V následujícím textu užíváme označení: $\mathbb{Z}_n$ je množina všech zbytkových tříd modulo n, dále $(\mathbb{Z}_n^\times, \cdot)$ je grupa jednotek okruhu $(\mathbb{Z}_n, +, \cdot)$. Naším cílem je dokázat následující větu:

Věta. *Nechť $n \in \mathbb{N}$ je liché složené číslo, $N > 10$. Rozložme $N-1 = 2^t \cdot q$, kde $t, q \in \mathbb{N}$, $2 \nmid q$. Pak z množiny $\{a \in \mathbb{Z}; 0 \le a < N, (a, N) = 1\}$ nejvýše čtvrtina čísel splní podmínku*

$$a^q \equiv 1 \pmod N \quad \textit{nebo} \quad \exists e \in \{0, 1, \ldots, t-1\} : a^{2^e \cdot q} \equiv -1 \pmod N. \quad (1)$$

Nejdříve zformulujme několik tvrzení, která budou v důkaze věty užitečná:

1. Pro libovolná $u, v \in \mathbb{N}$, $(u, v) = 1$ předpis $[a]_{uv} \mapsto ([a]_u, [a]_v)$ pro libovolné $a \in \mathbb{Z}$ zadává korektně izomorfismus okruhů

   $$(\mathbb{Z}_{uv}, +, \cdot) \to (\mathbb{Z}_u, +, \cdot) \times (\mathbb{Z}_v, +, \cdot),$$

   a tedy i izomorfismus aditivních grup

   $$(\mathbb{Z}_{uv}, +) \to (\mathbb{Z}_u, +) \times (\mathbb{Z}_v, +)$$

   a izomorfismus multiplikativních grup jednotek

   $$(\mathbb{Z}_{uv}^\times, \cdot) \to (\mathbb{Z}_u^\times, \cdot) \times (\mathbb{Z}_v^\times, \cdot).$$

2. Jestliže $(G, \cdot)$ je komutativní grupa a $q \in \mathbb{N}$, pak zobrazení $f : G \to G$, dané předpisem $f(a) = a^q$ pro libovolné $a \in G$, je homomorfismus grup. Je-li navíc G konečná a její řád $|G|$ je nesoudělný s q, pak je f izomorfismus.

3. Je-li $f : G \to H$ homomorfismus grup, pak pro libovolné $a, b \in G$ platí $f(a) = f(b)$, právě když $a \cdot \ker f = b \cdot \ker f$. Proto index podgrupy $\ker f$ v grupě G je $|G/\ker f| = |f(G)|$, kde $f(G) = \{f(a); a \in G\}$. Je-li G konečná, tak každá třída rozkladu $G/\ker f$ má $|\ker f|$ prvků, a tedy na každý prvek $f(G)$ se zobrazí právě $|\ker f|$ prvků.

4. Každá konečná cyklická grupa $(G, \cdot)$ řádu m je izomorfní s grupou $(\mathbb{Z}_m, +)$.

5. Libovolná konečná cyklická grupa řádu 2^c, kde $c \in \mathbb{N}$, má 1 prvek řádu 1, 1 prvek řádu 2, 2 prvky řádu 4, 4 prvky řádu 8, …, 2^{c-1} prvků řádu 2^c.

6. Pro každé liché prvočíslo p a libovolné $n \in \mathbb{N}$ je grupa $(\mathbb{Z}_{p^n}^\times, \cdot)$ cyklická.

Důkaz věty. Rozložme $N = \prod_{i=1}^s p_i^{e_i}$, kde $p_1, \dots, p_s$ jsou různá lichá prvočísla, $e_1, \dots, e_s \in \mathbb{N}$. Pro každé $i = 1, \dots, s$ rozložme $p_i - 1 = 2^{t_i} \cdot q_i$, kde $t_i, q_i \in \mathbb{N}$, $2 \nmid q_i$. Máme následující izomorfismy grup

$$\begin{aligned}(\mathbb{Z}_N^\times, \cdot) &\cong \prod_{i=1}^s (\mathbb{Z}_{p_i^{e_i}}^\times, \cdot) \cong \prod_{i=1}^s (\mathbb{Z}_{(p_i-1)p_i^{e_i-1}}, +) \cong \\ &\cong \prod_{i=1}^s \big((\mathbb{Z}_{2^{t_i}}, +) \times (\mathbb{Z}_{q_i}, +) \times (\mathbb{Z}_{p_i^{e_i-1}}, +)\big) \cong (D, +) \times (L, +),\end{aligned}$$

kde $D = \prod_{i=1}^s \mathbb{Z}_{2^{t_i}}$, $L = \prod_{i=1}^s \big(\mathbb{Z}_{q_i} \times \mathbb{Z}_{p_i^{e_i-1}}\big)$.

Získaný izomorfismus pojmenujme $\psi : \mathbb{Z}_N^\times \to D \times L$. Nechť

$$\varphi : D \times L \to D \times L$$

je umocňování na q-tou (vzhledem k tomu, že operaci značíme aditivně, je asi lepší mluvit o násobení číslem q). Dále označme $\pi_D : D \times L \to D$ a $\pi_L : D \times L \to L$ projekce ze součinu.

Charakterizujme ta $a \in \mathbb{Z}$, $(a, N) = 1$, která splní podmínku (1). Jestliže a splní tuto podmínku, pak řád $[a^q]_N$ v grupě $(\mathbb{Z}_N^\times, \cdot)$ je mocnina dvou a navíc je roven řádu $[a^q]_{p_i^{e_i}}$ v grupě $(\mathbb{Z}_{p_i^{e_i}}^\times, \cdot)$ pro každé $i = 1, \dots, s$. Ekvivalentně to tedy můžeme popsat tak, že $[a]_N \in \ker(\pi_L \circ \varphi \circ \psi)$ a navíc každá z s složek $(\pi_D \circ \varphi \circ \psi)([a]_N)$ má stejný řád.

Ukažme, že zúžení homomorfismu $\pi_D \circ \varphi \circ \psi$ na podgrupu $\ker(\pi_L \circ \varphi \circ \psi)$ grupy $(\mathbb{Z}_N^\times, \cdot)$ je surjektivní. Protože q je liché, je násobení číslem q na grupě $(D, +)$ izomorfismus, a tedy pro každé $d \in D$ existuje $c \in D$ takové, že $qc = d$, kde qc znamená součet q kopií prvku c v grupě $(D, +)$. Protože ψ je izomorfismus, existuje $a \in \mathbb{Z}$, $(a, N) = 1$, tak, že $\psi([a]_N) = (c, 0)$, kde 0 znamená neutrální prvek grupy $(L, +)$. Zřejmě $(\varphi \circ \psi)([a]_N) = (d, 0)$, což dokazuje slíbené tvrzení o surjektivitě $(\pi_D \circ \varphi \circ \psi)|_{\ker(\pi_L \circ \varphi \circ \psi)}$.

Odhadněme nejprve, kolik z prvků grupy $(D, +)$ splní, že mají v každé své složce stejný řád. Je-li $s = 1$, tak to zřejmě splní všech 2^{t_1} prvků, v případě $s > 1$ to však všechny prvky nesplní.

Označme $r = \min\{t_1, \dots, t_s\}$. V každé složce řád 1 má jediný prvek, v každé složce řád 2 má jediný prvek, v každé složce řád 4 má 2^s prvků, v každé složce řád 8 má 2^{2s} prvků, v každé složce řád 16 má 2^{3s} prvků, ..., v každé složce řád 2^r má $2^{(r-1)s}$ prvků. Celkový počet těchto prvků zjistíme sečtením geometrické řady

$$1 + 1 + 2^s + 2^{2s} + 2^{3s} + \dots + 2^{(r-1)s} = 1 + \frac{2^{rs} - 1}{2^s - 1}.$$

Ukažme, že pokud je $s = 2$, pak lze počet takových prvků odhadnout shora číslem 2^{rs-1}, a pokud je $s \geq 3$, pak dokonce polovičním číslem 2^{rs-2}. Skutečně, pro $s = 2$ platí

$$1 + \frac{2^{rs} - 1}{2^s - 1} = 1 + \frac{2^{2r} - 1}{3} = \frac{2^{2r}}{2} - \frac{2^{2r}}{6} + \frac{2}{3} = \frac{2^{2r}}{2} - \frac{2^{2r-1} - 2}{3} \leq 2^{rs-1},$$

přičemž rovnost nastane jen v případě $r = 1$. Je-li $s \geq 3$, pak pro $r = 1$ platí

$$\frac{2^{rs} - 1}{2^s - 1} + 1 = 2 \leq 2^{s-2} = 2^{rs-2}$$

přičemž rovnost nastane jen v případě $s = 3$. Předpokládejme nyní $s \geq 3$ a $r \geq 2$, pak nerovnost

$$\frac{2^{rs} - 1}{2^s - 1} + 1 < 2^{rs-2}$$

je ekvivalentní s nerovností

$$2^{rs} + 2^s - 2 \leq \frac{2^s - 1}{4} \cdot 2^{rs}$$

(násobili jsme $2^s - 1 > 0$), a tedy i s nerovností

$$2^s - 2 \leq \frac{2^s - 5}{4} \cdot 2^{rs}$$

(odečetli jsme 2^{rs} od obou stran). Ovšem

$$\frac{2^s - 5}{4} \cdot 2^{rs} \geq \frac{2^s - 5}{4} \cdot 2^s \cdot 2^s > (2^s - 5) \cdot 2^s \geq 3 \cdot 2^s > 2^s - 2.$$

Odtud plyne tvrzení věty pro $s \geq 3$, protože v tomto případě nejvýše čtvrtina prvků grupy $(D, +)$ má ve všech složkách stejný řád, neboť $|D| \geq 2^{rs}$ (rovnost nastane jen v případě, kdy $r = 1$ a $s = 3$ a současně $t_1 = t_2 = t_3 = r$, aby $|D| = 2^{rs}$).

Připomeňme, že $a \in \mathbb{Z}$, $(a, N) = 1$, splní podmínku (1), právě když $[a]_N \in \ker(\pi_L \circ \varphi \circ \psi)$ a navíc každá z s složek $(\pi_D \circ \varphi \circ \psi)([a]_N)$ má stejný řád.

Platí, že $\ker(\pi_L \circ \varphi \circ \psi) = \mathbb{Z}_N^\times$, právě když řád každé cyklické grupy, jejichž součinem je L, je dělitelem čísla q. To se nemůže stát, pokud některé $e_i > 1$, protože $p_i | N$, $q | N - 1$, a tedy $(p_i, q) = 1$.

Zaměřme se na případ $s = 2$. Víme, že nejvýše polovina prvků grupy D splní podmínku o stejných řádech.

Je-li $e_1 > 1$ nebo $e_2 > 1$, pak nejvýše třetina z prvků grupy $\mathbb{Z}_N^\times$ leží v $\ker(\pi_L \circ \varphi \circ \psi)$ a z nich nejvýše polovina se zobrazí na prvky grupy D splňující podmínku o stejných řádech, odkud plyne tvrzení věty. Nechť dále $N = p_1p_2$. Jestliže $q_1 = q_2$, pak z $p_1 \neq p_2$ plyne $t_1 \neq t_2$, a tedy $|D| = 2^{t_1+t_2} \geq 2 \cdot 2^{rs}$, tedy nejvýše čtvrtina prvků grupy D splňuje podmínku o stejných řádech a věta je dokázána i v tomto případě. Předpokládejme, že $N = p_1p_2$ a $q_1 \neq q_2$, bez újmy na obecnosti například $q_1 > q_2$. Pak $q_1 \geq 3$, $q_1 \mid p_1 - 1$, $q_1 \nmid q_2$, a z lichosti q_1 plyne $q_1 \nmid 2^{t_2} \cdot q_2 = p_2 - 1$. Protože

$$2^t \cdot q = N - 1 = p_1p_2 - 1 \equiv p_2 - 1 \pmod{q_1},$$

platí $q_1 \nmid 2^t \cdot q$, a tedy $q_1 \nmid q$. To znamená, že nejvýše třetina z prvků grupy $\mathbb{Z}_N^\times$ leží v $\ker(\pi_L \circ \varphi \circ \psi)$. Věta je dokázána i v tomto případě.

Zbývá případ $s = 1$**.** Pak $N = p_1^{e_1}$, a protože N je složené, je $e_1 \geq 2$. Protože $q \mid N - 1$ a $p_1 \mid N$, je $(q, p_1) = 1$ a násobení číslem q na grupě $(\mathbb{Z}_{p_1^{e_1-1}}, +)$ je surjektivní. Proto

$$|(\pi_L \circ \varphi \circ \psi)(\mathbb{Z}_N^\times)| \geq p_1^{e_1-1} \geq 5,$$

neboť v případě $p_1 = 3$ z $N > 10$ plyne $e_1 \geq 3$. Odtud plyne

$$|\ker(\pi_L \circ \varphi \circ \psi)| = \frac{|\mathbb{Z}_N^\times|}{|(\pi_L \circ \varphi \circ \psi)(\mathbb{Z}_N^\times)|} \leq \frac{|\mathbb{Z}_N^\times|}{5}$$

a důkaz věty je ukončen.

Poznámka. Pro zajímavost analyzujme předchozí důkaz, abychom zjistili, pro která lichá složená $N > 10$ platí, že právě čtvrtina čísel z množiny $\{a \in \mathbb{Z}; 0 \leq a < N, (a, N) = 1\}$ splní podmínku (1).

V případě $s = 1$ se to nestane nikdy.

V případě $s = 2$ to nastane, právě když $q_1 = q_2$, $t_1 + t_2 = 2r + 1$, $e_1 = e_2 = 1$. Jestliže předpokládáme, že $p_1 < p_2$, tak nutně $t_1 = r$, $t_2 = r + 1$. Odtud

$$p_2 = 1 + 2^{t_2}q_2 = 1 + 2^{t_1+1}q_1 = 1 + 2(p_1 - 1) = 2p_1 - 1.$$

Jde tedy právě o čísla $N = p_1 \cdot (2p_1 - 1)$, přičemž prvočíslo p_1 splňuje, že také $2p_1 - 1$ je prvočíslo. Příkladem je $N = 15$ nebo $N = 91$.

V případě $s \geq 3$ musí nutně platit $s = 3$, $t_1 = t_2 = t_3 = r = 1$, $e_1 = e_2 = e_3 = 1$, $q_1|q$, $q_2|q$, $q_3|q$. Pak tedy každé prvočíslo $p_i \equiv 3 \pmod 4$, odkud $N = p_1p_2p_3 \equiv 3 \pmod 4$ a $p_i - 1 = 2q_i \mid 2q = N - 1$. Znamená to, že číslo N je Carmichaelovo číslo, které je součinem tří různých prvočísel, která dávají zbytek 3 po dělení čtyřmi. Příkladem je $N = 7 \cdot 19 \cdot 67 = 8911$.