4F－05

メルセンヌ 素数 の ふるい(篩) の アルゴリズム(2)

an Algorithm of the Cieve for Mercenne Prime Numbers(2)

(財)機械産業記念事業財団　ハイテク情報サービス室
ＴＥＰＩＡ ハイパー工房 主任研究員　林　大 雅 *
Hiromasa Hayashi (会員番号 196310951)

１．はじめに

エラトステネスの ふるい(篩)の アルゴリズム のように，メルセンヌ数の 素数 と 合成数 とを ふるい(篩)分けるアルゴリズム(算法)を提案する。

メルセンヌ数 Ｍｎ は，(２^Ｎ)－１ の数列で，その数が素数の場合が，メルセンヌ素数 Ｍｐ で，２０００年１月までに，３８個が発見されている。

２．記号の説明

Ｎ ： 自然数，Natural Number，１，２，３，…
Ｇ ： 偶数，Even Number，(Ｇ≧２：2以上の偶数)
Ｋ ： 奇数，Odd Number，(Ｋ≧３：3以上の奇数)
Ｐ ： 素数，Prime Number，(Ｐ≧３：奇数の素数)
Ｍｎ：メルセンヌ型の数，(Ｍｎ＝２^Ｎ－１の数)
Ｍｐ：メルセンヌ素数，(Ｍｐ＝２^Ｐ－１が素数)
ＴＬ：１／Ｋ の 二進循環小数の(循環節)の長さ。
　Thred Length，ＴＬ＝ＴＬ(Ｋ)，ＴＬ≦Ｋ－１
　ＴＬ は，２ を元とする 位数(Order)に当る。
Ｈ ： １／Ｋ の 二進循環小数の循環節の整数値。
　Hash，Ｈ＝(２^ＴＬ－１)／Ｋ の関係にある。

３．ＴＲＯＮ数，(Thred Length：TL)

奇数(Ｋ≧３)の逆数(Reciprocal) を 二進表示で求めると 循環小数 になり，その 循環する二進の小数 の セグメント：「循環節」：(Recurring Period)の 長さ：(Segment Length)の 値 を，ＴＲＯＮ数 または ＴＬ(Thred Length)と 呼ぶ。

bin(The Reciprocal of Odd Number)　図表 3

```
bin(1/ 3)=0.01…(TL=2) H=1
bin(1/ 5)=0.0011…(TL=4) H=3
bin(1/ 7)=0.001…(TL=3) H=1
bin(1/ 9)=0.000111…(TL=6) H=7
bin(1/11)=0.0001011101…(TL=10) H=93
bin(1/13)=0.000100111011…(TL=12) H=315
bin(1/15)=0.0001…(TL=4) H=1
bin(1/17)=0.00001111…(TL=8) H=15
bin(1/19)=0.000011010111100101…(TL=18)H=13797
```

４．循環小数と分数(分子／分母)の関係

十進の 循環小数，例えば，(１÷７)＝0.142857… は，循環節の 長さ だけ，999999 を 分母 に 用意して，分子 には 循環節 を 当て嵌めると，(142857／999999)＝ １／７ と 分数 に 再変換 できる。

二進の循環小数 では，bin(１÷５)＝ 0.0011… は，循環節の長さ だけ の，1111 を 分母 として用意 して，分子 には「循環節」を 当て嵌めると，(0011 / 1111) ＝ ３／１５ ＝ １／５ と 分数に再変換できる。 二進 の 循環節の長さは，ＴＬ として 求められる。 この場合，分母の 111… 1 の 二進数 は，メルセンヌ型の数(Ｍｎ) の 形式である。 この メルセンヌ数 が，合成数なら，因数には，分子 と なった 循環節 を 二進整数 にした値(Ｈ) が 含まれている。 また，(分母÷分子)で求まる 奇数(Ｋ)も 因数 である。

逆に，分母 の メルセンヌ数 が，素数(Ｑ) なら，Ｍｑ＝(２^Ｑ－１) の 因数 には，分子(Ｈ) と，奇数(Ｋ) がある が，Ｈ＝１ の 場合，分母(Ｑ) は １ と Ｋ 自身 が 約数 であり，「素数」即ち，メルセンヌ素数 に なる。

奇数(Ｋ) が 素数(Ｐ) の場合 を 示す。図表 4

$\frac{1}{P} = \frac{H}{111\cdots\cdots1}$	分母は二進の←記述であり，Mn
Ｐ ： 素数，　ＴＬ　Ｈ ： Hash，「循環節」1/P の循環節長(TL)：Thred Length，TL=TL(P)	

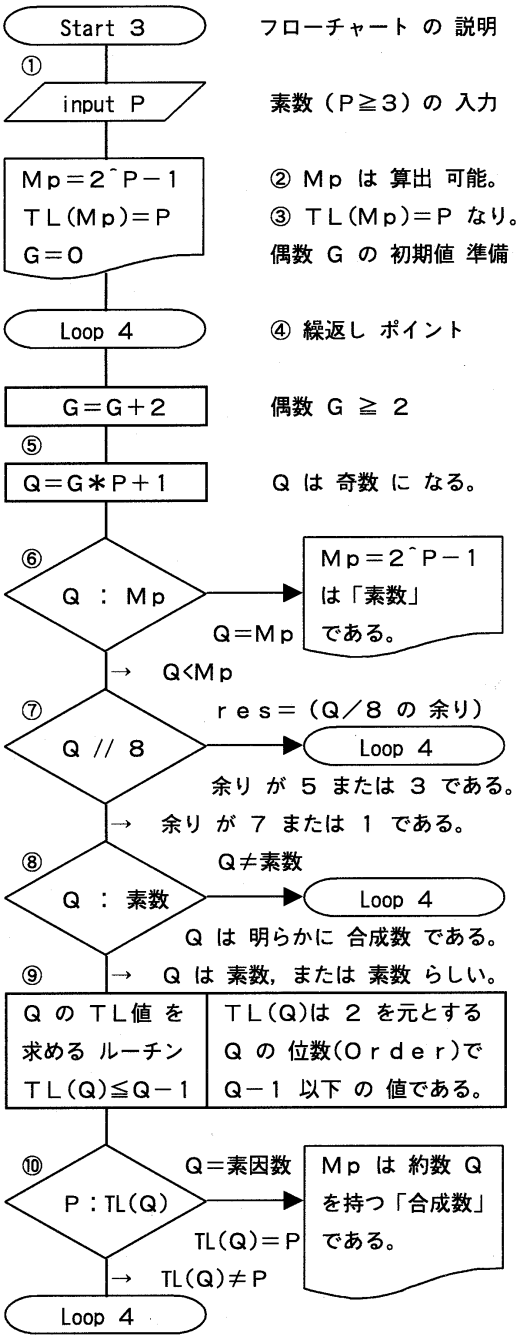
５．メルセンヌ数(Ｍｐ) の 素因数 の 検出

Ｍｐ＝２^Ｐ－１ に 素因数(Ｑ) が ある場合，Ｑ＝Ｇ＊Ｐ＋１ の ＴＬ値 は Ｐ である。即ち ＴＬ(Ｑ)＝Ｐ，ＴＬ(Ｍｐ)＝Ｐ であれば，Ｑ は Ｍｐ の 約数 である。

６．メルセンヌ数(Ｍｐ) の ふるい(篩)

メルセンヌ素数 (Ｍｐ) を 見つける アルゴリズム を提案する。 計算を早める判定を追加した。

フローチャート と 計算手順 を 次に 示す。



① 3 以上の素数 P≧3 を 入力 する。
② Mp＝2^P－1 は，算出できること。
③ Mp の TL(Thred Length)：すなわち，
TL(Mp)＝P は，算出するまでもない。
④ 偶数 G＝G＋2 を 計算する。（G≧2）
⑤ Q＝G＊P＋1 を 計算 する。(Q は 奇数)
⑥ Q<Mp ならば，とりあえず 次 ⑦ へ。
Q＝Mp ならば，Mp の 約数 は，1 と
Mp＝2^P－1 のみで，Mp は 素数。
⑦ Q を 8 で 割って，余りが 7 または 1 ，
であれば，次 ⑧ へ。余りが 5 または 3 で
あれば，Mp の 約数 にならないので ④ へ。
⑧ Q は 素数 か 合成数 か を 調べる。素数
か否か 解らなければ，とりあえず 次 ⑨ へ。
Q が 合成数 ならば，Mp の 約数にならな
いので ④ へ。Q が 素数 ならば，次 ⑨ へ。
⑨ Q の TL(Thred Length) を 計算 する。
TL(Q) ≦ Q－1 である。
⑩ TL(Q)＝P であれば，Mp＝2^P－1 は，
約数 Q を 持つ。従って，MP は 合成数。
TL(Q)≠P であれば，④ に戻る。

7．おわりに

メルセンヌ素数の発見者に，まだ日本人の名前は無い。組織的に探索する方法は無いものだろうか。ＩＰＳＪ の 会員の名前 ならば良い。自分の名前ならば 尚更であるが 余命の間に 発見できるとは思えない。せめて，メルセンヌ素数の候補を絞っておくべきであろうか。

謝辞：本稿を作成するに当たり，適切なパソコンとＯＳ環境を 使わせて頂いている，(財)機械産業記念事業財団 ハイテク情報サービス室 に 感謝します。また，フリーソフトウェアの「ＵＢＡＳＩＣ」使わせて 頂けるように された，木田祐司 先生に，感謝いたします。

参考資料：

1．パーソナル コンピュータ ユーザ 利用技術協会 機関誌 パソコンリテラシー 1999-9月号（ 林 ）
2．情報処理学会 第５９回 全国大会［１Ｇ-０２］

参考 インターネット・ホームページ

UBASIC Home Page
http://math.rikkyo.ac.jp/~kida/
The Great Internet Mersenne Prime Search
http://www.mersenne.org/prime.htm

＊ E-mail ： hhayashi@tepia.or.jp