Modern Logic
Volume 8, Number 1/2 (January 1998–April 2000), pp. 47–86.

THE INTERNAL CONSISTENCY OF ARITHMETIC WITH INFINITE DESCENT

YVON GAUTHIER

Abstract. The consistency of arithmetic is shown to obtain without the recourse of transfinite induction or the detour of an infinite set. Arithmetic without an induction postulate, but with infinite descent, is Fermat Arithmetic coupled with Kronecker's "general arithmetic" of indeterminates. Fermat arithmetic is self-consistent or self-contained. The main idea is to interpret a local (constructive) logic with a local "effinite" quantifier in a polynomial translation and show how logic is eliminated by infinite descent in the same way as the content is exhausted in the decomposition of polynomials (or forms) where the method of infinite descent is at work. The arithmetization of logic (and the topological interpretation) is effected through the (combinatorial) convolution product of polynomials and amounts to a parametrization of logic by polynomials with indeterminates. Although not always effective, infinite descent provides a finite constructivist setting for an arithmetic that encompasses most of number theory and a large part of algebraic or arithmetic geometry. The resulting arithmetical logic can be seen as a vindication of Kronecker's foundational outlook beyond Hilbert's programme.

Contents

1. Introduction

A proof of the consistency of arithmetic without the induction postulate, but with infinite descent is given in the following. No use is made of transfinite induction, and "internal" means that infinite descent will be shown to be self-consistent. We call this arithmetic with infinite descent Fermat arithmetic (FA) to contrast it with Peano arithmetic (PA) (see [Gauthier1989]). The main idea is to translate logic into arithmetic via a polynomial interpretation with Kronecker's indeterminates and is thus an attempt at the arithmetization of logic in the line of what can be called "Kronecker's programme". The logic is constructive, that is, it has all the intuitionistic features plus some constructive (local) characteristics to be described below. Fermat arithmetic is minimal in the sense that it is sufficient for (elementary or constructive) number theory up to (some important part of) algebraic or arithmetic geometry. André Weil has stressed the import of Fermat's infinite descent [Weil1] and Kronecker's arithmetical theory of algebraic quantities in the making of modern mathematics, but the constructive nature of such proof methods has not been generally recognized by logicians. Rather, logicians in general have tended to assimilate infinite descent and complete induction on the one side and to favor Dedekind's transcendental method over Kronecker's algorithmic approach on the other[1] (see Edwards [Edwards] and also [Gauthier1994]).

From a (classical) logical point of view, infinite descent is identified with the least number principle

$$\exists x A x \rightarrow \exists x[Ax \wedge \forall y(y < x \rightarrow \neg A(y))]$$

for a formula A and y different from x with no occurrence in A. This principle can be obtained from the principle of complete induction

$$\forall x[\forall y(y < x \rightarrow Ay) \rightarrow Ax] \rightarrow \forall x A x$$

which is deducible from Peano's induction postulate

$$\forall x[A0 \wedge \forall x(Ax \rightarrow ASx)] \rightarrow \forall x A x.$$

[1] Exceptions are found mainly among mathematicians. Poincaré, Mordell, Weil not to mention more recent workers in algebraic geometry have all used infinite descent as a "more" effective method of proof than complete induction. As for Kronecker, Weil has made clear that he is the true originator of algebraic "arithmetic" geometry. The present work could be seen as a vindication of "Kronecker's programme" of a general arithmetic (*allgemeine Arithmetik*) in the foundations of mathematics for which he claimed internal truth and consistency (*innere Wahrheit und Folgerichtigkeit*).

Transfinite induction substitutes ordinals σ for natural numbers in the following schema

$$\forall\sigma[\forall t((t < \sigma \rightarrow A(t,x)) \rightarrow A(\sigma,x)] \rightarrow \forall\sigma A(\sigma,x)$$

with the limit

$$\lim_{n\rightarrow\omega} \left.\omega^{\omega^{\cdot^{\cdot^{\cdot^{\omega}}}}}\right\}^{n} = \varepsilon_0.$$

Transfinite induction has been used by Gentzen in his proof of the consistency of arithmetic, and Ackermann could not but invoke it in his own proof [Ackermann].

From a different point of view, Nelson [Nelson] offers a predicative or bounded version of the least number principle. From

$$\begin{aligned}\min x_1 \ldots x_r\ A \equiv A \wedge \neg\exists y_1 \ldots \exists y_r(y_1 \leq x_1 \wedge \ldots \wedge y_r \leq x_r \wedge \\ (y_1 \neq x_1 \vee \ldots \vee y_r \neq x_r) \wedge Ax_1 \ldots x_r[y_1 \ldots y_r]),\end{aligned}$$

where the y's do not occur in A and are all different from the variables x, the principle simply states

$$\exists x_1 \ldots \exists x_r A \rightarrow \exists x_1 \ldots \exists x_r \min x_1 \ldots x_r\ A,$$

a metatheorem which is proven within predicative arithmetic. Buss [Buss] has shown how $\sum_i^b$-LMIN axioms are equivalent to the $\prod_i^b$-PIND or corresponding bounded induction axioms. But Nelson's arithmetization of (classical) logic stops short of a consistency proof for arithmetic with infinite descent, although there is a proof of the self-consistency of Robinson's theory Q using the Hilbert-Ackermann consistency proof with quantifier elimination. Our aim is to obtain self-consistency for a larger theory, FA, with constructive means in the polynomial interpretation.

We look at logic as arithmetical logic, that is logical formulas are interpreted as polynomials and constants as arithmetical operations. This last point was emphasized by Ackermann in his [Ackermann][2]. The introduction of Hilbert's ε-symbol and its subsequent elimination in proofs of consistency (cf. Herbrand and Ackermann) for the predicate calculus and pure number theory have also inspired the way we treat "effinite" quantification through reduction by infinite descent.

[2] Skolem's quantifier-free primitive recursive arithmetic and Goodstein's equational calculus foreshadow arithmetical logic, but explicit use of complete induction in Skolem [Skolem] is alien to Fermat arithmetic, while the unlimited (unbounded) substitution of number variables by definite numerals in Goodstein amounts to complete induction. See [Goodstein].

Finally, it should be noticed that infinite descent has entered axiomatic set theory by the front door. The axiom of foundation formulated by von Neumann

$$\forall x\{x \neq \varnothing \rightarrow \exists y(y \in x \wedge y \cap x = \varnothing)\}$$

comes from what Mirimanoff [Mirimanoff] called ordinary sets (*ensembles ordinaires*) which generate only finite descents. A sequence of elements $e_1 \ni e_2 \ni e_3 \ldots$ of a set E stops when one descends to an indecomposable element, that is $\varnothing$, also called "core" by Mirimanoff. The axiom of replacement also formulated by von Neumann [Neumann1] (inspired by Fraenkel) in the form

$$x \in V \wedge \mathrm{Func}(f) \rightarrow f''x \in V,$$

which means that if x belongs to the set-theoretic universe V, its image also belongs to V. It is easily seen that we have here the cumulative hierarchy. Mirimanoff had already the three operations (or postulates) for the cumulative hierarchy: union, power set and replacement which he explains as:

> If a set $(a, b, c, \ldots)$ exists, then any equivalent set $(E, F, G, \ldots)$ exists, where $E, F, G \ldots$ are existing (distinct) ordinary sets.

Takeuti has attempted a justification of transfinite induction by resorting to infinite descent in his [Takeuti]—for a critique see [Gauthier1985]—but von Neumann [Neumann2] under the impulse of Mirimanoff's infinite descent could already introduce ordinals through transfinite induction:

> "Every ordinal is the set of ordinals preceding it (*Jede Ordnungszahl ist die Menge der ihr vorangehenden Ordnungszahlen*)."

Together with the axiom of replacement it was the birth certificate of the cumulative hierarchy.

Historically, transfinite induction was introduced by Hausdorff as complete induction on Cantor's transfinite ordinals in their normal (polynomial) form

$$\phi = \omega^{\mu}\nu_0 + \omega^{\mu-1}\nu_1 + \cdots + \nu_{\mu}$$

with decreasing finite powers. In that context, transfinite induction is precisely infinite descent extended to transfinite ordinals. We shall see, however, that infinite descent is sufficient for arithmetic.

2. Logic

The logic is presented in a sequent calculus which is minimal, with no structural rules but with new notions, *i.e.*, two new connectives, local negation and local implication, and a new quantifier called the "effinite quantifier". The basic concept "sequence" is divided in two, finite sequences which are sets and effinite sequences which are not. There are no infinite sequences. An effinite sequence is open-ended, that is, it has a pre-positional bound, *e.g.*, 0, but no post-positional bound, *e.g.*, ω. An effinite sequence is somewhat like Brouwer's infinitely proceeding sequences without any pre-assigned limit. When an effinite sequence has post-positional bound, it becomes an initial segment, *i.e.*, a set. Though it is minimal, the radical logic we are devising aims at providing a natural framework for arithmetic, that is constructive theorems of number theory, *e.g.*, Euclid's theorem on the infinity of primes. In a way, our logic is a finite probe for the concept of infinity. All notions are meant to be local and the logic itself is a "local logic".

The universe consists of the effinite sequences of natural numbers which we call the arithmetical domain D.

Remark. This notion of domain has some similarity with the domains (*champs*) of Herbrand's Fundamental Theorem where "the necessary and sufficient condition for a proposition not to have property B is that it be false in some infinite domain" [Herbrand]. However, we do not need here Herbrand's notion of order, since a post-positional bound on an effinite sequence makes a (finite) set out of it.

2.1. **Syntax.**

2.1.1. *Vocabulary.* Our first-order language L(T) for our first-order theory T has an effinite supply of atomic symbols:

(1) letters (capital and small) for formulas (and sentences) A, B, C, ... together with their punctuation signs, points, commas, parentheses, brackets, *etc.*
(2) letters for variables x_1, x_2, ..., x_n,
(3) predicate letters p_j^n and the predicate symbol $=$,
(4) function letters f_j^n —when f is 0-ary, we consider it as a constant,
(5) the connectives $\wedge$, $\vee$, $\neg$, $\rightarrow$,
(6) the quantifiers $\forall$, $\exists$, and Ɨ.

The terms consists exclusively of:

(1) variables,

(2) sequences composed of terms and functions letters, *e.g.*, $f_j^n t_1, \ldots, t_n$ for the terms $t_1, \ldots, t_n$.

Formulas or wffs consist exclusively of:

(1) atomic formulas composed of terms and predicate letters, *e.g.*, $p_j^n t_1, \ldots, t_n$ for the terms $t_1, \ldots, t_n$,
(2) any wff consisting of formulas composed of connectives and quantifiers.

Remark. Sentences are closed formulas, *i.e.*, formulas are "open" sentences where variables occur free, that is, are not quantified upon. An instance $A(t_1, \ldots, t_n/x_1, \ldots, x_n)$ of a formula A is the result of subtituting terms t for the free occurrences of a variable x.

I adopt the standard formulation of the sequent calculus (see, for example, [Girard]). A sequent is an expression $\Gamma \vdash \Delta$ where Γ and Δ are finite sequences of formulas; Γ is the antecedent, *e.g.*, $A_1 \wedge \ldots \wedge A_n$ and Δ the succedent, *e.g.*, $B_1 \wedge \ldots \wedge B_m$, with the interpretation

$$(A_1 \wedge \ldots \wedge A_n) \rightarrow (B_1 \vee \ldots \vee B_m).$$

2.1.2. *Axioms.* The system of LL (Local Logic) has the axiom

Axiom 1. $$A \vdash A$$

for A an arbitrary formula. Axiom 1 is the identity axiom. Since we do not have structural rules (see below), we take as axioms all formulas of the form

$$\Gamma, A \vdash A, \Delta \qquad \text{(for the weakening rule)}$$

2.1.3. *Logical rules.* Logical rules are expressed in the sequent calculus with a left-right symmetry while in a system of natural deduction, this symmetry is replaced by the *intelim* rules (introduction and elimination rules). The bar indicates that the sequent of the conclusion under the bar has been obtained from the sequent of the premiss by the given rules. Since our system is a system of local logic (with minimalist and intuitionistic properties), in practice we can consider only sequents $\Gamma \vdash \Delta$, where Δ consists of a unique formula. The logical rules are the following:

Conjunction

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\ r\wedge$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma,\ A \wedge B \vdash \Delta}\ l1\wedge \qquad\qquad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ l2\wedge$$

Disjunction

$$\frac{\Gamma \vdash A,\ \Delta}{\Gamma \vdash A \vee B,\ \Delta}\ r1\vee \qquad \frac{\Gamma,\ A \vdash \Delta \qquad \Gamma,\ B \vdash \Delta}{\Gamma,\ A \vee B \vdash \Delta}\ l\vee \qquad \frac{\Gamma \vdash B,\ \Delta}{\Gamma \vdash A \vee B,\ \Delta}\ r2\vee\ .$$

Remark. Since the logic is local, conjunction and disjunction are assumed to be locally (individually) provable, in particular disjunction has the disjunction property of intuitionistic logic: if $A \vee B$ is provable, it means that either $\vdash A$ or $\vdash B$ is provable — for conjunction, $\vdash A$ and $\vdash B$ are provable.

Negation being local, the minimal derivation of negation can be written

Negation

$$\frac{\Gamma,\ A \vdash \Delta}{\Gamma \vdash \neg A,\ \Delta}\ r\neg \qquad \frac{\Gamma \vdash A,\ \Delta}{\Gamma,\ \neg A \vdash \Delta}\ l\neg\ .$$

Remark. One can introduce or eliminate negation (to the right or to the left), if one has reason to do so, *i.e.*, one has found a contradiction. Double negation cannot be eliminated, as we shall see later.

Implication

$$\frac{\Gamma,\ A \vdash B,\ \Delta}{\Gamma \vdash A \to B,\ \Delta}\ r\to \qquad \frac{\Gamma \vdash A,\ \Delta_1 \qquad \Gamma,\ B \vdash \Delta_2}{\Gamma,\ A \to B \vdash \Delta_1,\ \Delta_2}\ l\to\ .$$

Remark. Notice that since we do not have $a \to \neg\neg a$ (no more than $\neg\neg a \to a$), except in finite symmetric situations (see [Gauthier1985]), implication is also local, being intimately tied with negation.

Universal quantification

$$\frac{\Gamma \vdash A,\ \Delta}{\Gamma \vdash \forall x\ A,\ \Delta}\ r\forall(*) \qquad \frac{\Gamma,\ A(t) \vdash \Delta}{\Gamma,\ \forall x\ A(x) \vdash \Delta}\ l\forall(**)\ .$$

Remark. Since $\forall$ applies only to finite domains, it does not differ from the intuitionistic (or classical) finite quantifier – of course $\forall$ as well as $\exists$ and Ɪ below are subject to the usual restrictions on variables: $(*)$ means that x is not free in Γ, Δ and $(**)$ means that the substitute t is an arbitrary term of L.

Existential quantification

$$\frac{\Gamma \vdash A(t),\ \Delta}{\Gamma \vdash \exists x\ A(x),\ \Delta}\ r\exists(**) \qquad \frac{\Gamma,\ A \vdash \Delta}{\Gamma,\ \exists x\ A \vdash \Delta}\ l\exists(*)\ .$$

Remark. The existence property of intuitionistic logic, *i.e.*, $\vdash \exists x A(x)$ is provable means that $\vdash A(t)$ is provable for some (numerical) t.

Effinite quantification

$$\frac{\Gamma \vdash A(x_n),\ \Delta}{\Gamma \vdash \text{Ɨ}x\ A,\ \Delta}\ r\,\text{Ɨ}(*) \qquad \frac{\Gamma,\ A(x_n) \vdash \Delta}{\Gamma,\ \text{Ɨ}x_n\ A(x_n) \vdash \Delta}\ l\,\text{Ɨ}(*)\ .$$

Remark. Some words of explanation are in order. In the r part, Ɨ behaves like universal quantification, and in the l part, it behaves like existential quantification; this means that effinite quantification is really existential quantification iterated effinitely, that is "generalized existence" and not existential generalisation. On the other hand, universal generalisation applied to an effinite sequence means that there is no counterexample to be found, a fact similar to Hilbert's use of the ε-symbol to define universal quantification

$$\forall x A x \equiv A(\varepsilon_x \neg A(x)).$$

$\text{Ɨ}x_n$ means obviously that the variables in A occur effinitely often, and $A(x_n)$ means that there is an effinite sequence of variables in A (eigenvariables) not identified with those in A; only if they are the same, can $\text{Ɨ}xAx$ be eliminated, that is to say that the left rule is only there for the sake of symmetry. There are no structural rules in our calculus, but there is a general principle of local shift according to which main formulas remain lexicographically ordered either side of the turnstile $\vdash$ in additions, deletions or exchanges (permutations) — alphabetical order may be ascendant or descendant. The combinatorial principle is latent. There is no cut rule either. If cut should be added, it would be eliminable.

The rules for minimal negation do not capture the essence of intuitionist negation. In LJ (J for intuitionist), we have the rule

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}$$

for the symbol of absurdity $\bot$, which amounts to a structural weakening (or addition), while classical negation requires also

$$\frac{\Gamma,\ \neg A \vdash \bot}{\Gamma \vdash \neg\neg A}\ ,$$

but these are not local.

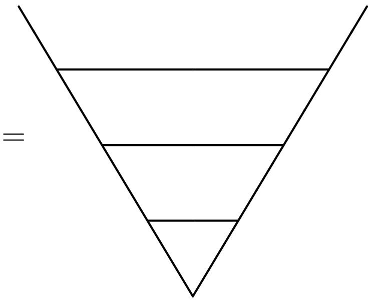
2.2. **Semantics.** Model is taken in the usual sense of a model for a given structure S which is a triple $S =< U_s, p_s, f_s >$, where U_s is the universe of the structure, p_s are the predicates and f_s the functions of the language L(T) of a first-order theory T. A structure is a model when the proper axioms of T are all valid in the structure. I depart slightly from the classical notion, as we shall see immediately.

The model of local logic is a quadruple $M =< D_M, f_M, p_M, \varphi_M >$ where D_M is the domain (of natural numbers), the f_M are arithmetic functions (operations) and the p_M are arithmetic predicates. To each formula is assigned a positive integer, its "valuator", *i.e.*, a number which locates the formula in the arithmetical universe. Conjunction, disjunction and implication correspond respectively to multiplication, addition and exponentiation, while the sum operation represents existential quantification, and the product operation represents universal quantification. Effinite quantification is interpreted as a continued product for a non-terminating sequence. φ_M is a function which maps the (closed) formulas of the theory into the natural numbers: I call it the *assignment map*, and it is defined in the following manner:

(1) $\varphi_M(A)[n] = 1 \quad \text{iff} \quad A_n \in D_M$.
(2) $\varphi_M(\neg A)[n] = 0 \quad \text{iff} \quad \neg A_n \in D_M$.
(3) $\varphi_M(A \wedge B)[n \times m] = 1 \quad \text{iff} \quad A_n \in D_M$ and $B_m \in D_M$.
(4) $\varphi_M(A \vee B)[n + m] = 1 \quad \text{iff} \quad A_n \in D_M$ or $B_m \in D_M$.
(5) $\varphi_M(A \overset{\text{loc}}{\rightarrow} B))[n^m] = 1 \quad \text{iff} \quad A_n \in D_M$ implies $B_m \in D_M$.
(6) $\varphi_M(\exists x Ax)[n + m + \ell\ \ldots] = 1 \quad \text{iff} \quad \sum A_n \in D_M$.
(7) $\varphi_M(\forall x Ax)[n \times m \times\ \ldots\ \times \ell] = 1 \quad \text{iff} \quad \prod A_n \in D_M$.
(8) $\varphi_M(\exists\!\!\!\!\mid x Ax)[n \times m \times \ell\ \ldots] = 1 \quad \text{iff} \quad \prod A_n \ldots \in D_M$.

Remarks. The assignment of natural numbers (and arithmetic operations) is not as arbitrary — like a Gödel numbering — as it may seem, but serves rather as a basis for the polynomial translation which interprets logic in arithmetical terms — as an arithmetical logic. This semantics bears some analogy to the Kleene-Nelson notion of realizability, but it is aimed here at a constructivist setting for arithmetical logic, not as an interpretation of intuitionistic logic – somewhat in the Kolmogorov style. In clause 8, the dots mean that the sequence does not terminate, while the sequence does terminate in clause 7 — $\forall x$ means that we have a (finite) set and that universal quantification is limited to sets (instead of taking sums and products over the variables, I indicate the quantification through the indexing of the predicate). The notion of domain of natural numbers (see [Gauthier1977]) can be schematized as the open structure of the arithmetical universe

$D =$



D_n

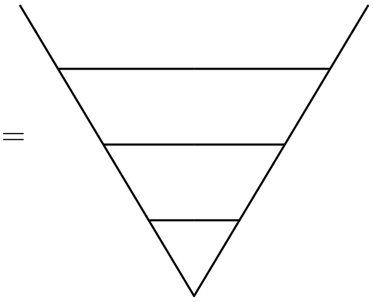
$D_{n-m} \qquad (1 \leq m < n)$

$D_{n-(n-1)}$

D_{n-n}

where the D_i represent stages indexed by integers — compare with the cumulative rank structure of Z-F set theory

$V =$



V_γ (for inaccessible ordinal γ)

$V_\alpha = \bigcup_{\beta<\alpha} \mathrm{V}_\beta$ (for limit-ordinal α)

$V_{\alpha+1} = \mathrm{V}_\alpha \bigcup \mathrm{P}(\mathrm{V}_\alpha)$

$V_0 = \varnothing$

where the axiom of foundation serves as the building principle (inherited from infinite descent).

2.3. **The interpretation of the logical constants.** I privilege an arithmetical interpretation of constants, as can be seen from the formulation of the model, and that means that constants have arithmetical existence. Not only disjunction and the existential quantifier, but also conjunction, negation, implication, universal and effinite quantification have arithmetical import. Conjunction is seen as multiplication, the universal quantifier as a finite product of numerical instances, disjunction as addition, and, while the existential quantifier is a finite sum, the effinite quantifier must be looked at as an iterated product, as an effinite product or sequence, not as an infinite sequence of conjunctions in set-theoretic semantics. Negation and implication stand in a close relationship. Let us start with the relative pseudo-complement of a, denoted by $a \Rightarrow b$ and defined as

$$a \Rightarrow b = \mathrm{In}((X - a) \cup b) \ ,$$

where a and b are open subsets of a topological space X, and In is the interior. $a \Rightarrow b$ is the greatest element different from a. $X - a$ is the difference or relative complementation. Negation is interpreted as arithmetic difference, remembering that substraction is not negation in the usual sense.

If implication can be seen as a continuous curve only in a non-standard model — the topological interpretation — we could interpret it arithmetically as a Cauchy product of power series, since a continuous function can be represented arithmetically by a power series (or a polynomial in the finite case)

$$\sum_0^\infty c_n x^n = \left(\sum_0^\infty a_n x^n\right)\left(\sum_0^\infty b_n x^n\right)$$

for $c_n = a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0$, that is, the Cauchy diagonal or convolution product, which does not lead out of the realm of natural numbers unlike Cantor's diagonal — of course, we have to reinterpret ∞ as the bad infinite of approximation, but this is done easily with the effinite quantifier on constants a_n and indeterminates x. The net result is that we can have a concept of local (strict) implication in an arithmetical setting, affording more than Ackermann's positive fragment of strong implication.

To what extent is our constructive logic arithmetical? To see this, we shall introduce arithmetic with (Fermat's) infinite descent and then reformulate Euclid's elementary proof of the infinity of primes which uses a primitive form of infinite descent. Gentzen says in [Gentzen] that Euclid's proof of the infinity of primes which uses infinite descent contains a somewhat disguised complete induction and translates it as such in his system — although Gentzen distinguishes between infinite descent and complete induction, he does not emphasize the constructive character of the former. Here, I want a more direct approach than Gentzen's. From a constructivist viewpoint, complete induction (or Peano's postulate) and infinite descent are not the same, and it is important to stress the difference if one wants to stick to the most stringent proof theory, as Gentzen undoubtedly wanted to in his perpetuation of Hilbert's programme.

3. Arithmetic

The minimal arithmetic we need is the usual arithmetic without the induction postulate. Any restricted system of axioms will do. Robinson's theory $R =< 0, S, +, \cdot >$ (as in Nelson [Nelson]) can serve as our basic arithmetic with the axioms

1) $Sx \neq 0$
2) $Sx = Sy \to x = y$
3) $x + 0 = x$
4) $x + Sy = S(x + y)$
5) $x \cdot 0 = 0$
6) $x \cdot Sy = x \cdot y + x$
7) $x \neq 0 \to \exists y Sy = x$

where 7 is replaced by an axiom for the notion of predecessor

7′) $Px = y \leftrightarrow Sy = x \vee \ (x = 0 \wedge y = 0)$.

Associative, distributive and commutative laws are assumed to hold, *i.e*, they could be added here as axioms. E. Nelson has shown that R (rather, a variant Q) is self-consistent, and we take it as our departure point. We extend R to a Kroneckerian general arithmetic or arithmetic of polynomials (forms) with limited exponentiation and without the infinite expansions of formal power series. Exponentiation when introduced will always "become" bounded in the sense that total exponentiation has a relative sense, *i.e.*, within the combinatorial world 2^n, once n has been found, computed or constructed; 2^n must be such as to allow for descent. Rather than an induction postulate, we add the schema of infinite descent. The schema of infinite descent fulfills two simultaneous functions: it is a (constructive) substitute for the induction postulate, and it introduces order in the sequence of natural numbers through the linear ordering of finite ordinals. Transfinite induction extends this process to well-ordered sets. Thus infinite descent is set-theoretically equivalent to transfinite induction, but infinite descent is independent of any set-theoretic assumption from an arithmetical point of view.

Fermat [Fermat] says of infinite (or indefinite) descent that it is an *άπαγωγὴν είς άδυνατον* or a *reductio ad absurdum.* He applies his method to the problem of right triangles (in rational integers), the areas of which should be squares. If there were such a triangle, Fermat says, there would be another one in smaller integers with the same properties; and if there is a second, there must be a third, a fourth, etc., still smaller and so on *ad infinitum.* But this is impossible, since there is no infinitely descending sequence in the natural numbers. Let us remark first that the *reductio* is harmless here, since it is finitary, and the double negation that ensues is perfectly legitimate, since it does not transcend the realm of the finite. The case is still more evident when Fermat says that he has applied his method not only to negative questions, but also to affirmative ones, such as "Any prime number, which is greater than a multiple of 4 by one, must be composed of two squares." If there were a prime number greater than a multiple of 4 by one, but not composed of squares, there would be a smaller one of that nature and still smaller ones, until 5 is reached, which is the least number having the said property. One must then conclude by indirect proof that the theorem is true. Here, one might find that we have the equivalent of the least number principle, but Fermat employs it in a totally different context, that is, a purely arithmetical context. The essential difference lies in the strictly finite or constructive formulation of Fermat, and, while infinite descent is perfectly acceptable as *reductio ad absurdum*, the least number principle as derived from complete induction obeys the excluded third principle via double negation over an infinite set and is then rejected by intuitionist (Brouwerian) standards. Thus the equivalence of transfinite induction (and complete induction over denumerable ordinals) and infinite descent has only a classical meaning and cannot be constructively justified. No such reprobation affects infinite descent, and I shall try to give some foundational legitimation for infinite descent. Poincaré has insisted that infinite descent (which he calls "*récurrence*") is not equivalent to (formal) complete induction (see [Poincare1906])[3] .

3.1. **The formalization of infinite descent.** Fermat's arithmetic is characterised by the method of infinite descent, and I maintain that from the metamathematical point of view, that is from the proof-theoretic point of view, infinite descent fulfills the role of induction without requiring the notion of infinite set. It is obvious that Fermat did not have the ω point of view in mind. Fermat says that he has invented the method of infinite or indefinite descent, but it is already *in nuce* in Euclid. Take, for example, proposition 31 of book VII of

[3] Poincaré uses infinite descent in his seminal work [Poincare1] on the arithmetic properties of algebraic curves. Poincaré 's phrase for infinite descent is "finite number of hypotheses". One possible implication of the present proof is that a transcendental proof of Fermat's theorem, for example, could be made constructive, which it is not in the present state of affairs: let's call this the *Herbrand's conjecture*, which says that every analytic (transcendental) proof in number theory and in (arithmetic) algebraic geometry has (will have) a constructive (elementary) counterpart. The parenthetical future means only that the constructive proof is (often) *post factum.* See my abstract [Gauthier1983]. Although infinite descent is not used explicitly in Wiles's proof of Fermat's Last Theorem [Wiles], finiteness conditions on the local Noetherian ring for complete intersections, as shown in Falting's simplification, point to a form of infinite ascent that is not effective, but nonetheless finitary. Falting's own proof of Mordell's conjecture is also a finiteness result akin to infinite descent but not yet effective. All this does not mean that the essential use of *reductio ad absurdum* over an infinite set in Wiles's proof can be overcome, at least in the near future.

the *Elements* “Any composite number can be divided by a prime number.” The proof uses a decomposition or reduction which cannot go on indefinitely since any descending sequence of natural numbers is finite. Fermat himself put his method to use in his proof of the impossibility of the Diophantine equation $x^4+y^4=z^2$, which is reduced to $x^4+y^4=z^4$; this is a particular case of Fermat’s last theorem

$$\forall n > 2\ \forall x\ \forall y\ \forall z\ (\, x^n + y^n \neq z^n\,)\ .$$

The principle of infinite descent can be formulated as follows: if the existence of a property for a given n implies the existence of the same property for an arbitrary smaller number, then this property is possessed by still smaller numbers *ad infinitum*, which is impossible since any descending sequence of natural numbers is finite. In order to formalize this principle, we introduce here the quantifier $\mp$, the “effinite” quantifier.

In symbols, we have for the rendering of the intuitive notion of an unbounded or unlimited sequence obtained by “positive” descent

$$\begin{aligned}&\mp x\{([Ax \wedge \exists y(y<x)Ay] \rightarrow \exists y \forall z(z<y)Az) \rightarrow\\ &\qquad\qquad\qquad \exists z(z=0 \vee z=1 \vee \cdots \vee z=n)Az\} \rightarrow \mp x Ax\end{aligned}$$

which means that the sequence is continuing on indefinitely, or rather “effinitely”, starting from the least number, which may be $0, 1$, or n.

This principle of descent does not need a universal quantifier, only an “effinite” quantifier for finite or rather indefinite descent; effinite still means potentially infinite, indefinite sequences or Brouwer’s “infinitely proceeding sequences”. To such effinite sequences, one could assign an “unlimited” natural number, as in Nelson [Nelson], while finite natural numbers are assigned to finite initial segments (sets) of those sequences.

Since infinite descent is impossible — any descending sequence of positive integers must stop at 0, the pre-positional bound of the sequence of natural numbers — one can add the following conclusion to our “negative” descent schema:

$$\mp x\{[Ax \wedge \exists y(y<x)Ay] \rightarrow \exists y \mp z(z<y)Az\} \rightarrow \mp x \neg Ax\ ,$$

which means that the property (or set of properties) postulated for the infinite descent is false for all natural numbers “effinitely” — with $\mp z Az$ instead of $\forall z Az$ in the antecedent.

3.2. **Euclid’s theorem on the infinity of primes.** It remains to show that our formalism can express in a most natural way elementary theorems in number theory. Elementary has the usual meaning of non-transcendental, *i.e.*, the proofs do not employ analytical methods like

L-functions or holomorphic (entire) functions of complex analysis, infinite series, limits and so on; elementary methods use only arithmetical properties of logarithms and finite sums instead of infinite limits, for example. The prime number theorem, which asserts that the ratio of the number of primes in a large set x to $x/\log x$ tends to the limit 1 as x tends to infinity, that is

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1 \ ,$$

has been proven by elementary means (by Selberg and Erdös), long after it had been proven by analytical methods; the same holds for Dirichlet's theorem on the infinity of primes in any arithmetical progression $ax + b$ for a and b relatively prime, *i.e.*, $(a, b) = 1$. Since Euclid's theorem, like the fundamental theorem of arithmetic on the unique representability of integers by a product of primes, needs only constructive methods for its proof, it is the concept of infinity which is at stake here. My contention is again that the concept is dispensable and that one can eliminate it or paraphrase it as Brouwer did by referring to "infinitely proceeding sequences" (or, as I call them, "effinite" sequences). It is really an effinite process which is at work in those proofs; Aristotle said in his *Physics* 203b, that the infinite is that which cannot be crossed ($\acute{\alpha}\delta\iota\varepsilon\zeta\acute{\iota}\tau\eta\tau o\varsigma$) — it may be worth noticing that Gentzen spoke rather of a potential crossing or running through (*ein potentielles Durchlaufen*) of the infinite in his justification of transfinite induction. If the infinite cannot be crossed, is the thought-experiment of a potential crossing in itself justifiable? In any case, the actual wording of Euclid's theorem is: "Prime numbers are more numerous than any definite quantity (of prime numbers)", which is proposition 20 of book IX of the *Elements* (see Davenport [Davenport]). It suffices for the proof to suppose that the sequence

$$p_1, \ \dots \ , p_k$$

enumerates all primes and we then form the number

$$n = p_1 \times p_2 \times \ \dots \ \times p_k + 1$$

which is equivalent to p! + 1; here we use theorem 31 of book VII of the *Elements* which says: "Any composite number is divisible by a prime number." By definition, a composite number is divisible by two factors, one of which must be a prime; if it is not the case, then it must be composite and it can be divided further into a composite number and a prime until it is necessarily found, since there is no infinite descent in integers. Thus, the number n defined above must have a prime divisor and such a prime must differ from all $p_i, i = 1, \ldots, k$, since p_i does not divide n (there is a remainder). In short, Euclid's theorem asserts the existence of an effinite sequence of primes. Let's use σ for that sequence.We know already that there is an effinite sequence of integers which is simply introduced by the rule of effinite induction

$$\begin{array}{ccc} & & [A(a) \in D_n] \\ A(a) \in D_0 & \vdash & A(a) \in D_{n+1} \\ \hline & \vdash \rlap{\,|}\exists x A(x) & \end{array}$$

($A(a) \in D_0$ stands for $A(0)$). In that context, infinite descent becomes the schema

$$\begin{array}{ccc} & & \left[\begin{array}{c} A(a) \in D_{n-1} \\ \vdots \\ A(a) \in D_{n-(n-1)} \end{array}\right] \\ A(a) \in D_n & \vdash & A(a) \in D_{n-n} \\ \hline & \vdash \rlap{\,|}\exists x A(x) & \end{array}$$

Here $\rlap{\,|}\exists x A(x)$ means $\exists \sigma$ and $\rlap{\,|}\exists x \neg A(x)$ means $\neg \exists \sigma$. The last two schemas are analogues of the intelim rules for $\rlap{\,|}\exists$. We can then formalize Euclid's proof in the following way:

Lemma 3.2.1. *Any composite number is divisible by a prime number.* In symbols

$$\rlap{\,|}\exists x(\text{Comp } x \ \rightarrow \ (\exists z \,\text{Prim } \ z \wedge z|x)) \ .$$

Proof. We proceed by *reductio ad absurdum* and we want to prove

$$\rlap{\,|}\exists x(\text{Comp}\, x \ \rightarrow \ \neg(\exists z \,\text{Prim}\, z \wedge z|x)) \ ,$$

which we take as a formula in a domain D_n (which means that x is divisible by $\dfrac{x}{z}$):

$$\begin{array}{c} \neg(\text{Comp}\, x_n \ \rightarrow \ \text{Prim}\, z_n \wedge z_n|x_n) \in D_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \neg(\text{Comp}\, x_{n-n} \ \rightarrow \ \text{Prim}\, z_{n-n} \wedge z_{n-n}|x_{n-n}) \in D_{n-n} \\ \hline \rlap{\,|}\exists x(\text{Comp } x \rightarrow \ (\text{Prim } z \wedge z|x)) \\ \rlap{\,|}\exists x((\text{Comp } x \rightarrow \neg\neg\exists z(\text{Prim}\, z \wedge z|x)) \ . \end{array}$$

□

We have a double negation, since the descent is finite. The conclusion is reached, because it is impossible to go on infinitely or rather effinitely in a descending sequence. We pass now to the theorem on primes which says

Theorem 3.2.1. *Prime numbers are more numerous than any definite quantity (of prime numbers).* In symbols, we simply write:

$$\forall \text{ finite } t \;\; \text{Ɨ}\sigma((\text{Prim } t \wedge \text{ Prim } \sigma) \to t < \sigma)$$

Proof. Note that $\text{Ɨ}\sigma$ can stand either "for σ effinitely" or for "there is an effinite sequence σ". We take as given the following prime:

$$\exists z_n[z_n \leq p_k! + 1 \wedge (\text{Prim } z_n \wedge z_n > p] \in D_n$$

defined above and show that all t's differ from it; we have to show that:

$$\exists z_n \forall t((t > 1 \wedge t \leq p_k!) \to \neg z_n = t).$$

Suppose that $t = p_k!$, and $z_n < p_k! + 1$. The only case of interest is $t = p$; but $z_n > p$, thus $t < z_n$. The fact that t is finite has been gotten by infinite descent and the statement of the theorem is obtained by effinite induction

$$\frac{\begin{array}{c}[((\text{Prim } t \wedge \text{ Prim } \sigma) \to t < \sigma) \in D_n)] \\ ((\text{Prim}t \wedge \text{Prim}\sigma) \to t < \sigma) \in D_0 \vdash ((\text{Prim}t \wedge \text{Prim}\sigma) \to t < \sigma) \in D_{n+1}\end{array}}{\vdash \;\forall t\, \text{Ɨ}\sigma((\text{Prim } t \wedge \text{ Prim } \sigma) \to t < \sigma)}$$

where we have a double introduction, the universal quantifier, since it was understood that t is finite and the effinite quantifier, for σ is not finite, being greater than t. □

Note that this induction is essentially reducible to the induction on natural numbers, *i.e.*, it says simply that to any (prime) natural number there is a greater one. Only the decomposition of composite numbers into primes needs infinite descent. A detailed analysis of the proof would exhibit a logical structure (with intelim rules) that is not more complicated, but more explicit than the mathematical argument. However, the important features of Euclid's proof have been put in the crude light of a constructive logic and shown to rest on radical assumptions about the infinite. No infinite set, no ω, no induction postulate other than infinite descent (or effinite induction) is necessary. Infinite descent is not always effective and is often used in a non-constructive way (see Ireland and Rosen, [Ireland]). But other constructive methods analogous to infinite descent (*e.g.*, logarithmic bounds, approximation procedures) have an effective number-theoretic content, not to speak of the dynamic techniques in real algebraic geometry. I hope to have made it clear enough that only effinite quantification is required if arithmetic is to be given its barest logical expression. Why such a need for a naked ontology of mathematical entities? Not because of the paradoxes, antinomies and other oddities, but for the sake of intelligibility which amounts to fundamental relevance and empirical adequacy, I mean in agreement with mathematical and logical practice.

4. The polynomial translation

There are various ways to translate a formal system into the natural numbers, simple substitution of numerical variables as in Ackermann [Ackermann], translation of logical into arithmetical operations as in Goodstein's equational calculus [Goodstein]. In view of our use of Kronecker's results, we choose the polynomial translation.

We are going to need some facts about the ring of polynomials in one indeterminate in our consistency proof. We pass briefly over the preliminaries (the graded ring of two or more polynomials has the same convolution product, which is our main tool — a Grassmannian product could be used to the same effect).

Polynomials of the form

$$f = f_0 + f_1x + f_2x^2 + \ldots + f_nx^n$$

where the f_i are the coefficients with the indeterminate x build up the subring $K[x]$ of the ring $K[[x]]$ of formal power series. The degree of a polynomial is the degree of the last non-zero coefficient ($k = n$), while the leading coefficient of a polynomial f of degree k is the constant f_k, and f is called monic if its leading coefficient is 1. Thus polynomials are power series having only a finite number of non-zero coefficients. The involution or Cauchy product of two polynomials will play an important role in our translation; we write it

$$f \cdot g = (\sum_m f_mx^m)(\sum_n g_nx^n) = \sum_m \sum_n f_mg_nx^{m+n}.$$

The sum $f + g$ of polynomials f and g is obtained by simply adding corresponding coefficients. Homogeneous polynomials have all their non-zero terms of the same degree and they can be put in the following convenient form

$$a_0x^m + a_1x^{m-1}y + \ldots + a_my^m.$$

We are interested in irreducible (= prime in $K[x]$) polynomials. Every linear polynomial is irreducible. $K[x]$ has the property of unique factorization, and this fact will be crucial in our future developments[4].

[4] Kronecker had proven the unique factorization theorem in the following formulation: "Every integral algebraic form (= polynomial) is representable as a product of irreducible (prime) forms in a unique way" (see [Kronecker6], p.352). Kronecker is interested in the theory of divisibility for forms and considers primitive forms (forms with no common divisor greater than 1), rather than prime polynomials

4.1. **The inner arithmetical model.** When we write, for example,

$$\varphi_M(\exists x Ax)[n+m+\ell\ \ldots] = 1 \text{ iff } \sum A_n \in D_M$$

we can drop the right part and write

$$\varphi_M(\exists x Ax)[n+m+\ell\ \ldots] < n+m+\ell\ \ldots >= 1$$

to mean that we have a complementary mapping (of the intuitionistic spread) $\xi : \mathbb{N} \to \mathbb{N}$, so that we really have a polynomial function which evaluates polynomials by sequences of natural numbers after having defined an evaluation map of formulas into polynomials. The whole process is made possible by substitution alone. Moreover, in category-theoretic language, the indeterminate x is a universal element for the functor $U(\varphi(x)) = n$. If we look at variables of logical formulas as indeterminates, then any number of variables may be reduced to one.

We are going to make an essential use of Kronecker's notion of the content of forms in ([Kronecker6], p.343). A form M is contained in another form M' when the coefficients of the first are convoluted (combined in a Cauchy product) in the coefficients of the second. This idea of a content (*Enthalten-Sein*) of forms can be summarized in the phrase "The content of the product is the product of the contents (of each form)," which can be extracted from Kronecker's paper [Kronecker9] (see also [Kronecker8] and [Kronecker10]). Thus, for a form to be contained or included in another form is simply to be linearly combined with it (to have its powers convoluted with the powers of the second form).

We can adopt here a general principle of substitution-elimination formulated by Kronecker [Kronecker6]. We state the *Substitution Principle*:

1) *Two homogeneous forms (polynomials) F and F^o are equivalent if they have the same coefficients (i.e. content)*;
2) *Forms can be substituted for indeterminates (variables) provided the (linear) substitution is performed with integer coefficients.*

We have immediately the following **Proposition 1** (proposition X in Kronecker):

in his work. The notions of integral domain and unique factorization domain are direct descendants of that theorem.

> *Linear homogeneous forms that are equivalent can be transformed into one another through substitution with integer coefficients.* [5]

We have also the following **Proposition 2** (proposition X^o in Kronecker):

> *Two polynomials F and F^o are equivalent, if they can be transformed into one another.*

These propositions can be considered as lemmas for the unique factorization theorem for forms which Kronecker considered as one of his main results. The substitution procedure is simultaneously an elimination procedure, since indeterminates (*Unbestimmte*) are replaced by integer coefficients. Thus an indefinite (or effinite) supply of variables can be made available to a formal system and then reduced by the substitution-elimination method to an infinitely descending or finite sequence of natural numbers, as will be shown in the following.

The substitution process takes place inside arithmetic, from within the Galois field F^*, *i.e.*, the minimal, natural or ground field of polynomials which is the proper arena of the translation, and indeterminates — Kronecker credits Gauss for the introduction of "indeterminatae" — are the appropriate tools for the mapping of formulas into the natural numbers. The important idea is that indeterminates in Kronecker's sense can be freely adjoined and discharged, and although Kronecker did not always suppose that his forms were homogeneous, we restrict ourselves to homogeneous polynomials.

Definition. The height of a polynomial is the maximum of its lengths (number of its components or terms)—the height of a polynomial is indicated by a lower index.

Let us rewrite the eight clauses of section 2 in the polynomial fashion of the *valuation map* $\hat{\varphi}$.

[5] This can be seen as the precursor of the problem of quantification over empty domains. We know that we have MP

$$\frac{A,\, A \supset B}{B}$$

in an empty domain, provided that A and B have the same free variables (see [Mostowski]). But Kronecker had a more general theory of inclusion or content of forms in mind, and the transformation in question is a composition of contents, an internal constitution of polynomials (forms) where indeterminates are not the usual functional variables.

Clause 1: An atomic formula A can be polynomially translated as

$$\hat{\varphi}(A)[n] = (a_0 x)$$

(where the a_0 part is called the determinate, the x part the indeterminate, and $\hat{\varphi}$ the polynomial *valuation function* or map). Here the coefficient a_0 corresponds to a given natural number (the "valuator"), and 0 indicates that it is the first member of a sequence, x being its associate indeterminate. The polynomial $(a_0 x)$ is thus a combination of the two polynomials $(1, 0, 0, 0 \ldots)$ and $(0, 1, 0, 0 \ldots)$. We identify polynomials by their first coefficients.

Clause 2: The negation of an atomic formula, that is $\neg A$, is translated as

$$\hat{\varphi}(\neg A)[n] = (1 - a_0 x).$$

Clause 3: The conjunction A *and* B is translated as $\hat{\varphi}(A \wedge B)(n \times m) = (a_0 x) \cdot (b_0 x)$ for the product of monomials $(a_0 x)$ and $(b_0 x)$.

Clause 4: The disjunction A *or* B is rendered by $\hat{\varphi}(A \vee B)(n + m) = (a_0 x + b_0 x)$.

Clause 5: Local implication $A \rightarrow B$ is rendered by $\hat{\varphi}(A \rightarrow B)(m^n) = (\bar{a}_0 x + b_0 x)^n$ for $\bar{a}_0 x = 1 - a_0 x$.

Remarks. How is implication to be interpreted polynomially? A developed product of polynomials has the form

$$a \cdot b = (\sum_i a_i x^i)(\sum_j b_j x^j) = \sum_i \sum_j a_i b_j x^{i+j}.$$

For a^b we could simply write $(a+b)^n$ for the binomial coefficients and put

$$(a_0 x + b_0 x)^n = a_0^n x + n a^{n-1} x b x + [n(n-1)/2!] a_2^{n-2} x^2 b_2 x^2 + \ldots + b_0^n x^n$$

in short

$$(a_0 x + b_0 x)^n_{i<n} = \sum_{i+j=n} (i+j) a^i b^j x^n.$$

The rationale for our translation is that we want to express the notion of inclusion of a in b by intertwining or combining their coefficients in a "crossed" product, the sum of which is 2^n which is also the sum of combinations of n different objects taken r at a time

$$\sum_{r=0}^{n} C_n^r.$$

Linear combination of coefficients is of course of central importance in Kronecker's view, and one of his fundamental results is stated: "Any integral function of a variable can be represented as a product of linear factors" [Kronecker6]. In his [Kronecker8], Kronecker refers to Gauss's concept of congruence and shows that a modular system with infinite (indeterminate) elements can be reduced to a system with finite elements. This is clearly the origin of Hilbert's basis theorem [Hilbert] on the finite number of forms in any system of forms with

$$F = A_1F_1 + A_2F_2 + \ldots + A_mF_m$$

for definite forms $F_1, F_2, \ldots, F_m$ of the system and arbitrary forms $A_1, A_2, \ldots, A_m$ with variables (indeterminates) belonging to a given field or domain of rationality (*Rationalitätsbereich*). The fact that exponentiation is not commutative is indicated by the inclusion $a \subset b$. The combinatorial nature of implication is made more explicit in polynomial expansion and is strengthened by the symplectic (interlacing) features of local inclusion of content. We may also define implication, in analogy with the relative complement, as

$$(1^N - a_0x) + b_0x \ ,$$

where 1^N is the arithmetic universe polynomially expanded.

Clause 6: $\hat{\varphi}(\exists xAx)[n + m + \ell \ldots] = \sum_{0\ldots}(a_0x + b_0x + c_0x \ldots)_{i<n}$ where $\sum$ is an iterated sum of numerical instances with a_0 as the first member of the sequence.
Clause 7: $\hat{\varphi}(\forall xAx)[n \times m \times \ell] = \prod_0(a_0xb_0xc_0x)_{i<n}$.
Clause 8: $\hat{\varphi}(\rlap{-}\exists xAx)[n \times m \times \ell \ldots] = \prod_{0\ldots}(a_0xb_0xc_0x \ldots)_n$.

Remarks. The effinite quantifier calls for some clarification. While the classical universal quantifier stands here for finite sets only, the effinite quantifier is meant to apply to infinitely proceeding sequences or effinite sequences. These are not sets and do not have a postpositional bound; we put an n to such a sequence and a 2^n to sequences of such sequences

$$0, 1, 2, \ldots, n, \ldots, 2^n$$

with the understanding that n signifies an arbitrary bound. It should be pointed out that Boole in his *Mathematical Analysis of Logic* (1847) had also a universe (of classes) denoted by 1; negation was interpreted as $1 - x$. The fact that the ring $K[x]$ of polynomials enjoys the unique factorization property exhibited by infinite descent coupled with the proof by infinite descent of the infinity of primes makes essential use, from our point of view, of the effinite quantifier. We then have a combinatorial formulation

$$\prod_{0\ldots}^{n}(a_0xb_0xc_0x\ \ldots\ n_nx^n)$$

for the effinite quantifier; since $n! = 2^n = \prod_{c \leq n} c$, the combinations of n . I call this scheme the absolute or standard scale. Any other scale is an associate scale (of indeterminates) and is reducible by substitution to the standard scale.

As a foundational precept, there is no ω. Any transnatural or trans-arithmetic (transfinite, in Cantorian terminology) ordinal scale, *e.g.*, up to ε_0, is an associate scale and is by definition reducible. It is clear, from a Kroneckerian point of view, that Cantor's transfinite arithmetic becomes a dispensable associate (with an indeterminate pay-off!). The arithmetic universe $\mathbb{N}$ is naturally bounded by 2^n and not by $2^{\aleph_0}$ for infinite power series!

5. The consistency proof

Gentzen's pairing of reduction rules with transfinite inductions in the ϵ_0 segment may be looked at as an associate scale — the scale of ordinal numbers associated with every derivation (see [Gentzen]). The theorem of transfinite induction makes all ordinal numbers "accessible" by running through them in an increasing order; the reduction procedure then allows a descent according to the decreasing order of the ordinal numbers. In the same spirit, Takeuti attempts in [Takeuti] a justification of transfinite induction by invoking the principle: " When all numbers smaller than β are recognized as accessible, the β is itself accessible". But instead of strictly increasing sequences of ordinals $\beta_0 < \beta_1 < \ \ldots\ < \beta_{\varepsilon_0}$, Takeuti introduces directly strictly decreasing sequences $\mu > \ \ldots\ > \mu_1 > \mu_0$ for $\mu = \lim \omega^{\mu_n}$. As I have shown (see [Gauthier1985]), these ordinals are not uniformly recessible (over an immediate predecessor) and cannot count as ordinals in the absolute scale. On the other side, the associate scale can be reduced by a uniform procedure and can be entirely dispensed with, in accordance with Kronecker's general arithmetic.

Ackermann's consistency proof in [Ackermann] also uses a decreasing sequence of ordinal indices in order to prove his finiteness result for global substitutions (*Gesammtersetzungen*) of fundamental types; his m-sequences are uniformly (immediately) recessible, and the reduction procedure ends after a finite number of steps. However, despite the fact that his general recursion procedure is also built in the fashion of infinite descent, Ackermann must refer to the associate (indeterminate) scale of transfinite ordinals, which he then reduces one-to-one to finite ordinals. But the transfinite ordinals are not immediately recessible, and the upper bound estimate 2^α for indices of m-sequences ([Ackermann], p. 193) has only a relative meaning, since it is not independent of some use of transfinite induction, as Ackermann admits.[6] Transfinite induction means always a detour via an infinite set.

Instead of the ordinal hierarchy of set-theoretic ascendency, I use here the arithmetic of irreducible polynomials to show the internal consistency of infinite descent in a direct way.

5.1. **The elimination of logical constants.** The connectives of negation, disjunction, and conjunction are directly eliminable by translation into the arithmetic interpretation, since they can be viewed as the difference, sum, and product of polynomials in a finite number of terms (constants and indeterminates, or variables). We have then

Proposition 5.1.1. *Connectives are eliminable through direct translation in the polynomial interpretation.*

Proof. Rewrite the logical rules as follows for the sequent calculus with Γ the antecedent and Δ the (single) consequent, both consisting of polynomials (monomials); we write for negation

$$\frac{(\Gamma + a_0x)\ \cdot\ \Delta}{\Gamma\ \cdot\ ((1-a_0x)+\Delta)} \qquad \frac{\Gamma\ \cdot\ (a_0x+\Delta)}{(\Gamma+(1-a_0x))\ \cdot\ \Delta}$$

with Δ empty, *i.e.*, "without content" in this case, or multiplication by zero and the understanding that the line has the meaning simply of an ordered sequence of sequents (consisting of sequences of formulas themselves). It should be obvious that we have replaced the sign $\vdash$ by the operation $\cdot$ in order to have polynomial uniformization which does not alter the meaning of the rules.

For disjunction:

$$\frac{\Gamma\ \cdot\ (a_0x+\Delta)}{\Gamma\ \cdot\ ((a_0x+b_0x)+\Delta)} \qquad \frac{\Gamma\ \cdot\ (b_0x+\Delta)}{\Gamma\ \cdot\ ((a_0x+b_0x)+\Delta)}$$

[6] Gödel's own consistency proof of arithmetic (the "Dialectica" interpretation) in [Goedel] makes use of a general recursion schema (of functionals) over all finite types, which is equivalent to complete induction. Herbrand's proof (see [Herbrand]) also requires general recursive functions. It is my contention that the concept of recursion stems from arithmetic reduction procedures originating with Dedekind, but mainly from Kronecker's more algorithmic general arithmetic. Recursion is also "*récurrence*," which in France was another name for infinite descent.

and also

$$\frac{(\Gamma + a_0 x)\ \cdot\ \Delta) \qquad\qquad (\Gamma + b_0 x)\ \cdot\ \Delta}{(\Gamma + (a_0 x + b_0 x))\ \cdot\ \Delta}\ .$$

For conjunction:

$$\frac{(\Gamma + a_0 x)\ \cdot\ \Delta}{(\Gamma + (a_0 x\ \cdot\ b_0 x))\ \cdot\ \Delta} \qquad\qquad \frac{(\Gamma + b_0 x)\ \cdot\ \Delta}{(\Gamma + (a_0 x\ \cdot\ b_0 x))\ \cdot\ \Delta}$$

and also

$$\frac{\Gamma\ \cdot\ (a_0 x + \Delta) \qquad\qquad \Gamma\ \cdot\ (b_0 x + \Delta)}{\Gamma\ \cdot\ ((a_0 x + b_0 x) + \Delta)}\ .$$

□

Remarks. We can treat implication as

$$\frac{\Gamma + a_0\ \cdot\ b_0 + \Delta}{\Gamma\ \cdot\ ((1 - a_0) + b_0) + \Delta} \qquad\qquad \frac{\Gamma\ \cdot\ (a_0 + \Delta_1) \qquad (\Gamma + b_0)\ \cdot\ \Delta_2}{(\Gamma + ((1 - a_0) + b_0))\ \cdot\ \Delta_1 + \Delta_2}$$

where Δ_1 and Δ_2 are two different sequences. There is some artificiality in the symmetrical treatment of intelim rules — the sagittal correspondence — in natural deduction systems (or in the sequent calculus). The symmetry induced by the inversion principle is not derived from the content (of symmetric polynomials), but from a formal duality which is not intrinsic or internal. Negation is generally not involutive — except in finite dual (Boolean) situations — and we could also introduce non-commuting variables in polynomials or in power series, while it is precluded by the double (dual) negation. In intuitionistic logic, this global symmetry is absent, and the more complex situations that are reflected in the logic are an indication of more genetic, less structural features. Internal logic is an analysis of content. Here, logical content = polynomial content. Finally, the detachment or elimination rule is equivalent to *modus ponens*, and the polynomial translation should make manifest the content of the sequential character of inference. Gentzen's linear logic — Gentzen used the phrase *lineares Räsonieren* — is by itself a phenomenon of polynomial content.

The existential quantifier and the universal quantifier over finite sets interpreted as iterated (finite) sum and iterated (finite) product are also directly eliminable. We have

Proposition 5.1.2. *The existential and universal quantifiers are eliminable through direct translation in the polynomial interpretation.*

Proof. The universal quantifier can be rendered by

$$\frac{\Gamma\ \cdot\ (a_0 x + \Delta)}{\Gamma\ \cdot\ (\prod_i (a_i x^i) + \Delta)}\ (*) \qquad\qquad \frac{(\Gamma + a x)\ \cdot\ \Delta}{(\Gamma + \prod_n (a_n x^n))\ \cdot\ \Delta}\ (**)\ ,$$

where $(*)$ means that x is an indeterminate not appearing in Γ and $(**)$ means that ax is an arbitrary term in the polynomial.

The existential quantifier is translated as

$$\frac{\Gamma \ \cdot \ (ax + \Delta)}{\Gamma \ \cdot \ (\sum_n (a_n x^n) + \Delta)} \, (**) \qquad\qquad \frac{(\Gamma + a_0 x) \ \cdot \ \Delta}{(\Gamma + \sum_i (a_i x^i)) \ \cdot \ \Delta} \, (*) \ .$$

□

Remarks. The terms $a_i x^i$ are arbitrary. Since we deal with polynomials (with integer coefficients), the existence property for the existential quantifier is immediately guaranteed, and since the (classical) universal quantifier is limited to finite domains, its scope is always well-defined.

5.2. **The elimination of implication.** We want to arithmetize (local) implication. We put $1 - a = \bar{a}$ for local negation. We have $(\bar{a}_0 x + b_0 x)^n$ and we want to exhaust the content of implication – in Gentzenian terms, this would correspond to the exhibition of subformulas (the subformula property). We just expand the binomial by decreasing powers

$$(\bar{a}_0 x + b_0 x)^n = \bar{a}_0^n x + n\bar{a}^{n-1} x b_0 x + [n(n-1)/2!]\bar{a}^{n-2} x b^2 x + \ldots + b_0^n x$$

where the companion indeterminate x shares the same power expansion. By an easy calculation (on homogeneous polynomials that are symmetric, *i.e.*, with a symmetric function $f(x,y) = f(y,x)$ of the coefficients)

$$(\bar{a}_0 x + b_0 x)^n = \bar{a}_0^n x + \sum_{k=1}^{n-1} (n-1/k-1)\bar{a}_0^{k-1} x + (n-1/k)\bar{a}_0^k x b_0^{n-k} x + b_0^n x$$

$$= \sum_{k=1}^{n} (n/k-1)\bar{a}_0^k x b_0^{n-k} x + \sum_{k=0}^{n-1} (n-1/k)\bar{a}_0^k x b_0^{n-k} x$$

$$= \sum_{k=0}^{n-1} (n-1/k)\bar{a}_0^{k+1} x b_0^{n-1-k} x + \sum_{k=0}^{n-1} (n-1/k)\bar{a}_0^k x b_0^{n-k} x$$

$$= \bar{a}_0 \sum_{k=0}^{n-1} (n-1/k)(\bar{a}_0 - 1)^k b_0^{n-1-k} x + \sum_{k=0}^{n-1} (n-1/k))\bar{a}_0^k x (b_0 - 1)^{n-1-k} x$$

$$= (\bar{a}_1 x + b_1 x)(\bar{a}_1 x + b_1 x - 1)^{n-1}$$

and continuing by descent and omitting the x's, we have

$$(\bar{a}_2 + b_2)(\bar{a}_2 + b_2 - 2)^{n-2}$$

$$\ldots$$

$$(\bar{a}_{n-2} + b_{n-2} + \bar{a}_{n-2} + b_{n-2} - (n-2))^{n-(n-2)}$$

$$(\bar{a}_{n-1}+b_{n-1}+\bar{a}_{n-1}+b_{n-1}-(n-1))^{n-(n-1)}$$
$$(\bar{a}_n+b_n)(\bar{a}_n+b_n)^{n-n}.$$

Applying descent again on $(\bar{a}_n+b_n)$, we obtain

$$(\bar{a}_0+b_0)$$

or, reinstating the x's

$$(\bar{a}_0x+b_0x).$$

Remembering that

$$(\bar{a}x+bx)^n_{k<n}=\sum_{k+m=n}(k+m/k)\bar{a}^kb^mx^n\ ,$$

we have

$$(\bar{a}x+bx)^{k+m=n}_{k<n}=\prod_{k+n=m}(k,m)=2^n\ ,$$

or more explicitly

$$\sum_{i=0}^{m+n}c_1x^{m+n-1}=\bar{a}_0x\cdot b_0x\prod_{i=1}^{m+n}(1+c_ix)=2^n\ ,$$

where the product is over the coefficients (with indeterminates) of convolution of the two polynomials (monomials) a_0 and b_0. We could of course calculate the generalized formula for polynomials

$$(a_0x+b_0x+c_0x+\ldots+k_0x)^n=\sum_{p,q,r,\ldots s}a^pb^qc^r\ \ldots\ k^s$$

in the same manner, but we shall postpone the general case till we come to the effinite quantifier for a unified treatment.

The combinatorial content of the polynomial is expressed by the power set 2^n of the n coefficients of the binomial. I contend that this combinatorial content expresses also the meaning of local (iterated) implication. Convolution exhibits the arithmetic connectedness that serves to render the logical relation of implication. Implication is seen here as a power of polynomials, a^k and b^m with $k<m$ having their powers summed up and expanded in the binomial expansion. Some other formula may be used for the product, but it is essential to the constructive interpretation that the arithmetic universe be bounded by 2^n. One way to make things concrete is to analyse $a\rightarrow b$ in terms of

$$a\rightarrow b=C((2^n-a)+b)$$

where C can stand for combinations or coefficients. The formula is an arithmetical analogue of the topological interpretation of intuitionistic implication.

Theorem 5.2.1. *Local implication $a \to b$ can be eliminated by interpreting it as $(\bar{a} + b)^n$.*

Proof. By the above construction. □

5.2.1. *Elimination of the effinite quantifier?* If we try to translate the effinite quantifier back into our logical rules, we meet with some difficulties. We may try

$$\frac{\Gamma \ \cdot \ ((a_n x^n) + \Delta)}{\Gamma \ \cdot \ (\prod_{i\ldots}(a_i x^i) + \Delta)} \ \ r\,\text{Ɨ}\,(*) \qquad\qquad \frac{(\Gamma + (a_n x^n)) \ \cdot \ \Delta}{\Gamma \ \cdot \ (\prod_{n\ldots}(a_n x^n)) \ \cdot \ \Delta} \ \ l\,\text{Ɨ}\,(**)\ ,$$

but then we haven't made much progress. The point is that (universal) effinite quantification amounts to an existential quantification which says simply "There is an effinite (infinitely proceeding) sequence of prime numbers", for example. It is manifest that the symbol Ɨ is not directly eliminable. Still, the constructive procedure of infinite descent in the cumulative degree structure of polynomials will enable us to discharge the Ɨ symbol in a finite number of steps, much in the same way as the ε symbol is eliminated in Ackermann's proof. But the ε symbol required transfinite induction for its elimination, since it is a transfinite choice function, and the reduction of global substitutions of true formulas for ε-formulas had to depend on the (transfinite) ordinal hierarchy of the second number class, as in Gentzen's proof.

By replacing the rank of a formula by the degree of the corresponding polynomial, we obtain a reduction by unique factorization, that is a finiteness result for arithmetic with infinite descent.

5.3. **Divisibility.** The method of descent we have used in [Gauthier1989] and which is most common could also be called the method of decomposition, as Weil has called it.[7] The decomposition process necessarily stops, and this form of the descent is the one most commonly used for the positive solutions of Diophantine equations. After Fermat, Legendre used the method, and it is the way it is used by most contemporary authors from Mordell and Weil on.[8] Local decomposition of forms in a descent corresponds to a division process. Kronecker has outlined in [Kronecker6] the most general setting for the decomposition of polynomial content. His notion of inclusion or content is expressed in terms

[7] Cf. A. Weil [Weil2].

[8] Mordell [Mordell] says that you start with an arbitrary n — an arbitrary choice made once and for all — and descend finitely. Hasse's principle of local solvability implying global solvability for quadratic forms relies on the same principle and is related to Legendre's "positive" infinite descent for the equation $ax^2 + by^2 = cz^2$. Cf. [Davenport].

of the convolution product. The general form of the convolution product of two polynomials (forms) encloses or contains higher-order forms and the substitution-elimination method enables one to remain within the confines of integral forms. The product of forms

$$\sum_{h=0}^{m} M_h U_h \ \cdot \ \sum_{i=1}^{m+1} M_{m+i} U_{m+1}$$

satisfies an algebraic equation of order r which defines a form containing the product of forms

$$\prod_{h=1}^{r} M_k V_{hk}.$$

Hence, the notions of inclusion and of equivalence (reciprocal inclusion) of forms are valid generally, *i.e.*, for both forms and divisors.[9] Factor decomposition — which we may call devolution — is a descending technique perfectly similar to the division algorithm for integers or the Euclidean algorithm for polynomials. The notion of greatest common divisor of a finite set of elements is an equivalence class of polynomials, and Kronecker's main result is as stated above.[10]

Every integral algebraic form is canonically representable as a product of irreducible (prime) forms. For this unique decomposition (devolution) of polynomials, descent is used to arrive at irreducible polynomials, much in the same way as in Euclid's proof of the divisibility of composite numbers by primes. Take a polynomial

$$f(x) = a_0 x^n + b_1 x^{n-1} + \ldots + b_n$$

of degree n. Suppose that n is not prime, then it must be divisible by two factors i and j one of which, say j, must be prime; if not, j must be divisible by two factors, h and g, one of which, say g, must be prime; if not, we go on in that process, until we reach an a which is necessarily prime, since there is no infinite descent, and we must stop at 1, that is, linear (and irreducible) polynomials. Formally,

$$\text{Ɨ}x\,\{[Ax \wedge \exists y\,(y < x)Ay] \rightarrow \exists y \text{Ɨ}z\,(z < y)Az\} \rightarrow \text{Ɨ}x \neg Ax.$$

By *reductio ad absurdum*, there are irreducible polynomials. Now the fact (Gauss's lemma) that the product of two primitive polynomials (with 1 as the greatest common divisor of their respective coefficients)

[9] My emphasis is different from Edwards's [Edwards], who has chosen to look at divisor theory rather than the theory of forms which is, in my view, the encompassing theory.

[10] See Kronecker [Kronecker6]. Edwards [Edwards] rightly says that Dedekind's Prague theorem — a generalization of Gauss's lemma to the algebraic case — is but a consequence of Kronecker's result.

is primitive can also be had with infinite descent and *reductio ad absurdum.* This fact combined with the fact that there is unique decomposition into irreducible (= prime) polynomials, we obtain unique prime factorization. Kronecker's version of unique decomposition rests on the formula quoted above

$$\prod_{h=1}^{r} M_k V_{hk}.$$

and

$$\prod_{i=j+k} c_i = \sum_{j+k=i} a_j b_k$$

with $j = (0, \ldots, m)$ and $k = (0, \ldots, n)$. We shall read it in the form (remembering that $a^{b-1} \equiv 1(\mod p)$ from a divisibility point of view)

$$\prod_{i=1}^{m+n} (1 + c_i x_i) = \sum_{i=0}^{m+n} (c_i x^{m+n-1}) = \sum_{m+n=1} (a_m b_n)$$

to prove the eliminability of the effinite quantifier. The procedure is quite similar to the process of elimination of implication which now appears as a decomposition of content — the notion of inclusion (*Enthalten-Sein*) which has been translated by "content." With the elimination of the effinite quantifier by infinite descent, we shall be done.

5.4. **The elimination of the effinite quantifier through infinite descent.** There is an intimate connection between implication as inclusion (filling a content) and effinite quantification as an iterated product. We have introduced the effinite quantifier in the form

$$\varphi_M(\exists\!\!\!| x A x)[n \times m \times \ell \ \ldots] < n \times m \times \ell \ \ldots >= 1 \ ,$$

and this can be translated in sequents

$$\frac{\Gamma \ \cdot \ ((a_n x^n) + \Delta)}{\Gamma \ \cdot \ (\prod_{i\ldots}(a_i x^i) + \Delta)} \, r \exists\!\!\!| \, (*) \qquad\qquad \frac{(\Gamma + (a_n x^n)) \ \cdot \ \Delta}{\Gamma \ \cdot \ (\prod_{n\ldots}(a_n x^n)) \ \cdot \ \Delta} \, l \exists\!\!\!| \, (**) \ .$$

We can see this product as an iterated product

$$\prod \cdots \prod (a_m x^m)(a_n x^n) \ ,$$

which we write as

$$\prod_{i=1}^{m} a_i \left(\prod_{j=1}^{n} \cdots \ a_{m+j} \right) \cdots = \prod_{r=1}^{m+n\ldots} \ = \ \prod_{i=1}^{n+1} a_i = \left(\prod_{i=1}^{n} a_i \right) a_{n+1}$$

$$\vdots$$

$$= \ \prod_{i=1}^{n+m} a_i = \left(\prod_{i=1}^{n} a_i \right) a_{n+1}, \ \ldots \ a_{n+n} \ ,$$

which we calculate by descending. We set

$$\prod_{i=1}^{m+n}(c_i)_n = a_m \cdot b_n \prod_{i=1}^{m+n}(1+c_ix)_1 \cdots (1+c_i)_n \ .$$

The lower index $(1 \ldots n)$ is the height of the polynomial. We take up again our calculations of coefficients. We put $((a_0x)\cdot(b_0x))^n$ to indicate that we have a product of monomials

$$(a_0x \cdot b_0x) = ((a_0x) \cdot (b_0x))$$

$$
\begin{aligned}
&= \begin{bmatrix} a_0^nx + \prod_{i=1}^n \sum_{k=1}^{n-1}(n-1/k-1)_1 a_0^{k-1}x + (n-1/k)_1(a_0^kxb_0^{n-k}x)_1 + b_0^nx_1 \\ \vdots \\ a_0^nx + \prod_{i=1}^n \sum_{k=1}^{n-1}(n-1/k-1)_n a_0^{k-1}x + (n-1/k)_n(a_0^kxb_0^{n-k}x)_n + b_0^nx_n \end{bmatrix} \\
&= \begin{bmatrix} \prod_{i=1}^{n-1}(\sum_{k=1}^{n})(n/k-1)_1(a_0^kxb_0^{n-k}x)_1 + \sum_{k=0}^{n-1}(n-1/k-1)_1(a_0^kxb_0^{n-k}x)_1 \\ \vdots \\ \prod_{i=1}^{n-1}(\sum_{k=1}^{n})(n/k-1)_n(a_0^kxb_0^{n-k}x)_n + \sum_{k=0}^{n-1}(n-1/k-1)_n(a_0^kxb_0^{n-k}x)_n \end{bmatrix} \\
&= \begin{bmatrix} \prod_{i=1}^{n}(\sum_{k=0}^{n-1})(n-1/k)_1(a_0^{k+1}xb_0^{n-1-k}x)_1 + \sum_{k=0}^{n-1}(n-1/k)_1(a_0^kxb_0^{n-k}x)_1 \\ \vdots \\ \prod^{n}(\sum_{k=0}^{n-1})(n-1/k)_n(a_0^{k+1}xb_0^{n-1-k}x)_n + \sum_{k=0}^{n-1}(n-1/k)_n(a_0^kxb_0^{n-k}x)_n \end{bmatrix} \\
&= \begin{bmatrix} a_n \prod_{i=1}^{n} \left[\sum_{k=0}^{n-1}(n-1/k)_1((a_0-1)^kx)_1(b^{n-1-k}x)_1 \right. \\ \left. \qquad + b_n \sum_{k=0}^{n-1}(n-1/k)_1(a_0^kx)_1((b_0-1)^{n-1-k}x)_1 \right] \\ \vdots \\ a_n \prod_{i=1}^{n} \left[\sum_{k=0}^{n-1}(n-1/k)_n((a_0-1)^kx)_n(b^{n-1-k}x)_n \right. \\ \left. \qquad + b_n \sum_{k=0}^{n-1}(n-1/k)_n(a_0^kx)_n((b_0-1)^{n-1-k}x)_n \right] \end{bmatrix} \\
&= (a_1x+b_1)_1(a_1x+b_1x-1)_1^{n-1} \\
&\cdots \\
&= (a_1x+b_1)_n(a_1x+b_1x-1)_n^{n-1} \ ,
\end{aligned}
$$

and continuing by descent, we have (again omitting the x's)

$$= \begin{bmatrix} (a_2+b_2)_1(a_2+b_2-2)_1^{n-2} \\ \vdots \\ (a_2+b_2)_n(a_2+b_2-2)_n^{n-2} \end{bmatrix}$$

$\dots$

$$= \begin{bmatrix} (a_{n-2}+b_{n-2})_1(a_{n-2}+b_{n-2}-n-2)_1^{n-(n-2)} \\ \vdots \\ (a_{n-2}+b_{n-2})_n(a_{n-2}+b_{n-2}-n-2)_n^{n-(n-2)} \end{bmatrix}$$

$\dots$

$$= \begin{bmatrix} (a_{n-1}+b_{n-1})_1(a_{n-1}+b_{n-1}-n-1)_1^{n-(n-1)} \\ \vdots \\ (a_{n-1}+b_{n-1})_n(a_{n-1}+b_{n-1}-n-1)_n^{n-(n-1)} \end{bmatrix}$$

$\dots$

$$= \begin{bmatrix} (a_n+b_n)_1(a_n+b_n)_1^{n-n} \\ \vdots \\ (a_n+b_n)_n(a_n+b_n)_n^{n-n} \end{bmatrix} ,$$

which is

$$= \begin{bmatrix} (a_0+b_0)_1 \\ \vdots \\ (a_0+b_0)_n \end{bmatrix} ,$$

which is just $(a_0 \cdot b_0) = \prod_0^n (a_0+b_0)$. □
We can also calculate the generalized formula

$$(a_0x \cdot b_0x \cdot c_0x \cdot \dots \cdot g_0x)^n = \prod_{abc\dots g} \sum_{pqr\dots s} a^p b^q c^r \dots g^s$$

in the same manner by simultaneous descent
$(a_0x \cdot b_0x \cdot c_0x \cdot \dots \cdot g_0x)^n$

$$= \left[\begin{array}{l} a_0^n x + \displaystyle\prod_{i=1}^{n}\sum_{k=1}^{n-1}(n-1/k-1)_1 a_0^{k-1}x + (n-1/k)_1(a_0^k x \,\cdot\, b_0^{n-k}x)_1 \\ \quad + (b_0^n x)_1 + (n-1/k)_1((a_0^k x \,\cdot\, c_0^{n-k}x)_1 + (c_0^n x)_1) + \,\dots \\ \quad + (n-1/k)_1((a_0^k x \,\cdot\, g_0^{n-k}x)_1 + (g_0^n x)_1) + \\ \quad + (b_0^n x \,\cdot\, c_0^n x)_1 \\ \quad \vdots \\ \quad + (c_0^n x \,\cdot\, g_0^n x)_1 \\ \quad \vdots \\ \quad + (b_0^n x \,\cdot\, g_0^n x)_1 \end{array}\right]$$

(Add up to the height $n-1$ for the product.)

$$= \left[\begin{array}{l} = \displaystyle\prod_{i=1}^{n-1}\left(\sum_{k=1}^{n}\right)(n/k-1)_1(a_0^k x b_0^{n-k}x)_1 \\ + \displaystyle\sum_{k=0}^{n-1}(n-1/k)_1(a_0^k x b_0^{n-k}x)_1 \dots \\ + \displaystyle\sum_{k=0}^{n-1}(n-1/k)_1((a_0^k x c_0^{n-k}x)_1 + (c_0^n x)_1) + \dots \\ + \displaystyle\sum_{k=0}^{n-1}(n-1/k)_1((a_0^k x g_0^{n-k}x)_1 + (g_0^n x)_1) + \dots \\ + \displaystyle\sum_{k=0}^{n-1}(n-1/k)_1(b_0^k x c_0^n x)_1 \dots \\ \vdots \\ + \displaystyle\sum_{k=0}^{n-1}(n-1/k)_1(c_0^n x \cdot \dots \cdot g_0^n)_1 \dots \\ \vdots \\ + \displaystyle\sum_{k=0}^{n-1}(n-1/k)_1(b_0^n x \cdot \dots \cdot g_0^n)_1 \end{array}\right]$$

(Add up to the height $n-1$ for the sum.)

$$= \left[\begin{array}{l} \displaystyle\prod_{i=1}^{n}(\sum_{k=0}^{n-1})(n-1/k)_1(a_0^{k+1}b_0^{n-1-k}x)_1 \\ \displaystyle\qquad +\sum_{k=0}^{n-1}(n-1/k)_1(a_0^k b_0^{n-k}x)_1 \\ \qquad \vdots \\ \displaystyle\qquad +\sum_{k=0}^{n-1}(n-1/k)_1+(b_0^k g_0^{n-k}x)_1 \end{array}\right]$$

(Add up to the height n for $p+q+r+s=n$.)

$$= \left[\begin{array}{l} \displaystyle a_n\prod_{i=1}^{n}\Bigg[\sum_{k=0}^{n-1}(n-1/k)_1((a_0-1)^k x)_1(b^{n-1-k}x)_1 \\ \displaystyle\qquad +b_n\sum_{k=0}^{n-1}(n-1/k)_1(a_0^k x)_1((b_0-1)^{n-1-k}x)_n\Bigg] \\ \displaystyle\qquad +c_n\sum_{k=0}^{n-1}(n-1/k)_1(b_0^k x)_1((c_0-1)^{n-1-k}x)_n \\ \qquad \vdots \\ \displaystyle\qquad g_n\sum_{k=0}^{n-1}(n-1/k)_1(c_0^k x)_1((g_0-1)^{n-1-k}x)_n \end{array}\right]$$

$$= \left[\begin{array}{l} (a_1x+b_1x)_1(a_1x+b_1x-1)_1(a_1x+c_1x-1)\ \ldots \\ (a_1x+g_1x-1)_1^{n-1} \end{array}\right]$$

$$\ldots$$

$$= \left[\begin{array}{l} (a_1x+b_1x)_n(a_1x+b_1x-1)_n(a_1x+c_1x-1)_n\ \ldots \\ (a_1x+g_1x-1)_n^{n-1} \end{array}\right] .$$

The descent is then effected simultaneously on the degree and the height of the polynomial and gives

$$(a_0\cdot b_0\cdot c_0\cdot\ldots\cdot g_0)=\prod_0^n(a_0+b_0+c_0+\ldots+g_0)\ .$$

Not having at our disposal the analytical tools of power series (with the notions of infinite series and limits), we can always call a computer for help in particular cases (which is not a case in question here), since we have the benefit of a finite calculation, not available in an ideal transarithmetical world.

We have extracted the content of the product (of the contents of each polynomial) by infinite descent. In so doing, we have also eliminated the logical content of the effinite quantifier: the effinite quantifier appears then as a long chain of implications (inclusions), any implication being itself a singular inclusion (or content).

Infinite descent for reducible polynomials terminates at 1 or 0; if it terminates at 1 (the degree 1), we have the linear irreducible polynomials, while constant polynomials have degree 0, then $1 \neq 0$; if the descent terminates at 0, the zero polynomial has no degree (denoted by $-\infty$). Then $1 \neq 0$ or $0 \neq -\infty$. In other terms,

$$\frac{}{\vdash A, \neg A}\ ,$$

which is

$$\frac{}{\vdash A + (1 - A)}\ ,$$

that is, $1 + (1 - 1) \neq 0$. Thus, consistency is proven, that is, $\neg(0 = 1)$. □

6. Concluding Remarks

We have shown that the system FA of Fermat's arithmetic is a consistent extension of R. Robinson's arithmetic. Self-consistency of arithmetic with infinite descent has been obtained by internal, that is, elementary or constructive means. The polynomial arithmetic we have used is equivalent to what Kronecker calls his "general arithmetic", the arithmetic of forms (polynomials) with indeterminates (algebraic quantities or abstract objects).[11] No detour via an infinite set (of natural numbers) is needed in the proof of internal consistency, nor is the extended induction on transfinite ordinals necessary.[12] In other words, arithmetic with infinite descent is self-contained, *selbstenthaltend*, as Kronecker would probably have said. Note that this does not entail completeness, since we want our arithmetic to be open-ended — of course, "relative" completeness ensues for fragments of arithmetic.

Transfinite arithmetic is but an associate (projective) scale (of algebraic quantities) immediately reducible to the absolute scale; in particular the ε_0 scale is reduced by taking Cantor's normal form theorem as the ordinal polynomial with finite coefficients c_i

$$\xi = \omega^\alpha c + \omega_1^\alpha c_1 + \ldots + \omega_n^\alpha c_n$$

for the transfinite hierarchy up to ε_0. Indeterminates, sometimes called transcendentals or infinites (see Weil [Weil2]), are merely symbols for

[11] S. Lang [Lang] says that "analysis becomes number theory at infinity." Here, "at infinity" means points at infinity or archimedean places for hermitian forms or divisors in the intersection theory of arithmetic surfaces. But the point at infinity can vanish! A nice illustration of this is the recent arithmetization of the Riemann-Roch theorem by Gillet and Soulé, where the calculus on an arithmetic variety is independent of the choice of any hermitian metric (*i.e.*, the point at infinity). Diophantine approximation (Vojta and others) is also responsible for the pushing away of the point at infinity (= analysis). This is one sign, among many others, of the arithmetization of algebraic geometry, a century after Kronecker. One needs only to remember that elliptic curves are cubic polynomials (with at least one rational point). The Taniyama-Weil conjecture, which says "every elliptic curve can be parametrized by elliptic modular forms," implies that quadratic polynomials (among them, Diophantine equations, like Fermat's last theorem) are exceptional among all polynomials — some of them have no remainder or residue, *i.e.*, they generate squares and can be shown to be *independent* from all other higher-degree polynomials. For the semistable (square-free) case, see Wiles [Wiles]. The Taniyama-Shimura-Weil conjecture is not thereby put to rest, nor the general Fermat equation

$$x^p + y^q = z^r \ ,$$

which could require still decades of work for a solution according to Henri Darmon of McGill University.

[12] Fragments of Peano arithmetic have their consistency defined from above, that is from a transfinitely consistent PA in a regressive manner, such that the consistency of a finite fragment depends on the consistency of a larger fragment. For a recent survey of the traditional (set-theoretic) point of view in arithmetic, see [Hajek].

quantities that are eliminated through substitution in the general arithmetical calculus, following Kronecker's programme. Recursive functions, primitive and general (with the symbol μ), are also readily translatable in the general calculus as polynomial functions and polynomials equations, the recursion equations and the μ-operation having their natural formulation in infinite descent (see Ackermann [Ackermann]).

Infinite descent is obviously finite and constructive, although not always effective, as we have repeatedly said. Upper bounds are defined in principle, but in practice they are not always available, and an arbitrary n in the arithmetical degree structure serves as a preliminary existence theorem (cf. Hilbert and E. Noether for the computation of invariants and finite bases for polynomials[13]). Finite existence theorems are *a priori* and can be looked at as invitations for effective proofs. The recent history of algebraic geometry is an eloquent example.

What about logic? The faithfulness of the polynomial translation is summarized in the arithmetical content (which is not set-theoretic), and its justification is achieved by infinite descent. An "arithmetical logic" is probably what Hilbert intended in his early attempts at the consistency problem, the combinatorial foundations of logic and arithmetic. The possibility of such an arithmetical logic, the polynomial interpretation, is hinted at and the finitary character of infinite descent is stressed in Kreisel [Kreisel]. The ambivalent ontological commitment to Cantor's paradise had some consequence for Hilbert's programme for the restoration of classical analysis via set theory and (traditional) logic, while Gödel's transfinite point of view made room for an abstract interpretation of concrete mathematical objects. The symbolic manipulation of identities or equalities in a substitutional calculus in which variables play the role of indeterminates in an infinite (or indefinite) domain — ultimately reducible to a single x — does not have any transcendent meaning, as abstract modern algebra, set theory, model theory and classical logic would have us believe. Logicians and philosophers have taken too seriously Frege's credo in numbers as concepts or Russell's disregard for actual mathematical practice, and they have not taken notice that mathematics most of the time is done with concepts

[13] As expected, E. Noether's proofs are by infinite descent using a splitting process (*Faltungsprozess*) for split extensions that can be reduced to fundamental splittings (*Grundfaltungen*) by descent — the splitting or minimal field. See [Noether1908] and [Noether1911] where Study's symbolic method of polynomial identities is put to use in the reduction of higher-order forms. It is interesting to note that modern algebra has developed (since Emmy Noether and with her) in a less and less constructive fashion while modern number theory and arithmetic geometry are more and more constructive.

that work (or do the work) on themes and motives in their proper arena and with the appropriate machinery. A calculus without the "good" or "right" concepts is useless. The equivalence between arithmetical logic and polynomial arithmetic does not involve any circularity, only a constructive interpretation of what logic is. In view of Gödel's *Dialectica* interpretation, one could wonder if logic is concrete or abstract, since it is the meaning of the concept which is at stake here. Gödel says — thinking probably of Gentzen — that the notion of accessibility (*Erreichbarkeit*) is an abstract concept which involves a kind of reflection on finite constructions. The notion of functional of finite simple type over the integers is such a concept. Gödel shows how to eliminate logic (implication and the quantifiers) by using a recursive functional

$$F' = \forall x \exists y A[x, y, z]$$

where y and z are finite sequences of variables of arbitrary type and A is a quantifier-free expression with the variables x, y, z. In the case of implication,

$$(F \supset G)' = \forall y,\ w\ \ \exists V,\ Z[\ A(y, Z(y, w), x) \supset B(V(y), w, u)\ ]\ ,$$

formulas are simply identified with (two) functionals (with their proper variables) which coordinate (*zuordnen*) the consequent with the antecedent. I claim that the convolution product achieves the aim (of the computational extraction of the content) of implication in a direct fashion. Here one would have for the example given by Gödel :

$$\exists x A x \supset \exists y B y = \sum_{0}^{n} \Big(\sum \bar{a}_0 x + \sum b_0 x \Big)^n$$

and

$$\forall x A x \supset \forall y B y = \prod_{0}^{n} \Big(\prod \bar{a}_0 x \ \cdot\ \prod b_0 x \Big)^n .$$

The formal content of forms (polynomials) in Kronecker's sense of entailment or inclusion *Enthalten-Sein* seems to call for such an interpretation by adjunction of indeterminates. Whether the calculus of content needs an abstract (intensional) setting is of foundational import. There is no doubt that the requirement of constructivity is satisfied, while the requirement of finiteness might be relaxed (with the effinite quantifier and infinite descent?). In any case, those requirements were the motivation for Gödel's extension of the finitist point of view in order to prove the consistency of Peano's arithmetic. In the case of FK or Fermat-Kronecker arithmetic, we have seen that the requirements are met in a most natural or purely internal way. Hilbert's consistency programme is vindicated. The embedding of arithmetic into a larger theory, the "general arithmetic" of polynomials with indeterminates in which logic is translated, allows for a consistency proof downwards, from complete (and transfinite) induction to infinite descent, and backwards, from Hilbert to Kronecker.

References

[Ackermann] Ackermann, W., "Zur Widerspruchsfreiheit der reinen Zahlentheorie," *Math. Ann*, 117 (1940), 162-194.

[Buss] Buss, S.R., *Bounded Arithmetic*, Napoli: Bibliopolis, 1986.

[Davenport] Davenport, H., *The Higher Arithmetic*, London: Hutchison University Library, 1968.

[Edwards] Edwards, H.M., *Divisor Theory*, Basel: Birkhaüser, 1989.

[Fermat] Fermat, P. de, *Oeuvres*, 3 vols, Paris: Gauthier-Villars, 1891, 1894, 1896. Quotations are from volume II.

[Gauthier1977] Gauthier, Y., "Intuitionistic Logic and Local Mathematical Theories," *Zeit. für math. Logik u. Grund. Math.*, 23 (1977), no. 5, 411-414.

[Gauthier1983] Gauthier, Y., "Le constructivisme de Herbrand" (Abstract), *Journal of Symbolic Logic*, 48 (1983), 1230.

[Gauthier1985] Gauthier, Y., "A Theory of Local Negation. The Model and some Applications," *Archiv für mathematische Logik und Grundlagenforschung*, 25 (1985), no. 3-4, 127-143.

[Gauthier1989] Gauthier, Y., "Finite Arithmetic with Infinite Descent," *Dialectica*, 43 (1989), no. 4, 329-337.

[Gauthier1994] Gauthier, Y., "Hilbert and the Internal Logic of Mathematics," *Synthese*, 101 (1994), no. 1, 1-14.

[Gentzen] Gentzen, G., *Collected Papers*, ed. by M. E. Szabo, Amsterdam: North-Holland, 1969.

[Girard] Girard, J.-Y., *Proof Theory and Logical Complexity*, Napoli: Bibliopolis, 1987.

[Goedel] Gödel, K., "Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes," *Dialectica* , 12 (1958), 280-287.

[Goodstein] Goodstein, R.L., *Constructive Formalism*, Leicester: University College, 1951.

[Hajek] Hajek, P. et Pudlak, P., *The Metamathematics of First-Order Arithmetic*, Berlin: Springer-Verlag, 1992.

[Herbrand] Herbrand, J., *Logical Writings*, ed. by W. Goldfarb, Cambridge, Mass.: Harvard University Press, 1971.

[Hilbert] Hilbert, D., "Über die Theorie der algebraischen Formen," *Gesammelte Abhandlungen*, vol. III, New York: Chelsea, (1965), 199-257.

[Ireland] Ireland, K. and Rosen, M., *A Classical Introduction to Modern Number Theory*, Berlin: Springer-Verlag, 1980.

[Kreisel] Kreisel, G. "What have we learnt from Hilbert's second problem?" in *Mathematical Developments arising from Hilbert's problems*, Amer. Math. Soc., Providence, R.I., 1976, 93-130.

[Kronecker] Kronecker, Leopold, *Leopold Kroneckers Werke: Herausgegeben auf Veranlassung der Königlich preussischen Akademie der Wissenschaften*, ed.

by K. Hensel, Leipzig, Berlin: B.G. Teubner, 1895-1931. Five vols. Chelsea, New York, 1968.

[Kronecker6] Kronecker, L., “Grundzüge einer arithmetischen Theorie der algebraischen Grössen,” *Werke* [Kronecker] , vol. III, pp. 245-387.

[Kronecker8] Kronecker, L., “Ein Fundamentalsatz der allgemeinen Arithmetik,” in *Werke* [Kronecker] , vol. III, 209-247.

[Kronecker9] Kronecker, L., “Über einige Anwendungen der Modulsystem auf elementare algebraische Fragen,” in *Werke* [Kronecker] , vol. III, 147-208.

[Kronecker10] Kronecker, L., “Zur Theorie der Formen höerer Stufen,” in *Werke* [Kronecker] , vol. II, 419-424.

[Lang] Lang, S., *Introduction to Arakelov Theory*, New York: Springer-Verlag, 1988.

[Mirimanoff] Mirimanoff, D., “Les antinomies de Russell et de Burali-Forti et le problème fondamental de la théorie des ensembles,” *L'ens. math.*, 19 (1917), 17-52.

[Mordell] Mordell, L.J., “On the rational solutions of the indeterminate equations of the third and fourth degrees,” *Proc. of the Cambridge Philos. Soc.*, 2 (1922), 179.

[Mostowski] Mostowski, A., “On the Rules of Proof in the Pure Functional Calculus of the First Order,” *Journal of Symbolic Logic*, 16 (1951), 107-111.

[Nelson] Nelson, E., *Predicative Arithmetic*, Mathematical Notes 32, Princeton, N.J.: Princeton University Press, 1986.

[Neumann1] Neumann, J.von, “Eine Axiomatisierung der Mengenlehre,” *Collected Works*, vol.I, 24-33, Oxford: Pergamon Press, 1961.

[Neumann2] Neumann, J.von, “Zur Einführung transfiniten Zahlen,” *Collected Works*, vol.I, 24-33, Oxford: Pergamon Pres, 1961.

[Noether1908] Noether, E., “Über die Bildung des Formensystems der ternären biquadratischen Form,” *J. Reine u. Angew. Math.*, 134 (1908), 23-90.

[Noether1911] Noether, E., “Zur Invariantentheorie der Formen von n Variabeln,” *J. Reine u. Angew. Math.*, 139, (1911), 118-154.

[Poincare] Poincaré, H., *Oeuvres*, 11 v., Paris: Gauthier-Villars, 1951.

[Poincare1] Poincaré, H., “Sur les propriétés arithmétiques des courbes algébriques”, *Oeuvres*, [Poincare] , vol.II, 483-550.

[Poincare1906] Poincaré, H., “Les mathématiques et la logique,” *Revue de métaphysique et de morale*, 14 (1906), 17-34 and 294-317.

[Skolem] Skolem, T., *Selected Works in Logic*, ed. by J. E. Fenstad, Oslo: Universitetsforlaget, 1970.

[Takeuti] Takeuti, G., *Proof Theory*, Amsterdam: North-Holland, 1975.

[Weil] Weil, A., *Oeuvres scientifiques, Collected Papers*, 3 vols, New York: Springer-Verlag, 1979.

[Weil1] Weil, A., “Number Theory and Algebraic Geometry,” *Oeuvres scientifiques* [Weil], vol. III, 442-452.

[Weil2] Weil, A., “L'arithmétique sur les courbes algébriques,” *Oeuvres scientifiques* [Weil], vol. I, 11-45.

[Wiles] Wiles, A., “Modular elliptic curves and Fermat's last theorem,” *Ann. of Math.*, 142, (1995), 443-551.

Department of Philosophy, University of Montréal, C.P. 6128 Succ. Centre-Ville, Montréal, Qc. H3C 3S7
E-mail address: gauthiyv@philo.umontreal.ca