دانشگاه کاشان

نظریه اعداد

حسن دقیق

دانشکده علوم ریاضی

بهمن ماه سال ۱۳۹۲

فهرست مطالب

بسمه تعالی

پیش گفتار

نظریه‌ی اعداد یکی از قدیمی‌ترین یا شاید قدیمی‌ترین شاخه‌ریاضیات می‌باشد. اولین آثار علمی انسجام یافته به عنوان یک نظریه، بیشتر منسوب به فیثاغورث است(۵۶۹ الی ۵۰۰ قبل از میلاد). در طول قرون، این نظریه، دانشمندان بزرگ و هم‌چنین افراد غیرحرفه‌ای بسیاری را به خود جلب کرده است.

دلیل این امر این است که مسائل بعضاً بسیار پیچیده در این نظریه، آن قدر ساده و بدون نیاز به زبانی پیچیده قابل بیان هستند که توجه و کنجکاوی هر فرد را بر می‌انگیزند. همواره تصور بر این بود که دلیل پرداختن به نظریه‌ی اعداد بیشتر سرگرمی و علاقه به پرداختن به چالش‌های فکری جدی در افراد بوده است. به طوری که حتی دانشمندان این شاخه‌ی ریاضی بعضاً هیچ‌گونه کاربردی عملی برای نظریه‌ی اعداد قائل نبوده‌اند. هاردی (۱۸۷۷ الی ۱۹۴۷ میلادی) دانشمند برجسته‌ی ریاضی در شاخه‌ی نظریه‌ی اعداد جایی می‌گوید:

«این ادعا و خوشحالی گاوس و سایر ریاضی‌دانان که، علم یکی بیشتر نیست و آن همان است که آنان دارند (نظریه‌ی اعداد)، شاید این‌گونه قابل درک و توجیه باشد که فاصله‌ی زیاد این نظریه از هرگونه فعالیت بشر معمولی، این نظریه را پاک و قابل احترام نگه می‌دارد.»

به‌همین دلیل در دهه‌های اخیر این زمینه از ریاضی در برنامه‌های درسی دبیرستان‌ها و دانشگاه‌ها به‌شدت مورد غفلت قرار گرفته و تقریباً به فراموشی سپرده شده است. این غفلت به دو دلیل جای تأسف است.

این زمینه یکی از بهترین زمینه‌ها برای آموزش ریاضی و آشنا کردن دانشجویان با روش‌های علمی در ریاضی، و هم‌چنین پرورش قدرت تفکر علمی و استدلال در آن‌هاست. پیش نیازها و مقدمات زیادی نیاز ندارد، قابل درک و فهم است و در عین حال روش‌ها به شدت علمی و استدلالی هستند. در حل مسائل نظریه‌ی اعداد، دانشجو ضمن قادر بودن به آزمون و خطا می‌تواند کنجکاوی، شهود، استعداد، خلاقیت و قدرت استدلال خود را به کار بندد. علاوه‌براین امروزه، با کاربرد وسیع این نظریه در برخی شاخه‌های علوم کامپیوتر به‌ویژه در رمزنگاری و مباحث مربوط به امنیت و صحت ارتباطات، نظریه‌ی اعداد در خط مقدم شاخه‌های کاربردی ریاضی قرار گرفته است. حتی نتایج و ایده‌های مقدماتی نوشته‌ی حاضر، امروزه اساس نظری سیستم‌های امنیتی و رمزنگاری بسیار پیشرفته‌ای در جهان را تشکیل می‌دهند.

متن حاضر خلاصه‌ای از مباحثی است که در درس نظریه‌ی اعداد دوره‌ی کارشناسی ریاضی مطرح می‌شود. مطالب به نحوی گزینش شده‌اند که حتی در سال اول دوره‌ی کارشناسی قابل ارائه‌اند. اگرچه توصیه می‌شود در سال‌های دوم یا سوم تدریس شوند.

متن به هیچ وجه کامل نیست و در واقع هسته‌ی اصلی بحث را پوشش می‌دهد. برای پخته شدن بحث برخی از مطالب به عنوان تکمیلی حسب علاقه‌ی دانشجویان و یا سلیقه‌ی مدرس باید اضافه شوند. برخی از این مطالب می‌تواند اعداد مرسن و اعداد اول مرسن، اعداد فرما، اعداد تام، زوج اعداد متحابه، حدس گلدباخ، لگاریتم گسسته، حل معادلات پِل و ... باشد.

علاوه‌براین، متن بدون اضافه شدن فصلی در خصوص کاربرد نظریه اعداد در سیستم‌های امنیتی و رمزنگاری ناقص است. سعی خواهد شد این بحث جداگانه در یادداشت‌های تکمیلی در اختیار دانشجویان قرار گیرد. به دانشجویان توصیه می‌شود ضمن مطالعه‌ی متن، حتماً تمرینات در بین بحث و پایان فصل‌ها و هم‌چنین کتب دیگری در این زمینه را حل نمایند. کتب فراوانی، اغلب به زبان انگلیسی، یافت می‌شوند که علاوه بر کامل‌تر بودن، حین عرضه‌ی مطالب، نکات تاریخی زیبایی را یادآور شده‌اند. مرور این کتب که برخی از آن‌ها در پایان این نوشتار ذکر شده‌اند به دانشجویان گرامی توصیه می‌شود.

حسن دقیق

قدردانی

بر خود لازم می‌دانم از دانشجویان عزیزی که در سال‌های قبل در خصوص محتوا و اشتباهات تایپی بخشی از نسخه‌های دست نویس این نوشتار، تذکراتی داده‌اند، تشکر نمایم. از خانم سمیه دیداري که ضمن مطالعه متن ،اصلاحات علمي و نگارشي را انجام داده اند، از آقای محمدرضا وحیدی‌فرد به خاطر تایپ بخشی از متن و از آقای سید عادل مروّجی به خاطر صفحه‌آرایی نهایی تشکر می‌نمایم.
تذکر هرگونه اشتباه تایپی یا محتوایی و ارائه‌ی پیشنهادات جهت تغییرات و تکمیل نوشتار از طرف خوانندگان محترم، موجب سپاس اینجانب خواهد بود.

حسن دقیق

از خانم‌ها وجیهه فهیمی تبار ، ملیحه صادقی کاشانی و سمیه کیاني جم، دانشجویان درس نظریه اعداد در ترم هاي گذشته که اشکالات زیاد در ویرایش قبل را یادداشت و به اینجانب تحویل نمودند، تشکر می‌نمایم.

حسن دقیق
بهمن ۱۳۹۰

فصل ۱
بخش‌پذیری

§ ۱.۱ اصل خوش‌ترتیبی

موضوع در درس نظریه‌ی اعداد مطالعه‌ی اعداد و خواص و برخی روابط در مجموعه‌ی اعداد است. منظور از عدد بیشتر اعداد صحیح است. اگر چه گاهی با اعداد گویا و حقیقی نیز سر و کار خواهیم داشت. این‌که این اعداد چه هستند و چگونه ساخته می‌شوند موضوع بحث ما نیست. پاسخ به این سئوال را شاید تا حدودی در درس مبانی ریاضیات یا مقدمات آنالیز دیده باشید. ما بدون کنکاش زیاد در مورد چیستی اعداد و طریقه‌ی ساختن آن‌ها، آن‌ها را شناخته شده می‌گیریم.

مجموعه‌ی

$$\mathbb{N} = \{۱, ۲, ۳, \ldots, n, \ldots\}$$

را مجموعه‌ی اعداد طبیعی و

$$\mathbb{Z} = \{\pm ۱, \pm ۲, \pm ۳, \ldots, \pm n, \ldots\}$$

را مجموعه‌ی اعداد صحیح می‌نامیم. اعمال جمع و ضرب و تقسیم و تفریق و خواص مقدماتی این اعمال در مجموعه‌ی $\mathbb{Z}$ آشنا است. شما حتماً با اصل اساسی زیر آشنا هستید:

- **اصل خوش ترتیبی:** هر زیر مجموعه‌ی ناتهی از $\mathbb{N}$ دارای کوچکترین عضو است.

اصل خوش ترتیبی بدین معناست که اگر S یک زیرمجموعه‌ی ناتهی از مجموعه‌ی $\mathbb{N}$ باشد، آن‌گاه عددی چون a در S یافت می‌شود به‌نحوی که برای هر عضو $b \in S$ داریم $a \leq b$.

به کمک اصل خوش‌ترتیبی می‌توان بسیاری از خواص اعداد صحیح و اعمال حساب را ثابت نمود.

- به مثال‌های زیر از این خواص توجه نمایید.

قضیه ۱.۱ (خاصیت ارشمیدسی). فرض کنیم a و b دو عدد طبیعی باشند. در این‌صورت عدد طبیعی n یافت می‌شود به‌نحوی که $na \geq b$

اثبات. فرض کنیم حکم برقرار نباشد. پس برای هر عدد طبیعی n داریم $na < b$. یعنی برای هر عدد طبیعی n عدد $b - na > 0$ و لذا عددی طبیعی است. درنتیجه، مجموعه‌ی

$$S = \{b - na \quad : \quad n \in \mathbb{N}\}$$

یک زیرمجموعه‌ی ناتهی از $\mathbb{N}$ است. بنابر اصل خوش‌ترتیبی S دارای کوچکترین عضو است. فرض کنیم $b - ma$ کوچکترین عضو S باشد که در آن $m \in \mathbb{N}$. حال داریم $m + 1 \in \mathbb{N}$ و لذا $b - (m+1)a \in S$.اما

$$b - (m+1)a = (b - ma) - a < b - ma$$

و این با این فرض که $b - ma$ کوچکترین عضو S است متناقض است. لذا فرض خلف نادرست است. پس حکم برقرار است. □

اصل معروف استقراء ریاضی نیز به‌راحتی از اصل خوش‌ترتیبی نتیجه می‌شود.

قضیه ۲.۱ (اصل استقراء). فرض کنیم T یک زیرمجموعه از اعداد طبیعی باشد به‌نحوی که

(۱) $۱ \in T$، و

(۲) برای هر عدد طبیعی k، اگر $k \in T$ آن‌گاه $k+۱ \in T$.

در این‌صورت $T = \mathbb{N}$.

اثبات. فرض کنیم

$$S = \{n \in \mathbb{N} \ : \ n \notin T\}$$

برای اثبات حکم کافی است نشان دهیم S تهی است. فرض کنیم S تهی نباشد. با به‌کار بردن اصل خوش‌ترتیبی در مورد S و با استفاده از خواص T به تناقض برسید. □

شکل زیر از اصل استقراء بارها برای اثبات گزاره‌نماهای ریاضی به کار برده‌اید:

قضیه ۳.۱ فرض کنیم $p(n)$ یک گزاره‌نما باشد که در آن n عددی طبیعی است. فرض کنیم

(۱) $p(۱)$ یک گزاره‌ی درست است. و

(۲) برای هر عدد طبیعی k، اگر $p(k)$ یک گزاره‌ی درست باشد آن‌گاه گزاره‌ی $p(k+۱)$ درست است.

در این‌صورت برای هر عدد طبیعی n گزاره‌ی $p(n)$ یک گزاره‌ی درست است.

اثبات. بگیرید $T = \{n \in \mathbb{N} \ : \ p(n)$ یک گزاره‌ی درست است $\}$. حال به کمک قضیه‌ی قبل ثابت کنید $T = \mathbb{N}$. این حکم قضیه را نتیجه می‌دهد. □

قضیه ۴.۱ (الگوریتم تقسیم). فرض کنیم a و $b \neq 0$ دو عدد صحیح باشند. در این‌صورت اعداد صحیح منحصربه‌فرد q و r یافت می‌شوند به‌نحوی که

$$a = bq + r \quad , \quad 0 \leq r < |b|$$

اعداد q و r را به ترتیب خارج قسمت و باقیمانده‌ی تقسیم a بر b گوییم.

اثبات. ابتدا فرض کنید $b > 0$. قرار دهید

$$S = \{a - nb \ : \ n \in \mathbb{Z} \ , \ a - nb \geq 0\}$$

نشان دهید S ناتهی است. سپس با به‌کار بردن اصل خوش‌ترتیبی قضیه را ثابت کنید. □

§ ۲.۱ شمردن

فرض کنیم a و $b \neq 0$ دو عدد صحیح باشند. اگر باقیمانده‌ی تقسیم a بر b برابر صفر باشد آن‌گاه داریم $a = bq$. این حالت خاص مبنای تعریف زیر است.

تعریف ۵.۱ فرض کنیم a و b دو عدد صحیح باشند و $b \neq 0$. گوییم عدد b، عدد a را می‌شمارد، هرگاه باقیمانده‌ی تقسیم a بر b برابر صفر باشد.

به عبارت دیگر عدد b، عدد a را می‌شمارد هرگاه عدد صحیح q یافت شود به‌نحوی که $a = bq$. علامت $b|a$ بدین معنی است که b عدد a را می‌شمارد. اگر b عدد a را بشمارد همچنین می‌گوییم b عدد a را **عاد** می‌کند، یا b یک مقسوم علیه a است، یا b یک عامل a است، یا a یک مضرب b است.

از تعریف فوق نتیجه می‌شود که برای هر عدد $a \neq 0$ داریم $a|a$ و $1|a$ و $a|0$. همچنین $a|1$ اگر و تنها اگر $a = \pm 1$. خواص بسیار دیگری را نیز می‌توان بیان کرد. برخی از این خواص در قضیه زیر آمده‌اند و به راحتی از تعریف شمارش نتیجه می‌شوند:

قضیه ۶.۱ فرض کنیم a، b، c و d اعدادی صحیح باشند. در این‌صورت

(۱) اگر $a|b$ و $c|d$ آن‌گاه $ac|bd$.

(۲) اگر $a|b$ و $b|c$ آن‌گاه $a|c$.

(۳) اگر $a|b$ و $b|a$ آن‌گاه $a = \pm b$.

(۴) اگر $a|b$ و $b \neq ۰$ آن‌گاه $|a| \leqslant |b|$.

(۵) اگر $a|b$ و $a|c$ آن‌گاه برای هر دو عدد صحیح m و n، $a|mc + nb$.

تعریف ۷.۱ فرض کنیم a و b اعدادی صحیح باشند. عدد صحیح d را یک **مقسوم‌علیه مشترک** a و b گوییم هرگاه $d|a$ و $d|b$. به‌ویژه بزرگترین مقسوم علیه مشترک a و b عدد صحیح و مثبت d است به نحوی که d یک مقسوم علیه مشترک a و b است و d از هر مقسوم علیه مشترک a و b ناکمتر است. بزرگترین مقسوم علیه مشترک دو عدد a و b را با (a, b)ب.م.م یا(در صورتی‌که با زوج مرتب (a, b) اشتباه گرفته نشود) به طور خلاصه با (a, b) نشان می‌دهیم.

مثال ۸.۱ $(۳, ۵) = ۱$، $(۳۵, -۱۴) = ۷$ و $(۳, ۰) = ۳$

تبصره ۹.۱ اگر $a = b = ۰$ آن‌گاه هر عدد صحیح یک مقسوم علیه مشترک a و b است. لذا بزرگترین مقسوم‌علیه مشترک a و b وجود ندارد. قضیه زیر نشان می‌دهد درصورتی‌که a یا b مخالف صفر باشند آن‌گاه بزرگترین مقسوم‌علیه مشترک a و b وجود دارد، و به‌علاوه یک ترکیب خطی از دو عدد a و b است.

قضیه ۱۰.۱ (بزو). فرض کنیم a و b دو عدد صحیح باشند و a یا b مخالف صفر باشد. در این‌صورت بزرگترین مقسوم‌علیه مشترک a و b وجود دارد و به‌علاوه اگر d این بزرگترین مقسوم‌علیه مشترک باشد، آنگاه اعداد صحیح λ و μ یافت می‌شوند به‌نحوی که $d = \lambda\, a + \mu\, b$

اثبات. قرار دهید

$$S = \{ua + vb \ : \ u, v \in \mathbb{Z},\ ua + vb > ۰\}$$

نشان دهید S ناتهی است و لذا بنابر اصل خوش ترتیبی دارای کوچکترین عضو است. فرض کنید $d = \lambda\, a + \mu\, b$ کوچکترین عضو S باشد. نشان می‌دهیم d بزرگترین مقسوم‌علیه مشترک a و b است.

با تقسیم a بر d بنابر الگوریتم تقسیم داریم

$$a = qd + r \quad ۰ \leq r < d$$

لذا

$$r = a - qd = a - q(\lambda\, a + \mu\, b) = (۱ - q\, \lambda)a + (-q\, \mu)b$$

اگر $r \neq ۰$ آنگاه $r \in S$ و $r < d$ که این با انتخاب d متناقض است. پس $r = ۰$، لذا $a = qd$ یعنی $d|a$. به طریق مشابه ثابت می‌شود $d|b$. پس d یک مقسوم‌علیه مشترک a و b است. اگر $d_۱ > ۰$ یک مقسوم‌علیه مشترک دلخواه a و b باشد آنگاه $d_۱|a$ و $d_۱|b$ و لذا $d_۱|\lambda a + \mu b = d$ و از این نتیجه می‌شود که $d_۱ \leq d$ و اثبات تمام است. □

تبصره ۱۱.۱ توجه کنیم که قضیه‌ی فوق وجود λ و μ را اثبات می‌نماید بدون آنکه روشی برای بدست آوردن آن‌ها ارائه دهد. بعداً الگوریتم اقلیدس را برای بدست آوردن λ و μ ارائه خواهیم نمود.

مثال ۱۲.۱ داریم $(۳۵, -۱۴) = ۷$. با فرض $\lambda = ۱$ و $\mu = ۲$ داریم

$$\lambda\,(۳۵) + \mu\,(-۱۴) = ۳۵ + ۲(-۱۴) = ۷$$

تعریف ۱۳.۱ فرض کنیم a و b دو عدد صحیح باشند. اگر بزرگترین مقسوم علیه مشترک a و b برابر ۱ باشد، a و b را **نسبت به هم اول** می‌گوییم.

اگر a و b نسبت به هم اول باشند، بنابر قضیه‌ی بزو اعداد صحیح λ و μ یافت می‌شوند که $\lambda a+\mu b = ۱$.
در این حالت خاص عکس قضیه‌ی بزو نیز برقرار است:

قضیه ۱۴.۱ فرض کنیم a و b دو عدد صحیح باشند. در این صورت a و b نسبت به هم اولند اگر و تنها اگر اعداد صحیح λ و μ یافت شوند به‌نحوی که $\lambda\, a + \mu\, b = ۱$.

اثبات. اگر a و b نسبت به هم اول باشند آن‌گاه بنابر قضیه‌ی بزو λ و μ یافت می‌شوند که $\lambda a+\mu b = ۱$. برعکس فرض کنیم اعداد صحیح λ و μ یافت شوند به‌نحوی که $\lambda a+\mu b = ۱$.فرض کنیم d بزرگترین مقسوم علیه مشترک a و b باشد. در این صورت $d|a$ و $d|b$ و لذا $d|\lambda\, a + \mu\, b$. یعنی $d|۱$. پس $d = ۱$ یعنی a و b نسبت به هم اولند. □

نتیجه ۱۵.۱ اگر $(a, b) = d$ آن‌گاه $(\frac{a}{d}, \frac{b}{d}) = ۱$.

اثبات. به کمک قضیه‌ی قبل ثابت کنید. □

نتیجه ۱۶.۱ اگر $a|c$ و $b|c$ و $(a, b) = ۱$ آن‌گاه $ab|c$

اثبات. بنابر قضیه‌ی بزو اعداد صحیح λ و μ یافت می‌شوند به‌نحوی که $\lambda\, a + \mu\, b = ۱$. لذا

$$\lambda ac + \mu bc = c$$

چون $a|c$ و $b|c$ لذا اعداد صحیح $q_۱$ و $q_۲$ یافت می‌شوند که $c = q_۱a = q_۲b$. لذا

$$c = \lambda ac + \mu bc = \lambda\, a(q_۲b) + \mu b\, (q_۱a) = (\lambda\, q_۲ + \mu q_۱)\, ab$$

پس $ab|c$ □

تبصره ۱۷.۱ توجه داشته باشید که در نتیجه‌ی بالا شرط $(a,b) = ۱$ لازم است. به عنوان مثال ۱۰|۹۰ و ۶|۹۰. اما ۶۰ ∤ ۹۰

نتیجه ۱۸.۱ (لم اقلیدس). فرض کنیم $a|b\,c$ و $(a,b) = ۱$ در این صورت $a|c$.

اثبات. بنابر قضیه‌ی بزو اعداد صحیح λ و μ یافت می‌شوند به‌نحوی که $\lambda\,a + \mu\,b = ۱$. لذا

$$\lambda\,a\,c + \mu\,b\,c = c$$

اما از $a|b\,c$ نتیجه می‌شود $b\,c = q\,a$ برای یک عدد صحیح q. لذا داریم

$$c = \lambda\,a\,c + \mu\,b\,c = \lambda\,a\,c + \mu\,q\,a = (\lambda\,c + \mu\,q)a$$

و لذا $a|c$. □

§ ۳.۱ الگوریتم اقلیدس

در بخش قبل بزرگترین مقسوم علیه مشترک دو عدد a و b را وقتی a یا b مخالف صفر است تعریف کردیم. همچنین در قضیه‌ی بزو ثابت کردیم اگر بزرگترین مقسوم‌علیه مشترک a و b برابر d باشد آن‌گاه اعداد صحیح λ و μ یافت می‌شوند به‌نحوی که $d = \lambda\,a + \mu\,b$. الگوریتم اقلیدس روشی کارآمد و سریع برای بدست آوردن d و همچنین λ و μ بدست می‌دهد. لم ساده‌ی زیر ایده اصلی بکار گرفته شده در الگوریتم اقلیدس است.

لم ۱۹.۱ فرض کنیم a و b دو عدد صحیح باشند و a یا b مخالف صفر باشد. برای هر عدد صحیح q داریم

$$(a,b) = (a, b + q\,a)$$

اثبات. فرض کنیم $d = (a,b)$ و $d' = (a, b + q\,a)$. داریم $d|a$ و $d|b$ پس $d|b + q\,a$. حال چون $d|a$ و $d|b + q\,a$ پس $d \le d'$. به طریق مشابه داریم $d'|a$ و $d'|b + q\,a$. لذا $d'|(b + q\,a) - q\,a = b$. لذا چون $d'|a$ و $d'|b$. پس $d' \le d$. پس $d = d'$. □

نتیجه ۲۰.۱ فرض کنیم $a = b\,q + r$. در این صورت

$$(a, b) = (b, r)$$

اثبات. بنابر لم قبل داریم

$$(b, r) = (b, r + q\,b) = (b, a) = (a, b)$$

□

قضیه ۲۱.۱ (الگوریتم اقلیدس). فرض کنیم a و b دو عدد صحیح مثبت باشند و a یا b مخالف صفر باشد. تقسیمات متوالی زیر را در نظر بگیرید:

$$\begin{array}{lll}
(۱) & a = q_۱\,b + r_۱ & ۰ \le r_۱ < b \\
(۲) & b = q_۲\,r_۱ + r_۲ & ۰ \le r_۲ < r_۱ \\
(۳) & r_۱ = q_۳\,r_۲ + r_۳ & ۰ \le r_۳ < r_۲ \\
 & \vdots & \vdots \\
(n) & r_{n-۲} = q_n\,r_{n-۱} + r_n & ۰ \le r_n < r_{n-۱} \\
(n+۱) & r_{n-۱} = q_{n+۱}\,r_n + r_{n+۱} & ۰ \le r_{n+۱} < r_n
\end{array}$$

در این صورت $n \in \mathbb{N}$ یافت می‌شود که $r_{n+۱} = ۰$. در این حالت

$$(a, b) = r_n$$

اثبات. داریم $r_۱ > r_۲ > r_۳ > \ldots$ و r_i ها اعداد نامنفی هستند. بنابراین nی یافت می‌شود که $r_{n+۱} = ۰$. حال با کاربرد مکرر نتیجه‌ی قبل داریم

$$(a, b) = (b, r_۱) = (r_۱, r_۲) = (r_۲, r_۳) = \ldots = (r_{n-۱}, r_n)$$

حال چون $r_{n+۱} = ۰$ لذا $r_{n-۱} = q_{n+۱}\,r_n$ یعنی $r_n | r_{n-۱}$. یعنی $(r_{n-۱}, r_n) = r_n$. پس

$$(a, b) = r_n$$

□

تبصره ۲۲.۱ الگوریتم فوق علاوه بر محاسبه‌ی بزرگترین مقسوم‌علیه مشترک a و b اعداد صحیح λ و μ را که بنابر قضیه‌ی بزو وجود دارند بدست می‌دهد. یعنی اگر $d = (a, b)$ آن‌گاه λ و μ را چنان می‌دهد که $d = \lambda\,a + \mu\,b$. کافی است قرار دهیم

$$d = r_n = r_{n-۲} - q_n\,r_{n-۱}$$

با بدست آوردن r_{n-1} از معادله‌ی $(n-1)$ داریم $r_{n-1} = r_{n-3} - q_{n-1}\, r_{n-2}$ و لذا

$$d = r_{n-2} - q_n(r_{n-3} - q_{n-1}\, r_{n-2}) = (1 + q_n\, q_{n-1})\, r_{n-2} + (-q_n)\, r_{n-3}$$

در گام بعد مقدار r_{n-2} را از معادله‌ی $(n-2)$ محاسبه و در معادله‌ی اخیر قرار می‌دهیم. با ادامه‌ی این روند بدست می‌آید

$$d = \lambda\, a + \mu\, b$$

اجازه دهید الگوریتم فوق را در مثالی تجربه کنیم:

مثال ۲۳.۱ اعداد $a = ۲۵۲$ و $b = ۱۹۸$ را در نظر بگیرید. داریم

$$\begin{aligned}
(۱) \quad & ۲۵۲ = ۱ \times ۱۹۸ + ۵۴ \\
(۲) \quad & ۱۹۸ = ۳ \times ۵۴ + ۳۶ \\
(۳) \quad & ۵۴ = ۱ \times ۳۶ + ۱۸ \\
(۴) \quad & ۳۶ = ۲ \times ۱۸ + ۰
\end{aligned}$$

در این‌جا $r_۴ = ۰$ و لذا $d = (۲۵۲, ۱۹۸) = r_۳ = ۱۸$. همچنین داریم

$$\begin{aligned}
d = ۱۸ &= ۵۴ - ۱ \times ۳۶ && = ۵۴ - ۱ \times (۱۹۸ - ۳ \times ۵۴) \\
&= ۴ \times ۵۴ - ۱۹۸ && = ۴(۲۵۲ - ۱ \times ۱۹۸) - ۱۹۸ \\
&= ۴ \times ۲۵۲ - ۵ \times ۱۹۸
\end{aligned}$$

لذا با فرض $\lambda = ۴$ و $\mu = -۵$ داریم

$$d = ۱۸ = \lambda(۲۵۲) + \mu(۱۹۸)$$

تبصره ۲۴.۱ الگوریتم اقلیدس علی‌رغم سادگی یکی از الگوریتم‌های بسیار مهم و کارآ در نظریه‌ی اعداد است. بدین معنی که تعداد محاسبات مورد نیاز برای بدست آوردن بزرگترین مقسوم‌علیه دو عدد a و b نسبت به اعداد a و b بسیار کم است. در واقع می‌توان نشان داد که تعداد تقسیمات متوالی مورد نیاز در الگوریتم اقلیدس حداکثر ۵ برابر تعداد ارقام عدد کوچکتر است. به عنوان مثال اگر a و b اعداد حدوداً ۲۰۰ رقمی باشند حداکثر با ۱۰۰۰ تقسیم متوالی می‌توان بزرگترین مقسوم‌علیه مشترک a و b را پیدا کرد. این کار با یک برنامه‌ی ساده‌ی کامپیوتری در چند ثانیه قابل انجام است. حتماً به یاد دارید که در دبیرستان گاهی برای بدست آوردن بزرگترین مقسوم‌علیه مشترک دو عدد ابتدا آن دو عدد را به عوامل اول تجزیه می‌کردیم و سپس بزرگترین مقسوم‌علیه مشترک را از روی تجزیه‌ی

اعداد می‌نوشتیم. ذکر این نکته در این‌جا ضروری است که تجزیه‌ی اعداد با حدود ۲۰۰ رقم در حالت کلی با سریعترین کامپیوترها، امروزه میلیاردها سال طول می‌کشد و لذا روش بدست آوردن بزرگترین مقسوم‌علیه مشترک با استفاده از تجزیه روشی کاملاً ناکارآمد و غیرعملی است.

§ ۴.۱ معادله‌ی دیوفانتی خطی

در این بخش به عنوان کاربردی از مفهوم بزرگترین مقسوم‌علیه مشترک و الگوریتم تقسیم، روشی سریع برای حل معادله‌ی دیوفانتی خطی

$$ax + by = c \qquad (۱.۱)$$

ارائه می‌دهیم. در حالت کلی یک معادله به شکل $f(x_۱, x_۲, \ldots, x_n) = ۰$ که در آن f یک چندجمله‌ای با n متغیر و ضرایب صحیح است، را یک **معادله‌ی دیوفانتی** گوییم. و منظور از حل چنین معادله‌ای به‌دست آوردن کلیه‌ی جواب‌های صحیح آن است. نام دیوفانتی برای چنین معادلاتی، منسوب و به افتخار ریاضی‌دان یونانی، دیوفانتوس ($Diophantus$، ۲۵۰ قبل از میلاد) می‌باشد. متون قدیمی ریاضی پر است از مسائل دیوفانتی که به دلیل عدم وجود علامات امروز در زبان ریاضی، بیشتر به زبان نوشتاری و بدون استفاده از علامات بیان شده‌اند. مثال زیر را احتمالاً شنیده‌اید.

مثال ۲۵.۱ باتوجه به این که

«ما و ما و نصف ما و نصفه ای از نصف ما گر تو هم با ما شوی ما جملگی صد می‌شویم»

تعداد ما چند تا است؟ با علامات ریاضی اگر جمعیت ما x باشد، آن‌گاه

$$x + x + \frac{۱}{۲}x + \frac{۱}{۲}(\frac{۱}{۲}x) + ۱ = ۱۰۰$$

و لذا $x = ۳۶$.

مثال زیر طول عمر دیوفانتوس را محاسبه می‌کند:

مثال ۲۶.۱ دیوفانتوس یک ششم از عمر خود را در کودکی صرف کرد. پس از گذشت یک دوازدهم دیگر ریش درآورد. پس از گذشت یک هفتم دیگر ازدواج کرد. و پس از پنج سال صاحب یک پسر

شد. طول عمر پسر نصف طول عمر پدر بود. پدر چهار سال بعد از پسر درگذشت.

به معادله‌ی (۱) بر می‌گردیم. که در آن a، b و c اعدادی صحیح هستند. می‌خواهیم کلیه‌ی جواب‌های صحیح (۱) را بیابیم. فرض کنیم بزرگترین مقسوم‌علیه مشترک a و b برابر $(a,b)=d$ باشد. فرض کنیم $(x_\circ,y_\circ)$ یک جواب معادله باشد. در این‌صورت

$$ax_\circ+by_\circ=c$$

از $d|a$ و $d|b$ نتیجه می‌شود که $d|ax_\circ+by_\circ=c$. لذا شرط $d|c$ یک شرط لازم برای وجود جواب صحیح برای معادله‌ی (۱) است . این شرط کافی نیز هست. زیرا فرض کنیم $c=dc'$. بنابه قضیه‌ی بزو اعداد صحیح λ و μ یافت می‌شود که $\lambda a+\mu b=d$ و لذا

$$(c'\lambda)a+(c'\mu)b=c'd=c$$

یعنی $(c'\lambda,c'\mu)$ یک جواب معادله‌ی (۱) است .

حال فرض کنیم $d|c$ و فرض کنیم $(x_\circ,y_\circ)$ یک جواب معادله‌ی (۱) باشد. فرض کنیم (x',y') یک جواب دلخواه (۱) باشد. در این‌صورت

$$ax_\circ+by_\circ=ax'+by'=c$$

و لذا $a(x'-x_\circ)=-b(y'-y_\circ)$. پس

$$\frac{a}{d}(x'-x_\circ)=-\frac{b}{d}(y'-y_\circ) \qquad (۲.۱)$$

(توجه کنیم که $\frac{a}{d}$ و $\frac{b}{d}$ دو عدد صحیح‌اند). حال از $\frac{b}{d}|\frac{a}{d}(x'-x_\circ)$ و این‌که $(\frac{a}{d},\frac{b}{d})=۱$ نتیجه می‌شود که $\frac{b}{d}|x'-x_\circ$. لذا $x'-x_\circ=k\frac{b}{d}$ برای یک $k\in\mathbb{Z}$. پس

$$x'=x_\circ+k\frac{b}{d}$$

حال از (۲) نتیجه می‌شود که $\frac{a}{d}(k\frac{b}{d})=-\frac{b}{d}(y'-y_\circ)$. پس

$$y'=y_\circ-k\frac{a}{b}$$

لذا $(x',y')=(x_k,y_k)$ که در آن

$$\begin{cases} x_k=x_\circ+k\dfrac{b}{d} \\ y_k=y_\circ-k\dfrac{a}{d} \end{cases}$$

برعکس، به‌راحتی دیده می‌شود که برای هر k زوج (x_k, y_k) در معادله‌ی (۱) صدق می‌کند.

بنابراین قضیه‌ی زیر را ثابت کردیم:

قضیه ۲۷.۱ فرض کنیم a، b و c اعدادی صحیح باشند و بزرگترین مقسوم‌علیه مشترک a و b برابر $(a,b)=d$ باشد. در این‌صورت معادله‌ی $ax+by=c$ دارای جواب صحیح است اگر وتنها اگر $d|c$.

به‌علاوه اگر $d|c$ و $(x_\circ, y_\circ)$ یک جواب معادله باشد آن‌گاه کلیه‌ی جواب‌های معادله عبارتند از

$$\begin{cases} x_k = x_\circ + k\dfrac{b}{d} \\ y_k = y_\circ - k\dfrac{a}{d} \end{cases}$$

که در آن k عددی صحیح است.

مثال ۲۸.۱ مطلوب است کلیه‌ی جواب‌های صحیح و مثبت معادله‌ی $۱۱x + ۲۴y = ۴۰۰$.

حل: با توجه به این که بزرگترین مقسوم‌علیه اعداد ۲۴ و ۱۱ برابر ۱ است، با استفاده از الگوریتم اقلیدس و تبصره‌ی بعد از آن اعداد $\lambda = ۱۱$ و $\mu = -۵$ به دست می‌آیند. یعنی $(۱۱)۱۱ + (-۵)۲۴ = ۱$ و لذا

$$(۴۴۰۰)۱۱ + (-۲۰۰۰)۲۴ = ۴۰۰$$

و لذا $(x_\circ, y_\circ) = (۴۴۰۰, -۲۰۰۰)$ یک جواب معادله است. و کلیه‌ی جواب‌های معادله عبارتند از

$$\begin{cases} x_k = ۴۴۰۰ + ۲۴k \\ y_k = -۲۰۰۰ - ۱۱k \end{cases} \qquad k \in \mathbb{Z}$$

حال شرط مثبت بودن x_k و y_k نتیجه می‌دهد که $k = -۱۸۲, -۱۸۳$ و با قراردادن k دو جواب $(۳۲, ۲)$ و $(۸, ۱۳)$ به‌دست می‌آیند.

§ ۵.۱ تمرین

۱. نشان دهید

(الف) مربع هر عدد به شکل $۳k$ یا $۳k+۱$ می‌باشد.

(ب) مکعب هر عدد به یکی از شکل های $۹k$، $۹k+۱$ و $۹k+۸$ می‌باشد.

(ج) مربع هر عدد فرد به شکل $۴k+۱$ می‌باشد.

۲. ده مقدار برای a بیابید به نحوی‌که عدد $۳a^۲+۱$ مربع کامل باشد.

۳. نشان دهید $\frac{n(n+۱)(۲n+۱)}{۶}$ همواره عددی صحیح است.

۴. مکعب هر عدد به شکل $۷k$ و $۷k\pm۱$ می‌باشد.

۵. نشان دهید هیچ یک از اعداد $۱۱, ۱۱۱, ۱۱۱۱, ۱۱۱۱۱, \ldots$ مربع کامل نیست.

۶. نشان دهید برای هر $n\geq ۱$.

(الف) $۸|۵^{۲n}+۷$.

(ب) $۱۵|۲^{۴n}-۱$.

(ج) $۲۴|۲\times ۷^n+۳\times ۵^n-۵$.

۷. نشان دهید برای عدد صحیح a،

(الف) اعداد $۲a+۱$ و $۹a+۴$ نسبت به هم اولند.

(ب) اعداد $۵a+۲$ و $۷a+۳$ نسبت به هم اولند.

۸. نشان دهید اگر $d|n$، آنگاه $۲^d-۱|۲^n-۱$.

۹. نشان دهید اگر a و b نسبت به هم اول و همچنین a و c نسبت به هم اول باشند، آنگاه a و bc نسبت به هم اولند.

۱۰. دهید اگر $a^n|b^n$، آنگاه $a|b$. (راهنمایی: ابتدا نشان دهید اگر a و b نسبت به هم اول باشند، آنگاه a^n و b^n نسبت به هم اولند.)

۱۱. کلیه‌ی جواب‌های صحیح مثبت معادلات زیر را بیابید:

(الف) $۱۸x + ۵y = ۴۸$.

(ب) $۵۴x + ۲۱y = ۹۰۶$.

(ج) $۱۲۳x + ۳۶۰y = ۹۹$.

(د) $۱۵۸x - ۵۷y = ۷$.

۱۲. فرض کنیم a و b دو عدد صحیح مثبت و نسبت به هم اول باشند. نشان دهید معادله‌ی $ax - by = c$ دارای بی‌نهایت جواب صحیح است.

۱۳. کلیه‌ی جواب‌های صحیح $۱۵x + ۱۲y + ۳۰z = ۲۴$ را بیابید.

۱۴. برای پذیرایی از ۱۰۰ نفر، ۱۰۰ تومان پول داریم. اگر خیار هر عدد ۱ ریال، سیب هر عدد ۱۰ ریال و پرتقال هر عدد ۳۰ ریال باشد. به چند طریق می‌توان دقیقاً ۱۰۰ میوه با بهای کل ۱۰۰ تومان خرید؟ چگونه؟

۱۵. کسر $\frac{a}{b}(b \neq ۰)$ را ساده گوییم هرگاه $(a, b) = ۱$. نشان دهید اگر مجموع دو کسر ساده‌ی $\frac{a}{b}$ و $\frac{c}{d}$ یک عدد صحیح باشد آنگاه $b = d$.

۱۶. فرض کنیم x و y دو عدد صحیح‌اند و $m = ax + by$ و $n = cx + dy$ و $ad - bc = ۱$. نشان دهید $(m, n) = (x, y)$.

۱۷. (الف) فرض کنیم $(a,b)=۱$ و $(\frac{a}{b})^m=n$. نشان دهید $b=۱$.

(ب) اگر n توان mام یک عدد طبیعی نباشد، ثابت کنید $n^{\frac{۱}{m}}$ عددی اصم است.

۱۸. اگر $(a,b)=۱$ و $x^a=y^b$ آنگاه $x=n^b$ و $y=n^a$ برای یک عدد طبیعی n.

فصل ۲
اعداد اول

مفهوم عدد اول، اساسی‌ترین و مهم‌ترین بحث در نظریه‌ی اعداد می‌باشد.

§۱.۲ تجزیه به عوامل اول

تعریف ۱.۲ (الف) عدد صحیح $p > ۱$ را **اول** گوییم، هرگاه برای هر دو عدد صحیح b و c اگر $p|bc$، آن‌گاه $p|b$ یا $p|c$.

(ب) عدد صحیح $p > ۱$ را **تحویل‌ناپذیر** گوییم، هرگاه تنها مقسوم‌علیه‌های مثبت p اعداد p و ۱ باشند.

(ج) عدد صحیح $p > ۱$ را **مرکب** گوییم، هرگاه اول نباشد.

تبصره ۲.۲ احتمالاً شما قبلاً با اعداد اول آشنا شده‌اید و تعریفی که برای عدد اول داشته‌اید همان است که در قسمت (ب) در تعریف فوق برای عدد تحویل‌ناپذیری ارائه نمودیم. گزاره‌ی زیر نشان می‌دهد که برای یک عدد صحیح مفهوم اول‌بودن و تحویل‌ناپذیر بودن معادل‌اند. علت ارائه دو تعریف آن است که در برخی دستگاه‌های دیگر از اعداد این دو مفهوم معادل نیستند. به عنوان مثال اگر دستگاه اعداد شما مجموعه‌ی

$$\mathbb{Z}[\sqrt{-۵}] = \{m + n\sqrt{-۵} : m, n \in \mathbb{Z}\}$$

باشد، آن‌گاه عدد $\alpha = ۱ + \sqrt{-۵}$ تحویل‌ناپذیر است. در عین حال

$$(۱ + \sqrt{-۵})(۱ + \sqrt{-۵}) = ۶ = ۲ \times ۳،$$

یعنی $\alpha | ۲ \times ۳$ ولی $\alpha \nmid ۲$ و $\alpha \nmid ۳$. لذا α عددی اول در دستگاه $\mathbb{Z}[\sqrt{-۵}]$ نیست.

گزاره ۳.۲ عدد صحیح $p > ۱$ اول است اگر و تنها اگر تحویل‌ناپذیر باشد.

اثبات. فرض کنیم p عددی تحویل‌ناپذیر باشد. فرض کنیم b و c دو عدد صحیح باشند و $p|bc$. فرض کنیم d بزرگترین مقسوم‌علیه مشترک p و b باشد. چون $d|p$ پس $d = p$ یا $d = ۱$. اگر $d = p$، آن‌گاه $p|b$. و اگر $d = ۱$، آن‌گاه p و b نسبت به هم اول‌اند و لذا بنابر لم اقلیدس داریم $p|c$. و لذا p اول است.

برعکس، فرض کنیم p عددی اول باشد. فرض کنیم d یک مقسوم‌علیه مثبت p باشد. لذا $p = dc$ برای یک عدد صحیح c. پس $p|dc$. چون p اول است لذا $p|d$ یا $p|c$. اگر $p|d$، آن‌گاه $d = pc'$ برای یک عدد صحیح c' . لذا $p = pcc'$. لذا $cc' = ۱$. پس $c = ۱$. به طریق مشابه اگر $p|c$ آن‌گاه $d = ۱$. پس p تحویل‌ناپذیر است. □

گزاره ۴.۲ فرض کنیم p عددی اول باشد.

(الف) اگر $a_۱, a_۲, \ldots, a_n$ اعدادی صحیح باشند و $p|a_۱a_۲\cdots a_n$، آن‌گاه $p|a_i$ برای یک $۱ \le i \le n$.

(ب) اگر $p_۱, p_۲, \ldots, p_n$ اعدادی اول باشند و $p|p_۱p_۲\cdots p_n$، آن‌گاه $p = p_i$ برای یک $۱ \le i \le n$.

اثبات. (الف) با استقراء روی n و (ب) با استفاده از (الف) به‌راحتی ثابت می‌شود. □

قضیه ۵.۲ (قضیه‌ی اساسی حساب). هر عدد صحیح $n > ۱$ را می‌توان به‌صورت حاصل‌ضرب اعداد اول نوشت. این نمایش صرف‌نظر از ترتیب عوامل منحصربه‌فرد است.

اثبات. فرض کنیم

$$A = \{n \in \mathbb{N} : n > ۱ \text{ } n \text{ را نمی‌توان به‌صورت حاصل‌ضرب اعداد اول نوشت}\}$$

اگر A تهی نباشد آن‌گاه بنابر اصل خوش ترتیبی دارای کوچک‌ترین عضوی چون d است. چون $d \in A$ لذا d اول نیست. پس $d = d_۱d_۲$ که در آن $۱ < d_۱ < d$ و $۱ < d_۲ < d$. با عنایت به انتخاب d نتیجه می‌شود که $d_۱ \notin A$ و $d_۲ \notin A$. پس $d_۱$ و $d_۲$ را می‌توان به‌صورت حاصل‌ضرب اعداد اول نوشت:

$$d = p_۱p_۲ \cdots p_k \quad \text{و} \quad d = q_۱q_۲ \cdots q_l$$

که در آن p_i ها و q_i ها اول‌اند. حال $d = d_۱d_۲ = p_۱p_۲ \cdots p_k \; q_۱q_۲ \cdots q_l$ و لذا $d \notin A$ و این متناقض با انتخاب d است. از این نتیجه می‌شود که A تهی است. پس قسمت اول قضیه ثابت می‌شود. برای اثبات منحصربه‌فردی نمایش فرض کنیم $n = p_۱p_۲ \cdots p_k = q_۱q_۲ \cdots q_l$. دو نمایش n به‌صورت حاصل ضرب اعداد اول باشند. فرض کنیم $k \leq l$. و با تغییر ترتیب عوامل می‌توانیم فرض کنیم $p_۱ \leq p_۲ \leq \cdots \leq p_k$ و $q_۱ \leq q_۲ \leq \cdots \leq q_l$. با توجه به گزاره‌ی قبل از این‌که $p_۱ | q_۱q_۲ \cdots q_l$ نتیجه می‌شود $p_۱ = q_s \geq q_۱$ برای یک $۱ \leq s \leq l$. به طریق مشابه از $q_۱ | p_۱p_۲ \cdots p_k$ نتیجه می‌شود $q_۱ = p_t \geq p_۱$ برای یک $۱ \leq t \leq k$. لذا $p_۱ = q_۱$. با حذف $p_۱$ داریم $p_۲p_۳ \cdots p_k = q_۲q_۳ \cdots q_l$. با تکرار روند فوق خواهیم داشت $p_۲ = q_۲, p_۳ = q_۳, \ldots, p_k = q_k$. چنانچه $l > k$ آن‌گاه داریم $q_{k+۱}q_{k+۲} \cdots q_l = ۱$. که این غیرممکن است، چون q_iها اعدادی بزرگتر از یک هستند. پس $k = l$ و اثبات تمام است. □

تعریف ۶.۲ اگر $n > ۱$ یک عدد صحیح باشد، آن گاه $n = p_۱^{\alpha_۱} p_۲^{\alpha_۲} \dots p_k^{\alpha_k}$ که در آن $p_۱ < p_۲ < \dots < p_k$ اعدادی اول‌اند و برای هر $۱ \le i \le k$، $\alpha_i \ge ۱$. این نمایش را **نمایش استانده‌ی** n به‌صورت حاصل ضرب عوامل اول گوییم.

تبصره ۷.۲ اگر چه قضیه‌ی اساسی حساب که با استدلالی نسبتاً ساده ثابت شد، وجود تجزیه‌ی منحصربه‌فرد هر عدد صحیح $n > ۱$ را تضمین می‌کند ولی روش اثبات به هیچ وجه راه‌کاری عملی و کارآمد برای تجزیه‌ی عدد صحیح $n > ۱$ ارائه نمی‌دهد. برای تجزیه عدد صحیح $n > ۱$ تنها با استفاده از تعریف، کافی است عدد n را بر کلیه اعداد طبیعی کوچکتر از n تقسیم کنیم. تجزیه یک عدد با حدود دویست رقم با این روش، با سریع‌ترین کامپیوترهای امروز میلیاردها سال زمان می‌برد. همچنین است تشخیص این که عدد داده شده‌ی $p > ۱$ عددی اول یا مرکب است. به همین دلیل تجزیه اعداد صحیح امروزه یکی از دشوارترین مسائل ریاضی محسوب می‌شود. این موجب گردیده است مسائل حل نشده‌ی فراوانی در خصوص اعداد اول و نحوه‌ی توزیع آن‌هادر بین مجموعه‌ی اعداد وجود داشته باشد.

با وجود این، نتایج فراوان و زیبایی تاکنون در این زمینه ثابت شده است و حدس‌های فراوانی دراین رابطه وجود دارند که تاکنون ثابت نشده است. برای نمونه به چند مورد اشاره می‌نماییم:

§ ۲.۲ فراوانی اعداد اول و فاصله بین آن‌ها

قضیه ۸.۲ (قضیه‌ی اقلیدس). بی‌نهایت عدد اول وجود دارد.

اثبات. فرض کنیم تعداد اعداد اول متناهی باشد. و فرض کنیم $p_۱, p_۲, \dots, p_n$ همه‌ی اعداد اول

باشند. در این‌صورت عدد $k = p_۱p_۲\cdots p_n + ۱$ را درنظر می‌گیریم. بنابر قضیه‌ی اساسی حساب k را می‌توان به‌صورت حاصل‌ضرب اعداد اول نوشت. به‌ویژه k بر تعدادی از اعداد اول بخش‌پذیر است. امّا k بر هیچ‌یک از اعداد اول $p_۱, p_۲, \ldots, p_n$ بخش‌پذیر نیست. (درواقع باقی‌مانده‌ی k بر هر یک از اعداد اول $p_۱, p_۲, \ldots, p_n$ برابر ۱ است.) و این یک تناقض است. و لذا حکم برقرار است. □

قضیه ۹.۲ فرض کنیم $n > ۱$ یک عدد صحیح باشد. اگر $n > ۱$ مرکب باشد، آن‌گاه عدد اول $q \leq \sqrt{n}$ یافت می‌شود به‌نحوی که $q|n$.

اثبات. فرض کنیم n مرکب باشد. لذا $n = n_۱n_۲$ که در آن $۱ < n_۱ < n$ و $۱ < n_۲ < n$. از این نتیجه می‌شود که $n_۱ \leq \sqrt{n}$ یا $n_۲ \leq \sqrt{n}$. فرض کنیم $n_۱ \leq \sqrt{n}$. چون $n_۱ > ۱$ لذا $n_۱$ بر یک عدد اول مانند q بخش‌پذیر است. لذا داریم $q \leq n_۱ \leq \sqrt{n}$ و $q|n$. □

مثال ۱۰.۲ عدد ۵۲۱ بر هیچ‌یک از اعداد اول $۲, ۳, ۵, ۷, ۱۱, ۱۳, ۱۷, ۱۹$ قابل قسمت نیست. پس اول است.

غربال اراتستن: به کمک قضیه‌ی فوق، ریاضی‌دان یونانی اراتستن (۲۷۶ تا ۱۹۴ قبل از میلاد) روشی برای به‌دست آوردن کلیه‌ی اعداد اول کمتر از عدد n ارائه داد. شیوه‌ی کار شبیه غربال کردن است و به همین دلیل به این روش غربال اراتستن گوییم. روش‌های غربالی متفاوتی بعداً کشف شده‌اند که از حوصله‌ی بحث ما خارج است. در روش اراتستن ابتدا اعداد صحیح از ۲ تا n را می‌نویسیم. اولین عدد (یعنی ۲) اول است. کلیه‌ی مضارب ۲ به جز ۲ را حذف می‌کنیم. اولین عدد باقی‌مانده بعد از ۲ (یعنی ۳) اول است. چون بر عدد اول کوچکتر از خودش بخش‌پذیر نیست. حال مضارب ۳ به جز ۳ را حذف می‌کنیم. اولین عدد باقی‌مانده بعد از ۳ (یعنی ۵) اول است. مضارب ۵ به جز ۵ را حذف می‌کنیم. اولین عدد باقی‌مانده بعد از ۵ (یعنی ۷) اول است. این کار را ادامه می‌دهیم تا جایی‌که اولین

عدد باقی‌مانده بعد از آخرین عدد اول یافته‌شده از $\sqrt{n}$ بزرگتر باشد. پس از آن کلیه‌ی اعداد باقی‌مانده اول هستند.

مثال ۱۱.۲ فرض کنیم کلیه اعداد اول کوچکتر یا مساوی ۵۰ را می‌خواهیم،

	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹	۲۰
۲۱	۲۲	۲۳	۲۴	۲۵	۲۶	۲۷	۲۸	۲۹	۳۰
۳۱	۳۲	۳۳	۳۴	۳۵	۳۶	۳۷	۳۸	۳۹	۴۰
۴۱	۴۲	۴۳	۴۴	۴۵	۴۶	۴۷	۴۸	۴۹	۵۰

لذا اعداد اول کوچکتر یا مساوی ۵۰ عبارتند از

$$۲, ۳, ۵, ۷, ۱۱, ۱۳, ۱۷, ۱۹, ۲۳, ۲۹, ۳۱, ۳۷, ۴۱, ۴۳, ۴۷$$

اگرچه قضیه‌ی اقلیدس وجود بی‌نهایت عدد اول را تضمین می‌کند ولی نحوه‌ی توزیع اعداد اول در بین مجموعه‌ی اعداد طبیعی بسیار اسرارآمیز به‌نظر می‌رسد. دو عدد اول را دو عدد اول **متوالی** گوییم هرگاه بین آن دو، هیچ عدد اولی وجود نداشته باشد. به عنوان مثال اعداد ۲۳ و ۲۹ دو عدد اول متوالی هستند. تنها عدد اول زوج عدد ۲ است. چون از هر دو عدد طبیعی متوالی یکی زوج است لذا به جز ۲ و ۳ هیچ دو عدد طبیعی متوالی دو عدد اول متوالی نیستند. لذا فاصله‌ی دو عدد اول متوالی (به جز ۲ و ۳) حداقل ۲ است. اگر p و $p+۲$ دو عدد اول باشند آن‌گاه زوج $(p, p+۲)$ را یک زوج از اعداد اول **دوقلو** نامیم. به عنوان مثال $(۳, ۵)$، $(۵, ۷)$ و $(۱۱, ۱۳)$ زوج‌هایی از اعداد اول دوقلو هستند. با یک نگاه به جدول اعداد اول مشاهده می‌شود در عین حالی که گاهی فاصله‌ی دو عدد اول متوالی بسیار زیاد است، اعداد اول دوقلوی بسیار بزرگ نیز یافت می‌شوند. بنابراین دو سؤال طبیعی به‌نظر می‌رسند. نخست این که آیا اعداد اول دوقلوی به دلخواه بزرگ یافت می‌شوند؟ دوم این‌که آیا فاصله‌ی دو عدد اول متوالی می‌تواند به دلخواه بزرگ باشد؟ پاسخ به هر دو سؤال به نظر متضاد، مثبت است. البته پاسخ مثبت به سؤال اول یک حدس اثبات نشده است و پاسخ مثبت به سؤال دوم آسان است.

حدس: بی‌نهایت زوج از اعداد اول دوقلو وجود دارد.

اگرچه هنوز کسی نتوانسته است اثباتی ریاضی برای حدس فوق ارائه نماید، نتایج جست‌وجوهای زیاد

به‌ویژه توسط محاسبات حجیم کامپیوتری بر درستی حدس دلالت دارد. به عنوان نمونه زوج

$$۱,۰۰۰,۰۰۰,۰۰۰,۰۶۳ \quad و \quad ۱,۰۰۰,۰۰۰,۰۰۰,۰۶۱$$

یک زوج از اعداد اول دوقلوست. آخرین زوج‌های اعداد اول دوقلو که تاکنون یافت شده‌اند دو زوج

$$۲,۰۰۳,۶۶۳,۶۱۳ \times ۲^{۱۹۵۰۰۰} \pm ۱$$

و

$$۶۵,۵۱۶,۴۶۸,۳۵۵ \times ۲^{۳۳۳۳۳۳} \pm ۱$$

می‌باشند که به‌ترتیب در سال‌های ۲۰۰۷ و ۲۰۰۹ میلادی یافت شده‌اند.

قضیه‌ی زیر پاسخ مثبت به سؤال دوم است:

قضیه ۱۲.۲ به ازای هر عدد طبیعی n، دو عدد اول متوالی p و q یافت می‌شود به‌نحوی که $q-p > n$.

اثبات. فرض کنیم p بزرگ‌ترین عدد اول کوچکتر از $(n+۱)! + ۲$ و q کوچک‌ترین عدد اول بزرگتر از $(n+۱)! + n + ۱$ باشند. اعداد متوالی

$$(n+۱)! + ۲, (n+۱)! + ۳, \ldots, (n+۱)! + n + ۱$$

هیچ‌یک اول نیستند (چرا؟) لذا اعداد p و q دو عدد اول متوالی هستند و $q - p > n$. □

توجه نمایید که برای عدد طبیعی n، اعداد متوالی ارائه شده در اثبات قضیه‌ی فوق به هیچ وجه کوچک‌ترین n عدد متوالی غیراول نیستند، به عنوان مثال ۵ عدد متوالی غیراول ارائه شده در اثبات قضیه‌ی اعداد۷۲۲، ۷۲۳، ۷۲۴، ۷۲۵ و ۷۲۶ می‌باشند و کوچک‌ترین ۵ عدد متوالی غیراول ۲۴، ۲۵، ۲۶، ۲۷ و ۲۸ می‌باشند.

اجازه دهید نامتناهی بودن تعداد اول را از زاویه‌ی دیگر نگاه کنیم. می‌دانیم تعداد اعداد طبیعی نامتناهی است. به‌علاوه سری

$$\sum_{n\in\mathbb{N}} \frac{۱}{n} = ۱ + \frac{۱}{۲} + \frac{۱}{۳} + \cdots \qquad (۱.۲)$$

واگراست. اگر در سری (۱) به‌جای همه‌ی جملات فقط جملات با n زوج انتخاب کنیم، سری

$$\sum_{\substack{n\in\mathbb{N}\\ n\text{زوج}}} \frac{۱}{n} = \sum_{n=۱}^{\infty} \frac{۱}{۲n} = \frac{۱}{۲} + \frac{۱}{۴} + \frac{۱}{۶} + \cdots$$

به‌دست می‌آید که هنوز واگراست. همچنین اگر از هر پنج جمله یک جمله را انتخاب کنیم سری

$$\sum_{n=۱}^{\infty} \frac{۱}{۵n} = \frac{۱}{۵} + \frac{۱}{۱۰} + \frac{۱}{۱۵} + \cdots$$

به‌دست می‌آید که باز هم واگراست. ولی اگر جملاتی را که در آن n مربع کامل یا n به شکل ۲^k است انتخاب کنیم، به‌ترتیب سری‌های

$$\sum_{n=۱}^{\infty} \frac{۱}{n^۲} = ۱ + \frac{۱}{۴} + \frac{۱}{۹} + \frac{۱}{۱۶} + \cdots$$

و

$$\sum_{k=۱}^{\infty} \frac{۱}{۲^k} = \frac{۱}{۲} + \frac{۱}{۴} + \frac{۱}{۸} + + \frac{۱}{۱۶} \cdots$$

به‌دست می‌آیند که همگرا هستند. این مثال‌ها به تعبیری می‌گوید تعداد اعداد طبیعی، یا تعداد اعداد زوج، یا تعداد مضارب ۵ از تعداد مربعات کامل و از تعداد توان‌های ۲ بیشتر است (اگرچه هر دو تعداد بی‌نهایت هستند) حال این سؤال طبیعی است که اگر جملاتی را که در آن n اول است، انتخاب کنیم چه اتفاقی می‌افتد؟ آیا سری حاصل همگراست یا واگرا؟ قضیه‌ی زیر را داریم:

قضیه ۱۳.۲ سری

$$\sum_{p\text{اول}} \frac{۱}{p} = \frac{۱}{۲} + \frac{۱}{۳} + \frac{۱}{۵} + \frac{۱}{۷} + \cdots$$

یک سری واگراست.

اثبات. اثبات این قضیه که نتیجه‌ی مستقیمی از خواص اعداد اول و تعریف همگرایی سری هاست، به دانشجویان واگذار می‌گردد. به عنوان راهنمایی یادآوری می‌شود که اگر سری فوق همگرا باشد آنگاه عدد اول $p_۰$ یافت می‌شود به‌نحوی که

$$\sum_{\substack{p\text{اول}\\ p>p_۰}} \frac{۱}{p} < \frac{۱}{۲}$$

□

در پایان این بخش قضیه‌ی اعداد اول را بدون اثبات بیان می‌کنیم که به روشی دیگر می‌گوید که تعداد اعداد اول نامتناهی است و این نامتناهی بودن از چه نوعی است.

قضیه ۱۴.۲ (قضیه‌ی اعداد اول) فرض کنیم برای هر عدد حقیقی و مثبت x، تعداد اعداد اول نابیشتر از x را با $\pi(x)$ نشان می‌دهیم. در این‌صورت

$$\lim_{x\to\infty} \frac{\pi(x)}{\left(\frac{x}{\log x}\right)} = ۱.$$

این بدان معنی است که $\pi(x)$ همانند $\frac{x}{\log x}$ به سمت بی‌نهایت میل می‌کند. قضیه‌ی فوق به‌طور جداگانه توسط گاوس و لژاندر پیشنهاد گردید. حدود یک‌صد سال طول کشید تا در ادامه‌ی تلاش دانشمندان بزرگی چون چبیشف $(Chebyshev)$ و ریمان $(Riemann)$ نهایتاً در سال ۱۸۹۶ میلادی به‌طور جداگانه توسط هادامارد $(J.Hadamard)$ و پوسین $(de\,la\,vallee\,Poussin)$ اثبات گردید.

§ ۳.۲ قضیه‌ی دیریکله و اعداد اول در تصاعد حسابی

یکی از نتایج بسیار جالب در خصوص اعداد اول قضیه‌ی دیریکله $(Dirichlet)$ در خصوص وجود بی‌نهایت عدد اول در هر تصاعد حسابی است. (با این شرط که جمله‌ی اول تصاعد و تفاضل جملات متوالی تصاعد نسبت به هم اول باشند.)

فرض کنیم d یک عدد طبیعی باشد. اگر $p > d$ یک عدد اول باشد آن‌گاه بنابر الگوریتم تقسیم

$$p = kd + r$$

که در آن $۰ < r < d$ و $(r, d) = ۱$ ب.م.م. قضیه‌ی دیریکله نتیجه می‌دهد که اگر r چنان باشد که $(r, d) = ۱$ آن‌گاه در تصاعد حسابی

$$r, r + d, r + ۲d, r + ۳d, \ldots, r + kd, \ldots$$

بی‌نهایت عدد اول یافت می‌شود.

اجازه دهید حالت $d = ۴$ را امتحان کنیم: هر عدد اول به یکی از شکل‌های $۴k + ۱$ یا $۴k + ۳$ می‌باشد. بنابر قضیه‌ی دیریکله بی‌نهایت عدد اول به شکل $۴k + ۱$ و بی‌نهایت عدد اول به شکل $۴k + ۳$ یافت می‌شود. اجازه دهید بدون استفاده از قضیه‌ی دیریکله مستقیماً ثابت کنیم بی‌نهایت عدد اول به شکل $۴k + ۳$ یافت می‌شود.

قضیه ۱۵.۲ بی‌نهایت عدد اول به شکل $۴k + ۳$ یافت می‌شود.

اثبات. روش اثبات شبیه اثبات قضیه‌ی اقلیدس است. فرض کنیم تعداد اعداد اول به شکل $۴k + ۳$ متناهی باشد. و فرض کنیم این اعداد اول $p_t, \ldots, p_۲, p_۱$ باشند. قرار می‌دهیم

$$N = ۴p_۱p_۲ \cdots p_t - ۱$$

بنابر قضیه‌ی حساب N حاصل ضرب تعدادی عدد اول است. روشن است که هیچ‌یک از اعداد از اول $p_t, \ldots, p_۲, p_۱$ عدد N را نمی‌شمارند. پس $N = q_۱q_۲ \cdots q_t$ که در آن q_iها اول و همگی به شکل $۴k + ۱$ می‌باشند. برای هر $۱ \leq i \leq r$. قرار می‌دهیم $q_i = ۴k_i + ۱$. در این‌صورت

$$N = (۴k_۱ + ۱)(۴k_۲ + ۱) \cdots (۴k_r + ۱) = ۴s + ۱$$

برای یک عدد طبیعی s. لذا $۴p_۱p_۲ \cdots p_t - ۱ = ۴s + ۱$. یعنی $۴(p_۱p_۲ \cdots p_t - s) = ۲$ که غیرممکن است. □

در فصل‌های بعد اثبات وجود بی‌نهایت عدد اول به شکل‌هایی چون $۴k + ۱$، $۸k - ۱$ و $۵k - ۱$ را خواهیم دید.

اثبات قضیه‌ی دیریکله نیاز به ابزاری قوی‌تر دارد که در درس‌های پیشرفته در نظریه‌ی اعداد قابل ارائه است. در این‌جا صورت قضیه را بدون اثبات ثابت می‌نماییم:

قضیه ۱۶.۲ (قضیه‌ی دیریکله در خصوص اعداد اول در یک تصاعد حسابی) فرض کنیم d و r دو عدد طبیعی نسبت به هم اول باشند. در این‌صورت تصاعد حسابی

$$r, r+d, r+۲d, r+۳d, \ldots, r+kd, \ldots$$

حاوی بی‌نهایت عدد اول است.

§ ۴.۲ تمرین

۱. (الف) اگر $p = a^n - ۱$ اول باشد. ثابت کنید $a = ۲$ و n عددی اول است.

(ب)نشان دهید عکس (الف) برقرار نیست.

تعریف: یک عدد به‌شکل $M_n = ۲^n - ۱$ رایک عدد مرسن و در صورتی که اول باشد آن را یک عدد اول مرسن گوییم.

۲. (الف) نشان دهید اگر $F_n = ۲^n + ۱$ اول باشد آن‌گاه $n = ۲^k$ برای یک عدد طبیعی k.

(ب) نشان دهید عکس (الف) برقرار نیست.

تعریف: یک عدد به‌شکل $F_k = ۲^{۲^k} + ۱$ را یک عدد فرما گوییم.

۳. نشان دهید برای $n > ۱$ عدد $n^۴ + ۴$ عددی مرکب است.

۴. نشان دهید هر عدد $n \geq ۲$ جمع دو عدد مرکب است.

۵. نشان دهید هر عدد طبیعی $n \geq ۲$ عدد $\sum_{k=۱}^{n} \frac{۱}{k}$ عددی صحیح نیست.

۶. نشان دهید بی‌نهایت عدد اول به شکل $n^۲ - ۲$ وجود دارد.

۷. نشان دهید هر عدد اول به شکل $۳n + ۱$ به شکل $۶m + ۱$ نیز هست.

۸. نشان دهید هر عدد به شکل $۳n + ۲$ مقسوم‌علیه اولی به شکل $۳m + ۲$ دارد.

۹. نشان دهید

(الف) تنها عدد اول به شکل $n^۳ - ۱$ عدد ۷ است.

(ب) تنها عدد اول p به‌نحوی که $۳p + ۱$ مربع کامل است عدد $p = ۵$ است.

(ج) تنها عدد اول به شکل $n^۲ - ۴$ عدد ۵ است.

۱۰. گزاره‌ی زیر را اثبات یا رد کنید:

«هر عدد فرد مجموع یک عدد اول و توانی از ۲ است.»

۱۱. نشان دهید اگر $f(x) = x^۲ - x + ۴۱$ آنگاه برای هر $۰ \leq n \leq ۴۰$ عدد $f(n)$ اول است. و نشان دهید $f(۴۱)$ اول نیست.

۱۲. اگر $f(x)$ یک چندجمله‌ای با ضرایب صحیح باشد. ثابت کنید عدد صحیح n یافت می‌شود به‌نحوی که $f(n)$ اول نیست. به‌عبارت دیگر هیچ چندجمله‌ای وجود ندارد که فقط عدد اول تولید کند.

۱۳. نشان دهید اگر p عددی اول باشد آنگاه $\binom{p}{k}$ برای $۱ \leq k < p$ بر p بخش‌پذیر است.

۱۴. فرض کنیم $n > ۱$ عددی طبیعی و فرض کنیم $p_۱, p_۲, \ldots, p_t$ اعداد اول نابیشتر از n باشند. ثابت کنید

$$p_۱p_۲ \ldots p_t < ۴^n$$

۱۵. فرض کنیم $n > ۳$ و p عددی اول و $\frac{۲n}{۳} < p \leq n$. نشان دهید p عدد $\binom{۲n}{n}$ را نمی‌شمارد.

۱۶. به کمک دو تمرین قبل ثابت کنید برای هر عدد طبیعی n عدد اول p یافت می‌شود به‌نحوی که $n < p < ۲n$.

۱۷. به کمک تمرین قبل ثابت کنید اگر p_n عدد اول n-ام باشد آنگاه $p_n \leq ۲^n$.

۱۸. ثابت کنید هر عدد طبیعی مجموع تعدادی عدد اول متمایز است.

۱۹. نشان دهید اگر $R_k = \frac{۱۰^k - ۱}{۹}$ اول باشد آنگاه k اول است. و با یک مثال نشان دهید عکس این مطلب بر قرار نیست.

فصل ۳
توابع حسابی

یک تابع که قلمرو آن اعداد طبیعی است را یک **تابع حسابی** گوییم. توابع حسابی گوناگونی در بخش‌های مختلف از نظریه اعداد وجود دارد. در این فصل به بررسی برخی توابع خاص عمومی توابع حسابی و معرفی چند تابع حسابی خاص می‌پردازیم.

§۱.۳ خواص توابع حسابی و ضرب دیریکله

تعریف ۱.۳ تابع حسابی f را **کاملاً ضربی** گوییم هرگاه برای هر دو عدد طبیعی m و n داشته باشیم $f(mn) = f(m)f(n)$. اگر برای هر دو عدد طبیعی با شرط $(m,n) = ۱$ داشته باشیم $f(mn) = f(m)f(n)$ آن‌گاه f را یک **تابع ضربی** گوییم.

تبصره ۲.۳ اگر f یک تابع حسابی باشد، آن‌گاه منظور از نماد

$$\sum_{d|n} f(d)$$

مجموع $f(d)$ ها است که در آن d در بین مقسوم‌علیه‌های مثبت n تغییر می‌کند.

به‌عنوان مثال

$$\sum_{d|۱۲} f(d) = f(۱) + f(۲) + f(۳) + f(۴) + f(۶) + f(۱۲)$$

تعریف ۳.۳ (ضرب دیریکله) فرض کنیم f و g دو تابع حسابی باشند. ضرب دیریکله‌ی f در g که با $f * g$ نمایش داده می‌شود، به‌صورت زیر تعریف می‌شود:

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

سه تابع حسابی تعریف شده‌ی زیر نقش مهمی در مطالعه‌ی توابع حسابی دارند.

تعریف ۴.۳ توابع حسابی کاملاً ضربی I، u و N^α (α عددی حقیقی) به‌صورت زیر تعریف می‌شود:

(الف) برای هر عدد طبیعی n، $I(n) = \left[\frac{۱}{n}\right] = \begin{cases} ۱ & n = ۱ \\ ۰ & n > ۱ \end{cases}$.

(ب) برای هر عدد طبیعی n، $u(n) = ۱$.

(ج) برای هر عدد طبیعی n، $N^\alpha(n) = n^\alpha$.

تعریف ۵.۳ فرض کنیم f یک تابع حسابی باشد. تابع حسابی g را **وارون دیریکله‌ی** f گوییم هرگاه

$$f * g = I$$

در این‌صورت g را با $f^{-۱}$ نمایش می‌دهیم.

قضیه ۶.۳ (الف) برای هرتابع حسابی f داریم، $f * I = I * f = f$.

(ب) ضرب دیریکله جابجایی است. یعنی برای هر دو تابع حسابی f و g داریم، $f * g = g * f$.

(ج) ضرب دیریکله شرکت پذیر است. یعنی برای هر سه تابع حسابی f و g و h داریم،

$$(f * g) * h = f * (g * h).$$

(د) اگر f یک تابع حسابی باشد به‌نحوی که $f(۱) \neq ۰$، آن‌گاه f دارای یک وارون دیریکله‌ی منحصربه‌فرد است. در واقع $f^{-۱}$ به‌طور منحصربه‌فرد به‌صورت زیر تعریف می‌شود:

$$f^{-۱}(۱) = \frac{۱}{f(۱)} \ , \ f^{-۱}(n) = \frac{-۱}{f(۱)} \sum_{\substack{d|n \\ d<n}} f(\frac{n}{d}) f^{-۱}(d) \ , \ \forall n > ۱$$

تبصره ۷.۳ اگر f و g دو تابع حسابی باشند به‌نحوی که $f(۱) \neq ۰$ و $g(۱) \neq ۰$ آن‌گاه

$$(f * g)(۱) = f(۱)\, g(۱) \neq ۰$$

لذا مجموعه‌ی توابع حسابی f با شرط $f(۱) \neq ۰$ تحت عمل ضرب دیریکله بسته است. لذا قضیه قبل می‌گوید این مجموعه با عمل ضرب دیریکله یک گروه آبلی است.

اثبات قضیه:

(الف) از تعریف به آسانی نتیجه می‌شود.

(ب) داریم،

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

وقتی d مقسوم‌علیه‌های n را می‌پیماید. $\frac{n}{d}$ نیز مقسوم‌علیه‌های n را می‌پیماید. لذا

$$(f * g)(n) = \sum_{d|n} f(\frac{n}{d}) g\left(\frac{n}{n/d}\right) = \sum_{d|n} g(d) f\left(\frac{n}{d}\right) = (g * f)(n)$$

(ج) با استفاده از تعریف به‌راحتی دیده می‌شود که

$$((f * g) * h)(n) = (f * (g * h))(n) = \sum_{a.b.c=n} f(a) f(b) f(c)$$

(د) فرض کنیم f^{-1} تابعی باشد که در صورت قضیه تعریف شده است. بنابه تعریف ضرب دیریکله داریم

$$(f * f^{-1})(1) = f(1)f^{-1}(1) = f(1)\frac{1}{f(1)} = 1$$

و برای هر $n > 1$

$$\begin{aligned}(f * f^{-1})(n) &= \sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) \\ &= f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) \\ &= f(1)\left[\frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d)\right] + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) = 0\end{aligned}$$

لذا $f * f^{-1} = I$. بنابراین f^{-1} وارون دیریکله‌ی f است. اگر تابع g چنان باشد که $f * g = I$، آن‌گاه داریم

$$f^{-1} = f^{-1} * I = f^{-1} * (f * g) = (f^{-1} * f) * g = I * g = g$$

لذا وارون دیریکله‌ی f منحصربه‌فرد است و اثبات تمام است.

اجازه دهید وارون تابع حسابی u را به‌دست آوریم. با استفاده از فرمول داده شده در قضیه داریم $u^{-1}(1) = 1$. برای هر عدد اول p داریم، $u^{-1}(p) = -u(p)u^{-1}(1) = -1$

$$u^{-1}(p^2) = -(u(p^2)u^{-1}(1) + u(p)u^{-1}(p)) = -(u^{-1}(1) + u^{-1}(p)) = 0$$

با روشی مشابه $u^{-1}(p^\alpha)) = 0$ برای هر $\alpha \geq 2$ و اگر p_1, p_2, p_3 سه عدد اول متمایز باشند، آن‌گاه $u^{-1}(p_1p_2) = 1$ و $u^{-1}(p_1p_2p_3) = -1$.

این مشاهدات ما را به تعریف زیر رهنمون می‌سازد.

تعریف ۸.۳ تابع موبیوس به‌صورت زیر تعریف می‌شود:

$$\mu(n) = \begin{cases} 1 & \text{اگر } n = 1 \\ 0 & \text{اگر } n \text{، بر مربع یک عدد اول بخش‌پذیر باشد} \\ (-1)^k & \text{اگر } n \text{، حاصل‌ضرب } k \text{ عدد اول متمایز باشد} \end{cases}$$

قضیه ۹.۳ μ وارون دیریکله‌ی تابع u است. یعنی $\mu * u = I$. به عبارت دیگر برای هر عدد طبیعی n،

$$(\mu * u)(n) = \sum_{d|n} \mu(d) = I(n) = \begin{cases} ۱ & n = ۱ \\ ۰ & n > ۱ \end{cases}$$

اثبات. رابطه به ازای $n = ۱$ به‌وضوح برقرار است. فرض کنیم $n > ۱$. فرض کنیم $n = p_۱^{\alpha_۱} p_۲^{\alpha_۲} \dots p_k^{\alpha_k}$ تجزیه‌ی استانده‌ی n به عوامل اول باشد. جملات غیرصفر در مجموع $\sum_{d|n} \mu(d)$ مربوط به $d = ۱$ و مقسوم‌علیه‌هایی از n هستند که حاصل‌ضرب اعداد اول متمایز است. لذا

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(۱) + \sum_{i \in \{۱,۲,\dots,k\}} \mu(p_i) + \sum_{\{i_۱,i_۲\} \subset \{۱,۲,\dots,k\}} \mu(p_{i_۱} p_{i_۲}) \\ &\quad + \sum_{\{i_۱,i_۲,i_۳\} \subseteq \{۱,۲,\dots,k\}} \mu(p_{i_۱} p_{i_۲} p_{i_۳}) + \dots + \mu(p_۱ p_۲ \dots p_k) \\ &= ۱ + \binom{k}{۱}(-۱)^۱ + \binom{k}{۲}(-۱)^۲ + \binom{k}{۳}(-۱)^۳ + \dots + \binom{k}{k}(-۱)^k \\ &= (۱ - ۱)^k = ۰ \end{aligned}$$

□

تمرین. نشان دهید μ تابعی ضربی است و سپس با استفاده از آن اثبات ساده‌تری از قضیه‌ی فوق ارائه دهید.

قضیه ۱۰.۳ (فرمول عکس موبیوس) فرض کنیم f و g دو تابع حسابی باشند. در این‌صورت

$$f(n) = \sum_{d|n} g(d)$$

اگر و تنها اگر $g(n) = \sum \mu(\frac{n}{d}) f(d)$.

اثبات. بنابه فرض $f = g * u$. لذا

$$f * \mu = (g * u) * \mu = g * (u * \mu) = g * I = g$$

و این یعنی $g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$.

برعکس، فرض کنیم تساوی دوم قضیه برقرار باشد. یعنی $g = f * \mu$. دراین‌صورت

$$g * u = (f * \mu) * u = f * (\mu * u) = f * I = f$$

که این همان تساوی اول در صورت قضیه است. □

تمرین. اثبات مستقیمی (بدون استفاده از ضرب دیریکله) برای قضیه بالا ارائه نمایید.

مثال ۱۱.۳ اگر $f(n) = \sum_{d|n} g(d)$ آن‌گاه

$$\begin{aligned} g(۶۰) &= \mu(۶۰)f(۱) + \mu(۳۰)f(۲) + \mu(۲۰)f(۳) + \mu(۱۵)f(۴) + \mu(۱۲)f(۵) + \mu(۱۰)f(۶) \\ &+ \mu(۶)f(۱۰) + \mu(۵)f(۱۲) + \mu(۴)f(۱۵) + \mu(۳)f(۲۰) + \mu(۲)f(۳۰) + \mu(۱)f(۶۰) \\ &= -f(۲) + f(۴) + f(۶) + f(۱۰) - f(۱۲) - f(۲۰) - f(۳۰) + f(۶۰) \end{aligned}$$

قضیه ۱۲.۳ اگر f و g دوتابع حسابی ضربی باشند آن‌گاه $f * g$ نیز ضربی است.

اثبات. اگر m و n دو عدد طبیعی باشند به‌قسمی‌که $(m, n) = ۱$ آن‌گاه مقسوم‌علیه‌های mn به‌صورت $c = d_۱ d_۲$ هستند به‌نحوی که $d_۱ | m$ و $d_۲ | n$. لذا

$$\begin{aligned} (f * g)(mn) &= \sum_{c|mn} f(c) g\left(\frac{mn}{c}\right) = \sum_{\substack{d_۱|m \\ d_۲|n}} f(d_۱ d_۲) g\left(\frac{mn}{d_۱ d_۲}\right) \\ &= \sum_{\substack{d_۱|m \\ d_۲|n}} f(d_۱) f(d_۲) g\left(\frac{m}{d_۱}\right) g\left(\frac{n}{d_۲}\right) \\ &= \left(\sum_{d_۱|m} f(d_۱) g(\frac{m}{d_۱})\right)\left(\sum_{d_۲|n} f(d_۲) g(\frac{n}{d_۲})\right) \\ &= (f * g)(m)(f * g)(n) \end{aligned}$$

و اثبات تمام است. □

نتیجه ۱۳.۳ اگر f و g دوتابع حسابی باشند و $f(n)=\sum_{d|n} g(d)$ آنگاه f ضربی است اگر و تنها اگر g ضربی باشد.

اثبات. داریم $f=g*u$. فرض کنیم g ضربی باشد. چون u ضربی است لذا از قضیه‌ی قبل نتیجه می‌شود کهf ضربی است. برعکس فرض کنیم f ضربی باشد. در این‌صورت از فرمول عکس موبیوس نتیجه می‌شود که $g=f*\mu$. چون μ ضربی است از قضیه‌ی قبل نتیجه می‌شود که g ضربی است. □

§ ۲.۳ برخی توابع حسابی خاص

در بخش قبل توابع حسابی I، u، N^α و μ را معرفی کردیم. در این بخش چند تابع حسابی دیگر را معرفی می‌کنیم. ابتدا به معرفی تابع حسابی شناخته شده‌ی اویلر (ϕ) و ارائه‌ی برخی خواص آن می‌پردازیم.

تعریف ۱۴.۳ برای عدد طبیعی n، تعداد اعداد طبیعی نابیشتر از n که نسبت به n اولند را با $\varphi(n)$ نشان می‌دهیم. تابع $\varphi(n)$ را **تابع اویلر** می‌گوییم.

به عنوان مثال $\varphi(۱)=\varphi(۲)=۱$، $\varphi(۳)=\varphi(۴)=۲$. برای عدد طبیعی n داریم $\varphi(n)=n-۱$ اگر و تنها اگر n عددی اول باشد. قضیه بعدی، $\varphi(n)$ را در حالت کلی محاسبه می‌نماید. لم ساده زیر در اثبات قضیه مورد نیاز است.

لم ۱۵.۳ فرض کنیم n عددی طبیعی و d یک مقسوم‌علیه n باشد. قرار می‌دهیم

$$A_d=\{k: ۱\le k\le n \ \text{ و } \ d|k\}$$

در این‌صورت $|A_d|=\left[\frac{n}{d}\right]$.

اثبات. روشن است که $d, ۲d, ۳d, \dots, \frac{n}{d}d \in A_d$. از طرف دیگر، اگر $k\in A_d$ آنگاه $k=sd$ برای یک عدد طبیعی s. داریم $sd=k\le n$ و لذا $s\le \frac{n}{d}$. پس

$$A_d = \left\{ sd \ : \ ۱ \leq s \leq \frac{n}{d} \right\}$$

و اثبات تمام است. □

قضیه ۱۶.۳ برای هر عدد طبیعی $n > ۱$ داریم

$$\varphi(n) = n \prod_{p|n} \left(۱ - \frac{۱}{p} \right)$$

اثبات. فرض کنیم P مجموعه اعداد اولی باشد که n را می‌شمارند و فرض کنیم

$$B = \{k \ : ۱ \leq k \leq n \ \text{ و } \ (k,n) \neq ۱\}$$

اگر $l \in B$ آنگاه $p \in P$ یافت می‌شود که $p|l$. لذا $l \in A_p$. لذا $l \in A_p$ که در آن A_p همان است که در لم بالا تعریف شده است. لذا

$$B = \bigcup_{p \in P} A_p$$

بنابراین

$$\begin{aligned} |B| &= \left| \bigcup_{p \in P} A_p \right| \\ &= \sum_{p \in P} |A_p| - \sum_{p_۱, p_۲ \in P} |A_{p_۱} \cap A_{p_۲}| + \cdots + (-۱)^{\alpha+۱} \sum_{p_۱, p_۲, \ldots, p_\alpha \in P} |A_{p_۱} \cap A_{p_۲} \cap \cdots \cap A_{p_\alpha}| \\ &\quad + \cdots \end{aligned}$$

اگر $p_۱, p_۲, \ldots, p_\alpha \in P$ آنگاه $p_۱, p_۲, \ldots, p_\alpha$ همگی k را می‌شمارند اگر و تنها اگر $p_۱ p_۲ \cdots p_\alpha$ عدد k را بشمارد. لذا

$$A_{p_۱} \cap A_{p_۲} \cap \cdots \cap A_{p_\alpha} = A_{p_۱ p_۲ \cdots p_\alpha}$$

حال از لم بالا نتیجه می‌شود که

$$|B| = \sum_{p \in P} \frac{n}{p} - \sum_{p_۱, p_۲ \in P} \frac{n}{p_۱ p_۲} + \cdots + (-۱)^{\alpha+۱} \sum_{p_۱, p_۲, \ldots, p_\alpha \in P} \frac{n}{p_۱ p_۲ \cdots p_\alpha} + \cdots$$

لذا

$$\begin{aligned}\varphi(n) &= n - |B| \\ &= n\left(1 - \sum_{p\in P}\frac{1}{p} + \sum_{p_1,p_2\in P}\frac{1}{p_1,p_2} + \cdots + (-1)^{\alpha}\sum_{p_1,p_2,\ldots,p_\alpha\in P}\frac{1}{p_1,p_2,\ldots,p_\alpha} + \cdots\right) \\ &= n\prod_{p|n}\left(1-\frac{1}{p}\right)\end{aligned}$$

□

نتیجه ۱۷.۳ تابع φ یک تابع ضربی است.

اثبات. فرض کنید m و n دو عدد طبیعی و نسبت به هم اول باشند. در این‌صورت بنابر قضیه بالا

$$\varphi(mn) = mn\prod_{p|mn}\left(1-\frac{1}{p}\right) = \left(m\prod_{p|m}\left(1-\frac{1}{p}\right)\right)\left(n\prod_{p|n}\left(1-\frac{1}{p}\right)\right) = \varphi(m)\varphi(n)$$

ضربی بودن φ را می‌توان از قضیه‌ی زیبای گاوس که در زیر ارائه می‌گردد، نیز نتیجه گرفت: □

قضیه ۱۸.۳ (قضیه گاوس) برای هر عدد طبیعی n،

$$\sum_{d|n}\varphi(d) = n$$

اثبات. برای هر مقسوم‌علیه مثبت d از n تعریف می‌کنیم:

$$s_d = \{m : \quad (m,n) = d\ ,\ 1 \le m \le n\}$$

به‌سادگی دیده می‌شود که s_d ها مجزا هستند و

$$\bigcup_{d|n} s_d = \{1,2,\ldots,n\}$$

لذا

$$\sum_{d|n}|s_d| = n \qquad (۱.۳)$$

حال $|s_d|$ را محاسبه می‌کنیم. داریم $(m,n)=d$ اگر و تنها اگر $(\frac{m}{d},\frac{n}{d})=۱$. لذا تعداد اعداد m با شرط $۱\le m\le n$ و $(m,n)=d$ برابراست با تعداد اعداد m' با شرط $۱\le m'\le \frac{n}{d}$ و $\left(m',\frac{n}{d}\right)=۱$. این تعداد برابر است با $\varphi\left(\frac{n}{d}\right)$. پس از رابطه(۱) داریم

$$\sum_{d|n}\varphi\left(\frac{n}{d}\right)=n$$

امّا وقتی d مقسوم علیه‌های مثبت n را اختیار می‌کند $\frac{n}{d}$ نیز چنین می‌کند. پس

$$n=\sum_{d|n}\varphi\left(\frac{n}{d}\right)=\sum_{d|n}\varphi(d)$$

□

اجازه دهید آن‌چه را در اثبات قضیه گفتیم در حالت $n=۱۸$ مشاهده کنیم:

در این‌جا d یکی از اعداد $۱,۲,۳,۶,۹,۱۸$ می‌باشد.

$$s_۱=\{۱,۵,۷,۱۱,۱۳,۱۷\},\quad s_۲=\{۲,۴,۸,۱۰,۱۴,۱۶\},\quad s_۳=\{۳,۱۵\},$$

$$s_۶=\{۶,۱۲\},\qquad s_۹=\{۹\},\qquad s_{۱۸}=\{۱۸\},$$

$$|s_۱|=۶=\varphi\left(\frac{۱۸}{۱}\right)\quad |s_۲|=۶=\varphi\left(\frac{۱۸}{۲}\right)\quad |s_۳|=۲=\varphi\left(\frac{۱۸}{۳}\right)$$

$$|s_۶|=۲=\varphi\left(\frac{۱۸}{۶}\right)\quad |s_۹|=۱=\varphi\left(\frac{۱۸}{۹}\right)\quad |s_{۱۸}|=۱=\varphi\left(\frac{۱۸}{۱۸}\right)$$

$$\begin{aligned}\sum_{d|۱۸}\varphi(d)&=\varphi(۱)+\varphi(۲)+\varphi(۳)+\varphi(۶)+\varphi(۹)+\varphi(۱۸)\\&=|s_{۱۸}|+|s_۹|+|s_۶|+|s_۳|+|s_۲|+|s_۱|\\&=۱+۱+۲+۲+۶+۶=۱۸\end{aligned}$$

با استفاده از قضیه‌ی گاوس می‌توان اثبات کوتاه‌تری برای ضربی بودن φ ارائه نمود.(تمرین)

تعریف ۱۹.۳ برای هر عدد حقیقی α **تابع حسابی** σ_α به‌صورت $\sigma_\alpha = u * N^\alpha$ تعریف می‌شود. یعنی برای هر عدد طبیعی n،

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha$$

معمولاً σ_0 را با τ و σ_1 را با σ نمایش می‌دهیم. لذا

$$\tau(n) = \sum_{d|n} 1$$

و

$$\sigma(n) = \sum_{d|n} d$$

پس $\tau(n)$ تعداد مقسوم‌علیه‌های مثبت n و $\sigma(n)$ مجموع مقسوم‌علیه‌های مثبت n است.

مثال ۲۰.۳ $\tau(1) = 1$، $\tau(2) = 2$، $\tau(3) = 2$، $\tau(4) = 3$، $\tau(5) = 2$ و $\tau(6) = 4$. در حالت کلی برای هر عدد اول p داریم $\tau(p) = 2$.

همچنین $\sigma(1) = 1$، $\sigma(2) = 3$، $\sigma(3) = 4$، $\sigma(4) = 7$، $\sigma(5) = 6$ و $\sigma(6) = 12$. در حالت کلی برای هر عدد اول p داریم $\sigma(p) = p + 1$.

لم ۲۱.۳ برای هر عدد α، تابع σ_α ضربی است. به‌ویژه توابع σ و τ ضربی هستند.

اثبات. چون $\sigma_\alpha = u * N^\alpha$ و U و N^α هر دو ضربی هستند لذا σ_α ضربی است. □

قضیه ۲۲.۳ اگر $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ تجزیه‌ی استانده‌ی n به عوامل اول باشد، آن‌گاه

(الف) $$\tau(n) = \prod_{i=1}^{r} (\alpha_i + 1) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$$

(ب) $$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}$$

اثبات. توجه می‌کنیم که مقسوم‌علیه‌های n عبارتند از اعداد به شکل

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$$

که در آن برای هر $1 \le i \le r$ داریم $0 \le \beta_i \le \alpha_i$.

(الف) با توجه به توضیح بالا برای هر $1 \le i \le r$ تعداد انتخاب‌های ممکن برای β_i برابر $\alpha_i + 1$ است. بنابراین تعداد کل انتخاب‌ها برای d برابر است با

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$$

(ب) داریم

$$(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}) \dots (1 + p_r + p_r^2 + \cdots + p_r^{\alpha_r})$$
$$= \sum_{\substack{0 \le \beta_1 \le \alpha_1 \\ \vdots \\ 0 \le \beta_r \le \alpha_r}} p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r} = \sum_{d|n} d$$

حال (ب) از تساوی‌های

$$1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1} = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}, \dots, 1 + p_r + p_r^2 + \cdots + p_r^{\alpha_r} = \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}$$

نتیجه می‌شود. □

تبصره ۲۳.۳ با استفاده از ضربی بودن σ و τ می‌توان اثبات کوتاه‌تری برای قضیه فوق ارائه نمود.

در واقع اگر p عددی اول باشد آن‌گاه مقسوم‌علیه‌های p^k عبارتند از $1, p, p^2, \ldots, p^k$ و لذا

$$\tau(p^k) = k + 1$$

$$\sigma(p^k) = 1 + p + p^2 + \cdots + p^k$$

حال با استفاده از ضربی بودن σ و τ نتیجه حاصل می‌شود.

تبصره ۲۴.۳ در این‌جا به یک نکته در خصوص مقسوم‌علیه‌های n اشاره می‌کنیم که در بسیاری از موارد در حل مسائل و ساده کردن عبارات به کار می‌آید. اگر d یک مقسوم‌علیه n باشد آن‌گاه $\frac{n}{d}$ نیز یک مقسوم‌علیه n است. زیرا $d \times \frac{n}{d} = n$. به‌علاوه اگر $d_1, d_2, \ldots, d_{\tau(n)}$ کلیه‌ی مقسوم‌علیه‌های مثبت متمایز n باشند آن‌گاه اعداد $\frac{n}{d_1}, \frac{n}{d_2}, \ldots, \frac{n}{d_{\tau(n)}}$ نیز کلیه‌ی مقسوم‌علیه‌های مثبت متمایز n می‌باشند. یعنی

$$\Big\{d : d \in \mathbb{N}, d|n\} = \{\frac{n}{d} : d \in \mathbb{N}, d|n\Big\}$$

به مثال زیر توجه نمایید.

مثال ۲۵.۳ حاصل‌ضرب مقسوم‌علیه‌های مثبت عدد n به‌دست آوریم.

فرض کنیم حاصل‌ضرب مقسوم‌علیه‌های n برابر عدد A باشد. در این‌صورت $A = \prod_{d|n} d$. با توجه به تبصره‌ی فوق می‌توان نوشت $A = \prod_{d|n} \frac{n}{d}$. حال می‌توان نوشت

$$A^2 = A \times A = \Big(\prod_{d|n} d\Big)\Big(\prod_{d|n} \frac{n}{d}\Big) = \prod_{d|n} n = n^{\tau(n)}.$$

لذا $A = \prod_{d|n} d = n^{\frac{\tau(n)}{2}}$.

§ ۳.۳ تابع جزء صحیح

آخرین تابعی را که معرفی و بررسی می‌کنیم با توجه به تعریف، نمی‌توان یک تابع حسابی نامید. امّا نظر به اهمیت آن در مباحث مربوط به توابع حسابی آن را معرفی و بررسی می‌نماییم.

برای هر عدد حقیقی x، بزرگترین عدد صحیح نابیشتر از x را جزء صحیح x می‌گوییم و با $[x]$ نشان می‌دهیم. در واقع $[x]$ عدد صحیح منحصر به فردی است که:

$$x - ۱ < [x] \leq x$$

در این‌جا به ذکر خواصی از این تابع می‌پردازیم.

لم ۲۶.۳ فرض کنیم n و k اعدادی طبیعی باشند. دراین صورت تعداد اعداد طبیعی نابیشتر از n که مضرب k هستند برابر است با $\left[\frac{n}{k}\right]$.

اثبات. بنابر الگوریتم تقسیم $n = qk + r$ که در آن $۰ \leq r < k$. لذا $\frac{n}{k} = q + \frac{r}{k}$ و $\frac{r}{k} < ۱$. پس $\left[\frac{n}{k}\right] = q$.

چون $qk \leq n$ و $(q+۱)k = qk + k > qk + r = n$ لذا اعداد طبیعی نابیشتر از n که مضرب k هستند عبارتند از : $k, ۲k, \ldots, qk$ که تعداد آنها برابر $\left[\frac{n}{k}\right] = q$ است. □

فرض کنیم n یک عدد طبیعی و p عددی اول باشد. اگر $p \leq n$ آن‌گاه بدیهی است که $p^{\alpha} | n!$. آیا $p^{۲} | n!$؟ به‌طور کلی بزرگترین عدد صحیح α به نحوی که $p^{\alpha} | n$ چیست ؟

چون $n! = ۱ \times ۲ \times \cdots \times n$، برای بدست آوردن α باید ببینیم از بین اعداد $۱, ۲, \ldots$ و n کدامیک بر p و بر چه توانی از p بخش‌پذیرند و سپس توانها را با هم جمع کنیم. به عنوان مثال اگر $n = ۱۵, p = ۲$ آن‌گاه

$$n! = ۱۵! = ۱ \times ۲ \times ۳ \times ۴ \times ۵ \times ۶ \times ۷ \times ۸ \times ۹ \times ۱۰ \times ۱۱ \times ۱۲ \times ۱۳ \times ۱۴ \times ۱۵$$

از بین اعداد ۱ تا ۱۵، چهار عدد $۲, ۶, ۱۰, ۱۴$ بر ۲ بخش‌پذیرند ولی بر $۴ = ۲^{۲}$ بخش‌پذیر نیستند. لذا در ضرب آنها دقیقاً ۴ بار عدد ۲ در خود ضرب می‌شود. دو عدد $۴, ۱۲$ بر ۴ بخش‌پذیرند ولی بر

۸ بخش‌پذیر نیستند. لذا در ضرب آنها $۲ \times ۲ = ۴$ بار عدد ۲ در خود ضرب می‌شود. نهایتاً عدد ۸ تنها عدد بخش‌پذیر بر ۸ است. این عدد از ضرب ۲ سه بار در خود حاصل می‌شود. لذا در این‌جا $\alpha = ۱ \times ۴ + ۲ \times ۲ + ۳ \times ۱ = ۱۱$.

اجازه دهید به حالت کلی برگردیم.

در بین اعداد از ۱ تا n، $\left[\frac{n}{p}\right]$ عدد مضرب p و $\left[\frac{n}{p^۲}\right]$ عدد مضرب $p^۲$ می‌باشند (لم بالا) لذا تعداد اعدادی که بر p بخش‌پذیرند ولی بر $p^۲$ بخش‌پذیر نیستند برابر $\left[\frac{n}{p}\right] - \left[\frac{n}{p^۲}\right]$ می‌باشند. به‌طور کلی تعداد اعداد نابیشتر از n که بر p^k بخش‌پذیرند ولی بر $p^{k+۱}$ بخش‌پذیر نیستند برابر است با $\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+۱}}\right]$. لذا

$$\begin{aligned}
\alpha &= \sum_{k=۱}^{\infty} k \left(\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+۱}}\right] \right) \\
&= \sum_{k=۱}^{\infty} k \left[\frac{n}{p^k}\right] - \sum_{k=۱}^{\infty} k \left[\frac{n}{p^{k+۱}}\right] \\
&= \sum_{k=۱}^{\infty} k \left[\frac{n}{p^k}\right] - \sum_{k=۲}^{\infty} (k-۱) \left[\frac{n}{p^k}\right] \\
&= \sum_{k=۱}^{\infty} \left[\frac{n}{p^k}\right]
\end{aligned}$$

بنابراین ثابت کردیم:

قضیه ۲۷.۳ فرض کنیم n یک عدد طبیعی و p عددی اوّ ل باشد. اگر α بزرگترین عدد صحیح باشد به‌نحوی که $p^\alpha | n!$ آن‌گاه

$$\alpha = \sum_{k=۱}^{\infty} \left[\frac{n}{p^k}\right]$$

نتیجه ۲۸.۳ (فرمول لژاندر).

$$n! = \prod_{\substack{p \leq n \\ p \text{ اول}}} p^{\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]}$$

نتیجه ۲۹.۳ اگر r و n اعداد طبیعی باشند و $r < n$، آنگاه عدد

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

عددی صحیح است.

اثبات: تمرین.

قضیه زیر به‌ویژه بدلیل نتایجی که در پی آن می‌آوریم جالب است:

قضیه ۳۰.۳ فرض کنیم f و F دو تابع عددی باشند و $F(n) = \sum_{d|n} f(d)$، در این صورت برای هر عدد طبیعی N داریم

$$\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right]$$

اثبات. داریم

$$\sum_{n=1}^{N} F(n) = \sum_{n=1}^{N} \sum_{d|n} f(d)$$

اگر $k \leq N$ ثابت باشند، برای $1 \leq n \leq N$ جملهٔ $f(k)$ در $\sum_{d|n} f(d)$ ظاهر می‌شود اگر و تنها اگر $k|n$. بنابراین تعداد دفعاتی که $f(k)$ ظاهر می‌شود برابر است با تعداد اعداد طبیعی نابیشتر از N که بر k بخش‌پذیرند یعنی $\left[\frac{N}{k}\right]$. این حکم را ثابت می‌کند. □

نتیجه ۳۱.۳

الف) $$\sum_{n=۱}^{N} \tau(n) = \sum_{n=۱}^{N} \left[\frac{N}{n}\right]$$

ب) $$\sum_{n=۱}^{N} \sigma(n) = \sum_{n=۱}^{N} n \left[\frac{N}{n}\right]$$

اثبات. الف) با توجه به رابطه‌ی $\tau = \sum_{d|n} ۱$ از قضیه بالا نتیجه می‌شود.
ب) باتوجه به رابطه‌ی $\sigma = \sum_{d|n} d$ از قضیه بالا نتیجه می‌شود. □

مثال ۳۲.۳

$$\sum_{n=۱}^{۶} \tau(n) = \left[\frac{۶}{۱}\right] + \left[\frac{۶}{۲}\right] + \left[\frac{۶}{۳}\right] + \left[\frac{۶}{۴}\right] + \left[\frac{۶}{۵}\right] + \left[\frac{۶}{۶}\right] = ۱۴$$

$$\sum_{n=۱}^{۶} \sigma(n) = ۱\left[\frac{۶}{۱}\right] + ۲\left[\frac{۶}{۲}\right] + ۳\left[\frac{۶}{۳}\right] + ۴\left[\frac{۶}{۴}\right] + ۵\left[\frac{۶}{۵}\right] + ۶\left[\frac{۶}{۶}\right] = ۳۳$$

§ ۴.۳ تمرین

در تمرینات ۱ الی ۱۰ گزاره‌ی داده شده را برای هر عدد طبیعی n ثابت کنید.

۱. $\tau(n) \leq ۲\sqrt{n}$.

۲. $\tau(n)$ فرد است اگر و تنها اگر n یک مربع کامل باشد.

۳. $\sigma(n)$ فرد است اگر و تنها اگر n یک مربع کامل یا دو برابر یک مربع کامل باشد.

۴. $\sum_{d|n} \frac{۱}{d} = \frac{\sigma(n)}{n}$.

۵. اگر n خالی از مربع باشد آن‌گاه $\tau(n)$ توانی از ۲ است.

۶. $\frac{\sigma(n!)}{n!} \geq ۱ + ۱/۲ + \cdots + ۱/n$

۷. $\sum_{d|n} \sigma(d) = \sum_{d|n} \frac{n}{d}\tau(d)$

۸. $\sum_{d|n} d\tau(d) = \sum_{d|n} \frac{n}{d}\sigma(d)$

۹. $\mu(n)\mu(n+۱)\mu(n+۲)\mu(n+۳) = ۰$.

۱۰. اگر $n \geq ۳$ $\sum_{k=۱}^{n} \mu(k!) = ۱$.

۱۱. تابع منگولت بصورت زیر تعریف می‌شود.

$$\Lambda(n) = \begin{cases} \log\ p & \text{اگر } n = p^k \text{ که در آن } p \text{ اول است و } k \geq ۱ \\ ۰ & \text{در غیر این صورت} \end{cases}$$

نشان دهید $\Lambda(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log\ d = -\sum_{d|n} \mu(d) \log\ d$

۱۲. فرض کنیم x و y اعداد حقیقی باشند. خواص زیر را برای تابع جزء صحیح ثابت کنید.

آ) اگر n عددی صحیح باشد آن‌گاه $[x+n] = [x] + n$.

ب) $[x]+[-x]=$ ۰ یا $-$۱.

ج) $[x+y]\leq[x]+[y]$ و اگر x و y مثبت باشند $[xy]\leq[x]\,[y]$.

د) برای هر عدد طبیعی n، $\left[\frac{x}{n}\right]=\left[\frac{[x]}{n}\right]$.

ه) برای اعداد طبیعی m و n و k داریم $\left[\frac{nm}{k}\right]\geq n\left[\frac{m}{k}\right]$.

۱۳. الف) نشان دهید عدد !۱۰۰۰ به ۲۴۹ صفر ختم می‌شود.

ب) کلیه اعداد n را بیابید به نحوی که $!n$ به ۳۷ صفر ختم می‌شود.

ج) نشان دهید $\frac{(۲n)!}{(n!)^۲}$ عددی صحیح و زوج است.

۱۴. الف) $\sum_{n=۱}^{N}\mu(n)\left[\frac{N}{n}\right]=$ ۱.

ب) $\left|\sum_{n=۱}^{N}\mu(n)/n\right|\leq$ ۱.

۱۵. تابع لیوویل بصورت زیر تعریف می‌شود:

$$\lambda(n)=\begin{cases}۱ & n=۱\\ (-۱)^{k_۱+\cdots+k_r} & n=p_۱^{k_۱}p_۲^{k_۲}\ldots p_r^{k_r}\ \text{ها اول‌اند } p_i\end{cases}$$

نشان دهید

الف) λ ضربی است.

ب)

$$\sum_{d|n}\lambda(d)=\begin{cases}۱ & \text{اگر } n \text{ مربع کامل باشد}\\ ۰ & \text{در غیر این صورت}\end{cases}$$

۱۶. نشان دهید $\sum_{n=۱}^{N}\lambda(n)\left[\frac{N}{n}\right]=\left[\sqrt{N}\right]$.

۱۷. نشان دهید $N=\sum_{n=۱}^{۲N}\tau(n)-\sum_{n=۱}^{N}\left[\frac{۲N}{n}\right]$.

۱۸. نشان دهید $\tau(N)=\sum_{n=۱}^{N}\left(\left[\frac{N}{n}\right]-\left[\frac{(N-۱)}{n}\right]\right)$.

۱۹. نشان دهید $\varphi(۳n) = \begin{cases} ۳\varphi(n) & ۳|n \\ ۲\varphi(n) & ۳ \nmid n \end{cases}$

۲۰. نشان دهید $\frac{۱}{۲}\sqrt{n} \leq \varphi(n) \leq n$.

۲۱. اگر $\varphi(n)|n-۱$ نشان دهید n خالی از مربع است.

۲۲. اگر n یک عدد طبیعی باشد، باقیمانده $۳^{۶n+۵}$ بر ۳۵چه اعدادی را اختیار می‌کند؟

۲۳. نشان دهید برای هر عدد طبیعی $n \geq ۲$ داریم $\sum_{\substack{۱\leq k<n \\ (k,n)=۱}} k = \frac{n\varphi(n)}{۲}$.

۲۴. نشان دهید برای هر عدد طبیعی n، $\varphi(n) = n\sum_{d|n} \frac{\mu(d)}{d}$.

۲۵. نشان دهید برای هر عدد طبیعی n، $\sum \varphi(d)\left[\frac{n}{d}\right] = \frac{n(n+۱)}{۲}$.

۲۶. نشان دهید $\sum_{d|n} \sigma(d)\varphi\left(\frac{n}{d}\right) = n\tau(n)$.

۲۷. با استفاده از ۱۲ ثابت کنید عدد طبیعی n اول است اگر و تنها اگر $\sigma(n)+\varphi(n) = n\tau(n)$.

۲۸. نشان دهید عدد طبیعی n اول است اگر و تنها اگر $\varphi(n)|n-۱$ و $n+۱|\sigma(n)$. (از ۲۱ کمک بگیرید).

۲۹. فرض کنید f یک تابع حسابی ضربی است. نشان دهید f کاملاً ضربی است اگر و تنها اگر برای هر n،

$$f^{-۱}(n) = \mu(n)f(n).$$

۳۰. اگر توابع حسابی g و $f*g$ ضربی باشند ثابت کنید f نیز ضربی است.

فصل ۴
هم‌نهشتی

در فصل قبل خواص و مسائلی مربوط به بحث تقسیم‌پذیری در اعداد صحیح را بررسی کردیم. مفهوم هم‌نهشتی و خواص و برخی قضایای اساسی آن در سال ۱۸۰۱ میلادی توسط گاوس [۱] ارائه گردید. تأثیر و کاربرد این نظریه در نظریه اعداد و به‌ویژه مسائل مربوط به تقسیم‌پذیری به حدی بوده است که بسیاری آن را ملکه‌ی نظریه اعداد می‌دانند. همان‌گونه که نظریه اعداد ملکه‌ی ریاضیات و ریاضیات را ملکه‌ی علوم می‌نامند.

در این فصل به معرفی و بررسی برخی خواص هم‌نهشتی و همچنین به ارائه‌ی برخی قضایای اساسی هم‌نهشتی می‌پردازیم.

§ ۱.۴ هم‌نهشتی و خواص آن

تعریف ۱.۴ فرض کنیم n یک عدد طبیعی باشد. دو عدد صحیح a و b را **هم‌نهشت** به پیمانه‌ی n گوییم هرگاه تفاضل a و b بر n بخش‌پذیر باشد. $(n|a-b)$. به عبارت دیگر، هرگاه عدد صحیح k یافت شود به‌نحوی که $a-b=kn$.

[۱] (*Carl Friedrich Gauss*)

علامات $a \equiv b \pmod{n}$ یا $a \overset{n}{\equiv} b$ بدین معنی هستند که a و b به پیمانه‌ی n هم‌نهشت هستند. اگر a و b به پیمانه‌ی n هم‌نهشت نباشند، آن‌گاه a و b را **ناهم‌نهشت به پیمانه‌ی** n گوییم و می‌نویسیم $a \overset{n}{\not\equiv} b$ یا $a \not\equiv b \pmod{n}$.

مثال ۲.۴ **(الف)** $۳ \overset{۱۱}{\equiv} ۲۵$ و $۳ \overset{۲}{\equiv} ۲۵$ و $-۱ \overset{۲}{\equiv} ۱$.

(ب) $a \overset{۲}{\equiv} ۰$ اگر و تنها اگر a زوج باشد و $a \overset{۲}{\equiv} ۱$ اگر و تنها اگر a فرد باشد.

(ج) برای هر دو عدد صحیح a و b همواره داریم $a \overset{۱}{\equiv} b$.

قضیه ۳.۴ برای هر عدد طبیعی n، رابطه‌ی هم‌نهشتی به پیمانه‌ی n یک رابطه‌ی هم‌ارزی روی مجموعه‌ی اعداد صحیح است. به عبارت دیگر، اگر a، bو c اعداد صحیح باشند، آن‌گاه

(الف) $a \overset{n}{\equiv} a$.

(ب) اگر $a \overset{n}{\equiv} b$ آن‌گاه $b \overset{n}{\equiv} a$.

(ج) اگر $a \overset{n}{\equiv} b$ و $b \overset{n}{\equiv} c$ آن‌گاه $a \overset{n}{\equiv} c$.

اثبات. به‌راحتی از تعریف هم‌نهشتی و خواص تقسیم نتیجه می‌شود. به عنوان مثال برای اثبات (ج)، از $a \overset{n}{\equiv} b$ و $b \overset{n}{\equiv} c$ نتیجه می‌شود که $a - b = k_۱ n$ و $b - c = k_۲ n$ که در آن $k_۱$ و $k_۲$ اعدادی صحیح هستند. از دو رابطه‌ی اخیر نتیجه می‌شود که $a-c = (a-b)+(b-c) = k_۱ n + k_۲ n = (k_۱ + k_۲) n$، این بدان معنی است که $a - c$ بر n بخش‌پذیر است. یعنی $a \overset{n}{\equiv} c$. □

خواص بسیار دیگری از هم‌نهشتی به‌راحتی قابل بیان و اثبات می‌باشند، و خواننده می‌تواند تعدادی را برای خود امتحان کند.

در چند قضیه‌ی زیر برخی از پرکاربردی‌ترین این خواص را ارائه می‌نماییم.

قضیه ۴.۴ فرض کنیم n عددی طبیعی و a، b، c و d اعدادی صحیح باشند به‌نحوی که $a \overset{n}{\equiv} b$ و $c \overset{n}{\equiv} d$. در این‌صورت

(الف) $a + c \overset{n}{\equiv} b + d$.

(ب) $a - c \overset{n}{\equiv} b - d$.

(ج) $ac \overset{n}{\equiv} bd$.

به عبارت دیگر می‌توان هم‌نهشتی‌های با یک پیمانه را با هم جمع، از هم کم یا در هم ضرب کرد.

اثبات. (الف) از مفروضات قضیه نتیجه می‌شود که $n|a-b$ و $n|c-d$. لذا $n|(a-b)+(c-d) = (a+c)-(b+d)$ و از این نتیجه می‌شود که $a + c \overset{n}{\equiv} b + d$.

(ب) شبیه (الف) اثبات می‌شود.

(ج) بنا به فرض قضیه داریم $a - b = k_1 n$ و $c - d = k_2 n$ برای اعداد صحیح k_1 و k_2. لذا $a = b + k_1 n$ و $c = d + k_2 n$. پس

$$ac = (b + k_1 n)(d + k_2 n) = bd + bk_2 n + dk_1 n + k_1 k_2 n^2 = bd + (bk_2 + dk_1 + k_1 k_2 n)n$$

در نتیجه $ac - bd = (bk_2 + dk_1 + k_1 k_2 n)n$ و لذا $n|ac - bd$. پس $ac \overset{n}{\equiv} bd$. □

نتیجه ۵.۴ فرض کنیم $a \overset{n}{\equiv} b$ و فرض کنیم c عددی صحیح و k یک عدد طبیعی باشد. در این‌صورت:

(الف) $a + c \overset{n}{\equiv} b + c$.

(ب) $a - c \overset{n}{\equiv} b - c$.

(ج) $ac \overset{n}{\equiv} bc$.

(د) $a^k \overset{n}{\equiv} b^k$.

اثبات. چون $c \overset{n}{\equiv} c$ لذا قسمت‌های (الف) و (ب) و (ج) از قسمت‌های همنام در قضیه‌ی قبل نتیجه

می‌شود. قسمت (د) از قسمت (ج) قضیه‌ی قبل و یک استقرا ساده نتیجه می‌شود. □

قبل از ارائه خواص بیشتر، با ذکر چند مثال نشان می‌دهیم چگونه استفاده از هم‌نهشتی می‌تواند به حل مسائل تقسیم‌پذیری کمک کند.

مثال ۶.۴ (الف) به عنوان اولین مثال اجازه دهید نشان دهیم عدد $N = ۲^{۲۹} + ۱$ بر ۵۹ بخش‌پذیر است. این کار به کمک هم‌نهشتی بدون محاسبه‌ی عدد N و انجام عمل تقسیم عدد بزرگ N بر ۵۹ میسر است. داریم $۵ \overset{۵۹}{\equiv} ۲^۶$. اگر دو طرف این هم‌نهشتی را به توان ۳ برسانیم، داریم $۷ \overset{۵۹}{\equiv} ۲^{۱۸}$. از ضرب سه هم‌نهشتی $۵ \overset{۵۹}{\equiv} ۲^۶$، $۷ \overset{۵۹}{\equiv} ۲^{۱۸}$ و $۳۲ \overset{۵۹}{\equiv} ۲^۵$ داریم

$$-۱ \overset{۵۹}{\equiv} -۶۰ \overset{۵۹}{\equiv} -۱۵ \times ۴ \overset{۵۹}{\equiv} ۴۴ \times ۴ \overset{۵۹}{\equiv} ۱۱ \times ۱۶ \overset{۵۹}{\equiv} ۷۰ \times ۱۶ \overset{۵۹}{\equiv} ۵ \times ۷ \times ۳۲ \overset{۵۹}{\equiv} ۲^{۲۹}$$

یعنی $-۱ \overset{۵۹}{\equiv} ۲^{۲۹}$. پس $۵۹ | ۲^{۲۹} + ۱$.

توجه کنید که در اثبات از تعریف هم‌نهشتی و برخی خواص ارائه شده، در قضایای بالا استفاده کردیم.

(ب) **(آزمون‌های تقسیم‌پذیری):** از دبیرستان به یاد دارید که یک عدد طبیعی بر ۹ بخش‌پذیر است اگر و تنها اگر مجموع ارقام آن بر ۹ بخش‌پذیر باشد. اجازه دهید به کمک هم‌نهشتی این مطلب را ثابت کنیم. فرض کنیم

$$\overline{a_n a_{n-۱} \dots a_۱ a_۰} = a_۰ + ۱۰a_۱ + ۱۰^۲ a_۲ + \cdots + ۱۰^n a_n$$

داریم $۱۰ \overset{۹}{\equiv} ۱$ و لذا $۱۰^k \overset{۹}{\equiv} ۱$ برای هر عدد طبیعی k. پس

$$A \overset{۹}{\equiv} a_۰ + a_۱ + a_۲ + \cdots + a_n$$

از این نتیجه می‌شود که باقی‌مانده‌ی تقسیم A بر ۹ همان باقی‌مانده‌ی تقسیم $a_۰ + a_۱ + \cdots + a_n$ بر ۹ است (چرا؟). به ویژه A بر ۹ بخش‌پذیر است اگر و تنها اگر $a_۰ + a_۱ + \cdots + a_n$ بر ۹ بخش‌پذیر باشد. توجه کنیم که رابطه‌ی اخیر نتیجه می‌دهد که $A \overset{۳}{\equiv} a_۰ + a_۱ + \cdots + a_n$ لذا باقی‌مانده تقسیم A بر ۳ برابر باقی‌مانده تقسیم $a_۰ + a_۱ + \cdots + a_n$ بر ۳ است. به‌ویژه A بر ۳ بخش‌پذیر است اگر و تنها اگر $a_۰ + a_۱ + \cdots + a_n$ بر ۳ بخش‌پذیر باشد.

به طریق مشابه از $۱۰ \overset{۱۱}{\equiv} -۱$ و $۱۰^k \overset{۱۱}{\equiv} (-۱)^k$ نتیجه می‌شود که

$$A \overset{۱۱}{\equiv} a_۰ - a_۱ + a_۲ - \cdots + (-۱)^k a_k + \cdots + (-۱)^n a_n$$

و لذا باقی‌مانده تقسیم A بر ۱۱ برابر باقی‌مانده‌ی تقسیم $a_۰ - a_۱ + a_۲ - \cdots + (-۱)^n a_n$ بر ۱۱ می‌باشد.

در قضایای قبل دیدیم که طریفین یک هم‌نهشتی را می‌توان با یک عدد جمع و یا در یک عدد ضرب کرد. تقسیم طرفین یک هم‌نهشتی به یک عدد در حالت کلی مجاز نیست. به عنوان مثال $۸ \overset{۶}{\equiv} ۲۰$. و ۲۰ و ۸ هر دو بر ۴ بخش‌پذیرند. ولی نمی‌توان طرفین این هم‌نهشتی را بر ۴ تقسیم کرد زیرا $۲ \overset{۶}{\not\equiv} ۵$.

قضیه‌ی زیر را در خصوص رفتار هم‌نهشتی‌ها با عمل تقسیم داریم؛

قضیه ۷.۴ فرض کنیم n عددی طبیعی و a، b و c اعدادی صحیح باشند. و فرض کنیم $d = (c, n)$ بزرگ‌ترین مقسوم‌علیه c و n باشد. در این صورت اگر $ac \overset{n}{\equiv} bc$ آن‌گاه $a \overset{\frac{n}{d}}{\equiv} b$ به عبارت دیگر یک عامل مشترک c از دو طرف یک هم‌نهشتی، قابل حذف است، به شرط آن‌که پیمانه بر $d = (c, n)$ تقسیم شود.

اثبات. از $ac \overset{n}{\equiv} bc$ نتیجه می‌شود که $n|ac - bc$. یعنی $n|c(a-b)$. در نتیجه $\frac{n}{d}|\frac{c}{d}(a-b)$. از آن‌جا که $(\frac{n}{d}, \frac{c}{d}) = ۱$ نتیجه می‌شود $\frac{n}{d}|a-b$ پس $a \overset{\frac{n}{d}}{\equiv} b$. □

نتیجه ۸.۴ فرض کنیم $ac \overset{n}{\equiv} bc$ و فرض کنیم $(c, n) = ۱$. در این‌صورت $a \overset{n}{\equiv} b$.

اثبات. از قضیه بالا نتیجه می‌شود. □

قضیه ۹.۴ فرض کنیم n عددی طبیعی و a و b دو عدد صحیح باشند.

(الف) اگر $a \overset{n}{\equiv} b$ و $|a-b| < n$ آن‌گاه $a = b$.

(ب) اگر r باقی‌مانده‌ی تقسیم a بر n باشد آن‌گاه $a \overset{n}{\equiv} r$.

(ج) $a \overset{n}{\equiv} b$ اگر و تنها اگر باقی‌مانده‌های تقسیم a و b بر n برابر باشند.

اثبات. (الف) فرض کنیم $a \overset{n}{\equiv} b$ و $|a-b| < n$. در این صورت $a - b = kn$، برای یک عدد صحیح k. لذا $|a-b| = |k|n$. پس $|k|n < n$. از این نتیجه می‌شود که $k = ۰$. پس $a = b$.

(ب) فرض کنیم r باقی‌مانده‌ی تقسیم a بر n باشد. در این صورت $a = qn + r$، برای یک عدد صحیح q. پس $a - r = qn$. یعنی $n|a-r$ پس $a \overset{n}{\equiv} r$.

(ج) فرض کنیم r باقی‌مانده‌ی تقسیم a بر n و s باقی‌مانده‌ی تقسیم b بر n باشد. بنابر (ب) داریم $a \overset{n}{\equiv} r$ و $b \overset{n}{\equiv} s$. حال اگر $r = s$ آن‌گاه از این دو رابطه نتیجه می‌شود $a \overset{n}{\equiv} b$. برعکس، فرض کنیم $a \overset{n}{\equiv} b$. در این صورت از روابط $a \overset{n}{\equiv} r$ و $b \overset{n}{\equiv} s$ نتیجه می‌شود $r \overset{n}{\equiv} s$. چون $۰ \leq r < n$ و $۰ \leq s < n$ لذا $|r-s| < n$. حال از $r \overset{n}{\equiv} s$ بنابر (الف) نتیجه می‌شود که $r = s$. □

فرض کنیم n یک عدد طبیعی و a یک عدد صحیح باشد. بنابر الگوریتم تقسیم اعداد صحیح q و r یافت می‌شوند به نحوی که $a = qn + r$ و $۰ \leq r < n$. در نتیجه $a \overset{n}{\equiv} r$.

بنابراین هر عدد صحیح با یکی از اعداد $۰, ۱, ۲, \ldots, (n-۱)$ هم‌نهشت به پیمانه n است. بدین دلیل n عدد $۰, ۱, ۲, \ldots, (n-۱)$ را دستگاه طبیعی مانده‌ها به پیمانه n گوییم. حال فرض کنیم $r_۱, r_۲, \ldots, r_{\varphi(n)}$ اعداد طبیعی نابیشتر از n باشند که نسبت به n اولند. داریم

$$(a, n) = (qn + r, n) = (r, n)$$

به‌ویژه a و n نسبت به هم اولند اگر و تنها اگر r و n نسبت به هم اول باشند، یعنی r یکی از r_i ها باشد. پس هر عدد صحیح که نسبت به n اول است با یکی از اعداد $r_۱, r_۲, \ldots, r_{\varphi(n)}$ هم‌نهشت به

پیمانه n است. لذا $\varphi(n)$ عدد $r_1, r_2, \ldots, r_{\varphi(n)}$ را دستگاه مخفف طبیعی مانده‌ها به پیمانه n گوییم. به‌طور کلی تعریف می‌کنیم:

تعریف ۱۰.۴ فرض کنیم n یک عدد طبیعی باشد.
(الف) n عدد $a_1, a_2, \ldots, a_n$ را یک **دستگاه کامل مانده‌ها به پیمانه** n گوییم هرگاه هر عدد صحیح با یکی از a_i ها هم‌نهشت به پیمانه n باشد.
(ب) $\varphi(n)$ عدد $b_1, b_2, \ldots, b_{\varphi(n)}$ را یک **دستگاه مخفف مانده‌ها به پیمانه** n گوییم هر گاه هر عدد صحیح که نسبت به n اول باشد با یکی از b_i ها هم‌نهشت به پیمانه n باشد.

به عنوان مثال n عدد $1, 2, \ldots, n$ و به‌طور کلی هر n عدد متوالی یک دستگاه مانده به پیمانه n است. اگر a یک عدد صحیح باشد و $(a, n) = 1$ و $a_1, a_2, \ldots, a_n$ یک دستگاه کامل مانده و $b_1, b_2, \ldots, b_{\varphi(n)}$ یک دستگاه مخفف مانده به پیمانه n باشند آن‌گاه $aa_1, aa_2, \ldots, aa_n$ یک دستگاه کامل مانده و $ab_1, ab_2, \ldots, ab_{\varphi(n)}$ یک دستگاه مخفف مانده به پیمانه n است (ثابت کنید).

§۲.۴ معادلات هم‌نهشتی خطی

بخش قابل توجهی از نظریه‌ی اعداد به یافتن جواب‌های معادلات (جواب‌های صحیح) اختصاص دارد. در این بخش ساده‌ترین معادلات هم‌نهشتی یعنی معادلات هم‌نهشتی خطی را بررسی می‌کنیم. ابتدا معادله‌ی

$$ax \overset{n}{\equiv} b \qquad (۱.۴)$$

را در نظر می‌گیریم که در آن a و b دو عدد صحیح و n یک عدد طبیعی است. منظور از حل این معادله به دست آوردن کلیه‌ی مقادیر صحیح x است که در معادله‌ی (۱) صدق می‌کند. ابتدا توجه می‌کنیم که اگر c یک جواب (۱) و $c' \overset{n}{\equiv} c$ آن‌گاه $ac' \overset{n}{\equiv} ac \overset{n}{\equiv} b$. لذا c' نیز یک جواب معادله‌ی (۱) است. لذا اگر معادله‌ی (۱) دارای یک جواب باشد آن‌گاه دارای بی‌نهایت جواب است. منظور از حل معادله‌ی (۱)

به دست آوردن کلیه‌ی جواب‌های غیر هم‌نهشت آن است.

فرض کنیم $c_\circ$ یک جواب معادله‌ی (۱) باشد. در این صورت $ac_\circ \overset{n}{\equiv} b$. لذا عدد صحیح k یافت می‌شود به‌نحوی که $ac_\circ - b = kn$. در نتیجه

$$ac_\circ - nk = b$$

این بدین معنی است که زوج $(c_\circ, -k)$ یک جواب از معادله‌ی سیاله‌ی

$$ax + ny = b \qquad (۲.۴)$$

می‌باشد. برعکس، اگر $(x_\circ, y_\circ)$ یک جواب (۲) باشد آن‌گاه $ax_\circ + ny_\circ = b$ و لذا $ax_\circ - b = -ny_\circ$ و این یعنی $ax_\circ \overset{n}{\equiv} b$. بنابراین معادله‌ی هم‌نهشتی (۱) دارای جواب است اگر و تنها اگر معادله‌ی سیاله‌ی (۲) دارای جواب باشد. در فصل ۱ دیدیم که (۲) دارای جواب است اگر و تنها اگر $d|b$ که در آن $d = (a, n)$. حال فرض کنیم c یک جواب (۱) باشد. می‌خواهیم کلیه‌ی جواب‌های ناهم‌نهشت به پیمانه‌ی n برای معادله‌ی (۱) را بیابیم. فرض کنیم c' یک جواب دیگر معادله‌ی (۱) باشد. در این صورت $ac' \overset{n}{\equiv} ac \overset{n}{\equiv} b$. لذا با حذف a از طرفین هم‌نهشتی داریم $c' \overset{\frac{n}{d}}{\equiv} c$. لذا $c' = c + k\frac{n}{d}$،برای یک عدد صحیح k. با تقسیم k بر d داریم $k = qd + r \quad (۰ \le r \le d-۱)$. پس

$$c' = c + k\frac{n}{d} = c + (qd + r)\frac{n}{d} = c + r\frac{n}{d} + qn$$

بنابراین $c' \overset{n}{\equiv} c + r\frac{n}{d}$. لذا هر جواب معادله‌ی (۱) به پیمانه‌ی n برابر $c + r\frac{n}{d}$ است که در آن $۰ \le r \le d-۱$. داریم

$$a(c + r\frac{n}{d}) \overset{n}{\equiv} ac + ar\frac{n}{d} \overset{n}{\equiv} b + \frac{a}{d}rn \overset{n}{\equiv} b$$

یعنی $c + r\frac{n}{d}$ یک جواب معادله‌ی (۱) است.

بنابراین جواب‌های (۱) به پیمانه‌ی n عبارتند از

$$c\ ,\ c + \frac{n}{d}\ ,\ c + ۲\frac{n}{d}\ ,\ \ldots\ ,\ c + (d-۱)\frac{n}{d}$$

حال نشان می‌دهیم این جواب‌ها به پیمانه‌ی n دوبدو ناهم‌نهشت‌اند. اگر $۰ \le r \le d-۱$ و $۰ \le r' \le d-۱$ چنان باشند که $c + r\frac{n}{d} \overset{n}{\equiv} c + r'\frac{n}{d}$ آن‌گاه $r\frac{n}{d} \overset{n}{\equiv} r'\frac{n}{d}$ و لذا $r \overset{d}{\equiv} r'$ (توجه کنید که با

حذف $\frac{n}{d}$ از دو طرف هم‌نهشتی پیمانه نیز بر $\frac{n}{d}$ تقسیم می‌شود). حال چون $|r-r'|<d$ از هم‌نهشتی $r \overset{d}{\equiv} r'$ نتیجه می‌شود $r=r'$.

آن‌چه را در بالا ثابت کردیم در قضیه‌ی زیر خلاصه می‌کنیم:

قضیه ۱۱.۴ فرض کنیم n یک عدد طبیعی و a و b دو عدد صحیح باشند. و فرض کنیم $d=(a,n)$. در این صورت معادله‌ی هم‌نهشتی

$$ax \overset{n}{\equiv} b$$

دارای جواب است اگر و تنها اگر $d|b$.

به‌علاوه اگر $d|b$ و c یک جواب هم‌نهشتی فوق باشد آن‌گاه هم‌نهشتی فوق دارای دقیقاً d جواب دوبدو ناهم‌نهشت به پیمانه‌ی n می‌باشد که عبارتند از

$$c\ ,\ c+\frac{n}{d}\ ,\ c+۲\frac{n}{d}\ ,\ \ldots\ ,\ c+(d-۱)\frac{n}{d}$$

تبصره ۱۲.۴ با عنایت به قضیه‌ی فوق برای پاسخ به سوال وجود یا عدم وجود برای معادله‌ی $ax \overset{n}{\equiv} b$ کافی است $d=(a,n)$ را محاسبه نماییم و این کار به کمک الگوریتم اقلیدس کاری آسان است. همچنین اگر $d|b$ آن‌گاه در فصل ۱ دیدیم که به کمک الگوریتم اقلیدس روش مؤثری برای حل معادله‌ی سیاله‌ی $ax+ny=b$ در دست است و لذا به دست آوردن یک جواب c آسان است و سپس قضیه‌ی فوق همه‌ی جواب‌ها را به دست می‌دهد.

نتیجه ۱۳.۴ فرض کنیم n یک عدد طبیعی و a و b دو عدد صحیح باشند. و فرض کنیم a و n نسبت به هم اول باشند. دراین صورت هم‌نهشتی

$$ax \overset{n}{\equiv} b$$

دارای یک جواب منحصربه‌فرد به پیمانه‌ی n است.

اثبات. از قضیه‌ی قبل با فرض $d = ۱$ نتیجه می‌شود. □

تعریف ۱۴.۴ فرض کنیم n یک عدد طبیعی و a عددی صحیح باشد که نسبت به n اول است. دراین‌صورت هم‌نهشتی

$$ax \overset{n}{\equiv} ۱$$

بنابر نتیجه‌ی قبل دارای یک جواب منحصربه‌فرد به پیمانه‌ی n است. هر جواب این معادله را یک **وارون حسابی** a به پیمانه‌ی n گوییم.

توجه کنیم که اگر a و n نسبت به هم اول باشند آن‌گاه وارون حسابی a به پیمانه‌ی n وجود دارد و منحصربه‌فرد است (به پیمانه‌ی n).

مثال ۱۵.۴ کلیه‌ی جواب‌های هم‌نهشتی $۵۷x \overset{۶۹}{\equiv} ۲۱$ را به دست می‌آوریم. ابتدا برای به دست آوردن d، بزرگ‌ترین مقسوم‌علیه مشترک ۵۷ و ۶۹ از الگوریتم اقلیدس بهره می‌گیریم

$$۶۹ = ۱ \times ۵۷ + ۱۲$$

$$۵۷ = ۴ \times ۱۲ + ۹$$

$$۱۲ = ۱ \times ۹ + ۳$$

$$۹ = ۳ \times ۳ + ۰$$

لذا $d = ۳$. چون $d|۲۱$ لذا معادله دارای ۳ جواب به پیمانه‌ی ۶۹ است. برای به دست آوردن یکی از جواب‌ها دوباره از الگوریتم اقلیدس برای حل معادله‌ی هم‌نهشتی $۵۷x + ۶۹y = ۲۱$ استفاده می‌کنیم. از تقسیمات متوالی بالا داریم

$$d = ۳ = ۱۲ - ۹ = ۱۲ - (۵۷ - ۴ \times ۱۲) = ۵ \times ۱۲ - ۵۷ = ۵(۶۹ - ۵۷) - ۵۷$$

$$= ۵ \times ۶۹ - ۶ \times ۵۷$$

در نتیجه $۲۱ = (۳۵)۶۹ + (-۴۲)۵۷$. پس $۲۱ \overset{۶۹}{\equiv} (-۴۲)۵۷$. بنابراین یک جواب هم‌نهشتی

$c = -۴۲$ می‌باشد. حال با توجه به قضیه‌ی اخیر ۳ جواب هم‌نهشتی عبارتند از $c\ ,\ c+\frac{n}{d}\ ,\ c+۲\frac{n}{d}$ که در اینجا $c = -۴۲$، $n = ۶۹$ و $d = ۳$. پس جواب‌ها عبارتند از ۴ و ۱۹− و ۴۲−. بنابراین کوچک‌ترین جواب‌های نامنفی معادله ۵۰ و ۲۷ و ۴ می‌باشند.

قضیه‌ی بعد که مربوط به حل همزمان یک دستگاه معادلات هم‌نهشتی است به قضیه‌ی باقی‌مانده‌ی چینی معروف است. توجه کنیم دو معادله‌ی هم‌نهشتی که هر دو دارای جواب هستند ممکن است جواب مشترک نداشته باشد. به عنوان مثال دو معادله‌ی $۲x \overset{۶}{\equiv} ۱۰$ و $۵x \overset{۱۵}{\equiv} ۵$ هر دو دارای جواب هستند. ولی جواب مشترک برای دو معادله وجود ندارد. زیرا هر جواب c از معادله‌ی اول در شرط $c \overset{۳}{\equiv} ۲$ ولی هر جواب c' از معادله‌ی دوم در شرط $c \overset{۳}{\equiv} ۱$ صدق می‌کند. قضیه باقی‌مانده‌ی چینی وجود جواب مشترک را تحت شرایطی تضمین می‌کند.

قضیه ۱۶.۴ (قضیه‌ی باقی‌مانده‌ی چینی) فرض کنیم $n_k, \ldots, n_۲, n_۱$ اعداد طبیعی و دوبدو نسبت به هم اول باشند. فرض کنیم $b_k, \ldots, b_۲, b_۱$ اعدادی صحیح باشند. در این‌صورت دستگاه هم‌نهشتی

$$x \overset{n_۱}{\equiv} b_۱$$
$$x \overset{n_۲}{\equiv} b_۲$$
$$\vdots$$
$$x \overset{n_k}{\equiv} b_k$$

دارای جواب است. به‌علاوه، این جواب به پیمانه‌ی $m = n_۱n_۲\ldots n_k$ منحصربه‌فرد است.

اثبات. قرار می‌دهیم $m = n_۱n_۲\ldots n_k$ و برای هر $۱ \le i \le k$ قرار می‌دهیم $m_i = \frac{m}{n_i}$. در این صورت $(m_i, n_i) = ۱$ زیرا $m_i = n_۱n_۲\ldots n_{i-۱}n_{i+۱}\ldots n_k$ و $n_۱, n_۲, \ldots, n_{i-۱}, n_{i+۱}, \ldots, n_k$ همگی نسبت به n_i اولند. بنابراین m_i دارای وارون حسابی به پیمانه‌ی n_i است. فرض کنیم m_i' وارون حسابی m_i به پیمانه‌ی n_i باشد. حال قرار می‌دهیم

$$x_۰ = b_۱m_۱m'_۱ + b_۲m_۲m'_۲ + \cdots + b_km_km'_k$$

حال فرض کنیم $۱ \le j \le k$. دراین صورت $n_j | m_i$ برای هر $i \neq j$ و $۱ \le i \le k$. لذا برای هر $i \neq j$ داریم $b_im_im'_i \overset{n_j}{\equiv} ۰$. بنابراین

$$x_۰ \overset{n_j}{\equiv} ۰ + ۰ + \cdots + ۰ + b_jm_jm'_j + ۰ + \cdots + ۰$$

امّا بنابه فرض $m_jm'_j \overset{n_j}{\equiv} ۱$. لذا $x_۰ \overset{n_j}{\equiv} b_j$ بنابراین $x_۰$ یک جواب دستگاه است. اگر $x'_۰$ و $x_۰$ هر دو جواب دستگاه باشند آن‌گاه داریم

$$x_۰ \overset{n_۱}{\equiv} x'_۰$$

$$x_۰ \overset{n_۲}{\equiv} x'_۰$$

$$\vdots$$

$$x_۰ \overset{n_k}{\equiv} x'_۰$$

لذا برای هر $۱ \le i \le k$ داریم $n_i | x_۰ - x'_۰$. لذا $m | x_۰ - x'_۰$.(زیرا n_iها دوبدو نسبت به هم اول‌اند و $m = n_۱n_۲ \dots n_k$.) پس $x_۰ \overset{m}{\equiv} x'_۰$ و اثبات تمام است. □

توجه کنیم که در اثبات قضیه‌ی بالا در واقع روش به دست آوردن جواب ارائه گردیده است.

مثال ۱۷.۴ کوچک‌ترین عدد صحیح مثبتی را می‌یابیم که باقی مانده‌ی آن بر ۳ و ۵ و ۷ به ترتیب ۱ و ۲ و ۳ باشد. برای حل باید کوچک‌ترین جواب مثبت دستگاه

$$x \overset{۳}{\equiv} ۱$$

$$x \overset{۵}{\equiv} ۲$$

$$x \overset{۷}{\equiv} ۳$$

می‌باشد. اجازه دهید داده‌ها و محاسبات را در یک جدول خلاصه کنیم.

i	n_i	m_i	m'_i	b_i	$b_i m_i m'_i$
۱	۳	۳۵	۲	۱	۷۰
۲	۵	۲۱	۱	۲	۴۲
۳	۷	۱۵	۱	۳	۴۵

بنابراین جواب دستگاه عبارت است از

$$x_۰ \overset{۱۰۵}{\equiv} ۷۰ + ۴۲ + ۴۵ = ۱۵۷ \overset{۱۰۵}{\equiv} ۵۲$$

پس جواب مساله **۵۲** است.

تبصره ۱۸.۴ صورت کلی‌تری از قضیه را می‌توان بیان و اثبات کرد. شکل ساده‌ی ارائه شده‌ی بالا، شکل دارای کاربرد بیشتر است. ضمن آن‌که شکل بیان شده به قضیه‌ی اصلی چینی نزدیک‌تر است. به عنوان مثال شکل عام‌تری از قضیه، در نتیجه‌ی ذیل به راحتی از قضیه نتیجه می‌شود.

نتیجه ۱۹.۴ فرض کنیم $n_k, \ldots, n_۲, n_۱$ اعداد طبیعی دوبدو نسبت به هم اول و $a_k, \ldots, a_۲, a_۱$ اعدادی صحیح باشند به‌نحوی که $(a_i, n_i) = ۱$ برای $۱ \leq i \leq k$. فرض کنیم $b_k, \ldots, b_۲, b_۱$ اعدادی صحیح دلخواهی باشند. در این صورت دستگاه ذیل دارای یک جواب منحصربه‌فرد به پیمانه‌ی $m = n_۱ n_۲ \ldots n_k$ است.

$$a_۱ x \overset{n_۱}{\equiv} b_۱$$

$$a_۲ x \overset{n_۲}{\equiv} b_۲$$

$$\vdots$$

$$a_k x \overset{n_k}{\equiv} b_k$$

اثبات. با توجه به مفروضات قضیه برای هر $۱ \leq i \leq k$ وارون حسابی a_i به پیمانه‌ی n_i وجود دارد. فرض کنیم a'_i این وارون حسابی باشد. هم‌نهشتی $a_i x \overset{n_i}{\equiv} b_i$ با هم‌نهشتی $x \overset{n_i}{\equiv} b_i a'_i$ معادل است.

لذا کافی است دستگاه

$$x \overset{n_1}{\equiv} b_1 a'_1$$

$$x \overset{n_2}{\equiv} b_2 a'_2$$

$$\vdots$$

$$x \overset{n_k}{\equiv} b_k a'_k$$

را حل کنیم. و این همان قضیه‌ی قبل است. □

اجازه دهید قضیه‌ی زیبای زیر را به عنوان نتیجه‌ای از قضیه‌ی چینی ثابت کنیم.

قضیه ۲۰.۴ مربع‌های به اندازه‌ی دلخواه بزرگ در صفحه موجودند به‌نحوی که هیچ یک از نقاط داخل آن‌ها که دارای مختصات صحیح‌اند در بین مجموعه‌ی همه‌ی نقاط با مختصات صحیح صفحه، از مبدأ قابل رؤیت نیستند.

اثبات. ابتدا توجه می‌کنیم که نقطه‌ی با مختصات صحیح c, d در بین مجموعه‌ی نقاط با مختصات صحیح از مبدأ قابل رؤیت است اگرو تنهااگر c و d نسبت به هم اول باشند.(چرا؟)

بنابراین کافی است برای هر عدد صحیح k مربعی با رئوس

$$\{(a, b), (a + k, b), (a, b + k), (a + k, b + k)\}$$

بیابیم به‌نحوی که هر نقطه داخل مربع با مختصات صحیح، دارای مختصاتی باشد که نسبت به هم اول نیستند. توجه می‌کنیم که نقاط داخل مربع فوق که دارای مختصات صحیح‌اند عبارتست از

$$(a + r, b + s) \qquad\qquad 0 < r < k \ , 0 < s < k$$

حال فرض کنیم $p_1 = 2$ و $p_2 = 3$ و برای هر $i \geq 1$ عدد p_i، i-امین عدد اول باشد. ماتریس

$k \times k$ زیر را درنظر می‌گیریم

$$A = \begin{bmatrix} p_۱ & p_۲ & \cdots & p_k \\ p_{k+۱} & p_{k+۲} & \cdots & p_{۲k} \\ \vdots & & & \\ p_{k^۲-k+۱} & & \cdots & p_{k^۲} \end{bmatrix}$$

فرض کنیم m_i حاصل‌ضرب مؤلفه‌های سطر i-ام و n_i حاصل ضرب مؤلفه‌های ستون i-ام A باشد. در این‌صورت m_i ها دوبدو نسبت به هم اول و n_i ها نیز دوبدو نسبت به هم اول‌اند. بنابراین بنابر قضیه‌ی باقی‌مانده‌ی چینی دستگاه

$$\begin{aligned} x &\overset{m_۱}{\equiv} -۱ \\ x &\overset{m_۲}{\equiv} -۲ \\ &\vdots \\ x &\overset{m_k}{\equiv} -k \end{aligned}$$

دارای جواب منحصربه‌فردی به پیمانه‌ی $m = n_۱n_۲\cdots n_k = m_۱m_۲\cdots m_k$ مانند a است.

به طریق مشابه دستگاه

$$\begin{aligned} y &\overset{n_۱}{\equiv} -۱ \\ y &\overset{n_۲}{\equiv} -۲ \\ &\vdots \\ y &\overset{n_k}{\equiv} -k \end{aligned}$$

به پیمانه‌ی m دارای جواب منحصربه‌فردی مانند b است.

حال مربع با رئوس $S = \{(a,b),(a+k,b),(a,b+k),(a+k,b+k)\}$ را در نظر می‌گیریم. فرض کنیم

$$(a+r,b+s) \qquad \circ < r < k\ ,\circ < s < k$$

یک نقطه‌ی دلخواه داخل S باشد. داریم

$$a \overset{m_r}{\equiv} -r \qquad , \qquad b \overset{n_s}{\equiv} -s$$

لذا

$$m_r|a+r \qquad , \qquad n_s|b+s$$

اگر p مؤلفه‌ی سطر r-ام و ستون s-ام ماتریس A باشد آن‌گاه $p|n_s$ و $p|m_r$. بنابراین

$$p|a+r \qquad , \qquad p|b+s$$

بنابراین اعداد $a+r$ و $b+s$ نسبت به هم اول نیستند. بنابراین نقطه‌ی $(a+r, b+s)$ در بین مجموعه‌ی نقاط با مختصات صحیح از مبدأ قابل رؤیت نیست. و اثبات تمام است. □

§۳.۴ چند قضیه‌ی اساسی هم‌نهشتی

در این بخش چند قضیه‌ی اساسی هم‌نهشتی از جمله قضایای اویلر، فرما و ویلسون را ثابت می‌کنیم، و کاربردهایی از آن‌ها ارائه می‌نماییم.

ابتدا یادآوری می‌کنیم که برای عدد طبیعی n مجموعه‌ی $\{a_۱, a_۲, \ldots, a_{\phi(n)}\}$ را یک دستگاه مخفف مانده‌ها به پیمانه‌ی n گوییم هرگاه هر عدد صحیح که نسبت به n اول است با یکی از a_iها به پیمانه‌ی n هم‌نهشت باشد. لم زیر در خصوص دستگاه مخفف مانده‌ها به پیمانه‌ی n بسیار مفید است:

لم ۲۱.۴ فرض کنیم n عدد طبیعی و $A = \{a_۱, a_۲, \ldots, a_{\phi(n)}\}$ یک دستگاه مخفف مانده‌ها به پیمانه‌ی n باشد. در این‌صورت

(الف) هر a_i نسبت به n اول است و a_iها دوبدو به پیمانه‌ی n ناهم‌نهشت‌اند.

(ب) اگر $B = \{b_۱, b_۲, \ldots, b_{\phi(n)}\}$ و b_i نسبت به n اول و دوبدو به پیمانه‌ی n ناهم‌نهشت باشند آن‌گاه B نیز یک دستگاه مخفف مانده‌ها به پیمانه‌ی n است.

(ج) اگر a یک عدد صحیح و نسبت به n اول باشد آن‌گاه مجموعه‌ی $C = \{aa_۱, aa_۲, \ldots, aa_{\phi(n)}\}$ نیز یک دستگاه مخفف مانده‌ها به پیمانه‌ی n است.

اثبات. (الف) فرض کنیم $r_۱, r_۲, \ldots, r_{\phi(n)}$ اعداد صحیح مثبت نابیشتر از n باشند که نسبت به n اولند. بنابه فرض هر r_i با یکی از a_iها هم‌نهشت است. چون r_iها به پیمانه‌ی n دوبدو ناهم‌نهشت اند لذا $\phi(n)$ عدد $r_۱, r_۲, \ldots, r_{\phi(n)}$ با $\phi(n)$ عضو متمایز A هم‌نهشت‌اند. چون A دارای $\phi(n)$ عضو است لذا هر r_i با یک عضو A به پیمانه‌ی n هم‌نهشت است و بالعکس. حال چون $r_۱, r_۲, \ldots, r_{\phi(n)}$ به پیمانه‌ی n دوبدو ناهم‌نهشت اند لذا $a_۱, a_۲, \ldots, a_{\phi(n)}$ نیز به پیمانه‌ی n دوبدو ناهم‌نهشت اند. حال فرض کنیم $۱ \leq i \leq \phi(n)$. در این صورت $a_i \overset{n}{\equiv} r_j$ برای یک $۱ \leq j \leq \phi(n)$. لذا $(a_i, n) = (r_j, n) = ۱$(چرا؟).

(ب) چون اعضای B نسبت به n اول‌اند لذا هر عضو B با یک عضو A به پیمانه‌ی n هم‌نهشت است. و چون اعضای B دوبدو به پیمانه‌ی n ناهم‌نهشت اند لذا اعضای متمایز B با اعضای متمایز A هم‌نهشت اند. از این نتیجه می‌شود که هر عضو A با یک عضو B هم‌نهشت به پیمانه‌ی n است. حال هر عدد صحیح که نسبت به n اول است با یک عضو A و در نتیجه بایک عضو B به پیمانه‌ی n هم‌نهشت است.پس B یک دستگاه مخفف مانده‌ها به پیمانه‌ی n است.

(ج) بنابر (الف) هر a_i نسبت به n اول است. همچنین بنابه فرض a نسبت به n اول است. پس هر aa_i نسبت به n اول است. از طرف دیگر اعضای C دوبدو ناهم‌نهشت به پیمانه‌ی n می‌باشند.(چرا؟) حال از (ب) نتیجه می‌شود که C نیز یک دستگاه مخفف مانده‌ها به پیمانه‌ی n است. □

مثال ۲۲.۴ مجموعه‌ی $A = \{۱, ۲, ۴, ۷, ۸, ۱۱, ۱۳, ۱۴\}$ دستگاه مخفف طبیعی مانده‌ها به پیمانه‌ی ۱۵ است. با ضرب اعضای A در عدد $a = ۴$ مجموعه‌ی $B = \{۴, ۸, ۱۶, ۲۸, ۳۲, ۴۴, ۵۲, ۶۴\}$ به دست می‌آید که یک دستگاه مخفف مانده‌ها به پیمانه‌ی ۱۵ است. اعداد $۴, ۸, ۱۶, ۲۸, ۳۲, ۴۴, ۵۲, ۶۴$ به پیمانه‌ی ۱۵ به ترتیب با اعداد $۴, ۸, ۱, ۱۳, ۲, ۱۴, ۷, ۴$ هم‌نهشت می‌باشد.

با استفاده از لم فوق، اثبات قضیه‌ی اویلر کاری آسان است.

قضیه ۲۳.۴ (قضیه‌ی اویلر) فرض کنیم n عدد طبیعی و a عددی صحیح باشد که نسبت به n اول است. در این‌صورت

$$a^{\phi(n)} \overset{n}{\equiv} ۱$$

اثبات. فرض کنیم $a_۱, a_۲, \ldots, a_{\phi(n)}$ یک دستگاه مخفف مانده‌ها به پیمانه‌ی n باشد. بنابه لم بالا اعداد $aa_۱, aa_۲, \ldots, aa_{\phi(n)}$ نیز تشکیل یک دستگاه مخفف مانده‌ها به پیمانه‌ی n می‌دهند. لذا هر a_i با یکی از aa_iها هم‌نهشت است و بالعکس. بنابراین اعداد $a_۱, a_۲, \ldots, a_{\phi(n)}$ به پیمانه‌ی n همان اعداد $aa_۱, aa_۲, \ldots, aa_{\phi(n)}$ می‌باشند(احتمالاً با ترتیبی متفاوت). پس

$$(aa_۱)(aa_۲)\ldots(aa_{\phi(n)}) \overset{n}{\equiv} a_۱a_۲\ldots a_{\phi(n)}$$

لذا

$$a^{\phi(n)}a_۱a_۲\ldots a_{\phi(n)} \overset{n}{\equiv} a_۱a_۲\ldots a_{\phi(n)}$$

حال بنابر لم قبل a_iها نسبت به n اولند و لذا می‌توان آن‌ها را از طرفین هم‌نهشتی بالا حذف کرد. پس

$$a^{\phi(n)} \overset{n}{\equiv} ۱$$

□

حالت خاص قضیه‌ی اویلر که در آن $n = p$ عددی اول است اولین بار توسط فرما ثابت شد و به قضیه کوچک فرما معروف است.

نتیجه ۲۴.۴ (قضیه کوچک فرما) فرض کنیم p عددی اول و a عددی صحیح باشد و $p \nmid a$. در این‌صورت

$$a^{p-۱} \overset{p}{\equiv} ۱$$

اثبات. چون p اول است از $p \nmid a$ نتیجه می‌شود که a و p نسبت به هم اول‌اند. همچنین چون p اول

است داریم $\phi(p) = p - ۱$. لذا حکم از قضیه‌ی اویلر نتیجه می‌شود. □

نتیجه ۲۵.۴ اگر p عددی اول و a عددی صحیح باشد، آن‌گاه $a^p \overset{p}{\equiv} a$.

اثبات. اگر $p|a$ آن‌گاه $p|a^n$ و لذا $a^p \overset{p}{\equiv} a \overset{p}{\equiv} ۰$. اگر $p \nmid a$ آن‌گاه بنابر نتیجه‌ی قبل

$$a^{p-۱} \overset{p}{\equiv} ۱$$

و در نتیجه $a^p \overset{p}{\equiv} a$. □

دو مثال زیر کاربرد مؤثر قضیه‌ی اویلر را در محاسبات نشان می‌دهد:

مثال ۲۶.۴ باقیمانده تقسیم $۲^{۱۰۰۰۰۰}$ بر ۳۵ چیست؟

حل: داریم $\varphi(۳۵) = \varphi(۵)\varphi(۷) = ۴ \times ۶ = ۲۴$. لذا بنابر قضیه اویلر $۱ \overset{۳۵}{\equiv} ۲^{۲۴}$.

$$۲^{۱۰۰۰۰۰} \overset{۳۵}{\equiv} ۲^{۲۴ \times ۴۱۶۶ + ۱۶} = (۲^{۲۴})^{۴۱۶۶} ۲^{۱۶} \overset{۳۵}{\equiv} ۲^{۱۶} \overset{۳۵}{\equiv} ۲^۶ \times ۲^۶ \times ۲^۴$$

$$\overset{۳۵}{\equiv} (-۶)(-۶)(۱۶) = ۵۷۶ \overset{۳۵}{\equiv} ۱۶$$

لذا پاسخ ۱۶ است.

مثال ۲۷.۴ اگر n یک عدد طبیعی باشد باقیمانده تقسیم $k = ۱۰^{۴۸n+۹}$ بر ۵۱ چیست؟

حل: داریم

$$۱۰^{۴۸n+۹} \overset{۳}{\equiv} ۱^{۴۸n+۹} \overset{۳}{\equiv} ۱$$

$$۱۰^{۴۸n+۹} \overset{۱۷}{\equiv} (۱۰^{۱۶})^{۳n} \times ۱۰^۹ \overset{۱۷}{\equiv} (۱۰^۲)^۴ \times ۱۰ = (-۲)^۴ \times ۱۰ \overset{۱۷}{\equiv} -۱۰ \overset{۱۷}{\equiv} ۷$$

فرض کنیم باقیمانده مورد نظر r باشد. داریم $n \overset{۵۱}{\equiv} r$ پس $n \overset{۳}{\equiv} r$ و $n \overset{۱۷}{\equiv} r$. لذا $r \overset{۳}{\equiv} ۱$ و $r \overset{۱۷}{\equiv} ۷$. تنها اعداد نامنفی کمتر از ۵۱ که در این دو هم‌نهشتی صدق می‌کند عدد ۷ است. لذا پاسخ ۷ است.

چینی‌ها حدود ۲۵۰۰ سال پیش ادعا کردند که عکس قضیه‌ی فرما نیز برقرار است. در واقع آن‌ها ادعا کردند که اگر عدد $n > ۲$ چنان باشد که $۲^n \overset{n}{\equiv} ۲$ آن‌گاه n اول است. این ادعا برای $۳ \leq n \leq ۳۴۰$

درست است. لذا می‌توان فهمید که ادعای آن‌ها بر مبنای تعداد قابل توجهی آزمایش صورت پذیرفته است. ولی در ریاضیات نمونه‌هایی داریم که گزاره نمایی بر حسب اعداد طبیعی n، برای نمونه‌های کوچک بسیاری درست است ولی در دوردست(اعداد بزرگ n) درست نیست. به همین دلیل است که آزمایش نمونه‌ها هرچه تعداد نمونه‌ها زیاد باشد به عنوان یک اثبات ریاضی پذیرفته نیست. در خصوص ادعای فوق نیز $n = ۳۴۱$ اولین عددی است که ادعا را نقض می‌کند. اجازه دهید نشان دهیم $n = ۳۴۱$ ادعا را نقض می‌کند.

ابتدا توجه می‌کنیم که $۳۴۱ = ۳۱ \times ۱۱$ اول نیست. نشان می‌دهیم $۲^{۳۴۱} \overset{۳۴۱}{\equiv} ۲$. داریم $۱۰۲۴ = ۳۱ \times ۳۳ + ۱$ لذا $۲^{۱۰} = ۲^{۱۰} \overset{۳۱}{\equiv} ۱$ پس $۲^{۱۱} \overset{۳۱}{\equiv} ۲$. در نتیجه بنابر قضیه‌ی کوچک فرما داریم

$$۲^{۳۴۱} = ۲^{۱۱ \times ۳۱} \overset{۳۱}{\equiv} ۲^{۱۱} \overset{۳۱}{\equiv} ۲$$

از طرف دیگر از قضیه‌ی کوچک فرما نتیجه می‌شود

$$۲^{۳۱} \overset{۱۱}{\equiv} ۲ \times (۲^{۱۰})^{۳} \overset{۱۱}{\equiv} ۲ \times ۱ = ۲$$

و در نتیجه

$$۲^{۳۴۱} = ۲^{۱۱ \times ۳۱} \overset{۱۱}{\equiv} ۲^{۱۱} \overset{۱۱}{\equiv} ۲$$

حال از دو هم‌نهشتی $۲ \overset{۳۱}{\equiv} ۲^{۳۴۱}$ و $۲ \overset{۱۱}{\equiv} ۲^{۳۴۱}$ نتیجه می‌شود که $۲ \overset{۳۴۱}{\equiv} ۲^{۳۴۱}$.

این مشاهده مبنای تعریف زیر است:

تعریف ۲۸.۴ (الف) عدد مرکب n را **شبه‌اول** گوییم هرگاه $۲^n \overset{n}{\equiv} ۲$.

(ب) به‌طور کلی عدد مرکب n را شبه‌اول نسبت به پایه‌ی a گوییم هرگاه $a^n \overset{n}{\equiv} a$. لذا عدد شبه اول همان عدد شبه‌اول نسبت به پایه‌ی ۲ است.

(ج) عدد مرکب n را **شبه‌اول مطلق** (یا کارمایکل $Carmichael$) گوییم هرگاه شبه‌اول نسبت به پایه‌ی a برای هر a باشد.

در بالا نشان دادیم ۳۴۱ یک عدد شبه اول است. در تمرینات از شما خواسته می‌شود ثابت کنید بی‌نهایت عدد شبه اول (نسبت به پایه‌ی ۲) وجود دارد. ثابت شده است نسبت به هر پایه‌ی a بی‌نهایت عدد شبه اول وجود دارد. در تمرینات مثال‌های بیشتری را خواهید دید.

تبصره ۲۹.۴ از آن‌جا که اعداد شبه اول نادرند(به عنوان نمونه تعداد اعداد شبه اول کمتر از یک میلیون فقط ۲۴۵ ولی تعداد اول کمتر از یک میلیون ۷۸۴۹۴ است.) اگر عدد n در شرط $۲^n \overset{n}{\equiv} ۲$ صدق کند آن‌گاه n به احتمال زیاد اول است. در بسیاری از نرم‌افزارها از این آزمون برای بررسی اول یا مرکب بودن عدد n استفاده می‌کنند. بدین معنی که اگر $۲^n \overset{n}{\equiv} ۲$ آن‌گاه n را اول می‌گیرند و اگر $۲^n \overset{n}{\not\equiv} ۲$ آن‌گاه n را مرکب می‌گیرند. توجه کنید که در چنین نرم‌افزارهایی اگر پاسخ اول یا مرکب بودن n، مرکب است آن‌گاه n یقیناً مرکب است. ولی اگر پاسخ اول باشد آن‌گاه n به احتمال زیاد اول است.

اکنون قضیه‌ی مهم دیگر در بحث هم‌نهشتی را ثابت می‌کنیم:

قضیه ۳۰.۴ (قضیه‌ی ویلسون) فرض کنیم p یک عدد اول باشد. در این صورت

$$(p-۱)! \overset{p}{\equiv} -۱$$

اثبات. قضیه در حالت $p = ۲$ و $p = ۳$ به راحتی قابل مشاهده است. لذا فرض کنیم $p \geq ۵$. فرض کنیم $۲ \leq k \leq p-۲$ دلخواه باشد. در این صورت k دارای وارون حسابی به پیمانه‌ی p است. فرض کنیم k' وارون حسابی k به پیمانه‌ی p باشد. چون k' یک جواب هم‌نهشتی $kx \overset{p}{\equiv} ۱$ است لذا می‌توان فرض کرد $۱ \leq k' \leq p-۱$. توجه کنیم که $۱^۲ \overset{p}{\equiv} ۱$ و $(p-۱)^۲ \overset{p}{\equiv} ۱$ لذا ۱ و $p-۱$ وارون حسابی خود به پیمانه‌ی p هستند. چون $۲ \leq k \leq p-۲$ لذا $k' \neq ۱$ و $k' \neq p-۱$. پس $۲ \leq k' \leq p-۲$ اگر $k' = k$ آن‌گاه $k^۲ \overset{p}{\equiv} ۱$ و لذا $p|k^۲ - ۱ = (k-۱)(k+۱)$ و در نتیجه $p|k-۱$ یا $p|k+۱$ و این غیر ممکن است. زیرا $۳ \leq k-۱ \leq p-۱$ و $۳ \leq k+۱ \leq p-۱$. از این نتیجه می‌شود که هر عدد $۲ \leq k \leq p-۲$ دارای وارون حسابی $۲ \leq k' \leq p-۲$ است و به علاوه $k' \neq k$. پس اعداد $۲, ۳, \ldots, p-۲$ را می‌توان زوج زوج دسته‌بندی کرد که در آن دو عضو هر زوج وارون حسابی

یکدیگرند. پس

$$۲ \times ۳ \times ۴ \times \cdots \times (p-۲) \overset{p}{\equiv} ۱$$

و لذا

$$۲ \times ۳ \times ۴ \times \cdots \times (p-۲)(p-۱) \overset{p}{\equiv} p-۱$$

در نتیجه

$$(p-۱)! \overset{p}{\equiv} -۱$$

□

اجازه دهید آن‌چه را در اثبات قضیه‌ی ویلسون گفتیم در یک مثال مشاهده کنیم. فرض کنیم $p = ۱۳$. در این صورت اعداد $۲, ۳, ۴, \ldots, ۱۱$ را در نظر می‌گیریم. در این لیست ۷ وارون حسابی ۲، ۹ وارون حسابی ۳، ۱۰ وارون حسابی ۴، ۸ وارون حسابی ۵ و ۱۱ وارون حسابی ۶ به پیمانه‌ی ۱۳ است: لذا

$$۲ \times ۳ \times ۴ \times \cdots \times ۱۱ = (۲ \times ۷)(۳ \times ۹)(۴ \times ۱۰)(۵ \times ۸)(۶ \times ۱۱)$$

$$\overset{۱۳}{\equiv} ۱ \times ۱ \times ۱ \times ۱ \times ۱ = ۱$$

به عنوان کاربردی از قضایای فرما و ویلسون قضیه‌ی زیر را در خصوص هم‌نهشتی‌های درجه دوم ثابت می‌کنیم.

قضیه ۳۱.۴ فرض کنیم p یک عدد اول فرد باشد. در این صورت معادله‌ی هم‌نهشتی

$$x^۲ \overset{p}{\equiv} -۱ \tag{۳.۴}$$

دارای جواب است اگر و تنها اگر $p \overset{۴}{\equiv} ۱$.

اثبات. ابتدا فرض کنیم هم‌نهشتی (۱) دارای جوابی چون b باشد. پس $b^۲ \overset{p}{\equiv} -۱$. لذا $(b^۲)^{\frac{p-۱}{۲}} \overset{p}{\equiv} (-۱)^{\frac{p-۱}{۲}}$. بنابر قضیه فرما $b^{p-۱} \overset{p}{\equiv} ۱$. لذا $(-۱)^{\frac{p-۱}{۲}} \overset{p}{\equiv} ۱$. پس $p | (-۱)^{\frac{p-۱}{۲}} - ۱$. اگر $\frac{p-۱}{۲}$ فرد باشد آن‌گاه

داریم $p|۲$ و این غیر ممکن است، چون p یک عدد اول فرد است. پس $\frac{p-۱}{۲} = ۲k$ عددی زوج است. پس $p = ۴k+۱$. لذا $p \overset{۴}{\equiv} ۱$.

برعکس فرض کنیم $p \overset{۴}{\equiv} ۱$ بنابر قضیه‌ی ویلسون داریم

$$(p-۱)! = ۱ \times ۲ \times ۳ \times \cdots \times \frac{p-۱}{۲} \times \frac{p+۱}{۲} \times \cdots \times (p-۲)(p-۱) \overset{p}{\equiv} -۱$$

حال توجه می‌کنیم که

$$p-۱ \overset{p}{\equiv} -۱$$

$$p-۲ \overset{p}{\equiv} -۲$$

$$\vdots$$

$$\frac{p+۱}{۲} \overset{p}{\equiv} -\frac{p-۱}{۲}$$

بنابراین

$$(p-۱)! \overset{p}{\equiv} ۱ \times ۲ \times \cdots \times (\frac{p-۱}{۲}) \times (-\frac{p-۱}{۲}) \times \cdots \times (-۲)(-۱) \overset{p}{\equiv} -۱$$

پس $(-۱)^{\frac{p-۱}{۲}}(۱ \times ۲ \times \cdots \times \frac{p-۱}{۲})^۲ \overset{p}{\equiv} -۱$ از طرفی چون $p \overset{۴}{\equiv} ۱$ لذا $p = ۴k+۱$ برای یک عدد صحیح k. و لذا $\frac{p-۱}{۲} = ۲k$ عددی زوج است. پس $(-۱)^{\frac{p-۱}{۲}} = ۱$. پس

$$\left(\frac{p-۱}{۲}!\right)^۲ \overset{p}{\equiv} -۱$$

لذا $\frac{p-۱}{۲}!$ یک جواب هم‌نهشتی (۱) است. و اثبات تمام است. □

§۴.۴ تمرین

۱. نشان دهید برای هر عدد صحیح a، عدد $۲^{۲۳} - ۲^{۱۵}$ عدد $a^{۱۵} - a^{۳}$ را می‌شمارد.

۲. اگر m و n دو عدد طبیعی نسبت بهم اول باشند نشان دهید $m^{\varphi(n)} + n^{\varphi(m)} \overset{mn}{\equiv} ۱$.

۳. دو رقم سمت راست عدد $۳^{۲۵۶}$ را بیابید.

۴. باقیمانده $۲^{۱۰^{۱۰^{۱۰}}}$ را بر ۷۷ بیابید.

۵. سه عدد متوالی بیابید که هر یک به مربع یک عدد صحیح بزرگتر از ۱ قابل قسمت باشد.

۶. ثابت کنید اگر $a \not| ۷$ آنگاه $a^{۳} + ۱$ یا $a^{۳} - ۱$ بر ۷ بخش‌پذیر است.

۷. نشان دهید

(الف) $۳۹ | ۵۳^{۱۰۳} + ۱۰۳^{۵۳}$.

(ب) $۷ | ۱۱۱^{۳۳۳} + ۳۳۳^{۱۱۱}$.

۸. (الف)نشان دهید اگر n شبه اول باشد آنگاه $M_n = ۲^n - ۱$ نیز شبه اول است.

(ب)ثابت کنید بی‌نهایت عدد شبه اول وجود دارد.

۹. نشان دهید عکس قضیه‌ی ویلسون نیز برقرار است.

۱۰. نشان دهید اگر p عددی اول باشد آنگاه $\binom{n}{p} \overset{p}{\equiv} \left[\frac{n}{p}\right]$.

۱۱. کلیه‌ی جواب‌های هم‌نهشتی‌های زیر را به‌دست آورید

(الف) $۱۰۳x \overset{۹۹۹}{\equiv} ۴۴۴$.

(ب) $۹۸۰x \overset{۱۶۰۰}{\equiv} ۱۵۰۰$.

(ج) $۹۸۷x \overset{۱۵۹۷}{\equiv} ۶۱۰$.

۱۲. کوچک‌ترین عدد طبیعی n را بیابید که باقی‌مانده‌ی تقسیم آن بر ۱۱ و ۱۲ و ۱۳ و ۱۷ و ۱۹ به‌ترتیب ۲ و ۳ و ۴ و ۵ و ۶ باشد.

۱۳. اگر a و b و c اعداد صحیح باشند و $(a, b) = ۱$ آن‌گاه عدد صحیح n یافت می‌شود به‌نحوی که $(an + b, c) = ۱$.

۱۴. کلیه‌ی جواب‌های هم‌نهشتی $x^۲ + ۶x - ۳۱ \overset{۷۲}{\equiv} ۰$ را به‌دست آورید.

۱۵. کلیه‌ی جواب‌های هم‌نهشتی $x^۲ + ۱۸x - ۸۲۳ \overset{۱۸۰۰}{\equiv} ۰$ را به‌دست آورید.

۱۶. قضیه‌ی کوچک فرما را به کمک استقرأ ثابت کنید.

فصل ۵
مرتبه و ریشه‌های اولیه

فرض کنیم n عددی طبیعی و a عددی صحیح باشد و $(a,n)=۱$. یادآوری می‌کنیم که بنابر قضیه اویلر $a^{\varphi(n)} \overset{n}{\equiv} ۱$.(* خواننده آشنا با نظریه گروه‌ها می‌داند مجموعه اعداد نابیشتر از n که نسبت به n اولند، با ضرب به پیمانه n، یک گروه است. این گروه را با $\mathbb{Z}_n^\times$ نشان می‌دهیم. $\mathbb{Z}_n^\times$ گروهی از مرتبه $\varphi(n)$ است و قضیه اویلر در واقع همان قضیه لاگرانژ در این گروه است *).

معمولاً اعداد طبیعی k یافت می‌شوند به‌نحوی که $k<\varphi(n)$ و $a^k \overset{n}{\equiv} ۱$.

§۱.۵ مرتبه یک عدد و خواص آن

تعریف ۱.۵ فرض کنیم n یک عدد طبیعی و a یک عدد صحیح باشد و $(a,n)=۱$. مرتبه a به پیمانه n بنابه تعریف کوچکترین عدد طبیعی k است به نحوی که $a^k \overset{n}{\equiv} ۱$.

مرتبه a به پیمانه n را معمولاً با $o_n(a)$ یا $o(a,n)$ نشان می‌دهیم.

از قضیه اویلر نتیجه می‌شود که مرتبه a به پیمانه n وجود دارد و حداکثر برابر $\varphi(n)$ است.

توجه فرمایید که اگر a و n نسبت بهم اول نباشند آنگاه برای هر عدد طبیعی k، $a^k \overset{n}{\not\equiv} ۱$ و لذا مرتبه a به پیمانه n قابل تعریف نیست (ثابت کنید).

مثال ۲.۵ اگر $n = ۱۴$ آنگاه اعداد نسبت به n اول کمتر از n عبارتند از $۱, ۳, ۵, ۹, ۱۱, ۱۳$. یک محاسبه ساده نشان می‌دهد مرتبه این اعداد به پیمانه ۱۴ به ترتیب برابر $۱, ۶, ۶, ۳, ۳, ۲$ می‌باشد. اعداد ۳ و ۵ در مثال اخیر دارای مرتبه دقیقاً $\varphi(n) = ۶$ می‌باشند.

بنابر مثال اخیر اعداد ۳ و ۵ مولد گروه $\mathbb{Z}_{۱۴}^{\times}$ می‌باشند و لذا $\mathbb{Z}_{۱۴}^{\times}$ دوری است. به‌طور کلی این سؤال بجاست که به ازاء چه n هایی $\mathbb{Z}_n^{\times}$ گروهی دوری است.

تعریف ۳.۵ فرض کنیم n عددی طبیعی و a عددی صحیح باشد و $(a, n) = ۱$. بنابه تعریف گوییم a یک ریشه اولیه n است هرگاه مرتبه a به پیمانه n برابر $\varphi(n)$ باشد.

توجه کنیم که عدد طبیعی دلخواه ممکن است دارای ریشه اولیه نباشد. در ادمه این بخش ابتدا به خواص مرتبه می‌پردازیم و سپس نشان می‌دهیم هر عدد اول دارای ریشه اولیه است. در تمرینهای آخر بخش این واقعیت ثابت شده است که n دارای ریشه اولیه است اگر و تنها اگر n به یکی از صورت‌های

$$n = ۲, ۴, p^k, ۲p^k$$

که در آن p یک عدد اول فرد و k عددی طبیعی است باشد.

قضیه ۴.۵ فرض کنیم مرتبه a به پیمانه n برابر h باشد. در این صورت برای هر عدد طبیعی k، $a^k \overset{n}{\equiv} ۱$ اگر و تنها اگر $h|k$. به‌ویژه $h|\varphi(n)$.

اثبات. بنابرالگوریتم تقسیم $k = qh + r$ که در آن $q, r \in \mathbb{Z}$ و $۰ \leq r < h$. اگر $h|k$ آنگاه $r = ۰$ ودر نتیجه

$$a^k \overset{n}{\equiv} a^{qh} \overset{n}{\equiv} (a^h)^q \overset{n}{\equiv} ۱^q \overset{n}{\equiv} ۱$$

بالعکس فرض کنیم $a^k \overset{n}{\equiv} ۱$. در این صورت

$$۱ \overset{n}{\equiv} a^k \overset{n}{\equiv} a^{qh+r} \overset{n}{\equiv} (a^h)^q a^r \overset{n}{\equiv} a^r$$

چون $r < h$ و $a^r \overset{n}{\equiv} ۱$ لذا بنابر تعریف مرتبه، r نمی‌تواند عددی مثبت باشد. پس $r = ۰$ یعنی $k = qh$. در نتیجه $h|k$، به‌ویژه بنابر قضیه اویلر $a^{\varphi(n)} \overset{n}{\equiv} ۱$ لذا $h|\varphi(n)$. □

قضیه قبل در محاسبه مرتبه یک عدد بسیار مفید است. به عنوان مثال مرتبه هر عدد به پیمانه ۱۷ یکی از اعداد $۱۶, ۸, ۴, ۲, ۱$ است. مثلاً

$$۲^۱ \overset{۱۷}{\equiv} ۲, ۲^۲ \overset{۱۷}{\equiv} ۴, ۲^۴ \overset{۱۷}{\equiv} (-۱), ۲^۸ \overset{۱۷}{\equiv} (-۱)^۲ = ۱$$

لذا مرتبه ۲ به پیمانه ۱۷ برابر ۸ است. همچنین

$$۳^۱ \overset{۱۷}{\equiv} ۳, ۳^۲ \overset{۱۷}{\equiv} ۹, ۳^۴ \overset{۱۷}{\equiv} -۴, ۳^۸ \overset{۱۷}{\equiv} (-۴)^۲ \overset{۱۷}{\equiv} -۱$$

و لذا مرتبه ۳ به پیمانه ۱۷هیچیک از اعداد $۱, ۲, ۴, ۸$ نیست و لذا برابر ۱۶است. یعنی ۳ یک ریشه اولیه به پیمانه ۱۷است.

قضیه ۵.۵ فرض کنیم مرتبه a به پیمانه n برابر h باشد. در این صورت برای هر دوعدد طبیعی i, j داریم

$$a^i \overset{n}{\equiv} a^j \Longleftrightarrow i \overset{h}{\equiv} j$$

اثبات. فرض کنیم $i \geq j$. داریم

$$i \overset{h}{\equiv} j \Longleftrightarrow i - j = qh \Longleftrightarrow a^i = a^{qh+j} = \left(a^h\right)^q a^j \overset{n}{\equiv} a^j$$

□

نتیجه ۶.۵ اگر مرتبه a به پیمانه n برابر h باشد در این صورت اعداد $a, a^۲, \ldots, a^h$ به پیمانه n دوبدو ناهم‌نهشت اند. به‌ویژه اگر a یک ریشه اولیه n باشد آن‌گاه $\varphi(n)$ عدد $a, a^۲, \ldots, a^{\varphi(n)}$ یک دستگاه مخفف مانده‌ها به پیمانه n است.

مثال ۷.۵ مرتبه ۲ به پیمانه ۱۷ برابر ۸است. اعداد $۲, ۲^۲, \ldots, ۲^۸$ به پیمانه ۱۷ به ترتیب برابرند با $۱, ۲, ۴, ۸, ۱۶, ۱۵, ۱۳, ۹, ۱$. عدد ۳یک ریشه اولیه ۱۷ است. اعداد $۳, ۳^۲, \ldots, ۳^{۱۶}$ به پیمانه ۱۷ به ترتیب برابرند با $۱, ۳, ۹, ۱۰, ۱۳, ۵, ۱۵, ۱۱, ۱۶, ۱۴, ۸, ۷, ۴, ۱۲, ۲, ۶, ۱$.

قضیه ۸.۵ فرض کنیم n عددی طبیعی و a عددی صحیح باشد و $(a,n)=۱$. برای هر عدد طبیعی k داریم

$$o_n\left(a^k\right)=\frac{o_n(a)}{(k,o_n(a))}$$

اثبات. فرض کنیم $o_n(a)=h$ و $(k,h)=d$. در این صورت $h=h_۱d$ و $k=k_۱d$ و $(h_۱,k_۱)=۱$. فرض کنیم $o_n(a^k)=r$، باید نشان دهیم $r=h_۱$. داریم

$$(a^k)^{h_۱}=\left(a^{k_۱d}\right)^{h_۱}=\left(a^{h_۱d}\right)^{k_۱}=\left(a^h\right)^{k_۱}\overset{n}{\equiv}۱^{k_۱}=۱$$

لذا با عنایت به تعریف r و قضیه ۴ داریم $r|h_۱$. از طرف دیگر با توجه به تعریف r داریم

$$a^{kr}=\left(a^k\right)^r\overset{n}{\equiv}۱$$

لذا بنابر قضیه ۴ داریم $h|kr$. یعنی $h_۱d|k_۱dr$ ودر نتیجه $h_۱|k_۱r$. حال از $(h_۱,k_۱)=۱$ نتیجه می‌شود که $h_۱|r$. این بهمراه رابطهٔ $r|h_۱$ حکم را نتیجه می‌دهد. □

نتیجه ۹.۵ (الف) فرض کنیم n عددی طبیعی و a صحیح باشد و $(a,n)=۱$. در این صورت برای هر عدد طبیعی k،

$$o_n\left(a^k\right)=o_n(a)\Longleftrightarrow(k,o_n(a))=۱$$

(ب) اگر a یک ریشه اولیه n باشد آنگاه برای هر عدد صحیح k، عدد a^k یک ریشه اولیه n است اگر و تنها اگر $(k,\varphi(n))=۱$

(ج) اگر n دارای ریشه اولیه باشد آنگاه به پیمانه n دارای $\varphi(\varphi(n))$ ریشه اولیه متمایز به پیمانه n است.

اثبات. (الف) و (ب) نتیجه مستقیم قضیه قبل هستند.

(ج)از (ب) با توجه به‌نتیجه ۶، نتیجه می‌شود. □

§۲.۵ وجود ریشه‌ی اولیه

تا این‌جا خواصی از ریشه‌های اولیه را بررسی کردیم. ولی وجود ریشه اولیه برای عدد داده شده n را ثابت نکرده‌ایم. بعضی از اعداد ریشه اولیه ندارند. به عنوان مثال بسادگی می‌توانید تحقیق کنید که عدد ۱۵ ریشه اولیه ندارد. در واقع داریم:

قضیه ۱۰.۵ فرض کنیم n یک عدد طبیعی باشد. اگر n به یکی از صورت‌های

$$n = ۲, ۴, p^k, ۲p^k \qquad (k \text{ عددی طبیعی و } p \text{ عددی اول و فرد})$$

نباشد آن‌گاه n ریشه اولیه ندارد.

اثبات. اگر n به هیچیک از صورت‌های فوق نباشد آن‌گاه یکی از سه حالت زیر اتفاق می‌افتد:

(الف) $n = ۲^\alpha$ برای یک $\alpha \geq ۳$،

(ب) n بر حداقل دو عدد اول فرد بخش‌پذیر است،

(ج) $n = ۲^\alpha p^\beta$ که در آن $\alpha \geq ۲$ و β عددی طبیعی و p عددی اول و فرد است.

حالت (الف): بااستقرا روی α براحتی ثابت می‌شود که اگر $\alpha \geq ۳$ و $(a, ۲^\alpha) = ۱$ آن‌گاه

$$a^{۲^{\alpha-۲}} \overset{۲^\alpha}{\equiv\equiv} ۱$$

(ثابت کنید). درنتیجه

$$o_n(a) \leq ۲^{\alpha-۲} < ۲^{\alpha-۱} = \varphi(n)$$

لذا a ریشه اولیه n نیست.

حالت‌های (ب) و (ج) :در این دو حالت می‌توان n را به صورت $n = n_۱n_۲$ نوشت که در آن $(n_۱, n_۲) = ۱$ و $n_۱ > ۲$ و $n_۲ > ۲$. اگر $(a, n) = ۱$ آن‌گاه داریم $(a, n_۱) = (a, n_۲) = ۱$ و لذا بنابر قضیه اویلر داریم:

$$a^{\frac{\varphi(n_1)\varphi(n_2)}{2}} = (a^{\varphi(n_1)})^{\frac{\varphi(n_2)}{2}} \overset{n_1}{\equiv} 1$$
$$a^{\frac{\varphi(n_1)\varphi(n_2)}{2}} = (a^{\varphi(n_2)})^{\frac{\varphi(n_1)}{2}} \overset{n_2}{\equiv} 1$$

در نتیجه چون $(n_1, n_2) = 1$ و $n = n_1 n_2$ لذا $a^{\frac{\varphi(n_1)\varphi(n_2)}{2}} \overset{n}{\equiv} 1$ (توجه کنیم که $\frac{\varphi(n_1)}{2}$ و $\frac{\varphi(n_2)}{2}$ اعدادی صحیح اند). پس

$$o_n(a) \leq \frac{\varphi(n_1)\varphi(n_2)}{2} < \varphi(n_1)\varphi(n_2) = \varphi(n)$$

و لذا a یک ریشه اولیه n نیست. □

عکس قضیه بالا نیز درست است. برای اثبات ابتدا ثابت می‌کنیم هر عدد اول دارای ریشه اولیه است. برای این کار به اثبات چند گزاره نیاز داریم.

قضیه ۱۱.۵ (قضیه لاگرانژ). فرض کنیم p عددی اول باشد. چندجمله‌ای درجه $n \geq 1$،

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n \quad , \quad p \nmid a_n$$

را که در آن ضرایب اعداد صحیح اند در نظر می‌گیریم. در این صورت هم‌نهشتی

$$f(x) \overset{p}{\equiv} 0 \tag{۱.۵}$$

حداکثر n جواب نا هم‌نهشت به پیمانه p دارد.

اثبات. با استقرا روی n ثابت می‌کنیم. اگر $n = 1$ آنگاه هم‌نهشتی $f(x) \overset{p}{\equiv} 0$ به شکل $a_1 x \overset{p}{\equiv} -a_0$ در می‌آید. چون $(a_1, p) = 1$، این معادله یک جواب منحصر بفرد به پیمانه p دارد. فرض کنیم حکم برای هر چندجمله‌ای از درجه $n-1$ درست باشد.

حکم را برای چندجمله‌ای $f(x)$ که از درجه n است ثابت می‌کنیم. اگر معادله هم‌نهشتی (۱) جواب نداشته باشد حکم برقرار است. در غیر این صورت فرض کنیم a یک جواب هم‌نهشتی (۱) باشد. بنابر الگوریتم تقسیم در چندجمله‌ای‌ها، داریم

$$f(x) = (x-a)q(x) + r$$

که در آن $q(x)$ یک چندجمله‌ای با ضرایب صحیح و از درجه $n-۱$ است و r یک عدد صحیح می‌باشد داریم:

$$۰ \overset{p}{\equiv} f(a) = (a-a)q(a) + r = r$$

لذا $f(x) \overset{p}{\equiv} (x-a)q(x)$. حال فرض کنیم b یک جواب (۱) و ناهم‌نهشت با a باشد. در این صورت $f(b) \overset{p}{\equiv} (b-a)q(b) \overset{p}{\equiv} ۰$. و لذا b یک جواب هم نهشتی $q(x) \overset{p}{\equiv} ۰$ می‌باشد. چون این هم‌نهشتی بنابر فرض استقرا حداکثر دارای $n-۱$ جواب ناهم‌نهشت است لذا برای b حداکثر $n-۱$ گزینه میسر است. لذا هم‌نهشتی (۱) حداکثر n جواب ناهم‌نهشت دارد. □

نتیجه ۱۲.۵ فرض کنیم p عددی اول باشد و $d|p-۱$. در این صورت هم‌نهشتی $x^d - ۱ \overset{p}{\equiv} ۰$ دقیقاً d جواب نا هم‌نهشت دارد.

اثبات. داریم $p-۱ = kd$. لذا با قرار دادن $x^d = y$ و اتحاد

$$y^k - ۱ = (y-۱)(y^{k-۱} + y^{k-۲} + \cdots + ۱)$$

$$x^{p-۱} - ۱ = (x^d - ۱)f(x) \qquad (۲.۵)$$

که در آن $f(x)$ یک چندجمله‌ای از درجه $d(k-۱) = p-۱-d$ است. بنابر قضیه کوچک فرما هم نهشتی $x^{p-۱} - ۱ \overset{p}{\equiv} ۰$ دقیقاً $p-۱$ جواب ناهم‌نهشت دارد. بنابر (۱) هر یک از این جواب‌ها حداقل جواب یکی از هم‌نهشتی های $x^d - ۱ \overset{p}{\equiv} ۰$ یا $f(x) \overset{p}{\equiv} ۰$ می‌باشد. چون $f(x) \overset{p}{\equiv} ۰$ حداکثر $p-۱-d$ جواب ناهم‌نهشت دارد پس هم‌نهشتی $x^d - ۱ \overset{p}{\equiv} ۰$ حداقل $p-۱-(p-۱-d) = d$ جواب نا هم‌نهشت دارد. از طرفی بنابر قضیه لاگرانژ این هم‌نهشتی حداکثر d جواب دارد. لذا حکم برقرار است. □

وجود ریشه اولیه برای هر عدد اول p نتیجه قضیه زیر است:

قضیه ۱۳.۵ فرض کنیم p یک عدد اول باشد و $d|p-۱$. در این صورت دقیقاً $\varphi(d)$ عدد ناهم‌نهشت به پیمانه p وجود دارد که دارای مرتبه d به پیمانه‌ی p هستند.

اثبات. برای هر مقسوم d از $p-۱$ فرض کنیم

$$s_d = \{k : ۱ \leq k \leq p-۱, o_p(k) = d\}$$

بدیهی است که s_d ها مجزا هستند و $\cup_{d|p-۱} s_d = \{۱, ۲, \ldots, p-۱\}$. لذا

$$\sum_{d|p-۱} |s_d| = p-۱$$

حکم قضیه این است که $|s_d| = \varphi(d)$. بنابر قضیه گاوس داریم

$$\sum_{d|p-۱} \varphi(d) = p-۱$$

پس

$$\sum_{d|p-۱} |s_d| = \sum_{d|p-۱} \varphi(d)$$

چون $|s_d|$ ها و $\varphi(d)$ ها اعدادی مثبتند لذا اگر نشان دهیم که برای هر d، $|s_d| \leq \varphi(d)$ آن‌گاه نتیجه می‌شود که $|s_d| = \varphi(d)$ برای هر d، و اثبات تمام می‌شود. بنابراین نشان می‌دهیم برای هر d داریم $|s_d| \leq \varphi(d)$

فرض کنیم $d|p-۱$. اگر $|s_d| = ۰$، به‌طور بدیهی $|s_d| \leq \varphi(d)$. فرض کنیم $|s_d| \neq ۰$. لذا عدد صحیح a از مرتبه d به پیمانه p وجود دارد. بنابر نتیجه ۱۷اعداد $a, a^۲, \ldots, a^d$ دوبدو ناهم‌نهشت و لذا بنابر قضیه لاگرانژ این اعداد کلیه جواب‌های هم‌نهشتی $x^d - ۱ \overset{p}{\equiv} ۰$ هستند. هر عضو s_d یک جواب هم‌نهشتی $x^d - ۱ \overset{p}{\equiv} ۰$ و لذاهم‌نهشت یکی از اعداد $a, a^۲, \ldots, a^p$ می‌باشد. لذا بنابر نتیجه ۹ (ب) مجموعه s_d دارای دقیقاً $\varphi(n)$ عضواست و اثبات تمام است. □

قضیه ۱۴.۵ اگر p یک عدد اول باشد آن‌گاه p دارای $\varphi(p-۱)$ ریشه اولیه است.

اثبات. در قضیه قبل قرار دهید $d = p-۱$. □

به کمک قضیه ۲۴ می‌توان بررسی وجود ریشه اولیه را کامل کرد:

قضیه ۱۵.۵ عدد $n > ۱$ دارای ریشه‌اولیه است اگر وتنها اگر n به یکی از صورت‌های

$$n = ۲, ۴, p^k, ۲p^k$$

که در آن k عددی طبیعی و p عددی اول و فرد است، باشد.

خلاصه اثبات: قبلاً ثابت کردیم اگر n به یکی از صورت های فوق نباشد ریشه اولیه ندارد.

فرض کنیم n به یکی از صورت های داده شده باشد. نشان می‌دهیم n دارای ریشه اولیه است.

در حالت های $n = ۲, ۴$ کار ساده است زیرا ۳ ریشه اولیّه ۴، و ۱ریشه اولیه۲ است.

حالت $n = p$ همان قضیه قبل است.

حالت $n = p^۲$ (p **اول و فرد**):

فرض کنیم a یک ریشه اولیّه p باشد. اگر a یک ریشه اولیه$p^۲$ نیز باشد حکم در این حالت برقرار است. فرض کنیم a یک ریشه اولیه $p^۲$ نباشد. در این صورت نشان می‌دهیم $a' = a + p$ یک ریشه اولیه $p^۲$ است. فرض کنیم مرتبه a' به پیمانه $p^۲$ برابر h باشد. لذا $a'^h \overset{p^۲}{\equiv} ۱$ و لذا $a'^h \overset{p}{\equiv} ۱$. چون $o_p(a') = o_p(a) = p - ۱$ لذا $p - ۱ | h$. از طرف دیگر داریم:

$$(a')^{p-۱} \overset{p^۲}{\equiv} (a+p)^{p-۱} \overset{p^۲}{\equiv} a^{p-۱} + (p-۱)pa^{p-۲}$$

چون a بنا به فرض یک ریشه اولیه $p^۲$ نیست لذا $o_{p^۲}(a) = p - ۱$ (چرا؟) در نتیجه

$$(a')^{p-۱} \overset{p^۲}{\equiv} ۱ + (p-۱)pa^{p-۲} \overset{p^۲}{\not\equiv} ۱$$

زیرا $p \not| a$. پس $h \neq p - ۱$. داریم $h | \varphi(p^۲) = p(p-۱)$ و $p - ۱ | h$ و $p - ۱ \neq h$. لذا $h = p(p-۱) = \varphi(p^۲)$ (چگونه). یعنی a' یک ریشه‌ی اولیّه $p^۲$ است.

حالت $n = p^k$ ($k \geq ۲$ **و** p **اول فرد**)

بنابر حالت قبل فرض کنیم a یک ریشه‌ی اولیّه $p^۲$ باشد. با استقراء روی k ثابت کنید a یک ریشه اولیّه p^k برای هر k می‌باشد.

حالت $n = ۲p^k$ (p اول فرد و $k \geq ۱$)

بنابر حالت قبل p^k ریشه اولیّه‌ای چون a دارد. می‌توان فرض کرد a فرد است (در غیراین‌صورت به‌جای a عدد $a + p^k$ قرار دهید که فرد است) نشان دهید a ریشه اولیّه $۲p^k$ است. □

در اثبات حالت $n = p^k$ در قضیه قبل مشاهده می‌شود که اگر a ریشه اولیّه $p^۲$ باشد آن‌گاه a ریشه اولیّه p^k برای هر $k \geq ۲$ نیز هست. بدلیل کاربردهای این مطلب آن را بصورت یک گزاره یادداشت می‌کنیم:

گزاره ۱۶.۵ اگر p یک عدد اول فرد و a یک ریشه اولیّه $p^۲$ باشد آن‌گاه a ریشه اولیّه p^k برای هر $k \geq ۲$ می‌باشد.

مثال ۱۷.۵ ۲ریشه اولیّه ۳^k و ۵^k برای هر k است.

حل: با محاسبه‌ای ساده داریم $o_۹(۲) = ۶ = \varphi(۹)$. یعنی ۲ یک ریشه اولیّه $۳^۲ = ۹$ است. از گزاره‌ی قبل نتیجه می‌شود که ۲ یک ریشه‌ی اولیه ۳^k (برای هر k) می‌باشد. همچنین به‌راحتی دیده می‌شود که $o_{۲۵}(۲) = ۲۰$ و لذا ۲ ریشه‌ی اولیه ۲۵ و درنتیجه ریشه‌ی اولیه ۵^k (برای هر k) می‌باشد.

§۳.۵ تمرین

۱. نشان دهید اگر $F_n = ۲^{۲^n} + ۱$ اول باشد و $n > ۱$، آن‌گاه ۲ریشه اولیّه F_n نیست.

۲. نشان دهید برای هر $n > ۱$، $n|\varphi(۲^n - ۱)$

۳. اگر مرتبه a به پیمانه عدد اول p برابر ۳باشد ثابت کنید مرتبه $a + ۱$ برابر ۶است.

۴. نشان دهید هر مقسوم علیه فرد اوّل عدد $n^۲ + ۱$ (n دلخواه) به شکل $۴k + ۱$ است و هر مقسوم علیه فرد اوّل عدد $n^۴ + ۱$ بشکل $۸k + ۱$ است.

۵. با استفاده از تمرین ۴ نشان دهید بینهایت عدد اوّل به شکل $۴k + ۱$ وجود دارد.
(راهنمایی: فرض کنید $p_۱, p_۲, \ldots, p_r$ همه اعداد اول بدین شکل باشند حال عدد $(۲p_۱p_۲ \ldots p_r)^۲ + ۱$ را در نظر بگیرید.)

۶. الف) فرض کنیم p و q دو عدد اوّل فرد باشند و $q|a^p - ۱$. ثابت کنید $q|a - ۱$ و یا $q = ۲kp + ۱$.
ب) اگر p عددی اوّل و فرد باشد نشان دهید مقسوم علیه‌های اول $۲^p - ۱$ به شکل $۲kp + ۱$ می‌باشند.
ج) کوچکترین مقسوم علیه (غیر از ۱) اعداد $۲^{۱۷} - ۱$ و $۲^{۲۹} - ۱$ را بیابید.

۷. با استفاده از اینکه عدد ۳یک ریشه اولیّه ۱۷ است، کلیّه ریشه‌های اولیّه ناهم‌نهشت ۱۷را بیابید.

۸. نشان دهید قضیّه لاگرانژ در حالتی که p عددی اوّل نباشد ممکن است برقرار نباشد.

۹. با استفاده از اینکه p دارای ریشه اولیّه است، قضیّه ویلسون را ثابت کنید.

۱۰. اگر a, a' دو ریشه اولیّه p باشند ثابت کنید $a^{\frac{p-۱}{۲}} \overset{p}{\equiv} -۱$ و ثابت کنید aa' ریشه اولیّه p نیست.

۱۱. همه ریشه‌های اولیّه ۲۶و۲۵ را بیابید.

۱۲. یک ریشه اولیّه برای ۱۷^k (k دلخواه) بیابید.

فصل ۶
هم‌نهشتی‌های درجه دوم و قانون تقابل مربعی

§۱.۶ معادلات هم‌نهشتی

فرض کنیم $f(x)$ یک چندجمله‌ای با ضرایب صحیح باشد. تاکنون تجربیات زیادی برای بدست آوردن جواب‌های معادله $f(x) = ۰$ در دبیرستان، ریاضی عمومی و آنالیز بدست آورده اید. با وجود این، در صورتی که $f(x)$ یک چندجمله‌ای از درجه بیش از دو باشد، بدست آوردن جواب‌ها در حالت کلی اصلاً آسان نیست. حتی گاهی تعیین وجود یا عدم وجود جواب، و تعداد جواب‌ها کاری دشوار است.

در نظریه اعداد یک معادله به صورت $f(x) = ۰$، که در آن $f(x)$ یک چندجمله‌ای با ضرایب صحیح است، را یک **معادله‌ی دیوفانتی** (دیوفانتوس نام دانشمند یونانی است که در قرن سوّم میلادی می‌زیسته است) گوییم. منظور از حل یک معادله‌ی دیوفانتی بدست آوردن اعداد صحیح (و گاهی گویا) است که در معادله صدق می‌کند. تعیین وجود یا عدم وجود جواب و بدست آوردن جواب‌ها در یک معادله‌ی دیوفانتی کاری دشوار است. اگر عدد صحیح a یک جواب معادله باشد آن‌گاه $f(a) = ۰$ و در نتیجه برای هر عدد طبیعی n داریم

$$f(a) \overset{n}{\equiv} ۰$$

لذا اگر بتوان عدد طبیعی n را یافت به نحوی که هم‌نهشتی $f(a) \overset{n}{\equiv} ۰$ برای هیچ عدد صحیح a

برقرار نباشد آن‌گاه می‌توان نتیجه گرفت که معادله $f(x) = ۰$ جواب صحیح ندارد. بنابراین هم‌نهشتی ها می‌توانند به حل معادلات کمک کنند. این موضوع مارا به تعریف معادلات هم‌نهشتی رهنمون می‌سازد.

تعریف ۱.۶ یک **معادله هم‌نهشتی** یک معادله به‌صورت

$$f(x) \overset{n}{\equiv} ۰ \tag{۱.۶}$$

می‌باشد که در آن n عددی طبیعی و $f(x)$ یک چندجمله‌ای با ضرایب صحیح است.

عدد صحیح a رایک جواب معادله (۱) گوییم هرگاه هم‌نهشتی $f(a) \overset{n}{\equiv} ۰$ برقرار باشد.
لم زیر به کمک خواص هم‌نهشتی براحتی قابل اثبات است:

لم ۲.۶ فرض کنیم $f(x)$ یک چندجمله‌ای با ضرایب صحیح باشد:

(الف) اگر a و b دو عدد صحیح باشند و $a \overset{n}{\equiv} b$ آن‌گاه $f(a) \overset{n}{\equiv} f(b)$.

(ب) اگر a و b دو عدد صحیح باشند و $a \overset{n}{\equiv} b$ آن‌گاه،a یک جواب (۱) است اگر و تنها اگر b یک جواب (۱) باشد.

(پ) اگر هیچیک از اعداد $\{۰, ۱, ۲, \ldots, n-۱\}$ در (۱) صدق نکند آن‌گاه (۱) جواب ندارد.

اثبات. تمرین. □

با توجه به لم فوق مشاهده می‌شود که بدست آوردن جواب‌های (۱) با محاسبه n مقدار $f(۰)$، $f(۱)$،...، $f(n-۱)$ میسر است. در حالیکه بدست آوردن جواب‌های صحیح $f(x) = ۰$ با تعدادی متناهی آزمون قابل انجام نیست.

مثال ۳.۶ (الف) معادله $x^۴ - ۱۳x^۲ + ۲۵ = ۰$ جواب ندارد. چون هم‌نهشتی $x^۴ - ۱۳x^۲ + ۲۵ \overset{۳}{\equiv} ۰$ دارای جواب نیست. (کافی است۰ و۱ و۲ را امتحان کنید).

(ب) معادله $۷x^۵ + ۲۱x^۳ - ۱۴x + ۵ = ۰$ جواب ندارد. چون $۷x^۵ + ۲۱x^۳ - ۱۴x + ۵ \overset{۷}{\equiv} ۰$ جواب ندارد. زیرا برای هر عددصحیح a، $۷a^۵ + ۲۱a^۳ - ۱۴a + ۵ \overset{۷}{\equiv} ۵$

تبصره ۴.۶ دیدیم اگر $f(x) = ۰$ دارای جواب باشد آن‌گاه $f(x) \overset{n}{\equiv} ۰$ برای هر n دارای جواب است. عکس این مطلب درست نیست. ممکن است معادله هم‌نهشتی $f(x) \overset{n}{\equiv} ۰$ برای هر n دارای جواب باشد ومعادله $f(x) = ۰$ جواب نداشته باشد. بعنوان مثال فرض کنیم $f(x) = (x^۲-۳)(x^۲-۵)(x^۲-۱۵)$. در این صورت برای هر عدد طبیعی n هم‌نهشتی $f(x) \overset{n}{\equiv} ۰$ دارای جواب است (تمرین آخر فصل)، ولی به‌راحتی دیده می‌شود که $f(x) = ۰$ جواب صحیح ندارد.

قضیه‌ای نسبتاً عمیق که اثباتش از حوصله این درس بیرون است بیان می‌دارد که اگر $f(x)$ یک چندجمله‌ای درجه ۲ باشد و$f(x) \overset{n}{\equiv} ۰$ برای هر n دارای جواب باشد آن‌گاه $f(x) = ۰$ جواب دارد (این قضیه به اصل هسه-مینکوفسکی معروف است) پس از این مقدمه به موضوع این فصل که هم‌نهشتی های درجه دوم است بر می‌گردیم:

منظور از یک هم‌نهشتی درجه دوم یک معادله هم‌نهشتی به صورت

$$f(x) \overset{n}{\equiv} ۰$$

است که در آن $f(x)$ یک چندجمله‌ای با ضرایب صحیح و از درجه ۲ است در ابتدا پیمانه را عدد اوّل فردی چون p فرض می‌کنیم وپس از آن رسیدگی به مسأله در حالتی‌که پیمانه، یک عدد طبیعی دلخواه است نسبتاً راحت است. لذا هم‌نهشتی زیر را در نظر می‌گیریم

$$f(x) = ax^۲ + bx + c \overset{p}{\equiv} ۰ \quad (p \nmid a) \tag{۲.۶}$$

که در آن p عددی اوّل و فرد است. برای رسیدگی به این هم‌نهشتی اجازه دهید به روشی که قبلاً برای حل معادله‌ی

$$ax^۲ + bx + c = ۰ \quad (a > ۰)$$

یاد گرفته‌ایم نگاه کنیم. برای این کار از روش مربع کامل کردن عبارت استفاده کردیم.

$$۰ = ax^۲ + bx + c = a\left(x^۲ + ۲\frac{b}{۲a}x + \frac{c}{a}\right) = a\left(\left(x + \frac{b}{۲a}\right)^۲ - \frac{b^۲}{۴a^۲} + \frac{c}{a}\right)$$

لذا

$$\left(x+\frac{b}{۲a}\right)^۲=\frac{b^۲}{۴a^۲}-\frac{c}{a}=\frac{b^۲-۴ac}{۴a^۲}$$

پس

$$x+\frac{b}{۲a}=\frac{\pm\sqrt{b^۲-۴ac}}{۲a}$$

در نتیجه

$$x=\frac{-b\pm\sqrt{b^۲-۴ac}}{۲a}$$

اگر $b^۲-۴ac=۰$ معادله جواب منحصربه‌فرد $\frac{-b}{۲a}$ را دارد. اگر $b^۲-۴ax\neq ۰$ آن‌گاه معادله دو جواب متمایز دارد که حقیقی هستند اگر و تنها اگر $b^۲-۴ac>۰$ و گویا هستند اگر و تنها اگر $b^۲-۴ac$ مربع یک عدد صحیح باشد (در حالتی که a و b و c صحیح اند).

شبیه این کار را برای معادله (۲) به کار می‌بریم.

چون $(a,p)=۱$ پس a دارای وارون حسابی a' به پیمانه p است و چون p فرد است پس $(۲,p)=۱$.

فرض کنیم $۲'$ وارون حسابی ۲به پیمانه p باشد.

$$\begin{aligned}f(x)&=ax^۲+bx+c\overset{p}{\equiv}ax^۲+۲\times ۲'aa'bx+aa'c\\&=a\left(x^۲+۲\left(۲'a'b\right)x+a'c\right)\\&=a\left(\left(x+۲'a'b\right)^۲-\left(۲'a'b\right)^۲+a'c\right)\end{aligned}$$

چون $(a,p)=۱$ لذا $p|f(x)$ اگر و تنها اگر

$$p\left|\left(x+۲'a'b\right)^۲-\left(۲'a'b\right)^۲+a'c\right.$$

لذا $f(x)\overset{p}{\equiv}۰$ اگر و تنها اگر

$$\left(x+۲'a'b\right)^۲\overset{p}{\equiv}\left(۲'a'b\right)^۲-a'c$$

با فرض

$$\left(۲'a'b\right)^۲-a'c=d\ \ ,\ \ x+۲'a'b=y$$

معادله‌ی فوق بصورت زیر خواهد بود:

$$y^۲ \overset{p}{\equiv} d$$

بنابراین باید y را چنان بیابیم که مربع آن به پیمانه p برابر d گردد.

§۲.۶ مانده‌های مربعی و علامت لژاندر

تعریف ۵.۶ فرض کنیم p یک عدد اوّل فرد و a عددی صحیح باشد و $(a,p) = ۱$. گوییم a یک مانده مربعی p است اگر هم‌نهشتی $x^۲ \overset{p}{\equiv} a$ دارای جواب باشد. در غیر این صورت گوییم a یک نامانده مربعی p است.

مثال ۶.۶ ۳ یک مانده مربعی ۱۱است زیرا$۳۱ \overset{۱۱}{\equiv} ۵^۲$ ولی ۶ یک نامانده مربعی ۱۱است. زیرا معادله هم‌نهشتی $x^۲ \overset{۱۱}{\equiv} ۶$ جواب ندارد.(بر اساس لم ابتدای فصل کافی است اعداد $۰, ۱, ۲, \ldots, ۱۰$ را امتحان کنید). داریم

$$۱^۲ \overset{۱۱}{\equiv} ۱۰^۲ \overset{۱۱}{\equiv} ۱$$

$$۲^۲ \overset{۱۱}{\equiv} ۹^۲ \overset{۱۱}{\equiv} ۴$$

$$۳^۲ \overset{۱۱}{\equiv} ۸^۲ \overset{۱۱}{\equiv} ۹$$

$$۴^۲ \overset{۱۱}{\equiv} ۷^۲ \overset{۱۱}{\equiv} ۵$$

$$۵^۲ \overset{۱۱}{\equiv} ۶^۲ \overset{۱۱}{\equiv} ۳$$

لذا اعداد ۱، ۴، ۹، ۵، ۳ مانده مربعی ۱۱و اعداد ۲، ۶، ۷، ۸ و ۱۰ نامانده مربعی ۱۱ هستند.

در مثال بالا دیدیم از بین اعداد $۱, ۲, ۳, \ldots, ۱۰$ نیمی، مانده‌ی مربعی p و نیمی، نامانده هستند. در واقع این همیشه درست است.

لم ۷.۶ فرض کنیم p یک عدد اول فرد باشد، آن‌گاه از اعداد $۱, ۲, \ldots, p-۱$ نیمی، مانده‌ی مربعی p و نیمی، نامانده‌ی مربعی p می‌باشند.

اثبات. فرض کنیم a یک مانده‌ی مربعی p باشد، در این صورت عدد صحیح $b_۱$ وجود دارد به‌نحوی که $a \overset{p}{\equiv} b_۱^۲$. فرض کنیم b باقیمانده‌ی تقسیم $b_۱$ بر p باشد. در این صورت $b \overset{p}{\equiv} b_۱$ لذا $b^۲ \overset{p}{\equiv} b_۱^۲ \overset{p}{\equiv} a$ و $۱ \leq b \leq p-۱$. همچنین $(p-b)^۲ \overset{p}{\equiv} b^۲ \overset{p}{\equiv} a$ و $۱ \leq p-b \leq p-۱$. از دو عدد b و $p-b$ دقیقاً یکی ازآن‌ها در مجموعه‌ی $\{۱, ۲, \ldots, \frac{p-۱}{۲}\}$ قرار دارد. پس a به پیمانه‌ی p برابر یکی از اعداد $۱^۲, ۲^۲, \ldots, (\frac{p-۱}{۲})^۲$ می‌باشد. پس مانده‌های مربعی p عبارتند از

$$۱^۲, ۲^۲, \ldots, \left(\frac{p-۱}{۲}\right)^۲$$

از طرفی این اعداد دو به دو به پیمانه‌ی p ناهم‌نهشتند، زیرا اگر $۱ \leq i < j \leq \frac{p-۱}{۲}$ و $i^۲ \overset{p}{\equiv} j^۲ \overset{p}{\equiv} c$ آن‌گاه $(p-i)^۲ \overset{p}{\equiv} (p-j)^۲ \overset{p}{\equiv} c$ و داریم

$$۱ \leq i < j < p-j < p-i \leq p-۱$$

لذا اعداد i، j، $p-j$ و $p-i$ چهار جواب ناهم‌نهشت برای معادله‌ی هم‌نهشتی $x^۲ - c \overset{p}{\equiv} ۰$ می‌باشند. اما بنابر قضیه‌ی لاگرانژ معادله‌ی $x^۲ - c \overset{p}{\equiv} ۰$ حداکثر دو جواب ناهم‌نهشت دارد. لذا فرض خلف درست نیست.

پس اعداد $۱^۲, ۲^۲, \ldots, \left(\frac{p-۱}{۲}\right)^۲$ (به پیمانه‌ی p) کلیه‌ی مانده‌های مربعی p و متمایز (به پیمانه‌ی p) هستند. پس تعداد مانده‌های مربعی p، به پیمانه‌ی p برابر است با $\frac{p-۱}{۲}$. □

مثال ۸.۶ مانده‌های مربعی ۱۷ عبارتند از $۱^۲, ۲^۲, ۳^۲, ۴^۲, ۵^۲, ۶^۲, ۷^۲, ۸^۲$ که اعداد $۱, ۴, ۹, ۱۶, ۸, ۲, ۱۵, ۱۳$ می‌باشند.

تعریف ۹.۶ فرض کنیم p یک عدد اول فرد و a عددی صحیح باشد و $(a,p) = ۱$. تعریف می‌کنیم

$$\left(\frac{a}{p}\right) = \begin{cases} ۱ & \text{اگر } a \text{ مانده‌ی مربعی } p \text{ است.} \\ -۱ & \text{اگر } a \text{ مانده‌ی مربعی } p \text{ نیست.} \end{cases}$$

$\left(\frac{a}{p}\right)$ را **علامت لژاندر** a **به پیمانه‌ی** p گوییم.

تبصره ۱۰.۶ هر معادله‌ی هم‌نهشتی درجه‌ی دوم به پیمانه‌ی p را توانستیم به شکل $x^۲ \overset{p}{\equiv} a$ تبدیل کنیم و دیدیم برای اینکه ببینیم آیا این معادله جواب دارد یا خیر کافی است اعداد $۱^۲, ۲^۲, \ldots, (\frac{p-۱}{۲})^۲$ را به پیمانه‌ی p محاسبه نماییم. با وجود این‌که اگر p عدد بزرگی باشد، این تعداد محاسبه کاری وقت‌گیر وغیرعملی (ناکارآمد) در زمان مناسب است. در ادامه‌ی این فصل روشی کارآمد برای تعیین اینکه چه وقت a مانده‌ی مربعی p است (یعنی برای تعیین علامت لژاندر) ارائه می‌نماییم. نتیجه‌ی نهایی که این روش کارآمد را ارائه می‌نماید در قانون تقابل مربعی خلاصه شده است.

محک زیر خواص زیادی از علامت لژاندر را نتیجه می‌دهد:

قضیه ۱۱.۶ (محک اویلر). فرض کنیم p یک عدد اول فرد و a عددی صحیح باشد و $(a,p) = ۱$، در این صورت

$$\left(\frac{a}{p}\right) = \begin{cases} ۱ & a^{\frac{p-۱}{۲}} \overset{p}{\equiv} ۱ \\ -۱ & a^{\frac{p-۱}{۲}} \overset{p}{\equiv} -۱ \end{cases}$$

اثبات. ابتدا توجه کنیم که بنابر قضیه‌ی کوچک فرما $a^{p-۱} \overset{p}{\equiv} ۱$ لذا

$$p \,\big|\, (a^{p-۱} - ۱) = \left(a^{\frac{p-۱}{۲}} - ۱\right)\left(a^{\frac{p-۱}{۲}} + ۱\right)$$

و چون p عددی اول است لذا $p | a^{\frac{p-۱}{۲}} - ۱$ یا $p | a^{\frac{p-۱}{۲}} + ۱$ (و نه هر دو، چرا؟) پس $a^{\frac{p-۱}{۲}} \overset{p}{\equiv} ۱$ یا $a^{\frac{p-۱}{۲}} \overset{p}{\equiv} -۱$. فرض کنیم $\left(\frac{a}{p}\right) = ۱$. پس a یک مانده مربعی p است. پس عدد صحیح b وجود دارد به‌نحوی که $b^۲ \overset{p}{\equiv} a$. داریم $(b,p) = ۱$ (چرا؟) لذا بنابر قضیه‌ی کوچک فرما داریم

$$۱ \overset{p}{\equiv} b^{p-۱} \overset{p}{\equiv} a^{\frac{p-۱}{۲}}$$

برعکس فرض کنیم $a^{\frac{p-۱}{۲}} \overset{p}{\equiv} ۱$. ثابت کردیم هر عدد اول دارای یک ریشه‌ی اولیه است. فرض کنیم r یک ریشه‌ی اولیه‌ی p باشد. چون $(a,p) = ۱$ و $r, r^۲, \ldots, r^{p-۱}$ یک دستگاه مخفف مانده‌ها به پیمانه‌ی p است لذا $a \overset{p}{\equiv} r^k$ (برای یک $۱ \le k \le p-۱$) لذا

$$۱ \overset{p}{\equiv} a^{\frac{p-۱}{۲}} \overset{p}{\equiv} \left(r^k\right)^{\frac{p-۱}{۲}} = r^{k\left(\frac{p-۱}{۲}\right)}$$

چون مرتبه‌ی r به پیمانه‌ی p برابر $p-۱$ است لذا $p-۱ \mid k$ یعنی $k(\frac{p-۱}{۲}) = t(p-۱)$ (برای یک عدد صحیح t). پس $k\,(p-۱) = ۲t(p-۱)$ پس $k = ۲t$ لذا $a \overset{p}{\equiv} r^k \overset{p}{\equiv} (r^t)^۲$. لذا r^t در هم‌نهشتی $x^۲ \overset{p}{\equiv} a$ صدق می‌کند. پس a یک مانده‌ی مربعی p است. پس $\left(\frac{a}{p}\right) = ۱$. □

مثال ۱۲.۶ بنابر محک اویلر

$$\left(\frac{-۱}{p}\right) = \begin{cases} ۱ & (-۱)^{\frac{p-۱}{۲}} \overset{p}{\equiv} ۱ \\ -۱ & (-۱)^{\frac{p-۱}{۲}} \overset{p}{\equiv} -۱ \end{cases}$$

اما $(-۱)^{\frac{p-۱}{۲}} \overset{p}{\equiv} ۱$ اگر و تنها اگر $p \mid (-۱)^{\frac{p-۱}{۲}} - ۱$، اما عدد $(-۱)^{\frac{p-۱}{۲}} - ۱$ برابر ۰ یا -۲ است. چون p فرد است پس $p \nmid ۲$ لذا $(-۱)^{\frac{p-۱}{۲}} - ۱ = ۰$ یعنی $(-۱)^{\frac{p-۱}{۲}} = ۱$ پس $\frac{p-۱}{۲} = ۲k$ یعنی $p - ۱ = ۴k$ و لذا

$$p \overset{۴}{\equiv} ۱$$

پس $\left(\frac{-۱}{p}\right) = ۱$ اگر و تنها اگر $p \overset{۴}{\equiv} ۱$. این مطلب را یکبار قبلاً ثابت کرده‌ایم. گفتیم معادله‌ی $x^۲ \overset{p}{\equiv} -۱$ دارای جواب است اگر و تنها اگر $p \overset{۴}{\equiv} ۱$.

برخی خواص علامت لژاندر در لم زیر خلاصه شده است:

لم ۱۳.۶ فرض کنیم p یک عدد اول فرد و a و b دو عدد صحیح باشند و $(a,p) = (b,p) = ۱$. در این صورت

(الف) اگر $a \overset{p}{\equiv} b$ آن‌گاه $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ب) $\left(\frac{a}{p}\right) \overset{p}{\equiv} a^{\frac{p-۱}{۲}}$.

(ج) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

اثبات.

۱. اگر $a \overset{p}{\equiv} c^۲$ چون $a \overset{p}{\equiv} b$ لذا $b \overset{p}{\equiv} c^۲$ و بالعکس. لذا $\left(\frac{a}{p}\right) = ۱$ اگر و تنها اگر $\left(\frac{b}{p}\right) = ۱$.

۲. همان محک اویلر است.

۳. بنابر(ب) داریم

$$\left(\frac{ab}{p}\right) \overset{p}{\equiv} (ab)^{\frac{p-1}{2}} \overset{p}{\equiv} a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \overset{p}{\equiv} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

لذا

$$p \;\Big|\; \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

داریم ۲ یا $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = ۰$. چون p فرد است لذا $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = ۰$ پس $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

□

مثال ۱۴.۶ آیا هم‌نهشتی $x^۲ \overset{۲۹}{\equiv} -۷۶$ دارای جواب است؟ چون $۷۶ \overset{۲۹}{\equiv} ۱۸$ داریم

$$\left(\frac{-۷۶}{۲۹}\right) = \left(\frac{-۱}{۲۹}\right)\left(\frac{۷۶}{۲۹}\right) = \left(\frac{-۱}{۲۹}\right)\left(\frac{۱۸}{۲۹}\right)$$
$$= \left(\frac{-۱}{۲۹}\right)\left(\frac{۳^۲ \times ۲}{۲۹}\right) = \left(\frac{-۱}{۲۹}\right)\left(\frac{۳}{۲۹}\right)^۲\left(\frac{۲}{۲۹}\right) = \left(\frac{۲}{۲۹}\right)$$

زیرا $۱۱ \overset{۴}{\equiv} ۲۹$ و لذا $\left(\frac{-۱}{۲۹}\right) = ۱$. بنابراین هم‌نهشتی فوق دارای جواب است اگر وتنها اگر هم‌نهشتی $x^۲ \overset{۲۹}{\equiv} ۲$ دارای جواب باشد. اما

$$۲^{\frac{۲۹-۱}{۲}} = ۲^{۱۴} = ۲^۵ \times ۲^۵ \times ۲^۴ = ۳۲ \times ۳۲ \times ۱۶ \overset{۲۹}{\equiv} ۳ \times \times ۳ \times ۱۶$$
$$\overset{۲۹}{\equiv} ۵۷ \overset{۲۹}{\equiv} ۱۹ \times ۳ \overset{۲۹}{\equiv} ۴۸ \times ۳ \overset{۲۹}{\equiv} -۱$$

لذا بنابر محک اویلر ۲ یک نامانده‌ی مربعی است. یعنی $\left(\frac{۲}{۲۹}\right) = -۱$ پس هم‌نهشتی $x^۲ \overset{۲۹}{\equiv} -۷۶$ جواب ندارد.

§۳.۶ قانون تقابل مربعی

در این بخش، به بیان و اثبات قانون تقابل مربعی که روش کارآمد برای محاسبه‌ی علامت لژاندر ارائه می‌نماید، ارائه می‌دهیم. اثبات‌های فراوانی تاکنون برای این قضیه ارائه شده است. ما در اینجا یکی از این اثبات‌ها را که به مطالب پیشرفته در نظریه اعداد متکی نیست، ارائه می‌نماییم. ابتدا به چند لم نیاز داریم:

قضیه ۱۵.۶ (لم گاوس). فرض کنیم p یک عدد اول فرد و a عددی صحیح باشد و $(a,p)=۱$ و λ تعداد اعدادی از مجموعه‌ی $A=\{a,۲a,\ldots,\frac{p-۱}{۲}a\}$ باشد که باقیمانده‌ی تقسیم آن‌ها بر p از $\frac{p-۱}{۲}$ بیشتر است. در این صورت

$$\left(\frac{a}{p}\right)=(-۱)^{\lambda}$$

اجازه دهید قبل از اثبات لم گاوس، از آن در محاسبه‌ی $(\frac{a}{p})$ در یک مثال استفاده کنیم.

مثال ۱۶.۶ مطلوبست محاسبه‌ی $(\frac{۵}{۱۷})$.

حل. داریم $\frac{p-۱}{۲}=۸$ و لذا $A=\{۵,۱۰,۱۵,۲۰,۲۵,۳۰,۳۵,۴۰\}$ باقیمانده‌های تقسیم اعضای A بر p به ترتیب عبارتند از $۵,۱۰,۱۵,۳,۸,۱۳,۱,۶$. لذا در این‌جا $\lambda=۳$. پس $(\frac{۵}{۱۷})=(-۱)^{۳}=-۱$

اثبات. (لم گاوس) فرض کنیم $r_۱,r_۲,\ldots,r_{\frac{p-۱}{۲}}$ به ترتیب باقیمانده‌های تقسیم اعداد $a,۲a,\ldots,\frac{p-۱}{۲}a$ بر p باشند، r_i ها متمایزند (چرا؟) و برای هر $۱\le i\le\frac{p-۱}{۲}$ داریم $۱\le r_i\le p-۱$. فرض کنیم

$$A_۱=\left\{r_i\ :\ ۱\le i\le\frac{p-۱}{۲},r_i\le\frac{p-۱}{۲}\right\}$$
$$A_۲=\left\{r_i\ :\ ۱\le i\le\frac{p-۱}{۲},r_i>\frac{p-۱}{۲}\right\}$$

با توجه به تعریف λ داریم $|A_۲|=\lambda$. گیریم $|A_۱|=\mu$. پس $\lambda+\mu=\frac{p-۱}{۲}$ با نام‌گذاری مجدد گیریم

$$A_۱ = \{t_۱, t_۲, \ldots, t_\mu\}$$

و

$$A_۲ = \{s_۱, s_۲, \ldots, s_\lambda\}.$$

گیریم

$$B = \{t_۱, t_۲, \ldots, t_\mu, p - s_۱, p - s_۲, \ldots, p - s_\lambda\}$$

از تعریف $A_۱$ و $A_۲$ نتیجه می‌شود که $B \subseteq \left\{۱, ۲, \ldots, \frac{p-۱}{۲}\right\}$. اما B دارای $\lambda + \mu = \frac{p-۱}{۲}$ عضو متمایز می‌باشد (ثابت کنید). پس

$$B = \left\{۱, ۲, \ldots, \frac{p-۱}{۲}\right\}.$$

حال داریم

$$(a)\,(۲a)\,(۳a)\ldots\left(\frac{p-۱}{۲}\,a\right) \overset{p}{\equiv} r_۱ r_۲ \ldots r_{\frac{p-۱}{۲}} \overset{p}{\equiv} t_۱ t_۲ \ldots t_\mu s_۱ s_۲ \ldots s_\lambda$$

لذا

$$a^{\frac{p-۱}{۲}}\left(\left(\frac{p-۱}{۲}\right)!\right) \overset{p}{\equiv} t_۱ t_۲ \ldots t_\mu s_۱ s_۲ \ldots s_\lambda \qquad (۳.۶)$$

از طرفی از تساوی $B = \{۱, ۲, \ldots, \frac{p-۱}{۲}\}$ نتیجه می‌شود

$$\left(\frac{p-۱}{۲}\right)! = t_۱ t_۲ \ldots t_\mu\,(p - s_۱)\,(p - s_۲)\ldots(p - s_\lambda) \overset{p}{\equiv} (-۱)^\lambda t_۱ t_۲ \ldots t_\mu s_۱ s_۲ \ldots s_\lambda$$

چون $p - s_i \overset{p}{\equiv} -s_i$. پس

$$t_۱ t_۲ \ldots t_\mu s_۱ s_۲ \ldots s_\lambda \overset{p}{\equiv} (-۱)^\lambda\left(\left(\frac{p-۱}{۲}\right)!\right)$$

از این تساوی و رابطه‌ی (۳) نتیجه می‌شود

$$a^{\frac{p-۱}{۲}}\left(\left(\frac{p-۱}{۲}\right)!\right) \overset{p}{\equiv} (-۱)^\lambda\left(\left(\frac{p-۱}{۲}\right)!\right)$$

چون $\left(\left(\frac{p-۱}{۲}\right)!, p\right) = ۱$ لذا از تساوی بالا داریم

$$a^{\frac{p-۱}{۲}} \overset{p}{\equiv} (-۱)^\lambda$$

اکنون از محک اویلر نتیجه می‌شود

$$\left(\frac{a}{p}\right) \overset{p}{\equiv} (-۱)^\lambda$$

با توجه به فرد بودن p از این هم‌نهشتی نتیجه می‌شود

$$\left(\frac{a}{p}\right) = (-۱)^{\lambda}$$

□

اکنون به کمک لم گاوس $\left(\frac{۲}{p}\right)$ را برای عدد اول p محاسبه می‌کنیم. با علامات لم گاوس در این‌جا داریم (برای $a = ۲$)

$$A = \{۲, ۴, ۶, \ldots, p-۱\} = \left\{۲k \ : \ ۱ \leq k \leq \frac{p-۱}{۲}\right\}$$

چون اعضای A همگی کمتر از p هستند لذا همگی خود باقی‌مانده‌ی تقسیم خود بر p هستند. لذا در این‌جا $(\frac{۲}{p}) = (-۱)^{\lambda}$ که در آن λ تعداد اعداد مجموعه‌ی $A_۲$ است که در آن

$$A_۲ = \left\{۲k \ : \ ۲k > \frac{p-۱}{۲} \ , \ ۱ \leq k \leq \frac{p-۱}{۲}\right\}$$

پس λ برابر است با تعداد k های صحیح با شرط $\frac{p-۱}{۴} < k \leq \frac{p-۱}{۲}$ لذا $\lambda = \frac{p-۱}{۲} - \left[\frac{p-۱}{۴}\right]$ که در آن $[\,]$ تابع بزرگترین جزء صحیح است. توجه کنیم که دانستن زوج یا فرد بودن λ مقدار $\left(\frac{a}{p}\right)$ را محاسبه می‌کند. برای تعیین زوجیت λ حالات مختلف p به پیمانه‌ی ۸ را در نظر می‌گیریم. توجه کنیم که چون p فرد است لذا به پیمانه‌ی ۸ عدد p هم‌نهشت یکی از اعداد ۱،۳،۵ یا ۷ است.

در حالت $p = ۸k+۱$ $\quad \lambda = \frac{۸k}{۲} - \left[\frac{۸k}{۴}\right] = ۲k$

در حالت $p = ۸k+۳$ $\quad \lambda = \frac{۸k+۲}{۲} - \left[\frac{۸k+۲}{۴}\right] = ۴k+۱-۲k = ۲k+۱$

در حالت $p = ۸k+۵$ $\quad \lambda = \frac{۸k+۴}{۲} - \left[\frac{۸k+۴}{۴}\right] = ۴k+۲-(۲k+۱) = ۲k+۱$

در حالت $p = ۸k+۷$ $\quad \lambda = \frac{۸k+۶}{۲} - \left[\frac{۸k+۶}{۴}\right] = ۴k+۳-(۲k+۱) = ۲k+۲$

در حالت اول و چهارم λ زوج و در حالات دوم و سوم λ فرد است. پس ثابت کردیم:

قضیه ۱۷.۶ برای هر عدد اول فرد p داریم

$$\left(\frac{۲}{p}\right) = \begin{cases} ۱ & p \overset{۸}{\equiv} \pm ۱ \\ -۱ & p \overset{۸}{\equiv} \pm ۳ \end{cases}$$

به عبارت دیگر $\left(\frac{۲}{p}\right) = (-۱)^{\frac{p^۲-۱}{۸}}$

لم ۱۸.۶ فرض کنیم p یک عدد اول فرد و a عدد صحیح فردی باشد که $p \nmid a$ در این صورت

$$\left(\frac{a}{p}\right) = (-۱) \sum_{k=۱}^{(p-۱)/۲} \left[\frac{ka}{p}\right]$$

اثبات. فرض کنیم $S = \left\{a, ۲\,a, \ldots, (\frac{p-۱}{۲})a\right\}$ بنابر الگوریتم تقسیم برای هر $۱ \le k \le \frac{p-۱}{۲}$ می‌توان نوشت

$$ka = q_k\, p + r_k$$

لذا $\frac{ka}{p} = q_k + \frac{r_k}{p}$ و در نتیجه $\left[\frac{ka}{p}\right] = q_k$ (چون $\frac{r_k}{p} < ۱$) پس

$$ka = \left[\frac{ka}{p}\right] p + r_k \qquad (۴.۶)$$

با توجه به علامات در اثبات لم گاوس به‌راحتی دیده می‌شود که

$$\left\{r_۱, r_۲, \ldots, r_{\frac{p-۱}{۲}}\right\} = \{t_۱, t_۲, \ldots, t_\mu, s_۱, s_۲, \ldots, s_\lambda\}$$

از این تساوی و رابطه‌ی (۴) نتیجه می‌شود که

$$\sum_{k=۱}^{(p-۱)/۲} ka = \sum_{k=۱}^{(p-۱)/۲} \left[\frac{ka}{p}\right] p + \sum_{k=۱}^{\mu} t_k + \sum_{k=۱}^{\lambda} s_k \qquad (۵.۶)$$

در اثبات لم گاوس دیدیم $\left\{۱, ۲, \ldots, \frac{p-۱}{۲}\right\} = \{t_۱, t_۲, \ldots, t_\mu, p - s_۱, p - s_۲, \ldots, p - s_\lambda\}$.

لذا

$$\sum_{k=۱}^{(p-۱)/۲} k = \sum_{k=۱}^{\mu} t_k + \sum_{k=۱}^{\lambda} (p - s_k) = \lambda\, p + \sum_{k=۱}^{\mu} t_k - \sum_{k=۱}^{\lambda} s_k \qquad (۳)$$

اگر رابطه‌ی (۳) را از (۲) کم کنیم داریم:

$$(a-۱)\sum_{k=۱}^{(p-۱)/۲} k = p\left(\sum_{k=۱}^{(p-۱)/۲}\left[\frac{ka}{p}\right]-\lambda\right)+۲\sum_{k=۱}^{\lambda} s_k$$

چون a فرد است (بنا به فرض)، از رابطه‌ی اخیر نتیجه می‌شود که $\sum_{k=۱}^{(p-۱)/۲}\left[\frac{ka}{p}\right]-\lambda$ زوج است.

لذا بنابر لم گاوس

$$\left(\frac{a}{p}\right)=(-۱)^{\lambda}=(-۱)^{\sum_{k=۱}^{(p-۱)/۲}\left[\frac{ka}{p}\right]}$$

□

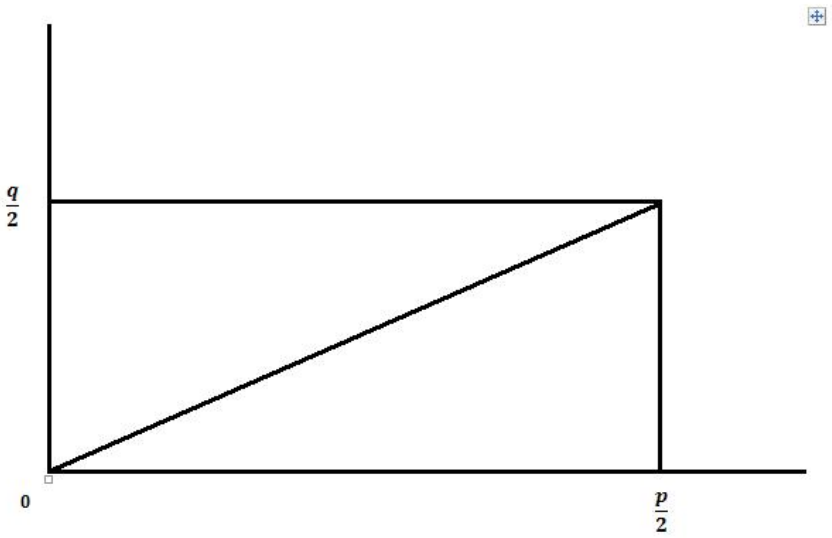
قضیه ۱۹.۶ (قانون تقابل مربعی). اگر p و q دو عدد اول فرد متمایز باشند آن‌گاه

$$\left(\frac{q}{p}\right)=(-۱)^{\frac{p-۱}{۲}\times\frac{q-۱}{۲}}\left(\frac{p}{q}\right)$$

به عبارت دیگر

$$\left(\frac{q}{p}\right)=\begin{cases}\left(\frac{p}{q}\right) & p\overset{۴}{\equiv}۱ \ \ or \ \ q\overset{۴}{\equiv}۱\\ -\left(\frac{p}{q}\right) & p\overset{۴}{\equiv}q\overset{۴}{\equiv}۳\end{cases}$$

اثبات. مستطیل زیر را در صفحه‌ی xy درنظر بگیرید



فرض کنیم T ناحیه‌ی داخل مستطیل، $T_۱$ ناحیه‌ی داخل مثلث پایینی و $T_۲$ ناحیه‌ی داخل مثلث بالایی باشد و فرض کنیم $t_۲, t_۱, t$ تعداد نقاط با مختصات صحیح به ترتیب در سه ناحیه‌ی فوق باشد. اولاً به راحتی داریم

$$t = \left(\frac{p-۱}{۲}\right)\left(\frac{q-۱}{۲}\right)$$

برای هر $۱ \le k \le \frac{p-۱}{۲}$ تعداد نقاط بالای نقطه‌ی $(k, ۰)$ و در داخل $T_۱$ برابر است با $\left[\frac{kq}{p}\right]$ پس

$$t_۱ = \sum_{k=۱}^{(p-۱)/۲} \left[\frac{kq}{p}\right]$$

برای هر $۱ \le l \le \frac{q-۱}{۲}$ تعداد نقاط روی خط افقی رسم شده از نقطه‌ی $(۰, l)$ و در داخل $T_۲$ برابر است با $\left[\frac{lp}{q}\right]$. پس

$$t_۲ = \sum_{l=۱}^{(q-۱)/۲} \left[\frac{lp}{q}\right]$$

چون هیچ نقطه‌ای با مختصات صحیح روی قطر مستطیل نیست (چرا؟) لذا $t = t_۱ + t_۲$ حال با استفاده از لم قبل داریم

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-۱)^{t_۱} \times (-۱)^{t_۲} = (-۱)^{t_۱+t_۲} = (-۱)^{t} = (-۱)^{\frac{p-۱}{۲}\frac{q-۱}{۲}}$$

لذا

$$\left(\frac{q}{p}\right) = (-۱)^{\frac{p-۱}{۲}\frac{q-۱}{۲}}\left(\frac{p}{q}\right)$$

□

مثال ۲۰.۶ (الف) آیا هم‌نهشتی $x^۲ \overset{۸۵۳}{\equiv} ۵۲۷$ دارای جواب است؟

توجه کنیم که ۸۵۳ عددی اول است و $۳۱ \times ۱۷ \overset{۳۱}{\equiv} ۵۲۷$. لذا

$$\left(\frac{۵۲۷}{۸۵۳}\right) = \left(\frac{۱۷}{۸۵۳}\right)\left(\frac{۳۱}{۸۵۳}\right)$$

$$\left(\frac{۱۷}{۸۵۳}\right) = (-۱)^{\frac{۱۷-۱}{۲}\frac{۸۵۳-۱}{۲}}\left(\frac{۸۵۳}{۱۷}\right) = \left(\frac{۳}{۱۷}\right) = \left(\frac{۱۷}{۳}\right) = \left(\frac{۲}{۳}\right) = -۱$$

$$\left(\frac{۳۱}{۸۵۳}\right) = (-۱)^{\frac{۳۱-۱}{۲}\frac{۸۵۳-۱}{۲}}\left(\frac{۸۵۳}{۳۱}\right) = \left(\frac{۱۶}{۳۱}\right) = \left(\frac{۲}{۳۱}\right)^{۴} = ۱$$

لذا $(\frac{۵۲۷}{۸۵۳}) = (-۱)\ (۱) = (-۱)$. یعنی هم‌نهشتی داده شده جواب ندارد.

(ب) آیا هم‌نهشتی $x^۲ \overset{۸۵۹}{\equiv} ۳۱$ دارای جواب است؟

$$\left(\frac{۳۱}{۸۵۹}\right) = -\left(\frac{۸۵۹}{۳۱}\right) = -\left(\frac{۲۲}{۳۱}\right) = -\left(\frac{۲}{۳۱}\right)\left(\frac{۱۱}{۳۱}\right)$$
$$= -(۱)\left(\frac{۱۱}{۳۱}\right) = -(-۱)\left(\frac{۳۱}{۱۱}\right) = \left(\frac{۳۱}{۱۱}\right) = \left(\frac{۹}{۱۱}\right) = \left(\frac{۳}{۱۱}\right)^۲ = ۱$$

لذا $\left(\frac{۳۱}{۸۵۹}\right) = ۱$. یعنی هم‌نهشتی داده شده جواب دارد.

§۴.۶ هم‌نهشتی‌های درجه دوم به پیمانه غیراول

قضیه ۲۱.۶ فرض کنیم p یک عدد اول فرد و a عددی صحیح و n عددی طبیعی باشد و $p \nmid a$. در این صورت هم‌نهشتی $x^۲ \overset{p^n}{\equiv} a$ دارای جواب است اگر و تنها اگر $\left(\frac{a}{p}\right) = ۱$.

اثبات. بدیهی است که اگر هم‌نهشتی $x^۲ \overset{p^n}{\equiv} a$ دارای جوابی چون b باشد، آن‌گاه b یک جواب هم‌نهشتی $x^۲ \overset{p}{\equiv} a$ نیز هست و لذا $\left(\frac{a}{p}\right) = ۱$.

برعکس. فرض کنیم $\left(\frac{a}{p}\right) = ۱$. لذا هم‌نهشتی $x^۲ \overset{p}{\equiv} a$ جواب دارد. با استقرا ثابت می‌کنیم هم‌نهشتی

$$x^۲ \overset{p^n}{\equiv} a \qquad (۶.۶)$$

برای هر $n \geq ۱$ جواب دارد. اگر $n = ۱$ با عنایت به تعریف $(\frac{a}{p})$ حکم برقرار است. فرض کنیم $k \geq ۱$ و معادله‌ی $x^۲ \overset{p^k}{\equiv} a$ دارای جوابی مانند x_k است، نشان می‌دهیم معادله‌ی $x^۲ \overset{p^{k+۱}}{\equiv} a$ دارای جواب است. با عنایت به فرض $p^k | x_k^۲ - a$. و لذا

$$x_k^۲ = a + b_k p^k$$

برای یک عدد صحیح b_k. هم‌نهشتی $x_k y \overset{p}{\equiv} -b_k$ ۲ دارای جواب منحصر به فردی مانند y_k (به پیمانه‌ی p) است،قرار می‌دهیم $x_{k+۱} = x_k + y_k p^k$. داریم

$$x_{k+1}^2 = \left(x_k + y_k\, p^k\right)^2 = a + b_k p^k + 2x_k y_k p^k + y_k^2 p^{2k} = a + \left(b_k + 2x_k y_k\right) p^k + y_k^2 p^{2k} \overset{p^{k+1}}{\equiv} a$$

چون $p \mid b_k + 2x_k y_k$. پس x_{k+1} یک جواب $x^2 \overset{p^{k+1}}{\equiv} a$ است. □

در اثبات قضیه‌ی بالا دیدیم که با داشتن جواب برای معادله‌ی $x^2 \overset{p}{\equiv} a$ می‌توان جواب معادله‌ی $x^2 \overset{p^k}{\equiv} a$ را بدست آورد. برای پیدا کردن جواب $x^2 \overset{p}{\equiv} a$ در صورت وجود، الگوریتم‌های مختلفی وجود دارد که از حوصله‌ی این نوشتار بیرون است.

مثال ۲۲.۶ نشان دهید هم‌نهشتی $x^2 \overset{1331}{\equiv} 75$ دارای جواب است. یک جواب آن‌را بدست آورید.

توجه کنیم که $11^3 = 1331$ و داریم

$$\left(\frac{75}{11}\right) = \left(\frac{9}{11}\right) = \left(\frac{3}{11}\right)^2 = 1$$

لذا بنابر قضیه‌ی قبل، هم‌نهشتی داده شده دارای جواب است. با توجه به اثبات قضیه قبل یک جواب به‌دست می‌آوریم. بافرض $x_1 = 3$ داریم $x_1^2 \overset{11}{\equiv} 75$.

$$x_1^2 = 9 = 75 - 6 \times 11$$

لذا $b_1 = -6$. هم‌نهشتی $2\, x_1\, y \overset{p}{\equiv} -b_1$ به شکل $6\, y \overset{11}{\equiv} 6$ در می‌آید. لذا گیریم $y_1 = 1$ و لذا

$$x_2 = x_1 + y_1\, p = 3 + (+1)\,(11) = 14$$

$x_2 = 14$ جوابی برای هم‌نهشتی $x^2 \overset{11^2}{\equiv} 75$ می‌باشد. حال

$$x_2^2 = 196 = 75 + 1 \times 11^2$$

لذا $b_2 = 1$. هم‌نهشتی $2x_2\, y \overset{p}{\equiv} -b$ به شکل $-1\, y \overset{11}{\equiv} 6$ در می‌آید. لذا گیریم $y_2 = -2$ و لذا

$$x_3 = x_2 + y_2 p^2 = 14 + (-2)\,(121) = -228$$

در نتیجه $x_3 = -228$ یک جواب $x^2 \overset{1331}{\equiv} 75$ می‌باشد.

قانون تقابل مربعی به همراه قضیه‌ی قبل وجود جواب برای معادله‌ی $x^2 \overset{p^k}{\equiv} a$ را برای زمانی که p

یک عدد اول فرد باشد بررسی می‌کند. برای $p = ۲$ قضیه‌ی زیر را داریم.

قضیه ۲۳.۶ فرض کنیم a یک عدد فرد باشد. در این صورت

(الف) $x^۲ \overset{p}{\equiv} a$ همواره جواب دارد.

(ب) $x^۲ \overset{۴}{\equiv} a$ فقط و فقط وقتی جواب دارد که $a \overset{۴}{\equiv} ۱$

(ج) $x^۲ \overset{۲^k}{\equiv\equiv} a$، $k \geq ۳$، فقط و فقط وقتی جواب دارد که $a \overset{۸}{\equiv} ۱$

اثبات. تمرین. □

با کمک چند قضیه‌ی بالا بررسی وجود جواب برای هم‌نهشتی

$$x^۲ \overset{n}{\equiv} a \qquad (a, n) = ۱$$

میسر است، در واقع داریم

قضیه ۲۴.۶ فرض کنیم $n = p_۱^{\alpha_۱} p_۲^{\alpha_۲} \dots p_r^{\alpha_r}$ تجزیه‌ی استانده n به عوامل اول باشد. در این صورت هم‌نهشتی $x^۲ \overset{n}{\equiv} a$، $(a, n) = ۱$، دارای جواب است اگر و تنها اگر هر یک از هم‌نهشتی‌های $x^۲ \overset{p_i^{\alpha_i}}{\equiv\equiv} a$، $۱ \leq i \leq r$، دارای جواب باشد.

اثبات. اگر b یک جواب $x^۲ \overset{n}{\equiv} a$ باشد، به وضوح b یک جواب معادله‌ی $x^۲ \overset{p_i^{\alpha_i}}{\equiv\equiv} a$، برای هر $۱ \leq i \leq r$، نیز هست.

برعکس، اگر برای هر i، $۱ \leq i \leq r$، b_i یک جواب هم‌نهشتی $x^۲ \overset{p_i^{\alpha_i}}{\equiv\equiv} a$ باشد، آن‌گاه بنابر قضیه‌ی باقی‌مانده چینی می‌توان b را چنان بدست آورد که برای هر i، $۱ \leq i \leq r$، $b \overset{p_i^{\alpha_i}}{\equiv\equiv} b_i$. حال برای هر i، $۱ \leq i \leq r$، داریم

$$b^۲ \overset{p_i^{\alpha_i}}{\equiv\equiv} b_i^۲ \overset{p_i^{\alpha_i}}{\equiv\equiv} a$$

لذا برای هر i، $۱ \leq i \leq r$، $p_i^{\alpha_i} | b^۲ - a$ و بنابراین $n | b^۲ - a$، یعنی $b^۲ \overset{n}{\equiv} a$ و اثبات تمام است.

□

§۵.۶ تمرین

۱. نشان دهید هر ریشه‌ی اولیه‌ی p یک نامانده‌ی p است.

۲. نشان دهید برای هر عدد اول p، $\sum_{a=۱}^{p-۱} \left(\frac{a}{p}\right) = ۰$

۳. نشان دهید بینهایت عدد اول به شکل $۴k+۱$ وجود دارد.

(راهنمایی: فرض کنید تعداد آن‌ها متناهی و عبارت باشند از $p_۱, p_۲, \ldots, p_k$ حال عدد $N = (۴p_۱p_۲\ldots p_k)^۲ + ۱$ را در نظر بگیرید)

۴. نشان دهید بی‌نهایت عدد اول به شکل $۸k-۱$ وجود دارد.

(راهنمایی: عدد $N = (۴p_۱p_۲\ldots p_k)^۲ - ۲$ را در نظر بگیرید.)

۵. فرض کنیم p و $q = ۲p+۱$ دو عدد اول فرد باشند. ثابت کنید $(-۱)^{\frac{p-۱}{۲}}۲$ یک ریشه‌ی اولیه‌ی q است.

۶. اگر $p = ۲^k + ۱$ اول باشد، نشان دهید هر نامانده‌ی p یک ریشه‌ی اولیه‌ی p است.

۷. نشان دهید ۲ یک ریشه‌ی اولیه‌ی ۱۹ است و با استفاده از آن کلیه‌ی ریشه‌های اولیه‌ی ۱۹ را بیابید.

۸. فرض کنیم p یک عدد اول فرد باشد، نشان دهید معادله‌ی $x^۲ + py + a = ۰$ جواب صحیح دارد اگر و تنها اگر $\left(\frac{-a}{p}\right) = ۱$.

۹. کدام‌یک از معادلات $x^۲ + ۷۹x - ۲ = ۰$ و $x^۲ + ۷۹x + ۲ = ۰$ جواب دارد؟

۱۰. اگر $p = ۳ \times ۲^n + ۱$ و اول باشد، نشان دهید ۲ ریشه‌ی اولیه نیست.

۱۱. اگر p یک عدد اول فرد باشد ثابت کنید $\sum_{a=۱}^{p-۲} \left(\frac{a(a+۱)}{p}\right) = -۱$

(**راهنمایی:** از وارون حسابی a به پیمانه‌ی p استفاده کنید.)

۱۲. اگر p و $q = ۲p + ۱$ اول فرد باشند، ثابت کنید -۴ ریشه‌ی اولیه‌ی q است.

۱۳. قبلاً دیدیم اگر $a^n - ۱$ اول باشد $a = ۲$ و n اول است. به کمک علامت لژاندر نشان دهید $۲^n - ۱$ برای اعداد اول $n = ۱۱, ۲۳, ۸۳, ۲۵۱$ اول نیست.

۱۴. نشان دهید بی‌نهایت عدد اول به شکل $۸k + ۳$ وجود دارد.

۱۵. نشان دهید بی‌نهایت عدد اول به شکل $۵k - ۱$ وجود دارد.

۱۶. هم‌نهشتی $x^۲ \overset{۳۵}{\equiv} ۱۱$ را حل کنید.

۱۷. فرض کنیم p و q دو عدد اول فرد باشند و $p = q + ۴a$. ثابت کنید $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

۱۸. محاسبه کنید:

(الف) $\left(\frac{-۲۱۹}{۳۸۳}\right)$

(ب) $\left(\frac{۴۶۱}{۷۷۳}\right)$

(پ) $\left(\frac{۳۶۵۸}{۱۲۷۰۳}\right)$

۱۹. نشان دهید معادله‌ی $(x^۲ - ۳)(x^۲ - ۵)(x^۲ - ۱۵) = ۰$ جواب صحیح ندارد ولی هم‌نهشتی $(x^۲ - ۳)(x^۲ - ۵)(x^۲ - ۱۵) \overset{p}{\equiv} ۰$ برای هر p جواب دارد.

۲۰. کلیه‌ی جواب‌های $x^۲ \overset{۱۸۰}{\equiv} -۱۱$ را بدست آورید (جواب‌های ناهم‌نهشت به پیمانه‌ی ۱۸۰).

فصل ۷
کسرهای مسلسل

تقریب یک عدد حقیقی توسط اعداد گویا، در محاسبات ریاضی بسیار مهم است. در این تقریب مطلوب آن است که تعداد ارقام در صورت و مخرج عدد گویای انتخاب شده تا حد ممکن کم باشد. بسط اعشاری یک عدد حقیقی x، یک دنباله از اعداد گویا به‌دست می‌دهد که به سمت عدد x میل می‌کند. درواقع، بسط اعشاری $\sqrt{۲} = ۱/۴۱۴۲۱۳۵۶۲\cdots$ و دنباله‌ی

$$۱, \frac{۱۴}{۱۰}, \frac{۱۴۱}{۱۰۰}, \frac{۱۴۱۴}{۱۰۰۰}, \ldots$$

را معرفی می‌نماید که همگرا به $\sqrt{۲}$ است.

کسر مسلسل x دنباله‌ی دیگری از اعداد گویا را معرفی می‌نماید که به x همگراست. در بسیاری از موارد اعداد گویای معرفی شده در این دنباله مطلوبیت بیشتری (به تعبیر بالا) دارند.

§۱.۷ کسرهای مسلسل متناهی

منظور از یک **کسر مسلسل متناهی** عددی به شکل زیر است

$$a_۰ + \cfrac{۱}{a_۱ + \cfrac{۱}{a_۲ + \cfrac{۱}{\ddots + \cfrac{۱}{a_{n-۱} + \cfrac{۱}{a_n}}}}}$$

که در آن a_iها اعداد حقیقی‌اند و برای $i \geq ۱$، $a_i > ۰$. a_iها ($i \geq ۱$) را **مخرج‌های جزئی کسر مسلسل** می‌گوییم. اگر a_i ها صحیح باشند کسر را یک **کسر مسلسل ساده متناهی** می‌گوییم. کسر مسلسل متناهی فوق را با $[a_۰; a_۱, \ldots, a_n]$ نمایش می‌دهیم.

واضح است که هر کسر مسلسل ساده‌ی متناهی برابر یک عدد گویاست. به عنوان مثال

$$[۲; ۳, ۱, ۵, ۲] = ۲ + \cfrac{۱}{۳ + \cfrac{۱}{۱ + \cfrac{۱}{۵ + \frac{۱}{۲}}}} = ۲ + \cfrac{۱}{۳ + \cfrac{۱}{۱ + \frac{۲}{۱۱}}}$$
$$= ۲ + \cfrac{۱}{۳ + \frac{۱۱}{۱۳}} = ۲ + \frac{۱۳}{۵۰} = \frac{۱۱۳}{۵۰}$$

عکس این مطلب نیز برقرار است:

قضیه ۱.۷ هر عدد گویا را می‌توان به صورت یک کسر مسلسل ساده‌ی متناهی نوشت.

اثبات. فرض کنیم $\frac{a}{b}$، $b > ۰$، یک عدد گویا باشد. با تقسیمات متوالی داریم

$$\begin{aligned}
a &= a_۰ b + r_۱ && ۰ \leqslant r_۱ < b \\
b &= a_۱ r_۱ + r_۲ && ۰ \leqslant r_۲ < r_۱ \\
r_۱ &= a_۲ r_۲ + r_۳ && ۰ \leqslant r_۳ < r_۲ \\
&\vdots \quad \vdots && \vdots \\
r_{n-۲} &= a_{n-۱} r_{n-۱} + r_n && ۰ \leqslant r_n < r_{n-۱} \\
r_{n-۱} &= a_n r_n + ۰
\end{aligned}$$

لذا داریم

$$\frac{a}{b} = a_۰ + \frac{r_۱}{b} = a_۰ + \frac{۱}{\frac{b}{r_۱}} = a_۰ + \frac{۱}{a_۱ + \frac{r_۲}{r_۱}} = a_۰ + \frac{۱}{a_۱ + \frac{۱}{\frac{r_۱}{r_۲}}}$$

$$= a_۰ + \frac{۱}{a_۱ + \frac{۱}{a_۲ + \frac{r_۳}{r_۲}}} = a_۰ + \frac{۱}{a_۱ + \frac{۱}{a_۲ + \frac{۱}{\cdots}}}$$

یعنی $\frac{a}{b} = [a_۰; a_۱, \ldots, a_n]$ □

مثال ۲.۷ اگر $\frac{a}{b} = \frac{۱۱۳}{۵۰}$، آنگاه داریم

$$\begin{aligned} ۱۱۳ &= ۲ \times ۵۰ + ۱۳ && \longrightarrow a_۰ = ۲ \\ ۵۰ &= ۳ \times ۱۳ + ۱۱ && \longrightarrow a_۱ = ۳ \\ ۱۳ &= ۱ \times ۱۱ + ۲ && \longrightarrow a_۲ = ۱ \\ ۱۱ &= ۵ \times ۲ + ۱ && \longrightarrow a_۳ = ۵ \\ ۲ &= ۲ \times ۱ + ۰ && \longrightarrow a_۴ = ۲ \end{aligned}$$

لذا $\frac{۱۱۳}{۵۰} = [۲; ۳, ۱, ۵, ۲]$.

توجه می‌کنیم که اگر $a_n \neq ۱$، آنگاه $[a_۰; a_۱, \ldots, a_n] = [a_۰, a_۱, \ldots, a_n - ۱, ۱]$ و اگر $a_n = ۱$ آنگاه $[a_۰; a_۱, \ldots, a_n] = [a_۰, a_۱, \ldots, a_{n-۱} + ۱]$.

لذا هر کسر مسلسل ساده‌ی متناهی دارای دو نمایش است که در یکی n زوج و در دیگری n فرد است.

مثال ۳.۷ دنباله‌ی $\{u_n\}_{n=۱}^{\infty}$ از اعداد فیبوناچی به صورت زیر تعریف می‌شود.

$$u_۱ = ۱ \quad , u_۲ = ۱ \quad , u_n = u_{n-۱} + u_{n-۲} \quad , \quad n \geq ۳$$

لذا

$$\frac{u_{n+۱}}{u_n} = \underbrace{[۱, ۱, ۱ \ldots, ۱, ۲]}_{n-۱ \text{ جمله}} = \underbrace{[۱, ۱, ۱ \ldots, ۱, ۱]}_{n \text{ جمله}}$$

تعریف ۴.۷ اگر $\alpha = [a_۰; a_۱, a_۲, \ldots, a_n]$، آنگاه برای هر k، $۰ \leq k \leq n$، **همگرای** k **ام** α را به صورت زیر تعریف می‌کنیم:

$$c_k = [a_۰; a_۱, a_۲, \ldots, a_k]$$

مثال ۵.۷ قبلاً دیدیم $\alpha = \frac{۱۱۳}{۵۰} = [۲; ۳, ۱, ۵, ۲]$. لذا

$$c_۰ = ۲$$
$$c_۱ = [۲; ۳] = ۲ + \frac{۱}{۳} = \frac{۷}{۳}$$
$$c_۲ = [۲; ۳, ۱] = ۲ + \frac{۱}{۳ + \frac{۱}{۱}} = \frac{۹}{۴}$$
$$c_۳ = [۲; ۳, ۱, ۵] = ۲ + \frac{۱}{۳ + \frac{۱}{۱ + \frac{۱}{۵}}} = \frac{۵۲}{۲۳}$$
$$c_۴ = [۲; ۳, ۱, ۵, ۲] = \frac{۱۱۳}{۵۰}$$

نمادگذاری ۶.۷ فرض کنیم $\alpha = [a_۰; a_۱, a_۲, \ldots, a_n]$. قرار می‌دهیم

$$\begin{array}{ll} p_۰ = a_۰ & q_۰ = ۱ \\ p_۱ = a_۱ p_۰ + ۱ & q_۱ = a_۱ \\ \vdots \quad \vdots & \vdots \\ p_k = a_k p_{k-۱} + p_{k-۲} & q_k = a_k q_{k-۱} + q_{k-۲} \quad (\forall k \geq ۲) \end{array}$$

قضیه ۷.۷ با نمادگذاری‌های فوق برای هر $k \geq ۰$ داریم

$$c_k = \frac{p_k}{q_k}$$

اثبات. با استقراء به راحتی اثبات می‌شود. □

لم ۸.۷ برای هر $k \geq ۱$ داریم

$$p_k q_{k-۱} - q_k p_{k-۱} = (-۱)^{k-۱}$$

اثبات. برای $k = ۱$ داریم $p_۱q_۰ - q_۱p_۰ = a_۰p_۰ - a_۱p_۰ = ۱ = (-۱)^{۱-۱}$. اگر فرض کنیم حکم برای k برقرار است، آن‌گاه

$$p_{k+۱}q_k - q_{k+۱}p_k = (a_{k+۱}p_k + p_{k-۱})\,q_k - (a_{k+۱}q_k + q_{k-۱})\,p_k = -\,(p_kq_{k-۱} - q_kp_{k-۱})$$

چون بنا به فرض برقراری حکم برای k داریم $p_kq_{k-۱} - q_kp_{k-۱} = (-۱)^{k-۱}$، لذا از رابطه‌ی اخیر نتیجه می‌شود که

$$p_{k+۱}q_k - q_{k+۱}p_k = -(-۱)^{k-۱} = (-۱)^k$$

لذا حکم با استقرا ثابت می‌شود. □

نتیجه ۹.۷ برای هر $k > ۱$ داریم

$$(q_k, q_{k-۱}) = ۱ \text{ ب.م.م} = (p_k, p_{k-۱}) \text{ ب.م.م} = (p_k, q_k) \text{ ب.م.م}$$

لم ۱۰.۷ $q_۱ \geq q_۰$ و برای هر $k \geq ۱$، $q_{k+۱} > q_k$.

در مثال قبل دیدیم $\alpha = \frac{۱۱۳}{۵۰} = [۲; ۳, ۱, ۵, ۲]$ و

$$c_۰ = ۲,\quad c_۱ = \frac{۷}{۳}\ , c_۲ = \frac{۹}{۴},\quad c_۳ = \frac{۵۲}{۲۳},\quad c_۴ = \frac{۱۱۳}{۵۰} = \alpha$$

مشاهده می‌شود که داریم

$$c_۰ < c_۲ < c_۴ < c_۳ < c_۱$$

در واقع $c_۳c_۴ = \frac{۱}{۱۱۵۰}$ عددی کوچک است، این اتفاقی نیست. در واقع داریم

قضیه ۱۱.۷ (الف) همگراهای با اندیس زوج تشکیل یک دنباله‌ی اکیداً صعودی می‌دهند. یعنی

$$c_۰ < c_۲ < c_۴ < \ldots < c_{۲k} < c_{۲k+۲} < \ldots$$

(ب) همگراهای با اندیس فرد تشکیل یک دنباله‌ی اکیداً نزولی می‌دهند. یعنی

$$c_۱ > c_۳ > c_۵ > \ldots > c_{۲k+۱} > c_{۲k+۳} > \ldots$$

(ج) هر همگرای با اندیس فرد بزرگتر از هر همگرای با اندیس زوج است. یعنی

$$c_۰ < c_۲ < c_۴ < \ldots < c_{۲k} < \ldots < c_{۲l+۱} < \ldots < c_۳ < c_۱$$

اثبات. داریم

$$\begin{aligned} c_{k+۲} - c_k &= (c_{k+۲} - c_{k+۱}) + (c_{k+۱} - c_k) \\ &= \left(\frac{p_{k+۲}}{q_{k+۲}} - \frac{p_{k+۱}}{q_{k+۱}}\right) + \left(\frac{p_{k+۱}}{q_{k+۱}} - \frac{p_k}{q_k}\right) \\ &= \left(\frac{(-۱)^{k+۱}}{q_{k+۲}q_{k+۱}} + \frac{(-۱)^k}{q_{k+۱}q_k}\right) \\ &= \frac{(-۱)^k(q_{k+۲} - q_k)}{q_{k+۲}q_{k+۱}q_k} \end{aligned}$$

چون q_k ها مثبت و اکیداً صعودی هستند **(الف)** و **(ب)** از رابطه‌ی بالا نتیجه می‌شوند. داریم

$$c_{۲j} - c_{۲j-۱} = \frac{p_{۲j}}{q_{۲j}} - \frac{p_{۲j-۱}}{q_{۲j-۱}} = \frac{(-۱)^{۲j-۱}}{q_{۲j}\, q_{۲j-۱}} < ۰$$

لذا برای هر r و s داریم

$$c_{۲s} < c_{۲s+۲r} < c_{۲s+۲r-۱} < c_{۲r-۱}$$

و این **(ج)** را ثابت می‌کند. □

§۲.۷ کسرهای مسلسل نامتناهی

تعریف ۱۲.۷ اگر $a_۰, a_۱, a_۲, \ldots, a_n, \ldots$ یک دنباله‌ی نا متناهی از اعداد صحیح باشد و برای هر $i \geq ۱$، $a_i > ۰$ آن‌گاه نماد

$$[a_۰; a_۱, a_۲, \ldots, a_n, \ldots] = a_۰ + \cfrac{۱}{a_۱ + \cfrac{۱}{a_۲ + \cfrac{۱}{\ddots + \cfrac{۱}{a_{n-۱} + \cfrac{۱}{a_n + \ldots}}}}}$$

را یک **کسر مسلسل ساده‌ی نامتناهی** می‌گوییم. برای هر $n \geq ۰$ قرار می‌دهیم

$$c_n = [a_۰; a_۱, \ldots, a_n]$$

قضیه ۱۳.۷ حد $\lim_{n\to\infty} c_n$ وجود دارد و این حد را **مقدار کسر مسلسل نامتناهی** قرار می‌دهیم

$$[a_۰; a_۱, a_۲, \ldots] = \lim_{n\to\infty} c_n$$

اثبات. دنباله‌ی $c_۰ < c_۲ < c_۴ < \ldots$ یک دنباله‌ی صعودی و از بالا کراندار است، (بنابر قضیه‌ی قبل $c_۱$ یک کران بالای آن است) و لذا حد این دنباله وجود دارد. قرار می‌دهیم

$$\lim_{k\to\infty} c_{۲k} = \alpha$$

به‌طریق مشابه قرار می‌دهیم

$$\lim_{k\to\infty} c_{۲k+۱} = \alpha'$$

با عنایت به صعودی بودن دنباله‌ی $\{c_{۲k}\}$ و نزولی بودن دنباله‌ی $\{c_{۲k+۱}\}$ داریم

$$c_{۲k} < \alpha \quad , \; c_{۲k+۱} > \alpha' \qquad \text{و} \qquad \forall k \geq ۱$$

لذا برای هر $k \geq ۱$ داریم

$$۰ \leq \alpha' - \alpha < c_{۲k+۱} - c_{۲k} = \frac{۱}{q_{۲k}\, q_{۲k+۱}} \quad \forall k$$

چون $q_k \to \infty$ لذا $\alpha' - \alpha = ۰$ و $\alpha = \alpha'$. در نتیجه $\lim_{n\to\infty} c_n = \alpha$ □

قضیه ۱۴.۷ مقدار هر کسر مسلسل نامتناهی عددی اصم است.

اثبات. فرض کنیم $\alpha = [a_۰; a_۱, a_۲, \ldots]$. چون برای هر $n \geq ۱$ عدد α اکیداً بین c_n و $c_{n+۱}$ قرار دارد. لذا

$$۰ < |\alpha - c_n| < |c_{n+۱} - c_n| = \frac{۱}{q_n\, q_{n+۱}}$$

اگر $\alpha = \frac{a}{b}$ گویا باشد $(b > ۰)$ آن‌گاه

$$۰ < \left|\frac{a}{b} - \frac{p_n}{q_n}\right| < \frac{۱}{q_n\, q_{n+۱}}$$

لذا

$$۰ < |a\, q_n - bp_n| < \frac{b}{q_{n+۱}}$$

حال اگر n را چنان بزرگ اختیار کنیم که $q_{n+۱} > b$ آنگاه

$$۰ < |aq_n - bp_n| < ۱$$

و این غیرممکن است. زیرا $aq_n - bp_n$ عددی صحیح است. □

قضیه ۱۵.۷ اگر دو کسر مسلسل ساده‌ی نامتناهی $[a_۰; a_۱, a_۲, \ldots]$ و $[b_۰; b_۱, b_۲, \ldots]$ مساوی باشند آنگاه برای هر $n \geq ۰$ داریم $a_n = b_n$.

اثبات. فرض کنیم $\alpha = [a_۰; a_۱, a_۲, \ldots] = [b_۰; b_۱, b_۲, \ldots]$ در این صورت

$$\alpha = a_۰ + \frac{۱}{[a_۱; a_۲, \ldots]} = b_۰ + \frac{۱}{[b_۱; b_۲, \ldots]}$$

لذا

$$a_۰ = b_۰ = [\alpha]$$

که در این‌جا $[\alpha]$ جزء صحیح α است. حال داریم

$$\frac{۱}{[a_۱; a_۲, \ldots]} = \frac{۱}{[b_۱; b_۲, \ldots]}$$

و لذا

$$[a_۱; a_۲, \ldots] = [b_۱; b_۲, \ldots]$$

با تکرار روند فوق داریم $a_۱ = b_۱$ و با ادامه‌ی این روند با استقرایی ساده نتیجه می‌شود که $a_n = b_n$ برای هر $n \geq ۰$. □

تعریف ۱۶.۷ هرگاه $\alpha = [a_۰; a_۱, a_۲, \ldots, a_m, b_۱, b_۲, \ldots, b_n, b_۱, b_۲, \ldots, b_n, \ldots]$ یعنی دنباله‌ی مخرج‌های جزئی پس از جمله‌ی mام، تکرار دنباله‌ی $b_۱, b_۲, \ldots, b_n$ باشد آنگاه کسر مسلسل را تناوبی گوییم و با $\alpha = [a_۰; a_۱, \ldots, a_m, \overline{b_۱, b_۲, \ldots, b_n}\,]$ نمایش می‌دهیم.

مثال ۱۷.۷ اگر $\alpha = [-۳; ۲, \overline{۱, ۴}]$، α را محاسبه کنید.

با فرض

$$y = [\overline{۱, ۴}] = ۱ + \frac{۱}{۴ + \frac{۱}{۱ + \frac{۱}{۴ + \cdots}}}$$

روشن است که $\alpha = [-۳; ۲, y]$، از طرفی

$$y = [۱, ۴, y] = ۱ + \frac{۱}{۴ + \frac{۱}{y}} = ۱ + \frac{۱}{\frac{۴y+۱}{y}} = \frac{۵y + ۱}{۴y + ۱}$$

در نتیجه $۴y^۲ - ۴y - ۱ = ۰$، چون $y > ۰$ لذا $y = \frac{۱ + \sqrt{۲}}{۲}$. حال

$$\alpha = -۳ + \frac{۱}{۲ + \frac{۱}{y}} = -۳ + \frac{۱}{۲ + \frac{۲}{۱ + \sqrt{۲}}} = -۳ + \frac{۱ + \sqrt{۲}}{۴ + ۲\sqrt{۲}}$$
$$= \frac{-۱۱ - ۵\sqrt{۲}}{۴ + ۲\sqrt{۲}} = \frac{-۱۲ + \sqrt{۲}}{۴}$$

در واقع می‌توان ثابت کرد یک کسر مسلسل ساده‌ی نامتناهی برابر $a + b\sqrt{d}$ (a و b گویا هستند و d عددی صحیح و مثبت است که مربع کامل نیست) است اگر و تنها اگر متناوب باشد.

آن‌چه در اثبات قضیه‌ی بالا دیدیم نشان می‌دهد اگر $\alpha = [a_۰; a_۱, a_۲, \ldots]$ آن‌گاه $a_۰ = [\alpha]$ از طرفی $\alpha = a_۰ + \frac{۱}{[a_۱; a_۲, \ldots]}$ و با فرض $\alpha_۱ = [a_۱; a_۲, \ldots]$ داریم $a_۱ = [\alpha_۱]$.

با توجه به رابطه‌ی $\alpha = a_۰ + \frac{۱}{\alpha_۱}$ داریم $\alpha_۱ = \frac{۱}{\alpha - [\alpha]}$ و لذا $a_۱ = [\frac{۱}{\alpha - [\alpha]}]$. این روابط به ما کمک می‌کند تا یک عدد اصم داده شده را نیز به صورت یک کسر مسلسل بنویسیم. فرض کنیم $x_۰$ یک عدد اصم باشد. قرار می‌دهیم

$$x_۱ = \frac{۱}{x_۰ - [x_۰]}, \qquad x_۲ = \frac{۱}{x_۱ - [x_۱]}, \qquad x_۳ = \frac{۱}{x_۲ - [x_۲]}, \quad \ldots$$

و

$$a_۰ = [x_۰], \qquad a_۱ = [x_۱], \qquad a_۲ = [x_۲], \qquad a_۳ = [x_۳], \quad \ldots$$

یعنی برای هر k،

$$a_k = [x_k] \qquad x_{k+۱} = \frac{۱}{x_k - a_k}$$

اگر x_k اصم باشد، آن‌گاه $x_{k+۱}$ اصم است. چون $x_۰$ اصم است پس هر x_k اصم است و لذا روش فوق دنباله‌ای نامتناهی از اعداد صحیح $a_۰, a_۱, a_۲, \ldots$ تولید می‌کند. به علاوه چون $۰ < x_k - [x_k] < ۱$ لذا $x_{k+۱} > ۱$ و در نتیجه $a_k \geq ۱$ برای $k \geq ۱$. با علامات بالا داریم

$$\begin{aligned} x_۰ &= a_۰ + \frac{۱}{x_۱} = a_۰ + \frac{۱}{a_۱ + \frac{۱}{x_۲}} = a_۰ + \frac{۱}{a_۱ + \frac{۱}{a_۲ + \frac{۱}{x_۳}}} = \ldots \\ &= [a_۰; a_۱, a_۲, \ldots, a_n, x_{n+۱}] \quad \forall n \geq ۱ \end{aligned}$$

حال به‌راحتی ثابت می‌شود که

قضیه ۱۸.۷ با علامات بالا داریم $x_۰ = [a_۱; a_۲, a_۳, \ldots]$ لذا هر عدد اصم را می‌توان به صورت منحصر به فردی به شکل یک کسر مسلسل ساده‌ی نامتناهی نوشت.

گزاره ۱۹.۷ اگر $c_n = \frac{p_n}{q_n}$ همگرای n اُم عدد صحیح α باشد، آن‌گاه

$$|\alpha - \frac{p_n}{q_n}| < \frac{۱}{q_{n+۱} q_n} < \frac{۱}{q_n^۲}$$

اثبات. تمرین. □

مثال ۲۰.۷ عدد $\sqrt{۲}$ را به صورت یک کسر مسلسل می‌نویسیم

$$\begin{aligned} x_۰ &= \sqrt{۲} & a_۰ &= [x_۰] = ۱ \\ x_۱ &= \frac{۱}{x_۰ - [x_۰]} = \frac{۱}{\sqrt{۲} - ۱} = \sqrt{۲} + ۱ & a_۱ &= [x_۱] = ۲ \\ x_۲ &= \frac{۱}{x_۱ - [x_۱]} = \frac{۱}{\sqrt{۲} - ۱} = \sqrt{۲} + ۱ & a_۲ &= [x_۲] = ۲ \end{aligned}$$

لذا $\sqrt{۲} = [۱; ۲, ۲, \ldots] = [۱; \overline{۲}]$.

§۳.۷ تقریب اعداد با کسرهای مسلسل

خواص ارائه شده برای کسرهای مسلسل در تقریب اعداد با کسرهای مسلسل و محاسبه‌ی میزان دقت تقریب‌ها بسیار مفیداند. به مثال زیر توجه کنید:

مثال ۲۱.۷ $\sqrt{۲۳}$ **را به صورت یک کسر مسلسل می‌نویسیم.**

$$\begin{aligned}
x_۰ &= \sqrt{۲۳} & a_۰ &= [x_۰] = ۴\\
x_۱ &= \frac{۱}{\sqrt{۲۳}-۴} = \frac{\sqrt{۲۳}+۴}{۷} & a_۱ &= [x_۱] = ۱\\
x_۲ &= \frac{۱}{\frac{\sqrt{۲۳}+۴}{۷}-۱} = \frac{۷}{\sqrt{۲۳}-۳} = \frac{\sqrt{۲۳}+۳}{۲} & a_۲ &= [x_۲] = ۳\\
x_۳ &= \frac{۱}{\frac{\sqrt{۲۳}+۳}{۲}-۳} = \frac{۲}{\sqrt{۲۳}-۳} = \frac{\sqrt{۲۳}+۳}{۷} & a_۳ &= ۱\\
x_۴ &= \frac{۱}{\frac{\sqrt{۲۳}+۳}{۷}-۱} = \frac{۷}{\sqrt{۲۳}-۴} = \sqrt{۲۳}+۴ & a_۴ &= ۸\\
x_۵ &= \frac{۱}{\sqrt{۲۳}-۴} = x_۱
\end{aligned}$$

لذا تکرار شروع می‌شود. پس

$$\sqrt{۲۳} = \left[۴; \overline{۱, ۳, ۱, ۸}\right]$$

حال فرض کنیم عدد گویایی می‌خواهیم که $\sqrt{۲۳}$ را با تقریب کمتر از ۰/۰۰۰۱ تخمین زند. بنابر گزاره‌ی قبل

$$\left|\sqrt{۲۳} - \frac{p_n}{q_n}\right| < \frac{۱}{q_n^۲}$$

داریم

$$\begin{aligned}
p_۰ &= ۴ & q_۰ &= ۱\\
p_۱ &= ۵ & q_۱ &= ۱\\
p_۲ &= ۱۹ & q_۲ &= ۴\\
p_۳ &= ۲۴ & q_۳ &= ۵\\
p_۴ &= ۲۱۱ & q_۴ &= ۴۴\\
p_۵ &= ۲۳۵ & q_۵ &= ۴۹\\
p_۶ &= ۹۱۶ & q_۶ &= ۱۹۱
\end{aligned}$$

لذا $|\sqrt{۲۳} - \frac{۹۱۶}{۱۹۱}| < \frac{۱}{۱۹۱^۲}$ و لذا $\sqrt{۲۳} \approx \frac{۹۱۶}{۱۹۱}$ با تقریب خواسته شده.

اگر x یک عدد اصم باشد تقریب x با عددی گویا، کاربردهای فراوان دارد. می‌دانیم دنباله‌ای مانند $\{\alpha_n\}_{n\geq ۱}$ از اعداد گویا یافت می‌شود به‌نحوی که $\lim_{n\to\infty} \alpha_n = x$. و لذا اگر $\alpha_n = \frac{r_n}{s_n}$ که در آن r و s اعدادی صحیح هستند، می‌توان n را به اندازه‌ی کافی بزرگ اختیار کرد به‌نحوی که $|x - \frac{r_n}{s_n}|$ به اندازه‌ی دلخواه کوچک باشد. در عین حال برای صرفه‌جویی در محاسبات تلاش می‌کنیم $|r_n|$ و $|s_n|$ به اندازه‌ی ممکن کوچک باشند. اگر b عدد صحیح مثبت دلخواهی باشد آن‌گاه $\frac{c}{b} < x < \frac{c+۱}{b}$ برای

یک عدد صحیح c. لذا با یکی از دو انتخاب $a = c$ یا $a = c + ۱$ داریم

$$\left| x - \frac{a}{b} \right| < \frac{۱}{۲b}$$

قبلاً دیدیم اگر $c_n = \frac{p_n}{q_n}$ یک همگرای x باشد آن‌گاه

$$\left| x - \frac{p_n}{q_n} \right| < \frac{۱}{q_n^۲}$$

بنابراین اعداد گویای بدست آمده به عنوان همگراهای x با مخرج کوچکتر، تخمین بهتری برای x توسط اعداد گویا بدست می‌دهند.

برای اثبات روشن‌تر این مطلب در قضیه‌ی بعد، ابتدا لم زیر را داریم

لم ۲۲.۷ فرض کنیم $\frac{p_n}{q_n}$ همگرای n اُم عدد اصم x باشد و فرض کنیم a, b اعداد صحیح‌اند و $۱ \leq b \leq q_{n+۱}$. در این صورت $|q_n x - p_n| \leq |bx - a|$.

اثبات. دستگاه زیر را در نظر می‌گیریم

$$\begin{cases} p_n \alpha + p_{n+۱} \beta = a \\ q_n \alpha + q_{n+۱} \beta = b \end{cases}$$

با استفاده از رابطه‌ی $p_{n+۱} q_n - p_n q_{n+۱} = (-۱)^n$، از دستگاه فوق بدست می‌آید

$$\begin{cases} \alpha = (-۱)^{n+۱} (a\, q_{n+۱} - b\, p_{n+۱}) \\ \beta = (-۱)^{n+۱} (b\, p_n - a\, q_n) \end{cases}$$

چون $(p_{n+۱}, q_{n+۱}) = ۱$ ب.م.م و $b < q_{n+۱}$، به راحتی دیده می‌شود که $\alpha \neq ۰$ (ثابت کنید).

اگر $\beta = ۰$، به راحتی ثابت می‌شود که حکم لم برقرار است (ثابت کنید). پس فرض کنیم $\beta \neq ۰$. در این صورت $\alpha\, \beta < ۰$ (ثابت کنید)، همچنین چون x بین $\frac{p_n}{q_n}$ و $\frac{p_{n+۱}}{q_{n+۱}}$ قرار دارد، لذا $q_n\, x - p_n$ و $q_{n+۱}\, x - p_{n+۱}$ نیز مختلف العلامه اند. پس اعداد $\alpha\, (q_n\, x - p_n)$ و $\beta\, (q_{n+۱}\, x - p_{n+۱})$ هم‌علامت هستند. لذا

$$|b\, x - a| = |(q_n\, \alpha + q_{n+۱}\, \beta)\, x - (p_n\, \alpha + p_{n+۱}\, \beta)| = |\alpha (q_n\, x - p_n) + \beta\, (q_{n+۱}\, x - p_{n+۱})|$$

$$= |\alpha|\, |q_{n\, x} - p_n| + |\beta|\, |q_{n+۱}\, x - p_{n+۱}| > |\alpha|\, |q_n\, x - p_n| \geq |q_n\, x - p_n|$$

□

حال قضیه را ثابت می‌کنیم.

قضیه ۲۳.۷ اگر $\frac{p_n}{q_n}$ همگرای n اُم xباشد و $\frac{a}{b}$ عددی گویا باشد با $1 \leq b \leq q_n$. آن‌گاه

$$\left|x - \frac{p_n}{q_n}\right| \leq \left|x - \frac{a}{b}\right|$$

اثبات. به کمک لم قبل به سادگی اثبات می‌شود (تمرین). □

قضیه‌ی بعد نشان می‌دهد که هر تقریب خیلی خوب (به مفهومی) برای x یکی از همگراهای x است.

قضیه ۲۴.۷ فرض کنیم x عددی اصم و $\frac{a}{b}$، $b \geq 1$, $(a,b) = 1$ب.م.م، عددی گویا باشد به‌نحوی که

$$\left|x - \frac{a}{b}\right| < \frac{1}{2b^2}$$

در این صورت $\frac{a}{b}$ یکی از همگراهای x است.

اثبات. فرض کنیم چنین نباشد. n را چنان می‌گیریم که $q_n \leq b < q_{n+1}$. بنابر لم قبل

$$|q_n\, x - p_n| \leq |b\, x - a| = b\left|x - \frac{a}{b}\right| < \frac{1}{2b}$$

لذا

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{2bq_n}$$

چون بنا به فرض $\frac{a}{b} \neq \frac{p_n}{q_n}$ لذا $b\, p_n \neq a\, q_n$. در نتیجه

$$\frac{1}{bq_n} \leq \left|\frac{b\, p_n - a\, q_n}{bq_n}\right| = \left|\frac{p_n}{q_n} - \frac{a}{b}\right| \leq \left|\frac{p_n}{q_n} - x\right| + \left|x - \frac{a}{b}\right| < \frac{1}{2bq_n} + \frac{1}{2b^2}$$

از این نامساوی نتیجه می‌شود $q_n > b$ و این خلاف انتخاب n است. لذا حکم ثابت می‌شود. □

مثال ۲۵.۷ به کمک قضیه‌ی فوق به‌راحتی ثابت می‌شود که $\frac{18}{13}$ یکی از همگراهای $\frac{1+\sqrt{10}}{3}$ است.

§۴.۷ تمرین

۱. اعداد ذیل را به صورت کسر مسلسل ساده بنویسید

(الف) $\sqrt{۵}$

(ب) $\sqrt{۷}$

(پ) $\frac{۱۱+\sqrt{۳۰}}{۱۳}$

(ت) $\frac{۵+\sqrt{۳۷}}{۴}$

۲. نشان دهید برای هر عدد صحیح و مثبت n

(الف) $\sqrt{n^۲+۲n}=[n;\overline{۱,۲n}\,]$

(ب) $\sqrt{n^۲+۱}=[n;\overline{۲\,n}\,]$

۳. اعداد $\sqrt{۲}$، $\sqrt{۳}$، $\sqrt{۱۵}$، $\sqrt{۳۷}$ را به صورت کسر مسلسل ساده بنویسید.

۴. در میان همگراهای $\sqrt{۱۵}$ عدد گویایی بیابید که $\sqrt{۱۵}$ را تا ۴ رقم اعشار تخمین زند.

۵. اگر p و q اعداد صحیح و مثبتی باشند که در رابطه‌ی $x^۲-d\,y^۲=۱$ صدق می‌کنند، ثابت کنید $\frac{p}{q}$ یکی از همگراهای $\sqrt{d}$ است.

۶. دنباله‌ی اعداد فیبوناچی به صورت زیر تعریف می‌شود:

$$u_۱=u_۲=۱\ ,\ \ u_n=u_{n-۱}+u_{n-۲}\quad \forall n\geq ۳$$

(الف) ثابت کنید $\binom{n}{۱}u_۱+\binom{n}{۲}u_۲+\ldots+\binom{n}{n}u_n=u_{nn}$

(ب) ثابت کنید $-\binom{n}{۱}u_۱+\binom{n}{۲}u_۲+\ldots+(-۱)^n\binom{n}{n}u_n=-u_n$

(پ) ثابت کنید $u_۱+u_۳+u_۵+\ldots+u_{۲\,n-۱}=u_{۲n}$

(ت) $\frac{u_{n+۱}}{u_n}$ را به صورت یک کسر مسلسل ساده بنویسید و با استفاده از آن $\lim_{n\to\infty} \frac{u_{n+۱}}{u_n}$ را حساب کنید.

۷. در برخی جاها عدد π را به جای ۳/۱۴ با $\frac{۲۲}{۷}$ تقریب می‌زنند. نشان دهید $\frac{۲۲}{۷}$ یک همگرای π است.

۸. نشان دهید $\frac{۱۸}{۱۳}$ یکی از همگراهای $\frac{۱+\sqrt{۱۰}}{۳}$ است.

۹. کلیه‌ی جواب‌های مثبت معادله‌ی $x^۲ - ۵\,y^۲ = ۱$ با شرط $y < ۲۵۰$ را بیابید.

۱۰. اگر $\alpha = [a_۰, a_۱, \ldots]$ یک کسر مسلسل ساده باشد. ثابت کنید

(الف) $\frac{p_k}{p_{k-۱}} = [a_k; a_{k-۱}, \ldots, a_۱, a_۰]$.

(ب) $\frac{q_k}{q_{k-۱}} = [a_k; a_{k-۱}, \ldots, a_۲, a_۱]$.

۱۱. بهترین تقریب برای عدد π را در بین اعداد گویای با مخرج نابیشتر از ۱۰۰,۰۰۰ بیابید.

فهرست منابع و کتب برای مطالعه ی تکمیلی

[1] Apostol, T.A. , 1976. Introduction to Analytic Number Theory, New York: Springer-Verlag.

[2] Burton, David. 1997. The History of Mathematics: An Introduction. 3rd ed. New York: McGraw-Hill.

[3] Burton, D.M. , 1997. Elementary Number Theory, 4th ed. New York: McGraw-Hill.

[4] Hardy, G.H. , and E.M. Wright. 1992. An Introduction to the Theory of Numbers. 10th ed. London: oxford University Press.

[5] Ireland, K. , and M.Rosen. 1990. A classical Introduction to Modern Number Theory. 2nd ed. New York: Springer-Verlag.

[6] Koblitz, Neal. 1994. A Course in Number Theory and Cryptography, 2nd ed. New York: Springer-Verlag.

[7] Ore, Oystein. 1948. Number Theory and Its History, New York: McGraw-Hill.(Reprinted, New York:Dover,1988).

[8] Rosen, Kenneth. 1992. Elementary Number Theory and Its Application. 3rd ed. Reading, Mass.: Addison-Wesley.

فهرست الفبایی