Dolgozatunk előzménye a következő feladat volt: bizonyítandó, hogy ha p prím, akkor $\left[\binom{3p}{p}-3\right]$ osztható p^2 -tel. Ennél kicsit többet és némileg általánosabb összefüggést sikerült megmutatnunk, ezt ismertetjük a továbbiakban.

Tétel: Ha p 3-nál nagyobb prímszám, akkor $\left[\binom{ap}{bp}-\binom{a}{b}\right]$ osztható p^3-nal.

A bizonyítás első részét kombinatorikus úton végezzük. Tekintsük az 1, 2, ..., ap számokat. Osszuk ezeket a darab „blokkra"; az első álljon az $1, 2, \ldots, p$; a második a $(p+1)$, $(p+2)$, ..., $2p$; ... az a -adik az $(a-1)p+1$, $(a-1)p+2$, ..., ap számokból. Vegyünk a fenti ap darab szám közül bp -t úgy, hogy ne b teljes blokkot válasszunk ki. Az ilyen „telítetlen" kiválasztások száma éppen $\left[\binom{ap}{bp}-\binom{a}{b}\right]$, mivel bp darab szám kiválasztása $\binom{ap}{bp}$ - féleképpen történhet, és ezek között $\binom{a}{b}$ kiválasztás áll b darab teljes blokkból. A telítetlen kiválasztásokat most olyan osztályokba soroljuk, melyeknek elemszáma – vagy több ilyen osztály elemszámának az összege – p^3-nal osztható, amiből a bizonyítandó állítás nyilván következik.

Nevezzük forgatásnak a következő műveletet: ha egy blokkban a kiválasztott számok $c_1 < c_2 < \ldots < c_k$ $(0 < k < p)$, akkor ebből a blokkból a művelet után (c_1+1), (c_2+1), ..., (c_k+1) szerepeljen az új kiválasztásban, a további blokkokat, illetve az azokból kiválasztott számokat pedig hagyjuk változatlanul. (Ha c_k a blokk legnagyobb eleme, akkor helyette vegyük a legkisebbet.) Tartozzanak ezek után egy osztályba azok a kiválasztások, amelyek több-kevesebb – nem szükségképpen ugyanazon a blokkon végrehajtott – forgatással egymásba vihetők. A telítetlen kiválasztások így kapott osztályai közül nyilván semelyik kettőnek nincs közös eleme. (Így ekvivalenciarelációt definiálunk a telítetlen kiválasztások halmazán. A szerk.)

A fenti műveletet szemléletessé tehetjük, ha az ap darab számot a darab szabályos p-oldalú sokszög csúcsaihoz írjuk és a csúcsokban megjelöljük a bp darab kiválasztott számot. Egy forgatás így az egyik sokszögön levő jelek elforgatását jelenti $\frac{2\pi}{p}$ szöggel (ábra).

1988-05-198-1.eps

Azt állítjuk, hogy ha egy – nem üres, nem teli – blokk kivételével rögzítjük az összes többi elemet, akkor egy adott kiválasztásból az adott blokk forgatásaival éppen p darab különböző kiválasztás érhető el. Többet nem kaphatunk, hiszen egy blokkon belül p darab elforgatás önmagába viszi a blokkot és így az adott kiválasztást. Így csak azt kell megmutatnunk, hogy p-nél kevesebb elforgatás az eredetitől különböző állapotra vezet. Tegyük fel, hogy állításunkkal ellentétben egy nem üres, nem teli blokkot r számú elforgatás $(0 < r < p)$ önmagába visz. Tekintsük a blokk egy kiválasztott c_1 elemét. Az r darab elforgatás ezt olyan c_2 számba viszi, amelyre $c_2 - c_1 \equiv r (\mathrm{mod}\ p)$, és c_2 maga is kiválasztott. A fenti gondolatmenetet c_2-re, és tovább alkalmazva a kiválasztott számoknak olyan c_3, c_4, ..., c_p sorozatához jutunk, amelyre $c_k - c_1 \equiv (k-1)r (\mathrm{mod}\ p)$. Ezek a számok mind *különbözők*, hiszen c_i és c_j $(i < j)$ csak akkor lehet egyenlő, ha $(j-i)r$ osztható p -vel $(0 = c_i - c_j \equiv (j-i)r (\mathrm{mod}\ p))$. Ez viszont nem fordulhat elő, hiszen $j, i < p$ miatt $j - i < p$, továbbá $r < p$, és p prímszám. Így viszont a blokk minden eleme kiválasztott, amit pedig kizártunk. Ezzel a kimondott állítást igazoltuk.

Vegyük most szemügyre az olyan osztályokat, amelyek kiválasztásai legalább három nem üres, nem teli blokkot tartalmaznak. Az ilyen osztályok elemszáma – figyelembe véve, hogy a nem üres, nem teli blokkokat egymástól függetlenül forgathatjuk p helyzetbe – p-nek legalább a harmadik hatványával osztható.

Olyan kiválasztás, melyben a nem üres, nem teli blokkok száma 1, nem létezik, hiszen a kiválasztott elemek száma p-vel osztható.

Az eddig figyelembe nem vett osztályok mindegyike tehát pontosan *két* nem üres, nem teli blokkot tartalmaz. Egyesítsük most azon osztályokat, amelyekre ez a két blokk ugyanaz, továbbá a teli blokkok is azonosak. Ha az egyik blokkban k, akkor a másikban $(p-k)$ kiválasztott elem van, így ebben az egyesítésben

$$\sum_{k=1}^{p-1} \binom{p}{k} \binom{p}{p-k} = \sum_{k=1}^{p-1} \binom{p}{k}^2$$

darab kiválasztás szerepel.

Tételünk bizonyításához most már elegendő megmutatnunk, hogy ez az összeg is osztható p^3-nal. (Maga az összeg egyébként $\binom{2p}{p} - \binom{2}{1}$, hiszen a rögzített két blokkban $2p$ darab szám közül választunk ki p darabot úgy, hogy a kiválasztott számok nem alkotnak teljes blokkot. Így tételünk speciális esetével állunk szemben: $a = 2$ és $b = 1$.)

$\binom{p}{k} = \frac{p!}{k!(p-k)!}$ osztható p-vel, hiszen a számláló osztható vele, a nevező nem. Ezért összegünk minden tagja osztható p^2-tel. A továbbiakban tehát annak bizonyítására szorítkozhatunk, hogy

$$\sum_{k=1}^{p-1} \left[\frac{\binom{p}{k}}{p}\right]^2$$

osztható p-vel.

Ha megmutatjuk, hogy

$$\frac{\binom{p}{k}}{p} \equiv \frac{\binom{p}{m}}{p} \pmod{p}, \quad (1 \leqq k, \quad m \leqq p-1) \tag{1}$$

akkor és csak akkor teljesül, ha $k = m$, vagy $k + m = p$; – tehát ha a számlálók egyenlők – továbbá, hogy

$$\frac{\binom{p}{k}}{p} \equiv -\frac{\binom{p}{m}}{p} \pmod{p} \tag{2}$$

sosem állhat, akkor a

$$\frac{\binom{p}{1}}{p}, \ \frac{\binom{p}{2}}{p}, \ \ldots, \ \frac{\binom{p}{p-1}}{p}$$

számok p-vel osztva az

$$(1,-1), \ (2,-2), \ \ldots, \ \left(\frac{p-1}{2}, -\frac{p-1}{2}\right)$$

maradék párok mindegyikének pontosan az egyik tagját állítják elő, s azt kétszer. Ez esetben pedig

$$\sum_{k=1}^{p-1}\left[\frac{\binom{p}{k}}{p}\right]^2 \equiv 2\left[1^2+2^2+\ldots+\left(\frac{p-1}{2}\right)^2\right] = 2\frac{\frac{p-1}{2}\cdot\frac{p+1}{2}\cdot p}{6} \pmod{p},$$

s ez utóbbi $p > 3$ miatt valóban osztható p-vel.

Az (1), (2) kongruenciák vizsgálatához először egy segédtételt igazolunk:
ha p prím, és $k < p$ nemnegatív egész, akkor

$$k!(p-k-1)! + (-1)^k$$

osztható p-vel.

A bizonyítás a k -ra vonatkozó teljes indukcióval történik. $k = 0$-ra *Wilson* tételét kapjuk.[1] Tegyük fel, hogy k -ra már beláttuk az állítást, azaz :

$$k!(p-k-1)! \equiv (-1)^{k+1} \pmod{p}.$$

Most $p - k - 1 \equiv -(k+1) \pmod{p}$ felhasználásával:

$$k!(p-k-2)! \cdot [-(k+1)] \equiv (-1)^{k+1} \pmod{p},$$

ahonnan (-1) -gyel szorozva

$$(k+1)!(p-k-2)! \equiv (-1)^{k+2} \pmod{p}.$$

Ez pedig éppen a $(k+1)$ -re vonatkozó állításunk, így a segédtételt beláttuk.

Lássuk tehát, hogy $\frac{\binom{p}{k}}{p} \equiv \frac{\binom{p}{m}}{p} \pmod{p}$ mikor állhat fönn.

$$\frac{(p-1)!}{k!(p-k)!} \equiv \frac{(p-1)!}{m!(p-m)!} \pmod{p}.$$

$k!(p-k)!m!(p-m)!$-sal szorozva és $(p-1)!$-sal osztva (ezek relatív prímek p -hez, így ekvivalens átalakításokat végeztünk):

$$m!(p-m)! \equiv k!(p-k)! \pmod{p}.$$

Segédtételünket felhasználva ez akkor és csak akkor igaz, ha

$$(-1)^{m+1}(p-m) \equiv (-1)^{k+1}(p-k) \pmod{p}.$$

Ha m és k azonos paritásúak, akkor innen $k = m$, ha pedig különböző paritásúak, akkor $k + m = p$ adódik. ($0 < k, \ m < p$; p páratlan). Utóbbi lépéseink is megfordíthatóak voltak. Ezzel a segédtétel első részét igazoltuk.

[1] Wilson tétele azt mondja ki, hogy $(p-1)! + 1$ osztható p -vel, azaz $(p-1)! \equiv -1 \pmod{p}$. Bizonyítása megtalálható pl. Hajós György–Neukomm Gyula–Surányi János: Matematikai Versenytételek II., Tankönyvkiadó 1965. 101–102. oldal.

A $\frac{\binom{p}{k}}{p} \equiv -\frac{\binom{p}{m}}{p} \pmod p$ föltevés a fentiek szerint arra vezet, hogy:

$$-(-1)^{m+1}(p-m) \equiv (-1)^{k+1}(p-k) \pmod p.$$

Itt viszont, ha k és m azonos paritásúak, akkor $k+m=p$, ha pedig különböző paritásúak, akkor $k=m$ következik, ami lehetetlen, mert a p páratlan. Ezzel a segédtételt teljes egészében beláttuk, és így tételünk bizonyítása is teljes.

*

Más úton is igazolható, hogy $\left[\binom{2p}{p}-2\right] \equiv 0 \pmod{p^3}$. Kiírva:

$$\frac{2p(2p-1)\dots(p+1)}{1\cdot 2\cdot \dots \cdot p} = \frac{2\cdot(2p-1)\dots(p+1)}{1\cdot 2\cdot \dots \cdot (p-1)} \equiv 2 \pmod{p^3}.$$

$(p-1)!$ és 2 is relatív prím p^3-hoz, ezért azonos átalakítás, ha $(p-1)!$-sal szorzunk és 2-vel osztunk:

$$(p+1)(p+2)\dots[p+(p-1)] \equiv (p-1)! \pmod{p^3}. \tag{3}$$

Végezzük el a beszorzást a bal oldalon. A p^3-os, p^4-es, $\dots, p^{p-1}$-es tagok oszthatók p^3-nal. A p^2 együtthatója ekkor

$$A_1 = \frac{(p-1)!}{1\cdot 2} + \frac{(p-1)!}{1\cdot 3} + \dots + \frac{(p-1)!}{(p-2)(p-1)}$$

(minden lehetséges pár megjelenik a nevezőben), a p együtthatója pedig

$$A_2 = \frac{(p-1)!}{1} + \frac{(p-1)!}{2} + \dots + \frac{(p-1)!}{p-1}.$$

A_1 osztható p-vel, A_2 pedig p^2-tel. (Ez utóbbiak bizonyítása megtalálható *D. O. Skljarszkij–N. N. Csencov–I. M. Jaglom:* Válogatott feladatok és tételek az elemi matematika köréből, 1. kötet. Bp. 1979. 135–136. oldal.) Ebből a (3) kongruencia következik, hiszen a bal oldalon a beszorzás és a p hatványai szerinti rendezés után a „konstans" $(p-1)!$-on kívül minden tag osztható p^3-nal. A lépések megfordíthatóak voltak, így tehát $\binom{2p}{p} \equiv 2 \pmod{p^3}$.

*

Tételünk állításából azonnal adódik hogy $\left[\binom{ap^k}{bp^k} - \binom{a}{b}\right]$ is osztható p^3-nal ($k \geqq 1$, egész). Ezt teljes indukcióval láthatjuk be; $k=1$ -re tételünk fent bizonyított állítását kapjuk. Tegyük most fel, hogy k-ra már igazoltuk az állítást; ekkor $(k+1)$-re:

$$\binom{ap^{k+1}}{bp^{k+1}} - \binom{a}{b} = \left[\binom{ap^{k+1}}{bp^{k+1}} - \binom{ap^k}{bp^k}\right] + \left[\binom{ap^k}{bp^k} - \binom{a}{b}\right],$$

és itt az első szögletes zárójelben álló tag kiinduló tételünk, a második szögletes zárójelben álló tag pedig az indukciós feltevés szerint osztható p^3 -nal, így az állítás $(k+1)$-re is következik.