Historie matematiky a informatiky
Cvičení 5

Doc. RNDr. Alena Šolcová, Ph. D.,
KAM, FIT ČVUT v Praze

2014

Evropský sociální fond
Investujeme do vaší budoucnosti

Fermatova čísla

Fermat Numbers , Fermat Primes

- Definice: Fermatovo číslo je přirozené číslo tvaru $F_n = 2^{2^n} + 1$, kde $n \geq 0$.
- Je-li F_n prvočíslem, nazveme jej Fermatovo prvočíslo.

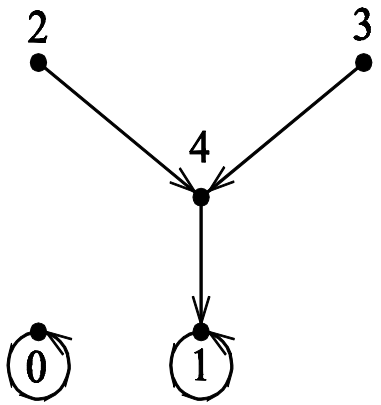
  $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65\,537$
- Fermatova domněnka: „Všechna čísla tohoto tvaru jsou prvočísla.“ byla vyvrácena Eulerem.

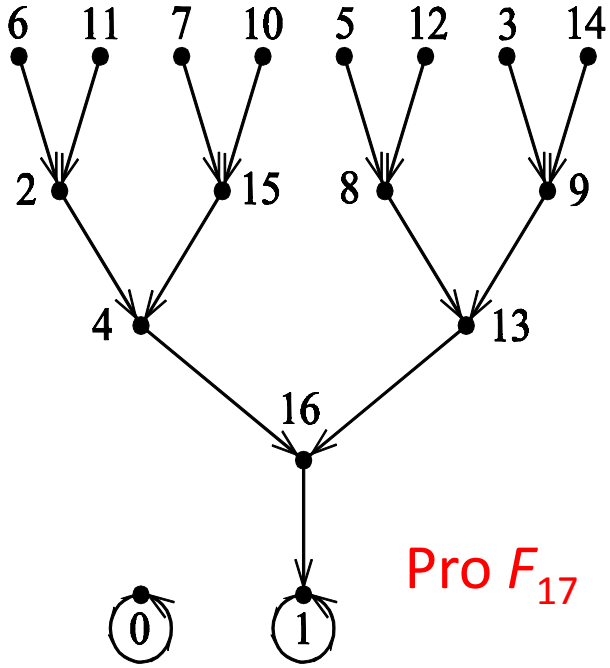
Pierre de Fermat (1601 – 1665)

Iterační graf Fermatových prvočísel

$X_{k+1} \equiv X_k^2 \pmod{F_n}$

Pro F_5





Pro F_{17}

Iterační graf má tvar stromu,
právě když F_n je prvočíslo.

Euler: 641 | F_5

- 1732 – Leonhard Euler

  F_5 není Fermatovo prvočíslo.

  $F_5 = 2^{2^5} + 1 = 4\ 294\ 967\ 297$

  je dělitelné číslem 641.

Důkaz (G. Bennett): Položme $a = 2^7$ a $b = 5$,

tedy $1 + ab = 1 + 2^7 . 5 = 641$. Pak odečteme b^4 od výrazu $1 + ab$,

tedy $1 + ab - b^4 = 1 + (a - b^3). b = 1 + 3b = 2^4$, protože $a - b^3 = 2^7 - 5^3 = 128 - 125 = 3$.

Euler: 641 | F_5

- $F_5 = 2^{2^n} + 1 = 2^{32} + 1$

$= 2^4 a^4 + 1$

$= (1 + ab - b^4)\, a^4 + 1$

$= (1 + ab)\, a^4 + (1 - a^4 b^4)$

$= (1 + ab)\, a^4 + (1 - a^2b^2)(1 + a^2b^2)$

$= (1 + ab)\, [a^4 + (1 - ab)\, (1 + a^2b^2)]$

Protože podle $1 + ab = 1 + 2^7 . 5 = 641$, $641 \mid F_5$.

Vlastnosti Fermatových čísel 1

- Věta: Fermatova čísla jsou vzájemně nesoudělná.

  Pro Fermatova čísla F_m a F_n, kde $m > n \geq 0$,

  je nsd $(F_m, F_n) = 1$

- 1880 - F. Landry – 82 let – metoda pokusu a omylu

  $F_6 = 2^{64} + 1 = 274177 \,.\, 67280421310721$

- 1905 - J. C. Morehead, A. E. Western použili Pépinův test na F_7 a určili, že F_7 je číslo složené.

- 1971 - trvalo to 66 let, než Brillhart a Morrison našli rozklad $F_7 = 2^{128} + 1 =$

  $= 59649589127497217 \,.\, 5704689200685129054721.$

Pépinův test

Pepin's Test for determining primality

1877 – J. T. Pépin, jezuitský kněz –
Test ke zjišťování prvočíselnosti Fermatových čísel

Věta:
Pro n ≥ 1 je Fermatovo číslo $F_n = 2^{2^n} + 1$ prvočíslem právě tehdy,
když $3^{(F_n - 1)/2} \equiv -1 \pmod{F_n}$.

Příklad 1: $F_3 = 17$ … $3^8 \equiv 9^4 \equiv 81^2 \equiv (81 - 5.17)^2 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17}$

Příklad 2: $F_3 = 257$

$$3^{(F_3 - 1)/2} = 3^{128} = 3^3 (3^5)^{25}$$
$$\equiv 27\,(-14)^{25}$$
$$\equiv 27\,(-14)^{24}\,(-14) \equiv 27\,(-2)^{8 \cdot 3}\,7^{3 \cdot 8}\,(-14)$$
$$\equiv 27\,256^3\,86^8\,(-14) \equiv 27\,(-1)^3\,86^8\,(-14) \ldots$$
$$\equiv 27 \cdot 17 \cdot (-14)$$
$$\equiv 27 \cdot 19 \equiv 513 \equiv -1 \pmod{257},$$

tedy F_3 je prvočíslo.

Vlastnosti Fermatových čísel 2

- 1747 - Euler, Lucas

Věta: Každý prvočíselný dělitel p Fermatova čísla

$$F_n = 2^{2^n} + 1, \text{ kde } n \geq 2, \text{ je ve tvaru}$$

$$p = k \,.\, 2^{n+2} + 1$$

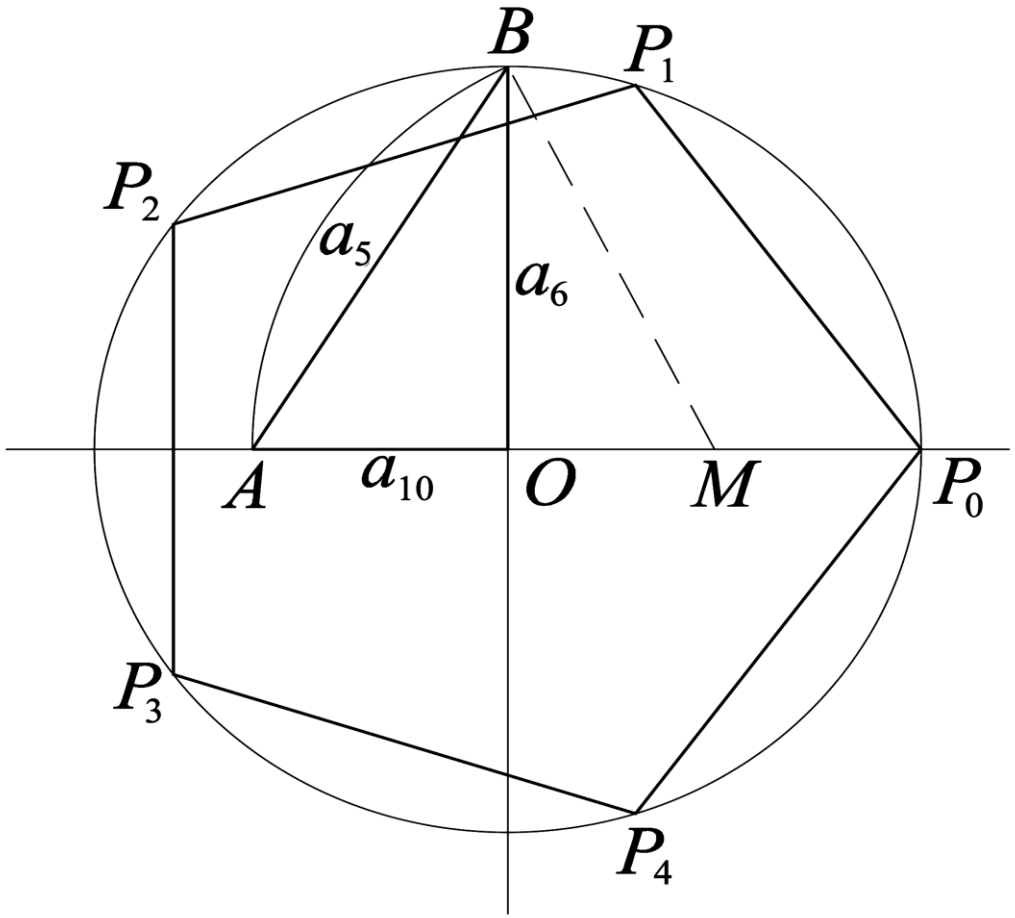
Konstruovatelnost pravidelných mnohoúhelníků

- 1801 - Gauss dokázal, že pravidelný mnohoúhelník o n vrcholech je konstruovatelný eukleidovsky (tj. kružítkem a pravítkem) právě tehdy, když $n = 2^k$ nebo $n = 2^k p_1 . p_2 \ldots p_r$ kde $k \geq 0$ a $p_1 . p_2 \ldots p_r$ jsou různá Fermatova prvočísla.

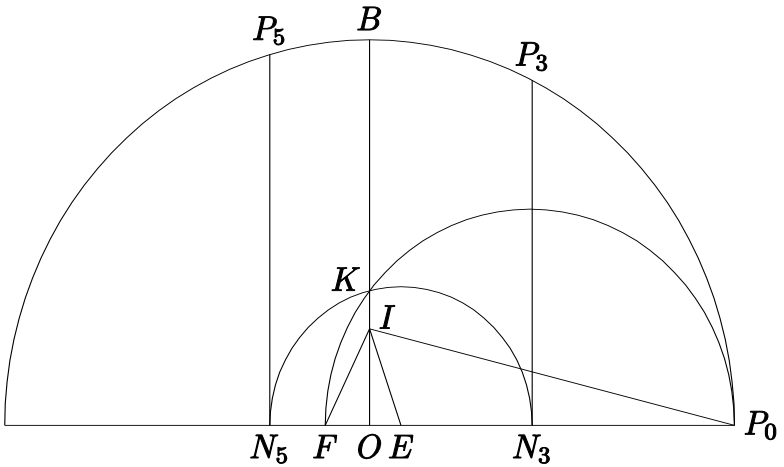
  (poslední kapitola *Disquisitiones arithmeticae*)

  Pravidelný sedmnáctiúhelník

Konstrukce mnohoúhelníků



Gaussův sedmnáctiúhelník



Fibonacciova čísla

- 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, …

Leonardo z Pisy (1180 – asi 1250)

12. kapitola Liber abaci – Kniha o abaku

Úloha o králících

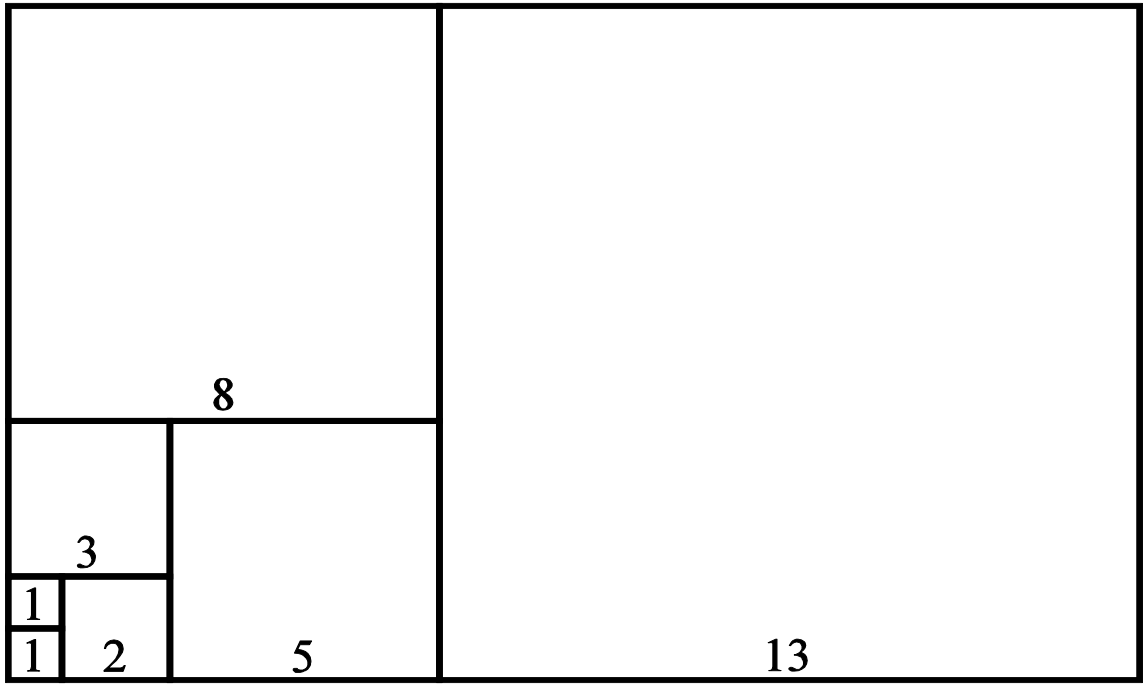
Fibonacci Quarterly, Fibonacci Association

četné aplikace

Souvislost s Pascalovým trojúhelníkem

Zlatý řez, zlatý obdélník

Aplikace v architektuře



Palindromická čísla

- Palindrom je skupina znaků nebo čísel, která je stejná, čte-li se zprava nebo zleva.
- Příklady: KRK, Kobyla má malý bok. 121, 111111, 2867682
  135797531 – souvisí s datem založení Karlova mostu
- Zajímavá vlastnost: Když přičteme k libovolnému číslu jeho zrcadlový obraz, tak po konečném počtu kroků dostaneme palindromické číslo.

Příklad: 18 + 81 = 99

68 + 86 = 154, 154 + 451 = 605, 605 + 506 = 1111

25 + 52 = 77, 38 + 83 = 121

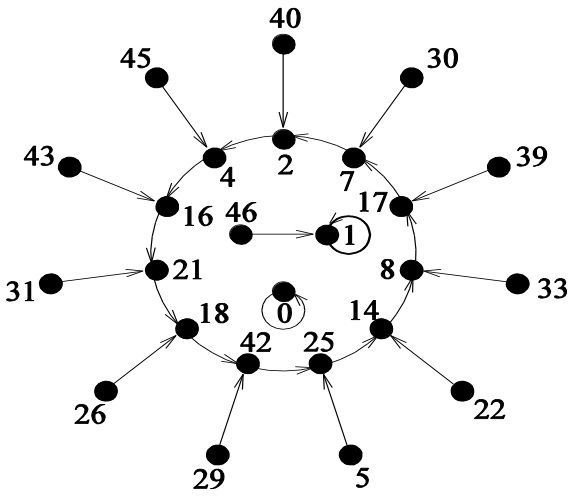
89 + 98 = 187, 187 + 781 … 24 kroků … 8813200023188

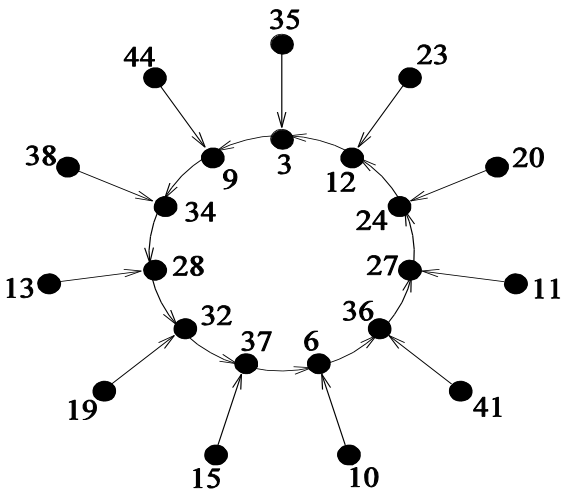
Prvočísla Sophie Germainové

Germain Prime

- Definice: Liché číslo *p* takové, že $2p + 1$ je také prvočíslo, se nazývá prvočíslo Sophie Germainové. Např. 5, 11, 23
- Největší známé takové číslo má 34 547 cifer.

2p + 1= 47





Literatura

- Křížek, M. , Somer, L., Šolcová, A.: *Kouzlo čísel*, ed. Galileo, Academia, Praha 2009
- Burton, D. : *Elementary Number Theory*, Mc Graw Hill, Boston 2007, 6th Edition
- Křížek, M. , Luca, F. , Somer, L.: *17 Lectures on Fermat Numbers, From Number Theory to Geometry,* Springer, New York 2001
- Šolcová, A., Křížek, M., Mink, G.: *Matematik Pierre Fermat,* CEFRES, Praha 2002