http://www.moderntechno.de/index.php/meit/article/view/meit35-00-029
DOI: 10.30890/2567-5273.2024-35-00-029

UDC [004.7-047.72]:656.2

FORMATION OF COMPETENCIES AND SOFT SKILLS WHEN PERFORMING BRIGADE DISCIPLINE TASKS «MATHEMATICAL FOUNDATION OF INFORMATION SECURITY»

ФОРМУВАННЯ КОМПЕТЕНТНОСТЕЙ ТА SOFT SKILLS ПРИ ВИКОНАННІ БРИГАДНИХ ЗАВДАНЬ 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 proposed methodology of "SoftSkillsMathFIS" for the formation of competencies of applicants for a bachelor's degree in blended learning in the discipline "Mathematical Foundations of Information Security": 1) study of mathematical concepts (symbols Legendre and Jacobi, their properties) during lectures conducted with the help of Zoom system, 2) algorithmization and programming for the implementation of the Solovey-Strassen test and the organization of relevant research during laboratory work, 3) acquisition of practical skills in using probabilistic tests to determine the primality of a number on based on various mathematical approaches and tools when performing independent work with use of recommended sources, 4) elaboration of theoretical material on using the lecturer's presentations and passing testing in the "Lider" system.*

Keywords*: competence, blended learning, Legendre symbol, Jacobi symbol, properties of symbols, calculation algorithm, Solovey-Strassen test.*

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, and development of Soft Skills skills in applicants for a bachelor's degree in the following difficult conditions of our time, which 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; 4) development of Soft Skills applicants' skills, and became the basis for the development of our own methodology.

The aim of the article is to develop a methodology of "SoftSkillsMathFIS" for the formation of competencies and Soft Skills for Bachelor's degree applicants specialty "Cybersecurity" in the performance of brigade tasks in the discipline "Mathematical Foundations of Information Security".

General characteristics of the "SoftSkillsMathFIS" 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 "SoftSkillsMathFIS" provides an opportunity for applicants for the first degree in the discipline "Mathematical Foundations of Information Security": to get an idea of probabilistic tests to determine the primality of a number; study the Solovey-Strassen test [2]; analyze the solution of control cases No. 1-2 [3]; solve brigade tasks with the development of Soft Skills; formulate an appropriate conclusion.

1. The Legendre symbol

Let p – a prime number, p>2, a is a whole. The Legendre symbol is $L(a;p) = a^{\frac{p-1}{2}} \pmod{p}$.

Properties of the Legendre symbol

1) If $a \equiv b \pmod{p}$, then $L(a;p) = L(b;p)$

2) $L(a^2;p) = 1$, including $L(1;p) = 1$

3) $L(-1;p) = (-1)^{\frac{p-1}{2}}$

4) $L(a \cdot b \cdot \ldots \cdot s;p) = L(a;p) \cdot L(a;p) \cdot L(b;p) \cdot \ldots \cdot L(s;p)$,

5) $L(a^n;P) = (L(a;p))^n$

6) $L(2;P) = (-1)^{\frac{p^2-1}{8}}$

7) $L(q;p) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} L(p;q)$, where $p \neq q$, p, q are prime odd numbers (quadratic law of reciprocity).

8) $L(p;q) \cdot L(q,p) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$

These properties make it easy to compute the Legendre symbol without solving comparisons using such an algorithm.

Algorithm for calculating the Legendre symbol $L(a;p)$

1) If $a = 1$, then $L(1;p) = 1$.

2) If a is even number, then $L(a;P) = (-1)^{\frac{p^2-1}{8}} L(a/2;p)$.

3) If a – odd number and $a \neq 1$, then $L(a;p) = (-1)^{\frac{(a-1)(p-1)}{4}} L(p \bmod a; a)$.

2. The Jacobi Symbol

The Jacobi symbol *J(a; P)* is a function defined for all integers a, reciprocally simple with a given odd number *P*, thus: if $P = p_1 \cdot p_2 \cdot ... \cdot p_r$ – decomposition of the number *P* into prime factors (not necessarily different), then

$$J(a;P) = L(a;p_1) \cdot L(a;p_2) \cdot ... \cdot L(a;p_r),$$

where $L(a;p_i)$, $i = 1,...,r$ – Legendre symbols.

Properties of the Jacobi symbol

1) If $a \equiv b(\mathrm{mod}\,P)$, then $J(a;P) = J(b;P)$.

2) $J(a^2;P) = 1$, including $J(1;P) = 1$.

3) $J(-1;P) = (-1)^{\frac{P-1}{2}}$.

4) $J(a \cdot b \cdot ... \cdot l;P) = L(a;p_1) \cdot L(a;P) \cdot L(b;P) \cdot ... \cdot L(l;P)$.

5) $J(a^n;P) = (J(a;P))^n$.

6) $J(2;P) = (-1)^{\frac{P^2-1}{8}}$.

7) $J(Q;P) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}} J(P;Q)$, where $P \neq Q$, GCD(P,Q)=1, i.e. P, Q - reciprocal prime odd numbers (quadratic law of reciprocity); GCD – greatest common divisor.

8) $J(P;Q) \cdot J(Q,P) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}$.

Therefore, the Jacobi symbol is calculated according to the same rules as the symbol Legendre. Here is an algorithm for calculating the Jacobi symbol.

Algorithm for calculating the Jacobi symbol $J(a;P)$

1) If $a = 1$, then $J(1;P) = 1$.

2) If $a = b \cdot c$, then $J(a;P) = J(b;P) \cdot J(c;P)$.

3) If $\dfrac{P^2-1}{8}$ – even number, then $J(2;P) = 1$, but if $\dfrac{P^2-1}{8}$ – odd number, then $J(2;P) = -1$.

4) $J(a;P) = J(a \bmod P;P)$.

5) $J(a;p_1 p_2 \cdot ... \cdot p_r) = J(a;p_1) \cdot J(a;p_2) \cdot ... \cdot J(a;p_r)$.

6) If GCD(*a,P*)=1, *a* i *P* – odd numbers, then :

- when $\dfrac{(a-1)(P-1)}{4}$ – even number, $J(a;P) = J(P;a)$;

- when $\dfrac{(a-1)(P-1)}{4}$ – odd number, $J(a;P) = -J(P;a)$.

Remarks: if $p = P$, where *p* is a prime number, by definition the Jacobi symbol is at the same time, the symbol of Legendre. Entering the Jacobi symbol quite often simplifies calculating the Legendre symbol.

3. Probabilistic tests to determine the primality of a number

Probabilistic tests require consistency evenly to work distributed random numbers from the segment [1; n]. For each random number In this sequence, the fulfillment of some conditions is checked. If any of these conditions are not met, then the number n is composite. If all the conditions are met, then with With some probability, it can be argued that n is a prime number. This probability the closer to 1, the greater the number of random numbers to be applied. So In this way, probabilistic tests are tried to be probabilistic methods that any number that a given method declares to be prime, with extremely low probability may actually turn out to be composite.

Let's consider the approach implemented in the Solovey-Strassen probabilistic test. For an odd number $n \geq 3$ in terms of S_n we denote a subset of multiplicative group of surpluses Z_n^*, consisting of those elements *a,* that satisfy the comparison $J(a; n) = a^{(n-1)/2}$ (mod n), where $J(a; n)$ – Jacobi symbol. Due to the multiplicativeness of the Jacobi symbol, the subset of S_n is a subgroup of Group Z_n^*. By Lagrange's theorem, the order of the subgroup S_n of a finite group Z_n^* has be the divisor of the order of the group. Because $\left|Z_n^* = \varphi(n)\right|$, where $\varphi(n)$ – value Euler's function, the order of the subgroup S_n can be at most $\varphi(n)/2$, i.e. $\left|S_n\right| \leq \dfrac{\varphi(n)}{2}$. Equality $\left|S_n\right| \leq \dfrac{\varphi(n)}{2}$ indeed is the case for some numbers Carmichael, for example, for the number 1729. Therefore, when a is a randomly chosen number with sets $\{1,2,3,...,n-1\}$ and $a \in S_n$, the probability of randomly taking n as prime the number is $\dfrac{\varphi(n)}{2(n-1)} > \dfrac{1}{2}$.

4. Solovey-Strassen test

Step 1. Pick a random positive number $1 < a < n-1$.

Step 2. If GCD(a; n)≠1, then n is the composite number and the work of the algorithm terminate.

Step 3. Calculate value $j = a^{(n-1)/2} (\bmod n)$.

Step 4. Calculate the Jacobi symbol $J(a; n)$.

Step 5. If $j \neq J(a;n)$, then the number n is composite.

Step 6. If $j = J(a;n)$, then the number n is prime and the probability that this the result is false, does not exceed 0.5.

The prime number n passes the test with probability 1, because for all integers $a \in (1; n-1)$ step 2 of the algorithm is performed by the definition of a prime number, and step 6 of the algorithm - according to the Euler criterion. If the number *n* is composite, then both of these steps will be able to overcome only the elements of the subgroup $S_{n.}$ Therefore, the composite number *n* can withstand test with a probability, not higher $\frac{\varphi(n)}{2(n-1)} < \frac{1}{2}$.

Thus, the logical conclusion next: the error in the Solovey-Strassen test is one-sided. Recurrence testing *k* times with different values of *a* reduces the probability of error to $1/2^k$. This means that when 2^k different implementations of this algorithm can be expected at most one incorrect conclusion about the primality of *n.* When *k* = 30 the probability of this error is less 10^{-9}.

5. Control example No. 1.

Check with the Solovey-Strassen test the primality of *n*=2023 by choosing *a* =792.

Solution.

GCD(*a*; *n)* = GCD(2023, 792) = 1.

Next, let's calculate

$$j = a^{(n-1)/2} (\bmod n) = 792^{(2023-1)/2} (\bmod 2023) = 932.$$

The Jacobi symbol is *J*(*a; n*) = *J*(792; 2023) = +1.

Because $j \neq J(a;n)$ according to the Solovey-Strassen test, the number *n*=2023 – composite. Really, $2023 = 7 \cdot 17^2$.

6. Control example No. 2.

Check with the Solovey-Strassen test the primality of *n*=5987, if the probability of mistaking for prime is be less than $\varepsilon = 0{,}001$.

Solution.

A composite number *n* passes one test with probability $< 1/2$. Into in the case of an erroneous answer to the Solovey-Strassen test for *k* different values of *a* the probability that the number n is still mistaken for prime is less or equal to $1/2^k$.

Let *k* – positive integer for which $1/2^k < \varepsilon$, i.e. $1/2^k < 0{,}001$. Away $k \geq 10$. So you need to choose 10 different values of *a,* to the probability of mistaking *n*=5987 for prime was less than $\varepsilon = 0{,}001$. Let's choose *a* = 3 as a random number.

GCD(*a*; *n)* = GCD(3, 5987) =1.

Next, let's calculate

$$j = a^{(n-1)/2} (\bmod n) = 3^{(5987-1)/2} (\bmod 5987) \equiv 3^{2993} \equiv 1 (\bmod 5987).$$

The Jacobi symbol is

J(3; 5987)= - *J*(5987; 3)= $J(5987(\bmod 3);5987)$ = - *J*(2; 3) = - (- 1) = +1 = *j*.

So, at a=3, the number passed the primality test. Test results the numbers n=5987 with other values of a are given in Table. 1 [3].

Table 1

a	$j = a^{(n-1)/2}(\mathrm{mod}\, n)$	$J(a; n)$
3	1	1
5	-1	-1
7	-1	-1
9	1	1
11	-1	-1
13	-1	-1
15	-1	-1
17	1	1
25	1	1
101	-1	-1

So, for all the different ten values of the number a, we get $j = J(a;n)$, i.e. ten times the number n=5987 passed the primality test and can be considered prime with an error probability of less than 0.001.

Conclusions.

1. The proposed methodology of "SoftSkillsMathFIS" for the formation of competencies of applicants for a bachelor's degree in blended learning under time to complete team tasks in the discipline "Mathematical Foundations information security" provides: the use of the "Zoom" system during the lectures; face-to-face performance of laboratory work based on the created programs; performing independent work based on recommended sources; communication in social networks; conducting self-testing and modular testing with the help of the "Lider" system.

2. Based on the use of the "SoftSkillsMathFIS" methodology, the degree applicant "Bachelor": firstly, mastering subject competencies in the discipline "Mathematical Foundations of Information Security" (using a probabilistic test Solovey-Strassen on the definition of the primality of a number); secondly, it acquires practical skills in scientific activities in the organization and conduct of research (use of mathematical apparatus, algorithmization, programming, organization research and analysis of the results obtained); thirdly, he masters professional competencies (application of the theory and methods of protection to ensure information security in information and telecommunication systems and computer networks); fourthly, "Soft skills" (development of the ability to manage own time, the ability to work in a team, the development of team members, when the result of the group is defined as a summary and takes into account the achievements of each student of the group).

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. Kuznetsov G. V., Fomichev V. V., Sushko S. O., Fomicheva L. Ya. Mathematical Foundations of Cryptography; manual. Dnipropetrovsk: NGU, 2004. 391 p.

Анотація. *Запропонована методика «SoftSkillsMathFIS» щодо формування компетентностей здобувачів ступеня «бакалавр» при змішаному навчанні з дисципліни «Математичні основи інформаційної безпеки»: 1) вивчення математичних понять (символи Лежандра та Якобі, їх властивості) під час лекційних занятій, що проводяться за допомогою системи «Zoom», 2) алгоритмізація та програмування щодо реалізації тесту Соловея-Штрассена та організації відповідних досліджень під час лабораторних робіт, 3) придбання практичних навичків використання імовірнісних тестів для визначення простоти числа на основі різних математичних підходів та засобів під час виконання самостійної роботи з використанням рекомендованих джерел, 4) опрацьовування теоретичного матеріалу з використанням презентацій лектора та проходження тестування в системі «Лідер».*

Ключові слова: *компетентність, змішане навчання, символ Лежандра, символ Якобі, властивості символів, алгоритм обчислення, тест Соловея-Штрассена.*