Елементи от теория на числата

Сайт: learn.fmi.uni-sofia.bg
Курс: Алгебра 2, поток 1, летен семестър 2021/2022
Книга: Елементи от теория на числата
Разпечатано от: Мартин Попов
Дата: Thursday, 24 March 2022, 21:28

Съдържание

1. Естествени и цели числа

„Бог е създал целите числа, всичко останало е дело на човека" - Леополд Кронекер

Цялостното изграждане на модерната алгебрата стартира и се развива като използва и обобщава свойствата на числата - целите числа, рационалните, реалните и комплексните. Всички тези числови множества са различни разширения на естствените числа, както и техните свойства се основават на свойствата на естествените числа.

1.1. аксиоми на Пеано

Множеството на естествените числа обикновено се бележи с $\mathbb{N}$ в математиката. При опитите да се определи това множество и да се опишат неговите свойства, да се изясни от какво зависи спецификата на естествените числа или да се построи модел на това основно числово множество става ясно, че в неговата основа стои факта, че чрез естествените числа се брои - като се започне от първото (числото 1) след всяко естествено число има точно определено следващо число, и след това има и следващо на следващото и т.н. като по този начин може да се достигне до всяко естествено число.

Тези основополагащи свойства на целите числа са намерили отражение в **аксиомите на Пеано**, италиански математик, който описва естествените числа $\mathbb{N}$, като такова непразно множество, което еднозначно и точно се описва със свойството че за всяко число има следващо го, което означава че съществува функция $\sigma : \mathbb{N} \Rightarrow \mathbb{N}$ (със $\sigma(x)$ ще бележим следващото след x) $\sigma(a) \in \mathbb{N}, \forall a \in \mathbb{N}$;

1. $1 \neq \sigma(x), \forall\, x \in \mathbb{N}$ и по този начин се описва, че съществува първоначално естествено число;
2. *метод на математическата индукция* - Ако за подмножеството $M \subseteq \mathbb{N}$, са изпълнени условията
   - $1 \in M$
   - ако $a \in M$, следователно $\sigma(a) \in M$

   тогава това подмножество съвпада с цялото множество на естествените числа $M = \mathbb{N}\}$

Забележка: *В някои области на науката и приложенията (например логиката и компютърните науки) за по-удобно се приема, че естествените числа започват от нулата* 0. *Но в алгебрата се възприема по-класическия подход и да се счита, че естествените числа започват от единицата* 1.

Стартирайки от тази дефиниция може да се въведе събиране и умножение на естествените числа, като се използва че

$$a + 1 = \sigma(a), \quad a + \sigma(b) = \sigma(a + b)$$

И се установява, че $a + b = \underbrace{\sigma(\ldots(\sigma}_{b}(a)))$.

Умножението се дефинира, чрез събирането, като е изпълнено

$$a.1 = a, \;\; a.\,(b+1) = a.\,b + a \;\; \Rightarrow \;\; a.\,b = \underbrace{a + \ldots + a}_{b}.$$

1.2. цели числа

Въвежда се и числото нула (0), което е неутрално относно събирането и е изпълнено

$$a + 0 = a, \quad \text{за произволно число } a, \quad a.0 = 0$$

Отрицателните цели числа са такива, че за всяко естествено число има отрицателно цяло число, чиято сума е равна на нула.

$$\mathbb{N}^- = \{-a | a \in \mathbb{N}\}, \quad \text{където } -a + a = a + (-a) = 0 \Rightarrow -(-a) = a.$$

Множеството на целите числа се състои от естествените числа, разглеждани заедно с нулата както и заедно с отрицателните цели числа

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \mathbb{N}^-$$

Действията събиране и умножение се продължават до действия в множеството на целите числа.

1.3. свойства на целите числа

Твърдение:

Основните свойства на събирането и умножението на цели числа са следните:

1. $a+b=b+a, \ \ \forall a,b \in \mathbb{Z}$ - комутативност на събирането;
2. $a+(b+c)=(a+b)+c, \ \ \forall a,b,c \in \mathbb{Z}$ - асоциативност на събирането;
3. $a+0=a, \ \ \forall a \in \mathbb{Z}$ - нулата е неутрален елемент относно събирането;
4. $a+(-a)=0, \forall a \in \mathbb{Z}$;
5. $a.\,b=b.\,a, \ \ \forall a,b \in \mathbb{Z}$ - комутативност на умножението;
6. $a.\,(b.\,c)=(a.\,b).\,c, \ \ \forall a,b,c \in \mathbb{Z}$ - асоциативност на умножението;
7. $a.\,(b+c)=a.\,c+b.\,c, \ \ \forall a,b,c \in \mathbb{Z}$ - дистрибутивност;
8. $1.a=a, \forall a \in \mathbb{Z}$ - единицата е неутрален елемент относно умножението.

Изваждането при целите числа се разглежда като обратно действие на събирането и разликата на числата $a-b$ представлява това число x, което изпълнява уравнението $b+x=a$. Решението е $x=a+(-b)=a-b$ и разликата може да се получи, като към a се прибави противоположното число на b.

1.4. наредба при целите числа

Ще припомним добре известните от училище свойства на "по-малко" и "по-голямо"

Твърдение:

Следните свойства са изпълнени при сравняване "по-малко" ("$<$") на цели числа:

1. Ако е изпълнено $a < b$ и $b < c$, следователно $a < c$;
2. Ако $a < b$, следователно $a + c < b + c$;
3. Ако $a_1 < b_1$ и $a_2 < b_2$, следователно $a_1 + a_2 < b_1 + b_2$;
4. Ако $a < b$ и $c > 0$, следователно $a.c < b.c$;
5. Ако $a < b$ и $c < 0 \Rightarrow \ a.c > b.c$;

Свойствата на "по-голямо" ("$>$") са аналогични на са свойствата на "по-малко" ("$<$"), защото за две различни цели числа $a \neq b \in \mathbb{Z}$ точно едно от $a > b$ или $a < b$ е изпълнено, но за пълнота ще ги посочим в явен вид и тях:

1. Ако $a > b$ и $b > c \ \Rightarrow a > c$;
2. Ако $a > b \Rightarrow a + c > b + c$;
3. Ако $a_1 > b_1$ и $a_2 > b_2 \ \Rightarrow a_1 + a_2 > b_1 + b_2$;
4. Ако $a > b$ и $c > 0$, следователно $a.c > b.c$;
5. Ако $a > b$ и $c < 0 \Rightarrow \ a.c < b.c$;

Едно често използвано свойство, което следва от горните е

- ако $a, b, c \geq 1$, следователно $\quad ab \geq a \quad \text{и} \quad ab \geq b$

За подмножествата $M \subset \mathbb{Z}$ от цели числа, които са ограничени отгоре е изпълнено, че съдържат максимален елемент, т.е.

$$\left.\begin{array}{r} M \subset \mathbb{Z}, \ \text{ такова че} \\ \exists\, t : x < t, \forall x \in M \end{array}\right\} \quad \Rightarrow \quad \exists\, a \in M, \text{за което} \quad x \leq a, \forall x \in M$$
$$(M - \ \text{ограничено отгоре}) \qquad\qquad (a - \ \text{максимален елемент})$$

По аналогичен начин ограничените отдолу множества имат минимален елемент

$$\left.\begin{array}{r} T \subset \mathbb{Z}, \ \text{ такова че} \\ \exists\, u : u < x, \forall x \in T \end{array}\right\} \quad \Rightarrow \quad \exists\, b \in T, \text{за което} \quad b \leq x, \forall x \in T$$
$$(T - \ \text{ограничено отдолу}) \qquad\qquad (b - \ \text{минимален елемент})$$

Въвежда се абсолютна стойност (модул) на цяло число, което е равно на

$$|a| = \begin{cases} a, & \text{когато } \ a \geq 0 \\ -a, & \text{когато } \ a < 0 \end{cases}$$

Ако геометрично се изобразят целите числа върху числовата ос, тогава модула ще представлява разстоянието на точката изобразяваща числото до началото на числовата ос.

2. деление и делимост

Известно е от училище, че разделяйки две цели числа не винаги се получава цяло число.

Ако искаме да получим цяло число, трябва да извършим деление с частно и остатък. Това е много характерно свойство на целите числа, и ще изучим основните му следствия.

2.1. теорема за делене с частно и остатък

Теорема за деление с частно и остатък:
Нека $a, b \in \mathbb{Z}$ са цели числа и $b \neq 0$. Съществуват единствени цели числа $q, r \in \mathbb{Z}$, за които е изпълнено

$$a = b.\,q + r, \quad \text{където} \quad 0 \leq r < |b|.$$

Числото q се нарича частно, а r остнатък при разделяне a на b.

Доказателство:
Съществуване: За да докажем съществуването на частно и остатък ще разгледаме следното множество от цели числа $M = \{a + b.\,t \mid t \in \mathbb{Z}\}$ и подмножеството му, състоящо се от тези числа от M, които са по-големи или равни на нула.

$$M^{(\geq 0)} = \{c = a + bt \in M \mid t \in \mathbb{Z} \text{ и } c \geq 0\}$$

Множеството $M^{(\geq 0)}$ е ограничено отдолу подмножество на целите числа и нека да означим неговия минимален елемент с $r \in M^{(\geq 0)}$, където $r = a + bt_0 \geq 0$.
Ще докажем, че това число r е търсеният остатък.
За целта, допускаме противното, т.е. че минималното число е по-голямо $r \geq |b|$. В такъв случай от него можем да извадим $|b|$ и да получим число $r_1 < r$, което също е от множеството M и отново е неотрицателно

$$r_1 = r - |b| = a + bt_0 \pm b \in M, \quad \text{и } r_1 \geq 0 \ \Rightarrow r_1 \in M^{(\geq 0)}$$

Получихме число от $M^{(\geq 0)}$, което е по-малко от минималното число в това множество, което е в противоречие с избора на числото r като минимално в $M^{(\geq 0)}$. Следователно допускането не е вярно, от където получаваме, че за r е изпълнено $0 \leq r < |b|$. Окончателно получихме, че е изпълнено

$$r = a + bt_0 \ \Rightarrow \ a = b(-t_0) + r, \ \ 0 \leq r < |b|.$$

Единственост: За да докажем единствеността на частното и остатъка, нека да са изпълнени две равенства:

$$\left.\begin{aligned} a &= bq_1 + r_1, \quad \text{ и } \ 0 \leq r_1 < |b| \\ a &= bq_2 + r_2, \quad \text{ и } \ 0 \leq r_2 < |b| \end{aligned}\right\} \ \Rightarrow |r_1 - r_2| < |b|$$

Изваждаме равенствата и получаваме, че е изпълнено

$$0 = b(q_1 - q_2) + (r_1 - r_2) \ \ \Rightarrow |r_1 - r_2| = |b|.\,|q_1 - q_2|$$

Допускаме, че $|q_1 - q_2| \neq 0$, откъдето получаваме, че $|r_1 - r_2|$ като произведение на две естествени числа е по-голямо или равно на всеки един от множителите

$$|r_1 - r_2| = |b.\,(q_1 - q_2)| \geq |b|$$

От една страна имаме, че е изпълнено $|r_1 - r_2| < |b|$, а от друга страна получихме че $|r_1 - r_2| \geq |b|$, което е противоречие и следователно направеното допускане не е вярно.

По този начин виждаме, че $q_1 - q_2 = 0$ и следователно $r_1 - r_2 = 0$. Откъдето се получава, че $q_1 = q_2$ и $r_1 = r_2$ и частното и остатъка при разделяне a на b единствени.

$\square$

2.2. позиционна бройна система

Едно основно следствие на теоремата за деление с частно и остатък е че, естествените числа могат да се записват в позиционни бройни системи по следния начин:

Следствие:
Нека $a, b \in \mathbb{N}$ и $b > 1$. Съществуват единствени числа $a_0, \ldots, a_k$, за които е изпълнено

$$a = a_0 + a_1 b + \ldots + a_k b^k, \text{ където } 0 \leq a_i < b, \forall i \text{ и } a_k \neq 0$$

Когато имаме такова представяне казваме че числото a е представено в позиционна бройна система с основа b и записваме $a = \overline{a_k a_{k-1} \ldots a_0}_{\,(b)}$.

Доказателство:
Търсеното представяне се получава постъпково:

<u>Начална стъпка:</u> Разделяме a на b с частно и остатък $a = b.\, q_0 + a_0$. Остатакът $0 \leq a_0 < b$ е първото от търсената поредица от числа.\begin{itemize}

- Ако полученото частно е равно на нула $q_0 = 0$, това означава че сме получили търсеното представяне на числото и то е $a = \overline{a_0}_{\,(b)}$.
- Ако частното е различно от нула $q_0 > 0$ с представянето $a = b.\, q_0 + a_0$ се преминава към стъпка 1.

<u>Стъпка s:</u> След като сме получили представянето $a = b^s q_{s-1} + b^{s-1} a_{s-1} + \ldots + b^0 a_0$, разделяме q_{s-1} на b с частно и остатък $q_{s-1} = b.\, q_s + a_s$. Остатъкът a_s, където $0 \leq a_s < b$, е следващото число, което участва в представянето на a. По този начин се получава

$$a = b^s \underbrace{(b.\, q_s + a_s)}_{=q_{s-1}} + b^{s-1} a_{s-1} + \ldots + b^0 a_0 = b^{s+1} q_s + b^s a_s + b^{s-1} a_{s-1} + \ldots + b^0 a_0$$

Ясно е, че новополученото частно е по-малко от частното получено но предишната стъпка $0 \leq q_s < q_{s-1}$.

- Ако полученото частно е равно на нула $q_s = 0$, това означава че остатакът е ненулев $a_s \neq 0$ и сме получили търсеното представяне и то е $a = \overline{a_s a_{s-1} \ldots a_0}_{\,(b)}$.
- Ако частното е различно от нула $q_s > 0$, тогава се преминава към стъпка с номер $s + 1$.

На всяка стъпка е изпълнено $0 \leq q_s < q_{s-1}$ и следователно след краен брой стъпки ще се получи нулево частно и ако това е на стъпка с номер k, тогава ще се получи окончателното представяне на числото a в търсения вид

$$a = b^k a_k + b^{k-1} a_{k-a} + \ldots + b a_1 + a_0 = \overline{a_k a_{k-1} \ldots a_0}_{\,(b)}$$

$\square$

<u>Пример:</u>

Да представим числото 2657 в осмична бройна система (с основа $b = 8$). За целта извършваме последователни деления на 8 и получаваме последователните цифри в записа на числото (но са подредени отзад напред):

- $2657 = 332.8 + 1$, получаваме че $a_0 = 1$;
- $332 = 41.8 + 4$, получаваме че $a_1 = 4$;
- $41 = 5.8 + 1$, получаваме че $a_2 = 1$;
- $5 = 0.8 + 5$, получаваме че $a_3 = 5$ и понеже полученото частно е равно на 0, следва че сме завършили

Окончателно се получава:

$$2657 = 5.8^3 + 1.8^2 + 4.8 + 1 = \overline{5141}_{(8)}$$

Ако искаме да получим представянето на същото число но с основа $b = 7$ извършваме последователност от деления с частно и остатък на 7:

- $2657 = 379.7 + 4 \ \Rightarrow \ r_0 = 4;$
- $379 = 54.7 + 1 \ \Rightarrow \ r_1 = 1;$
- $54 = 7.7 + 5 \ \Rightarrow \ r_2 = 5;$
- $7 = 1.7 + 0 \ \Rightarrow \ r_3 = 0;$
- $1 = 0.7 + 1 \ \Rightarrow \ r_4 = 1;$

Получава се
$2657 = \overline{10514}_{(7)} = 1.7^4 + 5.7^2 + 1.7 + 4.$

2.3. делимост, св-ва

Определение:
Нека a, b са цели числа и $b \neq 0$. Казваме, че b дели a, когато съществува цяло число $q \in \mathbb{Z}$, такова че $a = bq$. Когато b дели , накратко записваме $b \mid a$.

Виждаме, че числото b дели a точно когато се получи остатък нула когато разделим a на b с частно и остатък.

<u>*Забележка:*</u> *Ако числото b не дели числото a, това ще го отбелязваме по следния начин $b \nmid a$}*

Твърдение:
Основните свойства на делимостта са следните, където $a, b, c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$ и $c \neq 0$.

1. $\pm 1 \mid a, \ \forall a \in \mathbb{Z};$
2. $b \mid 0, \ \forall b \in \mathbb{Z};$
3. $\text{ако } \ b \mid a \ \Rightarrow -b \mid a;$
4. $\text{ако } \ b \mid a \text{ и } a \mid c \ \Rightarrow b \mid c;$
5. $\text{ако } \ b \mid a \text{ и } a \mid b \ \Rightarrow a = \pm b;$
6. $b \mid a \ \Rightarrow \ b \mid (a + kb), \ k \in \mathbb{Z}$
7. $\text{ако } \ b \mid a \ \Rightarrow \ b \mid ka,$ където $k \in \mathbb{Z};$}
8. $\text{ако } \ b \mid a_1 \ \text{ и } b \mid a_2 \ \Rightarrow \ b \mid (k_1 a_1 + k_2 a_2),$ където $k_1, k_2 \in \mathbb{Z};$
9. $\text{ако } \ b \mid a \text{ и } a \neq 0 \ \Rightarrow |b| \leq |a|;$

Доказателство:

Доказателствата на тези свойства използват директно определението.

<u>*Доказателство на свойство 4:*</u> Ако $b \mid a \ \Rightarrow \exists q \in \mathbb{Z} : \ a = bq$ и от $a \mid c \ \Rightarrow c = a.\, u \ (u \in \mathbb{Z})$. По този начин получаваме, че $c = a.\, u = bqu$ и следователно е изпълнено $b \mid c$.

<u>*Доказателство на свойство 5:*</u> Ако $b \mid a \ \Rightarrow \exists q \in \mathbb{Z} : \ a = bq$ и от $a \mid b \ \Rightarrow b = a.\, u \ (u \in \mathbb{Z})$. По този начин получаваме, че $b = a.\, u = bqu$ и следователно е изпълнено $qu = 1,$ откъдето се получава че $q = \pm 1$ и $a = \pm b$.

<u>*Доказателство на свойство 8:*</u> Ако $b \mid a_1 \ \text{ и } b \mid a_2 \ \Rightarrow$

$$\left.\begin{aligned} a_1 &= q_1 b \\ a_2 &= q_2 b \end{aligned}\right\} \Rightarrow k_1 a_1 + k_2 a_2 = (q_1 a_1 + q_2 a_2) b \ \Rightarrow \ b \mid (k_1 a_1 + k_2 a_2).$$

<u>*Доказателство на свойство 9:*</u> Ако $b \mid a \ \Rightarrow \exists q \in \mathbb{Z} : \ a = bq$ и от $a \neq 0 \Rightarrow q \neq 0.$ Изпълнено е, че $|a| = |b|.\, |q|$ и от свойството за умножение на естествени числа, следва $|b| \leq |a|$.

$\square$

2.4. пример

Използването на означението за делимост е удобен начин за описване на решенията на много задачи, свързани с теория на числата.

Пример:

Да се докаже верността на следния признак за делене на седем:

"*Числото n се дели на 7 тогава и само тогава, когато числото t се дели на 7, като t се получава по следния начин - от числото n премахнем последната цифра и от полученото извадим премахнатата последна цифра умножена по 2.*"

Последната цифра на числото n (записано в десетична бройна система) е точно остатъкът, който се получава, когато разделим n на 10. Тогава ако $n = 10x + y$, то числото $t = x - 2y$, следователно твърдението е следното

$$7 \mid (10x + y) \Leftrightarrow 7 \mid (x - 2y)$$

Прилагаме свойствата на делимостта и последователно получаваме:

$$\begin{aligned} \text{Ако } 7 \mid (10x+y) \quad &\Rightarrow \quad 7 \mid (3x+y) \Rightarrow \\ &\Rightarrow \quad 7 \mid 5(3x+y) \text{ т.е. } 7 \mid (x + 14x + 7y - 2y) \Rightarrow \\ &\Rightarrow \quad 7 \mid (x - 2y) \end{aligned}$$

Аналогично може да се получи:

$$\begin{aligned} \text{Ако } 7 \mid (x-2y) \quad &\Rightarrow \quad 7 \mid 3(x-2y) \Rightarrow \\ &\Rightarrow \quad 7 \mid (3x - 6y + 7(x+y)) \Rightarrow \\ &\Rightarrow \quad 7 \mid (10x + y) \end{aligned}$$

Чрез няколко пъти прилагане на този признак за делене на 7 можем да установим без деление, дали 5348 се дели на 7:

- от $n = 5348 = 10.534 + 8$, намираме $t = 534 - 2.8 = 518$ и следователно $7 \mid 5348 \Leftrightarrow 7 \mid 518$
- от $n_1 = t = 518 = 10.51 + 8$, намираме $t_1 = 51 - 16 = 35$ и следователно $7 \mid 518$, защото $7 \mid 35$.

По този начин се получи, че $7 \mid 5348$.

3. НОД

Определение:

Нека са дадени две цели числа $a, b \in \mathbb{Z}$ и поне едно от двете е различно от нула. Най-голямото естествено число d, което дели едновременно и двете числа $(d|a$ и $d|b)$ се нарича техен **най-голям общ делител** и се отбелязва по следния начин $d = (a, b)$.

Непосредствено от определението се получава, че са изпълнени следните свойства.

Свойства:

1. $(a, 0) = a$ за произволно $a \in \mathbb{N}$.
2. $(a, b) = (\pm a, \pm b)$.

3.1. Тъждество на Безу

Теорема (Безу)
Нека $a, b \in \mathbb{Z}$ са цели числа, като поне едно от тях е ненулево и $d = (a, b)$ е техният най-голям общ делител. Тогава съществуват цели числа $u, v \in \mathbb{Z}$, за които е изпълнено

$$d = (a, b) = au + bv \quad \text{(\textit{Тъждество на Безу})}$$

Доказателство: Разглеждаме множеството

$$M = \{xa + yb \mid x, y \in \mathbb{Z}\}$$

Ясно е, че това множество има както положителни, така и отрицателни числа.

Нека да изберем $d \in M$ да бъде минималното положително число от това множество. Тогава е изпълнено, че

$$d = au + bv, \;\; d > 0, \;\; d \leq t, \; \forall t \in M \cap \mathbb{N}$$

Ще докажем, че така избраното число d дели всяко число от множеството M. Нека $t = ax + by \in M$ е произволно число от разглежданото множество. Разделяма t на d с частно q и остатък r и получаваме

$$\begin{array}{rcl} t & = & dq + r, \;\; \text{където} \;\; 0 \leq r < d \\ & \Downarrow & \\ r & = & t - dq = ax + by - (au + bv)q = a(x - uq) + b(y - vq) \;\in\; M \end{array}$$

Виждаме, че остатъкът $r \in M$ е елемент от същото множество, и $d > r \geq 0$ е минималното естествено число от M, следователно $r = 0,$ откъдето следва че $d|t$.

Изходните числа $a, b \in M$ са от множеството защото $a = a.1 + b.0$ и $b = a.0 + b.1$ и следователно е изпълнено, че $d|a$ и $d|b$.

Нека да разгледаме произволен общ делител на дадените числа. Тогава е изпълнено

$$\left.\begin{array}{l} d_1|a \\ d_1|b \end{array}\right\} \Rightarrow d_1|\underbrace{(au + bv)}_{=d}, \text{ т.е. } d_1|d \;\Rightarrow\; d_1 \leq d$$

$\square$

При доказателството на теоремата доказахме следното свойство, което отличава най-големия общ делител от всички други общи делители.
Свойство:
Ако $d = (a, b)$ е най-големият общ делител на числата a и b, тогава d се дели на всеки общ делител на тези числа.

Забележка: *Числата от тъждеството на Безу не са единствени. Нека е изпълнено, че* $d = (a, b) = au + bv,$ *, тогава за произволно цяло число* k *също е изпълнено и*

$$d = au + bv = au + abk + bv - abk = a(u + bk) + b(v - ak)$$

3.2. Алгоритъм на Евклид

Когато на практика се търсим най-големия общ делител на две числа използваме алгоритъма на Евклид. В основата на този алгоритъм е следващото свойство на най-големия общ делител.

Свойство:
Нека a, b са ненулеви цели числа и $a = bq + r,$ където r е остатъкът от деленето $0 \leq r < b.$ Тогава най-големия общ делител на a, b е равен на най-големият общ делител на b, r, т.е.

$$\text{Ако } \; a = bq + r \; \Rightarrow (a, b) = (b, r).$$

Доказателство:
Нека $d = (a, b)$ и $d_1 = (b, r)$, и като се използва предишното свойство се получава

$$\left.\begin{array}{l} d \mid b \\ d \mid a \end{array}\right\} \Rightarrow d \mid \underbrace{(a - bq)}_{=r} \Rightarrow \left|\begin{array}{l} d \mid b \\ d \mid r \end{array}\right\} \Rightarrow d \mid d_1$$

Но от друга страна е изпълнено, че

$$\left.\begin{array}{l} d_1 \mid b \\ d_1 \mid r \end{array}\right\} \Rightarrow d_1 \mid \underbrace{(bq + r)}_{=a} \Rightarrow \left|\begin{array}{l} d_1 \mid b \\ d_1 \mid a \end{array}\right\} \Rightarrow d_1 \mid d$$

Получихме, че за естествените числа d, d_1 е изпълнено, че $d \mid d_1$ и $d_1 \mid d$, откъдето се получава $(a, b) = d = d_1 = (b, r_1).$

$\square$

Приложеният алгоритъм на Евклид е алгоритъм за намиране на най-голям общ делител, а ако се използват и всички междинно получени числа може да се намери и тъждеството на Безу.

Алгоритъм (Евклид)
При зададени a, b ненулеви цели числа се намира техния най-голям общ делител.

- Стъпка 1: Разделят се числата с частно и остатък

$$a = bq_1 + r_1, \quad \text{където } 0 \leq r_1 < b, \quad \text{и } \; (a, b) = (b, r_1)$$

  - ако $r_1 = 0$ следователно е намерен най-големият общ делител $b = (a, b)$ (край).
  - ако $r_1 \neq 0$,преминаваме към следващата стъпка.
- Стъпка 2: Разделят се b на r_1 с частно и остатък

$$b = r_1 q_2 + r_2, \quad \text{където } 0 \leq r_2 < r_1, \quad \text{и } \; (b, r_1) = (r_1, r_2)$$

  - ако $r_2 = 0$ следователно е намерен най-големият общ делител $r_1 = (a, b)$ (край).}
  - ако $r_2 \neq 0$,преминаваме към следващата стъпка.
- $\ldots\ldots\ldots$
- Стъпка $k + 1$: Разделят се r_{k-1} на r_k с частно и остатък

$$r_{k-1} = r_k q_{k+1} + r_{k+1}, \quad \text{където } 0 \leq r_{k+1} < r_k, \quad \text{и } \; (rk - 1, r_k) = (r_k, r_{k+1})$$

  - ако $r_{k+1} = 0$ следователно е намерен най-големият общ делител - последният ненулев остатък $r_k = (a, b)$ (край).
  - ако $r_{k+1} \neq 0$, преминаваме към следващата стъпка.
- $\ldots\ldots\ldots$

Така описания алгоритъм е краен, защото на всяка стъпка получаваме все по-малък остатък и остатъците са неотрицателни числа и $b > r_1 > r_2 > \ldots > r_k > r_{k+1} \ldots \geq 0.$

Използвайки преди това доказаното свойство, ако r_k е последният ненулев остатък ($r_{k+1} = 0$), тогава е изпълнено

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_k - 1, r_k) = (r_k, r_{k+1}) = (r_k, 0) = r_k.$$

3.3. Пример

<u>Пример:</u>

Да се пресметне най-големият общ делител на числата $a = 7293$ и $b = 3147$ и да се намери тъждеството на Безу за тях.

Прилагаме алгоритъма на Евклид, а после се връщаме в обратния ред по получените равенства, за да получим тъждеството на Безу

$$
\begin{array}{rcl}
7293 & = & 2.3147+999 & \Rightarrow & 3{=}20.3147-63.(7293-2.3147) = -63.a + 146.b \\
3147 & = & 3.999+150 & \Rightarrow & 3{=}-3.999{+}20(3147{-}3.999){=}20.3147{-}63.999 \Uparrow \\
999 & = & 6.150+99 & \Rightarrow & 3{=}2.150{-}3.(999{-}6.150){=}-3.999{+}20.150 \Uparrow \\
150 & = & 1.99+51 & \Rightarrow & 3{=}2(150{-}99){-}99{=}2.150{-}3.99 \Uparrow \\
99 & = & 1.51+48 & \Rightarrow & 3{=}51{-}(99{-}51){=}2.51{-}99 \Uparrow \\
51 & = & 1.48+3 & \Rightarrow & 3 = 51-48 \Uparrow \\
48 & = & 16.3+0 & \Rightarrow & \boxed{3 = (7293, 3147)}
\end{array}
$$

3.4. Взаимно прости числа

Определение:
Ненулевите цели числа a, b се наричат **взаимно прости**, ако техният най-голям общ делител е равен на 1. (т.е. $(a, b) = 1$)

Твърдение:
Нека $a, b \in \mathbb{Z}$ са взаимно прости числа $(a, b) = 1$, тогава е изпълнено

- ако $a \mid bc$, следва че $a \mid c$;
- ако $a \mid c$ и $b \mid c$, следва че $ab \mid c$;

Доказателство:
За да докажем тези свойства, прилагаме тъждеството на Безу.

- Изпълнено е, че $(a, b) = 1$, следователно съществуват числа $u, v \in \mathbb{Z}$, за които е изпълнено $1 = au + bv$. Като умножим двете страни на това равенство по c получаваме

$$a|bc \ \Rightarrow \ a|\underbrace{cau + cbv}_{=c} \ \Rightarrow \ a|c$$

- От $a|c$ следва, че $c = aq$. Знаейки, че a, b са взаимно прости числа прилагаме доказаното в т.1 и получаваме

$$\left.\begin{array}{r} b|c \\ c = aq \end{array}\right\} \Rightarrow \ b|aq \xrightarrow[(a,b)=1]{} b|q \Rightarrow \ q = bt \Rightarrow \ c = abt \Rightarrow \ ab|c.$$

$\square$

4. Прости числа

Определение:
Естественото число $p \in \mathbb{N},\ \ p > 1$ се нарича \textbf{просто число}, ако единствените естествени числа, които го делят са 1 и p.

$$p \text{ просто число } \Leftrightarrow \text{ ако от } \left. \begin{array}{|l} x|p \\ x \in \mathbb{N} \end{array} \right\} \rightarrow x = 1 \text{ или } x = p.$$

Числата, които са по-големи от 1 и не са прости се наричат съставни числа.

Свойство:
Всяко естествено число n, което е по-голямо от 1 е или просто или се дели на някакво просто число(различно от n). (т.е. всяко съставно число се дели на поне едно просто число)

Доказателство:
Ако допуснем, че числото n не е просто, следователно n се дели на някое число $t|n$, за което е изпълнено $1 < t < n$. Нека $k > 1$ е минималното число, което дели n изпълнено е, че $1 < k < n$.
Нека $s < k$ е такова че $s|k$, следователно $s|n$ и от минималността на $k > 1$ следва че $s = 1$. Получава се, че k е просто число което дели n.

4.1. решето на Ератостен

Използвайки, че всяко число > 1 е или просто или се дели на някое просто число може да се получи алгоритъм по който могат да се намерят първите няколко прости числа.

Алгоритъм (Решето на Ератостен}

Това е алгоритъм за получаване на простите числа, които са в интервала от 1 до N.

- Записват се числата от 2 до N и започвайки подред за всяко число k се прави следното:
  - ако числото k не е задраскано се отбелязва като просто число и задраскваме всяко $k-$то число след него. След това се преминава към следващото число;
  - ако числото k е задраскано, нищо не се прави и се преминава към следващото число;

В следващия пример е показано как могат да се определят простите числа, по-малки от 50.

	$\boxed{2}$	$\boxed{3}$	$\cancel{4}$	$\boxed{5}$	$\cancel{6}$	$\boxed{7}$	$\cancel{8}$	$\cancel{9}$	$\cancel{10}$
$\boxed{11}$	$\cancel{12}$	$\boxed{13}$	$\cancel{14}$	$\cancel{15}$	$\cancel{16}$	$\boxed{17}$	$\cancel{18}$	$\boxed{19}$	$\cancel{20}$
$\cancel{21}$	$\cancel{22}$	$\boxed{23}$	$\cancel{24}$	$\cancel{25}$	$\cancel{26}$	$\cancel{27}$	$\cancel{28}$	$\boxed{29}$	$\cancel{30}$
$\boxed{31}$	$\cancel{32}$	$\cancel{33}$	$\cancel{34}$	$\cancel{35}$	$\cancel{36}$	$\boxed{37}$	$\cancel{38}$	$\cancel{39}$	$\cancel{40}$
$\boxed{41}$	$\cancel{42}$	$\boxed{43}$	$\cancel{44}$	$\cancel{45}$	$\cancel{46}$	$\boxed{47}$	$\cancel{48}$	$\cancel{49}$	$\cancel{50}$

4.2. свойства

Твърдение: (Евклид)

Простите числа са безброй много.

Доказателство:
Допускаме, че простите числа са краен брой. Нека всички прости числа са $p_1, \ldots, p_k$. Разглеждаме числото $a = 1 + p_1 \ldots . p_1$, което не е просто, защото не е измежду $p_1, \ldots, p_k$. За a е изпълнено, че $p_i \nmid a$ за $i = 1, \ldots, k$, следователно a не се дели на нито едно от всичките прости числа $p_1, \ldots, p_k$, което е противоречие. Получихме, че допускането че простите числа са краен брой е грешно и поради тази причина се получава, че простите числа са безброй много.

$\square$

Следващото свойство е директно следствие от определението за просто число.

Свойство:

Ако p е просто число и a е произволно цяло число, тогава най-големият им общ делител е $(p, a) = \begin{cases} p, & \text{когато } p \mid a \\ 1, & \text{когато } p \nmid a \end{cases}$

Свойство:
Ако p е просто число, което дели произведение на няколко цели числа, тогава p дели поне един от множителите.

$$\text{ако } p\text{-просто число и } \; p \mid a_1 \ldots . a_s \;\Rightarrow\; \exists i : p \mid a_i$$

Доказателство:
Доказва се с индукция по s.

Ако $s = 1$, тогава $p \mid a_1$ и няма какво да се доказва.

Ако допуснем, че твърдението е вярно за s множителя $a_1, \ldots, a_s$, ще докажем че е вярно и за случая от $s + 1$ множителя.

Нека за простото число p е изпълнено $p \mid a_1 \ldots . a_s . a_{s+1}$. Тогава имаме два възможни случая

- ако $p \mid a_{s+1}$, следователно твърдението е изпълнено;
- ако $p \nmid a_{s+1}$, следователно $(p, a_{s+1}) = 1$ и

$$\left.\begin{array}{r} p \mid (a_1 \ldots a_s)a_{s+1} \\ (p, a_{s+1}) = 1 \end{array}\right\} \;\Rightarrow\; p \mid a_1 \ldots a_s.$$

Тогава по индукционно предположение се получава, че p дели някой от множителите $a_1, \ldots, a_s$.

4.3. Основна теорема на аритметиката

Основна Теорема на аритметиката:

Всяко естествено число $n > 1$ може да се представи по "единствен начин" (с точност до пренареждане на множителите) като произведение на прости числа.

Доказателство:
Съществуване: Съществуването на такова представяне се доказва с индукция по n

- *База на индукцията:* $n = 2$ - числото 2 е просто и можем да считаме, че 2 е представено като "произведение" на едно просто число.
- *Индукционно предположение:* Предполагаме, че твърдението е вярно за всички естествени числа $k,$ където $1 < k < n$.
- *Индукционна стъпка:* Ще докажем твърдението за $n.$ Имаме два случая:
  - Ако n е просто число, тогава считаме, че то е представено като "произведение" на един прост множител.
  - Ако n е съставно число, тогава $n = a.\, b,$ където $a < n, \quad b < n$ са естествени числа. Прилагаме индукционното предположение за a и b и получаваме търсеното представяне.

$$\left.\begin{array}{r} a = p_1. \ldots . p_s \\ a = q_1. \ldots . q_t \\ p_i \;\; q_j \; - \; \text{прости} \end{array}\right\} \;\Rightarrow\; n = a.\, b = p_1. \ldots . p_s . \, q_1. \ldots . q_t$$

"Единственост": За да докажем единствеността, нека да разгледаме числото n представено по два начина като произведение на прости числа
$n = p_1. \ldots . p_k$ и $n = q_1. \ldots . q_s$, където p_i и q_j са прости числа.
Тогава е изпълнено

$$p_1. \ldots . p_k = q_1. \ldots . q_s \quad \Rightarrow \quad p_k \mid q_1. \ldots . q_s$$

От доказаното свойство, следва че простото число p_k дели някой измежду множителите $q_1, \ldots, q_s$.
Преномерираме ги, така че да е изпълнено $p_k \mid q_s$. Числото q_s също е просто, откъдето получаваме, че $p_k = q_s$.

$$(p_1 \ldots . p_{k-1}).\, p_k = (q_1 \ldots . q_{s-1}).\, p_k \;\Rightarrow\; p_1 \ldots . p_{k-1} = q_1 \ldots . q_{s-1}$$

Продължава се по същия начин.

Ако допуснем, че $k \neq s$ (например, че $k < s$)след k стъпки ще получим равенство от следния вид $1 = q_1. \ldots . q_{s-k},$ което е невъзможно.

Следователно $s = k$ и след преномериране е изпълнено $p_i = q_i$ за $i = 1, \ldots, k$.

$\square$

5. Функция на Ойлер

Определение:
Нека $n \in \mathbb{N}$ е естествено число. Със $\varphi(n)$ отбелязваме броят на естествените числа, по-малки от n и взаимно прости с n. За определеност приемаме, че $\varphi(1) = 1$. Функцията, която се определя по този начин се нарича **функция на Ойлер**.

$$\varphi : \mathbb{N} \to \mathbb{N}, \text{ където } \varphi(n) = |\{k \in \mathbb{N} \mid k < n, \ (k,n) = 1\}|\,.$$

Непосредствено се вижда, че е изпълнено $\varphi(2) = 1$, $\varphi(3) = 2$ и $\varphi(5) = 4$. По-общо, знаем, че ако p е просто число, тогава p е взаимно просто с всички естествени числа, по-малки от него, и по този начин се получава на колко е равна функцията на Ойлер за прости числа.

Свойство:
Ако p е просто числото, тогава $\varphi(p) = p - 1.$

5.1. ф-я на Ойлер - при степен на просто

Да разгледаме следните примери $\varphi(4) = 2 = |\{1, 3\}|$ и $\varphi(8) = 4 = |\{1, 3, 5, 7\}|$. Взаимно-простите числа с 8 са тези които са нечетни. Аналогична е ситуацията с определянето на $\varphi(9) = 6 = |\{1, 2, 4, 5, 7, 8\}|$, при него е изпълнено че взаимно простите числа с 9 са тези, които не се делят на 3. Обобщавайки това наблюдение, лесно се установява че е изпълнено следното свойство.

Твърдение:
Ако p е просто число, тогава $\varphi(p^k) = p^k - p^{k-1}$, където $k \in \mathbb{N}$.

Доказателство:
Тъй като p е просто число, то е изпълнено че най-големия общ делител на p^k и кое да е друго число е 1 или някаква степен на p,следователно $(p^k, t) = 1 \Leftrightarrow p \nmid t$.

Тогава множеството от по-малките от p^k числа, които са взаимнопрости с p^k еТ

$$M = \{t \in \mathbb{N} \mid t < p^k,\ \ (t, p^k) = 1\} = \{t \in \mathbb{N}\ \mid\ t < p^k,\ p \nmid t\}$$

Това множество може да се получи по следния начин - като измежду всички числа от 1 до p^k премахнем, тези които се делят на p.

$$M = \{1, 2, \dots, p^k\} \setminus \{p, 2p, \dots, p^{k-1}.p\}$$

Окончателно се получи, че $\varphi(p^k) = |M| = p^k - p^{k-1}$

□

5.2. мултипликативност на ф-я на Ойлер

За естествени числа, които не са степени на просто число функцията на Ойлер може да се пресметне директно от определението, както $\varphi(6) = 2 = |\{1,5\}|$ или $\varphi(10) = 4 = |\{1,3,7,9\}|$.

Но за да се намери обща формула за стойността на $\varphi(n)$ ще трябва да се докаже "мултипликативност" на функцията на Ойлер. За нейното доказателство ще използваме следното свойство:

Твърдение:

Нека a, b, t са естествени числа, като a, b са взаимно прости $(a, b) = 1$, тогава е изпълнено t е взаимно просто с ab точно когато t е взаимнопросто както с a, така и с b.
Доказателство:
Нека $(t, ab) = 1$ и нека $d_1 = (t, a)$ и $d_2 = (t, b)$. Според теоремата на Безу, съществуват цели числа u, v, и използвайки тъждеството получаваме, че t е взаимно просто както с a, така и с b.

$$tu + abv = 1 \Rightarrow \begin{cases} d_1 \mid t, \quad d_1 \mid a \quad \Rightarrow \quad d_1 \mid 1 \quad \Rightarrow \quad d_1 = (t, a) = 1 \\ \\ d_2 \mid t, \quad d_2 \mid b \quad \Rightarrow \quad d_2 \mid 1 \quad \Rightarrow \quad d_2 = (t, b) = 1 \end{cases}$$

За да докажем твърдението в обратна посока, имаме че $(t, a) = 1$ и $(t, b) = 1$. Написваме двете тъждества на Безу $tu_1 + av_1 = 1$ и $u_2t + v_2b = 1$. Умножаваме тези две тъждества на Безу и получаваме

$$\begin{array}{rcl} 1 & = & (u_1t + v_1a).\,(u_2t + v_2b) = \\ & = & (u_1u_2t + u_1v_2b + v_1u_2a)t + v_1v_2ab \end{array}$$

Следователно най-големият общ делител на числата t, ab дели 1 и се получава, че t е взаимно просто с ab.

□

Теорема (мултипликативност на функция на Ойлер):

Нека a, b са естествени числа, които са взаимно прости $(a, b) = 1.$ Тогава за функцията на Ойлер е изпълнено $\varphi(a.\,b) = \varphi(a).\,\varphi(b).$

Доказателство:
Използваме доказаното свойство и търсим онези числа, които са едновременно взаимно прости както с a, така и с b. За удобство записваме последователно всички естествени числа от 1 до ab в $b \times a$ матрица M, стълбовете на тази матрица сме означили със $c_1, \ldots, c_a$.

$$M = \begin{pmatrix} 1 & 2 & \ldots & a \\ a+1 & a+2 & \ldots & 2a \\ \ldots & \ldots & \ldots & \ldots \\ (b-1)a+1 & (b-1)a+2 & \ldots & ba \end{pmatrix}, \quad c_k = \begin{pmatrix} k \\ a+k \\ \ldots \\ (b-1)a+k \end{pmatrix}.$$

Всички числа от един стълб c_k дават еднакъв остатък k при делене с a и $(sa + k, a) = (k, a)$. Следователно или всички числа от един стълб са взаимно прости с a или всички те не са взаимно прости с a. В първия ред имаме точно $\varphi(a)$ взаимно прости с a числа и следователно всички взаимно прости с a числа от матрицата M са разположени в точно $\varphi(a)$ стълба на матрицата.

За да установим по какъв начин са разположени взаимно простите с b числа, да разделим на b всички числа от един стълб на матрицата

$$\begin{array}{rcl} k & = & q_0b + r_0 \\ a+k & = & q_1b + r_1 \\ \ldots\ldots & \ldots & \ldots\ldots \\ (b-1)a+k & = & q_{b-1}b + r_{b-1} \end{array}, \quad 0 \le r_i < b, \ \text{ за } \ i = 0, 1, \ldots, b-1.$$

Ще докажем, че всички получени остатъци са различни.

Допускаме, че съществуват два равни остатъка, т.е. съществуват различни индекси i, j, за които $r_i = r_j$ и $0 \leq i < j < b$. Изваждаме съответните числа и получаваме

$$\begin{array}{c} ja + k = q_j b + r_j \\ ia + k = q_i b + r_i \\ \hline (j-i)a = b(q_j - q_i) \end{array} \quad \Rightarrow \; b \mid (j-i)a \xrightarrow[(a,b)=1]{} b \mid (j-i)$$

Получихме, че $b \mid (j-i)$, но от друга страна $0 < j - i < b$, което е противоречие.

Следователно всички остатъци $\{r_0, r_1, \ldots, r_{b-1}\}$ които се получават от един стълб са различни помежду си и това са в някакъв ред всички възможни остатъци $\{0, 1, \ldots, b-1\}$ които могат да се получат при делене на b. От това получаваме, че във всеки стълб на матрицата M има точно $\varphi(b)$ числа, които са взаимно прости с b.

Окончателно взаимнопростите с a числа се намират в $\varphi(a)$ стълба на матрицата и във всеки един такъв стълб има по $\varphi(b)$ числа които са взоимнопрости с b. Получи се, че числата които са взаимно прости както с a така и с b са $\varphi(a).\, \varphi(b)$ броя, следователно $\varphi(ab) = \varphi(a).\, \varphi(b)$.

$\square$

5.3. пресмятане на ф-я на Ойлер

Общите формули за намиране на стойността на функцията на Ойлер са следствие от доказаната теорема за мултипликативност на функцията на Ойлер и доказания начин за пресмятане функцията от степен на просто число.

Твърдение (общи формули за пресмятане на $\varphi(n)$)

Нека $n > 1$ и нека $n = p_1^{k_1}.\dots.p_s^{k_s}$, където $p_1, \dots, p_s$ са различни прости числа и $k_i > 0.$ Тогава са изпълнени следните равенства, които задават начини за пресмятане на функцията на Ойлер:

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{k_1}).\dots.\varphi(p_s^{k_s}) \\
\varphi(n) &= (p_1^{k_1} - p_1^{k_1-1}).\dots.(p_s^{k_s} - p_s^{k_s-1}) \\
\varphi(n) &= p_1^{k_1-1}.\dots.p_s^{k_s-1}(p_1-1).\dots.(p_s-1) \\
\varphi(n) &= n(1-\tfrac{1}{p_1}).\dots.(1-\tfrac{1}{p_s})
\end{aligned}$$

<u>Пример:</u>
За да пресметнем $\varphi(40)$ представяме го като $40 = 8.5$ и намираме $\varphi(40) = \varphi(8).\varphi(5) = 4.4 = 16$. В този случай е показана как изглежда матрицата M която се използва в доказателството на теоремата за мултипликативност и в нея са маркирани числата, които са взаимно прости с 40.

$$M = \begin{pmatrix}
\boxed{1} & 2 & \boxed{3} & 4 & 5 & 6 & \boxed{7} & 8 \\
\boxed{9} & 10 & \boxed{11} & 12 & \boxed{13} & 14 & 15 & 16 \\
\boxed{17} & 18 & \boxed{19} & 20 & \boxed{21} & 22 & \boxed{23} & 24 \\
25 & 26 & \boxed{27} & 28 & \boxed{29} & 30 & \boxed{31} & 32 \\
\boxed{33} & 34 & 35 & 36 & \boxed{37} & 38 & \boxed{39} & 40
\end{pmatrix}$$

Да обърнем внимание, че такъв тип формула е вярна само когато двата множителя са взаимно прости.
Например $40 = 4.10$, но тези числа не са взаимно прости и затова нямаме равенство

$$\varphi(40) = 16 \neq \varphi(4).\varphi(10) = 2.4 = 8$$

<u>Пример:</u>
Да се пресметне функцията на Ойлер за 144000.
Знаем, че $144000 = 144.1000 = 12^2.10^3 = 2^7.3^2.5^3$ и прилагаме последната формула от твърдението и получаваме

$$\varphi(144000) = 144000.(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5}) = 144000.\frac{1}{2}.\frac{2}{3}.\frac{4}{5} = 38400$$

6. Сравнения по модул

Определение:
Нека a, b, n са цели числа и $n > 1$. Казваме, че a е сравнимо с b по модул n, когато n дели разликата $b - a$. Когато a сравнимо с b по модул n, накратко записваме $a \equiv b \pmod{n}$, или $a \equiv b\ (n)$,

Свойство:
a сравнимо с b по модул n тогава и само тогава, когато числата a и b дават равни остатъци при делене на n.

Всяко едно число е сравнимо с множество най-различни числа по модул n, например са изпълнени следните сравнения, както и много други

$$\begin{array}{ll} 3 \equiv 53 \pmod{10}, & 3 \equiv -47 \pmod{10}, \\ 3 \equiv -777 \pmod{10}, & 3 \equiv 333\,333 \pmod{10}. \end{array}$$

6.1. свойства 1

Твърдение:
Сравнението по модул е релация на еквивалентност, защото са изпълнени свойствата

- $a \equiv a \pmod{n}, \ \forall a \in \mathbb{Z};$
- $\text{ако } a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n};$
- $\text{ако } \ a \equiv b \pmod{n} \text{ и } b \equiv c \pmod{n} \ \Rightarrow a \equiv c \pmod{n};$

Доказателство:
Всяко едно е следствие от основните свойства на делимостта:

- $n \mid (a-a) \Rightarrow a \equiv a(n);$
- ако $b \equiv a(n)$ и $n \mid (a-b) \Rightarrow n \mid (b-a) \Rightarrow b \equiv a(n);$
- ако $\left| \begin{array}{l} a \equiv b(n) \\ b \equiv c(n) \end{array} \right. \Rightarrow n \mid ((a-b)+(b-c)) \Rightarrow a \equiv c(n)$

6.2. свойства 2

Твърдение:
Нека $n > 1$ и нека са изпълнени

- $a_1 \equiv b_1 \pmod{n}$,
- $a_2 \equiv b_2 \pmod{n}$.

Тогава са в сила следните свойства :

1. $a_1 \pm c \equiv b_1 \pm c \pmod{n}, \ \forall c \in \mathbb{Z}$;
2. $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{n}$;
3. $a_1 . c \equiv b_1 . c \pmod{n}, \ \forall c \in \mathbb{Z}$;
4. $a_1 . a_2 \equiv b_1 . b_2 \pmod{n}$;
5. $a_1^k \equiv b_1^k \pmod{n}$, където $k \in \mathbb{N}$.

Доказателство:
Доказателствата на тези свойства използват директно определението.

<u>Доказателството на свойство 2</u> следва от равенството

$$(a_1 \pm a_2) - (b_1 \pm b_2) = (a_1 - b_1) \pm (a_2 - b_2) \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{n};$$

<u>Доказателство на свойство 3:</u>

$$\text{ако } a_1 \equiv b_1 \pmod{n} \Rightarrow n \mid (a_1 - b_1) \Rightarrow n \mid c(a_1 - b_1) \Rightarrow a_1 c \equiv b_1 c \pmod{n}$$

<u>Доказателство на свойство 4:</u> Ако $n \mid (a_1 - b_1)$ и $n \mid (a_2 - b_2)$, следователно получаваме

$$n \mid [(a_1 - b_1)a_2 + b_1(a_2 - b_2)] \Rightarrow a_1 a_2 \equiv b_1 b_2 \pmod{n}$$

<u>Доказателството на свойство 5</u> се получава като се приложи няколко пъти свойство 4.