

$$P = 500 \text{ gr.-ból } r = 0^{\text{mm}}.480,$$

és

$$P = 1000 \text{ gr.-ból } r = 0^{\text{mm}}.488$$

eredményeket találunk.

Egy második próba végett oly adatokból számítván, melyek $p=0.1$ túlsúlylyal tett észleletekből nyerettek, $\theta=0^{\text{mm}}.000020$, $r=0^{\text{mm}}.45$ találatott, mely eredmények az előbbiekkal igen jól egyeznek.

A TÖBB ISMERETLENT TARTALMAZÓ ELSŐFOKÚ CONGRUENTIA-RENDSZER ÁLTALÁNOS ELMÉLETE.

König Gyulától.

I.

A »Disquisitiones arithmeticae«, GAUSS ez alapvető munkája az egyetlen, mely az itt részletesen kifejtendő elméletet érinti. »E fejezet azonban,« — ezt olvassuk ott *) — »ha teljes szigorral akarnók a részleteket előterjeszteni, túlságos terjedelmet nyerne; minthogy azonban itt nem is feladatunk, hogy mindent kimerítsünk, hanem csak az, hogy a fontosabbakat előadjuk, jelenleg csak néhány megjegyzésre szorítkozom, és a dolog részletes tárgyalását fönn tartom magamnak más alkalomra.« GAUSS azonban e tárgyra többé soha sem tért vissza, és így a számelméletnek aránylag elemi részében hézag maradt, mely eddig nincs betöltve. Így történt, hogy a későbbi tan- és kézikönyvek (még SERRET-é is) a GAUSS által adottaknak reproductiójára szorítkoznak. Midőn ezeket saját tankönyvembe (»Bevezetés a felsőbb algebrába« 44 l.) fölvettem, részletesebben foglalkoztam e problémával, mely lényegére nézve a következő két föladatot foglalja magában: meghatározni a megoldás *lehetőségének* általános föltételét, és a lehetőség esetében meghatározni a különböző *gyökrendszert* és e gyökrendszerek *számát*. GAUSS maga csak arra szorítkozott, hogy kimutassa miként lehet az egyszerűbb esetekben, ép úgy mint az egyenleteknél, az adott rendszerből oly congruentiát szerkeszteni, mely csak az egyik ismeretlent tartalmazza.

*) Carl Friedrich Gauss Werke, 1. Band pag. 27.

előbb, legyen D . A tárgyalás különböző eredményekre fog vezetni, a szerint mint D és M relativ törzsszám, vagy pedig D és M -nek közös osztója van, vagy végre D az M többsége. Vizsgáljuk ez eseteket külön.

Első eset. A rendszer determinánsa és a modulus viszonylagos törzsszám. — Ekkor bármelyik x_i ismeretlen meghatározására a D determinánsnak

$$A_{1i}, A_{2i}, \dots, A_{ni}$$

által jelölt aldeterminánsait képezzük, ezekkel rendre megszorozzuk az 1-ső, 2-ik, ... n -ik congruenciát és összeadunk. A determinánsok ismert tulajdonságai alapján az eredmény:

$$Dx_i \equiv A_{1i}k_1 + A_{2i}k_2 + \dots + A_{ni}k_n, \text{ (mod. } M\text{)}. \quad (2.)$$

vagy rövidebben írva:

$$Dx_i \equiv K_i, \text{ (mod. } M\text{)}.$$

A jelen esetben, hol D és M relativ törzsszám, a congruentia mindig megoldható, és így minden x számára egy meghatározott értéket nyerünk. Az eddigiekből azonban csak azt tudjuk, hogy az (1.) minden lehető gyökrendszere a (2.)-ében is bennfoglaltatik, de megfordítva lehetséges volna, hogy a (2.) által adott gyökrendszer nem elégíti ki az (1.) alatti rendszert. Hogy ez nem áll, arról közvetlenül meggyőződünk a (2.)-ből nyert x értékek helyettesítése által. Ezek a következők: *)

$$x_i \equiv D^{\varphi(M)-1} K_i,$$

hol $\varphi(M)$ az M -nél kisebb és ehhez viszonylagos törzsszámok számát jelenti. Ezeknek helyettesítése az (1.) alatti rendszer, mondjuk, r -edik egyenletében valóban helyes eredményt ad. Ez ugyanis:

$$D^{\varphi(M)-1}(a_{r1}K_1 + a_{r2}K_2 + \dots + a_{rn}K_n) \equiv K_r \text{ (mod. } M\text{)}.$$

Ha tekintetbe vesszük, hogy

$$K_1 = A_{11}k_1 + A_{12}k_2 + \dots + A_{1n}k_n$$

$$K_2 = A_{21}k_1 + A_{22}k_2 + \dots + A_{2n}k_n$$

$$\dots \dots \dots \dots \dots \dots \dots \dots \dots \dots$$

$$K_n = A_{n1}k_1 + A_{n2}k_2 + \dots + A_{nn}k_n$$

a zárjelben álló kifejezés, az A -k aldetermináns jellegét tekintetbe véve, nem más mint Dk_r ; minthogy pedig FERMAT tétele szerint $D^{\varphi(M)} \equiv 1 \text{ (mod. } M\text{)}$, az egész baloldalon álló kifejezés értéke valóban k_r lesz.

*) A Fermat-féle tétel mutatja, hogy valóban ezen x értékek a (2.) alatti congruenciák megoldásai.

Igy tehát ezen első esetben a (2.) alatt foglalt, egy-egy ismeretlent tartalmazó congruentiák adják az (1.) rendszernek teljes megoldását. Az adott congruentia-rendszernek tehát, midőn a rendszer determinánsa és a modulus viszonylagos törzsszám, egyetlen egy gyökrendszer felel meg.

Ha a modulus törzsszám, akkor D ehhez vagy relativ törzsszám, vagy pedig ennek többsége, tehát congruens 0 -sal; látni fogjuk, hogy ezen utóbbi esetben a congruentiák baloldalán álló lineár függvények nem függetlenek, és így az n congruentia vagy tulajdonképen csak $n-1$, vagy pedig egymásközt ellenmondó, és így kijelenthetjük, hogy n független congruentiából álló rendszernek, ha a modulus törzsszám, egy és csak egy megoldása van.

Most mindenekeelőtt a $D \equiv 0 \pmod{M}$ feltétel jelentőségét akarjuk vizsgálni a congruentia-rendszerre nézve.

4. A második esetünk lesz az, hogy a rendszer determinánsa a modulus többsége, azaz $D \equiv 0 \pmod{M}$. Midőn a rendszer determinánsa eltűnik $\pmod{M}$, meglehet, hogy ugyanez történik még a determinánsból képezhető minden $n-1, n-2, \dots$ fokú aldeterminánssra nézve is. Az ezeknél fennforgó viszonyoknak fontos szerepe lévén, ezeket általánosságban az által akarjuk pontosan megállapítani, hogy az m -edfokú aldeterminánsok legyenek az elsők, melyek közt $\pmod{M}$ a 0 -tól különbözők is találatnak, míg az $m+1, m+2, \dots$ fokúak mindannyian eltűnnek. A legegyszerűbb eset lesz $m=n-1$, hol D zérus ugyan, de már az A_{ik} által jelölt $n-1$ -edfokú aldeterminánsok közt találatnak a 0 -tól különbözők. Az ily el nem tűnő, m -edfokú aldeterminánsnak az ismeretlenek és congruentiák kellő rendezése után mindig vehetjük ezt:

$$\begin{vmatrix} a_{11}, a_{12}, \dots, a_{1m} \\ a_{21}, a_{22}, \dots, a_{2m} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{m1}, a_{m2}, \dots, a_{mn} \end{vmatrix}$$

Ha ezt egy az eredeti determinánsból vett tetszőleges sor is p . az $m+1$ oszlop által $m+1$ fokúvá teszszük, akkor feltevésünk szerint ez

$$\begin{vmatrix} a_{12}, a_{12}, \dots, a_{1m}, a_{1,m+1} \\ a_{21}, a_{22}, \dots, a_{2m}, a_{2,m+1} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_{m1}, a_{m2}, \dots, a_{mm}, a_{m,m+1} \\ a_{s1}, a_{s2}, \dots, a_{sm}, a_{s,m+1} \end{vmatrix}$$

mindig eltűnik, bárminő értéke legyen s -nek $m+1$ -től u -ig. De akkor az 1. alatt kifejtett tétel értelmében 0-t kapunk még akkor is, ha az $m+1$ -ső oszlopban az a mennyiségek helyébe az u -kat írjuk. Ha ezt megteszszük, ha továbbá tekintetbe vesszük azt, hogy s fölvehet minden értéket $m+1$ -től n -ig, akkor nyerünk $n-m$ egyenletet, mely egymásután kifejezi az u_{m+1} , u_{m+2} , ... és u_n -t az u_1 , u_2 , ... u_n segítségével. Ezen egyenletek:

$$C_{s1}u_1 + \dots + C_{sm}u_m + C_{ss}u_s \equiv 0 \\ (s=m+1, \dots, n)$$

hol az u_s együttthatója előbbi megállapodásunk szerint a 0-tól különbözők.

Látjuk tehát, hogy az m -ed fokú alldeterminánsok lévén az első, melyek nem tűnnek el mindannyian, az egyenletek közül csak m marad meg, mint egymástól független. A többi lineár függvény az első m által kifejezhető. Ha az u_k helyébe az ő értékeit teszszük: a k mennyiségeket, kell hogy az így nyert alakzatok identitások legyenek. Így nyerjük tehát a congruentia-rendszer megoldhatására vonatkozó föltételeket, még pedig ha ezek ki vannak elégítve, csak m maradékegyenletet kell fölvennünk és így az n ismeretlen közül $n-m$ értéke tetszőlegesen lesz megállapítható. Föladatunk így át van alakítva egy másikba, mely már azért is egyszerűbb, mert a congruentiák és ismeretlenek száma kisebb; de a melyben még továbbá nem lehet $\equiv 0 \text{ mod. } M$, hanem vagy relatív törzsszám ehhez, vagy pedig, és ez a végül tárgyalandó harmadik eset: M és D' -nek van közös osztója: δ .

5. Ha a rendszer determinánsának (D) és a modulusának (M) legnagyobb közös osztója δ legyen

$$D = D'\delta, \quad M = M'\delta$$

hol D' és M' már is viszonylagos törzsszámok.

Minden gyökrendszer, mely az adott congruentiákat megoldja $\text{mod. } M$, még minden oly modulusra nézve is ad megoldást, mely ennek tényezője, p . M -re nézve is. Így tehát minden lehetséges gyökrendszer benn foglaltatik a következőkben,

$$x_1 \equiv \alpha_1, \quad x_2 \equiv \alpha_2, \quad \dots, \quad x_n \equiv \alpha_n \pmod{M'} \quad (3.)$$

melyet nyerünk, ha az adott congruentiákat megoldjuk $\text{mod. } M'$. A congruentia-rendszer bármely megoldása $\text{mod. } M$ szükségkép összeesik evvel, mihelyt a számokat csak $\text{mod. } M'$ tekintjük, és így egy tetszőleges gyökrendszer alakja a következő lesz:

$$\begin{aligned} x_1 &\equiv \alpha_1 + y M' \\ x_2 &\equiv \alpha_2 + y_2 M' \\ &\dots \dots \dots \\ x_n &\equiv \alpha_n + y_n M' \end{aligned} \quad (\text{mod. } M)$$

hol már egy maradékú értékeket nyerünk, ha valamely y az $\frac{M}{M'} = \delta$ többsével növekszik. Az y -ok meghatározása tehát csak *mod. δ* kívántatik meg és föladatunk meg van oldva, ha az ily meghatározást kivittük. Ez pedig ismét egy congruentia-rendszer megoldása által történik. Ha ugyanis ezen x értékeket az (I.) rendszerbe helyettesítjük, a következőket nyerjük

$$\begin{aligned} M'(a_{11}y_1 + a_{12}y_2 + \dots + a_{1n}y_n) &\equiv k_1 - a_{11}\alpha_1 - a_{12}\alpha_2 - \dots - a_{1n}\alpha_n \\ M'(a_{21}y_1 + a_{22}y_2 + \dots + a_{2n}y_n) &\equiv k_2 - a_{21}\alpha_1 - a_{22}\alpha_2 - \dots - a_{2n}\alpha_n \quad (\text{mod. } M) \\ &\dots \dots \dots \\ M'(a_{n1}y_1 + a_{n2}y_2 + \dots + a_{nn}y_n) &\equiv k_n - a_{n1}\alpha_1 - a_{n2}\alpha_2 - \dots - a_{nn}\alpha_n \end{aligned}$$

Itt nemcsak a baloldalon lehet M' -vel osztani, de a jobb oldalon álló kifejezésekben is, hisz az α -k épen úgy lettek meghatározva, hogy ezek eltűnjenek *mod. M'* . — Az M' -mel osztva, természetesen a modulus is, az y -ok meghatározására a következő congruentia-rendszert nyerjük:

$$\begin{aligned} a_{11}y_1 + a_{12}y_2 + \dots + a_{n1}y_n &\equiv l_1 \\ a_{21}y_1 + a_{22}y_2 + \dots + a_{n2}y_n &\equiv l_2 \\ &\dots \dots \dots \\ a_{n1}y_1 + a_{n2}y_2 + \dots + a_{nn}y_n &\equiv l_n \end{aligned} \quad (\text{mod. } \delta) \quad (4.)$$

E (4.) alatti rendszer ismét egyszerűsítést foglal magában, a mennyiben a modulus kisebb és kevesebb törzstényezőt tartalmaz, de egyszersmind át vezet a második esetre, mert itt ismét a determináns a modulusnak többsége. A második esetnek megfelelő tárgyalás ismét kisebbíti a congruentiák számát, tehát ismét egyszerűbb alakokra vezet; míg a tárgyalás be van fejezve, mihelyt az első esetre akadunk, minek természetesen előbb-utóbb meg kell történie.

6. Az eddigiek a gyakorlati eljárásra szükséges útmutatást már magukban foglalják; tárgyaljuk az itt adott módszerek segítségével a Gauss által a »Disquisitiones«-ben adott példát. Legyen:

$$\left. \begin{aligned} 3x + 5y + z &\equiv 4 \\ 2x + 3y + 2z &\equiv 7 \\ 5x + y + 3z &\equiv 6 \end{aligned} \right\} \quad (\text{mod. } 12).$$

A rendszer determinánsa:

$$\begin{vmatrix} 3, & 5, & 1 \\ 2, & 3, & 2 \\ 5, & 1, & 3 \end{vmatrix} \equiv \begin{vmatrix} 0 & 0 & 1 \\ 8 & 5 & 2 \\ 8 & 10 & 3 \end{vmatrix} \equiv 4 \pmod{12.}$$

A determináns és modulus legnagyobb közös osztója 4; megoldjuk tehát először a congruenciákat, mod. 3. Ha x, y, z helyett α, β, γ -t írunk és az együtthatókat egyszerűsítjük, lesznek ezek:

$$\left. \begin{aligned} 2\beta + \gamma &\equiv 1 \\ 2\alpha + \dots + 2\gamma &\equiv 1 \\ 2\alpha + \beta + \dots &\equiv 0 \end{aligned} \right\} \pmod{3.}$$

És így

$$\alpha \equiv 2, \quad \beta \equiv 2, \quad \gamma \equiv 0, \pmod{3.}$$

Igy tehát most

$$\left. \begin{aligned} x &\equiv 2 + 3\xi \\ y &\equiv 2 + 3\eta \\ z &\equiv 3\zeta \end{aligned} \right\} \pmod{12.}$$

Ezen értékeket az adott rendszerbe helyettesítve, lesz:

$$\left. \begin{aligned} 9\xi + 3\eta + 3\zeta &\equiv 0 \\ 6\xi + 9\eta + 6\zeta &\equiv 9 \\ 3\xi + 3\eta + 9\zeta &\equiv 6 \end{aligned} \right\} \pmod{12.}$$

Itt valóban mindenütt lehet osztani 3-mal és lesz:

$$\left. \begin{aligned} 3\xi + \eta + \zeta &\equiv 0 \\ 2\xi + 3\eta + 2\zeta &\equiv 3 \\ \xi + \eta + 3\zeta &\equiv 2 \end{aligned} \right\} \pmod{4.}$$

Itt a determináns:

$$\begin{vmatrix} 3, & 1, & 1 \\ 2, & 3, & 2 \\ 1, & 1, & 3 \end{vmatrix} \equiv 0, \pmod{4.}$$

Az A_{33} aldetermináns $\equiv 3$ lévén, megfelel a föltételnek és így kimondhatjuk, hogy:

$$\begin{vmatrix} 3, & 1, & u_1 \\ 2, & 3, & u_2 \\ 1, & 1, & u_3 \end{vmatrix} \equiv 0, \pmod{4.},$$

vagyis, a mint a helyettesítés mutatja:

$$3u_1 + 2u_2 + 3u_3 \equiv 0 \pmod{4.}$$

Congruentia-rendszerünk tehát:

$$\begin{aligned} 3\xi + \eta &\equiv -\zeta \\ 2\xi + 3\eta &\equiv 3-2\zeta \end{aligned} \quad (\text{mod. } 4.)$$

Evvel azonban már befejeztük a megoldást, mert itt a determináns $3 \cdot 3 - 2 \cdot 1 = 7$ relativ törzsszám a modulushoz. A ζ tetszőleges lévén, ξ , η , ζ -ra nézve négy gyökrendszert nyerünk, és így ugyanannyit az x , y , z -re is. Lesz:

$$\left. \begin{aligned} \zeta &\equiv 0, 1, 2, 3 \\ \xi &\equiv 3, 0, 1, 2 \\ \eta &\equiv 3, 3, 3, 3 \end{aligned} \right\} (\text{mod. } 4.)$$

Ezt az előbb nyert x , y , z -be helyettesítve, lesz:

$$\left. \begin{aligned} x &\equiv 2, 5, 8, 11 \\ y &\equiv 11, 11, 11, 11 \\ z &\equiv 3, 6, 9, 0 \end{aligned} \right\} (\text{mod. } 12.)$$

Látni, hogy az η értékét nem lehetett volna tetszőlegesnek venni; ez mindig egy és ugyanaz. Ennek oka abban rejlik, hogy a ξ , η , ζ -ra vonatkozó congruentia rendszer determinánsából az η együtthatóinak kihagyása által nem lehet oly másodfokú aldeterminánst kapni, mely nem többese a modulusnak, és így η -t nem is lehet tetszőleges értéknek megahagyni. *)

Egy az itt adottól eltérő módszer, mely — különösen a gyökrendszerek számára vonatkozólag — elméletileg jobb áttekintést ad, gyakorlatilag pedig szintén igen kényelmes, — több, magasabb fokú congruentiákra vonatkozó alkalmazással együtt, — egy legközelebbi második közleménynek marad föntartva.

EGY TÉTEL A DETERMINÁNSOKRÓL.

Scholtz Ágoston, budapesti ev. gymnasiumi igazgatótól.

A kérdéses tételt

$$(\alpha\beta\gamma) \cdot (\alpha'\beta'\gamma') - (\alpha\beta'\gamma) \cdot (\alpha'\beta\gamma') = \begin{vmatrix} \xi_{\alpha\beta} & \eta_{\alpha\beta} & \zeta_{\alpha\beta} \\ \xi_{\alpha'\beta'} & \eta_{\alpha'\beta'} & \zeta_{\alpha'\beta'} \\ \xi_{\gamma\gamma'} & \eta_{\gamma\gamma'} & \zeta_{\gamma\gamma'} \end{vmatrix} \quad (1.)$$

*) Fölhasználok ezt az alkalmat, hogy »Bevezetés a felsőbb algebra» című könyvem idevágó fejezetére nézve egy szükséges helyreigazítást közöljek. Az e tárgyra vonatkozólag adott példában (45 lap. 4 sor alulról) z helyett $-z$ olvasandó, és így a z -nek az utolsó sorban foglalt értékei szintén — előjellel veendőek