Признаки неприводимости многочлена над $\mathbb{Z}[x]$ особого типа

Камал Янгиров

Введение

В работе рассмотрены признаки неприводимости многочлена над кольцом $\mathbb{Z}[x]$, связанные с теоретико-числовыми свойствами его значения в некоторой точке. Основной составляющей работы является доказательство признаков неприводимости многочлена, которые автору не удалось обнаружить в иных работах.

Экскурс

В связи с вопросом о неприводимости многочленов над $\mathbb{Z}[x]$ известен признак неприводимости Кона, имеющий ряд схожих формулировок. Ниже представлена одна из них:

Признак неприводимости Кона. *Пусть многочлен $P(x) = \sum_{i=0}^{n} a_i x^i$ степени n над $\mathbb{Z}[x]$ таков, что $0 \leq a_i \leq t-1$ и $P(t)$ является простым числом. Тогда $P(x)$ неприводим над $\mathbb{Z}[x]$.*

В работе [1] представлен следующий признак неприводимости, обобщающий (и в некотором смысле усиливающий) признак неприводимости Кона на случай многочленов с коэффициентами любого знака:

Признак неприводимости Мурти. *Для многочлена $P(x) = \sum_{i=0}^{n} a_i x^i$ степени n над $\mathbb{Z}[x]$ обозначим*

$$H = \max_{0 \leq i \leq n-1} |a_i / a_n|$$

Тогда, если для некоторого натурального $t \geq H + 2$, $P(t)$ является простым числом, то $P(x)$ неприводим над $\mathbb{Z}[x]$.

Оба признака требуют простоты значения многочлена в некоторой (будем называть её *важной*) достаточно удалённой справа от нуля точке, причём минимальная требуемая удалённость зависит от коэффициентов многочлена и может быть сколь угодно большой при фиксированной степени многочлена. В работе будет доказан признак неприводимости для многочленов с неотрицательными коэффициентами, требующий удалённости важной точки от нуля на расстояние, которое не зависит от коэффициентов многочлена. При этом, для особой точки будет требоваться не простота значения многочлена в ней, а более общее условие, позволяющее в отдельных случаях получать неприводимость многочлена, не находя у него удалённых точек с простым значением.

Обозначения

$S_R(z)$ - круг радиуса R с центром в z на комплексной плоскости
$\mathbb{R}_{+0} = \mathbb{R}_+ \cup \{0\}$
$|\gamma|$ - длина контура γ на комплексной плоскости
$\Omega = W(1) = 0,567143...$ - постоянная омега, определяемая как единственный вещественный корень уравнения $xe^x = 1$ (здесь $W(x)$ - функция Ламберта)
$\Omega^{-1} = \frac{1}{\Omega} = e^{\Omega} = 1,763222...$

Основная теорема

Адвокатом натурального числа N будем называть число $adv(N)$, являющееся наибольшим делителем N, не превосходящим $\sqrt{N}$. Адвокат всегда определён постольку, поскольку множество делителей N, не превосходящих $\sqrt{N}$, непусто (в него входит по крайне мере единица) и конечно (его мощность не превосходит $\lfloor\sqrt{N}\rfloor$).

Сформулировав это определение, можно сформулировать основную теорему данной работы.

Теорема. *Пусть многочлен $P(x)$ степени n над $\mathbb{Z}[x]$ с неотрицательными коэффициентами, не имеющими нетривиального общего делителя, таков, что $P(t) = V$, $adv(V) = L$, где $t \in \mathbb{N}$. Тогда $P(x)$ неприводим над $\mathbb{Z}[x]$, если $t^n \geq nL(t+L)^{n-1}$.*

Перед доказательством основной теоремы докажем ряд вспомогательных лемм.

Лемма 1. *Пусть натуральное число N представимо в виде произведения двух натуральных чисел $N = d_1 d_2$. Тогда $min(d_1, d_2) \leq adv(N)$.*

Доказательство. Без ограничения общности, $d_1 \leq d_2$. Тогда $d_1^2 <= d_1 d_2 = n \Rightarrow d_1 \leq \sqrt{N}$ и $min(d_1, d_2) = d_1$. Если $min(d_1, d_2) > adv(N)$, то имеем $adv(N) < d_1 \leq \sqrt{N}$, что противоречит определению адвоката в силу того, что d_1 является делителем N.

□

Лемма 2. *Пусть задан многочлен $H(z)$ степени $n \geq 1$ над $\mathbb{C}[z]$ со старшим коэффициентом A такой, что $H(z_C) = C$. Тогда у $H(z)$ есть корень z_0, удовлетворяющий неравенству $|z_0 - z_C| \leq \sqrt[n]{\frac{|C|}{|A|}}$.*

Доказательство. Докажем от противного. Обозначим корни многочлена $H(z)$ как $z_1, z_2, \ldots, z_n$. Тогда для них выполнены неравенства вида $|z_i - z_C| > \sqrt[n]{\frac{|C|}{|A|}}$. Многочлен $H(z)$ можно представить в следующем виде:

$$H(z) = A \prod_{i=1}^{n} (z - z_i)$$

Подставив в это выражение $z = z_C$ и взяв обе стороны равенства под модуль, получим

$$|C| = |H(z_C)| = |A| \prod_{i=1}^{n} |z_C - z_i| > |A|(\sqrt[n]{\frac{|C|}{|A|}})^n = |C|$$

Противоречие.

□

Лемма 3. *Пусть задан многочлен* $P(x) = \sum_{i=0}^{n} a_i x^i$ *степени* $n \geq 1$ *над* $\mathbb{R}_{+0}[x]$. *Тогда для* $z \in S_R(c) \setminus \{c+R\}$ *выполнено* $|P'(z)| < \frac{nP(c+R)}{c+R}$, *где* c *и* R *- положительные вещественные числа*

Доказательство.

$$|P'(z)| = |\sum_{i=1}^{n} i a_i z^{i-1}| \leq \sum_{i=1}^{n} |i a_i z^{i-1}|$$

В силу того, что $a_i \in \mathbb{R}_{+0}$, верны равенства вида $|i a_i z^{i-1}| = i a_i |z|^{i-1}$. Отсюда

$$|P'(z)| \leq \sum_{i=1}^{n} i|a_i||z|^{i-1} \leq \sum_{i=1}^{n} n a_i |z|^{i-1} = n \sum_{i=1}^{n} a_i |z|^{i-1}$$

Так как для $z \in S_R(c) \setminus \{c+R\}$, с учётом того, что $c > 0$, верно неравенство $|z| < c+R$ из очевидных геометрических соображений, а функция $f(x) = \sum\limits_{i=1}^{n} a_i x^{i-1}$, очевидно, возрастает по x при $x \geq 0$, получаем

$$|P'(z)| \leq n \sum_{i=1}^{n} a_i |z|^{i-1} < n \sum_{i=1}^{n} a_i (c+R)^{i-1} \leq \frac{n a_0}{c+R} + n \sum_{i=1}^{n} a_i (c+R)^{i-1} = \frac{nP(c+R)}{c+R}$$

□

Лемма 4. *Пусть задан многочлен* $P(x) = \sum_{i=0}^{n} a_i x^i$ *степени* n *над* $\mathbb{R}_{+0}[x]$. *Тогда* $P(x+C) \leq (1 + \frac{C}{x})^n P(x)$, *где* x *и* C *- положительные числа.*

Доказательство.

$$P(x+C) = \sum_{i=0}^{n} a_i (x+C)^i = \sum_{i=0}^{n} a_i (1 + \tfrac{C}{x})^i x^i \leq \sum_{i=0}^{n} a_i (1 + \tfrac{C}{x})^n x^i = (1 + \tfrac{C}{x})^n P(x)$$

□

Доказательство основной теоремы. Докажем от противного. Допустим, $P(x)$ приводим над $\mathbb{Z}[x]$, то есть существует нетривиальное разложение $P(x)$ над $\mathbb{Z}[x]$:

$$P(x) = Q(x)R(x)$$

Поскольку у коэффициентов $P(x)$ нет нетривиальных общих делителей, ни $Q(x)$, ни $R(x)$ не являются константами (потому, очевидно, $deg\, P \geq 2$). Заметим, что

$$V = |P(t)| = |Q(t)||R(t)|$$

Без ограничения общности, пусть $|Q(t)| \leq |R(t)$. Тогда, согласно лемме 1, $|Q(t)| \leq L$. Так как $Q(x)$ не константа, то можно воспользоваться леммой 2, откуда имеем, что $Q(x)$ имеет корень $z \in \mathbb{C}$, удовлетворяющий неравенству $|z-t| \leq \sqrt[n]{\frac{|L|}{|A_Q|}}$, где A_Q - старший коэффициент $Q(x)$. Так как $|A_Q| \geq 1$, $L \geq 1$, имеем $\sqrt[n]{\frac{|L|}{|A_Q|}} \leq \sqrt[n]{L} \leq L$, откуда $|z-t| \leq L$. Осталось заметить, что любой корень $Q(x)$ также является корнем $P(x)$, откуда $P(z) = 0$.

Рассмотрим следующее соотношение:

$$P(z) - P(t) = \int\limits_{\gamma} P'(z) dz$$

Здесь γ - отрезок комплексной плоскости, соединяющий t и z. Из этого определения очевидно, что $\gamma \in S_L(t) \setminus \{t+L\}$ в силу того, что $|z-t| \leq L$ и $z \neq t+L$, поскольку $P(t+L) > 0$. Тогда, с учётом того, что $deg\, P \geq 2$, можно воспользоваться леммой 3 применительно к интегральному представлению разности выше:

$$V = |0 - V| = |P(z) - P(t)| = |\int\limits_{\gamma} P'(z)dz| \leq \int\limits_{\gamma} |P'(z)||dz| < \int\limits_{\gamma} \frac{nP(t+L)}{t+L}|dz| = \frac{nP(t+L)}{t+L}|\gamma| = \frac{nP(t+L)}{t+L}|z-t| \leq \frac{nLP(t+L)}{t+L}$$

Применяя лемму 4 к выражению $P(t+L)$, получаем

$$V < \frac{nLP(t+L)}{t+L} \leq \frac{nL(1+\frac{L}{t})^n P(t)}{t+L} = \frac{nL(1+\frac{L}{t})^n V}{t+L}$$

Поскольку, очевидно, $V > 0$, отсюда следует

$$1 < \frac{nL(1+\frac{L}{t})^n}{t+L} \Leftrightarrow t^n < nL(t+L)^{n-1}$$

Что противоречит условию теоремы.

□

Аналитические леммы и альтернативные формулировки основной теоремы

С учётом очевидного неравенства $L > 0$, неравенство $t^n \geq nL(t+L)^{n-1}$ равносильно неравенству $(\frac{t}{L})^n \geq n(1+\frac{t}{L})^{n-1}$. Определим следующее семейство функций:

$$f_n(x) = x^n - n(x+1)^{n-1},\ n \in \mathbb{N}$$

Тогда последнее неравенство можно переписать в виде $f_n(\frac{t}{L}) \geq 0$. В связи с этим представляет интерес вопрос об изучении поведения функций данного семейства. Этот вопрос будет изучен в этом разделе.

Лемма 5. *Для любого $n \in \mathbb{N}$ функция $f_n(x)$ на $\mathbb{R}_{+0}$ имеет единственный нуль χ_n, причём слева от него она принимает отрицательные значения, а справа - положительные.*

Доказательство. При $x \neq 0$ функцию $f_n(x)$ можно записать в следующем виде:

$$f_n(x) = x^n(1 - \frac{n}{x}(1+\frac{1}{x})^{n-1}) = x^n g_n(\tfrac{1}{x}),\ \text{где}\ g_n(x) = 1 - nx(1+x)^{n-1}$$

Нетрудно заметить, что $g_n(x)$ является строго убывающей функцией, а также то, что $g_n(0) = 1 > 0$ и $\lim\limits_{x\to\infty} g_n(x) = -\infty$. Отсюда следует, что $g_n(x)$ имеет единственный нуль γ_n на $\mathbb{R}_{+0}$, причём $\gamma_n \neq 0$. При этом, при $0 < x < \gamma_n$ имеем $g_n(x) > 0$, а при $x > \gamma_n$ имеем $g_n(x) < 0$. Пусть $\chi_n = \frac{1}{\gamma_n}$. Тогда, очевидно, $f(\chi_n) = \chi_n^n g_n(\gamma_n) = 0$. При $0 < x < \chi_n$ имеем $\frac{1}{x} > \gamma_n$, откуда $f_n(x) = x^n g_n(\frac{1}{x}) < 0$. Аналогично при $x > \chi_n$ имеем $f_n(x) > 0$. В совокупности с тем замечанием, что $f_n(0) = -n < 0$, мы получаем требуемое.

□

Из леммы 5 следует, что неравенство $f_n(\frac{t}{L}) \geq 0$ равносильно неравенству $t \geq \chi_n L$. откуда следует, что основную теорему можно сформулировать следующим образом:

Альтернативная формулировка. *Пусть многочлен $P(x)$ степени n над $\mathbb{Z}[x]$ с неотрицательными коэффициентами, не имеющими нетривиального общего делителя, таков, что $P(t) = V$, $adv(V) = L$, где $t \in \mathbb{N}$. Тогда $P(x)$ неприводим над $\mathbb{Z}[x]$, если $t \geq \chi_n L$.*

Полезно иметь представление о членах последовательности χ_n. С одной стороны, вывести их в явном виде как элементарную функцию от n не представляется возможным. С другой стороны, нетрудно доказать оценки, представленные в лемме ниже.

Лемма 6. $\Omega^{-1}n - 1 < \chi_n < \Omega^{-1}n$

Доказательство. Заметим, что $\Omega^{-1}n - 1 \geq \Omega^{-1} - 1 > 0$, а потому $\Omega^{-1}n - 1$, как и $\Omega^{-1}n$, принадлежит $\mathbb{R}_{+0}$. Потому для доказательства данных неравенств достаточно показать, что $f_n(\Omega^{-1}n - 1) < 0$ и $f_n(\Omega^{-1}n) > 0$, после чего воспользоваться леммой 5. Пользуясь тем, что $1 + x < e^x$ при всех вещественных $x \neq 0$, покажем, что последние неравенства действительно выполнены:

$$f_n(\Omega^{-1}n - 1) < 0 \Leftrightarrow (\Omega^{-1}n - 1)^n < n(\Omega^{-1}n)^{n-1} \Leftrightarrow (1 - \tfrac{\Omega}{n})^n < \Omega, \text{ что верно,}$$
$$\text{поскольку } (1 - \tfrac{\Omega}{n})^n < e^{-n\frac{\Omega}{n}} = e^{-\Omega} = \Omega$$

$$f_n(\Omega^{-1}n) > 0 \Leftrightarrow (\Omega^{-1}n)^n > n(\Omega^{-1}n + 1)^{n-1} \Leftrightarrow \Omega^{-1} > (1 + \tfrac{\Omega}{n})^{n-1}, \text{ что верно,}$$
$$\text{поскольку } (1 + \tfrac{\Omega}{n})^{n-1} < e^{(n-1)\frac{\Omega}{n}} < e^{\Omega} = \Omega^{-1}$$

□

Из леммы 6 следует, что неравенство $t > \Omega^{-1}nL$ является огрублением неравенства $t \geq \chi_n L$. Отсюда можно получить следующее следствие из альтернативной формулировки основной теоремы:

Следствие 1. *Пусть многочлен $P(x)$ степени n над $\mathbb{Z}[x]$ с неотрицательными коэффициентами, не имеющими нетривиального общего делителя, таков, что $P(t) = V$, $adv(V) = L$, где $t \in \mathbb{N}$. Тогда $P(x)$ неприводим над $\mathbb{Z}[x]$, если $t > \Omega^{-1}Ln$.*

Частные следствия из основной теоремы

V - дискретное полупростое[1] число

Если V является дискретным полупростым числом, то есть $V = p_1p_2$, где p_1 и $p_2 > p_1$ - некоторые простые числа, то, очевидно, $adv(V) = p_1$. Отсюда мы имеем частные следствия 2 и 3 из альтернативной формулировки основной теоремы и следствия 1 соответственно:

Следствие 2. *Пусть многочлен $P(x)$ степени n над $\mathbb{Z}[x]$ с неотрицательными коэффициентами, не имеющими нетривиального общего делителя, таков, что $P(t) = V$, где V - дискретное полупростое число с меньшим простым делителем p, $t \in \mathbb{N}$. Тогда $P(x)$ неприводим над $\mathbb{Z}[x]$, если $t \geq \chi_n p$.*

[1] Дискретным полупростым числом называется полупростое число, не являющееся квадратом простого числа

Следствие 3. *Пусть многочлен $P(x)$ степени n над $\mathbb{Z}[x]$ с неотрицательными коэффициентами, не имеющими нетривиального общего делителя, таков, что $P(t) = V$, где V - дискретное полупростое число с меньшим простым делителем p, $t \in \mathbb{N}$. Тогда $P(x)$ неприводим над $\mathbb{Z}[x]$, если $t > \Omega^{-1}pn$.*

Следствия 2 и 3 могут быть полезны, если неизвестны достаточно удалённые справа от нуля точки, в которых многочлен принимает простые значения, но известны такого же рода точки, в которых многочлен принимает значения вида $2p$, $3p$, $5p$ и так далее, где p - некоторое простое число.

V - простое число

Очевидно, что если V - простое число, то $adv(V) = 1$. В этом случае неравенство $t \geq \chi_n L$ принимает вид $t \geq \chi_n$, что в силу целостности t равносильно неравенству $t \geq \lceil \chi_n \rceil$. Потому введём обозначение $\overline{\chi}_n = \lceil \chi_n \rceil$.

Лемма 7. $\lfloor \Omega^{-1}n \rfloor \leq \overline{\chi}_n \leq \lceil \Omega^{-1}n \rceil$

Доказательство. Согласно лемме 6, $\chi_n \in (\Omega^{-1}n - 1,\ \Omega^{-1}n)$. Поскольку Ω трансцендентно [2], а, следовательно, иррационально, то концы этого интервала являются нецелыми. В любом интервале длины 1 с нецелыми концами содержится ровно одно целое число, и в данном случае это, очевидно, $\lfloor \Omega^{-1}n \rfloor$. Если $\chi_n \leq \lfloor \Omega^{-1}n \rfloor$, то $\overline{\chi}_n$ равняется $\lfloor \Omega^{-1}n \rfloor$ как ближайшему справа целому числу (поскольку оба числа лежат в одном интервале длины 1). Аналогично если $\chi_n > \lfloor \Omega^{-1}n \rfloor$, то $\overline{\chi}_n = \lfloor \Omega^{-1}n \rfloor + 1 = \lceil \Omega^{-1}n \rceil$. Отсюда либо $\overline{\chi}_n = \lfloor \Omega^{-1}n \rfloor$, либо $\overline{\chi}_n = \lceil \Omega^{-1}n \rceil$, откуда и следует требуемое.

□

Частным следствием из альтернативной формулировки основной теоремы в случае простого V является следствие 4, из которого в совокупности с леммой 7 следует следствие 5:

Следствие 4. *Пусть многочлен $P(x)$ степени n над $\mathbb{Z}[x]$ с неотрицательными коэффициентами, не имеющими нетривиального общего делителя, таков, что $P(t)$ является простым числом, $t \in \mathbb{N}$. Тогда $P(x)$ неприводим над $\mathbb{Z}[x]$, если $t \geq \overline{\chi}_n$.*

Следствие 5. *Пусть многочлен $P(x)$ степени n над $\mathbb{Z}[x]$ с неотрицательными коэффициентами, не имеющими нетривиального общего делителя, таков, что $P(t)$ является простым числом, $t \in \mathbb{N}$. Тогда $P(x)$ неприводим над $\mathbb{Z}[x]$, если $t \geq \lceil \Omega^{-1}n \rceil$.*

Приложение

n	χ_n	$\overline{\chi}_n$
1	1	1
2	2, 732...	3
3	4, 486...	5
4	6, 245...	7
5	8, 006...	9
6	9, 767...	10
7	11, 529...	12
8	13, 292...	14
9	15, 054...	16
10	16, 817...	17
11	18, 580...	19
12	20, 343...	21
13	22, 106...	23
14	23, 869...	24
15	25, 632...	26
16	27, 395...	28
17	29, 158...	30
18	30, 921...	31
19	32, 684...	33
20	34, 447...	35
21	36, 210...	37
22	37, 973...	38
23	39, 737...	40
24	41, 500...	42
25	43, 263...	44
26	45, 026...	46
27	46, 789...	47
28	48, 522...	49
29	50, 315...	51
30	52, 079...	53
31	53, 842...	54
32	55, 605...	56
33	57, 368...	58
34	59, 131...	60
35	60, 895...	61
36	62, 658...	63
37	64, 421...	65
38	66, 184...	67
39	67, 947...	68
40	69, 710...	70

Список литературы

[1] Murty, Ram (2002). "Prime Numbers and Irreducible Polynomials". American Mathematical Monthly. 109 (5): 452–458.

[2] Mező, István; Baricz, Árpád (November 2017). "On the Generalization of the Lambert W Function". Transactions of the American Mathematical Society. 369 (11): 7928.