ゼミレポート

kiyoshi ohashi

2023 年 4 月 7 日

次に，正の整数が素数であるかを判定する最古のアルゴリズムである**エラトステネスのふるい**について確認しよう．

Prop. 1.4.9 $n > 1$ が合成数ならば，$\sqrt{n}$ 以下の素数の約数を持つ

Proof. n が合成数と仮定すると，${}^{\exists}l \in \mathbb{Z}$ s.t. $l \mid n$ である．ただし，$n > 1$ の合成数より，$l \neq 1, n$．ここで，$m = n/l$ とおくと，$l, m \neq 1, n$，$n = lm$ である．(合成数の定義から $l > 0$)．もし，$l, m > \sqrt{n}$ であるとき，$lm > n$ となり矛盾する．よって，$l \leq \sqrt{n}$ または $m \leq \sqrt{n}$ となるため，n は $\sqrt{n}$ 以下の約数 l を持つ．
Prop 1.4.8 より，l は素数の約数を持ち，それを p と置くと $p \mid l$ であり，**Prop 1.4.7** より，推移律から $p \mid n$ となる．
したがって，$p \leq l \leq \sqrt{n}$ であるから，n は $\sqrt{n}$ 以下の素数の約数を持つ． □

この命題の対偶を取れば，次のような表現となる

Prop. 1.4.9′ $\sqrt{n}$ 以下の素数の約数を持たないならば，n は素数である．

「割り切れる（割り算）」の概念を規定するのは **Prop 1.4.15** とまだ先であるが，その概念を用いて説明するならば，本命題が主張することは ある正の整数 n が与えられた時，$\sqrt{n}$ 以下の素数全てで n を割り切れない時，n が素数であることを主張する．すなわち，n が素数であることを調べる際に，n 回ではなく $\sqrt{n}$ 回のステップのみで充分であることを意味する．

また，次の補題についても確認しよう．

Lem. 1.4.10 $m, n \in \mathbb{Z}$ のとき，$n \mid m,\ n \neq \pm 1 \implies n \nmid m + 1$

Proof. 仮定より ${}^{\exists}a \in \mathbb{Z}$ s.t. $m = na$ である．もし，$n \mid m + 1$ ならば，${}^{\exists}b \in \mathbb{Z}$ s.t. $m + 1 = nb$ であり，$1 = (m + 1) - m = n(b - a)$ である．**Cor 1.4.3** より，$n = \pm 1$ であるが，これは矛盾 □

今回のゼミにおいて，個人的に疑問に思ったのは $n \mid m$ によって $n \neq \pm 1 \implies n \nmid m + 1$ を束縛しているのではないか，という点である．この事については，束縛させても仮定に用いても，帰結されるものに変わりはない．むしろ，今回の場合には $n \mid m + 1$ を仮定した際に，$n \nmid m$ または $n = \pm 1$ を考え，それぞれの命題変数の成立の可否をを調べることが，考察の手立てとなる．