Tamsui Oxford Journal of Mathematical Sciences **23(4)** (2007) 435-448
Aletheia University

Number Decomposition, Algebraic Equations and Number Derivatives

G. Dattoli*, M. Quattromini†

Unitá di Fisica Teorica e Matematica Applicatas, CR ENEA-Frascati, via E. Fermi 45, I-00044 Frascati (Rome), Italy.

and

D. Sacchetti‡

Dipartimento di Statistica Probabilitá e Statistica Applicata, Universitá degli Studi di Roma "La Sapienza", Piazzale Aldo More 2, I-00185 Rome, Italy.

Received January 30, 2006, Accepted February 21, 2006.

Abstract

The authors use the point of view of the algebraic equations to study problems associated with number decomposition and number derivative.

1. Introduction

The use of algebraic equations in number decomposition and factorization is certainly not a new topic (Ref. [1]). We will reconsider the problem from

*E-mail: dattoli@frascati.enea.it
†E-mail: quattromini@frascati.enea.it
‡E-mail: sacchetti@uniroma1.it

a slightly different perspective to embed it with the more recent theories on number derivatives (Ref. [2]). We will see how the wealth of concepts and theorems, associated with the theory of algebraic equations, can be a fairly useful tool to study the properties of numbers, their factorisation and the logical structure underlying the formalism of the number derivatives.

Definition 1.1 *The sequence of digits*

$$[_{m-1}, \alpha_{m-2}, \ldots . \alpha_0] \qquad \alpha_r \in N \qquad r = 0, 1. \ldots , m-1 \tag{1}$$

will be called a reference number.

Definition 1.2 *The number*

$${}^{m}\{\alpha\}_p = (\alpha_{m-1}, \alpha_{m-2}, \ldots , \alpha_0)_p \equiv \sum_{r=0}^{m-1} \alpha_r p^r \qquad \alpha_r < p \tag{2}$$

will be called the image, in basis p, of the given reference number.

The three digit reference number [143] corresponds to the image $(1, 4, 3)_{10} = 10^2 + 4 \cdot 10 + 3$ in basis 10 and to $(1, 4, 3)_7 = 7^2 + 4 \cdot 7 + 3 = 80$ in basis 7.

Remark 1.3 The basis p is not restricted by the condition $p < 10$. For example $(1, 4, 3)_{31} = 1088$. Moreover, the conditions $\alpha_r < p$ and $\alpha_r > 0$ can be relaxed if necessary.

Remark 1.4 The components of a reference number are not restricted to numbers described by single digits in base 10 , For example, $[35, 38, 3]_{42} = 63339$.

Definition 1.5 *The polynomial having the digits of a given reference number as coefficients, namely*

$$P_{m-1}(x|\{\}) = \sum_{r=0}^{m-1} \alpha_r x^r \tag{3}$$

will be called the equivalent, or associated, polynomial to that reference number.

For example. the equivalent polynomial to the reference number [143] is

$$P_2(x|\{1, 4, 3\}) = x^2 + 4x + 3$$

Remark 1.6 The equivalent polynomial of reference number [1] is

$$P_0\left(x|\left\{1\right\}\right)=1$$

Definition 1.7 *An equivalent polynomial is called to be reducible on reals if its roots are all reals, irreducible on reals if its roots or part of them are complex. If reducible on reals it may be reducible on rationals or on integers.*

The reference numbers $[143]\,,[131]$ and $[133]$ are associated with polynomials reducible on integers:

$$x^2+4x+3=(x+1)\,(x+3)$$

reals:

$$x^2+3x+1=\frac{1}{4}\left[(2x+3)+\sqrt{5}\right]\left[(2x+3)-\sqrt{5}\right]$$

and complex numbers:

$$x^2+3x+3=\frac{1}{4}\left[(2x+3)+\imath\sqrt{3}\right]\left[(2x+3)-\imath\sqrt{3}\right]$$

respectively.

Remark 1.8 A reference number associated to a reducible equivalent polynomial will correspond to image numbers factored as product of integers, rationals, reals or complex numbers. The reference number $[1,4,3]$ has images which can be factored as $(p+1)\,(p+3)$, corresponding to the factorization of prime numbers $11,13$ in basis 10 and to the product $8\cdot 10$ in basis 7.

Definition 1.9 *The reference number*

$$[\alpha_0,\alpha_1,\ldots,\alpha_m]\qquad \alpha_r\in\mathbb{N}\qquad r=0,1,\ldots,m$$

will be called the reference complement of the reference number, its images the complement images and the equivalent polynomials the complement equivalent.

Remark 1.10 The number decomposition, associated to the equivalent polynomial reduction, does not necessarily lead to a factorisation in terms of prime numbers.

Definition 1.11 *The polynomial corresponding to a prime number factorization for a given image will be called a minimal or fundamental or absolute polynomial*
[1].

The polynomial $x^2 + 4x + 3$ is fundamental for $[1, 4, 3]_{10}$ but not for $[1, 4, 3]_7$. The concept of fundamental polynomial will be more thoroughly exploited in section 3, within the context of number derivatives.

Remark 1.12 A prime number will not be associated to any polynomial with degree larger then 1 admitting a reduction on rationals (and even on reals). The number $[1, 3, 1]_{10}$ is prime and is associated to an equivalent polynomial not reducible on rationals (see Def.1.5).

Remark 1.13 A reference number, which has a prime image in a give basis, will not have necessarily prime images in an other basis. For example, the reference number $[1, 3, 1]$ admits the prime image 131 for $p = 10$ and the non-prime image 55 for $p = 6$.

Definition 1.14 *A prime number in a given basis p will be denoted by*

$$^0\{\pi\}_p = \pi$$

Remark 1.15 The absolute polynomial of any prime number π will be the first order polynomial $x + \pi - p$ for a base $p \neq \pi$ and the zero order polynomial π for the base $p = \pi$.

Remark 1.16 The irreducibility on reals of the polynomial associated to a given reference number does not allow any particular conclusion on the nature of its image numbers. The image $[1, 3, 3]_{10} = 133$ is not prime, while

[1]Neither the equivalent nor the minimal polynomial corresponding to a given image number are unique. For example $x^2 + 4 \cdot x + 3$ and $x^2 + 6 \cdot x + 4$ are both equivalent polynomials for the same image number $143 = (1, 4, 3)_{10} = (1, 6, 4)_9$. In the same way, the polynomials $x^2 + 4 \cdot x + 3 = (x + 1)(x + 3)$ and $x^2 + 6 \cdot x + 8 = (x + 2)(x + 4)$ are both minimal for the same image number 143, for they give the same prime numer factorisation $11 \cdot 13$ for $x = 10$ and $x = 9$, respectively.

$[1,3,3]_5 = 43$ is prime.

Remark 1.17 We cannot put forward any conjecture, according to which if a reference number is associated to an equivalent polynomial, not reducible on reals or on rationals it will exist, in some basis, a corresponding image which is prime.

2. Higher Order Algebraic Equations and Number Decomposition

Theorem 2.1 *Three digits reference numbers corresponds to second degree equivalent polynomials, which are reducible on reals if* [2]

$$\Delta = \alpha_1^2 - 4\alpha_0\alpha_2 \geq 0. \tag{4}$$

The reduction on rationals is ensured if Δ *is a perfect square. If (2.1) on rationals.*

The proof is trivial and it is therefore omitted. As an example, we consider the complement reference numbers $[1,4,3]\,,[3,4,1]$ both corresponding to fundamental trinomials leading to prime number factorizations in the basis $p = 10$.

Theorem 2.2 *Reference numbers with a larger number of digits are associated with higher order equivalent polynomials, reducible on rationals if there is a prime* s *such that*

$$\begin{aligned} &a) \quad s|\alpha_0, \ldots, \alpha_{m-1} \\ &b) \quad s \nmid \alpha_0 \\ &c) \quad s^2 \nmid \alpha_0 \end{aligned} \tag{5}$$

[2] When the equal sign holds any corresponding image number is a perfect square.

Proof. The above statement is just a consequence of the Eisenstein criterion ([3]) of the reducibility of algebraic equations. All the images of the reference number $[1, 9, 9, 3]$, for which the prime 3 meets the Eisenstein conditions, cannot be factored on rationals in any basis.

The converse of the criterion is not true, in other words, such a number s may not exist and notwithstanding the reference number does not correspond to any polynomial reducible on rationals.

Theorem 2.3 *Given a polynomial associated to a given reference number* $\{\alpha\}$ *and an integer* q *satisfying the conditions:*

$$\begin{aligned} & q \mid \alpha_0, \\ & \alpha_{m-1} = 1, \\ & P_{m-1}\left(-q|\left\{\alpha\right\}\right) \;=\; \sum_{r=0}^{m-1} (-1)^r q^r \alpha_r = 0, \end{aligned} \tag{6}$$

then

$$(p+q)\,|^m \left\{\alpha\right\}_p . \tag{7}$$

Proof. According to the remark 1.6 and to the conditions 2.3 we can write

$$P_{m-1}\left(x|\left\{\alpha\right\}\right) = (x+q)\, P_{m-2}\left(x|\left\{\beta\right\}\right) \tag{8}$$

with

$$^{m-2}\left\{\beta\right\}_p = \left\{1, \beta_{m-2}, \ldots, \beta_0\right\}, \qquad \alpha_0 = \beta_0 q. \tag{9}$$

which proves the proposition. In this way we have obtained a general criterion of divisibility. According to this criterion the image in base p of a reference number$\{\alpha\}$ satisfying the above conditions can be divided by $p+q$, For example, the image number $(1, 3, 4, 9, 7)_{10}$ can be divided by 11, while the image of the same reference number in base 22 (i.e. $(1, 3, 4, 9, 7)_{22} = 268341$) has 23 among its divisors.

Once again, the converse is not true. We note, indeed, that the reference number $[7, 4, 8]$ does not fulfill the conditions (2.3) for $q = 1$ and notwithstanding $(7, 4, 8)_{10}$ is divisible by 11.[3]

[3] As is easily checked using the ordinary divisibilty criterion by 11 (any number is divided by 11 if the sum of its composing digit with alternating sign is zero or a multiple of 11).

Remark 2.4 The assumption that the digits of the reference number are all positive can be relaxed. The image number $(7,4,8)_{10} = (7,5,-2)_{10}$, is divisible by 11 according to the proposition (2.3) which also ensures that $p+1$ divides $(7,5,-2)_p$in any other basis with $p > 7$[4].

Corollary 2.5 *If* $\alpha_0 = 1$, $\alpha_m \neq 1$, $\alpha_m < 0$, $r|\alpha_m$ *and*

$$\sum_{s=0}^{m-1} \alpha_{m-1-s} (-r)^s = 0, \tag{10}$$

then the number is such that

$$(1+rp)\,|^m \{\alpha\}_p\,. \tag{11}$$

Proof. We can always associate to an equivalent polynomial its complement equivalent polynomial

$$\overline{P}_{m-1}\left(y|\overline{\{\alpha\}}\right) = \sum_{s=0}^{m-1} a_{m-1-s} y^s$$

whose roots are related to those of the equivalent polynomial by the relation $y = \dfrac{1}{x}$ and this proves our statement.

Theorem 2.6 *If the associated polynomials of the reference number* $[a_{m-1},\ldots,a_0]$ *with* $\alpha_{m-1} = 1$ *admits integer negative roots* $-r_i, i = 1,\ldots,m-1$ [5]*, then the sum of the divisors of the image number in basis p will satisfy the conditions*

$$\sum_{i=1}^{m} d_i = \alpha_{m-2} + (m-1)\,p \tag{12}$$

and

$$\sum_{i=1}^{m} (d_i - p)^{-1} = \frac{\alpha_1}{\alpha_0}. \tag{13}$$

[4]The restriction $p > 7$ is not necessary if we relax the condition $\alpha_r < p$.

[5]This condition can be relaxed if one is not interested in integer number factorizations.

According to the hypothesis we have

$$P_m\left(x|\left\{\alpha\right\}\right)=\prod_{i=1}^{m}\left(x+r_i\right)$$

which implies that the divisors of the number ${}^{m}\left\{\alpha\right\}_{p}$ are $d_i=r_i+p$. The proof is easily completed by noting that the sum of the roots of a $m-$th degree algebraic equation is provided by the coefficient with degree $m-1$ of the linear term with reversed sign, The little Fermat theorem (LFT) (ref. [2] states that if ξ and q are relatively primes and q is prime, then

$$\xi^q-\xi=nq, \tag{14}$$

where n is an integer.

Theorem 2.7 *The reference number*

$$F_{q|n}=\left\{\begin{array}{c} 1,\ \underbrace{0,0,\ldots 0}_{q-2},\ -1,-nq \end{array}\right\} \tag{15}$$

has images

$$F_{q|n}\left(p\right)=\left[\begin{array}{c} 1,\ \underbrace{0,0,\ldots 0}_{q-2},\ -1,-nq \end{array}\right]_p \tag{16}$$

such that

$$\left(p-\xi\right)|F_{q|n}\left(p\right). \tag{17}$$

The statement is just a consequence of the LTF and of Theorem (2.1). As an example of application we note that $F_{q|n}\left(56\right)=55073148$ is divisible by 53.

Definition 2.8 *The Carmichael numbers, which will be denoted by* ${}^{m}\left\{c\right\}_{10}$*, are not primes satisfying the LFT conditions. The Korselt theorem ensures that they can be factored as the product of* r *distinct primes* π_i *according to the relation*

$${}^{m}\left\{c\right\}_{10}=\prod_{i=1}^{r}\pi_i \tag{18}$$

and satisfy the property that $\pi_i - 1$ *are divisors of* ${}^m\{c\}_{10} - 1$.

An example of Carmichael number is provided by $\{5,6,1\}_{10} = 561 = 3 \cdot 11 \cdot 17$, and it is easily checked that $2, 10, 16$ are all divisors of 560.

Remark 2.9 The previous property can be generalized as follows: we can define r distinct basis

$$p_i = \pi_i - 1. \tag{19}$$

where the Carmichael number can be rewritten, namely 20

$${}^m\{c\}_{10} = (\chi_n, \ldots, \chi_0,)_{p_r} \tag{20}$$

such that $\chi_0 = 1$, and

$$\sum_{s=0}^{n} (-1)^s \chi_s = 0. \tag{21}$$

thus finding that $(\chi_n, \ldots, \chi_0,)_{p_r}$ is divisible by p_i+1 and that $(\chi_n, \ldots, \chi_0,)_{p_r}-1$ is divisible by p_i. To give a specific example we note that the Carmichael number $41041 = 7 \cdot 11 \cdot 13 \cdot 41$ can be rewritten in basis $p = 12$ as $(4,0,4,1)_{10} = (1,11,9,0,1)_{12}$, which fulfils both conditions (2.17) and (2.18).

3. Number Derivatives

We have so far exploited the concept of number equivalent polynomial, the introduction of image number derivative is therefore a fairly natural consequence. The number derivatives and the underlying formalism have been proposed in previous papers (Refs. ([1,5,3])), here we will mainly refer to the results of Ref. ([1]) and develop a different point of view, which treats the concept of number derivative as a natural consequence of that of ordinary derivative. We will take advantage from the definitions and remarks discussed in the previous sections, and the concept of absolute polynomial will be of noticeable importance in what follows.

Definition 3.1 *Given the reference number* $\{\alpha_{m-1}, \ldots, \alpha_0\}$ *possessing in some basis* p *an absolute polynomial, we will assume that it can be factored as*

$$P^A_{m-1}(x|\{\alpha\}) = \prod_{i=1}^{m-1} (x - r_i), \tag{22}$$

where r_i are not all positive and distinct roots.

Remark 3.2 The existence of such an absolute polynomial is always ensured if we relax the condition $\alpha_r < p$ (see Remark 1.6).

Remark 3.3 The above definition implies that

$$p - r_i = \pi_i$$

with π_i being a prime so that the image number in basis p possesses the (not necessarily square-free) factorization

$$P_m^A\left(p|\left\{\alpha\right\}\right) = \prod_{i=1}^{m} \pi_i.$$

Definition 3.4 *We will define the derivative of the image number* ${}^m\left\{\alpha\right\}_p$ *as*

$${}^m\left\{\alpha\right\}_p^{'} = \frac{d}{dx} P_m^A\left(p|\left\{\alpha\right\}\right)_{x=p}.$$

It is to be understood that such a definition implies that the ordinary derivative acts, according to the ordinary rules, on absolute polynomial only, factored as in (3.1).

Theorem 3.5 *The explicit form of the image number derivative is*

$${}^m\left\{\alpha\right\}_p^{'} = {}^m\left\{\alpha\right\}_p \sum_{i=1}^{m} \pi_i^{-1} \tag{23}$$

and

$${}^0\left\{1\right\}_p^{'} = 0 \tag{24}$$

and

$${}^1\left\{\pi\right\}_p^{'} = 1. \tag{25}$$

Proof. Eq.(3.2) is a direct consequence of the ordinary derivation rules, of Definitions 2.8 and 3.1 and of the remark 2.9, eq. (3.3) a consequence of (3.2) and of the Remark 1.6, eq. (3.4) is a consequence of (3.2) and of the Remark 2.9.

Corollary 3.6 *If π_i are the prime factors of a given reference number ${}^{m}\{\alpha\}_p$, that is*

$$ {}^{m}\{\alpha\}_p = \prod_{k=1}^{q} \pi_k^{e_k}, \qquad \sum_{i=1}^{k} e_k = m \tag{26} $$

the image number derivative writes

$$ {}^{m}\{\alpha\}_p^{'} = \{\alpha\}_p \sum_{k=1}^{q} \frac{e_k}{\pi_k} \tag{27} $$

The proof is trivial and is omitted for brevity.

Theorem 3.7 *The operation of image number derivative is not linear.*

Proof. According to Def. 3. the derivative of the sum of two reference number ${}^{m_1}\{\alpha_1\}_{p_1} + {}^{m_2}\{\alpha_2\}_{p_2}$ is not given by the sum of the two derivatives. The procedure for the evaluation of the derivative is described below

a) we define the reference number ${}^{m}\{\beta\}_p = {}^{m_1}\{\alpha_1\}_{p_1} + {}^{m_2}\{\alpha_2\}_{p_2}$,

b) we define the relevant absolute polynomial and evaluate the derivative according to Def. 3.

c) It is then checked that, in general ${}^{m}\{\beta\}_p^{'} \neq {}^{m_1}\{\alpha_1\}_{p_1}^{'} + {}^{m_2}\{\alpha_2\}_{p_2}^{'}$, As a straightforward example we note that $5' = 1 \neq 2' + 3' = 2$.

Corollary 3.8 *The k^{th} derivative of an image number cannot be expressed as*

$$ {}^{m}\{\alpha\}_p^{(k)} = \left(\frac{d}{dx}\right)^{k} P_m\left(x|\,\{\alpha\}\right)_{x=p}, \qquad k > 2, \tag{28} $$

using the same example as before, as $[1,4,3]_{10}^{'} = 33 + 11 = 44$ and we can associate to 44 the image $[1,3,-18]_5$, thus getting, for the relevant minimal polynomial

$$ P_3(x) = (x-3)(x+6) $$

which leads to $[1,4,3]_{10}^{''} = 48$.

Remark 3.9 As a practical rule we note that according to the previous definition and theorems we find that

$$\left(\pi^k\right)' = k\pi^{k-1}. \tag{29}$$

Theorem 3.10 *The derivative of the product of two reference numbers can be evaluated according to the following "Leibnitz type" rule*

$$\left[{}^{m_1}\left\{\alpha_1\right\}_p \cdot {}^{m_2}\left\{\alpha_2\right\}_p\right]' = {}^{m_1}\left\{\alpha_1\right\}_p' \cdot {}^{m_2}\left\{\alpha_2\right\}_p + {}^{m_1}\left\{\alpha_1\right\}_p \cdot {}^{m_2}\left\{\alpha_2\right\}_p'.$$

Proof. According to Def. 3.the above product can be associated to the absolute polynomial

$$P_m\left(x|\left\{\beta\right\}\right) = \prod_{i=1}^{m_1}\left(x - r_{1,i}\right)\prod_{j=1}^{m_2}\left(x - r_{2,j}\right), \qquad m = m_1 + m_2$$

with

$$p - r_{\alpha,i} = \pi_\alpha, \qquad \alpha = 1, 2.$$

so that the proofs of the theorem holds as a consequence of Def. 3.

Remark 3.11 The theorem holds also for different basis p_1, p_2. This allows the definition of the derivative of the product of numbers without any reference to absolute polynomial, reference numbers etc. as

$$\left(N_1 \cdot N_2\right)' = N_1' \cdot N_2 + N_1 \cdot N_2'$$

.

Theorem 3.12 *The derivative of the rational number* $R = \dfrac{N_1}{N_2}$ *is given by*

$$\left(\frac{N_1}{N_2}\right)' = \frac{N_1' N_2 - N_1 N_2'}{N_2^2} \tag{30}$$

Proof. Since

$$R \cdot N_2 = N_1 \tag{31}$$

we can differentiate both sides and get, by virtue of Remark 3

$$R' \cdot N_2 + R \cdot N_2' = N_1' \tag{32}$$

by solving with respect to $R^{'}$ and by using eq. (31) again we get (30), thus proving the theorem. We can proceed "ad libitum": other theorems can be proved and the definition can be extended to irrational and complex numbers. Our goal was proving that the formalism of algebraic polynomials may guarantee a fairly direct and natural definition of number derivatives. Further comments will be developed in the concluding section.

4. Concluding Remarks

In the course of the years some formulae became popular between "prime numbers busters". In particular Euler proposed the formulae

$$N_{17}(n) = n^2 + n + 17, \tag{33}$$

$$N_{41}^{+}(n) = n^2 + n + 41. \tag{34}$$

The first yields all prime numbers for n up to 15, the second for n up to 39. We can easily understand, using the point of view developed in the previous sections, why these formulae fails above 15 and 41 respectively. We note indeed that

$$N_{17}(16) = \{1, 2, 1\}_{16} = 17^2,$$
$$N_{41}^{+}(40) = \{1, 2, 1\}_{40} = 41^2.$$

Furthermore

$$N_{17}(20) = \{1, 2, -3\}_{20},$$
$$N_{41}(44) = \{1, 2, -3\}_{44}.$$

which are divisible by 19 and 43 as can be easily checked from the discussion of the previous section. On the other side for $n < 16, n < 40$, we end up with a polynomial which cannot be reduced on reals or rationals. The number $N_{17}(2) = \{1, 0, 1, 1, 1\}_2$ is associated to a polynomial which does not admit any decomposition on reals. Other formulae of the previous type have been proposed in the literature, as for example

$$N_{41}^{-}(n) = n^2 - n + 41, \qquad n \leq 40, \tag{35}$$

$$N_{79,1601}(n) = n^2 - 79n + 1601, \qquad n \leq 79, \tag{36}$$

it can however be easily checked that they can be bwritten in terms of the (14) and indeed

$$N_{41}^{-}(n+1) = N_{41}^{+}(n), \tag{37}$$
$$N_{79,1601}(n) = N_{41}^{-}(n-39).$$

it can also be proved that

$$N_{p}^{-}(n) = N_{41}^{-}(n-p), \qquad p \text{ prime} < 39.$$

yields prime numbers for $n \leq p-1$.

We have explored the concept of number derivative and we have provided a common framework with the theory of equivalent polynomials and number decomposition, in Fig. 1 we report a plot relevant to the first second and third derivatives of the first 20 integers, it is worth stressing that the primes in the plot lie on a straight line parallel to axis. In Fig. 2 we have reported the successive values of the number derivatives of given numbers vs the order of the derivative, we have considered stable and unstable cases. The plots have been derived using a very compact code written with Mathematica, which is enclosed to the paper and can be exploited to generate any sequence derivative.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, Berlin, **1980**.

[2] V. Ufnarovsky and B. Alander, How to differentiate a number, *J. Integer Seq.* **6** (2003).

[3] L. Gral, *Classical Galois Theory*, Chelsea, New York, **1988**.

[4] E. J. Barbeau, Remark on arithmetic derivation, *Canad. Math. Bull.* **4** (1961), 117-122.

[5] G. L. Cohen and D. E. Iannucci, Derived sequences, *J. Integer Seq.* **5** (2003).

[6] K. B. Oldham and J. Spanier, *The Fractional Calculus*, Academic Press, New York, **1974**.