The Mathematics Enthusiast

Volume 3 | Number 2 Article 3

7-2006

Numbers and Polynomials- 50 years since the publication of Wittgenstein's Bemerkungen über die Grundlagen der Mathematik (1956): Mathematical and Educational reflections

Giorgio T. Bagni

Numbers and Polynomials

50 years since the publication of Wittgenstein's *Bemerkungen über die grundlagen der mathematik* (1956): mathematical and educational reflections

Giorgio T. Bagni

Department of Mathematics and Computer Science
University of Udine (Italy)

Abstract: *According to L. Wittgenstein, the meaning of a mathematical object is to be grounded upon its use. In this paper we consider Robinson theory Q, the subtheory of first-order Peano Arithmetic PA; some theorems and conjectures can be interpreted over one model of Q given by a universe of polynomials; with respect to nonconstant polynomials some proofs by elementary methods are given and compared with corresponding results in the standard model of PA. We conclude that the creative power of the language can be pointed out in how the language itself is embedded into the rest of human activities, and this is an important track to follow for researchers in mathematics education.*

Keywords: Peano Arithmetic; Robinson Arithmetic; Wittgenstein

1. Introduction

> Knowledge in mathematics: Here one has to keep on reminding oneself of the unimportance of the 'inner process' or 'state' and ask «Why should it be important?» What does it matter to me? What is interesting is how we *use* mathematical propositions.
>
> Ludwig Wittgenstein (1969, n. 38)

Although, from the ontological point of view, the "Platonic" conception in which mathematical objects exist independent of their representations cannot be stated uncritically, mathematical objects do not exist as real, concrete objects and mathematical knowledge can only be attained through representations. This fact leads us to consider the so-called *cognitive paradox of mathematical thought*, pointed out by R. Duval, who underlines that although mathematical learning is conceptual, any activity involving mathematical objects takes place only through semiotic representations (Duval, 1995). As a consequence, it is necessary to make a clear distinction between the mathematical object (if it exists) and its different semiotic representations (Otte, 2001, p. 33).

However the plurality of representations of a mathematical object can imply the recognition of a plurality of objects: how can we coordinate this diversity of objects taking into account that the professional mathematician sees a unique object? It would be possible, according to Ludwig Wittgenstein (1889-1951), to accept the grammatical intra-discursive nature of mathematical objects: the doctrine of "meaning as use" (Wittgenstein, 1953, n. 43) is connected to the key concept of "context embeddedness", where the term is understood not merely as the physical environment of a linguistic utterance, but is referred to a wider cultural context (McGinn , 1984; McDonough, 1989; Godino & Batanero, 1997). A philosophical problem facing epistemological realism after the "linguistic turn" can be summarized in the following question: how can the assumption that there is an independently existing world be compatible with the linguistic position according to which we cannot have unmediated access to reality? (Habermas, 1999).

***The Montana Mathematics Enthusiast,* ISSN 1551-3440**, **Vol. 3, no.2, pp. 146-156**.

Let us consider a quotation from Wittgenstein's *Philosophical Investigations*, published posthumously in 1953 (*Philosophische Untersuchungen* in German):

"Perhaps you say: two can only be ostensively defined in this way: «This *number* is called 'two'». For the word «number» here shews what place in language, in grammar, we assign to the word. But this means that the word «number» must be explained before the ostensive definition can be understood. – The word «number» in the definition does indeed shew this place; does shew the post at which we station the word. (…) Whether the word «number» is necessary in the ostensive definition depends on whether without it the other person takes the definition otherwise than I wish. And that will depend on the circumstances under which it is given, and on the person I give it to. (…) So one might say: the ostensive definition explains the use –the meaning– of the word when the overall role of the word in language is clear" (Wittgenstein, 1953, nn. 29-30).

So the meaning of a mathematical object (for instance of numbers) can be grounded upon its use. But can we always consider a particular use of the mathematical words (for instance with regard to Arithmetics) as completely natural? In this paper we shall consider two non-isomorphic models of an arithmetic theory in order to investigate the following issue: apart from representation registers employed, is this philosophical approach embodied into mathematics itself? More generally, what is the relationship between Mathematics and some crucial philosophical issues regarding the meaning? For instance, can we state that "there are infinitely many couples of primes p, q such that $q = p+2$" (the celebrated Twin Prime Conjecture) without possible misunderstandings?

Previous considerations are related to teaching undergraduate mathematics: as a matter of fact the theoretical analysis of what it means to understand a concept and how understanding can be constructed by the learner (Asiala & Al., 1996) requires an investigation of some fundamental epistemological and, more generally, philosophical issues. So, in our opinion, problems dealing with the meaning of a mathematical object and of its expression are relevant to mathematics education, both for teachers and for students. Of course our aim is not to provide complete answers to these fundamental questions; but a reflection upon the language (in particular, the mathematical language) can be based upon some considerations, for instance about Mathematical Logic and Arithmetics. So we are going to propose a contribution to the debate based upon the discussion of a mathematical example that will be introduced and discussed by elementary methods.

2. Arithmetic theories and models

Natural numbers, or counting numbers, are grounded on our common everyday experience and their perception and interpretation can be considered as a very important aspect of our common sense (nevertheless some basic remarks can be considered: Wittgenstein, 1969). But can we state that this interpretation is always totally clear? More precisely, can we state that the meaning attributed to the common arithmetical language is independent from interpretation? We shall try to reflect about these questions: in other words, we are going to investigate if Arithmetics itself can be interpreted according several (theoretical, mathematical) point of views.

In this paper we shall consider, by elementary methods, the set **N** of natural numbers and a particular set of polynomials. In order to present and clarify our choice, let us remember some well known considerations about Number Theories[1]. *Robinson Arithmetic* (introduced by Tarski, Mostowski and Robinson in 1953 and usually denoted by *Q*) is weaker than *Peano*

[1] For a theoretical study of weak Arithmetics see Macintyre, 1987 and the quoted references.

Arithmetic, denoted by *PA* (Mendelson, 1997, p. 128 and p. 187); *Q* can be obtained from *PA* if the induction:

$$\varphi(0)\wedge(\forall y)(\varphi(y)\rightarrow\varphi(s(y)))\rightarrow(\forall y)\varphi(y)$$

(in the language $\{+, \cdot, s, 0\}$, s is the successor function) is replaced by the axiom:

$$(\forall y)(y \neq 0\rightarrow(\exists z)(y = s(z)))$$

that is a theorem in *PA* and can by easily proved by induction.[2]

In order to show the importance of the (mathematical) interpretation of basic arithmetical objects, we shall consider some models of arithmetic theories, in particular models of *PA* and *Q* (Kaye, 1991), by elementary methods.

The set **N** of natural numbers with the addition and the multiplication is the standard model of *PA*, <**N**, +, ·, s, 0>; the existence of non-standard models of *PA* (models non-isomorphic to the standard model) was proved in 1934 by Skolem. While non-standard models of *PA* are not (educationally) simple to be proposed, it is interesting to present models of *Q* non-isomorphic to **N**: for instance, we shall denote by $Z^*[x]$ the set whose elements are 0 and all polynomials with integral coefficients whose leading coefficients are positive: $Z^*[x]$ with the addition and the multiplication is a model of *Q* (Mendelson, 1997, p. 188), $<Z^*[x], +, \cdot, s, 0>$.

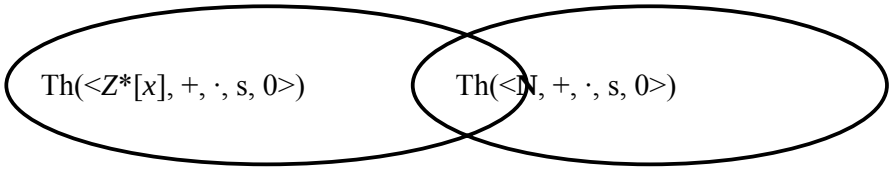
3. A comparison between $<Z^*[x], +, \cdot, s, 0>$ and <N, +, ·, s, 0>

First of all, let us underline some meaningful differences between the considered models: the paragraphs 3 and 4 will be devoted to this comparison, that will be relevant to the aim of our paper.

As a matter of fact, $<Z^*[x], +, \cdot, s, 0>$ is not a model of *PA*:

$$(\forall y)(\exists z)(z+z = y \vee z+z = y+1)$$

that can be proved by induction, is not in $Z^*[x]$ (every nonconstant polynomial of $Z^*[x]$, $B(x) = a_n x^n+a_{n-1}x^{n-1}+...+a_1x+a_0$ whose coefficients a_n, a_{n-1}, $...+a_1$ aren't all even can be considered as a counterexample)[3]: so considered models $<Z^*[x], +, \cdot, s, 0>$ and <**N**, +, ·, s, 0> are not elementary equivalent. Let us underline that we shall find true propositions in $<Z^*[x], +, \cdot, s, 0>$ that are false with reference to <**N**, +, ·, s, 0> (this can be stated theoretically, too: if not, the models <**N**, +, ·, s, 0> and $<Z^*[x], +, \cdot, s, 0>$ would be equivalent, and this is absurd; see for instance: Chang & Keisler, 1973, p. 32). We shall summarize previous statements in the following picture, where Th(*M*) usually indicates the set of all sentences true in *M*:



[2] The role of the axiom schema of induction and of the phenomenon of incompleteness in *PA* and in subtheories are important fields of contemporary research; see Hájek & Pudlák, 1993, where fragments of *PA* resulting by restricting the induction schema to formulas belonging to a prescribed class are studied.

[3] Every proposition that can be proved in *Q* can be proved in *PA*, too; there are propositions that can be proved in *PA* and that cannot be proved in *Q*; of course a proposition that can be proved in *PA* cannot be confuted in *Q*. If any proposition can be proved in *PA* and can be confuted in *Q*, being *PA* an extension *Q*, then *PA* would be inconsistent.

Of course Th(<**N**, +, ·, s, 0>)∩Th(<$Z^*[x]$, +, ·, s, 0>) ≠ ∅; in fact, it includes the set of all sentences deducible from *Q*.

We noticed that an element of Th(<**N**, +, ·, s, 0>)–Th(<$Z^*[x]$, +, ·, s, 0>) is: $(\forall y)(\exists z)(z+z = y \vee z+z = y+1)$. Later, we shall present an element of Th(<$Z^*[x]$, +, ·, s, 0>)–Th(<**N**, +, ·, s, 0>), too.

4. Order in $Z^*[x]$

According to an axiom of *Q*, the order is defined in $Z^*[x]$ as follows:

$$f(x) \le g(x) \quad \text{iff (def.)} \quad g(x)-f(x) \in Z^*[x]$$
$$f(x) < g(x) \quad \text{iff (def.)} \quad 0 \ne g(x)-f(x) \in Z^*[x]$$

We can state some basic properties: if $f(x)$, $g(x)$, $h(x)$ belong to $Z^*[x]$:

$$\text{if } f(x) \le g(x) \text{ then } f(x)+h(x) \le g(x)+h(x)$$
$$\text{if } f(x) < g(x) \text{ then } f(x)\cdot h(x) < g(x)\cdot h(x)$$
$$\text{if } f(x) \le g(x) \text{ then } f(x)+h(x) \le g(x)+h(x)$$
$$\text{if } f(x) < g(x) \text{ then } f(x)\cdot h(x) < g(x)\cdot h(x) \quad (\text{being } h(x) \ne 0)$$

If $f(x)$, $g(x)$, $h(x)$, $h(x)–f(x)$, $h(x)–g(x)$ belong to $Z^*[x]$:

$$\text{if } f(x) \le g(x) \text{ then } h(x)-g(x) \le h(x)-f(x)$$
$$\text{if } f(x) < g(x) \text{ then } h(x)-g(x) < h(x)-f(x)$$

As regards the minimum element of $Z^*[x]$, for every $f(x) \in Z^*[x]$: $0 \le f(x)$.

These properties hold in $Z^*[x]$ being provable in *Q*; moreover, the following results are trivial:

- If $f(x), g(x) \in Z^*[x]$, then either $f(x) \le g(x)$ or $g(x) \le f(x)$.
- If $f(x), g(x) \in Z^*[x]$ and $f(x) < g(x) \le f(x)+1$, then $g(x) = f(x)+1$.
- If $f(x) \in Z^*[x]$, $g(x)$ is a nonconstant element of $Z^*[x]$, $f(x) < g(x)$ and $g(x)–f(x)$ is nonconstant, for every n, k positive integers, it is $f(x)+n < g(x)–k$.

This last property is interesting: by that we present an infinity of couples of elements $f, g \in Z^*[x]$ such that $f<g$ and an infinity of couples of elements $n, k \in Z^*[x]$ such that $f+n<g–k$. Such property holds with reference to $Z^*[x]$, but it does not hold in **N**. So, have we found an element of Th(<$Z^*[x]$, +, ·, s, 0>)–Th(<**N**, +, ·, s, 0>)? The problem is that logical quantifiers are finitary, so we cannot use an infinity of existential quantifiers in the same sentence[4].

Let us now underline an interesting fact: any nonconstant $g(x) \in Z^*[x]$ could be considered as an "infinite" element; in fact, for every natural number n we can write $n<g(x)$ (proof is trivial). So in $Z^*[x]$ there are different "infinite" elements, for instance $x < x+1 < x^2 < x^2+1$ and so on.

For every $n \in \mathbf{N}$, $a \in \mathbf{Z}$ it is: $n<x+a$; so we have, in $Z^*[x]$:

$$0 < 1 < 2 < \ldots < x–2 < x–1 < x < x+1 < x+2 < \ldots$$

If by $[x]$ we mean $\ldots x–2, x–1, x, x+1, x+2 \ldots$ (a "copy of **Z**"), let us write:

[4] Concerning natural numbers, if we want to express that the property $P(n)$ holds for an infinity of n, we can write, for instance: $(\forall m)(\exists n)(m<n \wedge P(n))$, but a similar expression cannot be now used in $Z^*[x]$ in order to express our statement.

$$Z^*[x] = \{\mathbf{N}, [x]\}$$

where we state moreover that the copy of **Z** [x] is "adjacent" to **N**. The following results are trivial:

- No $f(x) \in Z^*[x]$ whose degree is 1 and leading coefficient is greater than 1, or whose degree is greater than 1, is such that $n < f(x) < x+a$, $n \in \mathbf{N}$, $a \in \mathbf{Z}$.
- If the degree of $f(x) \in Z^*[x]$ is lower than the degree of $g(x) \in Z^*[x]$, then $f(x) < g(x)$.
- If the degree of $f(x) \in Z^*[x]$ is equal to the degree of $g(x) \in Z^*[x]$ and if the leading coefficient of $f(x)$ is lower than the leading coefficient of $g(x)$, then $f(x) < g(x)$.
- Let $f(x)$, $g(x)$ nonconstant elements of $Z^*[x]$, having the same degree and the same leading coefficient; let n be the maximum degree for which coefficients a_n of $f(x)$ and b_n of $g(x)$ are not equal; if $a_n < b_n$, then $f(x) < g(x)$.

We write $Z^*[x]$ in the following way, with reference to ordered "copies of **Z**":

$$Z^*[x] = \{\mathbf{N}, [x], [2x], [3x], [4x] \ldots$$
$$\ldots [x^2-2x], [x^2-x], [x^2], [x^2+x], [x^2+2x] \ldots$$
$$\ldots [2x^2-2x], [2x^2-x], [2x^2], [2x^2+x], [2x^2+2x] \ldots [x^3] \ldots\}$$

5. Prime elements belonging to $Z^*[x]$

Let us now turn back to the questions proposed in the first paragraph; so we shall consider some propositions in order to point out differences between what happens in **N** and in $Z^*[x]$.

It is easy to interpret constant non-negative polynomials and natural numbers (**N** and the subset of constant elements belonging to $Z^*[x]$ are isomorphic), so **N** is a submodel of $Z^*[x]$ (Chang & Keisler, 1973, p. 21): so every proposition with a single existential quantifier that is true in **N** is of course true in $Z^*[x]$ too, and every proposition with a single universal quantifier true in $Z^*[x]$ is true in **N**, too. These considerations will be important with reference to the rest of our paper.

We shall present some conjectures and frequently we shall consider "prime elements". Let us give the following definition: $p \in Z^*[x]$ is *prime* if it is different from 0 and from 1 and if there are not two elements belonging to $Z^*[x]$, both of them different from 1, whose product is p; so a polynomial is prime if and only if it is irreducible and primitive (i.e. the gcd of its coefficients is 1), too. So we can express Pr(y) ("y is prime") by:

$$y \neq 0 \wedge y \neq 1 \wedge (\neg(\exists a)(\exists b)(a \neq 1 \wedge b \neq 1 \wedge ab = y))$$

As regards a comparison between numbers and polynomials, some differences are immediately clear: for instance, in $Z^*[x]$ for every integer k the polynomial $x+k$ is prime, while if a natural number $n>2$ is prime, its successor is even so it is not prime. This remark is interesting: in fact, by writing:

$$(\exists y)(y \neq 2 \wedge \mathrm{Pr}(y) \wedge \mathrm{Pr}(y+1))$$

we have found an element of Th(<$Z^*[x]$, +, ·, s, 0>)–Th(<**N**, +, ·, s, 0>).

It is trivial to show some arithmetic propositions in $Z^*[x]$ (as regards arithmetic conjectures, see: Guy, 1994). Let us consider the presence of primes in any arithmetic progression (according to a well known theorem proved in 1837 by Dirichlet, if $h>1$ and $a \neq 0$ are relatively prime then the progression: a, $a+h$, $a+2h$, $a+3h$, … includes infinitely many prime numbers: Ribenboim, 1995, p. 205). With respect to polynomials, it is easy to find arithmetic progressions entirely including prime elements; for instance, if h is any integer, $h \neq 0$, all

polynomials of the progression x, $x+h$, $x+2h$, $x+3h$, … are prime. It follows, for instance, the version of the Twin Prime conjecture in $Z^*[x]$[5]: it is trivial to verify that there are infinitely many couples of prime elements $(P(x); Q(x))$ belonging to $Z^*[x]$ such that $Q(x) = P(x)+2$ (e.g. $P(x) = x+k$, $Q(x) = x+k+2$, for every $k\in\mathbf{Z}$).

Another interesting remark is referred to prime elements that can be written as n^2+1: are they infinitely many? It is an open problem in **N** (2005). It is trivial to show that there are infinitely many elements $P(x) \in Z^*[x]$ such that $[P(x)]^2+1$ is a prime element of $Z^*[x]$ (e.g. $P(x) = x+k$ for every $k\in\mathbf{Z}$; it follows: $[P(x)]^2+1 = x^2+2kx+k^2+1$ that is prime, being primitive and irreducible: $\Delta(k) = -4 < 0$: Bagni, 2002). A general form of the last conjecture in **N** is the following: if a, b, c are relatively prime, a is positive, $a+b$ and c are not both even and b^2-4ac is not a square, then there are infinitely many primes an^2+bn+c (Hardy & Wright, 1979, p. 19). As regards $Z^*[x]$, it is trivial to prove that if a, b, c are relatively prime, a is positive, b^2-4ac is not a square, then there are infinitely many elements $P(x)\in Z^*[x]$ such that $a[P(x)]^2+bP(x)+c$ is a prime element of $Z^*[x]$ (once again, consider $P(x) = x+k$ for every $k\in\mathbf{Z}$).

It is interesting to consider in $Z^*[x]$ some results of the additive Number Theory. For instance, the well known Lagrange's theorem which states that every natural number is the sum of four squares (see for instance: Nathanson, 1996a, p. 37and 1996b) doesn't hold in $Z^*[x]$: there are elements of $Z^*[x]$ that cannot be expressed as a sum of square elements of $Z^*[x]$ (e.g. any polynomial of $Z^*[x]$ whose degree is 1 cannot be expressed as the sum of squares of $Z^*[x]$).

6. Two great problems: Catalan and Goldbach conjectures

Paragraphs 6 and 7 are devoted to some classical problems: we shall consider them with reference to both the models **N** and $Z^*[x]$.

Let us remember the Catalan conjecture in **N**, which asserts that 8 and 9 are the only consecutive powers (Nathanson, 2000, p. 186); equivalently, it states that the only solution of the equation $x^m-y^n = 1$, being x, y, m, n natural numbers greater than 1, is: $x = n = 3$, $y = m = 2$. To prove or disprove this conjecture was a great problem in Number Theory until its proof, announced by P. Mihailescu in 2002.[6]

Of course we shall not try to prove the Catalan conjecture in $Z^*[x]$ by elementary methods: such proof would imply a proof of the conjecture in **N**, too. However, it is possible to prove that $x^m-y^n = 1$, being $m\geq 2$, $n\geq 2$ natural numbers, has no solution x, y in nonconstant polynomials belonging to $\mathbf{C}(t)$ (Nathanson, 1974). So Catalan conjecture holds for nonconstant polynomials of $Z^*[x]$.

---

[5] From the formal point of view, let us underline once again that logical quantifiers are finitary, while the Twin Prime conjecture considers the existence of *infinitely* many couples of twin primes; so it must be expressed as follows: $(\forall n)(\exists p)[\mathrm{Pr}(p)\wedge\mathrm{Pr}(p+2)\wedge(p>n)]$ (where $\mathrm{Pr}(m)$ means "m is prime"). It is interesting to remember that we don't know if there are infinitely many twin primes (2005), but in 1919 Brun proved that the sum of the reciprocals of twin primes converges to 1.902160577783278… (it is the so-called Brun's constant).

[6] In 1999, M. Mignotte proved that eventual exceptions to Catalan conjecture (of course, if they exist) would be such that: $m > 7.15\cdot 10^{11}$, $n > 7.58\cdot 10^{16}$ (Peterson, 2000).

In order to consider the Goldbach conjecture in $Z^*[x]$, we must underline that it is a conjecture where there is a universal quantifier[7]: once again, we shall examine only nonconstant polynomials (Bagni, 2002). Let us prove the following result:

PROPOSITION 1. If the nonconstant polynomial $Q(x)\in Z^*[x]$ is not primitive, then there are two prime polynomials $Q_1(x)\in Z^*[x]$, $Q_2(x)\in Z^*[x]$ such that $Q(x) = Q_1(x)+Q_2(x)$.

PROOF. Let us consider a nonconstant and non-primitive polynomial belonging to $Z^*[x]$ (where pq is the gcd of its coefficients and p is prime):

$$Q(x) = pqa_nx^n+pqa_{n-1}x^{n-1}+...+pqa_1x+pqa_0$$

Let us consider the following polynomials belonging to $Z^*[x]$, being $t\in\mathbf{Z}$:

$$Q_1(x) = x^n+pqa_{n-1}x^{n-1}+...+pqa_1x-p(pt+1)$$
$$Q_2(x) = (pqa_n-1)x^n+p(qa_0+pt+1)$$

whose sum is $Q(x)$ for every t. We shall show that it is possible to find t such that both polynomials $Q_1(x)$ and $Q_2(x)$ are prime.

For every t, $Q_1(x)$ is irreducible from Eisenstein criterion: the prime p divides its coefficients apart the leading one and p^2 doesn't divide $p(pt+1)$; moreover $Q_1(x)$ is primitive so it is prime.

If it is not $qa_0 \equiv -1 \pmod p$, then qa_0+pt+1 is not a multiple of p so Eisenstein criterion can be applied to $Q_2(x)$ too and $Q_2(x)$ is irreducible for every t. Let us show that $Q_2(x)$ is primitive for some t: $(qa_0+1)+pt$ is prime for infinitely many t from Dirichlet theorem (qa_0+1 and p are relatively prime) and t can be chosen such that qa_0+pt+1 is prime and greater than pqa_n-1.

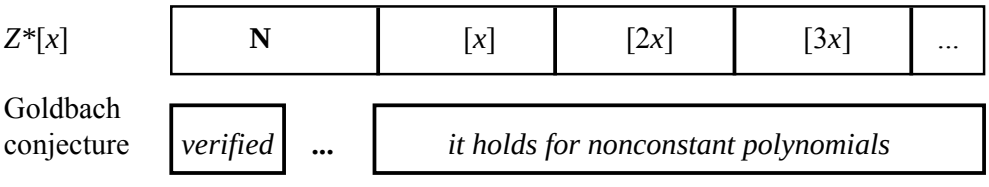
If $qa_0 \equiv -1 \pmod p$, so $qa_0 = kp-1$ being k an integer, it is:

$$Q_2(x) = (pqa_n-1)x^n+p^2(k+t)$$

There are infinitely many t such that $k+t$ is prime and greater than pqa_n-1: so we can find t such that $Q_2(x)$ is irreducible from Eisenstein criterion and primitive. ■

From this proposition (being $p = 2$) it follows that the Goldbach conjecture holds for nonconstant polynomials of $Z^*[x]$, where we call *even* a polynomial such that the gcd of its divisors is even.[8]

We can summarize previous statements in the following figure. With respect to $Z^*[x]$ (and to ordered "copies of $\mathbf{Z}$"), we notice that Goldbach conjecture is empirically verified for an initial (finite) set of natural numbers; then its validity is not proved for infinitely many natural numbers; finally, it holds for all nonconstant polynomials of $Z^*[x]$.



[7] In Goldbach conjecture there is not only a universal quantifier: in fact, it states that for every even integer n greater than 2 there is a couple of primes (p, q) such that $p+q = n$: so there are two existential quantifiers, too: however if n is an integer, p and q are integers, too. As regard experimental verifications, in 1998 Richstein verified Goldbach conjecture up to $4\cdot10^{14}$.

[8] Concerning Goldbach conjecture let us indicate Weyl, 1942, Erdös, 1965, Wang, 1984.

7. The Last Fermat Theorem

Another interesting situation can be finally described with reference to the Fermat Last Theorem. It is trivial to extend the theorem from **N** to $Z^*[x]$: if there are three non-zero and nonconstant polynomials $A(x)$; $B(x)$; $C(x)$ belonging to $Z^*[x]$ and a natural number $n \geq 3$ such that $[A(x)]^n+[B(x)]^n = [C(x)]^n$, we can assign a value to x such that $A(x)$, $B(x)$, $C(x)$ are positive (the leading coefficients are positive) so the (proved) Last Fermat Theorem in **N** would not hold: absurd.

Concerning nonconstant elements of $Z^*[x]$, it is possible to prove the Fermat Last Theorem independently from its proof in **N**, too: it is possible to prove that the Fermat equation $a^n+b^n = c^n$ has no (noncostant) polynomial solutions if $n \geq 3$ (Greenleaf, 1969; such equation has solutions in polynomials for $n = 2$, for instance $a = (x^2-1)^2$; $b = (2x)^2$; $c = (x^2+1)^2$: Nathanson, 2000, p. 183).

$Z^*[x]$	**N**	$[x]$	$[2x]$	$[3x]$	...
Fermat, Catalan (Mihailescu)	*proved*	*it holds for nonconstant polynomials*			

8. Final reflections

> One cannot contrast *mathematical* certainty with the relative uncertainty of empirical propositions. For the mathematical proposition has been obtained by a series of actions that are in no way different from the actions of the rest of our lives, and are in the same degree liable to forgetfulness, oversight and illusion. Now can I prophesy that men will never throw over the present arithmetical propositions, never say that now at last they know how the matter stands? Yet would that justify a doubt on our part?
>
> Ludwig Wittgenstein (1969, nn. 651-652)

Let us briefly turn back to the question proposed in the first paragraph of this paper: can we really state that "there are infinitely many couples of primes p, q such that $q = p+2$" with no possible misunderstandings? Previous considerations show that many other similar questions can be proposed.

Of course the answer would require attention and care. By that we do not mean that the mathematical language is surely ambiguous: nevertheless different models of arithmetic theories, in particular some models of *PA* and *Q*, can be considered: and the study of the presented model of *Q* non-isomorphic to **N** points out that, for instance, the sentence "there are infinitely many couples of primes p, q such that $q = p+2$" depends on the particular context.[9]

So how can we "translate" a mathematical statement? What is the meaning to be attributed to the sentence (see paragraph 5) "there is a prime different from 2 such that its successor is prime"? Is it true or false? According to Quine, there are always different ways to distribute functions among words, and this cause the so-called "indeterminacy of translation" (Quine,

[9] The fundamental problem of the meaning can be considered with reference to mathematical theories, too: is it possible to discuss the meaning of *PA* and *Q*? Further research can be devoted to this issue.

1960). As previoulsy noted, this does not lead to state that mathematical words and concepts are meaningless: but can we always raise absolute question of "right" or "wrong" in translating (or interpreting) mathematical language? Different "theories of translation" can be based upon different abnalytical hypotheses (let us remember that, according to Quine, in order for a statement to be analytic, it must be true by definition). And Wittgenstein, too, pointed out that mathematical propositions describe neither abstract entities nor empirical reality (their a priori status is due to the fact that their role is a normative one: Glock, 1996): their certainty is obtained by operations grounded in our actual lives (Wittgenstein, 1969, nn. 651-652), so it depends upon particular facts, that is, upon contexts or situations: words (mathematical words, too) have meaning insofar as they are candidates for use within propositions that have meaning, and propositions are meaningful as used within a context (Morawetz, 1980, p. 59).

As previously pointed out, our aim is not to provide answers to these philosophical questions (Habermas, 1999); but in our opinion, aforementioned remarks can be useful from the educational point of view, too. As a matter of fact, Steinbring underlines that in classroom interactions the use of mathematical language is frequently acquired "by means of social participation, and not (…) according to strict rules" (Steinbring, 2002, p. 10), so we underline the primary importance of an adequate negotiation of meanings between teacher and pupils.[10] Moreover, let us underline that the problem of the meaning is relevant to all representative registers employed (Duval, 1995), being connected to the language itself; let us quote once again Wittgenstein:

"Instead of producing something common to all that we call language, I am saying that these phenomena have no one thing in common which makes us use the same word for all, – but that they are related to one another in many different ways. And it is because of this relationship, or these relationships, that we call them all «language»" (Wittgenstein, 1953, n. 65).

But our language "did not emerge from some kind of ratiocination" (Wittgenstein, 1969, n. 475), and the origin of a "language game" (in the sense of: Wittgenstein, 1953) is a reaction. So, following Wittgenstein, we can conclude that language is not (just) a code, whose power can be mainly referred to its syntax; its creative power lies in how the language itself is embedded into the rest of human activities (Morawetz, 1980; Shotter, 1996), and the mathematical study of the models of a theory provides an example in order to underline the primary importance of the context. In our opinion, this is an interesting track to follow for researchers in mathematics education.

Acknowledgments

Warmest thanks to colleagues Prof. Claudio Bernardi and Prof. Maurizio Fattorosi-Barnaba (University of Rome 1 "La Sapienza") for their important suggestions.

References

Asiala, M., Brown, A., DeVries, D., Dubinsky, E., Mathews, D. & Thomas, K. (1996). A framework for research and curriculum development in undergraduate mathematics education. *Research in Collegiate Mathematics Education II*, Kaput, J., Schoenfeld, A.H. & Dubinsky, E. (Eds.), CBMS Issues in Mathematics Education, 6, 1-32.

Bagni, G.T. (2002), Congetture e teorie aritmetiche, *Archimede*, 2, 96-100.

Chang, C.C. & Keisler, H.J. (1973). *Model Theory*, North-Holland, Amsterdam-London.

Duval, R. (1995). *Sémiosis et pensée humaine*, Peter Lang, Paris.

[10] Of course this does not mean that if notation and terms are introduced correctly, no misconception will occur.

Erdös, P. (1965). Some recent advances and current problems in number theory, *Lectures on Modern Mathematics*, 3, 196-244, Wiley, New York.

Glock, H-J. (1996). *A Wittgenstein Dictionary*, Basil Blackwell, Oxford.

Godino, J. D. & Batanero, C. (1997). Clarifying the meaning of mathematical objects as a priority area of research in mathematics education, Sierpinska, A. & Kilpatrick. J. (Eds.), *Mathematics education as a research domain: a search for identity*, Kluwer, Dordrecht, 177-195.

Greenleaf, N. (1969). On Fermat's equation in **C**(*t*), *American Mathematical Monthly*, 76, 808-809.

Guy, R.K. (1994). *Unsolved Problems in Number Theory*, 2nd edition, Springer-Verlag, Berlin-Heidelberg-New York.

Habermas, J. (1999). *Wahrheit und Rechtfertigung. Philosophische Aufsätze*, Suhrkamp Verlag, Frankfurt am Mein (*Truth and Justification*, MIT Press, Cambridge 2003).

Hájek, P. & Pudlák, P. (1993). *Metamathematics of First-Order Arithmetic*, Springer-Verlag, Berlin-Heidelberg-New York.

Hardy, G.H. & Wright, E.M. (1979). *An Introduction to the Theory of Numbers*, 5th edition, Clarendon Press, Oxford (original edition, 1938).

Jacobson, N. (1974). *Basic Algebra I*¸ Freeman, San Francisco.

Kaye, R.W. (1991). *Models of Peano Arithmetic*, Clarendon Press, Oxford.

Macintyre, A. (1987). The strength of weak systems, *Schriftenreihe der Wittgenstein-Gesellschaft* 13, Logic, Philosophy of Science and Epistemology, Wien, 43-59.

McDonough, R. (1989). Towards a Non-Mechanistic Theory of Meaning, *Mind*, XCVIII (389), 1-21.

McGinn, C. (1984). *Wittgenstein on Meaning*, Basil Blackwell, Oxford.

Morawetz, T. (1980). *Wittgenstein and Knowledge: The Importance of 'On Certainty'*, Humanities Press, Atlantic Highlands, NJ.

Mendelson, E. (1997). *Introduction to mathematical logic*, 4th edition, Van Nostrand, Princeton.

Nathanson, M.B. (1974). Catalan's equation in K(*t*), *American Mathematical Monthly*, 81, 371-373.

Nathanson, M.B. (1996a). *Additive number theory. The classical bases*, Springer-Verlag, Berlin-Heidelberg-New York.

Nathanson, M.B. (1996b). *Additive number theory. Inverse problems and geometry of sumsets*, Springer-Verlag, Berlin-Heidelberg-New York.

Nathanson, M.B. (2000). *Elementary methods in Number Theory*, Springer-Verlag, Berlin-Heidelberg-New York.

Otte, M. (2001). Mathematical epistemology from a semiotic point of view, *Paper presented to the Discussion Group on Semiotics at the 25th PME*.

Peterson, I. (2000). *MathTrek: Zeroing In on Catalan's Conjecture*, Dec. 4, 2000: www.sciencenews.org/20001202/mathtrek.asp

Quine, W.V.O. (1960). *Word and Object*, MIT Press, Cambridge MA.

Ribenboim, P. (1995). *The Book of Prime Number Records*, 3rd edition, Springer-Verlag, Berlin-Heidelberg-New York.

Shotter, J. (1996). *Talk of saying, showing, gesturing, and feeling in Wittgenstein and Vygotsky*, http://www.massey.ac.nz/~alock/virtual/wittvyg.htm

Steinbring, H. (2002). What makes a sign a mathematical sign? An epistemological perspective on mathematical interaction, *Paper presented to the Discussion Group on Semiotics at the 26th PME*.

Wang, Y. (1984). *Goldbach Conjecture*, World Scientific Publishers, Singapore.

Weyl, H. (1942). A half-century of mathematics, *American Mathematical Monthly*, 58, 523-553.

Wittgenstein, L. (1953). *Philosophical Investigations*, Basil Blackwell, Oxford.

Wittgenstein, L. (1969). *On certainty*, Basil Blackwell, Oxford.