Mersennova števila

Pisni izdelek pri predmetu *Komuniciranje v matematiki*

Katarina Abramič

13. april, 2018

1 Uvod

Števila so poleg množic in funkcij ena najpomembnejših matematičnih pojmov; z drugo besedo so števila temelj, na katerem stoji matematika.
Poznamo veliko različnih števil, med njimi so tudi takšna, ki imajo posebne oblike. Vzemimo število oblike $2^n - 1$, pri čemer je n naravno število[1] večje od 1. Takšnim številom pravimo *Mersennova števila*, ki so svoje ime dobila po francoskem redovniku *Marinu Mersennu*[2] iz 17. stoletja.

Definicija 1.1. Praštevila oblike $2^n - 1$ imenujemo Mersennova praštevila.

V predgovoru svoje knjige *Cogita Physico-Mathematica*, ki je izšla leta 1644, je Mersenne zapisal, da je število

$$M_n = 2^n - 1$$

praštevilo za $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ in sestavljeno število za vse druge n, manjše od 257.

Kako je prišel do tega? Nihče ne ve; nekaj pa le drži. Bil je zelo blizu resnice. V njegovem času je bilo znanih le 7 Mersennovih praštevil, in sicer za $n = 2, 3, 5, 7, 13, 17$ in 19. Naslednje Mersennovo praštevilo je odkril *Leonhard Paul Euler* [3], ki je leta 1750 pokazal, da je $M_{31} = 2147483647$ res praštevilo. Ta njegova trditev je veljala vse do leta 1880, ko je bilo odkrito spet novo praštevilo. Merssennovo trditev so lahko preverili šele leta 1947, ko so se pojavila dobra računala. Takrat so ugotovili, da je napravil le pet napak. Ugotovili so, da M_{67} in M_{257} nista praštevili, M_{61}, M_{89} ter M_{107} pa so praštevila.

2 Mersennova praštevila

Osnovna zamisel je poiskati vrednost n, pri kateri je M_n praštevilo. Ampak tudi pri večini praštevil n dobimo za Mersennovo število M_n sestavljeno število. Zato iskanje ustreznih vrednosti za n, da bi dobili Mersennovo praštevilo, ni enostavno. Prvi štirje primeri:

[1] Naravna števila so števila s katerimi štejemo.

[2] Marin Mersenne (1588, 1648). Rojen v francoskem kraju Oize. Bil je mislec, filozof, fizik in matematik. Izobraževal se je na jezuitskem kolegiju v La Flecheju, kjer je bil Descartesov sošolec in prijatelj. Umrl je v Parizu.

[3] Leonhard Paul Euler (1707, 1783). Rojen v Švici. Po poklicu je bil matematik, fizik in astronom. Umrl pa je v Rusiji.

$$M_2 = 2^2 - 1 = 3,$$

$$M_3 = 2^3 - 1 = 7,$$

$$M_5 = 2^5 - 1 = 31,$$

$$M_7 = 2^7 - 1 = 127,$$

so sama praštevila.
Ko pa vzamemo $n = 11$,

$$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$$

dobimo sestavljeno število. Nato sledijo spet 3 praštevilske vrednosti:

$$M_{13} = 8191,\ M_{17} = 131071,\ M_{19} = 524287.$$

Ko za n vzamemo vedno večja praštevila, vedno težje najdemo Mersennova praštevila, saj je znano, da Mersennovo število M_n ne morem biti praštevilo, če n ni praštevilo.

Domneva 2.1. *Mersennovih praštevil je neskončno mnogo.*

Domneva je še odprta (ni niti dokazana niti ovržena).

Izrek 2.2. *Če je Mersennovo število M_n praštevilo, je tudi n praštevilo.*

Dokaz. Zapišimo n v obliki $n = pq$, kjer je q praštevilo. Izrek bo dokazan, če dokažemo, da je $p = 1$. Sedaj upoštevamo, da je $n = pq$. Tedaj dobimo:

$$2^n - 1 = (2^p - 1)(1 + 2^p + 2^{2p} + \ldots + 2^{(q-1)p})$$

Število $2^n - 1$ smo sedaj zapisali v obliki produkta dveh naravih števil. Ker je $2^n - 1$ praštevilo in je očitno, da je $q > 1$, mora biti $p = 1$.
Dokazali smo, da je n praštevilo, če je $2^n - 1$ praštevilo. ■

Mersennova praštevila so v tesni zvezi s *prijateljskimi števili*

Definicija 2.3. Prijateljski števili sta celi števili za kateri velja, da je vsota pravih deliteljev prvega števila enaka drugemu številu, in obratno.

Definicija 2.4. Pravi delitelj je delitelj celega števila n, ki se razlikuje od n.

Vsako sodo prijateljsko število se namreč izraža na način $2^{n-1}M_n$, pri čemer je M_n Mersennovo praštevilo.

Zgled 2.5. *Za primer vzemimo najmanjši prijateljski par, števili 220 in 284. Množica pravih deliteljev števila 220 je $1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110$, njihova vsota pa je enaka 284. Množica pravih deliteljev števila 284 je $1, 2, 4, 71, 142$, katere vsota je enaka 220.*

3 Zanimivost

Že v Antični Grčiji so poznali 4 Mersennova praštevila, sam Mersenne pa jih je v svojem času odkril 7. Do sedaj je odkritih 50 Mersennovih praštevil, med odkritimi Mersennovimi števili pa lahko ležijo še neodkrita, saj eksponentov ne preverjajo po vrsti. Zadnje praštevilo je odkril, 51 letni Američan, Jonathan Pace. Po štirinajstih letih vstrajanja, ga je odkril 26. decembra, 2017. Novo odkrito praštevilo je $2^{77,232,917} - 1$, ki ima v desetiškem sestavu kar 23.249.425 mest.

Mersennova praštevila odkrivajo s pomočjo *projekta GIMPS* [4], pri katerem računalniki izberejo naključen eksponent n, ki je tudi praštevilo. GIMPS (Great Internet Mersenne Prime Search) je skupni projekt prostovoljcev, ki uporabljajo prosto dostopno programsko opremo za iskanje Mersennovih praštevil.

Praštevila pa odkrivajo tudi s pomočjo *Lucas-Lehmerjevega testa* [5] , s katerim preverijo, ali je dobljeno število praštevilo.

4 Lucas-Lehmerjev algoritem

Ali je število $2^n - 1$ praštevilo, preverimo z Lucas-Lehmerjevim algoritmom. Najprej definirajmo rekurzivno [6] Lucas-Lehmerjevo zaporedje: $s_0 = 4$ in $s_i = s_{i-1}^2 - 2$, pri katerem so prvi členi zaporedja enaki 4, 14, 194, 37634. Algoritem temelji na naslednjem izreku:

Izrek 4.1. *Naj bo n praštevilo večje od 2. Če je $s_{n-2} \equiv 0 \pmod{M_n}$, potem je M_n praštevilo.*

Dokaza izreka ne bom navedla, najde pa se ga v knjigi Enciklopedija števil na straneh 445 - 449.

Zgled 4.2. *Z Lucas-Lehmerjevim algoritmom preverimo, ali je število $2^5 - 1$ praštevilo.*
$M_5 = 2^5 - 1 = 31$. Zaporedje računamo do $n = 5 - 2 = 3$ po modulu 31.

[4] Projekt je ustanovil George Woltman.

[5] Edouard Lucas(1842, 1891). Bil je matematik, delal pa je v Pariškem observatoriju, kasneje je postal profesor matematike v Parizu. Služil je tudi v vojski. Derrick Henty Lehmer (1905, 1991). Bil je ameriški matematik, ki je izpopolnil delo Edouarda Lucasa.

[6] Pri rekurzivnem zaporedju podamo nekaj začetnih členov in formulo, ki pove, kako se n-ti člen izraža s prejšnjimi členi.

i	$s_i \pmod{31}$	Kako računamo člene zaporedja
0	4	$4 = 31 \cdot 0 + 4$
1	14	$4^2 - 2 = 14 = 31 \cdot 0 + 14$
2	8	$14^2 - 2 = 194 = 31 \cdot 6 + 8$
3	0	$8^2 - 2 = 62 = 31 \cdot 2 + 0$

Ker je $s_3 \equiv 0 \pmod{31}$*, sledi, da je* 31 *res praštevilo.*

Zgled 4.3. *Z Lucas-Lehmerjevim algoritmom preverimo, ali je število* $2^7 - 1$ *praštevilo.*
$M_7 = 2^7 - 1 = 127$*. Zaporedje računamo do* $n = 7 - 2 = 5$ *po modulu 127.*

i	$s_i \pmod{127}$	Kako računamo člene zaporedja
0	4	$4 = 127 \cdot 0 + 4$
1	14	$4^2 - 2 = 14 = 127 \cdot 0 + 14$
2	67	$14^2 - 2 = 194 = 127 \cdot 1 + 67$
3	42	$67^2 - 2 = 4487 = 127 \cdot 35 + 42$
4	111	$42^2 - 2 = 1762 = 127 \cdot 13 + 111$
5	0	$111^2 - 2 = 12319 = 127 \cdot 97 + 0$

Ker je $s_5 \equiv 0 \pmod{127}$*, sledi, da je* 127 *res praštevilo.*

Zgled 4.4. *Z Lucas-Lehmerjevim algoritmom pokažimo, da je število* $2^{11} - 1$ *sestavljeno.*
$M_{11} = 2^{11} - 1 = 2047$*. Zaporedje računamo do* $n = 11 - 2 = 9$ *po modulu 2047.*

i	$s_i \pmod{2047}$	Kako računamo člene zaporedja
0	4	$4 = 2047 \cdot 0 + 4$
1	14	$4^2 - 2 = 14 = 2047 \cdot 0 + 14$
2	194	$14^2 - 2 = 194 = 2047 \cdot 0 + 194$
3	788	$194^2 - 2 = 37634 = 2047 \cdot 18 + 788$
4	701	$788^2 - 2 = 620942 = 2047 \cdot 303 + 701$
5	119	$701^2 - 2 = 491399 = 2047 \cdot 204 + 199$
6	1877	$119^2 - 2 = 14159 = 2047 \cdot 6 + 1877$
7	240	$1877^2 - 2 = 3523127 = 2047 \cdot 1721 + 240$
8	282	$240^2 - 2 = 57598 = 2047 \cdot 28 + 282$
9	1736	$282^2 - 2 = 79522 = 2047 \cdot 38 + 1736$

Ker $s_9 \neq 0 \pmod{2047}$*, pomeni, da je to število sestavljeno. 2047 lahko zapišemo kot produkt števil* $23 \cdot 89$*.*

5 Viri in literatura

- J. Grasselli, *Enciklopedija števil* [Mersennova števila, Mersennova praštevila, Prijateljska števila], DMFA-založništvo, Ljubljana (2008).
- K. Devlin, *Nova zlata doba matematike* [1. poglavje: Praštevila, razceplja-nje in tajnopisi], DMFA-založništvo, Ljubljana (1993).
- M. Chubellier, J. Sip, *Zgodovina matematike, zgodbe o problemih*[1. po-glavje: Praštevila], DMFA-založništvo, Ljubljana (2000)
- Sodelavci Wikipedie, "Mersenne prime" *Wikipedia, The Free Encyclopedia,* `https://en.wikipedia.org/wiki/Mersenne_prime` *(ogled: 7. april, 2018).*
- *U. Kržan,* Mersennova praštevila in Lucas-Lehmerjev algoritem*,* `http://www.nauk.si/materials/6755/out/#state=1` *(ogled: 7. april, 2018).*
- *E. Žagar,* Zapiski pri predmetu Proseminar B*,* `http://studentski.net/gradivo/ulj_fmf_ma2_prb_sno_zapiski_01?r=1` *, (ogled: 7. april, 2018).*
- *M. Huš,* Okrili največje doslej znano praštevilo*,* `https://slo-tech.com/novice/t714969` *(ogled: 7. april, 2018).*
- *Ciril Petr, "Odkrito največje (Mersennovo) praštevilo",* PRESEK, list za mlade matematike, fizike, astronome in računalničarje*,* `http://www.presek.si/31/1575-Petr.pdf` *(ogled: 10. april, 2018).*