

**$n$  が素数か否かの判定**

1 より大きい整数  $n$  が合成数ならば,  $2 \leq p \leq \sqrt{n}$  を満たす素因数  $p$  が存在する。

したがって,  $n$  が素数か否かを確かめたいとき,  $\sqrt{n}$  以下の素因数の有無を調べればよい。

**証明**

$n$  を割る素数のうち, 最小のものを  $p$  とすると,  $n = p \cdot q$  と表される。

また, このとき,  $p$  が最小の素数であるためには,

$q$  が素数であろうと合成数であろうと  $p \leq q$  であることが必要である。

よって,  $n = p \cdot q$  かつ  $p \leq q$

すると,  $p^2 \leq pq = n$  より,  $p \leq \sqrt{n}$

よって,  $2 \leq p \leq \sqrt{n}$