V. Update to the Introduction for the Third Edition.

The tables of the second edition contained all factors known to the authors on June 22, 1987. Since then more than two thousand new factorizations have been discovered. Appendix C lists the smallest composite cofactors in the tables. In the first edition this appendix contained numbers with 51 to 64 digits. In the second edition it contained numbers with 80 to 100 digits. It now contains numbers with 130 to 142 digits. The lists of "wanted" factorizations in the first edition had 25 numbers with 52 to 71 digits. These have all been factored. The lists of "wanted" factorizations in the second edition had 32 numbers with 86 to 291 digits. These have all been factored. Other "wanted" lists have since been issued and many of their entries have been factored. The current "wanted" lists (see **B** below) now contain numbers with 141 to 212 digits. All of the numbers considered in the 1925 Cunningham-Woodall book [**11**] have been completely factored!

The smallest probable prime (PRP) in Appendix A of the second edition had 222 digits. Prime proofs have now been completed for all prime numbers in that appendix, as well as for primes found since 1988. In this edition we have updated the tables and appendices to September 18, 2001, and reviewed the developments in technology, factorization and primality testing which have produced the recent advances. We also include a few references to recent related work which may interest the reader.

We extended the tables with base $b > 2$ in the second edition, and we have lengthened them again in the third edition. We have attempted to factor the new numbers added to these tables using about the same effort that was applied to numbers in the second edition.

The format of the tables and appendices has been changed a little in this edition. In the first and second editions, all penultimate prime factors fit on a single line, which allowed us to break lines only at multiplication dots. Because we can now factor much larger numbers than before, some penultimate prime factors have more than 75 digits and are given on two lines with a continuation slash (\) at the end of the first line. For example, in the 2− Table one finds the entry

571 5711.27409.69693366045316671685098712301007940958018325270028\
4954822613267591617292 7.*P*91

The prime factor 6969...00284954...2927 was too long to fit on one line and had to be broken.

A. Developments Contributing to the Third Edition.

1. Developments in Technology.

The use of many personal computers and supercomputers for factoring has continued, but no new machines especially designed for factoring have been built recently.

A. K. Lenstra and M. S. Manasse [**328**] ran their ECM and quadratic sieve programs on networks of hundreds of small computers. H. J. J. te Riele, W. M. Lioen and D. T. Winter have factored 7,122+ C87 and 6,131− C92 by the quadratic sieve algorithm on a NEC SX-2, the world's fastest single-CPU vector computer

(at least at that time). Later they factored 2,463+ C101 by the quadratic sieve algorithm running on one processor of a Cray Y-MP4. See also [**305**].

W. R. Alford and C. Pomerance [**302**] have implemented the quadratic sieve on hundreds of PC-class computers and factored the 95-digit numbers 7,128+ and 2,332+ and the impressive 100-digit number 12,119+. Y. Kida has factored several numbers of 95 to 101 digits with the quadratic sieve on many small computers.

B. Dixon and A. K. Lenstra [**316**] have written an ECM program for the MasPar computer. It found many factors reported in the third edition, including the 35-digit prime divisor of 2,511+. Lenstra [**324**] has factored many numbers in this edition by the quadratic sieve and the number field sieve on a MasPar computer.

ECMNET is a group of people who factor large numbers with T. Granlund's ECM program. They have found many factors reported in the third edition, including the 53-digit prime factor of 2,677−.

The group NFSNET [**320**] has used dozens of computers around the world to factor numbers by the special number field sieve. Their factorization of 3,349− yielded the largest penultimate prime factor known (80 digits) of any Cunningham primitive part at the time. This record has since been eclipsed by the 93-digit penultimate prime factor of 10,211− C211, found by another group called The Cabal. Yet another group, NFSNET′ continued this work by factoring 2,629− and several other numbers reported in this edition.

2. Developments in Factorization.

Most new factors in this third edition were discovered by the quadratic sieve algorithm, the elliptic curve method or the number field sieve. (See **IV A 2**(c) and (d).)

A. K. Lenstra and M. S. Manasse [**329**] gave a modification to the quadratic sieve in which up to two primes larger than the factor base limit may be saved and used. This modification also speeds the number field sieve. A different modification accelerates the quadratic sieve by amortizing the polynomial initialization time. The computer science term "amortizing" here means that the cost of setting up several polynomials together is averaged over them. The modification sets up 2^k polynomials for the effort of k setups, which has the effect of accelerating the setup by a factor of $k2^{-k}$. R. Peralta [**338**] calls this version the hypercube quadratic sieve, while W. R. Alford and C. Pomerance [**302**] call it the self-initializing quadratic sieve. Many factors reported in this edition were computed using these modifications. Just before the third edition went to press, P. Leyland and J. Franke experimented with a variation of the quadratic sieve which allows up to three large primes to be used. They found that this change speeds the algorithm beyond the use of two large primes. SSW aided Leyland's effort by combining the hypercube and three large primes variations, producing an even faster version of the quadratic sieve. This work resulted in the factorization of the 135-digit divisor of 2,1606L.

Several factors were found by an FFT extension to the $p-1$ method (see **III B 2**(e)) which was implemented by R. D. Silverman [**333**]. P. Montgomery [**330**] has invented an FFT extension to ECM, and it has found some new factors of Cunningham numbers. A. O. L. Atkin and F. Morain [**303**] describe an improved method of choosing ECM curves which speeds the algorithm. Silverman and SSW [**342**] tell how to choose the parameters in ECM.

A new factoring algorithm, the number field sieve [**326**], has been used by A. K. Lenstra and M. Manasse, by Silverman, by CWI and by NFSNET [**320**] to achieve

some factorizations reported here. Two impressive ones were the factorizations of 2,512+ C148 (see [**327**]) and of 2,523− C158. The original algorithm works best for numbers of the form $b^n \pm c$, where c is small. It does not take advantage of any small factors which may already be known of a number of this form. Thus, for example, Lenstra and Manasse had to factor the entire 155-digit number $F_9 = 2^{512} + 1$, not just the 148-digit cofactor.

L. M. Adleman [**301**] has described some improvements to the number field sieve. The general number field sieve is a variation which factors numbers without special form. Though less efficient than the special number field sieve, it beats the quadratic sieve for large enough numbers. So far, it has factored only a few Cunningham numbers. The first general number field sieve factorization was that of 3,367− C105 by FactOregon and CWI. Several papers about the number field sieve were published in the book [**325**]. See also C. Pomerance's paper [**339**].

See [**320**] for some clever ways to choose polynomials for the number field sieve. See [**319**] for some implementation details for the number field sieve. In a paper in [**325**], J. M. Pollard proposed the lattice sieve, a variation of the relation collection step of the number field sieve. In [**321**], R. A. Golliver, A. K. Lenstra and K. S. McCurley implemented this algorithm and achieved a substantial speed-up compared to other relation collection versions reported in the literature. Near the end of the number field sieve algorithm, one has to compute the square root of a product of thousands of algebraic numbers. J. M. Couveignes' article in [**325**] deals with this problem, as does P. Montgomery's paper [**331**].

In the final step of the quadratic sieve and the number field sieve one must find the null space of a huge matrix over $\mathbf{GF}(2)$. Several papers [**313,314,323**] tell how to perform this elimination step efficiently. The ideas in these papers speeded this part of the algorithm for some factorizations reported in this edition.

M. Morimoto and Y. Kida have published a table [**336**] of the factorizations of the numbers $\Phi_n(x)$ for $1 \le x \le 1000$ and those n for which $\phi(n) = 16$ or 18. Their book also lists the n and x for which $\phi(n) \le 100$, $1 \le x \le 1000$ and $\Phi_n(x)$ is prime or probably prime. A second volume [**337**] of their book factors the numbers $\Phi_n(x)$ for $1 \le x \le 1000$ and those n for which $\phi(n) = 20$ or 22. It also lists the n and x for which $102 \le \phi(n) \le 156$, $1 \le x \le 1000$ and $\Phi_n(x)$ is prime or probably prime.

Paper [**343**] by N. M. Stephens on ECM should have been cited in **IV A 2**(d). See P. Stevenhagen [**344**] for more about the Aurifeuillian factorizations in **III C 2**. R. P. Brent [**308**] tells how to compute the coefficients of Aurifeuillian factorizations, as does SSW [**346**]. D. M. Bressoud and H. Wada have published books [**311**] and [**345**] on factorization and primality testing. A second edition of H. Riesel's book ([**243**] of our first edition) has appeared as [**340**]. P. Montgomery has written an excellent survey article [**332**] on factoring.

H. C. Williams and J. O. Shallit have written an informative history [**347**] of factoring integers and primality testing from about 1750 to about 1950. These two authors and F. Morain [**341**] have discovered a sieve built 75 years ago by E.-O. Carissan.

3. Developments in Primality Testing.

W. Bosma and M. P. van der Hulst [**307**] have described an efficient version of the Jacobi sum primality test of Cohen and Lenstra (see **IV A 3** (a)). Bosma [**306**] has proved some new primality tests for $h \cdot 2^k \pm 1$. Using A. O. L. Atkin's method

(see **IV A 3**(b) and [**304**]), F. Morain [**334**], [**335**] has completed primality proofs for all probable primes in Appendix A, including the new large primes reported in this edition.

B. Status of the Project and of Important Factorizations.

The tables in this book presently reside in data sets at Purdue University. The latest versions of them are available at the web site

`http://www.cerias.purdue.edu/homes/ssw/cun/index.html`.

During the past thirteen years these tables have been improved by the factorization of about ten of their numbers per month. SSW reported the new factors in annual Updates to the book and more frequent "Pages" of new factors. If you factor any numbers in this book or if you would like to receive the Updates and Pages, please write to:

Professor Samuel S. Wagstaff, Jr.
Department of Computer Sciences
Purdue University
West Lafayette, IN 47907 USA
Email: `ssw@cerias.purdue.edu`

The pace of about ten new factorizations per month continues in 2001. In recent months no new prime factor < 35 digits has been reported to us.

The earlier editions of this book mentioned the Computer Museum in Massachusetts where one could view DHL's sieve machines discussed in **III B 1** (b) and (c) and **III B 2** (c). While the Computer Museum remains in Boston, the sieves have been moved to the Computer History Museum located at Moffett Field in Mountain View, California. H. C. Williams no longer uses the sieve built by C. D. Patterson [**258**]. It has been replaced by a new sieve called the MSSU, which is much faster and easier to use.

For many years we have maintained lists of "most wanted" and "more wanted" factorizations. At this time these lists read as follows:

Ten "Most Wanted" Factorizations

1.	2,673−	C151	6.	6,257−	C173
2.	2,647+	C169	7.	5,289+	C156
3.	3,397−	C178	8.	5,298+	C189
4.	3,397+	C162	9.	12,178+	C145
5.	10,223−	C211	10.	11,197+	C205

Twenty-Four "More Wanted" Factorizations

2,653+	C154	2,1262M	C178	6,244+	C178	10,227−	C212
2,659+	C188	2,1294L	C187	6,251+	C179	10,223+	C201
2,661+	C148	2,716+	C163	6,257+	C200	10,226+	C197
2,1238L	C160	3,404+	C141	7,233−	C155	10,229+	C164
2,1238M	C145	5,307−	C187	7,232+	C171	11,199−	C173
2,1262L	C177	5,302+	C187	7,233+	C150	12,179−	C190

Many of these numbers are, of course, the first "hole" in their respective tables. All numbers from the 1925 Cunningham-Woodall tables have been finished. All numbers from the base 3 to base 12 tables in our first and second editions have been factored.

It is known that $2^p - 1$ is prime for $p = 2$, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377 and 6972593, but for no other $p < 3945000$. Thus, $2^{3021377} - 1$ is the thirty-seventh Mersenne prime and $2^{6972593}$ is probably the thirty-eighth one. See [**101**] and [**222**] for the search to 100000. (See Haworth [**223**] for an extensive bibliography of papers on Mersenne numbers. See Colquitt and Welsh [**312**] for the discovery of the prime $2^{110503} - 1$.) See the web site

`http://www.utm.edu/research/primes/largest.html`

for the latest information about Mersenne and other large primes. The last few Mersenne primes have been found by GIMPS, the Great Internet Mersenne Prime Search, launched by George Woltman in 1996.

The "repunits" $(10^p - 1)/9$ are prime for $p = 2$, 19, 23, 317 and 1031 and for no other $p < 20000$. (See Williams and Seah [**112, 113**] and Williams and Dubner [**257**] for these results.) Dubner [**317**] has tested all p between 10000 and 50000 and found that $(10^{49081} - 1)/9$ is a probable prime and that no other repunit primes have p in this range. Recently, Lew Baxter found that $(10^{86453} - 1)/9$ is a probable prime.

Here is a list of the known prime and probable prime "repunits" $(b^p - 1)/(b - 1)$ to base b for $b = 3$, 5, 6, 7, 11 and 12. Williams and Seah [**113**] tested all $p \le 1000$ for these bases. Dubner [**317**] has tested all p less than at least 10000 for these bases. (The probable primes are marked with stars.)

Base b	$p \le 10000$ for which $(b^p - 1)/(b - 1)$ is prime or probable prime$*$.
3	$3, 7, 13, 71, 103, 541, 1091*, 1367*, 1627*, 4177*, 9011*, 9551*$
5	$3, 7, 11, 13, 47, 127, 149, 181, 619, 929, 3407*, 10949*$
6	$2, 3, 7, 29, 71, 127, 271, 509, 1049*, 6389*, 10613*$
7	$5, 13, 131, 149, 1699*$
11	$17, 19, 73, 139, 907, 1907*, 2029*, 4801, 5153*, 10867*$
12	$2, 3, 5, 19, 97, 109, 317, 353, 701*, 9739*$

The Fermat number F_{22} was shown composite in 1993 by Crandall, J. Doenias, C. Norrie, and J. Young [**315**]. Likewise, F_{24} was shown composite in 1999 by Mayer, Papadopoulos and Crandall. The remaining cofactors of F_{12}, F_{13}, F_{15}, F_{16}, F_{17}, F_{18}, F_{19} and F_{21} have been shown to be composite. McLaughlin found the factor of F_{25}. T. Taura found the factor of F_{28}. Thus, F_{33} is the smallest Fermat number whose character is unknown.

We now know that the Fermat numbers F_m are composite for $5 \le m \le 32$. No factor is known for F_{14}, F_{20}, F_{22} or F_{24}. These numbers were proved composite [**96, 263**] by Pépin's [**78**] test. The cofactors of F_{12}, F_{13}, F_{15} through F_{19}, and F_{21} are known to be composite. A résumé of the known prime factors $k.2^n + 1$ of F_m is given in the tables on the next pages. Some of the new factors may be found in [**221, 224, 250, 252, 309, 310, 318, 322, 348**]. See the URL

`http://www.prothsearch.net/fermat.html`

for Wilfrid Keller's list of all known Fermat factors and their discoverers.

Prime factors $k \cdot 2^n + 1$ of Fermat numbers $F_m = 2^{2^m} + 1$, $5 \le m \le 11$

m	k	$n-m$
5	5	2
	52347	2
6	1071	2
	262814145745	2
7	116503103764643	2
	11141971095088142685	2
8	604944512477	3
	456355662672646375825993936521518049726812683308780217677 15	3
9	37	7
	364043106721088096110224401181662837831219059 7	2
	362128936829849024182024971631805407255830459520272960891 5\	
	143145236405075706567422328216365693 07	2
10	11131	2
	395937	4
	113764057256348108966419940016522905 1	2
	159228362311386950350933555659802128841074866750014516829 7\	
	061716025786331194724897145266454804359190623764452256383 3\	
	477152239872181860196421948439690685317315553051258143326 4\	
	809455775168889760265648430068955735004981338256435940925 5\	
	5886322403200003	3
11	39	2
	119	2
	10253207784531279	3
	434673084282938711	2
	211746151341732855749827845293346897433376275297441509581 7\	
	224353776410878819325059296765604619248500707810191265277 6\	
	662834559689734635521223667093019353364100169585433799507 3\	
	209373716881590769708870374935815693521187765210649584221 6\	
	393381264904402650255855535677556006746164899342675004906 1\	
	580191794744396103493131476781686200989377719638682976424 8\	
	739735740859519803163713768591049927953187299848018697851 4\	
	558880949203896931728432065150041842594934549494444811005 7\	
	412733268967446592534704415768023768439849177511907048426 1\	
	368465618487113773793191457181770750 53	2

Prime factors $k \cdot 2^n + 1$ of Fermat numbers $F_m = 2^{2^m} + 1$, $12 \le m \le 18$

m	k	$n-m$
12	7	2
	397	4
	973	4
	11613415	2
	76668221077	2
13	41365885	3
	20323554055421	4
	6872386635861	6
	609485665932753836099	6
15	579	6
	17753925353	2
	1287603889690528658928101555	2
16	1575	3
	180227048850079840107	4
17	59251857	2
18	13	2
	9688698137266697	5

Prime factors $k \cdot 2^n + 1$ of Fermat numbers $F_m = 2^{2^m} + 1$, $19 \le m \le 4600$

m	k	$n-m$	m	k	$n-m$	m	k	$n-m$
19	33629	2	99	16233	5	375	733251	2
	308385	2	107	1289179925	4	376	810373	2
21	534689	2	116	3433149787	4	380	321116871	5
23	5	2	117	7	3	398	120845	3
25	48413	4	122	5234775	2	416	8619	2
	1522849979	2	125	5	2		38039	3
	16168301139	2	133	88075576149	2	417	118086729	4
26	143165	3	142	8152599	3	431	5769285	3
27	141015	3	144	17	3	452	27	3
	430816215	2	146	37092477	2	468	27114089	3
28	25709319373	8	147	3125	2	544	225	3
29	1120049	2		124567335	2	547	77377	3
30	149041	2	150	5439	4	556	127	2
	127589	3		1575	7	579	63856313	2
31	5463561471303	2	164	1835601567	3	620	10084141	4
32	1479	2	172	20569603303	2	635	4258979	10
36	5	3	178	313047661	2	637	11969	6
	3759613	2	184	117012935	3	642	52943971	2
37	1275438465	2	201	4845	3	667	491628159	2
38	3	3	205	232905	2	692	717	3
	2653	2	207	3	2	723	554815	7
39	21	2	215	32111	2	744	17	3
42	43485	3	226	15	3	851	497531	8
43	212675402445	2	228	29	3	885	16578999	2
48	2139543641769	2	230	372236097	2	906	57063	2
52	4119	2	232	70899775	4	931	1985	2
	21626655	2	250	403	2	1069	137883	4
55	29	2	251	85801657	3	1082	82165	2
58	95	3	255	629	2	1114	11618577	2
61	54985063	5	256	36986355	2	1123	25835	2
62	697	2	259	36654265	3	1225	79707	6
63	9	4	267	177	4	1229	29139	4
64	17853639	3	268	21	8	1451	13143	3
66	7551	3	275	22347	4	1551	291	2
71	683	2	284	7	6	1598	10923781	2
72	76432329	2		1061341513	2	1849	98855	2
73	5	2	287	5915	2	1945	5	2
75	3447431	2	298	247	4	1990	150863	3
77	425	2	301	7183437	3	2023	29	4
	5940341195	2	316	7	4	2059	591909	4
81	271	3	329	1211	4	2089	431	10
88	119942751127	2	334	27609	7	2456	85	2
90	198922467387	2	338	27654487	4	3310	5	3
91	1421	2	343	4844391185	2	3506	501	2
93	92341	3	353	18908555	2	4250	173373	2
94	482524552001	3	370	573230511	3	4258	1435	4

Prime factors $k \cdot 2^n + 1$ of Fermat numbers $F_m = 2^{2^m} + 1$, $4600 < m$

m	k	$n-m$	m	k	$n-m$	m	k	$n-m$
4724	29	3	13250	351	2	41894	4935	3
5320	21341	3	13623	48265	3	43665	2495	2
5957	421435	3	14252	1173	2	49093	165	2
6208	763	2	14276	157	4	63679	169	7
6355	115185	3	14528	17217	2	83861	99	2
6390	303	3	15161	55	3	90057	189	4
6537	17	2	17906	135	3	91213	585	2
6835	19	3	18749	11	10	94798	21	3
6909	6021	3	18757	33	9	95328	7	2
7181	168329	6	19211	13323	9	113547	39	2
7309	145	3	22296	4777	2	114293	13	3
8239	7473	3	23069	681	2	125410	5	3
8555	645	2	23288	19	2	142460	159	2
9322	8247	2	23471	5	2	146221	57	2
9428	9	3	24651	99	2	157167	3	2
9448	19	2	25006	57	4	213319	3	2
9549	1211	2	28281	81	4	303088	3	5
12185	81	4	35563	357	4	382447	3	2

C. Acknowledgements for the Third Edition.

We wish to thank the following people who have contributed to the Third Edition:

New factors of Fermat numbers and numbers in the main tables were discovered by K. Aardal, W. Alford, G. Axelsson, R. Baillie, R. Ballinger, B. Beesley, D. Bernstein, M. Bodschwinna, H. Boender, A. Bot, R. Brent, A. Brown, J. Buhler, S. Cavallar, S. Contini, J. Cosgrave, R. Crandall, C. Curry, N. Daminelli, F. Damm, V. Danilov, J. Davis, P. Demichel, K. Dilcher, B. Dodson, D. Doligez, H. Dubner, L. Durman, S. Edick, R. Edwards, M. Elkenbracht-Huizing, A. Erdmann, W. Florek, T. Forbes, J. Fougeron, J. Franke, Y. Gallot, P. Gaudry, J. Gilchrist, G. Gostin, W. Grabysz, M. Graff, T. Granlund, P. Grobstich, G. Gusev, R. Harley, F. Heider, D. Holdridge, R. Horn, S. Huddleston, M. Hürter, C. Kerchner, Y. Kida, T. Kleinjung, J. Klos, K. Koyama, A. Kruppa, H. Kuwakado, D. Leclair, J. Leherbauer, A. Lenstra, R. Lercier, R. Lewis, P. Leyland, W. Lioen, S. Lodin, J. Loho, A. Lynch, M. Mambo, M. Manasse, J. Marchand, E. Mayer, R. McIntosh, P. McLaughlin, Jr., J.-C. Meyrignac, N. Melo, D. Miller, P. Montgomery, F. Morain, D. Morenus, A. Muffett, B. Murphy, P. Nicholson, T. Nohara, T. Nokelby, E. Okamoto, R. Peralta, C. Pomerance, R. Prethaler, C. Putnam, M. Quercia, J. Rathert, J. Renze, R. Robson, R. Ruby, D. Rusin, P. Samidoost, G. Sassoon, A. Schmidt, R. Silverman, N. Smart, V. Stevens, H. Suyama, T. Szep, D. Takahashi, C. Tardif, T. Taura, H. te Riele, Y. Torii, V. Trevisan, C. van Halewyn, R. Wackerbarth, G. Wambach, S. Whitaker, M. Wiener, D. Winter, D. Wolf, G. Woltman, J. Young, J. Zayer, P. Zimmermann, SSW, many volunteers who keep factoring programs running on their workstations, and an anonymous factorer who calls himself "M. Mersenne".

The new results of the third edition required millions of hours of computer time. We are grateful to the directors and staffs of the following computer centers which

provided this time: Convex Computer Corporation, NeXT Computer, Inc., the National Center for Supercomputing Applications, JAIST, the Center for Cryptography, Computer and Network Security at the University of Wisconsin-Milwaukee, Microsoft Research, Unisys (formerly System Development Corporation), UCLA Department of Mathematics, Oregon State University Department of Mathematics, Centrum voor Wiskunde en Informatica the Dutch National Aerospace Laboratory in The Netherlands, the Universität des Sarlandes, Germany, INRIA (Institut National de Recherche en Informatique et Automatique), the Poznan Supercomputer and Networking Centre, Medicis Polytechique, the High Performance Computer Centre North, the Swedish Institute for Computer Science, the Maths Department of the Stockholm University, Swox, Circus Ulfberg, the Astonomy Department of Uppsala University, and Purdue University.

M. Senn and R. M. Jegadeesan wrote programs which formatted the tables in this book.

SSW gratefully acknowledges the support of the Lilly Foundation and the Center for Education and Research in Information Assurance and Security in the preparation of this edition and of the annual updates.

References

The first edition had references 1-118; they appear in **III E**. The second edition had references 201-263; they appear in **IV D**.

301. L. M. Adleman, *Factoring numbers using singular integers*, Proceedings 23nd Annual ACM Symposium on Theory of Computing (STOC) (1991), 64–71.
302. W. R. Alford and C. Pomerance, *Implementing the self-initializing quadratic sieve on a distributed network*, Number Theoretic and Algebraic Methods in Computer Science, A. van der Poorten, I. Shparlinski and H. G. Zimmer, editors, Moscow, 1993, pp. 163–174.
303. A. O. L. Atkin and F. Morain, *Finding suitable curves for the elliptic curve method of factorization*, Math. Comp. **60** (1993), 399–405, MR 93k:11115.
304. A. O. L. Atkin and F. Morain, *Elliptic curves and primality proving*, Math. Comp. **61** (1993), 29–68, MR 93m:11136.
305. H. Boender and H. J. J. te Riele, *Factoring integers with large-prime variations of the quadratic sieve*, Experimental Math. **5** (1996), 257–273, MR 97m:11155.
306. W. Bosma, *Explicit primality criteria for* $h \cdot 2^k \pm 1$, Math. Comp. **61** (1993), 97–109, MR 94c:11005.
307. W. Bosma and M. P. van der Hulst, *Primality Proving with Cyclotomy*, Proefschrift, University of Amsterdam, Amsterdam, 1990.
308. R. P. Brent, *On computing factors of cyclotomic polynomials*, Math. Comp. **61** (1993), 131–149, MR 93m:11131.
309. R. P. Brent, *Factorization of the tenth Fermat number*, Math. Comp. **68** (1999), 429–451, MR 99e:11154.
310. R. P. Brent, R. E. Crandall, K. Dilcher and C. van Halewyn, *Three new factors of Fermat numbers*, Math. Comp. **69** (2000), 1297–1304, MR 2000j:11194.
311. D. M. Bressoud, *Factorization and Primality Testing*, Springer-Verlag Undergraduate Texts in Mathematics, Berlin, New York, 1989.
312. W. N. Colquitt and L. Welsh, Jr., *A new Mersenne prime*, Math. Comp. **56** (1991), 867–870, MR 91h:11006.
313. Don Coppersmith, *Solving linear equations over GF(2): Block Lanczos algorithm*, Lin. Alg and its Apps. **192**, 33–60, MR 94c:11124.
314. Don Coppersmith, *Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm*, Math. Comp. **62**, 333–350.
315. R. Crandall, J. Doenias, C. Norrie and J. Young, *The twenty-second Fermat number is composite*, Math. Comp. **64** (1995), 863–868, MR 95f:11104.
316. B. Dixon and A. K. Lenstra, *Massively parallel elliptic curve factoring*, *Advances in Cryptology, Proceedings of Eurocrypt '92*, Lecture Notes in Computer Science 658, Springer-Verlag, Berlin, New York, 1993, pp. 183–193.
317. Harvey Dubner, *Generalized repunit primes*, Math. Comp. **61** (1993), 927–930, MR 94a:-11009.
318. Harvey Dubner and Wilfrid Keller, *Factors of generalized Fermat numbers*, Math. Comp. **64** (1995), 397–405, MR 95c:11010.
319. R.-M. Elkenbracht-Huizing, *An implementation of the number field sieve*, Experimental Math. **5** (1996), 231–253, MR 98a:11182.
320. R.-M. Elkenbracht-Huizing, P. L. Montgomery, R. D. Silverman, R. K. Wackerbarth and S. S. Wagstaff, Jr., *The number field sieve on many computers*, CRM Proceedings and Lecture Notes **19** (1999), 81–85, MR 2000e:11157.
321. Roger A. Golliver, Arjen K. Lenstra and Kevin S. McCurley, *Lattice sieving and trial division*, *Algorithmic Number Theory* (*Ithaca, NY* 1994), Lecture Notes in Computer Science 877, Springer-Verlag, Berlin, New York, 1994, pp. 18–27.
322. Gary B. Gostin, *New factors of Fermat numbers*, Math. Comp. **64** (1995), 393–395, MR 95c:11151.
323. B. A. LaMacchia and A. M. Odlyzko, *Solving large sparse linear systems over finite fields*, *Advances in Cryptology–Crypto '90*, Lecture Notes in Computer Science 537, Springer-Verlag, Berlin, New York, 1991, pp. 109–133.
324. A. K. Lenstra, *Massively parallel computing and factoring*, *Proceedings of LATIN '92*, Lecture Notes in Computer Science 583, Springer-Verlag, Berlin, New York, 1992, pp. 344–355.
325. A. K. Lenstra and H. W. Lenstra, Jr., *The development of the number field sieve*, Lecture Notes in Mathematics 1554, Springer-Verlag, Berlin, New York, 1993, MR 96m:11116.

326. A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse and J. M. Pollard, *The number field sieve*, Proceedings 22nd Annual ACM Symposium on Theory of Computing (STOC), Baltimore, 1990, pp. 564–572.
327. A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse and J. M. Pollard, *The factorization of the ninth Fermat number*, Math. Comp. **61** (1993), 319–349, MR 93k:11116.
328. A. K. Lenstra and M. S. Manasse, *Factoring by electronic mail*, Advances in Cryptology – Proceedings of Eurocrypt '89, Springer-Verlag Lecture Notes in Computer Science, Berlin, New York, 1990, pp. 355–371.
329. A. K. Lenstra and M. S. Manasse, *Factoring with two large primes*, Math. Comp. **63** (1994), 785–798, MR 95a:11107.
330. Peter L. Montgomery, *An FFT Extension of the Elliptic Curve Method of Factorization*, Ph. D. thesis at the University of California, Los Angeles, 1992.
331. Peter L. Montgomery, *Square roots of products of algebraic numbers*, Mathematics of Computation 1943–1993: a Half-Century of Computational Mathematics, Walter Gautschi, editor. Proceedings of Symposia in Applied Mathematics, Amer. Math. Soc., Providence, 1994, pp. 567–571, MR 96a:11148.
332. Peter L. Montgomery, *A survey of modern integer factorization algorithms*, CWI Quarterly **7 (4)** (1994), 337–366, MR 96b:11161.
333. Peter L. Montgomery and Robert D. Silverman, *An FFT extension to the $P-1$ factoring algorithm*, Math. Comp. **54** (1990), 839–854, MR 90j:11142.
334. François Morain, *Atkin's test: News from the front*, Advances in Cryptology – Proceedings of Eurocrypt '89, Springer-Verlag Lecture Notes in Computer Science, Berlin, New York, 1990, pp. 626–635, MR 91m:11111.
335. François Morain, *Courbes elliptiques et tests de primalité*, Ph. D. thesis at Université Claude Bernard–Lyon I, 1990, MR 95i:11149.
336. Mitsuo Morimoto and Yûji Kida, *Factorization of Cyclotomic Numbers*, Department of Mathematics, Sophia University, Tokyo, 1987 (in Japanese).
337. Mitsuo Morimoto, Yûji Kida and Michiyo Saitô, *Factorization of Cyclotomic Numbers, II*, Department of Mathematics, Sophia University, Tokyo, 1989 (in Japanese).
338. R. Peralta, *A quadratic sieve on the n-dimensional hypercube*, Proceedings of Crypto '92, vol. 740, Springer-Verlag, pp. 324–332, MR 95f:11108.
339. Carl Pomerance, *The number field sieve*, Mathematics of Computation 1943–1993: a Half-Century of Computational Mathematics, Walter Gautschi, editor. Proceedings of Symposia in Applied Mathematics, Amer. Math. Soc., Providence, 1994, pp. 465–480.
340. Hans Riesel, *Prime Numbers and Computer Methods for Factorization, second edition*, Birkhäuser, Boston, 1994, MR 95h:11142.
341. Jeffrey Shallit, Hugh C. Williams and François Morain, *Discovery of a lost factoring machine*, Math. Intel. **17** (1995), 41–47, MR 96f:01029.
342. Robert D. Silverman and Samuel S. Wagstaff, Jr., *A practical analysis of the elliptic curve factoring algorithm*, Math. Comp. **61** (1993), 445–462, MR 93k:11117.
343. N. M. Stephens, *Lenstra's factorisation method based on elliptic curves*, *Advances in Cryptology, Proceedings of Crypto '85*, H. C. Williams, ed., Springer-Verlag, Berlin, New York, 1986, pp. 409–416, MR 87k:11140.
344. Peter Stevenhagen, *On Aurifeuillian factorizations*, Nederl. Akad. Wetensch. Indag. Math. **49** (1987), 451–468, MR 89a:11015.
345. Hideo Wada, *Computers and Prime Factorization*, Nebula, Tokyo, 1987 (in Japanese).
346. Samuel S. Wagstaff, Jr., *Aurifeuillian factorizations and the period of the Bell numbers modulo a prime*, Math. Comp. **65** (1996), 383–391, MR 96f:11033.
347. H. C. Williams and J. O. Shallit, *Factoring integers before computers*, Mathematics of Computation 1943–1993: a Half-Century of Computational Mathematics, Walter Gautschi, editor. Proceedings of Symposia in Applied Mathematics, Amer. Math. Soc., Providence, 1994, pp. 481–531, MR 95m:11143.
348. J. Young, *Large primes and Fermat factors*, Math. Comp. **67** (1998), 1735–1738, MR 99a:11010.