https://www.proconference.org/index.php/gec/article/view/gec35-00-014
DOI: 10.30890/2709-1783.2024-35-00-014

UDC [004.7-047.72]:656.2

METHODS OF FORMING COMPETENCIES IN APPLICANTS FOR THE SPECIALTY «CYBERSECURITY» WHEN PERFORMING A COURSE ASSIGNMENT IN THE DISCIPLINE «MATHEMATICAL FOUNDATION OF INFORMATION SECURITY»

МЕТОДИКА ФОРМУВАННЯ КОМПЕТЕНТНОСТЕЙ У ЗДОБУВАЧІВ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА» ПРИ ВИКОНАННІ КУРСОВОГО ЗАВДАННЯ З ДИСЦИПЛІНИ «МАТЕМАТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Pakhomova V. M. / Пахомова В. М.
c.t.s., as. prof. / к.т.н., доц.
ORCID: 0000-0002-0022-099X
Ukrainian State University of Science and Technology, Ukraine,
Dnipro, Lazaryan St., 2, 49010
Український державний університет науки і технологій,
Україна, Дніпро, вул. Лазаряна, 2, 49010

Abstract. *The methodology of "ComparSystem MathFIS" for the formation of professional and subject competencies of applicants for the degree "Bachelor" in the specialty "Cybersecurity" at fulfillment of the course task in the discipline "Mathematical Foundations of Information Security": 1) getting an idea of the system of comparisons of the first degree; 2) the study of fundamental theorems (in particular, the Chinese remainder theorem); 3) analysis of the control example of the solution systems of comparisons by modules; 4) solving an individual problem using the substitution method and the Chinese remainder theorem; 5) formulation of the relevant conclusion.*

Keywords: *competence, course task, system of comparisons, substitution method, remainder, Chinese remainder theorem, greatest common divisor, smallest common multiple.*

Анотація. *Запропоновано методику «ComparSystem MathFIS» щодо формування фахових та предметних компетентностей здобувачів ступеня «бакалавр» спеціальності «Кібербезпека» при виконанні курсового завдання з дисципліни «Математичні основи інформаційної безпеки»: 1) отримання уявлення про систему порівнянь першого степеня; 2) вивчення фундаментальних теорем (зокрема китайську теорему про остачі); 3) аналіз контрольного прикладу розв’язання системи порівнянь за модулями; 4) розв’язання індивідуального завдання з використанням методу підстановки та китайської теореми про остачі; 5) формулювання відповідного висновку.*

Ключові слова: *компетентність, курсове завдання, система порівнянь, метод підстановки, остача, китайська теорема про остачі, найбільший спільний дільник, найменше спільне кратне.*

Entry

Statement of the problem. The current state of the world, which is associated with a constant the spread of infected diseases and the prolonged continuation of military events, life-threatening applicants, led to the use of mixed training, in particular in the discipline "Mathematical Foundations of Information Security", and as well as the formation of relevant professional and subject competencies in applicants for a bachelor's degree under such difficult conditions of our time that confirms the relevance of the topic.

Analysis of the latest research. Competency assessment is the subject of research by many scientists [1]. At the present stage, it is important to Comparison of Ukrainian education in international studies of the quality of education. The analysis of recent studies and publications revealed the following: 1) lack of unified information and communication technologies for training discipline "Mathematical Foundations of Information Security"; 2) necessity solving comparison systems by modules to ensure the security of information in information and telecommunication systems and computer networks; 3) the existence of a feature of generation Z, and became the basis for the development of our own methodology.

The aim of the work is to develop a methodology of "ComparSystem_MathFIS" for the formation of professional and subject competencies for applicants for a bachelor's degree specialty "Cybersecurity" when performing a course assignment in the discipline "Mathematical Foundations of Information Security".

General characteristics of the "ComparSystem_MathFIS" methodology. With mixed training (a combination of face-to-face and distance formats, the use of "Zoom" and "Lider", communication in social networks) proposed methodology provides an opportunity for applicants for the first degree in the discipline "Mathematical Fundamentals of Information Security" [2-3]: to get an idea of the system of comparisons of the first degree and study fundamental theorems; disassemble the control an example of solving a system of comparisons by modules; solve individual tasks using the substitution method and the Chinese remainder theorem; formulate an appropriate conclusion.

1. Understanding the system of comparisons of the first degree

A system of comparisons is called a system of appearance

$$\begin{cases} f_1(x) \equiv 0 (\operatorname{mod} m_1), \\ f_2(x) \equiv 0 (\operatorname{mod} m_2), \\ \ldots \\ f_n(x) \equiv 0 (\operatorname{mod} m_n), \end{cases} \tag{1}$$

where $f_1(x)$; $f_2(x)$; ...; $f_n(x)$ – are given polynomials with integer coefficients. Let M is the least common multiple of all modules m_1, m_2 ..., m_n. Solution of the system (1) will be a class of numbers module M, containing numbers that satisfy each comparison of the system.

A system of comparisons of the first degree consists of n comparisons with one and the same unknown, but with different modules:

$$\begin{cases} a_1 x \equiv b_1 (\bmod m_1), \\ a_2 x \equiv b_2 (\bmod m_2), \\ \ldots \\ a_n x \equiv b_n (\bmod m_n), \end{cases} \tag{2}$$

where $GCD(a_1, m_1) = 1$; $GCD(a_2, m_2) = 1$;...; $GCD(a_n, m_m) = 1$, GCD – greatest common divisor.

Each comparison in system (2) can be solved separately, i.e. first record the comparison as

$$\begin{cases} x \equiv c_1 (\bmod m_1), \\ x \equiv c_2 (\bmod m_2), \\ \ldots \\ x \equiv c_n (\bmod m_n), \end{cases} \tag{3}$$

If at least one of the comparisons has no solutions, then the system is incompatible.

2. Study of fundamental theorems

Theorem 1. Let $GCD(m_1, m_2) = d$ is the greatest common divisor of numbers m_1 and m_2, a $SCM(m_1, m_2) = M$ is their smallest common multiple. System of two comparisons

$$\begin{cases} x \equiv c_1 (\bmod m_1), \\ x \equiv c_2 (\bmod m_2) \end{cases} \tag{4}$$

has a solution

$$x \equiv x_0 (\bmod M) \tag{5}$$

only on the condition that $c_2 \equiv c_1 (\bmod d)$.

Consequence: if m_1 and m_2 – are reciprocally prime numbers, then $d = 1$ and system (4) always has a single solution.

Substitution method. If a system (3) consisting of n is solved comparisons, you must first solve any two of them and replace them in system (3) expression (5). Next, take the obtained comparison and the third from the system and In each such step, the number of comparisons in the system decreases and at the end we get one comparison of the form (5), where M is the smallest common multiple of all modules.

Theorem 2 (Chinese remainder theorem). Let the system have (3) modules $m_1,$ m_2 ..., m_n – pairwise mutually prime; M – is the least common multiple of the numbers $m_1, m_2 \ldots, m_n; y_1, y_2, \ldots, y_n$ selected in such a way that comparisons are made $\frac{M}{m_1}y_1 \equiv 1(\mathrm{mod}\, m_1)$, $\frac{M}{m_2}y_2 \equiv 1(\mathrm{mod}\, m_2), \ldots,$ $\frac{M}{m_n}y_n \equiv 1(\mathrm{mod}\, m_n)$.

Then system (3) will have a single solution $x \equiv x_0(\mathrm{mod}\, M)$, where $x_0 = \frac{M}{m_1}y_1c_1 + \frac{M}{m_2}y_2c_2 + \ldots + \frac{M}{m_n}y_nc_n$.

3. Consideration of a control example of solving a system of comparisons

Solve the system of comparisons $\begin{cases} x \equiv 6(\mathrm{mod}17), \\ x \equiv 4(\mathrm{mod}11), \\ x \equiv -3(\mathrm{mod}8). \end{cases}$

Decision. 17, 11, 8 – pairwise mutually prime; $M = SCM(17{,}11{,}8) = 1496$ – the smallest common multiple of the modules.

I way. Using the substitution method, let's first solve a system consisting of the last two comparisons: $\begin{cases} x \equiv 4(\mathrm{mod}11), \\ x \equiv -3(\mathrm{mod}8). \end{cases}$

The system has a solution because $GCD(11{,}18) = 1$. Second system comparison indicates that $x = -3 + 8t, t = 0, \pm 1, \pm 2, \ldots$ Let's substitute this expression for x in the first comparison: $-3 + 8t \equiv 4(\mathrm{mod}11)$ or $8t \equiv 7(\mathrm{mod}11)$, where $t = 0, \pm 1, \pm 2, \ldots$. Let's solve comparison by the extended Euclidean algorithm (Table 1)

$GCD(11{,}18) = 1$; $1 = 11 \cdot 3 - 4 \cdot 8$. The inverse of the number 8 the modulus of 11 is –4, in additio, $-4 \equiv 7(\mathrm{mod}11)$. Let's multiply the comparison by 7:

$$t \equiv 7 \cdot 7(\mathrm{mod}11) \equiv 49(\mathrm{mod}11) \equiv 5(\mathrm{mod}11) \Rightarrow t = 5 + 11k, k = 0, \pm 1, \pm 2, \ldots$$

Table 1

Remnant	Quotient	x	y
11	–	1	0
8	–	0	1
3	1	$1-1\cdot 0=1$	$0-1\cdot 1=-1$
2	2	$0-2\cdot 1=-2$	$1-2\cdot(-1)=3$
1	1	$1-1\cdot(-2)=3$	$-1-1\cdot 3=-4$
0	2	–	–

Let's substitute the value of t in the expression for x: $x=-3+8\cdot(5+11k)=37+88k\Rightarrow x\equiv 37(\mathrm{mod}\,88)$.

Next, let's solve the system, which consists of the obtained comparison and the first comparison (remaining) of the original systems

$$\begin{cases} x\equiv 6(\mathrm{mod}17), \\ x\equiv 37(\mathrm{mod}88). \end{cases}$$

The system has a solution because $GCD(17,88)=1$. First system comparison indicates that $x=6+17t, t=0,\pm1,\pm2,...$ Let's substitute this expression for x in the second comparison: $6+17t\equiv 37(\mathrm{mod}\,88)$ or $17t\equiv 31(\mathrm{mod}\,88)$, where $t=0,\pm1,\pm2,...$ Let us solve the comparison using the extended Euclidean algorithm (Table 2).

Table 2

Remnant	Quotient	x	y
88	–	1	0
17	–	0	1
3	5	$1-5\cdot 0=1$	$0-5\cdot 1=-5$
2	5	$0-5\cdot 1=-5$	$1-5\cdot(-5)=26$
1	1	$1-1\cdot(-5)=6$	$-5-1\cdot 26=-31$
0	2	–	–

$GCD(17{,}88)=1$; $1=88\cdot 6-31\cdot 17$. The inverse of the number 17 is the modulus of 88 is –31, in addition, $-31\equiv 57(\mathrm{mod}88)$. Multiply the comparison by 57:

$$t\equiv 57\cdot 31(\mathrm{mod}88)\equiv 1767(\mathrm{mod}88)\equiv 7(\mathrm{mod}88)\Rightarrow t=7+88k,k=0,\pm1,\pm2,...$$

Let's substitute the value of t in the expression for x:

$$x=6+17\cdot(7+88k)=125+1496k\Rightarrow x\equiv 125(\mathrm{mod}1496).$$

Answer: $x\equiv 125(\mathrm{mod}1496)$ – by substitution method.

II way. According to the Chinese remainder theorem, we find:

1) $\frac{1496}{17}y_1\equiv 1(\mathrm{mod}17),\ 88y_1\equiv 1(\mathrm{mod}17),\ 3y_1\equiv 1(\mathrm{mod}17)\Rightarrow y_1=6;$

2) $\frac{1496}{11}y_2\equiv 1(\mathrm{mod}11),\ 136y_2\equiv 1(\mathrm{mod}11),\ 4y_2\equiv 1(\mathrm{mod}11)\Rightarrow y_2=3;$

3) $\frac{1496}{8}y_3\equiv 1(\mathrm{mod}8),\ 187y_3\equiv 1(\mathrm{mod}8),\ 3y_3\equiv 1(\mathrm{mod}8)\Rightarrow y_3=3;$

4) $x\equiv 88\cdot 6\cdot 6+136\cdot 3\cdot 4-187\cdot 3\cdot 3(\mathrm{mod}1496);$

$x\equiv 3168+1632-1683=3117(\mathrm{mod}1496)\Rightarrow x\equiv 125(\mathrm{mod}1496).$

Answer: $x\equiv 125(\mathrm{mod}1496)$ – according to the Chinese remainder theorem.

Conclusions

Based on the use of the proposed "ComparSystem_MathFIS" methodology, when performing a course assignment in the discipline "Mathematical Foundations Information Security" applicant for the degree "Bachelor" in the specialty "Cybersecurity" masters: subject competencies (solving module comparison systems using the substitution method and Chinese remainder theorem); professional competencies (application of theory and methods of protection to ensure information security in information and telecommunication systems and computer networks).

References:

1. Hrynevych L. M., Morze N. V., Boyko M. A. Scientific education as a basis Formation of Innovative Competence in the Context of Digital Transformation Society. Information Technologies and Learning Tools. 2020. T. 77. № 3. 1-26.

2. Distance course in the discipline "Mathematical Foundations of Information Security" for applicants for the degree "Bachelor" in the specialty "Cybersecurity"; Compiler: assoc. prof. Pakhomova V. M. Certificate DK0304 dated 03.07.2019.

3. Coutinho S. C. The mathematics of ciphers. Number theory and RSA cryptography. New York, 1999. 198 p.