Fermatova števila in konstrukcije pravilnih večkotnikov

MATEJ MLAKAR

Pierre de Fermat (1601–1655), eden največjih matematikov svojega časa, je v svojem širokem opusu matematičnega ustvarjanja najbolj izstopal s svojimi rezultati iz teorije števil. Verjetno je najbolj znan po zadnjem Fermatovem izreku, ki pravi:

> **Enačba $a^n + b^n = c^n$ nima rešitev v množici naravnih števil za a, b, c, če je naravno število $n \geq 3$.**

Problem, ki so ga razrešili šele leta 1993, je Fermat našel v prevodu Diofantove *Aritmetike*. Na rob lista je zapisal, da „ima dokaz, vendar je na robu zanj premalo prostora“.

Po velikem matematiku se imenujejo tudi *Fermatova števila*. To so števila F_n, ki jih definiramo kot

- $F_n = 2^{2^n} + 1, \quad$ kjer je $\quad n \in \mathbb{N}_0$.

Leta 1640 je Fermat postavil hipotezo, v kateri je trdil, da *so vsa števila F_n praštevila.* Njegova domneva je najverjetneje posledica tega, da so Fermatova števila od $F_0 = 3$ do vključno $F_4 = 2^{2^4} + 2 = 65537$ res praštevila.

Hitro pa se da pokazati, da $F_5 = 2^{32} + 1$ ni praštevilo; velja namreč $641 = 2^4 + 5^4$ in $641 = 2^7 \cdot 5 + 1$. Torej je $2^7 \cdot 5 = 641 - 1$ in $2^{28} \cdot 5^4 = (641 - 1)^4 = 641m + 1$, kjer je $m \in \mathbb{N}$. Po drugi strani pa je $5^4 = 641 - 2^4$, tako da je $2^{28} \cdot (641 - 2^4) = 641 \cdot t + 1$, kjer je $t \in \mathbb{N}$. Sledi $641 \cdot 2^{28} - 2^{32} = 641t + 1$ in nato $2^{32} + 1 = 641(2^{28} - t)$, kar pomeni, da $641 | F_5$.

Fermatovo zmoto je prvi uvidel **Euler**. Na svojstven način je pokazal, da so morebitni delitelji Fermatovih števil oblike $k \cdot 2^{n+1} + 1$, kjer je $k \in \mathbb{N}$. Za $n = 5$ je delitelja števila $F_5 = 4294967297$ iskal v množici $64k + 1$ in ga tudi našel za $k = 10$ v številu 641. Kljub utemeljitvi na napačni hipotezi so Fermatova števila preživela v svetu teorije števil, saj imajo mnogo zanimivih lastnosti. Tako lahko hitro pokažemo, da so

vsa Fermatova števila paroma tuja.

Za vsako Fermatovo število F_n namreč velja $F_n - 2 = F_0 \cdot F_1 \cdot F_2 \cdots F_{n-1}$ (glej nalogo 1). Če je torej naravno število d delitelj števila F_n in števila F_m, kjer je $m < n$, potem d deli tudi $F_n - 2$, kar pomeni, da d deli 2. Ker pa so vsa Fermatova števila liha, mora biti $d = 1$.

Zgornjo lastnost je uporabil **Christian Goldbach** (1690–1764), znan po *Goldbachovi domnevi*[1], ko je leta 1730 podal zanimiv

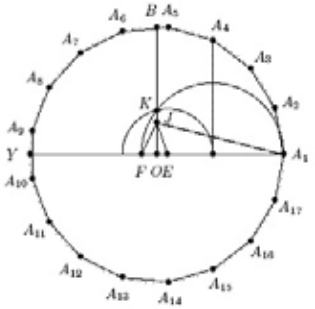
dokaz o obstoju neskončno praštevil.

Označimo s p_n praštevilski delitelj števila F_n. Ker vemo, da so si vsa Fermatova števila paroma tuja, so tudi vsi praštevilski delitelji različni, kar pomeni, da je tudi praštevil neskončno.

Povezanost med Fermatovimi števili in evklidsko geometrijo je ugotovil **Carl Friedrich Gauss.** Tako je leta 1796 uspel skonstruirati pravilni sedemnajstkotnik samo z uporabo šestila in ravnila. Potek konstrukcije je dokaj zapleten, dinamičen prikaz si lahko ogledate na spletni strani [1], dokaz pravilnosti konstrukcije pa v [2]. Gauss je odkril, da lahko

> **pravilni n-kotnik skonstruiramo s šestilom in ravnilom, če je število stranic enako $2^k p_1 p_2 \cdots p_n$, kjer je $k \in \mathbb{N}_0$, $p_1, p_2, \ldots, p_n$ pa so različna Fermatova praštevila.**

[1] Vsako sodo število, ki je večje od 2, se da zapisati kot vsota dveh praštevil.



Slika 1.

Danes vemo, da lahko pravilne večkotnike, ki imajo 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, ... stranic, narišemo s šestilom in ravnilom. Nedavno so uspeli pokazati, da so vsa Fermatova števila od F_5 do vključno F_{32} sestavljena števila, čeprav poznamo celotno faktorizacijo le za $5 \le n \le 11$.

Tako je prvi pravilni večkotnik, za katerega ne vemo, če ga je mogoče skunstruirati, večkotnik z $F_{33} = 2^{2^{33}} + 1$ stranicami.

Zanimivo je, da šestega Fermatovega praštevila še ne poznamo. V dobi računalnikov in hitrih procesorjev se zanimanje za Fermatova števila povečuje. Tako lahko na spletni strani [3] vsak aktivno sodeluje v njihovi faktorizaciji in iskanju morebitnega novega Fermatovega praštevila. Trenutni rekord v iskanju praštevilskega delitelja največjega Fermatovega števila ima irski matematik John Cosgrave, ki je uspel s pomočjo računalnika pokazati, da je $3 \cdot 2^{2478785} + 1$ praštevilski delitelj števila $F_{2478782}$ (glej [4]).

■ Naloge

1. Z matematično indukcijo pokaži, da je za $n \in \mathbb{N}$.

- $(2^{2^0}+1)(2^{2^1}+1)(2^{2^2}+1)\cdots(2^{2^{n-1}}+1) = (2^{2^n}-1)$.

2. Uporabi Eulerjev praštevilski kriterij za Fermatova števila in preveri, ali je F_4 praštevilo.

3. Dokaži lastnosti Fermatovih števil:

(a) $F_{n+1} = (F_n - 1)^2 + 1$, kjer je $n \in \mathbb{N}_0$;

(b) $F_{n+1} = F_n + 2^{2^n} F_0 F_1 \cdots F_{n-1}$, kjer je $n \in \mathbb{N}$;

(c) $F_{n+1} = F_n^2 - 2(F_{n-1} - 1)^2$, kjer je $n \in \mathbb{N}$.

4. Dokaži, da je za vsako naravno število $n > 1$ števka na mestu enic števila F_n enaka 7.

■ Rešitve

1. Preverimo za $n = 1$. Res je $(2^{2^0} + 1) = 2^{2^1} - 1$. Naj velja trditev za n, dokažimo še za $n + 1$: zaradi indukcijske predpostavke velja

- $$\underbrace{(2^{2^0}+1)(2^{2^1}+1)\cdots(2^{2^{n-1}}+1)}_{(2^{2^n}-1)} \cdot (2^{2^n}+1) =$$
$$= \left(2^{2^n}\right)^2 - 1 = 2^{2^{n+1}} - 1.$$

To med drugim tudi pomeni, da je $F_n - 2 = F_0 \cdot F_1 \cdot F_2 \cdots F_{n-1}$.

2. Po Eulerjevem kriteriju morajo imeti vsa praštevila, ki delijo F_4, obliko $k \cdot 2^5 + 1 = 32k + 1$, kjer je $k \in \mathbb{N}$. Števil, manjših ali enakih 66537, ki so take oblike, je 2048, smiselno pa je preverjati števila do vrednosti $\sqrt{65537} \sim 256$. Postavljenim zahtevam ustreza sedem števil. Ta so $33, 65, 97, 129, 161, 193$ ter 225. Števila $33, 65, 129, 225$ ter 161 niso praštevila, praštevili 97 in 193 pa nista delitelja F_4, zato mora biti F_4 praštevilo.

3. **(a)** $F_{n+1} = 2^{2^{n+1}} + 1 = 2^{2^n \cdot 2} + 1 = \left(2^{2^n}\right)^2 + 1 =$

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

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

$$= (F_n - 2)F_n + 2 = (F_n^2 - 2F_n + 1) + 1 =$$

$$= (F_n - 1)^2 + 1$$

(b) Pokažimo raje, da je

- $F_{n+1} - F_n = 2^{2^n} \cdot F_0 F_1 \cdots F_{n-1}$,

na koncu pa si pomagajmo z nalogo 1:

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

$$= 2^{2^{n+1}} - 2^{2^n} = 2^{2 \cdot 2^n} - 2^{2^n} = 2^{2^n + 2^n} - 2^{2^n} =$$

$$= 2^{2^n}(2^{2^n} - 1) = 2^{2^n}(F_n - 2) = 2^{2^n} F_0 F_1 \cdots F_{n-1}$$

(c) Uporabimo lastnost iz (a):

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

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

4. Če je $n > 1$, je 2^n večkratnik števila 4. Naj bo $2^n = 4k$, kjer je $k \in \mathbb{N}$, zato je $F_n = 2^{2^n} + 1 = 2^{4k} + 1$. Ker lahko 2^{4k} preoblikujemo v

- $2^{4k} = 16^k = (15 + 1)^k =$

  $= 15^k + \binom{k}{1}15^{k-1} + \binom{k}{2}15^{k-2} + \ldots + \binom{k}{k-1}15 + 1 =$

  $= 5m + 1\,,$

kjer je $m \in \mathbb{N}$, ima 2^{4k} ostanek 1 pri deljenju s 5. Torej je ostanek F_n pri deljenju s 5 enak 2, če je $n > 1$. Števka na mestu enic je lahko 2 ali pa 7. Ker je Fermatovo število liho, je števka enaka 7.

Literatura

[1] http://www2.arnes.si/~mmlaka10/fermat/n17/17kotnik.htm

[2] H. Dörrie: *100 Great Problems of Mathematics*, Dover publications, New York, 1965, str. 177–184.

[3] http://www.fermatsearch.org

[4] http://www.prothsearch.net/fermat.html

Družinska

BORIS LAVRIČ

Simona, ki je pravkar praznoval svoj rojstni dan, je obiskal njegov pozabljivi ded Jaka. Voščil mu je in ga povprašal o starosti. Simon mu je ponagajal: „Seštej števke (= cifre) moje rojstne letnice, pa jo dobiš," in nadaljeval: „In koliko let imaš ti?"

Jaka ni od muh in je brž izračunal vnukovo starost in ga zaposlil z naslednjim odgovorom na njegovo vprašanje: "Zmnoži števke moje rojstne letnice in dobil boš mojo starost." Simon ni padel daleč od Jake in je kmalu izračunal dedovo starost. Poiščite jo še vi in ugotovite, kateri rojstni dan je pravkar praznoval Simon.

Koledarji

REŠITEV NALOGE

DARJO FELDA

Z zbiranjem lahko konča, če ima v zbirki 14 različnih letnih koledarjev (prvi dan v letu je lahko katerikoli izmed sedmih dni v tednu, pa še na navadna in prestopna leta moramo paziti). Označimo z D_1, $D_2, \ldots, D_7$ dneve v tednu. Cikel štirih zaporednih let ima $366 + 3 \cdot 365$ dni ali 208 tednov in 5 dni. Če se je prvo prestopno leto po letu 1970, to je leto 1972, začelo z D_1, se naslednja prestopna leta začnejo takole: $1976 - D_6$, $1980 - D_4$, $1984 - D_2$, $1988 - D_7$, $1992 - D_5$, $1996 - D_3$. Leta 1996 je torej dedek zbral vse različne letne koledarje za prestopna leta.

Do tedaj je zagotovo zbral tudi vse različne letne koledarje za navadna leta. Navadna leta neposredno pred prestopnimi se namreč začnejo z dnem v tednu, ki je neposredno pred dnevom v tednu, s katerim se začnejo ta prestopna leta (tako imamo $1971 - D_7$, $1975 - D_5$, $1979 - D_3\,, \ldots, 1995 - D_2$). V resnici pa je dedek že leta 1978 imel vse možne koledarje za navadna leta.