Kod		Nazwa przedmiotu	Computational number theory
Prowadzący przedmiot			Paweł Gładki

Kierunek	Informatyka										Stopień	I
Specjalność												
Rodzaj studiów	stacjonarne	Rok studiów	4	Semestr	Zimowy	Numer semestru	7					
Rodzaje zajęć, liczba godzin*)	W	15	A	-	L	15	P	—	S	—	K	—
ECTS		Język	Angielski	Forma nauczania	traditional							
WWW	http://www.math.us.edu.pl/~pgladki/teaching/index.html											

Cel przedmiotu, uzyskiwane kompetencje (maksymalnie 4 wiersze)

The main purpose of this class is to present methods and algorithms in number theory, which find important applications in contemporary computer science. In particular we will be concerned with modern methods of recognizing prime numbers and eventually factoring composite numbers.

Program wykładu (maksymalnie 10 wierszy)

Prime and composite numbers. Sieve methods, Meissel, Lehmer, Odlyzk and Deleglise algorithms. Primality testing, Lucas sequences, pseudoprimes and Carmichael numbers and their distribution. Quadratic residues and their distribution, quadratic reciprocity law. Primitive roots and asymptotic distributions. Finite fields and their properties. Chinese remainder theorem and its applications. Indices and discrete logarithms. Adleman, Pomerance and Rumely algorithms and Jacobi sum Lenstra test. Conjectures in computational number theory and algorithms based on conjectures. Exponential and sub-exponential methods. Arithmetics of elliptic curves, Kilian-Goldwasser and Atkin Morain tests. Polynomial and normal bases. Optimal bases. Software packages. Network computing projects (GIMPS).

Charakterystyka pozostałych zajęć (maksymalnie 7 wierszy)

This course is essentially tied with lab sessions. During these sessions students will be required to deepen and strenghten whatever they will have learned in lectures. Students will be able to understand new concepts and effectively apply them in their current work.

Bibliografia (nie więcej niż 5 kluczowych pozycji, maksymalnie 7 wierszy

1.M. Bressoud: *Factorization and Primality Testing,* Springer, 1989.

2. H. Cohen: *A Course in Computational and Algebraic Number Theory,* Springer, 2008.

3. R. Crandall, C. Pomerance: *Prime Numbers, A Computational Perspective,* Springer, 2001.
4. R. J. MCEliece, *Finite Fields for Computer Scientists and Engineers,* Kluwer Accad. Publ.,1987;

Wymagane wiadomości z zakresu	No preliminaries.
Forma zaliczenia przedmiotu	Passing lab sessions.
Zasady wystawiania oceny końcowej	Lab sessions grade.
Słowa kluczowe (maksymalnie 5 słów)	Computational number theory, prime testing, finite fields, elliptic curves, network computing.

*) liczba godzin w semestrze; **W** – wykład, **A** – ćwiczenia audytoryjne, **L** – zajęcia laboratoryjne, **P** – zajęcia projektowe, **S** – seminarium, **K** – konwersatorium