Haladvány Kiadvány 12.01.25.

Egy régi műegyetemi tétel az oszthatóságról

Hujter Mihály

Tisztelettel dedikálva Reiman István műegyetemi tanár úr 85. születésnapjára.

Legyen p egy rögzített páratlan prím! Tekintünk a_0, a_1, ..., a_{p-2} egész számokat, és feltesszük, hogy a_0 nem osztható p-vel. Tekintjük az

$$f(x) = a_0 + a_1 x + \ldots + a_{p-2} x^{p-2}$$

polinomot. Megnézzük, hogy az $x = 1, 2, \ldots, p-1$ számok közül hány darabra lesz $f(x)$ osztható p-vel. Ezt a darabszámot jelölje μ_1. *Kőnig Gyula* (1849–1913) és *Rados Gusztáv* (1862–1942) közös tétele szerint

$$\mu_1 + r_f = p - 1$$

ahol r_f jelöli a $(p-1) \times (p-1)$ méretű alábbi mátrix rangját modulo p:

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_{p-3} & a_{p-2} \\ a_{p-2} & a_0 & \cdots & a_{p-4} & a_{p-3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_2 & a_3 & \cdots & a_0 & a_1 \\ a_1 & a_2 & \cdots & a_{p-2} & a_0 \end{bmatrix}$$

A mátrix első sorában listáztuk a polinom együtthatóit, az alatta lévő sorok mindegyike pedig ciklikus eltolással kapható az előzőből. A főátlóban tehát mindenhol a_0 van. A μ_1 jelölést (illetve elnevezést) az indokolja, hogy Kőnig és Rados a Műegyetem professzorai voltak (sőt többször rektorai is). A tétel történetéről csak annyit sikerült kinyomozni, hogy a legkorábbi említés 1882-ből való [1]. (Akkor Rados még a születési nevét használta: *Raussnitz*.)

Speciális esetként kapjuk: *Egész x-re az $f(x)$ számok között akkor és csak akkor találunk p-vel oszthatót, ha a mátrix determinánsa osztható p-vel.*

A fenti tétel nyilvánvaló abban az esetben, ha az $a_1, \ldots, a_{p-1}$ számok mindegyike osztható p-vel. A maradék esetekre pedig az általánosság korlátozása nélkül feltehető, hogy $a_0 = 1$. (Ugyanis ha a_0 nem 1 maradékot adna p-vel osztva, akkor ezzel a maradékkal modulo p leoszthatnánk az $f(x)$ polinomot, és ez a leosztás a mátrix rangját nem változtatná meg, hiszen bármely $k \times k$ méretű aldeterminánsmodulo p egy nemnullával osztódna. A leosztás azt sem változtatja meg, hogy egy konkrét x-re $f(x)$ osztható-e p-vel.)

Nézzük a fenti tételt $p = 3$ esetén. A nemtriviális esetek mindössze kétfélék: $f(x) = 1 + x$ vagy $f(x) = 1 + 2x$. A két esetben a mátrix a következő:

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \qquad\qquad \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$$

Modulo 3 mindkét mátrix rangja 1. Valóban, az $1 + 1$ és $1 + 2$ számok közül is, és az $1 + 2 \cdot 1$ és $1 + 2 \cdot 2$ számok közül is pontosan 1 darab osztható 3-mal.

Érdemes megjegyezni, hogy Kőnig és Rados tétele nemcsak páratlan prímekre igaz, hanem az összes prímhatványra is (ha a kitevő legalább 2). A polinomot, a mátrixot és a mátrix rangját is ilyenkor a p elemű számtestben értelmezzük. Például $p = 4$ esetén lényegében kilencféle nemtriviális polinomunk van, ahol a számtest elemei: $0, 1, s, t$:

$$\begin{array}{ccc} 1 + x & 1 + sx & 1 + x^2 \\ 1 + sx^2 & 1 + x + x^2 & 1 + x + sx^2 \\ 1 + sx + x^2 & 1 + sx + sx^2 & 1 + sx + tx^2 \end{array}$$

A legutolsó esetben a mátrix ez:

$$\begin{bmatrix} 1 & s & t \\ t & 1 & s \\ s & t & 1 \end{bmatrix}$$

Emlékeztetünk rá, hogy a 4-elemű számtestben $1 + 1 = s + s = t + t = 0$, $s + t = 1$, $1 + s = t$, $s \cdot s = t$, $s \cdot t = 1$, $t \cdot t = s$, ezért a fenti mátrix rangja 1. Tehát most azt állítja a tétel, hogy $f(x) = 1 + sx + tx^2$ esetén az $f(1), f(s), f(t)$ testelemek között kétszer lehet 0. Valóban, $f(1) = 0$, $f(s) = 0$, $f(t) = 1$.

Kőnig és Rados tételének érdekes speciális esete a következő: Tekintsünk egy legfeljebb tízjegyű N pozitív egész számot úgy, hogy az utolsó számjegye 1-es, a többi számjegy pedig mind 0-s vagy 1-es. Most tekintsük ugyanezt a számalakot kettes, hármas, ..., kilences számrendszerben is. Jelölje μ azt, hogy ezen kilenc szám közül hány darab osztható 11-gyel. Jelölje továbbá a

számjegyekből a fentiek szerint készített 9×9 méretű mátrix rangját r. Állítás: $\mu + r = 10$, ha sem N nem osztható 11-gyel, sem a számjegyeinek összege; ha mindkét oszthatóság fennáll, akkor $\mu + r = 8$, egyébként pedig $\mu + r = 9$.

Példa: $N = 1001001001$. Ezt a számalakot 2-es, 3-as, ...,9-es számrendszerben értve és visszaírva 10-es számrendszerbe, továbbá prímhatvány-tényezőkre bontva ezeket kapjuk:

$$\begin{aligned}
1 + 2^3 + 2^6 + 2^9 &= 3^2 \cdot 5 \cdot 13585 \\
1 + 3^3 + 3^6 + 3^9 &= 2^3 \cdot 5 \cdot 7 \cdot 73 \\
1 + 4^3 + 4^6 + 4^9 &= 5 \cdot 13 \cdot 17 \cdot 241 \\
1 + 5^3 + 5^6 + 5^9 &= 2^2 \cdot 3^2 \cdot 7 \cdot 13 \cdot 601 \\
1 + 6^3 + 6^6 + 6^9 &= 7 \cdot 13 \cdot 31 \cdot 37 \cdot 97 \\
1 + 7^3 + 7^6 + 7^9 &= 2^4 \cdot 5^2 \cdot 13 \cdot 43 \cdot 181 \\
1 + 8^3 + 8^6 + 8^9 &= 3^3 \cdot 5 \cdot 13 \cdot 19 \cdot 37 \cdot 109 \\
1 + 9^3 + 9^6 + 9^9 &= 2^2 \cdot 5 \cdot 41 \cdot 73 \cdot 6481
\end{aligned}$$

Ezen számok egyike sem osztható 11-gyel.

A megfelelő mátrix ez:

$$\begin{bmatrix}
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1
\end{bmatrix}$$

Ennek a mátrixnak az összes egész számok gyűrűjében értelmezett determinánsa 0, de ha az utolsó sort és az utolsó oszlopot elhagyjuk, akkor a determináns 2 lesz. Mindazonáltal modulo 11 értelmezve a mátrix rangja 9. Tehát most $\mu + r = 0 + 9 = 9$. Ugyanakkor $N = 1001001001 = 7 \cdot 11 \cdot 13 \cdot 101 \cdot 9901$, és N számjegyeinek összege 4.

Végezetül megadjuk Kőnig és Rados tétele általánosításának egy bizonyítását. Rögzített tehát egy $p \geq 3$ prímhatvány, és tekintjük a p-elemű számtesten értelmezve az

$$f(x) = a_0 + a_1 x + \ldots + a_{p-2} x^{p-2}$$

polinomot, ahol $a_0 \neq 0$ és az $a_1, \ldots, a_{p-2}$ testelemek között is legalább egy nemnulla van. A polinom foka tehát legalább egy és legfeljebb $p - 2$. Nyilván 0 nem gyöke a polinomnak. A nemnulla testelemek közül még legalább egynek kell lenni, ami nem gyök, hiszen a gyökök darabszáma legfeljebb a polinom

foka. Soroljuk fel a számtest nemnulla elemeit az $x_1, x_2, \ldots, x_{p-1}$ sorrendben, ahol hátul vannak a polinomgyökök. Ezekből a testelemekből készítsük el az úgynevezett *Vandermonde*-féle mátrixot, azaz azt a $(p-1) \times (p-1)$ méretű V mátrixot, melyben a k-adik sor j-edik eleme x_j^{k-1}. Legyen továbbá A az a $(p-1) \times (p-1)$ méretű mátrix, melyben az i-edik sor k-adik eleme a_{i+k-2} ahol $a_{p-1} = a_0$, $a_p = a_1$, $a_{p+1} = a_2$, ..., $a_{2p-4} = a_{p-3}$. Vegyük észre, hogy ez a mátrix a Kőnig–Rados-tétel eredeti kimondásában szereplő mátrixtól csak annyiban különbözik, hogy a sorok permutálva vannak. Tehát az A mátrix rangja is r_f. Azt kell megmutatnunk hogy a polinom nemnulla nemgyökeinek a darabszáma is éppen r_f.

A bizonyítás kulcsa az az észrevétel, hogy az AV mátrixszorzat speciális alakú. Az világos, hogy az AV szorzat első sorának j-edik eleme éppen $f(x_j)$. *Fermat* híres „kis" tétele miatt pedig mindegyik $x_j^{p-1} = 1$. Ezért az AV mátrix második, harmadik, ..., utolsó soraiban a j-edik helyen álló elemek szorzata éppen x_j^{-1}-szerese a felette álló mátrixelemnek. Tehát ha valamely x_j gyöke a polinomnak, akkor az AV szorzatban az egész j-edik oszlop csupa nulla.

Tekintettel az ismert tényre, hogy a Vandermonde-mátrix invertálható, azt kapjuk, hogy az AV mátrix rangja is r_f. Itt tartunk tehát: a polinom nemnulla nemgyökeinek darabszáma legalább r_f.

Hagyjuk el az AV mátrixból a csupa nulla oszlopokat és a mátrix aljáról ugyanannyi darab sort. Jelölje U a megmaradt négyzetes mátrixot. A bizonyítás befejezéséhez elegendő azt megmutatnunk, hogy U determinánsa nem nulla.

Az U mátrix első sorát tekintve világos, hogy

$$\det(U) = \prod_{f(x_j) \neq 0} f(x_j) \cdot \det(W)$$

ahol a W mátrix i-edik sorának k-adik eleme éppen x_k^{1-i}. Mivel W is egy Vandermonde-mátrix, készen vagyunk.

Köszönetnyilvánítás: Hála illeti Csizmadia Ákost, aki a múzeális értékű Raussnitz-cikket beszerezte.

Irodalom

[1] Raussnitz Gusztáv: *A felsőfokú kongruenciák elméletéhez*, Mathematikai és Természettudományi Értesítő I (1882/83) 296–308. oldalak.