

Prop 1. $N \geq 2$ を整数とする。 N をわりきる \sqrt{N} 以下の素数 p が存在しない $\implies N$ は素数である。

Proof. 対偶は、以下のとおりである。

N が合成数 $\implies N$ をわりきる \sqrt{N} 以下の素数 p が存在する。

これを示す。仮定より、素数 p_1, \dots, p_k ($k \geq 2$) を用いて、

$$N = p_1 \cdots p_k$$

と素因数分解することができる。このとき、 p_1, \dots, p_k のうち最小のものを p とおくと、

$$p^2 \leq p_1 p_2 \cdots p_k = N.$$

よって $p \leq \sqrt{N}$ 。ゆえに題意は示された。

□