Historie matematiky a informatiky 2
8. přednáška

Doc. RNDr. Alena Šolcová, Ph. D.,

KAM, FIT ČVUT v Praze

12. listopadu 2013

Evropský sociální fond

Investujeme do vaší budoucnosti

Čísla speciálních tvarů a jejich vlastnosti

Alena Šolcová

Čísla speciálních tvarů

- Dokonalá čísla (Perfect Numbers)
- Mersennova čísla (Mersenne Numbers)
- Spřátelená čísla (Amicable Numbers)
- Fermatova čísla (Fermat Numbers)
- Fibonacciova čísla atp.
- Speciální prvočísla –
  palindromická, prvočísla Sophie Germainové.

Vlastnosti Fermatových prvočísel, příklady aplikací.

Dokonalá čísla

Perfect Numbers

Pýthagorejci

$$6 = 1 + 2 + 3$$

$$28 = 1 + 2 + 4 + 7 + 14$$

Definice: Kladné celé číslo *n* je dokonalé, je-li rovno součtu všech kladných dělitelů vyjma sebe sama.

Řekové znali pouze 4 čísla: 6, 28, 496, 8128.

Nikomachos z Gerasy (Introductio Arithmeticae) okolo 100 n.l. – vytvořil matematickou teorii, zavedl čísla spřízněná (spřátelená), společenská, abundantní, deficientní.

Vlastnosti dokonalých čísel

- *n* je dokonalé, když je počet kladných dělitelů
  $\sigma(n) - n$

- *n* je dokonalé, když $\sigma(n) = 2n$

- Hypotézy:
  1. *n* –té dokonalé číslo má právě *n* cifer.
  2. Každé dokonalé číslo končí střídavě buď číslicí 6 nebo 8.

Obě hypotézy jsou vyvráceny:

Nemáme dokonalé číslo s 5 číslicemi

$P_5 = 33550336 = 2^{12} \cdot 8191 = 4096 \cdot 8191 = 4096 \cdot (2^{13} - 1)$

(nalezeno již v anonymním rukopisu v 15. století),

$P_6 = 8589869056 = 2^{16} \cdot 131071 = 65536 \cdot 131071 = 65536 \cdot (2^{17} - 1)$

(Cataldi, 1603)

Obě dokonalá čísla po sobě následující končí číslicí 6.

Obecný tvar dokonalého čísla

Eukleidés dokazuje:

$1 + 2 + 2^2 + 2^3 + \ \ldots \ + 2^{k-1} = p$ je prvočíslo, pak $2^{k-1}\, p$ je dokonalé číslo (nutně sudé). IX. Kniha – Základy

Příklady: $1 + 2 + 4 = 7$ je prvočíslo, tedy $4 \,.\, 7 = 28$ je dokonalé.

Eukleidés používá součet geometrické řady

$$1 + 2 + 2^2 + 2^3 + \ \ldots \ + 2^{k-1} = 2^k - 1$$

(lze najít ve starších pýthagorejských textech)

Pak z toho plyne: Je-li $2^k - 1$ prvočíslo ($k > 1$), pak

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

Důkaz, že každé sudé dokonalé číslo je tohoto tvaru, až za 2000 let.

Lemma

- Je- li $a^k - 1$ prvočíslo ($a > 0$, $k \geq 2$), pak $a = 2$ a k je také prvočíslo.

Příklady: Pro $p = 2, 3, 5, 7$ hodnoty $2^p - 1$ jsou prvočísla 3, 7, 31, 127.

Pak $2\,(2^2 - 1) = 6$

$2^2(2^3 - 1) = 28$

$2^4\,(2^5 - 1) = 496$

$2^6\,(2^7 - 1) = 8128$

jsou všechna dokonalá čísla.

Ale platí to vždy?

Je vždy $2^p - 1$ prvočíslo?

- Mnoho matematiků si domnívalo, že odpověď je kladná.
- 1536 – Hudalrichus Regius v *Utriusque Arithmetices* nalezl pěkný rozklad

$$2^{11} - 1 = 2047 = 23 \cdot 89$$

Poslední číslice sudého dokonalého čísla

- Věta:

Sudé dokonalé číslo n končí číslicí 6 nebo 8, tj.

$$n \equiv 6 \pmod{10} \quad \text{nebo} \quad n \equiv 8 \pmod{10}.$$

V důkazu se užije lemmatu a předcházející věty.

Zadáme si dvě úlohy k zamyšlení:

Lámejte si hlavu L7-4, L7-5

- L 7-3. Dokažte, že přirozené číslo
  $n = 2^{10}(2^{11} - 1)$ není dokonalé číslo,
  tj. $\sigma(n) \neq 2n$.
  (Návod: $2^{11} - 1 = 23 \cdot 89$.)

- L 7-4. Najdi dvě poslední cifry dokonalého čísla

$$n = 2^{19936}(2^{19937} - 1)$$

Odpověď zašlete na adresu:

alena.solcova@fit.cvut.cz

Předmět: HMI2-L7-x JménoPříjmení

Existuje liché dokonalé číslo?

Jeden z nejstarších otevřených problémů!

- René Descartes – NE
- James Joseph Sylvester , 2. pol. 19. stol.– pochybuje, muselo by vyhovovat vysokému počtu požadavků.
- Pokud existuje, víme o něm:
  - Bude mít nejméně 8 rozdílných prvočíselných dělitelů, z nichž jeden je větší než milión.
  - Bude mít nejméně 300 číslic.

Mersennova čísla

- Čísla tvaru $M_n = 2^n - 1$ tradičně nazýváme Mersennova podle P. Marina Mersenna.
- Pokud jsou čísla M_n prvočísla, mluvíme o Mersennových prvočíslech.
- P. Marin Mersenne (1588 – 1648),
- člen řádu minimů,
- zakladatel Pařížské akademie,
- získal vzdělání v jezuitské koleji La Flèche jako René Descartes.

Spřátelená čísla

Amicable Numbers or Friendly Numbers

- Dvojice čísel, pro něž je součet dělitelů každého z nich roven druhému číslu.
- Nejmenší spřátelená čísla jsou 220 a 284.
- Součet dělitelů čísla 220 je:

  1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284

- Součet dělitelů čísla 284 je:

  1 + 2 + 4 + 71 + 142 = 220

Thabitova věta

- Thabit ibn Qurra, 9. století:

Věta: Jsou-li 3 čísla

$$p = 3 \cdot 2^{n-1} - 1,\ q = 3 \cdot 2^{n} - 1,\ r = 9 \cdot 2^{2n-1} - 1$$

prvočísly, pak $2^n \cdot p \cdot q$ a $2^n r$ jsou spřátelená čísla.

1636 – v dopise Mersennovi oznamuje Pierre de Fermat, že našel čísla 17 296 a 18 416 jako spřátelená čísla.

1638 – v dopise Mersennovi píše René Descartes, že našel další dvojici použitím Thabitovy věty: 9363584 a 9437056.

Fermat: $n = 4$, $p = 23$, $q = 47$, $r = 1151$, p, q, r jsou prvočísla.

Descartes: $n = 7$, $p = 191$, $q = 383$, $r = 73727$, p, q, r jsou prvočísla.

Další spřátelená čísla

- 18. století

Leonhard Euler našel 64 dvojic spřátelených čísel.

2 dvojice byly později odhaleny jako nespřátelené.

(1909, 1914).

1830 – Adrien Maria Legendre – nalezl další dvojici:

2 172 649 216 a 2 181 168 896.

Dnes – nalezeno více než 50 000 dvojic.

Není známé pravidlo pro nalezení všech spřátelených dvojic.

Euler položil otázku:

Zda existuje dvojice spřátelených čísel, z níž jedno číslo je sudé a jedno liché. Odpověď není dosud známa.

Nejspřátelenější čísla

"Most" amicable numbers

Obě čísla spřátelené dvojice jsou sudá a mají součet dělitelný 9.

Příklad: $220 + 284 = 504 \equiv 0 \pmod 9$.

Nejmenší známá dvojice, která nemá tuto vlastnost , je

666030256 a 696630544.

Deficientní a abundantní čísla

Deficient Numbers and Abundant Numbers

Čísla, která nejsou dokonalá,

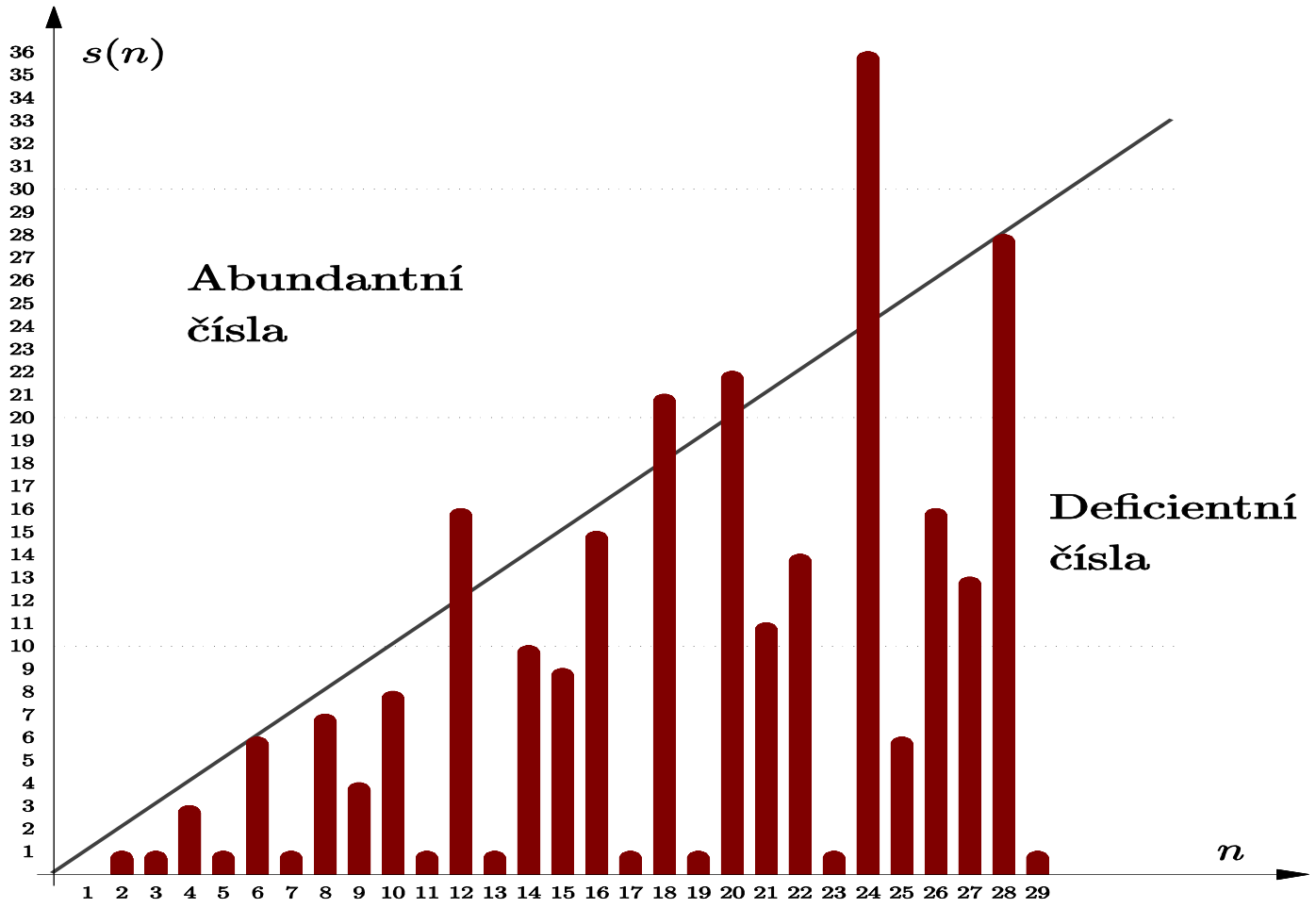
jsou deficientní nebo abundantní.

Definice:

- Přirozené číslo je deficientní, je-li $\sigma(n) < 2n$.

- Přirozené číslo je abundantní, je-li $\sigma(n) > 2n$.

Deficientní a abundantní čísla



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.

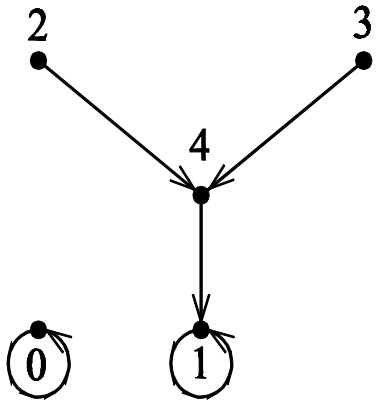
  $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65\,537$
- Fermatova domněnka: „Všechna čísla tohoto tvaru jsou prvočísla.“ byla vyvrácena Eulerem.

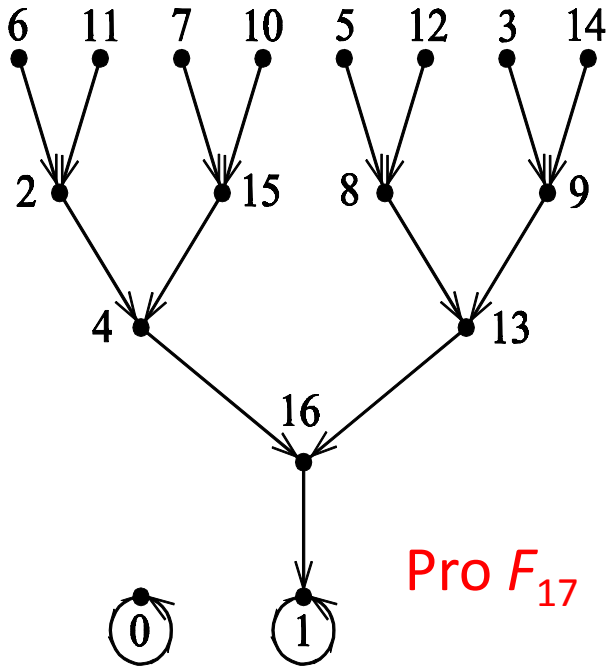
Pierre de Fermat (1601 – 1665)

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

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

$$= 2^4 a^4 + 1$$

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

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

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

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

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

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

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

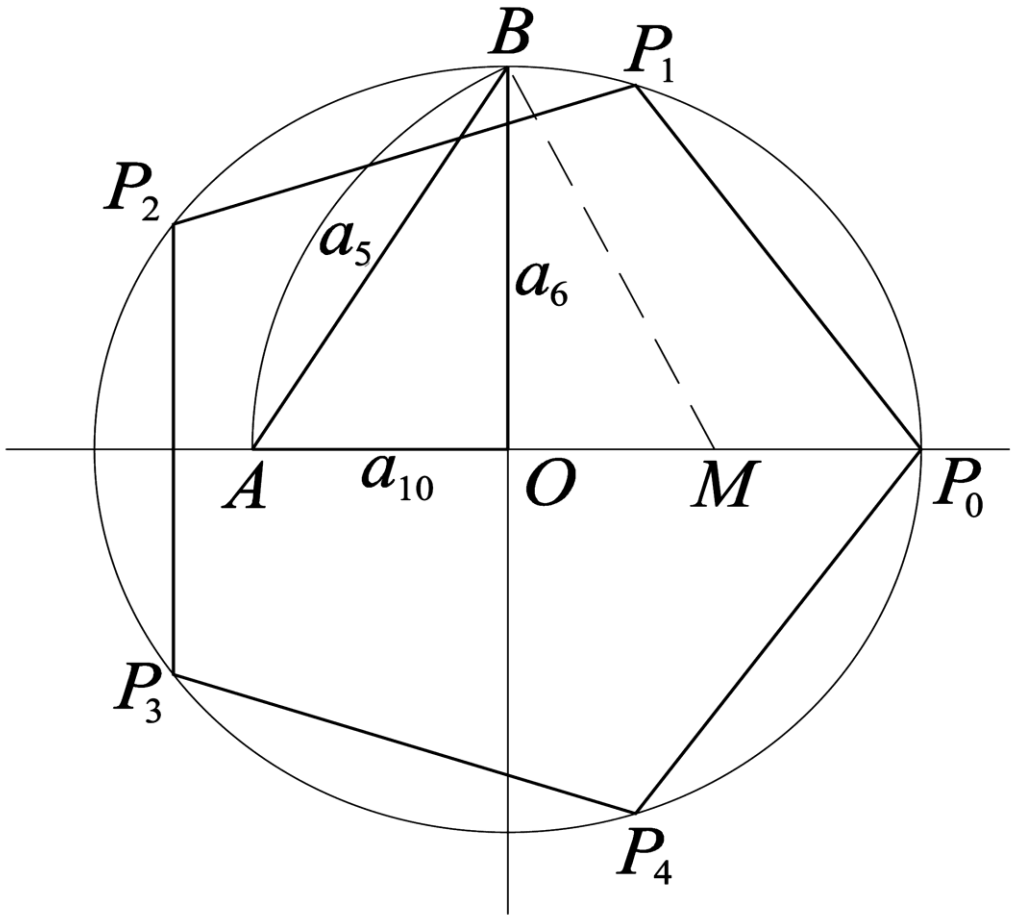
Konstruovatelnost pravidelných mnohoúhelníků

- 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.

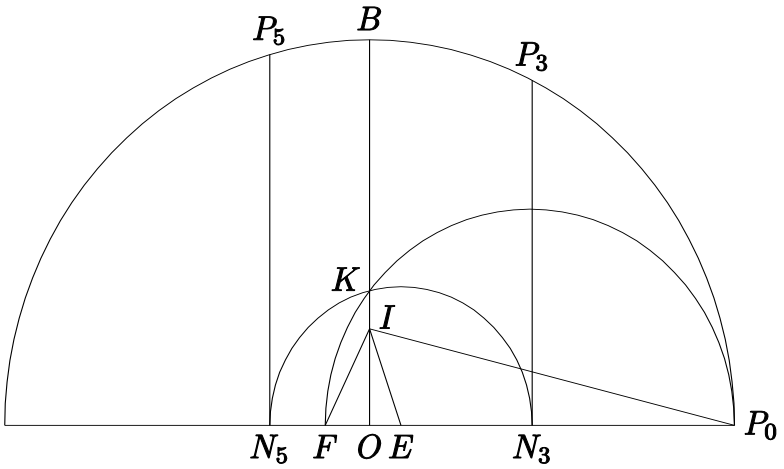
  (poslední kapitola *Disquisitiones arithmeticae*)

  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

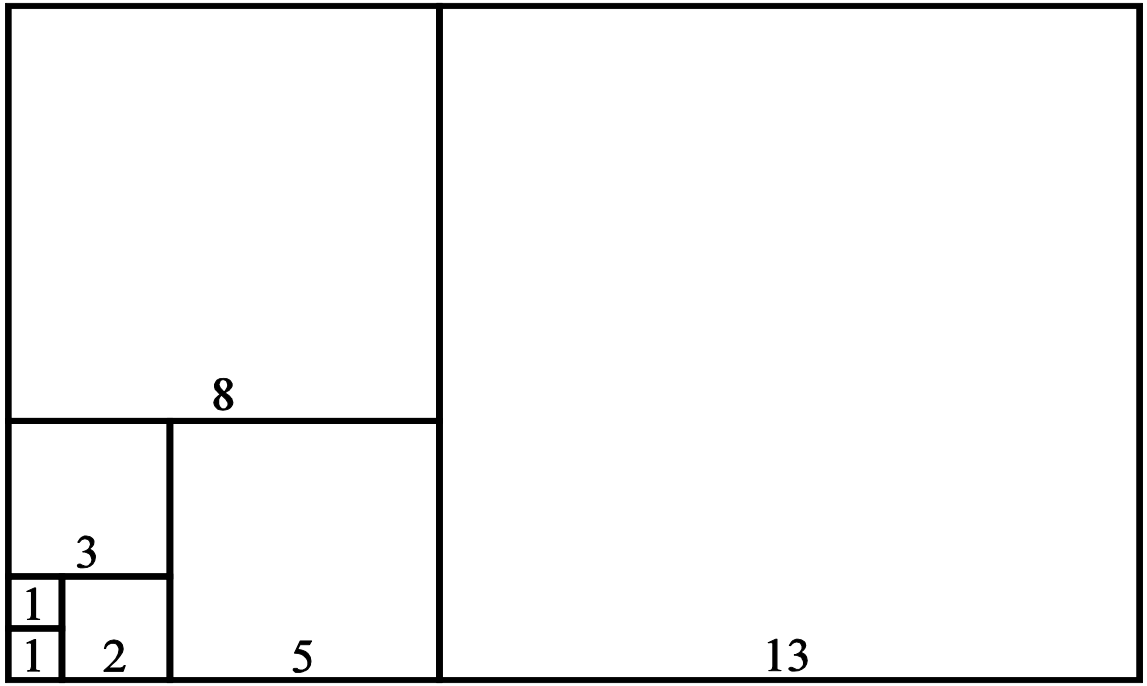
Fibonacci Quarterly, Fibonacci Association

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

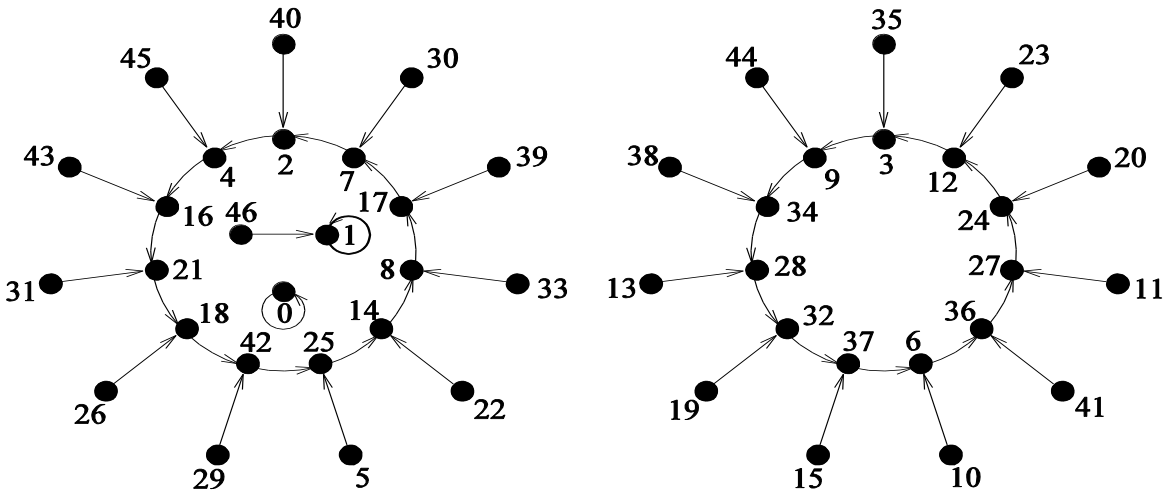
89 + 98 = 187, 187 + 781 … 24 kroků … 8813200023188

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