9 - Faktoryzacja Fermata

Thursday, 20 June 2024 16:51

Niech N będzie nieparzystą liczbą do sfaktoryzowania.

Niech $N = pq \quad p > q$

Wtedy $N = a^2 - b^2$ dla $a = \frac{p+q}{2}$, $b = \frac{p-q}{2}$

Zatem $b^2 = a^2 - N$

Możemy próbować kolejne wartości $a \geq \lceil \sqrt{N} \rceil$

Jeśli faktoryzacja istnieje to znajdziemy ją po $a - \sqrt{N}$ krokach.

$$a - \sqrt{N} = \frac{a^2 - N}{a + \sqrt{N}} = \frac{b^2}{a + \sqrt{N}} \leq \frac{(p-q)^2}{4\sqrt{N}}$$

□