Klasyfikacja trójek Pitagorejskich

Lemat 1.1 *Jeżeli liczby całkowite a, b, c spełniają*

$$a^2 + b^2 = c^2$$

to co najmniej jedna z liczb a, b jest parzysta.

Dowód:

Lemat 1.2 *Jeżeli liczby a, b, w, n są całkowite dodatnie, $NWD(a, b) = 1$ oraz*

$$ab = w^n$$

to a, b są n-tymi potęgami liczb całkowitych, innymi słowy istnieją takie t, u całkowite dodatnie, że

$$a = t^n,\ \ b = u^n$$

Dowód:

Twierdzenie 1.3 *Liczby całkowite dodatnie a, b, c względnie pierwsze spełniają równanie*

$$a^2 + b^2 = c^2$$

wtedy i tylko wtedy, gdy istnieją takie $m > n$ całkowite dodatnie, że

$$a = m^2 - n^2,\ \ b = 2mn,\ \ c = m^2 + n^2$$

lub

$$a = 2mn,\ \ b = m^2 - n^2,\ \ c = m^2 + n^2$$

1. $\Leftarrow$ Po pierwsze, jeżeli m, n z treści zadania istnieją to a, b, c są całkowite dodatnie i zachodzi

   $$a^2 + b^2 = (m^2 - n^2)^2 + (2mn)^2 = m^4 - 2m^2n^2 + n^4 + 4m^2n^2 = m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2 = c^2$$

   To kończy dowód implikacji w lewo .

2. $\Rightarrow$. Załóżmy, że $a, b, c \in \mathbb{Z}_+$ spełniają $a^2 + b^2 = c^2$.

3. Liczby a, b, c są względnie pierwsze , a więc dowolne 2 z liczb a, b, c są również względnie pierwsze. Faktycznie, załóżmy $NWD(a, b) > 1$. Istnieje wtedy liczba pierwsza p, taka, że

   $$p|NWD(a, b)$$

   czyli $p|a$ i $p|b$, a więc $p|a^2+b^2 = c^2$, a skoro p jest pierwsza, to $p|c$ i $p|NWD(a, b, c) = 1$. Sprzeczność.

4. Skoro a, b są względnie pierwsze, to przynajmniej jedna z nich jest nieparzysta. Z lematu wynika natomiast, że jedna z liczb a, b musi być parzysta. Załóżmy, że $2 \nmid a$.
   Zauważmy, że $2 \nmid a$ i $2|b$, więc $2 \nmid c$, czyli

   $$2|c - a \text{ i } 2|c + a$$

Istnieją więc k, l całkowite $c - a = 2k$, $c + a = 2l$.
Jest

$$b^2 = (c - a)(c + a) = 4kl$$

Skoro $2|b$ to możemy podstawić $b = 2b'$, gdzie $b' \in \mathbb{Z}$:

$$b'^2 = kl$$

Mamy $NWD(k, l) = \frac{1}{2}NWD(c - a, c + a) = \frac{1}{2}NWD(c + a, 2a) = \frac{1}{2}2 = 1$.
Z lematu wiemy więc, że dla pewnych n, m jest

$$k = n^2 \text{ i } l = m^2$$

Jest więc

$$b^2 = 4kl = 4m^2n^2 \text{ stąd } b = 2mn$$

$$2a = (c + a) - (c - a) = 2m^2 - 2n^2 \text{ stąd } a = m^2 - n^2$$

$$2c = (c + a) + (c - a) = 2m^2 + 2n^2 \text{ stąd } c = m^2 + n^2$$

Oczywiście $m > n$, gdyż $0 < a = m^2 - n^2$. Dowód $\Rightarrow$ jest więc zakończony.

5. Podany dowód klasyfikuje w zasadzie wszystkie trójki pitagorejskie, gdyż każda taka trójka powstaje przez pomnożenie trójki pitagorejskiej złożonej z liczb względnie pierwszych przez jakiś mnożnik.

6. Próba podsumowania - dlaczego właśnie tak dowodziliśmy?
Poniższe rozumowanie NIE ma nic wspólnego z dowodzeniem, jest to tylko spekulacja, którą przekuć można w dowód. *Jeżeli teza jest prawdziwa*, to z tezy możemy wyliczyć $2m^2 = a + c$ i $2n^2 = a - c$, pozostaje więc udowodnić, że ułamki $\frac{c+a}{2}$, $\frac{c-a}{2}$ są całkowite i są kwadratami liczb całkowitych. Tak właśnie przebiega dowód.