ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

314

NOTE ON AN EQUATION IN A FINITE FIELD

BY

VEIKKO ENNOLA

HELSINKI 1962
SUOMALAINEN TIEDEAKATEMIA

https://doi.org/10.5186/aasfm.1962.314

Communicated 9 February 1962 by P. J. Myrberg and K. Inkeri

KESKUSKIRJAPAINO
HELSINKI 1962

Note on an equation in a finite field

Our intention is to use our results on the conjugacy classes of the finite unitary groups [1] in order to prove the following result. Let $\mathfrak{F}_s = GF(q^s)$ denote the finite field with q^s elements (q = power of a prime).

Theorem. *Let* a *be* $q+1$ *or* q^5+1. *Then the number of vectors* (x, y, z) *such that*

$$x^a + y^a + z^a = 0\,, \tag{1}$$

where x, y, z *are linearly independent elements of* $\mathfrak{F}_6$ *over* $\mathfrak{F}_2$ *equals*

$$q^3(q+1)^2(q-1)(q^6-1)\,.$$

From this we can derive a new proof of the following fact. (For the general result see [2].)

Corollary. *The number of vectors* (x, y, z) *such that* (1) *is true for* $a = q+1$ *or* q^5+1 *and* x, y, z *are non-zero elements of* $\mathfrak{F}_6$ *equals*

$$(q^6-1)(q+1)^2(q^4-q^3+q-2)\,.$$

Thus the statement: »In every solution of (1) with $xyz \neq 0$, x, y, z are necessarily linearly independent over $\mathfrak{F}_2$» is true if and only if $q = 2$.

Proof of the theorem. Let ϱ be a primitive element of $\mathfrak{F}_6$. Put $\tau = \varrho^{q^3-1}$ and $\tau_i = \tau^{q^i}$ ($i = 0, 1, 2$; $\tau_0 = \tau$). Then the τ_i's are the conjugates of τ with respect to $\mathfrak{F}_2$ and we have

$$\tau_i^{q^3} = \tau_i^{-1}\,. \tag{2}$$

Clearly $\tau_i \neq \tau_j$ for $i \neq j$. If we write

$$f(t) = (t-\tau_0)(t-\tau_1)(t-\tau_2)\,,$$

then $f(t)$ is an irreducible polynomial over $\mathfrak{F}_2$. Let $f(t) = t^3 + at^2 + bt + c$. Write $\tilde{f}(t) = \bar{c}^{-1}(\bar{c}t^3 + \bar{b}t^2 + \bar{a}t + 1)$, where for $x \in \mathfrak{F}_6$ we put $\bar{x} = x^{q^3}$. (Note that if $x \in \mathfrak{F}_2$, then $\bar{x} = x^q$.) Now (2) easily implies. $f(t) = \tilde{f}(t)$. Let $M = M(f) \in GL(3, q^2)$ be the companion matrix of f. Then we know [1] that M is similar to a unitary matrix and the number $\gamma(M)$ (see [1]) is

$$\frac{g(1, q^6)}{u(1, q^6)} = q^3 - 1 .$$

Hence the number of non-singular matrices X with elements in $\mathfrak{F}_2$ such that

$$XMX^{-1} \in U(3, q^2) \tag{3}$$

equals (see [1])

$$(q^3 - 1)\, u(3, q^2) = q^3(q + 1)^2(q - 1)(q^6 - 1) . \tag{4}$$

We now go up to the field $\mathfrak{F}_6$. We can find a matrix P with elements in $\mathfrak{F}_6$ such that

$$P^{-1}MP = \operatorname{diag}(\tau_0, \tau_1, \tau_2) = D .$$

Since the column vectors of P are eigenvectors of M belonging to the distinct eigenvalues τ_i we may assume them to be conjugate over $\mathfrak{F}_2$.

Suppose now that Y is a non-singular matrix with elements in $\mathfrak{F}_6$ such that

$$YDY^{-1} \in U(3, q^2) . \tag{5}$$

From the results of [1] it follows that Y^*Y must be diagonal, i.e., if $Y = (y_{ij})$, then $\sum_{i=0}^{3} y_{ij}\bar{y}_{ik} = 0$, for $j \neq k$. Also, if we multiply each column vector by a suitable element of $\mathfrak{F}_6$, then we get a matrix in which the column vectors are conjugate over $\mathfrak{F}_2$.

But this is easily seen to hold also conversely, i.e., if Y satisfies these conditions, then (5) is true.

Denote by S the number solutions of (1) with a and x, y, z as required in the theorem. Let x, y, z be an arbitrary solution. Consider the matrix

$$\begin{pmatrix} x & x_1 & x_2 \\ y & y_1 & y_2 \\ z & z_1 & z_2 \end{pmatrix} ,$$

where $x_i = x^{q^{2i}}$ $(i = 1, 2)$ etc. It is non-singular, because x, y, z are linearly independent over $\mathfrak{F}_2$. If $a = q + 1$, we have

$$x\bar{x}_2 + y\bar{y}_2 + z\bar{z}_2 = 0$$

and raising this to the q^5-th power we have

$$x\bar{x}_1 + y\bar{y}_1 + z\bar{z}_1 = 0 .$$

If $a = q^5 + 1$, we get the same results. So we see that the total number of different non-singular matrices Y with conjugate column vectors satisfying (5) is equal to S.

Suppose now that X is a non-singular matrix with elements in $\mathfrak{F}_2$ satisfying (3). Then $Y = XP$ is a matrix with elements in $\mathfrak{F}_6$ and conjugate column vectors satisfying (5).

Conversely, by using the eigenvector argument again, it is easy to see that if Y is a non-singular matrix with elements in $\mathfrak{F}_6$ and with conjugate column vectors, then $X = YP^{-1}$ has its elements in $\mathfrak{F}_2$ and satisfies (3).

Hence S is equal to the expression (4) and this proves the theorem.

Proof of the Corollary Suppose that (1) is valid for $a = q + 1$ or $q^5 + 1$, x, y, z are linearly dependent over $\mathfrak{F}_2$ and $xyz \neq 0$. Write $u = \frac{x}{z}$, $v = \frac{y}{z}$. We may assume that $a = q + 1$, otherwise we raise (1) to the q-th power. We have

$$u^{q+1} + v^{q+1} + 1 = 0\,, \tag{6}$$

where $u, v, 1$ are linearly dependent over $\mathfrak{F}_2$. Clearly we may assume

$$u = bv + c, \quad b, c \in \mathfrak{F}_2\,.$$

Then

$$u^q = \bar{b}v^q + \bar{c}\,.$$

Multiplying these, using (6), and then raising the equation to the power q, q^2, q^3, respectively, we get the following system of equations

$$\begin{cases} (b\bar{b} + 1)\, v^{q+1} + \bar{b}c\, v^q + b\bar{c}\, v + c\bar{c} + 1 = 0\,, \\ (b\bar{b} + 1)\, v^{q^2+q} + \bar{b}c\, v^q + b\bar{c}\, v^{q^2} + c\bar{c} + 1 = 0\,, \\ (b\bar{b} + 1)\, v^{q^3+q^2} + \bar{b}c\, v^{q^2} + b\bar{c}\, v^{q^3} + c\bar{c} + 1 = 0\,, \\ (b\bar{b} + 1)\, v^{q^4+q^3} + \bar{b}c\, v^{q^3} + b\bar{c}\, v^{q^4} + c\bar{c} + 1 = 0\,. \end{cases} \tag{7}$$

Consider here $\bar{b}b + 1$, $\bar{b}c$, $b\bar{c}$, $c\bar{c} - 1$ as indeterminates. Then the determinant of (7) is

$$v^{q^2+2q+1}(v^{q^2-1} - 1)(v^{q^4-q^3} - 1)(v^{q^3-q} - 1)^2\,. \tag{8}$$

If $v \notin \mathfrak{F}_2$, then $v^{q^2-1} - 1 \neq 0$ and thus (8) does not vanish. Hence $b\bar{b} + 1 = c\bar{c} + 1 = b\bar{c} = 0$, which is impossible. So we must have u, $v \in \mathfrak{F}_2$.

Write (6) in the form

$$u^{q+1} = -(1 + v^{q+1})\,.$$

We can take v to be any one of the $q^2 - 1$ elements of $\mathfrak{F}_2$ except those $q + 1$ which make $v^{q+1} = -1$. For each v we have $q + 1$ possible u's.

So the total number of linearly dependent solutions of (6) is $(q+1)^2(q-2)$. Multiplying this by q^6-1 we get the corresponding number for the equation (1). From this the Corollary follows.

References

[1] Ennola, Veikko: *On the conjugacy classes of the finite unitary groups.* - Ann. Acad. Sci. Fenn. A I, No. 313 (1962).

[2] Mitchell, Howard H.: *On the congruence* $c x^\lambda + 1 \equiv d y^\lambda$ *in a Galois field.* - Ann. of Math. 18.3 (1917), pp. 120–131.

University of Turku
Finland

Printed April 1962.