بسمه‌تعالی

دانشگاه صنعتی اصفهان
دفتر مدیریت برنامه‌ریزی و ارتقای کیفیت آموزشی

فرم پیشنهاد ایجاد/فعال‌سازی درس

تاریخ ارسال: 1398 / 08/06

دانشکده پیشنهاد دهنده: **علوم ریاضی**	گروه آموزشی مطابق با کد درس: **گروه ریاضی**

عنوان درس: نظریه اعداد

Title: Number theory

درس سرویسی است؟ **خیر** **کد پیشنهادی:** مقطع درس: **کارشناسی**

پیش‌نیاز درس (هم نیاز): **ریاضی عمومی 2**

نوع درس: الف) **اصلی** ب) **نظری** تعداد واحد: **انتخاب کنید** درس آزمایشگاهی/کارگاهی است؟ **خیر**
تعداد ساعت آزمایشگاه در هفته **انتخاب کنید**

آیا درس مذکور دارای سرفصل مورد تائید وزارت عتف است؟ **بلی-سرفصل پیوست شده است.** در صورت مثبت بودن لطفا پیوست نامه فرمایید*.

میزان همپوشانی (مشابهت) با دروس موجود در دانشکده : • درصد و با سایر دروس دانشگاه : • درصد

نام دروس مشابه در دانشکده: نام دروس مشابه در دانشگاه:

اگر درس پیشنهادی جدید نیست اطلاعات زیر تکمیل شود:
فعال شدن درس نام درس: **نظریه اعداد** تعداد واحد: **4** کد درس: **1914392**

امکانات ویژه و الزامات مورد نیاز جهت ارائه درس: (شامل حل‌تمرین، بازدید علمی و سایر امکانات)

اهمیت و ضرورت ارائه درس: (شامل اهداف آموزشی درس نمی‌شود)

محور اصلی درس نظریه اعداد مطالعه اعداد است. از شاخه های اصلی نظریه اعداد میتوان به نظریه جبری اعداد، نظریه تحلیلی اعداد، نظریه محاسباتی اعداد، نظریه احتمالاتی اعداد و نظریه ترکیبیاتی اعداد اشاره کرد. الگوریتم های اعداد اول وتوابع توزیع آنها به ویژه الگوریتم‌های سریع برای امتحان اعداد اول و تجزیه اعداد صحیح در رمزنگاری و علوم کامپیوتر کاربردهای مهمی دارند.

هدف اصلی در این درس آشنایی با مفاهیم مقدماتی در مورد اعداد صحیح، اعداد اول، معادله های همنهشتی و معادله های سیاله است. ارائه این درس به عنوان درس اصلی در دوره کارشناسی ریاضی ضروری است.

شرح درس (بین 4 تا 10 خط کامل نوشته شده و سرفصلها تنها با کاما جدا شوند. از بکار بردن جمله دارای فعل، پرانتز، خط فاصله و دونقطه خودداری شود.)

بخشپذیری، الگوریتم تقسیم، بزرگترین مقسوم علیه مشترک، الگوریتمهای سریع برای محاسبه بزرگترین مقسوم علیه مشترک، معادله های دیوفانتین خطی، اعداد اول، تجزیه به توان‌های اعداد اول، توزیع اعداد اول، اعداد اول فرما و مرسن، هم نهشتی‌ها، محاسبات پیمانه ای، هم نهشتی‌های خطی، قضیه باقیمانده چینی، حساب در Zp، قضیه کوچک فرما، تابع اویلر، اعداد شبه اول، هم نهشتی‌ها در پیمانه توان یک عدد اول، گروه یکهها، ریشههای اولیه، مانده‌های مربعی، نماد لژاندر، محک اویلر، لم گاوس، قانون تقابل مربعی، اعداد تام، توابع حسابی، حلقه توابع حسابی، دستور عکس موبیوس، مجموع مربع‌ها، قضیه مجموع دو مربع، کسرهای مسلسل، حل برخی معادله‌های دیوفانتین، کاربرد فراگیر اعداد اول در رمزنگاری، آشنایی با نرم افزارهای ریاضی برای پیاده سازی الگوریتمهای ارائه شده در این درس.

English Course Description: (جز کلمه آغازین هر سرفصل و اسامی خاص، حرف اول همه واژگان، با حرف کوچک تایپ شود.)

Divisibility, Division algorithm, Greatest common divisor, Fast algorithms for computing Greatest common divisor, Linear Diophantine equations, Prime numbers, Prime-power factorizations, Distribution of primes, Fermat and Mersenne primes, Congruences, Modular arithmetic, Linear congruences, Chinese remainder theorem, The arithmetic of Zp, Fermat's little theorem, Euler's function, Pseudoprimes, Congruences with a prime-power modulus, The group of units, Primitive roots, Quadratic residues, The Legendre symbol, Euler's criterion, Gauss's lemma, Quadratic reciprocity, Perfect numbers, Arithmetic functions, The ring of arithmetic functions, The Mobius inversion formulae, Sum of squares, The sum of two squares theorem, Continued fractions, Solving some Diophantine equations, The ubiquity of prime numbers in cryptography, Introduction to mathematical software for implementing the algorithms in this course.

مراجع (لطفا مراجع فارسی و انگلیسی به روش **APA** نوشته شود؛ نام خانوادگی، حرف اول نام. (سال انتشار). عنوان مرجع (نوبت چاپ). محل انتشار: ناشر.)

توجه: برای درس آزمایشگاهی/کارگاهی، دستورکار به عنوان آخرین مرجع فارسی ذکر شود.

(1

References :

1) Jones, G.A. and Jones, J.M. (1998), Elementary Number Theory, Springer-Verlag.
2) Rosen, K.H. (2011), Elementary Number Theory, Pearson.

*** – در صورت ارائه درس جدید (در صورت عدم تصویب توسط وزارت عتف) موارد زیر پیوست شود:**

1- سوابق آموزشی و پژوهشی مدرس (مدرسین) مرتبط با درس پیشنهادی،

2- سوابق ارائه درس در سایر دانشگاه‌های کشور یا دانشگاه‌های معتبر خارج از کشور همراه با سرفصل‌ها (در مجموع حداقل دو مورد کافی است).