



ZÁPADOČESKÁ
UNIVERZITA
V PLZNI



WWW.KMA.ZCU.CZ
SINCE 1954

Bertrandův postulát aneb jak hustě jsou rozložena prvočísla?

Pavel Drábek

Katedra matematiky a Evropské centrum NTIS (Nové technologie pro informační společnost)
Fakulta aplikovaných věd, Západočeská univerzita v Plzni

VŠB – TU Ostrava, 23. ledna, 2014

Edmund Landau

mezinárodní kongres
matematiků 1912

① Goldbachova hypotéza:

"Každé sudé číslo větší než 2 lze vyjádřit jako součet dvou prvočísel."

(1742 v korespondenci mezi Goldbachem a Eulerem)

② Problém prvočíselných dvojčat:

"Je jich ∞ mnoho?"

③ Legendrova hypotéza:

" $\forall n \in \mathbb{N} \exists p$ (prvočíslo): $n^2 < p < (n+1)^2$."

④ " $\exists \infty$ mnoho prvočísel p tvaru $p = n^2 + 1$ pro nějaké $n \in \mathbb{N}$?"

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡

9245 513, 9245 557, 9245 591, 9245 611, 9245 617, 9245 627, 9245 633,
9245 653, 9245 689, 9245 711, 9245 729, 9245 741, 9245 759, 9245 777,
9245 791, 9245 813, 9245 851, 9245 911, 9245 921, 9245 927, 9245 947,
9245 959, 9245 963, 9245 969, 9245 987, 9246 007, 9246 019, 9246 031,
9246 037, 9246 047, 9246 053, 9246 071, 9246 077, 9246 131, 9246 151,
9246 163, 9246 199, 9246 227, 9246 229, 9246 233, 9246 287, 9246 301,
9246 323, 9246 329, 9246 343, 9246 353, 9246 359, 9246 371, 9246 379,
9246 403, 9246 427, 9246 439, 9246 467, 9246 473, 9246 491, 9246 551,
9246 553, 9246 557, 9246 569, 9246 571, 9246 577, 9246 593, 9246 599,
9246 617, 9246 631, 9246 637, 9246 647, 9246 661, 9246 683, 9246 701,
9246 703, 9246 709, 9246 761, 9246 767, 9246 779, 9246 803, 9246 821,
9246 841, 9246 847, 9246 859, 9246 869, 9246 877, 9246 889, 9246 899,
9246 907, 9246 917, 9246 931, 9246 949, 9246 967, 9246 971, 9246 973,
9247 009, 9247 019, 9247 033, 9247 057, 9247 079, 9247 087, 9247 123,
9247 157, 9247 169, 9247 171, 9247 177, 9247 211, 9247 283, 9247 289,
9247 307, 9247 339, 9247 349, 9247 351, 9247 361, 9247 379, 9247 397,
9247 409, 9247 423, 9247 463, 9247 477, 9247 489, 9247 501, 9247 519,
9247 529, 9247 543, 9247 573, 9247 577, 9247 583, 9247 597, 9247 603,
9247 613, 9247 619, 9247 621, 9247 663, 9247 687, 9247 691, 9247 727,
9247 739, 9247 741, 9247 751, 9247 757, 9247 769, 9247 787, 9247 793,
9247 801, 9247 829, 9247 831, 9247 853, 9247 877, 9247 879, 9247 907,
9247 913, 9247 921, 9247 933, 9247 937, 9247 939, 9247 969, 9247 993,
9247 999, 9248 009, 9248 011, 9248 059, 9248 069, 9248 081, 9248 089,
9248 101, 9248 111, 9248 123, 9248 147, 9248 159, 9248 171, 9248 189,
9248 201, 9248 219, 9248 233, 9248 243, 9248 249, 9248 251, 9248 273,

Bertrandův postulát:

$$\forall n \geq 1 \exists p \text{ (prvočíslo)} : n < p \leq 2n$$

Joseph Bertrand 1845 (ověřil $\forall n < 3\,000\,000$)

Pafnuty Chebyshev 1850 1. známý důkaz

.....

Ramanujan

.....

Paul Erdős 1932 (1. článek v 19ti letech)
elementární důkaz založený na dolním
a horním odhadu kombinačního čísla

$$? \leq \binom{2n}{n} \leq ?$$

Myšlenka důkazu B.p. : SPOREM

$\exists n \geq 1$: mezi n a $2n$ neleží prvočíslo



$$L = \frac{4^n}{2n} \leq \binom{2n}{n} \leq (2n)^{\sqrt{2n}} 4^{\frac{2}{3}n} = P$$

ukážeme, že pro $n > 4000$ platí $L > P$ (⚡)

Pro $n = 1, 2, \dots, 4000$ lze B.p. prověřit empiricky
(Eratosthenovo síto, program, ...)

p : 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001

Out[12]= (2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291, 1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1409, 1423, 1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, 1493, 1499, 1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889, 1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999, 2003, 2011, 2017, 2027, 2029, 2039, 2053, 2063, 2069, 2081, 2083, 2087, 2089, 2099, 2111, 2113, 2129, 2131, 2137, 2141, 2143, 2153, 2161, 2179, 2203, 2207, 2213, 2221, 2237, 2239, 2243, 2251, 2267, 2269, 2273, 2281, 2287, 2293, 2297, 2309, 2311, 2333, 2339, 2341, 2347, 2351, 2357, 2371, 2377, 2381, 2383, 2389, 2393, 2399, 2411, 2417, 2423, 2437, 2441, 2447, 2459, 2467, 2473, 2477, 2503, 2521, 2531, 2539, 2543, 2549, 2551, 2557, 2579, 2591, 2593, 2609, 2617, 2621, 2633, 2647, 2657, 2659, 2663, 2671, 2677, 2683, 2687, 2689, 2693, 2699, 2707, 2711, 2713, 2719, 2729, 2731, 2741, 2749, 2753, 2767, 2777, 2789, 2791, 2797, 2801, 2803, 2819, 2833, 2837, 2843, 2851, 2857, 2861, 2879, 2887, 2897, 2903, 2909, 2917, 2927, 2939, 2953, 2957, 2963, 2969, 2971, 2999, 3001, 3011, 3019, 3023, 3037, 3041, 3049, 3061, 3067, 3079, 3083, 3089, 3109, 3119, 3121, 3137, 3163, 3167, 3169, 3181, 3187, 3191, 3203, 3209, 3217, 3221, 3229, 3251, 3253, 3257, 3259, 3271, 3299, 3301, 3307, 3313, 3319, 3323, 3329, 3331, 3343, 3347, 3359, 3361, 3371, 3373, 3389, 3391, 3407, 3413, 3433, 3449, 3457, 3461, 3463, 3467, 3469, 3491, 3499, 3511, 3517, 3527, 3529, 3533, 3539, 3541, 3547, 3557, 3559, 3571, 3581, 3583, 3593, 3607, 3613, 3617, 3623, 3631, 3637, 3643, 3659, 3671, 3673, 3677, 3691, 3697, 3701, 3709, 3719, 3727, 3733, 3739, 3761, 3767, 3769, 3779, 3793, 3797, 3803, 3821, 3823, 3833, 3847, 3851, 3853, 3863, 3877, 3881, 3889, 3907, 3911, 3917, 3919, 3923, 3929, 3931, 3943, 3947, 3967, 3989, 4001, 4003, 4007, 4013, 4019, 4021, 4027, 4049, 4051, 4057, 4073, 4079, 4091, 4093, 4099, 4111, 4127, 4129, 4133, 4139, 4153, 4157, 4159, 4177, 4201, 4211, 4217, 4219, 4229, 4231, 4241, 4243, 4253, 4259, 4261, 4271, 4273, 4283, 4289, 4297, 4327, 4337, 4339, 4349, 4357, 4363, 4373, 4391, 4397, 4409, 4421, 4423, 4441, 4447, 4451, 4457, 4463, 4481, 4483, 4493, 4507, 4513, 4517, 4519, 4523, 4547, 4549, 4561, 4567, 4583, 4591, 4597, 4603, 4621, 4637, 4639, 4643, 4649, 4651, 4657, 4663, 4673, 4679, 4691, 4703, 4721, 4723, 4729, 4733, 4751, 4759, 4783, 4787, 4789, 4793, 4799,

ODHAD ZDOLA

$$\forall n \geq 1 : \binom{2n}{n} \geq \frac{4^n}{2n}$$

Důkaz: $4^n = 2^{2n} = (1+1)^{2n} =$

$$= \binom{2n}{0} + \binom{2n}{1} + \dots + \binom{2n}{n} + \dots + \binom{2n}{2n-1} + \binom{2n}{2n}$$
$$= \boxed{\binom{2n}{0} + \binom{2n}{2n}} + \boxed{\binom{2n}{1}} + \dots + \boxed{\binom{2n}{n}} + \dots + \boxed{\binom{2n}{2n-1}}$$

$\underbrace{\hspace{15em}}_{2n \text{ členů}}$

$\underbrace{\hspace{15em}}_{= 2}$

$$\binom{2n}{n} \geq \text{průměr} = \frac{2^{2n}}{2n} = \frac{4^n}{2n}.$$

největší

Q.E.D.

ODHAD STORA

Označení: $\binom{2n}{n} = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

$\sigma_p(a)$ je největší mocnina p , která dělí číslo a
např. $\alpha_1 = \sigma_{p_1}(\binom{2n}{n})$ atd.

platí: $\sigma_p(ab) = \sigma_p(a) + \sigma_p(b)$

$$\sigma_p\left(\frac{a}{b}\right) = \sigma_p(a) - \sigma_p(b)$$

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{\sigma_p(\binom{2n}{n})}$$

$$\left(\begin{array}{l} 2n(2n-1)(2n-2)\dots = \binom{2n}{n} n(n-1)(n-2)\dots n(n-1)(n-2)\dots 1 \\ \Rightarrow \text{prvočíslo } p \text{ v rozkladu } \binom{2n}{n} \text{ je } \leq 2n! \end{array} \right)$$

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{\sigma_p \left(\binom{2n}{n} \right)} =$$

$$= \prod_{p \leq \sqrt{2n}} p^{\sigma_p \left(\binom{2n}{n} \right)} \cdot \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^{\sigma_p \left(\binom{2n}{n} \right)}$$

$$\prod_{\frac{2n}{3} < p \leq n} p^{\sigma_p \left(\binom{2n}{n} \right)} \cdot \left(\prod_{n < p \leq 2n} p^{\sigma_p \left(\binom{2n}{n} \right)} \right)$$

předpoklad $\prod_{n < p \leq 2n} p^{\sigma_p \left(\binom{2n}{n} \right)} = 1$

Legendrova věta: Číslo $N!$ obsahuje prvočíslo p ve svém rozkladu právě

$$\sum_{k \geq 1} \left[\frac{N}{p^k} \right] \quad \begin{array}{l} \text{— krát.} \\ \text{celá část} \end{array}$$

Důkaz: $N(N-1)(N-2)\dots 1 = N! = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

1. v rozkladu $N!$ je $\left[\frac{N}{p} \right]$ činitelů dělitelných p
 2. — " — $\left[\frac{N}{p^2} \right]$ — " — p^2
- a ty musíme přidat

atd.

Q.E.D.

$$\forall p : p^{\sigma_p \left(\binom{2n}{n} \right)} \leq 2n$$

Důkaz: $\sigma_p \left(\binom{2n}{n} \right) = \sigma_p(2n!) - \sigma_p(n!n!) =$

$$= \sigma_p(2n!) - 2\sigma_p(n!) = \sum_{k \geq 1} \left[\frac{2n}{p^k} \right] - 2 \sum_{k \geq 1} \left[\frac{n}{p^k} \right]$$

Legendrova věta

$$= \sum_{k \geq 1} \left(\underbrace{\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right]}_{\leq 1} \right) \leq \max \{ r : p^r \leq 2n \}$$

(= 0 pokud $p^k > 2n$)

$$\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] < \frac{2n}{p^k} - 2 \left(\frac{n}{p^k} - 1 \right) = 2$$

Q.E.D.

JINÝMI SLOVY:

NEJVYŠŠÍ MOCNINA p , KTERÁ DĚLÍ
ČÍSLO $\binom{2n}{n}$ JE NEJVÝŠE ROVNA $2n$

DŮSLEDEK: Prvocísla $p > \sqrt{2n}$ se objeví
v rozkladu čísla $\binom{2n}{n}$
nejvýše jednou!

DŮLEŽITÉ POZOROVÁNÍ:

Prvocísla $\frac{2n}{3} < p \leq n$ ($n \geq 3$)

se v rozkladu čísla $\binom{2n}{n}$
neobjeví vůbec!

Důkaz: $\frac{2n}{3} < p \Rightarrow 3p > 2n \Rightarrow$

$$\underbrace{2n!}_{\cancel{p \cdot 2p}} = \binom{2n}{n} \cdot \underbrace{n!}_{\cancel{p}} \cdot \underbrace{n!}_{\cancel{p}}$$

↑
žádné p

Q.E.D.

ČÁSTEČNÉ SHRNUTÍ:

$$\binom{2n}{n} = \underbrace{\prod_{p \leq \sqrt{2n}} p^{\sigma_p\left(\binom{2n}{n}\right)}}_{\leq (2n)^{\sqrt{2n}}} \cdot \underbrace{\prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^{\sigma_p\left(\binom{2n}{n}\right)}}_{\leq (?)}$$

$$\underbrace{\prod_{\frac{2n}{3} < p \leq n} p^{\sigma_p\left(\binom{2n}{n}\right)}}_{= 1}$$

$$\underbrace{\prod_{n < p \leq 2n} p^{\sigma_p\left(\binom{2n}{n}\right)}}_{= 1 \text{ podle předpokladu}}$$

ZBÝVA' ODHADNOUT

$$\prod_{\sqrt{n} < p \leq \frac{2n}{3}} p^{\sigma_p\left(\binom{2n}{n}\right)} !$$

$$\forall N \geq 1 : \prod_{p \leq N} p \leq 4^N$$

Důkaz: 1. $N = 1, 2, 3, 4, 5$ platí. Dále
mat. indukce vzhledem k N .

2. N je sudé:

$$\prod_{p \leq N} p = \prod_{p \leq N-1} p \leq 4^{N-1} \leq 4^N$$

(indukční předpoklad)

3. N je liché: $\exists m : N = 2m + 1$

$$\prod_{p \leq N} p = \left(\prod_{p \leq m+1} p \right) \cdot \left(\prod_{m+2 \leq p \leq 2m+1} p \right)$$

$\leq 4^{m+1}$
(indukční předpoklad)

všechna tato prvočísla
dělí číslo $\binom{2m+1}{m}$
 $\leq \binom{2m+1}{m} \leq 2^{2m}$

$$\leq 4^{m+1} \cdot 2^{2m} = 4^{2m+1} = 4^N$$

$$2^{2m+1} = (1+1)^{2m+1} = \binom{2m+1}{0} + \dots + \binom{2m+1}{m} + \binom{2m+1}{m+1} + \dots + \binom{2m+1}{2m+1}$$

$\uparrow \qquad \qquad \uparrow$
 $= 2 \binom{2m+1}{m}$

$$\Rightarrow \cancel{2} \binom{2m+1}{m} \leq 2^{\cancel{2m+1}}$$

Q.E.D.

SHRNUTÍ:

$$\binom{2n}{n} = \underbrace{\prod_{p \leq \sqrt{2n}} p^{\sigma_p\left(\binom{2n}{n}\right)}}_{\leq (2n)^{\sqrt{2n}}} \underbrace{\prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^{\sigma_p\left(\binom{2n}{n}\right)}}_{\leq 4^{\frac{2n}{3}}}$$

$$\underbrace{\prod_{\frac{2n}{3} < p \leq n} p^{\sigma_p\left(\binom{2n}{n}\right)}}_{=1} \underbrace{\prod_{n < p \leq 2n} p^{\sigma_p\left(\binom{2n}{n}\right)}}_{=1}$$

ODHAD SHORA :

$$\binom{2n}{n} \leq (2n)^{\sqrt{2n}} \cdot 4^{\frac{2n}{3}}$$

$$\frac{4^n}{2n} \leq \binom{2n}{n} \leq (2n)^{\sqrt{2n}} 4^{\frac{2n}{3}}$$

Ukážeme, že

$$\frac{4^n}{2n} \leq (2n)^{\sqrt{2n}} 4^{\frac{2n}{3}} \quad (*)$$

neplatí pro $n \geq 4000$!

Důkaz: $2^k = (1+1)^k = \binom{k}{0} + \binom{k}{1} + \dots > 1+k \Rightarrow$

$$2n = \left(\sqrt[6]{2n}\right)^6 < (\lceil \sqrt[6]{2n} \rceil + 1)^6 < \left(2^{\lceil \sqrt[6]{2n} \rceil}\right)^6 = 2^{6\lceil \sqrt[6]{2n} \rceil} \leq$$

$$\leq 2^{6\sqrt[6]{2n}}$$

$$(*) \Leftrightarrow 4^{\frac{n}{3}} \leq (2n)^{\sqrt{2n}+1} \Leftrightarrow 2^{2n} \leq (2n)^{3(1+\sqrt{2n})}$$

$$\begin{aligned}
 2^{2n} &\leq (2n)^{3(1+\sqrt{2n})} < 2^{6\sqrt{2n} [3(1+\sqrt{2n})]} = \\
 &= 2^{\underbrace{6\sqrt{2n} (18 + 18\sqrt{2n})}_{< 2\sqrt{2n} \text{ (pokud } n \geq 50)}} < 2^{20\sqrt{2n} \sqrt{2n}} = \\
 &= 2^{20} (2n)^{2/3}
 \end{aligned}$$

$$2n < 20 \cdot (2n)^{2/3}$$

$$(2n)^{1/3} < 20$$

$$n < 4000$$



Q.E.D.

Děkuji za pozornost!