# A kis Fermat-tétel néhány bizonyítása

**Összegyűjtötte Kalló Bernát és Nagy Dániel**

Freud Róbert 2005. november 22-ei előadásán (lásd eloadas_2005_11_22_freud.doc) hallottuk az alábbi tételt, egy bizonyítását és alkalmazásait.

> **Kis Fermat-tétel**: Ha $p$ prím és $c$ tetszőleges egész szám, akkor $p \mid c^p - c$.

Ott teljes indukciós megoldást hallhattunk, most lássunk két másik gondolatmenetet!

**I. Bizonyítás (Teljes maradékrendszerrel)**

> **Definíció:** Azt mondjuk, hogy a $H$ számhalmaz teljes maradékrendszer modulo $n$, ha $H$ elemeinek $n$-es maradékai minden lehetséges $n$-es maradékot egyszer és csakis egyszer adnak ki.

Világos, hogy ha $H$ teljes maradékrendszer modulo $n$, akkor $H$ elemeinek $n$-es maradékai valamilyen sorrendben a 0, 1, 2, ..., ($n$-1) számok, tehát $H$ elemeinek száma $n$.

> **Lemma:** Ha $(a, n)=1$, akkor $\{a, 2a, ..., (n-1)a, na\}$ teljes maradékrendszer modulo $n$.

Bizonyítás indirekt úton:
Tegyük fel, hogy az állítás nem igaz. Az említett halmaz elemeinek száma épp $n$, így pontosan akkor nem teljes maradékrendszer, ha az elemek között van kettő, melyek $n$-es maradéka megegyezik. Legyenek ezek $ia$ és $ja$, ahol $1 \leq i < j \leq n$, azaz $n \mid ja - ia = (j - i)a$. Mivel $(a, n)=1$ és $0 < j - i < n$, így ez ellentmondás.

Térjünk most vissza a kis Fermat-tétel bizonyítására!
Ha $c$ osztható $p$-vel, akkor az állítás nyilvánvalóan igaz. Ha $c$ nem többszöröse $p$-nek, akkor $(c, p)=1$, mivel $p$ prím. Tekintsük a $\{c, 2c, 3c, ..., (p-1)c, pc\}$ teljes maradékrendszert modulo $p$. A legutolsó elem, a $pc$ szám $p$-s maradéka 0, a többié valamilyen sorrendben 1, 2, 3, ..., $p$-1. Szorozzuk össze a vizsgált teljes maradékrendszer elemeit a $pc$ kivételével!

$$(1) \quad c \cdot 2c \cdot 3c \cdot \ldots \cdot (p-1)c = (p-1)!c^{p-1}.$$

Mivel egy szorzat $p$-vel való osztási maradéka megegyezik a tagok $p$-vel való osztási maradékainak szorzatával, így a $(p-1)!c^{p-1}$ szám $p$-vel való osztási maradéka

$$(2) \quad 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = (p-1)!.$$

Az (1), (2) számok $p$-s maradékai egyenlők, tehát e két szám különbsége osztható $p$-vel:

$$p \mid (p-1)!c^{p-1} - (p-1)! = (p-1)!(c^{p-1} - 1).$$

A $p$ prímszám relatív prím a nála kisebb egészek szorzatából álló ($p$-1)!-hoz, így $p \mid c^{p-1} - 1$, amiből adódik, hogy $p \mid c^p - c$, ahogy állítottuk.

**Ajánló**
Ez a klasszikus bizonyítás megtalálható pld az alábbi könyvben (240. feladat):
D.O. Sklarszkij –N.N. Csencov – I. M. Jaglom, Válogatott feladatok és tételek az elemi matematika köréből, 1. kötet (Aritmetika és Algebra). Régen a Tankönyvkiadó, újabban a Typotex kiadó adja ki.
http://www.typotex.hu/book/m_0053.htm

## II. Bizonyítás (Kombinatorika)

**Feladat:** Adott egy szabályos hétszög. Színezzük ki a csúcsait két színnel, pld pirossal és kékkel. Hányféle különböző színezés lehetséges, ha a forgatással egymásba vihetőket nem különböztetjük meg egymástól?

Ha a forgatásokról először elfeledkezünk, akkor a következőképpen számolhatunk: mindegyik csúcs kétféle lehet, így a színezések száma $\underbrace{2\times 2\times 2\times \ldots \times 2}_{7\text{ tényező}} = 2^7$. Gondolatban készítsük el ezt a $2^7$-féle színezést, ez lesz a listánk, amely segítségével majd a feladat kérdésére is válaszolunk.

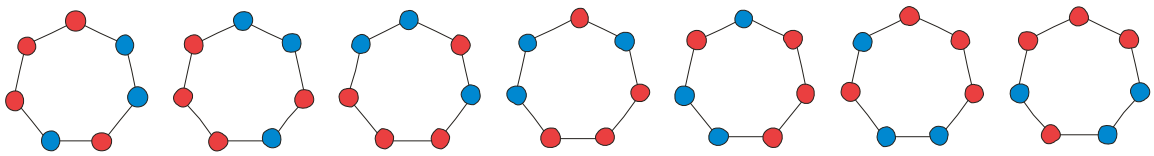
Hányszor szerepel a listában egy-egy színezés, ha most már a forgatással egymásba vihetőket nem különböztetjük meg?

Azokat a színezéseket, amelyeknél minden csúcs egyforma csak egyszer számoltuk. Két ilyen színezés van: a csupa kék és a csupa piros.

Maradt $2^7$-2 elem a listán. Ide már csak olyan színezések tartoznak, amelyek mindkét színből tartalmaznak csúcsot. Ha tekintjük a lista egy elemét, annak színezését elforgathatjuk a hétszög középpontja körül az alábbi szögek bármelyikével:

$$\frac{360°}{7}, 2\times\frac{360°}{7}, 3\times\frac{360°}{7}, 4\times\frac{360°}{7}, 5\times\frac{360°}{7}, 6\times\frac{360°}{7}.$$

Az így elforgatott színezések tehát nem lesznek új színezések, de esetleg a lista egy másik elemét adják meg. Így a lista egy eleméből kiindulva a listában akár – önmagával együtt – 7 listaelemet találhatunk, amelyek színezését egyformának kell tekintenünk. Alább azt fogjuk látni, hogy minden olyan esetben, amikor nem a csupa kék vagy a csupa piros színezésből indulunk ki, pontosan hét listaelem tartozik össze.



Ez az állítás azzal egyenértékű, hogy a fenti forgatások csupa különböző listaelemet hoznak létre, azaz egyik forgatás egyik elemet sem tudja önmagába vinni (kivéve a „csupa” színezésűeket). Tegyük fel, hogy a $k\times\frac{360°}{7}$-os szöggel való forgatás a lista egy elemét önmagába viszi. Akkor ebben az elemben egy tetszőlegesen választott piros csúcs $k\times\frac{360°}{7}$-os szöggel való elforgatottja is piros, sőt annak $k\times\frac{360°}{7}$-os szöggel való elforgatottja is piros, sőt .... Tehát az adott csúcs

$$k\times\frac{360°}{7}, 2k\times\frac{360°}{7}, 3k\times\frac{360°}{7}, 4k\times\frac{360°}{7}, 5k\times\frac{360°}{7}, 6k\times\frac{360°}{7}, 7k\times\frac{360°}{7}$$

-os szöggel való elforgatottjai is pirosak. Így mind a hét csúcsba beforgattuk az eredeti piros csúcsot. Valóban, a fenti hét elforgatott mind más: erről könnyű meggyőződni annak alapján, hogy 7 prím és $0 < k < 7$.

A színezések száma tehát $2+\frac{2^7 - 2}{7}$.

**Tétel:** Ha $p$ prímszám és egy szabályos $p$-szög csúcsait $c$ színnel színezzük, akkor

$$c + \frac{c^p - c}{p}$$

színezés lehetséges, ha a forgatással egymásba vihetőket nem különböztetjük meg egymástól.

Ennek a tételnek a bizonyítását nem részletezzük, mert az indoklás lényegi része azonos a Feladat megoldásával.

A Tétel állításából következik a kis Fermat-tétel állítása, hiszen a színezések száma egész szám és a rá kapott formula pontosan akkor egész értékű, ha $p|c^p-c$.

**Ajánló**
A „Feladat” forrása: George E. Andrews, Number Theory, Dover Publication, Inc. New York.