Available online at www.sciencedirect.com

ScienceDirect

Expositiones Mathematicae 41 (2023) 451–460

Expositiones Mathematicae

www.elsevier.com/locate/exmath

On Hasse's inequality[☆]

M. Ram Murty

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, K7L 3N6, Canada

Received 5 February 2023; received in revised form 26 March 2023; accepted 26 March 2023

Abstract

We give an elementary exposition of the little known work of Harold Davenport related to Hasse's inequality. We formulate a new conjecture suggested by this proof that has implications for the classical Riemann hypothesis.

MSC 2010 classifications: primary 11G05; secondary 11L40; 11T24

Keywords: Hasse's inequality; Elliptic curves; Character sums

1. Introduction

In his 1924 doctoral thesis, Emil Artin [1] introduced the congruence zeta function of an elliptic curve

$$E: \quad y^2 = x^3 + ax + b \tag{1}$$

over the finite field of p elements. Indeed, if $\mathbb{F}_p(x)$ is the rational function field over $\mathbb{F}_p$, then $K = \mathbb{F}_p(x, y)$ with y given by (1) can be viewed as a quadratic extension of $\mathbb{F}_p(x)$. The integral closure A of the polynomial ring $\mathbb{F}_p[x]$ is a Dedekind domain so that for each non-zero ideal $\mathfrak{a}$ of A, the index $[A : \mathfrak{a}]$ is finite and Artin's congruence zeta function is

$$Z(K, s) := \sum_{0 \neq \mathfrak{a} \in A} [A : \mathfrak{a}]^{-s}.$$

[☆] Research of the author is partially supported by an NSERC, Canada Discovery grant.
E-mail address: murty@queensu.ca.

https://doi.org/10.1016/j.exmath.2023.03.002

Setting $t = p^{-s}$, Artin showed that his zeta function has the form

$$\frac{f(t)}{1-pt}$$

with $f(t)$ a quadratic polynomial over $\mathbb{Z}$. If N_p denotes the number of points on this curve with co-ordinates in $\mathbb{F}_p$, the analog of the Riemann hypothesis for $Z(K, s)$ turns out to be equivalent to the inequality (see for example, Corollary 1.4 on page 132 of [13]):

$$|N_p - p| \leq 2\sqrt{p}. \tag{2}$$

In 1936, Hasse [7] proved this conjecture using new tools that mark the beginning of modern algebraic geometry. One can consider (1) over any finite field of q elements and Hasse showed (2) holds with p replaced by q. Since then, in 1956, Manin [8] gave an elementary proof using the addition formulas for points on the elliptic curve when q is not a power of 2. The case when q is a power of 2, an elementary proof modifying Manin's approach was given by Chahal, Soomro and Top [3]. In 1969, Stepanov [14] gave another proof inspired by Thue's method of auxiliary polynomials used in transcendental number theory. Stepanov's proof was streamlined by Bombieri [2] in 1973 and independently by Schmidt (see page 2 of [11] as well as [12]).

The purpose of this note is to highlight a little known 1932 work of Davenport [5] that seems to have been buried in the sands of time. Davenport shows using essentially the Cauchy–Schwarz inequality that $N_p - p = O(p^{3/4})$ where the implied constant is absolute. Because he derives explicit formulas at every stage of his proof, the simplicity and elegance of the idea is obscured. In this note, we will show that this deduction is practically instantaneous once a few elementary observations are made. We will then outline Hasse's proof. Finally, we discuss the implications of Davenport's method to the classical Riemann hypothesis that leads to an interesting link to a conjecture of Chowla.

2. Character sums over finite fields

Let q be a prime power and $\mathbb{F}_q$ the finite field of q elements. We consider (1) over $\mathbb{F}_q$ and let N_q denote the number of points of E over $\mathbb{F}_q$. If χ is the quadratic character of $\mathbb{F}_q^*$, then

$$N_q = \sum_{x\in\mathbb{F}_q} \big(1 + \chi(x^3 + ax + b)\big) = q + \sum_{x\in\mathbb{F}_q} \chi(x^3 + ax + b).$$

Our goal is to estimate the character sum on the right hand side. We will indicate in Section 5 that there is (essentially) no loss of generality in supposing that our cubic factors completely over $\mathbb{F}_q$ with roots $0, \alpha, \beta$ (say). Thus, our character sum is of the form

$$\sum_{x\in\mathbb{F}_q} \chi(x)\chi(x+\alpha)\chi(x+\beta).$$

Since we are interested in the absolute value of this sum, changing x to αx reduces the problem to estimating the character sum

$$\Phi(a) := \sum_{x\in\mathbb{F}_q} \chi(x)\chi(x+1)\chi(x+a),$$

with $a \neq 0, 1$. Since $\chi(0) = 0$, we see that the above sum is really over $x \in \mathbb{F}_q^*$.

Lemma 1. *For any non-trivial character χ of $\mathbb{F}_q^*$,*

$$\sum_{a \in \mathbb{F}_q} \chi(x+a)\overline{\chi}(y+a) = \begin{cases} q-1 & \textit{if } x = y \\ -1 & \textit{if } x \neq y. \end{cases}$$

Proof. If $x = y$, the result is clear. If $x \neq y$, we write the sum as

$$\sum_{a \neq -y} \chi\left(\frac{x+a}{y+a}\right)$$

and observe that setting

$$b = \frac{x+a}{y+a}$$

transforms the sum into

$$\sum_{b \neq 1} \chi(b) = -1. \quad \square$$

The following theorem shows that Hasse's inequality holds "on average".

Theorem 2.

$$\sum_{a \neq 0,1} |\Phi(a)|^2 \leq 4q^2$$

Proof. We have

$$\sum_{a \neq 0,1} |\Phi(a)|^2 = \sum_{x,y} \chi(x)\chi(x+1)\overline{\chi}(y)\overline{\chi}(y+1) \sum_{a \neq 0,1} \chi(x+a)\overline{\chi}(y+a).$$

The innermost sum is

$$\sum_a \chi(x+a)\overline{\chi}(y+a) - \chi(x)\overline{\chi}(y) - \chi(x+1)\overline{\chi}(y+1)$$

which by Lemma 1 is,

$$= \begin{cases} q-3 & \text{if } x = y, x \neq 0, -1 \\ q-2 & \text{if } x = y = 0 \quad \text{or } x = y = -1 \\ -1 - \chi(x)\overline{\chi}(y) - \chi(x+1)\overline{\chi}(y+1) & \text{if } x \neq y. \end{cases}$$

The sum in question is therefore equal to

$$(q-2)(q-3) - \sum_{x \neq y} \chi(x)\chi(x+1)\overline{\chi}(y)\overline{\chi}(y+1)[1 + \chi(x)\overline{\chi}(y) + \chi(x+1)\overline{\chi}(y+1)].$$

As the summand is bounded by 3, and there are at most q^2 summands, the result is now immediate. $\square$

Davenport [5] derives a sharper estimate with $4q^2$ replaced by q^2. This shows that Hasse's inequality is not always sharp.

We will now use the above theorem to derive a bound for $\Phi(a)$ itself by studying a related sum:

$$\Psi(a,b) := \sum_{x\in\mathbb{F}_q^*} \chi(x)\chi(x+1)\chi(x+a)\chi(x+b),$$

with χ a quadratic character. The relation between the two character sums is given by the following.

Lemma 3. *For $ab(a-1)(b-1)\neq 0$,*

$$|\Psi(a,b)+1| = |\Phi(c)|, \quad \textit{with} \quad c = \frac{a(b-1)}{b(a-1)}.$$

Proof. Changing x to $1/x$ in the summation gives

$$\Psi(a,b) = \sum_{x\in\mathbb{F}_q^*} \chi(1+x)\chi(1+ax)\chi(1+bx) = -1 + \sum_{x\in\mathbb{F}_q} \chi(1+x)\chi(1+ax)\chi(1+bx)$$

because χ is quadratic. As $ab\neq 0$,

$$\Psi(a,b)+1 = \chi(ab)\sum_{x\in\mathbb{F}_q}\chi(1+x)\chi(a^{-1}+x)\chi(b^{-1}+x).$$

Changing $x+1=u$, the sum becomes

$$\chi(ab)\sum_{u\neq 1}\chi(u)\chi(u+a')\chi(u+b')$$

where $a' = -1+a^{-1}$ and $b' = -1+b^{-1}$. Again changing u to $a'u$ shows that $|\Psi(a,b)| = |\Phi(c)|$ with $c = b'/a'$. Thus, a simple calculation shows that for $a, b \neq 0, 1$,

$$|\Psi(a,b)+1| = |\Phi(c)|, \quad \text{with} \quad c = \frac{a(b-1)}{b(a-1)}. \quad \square$$

We will use Theorem 2 to derive an estimate for $\Phi(a)$ itself as follows.

$$|\Phi(a)|^2 = \sum_{x,y\in\mathbb{F}_q^*} \chi\left(\frac{x}{y}\right)\chi\left(\frac{x+1}{y+1}\right)\chi\left(\frac{x+a}{y+a}\right).$$

We put $y = x/z$ so that the sum becomes

$$|\Phi(a)|^2 = \sum_{x,z}\chi(z)\chi\left(\frac{z(x+1)}{x+z}\right)\chi\left(\frac{z(x+a)}{x+az}\right).$$

Thus

$$|\Phi(a)|^2 \leq \sum_z \left|\sum_x \chi\left(\frac{x+1}{x+z}\right)\chi\left(\frac{x+a}{x+az}\right)\right|.$$

Since χ is quadratic, the innermost sum is a sum of the form $\Psi(a,b)$ with suitable a, b. Indeed, putting $x+1=u$, we get

$$\sum_x \chi\left(\frac{x+1}{x+z}\right)\chi\left(\frac{x+a}{x+az}\right) = \sum_u \chi(u)\chi(u+z-1)\chi(u+a-1)\chi(u+az-1),$$

suggesting another change of variables $u = (z-1)v$ which implies

$$\left|\sum_x \chi\left(\frac{x+1}{x+z}\right)\chi\left(\frac{x+a}{x+az}\right)\right| = \left|\sum_v \chi(v)\chi(v+1)\chi\left(v+\frac{a-1}{z-1}\right)\chi\left(v+\frac{az}{z-1}\right)\right|.$$

An application of Lemma 3 shows that

$$\left|\sum_x \chi\left(\frac{x+1}{x+z}\right)\chi\left(\frac{x+a}{x+az}\right)\right| \le 1 + |\Phi(c)|,$$

where

$$c = m(z) := \frac{(a-1)((a-1)z+1)}{az(a-z)}.$$

so that

$$|\Phi(a)|^2 \le q + \sum_z \left|\sum_u \chi(u)\chi(u+1)\chi(u+m(z))\right|.$$

The sum inside the absolute values is $\Phi(m(z))$. Applying the Cauchy–Schwarz inequality to the sum, we obtain

$$|\Phi(a)|^2 \le q + q^{1/2}\left(\sum_z |\Phi(m(z))|^2\right)^{1/2}.$$

For any given b, the equation $m(z) = b$ has at most two solutions for z so that by Theorem 2,

$$|\Phi(a)|^2 \le q + q^{1/2}\left(2\sum_b |\Phi(b)|^2\right)^{1/2} \le q + 2\sqrt{2}q^{3/2} \le 4q^{3/2}.$$

This proves:

Theorem 4. $|\Phi(a)| \le 2q^{3/4}$.

The key steps to note in this ingenious proof are Theorem 2 which is “Hasse’s inequality on average”, combined with a clever use of the Cauchy–Schwarz inequality to get an estimate for an individual character sum. The analogous construction of these two steps in the case of the classical Riemann hypothesis will be discussed in Section 4.

3. Outline of Hasse’s proof

Before we give an outline of Hasse’s proof, we begin with a general fact.

Let A be an abelian group and $d : A \to \mathbb{R}$. We say d is a **quadratic form** if $d(n\alpha) = n^2 d(\alpha)$ for all $\alpha \in A, n \in \mathbb{Z}$ and the map

$$A \times A \to \mathbb{R},$$

given by

$$(\alpha, \beta) \mapsto [\alpha, \beta] := d(\alpha + \beta) - d(\alpha) - d(\beta)$$

is bilinear. In particular, $d(\alpha) = \frac{1}{2}[\alpha, \alpha]$. We say that it is **positive definite** if $d(\alpha) \geq 0$ for all $\alpha \in A$ with equality if and only if $\alpha = 0$.

Lemma 5. *Let A be an abelian group and $d : A \to \mathbb{Z}$ a positive definite quadratic form. Then for all $\alpha, \beta \in A$, we have*

$$|d(\alpha + \beta) - d(\alpha) - d(\beta)| \leq 2\sqrt{d(\alpha)d(\beta)}.$$

Proof. Since d is positive definite,

$$0 \leq d(m\alpha + n\beta) = \frac{1}{2}[m\alpha + n\beta, m\alpha + n\beta] = d(\alpha)m^2 + [\alpha, \beta]mn + d(\beta)n^2,$$

using the bilinear property. Therefore, the discriminant satisfies

$$[\alpha, \beta]^2 - 4d(\alpha)d(\beta) \leq 0$$

and the result is now immediate. □

A very quick intuitive outline of Hasse's proof can be given as follows. For the precise technical background, we refer the reader to [13]. The extension $\overline{\mathbb{F}}_q/\mathbb{F}_q$ is procyclic and generated by the Frobenius map $\phi : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q$ given by $\phi(x) = x^q$. In particular, this means that for each n, the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a cyclic Galois extension with generator ϕ. If E is our elliptic curve, and we consider the group of points $E(\overline{\mathbb{F}}_q)$, then $E(\mathbb{F}_q)$ is simply the set of fixed points of ϕ acting on $E(\overline{\mathbb{F}}_q)$. In other words, viewing $1 - \phi$ as an element of the endomorphism ring $\mathrm{End}(E)$ (with 1 being the identity map), we have

$$E(\mathbb{F}_q) = \ker(1 - \phi).$$

The degree of a map can be defined formally, but for our purposes, we can take it to be the generic number of pre-images (counted with multiplicity) of any given element. Thus, the Frobenius map ϕ has degree q and the identity map has degree 1. Also, $|\ker(1 - \phi)| = \deg(1 - \phi)$ since this is the number of pre-images of zero of the map $1 - \phi$. Hasse showed that the degree function is a positive definite quadratic form on the abelian group $\mathrm{End}(E)$. By Lemma 5,

$$|\deg(1 - \phi) - \deg(1) - \deg(\phi)| \leq 2\sqrt{\deg(1)\deg(\phi)}.$$

In other words,

$$\left|\#E(\mathbb{F}_q) - 1 - q\right| \leq 2\sqrt{q},$$

which is Hasse's inequality. The presence of -1 on the left hand side of this inequality is the contribution from the point at "infinity" since in the geometric setting, one works over the projective space instead of the affine space.

4. The Chowla conjecture and the Riemann hypothesis

For an integer n, we denote by $\Omega(n)$ the total number of prime factors of n counted with multiplicity, then the Liouville function defined as $\lambda(n) = (-1)^{\Omega(n)}$ is a completely multiplicative arithmetical function. The classical Riemann hypothesis is then equivalent to the assertion: for any $\epsilon > 0$,

$$\sum_{n \le x} \lambda(n) = O(x^{1/2+\epsilon}),$$

where the implied constant depends on ϵ. More generally, it is an easy exercise to show that the estimate

$$\sum_{n \le x} \lambda(n) = O(x^{\theta}) \tag{3}$$

implies that $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > \theta$.

Chowla (see page 96, Problem 57 of [4]) conjectured that if $f(x) \in \mathbb{Z}[x]$ is not of the form $cg^2(x)$ with c an integer and $g(x) \in \mathbb{Z}[x]$, then as $x \to \infty$,

$$\sum_{n \le x} \lambda(f(n)) = o(x).$$

The case that f is linear is equivalent to the prime number theorem in arithmetic progressions. This is the only known case of the conjecture. A special case of the conjecture is that if $h \neq 0$, then

$$\sum_{n \le x} \lambda(n)\lambda(n+h) = o(x).$$

Ng [10] has conjectured that even a stronger estimate of the form $O(x^{\beta})$ with $1/2 < \beta < 1$ holds uniformly for $h \le x$. (Though the formulation in [10] is for the Möbius function, it is expected that an analogous hypothesis for the Liouville function holds.)

Inspired by Theorem 2, we propose an average version of this hypothesis: there exists β with $1/2 < \beta < 1$ such that for any $\epsilon > 0$,

$$\sum_{1 \le h \le x} \left| \sum_{n \le x-h} \lambda(n)\lambda(n+h) \right|^2 = O(x^{1+2\beta+\epsilon}). \tag{4}$$

We expect this to hold for any $\beta > 1/2$. The trivial bound is $O(x^3)$ and any $\beta < 1$ will imply a "quasi" Riemann hypothesis. The work of [9] implies that the right hand side of (4) is $o(x^3)$. The strategy of Davenport's derivation now leads to:

Theorem 6. *Assume (4). Then $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > \frac{1+\beta}{2}$. In particular, if any $\beta > 1/2$ is permissible in (4), then $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 3/4$.*

Proof. We have

$$\left| \sum_{n \le x} \lambda(n) \right|^2 = [x] + 2 \sum_{m < n \le x} \lambda(m)\lambda(n).$$

The last sum can be estimated using (4) by the Cauchy–Schwarz inequality. Indeed, writing $n = m + h$, we have

$$\left| \sum_{1 \le h \le x} \sum_{m \le x-h} \lambda(m)\lambda(m+h) \right| \le x^{1/2} \left(\sum_{1 \le h \le x} \left| \sum_{m \le x-h} \lambda(m)\lambda(m+h) \right|^2 \right)^{1/2}.$$

Inserting (4), the final estimate is

$$\sum_{n\le x} \lambda(n) \ll x^{\frac{1+\beta}{2}+\epsilon}$$

which by the remark (3) implies the result. □

5. Concluding remarks

The Hilbert–Pólya dream of interpreting the zeros of the Riemann zeta function as the eigenvalues of a Hermitian operator acting on a suitable Hilbert space is yet to be realized. In the case of function fields, this is (in a sense) a reality. This viewpoint does not come from Hasse's proof but rather from the realization that Artin's congruence zeta function is the characteristic polynomial of the Frobenius map acting on a rank 2 module (called the Tate module) over the ℓ-adic integers where ℓ is a prime unequal to p. Here is a quick description of this viewpoint.

For any natural number m, we will denote by $E[m]$ the group of m-division points of $E(\overline{\mathbb{F}}_q)$. If ℓ is a prime, the Tate module of E, denoted $T_\ell(E)$, is the inverse limit

$$\lim_{\leftarrow} E[\ell^n]$$

with the limit being taken over the natural maps $E[\ell^{n+1}] \xrightarrow{\ell} E[\ell^n]$. Any endomorphism of E acts on $T_\ell(E)$ and so we have a natural map

$$\mathrm{End}(E) \to \mathrm{End}(T_\ell(E)), \quad \psi \mapsto \psi_\ell .$$

If $\ell \neq p$, $T_\ell(E)$ is a free $\mathbb{Z}_\ell$-module of rank 2, and we can therefore choose a basis of $T_\ell(E)$ so that ψ is represented as an element $\psi_\ell \in GL_2(\mathbb{Z}_\ell)$. Using the Weil pairing, one can show that $\deg(\psi) = \det(\psi_\ell)$ and $\mathrm{tr}(\psi_\ell) = 1 + \deg(\psi) - \deg(1-\psi)$ so that $\det(\psi_\ell)$ and $\mathrm{tr}(\psi_\ell)$ are in $\mathbb{Z}$ and independent of ℓ. In particular, this applies to the action of Frobenius map ϕ on $T_\ell(E)$ which gives rise to an ℓ-adic representation of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. The characteristic polynomial of ϕ_ℓ is then $\det(tI - \phi_\ell) = t^2 - \mathrm{tr}(\phi_\ell)t + \det(\phi_\ell)$ which is the numerator of Artin's congruence zeta function. Thus, as $\det(\phi_\ell) = \deg(\phi) = q$, we have

$$\#E(\mathbb{F}_q) = \deg(1-\phi) = \det(I - \phi_\ell) = 1 - \mathrm{tr}(\phi_\ell) + q .$$

Then

$$\#E(\mathbb{F}_{q^n}) = \deg(1-\phi^n) = \det(1-\phi_\ell^n)$$

The success of the proof of the analog of the Riemann hypothesis for the zeta function of an elliptic curve over finite field is rooted in this interpretation of the zeta function as a characteristic polynomial of ϕ_ℓ. Moreover, the base change of the zeta function to $\mathbb{F}_{q^n}$ is simply the characteristic polynomial of ϕ_ℓ^n. Thus proving the Riemann hypothesis for the congruence zeta function over $\mathbb{F}_{q^n}$ for some n is tantamount to proving it over $\mathbb{F}_q$. This explains our remark of there being no loss of generality in assuming our cubic factors completely over $\mathbb{F}_q$.

This reduction can also be seen without the use of the Tate module as was done by Davenport [6] in a later paper written in 1939. In this paper, he derives non-trivial estimates for character sums using very basic finite field theory. He also observes how the zeta function changes when the base field is extended to a larger field. But this paper again seems to have been buried in the sands of time when Weil's definitive work proving the Riemann hypothesis for curves was announced [15] in 1940. The complete proof was published only much later in 1948 by Weil [16]

There have been some developments worth reporting that indicate that our conjecture (4) is plausible. Recent work of Matomäki, Radziwill and Tao [9] shows that

$$\sum_{|h|\leq H}\left|\sum_{n\leq X}\lambda(n)\lambda(n+h)\right| = o(HX)$$

for H tending to infinity first and X tending to infinity. These works indicate that looking towards alternate ways of arriving at the Riemann hypothesis, especially through the study of shifted convolutions of arithmetical functions, is promising.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgements

I would like to thank Jasbir Chahal, Kumar Murty, Siddhi Pathak, Brad Rodgers, Mike Roth, Biswajyoti Saha and the referee for their comments on an earlier version of this paper.

References

[1] E. Artin, Quadratische Körper im Gebeit der höheren Kongruenzen I, II, Math. Z. 19 (1924) 153–246.
[2] E. Bombieri, Counting points on curves over finite fields, 1973, (d'après S. A. Stepanov), Séminaire Bourbaki, 25e année 1972/73, No. 430.
[3] J.S. Chahal, A. Soomro, J. Top, A supplement to Manin's proof of the Hasse inequality, Rocky Mountain J. Math. 44 (5) (2014) 1457–1470.
[4] S. Chowla, The Riemann Hypothesis and Hilbert's Tenth Problem, Gordon and Breach, New York, 1965.
[5] H. Davenport, On the distribution of ℓ-th power residues (mod p), J. Lond. Math. Soc. 7 (1932) 117–121.
[6] H. Davenport, On character sums in finite fields, Acta Math. 71 (1939) 99–121.
[7] H. Hasse, Zur Theorie der abstrakten elliptischen Funktionenkörper, II, III, J. Reine Ang. Math. 175, 69–88, and 193–206.
[8] Yu. I. Manin, On cubic congruences to a prime modulus, Izv. Akad. Nauk. SSSR, Ser. Mat. 20 (1956) 673–678, (in Russian); Amer. Math. Soc. Transl. 13 (2) (1960) 1–7.
[9] K. Matomäki, M. Radziwill, T. Tao, An averaged form of chowla's conjecture, Algebra Number Theory 9.9 (2015) 2167–2196.

[10] N. Ng, The Möbius function in short intervals, in: J.-M. de Koninck, A. Granville, F. Luca (Eds.), Anatomy of Integers, in: CRM Proceedings and Lecture Notes, vol. 46, 2008, pp. 247–258.

[11] W.M. Schmidt, Equations over Finite Fields, an Elementary Approach, in: Lecture Notes in Mathematics, vol. 536, Springer-Verlag, Heidelberg, 1976.

[12] W.M. Schmidt, Equations over Finite Fields: An Elementary Approach, second ed., Kendrick Press, Inc, 2004.

[13] J.H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986.

[14] S.A. Stepanov, The number of points of a hyperelliptic function over a prime field (in Russian), Izv. Akad. Nauk. SSSR Ser. Mat. 33 (1969) 1171–1181.

[15] A. Weil, Sur les fonctions algébriques à corps de constantes fini, C. R. Acad. Sci. Paris 210 (1940) 592–594.

[16] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, in: Actualités Sci. et Ind., Vol. 1041, Hermann, 1948.