Program	Type of studies (cycle)	Third cycle
	Name of the program	SEE Doctoral Studies in Mathematical Science

COURSE

Course title	**Algorithmic number theory**			
Course code	Semester	Course status	ECTS credits	Contact hours
PMAT 605		Optional	10	30
Teaching staff	Teacher	Prof. Dr. Almasa Odžak		
	Other staff			
Course goals	Number theory has always exhibited a unique feature that some appealing and easily stated problems tend to resist the attempts for solutions over very long periods of time. It has influenced and has been influenced by developments in many mathematical disciplines. Several breakthroughs that took place during the last decades on one hand and an unprecedented range of applications on the other have significantly enlarged the interested mathematical community. The part of the number theory dealing with algorithms constructed to solve problems in number theory is algorithmic number theory. The course is designed to provide insights into this mathematical discipline. Specific topics will be selected according to student's interests.			

Course content/topics

- Number theory and complexity.
- Euclidean algorithm for greatest common divisor, worst case complexity analysis.
- Binary GCD algorithm, continuous fractions.
- Modular arithmetic, Chinese reminder theorem, quadratic residues.
- Legendre and Jacobi symbols.
- Solving equations over finite fields, roots, Hensel's lemma.
- Basic algorithms for prime numbers, and primality tests for numbers of a special form.
- Pseudoprimes and Carmichael numbers, probabilistic primality tests.
- Sieve primality tests, generating random prime numbers.
- Factorization algorithms.

LITERATURE

[1] Eric Bach and Jeffrey Shallit: Algorithmic Number Theory, Volume I: Efficient Algorithms, MIT Press, August 1996.

[2] Yan, Song Y.: Number Theory for Computing, 2nd ed., Springer Verlag, 2002.

[3] H. Cohen: A Course in Computational Number Theory, Graduate Texts in Mathematics 138, Springer Verlag, Berlin, 1993.

Grading

	Criterion	Points	Cut-off points
1.	Written assignment		
2.	Project		
3	Final exam		
Total		100	55