MÉMOIRES DE LA S. M. F.

J. V. ARMITAGE

The product of N linear forms in a field of series and the Riemann hypothesis for curves

Mémoires de la S. M. F., tome 25 (1971), p. 17-27

<http://www.numdam.org/item?id=MSMF_1971__25__17_0>

Colloque Th. Nombres [1969, Bordeaux]
Bull. Soc. math. France,
Mémoire 25, 1971, p. 17 à 27

THE PRODUCT OF N LINEAR FORMS IN A FIELD OF SERIES AND THE RIEMANN HYPOTHESIS FOR CUVES

by

J.V. ARMITAGE

-:-:-:-

I. - Introduction. Minkowki's creation of the geometry of numbers was likened to the story of Saul, who set out to look for his father's asses and discovered a Kingdom. This lecture illustrates the reverse process, for it is concerned with the remains of my attempt to make a systematic use of Minkowski's ideas to questions of reduction theory in algebraic geometry. But I discovered that such methods were usually inappropriate for functionfields in more than one variable and that where they were not inappropriate I had already been anticipated (albeit in a different language).

So I shall be concerned primarily with a few debris, together with some conjectures which may be of interest to number theorists and algebraic geometers . In particular, I propose a conjecture about linear forms which implies the Riemann Hypothesis for hyperelliptic curves (and probably more generally) and I outline, very briefly, an alternative formulation of Weil's proof of the Riemann Hypothesis.

2. - Statement of the Riemann Hypothesis. From an arithmetical point of view, the basic question is the following : how many solutions has a polynomial congruence

$$f(x,y) \equiv 0 \pmod{p} \quad , \quad f(x,y) \in \mathbb{Z}[x,y] \, ? \qquad (I)$$

The congruence (I) may be construed either as the equation of a curve, Γ , over $\mathbb{F}_p$ in the affine plane or as defining a function field $L = \mathbb{F}_p(x,y)$. More generally, one considers a function field $k(x,y)$ (or a curve Γ/k) over a finite field, k , of q elements.

From a geometrical point of view, the problem is to count the rational points on Γ/k ; in terms of function fields, one asks for the number of finite prime divisors of L of degree 1 (or the number of places of degree 1 at finite distance). From both points of view, it is more natural to consider curves in projective space and to include the places at infinity. We shall do so in what follows.

Let N_n denote the number of places of degree 1 of the function field Lk_n ,

where $[k_n : k] = n$. (Alternatively, N_n is the number of places of L of degree n , or the number of points of Γ/k , rational over k_n). Then the Riemann Hypothesis asserts that

$$| N_n - q^n - 1 | \leq 2g\, q^{n/2} \quad , \tag{2}$$

where g is the genus. (See Weil's article [8] for a history of the problem).

The zeta function $Z(u)$ of L is the function, of a complex variable u , defined by

$$u \frac{d}{du} Z(u) = \sum_{n=1}^{\infty} N_n u^n = \sum_{n=1}^{\infty} N_n q^{-ns} \quad (s = \sigma+it). \tag{3}$$

On using the functional equation (essentially the Riemann-Roch Theorem) and (2) , one deduces that the series (3) has radius of convergence not less than $q^{-1/2}$ and it follows that the zeros of $Z(u)$ have absolute value $q^{1/2}$. The latter result is the one usually known as the Riemann Hypothesis. It was first proved, for $g = 1$, by Hasse [5], using abstract complex multiplication, and the general case was proved by Weil [7] , using the inequality of Castelnuovo-Severi in a setting of abstract algebraic geometry whose foundations he had already laid. (All the ideas introduced thus far are exposed in Chevalley's Bourbaki Seminar, [4]).

3. - The product of N linear forms in a field of series. Let $\mathrm{Card}(k) = q$, let K be the transcendental field $k(t)$ and write $R = k[t]$. For $a,b \in R$, $b \neq 0$, define the 'infinite' valuation (1) by

$$\left|\frac{a}{b}\right| = q^{\text{degree } a - \text{degree } b} = q^{-\nu_\infty(a/b)} \tag{4}$$

We denote the completion of K with respect to the valuation (4) by $\hat{K}$. (Thus $\hat{K}$ consists of the formal Laurent series

$$a_m t^m + a_{m-1} t^{m-1} + \ldots \quad .)$$

We write P_N for the ultrametric, locally compact, space $\hat{K}^N$, with distance definde by

$$||x|| = \max(|x_1|, \ldots, |x_N|) \quad (x \in P_N) \, . \tag{5}$$

A lattice Λ in P_N is a free R-module given by N linear forms

$$\left.\begin{aligned} L_1 &= a_{11} u_1 + \ldots + a_{1N} u_N \\ &\cdots \\ L_N &= a_{N1} u_1 + \ldots + a_{NN} u_N \end{aligned}\right\} \tag{6}$$

where $a_{ij} \in \hat{K}$, $u_i \in R$ and $\Delta = \Delta(\Lambda) = |\det (a_{ij})| \neq 0$.

The basic question on the product of linear forms is this : given $L_1,\dots,L_N$ of determinant Δ , to find the least M_N (a power of q) such that there exist polynomials $u_1,\dots,u_N$, not all 0 , for which

$$|L_1 \dots L_N| \le M_N \quad \Delta \ . \tag{7}$$

If $q \ge N-1$, then it follows form the analogue of Minkowski's Convex Body Theorem [6] (essentially the Riemann-Roch Theorem, cf. [3]) that

$$M_N = q^{-(N-1)} \ . \tag{8}$$

If $q < N-1$, then (8) is no longer best possible and I have shown [2] that

$$M_N \le q^{-(N-1)-s} \ , \tag{9}$$

where s is the least integer defined by $s \ge (N-1)/q-1$.

Computations in special cases, together with the consequences which it implies, suggest the truth of the following conjecture.

CONJECTURE. If $q < N-1$, then

$$M_N = q^{-(N-1+\gamma)} \ , \tag{10}$$

where γ is the integer defined by

$$\gamma-1 \le (N-q-1)/2q^{1/2} < \gamma \ . \tag{11}$$

4. - The conjecture implies the Riemann Hypothesis in the hyperelliptic case. Let L be a function field of transcendence degree 1 defined over the finite field k and let $N = N_1$ denote the number of places of L of degree 1 . We show that if N is bigger than q , then the genus of L cannot be too small. More precisely, we have :

PROPOSITION. Let $q \ge 2g$, $N > q+1$ and suppose that the Conjecture is true. Then

$$2q^{1/2}\, g \ge N-q-1 \ . \tag{12}$$

Proof. It follows from the Riemann-Roch Theorem that there exists $t \in L$ that has simple poles at the places of degree 1 and no other singularities. Thus L is a "totally real" extension of $k(t)$ of degree N ; that is, L has an imbedding

$$\theta : L \to \hat{K} \times \dots \times \hat{K} \ ,$$

along the diagonal, where at each infinite place L is to be viewed as contained in $\hat{K}$.

The integral closure O_L of R in L has an R-basis $(\alpha_1,\dots,\alpha_N)$ and if

$$\theta(\alpha_i) = (a_{i1}, \dots, a_{iN}) , \tag{I3}$$

then the matrix $A = (a_{ij})$ gives rise to a lattice Λ and a corresponding set of linear forms. The determinant $\det A$ is D, where D^2 is the discriminant of the extension L/K and

$$|D^2| = q^{2(g+N-1)} . \tag{I4}$$

Now, for $u_1,\dots,u_N \in R$, the product $L_1 \dots L_N$ is the norm $N_{L \to K}\xi$ of an element $\xi \in O_L$ and so has absolute value (4) at least 1 if $\xi \neq 0$. On the other hand, the Conjecture implies that

$$1 \le |L_1 \dots L_N| \le q^{-N+1-\gamma}\, q^{N-1+g} . \tag{I5}$$

So, from (II),

$$(N-q-1) / 2q^{1/2} \le g .$$

This completes the proof of the Proposition. Of course, the result (I2) is an immediate consequence of (2), but our purpose is to derive (2) from (I2).

COROLLARY. If L is hyperelliptic, then the Riemann Hypothesis is true for L.

Proof. If L is hyperelliptic, then it is quadratic over some subfield, $k(x)$. Namely, $L = k(x,y)$ where $y^2 = g(x)$ and $x = \omega'/\omega$ is the ratio of differentials of the first kind.

Without loss of generality, we may suppose that the condition $q \ge 2g$ of the Proposition holds. So it suffices to verify $N > q+1$. We show that if this condition does not hold, then the desired result can be obtained by considering a related field.

Suppose that L has $N < q-1$ places of degree 1. Consider the field L^* defined by

$$y^2 = a\, g(x) \tag{I6}$$

where $a \notin k^2$. For $x \in k$, the equation (I6) has a solution if and only if $y^2 = g(x)$ has not. Consequently, the new field has $2q-N > q+1$ places of degree 1. We now apply the Proposition with L^* in place of L and $2q-N$ in place of N, and so obtain the desired inequality.

One would like to find an argument (2) resembling the proof of the Corollary in the general case, but there are apparently insurmountable obstacles. In the general case, we have a curve Γ/k and the Frobenius $F(\Gamma)$ on Γ induces an endomorphism on the Jacobian. We want a curve Γ^* such that the Frobenius $F(\Gamma^*) = -F(\Gamma)$.

Professor Serre has pointed out to me that the argument given above in the hyperelliptic case is essentially a Galois descent applied to the Jacobian. Since, in that case, Γ has an automorphism of order 2 which is -1 on the Jacobian, one can descend the Jacobian to obtain the Jacobian of Γ^*. In general, the descent yields an abelian variety which is not obviously a Jacobian.

5. - Comments on the Conjecture. Perhaps the most interesting feature of the Conjecture and the consequent Proposition is that, together, they throw some light on the relative depths of the ordinary Riemann Hypothesis and its analogue for curves. The latter appears to be analogous to the problem of finding the precise lower bound for the discriminant of a number field and so, presumably, is less deep than the problem of determining the abscissae of the zeros of $\zeta(s)$.

From the point of view of the geometry of numbers, there are at least two possible approaches to a proof of (I0).

The first begins by observing that if $q = N-2$, then (9) already gives the same bound for M_N as does (I0). This suggests the possibility of using induction on N, for fixed q.

In order to make the induction step, one would like to use an argument along the following lines. Without loss of generality (cf. the proof of (9) given in [2]), we can write the linear forms as

$$L_i = u_1 + \alpha_i u_2 + \ldots + \alpha_i^{(n-1)} u_N \quad (1 \le i \le N) \qquad (I7)$$

with $|\alpha_1| \le q^{-1}$. Write $L'_i = L_i - L_1$. Then we obtain $N-1$ linear forms in $N-1$ variables of determinant Δ and the induction hypothesis implies that there exist polynomials, not all 0, such that

$$|L'_2 \ldots L'_N| \le q^{-\delta} \Delta \quad , \qquad (I8)$$

where $\delta = (N-2) + (N-q-2)/2q^{1/2}$. After a suitable unimodular substitution on the variables, we may suppose that

$$|(\alpha_2-\alpha_1) \ldots (\alpha_N-\alpha_1)| \le q^{-\delta} \Delta \quad . \qquad (I9)$$

Now, if there is no cancellation of terms of highest degree in t on the left hand side, then the inequality (I9) implies that

$$|\alpha_1 \ldots \alpha_N| \le q^{-\delta-1} \Delta \qquad (20)$$

and this implies (I2).

Unfortunately, there does not seem to be any way of dealing with the case when cancellation takes place. Maybe one could deal with this by making further normalizations of the coefficients in (I7). Even if it did not lead to a best possible result, such an approach might still yield a result which would imply good estimates for character sums. Again, if the $\alpha_i^{(j)}$ are taken to be a basis for a hyperelliptic field, then one might be able to achieve a normalization of the desired kind.

A variation on the induction theme is suggested by a method of Mordell, which allows one, in certain circumstances, to replace an N-dimensional problem by a related (N-1)-dimensional problem. (cf. [1], for references and a generalization). In the present situation, we denote by λ_N the lower bound of the numbers λ with the property that for any set of N linear forms , L_1 ,..., L_N , in N variables, of determinant 1 , the inequality

$$|L_1 \dots L_N| \leq \lambda \quad , \tag{2I}$$

has a non-zero solution in R . If μ_{N-1} is similarly defined with reference to the inequality

$$|L_1 \dots L_{N-1} (L_1 + \dots + L_{N-1})| \leq \mu \quad , \tag{22}$$

where $L_1, \dots L_{N-1}$ are linear forms of determinant 1 in N-1 variables, then an argument analogous to that in [1] yields the relation

$$\lambda_N^{N-2} \leq \mu_{N-1}^{N-1} \quad . \tag{23}$$

If one could ensure that the minimum of the product on the left hand side of (22) were attained for values of the variables such that $|L_1 + \dots + L_{N-1}| \leq 1$, then one could deduce, from (23) and the induction hypothesis, that

$$\lambda_N \leq q^{-a}$$

where $$a = (2q^{1/2}(N-1)(N-2) + (N-1)(N-q-2))/2q^{1/2}(N-2)$$

and, once again, this gives the desired result (with $\Delta = 1$).

Accordingly, this second approach reduces the problem to that of the study of the critical lattices of the regions

$$|x_1 x_2 \dots x_{N-1} (x_1 + \dots + x_{N-1})| \leq \mu$$

and

$$|x_1 x_2 \dots x_{N-1}| \leq \mu$$

in the space P_{N-1} .

6. - Weil's proof in the language of the geometry of numbers. The problem considered in § 2, is, in some ways, more general than that of the Riemann Hypothesis for curves, since the coefficients a_{ij} of the linear forms (6) are arbitrary elements of $\hat{K}$. This suggests that one might try to imitate Weil's argument in the more general setting. It was with this in mind that I translated Weil's proof into the language of the geometry of numbers, but, so far, I have not been able to carry out the details of the argument except in the case when the a_{ij} come from a basis of an algebraic extension L/K.

The first part of the translation has already been published, [3], and we begin by recalling the main ideas.

Let L be a finite algebraic extension of degree N of the field $K = k(t)$ and suppose that the divisor of poles of t splits completely in L. (This latter supposition is not necessary; it makes the situation analogous to the case of a totally real number field and affords considerable simplification in the present exposition).

Let $\mathfrak{a}$ be a divisor of L/k of degree $\deg(\mathfrak{a})$ and write $\mathfrak{a} = \mathfrak{a}_e \mathfrak{a}_u$, where $\mathfrak{a}_e$ is divisible only by finite primes and $\mathfrak{a}_u$ by infinite primes. The Riemann-Roch Theorem is concerned with the dimension of the k-vector space $L(\mathfrak{a})$ where

$$L(\mathfrak{a}) = \{\alpha \in L : \nu_{\mathfrak{p}}(\alpha) \geq \nu_{\mathfrak{p}}(\mathfrak{a})$$

and $\mathfrak{p}$ runs through all prime divisors of L. It is easy to see that the space $L(\mathfrak{a})$ can be regarded as the intersection of two k-vector spaces $L(\mathfrak{a}_e)$ and $L(\mathfrak{a}_u)$ and that $L(\mathfrak{a}_e)$ defines a lattice $\Lambda(\mathfrak{a})$ in P_N, of determinant $\Delta(\mathfrak{a})$, whilst $L(\mathfrak{a}_u)$ defines a convex body $C(\mathfrak{a})$ of volume $V(\mathfrak{a})$. The ratio

$$\frac{\Delta(\mathfrak{a})}{V(\mathfrak{a})} = q^{\deg \mathfrak{a}} \, q^{N-1+g} \tag{24}$$

and the Riemann-Roch Theorem is now an immediate consequence of Mahler's analogue of Minkowski's Theorem, together with a suitable identification of the polar lattice and polar body.

It follows from the foregoing that each integral divisor $\mathfrak{a}$ has a unique representation in the form $(\Lambda(\mathfrak{a}), C(\mathfrak{a}))$ where $\Lambda(\mathfrak{a})$ is a sub-lattice of the lattice $\Lambda(e)$ correspondig to the ring O_L and $C(\mathfrak{a})$ is a convex body (in fact a "rectangular box") contained in the unit cube $\|x\| \leq 1$ in P_N. Thus each integral divisor $\mathfrak{a}$ has a unique representation

$$A = \begin{bmatrix} v_{11} & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ v_{21} & v_{22} & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ & \dots & & \dots & & \dots & & & \dots & \\ v_{N1} & v_{N2} & v_{N3} & \dots & v_{NN} & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & t^{a_1} & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & t^{a_2} & 0 & \dots & 0 \\ & \dots & & \dots & & \dots & & & \dots & \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & t^{a_N} \end{bmatrix} \tag{25}$$

where $|v_{ij}| < |v_{ii}|$, $1 \leq j < i \leq N$, $v_{ij} \in R$ and $|\det A| = q^{\deg \mathfrak{a}}$. We may accordingly identify divisors of given degree as points of certain subsets of the locally compact topological vector space

$$\mathcal{D} = \hat{K}{}^{4N^2} \quad . \tag{26}$$

It is now a comparatively straightforward matter to set up the theory of correspondences in the space $\mathcal{D}$, to obtain the appropriate version of the Lefschetz fixed point formula and finally to imitate Weil's proof of the inequality of Castelnuovo-Severi.

We turn now to the situation presented by N linear forms in the most general case. We consider the algebra $\hat{K}{}^N$ with componentwise multiplication and we replace the integers O_L by a fixed R-order Λ of $\hat{K}{}^N$; namely, the R-order generated by the N linear forms (6). Suppose that

$$|\det \Lambda| = q^{N-1+\gamma} \quad . \tag{27}$$

We consider those lattices (free R-modules) $M \subset \Lambda$ which are "irreducible" and have the property that

$$\Lambda M \subset M \quad . \tag{28}$$

Then Λ/M is a k-vector space of dimension m , where

$$q^m = |\det M| \; / \; |\det \Lambda| \; .$$

We define such a lattice to be prime and of degree m . Then the number of prime lattices of degree 1 generalizes the number of finite prime divisors of degree 1 in a function field and one might hope to prove the appropriate generalization of (2) , with the number γ in (27) in place of the genus g .

Unfortunately, in order to introduce enough multiplicative structure into the problem, it appears to be necessary to take Λ to be the lattice corresponding to the order O_L in the function field L ; so the hope of a significant generalization may prove to be illusory.

When Alice performed the subtraction 365 - 1 for Humpty Dumpty in her head, he looked doubtful and said : "I'd rather see that done on paper". No doubt a similar preference is felt by the reader on seeing the foregoing sketch. I do intend to publish the details some time, though I still hanker after the linear forms conjecture.

7. - Postscript to the lecture. Professor Serre suggested to me that there ought to be a restatement of the conjecture in the language of vector bundles. He had already supplied me with some of the necessary vocabulary when commenting on the work alluded to in § 1 . Needless to say, anything that is incorrect in what follows represents my contribution, though the converse is not necessarily true.

The matrix $A = (a_{ij})$ of coefficients in (6) defines a vector bundle over the projective line. The statement that there exist $u_1,\dots,u_n \neq 0,\dots,0$ in R such that (I0) holds can be reinterpreted as saying that there exist integers $\lambda_1,\dots,\lambda_N$, with

$$\lambda_1+\dots+\lambda_N \leq -(N-1)-\gamma + \deg(\det A) , \tag{29}$$

for which

$$\| T(\lambda_1,\dots,\lambda_N)\, A\, u \| \leq 1 \tag{30}$$

where $u = (u_1,\dots,u_N)$ and $T(\lambda_1,\dots,\lambda_N)$ is the diagonal matrix diag $\{t^{-\lambda_1},\dots,t^{-\lambda_N}\}$.

The inequality (30) asserts that at least one member of the family , $\mathcal{B}$, of vector bundles corresponding to the matrices $T(\lambda_1,\dots,\lambda_N)\, A$ possesses a non-trivial section. On taking the Nth exterior power of $\mathcal{B}$, we see that the Chern class $c_1(\lambda_1,\dots,\lambda_N)$ of the bundle determined by $T(\lambda_1,\dots,\lambda_N)\, A$ is

$$c_1(\lambda_1,\dots,\lambda_N) = -\deg(\det A) + \lambda_1 + \dots + \lambda_N . \tag{31}$$

So the conjecture now reads : *if* $c_1(\lambda_1,\dots,\lambda_N) \geq -(N-1)-\gamma$, *where* γ *is given by* (II) , *then at least one member of the family* $\mathcal{B}$ *has a non-trivial section.*

In this context, it is interesting to note that, given such a bundle (or matrix), there exists a matrix $Y = \operatorname{diag}\{y_1,\dots,y_N\}$ such that $|y_1| \leq 1,\dots,|y_N| \leq 1$ and a unimodular aatrix U (with elements in R and determinant 1) such that

$$A = Y \operatorname{diag}\{t^{-\mu_1},\dots,t^{-\mu_N}\}.\, U \tag{32}$$

where the $\mu_1, \ldots, \mu_N$ are the successive minima of the convex body

$$C = \{ x \in P_N : \| A^{-1} x \| \leq 1 \}.$$

(The reduction (32) follows immediately from the characterization of convex bodies given by Mahler [6] . It is strongly reminiscent of Grothendieck's Theorem on the decomposition of vector bundles over the Riemann sphere).

-:-:-:-

BIBLIOGRAPHIE

[1] J.V. ARMITAGE. - On a method of Mordell in the geometry of numbers, Mathematika 2 (1955), 132-140.

[2] J.V. ARMITAGE. - The product of n linear forms in a field of series, Mathematika 4 (1957), 132-137.

[3] J.V. ARMITAGE. - Algebraic functions and an analogue of the geometry of numbers : the Riemann-Roch Theorem, Archiv der Mathematik 18 (1967), 383-393.

[4] C. CHEVALLEY. - L'hypothèse de Riemann pour les corps de fonctions algébriques de caractéristique p , Séminaire Bourbaki 1 (1948/49), n° 3 and n° 9.

[5] H. HASSE. - Zur Theorie der abstrakten elliptischen Funktionenkörper, J. reine u. angew. Math. 175 (1936), 69-88 and 193-208.

[6] K. MAHLER. - An analogue to Minkowski's geometry of numbers in a field of series, Ann. Math. , II Ser. 42 (1941), 481-522.

[7] A. WEIL. - Sur les courbes algébriques et les variétés qui s'en déduisent, Actualités scientifiques et industrielles, n° 1041, Paris, (1948).

[8] A. WEIL. - Numbers of solutions of equations in finite fields, Bull. Amer. Math. Soc. 55 (1949), 497-508.

-:-:-:-

FOOTNOTES

P. 18 (1) We use the same notation for the ordinary absolute value, as in (2). There will be no danger of confusion.

P. 20 (2) The argument just given may be adaptable to the cases of curves (or function fields) $y^{\ell} = g(x)$. Those would include all cases necessary for the estimation of character sums and Kloosterman sums.

-:-:-:-

University of London King's College
Departement of Mathematics
Strand, W.C.2.
(Grande-Bretagne)