Egy kongruenciarendszerekről szóló problémáról

Írta: Erdős Pál

Az

$$x \equiv a_i \pmod{n_i}, \quad 1 < n_1 < n_2 < \ldots < n_k \tag{1}$$

kongruenciarendszert nevezzük lefedő rendszernek, ha minden egész szám az (1) kongruenciák közül legalább az egyiket kielégíti. Mielőtt az ezekre vonatkozó kérdések diszkutálásába belekezdenék, talán megmutatom, hogyan jutottam ezekre a kérdésekre.

A dolgozatban p, q, p_i, q_i prímszámokat fognak jelenteni, $\pi(x)$ pedig a prímszámok számát x-ig; $c_1, c_2, \ldots$ pozitív abszolút konstansok.

Romanov még 1934-ben kimutatta, hogy a $2^l + p (p > 0, l$ pozitív egész) alakú számoknak pozitív sűrűségük van. Más szóval: létezik olyan c_1, hogy x-ig a $2^l + p$ alakban írható számok száma nagyobb, mint $c_1 x$. Romanov bizonyítása, bár elemi, mélyebb segédeszközöket igényel és itt csak azt kívánom megjegyezni, hogy Romanov tétele főleg azért érdekes, mert aránylag kevés $2^l + p$ alakú szám van. Pontosabban; ha $f(n)$ jelenti az $n = 2^l + p$ egyenlet megoldásainak számát, akkor

$$\sum_{n=1}^{x} f(n) < c_2 x.$$

Mármost Romanov, egy még 1934-ben hozzám intézett levelében, azt kérdezte: igaz-e, hogy minden elegendően nagy páratlan szám $2^l + p$ alakban írható? Kimutattam, hogy ez nem igaz, sőt:

létezik olyan, csupa páratlan számból álló, számtani sor, melynek egyetlen pozitív tagja sem állítható elő $2^l + p$ alakban.

A bizonyításhoz felhasználjuk Bang érdekes tételét: Legyen $1 < n \neq 6$ tetszőleges egész szám. Akkor van olyan p, hogy

$$p \mid 2^n - 1 \text{ és } p \nmid 2^m - 1, \text{ ha } 1 \leqq m < n. \tag{2}$$

A továbbiakban az ilyen tulajdonsággal rendelkező p prímszámot (több ilyen is lehet) n-hez tartozó prímszámnak fogjuk hívni.

Legyen mármost adva egy (1) lefedő rendszer, melyben $n_i \neq 6$, $1 \leqq i \leqq k$ és legyen p_i az n_i-hez tartozó prímszámok valamelyike. Ekkor ezen p_i-k (2) értelmében mind különbözők. Tekintsük a következő kongruenciarendszert:

$$(3) \qquad \begin{aligned} t &\equiv 2^{n_i} \pmod{p_i}, \quad 1 \leqq i \leqq k; \\ t &\equiv 2^{n_k+2} + 2^{n_k+1} + 1 \pmod{2^{n_k+3}}. \end{aligned}$$

Mivel előbbiek szerint a p_i-k mind különböző páratlan prímek, a (3) rendszer megoldható. Ezen kongruenciarendszert kielégítő t számok nyilván mind páratlanok és egy $2^{n_k+3} \Pi p_i$ differenciájú számtani sort alkotnak. Azt állítom, hogy

$$(4) \qquad t + 2^l + p; \; l \text{ egész szám}, \; l \geqq 0.$$

Mivel az (1) kongruenciarendszer lefedő, tehát legalább egy i-re

$$l \equiv a_i \pmod{n_i}.$$

Viszont p_i definíciója szerint $2^{n_i} \equiv 1 \pmod{p_i}$, tehát

$$2^l \equiv 2^{a_i} \equiv t \pmod{p_i}.$$

Vagyis $t - 2^l$ mindig osztható a $p_1, p_2, \ldots, p_k$ prímszámok valamelyikével. Mivel $\max p_i < 2^{n_k} (1 \leqq i \leqq k)$, tehát (4) bizonyításához elég lesz kimutatnunk, hogy

$$|t - 2^l| > 2^{n_k}.$$

Ennek bizonyítására van szükség a (3) alatti utolsó feltételre, mely szerint

$$(5) \qquad t - 2^l \equiv 2^{n_k+2} + 2^{n_k+1} - 2^l + 1 \pmod{2^{n_k+3}}.$$

Ha $l \geqq n_k + 3$, akkor $2^l \equiv 0 \pmod{2^{n_k+3}}$, tehát

$$|t - 2^l| \geqq 2^{n_k+1} - 1 > 2^{n_k}.$$

Ha pedig $0 \leqq l \leqq n_k + 2$, akkor (3) második kongruenciájából $t \geqq 2^{n_k+2} + 2^{n_k+1} + 1$ azaz $t - 2^l \geqq 2^{n_k+1} + 1 > 2^{n_k}$.

Bizonyításunk befejezéséhez már csak azt kell belátnunk, hogy van olyan lefedő rendszer, melyre $n_i \neq 6$. Ilyen rendszer például:

0 (mod 2), 0 (mod 3), 1 (mod 4), 7 (mod 8), 11 (mod 12), 19 (mod 24).

A lefedő kongruenciarendszerekre vonatkozó legérdekesebb probléma a következő:

Legyen A tetszőleges szám; létezik-e olyan lefedő rendszer, melynél $A < n_1 < n_2 < \ldots < n_k$.

Amennyiben a válasz e kérdésre igenlő, akkor azonnal belátható, hogy ha r tetszőleges egész szám, úgy mindig van végtelen

sok t egész szám, mely nem $2^l + a_r$ (l egész szám, $l \geqq 0$) alakú, ahol a_r különböző prímfaktorainak száma $\leqq r$. Ugyanis akkor megadható $r+1$ darab kongruenciarendszer

$$\begin{aligned} x &\equiv a_i^{(1)} \pmod{n_i^{(1)}}, \quad 1 \leqq i \leqq k_1; \\ x &\equiv a_i^{(2)} \pmod{n_i^{(2)}}, \quad 1 \leqq i \leqq k_2; \\ &\vdots \\ x &\equiv a_i^{(r+1)} \pmod{n_i^{(r+1)}} \quad 1 \leqq i \leqq k_{r+1}, \end{aligned}$$

melyekre

$$6 < n_1^{(1)} < \ldots < n_{k_1}^{(1)} < n_1^{(2)} < \ldots < n_{k_2}^{(2)} < \ldots < n_1^{(r+1)} < \ldots < n_{k_{r+1}}^{(r+1)}.$$

Elégítse ki t a következő kongruenciákat:

$$t \equiv 2^{a_i^{(s)}} \pmod{p_i^{(s)}}, \quad 1 \leqq i \leqq k_s, \quad 1 \leqq s \leqq r+1,$$

ahol $p_i^{(s)}$ jelenti az $n_i^{(s)}$-hez tartozó prímszámok valamelyikét. Pontosan úgy, mint az $r=1$ esetben belátható, hogy minden egyes s-re ($1 \leqq s \leqq r+1$) van olyan $p_i^{(s)}$, hogy

$$t - 2^l \equiv 0 \bmod p_i^{(s)}.$$

Tehát $(t-2^l)$-nek legalább $r+1$ darab prímfaktora van.

Azonban azon sejtés bizonyítása, hogy a feltett kérdésre a válasz igenlő — nem látszik könnyűnek. DAVENPORT és én konstruáltunk olyan lefedő rendszert, melyre $n_1 = 3$. Egy ilyen rendszer a következő:

0 (mod 3)	11 (mod 15)
0 (mod 4)	7 (mod 20)
0 (mod 5)	10 (mod 24)
1 (mod 6)	2 (mod 30)
6 (mod 8)	34 (mod 40)
3 (mod 10)	59 (mod 60)
5 (mod 12)	98 (mod 120)

Néhány perc alatt meggyőződhetünk arról, hogy e rendszer valóban lefedő. Valószínűleg ez a legegyszerűbb lefedő rendszer, melyre $n_1 > 2$ (azaz ha $n_1 > 2$, akkor a modulusok száma $\geqq 14$ és a legnagyobb modulus $\geqq 120$).

DEAN SWIFT konstruált egy lefedő rendszert, melyben $n_1 = 4$, $k = 38$, $n_k = 1440$.

Ha az

$$x \equiv a_i \pmod{n_i}; \quad 1 \leqq i \leqq k \tag{6}$$

rendszer lefedő, akkor

$$\sum_{i=1}^{k} \frac{1}{n_i} \geqq 1.$$

Ugyanis legyen $f(N)$ azon N-nél nagyobb számok száma, melyek kielégítik az $x \equiv a_i \pmod{n_i}$ kongruenciát. Akkor

$$f(N) \leqq \frac{N}{n_i} + 1.$$

Mivel (6) lefedő rendszer, tehát

$$\sum_{i=1}^{k} \frac{N}{n_i} + k \geqq N, \tag{7}$$

vagyis

$$\sum_{i=1}^{k} \frac{1}{n_i} \geqq 1 - \frac{k}{N}$$

és, mivel N-et tetszőlegesen nagyra választhatjuk, tehát

$$\sum_{i=1}^{k} \frac{1}{n_i} \geqq 1.$$

Ha (6) lefedő rendszer és

$$\sum_{i=1}^{k} \frac{1}{n_i} = 1,$$

akkor minden egész szám pontosan egy (6) alatti kongruenciát elégít ki.

Tegyük fel ugyanis, hogy vannak olyan egész számok, amelyek legalább két (6) alatti kongruenciát kielégítenek, pl. az

$$\begin{aligned} x &\equiv a_{i_1} \pmod{n_{i_1}}; \\ x &\equiv a_{i_2} \pmod{n_{i_2}}; \end{aligned} \qquad 1 \leqq i_1, i_2 \leqq k; \quad i_1 \neq i_2$$

kongruenciákat és legyen $f_1(N)$ azon N-nél nem nagyobb számok száma, melyek ezeknek eleget tesznek. Akkor

$$f_1(N) \geqq \frac{N}{n_{i_1} n_{i_2}} - 1$$

és, (7)-el egybevetve,

$$\sum_{i=1}^{k} \frac{N}{n_i} + k - \left(\frac{N}{n_{i_1} n_{i_2}} - 1 \right) \geqq N,$$

$$\sum_{i=1}^{k} \frac{1}{n_i} \geqq 1 + \frac{1}{n_{i_1} n_{i_2}} - \frac{1+k}{N} > 1.$$

Azt sejtettem, hogy ha a (6) alatti rendszer lefedő, akkor

$$\sum_{i=1}^{k} \frac{1}{n_i} > 1, \tag{8}$$

vagyis a rendszer nem egyszeresen fedi le az egész számokat. Ezt azonban nem tudtam bebizonyítani. (8)-ra MIRSKY és NEWMANN a következő szellemes bizonyítást találta (ugyanezt a bizonyítást találta később DAVENPORT és RADÓ is):

Tegyük fel, hogy (6) lefedő rendszer és $\sum_{i=1}^{k} \frac{1}{n_i} = 1$. Akkor, mint már láttuk, minden egész szám pontosan egy (6) alatti kongruenciát elégít ki. Akkor

$$(9) \qquad \sum_{t=0,1,2,3,\ldots} z^t = \sum_{t\equiv a_1 \pmod{n_1}} z^t + \sum_{t\equiv a_2 \pmod{n_2}} + \ldots + \sum_{t\equiv a_k \pmod{n_k}} z^t.$$

Ha $|z| < 1$, akkor

$$\sum_{t\equiv a_i \pmod{n_i}} z^t = z^{a_i} + z^{a_i+n_i} + z^{a_i+2n_i} + \ldots = \frac{z^{a_i}}{1-z^{n_i}}$$

és (9)-ből

$$(10) \qquad \frac{z^{a_1}}{1-z^{n_1}} + \frac{z^{a_2}}{1-z^{n_2}} + \ldots + \frac{z^{a_k}}{1-z^{n_k}} = \frac{1}{1-z}$$

volna. Ez azonban nem lehetséges, mert ha z-vel a sugár mentén közeledünk $e^{\frac{2\pi i}{n_k}}$-hoz, akkor (10) jobboldala korlátos marad, míg a baloldal végtelenhez tart. (T. i. $\frac{z^{a_k}}{1-z^{n_k}} \to \infty$, a baloldal többi tagja pedig korlátos marad.) Ez az egyszerű és szellemes bizonyítás talán alkalmas annak megmutatására, milyen jól használható az analízis módszere a számelméletben.

Eddig egyikünknek sem sikerült (8)-ra teljesen elemi bizonyítást adni.

Meg kell jegyeznem azt, hogy ha lefedő rendszerünk végtelen sok kongruenciát tartalmazhat, akkor (8) nem marad igaz. Ellenpélda: az

$$(11) \qquad x \equiv 2^{k-1} - 1 \pmod{2^k}; \qquad k = 1, 2, \ldots$$

rendszer lefedő és minden egész szám csak egyet elégít ki ezen kongruenciák közül. Ugyanis ha az a számot a kettes számrendszerben felírva az első 0 az $(n-1)$-edik helyen áll, akkor

$$a = \sum_{t=0}^{n-2} 2^t + 2^{r_1} + 2^{r_2} + \ldots + 2^{r_s}; \qquad r_i \geqq n, \; 1 \leqq i \leqq s;$$

$$a = 2^{n-1} - 1 + 2^n A,$$

$$a \equiv 2^{n-1} - 1 \pmod{2^n};$$

tehát a rendszer lefedő. Ha valamely a szám két (11) alatti kon-

gruenciát elégítene ki, akkor

$$a = 2^k A_1 + 2^{k-1} - 1 = 2^l A_2 + 2^{l-1} - 1$$

volna és, $k < l$ mellett,

$$2A_1 + 1 = 2^{l-k}(2A_2 + 1)$$

lenne, ami lehetetlen.

Ugyanakkor (8) nem javítható, mert pl. az

$$x \equiv 2^{t-1} - 1 \pmod{2^t} \qquad 1 \leqq t \leqq l;$$
$$x \equiv 2^l - 1 \pmod{3.2^{l-2}}$$
$$x \equiv 2^{l+1} - 1 \pmod{3.2^{l-1}}$$
$$x \equiv 3.2^l - 1 \pmod{3.2^l}$$

kongruenciarendszer lefedő és

$$\sum_{i=1}^{l-3} \frac{1}{n_i} = \frac{3.2^l - 3 + 4 + 2 + 1}{3.2^l} = 1 + \frac{1}{3.2^{l-2}},$$

ami 1-hez tetszőleges közel lehet.

DAVENPORT megjegyzése szerint ha $n_1 > 2$, akkor (8) talán javítható, de ez a kérdés nem látszik könnyűnek.

Diszkutáljunk még egy ide tartozó problémát! Egy lefedő rendszert nevezzünk primitívnek, ha egyetlen kongruencia sem felesleges, azaz ha elhagyjuk az $x \equiv a_i \pmod{n_i}$ kongruenciák bármelyikét, a megmaradó rendszer nem lefedő. Be fogjuk bizonyítani, hogy rögzített k mellett csak véges sok olyan primitív lefedő rendszer létezik, melynek k darab modulusa van.

Legyen

$$x \equiv a_i \pmod{n_i}, \qquad 1 \leqq i \leqq k$$

valamely primitív lefedő rendszer. Ha kimutatjuk, hogy

$$n_i < (k - i + 1)\,[n_1, n_2, \ldots, n_{i-1}] \tag{12}$$

($[n_1, n_2, \ldots, n_{i-1}]$ az $n_1, \ldots, n_{i-1}$ számok legkisebb közös többszörösét jelenti), akkor már következik, — mivel nyilvánvalóan $n_i < k$ —, hogy n_k egy felső korlát alatt marad, vagyis állításunk igaz. Bizonyítsuk be (12)-t.

Mivel kongruenciarendszerünk primitív, tehát van olyan t szám, hogy

$$t \not\equiv a_j \pmod{n_j}, \qquad 1 \leqq j \leqq i-1.$$

Ez azt jelenti, hogy ha

$$u \equiv t \pmod{[n_1, n_2, \ldots, n_{i-1}]},$$

akkor

$$u \not\equiv a_j \pmod{n_j}, \qquad 1 \leqq j \leqq i-1.$$

Ha tehát $f(N)$-nel jelöljük azon, N-nél nem nagyobb számok számát, melyek nem tesznek eleget az

$$x \equiv a_j \pmod{n_j}, \qquad 1 \leqq j \leqq i-1$$

kongruenciák egyikének sem, akkor

$$f(N) \geqq \frac{N}{[n_1, \ldots, n_{i-1}]} - 1.$$

Ezért (lásd (7) bizonyítását)

$$\frac{1}{n_i} + \frac{1}{n_{i+1}} + \ldots + \frac{1}{n_k} \geqq \frac{1}{[n_1, n_2, \ldots, n_{i-1}]},$$

illetőleg

$$\frac{k-i+1}{n_i} > \frac{1}{[n_1, n_2, \ldots, n_{i-1}]}.$$

A k darab kongruenciából álló primitív lefedő rendszerre n^k pontos maximumát nem tudom meghatározni.

ОБ ОДНОЙ ПРОБЛЕМЕ О СИСТЕМАХ СРАВНЕНИЙ

П. ЭРДЁШ

Система сравнений (1) называется покрывающей системой, если для всякого целого числа выполняется по крайней мере одно из сравнений системы (1). Автор доказывает следующую теорему: Существует арифметическая прогрессия из нечетных целых чисел, ни один член которого не может быть представлен в виде $2^l + p$ где l-натуральное число и p-простое число. Далее автор излагает ряд вопросов относящиеся к покрывающим системам и предлагает некоторые неразрешенные проблемы.

ON A PROBLEM CONCERNING CONGRUENCE SYSTEMS

P. Erdős

We call the congruence system (1) overlapping, if each integer satisfies at least one of the congruences (1). By making use of such systems, the author proves the following theorem: *There exists an arithmetic progression consisting of odd integers none of which can be represented in the form* $2^l + p$ *(p natural prime, l natural integer).* Furthermore, a number of questions relating to overlapping systems is discussed and several unsolved problems are proposed.