$p$ zafixované prvočíslo

**Přípravné lemma:** $\forall a,b\in\mathbb{Z}\ \forall n\in\mathbb{N}:\ a\equiv b \pmod{p^n} \Rightarrow a^p\equiv b^p \pmod{p^{n+1}}$

Dk. $n\in\mathbb{N} \Rightarrow a\equiv b \pmod p$

$$a^p-b^p=\underbrace{(a-b)}_{p^n\mid\dots}\underbrace{(a^{p-1}+a^{p-2}\cdot b+a^{p-3}b^2+\dots+ab^{p-2}+b^{p-1})}_{\dots\equiv p\cdot a^{p-1}\equiv 0 \pmod p}\equiv 0 \pmod{p^{n+1}}$$

Okruh $\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z}$

pro každé $n\in\mathbb{N}$ máme spojitou projekci $\pi_n:\mathbb{Z}_p\longrightarrow\mathbb{Z}/p^n\mathbb{Z}$, což je homomorfismus okruhů.

Systém $\ker\pi_n$ je bází otevřených okolí nuly v $\mathbb{Z}_p$. Průnik $\bigcap_{n=1}^{\infty}\ker\pi_n=\{0\}$.

1) Grupa jednotek okruhu $\mathbb{Z}_p$ je $\mathbb{Z}_p^\times=\mathbb{Z}_p-\ker\pi_1$

Dk. Nechť $a=([a_n]_{p^n})_{n=1}^{\infty}\in\mathbb{Z}_p$.
Je-li $a\in\mathbb{Z}_p^\times$, existuje $b=([b_n]_{p^n})_{n=1}^{\infty}\in\mathbb{Z}_p$ tak, že $a\cdot b=1$. Pak $\pi_1(a)\cdot\pi_1(b)=\pi_1(1)$, tj. $[a_1]_p\cdot[b_1]_p=[1]_p$, odkud $p\nmid a_1$. Proto $a\notin\ker\pi_1$.
Nechť nyní $a\notin\ker\pi_1$. Pak $[a_1]_p\neq[0]_p$, tj. $p\nmid a_1$. Z kompatibility prvku $a$ plyne, že pro každé $k\in\mathbb{N}$ je $a_k\equiv a_1\not\equiv 0 \pmod p$, proto $p\nmid a_k$ a kongruence $a_k\cdot x\equiv 1 \pmod{p^k}$ má řešení $b_k\in\mathbb{Z}$. Ukažme, že $([b_k]_{p^k})_{k=1}^{\infty}\in\mathbb{Z}_p$, tj. že platí pro každé $k\in\mathbb{N}$: $b_{k+1}\equiv b_k \pmod{p^k}$.
Platí $a_k\cdot b_{k+1}\equiv a_{k+1}\cdot b_{k+1}\equiv 1\equiv a_k\cdot b_k \pmod{p^k}$. Protože $(a_k,p^k)=1$, dostáváme $b_{k+1}\equiv b_k \pmod{p^k}$. Jistě $a\cdot b=1$.

2) Po ztotožnění je $\mathbb{Z}$ podokruhem $\mathbb{Z}_p$.

Dk. Jediný homomorfismus $\mathbb{Z}\to\mathbb{Z}_p$ je dán předpisem $m\longmapsto([m]_{p^n})_{n=1}^{\infty}\in\mathbb{Z}_p$ pro každé $m\in\mathbb{Z}$. Je-li $m\neq 0$, existuje $k\in\mathbb{Z}$, že $p^k\nmid m$, tj. $[m]_{p^k}\neq[0]_{p^k}$, proto tento homomorfismus je prostý. Proto char $\mathbb{Z}_p=0$ a (po ztotožnění) dostáváme dokazované.

3) Každé $a\in\mathbb{Z}_p$, $a\neq 0$, je tvaru $a=p^n\cdot e$, kde $n\in\mathbb{N}\cup\{0\}$, $e\in\mathbb{Z}_p^\times$.

Dk. Protože $a\notin\bigcap_{n=1}^{\infty}\ker\pi_n$, existuje $n\in\mathbb{N}\cup\{0\}$ tak, že $a\in\ker\pi_n$, $a\notin\ker\pi_{n+1}$ (kde $\pi_0:\mathbb{Z}_p\to\mathbb{Z}/\mathbb{Z}$ je konstantní zobrazení do triviálního okruhu, tj. $\ker\pi_0=\mathbb{Z}_p$).
Nechť $a=([a_n]_{p^n})_{n=1}^{\infty}\in\mathbb{Z}_p$. Protože $a\in\ker\pi_n$, platí $[a_n]_{p^n}=[0]_{p^n}$, tj. $a_n\equiv 0 \pmod{p^n}$, z kompatibility dostáváme pro každé $k\in\mathbb{N}$
$a_{n+k}\equiv a_k\equiv 0 \pmod{p^n}$. Podobně z $a\notin\ker\pi_{n+1}$ plyne $[a_{n+1}]_{p^{n+1}}\neq[0]_{p^{n+1}}$, tedy $a_{n+1}\not\equiv 0 \pmod{p^{n+1}}$, proto pro každé $k\in\mathbb{N}$ je $a_{n+k}\equiv a_{n+1}\not\equiv 0 \pmod{p^{n+1}}$.
Označme $b_k=\dfrac{a_{n+k}}{p^n}$, pak $b_k\in\mathbb{Z}$ a $p\nmid b_k$. Pro každé $k\in\mathbb{N}$ tedy

$a_{n+k+1} \equiv a_{n+k} \pmod{p^{n+k}}$. Dělíme $p^n$, dostaneme $b_{k+1} \equiv b_k \pmod{p^k}$.
Tedy $b = \left([b_k]_{p^k}\right)_{k=1}^{\infty} \in \mathbb{Z}_p$. Protože $p^n \cdot b_k = a_{n+k} \equiv a_k \pmod{p^k}$, platí $p^n \cdot b = a$. Platí $\pi_1(b) = [b_1]_p \neq [0]_p$, tj. $b \in \mathbb{Z}_p^\times$ dle 1).

4) <u>$\mathbb{Z}_p$ je obor integrity.</u>

Dk. Víme, že $\mathbb{Z}_p$ je komutativní a netriviální okruh. Ukážeme, že nemá dělitele nuly. Stačí ukázat, že $p$ není dělitel nuly: nechť $a \in \mathbb{Z}_p$, $a \neq 0$, ukážeme, že $p \cdot a \neq 0$. Existuje $n \in \mathbb{N} \cup \{0\}$ tak, že $a = e \cdot p^n$ pro $n \in \mathbb{N} \cup \{0\}$, $e \in \mathbb{Z}_p^\times$.
Pak $e = \left([e_k]_{p^k}\right)_{k=1}^{\infty}$, $p \nmid e_1$, z kompatibility $p \nmid e_{n+2}$. Pak
$\pi_{n+2}(p \cdot a) = \pi_{n+2}(p^{n+1} \cdot e) = [p^{n+1}]_{p^{n+2}} \cdot [e_{n+2}]_{p^{n+2}} = [p^{n+1} \cdot e_{n+2}]_{p^{n+2}} \neq [0]_{p^{n+2}}$.
Proto $p \cdot a \neq 0$.
Jsou-li $a, b \in \mathbb{Z}_p$, $a \neq 0$, $b \neq 0$, pak $a = p^n \cdot e$, $b = p^m \cdot f$ pro $n, m \in \mathbb{N} \cup \{0\}$, $e, f \in \mathbb{Z}_p^\times$. Pak $a \cdot b = p^{n+m} \cdot e \cdot f \neq 0$, neboť $p$ není dělitel nuly.

5) <u>$\ker \pi_n = p^n \cdot \mathbb{Z}_p = \{p^n \cdot a;\ a \in \mathbb{Z}_p\}$ pro každé $n \in \mathbb{N}$</u>

Dk. Postupem analogickým důkazu 3) lze odvodit, že pro každé $a \in \ker \pi_n$ existuje $b \in \mathbb{Z}_p$ tak, že $a = p^n . b$. Naopak zřejmě $\pi_n(p^n \cdot b) = \pi_n(p^n) \cdot \pi_n(b)$, přičemž $\pi_n(p^n) = [p^n]_{p^n} = [0]_{p^n}$, tj. $p^n \cdot b \in \ker \pi_n$.

6) <u>Okruh $\mathbb{Z}_p$ je okruh s jednoznačným rozkladem, který má (až na asociovanost) jediný ireducibilní prvek, totiž $p$.</u> (Je tedy $\mathbb{Z}_p$ okruh diskrétní valuace, anglicky discrete valuation ring, zkráceně DVR.)

Dk. Plyne z 4). Každé $a \in \mathbb{Z}_p$, $a \neq 0$, $a \notin \mathbb{Z}_p^\times$ lze podle 3) psát ve tvaru $a = p^n \cdot e$, kde $n \in \mathbb{N}$, tj. $a = (p \cdot e) \cdot p \cdot \ldots \cdot p$. Ukážeme, že $p$ je ireducibilní prvek v $\mathbb{Z}_p$. Jsou-li $r, s \in \mathbb{Z}_p$ takové, že $r \cdot s = p$, pak $r \neq 0$, $s \neq 0$, tedy podle 3 platí $r = p^n \cdot e$, $s = p^m \cdot f$, $n, m \in \mathbb{N} \cup \{0\}$, $e, f \in \mathbb{Z}_p^\times$, tj.
$p^{n+m} \cdot ef = p$, tedy z $p \notin \mathbb{Z}_p^\times$ dle 1) plyne $n+m \geq 1$, zkrácením dle 4
$p^{n+m-1} \cdot ef = 1$, tj. $p^{n+m-1} \in \mathbb{Z}_p^\times$, odkud dle 1) $p \nmid p^{n+m-1}$, tj.
$n+m-1 = 0$, tj. $n+m = 1$, odtud $n = 0$ nebo $m = 0$, proto $r \in \mathbb{Z}_p^\times$ nebo $s \in \mathbb{Z}_p^\times$.
Ukážeme jednoznačnost rozkladu. Nechť $t$ je libovolný ireducibilní prvek v $\mathbb{Z}_p$. Víme, že $t = (p \cdot e) \cdot p \ldots p$, z ireducibility $t$ plyne $t = p \cdot e$ je asociovaný s $p$.
Pro jednoznačnost rozkladu stačí ověřit, že pro každé $a \in \mathbb{Z}_p$, $a \neq 0$, $a \notin \mathbb{Z}_p$ je zápis $a = p^n \cdot e$ jednoznačný ($n \in \mathbb{N}$, $e \in \mathbb{Z}_p^\times$). Předpokládejme, že $a = p^n \cdot e = p^m \cdot f$, kde $n, m \in \mathbb{N}$, $e, f \in \mathbb{Z}_p^\times$, $n \geq m$. Pak dle 4) je $p^{n-m} \cdot e = f$, opakováním předchozí úvahy z $p^{n-m} \in \mathbb{Z}_p^\times$ plyne $n - m = 0$.
Proto $n = m$, $e = f$.

7) Uzavřené podgrupy grupy $(\mathbb{Z}_p,+)$ jsou právě $p^n\mathbb{Z}_p$ pro $n\in\mathbb{N}\cup\{0\}$ a podgrupa $\{0\}$. Přitom podgrupy $p^n\mathbb{Z}_p$ jsou též otevřené, kdežto $\{0\}$ není.

Dk. Z 5) víme, že vyjmenované podgrupy mají uvedené vlastnosti. Zbývá dokázat, že jiné uzavřené podgrupy grupa $(\mathbb{Z}_p,+)$ už nemá. Nechť $H\neq\{0\}$ je uzavřená podgrupa grupy $(\mathbb{Z}_p,+)$. Podle 3) každé $a\in H$, $a\neq 0$ je tvaru $a=p^n\cdot e$, $n\in\mathbb{N}\cup\{0\}$, $e\in\mathbb{Z}_p^\times$. Nechť $m$ značí nejmenší z těchto exponentů $n$ pro všechna $a\in H$, $a\neq 0$. Zvolme $a\in H$, $a=p^m e$, $e\in\mathbb{Z}_p^\times$. Ukažme, že $H=p^m\mathbb{Z}_p$. Z volby $m$ plyne $H\subseteq p^m\mathbb{Z}_p$. Pro důkaz opačné inkluze zvolme libovolně $b\in p^m\mathbb{Z}_p$. Tedy $b=([b_n]_{p^n})_{n=1}^\infty$, přitom pro každé $n\geq m$ platí $b_n\equiv 0 \pmod{p^m}$. Protože $H$ je uzavřená podgrupa, stačí ukázat, že v každém otevřeném okolí čísla $b$ leží nějaký prvek z $H$. Ukažme, že pro každé $k\in\mathbb{N}$ leží v $b+p^k\mathbb{Z}_p$ nějaký prvek z $H$. Postačí to ukázat pro $k\geq m$, takto prvek z $H$ hledejme ve tvaru $x\cdot a$ pro nějaké $x\in\mathbb{Z}$. Přitom $x\cdot a\in b+p^k\mathbb{Z}_p$ je ekvivalentní s $\pi_k(x\cdot a-b)=[0]_{p^k}$. Víme, že $a=p^m e$, $e\in\mathbb{Z}_p^\times$. Pak $e=([e_n]_{p^n})_{n=1}^\infty$, pak $\pi_k(a)=[p^m\cdot e_k]_{p^k}$, $p\nmid e_k$. $\pi_k(x\cdot a-b)=[x\cdot p^m\cdot e_k-b_k]_{p^k}$. Potřebujeme, aby $x\cdot p^m e_k\equiv b_k \pmod{p^k}$. Takové $x\in\mathbb{Z}$ existuje, právě když $(p^m\cdot e_k,p^k)\mid b_k$. Přitom $(p^m\cdot e_k,p^k)=p^m$ a $p^m\mid b_k$. Proto takové $x\in\mathbb{Z}$ existuje. V libovolném otevřeném okolí čísla $b$ leží nějaký prvek podgrupy $H$, proto $b\in\overline{H}=H$.

8) Algebraicky i topologicky platí $\mathbb{Z}_p^\times=\varprojlim(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Protože $[a_n]_{p^n}\in(\mathbb{Z}/p^n\mathbb{Z})^\times$ právě když $p\nmid a_n$, plyne tato rovnost z 1). Ukažme, že topologie $\mathbb{Z}_p^\times$ získaná jako topologie podprostoru $\mathbb{Z}_p$ je stejná jako topologie pocházející z inverzní limity. Porovnejme báze okolí 1. V $\mathbb{Z}_p$ to jsou otevřená okolí $1+p^n\mathbb{Z}_p$, $n\in\mathbb{N}$. V inverzní limitě to jsou jádra homomorfismů $\mathbb{Z}_p^\times\to(\mathbb{Z}/p^n\mathbb{Z})^\times$, tj. opět $1+p^n\mathbb{Z}_p$.

9) Je-li $p\neq 2$, pak $\mathbb{Z}_p^\times$ obsahuje cyklickou podgrupu $\Delta_p$ řádu $p-1$. V případě $p=2$ obsahuje $\mathbb{Z}_2^\times$ cyklickou podgrupu $\Delta_2=\{1,-1\}$ řádu 2.

Dk. Druhé tvrzení je zřejmé, nechť $p\neq 2$. Pro libovolné $c\in\{1,2,\dots,p-1\}$ označme $\alpha_c=([c^{p^{n-1}}]_{p^n})_{n=1}^\infty$. Ukažme, že $\alpha_c\in\mathbb{Z}_p$. Z malé Fermatovy věty plyne

$c^p \equiv c \pmod p$. Indukcí užitím připraveného lemmatu $c^{p^n} \equiv c^{p^{n-1}} \pmod{p^n}$ pro každé $n \in \mathbb{N}$. Proto $\alpha_c \in \mathbb{Z}_p$. Z Eulerovy věty $(c^{p^{n-1}})^{p-1} \equiv 1 \pmod{p^n}$, tedy $\alpha_c^{p-1} = 1$. Protože $\pi_1(\alpha_c) = [c]_p$, jsou $\alpha_1, \dots, \alpha_{p-1}$ po dvou různé.

Označme $\Delta_p = \{\alpha_1, \dots, \alpha_{p-1}\}$ a ukažme, že jde o podgrupu grupy $\mathbb{Z}_p^\times$. Jistě $\Delta_p \subseteq \mathbb{Z}_p^\times$. Pro libovolná $c, d \in \{1, \dots, p-1\}$ existuje $f \in \{1, \dots, p-1\}$ tak, že $c \cdot d \equiv f \pmod p$. Pak indukcí užitím připraveného lemmatu dostáváme $c^{p^{n-1}} \cdot d^{p^{n-1}} \equiv f^{p^{n-1}} \pmod{p^n}$, a tedy $\alpha_c \cdot \alpha_d = \alpha_f$. Proto $\Delta_p$ je uzavřené na násobení, a proto i na inverzní prvky, jde tedy o podgrupu grupy $\mathbb{Z}_p^\times$. Protože $\mathbb{Z}_p$ je obor integrity dle 4), je $\Delta_p$ podgrupou multiplikativní grupy podílového tělesa oboru $\mathbb{Z}_p$, a tedy je $\Delta_p$ cyklická.

10) Je-li $p \neq 2$, pak $\mathbb{Z}_p^\times = \Delta_p \cdot (1 + p\mathbb{Z}_p)$ je přímý součin podgrup.
Je-li $p = 2$, pak $\mathbb{Z}_2^\times = \Delta_2 \cdot (1 + 4\mathbb{Z}_2)$ je přímý součin podgrup
(tj. každý prvek ze $\mathbb{Z}_p^\times$ lze jediným způsobem psát jako součin prvků zmíněných podgrup). Tyto rovnosti platí i topologicky.

Dk. Využijeme bodu 1). Protože $\pi_1(\alpha_c) = [c]_p$, tak $\alpha_c \cdot (1 + p\mathbb{Z}_p) = c + p\mathbb{Z}_p$, neboť $1 + p\mathbb{Z}_p = \ker(\mathbb{Z}_p^\times \to (\mathbb{Z}/p\mathbb{Z})^\times)$. Zřejmě $\bigcup_{c=1}^{p-1} (c + p\mathbb{Z}_p) = \mathbb{Z}_p^\times$.
Protože $\Delta_p \cap (1 + p\mathbb{Z}_p) = \{1\}$, je část pro $p \neq 2$ dokázána.
Analogicky pro $p = 2$ je $\mathbb{Z}_2^\times = (1 + 4\mathbb{Z}_2) \cup (3 + 4\mathbb{Z}_2)$, $(3 + 4\mathbb{Z}_2) = (-1) \cdot (1 + 4\mathbb{Z}_2)$, neboť $1 + 4\mathbb{Z}_2 = \ker(\mathbb{Z}_2^\times \to (\mathbb{Z}/4\mathbb{Z})^\times)$.
Podobně $\{1, -1\} \cap (1 + 4\mathbb{Z}_2) = \{1\}$.
Protože $\Delta_p$ je konečná podgrupa, má diskrétní topologii. Navíc množiny $c + p\mathbb{Z}_p$, resp. $1 + 4\mathbb{Z}_2$ a $3 + 4\mathbb{Z}_2$, jsou otevřené, neboť podgrupy $1 + p\mathbb{Z}_p$ a $1 + 4\mathbb{Z}_2$ jsou otevřené.

11) Je-li $p \neq 2$, pak $(1 + p\mathbb{Z}_p, \cdot) \cong (\mathbb{Z}_p, +)$ algebraicky i topologicky.
Je-li $p = 2$, pak $(1 + 4\mathbb{Z}_2, \cdot) \cong (\mathbb{Z}_2, +)$ algebraicky i topologicky.

Dk. Indukcí z připraveného lemmatu lze pro $p \neq 2$ odvodit
$$(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \pmod{p^k} \quad \text{pro každé } k \geq 2.$$
Proto řád $[1+p]_{p^k}$ v grupě $(\mathbb{Z}/p^k\mathbb{Z})^\times$ je $p^{k-1}$, je tedy $p$-Sylowská podgrupa této grupy rovna $\langle [1+p]_{p^k} \rangle$, a je izomorfní s $(\mathbb{Z}/p^{k-1}\mathbb{Z}, +)$. Jde o podgrupu těch tříd, které mají reprezentanta dávajícího zbytek 1

po dělení $p$.

$$(1+p\mathbb{Z}_p,\cdot) = \varprojlim (\langle [1+p]_{p^k} \rangle, \cdot) \cong \varprojlim (\mathbb{Z}/p^{k-1}\mathbb{Z}, +) = (\mathbb{Z}_p, +)$$

$$\left([(1+p)^{a_k}]_{p^k}\right)_{k=2}^{\infty} \longleftarrow\!\shortmid \left([a_k]_{p^{k-1}}\right)_{k=2}^{\infty}$$

(chybějící první člen podposloupnosti vlevo $[1]_p$, jeho absence nevadí)

Pro $p=2$ analogicky $5^{2^{k-3}} \equiv 1+2^{k-1} \pmod{2^k}$ pro $k \geq 3$

Podgrupa $\langle [5]_{2^k} \rangle \leq (\mathbb{Z}/2^k\mathbb{Z})^\times$ má řád $2^{k-2}$, jde o podgrupu těch tříd, které mají reprezentanty dávající zbytek 1 po dělení čtyřmi.

$$(1+4\mathbb{Z}_2, \cdot) = \varprojlim (\langle [5]_{2^k} \rangle, \cdot) \cong \varprojlim (\mathbb{Z}/2^{k-2}\mathbb{Z}, +) = (\mathbb{Z}_2, +)$$

$$\left([5^{a_k}]_{2^k}\right)_{k=3}^{\infty} \longleftarrow\!\shortmid \left([a_k]_{2^{k-2}}\right)_{k=3}^{\infty}$$

(absence prvních dvou členů $[1]_2$, $[1]_4$ nevadí).

12) <u>Každá uzavřená podgrupa grupy $\mathbb{Z}_p^\times$, která není otevřená, je konečná a je to podgrupa grupy $\Delta_p$. Naopak každá podgrupa grupy $\Delta_p$ je uzavřená a není otevřená.</u>

Dk Označme $H \leq \mathbb{Z}_p^\times$ podgrupu, která je uzavřená, ale není otevřená. Předpokládejme, že $p \neq 2$. Protože $1+p\mathbb{Z}_p$ je uzavřená podgrupa grupy $\mathbb{Z}_p^\times$, je $H \cap (1+p\mathbb{Z}_p)$ uzavřená podgrupa grupy $(1+p\mathbb{Z}_p, \cdot) \cong (\mathbb{Z}_p, +)$ podle 11. Podle bodů 7 a 11 je tedy $H \cap (1+p\mathbb{Z}_p)$ buď triviální podgrupa $\{1\}$ anebo otevřená podgrupa $1+p^n\mathbb{Z}_p$ pro vhodné $n \in \mathbb{N}$. Ve druhém případě však by měla $H$ otevřenou podgrupu $1+p^n\mathbb{Z}_p$, a tedy by 1 ležela v $H$ i se svým otevřeným okolím $1+p^n\mathbb{Z}_p$. Pak každý prvek grupy $H$ leží v $H$ se svým otevřeným okolím a tedy $H$ je otevřená množina, spor. Je tedy $H \cap (1+p\mathbb{Z}_p) = \{1\}$. Libovolný $a \in H$ je tvaru $a = d \cdot b$, kde $d \in \Delta_p$, $b \in 1+p\mathbb{Z}_p$ podle 10. Pak $a^{p-1} = d^{p-1} \cdot b^{p-1} = b^{p-1} \in (1+p\mathbb{Z}_p) \cap H = \{1\}$. Ovšem všech $p-1$ kořenů polynomu $x^{p-1}-1$ leží v $\Delta_p$. Proto $a \in \Delta_p$. Je tedy $H \leq \Delta_p$.

Je-li $p=2$, lze postupovat analogicky užitím $1+4\mathbb{Z}$ místo $1+p\mathbb{Z}_p$.

13) Je-li $p \neq 2$, pak libovolná otevřená podgrupa grupy $(\mathbb{Z}_p^\times, \cdot)$ je tvaru $H \cdot (1 + p^n \mathbb{Z}_p)$, kde $H \leq \Delta_p$ a $n \in \mathbb{N}$. Naopak každá taková podgrupa je otevřená.

Je-li $p = 2$, pak libovolná otevřená podgrupa grupy $(\mathbb{Z}_2^\times, \cdot)$ je tvaru buď $H \cdot (1 + 2^n \mathbb{Z}_2)$, kde $H \leq \Delta_2$ a $n \in \mathbb{N}, n \geq 2$, anebo tvaru $(1 + 2^n \mathbb{Z}_2) \cup ((2^{n-1} - 1) + 2^n \mathbb{Z}_2)$, kde $n \in \mathbb{N}$, $n \geq 3$. Naopak každá taková podgrupa je otevřená.

Dk. Nejprve nechť $p = 2$. Označme $L \leq \mathbb{Z}_2^\times$ libovolnou otevřenou podgrupu. Pak $L \cap (1 + 4\mathbb{Z}_2)$ je otevřená podgrupa grupy $1 + 4\mathbb{Z}_2$. Podle bodů 7 a 11 je $L \cap (1 + 4\mathbb{Z}_2) = 1 + 2^n \mathbb{Z}_2$ pro vhodné $n \in \mathbb{N}$, $n \geq 2$.
Je-li $n = 2$, pak $1 + 4\mathbb{Z}_2 \leq L \leq \mathbb{Z}_2^\times$. Protože $1 + 4\mathbb{Z}_2$ má index 2 v $\mathbb{Z}_2^\times$, a tedy buď $L = 1 + 4\mathbb{Z}_2$ anebo $L = \mathbb{Z}_2^\times = \Delta_2 \cdot (1 + 4\mathbb{Z}_2)$.
Je-li $n > 2$, pak platí $1 + 2^n \mathbb{Z}_2 \leq L$, $1 + 2^{n-1} \mathbb{Z}_2 \not\leq L$.
Protože $1 + 2^n \mathbb{Z}_2$ je jádro surjektivního homomorfismu $\pi_n : \mathbb{Z}_2^\times \to (\mathbb{Z}/2^n\mathbb{Z})^\times$, který je projekcí z inverzní limity z bodu 8. Proto podgrupa $L$ je úplný vzor podgrupy $\pi_n(L) \leq (\mathbb{Z}/2^n\mathbb{Z})^\times$ vůči $\pi_n$. Přitom $[1 + 2^{n-1}]_{2^n} \notin \pi_n(L)$. Je-li $\pi_n(L)$ triviální podgrupa, pak $L = 1 + 2^n \mathbb{Z}_2$.
Víme, že $(\mathbb{Z}/2^n\mathbb{Z})^\times = \langle [-1]_{2^n} \rangle \cdot \langle [5]_{2^n} \rangle$, tato grupa má právě tři prvky řádu 2, totiž $[-1]_{2^n}$, $[5^{2^{n-3}}]_{2^n} = [1 + 2^{n-1}]_{2^n}$, $[-1 + 2^{n-1}]_{2^n}$.
Jestliže $\pi_n(L)$ je netriviální, obsahuje alespoň jeden prvek řádu 2, ale ne všechny tři, protože neobsahuje prvek $[1 + 2^{n-1}]_{2^n}$. Proto obsahuje jediný prvek řádu 2, navíc z cyklické podgrupy $\langle [5]_{2^n} \rangle$ obsahuje jen neutrální prvek. Proto $\pi_n(L) = \{[1]_{2^n}, [-1 + 2^{n-1}]_{2^n}\}$ anebo $\pi_n(L) = \{[1]_{2^n}, [-1]_{2^n}\}$. Tím je dokázán případ $p = 2$.
Případ $p \neq 2$ je analogický a jednodušší, protože grupa

$$(\mathbb{Z}/p^n\mathbb{Z})^\times = \underbrace{\pi_n(\Delta_p)}_{\text{cykl. grupa řádu } p-1} \cdot \underbrace{\langle [1+p]_{p^n} \rangle}_{\text{cykl. grupa řádu } p^{n-1}}.$$

Protože $(p-1, p^{n-1}) = 1$, je každá podgrupa grupy $(\mathbb{Z}/p^n\mathbb{Z})^\times$ součinem podgrupy grupy $\pi_n(\Delta_p)$ a podgrupy grupy $\langle [1+p]_{p^n} \rangle$.