

Historie Fermatových kvocientů (Fermat – Lerch)

Fermatova čísla

In: Karel Lepka (author): Historie Fermatových kvocientů (Fermat – Lerch). (Czech). Praha: Prometheus, 2000. pp. 97–103.

Persistent URL: <http://dml.cz/dmlcz/401894>

Terms of use:

© Lepka, Karel

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://dml.cz>

Příloha 3

Fermatova čísla

V této tabulce jsou uvedeni prvočíselní dělitelé tvaru $k \cdot 2^n + 1$ Fermatových čísel F_m .

m	k	n	Metoda	Datum	Objevitel
5	5	7		1732	Euler
	52347	7		1732	Euler
6	1071	8		1880	Landry
	262814145745	8		1880	LandryLassGer
7	k_1 (15 míst)	9	CFrac	13. 9. 1970	MorrBrillhart
	k_2 (20 míst)	9	CFrac	13. 9. 1970	MorrBrillhart
8	604944512477	11	Rho	1980	BrentPollard
	k_3 (59 míst)	11		1980	BrentPollard
9	37	16		1903	Western
	k_4 (46 míst)	11	NFS	15. 6. 1990	LenstraManasse
10	k_5 (96 míst)	11	NFS	15. 6. 1990	LenstraManasse
	11131	12	TrDiv	15. 8. 1953	Selfridge
	395937	14	TrDiv	1962	Brillhart
	k_6 (37 míst) (248 míst)	12 13	ECM ECPP	20. 10. 1995 1995	Brent Brent
11	39	13		1899	Cunningham
	119	13		1899	Cunningham
	k_7 (17 míst)	14	ECM	17. 5. 1988	Brent
	k_8 (18 míst) (560 míst)	13 13	ECM ECPP	13. 5. 1988 20. 6. 1988	Brent BrentMorain
12	7	14		1877	LucasPervushin
	397	16		1903	Western
	973	16		1903	Western
	11613415	14	TrDiv	1974	HallBrillhart
	76668221077	14	p-1	25. 7. 1986	Baillie

m	k	n	Metoda	Datum	Objevitel
13	41365885	16	TrDiv	1974	HallBrillhart
	20323554055421	17	ECM	5. 1. 1991	Crandall
	6872386635861	19	ECM	9. 5. 1991	Crandall
	k_9 (21 míst)	19	ECM	19. 6. 1995	Brent
14	S l o ž e n é		Pepin	1963	SelfridgeHurw
15	579	21	TrDiv	1925	Kraitchik
	17753925353	17	TrDiv	4. 8. 1987	Gostin
	k_{10} (28 míst)	27	ECM	1997	CrandallDilcher
16	1575	19	TrDiv	14. 8. 1953	Selfridge
	k_{11} (21 míst)	20	ECM	1996	CrandallDilcher
17	59251857	19	TrDiv	květen 1978	Gostin
18	13	20		1903	Western
19	33629	21	TrDiv	16. 11. 1962	Riesel
	308385	21	TrDiv	1963	Wrathall
20	složené		Pepin	1987	BuellYoung
21	534689	23	TrDiv	1963	Wrathall
22	složené		Pepin	říjen 1993	CDNY
23	5	25	TabPr	1878	Pervushin
25	48413	29	TrDiv	1963	Wrathall
	1522849979	27	TrDiv	7. 8. 1985	Gostin
	16168301139	27	TrDiv	16. 12. 1987	McLaughlin
26	143165	29	TrDiv	1963	Wrathall
27	141015	30	TrDiv	1963	Wrathall
	430816215	29	TrDiv	21. 2. 1985	Gostin
28	25709319373	36	TrDiv	5. 2. 1997	Taura
29	1120049	31	TrDiv	17. 10. 1980	GosMcL
30	149041	32	TrDiv	1963	Wrathall
	127589	33	TrDiv	1963	Wrathall
32	1479	34	TrDiv	1963	Wrathall
36	5	39	TabPr	1886	Seelhoff
	3759613	38	TrDiv	2. 1. 1981	GosMcL
37	1275438465	39	TrDiv	29. 4. 1991	Gostin
38	3	41		1903	CullCunnWest
	2653	40	TrDiv	1963	Wrathall
39	21	41	TabPr	1956	Robinson
42	43485	45	TrDiv	1963	Wrathall
52	4119	54	TrDiv	1963	Wrathall
	21626655	54	TrDiv	1982	Keller
55	29	57	TabPr	1956	Robinson
58	95	61	TabPr	1957	Robinson
61	54985063	66	TrDiv	17. 5. 1986	Gostin
62	697	64	TrDiv	1977	Shippee
63	9	67	TabPr	1956	Robinson
64	17853639	67	TrDiv	13. 5. 1986	Gostin

m	k	n	Metoda	Datum	Objevitel
66	7551	69	TrDiv	1977	Shippee
71	683	73	TrDiv	1977	Shippee
72	76432329	74	TrDiv	31. 5. 1986	Gostin
73	5	75		1906	Morehead
75	3447431	77	TrDiv	duben 1982	Gostin
77	425	79	TrDiv	1957	RobinsonSelf
81	271	84	TrDiv	1957	RobinsonSelf
91	1421	93	TrDiv	1977	Shippee
93	92341	96	TrDiv	1979	Baillie
99	16233	104	TrDiv	listopad 1979	GosMcLSu
107	1289179925	111	TrDiv	8. 11. 1992	Gostin
117	7	120	TabPr	1956	Robinson
122	5234775	124	TrDiv	21. 5. 1986	Gostin
125	5	127	TabPr	1956	Robinson
142	8152599	145	TrDiv	22. 5. 1986	Gostin
144	17	147	TabPr	1956	Robinson
146	37092477	148	TrDiv	23. 12. 1987	Gostin
147	3125	149	TrDiv	prosinec 1979	GosMcL
	124567335	149	TrDiv	1. 12. 1990	Gostin
150	1575	157	TrDiv	1956	Robinson
	5439	154	TrDiv	květen 1980	GosMcLSu
164	1835601567	167	TrDiv	31. 5. 1993	Gostin
178	313047661	180	TrDiv	18. 6. 1991	Gostin
184	117012935	187	TrDiv	17. 12. 1990	Gostin
201	4845	204	TrDiv	27. 7. 1980	GosMcL
205	232905	207	TrDiv	1. 1. 1984	Keller
207	3	209	TabPr	1956	Robinson
215	32111	217	TrDiv	2. 12. 1980	Suyama
226	15	229	TabPr	1956	Robinson
228	29	231	TabPr	1956	Robinson
232	70899775	236	TrDiv	24. 11. 1991	Gostin
250	403	252	TrDiv	1957	RobinsonSelf
251	85801657	254	TrDiv	30. 11. 1991	Gostin
255	629	257	TabPr	1979	Baillie
256	36986355	258	TrDiv	20. 1. 1991	Gostin
259	36654265	262	TrDiv	21. 1. 1991	Gostin
267	177	271	TrDiv	1957	RobinsonSelf
268	21	276	TabPr	1956	Robinson
275	22347	279	TrDiv	16. 1. 1984	Keller
284	7	290	TabPr	1956	Robinson
287	5915	289	TrDiv	26. 12. 1980	Suyama
298	247	302	TabPr	1979	Baillie
301	7183437	304	TrDiv	4. 11. 1990	Gostin
316	7	320	TabPr	1956	Robinson
329	1211	333	TrDiv	12. 1. 1981	Suyama

m	k	n	Metoda	Datum	Objektivitel
334	27609	341	TrDiv	25. 1. 1984	Keller
338	27654487	342	TrDiv	22. 12. 1990	Gostin
353	18908555	355	TrDiv	25. 12. 1990	Gostin
375	733251	377	TrDiv	9. 6. 1986	Gostin
376	810373	378	TrDiv	9. 6. 1986	Gostin
398	120845	401	TrDiv	18. 4. 1984	Keller
416	8619	418	TrDiv	1981	Suyama
	38039	419	TrDiv	16. 2. 1984	Keller
417	118086729	421	TrDiv	13. 6. 1992	Gostin
431	5769285	434	TrDiv	30. 11. 1990	Gostin
452	27	455	TabPr	1956	Robinson
468	27114089	471	TrDiv	25. 9. 1992	Gostin
544	225	547	TabPr	1979	Baillie
547	77377	550	TrDiv	5. 6. 1986	Gostin
556	127	558	TabPr	1976	MattWilliams
620	10084141	624	TrDiv	19. 1. 1992	Gostin
635	4258979	645	TrDiv	12. 7. 1991	Gostin
637	11969	643	TrDiv	08. 3. 1984	Keller
692	717	695		1979	AtRick
723	554815	730	TrDiv	4. 1. 1991	Gostin
744	17	747	TabPr	1976	MattWilliams
851	497531	859	TrDiv	18. 1. 1988	Gostin
885	16578999	887	TrDiv	12. 7. 1992	Gostin
906	57063	908	TrDiv	19. 5. 1986	Gostin
931	1985	933	TrDiv	22. 12. 1980	Keller
1069	137883	1073	TrDiv	1. 9. 1992	Gostin
1082	82165	1084	TrDiv	8. 4. 1991	Gostin
1123	25835	1125	TrDiv	15. 1. 1987	Gostin
1225	79707	1231	TrDiv	8. 6. 1991	Gostin
1229	29139	1233	TrDiv	7. 12. 1987	Gostin
1451	13143	1454	TrDiv	30. 10. 1986	Gostin
1551	291	1553		1979	AtRick
1849	98855	1851	TrDiv	1. 9. 1992	Gostin
1945	5	1947	TabPr	1957	Robinson
1990	150863	1993	TrDiv	30. 10. 1995	Taura
2023	29	2027	TabPr	1979	AtRick & CorWill
2089	431	2099	TabPr	17. 8. 1983	Suyama
2456	85	2458		1979	AtRick
3310	5	3313	TabPr	1979	AtRick & CorWill
3506	501	3508	TrDiv	26. 7. 1986	Gostin
4258	1435	4262	TrDiv	5. 8. 1993	Gostin
4724	29	4727	TabPr	1979	CorWill
6208	763	6210	TabPr	5. 8. 1993	Gostin
6390	303	6393	TabPr	6. 10. 1993	Gostin

m	k	n	Metoda	Datum	Objevitel
6537	17	6539	TabPr	1979	CorWill
6835	19	6838	TabPr	30. 9. 1978	Keller
6909	6021	6912	TabPr	12. 11. 1993	Gostin
7309	145	7312	TabPr	25. 10. 1992	Dubner
8555	645	8557	TabPr	1. 11. 1993	Dubner
9428	9	9431	TabPr	1. 4. 1983	Keller
9448	19	9450	TabPr	30. 8. 1980	Keller
12185	81	12189	TabPr	4. 9. 1993	Dubner
13250	351	13252	TabPr	1. 10. 1996	Taura
14252	1173	14254		1997	Taura
14276	157	14280	TabPr	31. 8. 1996	Taura
15161	55	15164	TabPr	28. 8. 1993	Dubner
17906	135	17909	TabPr	31. 8. 1996	Taura
18749	11	18759	TabPr	12. 9. 1992	Dubner
18757	33	18766	TabPr	20. 8. 1993	Dubner
23069	681	23071		1996–1997	DTG
23288	19	23290	TabPr	14. 12. 1992	Dubner
23471	5	23473	TabPr	5. 9. 1984	Keller
24651	99	24653	TabPr	11. 9. 1996	Taura
25006	57	25010	TabPr	18. 12. 1993	Young
28281	81	28285	TabPr	18. 8. 1996	Taura
94798	21	94801	TabPr	březen 1995	Young
95328	7	95330	TabPr	23. 8. 1994	Young
114293	13	114296	TabPr	1995	Young
125410	5	125413	TabPr	1995	Young
157167	3	157169	TabPr	14 .6. 1995	Young
213319	3	213321	TabPr	1997	Young

Velcí činitelé k_i

- $k_1 = 116503103764643$
 $k_2 = 11141971095088142685$
 $k_3 = 45635566267264637582599393652151804972681268330878021767715$
 $k_4 = 3640431067210880961102244011816628378312190597$
 $k_5 = 362128936829849024182024971631805407255830459520272960891514$
 $314523640507570656742232821636569307$
 $k_6 = 1137640572563481089664199400165229051$
 $k_7 = 10253207784531279$
 $k_8 = 434673084282938711$
 $k_9 = 609485665932753836099$
 $k_{10} = 1287603889690528658928101555$
 $k_{11} = 180227048850079840107$

Metody

TrDiv	Zkusmé dělení
TabPr	Testování tabelovaných prvočísel
CFrac	Metoda řetězových zlomků
Rho	Pollardova ρ metoda
p-1	Pollardova $p - 1$ metoda
ECM	Metoda eliptických křivek (faktorizační)
NFS	Metoda síta v číselných tělesech
ECPP	Metoda eliptických křivek (dokázání prvočíselnosti)
Pepin	Pepinův test

Objevitelé

AtRick	A. Oliver, L. Atkin, N. W. Rickert
Baillie	Robert Baillie
Brent	Richard P. Brent
BrentMorain	Richard P. Brent, Francois Morain
BrentPollard	Richard P. Brent, John M. Pollard
Brillhart	John Brillhart
BuellYoung	Duncan A. Buell, Jeff Young
CorWill	G. V. Cormack, Hugh C. Williams
Crandall	Richard E. Crandall
CrandallDilcher	Richard E. Crandall, Karl Dilcher
CDNY	R. E. Crandall, J. Doenias, C. Norrie, J. Young
CullCunnWest	James Cullen, A. Cunningham, A. E. and F. J. Western
Cunningham	Allan Cunningham
DTG	Demichel-Taura-Gallot
Dubner	Harvey Dubner
Euler	Leonhard Euler
GosMcL	Gary B. Gostin, Philip B. McLaughlin, Jr.
Gostin	Gary B. Gostin
HallBrillhart	John C. Hallyburton, Jr., John Brillhart
Keller	Wilfrid Keller
Landry	Fortune Landry
LandryLassGer	Fortune Landry, H. Le Lasseur, A. Gerardin
LenstraManasse	Arjen K. Lenstra, Mark S. Manasse a spolupracovníci
LucasPervushin	Edouard Lucas, Ivan M. Pervushin
MattWilliams	G. Matthew, Hugh C. Williams
McLaughlin	Philip B. McLaughlin, Jr.
Morehead	J. C. Morehead
MorrBrillhart	Michael A. Morrison, John Brillhart
Pervushin	Ivan Mikheevich Pervushin
Riesel	Hans Riesel
Robinson	Raphael M. Robinson
RobinsonSelf	Raphael M. Robinson, John L. Selfridge

Seelhoff	Paul Seelhoff
SelfridgeHurw	John L. Selfridge, Alexander Hurwitz
Shippee	D. E. Shippee
Suyama	Hiromi Suyama
Taura	Tadashi Taura
Western	A. E. Western
Wrathall	Claude P. Wrathall
Young	Jeffrey Young