

Az alábbiakban közöljük *Ivanyos Gábornak* a 3. feladatra adott megoldását, amelyért a zsűritől különdíjat kapott.¹

Feladat: Legyen n adott, 2-nél nagyobb természetes szám! Jelöljük V_n -nel azt a halmazt, amelynek elemei: $1 + kn$, ahol $k = 1, 2, \dots$. Egy $m \in V_n$ számot V_n -ben felbonthatatlannak mondunk, ha nincsenek olyan $p, q \in V_n$ számok, amelyekre $pq = m$.

Bizonyítsuk be, hogy van olyan $r \in V_n$ szám, amely több, mint egyféleképpen állítható elő V_n -ben felbonthatatlan számok szorzataként! (Azokat a felbontásokat, amelyek csak a V_n -ből vett tényezők sorrendjében különböznek egymástól, azonosaknak vesszük.)

Megoldás. a) Először azt fogjuk bizonyítani, hogy végtelen sok olyan prímszám van, amely n -nel osztva 1-től különböző maradékot ad.

Tegyük fel, hogy csak véges sok van, és szorozzuk ezeket össze. Az így kapott szorzatot szorozzuk meg még n -nel, majd vonjunk ki belőle 1-et. ($n > 2$ miatt ez nem 1 maradékot ad $(\text{mod } n)$). Az így kapott szám nem osztható a véges sok prím egyikével sem, tehát összes prímtényezői $(1 + mn)$ alakúak lehetnek csak, azaz előállítható $(1 + mn)$ alakú számok szorzataként. Azonban az $(1 + mn)$ alakú számok szorzata szintén ilyen alakú, s a mi számunk nem 1 maradékot ad $(\text{mod } n)$, tehát ellentmondásra jutottunk.

Ebből következik, hogy létezik végtelen sok olyan prímszám, amely n -nel osztva nem 1-et ad maradékul, tehát alkalmazható az adott bizonyítás.

b) Ismeretes, hogy végtelen sok prímszám van, ebből, és hogy $(\text{mod } n)$ véges sok maradékosztály van, következik, hogy van olyan maradékosztály $(\text{mod } n)$, amelybe legalább $2(n + 1)$ prím esik.

Legyenek ezek

$$p_1, p_2, \dots, p_n, p_{n+1}, p_{n+2} = q_1, p_{n+3} = q_2, \dots, q_{n+1} = p_{2n+2},$$

melyek tehát $(\text{mod } n)$ ugyanazt az a maradékot adják.

Segéd-tétel: van olyan $\alpha \leq n$ kitevő, hogy

$$a^\alpha \equiv 1 \pmod{n}.$$

Tekintsük az $a^1, a^2, \dots, a^n, a^{n+1}$ hatványokat, a skatulyaelv szerint van köztük kettő, amely azonos maradékosztályba esik, azaz van olyan $n + 1 \geq \alpha_1 > \alpha_2$ természetes számpár, hogy

$$a^{\alpha_1} \equiv a^{\alpha_2} \pmod{n},$$

azaz

$$n | a^{\alpha_2}(a^{\alpha_1 - \alpha_2} - 1).$$

De a maradékot $(\text{mod } n)$ legalább $2(n + 1)$ prím ad, tehát van ezek között olyan, amely n -hez relatív prím, azaz $(a, n) = 1$.

Így csakis $n | a^{\alpha_1 - \alpha_2} - 1$ lehet, azaz $a^\alpha \equiv 1 \pmod{n}$, $n \geq \alpha = \alpha_1 - \alpha_2 \geq 1$ (egész) mellett.

c) Legyen a legkisebb ilyen α kitevő az r (ilyen létezik, mert $\alpha \leq n$ miatt az ilyen α számok véges sokan vannak). Ekkor

$$P = p_{i_1} p_{i_2} \dots p_{i_r} = a^r \equiv 1 \pmod{n},$$

tehát $P \in V_n$. P a V_n -ben felbonthatatlan, mert 1-től és P -től különböző osztói $p_{j_1} p_{j_2} \dots p_{j_1} \equiv a^i \pmod{n}$, de r minimális volta miatt $a^i \not\equiv 1 \pmod{n}$, tehát a felírt szorzat nem eleme V_n -nek, így az egyetlen lehetséges felbontás $1 \cdot P$ lenne, de $1 < 1 + mn$ ($mn = 1, 2, \dots$) miatt $1 \notin V_n$. Mivel a $a \not\equiv 1 \pmod{n}$, ezért $r > 1$.

Válasszunk két V_n feletti felbonthatatlan számot:

$$P = p_1 p_2 \dots p_r, \quad Q = q_1 q_2 \dots q_r,$$

akkor $PQ \in V_n$ és

$$PQ = p_1 p_2 \dots p_r q_1 q_2 \dots q_r = q_1 q_2 \dots q_r p_1 p_2 \dots p_r = P' Q'.$$

($P' = q_1 p_2 \dots p_r$, $Q' = p_1 q_2 \dots q_r$), $r > 1$ miatt $P' \neq P$, $Q' \neq Q$. Az előbb láttuk hogy P' és Q' V_n -ben felbonthatatlan, így beláttuk a feladat állítását.

¹ A megoldás megszövegezése helyenként nem elég csiszolt, de ez érthető is. A rövid versenyidő nem ad lehetőséget arra, hogy a megoldók gondolataikat szépen fogalmazzák meg. Az értékelésnél itt az ötletek szépségét és egyszerűségét jutalmazták a bírálók. (A szerk.)