FACTORS AND PRIMES IN TWO SMARANDACHE SEQUENCES

RALF W. STEPHAN

ABSTRACT. Using a personal computer and freely available software, the author factored some members of the Smarandache consecutive sequence and the reverse Smarandache sequence. Nearly complete factorizations are given up to Sm(80) and RSm(80). Both sequences were excessively searched for prime members, with only one prime found up to Sm(840) and RSm(750): RSm(82)= $828180\cdots10987654321$.

1. INTRODUCTION

Both the Smarandache consecutive sequence, and the reverse Smarandache sequence are described in [S93]. Throughout this article, Sm(n) denotes the nth member of the consecutive sequence, and RSm(n) the nth member of the reverse sequence, e.g. Sm(11)=1234567891011, and RSm(11)=1110987654321.

The Fundamental Theorem of Arithmetic states that every $n \in \mathbf{N}$, $n > 1$ can be written as a product $p_1 p_2 p_3 \ldots p_k$ of a finite number of primes. This "factorization" is unique for n if the p_k are ordered by size. A proof can be found in [R85].

Factorization of large numbers has rapidly advanced in the past decades, both through better algorithms and faster hardware. Although there is still no polynomial-time algorithm known for finding prime factors p_k of composite numbers $n = \prod p_k$, several methods have been developed that allow factoring of numbers with 100 digits or more within reasonable time:

- the elliptic curve method (ECM) by Lenstra [L87], with enhancements by Montgomery [M87][M92] and others, has found factors with up to 49 digits, as of April 1998. Its running time depends on the size of the unknown p, and only slightly on the size of n.
- the quadratic sieve [S87] and the number field sieve [LL93]. The running time of these methods depends on the size of n. Factors with 60-70 digits are frequently found by NFSNet[1].

For $\log p \gg 50$ and $\log n / \log p \approx 2$, sieving methods are faster than ECM. Because ECM time depends on p, which is unknown from the start, it is difficult to predict when a factor will be found. Therefore, when fully factoring a large number, one tries to eliminate small factors first, using conventional sieving and other methods, then one looks for factors with 20, 30, and 40 digits using ECM, and finally, if there is enough computing power, one of the sieving methods is applied.

The primality of the factors and the remaining numbers is usually shown first through a probabilistic test [K81] that has a small enough failure probability like 2^{-50}. Such a prime is called a probable prime. Proving primality can be done using number theory or the ECPP method by Atkin/Morain [AM93].

[1] *URL:* `http://www.dataplex.net/NFSNet/`

In the following, p_n denotes a probable prime of n digits, P_n is a proven prime with n digits, and c_n means a composite number with n digits.

2. Free software

For computations with large numbers, it is not necessary to buy one of the well known Computer Algebra software packages like Maple or Mathematica. There are several multiprecision libraries freely available that can be used with the programming language C. The advantage of using one of these libraries is that they are usually by an order of magnitude faster than interpreted code when compared on the same machine [Z98].

For factoring, we used `science0`[2] and `GMP-ECM`[3]. To write the program for finding prime members of $\mathrm{Sm}(n)$ and $\mathrm{RSm}(n)$, we used the `GMP`[4] multiprecision library. For proving primality of $\mathrm{RSm}(82)$, we used `ECPP`[5].

3. Factorization results

We used `science0` to eliminate small factors of $\mathrm{Sm}(n)$ and $\mathrm{RSm}(n)$ with $1 < n \leq 80$, and `GMP-ECM` to find factors of up to about 40 digits. The system is a Pentium 200 MHz running Linux[6].

The timings we measured for reducing the probability of a factor with specific size to $1/e$ are given in the following table:

$\log p$	$\log n$	B1	curves	time
20	40	$1.5 \cdot 10^4$	100	7 minutes
30	60	$3 \cdot 10^5$	780	23 hours
40	80	$4 \cdot 10^6$	4800	107 days

Table 1. Time to find p with probability $1 - 1/e$ on a Pentium 200 MHz using `GMP-ECM` under Linux

All remaining composites were searched with ECM parameter B1=40000 and 200 curves were computed. Therefore, the probability of a remaining factor with less than 24 digits is less than $1/e$. No primes were proven. The following tables list the results.

[2] *URL:* `http://www.perfsci.com`
[3] *URL:* `http://www.loria.fr/~zimmerma/records/ecmnet.html`
[4] *URL:* `http://www.matematik.su.se/~tege/gmp/`
[5] *URL:* `http://lix.polytechnique.fr/~morain/Prgms/ecpp.english.html`
[6] *URL:* `http://www.linux.org`

n	known factors of $\mathrm{Sm}(n)$
2	$2^2 \cdot 3$
3	$3 \cdot 41$
4	$2 \cdot 617$
5	$3 \cdot 5 \cdot 823$
6	$2^6 \cdot 3 \cdot 643$
7	$127 \cdot 9721$
8	$2 \cdot 3^2 \cdot 47 \cdot 14593$
9	$3^2 \cdot 3607 \cdot 3803$
10	$2 \cdot 5 \cdot 1234567891$
11	$3 \cdot 7 \cdot 13 \cdot 67 \cdot 107 \cdot 630803$
12	$2^3 \cdot 3 \cdot 2437 \cdot p_{10}$
13	$113 \cdot 125693 \cdot 869211457$
14	$2 \cdot 3 \cdot p_{18}$
15	$3 \cdot 5 \cdot p_{19}$
16	$2^2 \cdot 2507191691 \cdot p_{13}$
17	$3^2 \cdot 47 \cdot 4993 \cdot p_{18}$
18	$2 \cdot 3^2 \cdot 97 \cdot 88241 \cdot p_{18}$
19	$13 \cdot 43 \cdot 79 \cdot 281 \cdot 1193 \cdot p_{18}$
20	$2^5 \cdot 3 \cdot 5 \cdot 323339 \cdot 3347983 \cdot p_{16}$
21	$3 \cdot 17 \cdot 37 \cdot 43 \cdot 103 \cdot 131 \cdot 140453 \cdot p_{18}$
22	$2 \cdot 7 \cdot 1427 \cdot 3169 \cdot 85829 \cdot p_{22}$
23	$3 \cdot 41 \cdot 769 \cdot p_{32}$
24	$2^2 \cdot 3 \cdot 7 \cdot 978770977394515241 \cdot p_{19}$
25	$5^2 \cdot 15461 \cdot 31309647077 \cdot p_{25}$
26	$2 \cdot 3^4 \cdot 21347 \cdot 2345807 \cdot 982658598563 \cdot p_{18}$
27	$3^3 \cdot 19^2 \cdot 4547 \cdot 68891 \cdot p_{32}$
28	$2^3 \cdot 47 \cdot 409 \cdot 416603295903037 \cdot p_{27}$
29	$3 \cdot 859 \cdot 24526282862310130729 \cdot p_{26}$
30	$2 \cdot 3 \cdot 5 \cdot 13 \cdot 49269439 \cdot 370677592383442753 \cdot p_{23}$
31	$29 \cdot 2597152967 \cdot p_{42}$
32	$2^2 \cdot 3 \cdot 7 \cdot 45068391478912519182079 \cdot p_{30}$
33	$3 \cdot 23 \cdot 269 \cdot 7547 \cdot 116620853190351161 \cdot p_{31}$
34	$2 \cdot p_{50}$
35	$3^2 \cdot 5 \cdot 139 \cdot 151 \cdot 64279903 \cdot 4462548227 \cdot p_{37}$
36	$2^4 \cdot 3^2 \cdot 103 \cdot 211 \cdot p_{56}$
37	$71 \cdot 12379 \cdot 4616929 \cdot p_{52}$
38	$2 \cdot 3 \cdot 86893956354189878775643 \cdot p_{43}$
39	$3 \cdot 67 \cdot 311 \cdot 1039 \cdot 62161577813320317996884 69 \cdot p_{36}$
40	$2^2 \cdot 5 \cdot 3169 \cdot 60757 \cdot 579779 \cdot 4362289433 \cdot 79501124416220680469 \cdot p_{26}$
41	$3 \cdot 487 \cdot 493127 \cdot 32002651 \cdot p_{56}$
42	$2 \cdot 3 \cdot 127 \cdot 421 \cdot 22555732187 \cdot 45623714922273271251101 77 \cdot p_{34}$
43	$7 \cdot 17 \cdot 449 \cdot p_{72}$
44	$2^3 \cdot 3^2 \cdot 12797571009458074720816277 \cdot p_{52}$

continued...

n	known factors of $\mathrm{Sm}(n)$
45	$3^2 \cdot 5 \cdot 7 \cdot 41 \cdot 727 \cdot 1291 \cdot 2634831682519 \cdot 379655178169650473 \cdot p_{41}$
46	$2 \cdot 31 \cdot 103 \cdot 270408101 \cdot 374332796208406291 \cdot 389095182135512341316920 9 \cdot p_{28}$
47	$3 \cdot 4813 \cdot 679751 \cdot 4626659581180187993501 \cdot p_{53}$
48	$2^2 \cdot 3 \cdot 179 \cdot 1493 \cdot 1894439 \cdot 157719406241884267103235886 57 \cdot p_{46}$
49	$23 \cdot 109 \cdot 3251653 \cdot 2191196713 \cdot 53481597817014258108937 \cdot p_{47}$
50	$2 \cdot 3 \cdot 5^2 \cdot 13 \cdot 211 \cdot 20479 \cdot 160189818494829241 \cdot 46218039785302111919 \cdot p_{44}$
51	$3 \cdot 17708093685609923339 \cdot p_{73}$
52	$2^7 \cdot 43090793230759613 \cdot p_{76}$
53	$3^3 \cdot 7^3 \cdot 127534541853151177 \cdot p_{76}$
54	$2 \cdot 3^6 \cdot 79 \cdot 389 \cdot 3167 \cdot 13309 \cdot 69526661707 \cdot 8786705495566261913717 \cdot p_{51}$
55	$5 \cdot 768643901 \cdot 641559846437453 \cdot 1187847380143694126117 \cdot p_{55}$
56	$2^2 \cdot 3 \cdot c_{102}$
57	$3 \cdot 17 \cdot 36769067 \cdot 2205251248721 \cdot c_{83}$
58	$2 \cdot 13 \cdot c_{105}$
59	$3 \cdot 340038104073949513 \cdot c_{91}$
60	$2^3 \cdot 5 \cdot 97 \cdot 157 \cdot p_{104}$
61	$10386763 \cdot 35280457769357 \cdot p_{92}$
62	$2 \cdot 3^2 \cdot 1709 \cdot 329167 \cdot 1830733 \cdot c_{98}$
63	$3^2 \cdot 17028095263 \cdot c_{105}$
64	$2^2 \cdot 7 \cdot 17 \cdot 19 \cdot 197 \cdot 522673 \cdot 1072389445090071307 \cdot c_{89}$
65	$3 \cdot 5 \cdot 31 \cdot 83719 \cdot c_{113}$
66	$2 \cdot 3 \cdot 7 \cdot 20143 \cdot 971077 \cdot c_{111}$
67	$397 \cdot 183783139772372071 \cdot p_{105}$
68	$2^4 \cdot 3 \cdot 23 \cdot 764558869 \cdot 1811890921 \cdot c_{105}$
69	$3 \cdot 13 \cdot 23 \cdot 8684576204660284317187 \cdot 281259608597535749175083 \cdot c_{80}$
70	$2 \cdot 5 \cdot 2411111 \cdot 109315518091391293936799 \cdot c_{100}$
71	$3^2 \cdot 83 \cdot 2281 \cdot c_{126}$
72	$2^2 \cdot 3^2 \cdot 5119 \cdot c_{129}$
73	$37907 \cdot c_{132}$
74	$2 \cdot 3 \cdot 7 \cdot 1788313 \cdot 21565573 \cdot 99014155049267797799 \cdot c_{103}$
75	$3 \cdot 5^2 \cdot 193283 \cdot c_{133}$
76	$2^3 \cdot 828699354354766183 \cdot 21364389535249004731005898 1 \cdot p_{97}$
77	$3 \cdot 383481022289718079599637 \cdot 874911832937988998935021 \cdot c_{97}$
78	$2 \cdot 3 \cdot 31 \cdot 185897 \cdot c_{139}$
79	$73 \cdot 137 \cdot 22683534613064519783 \cdot 132316335833889742191773 \cdot c_{102}$
80	$2^2 \cdot 3^3 \cdot 5 \cdot 101 \cdot 10263751 \cdot 12953313401954533664084 89 \cdot p_{115}$

TABLE 2. Factorizations of $\mathrm{Sm}(n)$, $1 < n \leq 80$

n	known factors of $\mathrm{RSm}(n)$
2	$3 \cdot 7$
3	$3 \cdot 107$
4	$29 \cdot 149$
5	$3 \cdot 19 \cdot 953$
6	$3 \cdot 218107$
7	$19 \cdot 402859$
8	$3^2 \cdot 1997 \cdot 4877$
9	$3^2 \cdot 17^2 \cdot 379721$
10	$7 \cdot 28843 \cdot 54421$
11	$3 \cdot p_{12}$
12	$3 \cdot 7 \cdot p_{13}$
13	$17 \cdot 3243967 \cdot 237927839$
14	$3 \cdot 11 \cdot 24769177 \cdot p_{10}$
15	$3 \cdot 13 \cdot 19^2 \cdot 79 \cdot p_{15}$
16	$23 \cdot 233 \cdot 2531 \cdot p_{16}$
17	$3^2 \cdot 13 \cdot 17929 \cdot 25411 \cdot 47543 \cdot 677181889$
18	$3^2 \cdot 11^2 \cdot 19 \cdot 23 \cdot 281 \cdot 397 \cdot 8577529 \cdot 399048049$
19	$17 \cdot 19 \cdot 1462095938449 \cdot p_{14}$
20	$3 \cdot 89 \cdot 317 \cdot 37889 \cdot p_{21}$
21	$3 \cdot 37 \cdot 732962679433 \cdot p_{19}$
22	$13 \cdot 137 \cdot 178489 \cdot 1068857874509 \cdot p_{14}$
23	$3 \cdot 7 \cdot 191 \cdot p_{33}$
24	$3 \cdot 107 \cdot 457 \cdot 57527 \cdot p_{29}$
25	$11 \cdot 31 \cdot 59 \cdot 158820811 \cdot 410201377 \cdot p_{20}$
26	$3^3 \cdot 929 \cdot 1753 \cdot 2503 \cdot 4049 \cdot 11171 \cdot p_{24}$
27	$3^5 \cdot 83 \cdot 3216341629 \cdot 7350476679347 \cdot p_{18}$
28	$23 \cdot 193 \cdot 3061 \cdot 2150553615963932561 \cdot p_{21}$
29	$3 \cdot 11 \cdot 709 \cdot 105971 \cdot 2901761 \cdot 1004030749 \cdot p_{24}$
30	$3 \cdot 73 \cdot 79 \cdot 18041 \cdot 24019 \cdot 32749 \cdot 5882899163 \cdot p_{24}$
31	$7 \cdot 30331061 \cdot p_{45}$
32	$3 \cdot 17 \cdot 1231 \cdot 28409 \cdot 103168496413 \cdot p_{35}$
33	$3 \cdot 7 \cdot 7349 \cdot 9087576403 \cdot p_{42}$
34	$89 \cdot 488401 \cdot 2480227 \cdot 63292783 \cdot 254189857 \cdot 3397595519 \cdot p_{19}$
35	$3^2 \cdot 881 \cdot 1559 \cdot 755173 \cdot 7558043 \cdot 1341824123 \cdot 4898857788363449 \cdot p_{16}$
36	$3^2 \cdot 11^2 \cdot 971 \cdot 1114060688051 \cdot 1110675649582997517457 \cdot p_{24}$
37	$29 \cdot 2549993 \cdot 39692035358805460481 \cdot p_{38}$
38	$3 \cdot 9833 \cdot p_{63}$
39	$3 \cdot 19 \cdot 73 \cdot 709 \cdot 66877 \cdot p_{58}$
40	$11 \cdot 41 \cdot 199 \cdot 537093776870934671843838337 \cdot p_{39}$
41	$3 \cdot 29 \cdot 41 \cdot 89 \cdot 3506939 \cdot 18697991901857 \cdot 59610008384758528597 \cdot p_{28}$
42	$3 \cdot 13249 \cdot 14159 \cdot 25073 \cdot 6372186599 \cdot p_{52}$
43	$52433 \cdot 73638227044684393717 \cdot p_{53}$
44	$3^2 \cdot 7 \cdot 3067 \cdot 114883 \cdot 245653 \cdot 657119070884376607609 39 \cdot p_{41}$

continued...

n	known factors of RSm(n)
45	$3^2 \cdot 23 \cdot 167 \cdot 15859 \cdot 25578743 \cdot p_{65}$
46	$23 \cdot 35801 \cdot 543124946137 \cdot 45223810713458070167393 \cdot p_{43}$
47	$3 \cdot 11 \cdot 31 \cdot 59 \cdot 1102254985918193 \cdot 480842121756396l987019820401 \cdot p_{38}$
48	$3 \cdot 151 \cdot 457 \cdot 990013 \cdot 246201595862687 \cdot 636339569791857481119613 \cdot p_{39}$
49	$71 \cdot 9777943361 \cdot p_{77}$
50	$3 \cdot 157 \cdot 3307 \cdot 3267926640703 \cdot 771765128032466758284258631297 \cdot p_{43}$
51	$3 \cdot 11 \cdot p_{92}$
52	$7 \cdot 29 \cdot 670001 \cdot 403520574901 \cdot 70216544961751 \cdot 1033003489172581 \cdot p_{47}$
53	$3^4 \cdot 499 \cdot 673 \cdot 6287 \cdot 57653 \cdot 199236731 \cdot 1200017544380023$ $\cdot 110154194154057688350569200 3 \cdot p_{31}$
54	$3^3 \cdot 7^4 \cdot 13 \cdot 1427 \cdot 632778317 \cdot 57307460723 \cdot 7103977527461 \cdot 617151073326209 \cdot p_{43}$
55	$357274517 \cdot 460033621 \cdot p_{84}$
56	$3 \cdot 13^2 \cdot 85221254605693 \cdot p_{87}$
57	$3 \cdot 41 \cdot 25251380689 \cdot p_{93}$
58	$11 \cdot 2425477 \cdot 178510299010259 \cdot 377938364291219561$ $\cdot 546572896582343748037156624 9 \cdot p_{40}$
59	$3 \cdot c_{109}$
60	$3 \cdot 8522287597 \cdot p_{101}$
61	$13 \cdot 373 \cdot 6399032721246153065183 \cdot c_{88}$
62	$3^2 \cdot 11 \cdot 487 \cdot 6870011 \cdot 3921939670009 \cdot 11729917979119$ $\cdot 938364538509696981249417 823 \cdot p_{50}$
63	$3^2 \cdot 97 \cdot 26347 \cdot 33885691850835344918766 7 \cdot p_{86}$
64	$397 \cdot 653 \cdot 459162927787 \cdot 27937903937681 \cdot 386877715040952336040363 \cdot p_{65}$
65	$3 \cdot 7 \cdot 23 \cdot 13219 \cdot 24371 \cdot c_{110}$
66	$3 \cdot 53 \cdot 83 \cdot 2857 \cdot 1154129 \cdot 9123787 \cdot p_{103}$
67	$43 \cdot 38505359279 \cdot c_{113}$
68	$3 \cdot 29 \cdot 277213 \cdot 68019179 \cdot 152806439 \cdot 295650514394629363$ $\cdot 14246700953701310411 \cdot p_{67}$
69	$3 \cdot 11 \cdot 71 \cdot 167 \cdot 1481 \cdot 2326583863 \cdot 19962002424322006111361 \cdot p_{89}$
70	$1157237 \cdot 41847137 \cdot 8904924382857569546497 \cdot p_{96}$
71	$3^2 \cdot 17 \cdot 131 \cdot 16871 \cdot 1504047269 \cdot 82122861127 \cdot 1187275015543580261 \cdot p_{87}$
72	$3^2 \cdot 449 \cdot 1279 \cdot p_{129}$
73	$7 \cdot 11 \cdot 21352291 \cdot 1051174717 \cdot 92584510595404843 \cdot 33601392386546341921 \cdot p_{83}$
74	$3 \cdot 177337 \cdot 6647068667 \cdot 31386093419 \cdot 669035576309897 \cdot 4313244765554839 \cdot c_{83}$
75	$3 \cdot 7 \cdot 230849 \cdot 7341571 \cdot 24260351 \cdot 1618133873 \cdot 19753258488427$ $\cdot 46752975870227777 \cdot c_{81}$
76	$53 \cdot c_{142}$
77	$3 \cdot 919 \cdot 571664356244249 \cdot c_{127}$
78	$3 \cdot 17 \cdot 47 \cdot 17795025122047 \cdot c_{131}$
79	$160591 \cdot 274591434968167 \cdot 1050894390053076193 \cdot p_{112}$
80	$3^3 \cdot 11 \cdot 443291 \cdot 1575307 \cdot 19851071220406859 \cdot c_{121}$

TABLE 3. Factorizations of RSm(n), $1 < n \leq 80$

4. Searching for primes in Sm and RSm

Using the GMP library, a fast C program was written to search for primes in Sm(n) and RSm(n). We used the Miller-Rabin [K81] test to check for compositeness.

No primes were found in $\mathrm{Sm}(n)$, $1 < n < 840$, and only one probable prime in $\mathrm{RSm}(n)$, $1 < n < 750$, namely $\mathrm{RSm}(82) = 82818079...1110987654321$. This number proved prime with `ECPP`.

5. Acknowledgements and contact information

Thanks go to Paul Zimmermann for discussion and review of the paper. He also contributed one factor to the data.

This work wouldn't have been possible without the open-source software provided by the respective authors: Richard Crandall (`science0`), Torbjorn Granlund (`GMP`), Paul Zimmermann (`GMP-ECM`), and François Morain (`ECPP`).

The author can be reached at the E-mail address `stephan@tmt.de` and his homepage is at the URL `http://rws.home.pages.de`.

References

[AM93] A.O.L.Atkin and F.Morain: *Elliptic curves and primality proving*, Math. Comp. **60** (1993) 399-405

[K81] Donald E. Knuth: *The Art of Computer Programming*, Vol. 2, *Seminumerical Algorithms*, 2nd ed, Addison-Wesley, 1981

[L87] H.W.Lenstra, Jr.: *Factoring integers with elliptic curves*, Annals of Mathematics (2) **126** (1987), 649-673

[LL93] A.K.Lenstra and H.W.Lenstra, Jr. (eds.): *The development of the number field sieve*, Notes in Mathematics **1554**, Springer-Verlag, Berlin, 1993

[M87] Peter L. Montgomery: *Speeding the Pollard and Elliptic Curve Methods of Factorization*, Math. Comp. **48** (1987), 243-264

[M92] Peter L. Montgomery: *An FFT Extension of the Elliptic Curve Method of Factorization*, Ph.D. dissertation, Mathematics, University of California at Los Angeles, 1992

[R85] Hans Riesel: *Prime Numbers and Computer Methods for Factorization*, Birkhuser Verlag, 1985

[S87] R.D.Silverman: *The multiple polynomial quadratic sieve*, Math. Comp. **48** (1987), 329-339

[S93] F.Smarandache: *Only Problems, Not Solutions!*, Xiquan Publ., Phoenix-Chicago, 1993

[Z98] P.Zimmermann: *Comparison of three public-domain multiprecision libraries: Bignum, Gmp and Pari*