ZÉRUSOSZTÓK TANULMÁNYOZÁSA A MARADÉKOSZTÁLYOK GYŰRŰJÉBEN

Horobeţ Emil,
Babeş Bolyai Tudományegyetem, Matematika-Informatika szak, I év
Témavezető: prof.dr.Mărcuş Andrei, Babeş Bolyai Tudományegyetem,
Algebra tanszék

Készült a XI. Erdélyi Tudományos Dikákköri Konferencia alkalmából
Kolozsvár 2008 május 23-24

1. Bevezetés

Ennek a dolgozatnak a célja a zérusosztók tanulmányozása a $(\mathbb{Z}_n, +, \cdot)$ gyűrűben és segítségükkel a tökéletes számok vizsgálata. Legelőször általános megfigyelések, mint például a zérusosztók részgyűrűje, a zérusosztók, nilpotens és potens elemek közötti összefüggések és polinomok vizsgálata a $(\mathbb{Z}_n, +, \cdot)$-ban. A zérusosztók összegére vonakozó eredmények, a valódi osztók kiválogatása a z.o-k(zérusosztók) közül. Befejezésként pedig egy módszer, ahogyan megpróbáltam megközelíteni a tökéletes számok problémáját a z.o-k segítségével, vagyis a $Z_d = \{x|(\exists)y \in \mathbb{Z}_d, \widehat{xy} = \widehat{0}\}$ halmazok vizsgálata és a $(U_n = \{Z_d|d \in Z_n\}, \bigcap, \bigcup)$ tanulmányozása.
A tökéletes számok problémáját legelőször Euklidész fogalmazta meg, az Elemek című munkájában i.e.300-ban. Ugyanitt részleges választ adott a páros tökéletes számok problémájára. Ezt követően megjelenik a probléma i.sz.100-ban Nichomacusnál is. Elődei munkáját folytatta Thaib ibn Qurra, aki bevezette a Mersenne típusú prímek fogalmát.
Azóta gazdagodott a matematika története, de a tökéletes számok problémája még mindig nincs megoldva teljesen. 1500-tól napjainkig rengeteg neves matematikus foglalkozott már ezzel a témával, mint például Cataldi, Descartes, Fermat, Mersenne, Frenicle, Leibnitz, Euler, Lucas, Catalan, Sylvester, Cunningham, Pepin, Putnam, Lehmer, stb. Még napjainkban is sokan foglalkoznak a témával, hisz nagy jelentőséggel bír a tradíciója és fontos szerepe van a prímkutatásban, illetve a modern kódolási technikák továbbfejlesztésében is.
Ebben a dolgozatban felsorolnék néhány eddigi fontos eredményt a témában, illetve egyéni megközelítési módokat és egyéni erdményeket mutatnék be. Első sorban a zérusosztók vizsgálatára alapoztam a munkámat.

2. Eddigi eredmények

Definíció 2.1. Tökéletes számnak nevezzük azt az $n \in \mathbb{N}$ számot, amely egyenlő az osztóinak az összegével, ahol az 1-es osztónak számít és a szám maga nem.
Pld. $6 = 1 + 2 + 3$

Definíció 2.2. A $Z_n = \{x|(\exists)y \in \mathbb{Z}_n, \widehat{x}\widehat{y} = \widehat{0}\}$ halmazt a $\mathbb{Z}_n$ zérusosztói halmazának nevezzük.

Definíció 2.3. A $D_n = \{d \leq n|\ d|n\}$ az osztók halmaza.

Definíció 2.4. Legyen $s(n) = \sum_{d|n} d$ az osztó függvény.

Definíció 2.5. Legyen

$$\sigma(n) = \sum_{d|n, d<n} d$$

az osztó összeg, vagy megszorított osztó függvény.

Megjegyzés 2.6. A közhasználatú jelölésben ez a két függvény felcserélve használatos.

Következmény 2.7. *Az $n \in \mathbb{N}$ akkor és csakis akkor tökéletes, ha $\sigma(n) = n$ vagy $s(n) = 2n$.*

Definíció 2.8. Egy $p \in \mathbb{N}$ számot Mersenne prímnek nevezünk, ha p prím és $\exists k \in \mathbb{N} : p = 2^k - 1$.

Definíció 2.9. Egy $n \in \mathbb{N}$ számot háromszög számnak nevezünk, ha $\exists k \in \mathbb{N} : n = \frac{k(k+1)}{2}$.

Tétel 2.10. *Ha p prím, akkor $s(n) = p + 1$, $s(p^k) = p^{k+1} - 1$.*
Ugyanakkor, ha $n = \prod_{i \leq k} p_i^{q_i}$, akkor $s(n) = \prod_{i \leq k} s(p_i^{q_i})$.

Tétel 2.11. *(Euler) $n \in \mathbb{N}$ páros tökéletes szám $\Leftrightarrow n = 2^{p-1}(2^p - 1)$ alakú, ahol $2^p - 1$ Mersenne prím.*

Tétel 2.12. *$2^p - 1$ prím, akkor p is prím.*

Tétel 2.13. *(Lucas-Lehmer) Adott az $(u_n)_{n \geq 1}$,$u_0 = 4$, $u_{k+1} = (u_k^2 - 2) mod\ n$ sorozat. Az $n = 2^p - 1$, (p prím), szám, akkor és csakis akkor prím, ha $u_{p-2} = 0$.*

Tétel 2.14. *(Eaton 1995) n akkor és csakis akkor tökéletes, ha $n = 1 + 9T_p$, alakú, ahol $T_p = \frac{p(p+1)}{2}$ és $p = 8j + 2$ alakú.*

Tétel 2.15. *Ha n tökéletes szám, akkor*

$$\sum_{d \in D_n} \frac{1}{d} = 2$$

.

Tétel 2.16. *(Makowski 1962) Az egyetlen $x^3 + 1$ alakú páros tökéletes szám a 28.*

Tétel 2.17. *(Euler) Ha létezik páratlan tökéletes szám, akkor az $p^{4r+1}q^2$, alakú, ahol $p = 4t + 1$ alakú.*

Tétel 2.18. *Ha létezik páratlan tökélet szám, akkor az $12k + 1$ vagy $36k + 9$ alakú.*

Tétel 2.19. *(Stuyvaert 1896) Ha létezik páratlan tökéletes szám, akkor az két négyzet összege.*

Definíció 2.20. Bővelkedő számnak nevezzük azt a számot amelyre $\sigma(n) > n$, hiányosnak nevezzük ha $\sigma(n) < n$.
Féltökéletes számnak nevezzük azokat a számokat melykre $\exists d_1, \ldots, d_k \in D_n$: $\sum_{i=1}^{k} d_i = n$.

Megjegyzés 2.21. Minden féltökéletes szám egyben bővelkedő szám is.

Tétel 2.22. *Bármely tökéletes és bármely bővelekdő számnak a többszörösei bővelkedő számok.*
Minden prím, prímhatvány, tökéletes, illetve hiányos szám osztói mind hiányosak.

Definíció 2.23. Barátságosnak nevezünk egy (p, k) számpárt, ha $\sigma(p) = k, \sigma(k) = p$.
$(k_1, \ldots, k_t)$ szociális számok, ha $\sigma(k_1) = k_2, \sigma(k_2) = k_3, \ldots, \sigma(k_t) = k_1$.

Tétel 2.24. *Adott a $(V_n^a)_{n\geq 1}$, $V_1^a = a \in \mathbb{N}, V_1^a = \sigma(V_k^a)$ sorozat.Ekkor*
a.) Ha a $(V_n^a)_{n\geq 1}$ elér egy konstanst, akkor ez egy tökéletes szám.
b.) Ha a $(V_n^a)_{n\geq 1}$ elér egy váltakozó számpárig, akkor ezek barátságosak.
c.) Ha a $(V_n^a)_{n\geq 1}$ elér egy váltakozó szám n-esig, akkor ezek szociális számok.

Megjegyzés 2.25. Az $a = 276$ a legelső olyan szám amelyre a fenti tétel egyetlen alpontja sem teljesül. Öt darab 1000-nél kisebb ilyen szám van:$276, 552, 564, 660, 960$(Lehner-ötösnek nevezik)

Tétel 2.26. *Ha $p, q \in \mathbb{N}$ prímek és $q|M_p = 2^p - 1$, akkor $q = \pm 1(mod\ 8)$ és $q = 2kp + 1, k \in \mathbb{N}$.*

Tétel 2.27. *Legyen $p = 3(mod\ 4)$. $2p + 1$ prím, akkor és csakis akkor, ha $2p + 1|M_p = 2^p - 1$.*

Tétel 2.28. *Ha összeadjuk egy páros tökéletes szám(kivétel a 6) számjegyeit, az így kapott számra megint elvégezzük ezt és így tovább, akkor végeredményben mindig 1-et kapunk.*

Lemma 2.29. *Az $s^2 = -1(mod\ p)$, $s \in \{1, 2, \ldots, p-1\}$, p prím egyenletnek*
a.) két különböző megoldása van, ha $p = 4k + 1$ alakú
b.) nincs megoldása, ha $p = 4k + 3$ alakú
c.) $s = 1$ megoldása, ha $p = 2$.
Bizonyítás: Megszerkesztjük az $\{x, -x, x^{-1}, -x^{-1}\}$ ekvivalencia osztályokat a $\mathbb{Z}_p$-ben. Feltevődik a kérdés, hogy ezek az osztályok mindig négy különböző elemet tartalmaznak-e?
Az $x = -x$-nek nincs megoldása, mivel p páratlan prím. Tehát az x és $-x$ mindig különböző elemek. Az $x = x^{-1} \Leftrightarrow x^2 = 1 \Leftrightarrow (x-1)(x+1) = 0 \Leftrightarrow x = 1 vagy x = p - 1$, hisz p prímszám. Tehát az $< 1 >$ osztály mindig a { 1,p-1}-ből áll.
Ugyanakkor az $x = -x^{-1} \Leftrightarrow x^2 = -1$ megoldhatóságáról nem tudunk semmit. A $\mathbb{Z}_p$-nek $p - 1$ eleme van amelyeket 4,2, illetve 1 hosszúságú partíciókra osztottuk. Ha $p - 1 = 4k + 2$ alakú, akkor egy db. 2-hosszúságú partíció van és ez kötelezően az $< 1 >$ osztály. $\Rightarrow x^2 = -1$-nek nincs megoldása. Ha $p - 1 = 4k$ alakú, akkor pontosan kétdarab 2-hosszúságú partíció van $x^2 = -1$nek van megoldása és két különböző megoldása van, hisz ha x_0 megoldás, akkor $p - x_0$ is megoldás.

Lemma 2.30. *Ha $n \in \mathbb{N}$ és $n = 4k + 3$ alakú, akkor nem írható fel két négyzet összegeként.*
Bizonyítás: Feltételezzük, hogy $\exists x, y \in \mathbb{N} : n = x^2 + y^2$.

$x = 2k, y = 2p \Rightarrow x^2 + y^2 = 0 \neq n(mod4)$
$x = 2k, y = 2p + 1 \Rightarrow x^2 + y^2 = 1 \neq n(mod4)$
$x = 2k + 1, y = 2p \Rightarrow x^2 + y^2 = 1 \neq n(mod4)$
$x = 2k + 1, y = 2p + 1 \Rightarrow x^2 + y^2 = 2 \neq n(mod4)$.

Tétel 2.31. *Minden $4k + 1$ alkú prím felírható két négyzet összegeként.*
Bizonyítás: Legyen $M = \{(x^{'}, y^{'}) \in \mathbb{N}^2 | 0 \leq x^{'}, y^{'} \leq \sqrt{p}\}$. Mivel $|\{0, 1, \ldots, [\sqrt{p}]\}| = 1 + [\sqrt{p}]$ ezért az alkotható párok száma $(1 + [\sqrt{p}])^2$. Ugyanakkor ismeretes, hogy $[x] + 1 > x \Rightarrow 1 + [\sqrt{p}] > \sqrt{p} \Rightarrow (1 + [\sqrt{p}])^2 > p$. Tehát az M-ben több mint p darab elem van. Jelöljük sM-el a kövelkező halmazt $\{x - sy | (x, y) \in M\}, \forall s \in \mathbb{R}$. Mivel az M-ben több mint p elem van ezért az sM-ben biztosan lesz két elem amelyek kongruensek mod p, különböző (x, y) párok esetén. Tehát $\exists (x^{'}, y^{'}) \neq (x^{"}, y^{"}) \in M : x^{'} - sy^{'} = x^{"} - sy^{"} (mod\ p)$. Átcsoportosítva és jelölve $x^{'} - x^{"} = x, y^{'} - y^{"} = y, x, y \in \{0, 1, \ldots, [\sqrt{p}]\}$, ekkor kapjuk, hogy $\forall s \in \mathbb{R} \exists x, y \in \{0, 1, \ldots, [\sqrt{p}]\} : x = sy$. Majd válasszuk s-nek az előző lemmában szereplő értéket. Ekkor $x = sy \Rightarrow x^2 = s^2 y^2 \Rightarrow x^2 = -y^2 \Rightarrow x^2 + y^2 = 0(modp) \Rightarrow x^2 + y^2 = kp$, de $x, y \in \{0, 1, \ldots, [\sqrt{p}]\} \Rightarrow k = 1 \Rightarrow x^2 + y^2 = p$.

Lemma 2.32. *Ha $n, m \in \mathbb{N}$ felírható két négyzet összegeként, akkor nm is felírható két négyzet összegeként.*

Lemma 2.33. *Ha $n = x^2 + y^2$, akkor $nz^2 = (xz)^2 + (yz)^2$.*
Ha $p = 4k + 3$ prím és osztja $n = x^2 + y^2 - et$, akkor $p^2 | n$..
Bizonyítás: Igazolni kell, hogy $p|x$ és $p|y$. Feltételezzük, hogy x nem osztható p-vel $\Rightarrow (p, x) = 1 \Rightarrow \exists x^{-1} \in \mathbb{Z}_p . x^2 + y^2 = o(modp) | (x^{-2}) \Rightarrow (xx^{-1})^2 + (yx^{-1})^2 = 0$ ami viszont ellentmond a 2.30.Lemmának.

Tétel 2.34. *Az $n \in \mathbb{N}$ szám akkor és csakis akkor írjató fel két négyzet összegeként, ha a prímtényezös felbontásában $4k+3$ alakú prímek páros hatványon szerepelnek.*
Bizonyítás: lásd 2.31. tétel, 2.32,2.33,2.34 Lemmák.

Következmény 2.35. *Ha van páratlan tökéletes szám, akkor a prímtényezös felbontásában $4k+3$ alakú prímek páros hatványon szerepelnek.*

Definíció 2.36. Legyen $\varphi(n)$ az n-nél kissebb, n-el relatív prímek száma. Ismeretes, hogy ha $n = \prod_{i=1}^{k} p_i^{q_i}$, akkor $\varphi(n) = n \prod_{i=1}^{k} (1 + \frac{1}{p_i})$.

Tétel 2.37. *A $\mathbb{Z}_n$-ben a zérusosztók száma $n - \varphi(n)$. Az $n = p_1^{q_1} p_2^{q_2} \ldots p_k^{q_k}$ osztóinak a száma $\prod_{i=1}^{k} (q_i + 1)$.*
Bizonyítás: Mivel $\varphi(n)$ az n-el relatív prímek száma $\Rightarrow n - \varphi(n)$ darab szám nem relatív prím az n-el. Ha egy n-nél kissebb szám nem relatív prím az n-el, akkor ő zérusosztó. Tehát a zérusosztók darabszáma $n - \varphi(n)$. A másadik eredmény pedig egy ismert eredmény.

Definíció 2.38. Egy gyűrűt akkor nevezünk D^* gyűrűnek ha minden elem felírható egy nilpotens és egy potens elem összegeként.

Tétel 2.39. *Ha R egy periódikus gyűrű, akkor $\forall x \in R$ esetén*
a.) x valamely hatványa idempotens
b.) $\exists k > 1 : x - x^k$ nilpotens.

Tétel 2.40. *Egy R gyűrű, akkor és csakis akkor D^* gyűrű, ha mindenik zérusosztója periódikus.*

Tétel 2.41. *Legyen R egy gyűrű, amelyben mindenik zérusosztó potens, akkor nem létezik nilpotens elem és ha R nem test, akkor $J = \{0\}$, ahol J a Jacobson gyöke a gyűrűnek.*

3. Saját eredmények

Lemma 3.1. *Ha $d \in Z_n$, akkor $-d = n - d \in Z_n$.*
Bizonyítás: $d \in Z_n \Rightarrow \exists k \in Z_n : dk = 0 \Rightarrow (-d)k = 0 \Rightarrow -d \in Z_d$.

Tétel 3.2. *A $\mathbb{Z}_n$-ben*

$$\sum_{d \in Z_n} d = \sum_{n^2=0} n + \sum_{2p=0} p$$

Bizonyítás: 3.1 Lemma $\Rightarrow$ ha $d \in Z_n$, akkor $-d \in Z_n$, tehát összegük nullát ad ki. Akkor van kivétel, ha $x = -x \Leftrightarrow x = 2x$, vagy ha $xx = 0 \Leftrightarrow x^2 = 0 \Rightarrow$ a tétel állítása.

Tétel 3.3. *Páratlan tökéletes szám nem lehet négyzetszám.*
Bizonyítás: n páratlan$\Rightarrow \forall d \in D_n$ esetén d páratlan, de $\sigma(n)-1$ páros $\Rightarrow \prod_{i=1}^{k}(q_i+1)$ páros $\Rightarrow \exists j \in \mathbb{N} : q_j$ páratlan $\Rightarrow n$ nem négyzetszám.

Lemma 3.4. *Ha n páratlan és tökéletes, akkor nem létezik nilpotens elem a $(\mathbb{Z}_n, +, \cdot)-$ban.*
Bizonyítás: Feltételezzük, hogy $x \in \mathbb{Z}_n$ nilpotens elem $\Rightarrow x^2 = 0 \Rightarrow \exists k \in \mathbb{N} : x^2 = nk$, de $x < n \Rightarrow n$ négyzetszám(mert x-nek kell tartalmaznia n-nek minden prímtényezőjét egy kissebb hatványon, melyet négyzetre emelve visszakapjuk az n-et), ami ellentmondás a 3.3 tétel alapján.
A tťel kijelentése hasonló a 2.41 tťeléhez.

Lemma 3.5. *Ha n páratlan szám, akkor nem fordulhat elő a $\mathbb{Z}_n$-ben, hogy $x = -x$.*
Bizonyítás: Feltételezzük, hogy $x = -x \Rightarrow 2x = 0 \Rightarrow \exists k \in \mathbb{N} : 2x = kn$, de $x < n \Rightarrow n$ páros, ami ellentmond a kezdeti feltételeknek.

Tétel 3.6. *Ha n páratlan tökéletes szám, akkor a $\mathbb{Z}_n$-ben a zérusosztók összege nulla.*
Bizonyítás: Lemma 3.4 $\Rightarrow \sum_{n^2=0} n = 0$, Lemma 3.5 $\Rightarrow \sum_{2p=0} p = 0$, tehát $\sum_{d \in Z_n} d = 0 + 0 = 0$.

Megjegyzés 3.7. A fenti kijelentés igaz, ha n egy páratlan és négyzetmentes természetes szám.

Tétel 3.8. *Ha n páros tökéletes szám, akkor $\sum_{d \in Z_n} = \frac{n}{2}$.*
Bizonyítás: mivel n tökéletes szám $\Rightarrow n = 2^{p-1}(2^p - 1) \Rightarrow n$ nem négyzetszám $\Rightarrow$ nincsenek nilpotens elemek $\Rightarrow$ a tétel kijelentése.

Tétel 3.9. *Ha van idempotens elem, akkor ő egyben zérusosztó is.*
Bizonyítás: $x^2 = x \Rightarrow x^2 - x = 0 \Rightarrow x(x-1) = 0 \Rightarrow x$ *zérusosztó.*

Tétel 3.10. *A $\mathbb{Z}_n$-ben minden elem periódikus, vagyis $\exists m \neq n : x^n = x^m, \forall x \in \mathbb{Z}_n$.*
Bizonyítaás: $\forall n \in \mathbb{N}$ esetén az n-el vett osztási maradékok végesek és egy idö után ismétlödnek $\Rightarrow \forall x \in \mathbb{Z}_n \exists k \in \mathbb{N} : x^k = x$, vagyis minden elem potens.

Következmény 3.11. *Ha x zérusosztó, akkor a fenti $k \neq n$, ha pedig nem akkor $k = n$.*

Tétel 3.12. *A $\mathbb{Z}_n$ egy periódikus és D^* gyűrű.*
Bizonyítás:Mivel minden elem potens $\Rightarrow$ a tétel állítása.

Tétel 3.13. *$\forall x \in \mathbb{Z}_n$ segítségével generálható egy zérusosztó vagy a 0, de nem bíztos, hogy különböző értékeket kapunk.*
Bizonyítás: Mivel $\mathbb{Z}_n$ egy periódikus gyűrű $\Rightarrow \forall x \in \mathbb{Z}_n$ x valamelyik hatványa idempotens. Legyen $(x^a)^2 = x^a \Rightarrow x^a$ és $x^a - 1$ zérusosztók.

Tétel 3.14. *Tekintsük a $P(X) = (x - d_1)(x - d_2)\dots(x - d_{2k}) \in \mathbb{Z}_n[X]$ polinomot, ahol d_i zérusosztó a $\mathbb{Z}_n$-ben és n páratlan. Ekkor igaz, hogy*
a.)$P(X) = \sum_{i=1}^{k}(x^2 - d_i^2)$
b.)gyökei az $x^2 = d_i^2$ megoldásai
c.)$P(0) = 0, P(1) = 0$
d.)ha $P(X) = a_{2k}x^{2k} + a_{2k-1}x^{2k-1} + \dots + a_1x + a_0$, akkor $a_{2k-1} + \dots + a_k = -1$
e.)$P(X) = x^kQ(x)$, ahol $Q(X) = x^k + a_{2k-1}x^{k-1} + \dots + a_k$
Bizonyítás: Az a.),b.) és c.) pontok könnyen beláthatóak. Ha $d \in \mathbb{Z}_n$ zérusosztó, akkor -d is zérusosztó.A Viete képleteket alkalmazva igazolható, hogy $a_{k-1} = \dots = a_0 = 0 \Rightarrow$ d.) és e.)

Tétel 3.15. *A $(Z_n \bigcup \{0\}, \cdot)$ kommutatív grupoid.*
Bizonyítás: a.) $\forall a, b \in Z_n$ esetén $\exists x \in Z_n : ax = 0 \Rightarrow x(ab) = (xa)b = 0b = 0 \Rightarrow ab \in Z_n$.
b.)Az asszociativitást és a kommutativitást örokli a $(\mathbb{Z}_n, +, \cdot)$-tól.

Definíció 3.16. $(U_n = \{Z_d | d \in Z_n\}, \bigcap, \bigcup)$ struktúrát nevezzük univerzális struktúrának.

Tétel 3.17. *Legyen $Z_a, Z_b \in U_n$, ekkor a $Z_a \bigcup Z_b$ olyan elemeket tartalmaz, amelyek tartalmaznak legalább egy prímtényezőt vagy az a vagy a b felbontásából és kissebbek mint $max(a, b)$. A $Z_a \bigcap Z_b$ olyan elemeket taratalmaz amelyek tartalmaznak legalább egy-egy prímtényezőt az a és a b felbontásából is. A $Z_a \backslash Z_b$ olyan a-nál kissebb x elemeket taratlmaz amelyekre $(x, b) = 1$, vagyis $Z_a \backslash Z_b = \{x \in Z_a | (x, b) = 1\}$.*

Megjegyzés 3.18. *$\forall a, b \in Z_n$* estén *$lnko(a, b) \in Z_a \bigcap Z_b$.*
Bizonyítás: Legyen $d = lnko(a, b) \Rightarrow d|a, d|b \Rightarrow d \in Z_a, d \in Z_b \Rightarrow d \in Z_a \bigcap Z_b$.

Tétel 3.19. *Ha $d \in D_n \Rightarrow n - d \notin D_n$.(n páratlan)*
Bizonyítás:$d \in D_n \Rightarrow d < \frac{n}{2} \Rightarrow \frac{n}{2} < n - \frac{n}{2} < n - d \Rightarrow n - d \notin D_n$.

Tétel 3.20. *Nem létezik olyan $a \in \mathbb{N} : Z_a$ csak az n osztóit tartalmazza.*
Bizonyítás: Ha $d \in Z_a \Rightarrow -d \in Z_a$, de az előző tétel alapján $-d = n - d$ nem osztója az n-nek.

Tétel 3.21. *$\forall a \in Z_n$ esetén igaz, hogy $\exists d \in Z_a : d|n$ vagy $Z_a = \oslash$ Vagyis mindenik zérusosztó halmaz tartalmazza az n-nek legalább egy valódi osztóját.*
Bizonyítás: mivel $a \in Z_n \Rightarrow$ tartalmazza az n-nek legalább egy prímtŕnyezőjét $\Rightarrow$ ez a prímtényező benne lesz a Z_a-ban.

Tétel 3.22. *Az $(U_n, \bigcap, \bigcup)$ struktúrát használva nem lehet elérni, egy olyan halmazt amely csak a valódi osztókat tartalmazza.*
*Bizonyítás:Legyen $A = Z_a * Z_b$ halmaz, ahol * vagy $\bigcap$ vagy $\bigcup$.Ekkor igaz, hogy A vagy üres vagy vagy bíztosan tartalmazz egy $d \in D_n$ és vele együtt a $-d$-t is tartalmazza.A $B = A * Z_a$ halmazra is ugyanez igaz. Ha a $C = A * B$, ahlmazt tekintjük, akkor is teljesülnek a fenti kijelentések. Tehát végeredményben vagy üres halmazt érhetünk el vagy egy olyan halmazt amiben bíztos, hogy van egy d osztó, de bíztosan benne van a $-d$-is, ami viszont nem osztó $\Rightarrow$ a tétel kijelentése.*

Tétel 3.23. *$d|n \Rightarrow Z_d \subseteq Z_n$.*
$Z_d \subseteq Z_n \Rightarrow$ a d-nek a prímtényezős felbontásában nem szerepel idegen tényező az n-éhez képest.
Bizonyítás: Feltételezzük, hogy $d|n \Rightarrow \forall a \in Z_d : \exists k \in Z_d, \exists p \in \mathbb{N} : ak = pd \Rightarrow (ak)\frac{n}{d} = (pd)\frac{n}{d} \Rightarrow a(k\frac{n}{d}) = np \Rightarrow a \in Z_n \Rightarrow Z_d \subseteq Z_n$.
Visszafele természetesen nem igaz. Vegyük például a $\mathbb{Z}_{45}$-ben a Z_{25} és a Z_{45} viszonyát. $Z_{25} \subseteq Z_{45}$, de 25 nem osztja a 45-öt.

Tétel 3.24.

$$\bigcup_{d \in Z_n} (Z_d \bigcap Z_n) = Z_n \backslash \{max(Z_n)\}$$

Bizonyítás: Mivel $Z_d \bigcap Z_n$ tartalmazza az n-nek mindenik d-nél kissebb zérusosztóját, ezért könyen belátható a tétel kijelentése.

References

1. Hardy and Wright, An introduction to the theory of numbers
2. Five and Rosenberg, Number Theory
3. Burton, Elementary Number Theory
4. Carandall, Prime Numbers-A computational Perspective
5. Mărcuş Andrei, Komputeralgebra
6. Mărcuş Andrei, Algebra
7. O'Conor and Robertson, Perfect Numbers
8. Hazar Abu Khuzam, Strcture of rings with certain conditions on zero divisors
9. Rotmann, Advanced Modern Algebra
10. Aigner and Ziegler, Proofs from the book