بسم ا... الرحمن الرحیم

مقدمه‌ای بر

تئوری اعداد

قابل استفاده برای دانش‌آموزان داوطلب

شرکت در المپیاد ریاضی

مؤلف: مهدی صفا

سر شناسه	: صفا، مهدی، ۱۳۵۹ـ
عنوان و پدیدآور	: مقدمه‌ای بر تئوری اعداد / مؤلف مهدی صفا.
مشخصات نشر	: تهران: خوشخوان، ۱۳۸۶.
مشخصات ظاهری	: ۳۲۰ص: مصور.
شابک	: 964-8601-74-7
وضعیت فهرست‌نویسی	: فیپا
موضوع	: نظریه اعداد ـ ـ راهنمای آموزشی.
موضوع	: نظریه اعداد ـ ـ مسایل، تمرینها و غیره.
رده‌بندی کنگره	: QA ۲۴۱/م۷ص۷
رده‌بندی دیویی	: ۵۱۲/۷۰۷۶
شماره کتابخانه ملی	: ۸۵ـ۴۶۹۱۷م

مقدمه‌ای بر **تئوری اعداد**

مؤلف: مهدی صفا
حروفچینی: نساء پورحسین
چاپ دوم: پاییز ۱۳۸۹
تیراژ: ۲۰۰۰
قیمت: ۴۸۰۰ تومان

شابِک: ۹۶۴ـ۸۶۰۱ـ۷۴ـ۷ ISBN 964-8601-74-7

آدرس: تهران ـ خیابان جمهوری ـ خیابان دانشگاه شمالی ـ کوچه بهار ـ پلاک ۴ ـ طبقه دوم ـ تلفن: ۶۶۴۹۴۰۲۰

فهرست مطالب

مقدمه

نظریه‌ی اعداد مقدماتی یکی از مهمترین مباحثی است که در المپیاد ریاضی مورد توجه می‌باشد. هر چند دانش‌آموزان با مباحث اولیه‌ی آن مانند بخش‌پذیری و ب.م.م و ک.م.م از دوران راهنمایی آشنایی دارند ولی اضافه شدن مباحث جدیدی از جمله تابع فی‌اویلر و قضیه‌ی فرما که از سطح دبیرستان نیز فراتر می‌باشد، موجب جذابیت بیشتر این شاخه‌ی ریاضیات می‌شود. کتاب‌های فراوانی در زمینه‌ی نظریه‌ی اعداد مقدماتی تألیف و ترجمه شده است که به برخی از آن‌ها در قسمت مراجع اشاره شده است. مطالب برخی از این کتب تا حدی سطح بالا و شاید فهم آن برای دانش‌آموزان مشکل باشد و برخی از کتب نیز هر چند مطالب ساده‌ای دارند ولی به دلیل آنکه مدت زیادی از تألیف‌شان گذشته است، دارای سؤالات قدیمی و تکراری می‌باشد. دلایل فوق انگیزه‌ی تألیف کتابی است که اکنون پیش روی شماست. نویسنده سعی کرده است مطالب تا حد امکان ساده بیان شود و در ضمن تمام مطالب کاملاً برای داوطلبان المپیاد ریاضی مفید باشد. اشاره به این نکته ضروری است که این کتاب برای آمادگی شرکت در مرحله‌ی دوم المپیاد ریاضی نگاشته شده است و به نظر نویسنده یادگیری این مطالب برای شرکت در مرحله‌ی دوم المپیاد ریاضی لازم و البته کافی می‌باشد.

سؤالاتی که در مثال‌ها و یا مسایل پایانی فصل‌ها مطرح شده‌اند، غالباً از سوالات مهم و مشهور انتخاب شده‌اند و در ضمن سعی شده است تا حدودی نیز سؤالات جدید در آن‌ها گنجانده شود. یکی از نقاط قوت این کتاب تأکید آن در بررسی و حل معادلات سیاله می‌باشد که در فصل‌های ۹ و ۱۰ کاملاً به آن پرداخته شده است. در ضمن حل تمام مسایل پایانی فصل‌ها در قسمت پایانی کتاب موجود می‌باشد و البته فصل ۱۱ به سؤالات بدون حل اختصاص داده شده است تا دانش‌آموزانی که علاقه‌مند به حل کردن مسایل بیشتری هستند بتوانند خود را محک بزنند. حل سؤالات مرجع [۳] نیز که با مباحث این کتاب هماهنگی کامل دارد می‌تواند برای خوانندگان بسیار مفید باشد. در خاتمه لازم است از تمام عزیزانی که نویسنده را در تألیف کتاب یاری نموده‌اند تشکر شود و به خصوص از آقای محمد شریفی و آقای علی‌محمد باغستانی کمال تشکر به عمل می‌آید.

این کتاب فروتنانه تقدیم به شهداء و خانواده‌های محترم ایشان می‌گردد که بی‌شک حق بزرگی بر گردن همگان دارند.

مهدی صفا

پاییز ۱۳۸۵

فصل اول

بخش‌پذیری

نظریه‌ی اعداد شاخه‌ای از ریاضیات است که بر روی اعداد صحیح بحث می‌کند و به عبارت دیگر وقتی به متغیری مانند a در یک مسأله اشاره می‌شود، از پیش فرض می‌شود که a عددی صحیح است و نه گویا یا گنگ یا موهومی.

از دوران تحصیل ابتدایی می‌دانیم که جمع، تفریق و ضرب هر دو عدد صحیح باز هم عددی صحیح خواهد بود، ولی تقسیم آن‌ها لزوماً عددی صحیح نیست، بلکه گویا خواهد بود. در ضمن از همان سال‌های اوایل تحصیل فراگرفته‌ایم که چگونه یک عدد صحیح را بر دیگری تقسیم کنیم و خارج‌قسمت و باقی‌مانده را به‌دست آوریم. پس اجازه بدهید از همین مطلب ساده، بحث این کتاب را آغاز کنیم و قضیه‌ی الگوریتم تقسیم را بیان نماییم.

قضیه ۱-۱ (الگوریتم تقسیم)

فرض کنید a, b دو عدد صحیح باشند که داشته باشیم $b \neq 0$، در این صورت می‌توان اعداد صحیح و منحصر به‌فردی مانند r و q را یافت به نحوی که داشته باشیم:

$$a = bq + r$$

و عدد صحیح r در رابطه‌ی $0 \leqslant r < |b|$ صدق کند.

توضیح: در رابطه‌ی $a = bq + r$ در قضیه‌ی فوق، در واقع ما a را بر b تقسیم کرده‌ایم و به باقی‌مانده‌ی r و خارج‌قسمت q رسیده‌ایم. توجه کنید که به a مقسوم و به b مقسوم‌علیه گفته می‌شود.

نکته‌ی مهم دیگری که در قضیه‌ی بالا به چشم می‌خورد رابطه‌ی $\circ \leqslant r < |b|$ است که بیان می‌دارد باقی‌مانده‌ی r همواره کمتر از قدرمطلق مقسوم‌علیه و بزرگ‌تر یا مساوی صفر خواهد بود.

مثال ۱-۱ با فرض a, b داده شده در هر قسمت، باقی‌مانده و خارج‌قسمت تقسیم a بر b را بیابید.

الف) $a = ۸۵$، $b = ۱۳$

ب) $a = ۲۷$، $b = -۱۴$

ج) $a = n^۲ - ۱$، $b = n - ۱$ ($n \geqslant ۲$ طبیعی)

د) $a = n^۳$، $b = n - ۱$ ($n \geqslant ۳$ طبیعی)

راه حل: الف) به‌سادگی داریم $۸۵ = ۱۳ \times ۶ + ۷$ بنابراین $r = ۷$ و $q = ۶$.

ب) مشابهاً داریم $۲۷ = (-۱۴) \times (-۱) + ۱۳$ بنابراین $r = ۱۳$ و $q = -۱$.

ج) با توجه به اتحاد مزدوج داریم $n^۲ - ۱ = (n-۱)(n+۱) + \circ$ بنابراین $r = \circ$ و $q = n + ۱$.

د) با توجه به اتحاد سه‌جمله‌ای داریم $n^۳ - ۱ = (n-۱)(n^۲ + n + ۱)$ که نتیجه می‌دهد $n^۳ = (n-۱)(n^۲ + n + ۱) + ۱$ بنابراین داریم $r = ۱$ و $q = n^۲ + n + ۱$.

توجه کنید که در تمام قسمت‌های رابطه‌ی $\circ \leqslant r < |b|$ برقرار می‌باشد و در واقع در قسمت (د) شرط $n \geqslant ۳$ برای همین منظور لحاظ شده است.

مثال ۱-۲ ثابت کنید:

الف) اگر a عددی صحیح و دلخواه باشد، آنگاه a به‌صورت $۲k$ یا $۲k + ۱$ قابل نوشتن است که در آن k عددی صحیح است.

ب) اگر a عددی صحیح و دلخواه باشد، آنگاه a به‌صورت $۳k$ یا $۳k + ۱$ یا $۳k + ۲$ قابل نوشتن است که در آن k عددی صحیح است.

ج) اگر a عددی صحیح و دلخواه باشد و n عددی طبیعی باشد، آن‌گاه a به‌صورت یکی از اعداد nk یا $nk + ۱$ یا ... یا $nk + (n - ۱)$ قابل نوشتن است که در آن k عددی صحیح است.

راه حل: واضح است که قسمت (ج) حالت کلی قسمت‌های (الف) و (ب) است و با مقدارگذاری $n = ۲$ و $n = ۳$ به آن‌ها تبدیل می‌شود. در عین حال از اثبات قسمت (الف) صرف‌نظر کرده و به اثبات قسمت‌های (ب) و (ج) می‌پردازیم.

ب) در قضیه‌ی ۱-۱ فرض کنید $b = ۳$ باشد، پس اگر a را بر b تقسیم کنیم، می‌توان نوشت:

$$(q = k) \quad a = ۳k + r \quad \text{که} \quad ۰ \leqslant r < ۳$$

اکنون با توجه به رابطه‌ی $۰ \leqslant r < ۳$ واضح است که یکی از سه حالت زیر امکان دارد:

حالت ۱ : $r = ۰ \Longrightarrow a = ۳k$

حالت ۲ : $r = ۱ \Longrightarrow a = ۳k + ۱$

حالت ۳ : $r = ۲ \Longrightarrow a = ۳k + ۲$

بنابراین با توجه به مقدار باقی‌مانده r، یکی از حالات فوق اتفاق می‌افتد و اثبات مسأله کامل می‌شود.

ج) مشابه اثبات قسمت (ب)، اگر a را بر $b = n$ تقسیم کنیم، می‌توان نوشت:

$$a = nk + r \quad \text{که} \quad ۰ \leqslant r < n$$

در ادامه با توجه به رابطه‌ی $۰ \leqslant r < n$ ، r می‌تواند n مقدار متمایز زیر را داشته باشد:

$$r = n - ۱ \quad \text{یا} \quad \ldots \quad \text{یا} \quad r = ۱ \quad \text{یا} \quad r = ۰$$

که معادل هر کدام از مقادیر r، a را می‌توان به یکی از n حالت زیر نوشت:

$$a = nk + (n - ۱) \quad \text{یا} \quad \ldots \quad \text{یا} \quad a = nk + ۱ \quad \text{یا} \quad a = nk$$

مثال ۱-۳ پس از انجام یک عمل تقسیم، ۲۰ واحد به مقسوم‌علیه اضافه می‌کنیم و بدون تغییر دادن مقسوم‌علیه، عمل تقسیم را مجدداً انجام می‌دهیم. مشاهده می‌شود که خارج‌قسمت سه واحد اضافه می‌شود ولی باقی‌مانده چهار واحد کاهش می‌یابد. مطلوبست مقدار دقیق مقسوم‌علیه و تمام مقادیر ممکن برای باقی‌مانده‌ی عمل تقسیم اولیه.

راه حل: اگر تقسیم اولیه چنین باشد:

$$a = bq + r \qquad (۱)$$

با توجه به‌صورت مسأله در تقسیم دوم داریم:

$$a + ۲۰ = b(q + ۳) + (r - ۴) \qquad (۲)$$

اکنون از کم کردن روابط ۲ و ۱ به‌دست می‌آید:

$$۲۰ = ۳b - ۴ \Longrightarrow b = ۸$$

امّا از تقسیم اوّل می‌دانیم باید داشته باشیم $۸ > r \geqslant ۰$ و از تقسیم دوم باید داشته باشیم $۸ > r - ۴ \geqslant ۰$.
از دو رابطه‌ی اخیر به‌دست می‌آید $۸ > r \geqslant ۴$، یعنی r باقی‌مانده‌ی تقسیم اولیه می‌تواند یکی از مقادیر $۴, ۵, ۶, ۷$ را داشته باشد.

تعریف ۱-۱ برای هر عدد حقیقی x، جزء صحیح x که با نماد $\lfloor x \rfloor$ نمایش داده می‌شود، عدد صحیح و یکتایی تعریف می‌شود که برای آن داشته باشیم:

$$\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + ۱ \quad \text{یا معادلاً} \quad x - ۱ < \lfloor x \rfloor \leqslant x$$

برای مثال داریم $\lfloor ۲/۷۱ \rfloor = ۲$، $\lfloor ۰/۶۳ \rfloor = ۰$ و $\lfloor -۱/۳ \rfloor = -۲$.

تعریف ۱-۲ برای هر عدد حقیقی x، جزء اعشاری x که با نماد $\{x\}$ نمایش داده می‌شود، برابر $x - \lfloor x \rfloor$ تعریف می‌شود. برای مثال داریم $\{۲/۷۱\} = ۰/۷۱$، $\{۰/۶۳\} = ۰/۶۳$ و $\{-۱/۳\} = ۰/۷$.

مثال ۱-۴ اگر a, b دو عدد طبیعی باشند، ثابت کنید تعداد مضارب صحیح و مثبت b که از a کوچک‌تر هستند، برابر $\lfloor \frac{a}{b} \rfloor$ است.

راه حل: فرض کنید a را بر b تقسیم کنیم و بنویسیم:

$$a = bq + r\ , \quad ۰ \leqslant r < b$$

واضح است که $bq \leqslant a = bq + r < bq + b = b(q + ۱)$، پس داریم $bq \leqslant a < b(q + ۱)$. پس مضارب مثبت b که کمتر از a هستند، عبارتند از $b, ۲b, ۳b, \ldots, qb$، که تعداد آن‌ها q می‌باشد. امّا داریم $bq \leqslant a < b(q + ۱)$ پس به‌دست می‌آید $q \leqslant \frac{a}{b} < q + ۱$، اکنون به راحتی و با توجه به تعریف ۱-۱ می‌توان نوشت $q = \lfloor \frac{a}{b} \rfloor$. پس $\lfloor \frac{a}{b} \rfloor$ یا همان q، برابر تعداد مضارب مثبت b که کمتر از a هستند، می‌باشد.

مثال ۱-۵ الف) بین اعداد ۱۰۰ تا ۱۰۰۰ چند عدد مضرب ۱۷ وجود دارد؟

ب) اگر اعداد a, b, m طبیعی باشند و $a > b$ باشد، ثابت کنید تعداد مضارب m از عدد $b + ۱$ تا عدد a برابر $\lfloor \frac{a}{m} \rfloor - \lfloor \frac{b}{m} \rfloor$ می‌باشد.

راه حل: الف) تعداد مضارب ۱۷ بین اعداد ۱۰۰ تا ۱۰۰۰ برابر است با تعداد مضارب ۱۷ بین اعداد ۱ تا ۱۰۰۰، منهای تعداد مضارب ۱۷ بین اعداد ۱ تا ۱۰۰. پس با توجه به مثال ۱-۴ به‌دست می‌آید:

$$\text{تعداد مضارب ۱۷ بین ۱۰۰ تا ۱۰۰۰} = \lfloor \frac{۱۰۰۰}{۱۷} \rfloor - \lfloor \frac{۱۰۰}{۱۷} \rfloor = ۵۸ - ۵ = ۵۳$$

ب) مشابه راه حل قسمت (الف) سعی کنید از مثال ۱-۴ استفاده کنید.

در ادامه در قضیه‌ی ۱-۱ حالتی را در نظر می‌گیریم که $r = ۰$ باشد، یعنی داشته باشیم $a = bq$. در این صورت گوییم a مضرب b می‌باشد و به‌طور دقیق می‌توان تعریف زیر را انجام داد.

تعریف ۱-۳ عدد a بر عدد صحیح $b \neq ۰$ بخش‌پذیر است هرگاه باقی‌مانده‌ی تقسیم a بر b، برابر صفر باشد و به عبارت دیگر داشته باشیم $a = bk$. در این صورت می‌نویسیم $b|a$ و می‌خوانیم:

الف) عدد صحیح b، عدد صحیح a را عاد می‌کند.

ب) عدد صحیح b، عدد صحیح a را عاد می‌شمارد.

ج) b یک شمارنده‌ی a است.

د) b یک عامل a است.

نکته: دقت کنید اگر a بر b بخش‌پذیر نباشد می‌نویسیم $b \nmid a$.

مثال ۱-۶ درستی یا نادرستی هر یک از گزاره‌های زیر را مشخص کنید:

الف) $-۱۱|۱۳۲$

ب) $۷|۰$

ج) $a|a \quad (a \neq ۰)$

د) $a + ۲|a^۲ + a + ۳ \quad (a \in \mathbb{Z}$ دلخواه)

راه حل: الف) گزاره درست است زیرا داریم $(-۱۲) \times (-۱۱) = ۱۳۲$.

ب) گزاره درست است زیرا داریم $۰ \times ۷ = ۰$.

ج) گزاره درست است زیرا برای هر $a \neq ۰$ می‌توان نوشت $a = a \times ۱$.

د) گزاره نادرست است. برای مثال برای $a = ۱$ باید داشته باشیم $۳|۵$ که به‌وضوح اشتباه می‌باشد.

در ادامه‌ی بحث در قضیه‌ی ۱-۲، برخی از خواص و ویژگی‌های بخش‌پذیری را بیان و اثبات می‌کنیم.

قضیه ۱-۲ (خواص بخش‌پذیری)

فرض کنید a, b, c سه عدد صحیح و غیر صفر باشند، آنگاه داریم:

(۱) اگر $a|b \Longrightarrow a|-b\,, \quad -a|b\,, \quad -a|-b$

(۲) اگر $a|b \Longrightarrow |b| \geqslant |a|$

(۳) $a|a$

(۴) $a|0$

(۵) $1|a\ ,\ \ -1|a$

(۶) اگر $a|b\ ,\ \ b|c \Longrightarrow a|c$

(۷) اگر $a|b\ ,\ \ b|a \Longrightarrow a = \pm b$

(۸) اگر $a|1 \Longrightarrow a = \pm 1$

(۹) اگر $a|b\ ,\ \ a|c \Longrightarrow a|b+c\ ,\ \ a|b-c$

(۱۰) اگر $a|b \Longrightarrow a|bc$

(۱۱) فرض کنید $d \neq 0$ عددی صحیح باشد که داشته باشیم $c|d$ و $a|b$ ، آنگاه داریم $ac|bd$ ولی توجه کنید که نمی‌توان نتیجه گرفت $a+c|b+d$.

اثبات قضیه: از آنجایی که اثبات اکثر روابط به سادگی می‌تواند توسط خوانندگان انجام شود، تنها اثبات برخی از قسمت‌ها را انجام می‌دهیم و اثبات سایر قسمت‌ها را به عنوان تمرین به عهده‌ی خوانندگان می‌گذاریم.

$$(1)\qquad a|b \Longrightarrow b = ak \Rightarrow -b = a\times(-k) \Rightarrow a|-b\ \ (\text{زیرا}\ -k\in\mathbb{Z})$$

$$b = ak \Rightarrow b = (-a)\times(-k) \Rightarrow -a|b\ \ (\text{زیرا}\ -k\in\mathbb{Z})$$

$$b = ak \Rightarrow -b = (-a)\times(k) \Rightarrow -a|-b\ \ (\text{زیرا}\ k\in\mathbb{Z})$$

$$(2)\qquad a|b \Longrightarrow b = ak \Rightarrow |b| = |a|\times|k|$$

اکنون چون $b \neq 0$، پس $k \neq 0$ و لذا داریم $|k| \in \mathbb{N}$ یعنی $|k| \geqslant 1$، پس به‌دست می‌آید $|b| \geqslant |a|$.

$$(6)\qquad \left.\begin{aligned} a|b &\Longrightarrow b = ak_1 \\ b|c &\Longrightarrow c = bk_2 \end{aligned}\right\} \overset{\text{ضرب روابط}}{\Longrightarrow} c = a(k_1k_2) \Longrightarrow a|c$$

$$(7)\qquad \left.\begin{aligned} a|b &\Longrightarrow |b| \geqslant |a| \\ b|a &\Longrightarrow |a| \geqslant |b| \end{aligned}\right\} \Longrightarrow |a| = |b| \Longrightarrow a = \pm b$$

$$(9)\qquad \left.\begin{aligned} a|b &\Longrightarrow b = ak_1 \\ a|c &\Longrightarrow c = ak_2 \end{aligned}\right\} \Longrightarrow \begin{aligned} b+c = a(k_1+k_2) &\Longrightarrow a|b+c \\ b-c = a(k_1-k_2) &\Longrightarrow a|b-c \end{aligned}$$

$$(۱۰) \qquad a|b \implies b = ak \quad \overset{\text{ضرب در } c}{\implies} bc = a(ck) \implies a|bc$$

$$(۱۱) \qquad \left.\begin{array}{l} a|b \implies b = ak_۱ \\ c|d \implies d = ck_۲ \end{array}\right\} \overset{\text{ضرب روابط}}{\implies} bd = (ac) \times (k_۱k_۲) \implies ac|bd$$

برای رد کردن نتیجه‌ی اشتباه $a + c|b + d$، کافی است یک مثال نقض آورده شود. مثلاً داریم

$$\begin{array}{l} ۵|۱۰ \\ ۳|۹ \end{array} \implies ۵ + ۳|۱۰ + ۹ \implies ۸|۱۹$$ که به‌وضوح اشتباه است

تعریف ۱-۴ فرض کنید a, b دو عدد صحیح دلخواه باشند. برای هر دو عدد صحیح و دلخواه n و m عدد صحیح $ma + nb$ را یک ترکیب خطی از a و b گوییم. برای مثال اعداد $۳a + ۲b$، $۱۰a + ۷b$ و $۱۱a$ هر کدام ترکیبهای خطی از a و b می‌باشند.

قضیه ۱-۳ الف) اگر عدد صحیح c هر کدام از اعداد صحیح a و b را عاد کند، آنگاه c هر ترکیب خطی از a و b را هم عاد می‌کند.

ب) اگر c هر کدام از اعداد صحیح $a_۱, a_۲, \dots, a_k$ را عاد کند و اعداد صحیح و دلخواه $m_۱, m_۲, \dots, m_k$ مفروض باشند، آنگاه داریم

$$c|a_۱m_۱ + a_۲m_۲ + \cdots + a_km_k$$

اثبات قضیه: الف) با توجه به فرض داریم $c|b$ و $c|a$.

اکنون از رابطه‌ی (۱۰) و سپس (۹) در قضیه‌ی ۱-۲ استفاده می‌کنیم:

$$\left.\begin{array}{l} c|a \overset{(۱۰)}{\implies} c|ma \\ c|b \overset{(۱۰)}{\implies} c|nb \end{array}\right\} \overset{(۹)}{\implies} c|ma + nb$$

یعنی c هر ترکیب خطی مانند $ma + nb$ را هم عاد می‌کند.

ب) این قسمت در واقع حالت کلی قسمت قبل است و هم می‌توان اثباتی مشابه برای آن آورد و هم می‌توان برای اثبات به روش زیر عمل کرد:

برای هر $۱ \leqslant i \leqslant k$ داریم $c|a_i$، پس اعداد $q_۱, q_۲, \dots, q_k$ موجودند که داشته باشیم $a_i = cq_i$.

اکنون iامین رابطه را در m_i ضرب می‌کنیم، به عبارت دیگر داریم:

$$a_i = cq_i \implies a_im_i = c \times (q_im_i) \qquad (k \geqslant i \geqslant ۱)$$

اکنون کافی است این روابط را برای $i = 1, 2, \ldots, k$ با هم جمع کنیم و به‌دست آوریم:

$$\begin{aligned} a_1 m_1 + a_2 m_2 + \cdots + a_k m_k &= c(q_1 m_1 + q_2 m_2 + \cdots + q_k m_k) \\ &\Longrightarrow c | a_1 m_1 + a_2 m_2 + \cdots + a_k m_k \end{aligned}$$

مثال ۱-۷ الف) برای هر عدد طبیعی n ثابت کنید $2 | n(n+1)$

ب) برای هر عدد طبیعی n ثابت کنید $3 | n(n+1)(n+2)$

راه حل: الف) با توجه به مثال ۱-۲ می‌دانیم هر عدد طبیعی مانند n یا به صورت $2k$ است و یا $2k+1$، در هر حالت داریم:

$$\text{اگر} \quad n = 2k \Longrightarrow n(n+1) = 2k(2k+1) \Rightarrow 2 | n(n+1)$$

$$\begin{aligned} \text{اگر} \quad n = 2k+1 \Longrightarrow n(n+1) &= (2k+1)(2k+2) = 2(2k+1)(k+1) \\ &\Rightarrow 2 | n(n+1) \end{aligned}$$

ب) با توجه به مثال ۱-۲ می‌دانیم هر عدد طبیعی به یکی از سه صورت $3k$ یا $3k+1$ یا $3k+2$ است، در هرکدام از این حالات داریم:

$$\text{اگر} \quad n = 3k \Longrightarrow 3 | n \Rightarrow 3 | n(n+1)(n+2)$$

$$\text{اگر} \quad n = 3k+1 \Longrightarrow 3 | n+2 \Rightarrow 3 | n(n+1)(n+2)$$

$$\text{اگر} \quad n = 3k+2 \Longrightarrow 3 | n+1 \Rightarrow 3 | n(n+1)(n+2)$$

پس در همه‌ی حالات داریم $3 | n(n+1)(n+2)$ و حکم مورد نظر اثبات می‌شود.

مثال ۱-۸ ثابت کنید مربع هر عدد فرد به صورت $8k+1$ است.

اثبات: اگر فرض کنیم $a = 2n+1$ عددی فرد باشد، داریم:

$$a^2 = (2n+1)^2 = 4n^2 + 4n + 1 = 4n(n+1) + 1 = 8k + 1$$

در رابطه‌ی بالا از قسمت (الف) مثال ۱-۷ استفاده شد که در واقع داریم $n(n+1) = 2k$.

مثال ۱-۹ اگر a و b دو عدد صحیح باشند، ثابت کنید $a^2 - b^2$ نمی‌تواند به صورت $4k+2$ باشد.

راه حل: با استفاده از برهان خلف فرض کنید داشته باشیم $a^۲ - b^۲ = ۴k + ۲$. چون $a^۲ - b^۲$ عددی زوج است پس یا هر دوی a و b اعدادی فرد هستند، یا هر دو زوج می‌باشند. اگر a و b هر دو اعدادی فرد باشند آنگاه طبق مثال ۱-۸ داریم:

$$a^۲ = ۸\ell + ۱\ ,\ \ b^۲ = ۸t + ۱ \Longrightarrow a^۲ - b^۲ = ۸(\ell - t)$$

که به‌وضوح مضرب ۸ است و نمی‌تواند به صورت $۴k + ۲$ باشد.

در حالت بعدی اگر a و b هر دو زوج باشند هم داریم:

$$a^۲ = (۲\ell)^۲ = ۴\ell^۲\ ,\ \ b^۲ = ۴t^۲ \Longrightarrow a^۲ - b^۲ = ۴(\ell^۲ - t^۲)$$

که مضرب ۴ است و باز هم نمی‌تواند به صورت $۴k + ۲$ باشد.

مثال ۱-۱۰ الف) با فرض $a|b$ ثابت کنید $a^n|b^n$، که n عددی طبیعی و دلخواه است.

ب) آیا لزوماً از رابطه‌ی $a^۲|b^۳$، می‌توان نتیجه گرفت $a|b$؟

راه حل: **الف)** اگر $a|b$ خواهیم داشت $b = ak$. طرفین را به توان n می‌رسانیم:

$$b^n = a^n \times (k^n) = a^n k' \Longrightarrow a^n|b^n$$

ب) خیر، لزوماً نمی‌توان چنین نتیجه‌ای گرفت. برای مثال نقض فرض کنید قرار دهیم $b = ۳^۲$ و $a = ۳^۳$، واضح است که داریم $a^۲ = b^۳ = ۳^۶$ پس $a^۲|b^۳$، ولی داریم $۳^۳ \nmid ۳^۲$.

یادآوری چند اتحاد مهم: در ادامه به عنوان یادآوری به سه اتحاد مهم که در این فصل و فصول دیگر کاربرد دارند، اشاره می‌کنیم و اثبات آن‌ها را به عهده‌ی خوانندگان می‌گذاریم.

اتحاد اوّل: اگر n عددی طبیعی و دلخواه باشد و a و b دو عدد حقیقی باشند، داریم:

$$a^n - b^n = (a - b)(a^{n-۱} + a^{n-۲}b + \cdots + ab^{n-۲} + b^{n-۱})$$

اتحاد دوم: اگر n عددی طبیعی و فرد باشد و a و b دو عدد حقیقی باشند، داریم:

$$a^n + b^n = (a + b)(a^{n-۱} - a^{n-۲}b + a^{n-۳}b^۲ - \cdots - ab^{n-۲} + b^{n-۱})$$

اتحاد سوم: اگر n عددی طبیعی و دلخواه باشد و a و b دو عدد حقیقی باشند، داریم:

$$(a + b)^n = a^n + \binom{n}{۱} a^{n-۱}b + \binom{n}{۲} a^{n-۲}b^۲ + \cdots + \binom{n}{n-۱} ab^{n-۱} + b^n$$

دقت کنید که ضرایب $\binom{n}{k}$ به صورت زیر تعریف می‌شوند:

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

و داریم $n! = ۱ \times ۲ \times ۳ \times \cdots \times n$ (n عددی طبیعی) که n **فاکتوریل** خوانده می‌شود.

مثال ۱-۱۱ الف) ثابت کنید $۲^۳|۳^{۱۰۰} - ۱$.

ب) ثابت کنید $۱۷|۳^{۳۰} + ۵^{۳۰}$

ج) برای هر عدد طبیعی n، ثابت کنید $n^۲|(n+۱)^n - ۱$.

راه حل: الف) از اتحاد اوّل استفاده می‌کنیم. باید ثابت کنیم:

$$۸|۳^{۱۰۰} - ۱ \Longrightarrow ۸|۹^{۵۰} - ۱$$

این هم بدیهی است، زیرا کافی است در اتحاد اوّل قرار دهیم $n = ۵۰\ ,\ \ b = ۱\ ,\ \ a = ۹$.

ب) با توجه به اتحاد دوم داریم:

$$۳^{۳۰} + ۵^{۳۰} = ۹^{۱۵} + ۲۵^{۱۵} = (۹ + ۲۵)(۹^{۱۴} - ۹^{۱۳} \times ۲۵ + \cdots - ۹ \times ۲۵^{۱۳} + ۲۵^{۱۴}) = ۳۴k$$

توجه کنید که چون ۱۵ عددی فرد است می‌توان از اتحاد دوم استفاده کرد. از روابط بالا داریم $۳۴|۳^{۳۰} + ۵^{۳۰}$ پس به‌وضوح باید داشته باشیم $۱۷|۳^{۳۰} + ۵^{۳۰}$.

ج) از اتحاد سوم استفاده می‌کنیم:

$$\begin{aligned}(n+۱)^n &= n^n + \binom{n}{۱}n^{n-۱} + \cdots + \binom{n}{n-۲}n^۲ + \binom{n}{n-۱}n + ۱ \\ &= n^۲k + \binom{n}{n-۱}n + ۱\end{aligned}$$

از طرفی داریم $\binom{n}{n-۱} = \binom{n}{۱} = n$، پس می‌توان نوشت:

$$(n+۱)^n = n^۲k + n^۲ + ۱$$

که معادل رابطه‌ی $(n+۱)^n - ۱ = n^۲(k+۱)$ است و لذا اثبات می‌شود $n^۲|(n+۱)^n - ۱$.

مثال ۱-۱۲ فرض کنید برای اعداد x و y داریم $۱۱|۵x+۹y$، ثابت کنید باید رابطه‌ی زیر هم برقرار باشد:

$$۱۱|۳x+y$$

راه حل: در این گونه مسایل یک روش این است که آنقدر فرض مسأله را ساده کنیم تا به حکم برسیم و یک روش دیگر این است که فرض کنیم حکم مسأله هم درست است و سپس با ساده‌سازی روابط به یک گزاره‌ی بدیهی برسیم.

ما از روش اوّل استفاده می‌کنیم. با توجه به خواص بخش‌پذیری که قبلاً معرفی شدند داریم:

$$۱۱|۵x+۹y \overset{\times ۵}{\Longrightarrow} ۱۱|۲۵x+۴۵y \Longrightarrow ۱۱|(۲۲x+۴۴y)+(۳x+y)$$

امّا می‌دانیم که به‌وضوح داریم $۱۱|۲۲x+۴۴y$، پس باید داشته باشیم $۱۱|۳x+y$ که همان خواسته‌ی مسأله می‌باشد.

مثال ۱-۱۳ اگر m و n دو عدد طبیعی باشند و تعریف کنیم $F(m)=۱^m+۲^m+\cdots+n^m$، ثابت کنید:

الف) $F(۱)|۳F(۲)$

ب) $F(۱)|F(۳)$

راه حل: برای حل این مسأله ابتدا روابط زیر را که خوانندگان می‌توانند به راحتی با استقراء آن‌ها را ثابت کنند، یادآوری می‌کنیم:

$$F(۱)=۱+۲+\cdots+n=\frac{n(n+۱)}{۲}$$

$$F(۲)=۱^۲+۲^۲+\cdots+n^۲=\frac{n^۲}{۲}+\frac{n^۳}{۳}+\frac{n}{۶}=\frac{n(n+۱)(۲n+۱)}{۶}$$

$$F(۳)=(F(۱))^۲=(\frac{n(n+۱)}{۲})^۲$$

با توجه به این روابط، اثبات قسمت‌های (الف) و (ب) کار ساده‌ای خواهد بود و به عهده‌ی خواننده‌ی گرامی گذاشته می‌شود.

مثال ۱-۱۴ اگر اعداد a، b، x و y صحیح باشند و $x\neq y$، و عدد $A=ax+by$ بر $x-y$ بخش‌پذیر باشد، ثابت کنید عدد $B=(a+b)(x+y)$ هم بر $x-y$ بخش‌پذیر است.

راه حل: داریم $x-y|ax+by$ و می‌خواهیم ثابت کنیم $x-y|(ax+by)+(ay+bx)$، بنابراین کافی است ثابت کنیم $x-y|ay+bx$، این هم واضح است زیرا می‌توان نوشت:

$$x-y|(x-y)(a-b) \Longrightarrow x-y|(ax+by)-(ay+bx) \Longrightarrow x-y|ay+bx$$

و اثبات مسأله کامل می‌شود.

مثال ۱-۱۵ (کانادا ۱۹۶۹) ثابت کنید اعداد صحیح a، b و c وجود ندارند که برای آن‌ها داشته باشیم:

$$a^۲+b^۲-۸c=۶$$

راه حل: توجه کنید اگر بنویسیم $a^۲+b^۲=۸c+۶$، صورت مسأله به این حالت تبدیل می‌شود که $a^۲+b^۲$ نمی‌تواند به صورت $۸c+۶$ باشد یعنی باقی‌مانده‌ی $a^۲+b^۲$ بر ۸، برابر ۶ نیست. ابتدا توجه کنید طبق مثال ۱-۸ اگر a عددی فرد باشد آنگاه باقی‌مانده‌ی $a^۲$ بر ۸ برابر یک خواهد بود ولی اگر a زوج باشد دو حالت داریم:

$$a=۴k+۲ \Longrightarrow a^۲=۱۶k^۲+۱۶k+۴ \Longrightarrow a^۲=۸t+۴$$
$$a=۴k \qquad \Longrightarrow a^۲=۱۶k^۲ \Longrightarrow a^۲=۸t$$

پس در حالت زوج بودن a، باقی‌مانده‌ی $a^۲$ بر ۸، برابر ۰ یا ۴ است. پس در کل باقی‌مانده‌ی $a^۲$ بر ۸ برابر یکی از اعداد $\{۰,۱,۴\}$ می‌باشد. مشابهاً برای $b^۲$ نیز چنین مطلبی برقرار است. اکنون با بررسی تمام حالات مختلف برای باقی‌مانده‌های $a^۲$ و $b^۲$، به سادگی معلوم است که مجموعه‌ی باقی‌مانده‌های $a^۲+b^۲$ بر ۸ به صورت $\{۰,۱,۲,۴,۵\}$ است و لذا ۶ را شامل نمی‌شود.

مثال ۱-۱۶ (مقدماتی آمریکا ۱۹۸۳) باقی‌مانده‌ی عدد $۶^{۸۳}+۸^{۸۳}$ را بر ۴۹ بیابید.

راه حل: جواب مسأله ۳۵ است. از سومین اتحاد معرفی شده در این فصل استفاده می‌کنیم و می‌نویسیم:

$$A=۶^{۸۳}+۸^{۸۳}=(۷-۱)^{۸۳}+(۷+۱)^{۸۳}$$
$$=\left[۷^{۸۳}-\binom{۸۳}{۱}۷^{۸۲}+\cdots+\binom{۸۳}{۱}۷-۱\right]+\left[۷^{۸۳}+\binom{۸۳}{۱}۷^{۸۲}+\cdots+\binom{۸۳}{۱}۷+۱\right]$$

اکنون با توجه به این که داریم $۷^۲=۴۹$، عبارت بالا را می‌توان به صورت زیر نوشت:

$$A=۴۹k+\binom{۸۳}{۱}۷-۱+۴۹t+\binom{۸۳}{۱}۷+۱=۴۹(k+t)+۱۶۶\times۷$$

اکنون به‌وضوح داریم $۱۶۶=۷\times۲۳+۵$ پس داریم:

$$A=۴۹(k+t+۲۳)+۳۵$$

پس باقی‌مانده‌ی مورد نظر برابر ۳۵ است.

مسایل پایانی فصل اوّل

۱) ثابت کنید به ازای هر عدد صحیح و دلخواه a، دقیقاً یکی از اعداد a، $a + ۱۳$ و $a + ۸۶$ بر ۳ بخش‌پذیر هستند.

۲) نشان دهید رقم یکان یک مربع کامل فقط می‌تواند یکی از اعضای مجموعه‌ی $\{۰, ۱, ۴, ۵, ۶, ۹\}$ باشد.

۳) ثابت کنید مربع هر عدد طبیعی یا به شکل $۳k$ است و یا $۳k + ۱$، به عبارت دیگر مربع هیچ عدد طبیعی نمی‌تواند به شکل $۳k + ۲$ باشد.

۴) برای هر عدد طبیعی n ثابت کنید $۴ \nmid n^۲ + ۲$.

۵) تمام اعداد طبیعی n را بیابید که به ازای آن‌ها عدد $n^۲ + ۱$ بر $n + ۱$ بخش‌پذیر باشد.

۶) ثابت کنید اگر $a^۲ + b^۲$ بر ۳ بخش‌پذیر باشد آنگاه باید هرکدام از a و b نیز بر ۳ بخش‌پذیر باشند.

۷) ثابت کنید اگر داشته باشیم $۷|a^۲ + b^۲$ آنگاه خواهیم داشت $۷|a$ و $۷|b$.

۸) برای هر عدد طبیعی $k \geqslant ۲$ تعریف می‌کنیم $a_k = \underbrace{۱۱۱\ldots۱}_{k \text{ بار}}$. ثابت کنید:

الف) هیچ‌یک از a_kها مربع کامل نیستند.

ب) هیچ‌یک از a_kها به صورت مجموع دو مربع کامل نیستند.

۹) (مقدماتی آمریکا ۱۹۸۷) اگر برای اعداد صحیح m و n داشته باشیم $m^۲ + ۳m^۲n^۲ = ۳۰n^۲ + ۵۱۷$، مقدار $۳m^۲n^۲$ را بیابید.

۱۰) ثابت کنید:

$$۵|۱^{۱۰۱} + ۲^{۱۰۱} + ۳^{۱۰۱} + ۴^{۱۰۱}$$

۱۱) با فرض $۷|۳n + ۱$ ثابت کنید $۴۹|۲۷n^۲ + ۳۹n + ۱۰$.

۱۲) برای عدد طبیعی و دلخواه n روابط زیر را اثبات کنید:

الف) $۸|۹^n + ۷$

ب) $۲^{۱۱}|۳^{۵۱۲} - ۱$

ج) $۵|۲^{۴n-۲} + ۱$

د) $۸|۵^n + ۲ \times ۳^{n-۱} + ۱$

ه) $\text{۸} \nmid \text{۳}^n + \text{۱}$

۱۳) ثابت کنید حاصل‌ضرب هر سه عدد متوالی بر ۶ بخش‌پذیر است.

۱۴) ثابت کنید اگر a عددی فرد باشد آنگاه $a^{\text{۴}}$ به صورت $\text{۱۶}k + \text{۱}$ خواهد بود.

۱۵) فرض کنید m و n دو عدد فرد باشند، ثابت کنید:

الف) $\text{۸}|m^{\text{۲}} - n^{\text{۲}}$

ب) $\text{۱۶}|m^{\text{۴}} + n^{\text{۴}} + \text{۱۴}$

۱۶) تمام اعدادی مانند d را بیابید که d هر دو عدد صحیح $a - \text{۳}$ و $a^{\text{۲}} - \text{۴}a + \text{۲}$ را عاد کند.

۱۷) ثابت کنید تفاضل مکعبات دو عدد صحیح متوالی به صورت $\text{۶}k \pm \text{۱}$ خواهد بود.

۱۸) برای مطرح کردن این مسأله به تعریف زیر نیازمندیم:

تعریف: مجموعه‌ی A را تحت عمل x بسته می‌گوییم اگر برای هر دو عضو در A که تحت عمل x واقع شوند، عضو جدیدی که حاصل می‌شود باز هم درون A باشد. برای مثال مجموعه‌ی اعداد صحیح $\mathbb{Z}$ تحت عمل جمع بسته است چون جمع هر دو عدد صحیح باز هم عددی صحیح می‌شود ولی مجموعه‌ی اعداد طبیعی $\mathbb{N}$ نسبت به عمل تفریق یا تقسیم بسته نمی‌باشند. با این توضیح، ثابت کنید:

الف) مجموعه‌ی اعداد صحیح به صورت $\text{۴}k + \text{۱}$ نسبت به عمل ضرب بسته هستند.

ب) مجموعه‌ی اعداد صحیح به صورت $\text{۴}k + \text{۳}$ نسبت به عمل ضرب بسته نیستند.

ج) مجموعه‌ی اعداد طبیعی به صورت $a^{\text{۲}} + b^{\text{۲}}$ نسبت به عمل ضرب بسته هستند.

۱۹) ثابت کنید اگر $a \nmid \text{۷}$ و $b \nmid \text{۷}$ آنگاه داریم: $\text{۷}|a^{\text{۶}} - b^{\text{۶}}$.

۲۰) ثابت کنید به ازای هر عدد صحیح a داریم $\text{۵}|a^{\text{۵}} - a$.

۲۱) ثابت کنید مجموع مکعبات سه عدد متوالی همواره بر ۹ بخش‌پذیر است.

۲۲) تمام اعداد طبیعی n را بیابید که $\text{۵}^n + \text{۳}^n$ بر $\text{۵}^{n-\text{۱}} + \text{۳}^{n-\text{۱}}$ بخش‌پذیر باشد.

۲۳) (مقدماتی آمریکا ۱۹۸۶) بزرگ‌ترین عدد طبیعی n را بیابید که داشته باشیم: $n + \text{۱۰}|n^{\text{۳}} + \text{۱۰۰}$.

۲۴) (فنلاند ۱۹۹۲) برای هر عدد طبیعی n بزرگ‌ترین عدد k را بیابید که $\text{۲}^k|\text{۳}^n + \text{۱}$.