INTRODUCING FERMAT SEQUENCES

Ridlo W. Wibowo[1,2]

[1]**Astronomy Department, Institut Teknologi Bandung, Bandung, Indonesia**
[2]**European Southern Observatory, Santiago, Chile**
ridlo.w.wibowo@gmail.com

Abstract. The number of iteration used in the Fermats factorization method is related to the factor that the method found for each odd number. A new collection of sequence (we called it Fermats sequences) can be generated based on the factor that we found using this method. For example, the first member ($F_{[1]}$) in this collection of sequences is odd prime number sequence, which has factor–of course–of 1 and has highest number of iteration in the Fermats factorization, which is ∼half of the number itself. The next member is always composite number with interesting structure and also randomness related to the prime number distribution. First exploration of these new sequences (not registered in oeis.org yet) and the beauty of the location of these sequences in the Ulams and Sacks spiral will be presented.

Key words and Phrases: Fermat's factorization method, new integer sequences, prime number.

1. FERMAT'S FACTORIZATION

An odd integer N can always be represented by the difference between two square of integers (Eq 1), a and b for instance. This property is used in Fermat's factorization method to find the factors: c and d which are also odd integers,

$$N = a^2 - b^2 = (a+b)(a-b) = c \cdot d. \tag{1}$$

Other relation can also be derived: $a = (c+d)/2$ and $b = (c-d)/2$.

This method starts from ceiling the square root value of the number, $a = \lceil\sqrt{N}\rceil$. Iteration of $a \mathrel{+}= 1$ is then carried out until we find its pair, $b = a^2 - N$, to be a perfect square. We will get Fig 1, if we plot the number of iteration needed to find the factor of odd integers using this method. I found this graph in 2013 when I play with this method in a homework from a computational class, yet at that time I can not explain this graph directly and not to interested in this result. Lately, I understand how this plot produced and also I found that the sequences resulted from this method is interesting.

Fermat's method is efficient if c/d is close to 1. One example is if N an odd square, then this method only needs 0 step. On the other hand, it requires a considerable number of trials when c/d is much larger than 1. The most extreme case would be if N is a large prime number. Fermat's method will spend $(N+1)/2 - \lceil\sqrt{N}\rceil$ steps to finish the procedure. This is not efficient to perform a primality test ($\mathcal{O}(N)$ steps). In general, the required total number of steps ($n_{\rm iter}$) can be approximated by

$$n_{\rm iter} = a_{\rm found} - a_{\rm initial} \approx \frac{(c+d)}{2} - \sqrt{N} = \frac{(\sqrt{c}-\sqrt{d})^2}{2} = \frac{(\sqrt{N}-d)^2}{2d}. \tag{2}$$

2000 Mathematics Subject Classification:
Received: dd-mm-yyyy, accepted: dd-mm-yyyy.

Evidently, when N is enormous compared to d, the number of steps in this method becomes $n_{\text{iter}} \approx N/2d$. This formula explain "lines" structure in Fig 1.

Now, we can try to solve quadratic equation in Eq 2,

$$\begin{aligned} n_{\text{iter}} &\approx \frac{(\sqrt{N}-d)^2}{2d} \\ 0 &\approx d^2 - 2(\sqrt{N}+n_{\text{iter}})d + N \\ c \text{ and } d &\approx \left(\sqrt{N}+n_{\text{iter}}\right) \pm \left(\sqrt{2\sqrt{N}n_{\text{iter}} + n_{\text{iter}}^2}\right) \end{aligned} \tag{3}$$

Two terms in the parenthesis are a and b. Eq 3 gives us bounds and relation between the number N, factors (c and d), and the number of iteration in Fermat's method.

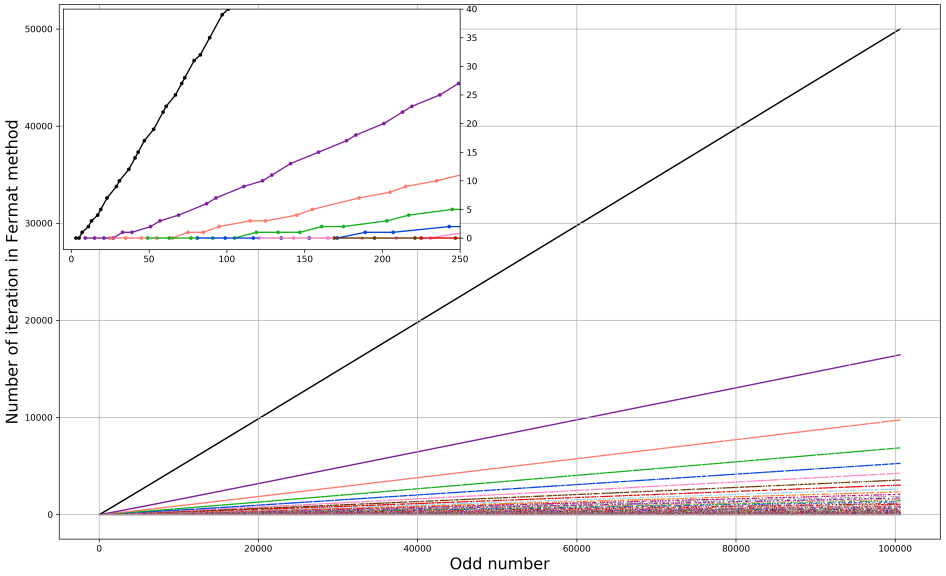

FIGURE 1. Number of iteration (n_{iter}) in Fermat's factorization for each odd number N. Each point are colored based on the factor of d found in Fermat's method. For $d = 1$ (black), all the member are odd prime number; the next color are for $d = 3, 5, 7, 9, 11, \ldots$. As N become larger, the trend $n_{\text{iter}} \approx N/2d$ appear in this plot.

2. FERMAT SEQUENCES/SETS

If we divide the odd integers based on the factor d that the Fermat's method found (i.e. coloring in Fig 1), we can make several "sequences" or "sets" of number. I will call it Fermat sequences, and more specifically Fermat d-sequences ($F_{[d]}$, d is

odd number). Several member of this d-sequences are listed below:

$$\begin{aligned}
F_{[1]} &= (1), 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, \ldots \\
F_{[3]} &= 9, 15, 21, 27, 33, 39, 51, 57, 69, 87, 93, 111, 123, 129, 141, 159, 177, 183, \ldots \\
F_{[5]} &= 25, 35, 45, 55, 65, 75, 85, 95, 115, 125, 145, 155, 185, 205, 215, 235, 265, \ldots \\
F_{[7]} &= 49, 63, 77, 91, 105, 119, 133, 147, 161, 175, 203, 217, 245, 259, 287, 301, \ldots \\
F_{[9]} &= 81, 99, 117, 135, 153, 171, 189, 207, 243, 261, 279, 333, 369, 387, 423, \ldots \\
F_{[11]} &= 121, 143, 165, 187, 209, 231, 253, 275, 297, 319, 341, 363, 385, 407, 451, \ldots \\
F_{[13]} &= 169, 195, 221, 247, 273, 299, 325, 351, 377, 403, 429, 455, 481, 507, 533, \ldots
\end{aligned}$$

These d-sequences always start from d^2. Each of d-sequence progress with an arithmetic progression of $2d$, except for $F_{[1]}$ which are odd primes. Pseudo-Fermat sequences are sequences with formula:

$$\text{Pseudo–}F_{[d]}(i) = d^2 + 2d \cdot i = d(d + 2i) \qquad d = 3, 5, 7, 9, ... \qquad i = 0, 1, 2, 3, ... \quad (4)$$

but some of the terms are missing and appear in other sequences, e.g. 45 and 75 are missing from $F_{[3]}$ but appear in $F_{[5]}$, 63 appear in $F_{[7]}$, 81 appear in $F_{[9]}$, and so on.

We can also say that these d-sequence are product of odd number d and odd number equal or greater than d, but missing some of terms. In that sense, we can look for the behaviour of these sequences in multiplication table of odd number like shown in Fig 2.

- The missing part are maybe the main interest.
- First member are d^2, second member is $n^2 - 1$, third member, $n^2 - 4$, forth member $n^2 - 9$, start from fifth member this structure have some missing early terms because already appear before. (like d-sequences)

3. ULAM AND SACKS SPIRAL

4. DISCUSSION

- Fermat's and trial division
- Sieve improvement
- Or is this property/sequences can be used as a new sieving method?
- Relation with quadratic sieve?
- Relation with rational sieve?
- Relation with general number field sieve?
- Is there any relation with arithmetic progression on primes?
- Strip based on prime or composite multiplier in multiplication table.
- Smooth number and Rough number
- These sequence ditribution and prime distribution
- Modular arithmatic?

Acknowledgement. This work is mainly done in free time (sometimes not) during author's PhD life, which is supported by ESO studentship and Voucher ITB scholarship.

N	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39
1	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39
3	3	9	15	21	27	33	39	45	51	57	63	69	75	81	87	93	99	105	111	117
5	5	15	25	35	45	55	65	75	85	95	105	115	125	135	145	155	165	175	185	195
7	7	21	35	49	63	77	91	105	119	133	147	161	175	189	203	217	231	245	259	273
9	9	27	45	63	81	99	117	135	153	171	189	207	225	243	261	279	297	315	333	351
11	11	33	55	77	99	121	143	165	187	209	231	253	275	297	319	341	363	385	407	429
13	13	39	65	91	117	143	169	195	221	247	273	299	325	351	377	403	429	455	481	507
15	15	45	75	105	135	165	195	225	255	285	315	345	375	405	435	465	495	525	555	585
17	17	51	85	119	153	187	221	255	289	323	357	391	425	459	493	527	561	595	629	663
19	19	57	95	133	171	209	247	285	323	361	399	437	475	513	551	589	627	665	703	741
21	21	63	105	147	189	231	273	315	357	399	441	483	525	567	609	651	693	735	777	819
23	23	69	115	161	207	253	299	345	391	437	483	529	575	621	667	713	759	805	851	897
25	25	75	125	175	225	275	325	375	425	475	525	575	625	675	725	775	825	875	925	975
27	27	81	135	189	243	297	351	405	459	513	567	621	675	729	783	837	891	945	999	1053
29	29	87	145	203	261	319	377	435	493	551	609	667	725	783	841	899	957	1015	1073	1131
31	31	93	155	217	279	341	403	465	527	589	651	713	775	837	899	961	1023	1085	1147	1209
33	33	99	165	231	297	363	429	495	561	627	693	759	825	891	957	1023	1089	1155	1221	1287
35	35	105	175	245	315	385	455	525	595	665	735	805	875	945	1015	1085	1155	1225	1295	1365
37	37	111	185	259	333	407	481	555	629	703	777	851	925	999	1073	1147	1221	1295	1369	1443
39	39	117	195	273	351	429	507	585	663	741	819	897	975	1053	1131	1209	1287	1365	1443	1521
41	41	123	205	287	369	451	533	615	697	779	861	943	1025	1107	1189	1271	1353	1435	1517	1599
43	43	129	215	301	387	473	559	645	731	817	903	989	1075	1161	1247	1333	1419	1505	1591	1677
45	45	135	225	315	405	495	585	675	765	855	945	1035	1125	1215	1305	1395	1485	1575	1665	1755
47	47	141	235	329	423	517	611	705	799	893	987	1081	1175	1269	1363	1457	1551	1645	1739	1833
49	49	147	245	343	441	539	637	735	833	931	1029	1127	1225	1323	1421	1519	1617	1715	1813	1911
51	51	153	255	357	459	561	663	765	867	969	1071	1173	1275	1377	1479	1581	1683	1785	1887	1989
53	53	159	265	371	477	583	689	795	901	1007	1113	1219	1325	1431	1537	1643	1749	1855	1961	2067
55	55	165	275	385	495	605	715	825	935	1045	1155	1265	1375	1485	1595	1705	1815	1925	2035	2145

Figure 2. Multiplication table of odd number.

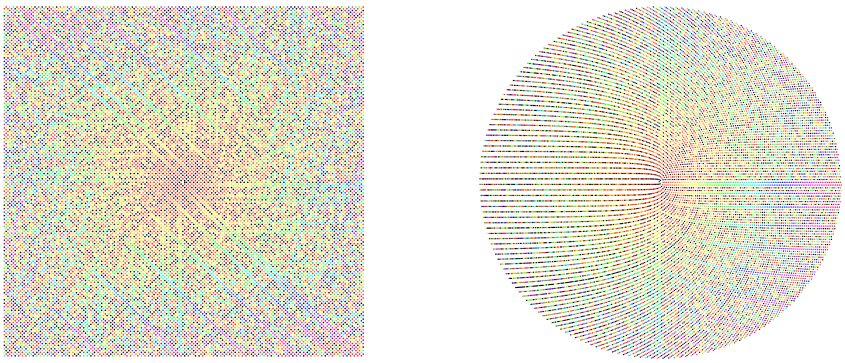

Figure 3. Ulam and Sacks spiral

REFERENCES

[1] Lehman, R. Sherman, "Factoring Large Integers", *Mathematics of Computation* **28** (1974): 637 - 646.