# 4. soutěžní série – řešení

**1.** Počet šestiúhelníků $(2n+1)^2 - 1 = 4n(n+1)$ je násobkem tří pro $n \equiv 0, 2 \pmod 3$, takže pokrytí neexistuje pro $n \equiv 1 \pmod 3$. Ukážeme, že pokrytí existuje pro $n \equiv 0, 2$. Útvar lze rozdělit na čtyři rovnoběžníky $n \times (n+1)$. Protože rovnoběžník $2 \times 3$ lze pokrýt dvěma triminy, lze pokrýt i každý rovnoběžník s jednou stranou dělitelnou třemi a druhou dělitelnou dvěma (nazvěme je *dobré*). Pokud $3|n$ a $n+1$ je sudé, nebo pokud $3|(n+1)$ a $n$ je sudé, je rovnoběžník $n \times (n+1)$ dobrý. Pokud $3|n$ a $n+1$ je liché, lze rovnoběžník $n \times (n+1)$ rozdělit na dobré rovnoběžníky $n \times (n-3)$ a $n \times 4$. Pokud $3|(n+1)$ a $n$ je liché, jsou dobré rovnoběžníky $(n+1) \times 3$ a $(n+1) \times (n-3)$.

**2.** Dva body nestačí, pro libovolné dva body totiž najdeme bod, který má od obou racionální vzdálenost. Ukážeme, že tři body stačí. Zvolme libovolné dva body $P$ a $Q$, třetí bod budeme hledat například na přímce $PQ$. Jistě každá z racionálních kružnic (= kružnic s racionálním poloměrem) se středem $P$ má nejvýše dva průsečíky s každou racionální kružnicí se středem $Q$, tj. existuje jen spočetně mnoho bodů, které neleží ve sjednocení iracionálních množin $P$ a $Q$. Uvažume všechny racionální kružnice se středy v těchto bodech, těch je opět spočetně mnoho, a tedy i jejich průsečíků s přímkou $PQ$ je jen spočetně mnoho. Tj. na této přímce existuje bod $R$, který má od všech těchto bodů iracionální vzdálenost.

**3.** Ukážeme, že $d$ vyhovuje právě když je čtvercem. Nejprve si všimneme, že $d$ vyhovuje právě když $dn^2$ vyhovuje. Proto stačí ověřit square-free čísla $d$. Pro $d = 1$ lze uhodnout, že vyhovuje $k = 15$ a posloupnost $8, 1, 15, 10, 6, 3, 13, 12, 4, 5, 11, 14, 2, 7, 9$. Nechť máme $d > 1$ dělitelné prvočíslem $p$. Pokud bychom našli vyhovující $k$ a uspořádání $a_1 d, a_2 d, \ldots, a_k d$ (tj. $a_i d + a_{i+1} d$ jsou čtverce pro všechna $i = 1, \ldots, k-1$), pak z $p|d$ plyne $p^2 | a_i d + a_{i+1} d$. To znamená, že $a_i + a_{i+1} \equiv 0 \pmod p$, speciálně všechna $a_1, a_3, \ldots$ (resp. $a_2, a_4, \ldots$) jsou navzájem kongruentní modulo $p$. Pro $p = 2$ dostáváme, že $a_i$ jsou buď všechna sudá nebo všechna lichá, pro $p \geq 3$ dávají $a_i$ nejvýše dva zbytky modulo $p$, ale $k \geq 3$. Spor.

**4.** Nechť $x, y \in G$. Pak platí

$$xy\Phi(x)\Phi(y) = xy\Phi(xy) = \Phi(xy)xy = \Phi(x)\Phi(y)xy.$$

Protože $y\Phi(y) = \Phi(y)y$, je taky $\Phi(y)y^{-1} = y^{-1}\Phi(y)$, tedy platí

$$\begin{aligned} y\Phi(x)y^{-1} &= x^{-1}xy\Phi(x)y^{-1}\Phi(y)\Phi(y)^{-1} \\ &= x^{-1}xy\Phi(x)\Phi(y)y^{-1}\Phi(y)^{-1} \\ &= x^{-1}\Phi(x)\Phi(y)xyy^{-1}\Phi(y)^{-1} \\ &= \left(x^{-1}\Phi(x)\right)\left(\Phi(y)x\Phi(y)^{-1}\right). \end{aligned}$$

Nhradíme-li v této rovnosti $x$ za $x^{-1}$, pak invertováním dostaneme

$$\begin{aligned} y\Phi(x)y^{-1} &= \left(y\Phi(x^{-1})y^{-1}\right)^{-1} \\ &= \left(\Phi(y)x^{-1}\Phi(y)^{-1}\right)^{-1}\left(x\Phi(x^{-1})\right)^{-1} \\ &= \left(\Phi(y)x\Phi(y)^{-1}\right)\left(\Phi(x)x^{-1}\right) \\ &= \left(\Phi(y)x\Phi(y)^{-1}\right)\left(x^{-1}\Phi(x)\right). \end{aligned}$$

Tedy pro libovolné $x, y \in G$ komutuje $x^{-1}\Phi(x)$ s $\Phi(y)x\Phi(y)^{-1}$. Tedy, protože $\Phi$ je automorfisums, komutuje $x^{-1}\Phi(x)$ dokonce s $yxy^{-1}$ pro libovolné $x, y \in G$.

Zafixujme si nyní $x$. Pokud $x = e$ (kde jako $e$ značíme neutrální prvek), pak určitě $\Phi(x) = x$. Dále nechť $x \neq e$. Podgrupa $G$ generovaná všemi prvky tvaru $yxy^{-1}$ je normální, tedy díky $x \neq e$ se musí jednat o celou $G$ (jinak by $G$ nebyla jednoduchá). Centrum $G$ (tj. množina prvků $G$, které komutují se všemi prvky $G$) je komutativní normální podgrupa, tedy (protože $G$ není komutativní, ale je jednoduchá), musí být rovno $\{e\}$. Ale protože $x^{-1}\Phi(x)$ komutuje se všemi $yxy^{-1}$ a ty generují $G$, komutuje $x^{-1}\Phi(x)$ se všemi prvky $G$, čili leží v centru $G$, čili v $\{e\}$. Takže $x^{-1}\Phi(x) = e$, neboli $x = \Phi(x)$.