



**HAL**  
open science

# SOME FACTORS OF NUMBERS OF THE FORM $b^n \pm 1$ FOUND USING ECM WITH NEW CLASSES OF CURVES

François Morain

► **To cite this version:**

François Morain. SOME FACTORS OF NUMBERS OF THE FORM  $b^n \pm 1$  FOUND USING ECM WITH NEW CLASSES OF CURVES. 2021. hal-03437714v1

**HAL Id: hal-03437714**

**<https://inria.hal.science/hal-03437714v1>**

Preprint submitted on 20 Nov 2021 (v1), last revised 31 Mar 2022 (v2)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# SOME FACTORS OF NUMBERS OF THE FORM $b^n \pm 1$ FOUND USING ECM WITH NEW CLASSES OF CURVES

F. MORAIN

The elliptic curve method of factorization (ECM) [2] is one of the powerful algorithms able to find moderate size factors of large integers. The following tables list some unknown factors of composite numbers  $b^n \pm 1$  for values of  $13 \leq b \leq 10^4$ , full tables of which are managed by Jonathan Crombie (continuing the work of Brent, Montgomery and te Riele, see <http://myfactors.mooo.com/>). This is an extension of the Cunningham project [1] for  $2 \leq b \leq 12$ . All the factors were found using GMP-ECM [4] (with the algorithms described in [3]).

More details on the computations and curves used will be given in the full version of the article.

**Format of the tables:** pretty straightforward. Remember that  $b, n+$  (resp.  $b, n-$ ) designates  $b^n + 1$  (resp.  $b^n - 1$ ). The last column contains a time stamp. For instance, 210919220236 should be decoded as 21/09/19:22.02.36 or 22h 02 min 36 sec on 19, September 2021. Numbers are sorted by increasing date of discovery. More factorizations will be added as time goes by.

## REFERENCES

- [1] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr. *Factorizations of  $b^n \pm 1$ ,  $b = 2, 3, 5, 6, 7, 10, 11, 12$  up to high powers*. Number 22 in Contemporary Mathematics. AMS, 2 edition, 1988.
- [2] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126:649–673, 1987.
- [3] P. Zimmermann and B. Dodson. 20 years of ECM. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Algorithmic Number Theory – ANTS-VII*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 525–542. Springer-Verlag, 2006.
- [4] P. Zimmermann et al. GMP-ECM (elliptic curve method for integer factorization). <https://gforge.inria.fr/projects/ecm/>, 2010.

$rk$	$N$ factor of $(dd)$	$p \mid N$	$dd$	when
1	89, 136 + (226dd)	203670153440347727407773377	27	210919220236
2	76, 143 - (226dd)	1081673573275568956913253438874031	34	210919220301
3	91, 143 + (229dd)	39097487455641709584561227838397	32	210919233345
4	91, 136 + (238dd)	9909969840558744190100319969953	31	210920000550
5	77, 148 + (246dd)	6133384128714567850895531329681	31	210920012712
6	85, 143 - (228dd)	6314059662689865591498003869	28	210920023351
7	91, 136 + (238dd)	88917809909800972925556006648298103113249	41	210920191115
8	83, 136 + (224dd)	122131139150783253754177955960717201	36	210920233543
9	85, 136 + (244dd)	4812510031276568181537132034273006315681	40	210921034739
10	90, 136 + (243dd)	95029336145694838957824482284328662990992760116961	50	211001001346
11	86, 143 + (226dd)	121802385644813164533936967364856084136235563	45	211002060429
12	89, 136 + (226dd)	1507236940222560786386041061745902423210609	43	211002233552
13	91, 143 - (229dd)	72384483510845642297891730646993695081321681523	47	211003103136
14	93, 136 + (224dd)	144361306010767021849232771856031876990280881	45	211004015217
15	58, 148 + (245dd)	112506882306629149019180463529	30	211014110840
16	59, 148 + (246dd)	26642397493750326276664956281	29	211014124008
17	63, 148 + (239dd)	24427916239531892701088033849	29	211014133356
18	57, 148 + (243dd)	169148129899316676754479151313	30	211014135020
19	57, 148 + (243dd)	421009383140130353639417265637529	33	211014143406
20	62, 148 + (231dd)	174489389275935490478092942757189489	36	211015013516
21	63, 148 + (239dd)	126775587192783617996871593158271705801	39	211015021559
22	75, 148 + (239dd)	287256660129937632149933799072015793	36	211015025728
23	72, 143 + (219dd)	257046566603437226512911589147	30	211016071715
24	95, 143 + (223dd)	1083464823584081602004225920974229961236997	43	211016115307
25	63, 148 + (239dd)	2708217308807273429767899154174901407393	40	211017013219
26	80, 148 + (249dd)	528008828433104496135816963159066412667528154401	48	211019054012
27	59, 148 + (246dd)	6153600891183451358288633718234351691755490502156977	52	211019130348
28	68, 148 + (226dd)	6293335603138665673753869409668883438923628000153	49	211023050826
29	58, 148 + (245dd)	195506542210979176522718797760192511806277913	45	211026193511
30	59, 148 + (246dd)	32549598165881659323145053260648245905788521	44	211027053852
31	95, 145 - (222dd)	200665557019668388820419786457045587248891341	45	211030231819
32	88, 143 + (215dd)	6358121600282021249167413373357836215012153	43	211103190804
33	74, 145 + (210dd)	3242269523406605838609691912552260883503075877086401	52	211103235736
34	82, 145 + (211dd)	8674789605346661424832133115073007844671	40	211104111001
35	69, 145 + (206dd)	286508193459105224545095761	27	211104120058
36	80, 136 + (208dd)	14282340552001320145244125431697889	35	211104121931
37	832, 67 - (191dd)	5152060195650213711128948395000809254091832789	46	211105073607
38	82, 145 + (171dd)	684748065015589423265391174612848221496545022161	48	211105104548
39	908, 67 - (190dd)	314924992520095186813704379189470025083148513889	48	211105120519
40	97, 143 + (205dd)	5029284168421691009474960293330997501	37	211105133632
41	85, 143 + (211dd)	1256721029775715696257972132260210008844808941	46	211106032159
42	80, 136 + (173dd)	1779586756730767305188268537007290668449	40	211106123700
43	78, 145 + (207dd)	810726926248106462415561622241332161181	39	211106123941
44	77, 145 + (204dd)	5351129477105280700750350283769394807311831	43	211106160032
45	61, 148 + (206dd)	5392083635732772033735788905270233582687837357169	49	211107010418
46	77, 145 + (161dd)	15284105262481307713678612469222143741121	41	211107144237
47	69, 145 + (180dd)	51642735295054165114200696495014578655491621	44	211109025120
48	78, 143 - (203dd)	58906988500210848827148393647	29	211109124303
49	74, 145 - (198dd)	115699409434579757150069122314705902015821	42	211110124157
50	74, 145 - (157dd)	82680336163400607564958279513497353433701	41	211110131700

$rk$	$N$ factor of $(dd)$	$p \mid N$	$dd$	when
51	71, 145 + (200dd)	3081838728839138646824667134834215417088225761	46	211110222511
52	74, 145 - (116dd)	672757891558157197623408574883629411681	39	211110222529
53	737, 67 + (184dd)	870917417466838788698821597667901172952093040299	48	211111104615
54	682, 67 + (185dd)	3960431214365287888129140722498272391957628371	46	211112150625
55	68, 145 + (201dd)	759522532722573631464900168860811795924541	42	211112165156
56	79, 136 + (212dd)	1676257114889837463366010414743038265629041	43	211113115453
57	79, 143 + (201dd)	617165874719529966578857601636808679159	39	211113125510
58	69, 143 + (195dd)	46032704990894163010799652245639	32	211114031451
59	564, 67 - (182dd)	1200634750265355597309123978159925198537240793	46	211114070952
60	97, 145 + (195dd)	20475011708627365490421549472180159901	38	211115132205
61	75, 145 - (195dd)	145820922799205411577526521075547603991	39	211115215945
62	87, 145 + (194dd)	59493967220771242233729202831	29	211115224834
63	76, 136 + (193dd)	230638965208492675830062875068689	33	211115232601
64	76, 136 + (161dd)	156680649601795675183141661297	30	211116040304
65	98, 145 - (192dd)	4538131062026968680387147363911	31	211116115540
66	76, 136 + (131dd)	438641314708689994945803094414364017	36	211116121717
67	97, 145 + (158dd)	20325839679108068942542957640818669021	38	211116145935
68	98, 145 - (161dd)	106565478545504059784085620836190321	36	211116155111
69	88, 143 - (205dd)	176631419599003306284596237977817343802484627	45	211116162947
70	89, 145 - (192dd)	243056674739683873052967962822255497291	39	211116235218
71	76, 136 + (96dd)	748413049020504684792641386896154057664353	42	211117023558
72	89, 145 - (154dd)	267697400207700352494793748295552781	36	211117051016
73	93, 143 + (185dd)	1107143747609638086483933799	28	211117102506
74	71, 143 + (185dd)	6147619877984764806596458300991243997791	40	211117143423
75	54, 148 + (181dd)	1873736382664056942125771790331768514929	40	211117170211
76	87, 143 - (186dd)	869739041700065774535952087462183871	36	211117170847
77	54, 148 + (142dd)	47745297013416763673913373201	29	211117191122
78	87, 143 - (150dd)	136899949256066917953836347405696564733147	42	211119071214
79	84, 145 - (177dd)	1280935678670178982674695168311861	34	211119175550
80	54, 148 + (113dd)	79647427812727331528378671705173747075361	41	211119204943
81	85, 145 - (174dd)	201832808531929277425202546329975236601	39	211120030246
82	85, 145 - (136dd)	186647494681298441991785036724963841	36	211120034412