[5] Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantische Gleichungen*, 8de Skand. Math.-Kongress, Stockholm (1934), стр. 163-188.

[6] Б. Н. Делоне и Д. К. Фаддеев, *Теория иррациональностей третьей степени*, Москва-Ленинград 1940.

[7] L. J. Mordell, *On the integer solutions of the equation* $ey^2 = ax^3+bx^2+cx+d$, Proc. Lond. Math. Soc. 21, 6 (1923), стр. 415-419.

Reçu par la Rédaction le 26. 8. 1966

ACTA ARITHMETICA
XII (1967)

The number of solutions of a system of equations in a finite field

by

CHARLES WELLS (Cleveland, Ohio)

1. Introduction. Let GF(q), where $q = p^e$, p prime, denote the finite field of order q. Let $k_1, \ldots, k_n, s_1, \ldots, s_t$ denote positive integers, $a_1, \ldots, a_n$ nonzero elements of GF(q), and b_{ij} $(i = 1, 2, \ldots, n, j = 1, 2, \ldots, t)$ arbitrary elements of GF(q). Let

$$c_i = \sum_{j=1}^{t} b_{ij} \qquad (i = 1, 2, \ldots, n). \tag{1.1}$$

We consider the number N of solutions in GF(q) of the system of equations

$$y_i^{k_i} = a_i + \sum_{j=1}^{t} b_{ij} x_j^{s_j} \qquad (i = 1, 2, \ldots, n) \tag{1.2}$$

where for c_i as in (1.1)

$$c_i \neq 0 \qquad (i = 1, 2, \ldots, n) \tag{1.3}$$

and

$$a_i c_k \neq a_k c_i \qquad (i \neq k, i, k = 1, 2, \ldots, n). \tag{1.4}$$

L. Carlitz and the author [1] proved that for $t = 1$, $N = q+O(q^{1/2})$ as $q \to \infty$. Here the following generalization is proved:

THEOREM 1. *The number of solutions of the system* (1.1) *satisfies*

$$N = q^t + O(q^{t-1/2}) \qquad (q \to \infty).$$

As in [1] the proof uses the Riemann hypothesis for an algebraic function field over GF(q), proved by A. Weil [3]. If we use a weaker result of Davenport [2], we have

$$N = q^t + O(q^{t-\delta})$$

for some $\delta > 0$.

2. Preliminary lemmas. We shall use the following three lemmas. The first two are well known. The third is proved in [1].

Let χ, ψ denote characters of the multiplicative group of GF(q) and put

$$e(a) = e^{2\pi i t(a)} \qquad (a \in \mathrm{GF}(q)), \tag{2.1}$$

where

$$t(a) = a + a^p + \ldots + a^{p^{e-1}}.$$

Also put

$$\tau(\chi) = \sum_a e(a)\chi(a).$$

Then we have

LEMMA 1. *The quantity*

$$\begin{aligned} |\tau(\chi)| &= q^{1/2}, \\ \tau(\chi_0) &= -1, \end{aligned} \qquad (\chi \neq \chi_0),$$

where χ_0 denotes the principal character.

Let $t > 0$ and put

$$S(a, t) = \sum_b e(ab^t) \qquad (a \in \mathrm{GF}(q)).$$

LEMMA 2. *For $a \neq 0$,*

$$S(a, t) = \sum_{\psi} \psi(a)\tau(\overline{\psi})$$

where the summation is over all nonprincipal characters such that $\psi^t = \psi_0$.

Now let $r > 0$ and $h_1, \ldots, h_r$ be arbitrary positive integers. For $i = 1, \ldots, r$ let ψ_i denote a character satisfying

$$\psi_i^{h_i} = \psi_0 \qquad (i = 1, \ldots, r). \tag{2.2}$$

For $r > 1$ put

$$\begin{aligned} T_r &= T_r(c_1, \ldots, c_r) \\ &= \sum_{\lambda_1, \ldots, \lambda_r} e(c_1\lambda_1 + \ldots + c_r\lambda_r)\, \psi_1(\lambda_1)\, \psi_2(\lambda_2) \ldots \psi_r(\lambda_r) \end{aligned}$$

where the summation is over all $\lambda_1, \ldots, \lambda_r \in \mathrm{GF}(q)$ for which $\lambda_1 + \ldots + \lambda_r = 0$, the ψ_i are any nonprincipal characters satisfying (2.2), and $c_1, \ldots, c_r \in \mathrm{GF}(q)$. We then have

LEMMA 3. *If $\psi_1\psi_2 \ldots \psi_r \neq \psi_0$ or if $c_1, \ldots, c_r$ are not all equal, then*

$$T_r(c_1, \ldots, c_r) = O(q^{(r-1)/2}) \qquad (r \geqslant 2).$$

3. Proof of Theorem 1. Let L be the set of n-tuples $(\lambda_1, \ldots, \lambda_n)$, X the set of t-tuples $(x_1, \ldots, x_t)$, and Y the set of n-tuples $(y_1, \ldots, y_n)$, of elements of GF(q). Then

$$\begin{aligned} q^n N &= \sum_{L,X,Y} e\Big[\sum_{i=1}^{n} \lambda_i \Big(a_i + \sum_{j=1}^{t} b_{ij} x_j^{s_j} - y_i^{k_i}\Big)\Big] \\ &= \sum_{L} e\Big(\sum_{i=1}^{n} \lambda_i a_i\Big) \sum_{X,Y} e\Big(\sum_{i=1}^{n} \sum_{j=1}^{t} \lambda_i b_{ij} x_j^{s_j}\Big) e\Big(-\sum_{i=1}^{n} \lambda_i y_i^{k_i}\Big). \end{aligned} \tag{3.1}$$

Let L_r be the set of r-tuples $(\lambda_1, \ldots, \lambda_r)$ of *nonzero* elements of GF(q), and let Y_r be the set of $(y_1, \ldots, y_r)$ of *arbitrary* elements of GF(q). Then (3.1) contains $\binom{n}{r}$ terms like

$$q^{n-r} \sum_{L_r} e\Big(\sum_{i=1}^{r} \lambda_i a_i\Big) \sum_{X,Y_r} e\Big(\sum_{i=1}^{r} \sum_{j=1}^{t} \lambda_i b_{ij} x_j^{s_j}\Big)\, e\Big(-\sum_{i=1}^{r} \lambda_i y_i^{k_i}\Big) \tag{3.2}$$

where $a_1, \ldots, a_r$ and $b_{1j}, \ldots, b_{rj}$ $(j = 1, \ldots, t)$ have been obtained from $a_1, \ldots, a_n$ and $b_{1j}, \ldots, b_{nj}$ by renumbering (in a different way for each of the $\binom{n}{r}$ occurrences) in such a way that, after renumbering, $\lambda_1\lambda_2 \ldots \lambda_r \neq 0$, $\lambda_{r+1} = \ldots = \lambda_n = 0$. Conditions (1.3) and (1.4), with n replaced by r, now hold for $a_1, \ldots, a_r$ and $b_{1j}, \ldots, b_{rj}$, since these conditions are symmetrical.

We now decompose (3.2) further. After another renumbering, if necessary, we have for some u, $0 \leqslant u \leqslant t$,

$$\sum_{i=1}^{r} \lambda_i b_{ij} \begin{cases} \neq 0 & (j = 1, \ldots, u), \\ = 0 & (j = u+1, \ldots, t). \end{cases} \tag{3.3}$$

Let X_u be the set of u-tuples $(x_1, \ldots, x_u)$ of arbitrary elements of GF(q). Then (3.2) is composed of $\binom{t}{u}$ terms (each the result of a different renumbering) of the form (3.4) for each $u = 0, 1, \ldots, t$.

$$\begin{aligned} q^{n-r+t-u} \sum_{L_r} e\Big(\sum_{i=1}^{r} \lambda_i a_i\Big) \sum_{X_u} e\Big(\sum_{i=1}^{r} \sum_{j=1}^{u} \lambda_i b_{ij} x_j^{s_j}\Big) \sum_{Y_r} e\Big(-\sum_{i=1}^{r} \lambda_i y_i^{k_i}\Big) \\ = q^{n-r+t-u} M(r, u). \end{aligned} \tag{3.4}$$

Now

$$M(r, u) = \sum_{L_r} e\Big(\sum_{i=1}^{r} \lambda_i a_i\Big) \prod_{j=1}^{u} S\Big(\sum_{i=1}^{r} \lambda_i b_{ij}, s_j\Big) \prod_{i=1}^{r} S(-\lambda_i, k_i)$$

which by Lemma 2 is

$$\sum_{L_r} e\Big(\sum \lambda_i a_i\Big) \prod_{j=1}^{u} \sum_{\varphi_u} \varphi_j\Big(\sum \lambda_i b_{ij}\Big)\, \tau(\varphi_j) \prod_{i=1}^{r} \sum_{\varphi_u} \psi_i(-\lambda_i)\, \tau(\overline{\psi}_i)$$

which becomes

$$(3.5)\qquad \sum_{\Phi_j,\Psi_r}\prod_{i=1}^{r}\tau(\psi_i)\prod_{j=1}^{u}\tau(\varphi_j)\sum_{L_r}e\Big(\sum_{i=1}^{r}\lambda_i a_i\Big)\prod_{i=1}^{r}\psi_i(-\lambda_i)\prod_{j=1}^{u}\psi_j\Big(\sum_{i=1}^{r}\lambda_i b_{ij}\Big),$$

where Ψ_r ranges over the r-tuples $(\psi_1, \dots, \psi_r)$ of nonprincipal characters such that $\psi_i^{k_i} = \psi_0 (i = 1, \dots, r)$, and Φ_u ranges over the u-tuples $(\varphi_1, \dots, \varphi_r)$ such that $\varphi_j^{s_j} = \varphi_0$ $(j = 1, \dots, u)$.

The inner sum of (3.5) is

$$(3.6)\qquad \prod_{i=1}^{r}\psi_i(c_i^{-1})T_{r+u}(-c_1^{-1}a_1, -c_2^{-1}a_2, \dots, -c_r^{-1}a_r, 0, \dots, 0)$$

where now $c_i = \sum_{j=1}^{u} b_{ij}\,(i = 1, \dots, r)$ and $c_i \neq 0$ $(i = 1, \dots, r)$ by (1.3) and the fact that the c_i are symmetrical in the b_{ij} so that the renumbering is irrelevant. Now the first r terms $-c_i^{-1}a_i$ $(i = 1, \dots, r)$ are all different, so by Lemma 3,

$$M(r, u) = O(q^{\frac{1}{2}(r+u)+\frac{1}{2}(r+u-1)}) = O(q^{r+u-1/2}) \quad (0 < r \leqslant h),$$

but

$$M(0, u) = q^u.$$

Hence

$$q^n N = q^{n+t} + \sum_{u=0}^{t-1} O(q^{n+u}) + \sum_{r=1}^{n}\sum_{u=0}^{t} q^{n+t-r-u}O(q^{r+u-1/2}),$$

so that

$$N = q^t + O(q^{t-1/2})$$

as was to be proved.

References

[1] L. Carlitz and C. Wells, *The number of solutions of a special system of equations*, Acta Arith. 12 (1966), pp. 77-84.

[2] H. Davenport, *On character sums in finite fields*, Acta Math. 71 (1939), pp. 99-121.

[3] A. Weil, *On the Riemann hypothesis in function fields*, Proc. Nat. Acad. Sci. 27(1941), pp. 97-98.

Reçu par la Rédaction le 8. 9. 1966

ACTA ARITHMETICA
XII (1967)

Corrigendum to the paper "On a theorem of Bauer and some of its applications"

(Acta Arithmetica 11 (1966), pp. 333-344)

by

A. Schinzel (Warszawa)

In Theorem 4 (p. 335) the assumption must be added that the multiplicity of each zero and pole of $g(x)$ is relatively prime to n/p. Without this assumption the theorem is false, as the example (1) p. 115 of the paper "Polynomials of certain special types" (these Acta 9 (1964), pp. 107-116) shows.