References

[1] L. Carlitz, *Some arithmetic properties of a special sequence of polynomials*, Duke Math. Journ. 26 (1959), pp. 583-590.

[2] L. E. Dickson, *History of the theory of numbers*, vol. 1, Washington 1919.

[3] E. Hecke, *Theorie der algebraischen Zahlen*, Leipzig 1923.

Reçu par la Rédaction le 12. 2. 1962

ACTA ARITHMETICA
VII (1962)

Solvability of certain equations in a finite field *

by

L. CARLITZ (Durham, N. C.)

1. Let $q = p^n$, where p is a prime, and let $GF(q)$ denote the finite field of order q. Schwarz [4] has given an elegant proof of the following theorem. *If $k|p-1$, if $a_1, \ldots, a_k$ are non-zero numbers of $GF(q)$ and a is an arbitrary number of the field, then the equation*

$$a_1 x_1^k + \ldots + a_k x_k^k = a$$

has at least one solution in the field.

Using the same method, the writer [2] has proved the following theorems.

THEOREM 1. *Let $k|p-1$ and let $a_1, \ldots, a_k$ be non-zero numbers of $GF(q)$. Let $g(x_1, \ldots, x_k)$ be an arbitrary polynomial with coefficients in $GF(q)$ of degree less than k. Then the equation*

$$a_1 x_1^k + \ldots + a_k x_k^k = g(x_1, \ldots, x_k)$$

has at least one solution in the field.

THEOREM 2. *If $f(x_1, \ldots, x_k)$ is homogeneous of degree k while $g(x_1, \ldots, x_k)$ is arbitrary of degree less than k, and*

$$\sum_{x_1, \ldots, x_k \in GF(q)} \{f(x_1, \ldots, x_k)\}^{q-1} \neq 0\,, \tag{1.1}$$

then the equation

$$f(x_1, \ldots, x_k) = g(x_1, \ldots, x_k) \tag{1.2}$$

has at least one solution in the field. Alternatively the condition (1.1) may be replaced by the equivalent statement that the number of solutions of the equation

$$f(x_1, \ldots, x_k) = 0 \tag{1.3}$$

is not divisible by p.

By the degree of $g(x_1, \ldots, x_k)$ is understood the total degree.

---

* Supported in part by National Science Foundation grant G 16485.

In Theorems 1 and 2 it is possible that only the trivial solution $(0, \ldots, 0)$ occurs. We may however state the following theorem which supplements Theorem 2.

THEOREM 3. *Let $f(x_1, \ldots, x_k)$ be homogeneous of degree k while $g(x_1, \ldots, x_k)$ is arbitrary of degree less than k and $g(0, \ldots, 0) = 0$. Also let*

$$\sum_{x_1, \ldots, x_k \in GF(q)} \{f(x_1, \ldots, x_k)\}^{q-1} = 0 \tag{1.4}$$

(so that the number of solutions of (1.3) is divisible by p). Then the number of solutions of (1.2) is divisible by p. It follows that (1.2) has at least $p-1$ non-trivial solutions.

This result may be compared with Warnung's refinement [5] of Chevalley's theorem on systems of equations in a finite field [3].

The proof of Theorem 3 is very simple. If the theorem is false then

$$\sum_{x_1, \ldots, x_k \in GF(q)} \{f(x_1, \ldots, x_k) - g(x_1, \ldots, x_k)\}^{q-1} \neq 0 . \tag{1.5}$$

Put

$$\{f(x_1, \ldots, x_k) - g(x_1, \ldots, x_k)\}^{q-1} = f^{q-1}(x_1, \ldots, x_k) + F(x_1, \ldots, x_k) ,$$

so that

$$\deg F(x_1, \ldots, x_k) < k(q-1) . \tag{1.6}$$

Now it is familiar that for $m \geqslant 1$

$$\sum_{x \in GF(q)} x^m = \begin{cases} -1 & (q-1 \mid m) , \\ 0 & (\text{otherwise}) . \end{cases}$$

It follows that for any polynomial that satisfies (1.6) we have

$$\sum_{x_1, \ldots, x_k \in GF(q)} F(x_1, \ldots, x_k) = 0 .$$

Hence (1.5) becomes

$$\sum_{x_1, \ldots, x_k \in GF(q)} \{f(x_1, \ldots, x_k)\}^{q-1} \neq 0 ,$$

which contradicts (1.4). Hence the number of solutions of (1.2) is a multiple of p; since the trivial solution is certainly present, there must be at least $p-1$ non-trivial solutions.

2. Theorem 3 can be extended to system of equations as follows.

THEOREM 4. *Let $f_j(x_1, \ldots, x_k)$ be homogeneous of degree k_j while $g_j(x_1, \ldots, x_k)$ is arbitrary of degree less than k_j $(j = 1, \ldots, r)$ and let*

$$g_j(0, \ldots, 0) = 0 \quad (j = 1, \ldots, r) .$$

Also let

$$\sum_{x_1, \ldots, x_k \in GF(q)} \prod_{j=1}^{r} \{f_j(x_1, \ldots, x_k)\}^{q-1} = 0 . \tag{2.1}$$

Then if

$$\sum_{j=1}^{r} k_j = k , \tag{2.2}$$

the number of solutions of the system

$$f_j(x_1, \ldots, x_k) = g_j(x_1, \ldots, x_k) \quad (j = 1, \ldots, r) \tag{2.3}$$

is divisible by p. It follows that (2.2) has at least $p-1$ non-trivial solutions.

Proof. Clearly the product

$$\prod_{j=1}^{r} \{1 - (f_j(x_1, \ldots, x_k) - g_j(x_1, \ldots, x_k))^{q-1}\}$$

is equal to 1 or 0 accordingly as $(x_1, \ldots, x_k)$ is or is not a solution of (2.3). Hence if the theorem is false we have

$$\sum_{x_1, \ldots, x_k} \prod_{j=1}^{r} \{1 - (f_j(x_1, \ldots, x_k) - g_j(x_1, \ldots, x_k))^{q-1}\} \neq 0 . \tag{2.4}$$

Expanding the summand it is evident that

$$\prod_{j=1}^{r} \{1 - (f_j(x_1, .., x_k) - g_j(x_1, .., x_k))^{q-1}\} = (-1)^r \prod_{j=1}^{r} (f_j(x_1, \ldots, x_k))^{q-1} + F(x_1, \ldots, x_k) ,$$

where

$$\deg F(x_1, \ldots, x_k) < k(q-1) .$$

It follows as in the proof of Theorem 3 that

$$\sum_{x_1, \ldots, x_k} F(x_1, \ldots, x_k) = 0 .$$

Thus (2.4) becomes

$$(-1)^r \sum_{x_1, \ldots, x_k} \prod_{j=1}^{r} (f_j(x_1, \ldots, x_k))^{q-1} = 0 ,$$

which contradicts (2.1). This completes the proof of the theorem.

The condition (2.1) is equivalent to the statement that the number of solutions of the system

$$f_j(x_1, \ldots, x_k) = 0 \quad (j = 1, \ldots, r) \tag{2.5}$$

is divisible by p. We observe that we have made no essential use of the homogeneity of the $f_j(x_1, \dots, x_k)$ but merely of the fact that

$$\deg f_j(x_1, \dots, x_k) \leqslant k_j \qquad (j = 1, \dots, r).$$

However for the last sentence in the statement of Theorem 4 we do require the fact that the system (2.5) possesses the trivial solution $(0, \dots, 0)$.

We may accordingly replace Theorem 4 by the following slightly more general result.

THEOREM 5. *Let $f_j(x_1, \dots, x_k)$ be of degree $\leqslant k_j$ while $g_j(x_1, \dots, x_k)$ is of degree $< k_j$ $(j = 1, \dots, r)$ and let*

$$f_j(0, \dots, 0) = g_j(0, \dots, 0) = 0 \qquad (j = 1, \dots, r).$$

Also assume that the number of solutions of the system

$$f_j(x_1, \dots, x_k) = 0 \qquad (j = 1, \dots, r)$$

is divisible by p. Then if

$$\sum_{j=1}^{r} k_j = k,$$

the number of solutions of the system

$$f_j(x_1, \dots, x_k) = g_j(x_1, \dots, x_k) \qquad (j = 1, \dots, r) \tag{2.6}$$

is divisible by p. It follows that the system (2.6) has at least $p-1$ non-trivial solutions.

3. In place of (2.1) we may assume that

$$\sum_{x_1, \dots, x_k} \prod_{j=1}^{r} \{1 - (f_j(x_1, \dots, x_k))^{q-1}\} \neq 0, \tag{3.1}$$

which is equivalent to the assumption that the number of solutions of the system

$$f_j(x_1, \dots, x_k) = 0 \qquad (j = 1, \dots, r) \tag{3.2}$$

is not divisible by p. We now get

THEOREM 6. *Let $f_j(x_1, \dots, x_k)$ be of degree $\leqslant k_j$ while $g_j(x_1, \dots, x_k)$ is of degree $< k_j$ $(j = 1, \dots, r)$ and assume that the number of solutions of the system (3.2) is not divisible by p. Then if*

$$\sum_{j=1}^{r} k_j = k,$$

the number of solutions of

$$f_j(x_1, \dots, x_k) = g_j(x_1, \dots, x_k) \qquad (j = 1, \dots, r) \tag{3.3}$$

is not divisible by p. It follows that (3.3) has at least one solution.

Proof. If the theorem is false we have

$$\sum_{x_1, \dots, x_k} \prod_{j=1}^{r} \{1 - (f_j(x_1, \dots, x_k) - g_j(x_1, \dots, x_k))^{q-1}\} = 0.$$

Expanding the left member we get

$$\sum_{x_1, \dots, x_k} \prod_{j=1}^{r} \{1 - (f_j(x_1, \dots, x_k))^{q-1}\} = 0,$$

which contradicts the assumption concerning the number of solutions of (3.2).

As we have seen in the proof of Theorem 4,

$$\sum_{x_1, \dots, x_k} \prod_{j=1}^{r} \{1 - (f_j(x_1, \dots, x_k))^{q-1}\} \equiv N_0 \pmod{p}, \tag{3.4}$$

where N_0 denotes the number of solutions of the system (3.2). Similarly

$$\sum_{x_1, \dots, x_k} \prod_{j=1}^{r} \{1 - (f_j(x_1, \dots, x_k) - g_j(x_1, \dots, x_k))^{q-1}\} \equiv N \pmod{p},$$

where N denotes the number of solutions of the system (3.3).

We have therefore the following

THEOREM 7. *Let $f_j(x_1, \dots, x_k)$ be of degree $\leqslant k_j$ while $g_j(x_1, \dots, x_k)$ is of degree $\leqslant k_j$, where*

$$\sum_{j=1}^{r} k_j = k.$$

Let N_0 denote the number of solutions of (3.2) and N the number of solutions of (3.3). Then

$$N \equiv N_0 \pmod{p}. \tag{3.5}$$

If the f_j are polynomials in $k-1$ or fewer indeterminates it is evident that (3.4) becomes

$$N_0 \equiv 0 \pmod{p}.$$

We accordingly get the following corollary of Theorem 7.

THEOREM 8. *Let the f_j in Theorem 7 be polynomials in at most $k-1$ indeterminates. Then the number of solutions of (3.3) is divisible by p. In particular if*

$$f_j(0, \dots, 0) - g_j(0, \dots, 0) = 0 \qquad (j = 1, \dots, r),$$

then the system (3.3) has at least $p-1$ non-trivial solutions.

4. We shall now discuss a few special cases. To begin with let

(4.1) $$y_j = \sum_{s=1}^{k} a_{js} x_s \quad (a_{js} \in GF(q),\ j = 1, \ldots, s)$$

be n linear forms with coefficients in $GF(q)$ and put

(4.2) $$f_j(x_1, \ldots, x_k) = \prod_{s=k_j+1}^{k_{j+1}} y_s \quad (j = 1, \ldots, r),$$

where

$$k_0 = 0,\ k_1 > 0, \ldots, k_r > 0, \quad \sum_{j=1}^{r} k_j = k.$$

Now assume that the y_j are linearly independent. Then the number of solutions of the system

(4.3) $$f_j(x_1, \ldots, x_k) = 0$$

is equal to

(4.4) $$\prod_{j=1}^{r} \left(q^{k_j} - (q-1)^{k_j}\right).$$

To prove this we observe that since the y_j are linearly independent one may, by means of the linear transformation (4.1), define the f_j by

$$f_j(x_1, \ldots, x_k) = \prod_{s=k_j+1}^{k_{j+1}} x_s \quad (j = 1, \ldots, r).$$

Thus it suffices to show that the number of solutions of

(4.5) $$x_1 x_2 \ldots x_k = 0$$

is equal to

$$q^k - (q-1)^k.$$

This follows at once from the fact that number of solutions of (4.5) is equal to q^k minus the number of solutions of

$$x_1 x_2 \ldots x_k \neq 0.$$

If in the next place the y_j are linearly dependent it follows (compare Theorem 8) that the number of solutions of (4.3) is divisible by p. We may state

THEOREM 9. *Let $f_j(x_1, \ldots, x_k)$ be defined by* (4.1) *and* (4.2) *and let $g_j(x_1, \ldots, x_k)$ be arbitrary polynomials of degree $< k_j$. Also let N denote the number of solutions of the system*

(4.6) $$f_j(x_1, \ldots, x_k) = g_j(x_1, \ldots, x_k) \quad (j = 1, \ldots, r).$$

Then if the y_j are linearly independent,

(4.7) $$N \equiv (-1)^{r+k} \pmod{p},$$

while if the y_j are linearly dependent,

(4.8) $$N \equiv 0 \pmod{p}.$$

In the latter case, if also

$$g_j(0, \ldots, 0) = 0 \quad (j = 1, \ldots, r),$$

it follows that (4.6) *has at least $p-1$ non-trivial solutions.*

Returning to (4.1) and (4.2), another case of interest is that in which the a_{js} lie in some $GF(q^t)$ but the coefficients of f_j are in $GF(q)$. For some properties of such *factorable* polynomials see [1]. We shall however consider only the following special case. Let θ denote a primitive number of $GF(q^n)$ and put

$$f(x_1, \ldots, x_n) = \prod_{j=0}^{n-1} \left(x_1 + \theta^{q^j} x_2 + \ldots + \theta^{(n-1)q^j} x_n\right);$$

f is called a *norm-form*. It follows that the only solution (in $GF(q)$) of

$$f(x_1, \ldots, x_n) = 0$$

is the trivial solution.

We now define the f_j as follows: f_1 is a norm-form in $x_1, \ldots, x_{k_1}$; f_2 is a norm-form in $x_{k_1+1}, \ldots, x_{k_2}$ and so on. It follows that the only solution of the system

$$f_j(x_{k_j+1}, \ldots, x_{k_{j+1}}) = 0 \quad (j = 1, \ldots, r)$$

is the trivial solution.

We may state

THEOREM 10. *Let $f_j(x_{k_j+1}, \ldots, x_{k_{j+1}})$ denote norm-forms in the indicated indeterminates and let $g_j(x_1, \ldots, x_k)$ be arbitrary polynomials of degree $< k_j$. Then the number of solutions of the system*

(4.9) $$f_j(x_{k_j+1}, \ldots, x_{k_{j+1}}) = g_j(x_1, \ldots, x_k) \quad (j = 1, \ldots, r)$$

satisfies

$$N \equiv 1 \pmod{p}.$$

If at least one g_j has a non-zero constant term, then the system (4.9) *has at least one (non-trivial) solution.*

We remark that when q is odd the form

$$ax^2 + 2bxy + cy^2,$$

where $b^2 - ac$ is a non-square of $GF(q)$, is a constant multiple of a norm-form.

5. If in Theorem 7 we assume that the system

$$f_j(x_1, \dots, x_k) = 0 \qquad (j = 1, \dots, r)$$

has a single solution, then the number of solutions N of the system

$$f_j(x_1, \dots, x_k) = g_j(x_1, \dots, x_k) \qquad (j = 1, \dots, r)$$

satisfies

$$N \equiv 1 \pmod{p}.$$

Compare also Theorem 10. It is however quite possible that $N > 1$.

We shall illustrate this in a very special case. Let q be odd and β a non-square of $GF(q)$. Then the equation

$$x^2 - \beta y^2 = 0$$

has only the solution $(0, 0)$. On the other hand, the equation

$$x^2 - \beta y^2 = 2ax - 2\beta by \qquad (a, b \in GF(q)), \tag{5.1}$$

where a, b are not both zero, has $q-1$ solutions. Indeed (5.1) is equivalent to

$$(x-a)^2 - \beta(y-b)^2 = a^2 - \beta b^2. \tag{5.2}$$

Since $a^2 - \beta b^2 \neq 0$ it follows from a familiar result that the number of solutions of (5.2) is $q+1$.

Note that the equation

$$x^2 - \beta y^2 = 2ax - 2\beta by - c,$$

where $c = a^2 - \beta b^2$, has a single solution.

The result concerning (5.1) does not seem to generalize in an obvious way. For example if $Q(x, y)$ is a binary quadratic form with discriminant equal to a non-square of $GF(q)$ then the system

$$\begin{cases} z^2 = Q(x, y), \\ w^2 = cQ(x, y), \end{cases} \tag{5.3}$$

where c is some fixed non-square of $GF(q)$, has only the trivial solution. Indeed (5.3) implies

$$w^2 - cz^2 = 0, \qquad w = z = 0$$

and therefore $x = y = 0$. If L is an arbitrary linear form in z, w, the system

$$\begin{cases} z^2 = Q(x, y) + L(z, w), \\ w^2 = cQ(x, y) + cL(z, w) \end{cases}$$

has only the trivial solution; the proof is exactly the same as that for (5.3).

References

[1] L. Carlitz, *On factorable polynomials in several indeterminates*, Duke Math. Joun. 2 (1936), pp. 660-670.

[2] — *Solvability of certain equations in a finite field*, Quart. Journ. Math. Oxford (2), 7 (1956), pp. 3-4.

[3] C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abhandl. Math. Sem. der Hansischen Univ. 11 (1936), pp. 73-75.

[4] St. Schwarz, *On the equation* $a_1x_1^k + \dots + a_kx^k + b = 0$ *in finite fields*, Quart. Journ. Math., Oxford, 19 (1948), pp. 160-163.

[5] E. Warnung, *Bemerkungen zur vorstehenden Arbeit von Herrn Chevalley*, Abhandl. Math. Sem. der Hansischen Univ. 11 (1936), pp. 76-83.

Reçu par la Rédaction le 12. 2. 1962