Úloha č.1

Dělitelnost a prvočísla

Mirko Rokyta, KMA MFF UK Praha
Janov, 12.10.2013

Menu:

- Různé dělitelnosti, třeba 11 a 7 (aneb Jak zfalšovat rodné číslo).
- Prvočísla: které je nejlepší, které je největší a jak jsou hustá.
- Spočteme 4 příklady, které by mohly pomoci v olympiádě.
- Kolik let měl Gauss, když už bylo jasné, že je to genius?
- Co je Ulamova prvočíselná spirála?
- Co je hypotéza prvočíselných dvojčat, Goldbachova hypotéza, Riemannova hypotéza, aneb jak (ne)vydělat milion dolarů.
- A co na to Sheldon Cooper?

1 Trochu o kritériích dělitelnosti

Dobře známá jsou kritéria, určující, kdy je nějaké přirozené číslo a dělitelné následujícími čísly:

2	poslední cifra a je sudá (tj. dělitelná dvěma)
3	ciferný součet a je dělitelný 3
4	poslední dvojčíslí a je dělitelné 4
5	poslední cifra a je 0 nebo 5 (tj. dělitelná pěti)
(6	a je dělitelné 2 a 3)
8	poslední trojčíslí a je dělitelné 8
9	ciferný součet a je dělitelný 9
10	poslední cifra zkoumaného čísla je 0

7? 11? ...

Obecnější než zkoumat dělitelnost je zkoumat zbytek při dělení.

Definice. Uvažujme celá čísla a, b a přirozené n (tj. $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$) a označme symbolem "$a \bmod n$" zbytek při dělení čísla a číslem n.

Řekneme, že a je **kongruentní** s b **modulo** n, pokud je $a \bmod n = b \bmod n$, tedy pokud je zbytek při dělení a/n a b/n tentýž. Píšeme:

$$a \equiv b \pmod{n}\,.$$

Příklady:

$11 \bmod 2 = 1$, $53 \bmod 7 = 4$,
$11 \equiv 1 \pmod 2$, $53 \equiv 4 \pmod 7$,
$22 \equiv 71 \pmod 7$, $10 \equiv -1 \pmod{11}$.

Platí:

$$a \equiv b \pmod{n} \qquad \Longleftrightarrow \qquad n \text{ dělí } (a-b)\,.$$

2 Modulární aritmetika

. . . aneb počítání s kongruencemi.

- Dobrá zpráva č.1: s modulárním počítáním se setkáváme odmalička:

  hodiny, týdny, roky . . . $14 \equiv 2 \pmod{12}$, $730 \equiv 0 \pmod{365}$,. . .

- Dobrá zpráva č.2: sčítání, odečítání, násobení i umocnění kongruencí je snadné:

Tvrzení 2.1.

$$\begin{aligned} a_1 &\equiv b_1 \pmod{n} \\ a_2 &\equiv b_2 \pmod{n} \end{aligned}$$

$$\Downarrow$$

$$\begin{aligned} (a_1 + a_2) &\equiv (b_1 + b_2) \pmod{n} \\ (a_1 - a_2) &\equiv (b_1 - b_2) \pmod{n} \\ (a_1 \cdot a_2) &\equiv (b_1 \cdot b_2) \pmod{n} \\ a_1^k &\equiv b_1^k \pmod{n} \qquad \text{pro } k \in \mathbb{N}\,. \end{aligned}$$

Příklady:

- $14 \equiv 2 \pmod{12}$, $23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 + 23 \equiv 2 + 11 \pmod{12}$
  $\Rightarrow \quad 37 \equiv 13 \equiv 1 \pmod{12}$
- $14 \equiv 2 \pmod{12}$, $23 \equiv 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 2 \cdot 11 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 \equiv 22 \pmod{12}$
  $\Rightarrow \quad 14 \cdot 23 = 322 \equiv 10 \pmod{12}$

- $10 \equiv -1 \pmod{11}$

  $\Rightarrow \quad 10^k \equiv (-1)^k \pmod{11}, \qquad k \in \mathbb{N},$

  $\Rightarrow \quad a_k 10^k \equiv a_k (-1)^k \pmod{11}, \quad a_k \in \{0, \ldots, 9\},$

  $\Rightarrow \quad \boxed{\sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k (-1)^k \pmod{11}.}$

$\Rightarrow$

Tvrzení 2.2. *Číslo $a \in \mathbb{N}$, jehož dekadický zápis je*

$$a = \overline{a_n a_{n-1} \cdots a_1 a_0}$$

je dělitelné 11 *právě tehdy, když je dělitelné* 11 *číslo*

$$a_0 - a_1 + a_2 - \cdots + (-1)^n a_n \,.$$

(Dokonce platí: obě čísla dávají při dělení 11 stejné zbytky).

Příklady:

- Je číslo $9\,888\,888\,888$ dělitelné číslem 11?

  Odpověď:

  $$9\,888\,888\,888 \equiv 8 - 8 + \cdots + 8 - 9 = -1 \equiv 10 \pmod{11}.$$

  Číslo $9\,888\,888\,888$ není dělitelné číslem 11, dokonce víme, že při dělení dostaneme zbytek 10.

- Rodná čísla jsou dělitelná 11. (Opatření proti zfalšování rodného čísla... které všichni znají).

  $$930106/1213 \;\Rightarrow\; 9301061213 \;\Rightarrow\; 11 - 15 = -4$$

  ... falešné rodné číslo.

Dělitelnost třemi:

- $10 \equiv 1 \pmod{3}$

  $\Rightarrow \quad 10^k \equiv 1^k \pmod{3}, \qquad k \in \mathbb{N},$

  $\Rightarrow \quad a_k 10^k \equiv a_k \pmod{3}, \quad a_k \in \{0, \ldots, 9\},$

  $\Rightarrow \quad \boxed{\sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k \pmod{3}.}$

Tím je ukázáno, že přirozené číslo dává při dělení třemi stejný zbytek jako jeho ciferný součet.

Dělitelnost sedmi:

- $10 \equiv 3 \pmod 7$
  $\Rightarrow \quad 10^k \equiv 3^k \pmod 7, \qquad k \in \mathbb{N},$
  $\Rightarrow \quad a_k 10^k \equiv a_k 3^k \pmod 7, \quad a_k \in \{0, \ldots, 9\},$
  $\Rightarrow \quad \boxed{\sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k 3^k \pmod 7.}$

Příklad:
Určete zbytek při dělení sedmi čísla 1 111 111.
Řešení:
$1\,111\,111 \equiv 1 + 3 + 3^2 + 3^3 + 3^4 + 3^5 + 3^6 = \frac{3^7-1}{3-1} = 1093 \pmod 7$
$1093 \equiv 3 + 9 \cdot 3 + 0 \cdot 3^2 + 1 \cdot 3^3 = 57 \equiv 1 \pmod 7.$

3 Prvočísla a některé jejich vlastnosti

Prvočíslo: přirozené číslo větší než 1 dělitelné jen sebou samým a jedničkou (tj. 1 není prvočíslo).

První prvočísla jsou:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 \ldots$$

Přirozená čísla, různá od jedné, která nejsou prvočísla, se nazývají složená čísla. Každé složené číslo lze jednoznačně napsat jako součin prvočísel.

Základní otázka: Kolik je prvočísel a jak jsou rozložena mezi ostatními přirozenými čísly?

Věta 3.1. *Prvočísel je nekonečně mnoho.*

Dukaz (sporem): Nechť existuje jen konečně mnoho prvočísel, $p_1, p_2, \ldots p_n$ a nechť je to úplný seznam všech prvočísel.

Potom číslo $x = p_1 \cdot p_2 \cdots p_n + 1$ není dělitelné žádným z těchto prvočísel, jelikož při dělení dostaneme vždy zbytek 1.

Tedy číslo x musí být buď prvočíslo, nebo musí být dělitelné nějakým jiným prvočíslem, jiným než $p_1, p_2, \ldots, p_n$.

To ale znamená, že množina prvočísel z počátku důkazu nebyla úplná, což je spor s předpokladem.

(Tento důkaz podal už Eukleidés.)

"Nejlepší" prvočíslo?

"The best number is 73. Because 73 is the 21st prime number. Its mirror (37) is the 12th prime number and its mirror (21) is the product of multiplying 7 and 3. In binary, 73 is a palindrome, 1001001, which backwards again is 1001001"

[TBBT, s04e10]

Je čas něco spočítat.

4 Čtyři (návodné) příklady

Příklad 1. Určete, pro které dvojice prvočísel p, q platí $p + q^2 = q + p^3$.

Řešení.

1. Pro $p = q$ bychom dostali $p + p^2 = p + p^3$ neboli $p^2 = p^3$, což nesplňuje žádné prvočíslo. Tedy je $p \neq q$.

2. Upravíme $p + q^2 = q + p^3$ na $q^2 - q = p^3 - p$, neboli

$$q(q-1) \quad = \quad p(p-1)(p+1)\,. \tag{1}$$

Odtud plyne, že p dělí $q - 1$, a proto je splněna nerovnost

$$p \leq q - 1\,, \tag{2}$$

kterou lze psát také jako $p < q$ (neboť jde o celá čísla).

Z (1) dále vidíme, že q dělí jedno z čísel p, $p-1$, $p+1$. Z nerovnosti $p < q$ plyne, že q nemůže dělit ani p ani $p - 1$, tedy q musí dělit $p + 1$. Odtud pak dostáváme, že je splněna nerovnost

$$q \leq p + 1\,. \tag{3}$$

Nerovnosti (2), (3) ovšem implikují $q = p + 1$, což znamená, že p, q jsou dvě po sobě jdoucí prvočísla. Taková prvočísla jsou však pouze 2 a 3.

Závěr: jediným řešením úlohy je dvojice $p = 2$, $q = 3$.

Příklad 2. Určete, pro které dvojice prvočísel p, q platí $p + q^2 = q + 145p^2$.

Řešení.

1. Pro $p = q$ bychom dostali $p + p^2 = p + 145p^2$ neboli $1 = 145$, což je spor. Tedy je $p \neq q$.

2. Upravíme $p + q^2 = q + 145p^2$ na

$$q(q-1) \quad = \quad p(145p-1)\,, \tag{4}$$

odkud opět plyne, že p dělí $q - 1$. Je tedy splněno $q - 1 = kp$ pro nějaké přirozené k. Po dosazení tohoto vztahu do (4) dostaneme po úpravě

$$p \quad = \quad \frac{k+1}{145-k^2}\,. \tag{5}$$

Jmenovatel zlomku v (5) je kladný pouze pro $k = 0, 1, \ldots, 12$. Můžeme těchto 13 možností vyzkoušet buď dosazením, nebo si uvědomit, že také potřebujeme, aby čitatel zlomku nebyl menší než jeho jmenovatel. Zajímá nás tedy kvadratická nerovnost $k + 1 \geq 145 - k^2$, neboli

$$k^2 + k - 144 \geq 0\,,$$

která je v oboru přirozených čísel splněna pouze pokud $k \geq 12$. Vztah (5) dává tedy přirozené číslo pouze pro $k = 12$.

Pak (5) dá $p = 13$, což je (naštěstí) prvočíslo, a dále $q(q-1) = 24\,492$, což má (také naštěstí) v oboru prvočísel jediné řešení, a sice $q = 157$.

Závěr: jediným řešením úlohy je dvojice $p = 13$, $q = 157$.

Příklad 3. Zjistěte, kdy pro tři prvočísla p, q, r má rozdíl $(p+1)(q+1)(r+1) - pqr$ hodnotu, která při dělení šesti dává zbytek 3.

Řešení.

1. Označíme $A := (p+1)(q+1)(r+1)$, $B := pqr$, jde tedy o to, kdy $A - B \equiv 3 \pmod 6$. Možnosti pro $A - B$: například $(3-0) \mod 6$, $(4-1) \mod 6$, $(5-2) \mod 6$, ... Pokud je tedy pqr sudé, je $(p+1)(q+1)(r+1)$ liché (obojí modulo 6, ale to na pojmu sudosti a lichosti nic nemění). Tedy každé z $(p+1), (q+1), (r+1)$ je liché, proto každé z p, q, r je sudé, a protože jsou to provočísla, musí být $p = q = r = 2$. Pak ale máme, že $(p+1)(q+1)(r+1) - pqr = 27 - 8 = 19 \equiv 1 \pmod 6$, což nevyhovuje zadání. Právě jsme tedy ukázali, že žádné z p, q, r není rovno 2.

2. Je-li $A - B \equiv 3 \pmod 6$, znamená to, že $A - B$ je dělitelné třemi. Tvrdím, že i $B = pqr$ musí být dělitelné třemi: Nechť $B = pqr$ (a tedy ani žádné z čísel p, q, r) není dělitelné třemi. Pak ani $A = (p+1)(q+1)(r+1)$ není dělitelné třemi (to plyne z toho, že $A - B$ je třemi dělitelné). Čísla p, q, r nemohou při dělení třemi dávat zbytky 2, to by $(p+1), (q+1), (r+1)$ (a tedy i A) byly dělitelné třemi. Proto

$$p \equiv 1 \pmod 3, \quad q \equiv 1 \pmod 3, \quad r \equiv 1 \pmod 3,$$

a tedy

$$p+1 \equiv 2 \pmod 3, \quad q+1 \equiv 2 \pmod 3, \quad r+1 \equiv 2 \pmod 3.$$

Celkově tedy pro $A - B$ podle pravidel modulární aritmetiky:

$$(p+1)(q+1)(r+1) - pqr = 2 \cdot 2 \cdot 2 - 1 \cdot 1 \cdot 1 \equiv 1 \pmod 3,$$

což je spor. Právě jsme tedy ukázali, že pqr je dělitelné 3.

3. Víme tedy už, že p, q, r nejsou rovny 2 a pqr je dělitelné třemi. Jedno z p, q, r musí být proto rovno třem, nechť BÚNO $p = 3$. Z dělitelnosti pqr třemi také plyne $pqr \equiv 3 \pmod 6$ a podle zadání musí pak být

$$(p+1)(q+1)(r+1) = 4(q+1)(r+1) \equiv 0 \pmod 6,$$

tedy je dělitelné šesti. Žádné z $(q+1), (r+1)$ není ovšem dělitelné třemi, tedy aspoň jedno z nich musí být dělitelné šesti: např. $q + 1 = 6k$, tj. $q = 6k - 1$.

Žádné jiné podmínky na daná čísla nemáme, tedy řešením je trojice $p = 3$, q prvočíslo tvaru $6k - 1$, a r libovolné liché prvočíslo.

Zkouška. $A = (p+1)(q+1)(r+1) = 4 \cdot 6k \cdot (r+1) \equiv 0 \pmod 6$. $B = pqr = 3 \cdot (6k-1) \cdot r \equiv 3 \pmod 6$, neboť je to lichý násobek tří. Celkem $A - B = 0 - 3 \equiv 3 \pmod 6$, což jsme chtěli.

Příklad 4. Číslo n je součinem čtyř prvočísel. Jestliže každé z těchto prvočísel zvětšíme o 1 a vzniklá čtyři čísla vynásobíme, dostaneme číslo o 2886 větší než původní číslo n. Určete všechna taková n.

Řešení.

Označme $n = pqrs$, kde p, q, r, s jsou prvočísla, a

$$(p+1)(q+1)(r+1)(s+1) = pqrs + 2886. \tag{6}$$

1. Tvrdím, že alespoň jedno z p, q, r, s je rovno 2: nechť ne, pak jsou všechna lichá, a také součin $n = pqrs$ je lichý a tím i pravá strana rovnice (6) je lichá. Protože p, q, r, s jsou lichá, jsou

$(p+1), (q+1), (r+1), (s+1)$ sudá a tedy i jejich součin je sudý, tedy levá strana rovnice (6) je sudá, což je spor s (6).

2. Tedy alespoň jedno z čísel p, q, r, s je rovno 2, BÚNO $p = 2$. Rovnice (6):

$$(p+1)(q+1)(r+1)(s+1) = pqrs + 2886$$

se pak redukuje na

$$3(q+1)(r+1)(s+1) = 2qrs + 2886\,. \tag{7}$$

Levá strana (7) je dělitelná 3, tedy i pravá strana (7) je dělitelná 3, proto $2qrs$ musí být dělitelné 3, a tedy alespoň jedno z čísel q, r, s je rovno 3. BÚNO $q = 3$. Rovnice (7) se tedy dále redukuje na

$$\begin{aligned} 12(r+1)(s+1) &= 6rs + 2886 \\ 2(r+1)(s+1) &= rs + 481\,. \end{aligned} \tag{8}$$

Odtud plyne mj., že rs je liché, tedy $r \geq 3$, $s \geq 3$.

3. Roznásobením v rovnici (8) dostaneme:

$$\begin{aligned} 2rs + 2r + 2s + 2 &= rs + 481 \\ rs + 2r + 2s + 2 &= 481 \\ (r+2)(s+2) - 2 &= 481 \\ (r+2)(s+2) &= 483\,. \end{aligned}$$

Máme $483 = 3 \cdot 7 \cdot 23$ a tedy přicházejí do úvahy možnosti

- $(r+2)(s+2) = 3 \cdot 161 \implies r = 1$ není prvočíslo;
- $(r+2)(s+2) = 7 \cdot 69 \implies r = 5, s = 67$ je řešení;
- $(r+2)(s+2) = 23 \cdot 21 \implies r = 21$ není prvočíslo;

(a 3 možnosti, kde se symetricky prohodí hodnoty r, s, ale ty už nemusíme uvažovat.)

Závěr: jediné řešení úlohy je $n = 2 \cdot 3 \cdot 5 \cdot 67 = 2010$.

Zkouška: $3 \cdot 4 \cdot 6 \cdot 68 = 4896 = 2010 + 2886$.

5 Zpět k prvočíslům

Hustota prvočísel

... označme $\pi(n)$ počet prvočísel menších než n; jaký je vztah mezi $\pi(n)$ a n?

$\pi(10) = 4 \qquad (2, 3, 5, 7)$.
$\pi(20) = 8 \qquad (2, 3, 5, 7, 11, 13, 17, 19)$.

C. F. Gauss v roce 1792, ve věku 15 let (!), navrhl, že by mohlo platit

$$\pi(n) \simeq \frac{n}{\ln n}\,.$$

$\pi($ 1 000$) =$ 168 $\frac{n}{\ln n} =$ 144

$\pi(\ \ 10\,000) = \ \ 1\,229 \quad \frac{n}{\ln n} = \ \ 1\,085$
$\pi(\ \ 100\,000) = \ \ 9\,592 \quad \frac{n}{\ln n} = \ \ 8\,686$
$\pi(\ 1\,000\,000) = \ 78\,498 \quad \frac{n}{\ln n} = \ 72\,382$
$\pi(10\,000\,000) = 664\,579 \quad \frac{n}{\ln n} = 620\,420$

Později, v roce 1863, Gauss v dopise Enckemu napsal, že si myslí, že ještě přesnější odhad je

$$\pi(n) \simeq \int_2^n \frac{dx}{\ln x} =: \mathrm{Li}(n).$$

$\pi(\ \ 1\,000) = \ \ 168\ , \frac{n}{\ln n} = \ \ 144\ , \mathrm{Li}(n) = \ \ 176$
$\pi(\ \ 10\,000) = \ \ 1\,229\ , \frac{n}{\ln n} = \ \ 1\,085\ , \mathrm{Li}(n) = \ \ 1\,245$
$\pi(\ \ 100\,000) = \ \ 9\,592\ , \frac{n}{\ln n} = \ \ 8\,686\ , \mathrm{Li}(n) = \ \ 9\,629$
$\pi(\ 1\,000\,000) = \ 78\,498\ , \frac{n}{\ln n} = \ 72\,382\ , \mathrm{Li}(n) = \ 78\,626$
$\pi(10\,000\,000) = 664\,579\ , \frac{n}{\ln n} = 620\,420\ , \mathrm{Li}(n) = 664\,917$

Ohledně těchto Gaussových odhadů, oba byly později skutečně dokázány. Dnes dokonce víme, že platí

$$0.922 \cdot \frac{n}{\ln n} \le \pi(n) \le 1.105 \cdot \frac{n}{\ln n}$$

a

$$0.89\,\mathrm{Li}(n) \le \pi(n) \le 1.11\,\mathrm{Li}(n)$$

K čemu je to dobré?

- Baví nás to.
- Velký praktický význam mají prvočísla a znalost jejich rozložení v kryptografii, například v šifrovacích systémech jako je RSA.

Otázka: Jaké je největší prvočíslo?

(Ha, ha)

Dobře, tak jaké je největší **známé** prvočíslo?

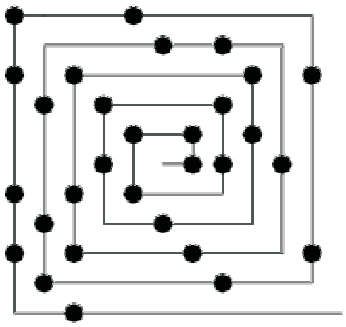
Nejvetší k dnešnímu datu známé prvočíslo (bylo nalezeno 25. ledna 2013) je

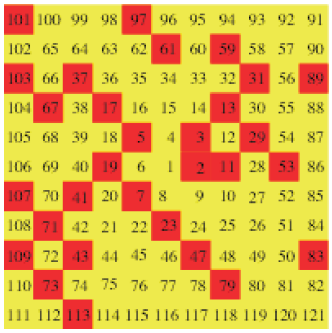
$$2^{57\,885\,161} - 1\,,$$

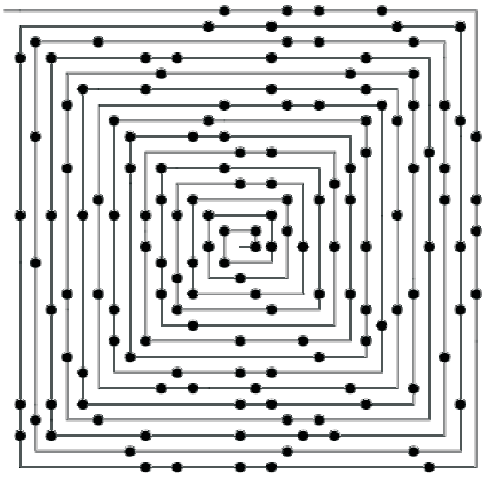
má $17\,425\,170$ dekadických cifer.

(Při 30 řádcích a 60 znacích na řádek by bylo potřeba asi $10\,000$ stran papíru na jeho vytištění.)

Krása prvočísel: Ulamova spirála







Další zajímavosti o výskytu prvočísel:

- Mezi čísly n a $2n$ (pro $n > 1$) leží vždy alespoň jedno prvočíslo (Čebyšev, 1850).
- Pro každé přirozené n existují $a, b \in \mathbb{N}$ tak, že čísla $a + kb$ jsou prvočísla pro všechna $k = 1, \ldots, n$, (Ben Green & Terence Tao, 2004), tedy prvočísla obsahují libovolně dlouhou aritmetickou posloupnost.

- Naprotitomu pro každé přirozené k existuje k po sobě jdoucích přirozených čísel, z nichž ani jedno není prvočíslem: Stačí uvažovat čísla

$$(k+1)!+2, (k+1)!+3, \ldots (k+1)!+k+1,$$

  kterých je k a jsou po řadě dělitelná dvěma, třemi, ..., $k+1$.

Dodnes nevyřešené otázky/hypotézy:

- Hypotéza prvočíselných dvojčat: Existuje nekonečně mnoho prvočíselných dvojčat, tj. dvojic prvočísel lišících se o 2 (např. $5, 7$ nebo $41, 43$)?
- Goldbachova hypotéza: každé sudé přirozené číslo větší než 4 lze napsat jako součet dvou pvočísel. (1742, dosud nevyřešeno).
- Riemannova hypotéza (cca 1890, velmi těžce zformulovatelná, supertěžká na důkaz) - souvisí s pravidelností rozložení prvočísel. Za její důkaz je vypsána odměna milion dolarů (Vypsal ji Clayův institut v roce 2000).

Prvočíselný vzorec.
Existuje vzorec, který pro každé n dá prvočíslo? Ha, ha:

$$p_n = 1 + 1^n \,.$$

Dobře, tak existuje vzorec, který pro každé n dá n-**té prvočíslo**? Překvapení: Ano!

$$p_n = 1 + \sum_{m=1}^{2^n} \left[\sqrt[n]{\left[\frac{n}{1 + \sum_{j=1}^{m} \left(\left[\frac{(j-1)!+1}{j} \right] - \left[\frac{(j-1)!}{j} \right] \right)} \right]} \right]$$

viz

P. Ribenboim: *The new book of prime number records*, 3rd edition, Springer-Verlag, New York, NY, 1995. pp. xxiv+541, ISBN 0-387-94457-5. MR 96 k:11112

Děkuji za pozornost.

Mirko Rokyta
KMA MFF UK Praha

rokyta@karlin.mff.cuni.cz