Journal of Universal Computer Science, vol. 2, no. 5 (1996), 396-409
submitted: 13/5/96, accepted: 13/5/96, appeared: 28/5/96 *© Springer Pub. Co.*

POLYNOMIALS, CONSTRUCTIVITY AND RANDOMNESS [1]

Doru Ştefănescu
University of Bucharest, P.O. Box 39-95, Bucharest 39 Romania, email: stef@imar.ro, stef@fizica.fizica.unibuc.ro, stef@math.math.unibuc.ro.

Abstract: We discuss some effective characterizations of the prime elements in a polynomial ring and polynomial factorization techniques. We emphasize that some factorization methods are probabilistic; their efficiency justifies the experimental trend in mathematics. The possibility of an effective version of Hilbert's irreducibility theorem and the probabilistic techniques of Berlekamp will be also discussed. Finally, bounds on the heights of integer polynomials are used as tools for improving polynomial factorizations.

1 Introduction

Many problems of nowadays algebra originate in extensions of fundamental results from arithmetic to more general structures. The study of primality is one of them.

In commutative algebra the role of primes is taken by irreducible elements from a domain, and one of its main problems is exactly the effective description of the irreducible elements in an unique factorization domain (UFD). In the case of polynomial rings the irreducible elements are called *irreducible polynomials*. There are two main problems in the study of irreducible polynomials:

1. To decide whether or not a given polynomial is irreducible.
2. To factorize a given polynomial in a product of irreducible polynomials.

We shall discuss various aspects of these two problems, emphasizing the constructive and probabilistic aspects.

2 Irreducible Polynomials

What an irreducible polynomial is? In analogy with the case of prime numbers, a polynomial is called *irreducible* if it can not be represented as the product of two nonconstant polynomials.

For example

$$X+1, \qquad X^2+1$$

are irreducible polynomials in $\mathbb{R}[X]$, but

$$X^2+1$$

[1] C. Calude (ed.). *The Finite, the Unbounded and the Infinite, Proceedings of the Summer School "Chaitin Complexity and Applications",* Mangalia, Romania, 27 June – 6 July, 1995.

is not irreducible in $\mathbb{C}[X]$ because

$$X^2 + 1 = (X + i)(X - i).$$

From the above examples it follows that the coefficient ring plays an essential role in the factorization of a polynomial. The "larger" the coefficient ring is, the greater is the probability to find proper factors of a given polynomial.

Similarly is considered the irreducibility of multivariate polynomials. Thus, the polynomial

$$X^2 - 3Y^2$$

is irreducible in $\mathbb{Z}[X, Y])$, but it is reducible in the ring $\mathbb{R}[X, Y]$, because of the following factorization:

$$X^2 - 3Y^2 = (X + \sqrt{3}Y)(X - \sqrt{3}Y).$$

Problem 1. Is the irreducibility of a given polynomial F with coefficients in a domain algorithmically decidable ?

The problem 1 is solved only for some particular coefficient rings, including the integers $\mathbb{Z}$. The solution is based on polynomial factorization algorithms discussed in section 4.

The problem of the primality test of an integer number is not an easy one for large integers, even if it is theoretically solved. For most coefficient rings there is no known solution of problem 1. A case for which there are known factorization algorithms is that of integer polynomials (cf. section 4).

3 Hilbert's Irreducibility Theorem

One of the seminal results of David Hilbert is his *irreducibility theorem* published in 1892. It can be found in Hilbert [13], p. 106:

Theorem 3.1 (Hilbert's irreducibility theorem, HIT) *If $f(x, t)$ is an irreducible polynomial in $\mathbb{Z}[x, t]$, then $f(x, a)$ is an irreducible polynomial in $\mathbb{Z}[x]$ for infinitely many integer values of a.*

The above theorem is a standard example of a crucial mathematical result. Its statement is elementary, concise and sensitive. However the various proofs are not elementary at all[2], involving thorough methods. There are many extensions of the theorem, some of them spectacular. This theorem was and it still is the origin of many studies in various fields, for instance in algebra, number theory, algebraic geometry, model theory, nonstandard mathematics.

We shall discuss here some versions of Hilbert's irreducibility theorem. Any of them emphasizes another aspect of the theorem. In the sequel we abbreviate *Hilbert's irreducibility theorem* by HIT.

[2] We note that in 1962 S. Lang [14] showed that the original proof by Hilbert contained an erroneous argument. However subsequent proofs of various authors were correct.

HIT - The general case

In his seminal paper [13] Hilbert also obtained a generalization of the irreducibility theorem for polynomials in many variables. Subsequently HIT was extended also to the case of polynomials with coefficients in an algebraic number field.

Definition: K is an algebraic number field if it is a finite extension of the field of rational numbers $\mathbb{Q}$.

Theorem 3.2 (HIT - The general case) *Let $F_i(x_1,\ldots,x_s,t_1,\ldots,t_r)$ $(1 \le i \le h)$ be irreducible polynomials in $r+s$ indeterminates with coefficients in an algebraic number field K and let $P \in K[t_1,\ldots,t_r], P \neq 0$.*

Then there are infinitely many vectors $(a_1,\ldots,a_r) \in \mathbb{Z}^r$ such that the polynomial

$$F_i(x_1,\ldots,x_s,a_1,\ldots,a_r) \in K[x_1,\ldots,x_s]$$

is irreducible in $K[x_1,\ldots,x_s]$, for all $i = 1,2,\ldots$, $P(a_1,\ldots,a_r) \neq 0$.

The proof of theorem 3.2 is difficult, involving various techniques. It can be divided in several steps, each of them corresponding to a particular case:

STEP 1: $r = s = 1, K = \mathbb{Q}$.

STEP 2: $r = s = 1$, K is a normal extension of $\mathbb{Q}$.

STEP 3: $r = s = 1$, K is an algebraic number field.

STEP 4: $s > 1, r = 1$, K is an algebraic number field.

STEP 5: The general case.

We sketch the main ideas of step 1, that is the case originally considered by Hilbert (theorem 3.1).

Let $a \in \mathbb{Z}$. Then each solution of the polynomial equation

$$F(x,a) = 0$$

is a series $x(T) = \sum_{i \in I\!N} \alpha_i T^{m_i}$ with coefficients complex numbers and all exponents rational numbers having a finite common denominator. These solutions are called *Puiseux series*. Note that all coefficients are complex numbers, i.e. they are in a field of characteristic zero. For polynomial equations $F(x,a) = 0$ with coefficients in a field of positive characteristic, the corresponding solutions can be described by some special series with rational exponents, called *restricted power series* (see D. Ştefănescu [26]).

It follows that $x(a)$ is not an integer for infinitely many integer values of a, therefore the equation $F(t,a) = 0$ has no rational solutions. So, for infinitely many integers a, the x-discriminant of the polynomial $F(x,t)$ satisfies a condition which implies the irreducibility over $\mathbb{Q}$ of the polynomial $F(x,a)$.

Theorem 3.2 and related results can be proven in several ways. These proofs contain different insights on Hilbert's irreducibility theorem. One of them refers to the following effectiveness problem:
Is HIT constructively consistent, i.e. can we use HIT to construct effectively families of irreducible polynomials ?

The answer, as we shall see in the sequel, reveals the merits and the limits of a result based on the axiom of choice. It is a typical nonconstructive argument.

V. G. Sprindzhuk has proved in [25] that it is possible to evaluate the cardinality of the set of integers a such that the polynomial $F(x,a)$ is reducible. Moreover, there exist a computable function $m = m(F)$ and a sequence of rational numbers (a_n) such that each polynomial $F(x,a_n)$ is irreducible over $\mathbb{Q}$, as soon as $n > m(F)$.

Apparently, Sprindzhuk's result should be sufficient to construct effectively an enumerable family of irreducible polynomials in $\mathbb{Q}[x]$ starting from an irreducible polynomial in two variables. But his method does not produce a computable function $m = m(F)$ and it is not possible to list the integers a such that the polynomial $F(x, a)$ is reducible in $\mathbb{Z}[x]$. M. Yasumoto [27] explained the lack of effectivity of Sprindzhuk's result because of the use of the nonstandard version of the theorem of Siegel [23] on 'diophantine approximations' in the field of power series.

Theorem 3.2 has many applications. We mention that Andrew Wiles, in his 1993 approach to Fermat's last theorem [22] on the Diophantine equation

$$x^n + y^n = z^n$$

has invoked theorem 3.2. In Wiles' arguments Hilbert's irreducibility theorem is essential in proving the existence of a special rational noncuspidal point.

HIT - Gilmore-Robinson version

There exists a version of Hilbert's irreducibility theorem which invokes techniques from model theory. It was obtained by P. C. Gilmore and A. Robinson in the fifties [12]. Here is a brief account of their work.

They use the predicate calculus with a number of individual parameters and atomic predicates. For each field K and each element t which is transcendental over K, the language $\mathcal{F}$ is that of first order predicates applied in the following way: To each element from K and to the transcendental t one assigns an individual parameter, and these are all individual parameters of $\mathcal{F}$; to each subset of K, to each subset of $K \times K$, to each subset of $K \times K \times K$ ...one assigns an atomic predicate, and these are all atomic predicates of $\mathcal{F}$. Finally, by definition, the language $\mathcal{L}$ is defined to be identical to $\mathcal{F}$, except that it lacks an individual parameter for t.

In The Gilmore-Robinson approach of HIT the following condition is involved:

Condition C. Let K be an infinite field, t, x indeterminates over K (algebraically independent over K). For any polynomial $p(t, x) \in K(t)[x]$ which has no zeros in $K(t)$, there is a $t^* \in K$ such that $p(t^*, x) \in K[x]$ has no zeros in K.

Their key result is:

Theorem 3.3 (Gilmore-Robinson) *For any field K fulfilling condition C, there is an extension S' of $S = K(t)$ which is a model of $\mathcal{K}$ and for which every member of $S' \setminus S$ is transcendental with respect to S.*

The proof of theorem 3.3 appeals to the next convention:

Convention. The assignment of parameters and predicates for the languages $\mathcal{F}$ and $\mathcal{L}$ will be considered as fixed, so that a statement of $\mathcal{F}$ and $\mathcal{L}$ holding for K or $K(t)$, is assumed to be satisfied under the given assignment. Then $\mathcal{L}$ will be, by definition, the set of all the statements of $\mathcal{L}$ holding for $\mathcal{K}$, that is $\mathcal{K}$ is the largest set of statements of $\mathcal{L}$ for which K is a model.

From all these technical considerations Gilmore and Robinson have obtained the following version of HIT.

Corollary 3.4 (Gilmore-Robinson HIT) *If K fulfills condition C, then for each irreducible polynomial $p = p(t, x) \in K(t)[x]$ there exist infinitely many $t^* \in K$ such that $p(t^*, x) \in K[x]$ is irreducible in $K[x]$.*

Remark: Corollary 3.4 proves that Hilbert's irreducibility theorem holds for every field fulfilling condition C.

Remark: S. Lang [14] has introduced even a class of special fields for which HIT holds. He called such fields *Hilbert fields*. More precisely, a field K is called a *Hilbert field* if the following statement is fulfilled:

If $F \in K[x_1, ..., x_n]$ is irreducible, then $F(x_1, a_2, ..., a_n) \in K[x_1]$ is irreducible for almost all $a_2, \ldots, a_n \in K$,

(where 'almost' all has not the meaning from measure theory, but assumes the existence of a polynomial with certain properties). Let's note that the family of Hilbert fields includes, for example, the algebraic number fields. But the finite fields and the algebraically closed fields are not Hilbert.

HIT - A probabilistic version

We now discuss the probabilistic version of J. v. Gathen [11]. Gathen obtained it as a result of his search for an effective version of Hilbert's irreducibility theorem. His results allow the (probabilistic) reduction of multivariate factorization to the bivariate case.

The probabilistic version of HIT uses the concept of factorization pattern. If $F \in K[x_1, \ldots, x_n]$ then the vector $(d_1, m_1, \ldots, d_r, m_r)$ is called a *factorization pattern* of the polynomial F if there exist r irreducible distinct polynomials $F_1, \ldots, F_r$ and r natural numbers $m_1, \ldots, m_r$ such that

$$F = F_1^{m_1} \ldots F_r^{m_r}, \quad \deg F_i = d_i, \quad d_i \leq d_j \quad i < j.$$

A simplified probabilistic version of Hilbert's irreducibility theorem can be obtained:

Theorem 3.5 (HIT - probabilistic version) *Let F be an effectively computable field and $f \in F[x_1, \ldots, x_n]$. Then there is a field extension of F and a subsidiary polynomial in $3(n-2)$ variables with coefficients in K, of degree 9^{d^2}, which allows the construction of a polynomial $f_t \in F[x_1, x_2]$ such that the polynomials f and f_t have the same factorization pattern.*

The proof of theorem 3.5 involves techniques from algebraic geometry, including a theorem of Bertini legitimating the existence of the associated polynomial f_t. This polynomial is described through a suitable substitution. If the polynomial f is irreducible one obtains a bivariate irreducible polynomial, i.e. a "classic" version of HIT.

Theorem 3.5 leads to some probabilistic factorization algorithms. They are dependent on the coefficient field (algebraic number fields, finite fields etc.). Their common characteristic is that they produce the correct answer with some probability, usually a function of the degree of the polynomial. For example, from theorem 3.5 it follows the existence of a bivariate polynomial g of degree $\leq n$ such that the probability that the polynomials f and g have different factorization patterns is at most $\frac{9^{n^2}}{a}$, with a being the cardinality of a finite subset of K. For a sufficiently large one has a probabilistic polynomial-time reduction from multivariate to a bivariate factorization pattern.

In the mathematical literature there exist many algorithms which depend on additional hypotheses formulated on the basis of empirical observations. Such a hypothesis is the existence of an effective version of Hilbert's irreducibility theorem holding over $\mathbb{Q}$ for simple substitutions. Such results, obtained assuming the validity of plausible but not yet proved mathematical facts, are specific to *experimental mathematics*.[3] One of the

[3] See the delightful discussion on experimental mathematics in Chaitin's lecture [8], section 5.

most invoked assumptions used by experimental techniques is Riemann hypothesis. An interesting result in this direction, obtained by Weinberger [28], is a polynomial-time algorithm for computing the number of factors of an integer polynomial, assuming the extended Riemann hypothesis.

Although probabilistic algorithms cannot be applied "with certitude" to any polynomial, they are useful for effective polynomial factorization. The evaluation of the probability is important, because it measures the efficiency of the method. Such an algorithm also includes the point of the failure cases. For the "exceptional" polynomials for which the method does not work, one may try other factorization methods. Among these we mention the *Norman-Moore algorithm*, included in the algebraic programming system REDUCE, and the *Musser algorithm*. These algorithms involved some results of Zassenhaus on Hensel factorization. Their cost is polynomial, so they are an alternative to modular algorithms, with exponential cost.

We also mention Chaitin's conditions for the conversion of probabilistic algorithms into deterministic ones (for a proof see C. Calude [6], ch. 7.5), with a direct application to the problem of factorization of integers.

4 Factorization Algorithms

The factorization of integers into a product of primes is one of the basic problems in number theory. Even if there are known many factorization methods, they may be applied only to few classes of integers, usually "small" numbers[4]. Let us observe that the methods used in public key cryptography for encoding messages are based exactly on the practical impossibility of factorizing "very large" integers. A message encoded in such a way can not be "broken".

The same difficulties are encountered in polynomial factorization. We shall limit ourselves to the case of polynomials with coefficients in a field K (but the same considerations remain valid for polynomials with coefficients in an UFD). We first note the following result:

Theorem 4.1 *If $F \in K[x_1, \ldots, x_n]$ is a nonconstant polynomial then there exist unique irreducible polynomials $F_1, \ldots, F_r$ and natural numbers $m_1, \ldots, m_r$ such that*

$$F = F_1^{m_1} \ldots F_r^{m_r}. \tag{1}$$

The relation (1) is called the *factorization* of the polynomial F. A natural question is:

Problem 2. Given a nonconstant polynomial F with coefficients in a field (or in an UFD), does there exists a factorization algorithm for F?

In most cases there is not known an answer to problem 2. However, for some particular coefficient rings (including the integers), there exist general *factorization algorithms.*

The main factorization algorithms for polynomials with integer coefficients are the following:

1. The algorithm of Kronecker.
2. The algorithm of Berlekamp.
3. The L^3 algorithm.

[4] Here the notion of "small number" is vague; often it depends on the size of the system used for making the computation. A number of 15 ciphers, for example, can be quickly factorized by a computer, while it takes some time to a human being using only paper and pencil.

We shall not describe here all these methods. We only mention that the algorithm of Kronecker is based on the factorization of integers and polynomial interpolation, and the algorithm of Berlekamp uses the factorization of polynomials over finite fields and Hensel's lemma. The L^3 algorithm (developed in 1982 and called L^3 after its authors A. K. *L*enstra, H. W. *L*enstra and L. *L*ovàsz) involves the Gram-Schmidt orthogonalization.

As in the case of integer numbers, we are interested in evaluating the time necessary to factor a polynomial. It was observed that the method of Kronecker is slow, while the L^3 algorithm is fast. The evaluation of the factorization time can be done by a *"cost"* function. The cost can be defined in many ways: in function of the degree of the polynomial, with respect to the 'size' of the coefficients a.s.o. With respect to the polynomial degree, the cost of the algorithms 1. and 2. are exponential, but the cost of the algorithm 3. is polynomial.[5]
The problem of factorization of univariate polynomials over finite fields is essential for the factorization of univariate and multivariate integer polynomials. This is an attractive and difficult mathematical problem.
Let $\mathbb{F}$ be a fixed finite field. Therefore it is isomorphic to a field $\mathbb{F}_q$ with $q = p^s$ elements, where p is prime and $s \geq 1$. We may write a list of all the polynomials of degree n with coefficients in $\mathbb{F}$. Then the problem of factorizing a polynomial f of degree n could be *theoretically* solved in the following way:

STEP 1: Divide the polynomial f by all polynomials of degree $n-1$.
One obtains all possible divisors of degree $n-1$.

STEP 2: Divide the polynomial f by all polynomials of degree $n-2$.
One obtains all possible divisors of degree $n-2$.

. . . . . .

STEP n-1: Divide the polynomial f by all polynomials of degree 1.
One obtains all possible divisors of degree 1.

In this way one obtains the factorization of f. Unfortunately, this method is not practical. For large degrees, even for the field $\mathbb{Z}_2$ which has only two elements, this method involves very long computations, impossible to accomplish. But there are other devices which allow an effective factorization over finite fields. The most famous is the *probabilistic method* of E. R. Berlekamp [3].

The algorithm of Berlekamp

The device of Berlekamp is based on the decomposition

$$X^p - p = \prod_{j=0}^{p-1} (X - j),$$

valid in $\mathbb{Z}_p[X]$. It leads to

Proposition 4.2 (Berlekamp) *Let $f \in \mathbb{Z}_p[x]$, $\deg(f) = d > 0$. If there exist $g \in \mathbb{Z}_p[x]$ such that $1 \leq \deg(g) < d$ and f divides $g^p - g$ then*

$$f = \gcd(f, g)\gcd(f, g-1)\ldots\gcd(f, g-p+1) \tag{2}$$

is a nontrivial factorization of f.

[5] Let us note that with minor modifications the three methods above can also be used for the factorization of integer multivariate polynomials.

Theorem 4.3 (Berlekamp's algorithm) *Let $f \in \mathbb{Z}_p$, $\deg(f) = d \geq 1$. Then there exists an algorithm that describe a nontrivial factorization of f.*

The algorithm corresponding to the proof of Theorem 4.3 can be summarized as follows.

Algorithm: Let $I = I_d$ the $d \times d$ identity matrix and let

$$Q = \begin{pmatrix} r_{00} & r_{01} & \dots & r_{0,d-1} \\ r_{10} & r_{11} & \dots & r_{1,d-1} \\ \dots\dots & \dots\dots & \dots & \dots\dots\dots \\ r_{d-1,0} & r_{d-1,1} & \dots & r_{d-1,d-1} \end{pmatrix}$$

be the matrix of the coefficients of the remainders of division of $1, x, x^2, \dots, x^{d-1}$ by f. If f factorizes then

$$(b_0, b_1, \dots, b_{d-1})(Q - I) = (0, 0, \dots, 0) \tag{3}$$

The coefficients of g are the solutions of (3).

When p is large, the use of formula (2) involves an enormous amount of work. An alternative was described by Cantor-Zassenhaus [4]. They observed that for p an odd prime one has

$$g^p - g = g(g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}})$$

and this suggested the consideration of

$$\gcd(f, g^{\frac{p-1}{2}} - 1). \tag{4}$$

They proved that the probability that (4) gives a nontrivial factor of f is $\geq \frac{1}{2}$. This implies that, in general, using possible factors suggested by (4), one should reach more quickly a nontrivial factorization of the polynomial f.

Remark: Note that, although it is not possible to list all the irreducible polynomials of degree n over $\mathbb{F}_q$, there exists a formula which gives their number $N_{n,q}$. The formula giving $N_{n,q}$ uses the function μ of Möbius and allows a quick computation. A probabilistic settlement was obtained by Mignotte-Nicolas. Their result is useful for evaluating the cost of factorization algorithms.

Theorem 4.4 (Mignotte-Nicolas, [18]) *A randomly chosen polynomial of degree n over a finite field is reducible with a probability close to $1 - \frac{1}{n}$.*

Proof. Suppose $\mathbb{F}_q$ is a finite field with q elements. For any $m \in \mathbb{N}$ one has

$$q^m = \sum_{n|m} nN_{n,q}.$$

By Mœbius inversion formula it is deduced that

$$N_{n,q} = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

(Cf. L.E. Dickson [9], p. 18)

Let $\mathcal{P}_{\text{irr}}(F)$ be the probability that a monic polynomial $F \in \mathbb{F}_q[X]$ of degree n to be irreducible. Using the formula of Dickson we compute directly the probability $\mathcal{P}_{\text{irr}}$. We

denote by $M_{n,q}$ the number of monic polynomials of degree n from $\mathbb{F}_q[X]$. Note that $M_{n,q} = q^n$. It follows

$$\mathcal{P}_{\text{irr}}(F) = \frac{N_{n,q}}{M_{n,q}} = \frac{\frac{1}{n}\sum_{d|n}\mu(d)q^{\frac{n}{d}}}{q^n}$$

$$\frac{q^n - q^{\frac{n}{p_1}} + \ldots + (-1)^s q^{\frac{n}{p_1 \cdots p_n}}}{nq^n} = \frac{1}{n} - \frac{1}{nq^{n-\frac{n}{p_1}}} + \ldots + (-1)^s \frac{1}{nq^{n-\frac{n}{p_1 \cdots p_s}}},$$

where $p_1, \ldots p_s$ are the distinct prime divisors of n.

Now the probability $\mathcal{P}_{\text{red}}(F)$ that a monic polynomial of degree n from $\mathbb{F}_q[X]$ is reducible can be computed by the formula

$$\mathcal{P}_{\text{red}} = 1 - \mathcal{P}_{\text{irr}} = 1 - \frac{1}{n} + \frac{1}{nq^{n-\frac{n}{p_1}}} - \ldots + (-1)^{s+1}\frac{1}{nq^{n-\frac{n}{p_1 \cdots p_s}}}.$$

which shows that $\mathcal{P}_{\text{red}}$ is close to $1 - \frac{1}{n}$. □

Remark: M. Mignotte has obtained sharper results than in Theorem [18]. In his monograph [17] one estimates the constants involved in computing the number $\omega_m(F)$ of monic irreducible polynomial divisors of degree $\leq m$ of a given monic polynomial P of degree n from $\mathbb{F}_q[X]$. He proved, for example, that

$$\sum_F \omega_m(F) = q^n(\text{Log } n - c), \quad \text{with} \quad -1 < c < 2.5.$$

Remark: There exist factorization techniques also for bivariate polynomials over k, such as *generalized difference polynomials*. These devices are partially based on properties of Newton polygons (see [19]).

A *difference polynomial* is a polynomial of the form

$$f(x) - g(y),$$

where $f(x)$, $g(y)$ are univariate polynomials.

A *generalized difference polynomial* is a polynomial in two variables satisfying a special Newton polygon condition. Difference polynomials are examples of generalized difference polynomials. The techniques developed in [19] can be extended to the factorization of arbitrary bivariate polynomials.

Bounds for Divisors of Integer Polynomials

A key step in designing factorization algorithms for univariate integer polynomials is the estimation of the moduli of the coefficients of all possible divisors. Such methods use convenient polynomial sizes as the measure of a polynomial (see M. Mignotte [16]) and the l_2-weighted norms of E. Bombieri (see [2]).[6]

We describe a device based on estimates of product of roots of a complex polynomial. Suppose $P(X) = X^n + a_1X^{n-1} + \ldots + a_n \in \mathbb{C}[X] \setminus \mathbb{C}$ and let

$$\beta_1 \geq \beta_2 \geq \ldots \geq \beta_n \geq 0$$

be the ordered sequence of the moduli of coefficients a_i of the polynomial P. W. Specht [24] has established the following result.

[6] Another size associated to a polynomial P is the height $H(P)$: the largest absolute value of the coefficients.

Theorem 4.5 (Specht) *If $\xi_1, \ldots, \xi_n \in \mathbb{C}$ are the roots of the polynomial P and*

$$|\xi_1| \geq |\xi_2| \geq \ldots \geq |\xi_n|,$$

then

$$|\xi_1 \xi_2 \ldots \xi_k| \leq 1 + \beta_1 + \beta_2 + \ldots + \beta_k \quad \text{and} \quad |\xi_k| \leq \sqrt[k]{1 + \beta_1 + \beta_2 + \ldots + \beta_k}$$

for any $k = 1, 2, \ldots, n$.

The theorem of Specht will be used for describing evaluations of the height of polynomial divisors of integer polynomials. Other bounds for the height were obtained by L. Panaitopol and D. Ştefănescu [21].

Theorem 4.6 *Let $P(X) = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbb{C}[X] \setminus \mathbb{C}$. If $Q \in \mathbb{C}[X] \setminus \mathbb{C}$ is a divisor of P, $\deg(Q) = d$, then*

$$H(Q) \leq \binom{d}{\lfloor \frac{h+1}{2} \rfloor} (1 + \beta_1 + \ldots + \beta_{\lfloor \frac{d+1}{2} \rfloor}).$$

Proof. If $\eta_1, \ldots, \eta_h \in \mathbb{C}$ are the roots of Q, then we may suppose that

$$\{\eta_1, \ldots, \eta_h\} = \{\xi_1, \ldots, \xi_h\}.$$

We have

$$|b_j| = |\sum \eta_{i_1} \ldots \eta_{i_j}| = |\xi_{s_1} \ldots \xi_{s_j}| \leq \binom{h}{j} |\xi_1 \ldots \xi_j| \leq \binom{h}{j} (1 + \beta_1 + \beta_2 + \ldots + \beta_j).$$

We consider now

$$B(h, j) = \binom{h}{j} - \binom{h}{j-1},$$

and observe that

$$B(h, j) = \binom{h}{j} - \binom{h}{j-1} = \frac{h!}{j!(h-j+1)!}(h - 2j + 1).$$

Therefore

$$B(h, j) \quad = \quad \begin{cases} \geq 0 & \text{if} \quad j \leq \frac{h+1}{2}, \\ < 0 & \text{if} \quad j > \frac{h+1}{2}. \end{cases}$$

We consider

$$C(h, j) = \binom{h}{j} (1 + \beta_1 + \beta_2 + \ldots + \beta_j).$$

If $j \leq \dfrac{h+1}{2}$ then

$$C(h, j) - C(h, j-1) =$$

$$(1 + \beta_1 + \ldots + \beta_{j-1})(\binom{h}{j} - \binom{h}{j-1}) + \beta_j \binom{h}{j} = \tag{5}$$

$$(1 + \beta_1 + \ldots + \beta_{j-1}) \frac{h!}{j!(h-j+1)!}(h - 2j + 1) + \beta_j \binom{h}{j} \geq 0.$$

If $j > \frac{h+1}{2}$, we evaluate $C(h, j-1) - C(h, j)$.

We first note that

$$\beta_1 + \ldots + \beta_{j-1} \geq (j-1)\beta_j.$$

Therefore

$$C(h, j-1) - C(h, j) = \binom{h}{j}$$

$$\Big(\frac{2j-h-1}{h-j+1}(1 + \beta_1 + \ldots + \beta_{j-1}) - \beta_j\Big)$$

$$> \binom{h}{j}\Big(\frac{2j-h-1}{h-j+1}\big(1 + (j-1)\beta_j\big) - \beta_j\Big) \tag{6}$$

$$> \binom{h}{j}\beta_j \frac{(2j-h-1)(j-1) - (h-j+1)}{h-j+1}$$

$$= \binom{h}{j}\beta_j \frac{j(2j-h-2)}{h-j-1} > 0, \quad \text{for} \quad j > \frac{h+2}{2}.$$

Let $K(h) = \max\limits_{0 \leq j \leq h} C(h, j)$. By (5) and (6) we conclude that

$$K(h) = \max_{\frac{h}{2} \leq j \leq \frac{h+2}{2}} C(h, j).$$

Let t be such that $K(h) = C(h, t)$. We note that t is one of the rationals $\frac{h}{2}$, $\frac{h+1}{2}$, $\frac{h+2}{2}$.

For h even t can be equal to $\frac{h}{2}$ or $\frac{h+2}{2}$. Supposing $h = 2s$ we have

$$\binom{h}{\lfloor \frac{h+1}{2} \rfloor} - \binom{h}{\frac{h+2}{2}} = \binom{2s}{s} - \binom{2s}{s+1} =$$

$$\frac{(2s)!}{(s!)^2} - \frac{s}{s+1}\frac{(2s)!}{(s!)^2} = (1 - \frac{s}{s+1})\frac{(2s)!}{(s!)^2}$$

$$= \frac{(2s)!}{(s+1)(s!)^2} = \frac{1}{s}\frac{(2s)!}{(s+1)!(s-1)!} = \frac{1}{s}\binom{2s}{s+1}.$$

On the other hand $\beta_1 + \ldots + \beta_s > s\beta_{s+1}$ and it follows that

$$C(h, \lfloor \frac{h+1}{2} \rfloor) - C(h, \frac{h+2}{2}) =$$

$$\binom{2s}{s}(1 + \beta_1 + \ldots + \beta_s) - \binom{2s}{s+1}(1 + \beta_1 + \ldots + \beta_s + \beta_{s+1}) = \tag{7}$$

$$\frac{1}{s}\binom{2s}{s+1}(1 + \beta_1 + \ldots + \beta_s) - \binom{2s}{s+1}\beta_{s+1} > \binom{2s}{s+1}(\frac{1}{s}s\beta_{s+1} - \beta_{s+1}) = 0.$$

(8) If h is odd, then $t = \dfrac{h+1}{2}$.

From (7) and (8) we deduce

$$K(h) = \max_{0\le j\le h} C(h,j) = C(h, \lfloor \frac{h+1}{2} \rfloor) = \left(\begin{matrix} h \\ \lfloor \frac{h+1}{2} \rfloor \end{matrix} \right)(1+\beta_1+\ldots+\beta_{\lfloor \frac{h+1}{2} \rfloor}).$$

This gives the estimation of the height of Q.

□

Corollary 4.7 *Let $P(X) = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathcal{C}[X] \setminus \mathcal{C}$. If $Q \in \mathcal{C}[X] \setminus \mathcal{C}$ is a divisor of P, then*

$$H(Q) \le \left(\begin{matrix} n-1 \\ \lfloor \frac{n}{2} \rfloor \end{matrix} \right)(1+\beta_1+\beta_2+\ldots+\beta_{\lfloor \frac{n}{2} \rfloor}).$$

Proof. We may suppose that

$$Q(X) = X^h + \sum_{j=0}^{h-1} b_j X^j \in \mathcal{C}[X], \qquad 1 \le h \le n-1.$$

Let $K(h) = \max\limits_{0\le j\le h} C(h,j)$. From Theorem 4.6 we know that

$$K(h) = \max_{0\le j\le h} C(h,j) = C(h, \lfloor \frac{h+1}{2} \rfloor) == \left(\begin{matrix} h \\ \lfloor \frac{h+1}{2} \rfloor \end{matrix} \right)(1+\beta_1+\ldots+\beta_{\lfloor \frac{h+1}{2} \rfloor}).$$

To prove

$$K(h) \le K(h+1), \quad h \in \{1,\ldots,n-2\}.$$

we evaluate $K(h+1) - K(h)$.

For h odd, supposing $h = 2u+1$, one has

$$K(h+1) - K(h) = K(2u+2) - K(2u+1) =$$

$$\binom{2u+2}{u+1}(1+\beta_1+\ldots+\beta_{u+1}) - \binom{2u+1}{u+1}(1+\beta_1+\ldots+\beta_{u+1})$$

$$= \frac{2u+1}{u+1}\binom{2u+1}{u+1}(1+\beta_1+\ldots+\beta_{u+1}) > 0.$$

For h even, supposing $h = 2u$, one has

$$K(h+1) - K(h) = K(2u+1) - K(2u) =$$

$$\binom{2u+1}{u+1}(1+\beta_1+\ldots+\beta_{u+1}) - \binom{2u}{u}(1+\beta_1+\ldots+\beta_u)$$

$$= \frac{u}{u+1}\binom{2u+1}{u+1}(1+\beta_1+\ldots+\beta_u) + \binom{2u+1}{u+1}\beta_{u+1} > 0.$$

It follows that $\max\limits_{1\le h\le n-1} K(h) = K(n-1)$. Therefore

$$H(Q) \le \left(\begin{matrix} n-1 \\ \lfloor \frac{n}{2} \rfloor \end{matrix} \right)(1+\beta_1+\ldots+\beta_{\lfloor \frac{n}{2} \rfloor}),$$

which is the desired result. □

References

1. A. G. Akritas: *Elements of Computer Algebra with Applications*, Wiley& Sons (1989).
2. B. Beauzamy, E. Bombieri, P. Enflo, H. Montgomery: Products of polynomials in many variables, *J. Number Theory*, **36**, 219–245 (1990).
3. E. R. Berlekamp: Factoring polynomials over large finite fields, *Math. Comp.*, **24**, 713–735 (1970).
4. D.G. Cantor, H. Zassenhaus: A new algorithm for factoring polynomials over finite fields, *Math. Comp.*, **36**, 587–592 (1981).
5. A.–L. Cauchy: *Exercises de Mathématiques*, 4ème année, De Bure Frères, Paris (1829).
6. C. Calude: *Information and Randomness: an algorithmic perspective*, Springer Verlag (1994).
7. G. Chaitin: *Algorithmic Information Theory*, Cambridge University Press (1990).
8. G. J. Chaitin: Randomness in Arithmetic and the Decline and Fall of Reductionism in Pure Mathematics, *Chaos, Solitons & Fractals*, **5**, No. 2, 143–159, (1995).
9. L.E. Dickson: *Linear Groups*, Teubner–Leipzig (1901).
10. Pierre de Fermat: *Précis des œuvres mathématiques de P. Fermat et de l'Arithmétique de Diophante*. Reprint of the 1853 edition. Éditions Jacques Gabay, Sceaux, (1989).
11. J.v. Gathen: Irreducibility of multivariate polynomials, *J. Comp. Syst. Sc.*, **31**, 225–264 (1985).
12. P.C.Gilmore, A.Robinson: Metamathematical considerations on the relative irreducibility of polynomials, *Canad. J. Math.*, **7**, 483–489 (1955).
13. D. Hilbert Ueber die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten, *J.reine u. ang. Math.*, **110**, 104–129 (1892).
14. S. Lang: *Introduction to Algebraic Geometry*, Addison–Wesley (1962).
15. K. Mahler: An application of Jensen's formulæ to polynomials. *Mathematica*, **7**, 98–100 (1960).
16. M. Mignotte: An inequality about factors of polynomials, *Math. Comp.*, **28**, 1153 – 1157 (1974).
17. M. Mignotte: *Mathematics for Computer Algebra*, Springer Verlag (1991).
18. M. Mignotte, J.L. Nicolas: Statistiques sur $\mathbb{F}_q[X]$, *Ann. de l'Institut H. Poincaré*, **19**, 113–121 (1983).
19. L. Panaitopol, D. Ştefănescu: On generalized difference polynomials, *Pacific J. Math.*, **143**, 341–348 (1990).
20. L. Panaitopol, D. Ştefănescu: Some polynomial factorizations over the integers, *Bull. Math. Soc. Sc. Math. Roumanie*, **37** (**85**), n. 3–4, 127–131 (1993).
21. L. Panaitopol, D. Ştefănescu: New bounds for factors of integer polynomials, *J. UCS*, **1**,no. 8, 599–609 (1995).
22. K. A. Ribet: Wiles proves Taniyama's Conjecture; Fermat's Last Theorem Follows, *Notices Amer. Math. Soc.*, **40**, 575 – 576 (1993).
23. C. L. Siegel: Über einige Anwendungen diophantischer Approximationen, *Abh. Preus. Akad. Wiss. Phys.—Math. Kl.*, **1**, 14–67 (1929).
24. W. Specht: Zur Theorie der algebraischen Gleichungen, *Jahr. Deutsch. Math. Ver.*, **48**, 142–145 (1938).
25. V. G. Sprindzhuk: Arithmetic specializations in polynomials, *J. reine ang. Math.*, **342**, 1–11 (1983).
26. D. Ştefănescu: On meromorphic formal power series, *Bull. Math. Soc. Sc. Math. Roumanie*, **27** (**75**), 170–178 (1983).

27. M. Yasumoto: Hilbert Irreducibility Sequences and Nonstandard Arithmetic, *J. Number Theory*, **26**, 274–285 (1987).
28. P. J. Weinberger: Finding the numbers of factors of a polynomial, *J. Algorithms*, **5**, 180–186 (1984).