Eötvös Loránd Tudományegyetem

Természettudományi Kar

Fónagy Fanni

Matematika BSc, Alkalmazott matematikus szakirány

Számelmélet feladatok szakkörre

Szakdolgozat

Témavezető: Dr. Szalay Mihály egyetemi docens

Algebra és Számelmélet Tanszék

Köszönetnyilvánítás

Ezúton szeretném megköszönni témavezetőmnek, Dr. Szalay Mihálynak, hogy elvállalta a konzulensi teendőket, hogy mindig segítséget nyújtott, ha elakadtam egy-egy ponton, és értékes tanácsaival, útmutatásával elkészülhetett a szakdolgozatom.
Szintén köszönettel tartozom a családomnak és barátaimnak, akik mindig támogattak és biztattak, s bármikor számíthattam türelmükre, szeretetükre az évek során.
Végül, de nem utolsó sorban szeretném kifejezni hálámat gimnáziumi és egyetemi tanáraimnak egyaránt, akik hozzájárultak szakmai fejlődésemhez.

Tartalomjegyzék

1. Bevezetés

Szakdolgozatom, ahogy a címe is mutatja, nem éppen tipikusan egy alkalmazott matematikus által választott téma. Akkor mégis miért éppen erre adtam a fejem? Már gimnáziumban is sokszor tartottunk egymásnak szakköröket, ezzel fejlesztve egymást, és ezek az órák nemcsak szép emlékekként élnek bennem, hanem mai napig hasznomra válnak. Az óraadás azóta sem áll távol tőlem, jó érzés amikor a kisebb, különböző feladatok hozzásegítik az embert egy nagyobb tétel beigazolásához. Erre több példát is látunk a dolgozatom során.
És miért éppen számelmélet? Egy Gauss klasszikust idézve: "A matematika a tudományok királynője, a számelmélet pedig a korona rajta." Valóban így gondolom én is: az egyetemi évek alatt rengeteg érdekes, olykor szép oldalát ismertük meg a matematikának, azonban a számelmélet tisztasága, kézenfekvősége miatt mindig is közelebb állt hozzám.
Mivel speciális matematika tagozatra jártam, ezért szakdolgozatom témája egy olyan szakkör, amin osztálytársaim és jómagam is minden héten részt vettünk. A tételek és feladatok különböző nehézségűek, hogy mindenki találjon köztük kedvére valót, amin elgondolkodhat. Minden óra különféle témákat dolgozott fel, szóval elmondható, hogy ezen szakkör előtt már volt szó a különböző algebrák felépítéséről, a természetes számoktól kezdve a komplex számokig bezárólag, és ismerjük már a különböző műveleteket tulajdonságaikkal együtt. Az előző óra szintén számelmélettel volt kapcsolatos, de az a kongruenciákról és az azzal kapcsolatos tételekről szólt leginkább.
Szakdolgozatom elején olyan alapfogalmakat ismételnék meg az előző szakkörről, amik nélkülözhetetlenek a későbbiekben, s a számelmélet alaptételével talán a legnevezetesebb algebrai tételt fogalmazom meg. A prímeknek nemcsak a matematikában, hanem a természetben is jelentős szerepük van, ezért kicsit mélyebben belemerülök a témába, sok érdekes állítással megfűszerezve. Végül a Gauss-egészekről írok azért, hogy megmutassam, nemcsak az egész számok körében érvényesek az alapfogalmak, a számelméleti tételek sokkal több számkörre kiterjeszthetőek.

2. A számelmélet alapjai

2.1. Alapfogalmak

Az alapvető matematikai műveleteket és számköröket a tulajdonságaikkal együtt már ismert tananyagnak tekintem, így ezek tudatában bevezetnék olyan alapfogalmakat, amikre a szakdolgozatom későbbi részében támaszkodni fogok.

1. Definíció: Adottak a és b egész számok. Azt mondjuk, hogy a osztója b-nek, ha létezik olyan c egész szám, hogy $ac = b$. Jele: $a \mid b$, ha a nem osztja b-t: $a \nmid b$.

Megjegyzés: $a = 0$ csak akkor lehet, ha $b = 0$, vagyis $0|0$, de $b = 0$ esetén a tetszőleges egész lehet.

2. Definíció: Egy egész számot **egységnek** nevezünk, ha minden egész számnak osztója. Jele: e.

Akkor mely egész számok egységek?

Nyilvánvalóan 1 és -1 azok, hiszen $1b = b$, így $1|b$, és $(-1)(-b) = b$, így $-1|b$. Tegyük fel, hogy e egység. Ekkor e így minden egésznek, vagyis 1-nek is osztója, tehát van olyan c egész szám, melyre $ec = 1$. $|e| \cdot |c| = 1$, így azonban e csak 1 vagy -1 lehet, mert $|e| \geq 1, |c| \geq 1$ miatt $|e| = 1$.

Megjegyzés: Mivel minden egész szám osztható az egységekkel, önmagukkal és ellentettjükkel, ezért ezeket *triviális osztóknak* nevezzük. Ebből adódóan egy adott egész szám többi osztóját *nemtriviális osztóknak* nevezzük.

3. Definíció: Egy k egész számot **felbonthatatlannak** nevezünk, ha $k \neq 0, e$ és bármely $k = cd$ felbontás esetén c vagy d egység.

Nézzünk egy példát! Bontsuk fel a 12*-t felbonthatatlanok szorzatára!* $12 = 2{\cdot}2{\cdot}3 = (-2){\cdot}(-2){\cdot}3 = (-2){\cdot}2{\cdot}(-3) = 2{\cdot}(-2){\cdot}(-3) = 2{\cdot}3{\cdot}2 = (-2){\cdot}(-3){\cdot}2 = (-2){\cdot}3{\cdot}(-2) = 2 \cdot (-3) \cdot (-2) = 3 \cdot 2 \cdot 2 = (-3) \cdot (-2) \cdot 2 = (-3) \cdot 2 \cdot (-2) = 3 \cdot (-2) \cdot (-2)$

Ez elsőre nagyon sokféle felbontásnak tűnhet, azonban észrevehető, hogy az eltérés csak a sorrendben és az egységszorzókban tapasztalható. Azt mondhatjuk, hogy a 12 esetében a felbonthatatlanok szorzatává való alakítás lényegében egyértelmű, azaz bármely két felbontásban a tényezők egyértelműen összepárosíthatóak úgy, hogy az egymásnak megfelelő tényezők egymás egységszeresei legyenek. Természetesen adódik a kérdés, hogy minden egész számra teljesül-e ez a megállapítás. Sokan

ezt nyilvánvalónak érzik, mégis szükség van a bizonyításra, mert más számkörökben ez nem feltétlenül igaz.

4. Tétel (A számelmélet alaptétele): Bármely $n \neq 0, e$ egész szám felbontható véges sok felbonthatatlan egész szorzatára, és ez a felbontás lényegében egyértelmű.

Bizonyítás: az állítás két részből áll; a felbonthatóságból és a lényegi egyértelműségből.

a) a felbonthatóság bizonyítása: Ha n felbonthatatlan, akkor az n egytényezős szorzat megfelelő. Ha n nem felbonthatatlan, akkor van legkisebb pozitív nemtriviális osztója, legyen ez f_1. Ez nyilván felbonthatatlan (máskülönben nem lenne minimális), így $n = f_1 n_1$. Ha n_1 felbonthatatlan, akkor az $f_1 n_1$ szorzat már megfelelő, azonban ha nem, akkor ugyanazt csináljuk n_1-gyel, mint n-nel, így $n_1 = f_2 n_2$. Mivel $1 < |n_1| < |n|$, továbbfolytatva a gondolatot $1 < |n_2| < |n_1| < |n|$. Ha n_2 még mindig nem felbonthatatlan, ugyanezt az eljárást folytatjuk k lépésben, így $n = f_1 f_2 \dots f_k n_k$, ahol $f_1, f_2, ..., f_k$ felbonthatatlanok, és $1 < |n_k| < \dots < |n_2| < |n_1| < |n|$. Ezekből az egyenlőtlenségekből látszik, hogy az eljárás véges sok lépésben véget ér, mert 1 és n között is véges sok különböző egész szám van, így valamikor az utolsó tényező is felbonthatatlan lesz.

b) a lényegi egyértelműség bizonyítása: Legyen n olyan egész, ami nem 0, nem egység, és $n = f_1 f_2 .. f_r = g_1 g_2 \dots g_s$,ahol $f_1, \dots, f_r, g_1, \dots, g_s$ felbonthatatlanok. Ekkor $|n| > 1$ és $|n| = |f_1| \dots |f_r| = |g_1| \dots |g_s|$, és nyilván az összes szorzótényező pozitív, tehát elég lenne belátni, hogy $n > 1$ esetén n bármely pozitív felbonthatatlanok szorzatára való felbontásában ugyanazok a felbonthatatlanok szerepelnek ugyanannyiszor, legfeljebb eltérő sorrendben. Ez $n = 2$ esetén nyilvánvaló, sőt akkor is, ha $n > 2$ és felbonthatatlan.

Tegyük fel indirekt módon, hogy létezik olyan $n > 2$ egész, amelyre nem érvényes az egyértelműség. Elvben több is lehet, vegyük ezek közül a legkisebbet, legyen ez n_0, vagyis $2, 3, \dots, n_0 - 1$ egészekre még érvényes az egyértelműség. Mivel n_0 nem felbonthatatlan, ezért létezik legkisebb pozitív nemtriviális osztója, legyen ez p. Nyilván p felbonthatatlan (máskülönben nem lenne minimális), így $n_0 = pc$, ahol $1 < c < n_0$, vagyis c-re még érvényes az egyértelműség. Ezek szerint n_0 szám p-t tartalmazó felbontása egyértelmű, azonban az indirekt feltevés miatt akkor van p-t nem tartalmazó felbontása is. Ha belátnánk, hogy n_0 minden pozitív felbonthatatlanok szorzatává való alakításában benne van p, akkor ellentmondásra jutnánk, és így teljesülne az állítás.

Legyen $n_0 = h_1 \dots h_t$ egy tetszőleges felbontás ($t > 1$, mivel n_0 nem felbonthatatlan), s a könnyebb vizsgálhatóság szempontjából legyen $a = h_1, b = h_2 \dots h_t$, vagyis $n_0 = ab, a|n_0, b|n_0$. A p definíciójából adódik, hogy $p \leq a$ és $p \leq b$, azonban ha valamelyiknél egyenlőség lenne, rögtön ellentmondásra jutnánk, így elég azt vizsgálni, amikor $p < a$ és $p < b$. Legyen $a' = a - p, n' = a'b$. Így $1 \leq a' < a$, ebből $1 < b \leq a'b < ab$, tehát $1 < n' < n$ (vagyis n'-re még érvényes az egyértelműség), és $n' = a'b = (a-p)b = ab - pb = n_0 - pb = pc - pb = p(c-b)$, tehát n' minden felbontásában szerepel p. Mivel $n' = a'b$, így p szerepel a' vagy b felbontásában. Az utóbbi esetben rögtön látszik az ellentmondás, hiszen $1 < b < n_0$, és ha $a' = pq$, akkor $a = a' + p = pq + p = p(q+1)$, vagyis $p|a$, és $1 < a < n_0$ miatt szintén ellentmondásra jutottunk.

Megjegyzés: A fenti bizonyítás *b)* része *Surányi Jánostól* származik.

A köztudatban azonban alig használatos a felbonthatatlan fogalom, ehhez a definícióhoz az emberek automatikusan a prím szót társítják. Ennek az az egyszerű oka van, hogy az egész számok körében a két fogalom ekvivalens, viszont ahhoz, hogy ezt belássuk, nézzük meg miként is definiáljuk a prímeket.

2.2. Prímek

5. Definíció: Azt mondjuk, hogy a p egész szám rendelkezik **prímtulajdonsággal** (röviden p prím), ha $p \neq 0, e$, és minden olyan a és b egész számra, melyre $p|ab$ teljesül, akkor $p|a$ vagy $p|b$ közül legalább az egyik igaz.

6. Tétel: Az egész számok körében minden felbonthatatlan szám rendelkezik prímtulajdonsággal.
Bizonyítás: Adott a, b egész számok, az alaptétel szerint egyértelműen felbonthatóak felbonthatatlanok szorzatára, legyen ez $a = f_1 f_2 ... f_m$ és $b = g_1 g_2 ... g_n$. Ha tetszőleges k felbonthatatlan számra igaz, hogy $k|ab$, vagyis $k|f_1 f_2 ... f_m g_1 g_2 ... g_n$, az alaptétel egyértelműsége miatt van olyan i vagy j ($i = 1, 2, ...m$; $j = 1, 2, ...n$), melyre $k = f_i$ vagy $k = g_j$, vagyis $k|a$ vagy $k|b$ igaz, tehát k rendelkezik prímtulajdonsággal.

Ha a tételt az alaptétel nélkül szeretnénk belátni, a bizonyítás előtt szükséges bevezetnünk egy újabb definíciót és állítást.

7. Definíció: Adott a, b egész számok, legalább az egyik nem 0. Ekkor d egész számot a **legnagyobb közös osztójuknak** nevezzük, ha $d|a$ és $d|b$, és minden olyan c egész számra, melyre $c|a$ és $c|b$ igaz, hogy $c \leq d$. Jelölés: $(a, b) = d$.

8. Állítás: Adott a, b, c egészek, $a \neq 0$. Ha $a|bc$ és $(a, b) = 1$, akkor $a|c$.
Bizonyítás: Mivel $(a, b) = 1$, ezért léteznek x, y egészek, melyre $ax + by = 1$, így $c = a(cx) + (bc)y$, amiből $a|bc$ miatt következik, hogy $a|c$.

Megjegyzés: Az, hogy léteznek ilyen x, y egészek, melyre felírható egy a fenti egyenlőség, egy későbbi alkalmazás során belátom.

6. Tétel bizonyítása: Legyen f felbonthatatlan egész, vagyis $f \neq 0, e$, és tekintsünk tetszőleges a, b egész számokat, melyre $f|ab$. Nyilvánvaló, hogy $(a, f)|f$, vagyis van olyan c egész szám, mely $c(a, f) = f$. Mivel f felbonthatatlan, ezért vagy c vagy (a, f) egység. Ha c egység, akkor $|f| = (a, f)$ vagyis $f|a$. Ha viszont $(a, f) = 1$, akkor a **8. Állítás** alapján $f|b$ adódik.

Ezzel azonban még csak annyit láttunk, hogy minden felbonthatatlan szám egyben prím is, viszont az még hátra van, hogy minden prímtulajdonsággal bíró szám egyúttal felbonthatatlan is.
Vegyünk egy $e, 0 \neq p$ prímet, és ha $p = ab$, akkor $p|a$ vagy $p|b$, azaz $a = pa_1$ vagy $b = pb_1$, ahol a_1, b_1 egészek. Ezek szerint $1 = a_1 b$ vagy $1 = ab_1$ igaz, így b vagy a valóban egység.

Következmény: Az egész számok körében a felbonthatatlan számok és a prímszámok ugyanazok, így a későbbiekben csak prímszámok vagy prímek elnevezést fogom használni.

2.3. Alkalmazások

9. Definíció: Adott a és b egész számok mellett d egész számot a **kitüntetett közös osztójuknak** nevezzük, ha $d|a$ és $d|b$, és minden c egészre, melyre $c|a$ és $c|b$ teljesül, igaz az is, hogy $c|d$.
Hány kitüntetett közös osztója lehet két egész számnak?
Nyilván $a = b = 0$ esetén 0 az egyetlen lehetőség, viszont nézzük most azt a lehetőséget, amikor a vagy b különbözik 0-tól, és d, d' egyaránt kitüntetett közös osztója a-nak és b-nek. A definícióból adódik, hogy $d|a$ és $d|b$, és minden c egészre, melyre $c|a$ és $c|b$ teljesül, igaz az is, hogy $c|d$, valamint $d'|a$ és $d'|b$, és minden c' egészre, melyre $c'|a$ és $c'|b$ teljesül, igaz az is, hogy $c'|d'$.

Mivel d közös osztó, ezért $d|d'$ igaz, s mivel d' is közös osztó, ezért $d'|d$ is igaz, vagyis ha $d = d'e$ és $d' = df$, akkor $d = d(ef)$. Nyilván $d \neq 0$, így $ef = 1$, vagyis a és b kitüntetett közös osztói legfeljebb egységszorzóban különbözhetnek $(d, -d)$. Legyen d_0 a legnagyobb közös osztó, s a definíciójából adódik, hogy $d \leq d_0$ és $-d \leq d_0$, vagyis $|d| \leq d_0$. Viszont 9. Definícióból $d_0|d$, vagyis $d_0 \leq |d|$. Eszerint csak d_0 és $-d_0$ lehet kitüntetett közös osztó, azonban ezekről még nem tudjuk, hogy tetszőleges c egészre $c|a$ és $c|b$ esetén $c|d_0$ és $c|-d_0$ is igaz-e. A következő két tétel ebben segít.

10. Tétel (A maradékos osztás tétele): Adott a, b egész számok, és $b \neq 0$. Ekkor van olyan q, r egész számok, melyekre $a = bq + r$, ahol $0 \leq r < |b|$. Az ilyen q, r egészek egyértelműen meghatározottak.
Bizonyítás: Vegyük az $a - bx$ alakú számokat, ahol x egész. Ezek között biztosan van nemnegatív (ha $a \geq 0$, akkor $a - 0 \cdot b$ jó, ha $a < 0$, akkor $a - ba$ vagy $a - b(-a)$ megfelelő, attól függően, hogy b pozitív vagy negatív). Tehát van olyan x_0 egész, melyre $a - bx_0 \geq 0$. Ha ez egyenlőséggel teljesül, akkor $q = x_0, r = 0$ máris jó. Ha viszont $a - bx_0 > 0$, akkor keressük a legkisebb $a - bx$ alakú számot $0, 1, ..., a - bx_0$ egészek között (van ilyen, legrosszabb esetben $a - bx_0$ jó), s legyen ez a legkisebb szám $a - bq = r$. Így $r \geq 0$ is igaz, és $r < |b|$-nek is teljesülnie kell, máskülönben $r - |b|$ egy r-nél kisebb, nemnegatív $a - bx$ alakú szám volna $(r - |b| = a - b(q \pm 1))$, ami ellentétben áll r választásával.

11. Tétel (Euklideszi algoritmus): Legyenek a, b egészek és $b \neq 0$. Ha $b|a$, akkor $|b|$ pozitív kitüntetett közös osztója a-nak és b-nek. Ha $b \nmid a$, akkor a maradékos osztás tételének legfeljebb $|b|$-szeri alkalmazásával kapunk olyan $q_1, q_2, ...q_{n+1}; r_1, r_2, ..., r_n$ egészeket, melyekre igaz a következő:

$a = bq_1 + r_1;\ 0 < r_1 < |b|;$
$b = r_1q_2 + r_2;\ 0 < r_2 < r_1;$
.
.
.
$r_{n-2} = r_{n-1}q_n + r_n;\ 0 < r_n < r_{n-1};$
$r_{n-1} = r_nq_{n+1} + 0.$

Ekkor r_n pozitív kitüntetett osztója a-nak és b-nek, továbbá léteznek olyan x, y egészek, melyre $r_n = ax + by$.
Bizonyítás: A előzőek miatt elég az utolsó két megállapítást bizonyítani. Először belátjuk, hogy $r_n|a$ és $r_n|b$. A legalsó sortól visszafelé lépegetve haladunk:

$r_n|r_{n-1}$, és nyilván $r_n|r_n$, vagyis az utolsó előtti sorból következik, hogy $r_n|r_{n-2}$ is teljesül. Teljes indukcióval belátható a folytatás: mivel $j = 0, 1, 2$-re már láttuk, hogy $r_n|r_{n-j}$, ezért tegyük fel, hogy alulról a j-edik sorig már eljutottunk, vagyis $r_n|r_n, r_n|r_{n-1}, ..., r_n|r_{n-j}$. Írjuk fel az $(n-j+1)$-edik egyenlőséget: $r_{n-(j+1)} = r_{n-j}q_{n-j} + r_{n-(j-1)}$. Az indukciós feltételből adódik, hogy így $r_n|r_{n-(j+1)}$ is igaz, és így haladva eljutunk oda, hogy $r_n|r_1, r_n|b, r_n|a$ is teljesül.
Ahhoz, hogy r_n kitüntetett legyen, vennünk kell egy c egész számot úgy, $c|a$ és $c|b$, s be kell látni, hogy ilyenkor $c|r_n$ is teljesül. Átrendezve az előbbi egyenlőségeket:

$r_1 = a - bq_1$;
$r_2 = b - r_1q_2$;
$r_3 = r_1 - r_2q_3$;
.
.
.
$r_n = r_{n-2} - r_{n-1}q_n$.

Az előző elvhez hasonlóan látható, hogy mivel $c|a$ és $c|b$, ezért $c|r_1$, és most lefelé haladva megkaphatjuk, hogy $c|r_n$.

Ezt használva a tétel utolsó állításához is eljuthatunk: az első sort behelyettesítjük a másodikba r_1 helyére, így $r_2 = -aq_1 + b(1 + q_1q_2)$ adódik, s ezt a két kifejezést a harmadik sorba helyettesítve, majd így tovább, mindig azt használva, hogy két szomszédos indexű r felírható $ax + by$ alakban, a végén eljutunk r_n kívánt előállításához.

Megjegyzés: Ezt az alakot használtam fel a **8. Állítás** bizonyításánál.

Megjegyzés: Most már látjuk, hogy a és b egész számoknak létezik kitüntetett közös osztója, azt hogy csak a legnagyobb közös osztó egységszeresei jöhetnek szóba már a 9. Definíció után tudtuk. Szóval így már bátran használhatjuk, hogy a legnagyobb közös osztó minden közös osztóval osztható.

12. Definíció: Adott m, n egészek, nem mindkettő 0. Azt mondjuk, hogy m, n **relatív prímek**, ha $(m, n) = 1$. (Vagyis akkor, ha $d|m$ és $d|n$, akkor d egység.)

13. Tétel: Tetszőleges a, b, m egészek, és $m \neq 0$ esetén:
a) ha $(a, m) = 1$, akkor $(a + mb, m) = 1$
b) ha $(a, m) = 1$ és $(b, m) = 1$, akkor $(ab, m) = 1$.

Bizonyítás: Az *a)* résznél ha $1 < c = (a + mb, m)$ lenne, akkor $c|m$ és $c|a + mb$, vagyis $c|a$, ami ellentmondana $(a, m) = 1$-nek. A *b)* állításnál felírható, hogy $1 = ax_1 + my_1; 1 = bx_2 + my_2$, és összeszorozva a kettőt kapnánk, hogy $1 = (ab)(x_1x_2) + m(by_1x_2 + ax_1y_2 + my_1y_2)$. Vagyis $(ab, m) = 1$, hiszen $c|ab$, $c|m$ esetén $c|1$.

Az alaptétel átalakítása: Ha adott n egész számot pozitív prímek szorzatára akarjuk bontani, megtehetjük úgy is, hogy a tényezőket nagyság szerint rendezzük, és az azonos prímeket pedig hatványalakban írjuk fel. Vagyis bármely $n \geq 2$ egészhez egyértelműen megadható véges sok pozitív prím: $p_1 < p_2 < ... < p_r$ és $\alpha_1; \alpha_2; ...; \alpha_r$ pozitív egészek úgy, hogy $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$.

Megjegyzés: Ezt az alakot n *kanonikus felbontásának* szokás nevezni. A kanonikus alakot sokszor használják a gyakorlatban, ugyanis gyakran felmerülő kérdésekre ad könnyen érthető választ.

Mennyi osztója van egy számnak? Mennyi ezek összege?
Ha $d|n$, akkor nyilván d prímosztói is csak n prímosztói közül kerülhetnek ki, és egyetlen prím sem lehet nagyobb hatványon, mint amivel n-ben van. Tehát n összes d osztója $p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r}$ alakú, ahol $0 \leq \beta_1 \leq \alpha_1; 0 \leq \beta_2 \leq \alpha_2; ...; 0 \leq \beta_r \leq \alpha_r$.

Ebből már látható, hogy összesen $(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_r + 1)$ darab osztója van n-nek (hiszen ha $\forall i : \beta_i = 0$ $(i = 1, 2, ..., r)$, akkor az 1 triviális osztót kapjuk meg, és ha $\forall i : \beta_i = \alpha_i$ $(i = 1, 2, ..., r)$, akkor az n triviális osztót kapjuk meg). Az osztók számának jele: $d(n)$.

A pozitív osztók összege se nehezebb: $(1 + p_1 + p_1^2 + ... + p_1^{\alpha_1})(1 + p_2 + p_2^2 + ... + p_2^{\alpha_2})...(1 + p_r + p_r^2 + ... + p_r^{\alpha_r})$, mivel itt a beszorzás után a különböző d-k jönnek ki, mindegyik pontosan egyszer, mert a tagok száma pontosan $(\alpha_1+1)(\alpha_2+1)...(\alpha_r+1)$. Az osztók összegének a jele: $\sigma(n)$.

14. Tétel: Végtelen sok prímszám létezik.

Bizonyítás: Azt tudjuk, hogy léteznek prímek: $2, 3, 5, 7, ...$ Tegyük fel, hogy csak véges sok (pozitív) prím van, legyenek ezek $p_1, p_2, p_3, ..., p_k$. Tekintsük a következő számot: $n = p_1p_2p_3...p_k + 1$. Mivel $n > 1$, így az alaptétel szerint n-nek is van egy p pozitív prím osztója. Nyilván $p \nmid 1$, ezért különbözik $p_1, p_2, ..., p_k$ mindegyikétől, ami ellentmondás, hiszen feltételeztük, hogy csak ezek léteznek.

Mivel a legkisebb prímszámok elég közel vannak egymáshoz, így érdekesség, hogy a prímszámok között tetszőleges nagy hézag lehet, pontosabban:

15. Tétel: Bármely m pozitív egész számhoz megadható m db egymás utáni egész szám, melyek egyike sem prím.

Bizonyítás: Az $(m+1)!+2; (m+1)!+3; (m+1)!+4; \ldots; (m+1)!+m; (m+1)!+m+1$ egymás utáni egész számok, összesen m db és mindegyik összetett, ugyanis $1 < i < m+2$ esetén i nemtriviális osztója $(m+1)!+i$ - nek.

Megjegyzés: A

$$\prod_{p \leq m+1} p = K$$

is használható $(m+1)!$ helyett, ugyanis $K+i$ (i mint az előbb) szintén összetett, hiszen az alaptétel miatt i-nek is van olyan osztója (az 1-en kívül), ami osztója K-nak is.

Vizsgáljuk azt, hogy milyen különbség fordulhat elő még két prímszám között! 1-et csak akkor kaphatunk, ha a két szám szomszédos, vagyis az egyik páros, azt viszont tudjuk, hogy a 2 az egyetlen páros prím, így csak a $3-2=1$ lehetséges. A 2, mint differencia sokkal gyakoribb: $5-3, 7-5, 13-11, 19-17$, stb.

16. Definíció: Ha p és $p+2$ egyaránt prímszám, akkor $\{p, p+2\}$ ikerprím-pár.

Felvetődik az a kérdés, hogy hányszor fordulhat elő, hogy két prím különbsége 2, vagyis mennyi ikerprím-pár létezik. Ez egy máig megoldatlan probléma, holott már az ókorban is foglalkoztak a kérdéssel.

Hasonló érdekesség, hogy létezik-e végtelen sok p prím, melyre $p-1$ négyzetszám? (pl. $17-1=4^2$)
Ha ebben a problémában $p-1$ helyett $p+1$ -re lenne feltétel, hogy négyzetszám legyen, lényegesen könnyebb feladatot kapnánk.

2.4. Feladatok

1. Feladat: Milyen p prímekre teljesül, hogy $p+1=n^2$, ahol n egész szám?
Megoldás: Feltehető, hogy $n > 0$. Nézzük azon p prímeket, melyre $p+1=n^2$, vagyis $n^2-1=p$. Szorzattá bontva a bal oldalt azt kapjuk, hogy $(n-1)(n+1)=p$, vagyis a két tag közül az egyik 1, a másik p, és nyilván csak $n-1$ lehet 1, így $n=2$, és $p=3$ adódik. (Valóban: $3+1=2^2$)

2. Feladat: Határozzuk meg 6930 és 14994 legnagyobb közös osztóját!
Megoldás: $6930 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$ és $14994 = 2 \cdot 3^2 \cdot 7^2 \cdot 17$, vagyis a $(6930, 14994) = 2 \cdot 3^2 \cdot 7 = 126$.

3. Feladat: Bizonyítandó, hogy $n > 2$ esetén az $n, n+1, n+2, n+3$ között van olyan, aminek legalább 2 különböző prímosztója van.
Megoldás: Négy egymást követő egész szám között biztosan van két páros, és ezek közül pontosan az egyik osztható néggyel is. Nézzük azt a számot, ami 2-vel osztható, de 4-gyel nem! Ha ennek nem lenne a 2-n kívül más prímosztója, akkor ez csak a 2 lehet, vagyis a négy szám közül az egyik biztosan a 2. Mivel az adott négy szám közül a legkisebb n, de a másik feltétel szerint $n > 2$, vagyis egyik sem lehet a 2, ezért ellentmondásra jutottunk, biztosan kell lennie olyan számnak, aminek két különböző prímosztója van ($n =$ 2-re még nem igaz: $2, 3, 4, 5$ még ellentmond a feladat feltételének).

4. Feladat: Bizonyítandó, hogy $n > 6$ esetén az $n, n+1, n+2, ..., n+23$ között van olyan, aminek legalább 3 különböző prímosztója van.
Megoldás: 24 egymást követő egész szám között biztosan van négy, ami osztható 6-tal. E négy szám között pontosan kettő van, ami 2-vel osztható, de 4-gyel nem, s ezek különbsége 12. Mivel a különbségük nem osztható 9-cel, ezért legalább az egyik kanonikus alakjában a 3 kitevője csak 1 lehet, nagyobb nem. Vagyis van olyan szám, ami 6-tal osztható, de sem 12-vel, sem 18-cal nem. Ha lenne harmadik prímosztója, akkor kész lennénk a feladattal. Feltehetjük tehát, hogy nincs más prímosztója, akkor a szám maga a 6. Mivel az adott 24 szám közül a legkisebb n, de a másik feltétel szerint $n > 6$, vagyis egyik sem lehet a 6, ezért ellentmondásra jutottunk, biztosan kell lennie olyan számnak, aminek két különböző prímosztója van ($n =$ 6-ra még nem igaz: $6, 7, 8, ..., 29$ még ellentmond a feladat feltételének).

5. Feladat: $2^n - 1$ és $2^n + 1$ mikor lehet ikerprím-pár?
Megoldás: Mivel $2^n - 1, 2^n, 2^n + 1$ három egymást követő egész szám, ezért biztosan van köztük 3-mal osztható, viszont nyilván nem 2^n lesz az. Így a szóban forgó két szám közül az egyik osztható 3-mal, viszont mivel prímnek is kell lennie, ezért az egyik 3. Ha a nagyobbik lenne az, akkor a kisebbik 1, ami nem prím, vagyis így nem lennének ikerprímek, így tehát csak $2^n - 1 = 3$ és $2^n + 1 = 5$ jöhet szóba, amik valóban ikerprímek.

6. Feladat: $p, p + 10, p + 14$ mikor lesz egyszerre prím?
Megoldás: Mivel a $0, 10, 14$ a 3 különböző maradékosztályaiba tartoznak, ezért a

$p, p+10, p+14$ közül az egyik biztosan osztható 3-mal, viszont mivel prímnek is kell lennie, az egyik 3. Ha csak pozitív prímek lehetnek a megoldások, akkor csak $p = 3$ lehet, így $p + 10 = 13$ és $p + 14 = 17$, amik valóban prímek, ha negatív prímek is szóba jöhetnek, akkor $p+10 = 3$ esetén $p = -7$ és $p+14 = 7$ is jó, viszont $p+14 = 3$ esetén $p + 10 = -1$ miatt ez nem jó megoldás.

7. Feladat: Az M alatti, de $p_1, ..., p_k$ prímek egyikével sem osztható pozitív egészek száma: $M + \sum_{l=1}^{k} \sum_{1 \le i_1 < ... < i_l \le k} (-1)^l \frac{M}{p_{i_1} ... p_{i_l}}$.
Bizonyítás: A logikai szita formulájának mintájára gondolkodhatunk most is! Az alaphalmaz 1-től M-ig az egész számok, és legyen benne k darab egymást metsző halmaz, az i-edikbe azok kerülnek, amik oszthatóak p_i-vel ($i = 1, 2, ..., k$). Most képzeletben helyezzük el az alaphalmaz elemeit az ábránkon! Arra vagyunk kíváncsiak, hány olyan elem van, ami egyetlen p_i halmazban sincs benne.
$1, ..., M$ között $\lfloor \frac{M}{p_i} \rfloor$ darab elem van, ami nem osztható p_i-vel. Ennek mintájára a logikai szitát használva az alábbi eredményt kapjuk a vizsgált kérdésre: $M - (\lfloor \frac{M}{p_1} \rfloor + \lfloor \frac{M}{p_2} \rfloor + ... \lfloor \frac{M}{p_k} \rfloor) + (\lfloor \frac{M}{p_1 p_2} \rfloor + \lfloor \frac{M}{p_1 p_3} \rfloor + ... + \lfloor \frac{M}{p_{k-1} p_k} \rfloor) - (\lfloor \frac{M}{p_1 p_2 p_3} \rfloor + ... + \lfloor \frac{M}{p_{k-2} p_{k-1} p_k} \rfloor) + ... + (-1)^k \lfloor \frac{M}{p_1 p_2 ... p_k} \rfloor$. Ha megfelelően átindexeljük és bevezetjük az összegzéseket, akkor pontosan azt a képletet kapjuk, amit a feladatban bizonyítani kellett.

8. Feladat: Bizonyítandó, hogy az n-edik prím, $p_n < 2^{2^n}$.
Megoldás: Legyen $n > m \ge 0$ és határozzuk meg először $(2^{2^n} + 1, 2^{2^m} + 1)$-et! Mivel $n \ge m+1$, ezért $2^{2^n} - 1 = (2^{2^{m+1}})^{2^{n-m-1}} - 1$ osztható $2^{2^{m+1}} - 1 = (2^{2^m} - 1)(2^{2^m} + 1)$-gyel, vagyis $(2^{2^m} + 1)$-gyel is. Tehát $(2^{2^n} + 1, 2^{2^m} + 1) = (2, 2^{2^m} + 1) = 1$. Így a $2^{2^n} + 1$ $(n = 0, 1, 2, ...)$ alakú számok között mindegyike szolgáltat legalább egy új prímet. Sőt, így látjuk, hogy $(2^{2^n} + 1)$-ig legalább $n + 2$ prímszám van a 2-vel együtt, vagyis $p_{n+2} \le 2^{2^n} + 1$, így $p_n \le 2^{2^n} - 1$.

3. Az $ak + b$ alakú prímek

3.1. Speciális esetek

Minél több szempontból vizsgáljuk a prímeket, annál érdekesebb eredményekhez jutunk, és minden nézőpont más-más alkalmazás miatt érdekes. Ebben a részben azt vizsgálom, milyen alakú prímek léteznek, illetve mennyi van belőlük. A 2-n kívül minden prím páratlan, vagyis $2j + 1$ alakú. A legalapvetőbb kérdés j paritásának vizsgálata, vagyis $4k + 1$ vagy $4k - 1$ alakú prímből létezik végtelen sok, esetleg mindkettőből (mivel végtelen sok prím van, ezért legalább az egyikből is végtelen soknak kell lenni).

9. Feladat: Minden $4k - 1$ alakú számnak van $4l - 1$ alakú prímosztója.

Bizonyítás: Ha prím, akkor nyilvánvalóan igaz. Mivel 2-vel nyilván nem osztható, ezért minden osztója páratlan. Ha a kanonikus felbontásában minden prím $4l + 1$ alakú lenne, akkor a prímek szorzata (vagyis az eredeti szám) is $4L + 1$ alakú lenne, hiszen $(4l_1+1)(4l_2+1)...(4l_p+1)$ számban beszorzás után minden tag osztható 4-gyel kivéve az utolsót, ami $1^p = 1$, vagyis az eredmény $4L + 1$ alakú. Ez viszont nem lehet, mert az eredeti szám $4k - 1$ alakú volt, ellentmondásra jutottunk, vagyis létezik $4l - 1$ alakú prímosztója.

10. Feladat: Végtelen sok $4k - 1$ alakú prímszám létezik.

Bizonyítás: Ilyen prím létezik, például $3, 7, 11$. Tegyük fel, hogy véges sok $4k - 1$ alakú prím van, legyenek ezek $p_1, p_2, ..., p_r$. Tekintsük az $A = 4p_1p_2...p_r - 1$ számot! Ha ez prím, akkor rögtön ellentmondásra jutottunk, mert A nyilván nem lehet egyenlő p_i $(i = 1, 2, ..., r)$ egyikével sem. Ha nem prím, akkor az előző lemma alapján létezik $4l - 1$ alakú prímosztója, legyen ez q. Azonban q különbözik p_i-k mindegyikétől (nyilván, mert p_i nem osztja az eredeti számot), vagyis találtunk egy újabb $4l - 1$ alakú prímszámot, ezzel ismét ellentmondásra jutottunk.

A következő kérdés, hogy létezik-e végtelen sok $4k + 1$ alakú prím is, vagy a prímek zöme $4k - 1$ alakú.

11. Feladat: Végtelen sok $4k + 1$ alakú prím létezik.

Bizonyítás: Ilyen prím mindenképpen létezik, például $5, 13, 17$. Tegyük fel, hogy csak véges sok ilyen prím van, legyenek ezek $q_1, q_2, ..., q_s$. Tekintsük az $B = (2q_1q_2...q_s)^2 + 1$ számot! Ha ez prím, akkor rögtön ellentmondásra jutottunk, mert

nyilván $B \neq q_i; (i = 1, 2, ..., s)$ egyikével sem. Ha nem prím, akkor vegyük egy tetszőleges p prímosztóját! Mivel $2, q_1, q_2, ..., q_s$ egyike sem osztója B-nek, így p ezektől különböző, vagyis $4l-1$ alakú. Mivel $(2q_1q_2...q_s)^2 \equiv -1 \bmod p$, innen $(2q_1q_2...q_s)^{p-1} \equiv (-1)^{\frac{p-1}{2}} \equiv (-1) \bmod p$ (mivel $p = 4l-1$, ezért $p-1 = 4l-2$, így $\frac{p-1}{2} = 2l-1$, vagyis páratlan). A Fermat-tétel szerint ha $p \nmid x$, akkor $x^{p-1} \equiv 1 \bmod p$, így $-1 \equiv 1 \bmod p$, vagyis $p = 2$, ami ellentmondás.

Vannak még elég könnyen vizsgálható esetek, ilyen például a $6k-1$ alakú prímek (ami ugyanúgy belátható, mint a $4k-1$ alakúak).

3.2. Általános eset, Dirichlet-tétel

Most tekintsük azonban az általános esetet! Milyen a, b esetén lesz $ak+b$ végtelen sok k-ra prím?

Szükséges feltétel, hogy a és b legnagyobb közös osztója 1 legyen (vagyis a és b relatív prímek legyenek), máskülönben ha $(a, b) = d > 1$, akkor $d|ak+b$ minden k egészre, így csak $d, -d$ jöhet szóba prímként, vagyis nem lehet végtelen sok $ak+b$ alakú prím. Azt viszont, hogy ez a feltétel elégséges is, csak 1837-ben sikerült belátnia *Peter Gustav Lejeune Dirichlet* matematikusnak.

17. Tétel (Dirichlet): Adott a, b egészek és $(a, b) = 1$. Ekkor végtelen sok k egész számra lesz $ak+b$ prím.

Tekintsünk bele a bizonyítás egyes részleteibe! Apró lépésnek tűnhet, de ez a legfontosabb gondolata a bizonyításnak: adott a, b relatív prímek mellett honnan tudhatjuk, hogy egyáltalán létezik-e $ak+b$ alakú prím, ha k pozitív egész? Ha ezt belátnánk, már könnyű lenne végtelen sok ilyen alakú prímet megadni, ugyanis ha $(a, b) = 1$, akkor a^m és b is relatív prímek minden m pozitív egészre. Így ha már tudjuk, hogy létezik $ak+b$ alakú prím (k pozitív egész), akkor az $a^m k_m + b$ ($m = 1; 2; 3; ...$) alakú számok között lesz végtelen sok prím (még ha olykor átfedés is lesz), ha $a \geq 2$, ugyanis $a^m k_m + b \geq 2^m + b > 2^m$. (Az $a = 1$ eset a végtelen sok prím van problémához vezet vissza, amit már beláttunk.)

A bizonyítás folytatása előtt szükséges bevezetnünk néhány definíciót.

18. Definíció (Euler-féle φ-függvény:) Tetszőleges n pozitív egész esetén $\varphi(n)$ az $1, 2, ..., n$ számok közül az n-hez relatív prímek számát jelöli (vagyis $\varphi(n)$ éppen a modulo n maradékosztályok száma).

19. Definíció: Az **n-edik komplex egységgyökök** azok a z komplex számok, melyekre igaz, hogy $z^n = 1$, ahol $n = 1, 2, 3, ...$ egy pozitív egész szám.

Megjegyzés: A komplex számokról a **4. fejezetben** érintőlegesen lesz szó, viszont mivel egy korábbi szakkörön már ez téma volt, ezért ismert anyagként kezelem.

20. Tétel: A prímek reciprokaiból képzett sor divergens, vagyis $\sum_p \frac{1}{p} = \infty$.

Megjegyzés: Ez volt az előző szakkörön az Euler-féle gondolattal.

Térjünk vissza a **Dirichlet-tétel** bizonyításának vázlatához!
Ha $P(x) = \sum_{\substack{p\leq x \\ p\equiv 1(4)}} \frac{1}{p} + \sum_{\substack{p\leq x \\ p\equiv -1(4)}} \frac{1}{p}$, akkor az előző tétel alapján $P(x) \to \infty$, ha $x \to \infty$.
Azonban jó lenne ezt szétválasztani! Legyen $Q(x) = \sum_{\substack{p\leq x \\ p\equiv 1(4)}} \frac{1}{p} - \sum_{\substack{p\leq x \\ p\equiv -1(4)}} \frac{1}{p}$. Így persze:

$$\sum_{\substack{p\leq x \\ p\equiv 1(4)}} \frac{1}{p} = \frac{1}{2}(P(x) + Q(x)); \qquad \sum_{\substack{p\leq x \\ p\equiv -1(4)}} \frac{1}{p} = \frac{1}{2}(P(x) - Q(x)).$$

A közös alsó korlát tehát $\frac{1}{2}(P(x) - |Q(x)|)$, a kérdés pedig az, hogy el tudja-e rontani $-|Q(x)|$ a $P(x)$ viselkedését. Ha $|Q(x)|$ egy x-től független alsó korlát alatt marad, s még általánosítható is lenne, akkor $\sum_{\substack{p\leq x \\ p\equiv a(m)}} \frac{1}{p}$ jól közelíthető lenne egy a-tól független $\sum_{p\leq x} \frac{1}{p}$-vel kapcsolatos kifejezéssel, amiből következne Dirichlet-tétele. Próbáljuk $Q(x)$-et megbecsülni! Ha a

$$\sum_{\substack{n\leq x \\ n\equiv 1(4)}} \frac{1}{n} - \sum_{\substack{n\leq x \\ n\equiv -1(4)}} \frac{1}{n} = \sum_{n\leq x} \frac{f(n)}{n}$$

kifejezés "megfelelő" $Q(x)$-nek, ahol f értelmezési tartománya a pozitív egész számok, és $f(n) = (-1)^{\frac{n-1}{2}}$ ha n páratlan, különben 0 (ekkor

$$\sum_{n\leq x} \frac{f(n)}{n} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + ... + \frac{1}{2[\frac{x-1}{2}] + 1}(-1)^{[\frac{x-1}{2}]},$$

ami $\frac{1}{n} - \frac{1}{n+2} = \frac{2}{n(n+2)} < \frac{2}{n^2}$ miatt korlátos), vagyis ekkor $Q(x)$ is korlátos lenne.

Nézzük most f tulajdonságait! Észrevehető, hogy:

1. $f(1) = 1$;

2. $a, b \in \mathbb{N}^+$ esetén $f(ab) = f(a)f(b)$;

3. $c, d \in \mathbb{N}^+$; $c \equiv d \bmod 4$ esetén $f(c) = f(d)$;

4. $n \in \mathbb{N}^+$; $(n, 4) \neq 1$ esetén $f(n) = 0$.

Ha most $m = 4$ helyett $m = 5$-re keresnénk hasonló tulajdonságú függvényt, akkor elég az $1, 2, 3, 4, 5$ modulo 5 teljes maradékrendszert vizsgálni! Nyilván ekkor $f(1) = 1$; $f(5) = 0$, és mivel $1 \equiv 2^4(5)$; $3 \equiv 2^3(5)$; $4 \equiv 2^2(5)$, ebből látszik, hogy $f(1) = f(2)^4$; $f(3) = f(2)^3$; $f(4) = f(2)^2$. Innen két jó választás is látszik azonnal: $f_1(2) = 1$; $f_2(2) = -1$, így azonban $f_1(2) = f_1(3)$ és $f_2(2) = f_2(3)$, vagyis nem sikerült a maradékosztályokat szétválasztani. Ha viszont figyelembe vennénk az $f(2)^4 = 1$ egyenlet nem valós gyökeit is, két újabb lehetőség adódna. *Összefoglalva:*

$m = 5$	1	2	3	4	5
f_1	1	1	1	1	0
f_2	1	-1	-1	1	0
f_3	1	i	$-i$	-1	0
f_4	1	$-i$	i	-1	0

Tehát úgy tűnik, sikerült egy olyan f függvényt találnunk $\mathbb{C}$-ben, ami érzékeny egy konkrét maradékosztályra. Így viszont általánosabban megfogalmazható definícióhoz jutunk, ha $m = 4, 5$ helyett általános m-et vizsgálunk.

21. Definíció: Legyen $m \geq 2$ egész. Azt mondjuk, hogy χ *karakter* mod m, ha $\chi : \mathbb{N}^+ \to \mathbb{C}$, és

1. $\chi(1) = 1$;

2. $a, b \in \mathbb{N}^+$ esetén $\chi(ab) = \chi(a)\chi(b)$;

3. $c, d \in \mathbb{N}^+$; $c \equiv d \bmod m$ esetén $\chi(c) = \chi(d)$;

4. $n \in \mathbb{N}^+$; $(n, m) \neq 1$ esetén $\chi(n) = 0$.

Megjegyzés: Ez a definíció $\mathbb{R}$-ben nem működik a célnak megfelelően, már kis m esetén is szükség van a komplex értékekre (ahogy $m = 5$ esetén láttuk).

$m=3$	1	2	3
χ_0	1	1	0
χ_1	1	-1	0

1. táblázat. Karakterek mod 3

$m=4$	1	2	3	4
χ_0	1	0	1	0
χ_1	1	0	-1	0

2. táblázat. Karakterek mod 4

Ha ezt a definíciót algebrai szempontok alapján is megvizsgáljuk, akkor érdekes megállapításokhoz jutunk. Az első pont "csak" azért lényeges, mert így látjuk, hogy χ egy olyan függvény, ami nem azonosan 0. A második pont láttán arra következtethetünk, hogy χ egy *teljesen multiplikatív* számelméleti függvény, ami - figyelembe véve a harmadik pontot - a modulo m redukált maradékosztályok multiplikatív csoportjából megy a nem 0 komplex számok csoportjába. Ez a leképezés egy csoporthomomorfizmus, s mindkét csoportban a szorzás kommutatív (vagyis Abel-csoportok), s így a **véges Abel-csoportok alaptétele** miatt felbonthatóak véges sok prímhatványrendű ciklikus csoport direkt szorzatára. A négyes pont azt mondja, hogy χ a nem redukált maradékosztályokon 0 (vagyis ezzel kiterjesztettük).

Nyilvánvaló példa a 21. definícióra az úgynevezett **főkarakter** modulo m: $\chi_0(n)=1$, ha $(n,m)=1$, különben 0.
Az $m=2$ esetben nincs is más karakter, az $m=3$, $m=4$ lehetőségei: (lásd 1. és 2. táblázat)

Legyen most $m\geq 2$ egész, χ karakter mod m, és $n\in\mathbb{N}^+$; $(n,m)\neq 1$ estén $\chi(n)=0$ egyértelmű, viszont $(n,m)=1$ esetén $n^{\varphi(m)}\equiv 1 \bmod m$, így $(\chi(n))^{\varphi(m)}=1$, vagyis $\chi(n)$ szükségképpen $\varphi(m)$-edik egységgyök, ez elvben $\varphi(m)$ darab lehetőség $\chi(n)$-re. Mivel egy mod m redukált maradékrendszeren felvett (legfeljebb $\varphi(m)^{\varphi(m)}$-féle) értékek már meghatározzák χ-t, ezért véges sok mod m karakter létezik, jelöljük a számukat K_m-mel. Ez a felső becslés várhatóan durva K_m-re a maradékosztályok közötti multiplikatív összefüggések miatt. (Ha például létezik egy g pozitív primitív gyök mod m, akkor $\forall n\in\mathbb{N}^+$; $(n,m)=1$ esetén létezik $k\in\mathbb{N}^+$, melyre $n\equiv g^k \bmod m$, így $\chi(n)=\chi(g^k)=(\chi(g))^k$, s ebből $K_m=\varphi(m)$ következne, de csupán bizonyos esetekre ($m=2;4;p^\alpha;2p^\alpha$ ($p>2$ prím). Egy röpke gondolat erejéig visszatérve az algebrai szemponthoz, ezek a pozitív primitív gyökök hatványai mod m megfeleltethetőek a modulo m redukált maradékosztályoknak. Hasonlóan lehet ciklikus csoportok karakterei segítségével az alaptétel révén az összes karaktert előállítani.) A következő tételek segítségével K_m pontos értékét kívánjuk kiszámolni, viszont nehézségük miatt olykor bizonyítások nélkül szerepeltetem őket.

22. Tétel: Legyen $a, m \in \mathbb{N}^+;\ (a,m) = 1;\ a \not\equiv 1 \bmod m$. Ekkor létezik olyan $\chi \bmod m$ karakter, amelyre $\chi(a) \neq 1$.

Most vizsgáljuk a mod m karakterek értékei közötti összefüggéseket! Legyen $m \geq 2;\ \chi$ karakter mod m. Ha $\chi = \chi_0$, akkor $\sum_{n=1}^{m} \chi_0(n) = \varphi(m)$ nyilvánvalóan. Ha $\chi \neq \chi_0$, akkor $m > 2$ és létezik olyan $a \in \mathbb{N}^+$, hogy $(a,m) = 1$, de $\chi(a) \neq 1$. Ekkor $\sum_{n=1}^{m} \chi(n) = \sum_{n=1}^{m} \chi(an) = \chi(a) \sum_{n=1}^{m} \chi(n)$, vagyis $\sum_{n=1}^{m} \chi(n) = 0$. Most legyen $m \geq 2;\ a \in \mathbb{N}^+$, és $\chi_1, \chi_2, ..., \chi_{K_m} = \chi_0$ az összes mod m karakter. Ekkor ha

- $a \equiv 1 \bmod m$, akkor $\sum_{j=1}^{K_m} \chi_j(a) = K_m$.
- $a \not\equiv 1 \bmod m$ és $(a,m) \neq 1$, akkor $\sum_{j=1}^{K_m} \chi_j(a) = 0$.
- $a \not\equiv 1 \bmod m$ és $(a,m) = 1$, így $m > 2$, és a **22. Tétel** alapján létezik χ karakter mod m, melyre $\chi(a) \neq 1$. Bevezetvén az $f_j : \mathbb{N}^+ \to \mathbb{C};\ f_j(n) = \chi(n)\chi_j(n)$ $(j = 1, 2, ..., K_m)$ hozzárendelést könnyen látható, hogy f_j is karakter mod m, és $f_j \neq f_k$, ha $j \neq k$. Így $\sum_{j=1}^{K_m} \chi_j(a) = \sum_{j=1}^{K_m} f_j(a) = \chi(a) \sum_{j=1}^{K_m} \chi_j(a)$, vagyis $\sum_{j=1}^{K_m} \chi_j(a) = 0$.

Így azt kaptuk, hogy $\sum_{j=1}^{K_m} \chi_j(a) = \sum_{\chi} \chi(a)$ vagy egyenlő K_m-mel (ha $a \equiv 1 \bmod m$), vagy 0 ($a \not\equiv 1 \bmod m$). Vagyis sikerült kikevernünk egy olyan függvényt, ami érzékeny a mod m maradékosztályra, ez $\sum_{\chi} \chi(a)$ (egyelőre $a \equiv 1$ esetben). Végül:

$$K_m = \sum_{n=1}^{m} \sum_{\chi} \chi(n) = \sum_{\chi} \sum_{n=1}^{m} \chi(n) = \sum_{n=1}^{m} \chi_0(n) = \varphi(m).$$

Legyen most $m \geq 2;\ \chi$ karakter mod m. Már láttuk, hogy $(n,m) = 1$ esetén $\chi(n)$ biztosan $\varphi(m)$-edik egységgyök, így $\chi(n)\overline{\chi(n)} = |\chi(n)|^2 = 1$.
A $\overline{\chi} : \mathrm{N}^+ \to \mathbb{C};\ \overline{\chi}(n) = \overline{\chi(n)} = \frac{1}{\chi(n)}$, ha $(n,m) = 1$ (különben 0) definícióval $\overline{\chi}$ ismét egy mod m karakter lesz. Számítsuk ki most $a, n \in \mathrm{N}^+$-ra $\sum_{\chi} \chi(n)\overline{\chi}(a)$ értéket!

- Ha $(n,m) \neq 1$ vagy $(a,m) \neq 1$, akkor az összeg 0.
- Ha $(n,m) = 1$ és $(a,m) = 1$, akkor létezik olyan $u \in \mathbb{N}^+$, hogy $au \equiv n \bmod m$, és $(u,m) = 1$. Ekkor tehát

$$\sum_{\chi} \chi(n)\overline{\chi}(a) = \sum_{\chi} \chi(au)\overline{\chi}(a) = \sum_{\chi} \chi(a)\chi(u)\frac{1}{\chi(a)} = \sum_{\chi} \chi(u) = K_m = \varphi(m)$$

ha $u \equiv 1 \bmod m$, különben pedig 0.

Mivel $(n,m) = (a,m) = 1$ esetén az $u \equiv 1 \bmod m$ azt jelenti, hogy $a \equiv n \bmod m$ (ez az előzőekből is érezhető volt: $\sum_{\chi} \chi(n)\overline{\chi}(a) = \sum_{\chi} \chi(n)\frac{1}{\chi(a)} = \sum_{\chi} \chi(\frac{n}{a})$, vagyis ahogy az előbb $a \equiv 1 \bmod m$ volt a választó eset, most $\frac{n}{a} \equiv 1 \bmod m$ a választó eset, azaz $a \equiv n \bmod m$ kongruenciát kell vizsgálni). Ezek után megfogalmazható az előző megállapítások konzekvenciája:

23. Tétel: $m \geq 2$ esetén a mod m karakterek száma $K_m = \varphi(m)$, továbbá $\sum_{n=1}^{m} \chi(n) = \varphi(m)$, ha $\chi = \chi_0$, különben 0. Ha $n, a \in \mathbb{N}^+$ és $(a,m) = 1$, akkor $\sum_{\chi} \chi(n)\overline{\chi}(a) = \varphi(m)$, ha $n \equiv a \bmod m$, egyébként pedig 0.

A legfontosabb alkalmazás, ami miatt boncolgattuk a karakterek témáját, s fel kell írjuk az előző tételt: $a \in \mathbb{N}^+$; $(a,m) = 1$ esetén:

$$\frac{1}{\varphi(m)} \sum_{p \leq x} \frac{1}{p} \sum_{\chi} \chi(p)\overline{\chi}(a) = \sum_{\substack{p \leq x \\ p \equiv a(m)}} \frac{1}{p},$$

s ezzel pont az elején szereplő $\frac{1}{2}(P(x) \pm Q(x))$ kifejezést sikerült általánosítani. Ha $|Q(x)|$ valóban egy x-től független korlát alatt maradna, s még általánosítható is lenne, akkor rögzített m és $(a,m) = 1$ esetén nagy x-re $\sum_{\substack{p \leq x \\ p \equiv a(m)}} \frac{1}{p}$ jól közelíthető lenne $\frac{1}{\varphi(m)} \sum_{p \leq x} \frac{1}{p}$-vel, amiből következne Dirichlet-tétele. A következőkben $\sum_{p \leq x} \frac{1}{p}$ helyett érdemesebb a könnyebben kezelhető $\sum_{p \leq x} \frac{\log p}{p}$ kifejezéssel dolgozni.

24. Tétel: Létezik olyan $c > 0$ konstans, hogy $\forall x \geq 2$-re $|\sum_{p \leq x} \frac{\log p}{p} - \log x| < c$.

Megjegyzés: Be lehet látni $n!$ Legendre-alakjából ($n! = \prod_{p \leq n} p^{\alpha_{p,n!}}$, ahol $\alpha_{p,n!} = \sum_{i=1}^{\infty} [\frac{n}{p^i}]$).

S ezek után már megfogalmazható az a tétel, amiből Dirichlet tétele azonnal következik. A bizonyítás redukciós lépésekben történik, amit 1950-ben *H.N. Shapiro* dolgozott ki.

25. Tétel: Legyen $a, m \in \mathrm{N}^+;\ m \geq 2;\ (a,m) = 1$. Ekkor létezik olyan pozitív c_m korlát, hogy $\forall x \geq 2$-re: $|\sum\limits_{\substack{p \leq x \\ p \equiv a(m)}} \frac{\log p}{p} - \frac{1}{\varphi(m)} \log x| < c_m$.

Bizonyítás: m-et rögzítjük, és mod m karaktereket használunk. A **23. Tétel** révén

$$\frac{1}{\varphi(m)} \sum_{p \leq x} \frac{\log p}{p} \sum_{\chi} \chi(p)\overline{\chi}(a) = \sum_{\substack{p \leq x \\ p \equiv a(m)}} \frac{\log p}{p}.$$

A becslés domináns részét a χ_0 főkarakter adja, mert

$$\frac{1}{\varphi(m)} \sum_{p \leq x} \frac{\log p}{p} \chi_0(p)\overline{\chi_0}(a) = \frac{1}{\varphi(m)} \sum_{p \leq x} \frac{\chi_0(p) \log p}{p} =$$

$$= \frac{1}{\varphi(m)} \sum_{\substack{p \leq x \\ (p,m)=1}} \frac{\log p}{p} = \frac{1}{\varphi(m)} \sum_{p \leq x} \frac{\log p}{p} - \frac{1}{\varphi(m)} \sum_{\substack{p \leq x \\ p \mid m}} \frac{\log p}{p}.$$

Most a **25. Tétel** felhasználásával

$$|\sum_{\substack{p \leq x \\ p \equiv a(m)}} \frac{\log p}{p} - \frac{1}{\varphi(m)} \log x| \leq \frac{c}{\varphi(m)} + \frac{1}{\varphi(m)} \sum_{p \mid m} \frac{\log p}{p} + \frac{1}{\varphi(m)} \sum_{\chi \neq \chi_0} |\sum_{p \leq x} \frac{\chi(p) \log p}{p}|.$$

(A): Vagyis elég volna belátni, hogy $\chi \neq \chi_0$ esetén $|\sum\limits_{p \leq x} \frac{\chi(p) \log p}{p}|$ egy x-től független korlát alatt marad.
A könnyebb kezelhetőség miatt vezessük be a $\Lambda : \mathbb{N}^+ \to \mathbb{R}$ függvényt, ami $\Lambda(n) = \log p$, ha $n = p^\alpha$, és 0 különben (vagyis ha $n = 1$ vagy $n = p_1^{\alpha_1} ... p_r^{\alpha_r};\ r \geq 2$).

(B): Így *(A)* helyett elég volna belátni, hogy $\chi \neq \chi_0$ esetén $|\sum\limits_{n \leq x} \frac{\chi(n)\Lambda(n)}{n}|$ egy x-től független korlát alatt marad.
A Λ definíciójából leolvasható, hogy $\sum\limits_{d \mid n} \Lambda(d) = \log n$, így $\Lambda(n) = \sum\limits_{d \mid n} \mu(d) \log(\frac{n}{d})$, így:

$$\sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{d \leq x} \frac{\chi(d)}{d} \mu(d) \sum_{n' \leq \frac{x}{d}} \frac{\chi(n') \log n'}{n'}.$$

A folytatáshoz *Shapiro* a következő nemnegatív értékű függvényt vizsgálta: $f : \mathbb{N}^+ \to \mathbb{R}$; $f(n+1) \leq f(n)$, ha $n \geq 3$, és $\lim_{n\to+\infty} f(n) = 0$. Belátható, hogy $\chi \neq \chi_0$ esetén $\sum_{n=1}^{\infty} \chi(n)f(n)$ konvergens (de nem abszolút konvergens), vagyis $L_f(\chi) = \lim_{K\to+\infty} \sum_{n=1}^{K} \chi(n)f(n)$ létezik és véges. Ekkor

$$|L_f(\chi) - \sum_{n=1}^{K} \chi(n)f(n)| \leq 2\varphi(m)f(K+1)$$

Ez $K \geq 2$ esetén mindig igaz, $K = 1$ esetén pedig akkor, ha $f(2) \geq f(3)$ (különben $2\varphi(m)(f(K+2) + f(K+1))$ biztosan jó korlát).
Az $f_0(n) = \frac{1}{n}$; $f_1(n) = \frac{\log n}{n}$; $f_2(n) = \frac{1}{\sqrt{n}}$ választásokkal a feltételek mind teljesülnek, s miután alkalmazzuk az előző felsőbecslést erre a három függvényre (és megkapjuk $L_0(\chi)$; $L_1(\chi)$; $L_2(\chi)$ komplex számokat, mint határértékeket), megmutatható, hogy *(B)* helyett elég volna belátni ezt:

(C): $\chi \neq \chi_0$ esetén $|\sum_{d\leq x} \frac{\chi(d)}{d}\mu(d)|$ egy x-től független korlát alatt marad.

Belátható, hogy ha $x \geq 1$, akkor $\sum_{d\leq x} \frac{\chi(d)\mu(d)}{d} \sum_{n\leq \frac{x}{d}} \frac{\chi(n)}{n} = 1$ (elindulásképpen $(\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2})(\sum_{k=1}^{\infty} \frac{1}{k^2}) = \sum_{d,k=1}^{\infty} \frac{\mu(d)}{(dk)^2} = \sum_{n=1}^{\infty} \frac{1}{n^2} \sum_{d|n} \mu(d) = 1$, illetve fontos megjegyezni, hogy a második szumma $n \leq \frac{x}{d}$-re vonatkozik, vagyis függ az első szummától), s ebből újabb becsléssel adódik, hogy

$$|L_0(\chi) \sum_{d\leq x} \frac{\chi(d)\mu(d)}{d} - 1| \leq 2\varphi(m),$$

ha $x \geq 1$. Ez átalakítható úgy, hogy

$$|\sum_{d\leq x} \frac{\chi(d)\mu(d)}{d} - \frac{1}{L_0(\chi)}| \leq \frac{2\varphi(m)}{|L_0(\chi)|},$$

így csak akkor kérdéses, ha $L_0(\chi) = 0$. Vagyis *(C)* helyett elég volna belátni, hogy:

(D): tetszőleges $\chi \neq \chi_0$ esetén $L_0(\chi) \neq 0$.
Annyi már az előző pontokból kijött, hogy van olyan pozitív c'_m korlát, mely $\chi \neq \chi_0$ esetén $\forall x \geq 2$-re

$$|\sum_{p\leq x} \frac{\chi(p)\log p}{p} - L_1(\chi) \sum_{d\leq x} \frac{\chi(d)}{d}\mu(d)| \leq c'_m.$$

Ha bevezetjük a $\delta(\chi) = 1$, ha $L_0(\chi) = 0$ (különben $\delta(\chi) = 0$) függvényt $\chi \neq \chi_0$ esetére és az előző egyenlőséget összevetjük azzal, hogy $L_0(\chi) = 0$, akkor megkapható egy újabb becslés, mely $\forall x \geq$ 2-re

$$|\sum_{p \leq x} \frac{\chi(p) \log p}{p} + \delta(\chi) \log x| \leq c''_m.$$

Ebből a bizonyítás elejét újragondolva egy újabb becslést kapunk, amiben már nincs feltételezés: $\exists c^*_m > 0$, hogy $\forall x \leq$ 2-re

$$|\sum_{\substack{p \leq x \\ p \equiv a(m)}} \frac{\log p}{p} - \frac{1}{\varphi(m)} \log x + \frac{1}{\varphi(m)} \sum_{\chi \neq \chi_0} \overline{\chi}(a)\delta(\chi) \log x| \leq {c^*}_m.$$

Ez $a = 1$ esetén okozza a legnagyobb problémát, mert ekkor $\overline{\chi}(a) = 1$, vagyis bejönnek a "rossz" χ-k, amikből $M = \sum_{\chi \neq \chi_0} \delta(\chi)$ van. Ekkor:

$$\sum_{\substack{p \leq x \\ p \equiv 1(m)}} \frac{\log p}{p} \leq \frac{1 - M}{\varphi(m)} \log x + c^*_m$$

A bal oldal nemnegatív (elvben üres összeg még lehetne), de $M \geq 2$ esetén a jobb oldal nem lehet mindig nemnegatív, ha $x \geq 2$. Így $M \leq 1$, vagyis ha van "rossz" χ, akkor szükségképpen valós minden $\chi(n)$ értéke (hiszen ha "rossz", akkor $\overline{\chi}$ is "rossz", vagyis volna két "rossz"). Így *(D)* helyett elég volna belátni, hogy

(E): tetszőleges valós értékkészletű $\chi \neq \chi_0$ esetén $L_0(\chi) \neq 0$.

Ez azért jó, mert egy valós értékkészletű karakter csak a $0, 1, -1$ értékeket veheti fel. Legyen $\chi \neq \chi_0$ valós értékkészletű karakter, és vezessük be a következő függvényt: $\xi : \mathbb{N}^+ \to \mathbb{R}$; $\xi(n) = \sum_{d|n} \chi(d)$. Ekkor $\xi(1) = \chi(1) = 1$, s mivel χ multiplikatív, ezért ξ is az, vagyis $n = p_1^{\alpha_1} ... p_r^{\alpha_r}$ esetén

$$\xi(n) = \prod_{j=1}^{r} \xi(p_j^{\alpha_j}) = \prod_{j=1}^{r} (1 + \chi(p_j) + \chi^2(p_j) + ... + \chi^{\alpha_j}(p_j)).$$

Itt a j-edik tényező értéke:

- 1, ha $\chi(p_j) = 0$;

- $1+\alpha_j$, ha $\chi(p_j)=1$;
- 1, ha $\chi(p_j)=-1$ és α_j páros;
- 0, ha $\chi(p_j)=-1$ és α_j páratlan.

Így $\forall n\in\mathbb{N}^+:\ \xi(n)\geq 0$, sőt, ha n négyzetszám, akkor minden tényező pozitív egész, így $\forall b\in\mathbb{N}^+$-ra $\xi(b^2)\geq 1$. Tekintsük a következő F függvényt!

$$F(x)=\sum_{n\leq x}\frac{\xi(n)}{\sqrt{n}}\geq\sum_{b\leq\sqrt{x}}\frac{\xi(b^2)}{b}\geq\sum_{b\leq\sqrt{x}}\frac{1}{b}$$

Ebből látszik, hogy $F(x)\to\infty$, ha $x\to\infty$. Viszont megmutatható, hogy

$$F(x)=\sum_{n\leq x}\frac{1}{\sqrt{n}}\sum_{d|n}\chi(d)=\sum_{d\leq x}\sum_{k\leq\frac{x}{d}}\frac{\chi(d)}{\sqrt{kd}}=\sum_{d\leq x}\frac{\chi(d)}{\sqrt{d}}\sum_{k\leq\frac{x}{d}}\frac{1}{\sqrt{k}}$$

kifejezés $L_0(\chi)=0$ esetén egy x-től független korlát alatt marad (ehhez $x\geq 1$ esetén elég pontosan kell becsülni $\sum\limits_{k\leq x}\frac{1}{\sqrt{k}}$ értéket ($\sum\limits_{k\leq x}\frac{1}{\sqrt{k}}=2\sqrt{x}+c_0+\Delta(x)$, ahol $|\Delta(x)|<\frac{4}{\sqrt{x}}$), de ez csak $d\leq\sqrt{x}$ esetén alkalmazható $F(x)$ becslésére, $\sqrt{x}<d\leq x$ között más, $L_2(\chi)$-vel kapcsolatos közelítést kell alkalmazni). Így azonban mivel $x\to\infty$ esetén $F(x)\to\infty$, ezért $L_0(\chi)\neq 0$ valós értékkészletű $\chi\neq\chi_0$-ra, így *(E)* értelmében a bizonyítás befejeződött.

12. Feladat: Bizonyítandó, hogy létezik végtelen sok prímszám, ami nem tagja ikerprím-párnak.
Megoldás: A Dirichlet-tétel alapján létezik végtelen sok $30k+7$ alakú prímszám, mert $(30,7)=1$. Az ilyen alakú prímek azonban sosem lehetnek ikerprím-párnak a tagjai, ugyanis a tőlük 2-vel nagyobb számok $30k+9$ alakúak, amik minden egész k esetén oszthatóak 3-mal ($k=0$-ra sem prím), illetve a tőlük 2-vel kisebb számok pedig $30k+5$ alakúak, amik minden egész k esetén oszthatóak 5-tel (és ugyan $k=0$-ra ez ikerprím-párt ad: {5,7}, viszont a többi végtelen sok k-ra nem lehet prím).

13. Feladat: Írjuk le a tizedesvessző után rendre a prímszámokat. Bizonyítsuk be, hogy az így keletkező $x=0,235711131719...$ szám irracionális.
Megoldás: Tegyük fel indirekt, hogy x szakaszos, k hosszúságú szakasszal. Azonban a Dirichlet-tétel miatt végtelen sok prím van, amelynek az utolsó $2k$ jegye 1-es, és olyan prím is végtelen sok van, amelynek az utolsó $2k$ jegye 3-as, ezért a szakasznak

egyrészt csupa 1-esből, másrészt csupa 3-asból kellene állnia, ami ellentmondásra vezet, vagyis x nem szakaszos.

14. Feladat: Mely a, b, c pozitív egészek esetén lesz végtelen sok prím az $a + bk + cn$ alakú számok között, ahol $k = 0, 1, 2, ...$, $n = 0, 1, 2, ...$?
Megoldás: A Dirichlet-tétel mintájára kikövetkeztethető a feltétel: $(a, b, c) = 1$. A szükségesség nyilvánvaló. Az elégségesség belátásához legyen $(a, b) = s$, ekkor $(s, c) = 1$. A Dirichlet-tétel alapján van olyan k , amelyre $a + bk = sp$, ahol p egy c-nél nagyobb prím. Ezután alkalmazzuk ismét a Dirichlet-tételt az $sp + cn$, $n = 0, 1, ...$ számtani sorozatra, s mivel $(s, c) = 1$ ezek között is végtelen sok prím lesz.

4. A Gauss-egészek

4.1. Alapfogalmak

Eddig szinte csak prímekkel kapcsolatos problémákat láttunk, és bár nagyon hasznos területet fednek le a számelméletben, bőven vannak még olyan egyszerűbb példák is, amiknek *látszólag* nincs köze a témakörhöz.

15. Feladat: Lássuk be, hogy egy szám akkor áll elő két négyzetszám különbségeként, ha 4-gyel osztva nem 2 maradékot ad.

Megoldás: Alakítsuk szorzattá! $n = x^2 - y^2 = (x-y)(x+y)$. Legyen $a = x-y, b = x+y$, ekkor a és b paritása ugyanaz, mert $b = a + 2y$, tehát n vagy páratlan, vagy 4-gyel osztható.
Fordítva: Nyilván $x = \frac{a+b}{2}$ és $y = \frac{b-a}{2}$. Ha n páratlan, akkor legyen $a = 1$ és $b = n$, ekkor x, y egész. Ha $4|n$, akkor legyen $a = 2$ és $b = \frac{n}{2}$.

16. Feladat: Egy szám mikor áll elő két négyzetszám összegeként, vagyis $n = x^2 + y^2$ milyen n-ekre igaz?

Ötlet: Tudjuk-e hasonlóan szorzattá alakítani, mint az előbb?

A valós számok körében ez nem alakítható szorzattá, de mivel már ismerjük a komplex számokat, ezért érdemes itt alkalmaznunk!
$n = x^2 + y^2 = (x - iy)(x + iy)$, ahol $i = \sqrt{-1}$ komplex szám a felső félsíkban, ahogy már korábban definiáltuk, és $x + iy$ ún. Gauss-egész.

26. Definíció: $\mathbb{G} := \{a + bi | a, b \in \mathbb{Z}\}$, $i = \sqrt{-1}$, $i \in \mathbb{C}$.

Megjegyzés: Felmerülhet a kérdés, hogy érdemes-e középiskolában a komplex számokról tanulni. Saját tapasztalatból mondhatom, hogy ez később matematikai pályán hasznos tud lenni (márpedig valószínűsíthető, hogy aki egy speciális matematika tagozat külön szakkörén vesz részt, az később is foglalkozni fog a témával). Esetemben nemcsak érdekességként tanultunk a komplex számokról, hanem a gimnázium második évében tananyagként kezeltük, hiszen az osztályom döntő többsége már ekkor értette, mi az, amikor egy művelet kivezet egy valós számkörből. Amikor a hatványozást kezdtük egyre általánosabban venni, mi magunk vetettük fel a negatív számoknál a törtkitevőt, s szerencsére az algebra tanárunk nem homályosan felvázolta a komplex számokat, hanem felépítette a számkört. Kis kitérőt téve a

tananyagban nemcsak érintőlegesen vettük a komplexeket: a bevezetés és az alapműveletek után a trigonometrikus alakkal a hatványozás, gyökvonás is világossá vált, illetve alkalmazásként beláttuk a harmad- és negyedfokú egyenlet megoldóképletét. Ez később, az egyetemi éveim során bizonyos előnyt jelentett, így azt gondolom, hogy ha a diákok érdeklődnek egy téma iránt, akkor szélesíteni kell a látókörüket, még ha hivatalosan nincs is a tanrendben - végül is, mire jó egy ilyen szakkör?

Visszatérve a Gauss-egészekhez: könnyen látható, hogy $\mathbb{G}$ zárt összeadásra, kivonásra (s az összeadás kommutatív), zárt szorzásra ($(a+bi)(c+di) = ac-bd+i(ad+bc) \in \mathbb{G}$), és ez kommutatív, asszociatív és disztributív az összeadásra nézve, vagyis $\mathbb{G}$ gyűrű, és nyilván $\mathbb{G} \subseteq \mathbb{C}$.

27. Definíció: Az $\alpha = a+bi$ Gauss-egész normája $N(\alpha) = \alpha\overline{\alpha} = a^2+b^2 = |\alpha|^2$.

28. Definíció: Adott $\alpha, \beta \in \mathbb{G}$, ekkor $\beta|\alpha \Leftrightarrow \exists\gamma \in \mathbb{G} : \beta\gamma = \alpha$.

29. Állítás: *Tulajdonságok α, β Gauss-egészekre*:

1. $N(\alpha)$ nemnegatív egész.
2. $N(\alpha) = 0 \Leftrightarrow \alpha = 0$.
3. $N(\alpha\beta) = N(\alpha)N(\beta)$.
4. $\alpha|\beta$ $\mathbb{G}$-ben $\Rightarrow N(\alpha)|N(\beta)$ $\mathbb{Z}$-ben.

17. Feladat: Lássuk be az előbb említett tulajdonságokat!

1-2) Mivel a valós számok körében a négyzetszámok nemnegatívak, vagyis $a^2 \geq 0$ és $a^2 = 0 \Leftrightarrow a = 0$, hasonlóan igaz b^2-re is, így $N(\alpha) = a^2+b^2 \geq 0$ és $a^2+b^2 = 0 \Leftrightarrow a = 0$ és $b = 0$, vagyis $\alpha = 0+0i = 0$.

3)$N(\alpha\beta) = |\alpha\beta|^2 = (|\alpha||\beta|)^2 = |\alpha|^2|\beta|^2 = N(\alpha)N(\beta)$.

4) $\beta = \alpha\gamma \Rightarrow N(\beta) = N(\alpha)N(\gamma)$.

30. Definíció: ε Gauss-egészet *egységnek* nevezünk $\mathbb{G}$-ben, ha $\varepsilon|\alpha$ $\forall\alpha \in \mathbb{G}$-re.

18. Feladat: Melyek az egységek $\mathbb{G}$-ben?
Megoldás: Ha $\varepsilon|1$, akkor $N(\varepsilon)|N(1) = 1$. Vagyis ha ε egység $\mathbb{G}$-ben, akkor normája 1 vagy -1. Legyen $\varepsilon = a + bi$, akkor $a^2 + b^2 = \pm 1$. Mivel a^2 és b^2 nemnegatív egészek, ezért az egyik 1, a másik 0. Ha $a^2 = 1$, akkor $\varepsilon = \pm 1$, ha $b^2 = 1$, akkor $\varepsilon = \pm i$.
Fordítva: ± 1 és $\pm i$ invertálhatók $\mathbb{G}$-ben, hiszen $1 = 1 \cdot 1 = (-1) \cdot (-1) = i \cdot (-i)$, ezért minden Gauss-egésznek osztói.

31. Tétel (Maradékos osztás Gauss-egészekre): Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez $\exists \gamma$ és ρ Gauss-egészek, hogy $\alpha = \beta\gamma + \rho$ és $N(\rho) < N(\beta)$.

Bizonyítás: Az egyenletet átalakítva $\frac{\alpha}{\beta} - \gamma = \frac{\rho}{\beta}$. Nyilván $N(\rho) < N(\beta) \Leftrightarrow |\rho|^2 < |\beta|^2 \Leftrightarrow |\frac{\rho}{\beta}|^2 < 1$, vagyis olyan γ kell, amire $|\frac{\alpha}{\beta} - \gamma|^2 < 1$. Az elég, ha ilyet találunk, mert akkor $\rho = \alpha - \beta\gamma$ jó lesz.
Legyen $\frac{\alpha}{\beta} = c + di$, c' a c-hez, d' a d-hez legközelebbi egész, ekkor $|c - c'| \leq \frac{1}{2}$ és $|d - d'| \leq \frac{1}{2}$. Tehát $\gamma = c' + d'i$ megfelelő Gauss-egész, mert $|\frac{\alpha}{\beta} - \gamma|^2 = (c - c')^2 + (d - d')^2 \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 < 1$.
Tehát $\mathbb{G}$ *euklideszi* gyűrű, vagyis érvényes benne az alaptétel, ami $\mathbb{Z}$-hez hasonlóan itt is belátható, azonban előtte definálnunk kell néhány alapfogalmat is.

32. Definíció: $\alpha, \beta \in \mathbb{G}$, nem mindkettő 0. Ekkor δ **a kitüntetett közös osztójuk**, ha $\delta|\alpha$ és $\delta|\beta$, és $\forall \omega$ Gauss-egészre ha $\omega|\alpha$ és $\omega|\beta$, akkor $\omega|\delta$ (mivel a komplex számokat nem lehet úgy rendezni, ahogy a valós számokat, ezért nem írhatunk olyat, hogy: $\omega < \delta$).

33. Definíció: Egy κ Gauss-egészet **felbonthatatlannak** nevezünk $\mathbb{G}$-ben, ha $\kappa \neq 0, \varepsilon$ és bármely $\kappa = \lambda\mu$ felbontás esetén λ vagy μ egység.

34. Definíció: Azt mondjuk, hogy a π Gauss-egész rendelkezik **prímtulajdonsággal** (röviden π prím), ha $\pi \neq 0, \varepsilon$, és minden olyan α és β Gauss-egészre, melyre $\pi|\alpha\beta$ teljesül, akkor $\pi|\alpha$ vagy $\pi|\beta$ közül legalább az egyik igaz.

35. Állítás: $\mathbb{G}$-ben α felbonthatatlan $\Leftrightarrow$ α prím.
Megjegyzés: A bizonyítás hasonlóan működik, mint $\mathbb{Z}$-nél, amit a **6. tétel** bizonyításánál olvashatunk.

36. Tétel (A számelmélet alaptétele $\mathbb{G}$-ben): Teszőleges $0, \varepsilon \neq \alpha \in \mathbb{G}$ szám lényegében egyértelműen felbontható $\mathbb{G}$-beli prímek szorzatára.
Megjegyzés: A bizonyítás úgy, mint $\mathbb{Z}$-ben, viszont $|\alpha|$ helyett $N(\alpha)$-t kell vizsgálni.

4.2. Prímek

Ez nagyon logikusan hangzik, amit az előbb leírtunk, viszont próbáljunk meg Gauss-prímeket sorolni! Nem is olyan könnyű! A következő tétel ebben segít:

37. Tétel: $\mathbb{G}$-ben csak az alább felsorolt számok és *egységszereseik* a prímek:

1. $1+i$,
2. Minden pozitív, $4k+3=p$ alakú egész prímszám,
3. Minden pozitív, $4k+1=p$ alakú egész prímszám esetén a $p=\pi_1\pi_2$ felbontásból kapott, p *normájú* π_1 és π_2 prímek $\mathbb{G}$-ben, és $\pi_1 \neq \pi_2\varepsilon$.

Példák:

- $2=(1+i)(1-i)=(-1-i)(i-1)=(-i)(1+i)^2$,
- $3,-7,11i,-19i$ mind prímek $\mathbb{G}$-ben,
- $5=(2+i)(2-i)=(1+2i)(1-2i)$,

A 37. Tétel bizonyításához szükségünk van néhány segédállításra, amit akár külön feladatokként is kezelhetünk!

19. Feladat: Adott $0,\varepsilon \neq \pi \in \mathbb{G}$. Ekkor pontosan egy $p \in \mathbb{Z}^+$ prím van, melyre $\pi|p$.
Bizonyítás: $\pi|N(\pi)=\pi\overline{\pi}$, így ha $N(\pi)=p_1p_2...p_r$, akkor $\pi|p_1p_2...p_r$, vagyis $\exists i$: $\pi|p_i(i=1,2,...,r)$. Mivel $(p_i,p_j)=1$, és ha $\pi|p_i$ és $\pi|p_j$ lenne, akkor $\pi|1$, ami nem lehet, vagyis p_i egyértelmű.

20. Feladat: Egy $p \in \mathbb{Z}$ prím vagy prím $\mathbb{G}$-ben, vagy két $\mathbb{G}$-beli prím szorzata: $p=\pi_1\pi_2$, és $N(\pi_1)=N(\pi_2)=p$, $\pi_1=\overline{\pi_2}$.
Bizonyítás: Legyen $p \in \mathbb{Z}$ prím, p nem prím $\mathbb{G}$-ben, vagyis $p=\pi_1\pi_2...\pi_s$ ($\pi_i \in \mathbb{G}$ prímek, $i=1,...,s$; $s \geq 2$.). Mindkét oldal normáját véve $N(p)=p^2=N(\pi_1)N(\pi_2)...N(\pi_s)$, ahol $N(\pi_i)>1$ egész, s ebből látszik, hogy $s=2$, $N(\pi_1)=N(\pi_2)=p$. Mivel $p=\pi_1\pi_2$ és $p=N(\pi_1)=\pi_1\overline{\pi_1} \Rightarrow \pi_2=\overline{\pi_1} \Rightarrow \pi_1=\overline{\pi_2}$.

21. Feladat: Lássuk be, hogy a 2 nem prím $\mathbb{G}$-ben!
Bizonyítás: Mivel $2|(1+i)(1-i)$, ezért ha a 2 prím lenne, akkor osztaná valamelyik

tényezőt, viszont $\frac{i+1}{2} \notin \mathbb{G}$ és $\frac{i-1}{2} \notin \mathbb{G}$. Vagyis a 2 két prím szorzata $\mathbb{G}$-ben, és mivel $2 = (-i-1)(i-1)$, ezért $1+i, 1-i, -i-1, i-1$ prímek $\mathbb{G}$-ben (és ugye ezek egymás egységszeresei). Ezzel beláttuk a **37. Tétel** első pontját.

37. Tétel bizonyítása:

1. Az $1+i$-hez és egységszereseihez tartozó $\mathbb{Z}$-beli prím a 2.

2. Ha volna valódi $\pi = a + bi$ prímosztója $\mathbb{G}$-ben, akkor $N(\pi) = p = a^2 + b^2$, viszont egy négyzetszám négyes maradéka csak $0, 1$ lehet, így két négyzetszám összegének a négyes maradéka csak $0, 1, 2$ lehet, ami ellentmond p feltételének.

3. Mivel van $d \in \mathbb{Z}$, melyre $d^2 \equiv -1 \bmod p \Rightarrow p | d^2+1 = (d+i)(d-i)$, de nyilván $p \nmid (d+i)$ és $p \nmid (d-i)$, mert $\frac{d+i}{p} \notin \mathbb{G}$ és $\frac{d-i}{p} \notin \mathbb{G} \Rightarrow p$ nem prím $\mathbb{G}$-ben $\Rightarrow$ $p = \pi_1\pi_2$; $N(\pi_1) = N(\pi_2)$.

   Miért nem lehetnek ezek egymás egységszeresei?
   Egyrészt már beláttuk, hogy $\pi_1 = \overline{\pi_2}$, másrészt nyilván ha $\pi_1 = a + bi$, akkor $|a| \neq |b|$, vagyis $a \neq \pm b$, máskülönben nem lenne prím (ha $|a| = |b|$, akkor π_1 csak akkor prím, ha $|a| = |b| = 1$, viszont ezt már az 1. pontban vizsgáltuk). Így $\pi_2 = a - bi$, és most nézzük meg a négy egységgel, mi lenne ha $\pi_1 = \varepsilon\overline{\pi_2}$.

   - $a+bi = 1(a-bi)$-ből $b = 0$ adódna, vagyis $p = a^2$ lenne, ami ellentmondás.
   - $a + bi = (-1)(a - bi)$-ből $a = 0$ adódna, vagyis $p = b^2$ lenne, ami ellentmondás.
   - $a + bi = i(a - bi)$-ből $a = b$ adódna, amit már kizártunk.
   - $a + bi = -i(a - bi)$-ből $a = -b$ adódna, amit már kizártunk.

Visszatérve az eredeti problémához: mik azok az egész számok, amik felírhatóak két négyzetszám összegeként?

38. Tétel: Egy 1-nél nagyobb egész szám akkor és csak akkor áll elő két négyzetszám összegeként, ha *minden* $4k+3$ *alakú prím páros kitevőn* szerepel benne.

Példák:

- A 15 a tétel szerint nem lehet jó, mert a 3 páratlan kitevőn szerepel. Valóban: $0^2 + 15 = 1^2 + 14 = 2^2 + 11 = 3^2 + 6$ felbontások közül egyik se jó.

- $90 = 2 \cdot 5 \cdot 3^2$ jó, mert a 3 páros kitevőn szerepel, pl. $90 = 3^2 + 9^2$.
- $4050 = 2 \cdot 3^4 \cdot 5^2$ jó, mert a 3 páros kitevőn szerepel: $4050 = (\pm 45)^2 + (\pm 45)^2 = (\pm 9)^2 + (\pm 63)^2 = (\pm 63)^2 + (\pm 9)^2$. (Összesen 12 darab, ha az előjelben eltérő megoldásokat is különbözőnek tekintjük.)

Bizonyítás: Legyen $n = 2^\alpha p_1^{\beta_1} ... p_m^{\beta_m} q_1^{\gamma_1} ... q_l^{\gamma_l}$, ahol $p_i \equiv 1 \bmod 4$ és $q_j \equiv 3 \bmod 4$. Ha $n = x^2 + y^2$, akkor írjuk fel $x + iy$-t Gauss-prímek szorzataként!

$$x + iy = \varepsilon (1+i)^\delta \pi_1^{\theta_1} ... \pi_u^{\theta_u} r_1^{\sigma_1} ... r_v^{\sigma_v}.$$

Ekkor ε egység, r_j egész, $4k+3$ alakú prím, $N(\pi_i)$ $4k+1$ alakú prím. Mindkét oldalt konjugálva:

$$x - iy = \overline{\varepsilon} (1-i)^\delta \overline{\pi_1}^{\sigma_1} ... \overline{\pi_u}^{\sigma_u} r_1^{\sigma_1} ... r_v^{\sigma_v}.$$

Ezeket összeszorozva $n = (x+iy)(x-iy)$ egyik felbontását kapjuk, a másikat $n = 2^\alpha p_1^{\beta_1} ... p_m^{\beta_m} q_1^{\gamma_1} ... q_l^{\gamma_l}$ alakból kaphatjuk, ha a 2-t és a p_i-ket Gauss-prímek szorzatára bontjuk. Az alaptétel egyértelműségi állítása miatt ez a két felbontás csak egységszeresben és sorrendben térhet el. A q_1 prím normája q_1^2, az $1+i, 1-i, \pi_i, \overline{\pi_i}$ normája azonban prím, így q_1 csakis valamelyik r_j egységszerese lehet. De r_j kitevője n-ben $2\sigma_j$, ami páros. Ezért q_1 kitevője $\gamma_1 = 2\sigma_j$ is páros. Hasonlóan belátható, hogy $q_2, ..., q_l$ kitevője is páros, vagyis a tétel egyik irányát beláttuk.
Másik irány: vegyünk egy $n = 2^\alpha p_1^{\beta_1} ... p_m^{\beta_m} q_1^{\gamma_1} ... q_l^{\gamma_l}$ alakú számot, ahol $p_i \equiv 1 \bmod 4$ és $q_j \equiv 3 \bmod 4$ és γ_j páros ($j = 1, 2, ..., l$, $i = 1, 2, ..., m$). Ekkor minden p_i felírható két Gauss-prím szorzataként, amik egymás konjugáltjai ($p_i = \pi_i \overline{\pi_i}$), vagyis n két szorzótényezőre bontható úgy, hogy egymás konjugáltjai:

$$n = [(1+i)^\alpha \pi_1^{\beta_1} ... \pi_m^{\beta_m} q_1^{\frac{\gamma_1}{2}} ... q_l^{\frac{\gamma_l}{2}}][(1-i)^\alpha \overline{\pi_1}^{\beta_1} ... \overline{\pi_m}^{\beta_m} q_1^{\frac{\gamma_1}{2}} ... q_l^{\frac{\gamma_l}{2}}]$$

Így ha $(1+i)^\alpha \pi_1^{\beta_1} ... \pi_m^{\beta_m} q_1^{\frac{\gamma_1}{2}} ... q_l^{\frac{\gamma_l}{2}}$ Gauss-egész egyszerűbb alakja $x+iy$, akkor a konjugáltja $(1-i)^\alpha \overline{\pi_1}^{\beta_1} ... \overline{\pi_m}^{\beta_m} q_1^{\frac{\gamma_1}{2}} ... q_l^{\frac{\gamma_l}{2}} = x - iy$, vagyis $n = (x+iy)(x-iy) = x^2 + y^2$.

Megjegyzés: Belátható, hogy a megoldások száma, vagyis azon (x, y) számpárok száma, melyekre $x^2 + y^2 = n$ pontosan $4(\beta_1 + 1)...(\beta_m + 1)$.

4.3. Alkalmazások

Most nézzünk néhány olyan feladatot, ami a **37. Tétel** *újabb bizonyításához vezet!* Ugyan nem minden pontját látjuk be, de a Gauss-prímek gyakorlására teljesen

megfelel. (A megoldások során próbáljunk új utakat keresni, minél kevesebbszer alkalmazva a már eddig belátott feladatokat!)

22. Feladat Ha $N(\alpha)$ prím $\mathbb{Z}$-ben, akkor α prím $\mathbb{G}$-ben.
Bizonyítás: $\alpha = \beta\gamma \Rightarrow N(\alpha) = N(\beta)N(\gamma) = p$. Így $N(\beta)$ vagy $N(\gamma)$ egyike 1, vagyis β vagy γ egyike egység.

23. Feladat: Ha $N(\alpha) = p^2$, ahol p egy $4k+3$ alakú prím $\mathbb{Z}$-ben, akkor α prím (felbonthatatlan) $\mathbb{G}$-ben.
Bizonyítás: $\alpha = \beta\gamma \Rightarrow N(\alpha) = N(\beta)N(\gamma) = p^2$. Ha $N(\beta)$ vagy $N(\gamma)$ egyike 1, akkor β vagy γ egyike egység. Ha nem, akkor $N(\beta) = N(\gamma) = p$. Legyen $\beta = u+vi$, akkor $u^2 + v^2 = p$. Négyzetszám 4-gyel osztva 0 vagy 1 maradékot ad, p pedig 3-at, ez ellentmondás, vagyis nem lehet olyan, hogy $N(\beta) = N(\gamma) = p$, így szükségképpen β vagy γ egyike egység.

Ez a két feladat igazolja, hogy a 29. Tételben szereplő számok Gauss-prímek, de az még hátra van, hogy csak ilyen alakúak lehetnek-e, azaz lefedik-e az összes Gauss-prímet. Ehhez segítségre hívjuk az alábbi állításokat.

39. Tétel (Wilson-tétel): Ha $p > 0$ prím $\mathbb{Z}$-ben, akkor $(p-1)! \equiv -1 \mod p$.
Bizonyítás: $p = 2, 3$ esetén nyilván igaz, így elég azt megmutatni, hogy ha $p \geq 5$, akkor a $2, 3, ..., p-2$ számok párba állíthatók úgy, hogy az egyes párokban az elemek szorzata 1-gyel legyen kongruens modulo p. Ebből a tétel már következik, hiszen ekkor $2 \cdot 3 \cdot ... \cdot (p-2) \equiv 1 \pmod{p}$, és így $(p-1)! \equiv 2 \cdot 3 \cdot ... \cdot (p-2) \cdot 1 \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}$. A párbaállítást illusztráljuk $p = 11$-re!
$10! = (2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8) \cdot 1 \cdot 10 \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot (-1) \equiv -1 \pmod{11}$
Általánosan a párba állításhoz a következőket kell igazolni:

1. Minden $2 \leq a \leq p-2$ egészhez pontosan egy olyan $b = g(a)$ létezik, amelyre $ab = 1 \pmod{p}$ és $2 \leq b \leq p-2$.
2. Ha $g(a) = b$, akkor $g(b) = a$, vagyis a és b valóban "egymás párjai".
3. $g(a) \neq a$, azaz egyik elem párja sem önmaga.

24. Feladat: Lássuk be a fenti 3 állítást! *Megoldás:*

1. Az $ax \equiv 1 \pmod{p}$ kongruencia $(a,p) \equiv 1$ miatt megoldható, és egyetlen b megoldása van a $0, 1, 2, ..., p-1$ teljes maradékrendszerben. Mivel $x = 0, 1, p-1$ esetén $ax \equiv 0, a, -a \pmod{p}$, így ezekre az x értékekre $ax \not\equiv 1 \pmod{p}$, tehát b valóban a megadott $2 \leq b \leq p-2$ intervallumba esik.

2. A $g(a) = b$ feltétel átírva: $ab \equiv 1 \pmod{p}$. Az $g(b)$ értéket a $by \equiv 1 \pmod{p}$ kongruenciából következik. Ezt a kongruenciát $y = a$ nyilván kielégíti, továbbá 1)-ből tudjuk, hogy ennek a kongruenciának pontosan egy megoldása van, ha $2 \leq y \leq p-2$, így valóban $g(b) = a$.

3. Ha $b = a$ igaz, akkor $a^2 \equiv 1 \pmod{p}$. Ezt oszthatóságként felírva: $p|(a-1)(a+1) \Rightarrow p|a-1$ vagy $p|a+1 \Rightarrow a \equiv \pm 1 \pmod{p}$ (mivel p prím). Viszont mivel $2 \leq a \leq p-2$, ezért ez ellenmondás.

25. Feladat: Ha p egy $4k+1$ alakú prím $\mathbb{Z}$-ben, akkor p nem prím $\mathbb{G}$-ben.
Bizonyítás: Párosítsuk j-t $p-j$-vel! Mivel $4|p-1$, ezért senki sem önmaga párja.

$$(p-1)! \equiv (\frac{p-1}{2})! \cdot (\frac{p-1}{2})! \cdot (-1)^{\frac{p-1}{2}} (p)$$

Legyen $x = (\frac{p-1}{2})!$, ekkor ugye $p|x^2+1 = (x+i)(x-i)$. Ha p Gauss-prím lenne, akkor $p|x+i$ vagy $p|x-i$ következne, de $p(a+bi) = x \pm i$-ből $pb = \pm 1$ következne, vagyis $p| \pm 1$, ami ellentmondás.

A szükségesség bizonyítása a Gauss-prímekhez.

Tegyük fel, hogy α Gauss-prím. Ekkor $\alpha|\alpha\overline{\alpha} = N(\alpha) \in \mathbb{Z}$. Bontsuk $N(\alpha)$-t $\mathbb{Z}$-ben prímek szorzatára! Mivel α Gauss-prím, valamelyik tényezőnek osztója lesz. Azaz $\alpha|p$ alkalmas $\mathbb{Z}$-beli pozitív p prímre.
Ha $p = 2 = (i+1)(1-i) = (-i)(1+i)^2$, akkor $\alpha|1+i$. Mivel $1+i$ Gauss-prím, ezért α az $1+i$ egységszerese.
Ha $p \equiv 3 \bmod 4$, akkor p prím $\mathbb{G}$-ben, és α a p egységszerese.
Ha $p \equiv 1 \bmod 4$, akkor p nem Gauss-prím. Mivel normája p^2, csak két Gauss-prím szorzatára bomolhat (ahogy a **19. Feladatban** beláttuk). Ekkor $\alpha|p = \pi_1\pi_2$ miatt $\alpha|\pi_1$ vagy $\alpha|\pi_2$. Így α a π_1 vagy a π_2 egységszerese.

Most, hogy végigjártuk, mely egész számok írhatóak fel két négyzetszám összegeként, folytathatnánk tovább a gondolatot: mely számok állnak elő $3, 4$ négyzetszám összegeként? Érintőlegesen ugyan, de erről is ejtsünk néhány szót!

40. Tétel (Három-négyzetszám-tétel): Egy n pozitív egész akkor és csak akkor **nem** áll elő három négyzetszám összegeként, ha $n = 4^k(8m + 7)$ alakú
Bizonyítás - részben: (Az $n = 4^k(8m+7)$ alakú számok nem állnak elő három négyzet összegeként.) A bizonyításhoz k-ra történő teljes indukciót használunk. $k = 0$ esetén azt állítjuk, hogy $8m+7$ alakú számok nem írhatóak fel három négyzet összegeként. Egy négyzetszám 8-as maradéka $0, 1, 4$ lehet, ezek közül akárhogy is választunk ki hármat, összegük nem lehet 7. Tegyük fel, hogy $(k-1)$-ig igaz az állítás. Indirekt módon feltesszük, hogy $\exists n$, mely előáll három négyzetszám összegeként, vagyis $n = 4^k(8m + 7) = x^2 + y^2 + z^2$. Mivel a bal oldal osztható 4-gyel, ezért a jobbnak is oszthatónak kell lennie, ami csak úgy lehet, ha x, y, z mindegyike páros. Ekkor az egyenlet mindkét oldalát 4-gyel osztva kapjuk, hogy $4^{k-1}(8m+7) = (\frac{x}{2})^2+(\frac{y}{2})^2+(\frac{z}{2})^2$, de ez ellentmond az indukciós feltételnek, mivel $\frac{x}{2}, \frac{y}{2}, \frac{z}{2}$ pozitív egészek.
A kölcsönösség másik iránya jóval nehezebb, ezért bizonyítás nélkül szerepeltetem.

26. Feladat: Lássuk be, hogy minden természetes szám előáll három $\frac{n(n+1)}{2}$ alakú, úgynevezett *háromszögszám* összegeként!
Bizonyítás: Nézzük az $n = \frac{a(a+1)}{2} + \frac{b(b+1)}{2} + \frac{c(c+1)}{2}$ egyenlőséget! Mindkét oldalt 8-cal felszorozva és hozzáadva 3-at: $8n + 3 = (2a + 1)^2 + (2b + 1)^2 + (2c + 1)^2$. A **31. Tételből** adódik, hogy egy $8n + 3$ alakú szám előáll három négyzetszám összegeként, már csak azt kell belátnunk, hogy ezek az összeadandók ekkor szükségképpen páratlanok. Mivel páros szám négyzete 8-cal osztva csak 0 vagy 4 maradékot adhat, páratlané pedig 1-et, ezért a 3-as maradékot csak úgy kaphatjuk meg, ha minden összeadandó páratlan.

41. Tétel (Négy-négyzetszám-tétel): Minden természetes szám előáll négy darab négyzetszám összegeként.
(*Megjegyzés:* Ha elfogadjuk a **Három-négyzetszám-tételt**, akkor már csak azt kell látnunk, hogy minden $n = 4^k(8m + 7)$ alakú szám előáll négy négyzetszám összegeként. Ekkor $n = (2^k)^2 + [4^k(8m + 6)]$, s a második összeadandó a 31. tétel alapján felírható három négyzetszám összegeként, ezért n négy négyzetszám összege.)
Bizonyítás: Nevezzük *szépnek* a négy négyzetszám összegeként felírható számokat! Most írjuk fel az **Euler-azonosságot**, vagyis két szép szám szorzata is szép!
$(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = (aw + bx + cy + dz)^2 + (ax - bw + cz - dy)^2+(ay-cw+dx-bz)^2+(az-dw+by-cx)^2$. (A szorzások elvégzéséből adódik.)

A bizonyításhoz szükséges kimondanunk a **Cauchy-Davenport lemmát**, s bár két részből áll, csak az egyik állítást bizonyítanám, amire később szükségem lesz.

42. Lemma (Cauchy-Davenport): *a)* Ha p prímszám és A, B a p szerinti maradékosztályok nemüres halmazai, és $|A|+|B| \leq p+1$, akkor $|A|+|B|-1 \leq |A \bigoplus B|$. *b)* Ha $|A|+|B| > p$, akkor $A \bigoplus B$ tartalmaz minden p szerinti maradékosztályt, ahol $A \bigoplus B = \{x+y | x \in A, y \in B\}$-t jelöli.
Bizonyítás b): Legyen c tetszőleges p szerinti maradékosztály és tekintsük a következő halmazt: $B' = \{c - x | x \in B\}$. Nyilván B és B' elemszáma ugyanannyi, így $|A| + |B'| > p$, vagyis A és B' halmazoknak van közös elemük, legyen ez y. Viszont ekkor $c \equiv y + (c - y) \bmod p$, azaz c kongruens egy A-beli és B-beli elem összegével.

41. Tétel bizonyítása: Az **Euler-azonosságot** indukcióval nemcsak kettő, hanem akárhány szám szorzatára igazolhatjuk, vagyis elég csak a prímekre bizonyítani a tételt, mert minden szám prímek szorzatára bontható, így ezzel készen lennénk.
Minden prímnek van szép többszöröse: Vegyünk egy $p > 3$ prímet ($2 = 1+1+0+0$). Olyan többszöröst keresünk, amiben a négyzetszámok nem mind oszthatóak p-vel; ennél erőssebb az az állítás, hogy p-nek van x^2+y^2+1 alakú többszöröse. Ha vesszük a négyzetszámok p-vel osztva vett maradékait, azaz a *mod p kvadratikus maradékokat* (beleértve a 0-t is), akkor a maradékosztályoknak egy $\frac{p+1}{2}$ elemű A halmazát kapjuk. A *Cauchy-Davenport lemma* szerint $A \bigoplus A$ tartalmaz minden mod p vett maradékosztályt, így a (-1)-et is, ami pontosan a bizonyítandó állítás.
Most azt szeretném bizonyítani a végtelen leszállás módszerével, hogy ha $n > 1$ olyan pozitív egész, amire np szép, akkor $\exists 1 \leq m < n$, amire mp szintén szép.
Tegyük fel először, hogy n páros. Ekkor az $np = x^2 + y^2 + z^2 + u^2$ egyenlőségből x, y, z, u közül $0, 2$ vagy 4 darab páros szám van. Permutálva őket feltehetjük, hogy x, y és z, u azonos paritású. Ekkor viszont a négy négyzetszám összegeként írható $(\frac{x+y}{2})^2 + (\frac{x-y}{2})^2 + (\frac{z+u}{2})^2 + (\frac{z-u}{2})^2$ kiszorozva $\frac{x^2+y^2+z^2+u^2}{2}$, azaz ez p-nek egy kisebb többszöröse ($\frac{n}{2}$-szerese).
Tegyük fel végül, hogy $n > 1$ páratlan, és $np = x^2 + y^2 + z^2 + u^2$. Legyen az x, y, z, u számoknak n-nel vett legkisebb abszolútértékű maradéka rendre $\alpha, \beta, \gamma, \delta$. Mivel n páratlan, ezért $\alpha, \beta, \gamma, \delta$ midegyikének abszolútértéke kisebb $\frac{n}{2}$-nél. Így $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 < (\frac{n}{2})^2 + (\frac{n}{2})^2 + (\frac{n}{2})^2 + (\frac{n}{2})^2 = n^2$. Továbbá $(\alpha^2 + \beta^2 + \gamma^2 + \delta^2)$-nek ugyanannyi az n-es maradéka, mint $x^2 + y^2 + z^2 + u^2$-nek, vagyis 0. Tehát $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = kn$ valamilyen $k < n$ egész számra. Az Euler-azonosság szerint $(x^2+y^2+z^2+u^2)(\alpha^2+\beta^2+\gamma^2+\delta^2) = a^2+b^2+c^2+d^2$, ahol a, b, c, d az azonosság jobb oldalából következő kifejezések. A fentiek szerint $(x^2+y^2+z^2+u^2)(\alpha^2+\beta^2+\gamma^2+\delta^2) = kn^2p$, viszont: $a \equiv x^2+y^2+z^2+u^2 \equiv 0 \bmod n$ és $b \equiv xy-yx+zu-uz \equiv 0 \bmod n$, és hasonlóan $c \equiv 0 \bmod n$, $d \equiv 0 \bmod n$. Ezért a, b, c, d mindegyikét leoszhatjuk n-nel, amiből az adódik, hogy kp négy négyzetszám összege, vagyis szép.

5. Irodalomjegyzék

[1] Szalay Mihály: Számelmélet, Tankönyvkiadó, 1991; TYPOTEX-Nemzeti Tankönyvkiadó, 1998.

[2] Freud Róbert; Gyarmati Edit: Számelmélet, Nemzeti Tankönyvkiadó, 2000.

[3] Sárközy András; Surányi János: Számelmélet feladatgyűjtemény. ELTE egyetemi jegyzet.

[4] http://hu.wikipedia.org/wiki/Háromnégyzetszám-tétel

[5] http://hu.wikipedia.org/wiki/Cauchy-Davenport-lemma

[6] http://hu.wikipedia.org/wiki/Négynégyzetszám-tétel