

Megoldás. Felhasználjuk, hogy

$$(1) \quad \nu(n) = \sum_{k=1}^{\infty} \left[\frac{n}{2^k} \right];$$

ez speciális esete az úgynevezett *Legendre-formulának*. (A Legendre-formuláról bővebben lásd az 1. megjegyzést.)

Ha az n szám kettes számrendszerbeli alakja

$$n = \overline{d_\ell d_{\ell-1} \dots d_1 d_0} = \sum_{i=0}^{\ell} d_i \cdot 2^i,$$

ahol a d_0, \dots, d_ℓ számjegyek mindegyike 0 vagy 1, akkor (1)-ben csak $k \leq \ell$ esetén kapunk 0-tól különböző tagokat, és

$$\begin{aligned} \nu(n) &= \sum_{k=1}^{\infty} \left[\frac{n}{2^k} \right] = \sum_{k=1}^{\ell} \left[\frac{\overline{d_\ell d_{\ell-1} \dots d_1 d_0}}{2^k} \right] = \sum_{k=1}^{\ell} \overline{d_\ell d_{\ell-1} \dots d_k} = \\ &= \sum_{k=1}^{\ell} \left(\sum_{i=k}^{\ell} d_i \cdot 2^{i-k} \right) = \sum_{i=1}^{\ell} d_i \left(\sum_{k=1}^i 2^{i-k} \right) = \sum_{i=1}^{\ell} d_i \cdot (2^i - 1). \end{aligned}$$

Ennek egyszerű következménye, hogy *pontosan azok a pozitív egészek állnak elő $\nu(n)$ alakban, amelyek felírhatók különböző $2^i - 1$ alakú számok összegeként.*

Következő lépésként megmutatjuk, hogy van olyan r szám, ami relatív m -mel, és végtelen sokszor áll elő $2^i - 1$ alakú számok m -mel való osztási maradékaként, vagyis léteznek olyan $i_1 < i_2 < i_3 < \dots$ pozitív egészek, amelyekre

$$2^{i_1} - 1 \equiv 2^{i_2} - 1 \equiv 2^{i_3} - 1 \equiv \dots \equiv r \pmod{m}.$$

Írjuk m -et $2^t u$ alakban, ahol u páratlan szám, és tekintsünk egy tetszőleges olyan $i \geq t$ pozitív egészt, amire $i - 1$ osztható $\varphi(u)$ -val. Nyilván végtelen sok ilyen i létezik. Az Euler–Fermat-tétel alapján minden egyes ilyen i értékre

$$(2) \quad \begin{aligned} u | 2^{\varphi(u)} - 1 | 2^{i-1} - 1, \\ 2^i - 1 = 2(2^{i-1} - 1) + 1 \equiv 1 \pmod{u}, \end{aligned}$$

és $i \geq t$ miatt

$$(3) \quad 2^i - 1 \equiv -1 \pmod{2^t}.$$

A $2^i - 1$ szám (2) és (3) miatt relatív prím u -val és 2^t -vel is, továbbá (2) és (3) egyértelműen meghatározza $2^i - 1$ maradékát modulo $[u, 2^t] = m$. Ez a maradék tehát valóban végtelen sokszor előfordul.

Mivel m és r relatív prímekek, az $r, 2r, 3r, \dots$ számok teljes maradékrendszert alkotnak modulo m , és létezik olyan u pozitív egész, amire $a \equiv ur \pmod{m}$. Ekkor az $n = 2^{i_1} + \dots + 2^{i_u}$ számra

$$\nu(n) = \nu(2^{i_1} + \dots + 2^{i_u}) = (2^{i_1} - 1) + \dots + (2^{i_u} - 1) \equiv u \cdot r \equiv a \pmod{m}.$$

Ezzel megkonstruáltuk a kívánt n számot.

Megjegyzések. 1. Ha $\nu_p(n)$ -nel jelöljük tetszőleges p prímszámra és nemnegatív egész n -re a p kitevőjét az $n!$ prímtényezős felbontásában, akkor az úgynevezett *Legendre-formula* szerint

$$\nu_p(n) = \left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \left[\frac{n}{p^3} \right] + \dots = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right].$$

Ha összeszámoljuk azt, hogy az $1, 2, \dots, n$ számok között hány p -vel osztható, hány p^2 -tel osztható stb. van, éppen a jobboldalon álló összeget kapjuk. Ez szemléletesen bizonyítja a képletet.

A formálisabb bizonyításhoz tetszőleges ℓ pozitív egészre jelöljük $\mu_p(\ell)$ -lel a p kitevőjét az ℓ prímtényezős felbontásában. Mivel szorzásnál a kitevők összeadódnak,

$$\nu_p(n) = \mu_p(1 \cdot 2 \cdot \dots \cdot n) = \mu_p(1) + \mu_p(2) + \dots + \mu_p(n).$$

Tekintsük most az összes olyan (k, ℓ) párt, amelyekben $1 \leq \ell \leq n$ és p^k osztója ℓ -nek, és számoljuk össze kétféleképpen az ilyen tulajdonságú párokat.

Először csoportosítsuk a (k, ℓ) párokat ℓ értékei szerint. Egy rögzített ℓ szám a p -nek mindig pontosan $\mu_p(\ell)$ különböző hatványával osztható: ezek a $p, p^2, \dots, p^{\mu_p(\ell)}$ számok, ezért

$$(4) \quad \sum_{(k, \ell)} 1 = \sum_{\ell} \sum_{p^k | \ell} 1 = \sum_{\ell} \mu_p(\ell) = \nu_p(n).$$

Most csoportosítsuk a párokat k értékei szerint. Minden egyes k -ra azokat az ℓ -eket keressük, amelyek többszöresei p^k -nak; az $1, 2, \dots, n$ között ezek száma $\left[\frac{n}{p^k} \right]$. A párok száma tehát

$$(5) \quad \sum_{(k, \ell)} 1 = \sum_{k=1}^{\infty} \sum_{\ell \leq n, p^k | \ell} 1 = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right].$$

A (4) és (5) képletek együtt bizonyítják a Legendre-formulát.

2. Az állítást a 2 helyett bármelyik másik prímmel kimondhatjuk; a bizonyítás minden nehézség nélkül átirható.