Definice 1. *Redukovanou (druhou) odmocninou* čísla $n \in \mathbb{N}$ rozumíme rozklad $\sqrt{n} = k \cdot \sqrt{l}$, $k, l \in \mathbb{N}$ takový, že $\forall i, j \in \mathbb{N} : \sqrt{n} = i \cdot \sqrt{j} \Rightarrow i \leq k$.

Příklad. Různé rozklady odmocnin, poslední je vždy redukovaná odmocnina:
$\sqrt{3} = 1.\sqrt{3}$,
$\sqrt{12} = 1 \cdot \sqrt{12} = 2 \cdot \sqrt{3}$,
$\sqrt{36} = 1 \cdot \sqrt{36} = 2 \cdot \sqrt{9} = 3 \cdot \sqrt{4} = 6 \cdot \sqrt{1}$.

Zabývejme se nyní otázkou, jak vypadá redukovaná odmocnina obecně.

Pozorování 1. $\forall n, k, l \in \mathbb{N} : \sqrt{n} = k \cdot \sqrt{l} \Rightarrow k^2 \big| n$.

Důkaz. $\sqrt{n} = k \cdot \sqrt{l} \Leftrightarrow n = k^2 \cdot l$. □

Lemma 1. *Redukovaná odmocnina čísla p^i, kde p je prvočíslo a $i \in \mathbb{N}$, je $p^{\frac{i}{2}} \cdot \sqrt{1}$ pro i sudé a $p^{\frac{i-1}{2}} \cdot \sqrt{p}$ pro i liché.*

Důkaz. Uvedené rozklady jsou zjevně rovny $\sqrt{p^i}$, dokažme, že jde o redukované odmocniny. Dělitelé p^i jsou právě všechna čísla p^j, $0 \leq j \leq i$. Největší druhou mocninou (viz Pozorování 1) mezi nimi je pro sudé i p^i, pro liché i p^{i-1}. □

Pozorování 2. *Nechť $\sqrt{n} = k \cdot \sqrt{l}$ je redukovaná odmocnina. Pak $\sqrt{n} = i \cdot \sqrt{j} \Rightarrow i | k$.*

Důkaz. Nechť $K = \mathrm{nsn}(i, k)$. Protože podle Pozorování 1 $i^2 \big| n$ a $k^2 \big| n$, i $K^2 \big| n$, tedy $\exists L : \sqrt{n} = K \cdot \sqrt{L}$. $k \cdot \sqrt{l}$ je redukovaná, tedy $k \geq K = \mathrm{nsn}(i, k) \geq k$, a tedy $K = k$ a $i | k$. □

Věta 1. *Nechť $\prod_{j=1}^{m} p_j^{i_j}$ je prvočíselný rozklad n a $p_j^{i_j} = k_j \cdot \sqrt{l_j}$, $1 \leq j \leq m$ jsou redukované odmocniny. Pak*

$$\prod_{j=1}^{m} k_j \cdot \sqrt{\prod_{j=1}^{m} l_j} \tag{R1}$$

je redukovaná odmocnina n.

Důkaz. Zřejmě je $\sqrt{n}$ rovno R1, dokážeme, že je tento rozklad redukovanou odmocninou. Nechť $\sqrt{n} = k \cdot \sqrt{l}$ je redukovaná odmocnina. Pak $\prod_{j=1}^{m} k_j \Big| k$, tedy $\exists d \in \mathbb{N} : d \cdot \prod_{j=1}^{m} k_j = k$. Odtud

$$\sqrt{n} = k \cdot \sqrt{l} = d \cdot \prod_{j=1}^{m} k_j \cdot \sqrt{l} = \prod_{j=1}^{m} k_j \cdot \sqrt{\prod_{j=1}^{m} l_j}$$

a po vykrácení a umocnění

$$d^2 \cdot l = \prod_{j=1}^{m} l_j.$$

Protože však jsou l_j různá prvočísla nebo jedničky, může tato rovnost nastat jen pro $d = 1$, a tedy $\prod_{j=1}^{m} k_j = k$. □

Lemma 2. $\forall n \in \mathbb{N} : \sqrt{n} \in \mathbb{Q} \Rightarrow \sqrt{n} \in \mathbb{N}$ *(slovně: odmocnina z přirozeného čísla je celá nebo iracionální).*

Důkaz. Nechť $\sqrt{n} = k \cdot \sqrt{l}$ je redukovaná odmocnina. Pak podle předchozího buď $l = 1$ a tedy $\sqrt{n} = k \in \mathbb{N}$, nebo $l = \prod_{j=1}^{m} l_j$, kde l_i jsou navzájem různá prvočísla. Je-li v tomto druhém případě $\sqrt{n} \in \mathbb{Q}$, je i $\sqrt{l} \in \mathbb{Q}$ a tedy existují nesoudělná p, q taková, že

$$\sqrt{\prod_{j=1}^{m} l_j} = \frac{p}{q}.$$

Pak ovšem $q^2 \prod_{j=1}^{m} l_j = p^2 \Rightarrow l_1 | p^2 \Rightarrow l_1 | p \Rightarrow l_1 | q^2 \Rightarrow l_1 | q$, což je spor s nesoudělností p a q. □

Věta 2. *Nechť $\alpha, \beta \in \mathbb{N}$, $\alpha > \beta$. Pak $\sqrt{\alpha} \pm \sqrt{\beta} \in \mathbb{N} \Leftrightarrow \sqrt{\alpha}, \sqrt{\beta} \in \mathbb{N}$.*

Důkaz. Implikace $\Leftarrow$ je triviální, dokažmě implikaci $\Rightarrow$. Nechť $\sqrt{\alpha} = k_1 \cdot \sqrt{l_1}$, $\sqrt{\beta} = k_2 \cdot \sqrt{l_2}$ jsou redukované odmocniny. Pak

$$\begin{aligned} k_1\sqrt{l_1} \pm k_2\sqrt{l_2} &= n \in \mathbb{N} \\ k_1^2 l_1 \pm 2k_1k_2\sqrt{l_1 l_2} + k_2^2 l_2 &= n^2 \\ \pm\sqrt{l_1 l_2} &= \frac{n^2 - k_1^2 l_1 - k_2^2 l_2}{2k_1k_2} \qquad \text{(R2)} \end{aligned}$$

Vzhledem k pravé straně R2 je $\sqrt{l_1 l_2}$ zjevně racionální a podle Lemmatu 2 i přirozené. Tedy $\exists \gamma \in \mathbb{N} : l_1 l_2 = \gamma^2$, což vzhledem k tomu, že l_1, l_2 jsou jedničky nebo součiny prvních mocnin prvočísel, znamená, že $l_1 = l_2$. Můžeme proto přepsat $\sqrt{\alpha} \pm \sqrt{\beta} = (k_1 \pm k_2)\sqrt{l_1}$ a protože $k_1 > k_2$, může být tento výraz celý pouze tehdy, je-li $\sqrt{l_1} \in \mathbb{N}$, neboli je-li $l_1 = 1$. Pak ovšem $\sqrt{\alpha}, \sqrt{\beta} \in \mathbb{N}$. $\square$