Erdős egy kedvenc problémájáról:
kongruencia-fedőrendszerek

Bevezetés

1993-ban a 80 éves Erdős Pál az ELTE díszdoktorává történt avatása alkalmából előadást tartott néhány kedvenc problémájáról a zsúfolásig megtelt Gólyavárban. Idézzünk ebből néhány mondatot: „Az elsőt 1931-ben vetettem fel, olyan régen, hogy nem is vagyok biztos benne, hogy ez Krisztus előtt volt vagy Krisztus után. Egy régi viccem különben, hogy két és fél milliárd éves vagyok. Erre az a bizonyíték, hogy amikor kicsi voltam, a Föld kora kétmilliárd év volt, és most közismert, hogy 4,6 milliárd év. Nyilván a különbség az én korom, és egyszer Los Angelesben tartottam egy előadást, melynek ez volt a címe: „Az első kétmilliárd évem a matematikában", és a diákok készítettek egy ábrát, amelyre felrajzoltak egy diagramot: „a Föld születése, Erdős születése, a dinoszauruszok születése", és volt egy kép, amelyen egy dinoszaurusz hátán ülök."

Mi most az akkori előadás második problémájával foglalkozunk: Fedjük le a nemnegatív egészeket különböző differenciájú számtani sorozatokkal:

$$\{0, 1, 2, \ldots, n, \ldots\} = \{a_1, a_1 + m_1, a_1 + 2m_1, \ldots\} \cup \ldots \cup \{a_k, a_k + m_k, a_k + 2m_k, \ldots\},$$

ahol $1 < m_1 < m_2 < \ldots < m_k$.

Ha $0 \leq a < m$, akkor az $a, a+m, a+2m, \ldots$ számtani sorozat azokat a számokat jelenti, amelyek m-mel osztva a maradékot adnak, vagyis ez tulajdonképpen egy maradékosztály (pontosabban annak nemnegatív része). Ezt a maradékosztályt $a \pmod m$-mel jelöljük, és m-et modulusnak nevezzük. Ha egy b és c egész szám m-mel osztva ugyanazt a maradékot adják, akkor azt mondjuk, hogy b kongruens c-vel modulo m, és ezt $b \equiv c \pmod m$ formában jelöljük.

Így a problémát átfogalmazhatjuk arra, hogy az egész számokat különböző modulusok szerinti maradékosztályokkal fedjük le: Minden t egész szám eleme az

$$a_1 \pmod{m_1}, \quad a_2 \pmod{m_2}, \quad \ldots, \quad a_k \pmod{m_k}$$

maradékosztályok közül legalább az egyiknek, azaz van olyan i, amelyre $t \equiv a_i \pmod{m_i}$.

Hogyan készíthetünk ilyen kongruencia-fedőrendszert? A modulusok legkisebb közös többszörösére nézve a számok maradékai mindegyik modulus szerint periodikusak, így elég 1-től eddig az lkkt-ig ellenőrizni a számok lefedettségét. Próbálkozzunk a 12-vel mint legkisebb közös többszörössel, ekkor modulusokként a 12 osztóit használhatjuk (azért érdemes a 12-t nézni, mert nagyságához képest elég sok osztója van). A páros számokat lefedi a $0 \pmod 2$, a hárommal oszthatókat a $0 \pmod 3$. Így 12-ig már csak az 1, 5, 7 és 11 fedését kell biztosítani a 4, 6 és 12 modulusok segítségével; megfelel pl. $1 \pmod 4$, $1 \pmod 6$, $11 \pmod{12}$. Ez az összesen öt kongruencia tehát egy fedőrendszert alkot. Egy másik példa: $0 \pmod 2$, $0 \pmod 3$, $1 \pmod 4$, $7 \pmod 8$, $11 \pmod{12}$, $19 \pmod{24}$.

A témával kapcsolatban a leghíresebb megoldatlan probléma, amelynek tisztázásáért Erdős 1000 dollárt ajánlott fel, hogy egy fedőrendszerben lehet-e a legkisebb modulus akármilyen nagy, azaz bármely N-hez van-e olyan fedőrendszer, ahol mindegyik modulus legalább N.

A jelenlegi rekord $N = 40$, ezt 2008-ban állította fel P. Nielsen, és egy 26 oldalas cikkben adta meg a konstrukciót, pontosabban az ahhoz vezető algoritmust: a modulusok a 103-ig terjedő prímek hatványainak bizonyos szorzatai, de sem ezek, sem a megfelelő maradékosztályok nincsenek explicite leírva.

Egy másik („csak" 25 dolláros) megoldatlan probléma, hogy lehet-e minden modulus páratlan.

Nagyon szép tétel, hogy nincs egzakt fedés, azaz nincs olyan fedőrendszer, ahol minden szám pontosan egy kongruenciát elégít ki.

És most térjünk rá arra a kérdésre, amelynek kapcsán Erdős kitalálta a fedőrendszereket: Előáll-e minden elég nagy páratlan szám egy prímszám és egy kettőhatvány összegeként?

Ezt Romanov szovjet matematikus kérdezte 1934-ben, és Erdős 1950-ben a fedőrendszerek segítségével nemleges választ adott: Létezik páratlan számokból álló végtelen számtani sorozat, amelynek elemei nem állnak így elő.

A következőkben ezt a tételt fogjuk igazolni.

Előkészületek, segédeszközök

Először megmutatjuk, hogy ha q páratlan prím, akkor a 2 hatványainak q-val vett maradékai periodikusan ismétlődnek.

Ehhez elég belátni, hogy van olyan $t > 0$, amelyre 2^t maradéka 1, hiszen akkor 2^{t+1} maradéka ugyanaz, mint 2-é, 2^{t+2} maradéka ugyanaz, mint 2^2-é stb., azaz a maradékok t szerint periodikusak lesznek.

Mivel végtelen sok kettőhatvány van, de csak q-féle maradék lehet, ezért a skatulyaelv miatt lesz olyan $i < j$, amelyre $q \mid 2^j - 2^i = 2^i(2^{j-i} - 1)$, és így q páratlansága miatt $q \mid 2^{j-i} - 1$, vagyis $t = j - i$ megfelel.

A legkisebb ilyen periódust a 2 *rend*jének nevezzük mod q.

Példa: A kettőhatványok 17-es maradékai: $1, 2, 4, 8, 16, 15, 13, 9, 1, 2, \ldots$, tehát a 2 rendje 8 mod 17.

A fentiekhez hasonlóan általában is megmutatható, hogy ha h és v relatív prímek, akkor h hatványainak v-vel vett maradékai is periodikusan ismétlődnek (és a rend fogalmát is általánosan be lehet vezetni).

Szükségünk lesz még a kínai maradéktételre: Ha előírunk véges sok páronként relatív prím modulus szerint tetszőleges maradékokat, akkor lesz olyan szám, amely egyszerre teljesíti mindegyik feltételt, és az összes ilyen szám egy, a modulusok szorzata szerinti maradékosztályt alkot (azaz egy számtani sorozatot, amelynek a differenciája a modulusok szorzata). Képlettel: Ha a $v_1, \ldots, v_r$ számok páronként relatív prímek, akkor az

$$x \equiv b_i \pmod{v_i}, \quad i = 1, \ldots, k$$

szimultán kongruenciarendszer bármely $b_1, \ldots, b_k$ esetén megoldható, és a megoldások egy modulo $v_1 \ldots v_k$ maradékosztályt alkotnak.

A bizonyítás

Tegyük fel, hogy a q prímre a 2 rendje m, és $n \equiv a \pmod{m}$. Mivel a 2 hatványainak q szerinti maradékai az m periódus szerint ismétlődnek, ezért ekkor $2^n \equiv 2^a \pmod{q}$.

Így ha $c = 2^n + p$, ahol p prím, és $c \equiv 2^a \pmod{q}$, akkor $p = c - 2^n \equiv c - 2^a \equiv 0 \pmod{q}$, tehát csak $p = q$ lehetséges.

Ez azt jelenti, hogy ha néhány q_i prímmel az összes n-hez tartozó c-ket „le tudjuk fogni", akkor már csak a $2^n + q_i$ számokat kell a c-k közül kizárni (ami nem lesz túl nehéz).

Legyen ezért $a_i \pmod{m_i}$, $i = 1, 2, \ldots, k$ egy fedőrendszer, legyenek $q_1, q_2, \ldots, q_k$ olyan prímek, hogy mod q_i a 2 rendje éppen m_i.

Megmutatható, hogy ha $m_i \neq 6$, akkor mindig vannak ilyen különböző q_i prímek. Keressük meg ezeket a második példaként megadott $m_1 = 2$, $m_2 = 3$, $m_3 = 4$, $m_4 = 8$, $m_5 = 12$, $m_6 = 24$ modulusú fedőrendszerhez (és ez már teljesen elegendő lesz a tételünk bizonyításához). Az kell, hogy a 2 rendje m_i legyen mod q_i, ami azt jelenti, hogy $2^{m_i} \equiv 1 \pmod{q_i}$, azaz $q_i \mid 2^{m_i} - 1$, és itt m_i a minimális ilyen (pozitív egész) kitevő. Ekkor $m_1 = 2$-nél $q_1 \mid 2^2 - 1 = 3$, azaz $q_1 = 3$ megfelel. Hasonlóan adódik $q_2 = 7$. Továbbmenve $m_3 = 4$-re $q_3 \mid 2^4 - 1 = 15 = 3 \cdot 5$, de a 3 nem jó, mert mod 3 a 2 rendje 2 volt és nem 4, így csak $q_3 = 5$ lehet, ami tényleg jó. Az $m_4 = 8$ modulushoz $q_4 \mid 2^8 - 1 = (2^4 - 1)(2^4 + 1)$, itt q_4 nem lehet az első tényező osztója, mert akkor a 2 rendje legfeljebb 4 lenne, így csak $q_4 = 17$ lehet, ami jó. Az $m_5 = 12$-t véve $q_5 \mid 2^{12} - 1 = (2^6 - 1)(2^6 + 1) = (2^6 - 1)(2^2 + 1)(2^4 - 2^2 + 1)$, és itt az első két tényező nem jöhet szóba (miért?), ahonnan $q_5 = 13$. Végül $m_6 = 24$-re $q_6 \mid 2^{24} - 1 = (2^{12} - 1)(2^4 + 1)(2^8 - 2^4 + 1)$, ismét csak az utolsó tényezőből $q_6 = 241$. Azaz a megfelelő q_i prímek a $3, 7, 5, 17, 13, 241$.

A bizonyítás elején vázolt ötletnek megfelelően tekintsük most a $c \equiv 2^{a_i} \pmod{q_i}$ szimultán kongruenciarendszert, és ezt egészítsük ki egy $c \equiv 1 \pmod{2^s}$ kongruenciával, ahol s értékét úgy választjuk, hogy $2^{s-1} > q_i$ minden i-re. (Az utolsó kongruencia egyrészt biztosítja c páratlanságát, másrészt — amint látni fogjuk — a $c = 2^n + q_i$ típusú előállítás lehetetlenségét.)

Ez a szimultán rendszer a modulusok páronkénti relatív prímsége miatt megoldható, és a megoldások egy maradékosztályt alkotnak a modulusok M szorzata szerint, azaz egy M differenciájú számtani sorozatot kapunk, amelynek minden eleme páratlan szám (az utolsó kongruencia miatt).

Megmutatjuk, hogy a sorozat egyik eleme sem áll elő egy kettőhatvány és egy prímszám összegeként.

Indirekt, tegyük fel, hogy $c = 2^n + p$. Ekkor a fedőrendszer miatt valamelyik i-re $n \equiv a_i \pmod{m_i}$. A bizonyítás elején tett meggondolások miatt ekkor p csak valamelyik q_i lehetne.

Belátjuk, hogy ez sem teljesülhet. Ha $n \leq s - 1$, akkor $1 < c = 2^n + q_i < 2^{s-1} + 2^{s-1} = 2^s$, ami ellentmond a $c \equiv 1 \pmod{2^s}$ feltételnek. Ha pedig $n \geq s$, akkor $c = 2^n + q_i \equiv q_i \pmod{2^s}$, ami ismét ellentmondás.