Čo vieme o prvočíslach?
What Do We Know about Prime Numbers?

Daniela Hricišáková

Katedra KEaE, TnUAD, FSEV, Študentská 2, Trenčín 911 50

e-mail: daniela.hricisakova@tnuni.sk

Abstrakt: Termín teória čísel vyvoláva dojem, že ide o časť matematiky, ktorej predmetom je vychádzajúc z pojmu prirodzeného čísla budovať pojem celého, racionálneho, reálneho a komplexného čísla a študovať vlastnosti oborov prirodzených čísel, racionálnych, reálnych, resp. komplexných čísel. Avšak teória čísel vznikla ako bezprostredné rozvinutie aritmetiky celých čísel a jej náplňou bolo pôvodne štúdium istých špecifických vlastností celých čísel.

Kľúčové slová: prirodzené číslo, celé číslo, reálne číslo, prvočíslo, teória čísel, Mersennove čísla, prvočíselné dvojčatá

Abstract: The term theory of numbers gives the impression that it is a part of mathematics, the subject is based on the concept of natural number concept to build the whole, rational, and real and complex numbers and study the properties of the field of positive integers, rational, real or complex numbers. However, number theory arose as the immediate deployment of arithmetic of integers and the filling was originally studying certain specific properties of integers.

Keywords: natural number, integer, real number, prime number, theory numbers, Mersenn numbers, prime twins

„Matematika je kráľovnou vied. Jej milencom je pravda a prostota a priezračnosť sú jej odevom… Matematika, ktorá toľko prospela spoločnosti, vedám a umeniu, stane sa nakoniec vodcom ľudského rozumu vo všetkom poznaní.“

(Jan Sniadecki)

1 Úvod

Ak hovoríme o prirodzených číslach 1, 2, 3, … n si len málokto pri počítaní s nimi uvedomuje ich zaujímavé vlastnosti. Tá časť matematiky, ktorá sa zaoberá skúmaním prirodzených čísel sa nazýva *teória čísel*. Tvrdenia v teórii čísel sa zdajú nesmierne jednoduché, slovné vyjadrenia týchto tvrdení zrozumiteľné, ale dôkazy týchto jednoduchých tvrdení sú často veľmi náročné a často presahujú možnosti i tých najlepších matematických mozgov a preto neboli doteraz dokázané. Teória čísel vzniká ako bezprostredné rozvinutie aritmetiky celých čísel a jej náplňou bolo pôvodne štúdium istých špecifických vlastností celých čísel. Teória čísel používa vo veľkom rozsahu metódy rôznych matematických disciplín a do *teórie čísel patrí aj problematika prvočísel a ich vlastnosti*.

2 Z histórie teórie čísel

Prvé poznatky z teórie čísel sú spojené s menami starogréckych matematikov Pytagora, Euklida a Diofanta. Teóriu párneho a nepárneho objavil Pytagoras v 6. st. pred n. l. Všeobecné zákonitosti o číslach a rovinných útvaroch predstavovali prvé kroky teoretického matematického myslenia. Preto je teória čísel spolu s planimetriou zakladajúcim členom *spoločenstva matematických disciplín*. Starým Grékom (6. – 3. storočie pred n. l.) bol známy aj istý veľmi praktický spôsob vyznačovania prvočísel v zápise 1, 2, 3 … n. prirodzených čísel (metóda Eratostenovho sita). V *Euklidových Základoch* (300 rokov pred n. l.) nachádzame všetko, čo v tejto dobe tvorilo časť matematiky. Od Euklida pochádza napríklad aj prvý elementárny dôkaz existencie nekonečného počtu prvočísel. Výsledky gréckej teórie čísel nachádzame v *Diofantovej Aritmetike* (250 r. pred n. l.).

Diofantova Aritmetika je venovaná riešeniu rovníc v obore racionálnych čísel. *Diofantova Aritmetika* sa stala základnou učebnicou teórie čísel pre mnoho storočí. Možno skonštatovať, že od čias Euklida a Diofanta neurobila *teória čísel* skoro žiaden pokrok a v podstate stagnovala až do 17. st. n. l., keď sa zásluhou Fermata (1601 – 1665) začala prudko rozvíjať, čo súviselo aj s rozvojom celej matematiky.

Poznámka pod názvom *Veľká Fermatova veta*, kde rovnica $x^n + y^n = z^n$, pričom kde x, y, z, n sú prirodzené čísla a pre $n \geq 3$ je neriešiteľná. Fermatov dôkaz sa nenašiel a dodnes sa nikomu nepodarilo toto tvrdenie ani dokázať ani vyvrátiť, hoci sa o to mnohí pokúšali. Existuje aj Malá Fermatova veta, ktorej dôkaz je známy a nie je ani veľmi náročný.

Fermat vyslovil i hypotézu o pravdivosti ktorej bol hlboko presvedčený a to, že číslo $F_n = 2^{2^n} + 1$ *je prvočíslo.* Vo všeobecnosti však Fermatova hypotéza neplatí. Vývin teórie čísel je spojený s menami popredných matematikov P. G. Dirichleta, L. Eulera, K. F. Gaussa, P. L. Čebyševa a ďalších. Euler vypočítal, že piate Fermatovo číslo je zložené. Eulerom sa začína teória čísel založená na aritmetických funkciách a prepletená myšlienkami nekonečných radov a súčinov. Vlastnosti čísel, ktoré dnes poznáme, boli zväčša odhalené cestou poznávania.

Pojem *prvočísla* nadväzuje na pojem deliteľnosti v obore celých čísel, čo je základný pojem v teórii čísel. *Každé prirodzené číslo p je deliteľné číslami 1 a p. Čísla 1, p nazývame triviálnymi deliteľmi čísla p.* Každého iného prirodzeného deliteľa čísla p nazývame jeho netriviálnym deliteľom.

Prirodzené číslo p > 1 nazývame prvočíslom, keď má len triviálnych deliteľov.

Množinu všetkých prirodzených čísel tak môžeme rozdeliť na tri disjunktné podmnožiny z ktorých:

- prvá obsahuje len číslo jedna,
- druhá všetky prvočísla,
- tretia všetky prirodzené čísla, ktoré majú aspoň jedného netriviálneho deliteľa. Čísla tretej množiny nazývame zloženými číslami.

Najmenšie prvočíslo je číslo 2, je súčasne jediným párnym prvočíslom. Ostatné párne čísla sú deliteľné dvoma, teda sú zložené. Ak chceme v danom úseku prirodzených čísel 1, 2, … n určiť všetky prvočísla, používame k tomu metódu tzv. *Eratostenovo sito*, gréckeho matematika Eratostena (276 – 194 pred n. l.). Je to mechanická metóda, ktorú možno použiť na nájdenie všetkých prvočísel po akúkoľvek hranicu. V rozložení prvočísel sa matematikom dodnes nepodarilo nájsť nejakú rozumnú pravidelnosť. Ťažko povedať, čo všetko poznal Pytagoras z teórie čísel, pretože písomné záznamy sa nezachovali.

3 Cifry zápisu prvočísel

Aké cifry môžu byť na začiatku a na konci zápisu prvočísel?

Posledná cifra zápisu prvočísla *p*, ktorý má viac než jednu cifru, nemôže byť 0, 2, 4, 6, 8, lebo potom by *p* bolo väčšie než číslo 2, deliteľné číslom 2, a teda bolo by to číslo zložené. Posledná cifra nemôže byť ani číslo 5, deliteľné číslom 5, lebo vtedy by bolo číslo väčšie ako číslo 5, deliteľné číslom 5, a teda zložené.

Na poslednom mieste zápisu prvočísla $p > 10$ môžu teda byť len čísla 1, 3, 7 alebo 9. Riešime otázku, či môžeme povedať niečo viac o čísliciach zápisu prvočísel $p > 10$, napríklad o skupinách niekoľkých prvých alebo posledných cifier. Ukazuje sa, že možno, lebo platí táto veta.

Veta: *Ak sú dva ľubovoľné konečné rady cifier (desiatkovej sústavy)* $a_1, a_2, \ldots a_m$ *a* $b_1, b_2, \ldots b_n$*, kde* $b_n = 1, 3, 7, 9$*, potom existuje ľubovoľne veľké prvočíslo p, ktorého zápis má na prvým m miestach ciferný rad* $a_1, a_2, \ldots a_m$ *a na posledných n miestach ciferný rad* $b_1, b_2, \ldots b_n$.

Dôkaz tejto vety je dosť náročný. Z tejto vety vyplýva, že existujú prvočísla, ktorých zápis má na začiatku i na konci ľubovoľný počet jednotiek (ale medzi obidvoma skupinami môžu byť aj iné cifry ako 1).

Teda vzniká otázka, či existuje nekonečne mnoho prvočísel zapísaných samými jednotkami. Odpoveď na túto otázku nevieme. Poznáme len málo prvočísel, ktoré sú v desiatkovej sústave zapísané samými jednotkami, napríklad

$$11 \text{ a } 11\,111\,111\,111\,111\,111\,111\,111\,111 = (10^{23} - 1) / 9.$$

Dôkaz, že $(10^{23} - 1) / 9$ je prvočíslo, nie je ľahký a urobil ho M. Kraitchik.

Je možné dokázať toto tvrdenie: Ak je číslo zapísané v desiatkovej sústave n jednotkami prvočíslo, potom n je prvočíslo.

Táto nutná podmienka nie je postačujúca, lebo napríklad

$$111 = 3 \cdot 37,\ 11\,111 = 41 \cdot 271,\ 1\,111\,111 = 239 \cdot 4\,649.$$

Tiež číslo $(10^{37} - 1) / 9$, ktoré je zapísané 37 jednotkami je zložené.

Aké sú prvočísla po zmene poradia cifier? Hľadali sa tiež iné *prvočísla*, zapísané inými ciframi než jednotkami, ktoré sú prvočíslami pri každej zmene poradia cifier v ich zápise. Z dvojciferných čísel sú to čísla 13 a 31, 17 a 71, 79 a 97, z čísel trojciferných sú to čísla 113, 131, 311, 199, 919, 991, 337, 373, 733. Nevieme však, či počet takýchto čísel je konečný.

Nevieme tiež, či existuje nekonečne mnoho prvočísel, v ktorých zápise je na prvom a na poslednom mieste číslica jedna, zatiaľ čo na každom ostatnom mieste je číslica nula, takým je číslo 101.

Možno dokázať, že také prvočísla musia mať tvar $10^{2n} + 1$, kde *n* je prirodzené číslo, avšak táto podmienka nie je postačujúca, lebo napríklad $10^{2n} + 1 = 73 \cdot 137$.

4 Prvočíselní delitelia prirodzených čísel

Každé prirodzené číslo $a > 1$ *má aspoň jedného prvočíselného deliteľa.*

Túto vetu dokazujeme takto: Nech $a > 1$. Potom číslo a má aspoň jedného deliteľa väčšieho než číslo 1.

Nech *p* je najmenší deliteľ čísla a, $p > 1$.

Najprv si kážeme, že *p* je prvočíslo.

Dôkaz tejto vety robíme nepriamo. Nech *p* nie je prvočíslo. Potom existuje prirodzené číslo *q* tak, že $q \backslash p$, $1 < p < q$.

Z podmienky $q \backslash p$, $p \backslash a$ vyplýva, že $q \backslash a$, pritom $q < p$.

To je ale v spore s definíciou čísla *p*, *ako vidíme*, predpoklad viedol k sporu, preto *p* musí byť prvočíslo.

Môžeme ešte dokázať vetu:

Každé zložené číslo a má aspoň jedného prvočíselného deliteľa $p \leq \sqrt{a}$.

Nech *a* je zložené číslo. Potom $a = a_1 . a_2$, kde a_1, a_2 sú prirodzené čísla, $1 < a_1 < a$, $1 < a_2 <$ a.

Pri vhodnej voľbe označenia oboch činiteľov môžeme predpokladať, že $a_1 \leq a_2$.

Teda $a = a_1 . a_2 \geq a_1^2$, odtiaľ $a_1 \leq \sqrt{a}$.

Ale podľa vety číslo a_1 má prvočíselného deliteľa $p \leq a_1$, a teda $p \leq \sqrt{a}$, *preto* avšak číslo *p* je deliteľom čísla a_1, ktoré je deliteľom čísla *a*.

Teda číslo a má prvočíselného deliteľa $p \leq \sqrt{a}$. Tento dôkaz možno použiť k metóde na rozhodnutie, či nejaké číslo je prvočíslom, teda ho využijeme aj pri metóde Eratostenovho sita.

5 Rozklad prirodzeného čísla na prvočinitele

Každé zložené číslo sa dá napísať v tvare súčinu prvočísel, pričom pripúšťame aj trochu neobvyklé súčiny s jedným činiteľom.

Veta: *Každé prirodzené číslo a* > 1 *môžeme vyjadriť práve jedným spôsobom ako súčin prvočísel, keď odhliadneme od poradia činiteľov.*

Pri dôkaze musíme ukázať existenciu (možnosť) a potom unicitu (jednoznačnosť) vyjadrenia prirodzeného čísla *a* > 1 ako súčinu prvočísel.

6 Čo vieme o prvočíslach

Prvý elementárny dôkaz o nekonečnom počte prvočísel urobil 500 rokov pred n. l. grécky matematik Euklides.

- *Euklides predpokladal, že prvočísel je konečný počet.* Potom našiel číslo *n*, ktoré nie je prvočíslom ani zloženým číslom. To predsa nie je ale možné, pretože každé prirodzené číslo je *prvočíslo alebo zložené číslo* a to znamená, že predpoklad nebol dobrý a teda Euklides dokázal, že *prvočísel je nekonečne veľa*. Od čias Euklida túto vetu dokázalo viac matematikov rôznymi metódami.
- V roku 1850 dokázal P. L. Čebyšev ešte *silnejšie tvrdenie*. Podľa neho pre prirodzené číslo $n \geq 2$ medzi číslami *n* a 2*n* existuje jedno prvočíslo. Tento výsledok ukazujúci na istú pravidelnosť v rozdelení prvočísel bolo potvrdením hypotézy francúzskeho matematika J. Bertranda ako *Bertrandov postulát*. Treba uviesť, že pravidelnosť v určení prvočísel je veľmi problematická.

Prvočísla sa vyskytujú v postupnosti všetkých prirodzených čísel veľmi nepravidelne.

Dve najmenšie prvočísla sú 2 a 3, sú to po sebe nasledujúce prirodzené čísla. Vznikla otázka, či sú ešte iné po sebe nasledujúce prirodzené čísla také, že sú prvočísla. Dve nepárne prvočísla, ktorých rozdiel je dva, nazývame *prvočíselnými dvojčatami*.

Takýmito dvojčatami sú napríklad 3 *a* 5, 5 *a* 7, 11 *a* 13, 17 *a* 19, 29 *a* 31, 41 *a* 43, 59 *a* 61, 71 *a* 73, *atď.* Doteraz sa však nedokázalo, či prvočíselných dvojčiat je alebo nie je nekonečno mnoho. Nevieme teda, či číslo 2 je možno nekonečne veľa spôsobmi vyjadriť ako rozdiel dvoch prvočísel. Bola vyslovená hypotéza, že každé párne číslo sa dá vyjadriť nekonečne veľa spôsobmi ako rozdiel dvoch po sebe idúcich prvočísel. Dokážeme nájsť všetky nepárne čísla, ktoré sú rozdielom dvoch prvočísel, aj keď nie po sebe idúcimi, sú to čísla o dva menšie ako nepárne prvočísla, teda čísla 1, 5, 9, 11, 15, … a takých čísel je nekonečne veľa.

- V roku 1967 urobil Ľubomír Železný zaujímavé zistenie, pokus s prvočíslami (nie je matematik, ale zaoberal sa prvočíslami).

Zostavil prvočísla do súčtu (alebo rozdielu) dvoch súčinov z a + b alebo a – b. Každé prvočíslo je obsiahnuté buď v súčine *a* alebo v súčine *b*.

Uvažujeme nasledujúce dva príklady.

príklad:	$1 + 2 . 3 = 7$	príklad:	$2 + 3 . 5 = 17$
	$2 + 3 = 5$		$3 . 5 – 2 = 13$
	$2 . 3 – 1 = 5$		$1 + 2 . 3 . 5 = 31$
	$3 – 2 = 1$		

Tieto poznatky môžeme vyjadriť vetou: ak uvažujeme všetky prvočísla od 1 do p a zostavíme tieto prvočísla do súčtu alebo rozdielu dvoch súčinov a ± b, potom výsledok v = a ± b je prvočíslo, keď $v < (p')^2$, kde *p* je najmenšie prvočíslo nevyskytujúce sa v *a* i *b*.

Ak $v > (p')^2$, potom *v* je buď prvočíslo alebo zložené číslo.

- *Zovšeobecnenie Pytagorovej a Fermatovej vety.* Pytagorov výraz $x^2 + y^2 = z^2$ a Fermatov výraz (rovnica) $x^n + y^n$ *n* = z^n má niekoľko rôznorodých zovšeobecnení. Vyjmeme z výrazu $x^2 + y^2 = z^2$ najväčšieho spoločného deliteľa, Zostáva výraz, keď súčet dvoch nesúdeliteľných čísel je taký, že výsledok je číslo nesúdeliteľné s *x*, *y*.

Uvádzame príklad zovšeobecnenia Fermatovej vety $(xy)^n + (xz)^n + (yz)^n = u^n$. Našlo sa riešenie týchto rovníc pre 9 a 91 premenných.

- Pri hľadaní prvočísel sú dôležité *Mersennove čísla*, sú to čísla tvaru $M_n = 2^n - 1$, kde *n* = 1, 2, 3, … zaujímavé sú z dvoch dôvodov. Prvý z nich je ten, že najväčšie známe prvočísla patria medzi čísla Mersennove a druhý je ten, že pomocou Mersennovych čísel môžeme nájsť *párne dokonalé čísla*. *Prirodzené číslo n sa nazýva dokonalé číslo*, ak sa rovná súčtu všetkých svojich prirodzených deliteľov menších než *n*.

Príkladom dokonalého čísla je číslo 6 = 1 + 2 + 3.

Ak skúmame prvočísla, bolo zistených mnoho závažných tvrdení ale dôkazy k nim boli nájdené až neskôr. Často viedla táto cesta k vysloveniu hypotéz, ktoré sa potom ukázali nesprávnymi. Poznáme rôzne hypotézy o prvočíslach preverené v mnohých zvláštnych prípadoch, u ktorých ale nevieme, či sú pravdivé alebo nepravdivé. Problematika prvočísel je veľmi zaujímavá, avšak v literatúre spracovaná len útržkovite.

Tabuľka Mersennove čísla – prehľad

#	*p*	M_p	Cifry v M_p	Dátum objavu	Objaviteľ
1	2	3	1	500 pred n. l.	starí Gréci
2	3	7	1	500 pred n. l.	starí Gréci
3	5	31	2	275 pred n. l.	starí Gréci
4	7	127	3	275 pred n. l.	starí Gréci
5	13	8191	4	1456	*anonym*

#	*p*	M_p	Cifry v M_p	Dátum objavu	Objaviteľ
6	17	131071	6	1588	Cataldi
7	19	524287	6	1588	Cataldi
8	31	2147483647	10	1772	Euler
9	61	2305843009213693951	19	1883	Ivan Pervušin
10	89	618970019…449562111	27	1911	Powers
11	107	162259276…010288127	33	1914	Powers
12	127	170141183…884105727	39	1876	Lucas
13	521	686479766…115057151	157	30. január 1952	Robinson pomocou SWAC
14	607	531137992…031728127	183	30. január 1952	Robinson
15	1 279	104079321…168729087	386	25. jún 1952	Robinson
16	2 203	147597991…697771007	664	7. október 1952	Robinson
17	2 281	446087557…132836351	687	9. október 1952	Robinson
18	3 217	259117086…909315071	969	8. september 1957	Riesel pomocou BESK
19	4 253	190797007…350484991	1 281	3. november 1961	Hurwitz using IBM 7090
20	4 423	285542542…608580607	1 332	3. november 1961	Hurwitz
21	9 689	478220278…225754111	2 917	11. máj 1963	Gillies using ILLIAC II
22	9 941	346088282…789463551	2 993	16. máj 1963	Gillies
23	11 213	281411201…696392191	3 376	2. jún 1963	Gillies
24	19 937	431542479…968041471	6 002	4. marec 1971	Tuckerman using IBM 360/91
25	21 701	448679166…511882751	6 533	30. október 1978	Noll & Nickel pomocou CDC Cyber 174
26	23 209	402874115…779264511	6 987	9. február 1979	Noll
27	44 497	854509824…011228671	13 395	8. apríl 1979	Nelson & Slowinski
28	86 243	536927995…433438207	25 962	25. september 1982	Slowinski

#	*p*	M_p	Cifry v M_p	Dátum objavu	Objaviteľ
29	110 503	521928313…465515007	33 265	28. január 1988	Colquitt & Welsh
30	132 049	512740276…730061311	39 751	19. september 1983	Slowinski
31	216 091	746093103…815528447	65 050	1. september 1985	Slowinski
32	756 839	174135906…544677887	227 832	19. február 1992	Slowinski & Gage na Harwell Lab Cray-2
33	859 433	129498125…500142591	258 716	4. január 1994	Slowinski & Gage
34	1 257 787	412245773…089366527	378 632	3. september 1996	Slowinski & Gage
35	1 398 269	814717564…451315711	420 921	13. november 1996	GIMPS/Joel Armengaud
36	2 976 221	623340076…729201151	895 932	24. august 1997	GIMPS/Gordon Spence
37	3 021 377	127411683…024694271	909 526	27. január 1998	GIMPS/Roland Clarkson
38	6 972 593	437075744…924193791	2 098 960	1. jún 1999	GIMPS/Nayan Hajratwala
39	13 466 917	924947738…256259071	4 053 946	14. november 2001	GIMPS/Michael Cameron
40	20 996 011	125976895…855682047	6 320 430	17. november 2003	GIMPS/Michael Shafer
41	24 036 583	299410429…733969407	7 235 733	15. máj 2004	GIMPS/Josh Findley
42	25 964 951	122164630…577077247	7 816 230	18. február 2005	GIMPS/Martin Nowak
43	30 402 457	315416475…652943871	9 152 052	15. december 2005	GIMPS/Curtis Cooper & Steven Boone
44	32 582 657	124575026…053967871	9 808 358	4. september 2006	GIMPS/Curtis Cooper & Steven Boone
45	37 156 667	202254406…308220927	11 185 272	6. september 2008	GIMPS/Hans-Michael Elvenich
46	42 643 801	169873516…562314751	12 837 064	12. apríl 2009	GIMPS/Odd M. Strindmo
47	43 112 609	316470269…697152511	12 978 189	23. august 2008	GIMPS/Edson Smith

#	*p*	M_p	Cifry v M_p	Dátum objavu	Objaviteľ
48	57 885 161	581887266…724285951	17 425 170	25. január 2013	GIMPS/Curtis Cooper
49			22 338 618	17. september 2015	GIMPS/Curtis Cooper

Zdroj: http://www.mersenne.org/primes/

7 Záver

S prvočíslami sa stretávame v elementárnej aritmetike, ale aj v ďalších matematických disciplínach, pokiaľ sa jedná o prvočísla bolo objavených mnoho závažných tvrdení, ktorých dôkazy boli urobené neskôr. Často bola vyslovená veta o prvočíslach, preverená v mnohých zvláštnych prípadoch, o ktorých nevieme, či sú pravdivé alebo nie. Téma prvočísel je veľmi zaujímavá a niektorí matematici vravia o nej ako o téme kráľovskej.

Matematik Courtis Cooper objavil *48. Mersennove číslo*, ktoré má 17 miliónov čísel (zdroj: mersenne.org., 7. 2. 2013).

K napísaniu tohto článku nás viedla informácia z januára roku 2016, že *Mersennove číslo* $M_n = 2^n - 1$ sa podarilo vygenerovať opäť matematikovi Cooperovi Courtisovi a má viac ako 22 miliónov číslic. Prvý oznam však o *49. Mersennovom čísle* bol zverejnený v septembri v roku 2015. Význam týchto čísel je známy *v oblasti kryptografie a kódovania údajov*.

Literatúra

[1] ŠALÁT, T. a kol.: *Algebra a teoretická aritmetika 2.* Bratislava : Alfa, 1986.

[2] ŠALÁT, T. a kol.: *Malá encyklopédia matematiky.* Bratislava : Obzor, 1981.

[3] ZNÁM, Š.: *Teória čísel.* Bratislava : Alfa, 1977.

[4] ŽELEZNÝ, L.: *O prvočíselných aritmetických posloupnostech.* Rozhledy, 1977, č. 6.