A Quadratic Reciprocity Theorem for Arithmetical Logic

Yvon Gauthier

Faculty of Arts and Sciences, University of Montreal
Montreal, Que. Canada

Abstract

I have introduced in (Gauthier 2015, see [6]) an interpretation of a logical calculus in terms of congruent arithmetic for a modular polynomial logic. The motive was to develop a purely syntactical approach to the internal consistency of arithmetic. Such an arithmetic was defined as classical Fermat-Kronecker (F-K) arithmetic, that is the general theory of homogeneous polynomials (forms) with infinite descent as a proof procedure. In particular, I treated logical implication (the conditional) as a congruence relation that is interpreted by infinite descent on the binomial expansion. The objective was to endow theorems and proofs in logic with a numerical content.

Mathematics Subject Classification: 11A15,11R09, 03F03, 03F35

Keywords: Quadratic reciprocity, divisor theory, polynomials, infinite descent

1 Quadratic reciprocity

The history of the theorem in number theory is well known. Euler had proven, using infinite descent, Fermat’s minor theorem in congruent arithmetic:

\[ a^{p-1} \equiv 1 \pmod{p} \]

i.e. if \( p \) is a prime and \( a \) is a prime relative to \( p \), \( a^p \) is divisible by \( p \). This important theorem, despite its name, has been instrumental in the recent
Agrawal-Kayal-Saxena test (see [1]) for primality in polynomial time. Euler went on calculating quadratic residues for congruences, e.g. $x^2 \equiv q \pmod{p}$ – if it has a solution, $q$ is a quadratic residue $\pmod{p}$, if not, it is a quadratic nonresidue – in the form that Legendre codified later (the Legendre symbol):

$$
(p/q) = \begin{cases} 
1, & \text{if } p \text{ is a quadratic residue of } q \\
-1, & \text{if } p \text{ is a quadratic nonresidue of } q \\
0, & \text{if } q \text{ divides } p \text{ exactly (no residue).}
\end{cases}
$$

For distinct odd primes $p$ and $q$, the law of quadratic reciprocity states:

$$
(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}
$$

with an even exponent for $(-1)$, $p$ and $q$ have reciprocal quadratic residues or they don’t. Euler didn’t prove this and Legendre had an incomplete proof till Gauss proved the quadratic reciprocity theorem, the golden theorem (aureum theorema) as he called it, in his 1801 Disquisitiones arithmeticae using infinite descent on indeterminates (indeterminatae) or unknown quantities accompanying integral coefficients in polynomials – for the history of quadratic reciprocity, one can consult (Weil [10]), (Davenport [2]) or (Ireland and Rosen [7]). Kronecker who credited Gauss with the introduction of indeterminates will exploit fully the notion in his general arithmetic (allgemeine Arithmetik) of polynomials. Gauss has provided many proofs of his theorem from his adolescence on and there are now two hundred proofs of the theorem in different clothes, but it has also far-reaching generalizations up to E. Artin’s reciprocity law for global fields in finite field theory where Artin builds on the Kronecker-Weber theorem originally conjectured by Kronecker for finite abelian extensions of $\mathbb{Q}$, the field of rational numbers (Hilbert’s twelfth problem) – for this, see (H. Weyl [11]) for an authoritative work on algebraic number theory in which Weyl privileges Kronecker’s constructive theory of rationality domains over Dedekind’s set-theoretic treatment of the field theory of ideals –.

Kronecker had early a version of the quadratic reciprocity law involving the monic polynomial (with leading coefficient 1 and prime $p$):

$$1 + x + \ldots + x^{p-1}$$

which is irreducible in $\mathbb{Q}[x]$, the field of rational numbers and Kronecker went on to elaborate a theory of the content (Inhalt or Enthalten-Sein in German) of homogeneous polynomials, divisor theory (Modulsyteme) and elimination theory which I briefly expose.

The general theory of elimination for polynomial equations proceeds along the lines of a general arithmetic of rational functions with integer coefficients and indeterminates. Forms (polynomials) can contain $\text{enthalten}_i$ other forms
or be contained in other forms and two forms are said to be “absolutely equivalent” when they contain each other. Definitions of primitive, prime, irreducible forms follow. It is useful to quote in full proposition IX (Kronecker [8], p. 345):

When a homogeneous linear form $F$ is contained in another form $F_0$, the latter can be transformed in the former provided that forms of the domain (of rationality) are substituted for the indeterminates of $F_0$; those forms are linear if $F_0$ is itself a linear form. In such a case the contained linear form $F$ is transformed into the containing form through a linear substitution with integral coefficients and this a sufficient condition for the containment $Enthalten-Sein$ of $F$ in $F_0$.

Kronecker explains that the linear substitution refers to the indeterminates and the integer coefficients are the entire rational functions or integral quantities of the domains of rationality $R, R', R''$. Proposition X then ensues:

Equivalent homogeneous linear forms can be transformed one into the other through substitution with integral coefficients (ibid.).

Divisibility properties are easily deducible e.g. absolutely equivalent forms have the same divisors and the final conclusion is reached with the statement XIII (and XIII') on the unique factorization of integral algebraic forms as products of irreducible (prime) forms. What this shows, Kronecker maintains, is that the fundamental laws of ordinary arithmetic are preserved in the encompassing sphere of algebraic quantities by the process of association of algebraic forms.

The association of integral algebraic forms, Kronecker continues, is shown by the result on unique factorization to conserve the conceptual determinations and the laws (of arithmetic) in the extension of the rational to the algebraic; still further, it provides the simplest apparatus, which is also necessary and sufficient, capable to fully exhibit the arithmetical properties of the most general algebraic quantities (Kronecker [8], p. 353).

Now, the fundamental theorem of arithmetic states that every positive integer can be represented uniquely as a product of prime powers:

$$n = p_1^{a_1}p_2^{a_2}...p_k^{a_k} = \prod_{i=1}^{k} p_i^{a_i}$$

and Kronecker ends up with his fundamental result on the unique factorization of integral algebraic forms (homogeneous polynomials with integer coefficients) as product of prime forms:
Every integral form is representable as a product of irreducible (prime) forms in a unique way. (Kronecker [8], p. 352)

And in his 1883 paper, Kronecker [9] proceeds to formulate a theory of higher-order forms that amounts to a proof of quadratic reciprocity for higher powers or degrees of polynomials. It is this proof that I want to adapt for the following theorem for what I call polynomial functionals $P_L$ and $Q_L$ representing logical propositional functions in $F[x]$, the ring of polynomials.

**Theorem 1. A quadratic reciprocity theorem for modular polynomial logic**

In the ring of polynomials $F[x]$ with one indeterminate $x$ and integer coefficients in the finite field $F$ with $p^n$ elements – $p$ an odd prime and $n$ a positive integer – $P_L$ and $Q_L \in F[x]$ with $Q_L$ an irreducible monic polynomial of positive degree, then:

$$\left(\frac{P_L}{Q_L}\right)\left(\frac{Q_L}{P_L}\right) = (-1)^{\deg(\frac{P_L}{2})\deg(\frac{Q_L}{2})}.$$  

**Proof.** Since we work with polynomials in the sense of Kronecker, we shall use essentially Kronecker’s notion of the content of polynomials $\text{con}(P_L)$ and $\text{con}(Q_L)$ in our proof for which I reconstruct Kronecker’s argument (see Gauthier [5]). 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 divisibility of composite numbers by primes. Now the fact (Gauss’s lemma) 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

$$\prod_{k=1}^{r} M_k U_{hk}$$

and

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

where the $M$s are integral forms, the $U$s indeterminates and the $c$s integral coefficients with $j = (0, \ldots, m)$ and $k = (0, \ldots, n)$. We shall read it in the form (remembering that $a^{p-1} \equiv 1 (mod \ p)$ from a divisibility point of view)
A quadratic reciprocity theorem for arithmetical logic

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

Kronecker’s generalization uses the convolution product for polynomials

\[ \sum_{h} M_h U_h \cdot \sum_{i} M_{m+i} U_{i-1} = \sum_{k} M'_k U^k \]

so that the product

\[ \prod_h \sum_k M'_k U_{h k} \]

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

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

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 (following Edwards [3], 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. Relying finally on Kronecker’s notion of content for our polynomial functionals, we can assert the equivalence:

\[ \text{con}((P_L)(Q_L)) = \text{con}(P_L) \text{ con}(Q_L) \]

which satisfies the equation:

\[ \frac{P_L}{Q_L} \left(\frac{Q_L}{P_L}\right) = (-1)^{\deg(P_L-1)\deg(Q_L-1)}. \]
What does this theorem mean for what I call modular polynomial logic? Quadratic reciprocity is a kind of syntactic consistency and arithmetic completeness and I want to exploit briefly a logical calculus for local implication or conditional together with the connectives of local negation and local disjunction (see Gauthier [4]). The conditional is our best candidate since we have the inclusion:

\[ a \supset b \text{ for } (a \rightarrow b) \text{ and } b \supset a \text{ for } (b \rightarrow a) \rightarrow (a \equiv b) \]

I mean by local the strongest logical strength for the connectives (and quantifiers) in the sense that they have an arithmetical content which is susceptible of computation in a finite (polynomial) calculus. I take for example the derivation of the polynomially interpreted conditional

\[ a \rightarrow b = (\bar{a}_0x + b_0x). \]

The modular version of implication in (Gauthier [6]) reads

\[ a_0x \equiv b_0x (\text{mod } a_0x + 1) \]

\[ 1 - a_0x \equiv b_0x (\text{mod } a_0x). \]

Remark that the translation is on \( a \rightarrow b = \neg a \lor b \) for \( \bar{a} = 1 - a \) and it is constructive since it supports a numerical content which supports in its turn the topological interpretation of the intuitionistic conditional on the relative complement on the open sets of a topological space \( X \)

\[ a \rightarrow b = \text{In}((X - a) + b) \]

for \( \text{In} \) the interior of \( X \); this has also a combinatorial interpretation in the following derivation of decomposition or binomial expansion (see Gauthier [6], chap. 7. 7).

### 2 The elimination of implication

We want to arithmetize (local) implication. We put \( 1 - a = \bar{a} \) for local negation. We have \( (a_0x + b_0x)^n \) 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

\[(\bar{a}_0x + b_0x)^n = \bar{a}_0^n x + n\bar{a}^{n-1}xb_0x + [n(n-1)/2!]\bar{a}^{n-2}xb_0^2x + ... + b_0^n x\]

where the companion indeterminate \( x \) shares the same power expansion. By an arithmetical calculation (on homogeneous polynomials that are symmetric i.e. with a symmetric function \( f(x, y) = f(y, x) \) of the coefficients)
A quadratic reciprocity theorem for arithmetical logic

\[(\bar{a}_0 + b_0 x)^n = \bar{a}_0^n x + \sum_{k=1}^{n-1} (n - 1/k - 1)\bar{a}_0^{k-1} x + (n - 1/k) a_0^k b_0^{n-k} x + b_0^n x\]

\[= \sum_{k=1}^{n} (n/k - 1) a_0^k x b_0^{n-k} x + \sum_{k=0}^{n-1} (n - 1/k) a_0^k x b_0^{n-k} x\]

\[= \sum_{k=0}^{n-1} (n - 1/k) a_0^k x b_0^{n-k} x + \sum_{k=0}^{n-1} (n - 1/k) a_0^k x b_0^{n-k} x\]

\[= \bar{a}_0 \sum_{k=0}^{n-1} (n - 1/k)(\bar{a}_0 - 1)^k b^{n-k} x +\]

\[\sum_{k=0}^{n-1} (n - 1/k) a_0^k x b_0^{n-k} x\]

\[= (\bar{a}_1 + b_1 x)(a_1 x + b_1 x - 1)^{n-1}\]

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

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

\[... ... ... ...\]

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

\[(\bar{a}_{n-1} + b_{n-1} + \bar{a}_{n-1} + b_{n-1} - (n - 1))^{(n-(n-1))}\]

\[(\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

\[(\bar{a}_0 + b_0 x).\]

Remembering that

\[(\bar{a}_x + b_x)_{k<n}^{n} = \sum_{k+m=n} (k + m/k) \bar{a}^k b^m x^n\]

we have

\[(\bar{a}_x + b_x)_{k<n}^{n+m=n} = \prod_{k+m=n} (k, m) = 2^n\]

or more explicitly

\[\sum_{i=0}^{m+n} c_i x^{m+n-1} = \bar{a}_0 x \cdot b_0 x \prod_{i=1}^{m+n} (1 + c_i x) = 2^n\]
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

$$(a_0 x + b_0 x + c_0 x + ... + k_0 x)^n = \sum_{p,q,r...s} a^p b^q c^r ... k^s$$

in the same manner.

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 $a \to b$ in terms of

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

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

**Theorem 2.** Local implication $a \to b$ can be eliminated by interpreting it as $(\bar{a} + b)^n$.

**Proof.** By the above construction. \qed

The derivation has been effected here on a binary form of higher order $n$ in the spirit of Kronecker’s theory, but it applies easily to a quadratic form with numerical content.

### 3 Logic

The proof theory involved in the modular polynomial interpretation is purely syntactic and doesn’t need any semantics either in set-theoretic terms for the (first-order) logic of Peano arithmetic or for the possible worlds semantics (Kripke) of intuitionistic logic. This means that logical truths and truth values can be dispensed with or that logical truth is only an approximation to arithmetical truth – logical truths are essentially tautologies as L. Wittgenstein would say –. The fundamental relation is congruence for arithmetical logic and the logical or set-theoretical equivalence relations are only surface phenomena of arithmetical facts.
Finally, I give a few more illustrations of the polynomial translation. Take for example the implicational fragment of classical logic:

1. \( A \to (B \to A) \),
2. \( (A \to B) \to (B \to C) \to (A \to C) \),
3. \( ((A \to B) \to A) \to A \).

That is easily translated as:

1. \( \bar{a}_0 x \to (b_0 x \to \bar{a}_0 x) \),
2. \( (\bar{a}_0 x \to b_0 x) \to (b_0 x \to c_0 x) \to (\bar{a}_0 x \to c_0 x) \),
3. \( ((\bar{a}_0 x \to b_0 x) \to a_0 x) \to a_0 x \).

For the intuitionistic conditional with:

1. \( (A \to \neg A) \to \neg A \) and
2. \( A \to (A \to B) \) interpreted again as \( \bar{a}_0 x \equiv 1 - a_0 x \)

we have

1. \( \bar{a}_0 x + a_0 x + b_0 x \) and
2. \( a_0 x + (\bar{a}_0 x + b_0 x) \).

Residual polynomial logic versus nonresidual logic for implication supposes again that logical truth is trivial compared to the arithmetical logical calculus since attributing a numerical content to a sentence or closed formula and its terms or to a propositional function (à la Russell) will always give a residue according to the inclusion structure of the conditional or logical implication. The fundamental arithmetic congruence relation is basic to all logical calculi from combinatorial logic to algebraic logic and categorical logic, including the probability calculus. We have:

\[
P(A/B) = P(AB)P(B)
\]
the conditional probability of \( A \) given \( B \) gives:

\[
P(\bar{a}_0 x + b_0 x) = P(\bar{a}_0 x \times b_0 x)/P(\bar{a}_0 x)
\]
and Bayes theorem stating:

\[
P(A/B) = \frac{P(B/A)P(A)}{P(B)}
\]
gives:

\[
P(\bar{a}_0 x + b_0 x) = \frac{P(b_0 x + \bar{a}_0 x)P(\bar{a}_0 x)}{P(b_0 x)}
\]
and for the inverse probability

\[
P(E_i/A) = \frac{P(E_i)P(A/E_i)}{\sum_{j=1}^{n} P(E_j)P(A/E_j)}
\]
we have

\[
P(e_i x + \bar{a}_0 x) = \frac{P(e_i x)P(\bar{a}_0 x/e_i x)}{\sum_{j=1}^{n} P(e_j x)P(\bar{a}_0 x/e_j x)}.
\]
4 Conclusion

Leibniz who knew about Fermat’s work and the fundamental theorem of arithmetic had the idea of a “calculus ratiocinator” in his universal characteristics “characteristica universalis”, a kind of universal logic assigning prime numbers to all concepts starting with God (God = 1). The idea was to calculate everything as he exclaimed “Calculemus!” Leibniz’ dream was not realized by Leibniz, but many logicians have thought after the advent of symbolic logic with Boole’s logic and Frege’s Begriffsschrift or “the writing of concepts” that formal logic was such a realization. But Frege had asked in his Grundlagen der Arithmetik “How far can one go in arithmetic with logic alone?” and, as we know, he stopped short of polynomial arithmetic with the paradoxical unlimited comprehension principle. The polynomial interpretation is not foreign to Gdel’s arithmetization of syntax for first-order logic, but Gdel’s numbering of formulas and their content is an “external” association of the sequence of integers to obtain ω-consistency for the infinitary Peano arithmetic – ω-consistency is reducible to simple consistency or 1-consistency, but the set-theoretical setting of Peano arithmetic is still infinitary. Kronecker’s theory of forms or homogeneous polynomials with finite descent is rather a polynomialization of content aimed at a finite computation of any logical calculus, from combinatorial logic, type theory, typed λ-calculus to algebraic logic (including categorical logic which is essentially algebraic) to the extent that modular polynomial logic as the internal logic of arithmetic encompasses the arithmetical content of all logics with the goal of reducing logic to arithmetic in the perspective of constructive mathematics.

References


A quadratic reciprocity theorem for arithmetical logic


Received: October 27, 2019; Published: November 25, 2019