I. megoldás. Az x^3-x-1 polinomnak három különböző komplex gyöke van, α, β és γ (ezek közül pontosan egy valós); ez például a szokásos függvényvizsgálattal könnyen igazolható. Ismeretes, hogy ekkor alkalmas A, B, C (komplex) konstansokkal $a_n=A\alpha^n+B\beta^n+C\gamma^n$ ($n=0,\ 1,\ 2,\ \dots$). Az A, B, C értékét a sorozat első három tagja egyértelműen meghatározza. Esetünkben $A=B=C=1$, hiszen a gyökök és együtthatók összefüggéseiből $\alpha+\beta+\gamma=0=a_1$, $\alpha^2+\beta^2+\gamma^2=(\alpha+\beta+\gamma)^2-2(\alpha\beta+\beta\gamma+\gamma\alpha)=0^2-2(-1)=2=a_2$, és persze $\alpha^0+\beta^0+\gamma^0=3=a_0$. Tehát

$$a_n=\alpha^n+\beta^n++\gamma^n \qquad (n=0,\ 1,\ 2,\dots). \tag{1}$$

Felhasználva, hogy α, β, γ kielégíti az $x^3=x+1$ egyenletet (1)-ből kapjuk, hogy

$$a_{3n}=(\alpha+1)^n+(\beta+1)^n+(\gamma+1)^n=\sum_{k=0}^{n}\binom{n}{k}\left(\alpha^k+\beta^k+\gamma^k\right)=\sum_{k=0}^{n}\binom{n}{k}a_k(1)sa_n=(\alpha^3-1)^n+(\beta^3-1)^n+(\gamma^3-1)^n=\sum_{t=0}^{n}(-$$

Tetszőleges p prímre és $1\le r\le p-1$ egészre $\binom{p}{r}=\dfrac{p(p-1)\dots(p-r+1)}{r!}$ osztható p-vel; ezért (2) szerint

$$a_p\equiv a_0+(-1)^p a_{3p}\equiv a_0+(-1)^p(a_0+a_p)\pmod p.$$

Így $p>2$-re $a_p\equiv -a_p\pmod p$, azaz $p\mid 2a_p$. adódik, amiből következik a feladat állítása.

II. megoldás. Legyen n pozitív egész; írjunk bele egy körbe egy szabályos (konvex) $A_1A_2\dots A_n$ n-szöget (itt és a továbbiakban is megengedve az elfajuló „1- és 2-szög” esetét is). Jelölje b_n azoknak a konvex sokszögeknek a számát, amelyek csúcsai A_1, A_2, $\dots$, A_n közül valók, és bármely két szomszédos csúcsuk az eredeti $A_1A_2\dots A_n$ sokszögben másod- vagy harmadszomszédos (egy vagy két eredeti csúcspont esik közéjük). Megmutatjuk, hogy $b_n=a_n$ ($n=1$, $2,\ \dots$). Nyilván $b_1=0=a_1$, $b_2=2=a_2$, $b_3=3=a_3$; elegendő tehát igazolni a $b_n=b_{n-2}+b_{n-3}$ rekurziót ($n\ge 4$). Tekintsünk egy tetszőleges, a kívánalmaknak eleget tevő sokszöget; A_n, A_{n-1} és A_{n-2} valamelyike biztosan előfordul ennek csúcsaként, ezért e sokszög két legnagyobb sorszámú csúcsa a következő lehet:

2(1)	A_n és A_{n-2};	(4)	A_n és A_{n-3};
(2)	A_{n-1} és A_{n-3};	(5)	A_{n-1} és A_{n-4};
(3)	A_{n-2} és A_{n-4};	(4)	A_{n-2} és A_{n-5}.

Ha e két csúcsot egymással és a köztük fekvő eredeti csúcspontokkal egybeejtjük („összehúzzuk”), majd a csúcsok számozását folyamatosan változtatjuk, akkor az (1), (2) és (3) esetben az $n-2$, míg a (4), (5), ill. (6) esetben az $n-3$ oldalú szabályos sokszögbe írt megfelelő sokszöghöz jutunk. Utóbbi sokszögek valamennyien elő is fordulnak – mégpedig pontosan egyszer – ezen a módon, így valóban $b_n=b_{n-2}+b_{n-3}$, tehát $b_n=a_n$.

Legyen ezután $n=p$ prím. Ha S egy megfelelően beírt sokszög, akkor ennek a kör középpontja körüli $\dfrac{360^\circ}{p}i$-vel való elforgatottjai ($i=1,\ 2,\ \dots,\ p$) is megfelelőek. Ezek páronként különbözők, hiszen ha lenne közöttük két megegyező, akkor S-et valamilyen $\dfrac{360^\circ}{p}\cdot t$ fokos forgatás önmagába vinné ($1\le t\le p-1$). Ekkor azonban a $\dfrac{360^\circ}{p}tj$ fokos forgatások is önmagába viszik S-et ($j=1,\ 2,\ \dots,\ p-1$), és e forgatások között ott van a $\dfrac{360}{p}$ fokos is; ez a forgatás viszont láthatóan nem viheti S-et önmagába.

Tehát a feltételeknek megfelelően beírt a_p darab sokszög p-s csoportokba osztható, azaz $p\mid a_p$.

Frenkel Péter (Fazekas M. Főv. Gyak. Gimn., III. o.t.)