

Kod		Nazwa przedmiotu	Obliczeniowa algebra i teoria liczb
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	Polski		Forma nauczania		tradycyjna							
WWW	http://www.math.us.edu.pl/~pgladki/teaching/index.html													

Cel przedmiotu, uzyskiwane kompetencje (maksymalnie 4 wiersze)

Główny cel tego wykładu to omówienie metod i algorytmów algebry i teorii liczb, które znajdują ważne zastosowania w ramach współczesnej informatyki. W szczególności dotyczy to nowoczesnych metod kryptograficznych i obliczeń symbolicznych.

Program wykładu (maksymalnie 10 wierszy)

Pierścienie przemienne. Pierścienie wielomianów. Porządki dopuszczalne w zbiorze jednomianów, bazy Groebnera i S-wielomiany. Omówienie wybranych algorytmów obliczania baz Groebnera, algorytm Buchbergera. Przykłady zastosowań (algebra różniczkowa i całkowanie symboliczne, algorytmy Almkvista i Zeilbergera, sumowanie symboliczne, algorytm Gospera, sieci Petriego, analiza algorytmów). Liczby pierwsze i złożone. Metody sita, Algorytmy Meissela, Lehmera, Odlyzki i Deleglise'a. Testy pierwszości, ciągi Lucasa, liczby pseudopierwsze i Carmichaela i ich rozkład. Prawo wzajemności reszt i szyfry strumieniowe. Pierwiastki pierwotne, rozkłady asymptotyczne. Ciała skończone i ich własności. Twierdzenie chińskie o resztach i jego zastosowania. Indeks i logarytm dyskretny. Algorytm Adlemana, Pomerance'a i Rumely'ego oraz test sum Jacobiego Lenstry. Algorytmy oparte na hipotezach. Metody wykładnicze i subwykładnicze. Arytmetyka krzywych eliptycznych, test Kiliana-Goldwassera oraz Atkina Moraina. Bazy wielomianowe i normalne. Bazy optymalne. Pakiety programowe. Projekty sieciowe (GIMPS).

Charakterystyka pozostałych zajęć (maksymalnie 7 wierszy)

Przedmiot obejmuje też zajęcia laboratoryjne. Treści tych zajęć ugruntowują i rozszerzają wiedzę przekazywaną podczas wykładów. Studenci będą mogli zrozumieć pojawiające się nowe koncepcje oraz stosować je efektywnie w swojej bieżącej pracy.

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. J. Von zur Gathen, J. Gerhard, *Modern computer algebra*, 2nd Edition, Cambridge, 2003.
4. M.F. Atiyah, I.G. Macdonald, *Introduction to commutative algebra*, Springer, 2008.
5. G.-M. Greuel, G. Pfister, *A Singular introduction to commutative algebra*, Springer, 2008.

Wymagane wiadomości z zakresu	Brak preliminariów.
Forma zaliczenia przedmiotu	Zaliczenie zajęć laboratoryjnych.
Zasady wystawiania oceny końcowej	Ocena z zajęć laboratoryjnych.
Słowa kluczowe (maksymalnie 5 słów)	Obliczeniowa teoria liczb, testy pierwszości, ciała skończone, krzywe eliptyczne, pakiety sieciowe.

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

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