A feladat annak a bizonyítása volt, hogy a $\dfrac{21n+4}{14n+3}$ tört egyetlen n egész szám esetén sem egyszerűsíthető.*[0]

Egy tört egyszerűsíthetősége azon múlik, hogy mi a számláló és a nevező legnagyobb közös osztója. A gondot az jelenti, hogy egy „változó" szám is szerepel. Ennek következtében lehet, hogy bizonyos esetekben nincs 1-től különböző közös osztó, máskor meg van.

Mindenekelőtt gondoljuk végig, miképpen lehet két szám legnagyobb közös osztóját meghatározni. Erre a legjobb és leggyorsabb módszer az úgynevezett *Eukideszi algoritmus,* amelyik a maradékos osztáson alapszik. A maradékos osztás a következőképpen szól:

Ha adott az a és a 0-tól különböző b egész szám, akkor mindig léteznek olyan q és r egész számok, hogy $|r| < |b|$, és fennáll az $a = q \cdot b + r$ egyenlőség.

Maga a felírt egyenlőség igen érzékeny a legnagyobb közös osztóra (mindjárt kiderül mely számokéra). Tegyük fel, hogy d osztója a-nak és b-nek: $a = d \cdot a_1$ és $b = d \cdot b_1$. Ekkor $r = d \cdot (a_1 - q \cdot b_1)$, azaz d b-nek és r-nek is közös osztója. Ha viszont d_1 a b-nek és az r-nek közös osztója, azaz $b = d_1 \cdot b_2$ és $r = d_1 \cdot r_2$, akkor $a = d_1 \cdot (q \cdot b_2 + r_2)$. Eszerint az $(a,\ b)$ pár közös osztói ugyanazok, mint a $(b,\ r)$ pár közös osztói. Ez a megállapítás természetesen nem függ attól, hogy léteznek-e legnagyobb közös osztók.

Ha most a maradékos osztást a b és r számokra végezzük el, akkor a kapott r_1 maradékra ismét teljesül az $|r_1| < |r|$; továbbá az is, hogy az $(r,\ r_1)$ pár osztói megegyeznek a $(b,\ r)$ pár osztóival; és így ugyanazok, mint az eredeti $(a,\ b)$ pár osztói. Mivel pozitív egészek csökkenő sorozata csak véges lehet, ezért az eljárás egyszer véget ér. A legvégül kapott maradékra csak 0 adódhat. Az előző maradékot jelölje r_{s+1}. Ekkor ennek és 0-nak a közös osztói ugyanazok, mint az $(a,\ b)$ párnak. Tekintettel arra, hogy 0-nak minden szám osztója, ezért r_{s+1} lesz a két adott szám legnagyobb közös osztója.

Az eljárás során még valami öröklődik lépésről lépésre. Az első két szám felírható, mint a és b úgynevezett egész együtthatós *lineáris kombinációja:* $a = a \cdot 1 + b \cdot 0$ és $b = a \cdot 0 + b \cdot 1$. Ez a tulajdonság is végig öröklődik. Ha valamelyik két maradék (b a „nulladik" és a a „mínusz egyedik" maradék) ilyen alakú, akkor a következő is ilyen alakú lesz. Legyen $r_{t-1} = ax_{t-1} + by_{t-1}$ és $r_t = a \cdot x_t + b \cdot y_t$. Az $r_{t-1} = q_t r_t + r_{t+1}$ összefüggésből:

$$r_{t+1} = a \cdot x_{t-1} + b \cdot y_{t-1} - q_t(a \cdot x_t + b \cdot y_t) = a \cdot (x_{t-1} - q_t x_t) + b \cdot (y_{t-1} - q_t y_t)$$

adódik; ami éppen a kívánt alakú felírás.

Megjegyezzük, hogy hasonló eljárás létezik például racionális vagy valós együtthatós polinomok esetében is: adott $f(x)$ és 0-tól különböző $g(x)$ polinomokhoz létezik olyan $q(x)$ és $r(x)$ polinom, amelyekre $f(x) = q(x)g(x) + r(x)$, de itt nem az abszolút érték, hanem a fokszám csökken az eljárás lépéseiben: $\operatorname{gr}(r(x)) < \operatorname{gr}(g(x))$, vagy $r(x) = 0$, az azonosan 0 polinom. (Ez utóbbira azért van szükség, mert az azonosan 0 polinomnak nincs foka.)

Ezt az eljárást nevezik *Euklideszi algoritmusnak*. Ennek eredményeként azt láttuk be, hogy az a és b egész számok d legnagyobb közös osztóját $d = ax + by$ alakba írhatjuk.

Az általában igaz, hogy $ax + by$ mindig osztható a és b minden közös osztójával. Ha azonball nem „konkrét" számokról van szó, akkor nem feltétlen kapjuk meg a legnagyobb közös osztót. Eredeti példánkban $21n+4$ és $14n+3$ legnagyobb közös osztóját kerestük. $1 = 3(14n+3) - 2(21n+4)$ miatt ez csak 1 lehet.

Kiindulási példánk helyett vegyük az n-et és 2-t. Egy $nx+2y$ alakú szám csak úgy lehet tetszőleges n mellett osztója 2-nek, ha $x = 0$. Egy $2y$ alakú szám viszont nem lehet tetszőleges n esetén az n osztója (például az $n = 1$ esetben sem). Mégis, azt meg tudjuk mondani, hogy minden n-re csak 1 lehet közös osztó, míg páros n-re 2 a legnagyobb közös osztó. Persze itt csak azért lett minden viszonylag egyszerűbb, mert a két kiindulási szám is elég egyszerű volt. Általában egész a, b, c, d mellett kell keresni az $an + b$ és $cn + d$ legnagyobb közös osztóját. A $c(an + b) - a(cn + d) = cb - ad$ összefüggésből azonnal látszik, hogy a legnagyobb közös osztó mindig osztója $(bc - ad)$-nek is. Nem biztos azonban, hogy e szám minden osztója közös osztó. Az eredeti példa alapján is látható, hogy itt „túl nagy" számokkal szoroztunk. Célszerűbb az a és b legnagyobb közös osztójától eltekinteni. Ennek megfelelően az alábbi kiindulást érdemes tekinteni: Legyen a két szám $A = aun + bv$ és $C = cun + dv$, ahol a és c, valamint b és d relatív prímek (nincs 1-tól különböző pozitív osztójuk). Ekkor A-nak és C-nek minden közös osztója osztja a $cA - aC = (cb - ad)v = V$ számot.

Jó lenne most emellé a V szám mellé egy olyan U számot találni, hogy U és V közös osztói megegyezzenek A és C közös osztóival. Ilyen számot találhatunk!

Mivel a és c legnagyobb közös osztója 1, azért ennek a lineáris kombinációként való előállíthatósága alapján vannak olyan x és y egész számok, amelyekre $ax - cy = 1$. Azt állítjuk, hogy megfelelő lesz az ezekkel képzett $U = xA - yC$ szám. Természetesen A és C minden közös osztója U-nak is osztója. A $cU - xV = (-cy + ax)C = C$, valamint az $aU - yV = (ax - cy)A = A$ összefüggések alapján U és V valóban megfelelnek a kívánalmaknak. U-t kiszámítva az $U = x(aun + bv) - y(cun + dv) = un + (bx - dy)v$ egyenlőséghez jutunk. Még abban is „szerencsénk van", hogy n együtthatója az eredeti két együttható legnagyobb közös osztója.

Az $e = cb - ad$ és $f = bx - dy$ jelöléssel tehát feladatunk az $un + fv$ és az ev számok legnagyobb közös osztójának a meghatározása. Vegyük azonban észre, hogy e és f nem teljesen függetlenek egymástól. Fennállnak ugyanis a $cf - xe = -dcy + dax = d$ és $af - ye = abx - ycb = b$ összefüggések. Eszerint e és f minden közös osztója b-nek és d-nek is közös osztója lesz. Mivel ezek relatív prímek, azért e és f is relatív prímek.

Tehát az $un + fv$ és az ev számok legnagyobb közös osztóját keressük, ahol e és f relatív prímek.

[0] Megoldását ld. a cikket követően a a 481. oldalon.

Ha itt az u és v számok legnagyobb közös osztója 1-nél nagyobb, akkor ez természetesen mindig közös osztó lesz. A kérdés az, hogy lesz-e mindig vagy néha ennél nagyobb közös osztó is. Ennek megállapítása céljából egyszerűsítsünk u és v legnagyobb közös osztójával, és az ezután keletkező számokat vizsgáljuk. Tulajdonképpen így egy olyan esethez jutunk el, amelyikben az u és v is relatív prímek.

Az első kérdés most már az, hogy lehet-e az $un + fv$ és az ev számoknak n-től független 1-nél nagyobb közös osztója. Ennek lehetetlenségét elég úgy megmutatni, hogy az $n = 0$ és az $n = 1$ esetet nézzük meg. A figyelembe veendő három szám ev, fv és $u + fv$. Az ev és fv számok legnagyobb közös osztója v. Ennek és $(u + fv)$-nek minden közös osztója az $(u + fv) - f \cdot (v) = u$ számnak is osztója. Tekintettel arra, hogy u és v relatív prímek, tehát nem létezik 1-nél nagyobb közös osztó.

A második kérdés az, hogy lehet-e „néha" 1-nél nagyobb közös osztójuk. Amennyiben $|v| \neq 1$, akkor például az $n = kv$ esetben $un + fv$ is osztható v-vel, tehát végtelen sok ilyen számnak van 1-nél nagyobb közös osztója. Nézzük most a $v = 1$ esetet (a $v = -1$ eset teljesen hasonló). A vizsgált számok az $un + f$ alakúak, valamint az e.

Két esetet különböztetünk meg. Tegyük fel először, hogy e-nek minden prímosztója osztója u-nak is. Ha volna valamilyen n esetén az $un + f$ és az e számoknak 1-nél nagyobb közös osztója, akkor volna közös osztója, amely persze osztója lenne e-nek; és feltételünk szerint u-nak is. Ekkor viszont osztója lenne un-nek és így az $f = (un + f) - un$ számnak is, ami lehetelen, mert f és e relatív prímek. Ebben az esetben tehát soha sincs 1-nél nagyobb közös osztó.

A másik lehetőség az, hogy van az e-nek olyan p prímosztója, amelyik nem osztja u-t. Ebben az esetben u és p relatív prímek, tehát léteznek olyan x és y egész számok, amelyekre $ux + py = 1$ teljesül. Nézzük most tetszőleges k egész szám mellett az $n = pk - fx$ számokat. Ezekre $un + f = upk - ufx + f = upk - f(1 - py) + f = upk + fpy = p(uk + fy)$ ugyancsak osztható p-vel tehát ezeknek és e-nek a legnagyobb közös osztója nagyobb mint 1. Tekintettel arra, hogy $u(pk - fx) + f$ alakú szám végtelen sok van, míg e osztóinak a száma véges, ezért biztosan található végtelen sok olyan n, amelyekre $un + f$ és e legnagyobb közös osztója ugyanaz az 1-nél nagyobb szám.

Tulajdonképpen az egész bonyodalomnak a hátterében az egész együtthatós polinomok viselkedése van.

Tetszőleges $\mathbf{S}$ számkörbeli együtthatós *polinomok* $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ alakú *formális* kifejezések, ahol az a_0, a_1, a_2, …, a_n *együtthatók* az adott $\mathbf{S}$ számkörből valók, és nem minden együttható 0. Ha $a_n \neq 0$, akkor a polinomot n-edfokúnak nevezzük; és a_n neve a polinom főegyütthatója. Az $\mathbf{S}$ számkörről feltesszük, hogy nem üres; és zárt az összeadásra, kivonásra és a szorzásra. A polinomok „készen állnak arra", hogy az x *határozatlan* helyébe egy számot írjunk. Ennek megfelelően úgy számolhatunk velük, mintha x szám volna. Az együtthatókat leggyakrabban a racionális számok $\mathbf{Q}$, vagy a valós számok $\mathbf{R}$ halmazából vesszük. Így vannak racionális vagy valós együtthatós polinomok, amelyek körében (mint említettük) elvégezhető a maradékos osztás; ezért az euklideszi algoritmus is. Ennek megfelelően létezik bármely két polinomnak legnagyobb közös osztója (ami azt jelenti, hogy olyan közös osztó, amely minden közös osztónak többszöröse). Ennek következménye az, hogy minden legalább elsőfokú polinom felírható tovább már nem bontható legalább elsőfokú polinomok szorzatára; és ez a felbontás lényegében egyértelmű. (Ezeknek a fogalmaknak a precíz tárgyalása túl messzire vezetne; maradjunk meg annál, amit könnyen elképzelhetünk.) Ezt úgy mondjuk, hogy *érvényes az egyértelmű faktorizáció.*

Beszélhetünk egész együtthatós polinomokról is. Nem meglepő, de elég nehezen bizonyítható, hogy ezek körében is érvényes az egyértelmű faktorizáció. Hasonló a helyzet többhatározatlanú polinomok esetében is.

A nehézségnek az az oka, hogy a legnagyobb közös osztó nem mindig írható fel „lineáris kombináció alakban". (Ebből persze következik, hogy nem is létezhet euklideszi algoritmus.) Tekintsük például az x és a 2 egész együtthatós polinomokat. Legyen $d(x)$ ezeknek legnagyobb közös osztója, és tegyük fel, hogy felírható lineáris kombinációként: $d(x) = f(x) \cdot x + g(x) \cdot 2$. A jobb oldalon egy olyan polinom áll, amelynek a konstans tagja páros. Mivel $d(x)$ osztója 2-nek (az egész együtthatós polinomok körében!), azért $d(x)$ csak konstans lehet; amely ráadásul 2-nek az egész számok körében osztója, azaz vagy 2, vagy -2. Ezt viszont bármely egész együtthatós polinommal szorozzuk is meg, mindig olyan polinomot kapunk, amelynek együtthatói párosak; tehát ennek nem többszöröse az x polinom.

Hasonlóképpen látható be, hogy az x és y határozatlanok racionális együtthatós polinomjai között az x és y polinomok legnagyobb közös osztója nem állítható elő ezek lineáris kombinációjaként.

A lineáris kombinációként való előállíthatóság igen fontos tulajdonság. Tekintsük az egész együtthatós polinomok $\mathbf{Z}[x]$ összességét; beleértve az összeadás (kivonás) és szorzás műveletét. ($\mathbf{R}$ jelöli az egész számok összességét a szokásos műveletekkel, és x jelöli a határozatlant.) Ennek egy I (nem üres) részhalmazát *ideálnak* nevezzük, ha zárt a $\mathbf{Z}[x]$-beli lineáris kombinációra; azaz tetszőleges $f(x)$, $g(x) \in I$ és $u(x0$, $v(x) \in \mathbf{Z}$ esetén $u(x)f(x)|v(x)g(x) \in I$.

Könnyű belátni, hogy minden I ideálra teljesülnek az alábbiak:

(1) $0 \in I$,

(2) ha $f(x)$, $g(x) \in I$, akkor $f(x) + g(x)$, $f(x) - g(x) \in I$,

(3) Ha $f(x) \in I$ és $u(x) \in \mathbf{Z}[x]$, akkor $u(x)f(x) \in I$.

Triviális, hogy az egyedül 0-ból álló halmaz, valamint az egész $\mathbf{Z}[x]$ ideálok. $\mathbf{Z}[x]$-beli ideálokra igen fontos példa egyetlen $f(x)$ polinom $\mathbf{Z}[x]$-beli polinomokkal való szorzata (az $\{u(x)f(x)\}$ polinomhalmaz, ahol $u(x)$ végigfut $\mathbf{Z}[x]$ elemein). Az $f(x) = 0$ és az $f(x) = 1$ esetben éppen az előbb felírt két triviális ideált kaptuk.

Vannak azonban más ideálok is. Ugyancsak könnyű belátni, hogy tetszőlegesen adott $f_1(x)$, …, $f_n(x)$ esetében az $u_1(x)f_1(x) + \cdots + u_n(x)f_n(x)$ alakú polinomok – ahol az $u_1(x)$, …, $u_n(x)$ polinomok egymástól függetlenül végigfutnak a $\mathbf{Z}[x]$ elemein – mindig egy ideált alkotnak. Ezt az ideált az $f_1(x)$, …, $f_n(x)$ *generálta ideálnak* nevezzük; és az $f_1(x)$, …, $f_n(x)$ polinomhalmazt ezen ideál egy *generátorrendszerének*. Természetesen egy ideálnak több generátorrendszere

is lehet. A fenti ideált $(f_1(x),\ \ldots,\ f_n(x))$ fogja jelölni.

Ha csak egyetlen polinomot tekintünk, akkor éppen az előbb megadott példákat kapjuk. Az egyetlen elem által generált ideál neve főideál.

Ezek a fogalmak – megfelelően – kialakíthatók az egész számok körében. Könnyű belátni, hogy az euklideszi algoritmus következménye az, hogy ott minden ideál főideál. Ez annak a ténynek az átfogalmazása, hogy bármely két egész szám legnagyobb közös osztója előállítható ezek egész együtthatós lineáris kombinációjaként.

Az előzőekben megmutattuk, hogy az egész együtthatós polinomok körében ez nem igaz; nevezetesen az $(x,\ 2)$ ideál nem főideál. A továbbiakban belátjuk, hogy a helyzet még ennél is „rosszabb":

1. Tétel. *Minden n természetes számhoz található $\mathbf{Z}[x]$-ben olyan I_n ideál, amely nem generálható n-nél kevesebb elemmel.*

Azt is be fogjuk látni, hogy azért a helyzet nem „végtelenszer rosszabb", ugyanis igaz az alábbi:

2. Tétel. *Minden $\mathbf{Z}[x]$-beli I ideálhoz létezik olyan n_I természetes szám, hogy I generálható n_I számú elemmel.*

Érdemes megjegyezni, hogy hasonló a helyzet a racionális vagy valós együtthatós kéthatározatlanú polinomok esetében is (még a bizonyítás is hasonlóképpen történhet). Sőt, mi több, három, négy stb. határozatlan esetében is hasonló eredmény igaz; a 2. Tétel bizonyítása viszont lényegesen bonyolultabb. Ha viszont a határozatlanok száma végtelen, akkor a 2. Tétel nem igaz: könnyen be lehet látni, hogy azok a polinomok, amelyeknek a konstans tagja 0, egy ideált alkotnak; és ez az ideál nem generálható véges sok elemmel.

A bizonyítás előtt előrebocsátunk néhány dolgot:

1. Állítás. Mint már láttuk, ha d az ad és bd egész számok legnagyobb közös osztója, akkor vannak olyan p és q egész számok, amelyekre $adp + bdq = d$, illetve $ap + bq = 1$.■

A rövidebb jelölés kedvéért, ha nem konkrét polinomokról van szó, akkor ezeket nagy betűkkel fogjuk jelölni. Így az $(F_1,\ \ldots,\ F_n)$ ideál elemei az $U_1F_1 + \cdots + U_nF_n$ polinomok.

2. Állítás. $I = (F_1,\ \ldots\ F_n)$ az a legkisebb ideál, amely e polinomok mindegyikét tartalmazza.

Ha egy J ideál tartalmazza ezeket a polinomokat, akkor tartalmazza ezek lineáris kombinációt is, tehát I-t. Másrészt tetszőleges i indexre legyen $U_i = 1$ és minden más j indexre $U_j = 0$. Ekkor az ezekkel képezett lineáris kombináció pontosan F_i; így az adott polinomok mindegyike eleme I-nek.■

3. Állítás. Ha a, b relatív prím egészek és a p, q egészekre $ap + bq = 1$, akkor az $U = aF + bG$ és $V = qF - pG$ polinomokra

$$(F,\ G,\ H_1,\ \ldots,\ H_n) = (U,\ V,\ H_1,\ \ldots,\ H_n).$$

A 2. Állítás alapján elég azt belátni, hogy a generátorelemek mindegyike eleme a másik ideálnak. Csak az első két polinommal kell foglalkozni, mert a többiek mindkét ideálban benne vannak. $U, V \in (F,\ G,\ H_1,\ \ldots,\ H_n)$ nyilvánvaló. $F = pU + bV$ és $G = qU - aV$ alapján $F, G \in (U,\ V,\ H_1,\ \ldots,\ H_n)$ is igaz.■

Mivel $a = 1$ és tetszóleges b relatív prímek, azért ezekhez található alkalmas p és q; valóban $p = 1$ és $q = 0$ megfelelők. Ebben az esetben $U = F + bG$ és $V = -pG$ (illetve $V = pG$) megfelelőek. Ez a speciális eset b helyett tetszőleges B polinomra is átvihető:

4. Állítás. Tetszőleges B polinom esetén az $U = F + BG$ polinomra

$$(F,\ G,\ H_1,\ \ldots,\ H_n) = (U,\ G,\ H_1,\ \ldots,\ H_n).$$

A 3. Állításhoz hasonlóan itt is minden igaz, csak azt kell még belátni, hogy $F \in (U,\ G,\ H_1,\ \ldots,\ H_n)$. Ez viszont következik az $F = U - BG$ összefüggésből.■

Az a, b egész számok legnagyobb közös osztóját $(a,\ b)$ szokta jelölni. Nem baj, ha ezt „összetévesztjük" az ideáljelöléssel, mert, ha d a legnagyobb közös osztó, akkor éppen az $(a,\ b) = (d)$ ideál egyenlőséget kapjuk.

Az $a_1, \ldots, a_n$ egész számok legnagyobb közös osztóját $(a_1,\ \ldots,\ a_n)$ jelöli.

5. Állítás. A legnagyobb közös osztó képzése „asszociatív", azaz $(a_1,\ \ldots, a_n,\ a_{n+1}) = ((a_1,\ \ldots,\ a_n),\ a_{n+1})$. Az $a_1, \ldots, a_n$ egész számok legnagyobb közös osztóját elő tudjuk állítani $n-1$ lépésben úgy, hogy mindig egy már megkapott legnagyobb közös osztónak és a következő egész számnak relatív prím egész együtthatókkal képezett lineáris kombinációját vesszük.

Az első állítás azonnal következik abból, hogy d pontosan akkor osztója a fenti $n+1$ számnak, ha az első n számnak osztója, és ezen kívül az $(n+1)$-ediknek is. A második állítást teljes indukcióval igazoljuk. Az $n = 2$ eset az 1. Állítás szerint igaz. Tegyük fel, hogy az állítás igaz n-re, és legyen $d_n = (a_1,\ \ldots,\ a_n)$. Az 5. Állítás első része szerint $d_{n+1} = (a_1,\ \ldots,\ a_n,\ a_{n+1}) = (d_n,\ a_{n+1})$. Az 1. Állítás alapján viszont ehhez léteznek olyan relatív prím p és q egész számok, amelyekre $d_{n+1} = pd_n + qa_{n+1}$.■

6. Állítás. Legyen $d = (a_1,\ \ldots,\ a_k)$, és tekintsük az $I = (F_1,\ \ldots,\ F_n)$ ideált, ahol $k < n$. Ekkor léteznek olyan $p_1, \ldots, p_k$ egész számok, hogy $d = p_1a_1 + \cdots + p_ka_k$, és I-nek van olyan $G_1, \ldots, G_n$ generátorrendszere, amelyre $G_1 = p_1F_1 + \cdots + p_kF_k$.

Alkalmazzuk az 5. Állításban leírt eljárást az adott $a_1, \ldots, a_k$ számokra. Ugyanezt az eljárást elvégezhetjük az adott polinomokra is. Az első lépésben $d_2 = pa_1 + qa_2$. A 3. Állítás szerint a $H_1 = pF_1 + qF_2$ és alkalmas a', b' egészekkel képezett $G_2 = a'F_1 + b'F_2$ polinomokra $I = (H_1,\ G_2,\ F_3,\ \ldots,\ F_n)$. Most folytatjuk az eljárást d_2-vel és a_3-mal párhuzamosan H_1-re és F_3-ra. Ezeket helyettesítve egy H_2, G_2, G_3, F_4, $\ldots$, F_n generátorrendszert nyerünk.

Az utolsó lépésként kapott $G_1 = H_{k-1}$ polinom pontosan úgy lett előállítva az $F_1, \ldots, F_k$ polinomokból, mint d az $a_1, \ldots, a_k$ számokból. Mivel $G_1, \ldots, G_k, G_{k+1}, \ldots, F_k$ is generátorrendszer, azért az állítás valóban igaz.■

Az 1. Tétel bizonyítása. Tekintsük az

$$I = \{2^n,\ 2^{n-1}x,\ 2^{n-2}x^2,\ \ldots,\ 2^2x^{n-2},\ 2x^{n-1}, x^n\}$$

ideált. Azt fogjuk megmutatni, hogy n darab polinommal nem generálható az I ideál.

Mivel egy ideál elemei a generátorelemek polinomegyüttthatós lineáris kombinációi, azért I elemei pontosan az

$$a_n 2^n + a_{n-1}2^{n-1}x + a_{n-2}2^{n-2}x^2 + \cdots + a_2 2^2 x^{n-2} + a_1 2x^{n-1} + Fx^n$$

alakú polinomok, ahol $a_n, \ldots, a_1$ tetszőleges egész számok és F egy egészegyüttthatós polinom. Tegyük fel tehát, hogy az ilyen alakú F_0, F_1, $\ldots$, F_k polinomok I-nek egy generátorrendszerét alkotják. Ez azt jelenti, hogy e polinomok lineáris kombinációjaként az eredeti generátorrendszer minden eleme előállítható. Az F_0, F_1, $\ldots$, F_k polinomrendszert lépésről lépésre meg fogjuk változtatni úgy, hogy az elemszám változatlanul marad, és rendre felhasználjuk, hogy ebből elő tudjuk állítani az eredeti generátorrendszer elemeit.

Tekintsük először az $U_0F_0 + \ldots U_kF_k = 2^n$ előállítást. Ha a fellépő polinomok konstans tagját a megfelelő kisbetűkkel jelöljük, akkor ebből – a konstans tagok figyelembevételével – az $u_0f_0 + \cdots + u_kf_k = 2^n$ egyenlőséghez jutunk. Tekintettel arra, hogy minden egyes f_i együttható osztható 2^n-nel, ezért 2^n ezeknek az együtthatóknak a legnagyobb közös osztója. A 6. Állítás szerint tehát vannak olyan p_0, $\ldots$, p_k egész számok, hogy $G_0 = p_0F_0 + \cdots + p_kF_k$, G_1, $\ldots$, G_k ismét generátorrendszer és $p_0f_0 + \cdots + p_kf_k = 2^n$. Ez a szám viszont éppen a G_0 konstans tagja, ami azt jelenti, hogy a kapott generátorrendszer egyik elemének a konstans tagja pontosan 2^n. Ennek a polinomnak a megfelelő egész-számszorosát a generátorrendszer többi eleméből levonva a 4. Állítás alapján ismét generátorrendszert kapunk, és a kapott többi polinom konstans tagja 0 lesz.

A most kapott generátorrendszer elemeinek lineáris kombinációjaként előállítható a $2^{n-1}x$ polinom is. Mivel G_0 konstans tagja nem 0, míg a többié 0, azért az előállításban az ehhez tartozó szorzó konstans tagja csak 0 lehet, mert különben a lineáris kombináció konstans tagja nem volna 0. Így a következő alakú előállításhoz jutunk:

$$xU_0G_0 + U_1G_1 + \cdots + U_kG_k = 2^{n-1}x.$$

x-szel osztva és a konstans tagokra áttérve az $u_0g_0 + \cdots + u_kg_k = 2^{n-1}$ egyenlőséghez jutunk, ahol a kisbetűk a megfelelő polinomok konstans tagját jelölik. Mivel mindegyik g_i osztható 2^{n-1}-gyel, azért a fenti egyenlőségből az következik, hogy 2^{n-1} a g_0, g_1, $\ldots$, g_k számok legnagyobb közös osztója.

Igen lényeges észrevétel az, hogy g_0 osztható 2^n-nel is, és ezért már a g_1, $\ldots$, g_k számok legnagyobb közös osztója is 2^{n-1}. Ismét a 7. Állítást használjuk fel. Eszerint a G_1, $\ldots$, G_k polinomok helyettesíthetőek $H_1 = p_1G_1 + \cdots + p_kG_k$, H_2, $\ldots$, H_k polinomokkal úgy, hogy H_1 konstans tagja 0, elsőfokú tagjának együtthatója 2^{n-1}, és a többi polinomban a konstans is és az elsőfokú tag együtthatója is 0. Emellett a G_0 változatlanul maradt. Mivel G_0 is I-beli, azért H_1 alkalmas egész-számszorosát levonva belőle egy olyan H_0 polinomot nyerünk, amelyben az elsőfokú tag együtthatója 0. A 4. Állítás miatt ez ismét egy H_0, H_1, $\ldots$, H_k generátorrendszert szolgáltat. Az eljárást folytatva végül egy olyan M_0, M_1, $\ldots$, M_k generátorrendszert nyerünk, amelyben $M_i = 2^{n-i}m_ix^i + x^{k+1}N_i$ alakú. Ezeknek a lineáris kombinációjaként pedig csak úgy állítható elő az eredeti generátorrendszer, ha $k > n$.■

A 2. Tétel bizonyítása. Legyen I a $\mathbf{Z}[x]$-nek egy tetszőleges ideálja. Minden n természetes számhoz tekintsük az egész számoknak azt a H_n halmazát, amely az I-beli n-edfokú polinomok főegyütthatóit és még a 0-t tartalmazza. Mivel I ideál és $0 \in H_n$, azért H_n zárt az egész számokkal való lineáris kombináció képzésére. (Minden egyes H_n a $\mathbf{Z}$-nek ideálja.) Tetszőleges I-beli F polinommal együtt $xF \in I$ is igaz, és ezért $H_{n+1} \supseteq H_n$.

Legyen d_n a H_n legkisebb pozitív eleme, ha ilyen létezik; és legyen $d_n = 0$ egyébként. Ez utóbbi esetben persze H_n-ben nem is lehet más szám.

Tekintettel arra, hogy H_n zárt a lineáris kombináció képzésére, ezért bármely két H_n-beli elemmel együtt azok legnagyobb közös osztója is H_n-ben van. Ha $d_n \neq 0$, akkor ennek minden pozitív osztója nála kisebb; s mivel d_n a H_n-beli legkisebb pozitív egész szám, ezért d_n-nek és bármely H_n-beli számnak csak d_n lehet a legnagyobb közös osztója. Másszóval, H_n pontosan a d_n többszöröseiből áll. Mint láttuk $H_{n+1} \supseteq H_n$; és így d_n is többszöröse d_{n+1}-nek.

Lehetséges, hogy minden egyes $d_n = 0$. Ekkor persze I-ben nincs is 0-n kívül más polinom. Ebben az esetben 0 természetesen generátorrendszere I-nek. Egyébként van a d_n számok között pozitív; legyen egy ilyen a d_k. A pozitív számok oszthatósági tulajdonságainak alapján ekkor $d_k \geq d_{k+1} \geq \ldots$ teljesül. Mivel pozitív egész számok csökkenő sorozata csak véges lehet, azért van olyan természetes szám, hogy minden i természetes szám esetén már $d_{m+1} = d_m$.

A H_n halmazok megadása szerint minden n-hez van olyan F_n polinom, amelynek a főegyütthatója pontosan d_n. Megmutatjuk, hogy az F_0, F_1, $\ldots$, F_m polinomok I-nek egy generátorrendszerét alkotják. Tekintsük a $J = (F_0,\ F_1,\ \ldots,\ F_n)$ ideált. Legyen F tetszőleges I-beli polinom. Az f fokára vonatkozó teljes indukcióval bizonyítjuk, hogy $F \in I$.

Ha F konstans, akkor H_0 definiciója szerint F egész-számszorosa d_0-nak, azaz valóban $F \in J$. Tegyük fel, hogy az állítás igaz minden olyan polinomra, amelynek a foka kisebb mint n, és legyen $F = a_nx^n + \ldots$ egy n-edfokú polinom. A H_n definicója szerint a_n többszöröse d_n-nek: $a_n = bd_n$. Ha $n \leq m$, akkor tekintsük a $G = F - bF_n$ polinomot, ha

$n > m$, akkor meg a $G = F - bx^{n-m}F_m$ polinomot. Az ideál-tulajdonság következtében $G \in I$; és mindkét esetben G-nek a foka kisebb, mint F-é. Az indukciós feltétel szerint tehát $G \in J$; s az ideáltulajdonság alapján $F \in J$ is igaz.■

Ez a gondolat átvihető annak a bizonyítására, hogy a 2. Tétel igaz véges sok határozatlanú polinomokra is. Igaz, a bizonyítás lényegesen hosszadalmasabb. Fogalmazzunk egy kicsit általánosabban.

Számok vagy polinomok egy (nem üres) halmazát *gyűrűnek* nevezzük, ha zárt az összeadásra, kivonásra és szorzásra. Tetszőleges gyűrűben hasonlóan definiálhatók az ideálok, mint ahogy fentebb tettük. Az algebrai geometriában alapvető fontosságúak azok a gyűrűk, amelyekben minden ideál véges sok elemmel generálható. Az ilyen gyűrűk neve Nöther gyűrű[1]. Az az alapvető tulajdonság, amit a 2. Tétel bizonyításánál használtunk általában a következőképpen fogalmazható:

3. Tétel. *Egy* **S** *gyűrű ideáljai pontosan akkor generálhatók véges sok elemmel, ha ideáljainak minden* $I_1 \subseteq I_2 \subseteq \ldots$ *sorozatában valahonnét kezdve mindegyik ideál megegyezik.*

Bizonyítás. Tegyük fel először, hogy **S** minden ideálja véges sok elemmel generálható, és tekintsünk egy $I_1 \subseteq I_2 \subseteq \ldots$ ideálsorozatot. Legyen I ezeknek az ideáloknak az egyesítési halmaza. Tekintsük e halmaz a és b elemeit; illetve ezek egy $c = ua + vb$ leneáris kombinációját. I definiciója alapján vannak olyan i, j indexek, hogy $a \in I_i$ és $b \in I_j$. Feltehető, hogy $i \leq j$, amikor is a, $b \in I_j$, tehát $c \in I_j$; és így $c \in I$. Így I ideál. Eszerint generálható véges sok elemmel; legyenek ezek $u_1, \ldots, u_r$. Mivel I az adott ideálok egyesítési halmaza, ezért vannak olyan indexek, hogy $u_t \in I_{i_t}$. Ha n a fenti indexek maximuma, akkor $u_1, \ldots, u_r \in I_n$; így $I \subseteq I_n$, tehát minden i-re $I_{n+i} = I_n$.

Tegyük most fel azt, hogy minden $I - 1 \subseteq I_2 \subseteq \ldots$ ideálsorozat valahonnét kezdve ugyanabból az ideálból áll. Legyen I az **S** egy ideálja, és vegyük I-beli elemek egy $v_1, \ldots, v_s, \ldots$ sorozatát a következő'képpen:

v_1 legyen tetszőleges. Ha már a $v_1, \ldots, v_i$ elemeket kiválasztottuk, akkor tekintsük az $I_i = (v_1, \ldots, v_i)$ ideált. Ha van az I-ben olyan elem, amelyik nincs az I_i-ben akkor ezek valamelyikét válasszuk v_{i+1}-nek. Így egy növekvő ideálsorozatot kapunk, amelynek feltétel szerint vége szakad. Ez csak azért történhet meg, mert valamilyen n index esetén már I_n tartalmazza I minden elemét. Ez viszont pontosan azt jelenti, hogy $I = (v_1, \ldots, v_i)$.■

Fried Ervin

[1] A század első felében élt Emmy Nöther matematikus tiszteletére.