Federal State Autonomous Educational Institution of Higher Education "Moscow Institute of Physics and Technology (National Research University)"

APPROVED
Head of the Phystech School of Applied Mathematics and Informatics
A.M. Raygorodskiy

Work program of the course (training module)

course: Algebra and Number Theory/Алгебра и теория чисел
major: Information Science and Computer Engineering
specialization: Computer Science/Информатика
Phystech School of Applied Mathematics and Informatics
Chair of Discrete Mathematics
term: 2
qualification: Bachelor

Semester, form of interim assessment: 3 (fall) - Grading test

Academic hours: 60 AH in total, including:
lectures: 30 AH.
seminars: 30 AH.
laboratory practical: 0 AH.

Independent work: 75 AH.

In total: 135 AH, credits in total: 3

Number of course papers, tasks: 2

Author of the program: A.A. Glibichuk, candidate of physics and mathematical sciences, associate professor

The program was discussed at the Chair of Discrete Mathematics 04.06.2020

Annotation

The course introduces the basic concepts of number theory. Definitions, basic theories, properties.

1. Study objective

Purpose of the course

- mastering the basic modern number theory.

Tasks of the course

- Students mastering basic knowledge (concepts, concepts, methods and models) in number theory;
- acquisition of theoretical knowledge and practical skills in number theory;
- providing advice and assistance to students in conducting their own theoretical studies in number theory.

2. List of the planned results of the course (training module), correlated with the planned results of the mastering the educational program

Mastering the discipline is aimed at the formation of the following competencies:

Code and the name of the competence	Competency indicators
UC-1 Search and identify, critically assess and synthesize information, apply a systematic approach to problem-solving	UC-1.2 Find, critically assess, and select information required for the task in hand
	UC-1.1 Analyze problems, highlight the stages of their solution, plan actions required to solve them
	UC-1.3 Consider various options for solving a problem, assess the advantages and disadvantages of each option
	UC-1.4 Make competent judgments and estimates supported by logic and reasoning
	UC-1.5 Identify and evaluate practical consequences of possible solutions to a problem
Gen.Pro.C-2 Use modern IT and software tools to perform professional tasks in compliance with information security requirements	Gen.Pro.C-2.3 Fulfill basic information security requirements
	Gen.Pro.C-2.2 Apply numerical mathematical methods and use software applications for scientific problem-solving in professional settings
	Gen.Pro.C-2.1 Apply modern computing tools and Internet services in professional settings
Gen.Pro.C-4 Collect and process scientific and technical and/or technological data for fundamental and applied problem-solving	Gen.Pro.C-4.1 Apply scientific research and intellectual analysis methods for professional problem-solving
	Gen.Pro.C-4.2 Search for primary sources of scientific and technical and/or technological information in professional settings
	Gen.Pro.C-4.3 Prepare abstracts, reports, bibliographies, and reviews of information in professional settings
	Gen.Pro.C-4.4 Use computer and network skills to obtain, store, and process scientific (technical, technological) information
Pro.C-1 Assign, formalize, and solve tasks, develop and research mathematical models of the studied phenomena and processes, systematically analyze scientific problems, obtain new scientific outcomes	Pro.C-1.1 Locate, analyze, and summarize information on current research findings within the subject area
	Pro.C-1.2 Make hypotheses, build mathematical models of the studied phenomena and processes, evaluate the quality of the developed model
	Pro.C-1.3 Apply theoretical and/or experimental research methods to a specific scientific task and interpret the obtained results

3. List of the planned results of the course (training module)

As a result of studying the course the student should:

know:

- Fundamental concepts, laws, theories of algebraic methods in number theory;
- modern problems of the relevant sections of the theory of algebraic methods in number theory;
- concepts, axioms, methods of proof and proof of the main theorems in the sections included in the basic part of the cycle of the theory of algebraic methods in number theory;
- basic properties of the corresponding mathematical objects;
- analytical and numerical approaches and methods for solving typical applied problems of the theory of algebraic methods in number theory.

be able to:

- Understand the task;
- use your knowledge to solve fundamental and applied problems;
- evaluate the correctness of the problem statements;
- strictly prove or disprove the statement;
- independently find algorithms for solving problems, including non-standard ones, and conduct their analysis;
- independently see the consequences of the results;
- accurately represent mathematical knowledge in topology orally and in writing.

master:

- Skills of mastering a large amount of information and solving problems (including complex ones);
- skills of independent work and mastering new disciplines;
- the culture of the formulation, analysis and solution of mathematical and applied problems that require the use of mathematical approaches and methods for their solution;
- the subject language of topology and the skills of competent description of problem solving and presentation of the results.

4. Content of the course (training module), structured by topics (sections), indicating the number of allocated academic hours and types of training sessions

4.1. The sections of the course (training module) and the complexity of the types of training sessions

№	Topic (section) of the course	Types of training sessions, including independent work			
		Lectures	Seminars	Laboratory practical	Independent work
1	Theory of Divisibility. The greatest common factor. Least common multiple.	6	6		12
2	Comparisons modulo. Properties of comparisons modulo.	6	6		15
3	Equations of the second degree modulo. The symbol of Legendre. The symbol of Jacobi. Compound module case.	8	6		16
4	Equations of arbitrary degree modulo simple.	4	6		16
5	Euclidean Algorithm. The main theorem of arithmetic.	6	6		16
AH in total		30	30		75
Exam preparation		0 AH.			
Total complexity		135 AH., credits in total 3			

4.2. Content of the course (training module), structured by topics (sections)

Semester: 3 (Fall)

1. Theory of Divisibility. The greatest common factor. Least common multiple.

Equivalence relations. Theorem on equivalence classes.

2. Comparisons modulo. Properties of comparisons modulo.

Equations of one variable modulo. Systems of equations of one variable for different modules. Chinese remainder theorem. Equations of a single variable in a compound module.

3. Equations of the second degree modulo. The symbol of Legendre. The symbol of Jacobi. Compound module case.

Primitive roots in a simple module.

4. Equations of arbitrary degree modulo simple.

Indices by an arbitrary module.

5. Euclidean Algorithm. The main theorem of arithmetic.

Complete deduction systems. The reduced system of deductions. Euler and Fermat's theorem.

5. Description of the material and technical facilities that are necessary for the implementation of the educational process of the course (training module)

A standard classroom.

6. List of the main and additional literature, that is necessary for the course (training module) mastering

Main literature

1. Языки и исчисления [Текст] : лекции по мат. логике и теории алгоритмов / Н. К. Верещагин, А. Шень .— 4-е изд., испр. — М. : МЦНМО, 2012 .— 240 с.
2. Алгоритмы [Текст] : [учеб. пособие для вузов] / С. Дасгупта, Х. Пападимитриу, У. Вазирани ; пер. с англ. А. А. Куликова ; под ред. А. Шеня .— М. : МЦНМО, 2014 .— 320 с.

Additional literature

1. Теория чисел [Текст] / Ш. Х. Михелович - М.Высшая школа,1967
2. Лекции по алгебраическому кодированию [Текст] : учеб. пособие для вузов / Э. М. Габидулин ; М-во образования и науки РФ, Моск. физ.-техн. ин-т (гос. ун-т) .— М. : МФТИ, 2015 .— 107 с.

7. List of web resources that are necessary for the course (training module) mastering

http://dm.fizteh.ru/

8. List of information technologies used for implementation of the educational process, including a list of software and information reference systems (if necessary)

Multimedia technologies can be used in lectures and practical exercises, including presentations.

9. Guidelines for students to master the course

1. It is recommended to successfully pass the test papers, as this simplifies the final certification in the subject.
2. To prepare for the final certification in the subject, it is best to use the lecture materials.

SUPPLEMENT

Assessment funds for course (training module)

major:	Information Science and Computer Engineering
specialization:	Computer Science/Информатика Phystech School of Applied Mathematics and Informatics Chair of Discrete Mathematics
term:	2
qualification:	Bachelor

Semester, form of interim assessment: 3 (fall) - Grading test

Author: A.A. Glibichuk, candidate of physics and mathematical sciences, associate professor

1. Competencies formed during the process of studying the course

Code and the name of the competence	Competency indicators
UC-1 Search and identify, critically assess and synthesize information, apply a systematic approach to problem-solving	UC-1.2 Find, critically assess, and select information required for the task in hand
	UC-1.1 Analyze problems, highlight the stages of their solution, plan actions required to solve them
	UC-1.3 Consider various options for solving a problem, assess the advantages and disadvantages of each option
	UC-1.4 Make competent judgments and estimates supported by logic and reasoning
	UC-1.5 Identify and evaluate practical consequences of possible solutions to a problem
Gen.Pro.C-2 Use modern IT and software tools to perform professional tasks in compliance with information security requirements	Gen.Pro.C-2.3 Fulfill basic information security requirements
	Gen.Pro.C-2.2 Apply numerical mathematical methods and use software applications for scientific problem-solving in professional settings
	Gen.Pro.C-2.1 Apply modern computing tools and Internet services in professional settings
Gen.Pro.C-4 Collect and process scientific and technical and/or technological data for fundamental and applied problem-solving	Gen.Pro.C-4.1 Apply scientific research and intellectual analysis methods for professional problem-solving
	Gen.Pro.C-4.2 Search for primary sources of scientific and technical and/or technological information in professional settings
	Gen.Pro.C-4.3 Prepare abstracts, reports, bibliographies, and reviews of information in professional settings
	Gen.Pro.C-4.4 Use computer and network skills to obtain, store, and process scientific (technical, technological) information
Pro.C-1 Assign, formalize, and solve tasks, develop and research mathematical models of the studied phenomena and processes, systematically analyze scientific problems, obtain new scientific outcomes	Pro.C-1.1 Locate, analyze, and summarize information on current research findings within the subject area
	Pro.C-1.2 Make hypotheses, build mathematical models of the studied phenomena and processes, evaluate the quality of the developed model
	Pro.C-1.3 Apply theoretical and/or experimental research methods to a specific scientific task and interpret the obtained results

2. Competency assessment indicators

As a result of studying the course the student should:

know:

- Fundamental concepts, laws, theories of algebraic methods in number theory;
- modern problems of the relevant sections of the theory of algebraic methods in number theory;
- concepts, axioms, methods of proof and proof of the main theorems in the sections included in the basic part of the cycle of the theory of algebraic methods in number theory;
- basic properties of the corresponding mathematical objects;
- analytical and numerical approaches and methods for solving typical applied problems of the theory of algebraic methods in number theory.

be able to:

- Understand the task;
- use your knowledge to solve fundamental and applied problems;
- evaluate the correctness of the problem statements;
- strictly prove or disprove the statement;
- independently find algorithms for solving problems, including non-standard ones, and conduct their analysis;
- independently see the consequences of the results;
- accurately represent mathematical knowledge in topology orally and in writing.

master:

- Skills of mastering a large amount of information and solving problems (including complex ones);
- skills of independent work and mastering new disciplines;
- the culture of the formulation, analysis and solution of mathematical and applied problems that require the use of mathematical approaches and methods for their solution;
- the subject language of topology and the skills of competent description of problem solving and presentation of the results.

3. List of typical control tasks used to evaluate knowledge and skills

Current control consists of two tests per semester, as well as oral delivery of tasks for independent solution. Evaluation criteria are attached. Also attached is an example of a test assignment and several tasks for independent solution on various topics at the end of the program.

4. Evaluation criteria

1. The theory of divisibility. The greatest common factor. Least common multiple. Euclidean Algorithm. The main theorem of arithmetic.
2. Relations of equivalence. Theorem on equivalence classes.
3. Comparisons modulo. Properties of comparisons modulo. Complete deduction systems. The reduced system of deductions. Euler and Fermat's theorem.
4. The equations of one variable modulo. Systems of equations of one variable for different modules. Chinese remainder theorem. Equations of a single variable in a compound module.
5. The equations of the second degree modulo. The symbol of Legendre. The symbol of Jacobi. Compound module case.
6. Primitive roots in a simple module. Primitive roots modulo p.
7. Indices by a simple module.
8. Equations of arbitrary degree modulo simple. Equations of arbitrary degree modulo pα and p2α.
9. Indices modulo 2α. Indices by an arbitrary module.

Assessment “excellent (10)” is given to a student who has displayed comprehensive, systematic and deep knowledge of the educational program material, has independently performed all the tasks stipulated by the program, has deeply studied the basic and additional literature recommended by the program, has been actively working in the classroom, and understands the basic scientific concepts on studied discipline, who showed creativity and scientific approach in understanding and presenting educational program material, whose answer is characterized by using rich and adequate terms, and by the consistent and logical presentation of the material;

Assessment “excellent (9)” is given to a student who has displayed comprehensive, systematic knowledge of the educational program material, has independently performed all the tasks provided by the program, has deeply mastered the basic literature and is familiar with the additional literature recommended by the program, has been actively working in the classroom, has shown the systematic nature of knowledge on discipline sufficient for further study, as well as the ability to amplify it on one’s own, whose answer is distinguished by the accuracy of the terms used, and the presentation of the material in it is consistent and logical;

Assessment “excellent (8)” is given to a student who has displayed complete knowledge of the educational program material, does not allow significant inaccuracies in his answer, has independently performed all the tasks stipulated by the program, studied the basic literature recommended by the program, worked actively in the classroom, showed systematic character of his knowledge of the discipline, which is sufficient for further study, as well as the ability to amplify it on his own;

Assessment “good (7)” is given to a student who has displayed a sufficiently complete knowledge of the educational program material, does not allow significant inaccuracies in the answer, has independently performed all the tasks provided by the program, studied the basic literature recommended by the program, worked actively in the classroom, showed systematic character of his knowledge of the discipline, which is sufficient for further study, as well as the ability to amplify it on his own;

Assessment “good (6)” is given to a student who has displayed a sufficiently complete knowledge of the educational program material, does not allow significant inaccuracies in his answer, has independently carried out the main tasks stipulated by the program, studied the basic literature recommended by the program, showed systematic character of his knowledge of the discipline, which is sufficient for further study;

Assessment “good (5)” is given to a student who has displayed knowledge of the basic educational program material in the amount necessary for further study and future work in the profession, who while not being sufficiently active in the classroom, has nevertheless independently carried out the main tasks stipulated by the program, mastered the basic literature recommended by the program, made some errors in their implementation and in his answer during the test, but has the necessary knowledge for correcting these errors by himself;

Assessment “satisfactory (4)” is given to a student who has discovered knowledge of the basic educational program material in the amount necessary for further study and future work in the profession, who while not being sufficiently active in the classroom, has nevertheless independently carried out the main tasks stipulated by the program, learned the main literature but allowed some errors in their implementation and in his answer during the test, but has the necessary knowledge for correcting these errors under the guidance of a teacher;

Assessment “satisfactory (3)” is given to a student who has displayed knowledge of the basic educational program material in the amount necessary for further study and future work in the profession, not showed activity in the classroom, independently fulfilled the main tasks envisaged by the program, but allowed errors in their implementation and in the answer during the test, but possessing necessary knowledge for elimination under the guidance of the teacher of the most essential errors;

Assessment “unsatisfactory (2)” is given to a student who showed gaps in knowledge or lack of knowledge on a significant part of the basic educational program material, who has not performed independently the main tasks demanded by the program, made fundamental errors in the fulfillment of the tasks stipulated by the program, who is not able to continue his studies or start professional activities without additional training in the discipline in question;

Assessment “unsatisfactory (1)” is given to a student when there is no answer (refusal to answer), or when the submitted answer does not correspond at all to the essence of the questions contained in the task.

5. Methodological materials defining the procedures for the assessment of knowledge, skills, abilities and/or experience

During examination the student are allowed to use the program of the discipline.