БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ * ACADÉMIE BULGARE DES SCIENCES
ИЗВЕСТИЯ НА МАТЕМАТИЧЕСКИЯ ИНСТИТУТ
BULLETIN DE L'INSTITUT DE MATHÉMATIQUES
Том (Tome) XI

НЯКОИ ТЕОРЕМИ ЗА НЕРАЗЛОЖИМОСТ НА ЦЕЛОЧИСЛЕНИ ПОЛИНОМИ В ПОЛЕТО НА РАЦИОНАЛНИТЕ ЧИСЛА, КОИТО ПРИЕМАТ СТОЙНОСТИ СТЕПЕНИ НА ПРОСТО ЧИСЛО

Димитър Пиргов и Елена Кантарджиева

В настоящата работа обект на разглеждане са примитивните целочислени полиноми, които в една съвкупност от цели числа приемат стойност степен на едно и също просто число.

Полиноми от подобен вид са разглеждани от Яковкин [1], а така също и от Рейнолдс [2].

Предварително ще цитираме някои известни резултати, които ще използваме в изложението по-нататък.

I. Нека $\varphi(x)$ и $\psi(x)$ са целочислени полиноми от степен $2k$ и $\varphi(x)\psi(x)>0$, Полиномите $\varphi(x)$ и $\psi(x)$ не могат да приемат стойности p_1 и p_2, $p_1 \neq p_2$, $p_1<p_2$, в по $2k$ различни цели стойности на x, ако $\varphi(x_i)\psi(x_i)=p_1p_2$, $i=1, 2, \ldots, 4k$ [4].

II. Ако конгруенцията $f(x)\equiv 0 \pmod p$ от степен n има повече от n решения, всички коефициенти на целочисления полином $f(x)$ се делят на простото число p [3].

Т е о р е м а 1. Целочисленият примитивен полином $f(x)$ от степен n, който няма реални корени, е неразложим в полето на рационалните числа, ако съществуват цели числа $x_1, x_2, \ldots, x_n$, неконгруентни помежду си по модул p, за които $f(x)$ приема стойност p^k, $k\geqq 1$, p—просто число.*

Доказателство. Допускаме противното:

$$f(x)=\varphi(x)\psi(x). \tag{1}$$

От условието на теоремата следва, че $\varphi(x)$ и $\psi(x)$ нямат реални корени и са примитивни. Да означим с m степента на $\varphi(x)$; тогава степента на $\psi(x)$ е $n-m$. Да заместим в (1) $x=x_i$, $i=1, 2, \ldots, n$. Получаваме равенствата

$$\begin{aligned} p^k &= \varphi(x_1)\psi(x_1), \\ p^k &= \varphi(x_2)\psi(x_2), \\ &\cdots \\ p^k &= \varphi(x_n)\psi(x_n). \end{aligned} \tag{2}$$

* Разглежданата класа полиноми е безкрайна, тъй като числото p може да бъде избрано достатъчно голямо.

Понеже полиномите $\varphi(x)$ и $\psi(x)$ нямат реални корени, за тях имаме една от следните възможности: $q(x)>0$ и $\psi(x)>0$ или $q(x)<0$ и $\psi(x)<0$ за всяко реално x. Нека $q(x)>0$ и $\psi(x)>0$. Тогава произведенията в дясната страна на (2) са от вида $p^{k_i}p^{k_j}$, $i, j=1, 2, \ldots, n$. За числата k_i и k_j са в сила релациите $k_i+k_j=k$, $0\leq k_i\leq k$ и $0\leq k_j\leq k$. Някои от числата k_i, а така също от числата k_j могат да бъдат равни помежду си. За степените на полиномите $\varphi(x)$ и $\psi(x)$ имаме една от следните възможности:

$$m<n-m,\ m>n-m \text{ и } m=n-m.$$

а) Нека $m<n-m$. Тогава измежду числата k_i, $i=1, 2, \ldots, n$, може да има най-много m на брой равни на нула, защото в противен случай $q(x)$ 1. Измежду числата x_i, $i=1, 2, \ldots, n$, да означим съответно с $x'_1, x'_2, \ldots, x'_m$ тези, за които $k_i=0$, т. е. $q(x'_\nu)=1$, $\nu=1, 2, \ldots, m$. За останалите от числата x_i, които са $n-m$ на брой, $\varphi(x)$ приема стойност степен на p. От $m<n-m$ и II следва, че всички коефициенти на $q(x)$ се делят на p, т. е. $\varphi(x)$ не е примитивен, което противоречи на условието на теоремата.

б) Нека $m>n-m$. В този случай разсъжденията са аналогични на тези от а), само че за полинома $\psi(x)$.

в) Нека $m=n-m$. Понеже $\varphi(x)$ и $\psi(x)$ нямат реални корени, имаме $m=n-m=n/2$ 0 (mod 2).

От числата x_i, $i=1, 2, \ldots, n$, има най-много $m=n/2$, за които $\varphi(x)$ приема стойност единица, защото в противен случай $\varphi(x)\equiv 1$. Нека x'_1 $x'_2, \ldots, x'_m$ са числата, за които $\varphi(x'_\nu)=1$, $\nu=1, 2, \ldots, n/2$. Тогава за $\psi(x)$ ще имаме $\psi(x'_\nu)=p^k$, $\nu=1, 2, 3, \ldots, n/2$. Останалите от числата x_i, $i=1, 2, \ldots, n$, за които $\varphi(x)$ 1, да означим с $x''_1, x''_2, \ldots, x''_{n/2}$. Ако поне за едно от тях $\psi(x)\neq 1$, съгласно II следва, че всички коефициенти на $\psi(x)$ се делят на p, т. е. $\psi(x)$ не е примитивен, което противоречи на условието на теоремата. Следователно $\psi(x''_\nu)=1$, $\nu=1, 2, \ldots, n/2$. От казаното дотук се вижда, че в точките x'_ν, $\nu=1, 2, \ldots, n/2$, за полиномите $q(x)$ и $\psi(x)$ имаме $q(x'_\nu)=1$ и $\psi(x'_\nu)=p^k$, аналогично за числата x''_ν, $\nu=1, 2, \ldots, n/2$, имаме $q(x''_\nu)=p^k$, $\psi(x''_\nu)=1$, което е невъзможно съгласно I ($p_1=1$, $p_2=p^k$). Следователно $f(x)$ е неразложим в полето на рационалните числа.

Доказаната теорема е по-силна от критерия на Рейнолдс [2]. Действително доказаната от нас теорема не допуска разлагане на полинома $f(x)$ на множители, степените на които могат да бъдат равни на 4, 5, 8, 9, 10 или 12, както това е възможно според теоремата на Рейнолдс. Тук, разбира се, трябва да отбележим, че броят на числата, при които $f(x)$ приема стойност p^k, при Рейнолдс е $\tau>\frac{4}{5}n$.

Ще докажем едно помощно твърдение, което ще използваме за доказателството на следващата теорема.

Лема. Ако $f(x)$ е целочислен полином от степен n, на който всички корени лежат вън от ивицата $|I_m(z)|\leq q_1$, то $f(x)>a_0q_1^n$, $a_0\neq 1$.

Доказателство. Понеже $f(x)$ има само комплексни корени, имаме

$$f(x)=a_0\prod_{k=1}^{n/2}[(x-\alpha_k)^2+\beta_k^2]. \tag{3}$$

От условието на лемата имаме $|\beta_k|>q_1$, $k=1, 2, \ldots, n/2$.
Тогава от (3) получаваме

$$f(x)=a_0\prod_{k=1}^{n/2}[(x-\alpha_k)^2+\beta_k^2]>a_0\prod_{k=1}^{n/2}[(x-\alpha_k)^2+q_1^2]>a_0q_1^n,$$

което искахме да докажем.

Теорема 2. Ако всички корени на примитивния целочислен полином $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$, $a_0\neq 0$ лежат вън от ивицата $|I_m(z)|\leqq q_1$ и съществуват цели числа, неконгруентни помежду си по модул p, x_1, $x_2, \ldots, x_\nu$, $\nu>n/2$, за които $f(x)$ приема стойност p^kq_1 (p — просто число, $k\geqq 1$), $f(x)$ е неразложим в полето на рационалните числа.

Доказателство. Допускаме противното:

$$f(x)=\varphi(x)\psi(x). \tag{4}$$

От условието на теоремата следва, че $\varphi(x)$ и $\psi(x)$ са примитивни и нямат реални корени. Като заместим в (4) $x=x_j$, $j=1, 2, \ldots, \nu$, получаваме равенствата

$$\begin{aligned} p^kq_1&=\varphi(x_1)\psi(x_1),\\ p^kq_1&=\varphi(x_2)\psi(x_2),\\ &\cdots\\ p^kq_1&=\varphi(x_\nu)\psi(x_\nu). \end{aligned} \tag{5}$$

Да означим с m степента на $\varphi(x)$, тогава степента на $\psi(x)$ ще бъде $n-m$.

За степените на полиномите $\varphi(x)$ и $\psi(x)$ съществуват следните възможности: $m<n-m$, $m>n-m$ и $m=n-m$. Понеже корените на полиномите $\varphi(x)$ и $\psi(x)$ лежат също вън от ивицата $|I_m(z)|\leqq q_1$, съгласно лемата имаме $\varphi(x_i)>|b_0|q_1^m$ и $\psi(x_i)>|c_0|q_1^{n-m}$, $i=1, 2, \ldots, \nu$, $b_0c_0=a_0$, b_0, c_0 — цели числа.

а) Нека $m<n-m$ ($m<n/2$). За числата $\varphi(x_i)$, $i=1, 2, \ldots, \nu$, от (5) и $\varphi(x_i)>|b_0|q_1^m$ следва, че се делят на p. Тогава от $m<\nu$ ($\nu>n/2$) и съгласно II следва, че $\varphi(x)$ не е примитивен, тъй като x_i, $i=1, 2, \ldots, \nu$, не са конгруентни помежду си по модул p. Достигнахме до противоречие.

б) Нека $m>n-m$ ($n-m<n/2$)). Разсъжденията са аналогични на тези от а), само че сега за полинома $\psi(x)$.

в) Нека $m=n-m=n/2$. Разсъжденията са същите както в а) и б), тъй като $\nu>n/2$.

Следователно теоремата е доказана напълно.

В своята работа [1] Яковкин доказва следната теорема, от която следва усиленият критерии на Рейнолдс.

Ако примитивният полином $f(x)$ от степен n в целите точки x_1, $x_2, \ldots, x_r$, неконгруентни помежду си по модул p (p — просто число) и несъдържащи в своите околности с радиус q нито една от реалните части на корените на $f(x)$, приема значение от вида $f(x_i)=p^kt$ ($t\leqq q^s$), този полином в полето на рационалните числа не може да има делители от степен m, $s\leqq m<r$.

От тази теорема следва усиленият критерий на Рейнолдс, който гласи следното.

Ако примитивният целочислен полином $f(x)$ в $r>[n/2]$ цели точки, неконгруентни помежду си по модул p и несъдържащи в своите околности с радиус $q=1$ реални части на корените на $f(x)$, приема стойности степен на едно и също просто число p, този полином е неразложим в полето на рационалните числа.

Ще докажем една теорема, от която следва твърдение, по-силно от усиления критерий на Рейнолдс.

Предварително да отбележим следното известно твърдение. Нека $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ е целочислен полином. Да означим с α_1, $\alpha_2,\ldots,\alpha_n$ корените на $f(x)$ (някои от числата α_i, $i=1,2,\ldots,n$, могат да бъдат и комплексни). Тогава за $f(x)$ имаме

$$f(x)=a_0\prod_{k=1}^{n}(x-\alpha_k). \tag{6}$$

Нека $x_1, x_2, \ldots, x_\nu$, $\nu<n$, са цели различни числа. Ако $q_2=\min|x_\tau-\alpha_i|$ $\tau=1,2,\ldots,\nu$, $i=1,2,\ldots,n$, то очевидно е в сила неравенството

$$|f(x_\tau)\geq|a_0|q_2^n,\ \tau=1,2,\ldots,\nu. \tag{7}$$

Теорема 3. Примитивният целочислен полином $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$, който в ν цели значения на $x, x_1, x_2, \ldots, x_\nu$, $\nu\leq n$, неконгруентни по модул p, приема стойност p^kt, $t\leq q_2^m$, $m<\nu$, няма целочислен делител от степен $m<\nu$.

Доказателство. Допускаме противното:

$$f(x)=\varphi(x)\psi(x). \tag{8}$$

Съгласно допускането един от полиномите $\varphi(x)$, $\psi(x)$ е от степен, по-ниска от ν. Нека $\varphi(x)$ е от степен $m<\nu$. Понеже $f(x)$ е примитивен, следва, че $\varphi(x)$ и $\psi(x)$ са също примитивни.

Като заместим в (8) $x=x_\tau$, $\tau=1,2,\ldots,\nu$, получаваме равенствата

$$\begin{aligned}
p^kt&=\varphi(x_1)\psi(x_1),\\
p^kt&=\varphi(x_2)\psi(x_2),\\
&\cdots\\
p^kt&=\varphi(x_\nu)\psi(x_\nu).
\end{aligned} \tag{9}$$

От (9) се вижда, че числата $\varphi(x_\tau)$, $\tau=1,2,\ldots,\nu$, са целочислени делители на числата p^kt. От $q_2=\min|x_\tau-\alpha_i|$, $\tau=1,2,\ldots,\nu$, $i=1,2,\ldots,n$, следва, че $|\varphi(x_\tau)|>b_0q_2^m$. Но $q_2^m>t$. Следователно $\varphi(x_\tau)$, $\tau=1,2,\ldots,\nu$, са числа, които се делят на p. От $\nu>m$ и II следва, че $\varphi(x)$ не е примитивен, което противоречи на условието на теоремата. Следователно допускането е невъзможно, с което теоремата е доказана напълно.

Теорема 3 е по-силна от теоремата на Яковкин, която цитирахме. Действително, ако $\alpha_k=\beta_k+i\gamma_k$, $k=1,2,\ldots$ (тук някои от числата γ_k могат да бъдат равни на нула), изискването в теоремата на Яковкин $|x_\tau-\beta_i|\geq q$ е по-ограничаващо от изискването $|x_\tau-\alpha_i|=\sqrt{(x_\tau-\beta_i)^2+\gamma_i^2}>q_2$ в доказаната от нас теорема, тъй като при Яковкин имаме $t\leq q^s$, т. е. $t<|x_\tau-\beta_i|^s$, $s=m$, а при нас $t<q_2^m$, т. е. $t<(\sqrt{(x_\tau-\beta_i)^2+\gamma_i^2})^m$.

Следствие 1. Примитивният целочислен полином $f(x)$ от степен n, който в $\nu > \left[\frac{n}{2}\right]$ цели значения на $x, x_1, x_2, \ldots, x_\nu$, неконгруентни помежду си по модул p, приема стойност $p^k t$, $t \leqq q_2^m$, е неразложим в полето на рационалните числа.

Действително в този случай полиномът $f(x)$ не може да има делители от степен, по-ниска от ν. Но $\nu > \left[\frac{n}{2}\right]$, т. е. най-малката възможна стойност за ν е $\nu = \left[\frac{n}{2}\right] + 1$. Тогава степента на делителите на $f(x)$ е най-малко $\left[\frac{n}{2}\right] + 1$, което е невъзможно, понеже $2\left(\left[\frac{n}{2}\right] + 1\right) = 2\left[\frac{n}{2}\right] + 2$. Ако $n = 2k$, $2\left[\frac{n}{2}\right] + 2 = n + 2 > n$, което е невъзможно. Ако $n = 2k+1$, $2\left[\frac{n}{2}\right] + 2 = n + 1 > n$, което е също невъзможно, понеже $f(x)$ е от степен n.

Следствие 2. При $q_2 = t = 1$ от следствие 1 получаваме следния усилен критерии на Рейнолдс:

Примитивният целочислен полином $f(x)$ от степен n, който в $\nu > \left[\frac{n}{2}\right]$ цели значения на x, неконгруентни помежду си по модул p и несъдържащи в кръг с радиус $q_2 = 1$ корени на $f(x)$, приема стойност p^k, е неразложим в полето на рационалните числа.

Тук изискването $q_2 = t = 1$ е еквивалентно на неравенството $\sqrt{(x_\tau - \beta_i)^2 + \gamma_i^2} \geqq 1$, което очевидно е по-слабо изискване от това в усиления критерии на Рейнолдс от Яковкин, а именно $|x_\tau - \beta_i| \geqq 1$.

ЛИТЕРАТУРА

1. Яковкин, М. В. Численная теория приводимости многочленов. Москва, 1959, 36—40.
2. Reynolds, J. O. On the Irreducibility of Certain Polynomials. J. Elisa Mitchell Sci Soc., **63**, 1947, 120—132.
3. Виноградов, И. М. Основы теории чисел. Москва, 1949, 60.
4. Пиргов, Д., Д. Токарев. Някои теореми за неразложимост на целочислени полиноми в полето на рационалните числа. Год. ВТУЗ. Математика, т. IV, кн. 2 (под печат

Постъпила на 17. III. 1969 г.

НЕКОТОРЫЕ ТЕОРЕМЫ О НЕРАЗЛОЖИМОСТИ ЦЕЛОЧИСЛЕННЫХ МНОГОЧЛЕНОВ В ПОЛЕ РАЦИОНАЛЬНЫХ ЧИСЕЛ, ПРИНИМАЮЩИХ ЗНАЧЕНИЯ СТЕПЕНИ ПРОСТОГО ЧИСЛА

Димитр Пиргов и Елена Кантарджиева

(Резюме)

В этой работе рассматриваются примитивные целочисленные многочлены, которые на некотором множестве целых чисел принимают значения, равные степеням одного и того же простого числа.

Многочлены подобного вида изучались Яковкином [1] и Рейнолдсом [1].

Основные результаты обобщают критерии Рейнолдса и Яковкина для рассматриваемых классов многочленов:

Теорема 1. Целочисленный примитивный многочлен $f(x)$ степени n, который не имеет действительных нулей, неразложим в поле рациональных чисел, если существуют целые числа $x_1, x_2, \ldots, x_n$, несравнимые между собой по модулю p, для которых $f(x)$ принимает значение p^k, $k \geqq 1$, p — простое число.

Теорема 2. Если все корни примитивного целочисленного многочлена $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, $a_n \neq 0$, лежат вне полосы $|I_m(z)| \leqq q_1$ и существуют целые числа, несравнимые между собой по модулю p, $x_1, x_2, \ldots x_\nu$, $\nu > n/2$, для которых $f(x)$ принимает значение p^kq, $k \geqq 1$, p — простое число, то $f(x)$ не разложим в поле рациональных чисел.

Следствие 2 из теоремы 3. Примитивный целочисленный многочлен $f(x)$ степени n, который для $\nu > \left[\frac{n}{2}\right]$ целых значений $x_1, x_2, \ldots, x_\nu$ являющихся несравнимыми между собой по модулю p таких, что в кругах радиуса $q_2 = 1$ около $x_1, \ldots, x_\nu$ не содержатся нули $f(x)$, принимает значение p^k, является неразложимым в поле рациональных чисел.

EINIGE SÄTZE ÜBER DIE UNZERLEGBARKEIT SOLCHER GANZZAHLIGER POLYNOME IM KÖRPER DER RATIONALEN ZAHLEN, WELCHE WERTE ANNEHMEN, DIE POTENZEN EINER PRIMZAHL SIND

Dimitâr Pirgov und Elena Kantardžieva

(Zusammenfassung)

In der Arbeit werden diejenigen primitiven ganzzahligen Polynome betrachtet, die in einer Menge ganzer Zahlen Werte annehmen, welche Potenzen einer und derselben Primzahl sind.

Polynome von dieser Art sind von Jakovkin [1] und Reynolds [1] untersucht worden.

Die gefundenen Grundergebnisse, welche im Grunde genommen für die untersuchten Polynomklassen eine Verallgemeinerung der Kriterien von Reynolds und Jakovkin darstellen, sind die folgenden:

Satz 1. Das ganzzahlige primitive Polynom $f(x)$ n-ten Grades, das keine reellen Wurzeln besitzt, ist im Körper der Rationalzahlen unzerlegbar, wenn ganze Zahlen $x_1, x_2, \ldots, x_n$, existieren, welche untereinander modulo p nicht kongruent sind, für welche $f(x)$ Werte p^k annimmt, wobei $k \geqq 1$ und p Primzahl sind.

Satz 2. Wenn alle Nullstellen des primitiven ganzzahligen Polynoms $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, $a_0 \neq 0$, außerhalb des Streifens $I_m(z) \leqq q_1$ liegen und wenn es ganze Zahlen gibt, die untereinander modulo p nicht kongruent sind, $x_1, x_2, \ldots, x_\nu$, $\nu > n/2$, für die $f(x)$ Wert p^kq annimmt, $k \geqq 1$, p — Primzahl, so ist $f(x)$ im Körper der Rationalzahlen unzerlegbar.

Folgerung 2 aus Satz 3. Das primitive ganzzahlige Polynom $f(x)$ n-ten Grades, welches für $\nu > \left[\frac{n}{2}\right]$ ganze Zahlen $x_1, x_2, \ldots, x_\nu$, die untereinander modulo p nicht kongruent sind und so, daß in den Kreisen um $x_1, \ldots, x_\nu$ mit dem Radius $q_2 = 1$ Nullstellen von $f(x)$ nicht enthalten sind, Werte p^k annimmt, ist im Körper der Rationalzahlen nicht zerlegbar.