メルセンヌ 素数 の 篩(ふるい)の アルゴリズム(算法)

1G－2

an Algorithm of the Cieve for Mercenne Prime Numbers

(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 篩(ふるい)の アルゴリズムのように，メルセンヌ数の(素数)と(合成数)とを篩(ふるい)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，１９９９年８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,…
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。
Ｈ　：　１／Ｋ の 二進循環小数の循環節の整数値。

3．ＴＲＯＮ数，(Thred Length：TL)

The Segment Length of the Recurring Period of The Reciprocal of Odd Number(K≧3) using Binary Notation, should be called as "TRON" number, or merely Thred Length, or (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)
bin(1/ 5)=0.0011…(TL=4)
bin(1/ 7)=0.001…(TL=3)
bin(1/ 9)=0.000111…(TL=6)
bin(1/11)=0.0001011101…(TL=10)
bin(1/13)=0.000100111011…(TL=12)
bin(1/15)=0.0001…(TL=4)
bin(1/17)=0.0001111…(TL=8)
bin(1/19)=0.000011010111100101…(TL=18)
```

4．循環小数と分数(分子／分母)の関係

The relations between Recurring Decimals and Fractional notation (Numerator / Denominator) are likely both Decimal and Binary Notation.

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。 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。

更に,この メルセンヌ数 は,合成数であり,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。 但し，Ｈ＝１ の 場合,分母 は １ と Ｋ 自身 が 約数 に なるので 素数 であり，Ｐ＝(２＾ＴＬ－１) は 素数。

図表 4a

$\frac{1}{P} = \frac{H}{111\cdots\cdots1}$	分母は二進の←記述である。
◀——TL——▶	
1/P の循環節長(ＴＬ)：Thred Length	

Ｐ は ３以上の素数。 分母 は (２＾ＴＬ－１) 即ち，分母 は 二進 ＴＬ桁 の メルセンヌ数。
２＾ＴＬ－１／Ｐ＝Ｈ：循環節を整数化した値。
但し， Ｈ＝１ ならば Ｐ は メルセンヌ素数。
Ｈ＞１ならば Ｐ は メルセンヌ素数 ではない。

図表 4b

１／Ｐ の 二進循環節長 ＴＬ が 素数(Ｑ)である場合は，(２＾Ｑ－１) の メルセンヌ型の数 Ｍｑ は，約数 Ｐ を 持つ。Ｐ≠Ｍｑ であれば，Ｍｑ は メルセンヌ素数 ではない。

5．メルセンヌ素数 の 篩(Mp Ｃｉｅｖｅ)

Ｍｐ を 見つける アルゴリズム を 提案する。

① 素数(Ｐ)を 小さい順に 並べて 表 にする。

② 素数 の 二進循環節長(ＴＬ)と メルセンヌ数(Mn)＝(２＾Ｐ－１) は，算出 できる。

③ 素数表 に 残っている 素数 の 最小 の もの から，その 数 の 二進循環節長(ＴＬ)を 求める。 (注),(ＴＬ)は(Ｐ)より 小 である。

④ ＴＬ が，素数 であるか否かを 調べる。即ち，素数表 で Ｐ より 小さい 部分から 検索する。

⑤ もし，ＴＬ が 素数(Ｑ)であれば，(Ｍｑ)＝(２＾Ｑ－１)は，合成数 であるから，素数 Ｑ を メルセンヌ素数 の 候補 から 削除する。

⑥ ⑤で，ＴＬ が 素数(Ｑ)であって，(Ｍｑ)＝(２＾Ｑ－１)＝Ｐ であれば，Ｍｑ は Ｐ より 小さい約数 が 無いので，メルセンヌ素数として 確定 されて，篩(ふるい)分けられる。

⑦ 表 の 中に 残っている 数 が 無くなるまで③ の 手順 に 戻って 繰り返す。

図表 5

	2		3	2	5	4	7	3
確定→	3		7		31		127	
	11	10	13	12	17	8	19	18
削除→	2047		8191		131071		524287	
	23	11	29	28	31	5	37	36
削除→	8388607		5.4E+08		2.1E+09		1.4E+11	
	41	20	43	14	47	23	53	52
未定→	2.2E+12		8.8E+12		1.4E+14		9E+15	
	61	60	67	66	71	35	73	9
未定→	2.3E+18		1.5E+20		2.4E+21		9.4E+21	
：	79	39	83	82	89	11	97	48
：	6E+23		9.7E+24		6.2E+26		1.6E+29	
：	101	100	103	51	107	106	109	36
：	2.5E+30		1E+31		1.6E+32		6.5E+32	
：	113	28	127	7	131	130	137	68
	1E+34		1.7E+38		2.7E+39		1.7E+41	

(注)

P	TL
2^P-1	

TL が 素数 Q ならば,P は 2^TL-1 の 素数 Q を 整除 するので，Q を メルセンヌ素数 の 候補 から 削除 する。但し，2^Q-1＝P ならば,Q は メルセンヌ素数として,確定される。2,3,5,7 は 確定。11 は 約数 に 23,89 が 見つけられた。23 は 47…。

6．篩(ふるい)落とされた Ｑ の 分布

図表 6

数 の 範囲	素数累計	Ｐ 分布	Ｑ 分布	Ｑ／Ｐ
～1,000,000	78,498	78,498	3,846	4.90%
～2,000,000	148,933	70,435	2,958	4.20%
～3,000,000	216,816	67,883	2,713	4.00%
～4,000,000	283,146	66,330	2,622	3.95%
～5,000,000	348,513	65,367	2,621	4.01%
～6,000,000	412,849	64,336	2,457	3.82%
～7,000,000	476,648	63,799	2,429	3.81%
～8,000,000	539,777	63,129		
～9,000,000	602,489	62,712		
～10,000,000	664,579	62,090		

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,フリーソフトの「ＵＢＡＳＩＣ」を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.ＵＢＡＳＩＣによるコンピュータ整数論
木田祐司・牧野潔夫共著 日本評論社 1994
3.ＵＢＡＳＩＣ ８６ 多倍長計算用ＢＡＳＩＣ
ＵＢＡＳＩＣ８６［第8.7版］ユーザーズ・マニュアル 木田祐司著 日本評論社 1994
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