

**I. megoldás.** Mivel a 71 prímszám, Wilson tétele szerint (lásd pl. Freud R. – Gyarmati E. *Számelmélet* c. egyetemi tankönyvét)  $70! + 1$  osztható 71-gyel. Elegendő tehát azt megmutatni, hogy  $61!$  ugyanazt a maradékot adja 71-gyel osztva, mint  $70!$ . Vizsgáljuk meg ennek megfelelően az  $A = 62 \cdot 63 \cdot \dots \cdot 70$  szorzatot.

$$\begin{aligned} A &\equiv (71 - 9) \cdot (71 - 8) \cdot (71 - 7) \cdot \dots \cdot (71 - 1) \equiv (-9) \cdot (-8) \cdot (-7) \cdot \dots \cdot (-1) = \\ &= 72 \cdot (-7!) \equiv -7! = -70 \cdot 72 \equiv 1 \pmod{71}, \end{aligned}$$

vagyis  $70! = A \cdot 61! \equiv 61! \pmod{71}$ , amit bizonyítani akartunk.

*Megjegyzés.* A beérkezett megoldások két csoportba sorolhatók: a Wilson tételt használókra és azokra, amelyekben a  $61!$  maradékát több lépésben számolták ki. Az utóbbi megoldásnak az az előnye, hogy az összes olyan  $n$  számot megadhatja, amelyre 71 osztója  $n! + 1$ -nek. Ezek az  $n$  értékek a 7, 9, 19, 51, 61, 63. Ezt Bartha Ágnes, Birkner Tamás, Haszpra Tímea és Visnovitz Ferenc ki is emelték dolgozatukban.

**II. megoldás.** Számoljuk ki, hogy mely  $n$  számokra osztható 71-gyel az  $n! + 1$  ( $n$  pozitív egész). Az  $n!$  osztási maradékát,  $r_n$ -t az  $(n-1)!$  osztási maradékából,  $r_{n-1}$ -ből a következőképpen kaphatjuk meg:  $r_n = r_{n-1} \cdot n - 71 \left[ \frac{r_{n-1} \cdot n}{71} \right]$ , ahol  $[x]$  az  $x$  szám egész részét jelöli.

$n$	0	1	2	3	4	5	6	<b>7</b>	8	<b>9</b>	...	<b>19</b>	...	<b>51</b>	...	<b>61</b>	62	<b>63</b>
$r_n$	1	1	2	6	24	49	10	<b>70</b>	63	<b>70</b>	...	<b>70</b>	...	<b>70</b>	...	<b>70</b>	9	<b>70</b>

A 71-gyel osztva 70 maradékot adó számokhoz 1-et adva 71-gyel osztható számokat kapunk. Ezek a megjegyzésben már említett számok, közöttük az utolsó előtti a 61. Ezzel feladatunk állítását is beláttuk.