Irreducibilis polinomok

BSc Szakdolgozat

Írta: Nyári Vanda

Alkalmazott matematikus szak

Témavezető:

Ágoston István, egyetemi docens
Algebra és Számelmélet Tanszék
Eötvös Loránd Tudományegyetem, Természettudományi Kar

Eötvös Loránd Tudományegyetem
Természettudományi Kar
2013

Tartalomjegyzék

Köszönetnyilvánítás

Elsősorban szeretnék köszönetet mondani témavezetőmnek, Ágoston Istvánnak, hogy folyamatosan figyelemmel kísérte munkámat, ötleteivel segített, illetve felhívta a figyelmemet az esetleges hibákra. Szeretném még megköszönni tanáraimnak, hogy hozzájárultak matematikai tudásom bővítéséhez. Szeretném megköszönni Varga Ádámnak, aki az angol nyelv megértésében segített. Végül, de nem utolsósorban, köszönöm a családomnak a támogatást és a türelmet.

Előszó

A dolgozat Prasolov Polynomials című könyvének Irreducible Polynomials fejezetének egy része alapján készült, főleg racionális és egész számok feletti irreducibilitásra épül. Az első fejezetben az irreducibilitás definíciója, hozzá tartozó alap állítások illetve egyszerűbb faktorizációs algorimusok találhatók. A második fejezet irreducibilitási kritériumokkal foglalkozik. A Schönemann–Eisenstein-kritérium mellett kevésbé ismert kritériumok is szerepelnek. A harmadik fejezetben speciális alakú polinomok irreducibilitása található.

1. Irreducibilitás

1.1. Polinomok irreducibilitása racionális számtest felett

A polinomok oszthatósága hasonló az egész számok oszthatóságához, a legnagyobb közös osztó definíciója is megegyezik. Egy f polinom osztható a g polinommal, ha létezik egy h polinom, hogy $f = gh$. Egy d polinom közös osztója f-nek és g-nek, ha f és g is osztható d-vel. A d polinom a legnagyobb közös osztója f-nek és g-nek, ha f és g minden közös osztójával osztható.

Két racionális együtthatós polinom legnagyobb közös osztóját Euklideszi algoritmus segítségével kaphatjuk meg. Az algoritmus a következőképpen működik:

Keressük az f és g valós együtthatós polinomok legnagyobb közös osztóját. Tegyük fel, hogy $deg\, f \geq degg$, ez megtehető, ugyanis ha $degg$ lenne a nagyobb, akkor felcseréljük a két polinomot. Első lépésben osszuk el f-et g-vel maradékosan, a kapott maradék legyen r_1. Második lépésben osszuk el g-t r_1-gyel és a maradék legyen r_2, majd osszuk el r_1-et r_2-vel, és a maradék legyen r_3, a k-adik lépésben osszuk el r_{k-2}-t r_{k-1}-gyel és a maradék legyen r_k. Az r_k polinomok foka szigorúan csökken, ezért létezik olyan n szám, amire $r_n = 0$, azaz r_{n-2} osztható r_{n-1}-el. Az r_{n-1} osztója az r_{n-2}, r_{n-3}, ..., r_1 polinomoknak, ezért r_{n-1} osztója az f és g polinomoknak. Ráadásul ha f és g osztható egy h polinommal, akkor r_{n-1} is osztható h-val.

Az euklideszi algoritmus egy fontos következménye a következő tétel:

Tétel: *a) Ha az f és g polinomok legnagyobb közös osztója d, akkor léteznek olyan a és b polinomok, hogy $d = af + bg$.*
b) Legyenek f és g polinomok $t \subset T$ felett, ahol t és T testek. Ha f-nek és g-nek van nemtriviális közös osztója T felett, akkor van nemtriviális közös osztójuk t felett is.

Egy nulltól különböző $f \in \mathrm{T}[\mathrm{x}]$ polinom irreducibilis a T test fölött, ha f nem egység és csak úgy bontható szorzattá, hogy valamelyik tényező egység.

Állítás: *Egy $f \in \mathrm{T}[\mathrm{x}]$ polinom akkor és csak akkor irreducibilis a T test fölött, ha nem konstans, és nem bontható fel két alacsonyabbfokú T-beli együtthatós polinom szorzatára.*

Tétel (Számelmélet Alaptétele): *Legyen T egy test, ekkor minden $f \in T[x]$ polinom felbontható irreducibilis tényezők szorzatára, és ez a felbontás egyértelmű.*

Lemma: *Ha a qr polinom osztható egy irreducibilis p polinommal, akkor vagy q vagy r osztható p-vel.*

1.2. Polinomok irreducibilitása az egész számok felett

Egy nulltól különböző $f \in \mathbb{Z}$ [x] polinom irreducibilis $\mathbb{Z}$ fölött, ha f nem egység és csak úgy bontható szorzattá, hogy valamelyik tényező egység.

Egész számok felett is igaz a Számelmélet alaptétele.

Egy g polinom primitív polinom, ha a polinom együtthatóinak legnagyobb közös osztója 1.

A polinomok együtthatói az együtthatók legnagyobb közös osztójával oszthatók. Legyen $f(x) = \sum a_i x^i$, ahol $a_i \in \mathbb{Z}$. Jelöljük az f polinom $a_0, ..., a_n$ együtthatóinak legnagyobb közös osztóját $cont(f)$-el. Ekkor $f(x) = cont(f)\, g(x)$, ahol g primitív polinom.

Lemma: $cont(fg) = cont(f)\, cont(g)$

Bizonyítás: Elég azt az esetet nézni, amikor $cont(f) = cont(g) = 1$. Ugyanis, ha ez nem lenne így, akkor f és g polinomok együtthatói oszthatók $cont(f)$-fel és $cont(g)$-vel egyenként. Ezért könnyen belátható, hogy $cont(fg)$ osztható $cont(f) \cdot cont(g)$-vel.
Legyen $f(x) = \sum a_i x^i$, $g(x) = \sum b_i x^i$ és $fg(x) = \sum c_i x^i$. Tegyük fel indirekt módon, hogy $cont(fg) = d > 1$, és p egy prímosztója d-nek. Ekkor fg minden együtthatója osztható p-vel, de f-nek és g-nek van olyan együtthatója, ami nem osztható p-vel. Legyen a_r az első olyan együtthatója f-nek, ami nem osztható p-vel, b_s pedig az első olyan együtthatója g-nek, ami nem osztható p-vel. Ekkor

$$c_{r+s} = a_r b_s + a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \ldots + a_{r-1} b_{s+1} + a_{r-2} b_{s+2} \ldots \equiv a_r b_s \not\equiv 0 \pmod{p},$$

ugyanis

$$b_{s-1} \equiv b_{s-2} \equiv \ldots b_0 \equiv 0 \pmod{p}$$

$$a_{r-1} \equiv a_{r-2} \equiv \ldots a_0 \equiv 0 \pmod{p}$$

Tehát ellentmondást kaptunk. □

Megjegyzés: $cont(f) = cont(g) = 1$ esetén az 1. Gauss-lemmát kapjuk.

1. Gauss lemma: *Ha $f, g \in \mathbb{Z}[x]$ és f, g primitív polinomok, akkor fg is primitív polinom.*

2. Gauss-lemma: *Legyen $f \in \mathbb{Z}[x]$ olyan, hogy felírható g és h racionális együtthatós polinomok szorzataként, tehát $f = gh$, ahol $g, h \in \mathbb{Q}[x]$. Ekkor f előáll $f = g_0 h_0$ alakban is, ahol $g_0, h_0 \in \mathbb{Z}[x]$ és g_0 a g-nek konstansszorosa, h_0 a h-nak konstansszorosa, vagyis $\deg g_0 = \deg g$ és $\deg h_0 = \deg h$.*

Bizonyítás: Írjuk fel g-t rg_1 alakban, ahol $r \in \mathbb{Q}$, és $g_1 \in \mathbb{Z}[x]$ primitív.
Írjuk fel h-t sh_1 alakban, ahol $s \in \mathbb{Q}$, és $h_1 \in \mathbb{Z}[x]$ primitív.
Ekkor: $f = gh = rg_1 sh_1 = rsg_1 h_1$, ahol $rs \in \mathbb{Q}$ és $g_1 h_1$ primitív (1. Gauss-lemma miatt)

Segédállítás: Ha $f \in \mathbb{Z}[x]$ olyan, hogy $f = rf_1$, ahol $r \in \mathbb{Q}$ és f_1 primitív, akkor $r \in \mathbb{Z}$. (Nem bizonyítom)

$f = ((rs)g_1)h_1$, mivel $g_1 h_1$ primitív, $rs \in \mathbb{Q}$ és $f \in \mathbb{Z}[x]$, ezért $rs \in \mathbb{Z}$.
Tehát a $g_0 = rsg_1$ és $h_0 = h_1$ jó lesz, $f = g_0 h_0$. És teljesül $\deg g_0 = \deg g$ és $\deg h_0 = \deg h$ is. □

Következmény: *Ha egy legalább elsőfokú egész együtthatós primitív polinom reducibilis $\mathbb{Q}$ felett, akkor reducibilis $\mathbb{Z}$ felett is.*

Bizonyítás: Legyen $f \in \mathbb{Z}[x]$ és $f = gh$, ahol $g, h \in \mathbb{Q}[x]$. Tegyük fel, hogy $cont(f) = 1$.
Válasszunk g-hez egy pozitív egész m-et úgy, hogy $mg \in \mathbb{Z}[x]$. Legyen $n = cont(mg)$. Ekkor a racionális $r = \frac{m}{n}$ is olyan, hogy $rg \in \mathbb{Z}[x]$ és $cont(rg) = 1$.
Hasonlóan válasszunk h-hoz egy s pozitív racionális számot úgy, hogy $sh \in \mathbb{Z}[x]$ és $cont(sh) = 1$.
Be kell látni még, hogy ekkor $rs = 1$, azaz a $f = (rg)(sh)$ egy faktorizáció $\mathbb{Z}$ felett.
Az 1. Gauss-lemma miatt $cont(rsgh) = cont(rg)cont(sh)$, azaz $1 = cont(rsgh) = cont(rsf)$.
Mivel $cont(f) = 1$, ezért $rs = 1$. □

Egy $f \in \mathbb{Z}[x]$ polinom irreducibilis $\mathbb{Z}$ felett, ha prímszám, vagy nem írható fel két alacsonyabb fokú, egész együtthatós polinom szorzataként.
Egy g polinom primitív polinom, ha együtthatói relatív prímek, tehát legnagyobb közös osztójuk 1.

1.3. Egyszerűbb faktorizációs algoritmus

Kronecker algoritmusa

Keressük $f \in \mathbb{Z}[x]$ reducibilis n-edfokú polinom felbontását.
Legyen $r = \left[\frac{n}{2}\right]$. Ha f reducibilis, akkor van $g(x)$ osztója, aminek foka k, nem nagyobb, mint r.

Tegyük fel, hogy f felbontható a g és h függvény szorzatára, ahol $g,\ h \in \mathbb{Z}[x]$. Nézzük f értékeit a $j = 0, 1, \ldots, k$ helyeken, ezeket a számokat jelölje a következő: $c_j = f(j)$.

Ha valamely j-re: $c_j = 0$, akkor $x - j$ osztja f-et és így megtaláltuk f-nek az elsőfokú faktorát. A továbbiakban feltesszük, hogy $c_j \neq 0$ $(j = 0, \ldots, r)$, ekkor $g(j)$ osztja c_j-t. Ugyanis $c_j = f(j) = g(j)\,h(j)$, azaz $\frac{f(j)}{g(j)} \in \mathbb{Z}$.

A $c_0, \ldots, c_k$ számok osztói közül vegyünk $d_0, d_1, \ldots, d_k$ osztókat úgy, hogy d_0 osztója c_0-nak, d_1 osztója c_1-nek, és így tovább. Ekkor az interpolációs tétel miatt pontosan egy olyan $g(x)$ polinom létezik $(deg\, g \leq k)$, amire $g(j) = d_j$, ahol $j = 0, 1, \ldots, k$.

Minden ilyen polinomra ellenőrizni kell, hogy az együtthatói egészek-e, és a polinom osztja-e $f(x)$-et. Ha ez teljesül, akkor találtunk egy osztót.

Ha ez egyszer sem teljesül, akkor nem létezik ilyen felbontás.

2. Néhány egyszerű irreducibilitási kritérium

2.1. Schönemann–Eisenstein-kritérium

Ez az irreducibilitási kritérium az egyik legismertebb kritérium, könnyen ellenőrizhető elégséges feltételt ad egész együtthatós polinom $\mathbb{Q}$ feletti irreducibilitására.

Tétel: *Legyen $f(x) = a_0 + a_1x + \ldots + a_nx^n$ egész együtthatós polinom. Ekkor f irreducibilis $\mathbb{Q}$ felett, ha van olyan p prím, melyre egyszerre teljesülnek a következők:*
a) a_n együttható nem osztható p prímmel,
b) $a_0, \ldots, a_{n-1}$ együtthatók oszthatók p-vel,
c) a_0 nem osztható p^2-tel.
Ha f primitív polinom, akkor $\mathbb{Z}$ fölött is irreducibilis.

Bizonyítás: Tegyük fel indirekt módon, hogy f felírható gh alakban $\mathbb{Q}[x]$-ben, ahol $deg\, g < deg\, f$ és $deg\, h < deg\, f$. Feltehető, hogy $g, h \in \mathbb{Z}[x]$ (a 2. Gauss-lemma miatt). Tekintsük moduló p a felírást: $\bar{f} = \bar{g}\bar{h}$.

$$\bar{f} = \bar{a}_n x^n = \bar{a}_n x^k x^{n-k}$$

A $\bar{g}$ és $\bar{h}$ polinomok x-hatványszor konstans alakban állnak elő, mert $\mathbb{Z}_p[x]$-ben igaz a Számelmélet Alaptétele.
$\Rightarrow g$ és h konstans tagja osztható p-vel
$\Rightarrow gh$ konstans tagja osztható p^2-tel
Ez ellentmondás. □

Ha az $f(x) = a_0 + a_1x + \ldots + a_nx^n$ polinom helyett vesszük az $\hat{f}(x) = x^n f\left(\frac{1}{x}\right)$ polinomot, akkor az f polinom reciprok polinomját kapjuk. A $\hat{f}$ polinom gyökei pontosan az f polinom gyökeinek a reciprokai lesznek. A fordított Schönemann–Eisenstein-kritérium hasonlóan igazolható, mint a Schönemann–Eisenstein kritérium.

A fordított vagy reciprok Schönemann–Eisenstein-kritérium: Legyen $\hat{f}(x) = a_0 + a_1x + \ldots + a_nx^n$ olyan egész együtthatós polinom, amire az a_0 együttható nem osztható a p prímmel, az $a_1, \ldots, a_n$ együtthatók oszthatók p-vel de a_n nem osztható p^2-tel. Ekkor $\hat{f}$ irreducibilis $\mathbb{Q}$ felett. Ha $\hat{f}$ primitív polinom, akkor $\mathbb{Z}$ fölött is irreducibilis.

2.2. Eltolt Eisenstein kritérium

Ha $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ egész együtthatós polinomra nincs olyan p prím, hogy a Schönemann–Eisenstein-kritérium feltételei teljesülnek, akkor nézzük meg, hogy a-val eltolva a polinomot teljesül-e valamely p prímre a kritérium. Tehát $f(x+a) = a'_0 + a'_1 x + \ldots + a'_n x^n$, ahol $p \nmid a'_n$, $p \mid a'_0, \ldots, p \mid a'_{n-1}$ és $p^2 \nmid a'_0$. Ha van ilyen a és p, akkor azt mondjuk, hogy $f(x)$-re teljesül az Schönemann–Eisenstein-kritérium kritérium p prímre.

Állítás: *Egy f racionális polinom akkor és csak akkor irreducibilis $\mathbb{Q}$ felett, ha valamelyik eltoltja irreducibilis $\mathbb{Q}$ felett, azaz létezik olyan $a \in \mathbb{Q}$, hogy $f(x+a)$ irreducibilis $\mathbb{Q}$ felett.*

Bizonyítás: Ha az f polinomot szorzattá lehet bontani, tehát $f = gh$, akkor az eltoltjai is szorzattá bonthatók, ugyanis

$$f(x+a) = g(x+a)\, h(x+a)$$

is teljesül.

Ha $f(x+a)$ szorzattá bontható, akkor az $x = x - a$ helyettesítéssel az f polinom egy felbontását kapjuk. □

Példa: $f(x) = x^2 + x + 1$ polinomra nem teljesül a Schönemann–Eisenstein-kritérium, de teljesül az eltoltjára a Schönemann–Eisenstein-kritérium, mert $a = 1$ esetén a következőt kapjuk:

$$f(x+1) = (x+1)^2 + (x+1) + 1 = x^2 + 3x + 3$$

Az $f(x+1)$ polinomra $p = 3$ esetén teljesülnek az Schönemann–Eisenstein-kritérium feltételei, tehát irreducibilis a polinom, vagyis az eredeti $f(x)$ is irreducibilis.

Adott egy $f(x)$ polinom. Azt szeretnénk eldönteni, hogy létezik-e olyan a szám, amivel eltolva a polinomot, létezik olyan p prím, hogy ezzel a prímmel az eltolt polinomra teljesül az Schönemann–Eisenstein-kritérium. Tegyük fel, hogy $f(x)$ fokszáma legalább 2.

Ahhoz, hogy egy $f(x)$ polinomról eldönthessük, hogy valamelyik eltoltjára teljesül-e a Schönemann–Eisenstein-kritérium feltétele, szükségünk van a rezultáns fogalmára.

Adott $f(x) = \sum_{j=0}^{n} a_j x^j$ és $g(x) = \sum_{j=0}^{r} b_j x^j$ polinomok mellett f és g rezultánsának nevezzük és $R(f,g)$-vel jelöljük egy $(n+r) \times (n+r)$-es mátrix determinánsát, ahol az első r sorba $f(x)$együtthatóit írjuk úgy, hogy minden sorba eggyel több 0-t írunk az együtthatók elé, mint a megelőző sorban, és az utolsó n sorba $g(x)$ együtthatóit írjuk úgy, hogy minden sorba eggyel több 0-t írunk az együtthatók elé, mint

az előző sorban. Tehát a következőképpen fog kinézni:

$$R(f,g)=\begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{vmatrix}$$

Például: $f(x)=x^3+2x^2+3$ és $g(x)=3x^2+2x+4$. Ekkor a rezultáns a következőképpen néz ki:

$$R(f,g)=\begin{vmatrix} 1 & 2 & 0 & 3 & 0 \\ 0 & 1 & 2 & 0 & 3 \\ 3 & 2 & 4 & 0 & 0 \\ 0 & 3 & 2 & 4 & 0 \\ 0 & 0 & 3 & 2 & 4 \end{vmatrix}$$

Lemma: *Legyen $f(x)$ és $g(x)\in\mathbb{C}[x]$. Tegyük fel, hogy létezik olyan α, hogy $f(\alpha)=g(\alpha)=0$. Ekkor $R(f,g)=0$.*

Bizonyítás: Adjuk hozzá a determináns utolsó oszlopához az első oszlopnak az α^{n+r-1}-szeresét, a második oszlopnak az α^{n+r-2}-szeresét, a j-edik oszlopnak a α^{n+r-j}-szeresét ($j=3,\dots,n+r-2$), és az $(n+r-1)$-edik oszlopnak az $\alpha^{n+r-(n+r-1)}$-szeresét. Nézzük meg, hogy mik lesznek az utolsó oszlop elemei:

1. eleme:

$$0+\alpha^{n+r-1}a_n+\alpha^{n+r-2}a_{n-1}+\dots+\alpha^{n+r-j}a_{n-j+1}+\dots+\alpha^{n+r-n-1}a_0+$$

$$+\alpha^{n+r-n-2}\cdot 0+\dots+\alpha^{n+r-(n+r-1)}\cdot 0=$$

$$=\alpha^{n+r-1}a_n+\alpha^{n+r-2}a_{n-1}+\dots+\alpha^{n+r-j}a_{n-j+1}+\dots+\alpha^{r-1}a_0=$$

$$=\alpha^{r-1}\left(\alpha^n a_n+\alpha^{n-1}a_{n-1}+\dots+\alpha^{n-j+1}a_{n-j+1}+\dots+a_0\right)=\alpha^{r-1}f(\alpha)$$

n. eleme:

$$a_0 + 0 \cdot \alpha^{n+r-1} + \ldots + 0 \cdot \alpha^{n+r-(n+r-(n+1))} + \alpha^{n+r-(n+r-n)} a_n +$$

$$+\alpha^{n+r-(n+r-(n-1))} a_{n-1} + \cdots + \alpha^{n+r-(n+r-(n-j+1))} a_{n-j+1} + \ldots + \alpha^{n+r-(n+r-1)} a_1 =$$

$$= \alpha^n a_n + \alpha^{n-1} a_{n-1} + \cdots + \alpha^{n-j+1} a_{n-j+1} + \ldots + \alpha^1 a_1 + a_0 = f(\alpha)$$

$(n+1)$. eleme:

$$0 + \alpha^{n+r-1} b_r + \alpha^{n+r-2} b_{r-1} + \cdots + \alpha^{n+r-j} b_{r-j+1} + \ldots +$$

$$+\alpha^{n+r-r-1} b_0 + \alpha^{n+r-r-2} \cdot 0 + \ldots \alpha^{n+r-(n+r-1)} \cdot 0 =$$

$$= \alpha^{n+r-1} b_r + \alpha^{n+r-2} b_{r-1} + \cdots + \alpha^{n+r-j} b_{r-j+1} + \ldots + \alpha^{n-1} b_0 =$$

$$= \alpha^{n-1} \left(\alpha^r b_r + \alpha^{r-1} b_{r-1} + \cdots + \alpha^{n-j+1} b_{r-j+1} + \ldots + b_0 \right) = \alpha^{n-1} g(\alpha)$$

$(n+r)$. eleme:

$$b_0 + \alpha^{n+r-n} b_r + \alpha^{n+r-(n+1)} b_{r-1} + \cdots + \alpha^{n+r-(n+j-1)} b_{r-j+1} + \ldots + \alpha^{n+r-(n+r-1)} b_1 =$$

$$= \alpha^r b_r + \alpha^{r-1} b_{r-1} + \cdots + + \alpha^{r-j+1} b_{r-j+1} + \ldots + \alpha^{n+r-(n+r-1)} b_1 + b_0 = g(\alpha)$$

Tehát az utolsó oszlop elemei sorra:

$$\alpha^{r-1} f(\alpha), \alpha^{r-2} f(\alpha), \ldots, f(\alpha), \alpha^{n-1} g(\alpha), \alpha^{n-2} g(\alpha), \ldots, g(\alpha)$$

A lemma feltétele miatt csupa 0 az utolsó oszlop, ezért a determináns 0. □

Állítás: *Ha $\alpha_1, \ldots, \alpha_n$ az $f(x)$ polinom gyökei, akkor*

$$R(f,g) = a_n^r g(\alpha_1) \cdots g(\alpha_n).$$

Bizonyítás: n szerinti indukcióval:

Ha $n = 0$, akkor az $f(x)$ polinom 0-adfokú, tehát $f(x) = a_0$. Ekkor:

$$R(f,g) = \begin{vmatrix} a_0 & 0 & 0 & ... & 0 & 0 & 0 & ... & 0 \\ 0 & a_0 & 0 & ... & 0 & 0 & 0 & ... & 0 \\ 0 & 0 & a_0 & ... & 0 & 0 & 0 & ... & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & ... & a_0 & 0 & 0 & ... & 0 \\ 0 & 0 & 0 & ... & 0 & a_0 & 0 & ... & 0 \\ 0 & 0 & 0 & ... & 0 & 0 & a_0 & ... & 0 \\ \vdots & \vdots & \vdots & ... & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & ... & 0 & 0 & 0 & ... & a_0 \end{vmatrix} = a_0^r$$

Ha $n = 1$, akkor az $f(x)$ polinom elsőfokú, $f(x) = a_0 + a_1 x$, az $f(x)$ polinom gyöke: $\alpha_1 = -\frac{a_0}{a_1}$
Ekkor:

$$R(f,g) = \begin{vmatrix} a_1 & a_0 & 0 & ... & 0 & 0 \\ 0 & a_1 & a_0 & ... & 0 & 0 \\ 0 & 0 & a_1 & ... & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & ... & a_1 & a_0 \\ b_r & b_{r-1} & b_{r-2} & ... & b_1 & b_0 \end{vmatrix}_{(r+1)\times(r+1)} =$$

$$= b_0 a_1^r - a_0 \begin{vmatrix} a_1 & a_0 & 0 & ... & 0 & 0 \\ 0 & a_1 & a_0 & ... & 0 & 0 \\ 0 & 0 & a_1 & ... & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & ... & a_1 & a_0 \\ b_r & b_{r-1} & b_{r-2} & ... & b_2 & b_1 \end{vmatrix}_{r\times r} =$$

$$= b_0 a_1^r - a_0 b_1 a_1^{r-1} + a_0^2 \begin{vmatrix} a_1 & a_0 & 0 & ... & 0 & 0 \\ 0 & a_1 & a_0 & ... & 0 & 0 \\ 0 & 0 & a_1 & ... & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & ... & a_1 & a_0 \\ b_r & b_{r-1} & b_{r-2} & ... & b_3 & b_2 \end{vmatrix}_{(r-1)\times(r-1)} =$$

$$= b_0 a_1^r - a_0 b_1 a_1^{r-1} + a_0^2 b_2 a_1^{r-2} - a_0^3 \begin{vmatrix} a_1 & a_0 & 0 & ... & 0 & 0 \\ 0 & a_1 & a_0 & ... & 0 & 0 \\ 0 & 0 & a_1 & ... & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & ... & a_1 & a_0 \\ b_r & b_{r-1} & b_{r-2} & ... & b_4 & b_3 \end{vmatrix}_{(r-2)\times(r-2)} = \ldots =$$

$$= b_0 a_1^r - a_0 b_1 a_1^{r-1} + a_0^2 b_2 a_1^{r-2} + \ldots + (-1)^k a_0^k b_k a_1^{r-k} + + \ldots + (-1)^{r-1} a_0^{r-1} \begin{vmatrix} a_1 & a_0 \\ b_r & b_{r-1} \end{vmatrix}_{2\times 2} =$$

$$= b_0 a_1^r - a_0 b_1 a_1^{r-1} + a_0^2 b_2 a_1^{r-2} + + \ldots + (-1)^k a_0^k b_k a_1^{r-k} + \ldots + (-1)^{r-1} a_0^{r-1} a_1 b_{r-1} + (-1)^r a_0^r b_r =$$

$$= a_1^r \left(b_0 - \frac{a_0}{a_1} b_1 + \ldots + (-1)^k \left(\frac{a_0}{a_1} \right)^k b_k + \ldots + (-1)^{r-1} \left(\frac{a_0}{a_1} \right)^{r-1} b_{r-1} + (-1)^r \left(\frac{a_0}{a_1} \right)^r b_r \right) =$$

$$= a_1^r \left(b_0 + \alpha_1 b_1 + \alpha_1^2 b_2 + \ldots + \alpha_1^k b_k + \ldots + \alpha_1^{r-1} b_{r-1} + \alpha_1^r b_r \right) = a_1^r g(\alpha_1)$$

Tegyük fel, hogy $n = k-1$-re igaz az állítás, bizonyítsuk k-ra. Írjuk fel $k-1$-re az állítást:

$$\hat{f}(x) = \hat{a}_{k-1}(x-\alpha_1)\ldots(x-\alpha_{k-1}) = \hat{a}_{k-1}x^{k-1} + \hat{a}_{k-2}x^{k-2} + \hat{a}_{k-3}x^{k-3} + \ldots + \hat{a}_0$$

Az $(m+k-1)$ soros determináns a következő:

$$\begin{vmatrix} \hat{a}_{k-1} & \hat{a}_{k-2} & \ldots & \hat{a}_0 & 0 & 0 & \ldots & 0 \\ 0 & \hat{a}_{k-1} & \ldots & \hat{a}_1 & \hat{a}_0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_m & b_{m-1} & \ldots & b_1 & b_0 & 0 & \ldots & 0 \\ 0 & b_m & \ldots & b_2 & b_1 & b_0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & b_m & b_{m-1} & b_{m-2} & \ldots & b_0 \end{vmatrix} = \hat{a}_{k-1}^m g(\alpha_1)\ldots g(\alpha_{k-1})$$

Írjuk fel k-ra:

$$f(x) = \hat{f}(x)(x-\alpha_k) = \left(\hat{a}_{k-1}x^{k-1} + \hat{a}_{k-2}x^{k-2} + \hat{a}_{k-3}x^{k-3} + \ldots + \hat{a}_0\right)(x-\alpha_k) =$$

$$= \hat{a}_{k-1}x^k + (\hat{a}_{k-2} - a_{k-1}\alpha_k)x^{k-1} + (\hat{a}_{k-3} - \hat{a}_{k-2}\alpha_k)x^{k-2} + \ldots + (\hat{a}_0 - \hat{a}_1\alpha_k)x - \hat{a}_0\alpha_k$$

Az együtthatókat beírva a determináns a következő:

$$\begin{vmatrix}
\hat{a}_{k-1} & \hat{a}_{k-2}-a_{k-1}\alpha_k & \hat{a}_{k-3}-\hat{a}_{k-2}\alpha_k & \dots & -\hat{a}_0\alpha_k & 0 & \dots & 0 \\
0 & \hat{a}_{k-1} & \hat{a}_{k-2}-a_{k-1}\alpha_k & \dots & \hat{a}_0-\hat{a}_1\alpha_k & -\hat{a}_0\alpha_k & \dots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
b_m & b_{m-1} & b_{m-2} & \dots & b_0 & 0 & \dots & 0 \\
0 & b_m & b_{m-1} & \dots & b_1 & b_0 & \dots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \dots & b_m & b_{m-1} & \dots & b_0
\end{vmatrix}$$

Adjuk hozzá a második oszlophoz az első oszlop α_k-szorosát:

$$\begin{vmatrix}
\hat{a}_{k-1} & \hat{a}_{k-2} & \hat{a}_{k-3}-\hat{a}_{k-2}\alpha_k & \dots & -\hat{a}_0\alpha_k & 0 & \dots & 0 \\
0 & \hat{a}_{k-1} & \hat{a}_{k-2}-\hat{a}_{k-1}\alpha_k & \dots & \hat{a}_0-\hat{a}_1\alpha_k & -\hat{a}_0\alpha_k & \dots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
b_m & b_{m-1}+b_m\alpha_k & b_{m-2} & \dots & b_0 & 0 & \dots & 0 \\
0 & b_m & b_{m-1} & \dots & b_1 & b_0 & \dots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \dots & b_m & b_{m-1} & \dots & b_0
\end{vmatrix}$$

Adjuk hozzá a harmadik oszlophoz a második oszlop α_k-szorosát:

$$\begin{vmatrix}
\hat{a}_{k-1} & \hat{a}_{k-2} & \hat{a}_{k-3} & \dots & -\hat{a}_0\alpha_k & 0 & \dots & 0 \\
0 & \hat{a}_{k-1} & \hat{a}_{k-2} & \dots & \hat{a}_0-\hat{a}_1\alpha_k & -\hat{a}_0\alpha_k & \dots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
b_m & b_{m-1}+b_m\alpha_k & b_{m-2}+b_{m-1}\alpha_k+b_m\alpha_k^2 & \dots & b_0 & 0 & \dots & 0 \\
0 & b_m & b_{m-1}+b_m\alpha_k & \dots & b_1 & b_0 & \dots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \dots & b_m & b_{m-1} & \dots & b_0
\end{vmatrix}$$

És így tovább, ekkor a következőt kapjuk:

$$\begin{vmatrix} \hat{a}_{k-1} & \hat{a}_{k-2} & \dots & \hat{a}_0 & 0 & \dots & 0 \\ 0 & \hat{a}_{k-1} & \dots & \hat{a}_1 & \hat{a}_0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ b_m & b_{m-1}+b_m\alpha_k & \dots & g(\alpha_k) & \alpha_k g(\alpha_k) & \dots & \alpha_k^{k-1} g(\alpha_k) \\ 0 & b_m & \dots & b_1+b_2\alpha_k+\ldots+b_m\alpha_k^{k-1} & g(\alpha_k) & \dots & \alpha_k^{k-2} g(\alpha_k) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & b_m & b_{m-1}+b_m\alpha_k & \dots & g(\alpha_k) \end{vmatrix}$$

Vonjuk le az $m+1$. sortól kezdve az alatta lévő sor α_k-szorosát:

$$\begin{vmatrix} \hat{a}_{k-1} & \hat{a}_{k-2} & \hat{a}_{k-3} & \dots & \hat{a}_0 & 0 & \dots & 0 \\ 0 & \hat{a}_{k-1} & \hat{a}_{k-2} & \dots & \hat{a}_1 & \hat{a}_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ b_m & b_{m-1} & b_{m-2} & \dots & b_0 & 0 & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & b_m & b_{m-1}+b_m\alpha_k & \dots & g(\alpha_k) \end{vmatrix}$$

Az utolsó oszlop mindegyik eleme 0, kivéve az utolsót. Az utolsó oszlop szerint kifejtve a következőt kapjuk:

$$g(\alpha_k) \begin{vmatrix} \hat{a}_{k-1} & \hat{a}_{k-2} & \dots & \hat{a}_0 & 0 & 0 & \dots & 0 \\ 0 & \hat{a}_{k-1} & \dots & \hat{a}_1 & \hat{a}_0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_m & b_{m-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & b_m & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & b_m & b_{m-1} & b_{m-2} & \dots & b_0 \end{vmatrix} =$$

$$= g(\alpha_k)\,\hat{a}_{k-1}^m g(\alpha_1)\dots g(\alpha_{k-1}) = \hat{a}_{k-1}^m g(\alpha_1)\dots g(\alpha_k)$$

Az $a_k = \hat{a}_{k-1}$ helyettesítéssel pont az állítást kapjuk.Az $R(f,g)$ akkor és csak akkor 0, ha $f(x)$ és $g(x)$ polinomoknak van közös gyöke. $\square$

Algoritmus:

Adott egy $f(x)$ polinom. Azt szeretnénk eldönteni, hogy létezik-e p prím és a szám, hogy a-val eltolva a polinomot teljesül rá a Schönemann–Eisenstein-kritérium. Tegyük fel, hogy $2 \leq degf(x)$. Számoljuk ki az $R(f, f')$ determinánst.
Ha $R(f, f') = 0$, akkor $f(x)$ eltoltjára nem teljesül a Schönemann–Eisenstein-kritérium semmilyen p prímre, ugyanis ekkor van közös gyöke f-nek és f'-nek.
Ha $R(f, f') \neq 0$, akkor bontsuk prímtényezős szorzatra. Minden p prímre, ami osztja $R(f, f')$-t nézzük meg, hogy a létezik-e olyan $a \in \{0, 1, \ldots, p-1\}$, amivel eltolva f-et, p-vel teljesül-e Schönemann–Eisenstein-kritérium az $f(x+a)$ polinomra. Ha nincs ilyen p és a, akkor $f(x)$ polinom egyetlen eltoltjára sem teljesül a Schönemann–Eisenstein-kritérium.

Az algoritmus működésének bizonyítása Michael Filaseta: Irreducible polynomials theory című könyvében található ([2]).

Példa: Legyen a polinom: $f(x) = x^4 + 4x + 1$, ekkor: $f'(x) = 4x^3 + 4$. Írjuk fel $R(f, f')$-t:

$$R(f,f') = \begin{vmatrix} 1 & 0 & 0 & 4 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 4 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 4 & 1 \\ 4 & 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 & 4 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 4 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 4 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & -12 & -4 & 0 & 0 \\ 0 & 0 & 0 & 0 & -12 & -4 & 0 \\ 0 & 0 & 0 & 0 & 0 & -12 & -4 \\ 0 & 0 & 0 & 4 & 0 & 0 & 4 \end{vmatrix} =$$

$$= \begin{vmatrix} -12 & -4 & 0 & 0 \\ 0 & -12 & -4 & 0 \\ 0 & 0 & -12 & -4 \\ 4 & 0 & 0 & 4 \end{vmatrix} = 4 \cdot (-12)^3 - 4 \cdot (-4)^3 = -2^9 \cdot 13$$

Tehát $p = 2$ vagy $p = 13$ lehet.
Ha $p = 2$, akkor csak az $a = 1$ jöhet szóba, mivel az $f(x)$ nem Schönemann–Eisenstein $p = 2$-re. Ekkor $f(x+1)$-re a következőt kapjuk:

$$f(x+1) = (x+1)^4 + 4(x+1) + 1 = x^4 + 4x^3 + 6x^2 + 4x + 1 + 4x + 4 + 1 =$$

$$= x^4 + 4x^3 + 6x^2 + 8x + 6$$

Erre valóban teljesül a Schönemann–Eisenstein-kritérium 2-re. Tehát az $f(x) = x^4 + 4x + 1$ Schönemann–Eisenstein $p = 2$-vel, így irreducibilis polinom.

Ha $p = 13$, akkor az eltolt polinom a következő lesz:

$$f(x+a) = (x+a)^4 + 4(x+a) + 1 = x^4 + 4ax^3 + 6a^2x^2 + 4a^3x + a^4 + 4x + 4a + 1 =$$

$$= x^4 + 4ax^3 + 6a^2x^2 + 4x\left(a^3 + 1\right) + a^4 + 4a + 1$$

Ahhoz, hogy erre a polinomra teljesüljön a Schönemann–Eisenstein-kritérium $p = 13$-ra, a $4a$-nak oszthatónak kell lennie 13-mal. Ez csak akkor lehet, ha $a = 0$. Ekkor az $f(x)$-et kapnánk vissza. Tehát nincs ilyen a, azaz az $f(x)$ polinomra nem teljesül a Schönemann–Eisenstein-kritérium $p = 13$-mal.

2.3. Irreducibilitás mod p felett

Legyen $\mathbb{Z}_p$ a modulo p maradékosztálytest. Minden egész együtthatós polinom tekinthető, mint egy polinom $\mathbb{Z}_p$-beli együtthatókkal. Ha egy polinom $\mathbb{Z}_p$ felett irreducibilis, akkor az a polinom $\mathbb{Z}$ felett is irreducibilis, ha a p nem osztója a főegyütthatónak. Viszont egy $\mathbb{Z}$ felett irreducibilis polinom lehet $\mathbb{Z}_p$ felett reducibilis minden p-re, ilyen polnomokra ad példát a következő tétel.

Tétel: *A $P(x) = x^4 + ax^2 + b^2$, ahol $a,\ b \in \mathbb{Z}$ reducibilis $\mathbb{Z}_p$ felett minden p prímre.*

Bizonyítás: $p = 2$-re csak négy ilyen alakú polinom van. Ezek a következők:

$$x^4,\ x^4 + x^2 = x^2\left(x^2 + 1\right),\ x^4 + 1 = (x+1)^4,\ x^4 + x^2 + 1 = \left(x^2 + x + 1\right)^2$$

Mind a négy polinom reducibilis.
Legyen p páratlan prím. Ekkor válasszunk egy s egészet úgy, hogy $a \equiv 2s \pmod p$. A $P(x)$ polinom a következő:

$$P(x) = x^4 + ax^2 + b^2 \equiv \left(x^2 + s\right)^2 - \left(s^2 - b^2\right) \equiv \left(x^2 + b\right)^2 - (2b - 2s)\,x^2 \equiv$$

$$\equiv \left(x^2 - b\right)^2 - (-2b - 2s)\,x^2 \pmod p$$

Egy z számot akkor nevezünk kvadratikus maradéknak $(mod\, p)$, ha az $y^2 \equiv z \pmod p$ kongruencia megoldható. Ha ez nem oldható meg, akkor kvadratikus nem maradéknak nevezzük z-t.
Elég bizonyítani, hogy a $s^2 - b^2$, $2b - 2s$, $-2b - 2s$ számok közül az egyik kvadratikus maradék modulo p.
Modulo p a különböző kvadratikus maradékok száma $\frac{p-1}{2}$, és ugyanennyi kvadratikus nem maradékok száma is.

Ha $z = y^2$, akkor $z^{\frac{p-1}{2}} = y^{p-1} \equiv 1 \ (mod\ p)$. Ha $z \neq y^2$, akkor $z^{\frac{p-1}{2}} \equiv -1$, ugyanis $\left(z^{\frac{p-1}{2}}\right)^2 \equiv z^{p-1} \equiv 1$, tehát két kvaratikus nem maradék modulo p szorzata kvadratikus maradék modulo p.

Tegyük fel, hogy $2b - 2s$ és $-2b - 2s$ egyike sem négyzetszám modulo p, tehát nem kvadratikus maradékok. Ekkor a szorzatuk lesz négyzetszám mod p, és $(2b - 2s)(-2b - 2s) = 4s^2 - 4b^2 = 4\left(s^2 - b^2\right)$ négyzetszám modulo p, és így $s^2 - b^2$ is az. □

Példa: Az $x^4 + 1$ polinom irreducibilis $\mathbb{Z}$ felett, de minden p prímre reducibilis $\mathbb{Z}_p$ felett.

Bizonyítás: Az előző tételből következik $a = 0$ és $b = 1$ mellett, hogy minden p-re reducibilis $\mathbb{Z}_p$ felett.

Az $x^4 + 1$ polinom gyökei $\mathbb{C}$ felett $\frac{\pm 1 \pm i}{\sqrt{2}}$. Tehát a polinom a következőképpen bomlik szorzatra $\mathbb{C}$ felett:

$$x^4 + 1 = \left(x - \frac{1+i}{\sqrt{2}}\right)\left(x - \frac{1-i}{\sqrt{2}}\right)\left(x - \frac{-1+i}{\sqrt{2}}\right)\left(x - \frac{-1-i}{\sqrt{2}}\right) =$$

$$= \left(x - \frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}\right)\left(x - \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right)\left(x + \frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}\right)\left(x + \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right)$$

Csak úgy kaphatunk $\mathbb{R}$ felett felbontást, ha a konjugált párokat összeszorozzuk. Ekkor azt kapjuk, hogy:

$$x^4 + 1 = \left(\left(x - \frac{1}{\sqrt{2}}\right)^2 - \left(\frac{i}{\sqrt{2}}\right)^2\right)\left(\left(x + \frac{1}{\sqrt{2}}\right)^2 - \left(\frac{i}{\sqrt{2}}\right)^2\right) =$$

$$= \left(\left(x - \frac{1}{\sqrt{2}}\right)^2 + \frac{1}{2}\right)\left(\left(x + \frac{1}{\sqrt{2}}\right)^2 + \frac{1}{2}\right) = \left(x^2 - \frac{2x}{\sqrt{2}} + \frac{1}{2} + \frac{1}{2}\right)\left(x^2 + \frac{2x}{\sqrt{2}} + \frac{1}{2} + \frac{1}{2}\right) =$$

$$= \left(x^2 - \frac{2\sqrt{2}x}{2} + 1\right)\left(x^2 + \frac{2\sqrt{2}x}{2} + 1\right) = \left(x^2 - \sqrt{2}x + 1\right)\left(x^2 + \sqrt{2}x + 1\right)$$

És ez a felbontás nem $\mathbb{Z}$ felett van, tehát a polinom irreducibilis $\mathbb{Z}$ felett. □

2.4. Dumas kritérium

Newton poligon

Legyen p adott prím, és legyen $f(x) = \sum_{i=0}^{n} A_i x^i$ polinom egész együtthatókkal úgy, hogy $A_0 \neq 0$ és $A_n \neq 0$. Az f nemnulla együtthatóit írjuk fel mint p hatványa szorozva egy p-vel nem osztható egész számmal, tehát $A_i = a_i p^{\alpha_i}$, ahol a_i egy p-vel nem osztható egész. Rendeljünk hozzá minden nemnulla együtthatóhoz, $a_i p^{\alpha_i}$-hez, egy pontot a síkban (i, α_i) koordinátákkal. Amelyik együttható nulla, ahhoz ne rendeljünk hozzá pontot a síkban.

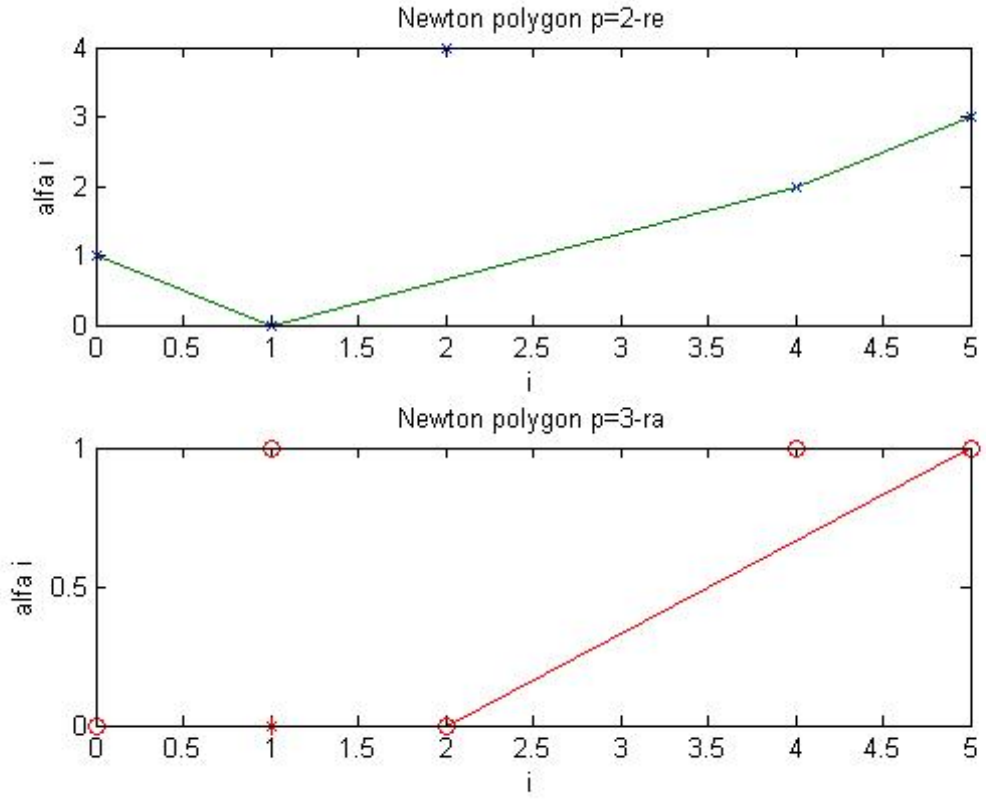
A poligon konstukciója a következő:

Vegyük az ábrázolt pontok konvex burkának az alsó részét, ezt a következőképpen tesszük meg.
Legyen $P_0 = (0, \alpha_0)$. Válasszuk $P_1 = (i_1, \alpha_{i_1})$ pontot úgy, hogy a P_0P_1 egyenes alatt ne legyen (i, α_i) pont, és i_1 a legnagyobb ilyen egész szám. Továbbá legyen $P_2 = (i_2, \alpha_{i_2})$ pont olyan, hogy a P_1P_2 egyenes alatt nincs (i, α_i) pont, és i_2 a legnagyobb ilyen egész szám, stb. Az utolsó része $P_{r-1}P_r$ alak, ahol $P_r = (n, \alpha_n)$. Vegyük hozzá a töröttvonal csúcsaihoz azokat az egészkoordinátájú pontokat, amin a $P_0 \dots P_r$ töröttvonalnak valamely része keresztülmegy. Így a $P_0, \dots, P_r$ csúcsokhoz hozzáadunk $s \geq 0$ további csúcsot. Kapunk egy $Q_0 \dots Q_{r+s}$ töröttvonalat, ami a Newton poligon ($Q_0 = P_0$ és $Q_{r+s} = P_r$). A $\overrightarrow{Q_iQ_{i+1}}$ vektorok a Newton poligon vektorrendszere lesz.

A Newton poligon vektorrendszerében minden vektort multiplicitással vesszük, tehát minden vektort annyiszor rakunk bele, ahányszor a vektorhalmazban benne lesz.

Példa: Legyen $f(x) = 2 + 3x + 16x^2 + 12x^4 + 24x^5$ és p legyen 2. Ekkor $a_0 = 1$, $\alpha_0 = 1$, $a_1 = 3$, $\alpha_1 = 0$, $a_2 = 1$, $\alpha_2 = 4$, $a_4 = 3$, $\alpha_4 = 2$,$a_5 = 3$,$\alpha_5 = 3$. Az ábrázolandó pontok a következők: $(0,1)$, $(1,0)$, $(2,4)$, $(4,2)$ és $(5,3)$. Tehát $P_0 = (0,1)$, $P_1 = (1,0)$, $P_2 = (4,2)$, $P_3 = (5,3)$. Mivel a $P_0 \dots P_3$ töröttvonal nem tartalmaz egész koordinátájú pontot, ezért ez lesz a Newton poligon.

Nézzük meg ugyanerre az f függvényre a Newton poligont, ha $p = 3$. Ekkor $a_0 = 2$, $\alpha_0 = 0$, $a_1 = 1$, $\alpha_1 = 1$, $a_2 = 16$, $\alpha_2 = 0$, $a_4 = 4$, $\alpha_4 = 1$, $a_5 = 8$, $\alpha_5 = 1$, az ábrázoldandó pontok: $(0,0)$, $(1,1)$, $(2,0)$, $(4,1)$ és $(5,1)$. Tehát $P_0 = (0,0)$, $P_1 = (2,0)$ és $P_2 = (5,1)$, mivel ez a töröttvonal tartalmaz egész koordinátájú pontot, a $(1,0)$-t ,ezért ezt hozzávesszük a töröttvonal csúcsaihoz, azaz $Q = (0,0)$, $Q_1 = (1,0)$, $Q_2 = (2,0)$ és $Q_3 = (5,1)$.



Tétel (Dumas): *Legyen $f = gh$, ahol f, g és h egész együtthatós polinomok. Ekkor f vektorhalmazrendszere a g és h vektorhalmazrendszerének uniója (ugyanarra a p-re nézve).*

Bizonyítás: Legyenek

$$f(x) = \sum_{\substack{i=0 \\ a_i \neq 0}}^{n} a_i p^{\alpha_i} x^i, \quad g(x) = \sum_{\substack{j=0 \\ b_j \neq 0}}^{m} b_j p^{\beta_j} x^j, \quad h(x) = \sum_{\substack{k=0 \\ c_k \neq 0}}^{n-m} c_k p^{\gamma_k} x^k,$$

ahol a_i, b_j, c_k számok nem oszthatók p-vel.

Vegyük f-nek a Newton poligonját. Nézzük a poligon egy $P_l P_{l+1}$ oldalának a meredekségét. Legyenek a végpontok koordinátái a következők: $P_l = \left(i_-, \alpha_{i_-}\right)$ és $P_{l+1} = \left(i_+, \alpha_{i_+}\right)$. Ekkor az

oldal meredeksége:

$$M = \frac{\alpha_{i_+} - \alpha_{i_-}}{i_+ - i_-}.$$

Egyszerűsítsük M-et. Legyen $\alpha_{i_+} - \alpha_{i_-}$ és $i_+ - i_-$ legnagyobb közös osztója $t > 0$, vagyis $\alpha_{i_+} - \alpha_{i_-} = At$ és $i_+ - i_- = It$. Ekkor $M = \frac{A}{I}$, ahol A és I relatív prímek. Írjuk fel a $P_l P_{l+1}$ oldalon átmenő egyenes egyenletét:

$$I\alpha - Ai = F, \text{ ahol } F = I\alpha_{i_+} - Ai_+ = I\alpha_{i_-} - Ai_-.$$

Tegyük fel, hogy minden (i, α_i)pont $(i = 0, 1, \ldots, n)$ vagy az egyenesen vagy fölötte fekszik. Azaz $I\alpha_i - Ai \geq F$, ahol egyenlőség csak az $i_- \leq i \leq i_+$ pontokban van. Legyen az $I\alpha_i - Ai$ szám a $ap^\alpha x^i$ egytagú polinom súlya, ahol $(a, p) = 1$. Az i_- egyértelműen meg van határozva, olyan minimális szám, amihez az F súly tartozik. Az i_+ egyértelműen meg van határozva, olyan maximális szám, amihez az F súly tartozik.
Nézzük az g polinomhoz tartozó

$$G = \min_{j=0,\ldots,m} \{I\beta_j - Aj\}$$

mennyiséget, és definiáljuk j_--t ésés j_+-t, mint legkisebb és legnagyobb indexet, amire teljesül, hogy:

$$G = I\beta_{j_-} - Aj_- = I\beta_{j_+} - Aj_+.$$

Hasonlóan nézzük a h polinomhoz tartozó

$$H = \min_{k=0,\ldots,n-m} \{I\gamma - Ak\}$$

mennyiséget, és definiáljuk k_--t ésés k_+-t, mint legkisebb és legnagyobb indexet, amire teljesül, hogy:

$$H = I\gamma_{k_-} - Ak_- = I\gamma_{k_+} - Ak_+.$$

Világos, hogy

$$a_{j_-+k_-} \cdot p^{\alpha_{j_-+k_-}} = \sum_{j+k=j_-+k_-} \left(b_j p^{\beta_j} x^j\right) \left(c_k p^{\gamma_k} x^k\right).$$

A két tag szorzatának súlya egyenlő a súlyaik összegével, ezért a súlyok szummája $j = j_-$ésk $= k_-$ esetén egyenlő $G + H$-val. Minden más esetben a súlyok összege nagyobb, mint $G + H$, ugyanis ekkor vagy $j < j_-$ vagy $k < k_-$.
Nézzük ugyanis pl. azt az esetet, amikor $j < j_-$. Ekkor a $b_j p^{\beta_j} x^j$ súlya szigorúan nagyobb, mint G és $c_k p^{\gamma_k} x^k$ súlya nem kisebb, mint H.
A $\left(b_j p^{\beta_j} x^j\right) \left(c_k p^{\gamma_k} x^k\right)$ súlya $j + k = konstans$ esetén monoton úgy nő, ahogy a $\beta_j + \gamma_k$ nő, mivel

$I > 0$. Vegyük figyelembe, hogy $j + k = j_- + k_-$ és ezért $j = j_-$ és $k = k_-$ esetén a $\beta_j + \gamma_k$ összeg szigorúan minimális. Ezért a $a_{j_-+k_-} \cdot p^{\alpha_{j_-+k_-}}$ súlya egyenlő $G + H$-val.
Ha $i < j_- + k_-$, akkor az $a_i p^{\alpha_i} x^i$ szigorúan nagyobb, mint $G + H$. Míg $i \geq j_- + k_-$ esetén az $a_i p^{\alpha_i} x^i$ súlya nem kisebb, mint $G + H$. Ezért $G + H = F$ és $j_- + k_- = i_-$.
Hasonlóképpen igazolható, hogy $j_+ + k_+ = i_+$. Így

$$i_+ - i_- = (j_+ - j_-) + (k_+ - k_-)\,. \qquad (1)$$

A $j_+ - j_-$ és a $k_+ - k_-$ közül legalább az egyik nemnulla.
Ha $j_+ - j_-$ és $k_+ - k_-$ közül minkettő nemnulla, akkor $\left(j_-, \beta_{j_-}\right)$ és $\left(j_+, \beta_{j_+}\right)$ végpontú szakasz a g Newton-poligonjának oldala, és a $\left(k_-, \gamma_{k_-}\right)$ és $\left(k_+, \gamma_{k_+}\right)$végpontú szakasz a h Newton-poligonjának oldala. Mindkét oldal meredeksége egyenlő $M = \frac{A}{I}$-vel, mivel

$$\frac{\beta_{j_+} - \beta_{j_-}}{j_+ - j_-} = \frac{A}{I} = \frac{\gamma_{k_+} - \gamma_{k_-}}{k_+ - k_-}.$$

Az (1) egyenlet azt mutatja, hogy az M meredekségű oldalak hosszának összege az g és h Newton-poligonjában egyenlő az M meredkségű oldal hosszával az f Newton-poligonjában.
Ha a $j_+ - j_-$ és $k_+ - k_-$ közül az egyik eltűnik, akkor a g és h polinomok közül az egyik Newton-poligonjának van M meredekségű oldala, aminek hossza megegyezik az f Newton-poligonjának M meredekségű oldalának hosszával, míg a másik polinom Newton-poligonjának nincs M meredekségű oldala.
Azt kapjuk, hogy az f polinom Newton-poligonjának M meredekségű oldalának hossza megegyezik a g és h polinomok Newton-poligonjának M meredekségű oldalai hosszának összegével. És az (1) egyenlet azt mutatja, hogy ha g és h polinomok Newton-poligonjai közül csak az egyiknek van M meredekségű oldala, akkor az f Newton-poligonjának is van M meredekségű oldala, mégpedig a kettő hossza megegyezik. □

Következmény: Ha p prímre az f polinom Newton-poligonja pontosan egy részből áll, azaz a rész nem tartalmaz egész koordinátájú pontot, akkor az f polinom irreducibilis.

Példa: *Legyen p prím, $(c, p) = 1$ és $(m, n) = 1$. Ekkor a $x^n + cp^m$ polinom irreducibilis.*

Bizonyítás: A polinom Newton-poligonja egy részből áll, aminek végpontjai $(0, m)$ és $(n, 0)$. Mivel $(m, n) = 1$, ezért nem tartalmaz egész koordinátájú pontot a rész. Tehát a polinom irreducibilis. □

Példa: *A Schönemann–Eisenstein-kritérium bebizonyítható a tétel segítségével is.*

Bizonyítás: Az f polinom Newton-poligonja egy részből áll, aminek végpontjai $(0, 1)$ és $(n, 0)$, és ez a rész nem tartalmaz egész koordinátájú pontot. Tehát az f polinom irreducibilis. □

2.5. Polinomok domináns együtthatókkal

Ha egy polinomnak van egy elég nagy együtthatója, akkor ez biztosíthatja irreducibilitását. A következő tételek elégséges feltételeket adnak f polinom irreducibilitására.

A következő tételre szükség lesz az irreducibilitási tételek bizonyításához.

Tétel (Rouché): *Legyen f és g polinomok, és γ egy önmagát nem metsző zárt görbe a komplex síkban. Ha $|f(z)-g(z)|<|f(z)|+|g(z)|$ teljesül minden $z\in\gamma$ pontban, akkor f-nek és g-nek ugyanannyi gyöke van a γ görbe belsejében (multiplicitással számolva).*

A tétel bizonyítása megtalálható Prasolov könyvének első fejezetében ([1]).

Tétel (Perron-kritérium): *Legyen $f(x)=x^n+a_1x^{n-1}+\ldots+a_n$ egész együtthatós polinom, ahol $a_n\neq 0$.*
a) Ha $|a_1|>1+|a_2|+\ldots+|a_n|$, akkor f irreducibilis.
b) Ha $|a_1|\geq 1+|a_2|+\ldots+|a_n|$, és $f(\pm 1)\neq 0$, akkor f irreducibilis.

Bizonyítás: a) Először bizonyítsuk azt, hogy az f gyökei pontosan egy gyök kivételével az $|z|<1$ egységkör belsejébe esnek. A $g(x)=x^n+a_1x^{n-1}=x^{n-1}(x+a_1)$ polinomra igaz, hogy egy gyök kivételével a $|z|<1$ egységkörbe esnek, mivel a polinom gyökei: 0, ami $(n-1)$-szeres és $-a_1<-1$, ami egyszeres gyök. A Rouché-tétel miatt elég igazolni, hogy $|z|=1$-re:

$$|f(z)-g(z)|<|f(z)|+|g(z)|$$

De $|z|=1$-re egyrészt azt kapjuk, hogy:

$$|f(z)-g(z)|=\left|a_2z^{n-2}+\ldots+a_n\right|\leq|a_2|+\ldots+|a_n|<|a_1|-1 \qquad (1)$$

Másrészt:

$$|f(z)|+|g(z)|\geq|g(z)|=\left|z^n+a_1z^{n-1}\right|=|z+a_1|\geq|a_1|-1 \qquad (2)$$

Tegyük most fel indirekt módon, hogy f felírható f_1 és f_2 polinomok szorzataként, amiknek fokszáma pozitív. Az f_1 és f_2 polinomok gyökeinek szorzata nem nulla egész szám (azaz a szorzat abszolút értéke határozottan pozitv egész), ezért mindkét polinomnak van egynél nem kisebb abszolútértékű gyöke. De az f polinomnak csak egy egységkör belsején kívül elhelyezkedő gyöke van. Ez ellentmondás.

b) Ha a $|a_1| = 1+|a_2|+\ldots+|a_n|$, akkor az (1)-ben a határozott egyenlőtlenség helyett enyenlőség van. Ilyenkor viszon az $f(\pm 1) \neq 0$ feltétel teljesülése esetén a (2)-ban szereplő egyenlőtlenség lesz szigorú egyenlőtlenség: $|z| = 1$ esetén ugyanis $|f(z)| + |g(z)| = |a_1| - 1$ csak akkor teljesülhetne, ha mindkét egyenlőtlenségnél egyenlőség áll, azaz $|f(x)| = 0$ és $|z + a_1| = |a_1 - 1|$ egyszerre teljesül. Az utóbbi egyenlőség $a_1 \in \mathbb{R}$ miatt csak $z \in \mathbb{R}$ esetén teljesülhetne, így $z = \pm 1$. A feltevés miatt azonban $f(\pm 1) \neq 0$. $\square$

Tétel (Brauer): *Legyenek $a_1 \geq a_2 \geq \ldots \geq a_n$ pozitív egyészek és $n \geq 2$. Ekkor a $p(x) = x^n - a_1 x^{n-1} - a_2^{n-2} - \ldots - a_n$ polinom irreducibilis $\mathbb{Z}$ felett.*

Bizonyítás: Vegyük az $f(x) = (x-1)\,p(x)$ polinomot.

$$f(x) = (x-1)\,p(x) = (x-1)\left(x^n - a_1 x^{n-1} - a_2^{n-2} - \ldots - a_n\right) =$$

$$= x^{n+1} - x^n(a_1+1) + x^{n-1}(a_1 - a_2) + x^{n-2}(a_2 - a_3) + \ldots + x(a_{n-1} - a_n) + a_n$$

Jelöljük az együtthatókat b_i-vel $(i = 1, \ldots, n+1)$, tehát: $b_2 = a_1 - a_2, \ldots, b_n = a_{n-1} - a_n, b_{n+1} = a_n$, és legyen b_1 az x^n együtthatójának ellentetje, azaz $b_1 = a_1 + 1$. A $b_2, \ldots, b_n$ számok nemnegatív egészek; b_1, b_{n+1} pozitív egészek

$$b_1 = 1 + b_2 + \ldots + b_{n+1} \qquad (1)$$

a feltétel miatt. Az $f(x)$ függvényre teljesül a Perron-kritérium b) részének első feltétele, de a második feltételt nem teljesíti, mert $f(1) = 0$.
Legyen:

$$h(z) = b_1 z^n - b_2 z^{n-1} - \ldots - b_{n+1}$$

Megmutatjuk, hogy minden elég kicsi $\varepsilon > 0$-ra teljesül a $|z| = 1 + \varepsilon$ körön teljesül az alábbi:

$$|h(z)| > \left|z^{n+1}\right| = |f(z) + h(z)|$$

Ha $|z| = 1 + \varepsilon$, akkor

$$|h(z)| - \left|z^{n+1}\right| \geq b_1(1+\varepsilon)^n - b_2(1+\varepsilon)^{n-1} - \ldots - b_{n+1} - (1+\varepsilon)^{n+1}$$

A binomiális tétel szerint kifejtve a következőt kapjuk (csak a konstans tagot és az ε együtthatóját írjuk ki részletesen, a többi tag elhanyagolható ha ε elég kicsi):

$$|h(z)| - \left|z^{n+1}\right| \geq b_1 - b_2 - \ldots - b_{n+1} - 1 +$$

$$+\varepsilon\left(nb_1 - (n-1)\,b_2 - (n-2)\,b_3 \ldots - 2b_{n-1} - b_n - (n+1)\right) + \ldots =$$

Felhasználva az (1) egyenlőséget, a konstans tag 0.

$$\varepsilon\left(nb_1 - nb_2 + b_2 - nb_3 + 2b_3 \ldots - nb_{n-1} + (n-2)\,b_{n-1} - nb_n + (n-1)\,b_n - n - 1\right) + \ldots =$$

Minden n-nel szorzott tagot hozzunk az elejére:

$$= \varepsilon\left(nb_1 - nb_2 - \ldots - nb_n - n + b_2 + 2b_3 + \ldots + (n-1)\,b_n - 1\right) + \ldots =$$

Használva az (1) egyenlőség n-szeresét, kapjuk:

$$= \varepsilon\left(nb_{n+1} + b_2 + 2b_3 + \ldots + (n-1)\,b_n - 1\right) + \ldots$$

Mivel $b_{n+1} = a_n \geq 1$, ezért ε együtthatója alulról becsülhető a következő számmal

$$n + b_2 + 2b_3 + \ldots + (n-1)\,b_n - 1 \geq n - 1 \geq 1$$

Az ε együtthatója pozitív, ezért elég kicsi $\varepsilon > 0$-ra kapjuk, hogy $|h(z)| - \left|z^{n+1}\right| > 0$. Teljesül a következő:

$$|f(z) + h(z)| = \left|z^{n+1}\right| < |h(z)| \leq |f(z)| + |h(z)|$$

A Rouché-tétel miatt az $f(z)$ polinomnak annyi gyöke van a $|z| < 1 + \varepsilon$ körben, mint a $h(z)$ polinomnak. De $h(z)$-nek minden gyöke az egységkör belsejében van. Ha ugyanis $|z| \geq 1$, akkor:

$$|h(z)| \geq b_1 |z|^n - b_2 |z|^{n-1} - \ldots - b_{n+1} = |z|^n \left(b_1 - \frac{b_2}{|z|} - \frac{b_3}{|z|^2} - \ldots - \frac{b_{n+1}}{|z|^n}\right) \geq$$

$$\geq |z|^n \left(b_1 - b_2 - b_3 - \ldots - b_{n+1}\right) = |z|^n > 0$$

Ha $\varepsilon \to 0$, akkor az egységkör belsejében és határán az $f(x) = (x-1)\,p(x)$ polinomnak pontosan n gyöke van. Így a $p(x)$ polinomnak pontosan $n-1$ gyöke van az egységkör belsejében és legalább egy gyöke fekszik az egységkörön kívül. Ezért p irreducibilis. □

Tétel (Osada): *Legyen $f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x \pm p$ egész együtthatós polinom, ahol p prím.*
a) Ha $p > 1 + |a_1| + \ldots + |a_{n-1}|$, akkor f irreducibilis.
b) Ha $p \geq 1 + |a_1| + \ldots + |a_{n-1}|$ és f-nek nincs egy abszolútértékű gyöke, akkor f irreducibilis.

Bizonyítás: Tegyük fel, hogy $f(x) = g(x)\,h(x)$, ahol g és h pozitív fokú egész együtthatós polinomok. A g és h polinomok konstans tagjainak szorzata $\pm p$. Mivel p prím, ezért vagy g vagy h konstans tagja egyenlő ± 1-gyel. Ezért g és h közül az egyik gyökei abszolútértékeinek szorzata 1-gyel egyenlő. Ennek a polinomnak van egy α gyöke, melyre $|\alpha| \leq 1$. Mivel α gyöke f-nek is, ezért

$f(\alpha) = 0$-ból kapjuk, hogy:

$$p = \left|\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha\right| \leq 1 + |a_1| + \ldots + |a_{n-1}|$$

Az a) esetén ellentmondás.

A b) esetén α nem lehet az egységkörön, ezért $|\alpha| < 1$. Tehát $p < 1 + |a_1| + \ldots + |a_{n-1}|$, ami ellentmondás. $\square$

Tétel (Pólya): *Legyen f n-edfokú egész együtthatós polinom, és legyen $m = \left[\frac{n+1}{2}\right]$. Tegyük fel, hogy az $a_1, \ldots, a_n$ különböző egészekre $|f(a_i)| < 2^{-m}m!$ és az $a_1, \ldots, a_n$ számok nem gyökei az f-nek. Ekkor f irreducibilis.*

Bizonyítás: A következő segédállítás segítségével bizonyítjuk a tételt:

Lemma (Pólya): *Legyen g k-adfokú egész együtthatós polinom és legyenek $d_0 < d_1 < \ldots < d_k$ egész számok. Ekkor létezik olyan i, hogy $|g(d_i)| \geq k!2^{-k}$ teljesül.*

Bizonyítás: Vegyük a következő polinomot:

$$G(x) = (x - d_0) \cdot \ldots \cdot (x - d_k) \sum_{i=0}^{k} \frac{g(d_i)}{x - d_i} \prod_{j \neq i} \frac{1}{d_i - d_j}$$

Látható, hogy $deg\, G \leq k$ és $G(d_i) = g(d_i)$ minden $i = 0, \ldots, k$-ra, ezért $G(x) = g(x)$.

A G polinom legnagyobb fokú tagjának együtthatója:

$$\sum_{i=0}^{k} g(d_i) \prod_{j \neq i} \frac{1}{d_i - d_j}$$

A feltevés szerint ez az együttható nemnulla egész, ezért az abszolútértéke legalább 1.

Legyen ℓ az az index, melyre $|g(d_\ell)| \geq |g(d_j)|$ minden j-re. Ekkor

$$1 \leq \sum_{i=0}^{k} g(d_i) \prod_{j \neq i} \frac{1}{d_i - d_j} \leq |g(d_\ell)| \cdot \left| \sum_{i=0}^{k} \prod_{j \neq i} \frac{1}{d_i - d_j} \right|,$$

ezért

$$1 \leq \frac{g(d_\ell)}{\left| \sum_{i=0}^{k} \prod_{j \neq i} \frac{1}{d_i - d_j} \right|}.$$

Így a $|g(d_i)|$ számok közül valamelyik nem kisebb, mint

$$\frac{1}{\left|\sum\limits_{0\le i\le k}\prod\limits_{j\neq i}\frac{1}{|d_i-d_j|}\right|}\geq\frac{1}{\left|\sum\limits_{0\le i\le k}\prod\limits_{j\neq i}\frac{1}{|i-j|}\right|}=\frac{1}{\sum\limits_{0\le i\le k}\frac{1}{i!(k-i)!}}=\frac{k!}{\sum\limits_{0\le i\le k}\binom{k}{i}}=\frac{k!}{2^k}\ \square$$

A tétel bizonyításához visszatérve:
Tegyük fel indirekt módon, hogy f felírható g és h egész együtthatós polinomok szorzataként.
Feltehetjük, hogy $deg\, h\le deg\, g=k$. Ekkor $m\le k<n$. Világos, hogy $g(a_i)\neq 0$, és $g(a_i)$ osztója $f(a_i)$-nek, ezért

$$|g(a_i)|\le|f(a_i)|<\frac{m!}{2^m}.$$

Másrészt a Pólya lemmából tudjuk, hogy $|g(a_i)|\geq k!2^{-k}$ néhány a_i-re (a Pólya lemmát alkalmazzuk $d_i=a_{i+1}$-re). Ha $k\geq m$, akkor $k!2^{-k}\geq m!2^{-m}$. Ugyanis, ha $m=k+r$, akkor

$$\frac{m!}{k!}=(k+1)(k+2)\dots(k+r)\le 2^r=\frac{2^m}{2^k},$$

ami ellentmondás. $\square$

3. Háromtagú és négytagú polinomok irreducibilitása

3.1. Az $\mathbf{x^n \pm x^m \pm x^p \pm 1}$ alakú polinomok irreducibilitása

Legyen $f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3$, ahol $n > m > p \geq 1$, és $\varepsilon_i = \pm 1$. A kérdés, hogy mikor lesz az f polinom irreducibilis. Először megmutatjuk, hogy elég meggondolni azt az esetet, amikor $n \geq m + p$. Az f polinom akkor és csak akkor irreducibilis, ha az

$$\hat{f}(x) = x^n f\left(\frac{1}{x}\right) = 1 + \varepsilon_1 x^{n-m} + \varepsilon_2 x^{n-p} + \varepsilon_3 x^n$$

polinom irreducibilis. Ha $m+p > n$, akkor $(n-m)+(n-p) < n$, így ilyenkor az $f(x)$ polinom helyett az $\hat{f}(x)$ polinomot vizsgálhatjuk. Ha $m + p < n$, akkor azt kapjuk, hogy $(n-m)+(n-p) > n$. Kizárhatjuk a triviális esetet is, amikor $f(x) = (x^m + \varepsilon_2)(x^p + \varepsilon_1)$, azaz amikor $n = m+p$ és $\varepsilon_3 = \varepsilon_1\varepsilon_2$.

Egy s-edfokú $\varphi(x)$ polinomot rekurzívnak nevezünk, ha

$$\varphi(x) = \pm x^s \varphi\left(\frac{1}{x}\right).$$

Lemma (1): *Legyenek λ és λ^{-1} gyökei az $f(x)$ polinomnak. Ekkor a következő három pár feltételből az egyik teljesülni fog:*

$$(i)\ \ \lambda^n = -\varepsilon_3 \text{ és } \lambda^{m-p} = -\varepsilon_1\varepsilon_2,$$

$$(ii)\ \ \lambda^m = -\varepsilon_1\varepsilon_3 \text{ és } \lambda^{n-p} = -\varepsilon_2,$$

$$(iii)\ \ \lambda^p = -\varepsilon_2\varepsilon_3 \text{ és } \lambda^{n-m} = -\varepsilon_1.$$

Bizonyítás: Az $f(\lambda) = 0$ és az $f(\lambda^{-1}) = 0$ feltételek azt jelentik, hogy $\lambda^n + \varepsilon_1\lambda^m + \varepsilon_2\lambda^p + \varepsilon_3 = 0$, és $\lambda^n + \varepsilon_2\varepsilon_3\lambda^{n-p} + \varepsilon_1\varepsilon_3\lambda^{n-m} + \varepsilon_3 = 0$.

A második egyenletből kivonva az elsőt kapjuk, hogy

$$\varepsilon_2\varepsilon_3\lambda^{n-p} + \varepsilon_1\varepsilon_3\lambda^{n-m} - \varepsilon_1\lambda^m - \varepsilon_2\lambda^p = 0,$$

azaz,

$$\left(\varepsilon_2\lambda^{m-p} + \varepsilon_1\right)\left(\varepsilon_3\lambda^{n-m} - \varepsilon_1\varepsilon_2\lambda^p\right) = 0.$$

Így $\lambda^p = -\varepsilon_1\varepsilon_2\lambda^m$ vagy $\lambda^p = \varepsilon_1\varepsilon_2\varepsilon_3\lambda^{n-m}$. Helyettesítsük λ^p értékeit az $f(\lambda) = 0$ egyenletbe, eszerint fennáll, hogy vagy $\lambda^n = -\varepsilon_3$ vagy $(\lambda^m + \varepsilon_1\varepsilon_2)(\lambda^{n-m} - \varepsilon_1) = 0$. □

Prasolov könyvében (és Ljunggren cikkében) az alábbi - nem igaz - tétel szerepel:

Tétel *(Ljunggren): a) Ha az $f(x)$ polinomnak nincs egységgyöke, akkor $f(x)$ irreducibilis.*
b) Ha az $f(x)$ polinomnak pontosan q olyan gyöke van, amik egységgyökök, akkor az $f(x)$ polinom felírható két polinom szorzataként. Ahol az egyik fokszáma q és a gyökei az egységgyökök, míg a másik polinom irreducibilis.

A tétel "bizonyítás"-a a következő nem igaz lemmán alapul:

Lemma (2): *Legyen $f(x) = \varphi(x)\psi(x)$, ahol $\varphi(x)$ és $\psi(x)$ egy főegyütthatós pozitív fokszámú egész együtthatós polinomok. Ekkor az $\varphi(x)$ és $\psi(x)$ polinomok közül legalább az egyik rekurzív polinom.*

A könyvben szereplő bizonyítás a lemmára a következő:

„Bizonyítás": Legyen $r = deg\,\varphi$ és $s = n - r = deg\,\psi$. Tekintsük a következő polinomokat:

$$f_1(x) = x^r \varphi\left(\frac{1}{x}\right)\psi(x) = \sum_{i=0}^{n} c_i x^{n-i},$$

$$f_2(x) = x^s \psi\left(\frac{1}{x}\right)\varphi(x) = x^n f_1\left(\frac{1}{x}\right) = \sum_{i=0}^{n} c_{n-i} x^{n-i}.$$

Világos, hogy

$$f_1(x) f_2(x) = x^n f\left(\frac{1}{x}\right) f(x) = \left(\sum_{i=0}^{n} c_i x^{n-i}\right)\left(\sum_{i=0}^{n} c_{n-i} x^{n-i}\right) =$$

$$= \left(\varepsilon_3 x^n + \varepsilon_2 x^{n-p} + \varepsilon_1 x^{n-m} + 1\right)\left(x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3\right).$$

Az x^{2n} együtthatóját összevetve kapjuk, hogy $c_0 c_n = \varepsilon_3$, tehát $c_0 = \pm 1$ és $c_n = \pm 1$.
Az x^n együtthatóját összevetve kapjuk, hogy

$$c_0^2 + c_1^2 + \ldots + c_{n-1}^2 + c_n^2 = \varepsilon_3^2 + \varepsilon_2^2 + \varepsilon_1^2 + 1 = 4.$$

Mivel $c_0 = \pm 1$ és $c_n = \pm 1$, vagyis $c_0^2 = c_n^2 = 1$, ezért $c_1^2 + \ldots + c_{n-1}^2 = 2$. Azaz azt kapjuk, hogy $c_\alpha = \pm 1$ és $c_\beta = \pm 1$ valamely $1 \le \alpha < \beta \le n-1$-re, és minden más c_i együttható nulla. Az $f_1(x) f_2(x)$ polinom a következő két alakban írható (az x^n együtthatóit összevonva):

$$\left(c_0 x^n + c_\alpha x^{n-\alpha} + c_\beta x^{n-\beta} + c_n\right)\left(c_n x^n + c_\beta x^\beta + c_\alpha x^\alpha + c_0\right) =$$

$$= c_0 c_n x^{2n} + c_\alpha c_n x^{2n-\alpha} + c_\beta c_n x^{2n-\beta} + c_0 c_\beta x^{n+\beta} +$$

$$+c_0c_\alpha x^{n+\alpha}+c_\alpha c_\beta x^{n-\alpha+\beta}+\left(c_n^2+c_\beta^2+c_\alpha^2+c_0^2\right)x^n+c_nc_\beta x^\beta+$$

$$+c_\beta c_\alpha x^{n-\beta+\alpha}+c_nc_\alpha x^\alpha+c_0c_\alpha x^{n-\alpha}+c_0c_\beta x^{n-\beta}+c_0c_n \qquad (1)$$

és

$$\left(\varepsilon_3x^n+\varepsilon_2x^{n-p}+\varepsilon_1x^{n-m}+1\right)\left(x^n+\varepsilon_1x^m+\varepsilon_2x^p+\varepsilon_3\right)=$$

$$=\varepsilon_3x^{2n}+\varepsilon_2x^{2n-p}+\varepsilon_1x^{2n-m}+\varepsilon_1\varepsilon_3x^{n+m}+\varepsilon_2\varepsilon_3x^{n+p}+$$

$$+\varepsilon_1\varepsilon_2x^{n-p+m}+\left(1+\varepsilon_1^2+\varepsilon_2^2+\varepsilon_3^2\right)x^n+\varepsilon_1x^m+$$

$$+\varepsilon_2\varepsilon_1x^{n-m+p}+\varepsilon_2x^p+\varepsilon_3\varepsilon_2x^{n-p}+\varepsilon_3\varepsilon_1x^{n-m}+\varepsilon_3 \qquad (2)$$

Ezért, hogy összehasonlítsuk a két felírást, rendezzük az egy főegyütthatós polinomokat a fokszám szerint, csak a három legmagasabb fokú tagot figyelembe véve.
Az első felírásból a következő négy lehetőséget kapjuk:

$$\beta\le\frac{n}{2}\ :\ 2n>2n-\alpha>2n-\beta,$$

$$\beta>\frac{n}{2},\ \alpha\le n-\beta\ :\ 2n>2n-\alpha\ge n+\beta,$$

$$\beta>\frac{n}{2},\ \frac{n}{2}\ge\alpha>n-\beta\ :\ 2n>n+\beta>2n-\alpha, \qquad (3)$$

$$\beta>\frac{n}{2},\ \alpha>\frac{n}{2}\ :\ 2n>n+\beta>n+\alpha.$$

A második felírásból a következő két lehetőséget kapjuk:

$$n\ge 2m\ :\ 2n>2n-p>2n-m,$$

$$2m>n\ge m+p\ :\ 2n>2n-p\ge n+m. \qquad (4)$$

A két felírásban a legnagyobb tagokat összehasonlítva az (α,β) számpárnak négy lehetséges értéke van:

$$(\alpha,\beta)=(p,m)\,,\ (p,n-m)\,,\ (m,n-p)\ \text{vagy}\ (n-m,n-p)\,.$$

Vizsgáljuk meg a különböző lehetőségeket.
Ha $(\alpha,\beta)=(p,m)$, akkor összevetve a két egyenletet azt kapjuk, hogy $c_0c_n=\varepsilon_3$, $c_pc_n=\varepsilon_2$, $c_mc_n=\varepsilon_1$. Ezért $f_1(x)$-re a következőt kapjuk (felhasználva, hogy $c_n=\frac{1}{c_n}$):

$$f_1(x)=c_0x^n+c_px^{n-p}+c_mx^{n-m}+c_n=\frac{\varepsilon_3}{c_n}x^n+\frac{\varepsilon_2}{c_n}x^{n-p}+$$

$$+\frac{\varepsilon_1}{c_n}x^{n-m}+c_n=\frac{1}{c_n}\left(\varepsilon_3x^n+\varepsilon_2x^{n-p}+\varepsilon_1x^{n-m}+c_n^2\right)=$$

$$c_n\left(\varepsilon_3 x^n+\varepsilon_2 x^{n-p}+\varepsilon_1 x^{n-m}+1\right)=c_n x^n f\left(\frac{1}{x}\right)$$

Helyettesítsük be az $f_1(x)$ definíciójába a kapott értéket:

$$c_n x^n f\left(\frac{1}{x}\right)=x^r\varphi\left(\frac{1}{x}\right)\psi(x)$$

$$c_n x^s\varphi\left(\frac{1}{x}\right)\psi\left(\frac{1}{x}\right)=\varphi\left(\frac{1}{x}\right)\psi(x)$$

$$c_n x^s\psi\left(\frac{1}{x}\right)=\psi(x).$$

Tehát ekkor a $\psi(x)$ polinom rekurzív polinom.
Ha $(\alpha,\beta)=(n-m,n-p)$, akkor azt kapjuk, hogy $c_0c_n=\varepsilon_3,\quad c_0c_{n-m}=\varepsilon_1,\quad c_0c_{n-p}=\varepsilon_2$.
Ezért felhasználva, hogy $c_0=\dfrac{1}{c_0}$, azt kapjuk, hogy:

$$f_1(x)=c_0x^n+c_{n-m}x^{n-(n-m)}+c_{n-p}x^{n-(n-p)}+c_n=$$

$$=c_0x^n+\frac{\varepsilon_1}{c_0}x^m+\frac{\varepsilon_2}{c_0}x^m+\frac{\varepsilon_3}{c_0}=$$
$$=c_0\left(x^n+\varepsilon_1x^m+\varepsilon_2x^m+\varepsilon_3\right)=c_0f(x).$$

Hasonlóan kapjuk, hogy

$$\varphi(x)=c_0x^r\varphi\left(\frac{1}{x}\right).$$

Ekkor a $\varphi(x)$ polinom rekurzív polinom.
Ha $(\alpha,\beta)=(p,n-m)$, akkor hasonlítsuk össze az (1) egyenlet egytagú polinomjainak kitevőit $2n$-től n-ig

$$2n,\ 2n-p,\ n+m,\ 2n-m,\ n+p,\ 2n-m-p,\ n,$$

és a (2) egyenlet egytagú polinomjainak kitevőit $2n$-től n-ig

$$2n,\ 2n-p,\ 2n-m,\ n+m,\ n+p,\ n+m-p,\ n.$$

Ezért a $2n-m-p$ szám egyenlő az $n+m$, $n+p$, $n+m-p$ számok valamelyikével. A $2n-m-p=n+m$ és a $2n-m-p=n+p$ egyenlőségek ellentmondanak az $n\le m+p$ feltevésnek. Ezért $2n-m-p=n+m-p$, azaz $n=2m$. Így $(\alpha,\beta)=(p,m)$, azaz a $\psi(x)$ polinom rekurzív polinom.
Ha $(\alpha,\beta)=(m,n-p)$, akkor szintén azt kapjuk, hogy $n=2m$, azaz $(\alpha,\beta)=(n-m,n-p)$, tehát a $\varphi(x)$ polinom rekurzív polinom. "□"

A bizonyításban a (3)és (4) egyenleteknél van a hiba. Nem biztos, hogy a harmadiknak felírt kitevő a harmadik legnagyobb fokszámú, ugyanis lehet vele egyenlő fokszámú tag is, például a $\beta \leq \frac{n}{2} : 2n > 2n-\alpha > 2n-\beta$ esetben $2n-\beta = n+\beta$, ha $\beta = \frac{n}{2}$. Ekkor kieshet a $2n-\beta = n+\beta$ kitevőjű tag. Hasonlóan látható, hogy

$$n \geq 2m \,:\, 2n > 2n-p > 2n-m \geq n+m$$

Az egybeeső kitevőknél a tagok kiejthették egymást, így az adott kitevő eltűnt, és a kitevők összehasonlítása hamis alapföltevésből indult ki.

A lemmából az alábbi módon jönne ki a tétel (felhasználva az első lemmát is):

„Bizonyítás": Nyilván elegendő bizonyítanunk a b) részt, hiszen az a) rész ennek speciális esete.

Ha az $f(x)$-ek minden gyöke egységgyök, akkor készen vagyunk. Föltehető tehát, hogy $f(x)$-nek van olyan gyöke, ami nem egységgyök. Bontsuk $f(x)$-et irreducibilisek szorzatára $\mathbb{Q}[x]$-ben. (Nyilván föltehető, hogy az irreducibilis faktorok egész együtthatósak.) Legyen $\psi(x)$ ebben a fölbontásban olyan irreducibilis tényező, amelynek valamelyik gyöke nem egységgyök. Könnyen látható, hogy ekkor $\psi(x)$-nek egyik gyöke sem egységgyök, ellenkező esetben $\psi(x)$-nek valamelyik x^k-1 polinommal vett legnagyobb közös osztója $\psi(x)$-nek egy 1-től különböző valódi osztóját adná, ami $\psi(x)$ irreducibilitása miatt nem lehetséges. Így az alábbi fölbontást kapjuk: $f(x) = \varphi(x)\psi(x)$, és itt $\psi(x)$ irreducibilis, és egyik gyöke sem egységgyök. A 2-es lemma miatt $\varphi(x)$ és $\psi(x)$ közül az egyik polinom rekurzív, így minden gyökének a reciproka is gyök lesz. Az (1)-es lemma miatt ezek a gyökök egységgyökök. Így egyrészt azt kapjuk, hogy csak $\varphi(x)$ lehet rekurzív, másrészt $\varphi(x)$ minden gyöke egységgyök. Ezzel a b) rész bizonyítását befejeztük. "□"

A tételre egy ellenpélda a következő polinom:

$$x^8+x^4+x^2-1 = \left(x^2+1\right)\left(x^3+x^2-1\right)\left(x^3-x^2+1\right).$$

Ez valóban ellenpélda a fönti tételre, hiszen a racionális gyökteszt alapján x^3+x^2-1 és x^3-x^2+1 közül egyiknek sincs racionális gyöke, így mindketten irreducibilisek $\mathbb{Q}[x]$-ben. Másrészt egyikük sem egyezik meg egyik körosztási polinommal sem (ezek két elsőfokú eset kivételével páros fokúak), így a gyökeik nem egységgyökök. Van tehát két irreducibilis faktorunk is, amelynek nem egységgyökök a gyökei.

Mivel a Ljunggren tétel nem igaz, nézzük meg, hogy mi igaz helyette.

Az előbbi bizonyításban is, a fordított Schönemann–Eisenstein-kritériumnál is használtuk már a polinom reciprok polinomjának fogalmát: ha $h(x) = a_n x^n + \cdots + a_0$, és $a_0 \neq 0$, akkor legyen $\hat{h}(x) =$

$a_0x^n + \cdots + a_n = x^n h\left(x^{-1}\right)$.
Ha az $f(x)$ polinom faktorizálható, legyen $f(x) = c(x)\,d(x)$, ekkor legyen $g(x) = c(x)\,\hat{d}(x)$.Azt kapjuk, hogy $g(x)\,\hat{g}(x) = f(x)\,\hat{f}(x)$. $\qquad (I)$

Lemma (Ljunggren): *Legyen $f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3$, és $g(x)$ olyan egész együtthatós polinom, hogy teljesül rá a (I) egyenlőség. Ekkor $g(x)$ polinomnak pontosan négy nemnulla együtthatója van, és ezen együtthatók mindegyike ± 1.*

Bizonyítás: A $g(x)$ polinom n-edfokú, ezért $g(x) = \sum_{i=0}^{n} g_i x^i$. A hibás lemma bizonyításában megkaptuk, hogy $f(x)\,\hat{f}(x)$ polinomban az x^n együtthatója 4, ezért $g(x)\,\hat{g}(x)$ polinomban is 4-nek kell lennie x^n együtthatójának. Az x^n együtthatója a $g(x)\,\hat{g}(x)$ polinomban: $\sum_{i=0}^{n} g_i^2$. Mivel a $g(x)$ polinom nem állhat egyetlen tagból, ezért a polinomnak pontosan négy nemnulla együtthatója van, és ezek mindegyike ± 1. $\square$

A g polinom főegyütthatójáról feltehetjük, hogy 1. Ugyanis -1-gyel megszorozva a g polinomot a kapott polinom teljesítené a (I) egyenlőséget. Ekkor $g(x) = x^n + \delta_1 x^s + \delta_2 x^t + \delta_3$, ahol $n > s > t > 0$, és δ_1, δ_2, δ_3 mindegyike ± 1. Feltehető, hogy $n \geq s + t$, és ha $n = s + t$, akkor $\delta_1 \geq \delta_2\delta_3$. Ha nem így lenne, akkor kicserélhetnénk a g polinomot a $\delta_3\hat{g}$ polinommal, és $g(x)\,\hat{g}(x)$ változatlan lenne.

Tétel (Mills): *Tegyük fel, hogy $f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3$ és $g(x) = x^n + \delta_1 x^s + \delta_2 x^t + \delta_3$. Tegyük fel, hogy $n \geq m+p$, és ha $n = m+p$, akkor $\varepsilon_1 \geq \varepsilon_2\varepsilon_3$. Tegyük fel, hogy $n \geq s+t$, és ha $n = s+t$, akkor $\delta_1 \geq \delta_2\delta_3$. Ha $f(x)\,\hat{f}(x) = g(x)\,\hat{g}(x)$, akkor vagy $f(x) = g(x)$ vagy n osztható 8-cal és valamelyik $f(x)$ és $g(x)$ polinok közül*

$$x^{8r} + x^{7r} + x^r - 1 = \left(x^{2r} + 1\right)\left(x^{3r} + x^{2r} - 1\right)\left(x^{3r} - x^r + 1\right),$$

és a másik

$$x^{8r} + x^{4r} + x^{2r} - 1 = \left(x^{2r} + 1\right)\left(x^{3r} + x^{2r} - 1\right)\left(x^{3r} - x^{2r} + 1\right),$$

ahol $n = 8r$.

Bizonyítás: Kifejtve $f(x)\,\hat{f}(x)$, és $g(x)\,\hat{g}(x)$ polinomokat:

$$f(x)\,\hat{f}(x) = \varepsilon_3 x^{2n} + \varepsilon_2 x^{2n-p} + \varepsilon_1 x^{2n-m} + \varepsilon_1\varepsilon_3 x^{n+m} + \varepsilon_2\varepsilon_3 x^{n+p} + \varepsilon_1\varepsilon_2 x^{n-p+m} + h(x),$$

ahol $h(x) = 4x^n + \varepsilon_1 x^m + \varepsilon_2\varepsilon_1 x^{n-m+p} + \varepsilon_2 x^p + \varepsilon_3\varepsilon_2 x^{n-p} + \varepsilon_3\varepsilon_1 x^{n-m} + \varepsilon_3$ és

$$g(x)\,\hat{g}(x) = \delta_3 x^{2n} + \delta_2 x^{2n-t} + \delta_1 x^{2n-s} + \delta_1\delta_3 x^{n+s} + \delta_2\delta_3 x^{n+t} + \delta_1\delta_2 x^{n-t+s} + j(x),$$

ahol $j(x) = 4x^n + \delta_1 x^s + \delta_2\delta_1 x^{n-s+t} + \delta_2 x^t + \delta_3\delta_2 x^{n-t} + \delta_3\delta_1 x^{n-s} + \delta_3$.
A $h(x)$ és $j(x)$ polinomok n-edfokú polinomok.
Ha a két egyenletet egyenlővé tesszük, akkor kapjuk, hogy $\varepsilon_3 = \delta_3$ és (csak a legnagyobb tagokat kiírva)

$$\varepsilon_2 x^{2n-p} + \varepsilon_1 x^{2n-m} + \varepsilon_1\varepsilon_3 x^{n+m} + \varepsilon_2\varepsilon_3 x^{n+p} + \varepsilon_1\varepsilon_2 x^{n-p+m} + h(x) =$$

$$= \delta_2 x^{2n-t} + \delta_1 x^{2n-s} + \delta_1\delta_3 x^{n+s} + \delta_2\delta_3 x^{n+t} + \delta_1\delta_2 x^{n-t+s} + j(x) \qquad (II)$$

Tudjuk, hogy $2n-p > 2n-m$, $2n-p \geq n+m$, $n+m > n+p$, és $n+m > n+m-p$. A bal oldal legnagyobb fokú tagjának együtthatójához meg kell vizsgálnunk $\varepsilon_2 x^{2n-p}$ és $\varepsilon_1\varepsilon_3 x^{n+m}$ tagokat. Ezek a tagok vagy kiejtik egymást, vagy a legmagasabb fokszám a bal oldalon $2n-p$. Hasonlóan kapjuk, hogy $\delta_2 x^{2n-t}$ és $\delta_1\delta_3 x^{n+s}$ tagok vagy kiejtik egymást, vagy a bal oldalon a legmagasabb fokszám $2n-t$.

1. eset: Ha $\varepsilon_2 x^{2n-p} + \varepsilon_1\varepsilon_3 x^{n+m} = 0$ és $\delta_2 x^{2n-t} + \delta_1\delta_3 x^{n+s} = 0$. Ekkor $n = m+p = s+t$, $\varepsilon_2 + \varepsilon_1\varepsilon_3 = 0$, és $\delta_2 + \delta_1\delta_3 = 0$. Kapjuk, hogy $\varepsilon_1 = -\varepsilon_2\varepsilon_3$ és $\delta_1 = -\delta_2\delta_3$. Tudjuk, hogy $\varepsilon_1 \geq \varepsilon_2\varepsilon_3$ és $\delta_1 \geq \delta_2\delta_3$. Ezért $\varepsilon_1 = \delta_1 = 1$ és $\varepsilon_2\varepsilon_3 = \delta_2\delta_3 = -1$. Mivel $\varepsilon_3 = \delta_3$, ezért azt is kapjuk, hogy $\varepsilon_2 = \delta_2$. Az egyenlet a következő lesz:

   $$\varepsilon_2 x^{n-p+m} + h(x) = \delta_2 x^{n-t+s} + j(x)$$

   Mivel $m+p = s+t$, ezért $m = s$ és $p = t$, ekkor $h(x) = j(x)$, ezért $f(x) = g(x)$.
2. eset: Ha $\varepsilon_2 x^{2n-p} + \varepsilon_1\varepsilon_3 x^{n+m}$ és $\delta_2 x^{2n-t} + \delta_1\delta_3 x^{n+s}$ közül pontosan az egyik 0. Feltehetjük, hogy Ha $\varepsilon_2 x^{2n-p} + \varepsilon_1\varepsilon_3 x^{n+m} = 0$ és $\delta_2 x^{2n-t} + \delta_1\delta_3 x^{n+s} \neq 0$. Ekkor $n = m+p$, és $\varepsilon_2 + \varepsilon_1\varepsilon_3 = 0$, azaz $\varepsilon_1 = 1$ és $\varepsilon_2\varepsilon_3 = -1$. Az (II) egyenlet bal oldala $\varepsilon_2 x^{n+m-p} + h(x)$, a jobb oldal

   $$\delta_2 x^{2n-t} + \delta_1 x^{2n-s} + \delta_1\delta_3 x^{n+s} + \delta_2\delta_3 x^{n+t} + \delta_1\delta_2 x^{n-t+s} + j(x).$$

   A (II) egyenlet csak akkor teljesülhet, ha

   $$\varepsilon_2 x^{n+m-p} = \delta_2 x^{2n-t},\ \delta_1 x^{2n-s} + \delta_1\delta_3 x^{n+s} = 0,\ \delta_2\delta_3 x^{n+t} + \delta_1\delta_2 x^{n-t+s} = 0,\ h(x) = j(x),$$

   így $n+m-p = 2n-t$, $2n-s = n+s$, és $n+t = n-t+s$. Ezekből kapjuk, hogy

   $$s = \frac{n}{2},\ t = \frac{s}{2} = \frac{n}{4},\ \text{és}\ m-p = \frac{3n}{4}.$$

   Mivel $n = m+p$, ezért $m = \frac{7n}{8}$, és $p = \frac{n}{8}$. Tehát n osztható 8-cal.
   Az együtthatókból kapjuk, hogy $\varepsilon_2 = \delta_2$, $\delta_3 = -1$, és $\delta_1 + \delta_3 = 0$. Így $\delta_1 = 1$, $\varepsilon_3 = \delta_3 = -1$, és $\varepsilon_2 = \delta_2 = 1$. Ekkor $h(x) = j(x)$ is teljesül.

Mivel n osztható 8-cal, ezért legyen $n = 8r$, ekkor

$$f(x) = x^{8r} + x^{7r} + x^r - 1 = \left(x^{2r} + 1\right)\left(x^{3r} + x^{2r} - 1\right)\left(x^{3r} - x^r + 1\right),$$

és

$$g(x) = x^{8r} + x^{4r} + x^{2r} - 1 = \left(x^{2r} + 1\right)\left(x^{3r} + x^{2r} - 1\right)\left(x^{3r} - x^{2r} + 1\right).$$

3. eset: $\varepsilon_2 x^{2n-p} + \varepsilon_1\varepsilon_3 x^{n+m} \neq 0$ és $\delta_2 x^{2n-t} + \delta_1\delta_3 x^{n+s} \neq 0$. A (II) egyenletben a legmagasabb fokú tagnak meg kell egyeznie mindkét oldalon, azaz $\varepsilon_2 x^{2n-p} = \delta_2 x^{2n-t}$, ezért $\varepsilon_2 = \delta_2$ és $p = t$. Tudjuk még, hogy $\varepsilon_3 = \delta_3$, ezért $\varepsilon_2\varepsilon_3 x^{n+p} = \delta_2\delta_2 x^{n+t}$. A (II) egyenlet a következő lesz:

$$\varepsilon_1 x^{2n-m} + \varepsilon_1\varepsilon_3 x^{n+m} + \varepsilon_1\varepsilon_2 x^{n-p+m} + h(x) = \delta_1 x^{2n-s} + \delta_1\delta_3 x^{n+s} + \delta_1\delta_2 x^{n-t+s} + j(x)$$

Tegyük fel, hogy $h(x) = j(x)$, a kapott értékekre ellenőrizzuk majd, hogy ez teljesül-e. Ekkor

$$\varepsilon_1 x^{2n-m} + \varepsilon_1\varepsilon_3 x^{n+m} + \varepsilon_1\varepsilon_2 x^{n-p+m} = \delta_1 x^{2n-s} + \delta_1\delta_3 x^{n+s} + \delta_1\delta_2 x^{n-t+s}. \qquad (III)$$

Ha valamelyik teljesül a

$$\varepsilon_1 x^{2n-m} = \delta_1 x^{2n-s}, \qquad (IV)$$

vagy

$$\varepsilon_1\varepsilon_3 x^{n+m} = \delta_1\delta_3 x^{n+s}, \qquad (V)$$

vagy

$$\varepsilon_1\varepsilon_2 x^{n-p+m} = \delta_1\delta_2 x^{n-t+s} \qquad (VI)$$

közül, akkor azt kapjuk, hogy $m = s$ és $\varepsilon_1 = \delta_1$, így $f(x) = g(x)$. Ezért tegyük fel, hogy semelyik sem teljesül (IV), (V) és (VI) közül.
Ha az (III) egyenlet bal oldalának semelyik 2 nem ejti ki egymást, akkor a bal oldal tagjai valamilyen sorrendben megegyeznek a jobb oldal tagjaival, így

$$2n - m + n + m + n - p + m = 2n - s + n + s + n - t + s,$$

és

$$\varepsilon_1\varepsilon_1\varepsilon_3\varepsilon_1\varepsilon_2 = \delta_1\delta_1\delta_3\delta_1\delta_2.$$

Az egyenletekből következik, hogy $m - p = s - t$ és $\varepsilon_1\varepsilon_2\varepsilon_3 = \delta_1\delta_2\delta_3$, megint azt kapjuk, hogy $m = s$ és $\varepsilon_1 = \delta_1$, így $f(x) = g(x)$.

Ezért tegyük fel, hogy a (III) egyenlet bal oldalának 2 tagja kiejti egymást, így a jobb oldalon is kiejti egymást két tag. Az egyenlet egyik oldalán sem lehet az utolsó két tag összege 0, mert a fokszámaik különbözőek. Mivel a (IV), (V) és (VI) egyenletek közül egyik sem teljesül, ezért feltehetjük, hogy a bal oldalon az első és a harmadik tag összege, a jobb oldalon pedig az első és a második tag összege 0.
Azaz

$$\varepsilon_1 x^{2n-m} + \varepsilon_1\varepsilon_2 x^{n-p+m} = 0 \qquad (VII)$$

és

$$\delta_1 x^{2n-s} + \delta_1\delta_3 x^{n+s} = 0. \qquad (VIII)$$

A (III) egyenletből $\varepsilon_1\varepsilon_3 x^{n+m} = \delta_1\delta_2 x^{n-t+s}$.
A (VII) és $(VIII)$ egyenletből kapjuk, hogy $n = 2m - p$ és $n = 2s$, ezekből következik, hogy $s < m$. Másrészt a $(VIII)$ egyenletből kapjuk, hogy $m = s - t$, amiből következik, hogy $m < s$. Ellentmondást kaptunk.
A 3. esetben azt kaptuk, hogy $f(x) = g(x)$. □

Szeretnénk egy Ljunggren tételhez hasonló tételt kapni.

Legyen az $f(x)$ négytagú polinom, amit foktorizálni szeretnénk. Tegyük fel, hogy $n \geq m + p$, és ha $n = m + p$, akkor $\varepsilon_1 \geq \varepsilon_2\varepsilon_3$. Legyen $f(x) = a(x)\, b(x)$, ahol az $a(x)$ polinom minden gyöke egységgyök és a $b(x)$ polinomnak nincs egységgyöke. (Lehet $a(x)$ és $b(x)$ polinomok közül az egyik konstans.) Ekkor $\hat{a}(x) = \pm a(x)$és az első lemma miatt $b(x)$ polinomnak egyetlen gyöke sem gyöke a $\hat{b}(x)$ polinomnak. Ezért $a(x)$ a legnagyobb közös osztója az $f(x)$ és $\hat{f}(x)$ polinomoknak.
Tegyük fel, hogy a $b(x)$ polinom reducibilis, azaz $b(x) = b_1(x)\, b_2(x)$, ahol a $b_1(x)$ és $b_2(x)$ polinomok fokszáma pozitív. Ekkor

$$f(x) = a(x)\, b_1(x)\, b_2(x),$$

és

$$g(x) = a(x)\, b_1(x)\, \hat{b}_2(x).$$

Tudjuk, hogy $f(x)\,\hat{f}(x) = g(x)\,\hat{g}(x)$.
Ha $g(x) = \pm f(x)$, akkor $\hat{b_2}(x) = \pm b_2(x)$, ami nem lehetséges. Ezért $g(x) \neq \pm f(x)$.
Ha $g(x) = \pm\hat{f}(x)$, akkor

$$a(x)\, b_1(x) = \pm\hat{a}(x)\,\hat{b}_1(x) \text{ és } \hat{b}_1(x) = \pm b_1(x),$$

ami nem lehetséges. Ezért $g(x) = \pm\hat{f}(x)$.

Ljunggren tétele helyett az alábbi igaz.

Tétel (Mills): *Tegyük fel, hogy* $f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3$, *ahol* $n > m > p \geq 1$, *és* $\varepsilon_i = \pm 1$. *Legyen* $f(x) = a(x)\, b(x)$, *ahol az* $a(x)$ *polinomnak minden gyöke egységgyök és a* $b(x)$ *polinomnak nincs egységgyöke. Ekkor* $a(x)$ *polinom a legnagyobb közös osztója az* $f(x)$ *és* $\hat{f}(x)$ *polinomnak. A* $b(x)$ *tényező irreducibilis, kivéve, ha* $f(x)$ *a felírható a következő négy alak egyikeként:*

$$x^{8r} + x^{7r} + x^r - 1 = \left(x^{2r} + 1\right)\left(x^{3r} + x^{2r} - 1\right)\left(x^{3r} - x^r + 1\right),$$

$$x^{8r} - x^{7r} - x^r - 1 = \left(x^{2r} + 1\right)\left(x^{3r} - x^{2r} + 1\right)\left(x^{3r} - x^r - 1\right),$$

$$x^{8r} + x^{4r} + x^{2r} - 1 = \left(x^{2r} + 1\right)\left(x^{3r} + x^{2r} - 1\right)\left(x^{3r} - x^{2r} + 1\right),$$

$$x^{8r} - x^{4r} - x^{2r} - 1 = \left(x^{2r} + 1\right)\left(x^{3r} - x^{2r} + 1\right)\left(x^{3r} - x^{2r} + 1\right).$$

Ezekben az esetekben a harmadfokú tényezők irreducibilisek.

A lemma (2) helyett a következő igaz:

Lemma: *Ha* $f(x) = \varphi(x)\,\psi(x)$, *ahol* $\varphi(x)$ *és* $\psi(x)$ *egy főegyütthatós pozitív fokszámú egész együtthatós polinomok. Ekkor vagy a* $\varphi(x)$ *és* $\psi(x)$ *polinomok közül legalább az egyik rekurzív polinom, vagy az* $f(x)$ *polinom az előző tételbeli 4 speciális alak közül az egyik.*

A következő tételben feltesszük, hogy $f(x) \neq (x^m + \varepsilon_2)(x^p + \varepsilon_1)$. A tételek az előző két lemma segítségével bizonyíthatók.

A következő tétel segítségével meghatározható, hogy az f polinomnak mikor van egységgyöke.

Tétel: *Legyen* d *a legnagyobb közös osztója az* n, m *és* p *számoknak. Legyen*

$$n_1 = \frac{n}{d},\ m_1 = \frac{m}{d},\ p_1 = \frac{p}{d}$$

$$d_1 = (n_1, m_1 - p_1),\ d_2 = (m_1, n_1 - p_1),\ d_3 = (p_1, n_1 - m_1).$$

Ekkor ha van f*-nek egységgyöke, akkor az kielégíti az egyik egyenlőséget a következők közül:*

$$x^{dd_1} = \pm 1,\ x^{dd_2} = \pm 1,\ x^{dd_3} = \pm 1,$$

és ez egyszeres gyöke az f*-nek.*

Bizonyítás: Legyen f-nek az egységgyöke λ. Ekkor λ^{-1} is gyöke az f polinomnak. A (1) lemma szerint 3 feltétel lehetséges λ-ra.

Tekintsük például az (i) esetet: $\lambda^n = -\varepsilon_3$ és $\lambda^{m-p} = -\varepsilon_1\varepsilon_2$. Világos, hogy $(n, m-p) = dd_1$ és mivel léteznek olyan u és v egészek, hogy $dd_1 = nu + (m-p)v$. Mivel $\lambda^n = -\varepsilon_3 = \pm 1$ és $\lambda^{m-p} = -\varepsilon_1\varepsilon_2 = \pm 1$, ezért

$$\lambda^{dd_1} = (\lambda^n)^u \left(\lambda^{m-p}\right)^v = \pm 1.$$

A (ii) és (iii) eset hasonlóan meggondolható.
Már csak azt kell bizonyítani, hogy λ egyszeres gyöke az f polinomnak, azaz

$$\lambda f'(\lambda) = n\lambda^n + \varepsilon_1 m\lambda^m + \varepsilon_2 p\lambda^p \neq 0.$$

Helyettesítsük az (i), (ii) és (iii) eseteket egyenként a $n\lambda^n + \varepsilon_1 m\lambda^m + \varepsilon_2 p\lambda^p = 0$ egyenletbe. Az (i)-ből kapjuk:

$$n(-\varepsilon_3) + \lambda^p\left(\varepsilon_1 m\lambda^{m-p} + \varepsilon_2 p\right) = 0$$

$$\lambda^p(-\varepsilon_1\varepsilon_1\varepsilon_2 m + \varepsilon_2 p) = n\varepsilon_3$$

$$\varepsilon_2\lambda^p(p-m) = n\varepsilon_3$$

Hasonlóan kapjuk a (ii)-ból: $\varepsilon_2\lambda^p(p-n) = m\varepsilon_3$,
a (iii)-ból: $\varepsilon_1\lambda^m(m-n) = p\varepsilon_2\varepsilon_3$.
Azt szeretnénk tudni, hogy mely esetben lehetséges, hogy egy egységgyök gyöke a kapott egyenletnek.
A $\varepsilon_2\lambda^p(p-m) = n\varepsilon_3$ esetben $|\lambda| = 1$ nem lehet, mert az egyenlet két oldalnak abszolútértéke nem egyezhet meg, mert $n > m > p \geq 1$.
A $\varepsilon_2\lambda^p(p-n) = m\varepsilon_3$ és $\varepsilon_1\lambda^m(m-n) = p\varepsilon_2\varepsilon_3$ esetben $|\lambda| = 1$ esetén azt kapjuk, hogy $n = m+p$.
Ha $n = m+p$, akkor ezt visszahelyettesítve a lemma eseteibe, azt kapjuk, hogy a (ii) esetben a két egyenlet: $\lambda^m = -\varepsilon_1\varepsilon_3$, és $\lambda^m = -\varepsilon_2$, míg a (iii) esetben a két egyenlet: $\lambda^p = -\varepsilon_2\varepsilon_3$, és $\lambda^p = -\varepsilon_1$.
Mindkét esetben azt kapjuk, hogy $\varepsilon_3 = \varepsilon_1\varepsilon_2$, azaz az elején kizárt triviális esetet kapjuk, azaz $f(x) = (x^m + \varepsilon_2)(x^p + \varepsilon_1)$. □

3.2. Rabinowitz tétele

Tétel (Rabinowitz): *a) A $x^5 + x + n$ polinom akkor és csak akkor bontható irreducibilis másodfokú és harmadfokú polinomok szorzatára, ha $n = \pm 1$ vagy $n = \pm 6$.*
b) A $x^5 - x + n$ polinom akkor és csak akkor bontható irreducibilis másodfokú és harmadfokú polinomok szorzatára, ha $n = \pm 15$, $n = \pm 22440$ vagy $n = \pm 2759640$.

Bizonyítás: Bizonyítsuk egyben a két esetet, legyen a polninom $x^5 + mx + n$, ahol $m = \pm 1$. Tegyük

fel, hogy van faktorizációja a polinomnak:

$$x^5 + mx + n = \left(x^2 + ax + b\right)\left(x^3 + cx^2 + dx + e\right) =$$

$$= x^5 + x^4\left(c + a\right) + x^3\left(d + ac + b\right) + x^2\left(e + ad + bc\right) + x\left(ae + bd\right) + be,$$

x^4 együtthatójából kapjuk: $c = -a$,
x^3 együtthatójából kapjuk: $d - a^2 + b = 0 \Rightarrow d = a^2 - b$,
x^2 együtthatójából kapjuk: $e + a\left(a^2 - b\right) + b\left(-a\right) = 0 \Rightarrow e = a\left(2b - a^2\right)$,
x együtthatójából kapjuk: $aa\left(2b - a^2\right) + b\left(a^2 - b\right) = m \Rightarrow m = 3a^2b - a^4 - b^2,$ (1)
a konstans tag pedig: $n = ba\left(2b - a^2\right) = 2ab^2 - a^3b.$ (2)
Fejezzük ki az (1) egyenlőségből b^2-et:

$$b^2 = 3a^2b - a^4 - m,$$

és helyettesítsük be ezt a (2) egyenlősségbe:

$$n = 2a\left(3a^2b - a^4 - m\right) - a^3b$$
$$\Downarrow$$
$$n = 5a^3b - 2a^5 - 2am.$$

Fejezzük ki b-t az egyenlősségből

$$b = \frac{n + 2a^5 + 2am}{5a^3},$$

helyettesítsük vissza az (1) egyenlősségbe, és alakítsuk át.

$$\left(\frac{n + 2a^5 + 2am}{5a^3}\right)^2 = 3a^2\left(\frac{n + 2a^5 + 2am}{5a^3}\right) - a^4 - m$$

$$\frac{n^2 + 4a^{10} + 4a^2m^2 + 4a^5n + 4amn + 8a^6m}{25a^6} = \frac{3a^2n + 6a^7 + 6a^3m - 5a^7 - 5a^3m}{5a^3}$$

$$n^2 + 4a^{10} + 4a^2m^2 + 4a^5n + 4amn + 8a^6m = 5a^3\left(3a^2n + a^7 + a^3m\right)$$

$$n^2 + 4a^{10} + 4a^2m^2 + 4a^5n + 4amn + 8a^6m = 15a^5n + 5a^{10} + 5a^6m$$

$$n^2 - a^{10} + 4a^2m^2 - 11a^5n + 4amn + 3a^6m = 0$$

Rendezzük n szerint az egyenletet, és elmeljünk ki a konstans tagból a^2-et:

$$n^2 + n\left(4am - 11a^5\right) + a^2\left(4m^2 + 3a^4m - a^8\right) = 0$$

$$n^2 + n\left(4am - 11a^5\right) + a^2\left(m + a^4\right)\left(4m - a^4\right) = 0$$

Használva a megoldóképletet n-re:

$$n_{1,2} = \frac{11a^5 - 4am \pm \sqrt{\left(4am - 11a^5\right)^2 - 4a^2\left(m + a^4\right)\left(4m - a^4\right)}}{2} =$$

$$= \frac{11a^5 - 4am \pm \sqrt{16a^2m^2 + 121a^{10} - 88a^6m - 16a^2m^2 - 12a^6m + 4a^{10}}}{2} =$$

$$= \frac{11a^5 - 4am \pm \sqrt{125a^{10} - 100a^6m}}{2} = \frac{11a^5 - 4am \pm 5a^3\sqrt{5a^4 - 4m}}{2} \qquad (3)$$

Mivel az n szám egész, ezért $5a^4 - 4m$ négyzetszám, azaz létezik olyan z egész, hogy $5a^4 - 4m = z^2$. Tudjuk, hogy $m = \pm 1$, ezért a $z^2 - 5a^4 = \pm 4$ diofantikus egyenletet kell megoldani. Legyen $x = a^2$, tudjuk z és x paritásának meg kell egyeznie.Legyen $y = \frac{x+z}{2}$, ahol y is egész szám, z-t kifejezve: $z = 2y - x$ Ekkor a. diofantikus egyenlet a következőképpen néz ki:

$$(2y - x)^2 - 5x^2 = \pm 4,$$

$$4y^2 - 4xy + x^2 - 5x^2 = \pm 4,$$

$$y^2 - xy - x^2 = \pm 1, \qquad (4)$$

ahol x négyzetszám.
A következő állítás miatt x Fibonacci szám:

Állítás: *Ha egy (x, y) pozitív egész számpár kielégíti a $y^2 - xy - x^2 = \pm 1$ egyenletet, akkor $(x, y) = (F_k, F_{k+1})$ valamilyen $k \geq 0$-ra.*
Az állítás bizonyítása Phillip James-nek a When is a number Fibonacci? című cikkében megtalálható. ([8])

Ha $x = 0$ lenne, akkor $a = 0$, és akkor $n = 0$, ekkor triviális faktorizációk léteznek.
Ha $y = 0$, akkor $x = a^2 = 1$, ekkor $a = \pm 1$. Mivel 0 és 1 Fibonacci számok, ezért ezt az esetet az állítás is fedi.
Mivel csak a 0, 1 és 144 számok négyzetszámok a Fibonacci számok között, ezért $x = 0$ vagy $x = 1$ vagy $x = 144$. Az $x = 0$ nem lehet.
Vizsgáljuk az eseteket a szerint, hogy az $m = 1$ vagy $m = -1$.
Amikor $m = 1$:
Ha $a^2 = 1$, akkor $a = \pm 1$, és a (3) egyenletbe behelyettesítve $a = 1$-et

$$n_{1,2} = \frac{11 - 4 \pm 5\sqrt{5 - 4}}{2} = \frac{7 \pm 5}{2} \Rightarrow \begin{array}{l} n_1 = 6 \\ n_2 = 1 \end{array},$$

$a=-1$-et

$$n_{1,2}=\frac{-11+4\pm5\sqrt{5-4}}{2}=\frac{-7\pm5}{2}\Rightarrow\begin{array}{c}n_1=-1\\n_2=-6\end{array}.$$

Ha $a^2=144$, akkor $a=\pm12$, akkor $5\cdot144^2-4=103677$ nem négyzetszám.
Amikor $m=-1$:
Ha $a^2=1$, akkor $a=\pm1$, és a (3) egyenletbe befelyettesítve $a=1$-et

$$n_{1,2}=\frac{11+4\pm5\sqrt{5+4}}{2}=\frac{15\pm15}{2}\Rightarrow\begin{array}{c}n_1=15\\n_2=0\end{array},$$

$a=-1$-et

$$n_{1,2}=\frac{-11-4\pm5\sqrt{5+4}}{2}=\frac{-15\pm15}{2}\Rightarrow\begin{array}{c}n_1=0\\n_2=-15\end{array}.$$

Ha $a^2=144$, akkor $a=\pm12$, akkor $5\cdot144^2+4=103684=322^2$, a (3) egyenletbe befelyettesítve $a=12$-t

$$n_{1,2}=\frac{11\cdot12^5+4\cdot12\pm5\cdot12^3\cdot322}{2}=\frac{2737200\pm2782080}{2}\Rightarrow\begin{array}{c}n_1=2759640\\n_2=-22440\end{array},$$

$a=-1$-et

$$n_{1,2}=\frac{-11\cdot12^5-4\cdot12\pm5\cdot12^3\cdot322}{2}=\frac{-2737200\pm2782080}{2}\Rightarrow\begin{array}{c}n_1=22440\\n_2=-2759640\end{array}.\square$$

Irodalomjegyzék

[1] Victor V Prasolov: *Algorithms and Computation in Mathematics - Polynomials,* MCCME, 2001

[2] Michael Filaseta: *Irreducible polynomials theory,* 19-23, 1998

[3] Szele Tibor: *Bevezetés az algebrába*, 240-243, Tankönyvkiadó, 1977

[4] Kiss Emil: *Bevezetés az algebrába*, Typotex Kiadó, 2007

[5] Wilhelm Ljunggren: *On the Irreducibility of certain trinomials and quadrinomials*, Math. Scand. 8, 65-70, 1960

[6] W. H. Mills: *The factorization of certain quadrinomials*, Math. Scand. 57, 44-50,1985

[7] S. Rabinowitz: *The factorization of* $x^5 \pm x + n$, Math. Mag. 61, 191-193, 1988

[8] Phillip James: *When is a number Fibonacci?,* Department of Computer Science, Swansea University, 2009