобразовании $P(x) \to P_1(x) = x^n P\left(\frac{1}{x}\right)$.

Последнее доказывается так. Обозначим через $\alpha_1, \alpha_2, \ldots, \alpha_n$ корни многочлена $P(x) = a_n x^n + \ldots + a_1 x + a_0$. Тогда корни многочлена $P_1(x) = a_0 x^n + \ldots + a_{n-1} x + a_n$ – это $\beta_1 = \frac{1}{\alpha_1}, \beta_2 = \frac{1}{\alpha_2}, \ldots, \beta_n = \frac{1}{\alpha_n}$. По теореме Виета $(\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n)^2 = \left(\frac{a_0}{a_n}\right)^2$.

Далее

$$D(P_1) = a_0^{2n-2} \prod_{1 \le i < j \le n} (\beta_i - \beta_j)^2 =$$

$$= a_0^{2n-2} \prod_{1 \le i < j \le n} \frac{(\alpha_i - \alpha_j)^2}{(\alpha_i \alpha_j)^2} = a_0^{2n-2} \prod_{1 \le i < j \le n} \frac{(\alpha_i - \alpha_j)^2}{(\alpha_1 \ldots \alpha_n)^2} \cdot \left(\frac{a_0}{a_n}\right)^{2n-2} =$$

$$= D(P) \cdot \left(\frac{a_n}{a_0}\right)^{2n-2} \cdot \left(\frac{a_0}{a_n}\right)^{2n-2} = D(P).$$

При l достаточно большом по сравнению с n перейдем от многочлена $P(x)$ к многочлену $P_2(x) = P(x - l)$. Корни многочлена $P_2(x)$ есть $\gamma_1 = l + 1, \ldots, \gamma_n = l + n$, а $D(P_2) = D(P)$. Затем перейдем к многочлену $P_3(x) = x^n P_2\left(\frac{1}{x}\right)$. Корни многочлена $P_3(x)$ – это $\lambda_1 = \frac{1}{l+1}, \ldots, \lambda_n = \frac{1}{l+n}$,

а $D(P_3) = D(P)$. Высота многочлена $P_3(x)$ равна модулю старшего коэффициента многочлена $P_3(x)$ и равна $B_n = (l+1)\ldots(l+n)$, $B_n = (l+o(1))\ \ l^n$, $l = H(P_3)^{1/n}(1+o(1))$.
Поскольку

$$|\lambda_i - \lambda_j| = \frac{|j-i|}{(l+i)(l+j)}, \text{ то}$$

$$\frac{1}{(1+o(1))H(P_3)^{2/n}} < |\lambda_i - \lambda_j| < \frac{n-1}{(1+o(1))H(P_3)^{2/n}}. \tag{16}$$

Мы получили многочлен $P_3(x)$, высоту которого можно сделать сколь угодно большой. Расстояние между любыми корнями $P_3(x)$ стремятся к нулю с ростом $H(P_3(x))$, а дискриминант остается неизменным, равным $D(P)$. Тем самым справедлив следующий результат:

Теорема 5. *Для любого $n \in \mathbf{N}$, существуют целочисленные многочлены $P(x)$, $\deg P = n$, имеющие дискриминанты $D(P) = c(n)$, сколь угодно большую высоту и корни $\alpha_1, \alpha_2, \ldots, \alpha_n$ такие, что при любых $i \neq j$*

$$|\alpha_i - \alpha_j| \underset{H(P)\to\infty}{\to} 0.$$

Заключение

В результате исследований были получены метрические теоремы о приближении нуля моническими многочленами: условия, обеспечивающие ограниченность корней многочлена в разных метриках; исследованы связи величин коэффициентов и корней целочисленных многочленов и влияния преобразований сдвига и инверсии на взаимное расположение корней целочисленных многочленов в комплексной плоскости и в поле p-адических чисел. В работе сконструирована специальная последовательность арифметических прогрессий, в каждой из которых удается найти такой член, в котором p_j-адическая норма многочлена достаточно велика для любых заранее выбранных простых чисел $p_1, p_2, \ldots, p_k$. Затем в следующей арифметической прогрессии находится член, в котором велика и архимедова метрика многочлена.

ЛИТЕРАТУРА

1. ***Спринджук, В.Г.*** Проблема Малера в метрической теории чисел / В.Г. Спринджук. – М.: Наука и Техника, 1967.
2. ***Шамукова, Н.В.*** О неоднородных диофантовых приближениях и целых алгебраических числах // Весці НАН Беларусі. Сер. фіз.-мат. навук. – 2007. – № 2. – С. 34-36.

Поступила в редакцию 23.09.2009 г.