فصل شش

مقدمه‌ای بر نظریهٔ اعداد

نظریهٔ اعداد همانا مطالعه اعداد صحیح است. چرا مطالعه اعداد صحیح برای هر کسی که بخواهد بر روی اعداد صحیح مطالعه کند، بدیهی نیست. قبل از هر چیز، چه چیزی را باید بداند؟ داریم ۰، داریم ۱,۲,۳ و الی آخر، و اعداد منفی هم داریم. کدام یک را نمی‌فهمید؟

با این همه ریاضی‌دانی به نام جی اچ هاردی نوشت:

[نظریه اعداد دانان] ممکن است به این توجیه و دل‌خوشی رسیده باشند که علمی وجود دارد، که مال خودشان است، که هر چه از فعالیت‌های مردم عادی بیشتر دور باشد آن علم تمیز و دست نخورده می‌ماند.

آنچه بیشترین توجه هاردی را به خود معطوف داشت این بود که نظریه اعداد نباید در ستیز بکار برود؛ او یک صلح‌گرا بود. خوشا به حالش ولی اگر نظریهٔ اعداد از همهٔ فعالیتهای انسانی بدور باشد، پس چرا مطالعه‌اش کنیم؟ ما بعدها به این پرسش باز می‌گردیم، ولی از روی کنایه، خواهیم دید که هاردی بیچاره در آرامگاه خود منقلب می‌شود.

۱. بخش‌پذیری

در این یادداشتها خصوصیات اعداد صحیح را بررسی خواهیم کرد بنابر این از متغیرهایی استفاده خواهیم کرد که بر حوزه اعداد صحیح تغییر می‌کنند.

طبیعت راستین نظریهٔ اعداد از نخستین تعریف پدیدار می‌شود. می‌گوئیم که a مقسوم‌علیه b است.

اگر عدد صحیحی k باشد به طوری که $ak = b$. این را می‌گویند $a|b$ برای مثال:

$۷|۶۳$ زیرا $۶۳ = ۷.۹$. نتیجه‌ای که از این تعریف به دست می‌آید این است که هر عددی مقسوم‌علیه صفر است زیرا $a.۰ = ۰$ به ازاء هر عدد صحیح a. اگر a مقسوم بر b بشود، آنگاه b مضربی از a است. برای مثال، ۶۳ مضربی از ۷ است.

به نظر می‌آید این به اندازهٔ کافی ساده باشد، ولی بیائید با این تعریف بازی کنیم. پیروان فیثاغورث، فرقه‌ای کهن از صوفی‌های ریاضی، بر این باور بودند که عددی کامل است که با مجموع مقسوم‌علیه مثبت خود برابر باشد، به جز خودش. برای مثال، $۶ = ۳+۲+۱$ و $۲۸ = ۱+۲+۴+۷+۱۴$ اعدادی کامل هستند. از طرف دیگر، ۱۰ عدد کامل نیست زیرا $۸ = ۵+۲+۱$ و ۱۲ عدد کامل نیست زیرا $۱۶ = ۶+۳+۲+۱$. اقلیدس حدود ۳۰۰ سال قبل از مسیح کلیهٔ اعداد کامل صحیح زوج را مشخص کرد. ولی آیا یک عدد کامل فرد وجود دارد؟ بیشتر از دوهزار سال بعد، هنوز نمی‌دانیم! همهٔ اعداد کمتر از $۱۰^{۳۰۰}$ به محاسبه در آمدند، ولی هیچ کس به اثبات نرسانده است که یک عدد کامل فرد در افق به انتظار ننشسته است.

بنابر این هنوز نیم صفحه دربارهٔ نظریهٔ اعداد پیش نرفتیم، که به بیرون از مرزهای دانش بشری پاگذاشته‌ایم. این دیگر معرف همه است. نظریه اعداد پر از پرسشهایی است که آسان مطرح می‌شوند، ولی به طور باورنکردنی پاسخ به آنها مشکل است به طور شگفت‌انگیز، دانشمندان علم کامپیوتر، راههایی را برای تغییر این مشکلات به سودشان پیدا کردند. هرگاه کتابی از آمازون (انتشارات اینترنتی) خریداری کنید، نمرات خود را در شبکهٔ *websis* ببینید یا از یک حساب پرداخت قسطی استفاده کنید،دارید بر روی الگوریتم‌ای نظریه‌ای اعداد تکیه می‌کنید.

هراس نکنید– قصد داریم به تعدادی از قسمتهای ملایم نظریهٔ اعداد بچسبیم هیچ یک از این مسائل بسیار سخت حل نشده را در امتحانات مطرح نخواهیم کرد!

۱. ۱. حقایقی درباره‌ی بخش‌پذیری

لم زیر بعضی از حقایق اولیه درباره بخش‌پذیری را بیان می‌کند که برای ثابت کردن سخت نیستند:

لم۱. ۱ عبارات زیر دربارهٔ بخش‌پذیری صادق هستند.

۱- اگر $a|b$، آنگاه $a|bc$ برای هر c.

۲- اگر $a|b$ و $b|c$ آنگاه $a|c$.

۳- اگر $a|b$ و $a|c$ آنگاه $a|sb+tc$ برای هر s و t.

٤- برای هر $c \neq 0$، $a|b$ اگر و فقط اگر $ca|cb$.

برهان. فقط قسمت (۲) را ثابت خواهیم کرد؛ برهان‌های دیگر شبیه هم هستند.

برهان. (۲): از آنجائیکه $a|b$، یک عدد صحیح k_1 داریم، به طوری که $ak_1 = b$. از آنجائیکه $b|c$، یک عدد صحیح k_2 وجود دارد بطوری که $bk_2 = c$. با جایگزین ak_1 با b در معادلهٔ دوم $ak_1 k_2 = c$ بدست می‌آید، که نتیجه می‌دهد $a|c$. □

یک عدد $P > 1$ که هیچ مقسوم‌علیه مثبتی به غیر از ۱ و خودش ندارد، عدد اول نامیده می‌شود. هر عدد دیگر بزرگتر از ۱ مرکب نامیده می‌شود. برای مثال ۱۱، ۷، ۵، ۳، ۲ و ۳ همگی اوّل هستند، ولی ٤، ٦، ۸ و ۹، مرکب هستند عدد ۱ نه اول و نه مرکب در نظر گرفته می‌شود. این فقط مربوط به تعریف است، ولی این حقیقت را می‌نمایاند که عدد ۱ در بسیاری موارد مثل یک عدد اول رفتار نمی‌کند، به مانند قضیه اصول حساب، که بطور کوتاه به آن سری خواهیم زد.

۲. ۱- هنگامی که بخش‌پذیری جور در نمی‌آید

همان گونه که در مدرسهٔ ابتدایی آموختید، اگر عددی به طور مثبت تقسیم بر دیگری نشود، پس یک "باقی‌مانده" به جا مانده است.به طور مشخص‌تر اگر n را به d تقسیم کنید، آنگاه یک خارج قسمت q و یک باقی‌مانده r بدست می‌آورید. این حقیقت پایه‌ای موضوع یک قضیه مفید است:

قضیه ۲. ۱ (قضیه تقسیم) فرض کنید n و d اعداد صحیحی باشند بطوری که $d > 0$. آنگاه یک جفت عدد صحیح یکتای q و r وجود دارند به طوری که $n = qd + r$ و $0 \le r < d$.

به عنوان یک مثال، در نظر بگیرید که $a = 10$ و $b = 2716$. سپس خارج‌قسمت $q = 271$ می‌شود و باقی‌مانده می‌شود $r = 6$، از آنجائیکه $6 + 10 \times 271 = 2716$.

در قضیه تقسیم به باقی‌مانده r می‌گویند $n \ rem \ d$. به سخن دیگر $n \ rem \ d$ باقی‌مانده است وقتی که n به d تقسیم می‌شود. برای مثال، ۳۲ rem ۵ باقی‌مانده است وقتی که ۳۲ تقسیم بر ۵ بشود که می‌شود ۲. به طور مشابه، ۳ = ۷ rem ۱۱− از آنجائیکه ۳ + ۷.(۲-) = ۱۱−.

در بسیاری از زبانهای برنامه‌نویسی یک عامل باقی‌مانده طراحی شده است. برای مثال، ۳۲٪۵، به ۲ شکل درجاوا، c و $c++$ محاسبه می‌شود. با این وجود، تمامی این زبان‌ها اعداد منفی را غریبانه می‌بینند.

تعدادی از روشهای نام‌گذاری هستند که به قضیهٔ تقسیم مربوط است. ابتدا، قضیه غالباً "الگوریتم تقسیم" نامیده می‌شود،حتی[1] اگر در مفاهیم مدرن یک الگوریتم نباشد. دوم اینکه، برخی‌ها از نماد "mod" (که کوتاه شدهٔ mod*ulo* است) به جای "*rem*" استفاده می‌کنند. این مایهٔ تأسف است، برای اینکه قرن‌ها ریاضی‌دانان اشتباهاً از "mod" به جای "*rem*" در موارد مشابه استفاده می‌کردند، که به آن هم نظری کوتاه خواهیم انداخت. بنابر این در اینجا از "*rem*" بهره خواهیم برد.

مسائل مشهور در نظریهٔ اعداد

قضیهٔ آخر فرما آیا وجود دارد اعداد صحیح مثبت x، y و z به طوری که

$$x^n + y^n = z^n$$

برای یک عدد صحیح $n > ۲$؟ حدود سال ۱۶۳۰ در حال خواندن کتابی، فرما ادعا کرد که برهانی دارد، ولی در حاشیه آن جای کافی برای یادداشت آن ندارد. وایلز سرانجام در ۱۹۹۴ برهانی

دربارهٔ این قضیه، پس از گذراندن هفت سال در خفا و انزوا در اتاق زیر شیروانی ارائه کرد. برهان او در هیچ حاشیه‌ای جا نمی‌گرفت.

حدس گولدباخ این است که هر عدد زوج صحیح بزرگتر یا برابر با ۲ برابر با مجموع دو عدد اول است؟ برای مثال، ۵+۳=۳+۳,۸=۳+۲,۶=۲+۴ و غیره.این حدس برای کلیهٔ اعداد که تا $۱۰^{۱۶}$ رقم دارند صدق می‌کند. در ۱۹۳۹، اشنیرلمن ثابت کرد که هر عدد زوجی می‌تواند به مانند مجموع حداکثر ۳۰۰/۰۰۰ عدد اول نوشته شود، که تازه اول کار بود. امروزه می‌دانیم که هر عدد زوج صحیحی حداکثر مجموعی از ۶ عدد اول است.

حدس اعداد اول دوقلو: آیا به طور نامتناهی اعداد اول بسیاری نظیر p وجود دارند به طوری که $p+۲$ هم یک عدد اول باشد؟ ۱۹۹۶ چن نشان داد که بطور نامتناهی اعداد اول بسیاری نظیر P وجود دارند به طوری که $P+۲$ مضرب حداکثر دو عدد اول است. بنابر این آن حدس تقریباً صحیح خوانده می‌شود!

آزمون اول بودن: آیا روش مؤثری برای تعیین اینکه n یک عدد اول باشد وجود دارد؟ یک روش حیرت‌آور ساده، سرانجام در سال ۲۰۰۲ توسط آگراوال، کایال و ساکسنا کشف شد. مقالهٔ آنها با نقل‌قولی از گاس با تأیید بر اهمیت و قدمت مسئله حتی[۱] در زمان خود- دو قرن پیش، شروع می‌شد.

عوامل ضرب: فرض که مضرب دو عدد اول بزرگ $n = pq$ در دسترس باشد، آیا روش مؤثری

برای بدست آوردن اعداد اول p و q وجود دارد؟ بهترین الگوریتم شناخته شده "غربال میدان اعداد است، که در زمان متناسب است با:

$$e^{(1/9)(\ln n)^{1/3}(\ln \ln n)^{2/3}}$$

هنگامی که n به تعداد یکصد عدد یا بیشتر داشته باشد شدنی نیست.

قصد نداریم قضیهٔ تقسیم را ثابت کنیم، ولی یک وجه مهم هست که باید به آن توجه کنید. قضیه تأکید می‌کند که خارج‌قسمت q و باقی‌مانده r وجود دارند و همچنین این r,qها یکتا هستند. این چنین، قضیه‌ای مثالی از یک قضیهٔ "وجود و یکتایی " است؛ از این قبیل بسیارند. نه خیلی شگفت‌آور، برهان چنین قضیه‌ای همیشه دو وجه دارد:

- برهانی که می‌گوید چیزی وجود دارد، مثل خارج‌قسمت q و باقی‌مانده r.
- برهانی که می‌گوید هیچ چیز دیگری با صورت حساب مناسب نیست؛ یعنی که، هیچ خارج‌قسمت q' و باقی‌مانده r' در کار نیست.

۲. جان‌سخت

سیمون: در آن مخزن، ۲ تا کوزه باید باشد، می‌بینی شان؟ یکی ۵گالنی و یک ۳ گالنی. یکی از کوزه‌ها را دقیقاً با ۴ گالن آب پرکنید و آن را روی ترازو قرار دهید و زمان‌سنج خواهد ایستاد باید دقت کنید؛ یک اونس بیشتر یا کمتر نتیجه‌اش انفجار خواهد بود. اگر تا ۵ دقیقه دیگر بازهم زنده

باشید، حرف خواهیم زد.

بروس: صبر کن، یک لحظه صبر کن. متوجه نمی‌شوم. تو متوجه می‌شوی؟

ساموئل: نه.

بروس: ظرف‌ها را بیاور. معلوم است که با ظرف ۴ گالنی نمی‌توانیم ظرف ۳ گالنی را پر کنیم.

ساموئل: خب معلوم است.

بروس: بسیار خوب. فهمیدم، این کار را می‌کنیم. ظرف ۳ گالنی را تا سر پر می‌کنیم، درسته؟

ساموئل: آها.

بروس: خوب، حالا ظرف ۳ گالنی را در ۵ گالنی می‌ریزیم، که دقیقاً ۳ گالن در ظرف ۵ گالنی داریم، درست است؟

ساموئل: درست، بعدش چی؟

بروس: بسیار خوب. ظرف ۳ گالنی را بر می‌داریم و آن را از یک سوم پر می‌کنیم.

ساموئل: نه! او گفت که "دقت کنید" دقیقاً ۴ گالن.

بروس: گ . . . هر پلیس در ۵۰ مایلی اینجا دارد جان می‌دهد من دارم در این پارک بچه بازی در می‌آورم.

ساموئل: هی می‌خواهی روی مسئله تمرکز کنی؟

این قسمتی از فیلم جان‌سخت ۳ می‌باشد: در کینه‌جویی ساموئل ال‌جکسون و بروس ویلیس باید بمبی که سیمون کرو بر اهریمن صفت کار گذاشته را خنثی کنند. خوشبختانه، آنها راهی را در سربزنگاه می‌یابند. (احتمالاً با خواندن شرح کمکی) در ظاهر امر، فیلم جان‌سخت ۳ یک فیلم درجهٔ B اکشن است؛ با این وجود، به نظر می‌رسد پیام درونی فیلم این باشد که هر کسی باید حداقل کمی دربارهٔ نظریه اعداد بداند.

متأسفانه، هالیوود اجازهٔ استفاده از ترفند نمی‌دهد. در حال برنامه‌ریزی برای ادامهٔ سری‌های جان‌سخت هستند:

جان‌سخت ۴: سخت‌جان‌ترین – بروس به تعطیلات می‌رود و– بطور تکان دهنده‌ای – در یک توطئهٔ تروریستی گیر می‌افتد. برای نجات روز تعطیل، باید گالن با حجم ۳ را با استفاده از ظرفهای ۲۱ و ۲۶ گالنی پر کند.

جان‌سخت ۵: مرگ عصر کهن، بروس باید همکار در قید حیات خود را از دست یک نابغهٔ جانی با پر کردن گالن با حجم ۲ با ظرفهای ۸۹۹ و ۱۱۴۷ گالنی نجات بدهد.

جان‌سخت ۶: مرگ یک‌بار برای، همه، بروس باید گالن با حجم ۴ با استفاده از ظرف‌های ۳ و ۶ گالنی درست کند.

اگر می‌توانستیم این پرسشهای ظروف آب احمقانه را به یکباره حل کنیم خوب می‌شد. بطور خاص، چطور می‌توان گالن با حجم g را با استفاده از ظرفهایی با ظرفیت a و b تشکیل داد؟ اینجاست که قضیهٔ اعداد سودمند است.

۱. ۲ یافتن یک ویژگی پایا

فرض کنید کوزه‌هایی با ظرفیت‌های a و b داریم. بیائید چندین عملیات دل بخواهی انجام دهیم و ببینیم چه اتفاقی می‌افتد؟ وضع دستگاه در هر مرحله در پائین با یک جفت اعداد (x,y) شرح داده می‌شود، جایی که x مقدار آب درون کوزه است با ظرفیت a و y مقدار آب در کوزه با ظرفیت b است.

پر کردن اولین کوزه	$(۰,۰)\to(a,۰)$
ریختن اولین درون دومین کوزه	$\to(۰,a)$
پر کردن اولین کوزه	$\to(a,a)$
ریختن اولین درون دومین‌کوزه	$\to(۲a-b,b)$
خالی کردن دومین کوزه	$\to(۲a-b,۰)$
ریختن اولین کوزه در دومین کوزه	$\to(۰,۲a-b)$
پر کردن اولین کوزه	$\to(a,۲a-b)$
ریختن اولین در دومین کوزه	$\to(۳a-۲b,b)$

پر البته، در اینجا در حال ساختن گمان‌هایی دربارهٔ ظرفیت‌های نسبی دو کوزه هستیم. ولی نکته‌ای دیگر از نظر دور می‌شود: در مرحله، مقدار آب در هر کوزه به این شکل است.

$$s\,a+t\,b \qquad (۱)$$

برای بعضی از اعداد صحیح s و t. به نظر می‌رسد که شبیه ادعایی باشد که بتوانیم با استقراء آن را ثابت کنیم! اصطلاحی از شکل (۱) را یک ترکیب خطی صحیح از a و b می‌نامند، ولی در این یادداشت‌ها آن را ترکیب خطی می‌نامیم، از آن رو که فقط از اعداد صحیح حرف می‌زنیم.

در کلاس، می‌خواهیم لم زیر را ثابت کنیم:

لم۱. ۲ فرض کنید که کوزه‌هایی با ظرفیت‌های a و b داریم. آنگاه مقدار آب هر کوزه همیشه یک ترکیب خطی از a و b است.

این قضیه یک قضیهٔ فرعی مهم دارد، که آن را هم در کلاس ثابت خواهیم کرد.

قضیه فرعی ۲. ۲ بروس می‌میرد.

لم ۱. ۲ خیلی رضایت‌بخش نیست. ما هم‌اکنون ترتیبی داده‌ایم تا یک پرسش قابل فهم قشنگ دربارهٔ کوزه‌های آب را به یک پرسش دربارهٔ ترکیب خطی قالب‌ریزی کنیم. شاید این کار پیشرفت به نظر نیاید. خوشبختانه، ترکیب‌های خطی از نزدیک به چیزی بسیار آشناتر مربوطند و آن موضوع در حل مسئله کوزهٔ آب به ما کمک خواهد کرد.

۳. بزرگترین مقسوم‌علیه مشترک

بزرگترین مقسوم‌علیه مشترک a و b دقیقاً همان است که حدس زده‌اید: بزرگترین عددی که مقسوم‌علیه هر دوی a و b است. به صورت $gcd(a,b)$ نوشته می‌شود. برای مثال، $gcd(۱۸,۲۴) = ۶$

احتمالاً برخی از استادان جوان ریاضی شما را برای محاسبهٔ بزرگترین مقسوم‌علیه مشترک بدون هیچ دلیل بارزی تحت فشار گذاشته‌اند تا اینکه رنگ صورتتان کبود شده است. ولی، در کمال تعجب، بزرگترین مقسوم‌علیه مشترک عملاً به کاملاً مفید بودن درباره اعداد صحیح اشاره می‌کند بخصوص، مقدار کمیت $gcd(a,b)$ یک سری معلومات با ارزش دربارهٔ رابطهٔ میان اعداد a و b است. بنابر این در تمام مدت دربارهٔ بزرگترین مقسوم‌علیه مشترک بحث خواهیم کرد.

۱. ۳ ترکیب‌های خطی و GCD

قضیهٔ زیر بزرگترین مقسوم‌علیه مشترک را با ترکیب‌های خطی مرتبط می‌سازد این قضیه بسیار سودمند است؛ برای فهمیدنش وقت بگذارید و آن را به خاطر بسپارید!

قضیه ۱. ۳: بزرگترین مقسوم‌علیه مشترک عدد a,b مساوی است با کوچکترین ترکیب خطی مثبت اعداد a,b.

برای مثال: بزرگترین مقسوم‌علیه مشترک ۵۲ و ۴۴ همان ۴ است. و ،بقدر کافی مطمئن، ۴ ترکیب خطی ۵۲ و ۴۴ است.

$$۶.۵۲ + (-۷).۴۴ = ۴$$

باز هم بیشتر، هیچ ترکیب خطی ۵۲ و ۴۴ با کوچکترین عدد صحیح مثبت برابر نیست.

برهان. فرض کنید m کوچکترین ترکیب خطی مثبت a و b باشد. ثابت می‌کنیم که $m = gcd(a,b)$ با نشان دادن هر دوی $gcd(a,b) \le m$ و $m \le gcd(a,b)$.

ابتدا، نشان می‌دهیم که $gcd(a,b) \le m$. با استفاده از تعریف مقسوم‌علیه مشترک، $gcd(a,b)|a$ و $gcd(a,b)|b$ بنابراین، برای هر جفت عدد صحیح s و t:

$$gcd(a,b)|sa+tb$$

بنابر این، بطور خاص، $gcd(a,b)$ مقسوم‌علیه m است، و بنابر این $gcd(a,b) \le m$. اینک، نشان می‌دهیم که $m \le gcd(a,b)$. با نشان دادن اینکه $m|a$ این که کار را انجام می‌دهیم. یک استدلال متقارن نشان می‌دهد که $m|b$، که معنی‌اش این است که m یک مقسوم‌علیه مشترک a و b است. به این ترتیب، m باید کوچکتر، یا مساوی از بزرگترین مقسوم‌علیه مشترک a و b باشد.

همه آنچه باقی می‌ماند این است که نشان داده شود $m|a$. با استفاده از الگوریتم تقسیم، یک خارج‌قسمت q و باقی‌مانده r وجود دارد به طوری که:

$$a = q.m + r \qquad (\text{جایی که } 0 \le r < m)$$

یادتان باشد که $m = sa+tb$ برای بعضی عددهای صحیح s و t. با جایگزینی m و تنظیم مجدد عبارات بدست می‌آید:

$$a = q.\ (sa+tb) + r$$

$$r = (1 - qs)a + (-qt)b$$

همین حالا نتیجه شد که r به عنوان ترکیب خطی a و b است. با این وجود، m کوچکترین ترکیب خطی مثبت است و $0 \le r < m$. تنها امکان این است که باقی‌مانده r مثبت نباشد؛ یعنی که، $r = 0$. این نتیجه می‌دهد $m \mid a$. □

برهان خاطر نشان می‌کند هر ترکیب خطی a و b مضربی از $gcd(a,b)$ است. بطور معکوس، از آنجا که $gcd(a,b)$ یک ترکیب خطی a و b است، هر مضربی از $gcd(a,b)$ نیز چنین است. این یک قضیهٔ فرعی را پایه‌ریزی می‌کند:

قضیهٔ فرعی ۲. ۳ هر ترکیب خطی a و b مضربی از $gcd(a,b)$ است و برعکس.

حالا می‌توانیم لم کوزه‌های آب را به شکل عبارتهای بزرگترین مقسوم‌علیه مشترک بر زبان آوریم:

قضیهٔ فرعی ۳. ۳ فرض کنید که کوزه‌های آب با گنجایشهای a و b داریم. آنگاه مقدار آب هر کوزه همیشه مضربی از $gcd(a,b)$ است.

برای مثال، هیچ راهی برای درست کردن گالنی با گنجایش ۴ لیتر با استفاده از ظرف‌های ۳ لیتری و ۶ لیتری وجود ندارد، بدلیل اینکه ۴ مضربی از $gcd(۳,۶) = ۳$ نیست.

۲. ۳ خصوصیات بزرگترین مقسوم‌علیه مشترک

ادعا کردیم که بزرگترین مقسوم‌علیه مشترک ابزاری کارآمد برای بدست آوردن ثنایحی درباره اعداد صحیح هستند. بنابر این، غالباً از برخی حقایق پایه‌ای gcd استفاده خواهیم کرد:

لم ٤. ۳ بیانات زیر دربارهٔ بزرگترین مقسوم‌علیه مشترک صدق می‌کنند:

۱- هر مقسوم‌علیه مشترک a و b مقسوم‌علیه $gcd(a,b)$ است.

۲- (برای تمام $k > ۰$) $gcd(ka,bk) = k.\ gcd(a,b)$.

۳- اگر $gcd(a,c) = ۱$ و $gcd(a,b) = ۱$ آنگاه $gcd(a,bc) = ۱$

٤- اگر $a \mid bc$ و $gcd(a,b) = ۱$ آنگاه $a \mid c$.

۵- $gcd(a,d) = gcd(b, a \ \ rem \ \ b)$.

اینجا ترفند اثبات این بیانات را داریم: لغت gcd را با استفاده از قضیهٔ ۱. ۳ به لغت ترکیب خطی معنی کنید، دربارهٔ ترکیب خطی استدلال کنید، و باز هم با استفاده از قضیهٔ ۱. ۳ آنرا معنی کنید.

برهان. فقط قسمتهای (۳) و (٤) را ثابت می‌کنیم.

برهان (۳): فرض‌های مسأله در کنار هم با قضیهٔ ۱. ۳ دلالت می‌کند که اعداد صحیح s,t,u، و v وجود دارند بطوری که:

$$sa + tb = ۱$$

$$ua + vc = ۱$$

ضرب این دو معادله درهم نتیجه می‌شود:

$$(sa + tb)(ua + vc) = ۱$$

قسمت سمت چپ را می‌توان به صورت $a.(asu + btu + csv) + bc\,(tv)$ بازنویسی کرده این یک ترکیب خطی a و bc است که برابر با ۱ است، بنابر این با قضیهٔ ۱. ۳ داریم $gcd(a,bc) = ۱$

برهان (٤) قضیهٔ ۱. ۳ می‌گوید که $gcd(ac,bc)$ برابر است با ترکیب خطی ac و bc. اینک به طور بدیهی $a|ac$ و با فرض $a|bc$. بنابر این، a بر هر ترکیب خطی ac و bc تقسیم می‌شود. مخصوصاً a بر $gcd(ac,bc)=c.gcd(a,b)=c$ تفسیم می‌شود. اولین تساوی از قسمت (۲) این لم بهره می‌برد، و قسمت دوم از این نکته که $gcd(a,b)=۱$ استفاده می‌کند. □

قسمت (۵) لم برای محاسبهٔ سریع بزرگترین مقسوم‌علیه مشترک دو عدد مفید است. برای مثال، می‌توانیم بزرگترین مقسوم‌علیه مشترک ۱۱۷۴ و ۸۹۹ را با به کارگیری مکرر قسمت (۵) حساب کنیم:

$$gcd(۱۱۴۷,۸۹۹)=gcd\left(۸۹۹,\underbrace{۱۱۴۷\ \ rem\ \ ۸۹۹}_{=۲۴۸}\right)$$

$$=gcd\left(۲۴۸,\underbrace{۸۹۹\ \ rem\ \ ۲۴۸}_{=۱۵۵}\right)$$

$$=gcd\left(۱۵۵,\underbrace{۲۴۸\ \ rem\ \ ۱۵۵}_{=93}\right)$$

$$=gcd\left(۹۳,\underbrace{۱۵۵\ \ rem\ \ ۹۳}_{=۶۲}\right)$$

$$=gcd\left(۶۲,\underbrace{۹۳\ \ rem\ \ ۶۲}_{=۳۱}\right)$$

$$=gcd\left(۳۱,\underbrace{۶۲\ \ rem\ \ ۳۱}_{=۰}\right)$$

$$=gcd(۳۱,۰)$$

$= ۳۱$

این را می‌گویند الگوریتم اقلیدس. شاید آخرین معادله به نظر غلط بیاید، ولی ۳۱ مقسوم‌علیه ۳۱ و ۰ می‌باشد از آن‌جایی که هر عدد صحیحی بر ۰ تقسیم می‌شود.

این محاسبه، به اتفاق قضیهٔ فرعی ۳. ۳ ایجاب می‌کند که هیچ راهی برای اندازه‌گیری ۲ گالن آب با استفاده از ظرف‌هایی با گنجایش ۱۲۴۷ و ۸۹۹ وجود ندارد، فقط می‌توانیم مضرب‌های گالن ۳۱ لیتری را بدست آوریم. این که خبر خوبی است – بروس حتی نمی‌تواند در جان‌سخت ۵ زنده بماند!

بیائید ببینیم که شاید بروس احتمالاً بتواند گالن ۳ لیتری را با استفاده از ظرفهای ۲۱ و ۲۶ لیتری درست کند. ابتدا، بزرگترین مقسوم علیه مشترک ۲۱ و ۲۶ را با استفاده از الگوریتم اقلیدس محاسبه می‌کنیم:

$$gcd(۲۶,۲۱) = gcd(۲۱,۵) = gcd(۵,۱) = ۱$$

حالا ۳ مضربی از ۱ است، بنابر این نمی‌توانیم از این احتمال جلوگیری کنیم که بروس بتواند گالن ۳ لیتری درست کند. از سویی دیگر، نمی‌دانیم هم که او بتواند این کار را انجام دهد.

۳. ۳ یک راه حل برای تمام مسائل کوزه‌های آب

آیا بروس می‌تواند با استفاده از کوزه‌های ۲۶ و ۲۱ لیتری گالن ۳ لیتری را پر کند؟ پاسخ به این پرسش بدون برخی نکات از نظریهٔ اعداد خیلی هم آسان نیست.

قضیهٔفرعی ۲. ۳ می‌گوید که ۳ را می‌توان به صورت ترکیب خطی ۲۱ و ۲۶ نوشت، از آن‌رو که ۳ مضربی از $gcd(۲۱,۲۶)=۱$ است. به سخن دیگر، اعداد صحیح s و t را داریم به طوری که:

$$۳ = s.۲۱ + t.۲۶$$

نمی‌دانیم که ضریب‌های مشترک s و t چیست، ولی می‌دانیم که هستند.

اینک ضریب s هم می‌تواند مثبت و هم منفی باشد. با این همه، می‌توانیم به آسانی این ترکیب خطی را به یک تساوی ترکیب خطی تبدیل کنیم.

$$۳ = s'.۲۱ + t'.۲۶$$

جایی که ضریب s' مثبت است. راه‌حل این است که اگر s را بوسیله ۲۶ در معادلهٔ اصلی افزایش و t را با ۲۱ کاهش دهیم، آنگاه مقدار عبارت $s.۲۱+t.۲۶$ کاملاً ثابت می‌ماند. در این صورت، با افزایش مکرر مقدار s (با ۲۶ در یک زمان) و کاهش مقدار t (با ۲۱ در یک زمان)،می‌توان یک ترکیب خطی $s'.۲۱+t'۲۶=۳$ جایی که ضریب s' مثبت است بدست آورد. یادتان باشد که t' باید منفی باشد؛ در غیر این صورت، این عبارت خیلی بزرگتر از ۳ خواهد شد.

حالا چگونگی تشکیل ۳گالن با استفاده از ظرف‌هایی با گنجایش ۲۱ و ۲۶ را بررسی می‌کنیم:

- s' بار کار را تکرار کنید:
  - ظرف ۲۱ گالنی را پر کنید.

- تمام آب موجود در ظرف با گنجایش ۲۱ را در ظرف با گنجایش ۲۶ بریزید. هرگاه که ظرف ۲۶ پر شد، آن را خالی کنید.

در پایان این روند، باید دقیقاً گنجایش ۳ در ظرف با گنجایش ۲۶ باشد! چرایش چنین است: ما s'.۲۱ گالن آب از چشمه برداشته‌ایم، مضرب‌هایی از ۲۶ را بیرون ریخته‌ایم، و در نهایت ظرف ۲۶ گالنی در جایی بین ۰ و ۲۶ گالن است.از این گذشته، می‌دانیم که:

$$s'.۲۱+t'.۲۶ = ۳$$

با این حساب، بایستی دقیقاً- t' مرتبه ظرف با گنجایش ۲۶ را خالی کرده باشیم، اگر در دفعات کمتری آن را خالی می‌کردیم، آنگاه باید بیش از ۲۶ باقی بماند. و اینکه ما به اندازهٔ کافی آب از چشمه نکشیدیم تا ظرف ۲۶ را t' مرتبه خالی کنیم. بنابر این، با معادلهٔ بالا، بایستی دقیقاً گالنی با گنجایش ۳ بماند.

بطور قابل ملاحظه‌ای حتی برای استفاده از این راه کار نیاز به دانستن ضریب s' و t' نداریم! به جای تکرار s' مرتبه حلقهٔ بیرونی، می‌توانستیم فقط تا اینکه به گالنی با گنجایش ۳ برسیم کار را تکرار کنیم، آنچه که باید سرانجام اتفاق بیفتد. البته، باید ردپای مقادیر باقی‌مانده درون دو کوزه را نگه داریم تا اینکه بدانیم چه موقع این کار را کرده‌ایم. این حلی است که آن روش به دست می‌دهد:

$$
\begin{array}{llllllll}
(0,0) & \xrightarrow{\text{fill 21}} & (21,0) & \xrightarrow{\text{pour 21 into 26}} & (0,21) & & & \\
 & \xrightarrow{\text{fill 21}} & (21,21) & \xrightarrow{\text{pour 21 into 26}} & (16,26) & \xrightarrow{\text{empty 26}} & (16,0) & \xrightarrow{\text{pour 21 into 26}} & (0,16) \\
 & \xrightarrow{\text{fill 21}} & (21,16) & \xrightarrow{\text{pour 21 into 26}} & (11,26) & \xrightarrow{\text{empty 26}} & (11,0) & \xrightarrow{\text{pour 21 into 26}} & (0,11) \\
 & \xrightarrow{\text{fill 21}} & (21,11) & \xrightarrow{\text{pour 21 into 26}} & (6,26) & \xrightarrow{\text{empty 26}} & (6,0) & \xrightarrow{\text{pour 21 into 26}} & (0,6) \\
 & \xrightarrow{\text{fill 21}} & (21,6) & \xrightarrow{\text{pour 21 into 26}} & (1,26) & \xrightarrow{\text{empty 26}} & (1,0) & \xrightarrow{\text{pour 21 into 26}} & (0,1) \\
 & \xrightarrow{\text{fill 21}} & (21,1) & \xrightarrow{\text{pour 21 into 26}} & (0,22) & & & & \\
 & \xrightarrow{\text{fill 21}} & (21,22) & \xrightarrow{\text{pour 21 into 26}} & (17,26) & \xrightarrow{\text{empty 26}} & (17,0) & \xrightarrow{\text{pour 21 into 26}} & (0,17) \\
 & \xrightarrow{\text{fill 21}} & (21,17) & \xrightarrow{\text{pour 21 into 26}} & (12,26) & \xrightarrow{\text{empty 26}} & (12,0) & \xrightarrow{\text{pour 21 into 26}} & (0,12) \\
 & \xrightarrow{\text{fill 21}} & (21,12) & \xrightarrow{\text{pour 21 into 26}} & (7,26) & \xrightarrow{\text{empty 26}} & (7,0) & \xrightarrow{\text{pour 21 into 26}} & (0,7) \\
 & \xrightarrow{\text{fill 21}} & (21,7) & \xrightarrow{\text{pour 21 into 26}} & (2,26) & \xrightarrow{\text{empty 26}} & (2,0) & \xrightarrow{\text{pour 21 into 26}} & (0,2) \\
 & \xrightarrow{\text{fill 21}} & (21,2) & \xrightarrow{\text{pour 21 into 26}} & (0,23) & & & & \\
 & \xrightarrow{\text{fill 21}} & (21,23) & \xrightarrow{\text{pour 21 into 26}} & (18,26) & \xrightarrow{\text{empty 26}} & (18,0) & \xrightarrow{\text{pour 21 into 26}} & (0,18) \\
 & \xrightarrow{\text{fill 21}} & (21,18) & \xrightarrow{\text{pour 21 into 26}} & (13,26) & \xrightarrow{\text{empty 26}} & (13,0) & \xrightarrow{\text{pour 21 into 26}} & (0,13) \\
 & \xrightarrow{\text{fill 21}} & (21,13) & \xrightarrow{\text{pour 21 into 26}} & (8,26) & \xrightarrow{\text{empty 26}} & (8,0) & \xrightarrow{\text{pour 21 into 26}} & (0,8) \\
 & \xrightarrow{\text{fill 21}} & (21,8) & \xrightarrow{\text{pour 21 into 26}} & (3,26) & \xrightarrow{\text{empty 26}} & (3,0) & \xrightarrow{\text{pour 21 into 26}} & (0,3)
\end{array}
$$

صرف‌نظر از گنجایش ظرف‌ها و صرف‌نظر از آن مقداری که در صدد تولید آنیم همان راه حل بـه کار می‌آید. به سادگی شیوه زیر را دنبال کنید:

- تا اینکه مقدار آب مطلوب بدست آید تکرار کنید:
  - ظرف کوچک‌تر را پر کنید.
  - تمام آب موجود در ظرف کوچک‌تر را درون ظرف بزرگتر بریزید. هرگاه ظرف بزرگتر پر شود، آن را خالی کنید.

با استدلالی شبیه به قبل، این روش سرانجام هر مضرب بزرگترین مقسوم‌علیـه مشـترک گنجـایش ظرف‌ها –را که احتمالاً بتوانیم تولید کنیم را بوجود می‌آورد. اصلاً نیازی به هوش سرشار ندارد!

٤. ۳ خردکننده

دیدیم که مهم نیست کدام جفت عدد صحیح a و b را به ما بدهند، همیشه یک جفت ضریب عدد صحیح s و t وجود دارد به طوری که

$$gcd(a,b) = sa + tb$$

علاوه بر این، در زیر بخش پیشین، یک روش گرد کردن تقریبی برای یافتن چنین s و t ارائه کردیم. با این وجود، آن روش خیلی کارآمد نیست. یک راه خیلی بهتر در اینجا هست:

این روش با بهترین طرز ممکن توسط یک ابزار ریاضی که متعلق به قرن ششم هندوستان است انجام می‌شود که آن را کوتاک می‌نامیدند، که معنایش می‌شود "خورد کننده" امروزه بطور عام خورد کننده را الگوریتم بسط داده شدهٔ GCD اقلیدس می‌نامند، ولی اینکه لنگ می‌زند. گیر داده‌ایم به "خوردکننده".

الگوریتم اقلیدس برای یافتن GCD دو عدد بر کاربرد مکرر معادله زیر تکیه می‌کند:

$$gcd(a,d) = gcd(b, a \ \ rem \ \ b)$$

برای مثال می‌توانیم GCD ۲۵۹ و ۷۰ را به شکل زیر محاسبه کنیم:

$$\begin{aligned}
\gcd(259,70) &= \gcd(70,49) && \text{since } 259 \text{ rem } 70 = 49\\
&= \gcd(49,21) && \text{since } 70 \text{ rem } 49 = 21\\
&= \gcd(21,7) && \text{since } 49 \text{ rem } 21 = 7\\
&= \gcd(7,0) && \text{since } 21 \text{ rem } 7 = 0\\
&= 7.
\end{aligned}$$

خورد کننده همان مراحل را دنبال می‌کند، ولی در طول این راه به مقداری دفترداری اضافی نیاز دارد: همان طور که $\gcd(a,b)$ را محاسبه می‌کنیم، راه حل چگونگی نگارش هر یک از باقی‌مانده‌های (۴۹,۲۱,۷ و همانند مثال) را حفظ می‌کنیم به مانند ترکیب خطی a,b (این ارزش صرف وقت را دارد، زیرا هدف ما نوشتن آخرین باقی‌ماندهٔ غیر صفر است، که همان GCD است که یک ترکیب خطی است). برای مثال ما، دفترداری اضافی چنین است:

x	y	$(x \text{ rem } y)$		$x - q \cdot y$
259	70	49	=	$259 - 3 \cdot 70$
70	49	21	=	$70 - 1 \cdot 49$
			=	$70 - 1 \cdot (259 - 3 \cdot 70)$
			=	$-1 \cdot 259 + 4 \cdot 70$
49	21	7	=	$49 - 2 \cdot 21$
			=	$(259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			=	$\boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0		

با مبدأ قراردادن دو متغیر $y=b, x=a$ کارمان را شروع می‌کنیم. در دو ستون اولیهٔ بالا، الگوریتم اقلیدس را اجرا کردیم. در هر مرحله، $x \; rem \; y$ را که می‌توان به صورت $x - q.y$. نوشته شود محاسبه کردیم (به خاطر داشته باشید که الگوریتم تقسیم می‌گوید که $x = q.y + r$، که r باقیمانده است. $r = x - q.y$ را با ترتیب دوبارهٔ عبارت‌ها بدست می‌آوریم.) سپس y, x را در این معادله با ترکیب خطی هم‌ارز b, a جابه‌جا کردیم، که قبلاً محاسبه‌اش کرده بودیم. بعد از ساده کردن، با یک ترکیب خطی b, a که برابر بود با باقی‌ماندهٔ مورد نظر، روبرو شدیم. حل نهایی بدست آمد.

٤. قضیهٔ بنیادین علم حساب

هم اینک تقریباً به اندازهٔ کافی ابزارهایی برای اثبات چیزی که احتمالاً از قبل می‌دانستید را در اختیار داریم.

قضیهٔ (قضیهٔ بنیادین علم حساب.) هر عدد صحیح مثبت n را می‌توان به صورت حاصل‌ضربی از اعداد اول با روشی منحصر به فرد نوشت:

$$n = p_1 \quad p_2 \dots p_j \qquad \left(p_1 \le p_2 \le \dots \le p_j\right)$$

توجه کنید که اگر ۱ به عنوان عدد اول در نظر گرفته شود قضیهٔ اشتباه خواهد بود، برای مثال، ۱۵ را می‌توان به صورت ۳.۵ یا ۱.۳.۵ یا $1^2.3.5$ نوشت. همچنین، بر روی یک قانون استاندارد تکیه می‌کنیم: حاصل‌ضرب یک مجموعه تهی از اعداد، ۱ فرض می‌شود، همان طور که مجموع اعضای یک مجموعه تهی ۰ فرض می‌شود. بدون این قرارداد قضیه برای $n = ۱$ غلط خواهد بود.

شگفتی خاصی در قضیهٔ بنیادین وجود دارد، حتی اگر آن را از قنداق می‌شناختید. اعداد اول به طور نامنظمی در بخش اعداد صحیح به نمایش در می‌آیند. در واقع، توزیع آنها تقریباً اتفاقی به نظر می‌رسد:

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

پرسش اساسی دربارهٔ این بخش به مدت قرن‌ها انسانیت را گیج کرده است و هنوز هم می‌دانیم که هر عدد طبیعی را دقیقاً به یک روش از اعداد اول می‌توان ساخت. این اعداد دمدمی مزاج تکه‌های

ساختمانی برای اعداد صحیح هستند. اثبات قضیهٔ بنیادین سخت نیست، ولی ما به چند حقایق اولیه نیازمندیم.

لم ۱. ٤ اگر p یک عدد اول باشد و $p|ab$، سپس $p|a$ یا $p|b$.

برهان. بزرگترین مقسوم علیه مشترک a و p بایستی که ۱ یا p باشد، از آنرو که فقط این‌ها مقسوم علیه‌های p هستند. اگر $gcd(a,p)=p$، آنگاه قضیه صدق می‌کند، زیرا a مضربی از p است. در غیر این صورت، $gcd(a,p)=۱$ و بنابراین $p|b$ از قسمت (۴) لم ٤. ۳ نتیجه می‌شود □

قضیهٔ اعداد اول

فرض کنید $\pi(x)$ بیانگر اعداد اول کمتر یا مساوی با x باشند. برای مثال، $\pi(۱۰)=۴$ برای اینکه ۷,۵,۳,۲ اعداد اول کمتر یا برابر با ۱۰ هستند. اعداد اول خیلی به طور بی‌قاعده توزیع می‌شوند، بنابراین رشد π چه بسا ناگهانی است. با این وجود، قضیهٔ اعداد اول پاسخ تقریبی ارائه می‌کند:

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\ln x}=۱$$

با این حساب، اعداد اول به تدریج متوقف می‌شوند. به عنوان یک قاعده عملی، حدود ۱ عدد از هر $\ln x$ عدد در مجاورت x یک عدد اول موجود است.

قضیهٔ اعداد اول در سال ۱۷۹۸ توسط لجندار مطرح شد و یک قرن بعد بوسیله دلاواله پوسن وهادامارد در سال ۱۸۹٦ به اثبات رسید. با این وجود، دفترچه‌ای از گاس پس از مرگش پیدا شد که همان طرح در آن بود، که آشکارا نشان می‌دهد در سن ۱۵ سالگی آن را نوشته است (در غیر

این صورت باید برای ریاضی دانان "بزرگ" که مصیبت هم عصر بودن با گاس را داشته‌اند احساس تأسف کنید.)

در اواخر ۲۰۰۴ در سراسر کشور یک تابلو نمایشگر در محل‌های مختلف به ظهور رسید:

$$\left.\begin{array}{l}\text{نخستین عدد اول ۱۰ رقمی}\\ \text{در توالی أعداد } e \text{ پیدا شدند}\end{array}\right\}.com$$

جایگزینی عدد صحیح به جای عبارت درون آکولاد که توسط *URL* برای صفحه کاریابی گوگل ایجاد شده است. نظر بر این بود که گوگل علاقمند بود آن اشخاص را که بتوانند و بخواهند چنین مسئله‌ای را حل کنند به استخدام در بیاورد. مگر این مسئله چقدر سخت است؟ آیا مجبورید که از میان هزاران یا میلیون‌ها یا میلیاردها عدد، عدد اول ۱۰ رقمی را پیدا کنید؟ راه تجربی منشعب از قضیهٔ اعداد اول می‌گوید که در میان اعداد ۱۰ رقمی، حدود ۱ در

$$\ln ۱۰^{۱۰} \approx ۲۳$$

عدد اول وجود است. این اشاره می‌کند به اینکه مسئله براستی خیلی سخت نیست. مطمئناً، نخستین عدد اول در توالی اعداد خیلی زود پیدایشان می‌شود:

$e = ۲.۷۱۸۲۸۱۸۲۸۴۵۹۰۴۵۲۳۵۳۶۰۲۸۷۴۷۱۳۵$ (الی آخر)

یک استدلال استقرائی روتین این عبارت را به واقعیتی که قبلاً فرض کردیم می‌گستراند:

لم ۲. ٤ فرض کنید p یک عدد اول است. اگر $a_۱ ، a_۲ ... a_n$، $p \mid a_۱ a_۲ ... a_n$ آنگاه تعدادی از a_i یا بر p تقسیم می‌شوند.

اینک آماده‌ایم تا قضیهٔ بنیادین علم حساب را ثابت کنیم.

قضیهٔ ۳. ٤ (قضیهٔ بنیادین علم حساب) هر عدد صحیح مثبتی را می‌توان با روشی منحصر به فرد به شکل مضربی از اعداد اول نوشت:

$$n = p_1.p_2 \dots p_j \qquad (p_1 \le \dots \le p_j)$$

برهان. باید دو مورد را ثابت کنیم: (۱) هر عدد صحیح مثبتی را می‌توان به شکل مضربی از اعداد اول بیان نمود و (۲) این عبارتی منحصر به فرد است.

اولاً، از استقراء قوی برای اثبات اینکه هر عدد صحیح مثبتی n مضربی از اعداد اول است استفاده می‌کنیم. به عنوان حالت پایه، $n=1$ مضرب مجموعه تهی اعداد اول است. برای مرحله استقرائی، فرض کنید که هر $k<n$ مضربی از اعداد اول است. باید نشان بدهیم که n هم مضربی از اعداد اول است. اگر خود n عدد اول باشد، پس بطور بدیهی صحیح است. در غیر این صورت، اعداد صحیح کمتر از n، مانند b,a وجود دارد بطوری که $n=ab$. طبق فرض استقراء b,a خود حاصل‌ضرب اعدا اول هستند پس هم مضربی از اعداد اول است. بنابراین، ادعا بوسیله استقراء ثابت می‌شود.

دوماً، از اصل خوش ترتیبی برای اثبات اینکه هر عدد صحیح مثبتی می‌تواند به صورت مضربی از اعداد اول به روشی منحصر به فرد نوشته شود استفاده می‌کنیم. برهان با تناقض انجام می‌شود: فرض کنید، بر خلاف ادعا، که اعداد مثبت صحیحی وجود دارند که می‌توان آن‌ها را به صورت مضربی از اعداد اول با بیش از یک روش نوشت. بوسیله اصل خوش‌ترتیبی، کوچکترین عدد صحیح با این خاصیت وجود دارد. این را عدد صحیح n بنامید و فرض کنید

$$n = p_1 . p_2 \dots p_j$$

$$= q_1 . q_2 \dots q_k$$

دو روشی (احتمالاً بیشتر) برای نوشتن n به عنوان مضربی از اعداد اول باشد. چون $p_1 | n$ بنابراین $p_1 | q_1 \ q_2 \dots q_k$ و لم ۲. ٤ دلالت می‌کند که p_1 یکی از اعداد اول مانند: q را ایجاد می‌کند. ولی از آنجا که q_i یک عدد اول است، باید اینطور باشد که $p_1 = q_i$ با حذف p_1 از مضرب اول و q_i از مضرب دوم، متوجه می‌شویم که $\frac{n}{p_1}$ یک عدد صحیح مثبت کوچکتر از n است که می‌تواند به صورت مضربی از اعداد اول به دو روش مجزا نوشته شود. ولی این با تعریف n به عنوان کوچک‌ترین عدد صحیح مثبت تناقض دارد. □

۵. آلن تورینگ

مردی که در بالا به تصویر کشیده شده آلن تورینگ است، مشهورترین چهره در تاریخ علوم رایانه. به مدت چندین دهه، زندگی حیرت‌آورش بوسیله مخفی کاری دولت در زیر پوشش نگاه داری می‌شد، تابوی اجتماعی، حتی در مورد نیرنگ‌های خودش هم مخفی کاری می‌کرد. در ۲۴سالگی تورینگ مقاله‌ای نوشت با عنوان "پیش به سوی اعداد قابل شمارش، با کاربردی از مسئله انتشایدونگز". معمای مقاله، روشی عالی برای نمونه سازی یک رایانه در اصطلاح ریاضی بود. این یک پیشرفت غیر منتظره علمی بود، چونکه به ابزارهای ریاضیات اجازه داد پرسشهای محاسباتی را به میان آورند. برای مثال، با دردست داشتن نمونه او، تورینگ بلافاصله ثابت کرد که مسائلی وجود دارند که هیچ رایانه‌ای قادر به حل آن نیست – هر قدر که برنامه‌نویس نابغه باشد.

مقاله تورینگ باز هم بیش از اینها قابل ملاحظه است، چونکه آن را در سال ۱۹۳۶ یک دهه کامل قبل از آنکه هیچ کامپیوتری عملاً وجود بیاید، نوشت.

واژه "انتشایدونگز پرابلم" که در عنوان مقاله هست اشاره به یکی از ۲۸ مسئله ایست که توسط دیوید هیلبرت در سال ۱۹۰۰ به عنوان چالشی برای ریاضی‌دانان قرن بیستم مطرح شد. تورینگ در همان مقاله به یکباره دست از کار کشید. و شاید شما هم درباره "پایان نامه کلیسای – تورینگ" شنیده باشید؟ در همان مقاله معروف بنابراین تورینگ آشکارا مردی بارز بود که آشکارا عقاید حیرت‌آور زیادی را مطرح کرد. ولی این صحبت‌ها درباره یکی از عقاید کمتر حیرت‌آور تورینگ است. آن عقیده، درباره رمزها بود. راجع به تئوری اعداد بود. ویک جور حماقت بود.

٦. رمز تورینگ

بیائید به پائیز سال ۱۹۳۷ نگاهی کنیم. آلمان نازی داشت تحت رهبری آدولف هیتلر به پا می‌خاست، جنگ جهانی ویران‌گر قریب‌الوقوع بود و – مثل ما – آلن تورینگ در حال بذرپاشی بی‌فایده نظریه اعداد بود. او پیش‌بینی کرد که نگهداری اسرار نظامی در نبرد پیش رو حیاتی است و روش رمزنویسی ارتباطات را با استفاده از نظریه اعداد پیشنهاد کرد. عقیده‌ای که به زمان خودمان هم کمانه کرده است. امروز، نظریه اعداد پایه بسیاری از دستگاه‌های رمزنگاری- کلید- عمومی، طراحی امضاهای الکتریکی، تابع‌های ریز رمز و دستگاه‌های پول شمار الکتریکی است. هر بار که از انتشارات آمازون کتابی خریداری کنید، صورت مالی خود را در شبکه ***websis*** ببینید، یا از یک حساب پرداخت قسطی استفاده کنید، در آن صورت به الگوریتم‌های نظری اعداد

متکی هستند. وانگهی، بنگاه‌های سرمایه‌گذاری نظامی در اختیار بزرگترین سرمایه گـذارانی اسـت که به دنبال پژوهش در رمز نگاری هستند. هاردی متأسفیم!

خیلی زود پس از باز شدن رمزش، تورینگ از نظر مردم نهان شد و نیم قرن گذشت تا اینکه جهان از داستان کامل کجا رفتن و چه کردن تورینگ با خبر شود. کمی بعد سـری بـه زنـدگی تورینـگ خواهیم زد؛ فعلاً بیائید درباره رمز تورینگ که پشت‌سر گذاشتیم، بررسی کنیم. جزئیات نامعین‌اند، از آنرو که هیچ‌گاه رسماً عقایدش را منتشر نکرد، بنابراین چند تـای احتمـالی را در نظـر خـواهیم گرفت.

۱. ٦ رمز تورینگ (شرح ۰. ۱)

نخستین چالش، ترجمه یک پیام متنی به یک عدد صحیح است تا بتوانیم یک عملیـات ریاضـی را بر آن اجرا کنیم. این مرحله در نظر ندارد تا پیامی را برای خواندن سخت‌تر کند، بنابراین جزئیـات خیلی مهم نیستند. این یک راه است: هر حرف الفباء را با دو عدد جایگزین کنیـد $A=۰۱, B=۰۲$ و $C=۰۳$ و غیره کلیه اعداد را در کنار هم بگذارید تا عددی بسیار بزرگ تشکیل شود. برای مثال، پیام "پیروزی" به این شکل باز گردانده می‌شود

$$\begin{array}{c} \text{“} \quad v \quad i \quad c \quad t \quad o \quad r \quad y \text{”} \\ \rightarrow ۲۲\ ۰۹\ ۰۳\ ۲۰\ ۱۵\ ۱۸\ ۲۵ \end{array}$$

رمز تورینگ نیازمند است که پیام با عدد اول باشد، بنابراین ممکن است نیاز داشته باشیم با اعـداد بیشتری نتیجه را تبدیل کنیم تا عدد اول بدست آوریم، در این حالت، بـا افـزودن اعـداد ۱۳ عـدد ۱۳ ۲۵ ۱۸ ۱۵ ۲۰ ۰۳ ۰۹ ۲۲ بدست می‌آید، که عدد اول است.

حالا بررسی می‌کنیم که روش رمز نگاری چگونه کار می‌کند. در شرح زیر، m پیامی غیر رمزگذاری شده است (که می‌خواهیم راز نگه‌دار باشیم)، m^* پیام رمزگذاری شده است (که ممکن است نازی‌ها آن را دریافت کنند) و k هم کلید مورد نظر است.

پیشاپیش فرستنده و گیرنده بر یک کلید رمز، که یک عدد اول بزرگ k است توافق می‌کنند.

رمزنگاری فرستنده پیام m را با محاسبه رمز می‌کند:

$$m^* = m.k$$

بازگشایی رمز گیرنده پیام m^* را با محاسبه رمزگذاری بازگشایی می‌کند:

$$\frac{m^*}{k} = \frac{m.k}{k} = m$$

برای مثال، فرض کنید که کلید رمز عدد اول ۸۹ ۳۴ ۷۶ ۰۱ ۲۲ $= k$ است و پیام m' "پیروزی" است. آنگاه پیام رمزنگاری شده به شکل زیر است:

$$m^* = m.k$$

$$= ۲۲۰۹۰۳۲۰۱۵۱۸۲۵۱۳۰۲۲۸۰۱۱۷۶۳۴۸۹$$

$$= ۵۰۳۶۹۸۲۵۵۴۹۸۲۰۷۱۸۵۹۴۶۶۷۸۵۷$$

پرسش‌هایی چند درباره رمز تورینگ وجود دارد که طبیعتاً مورد تقاضای برخی قرار می‌گیرند.

۱- چگونه فرستنده و گیرنده می‌توانند مطمئن شوند که m و k، همانطور که باید اعداد اول هستند؟

مسئله کلی تعیین اینکه آیا عددی بزرگ اول است یا مرکب به مدت قرن‌ها مورد مطالعه بوده است و براستی که آزمون‌های اولیه خوبی حتی در زمان تولینگ شناخته شده بودند. در سال ۲۰۰۲ مانیندراآگراوال، یزاج کایال و نیتین ساکسنا اعلام کردند آزمونی اولیه یافتند که برای کار بر روی یک عدد n در حدود $(\log n)^{۱۲}$ مرحله ضمانت دارد. این مسئله سرانجام به طور قطع آزمون اولیه را در گروه مسائل محاسباتی "آسان" قرار داد. در کمال تعجب، (به طور شگفت آوری) شرح الگوریتم غیر مترقبه آنها فقط سی خط بود!

۲- آیا رمز تورینگ ایمنی دارد؟

نیروهای نازی فقط به پیام رمز شده $m^* = m.k$ توجه می‌کنند، بنابر این پوشش مجدد پیام اصلی m نیاز به تجزیه $m*$ دارد. علی‌رغم تلاشهای بسیار، تا کنون هیچ‌گونه الگوریتم تجزیه کار آمدی یافته نشده است. به نظر می‌رسد که اساساً مسئله سختی باشد، به طوری که در روزگاری عبور از مانع علمی غیرممکن نیست. در نتیجه، رمز تورینگ اکتشاف او را در بهره‌وری عملی میسر می‌سازد زیرا که اذعان بر محدودیت توانائی محاسبه داریم. اینچنین m و k فراهم شده، به طور کافی خوب، به نظر می‌رسد که نازی‌ها بخت یارشان نیست!

همه اینها به نظر وعده و وعید می‌آید، ولی در رمز تورینگ ایرادی به سزا وجود دارد.

۲. ٦ شکستن رمز تورینگ

بیائید ببینیم هنگامی که فرستنده پیام دومی را با استفاده از رمز تورینگ و همان کلید فرا می‌فرستد چه اتفاقی می‌افتد این کار دو پیام رمزنگاری شده را به نازی‌ها تحویل می‌دهد:

$$m_1^* = m_1.k \qquad \text{و} \qquad m_2^* = m_2.k$$

بزرگترین مقسوم‌علیه مشترک دو پیام رمزنگاری شده m_1^* و m_2^* کلید رمزی k است.

و همانطور که دیده‌ایم، gcd دو عدد می‌تواند بسیار کارآمدانه محاسبه شود. بنابراین بعد از اینکه دومین پیام ارسال شود، نیروهای نازی می‌توانند کلید رمز را مجدداً بخوانند و هر پیامی را دریافت کنند!

باور کردن اینکه ریاضی‌دان درخشانی مثل تورینگ از چنین مسئله خیره کننده‌ای چشم پوشی کند مشکل است. توضیح ممکن شاید این باشد که در مغزش شیوه‌ای کمی متفاوت داشته است، که یکی هم‌اندیشه روی حساب هم نهشتی بوده است.

۷. حساب هم‌نهشتی

در صفحه ۱ شاهکار خود در نظریه اعداد، رساله علم حساب، گاس مفهوم "هم‌نهشتی" را ارائه کرد. اینک گاس شخص دیگری است که موفق شد تا هر از گاهی به یک نظریه نیم آراسته بپردازد، پس بیائید نگاهی به این یکی کنیم. گاس گفت که a هم‌نهشت b به سنج n است اگر $n \mid (a-b)$. این مسئله به شکل $a \equiv b \pmod{n}$ نوشته می‌شود. برای مثال:

$۲۹ \equiv ۱۵ \pmod{۷}$ زیرا $۷ \mid ۲۹-۱۵$

به طور شهودی، نماد ≡ به نوعی شبیه علامت = است و به سنج ۷ حالتی ویژه را تشریح می‌کند که در آن ۲۹ با ۱۵ برابر است. پس، حتی در صورتی که (به سنج ۷) در بالای سمت راست قرار بگیرد، به هیچ‌وجه مفهوم این نیست که به عدد ۱۵ سهم بیشتری از عدد ۲۹ داده شده است، آن عملاً معنای علامت = را مشخص می‌کند.

در اینجا روشی دیگر برای فکر کردن به هم نهشت‌ها ارائه می‌شود: به سنج هم نهشت به سنج n اعداد صحیح را به n مجموعه افراز می‌کند بطوری که اعداد هم‌نهشت همگی در یک مجموعه باشند. برای مثال، فرض کنید داریم بر روی به سنج ۳ کار می‌کنیم. پس می‌توانیم اعداد صحیح را به ۳ مجموعه مانند زیر افراز کنیم:

$\{\ldots,-۶,-۳,۰,۳,۶,۹,\ldots\}$

$\{\ldots,-۵,-۲,۱,۴,۷,۱۰,\ldots\}$

$\{\ldots,۴,-۱,۲,۵,۸,۱۱,\ldots\}$

حالا اعداد صحیح در یک مجموعه همگی به سنج ۳ هم نهشت هستند. برای مثال، ۶ و ۳ هر دو در مجموعه اول هستند و هم‌نهشت هستند زیرا تفاوت آنها، $9=(-۳)-۶$ مضربی از ۳ است. همینطور هم، ۱۱ و ۵ هر دو در آخرین مجموعه قرار دارند، چونکه $۶-۵=-۱۱$ مضربی از ۳ است. از طرف دیگر، اعداد موجود در مجموعه‌های متفاوت هم‌نهشت نیستند. برای مثال ۹ در مجموعه نخست و ۱۱ در مجموعه آخر قرار دارند و هم‌نهشت نیستند زیرا $۲=۹-۱۱$ مضربی از ۳ نیست. نتیجه این است که وقتی که حساب به سنج n می‌شود فقط n نوع مختلف اعداد وجود دارند که

مورد بررسی‌اند. در این معنا، حساب هم‌نهشتی نوعی ساده‌سازی علم حساب معمولی است و بنابراین ابزار استدلالی کارآمدی است. حقایق سودمند بسیاری درباره هم‌نهشت‌ها وجود دارند، که برخی از آنها در لم زیر فهرست‌بندی شده‌اند. بن‌مایه همه آنها این است که هم‌نهشت‌ها بسیار شبیهه به معادله‌ها کار می‌کنند، هر چند که چندتایی هم استثناء وجود دارند.

لم ۱. ۷ (حقایقی درباره هم‌نهشت‌ها) عبارتهای زیر برای $n \geq ۱$ صدق می‌کنند:

۱- $a \equiv a \pmod{n}$

۲- $a \equiv b \pmod{n}$ نتیجه می‌دهد $b \equiv a \pmod{n}$

۳- $b \equiv a \pmod{n}$ و $c \equiv b \pmod{n}$ نتیجه $c \equiv a \pmod{n}$

٤- $b \equiv a \pmod{n}$ نتیجه می‌دهد $c + b \equiv c + a \pmod{n}$

۵- $b \equiv a \pmod{n}$ نتیجه می‌دهد $bc \equiv ac \pmod{n}$

٦- $b \equiv a \pmod{n}$ و $d \equiv c \pmod{n}$ نتیجه می‌دهد $d + b \equiv c + a \pmod{n}$

۷- $b \equiv a \pmod{n}$ و $d \equiv c \pmod{n}$ نتیجه می‌دهد $db \equiv ca \pmod{n}$

برهان. تنها قسمت‌های ۱ و ۷ را ثابت می‌کنیم، دیگر قسمت‌ها شبیه‌اند. (قسمت ۱) ◦ بر هر عدد صحیحی بخش پذیر است، بنابراین $n \mid (a - a)$ که معنی‌اش $a \equiv a \pmod{n}$ است.

(قسمت ۷) فرض که $a \equiv b \pmod{n}$ نتیجه می‌دهد $ac \equiv bc \pmod{n}$ (قسمت ۵). همین طور هم، قضیهٔ $c \equiv d \pmod{n}$ نتیجه می‌دهد $bc \equiv bd \pmod{n}$ بنابراین $ac \equiv bd \pmod{n}$ (قسمت ۳). □

رابطه‌ای نزدیک میان حساب هم‌نهشت و عمل باقی‌مانده وجود دارد، که دفعه پیش به آن نگاه کردیم. برای روشن کردن این ارتباط، بیائید افراز اعداد صحیح را که توسط هم‌نهشت به سنج ۳ مشخص شده را دوباره مورد بررسی قرار دهیم:

$\{\ldots,-۶,-۳,۰,۳,۶,۹,\ldots\}$

$\{\ldots,-۵,-۲,۱,۴,۷,۱۰,\ldots\}$

$\{\ldots,۴,-۱,۲,۵,۸,۱۱,\ldots\}$

یادتان باشد که دو عدد هم نهشت هستند اگر و فقط اگر در صورتی که تقسیم بر ۳ بشوند باقی‌مانده یکسان را داشته باشند. (توجه کنید که دو عدد در یک مجموعه قرار می‌گیرند که اگر و فقط اگر دارای یک باقی‌مانده باشند وقتی که تقسیم بر ۳ می‌شوند) اعداد موجود در مجموعه اول وقتی که تقسیم بر ۳ می‌شوند باقیمانده صفر ۰ دارند، اعداد مجموعه دوم باقی‌مانده ۱ دارند، و اعداد مجموعه سوم باقی‌مانده ۲ دارند. باز هم بیشتر، توجه کنید که هر عدد در مجموعه‌ای قرار دارد که باقیمانده خودش در آن است. برای مثال، ۱۱ و $۱۱ \ rem ۳ = ۲$ هر دو در یک مجموعه قرار دارند. بیائید همه این نیکی شادمانه را درون یک لم دسته‌بندی کنیم.

لم ۲. ۷ (هم نهشت‌ها و باقی‌مانده‌ها) ادعاهای زیر صادق هستند:

۱. $a \equiv (a \ \ rem \ \ n) (\mathrm{mod}\, n)$

۲. $a \equiv b (\mathrm{mod}\, n)$ اگر و فقط اگر $(a \ \ rem \ \ n) = (b \ \ rem \ \ n)$

برهان. (از قسمت ۲) با الگوریتم تقسیم، جفت‌های منحصر به فردی از اعداد صحیح q_1, r_1, q_2, r_2 وجود دارند بطوری که:

$a = q_1 n + r_1$ (جایی که $0 \le r_1 < n$)

$b = q_2 n + r_2$ (جایی که $0 \le r_2 n$)

در این عبارت‌ها، $(a \ \ rem \ \ n) = r_1$ و $(b \ \ rem \ \ n) = r_2$

تفریق معادله دوم از معادله اول بدست می‌آید:

$$a - b = (q_1 - q_2)n + (r_1 - r_2) \qquad (-n < r_1 - r_2 < n \text{ جایی که})$$

حالا $a \equiv b \pmod n$ اگر و فقط اگر n بر قسمت چپ تقسیم شود که مقدار صحیح است اگر و فقط اگر n بر عبارت سمت راست تقسیم شود، و برقرار است اگر و فقط اگر $r_1 - r_2$ مضربی از n باشد. کرانه‌های فرض در r_1, r_2، بطور مشخص وقتی اتفاق می‌افتد که $r_1 = r_2$ که هم‌ارز است با $(a \ \ rem \ \ n) = (b \ \ rem \ \ n)$. □

۸. رمز تورینگ (شرح ۰. ۲)

در سال ۱۹۴۰ فرانسه به اشغال ارتش هیتلر در آمده بود و انگلستان به تنهایی در اروپای غربی با نازی‌ها مقابله می‌کرد. مقاومت بریتانیا منوط به کمکهایی بود که با روندی ثابت از اقیانوس اطلس شمالی توسط ایالات متحده آمریکا با کشتی‌های ارسالی انجام می‌گرفت.آن کشتیهای ارسالی در یک بازی موش – و گربه با زیر دریایی‌های "قایق U شکل" آلمانی که در اقیانوس اطلس پرسه می‌زدند، درگیر بودند تا کشتی‌های مواد غذایی امداد رسان را غرق کنند و بریتانیا را وادار به

تسلیم کنند. ماحصل این مبارزه بر ترازویی از اطلاعات متکی بود: آیا آلمان‌ها بهتر می‌توانستند محل کشتی‌های ارسالی را تعیین کنند یا متفقین می‌توانستند محل قایق‌های U شکل را تشخیص بدهند یا برعکس؟

آلمان باخت.

ولی یک دلیل انتقادی در آن سوی شکست آلمن تنها در سال ۱۹۷۴ اقامه شد: بریتانیا رمز نیروی دریایی آلمن را شکسته بود، معما. در طی آن همه جنگ، متفقین قادر بودند با گوش دادن به تماس‌های آلمان کمک‌های ارسالی را در پیرامون زیر دریایی‌های آلمانی هدایت کنند. دولت انگلستان تا سال ۱۹۹۶ توضیح نداد که چگونه راز را گشوده است. وقتی که سرانجام تجزیه و تحلیل منتشر شد (بوسیله ایالات متحده) نگارنده کسی نبود مگر آلن تورینگ. او در سال ۱۹۳۹ به یگان رمز شکنی بریتانیا در پارک بلچلی پیوسته بود. آنجا نقشی مرکزی در شکستن رمز معمای آلمن ایفا کرد و از این طریق از افتادن بریتانیا در دست‌های هیتلر پیشگیری نمود.

دولت‌ها همیشه درباره رمزنگاری دهان بسته هستن، ولی با گذشت نیم‌قرن سکوت رسمی درباره نقش تورینگ در شکستن معما و نجات بریتانیا ممکن است به رویدادهای دست و پا گیری بعد از جنگ مربوط باشد.

بیائید تفسیری جانشین رمز تورینگ ارائه کنیم. چه بسا ایده اساسی ما صحیح بوده باشد، (ضرب کردن پیام در کلید) ولی در استفاده قراردادی علم حساب به جای حساب هم‌نهشت به خطا رفته باشیم. شاید منظور تورینگ این‌چنین بوده است:

پیشاپیش فرستنده و گیرنده بر روی یک عدد اول بزرگ P توافق می‌کنند، که شاید همگانی شده باشد. (این‌قدر مطلق کلیه علوم ریاضی ما خواهد بود.) آنها همچنین بر روی یک کلید سری $K \in \{۱,۲...,P-۱\}$ به توافق می‌رسند.

رمزنگاری پیام m در مجموعه $\{۱,۲,...,P-۱\}$ هر عدد صحیحی می‌تواند باشد؛ بویژه، دیگر نیازی نیست که پیام یک عدد اول باشد. فرستنده پیام m را برای ایجاد m^* با محاسبه زیر رمز نگاری می‌کند:

$$m^* = mk \quad rem \quad p$$

بازگشایی

مرحله بازگشایی رمز خود مسئله ایست. چه بسا امیدواریم که مانند همان روش قبل رمز گشایی کنیم:

با تقسیم پیام رمزگذاری شده m^* به کلید k. مشکل این است که m^* وقتی که mk به p تقسیم می‌شود باقی‌ماند دارد. بنابراین تقسیم m^* به k چه بسا حتی عدد صحیح هم به ما ندهد! براین رمز گشایی سخت، می‌توان با درک بهتری از حساب هم‌نهشت عدد اول غلبه کرد.

۱. ۸ وارون ضربی

وارون ضربی یک عدد x عددی دیگر $x^{-۱}$ است به طوری که:

$$x.x^{-۱}=۱$$

به طور کلی، وارون ضربی اعداد حقیقی وجود دارد. برای مثال، وارون ضربی ۳ می‌شود ۱/۳ از آنجا که:

$$۳.\frac{۱}{۳}=۱$$

یگانه استثنایی که هست این است که صفر ۰ معکوس ندارد.

از سوی دیگر، معکوس اعداد صحیح عموماًصحیح نیست. برای مثال، عدد ۷ نمی‌تواند با عدد صحیح دیگری ضرب شود تا ۱ بدست آید.

در کمال شگفتی، وارون ضربی هنگامی که داریم بر روی هم‌نهشت یک عدد اول کار می‌کنیم وجود دارد. برای مثال، اگر داریم روی هم‌نهشت ۵ کار می‌کنیم، ۳ وارون ضربی ۷ است از آنرو که:

$$۷.۳\equiv ۱ \pmod{۵}$$

(همه اعداد هم ارز ۳ هم‌نهشت ۵ همچنین وارون ضربی ۷ هستند؛ برای مثال $۷.۸\equiv ۱ \pmod{۵}$)

یگانه استثنا در اعدادی است که هم‌ارز ۰ در هم‌نهشتی به‌سنج ۵ هستند (یعنی که، مضربی از ۵ هستند) معکوس ندارند، مانند حالتی که ۰ معکوسی در اعداد حقیقی ندارد.

بیائید این را ثابت کنیم .

لم ۱. ۸ اگر p یک عدد اول باشد و k مضربی از p نباشد، آنگاه k وارون ضربی دارد.

برهان. از آنجا که p عدد اول است، فقط دو مقسوم دارد: ۱ و p. و از آنجایی که k مضربی از p نیست، باید داشته باشیم $\gcd(p,k)=۱$. بنابراین، یک ترکیب خطی p و k مساوی با ۱ وجود دارد:

$$sp+tk=۱$$

آرایش مجدد عبارت‌ها بدست می‌دهد:

$$sp=۱-tk$$

با توجه به تعریف قابلیت تقسیم درایم $p\mid(۱-tk)$ و بنابراین $tk\equiv ۱(med\quad p)$ و از اینرو، t وارون ضربی k درتعریف هم‌نهشتی است. □

وارون‌های ضربی کلید رمزگشایی معمای تورینگ هستند. بویژه، می‌توانیم پیام اصلی را با ضرب کردن پیام رمزنگاری شده در معکوس کلید مجدداً بدست آوریم:

$$\begin{aligned} m*.k^{-۱} &\equiv (mk \quad rem \quad p).k^{-۱}(\bmod \quad p) \\ &\equiv mkk^{-۱}(\bmod p) \\ &\equiv m(\bmod p) \end{aligned}$$

این نشان می‌دهد که $m*k^{-۱}$ هم‌ارز پیام اصلی m است. از آنجا که m در حوزه $۰,۱,\ldots,p-۱$ قرار داشت، می‌توانیم آن را دقیقاً با گرفتن باقی‌مانده مجدداً پوشش دهیم:

$$m=m*k^{-۱} \quad rem \quad p$$

بنابراین حالا می‌توانیم رمزگشایی کنیم.

۲. ۸ حذف

جهتی دیگر که در آن اعداد حقیقی مناسب‌اند این است که هر کسی می‌تواند عامل ضرب یکسان را حذف کند. به سخن دیگر، اگر بدانیم که $m_۱k = m_۲k$، پس می‌توانیم kها را حذف کنیم و نتیجه بگیریم که $m_۱ = m_۲$ وقتی که شده $k \neq ۰$. در کل، حذف در حساب هم‌نهشت معتبر نیست. برای مثال، این هم‌ارزی صحیح است:

$$۲.۳ \equiv ۴.۳ \pmod ۶$$

ولی اگر ارقام را حذف کنیم ، به نتیجه ای غلط می رسیم :

$$۲ \equiv ۴ \pmod ۶$$

این حقیقت که عبارت‌های ضربی نمی‌توانند حذف شوند معنادارترین تفاوت در معادلات هم‌ارزی از معادلات معمولی است. با این وجود، این فرق در صورتی که ما روی یک عدد اول هم‌نهشت کار کنیم زایل می‌شود، و حذف معتبر است.

لم ۲. ۸ فرض کنید p یک عدد اول است و k مضربی از p نیست. آنگاه از $ak \equiv bk \pmod p$ نتیجه می‌گیریم $a \equiv b \pmod p$

برهان. هر دو طرف هم ارز را به $k^{-۱}$ ضرب کنید . □

می‌توانیم از این لم استفاده کنیم تا قدری بیشتر به فراست عملکرد رمز تورینگ پی ببریم. بطور خاص، عملیات رمزنگاری در معمای تورینگ فضای پیام را پس و پیش می‌کند. این موضوع در قضیه فرعی زیر مشخص‌تر بیان می‌شود.

قضیه فرعی ۳. ۸ فرض کنید p عدد اول است و k مضربی از p نیست. آنگاه نتیجه می‌گیریم که دنباله

$$(۰.k) \ rem \ p, \quad (۱.k) \ rem \ p, \quad (۲.k) \ rem \ p, \ldots, (p-۱).k \ rem \ p$$

جایگشتی از دنباله زیر است:

$$۰,۱,۲,\ldots,(p-۱)$$

اگر عبارت اول از هر قسمت حذف شود باز هم صحیح می‌ماند.

برهان. قسمت اول حاوی p عدد است، که همگی در بین ۰ تا $(p-۱)$ با تعریف باقی‌مانده قرار دارند. افزون بر آن، اعداد موجود در قسمت اول متفاوت هستند؛ زیرا از لم ۲. ۸ داریم $ik = JK \pmod p$ اگر و فقط اگر $i \equiv j \pmod p$ و هیچ دو عدد متفاوت در بین $۰,۱,۲,\ldots,p-۱$ به سنج p هم‌ارز نیستند. بنابراین، قسمت اول باید حاوی تمام اعداد از ۰ تا $p-۱$ در یک ردیف باشد. ادعا صحیح است اگر عبارت‌های اول حذف شوند، زیرا هر دو قسمت با ۰ شروع می‌شوند.

□

برای مثال، فرض کنید $p = ۵, k = ۳$ است . پس نتیجه می‌گیریم:

$$\underbrace{(۰,۳)rem\ \ ۵}_{=۰},\ \underbrace{(۱,۳)rem\ \ ۵}_{=۳},\ \underbrace{(۲.۳)rem\ \ ۵}_{=۱},\ \underbrace{(۳.۳)rem\ \ ۵}_{=۴},\ \underbrace{(۴.۳)rem\ \ ۵}_{=۲}$$

جایگشتی از ۰,۱,۲,۳,۴ است و چهار عبارت پایانی جایگشتی از ۱,۲,۳,۴ است. مادامی که نیروهای نازی از کلید رمز k بی‌خبر باشند، نمی‌دانند فضای خالی پیام چگونه با روند رمزنگاری پس و پیش شده و بر این اساس نمی‌توانند پیام‌های رمزگذاری شده را بخوانند.

۳. ۸ قضیهٔ فرما

یک چالش باقی‌مانده در کاربرد رمز تورینگ این است که رمزگشایی نیاز به وارون کردن کلید رمز k دارد. ولی چگونه می‌توانیم معکوس k را بدست آوریم؟ یک راه آن تکیه بر قضیهٔ فرما است، که بسیار مشهورتر از آخرین قضیهٔ– و سودمندتر است.

قضیهٔ ٤. ۸ (قضیهٔ فرما) فرض کنید p عددی صحیح است و k مضربی از p نیست.

آنگاه:

$$k^{p-۱} \equiv ۱ \pmod{p}$$

برهان. به شکل زیر دلیل می آوریم :

$$۱.۲.۳\ldots(p-۱) \equiv (k \ \ rem \ \ p).(۲k \ \ rem \ \ p)\ldots((p-۱)k \ \ rem \ \ p) \pmod{p}$$

$$\equiv k.۲k.۳k\ldots(p-۱)k \pmod{p}$$

$$\equiv (p-۱)! \ .k^{p-۱} \pmod{p}$$

عبارت‌های خط اول با توجه به قضیه فرعی ۳. ۸ عملاً با هم برابرند، بنابراین آنها مطمئناً به سنج p هم‌نهشت هستند. مرحله دوم از قسمت ۱ لم ۲. ۷ استفاده می‌کند. در مرحله سوم، مجدداً عبارت‌ها را در مرتب می‌کنیم.

حالا ! $(p-۱)$ نمی‌تواند مضربی از p باشد، زیرا عوامل عدد $(p-۱)$.....۱.۲ فقط حاوی اعداد اول کوچکتر از p است. بنابراین، می‌توانیم! $(p-۱)$ را از عبارت اول و آخر با استفاده از لم ۲. ۸ که ادعا را ثابت می‌کند، حذف کنیم! □

در اینجا چگونگی یافت معکوس با استفاده از قضیهٔ فرما بیان می‌شود. فرض کنید p یک عدد اول است و k مضربی از p نیست، پس، با توجه به قضیهٔ فرما، می‌دانیم که:

$$k^{p-۲}.k \equiv ۱ (\bmod p)$$

بنابراین $k^{p-۲}$ باید وارون ضربی k باشد. برای مثال، فرض کنید می‌خواهیم وارون ضربی ۶، به سنج ۱۷ را بدست آوریم. پس نیاز به محاسبه $۶^{۱۵} \; rem \; ۱۷$ داریم، که با توان رساندن متوال می‌توانیم آن را انجام دهیم. تمام هم‌ارزهای زیر به سنج ۱۷ صادق هستند.

$$۶^۲ \equiv ۳۶ \equiv ۲$$

$$۶^۴ \equiv \left(۶^۲\right)^۲ \equiv ۲^۲ \equiv ۴$$

$$۶^۸ \equiv \left(۶^۴\right)^۲ \equiv ۴^۲ \equiv ۱۶$$

$$۶^{۱۵} \equiv ۶^۸.۶^۴.۶^۲.۶ \equiv ۱۶.۴.۲.۶ \equiv ۳$$

بنابراین، $۶^{۱۵} \; rem \; ۱۷ = ۳$ به قدر کافی قاطع، ۳ وارون ضربی ۶ به سنج ۱۷ است، از آنجا که:

$$۳.۶ \equiv ۱ \pmod{۱۷}$$

در کل، اگر داشتیم بر به سنج یک عدد اول p کار می‌کردیم، برای یافتن یک وارون ضربی باید هر مقدار میان ۱ و $p-۱$ را امتحان می‌کردیم.با این وجود، راه حل بالا فقط نیاز به $\log$عملیات نیاز دارد، که بسیار بهتر است وقتی که p بزرگ باشد.

٤. ٨ شکستن دوباره رمز تورینگ

گزارش‌های هواشناسی آلمان با دستگاه رمزنویسی با امنیت نه چندان بالا با نام آنیگما رمزگذاری شده بودند. به هر ترتیب، خب که چی اگر متفقین می‌فهمیدند در ساحل جنوبی ایسلند باران می‌بارید؟

ولی، در کمال شگفتی، این مسئله برای نیروهای بریتانیا در نبرد دریایی آتلانتیک سال ۱۹۴۱ موقعیتی بحرانی پدید آورد.

مسئله این بود که برخی از آن گزارش‌های هواشناسی در اصل از طرف قایق‌های U شکل از اقیانوس اطلس پخش شده بودند. از اینرو، بریتانیائی‌ها هر دو گزارشهای رمزگذاری نشده و گزارش‌های رمزنگاری شده را در اختیار گرفتند. با مقایسه هر دو، انگلیسی‌ها قادر بودند تشخیص بدهند آن روز آلمانی‌ها از کدام کلید استفاده می‌کنند و می‌توانستند دیگر معمای رمزنگاری شده رفت و آمد را بخوانند. که امروزه، **دانستن- متن‌صاف** نامیده می‌شود.

بیائید ببینیم دانستن– متن صاف چطور علیه رمز تورینگ کار می‌کند. فرض کنید نیروهای نازی هر دوی m و m^* را می‌شناسند در جایی که:

$$m^* \equiv mk \pmod{p}$$

حالا می‌توانند محاسبه کنند:

$$m^{p-2}.m^* \equiv m^{p-2}.(mk \quad rem\ p) \Leftarrow (\bmod p)(m^* \quad \text{تعریف})$$

$$\equiv m^{p-2}.mk \pmod{p} \qquad (\text{قسمت ۲ از لم ۲. ۷})$$

$$\equiv m^{p-1}.k \pmod{p} \qquad (\text{ساده کردن})$$

$$\equiv k \pmod{p} \qquad (\text{قضیهٔ فرما})$$

حالا نیروهای نازی کلید رمز را دارند و می‌توانند هر پیامی رمز گشایی کنند!

این یک آسیب پذیری هنگفت است، بنابراین رمز تورینگ هیچ ارزش عملی ندارد. خوشبختانه، پس از این که تورینگ در رمزنگاری بهتر شد؛ عملیات رمزگشایی بعدی‌اش در معما مطمئناً جان هزاران نفر را نجات داد، اگر نگوئیم تمام بریتانیا را.

۹. ضمیر نویسی تورینگ

چند سال پس از جنگ، خانه تورینگ مورد دستبرد قرار گرفت. کارآگاهان به زودی فهمیدند که یک همجنس‌باز قدیمی دوستدار تورینگ در سرقت دست داشته است. پس دستگیرش کردند؛ یعنی که، آلن تورینگ را بازداشت کردند. برای اینکه، در آن زمان، همجنس‌گرایی در بریتانیا جرم بود، که تا دو سال مجازات زندان داشت. تورینگ به "مداوای" خفت بار هورمونی به خاطر همجنس‌گرایی‌اش محکوم شد: استروژن به او تزریق شد. شروع کرد به پستان در آوردن.

سه سال بعد، آلن تورینگ، مؤسس علوم رایانه جان سپرد. مادرش در زندگی‌نامه پسر خودش توضیح داد که چه اتفاقی افتاد. بر خلاف هشدارهای مکرر مادر، تورینگ در خانه آزمایش‌های انجام می‌داد. ظاهراً بدترین ترس مادر به حقیقت پیوست: در حالی که سیب می‌خورد و با پوتاسیوم سیانید کار می‌کرد، خودش را مسموم کرد.

با این همه، تورینگ تا مدت‌های مدید یک معما باقی‌ماند. مادرش زن متدین پابندی بود که خودکشی را گناه می‌دانست و دیگر زندگی‌نامه نویسان اشاره کرده‌اند که تورینگ از قبل در این باره بحث کرده بود که با خوردن یک سیب مسموم خودکشی می‌کند.

پر آشکار، آلن تورینگ که علوم رایانه را پایه ریزی کرد و کشورش را نجات داد، در پایان زندگی را از خود سلب کرد، و آن هم با روشی که مادرش بر این باور بود که یک حادثه رخ داده است.

۱۰. علم حساب با یک سنج اختیاری

آن‌طور که تورینگ امیدوار بود رمزش مؤثر واقع نشد. با این حال، عقیده اساسی‌اش – استفاده از نظریه اعداد به عنوان پایه‌های رمزنگاری – در دهه‌های پس از مرگش بطور دیدنی بالا گرفت.

سال ۱۹۷۷ در *MIT* رونالدریوست، آدی شامیر و لئونارد آدلمن یک دستگاه رمزنگار موسوم به *RSA* با امنیت بالا که مبنی بر نظریه اعداد بود را پیشنهاد کردند. علی‌رغم گذشت دهه‌ها از ارائه آن، هیچ نقص معناداری در آن یافت نشده است. افزون بر آن *RSA* مزیتی بزرگ از مرزهای سنتی داراست: فرستند و گیرنده پیام رمزنگاری شده نیاز ندارند که قبلاً با هم دیدار کنند تا بر سر یک کلید رمز به توافق برسند. باز هم بیشتر، گیرنده هر دوی کلید رمز که نزدیک به خود نگهش

می‌دارد و کلید عمومی که تا جایی که بتواند آن را پخش می‌کند. برای فرستادن پیامی به او هر کسی از کلید عمومی توزیع شده استفاده می‌کند. سپس او با کلید محفوظ خصوصی‌اش پیام را رمزگشایی می‌کند. استفاده از چنین کلید رمزنگاری عمومی به شما و آمازون اجاره می‌دهد، برای مثال، در یک کارامنیتی بدون نیاز به ملاقات در کوچه‌ای تاریک برای رد و بدل کردن یک کلید متعهد شوید.

به طور جالب توجهی، RSA به سنج یک عدد اول را همانطور که طرح تورینگ باید داشته باشد، اجرا نمی‌کند، ولی بیشتر سنج حاصل‌ضرب دو عدد اول بزرگ را دارد. با این حساب، نیاز به کمی دانستن درباره اینکه علم حساب چگونه یک سنج را تبدیل به عدد مرکب می‌کند داریم تا RSA را بفهمیم. حساب به سنج اختیاری یک عدد صحیح مثبت در عمل فقط کمی پر زحمت‌تر از تبدیل به سنج یک عدد اول است، در همان مفهومی که دکتر می‌گوید "این فقط می‌خواهد کمی صدمه بزند" قبل از اینکه سوزن بزرگی را در بازویتان فرو کند.

۱. ۱۰ نسبت به هم‌اول بودن و فی

ابتدا به تعریفی تازه نیازمندیم. اعداد صحیح a و b را نسبت به هم‌اول گویند اگر $\gcd(a,b)=۱$ برای مثال ۸ و ۱۵ نسبت به هم‌اول هستند، از آنرو که $\gcd(a,b)=۱$ یادتان باشد که هر عدد صحیح در مواجهه با یک عدد اول p اولی است، مگر مضربی از p باشد.

همچنین به تابعی مطمئن نیاز داریم تا با استفاده از اول بودن نسبی تعریف شود. فرض کنید n یک عدد مثبت صحیح است. آنگاه $\varnothing(n)$ مقدار اعداد صحیح در مجموعه $\{1,2,\ldots,n-1\}$ را که نسبت به n اول هستند را مشخص می‌کند.

فرضیه ریمان

آخرین پروژه تورینگ پیش از آنکه در ۱۹۳۹ از دید همگان پنهان شود شامل ساختن یک اختراع بدقت طراحی شده مکانیکی برای آزمودن طرح‌های ریاضی به نام نظریه ریمان بود. طرح اولیه ابتدا در سال ۱۸۵۹ در مقاله‌ای سر دستی توسط برهارد ریمان حاضر شد و اینک یکی از مشهورترین مسائل حل نشده ریاضی است. فورمول برای میزان یک سری هندسه‌های نا متناهی مقرر می‌دارد:

$$1+x+x^2+x^3+\ldots=\frac{1}{1-x}$$

جایگزینی $x=\frac{1}{5^s}, x\frac{1}{3^s}, x=\frac{1}{2^s}$ و به همین ترتیب برای هر عدد اول حاصلی از معادلات به دست می‌دهد:

$$1+\frac{1}{2^s}+\frac{1}{2^{2s}}+\frac{1}{2^{3s}}+\ldots=\frac{1}{1-1/2^s}$$

$$1+\frac{1}{3^s}+\frac{1}{3^{2s}}+\frac{1}{3^{3s}}+\ldots=\frac{1}{1-1/3^s}$$

$$1+\frac{1}{5^s}+\frac{1}{5^{2s}}+\frac{1}{5^{3s}}+\ldots=\frac{1}{1-1/5^s}$$

با ضرب کردن تمام قسمتهای چپ به همه قسمتهای چپ بدست می‌آید:

$$\sum_{n=1}^{x} \frac{1}{n^s} = \prod_{p \in \text{اعداد اول}} \left(\frac{1}{1 - 1/p^s} \right)$$

حاصل‌جمع سمت چپ از ضرب کردن تمام سری‌های نامتناهی بدست می‌آید ونیز با بکار بستن تئوری بنیادین علم حساب. برای مثال با عبارت $1/300^s$ در حاصل‌جمع، از ضرب کردن $1/2^{2s}$ معادله اول در $1/3^s$ در معادله دوم و $1/5^{2s}$ در معادله سوم بدست آمده است. ریمان توجه کرد هر عدد اولی در عبارت سمت راست ظاهر می‌شود.

بنابراین پیشنهاد کرد با مطالعه معادل درباره اعداد اول آموزش ببینند، ولی سمت چپ عبارت ساده است. به ویژه s را به عنوان عددی مختلط در نظر گرفت و سمت چپ را به شکل یک تابع $\zeta(s)$ ریمان در نظر گرفت. ریمان فهمید که توزیع اعداد اول مرتبط به مقادیر s است که $\zeta(s) = 0$ و که به حدس مشهور او می‌انجامد:

حدس ریمان: هر صفر (تهی) غیر بدیهی تابع زتا $\zeta(s)$ بر خط $s = 1/2 + ci$ در مجموعه مسطح قرار دارد.

پژوهش‌گران برای اثبات این حدس به شدت به کار مشغولند، و در طول یک قرن این کار را انجام داده‌اند. بلافاصله با ارائه برهان ، افزون بر چیزهای دیگر، شکلی نیرومند از قضیهٔ اعداد اول– مبلغ یک میلیون دلار جایزه بگیرند! (حتم نداریم که مبلغ برای مثال نقض چقدر خواهد بود، ولی آن کاشف به صورت گسترده‌ای مورد تشویق ریاضی‌دانان در همه جا قرار خواهد گرفت.)

برای مثال، $\varnothing(۷)=۶$ از آنرو که ۱,۲,۳,۴,۵ و ۶ نسبت با ۷ اول هستند همین طور هم $\varnothing(۱۲)=۴$ از آنرو که ۱,۵,۷ و ۱۱ نسبت به ۱۲ اول هستند. اگر از عوامل اول n آگاه باشید، آنگاه محاسبه $\varnothing(n)$ تکه‌ای از کیک است، با سپاس از قضیهٔ زیر.

قضیهٔ ۱. ۱۰ تابع $\varnothing$ از روابط دو جانبه زیر تبعیت می‌کند:

۱- اگر a و b، نسبت به هم اول باشند، آنگاه $\varnothing(ab)=\varnothing(a)\varnothing(b)$

۲- اگر p یک عدد اول باشد، آنگاه $\varnothing(p^k)=p^k-p^{k-۱}$ $k\geq ۱$.

قضیهٔ هولناک سختی نیست، ولی برای چند هفته به این برهان متکی خواهیم شد. در عین حال، در اینجا مثالی برای چگونگی استفاده از قضیهٔ ۱. ۱۰ برای محاسبه $\varnothing(۳۰۰)$ ارائه می‌شود:

$$\begin{aligned}\varnothing(۳۰۰)&=\varnothing(۲^۲.۳.۵^۲)\\&=\varnothing(۲^۲).\varnothing(۳).\varnothing(۵^۲)\\&=(۲^۲-۲^۱)(۳^۱-۳^۰)(۵^۲-۵^۱)\\&=۸۰\end{aligned}$$

در مرحله اول عوامل ۳۰۰ را پیدا می‌کنیم، از قسمت (۱) قضیهٔ ۱. ۱۰ دو مرتبه در مرحله دوم استفاده کنید، در مرحله سوم، از قسمت (۲) استفاده کنید و بعد ساده کنید.

۲. ۱۰ تعمیم از سنج اختیاری

بیائید آنچه را دوباره حساب به سنج عدد اول می‌دانیم، تعمیم بدهیم. اینک به جای کارکردن بر به

سنج یک عدد اول p، روی سنج یک عدد صحیح مثبت اختیاری n کارخواهیم کرد موضوع اساسی این است که حساب به سنج n چه بسا پیچیده باشد، ولی اعداد صحیح نسبت به n اول انصافاً خوش– رفتار می‌مانند. برای مثال، اگر k نسبت به n اول باشد، آنگاه k به سنج n وارون ضربی را داراست:

لم ۲. ۱۰ فرضاً که n عدد صحیح مثبت باشد. اگر k نسبت به n اول باشد، آنگاه یک عدد صحیح k^{-1} وجود دارد به طوری که:

$$k.k^{-1} \equiv 1 \pmod{n}$$

به عنوان نتیجه‌ای بر این لم، می‌توانیم یک عبارت ضرب را از هر دو طرف یک معادله هم‌ارزی حذف کنیم اگر آن عبارت نسبت به n اول باشد:

قضیه فرعی ۳. ۱۰ فرض کنید n عدد صحیح مثبت و k نسبت به n عدد اول باشد. اگر

$$ak \equiv bk \pmod{n}$$

آنگاه

$$a \equiv b \pmod{n}$$

این قضیه صادق است زیرا می‌توانیم هر دو طرف معادله هم‌ارزی اول را به k^{-1} ضرب کنیم و برای بدست آوردن هم‌ارزی دوم ساده می‌کنیم.

۳. ۱۰ قضیه اویلر

RSA در اساس متکی به قضیه اویلر است، تعمیم قضیهٔ فرما به یک سنج اختیاری.

برهان بسیار شبیه به برهان قضیهٔ فرما است، بجز آن که بر اعداد صحیح نسبت به n اول متمرکز می‌شویم. بیائید با یک لم شروع کنیم.

لم ٤. ۱۰ فرض کنید n یک عدد صحیح مثبت است و k نسبت به n عدد اول باشد. در نظر بگیرید که $k_1,\ldots,k_r$ تمام اعداد صحیح نسبت به n را در بُرد $0 \le k_i \le n$ در بر بگیرد.

سپس دنباله:

$$(k_1.k)\ rem\, n, (k_2.k)\ rem\, n, (k_3.k)\ rem\, n, \ldots, (k_r.k)\ rem\, n$$

یک جایگشت از دنباله زیر است:

$$k_1, k_2, \ldots, k_r$$

برهان. نشان خواهیم داد که اعداد دنباله اول همگی مجزا هستند و همگی در دنباله دوم ظاهر می‌شوند. از آنجا که هر دو دنباله یک طول دارند، اولی باید جایگشتی از دومی باشد.

ابتدا، نشان می‌دهیم که اعداد موجود در دنباله اول همگی مجزا هستند. فرض کنید که $k_i k\ rem\, n \equiv k_j k\ rem\, n$. این معادل است با $k_i k \equiv k_j k (\mathrm{mod}\, n)$، که از قضیه فرعی ۳. ۱۰ نتیجه می‌دهد $k_i \equiv k_j (\mathrm{mod}\, n)$ که معنی‌اش این است که $k_i = k_j$ زیرا که هر دو میان ۱ و $n-1$ قرار دارند. بنابراین، یک عبارت در دنباله اول فقط با خودش برابر است.

بعداً، نشان می‌دهیم که هر عدد در دنباله اول در دنباله دوم ظاهر می‌شود. با فرض، $\gcd(k_i, n) = 1$ و $\gcd(k, n) = 1$ داریم

$$\gcd(k_i, k, n) = \gcd(k_i k \operatorname{rem} n) = ۱$$

از قسمت (٤) لم ٤. ۳. داریم، $k_i k \operatorname{rem} n$ نسبت به n اول هستند و در برد ۰ تا $n-۱$ می‌مانند. دنباله دوم از تشکیل تمام اعداد صحیح اینچنین معین می‌شود. □

می‌توانیم قضیهٔ اویلر را ثابت کنیم:

قضیهٔ ۵. ۱۰ (قضیه اویلر). فرض کنید n عدد صحیح مثبت است و k نسبت به n اول باشد آنگاه:

$$k^{\varnothing(n)} \equiv ۱ (\bmod n)$$

برهان. فرض کنید $k_۱,\ldots,k_r$ همه اعداد صحیح نسبت به n اول باشد به طوری که $۰ \le k_i \le n$. سپس با توجه به تعریف تابع $\varnothing$ $r = \varnothing(n)$. حالا به شکل زیر می‌توانیم استدلال کنیم:

$$k_۱.k_۲.k_۳ \ldots k_r$$

$$\equiv (k_۱.k \operatorname{rem} n).(k_۲.k \operatorname{rem} n).(k_۳.k \operatorname{rem} n)\ldots(k_r.k \operatorname{rem} n) (\bmod n)$$

$$\equiv (k_۱.k).(k_۲.k).(k_۳.k)\ldots(k_r.k) (\bmod n)$$

$$\equiv (k_۱.k_۲.k_۳ \ldots k_r).k^r \pmod p$$

دو گزاره اول عملاً با توجه به لم ٤. ۱۰ برابرند؛ بنابراین آنها مطمئناً همنهشت به سنج n هستند. مرحله دوم از خاصیت به سنج و باقی‌مانده که پیش از این ثابت کردیم استفاده می‌کند. در مرحله سوم، مجدداً عبارت‌ها را مرتب کرده‌ایم.

از قسمت (۳) لم ٤. ۳ می‌دانیم که $k_1.k_2.k_3\ldots,k_r$ نسبت به n اول است. بنابراین، می‌توانیم این عبارت را از گزاره اول و آخر با توجه به لم ۳. ۱۰ حذف کنیم. این کار قضیه را ثابت می‌کند.

□

می‌توانیم با استفاده از قضیهٔ اویلر همان طور که با قضیهٔ فرما این کار را کردیم وارون ضربی را پیدا کنیم اگر k نسبتاً به n اول باشد، پس $k^{\varnothing(n)-1}$ وارون ضربی k به سنج n است. با این وجود، این راه حل نیاز به محاسبه $\varnothing(n)$ دارد.

بهترین روش ما برای انجام چنین کاری نیاز به عوامل n دارد، که در کل می‌تواند کاملاً مشکل باشد. خوشبختانه، وقتی که بدانیم چطور عوامل را پیدا کنیم، به طور مؤثر می‌توانیم از قضیهٔ ۱. ۱۰ برای محاسبه $\varnothing(n)$ استفاده کنیم!

٤. ۱۰ *RSA*

بالاخره، آماده‌ایم ببینیم طرح اولیه رمزنگاری کلید همگانی *RSA* چگونه کار می‌کند:

کلید عمومی رمزنگاری *RSA*

پیشاپیش گیرنده یک کلید همگانی و یک کلید رمز به شکل زیر بوجود می آورد .

۱- دو عدد اول مجزا ایجاد کنید p و q،

۲- فرض کنید $n = pq$،

۳- یک عدد صحیح e را انتخاب کنید به طوری که $\gcd(e,(p-1)(q-1))=1$.کلید همگانی عبارت است از (e,n) این باید بطور گسترده‌ای توزیع شود.

٤- d را محاسبه کنید به طوری که $de \equiv ١ \pmod{(p-١)(q-١)}$ کلید رمزی عبارت است از جفت (e,n). این موضوع باید مخفی بماند!

رمزنگار فرستنده پیام m را برای تولید m' با استفاده از کلید همگانی رمزگزاری می‌کند:

$$m' = m^e \ rem \ n$$

رمز گشایی گیرنده پیام m' را به پیام m با استفاده از کلید رمزی رمزگشایی می‌کند:

$$m = (m')^d \ rem \ n.$$

سر کلاس توضیح خواهیم داد که چرا این روش رمزگشایی مؤثر است!