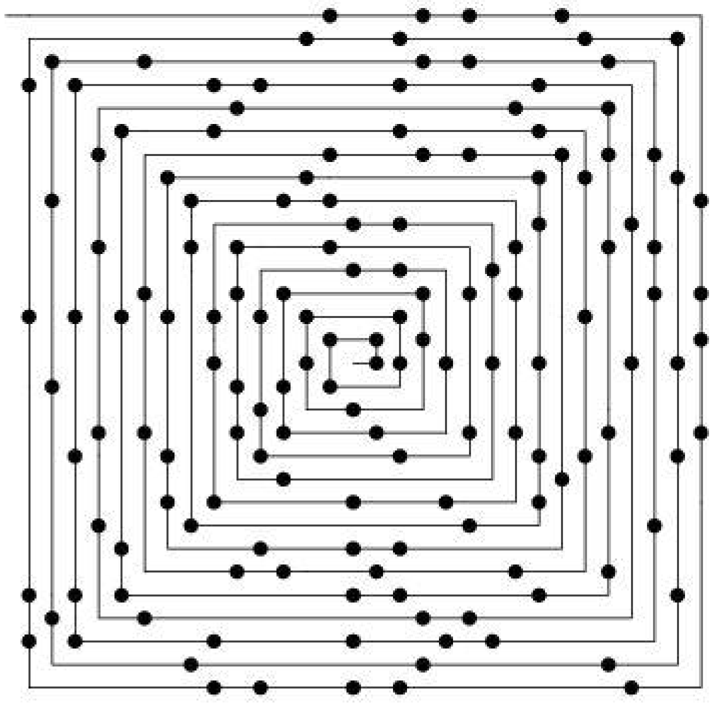
Vylepšené metódy hľadania prvočísiel / Improved prime numbers search methods



Autor: Ing. Robert Polák (Robopol), Email: robopol@gmail.com, Slovakia

Dátum/date:31.03.2022

Abstract

Táto publikácia sa venuje vylepšenej metóde hľadania prvočísiel postavenej na malej Fermatovej vete, filtrovaniu pseudoprvočísiel. V publikácií nájdete súvislosti tzv. špeciálnych prvočísiel, do tejto skupiny spadajú aj Mersennove prvočísla. Publikácia nadväzuje priamo na články referencia (1),(2),(3),(4),(5).

/This publication deals with an improved method of finding primes based on the small Fermat theorem, filtering pseudoprimes. In the publications you will find the context of the so-called special prime numbers, this group also includes Mersenne prime numbers. The publication follows directly on the articles reference (1), (2), (3),(4),(5).

Mala Fermatova veta / Fermat's little theorem

citation source (6):

Fermat's little theorem states that if p is a prime number, then for any integer a, the number $a^p - a$ is an integer multiple of p. In the notation of modular arithmetic, this is expressed as

$$a^{p-1} \equiv a \quad (mod\, p) \tag{1.0}$$

or

$$a^{p-1} \equiv 1 \quad (mod\, p) \tag{1.1}$$

<u>example:</u>

$a = 2,\ p = 17$

$2^{17-1} \equiv 1 \quad (mod\, 17)$

$2^{16}\, mod\, 17 = 1$

Redukovaná malá Fermatova veta / Reduced small Fermat's theorem

Malú Fermatovu vetu je možné upraviť na rovnicu: / Fermat's small theorem can be modified into the equation:

$$a^{\frac{p-1}{2}} \equiv \pm\, 1 \quad (mod\, p) \tag{1.2}$$

V literatúre sa táto rovnica objavuje ako Eulerovo kritérium viď. (1.3). /In the literature, this equation appears as Euler's criterion, see. (1.3).

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \quad (mod\, p) \tag{1.3}$$

<u>Dôkaz / proof:</u>
Rovnicu (1.0) môžeme zapísať aj ako rovnicu: / Equation (1.0) can also be written as an equation:

$$\left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{2}} - 1\right) \equiv 0 \quad (mod\, p) \tag{1.4}$$

Z rovnice jasne plynie, že ak má byť výsledok 0 (kongruencia), potom musí platiť: / It is clear from the equation that if the result is to be 0 (congruence), then:

$$a^{\frac{p-1}{2}} \equiv +\ 1 \quad or \quad a^{\frac{p-1}{2}} \equiv -\ 1 \quad (mod\ p) \qquad (1.5)$$

Poznámka:
V rovnici (1.2) sa zvyšok -1 chápe ako zvyšok (p -1). / In equation (1.2), residue -1 is understood as residue (p -1).

Pseudoprvočísla / Pseudorimes

Malá Fermatova veta nie je 100% nástroj na určenie prvočísla. Rovnica (1.1) vyhovuje aj pseudoprvočíslam. / Fermat's small theorem is not a 100% tool for determining a prime number. Equation (1.1) also satisfies pseudoprime numbers.

example:
$p\ =\ 341\ \ a\ =\ 2$

$2^{340}\ mod\ 341\ =\ 1$

341 is not a prime.

Existujú aj silné pseudoprvočísla, ktoré vyhovujú rovnici (1.1) aj (1.2) pre rôzne základy “a”. /There are also strong pseudoprime numbers that satisfy equations (1.1) and (1.2) for different bases "a".

example:
$p\ =\ 8911\ \ a\ =\ 4$

$4^{8910}\ mod\ 8911\ =\ 1$

$4^{\frac{8910}{2}}\ mod\ 8911\ =\ 1$

Periódy čísiel, prvočísiel / Periods of numbers, prime numbers

V modulárnej aritmetike majú všetky čísla aj prvočísla svoje periódy, viď. obr. č. 1. / In modular arithmetic, all numbers and primes have their periods, see. fig. no. 1.

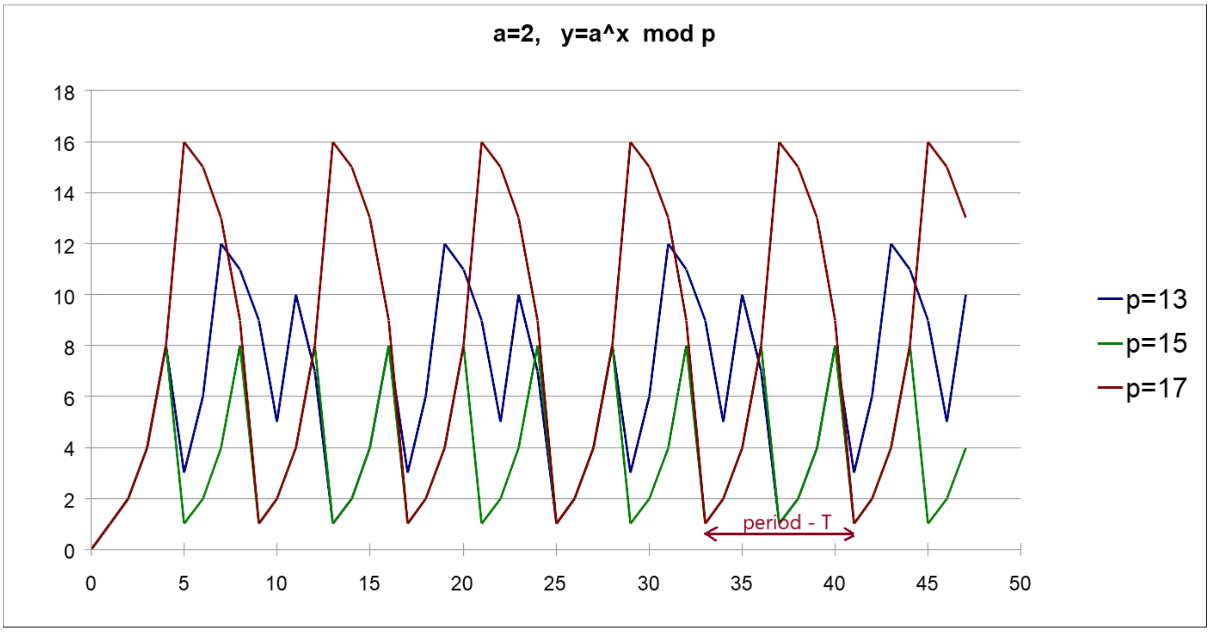


Fig. no.1. Chart function $y = a^x \, mod \, p$, periods of numbers -T

Na obr. č.1 vidíme opakujúcu sa sekvenciu zvyškov. Táto vlastnosť sa dá využiť. / In FIG. No. 1 we see a repeating sequence of residues. This feature can be used.

Prvočísla zvyknú mať dlhšie periódy - T ako zložené čísla. / Prime numbers tend to have longer periods - T, than composite numbers.

Najdlhšia perióda - T_{MAX} prvočísiel je: / The longest period - T_{MAX} prime numbers is:

$$T_{MAX} = p - 1 \tag{2.0}$$

V zmysle periód prvočísiel - T následne platí: / In terms of periods of prime numbers - T, the following applies:

$$a^T \equiv 1 \quad (mod \, p) \tag{2.1}$$

Táto vlastnosť periódy prvočísiel sa dá efektívne využiť pre algoritmus na preverenie prvočísla. / This feature of the period of primes can be effectively used for the algorithm for verifying primes.

Špeciálne prvočísla / Special prime numbers

A) Majme prvočíslo p, ktoré vyhovuje rovnici (3.0): / Let us have a prime number p that satisfies equation (3.0):

$$p = 2^k + 1; \quad k \in N; \quad N = \{1, 2, 3...\} \tag{3.0}$$

potom takéto prvočíslo má periódu T: / then such a prime number has a period T:

$$T = 2\,k; \quad for\colon\ a = 2; \quad a^T \equiv 1 \pmod p \tag{3.1}$$

<u>example:</u>

$17 = 2^4 + 1; \ T = 2 \cdot 4 = 8$

$2^8 \ mod\, 17 = 1$

Potom ak je splnená rovnica (3.2), číslo p je prvočíslo, resp. pseudoprvočíslo: / Then, if equation (3.2) is satisfied, the number p is a prime number, or pseudoprime number:

$$\begin{gathered} for\colon\ a = 2;\ Fermat's\ little\ theorem \\ if\ (p - 1)\ mod\ T = 0,\ then\ p\ is\ prime\ or\ pseudoprime \end{gathered} \tag{3.2}$$

or

$$\begin{gathered} for\colon\ a = 2;\ reduced\ Fermat's\ little\ theorem \\ if\ (p - 1)/2\ \ mod\ T = 0,\ then\ p\ is\ prime\ or\ pseudoprime \end{gathered} \tag{3.3}$$

B) Majme prvočíslo p, ktoré vyhovuje rovnici (3.2): / Let us have a prime number p that satisfies equation (3.2):

Takéto prvočíslo sa volá Mersennovo prvočíslo. / Such a prime number is called a Mersenne prime number.

$$p = 2^k - 1; \quad k \in N; \quad N = \{1, 2, 3...\} \tag{3.4}$$

potom takéto prvočíslo má periódu T: / then such a prime number has a period T:

$$T = k; \quad for\colon\ a = 2; \quad a^T \equiv 1 \pmod p$$

<u>example (1):</u>

$131071 = 2^{17} - 1; \ T = 17$

$2^{17} \ mod\, 17 = 1$

$(131071 - 1)\ mod\ 17 \quad = 0$

<u>example (2) - big Mersenne prime:</u>

$p = 2^{82\,589\,933} - 1;\ T = 82\,589\,933$

$2^{82\,589\,933}\ mod\ (2^{82\,589\,933} - 1) = 1$

$(2^{82\,589\,933} - 1)\ mod\ 82\,589\,933 = 0$

Preverenie kandidátov na Mersennove prvočísla je veľmi jednoduché postačuje preveriť, či je perióda T celočíselným násobkom $p - 1$, alebo $(p - 1)/2$. / Verifying candidates for Mersenne primes is very simple, it is enough to verify whether period T is an integer multiple of $p - 1$ or $(p - 1)/2$.

Pre Mersennove prvočísla platia rovnice (3.2) a (3.3) / Equations (3.2) and (3.3) apply to Mersenne primes.

Pre Mersennove prvočísla, základ a=2 v zmysle malej Fermatovej vety existuje pomerne dosť pseudoprvočísiel. Preto je nutné preveriť rovnicu (1.0) alebo (1.2) pre iné základy, napr. a=3,4,5..
/For Mersenne prime numbers, the base a = 2 in the sense of Fermat's small theorem there are quite a few pseudoprime numbers. Therefore it is necessary to check equation (1.0) or (1.2) for other bases, a = 3,4,5 ..

Z numerických testov sa pre Mersennove prvočísla objavila takáto závislosť: /From numerical tests, the following dependence appeared for Mersenne primes:

<u>Robopol theorem:</u>

$$for\!:\ p = 2^{k} - 1,\ only\ k \in prime\ \ can\ "p"\ be\ a\ Mersenne\ prime \qquad (3.5)$$

Dôkaz/ proof:
Dostaneme tak, že len pre prvočísla je splnená rovnica (1.2),(3.2),(3.3). /We get that equation (1.2), (3.2),(3.3) is satisfied only for primes.

Všeobecné prvočísla / General prime numbers

Každé prvočíslo môžeme zapísať ako : / Each prime number can be written:

$$p = 2^{k}s + 1; \qquad k, s \in N; \quad N = \{1, 2, 3...\} \qquad (3.6)$$

Rovnako ako pre špeciálne prvočísla aj pre všeobecné prvočísla platí rovnica (3.2) / Equations (3.2) apply to special prime numbers as well as general prime numbers.

nech “s” z rovnice (3.6) je: /let "s" from equation (3.6) be:

$$s = s_1 s_2 s_3 \ldots s_n;\ \ s_1, s_2, s_3 .. s_n \in prime \qquad (3.7)$$

potom perióda T je z množiny: / then period T is from the set:

$$T \ \in \ \left\{ s_1,\ s_1 s_2, s_1 s_3,\ s_2 s_3, s_1 s_2 s_3, ...;\ 2^j s_1 ... 2^j s_n,\ 2^j s_1 s_2, 2^j s_1 s_3, 2^j s_2 s_3,\ 2^j s_1 s_2 s_3 ...; 2^k s_1 s_2 s_3 \right\} \quad (3.8)$$
$$j \in (1, k) \leq k$$

Perióda T je z množiny všetkých kombinácii $2^j, s_1, s_2, s_3 .. s_n$. / Period T is from the set of all combinations $2^j, s_1, s_2, s_3 ... s_n$.

Ak pre p platí rovnica (3.2), potom je “p” prvočíslo alebo pseudoprvočíslo. / If equation (3.2) holds for “p”, then “p” is a prime number or a pseudoprime number.

<u>example (1):</u>

$$p = 997 = 2^2 \cdot 3 \cdot 83 + 1$$
$$T = 2^2 \cdot 83 = 332$$
$$2^{332}\, mod\, 997 = 1$$
$$(p - 1)\, mod\, T = 0,\ (997 - 1)\, mod\, 332 = 0$$

<u>example (2):</u>

$$p = 337 = 2^4 \cdot 3 \cdot 7 + 1$$
$$T = 3 \cdot 7 = 21$$
$$2^{21}\, mod\, 337 = 1$$
$$(p - 1)\, mod\, T = 0,\ (337 - 1)\, mod\, 21 = 0$$

Miller - Rabin test / Miller-Rabin primality test

citation source (8):
The Miller–Rabin primality test or Rabin–Miller primality test is a probabilistic primality test: an algorithm which determines whether a given number is likely to be prime, similar to the Fermat primality test and the Solovay–Strassen primality test.

The property is the following. For a given odd integer $p > 2$, let’s write n as $2^s d + 1$ where s and d are positive integers and d is odd. Let’s consider an integer a, called a base, such that $0 < a < p$. Then, p is said to be a strong probable prime to base a if one of these congruence relations holds:

$$a^d \equiv 1 \ (mod\, p);$$
$$a^{2^r \cdot d} \equiv -1 \ (mod\, p); \quad for\ some\ 0 \leq r \leq s \qquad (3.9)$$

Robopol test prvočísiel / Robopol prime test

Robopol theorem:

$$If\ \ a^{\frac{p-1}{2}} \equiv -\ 1\ \ mod\ (p);$$ then p is strong probably prime (4.0)

Tento teorém je veľmi podobný Miller - Rabin testu. Vychádza z numerických testov, kde pre zložené čísla sa neobjavuje polovičná perióda v zmysle rovnice (4.1):
/ This theorem is very similar to the Miller- Rabin test. It is based on numerical tests where half of the period in the sense of equation (4.1) does not appear for compound numbers:

$$period\ T_{1/2} = (p\ -\ 1)/2;\ \ for:\ a^{\frac{p-1}{2}}\ mod\ p\ =\ p\ -\ 1 \qquad (4.1)$$

Filtrácia pseudoprvočísiel sa dá účinné urobiť ako kombinácia klasického algoritmu a algoritmu postaveného na rovnici (4.1). / The filtering of pseudo-prime numbers can be done efficiently as a combination of the classical algorithm and the algorithm based on equation (4.1).
Ďalej sa odporúča vyskúšať výpočet pre viacero základov a=2,3,4,5… / It is also recommended to try the calculation for several bases a = 2,3,4,5…

Pre elimináciu výpočtu veľkých mocnín v rovnici (1.0), (1.2) sa využíva (4.2): / To eliminate the calculation of large powers in equation (1.0), (1.2) the following is used:

$$a^{x}\ mod\ p\ =\ k$$
$$a^{2x}\ mod\ p\ =\ k^{2}\ mod\ p \qquad (4.2)$$

<u>example:</u>

$$2^{1000}\ mod\ 15485863\ =\ 696244$$
$$2^{2000}\ mod\ 15485863\ =\ 696244^{2}\ mod\ 15485863\ =\ 1738047$$
$$2^{4000}\ mod\ 15485863\ =\ 1738047^{2}\ mod\ 15485863\ =\ 11050525$$
$$2^{8000}\ mod\ 15485863\ =\ 11050525^{2}\ mod\ 15485863\ =\ 4886002$$
…

To umožňuje vypočítať veľmi rýchlo obrovské mocniny modulo “p”. / This allows you to calculate huge powers modulo “p” very quickly.

```
Python 3.9.5 (tags/v3.9.5:0a7dcbd, May  3 2021, 17:27:52) [MSC v.1928 64 bit (AM
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
==== RESTART: C:\Users\robop\source\repos\Prime_numbers_py\prime_numbers.py ====
********************************************************************************
***
Prime number test:

This program uses a classical algorithm (for numbers < 10^18) and
improved finding of prime numbers using a small Fermat theorem.
If it gets the statement: prime or pseudoprime, then it is a probability
result, with pseudoprimes having a low probability.
Pseudoprimes are false primes. For a better result changes the basis a = 3,4,5,7
...

To end the program, press 0 and the enter.
********************************************************************************
***
Enter the number:
2305843009213693951
Enter the basis a:
3
wait
remainder is: 2305843009213693950
Number is strong probably prime.
 It is also recommended to try the calculation for several bases a = 2,3,4,5…
Enter the number:
```

Fig. no.2. - Console program for verifying prime numbers

Program - test prime numbers

Program (in Python) test prime numbers:
reference (9)
Download file in GitHub: prime_numbers.py

Hľadanie špeciálnych prvočísiel / Search for special prime numbers

A) Mersenne primes:

Pre Mersennove prvočísla platí Euclid–Euler theorem / The Euclid – Euler theorem applies to Mersenne primes.

citation source(10):
The Euclid–Euler theorem is a theorem in number theory that relates perfect numbers to Mersenne primes. It states that an even number is perfect if and only if it has the form

$r = 2^{k-1}\left(2^k - 1\right)$, where $2^k - 1$ is a Mersenne prime, r - is a perfect number.
(5.0)

$$\sigma(r) = \sigma\left(2^{k-1}\left(2^k - 1\right)\right) = r \quad (5.1)$$

sum of divisors function σ is multiplicative.

each number can be decomposed, prime decomposition:

$$n = \prod_{i,j} p_i^{j_i};\ n = p_1^{j_1} \cdot p_2^{j_2} \cdot p_2^{j_2} \dots p_n^{j_n}\ ; p_i \in prime;\ j_i \in N \quad (5.2)$$

Pre výpočet sigma použijeme vzťah: / To calculate sigma we use the equation:
reference (11):

$$\sigma(r) = \prod_{p_i \in prime}^{p_r} (1 + p_i + p_i^2 + p_i^3 + \dots p_i^{j_i}) - r \quad (5.3)$$

<u>example(1):</u>
$p = 2^3 - 1 = 7$
$r = 2^2 \cdot 7 = 28$
$\sigma(28) = 1 + 2 + 4 + 7 + 14 = 28$
$\sigma(28) = \left(1 + 2^1 + 2^2\right) \cdot (7 + 1) - 28 = 7 \cdot 8 - 28 = 28;\ \sigma(28) = 28;\ true$
$p = 7$ is Mersenne prime.

Algorithm for Mersenne primes:

1. find $k = prime\ number$ for $p = 2^k - 1$
2. calculate - “r”, equation (5.0)
3. decompose - “r”, equation (5.2)

4. calculate $\sigma(r)$, equation (5.3)
5. if $\sigma(r) = r$ is true, then p is Mersenne prime.

B) Special primes $p = 2^k + 1$:

Pre špeciálne prvočísla by malo platiť:

Robopol theorem:

$r = 2^{k-1}\left(2^k + 1\right)$, where $2^k + 1$ is special prime, (5.4)

then the equation applies:

$\sigma(r) + 2 = r$ (5.5)

Pre výpočet sigma použijeme vzťah (5.3): / To calculate sigma we use the equation (5.3).

example(1):
$p = 2^2 + 1 = 5$
$r = 2^1 \cdot 5 = 10$
$\sigma(20) = \left(1 + 2^1\right) \cdot (5 + 1) - 10 = 3 \cdot 6 - 10 = 8$
$\sigma(r) + 2 = r;\ 8 + 2 = 10;\ true;\ p = 5\ is\ a\ special\ prime.$

example(2):
$p = 2^4 + 1 = 17$
$r = 2^3 \cdot 17 = 136$
$\sigma(136) = \left(1 + 2^1 + 2^2 + 2^3\right) \cdot (17 + 1) - 136 = 15 \cdot 18 - 136 = 134$
$\sigma(r) + 2 = r;\ 134 + 2 = 136;\ true;\ p = 17\ is\ a\ special\ prime.$

Môžeme vytvoriť tabuľku špeciálnych prvočísiel / We can create a table of special prime numbers:

$p_{special} = 2^k + 1$

p.	k	$p_{special}$
1	2	5
2	4	17
3	8	257
4	16	65537

5	…	…

Tab. no. 1 Special prime numbers

Algorithm for special primes:

1. choose k; $p_{special} = 2^k + 1$
2. calculate - “r”, equation (5.4)
3. decompose - “r”, equation (5.2)
4. calculate $\sigma(r)$, equation (5.3)
5. if $\sigma(r) = r + 2$ is true, then $p_{special}$ is prime.

Result:
Algoritmus nie je menej výpočtovo náročný ako klasický algoritmus. / The algorithm is no less computationally intensive than the classical algorithm.

Proof:
Rovnica (5.1) platí aj napr. pre $p = 2^{11} - 1$ =2047 / Equation (5.1) also applies e.g. for $p = 2^{11} - 1$ =2047 (no Mersenne prime), $2047 = 23 \cdot 89$

calculate r:

$r = 2^{10} \cdot 2047 = 2096128$

$\sigma(r) = (1 + 2^1 + 2^2 .. + 2^{10}) \cdot (2047 + 1) - 2096128 = 2047 \cdot 2048 - 2096128 =$
$= 2096128$

$\sigma(r) = r;\ true$

Ak predpokladáme, že p=2047 je prvočíslo dostaneme pre rovnicu (5.1) pravdu. / If we assume that p = 2047 is a prime we get the truth for equation (5.1).

Rovnica (5.1), (5.5) platí pre ľubovoľné $k \in N$. / Equation (5.1),(5.5) applies to any $k \geq 2,\ k \in N$

Proof:

for: $p = 2^k - 1,\ k \geq 2,\ k \in N$

$perfect\ number\ “r”\ is\ r = 2^{k-1}\left(2^k - 1\right)$

$\sigma(r) = \left(1 + 2^1 + 2^2 .. + 2^{k-1}\right) \cdot \left(2^k - 1 + 1\right) - 2^{k-1}\left(2^k - 1\right) =$
$= \left(1 + 2\left(2^{k-1} - 1\right)\right) \cdot 2^k - 2^{k-1}\left(2^k - 1\right) = 2^{k-1}\left(2^k - 1\right)$

$\sigma(r) = r,\ true$

for: $p = 2^k + 1,\ k \geq 2,\ k \in N$

$r = 2^{k-1}\left(2^k + 1\right)$

$\sigma(r) + 2 = r$

$\sigma(r) = \left(1 + 2^1 + 2^2 .. + 2^{k-1}\right) \cdot \left(2^k + 1 + 1\right) - 2^{k-1}\left(2^k + 1\right) + 2 =$

$= \left(1 + 2\left(2^{k-1} - 1\right)\right) \cdot \left(2^{k} + 2\right) - 2^{k-1}\left(2^{k} + 1\right) + 2 = 2^{k-1}\left(2^{k} + 1\right)$
$\sigma(r) + 2 = r,\ true$

V zmysle dôkazu je potom množina všetkých perfektných čísiel nespočitáteľná. / According to the proof, the set of all perfect numbers is then innumerable.

Referencie/Reference:

(1) https://robopol.sk/blog/very-fast-algoritmus-na-prvocisla
(2) https://robopol.sk/blog/prvocisla-golden-part
(3) https://robopol.sk/blog/najvacsie-prvocisla
(4) https://robopol.sk/blog/program-na-prvo%C4%8D%C3%ADsla
(5) https://robopol.sk/blog/algoritmus-na-extremne-prvocisla-v-pythone
(6) https://en.wikipedia.org/wiki/Fermat%27s_little_theorem
(7) pseudoprime numbers
(8) Miller - Rabin primality test
(9) program Robopol primality test- code
(10) Euclid–Euler theorem - Wikipedia
(11) Evidence of equivalent conditions for the Riemann Hypothesis