GAUSS-EGÉSZEK ÉS DIRICHLET TÉTELE

KEITH KEARNES, KISS EMIL, SZENDREI ÁGNES

Második rész

Cikkünk első részében az elemrend és a körosztási polinomok fogalmára alapozva beláttuk, hogy ha n pozitív egész, akkor az $nk+1$ alakú számok halmaza, ahol $k = 1, 2, \ldots$, végtelen sok prímszámot tartalmaz. Most eszközeinket továbbfejlesztve az $nk-1$ alakú prímekről is belátjuk, hogy végtelen sokan vannak.

4. A körosztási polinom egy analogonja

A cikk második részében is rögzítjük az $n \geq 1$ egész számot, és végig használni fogjuk a komplex n-edik egységgyökök $\varepsilon_k = \cos(2\pi k/n) + i\sin(2\pi k/n)$ jelölését. Az $nk-1$ eset bizonyításában a cikk első részében definiált $\Phi_n(x)$ körosztási polinom helyett a következő polinomot fogjuk használni $n > 2$ esetén:

$$\Psi_n(x) = \prod_{\substack{1 \leq k < n/2 \\ (k,n)=1}} \big(x - 2\cos(2\pi k/n)\big)\,.$$

Mivel a $\cos(x)$ függvény a $[0, \pi]$ intervallumon szigorúan monoton, a képletben szereplő $2\cos(2\pi k/n)$ számok páronként különbözők.

4.1. Tétel. *Ha $n > 2$, akkor a következők teljesülnek.*

(1) $\Psi_n(x)$ *foka* $\varphi(n)/2$.
(2) $\Phi_n(x) = x^{\varphi(n)/2}\,\Psi_n(x + x^{-1})$.
(3) $\Psi_n(x)$ *egész együtthatós.*

Ezt a tételt egy öttagú feladatsorozattal bizonyítjuk.

4.2. Feladat. *Igazoljuk a 4.1. tétel* (1) *állítását.*

Megoldás. Az $[1, n-1]$ intervallum n-hez relatív prím egész számait párosíthatjuk a $k \leftrightarrow n-k$ megfeleltetéssel, hiszen $(k, n) = (n-k, n)$. Az $n > 2$ feltevés miatt n nem relatív prím n-hez, és ha $n/2$ egész, akkor $n/2$ sem az. Ezért $\Psi_n(x)$ képletében $\varphi(n)/2$ tényező szerepel, s így $\Psi_n(x)$ foka $\varphi(n)/2$. □

4.3. Feladat. *Igazoljuk, hogy $n > 1$ esetén $x^{\varphi(n)}\,\Phi_n(1/x) = \Phi_n(x)$.*

Megoldás. Mivel $\varepsilon_k^{-1} = \cos(2\pi k/n) - i\sin(2\pi k/n) = \varepsilon_{n-k}$, ezért az $x^{\varphi(n)}\,\Phi_n(1/x)$ polinomnak is gyöke mindegyik n-edik primitív egységgyök. A bizonyítandó egyenlőség mindkét oldalán $\varphi(n)$ fokú polinom szerepel, és most láttuk be, hogy van $\varphi(n)$ darab közös gyökük. Ha a főegyütthatójukról is igazolni tudnánk, hogy egyenlők, akkor különbségüknek több gyöke lenne, mint a foka, és így ez a különbség a nullapolinom

lehetne csak, amivel készen lennénk. (A polinomok azonossági tételét használtuk, lásd [2], 2.4.7. tétel és 2.4.10. következmény.)

A körosztási polinom főegyütthatója 1. Az $x^{\varphi(n)}\,\Phi_n(1/x)$ polinom főegyütthatója ugyanaz, mint $\Phi_n(x)$ konstans tagja, vagyis $\Phi_n(0)$. Ha $n=2$, akkor $\Phi_n(x)=x+1$ konstans tagja is 1. Ha $n>2$, akkor $\varphi(n)$ páros, ezért $\Phi_n(0)$ a primitív n-edik egységgyökök szorzata. Az előző feladatban használt $k\leftrightarrow n-k$ párosítás $\varepsilon_k\varepsilon_{n-k}=1$ miatt azt adja, hogy ez szintén 1. □

4.4. Feladat. *Igazoljuk, hogy $n\geq 1$ esetén x^n+x^{-n} felírható $x+x^{-1}$ egész együtthatós polinomjaként.*

Megoldás. Legyen $z_j=x^j+x^{-j}$. A binomiális tétel szerint páratlan n esetén

$$(x+x^{-1})^n = z_n + \sum_{1\leq j<n/2} \binom{n}{j} z_{n-2j}\,.$$

Ha n páros, akkor a jobb oldalhoz még $\binom{n}{n/2}$ is hozzáadandó. Mindkét esetben azt kaptuk, hogy $z_n=x^n+x^{-n}$ felírható egész együtthatókkal $(x+x^{-1})^n$, valamint az olyan z_k kifejezések segítségével, ahol $k<n$. Ezért n szerinti indukcióval készen vagyunk. □

4.5. Feladat. *Mutassuk meg, hogy van olyan egész együtthatós $S(x)$ polinom, melyre $\Phi_n(x)=x^{\varphi(n)/2}\,S(x+x^{-1})$.*

Megoldás. A 4.3. feladat azt fejezi ki, hogy $\Phi_n(x)$ együtthatósorozata szimmetrikus a „közepére”, vagyis x^j és $x^{\varphi(n)-j}$ együtthatója megegyezik. Ezért $x^{\varphi(n)/2}$-vel osztva x^j+x^{-j} alakú tagok egész együtthatós összegét kapjuk (illetve a $cx^{\varphi(n)/2}$ tagból a c egész szám keletkezik). Az előző feladat szerint ez az összeg felírható $x+x^{-1}$ egész együtthatós polinomjaként. □

4.6. Feladat. *Igazoljuk a 4.1. tétel (2) és (3) állítását.*

Megoldás. Elég belátni, hogy az előző feladatban szereplő $S(x)$ polinom megegyezik $\Psi_n(x)$-szel, hiszen $S(x)$ egész együtthatós. De ez igaz, mert mindkettő $\varphi(n)/2$ fokú, 1 főegyütthatós polinom, melyeknek gyöke a $\varphi(n)/2$ darab, páronként különböző $2\cos(2\pi k/n)$ számok mindegyike, ahol $1\leq k<n/2$ és $(k,n)=1$. A gyökökre vonatkozó iménti állítás $\Psi_n(x)$-re nyilvánvaló, $S(x)$ esetében pedig következik az $\varepsilon_k^{-1}=\cos(2\pi k/n)-i\sin(2\pi k/n)$ összefüggésből, hiszen

$$0=\Phi_n(\varepsilon_k)=\varepsilon_k^{\varphi(n)/2}S(\varepsilon_k+\varepsilon_k^{-1})=\varepsilon_k^{\varphi(n)/2}S\big(2\cos(2\pi k/n)\big)\,.$$

□

4.7. Gyakorlat. Számítsuk ki a $\Psi_{12}(x)$ polinomot.

Megoldás. Az első rész 3.5. gyakorlatában kiszámítottuk, hogy $\Phi_{12}(x)=x^4-x^2+1$. Innen

$$x^{-\varphi(12)/2}\Phi_{12}(x)=(x^2+x^{-2})-1=(x+x^{-1})^2-3\,.$$

Ezért $\Psi_{12}(x)=x^2-3$. □

A Dirichlet-tétel $nk-1$ esetének vizsgálatában a $\Psi_n(u)$ számok $4k-1$ alakú prímosztói lesznek segítségünkre. Ha az Olvasó ismeri a kvadratikus reciprocitási tételt ([1], 4.2.3. tétel), akkor máris beláthatja a $\Psi_{12}(u) = u^2 - 3$ kifejezést felhasználva, hogy végtelen sok $12k-1$ alakú prím van.

A cikk első részében az utolsó három feladat vezetett el az $nk+1$ alakú prímekre vonatkozó állítás bizonyításához. Ezek közül az elsőnek, vagyis a 3.10. feladatnak az $nk-1$ esetre adaptált változatát fogjuk belátni a 4.9. feladatban. Ezt készíti elő a következő állítás.

4.8. Feladat. *Legyen $g(x)$ egész együtthatós, pozitív főegyütthatós polinom, melynek konstans tagja negatív. Igazoljuk, hogy minden pozitív K egészhez van olyan u egész, hogy $g(u)$ osztható egy K-nál nagyobb, $4k-1$ alakú prímszámmal.*

Megoldás. Legyen $g(0) = -c < 0$ és $M = 4cLK!$, ahol L később megválasztandó pozitív egész. Ekkor $g(M) = 4mc - c$ teljesül alkalmas, $K!$-sal osztható m-re, és ezért $g(M)/c = 4m - 1$. Ha L-et elég nagynak választjuk, akkor elérhetjük, hogy $g(M)/c > 1$ legyen. Így $g(M)/c = 4m-1$-nek van egy $4k-1$ alakú p prímosztója. Szükségképpen $p > K$, mert p relatív prím m-hez, és így annak $K!$ osztójához is. □

4.9. Feladat. *Mutassuk meg, hogy minden pozitív K egészhez van olyan u egész, hogy $\Psi_n(u)$ osztható egy K-nál nagyobb, $4k-1$ alakú prímszámmal.*

Megoldás. A $\Psi_n(x)$ polinom definíciójából látszik, hogy $\Psi_n(x)$ csupa negatív értéket vesz föl a két legnagyobb gyöke közötti intervallumon (illetve ha elsőfokú, akkor a gyökétől balra). Így van olyan r/s racionális szám, melyre $s > 0$ és $\Psi_n(r/s) < 0$.

Készítsük el a $g(x) = s^d \Psi_n\big((x+r)/s\big)$ polinomot, ahol $d = \varphi(n)/2$ a $\Psi_n(x)$ foka. Ez egész együtthatós, pozitív főegyütthatós, és $g(0) = s^d \Psi_n(r/s) < 0$. Ezért az előző feladat miatt van olyan K-nál és s-nél is nagyobb $4k-1$ alakú p prím, melyre $p \mid g(v)$ alkalmas v egészre.

Mivel $p > s$, ezért $(p, s) = 1$, tehát van olyan t egész, melyre $ts \equiv 1\ (p)$. Megmutatjuk, hogy p osztója $\Psi_n\big(t(v+r)\big)$-nek, és így az $u = t(v+r)$ választással készen is leszünk. Valóban, ha $\Psi_n(x) = a_0 + \ldots + a_d x^d$, akkor

$$0 \equiv t^d g(v) = t^d s^d \Psi_n\big((v+r)/s\big) = \sum_{j=0}^{d} t^d s^{d-j} a_j (v+r)^j \equiv$$

$$\equiv \sum_{j=0}^{d} t^j a_j (v+r)^j = \Psi_n\big(t(v+r)\big) \quad (p)\,,$$

hiszen $t^d s^{d-j} \equiv t^j\ (p)$. □

Az előző megoldás utolsó bekezdését egyszerűsíthetjük, ha a $\mathbb{Z}_p$ testben számolunk, és t helyett egyszerűen $1/s$-et írunk.

5. Gauss-egészek

A Gauss-egészek az $a+bi$ alakú komplex számok, ahol a és b egészek. Ezek körében is értelmezhetők a számelmélet alapfogalmai, például az $\alpha \mid \beta$ oszthatóság azt jelenti, hogy van olyan γ Gauss-egész, melyre $\alpha\gamma = \beta$. Beszélhetünk kongruenciákról, lehet maradékosan osztani, és érvényes marad a számelmélet alaptétele is (a bizonyítás elolvasható az [1] könyv 7.4. szakaszában). Szép alkalmazása a Gauss-egészek elméletének annak meghatározása, hogy egy pozitív egész hányféleképpen bontható két négyzetszám összegére ([1], 7.5.1. tétel).

5.1. Feladat. *Legyen m (valós) egész szám. Igazoljuk, hogy $m \mid a+bi$ akkor és csak akkor igaz a Gauss-egészek között, ha $m \mid a$ és $m \mid b$.*

Megoldás. Vegyük az $m(c+di) = a+bi$ egyenlőség valós és képzetes részét. □

Természetesen vannak különbségek az egész számok számelméletéhez képest. Az egységek, vagyis 1 osztói négyen vannak, ± 1 mellett $\pm i$ is egység. Sem 2, sem 5 nem prímszám a Gauss-egészek között, hiszen $2 = (1+i)(1-i) = i(1-i)^2$ és $5 = (2+i)(2-i)$.

5.2. Feladat. *Legyen p egy $4k-1$ alakú prímszám. Igazoljuk, hogy p prímszám a Gauss-egészek körében is, azaz nem egység, és ha $p \mid \alpha\beta$, akkor $p \mid \alpha$ vagy $p \mid \beta$.*

A megoldáshoz idézzük föl az első rész 2.2. feladatát: ha a p prímszám $4k-1$ alakú, akkor $p \mid a^2+b^2$-ből $p \mid a$ és $p \mid b$ következik.

Megoldás. Tegyük föl, hogy $p\gamma = \alpha\beta$. Ezt az egyenlőséget a konjugáltjával megszorozva az adódik, hogy p^2 az egészek között osztója az $|\alpha|^2|\beta|^2$ szorzatnak (itt $|\alpha|^2$ és $|\beta|^2$ már egész számok). Mivel p az egészek között prímszám, osztója valamelyik tényezőnek. Ha ez például $|\alpha|^2$, akkor $\alpha = a+bi$ esetén p osztója $|\alpha|^2 = a^2+b^2$-nek. Így $p \mid a$ és $p \mid b$, tehát $p \mid \alpha$. □

5.3. Feladat. *Legyen p egy $4k-1$ alakú prímszám. Mutassuk meg, hogy minden (valós) egész számnak van négyzetgyöke a Gauss-egészek között modulo p.*

Megoldás. A p-vel osztható számok négyzetgyöke 0 modulo p. Emeljük négyzetre az $1, 2, \ldots, p-1$ számokat modulo p. Mivel x és $-x$ négyzete ugyanaz, továbbá $p \neq 2$ miatt x és $-x$ inkongruens modulo p, ezért legföljebb $(p-1)/2$ számot kaphatunk. Ennyi azonban biztosan lesz is, mert ha $x^2 \equiv y^2\ (p)$, akkor $p \mid x^2-y^2 = (x-y)(x+y)$ miatt x és y vagy egyenlők, vagy ellentettek modulo p.

A kapott „négyzetszámok" között semelyik kettő nem lehet egymás ellentettje modulo p, hiszen $p \mid a^2+b^2$-ből $p \mid a$ és $p \mid b$ következik. Ezért a fenti négyzetszámok ellentettjei kiadják a hiányzó $(p-1)/2$ darab nem nulla maradékot modulo p. Viszont a $-b^2$ számnak van négyzetgyöke a Gauss-egészek között: $\pm bi$. □

A négyzetgyökvonás lehetővé teszi bizonyos másodfokú egyenletek megoldását a Gauss-egészek között a megoldóképlet segítségével. Nekünk a (másodfokúra vezető) $x + x^{-1} = u$ egyenlet egy α megoldására lesz szükségünk modulo p, ahol u a 4.9. feladatban szereplő szám. Ez azért lesz hasznos, mert a $\Phi_n(\alpha) = \alpha^{\varphi(n)/2}\Psi_n(\alpha+\alpha^{-1})$

összefüggés miatt α gyöke lesz az n-edik körosztási polinomnak modulo p, és ezért α rendjének kiszámításával információt kapunk n és p kapcsolatáról, az első rész 3.6. tételében látott módon. Ezt az egyenletmegoldást végezzük el a következő feladatban.

5.4. Feladat. *Legyen p egy $4k-1$ alakú prímszám és u valós egész. Keressünk olyan α és β Gauss-egészeket, melyekre $\alpha+\beta \equiv u\ (p)$ és $\alpha\beta \equiv 1\ (p)$.*

Megoldás. Az $x+x^{-1}=u$ egyenletet átrendezve $x^2-ux+1=0$. A megoldóképletből

$$\alpha, \beta = \frac{u \pm \sqrt{u^2-4}}{2}.$$

A nevező nem okoz problémát, hiszen p páratlan, ezért a 2-vel való osztás helyettesíthető a $(p+1)/2$-vel való szorzással modulo p. Az 5.3. feladat szerint elvégezhető a négyzetgyökvonás is. Könnyű ellenőrizni, hogy a képletből kapott α és β számok megfelelnek. □

Most rátérünk az elemrend fogalmának általánosítására, és megkeressük az első rész 3.6. tételének megfelelőjét. Szükségünk lesz az Euler–Fermat-tétel módosított változatára. Némi óvatosságra int a következő állítás.

5.5. Feladat. *Legyen p egy $4k-1$ alakú prímszám és $a+bi$ Gauss-egész. Mutassuk meg, hogy $(a+bi)^p \equiv a-bi = \overline{a+bi}\ (p)$.*

Megoldás. Emeljük $a+bi$-t p-edik hatványra a binomiális tétel segítségével. Mivel $0<j<p$ esetén $\binom{p}{j}$ osztható p-vel, azt kapjuk, hogy $(a+bi)^p \equiv a^p+(bi)^p\ (p)$. Itt $i^p=-i$, hiszen a p prím $4k-1$ alakú. Másrészt $a^p \equiv a\ (p)$ és $b^p \equiv b\ (p)$ a kis Fermat-tétel miatt. Ezért $(a+bi)^p \equiv a-bi\ (p)$. □

5.6. Feladat. *Legyen p egy $4k-1$ alakú prímszám. Mutassuk meg, hogy ha az α Gauss-egész nem osztható p-vel, akkor $\alpha^{p^2-1} \equiv 1\ (p)$, továbbá $\alpha^{p-1} \equiv 1\ (p)$ akkor és csak akkor teljesül, ha α képzetes része p-vel osztható (vagyis ha α valós modulo p).*

Megoldás. Mivel α relatív prím p-hez, ezért $\alpha^{m-1} \equiv 1\ (p) \iff \alpha^m \equiv \alpha\ (p)$. Az előző feladat miatt $\alpha^p \equiv \overline{\alpha}$, és így α^p akkor és csak akkor kongruens α-val, ha α képzetes része p-vel osztható (hiszen p páratlan). Az előző feladat állítását kétszer alkalmazva $\alpha^{p^2} \equiv \overline{\overline{\alpha}} = \alpha\ (p)$, és így $\alpha^{p^2-1} \equiv 1\ (p)$. □

Az elemrend fogalmáról modulo p ugyanúgy beszélhetünk Gauss-egészek között is, mint egészek között, és a tulajdonságok is ugyanazok. Azt javasoljuk, hogy az Olvasó ismételje át a cikk első részében található 3.6. tétel bizonyítását, és győződjön meg róla, hogy e tétel következő változata a Gauss-egészek között is érvényben marad.

5.7. Tétel. *Ha a $4k-1$ alakú p prím osztója a $\Phi_n(\alpha)$ számnak, ahol α Gauss-egész, akkor $o_p(\alpha)=n$ vagy $p \mid n$.*

A most kimondott tétel még nem adja meg az $nk-1$ esethez azt a segítséget, amit az első rész 3.6. tétele adott az $nk+1$ esethez, ehhez szükség van a következő feladatra is. Ennek oka a következő. Az $nk+1$ alakú prímek keresésekor az $o_p(u) = n \mid \varphi(p) = p-1$ oszthatóságot alkalmaztuk. A módosított Euler–Fermat-tétel miatt most csak annyit tudunk, hogy ha p nem osztója α-nak, akkor $o_p(\alpha) = n \mid p^2 - 1$. Az $nk - 1$ alakú prímek megtalálásához viszont az $n \mid p + 1$ oszthatóságra van szükségünk.

5.8. Feladat. *Legyen p egy $4k - 1$ alakú prímszám. Tegyük föl, hogy α és β Gauss-egészek, α képzetes része nem osztható p-vel, de $\alpha + \beta$ képzetes része igen, továbbá $\alpha\beta \equiv 1\ (p)$. Igazoljuk, hogy $o_p(\alpha) \mid p + 1$.*

Az alábbi számolást egyszerűbb kitalálni, ha hajlandóak vagyunk eleve modulo p számolni, az osztást is beleértve, és β helyett $1/\alpha$-t írni. (Valójában arról van szó, hogy a Gauss-egészek modulo p maradékai egy p^2 elemű testet alkotnak.)

Megoldás. Mivel $\alpha + \beta$ valós modulo p, az 5.5. feladat miatt

$$\alpha + \beta \equiv \overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta} \equiv \alpha^p + \beta^p\ (p)\,.$$

Átrendezve és α^{p+1}-nel szorozva

$$(\alpha - \alpha^p)\alpha^{p+1} \equiv (\beta^p - \beta)\alpha^{p+1} = \beta^p\alpha^p\alpha - \beta\alpha\alpha^p \equiv \alpha - \alpha^p\ (p)\,.$$

Tudjuk, hogy α nem valós modulo p, vagyis az 5.5. feladat miatt $\alpha - \alpha^p$ nem osztható p-vel. Ezért a kongruenciát egyszerűsíthetjük $\alpha - \alpha^p$-nel. Így $\alpha^{p+1} \equiv 1\ (p)$. □

Most már a célegyenesben vagyunk. Az előző szakaszban beláttuk az első rész 3.10. feladatának megfelelő 4.9. feladatot. A most következő két feladat az első rész 3.11. és 3.12. feladatainak analogonja.

5.9. Feladat. *Tegyük föl, hogy a $4k - 1$ alakú p prím nagyobb, mint $4n$, és osztója $\Psi_{4n}(u)$-nak alkalmas u egészre. Mutassuk meg, hogy a p prím $nk - 1$ alakú.*

Megoldás. Legyen α és β az 5.4 feladatból kapott két Gauss-egész. Az $\alpha\beta \equiv 1\ (p)$ összefüggés miatt

$$\Phi_{4n}(\alpha) = \alpha^{\varphi(4n)/2}\Psi_{4n}(\alpha + \alpha^{-1}) \equiv \alpha^{\varphi(4n)/2}\Psi_{4n}(\alpha + \beta) \equiv \alpha^{\varphi(4n)/2}\Psi_{4n}(u) \equiv 0\ (p)$$

(aki még nem gyakorlott a modulo p osztásban, az írja ki a polinom tagjait, és vegye észre, hogy $(\alpha + \alpha^{-1})^j\alpha^j \equiv (\alpha + \beta)^j\alpha^j$). Az 5.7. tétel miatt $p \mid 4n$ vagy $o_p(\alpha) = 4n$. Mivel $p > 4n$, ezért csakis $o_p(\alpha) = 4n$ lehetséges.

Ha α valós modulo p, akkor innen $4n \mid p-1$ adódik (hiszen ekkor $\alpha^{p-1} \equiv 1\ (p)$). Ez lehetetlen, mert a p prím $4k-1$ alakú. Így az 5.8. feladat szerint $4n = o_p(\alpha) \mid p+1$. □

5.10. Feladat. *Igazoljuk, hogy minden $n > 0$ esetén végtelen sok $nk - 1$ alakú prímszám van.*

Megoldás. Tegyük föl indirekt, hogy csak véges sok ilyen prímszám van, legyenek ezek $p_1, p_2, \ldots, p_\ell$. Válasszuk a K számot úgy, hogy ezek mindegyikénél, továbbá $4n$-nél is nagyobb legyen. A 4.9. állítás miatt van olyan u egész, továbbá egy $4k - 1$ alakú, K-nál nagyobb p prím, melyre $p \mid \Psi_{4n}(u)$. Az előző feladat szerint a p prím $nk - 1$ alakú, ami ellentmondás. □

Összefoglalva, az $nk-1$ eset bizonyításának lényege a következő. Az állítást elég $4nk-1$-re igazolnunk, tehát $4k-1$ alakú p prímeket keresünk. Azt, hogy egy polinom ilyen prímekkel osztható értékeket is felvegyen, csak akkor tudjuk garantálni, ha a polinom nem mindenütt pozitív. Ilyen tulajdonságú a $\Psi_{4n}(x)$ polinom, amelyből x helyére $x+x^{-1}$-et írva „lényegében" a körosztási polinom adódik. Tegyük föl, hogy $p \mid \Psi_{4n}(u)$. A Gauss-egészeket modulo p nézve olyan p^2 elemű testet kapunk, melyben az $\alpha+\alpha^{-1}=u$ egyenlet megoldható. Ekkor α gyöke a körosztási polinomnak ebben a testben, így rendje $4n$. Annak felhasználásával, hogy $\alpha+\alpha^{-1}$ valós, kiszámoltuk, hogy ez a rend nemcsak p^2-1-nek, hanem $p+1$-nek is osztója.

Ajánlott irodalom

[1] Freud Róbert, Gyarmati Edit: *Számelmélet*. Nemzeti Tankönyvkiadó, 2006.
[2] Kiss Emil: *Bevezetés az algebrába*. TypoTEX Kiadó, 2007.