

Koľkými spôsobmi vieme spraviť náhrdelník (ktorému nezáleží na rotáciách), z a rôznych farieb o veľkosti k ? Vyriešte pre nekonečne veľa rôznych a .

Spočítame rozpojené náhrdelníky (rovné pásiky): a^k

Chceme to deliť veľkosťou k , ale čo ak sa tam niekedy opakujú možnosti, teda dva rôzne pásiky tvoria ten istý zapojený náhrdelník. Je to zložité, no pri prvočíslach sa nám to deje iba ak všetky korálky sú rovnaké. Inak nemôže vzniknúť otočiteľná vec, lebo taká musí mať periodicky sa opakujúce časti - teda sa dá rozdeliť na niekoľko rovnako veľkých častí.

Z toho dostávame že celočíselný počet náhrdelníkov je $(a^k - a)/k + a$

Teda keď je k prvočíslo, musí deliť čitateľ.

To je malá Fermatova veta, ktorú poznáme vo viacerých formuláciách:

$$F1: p \mid a^p - a$$

$$F2: a^p \equiv a \pmod{p}$$

$$F3: a^{p-1} \equiv 1 \pmod{p}$$

$$(F4) p \mid a^{p-1} - 1$$

Iný dôkaz je indukciou na a a využitím binomickej vety:

$a^p \equiv a \pmod{p}$ pre $a=1$ triviálne platí.

Dokážme, že ak platí $a^p \equiv a \pmod{p}$, tak platí aj $(a+1)^p \equiv a+1 \pmod{p}$:

Podľa binomickej vety všetky členy roz násobeného $(a+1)^p$ okrem prvého a posledného obsahujú kombinačné číslo $s \cdot p!$ v čitateli. V menovateli nie je $p!$, preto p delí každé z kombinačných a tým pádom aj všetky členy okrem prvého a posledného. Prvý a posledný člen sú $1 \times a^0 \times 1^p + 1 \times a^p \times 1^0 = 1 + a^p$. Ostatné členy môžeme škrtnúť lebo majú zvyšok 0 po delení p . Oстане:

$1 + a^p \equiv a+1 \pmod{p} \rightarrow a^p \equiv a \pmod{p}$, čo je predpoklad z ktorého vychádzame.

Úlohy na využitie malej Fermatovej vety

1. $5^{5729} \equiv ? \pmod{11}$

Riešenie:

$$F3(5, 11): 5^{10} \equiv 1 \pmod{11}, 5^{10k} \equiv k \pmod{11}, (5^{10})^n \equiv 1 \pmod{11}, (5^{10k})^n \equiv k \pmod{11}$$

2. Ukážte, že ak $p \neq q$, tak pre všetky a platí:

$$pq \mid a^{pq} - a^p - a^q + a$$

Riešenie:

$$p \mid a^{pq} - a^p - a^q + a$$

$$+F1(a, p): p \mid a^{pq} - a^q$$

$$F2(a, p): p \mid a^q - a$$

analogicky pre q

3. Ukážte, že ak $p \neq q$, tak:

$$a) p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

Riešenie:

$\text{mod } q$ je to $F3(p, q)$, $\text{mod } p$ je to $F3(q, p)$

prepojenie cez deliteľnosť/intuitívne

$$b) p^q + q^p \equiv p + q \pmod{pq}$$

Riešenie:

$pq \mid p^q + q^p - p - q$
 $p \mid p^q + q^p - p - q$
 $p \mid q^p - q$ F1()
analogicky pre $q \mid$

4. Dokážte, že pre každé $p > 5$ existuje jeho násobok, ktorý má v zápise (v desiatkovej sústave) iba cifru 1.

Riešenie:

F3(10,p): $10^{p-1} \equiv 1 \pmod{p}$

$p \mid 10^{p-1} - 1$

$p \mid (10^{p-1} - 1)/9$

5. Nájdite najmenšie prirodzené číslo n také, že:

a) $2^n \equiv 1 \pmod{257}$

b) $253^n \equiv 1 \pmod{257}$

Riešenie:

257 je prvočíslo. F3(2,257): $2^{256} \equiv 1 \pmod{257}$

Koľko môže byť 2^{128} ? Čo na druhú je 1? Buď 1 alebo -1. A tak ďalej...

Pri b) využijeme poznatok z a)