PRESEK
List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **21** (1993/1994)
Številka 2
Strani 92–95

Roman Drnovšek:

FERMATOVA ŠTEVILA

Ključne besede: matematika.

Elektronska verzija: http://www.presek.si/21/1169-Drnovsek.pdf

FERMATOVA ŠTEVILA

Slavni francoski matematik Pierre de Fermat (1601 - 1665)[1] je obogatil matematično znanost z množico novih spoznanj. Vsa, razen enega, so tudi dokazana, ali pa vsaj verjamemo v njihovo resničnost.[2] Edina izjema je njegov *izrek o binarnih potencah*. Le ta trdi, da so vsa števila oblike $2^m + 1$, kjer je $m = 2^n$, praštevila. Števila

$$F_n = 2^{2^n} + 1$$

zato imenujemo *Fermatova števila*.[3] Čeprav je bil Fermat sam prepričan o resničnosti te trditve, je ni znal dokazati. Pokazal pa je (kar je lahko), da je število $2^m + 1$ sestavljeno, če naravno število $m > 1$ ni potenca števila 2 (naloga 1). Seveda pa to še ne pomeni, da so potem vsa Fermatova števila praštevila, čeprav za $n = 1, 2, 3$ in 4 to res velja :

$$F_1 = 2^2 + 1 = 5\,,\quad F_2 = 2^4 + 1 = 17\,,\quad F_3 = 2^8 + 1 = 257\,,$$

$$F_4 = 2^{16} + 1 = 65537\,.$$

Leta 1732 je namreč švicarski matematik Leonhard Euler (1707 - 1783) pokazal, da že za $n = 5$ ne dobimo praštevila, saj je število F_5 deljivo s 641. Brez dolgoveznega računanja (in brez uporabe računalnika) se o tem najhitreje prepričamo na naslednji način. Število

$$641 = 5^4 + 2^4 = 2^7 \cdot 5 + 1$$

namreč deli števili

$$2^{28}(5^4 + 2^4) \quad \text{in} \quad (2^7 \cdot 5)^4 - 1\,,$$

kjer smo upoštevali znano pravilo o razcepu razlike četrtih potenc. Zato 641 deli tudi razliko teh števil

$$2^{28}(5^4 + 2^4) - [(2^7 \cdot 5)^4 - 1] = 2^{32} + 1 = F_5\,.$$

O številu F_5 je znana tudi naslednja resnična zgodba, ki bi jo Eva Longyka, če bi se zgodila pred kratkim, verjetno uvrstila med Neverjetne

---

[1] Več o Fermatu lahko prebereš v Preseku 3 (1975/76), št. 1, str. 9-14.
[2] Glej prispevek o Fermatovem zadnjem izreku v 1. številki letošnjega Preseka.
[3] O Fermatovih številih glej tudi članek: B. Pavšek, *Fermatova števila*, Presek 14 (1986/87), št. 4, str. 220-221.

zgodbe. Ameriški fenomen računanja na pamet, Z. Colburn (1804 - 1839), je na vprašanje, ali je število F_5 praštevilo, po kratkem premisleku odgovoril, da to ni, ker je deljivo s 641. Kot skoraj vsi fenomeni te vrste, pa tudi on ni bil sposoben razložiti, kako je prišel do takega zaključka. (Colburn je zaradi svojih neverjetnih sposobnosti tudi vplival pri izbiri življenske poti irskega matematika Williama Hamiltona (1805 - 1865).)

S pomočjo nekaterih izsledkov nemškega matematika C. F. Gaussa lahko dokažemo, da so vsa praštevila, ki se pojavijo v razcepu števila F_n (če je le to sestavljeno), oblike $2^{n+2} \cdot k + 1$, kjer je k naravno število. Tako je

$$F_5 = (2^7 \cdot 5 + 1)(2^7 \cdot 52347 + 1) .$$

Od leta 1880 pa tudi vemo, da je

$$F_6 = (2^8 \cdot 1071 + 1)(2^8 \cdot 262814145745 + 1) .$$

Leta 1905 je J. C. Morehead pokazal, da je število F_7 sestavljeno. Štiri leta kasneje pa je skupaj z A. E. Westernom prišel do enakega zaključka tudi za število F_8. To je najlažje preveriti z uporabo naslednjega kriterija, ki ga navedimo brez dokaza[4]:

F_n je praštevilo natanko tedaj, ko deli število $3^{(F_n-1)/2} + 1$.

Na ta način pa seveda ne dobimo vsaj enega od faktorjev v F_n. Tako so šele leta 1970 oziroma 1980 faktorizirali števili F_7 in F_8. Vsaj en faktor v F_n pa je znan tudi za vse n od 9 do 19 in še za precej večja naravna števila, kot na primer za $n = 23471$. V tem zadnjem primeru je W. Keller leta 1984 ugotovil, da je število F_{23471} deljivo z $2^{23473} \cdot 5 + 1$. To Fermatovo število je tudi eno največjih števil, ki so jih do zdaj raziskovali. Število njegovih cifer v desetiškem zapisu namreč močno presega število delcev v vesolju. Le teh naj bi bilo "samo" $51 \cdot 2^{260}$.

Vsi ti rezultati podpirajo domnevo, da so števila F_n za $n \geq 5$ sestavljena. To pa je še vedno nerešen problem.

Naloge:

1. Dokaži, da je število $2^m + 1$ sestavljeno, če naravno število $m > 1$ ni potenca števila 2!

---

[4] Izrek je dokazan v knjigi : W. Sierpinski, *Elementary Theory of Numbers*, Varšava 1964, str. 347.

2. Števila F_n resda niso vsa praštevila, so si pa paroma tuja. Dokaži!
3. S pomočjo prejšnje naloge pokaži, da množica vseh praštevil ne more biti končna!
4. Pokaži, da so števila $2^{2^n} + 5$, $n = 1, 2, 3, \ldots$, sestavljena!
5. S pomočjo "približne identitete" $2^{10} \doteq 10^3$ oceni število števk Fermatovega števila F_{23471}!
6. Katero število je večje F_n ali $(2^2)^n + 1$?

Rešitve nalog:

1. Denimo, da je $m = 2^k l$, kjer sta k in l taki (enolično določeni) nenegativni celi števili, da je l liho število. Po predpostavki je $l \geq 3$. S pomočjo znane formule o vsoti dveh lihih potenc dobimo, da je število

$$2^m + 1 = (2^{2^k})^l + 1$$

deljivo z $2^{2^k} + 1$.

2. Z zaporedno uporabo formule $a^2 - b^2 = (a + b)(a - b)$ dobimo

$$2^{2^n} - 1 = (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1) =$$

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

$$\ldots = (2^{2^{n-1}} + 1)(2^{2^{n-2}} + 1)(2^{2^{n-3}} + 1) \ldots (2^2 + 1)(2^2 - 1) =$$

$$= 3\, F_1\, F_2\, F_3 \ldots F_{n-1}.$$

Torej velja

$$F_n - 3\, F_1\, F_2\, F_3 \ldots F_{n-1} = 2. \qquad (l)$$

Če bi števili F_m in F_n $(m < n)$ imeli skupen delitelj, večji od 1, bi le ta delil tudi število 2 in bi bil zato enak 2. To pa je nemogoče, saj so vsa Fermatova števila F_n liha.

3. Denimo, da ima množica vseh praštevil n elementov. Potem bi bili med Fermatovimi števili F_1, F_2, ..., F_n, F_{n+1} vsaj dve deljivi z istim praštevilom. Protislovje!

4. Iz zveze (1) dobimo

$$F_n + 4 = 3(F_1 F_2 F_3 \ldots F_{n-1} + 2).$$

Torej so števila $2^{2^n} + 5$ deljiva s 3.

5. Približno velja

$$2^{23471} \doteq 10^{3 \cdot 23471/10} \doteq 10^{7041}.$$

Zato je

$$F_{23471} \doteq 2^{10^{7041}} \doteq 10^{3 \cdot 10^{7041}/10} \doteq 10^{10^{7040}}.$$

Torej ima Fermatovo število F_{23471} v desetiškem zapisu približno 10^{7040} števk, kar je neprimerno več kot je število delcev v vesolju.

6. S pomočjo indukcije je lahko videti, da je $2n \leq 2^n$ za vsako naravno število n. Enakost velja le v primeru, ko je $n = 1$. Zato velja neenakost

$$(2^2)^n = 2^{2n} \leq 2^{2^n}.$$

Torej je večje Fermatovo število F_n; števili sta enaki le za $n = 1$.

Roman Drnovšek