素数の分布

定理 1　素数は無限にある．

[**ユークリッドの証明 (再掲)**]　素数が有限個しかないと仮定する．
最大の素数を p として，

$$q = 1 \times 2 \times 3 \times \cdots \times p + 1$$

という数を考える．

1. q を素数とすると $\cdots p$ が最大の素数であるということに矛盾する．
2. q が素数でないとすると $\cdots q$ は p 以下のいずれかの素数で割り切れるはずだが，q の形より，q は 2 から p までのすべての数で割り切れないので矛盾する．

いずれにせよ，矛盾するので素数が有限個であるという仮定が誤りであることがわかる．
よって，素数は無限にある．　[証明おわり]

このユークリッドの証明は数学の数ある証明の中で，最も美しいものの一つであると言われている．

[**クンマー** (Kummer) **の証明**]　素数は有限個しかないと仮定して，その全ての素数を

$$p_1, p_2, p_3, \cdots, p_n$$

とする．

$$N = p_1 p_2 p_3 \cdots p_n$$

とおくと，$N-1$ は全ての素数 $p_1, p_2, p_3, \cdots, p_n$ の中でどれかを約数にもつ．その約数である素数の一つを p_k とする．つまり，

$$p_k | N, p_k | (N-1)$$

N と $N-1$ の差を考えれば

$$1 = N - (N-1)$$

より，

$$p_k | 1$$

これは素数が 2 以上であることと矛盾する．　［証明おわり］

定理 2　$4n+3$ 型の素数は無限にある．

[**証明**]　$4n+3$ 型の素数が有限個しかないと仮定する．
最大の $4n+3$ 型の素数を p として，

$$q = 4(7 \times 11 \times 19 \times \cdots \times p) + 3$$

という $4n+3$ 型の自然数を考える．

1. q を $4n+3$ 型の素数とすると $\cdots p$ が最大の $4n+3$ 型の素数であるということに矛盾する．

2. q が $4n+3$ 型の素数でないとすると $\cdots q$ は p 以下の $4n+3$ 型のいずれかの素数で割り切れるはずである．なぜならば，$4n+1$ 型の素数のみを因数に持つ数は $4n+3$ 型の数にはなりえないからである．しかしながら，q の形より，q は 3 から p までのすべての $4n+3$ 型の素数で割り切れない（7 以上で割ると余りが必ず 3 になる．3 で割るとカッコの中が全て 3 と互いに素なので割り切れない．）ので矛盾する．

いずれにせよ，矛盾するので $4n+3$ 型の素数が有限個であるという仮定が誤りであることがわかる．
よって，$4n+3$ 型の素数は無限にある． [証明おわり]

問題 1 $6n+5$ 型の素数は無限に存在することを証明せよ．

[**解**] $6n+5$ 型の素数が有限個しかないと仮定する．
最大の $6n+5$ 型の素数を p として，

$$q = 6(11 \times 17 \times 23 \times \cdots \times p) + 5$$

という $6n+5$ 型の自然数を考える．

1. q を $6n+5$ 型の素数とすると $\cdots p$ が最大の $6n+5$ 型の素数であるということに矛盾する．
2. q が $6n+5$ 型の素数でないとすると $\cdots q$ は p 以下の $6n+5$ 型のいずれかの素数で割り切れるはずである．なぜならば，$6n+1$ 型の素数のみを因数に持つ数は $6n+5$ 型の数にはなりえないからである．しかしながら，q の形より，q は 5 から p までのすべての $6n+5$ 型の素数で割り切れない（11 以上で割ると余りが必ず 5 になる．5 で割るとカッコの中が全て 5 と互いに素なので割り切れない．）ので矛盾する．

いずれにせよ，矛盾するので $6n+5$ 型の素数が有限個であるという仮定が誤りであることがわかる．
よって，$6n+5$ 型の素数は無限にある． [証明おわり]

定理 3 $4n+1$ 型の素数は無限にある．

[**証明**] $4n+1$ 型の最大の素数を p として，

$$q = (2 \times 5 \times 13 \times \cdots \times p)^2 + 1$$

という数を考える．かっこの中は 2 と小さいほうから並べた $4n+1$ 型の素数である．

1. q を素数とすると $\cdots p$ が最大の $4n+1$ 型の素数であるということに矛盾する．
2. q が素数でないとすると $\cdots q$ を割り切る素数を r とすると，q が奇数なので r は奇素数である．

$$(2 \times 5 \times 13 \times \cdots \times p)^2 \equiv -1 \pmod{r} \tag{1}$$
$$(2 \times 5 \times 13 \times \cdots \times p)^4 \equiv 1 \pmod{r} \tag{2}$$

$2 \times 5 \times 13 \times \cdots \times p \not\equiv 1, (2 \times 5 \times 13 \times \cdots \times p)^3 \not\equiv 1 \pmod{r}$ であることは明らかである．もし 1 に合同なら $r \neq 2$ なので (1) が成り立たない．つまり (2) より $2 \times 5 \times 13 \times \cdots \times p$ は r を法として指数 4 に対応する．一方フェルマーの小定理より

$$(2 \times 5 \times 13 \times \cdots \times p)^{r-1} \equiv 1 \pmod{r}$$

であるから $r-1$ は 4 の倍数である．つまり r は $4n+1$ 型であり，なおかつ r は $5, 13, 17, \cdots, p$ のどれとも異なる．もしどれかと等しければ r は q の約数となりえないからである．よって p が最大の $4n+1$ 型の素数であるということに矛盾する．

よって，$4n+1$ 型の素数は無限にある． [証明おわり]

参考文献

[1] 高木貞治『初等整数論講義第 2 版』（共立出版社，1997 年）

[2] 芹沢正三『素数入門』（講談社ブルーバックス，2002 年）

[3] 上野健爾『代数入門 1』（岩波講座 現代数学への入門，1995 年）