

М. В. ЯКОВКИН

ОБОБЩЕНИЯ ОДНОГО КРИТЕРИЯ НЕПРИВОДИМОСТИ ПОЛИНОМОВ

(Представлено академиком О. Ю. Шмидтом 24 VIII 1947)

В настоящей статье мы ставим своей целью дать некоторые улучшения одной теоремы ⁽¹⁾, обобщающей, в частности, критерии неприводимости полиномов, найденные Поля ⁽²⁾ и А. Сohn'ом ⁽³⁾ и которая реферировалась Н. Г. Чеботаревым ⁽⁴⁾ и Н. W. Brinkman'ом ⁽⁵⁾.

Первое улучшение относится к расширению области аргумента целой рациональной функции, неприводимость которой определяется данным критерием.

Во второй теореме работы ⁽¹⁾ аргумент x не может принимать значений, принадлежащих сегменту $[R(\alpha), -R(\alpha)]$, где $R(\alpha)$ — верхняя граница вещественных частей корней целой рациональной функции. Между тем, это ограничение для аргумента x является слишком сильным, аргумент x может принимать значения и из некоторых интервалов, лежащих на отрезке $[R(\alpha), -R(\alpha)]$.

Теорема 1. Если целочисленный полином $f(x)$ степени n при некотором значении аргумента x , равном рациональному числу $\frac{p}{q}$, взятом вне окрестностей единичного радиуса вещественных частей каждого из корней $f(x)$, принимает значение $f\left(\frac{p}{q}\right)$ такое, что $q^n f\left(\frac{p}{q}\right)$ есть простое число, то полином $f(x)$ неприводим в поле рациональных чисел.

Доказательство. Допустим, что $f(x)$ приводим в поле рациональных чисел. Тогда должны существовать по крайней мере два полинома $\varphi(x)$ и $\psi(x)$, по известной теореме Гаусса, также с целыми коэффициентами, удовлетворяющие равенству

$$f(x) = \varphi(x)\psi(x). \quad (1)$$

Обозначив через γ_φ вещественные корни функции $\varphi(x)$; $\alpha_\varphi \pm \beta_\varphi i$ — комплексные корни функции $\varphi(x)$; γ_ψ — вещественные корни функции $\psi(x)$ и $\alpha_\psi \pm \beta_\psi i$ — комплексные корни функции $\psi(x)$, равенство (1) можем переписать в следующем виде:

$$f(x) = b_0 \prod_{\varphi} \{(x - \gamma_\varphi)[(x - \alpha_\varphi)^2 + \beta_\varphi^2]\} \cdot c_0 \prod_{\psi} \{(x - \gamma_\psi)[(x - \alpha_\psi)^2 + \beta_\psi^2]\}, \quad (2)$$

где $\prod$ — символ произведения нескольких сомножителей, а b_0 и c_0 — старшие коэффициенты, соответственно, функций $\varphi(x)$ и $\psi(x)$.

При $x = \frac{p}{q}$ из равенства (2) мы получим

$$f\left(\frac{p}{q}\right) = b_0 \prod_{\varphi} \left\{ \left(\frac{p}{q} - \gamma_{\varphi}\right) \left[\left(\frac{p}{q} - \alpha_{\varphi}\right)^2 + \beta_{\varphi}^2 \right] \right\} \times \\ \times c_0 \prod_{\psi} \left\{ \left(\frac{p}{q} - \gamma_{\psi}\right) \left[\left(\frac{p}{q} - \alpha_{\psi}\right)^2 + \beta_{\psi}^2 \right] \right\}. \quad (3)$$

По условию теоремы $\left|\frac{p}{q} - \gamma_{\varphi}\right| > 1$, $\left|\frac{p}{q} - \gamma_{\psi}\right| > 1$, $\left|\frac{p}{q} - \alpha_{\varphi}\right| > 1$ и $\left|\frac{p}{q} - \alpha_{\psi}\right| > 1$. Но тогда все сомножители чисел $\varphi\left(\frac{p}{q}\right)$ и $\psi\left(\frac{p}{q}\right)$ по модулю превышают единицу, значит $\left|\varphi\left(\frac{p}{q}\right)\right| > 1$ и $\left|\psi\left(\frac{p}{q}\right)\right| > 1$.

Если s и r — степени полиномов $\varphi(x)$ и $\psi(x)$, то равенство (1) при $x = \frac{p}{q}$ умножением обеих частей равенства на $q^n = q^s q^r$ дает

$$\left| q^n f\left(\frac{p}{q}\right) \right| = \left| q^s \varphi\left(\frac{p}{q}\right) \right| \left| q^r \psi\left(\frac{p}{q}\right) \right|,$$

где $\left| q^s \varphi\left(\frac{p}{q}\right) \right| \geq \left| \varphi\left(\frac{p}{q}\right) \right| > 1$ и $\left| q^r \psi\left(\frac{p}{q}\right) \right| \geq \left| \psi\left(\frac{p}{q}\right) \right| > 1$, т. е. мы пришли к тому, что число $q^n f\left(\frac{p}{q}\right)$ должно быть составным, а оно по условию теоремы простое.

Примечание. В формулировке теоремы 1 условия $\left|\frac{p}{q} - \gamma\right| > 1$ и $\left|\frac{p}{q} - \alpha\right| > 1$ можно заменить более слабыми $\left|\frac{p}{q} - \gamma\right| \geq 1$ и $\left|\frac{p}{q} - \alpha\right| \geq 1$, добавив еще одно условие $f\left(\frac{p-1}{q}\right) \neq 0$.

Второе улучшение относится к числу и природе делителей рассматриваемого значения $q^n f\left(\frac{p}{q}\right)$ многочлена $f(x)$, неприводимость которого определяется данной теоремой.

Во второй теореме работы (1) требуется, чтобы целое число $\left[\frac{q_1 q_2}{(q_1; q_2)}\right]^n f\left(\frac{p_1}{q_1} + \frac{p_2}{q_2}\right)$ было простым. Это требование также является слишком сильным и вытекает как следствие из следующей, более общей теоремы.

Теорема 2. Если для целочисленной функции $f(x)$ степени n с верхней границей вещественных частей корней, равной $R(\alpha)$, найдутся два рациональных числа $\frac{p_1}{q_1} \geq R(\alpha)$ и $\frac{p_2}{q_2} > 0$ такие, что

$$\left[\frac{q_1 q_2}{(q_1; q_2)}\right]^n f\left(\frac{p_1}{q_1} + \frac{p_2}{q_2}\right)$$

не разложимо на два целых множителя, модули которых были бы не меньше числа

$$\left| \frac{\left[\frac{q_1 q_2}{(q_1; q_2)}\right]^{m+1} - p_2^{m+1}}{\left[\frac{q_1 q_2}{(q_1; q_2)}\right] - p_2} \right| \quad \left(\frac{n}{2} \geq m \geq 1 \right),$$

то функция $f(x)$ не может иметь в поле рациональных чисел делителя степени выше m .

Доказательство. Сделаем замену $x = y + \frac{p_1}{q_1}$ аргумента x функции $f(x)$ и допустим, что при условиях данной теоремы функция $f(x)$, а значит и функция $F(y) = f\left(y + \frac{p_1}{q_1}\right)$ в поле рациональных чисел имеют делителя степени выше m , т. е. допустим, что имеет место равенство

$$F(y) = \varphi(y) \psi(y). \quad (4)$$

Каждая из функций $F(y)$, $\varphi(y)$ и $\psi(y)$ равенства (4) имеет своими коэффициентами рациональные дроби одного знака ⁽¹⁾ со знаменателями, равными степеням q_1 .

Не нарушая общности рассуждений, допустим, что степень s функции $\varphi(y)$ превышает m , и тогда степень $r = n - s$ функции $\psi(y)$ также превышает m (учитывая условие теоремы $\frac{n}{2} \geq m \geq 1$).

Из равенства (4) при $y = \frac{p_2}{q_2}$ получим

$$F\left(\frac{p_2}{q_2}\right) = \varphi\left(\frac{p_2}{q_2}\right) \psi\left(\frac{p_2}{q_2}\right) \quad (5)$$

или

$$f\left(\frac{p_2}{q_2} + \frac{p_1}{q_1}\right) = \varphi\left(\frac{p_2}{q_2}\right) \psi\left(\frac{p_2}{q_2}\right). \quad (6)$$

Обозначив наименьшее кратное чисел q_1 и q_2 через q_0 и умножив обе части равенства (6) на

$$q_0^n = \left[\frac{q_1 q_2}{(q_1; q_2)}\right]^n = \left[\frac{q_1 q_2}{(q_1; q_2)}\right]^s \left[\frac{q_1 q_2}{(q_1; q_2)}\right]^r,$$

получим

$$\left[\frac{q_1 q_2}{(q_1; q_2)}\right]^n f\left(\frac{p_1}{q_1} + \frac{p_2}{q_2}\right) = \left[\frac{q_1 q_2}{(q_1; q_2)}\right]^s \varphi\left(\frac{p_2}{q_2}\right) \left[\frac{q_1 q_2}{(q_1; q_2)}\right]^r \psi\left(\frac{p_2}{q_2}\right). \quad (7)$$

Нетрудно видеть, что сомножители правой части равенства (7) имеют следующий вид:

$$\left[\frac{q_1 q_2}{(q_1; q_2)}\right]^s \varphi\left(\frac{p_2}{q_2}\right) = b_0 p_2^s + b_1 p_2^{s-1} q_0 + \dots + b_{s-1} p_2 q_0^{s-1} + b_s q_0^s$$

и

$$\left[\frac{q_1 q_2}{(q_1; q_2)}\right]^r \psi\left(\frac{p_2}{q_2}\right) = c_0 p_2^r + c_1 p_2^{r-1} q_0 + \dots + c_{r-1} p_2 q_0^{r-1} + c_r q_0^r.$$

где $|b_i| > 1$ ($i=0, 1, 2, \dots, s$) и $|c_i| \geq 1$ ($i=0, 1, 2, \dots, r$).

Таким образом, допустив, что $f(x)$ имеет делителя степени выше чем m , мы пришли к тому, что число $\left|\left[\frac{q_1 q_2}{(q_1; q_2)}\right]^n f\left(\frac{p_1}{q_1} + \frac{p_2}{q_2}\right)\right|$ может

быть представлено в виде произведения двух целых чисел

$$\left| \left[\frac{q_1 q_2}{(q_1; q_2)} \right]^s \varphi \left(\frac{p_2}{q_2} \right) \right| \geq \left| \frac{q_0^{s+1} - p_2^{s+1}}{q_0 - p_2} \right| > \left| \frac{q_0^{m+1} - p_2^{m+1}}{q_0 - p_2} \right|,$$

$$\left| \left[\frac{q_1 q_2}{(q_1; q_2)} \right]^r \psi \left(\frac{p_2}{q_2} \right) \right| \geq \left| \frac{q_0^{r+1} - p_2^{r+1}}{q_0 - p_2} \right| > \left| \frac{q_0^{m+1} - p_2^{m+1}}{q_0 - p_2} \right|,$$

модуль каждого из которых превышает число

$$\left| \frac{q_0^{m+1} - p_2^{m+1}}{q_0 - p_2} \right| = \left| \frac{\left[\frac{q_1 q_2}{(q_1; q_2)} \right]^{m+1} - p_2^{m+1}}{\left[\frac{q_1 q_2}{(q_1; q_2)} \right] - p_2} \right|,$$

что противоречит условию теоремы.

Из этой теоремы, как следствия, вытекают следующие критерии неприводимости многочленов в поле рациональных чисел.

Следствие 1. Если для целочисленной функции $f(x)$ степени n с верхней границей вещественных частей корней, равной $R(\alpha)$, найдутся два рациональных числа $\frac{p_1}{q_1} \geq R(\alpha)$ и $\frac{p_2}{q_2} > 0$ такие, что целое число $\left[\frac{q_1 q_2}{(q_1; q_2)} \right]^n f \left(\frac{p_1}{q_1} + \frac{p_2}{q_2} \right)$ не разложимо на два целых множителя, модули которых были бы не меньше числа $\left| \left[\frac{q_1 q_2}{(q_1; q_2)} \right] + p_2 \right|$, то функция $f(x)$ неприводима в поле рациональных чисел.

Это следствие получается из теоремы 2 настоящей статьи как частный случай при $m=1$, а из него, в свою очередь, как частный случай вытекает критерий неприводимости полиномов, доказанный нами в работе (1).

Следствие 2. Если для целочисленной функции $f(x)$ степени n с верхней границей вещественных частей корней, равной $R(\alpha)$, и не имеющей рациональных корней, найдутся два рациональных числа $\frac{p_1}{q_1} \geq R(\alpha)$ и $\frac{p_2}{q_2} > 0$ такие, что целое число $\left[\frac{q_1 q_2}{(q_1; q_2)} \right]^n f \left(\frac{p_1}{q_1} + \frac{p_2}{q_2} \right)$ не разложимо на два множителя, модули которых, были бы не меньше числа $\left| \left[\frac{q_1 q_2}{(q_1; q_2)} \right]^2 + \left[\frac{q_1 q_2}{(q_1; q_2)} \right] p_2 + p_2^2 \right|$, то функция $f(x)$ неприводима в поле рациональных чисел.

Математический институт
им. В. А. Стеклова
Академии Наук СССР

Поступило
24 VIII 1947

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

¹ М. В. Яковкин, ДАН, 28, № 9 (1940). ² Г. М. Шапиро, Высшая алгебра, 1938. ³ Полиа и Сеге, Задачи и теоремы из анализа, II, 1937. ⁴ Физ.-математ. реферативн. журн., 4, в. 4, апрель (1941). ⁵ Math. Rev., 2, 4, 117, April (1941).