M. D. PREŠIĆ

A METHOD FOR SOLVING EQUATIONS IN FINITE FIELDS

ON CERTAIN FORMULAS FOR EQUIVALENCE AND ORDER RELATIONS

Математички весник
7 (22) Св. 4, 1970.

МАТЕМАТИЧКИ ВЕСНИК
7 (22), 1970, стр. 507—509.

Marica D. Prešić

A METHOD FOR SOLVING EQUATIONS IN FINITE FIELDS

(Communicated April 29, 1970)

Summary

In this paper we give a method for solving equations of the form $\mathcal{G}(x)=0$, where $\mathcal{G}(x)$ is a polynomial over the finite field $GF[p^n]$. The general solution is determined by formula (2), providing the equation $\mathcal{G}(x)=0$ is possible.

Let $GF[p^n]$ be a Galois field of order p^n, and ε a generator of cyclic group of this field. Our main result is the following theorem.

Theorem. *Let*

$$\mathcal{G}(x)=0 \tag{1}$$

be an equation over $GF[p^n]$. *If the equation* (1) *has at least one solution, then the general solution of* (1) *is determined by the formula*

$$\begin{aligned} x = \Pi &+ \mathcal{G}(\Pi)^{p^n-1} + \varepsilon(\mathcal{G}(\Pi)\mathcal{G}(\Pi+1))^{p^n-1} + \varepsilon^2(\mathcal{G}(\Pi)\mathcal{G}(\Pi+1)\mathcal{G}(\Pi+1+\varepsilon))^{p^n-1} \\ &+ \cdots + \varepsilon^{p^n-3}(\mathcal{G}(\Pi)\mathcal{G}(\Pi+1)\ldots\mathcal{G}(\Pi+1+\cdots+\varepsilon^{p^n-4}))^{p^n-1} + \\ &+ (\varepsilon^{p^n-2}+\eta)(\mathcal{G}(\Pi)\mathcal{G}(\Pi+1)\ldots\mathcal{G}(\Pi+1+\cdots+\varepsilon^{p^n-3}))^{p^n-1} \end{aligned} \tag{2}$$

where $\eta = 2+3\varepsilon+\cdots+(p^n-1)\varepsilon^{p^n-3}$, *and* Π *is an arbitrary element of the field.*

In the proof we use:

(i) *If* $x \in GF[p^n]$, *then* $x^{p^n-1}=1 \quad (x\neq 0)$

$$=0 \quad (x=0)$$

(ii) *The elements*

$$0, \quad 1, \quad 1+\varepsilon, \ldots, \quad 1+\varepsilon+\cdots+\varepsilon^{p^n-3}$$

are all distinct.

The proposition (ii) may be proved as follows. Suppose that for some natural numbers m, m' the equality

$$1+\varepsilon+\cdots+\varepsilon^{m} = 1+\varepsilon+\cdots+\varepsilon^{m'} \quad (0\leqslant m'<m\leqslant p^n-3)$$

holds. Hence we obtain: $1+\varepsilon+\cdots+\varepsilon^{m-m'-1}=0$.

Further, multipying the last equality by $\varepsilon-1$ we conclude that $\varepsilon^{m-m'}=1$. This is not possible. because $m-m'<p^n-3$.

Similarly, it may be proved that $1,\ 1+\varepsilon,\ldots,\ 1+\varepsilon+\cdots+\varepsilon^{p^n-3}$ are different from 0.

The elements $1,\ 1+\varepsilon,\ldots,\ 1+\varepsilon+\cdots+\varepsilon^{p^n-3}$ (their number is p^n-2) are roots of the equation $x^{p^n-1}=1$. Denote by η a root of this equation different from them. Then, by Viète's formula we have

$$1+(1+\varepsilon)+\cdots+(1+\varepsilon+\cdots+\varepsilon^{p^n-3})+\eta-0,$$

therefore

$$\eta=2+3\varepsilon+\cdots+(p^n-1)\varepsilon^{p^n-3}.$$

Consequence. *If Π is a fixed element of $GF[p^n]$, then the elements*

$$\Pi,\ \Pi+1,\ \Pi+1+\varepsilon,\ldots,\ \Pi+1+\varepsilon+\cdots+\varepsilon^{p^n-3},\ \Pi+\eta$$

are all distinct. In other words, the set $\{\Pi,\ \Pi+1,\ \Pi+1+\varepsilon,\ldots,\ \Pi+1+\varepsilon+\cdots+\varepsilon^{p^n-3},\ \Pi+\eta\}$ is equal to the set $GF[p^n]$.

Proof of theorem. Let Π be an element of the field $GF[p^n]$. If Π is a solution of (1), then by formula (2) we obtain $x=\Pi$. It follows, immediately, from the structure of formula (2) and proposition (i). In the case Π is not a solution of equation (1) we consider the following sequence

$$\Pi,\ \Pi+1,\ \Pi+1+\varepsilon,\ldots,\ \Pi+1+\varepsilon+\cdots+\varepsilon^{p^n-3},\ \Pi+\eta \tag{3}$$

and the first member of it being a solution of (1). Such member exists as $\mathcal{J}(x)=0$ is a possible equation.

Suppose, first, that this assumed solution is of the form

$$\Pi+1+\varepsilon+\cdots+\varepsilon^m\ (m\leqslant p^n-3),$$

According to

$$\mathcal{J}(\Pi)\neq 0,\ \mathcal{J}(\Pi+1)\neq 0,\ldots,\ \mathcal{J}(\Pi+1+\cdots+\varepsilon^{m-1})\neq 0,\ \mathcal{J}(\Pi+1+\cdots+\varepsilon^m)=0$$

and proposition (i), by formula (2) we obtain

$$x=\Pi+1+\varepsilon+\cdots+\varepsilon^m.$$

In the case $\Pi+\eta$ is the first member of sequence (3) satisfying the condition $\mathcal{J}(\Pi+\eta)=0$, the formula (2) becomes

$$x=\Pi+(1+\varepsilon+\cdots+\varepsilon^{p^n-2})+\eta.$$

Since $1,\ \varepsilon,\ldots,\ \varepsilon^{p^n-2}$ are all roots of the equation $x^{p^n-1}=1$ their sum is 0.

Consequently, in both cases formula (2) gives a solution of equation (1). The proof is finished.

Remark. *In the case of Galois field $GF[p]$ it may be, similarly, proved that the general solution of the equation* (1) *is given by the following simple formula*:

$$x=\Pi+\mathcal{J}(\Pi)^{p-1}+\mathcal{J}(\Pi)^{p-1}\mathcal{J}(\Pi+1)^{p-1}$$
$$+\cdots+\mathcal{J}(\Pi)^{p-1}\mathcal{J}(\Pi+1)^{p-1}\cdots\mathcal{J}(\Pi+p-2)^{p-1}. \tag{4}$$

(Π—an arbitrary element of $GF[p]$)

For instance, the general solution of the equation

$$x^2 + bx + c = 0 \qquad x \in GF[3])$$

is given by formula

$$x = cb + D\,(2\,\Pi^2 + (2\,b + 1)\,\Pi + c^2) \qquad (D \underline{\underline{\text{def}}}\, b^2 + 2\,c)$$

providing $D^2 = D$.

REFERENCES:

[1] S. B. Prešić, *Une méthode de résolution des équations dont toutes les solutions appartiennent à un ensemble fini donné* (*in print*).