The Use of Infinity in Pure Number Theory and Algebra

Yvon Gauthier

Faculty of Arts and Sciences
University of Montreal
Montreal, Canada

Copyright © 2019 Yvon Gauthier. This article is distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract
What is meant here by pure number theory is elementary number theory from Fermat to Kronecker, what I call Fermat-Kronecker arithmetic, that is the method of infinite descent combined with the theory of forms or homogeneous polynomials which extends to algebraic number theory and beyond. I contend that these two motives still shape to some extent the contemporary number-theoretic foundations of arithmetic-algebraic geometry as I emphasize the work of the great French arithmetician André Weil.

Mathematics Subject Classification: 11R04, 11R09, 11S05, 12E05, 12E20, 12E30

Keywords: Elementary number theory, algebraic number theory, infinite descent, Kronecker’s homogeneous polynomials, Weil conjectures, arithmetic geometry

1 Introduction
I want to emphasize in this critical foundational note two central uses of infinities in contemporary number theory, the theory of \( p \)-adic numbers and the notion of infinite prime places in arithmetic geometry. K. Hensel introduced \( p \)-adic integers in his new foundations of the theory of algebraic numbers stating explicitly that his (valuation-theoretic) endeavour was independent of ideal theory (Hensel 1897) while E. Steinitz published his algebraic
theory of fields in the Dedekindian spirit (Steinitz 1910). Dedekind’s ideal theory is the set-theoretic counterpart of Kronecker’s theory of domains of rationality (Rationalitätsbereiche). Finally, André Weil, the founder of modern algebraic geometry has initiated his work on the arithmetic of algebraic curves avoiding ideal theory like Hensel in the line of Kronecker’s general arithmetic (allgemeine Arithmetik). Weil’s foundational viewpoint is alive in contemporary arithmetic geometry up to Grothendieck’s and Langland’s programs while Kronecker is still present in Grothendieck’s notion of scheme as a generalisation of Kronecker’s modular systems Modulsyteme (see Dieudonné 1974, pp. 59-61) and in Langlands’ idea of functoriality or transfer principle from arithmetic information to analytic data in the footsteps of Weil’s cohomology theory. One could even venture to say that Grothendieck’s general motivic program of correspondences between arithmetic, algebra and analysis is inspired by Kronecker’s Jugendtraum – Langland’s program explicitly refers to it (see Gauthier 2013, pp. 59-61). In that connection, Kronecker expresses himself unequivocally in his treatment of complex multiplication – over imaginary quadratic fields – as he says that its object is taken from analysis, i.e. elliptic functions, but the motive is given by algebra and the direction and goal are defined by arithmetic (see Gauthier 2015, p. 63). Hilbert in his famous 1900 list, emphasizes the significance of the 12th problem of his list concerning Kronecker’s proposition on abelian fields over an arbitrary algebraic domain of rationality, which he considers as one of the deepest and far-reaching problems at the internal junction of number theory, algebra and the theory of functions (analysis). It is in that context that I examine the role of infinities in number theory.

2 Hensel’s theory of $p$-adic numbers

In his 1897 paper on a new foundation of the theory of algebraic numbers (Über eine neue Begründung der Theorie der algebraischen Zahlen), Hensel introduces his theory of $p$-adic numbers by emphasizing the analogy between the theory of algebraic functions of one variable and the theory of algebraic numbers following in the footsteps Kronecker’s major work (see Kronecker 1882). Hensel puts down two formulas as the foundations of his theory

\[ f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n = a_0 (x - x_1) \ldots (x - x_n) = 0 \quad (1) \]

and

\[ F(x) = 0 \pmod{p^M} \quad (2) \]

for $M$ the power of prime $p$. His idea is to associate ramification points of an algebraic function to (rational) ramification places of a prime polynomial in a locally finite field. Hensel’s intention was to use infinite power series in
arithmetic while Kronecker insisted that one does not need the full formal power series beyond (homogeneous) polynomials of finite degree. However \( p \)-adic number theory involves infinite degree polynomials in an algebraic number field \( \mathbf{F} \), a finite extension of the rational field \( \mathbb{Q} \). We denote an infinite prime \( p \) as \( p^\infty \). An infinite prime \( p^\infty \) is a \( \mathbb{p} \)-adic valuation over the ring of integers \( \mathbb{Z} \)

\[
v_p : \mathbb{Z} \to \mathbb{N}
\]

defined as

\[
v_p = \max \{ v \in \mathbb{N} : p^v/n \} \text{ if } n \neq 0, \text{ otherwise } \infty \text{ if } n = 0
\]

where \( v \) is the highest exponent for \( p^v \) to divide \( n \) and Hensel lemma comes in to lift \( p \) to any finite power. From a set-theoretic point of view, the set

\[
\{0, p^\infty\}
\]

is a final segment of the well-ordered set of the \( \omega \)'s in Cantor's second number class. Since there is a countably infinite set of infinite primes over \( p^\infty \) and although \( \mathbb{Z}_p \), the ring of prime integers and \( \mathbb{Q}_p \) the field of fractional prime numbers are both uncountable sets, the set \( \mathbb{Z}/p^n\mathbb{Z} \) is countable and must be counted as belonging to Cantor's second class of ordinals up to \( \epsilon_0 \), which itself contains a countably infinite set of primes in the sequence of the \( \omega \)'s. But the final segment \( \{0, p^\infty\} \) is not expressible as an isomorphism type in that sequence since its order type is incomparable or irreducible to any \( n \) and is therefore not representable in Cantor's normal form which has the status of an infinite ordinal polynomial (see Gauthier 2018, Theorem 2). However, Kronecker's ideas extended into Hensel's \( \mathbb{p} \)-adic number theory are in the same arithmetical-algebraic spirit. Steinitz' extension goes a little further...

3 Steinitz' algebraic theory of fields

Steinitz published his *Algebraische Theorie der Körper* (Steinitz 1910) in which he explicitly says that he extends Kronecker's notion of indeterminates into the infinite in order to define the notion of the algebraic closure for any field with **supernatural** numbers as a generalization of the natural numbers in the formal product

\[
\omega = \prod p^{n_p}
\]

over all primes \( p \) with \( n_p = \infty \) for infinite primes or places. Steinitz numbers are alien to \( \mathbb{p} \)-adic numbers, since their absolute value is archimedean while \( \mathbb{p} \)-adic numbers live in complete ultrametric non-archimedean space. Ostrowski's theorem establishes though the equivalence of their absolute values over \( \mathbb{Q} \)

\[
| \cdot |_\infty \leftrightarrow | \cdot |_p,
\]

(7)
but Steinitz’ main point was to extend Kronecker’s domains of rationality (Rationalitätsbereiche), the effect of which was to translate Dedekind’s fields (Körper) into a full set-theoretic framework using the axiom of choice or Zorn’s lemma – Steinitz says axiom of Zermelo – in order to obtain the completion of every field (real numbers, complex numbers, valued fields), thus extending or replacing Kronecker’s indeterminates by what Steinitz calls transcendentals or infinites. One could conclude here that Steinitz achieved a set-theoretic continuation (akin to analytic continuation in complex analysis) of Kronecker’s general arithmetic of forms (homogeneous polynomials). The notion of algebraic closure for an arbitrary algebraic extension $K'$ of a commutative field $K$ implies that any polynomial $\geq 1$ has at least one root in $\mathbb{R}$ or $\mathbb{C}$, as if we had a transfinite version (in any cardinality $\aleph_0$, $2^{\aleph_0}$ or even $2^{2^{\aleph_0}}$) of Gauss’ fundamental existence theorem of algebra. Needless to say that contemporary algebraic geometry in the toposical landscape of Grothendieck’s universes requiring an uncountable (strongly) inaccessible cardinal transcends the territory of the algebraically closed fields and ascends to a Platonic realm of indeterminate ideal entities as if embedded in a set-theoretic meta-universe rejected by Kronecker and finally repudiated by Hilbert (see Gauthier 2013). It is not disputable that Dedekind’s ideal-theoretic enterprise with Steinitz completion has met with a great success in the hands of Hilbert, Emmy Noether, van der Waerden as a main object of abstract algebra, algebraic geometry and also mathematical logic, especially model theory from Tarski to A. Robinson. Still, arithmetic algebraic geometry strives for finiteness results with infinite means that lead ultimately to finite arithmetic. Let us notice, for example, that Arakelov’s theory of Diophantine equations in higher dimensions has made fruitful use of infinite primes not without recourse to the method of descent inspired by A. Weil’s work on isogeny heights active in Falting’s proof of Mordell’s conjecture. However, let us have a closer look at Kronecker’s finitistic theory of forms or modular systems in the background of a large part of contemporary arithmetic theory.

## 4 Kronecker’s theory of algebraic integers

Kronecker’s arithmetic program of algebraic quantities (algebraïsche Grössen) is essentially contained in two papers (Kronecker 1882 and 1883). Since we are dealing with polynomials in the sense of Kronecker, I shall use essentially Kronecker’s notion of the content of polynomials $\text{con}(P_L)$ and $\text{con}(Q_L)$ for which I reconstruct Kronecker’s argument (see Gauthier 2013). Remembering that the content of a polynomial with integer coefficients is condensed in the greatest common divisor of its coefficients, we shall exhaust the content in the canonical decomposition of polynomials where descent is effected to arrive at irreducible polynomials, much in the same way as in Euclid’s proof of the
The use of infinity in pure number theory and algebra

... divisibility of composite numbers by primes. Now the fact (Gauss’s lemma) states that the product of two primitive polynomials (with the g.c.d. of their respective coefficients = 1) is primitive can also be had with infinite descent and *reductio ad absurdum*. From 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 formulas

\[ \prod_{h=1}^{r} M_k U_{hk} \quad (8) \]

and

\[ \prod_{i=j+k} c_i = \sum_{j+k=i} a_j b_k \quad (9) \]

where the \( M \)'s are integral forms, the \( U \)’ indeterminates and the \( c \)'s

\[ j = (0, \ldots, m) \text{ and } k = (0, \ldots, n). \quad (10) \]

as integral coefficients.

We shall read it from a divisibility point of view in the form of

\[ \prod_{i=1}^{m+n} (1 + c_i x_i) = \sum_{i=0}^{m+n} (c_i x^{m+n-1}) = \sum_{m+n+1}^{a_m b_n} \quad (11) \]

Kronecker’s generalization uses the convolution product for polynomials

\[ \sum_h M_h U_h \cdot \sum_i M_{m+1} U^{i-1} = \sum_k M'_k U^k \quad (12) \]

so that the product mentioned above

\[ \prod_h \sum_k M'_k U_{hk} \quad (13) \]

is "contained" in the resulting form and the product can be expressed as

\[ \sum_k M'_k U^k = (M_k M_{m+1})^k + (M_k M_{m+1})^{k-1} + (M_k M_{m+1})^{k-2} + \ldots + (M_k M_{m+1}) \quad (14) \]

in the decreasing order of the rank \( k \) of the polynomial sum. This linear combination obtained by the convolution product and the finite descent of powers shows simply that integral rational forms generate integral algebraic forms, i.e. algebraic integers. One can see this decomposition of forms as a generalization of Gauss’s lemma (*Disquisitiones Arithmeticae*, art. 42) which states (see Edwards 1990, p. 1) :
Let $f$ and $g$ be monic polynomials in one indeterminate with rational coefficients. If the coefficients of $f$ and $g$ are not all integers, then the coefficients of $fg$ cannot all be integers.

Remembering that a simple form of Gauss’s lemma is that the product of two primitive polynomial is primitive and a primitive polynomial being a polynomial having 1 for the g.c.d. of all its coefficients, one sees immediately that Kronecker’s theory of content is a vast generalization of Gauss’s result. As shown above, the Kronecker’s notion of content or inclusion «Enthalten-Sein», that the coefficients of one form can be included in another and mutual inclusion, results in an equivalence relation; a further generalization is afforded by passing to forms of higher order «Stufe» where forms and divisor systems or modular systems coincide.

5 Weil’s arithmetic of finite fields

Already in his doctoral dissertation “L’arithmétique sur les courbes algébriques” (see Weil 1929), Weil adopts the method of infinite descent in the wake of Mordell’s work on finiteness results in the number field $\mathbb{Q}$ inspired by Poincaré’s 1901 pioneering paper on the arithmetical properties of algebraic curves – Poincaré used the expression “a finite number of hypotheses” to define infinite descent –. In that early work, Weil insists that his arithmetical orientation is independent of any ideal theory and Steinitz transcendental or infinites are called infinite systems of points as they are simply discarded to the profit of a finite calculus, the arithmetic of counting points. Faltings’ proof of Mordell’s conjecture on the finite number of rational points for an algebraic curve of genus $\geq 2$ uses also a generalized descent on heights under isogeny a notion developed by Arakelov and Faltings, but originally owed to Weil who in his work on algebraic varieties searched to connect arithmetic, algebra (abelian varieties) and analysis (Riemann surfaces) much in the manner of Kronecker’s Jugendtraum.

In order to emphasize the purely arithmetical side of infinite descent, let me quote Weil (see Weil 1983) on Fermat’s descent. Weil describes infinite descent in terms of contemporary algebraic number theory:

Infinite descent à la Fermat depends ordinarily upon no more than the following simple observation: if the product $\alpha \beta$ of two ordinary integers (resp. two integers in an algebraic number-field) is equal to an $m$-th power, and if the g.c.d. of $\alpha$ and $\alpha$ can take its values only in finit set of integers (resp. of ideals) then both $\alpha$ and $\beta$ are $m$-th powers, up to factors which take their values only in some assignable finite set. For ordinary integers this is obvious; it is
so for algebraic number-fields provided one takes for granted the finiteness of the number of ideal-classes and Dirichlet’s theorem about units. In the case of a quadratic number-field $\mathbb{Q}(\sqrt{N})$ this can be replaced by equivalent statements about binary quadratic forms of discriminant $N$.

(see Weil 1984, pp. 335-336).

The important fact about algebraic number fields is that they are not algebraically closed and the Steinitz’ desideratum with the axiom of choice is totally alien to Kronecker’s domains of rationality as H. Edwards puts it for numerical extensions of a function field $K$:

It is usual in algebraic geometry to consider function fields over an *algebraically closed field* – the field of complex numbers or the field of algebraic numbers rather than over $\mathbb{Q}$ (the field of rational numbers). In the Kroneckerian approach, the transfinite construction of algebraically closed fields is avoided by the simple expedient of adjoining new algebraic numbers to $\mathbb{Q}$ as needed.

(see Edwards 1990, p. 97).

The other major aspect of Weil’s arithmetical spirit is indeed the finite arithmetic of polynomials with integer coefficients and indeterminates of Gaussian and Kroneckerian heritage. In his seminal work “Number of solutions of equations in finite fields” (see Weil 1949) where appear the famous Weil conjectures, there is no place for Steinitz infinites or transcendentals, nor for infinite systems of points. Rather, Weil starts from the last entry of Gauss’ *Tagebuch* on congruences and biquadratic residues. This was the birth place of the generalized Riemann hypothesis according to Weil and it concerns the number of solutions of equations in $\mathbb{Q}(\sqrt{N})$ which is the firm ground of descent, as Weil states in his description of Fermat’s infinite descent. As a matter of fact, Weil begins his paper with (polynomial) equations in the form

$$a_0x_0^n + a_1x_1^{n_1} + \ldots + a_rx_r^{n_r} = b$$  (15)

to

$$a_0x_0^n + \ldots + a_rx_r^n = 0$$  (16)

to end up with the rational function of an alternating product of polynomials with integer coefficients

$$F(X) = \frac{(X^{m+1} - 1)(X^{m+1} - X) \ldots (X^{m+1} - X^m)}{(X^{r+1} - 1)(X^{r+1} - X) \ldots (X^{r+1} - X^r)}$$  (17)

which determines the number of rational points of $F(q)$ in a finite field of $q$ elements. That is the Riemann rational function in a Kroneckerian context.
(see Weil 1949) which Weil emphasizes in (Weil 1950). In that context, Weil (1976) also offers an appraisal of Kronecker’s work on elliptic functions with complex multiplication in (imaginary) quadratic fields \( K = \mathbb{Q}\sqrt{-d} \).

Kronecker makes use of infinite descent when he describes the decomposition procedure of homogeneous polynomials down to irreducible polynomials (see chapter 4. above). For Weil’s conjectures, B. Dwork succeeded in proving that the zeta function on any algebraic set is rational with the help of \( p\)-adic analysis, but S.A. Stepanov gave an elementary proof without the help of \( p\)-adic analysis and finally E. Bombieri still improved on it with a short proof on counting the number of rational points over finite fields. Deligne’s final proof of Weil’s conjectures follows diverse routes, generalized descent and decomposition procedures which are not (yet!) part of elementary or pure number theory, but remain a testimony to Weil’s arithmetic program on finite fields up to the Taniyama-Weil or Taniyama-Shimura-Weil conjecture (including Fermat’s Last Theorem proved by A. Wiles) to which Weil contributed essential conceptual developments or evidence as Wiles says (see Wiles 1995), for example the functional equations for Dirichlet’s \( L \)-series (see Weil 1967). The Taniyama-Weil conjecture states that “Every elliptic curve over \( \mathbb{Q} \) is modular” and Weil would not hesitate to trace its arithmetic-geometric ancestry to Kronecker’s work on the arithmetic of elliptic functions (see Weil 1949). A further indication of Kronecker’s influence or program (Weil coined the term), is Weil’s reference in (Weil 1967) to a paper by J.I. Igusa on the Kroneckerian model of fields of elliptic modular curves (Igusa 1959).

6 Concluding remarks. Arithmetical foundations

The internal arithmetic of algebraic quantities which Kronecker called general arithmetic is part and parcel of pure number theory as is Fermat’s infinite or indefinite descent. This Fermat-Kronecker arithmetic is the mathematical historical background of André Weil’s work in number theory and algebraic geometry. One could declare that infinities are banished in elementary number theory, only potential infinity “denumerable at infinity”, as the arithmetician would say, could resist banishment. Constructive mathematics extracts the elementary (non-analytic) content of mathematical statements and theories in order to gain more information. More information means more certainty, as Hilbert would claim in the finitist Kroneckerian viewpoint he finally endorsed after having appropriated many fundamental ideas of Kronecker not without criticizing the opponent to Cantor’s paradise. Hilbert created a metamathematical proof theory by arithmetizing mathematical proofs in formal logical systems in order to uncover what he called “\( \text{das inhaltliche logische Schliessen} \)” or the internal logic of mathematical theories. Hilbert did introduce ideal entities “\( \text{ideale Elemente} \)”, as detours “\( \text{Umwege} \)” to entertain infinites or tran-
The use of infinity in pure number theory and algebra

scendentals as Steinitz dubbed them, but only to eliminate them afterwards by a process of infinite descent (see Gauthier 2015, chap. 3). All this militates for a constructivist standpoint in the foundations of mathematics, particularly in number theory and in contemporary arithmetic geometry with the wealth of finiteness results and for an arithmetical logic as the internal logic of the F-K arithmetic on finite fields with Fermat’s descent and Kronecker’s modular systems. It is in order though to admit that the legacy of the F-K arithmetic with Kronecker’s program from Poincaré, Mordell to Weil, Grothendieck, Deligne, Faltings, Langlands, Scholze, the recent Fields medalist in arithmetic geometry, extends from the finitistic standpoint to an explicit infinitistic perspective opened by Kronecker’s descendents Hensel and his $p$-adic number theory enlarged to $p$-adic analysis (nowadays to $l$-adic and $p$-adic arithmetic geometry) and Steinitz’ algebraic theory of fields, but the original inspiration remains the same insofar as the ultimate goal is finiteness results unreachable in the set-theoretic Cantorian transfinite arithmetic or in the set-theoretic infinite Dedekind-Peano arithmetic. After all, Kronecker did not stop investigating elliptic functions in order to enucleate their algebraic arithmetic core.

A Personal Note. André Weil, in a letter – dated March 23, 1988 from Princeton Institute for Advanced Study – approved of my cogent use of the method of infinite descent in the preprint of my *Dialectica* paper (see Gauthier 1989), but declined any comment on my attempted formalization of the notion, pledging that he was not enough of a logician (*trop peu logicien*). It is well known though that Weil was no friend of mathematical logic, transfinite set theory or category theory. In the Foreword of his *Basic number Theory* (1974), Weil seems to launch an attack in the style of Kronecker vis-a-vis Cantor against useless generalizations of basic results like Riemann - Roch theorem saying that they border on theology – the attack is apparently directed at Grothendieck’s categorical version of the Riemann-Roch theorem –. My book on the arithmetical foundations of logic (see Gauthier 2015) is dedicated to the memory of the great arithmetician André Weil.

References


Received: January 7, 2019; Published: January 29, 2019