Serdica

Bulgariacae mathematicae publicationes

Сердика

Българско математическо списание

ON A PROBLEM OF SCHUR ON THE IRREDUCIBILITY OF INTEGER POLYNOMIALS

DIMITAR T. PIRGOV, RUMEN I. RAIČINOV

In this paper we prove the irreducibility over the field of the rational numbers Q of the type $q^m(x)+p$, where $q(x)=(x-x_1)(x-x_2), \dots, (x-x_n), n\geqq 1, x_1, x_2, \dots, x_n$ are different integers, p is a prime number, $n>2\sigma(p-1)+4$ and $m\geqq 2$ may be any even number where $\sigma(p-1)$ is defined in [2]. This result is an extension of a problem on irreducibility of integer polynomials belonging to Schur.

In 1908 Schur has put the problem about the irreducibility over Q of polynomials of the type $q(x)\pm 1$ and $q^m(x)+1$ $m=2, 4$, where $q(x)=(x-x_1)\dots(x-x_n)$ and $x_1, x_2, \dots, x_n$ are different integers cf. [1 : p 151, problem 121, 122, 123, 124]. This problem and some extensions were dealt with by Flugel cf. [1 : p 151, problem 121, 122, 123] and Brauer cf. [1 : p. 152, problem 124]. In [2] and [3] Pirgov studies polynomials of the type $\Phi(x)=q^2(x)+p$ and $\Phi_1(x)=Q(x)q(x)+p$, $\deg Q\leqq n$. The problem of the irreducibility of the polynomials $\Phi_1(x)$ when $p=1$ has been investigated by Seres [4].

In this paper we prove the irreducibility of polynomials of the type $q^m(x)+p$ where $m\geqq 2$ is an even number, p is prime and $n>2\sigma(p-1)+4$. Here $\sigma(p-1)$ is the introduced in [2] function representing the maximal number of different, not equal to ± 1, integer divisors in the factorisation of the number $p-1$.

By $Z[x]$ we denote the set of polynomials over the ring Z of the integers. By $Z_p[x]$ we denote the set of the polynomials over the field Z_p of the integers comparable by mod (p). If $f(x)=a_0x^n+a_2x^{n-1}+\dots+a_{n-1}x+a_n \in Z[x]$, then by $\bar{f}$ we shall denote the reduced polynomial $\bar{f}(x)=\bar{a}_0x^n+\bar{a}_1x^{n-1}+\dots+\bar{a}_{n-1}x+\bar{a}_n \in Z_p[x]$, where $\bar{a}_i=\{k\in Z \mid k\equiv a_i (\mathrm{mod}\ p)\}\in Z_p$.

Theorem. *If $n\geqq 1$, $x_1, x_2, \dots, x_n$ are different integers, p is prime, $m\geqq 2$ is an even number and $n>2\sigma(p-1)+4$ then the polynomial $f(x)=q^m(x)+p\in Z[x]$ is irreducible over the field Q.*

Proof. From the contrary. Then from Gauss lemma it follows that f will be reducible also over the ring Z and hence we have

$$f(x)=g(x)h(x), \qquad g, h\in Z[x] \tag{1}$$

and $n_g=\deg(g)\geqq 1$, $n_h=\deg(h)\geqq 1$. Obviously $f(x)>0$, $\forall x\in R$ so we may assume that $g(x)>0$ and $h(x)>0$, $\forall x\in R$. From (1) it follows that $\bar{f}=\bar{g}\,\bar{h}$ and because $\bar{f}(x)=(x-\bar{x}_1)^m\dots(x-\bar{x}_n)^m$, then from the uniqueness (to multiples of one) of the factorisation of any polynomial over the field Z_p for $\bar{g}$ and $\bar{h}$ we have

SERDICA Bulgaricae mathematicae publicationes. Vol. 9, 1983, p. 49—50.

(2) $\bar{g}(x)=\bar{a}(x-\bar{x}_1)^{\alpha_1}\ldots(x-\bar{x}_n)^{\alpha_n}, \quad \bar{h}(x)=\bar{b}(x-\bar{x}_1)^{\beta_1}\ldots(x-\bar{x}_n)^{\beta_n},$

where $\bar{a}\,\bar{b}=1$, $0\leqq\alpha_i$, $\beta_i\leqq m$, α_i, $\beta_i\in Z$, $\alpha_i+\beta_i=m$, $i=1, 2, \ldots, n$. From (1) it follows that $g(x)=1x^{n_g}+\ldots$ and $h(x)=1\,.\,x^{n_h}+\ldots$, hence $\bar{g}(x)=\bar{1}\,.\,x^{n_g}+\ldots$, $\bar{h}(x)=\bar{1}\,.\,x^{n_h}+\ldots$ (and thus $\bar{a}=\bar{b}=\bar{1}$). Since $n_{\bar{g}}=\deg(\bar{g})=n_g\geqq 1$ and $n_{\bar{h}}=\deg(\bar{h})=n_h\geqq 1$ we conclude that there exist indices i_0, $j_0\in\{1, 2, \ldots, n\}$ such that $\alpha_{i_0}>0$ and $\beta_{i_0}>0$. From the well known proposition *if* $f(x)=a_0x^n+\ldots+a_n\in Z[x]$ *and* $\bar{f}=\bar{0}\in Z_p[x]$ *then* $p/a_0, a_1, \ldots, a_h$, and from (2) we have the following equalities for g and h

$$g(x)=a(x-x_1)^{\alpha_1}\ldots(x-x_n)^{\alpha_n}+pg_1(x),$$

(3) $$h(x)=b(x-x_1)^{\beta_1}\ldots(x-x_n)^{\beta_n}+ph_1(x),$$

where g_1, $h_1\in Z[x]$. Now in (1) we substitute directly $x=x_{i_0}$ and $x=x_{j_0}$ and taking into account (3) we obtain the equalities

(4) $$g(x_{j_0})=h(x_{i_0})=1, \quad g(x_{i_0})=h(x_{j_0})=p.$$

Knowing that the sets $A=\{j=1, 2, \ldots, n\mid g(x_j)=1\}$ and $B=\{i=1, 2, \ldots, n\mid h(x_i)=1\}$ are not empty (naturally (1) shows that $A\cup B=\{1, 2, \ldots, n\}$ and $A\cap B=\emptyset$) we let $q'(x)=\Pi_{j\in A}(x-x_j)$ and $q''(x)=\Pi_{i\in B}(x-x_i)$. Evidently we have $n_{q'}=\deg q'\geqq 1$, $n_{q''}=\deg q''\geqq 1$ and since $A\cup B=\{1, 2, \ldots, n\}$ we have $n_{q'}+n_{q''}=n$.

Hence $\max(n_{q'}, n_{q''})\geqq n/2$. Also for the polynomials g and h we obtain the equalities

(5) $$g(x)-1=g'(x)G(x), \quad h(x)-1=g''(x)H(x),$$

where G, $H\in Z[x]$. In the first equality of (5) we substitute $x=x_{i_0}$ and in the second $x=x_{j_0}$ and because of (4) we find $p-1=q'(x_{i_0})G(x_{i_0})=q''(x_{j_0})H(x_{j_0})$. Taking in account that the numbers x_i are different, for $\sigma(p-1)$ we obtain the estimate $\sigma(\rho-1)\geqq\max(n_{q'}-2, n_{q''}-2)\geqq n/2-2$which contradicts the condition $\sigma(p-1)<n/2-2$ of the theorem. The theorem is proved.

At last we shall note, that the condition $n>2\sigma(p-1)+4$ is not a substantial limitation, because there exist sufficiently big prime numbers for which $\sigma(p-1)=2$. Really, the biggest prime number from Lemer's table [5] for which $\sigma(p-1)=2$ is the number 10006163.

This result is a substantial extension of the problem of Scur because when n and p are fixed the number m may be any even number, while the results of Flügel [1] and Brauer [1] are about polynomials of the same type but with non-prime p: for $m=2$, $p=1$ and $m=4$, $p=1$ respectively.

The question of the irreducibility of $f(x)$ when $2\leqq\deg f\leqq 2\sigma(p-1)+4$ remains unsolved at present.

REFERENCES

1. Г. Полиа, Г. Сеге. Задачи и теореми по анализ. **2**. София, 1974. Осми раздел. Гл. 2, § 3, Зад. 121, 122, 123, 124, решение стр. 367—368.
2. Д. Пиргов. Относно неразложимостта в полето на рационалните числа на две класи целочислени полиноми. *Годишник ВТУЗ Мат.* **4**, 1967, кн. 3, 27—35.
3. Д. Пиргов. Едно прецизиране на теоремата за неразложимост на целочислени полиноми на И. Серес. *Годишник ВТУЗ Мат.*. **8**, 1972, кн. 2, 31—34.
4. J. Seres. Bizonyos polinomok irreducibilitásáról. *Mat. Lapok*, **16**, 1965, № 1—2, 1—7.
5. Д. Лемер. Таблицы простых чисел от 1 до 10006721. Москва, 1967.

Institute for Chemical Technology, Sofia
Received 2. 3. 1981