ACTA DIDACTICA NAPOCENSIA

Volume 6, Number 4, 2013

ON A EQUATION IN FINITE ALGEBRAICALLY STRUCTURES

Dumitru Vălcan

Abstract: Solving equations in finite algebraically structures (semigroups with identity, groups, rings or fields) many times is not easy. Even the professionals can have trouble in such cases. Therefore, in this paper we proposed to solve in the various finite groups or fields, a binomial equation of the form (1). We specify that this equation has been given to solving the master students in mathematics, many years. Unfortunately, none of them were able to give its solution. Therefore, we proposed the drafting of this paper.

Key words: equations, solutions, groups, fields.

1. Introduction

Solving math problems is a complex ability, fundamental, shows Schoenfeld (1985, p. 15) on various resources such as:

a) mathematical knowledge (results of mathematical knowledge: concepts, hypotheses, models, facts, non-algorithmic procedures (routines), algorithms and strategies prescribed etc.), intuition and informal knowledge in the field, understand the conventions used in Mathematics;

b) heuristic strategies whose possession ensures solving the problems complex and less familiar or empirical procedures applied to the achievement the figures and their annotation using the appropriate symbols, text analysis problem, the reformulation of the problem and its solving control, testing / verification solution (ibid.);

c) techniques and procedures for the selection of resources and strategies, making decisions and of awareness of metacognitive, aspects applied at all stages: analysis problem, the design of solving, solve the problem and its assessment (ibid.).

Schoenfeld (1985, p 15) adds the components listed above and a set of beliefs about self, environment, mathematics, respectively the problem.

Polya (1973, p 7-14) shows that, beyond the fact that there are some general strategies that help solve problems correctly and can be taught to students, to help him learn Math, the teacher should try to put in mind of his pupil (ibid., p. 1). The approach proposed by Polya (1973, p. 7 - 14) is generally known and is structured in short in the following:

- *Problem analysis for understanding them*: What gives? What is required? What conditions or requirements to be complied? Additional data is required? How can shape the (graphic symbolic, verbal - phrase) the content matter? Stages can be identified around?
- *Foreshadowing solution by identifying category / class of problems*, reporting a solving model, reporting similar problems previously solved. Reformulation of the problem may facilitate the identification of the solution.
- *Solving the problem*, sometimes a stages manner: What we find first?
- *Check the solution* (results and solving). Reflecting on the difficulties encountered and how to solve them can help understanding of the problem and the deepening of the solution.

Polya (ibid.) insists on the the correctness questions that the teacher poses or suggests to his students to help solve the problem. In fact, the source cited proposes guiding student through questions and suggestions, about solving the problem. In the following we propose to illustrate the model approach to solve a problem proposed by Polya, referring to an issue that raises students' difficulties.

Therefore, referring to the abilities of solving mathematical problems, this paper exemplifies some

Received 21 November 2013

didactics aspects implied in solving a problem in the topic of the various finite groups, or fields, o binomial equation of the form (1).

Regarding the Theorem 1, it is important to specify that this problem was included in one of the tests to be solved by mathematics teachers that have participate in competition for obtaining the title *titular* in Romania, in 2001, see (Vălcan, 2002, p. 78).

2. Solving the equation (1) and applications

The main result of this paper is as follows:

Theorem 1: *Let $(G,\cdot)$ be a group with $4n+2$ elements, and $1\in G$ – the unit element and $n\in \mathbf{N}^*$. Then the equation*

$$x^{2n+1}=1, \tag{1}$$

has in the group G, exactly $2n+1$ solutions.

***Proof*:** We prove this result in several steps.

a) Let be:

$$H=\{t_g \mid g\in G\},$$

where, for any $g\in G$,

$$t_g : G \to G,$$

and for every $x\in G$,

$$t_g(x)=gx.$$

b) We show that, for every $g\in G$, the map t_g is bijective. Indeed, if $x, y\in G$, such that:

$$t_g(x)=t_g(y),$$

then:

$$gx=gy.$$

Since the last equality we look at the group G, where we can simplify any element, it follows that:

$$x=y,$$

that is t_g is an injective function. For surjectivity, we consider an element $y\in G$ and solve the equation:

$$t_g(x)=y,$$

that is:

$$gx=y.$$

This equation admits in the group G, the solution:

$$x=g^{-1}y\in G.$$

Therefore, t_g is a bijective function and, more than, for any $x\in G$,

$$t_g^{-1}(x)=g^{-1}x,$$

that is:

$$t_g^{-1}=t_{g^{-1}}\in H.$$

c) $H\subseteq S_G=S_{4n+2}$. This fact follows from the above, because now we can look at the set H as a set of bijective applications from G to G, i.e. permutations of G; here S_G denoted the group of permutations of G. How the set G is finite, the equality holds.

d) $(H,\circ)$ is a subgroup of the group $(S_{4n+2},\cdot)$. Indeed, if $g_1, g_2\in G$, then, for any $x\in G$,

$$\begin{aligned}(t_{g_1}\circ t_{g_2^{-1}})(x)&=(t_{g_1}(t_{g_2^{-1}}(x))\\ &=(t_{g_1}(g_2^{-1}x))\\ &=g_1(g_2^{-1}x)\\ &=(g_1g_2^{-1})x\\ &=t_{g_1g_2^{-1}}(x).\end{aligned}$$

These equalities show that:

$t_{g_1} \circ t_{g_2^{-1}} = t_{g_1 g_2^{-1}} \in H$.

According to the theorem of characterization of subgroups, we get the above statement.

e) The map:

$f : G \to H$,

defined by: for any $g \in G$,

$f(g) = t_g$,

is an isomorphism of groups. The fact that f is a morphism of groups resulting from the fact that, for any $g_1, g_2 \in G$, we have:

$$f(g_1 g_2) = t_{g_1 g_2} = t_{g_1} \circ t_{g_2} = f(g_1) \circ f(g_2).$$

We show now that the function f is bijective. The surjectivity of f follows from its definition. For injectivity, we consider $g_1, g_2 \in G$, such that:

$f(g_1) = f(g_2)$.

Then, for every $x \in G$,

$t_{g_1}(x) = t_{g_2}(x)$,

that is:

$g_1 x = g_2 x$.

Because we are in a group, from the last equality it follows that f is bijective. So, f is an isomorphism of groups.

f) So, the groups $(G,\cdot)$ and $(H,\circ)$ are isomorphic, which meant that:

$|H| = 4n+2$.

g) Since:

$|G| = 4n+2$,

it follows that there is a $g \in G \setminus \{1\}$ such that:

$g^2 = 1$.

It follows that:

$f(g) = t_g = \sigma \in H$

has everything order 2, so:

$\sigma^2 = e$,

where e is the identical permutation of S_{4n+2}, and hence of the subgroup H.

h) Since $g \neq e$, it follows that, for every $x \in G$, $t_g(x) \neq x$; which means that the permutation $\sigma(=tg) \in H$ does not have fixed points, in which case it is the product of 2n+1 transpositions. It follows that σ is odd. That means that there are an even permutation in H; be it $\tau \in H$.

i) We consider the sets:

$[H_p = \{\alpha \in H \mid \alpha \text{ is even}\}$ and $H_i = \{\beta \in H \mid \beta \text{ is odd}\}]$

and the map:

$F : H_p \to H_i$,

defined by: for any $\alpha \in H$,

$F(\alpha) = \sigma \cdot \alpha$,

where σ is the permutation of points g) and h). Then, as in paragraph b), it shows easily that F is bijective application and thus,

$|H_p| = |H_i| = 2n+1$.

j) Let be:

$S = \{\chi \in H \mid \chi^{2n+1} = e\}$.

Then, whatever the permutation $\delta \in H \setminus S$, $\delta^{2n+1} \neq e$, but, since:

$|H| = 4n+2$,

any such permutation δ verify equality:

$(\delta^{2n+1})^2=\delta^{4n+2}=e$.

So, as specified in step h), it follows that the permutation δ^{2n+1} is odd, which shows that the permutation δ is odd. Therefore,

$\{\delta\in H \mid \delta^{2n+1}\neq e\}\subseteq H_i$,

and, thus:

$|\{\delta\in H \mid \delta^{2n+1}\neq e\}|\leq|H_i|=2n+1$.

It follows that:

$|S|\geq 2n+1$.

But, any permutation $\chi\in S$ is even. So, $S\subseteq H_p$ and, thus,

$|S|\leq 2n+1$.

From the last two inequalities it follows that:

$|S|=2n+1$

and, now, the theorem is completely proved.

***Examples 2*: 1)** For:

$n=1$,

the group G, from Theorem 1, is of order 6 and, according to this theorem, the equation (1) has in the group G exactly three solutions. So, in this case, we have two possibilities:

a) $G=\mathbf{Z}_6=\mathbf{Z}_2\times\mathbf{Z}_3$. In this (sub)case, the equation (1) becomes:

$3x=0$,

and, immediately check that, the set S of solutions to this equation is:

$S=\{0,2,4\}$.

b) $G=S_3$. In this (sub)case, the equation (1), which becomes:

$x^3=1$,

just is verified any of permutations of the set:

$$S=\left\{e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \sigma=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \tau=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}.$$

2) For:

$n=2$,

the group G, from Theorem 1, is of order 10 and, according to this theorem, the equation (1) has in the group G exactly five solutions. So, and in this case, we have two possibilities:

a) $G=\mathbf{Z}_{10}=\mathbf{Z}_2\times\mathbf{Z}_5$. In this (sub)case, the equation (1) becomes:

$5x=0$,

and, immediately check that, the set S of solutions to this equation is:

$S=\{0,2,4,6,8\}$.

b) $G=D_5=\langle a,b\rangle$, wiht the conditions:

$[a^5=b^2=1$ and $ba=a^4b]$.

Hence:

$D_5=\{1,a,a^2,a^3,a^4,b,ab,a^2b,a^3b,a^4b\}$,

and the table of the operation of the group D_5 is as follows:

$\cdot$	**1**	**a**	$\mathbf{a^2}$	$\mathbf{a^3}$	$\mathbf{a^4}$	**b**	**ab**	$\mathbf{a^2b}$	$\mathbf{a^3b}$	$\mathbf{a^4b}$
1	1	a	a^2	a^3	a^4	b	ab	a^2b	a^3b	a^4b
A	a	a^2	a^3	a^4	1	ab	a^2b	a^3b	a^4b	b
$\mathbf{A^2}$	a^2	a^3	a^4	1	a	a^2b	a^3b	a^4b	b	ab
$\mathbf{A^3}$	a^3	a^4	1	a	a^2	a^3b	a^4b	b	ab	a^2b
$\mathbf{A^4}$	a^4	1	a	a^2	a^3	a^4b	b	ab	a^2b	a^3b
B	b	a^4b	a^3b	a^2b	ab	1	a^4	a^3	a^2	a
ab	ab	b	a^4b	a^3b	a^2b	a	1	a^4	a^3	a^2
$\mathbf{a^2b}$	a^2b	ab	b	a^4b	a^3b	a^2	a	1	a^4	a^3
$\mathbf{a^3b}$	a^3b	a^2b	ab	b	a^4b	a^3	a^2	a	1	a^4
$\mathbf{a^4b}$	a^4b	a^3b	a^2b	ab	b	a^4	a^3	a^2	a	1

In this (sub)case, the equation (1) becomes:

$x^5=1$,

and, as resulting from the group operation table, is verified at any of the elements of the set:

$S=<a>=\{1,a,a^2,a^3,a^4\}$.

It is observed that if $(G,\cdot)$ is a group, then equation (1) is in fact an equation of the form:

$$x^{\frac{|G|}{2}}=1. \quad (2)$$

Not always, given a group G of even order, equation (2) has the exact $\frac{|G|}{2}$ solutions. Therefore, we impose here a few remarks:

***Remarks 3:* 1)** *If $(G,\cdot)$ is a group of order 4n, $n\in\mathbf{N}^*$, then, generally, it does not follow that the equation (2), which in this case is:*

$x^{2n}=1$,

has exactly 2n solutions in the group G; 1 being the unit group G.

2) *For any $n\in\mathbf{N}^*$, in any group of the form $(\mathbf{Z}_{2n},+)$ the equation (2), which in this case is:*

$nx=0$,

has exactly n solutions.

3) *For any $n\in\mathbf{N}^*$, in the diedral group D_n, the equation:*

$x^n=1$

has exactly n solutions, namely, the elements of the set:

$S=<a>=\{1,a,a^2,...,a^{n-1}\}$.

Moreover, we can say that this equation has exactly 2n solutions if and only if n is an even number. And here $1\in D_n$ is the neutral element of the group D_n.

***Proof*: 1)** Indeed, consider the following (counter) examples:

a) If:

$G=\mathbf{Z}_2\times\mathbf{Z}_2$,

which is a group of order 4, known as Klein's group, then the equation:

$x^2=1$

has exactly 4 solutions in G, since all the elements of G satisfying this condition. Indeed,

$G=\{1,a,b,c\}$

with the conditions:

$a^2=b^2=c^2=1$.

Because:

$1^2=1$,

obtain the above statement. The group operation table of G is the following:

·	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

b) If:

$G=\mathbf{Z}_4$

- the cyclic group of order 4, then the equation:

$2x=0$

has exactly two solutions in G: 0 and 2. Indeed,

$G=\{0,1,2,3\}$.

In reality,

$G=<1>$,

$o(1)=o(3)=4$,

but

$o(2)=2$

and, since:

$2\cdot 0=0$,

obtain the statement. The group operation table of G is the following:

·	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

c) If:

$G=\mathbf{Z}_2\times\mathbf{Z}_4$,

Which is a group of order 8, then the equation:

$4x=0$

has exactly eight solutions in G, since all the elements of G satisfying this condition. Indeed,

$G=\{\overline{0},\overline{1}\}\times\{\hat{0},\hat{1},\hat{2},\hat{3}\}$
$=\{(\overline{0},\hat{0}),(\overline{0},\hat{1}),(\overline{0},\hat{2}),(\overline{0},\hat{3}),(\overline{1},\hat{0}),(\overline{1},\hat{1}),(\overline{1},\hat{2}),(\overline{1},\hat{3})\}$,

where:

$[2\cdot\overline{0}=2\cdot\overline{1}=\overline{0}$ and $4\cdot\hat{0}=4\cdot\hat{1}=4\cdot\hat{2}=4\cdot\hat{3}=\hat{0}]$.

Therefore, for any element $(\overline{x},\hat{y})\in G$, we have the equalities:

$4\cdot(\overline{x},\hat{y})=(4\cdot\overline{x},4\cdot\hat{y})=(\overline{0},\hat{0})$.

d) If:

$G=D_4$

– the diedral group of order 4, then the equation:

$x^4=1$

has, in G, exactly eight solutions, that also in this case, all elements of G satisfying this equality. Indeed,

$G=D_4=\langle a,b\rangle$,

with the conditions:

$[a^4=b^2=1$ and $ba=a^3b]$.

Therefore:

$D_4=\{1,a,a^2,a^3,b,ab,a^2b,a^3b\}$,

and the group operation table of D_4 is the following:

·	**1**	**a**	**a^2**	**a^3**	**b**	**ab**	**a^2b**	**a^3b**
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	1	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	1	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	1	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	1

In this (sub)case, the equation:

$x^4=1$,

as resulting from the group operation table is checked at any of the elements of the set G.

2) If G is the additive group $(\mathbf{Z}_{2n},+)$, then the set:

$S=\{\overline{x}\in\mathbf{Z}_{2n}\mid n\cdot\overline{x}=\overline{0}\}$

is a subgroup of order n of the group ($\mathbf{Z}_{2n}$,+). Indeed,

$$S=\{\overline{0},\overline{2},\overline{4},...,\overline{2n-2}\}=<\overline{2}>,$$

because, for every $\overline{x}\in\mathbf{Z}_{2n}$, we have:

$$2n\cdot\overline{x}=\overline{0}.$$

3) If:

$$G=D_n$$

– the diedral group of order n, then, always, the equation:

$$x^n=1$$

has in G at least n solutions. Indeed,

$$G=D_n=<a,b>,$$

with conditions:

$$[a^n=b^2=1 \text{ and } ba=a^{n+1}b].$$

Hence:

$$D_n=\{1,a,a^2,a^3,...,a^{n-1},b,ab,a^2b,a^3b,...,a^{n-1}b\},$$

and, for every $k=\overline{1,n}$, the equalities hold:

$$(a^k)^n=(a^n)^k=1.$$

On the other hand, we have:

$$ba^2=baa=a^{n-1}ba=a^{n-1}a^{n-1}b=a^{2n-2}b=a^{n-2}b,$$
$$ba^3=ba^2a=a^{n-2}ba=a^{n-2}a^{n-1}b=a^{2n-3}b=a^{n-3}b,$$
$$ba^4=ba^3a=a^{n-3}ba=a^{n-3}a^{n-1}b=a^{2n-4}b=a^{n-4}b,$$
$$\vdots$$
$$ba^k=ba^{k-1}a=a^{n-(k-1)}ba=a^{n-(k-1)}a^{n-1}b=a^{2n-k}b=a^{n-k}b,$$
$$\vdots$$

Hence:

$$(ab)^2=a(ba)b=aa^{n+1}bb=1,$$
$$(a^2b)^2=a^2(ba^2)b=a^2a^{n-2}bb=a^nb^2=1,$$
$$(a^3b)^2=a^3(ba^3)b=a^3a^{n-3}bb=a^nb^2=1,$$
$$\vdots$$
$$(a^kb)^2=a^k(ba^k)b=a^ka^{n-k}bb=a^nb^2=1,$$
$$\vdots$$
$$(a^{n-1}b)^2=a^{n-1}(ba^{n-1})b=a^{n-1}a^{n-(n-1)}bb=a^nb^2=1.$$

Therefore, for any $n\in\mathbf{N}^*$, equation in the statement is verified by any element of the set:

$$S=\{1,a,a^2,a^3,...,a^{n-1},\}=<a>$$

and each element of the set:

$$D_n\backslash S=\{b,ab,a^2b,a^3b,...,a^{n-1}b\},$$

is of order 2. If, in addition, each element of $D_n\backslash S$ verifies the statement equation, then n is an even number, because if:

$$n=2p+1,$$

with $p\in\mathbf{N}^*$, then, for every $x\in D_n\backslash S$,

$$x^n=x^{2p+1}=(x^2)^px=x\neq1.$$

If n is an even number, then equalities above show that any $x\in D_n$, satisfies the equation in statement.

We pass now to the fields.

In any field (K,+,·), the element 0 is o solution of equation (1). The question here naturally is that of determining the nonzero solutions of the field K, namely the determination of solutions of equation (1) of the group (K^*,·). If,

$$car(K)=p$$

– the characteristic of K is a prime number, then there are a number $m\in\mathbf{N}^*$, such that:

$$|K|=p^m,$$

in wihch case:

$$|K^*|=p^m-1.$$

Considering the group G as the group K^*, in the conditions of Theorem 1, we have equality:

$p^k=4n+3$,

that is, the number p is odd. Therefore, for such fields, have the following statements:

1) If K is a filed of characteristic 3, with 3^m elements and

$m=2q+1$,

$q\in\mathbf{N}^*$, then:

$|K^*|=3^m-1=3^{2q+1}-1=3\cdot 9^q-1=3\cdot(4\cdot 2+1)^q-1=4n+2$,

and, according to Theorem 1, the equation (1) has 2n+1 solutions in the group K^*.

2) In a field K, of characteristic p, with

$p^m=2n+1$

elements, the equation (2) has exactly n solutions in group K^*. In fact, in this case,

$|K^*|=p^m-1=2n$

and, because the group $(K^*,\cdot)$ is isomorphic to the (cyclic) group $(\mathbf{Z}_{2n},+)$, according to point 2) form Remarks 3, we obtain the statement.

3. Conclusions

From the proof of Theorem (1) it is found that the first great difficulty the issue in question is to apply Theorem Cayley: *Any group is isomorphic embedded in a group of permutations*. The fact that students do not apply this theorem in specific cases, but know that a simple theoretical result is seen from results. Then Sylow's theorems do not know - that apply in step g). Finally, no one can answer the question: *What does it mean a permutation of order 4n+2 does not coincide with identical permutation*? The answer here - permutation can not be fixed points - comes from not knowing the meaning of equality of two functions. Last question unanswered: *What means a permutation of order 4n+1 does not have fixed points*? - answer comes from knowing that every permutation is a product (in our case of 2n +1) transpositions. The rest of the proof should "*go*", but not really.

Examples considered are intended to help the student to understand more easily Theorem 1 and see how it applies in the simplest two cases. But also here must be known that there are two groups of the order 6 ($\mathbf{Z}_6$ and S_3), and two groups in the order 10 ($\mathbf{Z}_5$ and S_5).

Although the equation (1) is a particular case of equation (2), Remarks 3 shows that Theorem 1 does not apply always to equation (2) - counterexamples presented are eloquent of this. But here must be known that any group is completely determined by generators and relations, so I drafted and the group operation table in some cases.

Passing to fields is immediate, because an area of great interest to students and teachers is "*Solving equations in finite fields*", which often is resumed to solving the equations in the underlying multiplicative groups of fields.

Attentive and interested reader these issues will notice that I respected Polya's idea, that the teacher must put in mind of the student - stated in the introduction, because doing that is the essence of didactics of Mathematics.

References

[1] Călugăreanu, G., (1994), *Introduction to Abelian Groups Theory*, (in Romanian), Editura Expert, Cluj-Napoca.

[2] Dickson, J., E., (1905), *Defnitions of a group and a field by independent postulates*, Trans. Amer. Math. Soc., 6(1905), p. 198-204.

[3] Jungnickel, D., (1992), *On the Uniqueness of the Cyclic Group of Order n*, Amer. Math. Monthly, 6(1992), p. 545-547.

[4] Popescu, D., Vraciu, C., (1986), *Elements of Finite Group Theory*, (In Romanian), Editura Stiinţifică şi Enciclopedică, Bucureşti.

[5] Purdea, I., (1992), *On the groups of order n≤10*, Selected paper from "*Didactica Matematicii*",

Vol. 1984-1992, "Babeş-Bolyai" University, Faculty of Mathematics and Computer Science, Research Seminars, Cluj-Napoca.

[6] Polya, G., (1973), *How to solve it. A new aspect of mathematical model*, USA: Princenton University Press.

[7] Purdea, I., Pic, G., (1973), *Algebra*, (In Romanian), "Babeş-Bolyai" University, Faculty of Mathematics and Mechanics, Lit., Cluj-Napoca.

[8] Rotmann, J., J., (1968), *The Theory of Groups: An introduction*, Allyn and Bacon, Inc., Boston.

[9] Schoenfeld, A., (1985), *Matematical problem solving*, UK: Academic Press inc.

[10] Vălcan, D., (1998), *On some groups of finite order*, (In Romanian), Lucrările Seminarului de "*Didactica Matematicii*", Vol. 13(1998), p. 177-182.

[11] Vălcan, D., (coord.), (2002), *Math exams and competitions. Continuing training. Data subject to: exams bachelor, master, didactical, definitived, grade II, competition for vacancies in secondary education*, *Seria „MATHEMATICA MILENIUM 3”*, (In Romanian), Editura OPTIL GRAPHIC, Craiova.

Author

Teodor Dumitru Vălcan, Babeş-Bolyai University, Cluj-Napoca, Romania, E-mail: tdvalcan@yahoo.ca