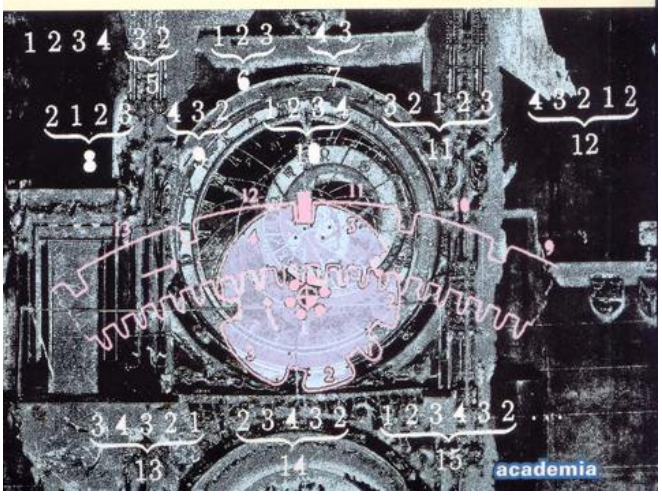
Galileo

Michal Křížek, Lawrence Somer, Alena Šolcová

Kouzlo čísel

Od velkých objevů k aplikacím



academia

Přirozená čísla: 1, 2, 3, ... $\quad \mathbb{N} = \{1, 2, 3, \dots\}$

Prvočísla: 2, 3, 5, 7, 11, 13, ...

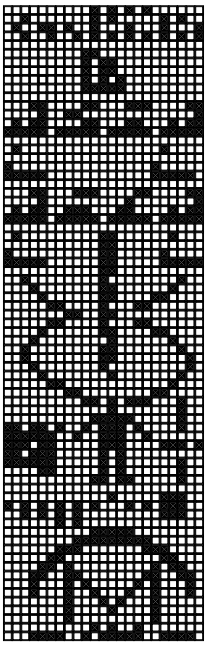
Základní věta aritmetiky. *Jestliže*

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s},$$

kde $p_1 < p_2 < \cdots < p_r$, $q_1 < q_2 < \cdots < q_s$ *jsou prvočísla a* $r, s, \alpha_i, \beta_i \in \mathbb{N}$, *pak*

$$r = s, \quad p_i = q_i, \quad \alpha_i = \beta_i$$

pro každé $i = 1, \dots, r$.



Poselství mimozemským civilizacím ($1679 = 73 \times 23$)

Eukleidova věta. *Prvočísel je nekonečně mnoho.*

D ů k a z . Předpokládejme naopak, že existuje jen konečně mnoho prvočísel $p_1 = 2$, $p_2 = 3$, ... , p_n a položme

$$m = p_1 p_2 \cdots p_n + 1.$$

Protože podíl m/p_i dá vždy zbytek 1, žádné p_i nedělí m. Podle Základní věty aritmetiky je tedy číslo m další prvočíslo, anebo je m dělitelné prvočíslem různým od $p_1, p_2, \ldots, p_n$, což je spor.

Prvočísla jsou surovinou,
z níž máme postavit aritmetiku,
a Eukleidova věta je zárukou,
že pro tento úkol máme
dostatečné množství materiálu.

G. H. Hardy
Obrana matematikova, 1999

V množině přirozených čísel můžeme najít libovolně dlouhé úseky po sobě jdoucích složených čísel. Položme

$$n! = 1 \cdot 2 \cdot 3 \cdots n$$

Příklad. Pro libovolné $n > 1$ uvažujme konečnou posloupnost

$$n! + 2,\ n! + 3, \ldots,\ n! + n,$$

která obsahuje $n - 1$ po sobě jdoucích čísel. Vidíme, že první člen této posloupnosti je dělitelný dvěma, druhý třemi atd. Konečně poslední člen je dělitelný n. Pro $n = 1001$ dostáváme 1000 po sobě následujících složených čísel.

Greenova-Taova věta (2008). *Pro každé $k \in \mathbb{N}$ množina prvočísel obsahuje aritmetickou posloupnost délky k.*

Např. aritmetická posloupnost

$$5,\ 11,\ 17,\ 23,\ 29$$

délky 5 obsahuje pouze prvočísla. Jiná aritmetická posloupnost prvočísel délky 10 je tato:

$$199,\ 409,\ 619,\ 829,\ 1039,\ 1249,\ 1459,\ 1669,\ 1879,\ 2089$$

Ještě delší posloupnost prvočísel je

$$(223092870n + 2236133941)_{n=0}^{15}.$$

Pamětní deska v Oizé připomíná, že M. Mersenne byl duchovním otcem Akademie věd. Byla odhalena ke 400. výročí jeho narození.

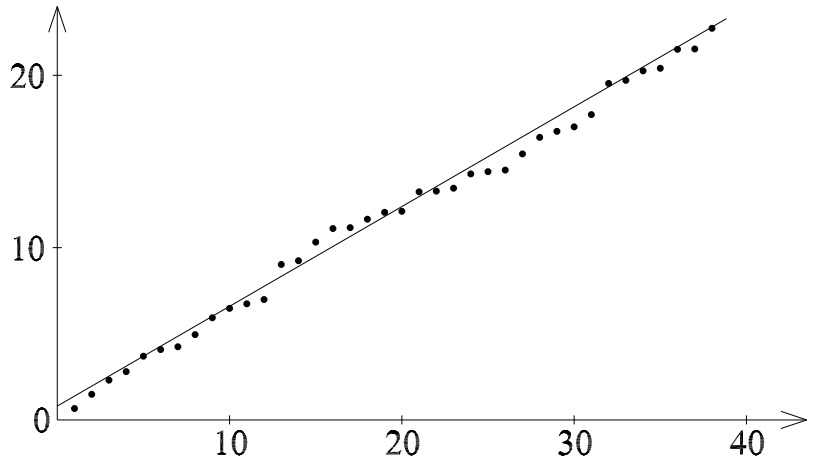
Mersenne studoval mj. čísla tvaru

$$M_p = 2^p - 1,$$

kde p je prvočíslo, která se po něm nazývají *Mersennova čísla.* Jestliže $2^p - 1$ je samo prvočíslo, nazývá se *Mersennovo prvočíslo.* Číslo M_p je prvočíslem, když

$$\begin{aligned} p = &2, 3, 5, 7, 13, 17, 19, 31, 61, 89, \ldots \\ &30402457, 32582657, 37156667, 43112609, \ldots \end{aligned}$$

Pozn. $2^{43112609} - 1 \approx 10^{12978188}$, zatímco počet elementárních částic v pozorovatelné části vesmíru je $\approx 10^{80}$.



Hodnoty $\log_2(\log_2 M(n))$ pro $n = 1, 2, 3, \ldots$, kde $M(1)$, $M(2)$, $M(3)$, $\ldots$ jsou po sobě jdoucí Mersennova prvočísla.

Eukleides (4.–3. stol. př. n. l.): *Pravidelný n-úhelník lze zkonstruovat pomocí pravítka a kružítka, jestliže*

$$n = 2^i 3^j 5^k,$$

kde $n \geq 3$ a $i \geq 0$ jsou celá čísla a $j, k \in \{0, 1\}$.

Pierre de Fermat (1601–1665): *Pro $m = 0, 1, 2, \ldots$ je posloupnost $F_m = 2^{2^m} + 1$ tvořena prvočísly. (Nepravdivé tvrzení.)*

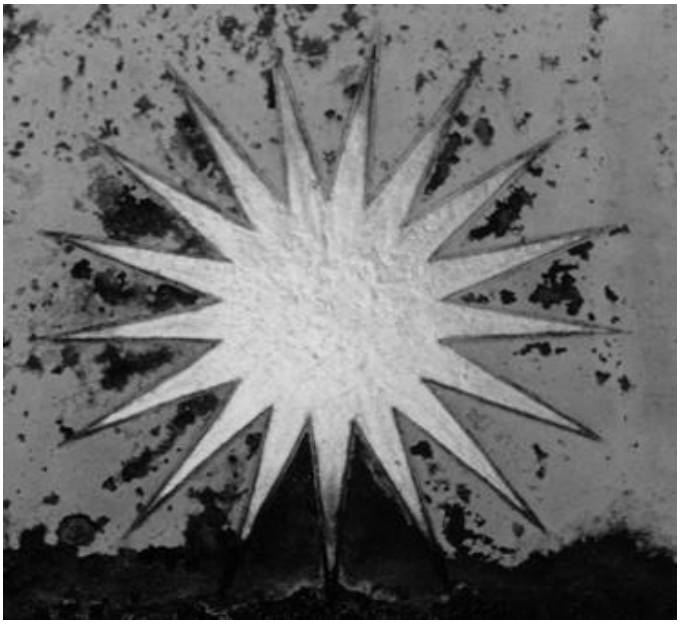
Leonhard Euler (1707–1783): $F_5 = 641 \cdot 6700417$.

Carl Friedrich Gauss (1777–1855): *Pravidelný n-úhelník lze zkonstruovat pomocí pravítka a kružítka právě tehdy, když*

$$n = 2^i F_{m_1} F_{m_2} \cdots F_{m_j},$$

kde $n \geq 3$, $i \geq 0$, $j \geq 0$ a F_{m_1}, $F_{m_2}, \ldots,$ F_{m_j} jsou vzájemně různá Fermatova prvočísla.

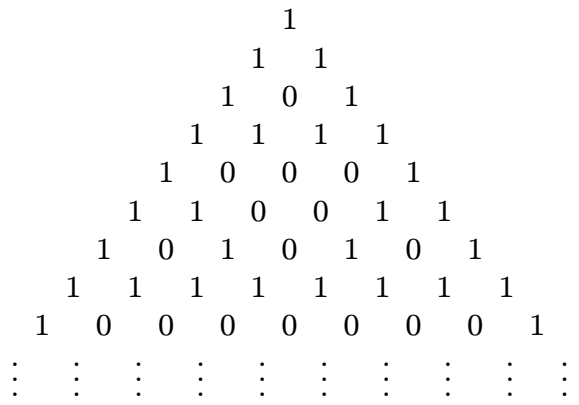
Socha C. F. Gausse v jeho rodném Braunschweigu v Německu. Zlatá sedmnácticípá hvězda je umístěna uprostřed podstavce.

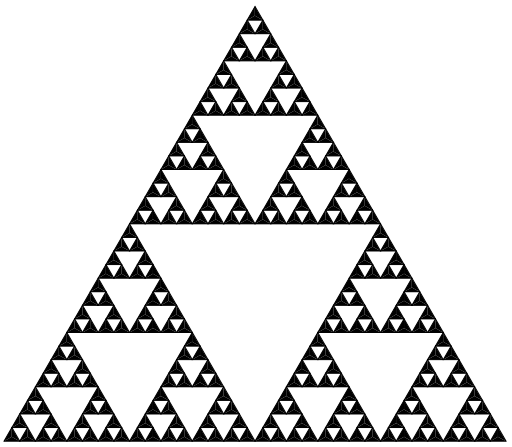


Sedmnácticípá hvězda

Fermatova prvočísla 3, 5, 17, ... a Sierpińského fraktál

Sudá čísla v Pascalově trojúhelníku nahraďme 0 a lichá jedničkou:

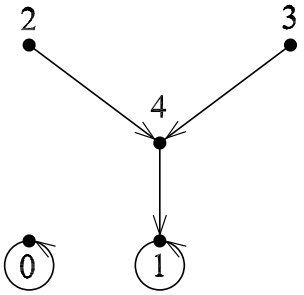




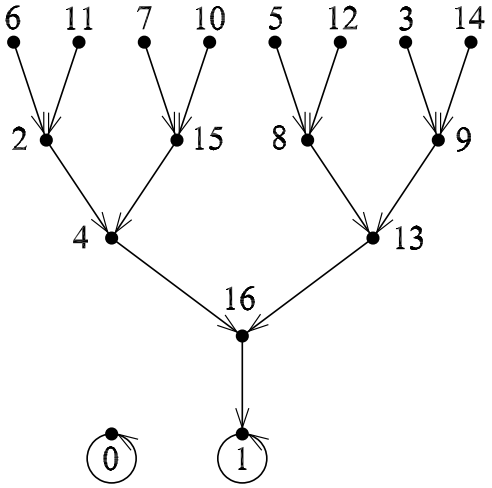
Převedeme-li řádky zapsané ve dvojkové soustavě do desítkové soustavy, dostaneme posloupnost 1, 3, 5, 15, 17, 51, 85, 255, 257, ...

Označme $H = \{0, 1, \ldots, n-1\}$. Pro $a \in H$ nechť existuje orientovaná hrana do vrcholu $b \in H$ tak, že $b \equiv a^2 \pmod{n}$.

Věta. *Graf příslušný n je binární $\Leftrightarrow$ n je Fermatovo prvočíslo.*



$n = 5$



$n = 17$

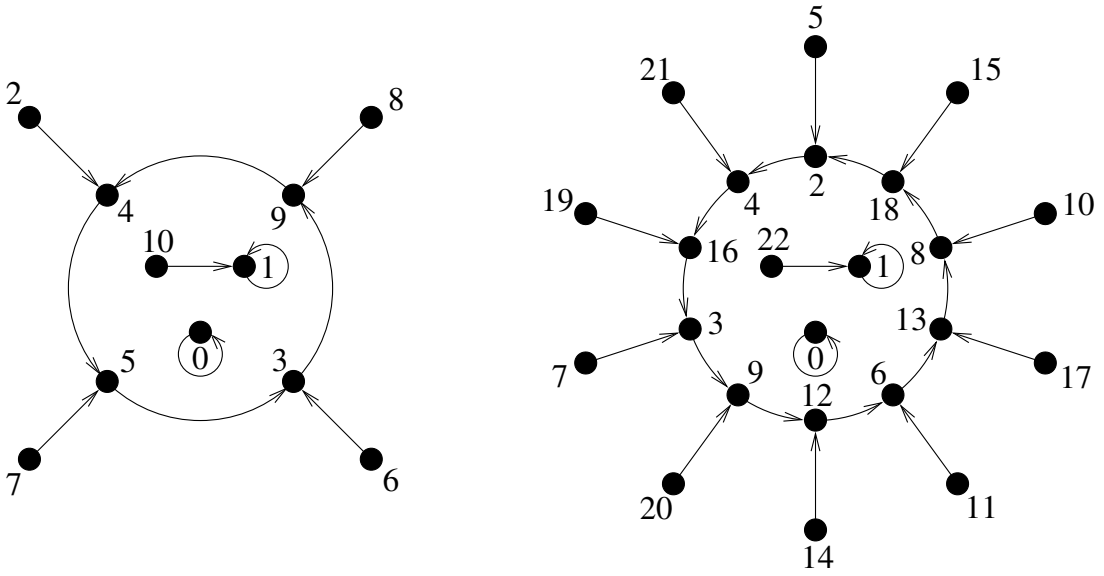
V roce 1819 se francouzská matematička **Sophie Germainová** proslavila částečným důkazem tzv. prvního případu Velké Fermatovy věty, tj. rovnice

$$x^p + y^p = z^p$$

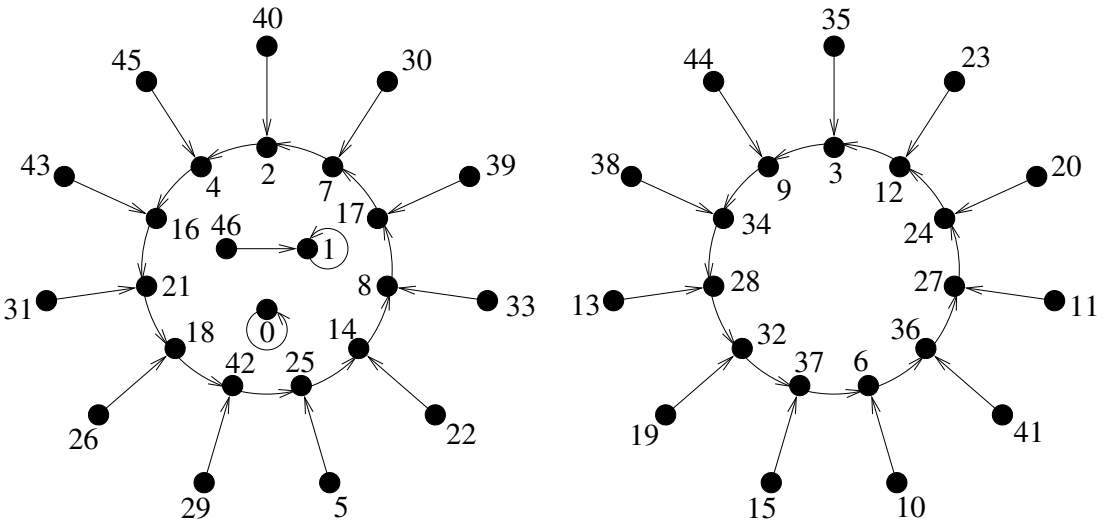
nemá řešení v přirozených číslech pro prvočíselný exponent $p > 2$ takový, že p nedělí součin xyz. Dokázala, že pokud p a $2p+1$ jsou současně prvočísla, pak první případ Velké Fermatovy věty platí pro exponent p.

Liché prvočíslo p, pro něž $2p + 1$ je také prvočíslo, se proto nazývá *prvočíslo Sophie Germainové.*

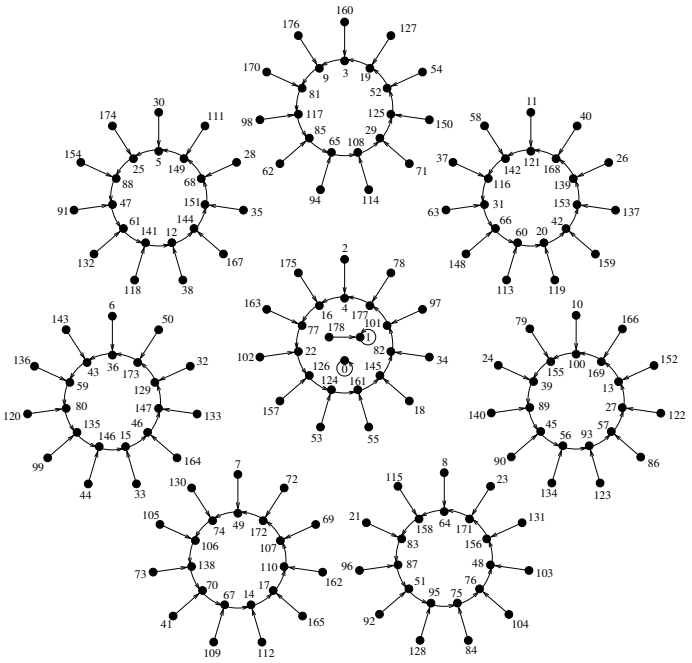
Např. 5, 11 a 23.



Orientované grafy odpovídající $n = 11$ a $n = 23$



Orientovaný graf pro $n = 2 \cdot 23 + 1 = 47$



Orientovaný graf pro $n = 179$

Existuje velké množství dalších zajímavých tříd prvočísel, např.:

prvočísla Cullenova, cyklická, elitní, Eisensteinova, Eukleidova, faktoriální, Fibonacciova, Gaussova, iregulární, jedinečná, Lucasova, multifaktoriální, palindromická, permutační, regulární, Thabitova, Wieferichova, Wilsonova, Woodallova aj.

Studiem prvočísel se zabývá lidstvo již několik tisíciletí. Ale teprve ve 20. století se dospělo k tomu, že prvočísla mohou mít řadu zajímavých technických aplikací.

Rodná čísla od roku 1986 dělitelná prvočíslem 11. Poslední čtyřčíslí je totiž voleno tak, aby celé deseticiferné rodné číslo (odhlédneme-li od lomítka) bylo dělitelné 11. Např. rodné číslo

(1) 975811/0428

(odpovídající narození děvčete dne 11. 8. 1997) je dělitelné 11.

Počítač totiž okamžitě odhalí chybu, jakmile se při zadávání rodného čísla zmýlíme v jedné jeho cifře. Pak rozdíl mezi správným a špatně zadaným rodným číslem bude $\pm c \cdot 10^n$, kde $c \in \{1, 2, \ldots, 9\}$, což nikdy není dělitelné 11, ale může být dělitelné složenými čísly $12, 14, 15, 16, \ldots$.

Napíšeme-li např. omylem 975811/0728 místo čísla v (1), počítač by při dělení dvanácti chybu neodhalil, protože obě čísla jsou dělitelná 12.

Podobně jako rodná čísla jsou chráněny proti případné chybě

- ISBN kódy knižních publikací
- ISSN kódy časopisů
- ISMN kódy hudebních nahrávek
- IČO
- čísla bankovních účtů
- kódy platebních karet
- kódy telefonních karet
- kódy v mobilních telefonech atd. atd.

Čárový kód byl poprvé patentován v USA již v roce 1949. Jeho masové použití je však spojeno až s obrovským pokrokem optoelektrotechniky. V supermarketech zvyšuje rychlost prodeje až o 400 %.

Jednorozměrné a dvourozměrné čárové kódy

Největší dvojciferné prvočíslo 97 se používá k zabezpečení kódu IBAN (International Bank Account Number).

Metoda RSA pro šifrování zpráv pomocí velkých prvočísel

Základní rozdíl mezi pojmy *šifrování* a *kódování* spočívá v tom, že při šifrování se využívá nějaká tajná informace (klíč), bez jejíž znalosti prakticky nelze získat ze zašifrované zprávy její obsah. Naproti tomu kódování je transformace jedné formy zápisu informace do jiné formy, která je z nějakého důvodu pro danou situaci výhodnější (např. ASCII kódy, Morseova abeceda, genetický kód).

$$x^* \equiv x^e \pmod{n} \qquad \text{(zašifrovaná zpráva)},$$

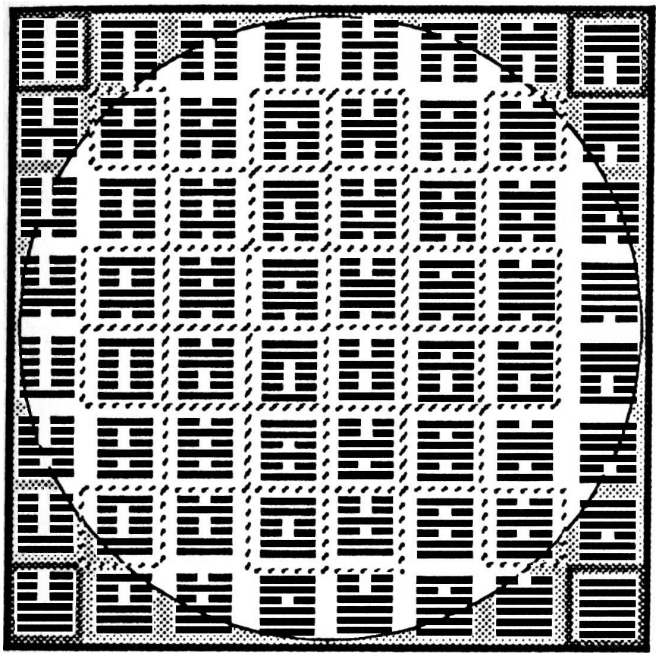
kde e je *šifrovací exponent,* x je přirozené číslo (utajovaná zpráva) a n je součin dvou velkých prvočísel, která nejsou veřejně známa.

$$(x^*)\hat{} \equiv (x^*)^d \pmod{n} \qquad \text{(odšifrovaná zpráva)}.$$

kde *dešifrovací exponent* d není veřejně znám. **Věta:** $(x^*)\hat{} = x$.

Další aplikace prvočísel

- digitální podpis
- hašovací funkce
- generátory pseudonáhodných čísel
- Fermatova transformace
- algoritmy rychlého násobení
- úsporné kódování aminokyselin
- poselství mimozemských civilizacím
- návrh ozubených kol
- řešení akustiky koncertních sálů
- rozpoznávání řeči atd.



První znázornění dvojkové soustavy z 8. století př. n. l.

I když staří Číňané neprováděli se symboly *jin* – *jang* žádné aritmetické operace, nelze jim upřít prioritu ve znázornění čísel zapsaných ve dvojkové soustavě. Tento fenomenální objev našel praktické uplatnění až v dnešní době počítačů, tj. téměř o tři tisíce let později. Počítače totiž zobrazují a zpracovávají veškerou informaci právě ve dvojkové soustavě. A tak i fungování celosvětové sítě internet, e-mailu, faxu, scannerů, kopírek, digitálních kamer, kompaktních disků CD a DVD či mobilních telefonů je vlastně založeno na principech *jin* (=0) a *jang* (=1).

Příroda ale v průběhu evoluce objevila dvojkovou (nebo chceteli čtyřkovou) soustavu již před více než třemi miliardami let. Na dvojšroubovici DNA se nacházejí čtyři druhy bází: adenin A, cytosin C, guanin G a thymin T. Nahradíme-li je postupně dvojicemi 00, 01, 10 a 11, bude každému vláknu DNA odpovídat posloupnost nul a jedniček, která tak vlastně představuje genetickou informaci zapsanou ve dvojkové soustavě.

Šifrování pomocí symetrického klíče

Kryptografie se zabývá ochranou přenosu a uchování dat, především zajištěním jejich důvěrnosti, integrity dat (tj. obsahové neporušenosti), autentičnosti informací a nepopiratelností jejich původu apod.

Na množině $\{0, 1\}$ definujme operaci sčítání $\oplus$ takto:

$$0 \oplus 0 = 0, \quad 1 \oplus 0 = 1, \quad 0 \oplus 1 = 1, \quad 1 \oplus 1 = 0.$$

$100001110\ldots$ tajná zpráva,
$\underline{000101101}\ldots$ šifrovací klíč,
$100100011\ldots$ přenášená zašifrovaná zpráva,
$\underline{000101101}\ldots$ dešifrovací klíč,
$100001110\ldots$ odšifrovaná zpráva.

Co knížka Kouzlo čísel ještě obsahuje?

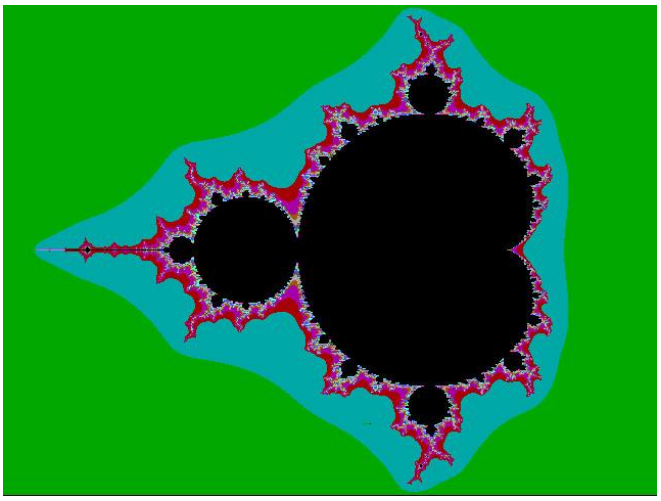
- samoopravné kódy
- jak teorie čísel souvisí s bicím strojem pražského orloje
- o jakou matematiku se opírá tradiční čínský kalendář
- Gaussův algoritmus výpočtu Velikonoc
- pokrytí roviny pravidelnými mnohoúhelníky
- eukleidovskou konstrukci pravidelného sedmnáctiúhelníku
- co jsou pseudoprvočísla
- jak spolu souvisí chaos, fraktály a teorie čísel
- historické poznámky
- aplikace Fermatovy vánoční věty
- 160 dalších vět z teorie čísel
- některé otevřené problémy z teorie čísel

Dirichletův princip. *Nechť $n \in \mathbb{N}$. Je-li více než n předmětů rozděleno do n skupin, pak v alespoň jedné skupině se nacházejí alespoň dva předměty.*

Je známo, že žádný člověk nemá více než $n = 100\,000$ vlasů a že Praha má více než jeden milion obyvatel. Její obyvatele rozdělme do skupin tak, že do i-té skupiny dáme všechny obyvatele Prahy, kteří mají právě i vlasů, kde $i = 0, 1, \ldots, n$. Protože Pražanů je více než počet skupin, musí být podle Dirichletova principu v alespoň jedné skupině alespoň dva občané (ve skutečnosti mnohem více) se stejným počtem vlasů.

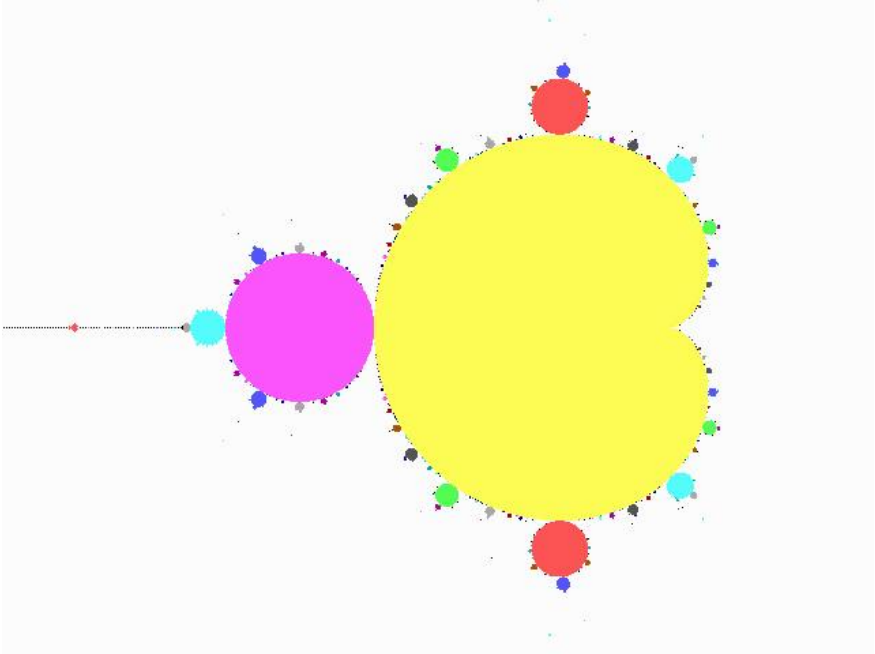
Logistická rovnice

$$y_{n+1} = y_n^2 + c, \quad y_0 = 0$$



Mandelbrotova množina

Fibonacciho čísla: 1, 1, 2, 3, 5, 8, 13, 21, 34, ...



Mandelbrotova množina