素数が無限に存在することの証明

フェルマー数の利用(ゴールドバッハによる証明)

フェルマー数とは $F_n = 2^{2^n}+1$（nは負でない整数)で表される自然数のことである。

フェルマー数は次の等式を満たす。

$$F_{n+1} = F_0F_1F_2\cdots\cdots F_n + 2$$

証明

$$F_0F_1F_2\cdots\cdots F_n = (2^1+1)(2^2+1)(2^4+1)\cdots\cdots(2^{2^n}+1)$$

$$= (2^1-1)(2^1+1)(2^2+1)(2^4+1)\cdots\cdots(2^{2^n}+1)$$

$$= 2^{2^{n+1}}-1 = 2^{2^{n+1}}+1-2 = F_{n+1}-2$$

よって

$$F_{n+1} = F_0F_1F_2\cdots\cdots F_n + 2$$

□

この性質より，F_{n+1}とF_k $(0 \leqq k < n+1)$ が共通の素因数pを持つと仮定すると，2 はpで割り切れることになるが，F_kが奇数であることよりpは奇数であるので，矛盾する。したがって，F_{n+1}とF_k $(0 \leqq k < n+1)$は互いに素である。

nは任意の負でない整数であるから，フェルマー数はどの 2 つも互いに素である。
よって，任意に多くの異なる素因数を作れるので，素数は無限に存在する。

フェルマー数による方法の簡略化

数列$\{a_n\}$は，a_1を自然数として，次の漸化式により定義される数列とする。

$$a_{n+1} = a_1a_2a_3\cdots\cdots a_n + 1$$

任意の自然数nについて，a_{n+1}とa_k $(k=1,2,3,\cdots\cdots,n)$は互いに素であるから，$\{a_n\}$の各項は，どの 2 つも互いに素である。
よって，任意に多くの異なる素因数を作れるので，素数は無限に存在する。

サイダック(Filip Saidak)による証明

nは 1 より大きい整数とする。nと$n+1$は連続する整数であるから，これらは互いに素である。
したがって，$N_2 = n(n+1)$は少なくとも 2 つの異なる素因数を持つ。
同様に，$n(n+1)$と$n(n+1)+1$は連続する整数であるから，互いに素である。

よって，$N_3 = n(n+1)\{n(n+1)+1\}$は少なくとも 3 つの異なる素因数を持つ。

この操作は，無限に続けることができる。

よって，任意に多くの異なる素因数を持つ数を作れるので，素数は無限に存在する。

数列 $\{N_n\}$ は次の漸化式により得られる。

$$N_1 > 1, \quad N_{n+1} = N_n(N_n + 1)$$

漸化式の類似性

上記の 2 つの証明は，一見すると無関係のようであるが，漸化式を用いると，類似性があることに気が付く。

フェルマー数について

$$F_{n+1} = F_0 F_1 \cdots\cdots F_{n-1} F_n + 2 \quad \cdots①$$

であるから，

$$F_0 F_1 \cdots\cdots F_{n-1} F_n = F_{n+1} - 2$$

よって

$$F_0 F_1 \cdots\cdots F_{n-1} = F_n - 2 \quad (n \geqq 1)$$

これを①に代入して

$$F_{n+1} = (F_n - 2)F_n + 2 \quad (n \geqq 1)$$

ただし　$F_1 = F_0 + 2$

$F_0 = 3, F_1 = 5$ より $F_1 = (F_0 - 2)F_0 + 2$ が成り立つから，漸化式は 1 つにまとめられて

$$F_0 = 3, \quad F_{n+1} = F_n(F_n - 2) + 2 \quad (n = 0, 1, 2, \cdots\cdots)$$

フェルマー数が満たす漸化式の一般化

フェルマー数の性質①を一般化すると，次のようになる。

p を 0 でない整数とする。数列 $\{a_n\}$ は，a_0 は p と互いに素な整数であるとし，次の漸化式により定義される数列とする。

$$a_{n+1} = a_0 a_1 \cdots\cdots a_{n-1} a_n + p \quad \cdots②$$

$a_k\ (k = 1, 2, \cdots\cdots, n)$ と p が互いに素であると仮定すると，$a_0 a_1 \cdots\cdots a_{n-1} a_n$ と p は互いに素であるから，②より，

a_{n+1} と p は互いに素である。よって，すべての負でない整数 n について，a_n と p は互いに素である。

また，ユークリッドの互除法の原理により，$k = 0, 1, 2, \cdots\cdots, n$ について

$$\begin{aligned}(a_{n+1}, a_k) &= (a_0 a_1 \cdots a_k \cdots a_{n-1} a_n + p, a_k) \\ &= (a_0 a_1 \cdots a_k \cdots a_{n-1} a_n + p - a_0 a_1 \cdots a_k \cdots a_{n-1} a_n, a_k) \\ &= (p, a_k) = 1\end{aligned}$$

したがって，$\{a_n\}$ の各項は，どの 2 つも互いに素である。

②より　$a_n = a_0 a_1 \cdots\cdots a_{n-1} a_n = a_{n+1} - p$　であるから

$$a_0 a_1 \cdots\cdots a_{n-2} a_{n-1} = a_n - p \quad (n \geqq 1)$$

これを②に代入して

$$a_{n+1}=a_n(a_n-p)+p \quad (n \geqq 1)$$

ただし，$a_1=a_0+p$

ここで，特性方程式 $\alpha=\alpha(\alpha-p)+p$ を考えると

$$\alpha^2-(p+1)\alpha+p=0$$
$$(\alpha-1)(\alpha-p)=0$$
$$\alpha=1,\ p$$

よって，$a_1=1,\ p$ のときは $\{a_n\}$ のすべての項が等しくなるので，$a_1 \neq 1$ かつ $a_1 \neq p$ とする。

したがって，$a_0 \neq 1-p$ かつ $a_0 \neq 0$ とする。

逆に，$a_0=a_1-p$ と定めると，a_1 と p は互いに素であるから，a_0 と p は互いに素であり，漸化式

$$a_{n+1}=a_n(a_n-p)+p$$

によって定められる数列 $\{a_n\}$ が，①を満たすことは明らかである。

一般化されたフェルマー数の漸化式とサイダックの漸化式の関係

漸化式 $a_{n+1}=a_0a_1\cdots\cdots a_{n-1}a_n+p$ において，$N_n=a_0a_1\cdots\cdots a_{n-1}a_n$ とおくと，

$$\begin{cases} a_{n+1}=N_n+p & \cdots ① \\ N_{n+1}=N_na_{n+1} & \cdots ② \end{cases}$$

① を②に代入して

$$N_{n+1}=N_n(N_n+p)$$

ただし，p を 0 でない整数，N_0 を整数とし，N_0 と p は互いに素，$N_0 \neq 0$ かつ $N_0 \neq 1-p$ であるとする。

このとき，$n>0$ であれば，N_n は少なくとも $n-1$ 個の素因数を含む。（N_n が 1 か−1 になることがあり得るので，$n-1$ 個とした。）

特に，$p=1,\ N_0>1$ のときは，

$$N_{n+1}=N_n(N_n+1)$$

となり，サイダックの漸化式と一致する。