

Jelölje $f(x)$ az $x^3 - 3x^2 + 1$ polinomot, ekkor $f(2/3) < 0 < f(0)$, és Bolzano tétele alapján f -nek van egy α_2 gyöke a $(0; 2/3)$ intervallumban. Nyilván $f(x) - f(-x) = 2x^3$, vagyis $f(-\alpha_2) < 0 < f(0)$, tehát ismét Bolzano tétele miatt f -nek van egy α_1 gyöke a $(-\alpha_2; 0)$ intervallumban. Végezetül $f(2) < 0 < f(3)$, és Bolzano tétele alapján f -nek van egy α_3 gyöke a $(2; 3)$ intervallumban. Így azt kaptuk, hogy f -nek három valós gyöke van: $\alpha_1 < \alpha_2 < \alpha_3$, tehát $\alpha = \alpha_3$. Jelöljük S_n -nel a gyökök n -edik hatványösszegét (n nemnegatív egész), azaz

$$S_n = \alpha_1^n + \alpha_2^n + \alpha_3^n.$$

Nyilván $s_0 = 3$. A harmadfokú polinomokra vonatkozó Viète-formulák szerint

$$\alpha_1 + \alpha_2 + \alpha_3 = 3 \text{ és } \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = 0,$$

ezen alapján könnyen kapjuk, hogy $s_1 = 3$, és $s_2 = 9$. Tetszőleges $n \geq 3$ egész mellett érvényes az $S_n = \sum \alpha_i^n = \sum \alpha_i^{n-3} \alpha_i^3 = \sum \alpha_i^{n-3} (3\alpha_i^2 - 1) = \sum 3\alpha_i^{n-1} - \alpha_i^{n-3} = 3s_{n-1} - s_{n-3}$

összefüggés, amiből azonnal következik, hogy az s_n -ek mind egészek. Tudjuk, hogy $|\alpha_1| < |\alpha_2| < 2/3, \alpha_1 < 0 < \alpha_2$, vagyis minden $n \geq 2$ egészre

$$\alpha^n < s_n < \alpha^n + 2 \cdot (2/3)^n < \alpha^n + 1, \quad \text{azaz}$$

$$s_n - 1 < \alpha^n < s_n, \quad \text{illetve}$$

$$[\alpha^n] = s_n - 1, \quad \text{hiszen } s_n \text{ egész.}$$

Mindezek alapján a bizonyítandó összefüggés egyenértékű a

$$(1) \quad s_{1993} \equiv 5 \pmod{17}$$

állításal. (1) szerint $s_{0,1,2}$ -ből kiindulva sorra meghatározhatjuk az $s_n \pmod{17}$ maradékait. Kis számolással kapjuk, hogy

$$s_3 \equiv 7, s_4 \equiv 1, s_5 \equiv -6, s_6 \equiv -8, s_7 \equiv -8, s_8 \equiv -1,$$

$$s_9 \equiv 5, s_{10} \equiv 6, s_{11} \equiv 2, s_{12} \equiv 1, s_{13} \equiv -3, s_{14} \equiv 6,$$

$$s_{15} \equiv 0, s_{16} \equiv 3, s_{17} \equiv 3, s_{18} \equiv 9 \quad \pmod{17}$$

Az utolsó három kongruenciát másképpen írva

$$s_{16} \equiv s_0, s_{17} \equiv s_1, s_{18} \equiv s_2, \quad \pmod{17}$$

összefüggést, ami azt jelenti, hogy $s_n \pmod{17}$ maradéka $n \pmod{16}$ maradékától függ. Mivel $1993 \equiv 9 \pmod{16}$, azért

$$s_{1993} \equiv s_9 \equiv 5 \pmod{17},$$

tehát (2)-t beláttuk.