BULLETIN (Old Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 55 (1949), Pages 497–508
S (XX)0000-0

NUMBERS OF SOLUTIONS OF EQUATIONS IN FINITE FIELDS

ANDRÉ WEIL

The equations to be considered here are those of the type

$$a_0 x_0^{n_0} + a_1 x_1^{n_1} + \cdots + a_r x_r^{n_r} = b. \tag{1}$$

Such equations have an interesting history. In art. 358 of the *Disquisitiones* [1, a],[1] Gauss determines the Gaussian sums (the so-called cyclotomic "periods") of order 3, for a prime of the form $p = 3n+1$, and at the same time obtains the number of solutions for all congruences $ax^3 - by^3 \equiv 1 \pmod{p}$. He draws attention himself to the elegance of his method, as well as to its wide scope; it is only much later, however, viz. in his memoir on biquadratic residues [1, b], that he gave in print another application of the same method; there he treats the next higher case, finds the number of solutions of any congruence $ax^4 - by^4 \equiv 1 \pmod{p}$, for a prime of the form $p = 4n+1$, and derives from this the biquadratic character of 2 mod p, this being the ostensible purpose of the whole highly ingenious and intricate investigation. As an incidental consequence (*"coronodis loco,"* p. 89), he also gives in substance the number of solutions of any congruence $y^2 \equiv ax^4 - b \pmod{p}$; this result includes as a special case the theorem stated as a conjecture (*"observatio per inductionem facta gravissima"*) in the last entry of his *Tagebuch* [1, c];[2] and it implies the truth of what has lately become known as the Riemann hypothesis, for the function–field defined by that equation over the prime field of p elements.

Gauss' procedure is wholly elementary, and makes no use of the Gaussian sums, since it is rather his purpose to apply it to the determination of such sums. If one tries to apply it to more general cases, however, calculations soon become unwieldy, and one realizes the necessity of inverting it by taking Gaussian sums as a starting point. The means for doing so were supplied, as early as 1827, by Jacobi, in a letter to Gauss [2, a] (cf. [2, b]). But Lebesgue, who in 1837 devoted two papers [3, a,b] to the case $n_0 = \cdots = n_r$ of equation (1), did not succeed in bringing out any striking result. The whole problem seems then to have been forgotten until Hardy and Littlewood found it necessary to obtain formulas for the number of solutions of the congruence $\sum_i x_i^n \equiv b \pmod{p}$ in their work on the singular series for Waring's problem [4]; they did so by means of Gaussian sums. More recently, Davenport and Hasse [5] have applied the same method to the case $r = 2, b = 0$ of equation (1) as well as to other similar equations; however, as they

Received by the editors October 2, 1948; published with the invited addresses for reasons of space and editorial convenience.

[1] Numbers in brackets refer to the bibliography at the end of the paper.

[2] It is surprising that this should have been overlooked by Dedekind and other authors who have discussed that conjecture (cf. M. Deuring, Abh. Math. Sem. Hamburgischen Univ. vol. 14 (1941) pp. 197–198).

were chiefly concerned with other aspects of the problem, and in particular with its relation to the Riemann hypothesis in function–fields,[3] the really elementary character of their treatment does not appear clearly.

As equations of type (1) have again recently been the subject of some discussion (cf. e.g. [6]), it may therefore serve a useful purpose to give here a brief but complete exposition of the topic. This will contain nothing new, except perhaps in the mode of presentation of the final results, which will lead to the statement of some conjectures concerning the numbers of solutions of equations over finite fields, and their relation to the topological properties of the varieties defined by the corresponding equations over the field of complex numbers.

We consider equation (1) over a finite field k with q elements; the a_i are in k, and not 0; the n_i are integers, which we assume to be >0 (only trifling modifications would be required if some were <0). We shall first discuss the case $b=0$.

Let therefore N be the number of solutions in k of the equation

$$a_0 x_0^{n_0} + a_1 x_1^{n_1} + \cdots + a_r x_r^{n_r} = 0.$$

For each i, let $d_i = (n_i, q-1)$ be the g.c.d. of n_i and $q-1$; for each i and each u in k, let $N_i(u)$ be the number of solutions of the equation $x^{n_i} = u$; $N_i(u)$ is 1 for $u=0$, and is otherwise equal to d_i or to 0 according as u is or is not a d_ith power in k. Put $L(u) = \sum_{i=0}^{r} a_i u_i$; we have

$$N = \sum_{L(u)=0} N_0(u_0)\cdots N_r(u_r), \tag{2}$$

where the sum is taken over all sets of values for the u_i satisfying $L(u)=0$, or, as we may say, over all points $(u) = (u_0,\dots,u_r)$ in the linear variety defined by $L(u)=0$ in the vector–space of dimension $r+1$ over k.

If k^* is the multiplicative group of all non–zero elements in k, we shall denote by the letter χ any character of k^*; as k^* is cyclic of order $q-1$, such a character is fully determined if one assigns its value at a generating element w of k^* (a "primitive root"), and this value may be any $(q-1)$th root of unity. Selecting such an element w once for all, we shall denote by χ_α the character of k^* determined by $\chi_\alpha(w) = e^{2\pi i\alpha}$, where α is a rational number satisfying $(q-1)\alpha \equiv 0 \pmod 1$. We also put $\chi_\alpha(0) = 0$ for $\alpha \not\equiv 0 \pmod 1$ and $\chi_\alpha(0) = 1$ for $\alpha \equiv 0 \pmod 1$. Then we have

$$N_i(u) = \sum_{\alpha} \chi_\alpha(u) \qquad (d_i\alpha \equiv 0 \pmod 1, 0 \le \alpha < 1).$$

In fact, for $u=0$, both sides have the value 1; for $u \neq 0$, the right–hand side can be written as $\sum_{\nu=0}^{d_i-1} \zeta^\nu$, with $\zeta = \chi_{1/d_i}(u)$; and ζ is then a d_ith root of unity, equal to 1 if and only if u is a d_ith power in k^*.

Using this in (2), we get:

$$N = \sum_{u,\alpha} \chi_{\alpha_0}(u_0)\cdots\chi_{\alpha_r}(u_r)$$
$$(L(u)=0; \quad d_i\alpha_i \equiv 0 \pmod 1, \quad 0 \le \alpha_i < 1).$$

As there are q^r points in $L(u)=0$, the terms in the above sum which correspond to $\alpha_0 = \cdots = \alpha_r = 0$, being all equal to 1, give a sum q^r. We now show that those terms for which some, but not all, of the α_i are 0, give a sum 0. In fact, consider e.g. those for which $\alpha_0,\dots,\alpha_{s-1}$ have given values, other than 0, and $\alpha_s = \cdots = \alpha_r = 0$, with $s \le r$;

[3] As to this, cf. Hasse, J. Reine Angew. Math. vol. 172 (1935) pp.37–54. I regret that I did not quote either of these papers, where the connection between various kinds of exponential sums and the Riemann hypothesis is quite clearly expressed, in my recent note on the same subject, Proc. Nat. Acad. Sci. U.S.A. vol. 34 (1948) pp. 204–207.

as there are q^{r-s} points (u) in the variety $L(u)=0$ for which $u_0,\dots,u_{s-1}$ have arbitrarily assigned values, the sum of those terms is

$$q^{r-s}\prod_{i=0}^{s-1}\left(\sum_{u_i}\chi_{\alpha_i}(u_i)\right),$$

and this is 0 since each factor is 0. This gives

$$N=q^r+\sum_{u,\alpha}\chi_{\alpha_0}(u_0)\dots\chi_{\alpha_r}(u_r)$$
$$(L(u)=0;\quad d_i\alpha_i\equiv 0\pmod 1,\quad 0<\alpha_i<1).$$

In this, we replace the u_i, respectively, by u_i/a_i, and get

$$N=q^r+\sum_{\alpha}\chi_{\alpha_0}(a_0^{-1})\cdots\chi_{\alpha_r}(a_r^{-1})\cdot S(\alpha)$$
$$(d_i\alpha_i\equiv 0\pmod 1, 0<\alpha_i<1),$$

if we put, for any values of α_i satisfying $(q-1)\alpha_i\equiv 0\pmod 1, \alpha_i\not\equiv 0\pmod 1$:

$$S(\alpha)=S(\alpha_0,\dots,\alpha_r)=\sum_{\sum u_i=0}\chi_{\alpha_0}(u_0)\dots\chi_{\alpha_r}(u_r).$$

As to the latter sum, the terms for which $u_0=0$ are 0, and we may exclude them; we may then put $u_i=u_0v_i$ $(1\le i\le r)$; the terms, in our sum, corresponding to given values of the v_i (satisfying $1+\sum_{i=1}^r v_i=0$) give

$$\chi_{\alpha_1}(v_1)\cdots\chi_{\alpha_r}(v_r)\sum_{u_0\neq 0}\chi_\beta(u_0),$$

with $\beta=\sum_{i=0}^r\alpha_i$, and this last sum is $q-1$ for $\beta\equiv 0\pmod 1$, and 0 otherwise, so that in the latter case $S(\alpha)$ is 0.

Let us therefore define, for any set of α_i satisfying the conditions

$$(q-1)\alpha_i\equiv 0,\qquad \alpha_i\not\equiv 0,\qquad \sum_{i=0}^r\alpha_i\equiv 0\pmod 1,$$

a number $j(\alpha)$ by the relation

$$j(\alpha)=\sum_{1+v_1+\cdots+v_r=0}\chi_{\alpha_1}(v_1)\cdots\chi_{\alpha_r}(v_r)$$
$$=\frac{1}{q-1}\sum_{u_0+\cdots+u_r=0}\chi_{\alpha_0}(u_0)\cdots\chi_{\alpha_r}(u_r).$$

In terms of the $j(\alpha)$, the number N of solutions of $\sum_{i=0}^r a_ix_i^{n_i}=0$ is now seen to be given by

$$N=q^r+(q-1)\sum_{\alpha}\chi_{\alpha_0}(a_0^{-1})\cdots\chi_{\alpha_r}(a_r^{-1})\cdot j(\alpha)$$
$$(d_i\alpha_i\equiv 0;\textstyle\sum\alpha_i\equiv 0\pmod 1; 0<\alpha_i<1). \tag{3}$$

The $j(\alpha)$ may be called the Jacobi sums for the field k; they were first introduced and studied, for the case of a prime field, by Jacobi [2, a,b], later by Stickelberger [7], and more recently by Davenport and Hasse [5]. They are closely related to the Gaussian sums for k:

$$g(\chi)=\sum_{x\in k}\chi(x)\psi(x),$$

where ψ is a character of the additive group of k, chosen once for all, and not everywhere equal to 1, and where χ is any one of the above defined multiplicative characters, other than χ_0. For the convenience of the reader, we shall briefly recall some of the known properties of these sums. In the first place, in the sum which defines $g(\chi)$, we may, as χ is not χ_0, restrict x to be $\neq 0$. Then we get

$$g(\chi)\overline{g}(\chi)=\sum_{y\neq 0}\sum_{x\neq 0}\chi(xy^{-1})\psi(x-y),$$

where we may substitute xy for x in the sum for x, and then interchange the order of summations:

$$g(\chi)\overline{g}(\chi) = \sum_{x\neq 0}\chi(x)\sum_{y\neq 0}\psi[(x-1)y].$$

As the sum of all values of ψ on k is 0, the second sum has the value $q-1$ for $x=1$, and -1 for $x\neq 1$; as the sum of all values of χ on k^* is 0, this gives

$$g(\chi)\overline{g}(\chi) = q. \tag{4}$$

Now, in the definition of $g(\chi)$, write tx for x with any $t\neq 0$ in k; this gives

$$g(\chi) = \chi(t)\sum_x \chi(x)\psi(tx),$$

hence, using (4), and interchanging x and t:

$$\chi(x) = \frac{g(\chi)}{q}\sum_t \overline{\chi}(t)\overline{\psi}(tx),$$

which is also true for $x=0$; this is the Fourier expansion of $\chi(x)$ on k according to the additive characters of k. Using this in the definition of $j(\alpha)$, we get

$$(q-1)\,j(\alpha) = q^{-r-1}\cdot g(\chi_{\alpha_0})\cdots g(\chi_{\alpha_r})\sum_t \overline{\chi}_{\alpha_0}(t_0)\cdots\overline{\chi}_{\alpha_r}(t_r)$$
$$\cdot\sum_{\sum u_i=0}\overline{\psi}\left(\sum_i t_i u_i\right).$$

But, in the additive groups of all vectors $(u)=(u_0,\dots,u_r)$, the vectors satisfying $\sum u_i = 0$ form a subgroup of q^r elements, on which $\overline{\psi}\left(\sum_i t_i u_i\right)$ is a character; the sum of the values of this character on the subgroup must therefore be either q^r, if the character has the constant value 1, or 0 otherwise. The former case occurs if and only if all the t_i are equal, since otherwise we can solve the equations $\sum u_i = 0$, $\sum t_i u_i = z$, where z is any element of k, e.g. one such that $\psi(z)\neq 1$. As we have $\sum \alpha_i \equiv 0 \pmod 1$ by the definition of $j(\alpha)$, this gives

$$j(\alpha) = \frac{1}{q}g(\chi_{\alpha_0})\cdots g(\chi_{\alpha_r}).$$

As a consequence, we have

$$j(\alpha)\overline{j}(\alpha) = q^{r-1},$$

and therefore

$$|N-q^r| \leq M(q-1)q^{(r-1)/2},$$

where M is the number of systems of rational numbers α_i satisfying

$$n_i\alpha_i \equiv 0, \quad \sum\alpha_i \equiv 0 \pmod 1, \quad 0<\alpha_i<1,$$

and is therefore an integer depending only upon the n_i.

From the above results, we can easily derive the number N_1 of solutions of the equation $\sum_{i=0}^r a_i x_i^{n_i}+1=0$. In fact, let N, as before, be the number of solutions of $\sum_{i=0}^r a_i x_i^{n_i} = 0$, and let N' be the number of solutions of $\sum_{i=0}^r a_i x_i^{n_i} + x_{r+1}^{q-1} = 0$. The previous results apply to the latter equation, with $d_{r+1} = n_{r+1} = q-1$. But, since x_{r+1}^{q-1} has the value 1, except for $x_{r+1}=0$, we have

$$N' = (q-1)N_1 + N.$$

This gives at once an expression for N_1; in order to write it more conveniently, we shall define the symbol $j(\alpha)$ even in the case when some, but not all, of the α_i are 0. Let the β_j be numbers, satisfying $(q-1)\beta_j\equiv 0$, $\sum_j\beta_j\equiv 0 \pmod 1$, and not all $\equiv 0 \pmod 1$;

assume that s of them are $\equiv 0 \pmod 1$, and let $\alpha_0, \dots, \alpha_r$ be the others, in any order; then we put $j(\beta) = (-1)^s j(\alpha)$. This being so, the formula for N_1 can be written as

$$N_1 = q^r + \sum_{\alpha} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1}) j\left(\alpha_0, \dots, \alpha_r, -\sum_{i=0}^{r} \alpha_i\right)$$
$$(d_i \alpha_i \equiv 0 \pmod 1, 0 < \alpha_i < 1),$$

and we get, as before:

$$|N_1 - q^r| \leq M_1 q^{r/2},$$

where M_1 is now given by

$$M_1 = (d_0 - 1) \cdots (d_r - 1) < n_0 n_1 \cdots n_r.$$

It is a matter of considerable interest to be able to compare the number of solutions of an equation (or, more generally, the number of rational points on an algebraic variety) in a given finite field and in all the extensions of finite degree of that field. This can easily be done, for the type of equations under consideration in this note, if we use a relation, due to Davenport and Hasse [5], between Gaussian sums in a finite field and in its extensions. We shall first give a brief account, in elementary language, of the proof of Davenport and Hasse for this relation.

Let k' be an extension of k, of degree ν; for y in k', let $N(y)$ and $T(y)$ denote the norm and the trace of y, respectively, over k. If w denotes, as before, a generator of the multiplicative group k^*, there is a generator z of k'^*, such that $N(z) = w$; then, if we denote, as before, by $\chi'_\alpha(y)$ the multiplicative character on k' determined by $\chi'_\alpha(z) = e^{2\pi i \alpha}$, we have, for $(q-1)\alpha \equiv 0 \pmod 1$, $\chi'_\alpha(y) = \chi_\alpha[N(y)]$. We also put $\psi'(y) = \psi[T(y)]$; this is an additive character of k', not everywhere equal to 1 since it is known that $T(y)$ maps k' *on* k. Let now $g'(\chi'_\alpha)$ be the Gaussian sum in k':

$$g'(\chi'_\alpha) = \sum_{y \in k'} \chi'_\alpha(y) \psi'(y).$$

The theorem of Davenport and Hasse is as follows:

$$-g'(\chi'_\alpha) = [-g(\chi_\alpha)]^\nu. \tag{5}$$

In order to prove this, consider the polynomials with coefficients in k, and highest coefficient 1; to every such polynomial

$$F(X) = X^n + c_1 X^{n-1} + \cdots + c_n,$$

of degree $n \geq 1$, we attach the number

$$\lambda(F) = \chi_\alpha(c_n) \psi(c_1).$$

For two such polynomials F_1, F_2, we have $\lambda(F_1 F_2) = \lambda(F_1)\lambda(F_2)$. If we also denote by $n(F)$ the degree of such a polynomial F, and by U an indeterminate, this gives the formal identity

$$1 + \sum_F \lambda(F) \cdot U^{n(F)} = \prod_P [1 - \lambda(P) \cdot U^{n(P)}]^{-1},$$

where the sum in the left–hand side is taken over *all* polynomials F over k, of degree ≥ 1, with highest coefficient 1, and the product in the right–hand side is taken over all *irreducible* polynomials P over k, with highest coefficient 1. As usual, this follows at once from the fact that every F can be expressed in a unique manner as product of powers of irreducible polynomials.

In the sum in the left hand–side, consider first the terms which correspond to polynomials $F(X) = X + c$ of degree 1; the sum of these terms is equal to $g(\chi_\alpha)U$. As to the sum of the terms corresponding to any given degree $n > 1$, it is 0, since, with the above notations, it is equal to

$$q^{n-2} \sum_{c_n} \chi_\alpha(c_n) \sum_{c_1} \psi(c_1) \cdot U^n,$$

where both sums are taken over k and are therefore 0. This gives

$$1+g(\chi_\alpha)U=\prod_P[1-\lambda(P)\cdot U^{n(P)}]^{-1}. \tag{6}$$

Similarly, if $F'(X)=X^n+d_1X^{n-1}+\cdots+d_n$ is a polynomial over k', we write

$$\lambda'(F')=\chi'_\alpha(d_n)\psi'(d_1),$$

and, taking another indeterminate U', get the formal identity

$$1+g'(\chi'_\alpha)U'=\prod_{P'}[1-\lambda'(P')\cdot U'^{n(P')}]^{-1} \tag{6'}$$

where the product is taken over all irreducible polynomials P' over k', with highest coefficient 1.

Now let P be as above; let P' be one of the irreducible factors of P over k'; let $-\xi$ be one of the roots of P'. Then ξ generates over k an extension $k(\xi)$ of degree $n=n(P)$, and over k' an extension $k'(\xi)$ of degree $n'=n(P')$; as $k'(\xi)$ is the composite of $k(\xi)$ and k', its degree over k must be the l.c.m. of the degree n of $k(\xi)$ over k, and of the degree v of k' over k, i.e. equal to nv/d if we write $d=(n,v)$. This gives $n'=n/d$; hence P has over k' exactly d irreducible factors, all of degree n/d. Moreover, if a and b are respectively the norm and the trace of ξ, taken in $k(\xi)$ relatively to k, we have

$$P(X)=X^n+bX^{n-1}+\cdots+a,$$

hence

$$\lambda(P)=\chi_\alpha(a)\psi(b).$$

Similarly, if a' and b' are the norm and the trace of ξ, taken in $k'(\xi)$ relatively to k', we have

$$\lambda'(P')=\chi'_\alpha(a')\psi'(b')=\chi_\alpha(Na')\psi(Tb'),$$

where Na' and Tb' are the norm of a' and the trace of b', taken in k' relatively to k; hence Na' and Tb' are respectively equal to the norm and to the trace of ξ, taken in $k'(\xi)$ relatively to k. We can therefore also obtain Na' by taking the norm of ξ in $k'(\xi)$ relatively to $k(\xi)$, this being equal to $\xi^{v/d}$, and then the norm of this in $k(\xi)$ relatively to k, which is $a^{v/d}$. Hence we have $Na'=a^{v/d}$, and similarly $Tb'=(v/d)b$, and therefore

$$\lambda'(P')=\lambda(P)^{v/d}.$$

Now, in the right–hand side of (6'), we can put together the d factors corresponding to all the irreducible factors of P over k'; if, moreover, we replace U' by U^v, we get

$$[1-\lambda(P)^{v/d}U^{vn/d}]^{-d},$$

which can also be written as

$$\prod_{\rho=0}^{v-1}[1-\lambda(P)\cdot(\zeta^\rho U)^n]^{-1}$$

where ζ is any primitive vth root of unity. This gives

$$\begin{aligned}1+g'(\chi'_\alpha)U^v&=\prod_{\rho=0}^{v-1}\prod_P[1-\lambda(P)\cdot(\zeta^\rho U)^{n(P)}]^{-1}\\&=\prod_{\rho=0}^{v-1}(1+g(\chi_\alpha)\zeta^\rho U)\\&=1+(-1)^{v+1}g(\chi_\alpha)^vU^v,\end{aligned}$$

which proves (5).

Now, N_v being the number of solutions of an equation of type (1), with or without constant term, over the extension of degree v of the ground–field k, it is easy, using the above results, to give a simple expression for the "generating power–series" for N_v, i.e.

for the formal power–series $\sum_1^\infty N_\nu U^\nu$; this turns out to be the expansion of a certain rational function in U. We shall, however, illustrate this idea by considering the case of the homogeneous equation

$$a_0 x_0^n + \cdots + a_r x_r^n = 0, \tag{7}$$

considered as the equation of a variety (without singular points) in the projective space P^r of dimension r over k. The number $\overline{N}$ of rational points over k, on that variety, is related to the number N of solutions of the same equation in affine space by $N = 1 + (q-1)\overline{N}$, so that, putting $d = (n, q-1)$, we get, from our earlier results:

$$\overline{N} = 1 + q + \cdots + q^{r-1} + \sum_{\alpha} \overline{\chi}_{\alpha_0}(a_0) \cdots \overline{\chi}_{\alpha_r}(a_r) \cdot j(\alpha)$$
$$(d\alpha_i \equiv 0, \quad \sum \alpha_i \equiv 0 \pmod 1;\ 0 < \alpha_i < 1).$$

Now call $\overline{N}_\nu$ the number of rational points, on the variety defined by (7), over the extension k_ν of k of degree ν; we shall calculate the series $\sum_1^\infty \overline{N}_\nu U^{\nu-1}$.

In order to do this, consider any set of rational numbers $\alpha_0, \ldots, \alpha_r$ satisfying $n\alpha_i \equiv 0$, $\sum \alpha_i \equiv 0 \pmod 1$, $0 < \alpha_i < 1$. For this set, let $\mu = \mu(\alpha)$ be the smallest integer such that $(q^\mu - 1)\alpha_i \equiv 0 \pmod 1$ for $0 \le i \le r$; then the extensions k_ν of k such that $(q^\nu - 1)\alpha_i \equiv 0 \pmod 1$ are those for which ν is a multiple of μ, and those only. Choosing a primitive root in k_μ, we can now, as before, define in k_μ the characters χ_{α_i}, the Gaussian sums $g(\chi_{\alpha_i})$, and the Jacobi sum

$$j(\alpha) = \frac{1}{q^\mu} g(\chi_{\alpha_0}) \cdots g(\chi_{\alpha_r}).$$

Furthermore, if we denote by $\chi'_{\alpha_i}, g'(\chi'_{\alpha_i})$ and $j'(\alpha)$ the corresponding characters and sums for the extension $k' = k_{\lambda\mu}$ of k of degree $\lambda\mu$, where λ is any integer, we get from our earlier results:

$$\chi'_{\alpha_i}(a_i) = \chi_{\alpha_i}(a_i)^\lambda,\ g'(\chi'_{\alpha_i}) = (-1)^{\lambda-1} g(\chi_{\alpha_i})^\lambda,\ j'(\alpha) = (-1)^{(\lambda-1)(r-1)} j(\alpha)^\lambda.$$

Then we get:

$$\sum_1^\infty \overline{N}_\nu U^{\nu-1} = -\sum_{h=0}^{r-1} \frac{d}{dU} \log(1 - q^h U)$$
$$+ (-1)^r \sum_{\alpha} \frac{1}{\mu(\alpha)} \frac{d}{dU} \log[1 - C(\alpha) \cdot U^{\mu(\alpha)}] \tag{8}$$
$$(n\alpha_i \equiv 0, \sum \alpha_i \equiv 0 \pmod 1; 0 < \alpha_i < 1).$$

where we have put

$$C(\alpha) = (-1)^{r-1} \overline{\chi}_{\alpha_0}(a_0) \cdots \overline{\chi}_{\alpha_r}(a_r) \cdot j(\alpha).$$

Furthermore, it is easily seen that $C(q\alpha) = C(\alpha)$, since $x \to x^q$ is an automorphism of k_μ which leaves the a_i invariant. Therefore, in the last sum in (8), the $\mu(\alpha)$ terms corresponding to the set $(\alpha) = (\alpha_0, \ldots, \alpha_r)$ and to the sets $(q^\rho \alpha)$ for $1 \le \rho \le \mu - 1$ are all equal, so that, putting them together, we can make the denominator $\mu(\alpha)$ disappear.

Let A be the number of solutions, in rational numbers α_i, of the system $n\alpha_i \equiv 0$, $\sum \alpha_i \equiv 0 \pmod 1$, $0 < \alpha_i < 1$. Then one finds[4] that the Poincaré polynomial (in the sense of combinatorial topology) of the variety defined, in the projective space P^r over complex numbers, by an equation of the form

$$c_0 x_0^n + \cdots + c_r x_r^n = 0$$

is equal to

$$\sum_{h=0}^{r-1} X^{2h} + A \cdot X^{r-1}.$$

[4] As obligingly communicated to me by P. Dolbeault in Paris.

This, and other examples which we cannot discuss here, seem to lend some support to the following conjectural statements, which are known to be true for curves, but which I have not so far been able to prove for varieties of higher dimension.

Let V be a variety without singular points, of dimension n, defined over a finite field k with q elements. Let N_ν be the number of rational points on V over the extension k_ν of k of degree ν. Then we have

$$\sum_1^\infty N_\nu U^{\nu-1} = \frac{d}{dU}\log Z(U),$$

where $Z(U)$ is a rational function in U, satisfying a functional equation

$$Z\left(\frac{1}{q^n U}\right) = \pm q^{n\chi/2} U^\chi Z(U),$$

with χ equal to the Euler–Poincaré characteristic of V (intersection–number of the diagonal with itself on the product $V \times V$).

Furthermore, we have:

$$Z(U) = \frac{P_1(U)P_3(U)\cdots P_{2n-1}(U)}{P_0(U)P_2(U)\cdots P_{2n}(U)},$$

with $P_0(U) = 1 - U$, $P_{2n}(U) = 1 - q^n U$, and, for $1 \le h \le 2n-1$:

$$P_h(U) = \prod_{i=1}^{B_h}(1 - \alpha_{hi}U)$$

where the α_{hi} are algebraic integers of absolute value $q^{h/2}$.

Finally, let us call the degrees B_h of the polynomials $P_h(U)$ the *Betti numbers* of the variety V; the Euler–Poincaré characteristic χ is then expressed by the usual formula $\chi = \sum_h (-1)^h B_h$. The evidence at hand seems to suggest that, if $\overline{V}$ is a variety without singular points, defined over a field K of algebraic numbers, the Betti numbers of the variety $V_\mathfrak{p}$, derived from $\overline{V}$ by reduction modulo a prime ideal $\mathfrak{p}$ in K, are equal to the Betti numbers of $\overline{V}$ (considered as a variety over complex numbers) in the sense of combinatorial topology, for all except at most a finite number of prime ideals $\mathfrak{p}$. For instance, consider the Grassmann variety $G_{m,r}$, the points of which are the r–dimensional linear varieties in a projective m–dimensional space, over a field with q elements. The number of rational points on the variety is easily seen to be $F(q)$, where F is the polynomial defined by

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

Then, if the above conjectures are true, the Poincaré polynomial of the Grassmann variety $G_{m,r}$ over complex numbers must be $F(X^2)$. This is indeed so, as can easily be verified from the well–known results of Ehresmann [8].[5]

REFERENCES

[1] C. F. Gauss. *Werke.* (a) vol. I, pp. 445–449; (b) vol. II, pp. 67–92; (c) vol. X_1, p. 571.
[2] C. G. Jacobi. *Gesammelte Werke.* (a) vol. VII, pp. 393–400; (b) vol. VI, pp. 254–274.
[3] V. A. Lebesgue. *J. Math. Pures Appl.* (a) vol. 2 (1837) pp. 253–292, (b) vol. 3 (1838) pp. 113–144.
[4] G. H. Hardy and J. E. Littlewood. *Math. Zeit.* vol. 12 (1922) pp. 161–188.
[5] H. Davenport and H. Hasse. *J. Reine Angew. Math.* vol. 172 (1935) pp. 151–182.
[6] L. K. Hua and H. S. Vandiver. *Proc. Nat. Acad. Sci. U.S.A.* vol. 34 (1948) pp. 258–263.
[7] L. Stickelberger. *Math. Ann.* vol. 37 (1890) pp. 321–367.
[8] Ch. Ehresmann. *Ann. of Math.* vol. 35 (1934) pp. 396–443.

THE UNIVERSITY OF CHICAGO

[5] *Added in proof.* Results, substantially identical to our formula (3), have just been published by L. K. Hua and H. S. Vandiver, Proc. Nat. Acad. Sci. U.S.A. vol. 35 (1949) pp. 94–99.