Az előző részben azoknak a természetes számoknak a **C** halmazát néztük, amelyek előállíthatók két négyzetszám összegeként. Megállapítottuk, hogy **C** zárt a szorzásra, és hogy egy **C**-beli a^2+b^2 szám minden a-hoz és b-hez relatív prím osztója is **C**-beli;

Ez végül is ahhoz az eredményhez vezetett, hogy a **C**-beli számok felismerhetőek prímtényezős felbontásukról: *Minden $4k+3$ alakú prímszámnak páros kitevőn kell szerepelnie.*

Nézzük most meg, hogy mely számok írhatóak fel három négyzetszám összegeként; lehet-e ezekről mondani valami „szépet"?

A valóság az, hogy már az első állítás sem vihető át erre az esetre: ez a halmaz nem zárt a szorzásra. Ennek megmutatására tekintsük a 3-at és az 5-öt. Ezek mindegyike három négyzetszám összege: 3=1+1+1, 5=0+1+4. Ezzel szemben kíséreljük meg szorzatukat, 15-öt így felírni. Nem lehet mindegyik tag legfeljebb 4, mert ekkor az összeg legfeljebb $3\cdot 4=12$ volna. A tagok között 16 (vagy annál nagyobb) nem szerepelhet, mert ekkor az összeg nagyobb lenne, mint 15. Ezért valamelyik tag 9, és $15-9=6$-ot kellene felírni két négyzetszám összegeként, ami nyilván nem lehetséges. A szorzat tehát nem írható fel.

Tekintsük most a természetes számoknak azt a **D** halmazát, amelynek az elemei négy négyzetszám összegeként felírhatók.

1. Tétel: D *zárt a szorzásra.*

Bizonyítás: Legyen $X=a^2+b^2+c^2+d^2$ és $Y=x^2+y^2+u^2+v^2$ a **D**-nek két eleme. Kimutatjuk, hogy ezek szorzata is négy négyzetszám összege (vö. Gy. 2550): (Tulajdonképpen meg lehetne indokolni, hogy miért éppen a következő alakú kifejezéseket írjuk fel; ez azonban túl hosszadalmas volna. Éppen ezért megelégszünk az azonosság felírásával). Legyen

$$Z=(ax+by+cu+dv)^2+(ay-bx+cv-du)^2+$$
$$+(au-bv-cx+dy)^2+(av+bu-cy-dx)^2.$$

ekkor:

$$(*)\qquad X\cdot Y=Z.$$

(Egyszerű számolással belátható, hogy a jobb oldalon a kétszeres szorzatok „kiesnek", és csak az egyes tagok négyzetösszege marad, ami éppen a két négyzetösszeg szorzata.)

Mint ahogy két négyzetszám összegénél tettük, itt is bizonyítani akarjuk az első tétel megfordítását. Ugyanúgy mint ott, itt is csak a **D**-beli számok prímosztóira szorítkozunk. Valamin azonban változtatni kell. Két négyzetszám összegénél olyan prímosztókat néztünk, amelyek a tagok egyikének sem voltak osztói. Itt ezt nem tehetjük, mert például lehet, hogy a tagok között 0 is szerepel, és ennek minden prímszám osztója. Éppen ezért azt tesszük fel, hogy a vizsgált prímszám a négy tag közül *legalább* az egyiknek nem osztója

2. Tétel: *Ha a p prímszám osztója egy* **D***-beli $a^2+b^2+c^2+d^2$ számnak, de nem osztója az a, b, c, d számok mindegyikének, akkor p is* **D***-beli.*

Bizonyítás: Itt is hasonlóképpen járunk el, mint a kéttagú összeg esetében, csak kissé bonyolultabb lesz az eljárás. Tegyük fel, hogy $X=a^2+b^2+c^2+d^2$ osztható p-vel, mondjuk $t\cdot p$ alakú, ahol t pozitív, és p nem osztója a, b, c, d mindegyikének. Azt is feltehetjük, hogy a, b, c, d-t úgy választottuk p-hez (a fenti feltételek mellett), hogy t minimális legyen. Azt fogjuk bizonyítani, hogy ekkor $t=1$. Mivel $2\in\mathbf{D}$ triviálisan igaz, ezért feltehető, hogy p páratlan.

Az a, b, c, d számokat osszuk el rendre p-vel úgy, hogy a legkisebb abszolút értékű maradékot kapjuk:

$$a=p\cdot a''+a',\quad b=p\cdot b''+b',\quad c=p\cdot c''+c',\quad d=p\cdot d''+d';$$

ahol $|a'|,|b'|,|c'|,|d'|<p/2$. (A p páratlansága következtében nem állhat egyenlőség.) Itt persze a', b', c', d' sem lehetnek mind p-vel oszthatók. Másrészt világos, hogy $a'^2+b'^2+c'^2+d'^2$ az eredeti összegtől p egy többszörösében tér el; ezért maga is p-nek egy többszöröse. Végül, a tagok abszolút értékére vonatkozó feltétel következtében ez a négyzetösszeg biztosan kisebb, mint $4\cdot(p/2)^2$. Eszerint létezik olyan **D**-beli $t'\cdot p$ szám, amely kisebb mint p^2, és így $t'<p$. A t minimalitása alapján tehát $t<p$ is igaz.

Ismét hasonlóképpen járunk el, mint két négyzetszám esetén; az a, b, c, d számokat maradékosan osztjuk t-vel, és a legkisebb abszolút értékű maradékot vesszük:

$$a=t\cdot a_1+x,\quad b=t\cdot b_1+y,\quad c=t\cdot c_1+u,\quad d=t\cdot d_1+v,$$

ahol $|x|,|y|,|u|,|v|\le t/2$ (Most nem mondhatjuk, hogy egyenlőség nem állhat fenn, hiszen nem tudhatjuk, hogy t nem páros szám-e!)

Feltételünk szerint $Y=t\cdot p$ és Z-ben, valamint $Y=x^2+y^2+u^2+v^2$-ben helyettesítsük be az x, y, u, v-re most kapott

$$x=a-t\cdot a_1,\quad y=b-t\cdot b_1,\quad u=c-t\cdot c_1,\quad v=d-t\cdot d_1$$

értékeket a $(*)$ azonosságban. Y-ban a négyzetre emelést elvégezve minden tagban szerepelni fog a t tényezőként, kivéve az $a^2+b^2+c^2+d^2$ összeg tagjait, de ez az összeg $t\cdot p$. Eszerint $X=s\cdot t$ alakú, ahol az abszolút értékekre vonatkozó feltétel szerint $Y\le 4\cdot(t/2)^2=t^2$, azaz $s\le t$.

Először tegyük fel, hogy $s<t$. ($s=0$ esetén $t|p$, amiből $t=1$ következik). Ekkor Z-ben a kapott négy tag rendre a következő alakú lesz:

$$a^2+b^2+c^2+d^2+t\cdot A',$$
$$(ab-ba+cd-dc)+t\cdot B,$$
$$(ac-bd-ca+db)+t\cdot C,$$
$$(ad+bc-cb-da)+t\cdot D;$$

ahol A', B, C, D egész számok. Az első tag maga is t-vel osztható: $t\cdot A=t\cdot p+t\cdot A'$ alakú. A többi tagok rendre $t\cdot B$, $t\cdot C$ és $t\cdot D$. Mivel $Z=Y\cdot X=(s\cdot t)\cdot(t\cdot p)$, ahol $s<p$. Z-re kapjuk, hogy $t^2\cdot s\cdot p=Z=(t\cdot A)^2+(t\cdot B)^2+(t\cdot C)^2+(t\cdot D)^2$; ezért:

$$A^2+B^2+C^2+D^2=s\cdot p,$$

ami ellentmond t minimalitásának.

Így tehát arra jutottunk, hogy $s=t$. Ez csak úgy lehet, ha $|x|=|y|=|u|=|v|=t/2$. Ez azt jelenti, hogy a, b, c, d mindegyike osztható $(t/2)$-lel, azaz $X=t\cdot p$ osztható $(t/2)^2$-nel. Mivel p prím és $t<p$, ezért ez csak úgy lehetséges, hogy $(t/2)^2$ t-nek osztója, amiből az következik, hogy t osztója 4-nek. Erre három lehetőségünk van: $t=4$, $t=2$ és $t=1$.

Az első esetben $|x|=|y|=|u|=|v|=2$, így a, b, c, d mindegyike páros. Ez ellentmond t minimalitásának, mert most

$$(a/2)^2+(b/2)^2+(c/2)^2+(d/2)^2=4\cdot p/4=p.$$

A $t=2$ esetben $|x|=|y|=|u|=|v|=1$, és így a, b, c, d mindegyike páratlan. Tekintettel arra, hogy páratlan szám négyzete 4-gyel osztva egyet ad maradékul, ezért négyzetösszegük $(2\cdot p)$ osztható 4-gyel, ami lehetetlen, hiszen p páratlan.

Végezetül a $t=1$ esetben éppen a bizonyítandó állítást nyerjük.

Így csak $t=1$ lehetséges, amivel a tételt bebizonyítottuk.

Azt kell még megvizsgálni, hogy mely prímszámok írhatóak fel négy négyzetszám összegeként.

3. Tétel: *Minden prímszám felírható négy négyzetszám összegeként.*

Bizonyítás: A $p=2$ esetben $2=1+1+0+0$ egy megfelelő felírás; ezért a továbbiakban elég páratlan p prímszámokat nézni.

Legyen $q=(p-1)/2$, és tekintsük a 0, 1, ..., q számok $\mathbf{Q}$ halmazát. Legyen $i,j\in\mathbf{Q}$, és tekintsük az $n=i^2-j^2=(i-j)\cdot(i+j)$ számot. $-q\le i-j\le q$ és $0\le i+j\le 2\cdot q<p$ alapján n csak $i=j$ esetén osztható p-vel. Ebből két dologra következtethetünk:

1) Az i^2+1 ($i\in\mathbf{Q}$) alakú számok p-vel osztva csupa különböző maradékot adnak, mert két ilyen szám különbsége nem lehet p-vel osztható.

2) A $-j^2$ ($j\in\mathbf{Q}$) alakú számok is csupa különböző maradékot adnak ugyancsak a fenti indok miatt.

Mármost $\mathbf{Q}$-nak $q+1$ eleme van, ezért mind az 1)-ben, mind a 2)-ben felsorolt számok $q+1$ különböző maradékot adnak p-vel osztva. Mivel ezek száma összesen $(q+1)+(q+1)=p+1$, és p-vel osztva pontosan p számú osztási maradék lehet, ezért kell olyan 1)-ben felsorolt i számnak és olyan 2)-ben felsorolt j számnak lennie, amelyek p-vel való osztási maradéka megegyezik. Ez azt jelenti, hogy különbségük, i^2+1+j^2 osztható p-vel. Ez a szám $1=1^2$ miatt három (és így négy) négyzetszám összege, tehát p osztója egy $\mathbf{D}$-beli számnak. Mivel $p\ne 1$, ezért a második tétel szerint p maga is $\mathbf{D}$-beli, mint állítottuk.

Az első tételt felhasználva most már azonnal adódik:

4.Tétel: *Minden pozitív egész szám felírható négy négyzetszám összegeként.*

Érdemes felfigyelni arra, hogy a kapott „négy négyzetszám tétel"-nek a bizonyítása, annak ellenére, hogy sok számolást és „trükköt" használt fel, teljesen elemi volt. Valamivel mélyebb segédeszköz csupán a „két négyzetszám tétel" bizonyításánál volt szükséges.