نظریهٔ اعداد و کامپیوتر

● ترجمهٔ: غلامرضا یاسی پور و سید حسین سیدموسوی

نظریهٔ اعداد موضوعی است که توجه بشر را برای هزاران سال به خود جلب کرده‌است. در این مقاله بررسی مختصری از نظریهٔ اعداد، باتشریح اینکه چرا این موضوع مجذوب کننده و مهم است به دست می‌دهیم.

نظریهٔ اعداد، در کلی‌ترین مفهوم خود، مطالعهٔ اعداد و خواص آنهاست. در این نظریه، ابتداءً به اعداد صحیح، ۰، ۱ ± ، ۲ ± ،... پرداخته می‌شود، و خواص جالب بسیاری از این اعداد و روابط بین آنها مورد بحث قرارمی‌گیرد. در این مقاله، موارد استعمال نظریهٔ اعداد، به‌خصوص آنها راکه متوجه دانش کامپیوترند، بررسی می‌کنیم. گسترش دانش و تکنولوژی جدید به گسترش روشهای باکفایت در ارائهٔ اعداد صحیح و حساب اعداد صحیح ورزیدن وابسته است. از ۵۰۰۰ سال پیش به این طرف، روشهای متفاوتی، با به کار گرفتن اعداد صحیح مختلفی به‌عنوان مبنا، در نمایش اعداد صحیح مطرح شده‌است. بابلیهای باستان ۶۰ را به‌عنوان مبنای دستگاه عددیشان به کار برده‌اند، و مایائیهای باستان ۲۰ را. روش مرسوم ما در بیان اعداد، یعنی، دستگاه اعشاری به کار برندهٔ ۱۰ به‌عنوان مبنا، ابتدا در هندوستان و در حدود شش قرن پیش مطرح شد. امروزه، دستگاه دوتایی، که ۲ را به‌عنوان مبنا اختیار می‌کند، به طرز وسیعی در ماشینهای محاسب به‌کار رفته‌است.

هنگامی که طریقی در ارائهٔ اعداد صحیح مطرح می‌شود، به روشهایی برای حساب ورزیدن، بااستفاده از این نمایشها، نیاز است. در واقع عبارت **آلگوریتم**[1] که امروزه به هر روش مربوط به حل کردن یک مسألهٔ کلی اشاره دارد، در اصل و به طور خاص به چنین روشهایی اشاره داشته‌است. طرح روشهای کارا برای حساب، از هنگامی که کامپیوترها به طور افزایش یابنده‌ای با اعداد بزرگتر سروکار پیدا کرده‌اند، از اهمیت بسیار زیادی برخوردار شده‌است. نظریهٔ اعداد به طرق بسیار در طرح آلگوریتمهای کارا برای حساب کامپیوتری کارا به‌کار رفته است. و در این زمینه، نتایج اساسی جدیدی در دههٔ گذشته کشف شده‌اند.

یونانیان باستان، ۲۵۰۰ سال پیش، در مکتب فیثاغورس، بین **اعداد اول**[2] و **اعداد مرکب**[3] تمایز قائل می‌شدند. عدد اول عدد صحیح مثبتی است که عاملی جز یک و خودش ندارد. مسائل مربوط به اعداد اول نظر ریاضیدانها را از عهد عتیق تا زمان حاضر به خود جلب کرده‌است. شاید اولین سؤالی که در مورد اعداد اول به ذهن خطور کرده این سؤال که آیا بی‌نهایت اعداد اول وجود دارد یا خیر، باشد. در مقدمات[4] اقلیدس، ریاضیدان یونان باستان می‌توان برهانی، در مورد این که بی‌نهایت عدد اول موجود است، یافت. سؤال دیگری که در این مورد مطرح می‌شود این است که: آیا فرمولی که اعداد اول را تولید کند وجود دارد؟ پی‌یرفرما، نظریهٔ اعداد پرداز بزرگ فرانسوی قرن هفدهم، تصور می‌کرد که جمیع اعداد صحیح به صورت $2^{2^n}+1$ اولند؛ اما دروغ بودن این مطلب، یک قرن بعد از آنکه فرما چنین ادعایی کرد، توسط لئوناردداولر، ریاضیدان مشهور سوئیسی، که مبرهن ساخت که $2^{2^5}+1$ عامل ۶۴۱ است، به اثبات رسید.

مسألهٔ متمایز کردن اعداد اول از اعداد مرکب به طور وسیعی مورد بررسی قرارگرفته است. این مسأله، گرچه در ابتدا تنها به خاطر کنجکاویهای روشنفکرانه مورد بررسی قرار گرفت، امروزه مسألهٔ بسیار مهمی در رمز شناسی است. اراتُستن دانشمند یونان باستان روشی، که امروزه غربال اراتستن[5] نامیده می‌شود، و جمیع اعداد اول کمتر از حد مشخصی را به دست می‌دهد، اختراع کرد. این روش ابتدا جمیع اعداد صحیح زوج را حذف می‌کند، بعد اعداد صحیح باقیماندهٔ قابل قسمت به سه را حذف می‌کند، سپس به حذف اعداد صحیح

باقیماندهٔ بخش‌پذیر بر پنج می‌پردازد، و همینطور ادامه می‌دهد، و هنگامی که اعداد صحیح بخش‌پذیر بر بزرگترین عدد اول نامتجاوز از جذر حد زبرین دنبالهٔ مورد بحث حذف شده باشند، از کار می‌ایستد. در این صورت جمیع اعداد صحیح مانده، به جز ۱، اول اند.

گاهی نیاز به تعیین اول بودن عدد صحیح خاصی داریم. متأسفانه استفاده از غربال اراتستن در تشخیص اینکه عدد صحیح خاصی اول است یا نه، بی‌فایده است، بنابراین ریاضیدانها به جستجوی روشهای دیگری در تعیین اول بودن یک عدد صحیح رفته‌اند. ریاضیدانهای چین باستان تصور می‌کردند که اعداد اول دقیقاً آن اعداد صحیح مثبت n اند که $2^n - 2$ را عاد می‌کنند. فرما نشان داد که اگر n اول باشد، در این صورت $2^n - 2$ را عاد می‌کنند. اما در اوایل قرن نوزدهم، معلوم شد که اعداد صحیح مرکب n ی ، چون $n=341$ ، چنانکه $2^n - 2$ ، n را عاد کند، موجودند. اعداد مرکب مزبور به شبه اول[6] موسومند. از آنجا که اغلب اعداد صحیح مرکب شبه‌اول نیستند، امکان طرح تستهای اول بودن برمبنای اندیشهٔ چینی اولیه، همراه با ملاحظاتی اضافی، موجود می‌شود. و اکنون یافتن اعداد اول به کارایی امکان می‌یابد؛ در واقع، اعداد اولی با ۲۰۰ رقم اعشاری را می‌توان با چند دقیقه کار کامپیوتر به‌دست آورد. در حال حاضر قسمت عظیمی از تحقیقات جاری به نشان دادن اعداد صحیحی که اولند اختصاص یافته‌اند.

قضیهٔ **اساسی حساب**[7]، معروف یونانیان باستان، براین است که هر عدد صحیح مثبت را می‌توان به‌طور منحصر به فردی به صورت حاصل ضرب اعداد اول نوشت. این تجزیه را می‌توان با آزمایش تقسیم آن عدد بر اولهای کمتر از جذر آن به‌دست آورد؛ اما این روش، متأسفانه، بسیار وقت‌گیر است. فرما، اولر، و بسیاری از ریاضیدانهای دیگر، در این مورد، روشهای تجزیهٔ ابتکاری ای ارائه داده‌اند. اما، تجزیهٔ عدد صحیحی با ۲۰۰ رقم اعشار، بااستفاده از کاراترین تکنیکی که تاکنون به وجود آمده، می‌تواند به بلیونها سال وقت کامپیوتر نیاز داشته‌باشد. به همین جهت است که امروزه برای یافتن راههایی تازه در تجزیهٔ سریع اعداد صحیح بزرگ، تلاشهای وسیعی در دست اقدام است.

کارل فریدریش گوس ریاضیدان آلمانی، که یکی از بزرگترین ریاضیدانهای تمام اعصار به حساب می‌آید، لسان هم نهشتیها[8] را در اوائل قرن نوزدهم مطرح کرد. در این صورت هنگام انجام محاسبات معینی، بااستفاده از لسان هم نهشتیها، به‌جای اعداد، می‌توان باقیمانده‌های آنها را، چون بر عدد معینی تقسیم شوند، قرار داد. با استفاده از مفهوم هم نهشتی می‌توان مسائل بسیاری را، که بدون این اصطلاح تنها می‌توانند به صورت پیچیده و ناهنجاری بیان شوند، به گونه‌ای ظریف و موجز به عبارت آورد. هم نهشتیها کاربردهای متعددی در دانش کامپیوتر، از جمله کاربردهایی در فایل * حافظهٔ کامپیوتری، حساب با اعداد صحیح بزرگ، و ایجاد اعداد شبه تصادفی[9] دارند.

یکی از مهمترین کاربردهای نظریهٔ اعداد در دانش کامپیوتر حوزهٔ رمزنگاری است. از هم نهشتیها می‌توان برای مطرح کردن انواع گوناگون رمزها استفاده کرد. اخیراً نوع جدیدی از سیستمهای رمزی، موسوم به **سیستم رمزی عام ـ کلید** ارائه شده است. در این صورت چون رمز عام ـ کلیدی به کار رود، هر فرد یک کلید رمز بندی عام و یک کلید رمزگشایی خاص دارد. پیغامها با استفاده از کلید عمومی گیرنده رمز بندی می‌شوند. گذشته از این، تنها گیرنده می‌تواند پیغام مورد بحث را رمزگشایی کند، زیرا رمزگشایی، هنگامی که تنها کلید رمز بندی معلوم است، به مقدار بسیار زیادی زمان کامپیوتری نیاز دارد. سیستم رمزی عام ـ کلید بیش از همه به کار رفتهٔ فوق بر تفاوت کلی زمان کامپیوتری مورد نیاز برای یافتن اعداد اول بزرگ و تجزیهٔ اعداد صحیح بزرگ متکی است. در حالت خاص، در تهیهٔ یک کلید رمز بندی به این نیاز است که دو عدد اول بزرگ پیدا و سپس در هم ضرب شوند؛ و این کار را می‌توان در چند دقیقه بر کامپیوتر انجام داد. در این صورت کلید رمزگشایی مورد نظر، چون اولهای بزرگ مزبور مشخص شوند، می‌تواند به سرعت به دست آید. اما یافتن کلید رمزگشایی از کلید رمزبندی نیاز به این دارد که یک عدد بزرگ، یعنی حاصل‌ضرب اعداد اول بزرگ مزبور تجزیه شود، و این کار ممکن است بلیونها سال طول بکشد.

۱ـ Algorithm
۲ـ Primes
۳ـ Composite
۴ـ Elements
۵ـ Sieve of Erathosthense
۶ـ Pseudoprime
۷ـ Fundamental theorem of arithmetic
۸ـ Congruences
۹ـ Pseudo - random numbers
*پرونده