

Appendix A

Tables of Fermat Numbers and Their Prime Factors

The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic.

Carl Friedrich Gauss
Disquisitiones arithmeticae, Sec. 329

Fermat Numbers

$F_0 = 3,$
 $F_1 = 5,$
 $F_2 = 17,$
 $F_3 = 257,$
 $F_4 = 65537,$
 $F_5 = 4294967297,$
 $F_6 = 18446744073709551617,$
 $F_7 = 340282366920938463463374607431768211457,$
 $F_8 = 115792089237316195423570985008687907853$
 $269984665640564039457584007913129639937,$
 $F_9 = 134078079299425970995740249982058461274$
 $793658205923933777235614437217640300735$
 $469768018742981669034276900318581864860$
 $50853753882811946569946433649006084097,$
 $F_{10} = 179769313486231590772930519078902473361$
 $797697894230657273430081157732675805500$
 $963132708477322407536021120113879871393$
 $357658789768814416622492847430639474124$
 $377767893424865485276302219601246094119$
 $453082952085005768838150682342462881473$
 $913110540827237163350510684586298239947$
 $245938479716304835356329624224137217.$

The only known Fermat primes are F_0, \dots, F_4 .

Completely Factored Composite Fermat Numbers

<i>m</i>	prime factor	year	discoverer
5	641	1732	Euler
5	6700417	1732	Euler
6	274177	1855	Clausen
6	67280421310721*	1855	Clausen
7	59649589127497217	1970	Morrison, Brillhart
7	5704689200685129054721	1970	Morrison, Brillhart
8	1238926361552897	1980	Brent, Pollard
8	p_{62}^{**}	1980	Brent, Pollard
9	2424833	1903	Western
9	p_{49}	1990	Lenstra, Lenstra, Jr., Manasse, Pollard
9	p_{99}^{***}	1990	Lenstra, Lenstra, Jr., Manasse, Pollard
10	45592577	1953	Selfridge
10	6487031809	1962	Brillhart
10	p_{40}	1995	Brent
10	p_{252}	1995	Brent
11	319489	1899	Cunningham
11	974849	1899	Cunningham
11	167988556341760475137	1988	Brent
11	3560841906445833920513	1988	Brent
11	p_{564}^{****}	1988	Brent

Table A.1. The only known completely factored composite Fermat numbers F_m , $5 \leq m \leq 11$. The primality was proved by * Landry, Le Lasseur, and G  rardin; ** Williams; *** Odlyzko; and **** Morain. The numbers p_j stand for primes with j digits, which are given below:

$$p_{62} = 93461639715357977769163558199606896584051237541638188580280321,$$

$$p_{49} = 7455602825647884208337395736200454918783366342657,$$

$$p_{99} = 74164006262753080152478714190193747405994078109751 \\ 9023905821316144415759504705008092818711693940737,$$

$$p_{40} = 4659775785220018543264560743076778192897,$$

$$\begin{aligned} p_{252} = & 130439874405488189727484768796509903946608530841611892186895295 \\ & 776832416251471863574140227977573104895898783928842923844831149 \\ & 032913798729088601617946094119449010595906710130531906171018354 \\ & 491609619193912488538116080712299672322806217820753127014424577, \end{aligned}$$

$$\begin{aligned} p_{564} = & 17346244717914755543025897086430977837742184472 \\ & 36640846493470190613635791928791088575910383304 \\ & 08837177983810868451546421940712978306134189864 \\ & 28082601454275870858924387368556397311894886939 \\ & 91585455066111474202161325570172605641393943669 \\ & 45793220968665108959685482705388072645828554151 \\ & 93640191246493118254609287981573305779557335850 \\ & 49822792800909428725675915189121186227517143192 \\ & 29788100979251036035496917279912663527358783236 \\ & 64719315477709142774537703829458491891759032511 \\ & 09393813224860442985739716507110592444621775425 \\ & 40706913047034664643603491382441723306598834177. \end{aligned}$$

Composite Fermat Numbers Without Any Known Prime Factor

m	status	year	discoverer
14	composite	1961	Selfridge, Hurwitz
20	composite	1987	Young, Buell
22	composite	1993	Crandall, Doenias, Norrie, Young
24	composite	1999	Crandall, Mayer, Papadopoulos

Table A.2. Fermat numbers that are known to be composite.

Factors of Fermat Numbers

m	prime factor	year	discoverer
12	114689	1877	Lucas, Pervouchine
12	26017793	1903	Western
12	63766529	1903	Western
12	190274191361	1974	Hallyburton, Brillhart
12	1256132134125569	1986	Baillie
13	2710954639361	1974	Hallyburton, Brillhart
13	2663848877152141313	1991	Crandall
13	3603109844542291969	1991	Crandall
13	319546020820551643220672513	1995	Brent
15	1214251009	1925	Kraitichik
15	2327042503868417	1987	Gostin
15	168768817029516972383024127016961	1997	Crandall, Van Halewyn
16	825753601	1953	Selfridge
16	188981757975021318420037633	1996	Crandall, Dilcher
17	31065037602817	1978	Gostin
18	13631489	1903	Western
18	81274690703860512587777	1999	McIntosh, Tardif
19	70525124609	1962	Riesel
19	646730219521	1963	Wrathall
21	4485296422913	1963	Wrathall
23	167772161	1878	Pervouchine
25	25991531462657	1963	Wrathall
25	204393464266227713	1985	Gostin
25	2170072644496392193	1987	McLaughlin
26	76861124116481	1963	Wrathall
27	151413703311361	1963	Wrathall
27	231292694251438081	1985	Gostin
28	1766730974551267606529	1997	Taura
29	2405286912458753	1980	Gostin, McLaughlin
30	640126220763137	1963	Wrathall
30	1095981164658689	1963	Wrathall

Table A.3. Known prime factors of the Fermat numbers F_m , $12 \leq m \leq 30$.

Prime Factors $p = k2^n + 1$ of Fermat Numbers F_m

m	p	k	n
5	641	5	7
5	6700417	52347	7
6	274177	1071	8
6	67280421310721	262814145745	8
7	59649589127497217	116503103764643	9
7	5704689200685129054721	11141971095088142685	9
8	1238926361552897	604944512477	11
8	p_{62}	[59 digits]	11
9	2424833	37	16
9	p_{49}	[46 digits]	11
9	p_{99}	[96 digits]	11
10	45592577	11131	12
10	6487031809	395937	14
10	p_{40}	[37 digits]	12
10	p_{252}	[248 digits]	13
11	319489	39	13
11	974849	119	13
11	167988556341760475137	10253207784531279	14
11	3560841906445833920513	434673084282938711	13
11	p_{564}	[560 digits]	13
12	114689	7	14
12	26017793	397	16
12	63766529	973	16
12	190274191361	11613415	14
12	1256132134125569	76668221077	14
13	2710954639361	41365885	16
13	2663848877152141313	20323554055421	17
13	3603109844542291969	6872386635861	19
13	319546020820551643220672513	609485665932753836099	19
15	1214251009	579	21
15	2327042503868417	17753925353	17
15	168768 ... 016961	1287603889690528658928101555	17

Table A.4. The form $p = k2^n + 1$ of prime factors of the Fermat numbers F_m , $5 \leq m \leq 15$. The primes p_j are listed after Table A.1.

m	p	k	n
16	825753601	1575	19
16	188981757975021318420037633	180227048850079840107	20
17	31065037602817	59251857	19
18	13631489	13	20
18	81274690703860512587777	9688698137266697	23
19	70525124609	33629	21
19	646730219521	308385	21
21	4485296422913	534689	23
23	167772161	5	25
25	25991531462657	48413	29
25	204393464266227713	1522849979	27
25	2170072644496392193	16168301139	27
26	76861124116481	143165	29
27	151413703311361	141015	30
27	231292694251438081	430816215	29
28	1766730974551267606529	25709319373	36
29	2405286912458753	1120049	31
30	640126220763137	149041	32
30	1095981164658689	127589	33

Table A.5. The form $p = k2^n + 1$ of prime factors of the Fermat numbers F_m , $16 \leq m \leq 30$.

Further factors of F_m can be found in [Brillhart, Lehmer, Selfridge, Tuckerman, Wagstaff] and [www1].

Appendix B

Mersenne Numbers

*The numbers $2^n - 1$ are prime for
 $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$
and composite for all other
positive integers $n < 257$.*

Incorrect statement by
Father Marin Mersenne,
from Preface to his *Cogitata*
Physica-Mathematica (1644)

The number $M_p = 2^p - 1$, where p is prime, is called a *Mersenne number*. If $2^p - 1$ itself is prime, then it is called a *Mersenne prime*. Primes of this type were investigated by the French mathematician Marin Mersenne (1588–1648).

Notice that the number $2^{ij} - 1$ for integers $i > 1$ and $j > 1$ can be written as a product of two nontrivial factors:

$$(B.1) \quad 2^{ij} - 1 = (2^i - 1)(2^{i(j-1)} + 2^{i(j-2)} + \cdots + 2^i + 1).$$

This is why we require that the exponent p of the Mersenne number $2^p - 1$ be prime. By a contradiction argument, factorization (B.1) immediately leads to the following theorem, which was already known by Pierre de Fermat (see [Dickson, p. 12], [Mahoney, p. 294]).

Theorem B.1. *If $2^p - 1$ is prime, then so is p .*

We see that the first four prime exponents $p = 2, 3, 5, 7$ yield the primes 3, 7, 31, 127. However, for $p = 11$ the number $2^{11} - 1 = 2047$ is divisible by 23. Hence, the converse of Theorem B.1 does not hold. The foregoing example with $p = 11$ is generalized in Theorem B.4 below.

At the present time, almost 40 Mersenne primes have been discovered, but very little is known about their distribution (some empirical formulae are surveyed, e.g., in [Schroeder]). The number M_p is prime if

$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89,$
107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423,
9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049,
216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, ?, 6972593,

Here the symbol ? indicates that as of 2000 not all lower exponents have been checked, i.e., it was not known whether 6972593 is the next Mersenne prime exponent after 3021377. According to [Kraitchik, 1952], Fermat himself factored $2^p - 1$ for $p = 11, 23, 37$. His results led him to the discovery of Fermat's little theorem.

Let us denote by $M(n)$ the n th Mersenne prime, i.e., $M(1) = 2^2 - 1 = 3$, $M(2) = 2^3 - 1 = 7$, $M(3) = 2^5 - 1 = 31$, $M(4) = 2^7 - 1 = 127$, \dots . In Figure B.1 we observe an interesting pattern in the distribution of the Mersenne primes $M(n)$.

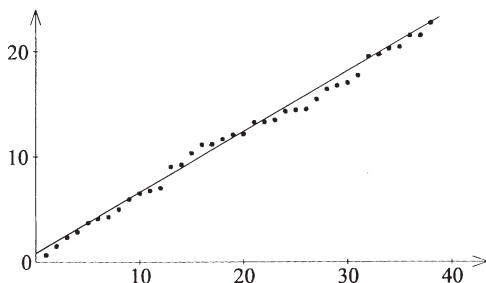


Figure B.1. The values of $\log_2(\log_2 M(n))$ versus n .

The 37th Mersenne prime number $M(37) = 2^{3021377} - 1$ was discovered in 1998. It has more than nine hundred thousand digits. The largest known Mersenne prime, $2^{6972593} - 1$, was discovered in 1999 and has more than two million digits. This is the first known prime with more than one million digits. A table of discoverers of Mersenne primes including the year of the discovery is, e.g., in [Ribenoim, 1996, p. 94] and in [www2].

Theorem B.2 (Lucas–Lehmer Test). *Let $S_1 = 4$ and $S_{k+1} = S_k^2 - 2$ for $k = 1, 2, \dots$. Then, for $p > 2$, the Mersenne number $M_p = 2^p - 1$ is prime if and only if M_p divides S_{p-1} .*

For a proof see [Lehmer, 1930, Theorem 5.4] or [Riesel, 1985, p. 126].

A table of factors of the Mersenne numbers M_p , $p \leq 257$ prime, is contained in [Riesel, 1985]. For more extensive tables see [Brillhart, Lehmer, Selfridge, Tuckerman, Wagstaff]. A general form of possible divisors of Mersenne numbers is given by the following theorem, which was also known by Fermat (see [Dickson, p. 12], [Mahoney, p. 294]).

Theorem B.3. *Let $p > 2$ be a prime. Then all prime divisors of $2^p - 1$ have the form $2kp + 1$.*

P r o o f . Let q be a prime divisor of $2^p - 1$. Then $2^p \equiv 1 \pmod{q}$. Since p is prime and $2^1 \not\equiv 1 \pmod{q}$, we derive that $\text{ord}_q 2 = p$. By Fermat's little theorem (i.e., $2^{q-1} \equiv 1 \pmod{q}$) we get $p \mid q - 1$. Thus there exists j such that $jp = q - 1$. Since p is odd and $q - 1$ is even, $j = 2k$ for some integer k . \square

The following theorem was also suggested by Fermat and later proved by Euler and independently also by Lagrange.

Theorem B.4. *Let p be a prime such that $p \equiv 3 \pmod{4}$. Then $2p + 1 \mid M_p$ if and only if $2p + 1$ is prime.*

For a proof see, e.g., [Ribenoim, 1996, pp. 90–91], [Robbins, p. 149]. Thus if $p = 11, 23, 83, \dots$, then M_p has a factor $23, 47, 167, \dots$ (compare with Remark 5.32 on the Sophie Germain primes).

Theorem B.5. *If $n \mid M_p$ and $p > 2$, then $n \equiv \pm 1 \pmod{8}$.*

For the proof see [Ribenoim, 1991, p. 66].

There is an interesting connection between Mersenne primes and the perfect numbers. Recall that a natural number n is said to be *perfect* if it is equal to the sum of all its divisors less than n . For example, the numbers 6 and 28 are perfect, since $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$. Let n be an arbitrary natural number. Denote by $\sigma(n)$ the sum of all its positive divisors. Then we have an equivalent definition, namely, n is perfect if and only if $\sigma(n) = 2n$. A necessary and sufficient condition for an even number n to be perfect is that it be of the form $n = 2^{p-1}(2^p - 1)$, where $p > 1$ is a natural number and $2^p - 1$ is a prime (i.e., p is also prime). Euclid (4th–3rd century B.C.) already knew that this condition is sufficient, but did not know whether it is also necessary. This question was answered two millennia later by Leonhard Euler (1707–1783), who proved its necessity.

Theorem B.6 (Euclid). *If $2^p - 1$ is prime, then the number $n = 2^{p-1}(2^p - 1)$ is perfect.*

P r o o f . We have

$$\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = \frac{2^p - 1}{2 - 1}(1 + 2^p - 1) = (2^p - 1)2^p = 2n,$$

and thus n is perfect. \square

Theorem B.7 (Euler). *All even perfect numbers are of the form*

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

where $p > 1$ and $2^p - 1$ is a prime.

P r o o f . If n is even, then we can write $n = 2^{p-1}u$, where $p > 1$ and u is odd. Since 2^{p-1} and u are coprime, the sum of the divisors of n is equal to

$$\sigma(n) = \sigma(2^{p-1})\sigma(u) = (2^p - 1)\sigma(u).$$

If n is perfect, we have

$$\sigma(n) = 2n = 2^p u,$$

and thus

$$(2^p - 1)\sigma(u) = 2^p u.$$

Since $2^p - 1$ and 2^p are coprime, we see that $\sigma(u) = 2^p t$ and $u = (2^p - 1)t$, where t is a natural number. However, since u has at least the divisors 1, t , $2^p - 1$, and $t(2^p - 1)$ for $t > 1$, the sum of the divisors of u satisfies the inequality

$$\sigma(u) \geq 1 + t + 2^p - 1 + t(2^p - 1) = 2^p(1 + t),$$

which contradicts $\sigma(u) = 2^p t$. Therefore, $t = 1$. But then $\sigma(u) \geq 1 + 2^p - 1 = 2^p$, and the required equality becomes true only if $2^p - 1$ is a prime. \square

According to Theorems B.6 and B.7, there is another interesting relation between the even perfect numbers n and the Mersenne primes M_p , namely,

$$n = 2^{p-1}(2^p - 1) = \frac{2^p}{2}(2^p - 1) = 1 + 2 + \cdots + (2^p - 1) = \sum_{i=1}^{M_p} i.$$

Theorem B.8. *If you sum the digits of any even perfect number greater than 6, then sum the digits of the resulting number, and repeat this process until you get a single digit, then that digit will be one.*

For the proof see [www2].

The following theorem can be found in [Kraitchik, 1952].

Theorem B.9 (Heath). *Every even perfect number $2^{p-1}(2^p - 1)$ for $p > 2$ is the sum of cubes of $2^{(p-1)/2}$ odd numbers.*

P r o o f . First note that by Theorems B.1 and B.7, p is prime. Let $p > 2$. Setting $k = (p - 1)/2$ and $m = 2^k$, we get

$$\begin{aligned} s &= 1^3 + 3^3 + 5^3 + \cdots + (2m - 1)^3 = \sum_{k=1}^m (2k - 1)^3 = \sum_{k=1}^m (8k^3 - 12k^2 + 6k - 1) \\ &= 8 \frac{m^2(m+1)^2}{4} - 12 \frac{m(m+1)(2m+1)}{6} + 6 \frac{m(m+1)}{2} - m \\ &= m^2(2m^2 - 1). \end{aligned}$$

Now we see that $s = 2^{2k}(2^{2k+1} - 1) = 2^{p-1}(2^p - 1)$. \square

Recall (see Theorem 5.11) that all Mersenne numbers are primes or pseudo-primes, that is,

$$2^{M_p} \equiv 2 \pmod{M_p}.$$

There are many open problems concerning Mersenne numbers. It is conjectured that there are infinitely many Mersenne primes, and thus infinitely many perfect numbers. However, up to now we do not know whether there is an odd perfect number. There are only necessary conditions for such a number to exist. For instance, it has been proved that each odd perfect number is larger than 10^{300} and has at least 8 different prime divisors. We also know that each odd perfect number has the form $12j + 1$ or $36j + 9$ for a suitable integer j .

It has also been conjectured that the prime M_p yields another prime $M_{M_p} = 2^{M_p} - 1$. However, a counterexample was found for $p = 13$, since $M_{13} = 8191$ is prime, whereas $2^{8191} - 1$ is composite (see [Ribenoim, 1987]). Anyway, there is still another unsolved conjecture: whether the sequence $m_{k+1} = 2^{m_k} - 1$ starting from $m_1 = 2$ contains only primes. Indeed, the first five terms $m_1 = 2$, $m_2 = 2^2 - 1 = 3$, $m_3 = 2^3 - 1 = 7$, $m_4 = 2^7 - 1 = 127$, and

$$m_5 = 2^{127} - 1 = 170141183460469231731687303715884105727$$

are the Mersenne primes M_1 , M_2 , M_3 , M_7 , and M_{127} . The character of m_6 is unknown at the present time. However, if m_k were to be composite for some k , then m_{k+1} would also be composite due to (B.1).

Other well-known conjectures include the following: Are there infinitely many composite Mersenne numbers? Is every Mersenne number square-free? (Cf. [Rotkiewicz, 1965] and also later [Warren, Bray].) We know only that if a prime p divides a Mersenne number M_q then

$$p^2 \mid M_q \iff 2^{p-1} \equiv 1 \pmod{p^2} \quad (\text{Wieferich's congruence}).$$

For more information about the Mersenne numbers see, e.g., [Dickson], [Ribenboim, 1996], or [www3]. The Mersenne number transform, which is defined similarly to the Fermat number transform (15.1), is examined, e.g., in [Crandall, Fagin], [Dimitrov, Cooklev, Donevsky], [Elliott, Rao, p. 425], [Gorshkov, 1994b], [Kučera].



Figure B.2. Memorial plaque of Marin Mersenne at his birthplace in Oizé (dépt. Sarthe, formerly dépt. Maine, France).

Appendix C

Remembrance of Pierre de Fermat

*Fermat, l'un des plus beaux génies
qui aient illustré la France.*

1839

CAUCHY

Inscription on the base of Fermat's
statue in Beaumont-de-Lomagne.



Figure C.1. Birthplace of Pierre de Fermat in Beaumont-de-Lomagne.



Figure C.2. Memorial plaque of Pierre de Fermat at his birthplace.



Figure C.3. Statue of Pierre de Fermat in his native Beaumont-de-Lomagne.



Figure C.4. Fermat and a muse in the “Salle des Illustres” in Capitole of Toulouse (see [Hiriart-Urruty, p. 53] for details).



Figure C.5. Bust of Pierre de Fermat in the “Salle Henri-Martin” in Capitole of Toulouse.



Figure C.6. Lycée Pierre de Fermat and Collège Pierre de Fermat in Toulouse.



Figure C.7. Statue of Pierre de Fermat in “Musée des Augustins” in Toulouse.



Figure C.8. Portrait of Pierre de Fermat by Roland Lefèvre in the Narbonne City Museums, France.

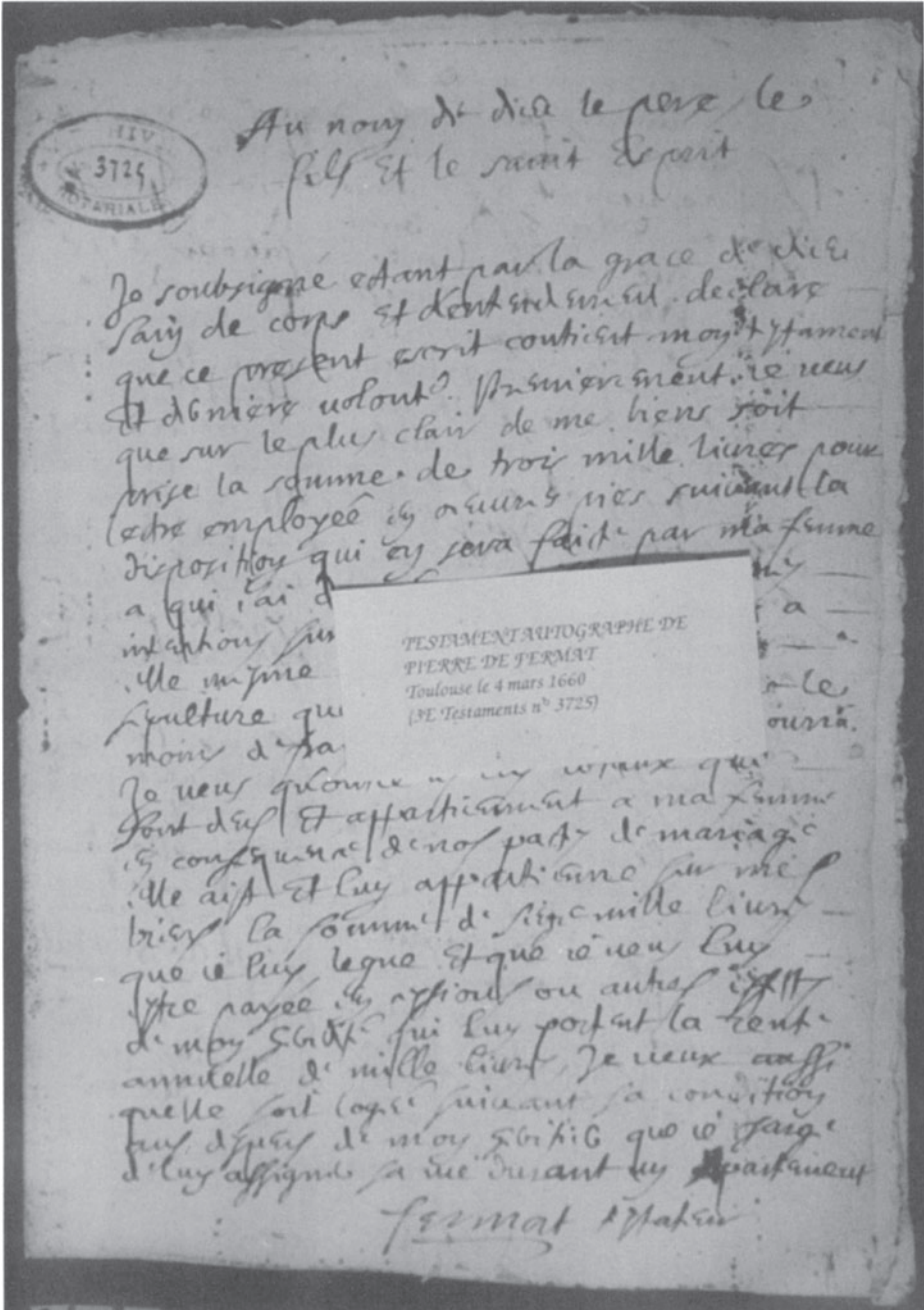


Figure C.9. Fermat's autographical testament (with his signature) saved in the Museum of Pierre de Fermat in Beaumont-de-Lomagne.

References

- Adleman, L. M., Pomerance, C., Rumely, R. S., *On distinguishing prime numbers from composite numbers*, Ann. of Math. (2) **117** (1983), 173–206. MR 84e:10008.
- Agarwal, R. C., Burrus, C. S., *Fast digital convolution using Fermat transforms*, Southwest IEEE Conf. Rec., Houston, Texas, 1973, 538–543.
- Agarwal, R. C., Burrus, C. S., *Fast convolution using Fermat number transforms with applications to digital filtering*, IEEE Trans. Acoust. Speech Signal Processing **22** (1974), 87–97. MR 53 #2501.
- Aigner, A., *On prime numbers for which (almost) all Fermat numbers are quadratic nonresidues (German)*, Monatsh. Math. **101** (1986), 85–93. MR 87g:11010.
- Akushskii, I. Ya., Burtsev, V. M., *Realization of primality tests for Mersenne and Fermat numbers (Russian)*, Vestnik Akad. Nauk Kazakh. SSR (1986), 52–59. MR 87f:11106.
- Alford, W. R., Granville, A., Pomerance, C., *There are infinitely many Carmichael numbers*, Ann. of Math. **140** (1994), 703–722. MR 95k:11114.
- André-Jeannin, R., *Irrationalité de la somme des inverses de certaines suites récurrentes*, C. R. Acad. Sci. Paris Sér. I Math. **308** (1989), 539–541. MR 90b:11012.
- Antonyuk, P. N., Stanyukovich, K. P., *Periodic solutions of the logistic difference equation (Russian)*, Dokl. Akad. Nauk SSSR **313** (1990a), 1033–1036, English translation in Soviet Math. Dokl. **42** (1991), 116–119. MR 92f:39003.
- Antonyuk, P. N., Stanyukovich, K. P., *The logistic difference equation. Period doublings and Fermat numbers (Russian)*, Dokl. Akad. Nauk SSSR **313** (1990b), 1289–1292, English translation in Soviet Math. Dokl. **42** (1991), 138–141. MR 92d:11019.
- Artjuhov, M. M., *Certain criteria for primality of numbers connected with the little Fermat theorem (Russian)*, Acta Arith. **12** (1966/67), 355–364. MR 35 #4153.
- Arya, S. P., *Fermat numbers*, Math. Ed. **6** (1989), 5–6.
- Arya, S. P., *More about Fermat numbers*, Math. Ed. **7** (1990), 139–141.
- Asadulla, S., *A note on Fermat numbers*, J. Natur. Sci. Math. **17** (1977), 113–118. MR 56 #11886.
- Atkin, A. O. L., Morain, F., *Elliptic curves and primality proving*, Math. Comp. **61** (1993), 29–68. MR 93m:11136.
- Atkin, A. O. L., Rickert, N. W., *Some factors of Fermat numbers*, Abstracts Amer. Math. Soc. **1** (1980), 211.
- Badea, C., *The irrationality of certain infinite series*, Glasgow Math. J. **29** (1987), 221–228. MR 88i:11044.

- Baillie, R., *New primes of the form $k2^n + 1$* , Math. Comp. **33** (1979), 1333–1336. MR 80h:10009.
- Baillie, R., Cormack, G., Williams, H. C., *The problem of Sierpiński concerning $k \cdot 2^n + 1$* , Math. Comp. **37** (1981), 229–231. MR 83a:10006a; Corrigenda ibid. **39** (1982), 308. MR 83a:10006b.
- Baker, A., *Linear forms in the logarithms of algebraic numbers*, Mathematika **13** (1966), 204–216. MR 36 #3732.
- Baker, A., *The theory of linear forms in logarithms*, Transcendence Theory: Advances and Applications, Academic Press, London, 1977, 1–27. MR 58 #16543.
- Balasubramanian, R., *Number theory and primality testing.*, Workshop on Mathematics of Computer Algorithms (Madras, 1986), Inst. Math. Sci., Madras, 1986, 1–29. MR 89i:11140.
- Beeger, N. G. W. H., *On even numbers m dividing $2^m - 2$* , Amer. Math. Monthly **58** (1951), 553–555. MR 13,320d.
- Beiler, A. H., *Recreations in the theory of numbers*, Dover Publications, New York, 1964, 1966. Zbl 154.04001.
- Bellon, M. P., Maillard, J.-M., Rollet, G., Viallet, C.-M., *Deformations of dynamics associated to the chiral Potts model*, Internat. J. Modern Phys. **B 6** (1992), 3575–3584. MR 93m:82028.
- Biermann, K.-R., *Thomas Clausen, Mathematiker und Astronom*, J. Reine Angew. Math. **216** (1964), 159–198. MR 29 #2153.
- Birkhoff, G. D., Vandiver, H. S., *On the integral divisors of $a^n - b^n$* , Ann. of Math. (2) **5** (1904), 173–180.
- Björn, A., Riesel, H., *Factors of generalized Fermat numbers*, Math. Comp. **67** (1998), 441–446. MR 98e:11008.
- Borwein, P., *On the irrationality of $\sum 1/(q^n + r)$* , J. Number Theory **37** (1991), 253–259. MR 92b:11046.
- Bosma, W., *Explicit primality criteria for $h2^k + 1$* , Math. Comp. **61** (1993), 97–109, S7–S9. MR 94c:11005.
- Brent, R. P., *Succinct proofs of primality for the factors of some Fermat numbers*, Math. Comp. **38** (1982), 253–255. MR 82k:10002.
- Brent, R. P., *Factorization of the eleventh Fermat number*, Abstracts Amer. Math. Soc. **10** (1989), 176–177.
- Brent, R. P., *Parallel algorithms for integer factorisation*, Number theory and cryptography (Sydney, 1989), London Math. Soc. Lecture Note Ser., 154, Cambridge Univ. Press, Cambridge, 1990, 26–37. MR 91h:11148.
- Brent, R. P., *Factorization of the tenth Fermat number*, Math. Comp. **68** (1999), 429–451. MR 99e:11154.
- Brent, R. P., Crandall, R. E., Dilcher, K., Van Halewyn, C., *Three new factors of Fermat numbers*, Math. Comp. **69** (2000), 1297–1304. MR 2000j:11194.
- Brent, R. P., Pollard, J. M., *Factorization of the eighth Fermat number*, Math. Comp. **36** (1981), 627–630. MR 83h:10014.
- Bressoud, D. M., *Factorization and primality testing*, Springer, New York, 1989. MR 91e:11150.
- Brillhart, J., Lehmer, D. H., Selfridge, J. L., *New primality criteria and factorizations of $2^m \pm 1$* , Math. Comp. **29** (1975), 620–647. MR 52#5546.

- Brillhart, J., Lehmer, D. H., Selfridge, J. L., Tuckerman, B., Wagstaff, S. S., *Factorization of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers*, Contemporary Math. vol. 22, second edition, Amer. Math. Soc., Providence, 1988. MR 90d:11009.
- Brillhart, J., Selfridge, J. L., *Some factorizations of $2^m \pm 1$ and related results*, Math. Comp. **21** (1967), 87–96, 751. MR 37 #131.
- Brun, V., *Ein Satz über Irrationalität*, Arch. for Math. og Naturvideskab (Kristiania) **31** (1910), 3.
- Buchmann, J., Düllmann, S., *A probabilistic class group and regulator algorithm and its implementation*, Computational Number Theory (Debrecen, 1989), de Gruyter, Berlin, 1991, 53–72. MR 92m:11150.
- Buell, D. A., Young, J., *Some large primes and the Sierpiński problem*, SRL Technical Report 88-004, Supercomputing Research Center, Lanham, Maryland, May, 1988.
- Bugeaud, Y., Mignotte, M., *Sur l'équation diophantienne $\frac{x^n-1}{x-1} = y^q$, II*, C. R. Acad. Sci. Paris Sér. I Math. **328** (1999), 741–744.
- Burton, D. M., *Elementary number theory*, fourth edition, McGraw-Hill, New York, 1989, 1998. MR 90e:11001.
- Canals, I., *Fermat numbers and the limitation of computers (Spanish)*, Acta Mexicana Ci. Tecn. **7** (1973), 29–30. MR 51 #8009.
- Carlip, W., Jacobson, E., Somer, L., *Pseudoprimes, perfect numbers, and a problem of Lehmer*, Fibonacci Quart. **36** (1998), 361–371. MR 99g:11013.
- Carmichael, R. D., *Note on a new number theory function*, Bull. Amer. Math. Soc. **16** (1910), 232–238.
- Carmichael, R. D., *On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$* , Amer. Math. Monthly **19** (1912), 22–27.
- Carmichael, R. D., *On the numerical factors of arithmetic forms $\alpha^n \pm \beta^n$* , Ann. of Math. **15** (1913), 30–70.
- Chang, C. C., *An ordered minimal perfect hashing scheme based upon Euler's theorem*, Inform. Sci. **32** (1984), 165–172. MR 85f:68012.
- Cipolla, M., *Sui numeri composti P , che verificano la congruenza di Fermat $a^{P-1} \equiv 1 \pmod{P}$* , Annali di Matematica (3) **9** (1904), 139–160.
- Cohen, H., Lenstra, H. W., *Primality testing and Jacobi sums*, Math. Comp. **42** (1984), 297–330. MR 86g:11078.
- Conway, J. H., Guy, R. K., *The book of numbers*, Springer-Verlag, New York, 1996. MR 98g:00004.
- Conway, J. H., Guy, R. K., Schneeberger, W. A., Sloane, N. J. A., *The primary pretenders*, Acta Arith. **LXXVIII** (1997), 307–313. Zbl 863.11005.
- Cooley, J. W., Tukey, J. W., *An algorithm for the machine calculation of complex Fourier series*, Math. Comp. **19** (1965), 297–301. MR 31#2843.
- Cormack, G. V., Williams, H. C., *Some very large primes of the form $k2^m + 1$* , Math. Comp. **35** (1980), 1419–1421. MR 81i:10011.
- Coxeter, H. S. M., *Introduction to geometry*, second edition, John Wiley & Sons, New York, 1969. MR 49#11369, MR 90a:51001.
- Crandall, R. E., *Topics in advanced scientific computation*, Springer, Berlin, 1996. MR 97g:65005.

- Crandall, R., Dilcher, K., Pomerance, C., *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 433–449. MR 97c:11004.
- Crandall, R., Doenias, J., Norrie, C., Young, J., *The twenty-second Fermat number is composite*, Math. Comp. **64** (1995), 863–868. MR 95f:11104.
- Crandall, R., Fagin, B., *Discrete weighted transforms and large-integer arithmetic*, Math. Comp. **62** (1994), 305–324. MR 94c:11123.
- Crandall, R. E., Mayer, E., Papadopoulos, J., *The twenty-fourth Fermat number is composite*, Math. Comp., submitted, 1999, 1–21.
- Crandall, R. E., Pomerance, C., *Prime numbers. A computational perspective*, Springer, New York, 2001.
- Creutzburg, R., *Application of Fermat-number transform to fast digital correlation*, Proc. of the 4th Internat. Meeting of Young Comput. Scientists, IMYCS '86 (Smolenice Castle, 1986). Tanulmányok—MTA Számítástech. Automat. Kutató Int. Budapest No. 185 (1986), 121–126.
- Creutzburg, R., Grundmann, H.-J., *Schnelle digitale Korrelation von Matrizen mittels Fermattransformation*, Beiträge zur Optik und Quantenphysik **8** (1983a), 126–127.
- Creutzburg, R., Grundmann, H.-J., *The Fermat transform and its application in the fast computation of digital convolutions (German)*, Rostock. Math. Kolloq. No. 24 (1983b), 77–98. MR 85k:94008.
- Creutzburg, R., Grundmann, H.-J., *Fast digital convolution via Fermat number transform (German)*, Elektron. Informationsverarb. Kybernet. **21** (1985), 35–46. MR 87d:94010.
- Creutzburg, R., Tasche, M., *Number-theoretic transformations and primitive roots of unity in a residue class ring modulo m , Parts I, II (German)*, Rostock. Math. Kolloq. No. 25 (1984), 4–22, No. 26 (1984), 103–109. MR 87f:11003a,b.
- Cullen, J., *Question 15897*, Math. Quest. Educ. Times **9** (1905), 534.
- Cunningham, A. J., *Solution of question 15897*, Math. Quest. Educ. Times **10** (1906), 44–47.
- Cunningham, A. J., Western, A. E., *On Fermat's numbers*, Proc. London Math. Soc. **2**(1) (1904), 175.
- Dickson, L. E., *History of the theory of numbers, vol. I, Divisibility and primality*, Carnegie Inst., Washington, 1919.
- Diffie, W., Hellman, M. E., *New directions in cryptography*, IEEE Trans. Inform. Theory **22** (1976), 644–654. MR 55 #10141.
- Dilcher, K., *Fermat numbers, Wieferich and Wilson primes: Computations and generalizations*, Proc. Conf. on Computational Number Theory and Public Key Cryptography (Warsaw, Sept. 2000), 1–22.
- Dimitrov, V. S., Cooklev, T. V., Donevsky, B. D., *Generalized Fermat–Mersenne number theoretic transform*, IEEE Trans. Circuits and Systems II, Analog Digit. Signal Process. **41** (1994), 133–139. Zbl 808.65146.
- Dirichlet, P. G. L., *Beweis des Satzes dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*, Abh. d. Königl. Akad. d. Wiss. (1837), 45–81; reprinted in Werke, vol. 1, 315–350, G. Reimer, Berlin, 1889.

- Dubner, H., *Generalized Fermat primes*, J. Recreational Math. **18** (1985/86), 279–280.
- Dubner, H., Keller, W., *Factors of generalized Fermat numbers*, Math. Comp. **64** (1995), 397–405. MR 95c:11010.
- Dudek, J., *On bisemilattices. III.*, Math. Sem. Notes Kobe Univ. **10** (1982), 275–279. MR 84h:06005.
- Duparc, H. J. A., *On Carmichael numbers, Poulet numbers, Mersenne numbers and Fermat numbers*, Rapport ZW 1953-004, Math. Centrum Amsterdam, 1953, 1–7. MR 15,933j.
- Dyson, F., *The sixth Fermat number and palindromic continued fractions*, Enseign. Math. (2) **46** (2000), 385–389.
- Elliott, D. F., Rao, K. R., *Fast transforms. Algorithms, analyses, applications*, Academic Press, London, 1982. MR 85e:94001.
- Erdős, P., *On arithmetical properties of Lambert series*, J. Indian Math. Soc. (N. S.) **12** (1948), 63–66. MR 10,594c.
- Erdős, P., *On the converse of Fermat's theorem*, Amer. Math. Monthly **56** (1949), 623–624. MR 11,131g.
- Erdős, P., *On almost primes*, Amer. Math. Monthly **57** (1950), 404–407. MR 12,80i.
- Erdős, P., *Some problems and results on the irrationality of the sum of infinite series*, J. Math. Sci. **10** (1975), 1–7. MR 80k:10029.
- Erdős, P., Graham, R. L., *Old and new problems and results in combinatorial number theory*, Université de Genève, L'Enseignement Mathématique, Imprimerie Kunding, 1980. MR 82j:10001.
- Erdős, P., Odlyzko, A. M., *On the density of odd integers of the form $(p-1)2^{-n}$ and related questions*, J. Number Theory **11** (1979), 257–263. MR 80i:10077.
- Erdős, P., Straus, E. G., *On the irrationality of certain Ahmes series*, J. Indian Math. Soc. (N. S.) **27** (1963), 129–133. MR 31#124.
- Euler, L., *Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus*, Comment. Acad. Sci. Petropol. **6**, ad annos 1732-33 (1738), 103–107.
- Euler, L., *Theoremata circa divisores numerorum*, Novi Comment. Acad. Sci. Petropol. **1**, ad annos 1747-48 (1750), 20–48.
- Fehér, J., Kiss, P., *Note on super pseudoprime numbers*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **26** (1983), 157–159. MR 85c:11008.
- Feigenbaum, M. J., *Quantitative universality for a class of nonlinear transformations*, J. Stat. Phys. **19** (1978), 25–52. MR 58#18601.
- Ferentinou-Nicolacopoulou, J., *Une propriété des diviseurs du nombre $r^{r^m} + 1$. Applications au dernier théorème de Fermat*, Bull. Greek Math. Soc. **4** (1963), 121–126. MR 29#68.
- Flammenkamp, A., Luca, F., *Binomial coefficients and Lucas sequences*, J. Number Theory, accepted in 2001, 1–30.
- Gardner, M., *Mathematical carnival: A new round-up of tantalizers and puzzles from Scientific American*, Vintage Books, New York, 1977, 1989. MR 90d:00006.
- Gauss, C. F., *Disquisitiones arithmeticae*, Springer, Berlin, 1986. MR 87f:01105.

- Golomb, S. W., *Sets of primes with intermediate density*, Math. Scand. **3** (1955), 264–274. MR 17,828d.
- Golomb, S. W., *On the sum of the reciprocals of the Fermat numbers and related irrationalities*, Canad. J. Math. **15** (1963), 475–478. MR 27 #105.
- Golomb, S. W., *Properties of the sequence $3 \cdot 2^n + 1$* , Math. Comp. **30** (1976), 657–663. MR 53 #7933, MR 82m:10025.
- Good, I. J., *A reciprocal series of Fibonacci numbers*, Fibonacci Quart. **12** (1974), 346. MR 50#4465.
- Gorshkov, A. S., *Method of fast multiplication modulo Fermat primes (Russian)*, Dokl. Akad. Nauk SSSR **336** (1994a), 175–178, English translation in Soviet Phys. Dokl. **39** (1994a), 314–317. Zbl 939.68963.
- Gorshkov, A. S., *On the method of the number-theoretic Mersenne transform (Russian)*, Dokl. Akad. Nauk **336** (1994b), 33–34, English translation in Phys. Dokl. **39** (1994b), 312–313. MR 95i:11003.
- Gorshkov, A. S., Kravchenko, V. F., *Fermat numbers in digital signal processing (Russian)*, Dokl. Akad. Nauk SSSR **320** (1991), 835–838, English translation in Soviet Phys. Dokl. **36** (1991), 669–671. Zbl 753.94004.
- Gorshkov, A. S., Kravchenko, V. F., Rvachev, V. A., Rvachev, V. L., *On a number-theoretic method for the fast Fourier transform in the Fermat ring (Russian)*, Dokl. Akad. Nauk SSSR **320** (1991), 303–306, English translation in Soviet Phys. Dokl. **36** (1991), 616–618 MR 93g:65171.
- Gostin, G. B., *A factor of F_{17}* , Math. Comp. **35** (1980), 975–976. MR 81f:10010.
- Gostin, G. B., *New factors of Fermat numbers*, Math. Comp. **64** (1995), 393–395. MR 95c:11151.
- Gostin, G. B., McLaughlin, P. B., *Six new factors of Fermat numbers*, Math. Comp. **38** (1982), 645–649. MR 83c:10003.
- Gottlieb, C., *The simple and straightforward construction of the regular 257-gon*, Math. Intelligencer **21** (1999), 31–37. MR 2000c:12006.
- Granville, A., *Primality testing and Carmichael numbers*, Notices Amer. Math. Soc. **39** (1992), 696–700.
- Grytczuk, A., *Some remarks on Fermat numbers*, Discuss. Math. **13** (1993), 69–73. MR 94k:11028.
- Grytczuk, A., Grytczuk, J., *A primality test for Fermat numbers*, Acta Acad. Paedagog. Agriensis, Sect. Mat. **23** (1995), 33–35. Zbl 881.11012.
- Grytczuk, A., Luca, F., Wójtowicz, M., *Another note on the greatest prime factors of Fermat numbers*, Southeast Asian Bull. Math. **25** (2001), 111–115.
- Gulliver, T. A., *Self-reciprocal polynomials and generalized Fermat numbers*, IEEE Trans. Inform. Theory **38** (1992), 1149–1154. MR 93h:11135.
- Gutfreund, H., Little, W. A., *Physicist's proof of Fermat's theorem of primes*, Amer. J. Phys. **50** (1982), 219–220.
- Guy, R. K., *The primes 1093 and 3511*, Math. Student **35** (1967), 205–206. MR 42 #4473.
- Guy, R. K., *The strong law of small numbers*, Amer. Math. Monthly **95** (1988), 697–712. MR 90c:11002.
- Guy, R. K., *The second strong law of small numbers*, Math. Mag. **63** (1990), 3–20. MR 91a:11001.

- Guy, R. K., *Unsolved problems in number theory*, second edition, Springer, Berlin, 1994. MR 96e:11002.
- Hallyburton, J. C., Brillhart, J., *Two new factors of Fermat numbers*, Math. Comp. **29** (1975), 109–112. MR 51 #5460. Corrigenda ibid. **30** (1976), 198. MR 52 #13599.
- Harborth, H., *Ein Primzahlkriterium nach Mann und Shanks*, Arch. Math. (Basel) **27** (1976), 290–294. MR 54 #5099.
- Harborth, H., *Prime number criteria in Pascal's triangle*, J. London Math. Soc. (2) **16** (1977), 184–190. MR 57 #16182.
- Hardy, G. H., Wright, E. M., *An introduction to the theory of numbers*, Clarendon Press, Oxford, 1945, 1954, 1960, 1979. MR 16,673c, MR 81i:10002.
- Hermes, J., *Über die Teilung des Kreises in 65537 gleiche Teile*, Nachr. Königl. Gesellsch. Wissensch. Göttingen, Math.-Phys. Klasse, 1894, 170–186.
- Hewgill, D., *A relationship between Pascal's triangle and Fermat's numbers*, Fibonacci Quart. **15** (1977), 183–184. MR 55 #10275.
- Hilton, P., Pedersen, J., *On folding instructions for products of Fermat numbers*, Southeast Asian Bull. Math. **18** (1994), 19–27. MR 96e:11005.
- Hiriart-Urruty, J.-B., *Historical associations of Fermat in Beaumont and Toulouse, France*, Math. Intelligencer **12** (2) (1990), 52–53. MR 90m:01068.
- Hoggatt, E. V., Bicknell, M., *A reciprocal series of Fibonacci numbers with subscripts 2^nk* , Fibonacci Quart. **14** (1976), 453–455. MR 54#216.
- Hooley, C., *Applications of sieve methods to the theory of numbers*, Cambridge Tracts in Mathematics, No. 70, Cambridge Univ. Press, Cambridge, 1976. MR 53 #7976.
- Huard, J. G., Spearman, B., Williams, K., *Pascal's triangle modulo 8*, European J. Combin. **19** (1998), 45–62. MR 99b:11012.
- Hungerford, T. W., *Algebra. Graduate texts in mathematics*, Vol. 73, Springer-Verlag, 1980. MR 82a:00006.
- Hurwitz, A., Selfridge, J. L., *Fermat numbers and perfect numbers*, Notices Amer. Math. Soc. **8** (1961), 601.
- Inkeri, K., *Tests for primality*, Ann. Acad. Sci. Fenn. Ser. A I No. 279 (1960), 1–19. MR 22 #7984.
- Ireland, K., Rosen, M., *A classical introduction to modern number theory*, second edition, Springer, New York, 1990. MR 92e:11001.
- Jaeschke, G., *Reciprocal hashing: A method for generating perfect hashing functions*, Comm. ACM **24** (1981), 829–833. MR 83f:68013.
- Jaeschke, G., *On the smallest k such that all $k \cdot 2^N + 1$ are composite*, Math. Comp. **40** (1983), 381–384. MR 84k:10006; Corrigendum ibid. **45** (1985), 637. MR 87b:11009.
- Jarden, D., *Existence of an infinitude of composite n for which $2^{n-1} \equiv 1 \pmod{n}$* (Hebrew, Engl. Summary), Riveon Lematematika **4** (1950), 65–67. MR 12,481e.
- Jeans, J. H., *The converse of Fermat's theorem*, Messenger of Mathematics **27** (1897/98), 174.
- Jiang, Z. R., Yu, P. N., *A mixed algorithm for fast polynomial transforms and Fermat number transforms of hyperlarge-scale two-dimensional cyclic convolutions (Chinese)*, Gaoxiao Yingyong Shuxue Xuebao vol 6 (1991), 530–537. MR 92m:65177.

- Jiménez Calvo, I., *A note on factors of generalized Fermat numbers*, Appl. Math. Lett. **13** (2000), 1–5. MR 2001b:11007.
- Jones, R., Pearce, J., *A postmodern view of fractions and the reciprocals of Fermat primes*, Math. Mag. **73** (2000), 83–97.
- Joseph, M., *An afterthought of Gauss on cyclotomy*, Proc. of the 2nd Gauss Symposium. Conference A: Mathematics and Theoretical Physics (Munich, 1993), de Gruyter, Berlin, 1995, 147–150. MR 96e:11003.
- Keller, W., *Factors of Fermat numbers and large primes of the form $k2^n + 1$* , Math. Comp. **41** (1983), 661–673. MR 85b:11117.
- Keller, W., *Whence come the largest presently known primes? (German)*, Mitt. Math. Ges. Hamburg **12** (1991), 211–229. MR 92j:11006.
- Keller, W., *Factors of Fermat numbers and large primes of the form $k \cdot 2^n + 1$, II*, Preprint Univ. of Hamburg, 1992, 1–40.
- Keller, W., *New Cullen primes*, Math. Comp. **64** (1995), 1733–1741. MR 95m:11015.
- Kiss, E., *Notes on János Bolyai's researches in number theory*, Historia Math. **26** (1999), 68–76. MR 2000a:01017.
- Klein, F., *Famous problems of elementary geometry*, Chelsea Publ. Company, New York, 1955. MR 17,445b.
- Knuth, D. E., *The art of computer programming, vol. 2: Seminumerical algorithms*, Addison-Wesley, Reading, Mass., 1969. MR 44 #3531; 1981, MR 83i:68003.
- Koblitz, N., *A course in number theory and cryptography*, second edition, Springer, New York, 1994. MR 88i:94001, MR 95h:94023.
- Koch, M., *Einige Primzahlkriterien im Pascaldreieck*, Ph.D. dissertation, Braunschweig, 1979.
- Korselt, A., *Problème chinois*, L'Interm. des Math. **6** (1899), 143.
- Kraitchik, M., *Théorie des nombres, vol. 2*, Gauthier-Villars, Paris, 1926.
- Kraitchik, M., *On the factorization of $2^n \pm 1$* , Scripta Math. **18** (1952), 39–52. MR 14,121e.
- Krishna, H. V., *On Mersenne and Fermat numbers*, Math. Student **39** (1971), 51–52. MR 48 #5989.
- Křížek, M., *On Fermat numbers (Czech)*, Pokroky Mat. Fyz. Astronom. **40** (1995), 243–253. MR 97b:11005.
- Křížek, M., Chlebout, J., *A note on factorization of the Fermat numbers and their factors of the form $3h2^n + 1$* , Math. Bohem. **119** (1994), 437–445. MR 95k:11006.
- Křížek, M., Chlebout, J., *Is any composite Fermat number divisible by the factor $5h2^n + 1$?*, Tatra Mt. Math. Publ. **11** (1997), 17–21. MR 98j:11003.
- Křížek, M., Křížek, P., *Magic dodecahedron (Czech)*, Rozhledy mat.-fyz. **74** (1997), 234–238.
- Křížek, M., Luca, F., Somer, L., *On the convergence of series of reciprocals of primes related to the Fermat numbers*, J. Number Theory, accepted in 2001.
- Křížek, M., Somer, L., *A necessary and sufficient condition for the primality of Fermat numbers*, Math. Bohem. **126** (2001), 541–549.
- Kučera, R., *Computation of the discrete convolution by means of number theoretic transforms (Czech)*, Elektrotechn. časopis **38** (1987), 50–60.
- Kummer, E. E., *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math. **44** (1852), 93–146.

- Labunets, V. G., *Algebraic theory of signals and systems. Digital processing of signals (Russian)*, Krasnoyarsk. Gos. Univ., Krasnoyarsk, 1984, MR 87c:94003.
- Landry, F., *Sur la décomposition du nombre $2^{64} + 1$* , C. R. Acad. Sci. Paris **91** (1880a), 138.
- Landry, F., *Méthode de décomposition des nombres en facteurs premiers*, Assoc. Française Avance. Sci. Comptes Rendus **9** (1880b), 185–189.
- Larras, J., *Sur la primarité des nombres de Fermat*, C. R. Acad. Sci. Paris Sér. I Math. **242** (1956), 2203–2204. MR 17,1055f.
- Laššák, M., Porubský, Š., *Fermat–Euler theorem in algebraic number fields*, J. Number Theory **60** (1996), 254–290. MR 97f:11086.
- Le, M., *A note on the greatest prime factors of Fermat numbers*, Southeast Asian Bull. Math. **22** (1998), 41–44. MR 2000a:11015.
- Lebesgue, V. A., *Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$* , Nouv. Annal. des Math. **9** (1850), 178–181.
- Lee, Y. C., Min, B. K., Suk, M., *Realization of adaptive digital filtering using the Fermat number transform*, IEEE Trans. Acoust. Speech Signal Processing **33** (1985), 1036–1039.
- Lehmer, D. H., *Tests for primality by the converse of Fermat's theorem*, Bull. Amer. Math. Soc. **33** (1927), 327–340.
- Lehmer, D. H., *An extended theory of Lucas' functions*, Ann. of Math. **31** (1930), 419–448.
- Lehmer, D. H., *On the converse of Fermat's theorem*, Amer. Math. Monthly **43** (1936), 346–354.
- Leibowitz, L. M., *A simplified binary arithmetic for the Fermat number transform*, IEEE Trans. Acoust. Speech Signal Processing **24** (1976), 356–359.
- Lenstra, A. K., Lenstra, H. W. (eds.), *The development of the number field sieve*, Lecture Notes in Math. 1554, Springer, Berlin, 1993. MR 96m:11116.
- Lenstra, A. K., Lenstra, H. W., Jr., Manasse, M. S., Pollard, J. M., *The factorization of the ninth Fermat number*, Math. Comp. **61** (1993), 319–349. MR 93k:11116. Addendum *ibid.* **64** (1995), 1357.
- Lenstra, H. W., *Factoring integers with elliptic curves*, Ann. of Math. **126** (1987), 649–673. MR 89g:11125.
- Lenstra, H. W., Pomerance, C., *A rigorous time bound for factoring integers*, J. Amer. Math. Soc. **5** (1992), 483–516. MR 92m:11145.
- Lepka, K., *History of the Fermat quotients (Czech)*, Prometheus, Prague, 2000.
- LeVeque, W. J., *Fundamentals of number theory*, Dover, Mineola, N.Y., 1996 (reprint of the 1977 original, MR 58 #465). MR 97a:11002.
- Leyendekkers, J. V., Shannon, A. G., *Fermat and Mersenne numbers and some related factors*, Internat. J. Math. Ed. Sci. Tech. **30** (1999), 627–629. MR 2000f:11006.
- Li, L., *A survey of research on prime factorizations and fast primality testing algorithms (Chinese)*, Math. Practice Theory (1989), 83–87. MR 91b:11145.
- Li, W., Peterson, A. M., *FIR filtering by the modified Fermat number transform*, IEEE Trans. Acoust. Speech Signal Processing **38** (1990), 1641–1645. Zbl 707.65108.
- Lidl, R., Niederreiter, H., *Finite fields. Encyclopedia of mathematics and its applications*, Vol. 20, second edition, Cambridge Univ. Press, Cambridge, 1997.

- MR 97i:11115.
- Ligh, S., Jones, P., *Generalized Fermat and Mersenne numbers*, Fibonacci Quart. **20** (1982), 12–16. MR 83f:10015.
- Ligh, S., Neal, L., *A note on Mersenne numbers*, Math. Mag. **47** (1974), 231–233. MR 50 #230.
- Liu, P., *An application of Fermat numbers to group theory (Chinese)*, Xinan Shifan Daxue Xuebao Ziran Kexue Ban **23** (1998), 273–277. MR 2000h:11011.
- Luca, F., *The anti-social Fermat number*, Amer. Math. Monthly **107** (2000a), 171–173. MR 2000k:11015.
- Luca, F., *Equations involving arithmetic functions of Fibonacci and Lucas numbers*, Fibonacci Quart. **38** (2000b), 49–55. MR 2000i:11009.
- Luca, F., *On the equation $\phi(|x^m - y^m|) = 2^n$* , Math. Bohem. **125** (2000c), 465–479.
- Luca, F., *Pascal's triangle and constructible polygons*, Util. Math. **58** (2000d), 209–214.
- Luca, F., *Fermat numbers in the Pascal triangle*, submitted, 2000e.
- Luca, F., *Fermat numbers and Heron triangles with prime power sides*, Amer. Math. Monthly, accepted, 2000f.
- Luca, F., *Multiply perfect numbers in Lucas sequences with odd parameters*, Publ. Math. Debrecen **58** (2001), 121–155.
- Luca, F., Křížek, M., *On the solutions of the congruence $n^2 \equiv 1 \pmod{\phi^2(n)}$* , Proc. Amer. Math. Soc. **129** (2001), 2191–2196.
- Luca, F., Somer, L., *A remark on a question of Rotkiewicz*, Colloq. Math., submitted, 2000, 1–5.
- Lucas, E., *Sur la division de la circonférence en parties égales*, C. R. Acad. Sci. Paris **85** (1877), 136–139.
- Lucas, E., *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France **6** (1877–78), 49–54.
- Lucas, E., *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878a), 184–240, 289–321.
- Lucas, E., *Théorèmes d'arithmétique*, Atti della Reale Accademia delle Scienze di Torino **13** (1878b), 271–284.
- Lucas, E., *Question 453*, Nouv. Corresp. Math. **5** (1879), 137.
- Lucas, E., *Théorie des nombres*, Gauthier-Villars, Paris, 1891; Reprinted by A. Blanchard, Paris, 1961.
- Lucká, M., Creutzburg, R., Grundmann, H.-J., Vajteršić, M., *Parallel SIMD convolution using the Fermat number transform*, ZKI Inf., Akad. Wiss. DDR **2** (1988), 67–86. Zbl 699.10007.
- Lucká, M., Vajteršić, M., Creutzburg, R., Grundmann, H.-J., *Parallel associative fast Fermat number transform implementation*, Comput. Artificial Intelligence **8** (1989), 267–280. Zbl 734.68042.
- Mahler, K., *On the transcendency of the solutions of a special class of functional equations*, Bull. Australian Math. Soc. **13** (1975), 389–410. MR 53#2850.
- Mahnke, D., *Leibniz auf der Suche nach einer allgemeinen Primzahlgleichung*, Bibliotheca Math. **13** (1913), 29–61.
- Mahoney, M. S., *The mathematical career of Pierre de Fermat (1601–1665)*, Princeton Univ. Press, 1973, 1994. MR 58 # 10055, MR 95g:01015.

- Mąkowski, A., *On a problem of Rotkiewicz on pseudoprime numbers*, Elem. Math. **29** (1974), 13. MR 49 #206.
- Malm, D.E.G., *On Monte-Carlo primality tests*, Notices Amer. Math. Soc. **24** (1977), A-529, abstract 77T-A22.
- Malo, E., *Nombres qui sans être premiers, vérifient exceptionnellement une congruence de Fermat*, L'Interm. des Math. **10** (1903), 88.
- Mandelbrot, B., *The fractal geometry of nature*, Freeman, New York, 1977.
- Mann, H.B., Shanks, D., *A necessary and sufficient condition for primality and its source*, J. Combin. Theory Ser. A **13** (1972), 131-134. MR 46 #5225.
- Martziou, J.-C., *The history of Chinese mathematics*, Springer, Berlin, 1997. MR 98a:01005.
- Maruyama, S., Kawatani, T., *On the Fermat numbers (Japanese)*, Res. Rep., Kitakyushu Coll. Technol. **20** (1987), 119-127. Zbl 627.10005.
- McClellan, J.H., *Hardware realization of a Fermat number transform*, IEEE Trans. Acoust. Speech Signal Processing **24** (1976), 216-225.
- McDaniel, W.L., *The gcd in Lucas and Lehmer number sequences*, Fibonacci Quart. **29** (1991), 24-29. MR 91m:11008.
- McIntosh, R., *A necessary and sufficient condition for the primality of Fermat numbers*, Amer. Math. Monthly **90** (1983), 98-99. MR 85c:11022.
- Mignotte, M., *Quelques problèmes d'effectivité en théorie des nombres*, Thesis, Univ. Paris XIII, Paris, 1974.
- Miller, G.L., *Riemann's hypothesis and tests for primality*, J. Comput. System Sci. **13** (1976), 300-317. MR 58 #470a.
- Monier, L., *Evaluation and comparison of two efficient probabilistic primality testing algorithms*, Theor. Comput. Sci. **12** (1980), 97-108. MR 82a:68078.
- Montgomery, P.L., *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** (1987), 243-264. MR 88e:11130.
- Montgomery, P.L., *New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$* , Math. Comp. **61** (1993), 361-363. MR 94d:11003.
- Montgomery, P.L., *A survey of modern integer factorization algorithms*, CWI Quarterly **7** (1994), 337-366. MR 96b:11161.
- Morehead, J.C., *Note on Fermat's numbers*, Bull. Amer. Math. Soc. **11** (1905), 543-545.
- Morehead, J.C., *Note on the factors of Fermat's numbers*, Bull. Amer. Math. Soc. **12** (1906), 449-451.
- Morehead, J.C., Western, A.E., *Note on Fermat's numbers*, Bull. Amer. Math. Soc. **16** (1910), 1-6.
- Morháč, M., *Precise deconvolution using the Fermat number transform*, Comput. Math. Appl. Part A **12** (1986), 319-329. MR 87g:65171.
- Morháč, M., *k-dimensional error-free deconvolution using the Fermat number transform*, Comput. Math. Appl. **18** (1989), 1023-1032. MR 90i:65256.
- Morikawa, Y., Hamada, H., Yamane, N., *Fast Fourier transform algorithm using Fermat number transform*, Systems-Comput.-Controls **13** (1982), 12-21. MR 86b:94005.
- Morimoto, M., *On primes of Fermat type (Japanese)*, Sûgaku **38** (1986), 350-354. MR 88h:11007.

- Morimoto, M., Kida, Y., *Factorization of cyclotomic numbers (Japanese)*, Sophia Kokyuroku in Math. **26** (1987), 1–240. Zbl 632.10001.
- Morrison, M. A., Brillhart, J., *The factorization of F_7* , Bull. Amer. Math. Soc. **77** (1971), 264. MR 42 #3012.
- Morrison, M. A., Brillhart, J., *A method of factoring and the factorization of F_7* , Math. Comp. **29** (1975), 183–205. MR 51 #8017.
- Narkiewicz, W., *The development of prime number theory. From Euclid to Hardy and Littlewood*, Springer, Berlin, 2000. MR 2001c:11098.
- Naur, T., *New integer factorizations*, Math. Comp. **41** (1983), 687–695. MR 85c:11123.
- Niven, I., Zuckerman, H. S., Montgomery, H. L., *An introduction to the theory of numbers*, fifth edition, John Wiley & Sons, New York, 1991. MR 91i:11001.
- Nussbaumer, H. J., *Complex convolutions via Fermat number transforms*, IBM J. Res. Develop. **20** (1976), 282–284. MR 54 #12394.
- Nussbaumer, H. J., *Digital filtering using pseudo Fermat number transforms*, IEEE Trans. Acoust. Speech Signal Process. **25** (1977), 79–83. Zbl 374.94003.
- Nussbaumer, H. J., *Fast Fourier transform and convolution algorithms*, Springer Series in Information Sci. 2, Springer, Berlin, 1981, 1982. MR 83e:65219.
- Papademetrios, I., *Concerning Fermat's numbers and Euclid's perfect numbers (Greek)*, Bull. Soc. Math. Grèce **24** (1949), 103–110. MR 12,243a.
- Paxson, G. A., *The compositeness of the thirteenth Fermat number*, Math. Comp. **15** (1961), 420. MR 23 #A1578.
- Pepin, P., *Sur la formule $2^{2^n} + 1$* , C. R. Acad. Sci. **85** (1877), 329–331.
- Pethe, S., Horadam, A. F., *Generalized Gaussian Lucas primordial functions*, Fibonacci Quart. **26** (1988), 20–30. MR 89m:11018.
- Petr, K., *Geometrical proof of Wilson's theorem (Czech)*, Časopis Pěst. Mat. Fyz. **34** (1905), 164–166.
- Pierpont, J., *On an undemonstrated theorem of the Disquisitiones Arithmeticae*, Bull. Amer. Math. Soc. **2** (1895/96), 77–83.
- Pocklington, H. C., *The determination of the prime or composite nature of large numbers by Fermat's theorem*, Proc. Cambridge Philos. Soc. **18** (1914–1916), 29–30.
- Pollard, J. M., *Theorems on factorization and primality testing*, Math. Proc. Cambridge Philos. Soc. **76** (1974), 521–528. MR 50 #6992.
- Pomerance, C., *On the distribution of pseudoprimes*, Math. Comp. **37** (1981), 587–593. MR 83k:10009.
- Pomerance, C., *A new lower bound for the pseudoprime counting function*, Illinois J. Math. **26** (1982), 4–9. MR 83h:10012.
- Pomerance, C., *Factoring, Cryptology and computational number theory* (Boulder, CO, 1989), Proc. Sympos. Appl. Math., 42, Amer. Math. Soc., Providence, RI, 1990, 27–47. MR 92b:11089.
- Pomerance, C., *A tale of two sieves*, Notices Amer. Math. Soc. **43** (1996), 1473–1485. MR 97f:11100.
- Pomerance, C., Selfridge, J. L., Wagstaff, S. S., *The pseudoprimes to $25 \cdot 10^9$* , Math. Comp. **35** (1980), 1003–1026. MR 82g:10030.
- Poulet, P., *Table des nombres composés vérifiant le théorème de Fermat pour le module 2 jusqu'à 100.000.000*, Sphinx **8** (1938), 42–52. Errata in Math. Comp.

- 25** (1971), 944-945, Math. Comp. **26** (1972), 814. MR 58 #31707.
- Proth, F., *Correspondance*, Nouv. Corresp. Math. **4** (1878a), 210-211.
- Proth, F., *Mémoires présentés*, C. R. Acad. Sci. Paris **87** (1878b), 374.
- Proth, F., *Théorèmes sur les nombres premiers*, C. R. Acad. Sci. Paris **87** (1878c), 926.
- Rabin, M. O., *Probabilistic algorithms for testing primality*, J. Number. Theory **12** (1980), 128-138. MR 81f:10003.
- Raclăuș, N., *Théorème pour les nombres de Fermat*, Bull. École Polytech. Bucarest **14** (1943), 3-9. MR 7,47g.
- Rademacher, H., *Lectures on elementary number theory*, Robert E. Krieger Publ. Company, New York, 1977. MR 58 #10677.
- Radovici-Mărculescu, P., *Diophantine equations without solutions, (Romanian)*, Gaz. Mat. Mat. Inform. **1** (1980), 115-117. MR 83m:10007.
- Reed, I. S., Scholtz, R. A., Truong, T. K., Welch, L. R., *The fast decoding of Reed-Solomon codes using Fermat theoretic transforms and continued fractions*, IEEE Trans. Inform. Theory **24** (1978), 100-106. MR 58#20794.
- Reed, I. S., Truong, T. K., Welch, L. R., *The fast decoding of Reed-Solomon codes using Fermat transforms*, IEEE Trans. Inform. Theory **24** (1978), 497-499. MR 58#20795.
- Reid, C., *From zero to infinity. What makes numbers interesting*, MAA Spectrum. Math. Association of America, Washington, DC, 1992. MR 93g:00006.
- Ribenboim, P., *On the square factors of the numbers of Fermat and Ferentinou-Nicolacopoulou*, Bull. Greek Math. Soc. **20** (1979a), 81-92. MR 83f:10016.
- Ribenboim, P., *13 lectures on Fermat's last theorem*, Springer, New York, 1979b. MR 81f:10023.
- Ribenboim, P., *Prime number records (a new chapter for the Guinness book of records) (Russian)*, Uspekhi Mat. Nauk **42** (1987), 119-176. MR 89c:11181.
- Ribenboim, P., *The book of prime number records*, Springer, New York, 1988, 1989. MR 89e:11052, MR 90g:11127.
- Ribenboim, P., *The little book of big primes*, Springer, Berlin, 1991. MR 92i:11008.
- Ribenboim, P., *Catalan's conjecture. Are 8 and 9 the only consecutive powers?*, Academic Press, London, 1994. MR 95a:11029.
- Ribenboim, P., *The new book of prime number records*, Springer, New York, 1996. MR 96k:11112.
- Richelot, F. J., *De resolutione algebraica aequationis $x^{257} = 1$, sive de divisione circuli per bisectionam anguli septies repetitam in partes 257 inter se aequales commentatio coronata*, Crelle's Journal **IX** (1832), 1-26, 146-161, 209-230, 337-356.
- Richmond, H. W., *A construction for a regular polygon of seventeen sides*, Quart. J. Pure Appl. Math. **26** (1893), 206-207.
- Richmond, H. W., *To construct a regular polygon of 17 sides*, Math. Ann. **67** (1909), 459-461.
- Riesel, H., *A factor of the Fermat number F_{19}* , Math. Comp. **17** (1963), 458. Zbl 115.26204.
- Riesel, H., *Common prime factors of the numbers $A_n = a^{2^n} + 1$* , Nordisk Tidskr. Informationsbehandling (BIT) **9** (1969), 264-269. MR 41 #3381.

- Riesel, H., *Prime numbers and computer methods for factorization*, Birkhäuser, Boston-Basel-Stuttgart, 1985, 1994. MR 88k:11002, MR 95h:11142.
- Riesel, H., Björn, A., *Generalized Fermat numbers*, Mathematics of Computation 1943–1993: a half-century of computational mathematics (Vancouver, BC, 1993), 583–587, Proc. Sympos. Appl. Math., 48 (ed. W. Gautschi), Amer. Math. Soc., Providence, RI, 1994, 583–587. MR 95j:11006.
- Ripley, B. D., *Stochastic simulations*, John Wiley & Sons, New York, 1987. MR 88b:68181.
- Rivest, R. L., Shamir, A., Adleman, L. A., *A method for obtaining digital signatures and public key cryptosystems*, Comm. ACM **21** (1978), 120–126. MR 83m:94003.
- Robbins, N., *Beginning number theory*, Dubuque, IA: Wm. C. Brown Publishers, 1993. Zbl 824.11001.
- Robinson, R. M., *Mersenne and Fermat numbers*, Proc. Amer. Math. Soc. **5** (1954), 842–846. MR 16,335b.
- Robinson, R. M., *Factors of Fermat numbers*, Math. Tables Aids Comput. **11** (1957a), 21–22. MR 19,14d.
- Robinson, R. M., *The converse of Fermat's theorem*, Amer. Math. Monthly **64** (1957b), 703–710. MR 20 #4520.
- Robinson, R. M., *A report on primes of the form $k2^n + 1$ and on factors of Fermat numbers*, Proc. Amer. Math. Soc. **9** (1958), 673–681. MR 20 #3097.
- Rosen, M., *Abel's theorem on the lemniscate*, Amer. Math. Monthly **88** (1981), 387–395. MR 82g:14041.
- Rosser, J. B., Schoenfeld, L., *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94. MR 25 #1139.
- Rotkiewicz, A., *Sur les nombres pseudopremiers de la forme $ax + b$* , C. R. Acad. Sci. Paris Sér. I Math. **257** (1963), 2601–2604. MR 29 #61.
- Rotkiewicz, A., *Sur les formules donnant des nombres pseudopremiers*, Colloq. Math. **12** (1964a), 69–72. MR 29 #3416.
- Rotkiewicz, A., *Remarque sur un théorème de F. Proth*, Mat. Vesnik **1** (16) (1964b), 244–245. MR 32 #7483b.
- Rotkiewicz, A., *Sur les nombres de Mersenne dépourvus de facteurs carres et sur les nombres naturels n tels que $n^2 \mid 2^n - 2$* , Mat. Vesnik **2** (17) (1965), 78–80. MR 33 #2596.
- Rotkiewicz, A., *On the pseudoprimes of the form $ax + b$* , Proc. Cambridge Philos. Soc. **63** (1967), 389–392. MR 35 #122.
- Rotkiewicz, A., *On the prime factors of the numbers $2^{p-1} - 1$* , Glasgow Math. J. **9** (1968), 83–86. MR 38 #2078.
- Rotkiewicz, A., *Pseudoprime numbers and their generalizations*, Stud. Assoc. Fac. Sci. Univ. Novi Sad, 1972. MR 48 #8373.
- Rotkiewicz, A., *Solved and unsolved problems on pseudoprime numbers*, in: Applications of Fibonacci Numbers, vol. 8 (ed. F. T. Howard), Kluwer Academic Publishers, Dordrecht, 1999, 293–306. MR 2000j:11010.
- Sándor, J., *Some classes of irrational numbers*, Studia Univ. Babeş-Bolyai Math. **29** (1984), 3–12. MR 86i:11035.
- Satyanarayana, M., *A note on Fermat and Mersenne's numbers*, Math. Student **26** (1958), 177–178. MR 22 #4660.

- Scharlau, W., Opolka, H., *From Fermat to Minkowski. A course on number theory and its development (German)*, Springer, Berlin, 1980. MR 82g:10001.
- Schinzel, A., *On primitive prime factors of $a^n - b^n$* , Proc. Cambridge Philos. Soc. **58** (1962), 555–562. MR 26 #1280.
- Schönhage, A., Strassen, V., *Fast multiplication of large numbers (German)*, Computing **7** (1971), 281–292. Zbl 223.68007.
- Schram, J. M., *A recurrence relation for Fermat numbers*, J. Recreational Math. **16** (1984), 195–197. Zbl 579.10005.
- Schroeder, M. R., *Number theory in science and communication*, Springer Series in Information Sci. **7**, second edition, Springer, Berlin, 1986. MR 85j:11003.
- Selfridge, J. L., *Factors of Fermat numbers*, Math. Tables Aids Comput. **7** (1953), 274–275.
- Selfridge, J. L., Hurwitz, A., *Fermat numbers and Mersenne numbers*, Math. Comp. **18** (1964), 146–148. MR 28 #2991.
- Shanks, D., *Solved and unsolved problems in number theory*, Chelsea, New York, 1962, 1978, 1985. MR 86j:11001.
- Shippee, D. E., *Four new factors of Fermat numbers*, Math. Comp. **32** (1978), 941. MR 57 #12359.
- Shorey, T. N., Stewart, C. L., *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. II*, J. London Math. Soc., II. **23** (1981), 17–23. MR 82m:10025.
- Sierpiński, W., *Remarque sur une hypothèse des Chinois concernant les nombres $(2^n - 2)/n$* , Colloq. Math. **1** (1948), 9. MR 9,331a.
- Sierpiński, W., *Theory of numbers (Polish)*, Warszawa, 1950. MR 13,821e.
- Sierpiński, W., *Les nombres de Mersenne et de Fermat*, Matematiche (Catania) **10** (1955), 80–91. MR 17,711c.
- Sierpiński, W., *Sur les nombres premiers de la forme $n^n + 1$* , Enseign. Math. (2) **4** (1958), 211–212. MR 21#29.
- Sierpiński, W., *Sur un problème concernant les nombres $k \cdot 2^n + 1$* , Elem. Math. **15** (1960), 73–74. MR 22 #7983.
- Sierpiński, W., *Sur un théorème de F. Proth*, Mat. Vesnik **1** (16) (1964a), 243–244. MR 32 #7483a.
- Sierpiński, W., *Elementary theory of numbers*, Państwowe Wydaw. Naukowe, Warszawa, 1964b. MR 89f:11003.
- Sierpiński, W., *250 problems in elementary number theory*, American Elsevier, New York, 1970. MR 42 #4475.
- Sierpiński, W., *Elementary theory of numbers, 2nd Engl. ed. revised and enlarged by A. Schinzel*, Państwowe Wydaw. Naukowe, Warszawa, 1988. MR 89f:11003.
- Skula, L., *Inclusion among special Stickelberger subideals*, Tatra Mt. Math. Publ. **11** (1997), 147–158. MR 98m:11126.
- Šofr, B., *Euclidean geometric constructions (Slovak)*, ALFA, Bratislava, 1976.
- Solovay, R., Strassen, V. A., *A fast Monte-Carlo test for primality*, SIAM J. Comput. **6** (1977), 84–85. MR 55 #2732.
- Somer, L., *On Fermat d-pseudoprimes*, In: Théorie des nombres (éd. J.-M. De Koninck & C. Levesque), Walter de Gruyter, Berlin, New York, 1989, 841–860. MR 90j:11006.

- Somer, L., *On Lucas d-pseudoprimes*, In: Applications of Fibonacci numbers, vol. 7 (eds. G. E. Bergum, A. N. Philippou, A. F. Horadam), Kluwer Academic Publishers, Dordrecht, 1998, 369–375. MR 2000a:11027.
- Somer, L., *On super-pseudoprimes*, Preprint, 2001, 1–8.
- Steuerwald, R., *Über die Kongruenz $2^{n-1} \equiv 1 \pmod{n}$* , S.- B. Math.-Nat. Kl., Bayer. Akad. Wiss., 1947, 177. MR 11,11e.
- Stewart, C. L., *On divisors of Fermat, Fibonacci, Lucas, and Lehmer numbers*, Proc. London Math. Soc., III. **35** (1977), 425–447. MR 58 #10694.
- Stewart, C. L., *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. III*, J. London Math. Soc., II. **28** (1983), 211–217. MR 85g:11021.
- Stewart, I., *Galois theory*, Chapman and Hall, London, 1973, 1989. MR 48 #8460, MR 90j:12001.
- Stewart, I., *Geometry finds factors faster*, Nature **325** (1987), 199.
- Suyama, H., *Searching for prime factors of Fermat numbers with a microcomputer (Japanese)*, BIT (Tokyo) **13** (1981), 240–245. MR 82c:10012.
- Suyama, H., *A note on the factors of Fermat numbers, II*, Abstracts Amer. Math. Soc. **5** (1984a), 132.
- Suyama, H., *The cofactor of F_{15} is composite*, Abstracts Amer. Math. Soc. **5** (1984b), 271–272.
- Szalay, L., *A discrete iteration in number theory (Hungarian)*, BDTF Tud. Közl. VIII. Természettudományok 3., Szombathely, 1992, 71–91.
- Szymiczek, K., *On prime numbers p , q , and r such that pq , pr , and qr are pseudoprimes*, Colloq. Math. **13** (1965), 259–263. MR 31 #4757.
- Szymiczek, K., *Note on Fermat numbers*, Elem. Math. **21** (1966a), 59. MR 33 #1278.
- Szymiczek, K., *Several theorems on pseudoprime numbers (Polish)*, Zeszyty Nauk. Wyż. Szkol. Ped. w Katowicach Sekc. Mat. Nr. 5 (1966b), 39–46. MR 51 #336.
- Szymiczek, K., *On pseudoprimes which are products of distinct primes*, Amer. Math. Monthly **74** (1967), 35–37. MR 34 #5746.
- Taylor, R., Wiles, A., *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), 553–572. MR 96d:11072.
- Trevisan, V., Carvalho, J. B., *The composite character of the twenty-second Fermat number*, J. Supercomput. **9** (1995), 179–182. MR 87j:11146.
- Truong, T. K., Chang, J. J., Hsu, I. S., Pei, D. Y., Reed, I. S., *Techniques for computing the discrete Fourier transform using the quadratic residue Fermat number systems*, IEEE Trans. Comput. **35** (1986), 1008–1012. MR 87j:11146.
- Vaidya, A. M., *On Mersenne's, Fermat's and triangular numbers*, Math. Student **37** (1969), 101–103. MR 42 #185.
- van Maanen, J., *Euler and Goldbach on Fermat's numbers: $F_n = 2^{2^n} + 1$ (Dutch)*, Euclides (Groningen) **57** (1981/82), 347–356. MR 85i:01014.
- Varshney, A. K., *An extension of Fermat's numbers*, Proc. Math. Soc. **7** (1991), 163–164. MR 94c:11007.
- Vasilenko, O. N., *On some properties of Fermat numbers (Russian)*, Vestnik Moskov. Univ. Ser. I Mat. Mekh., no. 5 (1998), 56–58. MR 2000g:11006.
- Vassilev-Missana, M., *The numbers which cannot be values of Euler's function ϕ* , Notes Number Theory Discrete Math. **2** (1996), 41–48. MR 97m:11012.

- Voorhees, B., *Geometry and arithmetic of a simple cellular automaton*, Complex Systems **5** (1991), 169–182. MR 93g:68099.
- Wantzel, P. L., *Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas*, J. Math. **2** (1837), 366–372.
- Warren, L. R. J., Bray, H. G., *On the square-freeness of Fermat and Mersenne numbers*, Pacific J. Math. **22** (1967), 563–564. MR 36 #3718.
- Watabe, M., *On class numbers of some cyclotomic fields*, J. Reine Angew. Math. **301** (1978), 212–215. MR 80h:12005.
- Weil, A., *Number theory. An approach through history. From Hammurapi to Legendre*, Birkhäuser Boston, Inc., Boston, Mass., 1984. MR 85c:01004.
- Western, A. E., *Notes and corrections*, Proc. London Math. Soc. **3**(2) (1905), xxi–xxii.
- Wiedemann, D., *An iterated quadratic extension of $GF(2)$* , Fibonacci Quart. **26** (1988), 290–295. MR 89m:11122.
- Wieferich, A., *Beweis des Satzes, dass sich eine jede ganze Zahl als Summe von höchstens neun positiven Kuben darstellen lässt*, Math. Ann. **66** (1909), 95–101.
- Wiles, A., *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), 443–551. MR 96d:11071.
- Williams, H. C., *Primality testing on a computer*, Ars Combin. **5** (1978), 127–185. MR 80d:10002.
- Williams, H. C., *A note on the primality of $6^{2^n} + 1$ and $10^{2^n} + 1$* , Fibonacci Quart. **26** (1988), 296–305. MR 89i:11013.
- Williams, H. C., *How was F_6 factored?*, Math. Comp. **61** (1993), 463–474. MR 93k:01046.
- Williams, H. C., *Édouard Lucas and primality testing*, Canad. Math. Soc. series of monographs and advanced texts, vol. 22, John Wiley & Sons, New York, 1998. MR 2000b:11139.
- Williams, H. C., Judd, J. S., *Some algorithms for prime testing using generalized Lehmer functions*, Math. Comp. **30** (1976), 867–886. MR 54 #2574.
- Williams, H. C., Zarnke, C. R., *A report on prime numbers of the forms $M = (6a + 1)2^{2m-1} - 1$ and $M' = (6a - 1)2^{2m} - 1$* , Math. Comp. **22** (1968), 420–422. MR 37#2680.
- Wrathall, C. P., *New factors of Fermat numbers*, Math. Comp. **18** (1964), 324–325. MR 29 #1167.
- Yang, W. Q., *A new algorithm for the rapid computation of the equal-size multi-dimensional Fermat number transform (Chinese)*, Sichuan Daxue Xuebao **25** (1988), 62–69. MR 90b:65257.
- Young, J., *Large primes and Fermat factors*, Math. Comp. **67** (1998), 1735–1738. MR 99a:11010.
- Young, J., Buell, D. A., *The twentieth Fermat number is composite*, Math. Comp. **50** (1988), 261–263. MR 89b:11012.
- Zsigmondy, K., *Zur Theorie der Potenzreste*, Monatsh. Math. **3** (1892), 265–284.

Web Site Sources

Valid as of May 17, 2001

- [www1] <http://www.prothsearch.net/fermat.html>
- [www2] <http://www.utm.edu/research/primes/glossary/Mersennes.html>
- [www3] <http://www.mersenne.org>
- [www4] www.utm.edu/research/primes/glossary/SierpinskiNumber.html
- [www5] <http://www.prothsearch.net/sierp.html>
- [www6] www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Fermat.html
- [www7] <http://www.ams.org>
- [www8] <http://www.emis.de/ZMATH>
- [www9] <http://forum.swarthmore.edu/dr.math/faq/formulas/faq.regpoly.html>
- [www10] <http://www.research.att.com/~njas/sequences/>
- [www11] <http://www.math.uga.edu/~ntheory/web.html>
- [www12] <http://www.seanet.com/~ksbrown/inumber.htm>
- [www13] <http://www.dmf.mathematics.dk/clausen.en.html>
- [www14] <http://www.utm.edu/research/primes/glossary/Cullens.html>
- [www15] <http://www.prothsearch.net/cullen.html>
- [www16] www.utm.edu/cgi-bin/caldwell/primes.cgi/Generalized%20Fermat
- [www17] <http://perso.wanadoo.fr/yves.gallot/primes/gfn.html>

Name Index

- Abel, N. H. 35, 193
 Adleman, L. M. 7, 13, 47, 138
 Agarwal, R. C. 167–170
 Aigner, A. 43, 44
 Akushskii, I. Ya. 58
 al-Farisi 101
 Alford, W. R. 136
 André-Jeannin, R. 115
 Antonyuk, P. N. 179, 182, 184–186
 Apollonius xii, xv
 Archimedes x, xii
 Artjuhov, M. M. 70
 Arya, S. P. 32
 Asadulla, S. 97
 Atkin, A. O. L. 4, 5
 Bachet de Méziriac, C. G. ix, x
 Bacon, F. xiii
 Badea, C. 115
 Baillie, R. 70, 73, 210
 Baker, A. 73
 Balasubramanian, R. 58
 Banachiewicz, T. 37
 Barner, K. vii
 Barrow, I. xv
 Beeger, N. G. W. H. 68, 131
 Beiler, A. H. 80, 203
 Bellon, M. P. 177
 Bennett, G. 38, 39
 Bernoulli, J. 36
 Beukers, F. 80
 Bicknell, M. 114
 Biermann, K.-R. 3
 Birkhoff, G. D. 140, 148
 Björn, A. 154
 Bojanič, R. 101
 Bolyai, J. 37
 Borwein, P. 116
 Bosma, W. 70
 Brahmagupta x
 Bray, H. G. 68, 217
 Brent, R. P. 3–5, 7, 67, 70, 158, 208, 210
 Bressoud, D. M. 7
 Brillhart, J. 3–5, 41, 63, 70, 142, 153,
 208, 210, 212, 214
 Broscius, J. xv
 Brožek, J. xv
 Brun, V. 113
 Buchmann, J. 154
 Buell, D. A. 5, 43, 73, 209
 Bugeaud, Y. 152
 Burrus, C. S. 167–170
 Burton, D. M. 12, 18–20, 24, 25, 31, 32,
 38, 43, 49, 50
 Burtsev, V. M. 58
 Canals, I. 43
 Carlip, W. 136, 137
 Carmichael, R. D. 20, 119, 134, 136
 Carvalho, J. B. 5
 Cauchy, A. L. x, 218
 Chabbert, P. viii
 Chang, C. C. 39, 174–176
 Chang, J. J. 171
 Chlebout, J. 40, 60, 67, 70, 160
 Cipolla, M. 132
 Clausen, T. 3, 4, 208
 Cohen, H. 47, 138
 Conway, J. H. 32, 35, 131
 Cooklev, T. V. 170, 217
 Cooley, J. W. 167
 Cormack, G. V. 70, 73
 Cosgrave 5
 Coxeter, H. S. M. 39
 Crandall, R. E. 5, 7, 43, 68, 159, 171,
 173, 209, 210, 217
 Creutzburg, R. 166–168, 170–173
 Cullen, J. 157
 Cunningham, A. J. 4, 153, 157, 208
 de Bessy, B. F. xi, xiii, xv, 130
 de Carcavi, P. xiii
 de Fermat, P. vii–xvii, 1, 2, 6, 37, 38, 41,
 79, 101, 130, 158, 213, 214, 218–225
 de la Vallée Poussin 5
 Dedekind xiii
 Descartes, R. vii, xiii, xv, xvi
 Dickson, L. E. 32, 42, 47, 59, 131, 158,
 213, 214, 217
 Diffie, W. 7
 Dilcher, K. 5, 32, 68, 210
 Dimitrov, V. S. 170, 217

- Diophantus x, xiv
 Dirichlet, P. G. L. xii, 22
 Doenias, J. 5, 43, 209
 Donevsky, B. D. 170, 217
 Dong, P. P. 73
 Dubner, H. 154
 Dudek, J. 58
 Düllmann, S. 154
 Duparc, H. J. A. 131
 Dyson, F. 39

 Einstein, A. xxi, 158
 Elliott, D. F. 168, 171, 217
 Erdős, P. 101, 104, 105, 113, 115, 116, 131, 132, 159
 Euclid 2, 194, 215
 Euler, L. x, xii, xvi, xvii, 1–3, 23, 33, 38, 39, 59, 64, 78, 95, 158, 208, 214, 215
 Eves, H. 26

 Fagin, B. 171, 217
 Faltings, G. xii
 Fehér, J. 144
 Feigenbaum, M. J. 177, 178, 184
 Ferentinou-Nicolacopoulou, J. 155
 Fermat, C.-S. viii, ix, xiii
 Fermat, P. – see de Fermat
 Flammenkamp, A. 82

 Gallot 5, 154
 Gardner, M. 35, 80
 Gauss, C. F. xi, xvii, 1–4, 9, 13, 18, 19, 24, 32, 33, 35, 187, 193–197, 201, 205, 207
 Gérardin 208
 Germain, S. xii
 Gillispie, Ch. C. viii
 Goldbach, Ch. 33
 Golomb, S. W. 65, 70, 77, 104, 108, 162
 Good, I. J. 114
 Gorshkov, A. S. 167, 171, 173, 217
 Gostin, G. B. 5, 68, 160, 210
 Gottlieb, C. 3, 204
 Graham, R. L. 115
 Granville, A. 136
 Grundmann, H.-J. 166–168, 170–173
 Grytczuk, A. 26, 28, 46, 73, 154
 Grytczuk, J. 46
 Gulliver, T. A. 154

 Gutfreund, H. 17
 Guy, R. K. 32, 35, 68, 131, 158, 164

 Hadamard 5
 Hallyburton, J. C. 5, 210
 Hamada, H. 171
 Hamilton, W. R. xvi
 Harborth, H. 90, 91, 93
 Hardy, G. H. 5, 32, 33, 38, 39, 158
 Hellman, M. E. 7
 Hérigone, P. xiv
 Hermes, J. 204
 Hewgill, D. 35, 80
 Hilbert, D. 147
 Hilton, P. 33
 Hiriart-Urruty, J.-B. 221
 Hoggatt, E. V. 114
 Hooley, C. 157
 Hsu, I. S. 171
 Huard, J. G. 86
 Hungerford, T. W. 188, 192
 Huron, R. viii
 Hurwitz, A. 5, 43, 209
 Huygens, Ch. xii, xv, xvi

 Inkeri, K. 46
 Ireland, K. 22, 65

 Jacobi, C. G. J. x
 Jacobson, E. 136, 137
 Jaeschke, G. 73, 176
 Jarden, D. 132
 Jeans, J. H. 131–133
 Jiang, Z. R. 170
 Jiménez Calvo, I. 154
 Jones, P. 147, 152
 Jones, R. 56, 57, 162
 Josephy, M. 206
 Judd, J. S. 4

 Kawatani, T. 7, 32
 Keller, W. 1, 5, 32, 37, 39, 40, 46, 70, 73, 152–154, 156, 157, 162
 Kepler, J. xiv
 Kida, Y. 148
 Kiss, E. 31, 37
 Kiss, P. 144
 Klein, F. 32, 201
 Kline, M. 33

- Knuth, D. E. 7, 43
 Koblitz, N. 7, 25
 Koch, M. 93
 Korselt, A. 136
 Kräitchik, M. 1, 39, 210, 214, 216
 Kravchenko, V. F. 167, 171
 Krishna, H. V. 66, 82, 97
 Křížek, M. 20, 32, 40, 50, 60, 67, 70, 77, 159, 160, 163
 Křížek, P. 163
 Kronecker, L. 117
 Kučera, R. 168, 217
 Kummer, E. E. xii, 86
 Labunets, V. G. 171
 Lagrange, J. L. x, xi, xvi, 214
 Lamé, G. xi, xii
 Landry, F. 3, 208
 Larras, J. 60
 Laššák, M. 20
 Le, M. 73
 Le Lasseur 208
 Lebesgue, V. A. 95, 99
 Lee, Y. C. 170
 Lefèvre, R. 224
 Legendre, A. M. xii
 Lehmer, D. H. 5, 42, 63, 70, 131, 142, 153, 212, 214
 Leibniz, G. W. xiv, 131
 Leibowitz, L. M. 170
 Lenstra, A. K. 4, 8, 38, 42, 66, 67, 208
 Lenstra, H. W. 4, 7, 8, 38, 42, 46, 47, 66, 67, 138, 159, 208
 Lepka, K. 17
 LeVeque, W. J. 68, 151
 Leyendekkers, J. V. 32
 Li, L. 8
 Li, W. 170
 Lidl, R. 148
 Ligh, S. 147, 152
 Little, W. A. 17
 Liu, P. 3
 Luca, F. 20, 73, 77, 82, 86, 97, 101, 117, 144, 146, 154, 163
 Lucas, E. 39, 41, 43, 46, 59, 60, 81, 210
 Lucká, M. 170
 Macrae, N. 165
 Mahler, K. 115
 Mahnke, D. 131
 Mahoney, M. S. viii, 41, 94, 130, 213, 214
 Maillard, J.-M. 177
 Mąkowski, A. 28, 135
 Malm, D. E. G. 138
 Malo, E. 133
 Manasse, M. S. 4, 8, 38, 42, 66, 67, 208
 Mandelbrot, B. 179
 Mann, H. B. 89
 Martzloff, J.-C. 14, 16, 80
 Maruyama, S. 7, 32
 Mayer, E. 5, 43, 209
 McClellan, J. H. 170
 McDaniel, W. L. 96
 McIntosh, R. 46, 210
 McLaughlin, P. B. 5, 68, 160, 210
 Meissner 68
 Mersenne, M. xv, 41, 213, 217
 Mignotte, M. 115, 152
 Miller, G. L. 7
 Min, B. K. 170
 Möbius 150
 Monier, L. 138
 Montgomery, P. L. 8, 19, 20, 24, 25, 32, 68
 Morain, F. 4, 5, 208
 Morehead, J. C. 5, 63
 Morhác, M. 171
 Morikawa, Y. 171
 Morimoto, M. 148, 154
 Morrison, M. A. 3, 208
 Narkiewicz, W. 19, 32
 Naur, T. 1
 Neal, L. 152
 Newton, I. xv
 Niederreiter, H. 148
 Niven, I. 19, 20, 24, 25, 32
 Norrie, C. 5, 43, 209
 Nussbaumer, H. J. 166, 170–172
 Odlyzko, A. M. 4, 159, 208
 Olbers, H. xi
 Opolka, H. 32
 Papademetrios, I. 70
 Papadopoulos, J. 5, 43, 209
 Pappus xii

- Pascal, B. vii, xii, xv, xvi
 Pascal, E. xii
 Paxson, G. A. 5, 43
 Pearce, J. 56, 57, 162
 Pedersen, J. 33
 Pei, D. Y. 171
 Pell, J. x
 Pepin, P. 41–43
 Pervouchine 210
 Peterson, A. M. 170
 Petr, K. 47, 48
 Pierpont, J. 187, 205
 Pocklington, H. C. 70
 Pollard, J. M. 3, 4, 7, 8, 38, 42, 66, 67, 208
 Pomerance, C. 7, 8, 47, 68, 135, 136, 138, 139, 152, 159, 173
 Porubský, Š. 20
 Poulet, P. 131
 Proth, F. 43, 70

 Qin, J. 16

 Rabin, M. O. 47, 138
 Racliş, N. 30
 Rademacher, H. 32, 201
 Radovici-Mărculescu, P. 82, 97
 Rao, K. R. 168, 171, 217
 Reed, I. S. 170, 171
 Reid, C. 32, 194
 Ribenboim, P. 32, 54, 60, 67–69, 95, 131, 135, 136, 155, 214–217
 Richelot, F. J. 204
 Richmond, H. W. 203
 Rickert, N. W. 5
 Riesel, H. 5, 8, 9, 23, 32, 142, 154, 158, 159, 210, 214
 Ripley, B. D. 13, 174
 Rivest, R. L. 7, 13
 Robbins, N. 32, 33, 47, 215
 Roberval, G. P. viii, xii, xv
 Robinson, R. M. 5, 36, 64, 70, 157
 Rollet, G. 177
 Rosen, M. 22, 35, 36, 65
 Rosser, J. B. 103
 Rotkiewicz, A. 43, 68, 131–133, 139, 144, 217
 Rumely, R. S. 47, 138

 Rvachev, V. A. 171
 Rvachev, V. L. 171
 Sándor, J. 113
 Sarrus 131
 Satyanarayana, M. 97
 Scharlau, W. 32
 Schinzel, A. 140
 Schneeberger, W. A. 131
 Schoenfeld, L. 103
 Scholtz, R. A. 170
 Schönhage, A. 165, 167, 173
 Schram, J. M. 26
 Schroeder, M. R. 5, 16, 32, 186, 204, 213
 Scott 154
 Selfridge, J. L. 4, 5, 41, 43, 63, 70, 73, 135, 137–139, 142, 152, 153, 158, 208–210, 212, 214
 Shamir, A. 7, 13
 Shanks, D. 32, 89, 147, 152, 158
 Shannon, A. G. 32
 Shippee, D. E. 5
 Shorey, T. N. 70
 Sierpiński, W. 20, 29, 32, 37, 41, 49, 60, 63, 70, 71, 133, 156, 158
 Singh, S. xi
 Skula, L. 154
 Sloane, N. J. A. 131
 Šofr, B. 202, 203
 Šolcová, A. xvii
 Solovay, R. 137
 Somer, L. 50, 77, 136, 137, 141–144, 146, 163
 Spearman, B. 86
 Stanyukovich, K. P. 179, 182, 184–186
 Steuerwald, R. 133
 Stewart, C. L. 70, 75
 Stewart, I. 8, 32, 201, 203
 Stillwell, J. xvii
 Strassen, V. 137, 165, 167, 173
 Straus, E. G. 104, 105, 113
 Suk, M. 170
 Sunzi, S. 14
 Suyama, H. 5, 46, 64, 65
 Szalay, L. 54, 55
 Szebehely, V. 104
 Szymiczek, K. 132, 135, 143, 144, 152, 160

- Tardif 210
 Tasche, M. 166, 171
 Taura 210
 Taylor, R. xii, 1, 68
 Theon of Alexandria x
 Torricelli, E. xi
 Trevisan, V. 5
 Truong, T. K. 170, 171
 Tuckerman, B. 5, 63, 142, 153, 212, 214
 Tukey, J. W. 167

 Vaidya, A. M. 94, 97
 Vajtersić, M. 170
 Van Halewyn, C. 5, 210
 van Maanen, J. 44
 Vandiver, H. S. 140, 148
 Varshney, A. K. 154
 Vasilenko, O. N. 29, 43, 45, 58
 Vassilev-Missana, M. 19
 Viallet, C.-M. 177
 Viète, F. viii, xii, xv
 von Neumann, J. 165
 Voorhees, B. 56

 Wagstaff, S. S. 5, 63, 135, 139, 142, 152, 153, 212, 214
 Wallis, J. xv

 Wantzel, P. L. 2, 187, 205
 Warren, L. R. J. 68, 217
 Watabe, M. 154
 Watkins, W. 35
 Weil, A. 32
 Welch, L. R. 170
 West, N. 70
 Western, A. E. 4, 5, 39, 208, 210
 Wiedemann, D. 154
 Wieferich, A. 69
 Wiles, A. xii, 1, 68
 Williams, H. C. 3, 4, 11, 32, 43, 46, 70, 73, 86, 134, 137, 138, 156, 208
 Wilson 47
 Wójtowicz, M. 73, 154
 Wrathall, C. P. 5, 210
 Wright, E. M. 5, 32, 33, 38, 39, 158

 Yamane, N. 171
 Yang, H. 14
 Yang, W. Q. 171
 Young, J. 5, 43, 73, 173, 209
 Yu, P. N. 170

 Zarnke, C. R. 156
 Zsigmondy, K. 140
 Zuckerman, H. S. 19, 20, 24, 25, 32

Subject Index

- acoustics 167
- address 174
- Ahmes series 104, 107, 113
- algebra, abstract 188
 - Hecke xii
- algebraic fraction 56
- algorithm 6, 7, 49, 173, 179, 186
 - deterministic polynomial-time 58
 - division 11, 189
 - Euclidean 11, 12, 16, 72
 - factoring 7
 - nondeterministic polynomial 8
 - parallel 170
- altitude 97, 98
- amplitude 167
- analysis, graphical 57
 - spectral 167
- ancient Greeks 3
- angle 97, 203
 - right 100
- applications ix, xiii, xvi, 3, 13, 165
- argument 191
 - contradiction 213
 - heuristic 3
 - heuristic probabilistic 158
 - modular 82
- arithmetic, binary 80, 165, 171, 173
 - complex 167
 - integer 171
 - long integer 171
 - modular 58, 171
 - modulo a Fermat number 171
 - modulo a Mersenne number 171
 - multiprecision 58
 - simplified binary 170
 - special binary 172
- array 186
- astronomy x
- asymptotic equality 5
- atom 6
- attractor-curve 185
- automorphism 192
 - Galois 192
- backward substitution 13
- base 43, 56, 57, 108, 135, 137, 138, 141, 142, 149–154
- basis 188
- bifurcation 182, 184
- bifurcation diagram 184
- binary expansion 87
- bit shift 167, 172
- branch 185
- calculus, differential vii
 - integral vii
- cardinality 22, 51, 174, 188, 192
- chaos 3, 177, 179
- Chinese calendar 16
- circle 193, 203
 - unit 181, 198
- circular arc 205
- cisoid xiv
- class NP 8
- coefficients, binary 172
 - binomial 80, 82, 117
 - integer 182, 199, 200
 - rational 182, 189, 190
- cofactor 46
- compact disk 170
- compass 2, 3, 33–35, 85, 109, 117, 187, 190–192, 194, 197, 202, 205, 206
- complex plane 179, 190, 198
- complexity of arithmetic operations 167
- component 55, 56
- compositeness 5, 7, 43
- computer 3, 158
- computer analysis 5
- computer factorization 163
- computer memory 174
- computer testing 3
- conchoid xiv
- condition, initial 182
 - necessary 6, 216
 - necessary and sufficient 41, 46, 47, 50, 51, 56, 58, 64, 194, 206, 215
 - sufficient 46, 78, 113, 160
- congruence xvii, 13, 14, 16, 20 33, 43, 47, 48, 56, 59, 71, 72, 81, 100, 145

- quadratic 23
- Wieferich's 68, 69, 217
- congruence conditions 78, 94
- congruence constraints 78
- conjecture 156, 157, 163
 - Fermat's 1
 - Mordell's xii
 - unsolved 216
- contradiction 51, 56, 65, 88, 89, 97, 120
- control parameter 177, 178
- converse implication 48, 205
- convolution 167, 168, 170
 - complex 171
 - cyclic 168, 169
 - digital 167
 - finite discrete 167
 - two-dimensional 170
 - two-dimensional cyclic 170
- coordinates vii, xiv, 191
- correlation 167
- counterexample 216
- criterion, Brun's 113
 - Euler's 23, 30, 42, 64, 71, 137, 140, 151
- cryptography 13, 173
- cube 15, 66, 163, 164, 202, 216
 - perfect 94
- curve vii, ix, xv, 36, 186
 - algebraic xiv, 184
 - cubic vii
 - irregular 48
 - oriented 48
 - plane xv
 - regular 48
- cycle 54
- cyclic convolution property 165
- cycloid vii, xiv, xv
- cylinder, infinite 13
- decoding 170
- decomposition 17
- deconvolution 170
- degree 183
 - minimal 189
- denominator 7
- density 22, 75, 76, 159
- derivative xiv
- diagonal 196, 197, 203
- diameter 203
- digit 29, 36, 94, 161
 - binary 87–89, 172
- digital computation 167
- dimension 188, 190
- Diophantus's *Arithmetics* ix, xi, xii
- discrete iteration 54, 55
- Disquisitiones arithmeticae* xvii, 205, 207
- divergence 179
- divisibility ix, 60
- divisor 70, 76, 116, 165, 214
 - composite 141
 - greatest common 10, 11, 13, 60, 99
 - nontrivial 13, 63
 - odd prime 151
 - positive 150, 183
 - prime 4, 69, 84, 143, 144, 145, 214
 - primitive prime 69, 139, 140, 142–144, 147, 148, 151
 - proper 13
 - proper prime 78
 - smallest prime 162
- dodecahedron 163, 164
- doubling 184
 - the period 177, 184
- edge 55, 56
 - directed 55, 56
- ellipse vii, xiv
- encrypting messages 7
- equation, algebraic 182
 - binomial 198
 - Catalan 94, 95, 99, 155,
 - Diophantine ix, x, 16, 66, 94, 117
 - irreducible algebraic 184
 - linear 171
 - linear Diophantine 12
 - logistic 3, 165, 177, 179, 182
 - nonlinear difference 177
 - of the second degree 192
 - partial differential 173
 - Pell x
 - quadratic 199–201
- error-correcting codes 170
- Euclidean construction 2, 3, 33, 159,

- 187, 193, 194, 202, 204, 205
- evolution 177
- exactly divides 13
- existence 15
- expectation, total 158
- face 164
- factor 3, 4, 43, 60, 66, 67, 71, 110,
 - largest prime 73, 75, 154
 - largest square 150
 - largest square-free 75
 - lucky Fermat 77–79
 - mutually coprime 155
 - nontrivial 5, 7, 8, 40, 213
 - odd 61
 - penultimate prime 4
 - prime 4, 43, 63, 66, 70, 71, 78, 83, 132, 142, 143, 152–154, 157–161, 183, 207, 209–212
 - proper prime 77
 - rational 111
- factoring 6, 173, 182, 183
- factorization 2, 4, 7, 22, 38, 60, 63, 153, 160, 213
 - complete 3, 41, 148, 159, 184
 - computer 163
 - prime 163, 181
 - prime-power 19, 21, 34, 42
- fast coding 170
- Feigenbaum cascade 178
- Fermat's assertion 49
- field 187, 191
 - complex 187
 - complex number 167
 - extension 187, 188, 192
 - finite-dimensional 189
- filter 170
- filtering 171
 - data 167
 - digital 170
- fine structure of the curve 185
- form, canonical 179
 - linear 73
- formula, asymptotic 75
 - Heron's 98
 - Lucas 1
 - Gauss 5, 19
- recurrence 26
- Stirling's 83
- symmetric 100
- fractal 179
- function, arithmetic 144
 - Carmichael's lambda 21, 136, 145
 - decreasing 74
 - Euler totient 19, 20, 22, 77, 85, 102, 117, 192
 - exponential xiv
 - hashing 174, 176
 - minimal perfect hashing 174–176
 - Möbius 147
 - number-theoretic 144
 - ordered minimal perfect hashing 176
 - pairwise coprime transformation 175
 - perfect hashing 174
 - Riemann ζ 10
- game, computer 173
- Gaussian notation 14
- generator of pseudorandom numbers 165, 174
- geometric interpretation 11, 12, 16, 17, 27, 47, 56, 95, 180
- geometry 33, 35
 - analytic vii, xii
 - non-Euclidean 37
- golden section 203
- Golomb's corollary 108
- graph 54
 - associated 57
 - asymmetric 57
 - binary 55, 56
 - iteration 55
 - nondirected 55
 - of the function 177
 - rotationally symmetric 57
 - topologically equivalent 56
- group 192
 - abelian Galois 192
 - cyclic 48, 192
 - finite 192
 - of permutations 192
- growth, exponential 105
- Hamiltonian path 48
- hardware 170

- hashing 174
- helix 13
- heptakaidecagon 203
- hyperbola vii, xii, xiv
- hypotenuse 98
- icosahedron 163, 164
- ideal, Stickelberger 154
- identity, convolution 168
 - Viète's 50
- imaginary unit 171
- incongruence 91–93
- index 185
- induction 13, 17, 50, 67, 106
 - complete xiii
 - incomplete xiii
 - mathematical xiii
- induction step 191
- inequality, Chleboun's 61
 - sharp 61, 63
 - triangular 98, 100
- input data 8
- integer, algebraic 98
 - composite 43, 137, 141
 - even 52, 96, 153
 - Gaussian 189
 - nonnegative 72, 96, 114, 120, 125
 - non-Sierpiński odd 159
 - odd 62, 140
 - odd composite 137, 141
 - perfectly symmetric 57
 - positive x , 28, 49, 72, 74, 107, 113, 116, 140, 145, 156, 205
 - square-free x
- integer part 5, 6
- integers, amicable 101
 - coprime 11, 20, 134, 140
 - coprime positive 105, 205
 - relatively prime 11
- inverse 166
- irrationality 104, 107, 110, 113, 116
- key 174, 176
- Kronecker delta 169
- law of refraction xv
 - of quadratic reciprocity 24, 44
 - strong of small numbers 164
- lemniscate 35, 36
- length, transformation 165
 - maximum transformation 165
- linear space 188, 190
- logarithm 73
- Lucas's lemma 81
- Lucas's primality test 41
- magnitude 8
- map, inverse 192
 - nonzero 192
- matrix, identity 169
 - inverse transformation 168
 - nonsingular 168
 - transformation 168
- median 98
- medicine 167
- mesh, square 11
- method, Baker's 73
 - continued fraction 3
 - elliptic curve 4, 8
 - factorization 3, 6, 7
 - Fermat factorization 7
 - mathematical ix
 - Monte Carlo 173
 - numerical ix
 - of infinite descent xiii
 - Pollard's rho 4
 - RSA 13
- midpoint 203
- model, chiral Potts 165, 177
 - mathematical 177
- modem 171
- multiple, least common 10, 13, 104
- multiplication 167
 - by powers 172
 - fast 165
 - of large numbers 173
- multiplicity 78, 143, 144, 151,
- n th root of unity 148
- negation 172
- norm 170
- number, algebraic 189
 - binary 3
 - Carmichael 131, 135, 136
 - complex 10, 167, 180, 187–191
 - composite 2, 3, 9, 36, 143, 159
 - composite Fermat 60, 62, 64, 79,

- 133, 138, 143, 160, 208
- composite Mersenne 138, 217
- constructible 190, 191
- Cullen 147, 157
- Cunningham 153
- even 215
- even perfect 216
- Feigenbaum 178
- Ferentinou-Nicolapoulou 154
- Fermat vii, 1–257 (a.e.)
- Fibonacci 11, 117
- figurate ix, x
- generalized Fermat 85, 108, 147, 153, 154
- innocent-looking 5
- irrational 104
- large 173
- Lucas 117
- Mersenne 44, 45, 82, 139, 143, 145, 147, 154, 181, 213, 214, 216, 217
- Mersenne square-free 217
- multiply perfect 103
- natural 10, 11, 13, 16, 19, 39, 50, 51, 59, 66, 71, 72, 161, 215
- n -gonal x
- non-Sierpiński 159
- not powerful 69
- odd 97, 161
- odd prime 150
- pentagonal 95
- pentagonal Fermat 97
- perfect ix, 215, 216
- polygonal x, 95
- positive 125
- prime xvi, 9, 10, 68, 74, 81, 163
- pseudorandom 3, 13, 173
- quadri-composite 158
- rational 98, 107, 116, 184, 188–190
- real 113, 167, 187
- Rotkiewicz 144–146
- Sierpiński 72, 73, 159, 165
- smallest Sierpiński 73
- square 95
- square-free 119, 160
- triangular 82, 95
- triangular Fermat 82, 97
- very large 165
- numbers, amicable ix, 101
 - consecutive composite 157
 - coprime 15, 19
 - Fermat pairwise coprime 183, 184
 - friendly ix
 - pairwise coprime 15
 - Pythagorean ix
- octahedron 163, 164
- one-to-one correspondence 186
- order 61
 - multiplicative 17
- Padé approximation 115, 116
- pair, amicable 101
 - twin prime 66
- pairs of Fermat numbers 185
- parabola vii, xii, xiv, 180
- paraboloid xiv
- parallel implementation 170
- parametrization 101
- pattern recognition 167
- period 180–186
 - minimal 180, 181, 183
- periodicity 182
- permutation 48
- physical particles 17
- point, accumulation 177
 - bifurcation 177
 - Fermat ix, x
 - fixed 54
 - lattice 12
- polygon, constructible regular 205
 - regular 2, 33–35, 85, 97, 109, 117, 159, 164, 191, 194
- polygonal shape 96
- polyhedra, Platonic 163, 164
- polyhedron, regular 163, 164
- polynomial, algebraic xiv
 - cyclotomic 148, 150, 181–186, 192
 - fundamental symmetric 85
 - in two variables 182
 - irreducible 192
 - irreducible lower-order 183
 - minimal 189, 190, 192
 - monic 98, 189
 - nonzero 189
- polynomial time 8

- power 31, 152
 - composite prime 152
 - higher 121–124, 126–129
 - negative 173
 - perfect 94, 150, 152, 155
 - prime 97–99, 149
- precision, finite 167
- primality 5, 7, 47, 50, 51 56, 58, 73
- primality testing 6, 41, 71, 153, 173
- prime xii, xvi, 2, 3, 9, 41, 45–47, 56, 59, 63, 70, 111, 147, 148, 163, 165, 169, 181
 - Cullen 157
 - elite 44, 163
 - Fermat 1–3, 54–57, 85, 88, 91, 93, 97, 99, 109, 110, 117, 118, 120, 125, 144, 157–159, 163, 184, 194, 206, 207
 - irregular xii
 - Mersenne 153, 154, 213–217
 - odd xv, 51–53, 56, 87, 140, 155, 156
 - probable 137, 138, 148, 154
 - Sophie Germain 54, 215
 - Wieferich's 68, 69
- principle 164, 206
 - Dirichlet pigeonhole 111
 - Fermat vii, xvi
 - well-ordering xiii, 11
- probability xvi, 137, 138, 158
- problem, algebraic 205
 - deconvolution 171
 - four-line xv
 - geometric xv, 205
 - of the duplicated cube 202
- processing, digital signal 3, 165
 - image 167
- product, infinite 113
 - pointwise 168
- progression 178
 - arithmetic 22, 77, 139
 - geometric 169, 178
- projection, orthogonal 203
- pseudoprime 3, 36, 37, 44, 47, 131–135
 - 137, 139, 141, 142, 149, 150, 152, 153, 165, 216
 - absolute 135–137
 - Euler 137–139, 150, 151
 - Fermat d 136, 137
 - for the function 144
 - odd 133
 - strong 137–139, 147, 150–152
 - to the base 137
- quadratic nonresidue 23, 30, 44, 50, 52, 54, 174
- quadratrix xiv
- quadrature xiv
- quantization 167
- quotient, Fermat 17
- radar 171
- ratio 154
- rationality 109
- reciprocal 104, 109
- record 174
- regular heptadecagon 33, 34, 193, 197, 198, 203
 - heptagon 194
 - nonagon 194
 - pentagon 3, 34, 198, 202, 203
 - triangle 34, 198
 - n -gon 3, 34, 203–205
 - p -gon 48
 - $2^i n$ -gon 205
 - 7-gon 3
 - 9-gon 3, 205
 - 15-gon 205
 - 17-gon 3, 194, 196, 204
 - 60-gon 33
 - 257-gon 3, 34, 204
 - 65537-gon 3, 34, 204
- relation, divisibility 96
 - recurrence 27
 - reflexive 14
 - symmetric 14
 - transitive 14
- remainder 11, 15, 16, 55–57, 173–176, 202
- repeller-curve 185
- representation, balanced 168
 - binary 121
- residue, cubic 64
 - quadratic 23, 24, 50, 64, 100, 120
 - k th power 64
 - nonnegative 94
 - nonzero 202

- of a modulo m 13
- root 2, 189, 190, 198, 201, 202, 205
 - incongruent primitive 20
 - of unity 191
 - primitive 9, 18, 20, 22, 24, 30, 41, 42, 50, 54, 56, 64, 145, 174, 186, 192, 201
 - smallest primitive 202
 - square 6, 171, 197
- rotation 48
- round-off error 167, 171
- ruler 2, 3, 33–35, 85, 109, 117, 187, 190–192, 194, 197, 202, 205, 206
- scheme, hashing 3, 165, 174
 - iteration 54, 55
- semiperimeter 97
- sequence 46, 72, 113, 179, 180
 - bounded 179
 - cyclic 54
 - deterministic 173
 - Fibonacci 114, 115
 - increasing 104, 113
 - Lucas 114, 119, 182
 - monotonically increasing 35
 - monotone 159
 - of positive integers 113
 - of pseudorandom numbers 174
 - of random numbers 173
 - periodic 57, 174
 - pseudorandom 173
- set, covering 72, 73
 - finite 54
 - fractal 35, 179
 - key 174
 - linearly independent 188, 189
 - Mandelbrot 179, 180
 - of positive integers 75
 - of prime numbers 75
 - of primes 22, 76
 - Sierpiński fractal 35
- sieve, number field 4
 - of Eratosthenes 9
- signal 166–168, 170
 - complex 171
 - digital 167
 - filtering 170
 - periodic 168
 - transformed 168
- simulation of physical processes 173
- Sino-representation 16
- solution, analytic xv
 - computable 85
 - general 15
 - integer 12
 - nonconstant periodic 178
 - nonperiodic 180, 181
 - nontrivial 85
 - periodic 179–184, 186
 - trivial 181, 183
 - true 8
 - unstable 177, 178
- sonar 171
- space 188
- spiral xv
 - Fermat vii
- square xiii, 6, 7, 10, 11, 17, 31, 49, 50, 63, 68, 94, 98, 99, 150, 151, 161
 - magic ix, xv
 - perfect 94, 152
- square-free kernel 140, 150
- star, 17-pointed 194, 196
- stereometry 163
- straight line 12
- straight line segment 197
- straightedge 2
- structural vibration 167
- subfield 187, 192
- subgraph 55
- subideal 154
- subgroup 192
- subsequence 182
- sum, irrational 108
 - of the series 104, 107, 108, 114
 - of the reciprocals 108, 162
- superpseudoprime 3, 139, 141–144, 150–152, 160
- supercomputer 4
- supercomputing 7
- symbol, Jacobi 25, 42–44, 137
 - Legendre 23–25, 151
- symmetrization 55
- symmetry 17, 82, 86
- system, binary 32

- convolution 171
- dynamical 178
- dynamical biological 177
- of congruences 72
- of equations 191
- of simultaneous congruences 14
- tangent vii, xiv, xv
- test, deterministic primality 47, 138
 - Lucas 41
 - Lucas–Lehmer 182, 214
 - Pepin’s 5, 42, 43, 46, 56, 70, 165
 - primality 49, 70
 - probabilistic primality 137, 138
 - Selfridge 42
 - Solovay–Strassen primality 138
 - statistical 173
 - strong probabilistic primality 47
- tetrahedron 163, 164
- theorem, Antonyuk, Stanyukovich 185
 - binomial 60, 68, 74, 151
 - Bolyai 31
 - Carmichael 21, 136, 145
 - Chang 176
 - Chinese remainder 14–16, 22, 71, 150, 171
 - Cipolla 132, 133, 152
 - converse 163
 - Dirichlet 22, 77, 162
 - Euclid 9, 215
 - Euclid for a right triangle 197
 - Euclid on the infinitude of primes 9, 33
 - Erdős 113
 - Erdős, Straus 113
 - Euler 20, 21, 38, 41, 42, 49, 175, 215
 - Fermat’s last vii, xi, xii, xvi, 1, 68, 69
 - Fermat’s last, first case 69
 - Fermat’s little vii, xv–xvii, 1, 6, 16–18, 24, 30, 31, 36, 38, 45, 47, 60, 64, 70, 119, 130, 132, 135, 138, 140, 151, 157, 214
 - four-squares x
 - fundamental of algebra 198
 - fundamental of arithmetic 9, 10
 - Gauss 33, 34, 109, 164, 187, 188, 190–192, 194, 205
 - Goldbach 33, 38, 40, 45, 47, 56, 60, 69, 112, 132, 134, 143, 147, 152, 161, 176, 184
 - Heath 216
 - Inkeri 46
 - Jones, Pearce 57
 - Korselt 136
 - Lucas 6, 39, 40, 49, 59, 64, 68, 74, 76, 101, 143, 152, 159, 160–162
 - McIntosh 46
 - Pocklington 70, 71
 - prime number 5, 135, 158
 - Proth 70, 71
 - Racliš 30
 - Rotkiewicz 133, 139
 - Sándor 113
 - Schinzel 140, 143
 - Sierpiński 71, 72
 - Sophie Germain 32
 - Suyama 40, 70, 71, 78, 79
 - Szalay 55
 - Szymiczek 153
 - Wieferich 69
 - Wilson 47–49
 - Zsigmondy 140, 144
- theory, algebraic number 154
 - analytic number 73
 - Galois 33, 187, 192
 - Gauss 193
 - group 3
 - Jacobi x
 - number vii, xiii, 14, 16, 22, 33, 35, 94, 130, 158, 165
 - of chaos 177
 - of fields 188
 - of indices 18
 - perturbation 182, 184
- transcendence 115
- transform, digital 167
 - discrete Fourier 167
 - discrete weighted 171
 - fast Fourier 167
 - Fermat number 3, 165, 170
 - Fourier 166, 167, 171
 - inverse 168
 - Laplace 166

- linear invertible 168
- Mersenne number 217
- number-theoretic 165, 171
- pseudo-Fermat number 170
- transformation 169
- transition to chaos 178
- transitivity 14, 188
- tree, bifurcation 184, 186
 - binary 56
 - of cyclotomic polynomials 186
- trial division 3, 6, 63
- triangle x , 100
 - equilateral x
 - Heron 97, 98
- infinite 80
- isosceles 98
- Pascal 35, 80–83, 85, 86
- Pythagorean xiii
 - right 197, 203
 - similar 191
- trigonometry ix
- triple, Pythagorean 98–100
 - reduced Pythagorean 101
- twin primes 66, 157
- universe 4, 187
- vertex 55, 164
- windows 178, 180



Rue Fermat in Paris.