

A RECIPROCITÁS TÉTELE A NÉGYZETES MARADÉKOK ELMÉLETÉBEN.

KÖNIG GYULA r. tagtól.

A következőkben a reciprocitás tételének oly bizonyítását kívánom bemutatni, mely — minden más segédeszköz kizárásával — csakis a LEGENDRE-, illetőleg JACOBI-féle jelnek közvetlenül értelmezéséből folyó tulajdonságait használja föl. Evvel az új bizonyításnak az ismert bizonyítások hosszú sorával szemben nemcsak egész külön szerepe jut, de formai menete is meg van állapítva. Mert a hol valamely műveleti jel értelmezéséből e jel általános tulajdonságait fejtjük ki, ez lényegében másképp, mint teljes inductióval nem történhetik. A közlendő bizonyítás csakugyan a teljes inductión alapszik, ép úgy mint GAUSS első bizonyítása, melyet a «Disquisitiones arithmeticae» IV. sectiojában közölt; de *nem használja Gauss ama híres lemmáját*, mely szerint ha p egy $8n+1$ alakú törzsszám, mindig találhatni egy másik $2\sqrt{p+1}$ -nél kisebb törzsszámot, q -t, melyre nézve p nem maradék.

E tétel forrása valójában a quadratikus alakok elméletének mélyeiben keresendő; elemi bizonyítása még GAUSS-nak is igen nagy nehézségeket okozott, «demonstratio satis diu operam nostram elusit» — mondja ő maga az említett helyen; míg KRONECKER* a következő szavakkal jellemzi: «Jene merkwürdige und scharfsinnige Deduction, welche ganz direct mit Überwindung aller Schwierigkeiten auf das Ziel losgehend fast wie eine Art Kraftprobe GAUSS'schen Geistes erscheint.»

A matematikus közvélemény, — a mennyire tudom — ezen erőpróbát a reciprocitási tétel inductiv bebizonyításánál elkerülhetetlennek tartotta; és már ezért is figyelemre méltók a következő

* Mon. Ber. d. K. p. Akad. der Wiss. zu Berlin, 1876, pag. 341.

tárgyalások. De ettől el is tekintve, fontos az aritmetika rendszerére nézve azon eredmény, hogy a reciprocitás tétele kizárólag a LEGENDRE-féle jel értelmezésének következménye és a felsőbb fokú congruentiák elméletének semmiféle legegyszerűbb eredményét sem tételezi föl, ide értve a FERMAT-féle congruentiát és az EULER-féle kriteriumot is.

Hogy ez teljes világosságra jusson, mindenekelőtt összeállítom a kizárólag alkalmazandó tételek sorozatát.

*

A tárgyalás előzményei. Ha p páratlan törzsszám és a a p -vel nem osztható, az $\left(\frac{a}{p}\right)$ jel jelentsen $+1$ vagy -1 -et, a mint az $x^2 \equiv a \pmod{p}$ congruentiának van gyöke, vagy nincsen; ha pedig a osztható p -vel, $\left(\frac{a}{p}\right)$ legyen 0 . Az így értelmezett LEGENDRE-féle jel szorzási szabálya

$$\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

mely a definitio közvetlen következménye, ha a és b maradékok; míg a többi esetben még fölhasználandó azon eredmény, hogy x -szel együtt az ax is a teljes maradékrendszert futja át.

E megfontolások mellesleg azt is kiadják, hogy a 0 kizárása után a maradékok és nem maradékok száma egyenlőképen $\frac{p-1}{2}$. A JACOBI-féle jel ennek csak formális általánosítása; ha ugyanis P páratlan, pozitív egész szám — tovább itt nem megyünk —, és törzstényezőkre bontott alakja $P = p_1 p_2 \dots p_r$ akkor

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \dots \left(\frac{a}{p_r}\right)$$

melyre nézve tehát a szorzási szabály ugyanaz mint előbb.

Az előzményekhez sorolom végre a -1 maradékjellegére vonatkozó tételt, mely szerint:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \varepsilon_p;$$

a következőkben ugyanis rövidség kedvéért $(-1)^{\frac{p-1}{2}}$ helyet ε_p -t írunk. E tételnek egyik EULER-től származó, és a «Disquisitiones» 109. cikkében előadott bizonyítása csakugyan kizárólag a most jellemzett elemi gondolatkörben marad. Hogy az olvasó erről magának egész kényelmesen tiszta képet szerezhessen, e bizonyítást, röviden és a mi célunkhoz képest szövegezve, itt fölveszem.

A p páratlan törzsszám maradékait:

$$a_1, a_2, \dots, a_{\frac{p-1}{2}}$$

két osztályba sorozzuk.

Az első osztályba tartozzanak azok, melyekre nézve

$$a^2 \equiv 1 \pmod{p}$$

De $a^2 - 1 = (a - 1)(a + 1)$ csak úgy osztható p -vel, ha vagy $a - 1$ vagy $a + 1$ osztható, vagyis csak akkor, ha $a \equiv 1$, vagy $a \equiv -1 \pmod{p}$. Ezen első osztályba tehát egy vagy két maradék tartozik, a mint -1 maradék vagy sem; mert hisz $+1$ mindig maradék.

A második osztályba tartozzanak az összes többi maradékok. Ezen osztályban minden a maradékhoz egy és csak egy társát b -t lehet úgy meghatározni, hogy $ab \equiv 1 \pmod{p}$; b ekkor különbözik az a -tól, mert különben a az első osztályba tartoznék, és b -nek társa ismét a . A másodosztályú maradékok tehát párokba sorakoznak, és számuk mindig páros.

Ha most már $p = 4n + 1$, és így $\frac{p-1}{2}$, az összes maradékok száma páros, kell hogy az első osztályú maradékok száma is ilyen legyen, azaz -1 maradék.

Ha pedig $p = 4n + 3$, és így $\frac{p-1}{2}$ páratlan, kell hogy az első osztályú maradékok száma is páratlan legyen, tehát -1 nem maradék. Ez pedig, mint ismeretes, a $\left(\frac{-1}{p}\right) = \varepsilon_p$ tétel tartalma.

E bevezetés után áttérek most már a tulajdonképeni tárgyra. A GAUSS első bizonyításától és DIRICHLET átdolgozásától (Crelle, Journal, 47. köt.) utunk lényegesen eltér, mert az előforduló törzsszámok jellege szerint egyáltalában nem kell különböző eseteket megkülönböztetni, hanem a reciprocitás tételét alkalmas módon egymástól független részlettételekre bontjuk, melyek vagy a teljes inductio segítségével igen könnyen bebizonyíthatók, vagy pedig a már nyert tételekből bizonyos megfordítások által keletkeznek.

1. tétel. Ha q és r két pozitív, páratlan törzsszám, és $q < r$, akkor, ha $\left(\frac{\varepsilon_q q}{r}\right) = 1$, egyszersmind $\left(\frac{r}{q}\right) = 1$.

Minthogy a tétel helyes a legkisebb törzsszámoknál, pl. azoknál, melyek 11-nél kisebbek, az általános bizonyítás úgy haladhat, hogy a tételt helyesnek véve az r -nél kisebb törzsszámok összeállítására, kimutatjuk, hogy akkor is helyes marad, ha valamely az r -nél kisebb törzsszámot magával az r -rel állítjuk össze.

A föltétel értelmében az

$$x^2 - \varepsilon_q q \equiv 0 \pmod{r}.$$

congruentia megoldható; van tehát egy pozitív és r -nél kisebb megoldása a és evvel együtt $r - a$ szintolyan; ezek közül az egyik páros, a másik páratlan. A páros neve legyen ξ , és így

$$\xi^2 - \varepsilon_q q = r\varphi \tag{1}$$

hol φ mindenesetre páratlan, mert ξ páros; pozitív, mert még akkor is, midőn $\varepsilon_q = 1$, és a baloldaton különbség áll, e különbség negatív értékéből az következne, hogy $q - \xi^2$ pozitív, tehát a q -nál kisebb, és mégis a q -nál nagyobb r -rel osztható volna. Továbbá

$$r\varphi \leq \xi^2 + q < (r-1)^2 + r$$

és ebből, mint rögtön látni

$$\varphi < r.$$

a) Ha már most φ nem osztható q -val, akkor φ minden π törzstényezőjére nézve

$$\left(\frac{\varepsilon_q q}{\pi_i}\right) = 1$$

és minthogy $\pi_i \leq \varphi < r$ a föltevés értelmében

$$\left(\frac{\pi_i}{q}\right) = 1,$$

vége még szorozva $\left(\frac{\varphi}{q}\right) = 1$. Másrészt azonban az (1) alapidentitásból $\left(\frac{r\varphi}{q}\right) = 1$ és így csakugyan

$$\left(\frac{r}{q}\right) = \left(\frac{\varphi}{q}\right) = 1$$

b) Ha pedig φ osztható q -val, legyen $\varphi = q\psi$; akkor (1) szerint ξ is osztható, legyen $\xi = q\eta$, akkor (1)-ből lesz

$$\begin{aligned} q^2\eta^2 - \varepsilon_q q &= r q \psi \\ \text{vagy } \varepsilon_q q \text{ -val osztva} \quad \varepsilon_q q \eta^2 - 1 &= \varepsilon_q r \psi \end{aligned} \quad (2)$$

hol ψ ismét r -nél kisebb pozitív és páratlan, de q -val többé nem osztható, a mint azt a baloldal közvetlenül mutatja. Ezen identitás ismét mutatja, hogy $\varepsilon_q q$ maradék a ψ minden π_i osztójára; tehát $\left(\frac{\varepsilon_q q}{\pi_i}\right) = 1$, és ebből föltevéseink szerint $\left(\frac{\pi_i}{q}\right) = 1$, vagy végre szorozva $\left(\frac{\psi}{q}\right) = 1$.

Másrészt pedig a (2)-ből

$$r\psi \equiv -\varepsilon_q \pmod{q}$$

tehát $\left(\frac{r\psi}{q}\right) = 1$, és ebből $\left(\frac{r}{q}\right) = \left(\frac{\psi}{q}\right) = 1$, a mivel tételünket a második esetben is bebizonyítottuk.

2. tétel. Ha q és r két pozitív törzsszám, és $q < r$, akkor ha $\left(\frac{q}{r}\right) = 1$, egyszersmind $\left(\frac{\varepsilon_r r}{q}\right) = 1$.

Teljesen ugyanazon gondolatmenetet használva, mint az első tételnél, legyen a most megoldhatónak állított

$$x^2 - q \equiv 0 \pmod{r}$$

congruentia pozitív, páros és r -nél kisebb gyöke ξ , akkor

$$\xi^2 - q = r\varphi \quad (3)$$

és φ ismét pozitív, páratlan és r -nél kisebb.

a) Ha most már φ nem osztható q -val, akkor φ minden π_i törzstényezőjére nézve $\left(\frac{q}{\pi_i}\right) = 1$, és minthogy ismét a tételt érvényesnek veszszük már az r -nél kisebb törzsszámokra $\left(\frac{\varepsilon_{\pi_i} \pi_i}{q}\right) = 1$; és végre összeszorozva $\left(\frac{\varepsilon_{\varphi} \varphi}{q}\right) = 1$; mert hiszen ismeretes, hogy

$$\varepsilon_a \varepsilon_b = \varepsilon_{ab}.$$

Másrészt azonban a (3) alapidentitásból

$$\left(\frac{r\varphi}{q}\right) = 1,$$

és így

$$\left(\frac{\varepsilon_r r}{q}\right) = \left(\frac{\varepsilon_r \varphi}{q}\right)$$

Ha $q \equiv 1 \pmod{4}$, akkor $\pm \varphi$ egyszerre maradék vagy nem maradék, tehát ekkor csakugyan $\left(\frac{\varepsilon_r r}{q}\right) = 1$, mert $\left(\frac{\varepsilon_{\varphi} \varphi}{q}\right) = 1$.

Ha pedig $q \equiv 3 \pmod{4}$, akkor $r\varphi = \xi^2 - q \equiv 1 \pmod{4}$ és így $\varepsilon_{r\varphi} = 1$, tehát $\varepsilon_r = \varepsilon_{\varphi}$, és így

$$\left(\frac{\varepsilon_r r}{q}\right) = \left(\frac{\varepsilon_{\varphi} \varphi}{q}\right) = 1,$$

a mi bebizonyítandó volt.

b) Ha pedig φ osztható q -val, akkor — ép úgy, mint az első tétel alkalmából — átmegyünk a

$$q\eta^2 - 1 = r\psi \quad (4)$$

identitáshoz. Ez is mutatja, hogy q maradék a ψ minden π_i törzstényezőjére nézve, vagyis $\left(\frac{q}{\pi_i}\right) = 1$, és ebből $\left(\frac{\varepsilon_{\pi_i} \pi_i}{q}\right) = 1$, vagy összeszorozva $\left(\frac{\varepsilon_{\psi} \psi}{q}\right) = 1$. Másrészt pedig

$$r\psi \equiv -1 \pmod{q}$$

azaz $\left(\frac{r\zeta^h}{q}\right) = \varepsilon_q$. Ebből ismét

$$\left(\frac{\varepsilon_r r}{q}\right) = \varepsilon_q \left(\frac{\varepsilon_r \zeta^h}{q}\right) = \left(\frac{\varepsilon_r \zeta^h}{q}\right)$$

a mi könnyen 1-nek bizonyul. Minthogy η páros most $r\zeta \equiv 3 \pmod{4}$ és $\varepsilon_{r\eta} = -1$, tehát $\varepsilon_{\eta} = -\varepsilon_r$, és így

$$\left(\frac{\varepsilon_r r}{q}\right) = \left(\frac{\varepsilon_r \zeta^h}{q}\right) = 1,$$

a mint állítottuk.

3. tétel. Ha q és r két pozitív törzsszám és $q < r$, akkor, ha $\left(\frac{\varepsilon_r r}{q}\right) = 1$, egyszersmind $\left(\frac{q}{r}\right) = 1$.

Föltételünk ismét azt jelenti, hogy az

$$x^2 - \varepsilon_r r \equiv 0 \pmod{q}$$

congruentia megoldható. Legyen a valamely páros gyöke, akkor $a + 2qu$ is olyan és

$$(a + 2qu)^2 - \varepsilon_r r = q\varphi,$$

hol φ páratlan, és ha csak u -t elég nagynak vesszük, pozitív.

Az u értékét most még úgy akarjuk megszabni, hogy a mindenesetre páratlan φ csupán az r -nél nagyobb törztényezőket tartalmazzon.

Hogy először is

$$\varphi = \frac{a^2 - \varepsilon_r r}{q} + 4au + 4qu^2$$

a q -val ne legyen osztható, elég lesz u -t úgy választani, hogy az

$$\frac{a^2 - \varepsilon_r r}{q} + 4au \equiv 1 \pmod{q} \quad (a)$$

congruentiának megfelelően, a mi mindenesetre lehetséges, mert hisz a nem osztható q -val.

Legyenek q kivételével $q_1, q_2, \dots$ az r -nél nem nagyobb törzsszámok teljes sorozata; ezek közül $q'_1, q'_2, \dots, r$ azok, me-

lyek $1 - \varepsilon_r r$ -ben nem fordulnak elő mint tényezők; ha ekkor u -t az

$$a + 2qu \equiv 1 \pmod{q_i'} \quad (b)$$

$(i=1, 2, \dots)$

congruentiáknak megfelelőleg választjuk, akkor

$$q\varphi \equiv 1 - \varepsilon_r r \pmod{q_i'},$$

és minthogy $1 - \varepsilon_r r$ nem osztható q_i' -vel, $q\varphi$ sem az.

Legyen továbbá a q_i törzsszámok sorából $q_1'', q_2'', \dots$ azon törzsszámok sorozata, melyek $1 - \varepsilon_r r$ -et osztják, de $4 - \varepsilon_r r$ -et nem osztják. Esetleg nincsenek ilyenek, és akkor a följáratandó föltételek kimaradnak egészen. Ha vannak, akkor az u -t még tovább alávétjük az

$$a + 2qu \equiv 4 \pmod{q_i''} \quad (c)$$

$(i=1, 2, \dots)$

congruentiáknak, és ekkor

$$q\varphi \equiv 4 - \varepsilon_r r \pmod{q_i''}$$

ismét mutatja, hogy φ nem lehet a q_i'' -vel osztható.

Ezek után r nél kisebb törzsszám már csak olyan maradhatott fönn, mely $1 - \varepsilon_r r$ -et és $4 - \varepsilon_r r$ -et is osztja, azaz a 3. Ha tehát a 3-ra vonatkozó föltétel nincs meg (a) vagy (b) vagy (c)-ben, akkor u választását újból megszorítjuk az

$$a + 2qu \equiv 0 \pmod{3} \quad (d)$$

congruentiával, és ekkor

$$q\varphi \equiv -r \pmod{3}$$

bizonyosan nem osztható 3-mal.

Hogy az (a), (b), (c) alatt foglalt elsőfokú congruentiák mind együttesen megoldhatók, igen egyszerűen belátható. Hisz a modulusok mind különböző törzsszámok, és az ismeretlen együtthatója mindig relatív törzsszám a modulushoz. E mellett u bármily nagy pozitív szám is lehet; tehát φ pozitív. Legyen most már az u így választott értéke mellett $\xi = a + 2qu$, a mi természetesen a -val együtt páros, erre nézve végre

$$\xi^2 - \varepsilon_r r = q\varphi, \quad (5)$$

hol tehát a φ -ben foglalt törzstényezők $\pi_1, \pi_2, \dots$ mindannyian r -nél nagyobbak,

Most ismét a φ minden törzstényezőjére nézve $\left(\frac{\varepsilon_r r}{\pi_i}\right) = 1$, és mint hogy itt $\pi_i > r$, az első tétel értelmében $\left(\frac{\pi_i}{r}\right)$, vagy összeszorozva $\left(\frac{\varphi}{r}\right) = 1$. De másrészt az (5) szerint $\left(\frac{q\varphi}{r}\right) = 1$ és így végre

$$\left(\frac{q}{r}\right) = \left(\frac{\varphi}{r}\right) = 1,$$

a mi bizonyítandó volt.

*

A *reciprocitás tétele* most már a II. és III. tétel egyszerű összeállításából ered. A II. szerint ugyanis, ha ismét $r > q$, abból, hogy $\left(\frac{q}{r}\right) = 1$ következik, hogy $\left(\frac{\varepsilon_r r}{q}\right) = 1$; a III. szerint pedig abból, hogy $\left(\frac{\varepsilon_r r}{q}\right) = 1$ ismét hogy $\left(\frac{q}{r}\right) = 1$; e kifejezések tehát vagy mindketten $+1$ -gyel, vagy mindketten -1 -gyel egyenlők; tehát

$$\left(\frac{\varepsilon_r r}{q}\right) = \frac{q}{r}$$

a mit még így is írhatunk

$$\left(\frac{r}{q}\right) \left(\frac{q}{r}\right) = \left(\frac{\varepsilon_r}{q}\right) = \left(\frac{\varepsilon_q}{r}\right) = (-1)^{\frac{q-1}{2} \frac{r-1}{2}}$$

a mi a reciprocitás tételének ismeretes alakja, és melyből mint-hogy q és r főcserélhetők, az $r > q$ megszorító föltétel is kiesett.

Hogy e tárgyalás végre teljes legyen, megjegyzem, hogy a 2 négyzetes jellegére vonatkozó tétel a reciprocitás tétele *után* — a mint ezt KRONECKER előadásában tette — két sorban el-intézhető, ha a JACOBI-féle jelt is használjuk. Lesz ugyanis,

minthogy, ha P páratlan, a P és $P-2$ számok közül az egyik mindig $4n+1$ alakú:

$$\left(\frac{2}{P}\right) = \left(\frac{-1}{P}\right) \left(\frac{P-2}{P}\right) = \left(\frac{-1}{P}\right) \left(\frac{P}{P-2}\right) = (-1)^{\frac{P-1}{2}} \left(\frac{2}{P-2}\right)$$

És ebből a reductiót folytatva:

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P-1}{2} + \frac{P-3}{2} + \dots + 1} = (-1)^{\frac{P^2-1}{8}}.$$

(A M. T. Akadémia III. osztályának 1895. nov. 18.-án tartott üléséből.)