Самоил Малчески , Скопје
Ристо Малчески, Скопје

ФЕРМАТОВИ БРОЕВИ

Многу математичари безуспешно се обидувале да најдат општа формула која ќе генерира само прости броеви, т.е. функција $f(n)$ чии вредности, за сите природни броеви n, ќе бидат прости броеви. Во оваа насока е и неточната хипотеза на големиот математичар Ферма. Тој ги проучувал броевите од видот $f_n = 2^{2^n} + 1$, каде n е природен број. Овие броеви, во негова чест, по неговата смрт се наречени *Ферматови броеви*. За првите пет вредности на бројот n, Ферма ги добил броевите $f_0 = 3$, $f_1 = 5$, $f_2 = 17$, $f_3 = 257$, $f_4 = 65537$ и со проверка утврдил дека тие се прости броеви. Ферма ја искажал хипотезата дека и за секој природен број $n \geq 5$, бројот f_n е прост. Меѓутоа, Ојлер докажал дека бројот f_5 е производ на два прости броја, т.е. дека

$$f_5 = 2^{32} + 1 = 2^{28}(5^4 + 2^4) - (5 \cdot 2^7)^4 + 1 = 2^{28} \cdot 641 - (640^4 - 1)$$
$$= 641(2^{28} - 639(640^2 + 1)) = 641 \cdot 6700417 = 4294967297.$$

Да споменеме дека до денес не е најден ниту еден прост Ферматов број поголем од f_4. Затоа се добило впечаток дека Ферматовите броеви не се од посебен интерес, но се покажало тие имаат низа интересни својства, без разлика дали се прости или сложени.

Прашање дали Ферматовиот број е прост или сложен е тесно поврзано со проблемот за конструкција на правилен многуаголник само со помош на шестар и линијар. Имено, Гаус ја докажал следнава теорема, чиј доказ нема да го презентираме бидејќи излегува надвор од рамките на нашите разгледувања.

Теорема. Правилен n-аголник може да се конструира со линијар и шестар ако и само ако $n = 2^s p_1 p_2 ... p_k$, $k > 0$, каде $s \in \mathbb{N}_0$, а $p_1, p_2, ..., p_k$ се различни Ферматови прости броеви или $n = 2^s$, каде $s \in \mathbb{N} \setminus \{1\}$. ■

1. Основни својства на Ферматовите броеви

Во следните разгледувања ќе дадеме повеќе својства на Ферматовите броеви.

Теорема 1. За секој $n \geq 1$ важи

$$f_n = (f_{n-1} - 1)^2 + 1. \qquad (1)$$

Доказ. *Прв начин*. Тврдењето ќе го докажеме со математичка индукција.

За $n=1$ имаме $(f_0-1)^2+1=(3-1)^2+1=5=f_1$, т.е. точна е формулата (1).

Нека претпоставиме дека (1) важи за $n=k$, т.е.

$$f_k=(f_{k-1}-1)^2+1. \qquad (2)$$

Ако ја искористиме (2), за $n=k+1$ добиваме

$$\begin{aligned}(f_k-1)^2+1&=((f_{k-1}-1)^2+1-1)^2+1\\&=(f_{k-1}-1)^4+1=(2^{2^{k-1}}+1-1)^4+1\\&=(2^{2^{k-1}})^4+1=2^{4\cdot 2^{k-1}}+1\\&=2^{2^2\cdot 2^{k-1}}+1=2^{2^{k+1}}+1\\&=f_{k+1},\end{aligned}$$

т.е. формулата (1) е точна и за $n=k+1$, па од принципот на математичка индукција следува дека таа е точна за секој природен број n.

Втор начин. Имаме

$$(f_{n-1}-1)^2+1=(2^{2^{n-1}}+1-1)^2+1=(2^{2^{n-1}})^2+1=2^{2\cdot 2^{n-1}}+1=2^{2^n}+1=f_n. \blacksquare$$

Теорема 2. За секој $n\geq 2$ важи

$$f_n=f_{n-1}^2-2(f_{n-2}-1)^2. \qquad (3)$$

Доказ. *Прв начин*. Тврдењето ќе го докажеме со математичка индукција.

За $n=2$ имаме $f_1^2-2(f_0-1)^2=5^2-2(3-1)^2=17=f_2$, т.е. точна е формулата (3).

Нека претпоставиме дека (3) важи за $n=k$, т.е.

$$f_k=f_{k-1}^2-2(f_{k-2}-1)^2. \qquad (4)$$

Ако ја искористиме (4), за $n=k+1$ добиваме

$$\begin{aligned}f_k^2-2(f_{k-1}-1)^2&=(f_{k-1}^2-2(f_{k-2}-1)^2)^2-2(f_{k-1}-1)^2\\&=((2^{2^{k-1}}+1)^2-2(2^{2^{k-2}}+1-1)^2)^2-2(2^{2^{k-1}}+1-1)^2\\&=(2^{2^k}+2\cdot 2^{2^{k-1}}+1-2(2^{2^{k-2}})^2)^2-2(2^{2^{k-1}})^2\\&=(2^{2^k}+2\cdot 2^{2^{k-1}}+1-2\cdot 2^{2^{k-1}})^2-2\cdot 2^{2^k}\\&=(2^{2^k}+1))^2-2\cdot 2^{2^k}\\&=2^{2^{k+1}}+2\cdot 2^{2^k}+1-2\cdot 2^{2^k}\\&=2^{2^{k+1}}+1=f_{k+1},\end{aligned}$$

т.е. формулата (3) е точна и за $n=k+1$, па од принципот на математичка индукција следува дека таа е точна за секој природен број n.

Втор начин. Според теорема 1 имаме $(f_{n-2}-1)^2 = f_{n-1}-1$, па затоа важи

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

што и требаше да се докаже. ■

Теорема 3. За Ферматовите броеви $f_0, f_1, ..., f_n, f_{n+1}$ важи

$$f_{n+1} = f_0 f_1 ... f_n + 2\,. \tag{5}$$

Доказ. *Прв начин*. Имаме

$$f_0 f_1 ... f_n + 2 = (2^{2^0}+1)(2^{2^1}+1)(2^{2^2}+1)...(2^{2^{n-1}}+1)(2^{2^n}+1)+2$$
$$=(2^{2^0}-1)(2^{2^0}+1)(2^{2^1}+1)(2^{2^2}+1)...(2^{2^{n-1}}+1)(2^{2^n}+1)+2$$
$$=(2^{2^1}-1)(2^{2^1}+1)(2^{2^2}+1)...(2^{2^{n-1}}+1)(2^{2^n}+1)+2$$
$$=(2^{2^2}-1)(2^{2^2}+1)...(2^{2^{n-1}}+1)(2^{2^n}+1)+2$$
....
$$=(2^{2^{n-1}}-1)(2^{2^{n-1}}+1)(2^{2^n}+1)+2$$
$$=(2^{2^n}-1)(2^{2^n}+1)+2$$
$$=2^{2^{n+1}}-1+2=2^{2^{n+1}}+1= f_{n+1},$$

што и требаше да се докаже.

Втор начин. Тврдењето ќе го докажеме со математичка индукција.

За $n=0$ имаме $f_0+2=3+2=5= f_1$, т.е. точна е формулата (5).

Нека претпоставиме дека (5) важи за $n=k-1$, т.е.

$$f_k = f_0 f_1 ... f_{k-1}+2 \tag{6}$$

Ако ја искористиме (6), за $n=k$ добиваме

$$f_0 f_1 ... f_{k-1} f_k + 2 = (f_k-2) f_k + 2$$
$$=(2^{2^k}+1-2)(2^{2^k}+1)+2$$
$$=(2^{2^k}-1)(2^{2^k}+1)+2$$
$$=2^{2^{k+1}}+1= f_{k+1}$$

т.е. формулата (5) е точна и за $n=k$, па од принципот на математичка индукција следува дека таа е точна за секој природен број n. ■

Теорема 4. За секој природен број $n \geq 1$ важи

$$f_{n+1} = f_n + 2^{2^n} f_0 f_1 ... f_{n-1}\,. \tag{7}$$

Доказ. Од теорема 3 следува

$$\begin{aligned} f_n + 2^{2^n} f_0 f_1 \dots f_{n-1} &= f_n + 2^{2^n}(f_n - 2) \\ &= 2^{2^n} + 1 + 2^{2^n}(2^{2^n} + 1 - 2) \\ &= 2^{2^n} + 1 + (2^{2^n})^2 - 2^{2^n} \\ &= 2^{2^{n+1}} + 1 \\ &= f_{n+1}, \end{aligned}$$

што и требаше да се докаже. ■

Теорема 5. Ако $m \neq n$, тогаш Ферматовите броеви f_m и f_n се заемно прости.

Доказ. Нека се f_n и f_{n+k}, $k > 0$, два различни Ферматови броја и нека претпоставиме дека m е природен број, таков да $m \mid f_n$ и $m \mid f_{n+k}$. Земаме $x = 2^{2^n}$ и добиваме

$$\frac{f_{n+k}-2}{f_n} = \frac{2^{2^{n+k}}+1-2}{2^{2^n}+1} = \frac{2^{2^n 2^k}-1}{2^{2^n}+1} = \frac{(2^{2^n})^{2^k}-1}{2^{2^n}+1} = \frac{x^{2^k}-1}{x+1} = x^{2^k-1} - x^{2^k-2} + \dots - 1,$$

што значи дека $f_n \mid (f_{n+k} - 2)$, па од $m \mid f_n$ следува дека $m \mid (f_{n+k} - 2)$. Но, од $m \mid f_{n+k}$ и $m \mid (f_{n+k} - 2)$ следува дека $m \mid 2$ и како Ферматовите броеви се непарни добиваме дека $m = 1$, што значи дека броевите f_n и f_{n+k}, $k > 0$ се заемно прости. ■

Теорема 6. За секој $n \geq 0$ важи $f_n \mid (2^{f_n} - 2)$.

Доказ. Ако го искористиме познатото неравенство $2^n \geq n+1$, за секој $n \in \mathbb{N}$, добиваме дека $2^{n+1} \mid 2^{2^n}$, од што следува дека $(2^{2^{n+1}} - 1) \mid (2^{2^{2^n}} - 1)$. Но, $(2^{2^n} + 1) \mid (2^{2^{n+1}} - 1)$, па затоа $(2^{2^n} + 1) \mid (2^{2^{2^n}} - 1)$, што значи

$$(2^{2^n} + 1) \mid 2(2^{2^{2^n}} - 1) = 2^{2^{2^n}+1} - 2 \text{, т.е. } f_n \mid (2^{f_n} - 2). \ ■$$

2. Примена на Ферматовите броеви

Покрај споменатата теорема на Гаус за тоа кога само со линијар и шестар може да се конструира правилен многуаголник, со Ферматовите броеви се докажуваат и други важни математички тврдења. Да разгледаме некои од нив.

Теорема 7. Постојат бесконечно многу прости броеви.

Доказ. Според теорема 5 Ферматовите броеви се по парови заемно прости, па затоа секој Ферматов број е делив со некој непарен прост број кој не е делител на ниту еден друг Ферматов број. Но, Ферматови броеви има бесконечно многу, па оттука следува дека и прости броеви има бесконечно многу. ■

Теорема 8. Ако природниот број $n>1$ не е степен на бројот 2, тогаш 2^n+1 е сложен број.

Доказ. Нека претпоставиме дека бројот n не е степен на бројот 2 и да го разгледаме бројот 2^n+1. Можни се два случаја: n е прост број или n е сложен, односно $n=2^s r$, каде r е непарен број поголем од 1. Во вториот случај, ако $s>1$, тогаш r е непарен број поголем од 1, а ако $s=0$, тогаш r е непарен сложен број.

Ако $n\geq 5$ е прост број, тогаш $n=6k\pm 1, k\in\mathbb{N}$, па затоа

$$2^n+1=2^{6k+1}+1=(2+1)(2^{6k}-2^{6k-1}+...-2+1)\text{, т.е. } 3\,|\,(2^n+1)$$

или

$$2^n+1=2^{6k-1}+1=(2+1)(2^{6k-2}-2^{6k-3}+...-2+1)\text{, т.е. } 3\,|\,(2^n+1)\text{,}$$

што значи дека и во двата случаја 2^n+1 е сложен број.

Ако $n=2^s r$, каде r е непарен број поголем од 1, тогаш

$$2^n+1=2^{2^s r}+1=(2^{2^s})^r+1=(2^{2^s}+1)[(2^{2^s})^{r-1}-(2^{2^s})^{r-2}+...-2^{2^s}+1]$$

т.е. $(2^{2^s}+1)\,|\,(2^n+1)$, што значи дека 2^n+1 е сложен број. ■

Последица 1. Бројот 2^n+1, $n\in\mathbb{N}$ е прост само ако е Ферматов број.

Доказ. Непосредно следува од теорема 8. ■

3. Решени задачи

Во овој дел ќе разгледаме неколку задачи поврзани со Ферматовите броеви, а поголем број решени задачи може да се најдат во [2].

Задача 1. Докажи дека ниту еден од Ферматовите броеви

$$f_n=2^{2^n}+1, n=2,3,...$$

не може да се запише како збир на два прости броја.

Решение. Броевите $f_n, n=2,3,...$ се непарни. Затоа, ако бројот f_n може да се запише како збир на два прости броја, тогаш едниот од нив мора да е парен, т.е. бројот 2, па другиот е бројот f_n-2. Но, ако $n>1$ тогаш

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

не е прост број. ■

Задача 2. Докажи дека Ферматовиот прост број $p = 2^{2^n} + 1$, $n \in \mathbb{N}$ не може да биде запишан како разлика на петти степени на два природни броја.

Решение. Нека

$$p = a^5 - b^5 = (a-b)(a^4 + a^3b + a^2b^2 + ab^3 + b^4),\ a,b \in \mathbb{N}.$$

Бидејќи p е прост број $a - b = 1$, т.е. $a = b+1$, $b \in \mathbb{N}$. Сега

$$a^5 - b^5 = (b+1)^5 - b^5 = 5b^5 + 10b^3 + 10b^2 + 5b + 1,$$

па затоа $5b^5 + 10b^3 + 10b^2 + 5b = 2^{2^n}$, што не е можно, бидејќи левата страна на последното равенство е делива со 5, а десната не е делива со 5. ■

Задача 3. Докажи, дека Ферматов број не може да биде точен квадрат на природен број.

Решение. Имаме $f_0 = 3$ и $f_1 = 5$ и тоа не се точни квадрати. Понатаму, лесно се докажува дека за $n \geq 2$ Ферматовиот број f_n има цифра на единици 7, па тој не може да биде точен квадрат, бидејќи цифрата на единиците на секој точен квадрат е 0, 1, 4, 5, 6 или 9. ■

Задача 4. Докажи дека ниту еден од Ферматовите броеви $f_n = 2^{2^n} + 1$, $n = 0,1,2,3,...$ не е точен куб.

Решение. Нека претпоставиме дека $2^{2^n} + 1 = k^3$ за некои природни броеви n и k. Јасно, k е непарен број и важи

$$2^{2^n} = k^3 - 1 = (k-1)(k^2 + k + 1).$$

Според тоа, $k - 1 = 2^s$ и $k^2 + k + 1 = 2^t$ за некои природни броеви s и t. Тогаш

$$2^t - 2^{2s} = k^2 + k + 1 - (k-1)^2 = 3k,$$

што не е можно, бидејќи $2^t - 2^{2s}$ е парен, а $3k$ е непарен број. ■

Литература

1. Baćić, Lj.: Fermatovi brojevi, Osječki matematički list (2023), 21-31
2. Малчески, Р.: Збирка задачи по теорија на броеви, Математички талент, Скопје, 2022
3. Малчески, Р.: Теорија на броеви, Математички талент, Скопје, 2022