Mersenne Numbers

Guy Haworth

PREFACE

These notes have been issued on a small scale in 1983 and 1987 and on request at other times.

This issue follows two items of news. First, Walter Colquitt and Luther Welsh found the 'missed' Mersenne prime M_{110503} and advanced the frontier of complete M_p-testing to 139,267. In so doing, they terminated Slowinski's significant string of four consecutive Mersenne primes. Secondly, a team of five established a non-Mersenne number as the largest known prime. This result terminated the 1952-89 reign of Mersenne primes.

All the original Mersenne numbers with $p < 258$ were factorised some time ago. The Sandia Laboratories team of Davis, Holdridge & Simmons with some little assistance from a CRAY machine cracked M_{211} in 1983 and M_{251} in 1984. They contributed their results to the 'Cunningham Project', care of Sam Wagstaff. That project is now moving apace thanks to developments in technology, factorisation and primality-testing.

New levels of computer power and new computer architectures motivated by the open-ended promise of parallelism are now available. Once again, the suppliers may be offering free buildings with the computer. However, the Sandia '84 CRAY-1 implementation of the quadratic-sieve method is now outpowered by the number-field sieve technique. This is deployed on either purpose-built hardware or large syndicates, even distributed world-wide, of collaborating standard processors.

New factorisation techniques of both special and general applicability have been defined and deployed. The elliptic-curve method finds large factors with helpful properties while the number-field sieve approach is breaking down composites with over one hundred digits.

The material is updated on an occasional basis to follow the latest developments in primality-testing large M_p and factorising smaller M_p; all dates derive from the published literature or referenced private communications. Minor corrections, additions and changes merely advance the issue number after the decimal point.

The reader is invited to report to the address below any errors and omissions that have escaped the proof-reading, to answer the unresolved questions noted and to suggest additional material associated with this subject.

Guy Haworth
33, Alexandra Rd., Reading, Berkshire
England, RG1 5PG

Issue 10.2 of 22/01/90

ACKNOWLEDGMENTS

I must first recall with great pleasure that I was introduced to elementary number theory and the Mersenne numbers by an Oxford copy of Dan Shanks' "Solved and Unsolved Problems in Number Theory". His entertaining text remains most readable in its current third edition and achieves the difficult objective of presenting the key concepts in both a logical and a historical perspective.

In the same spirit, I should next like to thank my colleague Stewart Reddaway of ICL whose interest in parallel processors, multiplication techniques and the Mersenne problem re-awakened my earlier interest in this area. Stewart's DAP implementation team included Steve Holmes, David Hunt and Tom Lake; their thorough approach to the major coding task resulted in their second sourcing all M_p-LRs available and filing all necessary M_p-LRs for $p < 100,000$.

I thank now everyone who has directly or indirectly contributed to the content of these notes, not least those who developed algorithms and carried out computations on the Mersenne Numbers. The completeness and topicality of the material is due in large part to those who, in private correspondence, were able to restore the colour to the events of the past or even recreate old computations.

I thank Nelson, Shanks and Tuckerman for having the foresight to preserve unpublished M_p-LLT results in private files. I thank Brent, Brillhart, Davis & Holdridge, Keller, Naur, Pollard, Suyama & Wagstaff for factorisations associated with the M_p. They were willing to attack the major peaks which 70-digit numbers represented at the time and also patient and thorough enough to dismiss the small composites which I listed.

This compilation has been significantly assisted by the services provided to assist such research. I was fortunate to be able to call on the help of the British Library, Reading University's Library and Computer Service, the abstracting service of Mathematical Reviews and the production facilities provided by ICL.

CONTENTS

p	Ch	
1		Preface
2		Acknowledgments
3		Contents
4		Introduction
6	1	Abbreviations
7	2	Mersenne Number Status Table
8	3	Prime Mersenne Numbers
10	4	Tables of Factors of Mersenne Numbers
11	5	Original Mersenne Numbers - Positive Results only: M_p Order
14	6	Original Mersenne Numbers - All Results and some errors: M_p Order
28	7	Further Mersenne Numbers - Lucas-Lehmer tests and errors: M_p Order
37	8	Published Work - Errors: Author Order
44	9	Conjectures Resolved
46	10	Conjectures Outstanding
48	11	Theoretical Results
52	12	Computational Details
55	13	Status-quo and Questions
57	14	Authors
58	15	References indexed in "Mathematical Reviews"
60	16	Bibliography
75	17	Keywords

INTRODUCTION

The number system has been studied since the earliest times and this history begins with Pythagoras and Euclid.

One of the earliest interests was the concept of the 'perfect' number - a number equal to the sum of its proper divisors. Here, '1' but not the number itself is regarded as a proper divisor.

Such numbers are rare and the earliest examples, 6 and 28, were invested with mystical significance by numerologists and philosophers.

The major moments in the history of the search for perfect numbers have been provided by Euclid (275BC), Mersenne (1644), Lucas (1876) and by the advent of the electronic computer in the 1950s.

Euclid showed that $2^{n-1}(2^n-1)$ was perfect if 2^n-1 was a prime. Again the early 2^n-1 primes, 3 and 7, were specific objects of numerological interest. Supplementary results have shown that 2^n-1 is prime only if 'n' is a prime 'p', that all even perfect numbers are of Euclid's form, and that the factors of 2^p-1 are of a specific form.

No odd perfect numbers are known. As successive papers add to the conditions which such numbers must satisfy, their existence looks increasingly unlikely. Had '1' not been regarded as a proper divisor, the story might well have been different.

Mersenne took a specific interest in numbers of the form 2^p-1 and incorrectly stated which $p < 258$ led to perfect numbers. He provided no proofs and it might be generous to regard his statement as a conjecture. Unwittingly or not, he contributed no results but threw down a challenge in 1644 which has been taken up ever since. Rouse Ball dubbed the 2^p-1 'Mersenne Numbers' in 1911, thereby creating the first nine Mersenne primes at a stroke. Some thousands of computational hours have been expended on the "Mersenne Numbers" $M_p = 2^p-1$ either to find their prime/composite status or to find their factors.

Lucas provided a convenient primality test for the M_p. D H Lehmer gave a full proof of a refined version of the test in 1930. The Lucas-Lehmer test was manually applied to 19 of the "original" M_p ($p < 258$) though correct computations were not always the result.

The status of Mersenne's statement - five errors - is commonly thought to have been resolved by Uhler's work in 1946. However, this is not so because the contributions of Fauquembergue (M_{101}, M_{137}) and Barker (M_{167}) were found in 1952 to be incorrect by Robinson's SWAC program. The SWAC results put on file for the first time a sufficient set of correct Lucas computations, correcting those errors and filling in for previous unpublished results. Robinson also ratified a number of Lucas computations; all Lucas results have been independently checked for these notes.

Before turning to the electronic computer, we should note the 'pre-history' work done with a variety of computational aids. These included factor stencils, mechanical or electro-mechanical calculators and D H Lehmer's various sieves which were specifically produced to attack residue problems. DHL's first sieve in 1927 relied on bicycle chains and pins attached to the links signalled a result. The second sieve in 1932 substituted holed gear-wheels for bicycle-chains and pins; a sensitive amplifier magnified the minute signal from a photo-electric cell when a ray of light fleetingly shone through the aligned holes in the wheels. An electronic sieve in 1965 continued the line.

The late 1940s provided a quantum jump in computational capability. Lehmer's 700 hour calculation on M_{257} was confirmed in 48 seconds by the SWAC machine in 1952; the phrase "a month a minute" even then understated the ratio between manpower and computer power. Man was liberated from the drudgery of calculation. By the early 1970s, the computer could put away a lifetime's calculations in a second. Today, the latest supercomputers are equivalent to 10^7 SWACs on the M_p benchmark and we are only just beginning to exploit mass parallelism in our computer architectures.

Progress on primality-testing the M_p themselves has been governed by the increasing power of computers though the latest approaches to multiplication have contributed. The Schonhage-Strassen technique reduces the squaring of an n-bit number to $O(n.\log n)$ as compared to the $O(n^2)$ of the schoolboy technique and makes a real contribution when n is of the order of 100000.

Considerable mathematical progress has been achieved on factorisation and general primality-testing since 1970. The complete factorisation of Mersenne's original numbers was achieved in February 1984 and the smallest unfactorised M_p is now M_{449}.

These notes tabulate the results in various ways and provides a full though inevitably incomplete reference to the relevant literature. The 'errors' section shows the difficulties of proof-reading and the desirability of automating the publication process.

The observations also tells a cautionary tale to those organising future computations for as noted above, occasional Lucas results connected with the M_p have later been revealed as incorrect. Computer programs are becoming increasingly important in our lives and their results, which cannot be checked manually, must as far as possible be self-checking or confirmed by independent program.

Mersenne requires no successor today but the 'Cunningham Project' [B17] provides the motivation and focus for current work aiming to advance the state of the art in factorisation and primality-testing. With Slowinski's code active on current and future CRAYs and with the advent of other supercomputers, we may anticipate further discoveries of Mersenne primes.

1 ABBREVIATIONS

ARPCL	-	Adleman-Rumely-Pomerance-Cohen-Lenstra primality test [A4; C31]
cf	-	Continued Fraction factorisation algorithm
cf-ea	-	Continued Fraction with early abort factorisation algorithm
cn	-	A composite number of 'n' decimal digits
DS	-	Difference-of-squares factorisation technique
ecm	-	Elliptic Curve (factorisation) method
E_p	-	the Perfect Number corresponding to prime M_p $(= 2^{p-1} * M_p)$
e_p	-	the number of digits in the decimal representation of E_p
FACT	-	Composite and completely factorised
FFNT	-	Fast Fermat-Number Transform multiplication algorithm
f_i	-	the 'ith' prime factor of the M_p in context
GCD	-	greatest common divisor
h°m's"	-	timing information: 'h' hours, 'm' minutes, 's' seconds
lprpn(p,q)	-	a 'Lucas probable prime' of 'n' decimal digits
lpspn(p,q)	-	a composite lprpn(p,q); a Lucas pseudoprime
LLT	-	Lucas-Lehmer test (M_p prime <===> LR = 0)
LR	-	Lucas Residue (S_{p-1} mod M_p where $S_n = S_{n-1}^2 - 2$, $S_1 = 4$)
M_p	-	the Mersenne number 2^p-1, p being prime
m_p	-	the number of digits in the decimal representation of M_p
mp-qs	-	multiple-polynomial quadratic sieve factorisation method
NFF	-	'no further factor'
NZLR	-	non-zero Lucas Residue
pn	-	a prime number of 'n' decimal digits
Pp	-	Pollard's 'P-1' factorisation technique
PPL-pf	-	Proth-Pocklington-Lehmer prime-factorisation (certificate)
prpn(a)	-	a 'probable prime' N of 'n' decimal digits satisfying: $a^{N-1} = 1 \bmod N$; $(a, N) = 1$
pspn(a)	-	a composite prpn(a), a pseudoprime to base 'a'
qs	-	Quadratic Sieve factorisation algorithm
rho	-	Monte-Carlo factorisation method
sprpn(a)	-	a 'strongly probable prime' N of 'n' decimal digits satisfying: $N-1 = d.2^s$; $a^d = 1 \bmod N$ or $a^{d.2} = -1 \bmod N$ for some r, $0 \leq r < s$
spspn(a)	-	a composite sprpn(a), a strong pseudoprime to base 'a'
TD	-	trial-division factorisation technique
ZLR	-	Zero Lucas residue (<===> 'M_p Prime')
[...]	-	References: an example [M3; c D1 p13 n66] - see [M3], also cited [D1 page 13 note 66]

2 MERSENNE NUMBER STATUS TABLE

The original Mersenne numbers are the 55 $M_p = 2^p-1$ with $p < 258$ and prime which were the subject of Mersenne's 1644 conjecture:

p	Status
2 3 5 7 13 17 19 31 61 89 107 127	12 prime M_p
11 23 29 37 41 43 47 53 59 67 71 73 79 83 97 101 103 109 113 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257	43 composite and completely factorised M_p

See [B17 Edition 2]. For further M_p:

p	Status
521 607 1279 2203 2281 3217 4253 4423 9689 9941 11213 19937 21701 23209 44497 86243 110503 132049 216091	19 prime M_p
263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 457 461 463 487 491 499 503 509 547 577 701 709 881 1049 1063	46 composite and completely factorised M_p
1303 1327 1459 1637 3041 3359 4127 4243 7673	9 composite and probably completely factorised M_p
449 467 479 541 557 563 569 571 587 593 599 601 613 617 619 631 641 643 647 653 659 661 673 677 683 691 719 733 739 743 757 761 769 773 787 797 811 821 827 ...	First 39 partially factorised M_p
523 727 751 809 823 971 983 997 1061 ...	First 9 M_p with no known factor

See [B17 Edition 2 & update 2.2] and [K31] for the 'probably' factorised M_p.

3 PRIME MERSENNE NUMBERS

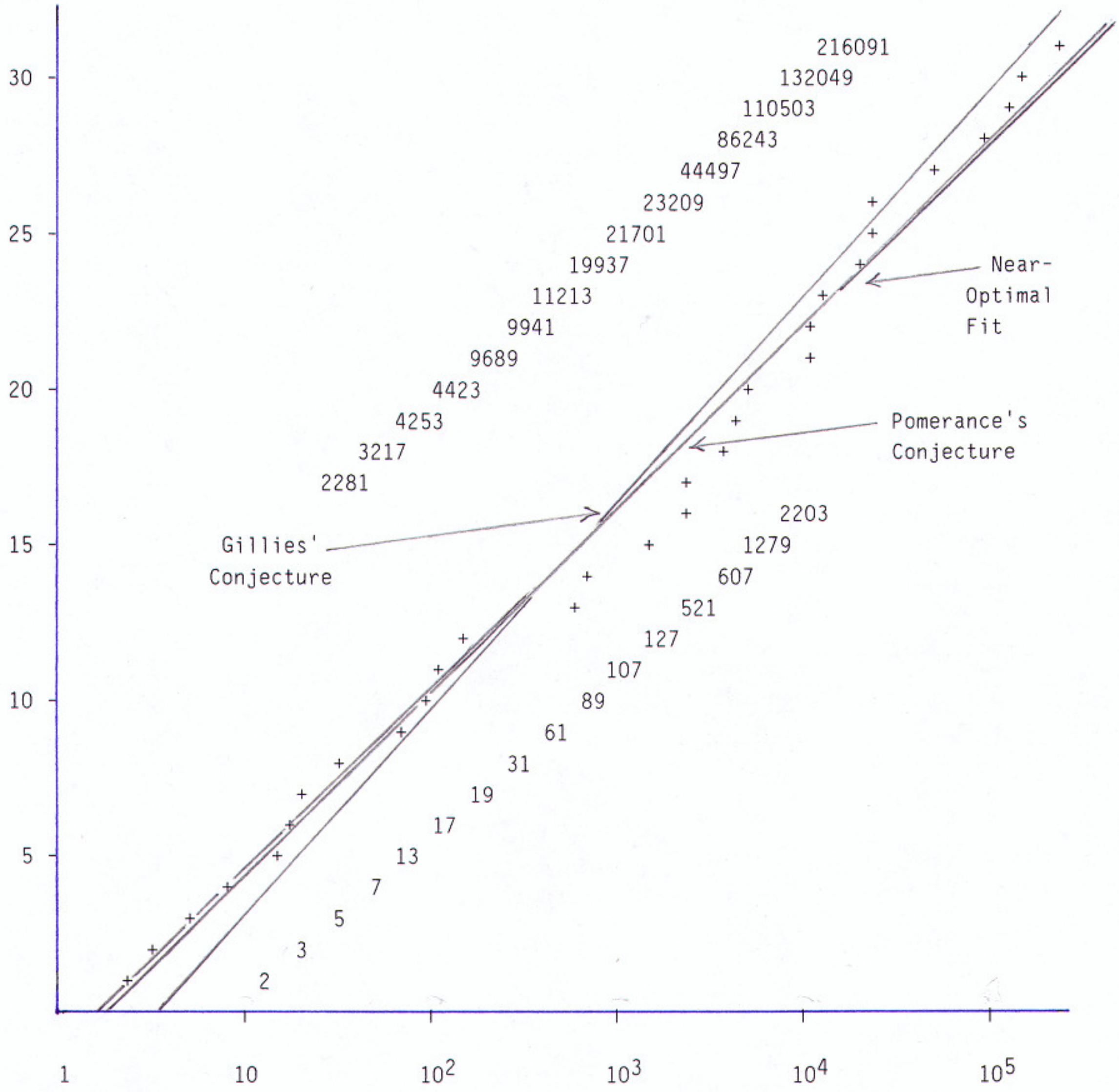
	DATE	p	m_p	e_p	NOTES
1	ca 275 BC	2	1	1	Euclid (275BC) [H3]; Nicomachus (ca 100AD)
2	ca 275 BC	3	1	2	Euclid; Nicomachus [c D1 p3 n2]
3	ca 275 BC ?	5	2	3	Euclid (?); Nicomachus
4	ca 275 BC ?	7	3	4	Euclid (?); Nicomachus
5	1456	13	4	8	Manuscript Codex lat. Monac [C26]
6	1588	17	6	10	Cataldi [C2; c D1 p10 n44]
7	1588	19	6	12	Cataldi [C2; c D1 p10 n44]
8	1772	31	10	19	Euler [E2 p584; E6 p35; c D1 p18 n95]
9	1883	61	19	37	Pervouchine [P13; P14; P16; c D1 p25 n140]
10	6/1911	89	27	54	Powers [P15]; independently, Fauquembergue
11	6/1914	107	33	65	Powers [P2]; independently, Fauquembergue
12	1876	127	39	77	Lucas [L16; L17]; confirmed, Fauquembergue
13	30/ 1/1952	521	157	314	Robinson (SWAC) [L3; R2]
14	30/ 1/1952	607	183	366	Robinson (SWAC) [L3; R2]
15	25/ 6/1952	1279	386	770	Robinson (SWAC) [L4; R2]
16	7/10/1952	2203	664	1327	Robinson (SWAC) [L5; R2]
17	9/10/1952	2281	687	1373	Robinson (SWAC) [L5; R2]
18	8/ 9/1957	3217	969	1937	Riesel (BESK) [R5; R1]
19	3/11/1961	4253	1281	2561	Hurwitz & Selfridge (IBM 7090) [H1; H2]
20	3/11/1961	4423	1332	2663	Hurwitz & Selfridge (IBM 7090) [H1; H2]
21	11/ 5/1963	9689	2917	5834	Gillies (Illiac II) [G1; G5; G7]
22	16/ 5/1963	9941	2993	5985	Gillies (Illiac II) [G1; G5; G7; M9]
23	2/ 6/1963	11213	3376	6751	Gillies (Illiac II) [G1; G7; M9]
24	4/ 3/1971	19937	6002	12003	Tuckerman (IBM 360/91) [T1; T3]
25	30/10/1978	21701	6533	13066	Nickel & Noll (CDC CYBER-174) [N5; N7; S4]
26	9/ 2/1979	23209	6987	13973	Noll (CDC CYBER-174) [N6; N7; S13]
27	8/ 4/1979	44497	13395	26790	Nelson & Slowinski (CRAY-1) [N1; S1; S13]
28	25/ 9/1982	86243	25962	51924	Slowinski (CRAY-1) [N21]
29	29/ 1/1988	110503	33265	66530	Colquitt & Welsh (NEC SX-2/400) [C32]
30	20/ 9/1983	132049	39751	79502	Slowinski (CRAY-XMP) [C33; D4; N25]
31?	6/ 9/1985	216091	65050	130100	Slowinski (CRAY-XMP) [D6]
	(6/ 8/1989	------	65087	------	$391581.2^{216193}-1$ Brown, Noll, Parady, Smith, Smith and Zarantonello (Amdahl 1200E) [D7])

The prime M_p in the 'original Mersenne number' range $p < 258$ were discovered without the aid of electronic computers. Prime M_p beyond that range were discovered with the aid of electronic computers.

An independent computation on the ICL 2900 DAP has confirmed the Lucas residues for all M_p in the range $p < 50024$ where no factor was known. A factor or LR has been calculated on the DAP for all M_p in the range $p < 100000$ [H18] and by Colquitt/Welsh on the NEC SX/2 [C32-C34] for all p in range $100000 < p < 139267$.

Assuming Pomerance's conjecture on the distribution of Mersenne Primes, a computer using FFNT (or 'schoolboy') multiplication will spend twice (or four times) as long discovering the next Mersenne Prime as confirming all previous results. FFNT algorithms been implemented on the ICL DAP, CRAY-XMP, CYBER-205 and NEC SX-2/400.

Slowinski has not filed all the required M_p-f_1/LRs for $139267 < p < 216092$ and there may be further prime M_p in this range.



INCIDENCE OF MERSENNE PRIMES

$$N = a \log_e P + c$$

	a	c
Best Gillies-fit:	2.88539	-3.61278
Best Pomerance-fit:	2.56954	-1.46586
Optimal fit:	2.56560	-1.43906

4 FACTORS OF MERSENNE NUMBERS

This section lists the major tabulations of M_p-factors.

1925 Cunningham & Woodall [C16]

1929 Kraitchik [K12]

1938 Kraitchik [K20]

1947 Lehmer [L6]: 32 factors of M_n, $n < 490$

1952 Ferrier [F4]: table of Factors of M_n, n = 3 (2) 499

1957 Robinson [R3]: some Factorizations of Numbers of the Form $2^n \pm 1$

1958 Riesel [R1]: first factors $f_1 < 10 * 2^{20}$ of M_p: $p < 10{,}000$

1960 Brillhart & Johnson [B2]: some factors q of M_p: $p < 1{,}194$

1961 Karst [K4]: 19 new factors of M_p: $3{,}036 < p < 3{,}434$

1961 Kravitz [K5]: first factors $f_1 < 10{,}485760$ of some M_p: $10{,}000 < p < 15{,}000$

1961 Karst [K2]: some factors q of M_p [NB especially p = 10,009]

1962 Karst [K23]: new divisors: $10{,}006 < p < 10{,}458$ & $5{,}500{,}224 < p < 5{,}501{,}708$

1962 Karst [K24]: synopsis of factors and search ranges

1962 Riesel [R4]: factors $q < 10^8$ of M_p: $p < 10^4$

1963 Brillhart [B3]: some miscellaneous factorizations

1963 Gillies [G1]: $2^{34} < q < 2^{36}$ of M_p: $5{,}000 < p < 17{,}000$

1963 Karst [K27]: factors q = 2kp+1, $k < 10$, of M_p, $p < 15{,}000$

1964 Karst [K6]: miscellaneous

1964 Brillhart [B4]: remaining $q < 2^{34}$ of M_p: $258 < p < 20{,}000$

1965 Kravitz & Madachy [K8]: the factors $q < 2^{25}$ of M_p: $20{,}000 < p < 100{,}000$

1966 Ehrman [E9]: factors $q < 2^{31}$ of M_p: $100{,}000 < p < 300{,}000$

1975 Brillhart, Lehmer & Selfridge [B6]: some factorizations of $2^n \pm 1$

1976 Wagstaff's factor-table [W8]:
  factors $q < 2^{35}$ of M_p: $17{,}000 < p < 50{,}000$
  further $f_1 < 10^{11}$ of M_p: $21{,}000 < p < 50{,}000$

1977 Keller [K30]: factors $q < \max(2^{36}, 10^7 p)$ of M_p, $p < 10^5$

1978 Ehrman's factors of M_p: factors $q < 2^{31}$ for $p < 1{,}000{,}000$ [c N3; N10]

1981 Brent [B23]: factors q of M_p, $p < 1{,}000$

1981 Lake [L45]: first factors $f_1 < 2^{40}$ for $50{,}000 < p < 100{,}000$

1982 Wagstaff [W12]: factors $2^{31} < q < 2^{34}$, $20000 < p < 10^5$ + others

1983 The 'Cunningham Project' [B17]: factors of M_p, $p < 1200$

5 ORIGINAL MERSENNE NUMBERS - POSITIVE RESULTS ONLY: M_p ORDER

Factorisation

This section lists M_p 'status' (prime or completely factorised), the number of known factors, discovering authorities and dates. References, confirmation results, negative results, errors and further details are included in the fuller Section 6.

p	Status	Notes
2	PR	? Pythagoras (500BC ?); ? Euclid (275BC ?); In earliest tables (250BC ?); Nicomachus (100AD)
3	PR	? Euclid (275BC ?); Earliest tables (250BC ?); Nicomachus (100AD)
5	PR	? Euclid (275BC ?); Earliest tables (250BC ?); Nicomachus (100AD)
7	PR	? Euclid (275BC ?); ? Earliest tables (250BC ?); Nicomachus (100AD)
11	FACT	Manuscript Codex lat. Monac. 14908 (1456); f_1 & f_2 - Regius (1536)
13	PR	Manuscript Codex lat. Monac. 14908 (1456)
17	PR	Cataldi (1588)
19	PR	Cataldi (1588)
23	FACT	f_1 - Fermat (1640); f_2 - Euler (1733)
29	FACT	f_1 (?) & f_2 - Euler (1733); f_3 - Euler (1750)
31	PR	Euler (1772)
37	FACT	f_1 - Fermat (1640); f_2 - Landry (1867)
41	FACT	f_1 & f_2 - Plana (1859)
43	FACT	f_1 - Euler (1733); f_2 & f_3 - Landry (1869)
47	FACT	f_1 - Euler (1741); f_2 - Reuschle (1856); f_3 - Landry (1869)
53	FACT	f_1, f_2 & f_3 - Landry (1869)
59	FACT	f_1 & f_2 - Landry (1869)
61	PR	Pervouchine by ZLR (1883)
67	FACT	COMP (?) - Lucas by NZLR (1876); COMP (?) - Fauquembergue (1894); f_1 & f_2 - Cole (1903)
71	FACT	f_1 - Cunningham (1909); f_2 & f_3 - Ramesam (1912)
73	FACT	f_1 - Euler (1733); f_2 & f_3 - Poulet (1923)
79	FACT	f_1 - Reuschle (1856); f_2 & f_3 - Lehmer (1933)
83	FACT	f_1 - Euler (1733); f_2 - Ferrier (1950)
89	PR	Independently by ZLR - Powers (June 1911), Tarry (?) (November 1911) and Fauquembergue (1912)
97	FACT	f_1 - Le Lasseur (1881); f_2 - Ferrier (1952)
101	FACT	COMP - Robinson by NZLR (1952); f_1 & f_2 - Brillhart, Lehmer & Johnson (1967)
103	FACT	COMP (?) - Powers by NZLR (1914); COMP - Robinson by NZLR (1952); f_1 & f_2 - Brillhart (1963)
107	PR	Powers by ZLR (1914) and independently Fauquembergue by ZLR (1914)
109	FACT	COMP (?) - Powers by NZLR (1914); COMP - Robinson by NZLR (1952); f_1 - Robinson (1957); f_2 - Gabard (1958)
113	FACT	f_1 - Reuschle (1856); f_2 & f_3 - Cunningham (1909); f_4 & f_5 - Lehmer (1946)
127	PR	Lucas by ZLR (1876)
131	FACT	f_1 - Euler (1733); f_2 - Brillhart (1966)
137	FACT	COMP - Robinson by NZLR (1952); f_1 & f_2 - Schroepepel (1971)
139	FACT	COMP - Lehmer by NZLR (1926); f_1 & f_2 - Brillhart (1974)
149	FACT	COMP - Lehmer by NZLR (1927); f_1 & f_2 - Schroepepel (1972)
151	FACT	f_1 - Le Lasseur (1881); f_2 - Cunningham (1909); f_3 - Kraitchik (1921); f_4 - Lehmer (1946); f_5 - Gabard (1952)

p	Status	Notes
157	FACT	COMP - Uhler by NZLR (1944); f_1 - Robinson (1957); f_2, f_3 & f_4 - Brillhart (1974)
163	FACT	f_1 - Cunningham (1908); f_2 - Lehmer (1946); f_3 - Brillhart (1960); f_4 & f_5 - Brillhart (1963)
167	FACT	COMP - Uhler by NZLR (1944); f_1 - Lehmer (1946); f_2 - Brillhart (1974)
173	FACT	f_1 - Cunningham (1912); f_2 - Lehmer (1946); f_3 & f_4 - Naur (1979)
179	FACT	f_1 - Euler (1733); f_2 - Reuschle (1856); f_3 - Brillhart (1963)
181	FACT	f_1 - Woodall (1911); f_2 - Lehmer (1946); f_3 - Brillhart (1960); f_4 - Brillhart (1963)
191	FACT	f_1 - Euler (1733); f_2 - Brillhart (1963); f_3, f_4 & f_5 - "Cunningham Project" (1974)
193	FACT	COMP - Uhler by NZLR (1947); f_1 - Brillhart (1960); f_2 & f_3 - Naur (1981)
197	FACT	f_1 - Cunningham (1895); f_2 - Brillhart (1974)
199	FACT	COMP - Uhler by NZLR (1946); f_1 & f_2 - Schroepepel (1976)
211	FACT	f_1 - Le Lasseur (1881); f_2 & f_3 - Davis & Holdridge (1983)
223	FACT	f_1 - Le Lasseur (1881); f_2 - Kraitchik (1921); f_3 & f_4 - Lehmer (1946); f_5 & f_6 - "Cunningham Project" (1981)
227	FACT	COMP - Uhler by NZLR (1947); f_1 & f_2 - Brent (1982)
229	FACT	COMP - Uhler by NZLR (Feb. 1946); f_1 - Lehmer (Oct. 1946); f_2 - Brillhart (1960); f_3 & f_4 - Brent (Aug. 1981)
233	FACT	f_1 - Reuschle (1856); f_2 - Kraitchik (1921); f_3 - Lehmer (1946); f_4 - Brillhart (1974)
239	FACT	f_1 - Euler (1733); f_2 - Reuschle (1856); f_3 - Bickmore (1896); f_4 - Kraitchik (1921); f_5 - Brillhart (1960); f_6 - Brillhart (1974)
241	FACT	COMP - Powers by NZLR (1934); f_1 - Brillhart (1960); f_2 - Brillhart (1974)
251	FACT	f_1 (?) - Euler (1733); f_1 - Lucas (1878); f_2 - Cunningham (1909); f_3, f_4 & f_5 - Davis, Holdridge & Simmons (1984)
257	FACT	COMP (?) - Kraitchik by NZLR (1922); COMP - Lehmer (1927); f_1 - Penk (1979?) [c B16, B17, B19]; f_2 & f_3 - Baillie (1980?) [c B16, B17, B19]

5.2 Lucas-Lehmer Test Calculations

The last octal digits of the LR are listed for the original LLT primality tests on the 'original' M_p; '†' denotes tests with S_1 = 3. This collection compensates for the fact that many of the LRs [G7; H8; N2; R10; T11; T12] have not been published.

Gillies' and Nelson's 1979 results confirmed that Robinson's 1952 results completed a correct set of LRs. Residual calculations in the 1980's second-sourced and sometimes corrected the other original LLT results:

1947 Uhler contributed last of 6 LRs (p = 157, 167, 193, 199, 227, 229)
1952 Robinson corrected 5 LRs (p = 101, 103†, 109, 137, 167†)
  contributed 2 further LRs (p = 103, 199)
  filled in for 2 unpublished LRs (p = 109, 139†)
  confirmed 10 LRs (p = 139†, 149, 157, 167, 193, 199†, 227, 229, 241, 257)
1963 Gillies contributed 1 LR (p = 139)
  confirmed 5 LRs (p = 101, 103, 137, 199, 227)
1979 Nelson confirmed 3 LRs (p = 109, 139, 229)
1981 Thomason ratified 2 LRs (p = 167†, 199†) in decimal & octal
1984 Haworth [H17] confirmed 2 Thomason LRs (p = 67†, 103†)

p	S_1	Date	Residue (oct, mod 2^{60})	Notes
61	4	1883	ZERO	Pervouchine [P13; P14; P16]; [H5; L38]
67	3	1876	UNKNOWN	Lucas [c D1 p22 n115]
		1894	UNKNOWN	Fauquembergue [F8; F9; c D1 p27]
		1981	54316 42002 04344 62606	Thomason [T12]; [H17]
	---	1903	FACTORISED	Cole [C17; c D1 p29]
89	4	1911	ZERO	Powers [C12; P9; P15; c D1 p30]; [F11]
101	4	1913	INCORRECT	Fauquembergue [F12; c D1 p32; R2]
		1952	03353 51067 27402 72066	Robinson [R2; R10; U9]; [G7]; [N2]
103	3	1914	UNKNOWN	Powers [P1]
		1914	INCORRECT	Fauquembergue [F1; R2]
		1981	74422 12107 12525 17576	Thomason [T12]; [H17]
	4	1952	24114 55042 52156 55476	Robinson [R2; R10]; [G7]; [H8; N2]
107	3	1914	ZERO	Powers [P2]; Fauquembergue [F1]
109	4	1914	UNKNOWN	Powers [P1]
		1914	INCORRECT	Fauquembergue [F1; R2]
		1952	42137 07051 44077 17542	Robinson [R2; R10]; [N2]; [H8]
127	3	1876	ZERO	Lucas [L16; L17; c D1 p22]; [F1]
137	4	1920	INCORRECT	Fauquembergue [F10; R2]
		1952	10134 33201 72733 77550	Robinson [R2; R10]; [G7]; [H8; N2]
139	3	1926	26402 01452 65351 23053	Lehmer (unpub.) [L1; c A1]; [R2; R10]; [T12]
	4	1963	72153 37573 37744 53004	Gillies [G7]; [N2]; [H8]
149	4	1927	16542 63652 25676 04577	Lehmer [L2]; [R2; R10]; [G7; H8; N2; T11]
157	4	1944	06164 72124 57400 52105	Uhler [U1; U2; U4]; [R2; R10]; [H8; N2; T11]
167	3	1945	INCORRECT	Barker [B1; R2]
		1952	55023 73422 34113 66527	Robinson [R2; R10]; [T11]
	4	1944	03606 22171 27126 24024	Uhler [U3; U4]; [R2; R10]; [H8; N2; T11]
193	4	1947	03252 67125 36636 06362	Uhler [U5]; [R2; R10]; [G7; H8; N2; T11]
199	3	1946	76417 74230 46161 34351	Uhler [U5; U6]; [R2]; [T11]
	4	1952	12500 24134 55074 67307	Robinson [R2; R10]; [G7]; [H8; N2]
227	4	1947	76675 34333 53115 63716	Uhler [U5; U7]; [R2]; [G7]; [H8; N2; T11]
229	4	1946	43244 27335 00106 53763	Uhler [U5; U8]; [R2]; [N2]; [H8; T11]
241	4	1934	21746 40770 36712 62747	Powers [P3]; [R2; R10]; [G7; H8; N2; T11]
257	4	1922	UNKNOWN	Kraitchik [L2]
		1927	53356 13134 20206 35250	Lehmer [L2; L26]; [R2; R10]; [G7; N2; T11]

6 ORIGINAL MERSENNE NUMBERS - ALL RESULTS AND SOME ERRORS: M_p ORDER

p = 2: 1st MERSENNE PRIME

1) $m_2 = 1$; $e_2 = 1$; $M_2 = 3$; $E_2 = 6$

-500 2) **PRIME (?)**: Pythagoras [c D1 p4 n4] regarded E_2 as 'marriage, health, beauty'

-275 3) **PRIME (?)**: Euclid [H3] presumably knew of E_2

-250 4) **PRIME**: Included in the earliest known tables of primes [D1 p347]: Eratosthenes may have recorded such a table

100 5) Nicomachus [c D1 p3 n2] implied prime (by Euclid Book IX Prop.36)

6) Lucas-Lehmer test not applicable as '2' is an even number

p = 3: 2nd MERSENNE PRIME

1) $m_3 = 1$; $e_3 = 2$; $M_3 = 7$; $E_3 = 28$

-275 2) **PRIME (?)**: Euclid [H3] presumably knew of E_3

-250 3) **PRIME**: Included in the earliest known tables of primes [D1 p347]: Eratosthenes may have recorded such a table

100 4) Nicomachus [c D1 p3 n2] implied prime (by Euclid Book IX Prop.36)

5) Confirmed (!) prime by ZLR [R1; H1; G1; T1; N1]

p = 5: 3rd MERSENNE PRIME

1) $m_5 = 2$; $e_5 = 3$; $M_5 = 31$; $E_5 = 496$

-275 2) **PRIME (?)**: Euclid [H3] presumably knew of E_5

-250 3) **PRIME**: Included in the earliest known tables of primes [D1 p347]: Eratosthenes may have recorded such a table

100 4) Nicomachus [c D1 p3 n2] implied prime (by Euclid Book IX Prop.36)

5) Confirmed (!) prime by ZLR [R1; H1; G1; T1; N1]

p = 7: 4th MERSENNE PRIME

1) $m_7 = 3$; $e_7 = 4$; $M_7 = 127$; $E_7 = 8128$

-250 2) May have been in earliest known prime-tables [D1 p347]

100 3) **PRIME**: Nicomachus [c D1 p3 n2] implied prime (by Euclid Book IX Prop.36)

4) Confirmed (!) prime by ZLR [R1; H1; G1; T1; N1]

p = 11

1456 1) **COMPOSITE**: The authors of Codex lat. Monac. 14908 are thought by Curtze to have known that M_{11} had the factor 23 [C26; c D1 p6 n14]

1509 2) ERROR: Carollus Bovillus [c D1 p7 n20] thought M_n prime for all odd n; an error repeated by others. Not true (e.g. 11, any composite 'n')

1536 3) **COMPOSITE**: Regius [c D1 p7 n26] found complete factorisation: $M_{11} = 23 * 89$

1588 4) Cataldi [C2; c D1 p10 n44] found full factorisation (published 1603)

1638 5) Stanislaus Pudlowski is credited with full factorisation by Broscius [c A1]

1640 6) Fermat [c D1 p12 n59] found full factorisation

1935 7) Archibald [A1] did not note Regius' or Cataldi's work p = 13:   5th MERSENNE PRIME

1) $m_{13} = 4$; $e_{13} = 8$; $M_{13} = 8191$; $E_{13} = 33,550336$
1456 2) **PRIME:** Manuscript Codex lat. Monac. 14908 [C26; c D1 p6 n14] correctly gave E_{13} as 5th Perfect Number, implying that M_{13} is prime.
1536 3) Regius [c D1 p7 n26] also declared E_{13} Perfect
4) Confirmed prime by Cataldi (1588), Pauli (1678), Euler (1733) [c D1 Ch1 ns44, 70 & 83 respectively]
5) Confirmed prime by ZLR [R1; H1; G1; T1; N1]

p = 17:   6th MERSENNE PRIME

1) $m_{17} = 6$; $e_{17} = 10$; $M_{17} = 131071$; $E_{17} = 8589,869056$
1588 2) **PRIME:** Cataldi [C2; c D1 p10 n44] tested with all 72 primes to 359
1750 3) Confirmed prime by Euler [E3 p27; E2 p104; c D1 p18 n89]
4) Confirmed prime by ZLR [R1; H1; G1; T1; N1]

p = 19:   7th MERSENNE PRIME

1) $m_{19} = 6$; $e_{19} = 12$; $M_{19} = 524287$; $E_{19} = 137438,691328$ [T3; T11; U11]
1588 2) **PRIME:** Cataldi [C2; c D1 p10 n44] tested with all 128 primes to 719
1752 3) Confirmed prime by Euler [E3 p27; E2 p104; c D1 p18 ns 89 & 92]
4) Confirmed prime by ZLR [R1; H1; G1; T1; N1; H8]

p = 23

1588 1) ERROR: regarded by Cataldi [C2; c D1 p10 n44] as prime
1640 2) **COMPOSITE:** Fermat [F5 p210; c D1 p12 n56] found $f_1 = 47$
1733 3) Euler [E3 p27; E2 p104; c D1 p18 n89] completed factorisation:
$M_{23} = 47 * 178481$

p = 29

1588 1) ERROR: regarded by Cataldi [C2; c D1 p10 n44] as prime
1644 2) Stated by Mersenne [M3; c D1 p13] to be composite
1733 3) **COMPOSITE:** Euler [E1 p106; E2 p2; c D1 p17 n83]: 1103 is a factor
1750 4) Euler [E3 p27; E2 p104; c D1 p18 n89] completed the full factorisation:
$M_{29} = 233 * 1103 * 2089$
1935 5) Archibald [A1] credited Euler with 233, Dickson [D1] did not

p = 31:   8th MERSENNE PRIME

1) $m_{31} = 10$; $e_{31} = 19$; $M_{31} = 2147,483647$; $E_{31} = 2,305843,008139,952128$ [T3; T11; U11]
1644 2) Stated by Mersenne [M3; c D1 p13] to be prime
1733 3) Conjectured by Euler [E1 p103; E2 p2; c D1 p17 n83] as prime
1751 4) Regarded by de Winsheim [W5; c D1 p18 n90] as prime
1752 5) Euler [E8; c D1 p18 n92]: no factor < 2000
1772 6) **PRIME:** Euler [E6 p35; E2 p584; c D1 p18 n95] tried the 84 eligible primes
7) Confirmed prime by Landry (1859), Seelhoff (?) [c D1 p25 n142] (1887), Lucas (1876), Moret-Blanc (1881)
8) Confirmed prime by ZLR [R1; H1; G1; T1; N1; H8]

p = 37

1588 1) ERROR: regarded by Cataldi [C2; c D1 p10 n44] as prime
1640 2) **COMPOSITE:** Fermat [F5 p199; c D1 p12 n59] found $f_1 = 223$
1867 3) Landry [c D1 p21 n112] claimed full factorisation
1869 4) Landry [L19; c D1 p22 n113] published full factorisation:
$M_{37} = 223 * 616,318177$

p = 41

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1678 2) ERROR: Pauli [P11; c D1 p15 n70] gave 83 as a factor
1733 3) Euler [E1 p106; E2 p2; c D1 p17 n83] wrongly conjectured prime
1859 4) **COMPOSITE:** Plana [P12; c D1 p21 n110] gave full factorisation:
$M_{41} = 13367 * 164,511353$
1888 5) ERROR: Christie [C27; C28; c D1 p27 n155] thought M_{41} prime

p = 43

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1733 2) **COMPOSITE:** Euler [E1 p106; E2 p2; c D1 p17 n83]: $f_1 = 431$
1867 3) Landry [L20; c D1 p21 n112] claimed full factorisation
1869 4) Landry [L19; c D1 p22 n113] published full factorisation:
$M_{43} = 431 * 9719 * 2,099863$

p = 47

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1733 2) Euler [E1 p106; E2 p2; c D1 p17 n83] wrongly conjectured prime
1741 3) **COMPOSITE:** Euler [K18; c D1 p19 n93] found $f_1 = 2351$
1751 4) De Winsheim [W5; c D1 p18 n90] independently (?) found $f_1 = 2351$
1856 5) Reuschle [R8; c D1 p21 n108] found $f_2 = 4513$ (note $f_3 < f_2 * f_2$)
1867 6) Landry [L20; c D1 p21 n112] claimed full factorisation
1869 7) Landry [L19; c D1 p22 n113] published full factorisation:
$M_{47} = 2351 * 4513 * 13,264529$
1888 8) ERROR: Christie [C27; C28; c D1 p27 n155] thought M_{47} prime

p = 53

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1859 2) ERROR: Plana [P12; c D1 p21 n110] found no factor < 50033
1867 3) Landry [L20; c D1 p21 n112] claimed full factorisation
1869 4) **COMPOSITE:** Landry [L19; c D1 p22 n113] published full factorisation:
$M_{53} = 6361 * 69431 * 20,394401$

p = 59

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1867 2) Landry [L20; c D1 p21 n112] claimed full factorisation
1869 3) **COMPOSITE:** Landry [L19; c D1 p22 n113] published full factorisation:
$M_{59} = 179951 * 3,203431,780337$

p = 61: **9th MERSENNE PRIME**

1) m_{61} = 19; e_{61} = 37; M_{61} = 2,305843,009213,693951;
E_{61} = 2,658455,991569,831744,654692,615953,842176 [H3; T3; T11; U11]
1644 2) ERROR: stated by Mersenne [M3; c D1 p13] to be composite
1869 3) Landry [L14; c D1 p22 n113] conjectured prime
1881 4) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1883 5) **PRIME:** Pervouchine [P13; P14; P16; c D1 p25 n140] computed a ZLR
1886 6) ERROR: Seelhoff [S12; c D1 p25 n141] wrongly stated M_{61} prime having only found it pseudoprime (base 3)
1887 7) Hudelot [H5; L38; c D1 p25 n144] confirmed prime by ZLR (54 hours work)
1903 8) Cole [C17; c D1 p29 n173] criticised Seelhoff's 'proof' of primality
1927 9) Lehmer [L11] indicated error in Seelhoff's 'proof' of primality
10) Confirmed prime by ZLR [R1; H1; G1; T1; N1; H8]

p = 67

1644 1) ERROR: stated by Mersenne [M3; c D1 p13] to be prime
1876 2) **COMPOSITE (?):** Lucas [c D1 p22 n115] computed NZLR (correctly?)
1881 3) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1894 4) **COMPOSITE (?):** Fauquembergue [F8; F9; c D1 p27 n160] - NZLR (?)
1895 5) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1903 6) **COMPOSITE:** Cole [C17; c D1 p29 n173] found the full factorisation:
M_{67} = 193,707721 * 761838,257287
1935 7) Archibald [A1] did not cite Lucas or Fauquembergue (2 and 4 above)
1981 8) Thomason [T12] computed NZLR as 67 54316 42002 04344 62606 (S_1 = 3) [H17]

p = 71

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) Cunningham [C8] found no factor < 200,000
1909 5) **COMPOSITE:** Cunningham [C10; c D1 p30 n181] found f_1 = 228479
1912 6) Ramesam [R9; B8; c D1 p31 n191] completed the full factorisation:
M_{71} = 228479 * 48,544121 * 212,885833

p = 73

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1733 2) **COMPOSITE:** Euler [E1 p106; E2 p2; c D1 p17 n83] found f_1 = 439
1923 3) Poulet [P7; c A1 n12] completed the factorisation:
M_{73} = 439 * 2,298041 * 9,361973,132609

p = 79

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1856 2) **COMPOSITE:** Reuschle [R8; c D1 p21 n108] found f_1 = 2687
1933 3) D H Lehmer [L7; c A1 n13] found f_2 & f_3 to complete the factorisation:
M_{79} = 2687 * 202,029703 * 1,113491,139767

p = 83

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1733 2) **COMPOSITE:** Euler [E1 p105; E2 p2; c D1 p17 n83] found f_1 = 167 (theorem)
1946 3) D H Lehmer [L6] found no further factor < 4,538800
1950 4) Ferrier [F3] used method [F2] to complete the full factorisation:
M_{83} = 167 * 57912,614113,275649,087721

p = 89: **10th MERSENNE PRIME**

1) m_{89} = 27; e_{89} = 54; M_{89} = 618,970019,642690,137449,562111;
E_{89} = 191561,942608,236107,294793,378084,303638,130997,321548,169216
[T11; U11] - [T3] is incorrect
1644 2) ERROR: stated by Mersenne [M3; c D1 p13] to be composite
1876 3) ERROR: Lucas [L13 p376; c D1 p22 n115] computed a NZLR
1881 4) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 5) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 6) Cunningham [C8] found no factor < 200,000
1911 7) **PRIME:** Powers [C12; P9; P15; c D1 p30 n185] computed ZLR (June)
1911 8) **PRIME (?):** Tarry [T4; c C12 & D1 p30 n186] completed (?) calculation
1912 9) **PRIME:** Fauquembergue [F11; c D1 p30 n187] found ZLR independently (base 2)
10) Confirmed prime by ZLR [R1; H1; G1; T1; N1; H8]

p = 97

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) **COMPOSITE:** Le Lasseur [c D1 p24 n131] found f_1 = 11447
1935 3) Archibald [A1] recorded that only f_1 had been found
1946 4) D H Lehmer [L6] found no further factor < 4,538800
1952 5) Ferrier [F4; K7 p13; K17 p48] found f_2 to complete the factorisation:
M_{97} = 11447 * 13,842607,235828,485645,766393

p = 101

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) Cunningham [C8] found no factor < 200,000
1911 5) Cunningham [C4; W1] found no factor < 500,000
1912 6) Cunningham [C1] found no factor < 800,000 (working with Gerardin)
1912 7) Gerardin [G6; c D1 p31 n192b] found no factor < 1,000,000
1913 8) ERROR: Fauquembergue [F12; c D1 p32 n192c] computed incorrect NZLR
1946 9) D H Lehmer [L6] found no factor < 4,538800
1952 10) **COMPOSITE:** Robinson [R2; R10; U9] computed NZLR - not Fauquembergue's
1957 11) Robinson [R3] on IBM701 found no factor < 2^{30}
1960 12) Brillhart [B2] on IBM701 found no factor < 2^{31}
1963 13) Brillhart [B4] found no factor < 2^{35}
1963 14) Gillies [G1; G7] confirmed (last 5 octal digits of) Robinson's NZLR
1967 15) Brillhart, Lehmer & Johnson [B5; c K26 p354, B19] found full factorisation:
M_{101} = 7,432339,208719 * 341117,531003,194129

p = 103

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) Cunningham [C8] found no factor < 200,000
1911 5) Cunningham [C4; W1] found no factor < 500,000
1912 6) Cunningham [C1] found no factor < 800,000 (working with Gerardin)
1912 7) Gerardin [G6; c D1 p31 n192b] found no factor < 1,000000
1914 8) ERROR: Fauquembergue [F1] computed incorrect NZLR [R2] (S_1 = 3)
1914 9) **COMPOSITE (?)**: Powers [P1] computed unpublished NZLR (correctly?) (S_1 = 3)
1946 10) D H Lehmer [L6] found no factor < 4,538800
1952 11) **COMPOSITE**: Robinson [R2; R10; U9] computed NZLRs (S_1 = 3 & 4)
1957 12) Robinson [R3] on IBM701 found no factor < 2^{30}
1960 13) Brillhart [B2] found no factor < 2^{31}
1963 14) Brillhart [B3] found complete factorisation:
M_{103} = 2550,183799 * 3976,656429,941438,590393
1963 15) Gillies [G1, G7] confirmed (last 5 octal digits of) Robinson's NZLR (S_1 = 4)
1981 16) Thomason [T12] computed NZLR .. 74422 12107 12525 17576 (S_1 = 3) [H17]

p = 107: 11th MERSENNE PRIME

1) m_{107} = 33; e_{107} = 65;
M_{107} = 162,259276,829213,363391,578010,288127 [R6]
E_{107} = 13164,036458,569648,337239,753460,458722,910223,472318, --->
---> 386943,117783,728128 [T11] - [T3; U11] are incorrect
1644 2) ERROR: stated by Mersenne [M3; c D1 p13] to be composite
1881 3) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 4) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 5) Cunningham [C8] found no factor < 200,000
1911 6) Cunningham [C4; W1] found no factor < 500,000
1912 7) Cunningham [C1] found no factor < 800,000 (working with Gerardin)
1912 8) Gerardin [G6; c D1 p31 n192b] found no factor < 1,000,000
1914 9) **PRIME**: Powers [P2; P6; P10] computed ZLR (S_1 = 3) (11th June)
1914 10) **PRIME**: Fauquembergue [F1; c D1 p32 n200] independently computed ZLR (June)
11) Confirmed prime by ZLR [R1; H1; G1; T1; N1; H8]

p = 109

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) Cunningham [C8] found no factor < 200,000
1911 5) Cunningham [C4; W1] found no factor < 500,000
1912 6) Cunningham [C1] found no factor < 800,000 (working with Gerardin)
1912 7) Gerardin [G6; c D1 p31 n192b] found no factor < 1,000,000
1914 8) ERROR: Fauquembergue [F1] computed incorrect NZLR (cf notes 11, 17)
1914 9) **COMPOSITE (?)**: Powers [P1] computed (unpublished) NZLR (correctly?)
1946 10) D H Lehmer [L6] found no factor < 4,538800
1952 11) **COMPOSITE**: Robinson [R2; R10; U9] computed NZLR - not Fauquembergue's
1957 12) Robinson [R3] found one factor < 2^{30}: f_1 = 745,988807
1958 13) Gabard [G2; c B5] found the unresolved part prime:
M_{109} = 745,988807 * 870035,986098,720987,332873
1960 14) Brillhart [B2] not knowing of [G2] found no f_2 < 2^{31}
1963 15) Brillhart [B4] not knowing of [G2] found no f_2 < 2^{35}
1966 16) Brillhart [B5] confirmed Gabard's factorisation
1979 17) Nelson [N1; N2] confirmed (last 24 octal digits of) Robinson's NZLR

p = 113

1644 1) Stated by Mersenne [M3; c D1] to be composite
1856 2) **COMPOSITE**: Reuschle [R8; c D1 p21 n108] found $f_1 = 3391$
1909 3) Cunningham [W1; c D1 p31 n192a] noted $f_2 = 23279$ and $f_3 = 65993$
1935 4) Archibald [A1 ns 7, 10] cited Reuschle and Cunningham for f_1, f_2 and f_3
1946 5) D H Lehmer [L6] completed the full factorisation:
M_{113} = 3391 * 23279 * 65993 * 1,868569 * 1066,818132,868207

p = 127: 12th MERSENNE PRIME

1) $m_{127} = 39$; $e_{127} = 77$;
M_{127} = 170,141183,460469,231731,687303,715884,105727 [O1 p73; B11]
E_{127} = 14474,011154,664524,427946,373126,085988,481573,677491, --->
---> 474835,889066,354349,131199,152128
[T3; T11] - [U11] is incorrect
1644 2) Stated by Mersenne [M3; c D1 p13] to be prime
1876 3) **PRIME**: Lucas [L16; L17; c D1 p22 n116, A1 n17] computed ZLR ($S_1 = 3$)
1881 4) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 5) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1914 6) Fauquembergue [F1; c D1 p32 n200] confirmed prime by ZLR ($S_1 = 3$)
7) Confirmed prime by ZLR [R1; H1; G1; T1; N1; H8]

p = 131

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1733 2) **COMPOSITE**: Euler [E1 p105; E2 p2; c D1 p17 n83] found $f_1 = 263$ by theorem
1946 3) D H Lehmer [L6] found no further factor < 4,538800
1957 4) Robinson [R3] found no further factor < 2^{30}
1960 5) Brillhart [B2] found no further factor < 2^{31}
1963 6) Brillhart [B4] found no further factor < 2^{35}
1966 7) Brillhart [B5] found f_2 prime to complete the factorisation:
M_{131} = 263 * 10,350794,431055,162386,718619,237468,234569

p = 137

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) Cunningham [C8] found no factor < 200,000
1911 5) Cunningham [C4; W1] found no factor < 500,000
1912 6) Cunningham [C1] found no factor < 800,000 (working with Gerardin)
1912 7) Gerardin [G6; c D1 p31 n192b] found no factor < 1,000,000
1920 8) ERROR: Fauquembergue [F10] computed incorrect NZLR (cf ns 10, 14)
1946 9) D H Lehmer [L6] found no factor < 4,538800
1952 10) **COMPOSITE**: Robinson [R2; R10; U9] computed NZLR - not Fauquembergue's
1957 11) Robinson [R3] found no factor < 2^{30}
1960 12) Brillhart [B2] found no factor < 2^{31}
1963 13) Brillhart [B4] found no factor < 2^{35}
1963 14) Gillies [G1; G7] confirmed (last 5 octal digits of) Robinson's NZLR
1971 15) Schroepepel [B7 p13; c B6 p645; B19] found full factorisation (cf):
M_{137} = 32,032215,596496,435569 * 5439,042183,600204,290159

p = 139

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) Cunningham [C8] found no factor < 200,000
1911 5) Cunningham [C4; W1] found no factor < 500,000
1912 6) Cunningham [C1] found no factor < 800,000 (working with Gerardin)
1912 7) Gerardin [G6; c D1 p31 n192b] found no factor < 1,000,000
1926 8) **COMPOSITE:** D H Lehmer [L1; c A1 n13] computed (unpublished) NZLR (S_1 = 3)
1946 9) D H Lehmer [L6] found no factor < 4,538800
1953 10) Robinson [R2; R10] on SWAC confirmed Lehmer's NZLR (S_1 = 3)
1957 11) Robinson [R3] found no factor < 2^{30}
1960 12) Brillhart [B2] found no factor < 2^{31}
1963 13) Brillhart [B4] found no factor < 2^{35}
1963 14) Gillies [G1; G7] computed NZLR (S_1 = 4)
1972 15) Brillhart [B6; S28] found full factorisation (cf):
M_{139} = 5,625767,248687 * 123876,132205,208335,762278,423601
1979 16) Nelson [N2] confirmed Gillies' NZLR
1981 17) Thomason [T12] confirmed Robinson's NZLR (S_1 = 3)

p = 149

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) Cunningham [C8] found no factor < 200,000
1911 5) Cunningham [C4; W1] found no factor < 500,000
1912 6) Cunningham [C1] found no factor < 800,000 (working with Gerardin)
1912 7) Gerardin [G6; c D1 p31 n192b] found no factor < 1,000,000
1927 8) **COMPOSITE:** D H Lehmer [L2; L27; c A1 n13] computed correct NZLR [R2; T11]
1946 9) D H Lehmer [L6] found no factor < 4,538800
1952 10) Robinson [R2; R10] confirmed Lehmer's NZLR on SWAC
1957 11) Robinson [R3] found no factor < 2^{30}
1960 12) Brillhart [B2] found no factor < 2^{31}
1963 13) Brillhart [B4] found no factor < 2^{35}
1972 14) Schroepepel [c B6 p645, B16, B17, B19] found full factorisation (cf):
M_{149} = 86,656268,566282,183151 * 8,235109,336690,846723,986161

p = 151

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) **COMPOSITE:** Le Lasseur [L18; c D1 p24 n131] found f_1 = 18121
1909 3) Cunningham [W1; c D1 p31 n192a] found f_2 = 55871
1921 4) Kraitchik [K3; K16; c A1 n18] found f_3 = 165799
1946 5) D H Lehmer [L6] found f_4 = 2,332951 and no other factor < 4,538800
1952 6) Gabard [G12] found the unresolved part prime:
M_{151} = 18121 * 55871 * 165799 * 2,332951 * 7,289088,383388,253664,437433

p = 157

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) Cunningham [C8] found no factor < 200,000
1911 5) Cunningham [C4; W1] found no factor < 500,000
1912 6) Cunningham [C1] found no factor < 800,000 (working with Gerardin)
1912 7) Gerardin [G6; c D1 p31 n192b] found no factor < 1,000,000
1944 8) **COMPOSITE:** Uhler [U1; U2; c A3] computed correct NZLR [R2; R10; T11]
1945 9) Barker [U4] confirmed Uhler's NZLR
1946 10) D H Lehmer [L6] found no factor < 4,538800
1952 11) Robinson [R2; R10] confirmed Uhler's NZLR on SWAC
1957 12) Robinson [R3] found f_1 = 852,133201 below search-limit 2^{30}
1960 13) Brillhart [B2] found no further factor < 2^{31}
1963 14) Brillhart [B4] found no further factor < 2^{35}
1974 15) Brillhart [B6] found f_2, f_3 and f_4 to complete the full factorisation:
M_{157} = 852,133201 * 60726,444167 * 1,654058,017289 *
2134,387368,610417

p = 163

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) **COMPOSITE:** Cunningham [C8; C9; c D1 p30 n180] found f_1 = 150287
1946 5) D H Lehmer [L6] found f_2 = 704161 and no other factor < 4,538800
1960 6) Brillhart [B2] found f_3 = 110,211473 below search-limit 2^{31}
1963 7) Brillhart [B3] found f_4 and f_5 to complete the factorisation:
M_{163} = 150287 * 704161 * 110,211473 * 27669,118297 *
36,230454,570129,675721

p = 167

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) Cunningham [C8] found no factor < 200,000
1911 5) Cunningham [C4; W1] found no factor < 500,000
1912 6) Cunningham [C1] found no factor < 800,000 (working with Gerardin)
1912 7) Gerardin [G6; c D1 p31 n192b] found no factor < 1,000,000
1944 8) **COMPOSITE:** Uhler [U3; U4; c A3] computed correct NZLR [R2; T11] (S_1 = 4)
1945 9) ERROR: Barker [B1] computed incorrect NZLR [R2; T11] (S_1 = 3)
1946 10) D H Lehmer [L6] found f_1 = 2,349023 and no further factor < 4,538800
1952 11) Robinson [R2; R10] computed NZLRs (S_1 = 3 & 4) confirming Uhler's NZLR
1960 12) Brillhart [B2] confirmed f_1 and found no further factor < 2^{31}
1963 13) Brillhart [B4] found no further factor < 2^{35}
1974 14) Brillhart [B6 p645] found f_2 prime to complete the factorisation:
M_{167} = 2,349023 *
79,638304,766856,507377,778616,296087,448490,695649
1981 15) Thomason [T11] confirmed Robinson's NZLR (S_1 = 3)

p = 173

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) Cunningham [C8] found no factor < 200,000
1911 5) Cunningham [C4; W1] found no factor < 500,000
1912 6) **COMPOSITE:** Cunningham [C1; c D1 p31 n190]: f_1 = 730753 (with Gerardin)
1946 7) D H Lehmer [L6] found f_2 = 1,505447 and no further factor < 4,538800
1960 8) Brillhart [B2] confirmed f_1 & f_2 and found no further factor < 2^{31}
1963 9) Brillhart [B4] found no further factor < 2^{35}
1974 10) Brillhart [B6] found the unresolved part composite
1979 11) Naur [N20] found f_3 (Pp) & f_4 prime to complete the factorisation:
M_{173} = 730753 * 1,505447 * 70084,436712,553223 *
155285,743288,572277,679887

p = 179

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1733 2) **COMPOSITE:** Euler [E1 p105; E2 p2; c D1 p17 n83] found f_1 = 359 (theorem)
1856 3) Reuschle [R8; c D1 p21 n108] found f_2 = 1433
1946 4) D H Lehmer [L6] found no further factor < 4,538800
1960 5) Brillhart [B2] confirmed f_1 & f_2 and found no further factor < 2^{31}
1963 6) Brillhart [B3] found f_3 prime to complete the factorisation:
M_{179} = 359 * 1433 *
1,489459,109360,039866,456940,197095,433721,664951,999121

p = 181

1644 1) Stated by Mersene [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) ERROR: Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) ERROR: Cunningham [C8] found no factor < 200,000
1911 5) **COMPOSITE:** Woodall [C11; W1; c D1 p30 n184] found f_1 = 43441
1946 6) D H Lehmer [L6] found f_2 = 1,164193 and no further factor < 4,538800
1960 7) Brillhart [B2] found f_3 = 7,648337 and no further factor < 2^{31}
1963 8) Brillhart [B3] found f_4 prime to complete the factorisation:
M_{181} = 43441 * 1,164193 * 7,648337 *
7,923871,097285,295625,344647,665764,672671

p = 191

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1733 2) **COMPOSITE:** Euler [E1 p105; E2 p2; c D1 p17 n83] found f_1 = 383 (theorem)
1946 3) D H Lehmer [L6] found no further factor < 4,538800
1960 4) Brillhart [B2] confirmed f_1 and found no further factor < 2^{31}
1963 5) Brillhart [B3] found f_2 = 7068,569257 (TD)
1963 6) Brillhart [B4] found no further factor < 2^{35}
1974 7) Brillhart [B6] found the unresolved part composite
1974 8) "Cunningham Project" [c B16; B17; B19; R12] found f_4 = 332,584516,519201 (Pp)
1974 9) "Cunningham Project" [c B16; B17; B19; R12] completed the factorisation (cf); note the four different factorisation methods used on M_{191}:
M_{191} = 383 * 7068,569257 * 39940,132241 * 332,584516,519201 *
87,274497,124602,996457

p = 193

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) Cunningham [C8] found no factor < 200,000
1911 5) Cunningham [C4; W1] found no factor < 500,000
1912 6) Cunningham [C1] found no factor < 800,000 (working with Gerardin)
1912 7) Gerardin [G6; c D1 p31 n192b] found no factor < 1,000,000
1946 8) D H Lehmer [L6] found no factor < 4,538800
1947 9) **COMPOSITE**: Uhler [U5; c A3] computed a NZLR
1952 10) Robinson [R2; R10; T11] on SWAC confirmed Uhler's NZLR
1960 11) Brillhart [B2] found f_1 = 13,821503 only below search-limit 2^{31}
1963 12) Brillhart [B4] found no further factor < 2^{35}
1963 13) Gillies [G1; G7] confirmed (last 5 octal digits of) Robinson's NZLR
1974 14) Brillhart [B6] found the the unresolved part composite
1981 15) Naur [N18; N19] found primes f_2 (cf) & f_3 to complete the factorisation:
M_{193} = 13,821503 * 61654,440233,248340,616559 *
14732,265321,145317,331353,282383

p = 197

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) ERROR: Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) **COMPOSITE**: Cunningham [C3; C6; c D1 p28 n164] found f_1 = 7487
1946 4) D H Lehmer [L6] found no further factor < 4,538800
1960 5) Brillhart [B2] confirmed f_1 and found no further factor < 2^{31}
1963 6) Brillhart [B4] found no further factor < 2^{35}
1974 7) Brillhart [B6] found f_2 prime to complete the factorisation:
M_{197} = 7487 *
26,828803,997912,886929,710867,041891,989490,486893,845712,448833
[S18; T10]

p = 199

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) Cunningham [C8] found no factor < 200,000
1911 5) Cunningham [C4; W1] found no factor < 500,000
1912 6) Cunningham [C1] found no factor < 800,000 (working with Gerardin)
1912 7) Gerardin [G6; c D1 p31 n192b] found no factor < 1,000,000
1946 8) **COMPOSITE**: Uhler [U5; U6] computed correct NZLR [R2; T11] (S_1 = 3)
1946 9) D H Lehmer [L6] found no factor < 4,538800
1952 10) Robinson [R2; R10] computed NZLRs (S_1 = 3 & 4) confirming Uhler's NZLR
1960 11) Brillhart [B2] found no factor < 2^{31}
1963 12) Brillhart [B4] found no factor < 2^{35}
1963 13) Gillies [G7] confirmed Robinson's NZLR (S_1 = 4)
1976 14) Schroepepel [c B16; B17; B19; c R12] found the factorisation (rho):
M_{199} = 164504,919713 * 4,884164,093883,941177,660049,098586,324302, --->
---> 977543,600799 [S18; T10]
1981 15) Thomason [T11] confirmed Uhler's NZLR (S_1 = 3)

p = 211

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) **COMPOSITE:** Le Lasseur [L18; c D1 p24 n131] found f_1 = 15193
1946 3) D H Lehmer [L6] found no further factor < 4,538800
1960 4) Brillhart [B2] confirmed f_1 and found no further factor < 2^{31}
1963 5) Brillhart [B4] found no further factor < 2^{35}
1974 6) Brillhart [B6] found the unresolved part composite, c60
1983 7) Davis & Holdridge found f_2 (qs) & f_3 to complete the factorisation:
M_{211} = 15193 * 60,272956,433838,849161 *
3593,875704,495823,757388,199894,268773,153439

p = 223

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) **COMPOSITE:** Le Lasseur [L18; c D1 p24 n131] found f_1 = 18287
1921 3) Kraitchik [K3 p24; K16; c A1 n18] found f_2 = 196687
1946 4) D H Lehmer [L6] added just f_3 = 1,466449 and f_4 = 2,916841 below 4,538800
1960 5) Brillhart [B2] confirmed f_1 to f_4 and found no further factor < 2^{31}
1963 6) Brillhart [B4] found no further factor < 2^{35}
1974 7) Brillhart [B6] found the unresolved part composite
1981 8) "Cunningham Project" [B22] completed the factorisation (cf):
M_{223} = 18287 * 196687 * 1,466449 * 2,916841 *
1469,495262,398780,123809 * 596242,599987,116128,415063

p = 227

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) Cunningham [C8] found no factor < 200,000
1911 5) Cunningham [C4; W1] found no factor < 500,000
1912 6) Cunningham [C1] found no factor < 800,000 (working with Gerardin)
1912 7) Gerardin [G6; c D1 p31 n192b] found no factor < 1,000,000
1946 8) D H Lehmer [L6] found no factor < 4,538800
1947 9) **COMPOSITE:** Uhler [U5; U7; c A3] computed correct NZLR [R2; T11]
1952 10) Robinson [R2] on SWAC confirmed Uhler's NZLR
1960 11) Brillhart [B2] found no factor < 2^{31}
1963 12) Brillhart [B4] found no factor < 2^{35}
1982 13) Brent [B30] found primes f_1 (rho) & f_2 to complete factorisation:
M_{227} = 26986,333437,777017 *
7992,177738,205979,626491,506950,867720,953545,660121,688631

p = 229

1644	1)	Stated by Mersenne [M3; c D1 p13] to be composite
1881	2)	Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895	3)	Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908	4)	Cunningham [C8] found no factor < 200,000
1911	5)	Cunningham [C4; W1] found no factor < 500,000
1912	6)	Cunningham [C1] found no factor < 800,000 (working with Gerardin)
1912	7)	Gerardin [G6; c D1 p31 n192b] found no factor < 1,000,000
1946	8)	**COMPOSITE:** Uhler [U5; U8; c A3] computed correct NZLR [R2; T11] (February)
1946	9)	D H Lehmer [L6] found f_1 = 1,504073 and no other factor < 4,538800 (Oct.)
1952	10)	Robinson [R2] on SWAC confirmed Uhler's NZLR
1960	11)	Brillhart [B2] confirmed f_1, added f_2 = 20,492753 and found NFF < 2^{31}
1963	12)	Brillhart [B4] found no further factor < 2^{35}
1974	13)	Brillhart [B6] found the unresolved part composite
1981	14)	Brent [B24; B27; B28] found f_3 (rho) & f_4 to complete the factorisation:

M_{229} = 1,504073 * 20,492753 * 59833,457464,970183 *
467,795120,187583,723534,280000,348743,236593

p = 233

1644	1)	Stated by Mersenne [c D1 p13] to be composite
1856	2)	**COMPOSITE:** Reuschle [R8; c D1 p21 n108] found f_1 = 1399
1921	3)	Kraitchik [K3 p24; K16; c A1 n18] found f_2 = 135607
1946	4)	D H Lehmer [L6] found f_3 = 622577 and no further factor < 4,538800
1960	5)	Brillhart [B2] confirmed f_1, f_2 and f_3 above and found NFF < 2^{31}
1963	6)	Brillhart [B4] found no further factor < 2^{35}
1974	7)	Brillhart [B6; B16] found f_4 prime by Corollary 11 [B6]:

M_{233} = 1399 * 135607 * 622577 *
116,868129,879077,600270,344856,324766,260085,066532,853492,178431
[S18; T10]

p = 239

1644	1)	Stated by Mersenne [M3; c D1 p13] to be composite
1733	2)	**COMPOSITE:** Euler [E1; E2 p2; c D1 p17 n83] found f_1 = 479 by observation
1856	3)	Reuschle [R8; c D1 p21 n108] found f_2 = 1913
1896	4)	Bickmore [B12; c D1 p28 n166] confirmed f_2 and added f_3 = 5737
1921	5)	Kraitchik [K3 p24; K16; c A1 n18] found f_4 = 176383
1946	6)	D H Lehmer [L6] found no further factor < 4,538800
1960	7)	Brillhart [B2] confirmed f_1 - f_4; added f_5 = 134,000609; found NFF < 2^{31}
1963	8)	Brillhart [B4] found no further factor < 2^{35}
1974	9)	Brillhart [B6] found f_6 prime to complete the factorisation:

M_{239} = 479 * 1913 * 5737 * 176383 * 134,000609 *
7,110008,717824,458123,105014,279253,754096,863768,062879
[S18; T10]

p = 241

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1908 4) Cunningham [C8] found no factor < 200,000
1911 5) Cunningham [C4; W1] found no factor < 500,000
1912 6) Cunningham [C1] found no factor < 800,000 (working with Gerardin)
1912 7) Gerardin [G6; c D1 p31 n192b] found no factor < 1,000,000
1934 8) **COMPOSITE:** Powers [P3] computed correct NZLR [R2; T11]
1946 9) D H Lehmer [L6] found no factor < 4,538800
1952 10) Robinson [R2; R10] on SWAC confirmed Powers' NZLR
1960 11) Brillhart [B2] found f_1 = 22,000409 and no further factor < 2^{31}
1963 12) Brillhart [B4] found no further factor < 2^{35}
1974 13) Brillhart [B6] found f_2 prime to complete the factorisation:
M_{241} = 22,000409 * 160619,474372,352289,412737,508720,216839, --->
---> 225805,656328,990879,953332,340439

p = 251

1644 1) Stated by Mersenne [M3; c D1 p13] to be composite
1733 2) An observation of Euler gives f_1 = 503; did Euler state this explicitly?
1878 3) **COMPOSITE:** Lucas [L14 p236; c D1 p23 n123] found f_1 = 503
1909 4) Cunningham [W1; c D1 p31 n192a, A1 n10] found f_2 = 54217
1946 5) D H Lehmer [L6] found no further factor < 4,538800
1960 6) Brillhart [B2] confirmed f_1 & f_2 and found no further factor < 2^{31}
1963 7) Brillhart [B4] found no further factor < 2^{35}
1974 8) Brillhart [B6] found the unresolved part composite, c69
1984 9) Davis et al found f_3, f_4 (qs) & f_5 prime [T14], completing the factorisation:
M_{251} = 503 * 54217 * 178,230287,214063,289511 *
61676,882198,695257,501367 * 12,070396,178249,893039,969681

p = 257

1644 1) ERROR: Stated by Mersenne [M3; c D1 p13] to be prime
1881 2) Le Lasseur [c D1 p24 n131] found no factor < 30,000
1895 3) Cunningham [C7; c D1 p28 n165] found no factor < 50,000
1911 4) Powers [C15; P8] found no factor < 10,017000
1922 5) **COMPOSITE (?):** Kraitchik [L2] computed a NZLR - lost in Gerardin's files
1927 6) **COMPOSITE:** D H Lehmer [L2; L26] computed correct NZLR [R2; R10; T11]
1936 7) ERROR: Krieger [K19] thought M_{257} prime
1952 8) Robinson [R2; R10] confirmed Lehmer's NZLR
1960 9) Brillhart [B2] found no factor < 2^{31}
1963 10) Brillhart [B4] found no factor < 2^{35}
1979 11) Penk [c B16; B17; B19] found f_1 = 535,006138,814359 (rho) to be prime
1980 12) Baillie [c B16; B17; B19] found f_2 (Pp) & f_3 to complete the factorisation:
M_{257} = 535,006138,814359 * 1,155685,395246,619182,673033 *
374,550598,501810,936581,776630,096313,181393 [S18; T10]

A trivial computation will satisfy the reader that the above statements $M_p = \prod_i f_i$ are correct. The confirmation, if required, that the f_i are prime is a much more significant computation which could be simplified by the provision of supporting evidence in the form of a primality-certificate; Vaughn Pratt [P5] proved that succinct certificates exist in all cases. The author [H20] has compiled certificates using factorisations by Brent, Davis & Holdridge, Naur, Pollard and Wagstaff. These certificates minimise the verifier's work and 'go down' the 'p-1 route'.

7 FURTHER MERSENNE NUMBERS - LUCAS LEHMER TESTS AND ERRORS: M_p ORDER

Results are grouped in line with the ranges of prime indexes of "original" computations. All prime-indexes 'p' have been accounted for by Lucas Residue (LR) or prime factor for p < 100,000.

258 < p < 2304

1949 NEWMAN, KILBURN & TOOTILL [H21; N16; T13]

1) Computed LRs for all (?) p < 354
2) Confirmed prime/composite pattern for p < 258
3) Did not publish p or LRs

1952 LEHMER & ROBINSON [L3; L4; L5; R2; R3]

1) Lehmer eliminated M_p where a factor was known
2) Robinson computed LR for all (sic) remaining M_p in this range
3) **PRIME:** 13th Mersenne Prime M_{521} discovered on 30/1/1952 [L3]
4) **PRIME:** 14th Mersenne Prime M_{607} discovered on 30/1/1952 [L3]
5) **PRIME:** 15th Mersenne Prime M_{1279} discovered on 25/6/1952 [L4]
6) **PRIME:** 16th Mersenne Prime M_{2203} discovered on 7/10/1952 [L5]
7) **PRIME:** 17th Mersenne Prime M_{2281} discovered on 9/10/1952 [L5]
8) Checked with identical runs on different days until two results agreed
9) Used an alternative starting value, S_1 = 10, for the Lucas test
10) Made residues available to subsequent workers (Selfridge & Hurwitz)
11) ERROR: incorrect NZLR for M_{1889}. Found by Hurwitz' IBM7090 [S3]
12) Did not use modulus check on the computation [R10]
13) Did not publish p, LRs, M_p-factors and factor-table sources
14) Did not remark on the frequency of residue disagreements (8 above)

1961 SELFRIDGE & HURWITZ [H1; H2; S3]

1) Computed LR for all (sic) M_p where no M_p-factor was known
2) Found SWAC LR for M_{1889} incorrect; SWAC confirmed error [S3]
3) Did not publish p, LRs, M_p-factors and factor-table references

1963 GILLIES [G1; G7]

1) Computed LR for all M_p where no M_p-factor was known [G7]
2) Tabled last 5 octal digits of LRs [G7]

1971 TUCKERMAN [T1]

1) Computed LR for all (sic) M_p where no M_p-factor was known
2) Did not publish p, LRs, M_p-factors and factor-table references

1979 NELSON & SLOWINSKI [N1; N12; S1]

1) Computed LR for all p < 16310, 16400 - 17188, 18020 - 24000 et al [N12]
2) Second-sourced all LRs in the above three ranges [N12]
3) Confirmed prime/composite-M_p pattern for p < 21000
4) Deposited LRs in Maths. Comp. UMT file for p < 50024 [N12]

1982 ICL 2900 DAP [H8 - H15]

1) Computed 2828 LRs for p < 50024
2) Confirmed all LRs or corrected LRs in [G1; G7; H2; K1; N7; R10; S3; T6]
3) Confirmed all LRs in [N12] where no factor was known with 16 corrections
4) Deposited LRs for p < 62982 in MC UMT file [H15]

2304 < p < 3300

1957 RIESEL [R5; R1]

1) Examined all M_p, p < 10000, for a factor q < 10.2^{20}
2) Computed LR for all (sic) remaining M_p in this range
3) **PRIME:** 18th Mersenne Prime M_{3217} discovered on 8/9/1957
4) Checked with second run that M_{3217} is prime
5) Checked all previously known prime M_p for zero residue
6) Checked factor values against other sources: Lehmer, Kraitchik, ...
7) Double-checked that (all?) factors are of form '2kp + 1'
8) Published first factor of M_p where known
9) Cautioned that 'factors' tabled may not be true divisors of M_p
10) Cautioned that BESK only did one run on 'composite' M_p
11) Made the LRs available (in hexadecimal) to Selfridge & Hurwitz [S3]
12) ERRORS: Two proof-preparation errors in factor table; corrected [S5]
13) ERRORS (?): 4 (?) NZLRs (p = 2957, 2969, 3049, 3109) incorrect [S3]
14) Did not use modulus check on the calculation [R12]
15) Did not use alternative starting value S_1 = 10 for Lucas test
16) Did not residue test for p < 2304 and check against SWAC LRs
17) Did not publish the computed LRs

1961 SELFRIDGE & HURWITZ [H1; H2; S3]

1) Computed LR for all (sic) M_p where no M_p-factor was known
2) Disagreed with Riesel's LRs for 4 indexes 'p', see note 13 above [S3]
3) ERRORS: 4 incorrect NZLRs originally computed; later corrected [S3]
4) Did not publish p, LRs, M_p-factors and factor-table references

1963 GILLIES [G1; G7]

1) Computed LR for all M_p where no factor was known for p < 12124
2) Tabled last 5 octal digits of LRs [G7]

1971 TUCKERMAN [T1]

1) Computed LR for all (sic) M_p where no factor was known for p < 21000
2) Did not publish p, LRs, M_p-factors and factor-table references

1979 NELSON & SLOWINSKI [N1; N12; S1]

1) Computed LR for all p < 16310, 16400 - 17188, 18020 - 24000 et al [N12]
2) Second-sourced all LRs in the above three ranges [N12]
3) Confirmed prime/composite-M_p pattern for p < 21000
4) Deposited LRs in Maths. Comp. UMT file for p < 50024 [N12]

1982 ICL 2900 DAP [H8 - H15]

1) Computed 2828 LRs for p < 50024
2) Confirmed all LRs or corrected LRs in [G1; G7; H2; K1; N7; R10; S3; T6]
3) Confirmed all LRs in [N12] where no factor was known with 16 corrections
4) Deposited LRs for p < 62982 in MC UMT file [H15]

$3300 < p < 5000$

1961 SELFRIDGE & HURWITZ [H1; H2; S3]

1) Computed LR for all M_p in this range where no factor was known
2) **PRIME:** 19th Mersenne Prime M_{4253} discovered on or before 3/11/1961
3) **PRIME:** 20th Mersenne Prime M_{4423} discovered on or before 3/11/1961
3) Used Lucas test with both $S_1 = 4$ and $S_1 = 10$ on **prime** M_p
4) Used Brillhart's factors to eliminate some composite M_p
5) Published last 5 octal digits of LRs
6) Published sign of S_{p-2} for prime M_p
7) ERRORS : 4 incorrect NZLRs (p = 3637, 3847, 4397, 4421) [S3]
8) Did not check Brillhart's factors
10) Did not modulus-check the computation

1963 GILLIES [G1; G7]

1) Computed LR for all M_p where no factor was known [G7]
2) Corrected Hurwitz' four errors [G7; G1], see note 7 above
3) Confirmed (last 5 octal digits of) all Hurwitz' remaining LRs in this range
4) Tabled last 5 octal digits of LRs [G7]

1971 TUCKERMAN [T1]

1) Computed LR for all (sic) M_p where no M_p-factor was known
2) Did not publish p, LRs, M_p-factors and factor-table references

1979 NELSON & SLOWINSKI [N1; N12; S1]

1) Computed LR for all M_p, $p < 16310$, 16400 - 17188, 18020 - 24000 et al [N12]
2) Second-sourced all LRs in the above three ranges [N12]
3) Confirmed prime/composite-M_p pattern for $p < 21000$
4) Deposited LRs in Maths. Comp. UMT file for $p < 50024$ [N12]

1982 ICL 2900 DAP [H8 - H15]

1) Computed 2828 LRs for $p < 50024$
2) Confirmed all LRs or corrected LRs in [G1; G7; H2; K1; N7; R10; S3; T6]
3) Confirmed all LRs in [N12] where no factor was known with 16 corrections
4) Deposited LRs for $p < 62982$ in MC UMT file [H15]

5000 < p < 6000

1963 SELFRIDGE & HURWITZ [S3]

1) Computed LR for all M_p where no M_p-factor was known
2) Published last 5 octal digits of LRs
3) Checked both S_i squaring and mod M_p reduction modulo $2^{35}-1$

1963 GILLIES [G1; G7]

1) Computed LR for all M_p where no M_p-factor was known [G7]
2) Tabled last 5 octal digits of LR [G7]
3) Found factor and did not compute NZLR for p = 5387, 5591, 5641, 5987
4) Confirmed (last 5 octal digits of) Selfridge/Hurwitz's remaining NZLRs

1971 TUCKERMAN [T1]

1) Computed LR for all (sic) M_p where no M_p-factor was known
2) Did not publish p, LRs, M_p-factors and factor-table references

1979 NELSON & SLOWINSKI [N1; N12; S1]

1) Computed LR for all M_p, p < 16310, 16400 - 17188, 18020 - 24000 et al [N12]
2) Second-sourced all LRs in the above three ranges [N12]
3) Confirmed prime/composite-M_p pattern for p < 21000
4) Deposited LRs in Maths. Comp. UMT file for p < 50024 [N12]

1982 ICL 2900 DAP [H8 - H15]

1) Computed 2828 LRs for p < 50024
2) Confirmed all LRs or corrected LRs in [G1; G7; H2; K1; N7; R10; S3; T6]
3) Confirmed all LRs in [N12] where no factor was known with 16 corrections
4) Deposited LRs for p < 62982 in MC UMT file [H15]

6000 < p < 7000

1963 KRAVITZ & BERG [K1]

1) Computed LR for all M_p in this range where no factors was known
2) Published last 5 octal digits of LRs: last 12 octal digits tabled [B14]
3) ERROR: originally computed incorrect NZLR for 10 M_p (asterisked [K1])
4) Corrected these errors after Gillies' letter and before publication
5) Did not modulus-check the computation [B14; K21; K22]

1963 GILLIES [G1; G7]

1) Computed LR for all M_p where no factor was known, $p < 12124$
2) Computed extended factor-table after LR computations
3) Tabled last 5 octal digits of LRs
4) Did not table computed LRs for p = 6089, 6661, 6779, 6907

1971 TUCKERMAN [T1]

1) Computed LR for all (sic) M_p where no M_p-factor was known
2) Did not publish p, LRs, M_p-factors and factor-table references

1979 NELSON & SLOWINSKI [N1; N12; S1]

1) Computed LR for all M_p, $p < 16310$, 16400 - 17188, 18020 - 24000 et al [N12]
2) Second-sourced all LRs in the above three ranges [N12]
3) Confirmed prime/composite-M_p pattern for $p < 21000$
4) Deposited LRs in Maths. Comp. UMT file for $p < 50024$ [N12]

1982 ICL 2900 DAP [H8 - H15]

1) Computed 2828 LRs for $p < 50024$
2) Confirmed all LRs or corrected LRs in [G1; G7; H2; K1; N7; R10; S3; T6]
3) Confirmed all LRs in [N12] where no factor was known with 16 corrections
4) Deposited LRs for $p < 62982$ in MC UMT file [H15]

7000 < p < 12144

1963 GILLIES [G1; G7]

1) Computed M_p-factors < 2^{36} to eliminated some composite M_p [B16]
2) Computed LR for all remaining M_p in this range
3) **PRIME:** 21st Mersenne Prime M_{9689} discovered on or before 11/5/1963 [G5]
4) **PRIME:** 22nd Mersenne Prime M_{9941} discovered around 16/5/1963 [G5; M9]
5) **PRIME:** 23rd Mersenne Prime M_{11213} discovered on 2/6/1963 [M9]
6) Checked calculation modulo $2^{44}-1$
7) Published p, LRs and M_p-factors discovered and/or used to eliminate M_p
8) ERROR: NZLR for p = 12143 corrected by Tuckerman [T2]
9) Did not use Lucas test with S_1 = 10 or do a confirmation run
10) Did not check available residues of composite M_p, p < 3300

1971 TUCKERMAN [T1; T2]

1) Computed LR for all (sic) M_p where no factor was known, p < 21000
2) Corrected Gillies' NZLR for p = 12143 [T2]
3) Did not publish p, LRs, M_p-factors and factor-table references

1979 NELSON & SLOWINSKI [N1; N12; S1]

1) Computed LR for all M_p, p < 16310, 16400 - 17188, 18020 - 24000 et al [N12]
2) Second-sourced all LRs in the above three ranges [N12]
3) Confirmed prime/composite-M_p pattern for p < 21000
4) Deposited LRs in Maths. Comp. UMT file for p < 50024 [N12]

1982 ICL 2900 DAP [H8 - H15]

1) Computed 2828 LRs for p < 50024
2) Confirmed all LRs or corrected LRs in [G1; G7; H2; K1; N7; R10; S3; T6]
3) Confirmed all LRs in [N12] where no factor was known with 16 corrections
4) Deposited LRs for p < 62982 in MC UMT file [H15]

12144 < p < 21000

1971 TUCKERMAN [T1; T6]

1) Eliminated some composite M_p using factor-tables
2) Computed LR for remaining M_p in this range
3) **PRIME:** 24th Mersenne Prime M_{19937} discovered on 4/3/1971
4) Checked calculation-steps modulo $2^{24}-1$ and $2^{24}-3$
5) Confirmed known factors of these M_p before eliminating them
6) Checked zero residue for M_{19937} with altered program
7) Communicated result to MIT; it was confirmed by Speciner & Schroepepel
8) Tabled last 5 octal digits of LRs [T3]
9) Did not use Lucas test with S_1 = 10

1979 NELSON & SLOWINSKI [N1; N12; S1]

1) Computed LR for all M_p, p < 16310, 16400 - 17188, 18020 - 24000 et al [N12]
2) Second-sourced all LRs in the above three ranges [N12]
3) Confirmed prime/composite-M_p pattern for p < 21000
4) Deposited LRs in Maths. Comp. UMT file for p < 50024 [N12]

1982 ICL 2900 DAP [H8 - H15]

1) Computed 2828 LRs for p < 50024
2) Confirmed all LRs or corrected LRs in [G1; G7; H2; K1; N7; R10; S3; T6]
3) Confirmed all LRs in [N12] where no factor was known with 16 corrections
4) Deposited LRs for p < 62982 in MC UMT file [H15]

$21000 < p < 24500$

1979 NICKEL & NOLL [N5; N6; N7; S4; S13]

1) Eliminated some composite M_p using Wagstaff's factor-table
2) Computed LR for remaining M_p in this range
3) **PRIME:** 25th Mersenne Prime M_{21701} discovered on 30/10/1978
4) **PRIME:** 26th Mersenne Prime M_{23209} discovered on 9/2/1979
5) Checked results with second computation
6) Submitted the prime M_{21701} to Lehmer & Tuckerman for checking [N5]
7) Published p, LRs, M_p-factors and factor-table references [N7]
8) ERROR: omitted "22501 67260" from first table [N7]: f_1 = 3026,834521
9) No modulus check included in the code [N4]

1979 NELSON & SLOWINSKI [N1; N2; N12; S1]

1) Computed LR for all M_p, p < 16310, 16400 - 17188, 18020 - 24000 et al [N2]
2) **PRIME:** independently discovered M_{23209} on 23/2/1979
3) Confirmed prime/composite-M_p pattern for p < 21000
4) Deposited LRs in Maths. Comp. UMT file [N12]
5) Did not compare NZLR values for all computed tests [N2]

1981 ICL 2900 DAP [H8 - H15]

1) Computed 2828 LRs for p < 50024
2) Confirmed all LRs or corrected LRs in [G1; G7; H2; K1; N7; R10; S3; T6]
3) Confirmed all LRs in [N12] where no factor was known with 16 corrections
4) Deposited LRs for p < 62982 in MC UMT file [H15]

$24500 < p < 50024$

1979 NELSON & SLOWINSKI [N1; N12; N14; N15; S1; S13]

1) Computed LR for all p < 16310 [N2]
2) Eliminated some composite M_p using Wagstaff's factor-table [W8]
3) Computed LR for remaining p, 30000 < p < 50024
4) **PRIME:** 27th Mersenne Prime M_{44497} discovered on 8/4/1979
5) Noll confirmed M_{44497} prime [N9]
6) Checked the squaring modulo $2^{24}-1$ [N1]
7) Deposited LRs in Maths. Comp. UMT file [N12]
8) Did not confirm the M_p-eliminating factors used
9) Did not check against many known Lucas residues
10) Did not use Lucas test with S_1 = 10
11) ERROR: omitted indexes 24733, 40639 and 44623
12) ERROR: wrong residue on 32831 due to 'p = 23 mod 24' error [N12; N14; N15]
13) ERROR: wrong residue on 43793 due to transient fault during (?) mod-reduction
14) ERROR: wrong residues on 14 indexes due to possible code-experimentation:
    46399, 47137, 48079, 48119, 48157, 48164, 48193, 48409, 48413, 48437, 48449, 48473, 48481, 50021
15) Corrected errors above given ICL DAP results below [N14; N15]

1981 ICL 2900 DAP [H8 - H15]

1) Computed 2828 LRs for p < 50024
2) Confirmed all LRs or corrected LRs in [G1; G7; H2; K1; N7; R10; S3; T6]
3) Confirmed all LRs in [N12] where no factor was known with 16 corrections
4) Deposited LRs for p < 62982 in MC UMT file [H15]

50024 < p < 62982

1982 ICL 2900 DAP [H8 - H15; L45]

1) Computed 2828 LRs for p < 50024
2) Confirmed all LRs or corrected LRs in [G1; G7; H2; K1; N7; R10; S3; T6]
3) Confirmed all LRs in [N12] after 16 corrections and 3 additions
4) Checked the squaring modulo 2^3-1 and computed on 32 numbers in parallel
5) Computed factor-table and checked against others [K30; L45; W8; W12]
6) Deposited last 15 octal digits of LRs and factor-table in MC UMT file [H15]

62982 < p < 216092

At this point, the previous strict chronology breaks down. Isolated M_p have been tested, a number of computer codes are simultaneously active and Slowinski's testing is both non-sequential and unfiled.

1978 NOLL [N10]

1) Computed NZLR (25/12/1978) for M_{65537} in 168° on CDC CYBER-174
2) NZLR for M_{65537} is 56172 70454 77750 45726

1979 NELSON [N17]

1) Confirmed NZLR (13/3/1979) for M_{65537} in 1°1'51"
2) Computed NZLR (29/4/1979) for M_{131071} as .... 21673 53757 40460 in 7°28'

1981 NELSON [N17]

1) Computed NZLR for M_{65539} as 21616 05464 50663
2) Computed NZLR for M_{65543} as 02405 16722 60672

1982 SLOWINSKI [N21; N23]

1) Computed factor or LR for 'most' M_p in 75000 < p < 90000 [N21]
2) **PRIME:** 28th known Mersenne prime M_{86243} discovered on 25/9/1982 in 1°36'22"
3) Nelson confirmed M_{86243} prime using the CRAY/1 '1979' code
4) McGrogan & Noll confirmed M_{86243} prime using a CYBER-205 in 1° [N23]
5) Holmes et al confirmed M_{86243} prime using an ICL-DAP on 22/12/1982 in 38'38"

1983 ICL 2900 DAP [B32; B33; B34; H15]

1) Tabulated the 1913 M_p-f_1 < 2^{40} for 62982 < p < 100000
2) Confirmed factor-table against those of Keller and Wagstaff [K30; W14]
3) Code C confirmed 520 known LRs
4) Computed NZLR for the 397 remaining p, 62982 < p < 73180
5) Computed NZLR for the 339 remaining p, 90534 < p < 100000
6) Checked the squaring modulo 2^{16}-1 and computed 16 M_p in parallel

1983 SLOWINSKI

1) **PRIME:** 29th known Mersenne prime M_{132049} discovered on 20/9/83 in 32'30"
2) Reportedly computed LR for all p < 103,000 [D4]

1984 ICL 2900 DAP [H18; H19]

1) Computed LR for the 626 M_p, 73180 < p < 90534
2) Confirmed M_{86243} as the 28th Mersenne Prime in order of size
3) Deposited LRs for the complete range, 50024 < p < 100000 [H19] in MC UMT

1985 SLOWINSKI [D6]

1) **PRIME:** 30th known Mersenne prime M_{216091} discovered on 6/9/86 in 3°
2) McGrogan confirmed prime prior to publication

1988 COLQUITT & WELSH [C32; C33]

1) **PRIME:** 31st known Mersenne prime M_{110503} discovered on 29/1/88
2) NEC SX-2 program included a modulus-check on the squaring
3) M_{110503} confirmed prime by McGrogan (ELXSI), SLowinski (CRAY XMP), Young (CRAY XMP) and Colquitt (NEC SX-2, 'schoolboy multiplication' code) [C33]
4) Computed an M_p-f_1 or M_p-LR for all p, $10^5 < p \leq 132049$ [C33]

1989 COLQUITT & WELSH [C34; H22]

1) Computed an M_p-f_1 or M_p-LR for all p, $10^5 < p \leq 139267$ [C34; H22]
2) Confirmed 1134 of 2828 LRs with p < 50000 [H19] with no disagreements [H22]

8 PUBLISHED WORK - ERRORS: AUTHOR ORDER

This section does not claim to be complete as the errors have been noticed 'en passant' rather than as a result of deliberate proof-reading. Published errata and corrigenda have been included here.

R. C. ARCHIBALD

A1 1) Attributions in doubt or incomplete: M_{11}, M_{13}, M_{23}, M_{37}
2) Note 6: Lucas authored Amer. J. Math. v1 p240 - table is 'apres Landry'
3) Note 10: On M_{163}, for "30th April 1908" read "7th May 1908"
The date was incorrectly printed on that page of 'Nature'.
4) Note 11: For "p80" read "p86" - unclear 'Nature' typeface
5) Note 13: end of 2nd paragraph: "p118" may be incorrect
6) Note 14: for "p383" read "p883"
7) Euler's "Opuscula": On p113, "2 ---> 36"; on p116, " ---> 37"

C. B. BARKER

B1 1) NZLR incorrect even though he used modulus checks [R2; T11]

A. H. BEILER

B21 1) p18, ending paragraph 1: Uhler found that none of the numbers corresponding to the six indices (157, 167, 193, 199, 227, 229) were perfect.
2) p247: references 5 & 6 are by D H Lehmer, not D N Lehmer

C. E. BICKMORE

B12 1) p17, line 10: for "$2^{31}-1$" read "$2^{37}-1$"

R. P. BRENT

B26 1) Against k = 337, for "prp67" read "prp68", later proved "p68" [B28]

J. BRILLHART

B2 1) p366, 3A: for "55" read "47"
2) p368: remove the "*" against all $f_i < 10^6$ except for p = 1049,
ie for p = 571, 641, 719, 761, 883, 967, 1019, 1093. See MR23#A832.
Source of factors for p = 719, 967, 1019, 1093 unknown to this author.

B4 1) Tenth reference needed - should be to [K2]
[K2] on p85 has a reference to 3 factors, namely:
f_2 of $M_{10,007}$; f_1 of $M_{10,009}$; f_2 of $M_{10,091}$

B6 1) p644: for "The eight new" read "The nine new" and insert "233" in the list. f_3 of M_{233} was found prime by Corollary 11 [B16]
2) p645: Schroeppel did not publish M_{149}'s factorisation in AIM 239 (ref [1]) but communicated it privately to the author [B16]
3) see MC v39 (1982) p747

P. A. CATALDI

C2 1) Regarded M_{23}, M_{29} and M_{37} as primes

R. W. D. CHRISTIE

C27 1) Regarded M_{41} and M_{47} as primes

A. J. C. CUNNINGHAM

C7 1) Found no factor < 50,000 for M_{181}; in fact f_1 = 43441 [C11; W1]

2) 14831 $\nmid M_{1483}$ but 14591 $\mid M_{1459}$ [B29; K30]

C8 1) For "Only 18 Mersenne's numbers remain unverified" read
"Only 18 Mersenne's numbers stated to be composite by Mersenne remain unverified. M_{257}, stated by Mersenne to be prime, also remains unverified."
Evidence of Cunningham's concentration on 'composite M_p' comes from [C11; C4; C29]

2) Found no factor < 200,000 for M_{181}; in fact f_1 = 43441 [C11; W1]

C16 1) Various errors; see original copy & Thorkil Naur's letter

L. E. DICKSON

D1 1) p18 n89: for "p25" read "pp26-7". Euler did not claim all factors prime.

2) p30 n184: for "BAMS v16" read "BAMS v17"

3) p31 n191: for "p87" read "p86"

4) p31 n192b: "d = 1 mod 24" is incorrect for p = 31, 61 (Gerardin's error?)

5) p31 n192c: Fauquembergue's NZLR for M_{101} was found incorrect in 1952 [R2]

6) p32 n199: for "31" read "131" in the reference to Lucas' test

7) p32 n200: Fauquembergue's NZLRs for M_{103} & M_{109} were also found to be incorrect in 1952 [R2]

L. EULER

E3 1) p27, against 2^{21}: for "3 23 89" read "3.23.89"
2) p27, against 3: for "2 " read "2^2"
3) p27, against 3^3: for "2 " read "2^3"
4) p27, against 5^5: for "3^3" read "3^2"
5) p27, against 7^{10}: for "329554457" read "1123.293459" [B29]
6) p28, against 37^3: for "2603" read "19.137"
7) p28, against 41^3: for "29_2" read "29^2"
8) p28, entries for 79, 79^2 and 79^3 have been omitted. They should read [E4]:
79 :: 2^4.5, 79^2 :: 3.7^2.43, 79^3 :: 2^5.5.3121
9) p28, against 137^3: for "2 " read "2^2"
10) p28, against 149^3: for "11.101" read "17.653"
11) p28, against 157^3: for "29 79" read "29.79"
12) p28, against 167^3: for "3 5.7 2789" read "3.5.7.2789"
13) p28, against 173^2: for "67.449" read "30103"
14) p28, against 193^2: for "3 7" read "3.7"
15) p29, against 257^2: for "43 1321" read "43.1321"
16) p29, against 283^2: for "2^2" read "2^3"
17) p29, against 311^3: for "2^4 3" read "2^4.3"
18) p29, against 347^3: for "2^3 3" read "2^3.3"
19) p29, against 353^3: for "5 17" read "5.17"
20) p30, against 461^3: for "11106261" read "11.106261"
21) p30, against 523^3: for "7" read "17"
22) p30, against 563^3: for "3 5 29" read "3.5.29"
23) p30, against 571^3: for "163041" read "163021"
24) p30, against 613^2: for "125461" read "7.17923"
25) p31, against 769^3: for "71" read "17"
26) p31, against 811: for "2" read "2^2"
27) p31, against 827: for "3^3" read "3^2"
28) p31, against 863: for "25" read "2^5"
29) p31, against 907^3: for "23" read "2^3"
30) p31, against 929^3: for "31 431521" read "31.431521"

E2 1) The errors in [E3] listed above as 4-6, 8, 10, 13, 16, 20, 21, 23-27 are reproduced here.
2) p104, against 17: for "3^3" read "3^2"
3) p105, against 41^3: for "29" read "29^2"
4) p106, against 359^3: for "3^3" read "3^2"
5) p109, below "929", for "919^2" read "929^2" and for "919^3" read "929^3"

E4 1) p90, against 7^{10}: for "329554457" read "1123.293459" [B29]

E. FAUQUEMBERGUE

F12 1) Incorrect NZLR for M_{101}: discovered by Robinson on SWAC in 1952 [R2]

F1 1) Incorrect NZLR for M_{103}: discovered by Robinson on SWAC in 1952 [R2]
2) Incorrect NZLR for M_{109}: discovered by Robinson on SWAC in 1952 [R2]

F10 1) Incorrect NZLR for M_{137}: discovered by Robinson on SWAC in 1952 [R2]

A. FERRIER

F4 1) p5, against p = 359: for "855851" read "855857" [K30]

D. B. GILLIES

G7 1) NZLR for M_{12143} incorrect [H8; T2]. For "27361" read "71510".
2) (Author's copy) M_{12641}, f_4: for "4124,947915" read "41249,479151" [G1]
3) (Author's copy) M_{14593}, f_5: for "6336,911017" read "63369,110177" [G1]

G1 1) NZLR for M_{12143} incorrect [H8; T2]. For "27361" read "71510".

V. A. GOLUBEV

G11 1) p258: add two columns to the table of Seredinskij:
(130 .. 23 .. 5197 .. 31183) and (50 .. 47 .. 10357 .. 62143) [K28]
2) p259: In Theoreme II, for "$2^{12n+1}-1$ ... 12n+1" read "$2^{2n+1}-1$ ... 2n+1"
3) p259: In Theoreme II, for "$=2^{12n+1}$" read "$=2^{2n+1}$"
4) p259: In the 5th row of the table, x, for "36" read "86"
5) p259: In the 7th row of the table, p_1, for "1692" read "1693"
6) p260: Theoreme IV. For "2^n-1" read "2^p-1"
7) p260: In the 3rd row of the first table, p, for "1365" read "1367"
8) p260: Delete the 14th column of the first table because 19337 = 61 * 317
9) p260: Exchange the "x" and "y" in the labellings of the second table
10) p260: In the 1st row of the second table, for "15" read "25"
11) p261: Add to the first table the column (13 .. 31 .. 4447 .. 71153)

G. H. HARDY & E. M. WRIGHT

H6 1) (3rd Edition: 1954), on p11, M_{2281} is said to have 686 decimal digits.
For "686" read "687".
2) (4th Edition: 1960, reprinted 1965), on p16, M_{11213} is said to have
3375 decimal digits. For "3375" read "3376". Noted by M. Lal [L12]

A. HURWITZ

H2 1) NZLRs found incorrect [S3] for 4 M_p with $p < 3300$
2) NZLRs found incorrect [G1; G7; N2; N3] for 4 M_p:
for M_{3637}'s "67413" read "53313", for M_{3847}'s "57652" read "14400",
for M_{4397}'s "40174" read "44327", for M_{4421}'s "25131" read "03013"

E. KARST

K2 1) p80: proof that $\nexists$ prime q s.t. $q^2 \mid M_p$ is fallacious [K8]

D. E. KNUTH

K26 1) p391: credited Lucas with showing M_{67} composite. NZLR unconfirmed
2) p391: credited Kraitchik with showing M_{257} composite. NZLR unconfirmed
3) p391: for "CRAY-I" read "CRAY-1"
4) p394: "The world's largest explicitly known prime numbers have always been
Mersenne primes, at least from 1772 until 1980" is incorrect.
In 1867 [L20; c D1] and 1869 [L19 p4; c D1], Landry preceded Lucas' prime
M_{127} of 1876 by listing 14 primes > M_{31}. Landry's work may be regarded
as reliable although he pronounced one composite number prime in those
tables. The two 1867 primes of the 14 are asterisked below:

$2931,542417 \mid 2^{44}+1$	$77158,673929 \mid 2^{63}+1$	$4,363953,127297 \mid 2^{49}+1$
$4278,255361 \mid 2^{40}+1$	$165768,537521 \mid 2^{47}+1$	$4,432676,798593 \mid 2^{49}-1$
$4562,284561 \mid 2^{60}+1$	$168749,965921 \mid 2^{69}+1$*	$3,203431,780337 \mid 2^{59}-1$
$8831,418697 \mid 2^{41}+1$	$1,133836,730401 \mid 2^{75}+1$*	$28,059810,762433 \mid 2^{53}+1$
$54410,972897 \mid 2^{56}+1$	$2,932031,007403 \mid 2^{43}+1$	

In 1951-2, the primes of Miller & Wheeler and of Ferrier [M2; M5]
superceded M_{127} and preceded M_{521}.

M. KRAITCHIK

K3 1) Chapter 3, p24, Section 65 table: against n=163, for "160287" read "150287"

K13 1) p756, table 1, against n = 67: for "19,370721" read "193,707721"
2) p756, table 2, against n = 163: for "160287" read "150287"

K32 1) p756, against n = 67: for "19,370721" read "193,707721"
2) p756, against n = 67: for "7,618388,257287" read "761838,257287"
3) p756, against n = 87: for "1107" read "1103" [B29; F4]
4) p756, against n = 127: for "...864..." read "...884..."

S. KRAVITZ

K5 1) After p = 13049, for "12063" read "13063"

K1 1) For ten asterisked M_p, incorrect NZLRs were corrected before publication. These were caused by an inadmissable value of S_1 being introduced by a card-punch error while making up three 'identical' program-decks.

Le LASSEUR de SANZY

L25 1) Found no factor < 30,000 for M_{197} [c D1 p24 n131]; f_1 = 7487 [C3; C6]

D. H. LEHMER

L2 1) M_{233} is listed as "only one factor known". N G W H Beeger noted [L7] that f_2 was known at that time.

L3 1) For "k = 744" read "k = 774": corrected by T Wilcox [W4]

E. LUCAS

L14 1) Incomplete proofs of his residue-tests

L32 1) p283: for "177951" read "179951"

L13 1) p376: the prime M_{89} was pronounced composite following NZLR computation

Several historical misattributions; unsubstantiated claims about machines [A1]

M. MERSENNE

M3 1) Stated M_{67} to be prime; it is composite [F8; F9; C17]
2) Stated M_{257} to be prime; it is composite [L2]
3) Stated M_{61} to be composite; it is prime [P13; P14; P16]
4) Stated M_{89} to be composite; it is prime [C12; P9; P15]
5) Stated M_{107} to be composite; it is prime [P2; P6; P10]
6) Stated in effect that M_p was composite for $17000 < p < 32000$: M_p is prime for p = 19937 [T1; N1], 21701 [S4; N5; N1; T6] and 23209 [N6; N1; S13; S1] and only for those p [N1]

M6 1) "$p = 2^{2n} + k$; k = 1, 2 or 3 ===> M_p prime"
Correct for p = 2, 3, 5, 7, 17, 19 (known to Mersenne)
Incorrect for p = 67, 257 & 4099

H. L. NELSON

N1 1) Credited Mersenne with a knowledge of M_{29}'s f_2

2) Did not credit Mersenne with the knowledge of M_{37}'s f_1

3) p266: for "2100 by 1971" read "21000 by 1971"

4) p266: for "2, 3, 4, 5" read "2, 3, 5, 7"

C. L. NOLL

N5 1) Cited Seelhoff as a discoverer of the prime M_{61}

N7 1) Credited Gillies with search-range $p < 11400$ and not $p < 12144$

2) Omitted "22501 67260" from first table: M_{22501}-f_1 = 3026,834521

3) Reference 2 - Knuth: for "1963" read "1973"

J. W. PAULI

P11 1) Gave 83 as a factor of M_{41}

J. PLANA

P12 1) Found no factor < 50,033 for M_{53}: in fact $f_1 = 6361$ [L19]

H. RIESEL

R1 1) Disputed NZLRs [N2; S3; R13] for M_{2957}, M_{2969}, M_{3049} and M_{3109}

2) In reference [3] to M. Kraitchik, for "1952" read "1924"

3) Archibald (p208) did not misprint f_1 of M_{163} [A1] as did Kraitchik [K3]

4) p210: against p = 2689, for "7158199" read "7158119". See Selfridge [S5]

5) p211: against p = 5743, for "543217" read "643217". See Selfridge [S5]

R4 1) In the editor's footnote, for "330" read "3300"

2) 4 errors/omissions in factor table [B20]

R. M. ROBINSON

R2 1) Incorrect NZLR detected [S3] for M_{1889}

2) 2nd para, 4th line: for '2^{n-1}' read '2^n-1'

P. SEELHOFF

S12 1) Declared M_{61} to be prime, having only found it probably-prime and made the obvious mistake of assuming a | b & a | c ===> b | c or c | b" [C17; L11]

W. SIERPINSKI

S17 1) p341, 2nd para: for "r_{101}" read "r_{100}"

2) p341, 4th para: for "376 digits" read "386 digits"

3) p341, 6th para: for "M $_{941}$" read "M_{9941}"

4) p341, 6th para: for "3381 digits" read "3376 digits"; see Lal [L12]

5) p341, 6th para: for "Gilles" read "Gillies"

D. SLOWINSKI

S1 1) p259: for "19737" read "19937"

2) p260: for "D. Wheeler, 1959" read "D. Wheeler, 1953"

The "TIMES"

T8 1) p9: for "2^{21701}" read "2^{21701} - 1": corrected [T9]

J. TRAVERS

T3 1) Against E_{89}, for "..378082.." read "..378084.." [T11; U11]
2) Against E_{107}, for "..975360.." read "..9753460.." [T11; U11]

H. S. UHLER

U2 1) For "page iii" read "page xxxvi"

U11 1) v_5: for "3335" read "3355"
2) v_{11}: for "14 13164" read "13164" (there are 65 digits not 67) [T3; T11]
3) v_{12}: for "47401" read "14 47401" (there are 77 digits not 75) [T3; T11]

9 CONJECTURES RESOLVED

In these notes, 'conjecture' is interpreted in the widest sense to include explicit conjectures, observations and statements not backed by proof whose status is lost in the mists of time.

1) "$2^{n-1} * M_n$ is perfect for all odd n" [c D1 Ch1 ns 20, 24, 38, 42, 43]
FALSE: n composite ===> $M_n = (2^a-1)(2^b-1)c$ ===> $2^{n-1}*(2^n-1)$ not perfect.
M_p composite ===> $2^{p-1} * M_p$ is not perfect, the case also for most prime p.

2) "E_p ends alternately in 6 and 8"
[c D1 Ch1 ns 4, 6, 15-20, 25, 26, 28, 38, 42, 43, 45]
FALSE: E_p ends in 6, 8, 6, 8, 6, $\underline{6}$, 8, $\underline{8}$, 6, $\underline{6}$, 8, $\underline{8}$, 6, 8, $\underline{8}$, $\underline{8}$, 6, $\underline{6}$, $\underline{6}$, 8,
6, $\underline{6}$, $\underline{6}$, $\underline{6}$, $\underline{6}$, $\underline{6}$, $\underline{6}$, 8, $\underline{8}$, 6, 8
Thus, "6 & 8 alternate" is so far (31 E_p) true 15 times, false 15 times, assuming M_{216091} is 31st in order of size.
It's likely that this conjecture arises from observation and the mistaken belief that E_n is perfect for all odd n.

3) "E_p exists with any number of decimal digits" [D1 Ch1 ns 4, 27, 29, 33, 45, 53]
FALSE: The E_p sequence begins 6; 28; 496; 8128; $\underline{33{,}550336}$
The 28th E_p has 51,924 decimal digits
Would not be true even if $2^{n-1} * M_n$ were perfect for all odd 'n'

4) MERSENNE: [M3; c D1 p12 n60]
Effectively, "For $28 < p < 258$, M_p is prime only for p = 31, 67, 127, 257"
FALSE: Incorrect on p = 61, 89 & 107 (later found prime) and on p = 67 & 257 (later found composite)
Mersenne knew the status of M_p for $p < 24$ and p = 37 (10 of 55 M_p)
His statement was correct on the remaining 40 M_p

5) MERSENNE: [c D1 p13 n60]
"There is no perfect number from the power 17000 to 32000"
FALSE: Let us assume this means "M_p is composite for $17000 < p < 32000$".
There are 3 prime M_p (p = 19937, 21701 & 23209) in this range.
This conjecture is perhaps based on the belief that 'M_p prime ===> p near 2^k', the relevant 2^k here being 16,384 and 32,768.

6) MERSENNE: "$p = 2^{2n} + k$; $k < 4$ ===> M_p prime" [M6; c D1 p13 n61]
FALSE: Correct for p = 2, 3, 5, 7, 17, 19, all known to Mersenne.
Incorrect for p = 67, 257, 4099, 65537 & 65539
Suggests that '67' was not a misprint of '61' - Conjecture 4 above
[B10 p316; B11]

7) MERSENNE (according to Lucas & Tannery) [c D1 p28 n162]:
"M_p prime <===> p prime and $p = 2^{2n} + 1$, $2^{2n} \pm 3$ or $2^{2n+1} - 1$"
FALSE: Correct only for (known) p = 2, 5, 7, 13, 17, 19 and p = 31, 61, 127
===> incorrect for p = 3, 89, 107 and the next 16 prime M_p, $p > 257$
<=== incorrect for p = 67, 257, 1021, 4093, 4099, 8191, 16381, 65537, 65539 & 131071.
These are the counterexamples for $p < 262140$.
This attribution explains four out of five of Mersenne' errors BUT
1) Clearly, Mersenne knew $M_3 = 7$ to be prime
2) Mersenne regarded M_{61} as composite (prime by this conjecture)

8) MERSENNE (according to Drake) [D2]:

"p prime, $p = 2^n \pm k$, $k < 4$ <===> M_p prime"

FALSE: Correct for p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 127

===> incorrect for p = 67, 257, 1021, 4093, 4099, 8191, 16381, 65537, 65539 & 131071.

<=== incorrect for p = 89, 107 and the 13th-31st prime M_p.

These are the counterexamples for p < 262140.

9) CATALAN: "$q = M_p$ prime ===> M_q prime" [c D1 p24 n135]:

FALSE: Correct for p = 2, 3, 5, 7. Incorrect for p = 13, 17, 19 and 31.

Catalan knew only of the cases p = 2 and 3. Let $\tilde{M}$ represent M_M.

NZLR for $M_{13} = M_{8191}$ computed by Wheeler et al [G1; H2; H14; N12; T1]

$2 * 20,644229 * M_{13} + 1 = 338193,759479 \mid \tilde{M}_{13}$ [K31]

$2 * 884 * M_{17} + 1 = 231,733529 \mid \tilde{M}_{17}$ [R3]

$2 * 245273 * M_{17} + 1 = 64296,354767 \mid \tilde{M}_{17}$ [K31]

$2 * 60 * M_{19} + 1 = 62,914441 \mid \tilde{M}_{19}$ [R3]

$2 * 68745 * M_{31} + 1 = 295,257526,626031 \mid \tilde{M}_{31}$ [K31]

10) CUNNINGHAM: "M_p prime ===> $p = 2^n \pm 1$ or $2^n \pm 3$" [C5; C7]

FALSE: Correct for p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 127, all known to Cunningham

Incorrect for p = 89, 107 and the known 19 prime M_p after M_{127}

Retracted by Cunningham [C12] when Powers announced the primality of M_{89}

11) GERARDIN [G6]:

"a) If p = 43 mod 60, the first factor of M_p, f_1 = 47 mod 96

b) If p = 33 mod 40, the first factor of M_p, f_1 = 7 mod 24

c) If p = 1 mod 30, the first factor of M_p, f_1 = 1 mod 24

- with the exception of (Euler) cases where p = 4n+3 and 2p+1 is prime"

FALSE: a) Correct for p = 43, 163, 223 [B3], three cases known to Gerardin

Incorrect for 291 of 319 known cases with $p < 10^5$, for example

p = 103 (f_1 = 2550,183799 [B3]) and p = 283 (f_1 = 9623 [B2])

b) Correct for p = 73, 113, 233 [B3], three cases known to Gerardin

Incorrect for 230 of 348 known cases with $p < 10^5$, for example

p = 193 (f_1 = 13,821503 [B2]), p = 313 (f_1 = 10,960009 [B2])

c) Correct for p = 151, 181, 211 [B3], three cases known to Gerardin

Incorrect for 573 of 672 known cases with $p < 10^5$, for example

p = 31 & 61 for which M_p is prime,

p = 241 (f_1 = 22,000409 [B2]) and p = 571 (f_1 = 5711 [B2])

Analysis [H22] based on merge of results [C34; H19]

12) GERARDIN: "q divides M_p and $q \neq 2^r - 1$ ===> M_q is composite" [c D1 p30 n188b]

FALSE: $M_{11} = 23 * 89$: M_{89} is prime [C12; P3; c D1 p30 n185]

$M_{967} = 23209 * 549257 *$ c281 [B2; B17]: M_{23209} is prime [S13; S1]

Presumably this was posed just before Powers found M_{89} prime

'$q \neq 2^r - 1$' excludes the (Catalan) cases q = 3, 7, 31, 127

13) TARRY: "If q is the least factor of a composite M_p, M_q is composite" [c D1 p30 n188b]

FALSE: $M_{967} = 23209 * 549257 *$ cofactor [B2]: M_{23209} is prime [S13; S1]

14) KNUTH: [K26 p394]

"One day, the largest explicitly-known prime will not be a Mersenne prime"

TRUE: p65050 = $M_{216091} < 391581.2^{216193}-1$ = p65087, found 6/8/89 [D7]

15) NAUR: Meta-conjecture on reading previous version of this section:

"All Mersenne-number conjectures are false".

FALSE: See resolution of conjecture 14 above.

10 CONJECTURES OUTSTANDING

1) MERSENNE: "M_p is composite for 1,050,000 < p < 2,090,000" [M3; c D1 p13 n60]
This statement is apparently based on the belief that M_p is prime only when p is near 2^k', the relevant 2^k here being 1,048576 & 2,097152. Based on Pomerance's conjecture on the distribution of prime M_p and current knowledge, the 'likelihood' of this conjecture being true is 0.15649.

2) MERSENNE: "No interval of powers can be assigned so great but that it can be given without perfect numbers" [M3; c D1 p13 n60]
This is interpreted as "$\forall N, \exists n(N)$ s.t. $p \in [n, n + N]$ ===> M_p composite"
This statement is perhaps based on a belief that 'M_p prime ===> p near 2^k'
This conjecture is wrongly motivated but probably correct - see 8 below.

3) CATALAN: "$p_1 = 3$ and $p_{n+1} = 2^{p_n} - 1$ ===> p_{n+1} is prime for all n"
True for p_1, p_2, p_3; M_p = 3, 7, 127 & M_{127} are prime
The generalisation, replacing '$p_1 = M_2$' by '$p_1 = M_q$' is false:
For $p_1 = M_5 = 31$, p_1 and p_2 are prime but M_q is composite for $q = M_{31}$
For $p_1 = M_q = r = M_{13}$, M_{17} or M_{19}, M_r is composite
See Section 9, Conjecture 9 for the first M_p-factors.
For $p_1 = M_q = r = M_{61}$, M_{89} or M_{127}, the status of M_r is unknown.

4) SCHINZEL: "There are an infinite number of Mersenne composites" [S2 p29]
This is likely to be correct; for stronger versions - see 6, 8-10 below.

5) "There are an infinite number of Mersenne primes" [S2 p29]
For a stronger version of this conjecture, see 8 and 9 below.
Golubev [G11] alone says "There are serious reasons for believing that the number of prime M_p is finite."

6) "There are an infinite number of prime p=4k+3 such that 2p+1 is prime" [S2 p29]
For such primes p, M_p has the factor 2p+1 by a theorem of Euler.
This conjecture therefore implies Conjecture 4 above.

7) JAKOBEZYK: "There is no prime q such that q^2 is a factor of some M_p" [S10 p92]
Karst's alleged proof [K2 p80] is incorrect [K8].
Brillhart [B4; B16] has checked this conjecture for
$q < 2^{35}$, $102 < p < 258$ & $q < 2^{34}$, $258 < p < 20,000$
$q^2 \mid M_p$ ===> $2^{q-1} = 1 \pmod{q^2}$ [W11]
There are no such M_p-factors $q < 6.10^9$ [L46]
More generally, this is incorrect for $M_n = 2^n-1$ with n composite [B17; R6]:
first examples: $3^2 \mid M_6$, $5^2 \mid M_{20}$, $7^2 \mid M_{21}$, $11^2 \mid M_{110}$, $13^2 \mid M_{156}$, $17^2 \mid M_{136}$, $31^2 \mid M_{155}$
later examples: $3^5 \mid M_{162}$, $5^3 \mid M_{100}$, $7^3 \mid M_{147}$

8) GILLIES: [G7; G1]
"a) The probability that M_p is prime $\sim (2 \log_e 2p)/(p \log_e 2)$,
b) The expected number of prime M_p s.t. $x < M_p < 2x$ is $2 + 2 \log_e(\log_e 2x/\log_e x)$,
c) The number of prime $M_p < x \sim 2 * (\log_e \log_e x)/\log_e 2$"
ie the number of prime M_p, $p < y \sim 2 \log_e y/\log_e 2 \sim 2.8853901 \log_e y$

9) POMERANCE & LENSTRA: [P24]
"The number of prime M_p with $p < y \sim e^{\gamma} \log_e y / \log_e 2 \sim 2.5695442 \log_e y$"
As seen in the Section 3 graph, this is a much better fit to the data than Gillies' conjecture above.
Euler's constant, $\gamma = 0.577215665$

10) SHANKS & KRAVITZ: [S6]

Let $f_k(x)$ be the number of M_p ($p < x$) such that $d = 2kp+1$ is a prime divisor of M_p

Let $Z'(x)$ be the conjectured estimate for the number of twin-prime pairs $< x$

Then:

$$f_k(x) \;=\; Z'(x)\,[\cos^2(k\pi/4)/k] \prod_{q\,|\,k}[(q-1)/(q-2)] \;*$$
$$[1 - \{\log(2k)/\log x\} + O(\log^2 x)^{-1}]$$

This conjecture accords with the known result "$k = 4m+2 \implies f_k(x) = 0$"

This conjecture implies $f_1(x) = Z'(x)/2$ and $f_3(x) = Z'(x)/3$ - see Conjectures 4 and 6 above.

11) SELFRIDGE: [N10]

"If two of the following statements are true, the third is also true"

a) $p = 2^m \pm 1$ or $p = 2^{2m} \pm 3$

b) M_p is prime

c) $(2^p + 1)/3$ is prime

If 'p' is not prime, then statements b and c are false [B35]

Each statement defines a set of primes 'p' to test the conjecture.

Bateman et al [B35] find the conjecture true for 56 'p' in these ranges:

'a' primes p < 1,000000

'b' primes p < 132050

'c' primes p < 4000

Prior to [N10], it was known that a^b^c was true 9 times; what was the probability of this being true 'at random'. It is unlikely to be true [B35] again on a random basis.

Statements a, b & c are separately true 12, 21 & 14 times respectively.

This condition is proposed [B35] as a neat way to discriminate between the Mersenne conjecture 'hits' (31, 61, 127) and 'misses' (67, 89, 107, 257). There is no evidence that Mersenne considered numbers of form $(2^p+1)/3$. Knowing that M_{11} is composite, he may have chosen not to speculate that M_{29} and M_{131} were prime.

k	0	1	2	3	4	:	5	6	7	8
2 -1	o	1	$\underline{3}$	$\underline{7}$	15	:	$\underline{31}$	63	$\underline{127}$	255
2^k+1	$\underline{2}$	$\underline{3}$	$\underline{5}$	9	$\underline{17}$	:	33	65	129	**257†**
2^k-3	-2	-1	1	(5)	$\underline{13}$	:	**29**	$\underline{61}$†	125	253
2^k+3	4	(5)	$\underline{7}$	**11**	$\underline{19}$	:	35	**67†**	**131**	259

Key:
p = composite M_p
$\underline{p}$ = prime M_p
: = M conjecture boundary
† = Mersenne wrong

12) SLOWINSKI - Meta-conjecture: [S1]

"There will always be more conjectures concerning Mersenne primes than there are known Mersenne primes".

This is trivially true if we allow the class of untested statements 'M_p is prime'. Therefore, Slowinski must be assuming some process for admitting statements as 'worthy' conjectures. Shanks [S2, 3rd Edition] proposes such a process but it has not been used here.

A formal definition of 'conjecture' must precede formal decidability.

Let us delete 'always' and substitute:

'Mersenne numbers' for the first 'Mersenne primes',

'unresolved conjecture' for 'conjecture'.

Slowinski has done more than most to make this meta-conjecture false. Interpreting 'conjecture' in its widest reasonable sense above, the resulting list of unresolved conjectures makes the score 31:12 in favour of the primes. Further submissions are invited.

If the word 'always' is heeded, this meta-conjecture is false.

11 THEORETICAL RESULTS

These are classified below and some sections are expanded.

11.1 EARLY RESULTS ON PERFECT AND MERSENNE NUMBERS

11.1.1 Euclid's Proposition 36: 2^n-1 prime $\Longrightarrow$ $2^{n-1}(2^n-1)$ perfect

11.1.2 2^n-1 prime $\Longrightarrow$ n prime

11.1.3 Even Perfect numbers are of Euclid's form

11.2 FACTORISATION TECHNIQUES

11.2.1 Pre-1970 factorisation methods

11.2.1.1 $q \mid M_p \Longrightarrow q = 2kp + 1$

11.2.1.2 $q \mid M_p \Longrightarrow q = 8r \pm 1$

11.2.1.3 $p = 4k+3$ & $q = 2p+1$: q prime $\Longleftrightarrow q \mid M_p$ [K27]

11.2.1.4 $p = 4k+1$ & $q = 6p+1 = u^2+27v^2$ prime, $u = 12m \pm 2$, v odd $\Longrightarrow q \mid M_p$ [K27]

11.2.1.5 $q = 8p+1 = u^2+64v^2$ prime, v odd, $3 \nmid u$, $3 \nmid v$ $\Longrightarrow q \mid M_p$ [K27]

11.2.1.6 $p = 30k+11$, $q = 8p+1 = u^4+8v^4$, v odd $\Longrightarrow q \mid M_p$ [S21]

11.2.1.7 $p = 4k+3$ & $q = 10p+1$ prime $\Longrightarrow q \mid M_p$ or $q \mid 2^{5p}-1$ [K27]

11.2.1.8 $p = 4k+1$ & $q = 14p+1$ prime $\Longrightarrow q \mid M_p$ or $q \mid 2^{7p}-1$ [K27]

11.2.1.9 $q = 16p+1 = u^2+256v^2 = w^2+32x^2$ prime, $v+x$ even, $3 \mid w$ $\Longrightarrow q \mid M_p$ [K27]

11.2.1.10 $p = 4k+3$ & $q = 18p+1$ prime $\Longrightarrow q \mid M_p$ or $q \mid 2^{3p}-1$ or $q \mid 2^{9p}-1$ [K27]

11.2.1.11 $q = 24p+1 = u^2+27v^2 = w^2+64x^2$ prime, x odd $\Longrightarrow q \mid M_p$ [G11]

11.2.1.12 $q = 48p+1 = u^2+27v^2 = w^2+256x^2 = y^2+32z^2$, $x+z$ even $\Longrightarrow q \mid M_p$ [G11]

11.2.2 Pollard's Monte-Carlo method [B18; P22]

11.2.3 Pollard's P-1 method [P21]

11.2.4 The Continued Fraction method [B15; W10]

11.3 PRIMALITY TESTING

11.3.1 The Lucas-Lehmer test on M_p [L8; L24]

11.3.2 On the Converse of Fermat's theorem [B6; L11; L33; L36; L43; P17; R11]

11.3.3 The general 'N+1' Lucas test [B6]

11.3.4 Combined 'N-1, N+1' methods [B6]

11.3.5 Adleman-Pomerance-Rumely's 'ARPCL' method [A4; C31]

11.4 MISCELLANEOUS RESULTS

11.4.1 The sum of the reciprocals of the divisors of a perfect number is 2

11.4.2 Composite M_p-factors are pseudoprime base 2

11.4.3 $q^2 \mid M_p \Longrightarrow 2^{q-1} = 1 \bmod q^2$ [L46; W11]

11.4.4 q pseudoprime base 2 $\Longrightarrow$ M_q pseudoprime base 2

11.4.5 All E_n are both triangular and hexagonal numbers

11.4.6 For n odd, $E_n = 1 \bmod 9$

11.4.7 For $n \geq 3$ and odd, $E_n = 8/6 \bmod 10$ alternately

11.4.8 For n odd, E_n is a partial sum of $(2i-1)^3$

11.4.9 Mersenne numbers M_p are coprime

11.4.10 $(2^n+1)/3$ prime, n odd $\Longrightarrow$ n prime

11.1.1 Euclid's Proposition 36: 2^n-1 prime ===> $2^{n-1}(2^n-1)$ perfect

Let $q = 2^n-1$ be prime and let $E_n = 2^{n-1}(2^n-1) = 2^{n-1}q$.
The set of factors of E_n is precisely $\{2^i q^j \mid i = 0, \ldots, n-1 \;\&\; j = 0 \text{ or } 1\}$
Let s(N) = the sum of the factors of N.
$s(E_n) = (1+2+ \ldots +2^{n-1}) * (1+q) = (2^n-1)*2^n = 2*E_n$ ##

Euclid did not prove the converse, E_n perfect ===> 2^n-1 prime:
Let $E_n = 2^{n-1}ab = 2^{n-1}(2^n-1)$.
Then $s(E_n) \geq (2^n-1) * (1+a+ab) = (2^n-1) * (1+a+2^n-1) = (2^n-1) * (2^n+a) > 2 * E_n$
Therefore, 2^n-1 composite ===> E_n not perfect
Therefore E_n perfect ===> 2^n-1 prime ##

11.1.2 2^n-1 prime ===> n prime

We will prove by induction on 'a' that $2^b-1 \mid 2^{ab}-1$. This is clearly true for a = 1.
$2^{ab}-1 = 2^b * (2^{(a-1)b}-1) + (2^b-1)$
Therefore $2^b-1 \mid 2^{(a-1)b}-1$ ===> $2^b-1 \mid 2^{ab}-1$.
Therefore, n = ab composite, a & b > 1 ===> $2^a-1 \mid 2^n-1$ and $2^b-1 \mid 2^n-1$.
Therefore 2^n-1 prime ===> n prime ##

11.1.3 Even Perfect Numbers are of Euclid's form

Let $E = 2^{n-1}q$ (q odd) be a perfect number.
Let s(x) = the sum of the divisors of x
Then $s(E) = s(2^{n-1})s(q) = (2^n-1)s(q)$ and $s(E) = 2E = 2^n q$.
$(2^n-1)s(q) = 2^n q$. Letting $M_n = 2^n-1$, we have $M_n Q = (2^n-1)Q = q$
$s(q) = 2^n Q > q + Q = 2^n Q$
Q = 1 and $q = 2^n-1$ is prime ##

.2.1.1 $q \mid M_p$ ===> q = 2kp+1

First, let q be a prime.
$q \mid M_p$ ===> $2^p-1 = 0 \bmod q$ ===> $2^p = 1 \bmod q$.
Let s be the smallest integer i such that $2^i = 1 \bmod q$.
$2^t = 1 \bmod q$ ===> t = rs.
Therefore $2^p = 1 \bmod q$ with p prime ===> p is that smallest integer 's'.
But by Fermat's 'little' theorem, q prime ===> $2^{q-1} = 1 \bmod q$
Therefore (q-1) = rp = 2kp and q = 2kp + 1.
If $Q \mid M_p$, then $Q = q_1^{\alpha_1} * \ldots * q_n^{\alpha_n} = \prod_i q_i^{\alpha_i} = \prod_i (2k_i p + 1)^{\alpha_i} = 2Kp + 1$ ##

11.4.1 The sum of the reciprocals of the divisors of a perfect number is 2

Let $D = \{d \mid d \mid M_p\}$
E_p perfect ===> $2E_p = \sum_D d$ ===> $2 = \sum_D d/E_p$ ===> $2 = \sum_D 1/d$ ##

11.4.2 Composite M_p-factors are psp(2)

The term 'pseudoprime' is reserved here for composite numbers N satisfying Fermat's equation $a^{N-1} = 1 \bmod N$ for some base a. Therefore, let q be a composite factor.

$q \mid M_p$ ===> $2^p-1 = 0 \bmod q$ and q = 2kp+1 ===> $2^p = 1 \bmod q$
===> $2^{kp} = 1^{2k} = 1 \bmod q$ ===> $2^{q-1} = 1 \bmod q$
===> q pseudoprime base 2 ##

11.4.3 $q^2 \mid M_p$ ===> $2^{q-1} = 1 \bmod q^2$

$q \mid M_p$ ===> $q = 2kp + 1$, see 11.2.1.1.
Therefore $2^{(q-1)/2}-1 = 2^{kp}-1 = (2^p-1) * a$, see 11.1.2.
Therefore $q^2 \mid M_p$ ===> $q^2 \mid 2^p-1$ ===> $q^2 \mid 2^{(q-1)/2}-1$ ===> $q^2 \mid 2^{q-1}-1$
Therefore $q^2 \mid M_p$ ===> $2^{q-1} = 1 \bmod q^2$ ##
This provides a test that $q^2 \nmid M_p$ independent of p and of any factorisation. This test also relates to Fermat's last theorem [W11]. However, for small q it is quicker to factorise (q-1)/2 and test-divide candidate M_p.

11.4.4 q pseudoprime base 2 ===> M_q is psp(2)

q pseudoprime ===> q composite ===> M_q composite
q pseudoprime base 2 ===> $2^{q-1} = 1 \bmod q$ ===> $2^q = 2 \bmod q$
===> $2^q-2 = 0 \bmod q$ ===> $2^q-2 = kq$
$M_q = 2^q-1$ ===> $2^q = 1 \bmod M_q$ ===> $2^{kq} = 1^k = 1 \bmod M_q$
===> $2^{2^q-2} = 1 \bmod M_q$ ===> $2^{M_q-1} = 1 \bmod M_q$
===> M_q pseudoprime base 2 ##

11.4.5 All E_n are both triangular and hexagonal numbers

The mth triangular number is $S_{1,m} = \sum i = m(m+1)/2$
The sequence starts 1, 3, 6, 10, ...
If $m = 2^n-1$, $S_{1,m} = 2^{n-1}(2^n-1) = E_n$ ##

The mth hexagonal number is $H_m = m(2m-1)$
The sequence starts 1, 6, 15, 28, 45, ... [K29 p67]
If $m = 2^{n-1}$, $H_m = 2^{n-1}(2^n-1) = E_n$ ##

11.4.6 For n odd, $E_n = 1 \bmod 9$

$E_n = 2^{n-1}(2^n-1)$: $E_1 = 1$, $E_3 = 28$ and $E_5 = 496$. Therefore E_1, E_3 & $E_5 = 1 \bmod 9$.
Compare E_n and E_{n+6}: $2^6 = 64$ ===> $2^6 = 1 \bmod 9$
Therefore $2^{n-1} = 2^{n+5} \bmod 9$, $2^n = 2^{n+6} \bmod 9$ and $2^n-1 = 2^{n+6}-1 \bmod 9$.
Therefore $E_n = E_{n+6} \bmod 9$ and $E_n = 1 \bmod 9$ for all odd n.

11.4.7 For $n \geq 3$ odd, E_n = 8/6 mod 10 alternately

$E_n = 2^{n-1}(2^n-1)$: $E_3 = 28 = 8 \bmod 10$ and $E_5 = 496 = 6 \bmod 10$.
By induction, we show that $E_n = E_{n+4} \bmod 10$.
$2^{n+4} = 2^n \bmod 10$ ===> $2^{n+3} = 2^{n-1} \bmod 10$ and $2^{n+4}-1 = 2^n-1 \bmod 10$.
Therefore $E_{n+4} = 2^{n+3}(2^{n+4}-1) = 2^{n-1}(2^n-1) = E_n \bmod 10$
Therefore $E_{4k+3} = E_3 = 8 \bmod 10$ and $E_{4k+5} = E_5 = 6 \bmod 10$ ##

11.4.8 For n odd, E_n is a partial sum of $(2i-1)^3$

$S_{2,m} = \sum i^2 = m(m+1)(2m+1)/6$ may be proved by induction

$S_{3,m} = \sum i^3 = m^2(m+1)^2/4 = S^2_{1,m}$ may be proved by induction

$S_m = \sum (2i-1)^3 = \sum (8i^3-12i^2+6i-1) = m^2(2m^2-1)$

If $n = 2k+1$ and $m = 2^k$ then $S_m = 2^{2k}(2^{2k+1}-1) = 2^{n-1}(2^n-1) = E_n$ ##
First proved by Heath [c K29 p72]

11.4.9 Mersenne numbers M_p are coprime

Let $b = k_0a + r_1$ with $0 \leq r_1 < a$. We first prove that $q \mid M_a,\ q \mid M_b$ ===> $q \mid M_{r_1}$.

$M_b = M_r + M_a \quad 2^{ai+r}$ ===> $q \mid M_r$ ##

Let $(a, b) = c$ be the GCD of a & b. We prove that $q \mid M_a,\ q \mid M_b$ ===> $q \mid M_c$.

$b = k_0a + r_1$ and $0 < r_1 < a$
$a = k_1r_1 + r_2$ and $0 < r_2 < r_1$
....
$r_i = k_ir_{i+1}$ and $(a, b) = c$ ===> $r_{i+1} = c$

But from the first proof: $q \mid M_a,\ q \mid M_b$ ===> $q \mid M_r$ for $j = 1, \ldots, i+1$
===> $q \mid M_c$ ##

Now we prove that M_{p_1} and M_{p_2} are coprime if p_1 and p_2 are distinct prime indexes.

$(p_1, p_2) = 1$. Thus: $q \mid M_{p_1},\ q \mid M_{p_2}$ ===> $q \mid M_1$ ===> $q = 1$ ##

11.4.10 $(2^n+1)/3$ prime, n odd ===> n prime

This is relevant in the context of unresolved conjecture 11 [B35, N10].
We will prove by induction on 'a' that $2^b+1 \mid 2^{ab}+1$. This is clearly true for a = 1.
$2^{ab}+1 = (2^b+1) * (2^{(a-1)b}-2^{(a-2)b}) + (2^{(a-2)b}+1)$
Therefore $2^b+1 \mid 2^{(a-2)b}+1$ ===> $2^b+1 \mid 2^{ab}+1$.
Therefore, odd n = ab composite, a & b > 1 ===> $2^a+1 \mid 2^n+1$ and $2^b+1 \mid 2^n+1$.
Note that this proof applies for b = 1. Therefore, $2^1+1 = 3 \mid 2^n+1$ for all odd n.
Therefore $(2^n+1)/3$ prime ===> n prime ##

12 COMPUTATIONAL DETAILS

12.1 LLT Modulus-checks

This section concerns modulus checks in Lucas-Lehmer-Test computations. These show the efforts made to ensure the correctness of NZLRs which are not self-evidently correct and the extent to which these efforts succeeded.

12.1.1 Modulus-check(s) included: residues confirmed correct

1926	Lehmer	M_{139}	Mod 10^3+1 [L1; R2; R10; T12]
1927	Lehmer	M_{149}	Mod 10^8+1, 10^9+1 [L2; R2; R10]
1927	Lehmer	M_{257}	Mod 10^8+1, 10^9+1 [L2; R2; R10]
1934	Powers	M_{241}	Mod 9, 10^3+1, 10^4+1, 10^7+1 [P3]
1944	Uhler	M_{157}	Mod 10^3+1, 10^4+1, 10^7+1 [U1; R2]
1946	Uhler	M_{199}	Mod 10^5+1, 10^8+1 [U6; R2; T11]
1947	Uhler	M_{227}	Mod 10^5+1, 10^6+1, 10^8+1 [U7; R2]
1947	Uhler	M_{193}	Mod 10^7+1 [U5; R2; R10; G7; T11]
1953	Wheeler	M_{8191}	Mod $2^{39}-1$ [H2; W7]
1961	Selfridge/Hurwitz	$5000 < p < 6000$	Mod $2^{35}-1$ [G7; H8; S3]
1963	Gillies	$2 < p < 4734$	Mod $2^{44}-1$ [G7; H2; N2; N3; N11]
		$4734 < p < 7000$	" " [G7; H2; H8; K1; N11; S3]
		$7000 < p < 12142$	" " [G7; G1; H2; H8; T1]
1971	Tuckerman	$12142 < p < 21000$	" $2^{24}-1$, $2^{24}-3$ [H8; T1]
1979	Nelson/Slowinski	$4 < p < 32830$	Mod $2^{24}-1$ [N1; N2; N12]
1982	ICL DAP	$18 < p < 50024$	Mod 2^3-1 [H14]

12.1.2 Modulus-check included: residues presumed correct

1982	ICL DAP	$50024 < p < 62982$	Mod 2^3-1 [H14]
1984	ICL DAP	$62982 < p < 100000$	Mod $2^{16}-1$ [H18]

12.1.3 Modulus-check(s) included: residue found incorrect

1945	Barker	$p = 167$	Mod 10^5+1, 10^7+1 [B1; U4]
1963	Gillies	$p = 12143$	Mod $2^{44}-1$ [G1; G7; T2]
1979	Nelson/Slowinski	16 values of p	Mod $2^{24}-1$ [H10; N11; N12; N14] Corrected, 1982 [N14]

12.1.4 Modulus-check not included: residues found correct

1979	Nickel & Noll	$21000 < p < 24500$	[H8; N7]

12.1.5 Modulus-check not included: residues found incorrect

1876	Lucas	M_{89}	[L13 p376; c D1 p22 n115]
1914	Fauquembergue	M_{101} M_{103} M_{109} M_{137}	[F1; F10; F12]
1952	Robinson	M_{1889}	[S3]
1957	Riesel	4 (?) values of p	[R13; S3]
1961	Hurwitz	8 values of p	4 published [G1; G7; H2; S3]
1963	Kravitz/Berg	10 values of p	Corrected before publication [K1] Wrong value of S_1; card-punch error

12.2 Computer Performance

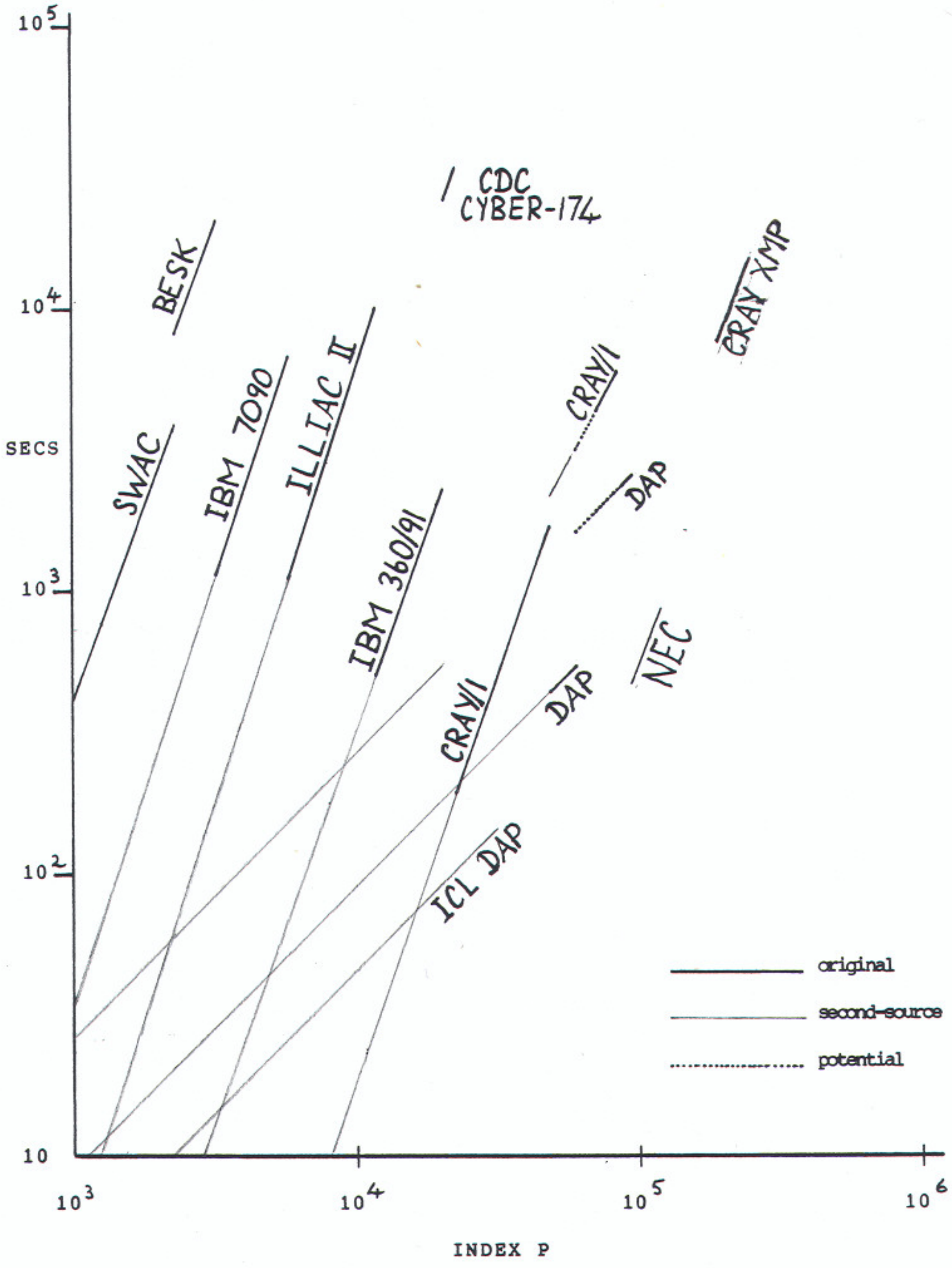
A comparison of one computer code with another cannot necessarily be made given the timings for primality-testing just one M_p. For example, the practice of comparing codes on the number M_{8191} is now out of date. Different codes for the same algorithm have different break-points at which new efficiencies or inefficiencies are introduced. Different algorithms have very different computational characteristics.

All Lucas-Lehmer primality-testing was carried out until 1981 using 'schoolboy' multiplication which gives an $O(p^3)$ algorithm for the LLT. The parallel lines on the following graph have a slope of about 3 and suggest this. Since 1981, new codes have been run using more efficient multiplication algorithms. Slowinski on the CRAY/1 used the 'divide-and-conquer' idea. Holmes et al on the ICL DAP used the Fast-Fermat transform idea which made the LLT linear over finite ranges and asymptotically $O(p^2 \log_e p)$.

Some miscellaneous details on computation times:

1)	Lehmer:	60° on M_{139} [L1], 70° on M_{149} [L2] and 700° on M_{257} [R7]
2)	ILLIAC-1:	100° on M_{8191} [W7]
3)	SWAC:	13'25" on M_{1279} [L4], 59' on M_{2203} and 66' on M_{2281} [L5; U10] The profile of $0.25p^3 + 125p^2$ [R2] μsecs for M_p underestimates the actual times but with a least-squares-fit multiplier of 1.0882 gives model times of 1'15" on M_{521}, 1'51" on M_{607}, 13'12" on M_{1279}, 59'29" on M_{2203} and 65'36" on M_{2281} Store-limited SWAC was actually faster than BESK or ILLIAC I.
4)	BESK:	5°30' on M_{3217} [R1]
5)	IBM7090:	50' on M_{4423} [H2] and 5.2° on M_{8191} [G1]
6)	ILLIAC II:	49' on M_{8191}, 1°23' on M_{9689}, 1°30' on M_{9941} and 2°15' on M_{11213} [G1]
7)	IBM 360/91:	3'06" on M_{8191}, 7'04" on M_{11213} and 35'01" on M_{19937} [T1]
8)	CYBER-174:	7°40'20" on M_{21701} and 8°39'37" on M_{23209} [N7]
9)	CRAY-1 '79:	0.179" on M_{1279}, 1.054" on M_{3217}, 23" on M_{11213}, 1'53" on M_{19937}, 2'52.766" on M_{23209}, 18'39.579" on M_{44497}, 2°9'36" on M_{86243} and by extrapolation 7°37'43" on M_{132049}. A model of this computation which fits closely on large p is: $T = a_1cw^2 + a_2cwv + a_4cw + a_6c + a_7$ seconds M_p is stored in 'v' vectors of 128 words or 'w' words holding 24 bits each. $c = p-2$ cycles. Possible a_3cv^2 and a_5cv terms were set to zero by the model: $a_1 = 0.661889 * 10^{-8}$, $a_2 = 0.113741 * 10^{-7}$, $a_4 = 0.101383 * 10^{-5}$, $a_6 = 0.166363 * 10^{-3}$, $a_7 = 0.210205$
10)	ICL DAP:	Code A - 2'22" on M_{31487}; Code B - 9'22" on M_{62929}; Code C - 38'38" on M_{86243} [H14; H15]
11)	CRAY-1 '82:	1°36'22" on M_{86243} [N23] and 2°32'18" on M_{89137} [N21]
12)	CYBER-205:	1° on M_{86243} [N24]
13)	CRAY-XMP '83:	32'30" on M_{132049} [D4; N25] (M_{132049} confirmed prime in 3°5'10" by CRAY-XMP '79 code [N26])
14)	CRAY-XMP '85:	3° on M_{216091} [D6]
15)	NEC SX-2 '88:	7.5091" on M_{11213}, 3'13.61" on M_{73709}, 9'7" on M_{100069} and 11'26" on M_{110503} [C32; C33]

Times for ICL DAP and CRAY-XMP are not elapsed times but represent the effective throughput on those processors. The ICL DAP was testing 16 or 32 M_p in parallel and therefore elapsed times were 16 or 32 times longer. The CRAY-XMP '83 code was testing 2 M_p in parallel.



COMPUTER TIMINGS

13 STATUS-QUO AND QUESTIONS

This section defines the current state of the art in primality-testing and factorising the M_p. It also lists some questions raised but not answered by this collection of notes.

13.1 The Status-Quo

1) M_{449} = p7.p13.p22.c95 = smallest unfactorised M_p [B17 Edition 2]
2) M_{523} = c158 = smallest M_p with no known factor [B17]
3) M_{1063} = largest fully-factorised composite M_p [B17]
4) M_{7673} = largest 'probably' fully-factorised M_p [Keller?]
5) M_{50069} = smallest M_p without twin-sourced LR [H15]
6) M_{139273} = first M_p of unknown prime/composite status [C34]
7) M_{216091} = largest known Mersenne prime [D6]
8) $391581.2^{216193}-1$ = p65087 = the largest known non-Mersenne prime [D7]
9) $391581.2^{216193}-1$ = largest known prime [D7]
   p65087 found by Brown, Noll, Parady, Smith, Smith and Zarantonello on 6/8/89 in 33' using an Amdahl 1200E. Confirmed by Cray Research
10) M_p with p = 4k+3 = $39051.2^{6001}-1$ is the largest known composite M_p [Y1]
   q = 2p+1 = $39051.2^{6002}-1$ prime ===> q | M_p by Euler's theorem (Germain, 1987)

11) M_{277}-f_2 = p38 = largest non-algebraic/cofactor M_p-factor found [B17]
12) M_{1063}-f_2 = p311 = largest proper M_p-factor proved prime [B17, Ed 2, Morain]
13) p = prp2298 | M_{7673}: p = largest known 'prp' M_p-factor, found by Keller

14) p = p26 | M_{241}-f_2 - 1: p = largest prime, other than algebraic factors and co-factors, used to create an M_p PPL-pf certificate (Brent, ecm, 1986)
15) M_{349} = smallest M_p lacking a PPL-pf certificate
16) M_{607} = largest prime featuring in an M_p PPL-pf certificate [B23]

13.2 General Primality-testing Progress

A 'probably-prime' test demonstrates that a number is probably prime and is ideally one which no composite number is known to have passed. The "Cunningham Project" [B17, IIIB3a.1] uses one such, the Baillie-PSW test, suggested by Baillie [P27] and published by Pomerance [P26, p1024]. It follows a 'Fermat' sprp(a) test with a 'Lucas' lprp(p, q) test.

A primality test proves that a number is prime; the latest tests are more efficient, rely less on factorisation results and are almost polynomial in complexity. None the less, new algorithms have been needed to test the largest [B17] numbers.

In 1981, some proofs on 70-digit numbers took several hours [B17, Update 1]. In 1984, the advent of codes based on the radically better 'ARPCL' test [A4; B17 Ed 2] enabled 100-digit numbers to be tested in less than a minute and 200-digit numbers to be tested in a reasonable time. In 1988, Morain's implementation of Atkin's elliptic curve primality-test [B17 IVA3c] cleared the last "Cunningham" prp, a prp343.

The "Cunningham Project" [B17] illustrates the impact of new algorithms in converting its Appendix A residue of prpn into pn. Against the dates below and B17 updates, in brackets, are tabulated the smallest prpn and the number of prpn remaining.

8/81	prp73	322	(1.0)	8/84	prp228	24	(1.2)	6/87	prp222	35	(1.5)
10/82	prp54	355	(1.0)	6/85	prp213	31	(1.3)	1/88	prp228	36	(2.1)
7/83	prp51	405	(1.1)	7/86	prp213	36	(1.4)	6/88	------	0	(2.2)

13.3 General Factorisation Progress

Brillhart et al [B6] saw c50s as the largest composite it was feasible to approach in 1975. No computation longer than twenty hours was thought worthwhile.

Around the dates below, the smallest 'cn' relevant to the Cunningham Project [B17] in Wagstaff's files increased to the size shown. This is a measure of progress in general factorisation methods (eg cf-ea & mp-qs) but is to some extent influenced by the priority given to factorising record-breaking rather than 'smallest' cn.

c47	31/ 8/81	c54	8/ 8/83	c72	4/ 8/86	c81	29/ 9/87	c88	27/ 5/89
c48	27/ 3/82	c55	25/10/85	c75	21/11/86	c82	19/11/87	c90	13/ 6/89
c49	26/ 6/82	c60	16/11/85	c76	10/ 2/87	c83	27/ 1/88	c91	
c50	8/ 8/82	c61	29/11/85	c77	22/ 4/87	c84	27/11/88	c92	
c51	10/ 9/82	c64	28/ 1/86	c78	29/ 4/87	c85	25/ 1/89	c93	
c52	14/ 6/83	c70	14/ 5/86	c79	2/ 6/87	c86	17/ 2/89	c94	
c53	1/ 8/83	c71	13/ 6/86	c80	10/ 6/87	c87	23/ 4/89	c95	

If computers double in speed every three years, then the length of numbers which it is feasible to factorise would increase by one decimal digit each year. The 43 digit advance in 8 years indicates greater progress in algorithms and technology.

13.4 Outstanding Questions

Pre-history:

a) Where does the 'prime number' concept surface in Greece, Egypt, China, Pythagoras and Euclid?
b) Can we infer that Euclid knew "M_p not prime ===> E_p not perfect"?
c) M_{11}: did the authors of Codex lat. Monac 14908 record the factors of M_{11}? Curtze [C26] reasonably infers that they knew M_{11} to be composite.
d) Did Euler enumerate M_{251}-f_1 = 503 or check it as a factor?
e) Are there sources for the '*' entries, especially for Sphinx-Oedipe?

Pre-computer:

a) M_{31}: what did Seelhoff actually achieve; cf his incomplete effort on M_{61}? [S14; S15; c D1 p25 n142]
b) M_{61}: what did Seelhoff prove and where did he go wrong? [S12]
c) M_{71}: How did Ramesam factorise this number?
d) M_{73}: How did Poulet factorise this number?
e) M_{113}: how did D H Lehmer check primality of f_5 [L6]?
f) How did Gillies [G6] get his interpretation of Shanks' argument [S2 p192]?

Are the, currently presumed lost, print-outs available for the following NZLRs:

a) M_{67}: Lucas' [L13; L15] and Fauquembergue's [F8; F9]
b) M_{89}: Tarry's result [T4; T5]
c) M_{103} and M_{109}: Powers' NZLRs
d) M_{257}: Kraitchik's NZLR
e) The Lehmer/Robinson SWAC NZLRs
f) The Riesel BESK NZLRs

When were the following results achieved?

a) Wunderlich's M_{173} factorisation
b) Penk's discovery of M_{257}-f_1 and Baillie's discovery of M_{257}-f_2 and M_{257}-f_3

Other:

a) Do the incorrect residues of Hurwitz, Gillies, Noll correspond to interim (or subsequent) residues or to the wrong starting value for S_1?

14 AUTHORS

Adleman, L M
Archibald, R C
Ball, W W R
Barker, C B
Bateman, P T
Beeler, M
Beiler, A H
Berg, M
Bickmore, C E
Bray, H G
Brent, R P
Brillhart, J D
Carmichael, R D
Cataldi, P A
Christie, R W D
Cohen, E L
Cohen, H
Cole, F N
Colquitt, W N
Cunningham, A J C
Curtze, M
Davis, J
Devlin, K
Dickson, L E
Drake, S
Ehrman, J R
Euler, L
Ewing, J
Fauquembergue, E
Fermat, P de
Ferrier, A
Gabard, E
Gardner, M
Gerardin, R A P
Gillies, D B
Golubev, V A
Good, I J
Hall, J A
Hardy, G H
Haworth, G McC
Heath, T L
Holdridge, D
Holmes, S M
Holte, R
Hudelot, J
Hurwitz, A
Isemonger, K R
Johnson, G D
Jones, J P
Judd, J S
Karst, E
Keller, W
Knuth, D E
Kraft, G W
Kraitchik, M B
Kravitz, S
Kronsjo, L I
Lake, T W
Lal, M
Landry, F
Le Lasseur
Legendre, A M
Lehmer, D H
Lehmer, D N
Lenstra H W, Jr.
Lucas, F E A
Macdivitt, A R G
Mason, T E
McDonnell, J
McGrogan, S K
McWhirter, N D
Mersenne, M
Metropolis, N
Miller, G L
Miller, J C P
Morrison, M A
Naur, T
Nelson, H L
Newman, M H A
Nickel, L A
Niewiadomski, R
Noll, C L
Ondrejka, R
Ore, O
Pauli, J W
Pepin, P
Pervouchine, I M
Plana, J
Pocklington, H C
Pollard, J M
Pomerance, C
Poulet, P
Powers, R E
Pratt, V R
Proth, M E
Ramesam, V
Reid, C
Reuschle, K G
Riesel, H
Robinson, R M
Rumely, R S
Scheffler, D
Schinzel, A
Schonfelder, J L
Schroepepel, R C
Seelhoff, P
Selfridge, J L
Servais, C
Shanks, D C
Sierpinski, W
Simmons, G J
Slowinski, D A
Smith, H V
Solovay, R M
Storchi, E
Strassen, V
Suyama, H
Tarry, H
Thomason, J T
Touchard, J
Travers, J
Tuckerman, B
Turing, A M
Uhler, H S
Valentin, G
Wagstaff, S S, Jr.
Warren, Le Roy J
Western, A E
Wheeler, D J
Wilcox, T
Williams, H C
Winsheim, de
Woodall, H J
Wright, E M
Wunderlich, M C
Yates, S

15 REFERENCES INDEXED IN "MATHEMATICAL REVIEWS"

V	ITEM	REF	NOTES
6 p	57	[U1]	Uhler's NZLR for M_{157}
6 p	255	[B1]	Barker's incorrect NZLR for M_{167}
7 p	273	[U4]	Uhler's note on M_{157} and M_{167}
7 p	413	[U8]	Uhler's NZLR for M_{229}
8 p	368	[U6]	Uhler's NZLR for M_{199}
8 p	441	[L6]	Lehmer's factors of $2^n \pm 1$
9 p	410	[U5]	Review of Uhler's work on six M_p with $p < 258$ including M_{193}
9 p	410	[U7]	Uhler's NZLR for M_{227}
10 p	100	[O1]	Ore's book on "Number Theory and its History"
10 p	681	[L43]	Lehmer on the converse of Fermat's 'little' theorem, II
11 p	11	[F2]	Ferrier's note on factors of 2^n+1 and the prime $(2^{92}-1)/17$
13 p	436	[M5]	Miller & Wheeler's large primes including $180(2^{127}-1)^2+1$
14 p	121	[K17]	Kraitchik's review of factorisations of $2^n \pm 1$
14 p	343	[U9]	Uhler's history on the M_p and latest primes
14 p	535	[K7]	Kraitchik's "Introduction a la Theorie des Nombres"
14 p	1063	[T7]	Touchard on prime and perfect numbers
14 p	1063	[W9]	Wright's theorem on the primality of kp^3+1
15 p	199	[U10]	Uhler on the values of the 16th and 17th perfect numbers
15 p	933	[G12]	Gabard's two factorisations including M_{109}
16 p	335	[R2]	Robinson's SWAC computations on M_p and F_n
16 p	447	[U11]	Uhler on the values of the first 17 perfect numbers
16 p	673	[H6]	Hardy & Wright's "Introduction to the Theory of Numbers"
17 p	127	[G4]	Good's conjectures on M_p
17 p	127	[S21]	Storchi's theorems and criteria for M_p factorisation
20 #	832	[R3]	Robinson: some factorisations of $2^n \pm 1$
20 #	4520	[R11]	Robinson: the converse of Fermat's theorem
21 #	28	[G11]	Golubev's review of factorisation theorems with enumeration
21 #	657	[R1]	Riesel's M_p-factors and the prime M_{3217}
22 #	22	[I1]	Isemonger's complete factorisation of $2^{132}+1$
22 #	3093	[S8]	Scheffler & Ondrejka's evaluation of E_{3217}
22 #	7268	[K2]	Karst's M_p-factors for $3000 < p < 3500$
22 #	10949	[K2]	Karst's review of M_p-factors including the range $10^5 < p < 10^8$
23 #	A 832	[B2]	Brillhart and Johnson's M_p-factors: $p < 1200$
23 #	A 833	[K5]	Kravitz' M_p-factors for $10{,}000 < p < 15{,}000$
23 #	A1577	[I2]	Isemonger's complete factorisation of $2^{159}-1$
26 #	3684	[H2]	Hurwitz' LRs for $3000 < p < 5000$ and two prime M_p
26 #	6139	[B9]	Bateman and Horn's heuristic formula for prime distribution
27 #	2462	[R4]	Riesel's M_p-factors: $p < 10^4$, $q < 10^8$
27 #	3609	[S9]	Schinzel's remark on the paper of Bateman and Horn
28 #	1152	[K1]	Kravitz' LRs for $6000 < p < 7000$
28 #	2990	[G1]	Gillies's LRs for $7000 < p < 12124$, three prime M_p and factors
28 #	2991	[S3]	Selfridge and Hurwitz' LRs for $5000 < p < 6000$ and F_n-factors
28 #	2992	[B4]	Brillhart's M_p-factors: $p < 20{,}000$ and $q < 2^{34}$
28 #	3952	[S2]	Shanks' "Solved and Unsolved Problems in Number Theory"
29 #	1169	[K6]	Karst's M_p-factors
29 #	3422	[K24]	Karst's review of search-limits on M_p-divisors
30 #	1106	[K27]	Karst's list of M_p-factors $q = 2Kp+1$ $(K < 10)$ for $p < 15000$

V	ITEM	REF	NOTES
36 #	3717	[S6]	Shanks' analysis of M_p-factor distribution
36 #	6368	[E5]	Ehrman's analysis of M_p-factor distibution
37 #	131	[B5]	Brillart and Selfridge's factors of some M_n
40 #	84	[L9]	Lehmer's review of computers as applied to number theory
41 #	1675	[K28]	Kravitz' study of Lucas-Lehmer-test cycles
42 #	4507	[R6]	Riesel's "En Bok om Primtal"
44 #	3531	[K26]	Knuth's "The Art of Computer Programming, Volume 2"
45 #	166	[T1]	Tuckerman's announcement of the prime M_{19937}
45 #	3314	[P20]	Pollard's algorithm for primality-testing any integer
47 #	3285	[L23]	"Computers in Number Theory " including D H Lehmer article
47 #	4932	[S19]	Shanks' "Class Number, Theory of Factorisation and Genera"
47 #	8407	[S7]	Selfridge & Guy's "Primality testing on small machines"
50 #	4229	[B11]	Rouse Ball's "Mathematical Recreations and Essays", 12th Ed.
50 #	6992	[P22]	Pollard's Monte-Carlo factorisation technique
51 #	8017	[B15]	Brillhart and Morrison's factorisation technique and F_7
52 #	5546	[B6]	Brillhart etc's primality criteria and factorisations of $2^n \pm 1$
53 #	4461	[L44]	Lehmer's corrigenda to MR10#681 [L36; L43]
55 #	2732	[S20]	Solovay and Strassen's fast Monte-Carlo Primality test
56 #	233	[T2]	Tuckerman's corrigendum to MR28#2990 [G1]
57 #	5885	[S22]	Solovay & Strassen's correction to MR55#2732 [S20]
58 #	470a	[M10]	Miller's primality test assuming the Riemann Hypothesis
58 #	10681	[R12]	Riesel's supplement to "En Bok Om Primtal"
58 #	26870	[D2]	Drake's analysis of Mersenne's "rule"
58 #	27706	[L31]	Lehmer on the exploitation of parallelism in number theory
80e:	10003	[S2]	Shanks' "Solved & Unsolved Problems in Number Theory" 2nd Edition
80g:	10013	[S1]	Slowinski's announcement of the prime M_{44497}
80m:	68004	[K15]	Kronsjo's "Algorithms - their complexity and efficiency"
81a:	10020	[J1]	Jones' Diophantine representation of M_p and E_p
81f:	10011	[W10]	Wunderlich's performance analysis of Brillhart's CF-factorisation
81i:	10002	[H6]	Hardy & Wright's "Introduction to the Theory of Numbers" 5th Ed.
81k:	10010	[N7]	Nickel & Noll on the 25th and 26th Mersenne primes
82a:	10007	[B18]	Brent's improved Monte-Carlo factorisation algorithm
82e:	10004	[L46]	Lehmer on Fermat's quotient, base two
83h:	10015	[P24]	Pomerance's review of recent developments in primality-testing
84e:	10006	[A4]	Adleman et al's almost-polynomial primality test
85b:	11117	[K33]	Keller's table of Fermat factors and large $k.2^n+1$ primes
86g:	11078	[C31]	Cohen and Lenstra's practical primality test

16 BIBLIOGRAPHY

The author has not seen those references marked with a '*'.
'Pr Comm' denotes a private communication.

L. M. ADLEMAN

A4 (C Pomerance & R S Rumely): "On distinguishing prime numbers from composite numbers", Annals of Maths. v117 (1983) pp173-206. MR**84**e:10006.

R. C. ARCHIBALD

A1 "Mersenne's Numbers", Scripta Mathematica v3 (1935) pp112-9

A2 RMT 434[F] - Review of [L6]: MTAC v2 (1946-7) p341

A3 Review Note 98 - "Mersenne's Numbers", MTAC v3 (1948-9) p398

W. W. R. BALL

B10 "A Short Account of the History of Mathematics" 3rd Ed. (1901) Macmillan

B11 "Mathematical Recreations and Essays" 5th Ed. (1911) p336. (18th Ed. MR**50**#4229.)

B8 "Mersenne's Numbers", Nature v89 (1912) p86

C. B. BARKER

B1 "Proof that the Mersenne Number M_{167} is Composite", BAMS v51 (1945) p389. MR**6**p255. In error, see [R2; T11].

P. T. BATEMAN & R. A. HORN

B9 (& R A Horn): "A Heuristic Asymptotic Formula concerning the Distribution of Prime Numbers", MC v16 (1962) pp363-7. MR**26**#6139.

B35 (J L Selfridge & S S Wagstaff Jr): "The Editor's Corner: The New Mersenne Conjecture", Amer. Math. Monthly 96 (1989) pp125-8

M. BEELER, R. W. GOSPER & R. SCHROEPEPEL

B7 "HAKMEM", MIT Artificial Intelligence Lab. Memo. 239 (1972), p13

A. H. BEILER

B21 "Recreations in the Theory of Numbers - the Queen of Mathematics Entertains", Dover (1964)

M. BERG

B14 Pr Comm: (20/10/1980)

C. E. BICKMORE

B12 "On the Numerical Factors of a^n-1", Messenger of Mathematics v25 (1895-6) pp1-44, esp. p19

B13 "On the Numerical Factors of a^n-1", Messenger of Mathematics v26 (1896-7) pp1-38

G. BOWGEN

B32 Pr Comm (21/7/83): 352 M_p-NZLRs for 90534 < p < 100184

B33 Pr Comm (20/10/83): 397 M_p-NZLRs for 63376 < p < 73180

B34 Pr Comm (16/11/83): 13 M_p-NZLRs for 62982 < p < 63376

R. P. BRENT

B18 "An Improved Monte Carlo Factorization Algorithm", BIT v20 (1980) pp176-84. MR**82**a:10007

B23 Pr Comm (9/7/1981): M_p-factors for p < 1000 (updated 1986)

B24 Pr Comm (26/8/1981): M_p-factors including those of M_{229}

B26 "New Factors of Mersenne Numbers", Abstracts of the AMS v2 no3 (1981) p367, 81T-10-246

B27 Pr Comm (22/9/1981): M_{229}'s factorisation

B28 "New Factors of Mersenne Numbers, II", Abstracts of the AMS v3 no1 (1982) p132, 82T-10-34

B29 Pr Comm (11/5/1982): various factorisations

B30 Pr Comm (23/8/1982): full M_{227} factorisation

B31 "New Factors of Mersenne Numbers, III", Abstracts of the AMS v4 no2 (1983) p197, 83T-10-138

J. D. BRILLHART

B2 (& G D Johnson): "On the Factors of Certain Mersenne Numbers", MC v14 (1960) pp365-9. (Corrected in) MR**23**#A832.

B3 "Some Miscellaneous Factorizations", MC v17 (1963) pp447-50

B20 Table Errata for [R4], MC v17 (1963) p486

B4 "On the Factors of Certain Mersenne Numbers, II", MC v18 (1964) pp87-92. MR**28**#2992.

B5 (& J Selfridge): "Some Factorizations of $2^n \pm 1$ and Related Results", MC v21 (1967) pp87-96. MR**37**#131. Corrected [B25].

B25 Corrigenda to [B5], MC v21 (1967) p751

B6 (D H Lehmer & J Selfridge): "New Primality Criteria and Factorizations of $2^m \pm 1$", MC v29 (1975) pp620-47. MR**52**#5546.

B15 (& M A Morrison) "A Method of Factoring and the Factorization of F_7", MC v29 (1975) pp183-205. MR**51**#8017. Corrected MCv35 (1980) p1444, MR**82**b:10009

B16 Pr Comm (16/12/1980): factorisations

B19 Pr Comm (29/1/1981): factorisations

B22 Pr Comm (17/2/1981): M_{223}'s factorisation

B17 (D H Lehmer, J L Selfridge, B Tuckerman & S S Wagstaff): "Factorizations of $b^n \pm 1$; b = 2, 3, 5, 6, 7, 10, 11, 12 up to high powers", Contemporary Mathematics v22, American Mathematical Society, (1st Edition 1983, 2nd Edition 1988), ISBN 0-8218-5078-4.
Updates: 1.1 (20/07/1983), 1.2 (27/08/1984), 1.3 (30/06/1985),
1.4 (3/07/1986), 1.5 (21/06/1987), 2.1 (13/01/1988)
2.2 (23/06/1988), 2.3 (14/07/1989)

R. D. CARMICHAEL

C30 "Multiply Perfect Numbers of Four Different Primes", Annals of Mathematics, s2 v8 (1906-7) pp149-

P. A. CATALDI

C2 "Trattato de Numeri Perfetti", Bologna (1603) esp pp12-22

R. W. D. CHRISTIE

C27* Maths. Questions Educational Times v48 (1888) pp.xxxvi, 183

C28* Maths. Questions Educational Times v49 (1889) p85

E. L. COHEN & D. W. DOWD

C25 Corrigendum to [K8], MC v27 (1973) p453

H. COHEN

C31 (& H W Lenstra Jr): "Primality testing and Jacobi Sums", MC v42 (1984) pp297-330. MR**86**g:11078.

F. N. COLE

C17 "On the Factoring of Large Numbers", BAMS v10 (1903) pp134-7

W. N. COLQUITT

C32 Pr Comm (12/10/88): complete NEC SX-2/400 results for $p < 112000$

C33 Pr Comm (16/11/88): complete NEC SX-2/400 results for $10^5 < p \leq 132049$

C34 Pr Comm (21/08/89): complete NEC SX-2/400 results for $10^5 < p \leq 139267$

A. J. C. CUNNINGHAM

C5 "On Mersenne's Numbers", Report of the BAAS (1894) pp563-4

C3 "Proceedings of 14/3/1895", Proc. London Math. Soc. v26 (1894-5) p261

C6 "On Mersenne's Numbers", Nature v51 (1895) p533

C7 "On Mersenne's Numbers", Report of the BAAS (1895) p614

C24 "On 2 as a 16-ic Residue", Proc. London Math. Soc. v27 (1895) pp85-122

C19 "On Hyper-Even Numbers and on Fermat's Numbers", Proc. London Math. Soc. s2 v5 (1907) pp 237-74 esp p250 & p259

C8 "Note of 30/4/1908 Meeting", Proc. London Math. Soc. s2 v6 (1908-9) p.xxii

C9 Nature v78 (1908) p23

C20 L'Intermediaire d. Math. v16 (1909) p252

C10 "Notes", Nature v81 (1909) p194

C22* Sphinx-Oedipe v4 (1909) pp36-7

C11 "Note of 8/6/1911 Meeting", Proc. London Math. Soc. s2 v9 (1910-1) p.xvi

C4 "On Mersenne's Numbers", Report of the BAAS (1911) p321

C29 Nature v87 (1911) p499

C12 "On Mersenne's Numbers", Proc. London Math. Soc. s2 v10 (1911-2) p.ii

C21* Sphinx-Oedipe v7 (1912) p38

C1 "Mersenne's Numbers", Proc. London Math. Soc. s2 v11 (1912-3) p.xxiv

C13 "On Mersenne's Numbers", Report of the BAAS (1912) pp406-7

C14 Nature v90 (1912) p425

C15 "On Mersenne's Numbers", Proc. London Math. Soc. s2 v12 (1913) p.xxxvi

C18 Proc. 5th International Congress of Mathematicians, Cambridge (1913), Edited by E W Hobson & A E H Love, v1 pp384-6

C23 (Creak & H J Woodall): "Haupt-Exponents, Residue-Indices, Primitive-Roots & Standard Congruences", London (1922) esp pp1-30, 101-131

C16 (& H J Woodall): "Factorisation of $(y^n \mp 1)$. $y = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers (n)", Hodgson, London (1925) 24pp. Authors' copy with addenda & corrigenda in Mathematical Association Library, Leicester University, UK

M. CURTZE

C26 "Mathematisch-historische Miscellen", Bibliotheca Mathematica s2 v9 (1895) pp33-42, esp pp39-42

L. DEMBART

D4 "Scientists Find New High in Prime Numbers Game", Los Angeles Times (23/9/1983) pp 1 & 21.

D5 "Number Feat Aids Security of Computers", Los Angeles Times (16/12/1983) pp 3 & 23.

D6 "Supercomputer comes up with whopping prime number", Los Angeles Times (17/9/1985) pp 3 & 19.

K. DEVLIN

D7 "Playing it by numbers", The (UK) Guardian (12/10/89)

L. E. DICKSON

D1 "History of the Theory of Numbers" (1919) v1, especially ch1

DISCOVER

D3 "Biggest Prime, Largest Pi", Discover (1983) pp92-3

S. DRAKE

D2 "The rule behind Mersenne's Numbers", Physis-Rivista Internazionale Storia Scienza v13 (1971) pp421-4. MR**58**#26870.

J. R. EHRMAN

E9 "Prime divisors of Mersenne numbers", TN-66-40 (1966), Stanford Linear Accelerator Center, Stanford, California

E5 "The Number of Prime Divisors of Certain Mersenne Numbers", MC v21 (1967) pp700-4. MR**36**#6368.

L. EULER

E1 Comm. Acad. Sci. Petropol. v6 (1738) ad annos 1732-3, pp103-7

E3 Opuscula Varii Argumenti v2 Berlin (1750) esp pp25-32

E6 Nouv. Mem. d. l'Acad. d. Sc. de Berlin 1772, 1774; Histoire pp35-6

E8 Corresp. Math. Phys. (ed., Fuss) v1 (1843) pp590-1 & 597-8

E2 Commentationes Arithmeticae Collectae, I, Petropoli (1849) esp pp1-3, 102-9, 584

E4 Opera Omnia s1 v2 (1915) pp1-5, 86-95

E7 Opera Omnia s1 v3 (1917) pp336-7

J. EWING

E10 "$2^{86243}-1$ is prime", Mathematical Intelligencer v5 no1 (1983) p60

E. FAUQUEMBERGUE

F8 Note 266, L'Intermediaire des Math. v1 (1894) p148

F11* Sphinx-Oedipe v7 (1912) pp20-2

F12* Sphinx-Oedipe v8 (1913) p176. In error, see [R2]

F1 * Sphinx-Oedipe v9 (1914) pp85 & 103-5. In error, see [R2]

F9 "Au sujet du nombre $2^{67}-1$", L'Intermediaire des Math. v22 (1915) p105

F6 L'Intermediaire des Math. v24 (1917) p33

F10 Sphinx-Oedipe v15 (1920) pp17-8. In error, see [R2]

P. de FERMAT

F5 Oeuvres de Fermat v2 (1894) pp176, 185, 194, 198-9, 210-1

F7 Oeuvres de Fermat v4 (1912) pp67, 250

A. FERRIER

F2 "Note on the Factors of 2^n+1", MTAC v3 (1948-9) pp496-7. MR**11**p11, 870.

F3 "New Factorizations of $2^n \pm 1$", MTAC v4 (1950) pp55-6 note 110

F4 "Table of Factors of 2^n-1" reviewed as UMT 137[F], MTAC v6 (1952) p39

E. GABARD

G12 "Sur deux factorisations", Mathesis v63 (1954) pp117-9. MR**15**p933.

G13 "Trois factorisations inedites", Mathesis v63 (1954) p285

G2 "Factorization d'un nouveau nombre de Mersenne", Mathesis v68 (1959) p61

M. GARDNER

G16 "A Short Treatise on the Useless Elegance of Perfect Numbers and Amicable Pairs", Scientific American v218 No3 (March 1968) pp121-4 and v218 No4 (April 1968) p120

GENAILLE

G10* Comptes Rendus (1891) ? part 1 p159

R. A. P. GERARDIN

G15 "Erreurs de Mathematiciens", L'Intermediaire des Math. v15 (1908) pp230-1

G3 "Sur une nouvelle machine algebrique", Report of the BAAS (1912) pp405-6

G6 * Sphinx-Oedipe v7 (1912) pp15-6

G14 "Methode Inedite de Recherche des Facteurs des Grands Nombres", Compte Rendu du Congres des Societes Savants (1920) pp53-5

G8 Sphinx-Oedipe v17 (1922) p64

G9 Sphinx-Oedipe v18 (1923) pp17-8

D. B. GILLIES

G5 Science News Letter v83 (11/5/1963) p291

G7 "Three New Mersenne Primes and a Conjecture", Report No. 138 Digital Computer Laboratory, University of Illinois, Urbana, Illinois (1963)

G1 "Three New Mersenne Primes and a Statistical Theory", MC v18 (1964) pp93-7. MR**28**#2990. Corrected [T2]

V. A. GOLUBEV

G11 "Nombres de Mersenne et caracteres du nombre 2", Mathesis v67 (1958) pp257-62. MR**21**#28.

I. J. GOOD

G4 "Conjectures Concerning the Mersenne Numbers", MTAC v9 (1955) pp120-1. MR**17**p127.

J. A. HALL

H22 Pr Comm (12/12/89): computer analysis of M_p-f_1/LR data from [C34; H19]

G. H. HARDY & E. M. WRIGHT

H6 "Introduction to the Theory of Numbers". 3rd Edition, MR**16**p673: 5th Edition, MR**81**i:10002

G. M[c]C. HAWORTH

H4 Pr Comm to R M Robinson (15/9/1980)

H7 Pr Comm to C L Noll (21/10/1980)

H9 Pr Comm to D Shanks (3/8/1981): ICL DAP "Code A" provisional results

H11 Pr Comm to D Shanks (26/1/1982): ICL DAP "Code B" provisional results including some for $50024 < p < 62982$

H15 Pr Comm to D Shanks (31/1/1983): deposition in MC UMT file of ICL DAP results. Twin-sourced for $18 < p < 50024$ and original for $50024 < p < 62982$

H17 Confirmation of Thomason's S_1=3 M_p-NZLRs for p = 67 & 103 (20/10/1984)

H18 "Primality-testing Mersenne Numbers, II", Abstracts of the AMS, v7 no2 (March 1986) pp224-5, 86T-11-57

H19 "Mersenne Numbers; Consolidated Results": all LRs etc ex DAP (1986)

H20 "M_p prime-factorisation certificates": PPL-pf certificates (1986)

T. L. HEATH

H3 "The Thirteen Books of Euclid's Elements" 2nd Ed. (1926) v2 pp421-6

A. HODGES

H21 "The Enigma of Intelligence", Hutchinson (1983) ISBN 0-04-510060-8

S. M. HOLMES

H8 Pr Comm (27/7/1981): ICL DAP "Code A" provisional results

H10 Pr Comm (24/1/1982): ICL DAP "Code B" provisional results

H12 Pr Comm (24/2/1982): ICL DAP "Code A" production results, $p < 31488$

H13 Pr Comm (20/10/1982): ICL DAP "Code B" production results for $31488 < p < 62982$

H14 (D J Hunt, T W Lake, P J Marron, S F Reddaway, N Westbury & G M[c]C Haworth): "Primality-testing Mersenne Numbers", Abstracts of the AMS, v4 no2 (Feb 1983) p196, 83T-10-82

H16 "Variable Precision Arithmetic on DAP", Section3.6 of "DAP in Action" edited by J Howlett, D Parkinson & J Sylwestrowicz, ICL Technical Journal v3 no3 (1983) pp330-44

J. HUDELOT

H5 Sphinx-Oedipe v4 (1909) p16

A. HURWITZ

H1 "Fermat Numbers and Perfect Numbers", Notices of the American Math. Soc. v8 (1961) p601

H2 "New Mersenne Primes", MC v16 (1962) pp249-51. MR**26**#3684. Corrected [G1]

K. R. ISEMONGER

I1 "The Complete Factorization of $2^{132}+1$", MC v14 (1960) pp73-4. MR**22**#22.

I2 "Complete Factorization of $2^{159}-1$", MC v15 (1961) pp295-6. MR**23**#A1577.

J. P. JONES

J1 "Diophantine representation of Mersenne and Fermat Primes", Acta Arithmetica v35 (1979) pp209-21. MR**81**a:10020.

E. KARST

K14* BYU - Applied Number Theory Newsletter (1960) pp3-6

K2 "Faktorenzerlegung Mersennescher Zahlen mittels programmgesteuerter Rechengerate", Numerische Math. v3 (1961) pp79-86. MR**22**#10949.

K4 "New Factors of Mersenne Numbers", MC v15 (1961) p51. MR**22**#7268.

K23 "Some New Divisors of Mersenne Numbers", BIT v2 (1962) p90

K24 "Search Limits on Divisors of Mersenne Numbers", BIT v2 (1962) pp224-7. MR**29**#3422.

K27 "List of all prime divisors $q = 2Kp+1$ of 2^p-1, $K < 10$, $p < 15000$", BIT v3 (1963) pp222-8. MR**30**#1106.

K6 "Some New Divisors of Mersenne Numbers", BIT v4 (1964) pp28-9. MR**29**#1169.

W. KELLER

K30 "Primteiler von Mersenne-Zahlen" (1977). Factors $q < \max(2^{36}, 10^7p)$ of M_p, $p < 10^5$.

K31 Pr Comm (27/11/1981): "New Factors of Mersenne Numbers and Some Related Primes", intended for publication but not published

K33 "Factors of Fermat Numbers and Large Primes of the form $k.2^n+1$", MC v41 (1983) pp661-673. MR**85**b:11117.

D. E. KNUTH

K26 "The Art of Computer Programming", Volume 2 "Seminumerical Algorithms", 2nd Edition, Addison-Wesley (1981 Printing). MR**44**#3531.

G. W. KRAFT

K18* Novi Comm. Ac. Petrop., v3 (1753), ad annos 1750-1

M. B. KRAITCHIK

K16* "Table de la plus grande solution de la Congruence $2^{(p-1)/x} = 1$ mod p pour tous les nombres premiers p inferieurs a 300,000 excepte les cas de x = 1 ou 2", Nancy (1921)

K10 "Théorie des Nombres", Paris (1922) v1, esp pp34-44, 146, 218

K3 "Recherches sur la Theorie des Nombres", Paris (1924) v1, esp pp 20-1, 24, 165, 170, 175

K11 "Théorie des Nombres", Paris (1926) v2, esp p135 & p142

K13 "Nombres Parfaits", L'Echiquier v3 (1927) pp755-6

K32 "Decomposition de $2^n \pm 1$", L'Echiquier v3 (1927) pp756-7

K12 "Recherches sur la Théorie des Nombres", Paris (1929) Tome 2

K25 "Les Grands Nombres Premiers", Mathematica v7 (1933) pp92-4

K20 "Factorizations de $2^n \pm 1$", Sphinx v8 (1938) pp148-150

K17 "On the Factorization of $2^n \pm 1$", Scripta Mathematica v18 (1952) pp39-52. MR**14**p121.

K7 "Introduction à la Theorie des Nombres": Paris 1952, esp pp39-40. MR**14**p535.

K29 "Mathematical Recreations", Allen & Unwin, London (1955)

S. KRAVITZ

K5 "Divisors of Mersenne Numbers 10,000 < p < 15,000", MC v15 (1961) pp292-3. MR**23**#A833.

K1 (& M Berg): "Lucas' Test for Mersenne Numbers, 6000 < p < 7000", MC v18 (1964) pp148-9. MR**28**#1152.

K8 (& J S Madachy): Review of UMT-113[F] "Divisors of Mersenne Numbers, 20,000 < p < 100,000", MC v19 (1965) p686 (Corr. MC v27 (1973) p453)

K9 "Distribution of Mersenne Divisors", MC v20 (1966) pp448-9

K28 "The Lucas-Lehmer test for Mersenne Numbers", Fibonacci Quarterly v8 (1970) pp1-3. MR**41**#1675.

K21 Pr Comm (4/9/1980)

K22 Pr Comm (7/10/1980): the Kravitz/Berg Code

L. I. KRONSJO

K15 "Algorithms - their complexity and efficiency" Wiley (1979) esp Ch. 5 & 6. MR**80m**:68004.

T. W. LAKE

L45 (& S M Holmes) Pr Comm (25/8/81): first factors < 2^{40}; $5*10^4 < p < 10^5$

M. LAL

L12* UMT 20[9] - "Decimal Expansions of Mersenne Primes", MC v22 (1968) p232

F. LANDRY

L20 "Aux Mathematicians de toutes les parties du monde; communications sur la decomposition des nombres en leurs facteurs simples", Paris (1867) p8

L19 "Decomposition des Nombres $2^n \pm 1$ en leurs Facteurs Premiers", Paris (1869) pp6-7

Le LASSEUR De SANZY

L25 Bullettino di Bibliografia e di Storia delle Scienze Matematiche e Fisiche (Boncompagni) v11 (1878) pp788-9

A. M. LEGENDRE

L21 "Essai sur la Théorie des Nombres" 3rd Ed. Paris (1830) v1 pp228-9

D. H. LEHMER

L39 "A Cross-Division Process and its Application to the Extraction of Roots", American Mathematical Monthly v33 (1926) pp198-206

L1 "Note on the Mersenne Number $2^{139}-1$", BAMS v32 (1926) p522

L11 "Tests for primality by the converse of Fermat's theorem", BAMS v33 (1927) pp327-40

L33 "A Further Note on the Converse of Fermat's Theorem", BAMS v34 (1928) pp54-6

L37 "The Mechanical Combination of Linear Forms", Amer. Math. Monthly v35 (1928) pp114-121

L24 "An Extended Theory of Lucas' Functions", Ann. Maths. v31 (1930) pp419-48

L41 "On the Factorization of Lucas' Functions", Tohoku Mathematical Journal v34 (1931) pp1-7

L26 "Sur Le Nombre $2^{257}-1$", Sphinx v1 (1931) pp31-2

L27 "Sur Le Nombre $2^{149}-1$", Sphinx v1 (1931) pp163-5

L2 "Note on Mersenne Numbers", BAMS v38 (1932) pp383-4

L10 "A number theoretic machine", BAMS v38 (1932) p635

L7 "Some New Factorizations of $2^n \pm 1$", BAMS v39 (1933) pp105-8

L28 "A photo-electric number sieve", Amer. Math. Monthly v40 (1933) pp401-6

L22 "A machine for combining sets of linear congruences", Mathematische Annalen v109 (1934) pp661-7

L8 "On Lucas' Test for the Primality of Mersenne's Numbers", J. London Math. Soc. v10 (1935) pp162-5

L36 "On the Converse of Fermat's Theorem", Amer. Math. Monthly v43 (1936) pp347-54

L6 "On the Factors of $2^n \pm 1$", BAMS v53 (1947) pp164-7. MR8p441.

L43 "On the Converse of Fermat's Theorem, II", Amer. Math. Monthly v56 (1949) pp300-9. MR10p681

L3 "Recent Discoveries of Large Primes", MTAC v6 (1952) p61 N131

L4 "A New Mersenne Prime", MTAC v6 (1952) p205

L5 "Two New Mersenne Primes", MTAC v7 (1953) p72

L9 "Computer Technology applied to the Theory of Numbers": MAA Studies in Mathematics v6 (1969) pp117-151, Prentice Hall. MR40#84.

L23 "The economics of Number Theoretic Computation", from "Computers in Number Theory" by A O L Atkin & B J Birch, Academic Press (1971) pp1-9. MR47#3285.

L44 Corrigendum to [L36] & [L43], MC v25 (1971) pp943-4. MR53#4461.

L31 "Exploitation of Parallelism in Number Theoretic and Combinatorial Computation", Proc. 6th Manitoba Conference on Numerical Math. (1976) pp95-111. MR58#27706.

L46 "On Fermat's Quotient, Base Two", MC v36 (1981) pp289-90

D. N. LEHMER

L42 "On the Multiplication of Large Numbers", American Mathematical Monthly v30 (1923) pp67-70

L34 "Hunting big-game in the theory of numbers", Scripta Mathematica v1 (1933) pp229-235

F. E. A. LUCAS

L29* Comptes Rendus v82 (1875) ? p1305

L30* Comptes Rendus v83 (1876) ? p68

L16 "Note sur l'application des series recurrentes a la recherche de la loi de distribution des nombres premiers", Comptes Rendus v82 (1876) pp165-7

L15* "Sur la theorie des nombres premiers", Turin (1876) esp p11

L35 Comptes Rendus de l'Association de Francaise pour l'avancement des sciences, v6 (1877) pp159-67

L17* Bulletino d. Bibliografia e d. Storia (Boncompagni) v10 (1877) pp129-193

L14 "Théorie des Fonctions Numériques Simplement Periodiques", American J. Math. v1 (1878) pp184-240, 289-231

L32 "Theoremes D'Arithmetique", Atti. R. Ac. Sc. Torino v13 (1877-8) pp271-84

L18 Recreations Mathematiques v2 (1883) pp230-5

L38 "Sur Le Neuvieme Nombre Parfait", Mathesis v7 (1887) pp45-6

L40 "Sur Les Nombres Parfaits", Mathesis v10 (1890) pp74-6

L13 "Théorie des Nombres" Paris (1891) v1 p376 & pp424-5

A. R. G. MACDIVITT

M4 "The most recently discovered prime number", Maths. Gaz. v63 (1979) pp268-70

T. E. MASON

M7 BAMS v21 (1914) p68

M8 "Mechanical Device for Testing Mersenne Numbers for Primes", Proc. Indiana Acad. Sci. (1914) p429-31

J. McDONNELL

M1 "On Mersenne's Primes", Proc. London Math. Soc. s2 v12 (1913) p.xvii

S. K. McGROGAN

M12 (& C L Noll): Letter confirming M_{86243} prime, Scientific American v248 no3 (March 1983) p11

N. D. McWHIRTER

M9 The Guinness Book of Records, Editions 12 - 16 (1965 - 1969)

M. MERSENNE

M3 "Cogitata Physico Mathematica", Parisiis (1644) Praefatio Generalis No.19

M6 "Novarum Observationum Physico-Mathematicarum", Tomus III, Parisiis (1647) Cap.21 p182

N. METROPOLIS

M11 (J Howlett & G-C Rota): "A History of Computing in the Twentieth Century", Academic Press (1980)

G. L. MILLER

M10 "Riemann's Hypothesis and Tests for Primality", J. of Computer and System Sciences v13 (1976) pp300-17. MR**58**#470a.

J. C. P. MILLER

M2 (& D J Wheeler): "Large Prime Numbers", Nature v168 (1951) p838

M5 "Large Primes", Eureka No.14 (1951) pp10-11. MR**13**p436.

T. NAUR

N18 "Integer Factorization", DAIMI PB-144, ISSN 0105-8517 (May 1982)

N19 Pr Comm (14/10/1982): review and M_{193} primality-proofs

N20 Pr Comm (27/10/1982): M_{173} and M_{223} proofs

H. L. NELSON

N12 Pr Comm to D C Shanks (7/6/1979): the deposition in the MC UMT file of CRAY/1 results for p < 50024

N1 "Multi-Precise Arithmetic on a Vector Processor, or how we found the 27th Mersenne Prime", IEEE COMPCON Proceedings (San Francisco) (1980) pp265-9

N2 Pr Comm (3/9/1980): residues for p < 4424

N3 Pr Comm (18/9/1980): 10 residues, 4450 < p < 6908

N9 Pr Comm (10/1/1981): Noll's confirmation of M_{44497}

N11 Pr Comm (24/6/1981): residues for 42018 < p < 42350

N13 Pr Comm (24/12/1981): some residues, 24048 < p < 30678

N17 Pr Comm (6/4/1982): M_p-NZLRS for p = 65537, 65539, 131071

N14 Pr Comm (19/4/1982): additions/corrections to [N12]

N15 Pr Comm (4/5/1982): discussion of errors in [N12]

N21 Pr Comm (28/10/1982): Slowinski finds M_{86243} prime

N22 Pr Comm (2/12/1982): CRAY/1 M_{86243} computation details

N23 Pr Comm (21/12/1982): Noll's CYBER-205 confirms M_{86243}

N25 Pr Comm (7/12/1983): Slowinski's M_{132049} computation

N26 Pr Comm (28/3/1984): Nelson's 11/3/1984 'M_{132049} prime' confirmation

M. H. A. NEWMAN

N16 "Some routines involving large integers", Proc. of Cambridge conference on automatic calculating machines (June 22-25, 1949), pp69-70

R. NIEWIADOMSKI

N8 Note 4202, L'Intermediaire des Math. v20 (1913) p78

C. L. NOLL

N6 "Discovering the 26th Mersenne Prime", Dr. Dobb's Journal v4 Iss6 (1979) pp4-5

N5 (& L A Nickel) "The 25th Mersenne Prime", Dr. Dobb's Journal v4 Iss6 (1979) p6

N4 Pr Comm (6/10/1980): residues for 21000 < p < 24500

N7 (& L A Nickel) "The 25th & 26th Mersenne Primes", MC v35 (1980) pp1387-90. MR81k:10010

N10 Pr Comm (10/4/1981): details of his computation

N24 Pr Comm (9/2/1983): details of new FFNT CYBER-205 code

R. ONDREJKA

O2 UMT 37[9] Review - "Mersenne Primes and Perfect Numbers", MC v26 (1972) p807

O. ORE

O1 "Number Theory and its History", McGraw-Hill (1948). MR10p100.

J. W. PAULI

P11* "De numero perfecto", Magister-disputation, Leipzig (1678)

P. PEPIN

P19 "Sur la formule 2^n-1", Comptes Rendus v86 (1878) pp307-10

I. M. PERVOUCHINE

P13* Melanges Math. et Astron. tires du Bull. de l'Acad. d. Sci. de St. Petersbourg v6 (1881-8) p553

P14 "Sur un nouveau nombre premier", Bull. Acad. d. Sc. St. Petersbourg s4 v31 (1887) cols 532-3

P16* "Memoires Russes de L'Academie" (Zapiski Imperatorskoi Akademii) v48

J. PLANA

P12* Memoria della Reale Accadem. della Scienze, Torino s2 v20 (1863) p130

H. C. POCKLINGTON

P17 "The Determination of the Prime or Composite Nature of Large Numbers by Fermat's Theorem", Proc. Cambridge Phil. Soc. v18 (1914-6) pp29-30

J. M. POLLARD

P20 "An Algorithm for Testing the Primality of any Integer", Bull. London Math. Soc. v3 (1971) pp337-40. MR45#3314.

P21 "Theorems on factorization and primality testing", Proc. Camb. Phil. Soc. v76 (1974) pp521-8

P22 "A Monte Carlo Method for Factorization", BIT v15 (1975) pp331-4. MR50#6992.

C. POMERANCE

P24 "Recent Developments in Primality Testing", Mathematical Intelligencer v3 no3 (1981) pp97-105. MR83h:10015.

P25 "The Search for Prime Numbers", Scientific American v247 no6 (Dec. 1982) pp122-130

P26 (Selfridge & Wagstaff) "The Pseudoprimes to 25.10^9" MC v35 (1980) pp1003-1026

P27 "Are there any counterexamples to the Baillie-PSW primality test?", 'Dopo Le Parole' (16/5/1984), edited and available from J K Lenstra, Amsterdam

P. POULET

P7 Sphinx-Oedipe v18 (1923) p64

R. E. POWERS

P15 Note 6, BAMS v18 (1911-2) p162

P9 American Math. Monthly v18 (1911) pp195-7

P8 * Sphinx-Oedipe v8 (1913) pp49-50

P10 "A Mersenne Prime", BAMS v20 (1914) p531

P2 "On Mersenne's Numbers", Proc. London Math. Soc. s2 v13 (1914) p.xxxix

P6 * Sphinx-Oedipe v9 (1914) pp105-8

P1 "Certain Composite Mersenne's Numbers", Proc. London Math. Soc. s2 v15 (1916) p.xxii

P3 "Note on a Mersenne Number", BAMS v40 (1934) p883

P23 "Sur les Nombres de Mersenne", Sphinx (Bruxelles) v5 (1935) pp57-8

V. R. PRATT

P5 "Every Prime has a succinct certificate": SIAM J. of Computing v4 (1975) pp214-220

M. E. PROTH

P18 "Théorèmes sur les nombres premiers", Comptes Rendus Acad. Sci. Paris v87 (1878) p926

V. RAMESAM

R9 "Note on Mersenne's Number $2^{71}-1$", Journal of the Indian Math. Soc. v4 (1912) p56

C. REID

R7 "Perfect Numbers", Scientific American v188 No3 (March 1953) pp84-6

K. G. REUSCHLE

R8 * "Mathematische Abhandlungen, enthaltend neue zahlen-theoretische Tabellen sammt einer dieselben betreffenden Correspondenz mit dem verewigten C. G. J. Jacobi", Stuttgart (1856) 61pp, esp. pp21-2, 42-53

H. RIESEL

R5 "A New Mersenne Prime", MTAC v12 (1958) p60

R1 "Mersenne Numbers", MTAC v12 (1958) pp207-13. MR**21**#657.

R4 "All Factors $q < 10^8$ in all Mersenne Numbers 2^p-1, p Prime $< 10^4$", MC v16 (1962) pp478-482. MR**27**#2462. Corrected MC v17 (1963) p486.

R6 "En Bok om Primtal" Studentlitteratur (1968) esp. pp44-65. MR**42**#4507.

R12 "En Bok om Primtal, Uppdateringar och Korrektioner" (Oct. 1979). MR**58**#10681.

R13 Pr Comm (30/10/1980): details of his computation

R14 Pr Comm (6/12/1980): largest-known composite M_p

R. M. ROBINSON

R2 "Mersenne & Fermat Numbers", PAMS v5 (1954) pp842-6. MR**16**p335.

R3 "Some Factorizations of Numbers of the Form $2^n \pm 1$", MTAC v11 (1957) pp265-8. MR**20**#832.

R11 "The Converse of Fermat's Theorem", Amer. Math. Monthly v64 (1957) pp703-10. MR**20**#4520.

R10 Pr Comm (26/8/1980)

D. SCHEFFLER & R. ONDREJKA

S8 "The Numerical Evaluation of the Eighteenth Perfect Number", MC v14 (1960) pp199-200. MR**22**#3093.

A. SCHINZEL

S9 "A Remark on a paper of Bateman and Horn", MC v17 (1963) pp 445-7. MR**27**#3609.

R. C. SCHROEPEPEL

S28 Pr Comm (6/01/90): earlier date for Brillhart's M_{139} factorisation

J. L. SCHONFELDER & J. T. THOMASON

S18 "Arbitrary Precision Arithmetic in Algol 68", Software - Practice and Experience v9 (1979) pp173-82

SCIENTIFIC AMERICAN

S24 "$2^{19,937}$ is Prime", Science & the Citizen Column, v224 no6 (June 1971) p56

S4 "Onward and Upward", Science & the Citizen Column, v240 no1 (January 1979) p67

S13 Announcement of Primes M_{23209} & M_{44497}, Martin Gardner, v241 no2 (Sept. 1979) p26

P. SEELHOFF

S14 "Ueber die vollkommenen Zahlen, insbesondere uber die bis jetzt zweifelhaften Falle $2^{40}(2^{41}-1)$, $2^{46}(2^{47}-1)$ und $2^{52}(2^{53}-1)$", Archiv fur Math. und Phys. s2 v2 (1885) pp327-9

S12 "Die neunte vollkommene Zahl", Zeitschrift fur Math. und Phys. v31 (1886) pp174-8

S15 "Untersuchung der Zahl $2^{37}-1$", Archiv fur Math. und Phys. s2 v5 (1887) pp221-3

J. L. SELFRIDGE

S5 Errata to [R1] MC v13 (1959) p142

S3 (& A Hurwitz): "Fermat Numbers and Mersenne Numbers", MC v18 (1964) pp146-8. MR**28**#2991.

S7 (& R K Guy): "Primality Testing on Small Machines" - Research Paper No 121 (1971) - Dept. of Mathematics, University of Calgary, Canada. MR**47**#8407.

C. SERVAIS

S16 "Sur les Nombres Parfaits", Mathesis v7 (1887) pp228-30

D. C. SHANKS

S2 "Solved & Unsolved Problems in Number Theory" Volume 1 - Spartan Books (1962); MR**28**#3952. 2nd Edition, Chelsea (1978); MR**80e**:10003. 3rd Edition (1985).

S6 (& S Kravitz): "On the Distribution of Mersenne Divisors", MC v21 (1967) pp97-101. MR**36**#3717.

S19 "Class number, a theory of factorization, and genera", Amer. Maths. Soc. Proc. Sympos. Pure Maths v20 pp415-40, Number Theory Institute (1969). MR**47**#4932.

S23 Pr Comm (28/10/1981): Nelson's results $24000 < p < 31000$

W. SIERPINSKI

S10 "A Selection of Problems in the Theory of Numbers", Pergamon (1964)

S17 "Elementary Theory of Numbers", Hafner (1964)

D. A. SLOWINSKI

S1 "Searching For the 27th Mersenne Prime", J. Recreational Math. v11 (1978-9) pp258-61. MR**80g**:10013.

H. V. SMITH

S11 "The 25th (known) perfect number", Mathematical Gazette v63 (1979) p271

R. M. SOLOVAY & V. STRASSEN

S20 "A Fast Monte-Carlo Test for Primality", SIAM J. Computing, v6 (1977) pp84-5. MR**55**#2732.

S22 Corrigendum to [S20], SIAM J. Computing, v7 (1978) p118. MR**57**#5885.

E. STORCHI

S21 "Alcuni criteri di divisibilita per i numeri di Mersenne e il carattere 6^{co}, 12^{mo}, 24^{mo}, 48^{mo}, dell'intero 2", Bolletino della Unione Matematica Italiana, v10 (1955) pp363-75. MR**17**p127

H. SUYAMA

S25 "Some new factors for numbers of the form $2^n \pm 1$", Abstracts of the AMS v3 no3 (1982) p257, 82T-10-230

S26 "Some new factors for numbers of the form $2^n \pm 1$, II", Abstracts of the AMS v4 no2 (1983) p195, 83T-10-57

S27 "Some new factors for numbers of the form $2^n \pm 1$, III", Abstracts of the AMS v4 no3 (1983) p294, 83T-10-207

H. TARRY

T4 * Sphinx-Oedipe v6 (1911) p192

T5 * Sphinx-Oedipe v7 (1912) p15 (or 17?)

J. T. THOMASON

T10 Pr Comm (1/2/1981): 5 original-M_p factorisations confirmed

T11 Pr Comm (4/2/1981): E_p and decimal/octal residues

T12 Pr Comm (22/6/1981): M_{239}'s factors and Lucas-residues

TIME Magazine

T14 "Cracking a Record Number" v123 no7 (13/2/1984) p54

The TIMES (London)

T8 "Prime Number Record Broken", The TIMES (17/11/78) p9 column 4

T9 "Prime Number", The TIMES (23/11/78) p19 column 4

J. TOUCHARD

T7 "On Prime Numbers & Perfect Numbers", Scripta Mathematica v19 (1953) pp35-9. MR**14**p1063.

J. TRAVERS

T3 "Perfect Numbers", Mathematical Gazette v23 (1939) p302

B. TUCKERMAN

T1 "The 24th Mersenne Prime", Proc. Nat. Acad. Sci. USA v68 (1971) pp2319-20. MR**45**#166.

T2 Corrigendum to [G1], MC v31 (1977) p1051. MR**56**#233.

T6 Pr Comm (28/8/1980): residues for $12142 < p < 21000$

A. M. TURING

T13 "Checking a large routine", Proc. of Cambridge conference on automatic calculating machines (June 22-25, 1949), pp67-8

H. S. UHLER

U2 "A New Result Concerning a Mersenne Number", MTAC v1 (1943-5) p333

U3 "A New Result Concerning a Mersenne Number", MTAC v1 (1943-5) p404

U1 "First Proof that the Mersenne Number M_{157} is Composite", Proc. Nat. Acad. Sci. v30 (1944) pp314-6. MR**6**p57.

U4 "Note on the Mersenne Numbers M_{157} and M_{167}", BAMS v52 (1946) p178. MR**7**p273.

U8 "A New Result Concerning a Mersenne Number", MTAC v2 (1946-7) p94. MR**7**p413.

U6 "On Mersenne's Number M_{199} and Lucas's Sequences", BAMS v53 (1947) pp163-4. MR**8**p368.

U7 "On Mersenne's Number M_{227} and Cognate Data", BAMS v54 (1948) pp378-80. MR**9**p410.

U5 "On all of Mersenne's Numbers Particularly M_{193}", Proc. Nat. Acad. Sci. v34 (1948) p102-3. MR**9**p410.

U9 "A Brief History of the Investigations on Mersenne Numbers and the latest immense primes", Scripta Mathematica v18 (1952) pp122-31. MR**14**p343.

U10 "On the 16th and 17th Perfect Numbers", Scripta Mathematica v19 (1953) pp128-131. MR**15**p199.

U11 "Full Values of the First Seventeen Perfect Numbers", Scripta Mathematica v20 (1954) p240. MR**16**p447.

G. VALENTIN

V1 "Einige Bemerkungen uber vollkommene Zahlen", Archiv. Math. Phys. s2 v4 (1886) pp100-3

S. S. WAGSTAFF, Jr.

W8 Pr Comm (21/1/1981): table of M_p-factors < 2^{35} for 17,000 < p < 50,000

W12 Pr Comm (2/2/1982): "Divisors of Mersenne Numbers"; $2^{31} < M_p - f_1 < 2^{35}$ for 20,000 < p < 10^5

W13 Pr Comm (27/7/1982): M_{193} factorised by two prps

W14 "Divisors of Mersenne Numbers", MC v40 (1983) pp385-97

Le Roy J. WARREN

W11 (& H G Bray): "On the Square-Freeness of Fermat and Mersenne Numbers", Pacific J. of Maths. v22 (1967) pp563-4

A. E. WESTERN

W2 "Some criteria for the residues of 8th & other powers" - Proc. London Math. Soc. s2 (1911) pp244-272

W3 "On Lucas's and Pepin's Tests for the Primeness of Mersenne's Numbers", J. London Math. Soc. v7 (1932) pp130-7

D. J. WHEELER

W7 Pr Comm (6/10/1980): ILLIAC I and M_{8191} Lucas-test

T. WILCOX

W4 Corrigendum to [L3], MC v19 (1965) p175

De WINSHEIM

W5 * Novi Comm. Ac. Petrop. v2 (1751) ad annum 1749, mem., 68-99

H. J. WOODALL

W6 "Note on a Mersenne Number", BAMS v17 (1910-1) p540

W1 "Mersenne's Numbers", Memoirs & Proceedings of the Manchester Literary and Philosophical Society, v56 (1911-12) No 1 pp5-8

E. M. WRIGHT

W9 "The Calculation of Large Primes", The Mathematical Gazette v37 (1953) pp104-6. MR**14**p1063.

M. C. WUNDERLICH

W10 "A running time analysis of Brillhart's continued fraction factoring method", Lecture Notes in Mathematics, 751, Springer (1979), pp328-42. Proc. of Southern Illinois Conference at Carbondale. MR**81**f:10011

S. YATES

Y1 Pr Comm (19/12/88): 876 titanic primes > 10^{999}.

17 KEYWORDS

Adleman, Leonard M
AMS, American Mathematical Society
Archibald, Raymond Clare
Atkin, Oliver L

BAAS, British Association for the
  Advancement of Science
Baillie, Robert: M_{257}-f_2
Ball, Walter William Rouse
BAMS, "Bulletin of the American
  Mathematical Society"
Barker, Charles B
Bateman, Paul Trevier
Beeler, M
Beiler, Albert H
Berg, Murray
Bickmore, C E
BIT, "Nordisk tidskrift for
  Informationsbehandling"
Bowgen, Grant: ICL DAP
Bray, H G
Brent, Richard Peirce
Brillhart, John David

Carmichael, Robert Daniel
Cataldi, Pietro Antonio
  (1550?-1626)
Christie, R W D
Cohen, Edward L
Cohen, H
Cole, Frank Nelson
  (1861-1927)
Colquitt, Walter N
Computer
  AMDAHL 470/V7: qv Williams
  BESK: M_{3217} [R5]
  CDC 6500:
  CDC 7600: M_{257}-f_1
  CDC CYBER-174: M_{21701} & M_{23209}
  CDC CYBER-205: M_{86243} confirmation
  CRAY/1: M_{44497}, M_{86243}
  CRAY/1S: M_{251}
  CRAY-XMP: M_{132049}, M_{216091}
  DEC
  EDSAC:
  EPOC: Extended-Precision Operand Computer
  IBM 360/91: M_{19937} [T1]
  IBM 650
  IBM 701: M_{109}-f_1 & M_{157}-f_1 [R3], [B2]
  IBM 704: M_{101}
  IBM 709
  IBM 7090
  IBM 7094: M_{103} & M_{163}
  ICL 2900 DAP: LR confirmations
  ILLIAC-I: M_{8191}
  ILLIAC-II: M_{9689}, M_{9941} & M_{11213}

Computer (continued):
  MATHILDA
  MU1: [N16]
  MZ-80C: 8-bit micro (Suyama) [B17]
  NEC SX-2/400: M_{110503}
  power: #12
  SWAC: 5 prime M_p
Continued Fraction factorisation method (cf):
  early-abort technique (cf-ea)
  results: M_{137}, M_{139}, M_{149}, M_{191}, M_{193}, M_{223}
Cunningham, Allan Joseph Champneys
  (1842-1928)
  Cunningham Project [B17]
Curtze, Maximilian

Davis, James A: M_{211}, M_{251}
Dickson, Leonard Eugene
  (1874-1954)
Drake, Stillman

ecm: elliptic curve (factorisation) method
EDSAC:
Ehrman, John R
Elliptic Curve factorisation method (ecm)
ENIAC: Electronic Numerical Integrator and Computer
  qv Computer
EPOC: Extended-Precision Operand Computer
Euclid
Euler, Leonhard
  (1707-1783)
  $f_1 = 2p+1$ observation
    M_{131}, M_{179}, M_{191}, M_{239}, M_{251}

Factorisation techniques
  cf: continued fractions
  ecm: elliptic curve
  mp-qs: multiple-polynomial qs
  qs: quadratic sieve
  rho: monte-carlo
  td: trial division

Fast Fermat-Number Transform
Fauquembergue, E
Fermat, Pierre de
  (1601?-1665)
  fermatian
  little theorem
  method of infinite descent
  number theory
Ferrier, A
FFNT, see Fast Fermat-Number Transform
Frenicle de Bessy, Bernhard
  (ca 1602-1675)

Gabard, Emilien
Gardner, Martin
Georgia Cracker, qv EPOC
Gerardin, Robert André Patrice
  (1879-19)

Gerardin, Robert André Patrice
(1879-19)
Gillies, Donald B
Golubev, V A
Good, Irving John

Hall, Jeremy A
Hardy, Godfrey Harold
(1877-1947)
Haworth, Guy M[c]Crossan
Heath, Thomas Little
(1861-1940)
Holdridge, Diane: M_{211}, M_{251}
Holmes, Stephen M
Holte, R
Hudelot, Jules
Hurwitz, Alexander

Isemonger, K R

Johnson, Gerald D
Jones, J P
Judd, J S

Karst, Edgar
Keller, W
Knuth, Donald Ervin
Kraft, George Wolfgang
Kraitchik, Maurice Borisovich
Kravitz, Sidney
Krieger, S I
Kronsjo, Lydia I

Lake, Tom W
Lal, Mohan
Landry, Fortune
Le Lasseur
Legendre, Adrien Marie
(1752-1833)
Lehmer, Derrick Henry
Lehmer, Derrick Norman
(1867-1938)
Lenstra, Hendrik W, Jr.
Lucas, Francois Edouard Anatole
(1842-1891)

Macdivitt, A R G
Machines
see computers
sieves
Mason, Thomas E
MATHILDA, qv Computers
MC, "Mathematics of Computation"
MC UMT, MC Unpublished maths. table
McDonnell, J
McGrogan, Stephen K
McWhirter, Norris D

Metropolis, N
Miller, Gary Lee
Miller, Jeffrey Charles Percy
  (1906-1981)
Monte-Carlo methods
  factorisation
  primality-testing
Morrison, Michael Allan
MR, "Mathematical Reviews"
MTAC, "Mathematical Tables and
  Aids to Computation", now
  "Mathematics of Computation"

Naur, Thorkil
Nelson, Harry L
Newman, M H A
Nickel, Laura Ann
Niewiadomski, R
Noll, Curt Landon
Numerology

Ondrejka, Rudolf
Ore, Oystein

PAMS, Proceedings of the
  American Mathematical Society
Pauli, J W
Penk, Michael: M_{257}-f_1
Pepin, P
Pervouchine, Ivan Mikheevich
Plana, J
Pocklington, H C
Pollard, John M
  p-1 factorisation algorithm
    M_{173}-f_3, M_{191}-f_4, M_{257}-f_2
  rho (Monte-Carlo) factorisation algorithm
    M_{199}-f_1, M_{227}-f_1, M_{229}-f_3, M_{257}-f_1
Pomerance, Carl
Poulet, P
Powers, Ralph Ernest
  (1875-1952)
  biography
Pp: see Pollard's p-1 method
Pratt, Vaughan Ronald
Primality testing
  Fermat's theorem converse
  Monte-Carlo
Proth, M E

Quadratic Sieve method
  multiple-polynomial technique
  results: M_{211}, M_{251}

Ramesam, V
Reid, Constance
Reuschle, K G
rho: Pollard's Monte-Carlo method
  results: M_{199}-f_1, M_{227}-f_1, M_{229}-f_3, M_{257}-f_1
Rickert, Neil W

Ramesam, V
Reid, Constance
Reuschle, K G
rho: Pollard's Monte-Carlo method
  results: M_{199}-f_1, M_{227}-f_1, M_{229}-f_3, M_{257}-f_1
Rickert, Neil W
Riesel, Hans
Robinson, Raphael Mitchel
Rumely, Robert S

Scheffler, D
Schinzel, Andrzej
Schonfelder, J L
Schroepepel, Richard C: see Tuckerman & M_{19937}
Seelhoff, P
Selfridge, John Lewis
Servais, C
Shanks, Daniel Charles
Sierpinski, Waclaw
Sieves
  Bicycle-Chain (1927):
  DLS127 (1965)
  DLS157
  Photoelectric (1932): M_{79}
  'ROM'-based:
  Williams' Shift-register:
Simmons, Gustavus J
Slowinski, David Allen
Smith, H V
Solovay, Robert Martin
Speciner, Michael: see Tuckerman & M_{19937}
Storchi, Edoardo
Strassen, Volker
Suyama, Hiromi
SWAC: Standards Western Automatic Computer
  M_{521}, M_{607}, M_{1279}, M_{2203} & M_{2281} primes

Tarry, H
Thomason, John T
Touchard, Jacques
Travers, J
Tuckerman, Bryant

Uhler, Horace Scudder
UMT, Unpublished Mathematical Table,
  see MC

Valentin, G