Számításelmélet

Babai László 2004. májusi előadása
Lejegyezte: Maga Péter

Prímszámtétel.
Jelöljük az x-nél nem nagyobb pozitív prímszámok számát $\Pi(x)$-el. Ekkor

$$\Pi(10) = 4; \qquad \Pi(100) = 25; \qquad \Pi(p) = 2$$

Az általános kérdés az, hogy egy nagy számig mennyi prímszám van. A tapasztalat azt mutatja, hogy bár a prímszámok egyenként meglehetősen rendezetlenül helyezkednek el a természetes számok között, összességében mégis valamilyen szabályosság jellemzi előfordulásukat. Gauss a következő észrevételt tette:

$$\frac{\Pi(x)}{x} \approx \frac{1}{\log x}$$

a logaritmus alapszáma az e. Ezt Gauss nem tudta bebizonyítani, csak 1896-ban sikerült Charles Jean de la Vallée Poussin és Jacques Hadamard matematikusoknak, egymástól függetlenül. A tétel megemlítése az előadás nyitánya volt, a későbbiekben más jellegű problémák következtek.

Sorrend
Az első feladat: van n kövünk, különböző nehézségűek, a sorrendjüket szeretnénk minél kevesebb méréssel megállapítani, ahol egy mérés két kő nehézségének összehasonlítását jelenti. Bármely kettő összemérése nyílván jó, de ez $n(n-1)/2$ mérés. Ennél jóval kevesebbel is meg lehet állapítani a sorrendet. Képzeljük el, hogy már néhány kő sorba van rakva, és egy újabbat szeretnénk a láncba beilleszteni. Ekkor felesleges minden eddigi kővel összemérni, hiszen a nehézség (mint reláció) tranzitív tulajdonsággal rendelkezik. Ha tehát például az új követ a középsővel (vagy „majdnem" középsővel) összemérjük, és annál nehezebbnek / könnyebbnek találjuk, akkor már a kövek felénél biztosan nehezebb / könnyebb. Így $[\log_2 2] + [\log_2 3] + \ldots + [\log_2 n] \leq \log_2 2 + \log_2 3 + \ldots + \log_2 n + (n-1) = \log_2(n!) + n - 1$, ahol [] most felső egész részt jelent. Ebben az összegben az $n - 1$ kicsi a $\log_2(n!)$-hoz képest, ha n nagy ($(n-1)/(\log_2(n!)) \to 0$, ha $n \to +\infty$). Tehát a mérések száma nagy n-ekre $\sim \log_2(n!)$. Ez lényegében pontos is, hiszen ha belegondolunk, n kőnek éppen $n!$ lehetséges sorrendje van, valamint egy mérés, mivel két követ hasonlít össze, a lehetséges eseteknek legfeljebb a felét teszi lehetetlenné, ezért a mérések száma legalább $\log_2(n!)$.

Szorzás
Az általános iskolában tanult szorzás a következőképpen megy: az ember megtanul egy szorzótáblát, ami szerint egy műveletben össze tud szorozni két egyjegyű (tízes számrendszerbeli) számot. Ezután ennek segítségével már nagy számokat is össze tud szorozni, minden egyes rendezett számjegy-párra végrehajtja ezt a műveletet, majd a kapott számokból egy összeadási műveletsorral összeállítja a végeredményt. Ez két n-jegyű szám esetében n^2 műveletet igényel, hiszen ennyi számjegy-pár van. A következőkben ennek a lecsökkentését vesszük célba. Tegyük fel, hogy két n-jegyű számot akarunk összeszorozni, x-et és y-t. Ekkor bontsuk fel őket úgy, hogy $x = x_1 \cdot 10^{n/2} + x_2$, valamint $y = y_1 \cdot 10^{n/2} + y_2$, a későbbiekre legyen $n = 2^k$. Ekkor $xy = x_1y_1 \cdot 10^n + (x_1y_2 + y_1x_2)10^{n/2} + x_2y_2$. Valamint vegyük észre a következő trükköt: $(x_1 - x_2)(y_1 - y_2) = x_1y_1 + x_2y_2 - (x_1y_2 + y_1x_2)$. Ekkor ha egy

szorzásban kiszámoljuk a feleannyi jegyű x_1y_1-t és x_2y_2-t, akkor már csak $(x_1 - x_2)(y_1 - y_2)$ szorzást kell elvégezni, ami szintén feleannyi jegyű. Tehát a jegyek számának kétszeresére való növekedése a műveletek számának csak háromszorosára való növekedését idézte elő (a rendes írásbeli szorzásnál kétszerannyi jegyhez négyszer annyi művelet kell). Tehát ha n jegyhez $T(n)$ művelet kell, akkor $T(n) = 3T(n/2) = \ldots = 3^kT(n/2^k) = 3^k$. Ebből azt kapjuk, hogy $T(n) = 3^{\log(2)n} = n^{\log(2)3} \approx n^{1,58}$, ami sokkal kevesebb az n^2-nél. Ez a módszer az összeadások számát is csökkenti nagy n-ekre. Az előadó megjegyezte, hogy ennél jóval gyorsabb szorzások is ismertek, van, ami $n\log n$ művelettel végigmegy.

Hamis érme I.

Van 12 érménk, közülük 1 hamis, de nem tudjuk, hogy melyik az, sem azt, hogy a többinél könnyebb, avagy nehezebb. Valamint van egy kétkarú mérlegünk, mely egy lépésben összehasonlítja a két tányérjára tett érméket, háromféle eredményt szolgáltathat (nehezebb valamelyik, ekkor azt is tudjuk, hogy melyik, vagy egyenlők). A feladat az, hogy három méréssel meghatározzuk azt, hogy melyik a hamis érme, és hogy a többinél nehezebb vagy könnyebb. Egy lehetséges megoldás: Az érméket három darab négyesre osztjuk, és kettőt összemérünk. 1. eset: egyenlők, ekkor a hamis érme a maradék négy között van, és már ismerünk nyolc jó érmét. Veszünk tehát három jó érmét, és összemérjük a maradék négy közül kiválasztott hárommal. Ha egyenlők, akkor a 12. érme a hamis, és egy méréssel a többihez való viszonyát megállapíthatjuk; ha nem, akkor tudjuk, hogy a hamis melyik három között van, és mivel a többihez való viszonyát is ismerjük, egy méréssel megtaláljuk. 2. eset: az első mérésnél valamelyik négyes nehezebb (legyen $\{a, b, c, d\} < \{e, f, g, h\}$). Ekkor tudjuk, hogy a hamis érme vagy könnyebb a többinél, és a, b, c, d valamelyike, vagy pedig nehezebb a többinél, és e, f, g, h valamelyike. Illetve azt is tudjuk, hogy az i, j, k, l érmék jók. Ekkor mérjük össze $\{a, e, i, j\}$-t és $\{b, c, f, g\}$-t. Ha egyenlők, akkor d vagy h a hamis, tehát például egy $\{d\} - \{k\}$ méréssel készen vagyunk. Ha $\{a, e, i, j\}$ a nehezebb, akkor e lehet a többinél nehezebb, vagy b vagy c könnyebb. Ez egy méréssel $(\{b\} - \{c\})$ megoldható. Ha pedig $\{b, c, f, g\}$ nehezebb, akkor f vagy g nehezebb, vagy a könnyebb a többinél, ez pedig $\{f\} - \{g\}$ méréssel megoldható. A felmerülő kérdések: Meg lehet-e ezt tenni előre leírt mérésekkel? Hány érme esetén elegendő még a három mérés? Azt a kövek sorba rendezéséhez hasonlóan be tudjuk bizonyítani, hogy 14 érme esetén már nem elegendő a három mérés. Ugyanis egy mérés a lehetséges eseteknek legalább egyharmadát lehetségesnek hagyja, tehát három mérés legfeljebb 27 esetet tud megkülönböztetni. A lehetséges esetek száma azonban kezdetben 28, mivel 14-féle lehet a hamis érme, és a többi érméhez való viszonya a nehézségük szerint kétféle lehet. Ekkor a 28 állapot közül nem különböztethető meg bármelyik kettő, ha csak három mérésünk van. A hamis érme 13 közül sem választható ki 3 méréssel.

Hamis érme II.

Van n érménk, közülük k (legalább 1) hamis, és a hamisak könnyebbek, ismét kétkarú mérlegünk van. Hány méréssel tudjuk a hamis érméket megtalálni? Hány mérésre van szükség, ha csak a hamis érmék száma kell? Ha a hamis érméket meg is kell határozni, akkor összesen 2^n-féle állapot van, minden mérés legalább egyharmadát lehetségesnek hagyja, tehát legalább $n\log_3 2$ mérésre szükség van. A kérdés fennmarad, hogy ennyi elég-e? Ha a hamis érméknek csak a száma kell, akkor $c(\log n)^2$ mérés elegendő, de nem tudni, lehet-e kevesebbel. Ez a következőképpen megy. Szintén abból indulunk ki, hogy n 2-hatvány. Ugyanis ha találunk olyan méréssorozatot, mely $c(\log n)^2$ lépésben megszámolja a rosszakat, akkor készen vagyunk a többi n-re is, mert két szomszédos 2-hatvány között a $\log x$ függvény

csak konstanssal változik. 2-hatványokra a következőképpen oldhatjuk meg a feladatot. Rakjuk az érméket körbe (egy szabályos n-szög csúcsaira), majd húzzunk olyan egyeneseket a középponton át, melyek nem mennek át érmén, és egy mérésben az egyenes két oldalán levő érméket hasonlítsuk össze. Ha páros sok hamis van köztük, akkor $\log_2 n$ lépésben megtaláljuk azt az egyenest, melynek a két oldalán ugyanannyi jó és ugyanannyi hamis érme van. Ha pedig páratlan sok hamis érme van, akkor $1 + \log_2 n$ lépésben találunk olyan helyzetet, melyben az egyik oldalon pontosan eggyel több hamis érme van, mint a másik oldalon. Ezután, $1 + \log_2(n/2)$ ugyanígy mindig megfelezi az érméket, mi pedig jegyezzük, hogy az elhagyottakban levő rosszak száma hogyan viszonyul a megmaradtak között levő rosszak számához. Így $\log_2 n + \log_2(n/2) + \ldots + \log_2 2 + \log_2 1 + \log_2 n$ lépésben megszámolhatjuk a rossz érméket. Ez $2\log_2 n + \log_2 n - 1 + \log_2 n - 2 + \ldots + \log_2 n - \log_2 n$, ami éppen $\log_2 n + (\log_2 n)^2 - \log_2 n(\log_2 n + 1)/2$, ami valóban $c(\log n)^2$ alakú.