# ЕДНО ПРИЛОЖЕНИЕ НА МУЛТИПЛИКАТИВНАТА ИНДУКЦИЯ В СЪВРЕМЕННАТА АРИТМЕТИКА

**Румяна Несторова, гр.Враца**

Предлага се една приспособена за училищния курс по математика (УКМ) теоретична разработка на темата: теорема на Ферма и обобщението ù от Ойлер. Изложението се основава на методите пълна индукция и мултипликативна индукция. Темата е подходяща за извънкласна работа по математика в IX и X клас на СОУ.

1. Същност на методите на индукцията. Широко известен метод за доказване на твърдения за естествените числа е пълната математическа индукция.

Същността на този метод е следната: за да докажем верността на едно твърдение $\mathbf{H_n}$ за всяко естествено число $\mathbf{n}$, достатъчно е да установим верността на твърдението $\mathbf{H_1}$ за $\mathbf{n=1}$ ( доказателството може да започне и от друга начална стойност за $n$) и че винаги, когато за някое $\mathbf{n}$ е вярно твърдението $\mathbf{H_n}$, то вярно е също твърдението $\mathbf{H_{n+1}}$ за следващото естествено число $\mathbf{n+1}$. В основата на този метод лежи една от аксиомите на Пеано (т.нар. принцип на математическата индукция).

По– малко популярен е един друг метод за доказване на теореми в аритметиката– т.нар. мултипликативна индукция:

Нека по някакъв начин сме достигнали до хипотезата:

Всяко естествено число, по– голямо от 1 притежава свойството $\mathbf{P}$.

Доказателството ù чрез мултипликативна индукция протича по следната схема:

1. Доказваме, че всички прости числа притежават свойството $\mathbf{P}$.
2. Приемаме, че естественото число $\mathbf{m}$ притежава свойството $\mathbf{P}$.
3. Доказваме с помощта на това допускане, че числото $\mathbf{m.p}$ има

същото свойство $\mathbf{P}$, когато $\mathbf{p}$ е произволно просто число. С това верността на хипотезата е установена. Тя се опира на следната основна теорема на аритметиката: Всяко естествено число $\mathbf{n}$, по– голямо от 1, може да се разложи на произведение от краен брой прости множители по единствен начин с точност до реда на множителите, т.е $n = p_1^{\alpha_1}.p_2^{\alpha_2}.....p_s^{\alpha_s}$, където $p_1, p_2, ..., p_s$ са различни прости числа, а $\alpha_1, \alpha_2, ..., \alpha_s$ са естествени числа (т.нар. канонично разлагане на $n$).

Мултипликативната индукция е лесно достъпна и бързо усвоима, поради сходството с често употребяваната пълна математическа индукция.

В настоящата работа ще докажем една теорема на Ойлер чрез мултипликативна индукция. Това доказателство за разлика от другите не изисква обстойно познаване на съвременната аритметика и предполага само знания от делимост на числата и числови сравнения.

2. Едно свойство на класовете от числа по модул $\mathbf{m}$. Нека $\mathbf{m}$ е естествено число по– голямо от 1.

Определение 1. Множеството от едно цяло число и всички сравними с него цели числа по модул $\mathbf{m}$ се нарича клас от числа по модул $\mathbf{m}$. С други думи, клас от числа по модул $\mathbf{m}$ се нарича множеството от всички цели числа, които дават един и същ отстатък при деление на $\mathbf{m}$.

Определение 2. Представител на даден клас от числа по модул $\mathbf{m}$ се нарича произволно взето число от същия клас от числа по модул $\mathbf{m}$.

Класовете от числа по модул $\mathbf{m}$ са $\mathbf{m}$ на брой (тъй като съществуват точно $\mathbf{m}$ на брой несравними по модул $\mathbf{m}$ числа и всяко друго цяло число е сравнимо по модул $\mathbf{m}$ с едно от тези числа– такива например са числата $\mathbf{0,1,2,.....,m-1}$). Избирайки по един представител от възможните $\mathbf{m}$ на брой класове от числа по модул $\mathbf{m}$, ще получим една система представители на тези класове от числа по модул $\mathbf{m}$. Такава система представители на класовете от числа по модул $\mathbf{m}$ образуват числата $\mathbf{0,1,2,.....,m-1}$.

Но ако две числа $a$ и $b$ са сравними помежду си по модул $\mathbf{m}$, то най– големият общ делител на $a$ и $\mathbf{m}$ съвпада с най– големият общ делите на $b$ и $\mathbf{m}$, т.е ако $a \equiv b(\mathrm{mod}m)$, то $(a,m)=(b,m)$ (имаме $a \equiv b(\mathrm{mod}m) \Leftrightarrow m/(a-b) \Leftrightarrow a-b=m.q \Rightarrow$ всеки общ делител на $a$ и $\mathbf{m}$ дели $b$ и в такъв случай е общ делител на $b$ и $\mathbf{m}$ и всеки общ делител на $b$ и $\mathbf{m}$ дели $a$ и в такъв случай е общ делител на $a$ и $\mathbf{m} \Rightarrow (a,m)=(b,m)$).

Съгласно това свойство на сравнимите по модул $\mathbf{m}$ числа и определение 1, следва извода: Всички числа от даден клас по модул $\mathbf{m}$ имат еднакъв най– голям общ делител с $\mathbf{m}$.

3. Една теорема на Ферма. След горните пояснения може да се формулира и докаже следната Теорема на Ферма. Ако простото число $p$ не дели цялото

число $a$, то вярно е сравнението $a^{p-1} \equiv 1(\mathrm{mod}\, p)$,т.е ако $p$ е просто, $a \in Z$ и $p$ не дели $a$, то $a^{p-1} \equiv 1(\mathrm{mod}\, p)$. (Формулировка 1)

Теоремата на Ферма се изказва често и така:

За всяко просто число $p$ и за произволно цяло число $a$ е вярно сравнението $a^p \equiv a(\mathrm{mod}\, p)$,т.е $a^p \equiv a(\mathrm{mod}\, p)$ за $\forall a \in Z$ и $p$- просто число. (Формулировка 2)

Действително, ако $p$ е просто число, $a \in Z$ и $p$ не дели $a$, то $a^{p-1} \equiv 1(\mathrm{mod}\, p)$, съгласно формулировка 1. Освен това очевидно $a \equiv a(\mathrm{mod}\, p)$. Умножаваме почленно тези две сравнения и получаваме $a^p \equiv a(\mathrm{mod}\, p)$.

Ако $p$ е просто число, $a \in Z$ и $p/a$, то $p/(a^p - a) \Leftrightarrow a^p \equiv a(\mathrm{mod}\, p)$.

Подходящо доказателство на теоремата на Ферма (Формулировка 2) е следното:

Първо ще докажем чрез пълна индукция верността на теоремата за всяко $a \in N$ ( $N$ е множеството на естествените числа).

Теоремата е вярна за числото $a = 1$.

Да допуснем, че теоремата е вярна за естественото число $a > 1$, т.е $a^p \equiv a(\mathrm{mod}\, p)$.

Съгласно формулата за развитие на Нютонов бином имаме

(1) $(a+1)^p = \binom{p}{0}.a^p + \binom{p}{1}.a^{p-1} + \binom{p}{2}.a^{p-2} + ..... + \binom{p}{p-1}.a + \binom{p}{p}.1$, където

$\binom{p}{0} = \binom{p}{p} = 1$ и $\binom{p}{k} = \frac{p.(p-1).(p-2).....(p-k+1)}{1.2.....k} \in Z$,

за $k = 1, 2, ....., p-1$. Но $1.2.....k.\binom{p}{k} = p.(p-1).(p-2).....(p-k+1)$. Очевидно $p / p.(p-1).(p-2).....(p-k+1)$. Тогава $p / 1.2.....k.\binom{p}{k}$, но $p$ не дели $1.2.....k$, (защото $k < p$), следователно $p / \binom{p}{k}$.

Съгласно (1) и направения извод получаваме, че е вярно

(2) $(a+1)^p \equiv (a^p + 1)(\mathrm{mod}\, p)$. По допускане имаме, че (3) $a^p \equiv a(\mathrm{mod}\, p)$.

Събираме почленно (2) и (3) и получаваме $(a+1)^p \equiv (a+1)(\mathrm{mod}\, p)$, т. е теоремата е вярна за следващото естествено число $a+1$- с това е доказана верността на теоремата за всяко естествено число $a$. За $a=0$ теоремата е също вярна.

Ще покажем верността ù за цели отрицателни числа.

Нека простото число $p=2$. Да проверим вярно ли е, че $(-a)^2 \equiv -a(\mathrm{mod}\, 2)$, т.е 2 дели ли сбора $a^2+a=a(a+1)$. От две последователни цели числа едното винаги е четно, затова $2/a(a+1)$.

Нека простото число $p \neq 2$ (т. е $p$ е нечетно число). Да проверим вярно ли е, че $(-a)^p \equiv -a(\mathrm{mod}\, p)$. Имаме $(-a)^p = -a^p = -(a^p) \equiv -(a)(\mathrm{mod}\, p)$, тъй като теоремата е вярна за $a>0$ и следователно $(-a)^p \equiv -a(\mathrm{mod}\, p)$.

С това теоремата е доказана за $\forall a \in Z$.

4.Числова функция на Ойлер и някои нейни свойства. Нека с $\varphi(m)$ означим броя на всички естествени числа, които не надминават $m$ и са взаимно прости с $m$. Приемаме, че $\varphi(1)=1$ и по този начин функцията $\varphi(m)$ е дефинирана за всяко естествено число $m$. Тази функция е т. нар. числова функция на Ойлер или индикатор на естественото число $m$. Обикновено се отделя внимание на пресмятане на индикатора на естественото число $m$ при степен на просто число. Вярно е следното

Твърдение1. Ако естественото число $m=p^\lambda$, където $\lambda \in N$, $p$ - просто число, то $\varphi(p^\lambda) = p^\lambda - p^{\lambda-1}$.

Доказателство. Да запишем естествените числа от 1 до $p^\lambda$ в редицата

(4) $1,2,3,....,p,....,2p,....,3p,....,(p-1).p,....,p^2,....,p^3,....,p^{\lambda-1},....,p^{\lambda-1}.p=p^\lambda$. Да пресметнем броя на естествените числа от редицата (4), които не са взаимно прости с $p^\lambda$. Такива са числата $p,2p,3p,....,p^2,....,p^{\lambda-1}.p$ - този брой е $p^{\lambda-1}$. Тогава $\varphi(p^\lambda) = p^\lambda - p^{\lambda-1}$, което е броят на естествените числа по– малки от $p^\lambda$ и взаимно прости с $p^\lambda$.

Следствие: Ако естественото число $m=p$, където $p$ е просто число, то $\varphi(p) = p-1$. Получава се от горното твърдение при $\lambda=1$.

Твърдение 2. Ако $a$ и $b$ са взаимно прости естествени числа, вярно е равенството $\varphi(a.b)=\varphi(a).\varphi(b)$, т.е ако $a,b\in N$ и $(a,b)=1$, то $\varphi(a.b)=\varphi(a).\varphi(b)$ (т.нар. мултипликативно свойство на числовата функция на Ойлер)

Доказателство. Да запишем естествените числа от 1 до $a.b$ в стълбове и редове по следния начин:

$$
\begin{array}{ccccccc}
 & 1, & 2, & ..., & k, & ..., & a; \\
 & a+1, & a+2, & ..., & a+k, & ..., & 2.a; \\
(5) & 2.a+1, & 2.a+2, & ..., & 2.a+k, & ..., & 3.a; \\
 & ... & ... & ... & ... & ... & (b-1).a; \\
 & (b-1).a+1, & (b-1).a+2, & ..., & (b-1).a+k, & ..., & (b-1).a+a=b.a.
\end{array}
$$

Едно число е взаимно просто с произведението $a.b$ тогава и само тогава, когато то е поотделно взаимно просто с $a$ и с $b$. За да пресметнем $\varphi(a.b)$, ще пресметнем числата от (5), взаимно прости както с $a$, така и с $b$. Числата на произволен стълб принадлежат на един и същи клас по модул $a$, затова те имат с $a$ еднакъв най– голям общ делител, в частност, ако поне едно от тях е взаимно просто с $a$, то и останалите числа от стълба са взаимно прости с $a$. В първия ред от числа има $\varphi(a)$ на брой естествени числа, по– малки от $a$ и взаимно прости с $a$. Следователно има $\varphi(a)$ на брой стълба от взаимно прости с $a$ числа. Всеки стълб е една система представители на класовете от числа по модул $b$, защото се състои от $b$ на брой несравними по модул $b$ числа (ако допуснем, че съществуват сравними по модул $b$ числа от стълба, ще стигнем до противоречие). В последния стълб имаме $\varphi(b)$ на брой естествени числа, взаимно прости с $b$, тъй като по условие $(b,a)=1$.и тогава $(b,i.a)=(b,i)\ (i=1,2,.....,b)$. Във всеки стълб има също $\varphi(b)$ на брой естествени числа взаимно прости с $b$, тъй като на произволно число от последния стълб можем да съпоставим числото– представител на същия клас по модул $b$ от кой да е друг стълб, а числата от един и същи клас по модул $b$ имат с $b$ еднакъв най– голям общ делител. Следователно, има $\varphi(a)$ на брой стълбове от взаимно прости с $a$ числа и във всеки от тях има по $\varphi(b)$ на брой числа взаимно прости с $b$ или $\varphi(a).\varphi(b)$ е броят на взаимно простите числа с $a.b$ от (5). Ето защо $\varphi(a.b)=\varphi(a).\varphi(b)$.

Теорема на Ойлер. Ако $a$ е цяло число, взаимно просто с естественото число $n$, то вярно е сравнението $a^{\varphi(n)} \equiv 1(\mathrm{mod} n)$, т.е $a \in Z$, $n \in N$ и $(a,n)=1$, то $a^{\varphi(n)} \equiv 1(\mathrm{mod} n)$.

Доказателство. Формулираме хипотезата.

Всяко естествено число $n$ взаимно просто с цялото число $a$ притежава свойството $a^{\varphi(n)} \equiv 1(\mathrm{mod} n)$.

За доказателството ù ще използваме мултипликативната индукция. Имаме:

1. Всички прости числа $p$ взаимно прости с цялото число $a$ притежават свойството $a^{\varphi(p)} \equiv 1(\mathrm{mod}\, p)$, защото $\varphi(p) = p-1$ (следствие) и $a^{p-1} \equiv 1(\mathrm{mod}\, p)$, съгласно теоремата на Ферма (тъй като условието $(p,a)=1$ е еквивалентно на условието $p$ не дели $a$);

2. Приемаме, че естественото число $m$ взаимно просто с цялото число $a$ притежава свойството $a^{\varphi(m)} \equiv 1(\mathrm{mod} m)$;

3. Ще докажем, че естественото число $m.p$, което е взаимно просто с цялото число $a$ (тъй като $m$ е взаимно просто с $a$; $p$ е взаимно просто с $a$) притежава свойството $a^{\varphi(m.p)} \equiv 1(\mathrm{mod} m.p)$, когато $p$ е произволно просто число.

Първи случай: $(m,p)=1$, т. е $p$ не дели $m$. Тогава $\varphi(m.p) = \varphi(m).\varphi(p)$, според твърдение 2. Следователно $a^{\varphi(m.p)} = a^{\varphi(m).\varphi(p)} = (a^{\varphi(m)})^{\varphi(p)} \equiv 1^{\varphi(p)} \equiv 1(\mathrm{mod} m)$ съгласно 2. Но според 1 $a^{\varphi(m.p)} = a^{\varphi(m).\varphi(p)} = (a^{\varphi(p)})^{\varphi(m)} \equiv 1^{\varphi(m)} \equiv 1(\mathrm{mod}\, p)$. От $a^{\varphi(m.p)} \equiv 1(\mathrm{mod} m)$, $a^{\varphi(m.p)} \equiv 1(\mathrm{mod}\, p)$ и $(m,p)=1$ следва $a^{\varphi(m.p)} \equiv 1(\mathrm{mod} m.p)$ (съгласно едно основно свойство на числовите сравнения).

Втори случай: $(m,p) \neq 1 \Leftrightarrow p/m$. Понеже $p/m$, то $m = p^{\lambda}.m_1$, където $p$ не дели $m_1$ и $\lambda \geq 1$. Следователно $\varphi(p.m) = \varphi(p^{\lambda+1}.m_1) = \varphi(p^{\lambda+1}).\varphi(m_1) = (p^{\lambda+1} - p^{\lambda}).\varphi(m_1)$
$= p.(p^{\lambda} - p^{\lambda-1}).\varphi(m_1) = p.\varphi(p^{\lambda}).\varphi(m_1) = p.\varphi(m)$.

Тогава $a^{\varphi(m.p)} - 1 = a^{p.\varphi(m)} - 1 = a^{p.\varphi(m)} - a^{\varphi(m)} + a^{\varphi(m)} - 1 =$

$$= a^{\varphi(m)}.(a^{(p-1).\varphi(m)} - 1) + (a^{\varphi(m)} - 1) = a^{\varphi(m)}.\left[(a^{\varphi(m)})^{p-1} - 1^{p-1}\right] + (a^{\varphi(m)} - 1) =$$

$$= a^{\varphi(m)}.(a^{\varphi(m)} - 1).\left[(a^{\varphi(m)})^{p-2} + (a^{\varphi(m)})^{p-3} + \ldots + a^{\varphi(m)} + 1\right] + (a^{\varphi(m)} - 1) =$$

$$= \underbrace{(a^{\varphi(m)} - 1)}_{\text{Означено с } A}.\underbrace{\{a^{\varphi(m)}.[(a^{\varphi(m)})^{p-2} + (a^{\varphi(m)})^{p-3} + \ldots + a^{\varphi(m)} + 1] + 1\}}_{\text{Означено с } B} = A.B.$$

По–нататък имаме $A \equiv 0(\mathrm{mod} m)$ (съгласно 2) $\Leftrightarrow m/A$.

От $a^{\varphi(m)} \equiv 1(\mathrm{mod} m)$ и $p/m \Rightarrow a^{\varphi(m)} \equiv 1(\mathrm{mod}\, p) \Rightarrow$

$$B \equiv 1.(\underbrace{1+1+...+1}_{p-1 единици})+1 = 1.(p-1)+1 = p \equiv 0(\mathrm{mod}\, p) \Leftrightarrow p/B$$

От $m/A$ и $p/B \Rightarrow m.p/A.B \Leftrightarrow A.B \equiv 0(\mathrm{mod} m.p) \Leftrightarrow a^{\varphi(m.p)} \equiv 1(\mathrm{mod} m.p)$.

И в двата възможни случая доказахме, че $a^{\varphi(m.p)} \equiv 1(\mathrm{mod} m.p)$. С това теоремата на Ойлер е доказана.

Доказването на теоремата на Ферма и теоремата на Ойлер с прости средства е необходимо и полезно, защото те са основни теореми в аритметиката и чрез тях се решават много теоретични и практични задачи.

**Литература:**


1. Т. Нагел, Увод в теорията на числата, С. (1971), стр. 13.
2. В. Серпински, Какво знаем и какво не знаем за простите числа, С. (1967), стр. 30 – 31.
3. М. Гаврилов, Д. Димитров, И. Димовски, Съвременна аритметика, С. (1975), стр. 56 – 60.