MODULE OUTLINE

1. GENERAL INFORMATION

SCHOOL	SCHOOL OF SCIENCE AND TECHNOLOGY		
PROGRAM COURSE	MASTER IN MATHEMATICS		
LEVEL OF STUDY	POSTGRADUATE		
MODULE CODE	MSM85	**YEAR OF STUDY**	2nd
MODULE TITLE	ALGEBRA AND GEOMETRY		
INDEPENDENT TEACHING ACTIVITIES *in case credits are awarded for separate components/parts of the course, e.g. in lectures, laboratory exercises, etc. If credits are awarded for the entire course, give the weekly teaching hours and the total credits*		**HOURS**	**CREDIS**
Weekly workload in hours: 17.5 x 32 weeks		560	20 ECTS
COURSE TYPE Compulsory, Optional, Optional mandatory	Elective, instead of MSM83.		
PREREQUISITE MODULES:	None		
LANGUAGE OF INSTRUCTION AND EXAMS	GREEK		
THE MODULE IS OFFERED TO ERASMUS STUDENTS	No (due to the annual duration of the module)		
MODULE WEBSITE (URL)	https://www.eap.gr/en/postgraduate-studies-in-mathematics/topics/#m85 Each module has its own space in the Learning Management System of EAP (http://study.eap.gr), with controlled access (use of code) for students and teaching staff.		

2. LEARNING OUTCOMES

Learning Outcomes

- *The course learning outcomes, specific knowledge, skills and competences of an appropriate (certain) level, which students will acquire upon successful completion of the course, are described in detail. It is necessary to consult:*

Learning Outcomes: Upon successful completion of MSM85 “Algebra and Geometry”, students will have developed the following skills:

- Knowledge of the basic elements of Number Theory
- Knowledge of the applications of Number Theory in Cryptography
- Knowledge and comprehension of Group Theory
- Knowledge of the structure of Euclidean spaces

- Knowledge of the theory of the isometric groups of Euclidean spaces, in particular dimensions 2 and 3.
- Ability to calculate and study groups of symmetries of simple geometric shapes

General Learning Outcomes: Upon successful completion of MSM85, students will have obtained the following:

- Knowledge and comprehension of the fundamental concepts of Number Theory and its applications in Cryptography
- Knowledge of the structure of Euclidean spaces and their isometric groups
- Knowledge of the interaction between Group Theory and Geometry in the study of Euclidean Spaces

General Competences

Taking into consideration the general competences that students/graduates must acquire (as those are described in the Diploma Supplement and are mentioned below), at which of the following does the course attendance aim?

Search for, analysis and synthesis of data and information by the use of appropriate technologies,
Adapting to new situations
Decision-making
Individual/Independent work
Group/Team work
Working in an international environment
Working in an interdisciplinary environment
Introduction of innovative research
Project planning and management
Respect for diversity and multiculturalism
Environmental awareness
Social, professional and ethical responsibility and sensitivity to gender issues
Critical thinking
Development of free, creative and inductive thinking
……
(Other…….citizenship, spiritual freedom, social awareness, altruism etc.) …….

Search for, analysis and synthesis of data and information by the use of appropriate technologies,
Adapting to new situations
Decision-making
Individual/Independent work
Project planning and management
Critical thinking
Development of free, creative and inductive thinking

3. MODULE CONTENT

Module MSMB85 discusses the basic elements of Number Theory and its applications in Cryptography, the basic elements of Group Theory and the theory of Euclidean spaces and their isometry groups.
The cognitive subjects of the module are the following:

- Number Theory
- Group Theory
- Groups and Geometry

In particular, the curriculum of the MSM85 includes the following topics:

Number Theory and Algebraic Structures
a). Euclidean Division – Arithmetic Algorithms – Fast Multiplication – Greatest Common Divisor – Least Common Multiple – Euclidean Algorithm - Primes– Primitive Analysis and Applications.
b). Monoids – Groups – Subgroups – Cyclic Groups – Group Morphisms – Rings – Polynomials – Greatest Common Divisor – Euclidean Algorithm – Polynomial over a Field – Irreducible Polynomials.
c). Congruences – Linear Congruences – The Euler ϕ function – Order of an Integer mod n – Finite Fields.
d) Integer Factorization Algorithms – Primality Tests – Algorithms for the Computation of Discrete Logarithm.

Cryptography and Codes
Fundamentals of Cryptology – RSA, Rabin and ElGamal cryptosystems – Digital Signatures RSA, Rabin and DSA – Diffie-Hellman key protocol– Error Correcting Codes – Linear Codes – Generator Matrices – Control Matrices – Decoding.

Affine Geometry
Affine Spaces – Barycenter – Affine Subspaces – Affine Frames – Affine Maps – Affine Groups – Multilinear Maps – Multiaffine Maps – Polynomial Curves – Berstein Polynomials – Bézier Form of a Polynomial Curve – De Casteljau Algorithm – Subdivision Algorithm – De Boor Algorithm – Derivatives of Polynomial Curves – Joining Polynomial Curves.

4. TEACHING METHODS--ASSESSMENT

<table>
<tr><td>MODES OF DELIVERY
Face-to-face, in-class lecturing, distance teaching and distance learning etc.</td><td>Distance education with six (6) Group Counseling Meetings [GSM (Greek abbreviation: «ΟΣΣ»] during the academic year, on weekends.</td></tr>
<tr><td>USE OF INFORMATION AND COMMUNICATION TECHNOLOGY
Use of ICT in teaching, Laboratory Education, Communication with students</td><td>• Cisco Wevex Platform (for the implementation of the Group Counseling Meetings) via teleconference meetings.
• Usage of Mathematica software for real-time presentation of examples and problem solving
• Presentation software (Powerpoint, LaTEx Beamer) for lecture notes presentation.
• Usage of Scientific Databases (Scopus, Web of Science) for research in the existing bibliography.</td></tr>
<tr><td>MODULE DESIGN
Description of teaching techniques, practices and methods: Lectures, seminars, laboratory practice, fieldwork, study and analysis of bibliography, tutorials, Internship, Art Workshop, Interactive teaching,</td><td>
<table>
<tr><th>Activity</th><th>Annual Workload</th></tr>
<tr><td>6 GSM (* 4 hours)</td><td>24</td></tr>
<tr><td>Preparation of Assignments (6 assignments * 24 hours)</td><td>144</td></tr>
<tr><td>Examination</td><td>4</td></tr>
<tr><td>Individual study</td><td>388</td></tr>
</table>
</td></tr>
</table>

Educational visits, projects, Essay writing, Artistic creativity, etc *The study hours for each learning activity as well as the hours of selfdirected study are given following the principles of the ECTS.*	**Total module workload (hours)** | **560**
STUDENT PERFORMANCE EVALUATION/ASSESSMENT METHODS *Detailed description of the evaluation procedures.* *Language of evaluation, assessment methods, formative or summative (conclusive), multiple choice tests, short- answer questions, open-ended questions, problem solving, written work, essay/report, oral exam, presentation, laboratory work, other……etc.* *Specifically defined evaluation criteria are stated, as well as if and where they are accessible by the students*	Elaboration of written assignments during the academic year, the average of the grades of which participates in the formation of the final grade of the module by 30%, under the condition of passing to the stage of the final examinations. The condition for passing to the stage of final examinations is the submission of 5/6 written assignments with grade 50/100. In the final written examinations the grade of the written assignments participates in the formation of the final grade of module by 70%. All the criteria are posted, both in each written assignment (in the LMS study.eap.gr), as well as in the general regulation of HOU at: https://www.eap.gr/education/study-regulations/

(6) SUGGESTED BIBLIOGRAPHY

- Δ. Πουλάκης, Υπολογιστική Θεωρία Αριθμών, Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών, 2015 (www.kallipos.gr).
- **Niederreiter,** Harald**, Winterhof**, Arne, Applied Number Theory, Springer 2015.
- Δ. Πουλάκης, Αλγεβρικοί Κώδικες, Εκδόσεις Ζήτη, Θεσσαλονίκη 2010.
- J. Gallier Curves and Surfaces in Geometric Modeling: Theory and Algorithms (διατίθεται ελεύθερα στην ηλεκτρονική διεύθυνση https://www.cis.upenn.edu/~jean/gbooks/geom1.html).

Relevant Scientific Journals

- Acta Arithmetica.
- Journal of Number Theory.
- Mathematics of Computation
- Journal of Algebra.
- Journal of Cryptology.
- Designs, Codes and Cryptography

- Computer Aided Geometric Design
- International Journal of Computational Geometry and Applications