Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Umberto Bartocci, Maria Cristina Vipera

On the Gauss-Lucas'lemma in positive characteristic

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **82** (1988), n.2, p. 211–216.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1988_8_82_2_211_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1988.

Atti Acc. Rend. fis.
(8), LXXXII (1988), pp. 211-216

Teoria dei numeri. — *On the Gauss-Lucas' lemma in positive characteristic.* Nota di UMBERTO BARTOCCI e MARIA CRISTINA VIPERA, presentata (*) dal Socio G. ZAPPA.

ABSTRACT. - If $f(x)$ is a polynomial with coefficients in the field of complex numbers, of positive degree n, then $f(x)$ has at least one root α with the following property: if $\mu \leq k \leq n$, where μ is the multiplicity of α, then $f^{(k)}(\alpha) \neq 0$ (such a root is said to be a "free" root of $f(x)$). This is a consequence of the so-called Gauss-Lucas' lemma.

One could conjecture that this property remains true for polynomials (of degree n) with coefficients in a field of positive characteristic $p > n$ (Sudbery's Conjecture).

In this paper it is shown that, on the contrary, if $n > p > 2n-2$ then there exist polynomials which do not have free roots at all. Then one replaces Sudbery's conjecture by supposing that the required property is true for simple polynomials.

KEY WORDS: Roots; Polynomials; Fields of characteristic p.

RIASSUNTO. - *Il lemma di Gauss-Lucas in caratteristica positiva.* Si dimostra che, contrariamente ad una congettura di Sudbery, per ogni intero $n \geq 4$ e almeno per ogni primo $p \in (n, 2n \div 2)$, esistono polinomi di grado n, su campi di caratteristica p, che non ammettono radici "libere" (diciamo che α è una radice libera di $f(x)$ se, detta μ la sua molteplicità, si ha $f^{(k)}(\alpha) \neq 0$ per ogni $k : \mu \leq k \leq n$).

Si esamina poi il caso particolare dei polinomi semplici, fornendo in proposito alcuni risultati e formulando una nuova congettura.

INTRODUCTION

In this paper we study a minor problem in number theory, but whose origin goes back to Gauss himself. It concerns the relations between the roots of a polynomial $f(x) \in \mathbb{C}[x]$ and those of its derivatives $f'(x)$, $f''(x)$, ... and so on.

When one generalises the situation to the case of any abstract field K, the question appears to be rather interesting and still partially unknown nowadays.

We firstly recall the so-called Gauss-Lucas' lemma over the complex number field.

THEOREM 1. - (Gauss-Lucas). *Given any* $n \geq 2$ *points* $P_j = (x_j, y_j)$ *in the plane* $\mathbb{R}^2$, *we put* $\alpha_j = x_j + i y_j \in \mathbb{C}$, $f(x) = \prod_{j=1}^{n} (x - \alpha_j) \in \mathbb{C}[x]$ *and* Π_f *the convex hull of the points* P_j.

(*) Nella seduta del 9 gennaio 1988.

Then, if we denote by $f'(x)$ the first derivative of f, we have $\Pi_{f'} \subset \Pi_f$, that is to say, all roots of $f'(x)$ lie in Π_f.

The proof can be found for instance in [1], p. 29, or [5], p. 84 (and in the older papers [4] and [6].)

From this theorem follows a rather interesting property of complex polynomials:

COROLLARY 2. - (Sudbery [7]). *If $f(x)$ is a complex polynomial with positive degree, then $f(x)$ has at least one "free" root, that is to say, a root α satisfying to the following condition:* (C) - *if μ is the multiplicity of α as a root of $f(x)$, then α is not a root of any derivated polynomial $f^{(\mu)}(x)$, $f^{(\mu+1)}(x)$, ..., $f^{(n)}(x)$.*

Proof. - Condition (C) is satisfied at least by all roots α_j of $f(x)$ which are vertices of Π_f.

It was conjectured by Sudbery himself that Corollary 2 could maintain its general validity for polynomials $f(x)$ defined over any algebraically closed field K, provided that the characteristic p of K is either 0 or greater than the degree n of $f(x)$. One can easily prove that, if $p = 0$, then Corollary 2 is true in this more general context.

In the case $p > 0$, the first author of this paper found counter-examples to Sudbery's conjecture; namely he showed in [2] polynomials of degree $n < p$ ($n = 4$, $p = 5$ and $n = 5$, $p = 7$) such that all of their roots do not satisfy to condition (C).

In the same paper it was proved also that:

THEOREM 3. - *For each $n \geq 1$ there exists a constant $C(n)$ such that Sudbery's conjecture is true for polynomials of degree n defined over fields of characteristic $p > C(n)$.*

The aim of this paper is to investigate more deeply this problem in the case of a field K with positive characteristic p.

We shall show that counter-examples to Sudbery's conjecture can be found for each value of the degree n, and that it is very likely that as such counter-examples one can never find simple polynomials.

2. CONSTRUCTION OF POLYNOMIALS WITH GENERAL DEGREE AND NO FREE ROOTS

We denote by P_n the set, possibly empty, of prime numbers p, greater than n, such "that" Sudbery's conjecture is not true for polynomials with degree n over a field with characterictic p.

By Theorem 3, P_n is a finite set and we put $r(n) = |P_n|$.

Obviously one has $r(1) = r(2) = r(3) = 0$; one could rephrase Sudbery's conjecture by asserting that $r(n) = 0$ for each value of n. We already said that $r(4)$ and

$r(5)$ are, on the contrary, different from 0. We are going to prove, more generally, that

THEOREM 4. - *For each value of the degree* $n \geq 4$, $r(n)$ *is a positive number.*

Proof. - We consider the polynomial $x^n - x^{n-2} = x^{n-2}(x^2 - 1)$, thinking of it as defined over different prime fields $\mathbb{Z}_p$, $p > n$.

First of all we observe that the i-th derivative of $f(x)$, $1 < i < n - 1$, is the polynomial

$$n(n-1)\dots(n-i+1)x^{n-i} - (n-2)\dots(n-i-1)x^{n-i-2} = a_i x^{n-i} - b_i x^{n-i-2}.$$

The $(n-1)$-th derivative is $n!x$, which has in common with $f(x)$ the root 0. Then it is enough to show that both values 1 and -1 are roots of some i-th derivative $(1 < i < n - 1)$. We show that both values are roots of the same i-th derivative, where $i = 2n - p - 1$, for any choice of a prime number $p : n < p < 2n - 2$. As a matter of fact, 1 and -1 are roots of this derivative if, and only if, a_i is congruent to b_i modulo p, that is to say, if such are $n(n-1)$ and $(n-i)(n-i-1)$; this precisely happens to be true for the index $i = 2n - p - 1$. The existence of a prime p in the interval $(n, 2n-2)$ is a well known consequence of Tchebytchev's results on the distribution of prime numbers (this is exactly the assertion of the so called Bertrand's Postulate: see for instance [3], p. 373). This ends the proof.

COROLLARY 5. - *For each* $n \geq 4$, *the cardinality* $r(n)$ *of* $P(n)$ *is greater or equal to the number of primes which are in the interval* $I(n) = (n, 2n-2)$.

Corollary 5 gives a positive lower bound for the function $r(n)$, with $n \geq 4$; after introducing the classical prime number function $\pi(x)$, we have

$$r(n) \geq \pi(2n-2) - \pi(n) \sim \frac{n}{\log n}. \tag{1}$$

A straightforward computation shows that

PROPOSITION 6. - *The prime* $p = 5$ *is the only "exceptional" prime with respect to* $n = 4$, *that is to say,* $r(4) = 1$.

Furthermore, numerical evidence in possession of the authors would suggest that also $r(5) = 1$. However one can check directly:

PROPOSITION 7. - *For* $n = 6, 7, 8$, $r(n)$ *is greater than the number of primes which are in the corresponding intervals* $I(n)$.

There is one more interesting aspect of the situation which seems to the authors still completely unknown, and to this they will dedicate the next section.

3. The case of a simple polynomial

The new problem rises out from the observation that all known counter-examples to Sudbery's conjecture have some multiple root, that is to say, they are not *simple* polynomials. Thus the problem of finding simple counter-examples seems interesting.

However, at least for values of n and p not too big, and for polynomials wich are completely reducible over a prive field $\mathbb{Z}_p$, such counter-examples have not been found (this has been verified for degrees $n \leqslant 7$ and values of p up to $p = 37$).

Then one could put forward the following conjecture, which replaces, in some sense, Sudbery's one, and to which one could refer as to the *Gauss-Lucas' lemma in positive characteristic*:

Conjecture - *Each simple polynomial* $f(x)$ *of degree n in characteristic* $p > n$, *has at least one free root.*

The validity of the previous assertion is ensured, by Theorem 3, when p is very large with respect to n, and, it is obvious, for each value of p, in the case $n \leq 4$. One can also show that:

Proposition 8. - *Gauss-Lucas' lemma in p.c. is true in the case* $n = 5$.

Proof. - As a matter of fact, taking a generic monic polymonial of degree $n = 5$, $f(x) = \prod_{j=1}^{5} (x - \alpha_j)$, if α_j were not free roots for $f(x)$, then either three of them would satisfy $f''(x) = 0$, or two of them would satisfy $f^{(3)}(x) = 0$ and a third one would satisfy $f^{(4)}(x) = 0$. In both cases, a direct computation shows the non-existence of such a polynomial.

We show now two more particular cases in which Gauss-Lucas' lemma in p. c. is true.

Theorem 9. - *Let* $f(x)$ *be a simple completely reducible polynomial over a finite prime field,* $\mathbb{Z}_p$. *Then, in the case* $n = p - 1$ *all roots of* $f(x)$ *are free; in the case* $n = p - 2$ *there are exactly* $\Phi(p - 1)$ *free roots of* $f(x)$, *where* Φ *denotes Euler's indicator.*

Proof. - First of all, we introduce an equivalence relation on monic polymonials over $\mathbb{Z}_p$, of the same degree n. We say that $f(x)$, $g(x)$ are equivalent if $g(x)$ can be obtained from $f(x)$ by means of an affine transformation over $\mathbb{Z}_p$, $x \to ax + b$, and a subsequent division by the leading coefficient a^n. Of course, equivalent polynomials have the same number of free roots. In the cases $n = p - 1$ and $n = p - 2$, all polynomials of degree n over $\mathbb{Z}_p$ are equivalent, and then one can check the assertion only for a fixed polynomial.

In the case $n = p - 1$, $f(x) = x^{p-1} - 1$ has obviously all of its roots which are free.

In the case $n = p - 2$ we put $f_c(x) = (x^p - x)/(x - 1)(x - c)$, $c \in \mathbb{Z}_p$, $c \neq 0, 1$, and we show that $f_c(x)$ has exactly $\Phi(p - 1)$ free roots. We firstly observe that 0 is a free root of $f_c(x)$ if, and only if, c is a generator of the multiplicative cyclic group $\mathbb{Z}_p - \{0\}$. Indeed, from the identity

$$f_c(x) = x(x^{p-2} + \ldots + 1)/(x - c) = x[x^{p-3} + (1 + c)x^{p-4} + \ldots + (1 + c + \ldots + c^{p-3})]$$

follows that 0 is a free root if and only if all coefficients $1 + c$, $1 + c + c^2$, $\ldots, 1 + c + \ldots + c^{p-3}$ are different from 0; this happens to be true if, and only if, c is a generator of $\mathbb{Z}_p - \{0\}$, since, for $c \neq 1$ and $1 \leq k \leq p - 3$, one has: $1 + c + \ldots + c^k = 0 \Leftrightarrow c^{k+1} = 1 \Leftrightarrow$ the period of c is not $p - 1$.

If we put $s = \Phi(p - 1)$ and we denote by $c_1, \ldots, c_s$ the generators of $\mathbb{Z}_p - \{0\}$, there exist exactly s distinct affine transformations which carry, up to division by the leading coefficient, the polynomials $f_{c_i}(x)$, $i = 1, \ldots, s$ into a fixed one $f_c(x)$. Therefore, free roots of $f_c(x)$ are exactly the s different images of 0 under such transformations. This completes the proof.

We end this paper giving a "theoretical" motivation for the validity of the previous conjecture, which will also indicate a possible way of proof.

Let us consider n indeterminates $\alpha_1, \ldots, \alpha_n$ over $\mathbb{Z}$ and put

$$\psi(x) = \prod_{j=1}^{n} (x - \alpha_j) \in \mathbb{Z}[x, \alpha_1, \ldots, \alpha_n],$$

$$\Psi(x) = \psi'(x)\psi''(x)\ldots\psi^{(n)}(x) \in \mathbb{Z}[x, \alpha_1, \ldots, \alpha_n],$$

where derivatives are taken with respect to x. Moreover we put

$$V(\alpha_1, \ldots, \alpha_n) = \prod_{i,\, j=1}^{n} (\alpha_j - \alpha_j) \in \mathbb{Z}[\alpha_1, \ldots, \alpha_n].$$

Then, for Gauss-Lucas' lemma in characteristic 0 and Hilbert's Nullstellensatz, one can deduce (see [2]) the existence of an identity of the kind

$$H \cdot V(\alpha_1, \ldots, \alpha_n)^s = \sum_{j=1}^{n} \Psi(\alpha_j) \cdot Q_j(\alpha_1, \ldots, \alpha_n),$$

where s, H are positive integers and, $\forall j$, $Q_j(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}[\alpha_1, \ldots \alpha_n]$. The truth of the conjecture would then follow from the conjectured existence of such an identity with a constant H all of whose divisors are less or equal to n.

This is true in the cases $n = 2, 3, 4$:

$$4 \cdot V(\alpha_1, \alpha_2) = 2(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_1) + 2(\alpha_2 - \alpha_1)(\alpha_1 - \alpha_2); \tag{2}$$

$$(3)\qquad 2 \cdot 3 \cdot 3! \cdot V(\alpha_1, \alpha_2, \alpha_3) = \Psi(\alpha_1)[\alpha_1(\alpha_2 - \alpha_2)^2] + \\ + \Psi(\alpha_2)[\alpha_2(\alpha_1 - \alpha_3)^2] + \Psi(\alpha_3)[\alpha_3(\alpha_1 - \alpha_2)^2];$$

$$(4)\qquad 2^3 \cdot 3^2 \cdot 4 \cdot 4! \cdot V(\alpha_1\, \alpha_2\, \alpha_3\, \alpha_4)^2 = \sum_{j=1}^{n} [\Psi(\alpha_j) \cdot \prod_{h<i}^{h\neq j\neq i} (\alpha_h - \alpha_i)^2].$$

ACKNOWLEDGEMENT. - The authors thank Dr. E. Ughi for gently providing them with identities (2), (3) and (4).

Note added in proof: While this paper was in print, we found a simple polynomial of degree n = 9, completely reducible over the prime field Z_{31}, and such that all its roots are not free. Then, as Sudbery's conjecture, ours is also not true in general. The question still remains open of determining these "exceptional" values of n and p.

REFERENCES

[1] AHLFORS L.V., *Complex Analysis*, Mc Graw and Hill, 1966.
[2] BARTOCCI U., *Su di una congettura di Sudbery*, Rend. Acc. Naz. Lincei, VIII, 56, 1974.
[3] HARDY G.H. and WRIGHT E.M., *An Introduction to the Theory of Numbers*, Oxford, 1960.
[4] HAYASHI T., *Relations between the zeros of a rational integral function and its derivate*, Ann. of Math., 15, 1913.
[5] HILLS E., *Analytic Function Theory*, Vol. I, Chelsea P.C., 1973.
[6] IRWIN F., *Relations between the roots of a rational integral function and its derivatives*, Ann. of Math., 16, 1915.
[7] SUDBERY A., *The number of distinct roots of a polynomial and its derivatives*, Bull. London Math. Soc., 5, 1973.