

# ۱۰۴ مسئله تئوری اعداد




گردآوری و تألیف:

تیتو آندرسکو

مترجم:

سعید نعمتی





انتشارات خوشخوان

# پیشگفتار ناشر

مسابقه‌ها، کنکورها و المپیادهای علمی نقش عمده‌ای در بارور کردن و شکفتن استعدادهای دانش آموزان ایفا می‌کنند و باید به جرأت ادعا کرد که این مسابقات توانسته‌اند اعتماد به نفس لازم در جوانان عزیز کشورمان برای رقابت علمی با جوانان سایر نقاط جهان را تا حد زیادی افزایش دهند. کتاب‌های موجود در دوره‌های تحصیلی به هیچ عنوان نمی‌توانند دانش‌آموزان را برای آماده شدن در این رقابت‌ها اغنا کنند، لذا لازم است در کنار کتاب‌های درسی، خلأ موجود خصوصاً برای دانش‌آموزان مستعد و ممتاز شناسایی و پر شود. در همین راستا **انتشارات خوشخوان** با استعانت از حضرت حق تعالی و به کمک تنی چند از اساتید و دبیران ممتاز ایران و نیز فارغ‌التحصیلان دانشگاه‌های مختلف که اغلب آنان در زمانی نه چندان دور، مدال‌آور المپیادهای علمی در سطح ایران و جهان بوده‌اند، کتاب‌هایی را تألیف و به دانش‌آموزان ارائه می‌نماید. امید است مورد پسند و استفاده‌ی دانش‌آموزان و دبیران این مرز و بوم قرار گیرند.

# فهرست


پیشگفتار مؤلفان ..... *vii*

فهرست علائم و اختصارات ..... *ix*

اصول تئوری اعداد ..... ۱

بخشپذیری ..... ۱

الگوریتم تقسیم ..... ۵

اعداد اول ..... ۶

قضیه بنیادی حساب ..... ۸

بزرگ‌ترین مقسوم علیه مشترک ..... ۱۳

الگوریتم اقلیدس ..... ۱۴

قضیه بزو ..... ۱۶

کوچک‌ترین مضرب مشترک ..... ۱۹

تعداد مقسوم‌علیه‌ها ..... ۲۰

مجموع مقسوم‌علیه‌ها ..... ۲۳

حساب پیمانه‌ای (همنهشتی) ..... ۲۴

دستگاه مانده‌ها ..... ۲۹

قضیه کوچک فرما و قضیه اویلر ..... ۳۳

تابع $\varphi$ اویلر ..... ۴۰
تابع ضربی ..... ۴۲
معادلات دیوفانتین خطی ..... ۴۵
دستگاه‌های عددی ..... ۴۸
شرایط بخش‌پذیری در دستگاه دهدهی ..... ۵۴
تابع جزء صحیح (تابع کف) ..... ۶۱
تابع لژاندر ..... ۷۶
اعداد فرما ..... ۸۲
اعداد مرسن ..... ۸۳
اعداد تام (کامل) ..... ۸۳

مسائل مقدماتی ..... ۸۷
مسائل پیشرفته ..... ۹۵
پاسخ مسائل مقدماتی ..... ۱۰۳
پاسخ مسائل پیشرفته ..... ۱۳۵
تعاریف و قضایا ..... ۱۸۷
منابعی برای مطالعه بیشتر ..... ۱۹۵
واژه نامه ..... ۱۹۶

# پیش‌گفتار مؤلفان

این کتاب شامل ۱۰۴ تا از بهترین مسائلی است که در تمرین و سنجش تیم المپیاد ریاضی بین‌المللی (*IMO*) ایالات متحده استفاده شده است. این مسائل صرفاً مجموعه‌ای از سؤالات خیلی مشکل نیستند بلکه به تدریج تکنیک‌ها و مهارت‌های دانش‌آموزان در تئوری اعداد را می‌سازند. بخش اول معرفی جامعی از تئوری اعداد و ساختارهای ریاضی آن ارائه می‌کند. از این بخش می‌توان به عنوان جزوه درسی برای دوره‌های کوتاه تئوری اعداد استفاده کرد. این کتاب به بهبود دید ریاضی دانش‌آموزان و آمادگی بهتر آنان برای شرکت در مسابقات مختلف ریاضی کمک می‌کند. علاوه بر آن با افزایش توانایی‌های دانش‌آموزان در حل مسائل، سبب غنای آنان در شاخه‌های مهم تئوری اعداد می‌شود. این کتاب علاقه‌ی دانش‌آموزان را برای مطالعه‌ی بیشتر در ریاضیات برمی‌انگیرد.

در ایالات متحده آمریکا، فرآیند انتخاب شرکت‌کنندگان در مسابقات جهانی المپیاد ریاضی (IMO) شامل چند مسابقه ملی است که مسابقه‌ی ریاضی آمریکا ویژه دانش‌آموزان سال دهم (AMC10)، مسابقه‌ی ریاضی آمریکا ویژه دانش‌آموزان سال دوازدهم (AMC12)، آزمون انتخابی ریاضی آمریکا (AIME) و المپیاد ریاضی ایالات متحده آمریکا (USAMO) نامیده می‌شود. شرکت در آزمون‌های AIME و USAMO با دعوت‌نامه و بر مبنای عملکرد در آزمون‌های قبلی می‌باشد. برنامه‌ی تابستانی المپیاد ریاضی (MOSP) یک برنامه‌ی تمرینی فشرده به مدت چهار هفته است که تقریباً برای ۵۰ دانش‌آموزی که به صدر رقابت‌های ریاضی آمریکا رسیده‌اند برگزار می‌شود. شش دانش‌آموزی که به نمایندگی از آمریکا در IMO شرکت می‌کنند بر مبنای نمراتشان در USAMO و آزمون‌هایی که در طول MOSP برگزار شده است، انتخاب می‌شوند. در طول MOSP کلاس‌ها و مجموعه‌ی سؤالاتی که به دانش‌آموزان داده می‌شود برای آمادگی کامل آنها در چند شاخه مهم از ریاضیات است. این موضوعات شامل استدلال‌های ترکیباتی، توابع مولد، نظریه گراف، روابط بازگشتی، مجموع‌ها و حاصل‌ضرب‌ها، احتمالات، تئوری اعداد، چند جمله‌ای‌ها، معادلات تابعی، اعداد مختلط در هندسه، اثبات‌های الگوریتمی، هندسه پیشرفته و ترکیباتی و نامساوی‌های کلاسیک می‌باشد.

آزمون‌هایی مانند آزمون المپیاد شامل چندین مسأله چالش‌برانگیز هستند. پاسخ صحیح اغلب نیاز به تحلیل عمیق و استدلال دقیق دارد. سؤالات المپیاد ممکن است برای افراد مبتدی غیر قابل نفوذ به نظر برسد اما اکثر آنها را می‌توان با روش‌های ریاضی دبیرستانی حل کرد.

در این‌جا چند پیشنهاد برای دانش‌آموزانی که برای حل مسائل تلاش می‌کنند، ارائه می‌کنیم:

- نگران زمان نباشید! افراد بسیار محدودی می‌توانند همه‌ی مسائل را حل کنند.
- سعی کنید بین مسائل ارتباط برقرار کنید. یک نکته مهم برای این کار این است که به همه‌ی روش‌ها و ایده‌های مهم که در کتاب مطرح شده‌اند بیش از یک‌بار اشاره شده است.
- مسائل المپیاد به سرعت شکست نمی‌خورند. صبور باشید. روش‌های مختلف را امتحان کنید. آزمایش با حالت‌های ساده و در برخی، بازگشت به عقب از حکم موردنظر، می‌تواند مفید باشد.
- حتی اگر توانستید یک مسأله را حل کنید، پاسخ را دوباره بخوانید. ممکن است نکاتی را در راه‌حل‌تان فراموش کرده باشید که روش‌ها و تاکتیک‌هایی که در جای دیگر استفاده کرده‌اید توجیه می‌کنند. وقتی پاسخ را می‌خوانید سعی کنید تفکری که منجر به آن شده است را بازسازی کنید. از خودتان بپرسید «ایده‌ی کلیدی چه بوده است؟ چگونه می‌توان این ایده‌ها را فراتر از این به کار برد؟»
- بعداً به مسأله‌ی اصلی برگردید و ببینید آیا می‌توانید آن را از روش دیگری حل کنید. اکثر مسائل چندین راه‌حل دارند اما همه‌ی آنها اینجا مطرح نمی‌شوند.
- افزایش توانایی در حل مسأله نیاز به تمرین دارد. اگر در ابتدا دچار مشکل شدید مأیوس و دلسرد نشوید. برای تمرین بیشتر از کتاب‌هایی که در انتها فهرست شده‌اند استفاده کنید.

تیتو آندریسکو

دورین آندریکا

زومینگ فنگ

اکتبر ۲۰۰۶

# فهرست علائم و اختصارات

## اختصارات

| | |
|---|---|
| AHSME | American High School Mathematics Examination |
| | آزمون ریاضی دبیرستانی آمریکا |
| AIME | American Invitational Mathematics Examination |
| | آزمون انتخابی ریاضی آمریکا |
| AMC10 | American Mathematics Contest 10 |
| | مسابقه ریاضی آمریکا ویژه کلاس دهم |
| AMC12 | American Mathematics Contest 12 |
| | مسابقه ریاضی آمریکا ویژه کلاس دوازدهم که جایگزین AHSME شده است |
| APMC | Austrian–Polish Mathematics Competition |
| | مسابقه ریاضی اتریش – لهستان |
| ARML | American Regional Mathematics League |
| | لیگ ریاضی منطقه‌ای آمریکا |
| HMMT | Harvard–MIT Math Tournament |
| | تورنمنت ریاضی هاروارد - MIT |
| IMO | International Mathematical Olympiad |
| | المپیاد ریاضی جهانی (بین المللی) |
| USAMO | United States of America Mathematical Olympiad |
| | المپیاد ریاضی ایالات متحده آمریکا |
| MOSP | Mathematical Olympiad Summer Program |
| | دوره تابستانی المپیاد ریاضی |

## علائم و نمادهای مورد استفاده در مجموعه‌ها، منطق و تئوری اعداد

| | |
|---|---|
| تعداد اعضای مجموعه‌ی $A$ | $\lvert A\rvert$ |
| $A$ کاملاً زیر مجموعه‌ی $B$ است (مساوی آن نیست) | $A \subset B$ |
| $A$ یک زیر مجموعه‌ی $B$ است | $A \subseteq B$ |
| $A$ بدون $B$ (تفاضل مجموعه‌ها) | $A \setminus B$ |
| اشتراک بین مجموعه‌های $A$ و $B$ | $A \cap B$ |
| اجتماع بین مجموعه‌های $A$ و $B$ | $A \cup B$ |
| عنصر $a$ متعلق به مجموعه‌ی $A$ است | $a \in A$ |
| $n$، $m$ را می‌شمارد | $n \mid m$ |
| بزرگ‌ترین مقسوم علیه مشترک $m$ و $n$ | $\gcd(m,n)$ |
| کوچک‌ترین مضرب مشترک $m$ و $n$ | $\operatorname{lcm}(m,n)$ |
| تعداد اعداد اول کوچک‌تر یا مساوی $n$ | $\pi(n)$ |
| تعداد مقسوم‌علیه‌های $n$ | $\tau(n)$ |
| حاصل جمع مقسوم‌علیه‌های مثبت $n$ | $\sigma(n)$ |
| $a$ و $b$ به پیمانه $m$ هم‌نهشت هستند | $a \equiv b \ (m \text{ پیمانه})$ |
| تابع $\varphi$ اویلر | $\varphi$ |
| مرتبه $a$ به پیمانه $m$ | $\operatorname{ord}_m(a)$ |
| تابع موبیوس | $\mu$ |
| نمایش در مبنای $b$ | $\overline{a_k a_{k-1} \dots a_1 a_0}_{(b)}$ |
| مجموع ارقام $n$ | $S(n)$ |
| بسط مبنای فاکتوریل | $(f_1, f_2, \dots, f_m)$ |
| کف $x$ (جزء صحیح $x$) | $\lfloor x \rfloor$ |
| سقف $x$ | $\lceil x \rceil$ |
| بخش اعشاری $x$ | $\{x\}$ |
| تابع لژاندر | $e_p$ |
| $p^k$ به طور کامل $n$ را می‌شمارد | $p^k \parallel n$ |
| عدد فرما | $f_n$ |
| عدد مرسن | $M_n$ |

# ۱- اصول تئوری اعداد

## بخشپذیری

در دوران ابتدایی چهار عمل اصلی روی اعداد (صحیح) به نام‌های جمع (+) تفریق (-)، ضرب (× یا .) و تقسیم (÷ یا /) را یاد گرفتیم. برای هر دو عدد صحیح $a$ و $b$ جمع آن‌ها $a+b$، اختلافشان $a-b$ یا $b-a$ و ضربشان $ab$، همگی اعداد صحیح هستند در حالیکه نسبت آن‌ها $a \div b$ ($a/b$ یا $\frac{a}{b}$) و $b \div a$ لزوماً اعداد صحیح نیستند.

برای عدد صحیح $m$ و عدد صحیح غیر صفر $n$، می‌گوییم $m$ بر $n$ بخشپذیر است یا $m,n$ را می‌شمارد اگر عدد صحیح $k$ وجود داشته باشد به طوری که $m=kn$؛ یا به عبارت دیگر $\frac{m}{n}$ یک عدد صحیح باشد. این خاصیت را به صورت $n \mid m$ نشان می‌دهیم. اگر $m$ بر $n$ بخشپذیر باشد $m$ مضربی از $n$ است و $n$ یک مقسوم‌علیه یا یک عامل $m$ می‌باشد.

از آنجا که $n \times 0 = 0$ بنابراین برای هر عدد صحیح $n$، $n \mid 0$. برای یک عدد صحیح ثابت $n$، مضارب $n$ عبارتند از $0, \pm n, \pm 2n, \ldots$. بنابراین به سادگی می‌توان دید که در بین هر $n$ عدد صحیح متوالی یک مضرب $n$ وجود دارد. اگر $m$ بر $n$ بخشپذیر نباشد، می‌نویسیم $n \nmid m$ (توجه کنید که اگر $m$ عدد صحیح غیر صفر باشد $0 \nmid m$ زیرا برای همه‌ی اعداد صحیح $k$، $0 \cdot k = 0 \neq m$)

**قضیه ۱. ۱.** فرض کنید $x, y, z$ اعداد صحیح باشند. در این صورت خواص اولیه زیر برقرار خواهند بود:

آ) $x \mid x$ (خاصیت بازتابی)

ب) اگر $y \mid x$ و $z \mid y$ آنگاه $x \mid z$ (خاصیت تعدی)

پ) اگر $y \mid x$ و $y \neq 0$ آنگاه $|x| \leq |y|$

ت) اگر $y \mid x$ و $x \mid z$ آنگاه $x \mid \alpha y + \beta z$ (برای هر عدد صحیح $\alpha$ و $\beta$)

ث) اگر $y \mid x$ و $x \mid y \pm z$ آنگاه $x \mid z$

ج) اگر $y \mid x$ و $x \mid y$ آنگاه $|x| = |y|$

چ) اگر $y \mid x$ و $y \neq 0$ آنگاه $\frac{y}{x} \mid y$

ح) برای $z \neq 0$ خواهیم داشت $x \mid y$ اگر و فقط اگر $xz \mid yz$

خواص بالا به طور مستقیم از تعریف نتیجه شده‌اند. ما اثبات‌های این خواص را فقط برای این که خواننده با چند مثال از چگونگی نوشتن اثبات‌ها آشنا شود، در اینجا ارائه می‌کنیم:

**اثبات:** برای (آ) می‌دانیم که $x = 1 \times x$ است. در (ب) تا (ج) شرط $x \mid y$ داده شده است یعنی عدد صحیح $k$ وجود دارد به طوری که $y = kx$.

برای (ب) داریم $y \mid z$ یعنی برای یک عدد صحیح $k_1$، $z = k_1 y$. بنابراین $z = (kk_1)x$ و در نتیجه $x \mid z$.

برای (پ) چون $y \neq 0$ است لذا $|k| \geq 1$ و بنابراین $|x| \geq |x| . |k|$ یا $|y| = |k| . |x|$

برای (ت) فرض می کنیم $z = k_2 x$. بنابراین $\alpha y + \beta z = (\alpha k + \beta k_2)x$

برای (ث) فرض می‌کنیم $y \pm z = k_3 x$ باشد. بنابراین $\pm z = k_3 x - y = (k_3 - k)x$ و در نتیجه $z = \pm(k - k_3)x$.

برای (ج) $y \mid x$ و $x \mid y$ نشان می‌دهند که $x \neq 0$ و $y \neq 0$ و لذا از خاصیت (پ) خواهیم داشت $|x| \geq |y|$ و $|y| \geq |x|$. پس: $|x| = |y|$

برای (چ) $\frac{y}{x} = k \neq 0$ یک عدد صحیح است. در نتیجه $y = xk$ و $k \mid y$.

برای (ح) از $z \neq 0$ نتیجه می‌گیریم که $x \neq 0$ اگر و فقط اگر $xz \neq 0$ و $y = kx$ اگر و فقط اگر $yz = kxz$

خاصیت (چ) ساده اما مفید است. برای یک عدد صحیح غیر صفر $n$، تعداد مقسوم‌علیه‌های مثبت $n$ زوج است مگر آنکه $n$ مربع کامل باشد؛ یعنی برای یک عدد صحیح $m$، $n = m^2$ باشد. (اگر عدد صحیحی بر هیچ عدد مربع کاملی بخش‌پذیر نباشد، این عدد در زبان انگلیسی *Square free* نامیده می‌شود. اگر $n = m^3$ باشد، $n$ یک مکعب کامل نامیده می‌شود. در حالت کلی اگر برای اعداد صحیح $m$ و $s$، $n = m^s$ باشد و $s \geq 2$ آنگاه $n$ یک توان کامل نامیده می‌شود) دلیل صحت گزاره فوق این است که همه‌ی عوامل $n$ به صورت زوج $x, \frac{n}{x}$ هستند (توجه

داشته باشید که اگر $n$ مربع کامل نباشد [به ازای تمام مقسوم‌علیه‌های $n$ که به جای $x$ قرار گیرند] $x \neq \frac{n}{x}$ خواهد بود). در اینجا یک مسأله کلاسیک را مطرح می‌کنیم:

**مثال ۱. ۱.** ۲۰ دانش‌آموز به نوبت از یک راهرو که دارای ۲۰ کمد در یک ردیف است عبور می‌کنند این کمدها از ۱ تا ۲۰ شماره‌گذاری شده‌اند. اولین دانش‌آموز همه‌ی کمدها را باز می‌کند. دومین دانش‌آموز کمدهای با شماره‌ی ۲، ۴، ۶، ۸، ۱۰، ۱۲، ۱۴، ۱۶، ۱۸ و ۲۰ را می‌بندد. سومین دانش‌آموز وضعیت کمدهای شماره‌ی ۳، ۶، ۹، ۱۲، ۱۵ و ۱۸ را تغییر می‌دهد. یعنی اگر کمدی باز بود آن را می‌بندد و اگر بسته بود آن را باز می‌کند. دانش‌آموز $i$اُم وضعیت کمدهایی را تغییر می‌دهد که شماره‌ی آن‌ها مضربی از $i$ باشند. بعد از این که همه‌ی دانش‌آموزان از راهرو عبور کردند چند کمد باز می‌ماند؟

**پاسخ:** وضعیت کمد $i$اُم توسط دانش‌آموز $j$اُم تغییر خواهد کرد اگر و فقط اگر $j \mid i$. با توجه به خاصیت (چ) در این صورت وضعیت کمد $i$، توسط دانش‌آموز $\frac{i}{j}$ نیز تغییر کرده است. بنابراین با توجه به بحث فوق فقط کمدهای شماره‌ی $۱=۱^۲, ۴=۲^۲, ۹=۳^۲, ۱۶=۴^۲$ به تعداد فرد بار تغییر وضعیت داده‌اند و لذا این کمدها بعد از عبور همه‌ی دانش‌آموزان باز خواهند بود. پس پاسخ مسأله ۴ است.

مجموعه‌ی اعداد صحیح که با $\mathbb{Z}$ نشان داده می‌شود را می‌توان به ۲ زیر مجموعه‌ی اعداد صحیح زوج و اعداد صحیح فرد تقسیم کرد:

$$\{ ۰, \pm ۲, \pm ۴, \ldots \} \text{ و } \{ \pm ۱, \pm ۳, \pm ۵, \ldots \}$$

اگرچه مفاهیم اعداد زوج و فرد ساده هستند، در حل مسائل گوناگون تئوری اعداد سودمند خواهند بود. در اینجا چند ایده ابتدایی ارائه می‌شوند:

۱) یک عدد فرد به شکل $۲k + ۱$ است که در آن $k$ عددی صحیح می‌باشد.

۲) یک عدد زوج به شکل $۲m$ است که در آن $m$ عددی صحیح می‌باشد.

۳) مجموع دو عدد فرد، یک عدد زوج است.

۴) مجموع دو عدد زوج، یک عدد زوج است.

۵) مجموع یک عدد فرد با یک عدد زوج، یک عدد فرد است.

۶) حاصل‌ضرب دو عدد فرد یک عدد فرد است.

۷) حاصل‌ضرب دو عدد صحیح، زوج است اگر و فقط اگر حداقل یکی از آن‌ها زوج باشد.

**مثال ۱. ۲.** فرض کنید $n$ یک عدد صحیح بزرگ‌تر از ۱ باشد. ثابت کنید:

آ) $۲^n$ برابر مجموع دو عدد فرد متوالی است.

ب) $۳^n$ برابر مجموع سه عدد صحیح متوالی است.

**پاسخ:** برای (آ) از رابطه‌ی $۲^n = (۲k-۱)+(۲k+۱)$، $k = ۲^{n-۲}$ به دست می‌آید و خواهیم داشت $۲^n = (۲^{n-۱}-۱)+(۲^{n-۱}+۱)$.

برای (ب) از رابطه‌ی $۳^n = (S-۱)+S+(S+۱)$، $S = ۳^{n-۱}$ به دست می‌آید و خواهیم داشت

$$۳^n = (۳^{n-۱}-۱)+۳^{n-۱}+(۳^{n-۱}+۱)$$

**مثال ۱. ۳.** فرض کنید $k$ یک عدد زوج باشد. آیا ممکن است عدد ۱ را به صورت مجموع معکوس‌های $k$ عدد فرد نشان داد؟

**پاسخ:** جواب منفی است. فرض کنید برای اعداد صحیح فرد $n_1, n_2, \ldots, n_k$ رابطه‌ی

$$۱ = \frac{۱}{n_۱}+\frac{۱}{n_۲}+\ldots+\frac{۱}{n_k}$$

برقرار باشد. بعد از مخرج مشترک گرفتن باید داشته باشیم $n_۱.n_۲\ldots n_k = S_۱+S_۲+\ldots+S_k$ که در آن $S_i$ها همگی فرد هستند. اما این رابطه نمی‌تواند برقرار باشد زیرا سمت چپ آن عددی فرد و سمت راست آن عددی زوج می‌باشد.

اگر $k$ فرد باشد چنین رابطه‌ای امکان‌پذیر است. یک مثال برای $k = ۹$ به صورت زیر می‌باشد:

$$۱ = \frac{۱}{۳}+\frac{۱}{۵}+\frac{۱}{۷}+\frac{۱}{۹}+\frac{۱}{۱۱}+\frac{۱}{۱۵}+\frac{۱}{۳۵}+\frac{۱}{۴۵}+\frac{۱}{۲۳۱}$$

**مثال ۱. ۴.** *[HMMT ۲۰۰۴]* زاک ۵ عدد از مجموعه‌ی $\{۱,۲,۳,۴,۵,۶,۷\}$ انتخاب کرده است. اگر او به کلودیا حاصل‌ضرب اعداد انتخابی را بگوید، این اطلاعات برای کلودیا کافی نخواهد بود تا تشخیص دهد مجموع اعداد انتخابی زوج است یا فرد. حاصل‌ضرب اعداد انتخابی چند است؟

**پاسخ:** جواب ۴۲۰ است.

داشتن حاصل‌ضرب اعداد انتخاب شده معادل با داشتن حاصل‌ضرب دو عدد دیگر است. تنها حاصل‌ضرب‌هایی که از روی دو زوج عدد متفاوت به دست می‌آید ۱۲ ($\{۲,۶\},\{۳,۴\}$) و ۶ ($\{۱,۳\},\{۱,۶\}$) هستند اما در حالت دوم مجموع دو عدد (انتخاب نشده) فرد است (و بنابراین

مجموع ۵ عدد انتخابی نیز فرد خواهد بود). بنابراین حالت اول باید برقرار باشد و حاصل‌ضرب اعداد انتخابی برابر است با:

$$\frac{۱\times۲\times۳\times\ldots\times۷}{۱۲}=۴۲۰$$

## الگوریتم تقسیم

نتیجه‌ی زیر الگوریتم تقسیم نامیده می‌شود و نقش مهمی در تئوری اعداد بازی می‌کند.

**قضیه‌ی ۱. ۲ (الف).** برای هر دو عدد صحیح مثبت $a$ و $b$ زوج یکتای $(q,r)$ از اعداد صحیح نامنفی وجود دارد به طوری که $b=aq+r$ و $r<a$. در این حالت $q$ خارج‌قسمت و $r$ باقی‌مانده‌ی تقسیم $b$ بر $a$ نامیده می‌شوند.

برای اثبات این مطلب، باید دو قسمت را در نظر گرفت: وجود این زوج عدد و یکتایی آن.

**اثبات:** برای نشان دادن وجود چنین زوجی سه حالت را بررسی می‌کنیم:

۱) در این حالت فرض می‌کنیم $a>b$ باشد. می‌توان قرار داد $q=۰$ و $r=b<a$ یا به عبارت دیگر $(q,r)=(۰,b)$.

۲) فرض می‌کنیم $a=b$ باشد. در این حالت $q=۱$ و $r=۰<a$ هستند یعنی $(q,r)=(۱,۰)$

۳) در آخرین حالت فرض می‌کنیم $a<b$ باشد. اعداد صحیح مثبت $n$ وجود دارند به طوری که $na>b$ باشد. $q$ را کوچک‌ترین عدد صحیح مثبتی قرار می‌دهیم که $(q+۱)a>b$ باشد در نتیجه $qa\le b$ خواهد بود. $r$ نیز از رابطه‌ی $r=b-aq$ به دست می‌آید. به این ترتیب $b=aq+r$ و $۰\le r<a$ خواهد بود.

با در نظر گرفتن هر سه حالت فوق، وجود زوج $(q,r)$ محرز خواهد بود.

برای اثبات یکتایی فرض کنید اعداد صحیح نامنفی $q',r'$ نیز وجود داشته باشند که روابط $b=aq'+r'$ و $۰\le r'<a$ برقرار باشند. بنابراین $aq+r=aq'+r'$ و از آنجا $a(q-q')=r'-r$ و سپس $a\mid r'-r$. از رابطه‌ی فوق نتیجه می‌شود که یا $a\le|r'-r|$ و یا $۰=|r'-r|$. از $۰\le r,r'<a$ نتیجه می‌گیریم که $|r'-r|<a$ و لذا رابطه $۰=|r'-r|$ باید برقرار باشد که به معنای برابری $r$ و $r'$ و به دنبال آن برابری $q$ و $q'$ است.

**مثال ۱. ۵.** $n$ یک عدد صحیح مثبت است. ثابت کنید $۳^{۲^n}+۱$ بر ۲ بخش‌پذیر است ولی بر ۴ بخش‌پذیر نیست.

**اثبات:** واضح است که $۳^{۲^n}$ عددی فرد و $۳^{۲^n}+۱$ عددی زوج است.

$$۳^{۲^n}=(۳^۲)^{۲^{n-۱}}=۹^{۲^{n-۱}}=(۸+۱)^{۲^{n-۱}}$$

با استفاده از بسط دو جمله‌ای

$$(x+y)^m = x^m + \binom{m}{1}x^{m-1}y + \binom{m}{2}x^{m-2}y^2 + \cdots + \binom{m}{m-1}xy^{m-1} + y^m$$

و قرار دادن $x=8$، $y=1$ و $m=2^{n-1}$ در رابطه‌ی بالا، مشاهده می‌شود که تمام جملات غیر از جمله‌ی آخر ($y^m=1$) مضربی از ۸ (که خود مضرب ۴ است) می‌باشند. بنابراین باقیمانده‌ی $3^{2^n}$ در تقسیم بر ۴ برابر ۱ و باقیمانده‌ی $3^{2^n}+1$ در تقسیم بر ۴ برابر ۲ است.

بحث بالا را می‌توان در مفهوم هم‌نهشتی به پیمانه‌ی ۴ بیان کرد. هم‌نهشتی یکی از بخش‌های مهم تئوری اعداد است که بعداً به طور گسترده روی آن بحث خواهیم کرد. الگوریتم تقسیم را می‌توان به تمام اعداد صحیح گسترش داد.

**قضیه ۱. ۲ (ب).** برای هر دو عدد صحیح $a$ و $b(a\neq 0)$ زوج یکتای $(q,r)$ از اعداد صحیح وجود دارد به طوری که $b=aq+r$ و $0\leq r<|a|$.

اثبات این حالت تعمیم یافته را به عهده خواننده می‌گذاریم.

## اعداد اول

عدد صحیح $p>1$ اول (یا یک عدد اول) نامیده می‌شود اگر هیچ عدد صحیح $d$ با شرایط $d>1$ و $d\neq p$ وجود نداشته باشد به طوری که $d\mid p$. هر عدد صحیح $n>1$ حداقل یک مقسوم‌علیه اول دارد. اگر $n$ خود یک عدد اول باشد، آنگاه $n$ یک مقسوم‌علیه اول است. اگر $n$ اول نباشد، فرض کنید $a>1$ کوچک‌ترین مقسوم‌علیه آن باشد. پس $n=ab$ در حالی که $1<a\leq b$. اگر $a$ اول نباشد پس $a=a_1a_2$ که $1<a_1\leq a_2<a$ و $a_1\mid n$ که با حداقل بودن $a$ در تضاد است.

هر عدد صحیح $n>1$ که اول نباشد یک عدد مرکب نامیده می‌شود. اگر $n$ یک عدد صحیح مرکب باشد آنگاه یک مقسوم‌علیه اول $p$ خواهد داشت که از $\sqrt{n}$ بزرگ‌تر نیست. برای اثبات همان شرایط بالا را در نظر بگیرید یعنی $n=ab$ و $1<a\leq b$ که $a$ کوچک‌ترین مقسوم‌علیه $n$ است. بنابراین $n\geq a^2$ و از آنجا $a\leq\sqrt{n}$. این فکر به ریاضیدان یونان باستان، اراتستن (۲۵۰ قبل از میلاد) تعلق دارد.

توجه کنید که همه‌ی اعداد صحیح زوج بزرگ‌تر از ۲ مرکب هستند. به عبارت دیگر ۲ تنها عدد اول زوج (و کوچک‌ترین عدد اول) است. همه‌ی اعداد اول دیگر، فرد هستند یعنی بر ۲ بخش‌پذیر نیستند. چند عدد اول ابتدایی عبارتند از ۲، ۳، ۵، ۷، ۱۱، ۱۳، ۱۷، ۱۹، ۲۳ و ۲۹. چند عدد اول وجود دارد؟ آیا مطمئن هستیم که تعداد اعداد اول نامتناهی است؟ برای پاسخ به این سؤال، قضیه ۱. ۳

رادر ادامه ببینید. مقایسه بین تعداد عناصر در دو مجموعه‌ی نامتناهی ممکن است مبهم باشد اما واضح است که تعداد اعداد مرکب بیش‌تر از اعداد اول (از نظر چگالی) هستند. ۲ و ۳ تنها اعداد اول متوالی هستند. اعداد اول فرد متوالی مانند ۳ و ۵، ۵ و ۷، ۴۱ و ۴۳ اعداد اول دوقلو نامیده می‌شوند. هنوز یک سؤال مفتوح وجود دارد که آیا تعداد اعداد اول دوقلو بی‌نهایت است؟ برون[1] نشان داده است که حتی اگر بی‌نهایت عدد اول دوقلو وجود داشته باشد، مجموع معکوس‌های آن همگرا می‌شود. البته اثبات این مطلب بسیار مشکل است.

**مثال ۱. ۶.** همه‌ی اعداد صحیح مثبت $n$ را چنان پیدا کنید که $3n-4$، $4n-5$ و $5n-3$ همگی اول باشند.

**پاسخ:** مجموع این سه عدد، یک عدد زوج است. بنابراین حداقل یکی از آن‌ها باید زوج باشد. تنها عدد اول زوج، ۲ است. فقط $3n-4$ و $5n-3$ می‌توانند زوج باشند. با حل معادلات $3n-4=2$ و $5n-3=2$ به ترتیب برای $n$ مقادیر ۲ و ۱ به دست می‌آید. در این میان فقط به ازای $n=2$ هر سه عدد، اول خواهند بود.

**مثال ۱. ۷.** [AHSME۱۹۷۶] اگر $p$ و $q$ اول باشند و $x^2-px+q=0$ ریشه‌های صحیح مثبت و متمایز داشته باشد، $p$ و $q$ را پیدا کنید.

**پاسخ:** فرض کنید $x_1$ و $x_2$ $(x_1<x_2)$ دو ریشه صحیح مثبت و متمایز باشند. بنابراین از $x^2-px+q=(x-x_1)(x-x_2)$ خواهیم داشت $p=x_1+x_2$ و $q=x_1x_2$. از آنجا که $q$ اول است $x_1=1$ بوده و لذا $q=x_2$ و $p=x_2+1$ دو عدد اول متوالی هستند؛ پس $q=2$ و $p=3$.

**مثال ۱. ۸.** ۲۰ عدد مرکب متوالی پیدا کنید؟

**پاسخ:** $20!+2, 20!+3, \ldots, 20!+21$

قضیه زیر بیش از ۲۰۰۰ سال قبل توسط اقلیدس شناخته شده است:

**قضیه ۱. ۳** (الف). بی‌نهایت عدد اول وجود دارد.

---

[1] Brun

**اثبات:** فرض کنید تعداد متناهی عدد اول وجود داشته باشد: $p_1 < p_2 < \ldots < p_m$. عدد $P = p_1 p_2 \ldots p_m + 1$ را در نظر بگیرید. اگر $P$ اول باشد، $P > p_m$ خواهد بود که با فرض بزرگ‌ترین عدد اول بودن $p_m$ تضاد دارد. بنابراین $P$ مرکب است و در نتیجه یک عامل اول $p > 1$ دارد که یکی از اعداد اول $p_m, \ldots, p_2, p_1$ می‌باشد. آن را $p_k$ می‌نامیم. بنابراین $p_k$ عدد $p_1 p_2 \ldots p_m + 1$ را می‌شمارد. این مطلب با توجه به اینکه $p_k$ عدد $p_1 p_2 \ldots p_m$ را نیز می‌شمارد نشان می‌دهد که $p_k$ باید ۱ را بشمارد که تناقض است.

با وجود این که بی‌نهایت عدد اول وجود دارد، هیچ فرمول مشخصی برای پیدا کردن آن‌ها وجود ندارد. قضیه‌ی ۳٫۱ب. در بخش بعد قسمتی از کارهای انجام شده را آشکار می‌کند.

## قضیه بنیادی حساب

قضیه بنیادی در حساب (تئوری اعداد) مربوط به تجزیه اعداد صحیح به عوامل اول است:

**قضیه ۱. ۴.** [قضیه بنیادی حساب] هر عدد صحیح $n$ بزرگ‌تر از ۱، یک نمایش یکتا از حاصل‌ضرب اعداد اول دارد.

**اثبات:** وجود چنین نمایشی را می‌توان به صورت زیر اثبات کرد: فرض کنید $p_1$ یک عامل اول $n$ باشد. اگر $p_1 = n$، آنگاه $n = p_1$ تجزیه $n$ به عوامل اول خواهد بود. اگر $p_1 < n$، آنگاه $n = p_1 r_1$ و $r_1 > 1$. اگر $r_1$ یک عدد اول باشد، $n = p_1 p_2$ $(p_2 = r_1)$ تجزیه مطلوب خواهد بود. اگر $r_1$ مرکب باشد آنگاه $r_1 = p_2 r_2$ که $p_2$ عدد اول بوده و $r_2 > 1$ است. از آنجا $n = p_1 p_2 r_2$ خواهد بود. اگر $r_2$ اول باشد آنگاه $n = p_1 p_2 p_3$ $(p_3 = r_2)$ پاسخ مطلوب خواهد بود. اگر $r_2$ مرکب باشد الگوریتم فوق را ادامه می‌دهیم تا یک دنباله از اعداد صحیح به صورت $r_1 > r_2 > \ldots \geq 1$ به دست آید. بعد از انجام چند مرحله متناهی به $r_{k+1} = 1$ خواهیم رسید و $n = p_1 p_2 \ldots p_k$ خواهد شد.

برای اثبات یکتایی فرض کنید حداقل یک عدد صحیح مثبت $n$ باشد که دو تجزیه متفاوت به عوامل اول دارد یعنی:

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_h$$

که $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_h$ همگی اعداد اول هستند که $p_1 \leq p_2 \leq \ldots \leq p_k$ و $q_1 \leq q_2 \leq \ldots \leq q_h$ بوده و $k$ تایی $(p_1, p_2, \ldots, p_k)$ با $h$ تایی $(q_1, q_2, \ldots, q_h)$ فرق دارد.

واضح است که $k \geq 2$ و $h \geq 2$. $n$ را کوچک‌ترین عدد صحیح با چنین خاصیتی در نظر می‌گیریم. با استفاده از برهان خلف و یافتن یک عدد صحیح کوچک‌تر که دو تجزیه متفاوت به عوامل اول دارد قضیه را ثابت می‌کنیم.

ادعا می‌کنیم که برای هر $i$ از ۱ تا $k$ و هر $j$ از ۱ تا $h$، $p_i \neq q_j$ است. برای مثال اگر $p_k = q_n = p$، آنگاه $n' = n/p = p_1 \dots p_{k-1} = q_1 \dots q_{h-1}$ و $1 < n' < n$ که با شرط حداقل بودن $n$ تضاد دارد. بدون از دست دادن کلیت مسأله فرض کنید $p_1 \leq q_1$ باشد به عبارت دیگر $p_1$ کوچک‌ترین عامل اول $n$ در نمایش فوق خواهد بود. با استفاده از الگوریتم تقسیم خواهیم داشت:

$$\begin{aligned} q_1 &= p_1 c_1 + r_1 \\ q_2 &= p_1 c_2 + r_2 \\ &\vdots \\ q_h &= p_1 c_h + r_h \end{aligned}$$

که برای $i = 1, \dots, h$، $0 \leq r_i < p_1$. داریم:

$$\begin{aligned} n = q_1 q_2 \dots q_h &= (p_1 c_1 + r_1)(p_1 c_2 + r_2) \dots (p_1 c_h + r_h) \\ &= m p_1 + r_1 r_2 \dots r_h \end{aligned}$$

که $m$ یک عدد صحیح مثبت است. با قرار دادن $n' = r_1 r_2 \dots r_h$ خواهیم داشت $n = p_1 p_2 \dots p_k = m p_1 + n'$ و لذا $p_1 \mid n'$ یا $n' = p_1 s$. همان طور که نشان داده‌ایم $s$ را می‌توان به صورت حاصل‌ضرب عوامل اول نشان داد لذا $s$ را به صورت $s = s_1 s_2 \dots s_i$ می‌نویسیم که $s_1, s_2, \dots, s_i$ اعداد اول هستند.

از طرف دیگر با استفاده از تجزیه $r_1, r_2, \dots, r_n$ به عوامل اول، همه‌ی عوامل آن‌ها کوچک‌تر از $p_1$ هستند. از $n' = r_1 \dots r_n$ نتیجه می‌شود که $n'$ به عوامل اول به صورت $n' = t_1 t_2 \dots t_j$ تجزیه می‌شود که در آن $t_u < p_1$ $(u = 1, \dots, j)$. این تجزیه با $n' = p_1 s_1 s_2 \dots s_i$ فرق دارد یعنی $n'$ نیز دو نمایش متفاوت در تجزیه به عوامل اول دارد که چون $n' < n$ می‌باشد با فرض مسأله (حداقل بودن $n$ با این خاصیت) در تضاد است.

از قضیه بالا نتیجه می‌شود که هر عدد صحیح $n > 1$ را می‌توان به صورت یکتا به شکل زیر نوشت:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

که $p_1, \dots, p_k$ اعداد اول متمایز و $\alpha_1, \dots, \alpha_k$ اعداد صحیح مثبت هستند. این نمایش عدد $n$، تجزیه کانونی (یا تجزیه) عدد $n$ نامیده می‌شود. به سادگی می‌توان دید که تجزیه کانونی حاصل‌ضرب دو عدد صحیح با حاصل‌ضرب تجزیه‌های کانونی آن دو عدد برابر است. این تجزیه به ما اجازه می‌دهد که خاصیت اساسی اعداد اول را به صورت زیر به دست آوریم.

**نتیجه ۱. ۵.** $a$ و $b$ اعداد صحیح هستند. اگر عدد اول $p$، $ab$ را بشمارد آنگاه $p$، $a$ یا $b$ را می‌شمارد.

**اثبات:** از آنجا که $p$، $ab$ را می‌شمارد، باید در تجزیه کانونی $ab$ ظاهر شود. تجزیه کانونی $a$، $b$ و $ab$ یکتا هستند و تجزیه کانونی $ab$ حاصل‌ضرب تجزیه‌های کانونی $a$و $b$ می‌باشد. بنابراین $p$ باید در حداقل یکی از تجزیه‌های کانونی $a$ و $b$ ظاهر شود که مبنی بر همان نتیجه مطلوب است.
یک کاربرد دیگر از قضیه تجزیه به عوامل اول، یک روش جایگزین برای اثبات وجود بی‌نهایت عدد اول، است. در اثبات قضیه ۱. ۳ فرض کردیم که تعداد محدودی عدد اول وجود داشته باشد. آن عددها را $p_1 < p_2 < \ldots < p_m$ در نظر گرفتیم. $N$ را به صورت زیر تعریف می‌کنیم:

$$N = \prod_{i=1}^{m}(1+\frac{1}{p_i}+\frac{1}{p_i^2}+\ldots) = \prod_{i=1}^{m}\frac{1}{1-\frac{1}{p_i}}$$

از طرف دیگر با بسط دادن و استفاده از تجزیه کانونی همه‌ی اعداد صحیح خواهیم داشت:

$$N = 1+\frac{1}{2}+\frac{1}{3}+\ldots$$

در نتیجه

$$\prod_{i=1}^{m}\frac{p_i}{p_i-1} = \infty$$

که تناقض است. در این جا ما از مفاهیم شناخته شده‌ای استفاده کردیم:

الف) سری هارمونیک $1+\frac{1}{2}+\frac{1}{3}+\ldots$ واگرا است.

ب) فرمول بسط

$$\frac{1}{1-x} = 1+x+x^2+\ldots$$

که برای اعداد حقیقی $x$ به شرط $|x|<1$ برقرار است. این فرمول بسط را می‌توان به عنوان فرمول مجموع یک تصاعد هندسی نامتناهی $1, x, x^2, \ldots$ نیز تفسیر کرد.

از روابط فوق داریم

$$\prod_{i=1}^{\infty}\frac{p_i}{p_i-1} = \infty$$

با استفاده از نامساوی $t \in \mathbb{R},\ 1+t \le e^t$ می‌توان به آسانی رابطه‌ی زیر را به دست آورد:

$$\sum_{i=1}^{\infty} \frac{1}{p_i} = \infty$$

برای عدد اول $p$ می‌گوییم $p^k$ کاملاً $n$ را می‌شمارد و می‌نویسیم $p^k \| n$ اگر $k$ بزرگ‌ترین عدد صحیح مثبتی باشد که $p^k \mid n$.

**مثال ۱. ۹.** *[ARML۲۰۰۳]* بزرگ‌ترین مقسوم‌علیه ۱۰۰۱۰۰۱۰۰۱ که از ۱۰۰۰۰ بزرگ‌تر نیست را پیدا کنید.

**پاسخ:**

$$۱۰۰۱۰۰۱۰۰۱ = ۱۰۰۱ \times ۱۰^۶ + ۱۰۰۱ = ۱۰۰۱ \times (۱۰^۶ + ۱) = ۷ \times ۱۱ \times ۱۳ \times (۱۰^۶ + ۱)$$

$$x^۶ + ۱ = (x^۲)^۳ + ۱ = (x^۲ + ۱)(x^۴ - x^۲ + ۱)$$

$$۱۰^۶ + ۱ = ۱۰۱ \times ۹۹۰۱ \quad \rightarrow \quad ۱۰۰۱۰۰۱۰۰۱ = ۷ \times ۱۱ \times ۱۳ \times ۱۰۱ \times ۹۹۰۱$$

واضح است که هیچ ترکیبی از ۷، ۱۱، ۱۳ و ۱۰۱ نمی‌تواند عددی بزرگ‌تر از ۹۹۰۱ و کوچک‌تر از ۱۰۰۰۰ تولید کند لذا جواب مسأله ۹۹۰۱ است.

**مثال ۱. ۱۰.** $n$ را چنان بیابید که $۲^n \| ۳^{۱۰۲۴} - ۱$.

**پاسخ:** جواب ۱۲ است.

$۱۰۲۴ = ۲^{۱۰}$ و $(x^۲ - y^۲) = (x - y)(x + y)$ بنابراین:

$$۳^{۲^{۱۰}} - ۱ = (۳^{۲^۹} - ۱)(۳^{۲^۹} + ۱) = (۳^{۲^۹} + ۱)(۳^{۲^۸} + ۱)(۳^{۲^۸} - ۱) = \cdots$$

$$= (۳^{۲^۹} + ۱)(۳^{۲^۸} + ۱)(۳^{۲^۷} + ۱) \cdots (۳^{۲^۱} + ۱)(۳^{۲^۰} + ۱)(۳ - ۱)$$

از مثال ۱. ۵ می‌دانیم $۲ \| ۳^{۲^k} + ۱$ (برای اعداد صحیح مثبت $k$) بنابراین پاسخ برابر است با:

$۹ + ۲ + ۱ = ۱۲$

قضیه ۱. ۴ نشان می‌دهد که همه‌ی اعداد صحیح با (حاصل‌ضرب) اعداد اول تولید می‌شوند. به دلیل اهمیت اعداد اول، افراد زیادی تلاش کرده‌اند تا یک فرمول صریح برای تولید اعداد اول پیدا

کنند. تاکنون همه‌ی تلاش‌ها ناقص بوده است ولی از طرف دیگر نتایج منفی زیادی وجود دارد. قضیه بعدی یکی از این نوع است که توسط گلدباخ[۲] ارائه شده است:

قضیه ۱. ۳ ب. برای هر عدد صحیح $m$، هیچ چند جمله‌ای $p(x)$ با ضرایب صحیح وجود ندارد به طوری که برای همه‌ی اعداد صحیح $n$ با شرط $n \geq m$، $p(n)$ اول باشد.

اثبات: به منظور رسیدن به تناقض فرض کنید چنین چند جمله‌ای وجود دارد:

$$p(x)=a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$$

که در آن $a_k, \ldots, a_1, a_0$ اعداد صحیح بود ه و $a_k \neq 0$.

اگر $p(m)$ مرکب باشد فرض ما غلط است و اگر نباشد فرض می‌کنیم $p(m)=q$ یک عدد اول باشد. پس

$$p(m)=a_k m^k + a_{k-1}m^{k-1} + \ldots + a_1 m + a_0$$

و برای اعداد صحیح مثبت $i$

$$p(m+qi)=a_k(m+qi)^k + a_{k-1}(m+qi)^{k-1} + \ldots + a_1(m+qi) + a_0$$

با توجه به این که

$$(m+qi)^j = m^j + \binom{j}{1} m^{j-1}(qi) + \binom{j}{2} m^{j-2}(qi)^2 + \cdots + \binom{j}{j-1} m(qi)^{j-1} + (qi)^j$$

لذا $(m+qi)^j - m^j$ مضربی از $q$ بوده و در نتیجه $p(m+qi)-p(m)$ نیز مضربی از $q$ می‌باشد. از آنجا که $p(m)=q$، $p(m+qi)$ مضربی از $q$ است. با فرض ما $p(m+qi)$ نیز اول است بنابراین تنها مقادیر ممکن برای آن $q$-,۰و $q$ هستند (برای تمام اعداد صحیح مثبت $i$). از طرف دیگر معادلات $p(x)=-q$، $p(x)=0$، $p(x)=q$ و حداکثر می‌توانند $3k$ ریشه داشته باشند. بنابراین (تعداد بی‌شماری) $i$ وجود دارد که $m+qi$ پاسخی برای هیچ کدام از معادلات $p(x)=-q$، $p(x)=0$ و $p(x)=q$ نیست؛ که این تناقض است. لذا فرض ما غلط بوده و چنین چند جمله‌ای‌هایی وجود ندارد.

با وجود این که هیچ راه مشخصی برای یافتن اعداد اول وجود ندارد، چگالی اعداد اول (میانگین حضور اعداد اول در بین اعداد صحیح) حدود ۱۰۰ سال است که شناخته شده است. این یافته یک نتیجه قابل توجه در ریاضیات در حوزه‌ی تئوری اعداد تحلیلی بود که نشان می‌دهد:

---

[2] Goldbach

$$\lim_{n\to\infty}\frac{\pi(n)}{n/\log n}=1$$

که $\pi(n)$ تعداد اعداد اول کوچک‌تر یا نامساوی $n$ را نشان می‌دهد. رابطه‌ی فوق به عنوان قضیه عدد اول شناخته می‌شود. این قضیه توسط دو دانشمند[3] در سال ۱۸۹۶ اثبات شده است. یک اثبات مقدماتی ولی مشکل نیز توسط اردوش و سلبرگ[4] ارائه شده است.

## بزرگ‌ترین مقسوم‌علیه مشترک

برای عدد صحیح مثبت $k$، مجموعه‌ی همه‌ی مقسوم‌علیه‌های مثبت $k$ را با $D_k$ نشان می‌دهیم. واضح است که $D_k$ یک مجموعه‌ی متناهی است. برای اعداد صحیح مثبت $m$ و $n$ بزرگ‌ترین عضو در مجموعه‌ی $D_m \cap D_n$، بزرگ‌ترین مقسوم‌علیه مشترک (G.C.D) $m$ و $n$ نامیده شده و با $\gcd(m,n)$ نشان داده می‌شود. در حالتی که $D_m \cap D_n = \{1\}$ باشد، $\gcd(m,n)=1$ خواهد بود و می‌گوییم $m$ و $n$ نسبت به هم اول هستند. در ادامه چند خاصیت اساسی G.C.D بیان خواهد شد.

**قضیه ۱. ۶.**

(آ) اگر $p$ اول باشد آنگاه $\gcd(p,m)=p$ یا $\gcd(p,m)=1$

(ب) اگر $\gcd(m,n)=d$، $m=m'd$ و $n=n'd$ آنگاه $\gcd(m',n')=1$

(پ) اگر $\gcd(m,n)=d$، $m=m''d'$ و $n=n''d'$ و $\gcd(m'',n'')=1$ آنگاه $d=d'$

(ت) اگر $d'$ یک مقسوم علیه مشترک $m$ و $n$ باشد آنگاه $d'$ را می‌شمارد.

(ث) اگر $p^x \| m$ و $p^y \| n$ آنگاه $p^{\min(x,y)} \| \gcd(m,n)$. در حالت کلی اگر $m=p_1^{\alpha_1}\dots p_k^{\alpha_k}$ و $n=p_1^{\beta_1}\dots p_k^{\beta_k}$ که برای $i=1,\dots,k$، $\alpha_i,\beta_i \geq 0$ آنگاه

$$\gcd(m,n)=p_1^{\min(\alpha_1,\beta_1)}\dots p_k^{\min(\alpha_k,\beta_k)}$$

(ج) اگر $m=nq+r$ آنگاه $\gcd(m,n)=\gcd(n,r)$

**اثبات:** اثبات این خواص به راحتی از روی تعریف به دست می‌آیند. ما در اینجا فقط اثبات خاصیت (ج) را ارائه می‌کنیم. فرض کنید $\gcd(m,n)=d$ و $\gcd(n,r)=d'$. چون $d \mid m$ و $d \mid n$ در نتیجه $d \mid r$ و لذا $d \mid d'$. از طرف دیگر چون $d' \mid n$ و $d' \mid r$ پس $d' \mid m$ و از آنجا $d' \mid d$ بنابراین $d=d'$.

---

[3] Hadamard and de la Vallee Poussin

[4] Erdos and Selberg.

تعریف بزرگ‌ترین مقسوم‌علیه مشترک (ب.م.م) را می‌توان به سادگی به بیش از دو عدد تعمیم داد. برای اعداد صحیح $a_1, a_2, \ldots, a_n$، $\gcd(a_1, a_2, \ldots, a_n)$ بزرگ‌ترین مقسوم‌علیه مشترک بین همه‌ی اعداد $a_1, a_2, \ldots, a_n$ است. بزرگ‌ترین مقسوم‌علیه مشترک $a_1, a_2, \ldots, a_n$ را می‌توان به صورت زیر تعیین کرد:

$$d_1 = \gcd(a_1, a_2),\ d_2 = \gcd(d_1, a_3),\ \ldots,\ d_{n-1} = \gcd(d_{n-2}, a_n)$$

اثبات این که $d_{n-1} = \gcd(a_1, \ldots, a_n)$ است و اثبات‌های ساده‌ی خواص زیر را به خواننده می‌سپاریم.

**قضیه ۱. ۶. (ادامه)**

(چ) $\gcd(\gcd(m, n), p) = \gcd(m, \gcd(n, p))$ که ثابت می‌کند $\gcd(m, n, p)$ به درستی تعریف شده است.

(ح) اگر برای $i = 1, \ldots, n$، $d \mid a_i$ آنگاه $d \mid \gcd(a_1, \ldots, a_n)$

(خ) اگر $a_i = p_1^{\alpha_{1i}} \ldots p_k^{\alpha_{ki}}$ $(i = 1, \ldots, n)$ آنگاه

$$\gcd(a_1, \ldots, a_n) = p_1^{\min(\alpha_{11}, \ldots, \alpha_{1n})} \ldots p_k^{\min(\alpha_{k1}, \ldots, \alpha_{kn})}$$

می‌گوییم $a_1, a_2, \ldots, a_n$ نسبت به هم اول هستند اگر بزرگ‌ترین مقسوم‌علیه مشترک آن‌ها برابر ۱ باشد.

توجه کنید که $\gcd(a_1, \ldots, a_n) = 1$ به معنی آن نیست که برای $1 \le i < j \le n$، $\gcd(a_i, a_j) = 1$ است (به طور مثال $a_1 = 2, a_2 = 3$ و $a_3 = 6$ را در نظر بگیرید). اگر $a_1, a_2, \ldots, a_n$ چنان باشند که برای $1 \le i < j \le n$، $\gcd(a_i, a_j) = 1$ باشد گوییم که این اعداد دو به دو نسبت به هم اول هستند.

## الگوریتم اقلیدس

تجزیه کانونی به ما کمک می‌کند تا بزرگ‌ترین مقسوم‌علیه مشترک اعداد صحیح را تعیین کنیم. اما تجزیه کردن اعداد، بخصوص اعداد بزرگ کار آسانی نیست (به این دلیل که نیاز به مطالعه و بررسی بخش‌پذیری اعداد داریم). یک الگوریتم مفید برای یافتن بزرگ‌ترین مقسوم‌علیه مشترک دو عدد صحیح مثبت $m$ و $n$ الگوریتم اقلیدس است. این الگوریتم شامل چندین بار استفاده از الگوریتم تقسیم می‌شود:

$$\begin{aligned} m &= nq_1 + r_1 \quad , \quad 1 \le r_1 < n \\ n &= r_1 q_2 + r_2 \quad , \quad 1 \le r_2 < r_1 \\ &\vdots \\ r_{k-2} &= r_{k-1} q_k + r_k \quad , \quad 1 \le r_k < r_{k-1} \\ r_{k-1} &= r_k q_{k+1} + r_{k+1} \quad , \quad r_{k+1} = 0 \end{aligned}$$

این زنجیره از تساوی‌ها محدود است زیرا $r_k < \cdots < r_2 < r_1 < n$.
آخرین باقی‌مانده‌ی غیر صفر، $r_k$، بزرگ‌ترین مقسوم‌علیه مشترک $m$ و $n$ است. در واقع با استفاده مکرر از خاصیت (ج) بالا خواهیم داشت:

$$\gcd(m,n) = \gcd(n,r_1) = \gcd(r_1,r_2) = \cdots = \gcd(r_{k-1},r_k) = r_k$$

**مثال ۱. ۱۱.** [HMMT۲۰۰۲] اگر یک عدد صحیح مثبت از مضارب ۸۶۴ به طور تصادفی انتخاب شود با فرض این که احتمال انتخاب هر مضرب یکسان باشد، احتمال این که عدد انتخاب شده بر ۱۹۴۴ بخش‌پذیر باشد چند است؟

**پاسخ اول:** احتمال این که مضربی از $۸۶۴ = ۳^۳ \times ۲^۵$ بر $۱۹۴۴ = ۳^۵ \times ۲^۳$ بخش‌پذیر باشد با احتمال این که مضربی از $۲^۲ = ۴$ بر $۳^۲ = ۹$ بخش‌پذیر باشد برابر است. از آنجا که ۴ و ۹ نسبت به هم اول هستند، جواب $\frac{۱}{۹}$ است.

**پاسخ دوم:** با استفاده از الگوریتم اقلیدس داریم:

$$gcd(۱۹۴۴, ۸۶۴) = gcd(۱۰۸۰, ۸۶۴) = gcd(۸۶۴, ۲۱۶) = ۲۱۶$$

بنابراین $۲۱۶ \times ۹ = ۱۹۴۴$ و $۸۶۴ = ۴ \times ۲۱۶$ و پاسخ را مانند قسمت قبل کامل می‌کنیم.

**مثال ۱. ۱۲.** [HMMT ۲۰۰۲] حاصل عبارت زیر را به دست آورید؟

$$gcd(۲۰۰۲ + ۲, ۲۰۰۲^۲ + ۲, ۲۰۰۲^۳ + ۲, \ldots)$$

**پاسخ:** g را برابر بزرگ‌ترین مقسوم‌علیه مشترک مطلوب در نظر می‌گیریم:

$$۲۰۰۲^۲ + ۲ = ۲۰۰۲ \times (۲۰۰۰ + ۲) + ۲ = ۲۰۰۰ \times (۲۰۰۲ + ۲) + ۶$$

با استفاده از الگوریتم اقلیدس

$$gcd(۲۰۰۲+۲, ۲۰۰۲^۲+۲) = gcd(۲۰۰۴, ۶) = ۶$$

بنابراین $g \mid gcd(۲۰۰۲+۲, ۲۰۰۲^۲+۲) = ۶$. از طرف دیگر همه‌ی اعداد دنباله $۲۰۰۲+۲, ۲۰۰۲^۲+۲, \ldots$ بر ۲ بخش‌پذیرند. علاوه بر این از آنجا که $۲۰۰۲^k = ۳a_k + ۱$، $k$ مثبت $۲۰۰۲ = ۲۰۰۱+۱ = ۶۶۷ \times ۳ + ۱$ برای همه‌ی اعداد صحیح ($a_k$ عددی صحیح است). بنابراین $۲۰۰۲^k + ۲$ بر ۳ بخش‌پذیر است. چون ۲ و ۳ نسبت به هم اول هستند تمام اعداد دنباله مذکور بر ۶ بخش‌پذیر است لذا $g = ۶$.

## قضیه بزو

بحث را با دو مسأله فکری کلاسیک آغاز می‌کنیم:

**مثال ۱. ۱۳** در یک بازی فوتبال ویژه، یک تیم برای تاچ‌دان ۷ امتیاز و برای یک فیلد گل ۳ امتیاز می‌گیرد. تعیین کنید بیش‌ترین امتیازی که یک تیم در یک بازی (با زمان نامتناهی) نمی‌تواند به دست بیاورد چند است؟

**پاسخ:** جواب ۱۱ است. به سادگی می‌توان دید که به هیچ عنوان نمی‌توان به امتیاز ۱۱ رسید. اما $۳+۳+۳+۳ = ۱۲$، $۳+۳+۷ = ۱۳$ و $۷+۷ = ۱۴$. برای همه‌ی اعداد صحیح بزرگ‌تر از ۱۱، باقی‌مانده‌ی تقسیم $n$ بر ۳ یکی از سه حالت صفر، ۱ و ۲ را دارد. اگر باقیمانده صفر باشد آنگاه به وضوح یک تیم می‌تواند $n$ امتیاز را فقط با فیلدگل به دست آورد. اگر باقیمانده ۱ باشد آنگاه $n-۷$ در تقسیم بر ۳ باقیمانده صفر دارد و لذا $n$ امتیاز را می‌توان با یک تاچ‌دان و تعداد کافی فیلدگل به دست آورد. اگر باقیمانده ۲ باشد آنگاه $n-۱۴$ در تقسیم بر ۳ باقیمانده صفر دارد و $n$ امتیاز را می‌توان با ۲ تاچ‌دان و تعداد کافی فیلدگل به دست آورد. به طور خلاصه همه‌ی اعداد صحیح $n$ بزرگ‌تر از ۱۱ را می‌توان به شکل $n = ۷a + ۳b$ نوشت که در آن $a$ و $b$ اعداد صحیح نامنفی هستند.

**مثال ۱. ۱۴** یک منبع کافی از شیر در یک تانکر شیر وجود دارد. به آقای چاق یک ظرف ۵ لیتری (بدون درجه‌بندی) و یک ظرف ۹ لیتری (بدون درجه‌بندی) داده شده است. او چگونه می‌تواند ۲ لیتر شیر بردارد؟

**پاسخ:** فرض کنید $T, L_۵$ و $L_۹$ به ترتیب بیانگر تانکر شیر، ظرف ۵ لیتری و ظرف ۹ لیتری باشند، می‌توان از جدول زیر برای رسیدن به نتیجه دلخواه استفاده کرد.

| $T$ | $L_۵$ | $L_۹$ |
|---|---|---|
| x | ۰ | ۰ |
| x − ۵ | ۵ | ۰ |
| x − ۵ | ۰ | ۵ |
| x − ۱۰ | ۵ | ۵ |
| x − ۱۰ | ۱ | ۹ |
| x − ۱ | ۱ | ۰ |
| x − ۱ | ۰ | ۱ |
| x − ۶ | ۵ | ۱ |
| x − ۶ | ۰ | ۶ |
| x − ۱۱ | ۵ | ۶ |
| x − ۱۱ | ۲ | ۹ |

کلید حل مسأله استفاده از رابطه‌ی $۲ = ۹\times۲ - ۵\times۴$ می‌باشد. با استفاده از معادله‌ی $۲ = ۵\times۵ - ۹\times۳$ نیز می‌توان به گونه‌ی دیگر به هدف رسید که آن را به خواننده وا می‌گذاریم. برای اعداد صحیح داده شده $a_n,\ldots,a_۲,a_۱$ عبارت $\alpha_۱a_۱ + \alpha_۲a_۲ + \ldots + \alpha_n a_n$ که در آن $\alpha_n,\ldots,\alpha_۲,\alpha_۱$ اعداد صحیح دلخواه هستند، ترکیب خطی $a_n,\ldots,a_۲,a_۱$ نامیده می‌شود. مثال‌های ۱. ۱۳ و ۱. ۱۴ به نظر مسائل نامرتبطی می‌آیند. اما در هر دوی آن‌ها ترکیب خطی دو عدد صحیح داده شده مطرح است. چه اتفاقی خواهد افتاد اگر در مثال ۱. ۱۳ جای (۳و۷) با (۳و۶) و در مثال ۱. ۱۴ جای (۹و۵) با (۹و۶) عوض شود؟ در حالت کلی نتیجه زیر را خواهیم داشت:

**قضیه ۱. ۷. [بزو]** برای اعداد صحیح مثبت $m$ و $n$ اعداد صحیح $x$و $y$ وجود دارند به طوری که

$$mx + ny = \gcd(m,n)$$

**اثبات:** از الگوریتم اقلیدس نتیجه می‌شود که

$$r_۱ = m - nq_۱ \ , \ r_۲ = -mq_۲ + n(۱ + q_۱q_۲) \ , \ \ldots$$

در حالت کلی $r_i = m\alpha_i + n\beta_i$ $(i = ۱,\ldots,k)$ چون $r_{i+۱} = r_{i-۱} - r_i q_{i+۱}$ است در نتیجه برای $i = ۲,\ldots,k-۱$

$$\alpha_{i+۱} = \alpha_{i-۱} - q_{i+۱}\alpha_i$$
$$\beta_{i+۱} = \beta_{i-۱} - q_{i+۱}\beta_i$$

و بالاخره $\gcd(m,n) = r_k = \alpha_k m + \beta_k n$.

با توجه به این که $\gcd(a,b)$، $ax+by$ را می‌شمارد و به دلیل قضیه بزو، برای اعداد صحیح داده شده $a,b,c$ معادله $ax+by=c$ برای اعداد صحیح $(x,y)$ جواب خواهد داشت اگر وفقط اگر $\gcd(a,b)$، $c$ را بشمارد. در جبر ما دستگاه معادلات را بطور کامل حل می‌کنیم. امّا در تئوری اعداد معمولاً به دنبال یافتن جواب‌های خاص مانند جواب‌های صحیح یا گویا هستیم. بنابراین در اکثر این دستگاه‌ها تعداد متغیرها از تعداد معادلات بیش‌تر است. این معادلات، معادلات دیوفانتین نامیده شده و به ریاضیدان یونان باستان دیوفانتوس نسبت داده می‌شوند. برای اعداد صحیح ثابت $a,b,c$، معادله‌ی $ax+by=c$ یک معادله‌ی دیوفانتین خطی دو متغیره است.

**نتیجه ۱. ۸.** اگر $a|bc$ و $\gcd(a,b)=1$ آنگاه $a|c$

**اثبات:** اگر $c=0$، حکم به وضوح برقرار است. فرض کنید $c\neq 0$. از $\gcd(a,b)=1$ با استفاده از قضیه بزو اعداد صحیح x و y وجود دارند که $ax+by=1$ بنابراین $acx+bcy=c$ چون $a$، $acx$ و $bcy$ را می‌شمارد پس $c$ را نیز می‌شمارد.

**نتیجه ۱. ۹.** $a$ و $b$ دو عدد نسبت به هم اول هستند. اگر $c$ یک عدد صحیح باشد به طوری که $a|c$ و $b|c$ آنگاه $ab|c$.

**اثبات:** چون $a|c$، عدد صحیح $x$ وجود دارد که $c=ax$ بنابراین $ax,b$ را می‌شمارد و چون $\gcd(a,b)=1$ است طبق نتیجه ۱. ۸. $b|x$؛ یعنی $x=by$ و از آنجا $c=aby$ و یا $ab|c$.

**نتیجه ۱. ۱۰.** اگر $p$ یک عدد اول بوده و $k$ یک عدد صحیح با شرط $1\leq k<p$ باشد آنگاه $p\left|\binom{p}{k}\right.$.

**اثبات:** از رابطه‌ی $k\binom{p}{k}=p\binom{p-1}{k-1}$ نتیجه می‌شود که $p$، $k\binom{p}{k}$ را می‌شمارد چون $\gcd(k,p)=1$ است، طبق نتیجه ۱. ۸. $p$، $\binom{p}{k}$ را می‌شمارد.

**مثال ۱. ۱۵.** [۲۰۰۱ روسیه] فرض کنید $a$ و $b$ دو عدد صحیح مثبت متمایز باشند به طوری که $ab(a+b)$ بر $a^2+ab+b^2$ بخش‌پذیر باشد. ثابت کنید $|a-b|>\sqrt[3]{ab}$.

**اثبات:** قرار می‌دهیم $\gcd(a,b)=g$ و می‌نویسیم $a=xg$ و $b=yg$ در حالی که $\gcd(x,y)=1$. بنابراین مقدار زیر یک عدد صحیح است

$$\frac{ab(a+b)}{a^2+ab+b^2}=\frac{xy(x+y)g}{x^2+xy+y^2}$$

توجه کنید که $\gcd(x^2+xy+y^2,x)=\gcd(y^2,x)=1$ و به طور مشابه $\gcd(x^2+xy+y^2,y)=1$. چون $\gcd(x+y,y)=1$ است، داریم

$$\gcd(x^2+xy+y^2,x+y)=\gcd(y^2,x+y)=1$$

با توجه به نتیجه ۱. ۸

$$x^2+xy+y^2 \mid g$$

و به موجب آن $g \geq x^2+xy+y^2$. بنابراین

$$|a-b|^3=|g(x-y)|^3=g^2|x-y|^3 .g \geq g^2\times 1\times(x^2+xy+y^2)>g^2xy=ab$$

و در نتیجه $|a-b|>\sqrt[3]{ab}$.

توجه کنید که مرحله‌ی کلیدی $x^2+xy+y^2 \mid g$ را می‌توان با یک عملیات جبری زیرکانه به صورت $a^3=(a^2+ab+b^2)a-ab(a+b)$ نیز به دست آورد.

## کوچک‌ترین مضرب مشترک

برای عدد صحیح مثبت $k$، $M_k$ را مجموعه‌ی همه‌ی مضارب $k$ می‌نامیم. برخلاف مجموعه‌ی $D_k$ که قبلاً تعریف شد، $M_k$ یک مجموعه‌ی نامتناهی است.

برای اعداد صحیح مثبت $s$ و $t$ کوچک‌ترین عضو مجموعه‌ی $M_s \cap M_t$، کوچک‌ترین مضرب مشترک $s$ و $t$ نامیده شده و با $\operatorname{lcm}(s,t)$ یا $[s,t]$ نشان داده می‌شود.

**قضیه ۱. ۱۱.**

(آ) اگر $\operatorname{lcm}(s,t)=m$ و $m=ss'=tt'$ آنگاه $\gcd(s',t')=1$

(ب) اگر $m'$ یک مضرب مشترک $s$ و $t$ بوده و $m'=ss'=tt'$ و $\gcd(s',t')=1$ آنگاه $m'=m$

(پ) اگر $m'$ یک مضرب مشترک $s$ و $t$ باشد آنگاه $m \mid m'$

(ت) اگر $m \mid s$ و $n \mid s$ آنگاه $\operatorname{lcm}(m,n) \mid s$

(ث) اگر $n$ عدد صحیح باشد، $n\,\mathrm{lcm}(s,t)=\mathrm{lcm}(ns,nt)$

(ج) اگر $s=p_1^{\alpha_1}\dots p_k^{\alpha_k}$ و $t=p_1^{\beta_1}\dots p_k^{\beta_k}$ که در آن برای $i=1,\dots,k$؛ $\alpha_i,\beta_i\geq 0$ آنگاه

$$\mathrm{lcm}(s,t)=p_1^{\max(\alpha_1,\beta_1)}\dots p_k^{\max(\alpha_k,\beta_k)}$$

خواص مطرح شده در قضیه ۱. ۱۱ به سادگی از تعریف ک.م.م به دست می‌آیند. لذا اثبات آن‌ها را به خواننده می سپاریم.

قضیه بعد ارتباط مهم بین بزرگ‌ترین مقسوم‌علیه مشترک و کوچک‌ترین مضرب مشترک را بیان می‌کند.

**قضیه ۱. ۱۲.** برای همه‌ی اعداد صحیح مثبت $m$ و $n$ رابطه‌ی زیر برقرار است:

$$mn=\gcd(m,n)\cdot\mathrm{lcm}(m,n)$$

**اثبات:** قرار می‌دهیم $m=p_1^{\alpha_1}\dots p_k^{\alpha_k}$ و $n=p_1^{\beta_1}\dots p_k^{\beta_k}$ که در آن برای $i=1,\dots,k$؛ $\alpha_i,\beta_i\geq 0$. از خاصیت ۱. ۶ (ث) و ۱. ۱۱ (ج) داریم:

$$\begin{aligned}\gcd(m,n)\cdot\mathrm{lcm}(m,n)&=p_1^{\min(\alpha_1,\beta_1)+\max(\alpha_1,\beta_1)}\dots p_k^{\min(\alpha_k,\beta_k)+\max(\alpha_k,\beta_k)}\\&=p_1^{\alpha_1+\beta_1}\dots p_k^{\alpha_k+\beta_k}=mn\end{aligned}$$

فرض کنید $a_1,a_2,\dots,a_n$ اعداد صحیح مثبت باشند. کوچک‌ترین مضرب مشترک $a_1,a_2,\dots,a_n$ با $\mathrm{lcm}(a_1,a_2,\dots,a_n)$ نشان داده شده و برابر کوچک‌ترین عدد صحیح مثبتی است که مضرب همه‌ی اعداد $a_1,a_2,\dots,a_n$ باشد. توجه کنید که قضیه ۱. ۱۲ را نمی‌توان به سادگی تعمیم داد. برای مثال رابطه‌ی زیر صحیح نیست:

$$\gcd(a,b,c)\cdot\mathrm{lcm}(a,b,c)=abc$$

(یافتن مثال نقض‌های جالب به عهده‌ی خواننده)

## تعداد مقسوم‌علیه‌ها

بحث را با سه مثال شروع می‌کنیم.

**مثال ۱. ۱۶.** [AIME۱۹۸۸] احتمال این که یک مقسوم‌علیسه مثبت $10^{99}$ که به طور تصادفی انتخاب شده است، مضرب صحیحی از $10^{88}$ باشد را محاسبه کنید.

**پاسخ:** مقسوم‌علیه‌های $۱۰^{۹۹}$ چه اعدادی هستند؟ آیا ۳ یک مقسوم‌علیه هست؟ ۲۲۰ چطور؟ تجزیه $۱۰^{۹۹}$ به عوامل اول، $۲^{۹۹}\times ۵^{۹۹}$ می‌باشد. بنابراین مقسوم‌علیه‌های $۱۰^{۹۹}$ به شکل $۲^{a}\times ۵^{b}$ هستند که $a$ و $b$ اعداد صحیح با شرط $۰\le a,b\le ۹۹$ می‌باشند. از آنجا که برای هر کدام از $a$ و $b$، ۱۰۰ انتخاب وجود دارد، عدد $۱۰^{۹۹}$، $۱۰۰\times ۱۰۰$ مقسوم‌علیه مثبت دارد. از این تعداد آنهایی که مضرب $۱۰^{۸۸}=۲^{۸۸}\times ۵^{۸۸}$ هستند باید در نامساوی $۸۸\le a,b\le ۹۹$ صدق کنند. بنابراین برای هریک از $a$ و $b$ ۱۲ انتخاب وجود دارد. به عبارت دیگر $۱۲\times ۱۲$ عدد از $۱۰۰\times ۱۰۰$ مقسوم‌علیه $۱۰^{۹۹}$، مضرب $۱۰^{۸۸}$ می‌باشند. در نتیجه احتمال موردنظر $\frac{۱۲\times ۱۲}{۱۰۰\times ۱۰۰}=\frac{۹}{۶۲۵}$ است.

**مثال ۱. ۱۷.** تعداد زوج مرتب‌های $(a,b)$ از اعداد صحیح مثبت را چنان پیدا کنید که کوچک‌ترین مضرب مشترک $a$ و $b$، $۲^{۳}\times ۵^{۷}\times ۱۱^{۱۳}$ باشد.

**پاسخ :** $a$ و $b$ هر دو مقسوم‌علیه $۲^{۳}\times ۵^{۷}\times ۱۱^{۱۳}$ می‌باشند لذا $a=۲^{x}\times ۵^{y}\times ۱۱^{z}$ و $b=۲^{s}\times ۵^{t}\times ۱۱^{u}$ که در آن $x,y,z,s,t$ و $u$ اعداد صحیح نامنفی هستند. چون $۲^{۳}\times ۵^{۷}\times ۱۱^{۱۳}$ کوچک‌ترین مضرب مشترک است پس $max(x,s)=۳$، $max(y,t)=۷$ و $max(z,u)=۱۳$. بنابراین $(x,s)$ برابر یکی از زوج‌های $(۳,۰)$، $(۳,۱)$، $(۳,۲)$، $(۳,۳)$، $(۳,۴)$، $(۳,۵)$ است و ۷ انتخاب برای $(x,s)$ وجود دارد. به طور مشابه برای $(y,t)$ و $(z,u)$ به ترتیب ۱۵ و ۲۷ انتخاب وجود دارد. به این ترتیب با استفاده از اصل ضرب $۷\times ۱۵\times ۲۷=۲۸۳۵$ زوج مرتب $(a,b)$ وجود دارد که کوچک‌ترین مضرب مشترکشان $۲^{۳}\times ۵^{۷}\times ۱۱^{۱۳}$ است.

**مثال ۱. ۱۸.** حاصل‌ضرب مقسوم‌علیه‌های مثبت و متمایز عدد $n=۴۲۰^{۴}$ تعیین کنید.

**پاسخ:** چون $n=(۲^{۲}\times ۳\times ۵\times ۷)^{۴}$ است، $k$ یک مقسوم‌علیه $n$ است اگر و فقط اگر بتوان آن را به شکل $۲^{a}\times ۳^{b}\times ۵^{c}\times ۷^{d}$ نوشت که $۰\le a\le ۸$ , $۰\le b\le ۴$ , $۰\le c\le ۴$ و $۰\le d\le ۴$. بنابراین برای $a,b,c$ و $d$ به ترتیب ۹، ۵، ۵ و ۵ مقدار ممکن وجود دارد در نتیجه $n$، $۹\times ۵\times ۵\times ۵=۱۱۲۵$ مقسوم‌علیه مثبت دارد. اگر $k\ne ۴۲۰^{۲}$ یک مقسوم‌علیه $n$ باشد آنگاه $\frac{۴۲۰^{۴}}{k}$ نیز مقسوم‌علیه دیگری از $n$ بوده و حاصل‌ضرب این دو مقسوم‌علیه $۴۲۰^{۴}$ است. بنابراین می‌توان ۱۱۲۴