عنوان درس	فارسی	نظریه اعداد محاسباتی								
	انگلیسی	Computational Number Theory								
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
پایه		اصلی		تخصصی		اختیاری		۳	۴۸	نظریه اعداد، برنامه‌سازی C
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی			
حل تمرین: ندارد						نیاز به اجرای پروژه عملی: ندارد				

هدف: آشنایی با روش‌های محاسباتی در نظریه اعداد با هدف تحلیل عددی و کاهش پیچیدگی محاسبات برای الگوریتم‌ها در نظریه اعداد که کاربردهای متعددی در رمزنگاری و علوم کامپیوتر دارند.

سرفصل‌های درس:

- مروری کوتاه بر مقدمات نظریه اعداد و جبر چون قضیه باقیمانده چینی، قضیه کوچک فرما، تابع اویلر، دنباله Lucas، نماد Jacoby و ...
- الگوریتم‌های کارای ضرب، جمع، تفسیم، توان رساندن و نظایر آن در حلقه‌های متناهی و الگوریتم‌های مختلف پیمانه گرفتن مانند Montgomery reduction و Barrett reduction
- الگوریتم‌های غربالگری اعداد مرکب Table-Lookup، Bit-Array و Constructive Methods
- الگوریتم‌های آزمون اول بودن: آزمون‌های احتمالاتی Miller-Rabin، Solovay-Strassen، Ballie-PSW و آزمون قطعی Agrawal-Kayal-Saxena و مقایسه آنها از لحاظ پیچیدگی زمانی و حافظه مصرفی
- الگوریتم‌های تجزیه اعداد و مطالعه پیچیدگی محاسباتی آنها
- حساب خم‌های بیضوی
- بکارگیری کتابخانه اعداد بزرگ زبان C++ برای پیاده‌سازی الگوریتم‌های ارائه شده در درس

منابع

[1] R. Crandall, C. Pomerance, Prime Numbers, A Computational Perspective, Springer, 2000.
[2] Victor Shoup, Computational Introduction to Number Theory and Algebra, Cambridge University Press, 2005.