A0945
A0946

Niel Sloane
AT & T Bell Laboratories
Room 2C-376
600 Mountain Avenue
Murray Hill
New Jersey 07974
U. S. A.

August 27, 1991

Dear Niel Sloane,

Thank you for your letter of May 26 1991 in which you ask for additional terms for your sequence 329: 2, 3, 7, 43, 53, 5, ... 5471 (where each term is the least prime factor of 1 + the product of all previous terms). Unfortunately, I haven't done any serious work in factoring since 1982. However, on receiving your request and noticing that the number whose least factor is sought to find the next term is not too large, I implemented a couple of the most simple methods in Miranda (a functional programming language that, fortunately, includes unlimited precision integer operations). The machinery used is a SUN workstation situated at Odense University.

Using trialdivision, Pollard's Rho, and the simple primality test based on knowledge of factors of N-1, I found the next two terms to be 52662739 and 23003, respectively. Please verify. The next term is beyond my current simple implementation and/or patience.

I enclose a listing that includes these numbers to guard against errors in the present letter. I also enclose a couple of other items that may be useful. The report PB-144 contains details of the factorizations for sequence 330.

Yours faithfully,

Thorkil Naur

Thorkil Naur

Fredensgade 4
DK-5560 Aarup
Denmark

PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 90, Number 1, January 1984

MULLIN'S SEQUENCE OF PRIMES IS NOT MONOTONIC

THORKIL NAUR

ABSTRACT. The sequence of primes defined by $p_1 = 2$ and $p_{n+1} =$ (largest prime factor of $p_1 \cdot p_2 \cdots p_n + 1$) is not monotone increasing. We present the first eleven primes of the sequence and observe that $p_{10} < p_9$.

Following Euclid's scheme for proving the infinitude of the primes, Mullin [**6**] defines the sequence of primes

$$p_1 = 2, \quad p_{n+1} = \text{largest prime factor of } p_1 \cdot p_2 \cdots p_n + 1$$

and asks (among other questions concerning this and a related sequence) whether it is monotone increasing. We have computed the first eleven terms of this sequence, which are given below (for completeness, we give all the known primes in the sequence):

n	p_n
1	2
2	3
3	7
4	43
5	139
6	50207
7	340999
8	2365347734339
9	4680225641471129
10	1368845206580129
11	889340324577880670089824574922371

We observe that $p_{10} < p_9$ and the sequence is thus not monotone increasing.

Each p_{n+1} was found by completely factoring $p_1 \cdot p_2 \cdots p_n + 1$. The factorizations corresponding to the last four primes are

n	Complete factorization of $p_1 \cdot p_2 \cdots p_n + 1$
7	$23 \cdot 79 \cdot p_8$
8	$17 \cdot 127770091783 \cdot p_9$
9	$89 \cdot 839491 \cdot 556266121 \cdot 836312735653 \cdot p_{10}$
10	$1307 \cdot 56030239485370382805887 \cdot p_{11}$

These factorizations were found using direct search and the methods described in Morrison and Brillhart [**5**] and Pollard [**8, 9**]. The larger prime factors were proved

Received by the editors January 21, 1983.
1980 *Mathematics Subject Classification*. Primary 10A40; Secondary 10A25.

prime by using the methods of Brillhart, Lehmer and Selfridge [1]. For details, see pp. 45–52 of Naur [7].

The first nine terms of the sequence, as published earlier in Guy and Nowakowski [3], agree with those given above. Guy and Nowakowski [3] also discuss several related sequences. The incorrect computation by Korfhage [4] is cited in Cox and van der Poorten [2] and Sloane [10] (sequence number 330).

Cox and van der Poorten [2] prove that if the jth prime q_j occurs as the $(k+1)$st term of the sequence, then a certain set of congruences (modulo 2), which depends on j and k, must be solvable. The congruences for $j = 16$, $k = 6$ are stated to be unsolvable, and this is taken as proving that none of the primes less than $q_{16} = 53$ occur in the sequence, except for $2, 3, 7$, and 43, which occur among the first $k = 6$ terms. However, to prove the nonoccurrence of a prime using this argument, it is clearly necessary to show that the congruences are unsolvable for *all* k, not just one, so it is still not known whether all primes occur in the sequence. The unproved result concerning the nonoccurrence of primes less than 53 is also cited in Guy and Nowakowski [3].

The author would like to thank Professor B. H. Mayoh for bringing his attention to this problem and the referee for pointing out the paper by Guy and Nowakowski [3].

References

1. J. Brillhart, D. H. Lehmer and J. L. Selfridge, *New primality criteria and factorizations of* $2^m \pm 1$, Math. Comp. **29** (1975), 620–647.
2. C. D. Cox and A. J. van der Poorten, *On a sequence of prime numbers*, J. Austral. Math. Soc. **8** (1968), 571–574.
3. R. Guy and R. Nowakowski, *Discovering primes with Euclid*, Delta (Waukesha) **5** (1975), 49–63.
4. R. R. Korfhage, *On a sequence of prime numbers*, Bull. Amer. Math. Soc. **70** (1964), 341–342; *Errata*, 747.
5. M. A. Morrison and J. Brillhart, *A method of factoring and the factorization of* F_7, Math. Comp. **29** (1975), 183–205.
6. A. A. Mullin, *Recursive function theory*, Bull. Amer. Math. Soc. **69** (1963), 737.
7. T. Naur, *Integer factorization*, DAIMI PB-144, Dept. Comput. Sci., Univ. of Aarhus, Denmark, 1982.
8. J. M. Pollard, *Theorems on factorization and primality testing*, Proc. Cambridge Philos. Soc. **76** (1974), 521–528.
9. ——, *A Monte Carlo method for factorization*, BIT **15** (1975), 331–334.
10. N. J. A. Sloane, *A handbook of integer sequences*, Academic Press, New York, 1973.

Department of Mathematics, Odense University, Odense, Denmark

MATHEMATICS OF COMPUTATION
VOLUME 41, NUMBER 164
OCTOBER 1983, PAGES 687-695

New Integer Factorizations

By Thorkil Naur

Abstract. New factorizations of Fibonacci numbers, Lucas numbers, and numbers of the form $2^n \pm 1$ are presented together with the strategy (a combination of known factorization methods) used to obtain them.

1. Introduction. This paper presents new complete factorizations of 174 large integers of interest. The factorizations have been obtained by the author over the past four years using a combination of known methods. Our factorization strategy, which has been implemented on a micro-programmable computer, makes extensive use of J. M. Pollard's factorization methods (Pollard [8] and Pollard [9]). The strategy also includes the well-known method of trial division, the continued fraction method (Morrison and Brillhart [6]), and the primality tests of Brillhart, Lehmer and Selfridge [3].

Section 2 contains a summary of our factorization strategy. Since we use known methods, no details of these methods are given. Section 3 contains the actual results and describes their form. We have attacked the cofactors (i.e. the factors remaining after the known factors are removed) of Fibonacci numbers, Lucas numbers, and numbers of the form $2^n \pm 1$, whose factorizations were not previously known.

The paper is a condensed version of Naur [7], which, in addition to the material in this paper, contains summaries of the factorization methods used and full factorization tables.

It should be noted that most of the factorizations presented here have been independently discovered by J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, S. S. Wagstaff, or their colleagues, possibly using a strategy similar to the one described here (Lehmer [5], Pollard [10], and Wagstaff [12]).

2. Strategy. The factorization strategy combines known methods and may be summarized as follows:

Step 1. Trial divide to 10^6. This step hardly needs further comment (for an efficient implementation of trial division, see Wunderlich and Selfridge [18]).

Step 2. Use Pollard's two methods simultaneously. The $P - 1$ method is able to discover a prime factor p, if the factors of $p - 1$ are small. We use the first stage of the method as described at the end of Pollard [8]. For previous uses of the $P - 1$ method, see Williams and Judd [15] and [16], Williams and Seah [17], and Williams [13], the latter giving an account of the related $P + 1$ method.

Received August 11, 1982; revised February 23, 1983.
1980 *Mathematics Subject Classification*. Primary 10-04, 10A25, 10A40.

The rho method (or Monte Carlo method, see Pollard [9]) is usually able to find a prime factor p in about $O(p^{1/2})$ steps. Improvements of the rho method (see Brent [1] and Brent and Pollard [2]) have only been recently published and have not been used.

Both the $P - 1$ method and the rho method can be broken into smaller steps, and a step from each method is executed alternately.

Step 3. Having executed a suitable number of steps of Pollard's methods, the continued fraction method (Morrison and Brillhart [6]) is invoked, if the number has 53 or fewer digits.

Step 4. Whenever a factorization is discovered in Steps 2 or 3, both factors are tested for primality using the tests from Brillhart, Lehmer and Selfridge [3] (the number itself is also tested after Step 1). Since these tests require a certain number of factors of $N \pm 1$ to be known before the primality of N can be verified, these auxiliary factorizations are attempted simultaneously using our strategy recursively. When a sufficient number of factors is found, the factoring is stopped and the primality tests are carried out.

The above strategy has been implemented on the micro-programmable computer Mathilda, developed at the Aarhus University (Schriver and Kornerup [11]).

TABLE 1. *Fibonacci numbers*

n	Factorization of U_n
191.	4870723671313 * 757810806256989128439975793
221.	233 * 1597 : 203572412497 * 906574987180246453263929 40193
233.	139801 * 25047390419633 * 631484089583693149557829547141
239.	10037 * 62141 * 2228536579597318057 * 2854690886229614923 3369
251.	582416774750273 * 21937080329465122026187124199656961913
253.	89 * 28657 : 4322114369 * 2201228236641589 * 13784973033380476 12061
257.	5653 * 32971978671645905645521 * 1230026721719313471360714649
259.	13 * 73 * 149 * 2221 : 1553 * 404656773793 * 3041266742295771985148799223649
265.	5 * 953 * 55945741 : 15901 * 2741218753681 * 926918599457468125920827581
267.	2 * 1069 * 1665088321800481 : 122887425153289 * 644558773497030428773 09
269.	5381 * 2517975182669813 * 32170944747810641 * 1693604398296487898 53
289.	1597 : 577 * 1733 * 98837 * 101232653 * 106205194357 * 658078658277725444483848541
291.	2 * 193 * 389 * 3084989 * 361040209 : 76674415738994499773 * 227993117754975870677
303.	2 * 743519377 * 770857978613 : 8550224389674481 * 9604965791727987485136 9421
305.	5 * 4513 * 555003497 : 2441 * 6101 * 204152539662476988 01 * 64727767071799824094 3861
319.	89 * 514229 : 1913 * 578029 * 1435522969 * 153541455600361 3 * 1862624318468346334828 3529
333.	2 * 17 * 73 * 149 * 2221 * 1459000305513721 : 12653 * 124134848933957 * 9305077315575902267675937 61
355.	5 * 6673 * 46165371073 : 4261 * 75309701 * 309273161 * 9207609261398081 * 492797226433918641928 01
361.	37 * 113 : 6567762529 * 1196762644057 * 315092782781693087814159 7 * 12020126510714734783009241
367.	733 * 17969789 * 75991753 * 5648966761 * 43397676601 * 114150315493 * 79735723562470149913444420 1
369.	2 * 17 * 2789 * 59369 * 68541957733949701 : 8117 * 199261 * 84738793193 * 9382599520669 * 1178385186333514 69
377.	233 * 514229 : 104264251753 * 361575655741 * 6081465853455679816708931999854492020150600 94237

TABLE 2. *Lucas numbers*

n Factorization of V_n

166. 3 : 6464041 * 245329617161 * 10341247759646081
197. 3149858711911339 * 4701907222895068350249889
211. 33128448586319 * 3768695026320506495615952689771
221. 521 * 3571 : 2337127044022973021 * 3531495042124863863141
227. 39499 * 5098421 * 4311537234701 * 317351386961794678797301
230. 3 * 41 * 4969 * 275449 : 3116523496881881 * 2224700455311857347241
242. 3 * 43 * 307 : 200872171147 * 3564873012035809 * 13253086025993542387
244. 7 : 487 * 52471477541626010209 * 5500902230146438151405489047
252. 2 * 7^2 * 23 * 167 * 14503 * 103681 * 65740583 : 503 * 4322424761927
 * 571385160581761
253. 139 * 199 * 461 : 13343097459037867049 * 439589715274978576995097049
256. 34303 * 73327699969 * 125960894984050328038716298487435392001
257. 2107028233569599 * 125090447782502159 * 1945042261468790758531
258. 2 * 3^2 * 313195711516578281 : 7772507 * 73254041816089 * 258422401920467
269. 13451 * 49098524855733491 * 290341026883813109 * 860882346042166879
272. 2207 : 4470047 * 7378607647 * 42848407775681 * 224189164930816106106049
274. 3 : 547 * 27947 * 86409516719752275209 * 461963939612677343458490143601
277. 1109 * 5923369 * 1003666289 * 322458613167451 * 3647646099535497480264359
281. 20567460049 * 46415343154434259 * 55678135331080359350346681814561
286. 3 * 43 * 307 * 90481 : 5147 * 2441129996120243
 * 13092861035652370656608696909281
287. 29 * 370248451 : 256579 * 319973431 * 101731310703289
 * 10635841025639256246541
288. 2 * 1087 * 4481 * 11862575248703 : 270143 * 25033626656641
 * 1974737795746080149567
292. 7 : 839207 * 121355783 * 2864461601 * 4953066392881
 * 1045794092558661358680161
296. 47 : 15400289 * 19088449 * 77894162661647 * 89311781152481
 * 754276330346432303
299. 139 * 461 * 521 : 599 * 2233531 * 1194215681621 * 143236388738249
 * 40197222522537856361
301. 29 * 6709 * 144481 : 39488879317091 * 1050474234583201
 * 689529693448123842995171
302. 3 : 70963651961 * 95305716283 * 64119657493918388500959028976916724219027
304. 2207 : 607 * 1823 * 20063 * 91807 * 1156984541407 * 12441241017224321
 * 52601970578546783
308. 7^2 * 263 * 881 * 967 * 14503 : 7872253927 * 9623520524969002343
 * 1935298980672778761041
309. 2^2 * 619 * 1031 * 5257480026438961 : 1270029990781
 * 2216051880587916003268636813231
310. 3 * 41 * 3020733700601 : 180501911066713425499001
 * 911316263659755894779625401
320. 127 * 186812208641 : 62379555831803099867272961
 * 5079180256659675431743744001
322. 3 * 281 * 4969 * 275449 : 643 * 770867 * 25154641 * 163674763583689
 * 8357802723902097130683089
331. 526291 * 54184296181 * 4386848568249611
 * 11957954590103942275063852978039182929
334. 3 : 821641 * 7162963 * 50187047747 * 14167898020159929481
 * 504752765667203736366779801
338. 3 * 90481 : 2027 * 141283 * 404112157123 * 478061565712797524641
 * 2892106995173496522201467
339. 2^2 * 412670427844921037470771 : 44607276283528829839
 * 954423225346040964978868549
340. 7 * 2161 * 23230657239121 : 5441 * 897601 * 17276792316211992881
 * 3834936832404134644974961
348. 2 * 7 * 23 * 299281 * 834428410879506721 : 56058952425321966662183
 * 1185031046372137517381447
350. 3 * 41 * 281 * 401 * 570601 * 12317523121 : 2801 * 28001
 * 248773766357061401 * 7358192362316341243805801
374. 3 * 43 * 67 * 307 * 63443 : 2243 * 49369 * 3827019260681
 * 1586361987756363049 * 12812807672672518125975550387

TABLE 2. (*Continued*)

n	Factorization of V_n
391.	139 * 461 * 3571 : 10949 * 2476673936041 * 8344848804983721285378913074459418529255664192499116 16229
393.	2^2 * 1049 * 414988698461 * 5477332620091 : 32845130922638389 * 4327437028088789068774934175058474 1809
399.	2^2 * 29 * 211 * 229 * 9349 * 95419 * 10694421739 * 2152958650459 : 28729 * 519499 * 561434197549 * 25217116745720727713 6719
400.	2207 * 23725145626561 : 107420801 * 177736001 * 5179368521466240 1 * 7601587101128729489773008667804801
402.	2 * 3^2 * 6163 * 201912469249 * 2705622682163 : 1609 * 2915186157721 * 36250499854335186207246297549451509565 69
410.	3 * 41^2 * 163 * 800483 * 350207569 : 628774904181521 * 1438601882967811671 61 * 2322429099336692919718294260481
411.	2^2 * 541721291 * 78982487870939058281 : 242491 * 104446810724929 * 18070186267894449189347092077457768249
441.	2^2 * 19 * 29 * 211 * 1009 * 31249 * 65269 * 620929 * 8844991 * 599786069 : 35281 * 806421131812444 69 * 1624735075664061773219277075034 9
444.	2 * 7 * 23 * 10661921 * 114087288048701953998401 : 887 * 2663 * 17761 * 21423730326721 * 175358325117577112755922815666434 9601
450.	2 * 3^3 * 41 * 107 * 401 * 601 * 2521 * 570601 * 10783342081 * 87129547172401 : 1801 * 18637456318905481020 1 * 4276941485843380877782200 01
457.	143392891 * 48175086409 * 864351271995241 * 538655620387010089753971464077054421188204623261302859056692 99
474.	2 * 3^2 * 21803 * 5924683 * 14629892449 * 184715524801 : 947 * 10279163 * 8411395441 * 59223094130623540 09 * 376943442492584130991581889
478.	3 : 632890270126128456721 * 414612475582425401119754697066276232016-4758443697460091641243037362105014072881
483.	2^2 * 29 * 139 * 211 * 461 * 691 * 1289 * 1485571 * 1917511 * 965840862268529759 : 9661 * 236235695207989 * 9952648158500556841649035737455844289
498.	2 * 3^2 * 6464041 * 245329617161 * 10341247759646081 : 20276569 * 93750172283 * 212216314620580244514251999177476639338737695720283

3. Results. The factorization results are given in Tables 1 through 6. All factorizations listed are complete, i.e. all factors are prime. The algebraic factors (if any) are separated from the primitive factors by a colon (:). We have not given any details of the actual methods used to obtain the various factorizations.

The author has investigated the Fibonacci numbers U_n, defined by $U_0 = 0$, $U_1 = 1$, $U_{n+2} = U_{n+1} + U_n$, for odd n, $1 \leqslant n \leqslant 399$, and the Lucas numbers V_n, defined by $V_0 = 2$, $V_1 = 1$, $V_{n+2} = V_{n+1} + V_n$, for all n, $0 \leqslant n \leqslant 500$. Tables 1 and 2 contain factorizations of U_n and V_n, respectively, which have not been listed as complete in Jarden [4], Morrison and Brillhart [6], Williams and Judd [15] and [16], Williams and Holte [14], or Williams [13].

The numbers $2^n - 1$ have been investigated for odd n, $1 \leqslant n \leqslant 299$, and Table 3 contains factorizations of numbers of this form which have not been listed as complete in Brillhart, Lehmer and Selfridge [3] or Williams [13]. The numbers $2^n + 1$ have been investigated for $0 \leqslant n \leqslant 300$, $2 \leqslant n \leqslant 598$, if $n = 4k + 2$. Table 4 contains factorizations of $2^n + 1$ with $n \neq 4k + 2$, which have not been listed as

TABLE 3. $2^n - 1$, *n odd*

n	Factorization of 2^n-1
169.	8191 : 4057 * 6740339310641 * 3340762283952395329506327023033
173.	730753 * 1505447 * 70084436712553223 * 155285743288572277679887
185.	31 * 223 * 616318177 : 1587855697992791 * 7248808599285760001152755641
191.	383 * 7068569257 * 39940132241 * 332584516519201 * 87274497124602996457
193.	13821503 * 61654440233248340616559 * 14732265321145317331353282383
199.	164504919713 * 4884164093883941177660049098586324302977543600799
205.	31 * 13367 * 164511353 : 2940521 * 70171342151 * 3655725065508797181674078959681
213.	7 * 228479 * 48544121 * 212885833 : 66457 * 2849881972114740679 * 4205268574191396793
215.	31 * 431 * 9719 * 2099863 : 1721 * 731516431 * 514851898711 * 297927289744047764444862191
217.	127 * 2147483647 : 5209 * 62497 * 6268703933840364033151 * 378428804431424484082633
219.	7 * 439 * 2298041 * 9361973132609 : 3943 * 671165898617413417 * 4815314615204347717321
223.	18287 * 196687 * 1466449 * 2916841 * 1469495262398780123809 * 596242599987116128415063
235.	31 * 2351 * 4513 * 13264529 : 2391314881 * 72296287361 * 73202300395158005845473537146974751
237.	7 * 2687 * 202029703 * 1113491139767 : 1423 * 49297 * 237288235123456092 79 * 313573734170900934 31
243.	7 * 73 * 2593 * 71119 * 262657 * 97685839 : 487 * 16753783618801 * 192971705688577 * 3712990163251158343
247.	8191 * 524287 : 15809 * 6459570124697 * 402004106269663 * 1282816117617265060453496956212169
267.	7 * 618970019642690137449562111 : 78903841 * 28753302853087 * 2412433243771392408426731653735 3
271.	15242475217 * 248927757868131890277330541567820045256364273970773286542188386932989391
273.	7^2 * 79 * 127 * 337 * 911 * 8191 * 121369 * 112901153 * 23140471537 : 108749551 * 4093204977277417 * 86977595801949844993
279.	7 * 73 * 2147483647 * 658812288653553079 : 16183 * 34039 * 1437967 * 833732508401263 * 20344398369518672998886 17
283.	9623 * 68492481833 * 23579543011798993222850893929565870383844167873851502677311057483194673
285.	7 * 31 * 151 * 191 * 32377 * 524287 * 1212847 * 420778751 * 30327152671 : 1491477035689218775711 * 2534924298663772057356 1
287.	127 * 13367 * 164511353 : 17137716527 * 51954390877748655744256192963206220919272895548843817842228913
295.	31 * 179951 * 3203431780337 : 4721 * 132751 * 5794391 * 128818831 * 3812358161 * 452824604065751 * 44109752306508279737 11

complete in Brillhart, Lehmer and Selfridge [3] or Williams [13]. For $n = 4k + 2$,

$$2^n + 1 = (2^{2k+1} - 2^{k+1} + 1)(2^{2k+1} + 2^{k+1} + 1),$$

which has been investigated for $1 \leqslant 2k + 1 \leqslant 299$. Tables 5 and 6 contain factorizations of these factors which have not been listed as complete in Brillhart, Lehmer and Selfridge [3] or Williams [13].

TABLE 4. $2^n + 1$

```
n   Factorization of 2^n+1

151. 3 : 18717738334417 * 5083405082410077967730646062149
152. 257 : 27361 * 6939446046394O481 * 1169955781771735890448
157. 3 : 15073 * 2350291 * 17751783757817897 * 96833299198971305921
163. 3 : 11281292593 * 1023398150341859 * 3375705470503904150417
169. 3 * 2731 : 4929910764223610387 * 1852623864601108673274261
172. 17 : 3855260977 * 64082150767423457 * 1425343275103126327372769
179. 3 : 58745093521 * 434786819066587937349595056277570770714380
184. 257 : 43717618369 * 549675408461419937 * 39702995674729028797917
188. 17 : 1198107457 * 23592342593 * 4501946625921233 * 1813523068524760695
193. 3 : 6563 * 35679139 * 1871670769 * 7455099975844049
     * 1280761337388845898643
197. 3 : 197002597249 * 1348959352853811313 * 251951573867253012259144010843
208. 65537 : 928513 * 18558466369 * 23877647873 * 21316654212673
     * 715668470267111297
209. 3 * 683 * 174763 : 419 * 34106232846546394407
     * 160779201878039402409551431700
211. 3 : 4643 * 9878177 * 5344743097 * 199061567251
     * 224811275125751758642341851902
219. 3^2 * 1753 * 1795918038741070627 : 907019754219664
     * 32782446901562224341359061
221. 3 * 2731 * 43691 : 443 * 4714692062809
     * 4507513575406446515845401458366741487526913
223. 3 : 219256122131 * 204934959209050439504076504509181712603183031547084055
227. 3 : 297371 * 3454631579714210387
     * 6998217065826544471311754525871203110339965
235. 3 * 11 * 283 * 165768537521 : 328006342451 * 4617979079499972
     * 23545737451009211508683469
243. 3^6 * 19 * 163 * 87211 * 135433 * 272010961 : 1459 * 139483
     * 1042940743191133461 * 918125051602568899753
245. 3 * 11 * 43 * 281 * 86171 * 4363953127297 : 491 * 15162868758218274451
     * 50647282035796125885000330641
249. 3^2 * 499 * 1163 * 2657 * 155377 * 13455809771 : 920241944668
     * 338809829056758737705201652562794859
253. 3 * 683 * 2796203 : 4049 * 85009 * 31797547 * 81776791273
     * 2822551529460330847604262086149015242689
260. 17 * 61681 * 858001 * 308761441 : 42641 * 5746001 * 2400573761
     * 65427463921 * 173308343918874810521923841
261. 3^3 * 19 * 59 * 3033169 * 96076791871613611 : 523 * 6929826139
     * 345341290183269055 * 33563856450515702761
264. 97 * 257 * 673 * 229153 * 119782433 * 43872038849 : 1687508167565088
     * 86945388997210442828259494992321
273. 3^2 * 43 * 2731 * 5419 * 224771 * 1210483 * 22366891 * 25829691707 : 547
     * 105310750819 * 29265311314715720577912752682
277. 3 : 25792643401363
     * 313828000939967901734463105154262276920587713495384512820233434582285
279. 3^3 * 19 * 529510939 * 715827883 * 2903110321 : 26227 * 119232435043
     * 85384915399027 * 644436537614061119902218
288. 641 * 6700417 * 18446744069414584321 : 3457 * 816769
     * 15629859013500857099553 * 1422346738975853644793916289
```

TABLE 5. $2^n - 2^{(n+1)/2} + 1$, *n odd*

```
n   Factorization of 2^n-2^((n+1)/2)+1

149. 5 : 12961064789 * 110118089519717459153132423369276 41
157. 5 : 2790467761 * 5941035366826969 * 220394203343914834 3973
169. 53 * 157 : 677 * 615946323850313 * 2156563293828915509201 92462661
173. 5 : 13625405957 * 175739665310505752968877740350313227534889
179. 5 : 31815461 * 416115013830990336221 * 1157570933663659527 8866333
181. 5 : 9413 * 178925762979037 * 3830538323149121 * 95016376135555 3173181
187. 5 * 397 * 26317 : 26509131221 * 35155077044989397 * 40292920656291 91839853
219. 5 * 293 * 9929 * 649301712182209 : 877 * 1013533 * 704710824913
     * 1424068687655254366706 17
225. 13 * 37 * 41 * 61 * 101 * 1201 * 8101 * 29247661 * 1182468601
     : 413150254353901 * 31922615042161 12476901
235. 5^2 * 3761 * 7484047069 : 941 * 894434441 * 3357909154141 * 38425816980821
     * 7225018096169268 41
243. 5 * 109 * 246241 * 106979941 * 168410989 : 3333950193493
     * 175347746967791320219053760667420 4157
245. 5^2 * 29 * 197 * 47392381 * 19707683773 : 306178659371201
     * 1372226516822701 * 100878790642429472 7221
249. 13 * 997 * 46202197673 * 209957719973 : 136453 * 218166829 * 41732461753
     * 579148740542722837871 7709
253. 5 * 397 * 1013 * 1657 : 6994042018866541
     * 621109541542884571802304568790331501283098925929529
257. 22988734297
     * 1007381161062241802842574173831975781810739698060547170245057092631 3
267. 5 * 123794003928545064364330189 : 3401264941 * 11221454641
     * 1003805584154595697911113729202066 1
269. 5 : 2153 * 3229 * 5381 * 4273873 * 1633401082697
     * 39186951793042143278851 57 * 1853821129478118282760762 81
273. 13^2 * 53 * 113 * 157 * 313 * 1249 * 1429 * 4733 * 55633852591232515 7
     : 503413 * 467811806281 * 275700717951546566946854497
275. 5^3 * 397 * 268501 * 3630105520141 : 12101 * 35201 * 698617420601
     * 18735216413769901 * 2251172339268843846064 01
289. 137 * 953 : 7698961 * 21886549 * 113478990853
     * 3984101605272210941787491811844722908052361878816994263 13
```

TABLE 6. $2^n + 2^{(n+1)/2} + 1$, *n odd*

```
n   Factorization of 2^n+2^((n+1)/2)+1

137. 5 : 168434085820849 * 20687567010495774491714761З
151. 5 : 437368927017637926120l * 1305303239018992l0670077
167. 5 : 75005713 * 27395325377910797 * 182082607811901565З6114609
169. 5 * 1613 : 180201997 * 1259036730797 * 408946876729703992293841657
173. 7152893721041 * 167381508518657470032217423206994218l681
183. 5 * 733 * 1709 * 368140581013 : 12836737570021 * 41419495873379653089918l
187. 137 * 953 * 2113 : 5237 * 551353793 * 1819762572673
     * 1353220459171186012734З7
191. 5 : 3821 * 896188753870б1 * 18330851538426654426522832341651434З3597
193. 5 : 3089 * 148997 * 1440203064470440587l * 37879130002708963567765228597З
203. 113 * 536903681 : 9810958633253 * 215974685494939586649025043316706457З7
209. 5 * 229 * 397 * 457 : 6689 * 2039731321 * 14983275068З283097
     * 1937385241416564065603093
217. 5 * 29 * 8681 * 49477 : 31249 * 776729668507005203702993
     * 139335546032913681584758997
219. 13 * 944473296560185147392l : 371335727233
     * 184786091137101220235501264251З7
237. 13 * 604462909806215075725313 : 18890331057055511701
     * 1487840558911519281039078769
239. 5 : 77852679293
     * 226947496325569308571143294838758211481755726354645794750120l
243. 13 * 37 * 279073 * 3618757 * 4977454861 : 2917 * 4861 * 26129603777437
     * 15778453094691989880197773477
249. 5 * 13063537 * 148067197374074653 : 1993 * 80485166514184335373
     * 5831175796919674915469611 81
253. 277 * 2113 * 30269 : 25301 * 109297 * 756550961 * 2569737193 * 9623862953
     * 156296877661 * 101027360307659633
263. 5 : 119929 * 731141 * 99972364781
     * 33815322934709348729340206164586405164149466120265140526 9
265. 5^2 * 1801439824104653 : 51941 * 24082141 * 31213331016701
     * 337165836682085104473681014724994l2321
285. 13 * 41 * 61 * 761 * 131101 * 160969 * 525313 * 2416923620660807201
     : 1457772869697961 * 643261967877279035519771508 61
297. 5 * 109 * 397 * 42373 * 246241 * 4327489 * 15975607282273 : 2377 * 22573
     * 155399494141 * 4712151755917 * 415232599942757862979 57
299. 53 * 157 * 277 * 30269 : 20333 * 956801 * 15595841 * 19294368341
     * 6339840806910833 * 393345821366273907459718331839045409
```

4. Acknowledgements. The author wishes to thank K. Andersen, P. Kornerup, J.K. Kjærgård, J. W. Nielsen, I. H. Sørensen, S. M. Sørensen, F. Wibroe, and O. Østerby for their generous support and guidance in various phases of this work. Many thanks are also due to D. H. Lehmer and S. S. Wagstaff for making the Cunningham Project tables available to the author.

Department of Computer Science
Odense University
DK-5230 Odense M., Denmark

1. R. P. BRENT, "An improved Monte Carlo factorization algorithm," *BIT*, v. 20, 1980, pp. 176–184.

2. R. P. BRENT & J. M. POLLARD, "Factorization of the eighth Fermat number," *Math. Comp.*, v. 36, 1981, pp. 627–630.

3. J. BRILLHART, D. H. LEHMER & J. L. SELFRIDGE, "New primality criteria and factorizations of $2^m \pm 1$," *Math. Comp.*, v. 29, 1975, pp. 620–647.

4. D. JARDEN, *Recurring Sequences*, 3rd ed., Riveon Lemathematica, Jerusalem, 1973.

5. D. H. LEHMER, Letter of July 14, 1982.

6. M. A. MORRISON & J. BRILLHART, "A method of factoring and the factorization of F_7," *Math. Comp.*, v. 29, 1975, pp. 183–205.

7. T. NAUR, *Integer Factorization*, DAIMI PB-144, Dept. of Computer Science, University of Aarhus, Denmark, 1982.

8. J. M. POLLARD, "Theorems on factorization and primality testing," *Proc. Cambridge Philos. Soc.*, v. 76, 1974, pp. 521–528.

9. J. M. POLLARD, "A Monte Carlo method for factorization," *BIT*, v. 15, 1975, pp. 331–334.

10. J. M. POLLARD, Letter of July 27, 1982.

11. B. D. SHRIVER & P. KORNERUP, *A Description of the MATHILDA Processor*, DAIMI PB-52, Dept. of Computer Science, University of Aarhus, Denmark, 1975.

12. S. S. WAGSTAFF, Letters of July 20 and 26, 1982.

13. H. C. WILLIAMS, "$A\ p + 1$ method of factoring," *Math. Comp.*, v. 39, 1982, pp. 225–234.

14. H. C. WILLIAMS & R. HOLTE, "Some observations on primality testing," *Math. Comp.*, v. 32, 1978, pp. 905–917.

15. H. C. WILLIAMS & J. S. JUDD, "Determination of the primality of N by using factors of $N^2 \pm 1$," *Math. Comp.*, v. 30, 1976, pp. 157–172.

16. H. C. WILLIAMS & J. S. JUDD, "Some algorithms for prime testing using generalized Lehmer functions," *Math. Comp.*, v. 30, 1976, pp. 867–886.

17. H. C. WILLIAMS & F. SEAH, "Some primes of the form $(a^n - 1)/(a - 1)$," *Math. Comp.*, v. 33, 1979, pp. 1337–1342.

18. M. C. WUNDERLICH & J. L. SELFRIDGE, "A design for a number theory package with an optimized trial division routine," *Comm. ACM.*, v. 17, 1974, pp. 272–276.