フェルマー数

定義 1　0 以上の整数 n に対してフェルマー数 F_n を

$$F_n = 2^{2^n} + 1$$

と定義する.

定理 1

$$F_n = \prod_{k=0}^{n-1} F_k + 2$$

［証明］

$$\begin{aligned}
F_n &= 2^{2^n} - 1 + 2 \\
&= (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1) + 2 \\
&= F_{n-1}(2^{2^{n-1}} - 1) + 2 \\
&= F_{n-1}(2^{2^{n-2}} + 1)(2^{2^{n-2}} - 1) + 2 \\
&= F_{n-1}F_{n-2}(2^{2^{n-2}} - 1) + 2 \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
&= F_{n-1}F_{n-2}F_{n-2}\cdots F_0 + 2
\end{aligned}$$

［証明おわり］

補題 1 素数 p が F_n の約数ならば，p は $F_{n-1}, F_{n-2}, F_{n-2}, \cdots, F_0$ のいずれの約数でもない.

［証明］p が F_n の約数で，かつ $F_{n-1}, F_{n-2}, F_{n-2}, \cdots, F_0$ のどれかの約数でもあると仮定すると,

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

より p は 2 の約数でもある．つまり 2 である．しかしフェルマー数は全て奇数であるので矛盾する．よってこの補題は証明された.　［証明おわり］

定理 2（再々掲）素数は無限にある.

［ポリア (Polya) の証明 (1924)］F_n を割り切る素数の一つを p_n とすると，補題 1 より p_n は $F_{n-1}, F_{n-2}, F_{n-2}, \cdots, F_0$ のいずれの約数でもない．つまり，p_n は $p_{n-1}, p_{n-2}, p_{n-2}, \cdots, p_0$ のどれとも異なる．フェルマー数は無限に作れるので素数も無限にある.　［証明おわり］

フェルマーはフェルマー数は全て素数であると予想したが, 1732 年オイラーにより否定される．オイラーは

$$F_5 = 641 \times 6700417$$

と素因数分解した．フェルマーの予想とは逆に F_5 以上で素数は現れていない．F_6 が素因数分解されたのは 1970 年コンピュータを使ってであった.

$$F_6 = 274177 \times 67280421310721$$

当時のコンピュータがどの程度の性能であったかわからないが，現在 (2010 年）のコンピュータではできるかどうか試してみたくなった．

```
for n:5 thru 8 do(print(factor(2^(2^n)+1)));
```

641×6700417
$274177 \times 67280421310721$
$59649589127497217 \times 5704689200685129054721$
$1238926361552897 \times 93461639715357977769163558199606896584051237541638188580280321$

意外にも F_5 から F_8 まで素因数分解するのに要した時間はちょうど 2 分であった（wxMacima 使用）．そのほとんどが F_8 に使われたと言ってよい．2010 年と言っても使っているのは 2005 年くらいのモデルなので，最新のものを使えばもっと速いのだろう．さすがに F_9 をやってみる気はおこらない．

参考文献

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