۱۰۴ مسئله‌ی
تئوری اعداد

104
NUMBER
THEORY
PROBLEMS
From the Training of
the USA IMO Team

مترجم: سعید نعمتی

بسم الله الرّحمن الرّحیم

۱۰۴ مسئله تئوری اعداد

انتشارات خوشخوان

تألیف: تیتو آندرسکو، دورین آندریکا و زومینگ فنگ

ترجمه و ویرایش: سعید نعمتی

سرشناسه	: آندرسکو، تیتو، ۱۹۵۶ - م. Andreescu, Titu
عنوان و نام پدیدآور	: ۱۰۴ مسئله تئوری اعداد / [مؤلفان تیتو آندرسکو، دورین آندریکا، زومینگ فنگ]؛ مترجم سعید نعمتی.
مشخصات ناشر	: تهران: خوشخوان، ۱۳۸۷.
مشخصات ظاهری	: ۲۰۸ص.: نمودار
شابک	: ۹۷۸-۹۶۴-۸۶۰۱-۹۲-۳
وضعیت فهرست نویسی	: فیپا
یادداشت	: عنوان اصلی: 104 number theory Problems: From The Training of The USA IMO Team, 2007.
عنوان گسترده	: صد و چهار مسئله تئوری اعداد
موضوع	: نظریه اعداد -- مسائل، تمرین‌ها و غیره
شناسه افزوده	: آندریکا، دورین، ۱۹۵۶ - م. Andrica, D. (Dorin)
شناسه افزوده	: فنگ، زومینگ Feng, Zuming
شناسه افزوده	: نعمتی، سعید، ۱۳۶۰-، مترجم
رده بندی کنگره	: QA۲۴۱/آ۸ص۴ ۱۳۸۷
رده بندی دیویی	: ۵۱۲/۷۰۷۶
شماره کتابشناسی ملی	: ۱۳۰۸۸۸۱

انتشارات خوشخوان
www.Khoshkhan.ir

۱۰۴ مسئله تئوری اعداد
ناشر: انتشارات خوشخوان
مترجم: سعید نعمتی
حروف چین: فریده مراد زاده
طرح جلد: علی عباسی
چاپ اول، پاییز ۱۳۸۷
تیراژ: ۲۰۰۰
قیمت: ۲۵۰۰ تومان

شابک: ۹۷۸-۹۶۴-۸۶۰۱-۹۲-۳ ISBN: 978-964-8601-92-3

آدرس: تهران - خیابان جمهوری - خیابان دانشگاه شمالی - کوچه بهار - پلاک ۱۳۴ - طبقه دوم - انتشارات خوشخوان. تلفن: ۶۶۴۹۴۰۲۰

فهرست

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

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

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 $a \div b$ (یا 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 $n \times ۰ = ۰$ بنابراین برای هر عدد صحیح n، $n \mid ۰$. برای یک عدد صحیح ثابت n، مضارب n عبارتند از $۰, \pm n, \pm ۲n, \ldots$. 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 $۰ \nmid m$ زیرا برای همه‌ی اعداد صحیح k، $k \cdot ۰ = ۰ \neq m$)

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

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 $y \mid x$ 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 $|y| = |k| . |x| \geq |x|$

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 $x \mid y - (k_3 - k)x = \pm z$ و در نتیجه $z = \pm(k - k_3)x$.

برای (ج) $x \mid y$ و $y \mid x$ 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 أم 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 أم توسط دانش‌آموز j أم 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 $n_1, n_2, ..., n_k$ رابطه‌ی

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

برقرار باشد. بعد از مخرج مشترک گرفتن باید داشته باشیم $n_۱.n_۲...n_k = S_۱+S_۲+...+S_k$ که در آن S_iها 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 ($\{۱,۶\},\{۱,۳\}$) 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 $a|r'-r$. 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. ۴ (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 عد مرکب متوالی پیدا کنید؟

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

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:

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

که $p_1 \leq p_2 \leq \ldots \leq p_k$ و $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_h$ همگی اعداد اول هستند که $q_1 \leq q_2 \leq \ldots \leq q_h$ 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[2] 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 $a_0, a_1, \ldots, a_k$ 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 و $-q$ هستند (برای تمام اعداد صحیح مثبت i). از طرف دیگر معادلات $p(x)=-q$، $p(x)=0$ و $p(x)=q$ 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 $\gcd(m,n)=d$، $m=m''d'$، $n=n''d'$ و $\gcd(m'',n'')=1$ آنگاه $d=d'$

(ت) اگر d' یک مقسوم علیه مشترک m و n باشد آنگاه $\gcd(m,n),d'$ 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 $a_1,a_2,...,a_n$، $\gcd(a_1,a_2,..,a_n)$ بزرگ‌ترین مقسوم‌علیه مشترک بین همه‌ی اعداد $a_1,a_2,...,a_n$ است. بزرگ‌ترین مقسوم‌علیه مشترک $a_1,a_2,...,a_n$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 $d_{n-1}=\gcd(a_1,...,a_n)$ 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 $i=1,...,n$ ، $d\mid a_i$ آنگاه $d\mid\gcd(a_1,...,a_n)$

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

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

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

توجه کنید که $\gcd(a_1,...,a_n)=1$ 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 $a_1,a_2,...,a_n$ 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:

$$\begin{aligned} m &= n q_1 + r_1 \quad , \quad 1 \le r_1 < n \\ n &= r_1 q_2 + r_2 \quad , \quad 1 \le r_2 < r_1 \\ &\vdots \\ r_{k-2} &= r_{k-1} q_k + r_k \quad , \quad 1 \le r_k < r_{k-1} \\ r_{k-1} &= r_k q_{k+1} + r_{k+1} \quad , \quad r_{k+1} = 0 \end{aligned}$$

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 $۱۹۴۴ = ۹ \times ۲۱۶$ 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 $۲۰۰۲^k = ۳a_k + ۱$ ، 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_5	L_9
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 $۲\times۹-۲\times۵=۴$ می‌باشد. با استفاده از معادله‌ی $۳\times۹-۵\times۵=۲$ نیز می‌توان به گونه‌ی دیگر به هدف رسید که آن را به خواننده وا می‌گذاریم. برای اعداد صحیح داده شده $a_1,a_2,...,a_n$ عبارت $\alpha_1a_1+\alpha_2a_2+...+\alpha_na_n$ که در آن $\alpha_1,\alpha_2,...,\alpha_n$ اعداد صحیح دلخواه هستند، ترکیب خطی $a_1,a_2,...,a_n$ 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

$$r_1=m-nq_1\ ,\ r_2=-mq_2+n(1+q_1q_2)\ ,\ \dots$$

در حالت کلی $r_i=m\alpha_i+n\beta_i$ $(i=1,...,k)$ چون $r_{i+1}=r_{i-1}-r_iq_{i+1}$ است در نتیجه برای $i=2,...,k-1$

$$\alpha_{i+1}=\alpha_{i-1}-q_{i+1}\alpha_i$$
$$\beta_{i+1}=\beta_{i-1}-q_{i+1}\beta_i$$

و بالاخره $\gcd(m,n)=r_k=\alpha_km+\beta_kn$.

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 $a\mid bc$ و $\gcd(a,b)=1$ آنگاه $a\mid c$

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 $a\mid c$ و $b\mid c$ آنگاه $ab\mid c$.

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

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

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

(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 مقسوم‌علیه 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، $۲^{۹۹}\times۵^{۹۹}$ می‌باشد. بنابراین مقسوم‌علیه‌های $۱۰^{۹۹}$ به شکل $۲^{a}\times۵^{b}$ 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 $۱۰^{۹۹}$، ۱۰۰×۱۰۰ مقسوم‌علیه مثبت دارد. از این تعداد آنهایی که مضرب $۱۰^{۸۸}=۲^{۸۸}\times۵^{۸۸}$ 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 ۱۲×۱۲ عدد از ۱۰۰×۱۰۰ مقسوم‌علیه $۱۰^{۹۹}$، مضرب $۱۰^{۸۸}$ می‌باشند. در نتیجه احتمال موردنظر $\frac{۱۲\times۱۲}{۱۰۰\times۱۰۰}=\frac{۹}{۶۲۵}$ است.

مثال ۱. ۱۱. تعداد زوج مرتب‌های (a,b) از اعداد صحیح مثبت را چنان پیدا کنید که کوچک‌ترین مضرب مشترک a و b، $۲^{۳}\times۵^{۷}\times۱۱^{۱۳}$ باشد.

پاسخ : a و b هر دو مقسوم‌علیه $۲^{۳}\times۵^{۷}\times۱۱^{۱۳}$ می‌باشند لذا $a=۲^{x}\times۵^{y}\times۱۱^{z}$ و $b=۲^{s}\times۵^{t}\times۱۱^{u}$ که در آن x,y,z,s,t و u اعداد صحیح نامنفی هستند. چون $max(x,s)=۳$، $max(y,t)=۷$ کوچک‌ترین مضرب مشترک است پس $۲^{۳}\times۵^{۷}\times۱۱^{۱۳}$ و $max(z,u)=۱۳$. بنابراین (x,s) برابر یکی از زوج‌های $(۳,۰)$، $(۳,۱)$، $(۳,۲)$، $(۳,۳)$، $(۲,۳)$، $(۱,۳)$ 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 $۷\times۱۵\times۲۷=۲۸۳۵$ زوج مرتب (a,b) وجود دارد که کوچک‌ترین مضرب مشترکشان $۲^{۳}\times۵^{۷}\times۱۱^{۱۳}$ است.

مثال ۱. ۱۲. حاصل‌ضرب مقسوم‌علیه‌های مثبت و متمایز عدد $n=۴۲۰^{۴}$ تعیین کنید.

پاسخ: چون $n=(۲^{۲}\times۳\times۵\times۷)^{۴}$ است، k یک مقسوم‌علیه n است اگر و فقط اگر بتوان آن را به شکل $۲^{a}\times۳^{b}\times۵^{c}\times۷^{d}$ 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، $۹\times۵\times۵\times۵=۱۱۲۵$ 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

مقسوم‌علیه n (به جز $۴۲۰^{۲}$) را به ۵۶۲ زوج مقسوم‌علیه به شکل $(k, \frac{n}{k})$ تقسیم کرد که حاصل‌ضرب دو مقسوم‌علیه هر زوج برابر $۴۲۰^{۴}$ است. لذا جواب برابر است با:

$$۴۲۰^{۴\times۵۶۲} \times ۴۲۰^{۲} = ۴۲۰^{۲۲۵۰}$$

با قرار دادن سه مثال فوق در کنار یکدیگر دو نتیجه جالب در تئوری اعداد به دست می‌آید. برای عدد صحیح مثبت n، تعداد مقسوم‌علیه‌های n را با $\tau(n)$ نشان می‌دهیم. واضح است که:

$$\tau(n) = \sum_{d|n} ۱$$

نوشتن τ به شکل فوق به ما اجازه خواهد داد تا بعداً آن را به عنوان یک مثال از تابع حسابی ضربی مورد بحث قرار دهیم.

قضیه ۱. ۱۳. اگر $n = p_۱^{a_۱} p_۲^{a_۲} \dots p_k^{a_k}$ تجزیه n به عوامل اول باشد. آنگاه n

$$\tau(n) = (a_۱ + ۱)(a_۲ + ۱)\dots(a_k + ۱)$$

مقسوم‌علیه دارد.

نتیجه ۱. ۱۴. اگر $n = p_۱^{a_۱} p_۲^{a_۲} \dots p_k^{a_k}$ تجزیه n به عوامل اول باشد آنگاه

$$(۲a_۱ + ۱)(۲a_۲ + ۱)\cdots(۲a_k + ۱)$$

زوج مرتب متمایز از اعداد صحیح به صورت (a,b) وجود دارد که $lcm(a,b) = n$

نتیجه ۱. ۱۵. برای هر عدد صحیح مثبت n

$$\prod_{d|n} d = n^{\frac{\tau(n)}{۲}}$$

اثبات این سه قضیه مشابه کاری است که در مثال‌های ۱. ۱۶، ۱. ۱۷ و ۱. ۱۸ انجام شد. نکته جالب این است که این سه نتیجه را می‌توان به حالاتی که توان‌های اعداد اول در تجزیه یک عدد به عوامل اول، نامنفی هستند نیز تعمیم داد. (زیرا اگر برای برخی از $۱ \le i \le k$ ،$a_i = ۰$ باشد، آنگاه $a_i + ۱ = ۲a_i + ۱ = ۱$ که تأثیری در حاصل‌ضرب نخواهد داشت).

نتیجه ۱. ۱۶. برای هر عدد صحیح مثبت n، $\tau(n) \leq 2\sqrt{n}$

اثبات: فرض کنید $d_1 < d_2 < \ldots < d_k$، مقسوم‌علیه‌هایی از n باشند که از $\sqrt{n}$ بزرگ‌تر نیستند. بقیه مقسوم‌علیه‌ها عبارتند از

$$\frac{n}{d_1}, \frac{n}{d_2}, \ldots, \frac{n}{d_k}$$

بنابراین $\tau(n) \leq 2k \leq 2\sqrt{n}$.

مجموع مقسوم‌علیه‌ها

برای عدد صحیح مثبت n، مجموع مقسوم‌علیه‌های مثبت آن شامل ۱ و n را با $\sigma(n)$ نشان می‌دهیم واضح است که:

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

این شکل نمایش به ما کمک خواهد کرد تا نشان دهیم که σ ضربی است.

قضیه ۱. ۱۷. اگر $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ تجزیه n به عوامل اول باشد آنگاه

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}$$

اثبات: مقسوم‌علیه‌های n را می‌توان به شکل $p_1^{a_1} \ldots p_k^{a_k}$ نوشت که در آن $a_1, \ldots, a_k$ اعداد صحیح هستند که در شرایط $0 \leq a_1 \leq \alpha_1$, $0 \leq a_2 \leq \alpha_2$, ... و $0 \leq a_k \leq \alpha_k$ صدق می‌کنند. هر مقسوم‌علیه n، دقیقاً یک بار در بسط حاصل عبارت زیر ظاهر می‌شود.

$$(1 + p_1 + \cdots + p_1^{\alpha_1}) \cdots (1 + p_k + \cdots + p_k^{\alpha_k})$$

لذا با استفاده از فرمول جمع تصاعد هندسی با جملات محدود به نتیجه مطلوب خواهیم رسید.

$$1 + r + \ldots + r^k = \frac{r^{k+1} - 1}{r - 1}$$

مثال ۱. ۱۹. مجموع مقسوم‌علیه‌های مثبت و زوج ۱۰۰۰۰ را پیدا کنید.

پاسخ: مقسوم‌علیه‌های زوج ۱۰۰۰۰ را می‌توان به شکل $2^a \times 5^b$ نوشت که a و b اعداد صحیح با شرایط $1 \le a \le 5$ و $0 \le b \le 5$ هستند. هر مقسوم‌علیه زوج ۱۰۰۰۰ دقیقاً یک بار در بسط عبارت زیر ظاهر می‌شوند.

$$(2+2^2+2^3+2^4+2^5)(1+5+5^2+5^3+5^4+5^5) = 62 \times \frac{5^6-1}{5-1}$$
$$= 244172$$

حساب پیمانه‌ای [همنهشتی]

فرض کنید a, b و m اعداد صحیح باشند و $m \neq 0$. گوییم a و b به پیمانه m هم‌نهشت هستند اگر m، $a-b$ را بشمارد. این رابطه را به شکل $a \equiv b \pmod m$ نشان می‌دهیم. رابطه‌ی "$\equiv$" روی مجموعه‌ی $\mathbb{Z}$ اعداد صحیح، رابطه‌ی هم‌نهشتی نامیده می‌شود. اگر m، $a-b$ را نشمارد گوییم a و b به پیمانه‌ی m هم‌نهشت نیستند و می‌نویسیم $a \not\equiv b \pmod m$.

قضیه ۱. ۱۸.

(آ) $a \equiv a \pmod m$ (بازتابی)

(ب) اگر $a \equiv b \pmod m$ و $b \equiv c \pmod m$ آنگاه $a \equiv c \pmod m$ (تعدی)

(پ) اگر $a \equiv b \pmod m$ آنگاه $b \equiv a \pmod m$

(ت) اگر $a \equiv b \pmod m$ و $c \equiv d \pmod m$ آنگاه $a+c \equiv b+d \pmod m$ و $a-c \equiv b-d \pmod m$

(ث) اگر $a \equiv b \pmod m$ آنگاه برای هر عدد صحیح k، $ka \equiv kb \pmod m$

(ج) اگر $a \equiv b \pmod m$ و $c \equiv d \pmod m$ آنگاه $ac \equiv bd \pmod m$. در حالت کلی اگر $a_i \equiv b_i \pmod m$ آنگاه $a_1 \dots a_k \equiv b_1 \dots b_k \pmod m$. در حالت خاص اگر $a \equiv b \pmod m$ آنگاه برای هر عدد صحیح مثبت k، $a^k \equiv b^k \pmod m$

(چ) $a \equiv b \pmod{m_i}$، $(i = 1, \dots, k)$ اگر و فقط اگر $a \equiv b \pmod{lcm(m_1, \dots, m_k)}$ در حالت خاص اگر $m_1, \dots, m_k$ دو به دو نسبت به هم اول باشند آنگاه $a \equiv b \pmod{m_i}$، $(i = 1, \dots, k)$ اگر و فقط اگر $a \equiv b \pmod{m_1 \dots m_k}$

اثبات: اثبات‌ها ساده هستند. ما در اینجا اثبات قسمت (چ) را می‌آوریم و بقیه را به خواننده می‌سپاریم.

از (پیمانه m_i) $a\equiv b$، $i=1,\dots,k$ نتیجه می‌گیریم که $m_i \mid a-b$. بنابراین $a-b$ مضرب مشترک $m_1,\dots,m_k$ است و لذا $lcm(m_1,\dots,m_k) \mid a-b$ ویا به عبارت دیگر (پیمانه $lcm(m_1,\dots,m_k)$) $a\equiv b$.

از طرف دیگر از (پیمانه $lcm(m_1,\dots,m_k)$) $a\equiv b$ و این حقیقت که $lcm(m_1,\dots,m_k)$، m_i را می‌شمارد نتیجه می‌گیریم که (پیمانه m_i) $a\equiv b$، $i=1,\dots,k$.

قضیه ۱. ۱۹. فرض کنید a,b و n اعداد صحیح باشند و $n\neq 0$ به طوری که $a=nq_1+r_1$، $b=nq_2+r_2$ و $0\le r_1,r_2<|n|$. (پیمانه n) $a\equiv b$ اگر و فقط اگر $r_1=r_2$.

اثبات: از $a-b=n(q_1-q_2)+(r_1-r_2)$ نتیجه می‌شود که $n \mid a-b$ اگر و فقط اگر $n \mid r_1-r_2$ با توجه به این که $|r_1-r_2|<|n|$ است $n \mid r_1-r_2$ اگر و فقط اگر $r_1=r_2$.

مثال ۱. ۲۰. ثابت کنید بی‌نهایت عدد اول به شکل $4k-1$ وجود دارد؛ یعنی به پیمانه ۴ با ۳ هم‌نهشت هستند.

اثبات: ابتدا توجه می‌کنیم که حداقل یک عدد فرد p با خاصیت (پیمانه ۴) $p\equiv 3$ وجود دارد ($p\equiv 3$). فرض کنید فقط تعداد محدودی عدد اول به پیمانه ۴ با ۳ هم‌نهشت هستند. آن اعداد اول را $p_1,p_2,\dots,p_k$ می‌نامیم و P را برابر حاصل‌ضرب آن‌ها قرار می‌دهیم. داریم (پیمانه ۴) $4P-1\equiv 3$. اگر همه‌ی عوامل اول $4P-1$ به پیمانه ۴ با ۱ هم‌نهشت باشند آنگاه با توجه به قضیه ۱. ۱۸ (ج). $4P-1$ به پیمانه ۴ با ۱ هم‌نهشت خواهد بود. بنابراین حداقل یکی از عوامل اول $4P-1$ به پیمانه ۴ با ۳ هم‌نهشت خواهد بود که آن را p می‌نامیم. از طرف دیگر برای هر i با شرط $1\le i\le k$، $gcd(4P-1,p_i)=1$ است. بنابراین عدد اول دیگری پیدا کردیم که به پیمانه ۴ با ۳ هم‌نهشت است و با فرض ما تناقض دارد. لذا بی نهایت عدد اول به شکل $4k-1$ وجود دارد.

به طور کاملاً مشابه می‌توان نشان داد که بی‌نهایت عدد اول به شکل $6k-1$ وجود دارد. می‌توان هم‌نهشتی را به عنوان (بخشی از) یک تصاعد حسابی مشاهده کرد. به طور مثال می‌توان دو نتیجه اخیر را به صورت زیر نوشت: بی‌نهایت عدد اول در تصاعد حسابی $\{-1+ka\}_{k=1}^{\infty}$ با $a=4$ و $a=6$ وجود دارد. این نتایج حالت خاصی از قضیه معروف دیریکله[5] است:

در هر تصاعد حسابی از اعداد صحیح که در آن قدرنسبت تصاعد با جملات آن نسبت به هم اول هستند، بی‌نهایت عدد اول وجود دارد. به عبارت دیگر اگر a و m نسبت به هم اول باشند آنگاه بی‌نهایت عدد اول وجود دارد به طوری که (پیمانه m) $p\equiv a$.

---

[5] Dirichlet

دیریکله هم‌چنین چگالی (یا به عبارت ساده‌تر، دوره وقوع) این اعداد اول در مجموعه‌ی همه‌ی اعداد اول را محاسبه کرد. این کار او یک مرحله‌ی مهم دیگر در تئوری اعداد تحلیلی است. اثبات این مطلب خارج از بحث این کتاب است. شکل جزئی‌تر این نتیجه در بخش تعاریف و قضایا در انتهای کتاب ارائه می‌شود. برخی مسائل این کتاب اگر مستقیماً از این قضیه استفاده شود، ساده خواهند شد. اما همه‌ی این مسائل را می‌توان با روش‌های دیگر نیز حل کرد و ما اکیداً به خوانندگان توصیه می‌کنیم که دنبال این روش‌های متفاوت باشند چرا که توانایی حل مسأله را در آن‌ها افزایش خواهد داد.

طبیعی است که در مثال ۱. ۲۰. با پیمانه ۴ کار کنیم. خیلی اوقات، چنین انتخابی واضح نیست. کلید حل بسیاری از مسائل در انتخاب صحیح پیمانه است.

مثال ۱. ۲۱. [۲۰۰۱ روسیه] همه‌ی اعداد اول p و q را چنان بیابید که $p+q=(p-q)^3$

پاسخ: تنها اعداد اول مطلوب $p=5$ و $q=3$ است.

چون $(p-q)^3=p+q\neq 0$ است، p و q متمایز بوده و لذا نسبت به هم اول می‌باشند. با توجه به اینکه (پیمانه $p+q$) $p-q\equiv 2p$ است، با استفاده از رابطه‌ی داده شده خواهیم داشت (پیمانه $p+q$) $8p^3\equiv 0$. از آن جا که p و q نسبت به هم اول هستند، p و $p+q$ نیز نسبت به هم اولند. بنابراین (پیمانه $p+q$) $8\equiv 0$ که به معنای آن است که $p+q$، ۸ را می‌شمارد.

به طور مشابه با در نظر گرفتن پیمانه $p-q$ خواهیم داشت (پیمانه $p-q$) $2p\equiv 0$ و چون p و q نسبت به هم اول هستند، p و $p-q$ نیز نسبت به هم اولند. در نتیجه (پیمانه $p-q$) $2\equiv 0$ یا $p-q$، ۲ را می‌شمارد. به سادگی می‌توان دید تنها اعدادی که رابطه‌ی موردنظر را برآورده می‌کنند $(p,q)=(5,3)$ هستند.

روش دیگری نیز برای حل مسأله اخیر وجود دارد: با قرار دادن $p-q=a$ و $p+q=a^3$، p و q به صورت زیر بدست می‌آیند

$$p=\frac{a^3+a}{2} \quad \text{و} \quad q=\frac{a^3-a}{2}$$

این نوع جایگزینی یک روش بسیار مرسوم در حل معادلات دیوفانتین است.

مثال ۱. ۲۲. [۲۰۰۱ بالتیک] فرض کنید a یک عدد صحیح فرد باشد. ثابت کنید $a^{2^n}+2^{2^n}$ و $a^{2^m}+2^{2^m}$ برای همه‌ی اعداد صحیح مثبت m و n $(m\neq n)$ نسبت به هم اول هستند.

پاسخ: بدون از دست دادن کلیت مسأله فرض کنید $m > n$. برای هر عدد اول p که $a^{۲^n} + ۲^{۲^n}$ را می‌شمارد داریم

$$a^{۲^n} \equiv -۲^{۲^n} \quad (\text{پیمانه } p)$$

طرفین رابطه‌ی فوق را $m-n$ بار به توان ۲ می‌رسانیم تا به رابطه‌ی زیر برسیم:

$$a^{۲^m} \equiv ۲^{۲^m} \quad (\text{پیمانه } p)$$

به دلیل فرد بودن a، $p \neq ۲$ است. بنابراین (پیمانه p) $۲^{۲^m} + ۲^{۲^m} = ۲^{۲^m+۱} \not\equiv ۰$. به این ترتیب:

$$a^{۲^m} \equiv ۲^{۲^m} \not\equiv -۲^{۲^m} \quad (\text{پیمانه } p)$$

بنابراین $p \nmid a^{۲^m} + ۲^{۲^m}$ که نتیجه مطلوب را می‌رساند.

اگر در مثال اخیر $a=۱$ باشد، یک خاصیت از اعداد فرما بدست می‌آید که به زودی بحث خواهند شد.

مثال ۱. ۲۳. تعیین کنید که آیا بی‌نهایت عدد صحیح زوج مانند k وجود دارد به طوری که برای هر عدد اول p عدد $p^۲ + k$ مرکب باشد.

پاسخ: جواب مثبت است.

در ابتدا توجه کنید که اگر $p=۲$ باشد، $p^۲ + k$ همواره برای همه‌ی اعداد زوج k، مرکب است. اگر $p>۳$ باشد آنگاه (پیمانه ۳) $p^۲ \equiv ۱$. بنابراین اگر k یک عدد صحیح زوج باشد که (پیمانه ۳) $k \equiv ۲$ آنگاه $p^۲ + k$ برای همه‌ی اعداد اول $p>۳$ مرکب خواهد بود ($p^۲ + k$ بزرگ‌تر از ۳ و بخش‌پذیر بر ۳ است)

سرانجام توجه کنید که برای $p=۳$ اگر (پیمانه ۵) $k \equiv ۱$ آنگاه (پیمانه ۵) $۳^۲ + k \equiv ۰$ است.

با کنار هم قرار دادن مباحث فوق نتیجه می‌گیریم که همه‌ی اعداد صحیح مثبتی که شرایط

$$\begin{cases} k \equiv ۰ & (\text{پیمانه } ۲) \\ k \equiv ۲ & (\text{پیمانه } ۳) \\ k \equiv ۱ & (\text{پیمانه } ۵) \end{cases} \qquad (*)$$

را برآوده سازند، پاسخ مسأله خواهند بود. با استفاده از قضیه ۱. ۱۸ (چ) (پیمانه $lcm(۲,۳,۵) =$) (پیمانه ۳۰) را مورد بررسی قرار می‌دهیم. به سادگی می‌توان دید که همه‌ی اعداد صحیح مثبت k با شرط (پیمانه ۳۰) $k \equiv ۲۶$ دستگاه فوق را برآوده کرد و لذا پاسخ مسأله خواهند بود.

دستگاه (*) یک دستگاه هم‌نهشتی خطی است و هر یک از سه معادله این دستگاه یک معادله‌ی هم‌نهشتی خطی است. پاسخ‌های دستگاه‌های هم‌نهشتی خطی پس از مطالعه‌ی قضیه مانده چینی قابل بحث خواهند بود. تفاوت اصلی بین حل معادلات جبری و حل معادلات هم‌نهشتی، محدودیت تقسیم در حالت دوم است. برای مثال در جبر $۴x = ۴y$ معادل با $x = y$ است. اما در حساب پیمانه‌ای از (پیمانه ۶) $۴x \equiv ۴y$ لزوماً نمی‌توان نتیجه گرفت که (پیمانه ۶) $x \equiv y$. (چرا؟) از طرف دیگر از (پیمانه ۱۵) $۴x \equiv ۴y$ می‌توان نتیجه گرفت که (پیمانه ۱۵) $x \equiv y$. (چرا؟) قضیه ۱. ۱۸ (چ) نقش کلیدی در این اختلاف بازی می‌کند. در جبر $xy = ۰$ بیان می‌کند که $x = ۰$ یا $y = ۰$ است. اما در حساب پیمانه‌ای از (پیمانه m) $xy \equiv ۰$ نمی‌توان نتیجه گرفت که (پیمانه m) $y \equiv ۰$ یا (پیمانه m) $x \equiv ۰$. (برای مثال (پیمانه ۱۵) $۳ \times ۵ \equiv ۰$ اما (پیمانه ۱۵) $۳ \not\equiv ۰$ و (پیمانه ۱۵) $۵ \not\equiv ۰$). این موضوع به طور جزئی هنگام بحث در معادلات هم‌نهشتی خطی مورد بررسی قرارمی‌گیرد. برای یک پیش زمینه کوچک، نتیجه ۱. ۵ را مجدداً به زبان حساب پیمانه‌ای می‌نویسیم نتیجه ۱. ۲۰. فرض کنید p یک عدد اول باشد. اگر x و y اعداد صحیح باشند به طوری که (پیمانه p) $xy \equiv ۰$ آنگاه یا (پیمانه p) $x \equiv ۰$ یا (پیمانه p) $y \equiv ۰$ یا هر دو.

این نتیجه یک مثال از تغییر چهره‌ی یک ایده مشترک در تئوری اعداد است: $p \mid xy$ (نماد بخش‌پذیری)، (پیمانه p) $xy \equiv ۰$ (نماد هم‌نهشتی) و $p = kxy$ (به شکل معادله‌ی دیوفانتین). کاربردهای ساده نتایج ۱. ۸ و ۱. ۹ نیز منجر به نتایج زیر می‌شود.

نتیجه ۱. ۲۱. m یک عدد صحیح مثبت و a, b, c اعداد صحیح هستند که $c \neq ۰$. اگر (پیمانه m) $ac \equiv bc$ آنگاه:

$$a \equiv b \quad (\text{پیمانه } \frac{m}{gcd(c, m)})$$

نتیجه ۱. ۲۲. فرض کنید m یک عدد صحیح مثبت باشد. a یک عدد صحیح نسبت به m اول است. اگر $a_۱$ و $a_۲$ اعداد صحیح باشند به طوری که (پیمانه m) $a_۱ \not\equiv a_۲$ آنگاه (پیمانه m) $a_۱a \not\equiv a_۲a$

رابطه‌ی زیر در کاهش توان در یک رابطه‌ی هم‌نهشتی مفید است.

نتیجه ۱. ۲۳. فرض کنید m یک عدد صحیح مثبت و a و b اعداد صحیح و نسبت به m اول باشند. اگر x و y اعداد صحیح باشند به طوری که (پیمانه m) $a^x \equiv b^x$ و (پیمانه m) $a^y \equiv b^y$ آنگاه

$$a^{gcd(x,y)} \equiv b^{gcd(x,y)} \quad (\text{پیمانه } m)$$

اثبات: با استفاده از قضیه بزو اعداد صحیح نامنفی u و v وجود دارند به طوری که $gcd(x,y) = ux - vy$. با شرایط داده شده داریم

$$a^{vy} \equiv b^{vy} \quad (\text{پیمانه } m) \quad \text{و} \quad a^{ux} \equiv b^{ux} \quad (\text{پیمانه } m)$$

در نتیجه (پیمانه m) $a^{ux}b^{vy} \equiv a^{vy}b^{ux}$. از $gcd(a,m) = gcd(b,m) = 1$ و نتیجه ۱. ۲۱. داریم

$$a^{gcd(x,y)} \equiv a^{ux-vy} \equiv b^{ux-vy} \equiv b^{gcd(x,y)} \quad (\text{پیمانه } m)$$

دستگاه مانده‌ها

از قضایای ۱. ۱۸ (آ)، (ب) و (پ) نتیجه می‌گیریم که برای هر عدد صحیح مثبت m می‌توان اعداد صحیح را با توجه به باقی‌مانده‌هایشان در تقسیم بر m به دسته‌های یکتایی دسته‌بندی کرد. به وضوح m دسته به این صورت وجود خواهد داشت. مجموعه‌ی S از اعداد صحیح یک دستگاه کامل مانده‌ها به پیمانه n نامیده می‌شود. اگر برای هر $0 \le i \le n-1$ دقیقاً یک عضو مانند s در S وجود داشته باشد به طوری که (پیمانه n) $i \equiv s$ آنگاه واضح است که مجموعه‌ی $\{a, a+1, a+2, \dots, a+m-1\}$ برای هر عدد صحیح a یک دستگاه کامل مانده‌ها به پیمانه m است. در حالت خاص برای $a = 0$، $\{0, 1, \dots, m-1\}$ کوچک‌ترین دستگاه کامل مانده‌ها از اعداد صحیح نامنفی است. استفاده از دو دستگاه کامل مانده‌ها به صورت $\{0, \pm 1, \pm 2, \dots, \pm k\}$ برای $m = 2k+1$ و $\{0, \pm 1, \pm 2, \dots, \pm(k-1), k\}$ برای $m = 2k$ نیز رایج می‌باشد.

مثال ۱. ۲۴. n یک عدد صحیح است. ثابت کنید:

(۱) $n^2 \equiv 0$ یا ۱ (پیمانه ۳) (۲) m_1 یا ± 1 (پیمانه ۵)

(۳) $n^2 \equiv 0$ یا ۱ یا ۴ (پیمانه ۸) (۴) $n^3 \equiv 0$ یا ± 1 (پیمانه ۹)

(۵) $n^4 \equiv 0$ یا ۱ (پیمانه ۱۶)

همه روابط فوق را می‌توان با بررسی دستگاه‌های کامل مانده‌ها اثبات کرد که ما آن‌ها را به خواننده می‌سپاریم. در ضمن به خوانندگان توصیه می‌شود روابط فوق را یک بار دیگر پس از مطالعه‌ی قضیه‌ی اویلر، مرور نمایند.

مثال ۱. ۲۵. [۲۰۰۳ رومانی] اعداد اول $n_1 < n_2 < \ldots < n_{31}$ را در نظر بگیرید. ثابت کنید اگر ۳۰ عدد $n_1^4 + n_2^4 + \ldots + n_{31}^4$ را بشمارد آنگاه می‌توان در بین این اعداد سه عدد اول متوالی پیدا کرد.

پاسخ: قرار دهید $s = n_1^4 + n_2^4 + \ldots + n_{31}^4$.

در ابتدا ادعا می‌کنیم $n_1 = 2$ است. در غیر این صورت همه‌ی اعداد n_i, $1 \le i \le 31$ فرد هستند و در نتیجه s فرد خواهد بود که تناقض است.

حال ادعا می‌کنیم $n_2 = 3$ است. در غیر این صورت برای هر $1 \le i \le 31$ داریم (پیمانه ۳) $n_i^4 \equiv 1$ و در نتیجه (پیمانه ۳) $s \equiv 31 \equiv 1$ که تناقض است.

در پایان ثابت می‌کنیم $n_3 = 5$ است. اگر این طور نباشد آنگاه (پیمانه ۵) $n_i^2 \equiv \pm 1$ و (پیمانه ۵) $n_i^4 \equiv 1$ ($1 \le i \le 31$). بنابراین (پیمانه ۵) $s \equiv 31 \equiv 1$ که تناقض است.

بنابراین سه عدد اول متوالی ۲، ۳ و ۵ در اعداد اول مذکور وجود دارند.

مثال ۱. ۲۶. m یک عدد صحیح مثبت زوج است. فرض کنید $\{b_1, \ldots, b_m\}$ و $\{a_1, \ldots, a_m\}$ دو دستگاه کامل مانده‌ها به پیمانه‌ی m باشند. ثابت کنید مجموعه‌ی $\{a_1 + b_1, a_2 + b_2, \ldots, a_m + b_m\}$ یک دستگاه کامل مانده‌ها نیست.

اثبات: به روش غیر مستقیم و با فرض آن که مجموعه‌ی موردنظر دستگاه کامل مانده‌ها هست حکم را اثبات می‌کنیم. لذا:

$$\begin{aligned} 1+2+\cdots+m &\equiv (a_1+b_1)+(a_2+b_2)+\cdots+(a_m+b_m) \\ &\equiv (a_1+a_2+\cdots+a_m)+(b_1+b_2+\cdots+b_m) \\ &\equiv 2(1+2+\cdots+m) \quad (\text{پیمانه } m) \end{aligned}$$

در نتیجه (پیمانه m) $1+2+\ldots+m \equiv 0$ یا $m \mid \frac{m(m+1)}{2}$ که برای اعداد صحیح زوج درست نیست. بنابراین فرض ما غلط بوده است.

مثال ۱. ۲۷. a یک عدد صحیح مثبت است. همه‌ی اعداد صحیح مثبت m را چنان پیدا کنید که

$$\{a \times 1, a \times 2, \ldots, a \times m\}$$

یک دستگاه کامل مانده‌ها به پیمانه m باشد.

پاسخ: جواب مسأله مجموعه‌ی اعداد صحیح مثبت m است که a و m نسبت به هم اول باشند. مجموعه‌ی داده شده را S_m می‌نامیم. ابتدا نشان می‌دهیم اگر $gcd(a,m)=1$ باشد آنگاه S_m یک دستگاه کامل مانده‌ها است. از آنجا که این مجموعه m عضو دارد کافی است ثابت کنیم اعضای این مجموعه با یکدیگر به پیمانه m هم‌نهشت نیستند. فرض کنید برای $1 \le i < j \le m$، $a \times i \equiv a \times j \pmod m$ باشد. چون $gcd(a,m)=1$ است، از نتیجه ۱. ۲۱ خواهیم داشت $i \equiv j \pmod m$ که به دلیل $|i-j| < m$، غیر ممکن است. پس فرض ما غلط بوده و S_m یک دستگاه کامل مانده‌ها به پیمانه m است.

از طرف دیگر اگر $g = gcd(a,m) > 1$ باشد آنگاه $a = a_1 g$، $m = m_1 g$ و m_1 یک عدد صحیح مثبت کوچک‌تر از m است. داریم: $am_1 \equiv a_1 m_1 g \equiv a_1 m \equiv am \equiv 0 \pmod m$. بنابراین S_m یک دستگاه کامل مانده‌ها نیست.

به طور مشابه می‌توان نتیجه زیر را به دست آورد.

قضیه ۱. ۲۴. m یک عدد صحیح مثبت است. a و b عدد صحیح بوده و a و m نسبت به هم اول هستند. فرض کنید S یک مجموعه‌ی کامل مانده‌ها به پیمانه m باشد. مجموعه‌ی

$$T = aS + b = \{ as + b \mid s \in S \}$$

نیز یک مجموعه‌ی کامل مانده‌ها به پیمانه m است.

حال با توجه به ابزارهای موجود، کمی بیش‌تر درباره‌ی معادلات هم‌نهشتی خطی بحث می‌کنیم.

قضیه ۱. ۲۵. m یک عدد صحیح مثبت است. a و b عدد صحیح بوده و a و m نسبت به هم اول هستند. اعداد صحیح x وجود دارند به طوری که $ax \equiv b \pmod m$ و همه‌ی این اعداد صحیح دقیقاً یک دسته هم‌نهشتی به پیمانه m را شکل می‌دهند.

اثبات: فرض کنید $\{ c_1, c_2, \ldots, c_m \}$ یک دستگاه کامل مانده‌ها به پیمانه m باشد. از قضیه ۱. ۲۴

$$\{ ac_1 - b, ac_2 - b, \ldots, ac_m - b \}$$

نیز یک دستگاه کامل مانده‌هاست. بنابراین c_i وجود دارد که $ac_i - b \equiv 0 \pmod m$ یا c_i یک پاسخ معادله‌ی هم‌نهشتی $ax \equiv b \pmod m$ است. به سادگی می‌توان دید که همه‌ی اعداد هم‌نهشت با c_i به پیمانه m نیز در معادله صدق می‌کنند. از طرف دیگر اگر دو عدد x و x' درمعادله صدق کنند داریم $ax \equiv ax' \pmod m$ و از نتیجه ۱. ۲۱ $x \equiv x' \pmod m$.

در حالت خاص، قرار دادن $b=1$ در قضیه ۱. ۲۵ نشان می‌دهد که اگر $gcd(a,m)=1$ باشد، عددی مانند x وجود دارد چنان که $ax \equiv 1 \pmod m$. در این حالت x را معکوس a به پیمانه m

نامیده و با (پیمانه m) $\frac{1}{a}$ یا a^{-1} نشان می‌دهیم. چون همه‌ی چنین اعدادی دقیقاً یک دسته هم-نهشتی m را تشکیل می‌دهند، معکوس a به پیمانه‌ی m برای همه‌ی اعداد صحیح نسبت به m اول بخوبی تعریف شده است.

حال می‌توانیم قضیه ویلسون را اثبات کنیم:

قضیه ۱. ۲۶. [قضیه ویلسون] برای هر عدد اول p، (پیمانه p) $(p-1)! \equiv -1$

اثبات: رابطه برای $p=2$ و $p=3$ برقرار است بنابراین می‌توان فرض کرد $p \geq 5$. مجموعه‌ی $S=\{2,3,\ldots,p-2\}$ را در نظر بگیرید. چون p اول است برای هر s در S، s یک معکوس یکتای s' در مجموعه‌ی $\{1,2,\ldots,p-1\}$ دارد. علاوه بر آن $s' \neq 1$ و $s' \neq p-1$؛ بنابراین $s' \in S$ و در ضمن $s' \neq s$ است زیرا در غیر این صورت (پیمانه p) $s^2 \equiv 1$ می‌باشد که زمانی اتفاق می‌افتد که $p \mid s-1$ یا $p \mid s+1$ که چون $s+1 < p$ امکان ندارد. پس می‌توان اعضای S را به $\frac{p-3}{2}$ زوج متمایز (s', s) گروه‌بندی کرد که (پیمانه p) . با ضرب کردن این هم‌نهشتی‌ها در هم خواهیم داشت (پیمانه p) $(p-2)! \equiv 1$ و حکم اثبات می‌شود.

توجه کنید که عکس قضیه ویلسون نیز صحیح است یعنی؛ اگر برای عدد صحیح $n \geq 2$ (پیمانه n) $(n-1)! \equiv -1$ برقرار باشد آنگاه n عددی اول است. اگر $n = n_1 n_2$ باشد $(n_1, n_2 \geq 2)$ خواهیم داشت $(n-1)! \times \ldots \times n_1 \times \ldots \times 2 \times 1 + (n-1)$ که $n_1 \mid 1$ که امکان ندارد. به این ترتیب می‌توان از این قضیه برای تعیین اول بودن یک عدد استفاده کرد. (البته این روش خیلی عملی نیست زیرا برای nهای بزرگ، $(n-1)!$ خیلی بزرگ خواهد بود)

در اکثر موارد تفاوت چندانی وجود ندارد که از یک دستگاه کامل مانده‌های خاص برای حل یک مسأله خاص استفاده کنیم. در اینجا یک مثال متفاوت ارائه می‌کنیم.

مثال ۱. ۲۶. [*MOSP* ۲۰۰۵] در هر کنج یک مکعب، یک عدد صحیح نوشته می‌شود. یک «انتقال مجاز» در مکعب عبارت است از انتخاب یک کنج مکعب و اضافه کردن مقدار نوشته شده در آن کنج به مقادیر نوشته شده در برخی از کنج‌های مجاور (یعنی انتخاب یک کنج با مقدار نوشته شده x در آن و یک کنج مجاور با مقدار نوشته شده y در آن، و عوض کردن y با $x+y$). ثابت کنید می‌توان بعد از تعداد متناهی از «انتقال‌های مجاز» اعداد نوشته شده در هر کنج را چنان تغییر داد که در نهایت هر ۸ عدد صحیح نوشته شده به پیمانه ۲۰۰۵ یکی باشند.

دو راه‌حل برای این مسأله ارائه می‌کنیم. توجه کنید که اگر ما یک «انتقال مجاز» را در نظر گرفته و آن را ۲۰۰۴ بار تکرار کنیم. به پیمانه ۲۰۰۵ معادل این است که y را با $-x$ y جایگزین کنیم. ۲۰۰۴ بار تکرار از یک انتقال مجاز را «سوپر انتقال» می‌نامیم.

پاسخ اول: اعداد صحیح نوشته شده را با هم‌نهشتشان در دسته‌های هم‌نهشتی $۲۰۰۵,\ldots,۲,۱$ جایگزین می‌کنیم اگر همه‌ی دسته‌های هم‌نهشتی یکی باشند نیاز به هیچ انتقالی نیست. در غیر این صورت یک یال با دسته‌های هم‌نهشتی M و N [در دو سر آن] وجود دارد که $۱\le N<M\le ۲۰۰۵$. با اجرای یک سوپر انتقال می‌توان M را با $M-N$ جایگزین کرد که چون $۱\le M-N\le ۲۰۰۵$، آن خود یک دسته هم‌نهشتی است. از آنجا که $N\ge ۱$، با این کار مجموع دسته‌های هم‌نهشتی حداقل یک واحد کاهش می‌یابد. چون جمع همه‌ی دسته‌های هم‌نهشتی حداقل ۸ است با تکرار این فرآیند سرانجام به حالتی خواهیم رسید که در آن همه‌ی دسته‌های هم‌نهشتی یکی خواهند بود.

توجه کنید که اگر اعداد را با هم‌نهشتشان در دسته‌های هم‌نهشتی $۲۰۰۴,\ldots,۱,۰$ عوض می‌کردیم این اثبات مؤثر نخواهد بود. چرا که در حالت $N=۰$ مجموع دسته‌های هم‌نهشتی کاهش نمی‌یابد.

پاسخ دوم: همه‌ی اعداد صحیح را به پیمانه ۲۰۰۵ نگاه کنید. اجرای یک سوپر انتقال روی یک یال (در پیمانه ۲۰۰۵) معادله یک مرحله از الگوریتم اقلیدس روی دو عدد آن یال است. با اجرای الگوریتم اقلیدس روی یک زوج عدد صحیح مثبت، بعد از چند مرحله آن‌ها برابر بزرگ‌ترین مقسوم‌علیه مشترکشان خواهند شد. بنابراین می‌توان دو عدد هر یال را بعد ازچند بار سوپر انتقال در پیمانه ۲۰۰۵ هم‌نهشت ساخت. در ابتدا این کار را روی همه‌ی یال‌ها در یک جهت انجام می‌دهیم سپس روی همه‌ی یال‌ها در جهت دیگر و در نهایت روی همه‌ی یال‌ها در جهت سوم. بعد از آن همه‌ی اعداد نوشته شده در کنج‌ها به پیمانه ۲۰۰۵ هم‌نهشت خواهند شد.

قضیه کوچک فرما و قضیه اویلر

از چند نتیجه اخیر متوجه می‌شویم که برای یک عدد صحیح مثبت m، بررسی دسته‌های هم‌نهشتی که نسبت به m اول می‌باشند، مفید خواهد بود. برای هر عدد صحیح مثبت m، تعداد همه‌ی عددهای صحیح مثبت n کوچک‌تر از m را که نسبت به m اول می‌باشند با $\varphi(m)$ نشان می‌دهیم. تابع φ، تابع اویلر نامیده می‌شود. واضح است که $\varphi(۱)=۱$ و برای هر عدد اول p، $\varphi(p)=p-۱$ بعلاوه اگر n یک عدد صحیح مثبت باشد به طوری که $\varphi(n)=n-۱$ آنگاه n یک عدد اول است.

مجموعه‌ی S از اعداد صحیح، یک دستگاه مخفف مانده‌ها به پیمانه m نامیده می‌شود اگر برای هر i با شرایط $۰\le i\le m-۱$ و $\gcd(i,m)=۱$ دقیقاً یک عضو در S وجود داشته باشد (مانند s) به طوری که (پیمانه m) $i\equiv s$. واضح است که دستگاه مخفف مانده‌ها به پیمانه m، $\varphi(m)$ عضو دارد.

قضیه ۱. ۲۷. فرض کنید m یک عدد صحیح مثبت بوده و a یک عدد صحیح نسبت به m، اول باشد. S را یک دستگاه مخفف مانده‌ها به پیمانه m در نظر می‌گیریم. مجموعه‌ی

$$T = aS = \{as \mid s \in S\}$$

نیز یک دستگاه مخفف مانده‌ها به پیمانه m است.

اثبات مشابه اثبات قضیه ۱. ۲۴ است و آن را به عهده خواننده می‌گذاریم. قضیه ۱. ۲۷ به ما اجازه می‌دهد تا دو قضیه مشهور در تئوری اعداد را مطرح کنیم.

قضیه ۱. ۲۸. [قضیه اویلر] فرض کنید a و m اعداد صحیح مثبت و نسبت به هم اول باشند آنگاه

$$a^{\varphi(m)} = ۱ \quad (\text{پیمانه } m).$$

اثبات: مجموعه‌ی $S = \{a_۱, a_۲, \ldots, a_{\varphi(m)}\}$ شامل همه‌ی اعداد صحیح مثبت کوچک‌تر از m که نسبت به m اول هستند را در نظر بگیرید. چون $\gcd(a,m) = ۱$ است بنا بر قضیه ۱. ۲۷

$$\{aa_۱, aa_۲, \ldots, aa_{\varphi(m)}\}$$

یک دستگاه مخفف مانده‌های دیگر به پیمانه m می‌باشد. بنابراین

$$(aa_۱)(aa_۲)\cdots(aa_{\varphi(m)}) \equiv a_۱a_۲\ldots a_{\varphi(m)} \quad (\text{پیمانه } m)$$

با در نظر گرفتن $\gcd(a_k, m) = ۱$ برای $k = ۱, \ldots, \varphi(m)$ حکم اثبات می‌شود.

اگر $m = p$ یک عدد اول باشد قضیه اولر به قضیه کوچک فرما تبدیل می‌شود.

قضیه ۱. ۲۹. [قضیه کوچک فرما] اگر a یک عدد صحیح مثبت و p یک عدد اول باشد آنگاه:

$$a^p \equiv a \quad (\text{پیمانه } p)$$

اثبات: در این جا اثباتی مستقل از قضیه اویلر ارائه می‌شود. از استقرا روی a استفاده می‌کنیم. برای $a = ۱$ همه چیز واضح است. فرض کنید $p \mid (a^p - a)$ آنگاه

$$(a+۱)^p - (a+۱) = (a^p - a) + \sum_{k=۱}^{p-۱} \binom{p}{k} a^k$$

با استفاده از این حقیقت که برای $۱ \le k \le p-۱$، $p \mid \binom{p}{k}$ (نتیجه ۱. ۱۰) و با توجه به فرض استقرا، $p \mid (a+۱)^p - (a+۱)$ را می‌شمارد یعنی $(a+۱)^p \equiv (a+۱) \quad (\text{پیمانه } p)$

واضح است که قضیه کوچک فرما حالت خاصی از قضیه اویلر است. اما با توجه به چند خاصیت تابع φ اویلر می‌توان قضیه اویلر را نیز از روی قضیه کوچک فرما به دست آورد. به شکل دیگری از قضیه کوچک فرما توجه کنید:

اگر a یک عدد صحیح مثبت باشد که نسبت به عدد اول p، اول است. آنگاه (پیمانه p)

$$a^{p-1} \equiv 1$$

در ادامه چند مثال با استفاده از این دو قضیه مهم حل می‌کنیم.

مثال ۱. ۲۹. فرض کنید p یک عدد اول باشد. ثابت کنید برای همه‌ی عددهای صحیح a و b، p عدد $ab^p - ba^p$ را می‌شمارد.

اثبات: داریم $ab^p - ba^p = ab(b^{p-1} - a^{p-1})$.

اگر $p \mid ab$ آنگاه $p \mid ab^p - ba^p$؛ اگر $p \nmid ab$ آنگاه $\gcd(a,p) = \gcd(b,p) = 1$ و با استفاده از قضیه کوچک فرما (پیمانه p) $b^{p-1} \equiv a^{p-1} \equiv 1$ بنابراین $p \mid b^{p-1} - a^{p-1}$ و از آنجا $p \mid ab^p - ba^p$. بنابراین برای همه‌ی p ها $p \mid ab^p - ba^p$.

مثال ۱. ۳۰. فرض کنید $p \geq 7$ یک عدد اول باشد. ثابت کنید عدد $\underbrace{11\ldots1}_{p-1}$ بر p بخش‌پذیر است.

اثبات: می‌دانیم $\frac{10^{p-1} - 1}{9} = \underbrace{11\ldots1}_{p-1}$ و نتیجه با استفاده از قضیه کوچک فرما به راحتی به دست می‌آید. (توجه کنید که $\gcd(10,p) = 1$)

مثال ۱. ۳۱. فرض کنید p یک عدد اول بزرگ‌تر از ۵ باشد. ثابت کنید (پیمانه ۲۴۰)

$$p^8 \equiv 1$$

اثبات: $240 = 2^4 \times 3 \times 5$ با استفاده از قضیه کوچک فرما داریم (پیمانه ۳) $p^2 \equiv 1$ و (پیمانه ۵) $p^4 \equiv 1$. از آن جا که یک عدد صحیح مثبت نسبت به 2^4 اول است اگر و فقط اگر آن عدد فرد باشد، لذا $\varphi(2^4) = 2^3$. با استفاده از قضیه اویلر داریم (پیمانه ۱۶) $p^8 \equiv 1$. بنابراین برای $m = 3,5,16$، (پیمانه m) $p^8 \equiv 1$ و لذا (پیمانه ۲۴۰) $p^8 \equiv 1$.

این راه‌حل نشان می‌هد که می‌توان قضیه اویلر را با قضیه کوچک فرما به دست آورد. در ضمن به سادگی می‌توان بررسی کرد که برای (پیمانه ۱۶) $n \equiv \pm 1, \pm 3, \pm 5, \pm 7$، خواهیم داشت (پیمانه ۱۶) $n^4 \equiv 1$ (مثال ۱. ۲۴ (۵) را ببینید). بنابراین می‌توان نتیجه فوق را به صورت (پیمانه ۲۴۰) $p^4 \equiv 1$ برای همه‌ی اعداد اول $p > 5$ اصلاح کرد.

مثال ۱. ۳۲. ثابت کنید برای هر عدد صحیح مثبت زوج n، $n^2 - 1$ عدد $2^{n!} - 1$ را می‌شمارد.

اثبات: قرار می‌دهیم $m = n + 1$. باید ثابت کنیم $m(m-2), 2^{(m-1)!} - 1$ را می‌شمارد. چون $(m-1)!, \varphi(m)$ را می‌شمارد داریم $2^{(m-1)!} - 1 \mid 2^{\varphi(m)} - 1$ و از قضیه اویلر $m \mid 2^{\varphi(m)} - 1$. بنابراین $m \mid 2^{(m-1)!} - 1$ و به طور مشابه $m-2 \mid 2^{(m-1)!} - 1$. با توجه به اینکه m فرد بوده و $\gcd(m, m-2) = 1$، حکم اثبات می‌شود.

برای هر عدد صحیح مثبت m، فرض کنید $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ یک دستگاه مخفف مانده‌ها به پیمانه m باشد با توجه به وجود و یکتایی معکوس، به سادگی می‌توان دید مجموعه‌ی معکوس‌ها که به صورت

$$\{a_1^{-1}, a_2^{-1}, \ldots, a_{\varphi(m)}^{-1}\} \text{ یا } \{\frac{1}{a_1}, \frac{1}{a_2}, \ldots, \frac{1}{a_{\varphi(m)}}\}$$

نشان داده می‌شود نیز یک دستگاه مخفف مانده‌ها به پیمانه m است. ممکن است کسی بخواهد قضیه ویلسون را با مزدوج کردن دسته‌های هم‌نهشتی که معکوس یکدیگر هستند، تعمیم دهد. اما این کار جواب نمی‌دهد زیرا بجز ۱ و ۱- (یا $m-1$) دسته‌های هم‌نهشتی دیگری وجود دارد که معکوسشان خودشان هستند (در اثبات قضیه ویلسون فقط دو مقدار ممکن برای s وجود داشت به طوری که (پیمانه‌ی p) $s^2 \equiv 1$ و آن $s = 1$ یا $s = p - 1$ است) برای مثال برای $m = 35$، (پیمانه ۳۵) $x^2 \equiv 1$.

فرض کنید m یک عدد صحیح مثبت باشد و a یک عدد صحیح که نسبت به m اول است. $na = b$ را یک مضرب a در نظر می‌گیریم یعنی $n = \frac{b}{a}$ یک عدد صحیح است. از (پیمانه m) $a^{-1}a \equiv 1$ نتیجه می‌گیریم (پیمانه m) $n \equiv a^{-1}an \equiv a^{-1}b$. این بدان معناست که تعریف طبیعی n به صورت $n = \frac{b}{a}$ منجر به برقراری رابطه (پیمانه m) $n \equiv \frac{1}{a}.b$ می‌شود. این امر به ما اجازه می‌دهد تا مرتبه عملیات را بسته به میزان مفید بودن آن انتخاب کنیم.

مثال ۱. ۳۳. [IMO ۲۰۰۵] دنباله‌ی $a_1, a_2, \ldots$ را در نظر بگیرید که به صورت

$a_n = 2^n + 3^n + 6^n - 1$ (برای همه‌ی اعداد صحیح n)

تعریف می‌شود. همه‌ی اعداد صحیح مثبتی را پیدا کنید که نسبت به هر عضو این دنباله اول هستند.

پاسخ اول: جواب ۱ است. کافی است نشان دهیم که هر عدد اول p برای برخی از nها، عدد a_n را می‌شمارد. $p = 2$ و $p = 3$ هر دو عدد $a_2 = 2^2 + 3^2 + 6^2 - 1 = 48$ را می‌شمارند.

عدد اول $p \geq 5$ را در نظر بگیرید. با استفاده از قضیه کوچک فرما (پیمانه p) $2^{p-1} \equiv 3^{p-1} \equiv 6^{p-1} \equiv 1$. لذا

$$3 \times 2^{p-1} + 2 \times 3^{p-1} + 6^{p-1} \equiv 3 + 2 + 1 \equiv 6 \quad (\text{پیمانه } p)$$

یا (پیمانه p) $6(2^{p-2} + 3^{p-2} + 6^{p-2} - 1) \equiv 0$ یعنی $6a_{p-2}$ بر p بخش‌پذیر است. چون p نسبت به ۶ اول است، a_{p-2} بر p بخش‌پذیر می‌باشد که همان حکم موردنظر ماست.

پاسخ دوم: اگر از مفهوم معکوس استفاده کنیم اثبات را می‌توان به صورت زیر نوشت: برای هر عدد اول p بزرگ‌تر از ۵

$$6a_{p-2} \equiv 6(2^{p-2} + 3^{p-2} + 6^{p-2} - 1)$$

$$\equiv 6\left(\frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1\right) \equiv 0 \quad (\text{پیمانه } p)$$

مثال ۱. ۳۴. یک تصاعد حسابی غیر ثابت نامتناهی از اعداد صحیح مثبت پیدا کنید که هر عضو، جمع دو عدد مکعب کامل نباشد.

پاسخ: فرض کنید تصاعد حسابی مطلوب به صورت $\{a, a+d, a+2d, \ldots\}$ باشد. ما در واقع همه‌ی اعداد صحیح دسته هم‌نهشتی a به پیمانه d را بررسی می‌کنیم. می‌خواهیم به دسته‌های هم‌نهشتی که به پیمانه d، مکعب هستند محدود شویم و از این طریق دسته‌های هم‌نهشتی که به پیمانه d مجموع دو مکعب هستند شناسایی کنیم [در واقع تعیین کنیم جمع دو عدد مکعب کامل درچه دسته‌های هم‌نهشتی به پیمانه d می‌تواند قرار گیرد].

در ابتدا دنبال یک d می‌گردیم به طوری که برای همه‌ی اعداد صحیح a، (پیمانه d) $a^3 \equiv 1$ باشد. با استفاده از قضیه کوچک فرما اگر قرار دهیم $p - 1 = 3$, $p = 4$ به دست می‌آید که اول نیست. لذا نمی‌توان قضیه کوچک فرما را به طور مستقیم اعمال کرد. از طرف دیگر اگر $p = 7$ باشد، برای همه‌ی اعداد نسبت به ۷ اول، (پیمانه ۷) $a^6 \equiv 1$. به سادگی می‌توان دید دسته‌های هم‌نهشتی برای a^3 به پیمانه ۷ عبارت از $0, 1, -1$ (۶) هستند. بنابراین دسته‌های مانده برای $a^3 + b^3$ به پیمانه ۷ عبارتند از $0, 1, -1, 2, 2, -2$. به این ترتیب دو دنباله $\{3, 3+7, 3+2\times7, \ldots\}$ و $\{4, 4+7, 4+2\times7, \ldots\}$ در شرایط مسأله صدق می‌کنند.

مثال ۱. ۳۵. [IMO ۲۰۰۳ پیشنهادی] کوچک‌ترین عدد صحیح مثبت k را چنان پیدا کنید که اعداد $x_1, x_2, \ldots, x_k$ وجود داشته باشند که $x_1^3 + x_2^3 + \cdots + x_k^3 = 2002^{2002}$

پاسخ: جواب $k = 4$ است.

ابتدا نشان می‌دهیم که 2002^{2002} جمع سه مکعب کامل نیست. برای محدود کردن تعداد مکعب‌ها به پیمانه n تمایل داریم که $\varphi(n)$ مضرب ۳ باشد. دوباره $n = 7$ را بررسی می‌کنیم. اما جمع سه مکعب کامل به پیمانه ۷ به دسته‌های هم‌نهشتی زیادی می‌تواند تعلق داشته باشد (چون ۷ خیلی کوچک است). حال $n = 9$ را بررسی می‌کنیم که $\varphi(9) = 6$ است. چون (پیمانه ۹) $2002 \equiv 4$ و (پیمانه ۹) $4^3 \equiv 1 \equiv 2002^3$ لذا:

$$2002^{2002} = (2002^3)^{667} \times 2002 \equiv 4 \quad (\text{پیمانه } 9)$$

از طرف دیگر برای اعداد صحیح x، (پیمانه ۹) $x^3 \equiv 0, \pm 1$. مشاهده می‌شود که (پیمانه ۹) $x_1^3 + x_2^3 + x_3^3 \not\equiv 4$ حال این باقی می‌ماند که نشان دهیم 2002^{2002} جمع چهار مکعب کامل است. با رابطه‌ی $2002 = 1^3 + 1^3 + 1^3 + 10^3$ شروع کرده و با استفاده مجدد از $2002 = 667 \times 3 + 1$ به روابط زیر می‌رسیم:

$$2002^{2002} = 2002 \times (2002^{667})^3$$
$$= (10 \times 2002^{667})^3 + (10 \times 2002^{667})^3 + (2002^{667})^3 =$$

قضیه کوچک فرما شرط خوبی برای تعیین مرکب بودن یک عدد فراهم می‌کند. اما برعکس آن صحیح نیست به طور مثال $3 \times 11 \times 17$ عدد $a^{3 \times 11 \times 17} - a$ را می‌شمارد زیرا ۳، ۱۱ و ۱۷ هر سه این عدد را می‌شمارند (مثلاً اگر ۱۱، a را نشمارد آنگاه از قضیه کوچک فرما $11 | a^{10} - 1$. بنابراین $11 | a^{10 \times 56} - 1$ و به تبع آن $11 | a^{561} - a$ که $561 = 3 \times 11 \times 17$). اعداد صحیح مرکب n که برای هر عدد صحیح a رابطه‌ی $a^n \equiv a \pmod n$ را برآورده سازند. اعداد کارمایکل نامیده می‌شوند. اعداد زوج کارمایکل نیز وجود دارد مانند $n = 2 \times 73 \times 1103$.

فرض کنید a و m دو عدد صحیح مثبت و نسبت به هم اول باشند. با قرار دادن $b = 1$ در نتیجه ۱. ۲۳ به یک نتیجه جالب می‌رسیم. از قضیه اویلر اعداد صحیح مثبت x وجود دارند که (پیمانه m) $a^x \equiv 1$. می‌گوییم a به پیمانه m از مرتبه‌ی d است و آن را به صورت $\mathrm{ord}_m(a) = d$ نشان می‌دهیم اگر d کوچک‌ترین عدد صحیح مثبت باشد که (پیمانه m) $a^d \equiv 1$. با توجه به قضیه اویلر، $\mathrm{ord}_m(a) = d \le \varphi(m)$. اگر x یک عدد صحیح مثبت باشد که (پیمانه m) $a^x \equiv 1$ از نتیجه ۱. ۲۳ خواهیم داشت:

$$a^{\gcd(x,d)} \equiv ۱ \ (\text{پیمانه } m)$$

از آن جا که $\gcd(x,d) \le d$ است این نتیجه با کمینه بودن d تناقض دارد مگر آن که $\gcd(x,d) = d$ یعنی $x,\ d$ را بشمارد. به این ترتیب می‌توان قضیه زیر را بیان کرد.

قضیه ۱. ۳۰. عدد صحیح مثبت x در رابطه‌ی $a^x \equiv ۱ \ (\text{پیمانه } m)$ صدق می‌کند اگر و فقط اگر x مضربی از مرتبه a به پیمانه d باشد.

برای یک زوج از اعداد صحیح مثبت نسبت به هم اول a و m، همیشه عدد صحیح مثبت s وجود ندارد که به ازای آن رابطه $a^s \equiv -۱ \ (\text{پیمانه } m)$ برقرار باشد (به طور مثال $a = ۲$ و $m = ۷$). فرض کنید توان کاملی از a وجود دارد که به پیمانه m با ۱- هم‌نهشت است و فرض کنید s کوچک‌ترین عدد صحیح با این خاصیت باشد. بنابراین خواهیم داشت $\text{ord}_m(a) = ۲s$. در واقع $a^{۲s} \equiv ۱ \ (\text{پیمانه } m)$ و لذا $۲s,\ d$ را می‌شمارد. اگر $d < ۲s$ باشد آنگاه $a^{۲s-d} \equiv -۱ \ (\text{پیمانه } m)$ و فرض حداقل بودن s را رد می‌کند. علاوه بر این اگر t یک عدد صحیح باشد به طوری که $a^t \equiv -۱ \ (\text{پیمانه } m)$ آنگاه t مضربی از s است. زیرا $a^{۲t} \equiv ۱ \ (\text{پیمانه } m)$ بوده و در نتیجه $d = ۲s,\ ۲t$ را می‌شمارد یعنی $t,\ s$ را می‌شمارد. واضح است که t باید مضرب فردی از s باشد. به عبارت دیگر:

$$a^t \equiv \begin{cases} -۱ & \text{اگر } t \text{ مضرب فردی از } s \text{ باشد.} \\ ۱ & \text{اگر } t \text{ مضرب زوجی از } s \text{ باشد.} \end{cases}$$

مثال ۱. ۳۶. [$AIME$ ۲۰۰۱] چند عدد صحیح مثبت از مضارب ۱۰۰۱ وجود دارد که بتوان آن را به شکل $۱۰^j - ۱۰^i$ بیان کرد که i و j اعداد صحیح بوده و $۰ \le i < j \le ۹۹$.

پاسخ: چون $۱۰^j - ۱۰^i = ۱۰^i \times (۱۰^{j-i} - ۱)$ و $۱۰۰۱ = ۱۳ \times ۱۱ \times ۷$ نسبت به ۱۰^i اول است، لذا لازم است که i و j را طوری پیدا کنیم که $۱۰^{j-i} - ۱$ بر اعداد اول ۷، ۱۱ و ۱۳ بخش‌پذیر باشد. با توجه به این که (پیمانه ۱۰۰۱) $۱۰^۳ \equiv -۱$ به سادگی می‌توان بررسی کرد که $\text{ord}_{۱۰۰۱}(۱۰) = ۶$.

بنا بر قضیه ۱. ۳۰ $۱۰^i \times (۱۰^{j-i} - ۱)$ بر ۱۰۰۱ بخش‌پذیر است اگر و فقط اگر $j - i = ۶n$ باشد (n عددی صحیح است) بنابراین لازم است تا تعداد جواب‌های صحیح $j = i + ۶n$ با شرایط $i \ge ۰,\ n > ۰$ و $j \le ۹۹$ را بشماریم. برای هر مقدار $n = ۱,۲,\ldots,۱۶$، $۱۰۰ - ۶n$ مقدار مناسب برای i (و در نتیجه برای j) وجود دارد بنابراین پاسخ مسأله برابر است با:

$$۹۴ + ۸۸ + ۸۲ + \ldots + ۴ = ۷۸۴$$

تابع φ اویلر

می‌خواهیم روی برخی از خواص مفید تابع φ اویلر بحث کنیم. اول از همه به سادگی می‌توان قضیه زیر را نوشت:

قضیه ۱. ۳۱. اگر p یک عدد اول و a یک عدد صحیح مثبت باشند آنگاه $\varphi(p^a)=p^a-p^{a-1}$

در قضیه بعد نشان می‌دهیم که φ ضربی است.

قضیه ۱. ۳۲. اگر a و b دو عدد صحیح مثبت و نسبت به هم اول باشند آنگاه $\varphi(ab)=\varphi(a)\varphi(b)$

اثبات: اعداد صحیح $ab,\dots,2,1$ را در یک آرایه (ماتریس) $b\times a$ به صورت زیر می‌نویسیم:

$$\begin{array}{cccc} 1 & 2 & \cdots & a \\ a+1 & a+2 & \cdots & 2a \\ \vdots & \vdots & \vdots & \vdots \\ a(b-1)+1 & a(b-1)+2 & \cdots & ab \end{array}$$

واضح است که $\varphi(ab)$ عدد در جدول بالا وجود دارد که نسبت به ab اول هستند.
از طرف دیگر $\varphi(a)$ ستون، عناصری را در بر دارند که نسبت به a اول هستند. هر یک از آن ستون‌ها یک دستگاه کامل مانده به پیمانه b هستند (از قضیه ۱. ۲۴) بنابراین دقیقاً $\varphi(b)$ عنصر در هر یک از آن ستون‌ها نسبت به b اول است. لذا در کل $\varphi(a)\varphi(b)$ عدد در جدول نسبت به ab اول هستند و رابطه‌ی $\varphi(ab)=\varphi(a)\varphi(b)$ برای اعداد صحیح نسبت به هم اول a و b برقرار است.

قضیه ۱. ۳۳. اگر $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}$. تجزیه $n>1$ به عوامل اول باشد آنگاه:

$$\varphi(n)=n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k})$$

اثبات اول: به طور مستقیم از قضایای ۱. ۳۱ و ۱. ۳۲ به دست می‌آید.

اثبات دوم: از اصل شمول و عدم شمول استفاده می‌کنیم. مجموعه‌های زیر را در نظر بگیرید

$$T_i = \{d : d \le n, p_i \mid d\} \qquad i = 1,\dots,k$$

بنابراین

$$T_1 \cup \dots \cup T_k = \{m : m \le n, \gcd(m,n) > 1\}$$

پس

$$\begin{aligned}\varphi(n) &= n - |T_1 \cup \dots \cup T_k| \\ &= n - \sum_{i=1}^{k} |T_i| + \sum_{1 \le i < j \le k} |T_i \cap T_j| - \dots + (-1)^k |T_1 \cap \dots \cap T_k|\end{aligned}$$

داریم:

$$|T_i| = \frac{n}{p_i},\ |T_i \cap T_j| = \frac{n}{p_i p_j}, \dots, |T_1 \cap \dots \cap T_k| = \frac{n}{p_1 \cdots p_k}$$

و لذا

$$\begin{aligned}\varphi(n) &= n\left(1 - \sum_{i=1}^{n} \frac{1}{p_i} + \sum_{1 \le i < j \le k} \frac{1}{p_i p_j} - \dots + (-1)^k \frac{1}{p_1 \cdots p_k}\right) \\ &= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)\end{aligned}$$

بر مبنای قضیه ۱. ۳۳ می‌توانیم قضیه اویلر را از روی قضیه کوچک فرما به دست آوریم. فرض کنید: $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ تجزیه n به عوامل اول باشد. می‌دانیم (پیمانه p_i) $a^{p_i - 1} \equiv 1$ بنابراین (پیمانه p_i^2) $a^{p_i(p_i-1)} \equiv 1$، (پیمانه p_i^3) $a^{p_i^2(p_i-1)}, \dots$ و (پیمانه $p_i^{\alpha_i}$) $a^{p_i^{\alpha_i - 1}(p_i-1)} \equiv 1$.

به عبارت دیگر برای $i = 1,\dots,k$ (پیمانه $p_i^{\alpha_i}$) $a^{\varphi(p_i^{\alpha_i})} \equiv 1$. با اعمال این خاصیت به هر عامل اول، نتیجه مطلوب به دست می‌آید.

قضیه ۱. ۳۴. [گاوس] برای هر عدد صحیح مثبت n

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

اثبات: n عدد گویای $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$ را در نظر بگیرید.

با ساده کردن هر عدد از اعداد فوق، به اعداد جدیدی می‌رسیم که در آن هر کسر به صورت نسبت دو عدد صحیح نسبت به هم اول می‌باشد. مخرج کسرها در اعداد جدید

همگی مقسوم‌علیه‌های n هستند. اگر $d \mid n$ دقیقاً مخرج $\varphi(d)$ کسر از این اعداد، برابر d خواهد بود. بنابراین در مجموع $\sum_{d \mid n} \varphi(d)$ کسر وجود دارد. چون تعداد اعضا در ابتدا n کسر بوده و عضوی هم از آن کم یا زیاد نشده است، حکم ثابت می‌شود.

مثال ۱. ۳۱. فرض کنید n یک عدد صحیح مثبت باشد.

(۱) مجموع همه‌ی اعداد صحیح مثبت کوچک‌تر از n و نسبت به n اول را پیدا کنید.

(۲) مجموع همه‌ی اعداد صحیح مثبت کوچک‌تر از $۲n$ و نسبت به n اول را پیدا کنید.

پاسخ: جواب به ترتیب $\frac{n\varphi(n)}{۲}$ و $۲n\varphi(n)$ می‌باشد.

فرض کنید

$$S_۱ = \sum_{\substack{d<n \\ \gcd(d,n)=۱}} d \quad \text{و} \quad S_۲ = \sum_{\substack{d<۲n \\ \gcd(d,n)=۱}} d$$

و $d_۱ < d_۲ < \cdots < d_{\varphi(n)}$ اعداد کوچک‌تر از n و نسبت به n اول باشند. می‌دانیم $\gcd(d,n)=۱$ اگر و فقط اگر $\gcd(n-d,n)=۱$. نتیجه می‌گیریم که

$$d_۱ + d_{\varphi(n)} = n \ , \ d_۲ + d_{\varphi(n)-۱} = n \ , \ \ldots \ , d_{\varphi(n)} + d_۱ = n$$

لذا

$$S_۱ = \frac{n\varphi(n)}{۲}$$

از طرف دیگر

$$\sum_{\substack{n<d<۲n \\ \gcd(n,d)=۱}} d = \sum_{\substack{d<n \\ \gcd(n,d)=۱}} (n+d) = n\varphi(n) + \sum_{\substack{d<n \\ \gcd(n,d)=۱}} d = n\varphi(n) + \frac{n\varphi(n)}{۲} = \frac{۳n\varphi(n)}{۲}$$

بنابراین

$$S_۲ = \frac{n\varphi(n)}{۲} + \frac{۳n\varphi(n)}{۲} = ۲n\varphi(n)$$

تابع ضربی

این بخش به دلیل بررسی بیشتر نتایج مربوط به سه تابعی که قبلاً معرفی شدند، آورده شده است ($\tau(n)$ تعداد مقسوم‌علیه‌های مثبت n، $\sigma(n)$ مجموع مقسوم‌علیه‌های مثبت n، $\varphi(n)$ تابع φ اولر) این بخش خلاصه‌ترین بخش کتاب است و مطالبی که در آن مطرح می‌شود برای ادامه کتاب ضروری نیستند. اما بهر حال برای مطالعه‌ی بیشتر در تئوری اعداد مفید می‌باشد.

توابع حسابی روی مجموعه‌ی اعداد صحیح مثبت تعریف می‌شوند و دارای مقداری مختلط هستند. تابع حسابی $f \neq 0$ ضربی نامیده می‌شود اگر برای هر دو عدد صحیح مثبت و نسبت به هم اول m و n رابطه زیر برقرار باشد

$$f(mn)=f(m)f(n)$$

اگر f ضربی باشد، $f(1)=1$ است. چرا که اگر a یک عدد صحیح مثبت باشد و $f(a)\neq 0$ آنگاه از $f(a\times 1)=f(a)f(1)$ نتیجه می‌شود $f(1)=1$ است. اگر f ضربی باشد و $n=p_1^{\alpha_1}...p_k^{\alpha_k}$ تجزیه عدد صحیح مثبت n به عوامل اول باشد آنگاه $f(n)=f(p_1^{\alpha_1})...f(p_k^{\alpha_k})$.

یک تابع حسابی مهم موبیوس است که به صورت زیر تعریف می‌شود:

$$\mu(n)=\begin{cases}1 & n=1\\ 0 & p^2 \mid n \text{ عدد اول } p>1 \text{ وجود دارد که}\\ (-1)^k & n=p_1...p_k \text{ اعداد اول متمایز هستند. } p_1,...,p_n\end{cases}$$

برای مثال $\mu(2)=-1$، $\mu(6)=1$ و $\mu(12)=\mu(2^2\times 3)=0$

قضیه ۱. ۳۵. تابع موبیوس یک تابع ضربی است.

اثبات: m و n دو عدد صحیح مثبت هستند به طوری که $\gcd(m,n)=1$. اگر عدد اول $p>1$ وجود داشته باشد که $p^2 \mid m$ آنگاه $p^2 \mid mn$ و $\mu(m)=\mu(mn)=0$ خواهد بود. حال حالتی که $m=p_1...p_k$، $n=q_1...q_h$ و $p_1,...,p_k,q_1,...,q_h$ اعداد اول متمایز هستند را بررسی می‌کنیم. در این صورت $\mu(m)=(-1)^k$، $\mu(n)=(-1)^h$ و $mn=p_1...p_kq_1...q_h$. در نتیجه $\mu(mn)=(-1)^{k+h}=(-1)^k.(-1)^h=\mu(m)\mu(n)$

برای تابع حسابی f تابع مجموع F را به صورت زیر تعریف می‌کنیم:

$$F(n)=\sum_{d\mid n} f(d)$$

توابع f و F طبق قضیه زیر با هم رابطه دارند.

قضیه ۱. ۳۶. اگر تابع f ضربی باشد، تابع مجموع F نیز ضربی است.

اثبات: فرض کنید m و n اعداد صحیح مثبت و نسبت به هم اول باشند و فرض کنید d یک مقسوم‌علیه mn باشد. d را می‌توان به صورت یکتای $d=kh$ نشان داد که $k\mid m$ و $h\mid n$. از آن جا که $\gcd(m,n)=1$ داریم $\gcd(k,h)=1$ بنابراین $f(kh)=f(k)f(h)$. به این ترتیب

$$F(mn)=\sum_{d\mid mn} f(d)=\sum_{\substack{k\mid m\\ h\mid n}} f(k)f(h)$$
$$=(\sum_{k\mid m} f(k))(\sum_{h\mid n} f(h))=F(m)F(n)$$

توجه کنید که اگر f یک تابع ضربی باشد و $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ آنگاه:

$$\sum_{d\mid n}\mu(d)f(d)=(1-f(p_1))\cdots(1-f(p_k))$$

برای اثبات می‌دانیم تابع $g(n)=\mu(n)f(n)$ ضربی است لذا طبق قضیه ۱. ۳۶ تابع مجموع G آن نیز ضربی است، بنابراین $G(n)=G(p_1^{\alpha_1})\cdots G(p_k^{\alpha_k})$ و

$$G(p_i^{\alpha_i})=\sum_{d\mid p_i^{\alpha_i}}\mu(d)f(d)=\mu(1)f(1)+\mu(p_i)f(p_i)=1-f(p_i)$$

که از آن نتیجه موردنظر به دست می‌آید.

قضیه ۱. ۳۷. [فرمول معکوس موبیوس] اگر f یک تابع حسابی و F تابع مجموع آن باشد. آنگاه:

$$f(n)=\sum_{d\mid n}\mu(d)F(\frac{n}{d})$$

اثبات: از آنجا که برای $\frac{n}{c}>1$، $\sum_{d\mid \frac{n}{c}}\mu(d)=0$ لذا

$$\sum_{d\mid n}\mu(d)F(\frac{n}{d})=\sum_{d\mid n}\mu(d)(\sum_{c\mid \frac{n}{d}} f(c))=\sum_{d\mid n}(\sum_{c\mid \frac{n}{d}}\mu(d)f(c))$$
$$=\sum_{c\mid n}(\sum_{d\mid \frac{n}{c}}\mu(d)f(c))=\sum_{c\mid n} f(c)(\sum_{d\mid \frac{n}{c}}\mu(d))=f(n)$$

در روابط فوق از این حقیقت استفاده کردیم که

$$\left\{(d,c)\,|\,d\,|\,n,c\,|\,\frac{n}{d}\right\}=\left\{(d,c)\,|\,c\,|\,n,d\,|\,\frac{n}{c}\right\}$$

قضیه ۱. ۳۸. فرض کنید f یک تابع حسابی بوده و F تابع مجموع آن باشد. اگر F ضربی باشد، f نیز ضربی است.

اثبات: فرض کنید m و n دو عدد صحیح مثبت و $\gcd(m,n)=1$ باشد. اگر d یک مقسوم‌علیه mn باشد $d=kh$ است در حالی که $k\,|\,m$، $h\,|\,n$ و $\gcd(k,h)=1$. با بکار بردن فرمول معکوس موبیوس:

$$f(mn)=\sum_{d|mn}\mu(d)F(\frac{mn}{d})=\sum_{\substack{k|m\\h|n}}\mu(kh)F(\frac{mn}{kh})$$

$$=\sum_{\substack{k|m\\h|n}}\mu(k)\mu(h)F(\frac{m}{k})F(\frac{n}{h})=(\sum_{k|m}\mu(k)F(\frac{m}{k}))(\sum_{h|n}\mu(h)F(\frac{n}{h}))=f(m)f(n)$$

توابع τ,σ و φ نیز ضربی هستند که اثبات را به خوانندگان می‌سپاریم. در ضمن پیشنهاد می‌کنیم با توجه به خواص کلی که ما در این بخش ارائه کردیم، خواص جدیدی برای این توابع به دست آورند.

معادلات دیوفانتین خطی

یک معادله به شکل

$$a_1x_1+\ldots+a_nx_n=b \qquad (*)$$

که در آن $a_1,a_2,\ldots,a_n$ و b اعداد صحیح ثابت هستند، یک معادله‌ی دیوفانتین خطی نامیده می‌شود. فرض می‌شود که $n\geq 1$ و ضرایب $a_1,\ldots,a_n$ همگی غیر صفر هستند.

مهم‌ترین نتیجه در مورد معادلات دیوفانتین، تعمیم قضیه ۱. ۷ (قضیه بزو) است که در ادامه بیان می‌شود.

قضیه ۱. ۳۹. معادله (*) جواب دارد [در مجموعه‌ی اعداد صحیح] اگر و فقط اگر

$$\gcd(a_1,\ldots,a_n)\,|\,b$$

در صورت جواب داشتن، همه‌ی اعداد صحیح جواب معادله‌ی (*) را می‌توان به صورت جمع $n-1$ پارامتر بیان کرد.

اثبات: فرض کنید $d = \gcd(a_1,...,a_n)$.

اگر b بر d بخش‌پذیر نباشد آنگاه (*) قابل حل نیست زیرا برای هر عدد صحیح $x_1,...,x_n$ سمت چپ بر d بخش‌پذیر است ولی سمت راست بر d بخش پذیر نیست.

اگر $d \mid b$ آنگاه معادله‌ی جدید به صورت زیر به دست می‌آید:

$$a'_1 x_1 + ... + a'_n x_n = b'$$

که $a'_i = \frac{a_i}{d}$ برای $i = 1,...,n$ و $b' = \frac{b}{d}$. واضح است که $\gcd(a'_1,...,a'_n) = 1$.

از استقرا روی n تعداد متغیرها استفاده می‌کنیم. در حالت $n = 1$ معادله به شکل $x_1 = b$ یا $-x_1 = b$ می‌باشد و بنابراین پاسخ یکتا به هیچ پارامتری بستگی ندارد.

حال فرض می‌کنیم $n \geq 2$ و خاصیت موردنظر برای همه‌ی معادلات خطی با $n-1$ متغیر برقرار باشد. قرار می‌دهیم $d_{n-1} = \gcd(a_1,...,a_{n-1})$. هر پاسخ $(x_1,...,x_n)$ در رابطه‌ی هم‌نهشتی زیر صدق می‌کند.

$$a_1 x_1 + a_2 x_2 + ... + a_n x_n \equiv b \pmod{d_{n-1}}$$

که معادل است با:

$$a_n x_n \equiv b \pmod{d_{n-1}} \qquad (\dagger)$$

دو طرف (†) را در $a_n^{\varphi(d_{n-1})-1}$ ضرب کرده و با توجه به $a_n^{\varphi(d_{n-1})} \equiv 1 \pmod{d_{n-1}}$ به رابطه‌ی زیر می‌رسیم

$$x_n \equiv c \pmod{d_{n-1}}$$

که $c = a_n^{\varphi(d_{n-1})-1} b$. بنابراین عدد صحیح t_{n-1} وجود دارد که $x_n = c + d_{n-1} t_{n-1}$. با قرار دادن این رابطه در (*) و مرتب کردن، معادله با $n-1$ متغیر به دست می‌آید:

$$a_1 x_1 + \cdots + a_{n-1} x_{n-1} = b - a_n c - a_n d_{n-1} t_{n-1}$$

حال فقط این باقی می‌ماند که نشان دهیم $d_{n-1} \mid (b - a_n c - a_n d_{n-1} t_{n-1})$ که معادل آن است که $a_n c \equiv b \pmod{d_{n-1}}$. رابطه‌ی اخیر با توجه به تعریف c صحیح است بنابراین می‌توان معادله‌ی آخر را بر d_{n-1} تقسیم کرد و به دست آورد:

$$a'_1 x_1 + \cdots + a'_{n-1} x_{n-1} = b' \qquad (\ddagger)$$

که $a'_i = \frac{a_i}{d_{n-1}}$ برای $i = 1,\dots,n-1$ و $b' = \frac{(b - a_n c)}{d_{n-1}} + a_n t_{n-1}$.

چون $\gcd(a'_1,\dots,a'_{n-1}) = 1$ از فرض استقرا نتیجه می‌گیریم که معادله (‡) برای هر عدد صحیح t_{n-1} قابل حل بوده و جواب آن را می‌توان به شکل مجموع $n-2$ پارامتر بیان کرد. با اضافه کردن $x_n = c + d_{n-1} t_{n-1}$ می‌توان جواب معادله‌ی (*) را به شکل مجموع $n-1$ پارامتر بیان کرد.

نتیجه ۱. ۴۰. فرض کنید a_1 و a_2 اعداد صحیح نسبت به هم اول باشند. اگر (x_1°, x_2°) یک جواب معادله $a_1 x_1 + a_2 x_2 = b$ باشد. آنگاه همه‌ی جواب‌های این معادله به صورت زیر هستند:

$$\begin{cases} x_1 = x_1^\circ + a_2 t \\ x_2 = x_2^\circ - a_1 t \end{cases} \qquad \text{برای هر عدد صحیح t}$$

مثال ۱. ۳۸. همه‌ی سه تایی‌های (x,y,z) از اعداد صحیح که در معادله‌ی $3x + 4y + 5z = 6$ صدق می‌کنند را تعیین کنید؟

پاسخ: داریم (پیمانه ۵) $3x + 4y \equiv 1$ بنابراین برای عدد صحیح s

$$3x + 4y = 1 + 5s$$

و یک جواب این معادله به صورت $x = -1 + 3s$ و $y = 1 - s$ است. با بکار بردن نتیجه ۱. ۴۰ به این نتیجه می‌رسیم که برای اعداد صحیح t, $x = -1 + 3s + 4t$ و $y = 1 - s - 3t$ و با قرار دادن این مقادیر در معادله‌ی اصلی $z = 1 - s$ به دست می‌آید. بنابراین همه‌ی جواب‌ها به صورت زیر هستند:

برای هر زوج از اعداد صحیح s و t

$$(x,y,z) = (-1 + 3s + 4t, 1 - s - 3t, 1 - s)$$

مثال ۱. ۳۹. فرض کنید n یک عدد صحیح مثبت باشد و ۶۶۶ سه تایی مرتب (x,y,z) از اعداد صحیح مثبت وجود دارد که در رابطه‌ی $x + 8y + 8z = n$ صدق می‌کنند. بیشترین مقدار n را پیدا کنید.

پاسخ: جواب ۳۰۳ است. می‌نویسیم $n = 8a + b$ که a و b اعداد صحیح بوده و $0 \le b < 8$. از (پیمانه ۸) $x \equiv n \equiv b$ مقادیر ممکن برای x عبارتند از $b, b+8, \dots, b+8(a-1)$. برای $x = b + 8i$ که $0 \le i \le a-1$ خواهیم داشت $8(y+z) = 8(a-i)$ یا $y + z = a - i$ که به موجب آن $a - i - 1$ زوج مرتب (y,z) از اعداد صحیح مثبت، پاسخ معادله بوده و عبارتند از: $(1, a-i-1), \dots, (a-i-1, 1)$. بنابراین به تعداد

$$\sum_{i=0}^{a-1}(a-i-1)=\sum_{i=0}^{a-1} i=\frac{a(a-1)}{2}$$

سه‌تایی مرتب وجود دارد که در شرایط مسأله صدق می‌کند. با حل $\frac{a(a-1)}{2}=666$، $a=37$ به دست می‌آید. بنابراین بیشترین مقدار n برابر $37\times 8+7=303$ می‌باشد که با قرار دادن $b=7$ به دست می‌آید.

دستگاه‌های عددی

نتیجه‌ی اساسی و اصلی این بخش با قضیه زیر بیان می‌شود:

قضیه ۱. ۴۱. فرض کنید b یک عدد صحیح بزرگ‌تر از ۱ باشد. برای هر عدد صحیح $n\geq 1$ دستگاه یکتای $(k,a_0,a_1,...,a_k)$ از اعداد صحیح وجود دارد به طوری که برای $i=0,1,...,k$، $0\leq a_i\leq b-1$، $a_k\neq 0$ و

$$(*)\quad n=a_k b^k+a_{k-1}b^{k-1}+...+a_1 b+a_0$$

اثبات: برای اثبات وجود، به طور مکرر الگوریتم تقسیم را به کار می‌بریم:

$$\begin{aligned} n&=q_1 b+r_1 && 0\leq r_1\leq b-1\\ q_1&=q_2 b+r_2 && 0\leq r_2\leq b-1\\ &\vdots\\ q_{k-1}&=q_k b+r_k && 0\leq r_k\leq b-1 \end{aligned}$$

که q_k آخرین خارج‌قسمت غیر صفر است. فرض کنید

$$q_0=n\ ,\ a_0=n-q_1 b\ ,\ a_1=q_1-q_2 b\ ,\ \ldots\ ,\ a_{k-1}=q_{k-1}-q_k b\ ,\ a_k=q_k$$

در این صورت

$$\sum_{i=0}^{k}a_i b^i=\sum_{i=0}^{k-1}(q_i-q_{i+1}b)b^i+q_k b^k=q_0+\sum_{i=1}^{k}q_i b^i-\sum_{i=1}^{k}q_i b^i=q_0=n$$

برای اثبات یکتایی فرض کنید $n=c_0+c_1 b+...+c_h b^h$ نمایش دیگری به شکل (*) باشد. اگر $h\neq k$ برای مثال $h>k$ آنگاه $n\geq b^h\geq b^{k+1}$. اما

$$n = a_0 + a_1 b + \ldots + a_k b^k \le (b-1)(1 + b + \ldots + b^k) = b^{k+1} - 1 < b^{k+1}$$

که تناقض است.

اگر $h = k$ آنگاه

$$a_0 + a_1 b + \ldots + a_k b^k = c_0 + c_1 b + \ldots + c_k b^k$$

و بنابراین $b \mid (a_0 - c_0)$. از طرف دیگر $|a_0 - c_0| < b$ بنابراین $a_0 = c_0$ و

$$a_1 + a_2 b + \ldots + a_k b^{k-1} = c_1 + c_2 b + \ldots + c_k b^{k-1}$$

با تکرار روال فوق به این نتیجه می‌رسیم که $a_1 = c_1, a_2 = c_2, \ldots, a_k = c_k$

رابطه (*) نمایش n در مبنای b نامیده شده و به صورت زیر نشان داده می‌شود.

$$n = \overline{a_k a_{k-1} \ldots a_0}_{(b)}$$

نمایش معمولی دهدهی متناظر با $b = 10$ است و در این حالت بجای نمایش فوق می‌نویسیم $n = a_k a_{k-1} \ldots a_0$ (به طور مثال $\overline{4567}_{(10)} = 4567$)

مثال ۱. ۴۰. فرض کنید $\overline{xy}$ و $\overline{yx}$ دو عدد صحیح دو رقمی باشند. ثابت کنید جمع آن‌ها مرکب است.

اثبات: از $\overline{xy} = 10x + y$ و $\overline{yx} = 10y + x$، جمع آن‌ها برابر $11x + 11y = 11(x + y)$ است که یک عدد مرکب می‌باشد.

مثال ۱. ۴۱. [AHSME ۱۹۷۳] در معادله‌ی زیر هر حرف به طور منحصر به فردی بیانگر یک رقم متفاوت در مبنای ۱۰ است

$$(YE).(ME) = TTT$$

مجموع $E + M + T + Y$ را تعیین کنید.

پاسخ: چون $TTT = 111 \times T = 3 \times 37 \times T$، یکی از اعداد YE یا ME، ۳۷ است لذا T .E = ۷ یک عدد یک رقمی بوده و $3 \times T$ یک عدد دو رقمی است که به ۷ ختم می‌شود. بنابراین $T = 9$ است و $TTT = 999 = 27 \times 37$ و

$$?=E+M+T+Y=۲+۳+۷+۹=۲۱$$

مثال ۱. ۴۲. [AIME ۲۰۰۱] مجموع همه‌ی اعداد صحیح دو رقمی مثبت که بر هر دو رقمشان بخش‌پذیرند را بیابید.

پاسخ: فرض کنید $\overline{ab}$ یک عدد صحیح با خاصیت مطلوب باشد. در این صورت $۱۰a+b$ باید بر a و b بخش‌پذیر باشد. این بدان معناست که b باید بر a بخش‌پذیر باشد و $۱۰a$ بر b. شرط اول نشان می‌دهد که $b=ka$ که k یک عدد صحیح مثبت است و از شرط دوم $k=۱$ یا $k=۲$ یا $k=۵$ می‌باشد. بنابراین اعداد دو رقمی موردنیاز عبارتند از: $۴۸,۳۶,۲۴,۱۲,۹۹,...,۲۲,۱۱$ و ۱۵. جمع این اعداد برابر است با $۱۵+۱۰\times۱۲+۴۵\times۱۱=۶۳۰$

مثال ۱. ۴۳. [AMC12A ۲۰۰۲] برخی از مجموعه‌های متشکل از اعداد اول مانند $\{۷,۸۳,۴۲۱,۶۵۹\}$ از هر ۹ رقم غیر صفر دقیقاً یک بار استفاده می‌کنند. کوچک‌ترین مقدار ممکن برای مجموع اعضای چنین مجموعه‌ای چند است؟

پاسخ: جواب ۲۰۷ است. توجه کنید ارقام ۴، ۶ و ۸ نمی‌توانند در رقم یکان ظاهر شوند. بنابراین مجموع حداقل برابر $۴۰+۶۰+۸۰+۱+۲+۳+۵+۷+۹=۲۰۷$ است. از طرف دیگر این مقدار را می‌توان در مجموعه‌ی $\{۲,۵,۷,۴۳,۶۱,۸۹\}$ مشاهده کرد.

مثال ۱. ۴۴. عدد $\overline{۱۰۱۰۱۱}_{(۲)}$ را در مبنای ۱۰ و عدد ۱۲۱۱ را در مبنای ۳ بنویسید.

پاسخ: داریم

$$\overline{۱۰۱۰۰۱۱}_{(۲)}=۱\times۲^۶+۰\times۲^۵+۱\times۲^۴+۰\times۲^۳+۰\times۲^۲+۱\times۲+۱=۶۴+۱۶+۲+۱=۸۳$$

با تقسیم‌های متوالی بر ۳، باقی مانده‌ها با شروع از آخرین باقیمانده ارقام عدد در مبنای ۳ هستند. اولین رقم، آخرین خارج‌قسمت غیر صفر است. می‌توان محاسبات را به صورت زیر انجام داد:

۱۲۱۱	۳				
۱۲۰۹	۴۰۳	۳			
۲	۴۰۲	۱۳۴	۳		
	۱	۱۳۲	۴۴	۳	
		۲	۴۲	۱۴	۳
			۲	۱۲	۴
				۲	۳
					۱

بنابراین: $\overline{۱۱۲۲۲۱۲}_{(۳)}=۱۲۱۱$

مثال ۱. ۴۵. حاصل‌ضرب عدد ۶ رقمی $\overline{abcdef}$ در عدد ۷ برابر با حاصل‌ضرب عدد ۶ رقمی $\overline{defabc}$ در عدد ۶ است. این دو عدد ۶ رقمی را بیابید.

پاسخ: فرض کنید x و y به ترتیب بیانگر اعداد سه رقمی $\overline{abc}$ و $\overline{def}$ باشند. به این ترتیب $\overline{abcdef}=۱۰۰۰x+y$ و $\overline{defabc}=۱۰۰۰y+x$. از شرایط داده شده نتیجه می‌گیریم که $۷\times(۱۰۰۰x+y)=۶\times(۱۰۰۰y+x)$ و یا $۶۹۹۴x=۵۹۹۳y$. با توجه به اینکه $\gcd(۶۹۹۴,۵۹۹۳)=\gcd(۱۰۰۱,۵۹۹۳)=\gcd(۱۰۰۱,۱۳)=۱۳$ لذا $۵۳۸x=۴۶۱y$ و بنابراین دو عدد موردنظر عبارتند از ۴۶۱۵۳۸ و ۵۳۸۴۶۱.

مثال ۱. ۴۶. [AMC12A ۲۰۰۵] یک دستگاه معیوب مسافت‌سنج در اتومبیل از رقم ۳ به رقم ۵ می‌پرد و همیشه رقم ۴ را بدون توجه به جایگاه آن در نظر نمی‌گیرد. به طور مثال بعد از طی مسافت یک مایل مسافت‌سنج از ۰۰۰۰۳۹ به ۰۰۰۰۵۰ تغییر می‌کند. اگر مسافت‌سنج در حال حاضر عدد ۰۰۲۰۰۵ را نشان دهد اتومبیل در واقع چه مسافتی را طی کرده است؟

پاسخ: از آن جا که مسافت‌سنج فقط از ۹ رقم استفاده می‌کند، مسافت را در مبنای ۹ اندازه می‌گیرد به جز این که ارقام ۵، ۶، ۷، ۸ و ۹ آن بیانگر ارقام ۴، ۵، ۶، ۷ و ۸ در مبنای ۹ هستند. بنابراین مسافت طی شده برابر است با:

$$۲۰۰۴_{(۹)}=۲\times۹^۳+۴=۲\times۷۲۹+۴=۱۴۶۲$$

مثال ۱. ۴۷. ثابت کنید عدد $\underbrace{۱۱...۱}_{n\text{ تا}}{}_{(۹)}$ در مبنای ۹ مثلثی است. یعنی برای یک عدد صحیح k برابر مجموع اولین k عدد صحیح مثبت است.

اثبات:

$$\underbrace{۱۱...۱}_{n\text{ تا}}{}_{(۹)}=۹^{n-۱}+۹^{n-۲}+...+۹+۱$$

$$=\frac{۹^n-۱}{۹-۱}=\frac{۱}{۲}\times\frac{۳^n-۱}{۲}\times\frac{۳^n+۱}{۲}$$

$$=۱+۲+...+\frac{۳^n-۱}{۲}$$

که یک عدد مثلثی است.

مثال ۱. ۴۶. همه‌ی اعداد صحیح مثبت n را چنان پیدا کنید که $(n)۱۱۱۱۱$ مربع کامل باشد.

پاسخ: جواب $n=۳$ است.

$$(n)۱۱۱۱۱ = n^۴ + n^۳ + n^۲ + n + ۱$$

اگر n زوج باشد $n^۲ + \frac{n}{۲}$ و $n^۲ + \frac{n}{۲} + ۱$ دو عدد صحیح متوالی هستند. داریم

$$(n^۲ + \frac{n}{۲})^۲ = n^۴ + n^۳ + \frac{n^۲}{۴} < n^۴ + n^۳ + n^۲ + n + ۱ < (n^۲ + \frac{n}{۲} + ۱)^۲$$

بنابراین برای اعداد صحیح زوج n، $(n)۱۱۱۱۱$ نمی‌تواند مربع کامل باشد.

اگر n فرد باشد، اعداد $n^۲ + \frac{n}{۲} - \frac{۱}{۲}$ و $n^۲ + \frac{n}{۲} + \frac{۱}{۲}$ صحیح متوالی هستند و

$$(n^۲ + \frac{n}{۲} - \frac{۱}{۲})^۲ < n^۴ + n^۳ + n^۲ + n + ۱$$

با توجه به اینکه

$$\begin{aligned}(n^۲ + \frac{n}{۲} + \frac{۱}{۲}) &= n^۴ + n^۳ + \frac{۵n^۲}{۴} + \frac{n}{۲} + \frac{۱}{۴} \\ &= n^۴ + n^۳ + n^۲ + n + ۱ + \frac{n^۲ - ۲n - ۳}{۴} \\ &= n^۴ + n^۳ + n^۲ + n + ۱ + \frac{(n-۳)(n+۱)}{۴}\end{aligned}$$

برای اعداد صحیح فرد n بزرگ‌تر از ۳، $(n)۱۱۱۱۱$ اکیداً بین دو مربع کامل متوالی قرار دارد که عبارتند از:

$$(n^۲ + \frac{n}{۲} - \frac{۱}{۲})^۲ \ , \ (n^۲ + \frac{n}{۲} + \frac{۱}{۲})^۲$$

بنابراین $(n)۱۱۱۱۱$ برای اعداد صحیح مثبت غیر از ۳ مربع کامل نیست. برای

$$(۳)۱۱۱۱۱ = ۱۲۱ = ۱۱^۲ \ , \ n = ۳$$

در آخرین مثال، نشان دادیم که یک عدد صحیح اگر بین دو عدد مربع کامل قرار گیرد نمی‌تواند مربع کامل باشد. این روش به دلیل گسسته بودن اعداد صحیح کارآمد است. چنین روش‌هایی به

ندرت برای اعداد حقیقی جواب می‌دهد چرا که هیچ فضای خالی بین اعداد حقیقی وجود ندارد. این روش در حل معادلات دیوفانتین خیلی مفید است.

در برخی دستگاه‌های عددی خاص مبنا نباید ثابت باشد. در این جا دو مثال می‌آوریم.

قضیه ۱. ۴۲. هر عدد صحیح مثبت k یک بسط یکتا بر مبنای فاکتوریل به صورت:

$$(f_1, f_2, f_3, \ldots, f_m)$$

دارد یعنی:

$$k = 1! \times f_1 + 2! \times f_2 + 3! \times f_3 + \ldots + m! \times f_m$$

که f_i یک عدد صحیح بوده و $0 \leq f_i \leq i$ و $f_m > 0$.

اثبات: توجه کنید که فقط یک عدد صحیح مثبت m_1 وجود دارد به طوری که $m_1! \leq k < (m_1+1)!$. از الگوریتم تقسیم می‌توان نوشت:

$$k = m_1! f_{m_1} + r_1$$

که درآن f_{m_1} و r_1 اعداد صحیح مثبت بوده و $0 \leq r_1 < m_1!$. با توجه به اینکه $k < (m_1+1)! = m_1!(m_1+1)$ نتیجه می‌گیریم که $f_{m_1} \leq m_1$. با تکرار این فرآیند می‌توان نوشت:

$$r_1 = m_2! f_{m_2} + r_2$$

که m_2 عدد صحیح مثبت یکتایی است که $m_2! \leq r_1 < (m_2+1)!$، $1 \leq f_{m_2} \leq m_2$ و $0 \leq r_2 < m_2!$. با تکرار این عمل روی r_2 و الی آخر به بسط یکتای k در مبنای فاکتوریل می‌رسیم.

قضیه ۱. ۴۳. دنباله‌ی $F_{n+1} = F_n + F_{n-1}, F_1 = 1, F_0 = 1$ برای هر عدد صحیح مثبت n را در نظر بگیرید. (این دنباله، دنباله فیبوناچی و اعداد تشکیل دهنده آن اعداد فیبوناچی نامیده می‌شوند) هر عدد صحیح نامنفی n را می‌توان به طور یکتا به صورت مجموع اعداد فیبوناچی مثبت غیر متوالی نوشت یعنی هر عدد صحیح نامنفی n را می‌توان به طور یکتا به شکل

$$n = \sum_{k=0}^{\infty} \alpha_k F_k$$

نوشت که برای هر k، $\alpha_k \in \{0,1\}$ و $(\alpha_k, \alpha_{k+1}) \neq (1,1)$. این بیان برای n، نمایش زکندورف آن نامیده می‌شود.

اثبات قضیه ۱. ۴۳ مشابه قضیه ۱. ۴۲ است که جزئیات آن را به خواننده می‌سپاریم.

مثال ۱. ۴۹. [AIME ۲۰۰۰] $(f_1, f_2, f_3, \ldots, f_j)$ بسط در مبنای فاکتوریل عدد

$$16! - 32! + 48! - 64! + \ldots + 1968! - 1984! + 2000!$$

است. مقدار عبارت $f_1 - f_2 + f_3 - f_4 + \ldots + (-1)^{j-1} f_j$ را بیابید.

پاسخ: از $n! \cdot n = (n+1)! - n!$ نتیجه می‌گیریم که:

$$\begin{aligned}(n+16)! - n! = \\ &= (n+16)! - (n+15)! + (n+15)! - (n+14)! + \ldots + (n+1)! - n! \\ &= (n+15)!(n+15) + (n+14)!(n+14) + \ldots + (n+1)!(n+1) + n!n\end{aligned}$$

این رابطه نشان می‌دهد که بسط در مبنای فاکتوریل $(n+16)! - n!$ برابر است با:

$$(0, 0, \ldots, 0, n, n+1, \ldots, n+14, n+15)$$

که با یک ردیف $n-1$ تایی صفر شروع می‌شود. بسط در مبنای فاکتوریل ۱۶! برابر $(0,0,\ldots,0,1)$ است لذا بسط مطلوب عبارت است از:

$$(0,0,\ldots,0;1;0,\ldots,0;32,33,\ldots,47;0,\ldots,0;64,\ldots,79;\ldots;1984,\ldots,1999).$$

توجه کنید که با شروع از جایگاه ۳۲، بسط فوق شامل گروه‌های ۱۶ تایی از اعداد غیر صفر و به دنبال آن یک گروه ۱۶ تایی صفر می‌باشد. با استثنای $f_{16} = 1$، هر f_i غیر صفر برابر i است. هر یک از ۶۲ گروه از ۱۶ عدد غیر صفر، عدد ۸ را در حاصل جمع موردنظر شرکت می‌دهند و f_{16} عدد ۱- را شرکت می‌دهد لذا مقدار مطلوب $8 \times 62 - 1 = 495$ است.

شرایط بخش‌پذیری در دستگاه دهدهی

در این بخش برخی از شرایط بخش‌پذیری اعداد صحیح در دستگاه دهدهی را اثبات می‌کنیم.

قضیه ۱. ۴۴. فرض کنید $n = \overline{a_h a_{h-1} \ldots a_0}$ یک عدد صحیح مثبت باشد.

(آ) $S(n)$ را برابر مجموع ارقام n یعنی $a_0+a_1+\ldots+a_h$ تعریف می‌کنیم. آنگاه (پیمانه ۳) $S(n)\equiv n$. در حالت خاص، n بر ۳ بخش‌پذیر است اگر و فقط اگر مجموع ارقامش، $S(n)$، بر ۳ بخش‌پذیر باشد.

(ب) می‌توان در رابطه‌ی قبلی ۳ را با ۹ جایگزین کرد یعنی (پیمانه ۹) $S(n)\equiv n$. در حالت خاص، n بر ۹ بخش‌پذیر است اگر و فقط اگر مجموع ارقامش $S(n)$ بر ۹ بخش‌پذیر باشد.

(پ) $S'(n)$ را برابر $a_0-a_1+a_2+\ldots+(-1)^h a_h$ قرار می‌دهیم. n بر ۱۱ بخش‌پذیر است اگر و فقط اگر $S'(n)$ بر ۱۱ بخش‌پذیر باشد.

(ت) n بر ۷، ۱۱ یا ۱۳ بخش‌پذیر است اگر و فقط اگر $\overline{a_h a_{h-1}\ldots a_2}-\overline{a_2 a_1 a_0}$ نیز این خاصیت را داشته باشد.

(ث) n بر ۲۷ یا ۳۷ بخش‌پذیر است اگر و فقط اگر $\overline{a_h a_{h-1}\ldots a_2}+\overline{a_2 a_1 a_0}$ نیز این خاصیت را داشته باشد.

(ج) n بر 2^k یا 5^k ($k\le h$) بخش‌پذیر است اگر و فقط اگر $\overline{a_{k-1}\ldots a_0}$ این خاصیت را داشته باشد.

اثبات: برای (آ) و (ب) از $10^k=(9+1)^k$ نتیجه می‌گیریم که (پیمانه ۹) $10^k\equiv 1$ بنابراین:

$$n\equiv\sum_{k=0}^{h}a_k 10^k\equiv\sum_{k=0}^{h}a_k\equiv S(n)\quad\text{(پیمانه ۹)}$$

برای (پ) توجه می‌کنیم که $10^k=(11-1)^k$ لذا (پیمانه ۱۱) $10^k\equiv(-1)^k$ و بنابراین:

$$n\equiv\sum_{k=0}^{h}a_k 10^k\equiv\sum_{k=0}^{h}a_k.(-1)^k\equiv S'(n)\quad\text{(پیمانه ۱۱)}$$

برای (ت) حکم از این حقیقت نتیجه می‌شود که $13\times 11\times 7=1001$ و

$$n=\overline{a_h a_{h-1}\ldots a_2}\times 1000+\overline{a_2 a_1 a_0}=\overline{a_h a_{h-1}\ldots a_2}\times(1001-1)+\overline{a_2 a_1 a_0}$$

برای (ث) حکم از این حقیقت نتیجه می‌شود که $37\times 27=999$ و

$$n=\overline{a_h a_{h-1}\ldots a_2}\times 1000+\overline{a_2 a_1 a_0}=\overline{a_h a_{h-1}\ldots a_2}\times(999+1)+\overline{a_2 a_1 a_0}$$

برای (ج) توجه می‌کنیم که (پیمانه m) $10^k\equiv 0$ برای $m=2^k$ یا $m=5^k$. بنابراین داریم

$$n=\overline{a_h...a_k}\times 10^{k}+\overline{a_{k-1}...a_0}$$

که به این ترتیب حکم نتیجه می‌شود.

مثال ۱. ۵۰. مربع کامل هست یا نه؟

(۱) همه‌ی اعداد صحیح مثبت k را چنان تعیین کنید که عدد k رقمی ۱...۱۱ مربع کامل نباشد.

(۲) آیا یک عدد ۵ رقمی شامل فقط ارقام زوج متمایز می‌تواند مربع کامل باشد.

(۳) تعیین کنید که آیا $\underbrace{200....04}_{2004}$ مربع کامل است؟

پاسخ: جواب‌ها برای همه‌ی این سؤال‌ها منفی هستند.

(۱) حکم برای $k=1$ برقرار است. ادعا می‌کنیم که جواب دیگری وجود ندارد.

از (پیمانه ۴) $3\equiv 11\equiv \underbrace{11....}_{k\ \text{تا}}$ نتیجه می‌گیریم که $\underbrace{11....}_{k\ \text{تا}}$ مربع کامل نیست (مثال ۱. ۲۴ (۳))

(۲) جواب منفی است. اگر n یک عدد ۵ رقمی شامل ارقام زوج متمایز باشد آنگاه مجموع ارقام آن برابر است با $20=8+6+4+2+0$ که به پیمانه ۹ با ۲ هم‌نهشت است. لذا مربع کامل نیست. (مثال ۱. ۲۴ (۴))

(۳) عدد داده شده مربع کامل نیست چون مجموع ارقام آن ۶ است یعنی مضرب ۳ می‌باشد اما مضرب ۹ نیست (مثال ۱. ۲۴ (۴))

مثال ۱. ۵۱. [AIME ۱۹۸۴] عدد صحیح n کوچک‌ترین مضرب مثبت ۱۵ است به طوری که هر رقم n یا صفر است یا ۸. n را پیدا کنید.

پاسخ: عدد صحیح n بر ۱۵ بخش‌پذیر است اگر و فقط اگر بر ۳ و ۵ بخش‌پذیر باشد. از قضیه ۱. ۴۴ (آ) و (ج) جواب $n=8880$ است.

مثال ۱. ۵۲. تعداد اعداد صحیح و مثبت ۵ رقمی $\overline{abcde}$ (a,b,c,d,e لزوماً متمایز نیستند) را تعیین کنید که مجموع عدد سه رقمی $\overline{abc}$ و عدد دو رقمی $\overline{de}$ بر ۱۱ بخش‌پذیر باشد.

پاسخ: جواب ۸۱۸۱ است.

$$\overline{abcde}=\overline{abc}\times 100+\overline{de}=\overline{abc}+\overline{de}+99\times\overline{abc}$$

بنابراین $\overline{abc}+\overline{de}$ بر ۱۱ بخش‌پذیر است اگر و فقط اگر $\overline{abcde}$ بر ۱۱ بخش‌پذیر باشد. عدد ۹۹۹۹۰ بزرگ‌ترین عدد ۵ رقمی است که بر ۱۱ بخش‌پذیر است و ۹۹۹۹ بزرگ‌ترین عدد ۴ رقمی

بخش‌پذیر بر ۱۱ است. بنابراین $\frac{۹۹۹۹۰}{۱۱}=۹۰۹۰$ مضرب ۱۱ وجود دارد که حداکثر ۵ رقم دارند و $\frac{۹۹۹۹}{۱۱}=۹۹۹$ مضرب ۱۱ وجود دارد که حداکثر ۴ رقم دارند. لذا دقیقاً $۹۰۹۰-۹۹۹=۸۱۸۱$ مضرب ۱۱ وجود دارد که دقیقاً ۵ رقم دارند.

مثال ۱. ۵۳. [USAMO ۲۰۰۳] ثابت کنید برای هر عدد صحیح مثبت n یک عدد n رقمی وجود دارد که بر ۵^n بخش‌پذیر بوده و همه‌ی ارقام آن فرد هستند.

پاسخ اول: از استقرا استفاده می‌کنیم. حکم برای $n=۱$ به وضوح برقرار است. فرض می‌کنیم $N=\overline{a_۱a_۲...a_n}$ بر ۵^n بخش‌پذیر بوده و فقط شامل ارقام فرد است. اعداد زیر را در نظر بگیرید:

$$N_۱=\overline{۱a_۱...a_n}=۱\times۱۰^n+۵^nM=۵^n(۱\times۲^n+M)$$
$$N_۲=\overline{۳a_۱...a_n}=۳\times۱۰^n+۵^nM=۵^n(۳\times۲^n+M)$$
$$N_۳=\overline{۵a_۱...a_n}=۵\times۱۰^n+۵^nM=۵^n(۵\times۲^n+M)$$
$$N_۷=\overline{۷a_۱...a_n}=۷\times۱۰^n+۵^nM=۵^n(۷\times۲^n+M)$$
$$N_۵=\overline{۹a_۱...a_n}=۹\times۱۰^n+۵^nM=۵^n(۹\times۲^n+M)$$

اعداد $M+۱\times۲^n$، $M+۳\times۲^n$، $M+۵\times۲^n$، $M+۷\times۲^n$ و $M+۹\times۲^n$ در تقسیم بر ۵ باقی‌مانده‌های متمایزی دارند. به عبارت دیگر اختلاف هیچ ۲ تا از این اعداد بر ۵ بخش‌پذیر نیست زیرا نه ۲^n بر ۵ بخش‌پذیر است نه اختلاف هر دو عدد از اعداد ۱، ۳، ۵، ۷ و ۹. این بدان معناست که یکی از اعداد $N_۱,N_۲,N_۳,N_۴,N_۵$ بر $۵^n\times۵$ بخش‌پذیر است و استقرا کامل می‌شود.

پاسخ دوم: برای عدد m رقمی a، که $m\geq n$ است $\ell(a)$ بیانگر $m-n$ رقم سمت چپ a است (یعنی $\ell(a)$ یک عدد $(m-n)$ رقمی است). واضح است که می‌توانیم عدد فرد و بزرگ k را چنان انتخاب کنیم که $a_۰=۵^n\times k$ حداقل n رقم داشته باشد. فرض کنید $m_۰,a_۰$ رقم دارد که $m_۰\geq n$. از آن جا که $a_۰$ مضرب فردی از ۵ است رقم یکان آن برابر ۵ می‌باشد.

اگر n رقم سمت راست $a_۰$ همگی فرد باشند آنگاه عدد $b_۰=a_۰-\ell(a_۰)\times۱۰^n$ در شرایط مسأله صدق می‌کند زیرا $b_۰$ فط از ارقام فرد تشکیل شده (همان n رقم سمت راست $a_۰$) و برابر تفاضل دو عدد مضرب ۵^n می‌باشد.

اگر در بین n رقم سمت راست a_0 یک رقم زوج وجود داشته باشد، i_1 را برابر کوچک‌ترین عدد صحیح مثبت بگیرید که i_1 امین رقم سمت راست a_0، زوج باشد. در این حالت عدد $a_1 = a_0 + 5^n \times 10^{i_1-1}$ مضربی از 5^n است که حداقل n رقم دارد. $i_1 - 1$ رقم سمت راست این عدد با $i_1 - 1$ رقم سمت راست a_0 یکی است و رقم i_1 ام a_1 فرد است. اگر n رقم سمت راست a_1 همگی فرد باشند. $b_1 = a_1 - \ell(a_1) \times 10^n$ در شرایط مسأله صدق می‌کند. اگر یک رقم زوج در بین n رقم سمت راست a_1 وجود داشته باشد، فرض کنید i_2 کوچک‌ترین عدد صحیح مثبت است که i_2 امین رقم سمت راست a_1 زوج است. طبیعی است $i_2 > i_1$. عدد $a_2 = a_1 + 5 \times 10^{i_2-1}$ را در نظر بگیرید. می‌توان فرآیند فوق را روی ارقام سمت راست a_2 و برای از بین بردن ارقام زوج آن تکرار کرد. اما این کار حداکثر می‌تواند $n-1$ بار تکرار شود زیرا رقم یکان a_0، ۵ است. بنابراین می‌توان عدد a_k را به دست آورد به طوری که a_k مضرب 5^n بوده و همه‌ی n رقم سمت راست آن فرد باشد. به این ترتیب $b_k = a_k - \ell(a_k) \times 10^n$ عددی است که شرایط مسأله را برآورده می‌کند.

می‌توان شرط فرد بودن ارقام را با هر مجموعه‌ی شامل ۵ رقم که یک دستگاه کامل مانده‌ها به پیمانه ۵ را تشکیل می‌دهند عوض کرد. دقیقاً به همان روش می‌توان نشان داد که برای هر عدد صحیح مثبت n، یک عدد n رقمی مضرب 2^n وجود دارد که همه‌ی ارقامش یک دستگاه کامل مانده‌ها به پیمانه ۵ را تشکیل می‌دهند.

این بخش را با بحث بیشتر روی $S(n)$، مجموع ارقام عدد صحیح مثبت n، به پایان می‌بریم.

قضیه ۱. ۴۵. فرض کنید n یک عدد صحیح مثبت و $S(n)$ مجموع ارقام آن باشد. آنگاه خواص زیر برقرارند:

(آ) $9 \mid S(n) - n$

(ب) $S(n_1 + n_2) \le S(n_1) + S(n_2)$

(پ) $S(n_1 n_2) \le \min(n_1 S(n_2), n_2 S(n_1))$

(ت) $S(n_1 n_2) \le S(n_1) S(n_2)$

اثبات: قسمت (آ) همان قضیه‌ی ۱. ۴۴ (ب) است. حال قسمت‌های ب، پ و ت را اثبات می‌کنیم. n_1, n_2 و $n_1 + n_2$ را به شکل $n_1 = \overline{a_k a_{k-1} \ldots a_0}$، $n_2 = \overline{b_h b_{h-1} \ldots b_0}$ و $n_1 + n_2 = \overline{c_s c_{s-1} \ldots c_0}$ در نظر بگیرید.

به منظور اثبات قسمت ب، کوچک‌ترین t را چنان انتخاب می‌کنیم به طوری که برای هر $t < i$، $a_i + b_i < 10$ باشد. به این ترتیب $a_t + b_t \ge 10$، $c_t = a_t + b_t - 10$ و $c_{t+1} \le a_{t+1} + b_{t+1} + 1$. در نتیجه به رابطه‌ی زیر می‌رسیم.

$$\sum_{i=1}^{t+1} c_i \le \sum_{i=1}^{t+1} a_i + \sum_{i=1}^{t+1} b_i$$

با ادامه دادن این روال، حکم اثبات می‌شود.

به دلیل تقارن، برای اثبات (پ) کافی است ثابت کنیم $S(n_1 n_2) \le n_1 S(n_2)$. نامساوی اخیر با تکرار متوالی خاصیت (ب) به دست می‌آید.

$$S(2n_2) = S(n_2 + n_2) \le S(n_2) + S(n_2) = 2S(n_2)$$

و بعد از n_1 مرحله

$$S(n_1 n_2) = S(\underbrace{n_2 + \ldots + n_2}_{n_1 \text{ بار}}) \le \underbrace{S(n_2) + \ldots + S(n_2)}_{n_1 \text{ بار}} = n_1 S(n_2)$$

برای قسمت (ت)، از (ب) و (پ) مشاهده می‌شود که:

$$\begin{aligned} S(n_1 n_2) &= S(n_1 \sum_{i=0}^{h} b_i \times 10^i) = S(\sum_{i=0}^{h} n_1 b_i \times 10^i) \\ &\le \sum_{i=0}^{h} S(n_1 b_i 10^i) = \sum_{i=0}^{h} S(n_1 b_i) \le \sum_{i=0}^{h} b_i S(n_1) \\ &= S(n_1) \sum_{i=0}^{h} b_i = S(n_1) S(n_2) \end{aligned}$$

که همان نتیجه مطلوب است.

از اثبات قضیه ۱. ۴۵ مشخص می‌شود که در مسائلی که با جمع ارقام عدد سر و کار داریم، کار با ده‌بریک‌ها اهمیت زیادی دارد.

مثال ۱. ۵۴. [۱۹۹۹ روسیه] در بسط دهدهی n، هر رقم (بجز اولین رقم) بزرگ‌تر از رقم سمت چپش است مقدار $S(9n)$ چند است؟

پاسخ: n را به صورت $n = \overline{a_k a_{k-1} \ldots a_0}$ می‌نویسیم. با انجام تفریق زیر

$$\begin{array}{cccccc} a_k & a_{k-1} & \ldots & a_1 & a_0 & 0 \\ - & a_k & \ldots & a_2 & a_1 & a_0 \\ \hline \end{array}$$

ارقام عدد $9n = 10n - n$ به صورت زیر به دست می‌آید.

$$a_k\ ,\ a_{k-1} - a_k\ \ ,\ldots,\ a_1 - a_2\ ,\ a_0 - a_1 - 1\ ,\ 10 - a_0$$

جمع این ارقام برابر $9 = 1 - 10$ است.

مثال ۱.۵۵. [۱۹۹۶ ایرلند] عدد صحیح مثبت n را چنان پیدا کنید که

$$S(n) = 1996S(3n)$$

پاسخ: عدد

$$n = 1\underbrace{33\ldots333}_{\text{۵۹۸۶ تا ۳}}5$$

را در نظر بگیرید. داریم

$$3n = 4\underbrace{00\cdots00}_{\text{۵۹۸۶ تا ۰}}5$$

بنابراین $1996S(3n) = 1996 \times 9 = 17964 = 3 \times 5986 + 1 + 5 = S(n)$ که همان نتیجه دلخواه است.

مثال ۱.۵۶. تعیین کنید که آیا عدد مربع کاملی وجود دارد که به ۱۰ رقم متمایز ختم شود.

پاسخ: جواب مثبت است. توجه کنید که

$$\begin{array}{r} 1\ 1\ 1\ 1 \\ \times\ 1\ 1\ 1\ 1 \\ \hline 1\ 1\ 1\ 1 \\ 1\ 1\ 1\ 1 \\ 1\ 1\ 1\ 1 \\ 1\ 1\ 1\ 1 \\ \hline 1\ 2\ 3\ 4\ 3\ 2\ 1 \end{array}$$

به همین ترتیب به سادگی می‌توان دید که

$$11111111111^2 = 123456789098765432 1$$

عددی است که شرایط مسأله را برآورده می‌سازد.

مثال ۱. ۵۵. [IMO ۱۹۷۶] وقتی که عدد $۴۴۴۴^{۴۴۴۴}$ در مبنای ۱۰ نوشته شود، مجموع ارقامش برابر A است. فرض کنید B مجموع ارقام A باشد. مجموع ارقام B را پیدا کنید.

پاسخ: جواب ۷ است.

اگر $a=۴۴۴۴^{۴۴۴۴}$ آنگاه $A=S(a)$، $B=S(A)$ و می‌خواهیم $S(B)$ را محاسبه کنیم. در ابتدا نشان خواهیم داد که مجموع ارقام B تا حدی کوچک است. با توجه به اینکه $۱۰^۴=۱۰۰۰۰>۴۴۴۴$ بنابراین

$$a=۴۴۴۴^{۴۴۴۴}<۱۰^{۴\times۴۴۴۴}=۱۰^{۱۷۷۷۶}$$

و بنابراین a نمی‌تواند بیش از ۱۷۷۷۶ رقم داشته باشد. از آنجا که هر رقم حداکثر ۹ است، $A=S(a)\le ۱۷۷۷۶\times۹=۱۵۹۹۸۴$. از اعداد طبیعی کوچک‌تر یا مساوی ۱۵۹۹۸۴ عددی که دارای بیشترین مجموع ارقام باشد، ۹۹۹۹۹ است و بنابراین $B=S(A)\le ۴۵$. از اعداد طبیعی کوچک‌تر یا مساوی ۴۵، عددی که دارای بیشترین مجموع ارقام باشد، ۳۹ است. بنابراین $S(B)\le ۱۲$.

از قضیه ۱. ۴۵ (آ) داریم (پیمانه ۹) $S(B)\equiv B\equiv S(A)\equiv A\equiv S(a)\equiv ۴۴۴۴^{۴۴۴۴}$

کافی است نشان دهیم که (پیمانه ۹) $۴۴۴۴^{۴۴۴۴}\equiv ۷$. داریم

$$\begin{aligned}۴۴۴۴^{۴۴۴۴}&\equiv(۴+۴+۴+۴)^{۴۴۴۴}\equiv ۱۶^{۴۴۴۴}\equiv(-۲)^{۴۴۴۴}\\&\equiv(-۲)^{۳\times۱۴۸۱+۱}\equiv((-۲)^۳)^{۱۴۸۱}\times(-۲)\equiv(-۸)^{۱۴۸۱}\times(-۲)\\&\equiv ۱\times(-۲)\equiv ۷\quad(\text{پیمانه }۹)\end{aligned}$$

تابع جزء صحیح (تابع کف)

برای عدد حقیقی x، عدد صحیح یکتای n وجود دارد که $n\le x<n+۱$. می‌گوییم n، بزرگ‌ترین عدد صحیح کوچک‌تر یا مساوی x و یا کف x است و می‌نویسیم $n=\lfloor x\rfloor$. تفاضل $x-\lfloor x\rfloor$ بخش اعشاری x نامیده شده و با $\{x\}$ نمایش داده می‌شود. کوچک‌ترین عدد صحیح بزرگ‌تر یا مساوی x، سقف x نامیده شده و با $\lceil x\rceil$ نشان داده می‌شود. اگر x عدد صحیح باشد آنگاه $\lceil x\rceil=\lfloor x\rfloor$ و $\{x\}=۰$؛ اگر صحیح نباشد $\lceil x\rceil=\lfloor x\rfloor+۱$.

بحث را با چهار مثال (جبری) آغاز می‌کنیم تا با این توابع بیشتر آشنا شوید.

مثال ۱. ۵۶. [۱۹۹۹ استرالیا] دستگاه معادلات زیر را حل کنید:

$$\begin{aligned}x+\lfloor y\rfloor+\{z\}&=۲۰۰/۰\\\{x\}+y+\lfloor z\rfloor&=۱۹۰/۱\end{aligned}$$

$$\{x\}+\lfloor y\rfloor=۱۰۵/۶۵$$

پاسخ: از آنجا که برای همه‌ی اعداد حقیقی x، $x=\lfloor x\rfloor+\{x\}$ است با جمع کردن سه معادله خواهیم داشت:

$$x+y+z=۲۸۴/۴۵ \text{ یا } ۲x+۲y+۲z=۵۶۸/۹$$

با کم کردن سه معادله داده شده از معادله‌ی فوق به معادلات زیر می‌رسیم:

$$\{y\}+\lfloor z\rfloor=۸۴/۴۵$$
$$\lfloor x\rfloor+\{z\}=۹۴/۳۵$$
$$\{x\}+\lfloor y\rfloor=۱۰۵/۶۵$$

بنابراین $\lfloor z\rfloor=\lfloor\{y\}+\lfloor z\rfloor\rfloor=\lfloor ۸۴/۴۵\rfloor=۸۴$ و در نتیجه $\lfloor z\rfloor=۸۴$ و $\{y\}=۰/۴۵$. به همین ترتیب $\lfloor y\rfloor=۱۰۵$ و لذا $y=۱۰۵/۴۵$. به طور مشابه خواهیم داشت $x=۹۴/۶۵$ و $z=۸۴/۳۵$.

مثال ۱. ۵۹. اعداد متمایز را در دنباله‌ی زیر مشخص کنید؟

$$\left\lfloor\frac{۱^۲}{۲۰۰۵}\right\rfloor,\left\lfloor\frac{۲^۲}{۲۰۰۵}\right\rfloor,\ldots,\left\lfloor\frac{۲۰۰۵^۲}{۲۰۰۵}\right\rfloor.$$

پاسخ: برای $۱\le i\le ۲۰۰۵$ فرض کنید $a_i=\left\lfloor\frac{i^۲}{۲۰۰۵}\right\rfloor$

از آن جا که $۴۴^۲=۱۹۳۶<۲۰۰۵<۲۰۲۵=۴۵^۲$ لذا $a_۱=a_۲=\cdots=a_{۴۴}=۰$. برای اعداد صحیح $m\le ۱۰۰۲$ از

$$\frac{(m+۱)^۲}{۲۰۰۵}-\frac{m^۲}{۲۰۰۵}=\frac{۲m+۱}{۲۰۰۵}\ge ۱$$

نتیجه می‌گیریم که $a_m<a_{m+۱}$. بنابراین $a_{۱۰۰۲},a_{۱۰۰۳},\ldots,a_{۲۰۰۵}$ مقادیر متمایزی دارند.
برای عدد صحیح $m>۱۰۰۲$ از

$$\frac{(m+۱)^۲}{۲۰۰۵}-\frac{m^۲}{۲۰۰۵}=\frac{۲m+۱}{۲۰۰۵}<۱$$

نتیجه می‌گیریم که $a_{m+۱}\le a_m+۱$. با توجه به این که این دنباله غیر نزولی است نتیجه می‌گیریم که همه‌ی مقادیر صحیح کوچک‌تر از $a_{۱۰۰۱}$ در دنباله وجود دارد.

مقدار $a_{۱۰۰۱}=۴۹۹$ و $a_{۱۰۰۲}=۵۰۰$ می باشند. بنابراین جواب مسأله $۱۵۰۴=۱۰۰۴+۵۰۰$ است (این مقادیر عبارتند از صفر، ۱، ... ، ۴۹۹، $a_{۱۰۰۲}, a_{۱۰۰۳}, \ldots, a_{۲۰۰۵}$).

مثال ۱. ۶۰. [ARML ۲۰۰۳] عدد صحیح مثبت n را چنان پیدا کنید که $\frac{۱}{n}$ نزدیک‌ترین مقدار به $\{\sqrt{۱۲۳۴۵۶۷۸۹}\}$ باشد.

پاسخ: چنان که در مثال ۱. ۵۶. نشان داده شد، داریم

$$۱۱۱۱۱/۱۲^۲ = ۱۲۳۴۵۶۷۶۵/۴۳۲۱ < ۱۲۳۴۵۶۷۸۹$$
$$< ۱۲۳۴۵۶۷۸۹/۸۷۶۵۴۳۲۱ = ۱۱۱۱۱/۱۱۱۱^۲$$

بنابراین

$$\frac{۱}{۹} > ۰/۱۱۱۱ > \{\sqrt{۱۲۳۴۵۶۷۸۹}\} > ۰/۱۱ > \frac{۱}{۱۰} \text{ و } \lfloor\sqrt{۱۲۳۴۵۶۷۸۹}\rfloor = ۱۱۱۱۱$$

مثال ۱. ۶۱. [AIME ۱۹۹۷] فرض کنید a مثبت بوده، $\{a^۲\}=\{a^{-۱}\}$ و $۲ < a^۲ < ۳$ باشد. مقدار $a^{۱۲} - ۱۴۴a^{-۱}$ را پیدا کنید.

پاسخ: ابتدا توجه کنید که توضیح ارائه شده منجر به نتایج $\{a^{-۱}\}=a^{-۱}$ (زیرا برای $a<۱$، داریم $۰<a^{-۱}<۱$) و $\{a^۲\}=a^۲-۲$ می‌شود. بنابراین a باید در معادله‌ی $a^{-۱}=a^۲-۲$ یا $a^۳-۲a-۱=۰$ صدق کند. تجزیه این معادله به صورت

$$(a+۱)(a^۲-a-۱)=۰$$

می‌باشد که تنها ریشه مثبت آن $a=\frac{۱+\sqrt{۵}}{۲}$ است. حال از روابط $a^۲=a+۱$ و $a^۳=۲a+۱$ برای محاسبه‌ی جواب استفاده می‌کنیم.

$$a^۶=۸a+۵ \text{ , } a^{۱۲}=۱۴۴a+۸۹ \text{ و } a^{۱۳}=۲۳۳a+۱۴۴$$

مقدار مورد نظر برابر است با:

$$a^{۱۲}-۱۴۴a^{-۱}=\frac{a^{۱۳}-۱۴۴}{a}=۲۳۳$$

توجه: از رابطه‌ی $a^۲=a+۱$ به سادگی می‌توان نشان داد که $a^n=F_{n-۱}a+F_{n-۲}$ که $\{F_n\}_{n=۰}^{\infty}$ دنباله‌ی فیبوناچی با روابط $F_۰=F_۱=۱$ و $F_{n+۱}=F_n+F_{n-۱}$، برای هر عدد صحیح

مثبت n، است. رابطه‌ی $a^{۲}=a+۱$ معادله مشخصه دنباله فیبوناچی است. برای جزئیات بیشتر در این زمینه می‌توانید به [۱۶] و [۱۷] مراجعه کنید.

مثال ۱. ۶۲ همه‌ی جواب‌های حقیقی معادله‌ی زیر را بیابید؟

$$۴x^{۲}-۴۰\lfloor x\rfloor+۵۱=۰$$

پاسخ:

$$(۲x-۳)(۲x-۱۷)=۴x^{۲}-۴۰x+۵۱\le ۴x^{۲}-۴۰\lfloor x\rfloor+۵۱=۰$$

بنابراین $\frac{۱۷}{۲}\le x\le\frac{۳}{۲}$ و از آنجا $۸\le\lfloor x\rfloor\le ۱$. داریم

$$x=\frac{\sqrt{۴۰\lfloor x\rfloor-۵۱}}{۲}$$

بنابراین لازم است که داشته باشیم $\left\lfloor\frac{\sqrt{۴۰\lfloor x\rfloor-۵۱}}{۲}\right\rfloor=\lfloor x\rfloor$.

با آزمون $\lfloor x\rfloor\in\{۱,۲,\dots,۸\}$ در این معادله متوجه می‌شویم که $\lfloor x\rfloor$ فقط می‌تواند مقادیر ۲، ۶، ۷ یا ۸ را اختیار کند. بنابراین تنها جواب‌های ممکن برای x عبارتند از

$$\frac{\sqrt{۲۶۹}}{۲},\frac{\sqrt{۲۲۹}}{۲},\frac{\sqrt{۱۸۹}}{۲},\frac{\sqrt{۲۹}}{۲}$$

آزمایش سریع این مقادیر مؤید آن است که همگی جواب‌های قابل قبول هستند.

قضیه ۱. ۴۶ خواص زیر درباره‌ی توابع کف و سقف x برقرارند.

(آ) اگر a و b اعداد صحیح باشند که $b>۰$ و q و r به ترتیب خارج‌قسمت و باقی‌مانده تقسیم a بر b باشند آنگاه $q=\left\lfloor\frac{a}{b}\right\rfloor$ و $r=\{\frac{a}{b}\}\times b$.

(ب) برای هر عدد حقیقی x و هر عدد صحیح n، $\lfloor x+n\rfloor=\lfloor x\rfloor+n$ و $\lceil x+n\rceil=\lceil x\rceil+n$.

(پ) اگر x یک عدد صحیح باشد آنگاه $\lfloor -x\rfloor+\lfloor x\rfloor=۰$؛ اگر x عدد صحیح نباشد $\lfloor -x\rfloor+\lfloor x\rfloor=۱$

(ت) تابع جزءصحیح (کف) غیر نزولی است یعنی برای $x\le y$، $\lfloor x\rfloor\le\lfloor y\rfloor$.

(ث) $\left\lfloor x+\frac{۱}{۲}\right\rfloor$ عدد x را به نزدیک‌ترین عدد صحیح به آن گرد می‌کند.

(ج) $\lfloor x\rfloor+\lfloor y\rfloor\le\lfloor x+y\rfloor\le\lfloor x\rfloor+\lfloor y\rfloor+1$

(چ) برای اعداد حقیقی نامنفی x و y، $\lfloor x\rfloor.\lfloor y\rfloor\le\lfloor xy\rfloor$

(ح) برای هر عدد حقیقی مثبت x و هر عدد صحیح مثبت n، تعداد مضارب مثبت n که از x بیشتر نیست برابر است با $\left\lfloor\frac{x}{n}\right\rfloor$

(خ) برای هر عدد حقیقی x و هر عدد صحیح مثبت n

$$\left\lfloor\frac{\lfloor x\rfloor}{n}\right\rfloor=\left\lfloor\frac{x}{n}\right\rfloor$$

اثبات: اثبات‌های قسمت‌های (آ) تا (ت) ساده است. ما فقط اثبات بخش‌های (ث) تا (خ) را می‌آوریم.

برای (ث) توجه کنید که اگر $\{x\}<\frac{1}{2}$ آنگاه $\lfloor x\rfloor=\lfloor x+\frac{1}{2}\rfloor$ که نزدیک‌ترین عدد صحیح به x است و اگر $\{x\}\ge\frac{1}{2}$ آنگاه $\lceil x\rceil=\lfloor x+\frac{1}{2}\rfloor$ که نزدیک‌ترین عدد صحیح به x است. این یک حربه ساده اما مفید در برنامه‌نویسی کامپیوتر است. برای (ج) می‌نویسیم $x=\lfloor x\rfloor+\{x\}$ و $y=\lfloor y\rfloor+\{y\}$. نتیجه دلخواه معادل با رابطه‌ی

$$0\le\lfloor\{x\}+\{y\}\rfloor\le 1$$

می‌باشد که از $0\le\{x\},\{y\}<1$ واضح است.

برای (چ) دوباره می‌نویسیم $x=\lfloor x\rfloor+\{x\}$ و $y=\lfloor y\rfloor+\{y\}$. $\lfloor x\rfloor,\lfloor y\rfloor,\{x\}$ و $\{y\}$ همگی نامنفی هستند. واضح است که

$$\begin{aligned}\lfloor xy\rfloor&=\lfloor(\lfloor x\rfloor+\{x\})(\lfloor y\rfloor+\{y\})\rfloor\\&=\lfloor\lfloor x\rfloor\lfloor y\rfloor+\lfloor x\rfloor\{y\}+\lfloor y\rfloor\{x\}+\{x\}\{y\}\rfloor\ge\lfloor x\rfloor\lfloor y\rfloor\end{aligned}$$

برای (ح) همه‌ی مضارب $1\times n,2\times n,\ldots,k\times n$ را در نظر می‌گیریم بطوریکه $kn\le x<(k+1)n$؛ یعنی $k\le\frac{x}{n}<k+1$ و نتیجه مطلوب به دست می‌آید.

قسمت (خ) از قسمت (ج) و این که مضارب یک عدد صحیح، صحیح هستند، به دست می‌آید.

علاوه بر اینها قضیه ۱. ۴۶ (ج) را به صورت زیر توسعه می‌دهیم.

مثال ۱. ۶۳. برای اعداد حقیقی x و y ثابت کنید:

$$\lfloor 2x\rfloor+\lfloor 2y\rfloor\ge\lfloor x\rfloor+\lfloor y\rfloor+\lfloor x+y\rfloor$$

اثبات: x و y را به صورت $x=\lfloor x\rfloor+\{x\}$ و $y=\lfloor y\rfloor+\{y\}$ می‌نویسیم. لذا

$$\lfloor ۲x\rfloor+\lfloor ۲y\rfloor=۲\lfloor x\rfloor+\lfloor ۲\{x\}\rfloor+۲\lfloor y\rfloor+\lfloor ۲\{y\}\rfloor$$

و

$$\lfloor x+y\rfloor=\lfloor x\rfloor+\lfloor y\rfloor+\lfloor \{x\}+\{y\}\rfloor$$

کافی است نشان دهیم

$$\lfloor ۲\{x\}\rfloor+\lfloor ۲\{y\}\rfloor\geq\lfloor \{x\}+\{y\}\rfloor$$

به دلیل تقارن می‌توان فرض کرد $\{y\}\geq\{x\}$. با توجه به اینکه $\{x\}$ نامنفی است لذا

$$\lfloor ۲\{x\}\rfloor+\lfloor ۲\{y\}\rfloor\geq\lfloor ۲\{x\}\rfloor\geq\lfloor \{x\}+\{y\}\rfloor$$

مثال ۱. ۶۴. برای عدد صحیح مثبت n نشان دهید.

$$\left\lfloor \sqrt{n}+\frac{۱}{۲}\right\rfloor=\left\lfloor \sqrt{n-\frac{۳}{۴}+\frac{۱}{۲}}\right\rfloor$$

اثبات: فرض کنید

$$\left\lfloor \sqrt{n}+\frac{۱}{۲}\right\rfloor=k \quad \text{و} \quad \left\lfloor \sqrt{n-\frac{۳}{۴}+\frac{۱}{۲}}\right\rfloor=m$$

بنابراین داریم $k\leq\sqrt{n}+\frac{۱}{۲}<k+۱$ یا $k-\frac{۱}{۲}\leq\sqrt{n}<k+\frac{۱}{۲}$. با مجذور کردن طرفین این نامساوی خواهیم داشت

$$k^۲-k+\frac{۱}{۴}\leq n<k^۲+k+\frac{۱}{۴}$$

از آن جا که n یک عدد صحیح است داریم $k^۲-k+۱\leq n\leq k^۲+k$ و به طور مشابه $m\leq\sqrt{n-\frac{۳}{۴}+\frac{۱}{۲}}<m+۱$ که از آن نتیجه می‌شود

$$m^۲-m+\frac{۱}{۴}\leq n-\frac{۳}{۴}<m^۲+m+\frac{۱}{۴}$$

چون n عدد صحیح است، لذا $m^۲-m+۱\leq n\leq m^۲+m$.

با ترکیب دو نتیجه فوق به دست می‌آید $m=k$ که همان نتیجه مطلوب است.

نمودار توابع $y=\lfloor x \rfloor$ و $y=\lceil x \rceil$ توابع پله‌ای هستند. خواص منحصر به فرد آن‌ها این اجازه را به ما می‌دهد که به شرح چند دنباله‌ی ویژه بپردازیم.

مثال ۱. ۶۵. [AIME ۱۹۸۵] چه تعداد از اولین ۱۰۰۰ عدد صحیح مثبت را می‌توان به شکل زیر بیان کرد؟

$$\lfloor 2x \rfloor+\lfloor 4x \rfloor+\lfloor 6x \rfloor+\lfloor 8x \rfloor$$ (x عددی حقیقی است)

پاسخ: تابع f را به صورت زیر تعریف می‌کنیم

$$f(x)=\lfloor 2x \rfloor+\lfloor 4x \rfloor+\lfloor 6x \rfloor+\lfloor 8x \rfloor$$

می‌توان دید که اگر n یک عدد صحیح مثبت باشد آنگاه $f(x+n)=f(x)+20n$. در حالت خاص اگر عدد صحیح k را بتوان به شکل $f(x_0)$ بیان کرد آنگاه برای $n=1,2,3,...$، $k+20n$ را نیز می‌توان به طور مشابه بیان کرد؛ یعنی $k+20n=f(x_0)+20n=f(x_0+n)$. با توجه به این مطلب کافی است به بررسی این موضوع بپردازیم که از اولین ۲۰ عدد صحیح مثبت کدام یک توسط $f(x)$ هنگامی که x در بازه‌ی $[0,1)$ تغییر می‌کند، تولید می‌شود.

مشاهده می‌شود که با افزایش x مقدار $f(x)$ تنها زمانی تغییر می‌کند که $2x, 4x, 6x$ و یا $8x$ به مقدار مشخصی برسند. تغییر در $f(x)$ همواره به یک مقدار جدید و بالاتر خواهد بود. در بازه‌ی $[0,1)$ این تغییرات زمانی اتفاق می‌افتد که x به شکل $\frac{m}{n}$ باشد که در آن $1 \le m \le n$ و $n=2,4,6$ یا ۸. بنابراین ۱۲ کسر به این صورت وجود دارد که به ترتیب صعودی عبارتند از:

$$\frac{1}{8},\frac{1}{6},\frac{1}{4},\frac{1}{3},\frac{3}{8},\frac{1}{2},\frac{5}{8},\frac{2}{3},\frac{3}{4},\frac{5}{6},\frac{7}{8},1$$

پس فقط ۱۲ تا از اولین ۲۰ عدد صحیح را می‌توان به صورت مطرح شده بیان کرد. از آن جا که $50\times20=1000$ لذا $50\times12=600$ عدد صحیح مثبت به شکل مطلوب وجود دارد.

مثال ۱. ۶۶. [کاوس] فرض کنید p و q اعداد صحیح نسبت به هم اول باشند. ثابت کنید

$$\left\lfloor \frac{p}{q} \right\rfloor+\left\lfloor \frac{2p}{q} \right\rfloor+\ldots+\left\lfloor \frac{(q-1)p}{q} \right\rfloor=\frac{(p-1)(q-1)}{2}$$

پاسخ: از $\gcd(p,q)=1$ نتیجه می‌گیریم که $\frac{ip}{q}$ عدد صحیح نیست. از قضیه ۱. ۴۶ (پ) برای $1 \le i \le q-1$ داریم

$$\left\lfloor \frac{ip}{q} \right\rfloor + \left\lfloor \frac{(q-i)p}{q} \right\rfloor = p + \left\lfloor \frac{ip}{q} \right\rfloor + \left\lfloor \frac{-ip}{q} \right\rfloor = p-1$$

بنابراین

$$2\left(\left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \cdots + \left\lfloor \frac{(q-1)p}{q} \right\rfloor\right) =$$
$$= \left(\left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{(q-1)p}{q} \right\rfloor\right) + \cdots + \left(\left\lfloor \frac{(q-1)p}{q} \right\rfloor + \left\lfloor \frac{p}{q} \right\rfloor\right)$$
$$= (p-1)(q-1)$$

که از آن نتیجه مطلوب به دست می‌آید.

نتیجه فوق را می‌توان به عنوان تعداد نقاط شبکه‌ای داخل مثلث محدود به خطوط $y=0$، $x=p$ و $y=\frac{qx}{p}$ نیز تفسیر کرد (یک نقطه در صفحه مختصات یک نقطه شبکه‌ای است اگر دارای مختصات صحیح باشد)

مثال ۱. ۶۷. دنباله‌ی $\{a_n\}_{n=1}^{\infty} = \{2,3,5,6,7,8,10,\ldots\}$ شامل همه‌ی اعداد صحیح مثبت است که مربع کامل نیستند. ثابت کنید:

$$a_n = n + \left\lfloor \sqrt{n} + \frac{1}{2} \right\rfloor$$

اثبات اول: ادعا می‌کنیم

$$\left\lfloor \sqrt{n} + \frac{1}{2} \right\rfloor^2 < n + \left\lfloor \sqrt{n} + \frac{1}{2} \right\rfloor < \left(\left\lfloor \sqrt{n} + \frac{1}{2} \right\rfloor + 1\right)^2 \qquad (\dagger)$$

از روی این ادعا واضح است که در بین اعداد صحیح $n + \left\lfloor \sqrt{n} + \frac{1}{2} \right\rfloor$ دقیقاً $1^2, 2^2, \ldots, \left\lfloor \sqrt{n} + \frac{1}{2} \right\rfloor^2$ مربع کامل وجود دارد که عبارتند از $1^2, 2^2, \ldots, \left\lfloor \sqrt{n} + \frac{1}{2} \right\rfloor^2$. بنابراین عدد

$$n + \left\lfloor \sqrt{n} + \frac{1}{2} \right\rfloor$$

n اُمین عدد در دنباله، پس از پاک کردن همه‌ی اعداد مربع کامل است. یعنی:

$$a_n = n + \left\lfloor \sqrt{n} + \frac{1}{2} \right\rfloor$$

حال ادعای خود را ثابت می‌کنیم. توجه کنید که $\sqrt{n}$ یک عدد صحیح یا یک عدد غیر گویا (گنگ) است بنابراین $\{\sqrt{n}\} \neq \frac{1}{2}$. دو حالت را بررسی می‌کنیم.

در حالت اول فرض می‌کنیم $\{\sqrt{n}\} < \frac{1}{2}$ و $\lfloor \sqrt{n} \rfloor = k$. لذا $k^2 \leq n < (k+\frac{1}{2})^2$ یا $k^2 < n < k^2 + k + \frac{1}{4}$ و از آنجا

$$\left\lfloor \sqrt{n} + \frac{1}{2} \right\rfloor = \lfloor \sqrt{n} \rfloor = k$$

و نامساوی (†) به صورت زیر در می‌آید:

$$k^2 < n + k < (k+1)^2 = k^2 + 2k + 1$$

که واضح است.

در حالت دوم فرض می‌کنیم $\{\sqrt{n}\} > \frac{1}{2}$ و $\lfloor \sqrt{n} \rfloor = k$. لذا $(k+\frac{1}{2})^2 < n < (k+1)^2$ یا $k^2 + k + \frac{1}{4} < n < k^2 + 2k + 1$ و از آنجا

$$\left\lfloor \sqrt{n} + \frac{1}{2} \right\rfloor = \lfloor \sqrt{n} \rfloor + 1 = k + 1$$

و نامساوی (†) به صورت زیر در می‌آید:

$$(k+1)^2 < n + k + 1 < (k+2)^2 = k^2 + 4k + 4$$

که این نیز واضح است.

با ترکیب این دو حالت ما نشان داده‌ایم که ادعایمان همواره صحیح بوده و اثبات‌مان کامل می‌شود.

اثبات دوم مبنای به وجود آمدن شکل بسته a_n را آشکار می‌سازد.

اثبات دوم: دنباله‌ی زیر را در نظر بگیرید

$$\{b_n\}_{n=1}^{\infty} = \{1,1;2,2,2,2;3,3,3,3,3,3,3;\ldots\}$$

می‌توان دید که

$$a_n - b_n = n \quad \text{(برای همه‌ی اعداد صحیح مثبت } n\text{)}$$

واضح است که دقیقاً $(n+1)^2 - n^2 - 1 = 2n$ عدد غیر مربع کامل بین دو عدد مربع کامل متوالی n^2 و $(n+1)^2$ وجود دارد. کافی است نشان دهیم

$$b_n = \left\lfloor \sqrt{n} + \frac{1}{2} \right\rfloor$$

اگر $b_n = k$، آنگاه b_n داخل k اُمین گروه بوده و بعد از حداقل $k-1$ گروه شامل $2(k-1)+\ldots+4+2$ عضو می‌آید. با در نظر گرفتن این حقیقت که $n-1$ عضو قبل از b_n آمده است نتیجه می‌گیریم

$$2+4+\cdots+2(b_n-1)\le n-1$$

علاوه بر آن b_n بزرگ‌ترین عدد صحیح است که این نامساوی را برآورده می‌کند. بنابراین b_n بزرگ‌ترین عدد صحیح است که در نامساوی $b_n(b_n-1)\le n-1$ صدق می‌کند به عبارت دیگر از مثال ۱. ۶۴ خواهیم داشت:

$$b_n=\left\lfloor\frac{1+\sqrt{4n-3}}{2}\right\rfloor=\left\lfloor\sqrt{n-\frac{3}{4}}+\frac{1}{2}\right\rfloor=\left\lfloor\sqrt{n}+\frac{1}{2}\right\rfloor$$

قضیه ۱. ۴۷ [قضیه بیتی] فرض کنید α و β دو عدد حقیقی گنگ مثبت باشند به طوری که

$$\frac{1}{\alpha}+\frac{1}{\beta}=1$$

مجموعه‌های

$$\{a_n\}_{n=1}^{\infty}=\{\lfloor\alpha\rfloor,\lfloor 2\alpha\rfloor,\lfloor 3\alpha\rfloor,\ldots\}\ \text{و}\ \{b_n\}_{n=1}^{\infty}=\{\lfloor\beta\rfloor,\lfloor 2\beta\rfloor,\lfloor 3\beta\rfloor,\ldots\}$$

هر کدام قسمتی از مجموعه‌ی اعداد صحیح مثبت را تشکیل می‌دهند. به عبارت دیگر $\{b_n\}_{n=1}^{\infty}$ و $\{a_n\}_{n=1}^{\infty}$ مجموعه‌های جدا ازهم هستند که اجتماعشان برابر مجموعه‌ی همه‌ی اعداد صحیح مثبت است.

اثبات: در ابتدا نشان می‌دهیم که آن‌ها جدا از هم هستند. این کار را به طور غیر مستقیم و با برهان خلف انجام می‌دهیم؛ یعنی فرض می‌کنیم اندیس‌های i و j وجود دارند به طوری که $k=a_i=b_j=\lfloor i\alpha\rfloor=\lfloor j\beta\rfloor$. از آنجا که $i\alpha$ و $j\beta$ هر دو گنگ هستند در نتیجه

$$k<i\alpha<k+1\ \text{و}\ k<j\beta<k+1$$

و یا

$$\frac{i}{k+1}<\frac{1}{\alpha}<\frac{i}{k}\ \text{و}\ \frac{j}{k+1}<\frac{1}{\beta}<\frac{j}{k}$$

و با جمع کردن این دو نامساوی با هم خواهیم داشت

$$\frac{i+j}{k+1}<\frac{1}{\alpha}+\frac{1}{\beta}=1<\frac{i+j}{k}$$

و یا $k<i+j<k+1$ که غیر ممکن است. بنابراین فرض ما غلط بوده و این دو دنباله اشتراکی ندارند. در مرحله‌ی بعد ثابت می‌کنیم هر عدد صحیح مثبت در یکی از این دو دنباله ظاهر می‌شود. باز هم به طور غیر مستقیم و با فرض این که عدد صحیح مثبت k وجود دارد که در این دو دنباله ظاهر نمی‌شود شروع می‌کنیم. به این ترتیب اندیس‌های i و j وجود دارند به طوری که

$$i\alpha<k,\quad (i+1)\alpha>k+1,\quad j\beta<k,\quad (j+1)\beta>k+1$$

یا

$$\frac{i}{k}<\frac{1}{\alpha}<\frac{i+1}{k+1}\ \text{و}\ \frac{j}{k}<\frac{1}{\beta}<\frac{j+1}{k+1}$$

با جمع کردن این دو نامساوی با هم خواهیم داشت:

$$\frac{i+j}{k}<\frac{1}{\alpha}+\frac{1}{\beta}=1<\frac{i+j+2}{k+1}$$

در نتیجه $k>i+j$، $k+1<i+j+2$ و یا $i+j<k<i+j+1$ که غیر ممکن است. لذا فرض ما غلط بوده و هر عدد صحیح مثبت دقیقاً در یکی از دو دنباله ظاهر می‌شود.

مثال ۱. ۶۸ (الف). [USAMO ۱۹۸۱] برای عدد مثبت x ثابت کنید:

$$\lfloor x\rfloor+\frac{\lfloor 2x\rfloor}{2}+\frac{\lfloor 3x\rfloor}{3}+\cdots+\frac{\lfloor nx\rfloor}{n}\le\lfloor nx\rfloor$$

البته ما نتیجه کلی‌تری داریم. از قضیه ۱. ۴۶ (ج)، مثال ۱. ۶۸ (الف) حالت خاصی از مثال ۱. ۶۸ (ب) است که با قرار دادن $a_i=-\lfloor ix\rfloor$ به دست می‌آید.

مثال ۱. ۶۸ (ب). [APMO ۱۹۹۹] فرض کنید $a_1,a_2,\ldots$ دنباله‌ای از اعداد حقیقی باشند که

$$a_{i+j}\le a_i+a_j\quad (\text{برای همه‌ی } i,j=1,2,\ldots)$$

ثابت کنید برای همه‌ی اعداد صحیح مثبت n

$$a_1+\frac{a_2}{2}+\frac{a_3}{3}+\cdots+\frac{a_n}{n}\ge a_n$$

اثبات اول: از استقرای قوی استفاده می‌کنیم. حالات اولیه برای $n=1$ و $n=2$ واضح هستند. فرض می‌کنیم حکم برای $n \le k$ که k یک عدد صحیح مثبت دلخواه و بزرگتر یا مساوی۲ است برقرار باشد؛ یعنی

$$a_1 \ge a_1$$

$$a_1 + \frac{a_2}{2} \ge a_2$$

$$\vdots$$

$$a_1 + \frac{a_2}{2} + \cdots + \frac{a_k}{k} \ge a_k$$

با جمع کردن همه‌ی این نامعادلات خواهیم داشت:

$$ka_1 + (k-1)\frac{a_2}{2} + \cdots + \frac{a_k}{k} \ge a_1 + a_2 + \cdots + a_k$$

با اضافه کردن $(a_1 + a_2 + \cdots + a_k)$ به طرفین نامساوی اخیر به رابطه‌ی زیر می‌رسیم

$$(k+1)(a_1 + \frac{a_2}{2} + \cdots + \frac{a_k}{k}) \ge (a_1 + a_k) + (a_2 + a_{k-1}) + \cdots + (a_k + a_1)$$
$$\ge k a_{k+1}$$

با تقسیم کردن طرفین رابطه فوق بر $(k+1)$ خواهیم داشت:

$$a_1 + \frac{a_2}{2} + \cdots + \frac{a_k}{k} \ge \frac{k a_{k+1}}{k+1}$$

و یا

$$a_1 + \frac{a_2}{2} + \cdots + \frac{a_k}{k} + \frac{a_{k+1}}{k+1} \ge a_{k+1}$$

و استقرا به این ترتیب کامل شده، حکم اثبات می‌گردد.

اثبات دوم: می‌توان شرط موردنظر را با استقرا به شرط زیر بسط داد.

$$a_{i_1 + i_2 + \cdots + i_k} \le a_{i_1} + a_{i_2} + \cdots + a_{i_k}$$

برای اثبات از مباحث ترکیبات بهره می‌جوییم.

یک جایگشت، تغییر جایگاه اعضا در یک مجموعه است. به طور دقیق‌تر، اگر S یک مجموعه باشد، یک جایگشت S نگاشتی از S به خودش است که آن را با تابع یک به یک π نشان داده می‌شود. اگر $S=\{x_1,x_2,\ldots,x_n\}$ یک مجموعه‌ی متناهی باشد یک جایگشت π از S را با $(y_1,y_2,\ldots,y_n)$ نشان می‌دهیم که $y_x=\pi(x_k)$.

k تایی مرتب $\{x_{i1},x_{i2},\ldots,x_{ik}\}$ یک k-دور π است اگر $\pi(x_{i1})=x_{i2}$، $\pi(x_{i2})=x_{i3}$، $\ldots,\pi(x_{ik})=x_{i1}$. فرض کنید S_n مجموعه‌ی جایگشت‌های n شیء باشد. برای یک عضو π در S_n، $f(\pi,k)$ را برابر تعداد k-دورها در π تعریف می‌کنیم. واضح است که

$$1\times f(\pi,1)+2\times f(\pi,2)+\ldots+n\times f(\pi,n)=n$$

زیرا هر دو طرف تعداد اعضای موجود در جایگشت π را نشان می‌دهند. در ضمن $\sum_{\pi\in S_n} f(\pi,k)$ تعداد کل k - دورها در تمام جایگشت‌های روی n شیء را نشان می‌دهد که برابر است با

$$\binom{n}{k}(k-1)!(n-k)!=\frac{n!}{k}$$

به عبارت دیگر

$$\sum_{\pi\in S_n} f(\pi,k)=\binom{n}{k}(k-1)!(n-k)!=\frac{n!}{k} \qquad (*)$$

این رابطه از آنجا ناشی می‌شود که

الف) به $\binom{n}{k}$ طریق می‌توان k عضو را برای تشکیل یک k-دور انتخاب کرد.

ب) به $(k-1)!$ طریق می‌توان یک k-دور را با استفاده از k عضو تشکیل داد.

پ) به $(n-k)!$ طریق می‌توان $n-k$ عضو انتخاب نشده را برای تکمیل جایگشت همه‌ی n عضو مرتب کرد. بنابراین از (*) و با توجه به اینکه دقیقاً $n!$ عضو در S_n وجود دارد (تعداد جایگشت‌های n شی، $n!$ است)، داریم

$$\begin{aligned} a_1+\frac{a_2}{2}+\frac{a_3}{3}+\ldots+\frac{a_n}{n} &= \frac{1}{n!}\sum_{\pi\in S_n}[f(\pi,1)a_1+f(\pi,2)a_2+\ldots+f(\pi,n)a_n] \\ &\geq \frac{1}{n!}\sum_{\pi\in S_n} 1\times f(\pi,1)+2\times f(\pi,2)+\ldots+n\times f(\pi,n) \\ &= \frac{1}{n!}\sum_{\pi\in S_n} a_n = a_n \end{aligned}$$

چنانچه در مثال‌های ۱. ۶۸ (الف) و ۱. ۶۸ (ب) نشان داده شده بسیاری از مسائل جذاب و پیکارجوی توابع کف و سقف، ارتباط نزدیکی با خواص تابعی آن‌ها دارند. این بخش را با معرفی اتحاد معروف هرمیت به پایان می‌بریم.

قضیه ۱. ۴۸. [اتحاد هرمیت] اگر x یک عدد حقیقی و n یک عدد صحیح مثبت باشند آنگاه

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \left\lfloor x + \frac{2}{n} \right\rfloor + \ldots + \left\lfloor x + \frac{n-1}{n} \right\rfloor = \lfloor nx \rfloor$$

اثبات: اگر x عدد صحیح باشد، حکم به وضوح برقرار است. فرض می‌کنیم x عدد صحیح نباشد یعنی $0 < \{x\} < 1$ بنابراین $1 \le i \le n-1$ وجود دارد که

$$\{x\} + \frac{i-1}{n} < 1 \text{ و } \{x\} + \frac{i}{n} \ge 1 \qquad (*)$$

به عبارت دیگر

$$\frac{n-i}{n} \le \{x\} < \frac{n-i+1}{n} \qquad (**)$$

از (*) داریم

$$\lfloor x \rfloor = \left\lfloor x + \frac{1}{n} \right\rfloor = \cdots = \left\lfloor x + \frac{i-1}{n} \right\rfloor$$

و

$$\left\lfloor x + \frac{i}{n} \right\rfloor = \cdots = \left\lfloor x + \frac{n-1}{n} \right\rfloor = \lfloor x \rfloor + 1$$

و بنابراین

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \left\lfloor x + \frac{2}{n} \right\rfloor + \cdots + \left\lfloor x + \frac{n-1}{n} \right\rfloor$$
$$= i\lfloor x \rfloor + (n-i)(\lfloor x \rfloor + 1) = n\lfloor x \rfloor + n - i$$

از طرف دیگر از (**) به دست می‌آید که

$$n\lfloor x \rfloor + n - i \le n\lfloor x \rfloor + n\{x\} = nx < n\lfloor x \rfloor + n - i + 1$$

لذا $\lfloor nx \rfloor = n\lfloor x \rfloor + n - i$.

با ترکیب این دو نتیجه مشاهده می‌شود که

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \left\lfloor x + \frac{2}{n} \right\rfloor + \ldots + \left\lfloor x + \frac{n-1}{n} \right\rfloor = n\lfloor x \rfloor + n - i = \lfloor nx \rfloor$$

مثال ۱. ۶۹ [AIME ۱۹۹۱] فرض کنید r یک عدد حقیقی باشد که

$$\left\lfloor r + \frac{19}{100} \right\rfloor + \left\lfloor r + \frac{20}{100} \right\rfloor + \cdots + \left\lfloor r + \frac{91}{100} \right\rfloor = 546$$

مقدار $\lfloor 100r \rfloor$ را پیدا کنید.

پاسخ: مجموع داده شده $73 = 1 + 19 - 91$ عضو دارد که هر کدام یا برابر $\lfloor r \rfloor$ است یا برابر $\lfloor r \rfloor + 1$. اما $546 < 73 \times 8 < 73 \times 7$ و بنابراین $\lfloor r \rfloor = 7$. از آن جا که $546 = 73 \times 7 + 35$ است ۳۸ عضو اول مقدار ۷ و ۳۵ عضو دیگر مقدار ۸ خواهند داشت. یعنی:

$$\left\lfloor r + \frac{56}{100} \right\rfloor = 7 \quad \text{و} \quad \left\lfloor r + \frac{57}{100} \right\rfloor = 8$$

در نتیجه $7/44 < r \leq 7/43$ و بنابراین $\lfloor 100r \rfloor = 743$

مثال ۱. ۷۰ [IMO ۱۹۶۸] فرض کنید x یک عدد حقیقی باشد. ثابت کنید:

$$\sum_{k=0}^{\infty} \left\lfloor \frac{x + 2^k}{2^{k+1}} \right\rfloor = \lfloor x \rfloor$$

پاسخ: با قرار دادن $n = 2$ در اتحاد هرمیت خواهیم داشت

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{2} \right\rfloor = \lfloor 2x \rfloor$$

یا

$$\left\lfloor x + \frac{1}{2} \right\rfloor = \lfloor 2x \rfloor - \lfloor x \rfloor$$

با تکرار این عمل خواهیم داشت

$$\sum_{k=0}^{\infty} \left\lfloor \frac{x + 2}{2^{k+1}} \right\rfloor = \sum_{k=0}^{\infty} \left\lfloor \frac{x}{2^{k+1}} + \frac{1}{2} \right\rfloor = \sum_{k=0}^{\infty} \left(\left\lfloor \frac{x}{2^k} \right\rfloor - \left\lfloor \frac{x}{2^{k+1}} \right\rfloor \right) = \lfloor x \rfloor$$

تابع لژاندر

از قضیه ۱. ۴۶ (ح) استفاده کرده و چند نتیجه جالب به دست می‌آوریم.

فرض کنید p یک عدد اول باشد. برای هر عدد صحیح مثبت n، توان p در تجزیه $n!$ به عوامل اول را با $e_p(n)$ نشان می‌دهیم. تابع حسابی e_p تابع لژاندر عدد اول p نامیده می‌شود. قضیه زیر رابطه‌ای برای محاسبه‌ی $e_p(n)$ بدست می‌دهد.

قضیه ۱. ۴۹ [فرمول لژاندر] برای هر عدد اول p و هر عدد صحیح مثبت n

$$e_p(n)=\sum_{i\geq 1}\left\lfloor\frac{n}{p^i}\right\rfloor=\left\lfloor\frac{n}{p}\right\rfloor+\left\lfloor\frac{n}{p^2}\right\rfloor+\left\lfloor\frac{n}{p^3}\right\rfloor+\dots$$

لازم به توجه است که این مجموع، متناهی است زیرا عدد به اندازه کافی بزرگ m وجود دارد که $n<p^{m+1}$ و $\left\lfloor\frac{n}{p^{m+1}}\right\rfloor=0$. فرض کنید m کوچک‌ترین عدد صحیح مثبت باشد که $n<p^{m+1}$ یعنی $m=\left\lfloor\frac{\ln n}{\ln p}\right\rfloor$. کافی است نشان دهیم

$$e_p(n)=\left\lfloor\frac{n}{p}\right\rfloor+\left\lfloor\frac{n}{p^2}\right\rfloor+\dots+\left\lfloor\frac{n}{p^m}\right\rfloor$$

در این جا دو اثبات نزدیک به هم ارائه می‌کنیم. یکی به زبان تئوری اعداد و دیگری به زبان ترکیبات است.

اثبات اول: برای $n<p$ واضح است که $e_p(n)=0$. اگر $n\geq p$ باشد به منظور تعیین $e_p(n)$، فقط لازم است تا مضارب p در $n!=1\times 2\times\dots\times n$ را مورد بررسی قرار دهیم؛ یعنی $(1\times p)(2\times p)\cdots(k\times p)=p^k k!$ که از قضیه ۱. ۴۶ (ج) $k=\left\lfloor\frac{n}{p}\right\rfloor$. بنابراین

$$e_p(n)=\left\lfloor\frac{n}{p}\right\rfloor+e_p\left(\left\lfloor\frac{n}{p}\right\rfloor\right)$$

با قرار دادن $\left\lfloor\frac{n}{p}\right\rfloor$ به جای n و استفاده از قضیه ۱. ۴۶ (خ) خواهیم داشت

$$e_p\left(\left\lfloor \frac{n}{p} \right\rfloor\right)=\left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p} \right\rfloor+e_p\left(\left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p} \right\rfloor\right)=\left\lfloor \frac{n}{p^2} \right\rfloor+e_p\left(\left\lfloor \frac{n}{p^2} \right\rfloor\right)$$

با تکرار این روال به نتایج زیر می‌رسیم

$$e_p\left(\left\lfloor \frac{n}{p^2} \right\rfloor\right)=\left\lfloor \frac{n}{p^3} \right\rfloor+e_p\left(\left\lfloor \frac{n}{p^3} \right\rfloor\right)$$

$$e_p\left(\left\lfloor \frac{n}{p^{m-1}} \right\rfloor\right)=\left\lfloor \frac{n}{p^m} \right\rfloor+e_p\left(\left\lfloor \frac{n}{p^m} \right\rfloor\right)=\left\lfloor \frac{n}{p^m} \right\rfloor$$

و با کنار هم قرار دادن نتایج فوق به نتیجه مطلوب خواهیم رسید.

اثبات دوم: برای هر عدد صحیح مثبت i، t_i را چنان تعریف می‌کنیم که $p^{t_i} \parallel i$. چون p اول است داریم $p^{t_1+t_2+\cdots+t_n} \parallel n!$ یا $t=t_{n!}=t_1+t_2+\cdots+t_n$. از طرف دیگر $\left\lfloor \frac{n}{p^k} \right\rfloor$ همه‌ی مضارب p^k که کوچک‌تر یا مساوی n هستند را دقیقاً یک بار می‌شمارد. بنابراین عدد $i=p^{t_i}\times a$ (a و p نسبت به هم اول هستند) t_i بار در مجموع زیر شمرده می‌شود

$$\left\lfloor \frac{n}{p} \right\rfloor+\left\lfloor \frac{n}{p^2} \right\rfloor+\cdots+\left\lfloor \frac{n}{p^m} \right\rfloor$$

که آن‌ها عبارتند از $\left\lfloor \frac{n}{p} \right\rfloor, \left\lfloor \frac{n}{p^2} \right\rfloor, \ldots, \left\lfloor \frac{n}{p^i} \right\rfloor$. بنابراین برای هر $1 \le i \le n$، مقدار t_i در هر دو عبارت

$$\left\lfloor \frac{n}{p} \right\rfloor+\left\lfloor \frac{n}{p^2} \right\rfloor+\cdots+\left\lfloor \frac{n}{p^m} \right\rfloor$$

و

$$t_1+t_2+\cdots+t_n$$

وجود دارد. لذا

$$t=t_1+t_2+\cdots+t_n=\left\lfloor \frac{n}{p} \right\rfloor+\left\lfloor \frac{n}{p^2} \right\rfloor+\cdots+\left\lfloor \frac{n}{p^m} \right\rfloor$$

با یک بیان شکیل‌تر، ماتریس $\mathbf{M}=(x_{i,j})$ با m سطر و n ستون را در نظر بگیرید که m کوچک‌ترین عدد صحیح است که $p^{m+1}>n$. با توجه به تعریف زیر

$$x_{i,j}=\begin{cases}1 & \text{اگر } p^i,j \text{ را بشمارد}\\ 0 & \text{در غیر اینصورت}\end{cases}$$

تعداد ۱ ها در jاُمین ستون ماتریس M t_j است یعنی مجموع عناصر هر ستون M برابر $t_1,t_2,\ldots,t_n$ است. بنابراین جمع همه‌ی عناصر M t است. از طرف دیگر تعداد ۱ ها در i اُمین سطر تعداد همه‌ی مضارب p^i را نشان می‌دهد. در نتیجه مجموع عناصر سطر i برابر $\left\lfloor \frac{n}{p^i} \right\rfloor$ بوده و جمع همه‌ی عناصر Mبرابر $\sum_{i=1}^{m}\left\lfloor \frac{n}{p^i} \right\rfloor$ نیز می‌باشد و لذا

$$t=\left\lfloor \frac{n}{p} \right\rfloor+\left\lfloor \frac{n}{p^2} \right\rfloor+\cdots+\left\lfloor \frac{n}{p^m} \right\rfloor$$

مثال ۱. ۱۱. فرض کنید s و t اعداد صحیح مثبت باشند که

$$7^s \parallel 400! \quad \text{و} \quad 3^t \parallel (((3!)!)!)!$$

$s+t$ را محاسبه کنید.

پاسخ: جواب ۴۲۲ است.

توجه کنید که $(((3!)!)!)=(6!)!=720!$. با بکارگیری فرمول لژاندر داریم

$$s=e_7(400)=\left\lfloor \frac{400}{7} \right\rfloor+\left\lfloor \frac{400}{7^2} \right\rfloor+\left\lfloor \frac{400}{7^3} \right\rfloor=57+8+1=66$$

$$t=e_3(720)=\left\lfloor \frac{720}{3} \right\rfloor+\left\lfloor \frac{720}{3^2} \right\rfloor+\left\lfloor \frac{720}{3^3} \right\rfloor+\left\lfloor \frac{720}{3^4} \right\rfloor+\left\lfloor \frac{720}{3^5} \right\rfloor$$
$$=240+80+26+8+2=356$$

و بنابراین $s+t=356+66=422$

مثال ۱. ۱۲. $2005!$ در مبنای ۱۰ به m صفر ختم می‌شود. m را بیابید.

پاسخ: حکم معادل این است که m را چنان پیدا کنیم که $10^m \| 2005!$. از آن جا که $10^m = 2^m \times 5^m$، داریم $m = \min(e_2(2005), e_5(2005))$ و چون $2 < 5$ لذا

$$m = e_5(2005) = \left\lfloor \frac{2005}{5} \right\rfloor + \left\lfloor \frac{2005}{25} \right\rfloor + \left\lfloor \frac{2005}{125} \right\rfloor + \left\lfloor \frac{2005}{625} \right\rfloor = 500$$

و جواب ۵۰۰ است.

مثال ۱. ۱۳. [HMMT 2003] کوچک‌ترین عدد n را چنان بیابید که $n!$ به ۲۹۰ صفر ختم شود.

پاسخ: همان طور که در پاسخ مثال ۱. ۷۲. نشان داده شد برای حل این مثال لازم است کوچک‌ترین n را چنان پیدا کنیم که

$$290 = e_5(n) = \left\lfloor \frac{n}{5} \right\rfloor + \left\lfloor \frac{n}{5^2} \right\rfloor + \left\lfloor \frac{n}{5^3} \right\rfloor + \ldots$$

که تقریباً یک سری هندسی است (با در نظر نگرفتن تابع جزءصحیح) و مجموع آن به طور تقریبی با $\frac{n/5}{1-1/5}$ نشان داده می‌شود. با حل

$$290 \approx \frac{\frac{n}{5}}{1-\frac{1}{5}}$$

$n = 1160$ و $e_5(1160) = 288$ خواهند بود. اگر ۱۰ تا به مقدار $n = 1160$ اضافه شود دو عامل ۵ دیگر(از ۱۱۶۵ و ۱۱۷۰) نیز به وجود خواهد آمد. لذا جواب ۱۱۷۰ است.

مثال ۱. ۱۴. m و n اعداد صحیح مثبت هستند. ثابت کنید:

(۱) $(mn)!, m! \times (n!)^m$ را می‌شمارد.

(۲) $(2m)!(2n)!, m!n!(m+n)!$ را می‌شمارد.

اثبات: روش متداولی را برای اثبات بکار می‌گیریم:

(۱) فرض کنید p یک عدد اول بوده و x و y اعداد صحیح نامنفی باشند که $p^x \| m! \times (n!)^m$ و $p^y \| (mn)!$. کافی است نشان دهیم $x \le y$. با توجه به اینکه $x = e_p(m) + me_p(n)$ و $y = e_p(mn)$ لذا کافی است نشان دهیم:

$$\sum_{i=1}^{\infty}\left\lfloor\frac{mn}{p^i}\right\rfloor\geq\sum_{i=1}^{\infty}\left\lfloor\frac{m}{p^i}\right\rfloor+m\sum_{i=1}^{\infty}\left\lfloor\frac{n}{p^i}\right\rfloor$$

اگر $p>n$، عبارت دوم در مجموع سمت راست صفر است و نامساوی به وضوح برقرار است. فرض می‌کنیم $p\leq n$. s را عدد صحیح مثبتی می‌گیریم که $p^s\leq n<p^{s+1}$. از قضیه ۱. ۴۶ (چ) داریم

$$\begin{aligned}\sum_{i=1}^{\infty}\left\lfloor\frac{mn}{p^i}\right\rfloor&=\sum_{i=1}^{s}\left\lfloor m\times\frac{n}{p^i}\right\rfloor+\sum_{i=1}^{\infty}\left\lfloor\frac{m}{p^i}\cdot\frac{n}{p^s}\right\rfloor\\&\geq m\sum_{i=1}^{s}\left\lfloor\frac{n}{p^i}\right\rfloor+\sum_{i=1}^{\infty}\left\lfloor\frac{m}{p^i}\right\rfloor\left\lfloor\frac{n}{p^s}\right\rfloor\\&\geq m\sum_{i=1}^{\infty}\left\lfloor\frac{n}{p^i}\right\rfloor+\sum_{i=1}^{\infty}\left\lfloor\frac{m}{p^i}\right\rfloor\end{aligned}$$

که همان نتیجه دلخواه است.

(۲) اثبات این قسمت بسیار شبیه اثبات قسمت (۱) است. آن را به خواننده می‌سپاریم.

توجه: می‌توان برای این حکم‌ها اثبات‌های ترکیباتی نیز ارائه کرد. به طور مثال

$$\frac{(mn)!}{m!(n!)^m}$$

تعداد طرق تقسیم mn نفر به m گروه n نفری است که قسمت (۱) را اثبات می‌کند.

مثال ۱. ۵۵. فرض کنید k و n اعداد صحیح مثبت باشند. ثابت کنید:

$$(k!)^{k^n+k^{n-1}+\cdots+k+1}\mid(k^{n+1})!$$

اثبات: برای هر i با شرط $0\leq i\leq n$، با قراردادن $(n,m)=(k,k^j)$ در مثال ۱. ۷۴ (۱) خواهیم داشت

$$k!\mid k!\,,\ k!(k!)^k\mid(k^2)!\,,\ (k^2)!(k!)^{k^2}\mid(k^3)!\,,\ \ldots,\ (k^n)!(k!)^{k^n}\mid(k^{n+1})!$$

با ضرب این روابط در هم به رابطه‌ی زیر می‌رسیم

$$k!k!(k^2)!(k^3)!\cdots(k^n)!k!^{k+k^2+\cdots+k^n}\mid k!(k^2)!(k^3)!\cdots(k^{n+1})!$$

که از آن می‌توان حکم را نتیجه گرفت.

مثال ۱.۱۶. فرض کنید $n>2$ یک عدد مرکب باشد. ثابت کنید همه‌ی اعضای دنباله زیر بر n بخش‌پذیر نیستند.

$$\binom{n}{1},\binom{n}{2},\ldots,\binom{n}{n-1}$$

اثبات: فرض کنید p یک عامل اول n و s عدد صحیحی باشد که $p^s \le n < p^{s+1}$. نشان می‌دهیم که

$$n \nmid \binom{n}{p^s} = \frac{n!}{(p^s)!(n-p^s)!}$$

از آن جا که $p \mid n$، کافی است نشان دهیم که $p \nmid \binom{n}{p^s}$. فرض کنید $p^k \parallel \binom{n}{p^s}$ آنگاه

$$k = e_p(n) - e_p(p^s) - e_p(n-p^s)$$

کافی است نشان دهیم $k=0$. از فرمول لژاندر داریم

$$\begin{aligned} k &= \sum_{i\ge 1}\left\lfloor \frac{n}{p^i}\right\rfloor - \sum_{i\ge 1}\left\lfloor \frac{p^s}{p^i}\right\rfloor - \sum_{i\ge 1}\left\lfloor \frac{n-p^s}{p^i}\right\rfloor \\ &= \sum_{i=1}^{s}\left\lfloor \frac{n}{p^i}\right\rfloor - \sum_{i=1}^{s}\left\lfloor \frac{p^s}{p^i}\right\rfloor - \sum_{i=1}^{s}\left\lfloor \frac{n-p^s}{p^i}\right\rfloor \\ &= \sum_{i=1}^{s}\left\lfloor \frac{n}{p^i}\right\rfloor - \sum_{i=1}^{s}\left\lfloor \frac{p^s}{p^i}\right\rfloor - \sum_{i=1}^{s}\left\lfloor \frac{n}{p^i}\right\rfloor + \sum_{i=1}^{s}\left\lfloor \frac{p^s}{p^i}\right\rfloor = 0 \end{aligned}$$

تساوی اخیر از آن جا ناشی می‌شود که برای هر $1\le i\le s$، $\frac{p^s}{p^i}$ عدد صحیح است.

فرمول لژاندر ابزار مهمی در تئوری اعداد ترکیباتی است. به کمک آن دو قضیه مهم لوکاس و کامر پایه‌گذاری شده است.

اعداد فرما

در تلاش برای یافتن همه‌ی اعداد اول به شکل $۲^m + ۱$، فرما متوجه شد که m باید توانی از ۲ باشد. اگر m برابر $k \times h$ باشد که k یک عدد فرد بزرگ‌تر از ۱ است آنگاه

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

و بنابراین $۲^m + ۱$ عدد اول نخواهد بود.

اعداد صحیح $f_n = ۲^{۲^n} + ۱ \; (n \geq ۰)$، *اعداد فرما* نامیده می‌شوند. چند عدد فرمای اولیه عبارتند از:

$$f_۰ = ۳ , f_۱ = ۵ , f_۲ = ۱۷ , f_۳ = ۲۵۷ , f_۴ = ۶۵۵۳۷ , f_۵ = ۴۲۹۴۹۶۷۲۹۷$$

بعد از بررسی ۵ عدد نخستین که همگی اول هستند، فرما حدس زد که f_n برای همه‌ی مقادیر n اول است. اما اویلر ثابت کرد که $۶۴۱ | f_۵$. استلال او بدین صورت بود:

$$\begin{aligned} f_۵ &= ۲^{۳۲} + ۱ = ۲^{۲۸}(۵^۴ + ۲^۴) - (۵ \times ۲^۷)^۴ + ۱ = ۲^{۲۸} \times ۶۴۱ - (۶۴ \cdot ۲^۴ - ۱) \\ &= ۶۴۱ \times (۲^{۲۸} - ۶۳۹ \times (۶۴ \cdot ۲^۲ + ۱)) \end{aligned}$$

هنوز مشخص نیست که آیا در بین اعداد فرما بی‌نهایت عدد اول (اعداد اول فرما) وجود دارد یا نه؟ پاسخ این سؤال حائز اهمیت است زیرا گاوس اثبات کرد که یک چند ضلعی منتظم $Q_۱Q_۲ \ldots Q_n$ را می‌توان با خطکش و پرگار رسم کرد اگر و فقط اگر $n = ۲^h p_۰ \ldots p_k$ که $p_۰ = ۱ , k \geq ۰$ و $p_۱ , \ldots , p_k$ اعداد اول فرمای متمایز هستند. گاوس اولین نفری بود که چنین چند ضلعی را برای $n = ۱۷$ رسم کرد. در عین حال هنوز مشخص نشده است که آیا در بین اعداد فرما، بی‌نهایت عدد مرکب وجود دارد یا خیر؟ (یک نکته خوب این است که حداقل جواب یکی از این دو سؤال باید مثبت باشد ☺)

مثال ۱. ۱۱. برای اعداد صحیح مثبت m و n که $m > n$ است $f_m - ۲ , f_n$ را می‌شمارد.

اثبات: با بکار بردن متوالی رابطه تفاضل مربعات $a^۲ - b^۲ = (a-b)(a+b)$، می‌توان به سادگی نشان داد که

$$f_m - ۲ = f_{m-۱} f_{m-۲} \cdots f_۱ f_۰$$

و از آن حکم مطلوب به دست می‌آید.

مثال ۱. ۱۲. برای اعداد صحیح مثبت و متمایز m و n اعداد فرمای f_m و f_n نسبت به هم اول هستند.

اثبات: از مثال قبلی داریم: $\gcd(f_m, f_n) = \gcd(f_n, ۲) = ۱$
این نتیجه حالت خاصی از مثال ۱. ۲۲ نیز هست.

مثال ۱. ۷۹. ثابت کنید برای همه‌ی اعداد صحیح مثبت n، عدد فرمای f_n، $۲^{f_n} - ۲$ را می‌شمارد.

اثبات:

$$۲^{f_n} - ۲ = ۲ \times (۲^{۲^{۲^n}} - ۱) = ۲[(۲^{۲^n})^{۲^{۲^n - n}} - ۱]$$

واضح است که $۲^{۲^n - n}$ زوج است. برای یک عدد صحیح مثبت زوج $۲m$، $x^{۲m} - ۱$ بر $x + ۱$ بخش‌پذیر است بنابراین $x + ۱$، $x^{۲^{۲^n - n}}$ را می‌شمارد. قرار دادن $x = ۲^{۲^n}$ منجر به نتیجه مطلوب می‌شود.

مثال ۱. ۷۹ نشان می‌دهد که (پیمانه f_n) $۲^{f_n} \equiv ۲$ که مثال نقض دیگری برای عکس قضیه کوچک فرما است. به عبارت دیگر (پیمانه $f_۵$) $۲^{f_۵} \equiv ۲$ اما $f_۵$ عدد اول نیست.

اعداد مرسن

اعداد صحیح $M_n = ۲^n - ۱ (n \geq ۱)$ *اعداد مرسن* نامیده می‌شوند. واضح است که اگر n مرکب باشد، M_n نیز مرکب است. بنابراین M_k اول است اگر k اول باشد. علاوه بر این اگر $n = ab$ که a و b اعداد صحیح بزرگ‌تر از ۱ هستند، آنگاه M_a و M_b هر دو M_n را می‌شمارند. اما اعداد اول n وجود دارند که به ازای آن‌ها M_n مرکب است. برای مثال $M_{۲۳} | ۴۷$، $M_{۸۳} | ۱۶۷$، $M_{۱۰۳} | ۲۶۳$، ...

قضیه ۱. ۵۰. اگر p یک عدد اول فرد و q یک عامل اول M_p باشد آنگاه $q = ۲kp + ۱$ (برای عدد صحیح k)

اثبات: از هم‌نهشتی (پیمانه q) $۲^p \equiv ۱$ و اول بودن p با استفاده از قضیه ۱. ۳۰ نتیجه می‌گیریم که p کوچک‌ترین عدد صحیح مثبت است که این خاصیت را دارد. با استفاده از قضیه کوچک فرما داریم (پیمانه q) $۲^{q-۱} \equiv ۱$ بنابراین از قضیه ۱. ۳۰، $p | q - ۱$. اما $q - ۱$ یک عدد صحیح زوج است و لذا $q - ۱ = ۲kp$ و از آن جا حکم اثبات می‌شود.

اعداد تام (کامل)

عدد صحیح $n \geq ۲$ تام نامیده می‌شود اگر مجموع مقسوم‌علیه‌های [مثبت] آن برابر $۲n$ باشد؛ یعنی $\sigma(n) = ۲n$. به طور مثال اعداد ۶، ۲۸ و ۴۹۶ تام هستند. اعداد تام ارتباط نزدیکی با اعداد

مرسن دارند. در ابتدا قضیه‌ای معروف در اعداد تام زوج را معرفی می‌کنیم. بخش «اگر» متعلق به اقلیدس و بخش «فقط اگر» متعلق به اویلر است.

قضیه ۱. ۵۱. عدد صحیح مثبت زوج n، تام است اگر و فقط اگر برای عد صحیح مثبت k، $n=2^{k-1}M_k$ و M_k اول باشد.

اثبات: در ابتدا بخش اگر را ثابت می‌کنیم. فرض کنید $n=2^{k-1}(2^k-1)$ که $M_k=2^k-1$ اول است. از آنجا که $\gcd(2^{k-1},2^k-1)=1$ و σ یک تابع ضربی است در نتیجه

$$\sigma(n)=\sigma(2^{k-1})\sigma(2^k-1)=(2^k-1)\times 2^k=2n$$

یعنی n یک عدد تام است.

حال قسمت «فقط اگر» را اثبات می‌کنیم. فرض کنید n یک عدد تام زوج باشد. قرار می‌دهیم $n=2^t\times u$ که $t>0$ و u فرد است. چون n تام است، $\sigma(n)=2n$ و بنابراین $\sigma(2^t\times u)=2^{t+1}\times u$. با استفاده مجدد از این مطلب که σ یک تابع ضربی است، می‌توان نوشت

$$2^{t+1}u=\sigma(2^t u)=\sigma(2^t)\sigma(u)=(2^{t+1}-1)\sigma(u)$$

از آنجا که $\gcd(2^{t+1},2^{t+1}-1)=1$ در نتیجه $2^{t+1}\mid\sigma(u)$ و یا $\sigma(u)=2^{t+1}v$ (v یک عدد صحیح مثبت) بنابراین $u=(2^{t+1}-1)v$

در گام بعدی نشان می‌دهیم $v=1$. اگر این گونه نباشد و $v>1$ آنگاه

$$\sigma(u)\geq 1+v+2^{t+1}-1+v(2^{t+1}-1)=(v+1)2^{t+1}>v\times 2^{t+1}=\sigma(u)$$

که تناقض است. پس $v=1$ و در نتیجه $u=2^{t+1}-1=M_{t+1}$ و $\sigma(u)=2^{t+1}$. اگر M_{t+1} اول نباشد آنگاه $\sigma(u)>2^{t+1}$ که غیر ممکن است. در نهایت $n=2^{k-1}M_k$ که $k=t+1$ است.

قضیه ۱. ۵۱ یک تناظر یک به یک بین اعداد مرسن اول و اعداد تام زوج برقرار می‌کند. قضیه زیر یک مسأله ساده درباره اعداد تام فرد است.

قضیه ۱. ۵۲. اگر n یک عدد تام فرد باشد آنگاه تجزیه n به عوامل اول به شکل زیر است

$$n=p^a q_1^{2b_1}q_2^{2b_2}\dots q_t^{2b_t}$$

که a و p هر دو به پیمانه ۴ با ۱ هم‌نهشت هستند و $t\geq 2$.

اثبات: فرض کنید $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ تجزیه کانونی n به عوامل اول باشد. از آنجا که n عدد تام است داریم

$$\prod_{i=1}^{k} (1 + p_i + p_i^2 + \cdots + p_i^{a_i}) = 2p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$

چون n فرد است، دقیقاً یک i ($1 \le i \le k$) وجود دارد که

$$1 + p_i + p_i^2 + \cdots + p_i^{a_i} \equiv 2 \quad (\text{پیمانه } 4)$$

بنابراین a_i باید فرد باشد و آن را به صورت $a_i = 2x + 1$ که x یک عدد صحیح است نشان می‌دهیم. چون (پیمانه ۴) $p_i^2 \equiv 1$، می‌توان معادله‌ی هم‌نهشتی فوق را به صورت (پیمانه ۴) $(x+1)(p_i+1) \equiv 2$ بازنویسی کرد که به موجب آن (پیمانه ۴) $p_i \equiv 1$ و x زوج است. بنابراین (پیمانه ۴) $a_i \equiv 1$.

برای $j \ne i$ و $1 \le j \le k$ داریم

$$1 + p_j + p_j^2 + \cdots + p_j^{a_j} \equiv 1 \quad (\text{پیمانه } 2)$$

و لذا j باید زوج باشد. بنابراین

$$n = p^a q_1^{2b_1} q_2^{2b_2} \dots q_t^{2b_t}$$

که a و p هر دو به پیمانه ۴ با ۱ هم‌نهشت هستند.

حال تنها این باقی می‌ماند که نشان دهیم $t \ge 2$. فرض کنید $t = 1$. دراین صورت

$$(1 + p + p^2 + \cdots + p^a)(1 + q + q_2 + \cdots + q^{2b}) = 2p^a q^{2b}$$

یا

$$\frac{p^{a+1} - 1}{p - 1} \cdot \frac{q^{2b+1} - 1}{q - 1} = 2p^a q^{2b}$$

بنابراین

$$2 = \frac{p - \frac{1}{p^a}}{p - 1} \cdot \frac{q - \frac{1}{q^{2b}}}{q - 1} < \frac{p}{p - 1} \cdot \frac{q}{q - 1} \le \frac{5}{4} \times \frac{3}{2} = \frac{15}{8}$$

که صحیح نیست لذا فرض ما غلط بوده و $t \ge 2$.

در ۱۹۸۰، هگیس[1] ثابت کرد $t \geq ۷$ و $n > ۱۰^{۵۰}$. مسأله وجود اعداد تام فرد هنوز یکی از چالش برانگیزترین مسائل در تئوری اعداد است.

[1] Hagis

۲- مسائل مقدماتی

۱. فرض کنید ۱، ۴، ... و ۹، ۱۶، ... دو تصاعد حسابی باشند. مجموعه‌ی S اجتماع ۲۰۰۴ عضو ابتدایی هر دنباله است. چند عدد متمایز در S وجود دارد؟

۲. یک دنباله از شش عدد صحیح مثبت اکیداً صعودی داده شده به طوری که هر عدد (بجز عدد اول) مضربی از عدد قبلی است. مجموع این شش عدد ۷۹ است. بزرگ‌ترین عدد در بین این اعداد چیست؟

۳. بزرگ‌ترین عدد صحیح مثبت n که به ازای آن عدد $n^۳ + ۱۰۰$ بر $n + ۱۰$ بخشپذیر باشد، چند است؟

۴. کسرهای ساده نشدنی

(۱) فرض کنید n یک عدد صحیح بزرگ تر از ۲ باشد. ثابت کنید تعداد زوجی از کسرهای زیر ساده نشدنی هستند.

$$\frac{۱}{n}, \frac{۲}{n}, \cdots, \frac{n-۱}{n}$$

(۲) نشان دهید کسر

$$\frac{۱۲n+۱}{۳۰n+۲}$$

به ازای تمام مقادیر n ساده نشدنی است.

۵. روی هر وجه یک مکعب یک عدد صحیح نوشته می‌شود. به هر رأس مکعب حاصلضرب اعداد روی سه وجهی که در آن رأس مشترک هستند نسبت داده می‌شود. مجموع اعدادی که به همه رئوس نسبت داده شده برابر ۱۰۰۱ است. مجموع اعدادی که روی وجوه مکعب نوشته شده است را بیابید.

۶. یک عدد، *شبه اول* نامیده می‌شود اگر مرکب بوده ولی بر ۲، ۳ یا ۵ بخشپذیر نباشد. کوچک ترین سه عدد شبه اول ۴۹، ۷۷ و ۹۱ هستند. می‌دانیم ۱۶۸ عدد اول کوچک تر از ۱۰۰۰ وجود دارد. چند عدد شبه اول کوچک تر از ۱۰۰۰ وجود دارد؟

۷. عدد صحیح مثبت k بزرگ تر از ۱ داده شده است. ثابت کنید عدد اول p و دنباله اکیداً صعودی $a_1, a_2, \ldots, a_n, \ldots$ از اعداد صحیح مثبت وجود دارند که به ازای آن اعضای دنباله

$$p + ka_1, p + ka_2, \ldots, p + ka_n, \ldots$$

همگی اول هستند.

۸. عدد صحیح مثبت n داده شده است. فرض کنید $p(n)$ بیانگر حاصلضرب ارقام غیر صفر n باشد. (اگر n فقط یک رقم داشته باشد، $p(n)$ برابر همان رقم است) اگر

$$S = p(1) + p(2) + \ldots + p(999)$$

بزرگ‌ترین عامل اول S چند است؟

۹. فرض کنید m و n اعداد صحیح مثبت باشند بطوری که

$$\operatorname{lcm}(m,n) + \gcd(m,n) = m + n$$

ثابت کنید یکی از این دو عدد بر دیگری بخشپذیر است.

۱۰. فرض کنید $n = 2^{31} \times 3^{19}$. چند مقسوم‌علیه مثبت n^2 کوچک‌تر از n هستند ولی n را نمی‌شمارند؟

۱۱. نشان دهید برای هر دو عدد صحیح مثبت a و b عدد $(a+36b)(36a+b)$ نمی‌تواند توانی از ۲ باشد؟

۱۲. مجموع بزرگ‌ترین مقسوم‌علیه‌های فرد هر یک از اعداد ۲۰۰۶، ۲۰۰۷، ...، ۴۰۱۲ را بیابید.

۱۳. مجموع همه اعداد به شکل $\frac{a}{b}$ که a و b نسبت به هم اول بوده و مقسوم‌علیه مثبت ۲۷۰۰۰ باشند را بیابید.

۱۴. L.C.M سه عدد.

(۱) تعداد سه‌تایی‌های مرتب (a,b,c) از اعداد صحیح مثبت که $\operatorname{lcm}(a,b) = 1000$، $\operatorname{lcm}(b,c) = 2000$ و $\operatorname{lcm}(c,a) = 2000$ را بیابید.

(۲) a, b و c اعداد صحیح هستند. ثابت کنید:

$$\frac{\operatorname{lcm}(a,b,c)^2}{\operatorname{lcm}(a,b)\operatorname{lcm}(b,c)\operatorname{lcm}(c,a)} = \frac{\gcd(a,b,c)^2}{\gcd(a,b)\gcd(b,c)\gcd(c,a)}$$

۱۵. فرض کنید x, y و z اعداد صحیح مثبت باشند به‌طوری‌که

$$\frac{۱}{x}-\frac{۱}{y}=\frac{۱}{z}$$

و h بزرگ‌ترین مقسوم علیه مشترک x, y و z باشد. ثابت کنید $hxyz$ و $h(y-x)$ مربع کامل هستند.

۱۶. فرض کنید p یک عدد اول به شکل $۳k+۲$ باشد که عدد $a^۲+ab+b^۲$ را می‌شمارد ثابت کنید a و b هر دو بر p بخشپذیرند.

۱۷. عدد ۲۷۰۰۰۰۰۱ دقیقاً ۴ عامل اول دارد. مجموع آنها را بیابید.

۱۸. همه‌ی اعداد صحیح مثبت n را چنان بیابید که $n!+۵$ مکعب کامل باشد.

۱۹. همه‌ی اعداد اول p را چنان بیابید که عدد $p^۲+۱۱$ دقیقاً ۶ مقسوم‌علیه متمایز (شامل ۱ و خود عدد) داشته باشد.

۲۰. عدد صحیح مثبت N یک دوبل ۷-۱۰ نامیده می‌شود اگر آن را در مبنای ۷ نوشته و عدد حاصل را در مبنای ۱۰ بخوانیم، عدد حاصل معادل دو برابر N در مبنای ۱۰ باشد. بطور مثال ۵۱ یک دوبل ۷-۱۰ است زیرا در مبنای ۷ برابر ۱۰۲ است. بزرگ‌ترین دوبل ۷-۱۰ چند است؟

۲۱. اگر (پیمانه n) $a\equiv b$ نشان دهید که (پیمانه $n^۲$) $a^n\equiv b^n$. آیا برعکس آن صحیح است؟

۲۲. فرض کنید p یک عدد اول و $۱\le k\le p-۱$ یک عدد صحیح باشد. ثابت کنید:

$$\binom{p-۱}{k}\equiv(-۱)^k \quad (\text{پیمانه } p)$$

۲۳. فرض کنید p یک عدد اول باشد. نشان دهید بی‌نهایت عدد صحیح مثبت n وجود داد به طوریکه p، عدد ۲^n-n را می‌شمارد.

۲۴. فرض کنید n یک عدد صحیح بزرگ تر از ۳ باشد. ثابت کنید $۱!+۲!+\ldots+n!$ نمی‌تواند یک توان کامل باشد.

۲۵. فرض کنید k یک عدد صحیح مثبت فرد باشد. ثابت کنید برای تمام اعداد صحیح مثبت n

$$(۱+۲+\ldots+n)\mid(۱^k+۲^k+\ldots+n^k)$$

۲۶. فرض کنید p یک عدد اول بزرگ تر از ۵ باشد. ثابت کنید $p-۴$ نمی‌تواند توان چهارم یک عدد صحیح باشد.

۲۷. برای عدد صحیح مثبت n ثابت کنید:

$$\sigma(1)+\sigma(2)+\ldots+\sigma(n)\le n^2$$

۲۸. همه‌ی مجموعه‌های ناتهی و متناهی S از اعداد صحیح مثبت را پیدا کنید به طوری‌که برای هر i و j (نه لزوماً متمایز) در S عدد $\dfrac{i+j}{\gcd(i,j)}$ نیز یک عضو S باشد.

۲۹. با دانستن اینکه 2^{29} یک عدد ۹ رقمی است که همه ارقامش متمایز هستند، بدون محاسبه عدد تعیین کنید که کدام رقم از ۰ رقم در آن وجود ندارد. روی جواب خود بحث کنید.

۳۰. ثابت کنید برای هر عدد صحیح n بزرگ‌تر از ۱ عدد n^5+n^4+1 مرکب است.

۳۱. حاصل‌ضرب چند عدد اول، ده برابر مجموعشان است. این اعداد اول (نه لزوماً متمایز) کدامند؟

۳۲. یک عدد ۱۰ رقمی *جالب* است اگر ارقامش همگی متمایز بوده و مضربی از ۱۱۱۱۱ باشد. چند عدد صحیح جالب وجود دارد؟

۳۳. آیا ۱۹ عدد صحیح مثبت متمایز وجود دارند که مجموعشان برابر ۱۹۹۹ بوده و مجموع ارقامشان با هم برابر باشد؟

۳۴. همه‌ی اعداد اول p و q را پیدا کنید به طوری‌که pq، عدد $(5^p-2^p)(5^q-2^q)$ را بشمارد.

۳۵. ثابت کنید بی‌نهایت عدد وجود دارد که شامل رقم صفر نبوده و بر مجموع ارقام خود بخشپذیرند.

۳۶. ثابت کنید که هر عدد شامل 2^n رقم یکسان، حداقل n عامل اول متمایز دارد.

۳۷. فرض کنید a و b دو عدد صحیح نسبت به هم اول باشند. تصاعد حسابی a، $a+b$، $a+2b$، $a+3b$، ... را در نظر بگیرید.

(۱) ثابت کنید بی‌نهایت عضو در تصاعد هستند که عوامل اول یکسانی دارند.

(۲) ثابت کنید بی‌نهایت عدد در تصاعد وجود دارد که دو به دو نسبت به هم اول هستند.

۳۸. فرض کنید n یک عدد صحیح مثبت باشد.

(۱) حاصل $\gcd(n!+1,(n+1)!+1)$ را محاسبه کنید.

(۲) اگر a و b اعداد صحیح مثبت باشند، ثابت کنید

$$\gcd(n^a-1,n^b-1)=n^{\gcd(a,b)}-1$$

(۳) a و b اعداد صحیح مثبت هستند. ثابت کنید $\gcd(۲^a+۱, ۲^b+۱)$، $۲^{\gcd(a,b)}+۱$ را می‌شمارد.

(۴) اگر m یک عدد صحیح مثبت بوده و $\gcd(m,n)=۱$، آنگاه عدد $\gcd(۵^m+۷^m, ۵^n+۷^n)$ را بر حسب m و n بیان کنید.

۳۹. مبنا

(۱) تعیین کنید که آیا می‌توان یک مکعب و یک صفحه پیدا کرد که فواصل رئوس مکعب از صفحه ۰، ۱، ۲، .... و ۷ باشد.

(۲) دنباله صعودی $۱,۳,۴,۹,۱۰,۱۲,۱۳,\ldots$ شامل همه‌ی اعداد صحیح مثبت است که توانی از ۳ یا مجموع توانهای متمایز ۳ هستند. صدمین عضو این دنباله را پیدا کنید. (۱، اولین عضو است، ۳، دومین عضو و ....)

۴۰. کسرها در حساب پیمانه‌ای

(۱) فرض کنید a یک عدد صحیح باشد به طوریکه

$$۱+\frac{۱}{۲}+\frac{۱}{۳}+\ldots+\frac{۱}{۲۳}=\frac{a}{۲۳!}$$

باقیمانده تقسیم a بر ۱۳ را محاسبه کنید.

(۲) فرض کنید $p>۳$ یک عدد اول و m و n اعداد صحیح نسبت به هم اول باشند به طوری که

$$\frac{m}{n}=(\frac{۱}{۱^۲}+\frac{۱}{۲^۲}+\ldots+\frac{۱}{(p-۱)^۲})$$

ثابت کنید m بر p بخشپذیر است.

(۳) فرض کنید $p>۳$ یک عدد اول باشد. ثابت کنید:

$$p^۲ \mid (p-۱)!(۱+\frac{۱}{۲}+\ldots+\frac{۱}{p-۱})$$

۴۱. همه‌ی زوجهای (x,y) از اعداد صحیح نامنفی که $x^۲+۳y$ و $y^۲+۳x$ مربع کامل باشند را بیابید.

۴۲. (۱) می‌دانیم $۲^{۲۰۰۴}$ یک عدد ۶۰۴ رقمی است که با رقم ۱ شروع می‌شود. تعداد اعضای مجموعه‌ی

$$\{۲^۰, ۲^۱, ۲^۲, \ldots, ۲^{۲۰۰۳}\}$$

که با رقم ۴ شروع می‌شوند را تعیین کنید.

(۲) فرض کنید k یک عدد صحیح مثبت باشد. $n=n(k)$ یک عدد صحیح مثبت است که بسط ۲^n و ۵^n در مبنای ده با k رقم یکسان شروع می‌شوند. این ارقام کدام‌ها هستند؟

۴۳. (۱) رقم انتهایی (رقم یکان) اعداد زیر را تعیین کنید.

$$\underbrace{۷^{۷^{\cdot^{\cdot^{۷}}}}}_{۱۰۰۱\text{ بار عدد }۷} \quad \text{و} \quad ۳^{۱۰۰۱}\times ۷^{۱۰۰۲}\times ۱۳^{۱۰۰۳}$$

(۲) سه رقم آخر عدد $۲۰۰۳^{۲۰۰۲^{۲۰۰۱}}$ را تعیین کنید.

(۳) ضریب دو جمله‌ای $\binom{۹۹}{۱۹}$ یک عدد ۲۱ رقمی است:

$$۱۰۷,۱۹۶,۶۷۴,۰۸۰,۷۶۱,۹۳۶,xyz$$

عدد سه رقمی xyz را پیدا کنید.

(۴) کوچک‌ترین عدد صحیح مثبت که مکعبش به ۸۸۸ ختم می‌شود را پیدا کنید.

۴۴. فرض کنید $p\geq ۳$ یک عدد اول بوده و $\{b_۱,b_۲,...,b_{p-۱}\}$ و $\{a_۱,a_۲,...,a_{p-۱}\}$ دو مجموعه کامل مانده‌ها به پیمانه p باشند. ثابت کنید

$$\{a_۱b_۱,a_۲b_۲,...,a_{p-۱}b_{p-۱}\}$$

یک مجموعه کامل مانده‌ها به پیمانه p نیست.

۴۵. فرض کنید $p\geq ۳$ یک عدد اول باشد. تعیین کنید آیا جایگشت

$$(a_۱,a_۲,...,a_{p-۱})$$

از $(۱,۲,...,p-۱)$ وجود دارد به طوری‌که دنباله $\{ia_i\}_{i=۱}^{p-۱}$ شامل $p-۲$ دسته متمایز هم‌نهشتی به پیمانه p باشد.

۴۶. ثابت کنید هر عدد صحیح مثبت کوچک‌تر از $n!$ را می‌توان به‌صورت مجموع چند (کمتر یا مساوی n) مقسوم علیه مثبت $n!$ نوشت.

۴۷. فرض کنید $n>۱$ یک عدد صحیح فرد باشد. ثابت کنید n ، $۳^n+۱$ را نمی‌شمارد.

۴۸. فرض کنید a و b اعداد صحیح مثبت باشند. ثابت کنید تعداد جوابهای (x,y,z) معادله $ax+by+z=ab$ در مجموعه اعداد صحیح نامنفی برابر است با:

$$\frac{۱}{۲}[(a+۱)(b+۱)+\gcd(a,b)+۱]$$

۴۹. (۱) فرض کنید p یک عدد اول فرد بوده و q و r اعداد اولی باشند که p، q^r+1 را می‌شمارد. ثابت کنید

$$p \mid q^2-1 \qquad \text{یا} \qquad 2r \mid p-1$$

(۲) فرض کنید $a>1$ و n اعداد صحیح مثبت باشند. اگر p یک مقسوم علیه اول $a^{2^n}+1$ باشد ثابت کنید $p-1$ بر 2^{n+1} بخشپذیر است.

۵۰. ثابت کنید

$$\left\lfloor \frac{(n-1)!}{n(n+1)} \right\rfloor$$

برای تمام مقادیر صحیح و مثبت n، زوج است.

۵۱. همه‌ی اعداد صحیح مثبت m را چنان پیدا کنید که دارای این خاصیت باشند که: عدد صحیح مثبت و منحصر به فرد n و مستطیل‌هایی وجود دارند که می‌توان آن مستطیل‌ها را هم به n مربع هم‌نهشت و هم به $n+m$ مربع هم‌نهشت تقسیم کرد.

۵۲. همه اعداد صحیح مثبت n را چنان تعیین کنید که n مضربی داشته باشد که ارقامش غیرصفر باشند.

۳- مسائل پیشرفته

۱. (آ) ثابت کنید مجموع مربعات ۳، ۴، ۵ و یا ۶ عدد صحیح متوالی مربع کامل نیست.
(ب) مثالی از ۱۱ عدد صحیح مثبت متوالی ارائه کنید که مجموع مربعات آن‌ها مربع کامل باشد.

۲. فرض کنید $S(x)$ مجموع ارقام عدد صحیح مثبت x در مبنای ۱۰ باشد.
(آ) ثابت کنید برای هر عدد صحیح مثبت x، $\frac{S(x)}{S(2x)} \leq 5$. آیا می‌توان این کران را بهبود بخشید؟
(ب) ثابت کنید $\frac{S(x)}{S(3x)}$ کراندار نیست.

۳. بیشتر اعداد صحیح را می‌توان به‌صورت جمع ۲ یا چند عدد صحیح مثبت متوالی نشان داد. بطور مثال $۹+۸+۷=۲۴$ و $۲۶+۲۵=۵۱$. یک عدد صحیح مثبت که نتوان آن را به صورت مجموع ۲یا چند عدد صحیح مثبت متوالی نشان داد، *جالب* نامیده می‌شود تمام اعداد جالب را بیابید.

۴. مجموعه $S=\{۱۰۵,۱۰۶,...,۲۱۰\}$ داده شده است. کمترین مقدار n را چنان تعیین کنیدکه هر زیر مجموعه n عضوی T از S شامل حداقل دو عضو که نسبت به هم اول نیستند باشد.

۵. عدد

$$\underbrace{۹۹...۹۹}_{\text{۱۹۹۷ تا}}$$

روی یک تخته سیاه نوشته می‌شود. در هر دقیقه یکی از اعدادی که روی تخته نوشته شده است به دو عامل تجزیه شده و پاک می‌شود. به هر عامل (بطور مستقل) ۲ واحد اضافه شده یا

از آن کسر می‌شود و دو عدد بدست آمده نوشته می‌شود. آیا امکان دارد بعد از گذشت چند دقیقه (بعد از اولین دقیقه) همه‌ی اعداد روی تخته سیاه برابر ۹ باشند؟

۶. فرض کنید d یک عدد صحیح مثبت باشد که برابر ۲، ۵ یا ۱۳ نیست. نشان دهید می‌توان اعداد متمایز a و b از مجموعه‌ی $\{۲,۵,۱۳,d\}$ را چنان انتخاب کرد که $ab-۱$ مربع کامل نباشد.

۷. یک جعبه توپ شامل هزار توپ ۱۰ گرمی و هزار توپ ۹/۹ گرمی است. می‌خواهیم ۲ بسته توپ با تعداد مساوی را برداریم که وزن کل آن‌ها یکی نباشد. کمترین تعداد توزین لازم برای انجام این‌کار چقدر است؟ (یک ترازوی تعادلی وزن اشیای کفه سمت چپ را با وزن اشیای کفه سمت راست مقایسه می‌کند)

۸. سه عدد a,b و c داده شده است به طوری‌که $a,b,c,a+b-c,b+c-a,c+a-b$ هفت عدد اول متمایز هستند. فرض کنید d اختلاف بین بزرگ‌ترین و کوچک‌ترین این هفت عدد اول باشد. اگر بدانیم ۸۰۰ یک عضو مجموعه‌ی $\{a+b,b+c,c+a\}$است، بیشترین مقدار ممکن برای d را تعیین کنید.

۹. ثابت کنید حاصل مجموع

$$S(m,n)=\frac{۱}{m}+\frac{۱}{m+۱}+\ldots+\frac{۱}{m+n}$$

برای هر دو عدد صحیح و مثبت m و n عدد صحیح نیست.

۱۰. برای همه‌ی اعداد صحیح مثبت $n<m$ ثابت کنید

$$\operatorname{lcm}(m,n)+\operatorname{lcm}(m+۱,n+۱)>\frac{۲mn}{\sqrt{m-n}}$$

۱۱. ثابت کنید هر عدد صحیح نامنفی را می‌توان به شکل $a^۲+b^۲-c^۲$ نشان داد که a,b و c اعداد صحیح مثبت با شرط $a<b<c$ هستند.

۱۲. تعیین کنید آیا دنباله اکیداً صعودی $\{a_k\}_{k=۱}^{\infty}$ از اعداد صحیح مثبت وجود دارد که دنباله $\{a_k+a\}_{k=۱}^{\infty}$ به ازای همه‌ی مقادیر صحیح a فقط شامل تعداد محدودی عدد اول باشد.

۱۳. ثابت کنید با انتخاب‌های مختلف علامت‌های + و − در عبارت

$$\pm ۱\pm ۲\pm ۳\pm\cdots\pm(۴n+۱)$$

همه اعداد صحیح مثبت فرد کوچک‌تر یا مساوی $(۲n+۱)(۴n+۱)$ بدست خواهند آمد.

۱۴. فرض کنید a و b دو عدد صحیح مثبت نسبت به هم اول باشند. نشان دهید

$$ax+by=n$$

برای همه‌ی مقادیر صحیح $ab-a-b<n$، دارای جواب صحیح نامنفی (x,y) می‌باشد. در حالت $n=ab-a-b$ چطور؟

۱۵. اندازه اضلاع یک مثلث، اعدادصحیح k, m و n است. فرض کنید $k>m>n$ و

$$\{\frac{۳^k}{۱۰^۴}\}=\{\frac{۳^m}{۱۰^۴}\}=\{\frac{۳^n}{۱۰^۴}\}$$

کمترین مقدار محیط مثلث را تعیین کنید.

۱۶. بازی دو نفره زیر را در نظر بگیرید. تعدادی سنگریزه روی میز قرار دارند. دو بازیکن به نوبت حرکات خود را انجام می‌دهند. یک حرکت شامل برداشتن x سنگریزه از روی میز است که x می‌تواند مربع هر عدد صحیح مثبت باشد. بازیکنی که نتواند حرکتی کند بازنده است. ثابت کنید بی‌نهایت شرایط اولیه وجود دارد که به ازای آن‌ها نفر دوم می‌تواند طوری بازی کند که برنده شود.

۱۷. ثابت کنید دنباله ۱,۱۱,۱۱۱,.... یک زیر دنباله نامتناهی دارد که اعضای آن دو به دو نسبت به هم اول هستند.

۱۸. فرض کنید m و n اعداد صحیح بزرگ‌تر از ۱ باشند به طوری که $\gcd(m,n-۱)=\gcd(m,n)=۱$. ثابت کنید اولین $m-۱$ عضو دنباله $n_۱,n_۲,...$ که $n_۱=nm+۱$ و $n_{k+۱}=nn_k+۱$ $(k\geq ۱)$ نمی‌توانند همگی اول باشند.

۱۹. همه‌ی اعداد صحیح مثبت m را چنان پیدا کنید که توان چهارم تعداد مقسوم‌علیه‌های مثبت m برابر m باشد.

۲۰. (۱) نشان دهید می‌توان از بین هر ۳۹ عدد صحیح مثبت متوالی یک عدد را انتخاب کرد که مجموع ارقامش بر ۱۱ بخشپذیر باشد.
(۲) اولین ۳۸ عدد صحیح مثبت متوالی را پیدا کنید که هیچ‌یک از آن‌ها مجموع ارقامش بر ۱۱ بخشپذیر نباشد.

۲۱. بزرگ‌ترین عدد صحیح n را چنان بیابید که n بر همه اعداد صحیح مثبت کوچک‌تر از $\sqrt[۳]{n}$ بخشپذیر باشد.

۲۲. نشان دهید برای هرعدد صحیح مثبت و ثابت n، دنباله

$$۲,۳^۲,۳^{۳^۲},۳^{۳^{۳^۲}},... \quad (n \text{ پیمانه})$$

در نهایت ثابت خواهد بود (برج توان به این‌صورت تعریف می‌شود که $a_1 = 2$ و برای هر عدد صحیح مثبت i، $a_{i+1} = 2^{a_i}$)

۲۳. ثابت کنید برای $n \geq 5$, $f_n + f_{n-1} - 1$ حداقل $n+1$ عامل اول دارد که $f_n = 2^{2^n} + 1$ است.

۲۴. ثابت کنید هر عدد صحیح را می‌توان به‌صورت مجموع مکعبات ۵ عدد صحیح نه لزوماً متمایز نوشت.

۲۵. بخش‌های صحیح و اعشاری

(۱) همه‌ی عددهای حقیقی x را چنان بیابید که

$$x\lfloor x\lfloor x\lfloor x\rfloor\rfloor\rfloor = 88$$

(۲) نشان دهید معادله

$$\{x^3\} + \{y^3\} = \{z^3\}$$

بی‌نهایت پاسخ گویای نا صحیح دارد.

۲۶. فرض کنید n یک عدد صحیح مثبت باشد. اگر p یک عامل اول عدد فرمای f_n باشد، ثابت کنید $p-1$ بر 2^{n+2} بخشپذیر است.

۲۷. دنباله‌ی

$$\{a_n\}_{n=1}^{\infty} = \{1,2,4,5,7,9,10,12,14,16,17,\ldots\}$$

از اعداد صحیح مثبت این‌گونه ساخته می‌شود: یک عدد فرد، دو عدد زوج، سه عدد فرد و .... a_n را به شکل بسته بیان کنید.

۲۸. ثابت کنید برای هر $n \geq 2$، مجموعه S از n عدد صحیح وجود دارد به طوری‌که برای هر دو عضو متمایز a و b از S, $(a-b)^2, ab$ را می‌شمارد.

۲۹. نشان دهید بی‌نهایت عدد صحیح مثبت n وجود دارد به‌طوریکه بزرگ‌ترین عامل اول n^4+1 بزرگ‌تر از $2n$ است.

۳۰. برای عدد صحیح مثبت k، $p(k)$ را برابر بزرگ‌ترین مقسوم‌علیه فرد k می‌گیریم. ثابت کنید برای هر عدد صحیح مثبت n

$$\frac{2n}{3} < \frac{p(1)}{1} + \frac{p(2)}{2} + \cdots + \frac{p(n)}{n} < \frac{2(n+1)}{3}$$

۳۱. اگر p^t توانی از یک عدد اول فرد و m یک عدد صحیح باشد که نسبت به p و $p-1$ اول است، آن‌گاه برای هر a و b که نسبت به p اول باشند

$$a^m \equiv b^m \quad (p^t \text{ پیمانه}) \Leftrightarrow a \equiv b \ (p^t \text{ پیمانه})$$

۳۲. ثابت کنید برای هر عدد اول $p \leq ۷$، عدد صحیح مثبت n و اعداد صحیح $x_۱, \ldots, x_n, y_۱, \ldots, y_n$ غیر بخشپذیر بر p وجود دارند به‌طوریکه

$$\begin{cases} x_۱^۲ + y_۱^۲ \equiv x_۲^۲ & (p \text{ پیمانه}) \\ x_۲^۲ + y_۲^۲ \equiv x_۳^۲ & (p \text{ پیمانه}) \\ \vdots & \\ x_n^۲ + y_n^۲ \equiv x_۱^۲ & (p \text{ پیمانه}) \end{cases}$$

۳۳. برای هر عدد صحیح مثبت n ثابت کنید:

$$\frac{\sigma(۱)}{۱} + \frac{\sigma(۲)}{۲} + \cdots + \frac{\sigma(n)}{n} \leq ۲n$$

۳۴. ثابت کنید دستگاه معادلات زیر هیچ پاسخی برای اعداد صحیح x, y و z ندارد.

$$x^۶ + x^۳ + x^۳y + y = ۱۴۷^{۱۵۷}$$
$$x^۳ + x^۳y + y^۲ + y + z^۹ = ۱۵۷^{۱۴۷}$$

۳۵. حداقل چندبار توزین با استفاده از یک ترازوی عقربه‌ای دو کفه‌ای لازم است تا بتوان وزنه‌های موجود در یک مجموعه که می‌دانیم شامل وزنه‌های $۱, ۳, ۳^۲, \ldots, ۳^{۲۶}$ است را بطور مشخص تعیین کرد؟ (یک ترازوی عقربه‌ای دو کفه‌ای تفاضل وزن اشیای موجود در کفه سمت چپ از وزن اشیای موجود در کفه سمت راست را گزارش می‌کند)

۳۶. فرض کنید λ ریشه مثبت معادله $t^۲ - ۱۹۹۸t - ۱ = ۰$ باشد. دنباله $x_۰, x_۱, \ldots$ را به‌صورت زیر تعریف می‌کنیم

$$x_۰ = ۱, \quad x_{n+۱} = \lfloor \lambda x_n \rfloor \quad (n \geq ۰)$$

باقیمانده تقسیم $x_{۱۹۹۸}$ بر ۱۹۹۸ را بیابید.

۳۷. تعیین کنید (با اثبات) آیا زیر مجموعه X از اعداد صحیح با خاصیت زیر وجود دارد: برای هر عدد صحیح n، دقیقاً یک جواب برای $a + ۲b = n$ $(a, b \in X)$ وجود داشته باشد.

۳۸. عدد x_n به عنوان آخرین رقم عدد صحیح $\lfloor \sqrt{۲^n} \rfloor$ $(n = ۱, ۲, \ldots)$ در مبنای ۱۰ تعریف می‌شود. تعیین کنید که آیا دنباله $x_۱, x_۲, \ldots, x_n, \ldots$ متناوب است؟

۳۹. ثابت کنید هر عدد صحیح n را می‌توان با انتخاب مناسب k و علامت‌های $+$ و $-$، به بی‌نهایت روش به صورت زیر بیان کرد:

$$n = \pm 1^2 \pm 2^2 \pm \ldots \pm k^2$$

۴۰. فرض کنید n یک عدد صحیح باشد که $n \geq 4$. برای عدد صحیح مثبت m، S_m را به‌صورت $S_m = \{m, m+1, \ldots, m+n-1\}$ تعریف می‌کنیم. کمترین مقدار $f(n)$ را چنان بیابید که هر زیر مجموعه‌ی $f(n)$ عضوی S_m (برای هر m) شامل حداقل سه عدد دو به دو نسبت به هم اول باشد.

۴۱. کوچک‌ترین عدد صحیح مثبت r را چنان بیابید که برای همه اعداد صحیح a, b, c و d عدد $((abcd)!)^r$ بر حاصلضرب اعداد زیر بخش‌پذیر باشد.

$$(a!)^{bcd+1}, (b!)^{acd+1}, (c!)^{abd+1}, (d!)^{abc+1}$$
$$((ab)!)^{cd+1}, ((bc)!)^{ad+1}, ((cd)!)^{ab+1}, ((ac)!)^{bd+1}$$
$$((bd)!)^{ac+1}, ((ad)!)^{bc+1}, ((abc)!)^{d+1}, ((abd)!)^{c+1}$$
$$((acd)!)^{b+1}, ((bcd)!)^{a+1}$$

۴۲. دو مسأله کلاسیک در L.C.M

(۱) فرض کنید $a_0 < a_1 < a_2 < \cdots < a_n$ اعداد صحیح مثبت باشند. ثابت کنید:

$$\frac{1}{\operatorname{lcm}(a_0, a_1)} + \frac{1}{\operatorname{lcm}(a_1, a_2)} + \cdots + \frac{1}{\operatorname{lcm}(a_{n-1}, a_n)} \leq 1 - \frac{1}{2^n}$$

(۲) چند عدد صحیح مثبت که هیچ‌یک، از عدد صحیح ثابت m بیشتر نیستند، داده شده‌اند. ثابت کنید اگر هر عدد صحیح مثبت کوچک‌تر یا مساوی m بر هر زوج از اعداد داده شده بخشپذیر نباشد آنگاه مجموع معکوس این اعداد کوچک‌تر از $\frac{3}{2}$ است.

۴۳. برای عدد صحیح مثبت n، $r(n)$ را برابر مجموع باقیمانده‌های تقسیم n بر $1, 2, \ldots, n$ می‌گیریم. ثابت کنید بی‌نهایت عدد n وجود دارد به‌طوری‌که $r(n) = r(n-1)$

۴۴. دو مسأله مرتبط به هم در IMO

(۱) *عدد لغزان* یک عدد صحیح مثبت است که ارقامش یکی در میان صفر و غیرصفر بوده و رقم یکانش نیز غیر صفر است. همه‌ی اعداد صحیح مثبت که هیچ عدد لغزانی را نمی‌شمارند پیدا کنید.

(۲) یک عدد صحیح مثبت *تناوبی* نامیده می‌شود اگر در بین هر دو رقم متوالی آن در مبنای ۱۰ یکی زوج و دیگری فرد باشد همه‌ی اعداد صحیح n را چنان پیدا کنید که n مضربی در بین اعداد تناوبی داشته باشد.

۴۵. فرض کنید p یک عدد اول فرد باشد. دنباله $(a_n)_{n \geq 0}$ به‌صورت زیر تعریف می‌شود: $a_0 = 0$، $a_1 = 1$، $a_{p-2} = p-2, \ldots, a_1 = 1$ و برای هر $p-1 \leq n$ a_n کوچک ترین عدد صحیح مثبت است که با هیچ یک از اعضای قبلی تشکیل یک تصاعد حسابی به طول p را ندهد. ثابت کنید برای

هر a_n, n عددی است که پس از نوشتن عدد n در مبنای $p-1$ و خواندن عدد حاصل در مبنای p، بدست می‌آید.

۴۶. تعیین کنید آیا عدد صحیح مثبت n وجود دارد که n دقیقاً بر ۲۰۰۰ عدد اول متفاوت و 2^n+1 بر n بخشپذیر باشند.

۴۷. (۱) تعیین کنید آیا اعداد صحیح دو به دو نسبت به هم اول a,b و c با شرط $a,b,c>1$ وجود دارند به‌طوری‌که

$$b \mid 2^a+1 \, , \, c \mid 2^b+1 \, , \, a \mid 2^c+1$$

(۲) همه سه‌تایی‌های مرتب (p,q,r) از اعداد اول را چنان تعیین کنید که

$$p \mid q^r+1 \, , \, q \mid r^p+1 \, , \, r \mid p^q+1$$

۴۸. فرض کنید n یک عدد صحیح مثبت و $p_1, p_2, \ldots, p_n$ اعداد اول متمایز بزرگ‌تر از سه باشند. ثابت کنید $2^{p_1 p_2 \cdots p_n}+1$ حداقل 4^n مقسوم‌علیه دارد.

۴۹. فرض کنید p یک عدد اول بوده و $\{a_k\}_{k=0}^{\infty}$ یک دنباله از اعداد صحیح باشد که $a_0=0$ و $a_1=1$

$$(k=0,1,2,\ldots) \quad a_{k+2}=2a_{k+1}-pa_k$$

با فرض این‌که عدد ۱- در دنباله وجود دارد همه‌ی مقادیر ممکن p را بیابید.

۵۰. فرض کنید F مجموعه‌ای از زیر مجموعه‌های مجموعه‌ی $\{1,2,\ldots,n\}$ باشد که
(۱) اگر A یک عضو F باشد آن‌گاه A دقیقاً سه عضو دارد.
(۲) اگر A و B دو عضو متمایز F باشند، A و B حداکثر یک عضو مشترک دارند.
فرض کنید $f(n)$ بیانگر بیشترین تعداد اعضای F باشد. ثابت کنید:

$$\frac{(n-1)(n-2)}{6} \le f(n) \le \frac{(n-1)n}{6}$$

۵۱. همه اعداد صحیح مثبت k را چنان تعیین کنید که

$$\frac{\tau(n^2)}{\tau(n)}=k \quad \text{(برای عدد صحیح } n\text{)}$$

۵۲. فرض کنید n یک عدد صحیح و مثبت بزرگ‌تر از ۲ باشد. ثابت کنید عدد فرمای f_n یک مقسوم علیه اول بزرگ‌تر از $2^{n+2}(n+1)$ دارد.

۴-پاسخ مسائل مقدماتی

۱. [AMC10B۲۰۰۴] کوچک‌ترین عددی که در هر دو دنباله ظاهر می‌شود، ۱۶ است. از آن‌جایی که کوچک‌ترین مضرب مشترک۳ و ۷ (قدر نسبت‌های دو تصاعد) ۲۱ است. فقط اعدادی در دو دنباله ظاهر می‌شوند که به فرم $16+21k$ باشند که k یک عدد صحیح نامنفی است. بزرگ‌ترین مقدار k به گونه‌ای است که $16+21k \le 3\times 2003+1$ و لذا $k=285$. بنابراین ۲۸۶ عدد در هر دو دنباله ظاهر می‌شوند و لذا جواب مسأله برابر است با $4008-286=3722$

۲. [HMMT۲۰۰۴] فرض کنید $a_1<a_2<\cdots<a_6$ آن شش عدد باشند. اگر $a_4 \ge 12$ آن‌گاه $a_5 \ge 2a_4 \ge 24$ و $a_6 \ge 2a_5 \ge 48$ و در نتیجه $a_4+a_5+a_6 \ge 84$ که شرایط مسأله را نقض می‌کند؛ بنابراین $a_4<12$. به این ترتیب تنها حالتی که می‌توان بخشپذیری‌های مورد نظر مسأله را در بین ۴ عدد اول برقرار کرد زمانی است که $a_1=1, a_2=2, a_3=4$ و $a_4=8$. برای دو عدد دیگر داریم: $a_5=ma_4=8m$ و $a_6=na_5=8mn$ که m و n اعداد صحیح و بزرگ تر یا مساوی دو هستند. داریم $8m+8mn=79-(1+2+4+8)=64$ و یا $m(1+n)=8$ که تنها پاسخ‌های قابل قبول این معادله $m=2$ و $n=3$ هستند بنابراین جواب مسأله $a_6=48$ است.

۳. [AIME۱۹۸۶] $n^3+100=(n+10)(n^2-10n+100)-900$ با تقسیم کردن خواهیم داشت بنابراین اگر $n+10, n^3+100$ را بشمارد آن‌گاه باید ۹۰۰ را هم بشمارد. بیشترین مقدار n وقتی است که $n+10$ بیشترین مقدار را داشته باشد و از آن‌جا که بزرگ‌ترین مقسوم‌علیه ۹۰۰، خود ۹۰۰ است، باید داشته باشیم $n+10=900$ و بنابراین $n=890$.

۴. بخش (۱) را با استفاده از زوجیت و بخش (۲) را با استفاده از الگوریتم اقلیدس اثبات می‌کنیم

(۱) کسر $\frac{k}{n}$ ساده نشدنی است اگر و فقط اگر کسر $\frac{n-k}{n}$ ساده نشدنی باشد زیرا $\gcd(k,n)=\gcd(n-k,n)$. اگر کسرهای $\frac{k}{n}$ و $\frac{n-k}{n}$ برای تمام مقادیر k متمایز باشند

زوج‌های فوق، زوج کسر ساده‌نشدنی را تشکیل می‌دهند. اگر $\frac{k}{n}=\frac{n-k}{n}$ آن‌گاه $n=2k$ و بنابراین $\frac{k}{n}=\frac{k}{2k}=\frac{1}{2}$ یک کسر ساده شدنی است و مسأله به همان قسمت قبل ختم می‌شود.

(۲) با توجه به

$$\gcd(30n+2,12n+1)=\gcd(6n,12n+1)=\gcd(6n,1)=1$$

به نتیجه دلخواه می‌رسیم.

۵. فرض کنید a,b,c,d,e و f اعداد نوشته شده روی وجوه مکعب باشند به طوریکه a و f، b و d و c و e اعداد نوشته شده روی وجوه مقابل هم باشند. می‌دانیم

$$1001=abc+abe+acd+ade+bcf+bef+bef+cdf+def$$
$$=(a+f)(b+d)(c+e)$$

از آن‌جا که $7\times11\times3=1001$ و هر یک از عبارات $a+f$، $b+d$ و $c+e$ بزرگ تر از ۱ هستند در نتیجه می‌شود که $\{a+f,b+d,c+e\}=\{7,11,13\}$ و لذا جواب مسأله برابر است با:

$$a+b+c+d+e+f=7+11+13=31$$

۶. [AMC12A ۲۰۰۵] از اعداد کوچک‌تر از ۱۰۰۰، $\left\lfloor\frac{999}{2}\right\rfloor=499$ تای آن‌ها بر ۲، $\left\lfloor\frac{999}{3}\right\rfloor=333$ تای آن‌ها بر۳ و $\left\lfloor\frac{999}{5}\right\rfloor=199$ تای آن‌ها بر ۵ بخشپذیرند. علاوه بر آن در بین اعداد ۱ تا ۱۰۰۰ $\left\lfloor\frac{999}{6}\right\rfloor=166$ مضرب ۶، $\left\lfloor\frac{999}{10}\right\rfloor=99$ مضرب ۱۰ و $\left\lfloor\frac{999}{15}\right\rfloor=66$ مضرب ۱۵ وجود دارد و $\left\lfloor\frac{999}{30}\right\rfloor=33$ عدد هم مضرب ۳۰ هستند. با استفاده از اصل شمول و عدم شمول

$$499+333+199-166-99-66+33=733$$

عدد حداقل بر یکی از اعداد ۲، ۳، ۵ بخشپذیرند از $999-733=266$ عدد باقیمانده، ۱۶۵ عدد، اعداد اول غیر از ۲،۳ و ۵ هستند. با توجه به این‌که ۱ نه اول است نه مرکب؛ بنابراین دقیقاً ۱۰۰ عدد شبه اول در بین اعداد ۱ تا ۱۰۰۰ وجود دارد.

۷. اصل لانه کبوتری راه حل زیبایی برای این مسأله دارد. هیچ نگرانی در استفاده از این اصل وجود ندارد وقتی که بی‌نهایت کبوتر می‌خواهند در تعداد محدودی لانه بنشینند.

برای هر $i=1,2,\ldots,k-1$، مجموعه اعداد اول هم‌نهشت با i به پیمانه k را با P_i نشان می‌دهیم. هر عدد اول (بجز خود k که ممکن است اول باشد) دقیقاً در یکی از مجموعه‌های $P_1,P_2,\ldots,P_{k-1}$ حضور دارد. چون بی‌نهایت عدد اول وجود دارد حداقل یکی از این مجموعه‌ها مثلاً P_i نامتناهی است. فرض کنید $p=x_1<x_2<x_n<\ldots$ اعضای آن باشند که به ترتیب صعودی مرتب شده‌اند و

$$a_n=\frac{x_{n+1}-p}{k}\quad(\text{برای هر عدد صحیح مثبت } n)$$

بنابراین $p+ka_n$ اعضای P_i با شروع از x_2 را تولید می‌کند که در آن اعداد a_n صحیح مثبت هستند. عدد اول p و دنباله اکیداً صعودی $a_1, a_2, \ldots, a_n, \ldots$ خاصیت مورد نظر مسأله را دارا می‌باشند.

۸. [AIME ۱۹۹۴] همه‌ی اعداد صحیح مثبت کوچک تر از ۱۰۰۰ را سه رقمی در نظر بگیرید. برای اعداد کمتر از سه رقم، از رقم صفر در سمت چپ آن استفاده می‌کنیم. مجموع حاصل‌ضرب ارقام همه‌ی این اعداد برابر است با

$$(0\times0\times0+0\times0\times1+\cdots+9\times9\times9)-0\times0\times0=(0+1+\ldots+9)^3-0$$

اما $p(n)$ حاصل‌ضرب ارقام غیرصفر n است. مجموع این حاصل‌ضرب‌هارا می‌توان با جایگزین کردن ۱ به جای ۰ در عبارت بالا بدست آورد. زیرا چشم‌پوشی از صفرها معادل این است که در ضرب بجای ۰ از ۱ استفاده شده است. (توجه کنید که آخرین صفر در عبارت فوق نیز ۱ می‌شود و این کار اثر عدد ۰۰۰ که به ۱۱۱ تبدیل شده است را خنثی می‌کند.) بنابراین

$$S=46^3-1=(46-1)(46^2+46+1)=3^3\times5\times7\times103$$

و بزرگ ترین عامل اول آن ۱۰۳ است.

۹. [۱۹۹۴ روسیه] **اثبات اول:** قرار می‌دهیم $d=\gcd(m,n)$ و می‌نویسیم $m=ad$ و $n=bd$ که $\gcd(a,b)=1$ و

$$\operatorname{lcm}(m,n)=\frac{mn}{\gcd(m,n)}=abd$$

معادله داده شده به صورت $abd+d=ad+bd$ و یا $ab-a-b+1=0$ در می‌آید. بنابراین $(a-1)(b-1)=0$. در نتیجه $a=1$ یا $b=1$ و به عبارت دیگر $n=bd=bm$ و $m=d$ یا $m=an$ و $n=d$.

اثبات دوم: از $\operatorname{lcm}(m,n)\times\gcd(m,n)=mn$ و فرض مسأله نتیجه می‌شود که $\operatorname{lcm}(m,n)$ و $\gcd(m,n)$ همانند m و n ریشه‌های معادله $x^2-(m+n)x+mn=0$ هستند؛ یعنی $\{\gcd(m,n),\operatorname{lcm}(m,n)\}=\{m,n\}$ که از آن حکم مسأله نتیجه می‌شود.

۱۰. [AIME۱۹۹۵] **پاسخ اول:** فرض کنید $n=p^rq^s$ باشد که p و q اعداد اول متمایز هستند. بنابراین $n^2=p^{2r}q^{2s}$ و لذا n^2

$$(2r+1)(2s+1)$$

مقسوم علیه دارد. برای هر مقسوم علیه کوچک‌تر از n یک مقسوم‌علیه بزرگ‌تر از n متناظر با آن وجود دارد با خارج کردن n از مقسوم‌علیه‌ها، به تعداد

$$\frac{(2r+1)(2s+1)-1}{2}=2rs+r+s$$

مقسوم علیه n^2 از n کوچک‌تر هستند. از آن‌جا که n، $(r+1)(s+1)$ مقسوم علیه (شامل خودش) دارد و چون هر مقسوم‌علیه n، یک مقسوم‌علیه n^2 نیز هست بنابراین

$$2rs + r + s - [(r+1)(s+1) - 1] = rs$$

مقسوم علیه n^2 کوچک‌تر از n بوده و n را نمی‌شمارند. حال با $r = 31$ و $s = 19$ جواب مسأله $rs = 589$ خواهد بود.

پاسخ دوم: یک مقسوم‌علیه مثبت d از n^2 کوچک‌تر از n بوده اما n را نمی‌شمارد اگر و فقط اگر

$$d = \begin{cases} 2^{31+a} \times 3^{19-d} & \text{اگر } 2^a < 3^b \\ 2^{31-a} \times 3^{19+b} & \text{اگر } 2^a > 3^b \end{cases}$$

که a و b اعداد صحیح هستند که $1 \le a \le 31$ و $1 \le b \le 19$. چون برای اعداد صحیح مثبت a و b $2^a \neq 3^b$، لذا $589 = 19 \times 31$ مقسوم علیه با ویژگی مورد نظر وجود دارد.

۱۱. [APMO 1998] می‌نویسیم $a = 2^c \times p$ و $b = 2^d \times q$ که p و q فرد هستند. بدون از دست دادن کلیت مسأله فرض کنید که $c \ge d$ آنگاه

$$36a + b = 36 \times 2^c \times p + 2^d q = 2^d (36 \times 2^{c-d} \times p + q)$$

و در نتیجه

$$(36a+b)(36b+a) = 2^d (36 \times 2^{c-d} \times p + q)(36b + a)$$

که دارای عامل فرد $36 \times 2^{c-d} \times p + q$ است و بنابراین نمی‌تواند توانی از ۲ باشد.

۱۲. برای عدد صحیح مثبت n، $p(n)$ را برابر بزرگ‌ترین مقسوم‌علیه فرد n می‌گیریم. می‌توان نوشت $p(n)$. $n = 2^k$ که k عدد صحیح نامنفی است. اگر دو عدد صحیح مثبت n_1 و n_2 چنان باشند که $p(n_2) = p(n_1)$ آنگاه یکی از آنها حداقل دو برابر دیگری است.
چون هیچ یک از اعداد $2007, 2008, \ldots, 4012$ دو برابر عدد دیگری در این دنباله نیست بنابراین $p(2007), p(2008), \ldots, p(4012)$ همگی اعداد فرد متمایز هستند. این اعداد فرد به مجموعه $\{1, 3, 5, \ldots, 4011\}$ تعلق دارند که دقیقاً ۲۰۰۶ عضو دارد. در نتیجه

$$\{p(2007), p(2008), \ldots, p(4012)\} = \{1, 3, 5, \ldots, 4011\}$$

به این ترتیب مجموع خواسته شده برابر است با

$$p(2006) + 1 + 3 + \cdots + 4011 = 1003 + 2006^2$$
$$= 1003 \times 4013 = 4025039$$

۱۳. چون $27000 = 2^3 \times 3^3 \times 5^3$، هر a/b را می‌توان به شکل $2^a 3^b 5^c$ نوشت که a, b و c اعداد صحیح متعلق به بازه $[-3, 3]$ هستند. به این ترتیب هر a/b دقیقاً یکبار در عبارت زیر ظاهر می‌شود.

$$(۲^{-۳}+۲^{-۲}+\ldots+۲^{۳})\,(۳^{-۳}+۳^{-۲}+\ldots+۳^{۳})\,(۵^{-۳}+۵^{-۲}+\ldots+۵^{۳})$$

بنابراین مجموع خواسته شده برابر است با:

$$\frac{۱}{۲^{۳}\times۳^{۳}\times۵^{۳}}\cdot\frac{۲^{۷}-۱}{۲-۱}\cdot\frac{۳^{۷}-۱}{۳-۱}\cdot\frac{۵^{۷}-۱}{۵-۱}=\frac{(۲^{۷}-۱)\,(۳^{۷}-۱)\,(۵^{۷}-۱)}{۲^{۶}\times۳^{۳}\times۵^{۳}}$$

۱۴. ما دو روش متفاوت برای این دو بخش ارایه می‌کنیم. برای بخش (۱) با ب.م.م و ک.م.م سه عدد صحیح از طریق ب.م.م و ک.م.م دو به دوی آنها کار می‌کنیم ولی بخش (۲) را از طریق تجزیه به عوامل اول پیش می‌بریم.

(۱) [AIME ۱۹۸۷] چون ۱۰۰۰ و ۲۰۰۰ هر دو به شکل $۲^{m}۵^{n}$ هستند، اعداد a,b و c نیز باید به این شکل باشند. قرار می‌دهیم

$$a=۲^{m_۱}۵^{n_۱},\quad b=۲^{m_۲}۵^{n_۲},\quad c=۲^{m_۳}۵^{n_۳}$$

که m_i و n_i برای $i=۱,۲,۳$ اعداد صحیح نامنفی هستند. بنابراین تساوی‌های زیر باید برقرار باشند

$$(*)\qquad \max=(m_۱,m_۲)=۳\ ,\ \max(m_۲,m_۳)=۴\ ,\ \max(m_۳,m_۱)=۴$$

و

$$(**)\quad \max\{n_۱,n_۲\}=۳\ ,\ \max\{n_۲,n_۳\}=۳\ ,\ \max\{n_۳,n_۱\}=۳$$

از (*) در می‌یابیم که $m_۳=۴$ و از $m_۱$ و $m_۲$ یکی برابر ۳ بوده و دیگری هر یک از مقادیر ۰,۱,۲,۳ را می‌تواند داشته باشد. بنابراین ۷ سه‌تایی مرتب به این صورت خواهیم داشت که عبارتند از:

$$(۳,۰,۴),(۳,۱,۴),(۳,۲,۴),(۳,۳,۴),(۲,۳,۴)\ ,\ (۱,۳,۴),(۰,۳,۴)$$

برای برقراری (**) دو تا از $n_۱,n_۲$ و $n_۳$ باید ۳ باشند در حالی‌که سومی می‌تواند هر یک از مقادیر ۰,۱,۲,۳ را داشته باشد. بنابراین ۱۰ سه تایی مرتب به این صورت خواهیم داشت که عبارتند از:

$$(۳,۳,۰),(۳,۳,۱),(۳,۳,۲),(۳,۰,۳),(۳,۱,۳),(۳,۲,۳),(۰,۳,۳),(۱,۳,۳),(۲,۳,۳),(۳,۳,۳)$$

چون انتخاب $(m_۱,m_۲,m_۳)$ مستقل از انتخاب $(n_۱,n_۲,n_۳)$ است به $۷\times۱۰=۷۰$ طریق می‌توان آنها را انتخاب کرد که همان تعداد سه‌تایی‌های مرتب مورد نظر مسأله است.

(۲) فرض کنید $a=p_۱^{\alpha_۱}\ldots p_n^{\alpha_n}$, $b=p_۱^{\beta_۱}\ldots p_n^{\beta_n}$, $c=p_۱^{\gamma_۱}\ldots p_n^{\gamma_n}$ که $p_۱,\ldots,p_n$ اعداد اول متمایز و $\alpha_۱,\ldots,\alpha_n$, $\beta_۱,\ldots,\beta_n$, $\gamma_۱,\ldots,\gamma_n$ اعداد صحیح نامنفی هستند. بنابراین

$$\frac{lcm\,(a,b,c)^{۲}}{lcm\,(a,b)\,lcm\,(b,c)\,lcm\,(c,a)}=$$

$$= \frac{\prod_{i=1}^{n} p_i^{2\max\{\alpha_i,\beta_i,\gamma_i\}}}{\prod_{i=1}^{n} p_i^{\max\{\alpha_i,\beta_i\}} \prod_{i=1}^{n} p_i^{\max\{\beta_i,\gamma_i\}} \prod_{i=1}^{n} p_i^{\max\{\gamma_i,\alpha_i\}}}$$

$$= \prod_{i=1}^{n} p_i^{2\max\{\alpha_i,\beta_i,\gamma_i\}-\max\{\alpha_i,\beta_i\}-\max\{\beta_i,\gamma_i\}-\max\{\gamma_i,\alpha_i\}}$$

و

$$\frac{\gcd(a,b,c)^2}{\gcd(a,b)\gcd(b,c)\gcd(c,a)} =$$

$$= \frac{\prod_{i=1}^{n} p_i^{2\min\{\alpha_i,\beta_i,\gamma_i\}}}{\prod_{i=1}^{n} p_i^{\min\{\alpha_i,\beta_i\}} \prod_{i=1}^{n} p_i^{\min\{\beta_i,\gamma_i\}} \prod_{i=1}^{n} p_i^{\min\{\gamma_i,\alpha_i\}}}$$

$$= \prod_{i=1}^{n} p_i^{2\min\{\alpha_i,\beta_i,\gamma_i\}-\min\{\alpha_i,\beta_i\}-\min\{\beta_i,\gamma_i\}-\min\{\gamma_i,\alpha_i\}}$$

حال کافی است نشان دهیم برای همه‌ی اعداد صحیح نامنفی α,β,γ رابطه زیر برقرار است

$$2\max\{\alpha,\beta,\gamma\}-\max\{\alpha,\beta\}-\max\{\beta,\gamma\}-\max\{\gamma,\alpha\} =$$
$$= 2\min\{\alpha,\beta,\gamma\}-\min\{\alpha,\beta\}-\min\{\beta,\gamma\}-\min\{\gamma,\alpha\}$$

از تقارن می‌توانیم فرض کنیم که $\alpha \le \beta \le \gamma$ و به سادگی می‌توان دید که دو طرف رابطه‌ی فوق برابر $-\beta$ است و اثبات تکمیل می‌شود.

به عنوان یک نتیجه جانبی از اثبات (۲) می‌توان بیان کرد که

$$\frac{\gcd(a,b)\gcd(b,c)\gcd(c,a)}{\gcd(a,b,c)^2} \quad \text{و} \quad \frac{\operatorname{lcm}(a,b)\operatorname{lcm}(b,c)\operatorname{lcm}(c,a)}{\operatorname{lcm}(a,b,c)^2}$$

اعداد صحیح مساوی هستند.

۱۵. (۱) [UK ۱۹۹۸] قرار می‌دهیم $x=ha, y=hb, z=hc$ که a,b و c اعداد صحیح مثبت بوده و $\gcd(a,b,c)=1$. فرض کنید $\gcd(a,b)=g$ بنابراین $a=ga', b=gb'$ و a' و b' اعداد صحیح مثبت هستند که

$$\gcd(a',b')=\gcd(a'-b',b')=\gcd(a',a'-b')=1$$

داریم

$$\frac{1}{a}-\frac{1}{b}=\frac{1}{c} \Leftrightarrow c(b-a)=ab \Leftrightarrow c(b'-a')=a'b'g$$

بنابراین چون $\gcd(g,c)=1$ است خواهیم داشت $g=b'-a'$ و $c=a'b'$ و لذا

$$h(y-x)=h^{۲}(b-a)=h^{۲}g(b'-a')=h^{۲}g^{۲}=(hg)^{۲}$$

و

$$hxyz=h^{۴}abc=h^{۴}g^{۲}a'b'c=h^{۴}g^{۲}c^{۲}=(h^{۲}gc)^{۲}$$

که هر دو عدد مربع کامل هستند.

۱۶. مسأله را بطور غیرمستقیم اثبات می‌کنیم. فرض کنید a, p را نمی‌شمارد. چون p , $a^{۲}+ab+b^{۲}$ را می‌شمارد بنابراین $a^{۳}-b^{۳}=(a-b)(a^{۲}+ab+b^{۲})$ را نیز می‌شمارد. لذا $a^{۳}\equiv b^{۳}$ (پیمانه p) و از آنجا

$$a^{۳k}\equiv b^{۳k} \quad (\text{پیمانه } p)$$

پس p , b را هم نمی‌شمارد. از قضیه کوچک فرما داریم $a^{p-۱}\equiv b^{p-۱}\equiv ۱$ (پیمانه p) یا

$$a^{۳k+۱}\equiv b^{۳k+۱} \quad (\text{پیمانه } p)$$

چون p نسبت به a اول است نتیجه می‌گیریم که $a\equiv b$ (پیمانه p) این نتیجه در ترکیب با رابطه $a^{۲}+ab+b^{۲}\equiv ۰$ (پیمانه p) به این معناست که $۳^{۲}a\equiv ۰$ (پیمانه p) که چون $p\neq ۳$ بنابراین p باید a را بشمارد که تناقض است.

۱۷. [HMMT ۲۰۰۵]

از آنجایی که $x^{۳}+۱=(x+۱)(x^{۲}-x+۱)$ و $(x^{۲}-y^{۲})=(x+y)(x-y)$ در نتیجه

$$\begin{aligned}۲۷۰۰۰۰۰۱&=۳۰۰^{۳}+۱=(۳۰۰+۱)(۳۰۰^{۲}-۳۰۰+۱)\\&=۳۰۱\times(۳۰۰^{۲}+۲\times۳۰۰+۱-۹۰۰)\\&=۳۰۱\times[(۳۰۰+۱)^{۲}-۹۰۰]=۳۰۱\times(۳۰۱^{۲}-۳۰^{۲})\\&=۳۰۱\times۳۳۱\times۲۷۱=۷\times۴۳\times۲۷۱\times۳۳۱\end{aligned}$$

بنابراین جواب مسأله برابر است با: $۶۵۲=۳۳۱+۲۷۱+۴۳+۷$

۱۸. **پاسخ اول:** تنها جواب $n=۵$ است.

به سادگی می‌توان بررسی کرد که به ازای $n=۱,۲,۳,۴,۶,۷,۸,۹$, $n!+۵$ مکعب کامل نیست و $۵!+۵$ مکعب کامل است. اگر $n!+۵$ برای $n>۹$ مکعب کامل باشد از آنجا که مضرب ۵ است، باید مضرب ۱۲۵ باشد. اما این نمی‌تواند برقرار باشد زیرا! n برای $n>۹$ مضرب ۲۵ است ولی ۵ مضرب ۲۵ نیست. بنابراین تنها عدد صحیح مثبت با خاصیت مطلوب $n=۵$ است.

پاسخ دوم: مجدداً حالات $n=۱,۲,...,۶$ را مستقیماً بررسی می‌کنیم. برای $n\geq ۷$، (پیمانه ۷) $n!+۵\equiv ۵$ که در زمره مانده‌های یک مکعب کامل به پیمانه ۷ قرار نمی‌گیرد (تنها دسته مانده‌های یک مکعب کامل به پیمانه ۷، ۰ و ۱± هستند)

۱۹. [۱۹۹۵ روسیه] برای $p \neq 3$، (پیمانه ۳) $p^2 \equiv 1$ و بنابراین $3 \mid p^2+11$. بطور مشابه برای $p \neq 2$، (پیمانه ۴) $p^2 \equiv 1$ و $4 \mid p^2+11$. بنابراین بجز در این دو حالت $12 \mid p^2+11$. از آنجایی که ۱۲ خودش ۶ مقسوم‌علیه متمایز دارد $\{1,2,3,4,6,12\}$ و برای $p>1$, $p^2+11>12$، نتیجه می‌گیریم که p^2+11 باید بیش از ۶ مقسوم‌علیه داشته باشد. تنها حالات باقی مانده $p=2$ و $p=3$ هستند که آنها را بررسی می‌کنیم. اگر $p=2$ آنگاه $p^2+11=15$ که فقط ۴ مقسوم‌علیه دارد $\{1,3,5,15\}$. اگر $p=3$ آنگاه $p^2+11=20$ که ۶ مقسوم‌علیه دارد $\{1,2,4,5,10,20\}$. بنابراین $p=3$ تنها جواب مسأله است.

۲۰. [AIME ۲۰۰۱] فرض کنید $a_k \times 7^k + a_{k-1} \times 7^{k-1} + m + a_2 \times 7^2 + a_1 \times 7^1 + a_0$ یک عدد دوبل $7-10$ باشد که $a_k \neq 0$. از طرف دیگر

$$a_k \times 10^k + a_{k-1} \times 10^{k-1} + m + a_2 \times 10^2 + a_1 \times 10 + a_0$$

دو برابر عدد مذکور است لذا:

$$a_k \times (10^k - 2 \times 7^k) + a_{k-1} \times (10^{k-1} - 2 \times 7^{k-1}) + \cdots + a_1 \times (10 - 2 \times 7) + a_0 \times (1-2) = 0$$

چون ضرایب a_i ها فقط به ازای $i=0$ و $i=1$ منفی هستند لذا k حداقل ۲ است. از آنجا که ضرایب a_i حداقل برابر ۳۱۴ است (وقتی که $i>2$) و از آنجا که هیچ a_i بیشتر از ۶ نیست در نتیجه $k=2$ و $2a_2 = 4a_1 + a_0$. برای بدست آوردن بزرگ‌ترین عدد دوبل $7-10$ ابتدا با $a_2 = 6$ شروع می‌کنیم. معادله‌ی $4a_1 + a_0 = 12$ برای بزرگ‌ترین مقدار a_1 پاسخی معادل $a_1 = 3$ و $a_0 = 0$ دارد. بنابراین بزرگ ترین عدد دوبل $7-10$ برابر $315 = 7 \times 3 + 49 \times 6$ است.

۲۱. از (پیمانه n) $a \equiv b$ نتیجه می‌گیریم که برای یک عدد صحیح q , $a = b + nq$. از قضیه دو جمله‌ای داریم:

$$\begin{aligned} a^n - b^n &= (b+nq)^n - b^n \\ &= \binom{n}{1} b^{n-1} qn + \binom{n}{2} b^{n-2} q^2 n^2 + \cdots + \binom{n}{n} q^n n^n \\ &= n^2 \left(b^{n-1} q + \binom{n}{2} b^{n-2} q^2 + \cdots + \binom{n}{n} q^n n^{n-2} \right) \end{aligned}$$

بنابراین (پیمانه n^2) $a^n \equiv b^n$.

عکس این مطلب صحیح نیست. بطور مثال (پیمانه ۴) $1^4 \equiv 3^4$ اما (پیمانه ۴) $1 \not\equiv 3$.

۲۲. **اثبات اول:** از استقرا روی k استفاده می‌کنیم. حکم به وضوح برای $k=1$ برقرار است زیرا

$$\binom{p-1}{1} = p-1 \equiv -1 \quad (\text{پیمانه } p)$$

فرض می‌کنیم که حکم برای $k = i - ۱$ صحیح است که $۱ \le i \le p - ۱$. رابطه زیر شناخته شده است (و به سادگی با محاسبه مستقیم نیز می‌توان درستی آن را بررسی کرد)

$$\binom{p-۱}{i} + \binom{p-۱}{i-۱} = \binom{p}{i}$$

از نتیجه ۱. ۱۰ داریم

$$\binom{p-۱}{i} + \binom{p-۱}{i-۱} \equiv ۰ \pmod{p} \quad \text{(پیمانه } p\text{)}$$

از فرض استقرا داریم (پیمانه p) $\binom{p-۱}{i} \equiv -\binom{p-۱}{i-۱} \equiv -(-۱)^{i-۱} \equiv (-۱)^{i}$ و استقرا کامل می‌شود.

اثبات دوم: از آنجا که $\binom{p-۱}{k} = \dfrac{(p-۱)(p-۲)\dots(p-k)}{k!}$ یک عدد صحیح است و $\gcd(k!, p) = ۱$ کافی است نشان دهیم (پیمانه p) $(p-۱)(p-۲)\dots(p-k) \equiv (-۱)^k k!$ که بدیهی است.

۲۳. اگر $p = ۲$ باشد p، عدد $۲^n - n$ را برای هر عدد صحیح مثبت زوج n می‌شمارد. فرض می‌کنیم p فرد باشد. از قضیه کوچک فرما داریم (پیمانه p) $۲^{p-۱} \equiv ۱$ در نتیجه

$$۲^{(p-۱)^{۲k}} \equiv ۱ \equiv (p-۱)^{۲k} \quad \text{(پیمانه } p\text{)}$$

به عبارت دیگر p , $۲^n - n$ را برای $n = (p-۱)^{۲k}$ می‌شمارد.

۲۴. برای $n = ۴$ داریم $۱! + ۲! + ۳! + ۴! = ۳۳$ که توان کامل نیست. برای $k \ge ۵$ (پیمانه ۱۰) $k! \equiv ۰$ و لذا برای $n \ge ۵$

$$۱! + ۲! + ۳! + ۴! + \dots + n! \equiv ۳ \quad \text{(پیمانه ۱۰)}$$

بنابراین نمی‌تواند مربع کامل و یا یک توان زوج باشد.

برای توان‌های فرد، استدلالی که در ادامه می‌آید در همه موارد برقرار است: حکم را می‌توان برای $n < ۹$ بطور مستقیم بررسی کرد. برای $k \ge ۹$, $k!$ مضربی از ۲۷ است در حالی‌که $۸! + \dots + ۲! + ۱!$ مضربی از ۹ است ولی مضربی از ۲۷ نیست. بنابراین $n! + \dots + ۲! + ۱!$ نمی‌تواند یک مکعب یا توان بالاتر باشد.

۲۵. دو حالت را بررسی می‌کنیم.

در حالت اول فرض می‌کنیم n فرد است و می نویسیم $n = ۲m + ۱$ در این صورت $۱ + ۲ + ۳ + \dots + n = (m+۱)(۲m+۱)$. داریم:

$$1^k + 2^k + \cdots + n^k$$
$$= 1^k + 2^k + \cdots + (2m+1)^k$$
$$= [1^k + (2m+1)^k] + [2^k + (2m)^k] + \cdots + [m^k + (m+2)^k] + (m+1)^k$$

از آنجا که k فرد است $(x+y)$ یک عامل $x^k + y^k$ می‌باشد. بنابراین $2m+2$ $i^k + (2m+2-i)^k$ را برای $i = 1,\ldots,m$ می‌شمارد. در نتیجه $m+1$, $1^k + 2^k + \ldots + n^k$ را می‌شمارد. بطور مشابه داریم

$$1^k + 2^k + \cdots + n^k$$
$$= 1^k + 2^k + \cdots + (2m+1)^k$$
$$= [1^k + (2m)^k] + [2^k + (2m-1)^k] + \cdots + [m^k + (m+1)^k] + (2m+1)^k$$

که چون $2m+1$, $i^k + (2m+1-i)^k$ را برای $i = 1,2,\ldots,m$ می‌شمارد در نتیجه $2m+1$ $n^k + \cdots + 2^k + 1^k$ را می‌شمارد. تا اینجا نشان داده‌ایم که $m+1$ و $2m+1$ هر دو $n^k + \cdots + 2^k + 1^k$ را می‌شمارند. از آنجا که $\gcd(m+1, 2m+1) = 1$، نتیجه می‌گیریم که $(m+1)(2m+1)$، $n^k + \cdots + 2^k + 1^k$ را می‌شمارد.

در حالت دوم فرض می‌کنیم n زوج است. اثبات، مشابه حالت اول است که آن را به خواننده می‌سپاریم.

۲۶. فرض کنید برای عدد صحیح مثبت q, $p - 4 = q^4$ بنابراین $p = q^4 + 4$, $q > 1$. داریم:

$$p = q^4 + 4q^2 + 4 - 4q^2 = (q^2+2)^2 - (2q)^2$$
$$= (q^2 - 2q + 2)(q^2 + 2q + 2)$$

حاصلضرب دو عدد بزرگ تر از ۱، با اول بودن p تناقض دارد (توجه کنید که برای $p > 5$, $q > 1$ است و بنابراین $(q-1)^2 = q^2 - 2q + 1 > 0$ یا $q^2 - 2q + 2 > 1$).

۲۷. i امین عدد در مجموع سمت چپ عبارت مورد نظر، مجموع همه مقسوم‌علیه‌های i است. اگر همه‌ی این اعداد را به صورت تفکیک شده بنویسیم، هر عدد d $(1 \le d \le n)$, $\left\lfloor \frac{n}{d} \right\rfloor$ بار ظاهر می‌شود. بنابراین سمت چپ نامساوی مورد نظر برابر است با

$$1 \times \left\lfloor \frac{n}{1} \right\rfloor + 2 \times \left\lfloor \frac{n}{2} \right\rfloor + 3 \times \left\lfloor \frac{n}{3} \right\rfloor + \ldots + n \times \left\lfloor \frac{n}{n} \right\rfloor$$
$$\le 1 \times \frac{n}{1} + 2 \times \frac{n}{3} + 3 \times \frac{n}{3} + \ldots + n \times \frac{n}{n} = n^2$$

۲۸. [APMO ۲۰۰۴] جواب $S = \{2\}$ است.

ابتدا با قرار دادن $i=j$ در شرط داده شده بدست می‌آید که $\frac{i+j}{\gcd(i,j)}=\frac{۲i}{i}=۲$ در S است ادعا می‌کنیم که دیگر هیچ عضوی در S وجود ندارد. فرض کنید S اعضای دیگری غیر از ۲ دارد. s را کوچک‌ترین عضو S که برابر ۲ نیست در نظر می‌گیریم.

اگر s فرد باشد، آنگاه $\frac{s+۲}{\gcd(s,۲)}=s+۲$ عضو فرد دیگری در S است. بنابراین به این ترتیب بی‌نهایت عدد فرد عضو S خواهند بود که با فرض متناهی بودن S تناقض دارد.

بنابراین s باید زوج باشد و لذا $s>۲$. پس $\frac{s+۲}{\gcd(s,۲)}=\frac{s}{۲}+۱$ نیز در S است. برای $s>۲$ $۲<\frac{s}{۲}+۱<s$ که با فرض کوچک ترین عضو بودن S در تضاد است.

توجه: چه اتفاقی می‌افتاد اگر i و j در شرط داده شده متمایز بودند؟ Kevin Modzelewsla نشان داده است که جواب، همه مجموعه‌های به شکل $\{a+۱,a(a+۱)\}$ که a یک عدد صحیح مثبت است، می‌باشد. اثبات به عهده خواننده.

۲۹. توجه کنید که (پیمانه ۹) $۲^۳\equiv -۱$ و بنابراین (پیمانه ۹) $۲^{۲۹}\equiv (۲^۳)^۹\times ۲^۲\equiv -۴\equiv ۵$. یک عدد ده رقمی شامل همه‌ی ارقام ۰ تا ۹ مضربی از ۹ است زیرا مجموع ارقام آن، چنین است. بنابراین در عدد ۹رقمی مورد بحث، ۴ وجود ندارد. $(۲^{۲۹}=۵۳۶۸۷۰۹۱۲)$

۳۰. عبارت داده شده به صورت زیر تجزیه می‌شود

$$n^۵+n^۴+۱=n^۵+n^۴-n^۳-n^۳-n^۲-n+n^۲+n+۱$$
$$=(n^۲+n+۱)(n^۳-n+۱)$$

بنابراین برای $n>۱$، عبارت مورد نظر حاصلضرب ۲ عدد صحیح بزرگ‌تر از ۱ است.

با داشتن اطلاعات کمی در اعداد مختلط می‌توان دلیل دیگری برای این تجزیه ارائه کرد. می‌دانیم $۱, w$ و $w^۲$ سه ریشه معادله $x^۳-۱=(x-۱)(x^۲+x+۱)=۰$ هستند که $w=-\frac{۱}{۲}+\frac{\sqrt{۳}}{۲}i=cis\,۱۲۰^\circ$. w و $w^۲$ ریشه‌های $x^۵+x^۴+۱=۰$ نیز هستند در نتیجه $n^۲+n+۱$ باید یک عامل $n^۵+n^۴+۱$ باشد. با توجه به این استدلال می‌توان اعداد ۴ و ۵ در عبارت مطرح شده در این مسأله را با هر زوج از اعداد صحیح مثبت که به پیمانه ۳ با ۱ و ۲ همنهشت هستند جایگزین کرد.

۳۱. [۱۹۹۵ مجارستان] واضح است که ۲، ۵ و حداقل یک عدد اول دیگر باید در میان اعداد اول باشند. فرض کنید $p_۱\le p_۲\le\cdots\le p_n$ اعداد اول دیگر باشند. از شرط داده شده نتیجه می‌گیریم

$$(*)\qquad p_۱+p_۲+\ldots+p_n+۷=p_۱p_۲\cdots p_n$$

حاصل‌ضرب هر مجموعه‌ای از اعداد (که هریک حداقل برابر۲ هستند) باید حداقل به اندازه مجموعشان باشد. اثبات این مطلب برای ۲ عدد x و y به صورت زیر است

$$0 \le (x-1)(y-1)-1 = xy - x - y$$

و نتیجه کلی با بکار بردن متوالی این حقیقت به صورت زیر به دست می‌آید

$$x_1x_2\cdots x_k \ge x_1x_2\cdots x_{k-1} + x_k \ge \cdots \ge x_1 + x_2 + \cdots + x_k$$

در این مسأله داریم

$$p_1 + p_2 + \cdots + p_n + 1 = p_1p_2\cdots p_n \ge (p_1 + p_2 + \cdots + p_{n-1})p_n$$

با قرار دادن $s = p_1 + p_2 + \cdots + p_{n-1}$، معادله اخیر را می‌توان به صورت $s + p_n + 1 \ge sp_n$ و یا $(s-1)(p_n-1) \le 2$ نوشت. اگر عدد اول دیگری نباشد می‌توان s را برابر صفر قرار داد. اما در این حالت معادله (*) به صورت $p_n = p_n + 1$ در می‌آید که امکان ندارد. بنابراین $s \ge 2$ و $p_n - 1 \le 2$. تنها گزینه‌های ممکن برای برآورده ساختن این شرط $p_n = 2, 3, 5$ هستند.

اگر $p_n = 2$ آنگاه معادله (*) به صورت $2n + 1 = 2^n$ در می‌آید که به پیمانه ۲ غیرممکن است.
اگر $p_n = 3$ آنگاه $p_n - 1 = 2$ و بنابراین $s - 1 \le 4$. در این‌صورت $\{p_1, p_2, \ldots, p_{n-1}\}$ فقط می‌تواند برابر $\{2\}, \{3\}, \{2,2\}, \{2,3\}$ باشد. به آسانی با بررسی همه‌ی این حالات در می‌یابیم که هیچ‌کدام قابل قبول نیستند.
اگر $p_n = 5$ آنگاه $p_n - 1 = 4$ و بنابراین $s - 1 \le 2$. در این‌صورت اعداد اول دیگر یا یک ۲ و یا یک ۳ هستند. باز هم با یک بررسی ساده مشخص می‌شود که حالت دوم جواب است.
بنابراین اعداد اول مورد نظر این سؤال، مجموعه‌ی $\{2, 3, 5, 5\}$ هستند.

۳۲. [۱۹۹۵ روسیه] ۳۴۵۶ عدد جالب وجود دارد.
فرض کنید $n = abcdefghij$ یک عدد ۱۰ رقمی جالب باشد. ارقام n باید $0, 1, \ldots, 9$ باشند لذا به پیمانه ۹

$$n \equiv a+b+c+d+e+f+g+h+i+j \equiv 0+1+2+\cdots+9 \equiv 0$$

یعنی ۹، n را می‌شمارد. از آنجا که $\gcd(9, 11111) = 1$ در نتیجه $99999 = 9 \times 11111$ نیز n را می‌شمارد. فرض کنید $x = \overline{abcde}$ و $y = \overline{fghij}$ دو عدد ۵ رقمی باشند. داریم:
بنابراین $n = 10^5 x + y$

$$0 \equiv n \equiv 10^5 x + y \equiv x + y \quad (\text{پیمانه } 99999)$$

اما $0 < x + y < 2 \times 99999$ بنابراین n جالب است اگر و فقط اگر $x + y = 99999$ و یا به عبارت دیگر $a + f = \cdots = e + j = 9$.

$۱۲۰ = ۵!$ روش برای توزیع زوج‌های $(۰,۹), (۱,۸), \ldots, (۴,۵)$ بین $(a,f), (b,g), \ldots, (e,j)$ وجود دارد و برای هر زوج می‌توان جای ارقام را عوض کرد برای مثال (b,g) می‌تواند $(۰,۹)$ یا $(۹,۰)$ باشد. برای این کار نیز $۳۲ = ۲^۵$ روش وجود دارد بنابراین در کل ۱۲۰×۳۲ عدد موجود است. در یک دهم این اعداد $a = ۰$ که قابل قبول نیست. بنابراین $\frac{۹}{۱۰} \times ۳۲ \times ۱۲۰ = ۳۴۵۶$ عدد جالب وجود دارد.

۳۳. [۱۹۹۹ روسیه] جواب منفی است. از برهان خلف فرض کنید چنین اعدادی وجود دارد.
میانگین اعداد $\frac{۱۹۹۹}{۱۹} > ۱۰۶$ است. بنابراین یکی از اعداد حداکثر ۱۰۵ و مجموع ارقامش حداکثر ۱۸ (برای عدد ۹۹) است. هر عدد به پیمانه ۹ با مجموع ارقامش هم‌نهشت است. بنابراین همه‌ی اعداد و مجموع ارقامشان به پیمانه ۹ مثلاً با k هم‌نهشت هستند. در نتیجه (پیمانه۹) $k \equiv ۱۹k \equiv ۱۹۹۹ \equiv ۱$ و لذا مجموع ارقام ۱ یا ۱۰ است. اگر ۱ باشد، همه‌ی اعداد برابر $۱, ۱۰, ۱۰۰$ و یا ۱۰۰۰ بوده و به این ترتیب بعضی از آنها با هم برابر خواهند بود که قابل قبول نیست. بنابراین مجموع ارقام ۱۰ است. کوچک‌ترین ۲۰ عددی که مجموع ارقامشان ۱۰ است عبارتند از

$$۱۹, ۲۸, ۳۷, \ldots, ۹۱, ۱۰۹, ۱۱۸, ۱۲۷, \ldots, ۱۹۰, ۲۰۸$$

مجموع ۹ عدد اول

$$(۱۰ + ۲۰ + \ldots + ۹۰) + (۹ + ۸ + \ldots + ۱) = ۴۵۰ + ۴۵ = ۴۹۵$$

است. در حالی‌که مجموع ۹ عدد بعدی

$$۹۰۰ + (۱۰ + ۲۰ + \ldots + ۸۰) + (۹ + ۸ + ۷ + \ldots + ۱) = ۹۰۰ + ۳۶۰ + ۴۵ = ۱۳۰۵$$

است. بنابراین مجموع ۱۸ عدد ابتدایی ۱۸۰۰ است.
چون $۱۹۹۹ \neq ۱۹۰ + ۱۸۰۰$ لذا بزرگ‌ترین عدد در میان ۱۹ تا باید حداقل ۲۰۸ باشد. بنابراین کوچک‌ترین ۱۸ عدد با جمع حداقل ۱۸۰۰ مجموع کل حداقل $۲۰۰۸ > ۱۹۹۹$ را خواهد داشت که تناقض است.

۳۴. [۱۹۹۵ بلغارستان] به سادگی می‌توان بررسی کرد که مقادیر $(۱۳,۳)$ یا $(۳,۱۳), (۳,۳) = (p,q)$ جواب هستند. حال نشان می دهیم که این مقادیر تنها جواب‌های ممکن هستند. از تقارن فرض می‌کنیم $p \leq q$. از آنجا که $(۵^q - ۲^q)(۵^p - ۲^p)$ فرد است داریم $q \geq p \geq ۳$. اگر عدد اول k، $۵^k - ۲^k$ را بشمارد از قضیه کوچک فرما خواهیم داشت (پیمانه k) $۵^k - ۲^k \equiv ۵ - ۲ \equiv ۳$ و لذا $k = ۳$.
فرض کنید $p > ۳$. باتوجه به بحث فوق p، $۵^q - ۲^q$ را می‌شمارد و یا (پیمانه p) $۵^q \equiv ۲^q$. از قضیه کوچک فرما داریم (پیمانه p) $۵^{p-۱} \equiv ۲^{p-۱}$ و از نتیجه ۲۳.۱

$$۵^{\gcd(p-۱,q)} \equiv ۲^{\gcd(p-۱,q)} \quad \text{(پیمانه } p\text{)}$$

چون $q \geq p$ لذا $\gcd(p-1,q)=1$ و رابطه همنهشتی اخیر به صورت (پیمانه p) $2 \equiv 5$ در می‌آید. درنتیجه $p=3$ که تناقض است.

بنابراین $p=3$. اگر $q>3$، آنگاه q باید $13 \times 9 = 3^3 - 3^3 = 5^p - 2^p$ را بشمارد و بنابراین $q=13$ که منجر به پاسخ $(p,q)=(3,13)$ می‌شود.

۳۵. برای عدد صحیح مثبت n تعریف می‌کنیم

$$a_n = \underbrace{11\ldots1}_{3^n}$$

کافی است نشان دهیم که برای همه اعداد صحیح مثبت n، a_n بر مجموع ارقامش بخشپذیر است یعنی a_n بر 3^n بخشپذیر است. از استقرا روی n استفاده می‌کنیم. برای $n=1$ واضح است که $a_1=111$ بر ۳ بخشپذیر است. فرض کنید برای عدد صحیح مثبت $n=k$، a_n بر 3^n بخشپذیراست. a_{k+1} را مورد بررسی قرار می دهیم.

$$a_{k+1} = \underbrace{11\ldots1}_{3^{k+1}} = \underbrace{11\ldots1}_{3^k \times 3} = \underbrace{11\ldots1}_{3^k}\underbrace{11\ldots1}_{3^k}\underbrace{11\ldots1}_{3^k}$$

$$= \underbrace{11\ldots1}_{3^k} \times (10^{2\times 3^k} + 10^{3^k} + 1)$$

$$= a_k \times 1\underbrace{00\ldots0}_{3^k-1}1\underbrace{00\ldots0}_{3^k-1}1$$

چون ۳، $1\underbrace{00\ldots0}_{3^k-1}1\underbrace{00\ldots0}_{3^k-1}1$ را شمرده و a_k بر 3^k بخشپذیر است، در نتیجه 3^{k+1}، a_{k+1} را می‌شمارد و استقرا تکمیل می‌شود.

۳۶. عدد N با چنین خاصیتی رامی‌توان به صورت زیر نوشت

$$N = k\,\frac{10^{2^n}-1}{10-1} = k\,(10+1)(10^2+1)\ldots(10^{2^{n-1}}+1)$$

نتیجه مطلوب مسأله با توجه به اینکه در تجزیه فوق n عامل $10^{2^h}+1$ $(h=0,1,\ldots,n-1)$ دو به دو نسبت به هم اول هستند، بدست می‌آید. اگر $h_1 > h_2$ آنگاه

$$10^{2^{h_2}}+1 \mid 10^{2^{h_1}}-1 = 9\times(10+1)(10^2+1)\ldots(10^{2^{h_2}}+1)\ldots(10^{2^{h_1-1}}+1)$$

بنابراین

$$\gcd(10^{2^{h_2}}+1, 10^{2^{h_1}}+1) = \gcd(10^{2^{h_1}}-1, 10^{2^{h_1}}+1) = \gcd(2, 10^{2^{h_1}}+1) = 1$$

توجه: روش دیگری برای اثبات $\gcd(10^{2^{h_2}}+1, 10^{2^{h_1}}+1)=1$ وجود دارد. اگر p، $10^{2^{h_2}}+1$ را بشمارد، p باید فرد باشد. از (پیمانه p) $10^{2^{h_2}} \equiv -1$ نتیجه می‌شود که

$$10^{2^{h_1}} \equiv (10^{2^{h_2}})^{2^{h_1-h_2}} \equiv (-1)^{2^{h_1-h_2}} \equiv 1 \quad (\text{پیمانه } p)$$

بنابراین p، $10^{2^{h_1}}-1$ را می‌شمارد و چون $p \nmid 2$ لذا $10^{2^{h_1}}+1$ را نمی‌شمارد.

۳۷. **اثبات اول:** در این روش از خواص روابط هم‌نهشتی خطی استفاده می‌کنیم.

(۱) از $\gcd(a,b)=1$، a به پیمانه b یک معکوس دارد. فرض کنید x عدد صحیح مثبت باشد که $ax \equiv 1 \ (b)$ (پیمانه). برای هر عدد صحیح مثبت n فرض کنید $s_n=(a+b)(ax)^n$. بنابراین $s_n \equiv a \ (b)$ (پیمانه) و یا به عبارت دیگر s_n عضوی از تصاعد حسابی است. واضح است که اعضا مقسوم علیه‌های مشترکی دارند که عبارتند از a، x و $a+b$.

(۲) این جملات را به روش استقرایی و با اضافه کردن این شرط که نسبت به a اول باشند، می‌سازیم. قرار دهید $t_1=a+b$ که $\gcd(t_1,t_2)=1$ و $\gcd(t_1,a)=1$. فرض کنید جملات $t_1,\dots,t_k$ به گونه‌ای انتخاب شده باشند که برای $1 \le i \le j \le k$، $\gcd(t_i,t_j)=1$ و $\gcd(a,t_i)=1$. قرار می‌دهیم

$$t_{k+1}=t_1 \dots t_k b + a$$

به وضوح، t_{k+1} عضوی از تصاعد حسابی است. از آنجا که $t_1,\dots,t_k$ اعداد صحیح متمایز بزرگ‌تر از ۱ هستند به سادگی می‌توان دید که $t_{k+1} > t_i \ (1 \le i \le k)$. همچنین مشاهده می‌شود که $\gcd(a,t_{k+1})=1$ (از استقرا و فرض $\gcd(a,b)=1$). حال فقط این باقی می‌ماند که نشان دهیم برای $1 \le i \le k$، $\gcd(t_{k+1},t_i)=1$ که از روابط

$$\gcd(t_{k+1},t_i)=\gcd(t_1 t_2 \dots t_k b + a, t_i)=\gcd(a,t_i)=1$$

واضح است و به این ترتیب استقرا کامل می‌شود.

اثبات دوم: در این روش از قضیه اویلر استفاده می‌کنیم.

(۱) جملات $x_n=(a+b)^{n\varphi(b)+1}$ شرایط مسأله برآورده می‌کنند. این جملات دارای مقسوم علیه‌های مشترکی هستند که همان عوامل $a+b$ است. حال باید نشان دهیم که x_n برای هر n صحیح بزرگ در تصاعد حسابی وجود دارد. از قضیه اویلر داریم

$$x_n \equiv a^{n\varphi(b)+1} \equiv a^{n\varphi(b)} a \equiv a \ (b \text{ پیمانه})$$

بنابراین $x_n=a+kb$ و برای n بزرگ، x_n باید در تصاعد داده شده ظاهر شود.

(۲) فرض کنید $y_1 = a$ و $y_2 = a+b$. واضح است که $\gcd(y_1, y_2) = 1$. فرض کنید اعداد $y_1 < y_2 < \ldots < y_k$ در دنباله بوده و دو به دو نسبت به هم اول باشند. قرار می‌دهیم:

$$y_{k+1} = y_1 y_2 \ldots y_k a^{z_{k+1}\varphi(b)-k+1} + b$$

که z_{k+1} عدد صحیح بزرگی است که $y_{k+1} > y_k$. ادعا می کنیم y_{k+1} عضوی از تصاعد بوده و نسبت به همه $y_1, y_2, \ldots, y_k$ اول است. در این روش می توان به روش استقرایی هر لحظه یک عضو جدید ساخت و یک زیر دنباله از تصاعد حسابی تولید کرد که شرایط مسأله را برآورده می‌سازد. حال ادعای خود را ثابت می‌کنیم.

$$y_{k+1} \equiv a^k \; a^{z_{k+1}\varphi(b)-k+1} \equiv a \pmod{b}$$

یعنی y_{k+1} عضوی ازتصاعد است. با توجه به اینکه برای هر $1 \le i \le k$، y_i عضو دنباله است داریم:

$$\gcd(y_{k+1}, y_i) = \gcd(b, y_i) = \gcd(b, a) = 1$$

واثبات کامل است.

توجه: در بخش (۱)، لازم نیست $\gcd(a,b)$ برابر ۱ باشد زیرا با بیرون کشیدن $\gcd(a,b)$ از هر عضو دنباله به شرایط همین مسأله می‌رسیم.

۳۸. از الگوریتم اقلیدس و نتیجه ۲۳.۱ برای حل این مسأله استفاده می‌کنیم.

(۱) از الگوریتم اقلیدس داریم

$$\begin{aligned}\gcd(n!+1, (n+1)!+1) &= \gcd(n!+1, (n+1)!+1-(n+1)(n!+1)) \\ &= \gcd(n!+1, n) = 1\end{aligned}$$

(۲) بدون از دست دادن کلیت مسأله فرض می‌کنیم $a \ge b$. سپس

$$\begin{aligned}\gcd(n^a-1, n^b-1) &= \gcd(n^a - 1 - n^{a-b}(n^b-1), n^b-1) \\ &= \gcd(n^{a-b}-1, n^b-1)\end{aligned}$$

روش یافتن $\gcd(a,b) = \gcd(a-b, b)$ را بیاد بیاورید. مشاهده می‌شود که فرآیند محاسبه $\gcd(n^a-1, n^b-1)$ مشابه فرآیند محاسبه $\gcd(a,b)$ است وقتی که در توان استفاده شده باشند و نتیجه مطلوب از آن بدست می‌آید.

می‌توانیم مسأله را از طریق زیر نیز حل کنیم.

از آنجا که $\gcd(a,b)$، هر دوی a و b را می‌شمارد، چند جمله‌ای $x^{\gcd(a,b)} - 1$ هر دو چند جمله‌ای $x^a - 1$ و $x^b - 1$ را می‌شمارد. بنابراین $n^a - 1, n^{\gcd(a,b)} - 1$ و $n^b - 1$ را می‌شمارد و لذا

$$n^{\gcd(a,b)}-1 \mid \gcd(n^a-1, n^b-1)$$

از طرف دیگر، فرض کنید m هر دوی n^a-1 و n^b-1 را بشمارد؛ یعنی (پیمانه m) $n^a \equiv 1 \equiv 1^a$ و (پیمانه m) $n^b \equiv 1 \equiv 1^b$ (واضح است که m و n نسبت به هم اول هستند). از نتیجه ۲۳.۱ داریم (پیمانه m) $n^{\gcd(a,b)} \equiv 1$؛ یعنی m, $n^{\gcd(a,b)}-1$ را می‌شمارد بنابراین

$$\gcd(n^a-1, n^b-1) \mid n^{\gcd(a,b)}-1$$

و در نتیجه $n^{\gcd(a,b)}-1 = \gcd(n^a-1, n^b-1)$.

(۳) فرض کنید که m, 2^a+1 و 2^b+1 را بشمارد. بنابراین m فرد است. کافی است نشان دهیم m، $2^{\gcd(a,b)}+1$ را می‌شمارد.

از آنجا که (پیمانه m) $2^a \equiv 2^b \equiv -1$ داریم

$$2^{2a} \equiv 1 \ (\text{پیمانه } m) \quad \text{و} \quad 2^{2b} \equiv 1 \ (\text{پیمانه } m)$$

از نتیجه ۲۳.۱، (پیمانه m) $2^{\gcd(2a,2b)} \equiv 1$؛ یعنی m, $2^{\gcd(2a,2b)}-1 = 2^{2\gcd(a,b)}-1$ را می‌شمارد و یا

$$m \mid (2^{\gcd(a,b)}-1)(2^{\gcd(a,b)}+1)$$

برای رسیدن به نتیجه مورد نظر باید ثابت کنیم $\gcd(m, 2^{\gcd(a,b)}-1) = 1$ فرض کنید $\gcd(m, 2^{\gcd(a,b)}-1) = d$. همانطور که در قسمت (۲) نشان دادیم $2^{\gcd(a,b)}-1$, 2^a-1 را می‌شمارد پس d نیز 2^a-1 را می‌شمارد. از طرف دیگر فرض کرده‌ایم که m, 2^a+1 را می‌شمارد پس d هم 2^a+1 را می‌شمارد. بنابراین d، $\gcd(2^a-1, 2^a+1) = 2$ را می‌شمارد که چون m فرد است d باید برابر ۱ باشد و اثبات کامل می‌شود.

(۴) فرض کنید $s_n = 5^n + 7^n$. اگر $n \geq 2$ باشد

$$s_n = s_m s_{n-m} - 5^m 7^m s_{n-2m}$$

بنابراین $\gcd(s_m, s_n) = \gcd(s_m, s_{n-2m})$. بطور مشابه اگر $m < n < 2m$ باشد داریم:

$$s_n = s_m s_{n-m} - 5^{n-m} 7^{n-m} s_{2m-n}$$

و لذا $\gcd(s_n, s_m) = \gcd(s_m, s_{2m-n})$. از الگوریتم اقلیدس نتیجه می‌گیریم اگر $m+n$ زوج باشد، آنگاه $\gcd(s_m, s_n) = \gcd(s_1, s_1) = 12$ و اگر $m+n$ فرد باشد آنگاه $\gcd(s_m, s_n) = \gcd(s_0, s_1) = 2$.

توجه: علاقه‌مندان می‌توانند با بررسی رابطه بین $\gcd(n^a+1, n^b+1)$ و $n^{\gcd(a,b)}+1$، بخش (۳) را تعمیم دهند.

۳۹. در این مسأله از مبنای ۲ و مبنای ۳ استفاده می‌کنیم.

(۱) جواب مثبت است.

مکعب واحد با رئوس $(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)$ را در نظر بگیرید. این مختصات معادل باینری (دودویی) اعداد $0,1,2,3,4,5,6,7$ هستند. این موضوع ما را بر آن می‌دارد تا صفحه $x+2y+4z=0$ را مورد بررسی قرار دهیم. فواصل رئوس S از صفحه برابرند با

$$0, \frac{1}{\sqrt{21}}, \frac{2}{\sqrt{21}}, \frac{3}{\sqrt{21}}, \frac{4}{\sqrt{21}}, \frac{5}{\sqrt{21}}, \frac{6}{\sqrt{21}}, \frac{7}{\sqrt{21}}$$

با یک تغییر مقیاس ساده، می‌توان یک مکعب پیدا کرد که شرایط مسأله را برآورده سازد. S را با نسبت $\sqrt{21}$ بزرگ می‌کنیم تا مکعب T بدست آید. نقطه (a,b,c) به نقطه $(\sqrt{21}a, \sqrt{21}b, \sqrt{21}c)$ نگاشته می‌شود. به این ترتیب مکعب T و صفحه $x+2y+4z=0$ شرایط مسأله را برآورده می‌سازند.

(۲) توجه کنید که یک عدد صحیح مثبت عضو این دنباله است اگر و فقط اگر نمایش آن در مبنای ۳ فقط شامل ۰و۱ باشد. بنابراین می‌توان یک تناظر یک به یک بین اعداد صحیح مثبت و اعضای این دنباله از طریق نمایش هر دوی آنها با ارقام ۰و۱، یکی در مبنای ۲و دیگری در مبنای ۳ برقرار کرد:

$$\begin{aligned}
1 &= 1_{(2)} \quad \Leftrightarrow 1_{(3)} = 1 \\
2 &= 10_{(2)} \quad \Leftrightarrow 10_{(3)} = 3 \\
3 &= 11_{(2)} \quad \Leftrightarrow 10_{(3)} = 4 \\
4 &= 100_{(2)} \Leftrightarrow 100_{(3)} = 9 \\
5 &= 101_{(2)} \Leftrightarrow 101_{(3)} = 10 \\
&\vdots
\end{aligned}$$

این تناظر بین دو دنباله به ترتیبی است که در بالا می‌بینید؛ یعنی k امین عدد صحیح مثبت متناظر با k امین عددی است که می‌توان آن را به صورت مجموع توان‌های متمایز ۳ نوشت. دلیل این امر آن است که اعداد دودویی وقتی که به ترتیب صعودی نوشته می‌شوند، با تفسیر در هر مبنای دیگر نیز به ترتیب صعودی هستند.

بنابراین برای یافتن صدمین عضو دنباله فقط کافی است به ۱۰۰ امین خط تناظر فوق نگاه کنیم:

$$100 = 1100100_{(2)} \Leftrightarrow 1100100_{(3)} = 981$$

۴۰. (۱) [ARML ۲۰۰۲]

$$a=۲۳!+\frac{۲۳!}{۲}+\ldots+\frac{۲۳!}{۲۳}$$

بجز $\frac{۲۳!}{۱۳}$، همه‌ی اعداد سمت راست رابطه فوق بر ۱۳ بخشپذیرند. بنابراین از قضیه ویلسون داریم

$$a\equiv\frac{۲۳!}{۱۳}\equiv ۱۲!\times ۱۴\times ۱۵\times\ldots\times ۲۳$$

$$\equiv ۱۲!\,۱۰!\equiv\frac{(۱۲!)^۲}{۱۱\times ۱۲}\equiv\frac{۱}{۲}\equiv ۷ \qquad (\text{پیمانه } ۱۳)$$

(۲) عبارت

$$((p-۱)!)^۲\frac{m}{n}=((p-۱)!)^۲\left(\frac{۱}{۱^۲}+\frac{۱}{۲^۲}+\cdots+\frac{۱}{(p-۱)^۲}\right)$$

یک عدد صحیح و

$$\left\{۱,\frac{۱}{۲},\ldots,\frac{۱}{p-۱}\right\}$$

یک دستگاه مخفف مانده‌ها به پیمانه p است. از قضیه ۱۸.۱ (ح) و قضیه ویلسون داریم

$$((p-۱)!)^۲\left(\frac{۱}{۱^۲}+\frac{۱}{۲^۲}+\cdots+\frac{۱}{(p-۱)^۲}\right)$$

$$\equiv(-۱)^۲[۱^۲+۲^۲+\cdots+(p-۱)^۲]$$

$$\equiv\frac{(p-۱)p(۲p-۳)}{۶}\equiv ۰ \qquad (\text{پیمانه } p)$$

$p\geq ۵$ است لذا $\gcd(۶,p)=۱$ و در نتیجه p عدد صحیح $\frac{((p-۱)!)^۲m}{n}$ را می‌شمارد. از آنجا که $\gcd((p-۱)!,p)=۱$، لذا $p\mid m$ که همان نتیجه مطلوب است.

(۳) [قضیه ولستن هولم]* قرار می‌دهیم

$$S=(p-۱)!\left(۱+\frac{۱}{۲}+\cdots+\frac{۱}{p-۱}\right)$$

سپس

$$۲S=(p-۱)!\sum_{i=۱}^{p-۱}\left[\frac{۱}{i}+\frac{۱}{p-i}\right]=(p-۱)!\sum_{i=۱}^{p-۱}\frac{p}{i(p-i)}=pT$$

که

* wolstenholm'sTheorem

$$T=(p-1)!\sum_{i=1}^{p-1}\frac{1}{i(p-i)}$$

چون $2S$ یک عدد صحیح بوده و p نسبت به مخرج‌های اعداد جمع شونده در T اول است، T خود نیز باید صحیح باشد. از $p>3$ و $\gcd(p,2)=1$، p باید S را بشمارد. کافی است نشان دهیم p، T را هم می‌شمارد. از (۲) و اینکه $p\mid m$ و $\gcd(m,n)=1$ داریم

$$T\equiv(p-1)!\sum_{i=1}^{p-1}-\frac{1}{i^2}\equiv(p-1)!\frac{m}{n}\equiv 0 \pmod p \quad \text{(پیمانه } p\text{)}$$

۴۱. با یک بررسی ساده می‌توان نشان داد که زوج‌های $(x,y)=(1,1),(11,16),(16,11)$ جواب هستند. نشان می‌دهیم که این مقادیر تنها جواب‌های ممکن هستند. نامساوی‌های

$$x^2+3y\geq(x+2)^2 \quad , \quad y^2+3x\geq(y+2)^2$$

نمی‌توانند هر دو برقرار باشند زیرا با جمع آنها به $x+y+8\leq 0$ می‌رسیم که غلط است. بنابراین حداقل یکی از نامساوی‌های $x^2+3y<(x+2)^2$ و $y^2+3x<(y+2)^2$ درست هستند. بدون از دست دادن کلیت مسأله فرض می‌کنیم که $x^2+3y<(x+2)^2$. از $x^2<x^2+3y<(x+2)^2$ نتیجه می‌گیریم که $x^2+3y=(x+1)^2$ بنابراین $3y=2x+1$. پس $x=3k+1$ و $y=2k+1$ که k عدد صحیح نامنفی است. به این ترتیب داریم $y^2+3x=4k^2+13k+4$. اگر $k>5$ آنگاه

$$(2k+3)^2<4k^2+13k+4<(2k+4)^2$$

و در نتیجه y^2+3x نمی‌تواند مربع کامل باشد. به سادگی می‌توان دید که برای $k\in\{1,2,3,4\}$ نیز y^2+3x مربع کامل نیست. برای $k=0$, $y^2+3x=4=2^2$ و برای $k=5$, $y^2+3x=13^2$. برای این دو مقدار k، x^2+3y برابر 2^2 و 17^2 است که منجر به جواب‌های $(x,y)=(1,1)$ و $(x,y)=(16,11)$ می‌شود.

۴۲. (۱) [AMC12B ۲۰۰۴] برای قسمت (۱) دو راه حل ارائه می‌کنیم.

- *روش اول.* کوچک‌ترین توان ۲ با تعداد ارقام معین، با رقم ۱ (از سمت چپ) شروع می‌شود. اعضای موجود در S دارای n رقم هستند که $n\leq 603$. بنابراین رقم اول (از سمت چپ) ۶۰۳ عضو S، ۱ است. علاوه بر این اگر رقم اول $1,2^k$ باشد آنگاه رقم اول $2,2^{k+1}$ یا ۳ و رقم اول $6,5,4,2^{k+2}$ و یا ۷ است. بنابراین رقم اول ۶۰۳ عضو دیگر S، ۲ یا ۳ است. رقم اول ۶۰۳ عضو دیگر نیز ۴،۵،۶ یا ۷ است و $2004-3\times 603=195$ عضو باقی‌مانده با ۸ یا ۹ آغاز می‌شوند. لازم به ذکر است که

رقم اول 2^k، ۸ یا ۹ است اگر و فقط اگر اولین رقم $4,2^{k-1}$ باشد. بنابراین ۱۹۵ عضو S با ۴ آغاز می‌شوند.

- *روش دوم.* مجموعه‌ی S را به صورت زیر دسته‌بندی می‌کنیم.

$$\{2^0,2^1,2^2,2^3:2^4,2^5,2^6:2^7,\ldots,2^{2003}\}$$

عضو ابتدایی هر دسته با رقم ۱ شروع می‌شود. از آنجا که رقم اول $1,2^{2004}$ است بنابراین S به دسته‌های کامل تقسیم می‌شود. همانطور که در روش اول نشان دادیم دقیقاً ۶۰۳ عضو S با ۱ شروع می‌شوند، لذا ۶۰۳ دسته در S وجود دارد. هر دسته ۳یا ۴ عضو دارد. اگر یک دسته ۳ عضو $2^k,2^{k+1}$ و 2^{k+2} را داشته باشد، رقم‌های آغازین آنها ۱، ۲ یا ۳، ۵ یا ۶ یا ۷ و اگر یک دسته ۴ عضو $2^k,2^{k+1},2^{k+2}$ و 2^{k+3} را داشته باشد رقم‌های آغازین آنها ۱، ۲، ۴، ۸ یا ۹ هستند. بنابراین تعداد اعضای S که با ۴ شروع می‌شوند برابر تعداد دسته‌های ۴تایی است. فرض کنید x دسته سه عضوی و y دسته ۴ عضوی وجود دارد. می‌دانیم $3x+4y=2004$ (چون S در کل ۲۰۰۴ عضو دارد) و $x+y=603$ (چون۶۰۳ دسته کامل وجود دارد). با حل این معادلات $x=408$ و $y=195$ بدست می‌آید.

(۲) فرض کنید s و t اعداد صحیح مثبت یکتایی باشند که $10^s<2^n<10^{s+1}$ و $10^t<5^n<10^{t+1}$ قرار می‌دهیم $a=\frac{2^n}{10^s}$ و $b=\frac{5^n}{10^t}$. واضح است که $1<a<10$, $1<b<10$ و $ab=10^{n-s-t}$.

چون ab توانی از ۱۰ بوده و $1<ab<10^2$، تنها مقدار ممکن $ab=10$ است. در نتیجه

$$\min(a,b)<\sqrt{ab}=\sqrt{10}<\max(a,b)$$

بنابراین اولین k رقم مشترک، اولین k رقم $\sqrt{10}$ است. (برای $k=1$, $2^5=32$ و $5^5=3125$ که هر دو با یک رقم شروع می‌شوند و آن هم رقم ابتدایی $\sqrt{10}=3/1000$ است.)

۴۳. **پاسخ اول:** مقادیر کلیدی در این مسأله $\varphi(10)=4$ و $\varphi(1000)=400$ هستند. بطور مکرر از قضیه اویلر استفاده می‌کنیم.

(۱) جواب‌ها به ترتیب ۹ و۳ هستند.

$$3^{1001}\times 7^{1002}\times 13^{1003}\equiv 3^{1000}\times 91^{1002}\times 3\times 13$$
$$\equiv 81^{250}\times 91^{1002}\times 39\equiv 9 \quad \text{(پیمانه ۱۰)}$$

با توجه به این‌که (پیمانه ۱۰) $7^4\equiv 1$، (پیمانه ۴) $7^{2k}\equiv 1$ و (پیمانه۴) $7^{2k+1}\equiv 3$ داریم

$$\underbrace{7^{7^{\cdot^{\cdot^{\cdot^7}}}}}_{\text{۱۰۰۰ تا ۷}}\equiv 3 \quad \text{(پیمانه ۴)}$$

بنابراین

$$\underbrace{۷^{۷^{۷^{\cdot^{\cdot^{۷}}}}}}_{\text{۱۰۰۱ تا ۷}} \equiv ۷^{۳} \equiv ۳ \quad \text{(پیمانه ۱۰)}$$

(۲) [۲۰۰۳ کانادا] جواب ۲۴۱ است.

از $\varphi(۱۰۰۰)=۴۰۰$ و

$$۲۰۰۳^{۲۰۰۲^{۲۰۰۱}} \equiv ۳^{۲۰۰۲^{۲۰۰۱}} \quad \text{(پیمانه ۱۰۰۰)}$$

لازم است که $۲۰۰۲^{۲۰۰۱}$ به پیمانه ۴۰۰ را محاسبه کنیم. از آنجا که $۴۰۰=۱۶\times۲۵$ و ۱۶، $۲^{۲۰۰۱}$را می‌شمارد لذا (پیمانه ۴۰۰) $۲^{۲۰۰۱} \equiv ۱۶k$ که k یک عدد صحیح مثبت است. از نتیجه ۲۱.۱ داریم (پیمانه ۲۵) $۲^{۱۹۹۷} \equiv k$ و از $\varphi(۲۵)=۲۰$

$$k \equiv ۲^{۱۹۹۷} \equiv \frac{۲^{۲۰۰۰}}{۲^{۳}} \equiv \frac{۱}{۸} \equiv ۲۲ \quad \text{(پیمانه ۲۵)}$$

یا $k=۲۲$. به این ترتیب (پیمانه ۴۰۰) $۲^{۲۰۰۱} \equiv ۱۶k \equiv ۳۵۲$ و بنابراین $۲۰۰۳^{۲۰۰۲^{۲۰۰۱}} \equiv ۳^{۲۰۰۲^{۲۰۰۱}}$

$$۲۰۰۳^{۲۰۰۲^{۲۰۰۱}} \equiv ۳^{۲۰۰۲^{۲۰۰۱}} \equiv ۳^{۳۵۲} \equiv ۹^{۱۷۶} \equiv (۱۰-۱)^{۱۷۶} \quad \text{(پیمانه ۱۰۰۰)}$$

از قضیه دو جمله‌ای داریم

$$(۱۰-۱)^{۱۷۶} \equiv \binom{۱۷۶}{۲}\times۱۰^{۲} - \binom{۱۷۶}{۱}\times۱۰ + ۱^{۱۷۶}$$

$$\equiv ۰ - ۱۷۶۰ + ۱ \equiv ۲۴۱ \quad \text{(پیمانه ۱۰۰۰)}$$

(۳) جواب ۵۹۴ است.

$$\binom{۹۹}{۱۹} = \frac{۹۹!}{۱۹!\,۸۰!} = \frac{۹۹\times۹۸\times\ldots\times۸۱}{۱۹!}$$

از آنجا که $۱۰۰۰=۸\times۱۲۵$، لازم است $\binom{۹۹}{۱۹}$ را به پیمانه ۸ و ۱۲۵محاسبه کنیم. چون ۹۹ خیلی به ۱۰۰ نزدیک است ابتدا $\binom{۹۹}{۱۹}$ را به پیمانه ۴و۲۵ حساب می‌کنیم. (به عبارت دیگر در ابتدا y و z را محاسبه می‌کنیم)

$$\frac{۹۹\times۹۸\times\ldots\times۸۱}{۱۹!} = \frac{۹۹\times۹۸\times\ldots\times۹۶\times۹۵\times۹۴\times\ldots\times۹۱\times۹۰\times۸۹\times\ldots\times۸۶\times۸۵\times۸۴\times\ldots\times۸۱}{۴!\times۵\times۶\times\ldots\times۹\times۱۰\times۱۱\times\ldots\times۱۴\times۱۵\times۱۶\times\ldots\times۱۹}$$

$$= \frac{۱۹\times۱۸\times۱۷\times۹۹\times\ldots\times۹۶\times۹۴\times\ldots\times۹۱\times۸۹\times\ldots\times۸۶\times۸۴\times\ldots\times۸۱}{۳!\times۴!\times۶\times\ldots\times۹\times۱۱\times\ldots\times۱۴\times۱۶\times\ldots\times۱۹}$$

در نتیجه

$$\frac{۹۹\times۹۸\times\ldots\times۸۱}{۱۹!}\equiv\frac{۱۹\times۱۸\times۱۷}{۳!}\equiv۱۹ \qquad \text{(پیمانه ۲۵)}$$

به روشی مشابه می‌توان $\binom{۹۹}{۱۹}$ را به پیمانه ۴ محاسبه کرد. توجه کنید که

$$\sum_{n=۱}^{\infty}\left\lfloor\frac{۹۹}{۲^n}\right\rfloor-\sum_{n=۱}^{\infty}\left\lfloor\frac{۱۹}{۲^n}\right\rfloor-\sum_{n=۱}^{\infty}\left\lfloor\frac{۸۰}{۲^n}\right\rfloor=۹۵-۱۶-۷۸=۱$$

که به موجب آن (پیمانه۴) $\binom{۹۹}{۱۹}\equiv۲$.

با ترکیب دو نتیجه فوق داریم (پیمانه ۱۰۰) $\binom{۹۹}{۱۹}\equiv۹۴$ بنابراین $z=۴$ و $y=۹$. علاوه بر آن

$$e_۳\left(\binom{۹۹}{۱۹}\right)=\sum_{n=۱}^{\infty}\left\lfloor\frac{۹۹}{۳^n}\right\rfloor-\sum_{n=۱}^{\infty}\left\lfloor\frac{۱۹}{۳^n}\right\rfloor-\sum_{n=۱}^{\infty}\left\lfloor\frac{۸۰}{۳^n}\right\rfloor$$
$$=۴۸-۸-۳۶=۴$$

بنابراین (پیمانه۹) $\binom{۹۹}{۱۹}\equiv۰$. در پیمانه ۹ داریم

$$۱+۰+۷+۱+۹+۶+۶+۷+۴+۰+۸+۰+۷+۶+۱+۹+۳+۶+x+۹+۴\equiv۰$$

و یا (پیمانه ۹) $x\equiv۵$. چون x یک رقم در مبنای ۱۰ است لذا $x=۵$.

(۴) جواب ۱۹۲ است.

اگر مکعب یک عدد صحیح به ۸ ختم شود، خود عدد باید به ۲ ختم شود به عبارت دیگر آن عدد باید به شکل $۱۰k+۲$ باشد. بنابراین

$$n^۳=(۱۰k+۲)^۳=۱۰۰۰k^۳+۶۰۰k^۲+۱۲۰k+۸$$

بخش $۱۲۰k$ تعیین کننده رقم دهگان $n^۳$ است که آن نیز باید ۸ باشد. به‌عبارت دیگر

$$۸۸\equiv n^۳\equiv۱۲۰k+۸ \qquad \text{(پیمانه ۱۰۰)}$$

یا (پیمانه ۱۰۰) $۱۲۰k\equiv۸۰$. با توجه به نتیجه ۱. ۲۱، (پیمانه ۵) $۶k\equiv۴$ و یا (پیمانه ۵) $k\equiv۴$ لذا $k=۵m+۴$ و به پیمانه ۱۰۰۰ داریم

$$۸۸۸\equiv n^۳\equiv۶۰۰(۵m+۴)^۲+۱۲۰(۵m+۴)+۸\equiv۹۶۰۰+۶۰۰m+۴۸۸$$

و یا (پیمانه ۱۰۰۰) $۶۰۰m\equiv۸۰۰$. از نتیجه ۲۱.۱ (پیمانه ۵) $۳m\equiv۴$ و لذا (پیمانه ۵) $m\equiv۳$. کوچک‌ترین مقدار m، ۳ است که به موجب آن $k=۵\times۳+۴=۱۹$ و $n=۱۰\times۱۹+۲=۱۹۲$ خواهد بود. $(۱۹۲^۳=۷۰۷۷۸۸۸)$

پاسخ دوم: روش دیگری را برای حل قسمت (۳) ارائه می‌کنیم. مشابه آنچه در پاسخ اول نشان دادیم به سادگی می‌توان اثبات کرد $\left|\binom{۹۹}{۱۹},۱۱\right|\binom{۹۹}{۱۹}$. با استفاده از قضیه ۱. ۴۴ (ب)، (پ) و (ت) خواهیم داشت

$$x+y+z\equiv 0 \quad \text{(پیمانه ۹)}$$
$$x-y+z\equiv 0 \quad \text{(پیمانه ۱۱)}$$
$$\overline{xyz}+1\equiv 0 \quad \text{(پیمانه ۷)}$$

و یا

$$x+y+z\equiv 0 \quad \text{(پیمانه ۹)}$$
$$x-y+z\equiv 0 \quad \text{(پیمانه ۱۱)}$$
$$2x+3y+z+1\equiv 0 \quad \text{(پیمانه ۷)}$$

چون x,y,z ارقام از ۰ تا ۹ هستند رابطه‌ی اول منجر به معادله‌ی ۲۷ یا ۱۸ یا ۹ $x+y+z=9$ و رابطه‌ی دوم منجر به معادله‌ی ۱۱ یا ۰ $x-y+z=0$ می‌شود. به سادگی می‌توان دید که $(x+y+z,x-y+z)=(9,0)$ یا $(x+z,y)=(9,9)$ یا $(18,0)$. با قرار دادن این مقادیر در رابطه سوم داریم (پیمانه ۷) $x+3y+(x+z)+1\equiv x+2\equiv 0$ و لذا $x=5$ و $z=4$. پس $\overline{xyz}=594$.

توجه: یک اشتباه رایج در حل قسمت (۳) به صورت زیر است:

$$\binom{99}{19}=\frac{99\times 98\times\ldots\times 81}{19!}\equiv\frac{19\times 18\times\ldots\times 1}{19!}\equiv 1 \quad \text{(پیمانه ۸)}$$

چون $19!$ نسبت به ۸ اول نیست، نمی‌توان از عمل تقسیم در این رابطه استفاده کرد (بحث منجر به نتیجه ۱. ۲۱ را ببینید).

۴۴. از قضیه ویلسون

$$a_1a_2\ldots a_{p-1}\equiv b_1b_2\ldots b_{p-1}\equiv(p-1)!\equiv -1 \quad (p \text{ پیمانه})$$

بنابراین

$$(a_1b_1)(a_2b_2)\ldots(a_{p-1}b_{p-1})\equiv a_1a_2\ldots a_{p-1}b_1b_2\ldots b_{p-1}\equiv(-1)^2\equiv 1 \quad (p \text{ پیمانه})$$

مجدداً با توجه به قضیه ویلسون $\{a_1b_1,a_2b_2,\ldots,a_{p-1}b_{p-1}\}$ یک دستگاه کامل مانده‌ها به پیمانه p نیست.

۴۵. جواب مثبت است.

برای هر $2\le i\le p-1$ از $\gcd(i,p)=1$ نتیجه می‌گیریم که i به پیمانه p معکوس‌پذیر است و بنابراین (پیمانه p) $ix\equiv i+1$ یک جواب یکتا (به پیمانه p) دارد. فرض کنید a_i عدد صحیح یکتایی باشد که $1\le a_i\le p-1$ و (پیمانه p) $ia_i\equiv i+1$. حال باید نشان دهیم برای $1<i<j\le p-2$، $a_i\neq a_j$. فرض کنید برای $1<i<j\le p-2$ ، $a_i=a_j=a$. از آنجا که

$$ja_j\equiv j+1 \quad (p \text{ پیمانه}) \quad \text{و} \quad ia_i\equiv i+1 \quad (p \text{ پیمانه})$$

بنابراین

$$\circ \equiv a(j-i) \equiv ja_j - ia_i \equiv j-i \quad (p \text{ پیمانه})$$

که به دلیل $\circ < j-i < p-۲$ غیرممکن است.

توجه: از مسأله ۴۴ می‌دانیم $\{a_۱, ۲a_۲, ۳a_۳, \ldots, (p-۱)a_{p-۱}\}$ یک دستگاه کامل مانده‌ها نیست. از مسأله ۴۵ نتیجه می‌گیریم که بیشترین تعداد دسته‌های هم‌نهشتی متمایز در دنباله $\{a_۱, ۲a_۲, \ldots, (p-۱)a_{p-۱}\}$، $p-۲$ است.

۴۶. [پاول اردوش] **اثبات اول:** برای هر $k = ۱, ۲, \ldots, n$، a_k را به صورت $a_k = \frac{n!}{k!}$ تعریف می‌کنیم. فرض کنید چند عدد m داریم که $a_k \le m < a_{k-۱}$ و $۲ \le k \le n$. عدد $d = a_k \left\lfloor \frac{m}{a_k} \right\rfloor$ را در نظر بگیرید. داریم $\circ \le m - d < a_k$ و چون $s = \left\lfloor \frac{m}{a_k} \right\rfloor < \frac{a_{k-۱}}{a_k} = k$ می‌دانیم که

$$\frac{n!}{d} = \frac{a_k k!}{a_k s} = \frac{k!}{s}$$

یک عدد صحیح است. بنابراین می‌توان از m، d (یک مقسوم‌علیه $n!$) را کم کرد تا به یک عدد کوچک‌تر از a_k برسیم. بنابراین اگر با هر عدد صحیح مثبت $m < a_۱ = n!$ شروع کنیم با کم کردن حداکثر یک عامل $n!$ از m به یک عدد صحیح کوچک‌تر از $a_۲$ می‌رسیم؛ با کم کردن حداکثر یک عامل دیگر $n!$ به یک عدد صحیح کوچک‌تر از $a_۳$ می‌رسیم و به همین روال ادامه می‌دهیم. به این ترتیب می‌توان m را به‌صورت مجموع حداکثر $n-۱$ مقسوم‌علیه مثبت $n!$ بیان کرد.

اثبات دوم: از استقرا استفاده می‌کنیم. برای $n = ۳$، ادعای مطرح شده درست است. فرض کنید حکم برای $n-۱$ برقرار باشد. عدد k با شرط $۱ < k < n!$ را در نظر گرفته و فرض کنید k' و q به‌ترتیب خارج قسمت و باقیمانده تقسیم k بر n باشند؛ یعنی $k = k'n + q$ $(\circ \le q \le n)$ و

$$\circ < k' < \frac{k}{n} < \frac{n!}{n} = (n-۱)!$$

از فرض استقرا اعداد صحیح $(s \le n-۱)\ d'_۱ < d'_۲ < \ldots < d'_s$ وجود دارند که برای $i = ۱, ۲, \ldots, s$ $d'_i \mid (n-۱)!$ و $k' = d'_۱ + d'_۲ + \cdots + d'_s$. بنابراین $k = nd'_۱ + nd'_۲ + \cdots + nd'_s + q$. اگر $q = \circ$ آنگاه $k = d_۱ + d_۲ + \cdots + d_s$ که $(i = ۱, \ldots, s)\ d_i = nd'_i$ مقسوم علیه‌های متمایز $n!$ هستند. اگر $q \ne \circ$ آنگاه $k = d_۱ + d_۲ + \cdots + d_{s+۱}$ که $(i = ۱, \ldots, s)\ d_i = nd'_i$ و $d_{s+۱} = q$. واضح و مبرهن است که $(i = ۱, \ldots, s)\ d_i \mid n!$ و $d_{s+۱} \mid n!$ زیرا $q < n$. از طرف دیگر $d_{s+۱} < d_۱ < d_۲ < \cdots < d_s$ چون $d_{s+۱} = q < n \le nd'_۱ = d_۱$. بنابراین k را می‌توان به صورت مجموع حداکثر n مقسوم‌علیه متمایز $n!$ نوشت.

۴۷. فرض کنید چنین عدد صحیح فرد n وجود داشته باشد که $n, ۱+۳^n$ را بشمارد.

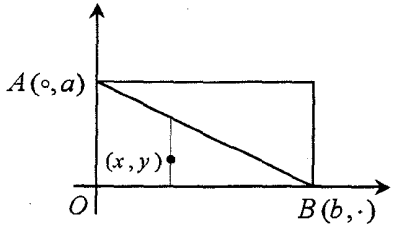
فرض کنید p کوچک‌ترین عامل اول n باشد. پس $p, ۱+۳^n$ را می‌شمارد؛ یعنی (پیمانه p) $۳^n \equiv -۱$ و از آنجا (پیمانه p) $۳^{۲n} \equiv ۱$. از قضیه کوچک فرما داریم (پیمانه p) $۳^{p-۱} \equiv ۱$ و با استفاده از نتیجه ۱. ۲۳

$$۳^{\gcd(۲n,p-۱)} \equiv ۱ \quad (\text{پیمانه } p)$$

چون p کوچک‌ترین عامل اول n است، $\gcd(n,p-۱)=۱$ و چون n فرد است، $p-۱$ زوج است بنابراین $\gcd(۲n,p-۱)=۲$ و (پیمانه p) $۳^۲ \equiv ۱$ در نتیجه $p, ۸$ را می‌شمارد که غیرممکن است (چون p فرد است).

۴۸. واضح است که برای هر جواب (x,y,z) در مجموعه اعداد صحیح نامنفی برای $ax+by+z=ab$، یک جواب (x,y) در اعداد صحیح نامنفی برای $ax+by \le ab$ داریم. برعکس برای هر جواب (x,y) برای $ax+by \le ab$ جواب $(x,y,ab-ax-by)$ را برای معادله داده شده داریم. بنابراین کافی است تعداد جواب‌های (x,y) در اعداد صحیح نامنفی را برای $ax+by \le ab$ پیدا کنیم.

واضح است این جواب‌ها متناظر به نقاط بامختصات صحیح در مستطیل $[۰,b]\times[۰,a]$ است.



تعداد نقاط با مختصات صحیح در این مستطیل $(a+۱)(b+۱)$ است. شرط $ax+by \le ab$ به معنای آن است که نقطه (x,y) باید زیر یا روی قطر AB باشد. به دلیل تقارن تعداد نقاط مطلوب (x,y) برابر است با

$$\frac{۱}{۲}(a+۱)(b+۱)+\frac{d}{۲}$$

که d تعداد نقاط روی قطر AB است. برای یافتن d، توجه کنید که $ax+by=ab$ معادل با $y=a-\frac{a}{b}x$ است. تعداد اعداد صحیح در دنباله

$$\frac{۱\times a}{b}, \frac{۲\times a}{b}, \cdots, \frac{b\times a}{b}$$

برابر $\gcd(a,b)$ است. در ضمن نقطه $A(۰,a)$ را نیز باید بشماریم. بنابراین $d=\gcd(a,b)+۱$ و نتیجه مطلوب بدست می‌آید.

۴۹. در این مسأله از قضیه ۱. ۳۰ استفاده می‌کنیم.

(۱) فرض کنید $d=\mathrm{ord}_p(q)$ (مرتبه q به پیمانه p). از $p\mid q^r+1$ و $p>2$ داریم

$$q^r\equiv -1\not\equiv 1 \quad (\text{پیمانه } p)$$

و بنابراین

$$q^{2r}\equiv (-1)^2\equiv 1 \quad (\text{پیمانه } p)$$

از روابط فوق، نتیجه می‌گیریم که $d, 2r$ را شمرده ولی r را نمی‌شمارد. از آنجا که r، اول است تنها مقادیر ممکن $d=2$ و $d=2r$ هستند. اگر $d=2r$ آنگاه چون از قضیه ۳۰.۱ و قضیه کوچک فرما $d\mid p-1$ لذا $2r\mid p-1$. اگر $d=2$ آنگاه (پیمانه p) $q^2\equiv 1$ و بنابراین $p\mid q^2-1$.

(۲) اثبات مشابه اثبات قضیه ۱. ۵۰ است.

از همنهشتی (پیمانه p) $a^{2^n}\equiv -1$ داریم

$$a^{2^{n+1}}=(a^{2^n})^2\equiv 1 \quad (\text{پیمانه } p)$$

از قضیه ۳۰.۱، $ord_p(a), 2^{n+1}$ را می‌شمارد. از (پیمانه p) $2^n\equiv -1$ نتیجه می‌گیریم که $ord_p(a)=2^{n+1}$. واضح است که $\gcd(a,p)=1$. از قضیه کوچک فرما داریم (پیمانه p) $a^{p-1}\equiv 1$. از قضیه ۳۰.۱ نتیجه می‌گیریم که 2^{n+1}، $p-1$ را می‌شمارد.

توجه: قرار دادن $a=2$ در (۲) نشان می‌دهد اگر p یک عامل اول عدد فرمای f_n باشد آنگاه $p-1$ بر 2^{n+1} بخشپذیر است.

۵۰. [APMO ۲۰۰۴] بررسی مستقیم اعداد $n=1,2,\ldots,6$ نشان می‌دهد که حکم برای این اعداد برقرار است. فرض می‌کنیم $n\geq 6$. سه حالت را در نظر می‌گیریم.

در حالت اول فرض می‌کنیم $n=p$ اول باشد. بنابراین $n+1=p+1$ زوج است و $n+1=2\times\frac{p+1}{2}$، $(n-1)!=(p-1)!$ را می‌شمارد و

$$k=\frac{(n-1)!}{n+1}=\frac{(p-1)!}{p+1}$$

یک عدد صحیح زوج بوده و لذا $k+1$ یک عدد صحیح فرد است، از قضیه ویسلون

$$k+1\equiv\frac{(p-1)!}{p+1}+1\equiv\frac{-1}{1}+1\equiv 0 \quad (\text{پیمانه } p)$$

در نتیجه $\frac{k+1}{p}$ یک عدد صحیح فرد است؛ یعنی

$$\frac{\frac{(p-1)!}{p+1}+1}{p}=\frac{(p-1)!}{p(p+1)}+\frac{1}{p}$$

یک عدد صحیح فرد و از آنجا

$$\left\lfloor\frac{(n-1)!}{n(n+1)}\right\rfloor=\left\lfloor\frac{(p-1)!}{p(p+1)}\right\rfloor$$

زوج است.

در حالت دوم فرض می‌کنیم $n+1=p$ اول باشد. بنابراین $n=p-1$ زوج است و $n=2\times\frac{p-1}{2}$ عدد $(n-1)!=(p-2)!$ را می‌شمارد و

$$k'=\frac{(n-1)!}{n}=\frac{(p-2)!}{p-1}$$

یک عدد صحیح زوج بوده و لذا $k'+1$ فرد است. از قضیه ویلسون داریم

$$k'+1\equiv\frac{(p-2)!}{p-1}+1\equiv\frac{(p-1)!}{(p-1)^2}+1\equiv-1+1\equiv 0 \quad (\text{پیمانه } p)$$

بنابراین $\frac{k'+1}{p}$ نیز یک عدد فرد است. یعنی

$$\frac{\frac{(p-2)!}{p-1}+1}{p}=\frac{(p-2)!}{p(p-1)}+\frac{1}{p}$$

یک عدد فرد و از آنجا

$$\left\lfloor\frac{(n-1)!}{n(n+1)}\right\rfloor=\left\lfloor\frac{(p-2)!}{p(p-1)}\right\rfloor$$

زوج است.

در حالت سوم فرض می‌کنیم هر دو عدد n و $n+1$ مرکب باشند. به سادگی می‌توان نشان داد که n و $n+1$ هر دو $(n-1)!$ را می‌شمارند. چون $\gcd(n,n+1)=1$ نتیجه می‌گیریم $n(n+1)\,,(n-1)!$ را می‌شمارد یعنی

$$\frac{(n-1)!}{n(n+1)}$$

عدد صحیح است. با استفاده از تابع لژاندر به سادگی می‌توان دید این عدد صحیح، زوج است.

۵۱. [ARML ۲۰۰۲] عدد صحیح m در شرایط مسأله صدق می‌کند اگر و فقط اگر m در مجموعه زیر باشد

$$S=\{۸, p, ۲p, ۴p\} \text{ (} p \text{ یک عدد اول فرد است)}$$

بدون از دست دادن کلیت مسأله مستطیل $ABCD$ را در نظر بگیرید که می‌توان آن را هم به $n+m$ مربع به ضلع واحد و هم به m مربع بزرگ‌تر به ضلع x تقسیم کرد. چون اضلاع $ABCD$ طول‌های صحیح دارند، x باید یک عدد گویا باشد. قرار می‌دهیم $x=\frac{a}{b}$ که a و b اعداد صحیح نسبت به هم اول هستند. چون $x>۱$ پس $a>b$. مساحت $ABCD$ برابر است با

$$(n+m)\times ۱=n.(\frac{a}{b})^۲$$

با حل معادله بالا برای n خواهیم داشت

$$n=\frac{mb^۲}{a^۲-b^۲}=\frac{mb^۲}{(a-b)(a+b)}$$

چون $\gcd(a,b)=۱$ لذا $\gcd(b,a+b)=\gcd(b,a-b)=۱$ بنابراین $(a+b)(a-b)$ ، m را می‌شمارد. توجه کنید که زوجیت $a-b$ و $a+b$ یکی است. اگر m دو عامل فرد داشته باشد که هر دو بزرگ‌تر از ۱ باشند می‌نویسیم $m=ijk$ که $j>۱$ ، $k>۱$ اعداد صحیح فرد هستند. به این ترتیب از $(a+b,a-b)=(j,k)$ و $(a+b,a-b)=(jk,۱)$ دو مقدار متمایز $n=i(j-k)^۲/۴$ و $n=i(jk-۱)^۲/۴$ برای n بدست می‌آید که با یکتایی n در تضاد است. پس m حداکثر یک عامل فرد بزرگ‌تر از ۱ دارد؛ یعنی $m=۲^c$ یا $m=۲^c\times p$ که p عددی اول است. این دو حالت را جداگانه بررسی می‌کنیم.

در حالت اول فرض می‌کنیم $m=۲^c$. به سادگی می‌توان بررسی کرد که برای $c=۱,۲$ هیچ جوابی برای n نیست. اگر $c>۳$ آنگاه $(a-b\ ,\ a+b)=(۲,۴)$ و $(a-b\ ,\ a+b)=(۲,۸)$ منجر به دو مقدار متمایز $n=۲^{c-۳}$ و $n=۲^{c-۴}$ برای n می‌شود که باز هم با یکتایی n در تضاد است. برای $c=۳$ $(m=۸)$ داریم $(a,b)=(۴,۲)$ و $n=۱$.

در حالت دوم فرض می‌کنیم $m=۲^c\times p$. مشابه با حالت اول می‌توان نشان داد که $c\le ۲$ (با در نظر گرفتن $(a+b,a-b)=(p,۱)$). بنابراین $m=p,۲p,۴p$. جدول زیر نشان می‌دهد که همه این مقادیر جواب هستند.

m	$(a+b,a-b)$	(a,b)	n
p	$(p,1)$	$(\frac{p+1}{2},\frac{p-1}{2})$	$\frac{(p-1)^2}{4}$
$2p$	$(p,1)$	$(\frac{p+1}{2},\frac{p-1}{2})$	$\frac{(p-1)^2}{2}$
$4p$	$(p,1)$ یا $(2p,2)$	$(\frac{p+1}{2},\frac{p-1}{2})$ یا $(p+1,p-1)$	$(p-1)^2$

۵۲. ادعا می‌کنیم عدد صحیح n شرایط مسأله را برآورده می‌کند اگر و فقط اگر n مضرب مثبت ۱۰ نباشد. یک عدد را خوب می‌نامیم اگر شرایط مسأله را برآورده سازد. واضح است که مضارب ۱۰ خوب نیستند زیرا مضارب آن همگی به ۰ ختم می‌شوند. نشان خواهیم داد که همه اعداد صحیح مثبت دیگر خوب هستند. فرض کنید n یک عدد صحیح مثبت باشد که بر ۱۰ بخشپذیر نیست. چند حالت را بررسی می‌کنیم.

در حالت اول فرض می‌کنیم $n=5^k$ یا $n=2^k$ که k عدد صحیح مثبت است. همانطور که در مثال ۱. ۴۹ نشان داده‌ایم مضرب k رقمی n وجود دارد که ارقام آن غیرصفر هستند بنابراین n خوب است.

در حالت دوم فرض می‌کنیم که n نسبت به ۱۰ اول است. ادعا می‌کنیم n مضربی دارد که ارقامش همگی ۱ هستند عدد زیر را در نظر بگیرید

$$\underbrace{11\ldots1}_{\varphi(9n)}=\frac{10^{\varphi(9n)}-1}{9}$$

از قضیه اویلر این عدد بر n بخشپذیر است.

در حالت سوم فرض می‌کنیم $n=a^s.m$ که ۵ یا ۲ $=a$ و m نسبت به ۱۰ اول است. همانطور که در حالت اول بحث کردیم مضرب s رقمی a^s وجود دارد که ارقامش غیرصفر هستند. فرض کنید $t=\overline{a_{s-1}a_{s-2}\cdots a_0}$ آن عدد باشد. دنباله زیر را در نظر بگیرید.

$$\overline{a_{s-1}a_{s-2}\ldots a_0}\ ,\ \overline{a_{s-1}a_{s-2}\ldots a_0\,a_{s-1}a_{s-2}\ldots a_0}\ ,\ \ldots$$

k اُمین عدد دنباله با کنار هم قرار دادن k عدد t بدست می‌آید. همانطور که در حالت دوم نشان دادیم دو عضو مثلاً i ام و j ام $(i<j)$ در دنباله به پیمانه m هم‌نهشت هستند بنابراین

$$\overline{\underbrace{a_{s-1}a_{s-2}\dots a_0\dots a_{s-1}a_{s-2}\dots a_0}_{\overline{a_{s-1}a_{s-2}\dots a_0}\ \text{تا}\ (j-i)}\ \underbrace{00\dots00}_{0\ \text{تا}\ (j-i)}} \equiv 0 \pmod{m}$$

از $\gcd(m,10)=\gcd(m,a^s)=1$ و اینکه $t=\overline{a_{s-1}\dots a_0}$ ، a^s را می‌شمارد نتیجه می‌گیریم که

$$\underbrace{a_{s-1}a_{s-2}\dots a_0\dots a_{s-1}a_{s-2}\dots a_0}_{\overline{a_{s-1}a_{s-2}\dots a_0}\ \text{تا}\ (j-i)}$$

مضربی از $n=a^s.m$ است که ارقامش غیرصفر هستند.

۵- پاسخ مسائل پیشرفته

۱. [$MOSP$ ۱۹۹۸] مجموع مربعات k عدد صحیح متوالی با شروع از n را به صورت

$$s(n,k)=n^۲+(n+۱)^۲+\cdots+(n+k-۱)^۲$$

تعریف می‌کنیم.

(آ) با توجه به اینکه $s(n-۱,۳)=(n-۱)^۲+n^۲+(n+۱)^۲=۳n^۲+۲$ و (پیمانه ۳) $s(n-۱,۳)\equiv ۲$ لذا $s(n-۱,۳)$ مربع کامل نیست یعنی مجموع مربعات سه عدد متوالی مربع کامل نیست.

$s(n,۴)=۴(n^۲+۳n+۳)+۲$ و (پیمانه۴) $s(n,۴)\equiv ۲$ لذا $s(n,۴)$ و به عبارت دیگر مجموع مربعات چهار عدد متوالی مربع کامل نیست.

$s(n-۲,۵)=۵(n^۲+۲)$. از (پیمانه ۴) $s(n-۲,۵)\equiv n^۲+۲\equiv ۳$ یا ۲ نتیجه می‌گیریم که $s(n-۲,۵)$ که همان مجموع مربعات پنج عدد متوالی است، مربع کامل نیست.

$s(n-۲,۶)=۶n^۲+۶n+۱۹$. از اینکه $n^۲+n=n(n+۱)$ زوج است، لذا (پیمانه ۴) $s(n-۲,۶)\equiv ۶n(n+۱)+۱۹\equiv ۳$ و بنابراین $s(n-۲,۶)$ یا همان مجموع شش عدد صحیح متوالی مربع کامل نیست.

(ب) داریم $s(n-۵,۱۱)=۱۱(n^۲+۱۰)$. باید n را طوری پیدا کنیم که $۱۱(n^۲+۱۰)$ مربع کامل باشد بنابراین $n^۲+۱۰$ را می‌شمارد و یا (پیمانه ۱۱) $n^۲+۱۰\equiv ۰$. در نتیجه $n^۲-۱\equiv ۰$ (پیمانه ۱۱) یا $n-۱\equiv ۰$ (پیمانه ۱۱) و یا بطور خلاصه $n=۱۱m\pm ۱$ که m عددی صحیح است. به این ترتیب

$$s(n-۵,۱۱)=۱۱[(۱۱m\pm ۱)^۲+۱۰]=۱۱^۲(۱۱m^۲\pm ۲m+۱)=۱۱^۲[۱۰m^۲+(m\pm ۱)^۲]$$

مشاهده می‌شود که برای $m=۲$, $۱۰m^۲+(m+۱)^۲=۴۹=۷^۲$ و از آنجا مثال مورد نظر مسأله بدست می‌آید. بنابراین $s(۱۸,۱۱)=۷۷^۲$.

۲. [MOSP ۱۹۹۸] (آ) بیشترین ده بر یک ایجاد شده ۱ است. بنابراین ده بر یک‌هایی که در $۲x$ شمرده می‌شوند در $S(۲d)$ برای هر رقم d از x (در مبنای ۱۰) شمرده می‌شوند. در نتیجه $S(۲x)=\sum S(۲d)$ که جمع روی همه ارقام x انجام می‌شود. واضح است که برای هر رقم دهدهی $d \neq ۰$، $S(d)/S(۲d) \leq ۵$. بنابراین

$$\frac{S(x)}{S(۲x)}=\frac{\sum S(d)}{\sum S(۲d)} \leq ۵$$

این کران را نمی‌توان بهبود بخشید زیرا $S(۱۰)=۵S(۵)$.

می‌توان از قضیه ۱. ۴۵ (ت) نیز به صورت زیر استفاده کرد

$$S(x)=S(۱۰x) \leq S(۵)S(۲x)=۵S(۲x)$$

(ب) قرار می‌دهیم

$$p_k=\underbrace{۳۳\ldots۳۳}_{k}۴$$

بنابراین

$$۳p_k=۳\times(\underbrace{۳۳\ldots۳۳}_{k+۱}+۱)=\underbrace{۹۹\ldots۹۹}_{k+۱}+۳=۱\underbrace{۰۰\ldots۰۰}_{k}۲$$

و لذا

$$\frac{S(p_k)}{S(۳p_k)}=\frac{۳k+۴}{۳}$$

که کراندار نیست و اثبات ما کامل می‌شود.

۳. عدد n جالب است اگر و فقط اگر n توانی از ۲ باشد؛ یعنی $n=۲^k$ که k عددی صحیح نامنفی است. فرض کنید n جالب نباشد پس می‌توان نوشت

$$(*) \qquad n=m+(m+۱)+\cdots+(m+k)=\frac{(k+۱)(۲m+k)}{۲}$$

که m و k اعداد صحیح مثبت هستند. چون زوجیت $k+۱$ و $۲m+k$ با هم فرق دارد، یکی از آنها عدد فرد بزرگ‌تر از ۳ است بنابراین n باید یک عامل فرد بزرگ‌تر از ۳ داشته باشد. از این‌جا می‌فهمیم که ۲^k برای عدد صحیح مثبت k، جالب است.

حال این باقی می‌ماند که نشان دهیم همه اعداد صحیح مثبت دیگر n جالب نیستند. می‌نویسیم $n=۲^h.\ell$ که h یک عدد صحیح نامنفی و ℓ یک عدد فرد بزرگ‌تر از ۱ است. با توجه به این‌که

$\ell \neq ۲^{h+۱}$ ، اگر $\ell < ۲^{h+۱}$، n جالب نیست زیرا می‌توانیم در $(*)$ k و m را به صورت زیر قرار دهیم:

$$m = \frac{\ell - k}{۲} = \frac{\ell + ۱ - ۲^{h+۱}}{۲} \qquad \text{و} \qquad k = ۲^{h+۱} - ۱$$

اگر $\ell > ۲^{h+۱}$، n جالب نیست زیرا می‌توانیم در $(*)$ k و m را به‌صورت زیر قرار دهیم:

$$m = \frac{۲^{h+۱} - k}{۲} = \frac{۲^{h+۱} + ۱ - \ell}{۲} \qquad \text{و} \qquad k = \ell - ۱$$

بنابراین در هر صورت اگر n یک عامل فرد بزرگ‌تر از ۱ داشته باشد، جالب نیست.

۴. کمترین مقدار n، ۲۶ است.

اولین گام ما، محاسبه تعداد اعداد اول در مجموعه‌ی Sاست. برای هر عدد صحیح مثبت k، A_k را برابر زیرمجموعه‌ی مضارب k در S می‌گیریم. فرض کنید $P = \{۲,۳,۵,۷,۱۱\}$. تعداد اعضای زیر مجموعه‌ای از S که شامل اعداد بخشپذیر بر یک یا چند عدد از اعداد ۲، ۳، ۵، ۷ یا ۱۱ هستند را محاسبه می‌کنیم:

$$A = \bigcup_{k \in P} A_k = A_۲ \cup A_۳ \cup A_۵ \cup A_۷ \cup A_{۱۱}$$

با استفاده از اصل شمول و عدم شمول داریم

$$\begin{aligned} |A| = & \sum_{k \in P} |A_k| - \sum_{i<j \in P} |A_i \cap A_j| + \sum_{i<j<k \in P} |A_i \cap A_j \cap A_k| \\ & - \sum_{i<j<k<l \in P} |A_i \cap A_j \cap A_k \cap A_l| + |\bigcap_{k \in P} A_k| \\ = & ۱۳۷ - ۶۶ + ۱۶ - ۱ + ۰ = ۸۶ \end{aligned}$$

تنها عدد مرکبی که در S بوده ولی در A نیست $۱۶۹ = ۱۳^۲$ است. زیرا $۱۳ \times ۱۷ = ۲۲۱ > ۲۱۰$ بنابراین S شامل ۸۷ عدد مرکب و ۱۹ عدد اول است.

حال می‌توانیم ثابت کنیم در بین هر ۲۶ عدد موجود در S، دو عدد وجود دارد که نسبت به هم اول نیستند. با استفاده از اصل لانه کبوتری ازآنجا که ۱۹ عدد اول در S وجود دارد، حداقل ۷ عدد از ۲۶ عدد انتخابی مرکب هستند یعنی حداقل ۶ عضو از A هستند. اما این به معنای آن است که ۲ تا از آنها به یک مجموعه A_k $(k \in P)$ تعلق داشته و یک عامل مشترک دارند (به نام k) و بنابراین نسبت به هم اول نیستند.

در نهایت می‌توانیم یک زیر مجموعه S با ۲۵ عضو بسازیم که هر زوج از اعضای آن نسبت به هم اول هستند. P را مجموعه همه اعداد اول در S در نظر بگیرید می‌توان دید که مجموعه

$$P \cup \{11^2, 5^3, 2^7, 3^2 \times 17, 13^2, 7 \times 29\} = P \cup \{121, 125, 128, 153, 169, 203\}$$

یک مجموعه ۲۵ عضوی است که اعضای آن دو به دو نسبت به هم اول هستند.

۵. [۱۹۹۷ سن پطرزبورگ] جواب منفی است.

اضافه یا کم کردن عدد ۲ از یک عدد ما را بر آن می‌دارد تا پیمانه ۴ را مورد بررسی قرار دهیم. چرا که برای عدد صحیح a داریم (پیمانه ۴) $a+2 \equiv a-2$ یعنی اضافه کردن یا کسر کردن ۲ واحد در پیمانه ۴ عمل یکسانی است. عدد اولیه به پیمانه ۴ با ۳ هم‌نهشت است. ادعا می‌کنیم که همواره یک عدد هم‌نهشت با ۳ به پیمانه ۴ روی تخته وجود دارد: با فاکتورگیری از چنین عددی، یک عامل دارد که به پیمانه ۴ با ۱ هم‌نهشت است و تغییر ۲ واحدی آن عددی را می‌دهد که به پیمانه ۴، با ۳ هم‌نهشت است. از طرف دیگر ۹ به پیمانه ۴ با ۱ هم‌نهشت است و بنابراین نمی‌تواند در یک لحظه تمام اعداد روی تخته ۹ باشند.

۶. [IMO ۱۹۸۶]

اثبات اول: از آنجا که $3^2 = 1 - 5 \times 2$, $5^2 = 1 - 13 \times 2$ و $8^2 = 1 - 13 \times 5$، به دنبال یک عدد غیرمربع کامل در مجموعه‌ی $\{13d-1, 5d-1, 2d-1\}$ می‌گردیم. فرض کنید همه‌ی این اعداد مربع کامل هستند. یعنی

$$2d-1 = a^2, \quad 5d-1 = b^2, \quad 13d-1 = c^2 \quad (a, b, c \text{ اعداد صحیح})$$

چون a فرد است آن را به صورت $a = 2x+1$ نشان می‌دهیم و لذا $d = 2x(x+1)+1$ خواهد بود. ازآنجا که $x(x+1)$ همواره زوج است در نتیجه (پیمانه ۴) $d \equiv 1$ و بنابراین b و c زوج هستند. فرض کنید $b = 2y$ و $c = 2z$. از $5d = b^2 + 1$ و $13d = c^2 + 1$ داریم $8d = c^2 - b^2$ لذا

$$d = \frac{4y^2+1}{5} = \frac{14z^2+1}{13} = \frac{4z^2-4y^2}{8} = \frac{z^2-y^2}{2}$$

بنابراین زوجیت y و z یکی است. در این حالت (پیمانه ۴) $z^2 - y^2 \equiv 0$ در حالی‌که (پیمانه ۴) $d \equiv 1$ که تناقض است.

اثبات دوم: به پیمانه ۱۶ کار می‌کنیم. ابتدا n^2 به پیمانه ۱۶ را برای $n = 0, 1, \ldots, 8, 9$ محاسبه می‌کنیم و مشاهده می‌شود که تنها مانده‌های ممکن ۰, ۱, ۴, ۹ هستند.

اگر $۲d-۱$ مربع کامل نباشد که مسأله حل است. فرض کنید $۲d-۱$ مربع کامل باشد. بنابراین به پیمانه ۱۶ با ۰,۱,۴ یا ۹ هم‌نهشت است. چون $۲d$ زوج است، به پیمانه ۱۶ با ۲ یا ۱۰ هم‌نهشت بوده و به تبع آن d به پیمانه ۱۶ با ۱,۵,۹ یا ۱۳ هم‌نهشت است. بنابراین جدول زیر را خواهیم داشت

d	$۵d-۱$	$۱۳d-۱$
۱	۴	۱۲
۵	۸	۴
۹	۱۲	۴
۱۳	۴	۸

هیچ‌کدام از اعدادی که زیرشان خط کشیده شده است مربع کامل نیستند و در هر سطر یک چنین عددی وجود دارد. بنابراین برای همه مقادیر ممکن d که $۲d-۱$ مربع کامل باشد، حداقل یکی از اعداد $۵d-۱$ و $۱۳d-۱$ مربع کامل نیستند و حکم اثبات می‌شود.

۷. [۲۰۰۱ روسیه] واضح است که حداقل یک بار توزین لازم است. ادعا می‌کنیم همین یک بار کافی است. دو هزار توپ را به سه بسته $H_۱, H_۲$ و $H_۳$ به ترتیب با ۶۶۷,۶۶۷ و ۶۶۶ توپ تقسیم می‌کنیم. $H_۱$ و $H_۲$ را با هم وزن می‌کنیم. اگر وزن کل مساوی نباشد که مسأله حل است در غیر این‌صورت یک توپ از $H_۱$ دور می‌اندازیم تا به بسته $H'_۱$ با ۶۶۶ توپ برسیم. ادعا می‌کنیم که $H'_۱$ و $H_۳$ وزن‌های متفاوتی دارند. اگر چنین نباشد، این دو بسته به تعداد مساوی توپ ۱۰ گرمی، مثلاً n عدد، دارند. بنابراین $H_۱$ و $H_۲$ هر دو یا n توپ ۱۰ گرمی و یا هر دو $n+۱$ توپ ۱۰ گرمی دارند این به معنای آن است که ۱۰۰۰ باید با $۳n$ یا $۳n+۲$ برابر باشد که غیرممکن است.

۸. [۲۰۰۱ چین]

پاسخ اول: جواب ۱۵۹۴ است.

در ابتدا مشاهده می‌شود که a, b و c همگی باید فرد باشند: این مطلب از اینجا ناشی می‌شود که ۷ عدد اول مورد نظر، متمایز هستند و فقط یک عدد اول زوج داریم (اگر مثلاً a زوج باشد، b و c باید فرد باشند و بنابراین $a+b-c$ و $a+c-b$ هر دو زوج خواهند بود و برابر ۲). بنابراین کوچک‌ترین عدد اول از این ۷ عدد حداقل ۳ است.

دوم، بدون از دست دادن کلیت مسأله فرض می‌کنیم $a+b=۸۰۰$. چون $a+b-c>۰$، لذا $c<۸۰۰$. همچنین می‌دانیم c اول است. بنابراین از آنجا که $۴۷\times۱۷=۷۹۹$، داریم $c\le ۷۹۷$ به این ترتیب بیش‌ترین مقدار عدد اول $a+b+c$ بیشتر از ۱۵۹۷ نیست. با ترکیب این دوکران، d را به صورت زیر محدود می‌کنیم

$$d\le ۱۵۹۷-۳=۱۵۹۴$$

حال این باقی می‌ماند که مشاهده کنیم با انتخاب $a=۱۳$, $b=۷۸۷$ و $c=۷۹۷$ به این حد دست پیدا می‌کنیم. ۴ عدد اول دیگر ۳, ۲۳, ۱۵۷۱ و ۱۵۹۷ می‌باشد.

پاسخ دوم: بدون از دست دادن کلیت مسأله فرض می‌کنیم $a+b=۸۰۰$ (واضح است که a و b هر دو فرد هستند) اعداد c, $a+b+c=۸۰۰+c$ و $a+b-c=۸۰۰-c$ اول هستند. آنها را به پیمانه ۳ بررسی می‌کنیم. به سادگی می‌توان دید دقیقاً یکی از آنها به پیمانه ۳ با صفر هم‌نهشت است. یعنی یکی از آنها ۳ است. پس یا $c=۳$ یا $۸۰۰-c=۳$ ($c=۷۹۷$). اگر $c=۳$ آنگاه $a+b+c=۸۰۳$. $d<a+b+c=۸۰۳$. اگر $c=۷۹۷$ آنگاه $d\le a+b+c-۳=۱۵۹۴$ و راه حل را مانند پاسخ اول به پایان می بریم.

۹. فرض می‌کنیم اعداد صحیح m و n وجود داشته باشند که $S(m,n)$ صحیح باشد. واضح است که $n\ge ۱$. در نتیجه در بین اعداد $m, m+۱, \dots, m+n$ چند عدد زوج وجود دارد لذا $\ell=\operatorname{lcm}(m,m+۱,\dots,m+n)$ زوج است. داریم

$$\ell S(m,n)=\frac{\ell}{m}+\frac{\ell}{m+۱}+\cdots+\frac{\ell}{m+n} \qquad (*)$$

طبق فرض ما سمت چپ عبارت فوق زوج است. با نشان دادن اینکه سمت راست این رابطه فرد است به تناقض خواهیم رسید.

برای هر عدد صحیح i , $۰\le i\le n$ فرض کنید ۲^{a_i} بطور کامل $m+i$ را می‌شمارد. قرار می‌دهیم $t=\max\{a_۰,a_۱,\dots,a_n\}$ بنابراین $۲^t \| \ell$.

فرض کنید $a_j=t$ $(۰\le j\le n)$ ادعا می‌کنیم که j منحصر به فرد است. فرض کنید $a_j=a_{j_۱}$ که $۰\le j<j_۱\le n$. بنابراین $m+j=۲^{a_j}.k$ و $m+j_۱=۲^{a_j}.k_۱$ که k و $k_۱$ اعداد صحیح مثبت فرد هستند. از این رو $k+۱$ عدد زوجی بین k و $k_۱$ خواهد بود و لذا

$$m+j<۲^{a_j}.(k+۱)<۲^{a_j}.k_۱=۲^{a_j}.k_۱=m+j_۱$$

بنابراین $۲^{a_j}.(k+۱)$ در بین اعداد m تا $m+n$ قرار دارد و بر $۲^{a_j+۱}$ بخشپذیر است که با فرض بیشینه بودن $a_j=t$ تناقض دارد لذا a_j یکتاست. به این ترتیب $\frac{\ell}{m+i}$ برای همه iها که $۰\le i\le n$ و $i\ne j$، زوج بوده و $\frac{\ell}{m+j}$ فرد است. بنابراین همه عبارات سمت راست رابطه (*) بجز یکی زوج هستند که به معنای آن است که سمت راست رابطه (*) فرد بوده و با زوج بودن سمت چپ آن در تناقض است. پس فرض ما غلط بوده و $S(m,n)$ عدد صحیح نیست.

۱۰. [۲۰۰۱ سن پطرزبورگ] قرار می‌دهیم $m=n+k$ در نتیجه

$$\begin{aligned}\operatorname{lcm}(m,n)+\operatorname{lcm}(m+1,n+1)&=\\ &=\frac{mn}{\gcd(m,n)}+\frac{(m+1)(n+1)}{\gcd(m+1,n+1)}\\ &>\frac{mn}{\gcd(n+k,n)}+\frac{mn}{\gcd(m+1,n+1)}\\ &=\frac{mn}{\gcd(k,n)}+\frac{mn}{\gcd(n+k+1,n+1)}\\ &=\frac{mn}{\gcd(k,n)}+\frac{mn}{\gcd(k,n+1)}\end{aligned}$$

چون $\gcd(k,n)\mid k$ و $\gcd(k,n+1)\mid k$ نتیجه می‌گیریم که $\gcd(k,n)$ هیچ عامل اول مشترکی با $\gcd(k,n+1)$ ندارد زیرا اگر چنین باشد n و $n+1$ عامل اول مشترک خواهند داشت که غیرممکن است. از آنجا که هر دوی آنها k را می‌شمارند، حاصلضربشان نیز k را می‌شمارد. بنابراین $\gcd(k,n).\gcd(k,n+1)\le k$. در نتیجه

$$\begin{aligned}\operatorname{lcm}(m,n)+\operatorname{lcm}(m+1,n+1)&>\frac{mn}{\gcd(k,n)}+\frac{mn}{\gcd(k,n+1)}\\ &\ge 2mn\sqrt{\frac{1}{\gcd(k,n)\gcd(k,n+1)}}\ge 2mn\sqrt{\frac{1}{k}}=\frac{2mn}{\sqrt{m-n}}\end{aligned}$$

که این رابطه از نامساوی واسطه حسابی ـ هندسی بدست آمده است.

۱۱. **اثبات اول:** فرض کنید k یک عدد صحیح نامنفی باشد.

اگر k زوج باشد، مثلاً $k=2n$، از رابطه

$$2n=(3n)^2+(4n-1)^2+(5n-1)^2$$

و حقایق ساده جبری که برای $n>1$ ، $3n<4n-1<5n-1$ و

$$0=3^2+4^2-5^2 \quad , \quad 2=5^2+11^2-12^2$$

حکم برای اعداد زوج ثابت می‌شود. اگر k فرد باشد، از رابطه زیر استفاده می‌کنیم

$$2n+3=(3n+2)^2+(4n)^2-(5n+1)^2$$

که برای $n>2$ ، $3n+2<4n<5n+1$. با توجه به روابط

$$۱=۴^۲+۷^۲-۸^۲\ ,\ ۳=۴^۲+۶^۲-۷^۲$$
$$۵=۴^۲+۵^۲-۶^۲\ ,\ ۷=۶^۲+۱۴^۲-۱۵^۲$$

حکم برای اعداد فرد نیز ثابت می‌شود.

اثبات دوم: یک روش کلی‌تر برای این مسأله ارایه می‌کنیم. نکته کلیدی این است که قدر مطلق تفاضل بین اعداد مربع کامل متوالی بطور خطی افزایشی است. برای هر عدد صحیح نامنفی k، عدد صحیح مثبت و بزرگ a را چنان انتخاب می‌کنیم که زوجیت آن با k فرق داشته باشد. سپس قرار می‌دهیم $c=b+۱$ و لذا $k=a^۲+b^۲-c^۲=a^۲-(۲b+۱)$. چون زوجیت a و k با هم فرق دارد $a^۲-k$ فرد است و بنابراین

$$b=\frac{a^۲-k-۱}{۲}$$

یک عدد صحیح مثبت است. از آنجا که سمت راست رابطه‌ی فوق با توان دوم a متناسب است، برای یک مقدار بزرگ a، طرف راست رابطه‌ی مذکور از a بزرگ‌تر است و بنابراین شرط $a<b<c=b+۱$ برقرار بوده و حکم ثابت می‌شود.

۱۲. توجه: ممکن است این فکر به ذهن برسد که $a_k=k!$. اما در این حالت مسأله برای $a=۱$ یا $a=-۱$ مشکل می‌شود. ما دو روش برای اصلاح این دنباله ارائه می‌کنیم.

پاسخ اول: جواب مثبت است و چنین دنباله‌ای وجود دارد.

برای هر عدد صحیح مثبت k، فرض کنید $a_k=(k!)^۳$. اگر $a=\pm۱$ آنگاه $a_k+a=(k!)^۳\pm۱$ مرکب است چرا که چند جمله ای های $x^۳+۱$ و $x^۳-۱$ به صورت $(x+۱)(x^۲-x+۱)$ و $(x-۱)(x^۲+x+۱)$ تجزیه می‌شوند. اگر $|a|>۱$ آنگاه برای $k\geq|a|$,a ,$k!$ را می‌شمارد لذا a ,a_k+a را نیز برای $k\geq|a|$ می‌شمارد.

پاسخ دوم: قرار می‌دهیم $a_k=(۲k)!+k$. برای همه‌ی اعداد صحیح $k\leq|a|$ و $k\geq۲-a$ داریم $۲\leq k+a\leq۲k$ بنابراین a_k+a بر $k+a$ بخشپذیر بوده و لذا برای هر k با شرایط فوق مرکب است.

۱۳. از استقرا روی n استفاده می‌کنیم. برای $n=۱$ از $۵\pm۴\pm۳\pm۲\pm۱$ همه اعداد صحیح مثبت فرد کوچک‌تر یا مساوی $(۱+۱)(۱+۴)=۱۵$ را می‌توان بدست آورد:

$$\pm ۱-۲+۳+۴-۵=۱\ ,\ -۱+۲+۳+۴-۵=۳$$
$$-۱+۲+۳-۴+۵=۵\ ,\ -۱+۲-۳+۴+۵=۷$$
$$-۱-۲+۳+۴+۵=۹\ ,\ +۱-۲+۳+۴+۵=۱۱$$
$$-۱+۲+۳+۴+۵=۱۳\ ,\ +۱+۲+۳+۴+۵=۱۵$$

فرض کنیم حکم برای $n=k$ برقرار باشد که k عدد صحیح مثبت است؛ یعنی از $\pm ۱\pm ۲\pm\cdots\pm(۴k+۱)$ با انتخاب‌های مناسب علائم + و − می‌توان همه‌ی اعداد صحیح مثبت فرد کوچک‌تر یا مساوی $(۱+۴k)(۱+۲k)$ را بدست آورد. حال فرض می‌کنیم $n=k+۱$.

مشاهده می‌شود که $-(۴k+۲)+(۴k+۳)+(۴k+۴)-(۴k+۵)=۰$ بنابراین از $\pm ۱\pm ۲\pm\cdots\pm(۴k+۵)$ با انتخاب‌های مناسب علائم + و − می‌توان همه اعداد صحیح مثبت فرد کوچک‌تر یا مساوی $(۱+۴k)(۱+۲k)$ را به‌دست آورد.

کافی است همه‌ی اعداد فرد m به‌صورت

$$(*)\quad (۲k+۱)(۴k+۱)<m\le(۲k+۳)(۴k+۵)=(۲n+۱)(۴n+۱)$$

را به‌دست آورد. تعداد

$$\frac{(۲k+۳)(۴k+۵)-(۲k+۱)(۴k+۱)}{۲}=۸k+۷$$

عدد فرد m وجود دارد. هر یک از این اعداد صحیح را می‌توان دقیقاً به یکی از شکل‌های زیر نوشت:

$$(۲n+۳)(۴n+۵)=+۱+۲+\cdots+(۴n+۵)$$

یا برای $k=۱,۲,\ldots,۴n+۵$

$$(۲n+۳)(۴n+۵)-۲k=+۱+۲+\cdots+(k-۱)-k+(k+۱)+\cdots+(۴n+۴)+(۴n+۵)$$

و یا برای $\ell=۱,۲,\ldots,۴n+۱$

$$(۲n+۱)(۴n+۵)-۲\ell=+۱+۲+\cdots+(\ell-۱)-\ell+(\ell+۱)+\cdots+(۴n+۴)-(۴n+۵)$$

به این ترتیب همه اعداد m از (*) به دست می‌آیند و استقرا کامل می‌شود.

۱۴. اثبات اول: عدد صحیح n را قابل ارائه می‌نامیم اگر اعداد صحیح نامنفی x و y وجود داشته باشند که $n=ax+by$. در ابتدا نشان می‌دهیم که $n=ab-a-b$ قابل ارائه نیست. فرض کنید $ab-a-b=ax+by$ که x و y اعداد صحیح نامنفی هستند. معادله اخیر را به پیمانه a و سپس به پیمانه b در نظر بگیرید. خواهیم داشت (پیمانه a) $-b\equiv by$ و (پیمانه b) $-a=ax$. از آنجا که $\gcd(a,b)=۱$ است، لذا (پیمانه a) $y\equiv -۱$ و (پیمانه b) $x\equiv -۱$. چون x و y نامنفی هستند در نتیجه $y\ge a-۱$ و $x\ge b-۱$. بنابراین

$$ab-a-b=n=ax+by\geq a(b-1)+b(a-1)=2ab-a-b$$

که برای اعداد صحیح مثبت a و b غیر ممکن است. پس فرض ما غلط بوده و $n=ab-a-b$ قابل ارائه نیست.

حال نشان می‌دهیم $n>ab-a-b$ قابل ارائه است. از $\gcd(a,b)=1$ و قضیه ۲۴.۱ می‌دانیم

$$\{n,n-b,n-2b,\ldots,n-(a-1)b\}$$

یک مجموعه کامل مانده‌ها به پیمانه a است. بنابراین دقیقاً یک y وجود دارد که $0\leq y\leq a-1$ و $n-yb\equiv 0\ (a)$ (پیمانه a) و یا برای عدد صحیح x، $n-yb=ax$. اگر $x\geq 0$ که مسأله حل است. اگر $x<0$ آنگاه $x\leq -1$ و بنابراین

$$n-(a-1)b\leq n-yb=ax\leq -a$$

یا $n\leq ab-a-b$ که با شرط $n>ab-a-b$ تناقض دارد. بنابراین هر دوی x و y نامنفی بوده و لذا $n>ab-a-b$ قابل ارائه است.

اثبات دوم: ادعای زیر را اثبات می‌کنیم:

اگر m و n اعداد صحیحی باشند که $m+n=ab-a-b$ آنگاه دقیقاً یکی از m و n قابل ارائه است.

اگر $n>ab-a-b$ آنگاه m باید منفی باشد که به وضوح قابل ارائه نیست. بنابر ادعای ما n باید قابل ارائه باشد. اگر $n=ab-a-b$ آنگاه $m=0$ که به وضوح قابل ارائه می‌باشد (با $x=y=0$) و لذا بنابر ادعای ما $n=ab-a-b$ قابل ارائه نیست.

حال این باقی می‌ماندکه ادعای خود را ثابت کنیم. از قضیه بزو زوج (x,y) از اعداد صحیح وجود دارند که $ax+by=n$. از $ax+by=a(x-bt)+b(y+at)$ نتیجه می‌گیریم که همواره می‌توان x را به اندازه یک مضرب b کم یا زیاد نمود. لذا می‌توان فرض کرد $0\leq x\leq b-1$. به این ترتیب عدد $n=ax+by$ قابل ارائه است اگر و فقط اگر تحت شرط اضافی $0\leq x\leq b-1$ قابل ارائه باشد. فرض کنید

$$n=ax+by\quad,\quad m=as+bt$$

که x,y,s و t اعداد صحیح بوده و x و s اعداد نامنفی کوچکتر از b هستند؛ یعنی $0\leq x,s\leq b-1$ بنابراین

$$ax+by+as+bt=m+n=ab-a-b$$

یا

$$(*)\quad ab-(x+s+1)a-(y+t+1)b=0$$

چون $\gcd(a,b)=1$، معادله (*) نشان می‌دهد که b باید $x+s+1$ را بشمارد. با توجه به این که $1\le x+s+1\le 2b-1$، لذا $x+s+1=b$ و معادله (*) به‌صورت $(y+t+1)b=0$ یا $y+t+1=0$ در می‌آید. به سادگی می توان دید که یکی از y و t نامنفی و دیگری منفی است یعنی یکی از آنها قابل ارائه و دیگری غیرقابل ارائه است.

توجه: آیا می‌توانید این نتیجه را برای سه عدد دو به دو نسبت به هم اول a,b,c تعمیم دهید؟

۱۵. [۲۰۰۳ چین] کافی است اعداد صحیح مثبت m,k و n را با شرایط $k>m>n$ و $k<m+n$ چنان پیدا کنیم که

$$3^k \equiv 3^m \equiv 3^n \quad (\text{پیمانه } 10^4)$$

یا

$$3^k \equiv 3^m \equiv 3^n \ (\text{پیمانه } 5^4) \quad \text{و} \quad 3^k \equiv 3^m \equiv 3^n \ (\text{پیمانه } 2^4) \quad (*)$$

فرض کنید $d_1=ord_{2^4}(3)$, $d_2=ord_{5^4}(3)$ و $d=\operatorname{lcm}(d_1,d_2)$. از قضیه ۳۰.۱، d ، $k-m$ و $m-n$ را می‌شمارد. می‌توان بررسی کرد که $d_1=4$، می‌دانیم $d_2,\ \varphi(5^4)=5^4-5^3=500$ را می‌شمارد. ادعا می‌کنیم $d_2=500$. اگر $d_2<500$، آنگاه باید یک مقسوم‌علیه $\frac{500}{2}=250$ یا $\frac{500}{5}=100$ باشد. کافی است نشان دهیم.

الف) (پیمانه 5^4) $3^{250}\not\equiv 1$ و ب) (پیمانه 5^4) $3^{100}\not\equiv 1$

قسمت (الف) از (پیمانه 5^4) $3^{250}\equiv 3^2\equiv -1$ و $\varphi(5)=4$ اثبات می‌شود. از قضیه دو جمله‌ای داریم

$$3^{100}\equiv (10-1)^{50}\equiv \binom{50}{48}\times 10^2-\binom{50}{49}\times 10+1\not\equiv 1 \quad (\text{پیمانه } 5^4)$$

که همان اثبات قسمت (ب) است. بنابراین $d_2=500$ و $d=500$. شرط (*) برقرار خواهد بود اگر و فقط اگر $k-m$ و $m-n$ مضارب $d=500$ باشند.

قرار می‌دهیم $m=500s+n$ و $k=500t+m=500(s+t)+n$ که s و t اعداد صحیح مثبت هستند. محیط مثلث برابر $k+m+n=500(2s+t)+3n$ است. شرط $k<m+n$ منجر به رابطه $n<500t$ می‌شود. بنابراین کمترین مقدار محیط برابر $3003=501\times 5+3\times 500+3$ است که از $s=t=1$ و $n=501$ بدست می‌آید.

۱۶. [۱۹۹۶ بالتیک] فرض کنید فقط شرایط اولیه محدودی وجود دارند که به ازای آنها نفر دوم می‌تواند طوری بازی کند که برنده شود. بنابر فرض ما عدد صحیح مثبت N وجود دارد که اگر $n>N$ سنگریزه روی میز باشد بازیکن اول می‌تواند طوری بازی کند که برنده شود.

حالت اولیه $(N+1)^۲-۱$ سنگریزه روی میز را در نظر بگیرید. فرض کنید $P_۱$ و $P_۲$ به ترتیب بیانگر بازیکن اول و دوم باشد. با فرض ما $P_۱$ می‌تواند طوری بازی کند که برنده شود و برای این منظور $P_۱$ در اولین حرکتش x سنگریزه بر می‌دارد واضح است که $x \le N^۲$ و برای $P_۲$ حداقل $(N+1)^۲-N^۲-۱$ سنگریزه روی میز باقی‌مانده است. بر اساس فرض ما، در این لحظه $P_۲$ می‌تواند طوری بازی کند که برنده شود. اما این امکان ندارد که برای یک شرط اولیه هر دو بازیکن بتوانند طوری بازی کنند که برنده شوند بنابراین فرض ما غلط بوده و بی‌نهایت شرط اولیه وجود دارد که به ازای آنها نفر دوم می‌تواند طوری بازی کند که برنده شود.

۱۷. [MOSP ۱۹۹۷]

اثبات اول: n اُمین عضو دنباله را با x_n نشان می‌دهیم. از $x_{n+۱}=۱۰x_n-۱$ نتیجه می‌گیریم که $\gcd(x_n,x_{n+۱})=۱$. برای اثبات اینکه زیردنباله نامحدودی از این دنباله وجود دارد که اعضای آن دو به دو نسبت به هم اول هستند کافی است ثابت کنیم تعداد اعضای زیردنباله اهمیتی نداشته و همواره می‌تواند شامل حداقل یک عضو بیشتر باشد. برای این منظور توجه کنید که x_n، x_{mn} را می‌شمارد. فرض کنید p حاصل‌ضرب (یا کوچک‌ترین مضرب مشترک) همه اندیس‌هایی باشد که قبلاً در زیر دنباله آمده‌اند. به این ترتیب هر عدد عضو دنباله، x_p را می‌شمارد بنابراین $x_{p+۱}$ می‌تواند به زیر دنباله اضافه شده و حکم اثبات می شود.

اثبات دوم: از همان تعریف متغیرهای اثبات اول استفاده می‌کنیم. با توجه به اینکه $x_n=\frac{۱۰^n-۱}{۹}$ از قسمت دوم مسأله مقدماتی ۳۸ برای اعداد صحیح m و n که $\gcd(m,n)=۱$ داریم

$$\gcd(x_m,x_n)=\frac{\gcd(۱۰^m-۱,۱۰^n-۱)}{۹}=\frac{۱۰^{\gcd(m,n)}-۱}{۹}=۱$$

بنابراین زیر دنباله $\{x_p\}$ که p عدد اول است، شرایط مسأله را برآورده می‌کند.

توجه: اثبات اویلر از وجود بی‌نهایت عدد اول ارتباط بین این دو اثبات را آشکار می‌سازد.

۱۸. با جایگذاری می‌توان نشان داد که

$$n_k=n^k m+n^{k-۱}+\cdots+n+۱=n^k m+\frac{n^k-۱}{n-۱}$$

که k عدد صحیح مثبت است. بنابراین

$$n_{\varphi(m)}=n^{\varphi(m)}.m+\frac{n^{\varphi(m)}-۱}{n-۱}$$

از قضیه اویلر داریم $m \mid n^{\varphi(m)}-1$ و چون $\gcd(m,n-1)=1$ در نتیجه

$$m \mid \frac{n^{\varphi(m)}-1}{n-1}$$

پس $n_{\varphi(m)}$ ، m را می‌شمارد. از آنجا که $\varphi_{(m)} \le m-1$ لذا $n_{\varphi(m)}$ اول نبوده و حکم اثبات می‌شود.

۱۹. [۱۹۹۹ ایرلند] اگر شرط داده برای عدد صحیح m برقرار باشد، m باید توان چهارم کامل باشد و می‌توان تجزیه آن به عوامل اول را به صورت $m = 2^{4a_2} \times 3^{4a_3} \times 5^{4a_5} \times 7^{4a_7} \times \cdots$ برای اعداد صحیح نامنفی $a_2, a_3, a_5, a_7, \ldots$ نشان داد. تعداد مقسوم علیه‌های مثبت m برابر است با

$$(4a_2+1)(4a_3+1)(4a_5+1)(4a_7+1)\cdots$$

این عدد فرد است لذا m نیز فرد بوده و $a_2 = 0$ بنابراین

$$1=\frac{4a_3+1}{3^{a_3}}\times\frac{4a_5+1}{5^{a_5}}\times\frac{4a_7+1}{7^{a_7}}\cdots = x_3 x_5 x_7 \ldots$$

که برای هر p ، $x_p = \frac{4a_p+1}{p^{a_p}}$. مقدار x_p را در سه حالت: $p=3$ ، $p=5$ و $p>5$ مورد بررسی قرار می‌دهیم. اگر $a_3 = 1$ آنگاه $x_3 = \frac{5}{3}$ و اگر ۲ یا ۰ $a_3 =$ آنگاه $x_3 = 1$. اگر $a_3 > 2$ از نامساوی برنولی داریم

$$3^{a_3} = (8+1)^{a_3/2} > 8\left(\frac{a_3}{2}\right)+1 = 4a_3+1$$

یعنی $x_3 < 1$. اگر ۱ یا ۰ $a_5 =$ آنگاه $x_5 = 1$ و اگر $a_5 \ge 2$، از نامساوی برنولی داریم

$$5^{a_5} = (24+1)^{a_5/2} \ge 24\times\frac{a_5}{2}+1 = 12a_5+1$$

به این ترتیب

$$x_5 \le \frac{4a_5+1}{12a_5+1} \le \frac{9}{25}$$

در نهایت برای $p>5$ وقتی که $a_p = 0$ داریم $x_p = 1$؛ وقتی‌که $a_p = 1$ داریم $p^{a_p} = p > 5 = 4a_p+1$ و بنابراین $x_p < 1$؛ وقتی $a_p > 1$ مجدداً از نامساوی برنولی داریم

$$p^{a_p} > 5^{a_p} > 12a_p+1$$

و مانند آنچه قبلاً انجام دادیم $x_p < \frac{9}{25}$.

حال اگر $a_3 \neq 1$، برای هر p، $x_p \leq 1$. با توجه به تساوی $x_3 x_5 x_7 \cdots = 1$، برای هر p، $x_p = 1$. این به معنای آن است که $a_3 \in \{0,2\}$، $a_5 \in \{0,1\}$ و $a_7 = a_{11} = \cdots = 0$. بنابراین $m = 1^4, (3^2)^4, 5^4$ یا $(5 \times 3^2)^4$ در غیر این‌صورت اگر $a_3 = 1$، عدد $m = 5^4 (4a_5 + 1)^4 (4a_7 + 1)^4 \cdots$ را می‌شمارد لذا برای عدد اول $p' \geq 5$، $4a_{p'} + 1 \mid 3$ و $a_{p'} \geq 2$. از مباحث فوق داریم $x_{p'} \leq \frac{9}{25}$ پس

$$x_3 x_5 x_7 \cdots \leq \frac{5}{3} \times \frac{9}{25} < 1$$

که تناقض است.

بنابراین تنها اعداد صحیح m عبارتند از $1, 5^4, 3^8$ و $3^8 \times 5^4$ هستند و به سادگی می‌توان بررسی کرد که این اعداد در شرایط مسأله صدق می‌کنند.

۲۰. [۱۹۹۹ رومانی] یک عدد صحیح را میرا گوییم اگر مجموع ارقامش بر ۱۱ بخشپذیر باشد. $d(n)$ را برابر مجموع ارقام عدد صحیح مثبت n می‌گیریم. مشاهده می‌شود که:

(آ) اگر n به یک صفر ختم شود، اعداد $n, n+1, \ldots, n+9$ فقط در رقم یکانشان با هم فرق دارند که از ۰ تا ۹ تغییر می‌کند. بنابراین $d(n), d(n+1), \ldots$ و $d(n+9)$ یک تصاعد حسابی با قدر نسبت ۱ است. لذا اگر (پیمانه ۱۱) $d(n) \not\equiv 1$ آنگاه یکی از این اعداد میرا است.

(ب) حال فرض کنید n به k تا ۹ ختم شده باشد که $k \geq 0$ سپس $d(n+1) = d(n) + 1 - 9k$ و k رقم آخر $n+1$ بجای ۹ همگی صفر هستند و رقم سمت چپ این صفرها یکی بیشتر از رقم متناظر آن در n است.

(پ) فرض کنید n به یک صفر ختم شود و (پیمانه۱۱) $d(n) \equiv d(n+10) \equiv 1$. چون (پیمانه ۱۱) $d(n) \equiv 1$، باید داشته باشیم (پیمانه ۱۱) $d(n+9) \equiv 10$. اگر $n+9$ به k تا ۹ ختم شود، داریم (پیمانه ۱۱) $d(n+10) - d(n+9) \equiv 1 - 9k \equiv 2$ یعنی (پیمانه۱۱) $k \equiv 6$.

(۱) فرض کنید ۳۹ عدد متوالی داریم که هیچ‌کدام میرا نیستند. یکی از ۱۰ عدد اول به یک صفر ختم می‌شود آن را n می‌نامیم. چون هیچ‌یک از اعداد $n+1, \ldots, n+9$ میرا نیستند از بخش (آ) باید داشته باشیم (پیمانه ۱۱) $d(n) \equiv 1$ و بطور مشابه (پیمانه ۱۱) $d(n+10) \equiv 1$ و (پیمانه ۱۱) $d(n+20) \equiv 1$. از بخش (پ)، هر دو عدد $n+9$ و $n+19$ باید به حداقل ۶ تا ۹ ختم شوند. اما این غیرممکن است زیرا $n+10$ و $n+20$ هر دو نمی‌توانند مضربی از یک میلیون باشند.

(۲) فرض کنید $N, N+1, \ldots$ و $N+37$، ۳۸ عدد متوالی باشند که هیچ‌یک از آن‌ها میرا نباشند. با تحلیلی مشابه بخش(۱) هیچ‌یک از ۹ عدد اول نمی‌تواند به صفر ختم شود. بنابراین $N+9$ همانند $N+19$ و $N+29$ باید به صفر ختم شود. باید داشته باشیم (پیمانه ۱۱) $d(N+9) \equiv 1 \equiv d(N+19)$. بنابراین (پیمانه ۱۱) $d(N+18) \equiv 10$. اگر $N+18$ به k تا ۹ ختم شود آنگاه باید داشته باشیم (پیمانه ۱۱) $k \equiv 6$.

کوچک‌ترین عدد با چنین خاصیتی ۹۹۹۹۹۹ است که منجر به ۳۸ عدد متوالی ۹۹۹۹۸۱, ۹۹۹۹۸۲, ... , ۱۰۰۰۰۱۸ می‌شود. هیچ یک از این اعداد میرا نیستند: مجموع ارقام آنها به پیمانه ۱۱ به‌ترتیب با ۱,۲,...,۱۰,۱,۲,...,۱۰,۱,۲,...,۱۰,۱,۲,...,۱۰,۹,...,۱۰ هم‌نهشت هستند.

۲۱. [APMO ۱۹۹۸] جواب ۴۲۰ است که $۷ < \sqrt[۳]{۴۲۰} < ۸$ و $\operatorname{lcm}(۱,۲,۳,۴,۵,۶) = ۴۲۰$.

فرض کنید $n < ۴۲۰$ یک عدد صحیح باشد که هر عدد صحیح مثبت کوچک‌تر از $\sqrt[۳]{n}$, n را بشمارد. چون $\sqrt[۳]{n} > ۷$ لذا $۴۲۰ = \operatorname{lcm}(۱,۲,۳,۴,۵,۶,۷)$، n را می‌شمارد. بنابراین $n \geq ۸۴۰$ و $\sqrt[۳]{n} > ۹$. به این ترتیب $۲۵۲۰ = \operatorname{lcm}(۱,۲,...,۹)$ باید n را بشمارد و $\sqrt[۳]{n} > ۱۳$. m را برابر بزرگترین عدد صحیح مثبت کمتر از $\sqrt[۳]{n}$ می‌گیریم یعنی $m < \sqrt[۳]{n} \leq m+۱$. داریم $m \geq ۱۳$ و $\operatorname{lcm}(۱,۲,...,m)$, n را می‌شمارد اما

$$\operatorname{lcm}(m-۳, m-۲, m-۱, m) \geq \frac{m(m-۱)(m-۲)(m-۳)}{۶} \qquad (\dagger)$$

چون ۲و۳ تنها عوامل مشترک ممکن بین این ۴ عدد هستند. بنابراین

$$\frac{m(m-۱)(m-۲)(m-۳)}{۶} \leq n \leq (m+۱)^۳$$

که به موجب آن

$$m \leq ۶(۱+\frac{۲}{m-۱})(۱+\frac{۳}{m-۲})(۱+\frac{۴}{m-۳})$$

سمت چپ این نامعادله یک تابع افزایشی m و سمت راست آن یک تابع کاهشی m است. اما برای $m = ۱۳$ داریم

$$۱۳ \times ۱۲ \times ۱۱ \times ۱۰ = ۱۷۱۶۰ > ۱۶۴۶۴ = ۶ \times ۱۴^۳$$

بنابراین این نامعادله برای همه‌ی مقادیر $m \geq ۱۳$ ناصحیح است. در نتیجه هیچ n بزرگ‌تر از ۴۲۰ شرایط مسأله را برآورده نمی‌کند.

توجه: رایان کو اشاره کرده است که نامساوی (†) را می‌توان به‌صورت زیر بهبود بخشید.

$$\operatorname{lcm}(m-۳, m-۲, m-۱, m) \geq \frac{(m-۱)(m-۲)(m-۳)(m-۴)}{۲}$$

۲۲. [USAMO ۱۹۹۱] از استقرای قوی روی n استفاده می‌کنیم. پایه استقرا $n = ۱$ به وضوح برقرار است. فرض کنید حکم برای $n \leq k$ برقرار باشد که k یک عدد صحیح مثبت است. حالت $n = k+۱$ را بررسی می‌کنیم.

اگر $n=k+1$ فرد باشد از قضیه اویلر (پیمانه n) $2^{\varphi(n)}\equiv 1$. چون $\varphi(n)<n$، از فرض استقرا دنباله $a_1,a_2,\ldots$ در نهایت به یک عدد ثابت به پیمانه $\varphi(n)$ می‌رسد به عبارت دیگر برای مقدار بزرگ i $a_i\equiv c$ (پیمانه $\varphi(n)$) در نتیجه

$$a_{i+1}\equiv 2^{a_i}\equiv 2^c \quad (\text{پیمانه } n)$$

که مقدار ثابتی بوده و حکم استقرا برای این حالت تکمیل می‌شود.

اگر $n=k+1$ زوج باشد. می‌نویسیم $n=k+1=2^q.m$ که k عدد صحیح مثبت و m یک عدد صحیح فرد است. از فرض استقرا دنباله $a_1,a_2,\ldots$ در نهایت به پیمانه m به یک عدد ثابت می‌رسد. واضح است که برای i به اندازه کافی بزرگ (پیمانه 2^q) $a_i\equiv 0$. چون m و 2^q نسبت به هم اول بوده و هردو $a_{i+1}-a_i$ را می‌شمارند در نتیجه $n=2^q m$ نیز $a_{i+1}-a_i$ را می‌شمارد یعنی دنباله $a_1,a_2,\ldots$ در نهایت به پیمانه $n=k+1$ با یک مقدار ثابت هم‌نهشت است و حکم استقرا برای این حالت نیز اثبات می‌شود.

۲۳. برای هر $k\geq 1$ داریم

$$f_{k+1}+f_k-1=2^{2^{k+1}}+2^{2^k}+1=(2^{2^k}+1)^2-(2^{2^{k-1}})^2$$
$$=(2^{2^k}+1-2^{2^{k-1}})(2^{2^k}+1+2^{2^{k-1}})$$

بنابراین

$$f_{k+1}+f_k-1=a_k(f_k+f_{k-1}-1) \qquad (*)$$

که $a_k=f_k-f_{k-1}+1$.

با استقرا ادامه می‌دهیم. داریم

$$f_5+f_4-1=3\times 7\times 13\times 97\times 2341\times 6673$$

و حکم برقرار است. فرض کنید برای $k\geq 5$، $f_k+f_{k-1}-1$ حداقل $k+1$ عامل اول دارد. با استفاده از (*) و این حقیقت که

$$\gcd(f_k+f_{k-1}-1,a_k)=\gcd(f_k+f_{k-1}-1,f_k-f_{k-1}+1)$$
$$=\gcd(f_k-f_{k-1}+1,\ 2\times 2^{2^{k-1}})=1$$

نتیجه می‌گیریم که $f_{k+1}+f_k-1$ حداقل $k+2$ عامل اول دارد و حکم اثبات می‌شود.

۲۴. از رابطه‌ی $6k=(k+1)^3+(k-1)^3-k^3-k^3$ در

$$k=\frac{n^{۳}-n}{۶}=\frac{n(n-۱)(n+۱)}{۶}$$

که به ازای همه‌ی مقادیر n عدد صحیح است، استفاده می‌کنیم. در این صورت خواهیم داشت

$$n^{۳}-n=(\frac{n^{۳}-n}{۶}+۱)^{۳}+(\frac{n^{۳}-n}{۶}-۱)^{۳}-(\frac{n^{۳}-n}{۶})^{۳}-(\frac{n^{۳}-n}{۶})^{۳}$$

بنابراین n برابر مجموع زیر است

$$n^{۳}+(\frac{n^{۳}-n}{۶})^{۳}+(\frac{n^{۳}-n}{۶})+(\frac{n-n^{۳}}{۶}-۱)^{۳}+(\frac{n-n^{۳}}{۶}+۱)^{۳}$$

توجه: می‌توان ثابت کرد که هر عدد گویا مجموع مکعبات سه عدد گویا است.

۲۵.(۱) [۱۹۹۸ چکسلواکی] قرار می‌دهیم $f(x)=x\lfloor x\lfloor x\lfloor x\rfloor\rfloor\rfloor$

ادعا می‌کنیم اگر a و b اعداد حقیقی هم علامت باشند و $|a|\geq|b|\geq ۱$ آنگاه $|f(a)|>|f(b)|$.

می‌دانیم که $\|a\rfloor\|\geq\|b\rfloor\|\geq ۱$. با ضرب این رابطه در $|a|>|b|\geq ۱$ خواهیم داشت $\|a\lfloor a\rfloor\|>\|b\lfloor b\rfloor\|\geq ۱$ توجه کنید که $a\lfloor a\rfloor$ و $a\lfloor a\lfloor a\rfloor\rfloor$ به ترتیب با $b\lfloor b\rfloor$ و $b\lfloor b\lfloor b\rfloor\rfloor$ هم علامت هستند. به طور مشابه

$$|a\lfloor a\lfloor a\rfloor\rfloor|>|b\lfloor b\lfloor b\rfloor\rfloor|\geq ۱\ ,\ \|\lfloor a\lfloor a\lfloor a\rfloor\rfloor\rfloor\|\geq\|\lfloor b\lfloor b\lfloor b\rfloor\rfloor\rfloor\|\geq ۱$$

و $|f(a)|>|f(b)|$ که ادعای ما را تأیید می‌کند.

برای $|x|<۱$ ، $f(x)=۰$ و $f(۱)=f(-۱)=۱$. فرض کنید $f(x)=۸۸$ بنابراین $|x|>۱$ و دو حالت زیر را بررسی می‌کنیم:

در حالت اول فرض می‌کنیم $x\geq ۱$. به سادگی می‌توان بررسی کرد که $f(\frac{۲۲}{۷})=۸۸$. از ادعای خود می‌دانیم که $f(x)$ برای $x>۱$ صعودی است، بنابراین $x=\frac{۲۲}{۷}$ پاسخ یکتای این بازه است.

در حالت دوم فرض می‌کنیم $x\leq -۱$. از ادعای خود می‌دانیم $f(x)$ برای $x<-۱$ نزولی است. داریم

$$|f(-۳)|=۸۱<f(x)=۸۸<|f(\frac{۱۱۲}{۳۷})|=۱۱۲$$

و لذا $-\frac{۱۱۲}{۳۷}<x<-۳$ و $\lfloor x\lfloor x\lfloor x\rfloor\rfloor\rfloor=-۳۷$. اما به این ترتیب $x=\frac{-۸۸}{۳۷}>-۳$، که تناقض است. بنابراین در این بازه هیچ جوابی وجود ندارد.

لازم به ذکر است که $\frac{۲۲}{۷}$ و $\frac{۱۱۲}{۳۷}$ – با یافتن به‌ترتیب $\lfloor x \rfloor$، $\lfloor \lfloor x \rfloor x \rfloor$ و $\lfloor \lfloor x \rfloor x \rfloor x \rfloor$ بدست آمدند.

به طور مثال برای $x \geq ۱$ ، $f(۴) < ۸۸ < f(۳)$ و لذا $۴ > x > ۳$. پس $۳ = \lfloor x \rfloor$ و $۸۸ = \lfloor \lfloor ۳x \rfloor x \rfloor x$ و از آنجا $f(۳) < ۸۸ < f(۱/۳)$ بنابراین $۹ = \lfloor \lfloor x \rfloor x \rfloor$ و الی آخر.

(۲) [۱۹۹۹ بلوروس] فرض کنید برای هر عدد صحیح k

$$x = \frac{۳}{۵}(۱۲۵k + ۱) \ , \ y = \frac{۴}{۵}(۱۲۵k + ۱) \ , \ z = \frac{۶}{۵}(۱۲۵k + ۱)$$

این اعداد هرگز عدد صحیح نیستند زیرا $۱۲۵k + ۱,۵$ را نمی‌شمارد. علاوه بر آن می‌توان نوشت

$$۱۲۵x^{۳} = ۳^{۳}(۱۲۵k + ۱)^{۳} \equiv ۳^{۳} \quad (\text{پیمانه } ۱۲۵)$$

بنابراین ۱۲۵، $۱۲۵x^{۳} - ۳^{۳}$ را شمرده و $x^{۳} - (\frac{۳}{۵})^{۳}$ عدد صحیح است. لذا

$$\{x^{۳}\} = \frac{۲۷}{۱۲۵}$$

بطور مشابه

$$\{y^{۳}\} = \frac{۶۴}{۱۲۵} \quad , \quad \{z^{۳}\} = \frac{۲۱۶}{۱۲۵} - ۱ = \frac{۹۱}{۱۲۵} = \frac{۲۷}{۱۲۵} + \frac{۶۴}{۱۲۵}$$

که نشان دهنده‌ی رابطه $\{z^{۳}\} = \{y^{۳}\} + \{x^{۳}\}$ است.

۲۶. از $n > ۱$ ، $f_{n-۱} = ۲^{۲^{n-۱}} + ۱$ به صورت $f_{n-۱}$ تعریف می‌شود.

$$(f_{n-۱})^{۲^{n+۱}} = (۲^{۲^{n-۱}} + ۱)^{۲^{n+۱}} = (۲^{۲^{n}} + ۱ + ۲^{۲^{n-۱}+۱})^{۲^{n}}$$
$$= (f_n + ۲^{۲^{n-۱}+۱})^{۲^{n}}$$

از قضیه دو جمله‌ای داریم

$$(f_{n-۱})^{۲^{n+۱}} \equiv (f_n + ۲^{۲^{n-۱}+۱})^{۲^{n}} \equiv (۲^{۲^{n-۱}+۱})^{۲^{n}} \equiv (۲^{۲^{n}})^{۲^{n-۱}+۱}$$
$$\equiv (f_n - ۱)^{۲^{n-۱}+۱} \equiv (-۱)^{۲^{n-۱}+۱} \equiv -۱ \quad (\text{پیمانه } f_n)$$

بنابراین f_n، $(f_{n-۱})^{۲^{n+۱}} + ۱$ را می‌شمارد. چون p ، f_n را می‌شمارد پس $(f_{n-۱})^{۲^{n+۱}} + ۱$ را نیز می‌شمارد. نتیجه دلخواه با قراردادن $a = f_{n-۱}$ در مسأله مقدماتی ۴۹.۱ (۲) بدست می‌آید.

۲۷. [USAMO ۱۹۹۹] پاسخ مشابه اثبات دوم مثال ۷۰.۱ است. ادعا می‌کنیم که

$$a_n = ۲n - \left\lfloor \frac{۱+\sqrt{۸n-۷}}{۲} \right\rfloor \qquad (\text{برای هر عدد صحیح مثبت } n)$$

دنباله داده شده را به صورت بسته‌هایی مانند

$$\{a_n\}_{n=۱}^{\infty} = \{۱\,;\, ۲,۴\,;\, ۵,۷,۹\,;\, ۱۰,۱۲,۱۴,۱۶\,;\, ۱۷,....\}$$

می‌نویسیم. دنباله زیر را در نظر بگیرید

$$\{b_n\}_{n=۱}^{\infty} = \{۱;۲,۲;۳,۳,۳;۴,۴,۴,۴;۵,...\}$$

نشان می‌دهیم

$$a_n + b_n = ۲n \qquad (\text{برای هر عدد صحیح مثبت } n) \qquad (*)$$

این رابطه برای $n=۱$ و $n=۲$ واضح است. در هر بسته در هر دنباله $a_{n+۱} = a_n + ۲$ و $b_{n+۱} = b_n$. بنابراین اگر رابطه (*) برای عدد اول هر بسته برقرار باشد، برای همه‌ی اعداد آن بسته برقرار است. اگر این رابطه برای آخرین عدد هر بسته درست باشد برای اولین عدد بسته بعد نیز درست است؛ زیرا a_n و b_n هر کدام ۱ واحد افزایش می‌یابند. به این ترتیب با استقرا رابطه (*) برای هر عدد صحیح مثبت n برقرار است.

کافی است نشان دهیم که

$$b_n = \left\lfloor \frac{۱+\sqrt{۸n-۷}}{۲} \right\rfloor \qquad (\dagger)$$

اگر $b_n = k$ آنگاه در kاُمین گروه قرار دارد و بعد از حداقل $k-۱$ گروه شامل $۱+۲+...+(k-۱)$ عضو آمده است. با در نظر گرفتن این حقیقت که $n-۱$ عضو قبل از b_n آمده است نتیجه می‌گیریم که

$$۱+۲+...+(b_n-۱) \le n-۱$$

یا

$$\frac{b_n(b_n-۱)}{۲} \le n-۱$$

با حل نامساوی مرتبه دوم فوق برای b_n خواهیم داشت

$$b_n \le \frac{۱+\sqrt{۸n-۷}}{۲}$$

b_n که از رابطه (†) بدست می‌آید بزرگترین عدد صحیحی است که این نامساوی را برآورده می‌کند.

۲۸. [USAMO ۱۹۹۸] مسأله را با استقرا روی n حل می کنیم و چنین مجموعه‌ای را که همه اعضای آن نامنفی هستند پیدا می‌کنیم. برای $n=۲$، می‌توان S را برابر $S=\{۰,۱\}$ قرار دارد.
فرض کنید برای $n\geq ۲$ مجموعه مطلوب S_n شامل n عدد صحیح نامنفی وجود داشته باشد. L را برابر کوچک‌ترین مضرب مشترک $(a-b)^۲$ها می‌گیریم که (a,b) روی هر دو عضو متمایز S_n تغییر می‌کند. تعریف می‌کنیم

$$S_{n+۱}=\{L+a:a\in S_n\}\cup\{۰\}$$

از آنجا که $L>۰$، $S_{n+۱}$ شامل $n+۱$ عدد صحیح نامنفی است. اگر $\alpha,\beta\in S_{n+۱}$ بوده و یکی از α و β صفر باشند آنگاه $(\alpha-\beta)^۲$, $\alpha\beta$ را می‌شمارد. اگر $L+a,L+b\in S_{n+۱}$ که a و b اعضای متمایز S_n هستند آنگاه

$$(L+a)(L+b)\equiv ab\equiv ۰\ \ ((a-b)^۲ \text{ پیمانه})$$

بنابراین $[(L+a)-(L+b)]^۲$, $(L+a)(L+a)$ را می‌شمارد و حکم استقرا ثابت می‌شود.

۲۹. [۲۰۰۱ سن‌پطرزبورگ] ادعا می‌کنیم بی‌نهایت عدد وجود دارد که برای mهای مختلف عوامل اول $m^۴+۱$ هستند. فرض کنید فقط تعداد محدودی چنین عدد اولی وجود داشته باشد. $p_۱,p_۲,\dots,p_k$ را همه آنها در نظر می‌گیریم. فرض کنید p یک عامل اول $(p_۱p_۲\dots p_k)^۴+۱$باشد. این عدد نمی‌تواند برابر هیچ‌یک از p_iها باشد. این تناقض به دلیل فرض ما بوده و ادعای ما را ثابت می‌کند.
فرض کنید P مجموعه‌ی همه‌ی اعدادی باشد که برای mهای مختلف عوامل اول $m^۴+۱$ هستند. یک عدد p عضو P و یک عدد صحیح m که p، $m^۴+۱$ را بشمارد، انتخاب می‌کنیم. فرض کنید r مانده‌ی m به پیمانه pباشد. بنابراین $r<p$ و p هر دو عدد $r^۴+۱$ و $(p-r)^۴+۱$ را می‌شمارد. n را برابر کمینه r و $p-r$ می‌گیریم. بنابراین $n<\frac{p}{۲}$ و یا $p>۲n$. اگر n را بتوان با ساختار فوق بدست آورد؛ آنگاه در شرط خواسته شده صدق می‌کند. اگر n با استفاده از عدد اول pساخته شود آنگاه p، $n^۴+۱$ را می‌شمارد. از آنجا که مجموعه P نامتناهی است و برای هر عدد صحیح m چنین عدد n را می‌توان ساخت، بی‌نهایت عدد صحیح n وجود دارد که در شرایط مسأله صدق می‌کند.

توجه: علاقمندان می‌تواند مسأله زیر را که در USAMO سال ۲۰۰۶ مطرح شده است حل کنند.
فرض کنید $p(m)$ بزرگ‌ترین عامل اول m باشد. به طور قراردادی تعریف می‌کنیم $p(\pm۱)=۱$ و $p(۰)=\infty$. همه چند جمله‌ای‌های f با ضرایب صحیح را چنان تعیین کنید که دنباله $\{p(f(n^۲))-۲n\}_{n\geq ۰}$ از بالا کراندار باشد. (به طور خاص لازم است که برای $n\geq ۰$, $f(n^۲)\neq ۰$).

۳۰. [۲۰۰۳ مجارستان] قرار می‌دهیم

$$s(n)=\frac{p(1)}{1}+\frac{p(2)}{2}+\cdots+\frac{p(n)}{n}$$

باید نشان دهیم

$$\frac{2n}{3}<s(n)<\frac{2(n+1)}{3} \qquad (*)$$

از استقرای قوی روی n استفاده می‌کنیم. رابطه (*) برای $n=1$ و $n=2$ صحیح است زیرا

$$\frac{2\times 1}{3}=\frac{2}{3}<s(1)=1<\frac{2(1+1)}{3}=\frac{4}{3}$$

و

$$\frac{2\times 2}{3}=\frac{4}{3}<s(2)=1+\frac{1}{2}=\frac{3}{2}<\frac{2(2+1)}{3}=2$$

فرض کنید عبارت (*) برای همه اعداد صحیح n کوچک‌تر از k درست باشد که k یک عدد صحیح مثبت است. نشان خواهیم داد که (*) برای $n=k+1$ نیز درست است. نکته کلیدی این است که $p(2k)=p(k)$ دو حالت را بررسی می‌کنیم.

در حالت اول فرض می‌کنیم k زوج باشد. می‌نویسیم $k=2m$ که m یک عدد صحیح مثبت کمتر از k است. برای $n=k+1=2m+1$ داریم:

$$\begin{aligned}
s(2m+1)&=\left(\frac{p(1)}{1}+\frac{p(3)}{3}+\cdots+\frac{p(2m+1)}{2m+1}\right)\\
&\quad+\left(\frac{p(2)}{2}+\frac{p(4)}{4}+\cdots+\frac{p(2m)}{2m}\right)\\
&=(m+1)+\left(\frac{p(1)}{2}+\frac{p(2)}{4}+\cdots+\frac{p(m)}{2m}\right)\\
&=(m+1)+\frac{1}{2}\left(\frac{p(1)}{1}+\frac{p(2)}{2}+\cdots+\frac{p(m)}{m}\right)\\
&=(m+1)+\frac{s(m)}{2}
\end{aligned}$$

از فرض استقرا داریم

$$(m+1)+\frac{m}{3}<(m+1)+\frac{s(m)}{2}=s(2m+1)<(m+1)+\frac{(m+1)}{3}$$

از $(m+1)+\frac{m}{3}=\frac{4m+3}{3}$ و $\frac{2(2m+1)}{3}=\frac{4m+2}{3}<\frac{4m+3}{3}$ و $(m+1)+\frac{(m+1)}{3}=\frac{4(m+1)}{3}=\frac{2(2m+1+1)}{3}$

نتیجه می‌گیریم که

$$\frac{۲(۲m+۱)}{۳} < s(۲m+۱) < \frac{۲(۲m+۱+۱)}{۳}$$

که همان (*) برای $n = ۲m+۱$ است.

در حالت دوم فرض می‌کنیم k فرد باشد. می‌نویسیم $k = ۲m+۱$ و $n = k+۱ = ۲m+۲$. مشابه حالت اول می‌توان نشان داد که

$$s(۲m+۲) = (m+۱) + \frac{s(m+۱)}{۲}$$

از فرض استقرا به سادگی می‌توان نشان داد که عبارت (*) برای $n = ۲m+۲$ نیز درست است که استقرا را کامل می‌کند.

۳۱. چون $(a-b)$, $(a^m - b^m)$ را می‌شمارد اگر p^t, $a-b$ را بشمارد آنگاه $(a^m - b^m)$ را نیز می‌شمارد.

برای عکس آن فرض کنید a و b نسبت به p اول بوده و (پیمانه p^t) $a^m \equiv b^m$. چون m نسبت به هر دو عدد p و $p-۱$ اول است، نسبت به $(p-۱)p^{t-۱} = \varphi(p^t)$ نیز اول است. بنابراین عدد صحیح مثبت k وجود دارد که (پیمانه $\varphi(p^t)$) $mk \equiv ۱$. از آنجا

$$a \equiv a^{mk} = (a^m)^k \equiv (b^m)^k = b^{mk} \equiv b \quad (\text{پیمانه } p^t)$$

که همان نتیجه دلخواه است.

توجه: می‌توان دید این مسأله یک خاصیت اضافی برای قضیه ۱۸.۱ است. در قضیه ۱۸.۱ (ج) اگر داشته باشیم (پیمانه m) $a \equiv b$، آنگاه برای هر عدد صحیح مثبت k، (پیمانه m) $a^k \equiv b^k$. این مسأله به ما اجازه می‌دهد تا برای روابط همنهشتی تحت روابط خاصی ریشه بگیریم.

۳۲.[۱۹۹۷ ترکیه] ادعا می‌کنیم $n = p-۱$ شرایط مسأله را برآورده می‌سازد. ابتدا دستگاه معادلات زیر را بررسی می‌کنیم:

$$\begin{aligned} x_۱^۲ + y_۱^۲ &= x_۲^۲ \\ x_۲^۲ + y_۲^۲ &= x_۳^۲ \\ &\vdots \\ x_n^۲ + y_n^۲ &= x_۱^۲ \end{aligned}$$

به طور متوالی از اعداد فیثاغورثی $۵^۲ = ۴^۲ + ۳^۲$ استفاده می‌کنیم تا به معادلات زیر برسیم

$$(۳^n)^۲ + (۳^{n-۱} \times ۴)^۲ = (۳^{n-۱} \times ۵)^۲$$
$$(۳^{n-۱} \times ۵)^۲ + (۳^{n-۲} \times ۵ \times ۴)^۲ = (۳^{n-۲} \times ۵^۲)^۲$$
$$(۳^{n-۲} \times ۵^۲)^۲ + (۳^{n-۳} \times ۵^۲ \times ۴)^۲ = (۳^{n-۳} \times ۵^۳)^۲$$
$$\vdots$$
$$(۳^{n+۱-i} \times ۵^{i-۱})^۲ + (۳^{n-i} \times ۵^{i-۱} \times ۴)^۲ = (۳^{n-i} \times ۵^i)^۲$$
$$\vdots$$
$$(۳ \times ۵^{n-۱})^۲ + (۵^{n-۱} \times ۴)^۲ = (۵^n)^۲$$

قرار می‌دهیم

$$x_i = ۳^{n+۱-i} \times ۵^{i-۱} \quad , \quad y_i = ۴ \times ۳^{n-i} \times ۵^{i-۱}$$

برای i از ۱ تا n و $x_{n+۱} = ۵^n$.

برای تکمیل اثبات فقط لازم است توجه کنیم که از قضیه کوچک‌فرما داریم

$$x_{n+۱}^۲ - x_۱^۲ \equiv ۵^{۲n} - ۳^{۲n} \equiv ۲۵^{p-۱} - ۹^{p-۱} \equiv ۰ \quad (\text{پیمانه } p)$$

توجه: بی‌نهایت عدد n وجود دارد که برای نمونه همه‌ی مضارب $p-۱$ را می‌توان نام برد.

۳۳. [HMMT ۲۰۰۴] اگر d یک مقسوم‌علیه i باشد، $\frac{i}{d}$ نیز یک مقسوم‌علیه i است و $\frac{i/d}{i} = \frac{۱}{d}$.

با جمع همه‌ی مقسوم‌علیه‌های d از i (که برابر $\sigma(i)$ است) می‌بینیم که $\frac{\sigma(i)}{i}$ جمع معکوس‌های همه‌ی مقسوم‌علیه‌های i است یعنی

$$\frac{\sigma(i)}{i} = \sum_{d|i} \frac{۱}{d} \quad (\text{برای هر عدد صحیح مثبت } i)$$

به این ترتیب نامساوی موردنظر به صورت زیر در می‌آید

$$\sum_{d|۱} \frac{۱}{d} + \sum_{d|۲} \frac{۱}{d} + \cdots + \sum_{d|n} \frac{۱}{d} \le ۲n$$

چنان که در پاسخ مسأله ۲۷مقدماتی نشان دادیم، اگر همه‌ی عبارات سمت چپ رابطه فوق را باز کنیم هر عدد $\frac{۱}{d}$ که $۱ \le d \le n$, $\left\lfloor \frac{n}{d} \right\rfloor$ بار ظاهر می‌شود، (برای هر مضرب d کوچک‌تر یا مساوی n، یک بار). بنابراین نامساوی مطلوب به صورت زیر در می‌آید

$$\frac{۱}{۱}\left\lfloor \frac{n}{۱} \right\rfloor + \frac{۱}{۲}\left\lfloor \frac{n}{۲} \right\rfloor + \frac{۱}{۳}\left\lfloor \frac{n}{۳} \right\rfloor + \cdots + \frac{۱}{n}\left\lfloor \frac{n}{n} \right\rfloor < ۲n$$

برای هر عدد صحیح مثبت i داریم $\frac{1}{i}\left\lfloor\frac{n}{i}\right\rfloor<\frac{1}{i}\frac{n}{i}=\frac{n}{i^2}$. بنابراین کافی است نشان دهیم

$$\frac{n}{1^2}+\frac{n}{2^2}+\cdots+\frac{n}{n^2}<2n$$

یا

$$\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{n^2}<1$$

که به ترتیب زیر به دست می‌آید

$$\frac{1}{2^2}+\frac{1}{3^2}+\ldots+\frac{1}{n^2}<\frac{1}{1\times2}+\frac{1}{2\times3}+\cdots+\frac{1}{n(n-1)}$$
$$=(\frac{1}{1}-\frac{1}{2})+(\frac{1}{2}-\frac{1}{3})+\cdots+(\frac{1}{n-1}-\frac{1}{n})$$
$$=1-\frac{1}{n}<1$$

توجه: از حسابان (*calculus*) می‌دانیم که

$$\frac{1}{1^2}+\frac{1}{2^2}+\cdots=\frac{\pi^2}{6}<2$$

۳۴. [USAMO ۲۰۰۵]

اثبات اول: دو معادله را با هم جمع کرده و ۱ را به طرفین اضافه می‌نمائیم تا به رابطه‌ی زیر برسیم:

$$(x^3+y+1)^2+z^9=147^{157}+157^{147}+1$$

اثبات می‌کنیم که دو طرف این عبارت نمی‌توانند به پیمانه ۱۹ هم‌نهشت باشند. ۱۹ را از این جهت انتخاب کردیم که کوچک‌ترین مضرب مشترک توان‌های ۲ و ۹، ۱۸ است و از قضیه کوچک‌فرما اگر a مضرب ۱۹ نباشد آنگاه (پیمانه ۱۹) $a^{18}\equiv1$. می‌دانیم (پیمانه ۱۹) $(z^9)^2\equiv0$ یا 1 است بنابراین تنها باقیمانده‌های ممکن در تقسیم z^9 بر ۱۹ عبارتند از:

$$-1,0,1$$

حال n^2 به پیمانه‌ی ۱۹ را برای $n=0,1,\ldots,9$ محاسبه می‌کنیم و می‌بینیم که تنها مانده‌های ممکن به پیمانه ۱۹ عبارتند از:

$$-8,-3,-2,0,1,4,5,6,7,9$$

به این ترتیب با جمع اعداد دو فهرست فوق، مانده‌های قابل قبول به پیمانه ۱۹ را برای $(x^3+y+1)^2+z^9$ به دست می‌آوریم:

	−۸	−۳	−۲	۰	۱	۴	۵	۶	۷	۹
−۱	−۹	−۴	−۳	−۱	۰	۳	۴	۵	۶	۸
۰	−۸	−۳	−۲	۰	۱	۴	۵	۶	۷	۹
۱	−۷	−۲	−۱	۱	۲	۵	۶	۷	۸	۱۰

با بکار بردن قضیه فرما مشاهده می‌شود که

$$۱۴۷^{۱۵۷} + ۱۵۷^{۱۴۷} + ۱ \equiv ۱۴ \quad \text{(پیمانه ۱۹)}$$

از آنجا که نمی‌توان ۱۴ (یا ۵-) را به دست آورد (چون در جدول نیامده‌اند) دستگاه معادله هیچ جواب صحیحی برای x, y, z ندارد.

اثبات دوم: نشان خواهیم داد که هیچ جوابی برای دستگاه به پیمانه ۱۳ وجود ندارد. دو معادله را باهم جمع کرده و ۱ را به طرفین اضافه می‌کنیم تا رابطه زیر به‌دست آید

$$(x^۳ + y + ۱)^۲ + z^۹ = ۱۴۷^{۱۵۷} + ۱۵۷^{۱۴۷} + ۱$$

از قضیه کوچک فرما اگر a مضرب ۱۳ نباشد آنگاه (پیمانه ۱۳) $a^{۱۲} \equiv ۱$. بنابراین (پیمانه ۱۳)

$۱۴۷^{۱۵۷} \equiv ۴^{۱} \equiv ۴$ و (پیمانه ۱۳) $۱۵۷^{۱۴۷} \equiv ۱^۳ \equiv ۱$ و لذا

$$(x^۳ + y + ۱)^۲ + z^۹ = ۶ \quad \text{(پیمانه ۱۳)}$$

اعداد مکعب کامل به پیمانه ۱۳ با $۰, ۱ \pm$ و $۵ \pm$ هم‌نهشت هستند. با نوشتن معادله اول به‌صورت

$$(x^۳ + ۱)(x^۳ + y) = ۴ \quad \text{(پیمانه ۱۳)}$$

می‌بینیم که در حالت (پیمانه ۱۳) $x^۳ \equiv -۱$ هیچ جوابی وجود ندارد و برای حالات $x^۳$ هم‌نهشت با $۰, ۱, ۵$ و -۵ به پیمانه ۱۳، $x^۳ + y$ باید به این پیمانه با $۴, ۲, ۵$ و -۱ هم‌نهشت باشد. بنابراین

$$(x^۳ + y + ۱)^۲ \equiv ۱۲, ۹, ۱۰, ۰ \quad \text{(پیمانه ۱۳)}$$

$z^۹$ نیز یک مکعب است و لذا باید به پیمانه ۱۳ با $۸, ۵, ۱, ۰$ یا ۱۲ هم‌نهشت باشد. جدول زیر نشان می‌دهد که به پیمانه ۱۳، نمی‌توان با جمع یکی از اعداد $۱۰, ۰, ۹, ۱۲$ با یکی از اعداد $۱۲, ۸, ۵, ۱, ۰$ مانده ۶ را بدست آورد

	۰	۱	۵	۸	۱۲
۰	۰	۱	۵	۸	۱۲
۹	۹	۱۰	۱	۴	۸
۱۰	۱۰	۱۱	۲	۵	۹
۱۲	۱۲	۰	۴	۷	۱۱

لذا دستگاه جوابی درمجموعه‌ی اعداد صحیح ندارد.

توجه: این استدلال نشان می‌دهدکه حتی اگر $z^{۹}$ با $z^{۳}$ نیز جایگزین شود باز هم دستگاه جواب صحیح ندارد.

۳۵. [۲۰۰۰ سن پطرزبورگ] حداقل سه بار توزین لازم است: هر کدام از دو توزین اولیه وزنه‌ها را به سه گروه تقسیم می‌کند (وزنه‌های کفه سمت چپ، وزنه‌های کفه سمت راست و وزنه‌های بیرون ترازو). چون $۲۷ > ۳ \times ۳$ لذا برخی وزنه‌ها در هر دو توزین در یک گروه قرار می‌گیرند لذا قابل تشخیص نیستند. نشان می‌دهیم که سه بار توزین کافی است. ۲۷ وزنه را با استفاده از کلمات سه حرفی با حروف O, R, L برچسب گذاری می‌کنیم. در i اُمین توزین وزنه‌هایی که i اُمین حرف آن L است را در کفه سمت چپ و وزنه‌هایی که i اُمین حرف آنها R است را در کفه‌ی سمت راست قرار می‌دهیم. اختلاف بین مجموع وزنهای کفه سمت چپ و مجموع وزنهای کفه سمت راست برابر است با:

$$\varepsilon_{۰}۳^{۰} + \varepsilon_{۱}۳^{۱} + \cdots + \varepsilon_{۲۶}۳^{۲۶}$$

که ε_j برابر ۱، ۱- و ۰ است اگر ۳^j به ترتیب در کفه سمت چپ، کفه سمت راست و یا بیرون ترازو باشد. مقدار مجموع فوق به‌طور یکتا همه‌ی ε_jها را مشخص می‌کند: مقدار مجموع به پیمانه ۳، $\varepsilon_{۰}$ را تعیین می‌کند، سپس مقدار مجموع به پیمانه ۹، $\varepsilon_{۱}$ را تعیین می‌کند و الی آخر.

بنابراین برای $j = ۰,\ldots,۲۶$، i اُمین توزین i اُمین حرف وزنه‌ی ۳^j را مشخص می‌کند. بعد از سه بار توزین به‌طور دقیق می‌توانیم وزنه ۳^j را بشناسیم.

توجه: این مسأله حالت خاصی از یک مسأله کلی‌تر است که هر عدد صحیح یک نمایش یکتا در مبنای ۳ با ارقام ۱−, ۰ و۱ دارد. به وضوح این مطلب برای اعداد n با شرط $۰ \le n < ۳^{۱}$ برقرار است (از آنجا که ۰=۰، ۱=۱ و ۱−۳=۲). فرض کنید مطلب فوق برای اعداد n با شرط $۰ \le n < ۳^k$ (k عدد صحیح مثبت) برقرار باشد. اگر $۳^k \le n < ۲ \times ۳^k$، حکم همچنان برقرار است زیرا $n = ۳^k + n_{۱}$ و $۰ \le n_{۱} < ۳^k$. اگر $۲ \times ۳^k \le n < ۳^{k+۱}$ باز هم حکم برقرار است زیرا $n = ۳^{k+۱} - ۳^k + n_{۱}$ و $۰ \le n_{۱} < ۳^k$. به سادگی می‌توان دید برای اعداد منفی نیز می‌توان چنین گفت و نمایش برای تمام اعداد صحیح یکتاست. می‌توان هر عدد در مبنای ۳ را به سادگی به این نوع جدید مبنای ۳ تبدیل کرد. برای مثال

$$۴۹ = ۱۲۱۱_{(۳)} = ۳^{۳} + ۲ \times ۳^{۲} + ۳ + ۱$$
$$= ۲ \times ۳^{۳} - ۳^{۲} + ۳ + ۱ = ۳^{۴} - ۳^{۳} - ۳^{۲} + ۳ + ۱$$

۳۶. [*Iberoamerican* ۱۹۹۸] داریم

$$۱۹۹۸ < \lambda = \frac{۱۹۹۸ + \sqrt{۱۹۹۸^۲ + ۴}}{۲} = ۹۹۹ + \sqrt{۹۹۹^۲ + ۱} < ۱۹۹۹$$

و $x_۱ = ۱۹۹۸$ و $x_۲ = ۱۹۹۸^۲$. از $\lambda^۲ - ۱۹۹۸\lambda - ۱ = ۰$ نتیجه می‌گیریم برای همه اعداد حقیقی x

$$x\lambda = ۱۹۹۸x + \frac{x}{\lambda} \qquad \text{و} \qquad \lambda = ۱۹۹۸ + \frac{۱}{\lambda}$$

چون $x_n = \lfloor x_{n-۱}\lambda \rfloor$، $x_{n-۱}$ عدد صحیح و λ عدد گنگ است در نتیجه

$$\frac{x_n}{\lambda} < x_{n-۱} < \frac{x_n + ۱}{\lambda} \qquad \text{یا} \qquad x_n < x_{n-۱}\lambda < x_n + ۱$$

و چون $\lambda > ۱۹۹۸$، $\left\lfloor \frac{x_n}{\lambda} \right\rfloor = x_{n-۱} - ۱$ و لذا

$$x_{n+۱} = \lfloor x_n \lambda \rfloor = \left\lfloor ۱۹۹۸x_n + \frac{x_n}{\lambda} \right\rfloor = ۱۹۹۸x_n + x_{n-۱} - ۱$$

یعنی (پیمانه ۱۹۹۸) $x_{n+۱} \equiv x_{n-۱} - ۱$. از این رو (پیمانه ۱۹۹۸) $x_{۱۹۹۸} \equiv x_۰ - ۹۹۹ \equiv ۱۰۰۰$ جواب مسأله را به ما می‌دهد.

۳۷. [*USAMO* ۱۹۹۶]

اثبات اول: بله - چنین زیر مجموعه‌ای وجود دارد. چنانچه درمسأله مقدماتی ۳۹ (۳) نشان داده شده است اگر مسأله به اعداد صحیح نامنفی محدود شود آنگاه مجموعه‌ی اعداد صحیح که نمایش در مبنای ۴ آنها فقط شامل رقم‌های ۰ و ۱ باشد شرایط خواسته شده را برآورده می‌کنند. برای بررسی اعداد صحیح منفی از مبنای (۴-) استفاده می‌کنیم؛ یعنی هر عدد صحیح را به شکل $\sum_{i=۰}^{k} c_i (-۴)^i$ می‌نویسیم که برای هر i , $c_i \in \{۰,۱,۲,۳\}$ و $c_k \neq ۰$ است. در این حالت مجموعه‌ی X را مجموعه‌ی اعدادی می‌گیریم که نمایش آنها فقط شامل ارقام ۰ و ۱ باشد. این X نیز خاصیت مطلوب را دارد چرا که نشان می‌دهیم هر عدد صحیح یک نمایش یکتا در این مُد دارد.

برای نشان دادن یکتایی نمایش اعداد درمبنای (۴-) فرض کنید $\{c_i\}$ و $\{d_i\}$ دو دنباله متناهی متمایز از اعضای مجموعه $\{۰,۱,۲,۳\}$ باشند و فرض کنید j کوچک‌ترین عدد صحیح باشد که $c_j \neq d_j$. بنابراین

$$\sum_{i=0}^{k} c_i (-4)^i \not\equiv \sum_{i=0}^{k} d_i (-4)^i \qquad (\text{پیمانه } 4^j)$$

و لذا دو عددی که با دنباله‌های $\{c_i\}$ و $\{d_i\}$ نشان داده می‌شوند، متمایز هستند. از طرف دیگر برای نمایش اینکه عدد n در مبنای ۴- قابل نمایش است، عدد صحیح k را چنان می‌یابیم که

$$1 + 4^2 + \cdots + 4^{2k} \geq n$$

و لذا

$$n + 4 + \cdots + 4^{2k-1} = \sum_{i=0}^{2k} c_i 4^i$$

حال با قرار دادن $d_{2i} = c_{2i}$ و $d_{2i-1} = 3 - c_{2i-1}$ خواهیم داشت $n = \sum_{i=0}^{2k} d_i (-4)^i$.

اثبات دوم: برای هر مجموعه‌ی S از اعداد صحیح تعریف می‌کنیم $S^* = \{a + 2b \mid a,b \in S\}$. مجموعه متناهی $S = \{a_1, a_2, \ldots, a_m\}$ از اعداد صحیح را خوب می‌نامیم اگر $|S^*| = |S|^2$ یا به عبارت دیگر اگر مقادیر $a_i + 2a_j \; (1 \leq i, j \leq m)$ متمایز باشند. ابتدا ثابت می‌کنیم با داشتن یک مجموعه‌ی خوب و عدد صحیح n، می‌توان همواره یک آبَر مجموعه‌ی خوب T از S یافت (مجموعه‌ای که S زیرمجموعه‌ی آن باشد) که n، عضوی در T^* باشد. اگر n در S^* باشد، قرار می‌دهیم $T = S$. در غیر این صورت قرار می‌دهیم $T = S \cup \{k, n-2k\}$ که k انتخاب می‌شود. سپس قرار می‌دهیم $T^* = S^* \cup Q \cup R$ که

$$Q = \{3k, 3(n-2k), k + 2(n-2k), (n-2k) + 2k\}$$

و

$$R = \{k + 2a_i, (n-2k) + 2a_i, a_i + 2k, a_i + 2(n-2k) \mid 1 \leq i \leq m\}$$

توجه کنید که برای هر انتخاب k، $n = (n-2k) + 2k$ در Q بوده که یک زیرمجموعه‌ی T^* است. به‌جز n، مقادیر جدید شکل‌های خطی غیرثابت متمایز از k هستند لذا اگر k به قدر کافی بزرگ باشد همه آنها از یگدیگر و از اعضای S^* متمایز خواهند بود. این اثبات می‌کند که T^* خوب است.

با شروع از مجموعه‌ی خوب $X_0 = \{0\}$، یک دنباله از مجموعه‌های X_1، X_2، X_3، ... به‌دست می‌آوریم که برای هر عدد صحیح مثبت j، X_j یک آبَر مجموعه‌ی خوب X_{j-1} بوده و X_j^* شامل j اُمین عضو دنباله ... $-3, 3, -2, 2, -1, 1$ است. بنابراین مجموعه‌ی

$$X = \bigcup_{j=0}^{\infty} X_j$$

دارای خاصیت مطلوب است.

۳۸. جواب منفی است.

اگر x_n زوج باشد، قرار می‌دهیم $y_n = 0$ و در غیر این صورت $y_n = 1$. دنباله جدید $y_1, y_2, \ldots, y_n, \ldots$ با مانده‌های اعداد x_n به پیمانه ۲ شکل می‌گیرد. اگر $x_1, x_2, \ldots, x_n, \ldots$ متناوب باشد، $y_1, y_2, \ldots, y_n, \ldots$ نیز متناوب است. باید ثابت کنیم $y_1, y_2, \ldots, y_n, \ldots$ متناوب نبوده و به موجب آن جواب سوال منفی است. دنباله $y_1, y_3, y_5, \ldots, y_{2n+1}, \ldots$ را بررسی می‌کنیم. عضو y_{2n+1} را می‌توان به صورت زیر به‌دست آورد. $\sqrt{2}$ را در مبنای دو می‌نویسیم و آن را در 2^n ضرب می‌کنیم (حاصل این مقدار $(\sqrt{2})^{2n+1}$ است). سپس بخش اعشاری آن را دور می‌ریزیم تا $\lfloor (\sqrt{2})^{2n+1} \rfloor$ بدست آید.

بعد از آن آخرین رقم این عدد صحیح y_{2n+1} است. ضرب 2^n در مبنای ۲ به معنای جابجایی ممیز اعشار به اندازه n مکان به سمت راست است. این بدان معناست که y_{2n+1} رقم nام $\sqrt{2}$ بعداز ممیز اعشار است. از آنجا که $\sqrt{2}$ گنگ است نتیجه می‌گیریم دنباله $y_1, y_3, \ldots, y_{2n+1}, \ldots$ متناوب نبوده و لذا $y_1, y_2, \ldots, y_n, \ldots$ نیز متناوب نیست.

۳۹. [اردوش] کافی است حکم را برای nهای نامنفی ثابت کنیم، زیرا برای nهای منفی می‌توان به سادگی همه‌ی علائم را تغییر داد. حکم با استقرای با گام ۴ اثبات می‌شود؛ یعنی اثبات حکم برای $k+4$ بر مبنای فرض استقرا برای $n = k$. ابتدا نشان می‌دهیم که حکم برای $n = 0, 1, 2, 3$ برقرار است.

$$1 = 1^2 \qquad 0 = 1^2 + 2^2 - 3^2 + 4^2 - 5^2 - 6^2 + 7^2$$

$$3 = -1^2 + 2^2 \qquad 2 = -1^2 - 2^2 - 3^2 + 4^2$$

اگر n قابل ارائه به شکل مطلوب باشد $n+4$ نیز قابل ارائه است زیرا ۴ را می‌توان به صورت زیر بیان کرد:

$$4 = (k+1)^2 - (k+2)^2 - (k+3)^2 + (k+4)^2 \qquad (*) \qquad (\text{برای هر } k)$$

بنابراین هر عدد صحیح نامنفی n را می‌توان به شکل مطلوب بیان کرد.

توجه: از (*) همچنین نتیجه می‌گیریم که برای هر k

$$(k+1)^2-(k+2)^2-(k+3)^2+(k+4)^2-(k+5)^2+(k+6)^2+(k+7)^2-(k+8)^2=0$$

بنابراین به سادگی می‌توان تفسیر کرد که یک عدد صحیح را می‌توان به بی‌نهایت روش به شکل مطلوب نمایش داد.

۴۰. [۲۰۰۴ چین]

پاسخ اول: جواب برابر است با

$$f(n)=\left\lfloor\frac{n+1}{2}\right\rfloor+\left\lfloor\frac{n+1}{3}\right\rfloor-\left\lfloor\frac{n+1}{6}\right\rfloor+1 \qquad (*)$$

مجموعه‌ی T را خوب می‌نامیم اگر T شامل سه عضو متمایز باشد که نسبت به هم اول باشند. درگام اول دو ادعای ساده داریم:

(آ) $f(n)$ وجود دارد و $f(n)\le n$

(ب) $f(n+1)\le f(n)+1$

از آنجا که $n\ge 4$ لذا m , $m+1$, $m+2$ و $m+3$ اعضای متمایز در S_m هستند. اگر m زوج باشد مجموعه $\{m+1,m+2,m+3\}$ خوب است؛ اگر m فرد باشد، $\{m,m+1,m+2\}$ خوب است. بنابراین مجموعه n عضوی S_m برای همه مقادیر m خوب است و $f(n)\le n$ که ادعای (آ) را تأیید می‌کند. ادعای (ب) بطور مستقیم از رابطه زیر بدست می‌آید

$$\{m,m+1,\ldots,m+n\}=\{m,m+1,\ldots,m+n-1\}\bigcup\{m+n\}$$

حال یک کران پایین برای $f(n)$ پیدا می‌کنیم. مجموعه‌ی $S_2=\{2,3,\ldots,n+1\}$ و زیرمجموعه‌ی T_2 از آن را که شامل اعضایی است که مضرب ۲ یا ۳ یا هر دو هستند، درنظر بگیرید. از اصل لانه کبوتری هر سه عضو T_2 بایدیک عامل مشترک (از ۲ یا ۳) داشته باشند . بنابراین T_2 خوب نیست. اما از اصل شمول و عدم شمول

$$|T_2|=\left\lfloor\frac{n+1}{2}\right\rfloor+\left\lfloor\frac{n+1}{3}\right\rfloor-\left\lfloor\frac{n+1}{6}\right\rfloor$$

و بنابراین

$$f(n)\ge\left\lfloor\frac{n+1}{2}\right\rfloor+\left\lfloor\frac{n+1}{3}\right\rfloor-\left\lfloor\frac{n+1}{6}\right\rfloor+1 \qquad (**)$$

ادعا می‌کنیم که همین کران پایین، مقدار دقیق $f(n)$ است. قبلاً نشان دادیم که S_m برای همه مقادیر m خوب است.

با یک محاسبه ساده از نامساوی فوق خواهیم داشت $f(۴)\geq ۴, f(۵)\geq ۵, f(۶)\geq ۵, f(۷)\geq ۶$ $f(۸)\geq ۷$ و $f(۹)\geq ۸$. از $f(n)\leq n$ نتیجه می‌گیریم که $f(۴)=۴$ و $f(۵)=۵$. ادعا می کنیم که $f(۶)=۵$. سپس از ادعای (ب) داریم $f(۷)=۶, f(۸)=۷$ و $f(۹)=۸$.

حال نشان می‌دهیم $f(۶)=۵$. یعنی هر زیر مجموعه ۵ عضوی T از یک مجموعه‌ی شامل ۶ عدد متوالی، خوب است. در بین این ۶ عدد سه عدد فرد متوالی (که یک سه تایی خوب را می‌سازد) و سه عدد زوج متوالی هستند. اگر هر سه عدد فرد در T باشند، آنگاه T خوب است. در غیر این‌صورت T باید شامل هر سه عدد زوج و دو تا از اعداد فرد باشد. اگر دو عدد فرد موجود در T متوالی باشند (به شکل $۲x+۱$ و $۲x+۳$) آنگاه T خوب است چون $(۲x+۳, ۲x+۲, ۲x+۱, ۲x)$ در T است. در غیر این صورت دو عدد فرد موجود در T به شکل $۲x+۱$ و $۲x+۵$ هستند. در این حالت نیز T خوب است زیرا حداقل یکی از سه تایی‌های $(۲x+۵, ۲x+۲, ۲x+۱)$ و $(۲x+۵, ۲x+۴, ۲x+۱)$ خوب هستند (زیرا حداقل یکی از اعداد $۲x+۱$ و $۲x+۵$ بر ۳ بخشپذیر نیست).

با توجه به $f(n)\leq f(n+۱)+۱$ و با استفاده از (**) خواهیم داشت $f(۶)=۶, f(۷)=۷, f(۸)=۷$ و $f(۹)=۸$.

حال (*) را با استقرار روی n ثابت می‌کنیم. استدلال‌های فوق نشان می‌دهند که حالات پایه برای $n\leq ۹$ برقرار هستند. فرض کنید (*) برای عدد صحیح بزرگ‌تر یا مساوی ۹، $n=k$ برقرار باشد. برای $n=k+۱$ داریم

$$\begin{aligned} S_m &= \{m, m+۱, \ldots, m+k\} \\ &= \{m, m+۱, \ldots, m+k-۶\} \cup \{m+k-۵, \ldots, m+k\} \end{aligned}$$

بنابراین از اصل لانه کبوتری $f(k+۱)\leq f(k-۵)+f(۶)-۱$. با استفاده از فرض استقرا برای $f(k-۵)$ و استفاده از $f(۶)=۵$ داریم

$$\begin{aligned} f(k+۱) &\leq \left\lfloor \frac{k-۴}{۲} \right\rfloor + \left\lfloor \frac{k-۴}{۳} \right\rfloor - \left\lfloor \frac{k-۴}{۶} \right\rfloor + ۵ \\ &= \left\lfloor \frac{k-۲}{۲} \right\rfloor + \left\lfloor \frac{k-۲}{۳} \right\rfloor - \left\lfloor \frac{k-۲}{۶} \right\rfloor + ۱ \end{aligned}$$

این نتیجه درترکیب با (**) نشان می‌دهد که (*) برای $n=k+۱$ نیز صحیح بوده و استقرا کامل می‌شود.

پاسخ دوم: از همان علائم و تعاریف پاسخ اول استفاده می‌کنیم. همان‌طور که در پاسخ اول نشان دادیم همه زیرمجموعه‌های ۵ عضوی یک مجموعه شامل ۶ عدد صحیح متوالی خوب هستند. حال چند حالت را بررسی می‌کنیم.

(i) در این حالت فرض می‌کنیم (پیمانه ۶) $n \equiv 0$ و می‌نویسیم $n = 6k$. می‌توان مجموعه‌ی S_m را به k زیر مجموعه شامل ۶ عدد صحیح متوالی تقسیم کرد. اگر $4k + 1$ عدد انتخاب شود، از اصل لانه کبوتری یکی از این زیر مجموعه‌ها شامل ۵ عدد از اعداد انتخاب شده است و لذا خوب است. از طرف دیگر هر زیرمجموعه، شامل ۴ عدد است که بر ۲ یا ۳ بخشپذیرند (اعدادی که به پیمانه ۶ با ۰,۲,۳,۴ هم‌نهشتند) لذا زیر مجموعه‌ی $4k$ عضوی شامل این اعداد خوب نیست. بنابراین

$$f(n) = 4k + 1 = 4\left\lfloor \frac{n}{6} \right\rfloor + 1.$$

(ii) در این حالت فرض می‌کنیم (پیمانه ۶) $n \equiv 1$ و می‌نویسیم $n = 6k + 1$. از (i) و (ب) در پاسخ اول داریم $f(n) = 4k + 1$ یا $f(n) = 4k + 2$. از طرف دیگر $4k + 1$ عضو در $S_1 = \{2, 3, \ldots, n + 1\} = \{2, 3, \ldots, 6k + 2\}$ وجود دارد که بر ۲ یا ۳ بخشپذیرند. بنابراین

$$f(n) = 4k + 2 = 4\left\lfloor \frac{n}{6} \right\rfloor + 2.$$

(iii) در این حالت فرض می‌کنیم (پیمانه ۶) $n \equiv 2$ و می‌نویسیم $n = 6k + 2$. از (ii) و (ب) در پاسخ اول داریم $f(n) = 4k + 2$ یا $f(n) = 4k + 3$. از طرف دیگر $4k + 2$ عضو در $S_1 = \{2, 3, \ldots, 6k + 3\}$ وجود دارند که بر ۲ یا ۳ بخشپذیرند لذا $f(n) = 4k + 3 = 4\left\lfloor \frac{n}{6} \right\rfloor + 3$.

(iv) در این حالت فرض می‌کنیم (پیمانه ۶) $n \equiv 3$ و می‌نویسیم $n = 6k + 3$. مجدداً داریم $f(n) = 4k + 3$ یا $f(n) = 4k + 4$. از طرف دیگر $4k + 3$ عضو در $S_1 = \{2, 3, \ldots, 6k + 4\}$ وجود دارد که بر ۲ یا ۳ بخش‌پذیرند و لذا $f(n) = 4k + 4 = 4\left\lfloor \frac{n}{6} \right\rfloor + 4$.

(v) در این حالت فرض می‌کنیم (پیمانه ۶) $n \equiv 4$ و می‌نویسیم $n = 6k + 4$. می‌توان S_m را به k زیر مجموعه شامل ۶ عدد متوالی تقسیم کرد. فرض کنید T یک زیر مجموعه S_m باشد که خوب نیست. هر یک از زیرمجموعه‌های ۶ عضوی می‌توانند ۴ عضو در T داشته باشند. همچنین $6k + 1$ و $6k + 3$ هر دو نمی‌توانند با هم در T باشند. لذا T حداکثر می‌تواند $4k + 3$ عضو داشته باشد. بنابراین $f(n) \geq 4k + 4$. از (iv) و (ب) نتیجه می‌گیریم که

$$f(n) = 4k + 4 = 4\left\lfloor \frac{n}{6} \right\rfloor + 4.$$

(vi) در این حالت فرض می‌کنیم (پیمانه ۶) $n \equiv 5$ و می‌نویسیم $n = 6k + 5$. مجداً داریم $f(n) = 4k + 4$ و یا $f(n) = 4k + 5$. از طرف دیگر $4k + 4$ عضو در $S_1 = \{2, 3, \ldots, 6k + 6\}$ وجود دارد که بر ۲ یا ۳ بخش‌پذیر است و لذا $f(n) = 4k + 5 = 4\left\lfloor \frac{n}{6} \right\rfloor + 5$.

از ترکیب این حالات خواهیم داشت

$$f(n)=۴\left\lfloor\frac{n}{۶}\right\rfloor+\begin{cases}۱ & n\equiv ۰ \quad (\text{پیمانه } ۶)\\ ۲ & n\equiv ۱ \quad (\text{پیمانه } ۶)\\ ۳ & n\equiv ۱ \quad (\text{پیمانه } ۶)\\ ۴ & n\equiv ۱ \quad (\text{پیمانه } ۶)\\ ۴ & n\equiv ۱ \quad (\text{پیمانه } ۶)\\ ۵ & n\equiv ۱ \quad (\text{پیمانه } ۶)\end{cases}$$

به سادگی می‌توان بررسی کرد

$$f(n)=\left\lfloor\frac{n+۱}{۲}\right\rfloor+\left\lfloor\frac{n+۱}{۳}\right\rfloor-\left\lfloor\frac{n+۱}{۶}\right\rfloor+۱$$

توجه: توجه کنید که $f(n)$ را می‌توان به صورت زیر نیز بیان کرد

$$f(n)=n-\left\lfloor\frac{n}{۶}\right\rfloor-\left\lfloor\frac{n+۱}{۶}\right\rfloor+۱$$

شاید بیان فوق برای پاسخ دوم مناسب‌تر باشد. معادل بودن این دو عبارت را می‌توان با بکار بردن متوالی اتحاد هرمیت (قضیه ۱۰۴۸) به صورت زیر نشان داد:

$$n=\left\lfloor ۲\times\frac{n}{۲}\right\rfloor=\left\lfloor\frac{n}{۲}\right\rfloor+\left\lfloor\frac{n}{۲}+\frac{۱}{۲}\right\rfloor=\left\lfloor\frac{n}{۲}\right\rfloor+\left\lfloor\frac{n+۱}{۲}\right\rfloor$$

$$\left\lfloor\frac{n}{۲}\right\rfloor=\left\lfloor ۳\times\frac{n}{۶}\right\rfloor=\left\lfloor\frac{n}{۶}\right\rfloor+\left\lfloor\frac{n+۲}{۶}\right\rfloor+\left\lfloor\frac{n+۴}{۶}\right\rfloor$$

$$\left\lfloor\frac{n+۱}{۳}\right\rfloor=\left\lfloor ۲\times\frac{n+۱}{۶}\right\rfloor=\left\lfloor\frac{n+۱}{۶}\right\rfloor+\left\lfloor\frac{n+۴}{۶}\right\rfloor$$

۴۱. [۱۹۹۹ چین] p را برابر حاصل‌ضرب ۱۴ عدد داده شده می‌گیریم. با قرار دادن $b=c=d=۱$ خواهیم داشت $p=(a!)^{۱۴}=(a!)^{۲+۳\times۲+۳\times۲}$ بنابراین $r\geq ۱۴$. ادعا می‌کنیم $r=۱۴$. کافی است نشان دهیم $p,((abcd)!)^{۱۴}$ را می‌شمارد.

اعداد $(a!)^{bcd+۱}$ و $((bcd)!)^{a+۱}$ را با هم در نظر می‌گیریم. داریم

$$(a!)^{bcd+۱}.((bcd)!)^{a+۱}=[(a!)^{bcd}.(bcd)!][((bcd)!)^{a}.a!]$$

و به‌طور مشابه داریم

$$((ab)!)^{cd+1}.((cd)!)^{ab+1}=[((ab)!)^{cd}.(cd)!][((cd)!)^{ab}.(ab)!]$$

به سادگی می‌توان ادعای مطرح شده را ازمثال ۷۴۰۱ (۱) مشاهده کرد.

۴۲. در حالیکه واضح است بخش (۱) از خواص ک.م.م است، مشخص نیست بخش (۲) به ک.م.م ربط دارد یا خیر.

(۱) از استقرا روی n استفاده می‌کنیم. حالت پایه $n=1$ واضح است زیرا $\text{lcm}(a_0,a_1)\le \text{lcm}(1,2)=2$. فرض می‌کنیم حکم برای $n=k$ درست باشد؛ یعنی اگر اعداد $a_0<a_1<a_2<....<a_k$ صحیح مثبت باشند آنگاه

$$\frac{1}{\text{lcm}(a_0,a_1)}+\frac{1}{\text{lcm}(a_1,a_2)}+\cdots+\frac{1}{\text{lcm}(a_{k-1},a_k)}\le 1-\frac{1}{2^k}$$

حال حالت $n=k+1$ را در نظر می‌گیریم. فرض کنید $a_0<a_1<a_2<...<a_k<a_{k+1}$ اعداد صحیح مثبت باشند. دو حالت را بررسی می‌کنیم.

- در حالت اول فرض می‌کنیم $a_{k+1}\ge 2^{k+1}$. در این صورت خواهیم داشت $\text{lcm}(a_k,a_{k+1})\ge a_{k+1}\ge 2^{k+1}$. با استفاده از فرض استقرا نتیجه می‌گیریم

$$\frac{1}{\text{lcm}(a_0,a_1)}+....+\frac{1}{\text{lcm}(a_{k-1},a_k)}+\frac{1}{\text{lcm}(a_k,a_{k+1})}\le 1-\frac{1}{2^k}+\frac{1}{2^{k+1}}=1-\frac{1}{2^{k+1}}$$

که حکم استقرا را اثبات می‌کند.

- در حالت دوم فرض می‌کنیم $a_{k+1}<2^{k+1}$. داریم

$$\frac{1}{\text{lcm}(a_{i-1},a_i)}=\frac{\gcd(a_{i-1},a_i)}{a_{i-1}a_i}\le\frac{a_i-a_{i-1}}{a_{i-1}a_i}=\frac{1}{a_{i-1}}-\frac{1}{a_i}$$

با جمع نامساوی‌های فوق برای i از ۱ تا $k+1$ خواهیم داشت:

$$\frac{1}{\text{lcm}(a_0,a_1)}+\cdots+\frac{1}{\text{lcm}(a_{k-1},a_k)}+\frac{1}{\text{lcm}(a_k,a_{k+1})}\le\frac{1}{a_0}-\frac{1}{a_{k+1}}\le 1-\frac{1}{2^{k+1}}$$

که باز هم اثبات حکم استقرا است.

(۲) کلید حل مسأله تفسیر جمله « هر عدد صحیح مثبت کوچک‌تر یا مساوی m که بر هر زوج از اعداد داده شده بخشپذیر نباشد» است. این جمله بیان می‌کند که کوچک‌ترین مضرب مشترک هر دو عدد از اعداد داده شده بزرگ‌تر از m است.

n عدد داده شده را با $x_1, x_2, \ldots, x_n$ نشان می‌دهیم. برای یک i داده شده، $\left\lfloor \frac{m}{x_i} \right\rfloor$ مضرب x_i در بین اعداد $1, 2, \ldots, m$ وجود دارد. هیچ‌یک از آنها مضرب x_j ($j \neq i$) نیستند زیرا کوچک‌ترین مضرب مشترک x_i و x_j بزرگ‌تر از m است. بنابراین

$$\left\lfloor \frac{m}{x_1} \right\rfloor + \left\lfloor \frac{m}{x_2} \right\rfloor + \cdots + \left\lfloor \frac{m}{x_n} \right\rfloor$$

عضو متمایز درمجموعه $\{1, 2, \ldots, m\}$ وجود دارد که بر یکی از اعداد $x_1, x_2, \ldots, x_n$ بخشپذیرند. هیچ کدام از این اعضا نمی‌توانند ۱ باشند (مگر آنکه $n = 1$ که در این حالت حکم واضح است) بنابراین

$$\left\lfloor \frac{m}{x_1} \right\rfloor + \left\lfloor \frac{m}{x_2} \right\rfloor + \cdots + \left\lfloor \frac{m}{x_n} \right\rfloor \leq m - 1$$

با در نظر گرفتن اینکه برای هر i، $\frac{m}{x_i} < \left\lfloor \frac{m}{x_i} \right\rfloor + 1$ خواهیم داشت

$$m\left(\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}\right) < m + n - 1$$

حال ادعا می‌کنیم $n \leq \frac{m+1}{2}$ که به موجب آن

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} < 1 + \frac{n-1}{m} < \frac{3}{2}$$

بزرگ‌ترین مقسوم علیه فرد $x_1, x_2, \ldots, x_n$ همگی متمایز هستند. در غیر این‌صورت اگر بزرگ‌ترین مقسوم علیه فرد دو تا از اعداد داده شده یکی باشد، یکی از آنها باید مضرب دیگری باشد که خلاف فرض است. بنابراین n نمی‌تواند بیش‌تر از تعداد اعداد فرد ۱ تا m باشد و لذا $n \leq \frac{m+1}{2}$.

۴۳. از قضیه ۴۶۰۱ (آ) باقیمانده تقسیم n بر k برابر است با $k. \left\{\frac{n}{k}\right\} = n - \left\lfloor \frac{n}{k} \right\rfloor k$. لذا داریم

$$r(n) = \sum_{k=1}^{n} \left(n - \left\lfloor \frac{n}{k} \right\rfloor . k\right)$$

و شرط $r(n) = r(n-1)$ معادل با رابطه زیر است

$$\sum_{k=1}^{n}(n-\left\lfloor\frac{n}{k}\right\rfloor k)=\sum_{k=1}^{n-1}(n-1-\left\lfloor\frac{n-1}{k}\right\rfloor k)$$

یا

$$(*)\qquad 2n-1=n+\sum_{k=1}^{n-1}(n-(n-1))=\sum_{k=1}^{n}\left\lfloor\frac{n}{k}\right\rfloor k-\sum_{k=1}^{n-1}\left\lfloor\frac{n-1}{k}\right\rfloor k$$

اگر k، n را نشمارد، $\left\lfloor\frac{n}{k}\right\rfloor=\left\lfloor\frac{n-1}{k}\right\rfloor$ و لذا $\left\lfloor\frac{n}{k}\right\rfloor k=\left\lfloor\frac{n-1}{k}\right\rfloor k$؛ اگر k، n را بشمارد آنگاه $\left\lfloor\frac{n}{k}\right\rfloor=\left\lfloor\frac{n-1}{k}\right\rfloor+1$ و لذا $\left\lfloor\frac{n}{k}\right\rfloor k=\left\lfloor\frac{n-1}{k}\right\rfloor k+k$. نتیجه می‌گیریم که رابطه (*) معادل است با

$$2n-1=\sum_{k|n}k$$

اما معادله اخیر با قرار دادن $n=2^m$ برآورده می‌شود که m یک عدد صحیح نامنفی است زیرا

$$2n-1=2^{m+1}-1=1+2+2^2+\cdots+2^m$$

به این ترتیب اگر n توان کاملی از ۲ باشد آنگاه $r(n)=r(n-1)$.

۴۴.این مسأله در ادامه مسأله ۵۲ مقدماتی است

(۱) [IMO ۱۹۹۴] اگر n مضرب ۱۰ باشد، آخرین رقم هر مضرب آن صفر است و بنابراین n هیچ عدد لغزانی را نمی‌شمارد. اگر n مضربی از ۲۵ باشد آن‌گاه دو رقم آخر هر یک از مضاربش ۲۵ یا ۵۰ یا ۷۵ و یا ۰۰ هستند و لذا n هیچ عدد لغزانی را نمی‌شمارد. حال ثابت می‌کنیم اینها تنها اعدادی هستند که هیچ عدد لغزانی را نمی‌شمارند.

اول، اعداد فرد m که بر ۵ بخشپذیر نیستند را بررسی می کنیم. بنابراین $\gcd(m,10)=1$ و برای هر عدد صحیح مثبت k، $\gcd((10^k-1)m,10)=1$. از قضیه اویلر عدد صحیح ℓ وجود دارد که

$$10^{\ell}\equiv 1 \qquad (\text{پیمانه } (10^k-1)m)$$

و به موجب آن

$$10^{k\ell}\equiv 1 \qquad (\text{پیمانه } (10^k-1)m)$$

از

$$10^{k\ell}-1=(10^k-1)(10^{k(\ell-1)}+10^{k(\ell-2)}+\cdots+10^k+1)$$

نتیجه می‌گیریم که

$$w_{۲}=\underbrace{\overline{۱۰۱۰۱۰....}}_{۲\ell-۱\ \text{رقم}}=۱۰^{۲(\ell-۱)}+۱۰^{۲(\ell-۲)}+\cdots+۱۰^{۲}+۱$$

بر m بخشپذیر است. $w_{۲}$ یک عدد لغزان (با ارقام ۰ ،۱) بخشپذیر بر m است.

دوم، اعداد فرد m' را بررسی می کنیم که بر ۵ بخشپذیرند. از آنجا که این عدد بر ۲۵ بخشپذیر نیست می‌توان نوشت $m'=۵m$. سپس $۵w_{۲}$ یک عدد لغزان (با ارقام ۵ ،۰) بخشپذیر بر m' است.

در حالت بعد، توان‌های کامل ۲ را بررسی می‌کنیم. کافی است نشان دهیم $۲^{۲t+۱}$ (برای هر عدد صحیح نامنفی t) یک عدد لغزان $۲t-۱$ رقمی را می‌شمارد. از استقرا روی t استفاده می‌کنیم. پایه استقرا $t=۱$ واضح است. در این حالت می‌توان عدد لغزان $v_{۱}=a_{۱}=۸$ را در نظر گرفت. برای $t=۲$ اعداد به شکل $\overline{a_{۲}\circ ۸}=۱۰\cdot a_{۲}+۸=۴(۲۵a_{۲}+۲)$ $v_{۲}$ را بررسی می‌کنیم. باید یک رقم غیر صفر $a_{۲}$ را چنان پیدا کنیم که (پیمانه ۸) $۲۵a_{۲}+۲\equiv ۰$. به آسانی می‌توان دید که $a_{۲}=۶$ این شرط را برآورده می‌کند و ۶۰۸ یک عدد لغزان مضرب $۲^{۵}$ است. در حالت کلی فرض کنید $۲^{۲t+۱}$ عدد لغزان $v_t=\overline{a_t\circ a_{t-۱}\cdots\circ a_{۱}}$ را می‌شمارد. می‌نویسیم $v_t=۲^{۲t+۱}u_t$. اعداد به شکل زیر را در نظر بگیرید

$$\overline{a_{t+۱}\circ a_t\circ a_{t-۱}\circ....\circ a_{۱}}=a_{t+۱}\times ۱۰^{۲t}+۲^{۲t+۱}\times u_t=۲^{۲t}(۵^{۲t}a_{t+۱}+۲u_t)$$

لازم است رقم $a_{t+۱}$ را چنان پیدا کنیم که (پیمانه ۸) $۵^{۲t}a_{t+۱}+۲u_t\equiv ۰$. از آنجا که مجموعه‌ی $S=\{۱,۲,۳,۴,۵,۶,۷,۸\}$ یک مجموعه کامل مانده‌ها به پیمانه ۸ است، عضو $a_{t+۱}$ در S وجود دارد که (پیمانه ۸) $۵^{۲t}a_{t+۱}+۲u_t\equiv ۰$ و برای این $a_{t+۱}$ عدد لغزان $۲t+۳$ رقمی

$$v_{t+۱}=\overline{a_{t+۱}\circ a_t\circ a_{t-۱}\cdots\circ a_{۱}}$$

بر $۲^{۲t+۳}$ بخشپذیر است و استقرا تکمیل می‌شود.

در نهایت اعداد به شکل $m.۲^t$ که $t\geq ۱$ و $\gcd(m,۱۰)=۱$ را بررسی می‌کنیم. کافی است نشان دهیم $m۲^{۲t+۱}$ یک عدد لغزان را می‌شمارد. ادعا می‌کنیم عددی که از به هم چسباندن $\ell-۱$، $۱۰\times v_t$ و یک $\overline{v_t\circ}=v_t$ به‌دست می‌آید، کار را انجام خواهد داد

$$\overline{v_t\circ v_t\circ ...v_t}=v_t w_{۲t}$$

چون $۲^{۲t+۱}$، v_t را و m، $w_{۲t}$ را می‌شمارد لذا حکم واضح است.

(۲) [IMO ۲۰۰۴] جواب، اعداد صحیح مثبتی است که بر ۲۰ بخشپذیر نیستند. عدد صحیح n را متناوب‌ساز گوییم اگر یک مضرب تناوبی داشته باشد. از آنجا که همه مضارب ۲۰ به یک رقم زوج و یک صفر ختم می‌شوند، مضارب ۲۰ تناوبی نبوده و بنابراین مضارب ۲۰ متناوب‌ساز نیستند. نشان می‌دهیم

همه اعداد دیگر متناوب‌ساز هستند. فرض کنید n یک عدد صحیح مثبت باشد که بر ۲۰ بخشپذیر نیست. توجه کنید که همه عوامل یک عدد متناوب‌ساز، متناوب‌ساز هستند. فرض می‌کنیم n زوج است.

ابتدا نکته کلیدی زیر را مطرح می‌کنیم:

اگر $n=2\times5^{\ell}$ یا $n=2^{\ell}$ (ℓ عدد صحیح مثبت)، آنگاه یک مضرب $X(n)$ از n وجود دارد که $X(n)$ تناوبی بوده و n رقم دارد. قرار می‌دهیم

$$m=\frac{10^{n+1}-10}{99}=\underbrace{\overline{1010101\ldots10}}_{n\text{ رقم}}$$

برای هر عدد صحیح $k=0,1,\ldots,n-1$، دنباله‌ی $e_0,e_1,\ldots,e_k\in\{0,2,4,6,8\}$ وجود دارد که

$$m+\sum_{i=0}^{k}e_i\times10^i$$

بر 2^{k+2} بخشپذیر است اگر n به شکل 2^{ℓ} باشد و بر $2\times5^{k+1}$ بخشپذیر است اگر $n=2\times5^{\ell}$. این مطلب را می‌توان با استقرا روی k (چنانچه در اثبات بخش (۱) مثال ۵۳۰۱ انجام دادیم) اثبات کرد. در حالت خاص $e_0,e_1,\ldots,e_{n-1}\in\{0,2,4,6,8\}$ وجود دارد که

$$X(n)=m+\sum_{i=0}^{n-1}e_i\times10^i$$

بر n بخشپذیر است. این $X(n)$ تناوبی بوده و n رقم دارد که نکته کلیدی مطرح شده را تأیید می‌کند.

حال حکم اصلی را اثبات می‌کنیم. چون n زوج بوده و بر ۲۰ بخشپذیر نیست، n را به صورت $n'm$ که $n'=2^{\ell}$ یا $n'=2\times5^{\ell}$ و $\gcd(m,10)=1$، نشان می‌دهیم. (واضح است $n'\geq\ell$) فرض کنید $c\geq n'$ یک عدد صحیح باشد که (پیمانه m) $10^c\equiv1$ (چنین c وجود دارد زیرا از قضیه اویلر (پیمانه m) $10^{\ell(m)}\equiv1$). فرض کنید M ترکیبی از $X(n')$ و $1010101\cdots$ باشد. بطور دقیق‌تر

$$M=\frac{10^{2mc+1}-10}{99}\times10^{n'}+X(n')=\underbrace{\overline{1010101\cdots10}X(n')}_{2mc\text{ رقم}}$$

چون $X(n')$ یک عدد تناوبی با دقیقاً n' رقم است، M نیز به وضوح یک عدد تناوبی است. چون $n'\geq\ell$ لذا M بر n' بخشپذیر است. از $\gcd(2,m)=1$، $k\in\{0,1,2,\ldots,m-1\}$ وجود دارد که (پیمانه m) $M\equiv-2k$. عدد زیر را در نظر بگیرید

$$X(n)=M+\sum_{i=1}^{k}2\times 10^{ci}$$

از $c\geq n'$ و اینکه $X(n')$ دقیقاً n' رقم دارد، نتیجه می‌گیریم $10^{c}>X(n')$ (با نکته کلیدی که قبلاً مطرح کردیم). به سادگی می‌توان نشان داد $X(n)$ نیز تناوبی است. واضح است که (پیمانه m) $X(n)\equiv m+2k\equiv 0$؛ یعنی $X(n)$ بر m بخشپذیر است. این $X(n)$، n' را نیز می‌شمارد (زیرا n'، $10^{n'}$ را شمرده و آن نیز 10^{c} را می‌شمرد) و تناوبی است. بنابراین $X(n)$ یک عدد تناوبی بخشپذیر بر n است؛ یعنی n متناوب‌ساز است.

توجه: روش‌های مختلفی برای هر دو قسمت وجود دارد. همه‌ی این روش‌ها روی توان‌های ۲ و ۵ کار می‌کنند و از اشکال مشخصی از اعداد تناوبی/ لغزان استفاده می‌کنند. روش‌های مطرح شده در اینجا از این جهت ارائه شده‌اند که مستقل از قضیه مانده چینی هستند.

۴۵. [*USAMO* ۱۹۹۵] گوییم یک زیرمجموعه ازاعداد صحیح مثبت، بدون تصاعد p است اگر شامل یک تصاعد حسابی به طول p نباشد. عدد به‌دست آمده از نوشتن n در مبنای $p-1$ و خواندن آن در مبنای p را با b_n نشان می‌دهیم. می‌توان به سادگی با استفاده از استقرا و خواص مجموعه‌ی $B=\{b_0,b_1,\ldots,b_n,\ldots\}$ که در ادامه می‌آید، ثابت کرد که برای هر $n=0,1,2,\ldots$، $a_n=b_n$:

(آ) B یک مجموعه‌ی بدون تصاعد p است.

(ب) اگر برای یک $n\geq 1$، $b_{n-1}<a<b_n$ آنگاه مجموعه‌ی $\{b_0,b_1,\ldots,b_{n-1},a\}$ بدون تصاعد p نیست.

فرض کنید (آ) و (ب) برقرار باشند. از تعریف a_k و b_k داریم: برای $k=0,1,\ldots,p-2$، $a_k=b_k$.
فرض کنید برای هر $n-1\geq k$، $a_k=b_k$ که $n\geq p-1$. از (آ) مجموعه‌ی

$$\{a_0,a_1,\ldots,a_{n-1},b_n\}=\{b_0,b_1,\ldots,b_{n-1},b_n\}$$

یک مجموعه‌ی بدون تصاعد p است بنابراین $a_n\leq b_n$. نامساوی $a_n<b_n$ نیز به دلیل (ب) غیرممکن است بنابراین $a_k=b_k$ و حکم برقرار است.

حال این باقی می‌ماند که خواص (آ) و (ب) را ثابت کنیم. ابتدا فرض کنید B شامل همه اعدادی باشد که نمایش آن در مبنای p شامل رقم $p-1$ نباشد. با توجه به اینکه اگر $a,a+d,\ldots,a+(p-1)d$ یک تصاعد حسابی به طول p باشد، آنگاه همه‌ی ارقام در مبنای p، در نمایش اعضای آن در مبنای p نیز وجود دارند، (آ) ثابت می‌شود. برای دیدن این موضوع d را به شکل $d=p^{m}k$ که

$\gcd(k,p)=1$، نشان می‌دهیم. به این ترتیب d به m صفر ختم شده و رقم δ قبل از آنها غیر صفر است. به سادگی می‌توان دید که اگر α، $(m+1)$ اُمین رقم a (از راست به چپ) باشد آنگاه ارقام متناظر $a, a+d, \ldots, a+(p-1)d$ به ترتیب مانده‌های $\alpha, \alpha+\delta, \ldots, \alpha+(p-1)\delta$ به پیمانه p هستند. با توجه به اینکه $\alpha, \alpha+\delta, \ldots, \alpha+(p-1)\delta$ یک مجموعه کامل مانده‌ها به پیمانه p است (زیرا δ نسبت به p اول است) اثبات (آ) کامل می‌شود.

اثبات (ب) را با توجه به این نکته آغاز می‌کنیم که $b_{n-1}<a<b_n$ به معنای آن است که a در B نیست. چون B دقیقاً شامل اعدادی است که در مبنای p رقم $p-1$ را ندارند. این ارقام باید در نمایش a درمبنای p نیز بیایند. فرض کنید d عددی باشد که با جایگزین کردن اعداد غیر $p-1$ با 0 و عدد $p-1$ با 1 در a بدست آید. تصاعد زیر را در نظر بگیرید

$$a-(p-1)d, a-(p-2)d, \ldots, a-d, a$$

از تعریف d، اولین $p-1$ عضو در نمایش مبنای p شان شامل $p-1$ نیستند. بنابراین به دلیل کوچک‌تر بودن از a باید متعلق به مجموعه‌ی $\{b_0, b_1, \ldots, b_{n-1}\}$ باشند. لذا $\{b_0, b_1, \ldots, b_{n-1}, a\}$ بدون تصاعد p نیست و اثبات به پایان می‌رسد.

۴۶. [IMO ۲۰۰۰] جواب مثبت است.

ادعا می‌کنیم نکته کلیدی زیر برقرار است:

برای هر عدد صحیح $a>2$ عدد اول p وجود دارد به طوری که p، (a^3+1) را می‌شمارد اما $(a+1)$ را نمی‌شمارد.

از $a^3+1=(a+1)(a^2-a+1)$ لازم است نشان دهیم عدد اول p وجود دارد که $p \mid a^2-a+1$ اما $p \nmid a+1$. از

$$a^2-a+1=(a+1)(a-2)+3$$

نتیجه می‌گیریم که $\gcd(a^2-a+1, a+1)=1$ یا 3. در حالت اول ادعای ما به وضوح برقرار است. در حالت دوم با توجه به اینکه ۳ هر دو عدد $a+1$ و $a-2$ را می‌شمارد، در نتیجه بطور کامل عدد a^2-a+1 را می‌شمارد. از $a>2$، نتیجه می‌گیریم که $a^2-a+1>3$ و لذا عدد اول $p \neq 3$ وجود دارد که a^2-a+1 را می‌شمارد و این عدد اول شرایط ادعای مورد نظر ما را برآورده می‌سازد.

از این ادعا، اعداد اول متمایز (فرد) $p_1, p_2, p_3, \ldots, p_{2\ldots}$ وجود دارند که $p_1=3$ ، $p_2 \neq 3$ ، $p_2 \mid 2^{3^2}+1$ و

$$p_{i+1} \mid (2^{3^{i+1}}+1) \ , \ p_{i+1} \nmid (2^{3^i}+1) \qquad (\text{برای هر } 2 \le i \le 1999)$$

به سادگی می‌توان دید که

$$n = p_1^{2^{000}} . p_2 \dots p_{2^{000}} = 3^{2^{000}} p_2 \dots p_{2^{000}}$$

شرایط مسأله را برآورده می‌کند. برای هر $2 \le i \le 2^{000}$، $3^i \mid 3^{2^{000}}$ و بنابراین

$$p_i \mid 2^{3^i}+1 \mid 2^{3^{2^{000}}}+1$$

با یک استقرا ساده می‌توان نشان داد که 3^{k+1} کاملاً $2^{3^k}+1$ را برای هر عدد صحیح مثبت k می‌شمارد زیرا ۳، a^2-a+1 را برای $a=2^{3^k}$ کاملاً می‌شمارد (همان طور که در اثبات ادعایمان نشان داده‌ایم). بنابراین چون n یک مضرب فرد $3^{2^{000}}$ است نتیجه می‌گیریم که

$$n \mid 2^{3^{2^{000}}}+1 \mid 2^n+1$$

۴۷. "مرتبه" نکته کلیدی در این مسأله است.

(۱)[۲۰۰۰ روسیه] جواب منفی است. ادعا می‌کنیم که چنین اعداد صحیحی وجود ندارند.

فرض کنید اعداد دو به دو نسبت به هم اول $a,b,c>1$ وجود داشته باشند که b، 2^a+1 را شمرده a، 2^c+1 شمرده و c، 2^b+1 را بشمرد. بنابراین a,b,c همگی فرد هستند.

برای اینکه کار کمی ساده‌تر شود ابتدا فرض می‌کنیم a,b,c اعداد اول باشند. با شرایط چرخشی مطرح شده در مسأله می‌توان فرض کرد $a<b$ و $a<c$. از قضیه کوچک‌فرما و قضیه ۳۰.۱ $\text{ord}_a(2) \mid \gcd(2c, a-1) = 2$ چرا که c یک عدد اول بزرگ‌تر از a است. چون a یک عدد اول فرد است $\text{ord}_a(2)$ باید ۲ باشد و به موجب آن $a=3$. به این ترتیب $b \mid 2^a+1=9$ که تناقض است.

حال اگر a,b,c هیچ‌کدام اول نباشند چه می‌شود؟ سعی می‌کنیم روش قبلی خود را تعمیم دهیم. فرض کنید $\pi(n)$ کوچک‌ترین عامل اول عدد صحیح مثبت n باشد. ادعا می‌کنیم:

اگر p یک عدد اول باشد که $p \mid (2^y+1)$ و $p < \pi(y)$ آنگاه $p=3$.

اثبات این ادعا مشابه بحث قبلی برای حالت اول بودن a,b,c است. پس

$$\text{ord}_p(2) \mid \gcd(2y, p-1) = 2$$

مجدداً داریم $\text{ord}_p(2)=2$ و $p=3$ که تأیید ادعای ماست.

حال مسأله اصلی را حل می‌کنیم. از این‌که a, b و c دو به دو نسبت به هم اول‌اند، $\pi(a), \pi(b)$ و $\pi(c)$ متمایز هستند. بدون از دست دادن کلیت مسأله فرض می‌کنیم $\pi(a) < \pi(b), \pi(c)$. با بکارگیری ادعای مطرح شده با جایگزینی $(p, y) = (\pi(a), c)$ در می‌یابیم که $\pi(a) = ۳$ و می‌نویسیم $a = ۳a_۰$. ادعا می‌کنیم ۳ به‌طور کامل a را می‌شمارد. در غیر این‌صورت ۹، $۲^c + ۱$ را خواهد شمرد و بنابراین $۲^{۲c} - ۱$ را نیز می‌شمرد. چون رابطه (پیمانه ۹) $۲^n \equiv ۱$ فقط زمانی برقرار است که $۶ | n$، باید داشته باشیم $۶ | ۲c$ و یا $۳ | c$ که با فرض اول بودن a و c نسبت به هم در تضاد است. بنابراین $a_۰, b$ و c هیچکدام بر ۳ بخشپذیر نیستند.

فرض کنید $q = \pi(a_۰bc)$ و $\pi(q) = q \le \min\{\pi(b), \pi(c)\}$. فرض کنید q، a را می‌شمارد. چون a و c نسبت به هم اول هستند، q نمی‌تواند c را بشمارد یعنی $\pi(q) = q$ با $\pi(c)$ برابر نیست. چون $\pi(q) \le \pi(c)$، باید داشته باشیم $\pi(q) < \pi(c)$. علاوه بر آن q باید $۲^c + ۱$ را بشمرد زیرا یک عامل $۲^c + ۱$ (به نام a) را می‌شمارد. با بکارگیری ادعای مطرح شده با جایگزینی $(p, y) = (q, c)$ در می‌یابیم $q = ۳$ که تناقض است. بنابراین فرض ما غلط بوده و q، a را نمی‌شمرد. به‌طور مشابه q، c را نیز نمی‌شمرد؛ لذا q باید b بشمرد.

حال فرض کنید e، مرتبه ۲ به پیمانه q باشد. پس $e \le q - ۱$ و e هیچ عامل اول بزرگ‌تر از q ندارد. در ضمن q، b را شمرده و بنابراین $۲^a + ۱$ و $۲^{۲a} - ۱$ را نیز می‌شمرد؛ در نتیجه $e | ۲a$. تنها عوامل اول $۲a$ کوچک‌تر از q، ۲ و ۳ هستند؛ لذا $e | ۶$. به این ترتیب $q | (۲^۶ - ۱)$ و $q = ۷$. می‌دانیم (پیمانه ۷) $۲^۳ \equiv ۱$ بنابراین (پیمانه ۷) $۲^{a_۰} + ۱ \equiv (۲^۳)^{a_۰} + ۱ \equiv ۲$. پس $۲^a + ۱ \equiv ۱$، q را نمی‌شمارد که با فرض این‌که q، b را می‌شمرد در تناقض است.

(۲) [TST ۲۰۰۳] جواب، $(۲, ۵, ۳)$ و هر جایگشت دوری آن است. جواب بودن این اعداد را بررسی می‌کنیم.

$$۲ | ۱۲۶ = ۵^۳ + ۱ \quad , \quad ۵ | ۱۰ = ۳^۲ + ۱ \quad , \quad ۳ | ۳۳ = ۲^۵ + ۱$$

حال p، q و r را سه عدد اولی می‌گیریم که روابط بخشپذیری داده شده در مسأله را برآورده می‌کنند. چون q، $q^r + ۱$ را نمی‌شمرد، پس $p \neq q$ و بطور مشابه $q \neq r$ و $r \neq p$. لذا r, q, p متمایز هستند. از مسأله مقدماتی ۴۹ (۱) کمک می‌گیریم.

ابتدا حالتی را که p، q و r همگی فرد هستند در نظر می‌گیریم. از $p | q^r + ۱$ و مسأله مقدماتی ۴۹ (۱) نتیجه می‌گیریم که $۲r | p - ۱$ یا $p | q^۲ - ۱$. اما $۲r | p - ۱$ غیرممکن است زیرا به موجب این

رابطه داریم (پیمانه r) $p \equiv ۱$ و یا (پیمانه r) $p^q + ۱ \equiv ۲ \equiv ۰$ که با فرض $r > ۲$ در تضاد است. بنابراین باید داشته باشیم $p \mid q^۲ - ۱ = (q-۱)(q+۱)$. چون p عدد اول فرد بوده و $q-۱$ و $q+۱$ هر دو زوج هستند باید داشته باشیم $p \mid \frac{q-۱}{۲}$ یا $p \mid \frac{q+۱}{۲}$. در هر صورت $p \le \frac{q+۱}{۲} < q$. با استدلالی مشابه نتیجه می‌گیریم $q < r$ و $r < p$ که تناقض است.

به این ترتیب حداقل یکی از p، q و r باید برابر ۲ باشد. با یک جایگشت دوری می‌توان فرض کرد $q = ۲$. حال $p \mid ۲^r + ۱$ و از مسأله مقدماتی ۴۹ (۱) $۲r \mid p-۱$ یا $p \mid ۲^۲ - ۱ = ۳$. اما $۲r \mid p-۱$ چنانچه قبلاً بحث کردیم غیر ممکن است زیرا r، $p^q + ۱ = p^۲ + ۱ = (p^۲ - ۱) + ۲$ را می‌شمارد و $r > ۲$. لذا داریم $p = ۳$ و $r \mid p^q + ۱ = ۳^۲ + ۱ = ۱۰$. چون $r \neq q$ باید داشته باشیم $r = ۵$. بنابراین $(۲,۵,۳)$ و جایگشت‌های دوری آن تنها جواب‌های ممکن هستند.

۴۸. [*IMO* ۲۰۰۲]

اثبات اول: از استقرا روی n استفاده می‌کنیم.

برای $n = ۱$ عدد $a_۱ = ۲^{p_۱} + ۱$ را بررسی می‌کنیم. چون $p_۱$ فرد است، (پیمانه ۳) $۲^{p_۱} + ۱ \equiv -۱ + ۱ \equiv ۰$. بنابراین $a_۱$، دارای مقسوم علیه‌های متمایز ۱ ، ۳ و خود $a_۱$ است. چون $p_۱ > ۳$، $a_۱ > ۹$ و بنابراین $\frac{a_۱}{۳}$ مقسوم علیه دیگر $a_۱$ است. در نتیجه $a_۱$ حداقل ۴ مقسوم علیه متمایز $۱, ۳, \frac{a_۱}{۳}$ و $a_۱$ را دارد و حکم برای پایه استقرا ثابت می‌شود.

فرض کنید حکم برای $n = k$ (k عددی صحیح و مثبت) برقرار باشد یعنی $a_k = ۲^{p_۱ p_۲ \cdots p_k} + ۱$، حداقل ۴^k مقسوم علیه متمایز دارد. حالت $n = k+۱$ را بررسی می‌کنیم. چون $p_۱, p_۲, \ldots, p_{k+۱}$ همگی فرد هستند، ۳ هر دو عدد a_k و $۲^{p_{k+۱}} + ۱$ را می‌شمارد. همچنین ازمسأله مقدماتی ۳۸ (۳) داریم

$$\gcd(a_k, ۲^{p_{k+۱}} + ۱) = \gcd(۲^{p_۱ p_۲ \cdots p_k} + ۱, ۲^{p_{k+۱}} + ۱) = ۳$$

یا

$$\gcd(a_k, \frac{۲^{p_{k+۱}} + ۱}{۳}) = ۱ \qquad (*)$$

a_k و $۲^{p_{k+۱}} + ۱$ هر دو $a_{k+۱}$ را می‌شمارند زیرا $p_۱ p_۲ \ldots p_k$ و $p_{k+۱}$ فرد هستند. در نتیجه

$$a_{k+۱} = a_k \cdot \frac{۲^{p_{k+۱}} + ۱}{۳} b_k \quad (b_k \text{ یک عدد صحیح است}) \qquad (**)$$

از فرض استقرا و با استفاده از (*) نتیجه می‌گیریم که حاصل‌ضرب $a_k.\frac{۳^{pk+۱}+۱}{۳}$ حداقل ۲×۴^k مقسوم علیه دارد که به‌طور مثال ۴^k تای آنها $d_۱,d_۲,....,d_{۴^k}$ مقسوم علیه‌های a_k بوده و ۴^k مقسوم علیه دیگر به‌صورت

$$d_i.\frac{۳^{pk+۱}+۱}{۳} \qquad (i=۱,...,۴^k)$$

هستند. این ۲×۴^k مقسوم علیه را به‌صورت صعودی مرتب می‌کنیم $d_{۲\times ۴^k}$ $<\cdots<d_۲<d_۱$. از (**)، این اعداد مقسوم علیه‌های $a_{k+۱}$ نیز هستند. حال اعداد زیر را در نظر بگیرید

$$d_۱b_k\ ,d_۲b_k\ ,...,d_{۲\times ۴^k}b_k$$

این اعداد نیز مقسوم علیه‌های $a_{k+۱}$ هستند. ادعا می‌کنیم

$$d_۱,d_۲,...,d_{۲\times ۴^k}\ ,d_۱b_k\ ,d_۲b_k\ ,...,d_{۲\times ۴^k}b_k$$

مقسوم علیه‌های متمایز $a_{k+۱}$ هستند. در نتیجه گام استقرا طی شده و $۴^{k+۱}$ مقسوم علیه متمایز برای $a_{k+۱}$ پیدا می‌شود. برای اثبات ادعایمان کافی است نشان دهیم

$$d_۱b_k>d_{۲\times ۴^k}$$

چون $d_۱\geq ۱$ و $a_k\frac{۳^{pk+۱}+۱}{۳}\leq d_{۲\times ۴^k}$، کافی است نشان دهیم

$$b_k>a_k.\frac{۳^{pk+۱}+۱}{۳}$$

یا از (**)

$$(a_k.\frac{۳^{pk+۱}+۱}{۳})^۲<a_{k+۱}$$

نامساوی اخیر معادل با نامساوی

$$(۳^{p_۱p_۲\cdots p_k}+۱)^۲(۳^{pk+۱}+۱)^۲<۹(۳^{p_۱p_۲\cdots p_k p_{k+۱}}+۱)$$

است که آن هم از نامساوی

$$(۳^u+۱)^۲(۳^v+۱)^۲<۹(۳^{uv}+۱)$$

(برای اعداد صحیح u و v که هر دو بزرگ‌تر یا مساوی ۵ هستند) اثبات می‌شود. داریم

$$(۳^u+۱)^۲(۳^v+۱)^۲=(۳^{۲u}+۲\times ۳^u+۱)(۳^{۲v}+۲\times ۳^v+۱)$$
$$<۳\times(۳^{۲u}+۱)\times ۳\times(۳^{۲v}+۱)=۹(۳^{۲u}+۱)(۳^{۲v}+۱)$$
$$=۹(۳^{۲u+۲v}+۳^{۲u}+۳^{۲v}+۱)<۹(۳^{۲u+۲v+۲}+۱)$$
$$<۹(۳^{uv}+۱)$$

چون $uv-۲u-۲v-۲=(u-۲)(v-۲)-۶>۳$

اثبات دوم: یک عدد صحیح را افسرده گوییم اگر فرد بوده، هیچ عامل مربع کامل نداشته باشد، بر ۳ بخشپذیر نبوده و حداقل ۵ باشد. برای هر عدد صحیح m، تعداد عوامل اول متمایز m را با $\tau(m)$ و تعداد مقسوم علیه‌های m را با $d(m)$ نشان می‌دهیم. می‌خواهیم ثابت کنیم برای همه‌ی اعداد صحیح افسرده $d(۳^a+۱)\geq ۴^{\tau(a)}$.

روی $\tau(a)$ استقرا می‌زنیم. برای حالت پایه $\tau(a)=۱$، $۳^a+۱$ دقیقاً یک‌بار بر ۳ بخشپذیر است و از ۳ بزرگ‌تر می‌باشد. بنابراین $\tau(۳^a+۱)\geq ۲$ و $d(۳^a+۱)\geq ۴$.

حال فرض کنید a و b اعداد صحیح افسرده نسبت به هم اول باشند به طوری که حکم برای هر دوی a و b برقرار باشد. واضح است که $۳^{ab}+۱$ بر هر دو عدد $۳^a+۱$ و $۳^b+۱$ بخشپذیر است لذا می‌توان نوشت

$$۳^{ab}+۱=C.\operatorname{lcm}[۳^a+۱,۳^b+۱]$$

چون $ab-۲a-۲b-۴=(a-۲)(b-۲)-۸>۰$ لذا

$$۳^{ab}+۱>۳^{۲a+۲b+۴}>(۳^a+۱)^۲(۳^b+۱)^۲>\operatorname{lcm}[۳^a+۱,۳^b+۱]^۲$$

بنابراین $C\geq \operatorname{lcm}[۳^a+۱,۳^b+۱]$. داریم $\gcd(۳^a+۱,۳^b+۱)=۳$. بنابراین ۳ هر یک از $۳^a+۱$ و $۳^b+۱$ را دقیقاً یک‌بار می‌شمرد و

$$d(\operatorname{lcm}[۳^a+۱,۳^b+۱])=\frac{d(۳^a+۱)\,d(۳^b+۱)}{۲}\geq ۳^{۲\tau(a)+۲\tau(b)-۱}$$

برای هر مقسوم علیه m از $\operatorname{lcm}[۳^a+۱,۳^b+۱]$، هر دو عدد m و Cm مقسوم علیه‌های $۳^{ab}+۱$ هستند. از $C>\operatorname{lcm}[۳^a+۱,۳^b+۱]$ نتیجه می‌گیریم که

$$d(۳^{ab}+۱)\geq ۲\times d(\operatorname{lcm}[۳^a+۱,۳^b+۱])\geq ۴^{\tau(a)+\tau(b)}$$

و استقرا تکمیل می‌شود.

اثبات سوم: با همان تعاریف اثبات دوم، یک ادعای قوی‌تر برای هر عدد صحیح افسرده این است که

$$\tau(2^a+1)\geq 2\tau(a)$$

با استقرا روی $\tau(a)$ پیش می‌رویم. حالت پایه مشابه راه حل نخست است.

حال فرض کنید a و b اعداد صحیح ا فسرده نسبت بـه هـم اول باشـند. ادعـا مـی‌کنـیم $\tau(2^{ab}+1)\leq \tau(2^a+1)+\tau(2^b+1)$. توجه کنید که

$$\frac{2^{ab}+1}{2^a+1}=\sum_{i=1}^{b}\binom{b}{i}(-2^a-1)^{i-1}\equiv b-\binom{b}{2}(2^a+1) \qquad ((2^a+1)^2 \text{ پیمانه})$$

بنابراین اگر عدد اول p، 2^a+1 را دقیقاً $k\geq 1$ بار بشمرد، آنگاه p، $2^{ab}+1$ را نیز k بار (اگر p، b را نشمرد) یا $k+1$ بار (اگر p، b را بشمرد) می‌شمرد. در هر صورت p، $2^{ab}+1$ را حـداکثر دو برابـر تعداد دفعاتی که p، 2^a+1 را می‌شمرد، می‌شمرد. این مطلب برای عوامل اول 2^b+1 نیز درست اسـت. همانند راه حل اول، $(2^b+1)^2(2^a+1)^2>2^{ab}+1$ و با توجه به مطالب فوق $2^{ab}+1$ بایـد عامـل اولـی داشـته باشـد کـه هـیچ‌یـک از 2^a+1 و 2^b+1 را نشـمرد. واضـح اسـت کـه $2^{ab}+1$ بـر $\operatorname{lcm}[2^a+1,2^b+1]$ بخشپذیر است. چـون $2^{ab}+1$ عامـل اولـی دارد کـه $\operatorname{lcm}[2^a+1,2^b+1]$ را نمی‌شمرد، لذا

$$\begin{aligned}\tau(2^{ab}+1)&\geq \tau(\operatorname{lcm}[2^a+1,2^b+1])+1\\&=\tau(2^a+1)+\tau(2^b+1)-\tau(\gcd(2^a+1,2^b+1))+1\\&=\tau(2^a+1)+\tau(2^b+1)-\tau(3)+1\\&=\tau(2^a+1)+\tau(2^b+1)\end{aligned}$$

و استقرا کامل می‌شود.

۴۹. جواب $p=5$ است. به سادگی می‌توان دید که این مقدار، جواب مسأله هست. برای $p=5$، $a_3=-1$. حال اثبات می‌کنیم که این تنها جواب است.

فرض کنید برای یک مقدار صحیح نامنفی m، $a_m=-1$. به وضـوح $p\neq 2$ زیـرا در غیـر ایـن صـورت $a_{k+2}=2a_{k+1}-2a_k$ زوج است و -1 در دنبالـه ظـاهر نخواهـد شـد. بنـابراین مـی‌تـوان فـرض کـرد $\gcd(2,p)=1$. حال رابطه بازگشتی

$$a_{k+2}=2a_{k+1}-pa_k$$

را به پیمانه p و سپس به پیمانه $p-1$ بررسی می‌کنیم. داریم

$$a_{k+2}\equiv 2a_{k+1} \quad (p \text{ پیمانه})$$

و در نتیجه

$$a_{k+1} \equiv 2^k a_1 \quad (p \text{ پیمانه})$$

در حالت خاص داریم

$$-1 \equiv a_m \equiv 2^{m-1} a_1 \equiv 2^{m-1} \quad (p \text{ پیمانه}) \qquad (*)$$

سپس با در نظر گرفتن پیمانه $p-1$ خواهیم داشت

$$a_{k+2} \equiv 2a_{k+1} - a_k \quad (p-1 \text{ پیمانه})$$

یا

$$a_{k+2} - a_{k+1} \equiv a_{k+1} - a_k \quad (p-1 \text{ پیمانه})$$

یعنی دنباله به پیمانه $p-1$، حسابی است. بنابراین

$$a_{k+1} \equiv (k+1)(a_1 - a_0) + a_0 \equiv k+1 \quad (p-1 \text{ پیمانه})$$

در حالت خاص داریم

$$-1 \equiv a_m \equiv m \quad (p-1 \text{ پیمانه})$$

یا

$$m+1 \equiv 0 \quad (p-1 \text{ پیمانه})$$

از $\gcd(2,p)=1$ و قضیه کوچک‌فرما داریم $2^{p-1} \equiv 1$ (پیمانه p). با در نظر گرفتن دو رابطه هم‌نهشتی اخیر و رابطه (*) داریم

$$1 \equiv 2^{m+1} \equiv 4 \times 2^{m-1} \equiv -4 \quad (p \text{ پیمانه})$$

و به موجب آن (پیمانه p) $5 \equiv 0$؛ یعنی $p=5$ تنها مقدار ممکن است.

۵۰. به دلیل ساده‌تر بودن، از نامساوی کران بالا شروع می‌کنیم. برای یک چنین مجموعه‌ی F تعداد دوتایی‌های متمایز $\{x,y\} \subset \{1,2,\ldots,n\}$ که زیر مجموعه‌های برخی از اعضای F هستند را می‌شماریم. از آنجا که هر مجموعه $A \in F$ شامل سه دوتایی متمایز است و هیچ دو عضوی از F نمی‌توانند دوتایی مشترکی داشته باشند درنتیجه

$$3f(x) \le \binom{n}{2} = \frac{n(n-1)}{2}$$

و نامساوی سمت راست اثبات می‌شود.

حال نامساوی کران پایین را ثابت می‌کنیم. مجموعه‌ی $S=\{1,2,\ldots,n\}$، $\frac{n(n-1)(n-2)}{6} = \binom{n}{3}$ زیرمجموعه‌ی سه عضوی دارد. مجموعه‌ی همه این زیرمجموعه‌های سه عضوی را با T نشان می‌دهیم. مجموعه‌های زیر را مورد بررسی قرار می‌دهیم.

$$T_i = \{\{a,b,c\} \mid \{a,b,c\} \in T \ , \ a+b+c \equiv i \ (n \text{ پیمانه})\} \qquad (i = ۰,۱,\ldots,n-۱)$$

واضح است که این زیرمجموعه‌ها جدا از هم بوده و اجتماعشان T است. به‌عبارت دیگر آنها یک افراز از T هستند. از آنجا که $\binom{n}{۳} = \frac{n(n-۱)(n-۲)}{۶}$ عضو دارد، از اصل لانه کبوتری نتیجه می‌گیریم که حداقل یکی از این n زیرمجموعه حداقل $\frac{n(n-۱)(n-۲)}{۶n} = \frac{(n-۱)(n-۲)}{۶}$ عضو دارد. مثلاً T_j چنین زیرمجموعه‌ای است. ادعا می‌کنیم T_j هر دو شرط آ و ب را برآورده می‌سازد.

واضح است که T_j شرط (آ) را برآورده می‌کند. برای (ب)، فرض کنید (از برهان خلف) دو عضو متمایز A و B در T_j وجود دارد که حداقل ۲ عضو مشترک دارند. فرض کنید $A = \{x, y, z_۱\}$ و $B = \{x, y, z_۲\}$. چون A و B اعضای T_j هستند داریم (پیمانه n) $x + y + z_۱ \equiv j \equiv x + y + z_۲$ و یا $z_۱ \equiv z_۲$ (پیمانه n). اما با توجه به اینکه $z_۱, z_۲ \leq n$، باید داشته باشیم $z_۱ = z_۲$ و لذا $A = B$ که تناقض است. به این ترتیب می‌توان قرار داد $F = T_j$ و بنابراین $f(n)$ حداقل برابر تعداد اعضای موجود در T_j است یعنی

$$f(n) \geq \frac{(n-۱)(n-۲)}{۶}$$

توجه: تحت شرایط مشابه، در ششمین المپیاد ریاضی بالکان خواسته شده بود که

$$\frac{n(n-۴)}{۶} \leq f(n) \leq \frac{(n-۱)n}{۶}$$

۵۱. [IMO ۱۹۹۸]

توجه: فرض کنید $n = p_۱^{a_۱} p_۲^{a_۲} \ldots p_r^{a_r}$ تجزیه n به عوامل اول باشد. آنگاه

$$\tau(n) = (a_۱ + ۱)(a_۲ + ۱)\ldots(a_r + ۱)$$

و

$$\tau(n^۲) = (۲a_۱ + ۱)(۲a_۲ + ۱)\ldots(۲a_r + ۱)$$

بنابراین $\tau(n^۲)$ همواره فرد است و لذا اگر k یک عدد صحیح است، باید فرد باشد. حال ثابت می‌کنیم بر عکس آن نیز صحیح است. یعنی اگر k یک عدد صحیح مثبت فرد باشد آنگاه برای اعداد صحیح نامنفی $a_r, \ldots, a_۲, a_۱$

$$(*) \qquad k = \frac{\tau(n^۲)}{\tau(n)} = \frac{(۲a_۱ + ۱)(۲a_۲ + ۱)\ldots(۲a_r + ۱)}{(a_۱ + ۱)(a_۲ + ۱)\ldots(a_r + ۱)}$$

(از آنجا که بی‌نهایت عدد اول وجود دارد، می‌توان همیشه قرار داد $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$). یک عدد صحیح مثبت را *قابل پذیرش* می‌نامیم اگر بتوان آن را به شکل فوق نوشت.

پاسخ اول: یک روش معمول، استقرای قوی روی k است. حکم برای $k = 1$، با قرار دادن $n = 1$، $r = 1$ و $a_1 = 0$ واضح است.

برای هر عدد صحیح فرد $k > 1$، اگر k به شکل $4m + 1$ باشد، آنگاه

$$k = \frac{4m+1}{2m+1} \cdot 2m + 1$$

از آنجا که $k < 2m + 1$، از فرض استقرا $2m + 1$ قابل پذیرش بوده و لذا k نیز قابل پذیرش است.

اما اگر k به شکل $4m + 3$ باشد آنگاه فرض می‌کنیم به شکل $8m + 3$ باشد. در این صورت داریم

$$k = \frac{24m+9}{12m+5} \cdot \frac{12m+5}{6m+3} \cdot (2m+1)$$

و بنابراین با استفاده از فرض استقرا برای $k > 2m + 1$، k قابل پذیرش است. حال اثبات برای $k = 8m + 7$ باقی می‌ماند. مجدداً آن را به دو حالت تقسیم می‌کنیم. برای پایان دادن به این فرآیند، ایده فوق را به صورت زیر به شکل فرمول در می‌آوریم.

از آنجا که هر عدد صحیح مثبت فرد k را می‌توان به شکل $3^s x - 1$ نوشت (x، عدد صحیح مثبت است) کافی است نشان دهیم اگر x قابل پذیرش باشد، $3^s x - 1$ نیز برای هر $s \geq 1$ قابل پذیرش است. فرض کنید ℓ چنان باشد که

$$\frac{\tau(\ell^2)}{\tau(\ell)} = x$$

اگر $s = 1$، آنگاه

$$k = 3^s x - 1 = 2x - 1 = \frac{2x-1}{x} x$$

نشان می‌دهد که $k = 2x - 1$، قابل پذیرش است.

برای $s > 1$ رابطه

$$3^s x - 1 = \frac{3^s \times 3x - 3}{3^{s-1} \times 3x - 1} \cdot \frac{3^{s-1} \times 3^2 x - 3}{3^{s-2} \times 3^2 x - 1} \cdot \frac{3^{s-2} \times 3^3 x - 3}{3^{s-3} \times 3^3 x - 1} \cdots$$
$$\frac{2^2 \times 3^{s-2} x - 3}{2 \times 3^{s-2} x - 1} \cdot \frac{2 \times 3^{s-1} x - 3}{3^{s-1} x} \cdot x$$

نشان می‌دهد که $k = 3^s x - 1$ قابل پذیرش است. به این ترتیب استقرا پایان می‌یابد.

پاسخ دوم: اثبات مجدداً ازاستقرای قوی است. واضح است که حکم برای $k=1$ برقرار است. فرض کنید $k>1$ یک عدد صحیح مثبت فرد بوده و حکم برای همه اعداد صحیح مثبت فرد کوچک‌تر از k برقرار باشد. مانند پاسخ اول می‌نویسیم $k=3^s x-1$ که x یک عدد فرد کوچک‌تر از k است. از فرض استقرا k قابل پذیرش است. کافی است $a_1,a_2,\ldots,a_t$ را چنان پیدا کنیم که

$$k=x\cdot\frac{2a_1+1}{a_1+1}\cdot\frac{2a_2+1}{a_2+1}\cdots\cdots\frac{2a_t+1}{a_t+1} \qquad (**)$$

توجه کنیدکه اگر قرار دهیم $a_2=2a_1$، $a_3=2a_2$ و الی آخر، معادله (**) به‌صورت زیر ساده می‌شود

$$3^s x-1=k=x\cdot\frac{3^t a_1+1}{a_1+1}$$

یا

$$1=3^s x-\frac{3^t a_1+1}{a_1+1}\cdot x=\frac{3^s a_1+3^s-3^t a_1-1}{a_1+1}\cdot x$$

قرار می‌دهیم $t=s$ و معادله فوق باز هم به‌صورت زیر ساده‌تر می‌شود

$$1=\frac{3^s-1}{a_1+1}\cdot x$$

یا $x(3^s-1)=a_1+1$. به این ترتیب معادله (**)را می‌توان با قرار دادن $t=s$ و $a_1=(3^s-1)x-1$، $a_2=2a_1$، $a_3=2a_2$، ... ، $a_t=2a_t$ برآورده کرد.

۵۲.[۲۰۰۵ چین] برای $1\le n\le 4$، می‌دانیم f_n اول بوده و حکم واضح است. حال فرض می‌کنیم $n\ge 5$. از مسأله مقدماتی ۴۹ می‌توان فرض کرد

$$f_n=p_1^{k_1}p_2^{k_2}\ldots p_m^{k_m} \qquad (*)$$

که m عدد صحیح مثبت، $p_1,\ldots,p_m$ اعداد اول متمایز و $k_1,\ldots,k_m$ اعداد صحیح مثبت هستند و $p_i=2^{n+1}x_i+1$ که x_i نیز عدد صحیح مثبت بوده و $1\le i\le m$. کافی است نشان دهیم برای یک i $(1\le i\le m)$

$$x_i\ge 2(n+1) \qquad (**)$$

ابتدا یک کران بالا برای مجموع $k_1+k_2+\cdots+k_m$ پیدا می‌کنیم. توجه کنید که برای هر i، $p_i\ge 2^{n+1}+1$. در نتیجه از (*) و قضیه دو جمله‌ای داریم

$$۲^{۲^n}+۱=f_n \geq (۲^{n+۱}+۱)^{k_۱+k_۲+\cdots+k_m} \geq ۲^{(n+۱)(k_۱+k_۲+\cdots+k_m)}+۱$$

که به موجب آن

$$k_۱+k_۲+\cdots+k_m \leq \frac{۲^n}{n+۱} \qquad (\dagger)$$

حال یک کران پایین برای مجموع $x_۱k_۱+x_۲k_۲+\cdots+x_mk_m$ پیدا می‌کنیم. مجدداً از قضیه دو جمله‌ای داریم

$$p_i^{k_i} \equiv (۲^{n+۱}x_i+۱)^{k_i} \equiv ۲^{n+۱}x_ik_i+۱ \quad (\text{پیمانه } ۲^{۲n+۲})$$

از $۲^n > ۲n+۲$ برای $n \geq ۵$ داریم (پیمانه $۲^{۲n+۲}$) $f_n \equiv ۱$. با محاسبه معادله (*) به پیمانه $۲^{۲n+۲}$ خواهیم داشت

$$\begin{aligned}۱ &\equiv (۲^{n+۱}x_۱k_۱+۱)(۲^{n+۱}x_۲k_۲+۱)\cdots(۲^{n+۱}x_mk_m+۱)\\ &\equiv ۱+۲^{n+۱}x_۱k_۱+۲^{n+۱}x_۲k_۲+\cdots+۲^{n+۱}x_mk_m \quad (\text{پیمانه } ۲^{۲n+۲})\end{aligned}$$

یا

$$۰ \equiv ۲^{n+۱}(x_۱k_۱+x_۲k_۲+\cdots+x_mk_m) \quad (\text{پیمانه } ۲^{۲n+۲})$$

در نتیجه

$$۰ \equiv x_۱k_۱+x_۲k_۲+\cdots+x_mk_m \quad (\text{پیمانه } ۲^{n+۱})$$

چون x_i ها و k_i ها نامنفی هستند، نتیجه می‌گیریم

$$x_۱k_۱+x_۲k_۲+\cdots+x_mk_m \geq ۲^{n+۱} \qquad (\ddagger)$$

با قرار دادن $x_i=\max\{x_۱,x_۲,\ldots,x_m\}$ نامساوی (‡) به شکل

$$x_i(k_۱+k_۲+\cdots+k_m) \geq ۲^{n+۱}$$

در آمده و از نامساوی (†) نتیجه می‌گیریم که

$$x_i \geq \frac{۲^{n+۱}}{k_۱+k_۲+\cdots+k_m} \geq \frac{۲^{n+۱}}{\frac{۲^n}{n+۱}}=۲(n+۱)$$

و نامساوی مطلوب (**) بدست می‌آید.

تعاریف و قضایا

اتحاد هرمیت

برای هر عدد حقیقی x و هر عدد صحیح مثبت n:

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \left\lfloor x + \frac{2}{n} \right\rfloor + \ldots + \left\lfloor x + \frac{n-1}{n} \right\rfloor = \lfloor nx \rfloor$$

اصل لانه کبوتری

اگر n شی در بین $n > k$ جعبه توزیع شوند برخی از جعبه‌ها حداقل حاوی ۲ شی هستند.

اعداد تام

یک عدد صحیح $n \geq 2$ با این خاصیت که مجموع مقسوم‌علیه‌هایش برابر $2n$ باشد، تام نامیده می‌شود.

اعداد فرما

اعداد صحیح به شکل $f_n = 2^{2^n} + 1$، $n \geq 0$.

اعداد کارمایکل

اعداد صحیح مرکب n که برای هر عددصحیح a رابطه (پیمانه n) $a^n \equiv a$ را برآورده می‌سازند.

اعداد مرسن

اعداد صحیح به شکل $M_n = 2^n - 1$، $n \geq 1$.

الگوریتم اقلیدس

استفاده مکرر از الگوریتم تقسیم:

$$M = nq_1 + r_1, 1 \le r_1 < n$$
$$n = r_1q_2 + r_2, 1 \le r_2 < r_1$$
$$\vdots$$
$$r_{k-2} = r_{k-1}q_k + r_k, 1 \le r_k < r_{k-1}$$
$$r_{k-1} = r_k q_{k+1} + r_{k+1}, r_{k+1} = 0$$

این زنجیره از معادلات محدود است زیرا:

$$n > r_1 > r_2 > \ldots > r_k$$

الگوریتم تقسیم

برای هر عدد صحیح مثبت a و b یک زوج یکتای (q,r) از اعداد صحیح نامنفی وجود دارد که $b = aq + r$ و $r < a$.

بخش اعشاری

تفاضل $x - \lfloor x \rfloor$ بخش اعشاری x نامیده شده و با $\{x\}$ نشان داده می‌شود.

بسط مبنای فاکتوریل

هر عدد صحیح مثبت k یک بسط یکتا به صورت

$$k = 1! \times f_1 + 2! \times f_2 + 3! \times f_3 + \ldots + m! f_m$$

دارد که هر f_i یک عدد صحیح است که $f_m > 0, 0 \le f_i \le i$

تابع جزء صحیح

برای یک عدد حقیقی x، عدد صحیح یکتای n وجود دارد که $n \le x < n+1$. گوییم n بزرگ‌ترین عدد صحیح کوچک‌تر یا مساوی x و یا کف x است و می‌نویسیم $n = \lfloor x \rfloor$.

تابع جمعی

برای یک تابع حسابی f، تابع جمعی F به صورت زیر تعریف می‌شود:

$$F(n) = \sum_{d \mid n} f(d)$$

تابع مسابی

تابعی که روی اعداد صحیح مثبت تعریف شده و دارای مقداری مختلط است.

تابع ضربی

تابع حسابی $f \neq 0$ با این خاصیت که برای هر دو عدد صحیح مثبت نسبت به هم اول m, n برقرار باشد. $f(mn) = f(m)f(n)$

تابع فی‌اویلر

تابع $\varphi(m)$ برابر تعداد اعداد صحیح بین ۱ و n که نسبت به n اول هستند، تعریف می‌شود.

تابع لژاندر

فرض کنید p یک عدد اول باشد. برای هر عدد صحیح مثبت n، $ep(n)$ را برابر توان p در تجزیه‌ی $n!$ به عوامل اول تعریف می‌کنیم.

تابع موبیوس

تابع حسابی μ که به صورت زیر تعریف می‌شود:

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{برای یک عدد اول } p > 1 \quad p^2 \mid n \\ (-1)^k & n = p_1 \cdots p_k \quad (p_k \cdots p_1 \text{ اعداد اول متمایز هستند}) \end{cases}$$

تجزیه کانونی

هر عدد صحیح $n > 1$ را می‌توان به طور یکتا به شکل زیر نوشت:

$$n = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$$

که $P_1, \ldots, P_k$ اعداد اول متمایز و $\alpha_1, \ldots, \alpha_k$ اعداد صحیح مثبت هستند.

تعداد مقسوم‌علیه‌ها

برای عدد صحیح مثبت n، $\tau(n)$ را برابر تعداد مقسوم‌علیه‌های n می‌گیریم. واضح است که:

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

دنباله‌ی فیبوناچی

دنباله‌ای که به این صورت تعریف می‌شود: $F_1=1, F_0=1$ و برای هر عدد صحیح مثبت n، $F_{n+1}=F_n+F_{n-1}$.

رابطه‌ی هم‌نهشتی

فرض کنید a، b و m اعداد صحیح باشند که $m\neq 0$. گوییم a و b به پیمانه‌ی m هم‌نهشت هستند اگر $m \mid (a-b)$ این خاصیت را با (پیمانه m) $a\equiv b$ نشان می‌دهیم. رابطه‌ی "$\equiv$" روی مجموعه‌ی Z از اعداد صحیح رابطه‌ی هم‌نهشتی نامیده می‌شود.

ضریب دو جمله‌ای

مقدار

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

ضریب x^k در بسط $(x+1)^n$ بوده و ضریب دوجمله‌ای نامیده می‌شود.

فرمول لژاندر

برای هر عدد اول p و هر عدد صحیح مثبت n

$$e_P(n)=\sum_{i\geq 1}\left\lfloor\frac{n}{p^i}\right\rfloor$$

فرمول معکوس موبیوس

فرض کنید f یک تابع حسابی و F تابع جمعی آن باشد. در این صورت:

$$f(n)=\sum_{d\mid n}\mu(d)F\left(\frac{n}{d}\right)$$

قضیه‌ی اویلر

فرض کنید a و m اعداد صحیح مثبت نسبت به هم اول باشند در این صورت:

$$a^{\varphi(m)}\equiv 1$$

قضیه‌ی بزو

برای اعداد صحیح مثبت m و n، اعداد صحیح x و y وجود دارند که $mx+by=\gcd(m,n)$

قضیه‌ی بنیادی حساب

هر عدد صحیح n بزرگ‌تر از ۱ یک نمایش یکتا به صورت حاصل‌ضرب اعداد اول دارد.

قضیه‌ی بیتی

فرض کنید α,β دو عدد حقیقی گنگ مثبت باشند به طوری که:

$$\frac{1}{\alpha}+\frac{1}{\beta}=1$$

مجموعه‌های $\{\lfloor\alpha\rfloor,\lfloor 2\alpha\rfloor,\lfloor 3\alpha\rfloor,\ldots\}$ و $\{\lfloor\beta\rfloor,\lfloor\beta 2\rfloor,\lfloor 3\beta\rfloor,\ldots\}$ بخشی از مجموعه‌ی اعداد صحیح مثبت را شکل می‌دهند.

قضیه‌ی دوجمله‌ای

$$(x+y)^n=\binom{n}{0}x^n+\binom{n}{1}x^{n-1}y+\binom{n}{2}x^{n-2}y^2+\ldots+\binom{n}{n-1}xy^{n-1}+\binom{n}{n}y^x$$

قضیه‌ی عدد اول

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

که $\pi(n)$ تعداد اعداد اول کوچک‌تر یا مساوی n است.

قضیه‌ی عدد اول برای تصاعدهای حسابی

برای اعداد صحیح نسبت به هم اول a و r تعداد اعداد اول در تصاعد حسابی $a,a+d,a+2d,a+3d,\ldots$ که کوچک‌تر یا مساوی n هستند را $\pi_{a,d}(n)$ می‌نامیم.

در این صورت:

$$\lim_{n\to\infty}\sqrt{2}\ \frac{\pi_{a,d}(n)}{n\mid\log n}=\frac{1}{\varphi(d)}$$

این نتیجه توسط لژاندر و دیریکله به دست آمده و توسط پوآسن اثبات شده است.

قضیه کوچک فرما

فرض کنید a یک عدد صحیح مثبت و p یک عدد اول باشد. در این صورت:

$$a^P \equiv a \quad (\text{پیمانه } p)$$

قضیه‌ی ویلسون

برای هر عدد اول p:

$$(P-1)! \equiv -1 \quad (\text{پیمانه } p)$$

مجموع مقسوم‌علیه‌ها

برای یک عدد صحیح مثبت n، $\sigma(n)$ را برابر مجموع مقسوم‌علیه‌های مثبت n شامل ۱ و خود n می‌گیریم. وضح است که:

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

مجموعه‌ی کامل مانده‌ها به پیمانه n

مجموعه‌ی S از اعداد صحیح به طوری که برای هر $0 \le i \le n-1$ عضوی مانند s در S وجود دارد که:

$$i \equiv s \quad (\text{پیمانه } n)$$

مرتبه به پیمانه‌ی m

گوییم a به پیمانه‌ی m، دارای مرتبه‌ی d است و آن را با $ord_m(a) = d$ نشان می‌دهیم اگر d کوچک‌ترین عدد صحیح مثبتی باشد که:

$$a^d \equiv 1 \quad (\text{پیمانه } n)$$

معادله‌ی دیوفانتین خطی

معادله‌ای به شکل $a_1x_1 + \ldots + a_nx_n = b$ که $a_n, \ldots, a_2, a_1$ و b اعداد صحیح ثابت هستند.

نامساوی برنولی

برای $x > -1$ و $a > 1$

$$(1+x)^a \ge 1 + ax$$

که تساوی زمانی است که $x = ۰$.

نامساوی میانگین‌های حسابی – هندسی

اگر n عدد صحیح مثبت و $a_۱, a_۲, ..., a_n$ اعداد حقیقی نامنفی باشند آن‌گاه:

$$\frac{۱}{n}\sum_{i=۱}^{n} a_i \geq (a_۱ a_۲ ... a_n)^{\frac{۱}{n}}$$

که تساوی فقط و فقط زمانی است که $a_۱ = a_۲ = ... = a_n$. این نامساوی حالت خاصی از نامساوی میانگین توانی است.

نمایش زکندورف

هر عدد صحیح نامنفی n را می‌توان به‌طور یکتا به شکل زیر نوشت:

$$n = \sum_{k=۰}^{\infty} \alpha_k F_k$$

که $\alpha_k \in \{۰,۱\}$ و برای هر k α $(\alpha_k, \alpha_{k+۱}) \neq (۱,۱)$

نمایش مبنای b

فرض کنید b یک عدد صحیح بزرگتر از ۱ باشد. برای هر عدد صحیح $n \geq ۱$ یک مجموعه‌ی یکتای $(k, a_۰, a_۱, ..., a_k)$ از اعداد صحیح وجود دارد که برای $a_k \neq ۰, ۰ \neq a_i \leq b-۱, i = ۰,۱,...,k$

$$n = a_k b^k + a_{k-۱} b^{k-۱} + ... + a_۱ b + a_۰$$

منابعی برای مطالعه بیشتر [پیشنهاد مترجم]

۱) سید موسوی، سید حسین و انوار، سید شمس الدین، «تئوری اعداد»، انتشارات مبتکران، چاپ نهم ۱۳۷۸.

۲) بهشتی زواره، رویا و میرزاخانی، مریم، «نظریه اعداد»، انتشارات فاطمی، چاپ دوم، ۱۳۸۰.

۳) صفا، مهدی، «مقدمه‌ای بر تئوری اعداد»، انتشارات خوشخوان، چاپ اول، ۱۳۸۶.

۴) باغستانی، علی‌محمد و صفا، مهدی، «مسائل برگزیده‌ی نظریه اعداد»، انتشارات خوشخوان، چاپ اول، ۱۳۸۵.

۵) سرپینسکی، واتسلاو، «تئوری اعداد، ۲۵۰ مسأله حساب»، انتشارات خوارزمی، چاپ دوم، ۱۳۶۹.

۶) نارنجانی، آدینه‌محمد، «آشنایی با نظریه اعداد»، مرکز نشر دانشگاهی، چاپ ششم، ۱۳۸۳.

۷) محمودیان، عبادالله، «المپیاد ریاضی در ایران»، مؤسسه انتشارات علمی دانشگاه صنعتی شریف، چاپ اول، ۱۳۷۴.

۸) محمودیان، عبادالله، ملاحی کارای، کیوان و اخباریفر، مهران، «المپیاد ریاضی در ایران جلد ۲»، مؤسسه انتشارات علمی دانشگاه صنعتی شریف، چاپ اول، ۱۳۷۹.

۹) شفیع زاده، حسین، «مجموعه سؤالات المپیاد ریاضی در ایران»، انتشارات خوشخوان، چاپ اول، ۱۳۸۳.

۱۰) آجرلو، امیر و خزایی، بهزاد، «مسائل پیشنهادی برای المپیادهای بین‌المللی ریاضی ۱۹۹۵-۲۰۰۱»، انتشارات دانش‌پژوهان جوان، چاپ اول، ۱۳۸۳.

۱۱) ولادیمیروویچ فومین، دمیتری، «المپیادهای ریاضی لنینگراد»، نشر گستره، چاپ دوم، ۱۳۷۹.

۱۲) آندریسکو، تیتو و فنگ، زومینگ، «۱۰۱ مسأله جبر»، انتشارات فاطمی، چاپ اول، ۱۳۸۵.

۱۳) آندریسکو، تیتو و فنگ، زومینگ، «۱۰۲ مسأله ترکیبیات»، انتشارات دانش‌پژوهان جوان، چاپ اول، ۱۳۸۳.

۱۴) آندریسکو، تیتو و فنگ، زومینگ، «۱۰۳ مسأله مثلثات»، انتشارات خوشخوان، چاپ اول، ۱۳۸۷.

۱۵) آندریسکو، تیتو، فنگ، زومینگ و لی جرج، «المپیادهای ریاضی مسائل و راه‌حل ها از سرتاسر جهان ۲۰۰۰-۲۰۰۱»، انتشارات مبتکران، چاپ اول، ۱۳۸۴.

و ...

واژه نامه فارسی – انگلیسی

آ

آبر superset
Hermite's identity
probability
Eratosthenes
induction

inclusion and exclusion principle
multiplication principle

pigeonhole principle
prime numbers
twin prime numbers

پ

perfect numbers
real Numbers
even numbers
integer numbers
odd numbers
Fermat numbers
irrational numbers
rational numbers
complex numbers
Mersenne numbers
composite numbers
relatively prime
coprime
Carmichael numbers

Euclidean algorithm
division algorithm

ب

interval
remainder
fractional part
divisibility

greatest common divisor

factorial base expansion

پ

modulo m m
continuous

ت

number Theory
number theory
function
floor function
arithmetic function
multiplicative function

Euler's totient function
Legendre's function

residue classes

sequence

Fibonacci sequence

carrying

ر

recursive relation

congruence relation

ز

subset

س

reducible

ض

binomial coefficient

scaling factor

ع

factor

ق

theorem

proposition

Bezout's identity

fundamental theorem of arithmetic

Beatty's theorem

binomial theorem

Wilson's theorem

Fermat's little theorem

summation function

Mobius function

canonical factorization

factoring

balance scale

linear combination

combinatorics

progression

one-to-one correspondence

contradiction

generating functions

perfect power

ج

permutation

ج

density

polynomial

ح

modular arithmetic

arithmetic

خ

quotient

reflexivity property

transitivity property

د

numerical systems

perfect cube

ن

Abel inequality

Bernoulli's inequality
Schur's inequality

power mean inequality
Jensen's inequality

Cauchy-schwarz inequality
corollary
critical points
Brocard points
lattice points
mapping

Zeckendorf representation

ه

equivalent
convergence
congruent
analytic geometry
synthetic geometry
geometric

ی

injective
one-to-one
monomial
uniqueness

ک

Cartesian
pure imaginary
bound

least common multiple

م

discriminant
distinct
proportional
consecutive
counterexample
trigonometry

reduced complete set of residue classes

complete set of residue classes

complete set of residue classes modulo n

convex
polar coordinates
spherical coordinates
perfect square
area
derivative
multiple
equivalent

Diophantine equation
inverse
divisor
weighted average