

# نظریه اعداد

تألیف:

**دکتر حسین خبازیان**

استاد یار دانشکده علوم ریاضی  
دانشگاه صنعتی اصفهان

۱۳۸۶



دانشگاه علمی اصفهان  
مرکز

گروه علوم ۳۹

شماره کتاب ۱۰۹

نظریه اعداد

|                        |   |                               |
|------------------------|---|-------------------------------|
| تألیف                  | : | دکتر حسین خبازیان             |
| ویراستار               | : | دکتر منصور معتمدی             |
| حروف چینی کامپیوتری    | : | مرکز نشر دانشگاه صنعتی اصفهان |
| لیتوگرافی، چاپ و صحافی | : | مرکز نشر دانشگاه صنعتی اصفهان |
| ناشر                   | : | مرکز نشر دانشگاه صنعتی اصفهان |
| چاپ اول                | : | تابستان ۱۳۸۶                  |
| تیراژ                  | : | ۱۵۰۰ جلد                      |
| شابک                   | : | ۹۶۴-۸۴۷۶-۲۸-۴                 |
| قیمت                   | : | ۲۷۰۰ تومان                    |

|                         |   |                                                                   |
|-------------------------|---|-------------------------------------------------------------------|
| سرشناسه                 | : | خبازیان اصفهانی، حسین، ۱۳۲۷-                                      |
| عنوان و نام پدیدآور     | : | نظریه اعداد/حسین خبازیان.                                         |
| وضعیت نشر               | : | اصفهان: دانشگاه صنعتی اصفهان، مرکز نشر، ۱۳۸۵.                     |
| مشخصات ظاهری            | : | چهار، ۲۲۳ ص.                                                      |
| فروست                   | : | دانشگاه صنعتی اصفهان، مرکز نشر، شماره کتاب؛ ۱۰۹،<br>گروه علوم؛ ۳۹ |
| شابک                    | : | ۹۶۴-۸۴۷۶-۲۸-۴                                                     |
| یادداشت کلی             | : | فیبا                                                              |
| یادداشت عنوان و پدیدآور | : | ص.ع. به انگلیسی: Hossein Khabazian. Number theory                 |
| موضوع                   | : | نظریه اعداد - راهنمای آموزشی (عالی).                              |
| موضوع                   | : | نظریه اعداد - مسائل، تمرینها و غیره (عالی).                       |
| شناسه افزوده            | : | دانشگاه صنعتی اصفهان، مرکز نشر                                    |
| رده بندی دیویی          | : | ۵۱۲/۰۷                                                            |
| رده بندی کنگره          | : | QA ۲۴۱/۶ ن ۶                                                      |
| شماره کتابشناسی ملی     | : | ۳۹۲۸۶-۳۸۵                                                         |

حق چاپ برای مرکز نشر دانشگاه صنعتی اصفهان محفوظ است.

اصفهان: دانشگاه صنعتی اصفهان - مرکز نشر - کد پستی ۸۴۱۵۶

تلفن: ۰۳۱۱-۳۹۱۲۵۰۹ (۰۳۱۱) دورنگار: ۳۹۱۲۵۵۲ (۰۳۱۱)

## بنام خدا

### پیش گفتار

بسیار دیده می‌شود که بحث‌هایی در ریاضیات شبیه هم هستند و با تعریف سامانه‌های مناسب می‌توان نتیجه‌گیری کلی به عمل آورده و سپس آن نتایج کلی را، در یک مبحث ریاضی که در آن سیستم جای می‌گیرد به کاربرد. این روش، به مطالب ریاضی نظم بهتری می‌بخشد، پیچیدگی مطالب را کم می‌کند و از طرف دیگر از تکرار بحث‌های به ظاهر متفاوت ولی در اصل یکسان، جلوگیری می‌کند. در نتیجه با صرف وقت بسیار کمتری می‌توان مطالب را فراگرفت و با تسلط بیشتری آنها را به کاربرد. جبر به چنین روش‌هایی می‌پردازد. پس یکی از موارد استفاده عمده جبر در دیگر شاخه‌های ریاضی و از جمله نظریه اعداد است.

در این کتاب سعی شده است تا از امکاناتی که مقدماتی از گروه‌ها و حلقه‌ها در اختیار ما قرار داده استفاده کرده تا از دوباره کاری و تکرار مطالب جلوگیری کرده باشیم. به همین لحاظ برای مطالعه این کتاب، لازم است خواننده با مقدمات نظریه گروه‌ها و حلقه‌ها آشنائی داشته باشد.

در تنظیم یک مطلب ریاضی، زمانی که تقسیم‌بندی مطالب به قضایای مختلف و نیز تقسیم مطالب هر فصل به بخش‌های مختلف مشخص شد، دو موضوع در تنظیم هر بخش حائز اهمیت است بخصوص اگر آن بخش طولانی و مثلاً در حد یک بخش از یک کتاب باشد. اول این که نتیجه‌گیری‌ها را چگونه به قضایای مختلف تقسیم کنیم که گویا تر و کمترین حجم ممکن را به خود اختصاص دهد و هر چه راحت تر به توان مطلبی را که به دنبالش هستیم در آن بخش پیدا کنیم. مثلاً تا آنجا که ممکن است نتایج شبیه هم و در ارتباط با یکدیگر را در قالب بندهای یک قضیه بیان کنیم. گاهی اتفاق می‌افتد که به دنبال جواب سوالی هستیم که مکرراً با آن سروکار پیدا می‌کنیم اما قضیه‌ای در کتاب وجود ندارد که به توان در آن جواب را پیدا کرد بلکه مجبوریم چندین قضیه را از قسمت‌های مختلف انتخاب کرده و با یک تحلیل از آنها به جواب برسیم درحالی‌که میشد با تغییر شکل تقسیم‌بندی چند قضیه و تغییر بیان آنها، بدون حجیم تر کردن کتاب و کاستن از نتایج، بر این مشکل فائق شد. دوم این که چه فرض‌ها و چه نتیجه‌هایی را برجسته تر بیان کنیم تا اهمیت قضیه را برای خواننده بهتر بیان کرده باشیم.

هدف ما از تألیف این کتاب سعی در هرچه بهتر تنظیم کردن مطالب نظریه اعداد مقدماتی به شکلی که شرح داده‌شد، در قالب یک کتاب است تا خواننده با مشکلات کمتر و بدون

سردرگمی بتواند مطالب کتاب را فراگیرد و نیز راحت تر بتواند به جواب سوال موردنظر خود برسد و احاطه بیشتری بر مطالب داشته باشد.

در فصل اول به بیان مقدمات می‌پردازیم. از جمله با مفاهیم بخش پذیری، اعداد اول، بزرگ‌ترین مقسوم علیه مشترک و کوچک‌ترین مضرب مشترک آشنا می‌شویم. در فصل دوم به بررسی حلقه  $\mathbb{Z}/n\mathbb{Z}$  می‌پردازیم و از نتایج آن در نظریه اعداد استفاده می‌کنیم. در فصل سوم به حل معادلات همنهشتی درجه دوم می‌پردازیم. در فصل چهارم، ابتدا معادلات دو مجهولی درجه دوم را مورد بحث قرار می‌دهیم و سپس به بحث مجموع دو مربع و معادله پل می‌پردازیم. در فصل پنجم به ارتباط بین زیرگروه‌های ضربی یک هیأت متناهی و مشخصه آن می‌پردازیم. نتایج حاصل، مورد نیاز در حل معادلات همنهشتی درجه دوم، درجه سوم و درجه چهارم است. در فصل ششم به حل معادلات همنهشتی درجه سوم و در فصل هفتم به حل معادلات همنهشتی درجه چهارم می‌پردازیم.

در این کتاب مجموعه اعداد طبیعی به  $\mathbb{N}$ ، مجموعه اعداد صحیح به  $\mathbb{Z}$ ، مجموعه اعداد گویا به  $\mathbb{Q}$ ، مجموعه اعداد حقیقی به  $\mathbb{R}$  و مجموعه اعداد مختلط به  $\mathbb{C}$  نشان داده شده است. همچنین مسائل مشکل با \* و مسائل مشکل تر با \*\* مشخص شده اند. این مسائل برای دانشجویان کنجکاو و مستعد در نظر گرفته شده اند.

از آقای دکتر منصور معتمدی استاد گروه ریاضی دانشگاه شهید چمران اهواز که ویرایش کتاب را بر عهده داشته اند سپاسگزاری مینمایم. همچنین برخورد لازم میدانم از شورای انتشارات دانشگاه صنعتی اصفهان و از کارکنان مرکز نشر دانشگاه بخاطر همکاری مؤثر در مراحل چاپ کتاب تشکر کنم.

دکتر حسین خبازیان

استادیار دانشکده علوم ریاضی  
دانشگاه صنعتی اصفهان

# فهرست مندرجات

|                    |    |
|--------------------|----|
| فصل اول: بخش پذیری | ۱  |
| ۱-۱ بخش پذیری      | ۱  |
| ۲-۱ اعداد اول      | ۱۵ |
| ۳-۱ تابع جزء صحیح  | ۲۳ |
| ۴-۱ توابع حسابی    | ۳۲ |

|                           |    |
|---------------------------|----|
| فصل دوم: همنهشتی          | ۳۹ |
| ۱-۲ همنهشتی               | ۳۹ |
| ۲-۲ حل معادلات خطی        | ۴۷ |
| ۳-۲ همنهشتی اعداد اول     | ۶۵ |
| ۴-۲ ساختمان گروه $U(Z_m)$ | ۶۹ |
| ۵-۲ روش های محاسباتی      | ۸۰ |

|                                          |    |
|------------------------------------------|----|
| فصل سوم: مانده درجه دوم - تقابل درجه دوم | ۸۳ |
| ۱-۳ مانده درجه دوم - نماد لژانر          | ۸۳ |
| ۲-۳ نماد ژاکوبی                          | ۹۴ |

|                                 |     |
|---------------------------------|-----|
| فصل چهارم: معادلات دیوفانتی     | ۱۰۱ |
| ۱-۴ معادلات دو مجهولی درجه دوم  | ۱۰۱ |
| ۲-۴ مجموع دو مربع               | ۱۱۸ |
| ۳-۴ معادله پل و چند معادله دیگر | ۱۲۶ |

|                                        |     |
|----------------------------------------|-----|
| فصل پنجم: مجموع گاوس - مجموع ژاکوبی    | ۱۴۱ |
| ۱-۵ اعداد جبری - اعداد صحیح جبری       | ۱۴۱ |
| ۲-۵ مشخصه ضربی روی یک گروه متناهی دوری | ۱۴۷ |

|          |                              |     |
|----------|------------------------------|-----|
| ۱۵۲..... | مجموع گاوس-مجموع ژاکوبی      | ۳-۵ |
| ۱۵۷..... | تعمیم مجموع ژاکوبی           | ۴-۵ |
| ۱۶۴..... | مشخصه‌های از مرتبه ۲ و ۳ و ۴ | ۵-۵ |

|          |                          |     |
|----------|--------------------------|-----|
| ۱۷۵..... | فصل ششم: حلقه‌های $Z[w]$ |     |
| ۱۷۶..... | خواص عمومی               | ۱-۶ |
| ۱۸۶..... | حلقه $Z[w]$              | ۲-۶ |
| ۱۹۸..... | حلقه $Z[i]$              | ۳-۶ |

|          |                               |     |
|----------|-------------------------------|-----|
| ۲۰۷..... | فصل هفتم: کاربرد مجموع گاوس   |     |
| ۲۰۷..... | تقابل درجه دوم-تقابل درجه سوم | ۱-۷ |
| ۲۱۴..... | تقابل درجه چهارم              | ۲-۷ |