THE TEACHING OF MATHEMATICS
2006, Vol. IX, 1, pp. 41–44

SOLUTIONS OF SOME CLASSES OF CONGRUENCES

Eugen Vedral

Abstract. We present a method for solving nonlinear congruences. It is different from methods often met in the literature, and it is based on reduction of nonlinear congruence to either linear or quadratic congruence. This paper is written for teachers and talented gymnasium students, interested in solving nonlinear congruences.

ZDM Subject Classification: F64; *AMS Subject Classification*: 00A35.

Key words and phrases: Congruence, congruences of higher degree.

In this article solutions of the following nonlinear congruence are considered:

$$x^k \equiv a \pmod{p}. \tag{1}$$

where a is an integer, $a \not\equiv 0 \pmod{p}$, and p is a prime satisfying the condition $p = k \cdot l + 2$ (or $p = k \cdot l + 3$), for some $k, l \in \mathbf{N}$. This congruence will be reduced either to the linear congruence

$$Ax \equiv B \pmod{p}, \tag{2}$$

$A, B \in \mathbf{Z}$, or to the quadratic one

$$x^2 \equiv b \pmod{p}, \tag{3}$$

$b \in \mathbf{Z}$.

The lecture on this topic can start by asking students to solve the following problem.

EXAMPLE 1. Solve the congruence $x^5 \equiv 9 \pmod{37}$.

A clever student might notice that computing the 7-th power of both sides of the given congruence leads to a quick solution. Namely, $x^{35} \equiv 9^7 \pmod{37}$ and consequently $x^{35} \equiv 16 \pmod{37}$. Now, multiplying both sides by x, we get $x^{36} \equiv 16x \pmod{37}$. Finally, applying Fermat theorem (it is obvious that $x \not\equiv 0 \pmod{37}$), we obtain the linear congruence $16x \equiv 1 \pmod{37}$, whose solution is $x \equiv 7 \pmod{37}$. It is easy to check that 7 is the solution of the given congruence as well.

Before presenting the general idea, we can offer to students another problem:

EXAMPLE 2. Solve the congruence $x^{17} \equiv 18 \pmod{37}$.

By squaring both sides of the given congruence, the following formulas occur: $x^{34} \equiv 18^2 \pmod{37}$ or $x^{34} \equiv 28 \pmod{37}$. Now, multiplying by x^2 and applying

Fermat theorem, we obtain the congruence $28x^2 \equiv 1 \pmod{37}$. Its solutions are $x \equiv 2 \pmod{37}$ and $x \equiv 35 \pmod{37}$. We check that 2 is the only solution of the given congruence.

The general idea, sketched in the two examples above, can be summarized as follows.

PROPOSITION 1. *Let p be a prime, $p = k \cdot l + 2$ for some $k, l \in \mathbf{N}$. Then the congruence (1) is equivalent to the linear congruence*

$$a^l x \equiv 1 \pmod{p}. \tag{4}$$

Proof. First, we are going to find the l-th power of both sides of (1). In this way the formula $x^{kl} \equiv a^l \pmod{p}$ will be obtained. Then, multiplying the last congruence by x, we get $x^{kl+1} \equiv a^l x \pmod{p}$. Since $kl + 1 = p - 1$ and using Fermat theorem we obtain $x^{kl+1} \equiv 1 \pmod{p}$. (Note that $a \not\equiv 0 \pmod{p}$ and therefore $x \not\equiv 0 \pmod{p}$.) We have $a^l x \equiv 1 \pmod{p}$. Finally, the solution of the congruence (4) satisfies $x \equiv a^{-l} \pmod{p}$. Let us prove that a^{-l} is the solution of (1) as well:

$$(a^{-l})^k \equiv a^{-lk-l+1} \equiv a^{-(p-1)} a \equiv a \pmod{p}.$$

The proof is completed. ■

EXAMPLE 3. Solve the congruence $x^7 \equiv 13 \pmod{23}$.

From $23 = 7 \cdot 3 + 2$ we obtain that $l = 3$. Applying Proposition 1, we obtain the solution 13^{-3}. First we find $13^{-1} \equiv 16 \pmod{23}$ by solving the congruence $13x \equiv 1 \pmod{23}$. Then we need to compute $16^3 \equiv 2 \pmod{23}$. So, 2 is the only solution of the given congruence.

The following proposition can also be proved.

PROPOSITION 2. *Let p be a prime, $p = k \cdot l + 3$ for some $k, l \in \mathbf{N}$. If x is a solution of the congruence (1), then x is a solution of the congruence*

$$x^2 \equiv a^{-l} \pmod{p}. \tag{5}$$

Proof. The proof of Proposition 2 is given by the following chain of formulas:

$$\begin{aligned} x^{kl} &\equiv a^l \pmod{p}, \\ x^{kl+2} &\equiv x^2 a^l \pmod{p}, \\ x^2 a^l &\equiv 1 \pmod{p}, \\ x^2 &\equiv a^{-l} \pmod{p}. \end{aligned}$$

Actually, $x^{kl+2} \equiv 1 \pmod{p}$ by Fermat theorem. ■

If (5) has a solution, then it has two solutions. It is necessary to check whether they are the solutions of (1). Namely, Proposition 2 is of the "implication" type,

which means that the converse need not be true. On the other hand, if (5) has no solutions, then (1) has no solutions either.

In order to discuss the number of solutions of (1), let us first recall Theorem 37 from [1].

If p is a prime and g.c.d. $(a,p) = 1$*, then the congruence (1) has either* g.c.d. $(k, p-1)$ *solutions or no solutions, depending on whether* $a^{\frac{p-1}{g.c.d.(k,pi-1)}} \equiv 1 \pmod{p}$*, holds or does not hold.*

Since $p = k \cdot l + 3$, then $p - 1 = k \cdot l + 2$. Therefore we have g.c.d. $(k, p-1) =$ g.c.d. $(k, 2)$. There exist two cases:

1. If g.c.d. $(k, 2) = 1$, then (1) has only one solution. The congruence (5) has two solutions, and only one of them is the solution of (1). The congruences (1) and (5) are not equivalent. It is necessary to check which of the solutions of (5) is the solution of (1).

2. If g.c.d. $(k, 2) = 2$ then congruence (1) has either two or zero solutions. In the first case (5) also has two solutions, and congruences (1) and (5) are equivalent.

EXAMPLE 4. Solve the congruence $x^5 \equiv 9 \pmod{23}$.

First, let us note that $23 = 5 \cdot 4 + 3$. Therefore $l = 4$ and, by using (5), we get $x^2 \equiv 9^{-4} \pmod{43}$. Since $9^4 \equiv 6 \pmod{23}$ and $6^{-1} \equiv 4 \pmod{23}$, we obtain the congruence $x^2 \equiv 4 \pmod{23}$ with the solutions 2 or 21. It is easy to check that 2 is the only solution of the given congruence.

EXAMPLE 5. Solve the congruence $x^{10} \equiv 35 \pmod{43}$.

We have $43 = 10 \cdot 4 + 3$. Since g.c.d. $(10, 42) = 2$ and $35^{21} \equiv 1 \pmod{43}$, the given congruence has two solutions. Both solutions of the quadratic congruence, to which the given congruence will be reduced, are the solutions of the given congruence. It is easy to follow the chain of formulas:

$$\begin{aligned} x^{40} &\equiv 11 \pmod{43}, \\ x^{42} &\equiv 11x^2 \pmod{43}, \\ 11x^2 &\equiv 1 \pmod{43}, \\ x^2 &\equiv 4 \pmod{43}, \\ x \equiv 2 \pmod{43} &\text{ or } x \equiv 41 \pmod{43}. \end{aligned}$$

Both 2 and 41 are the solutions of the given congruence.

The two propositions above show that the congruence (1), $k > 2$, can be reduced to either linear or quadratic one, and then solved by the well known methods. These two propositions can be applied under the condition that p is of the type $kl + 2$ or $kl + 3$, $k, l \in \mathbf{N}$.

REFERENCES

1. I. Niven, S. Zuckerman and H. Montgomery, *An Introduction to the Theory of Numbers*, New York, 1991.
2. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford 1979.

Peta beogradska gimnazija, I. Garašanina 24, Beograd, Serbia