Ристо Малчески, Скопје
Катерина Аневска, Скопје

МАЛА ТЕОРЕМА НА ФЕРМА

Францускиот љубител на математиката Пјер Ферма, кој по професија бил правник, дал забележителен придонес во развојот на теоријата на броеви. Негова најпозната теорема е таканаречената голема теорема на Ферма, која се однесува на решението на равенката $x^n + y^n = z^n$, $x, y, z, n \in \mathbf{N}$ и $n \geq 3$, и за која Ферма тврдел дека нема решение, но дека на маргината на книгата нема доволно место да го испише доказот. За да се докаже ова тврдење биле потребни неколку стотици години, но бројните обиди да се најде доказ придонесле за развојот на многу математички дисциплини. Дел од нив денес лежат во основата на современата математика и информатика.

Во нашите разгледувања нема да се задржуваме на големата теорема на Ферма, туку ќе ја разгледаме примената на таканаречената мала теорема на Ферма, која ќеја прифатиме без доказ. Притоа, да напоменеме дека, за решавање на задачи во кои се применува оваа теорема неопходни се знаења за конгруенциите во множеството цели броеви (види [1], [2] и [3]).

Теорема 1 (Ферма). Ако p е прост број и $\text{NZD}(a, p) = 1$, тогаш

$$a^{p-1} \equiv 1 \pmod{p}. \blacksquare$$

Последица 1. Ако p е прост број, тогаш за секој цел број a важи

$$a^p \equiv a \pmod{p}.$$

Доказ. Ако $p \mid a$, тогаш јасно $a^p \equiv a \pmod{p}$. Ако $p \nmid a$, тогаш од теорема 1 следува $a^{p-1} \equiv 1 \pmod{p}$, и ако последната конгруенцијата ја помножиме со a добиваме $a^p \equiv a \pmod{p}$. $\blacksquare$

Да разгледаме неколку примери.

Пример 1. Ако p и q се различни прости броеви, тогаш

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Докажи!

Решение. Од теорема 1 следува $q \mid (p^{q-1} - 1)$ и $p \mid (q^{p-1} - 1)$. Според тоа $pq \mid (p^{q-1} - 1)(q^{p-1} - 1)$, т.е.

$$pq \mid (p^{q-1}q^{p-1} - p^{q-1} - q^{p-1} + 1). \tag{1}$$

Бидејќи p и q се прости броеви важи

$$pq \mid p^{q-1}q^{p-1}. \tag{2}$$

Од (1) и (2) непосредно следува дека $pq \mid (p^{q-1} + q^{p-1} - 1)$, т.е.

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}. \blacksquare$$

Пример 2. Определи го остатокот од делењето на бројот $(85^{74}+19^{99})^{16}$ со 13.

Решение. Бидејќи 13 е прост број и $13\nmid 85$ од теоремата на Ферма следува $85^{12}\equiv 1(\mathrm{mod}\,13)$, па затоа $85^{72}\equiv 1(\mathrm{mod}\,13)$. Од друга страна $85\equiv 7(\mathrm{mod}\,13)$, па затоа $85^2\equiv 49\equiv -3(\mathrm{mod}\,13)$. Според тоа, $85^{74}\equiv -3(\mathrm{mod}\,13)$.

Аналогно, $19^{12}\equiv 1(\mathrm{mod}\,13)$, од каде следува дека $19^{96}\equiv 1(\mathrm{mod}\,13)$. Но, $19\equiv 6(\mathrm{mod}\,13)$, $19^2\equiv 36\equiv -3(\mathrm{mod}\,13)$ и $19^3\equiv -3\cdot 6\equiv -5(\mathrm{mod}\,13)$. Според тоа, $19^{99}\equiv -5(\mathrm{mod}\,13)$.

Од досега изнесеното следува дека

$$85^{74}+19^{99}\equiv -8\equiv 5(\mathrm{mod}\,13).$$

Но, $5^2\equiv -1(\mathrm{mod}\,13)$, па затоа $5^{16}\equiv 1(\mathrm{mod}\,13)$, т.е.

$$(85^{74}+19^{99})^{16}\equiv 1(\mathrm{mod}\,13).\ \blacksquare$$

Пример 3. Ако a е цел број таков што $\mathrm{NZD}(a,35)=1$, тогаш бројот

$$A=(a^4-1)(a^4+15a^2+1)$$

се дели со 35. Докажи!

Решение. Бидејќи $5\nmid a$ и 5 е прост број од теорема 1 следува $a^4\equiv 1(\mathrm{mod}\,5)$, т.е. $5\mid(a^4-1)$ и затоа $5\mid A$. Понатаму,

$$\begin{aligned}A&=(a^4-1)(a^4+15a^2+1)=(a^4-1)(a^4+14a^2+a^2+1)\\&=14a^2(a^4-1)+(a^2-1)(a^2+1)(a^4+a^2+1)\\&=14a^2(a^4-1)+(a^6-1)(a^2+1)\end{aligned}$$

Бидејќи $7\nmid a$, повторно од теорема 1 следува $a^6\equiv 1(\mathrm{mod}\,7)$. Така $7\mid(a^6-1)$ и $7\mid 14$, па затоа $7\mid A$. Конечно, од $5\mid A$, $7\mid A$ и $\mathrm{NZD}(5,7)=1$ следува $35\mid A$. $\blacksquare$

Пример 4. Ако a е цел број кој не е делив со 3, тогаш $a^{13}-a\equiv 0(\mathrm{mod}\,2^{13}-2)$. Докажи!

Решение. Имаме: $2^{13}-2=2\cdot 3^2\cdot 5\cdot 7\cdot 13$. Бидејќи множителите се заемно прости броеви доволно е да докажеме дека се исполнети конгруенциите

$$a^3-a\equiv 0(\mathrm{mod}\,m),\ \text{за}\ m=2,9,5,7\ \text{и}\ 13.$$

За $m=2,5,7$ и 13 точноста на последните конгруенции следува од теорема 1. Навистина, ако $m\mid a$, тогаш очигледно е дека $a^{13}-a\equiv 0(\mathrm{mod}\,m)$. Ако $\mathrm{NZD}(a,m)=1$ тогаш $a^{m-1}\equiv 1(\mathrm{mod}\,m)$, од каде степенувајќи со степен $\frac{12}{m-1}$ добиваме $a^{12}\equiv 1(\mathrm{mod}\,m)$, па затоа $a^{13}\equiv a(\mathrm{mod}\,m)$. Останува да го разгледаме случајот $m=9$. Бидејќи a не се дели со 3, имаме $a^2\equiv 1(\mathrm{mod}\,3)$, т.е. $a^2=1+3k$, $k\in\mathbf{Z}$. Оттука, $a^6=1+9k+27k^2+27k^3\equiv 1(\mathrm{mod}\,9)$, па затоа $a^{12}\equiv 1(\mathrm{mod}\,9)$, т.е. $a^{13}\equiv a(\mathrm{mod}\,9)$. $\blacksquare$

Пример 5. Нека p е прост број и $p = 4k+1, k \geq 1$ е природен број. Докажи дека важи $k^{2k} \equiv 1 (\mathrm{mod}\ p)$.

Решение. Очигледно $\mathrm{NZD}(k, p) = 1$. Од теоремата на Ферма следува дека $k^{4k} = k^{p-1} \equiv 1 (\mathrm{mod}\ p)$. Значи, $p \mid (k^{2k}+1)(k^{2k}-1)$ и доволно е да докажеме дека $p \nmid (k^{2k}+1)$, од што ќе следува дека $p \mid (k^{2k}-1)$.

Нека претпоставиме дека $p \mid (k^{2k}+1)$. Тогаш $k^{2k} \equiv -1 \equiv 4k (\mathrm{mod}\ p)$ и од $\mathrm{NZD}(k, p) = 1$ добиваме дека $k^{2k-1} \equiv 2^2 (\mathrm{mod}\ p)$. Ако двете страни на последната конгруенција ги степенуваме на степен $\frac{p-1}{2} = 2k$ добиваме $k^{2k(2k-1)} \equiv 2^{p-1} (\mathrm{mod}\ p)$. Но, од теоремата на Ферма следува $2^{p-1} \equiv 1 (\mathrm{mod}\ p)$, па затоа $k^{2k(2k-1)} \equiv 1 (\mathrm{mod}\ p)$. Конечно, од последната конгруенција и од $k^{2k} \equiv -1 (\mathrm{mod}\ p)$ добиваме дека $p = 2$, што е противречност. Од добиената противречност следува тврдењето на задачата. ■

Пример 6. Докажи дека за секој природен број n бројот $2^{2^{10n+1}} + 19$ е сложен.

Решение. Од теоремата на Ферма следува дека $2^{10} \equiv 1 (\mathrm{mod}\, 11)$, па затоа $2^{10n} \equiv 1 (\mathrm{mod}\, 11)$, што значи дека бројот $2^{10n+1} - 2$ се дели со 22, т.е. $2^{10n+1} = 22k + 2$, за некој $k \in \mathbf{N}$. Оттука, повторно од теоремата на Ферма следува дека:

$$2^{2^{10n+1}} = 2^2 (2^{22})^k \equiv 4 \cdot 1^k \equiv 4 (\mathrm{mod}\, 23),$$

па затоа $23 \mid (2^{2^{10n+1}} + 19)$. Конечно, бидејќи $2^{2^{10n+1}} + 19 > 23$, за $n \geq 1$ добиваме дека секој природен број n бројот $2^{2^{10n+1}} + 19$ е сложен. ■

Пример 7. Ако p е прост број, тогаш $7p + 3^p - 4$ не е точен квадрат. Докажи!

Решение. Нека претпоставиме дека p е прост број поголем од 3 и

$$m = 7p + 3^p - 4$$

е точен квадрат. Нека $m = n^2$ за некој $n \in \mathbf{Z}$. Од теоремата на Ферма следува дека

$$m = 7p + 3^p - 4 \equiv 3 - 4 \equiv -1 (\mathrm{mod}\ p).$$

Ако $p = 4k + 3$, $k \in \mathbf{Z}$, тогаш повторно од теоремата на Ферма добиваме дека

$$-1 \equiv m^{2k+1} \equiv n^{4k+2} = n^{p-1} \equiv 1 (\mathrm{mod}\ p),$$

што е противречност. Така $p \equiv 1 (\mathrm{mod}\, 4)$. Тогаш $m = 7p + 3^p - 4 \equiv 3 - 1 \equiv 2 (\mathrm{mod}\, 4)$, што е противречност бидејќи точен квадрат не е конгруентен со 2 по модул 4. За $p = 2$ добиваме $m = 19$, и за $p = 3$ добиваме дека $m = 44$, што значи дека и во двата случаи $m = 7p + 3^p - 4$ не е точен квадрат. ■

Пример 8. Докажи дека секој прост број p е делител на бесконечно многу броеви од видот $2^n - n$.

Решение. Ако $p=2$, тогаш за $n=2k$ броевите од видот $2^{2k}-2k$ се деливи со $p=2$. Нека претпоставиме дека p е непарен прост број. Бидејќи $\text{NZD}(2,p)=1$ според теоремата на Ферма, добиваме дека $2^{p-1}\equiv 1 \pmod p$. Тогаш за било кој природен број m важи $(2^{p-1})^m \equiv 1^m \pmod p$, односно

$$2^{m(p-1)} \equiv 1 \pmod p. \qquad (1)$$

Нека m е природен број таков што $m \equiv -1 \pmod p$. Тогаш

$$m(p-1) \equiv -1(p-1) = 1 \pmod p \qquad (2)$$

Од (1) и (2) добиваме дека

$$2^{m(p-1)} - m(p-1) \equiv 0 \pmod p.$$

Броеви m кои го исполнуваат условот $m \equiv -1 \pmod p$ има бесконечно многу. Бидејќи $m \equiv -1 \pmod p$ добиваме дека $p \mid (m+1)$, односно дека $m = pk-1$ за некој природен број k. Обратно, секој број од видот $m = pk-1$ го исполнува условот $m \equiv -1 \pmod p$.

Множеството $\{n=(pk-1)(p-1) \mid k \in \mathbf{N}\}$ е бесконечно множество на природни броеви за кои е исполнет условот $p \mid (2^n - n)$. ■

Пример 9. Докажи дека за секој непарен прост број p постојат бесконечно многу природни броеви n такви што $p \mid (2^n n+1)$.

Решение. Нека n е непарен прост број и $n=(p-1)(kp+1)$, за $k=0,1,2,3,\ldots$. Имаме $n \equiv -1 \pmod p$. Согласно со теоремата на Ферма $2^{p-1} \equiv 1 \pmod p$ и ако последната конгруенција ја степенуваме на степен $kp+1$, добиваме дека $2^n \equiv 1 \pmod p$ Според тоа, $2^n n+1 \equiv (-1)\cdot 1+1 = 0 \pmod p$. Но, $k=0,1,2,3,\ldots$, па затоа постојат бесконечно многу природни броеви n со бараното својство. ■

Пример 10. Докажи дека меѓу броевите $(2^{2n}+1)^2+2^2$, каде $n=1,2,\ldots$ има бесконечно многу сложени броеви.

Решение. Такви се на пример сите броеви од дадената низа за кои $n=28k+1$, $k=1,2,3,\ldots$. Од теоремата на Ферма имаме $2^{28} \equiv 1 \pmod{29}$ па за $k=1,2,3,\ldots$ важи $2^{2\cdot 28k} \equiv 1 \pmod{29}$. Значи, за $n=28k+1$ важи

$$(2^{2n}+1)^2+2^2 \equiv 25+4 \equiv 0 \pmod{29},$$

т.е $29 \mid (2^{2n}+1)^2+2^2$ при што бидејќи за секој природен број k важи $n=28k+1 \geq 29$, следува дека $(2^{2n}+1)^2+2^2 > 29$. Оттука следува дека броевите $(2^{2n}+1)^2+2^2$, за $n=28k+1$, каде $k=1,2,3,\ldots$ се сложени. ■

Пример 11. Ако p е прост број, тогаш $p \mid 11\ldots1\underset{p}{}22\ldots2\underset{p}{}\ldots99\ldots9\underset{p}{}-123456789$. Докажи!

Решение. За $p=2,\ p=3,\ p=5$ тврдењето непосредно следува од признаците за деливост со броевите 2,3 и 5. Нека $p>5$. Тогаш имаме

$$N=\underbrace{11...1}_{p}\underbrace{22...2}_{p}...\underbrace{99...9}_{p}-123456789$$
$$=(10^p-1)+\frac{8}{9}10^p(10^p-1)+\frac{7}{9}10^{2p}(10^p-1)+...+\frac{1}{9}10^{8p}(10^p-1).$$

Од теорема 1 следува дека $10^p-1\equiv 10-1=9(\text{mod } p)$, односно $\frac{10^p-1}{9}\equiv 1(\text{mod } p)$, па затоа

$$N\equiv 9+8\cdot 10^p+7\cdot 10^{2p}+...+10^{8p}\equiv 9+8\cdot 10+7\cdot 10^2+...+10^8=123456789(\text{mod } p),$$

што всушност и требаше да се докаже. ■

На крајот од овој наш осврт на малата теорема на Ферма ќе наведеме неколку задачи за самостојна работа.

1. Докажи дека од $5|(2a^3-3a^2b+2b^3)$ следува дека $5|a$ и $5|b$.
2. Природните броеви a и b се такви што броевите $15a+16b$ и $16a-15b$ се полни квадрати на природни броеви. Најди ја минималната можна вредност на помалиот од тие квадрати.
3. Најди ги сите природни броеви x, y и z за кои важи $7^x+13^y=2^z$.
4. Нека $N=n(n+1)(n+2)(n+3)$, каде n е природен број. Да се докаже, дека не постои цел број m, за кој $N+m^9=2008$.
5. Нека n е природен број. Да се определи најмалиот природен број k за кој постојат природни броеви $a_1,a_2,...,a_k$ такви да
$$7\cdot 2^n=a_1^2+a_2^2+...+a_k^2.$$

ЛИТЕРАТУРА

1. Малчески, Р., Малчески, А., Аневска, К. (2015). Вовед во елементарна теорија на броеви, СММ, Скопје
2. Малчески, Р., Аневска, К. (2012). Конгруенции во множеството на целите броеви I, Нумерус, Скопје
3. Аневска, К., Малчески, Р. (2012). Конгруенции во множеството на целите броеви II, Нумерус, Скопје
4. Бойваленков, П.; Колев, Е.; Мушкаров, О.; Николов, Н.: Български математически състезания 2009-2011, УНИМАТ СМБ, София, 2012

Статијата прв пат е објавена во списанието НУМЕРУС на СММ