| نظریه مقدماتی اعداد | | | |
|---|---|---|---|
| **تعداد واحد/ساعت** | **پیش نیاز/هم نیاز** | **از جدول** | **حل تمرین (ساعت)** |
| ۳ واحد/ ۵۱ ساعت | پس از مبانی جبر | ۷ | حداقل ۲۵ |

**هدف:**

نظریه‌ی اعداد مطالعه ویژگی‌های اعداد به ویژه اعداد صحیح و گویا است. هدف اصلی این درس مطالعه ویژگی‌های بخشپذیری، همنهشتی‌ها و حل معادله‌های سیاله (دیوفانتی) و کاربردهایی در رمزنگاری و کدگذاری است.

**سخنی با مدرس و دانشجـــو:**

نظریه اعداد به خاطر تاریخ غنی و مسئله های سهل و ممتنع آن مورد علاقه ریاضیدانان حرفه ای و همچنین دوستداران غیر حرفه ای آن بوده است. ولی در سال های اخیر نظریه اعداد را به خاطر کاربرد های آن در رمزنگاری و کدگذاری نیز مورد مطالعه قرار می دهند.

مسئله های این درس بسیار ساده به نظر می رسند ولی حل آن‌ها ممکن است چنین نباشد و وقت زیادی از شما را طلب کند و به دروس دیگر لطمه وارد کند. بنابراین سعی کنید روش ها را بیاموزید و وقت خود را با توجه به درس های دیگری که دارید تنظیم کنید. در درس های بعد و دوره های تحصیلات تکمیلی می توانید آموخته های خود را به کار ببرید.

**سرفصل درس:** بخشپذیری، الگوریتم تقسیم، بمم و کمم، قضیه اساسی حساب، معرفی و مطالعه حلقه همنهشتی $\mathbb{Z}_n$ و گروه ضربی $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ حل و بحث معادله های سیاله، توابع حسابی. قانون تقابل مربی، کاربرد هایی در رمزنگاری و کدگذاری.

**ریز مواد:** برای تنظیم زمان، ساعت‌های زیر برای تدریس مطالب پیشنهاد می‌شود.

**بخشپذیری و تجزیه (۶ ساعت):** بخشپذیری، الگوریتم تقسیم، اعداد اول، قضیه اساسی حساب (۳ ساعت). بزرگترین مقسوم علیه مشترک، نمایش خطی و الگوریتم اقلیدس (۱/۵ ساعت). حل معادله های سیاله ی خطی (۱/۵ ساعت).

**همنهشتی ها (۹ ساعت):** تعریف و ویژگی‌های مقدماتی، دستگاه مانده ها و مخفف مانده ها (معرفی حلقه $\mathbb{Z}_n$ و گروه ضربی $\mathbf{C_n}$ متشکل از عضوهای وارونپذیر $\mathbb{Z}_n$ و گروه ضربی $\mathbf{C_p}$ به زبان همنهشتی) (۳ ساعت). همنهشتی های خطی، دستگاه همنهشتی‌های خطی، قضیه‌ی مانده چینی (۳ ساعت). قضیه های فرما، اویلر، ویلسن (بیان ارتباط آن‌ها با گروه $\mathbf{C_n}$ و $\mathbf{C_p}$). برخی از نتایج (۳ ساعت).

**ریشه های اولیه (۶ ساعت):** تعریف رتبه ی ضربی به پیمانه های $n$ و $p$ (در $\mathbb{Z}_n$ و $\mathbf{C_p}$) و ویژگی های آن (۱/۵ ساعت). ریشه های اولیه (مولد های گروه ضربی $\mathbf{C_p}$) وجود آنها (۲ ساعت). حل و بحث معادله‌های همنهشتی چندجمله ای (به پیمانه n) $f(x) \equiv 0$ (۲/۵ ساعت).

**توابع حسابی (۶ ساعت):** تابع حسابی، ضربی. تعداد و مجموع مقسوم علیه ها، تابع موبیوس ، تابع فی اویلر (۳ ساعت). اعداد اول مرسن، اعداد تام، اعداد تام زوج (۳ ساعت).

**مانده های درجه دوم (۶ ساعت):** مانده و نامانده ی درجه دوم و ویژگی‌های آنها (۱/۵ ساعت). محک اویلر، لم گاوس( شاید بدون اثبات، همراه با مثال) (۱/۵ ساعت). قانون تقابل مربعی (۳ ساعت).

**مباحث دیگر (۱۲ ساعت):** کسرهای مسلسل (۳ ساعت). مجموع دو و چهار مربع (۲ ساعت). سه تایی های فیثاغورثی (۲ ساعت). معادله پل (۲ ساعت). اشاره به کاربرد نظریه اعداد در رمزنگاری و کدگذاری (۳ ساعت).