Szczegółowy opis zajęć
(KARTA PRZEDMIOTU)

Nazwa zajęć: ALGEBRA Z ZASTOSOWANIAMI
Kod zajęć: Alg
Przynależność do grupy zajęć: Algebra z zastosowaniami (grupa zajęć 4)
Rodzaj zajęć: kierunkowy
obowiązkowy
Kierunek studiów: MATEMATYKA
Poziom studiów: studia drugiego stopnia
Profil studiów: ogólnoakademicki
Forma studiów: stacjonarne
Specjalność (specjalizacja): wszystkie
Rok studiów: I
Semestr studiów: 2
Formy prowadzenia zajęć, wraz z liczbą godzin dydaktycznych:
wykłady – 30;
ćwiczenia –30.
Język/i, w którym/ch prowadzone są zajęcia: polski
Liczba punktów ECTS *(zgodnie z programem studiów)*: **4**
* – *pozostawić właściwe*

1. Założenia przedmiotu:

   Celem przedmiotu jest zapoznanie studenta z wybranymi zagadnieniami algebry współczesnej oraz ich zastosowaniami w innych działach matematyki, techniki, informatyki i kryptografii.

2. Odniesienie kierunkowych efektów uczenia się do form prowadzenia zajęć oraz sposobów weryfikacji i oceny efektów uczenia się osiągniętych przez studenta:

symbol	zakładane efekty uczenia się *student, który zaliczył zajęcia:*	formy prowadzenia zajęć	sposoby weryfikacji i oceny efektu uczenia się
Wiedza: zna i rozumie			
K2A_W11	matematyczne podstawy teorii informacji, teorii algorytmów i kryptografii oraz ich praktyczne zastosowania m.in. w naukach technicznych, ekonomii, programowaniu i szeroko rozumianej informatyce	wykład, ćwiczenia	kolokwium, referat
K2A_W12	elementy teorii grafów i ich przykładowe zastosowania informatyczne i techniczne	wykład, ćwiczenia	kolokwium, referat
Umiejętności: potrafi			
K2A_U09	stosować metody algebraiczne w rozwiązywaniu problemów z różnych działów matematyki i zadań praktycznych	wykład, ćwiczenia	kolokwium, referat
K2A_U12	stosować oraz przedstawiać w mowie i na piśmie, metody co najmniej jednej wybranej gałęzi matematyki: algebry i teorii liczb, matematyki dyskretnej i teorii grafów	wykład, ćwiczenia	kolokwium, referat
K2A_U16	rozpoznawać struktury matematyczne (np. algebraiczne, geometryczne) w teoriach fizycznych	wykład, ćwiczenia	kolokwium, referat

3. Treści programowe zapewniające uzyskanie efektów uczenia się *(zgodnie z programem studiów)*:

   Grupy, kody korekcyjne i kodowanie grupowe. Kody wielomianowe. Kod Hamminga. Ciała skończone. Kody BCH. Kryptografia. Podstawowe protokoły kryptograficzne. Problem faktoryzacji i kryptoanaliza RSA. Maszyny Turinga i obliczalność. Złożoność obliczeniowa. Złożoność obliczeniowa problemów algebraicznych.

4. Opis sposobu wyznaczania punktów ECTS:

Forma aktywności	Liczba godzin / punktów ECTS
Liczba godzin zajęć, niezależnie od formy ich prowadzenia	60 / 2 ECTS
Praca własna studenta - przygotowanie do zajęć	30 / 1 ECTS
Praca własna studenta – przygotowanie do kolokwium	15 / 0,5 ECTS
Inne: konsultacje, wykorzystanie platformy zdalnej edukacji	15 / 0,5 ECTS
Suma godzin	**120 / 5 ECTS**
Liczba punktów ECTS przypisana do zajęć	**4**

Objaśnienia:
* – praca własna studenta, należy wymienić formy aktywności, np. *przygotowanie do zajęć, interpretacja wyników, opracowanie raportu z zajęć, przygotowanie do egzaminu, zapoznanie się z literaturą, przygotowanie projektu, prezentacji, pracy pisemnej, sprawozdania itp.*

** – inne np. *dodatkowe godziny zajęć*

5. Wskaźniki sumaryczne:
   – liczba godzin zajęć oraz liczba punktów ECTS na zajęciach z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów: 60 / 2 ECTS
   – liczba godzin zajęć oraz liczba punktów ECTS na zajęciach związanych z prowadzoną w Politechnice Śląskiej działalnością naukową w dyscyplinie lub dyscyplinach, do których przyporządkowany jest kierunek studiów – w przypadku studiów o profilu ogólnoakademickim: 60 / 2 ECTS
   – liczba godzin zajęć oraz liczba punktów ECTS na zajęciach kształtujących umiejętności praktyczne – w przypadku studiów o profilu praktycznym: nie dotyczy
   – liczba godzin zajęć prowadzonych przez nauczycieli akademickich zatrudnionych w Politechnice Śląskiej jako podstawowym miejscu pracy: 60 / 2 ECTS
6. Osoby prowadzące poszczególne formy zajęć *(imię, nazwisko, stopień naukowy lub stopień w zakresie sztuki, tytuł profesora, służbowy adres e-mail)*:

   Nadiya Gubareni, dr hab., Nadiya.Gubareni@polsl.pl
7. Szczegółowy opis form prowadzenia zajęć:

   1) wykłady:
      – szczegółowe treści programowe:

        Elementy teorii liczb, grup, pierścieni i ciał. Konstrukcja ciała skończonego. Multiplikatywna grupa ciała skończonego. Pierwiastki pierwotne i indeksy. Przykłady zastosowań algebry i teorii liczb w kryptografii. Podstawowe algorytmy kryptograficzne z kluczem publicznym. Podpisy cyfrowe. Algorytmy współdzielenia sekretu. Algebry skończenie wymiarowe. Konstrukcja Cayley'a-Dicksona. Kwaterniony i ich zastosowanie w grafice komputerowej. Algebraiczne aspekty teorii kodów korekcyjnych. Kody wielomianowe, Hamminga, BCH.
      – stosowane metody kształcenia, w tym metody i techniki kształcenia na odległość:

        Wykład.
      – forma i kryteria zaliczenia, w tym zasady zaliczeń poprawkowych, a także warunki dopuszczenia do egzaminu:

        Warunkiem zaliczenia jest pozytywna ocena przygotowanego przez studenta referatu oraz zaliczenie wszystkich efektów kształcenia przewidzianych dla przedmiotu.
      – organizacja zajęć oraz zasady udziału w zajęciach, ze wskazaniem czy obecność studenta na zajęciach jest obowiązkowa,

        Obecność na wykładzie nie jest obowiązkowa, ale zalecana, ponieważ na kolokwiach obowiązują wiadomości nie tylko z ćwiczeń, ale również z wykładów.

   2) ćwiczenia:
      – szczegółowe treści programowe:

        Studenci rozwiązują (samodzielnie lub z pomocą prowadzącej) zadania związane z treścią wykładu oraz przedstawiają przygotowane przez siebie referaty na zadany temat.
      – stosowane metody kształcenia, w tym metody i techniki kształcenia na odległość:

        Rozwiązywanie zadań, dyskusja, referat.
      – forma i kryteria zaliczenia, w tym zasady zaliczeń poprawkowych, a także warunki dopuszczenia do egzaminu:

        Warunkiem zaliczenia jest pozytywna ocena przygotowanego przez studenta referatu oraz zaliczenie wszystkich efektów kształcenia przewidzianych dla przedmiotu.
      – organizacja zajęć oraz zasady udziału w zajęciach, ze wskazaniem czy obecność studenta na zajęciach jest obowiązkowa,

        Obecność na ćwiczeniach jest obowiązkowa.
8. Opis sposobu ustalania oceny końcowej (zasady i kryteria przyznawania oceny, a także sposób obliczania oceny w przypadku zajęć, w skład których wchodzi więcej niż jedna forma prowadzenia zajęć, z uwzględnieniem wszystkich form prowadzenia zajęć oraz wszystkich terminów egzaminów i zaliczeń, w tym także poprawkowych):

Nie dotyczy. Przedmiot kończy się zaliczeniem (bez egzaminu).

9. Sposób i tryb uzupełniania zaległości powstałych wskutek:
   - nieobecności studenta na zajęciach,

     Zaległości z wykładu i ćwiczeń student uzupełnia samodzielnie na podstawie notatek kolegów, dostępnej literatury oraz konsultacji z prowadzącą zajęcia.
   - różnic w programach studiów osób przenoszących się z innego kierunku studiów, z innej uczelni albo wznawiających studia na Politechnice Śląskiej,

     Każdy tego typu przypadek będzie rozpatrywany indywidualnie przez Prodziekan ds. Studenckich i prowadzącą przedmiot.
10. Wymagania wstępne i dodatkowe, z uwzględnieniem sekwencyjności zajęć:

    Algebra liniowa i geometria analityczna, algebra w zakresie obowiązującym modułowi kształcenia na I stopniu kierunku Matematyka.
11. Zalecana literatura oraz pomoce naukowe:
    1. A. Bialynicki-Birula, *Algebra*, PWN, Warszawa, 2009
    2. A.I. Kostrikin, *Wstęp do algebry*, t.I, III, PWN, Warszawa 2005
    3. W.J. Gilbert, W.K. Nicholson, *Algebra współczesna z zastosowaniami*, WNT, Warszawa, 2008
    4. N. Gubareni, *Algebra współczesna i jej zastosowania*, Wyd. PCz, Częstochowa, 2018
    5. N. Koblitz, *Wykład z teorii grup i kryptografii*, WNT, Warszawa 2006
    6. N. Koblitz, *Algebraiczne aspekty kryptografii*, WNT, Warszawa 2002.
12. Opis kompetencji prowadzących zajęcia *(np. publikacje, doświadczenie zawodowe, certyfikaty, szkolenia itp. związane z treściami programowymi realizowanymi w ramach zajęć)*:

    Publikacje oraz wieloletnie doświadczenie zawodowe.
13. Inne informacje: