PIERRE de FERMAT

1601 nar. v BAUMONT de LOMAGNE (u TOULOUSE)

nar. 17. 8. (?)

pokřtěn 20.8.

otec obchodník s kůžemi, matka z rodiny státních úředníků.

Základní a střední vzdělání ve františkánském klášteře v Grandselve

před 1631 bakalář civilního práva v Orleansu, nějakou dobu v Bordeaux

14. 5. 1631 titul soudního rady - Toulouse

15. 6. 1631 svatba s Luisou de Long, 2 synové, 3 dcery

Samuel: úředník, soudní rada v Toulouse, zachoval otcovo dílo

Jean: kanovník katedrály v Castres

Claire: provdala se

Cathérine a Luise: jeptišky

působení v Toulouse a v Castres (sídlo soudního dvora)

12. 1. 1665 umírá v úřadě

Nikdy nebyl dál než v Bordeaux.

Vynikající klasické vzdělání: latina, řečtina, italština, španělština.

Matematika: nejpozději konec 20. let v Bordeaux, Etienne de Espagnet - Vietovy spisy - kroky k analytické geometrii - dílo *Ad locos planos et solidos isagoge (Úvod do studia rovinných křivek a ploch)*

1636-1637 poslal práci do Paříže

od 1636 - teorie čísel

Toulouse - Pierre de Carcavi (1600-1684)- 1636 přeložen do Paříže - Marin Mersenne (1588-1648)

1636 - 1643 Malá a Velká Fermatova věta

1654 - korespondence s Blaisem Pascalem (1623 -1662) - teorie pravděpodobnosti

1654 - Fermat plánuje vydání svých prací - žádá Carcaviho a Pascala o spolupráci (Pascal - teorie čísel), nikdy neuskutečněno

Od 1670 - po Fermatově smrti - syn Samuel shromažďuje roztroušenou korespondenci. Vydává znovu Diofantovu *Aritmetiku* s otcovými poznámkami. K vydání připojena práce Jacquese de Billyho *Doctrinae Analyticae Inventum Novum*, psaná podle Fermatových dopisů - diofantické rovnice.

1679 - vydána práce *Varia Opera* (geometrie, algebra, diferenciální a integrální počet, dopisy)

TEORIE ČÍSEL

Motiv: vybudování aritmetiky jako nauky o celých číslech (na rozdíl od Diofanta)

2 okruhy zájmů: pythagorejské trojice

součty dělitelů čísel

1. oblast: prvočísla tvaru 4k+1 lze vyjádřit jako součet druhých mocnin, prvočísla tvaru 4k-1 nikoliv

Velká Fermatova věta

„Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem fane detexi. Hanc marginis exiguitasnon caperet.“

„Nelze rozdělit krychli na dvě krychle, bikvadrát na dva bikvadráty a obecně žádnou mocninu vyšší než dvě na dvě mocniny téhož stupně. Pro tuto skutečnost jsem nalezl podivuhodný důkaz, tento okraj je však příliš úzký.“

WILES (1953) 1993, 1995

2. oblast: Malá Fermatova věta

Věta: Nechť p je prvočíslo. Pak pro všechna přirozená a platí

$$a^p \equiv a \pmod p.$$

Je-li navíc (a,p) = 1, platí

$$a^{p-1} \equiv 1 \pmod p.$$

Symbol kongruence ovšem zavedl až GAUSS (1777-1855)

Fermat studoval *dokonalá čísla*

$$s(n) = n , \quad S(n) = 2n .$$

1638 René DESCARTES (1596 - 1650) dokázal

Věta: Nechť (a,b) = 1. Pak

$$s(ab) = s(a).s(b) + a.s(b) + b.s(a) .$$

Věta: Nechť (a,b) = 1. Pak

$$S(ab) = S(a).S(b).$$

Věta: Sudé n je dokonalé právě tehdy, když je tvaru

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

kde $k > 1$ a $2^k - 1$ je prvočíslo.

Dostatečnost podmínky znal už EUKLEIDÉS, nutnost však dokázal až EULER (1707 - 1783).

ŘEKOVÉ: 6, 28, 496, 8128

$6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$

EUKLEIDES : Je-li M_n prvočíslo, je $2^{n-1} . M_n$ dokonalé.

EULER: Sudá dokonalá čísla jsou právě uvedeného tvaru.

1814 BARLOW : $2^{30}.M_{31}$ je největší dokonalé číslo, jaké kdy bylo objeveno.

PROBLÉM : Existuje liché dokonalé číslo?

Pokud ano, musí být větší než 10^{200}, musí mít alespoň 8 prvočíselných dělitelů, z nichž aspoň jeden musí být větší než 300 000; je-li menší než $10^{9\,118}$, musí být dělitelné 6. mocninou některého prvočísla, ...

TABULKA MERSENNOVÝCH PRVOČÍSEL

	p	cifer M_p	cifer P_p	rok	objevil
1	2	1	1	-	-
2	3	1	2	-	-
3	5	2	3	-	-
4	7	3	4	-	-
5	13	4	8	1456	?
6	17	6	10	1588	Cataldi
7	19	6	12	1588	Cataldi
8	31	10	19	1772	Euler
9	61	19	37	1883	Pervušin
10	89	27	54	1911	Powers

11	107	33	65	1914	Powers
12	127	39	77	1876	Lucas
13	521	157	314	1952	Robinson
14	607	183	366	1952	Robinson
15	1279	386	770	1952	Robinson
16	2203	664	1327	1952	Robinson
17	2281	687	1373	1952	Robinson
18	3217	969	1937	1957	Riesel
19	4253	1281	2561	1961	Hurwitz
20	4423	1332	2663	1961	Hurwitz
21	9689	2917	5834	1963	Gillies
22	9941	2993	5985	1963	Gillies
23	11213	3376	6751	1963	Gillies
24	19937	6002	12003	1971	Tucker
25	21701	6533	13066	1978	Noll, Nickel
26	23209	6987	13973	1979	Noll
27	44497	13395	26790	1979	Nelson, Slowinski
28	86243	25962	51924	1982	Slowinski
29	110503	33265	66530	1988	Colquitt, Welsh
30	132049	39751	79502	1983	Slowinski
31	216091	65050	130100	1985	Slowinski
32	756839	227832	455663	1992	Slowinski, Gage
33	859433	258716	517430	1994	Slowinski, Gage
34	1257787	378623	757263	1996	Slowinski, Gage
35	1398269	420921	841842	1996	GIMPS
36	2976221	895932	1791864	1997	GIMPS
37	3021377	909526	1819050	1998	GIMPS

38	6972593	2098960		1999	Hajratwala
39?	13466917	4053946		2001	Cameron, GIMPS
40?	20996011	6320430		2003	GIMPS

Bernard FRENICLE de Bessy (1605 - 1675) rada soudního dvora v Monnais, zabýval se teorií čísel (magické čtverce). Korespondence s Fermatem.

1640 Frenicle se dotazuje Fermata (prostřednicvím Mersenna), zda ex. prvočíslo mezi 10^{20} a 10^{22} .

Rovnice

$$10^{20} < 2^{n-1}.(2^n - 1) < 10^{22}$$

má řešení n = 34, 35, 36, 37.

Fermat popsal Mersennovi, jak při řešení postupoval.

Vycházel ze znalosti tří faktů:

(I) Je-li n složené, je i $2^n - 1$ složené

(II) Je-li n prvočíslo, pak je $2^n - 2$ násobkem čísla 2n .

(III) Je-li n prvočíslo a p je prvočíselný dělitel čísla $2^n - 1$, pak je p-1 násobkem čísla n .

Podmínka (I) je důsledkem obecné identity

$$x^{ab} - 1 = (x^a - 1)(x^{a(b-1)} + x^{a(b-2)} + \ldots + 1)$$

pro případ $x = 2$.

Skutečnost, že tvrzení (I) považoval Fermat za svůj objev, svědčí o jeho nevelkých znalostech algebry. (II) a (III) jsou však typické případy vedoucí na Malou F. větu.

Jak na to přišel?

18. 10. 1840 píše Freniclovi: *Je-li dáno libovolné prvočíslo* p *a libovolná geometrická posloupnost* 1, a, a^2, *atd.* , p *musí dělit některé číslo* $a^n - 1$, *pro něž* n *dělí* p-1; *jestliže potom* N *je libovolný násobek nejmenšího* n *pro něž toto platí,* p *dělí také* $a^N - 1$. *Toto tvrzení platí pro všechny řady a všechna prvočísla. Poslal bych Vám jeho důkaz, obávám se však, že je příliš dlouhý.*

E. L. Dickson: *History of the Number Theory* (1919) - „čínská věta“ - staří Číňané znali „test prvočíselnosti“:

$$n \mid 2^n - 2 \Rightarrow n \text{ je prvočíslo .}$$

Námitka: Číňané vůbec neznali pojem „prvočíslo“.

Uvedená konverze M.F.věty přitom vůbec není správná!

SARRUS (1798 - 1861):

$$11.31 = 341 \mid 2^{341} - 2$$

Dickson tuto nesprávnou informaci pravděpodobně převzal z článku H. J. Jeanse v časopise *Messenger of Mathematics*, vol. 27, 1897-98, který nesprávně interpretoval úryvek z čínské *Matematiky v devíti knihách*.

Jiná hypotéza: Han Qi z *Institutu historie přírodních věd* v Pekingu v doktorské práci uvádí, že chyba se do čínských textů dostala v 18. stol. přenosem z Evropy.

LI SHANLAN (1811 - 1882) se domníval, že uvedený test objevil a kolem r 1869 ho v Šanghaji sdělil překladateli do čínštiny Alexanderu Wyliemu. Wylie, který matematiku dobře neznal, se domníval, že jde o významný objev a popsal ho v *Notes and Queries on Chine and Japan* (1869). (Na chybnost v dalších číslech poukázali čtenáři.) LI samotný na tento svůj omyl v r. 1872 upozornil, přesto v r. 1882 znovu výsledek publikuje Liův spolupracovník HUA HENGTANG (připsal ho Liovi).

Není jasné, zda Jeans tato fakta znal.
(Vše publikoval v r. 1997 Man-Keung Siu z Hongkongu.)

Vraťme se k problému hledání dokonalých čísel mezi 10^{20} a 10^{22} . Z uvedeného plyne, že jediným adeptem je n = 37, pokud ovšem $2^{37} - 1$ je prvočíslo.

Z Fermatova dopisu Freniclovi plyne, že znal následující důsledek Malé věty:

Věta: ***Nechť*** **n, p** ***jsou lichá prvočísla, přičemž*** $p \mid (2^{n-1}-1)$.
Pak $p = 2kn+1$.

Důkaz: Nechť $n > 2$ **je prvočíslo a** $2^{n-1}-1$ **je dělitelné lichým prvočíslem** p . **Pak** $p-1 = qn$, **kde** q **je přirozené. Protože** p **je liché, je** $p-1$ **sudé, takže** $2 \mid qn$. **Protože** n **je liché, je** q **sudé, tj.** $q = 2k$. **Prvočíselní dělitelé čísel** 2^n-1 **jsou tudíž tvaru** $p=2kn+1$.

Fermat se tedy mohl pokusit faktorizovat číslo $2^{37} - 1$. **Pokud existuje prvočíselný dělitel** p , **musí** 37 **dělit** $p-1$. **Protože** p **bude liché, musí být tvaru** $74n+1$. **První kandidát** 149 **nevyhovuje, druhý** 223 **ano.**

Odtud však vedla přímá cesta k Fermatovým prvočíslům.

$$F_m = 2^2 + 1 \quad \text{pro } m=0,1,2,... \quad \text{jsou prvočísla}$$

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65\,537$$

Jak na to přišel?

Věta: Je-li p **přirozené a** $q > 1$ **liché, platí**

$$2^{pq} + 1 = (2^p + 1)(2^{p(q-1)} - 2^{p(q-2)} + ... - 2^p + 1)$$

Důsledek: Je-li číslo $2^n + 1$ **prvočíslo, musí být exponent** n
tvaru $k=2^m$.

1732 L. EULER $F_5 = 2^{32} + 1 = 4\ 294\ 967\ 297 = 641 \cdot 6\ 700\ 417$

1880 F. LANDRY rozložil číslo

$$F_6 = 2^{64} + 1 = 274\ 147 \times 67\ 280\ 421\ 310\ 721$$

Carl Friedrich GAUSS (1777 - 1855):

Věta: Pravidelný mnohoúhelník je eukleidovsky konstruovatelný právě tehdy, když počet jeho vrcholů je roven číslu

$$k = 2^i p_1 p_2 \ldots p_j,$$

kde $p_1, p_2, \ldots, p_j$ jsou navzájem různá Fermatova prvočísla.

Je konstruovatelný: k = 3,4,5,6,8,10,12,15,16,17,.....

Není konstruovatelný: k = 7,9,11,13,14,...

Známé konstrukce: k = 17, 257, 65 537

Zatím známe $31 = 2^5 - 1$ eukleidovsky konstruovatelných mnohoúhelníků s lichým počtem vrcholů.

1897 Felix KLEIN (1849 - 1925) F_7 je složené, neurčil však žádného dělitele

1909 totéž pro F_8 J. C. Moreheard a A. E. Western

1970 $F_7 = (2^9 . 116\ 503\ 103\ 764\ 643 + 1) .$
$. (2^9 . 11\ 141\ 971\ 095\ 088\ 142\ 685 + 1)$

Zkoumejme prvočíselnost čísla F_m standardně - dělením všemi prvočísly menšími než F_m . Jak dlouho bychom ověřovali např. F_8 ?

Celá část F_8 má 39 cifer, takže před F_8 je cca

$$10^{38}/(38. \ln 10) = 10^{36}$$

prvočísel. Rok má cca $3{,}2 . 10^7$ sekund, takže při miliardě dělení za sekundu bychom potřebovali cca 3.10^{19} let. Stáří vesmíru je cca $15 . 10^9$ let.

Dnes je prověřeno, že pro $m = 5, 6, \ldots , 23$ jsou F_m složená.

1962 W. SIERPINSKI (1882 - 1969)

F_{1945} není prvočíslo (10^{582} číslic)

1980 F_{9448} je dělitelné číslem $19 . 2^{9450} + 1$

1983 W. KELLER Číslo F_{23471} je dělitelné číslem

$$5 . 2^{23473} + 1$$

Číslo F_{23471} má víc než 10^{7000} cifer. (Číslo 10^{7000} má „jen“ 7001 cifer.)

Proč FERMAT nefaktorizoval alespoň F_5 ?

Podle jeho výsledků může být prvočíselný dělitel pouze tvaru 64n+1 a 641 je opravdu dělitelem.

Ani Frenicle toto číslo nerozložil, ačkoliv ho o to Fermat žádal a potvrdil Fermatovo nesprávné tvrzení.

Fermat tomu do smrti věřil, i když důkaz neznal.

Ve 40. letech se Fermat přestal problémy dělitelnosti zabývat.

Pokračování :

LEIBNIZ (1646 - 1716) našel důkaz M.F.V., důkaz však nepublikoval. Z pozůstalosti ho publikoval GOLDBACH (1690 - 1764)

EULER (1707 - 1783) našel v r. 1736 důkaz pomocí binomické věty a považoval větu za svůj objev, později však uznal Fermatovo prvenství.