素　数　(Prime Numbers)

会員　堀　城之

序

素数とは、１と自身以外では割れない数をいう。

素数と技術とは結びつけられている。NHK スペシャルで「魔性の難問、～リーマン予想・天才たちの闘い～」を視聴した方は素数が暗号化技術と関わっていることをご存じであろう。暗号化と素数とキーワードとしてＩＰＤＬで検索すると６０００件以上ヒットする。まず、素数の基本的事項について説明する。次いで、素数を使った暗号化技術のクレームを紹介する。最後に、筆者が独自に作成したプログラムで計算した素数階段の距離について、１０万桁で面白い結果が出たので記載する。

１．レオンハルト・オイラーの発見

以下に示す式をオイラー級数という。

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots+\frac{1}{n^2}+\cdots \qquad (1.0)$$

ｎは自然数であり、無限に続く。そして、ついにオイラーは以下の式を導いた。

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6} \quad (1.1)$$

素数との関係を以下に示す。上式の証明にはもうワンクッションある。実は、オイラー級数（ｓ＝２）は、以下のように表すことも可能である。

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\prod_{P}^{\infty}\frac{1}{1-p^{-2}} \qquad \text{P: Prime number} \qquad (1.2)$$

$$\prod_{P}^{\infty}\frac{1}{1-p^{-2}}=\frac{1}{1-2^{-2}}*\frac{1}{1-3^{-2}}*\frac{1}{1-5^{-2}}*\frac{1}{1-7^{-2}}*\frac{1}{1-11^{-2}}\cdots$$

自然数の級数が、素数の積で表されるのである。故に式（１．１）は素数に関係有るのである。これだけでも筆者は素数の不思議さが分かる。

証明については、非常に明解である。

まず式（１．０）の両辺に第１素数２の－２乗をかける。

$$\frac{1}{2^2}\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{1}{2^2}+\frac{1}{4^2}+\frac{1}{6^2}+\cdots \qquad (1.3)$$

式（１．０）―（１．３）は、

$$(1-\frac{1}{2^2})\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{1}{1^2}+\frac{1}{3^2}+\frac{1}{5^2}+\cdots \qquad (1.4)$$

次に、式（１．４）の両辺に第１素数３の－２乗をかけると、

$$\frac{1}{3^2}(1-\frac{1}{2^2})\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{1}{3^2}+\frac{1}{9^2}+\frac{1}{15^2}+\cdots \qquad (1.5)$$

式（１．４）－（１．５）は、

$$(1-\frac{1}{3^2})(1-\frac{1}{2^2})\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{1}{1^2}+\frac{1}{5^2}+\frac{1}{7^2}+\cdots \qquad (1.6)$$

これを繰り返すと、

$$\left(1-\frac{1}{p^2}\right)\ldots\left(1-\frac{1}{5^2}\right)\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{2^2}\right)\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{1}{1^2} \qquad (1.7)$$

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{1}{\left(1-\frac{1}{p^2}\right)\ldots\left(1-\frac{1}{5^2}\right)\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{2^2}\right)}$$

∴

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\prod_{P}^{\infty}\frac{1}{1-p^{-2}}$$

故に、式（１．２）が証明された。コロンブスの卵。

次に、式（１．１）を示す。

sin$x$ をテーラー展開すると、

$$sinx=x-\frac{x^3}{3!}+\frac{x^5}{5!}-\frac{x^7}{7!}+\cdots+(-1)^{n+1}\frac{x^{2n-1}}{(2n-1)!}+\cdots \quad (1.8)$$

両辺を x で割ると、

$$\frac{sinx}{x}=1-\frac{x^2}{3!}+\frac{x^4}{5!}-\frac{x^6}{7!}+\cdots+(-1)^{n+1}\frac{x^{2n-1-1}}{(2n-1)!}+\cdots (1.9)$$

$$f(x)=\frac{sinx}{x}\quad(1.10)$$

とすると、

$$f(0)=1$$

x として有意な解が有るためには、

$$sinx=0\ \text{thus}\ x=n\pi\ (n:integer)$$

よって、式（１．１０）は、

$$f(x)=\left(1-\frac{x}{\pi}\right)\left(1-\frac{x}{-\pi}\right)\left(1-\frac{x}{2\pi}\right)\left(1-\frac{x}{-2\pi}\right)\left(1-\frac{x}{3\pi}\right)\left(1-\frac{x}{-3\pi}\right)\cdots\left(1-\frac{x}{n\pi}\right)\left(1-\frac{x}{-n\pi}\right)\quad(1.11)$$

$$f(x)=\left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{4\pi^2}\right)\left(1-\frac{x^2}{9\pi^2}\right)\cdots\left(1-\frac{x^2}{n\pi^2}\right)\cdots\quad(1.12)$$

オイラー級数の乗数である、２乗項だけを展開すると、

$$\frac{x^2}{3!}=\left(\frac{1^2}{\pi^2}+\frac{x^2}{4\pi^2}+\frac{x^2}{9\pi^2}+\cdots+\frac{x^2}{n\pi^2}+\cdots\right)x^2$$

$$=\frac{1^2}{\pi^2}\left(\frac{x^2}{4\pi^2}+\frac{x^2}{9\pi^2}+\cdots+\frac{x^2}{n\pi^2}+\cdots\right)x^2\quad(1.13)$$

係数は、

$$\frac{1}{3!}=\frac{1^2}{\pi^2}\sum_{n=1}^{\infty}\frac{1}{n^2}$$

$$\therefore\quad\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}$$

式（１．１）の証明終わり。流石オイラー。

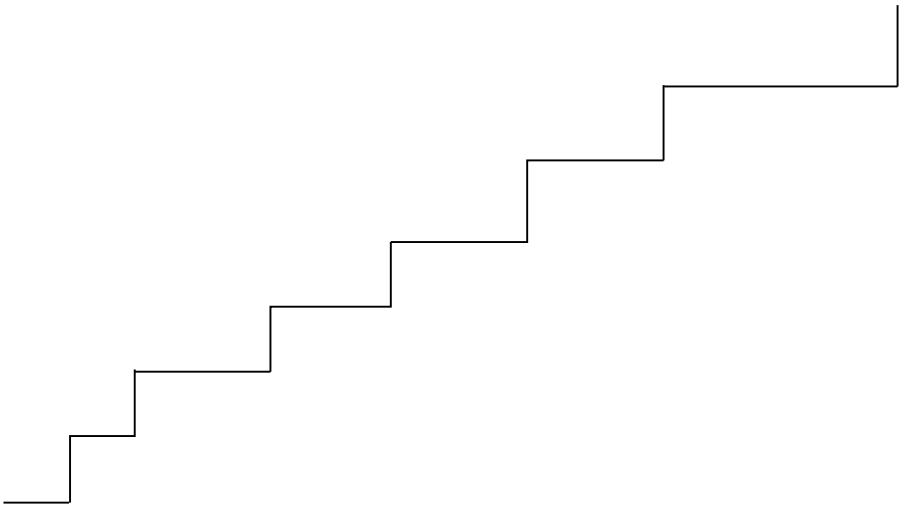
“自然数の無限級数”が“素数”の無限積になる。素数の無限積がパイのみに関わる。不思議だ。紙と鉛筆で証明すると不思議さに感動する。

２．ヨハン・カール・フリードリヒ・ガウスの発見

１０万までの素数リストを添付した。現在、“１”も１と自身以外では割れないが、１は素数ではないというのが現在の主流である。素数リストを眺めていると非常に興味深い事が分かる。隣接する素数との間隔がバラバラである。秩序が、有りそうで無い、無さそうで有る。もし、間違いがあったらご指摘頂けると有り難い。

ガウスは、素数階段を作った。素数階段は、素数が見つかると１段上が

り、水平方向距離を隣接素数の差分としたものが素数階段である。



１　２　３　４　５　６　７　８　９　１０　１１　１２　１３

ガウスは、素数階段の高さ（段数＝素数個数関数）を、ｘをｘの対数で割ったものが、ｘが大きくなるにつれて１に近づくことを発見した。

X	pai(x)	x/ln x	pai(x)/x/lnx
10	4	4.34294481903251	0.92103403719762
100	25	21.71472409516250	1.15129254649703
1000	168	144.76482730108400	1.16050288686900
10000	1229	1,085.73620475813000	1.13195083171588
100000	9592	8,685.88963806502000	1.10431981059995
1000000	78498	72,382.41365054180000	1.08448994777908
10000000	664579	620,420.68843321600000	1.07117478896183
100000000	5761455	5,428,681.02379064000000	1.06129923175648

pai(x)＝素数個数関数

以上はエクセルで計算。１６桁以降はエクセルの限界で‘０’。

３．リーマン予想

（１）　リーマン予想とは、ベルンハルト・リーマンが予想した数学上の難問であり、以下に定義される。

ゼータ関数における非自明な０点は一直線上にある。当然 CMI は、ポアンカレ予想、ナビエ・ストークス方程式（知恵の話 24_Navie-Stokes eq）と同様に 100 万ドルの賞金を掛けている。

http://www.claymath.org/millenium-problems/riemann-hypothesis

ゼータ関数とは、オイラー級数の乗数を s とし s の関数として表したものを言う。

$$\zeta(\mathrm{s}) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad (4.1)$$

リーマンが命名したのでリーマンゼータ関数ともいう。

リーマンゼータ関数をオイラー積で表すと、

１．で記載した式（１．２）の証明過程は乗数には左右されない。

因って、オイラー積で表すことが出来る。

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{P}^{\infty} \frac{1}{1-p^{-s}} \qquad \text{P: Prime number} \qquad (4.2)$$

$$\prod_{P}^{\infty} \frac{1}{1-p^{-s}} = \frac{1}{1-2^{-s}} * \frac{1}{1-3^{-s}} * \frac{1}{1-5^{-s}} * \frac{1}{1-7^{-s}} * \frac{1}{1-11^{-s}} \cdots$$

０点とは、

$$\zeta(\mathrm{s}) = 0$$

のときを言う。

非自明とは、ｓが負の偶数以外の場合を言う。

（2）　非可換幾何学　(Noncommutative Geometry)

フランスの数学者のアラン・コンヌ（フィールズ賞受賞者）が、リーマン予想に関して非可換幾何学との関係を第１回世界リーマン予想会議において示唆した。現在、非可換幾何学により解けるのではないかと期待されている。

コンヌの非可換幾何学（Noncommutative Geometry）に関しては

http://www.alainconnes.org/en/downloads.php

からダウンできる。

どなたか一緒に輪講しませんか？

$$dim(e \wedge f) + dim(e \vee f) = dim(e) + dim(f) \;\; \forall\, e, f$$

４．素数と暗号化

素数は身近なところに存在する。例えば、暗号化である。代表的な暗号化方法である RSA も素数を用いている。読者の中にも RSA を用いて明細書を暗号化している方もいるかもしれない。RSA は、発明者であるロナルド・リベスト (Ron Rivest) 、アディ・シャミア (Adi Shamir) 、レオナルド・エーデルマン (Len Adleman) の頭文字である。3 人は 1983 年に米国で特許を取得している（4, 405, 829 号）。ただし、権利者は、当時の 3 人が属していたマサチューセッツ工科大学である。RSA は、クレジットカードの引き落とし等に利用されている。それ故、秘匿性が極めて高い技術と言える。

日本では特許は取られていないので、英文でクレームを記載する。素数に下線を引く。

A cryptographic communications system comprising:
A. a communications channel,
B. an encoding means coupled to said channel and adapted for transforming a transmit message word signal M to a ciphertext word signal C and for transmitting C on said channel,
where M corresponds to a number representative of a message and
$0 \leqq M \leqq n-1$
where n is a composite number of the form
$n=p \cdot q$
where p and q are prime numbers, and
where C corresponds to a number representative of an enciphered form of said message and corresponds to
$C \equiv M^e \pmod{n}$
where e is a number relatively prime to 1 cm(p-1,q-1), and
C. a decoding means coupled to said channel and adapted for receiving C from said channel and for transforming C to a receive message word signal M'
where M' corresponds to a number representative of a deciphered form of C and corresponds to
$M' \equiv C^d \pmod{n}$
where d is a multiplicative inverse of e(mod(1 cm((p-1),(q-1)))).

翻訳すると、
暗号通信システムであって、

A. 通信チャンネルと、
B. 前記チャンネルに接続され、暗号文単語信号 C への送信メッセージ単語信号 M の変形及び前記チャンネル上の C の送信に適した符号化手段と、
ここで、M がメッセージと 0≦M≦n の 1 の数代表に相当し
n が形式の合成数であり、
n=p・q
p と q が素数であり、
C は、前記メッセージの暗号化された形式の数代表に相当し,
且つ C≡Me(mod n)に 対応し、
e は、1cm(p-1、q-1)に関連する素数であり、
C. 前記チャンネルに接続され、前記チャンネルから受信メッセージ文書シグナル M'に受信し変換するのに適した符号化手段とを備え、
ここで M'は、
C の復号化形式の代表的な数であり、且つ
$M' \equiv C^d \pmod n$
であり、
d が e(mod (1cm((p-1),(q-1))))の逆数である
暗号通信システム。

ウィキペディアによれば、「鍵ペア（公開鍵と秘密鍵）を作成して公開鍵を公開する。まず、適当な正整数 e（通常は小さな数。(65537 =2^{16}+1) がよく使われる）を選択する。また、大きな 2 つの素数 $\{p, q\}$ を生成し、それらの積 n (=pq) を求めて、$\{e, n\}$ を平文の暗号化に使用する鍵（公開鍵）とする。2 つの素数 $\{p, q\}$ は、暗号文の復号に使用する鍵（秘密鍵）d の生成にも使用し

($d = e^{-1} \pmod{(p-1)(q-1)}$) 、秘密に保管する。

- 暗号化（平文 m から暗号文 c を作成する）： $c = m^e \mod n$
- 復号（暗号文 c から元の平文 m を得る）： $m = c^d \mod n$

ここで、暗号化（e 乗）は、$\{e, n\}$ があれば容易に計算できるのに対して、復号（e 乗根）は、「n の素因数を知らないと難しい（大きい合成数の素因数分解も難しい）」と考えられている。つまり秘密鍵を用いずに暗号文から平文を得ることは難しい、と信じられている。これが RSA 暗号の安全性の根拠である。」

つまり、自身以外では因数分解できないから、恐ろしく巨大な素数をｐ、ｑにとれば、誰も解読できない可能性が極めて高いということになるのである。

５．素数階段の距離

筆者は、添付の素数リストを使って、隣接素数の差分（素数階段の１段の距離）の出現頻度をエクセルで計算してみた。

A:差分　B：出現頻度　C:A*B　D:log B　E:log C

A	B	C	D	E
2	1224	2448	7.109879	7.803027
3	0	0	#NUM!	#NUM!
4	1215	4860	7.102499	8.488794
5	0	0	#NUM!	#NUM!
6	1940	11640	7.570443	9.362203
7	0	0	#NUM!	#NUM!
8	773	6184	6.650279	8.729721
9	0	0	#NUM!	#NUM!
10	916	9160	6.820016	9.122601
11	0	0	#NUM!	#NUM!
12	964	11568	6.871091	9.355998
13	0	0	#NUM!	#NUM!
14	484	6776	6.182085	8.821142
15	0	0	#NUM!	#NUM!
16	339	5424	5.826	8.598589
17	0	0	#NUM!	#NUM!
18	514	9252	6.242223	9.132595
19	0	0	#NUM!	#NUM!
20	238	4760	5.472271	8.468003
21	0	0	#NUM!	#NUM!
22	223	4906	5.407172	8.498214
23	0	0	#NUM!	#NUM!
24	206	4944	5.327876	8.50593
25	0	0	#NUM!	#NUM!
26	88	2288	4.477337	7.735433
27	0	0	#NUM!	#NUM!
28	98	2744	4.584967	7.917172
29	0	0	#NUM!	#NUM!
30	146	4380	4.983607	8.384804

31	0	0	#NUM!	#NUM!
32	32	1024	3.465736	6.931472
33	0	0	#NUM!	#NUM!
34	33	1122	3.496508	7.022868
35	0	0	#NUM!	#NUM!
36	54	1944	3.988984	7.572503
37	0	0	#NUM!	#NUM!
38	19	722	2.944439	6.582025
39	0	0	#NUM!	#NUM!
40	28	1120	3.332205	7.021084
41	0	0	#NUM!	#NUM!
42	19	798	2.944439	6.682109
43	0	0	#NUM!	#NUM!
44	5	220	1.609438	5.393628
45	0	0	#NUM!	#NUM!
46	4	184	1.386294	5.214936
47	0	0	#NUM!	#NUM!
48	3	144	1.098612	4.969813
49	0	0	#NUM!	#NUM!
50	5	250	1.609438	5.521461
51	0	0	#NUM!	#NUM!
52	7	364	1.94591	5.897154
53	0	0	#NUM!	#NUM!
54	4	216	1.386294	5.375278
55	0	0	#NUM!	#NUM!
56	1	56	0	4.025352
57	0	0	#NUM!	#NUM!
58	4	232	1.386294	5.446737
59	0	0	#NUM!	#NUM!
60	1	60	0	4.094345
61	0	0	#NUM!	#NUM!
62	1	62	0	4.127134
63	0	0	#NUM!	#NUM!
64	1	64	0	4.158883
65	0	0	#NUM!	#NUM!
66	0	0	#NUM!	#NUM!

67	0	0	#NUM!	#NUM!
68	0	0	#NUM!	#NUM!
69	0	0	#NUM!	#NUM!
70	0	0	#NUM!	#NUM!
71	0	0	#NUM!	#NUM!
72	1	72	0	4.276666

図 B

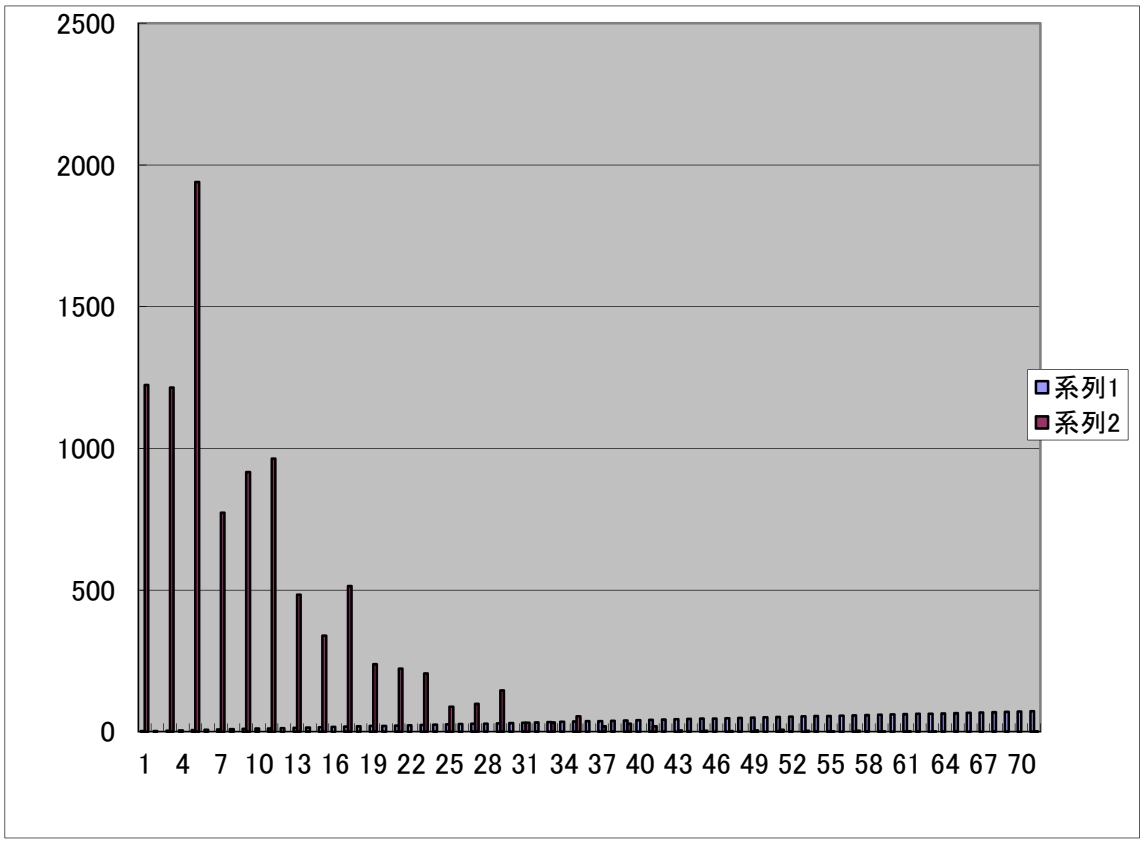


図 C

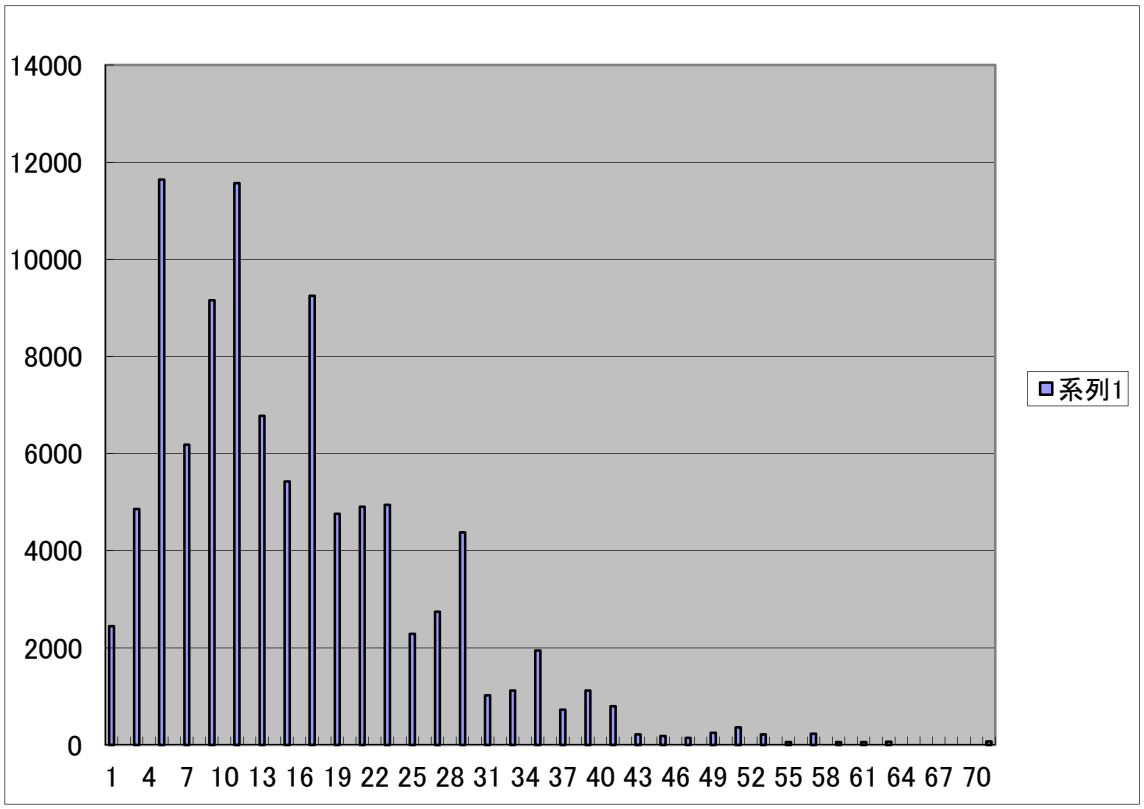

14000
12000
10000
8000
6000
4000
2000
0
1 4 7 10 13 16 19 22 25 28 31 34 37 40 43 46 49 52 55 58 61 64 67 70
系列1

図 D

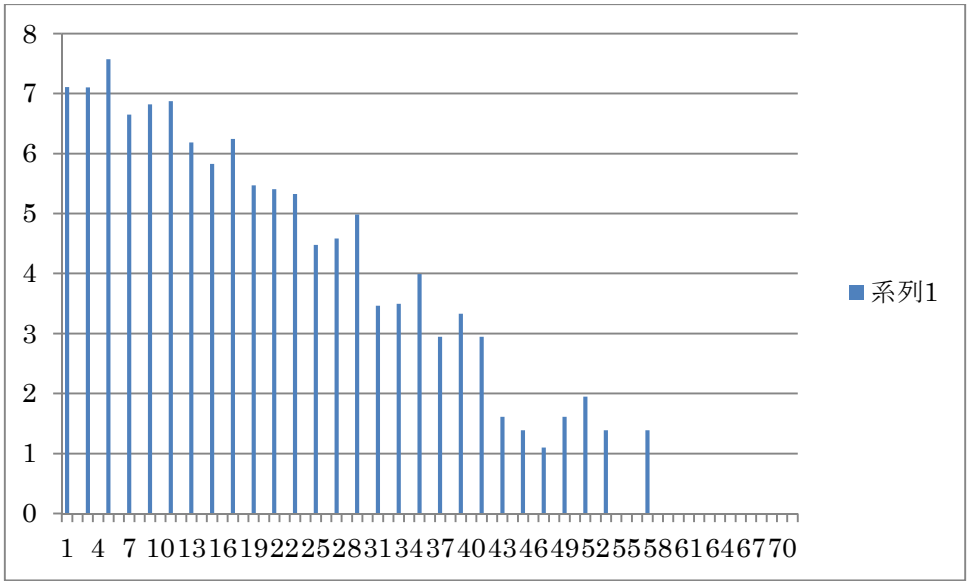

8
7
6
5
4
3
2
1
0
1 4 7 10131619222528313437404346495255586164670
系列1

図 E

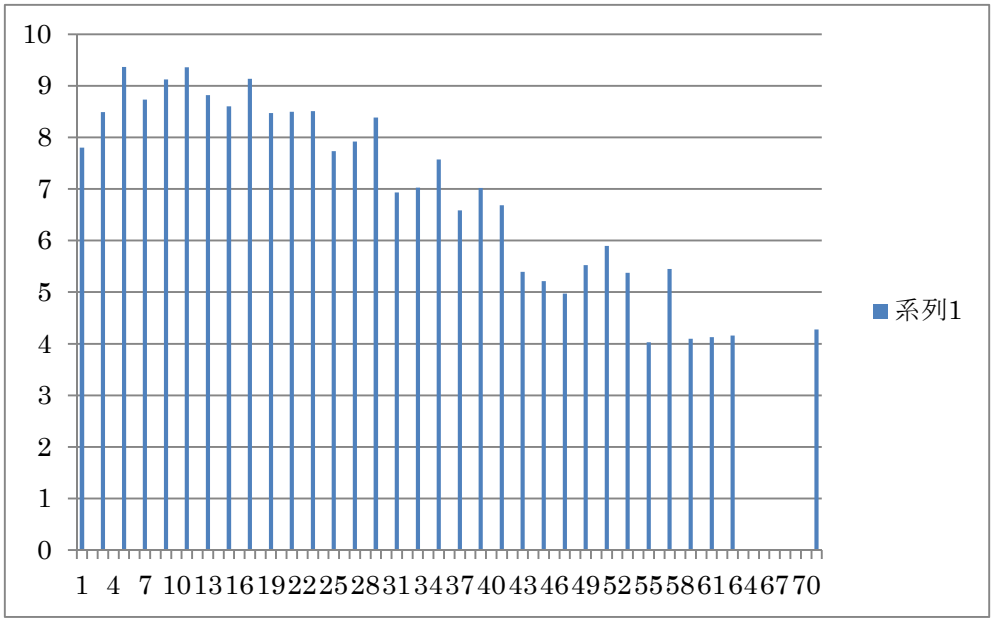


図 B を見ると‘６’が突出している。

６は最も小さい完全数である。完全数とは約数の和が当該数と一致する数である。

１＋２＋３＝６

なぜ、６が多いのか。不思議である。自分で検証してみないと分からないものである。

筆者が求めたのは、素数は１０万までであった。１００万、１０００万、１億とやってみたいが、筆者が持っているエクセルでは不可能である。ますます６が立ってくるか、或いは平準化するか、興味があるところである。

なお、C,D,E,F については特徴的な部分は見られない。

６．６について（セクシー素数）

セクシー素数とは、（ｐ、ｐ＋６，ｐ＋１２，…）の組み合わせを言う。つまり、セクシー素数は、素数階段の距離が６の組み合わせである。セクシーとは６の意味である。筆者が５．で求めたのは隣接素数なのでセクシー素数とは完全一致ではない。しかし、セクシー素数がトピックになるのだから、前記差分が６というのも何らかの意味が有るのかもしれない。

７．あとがき

人は、なぜか素数に惹かれる。

素数年目に地上に出てくる蝉がいる。生存確率が一番高いのであろう。

生物の遺伝子に素数が関係あるのかもしれない。

以上