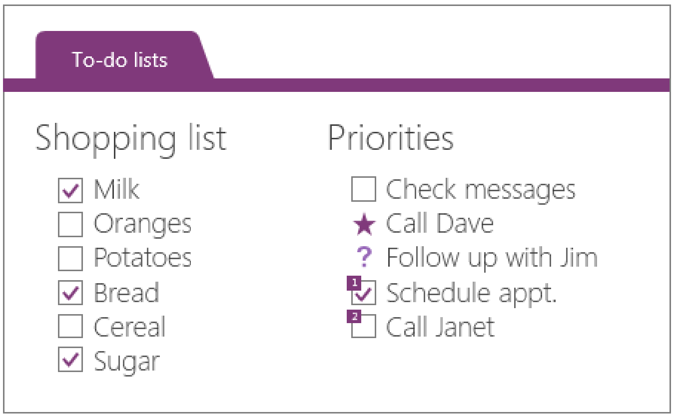
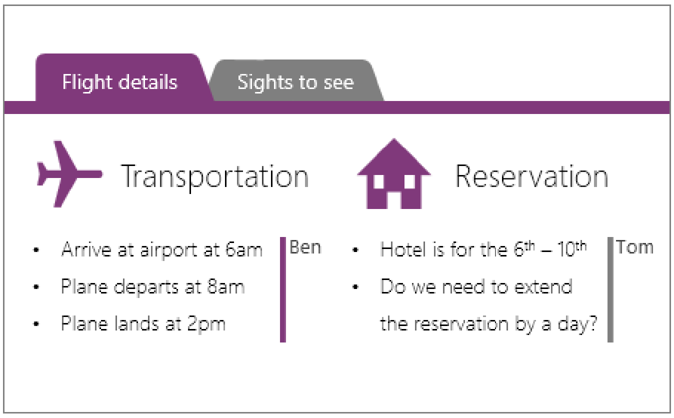
# OneNote Basics




## Remember everything

- Add Tags to any notes
- Make checklists and to-do lists
- Create your own custom tags

HOME → To Do Tag



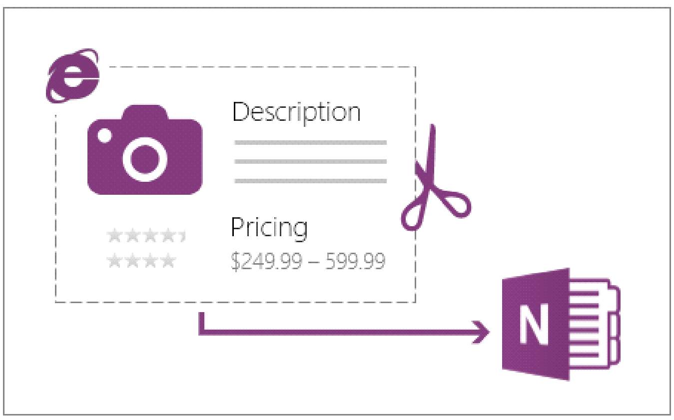

## Collaborate with others

- Keep your notebooks on OneDrive
- Share with friends and family
- Anyone can edit in a browser

FILE → New / Share

## Keep everything in sync

- People can edit pages at the same time
- Real-Time Sync on the same page
- Everything stored in the cloud
- Accessible from any device



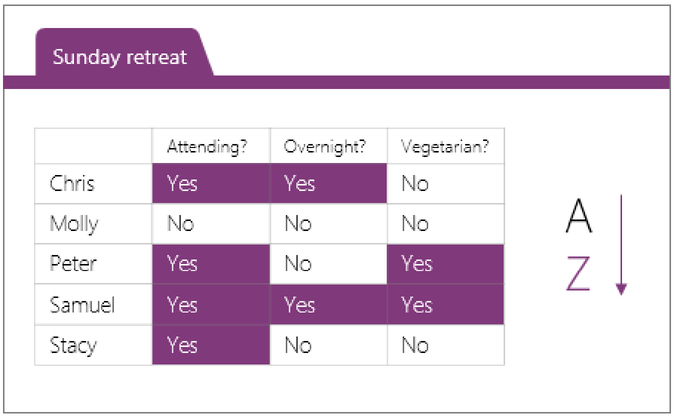

## Clip from the web

- Quickly clip anything on your screen
- Take screenshots of products online
- Save important news articles

in your taskbar

OR

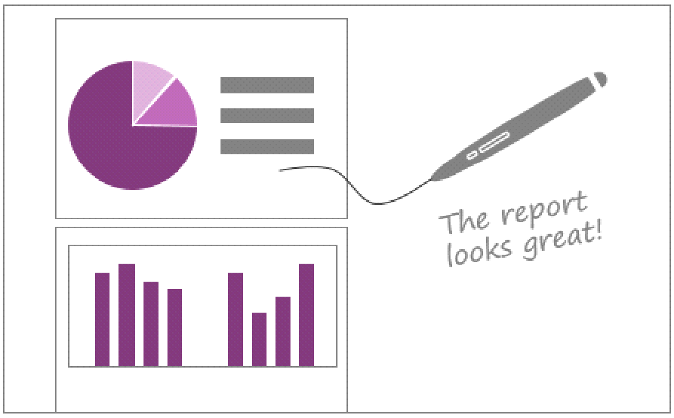
+ S on your keyboard




# Organize with tables

- Type, then press TAB to create a table
- Quickly sort and shade tables
- Convert tables to Excel spreadsheets

TABLE TOOLS LAYOUT → Shading Sort Convert to Excel Spreadsheet



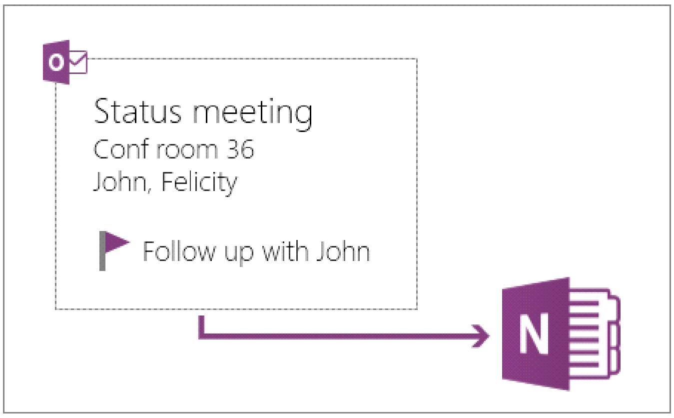

# Write notes on slides

- Send PowerPoint or Word docs to OneNote
- Annotate with a stylus on your tablet
- Highlight and finger-paint

in your taskbar

OR

+ N on your keyboard



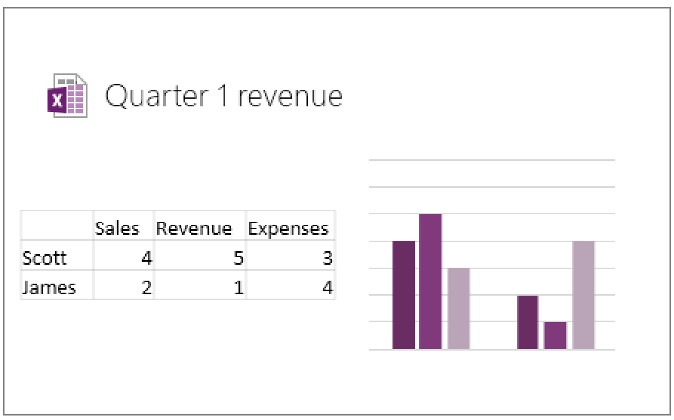

# Integrate with Outlook

- Take notes on Outlook or Lync meetings
- Insert meeting details
- Add Outlook tasks from OneNote

HOME → Outlook Tasks Meeting Details

From Outlook:

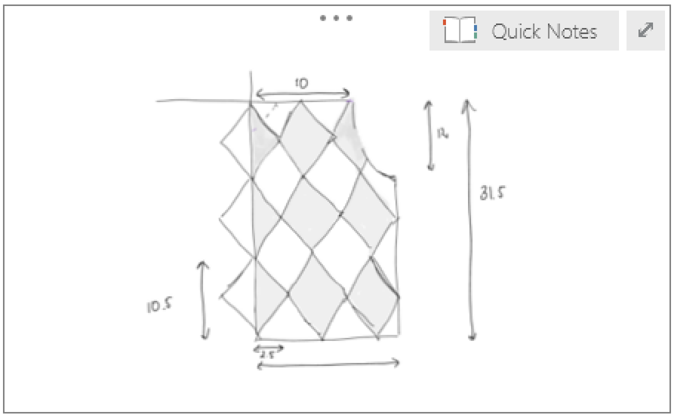
HOME → OneNote




# Add Excel spreadsheets

- Track finances, budgets, & more
- Preview updates on the page

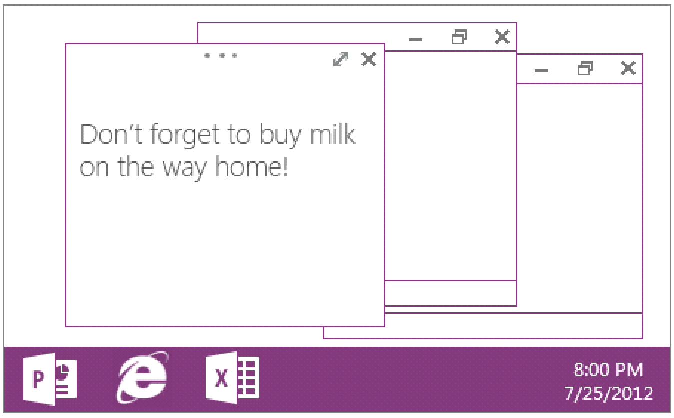
INSERT → Spreadsheet




## Brainstorm without clutter

- Hide everything but the essentials
- Extra space to focus on your notes

in the top corner of the page




## Take quick notes

- Quickly jot down thoughts and ideas
- They go into your Quick Notes section

in your taskbar

OR

+ N on your keyboard

# Printout

сабота, 21 мај 2022 01:21

## Теорија на Броеви

Лука Хаџи Јорданов

СММ

2022

# Што е Теорија на броеви?

Теорија на броеви е гранката од математика која се занимава со деливост, како и со својства на одредени множества на броеви (природни броеви, цели броеви...).

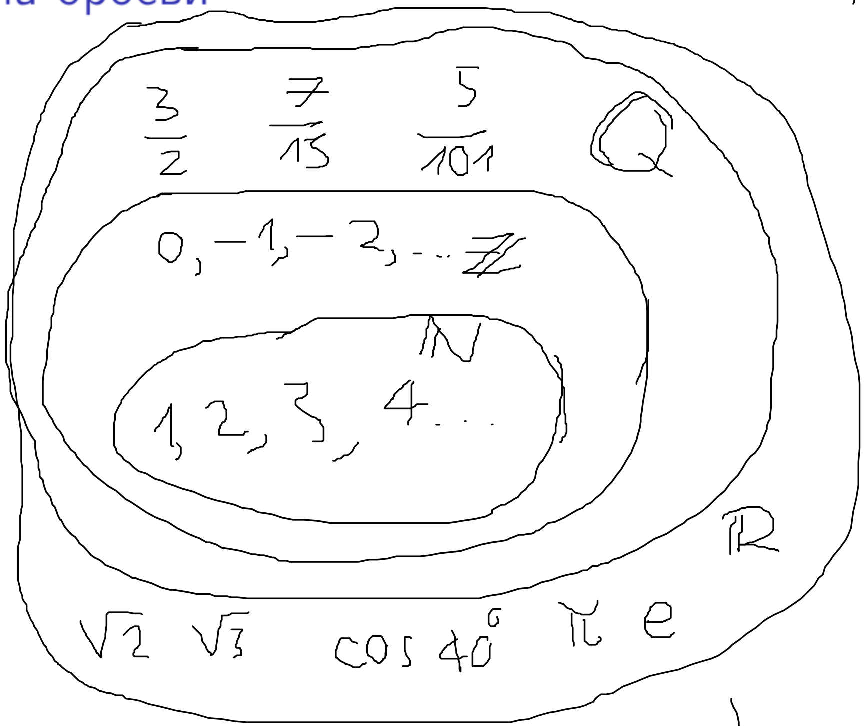
# Множества на броеви

$Q \neq \mathbb{Q}$

$a + bi$

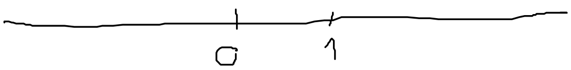
$i = \sqrt{-1}$

$a$




$a \in X$

$N_0 = (0, 1, 2, \ldots)$



# Деливост и ознака

$\leq$ $\geq$

$4 \nmid 2$

$\frac{0}{0} = \text{undef.}$

За бројот $b$ велиме дека е делив со бројот $a$ (или дека $a$ е делител на бројо $b$) ако постои цел број $k$ така што

$$b = k \cdot a$$

$a = 0$ $b = 0$

Ако бројот $b$ се дели со бројот $a$ тогаш запишуваме $a|b$.

$2 \mid 4$ $4 = k \cdot 2$ $k = 2$

$a$ $b$

$b = k \cdot 0 = 0$

$3 \nmid 5$ $5 = k \cdot 3$

$0 | 0$ $0 \nmid 2$ $0 \nmid 7$

## Основни својства

$a \neq 0$

$b$

Својство 1: За секој цел број $a$ важи $a|a$ (секој цел број се дели со самиот себе).

Доказ: За секој цел број $a$ важи $a = 1 \cdot a$. Според дефиницијата од претходниот слајд, тоа значи дека $a|a$.

$a \mid b \qquad \exists k \in \mathbb{Z} \qquad b = k \cdot a$

$a = k \cdot a$

$a = 1\ a$

$p.$

## Основни својства

$3 | 6$ $6 \nmid 3$

$a | b$

Својство 2: Ако за природни броеви $a$ и $b$ важат $a|b$ и $b|a$, тогаш $a = b$.

Доказ: Повторно користејќи ја дефиницијата за деливост, од $a|b$ имаме дека постои цел број $k$ така што $b = k \cdot a$, додека од $b|a$ имаме дека постои цел број $m$ така што $a = m \cdot b$. Комбинирајќи ги овие две еднаквости имаме $b = k \cdot a = k \cdot m \cdot b$, а како $b = 1 \cdot b$, имаме дека $m \cdot k = 1$, односно $m = k = 1$. Оттука имаме $a = m \cdot b = 1 \cdot b = b$, односно $a = b$.

С.

Пьмош: $|a| = |b|$

## Основни својства

$2 \mid 16$ $16 \mid 32$

$2 \mid 32$

Својство 3: Ако $a|b$ и $b|c$, тогаш $a|c$.

Доказ: Од $a|b$ имаме $b = k \cdot a$ за $k \in \mathbb{Z}$, додека од $b|c$ имаме $c = m \cdot b$ за $m \in \mathbb{Z}$. Оттука следува
$c = m \cdot b = m \cdot \underbrace{k \cdot a} = (m \cdot k) \cdot a$, што значи дека $a|c$.

$m \cdot k \in \mathbb{Z}$

$l = mk$

$c = l a$

$a \mid c$

# Основни својства

$27 + 15 = 42$

$3|27$ $3|15$ $3|42$

Својство 4: Ако имаме $a = b + c$ за некои цели броеви $a, b$ и $c$, и цел број $n$ (различен од 0) така што $n|b$ и $n|c$, тогаш важи $n|a$.

Доказ: Од $n|b$ и $n|c$ имаме $b = k \cdot n$ и $c = m \cdot n$ за $k, m \in \mathbb{Z}$, односно $a = b + c = k \cdot n + m \cdot n = (k + m) \cdot n$, што имплицира дека $n|a$.

$k + m = 1$ $a = 1 \cdot n$

Последица: Ако важи $a = b + c$ за $a, b, c \in \mathbb{Z}$ и имаме природен број $n$ така што $n|a$ и $n|b$, тогаш $n|c$.

$$\underbrace{a_1}_{c} + \underbrace{a_2 + \dots + a_n}_{b} = \underbrace{0}_{a}$$

$k|0$

$k|a_2$

$k|a_3$

$\vdots$

$k|a_n$

## Прости броеви

$1 \mid p$ $\quad p \mid p$

$p = k \cdot 1$ $\quad p = k \cdot p$

Прости броеви се тие природни броеви кои се делат само со 1 и самите себе ($1|p$ и $p|p$). $p > 1$

Со други зборови, простите броеви се броевите кои имаат ТОЧНО 2 делители.

Ова значи дека за бројот $p$ велиме дека е прост ако $k|p$ важи само за $k = 1$ и $k = p$.

Прости броеви се броевите $2, 3, 5, 7, 11, 13 \ldots$ $\quad 3 \mid 57$

## Сложени броеви

$k - 1, k$

Броевите кои имаат повеќе од 2 делители се нарекуваат сложени.

Сложени броеви се броевите 4, 6, 8, 9, 10, 12....

Бројот 1 не е ниту прост ниту сложен!

Page 11

сабота, 21 мај 2022 01:21

# Ератостеново сито

~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ . . . ~~25~~ . . .

~~35~~ . . .

## Основно теорема на аритметиката

ОТА: За секој природен број $n > 1$, постојат (уникатни) прости брови $p_1, p_2, \dots, p_k$ и (уникатни) природни броеви $a_1, a_2, \dots, a_k$ така што

$$\underline{n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}}$$

$p_1 < p_2 < p_3 < \dots < p_k$

Десната страна на еднаквоста се нарекува „каноничен запис на бројот $n$“.

$3 \cdot 2^3$

$24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3 = \underline{2^3 \cdot 3}$

$120 = 2 \cdot \underline{60} = 2 \cdot 2 \cdot \underline{30} = \underline{2 \cdot 2 \cdot 2} \cdot \underline{15} = 2^3 \cdot 3 \cdot 5$

# Делење со остаток

Теорема 1: За секои природни броеви $a, b$ постојат уникатни ненегативни цели броеви $q, r$ за кои важи

$a - qb = r$

$$a = qb + r,$$

$14 = 4 \cdot 3 + 2$

$14 = 4 \cdot 3 + 2$

при што важи $0 \leq r < b$. Бројот $r$ се нарекува остаток на $a$ при делење со $b$.

Забелешка: Бројот $a$ може да биде цел број, а доказот на теоремата во тој случај е аналоген на следниот доказ.

$4 : 1 = 4$ ост. $r$

$14 : 3 = 4$ ост. $2$

# Делење со остаток

$a = 0 \quad a + b = 4$

$b = 4 \quad a + 2b = 8$

Доказ: Да докажеме прво дека постојат такви броеви. Го разгледаме множеството

$$S = \{..., a - 3b, a - 2b, a - b, a, a + b, a + 2b, a + 3b, ...\}$$

Нека $T$ биде подмножество од $S$ така што $T$ ги содржи сите ненегативни елементи од $S$. Ова множество мора да има минимален елемент. Нека тој елемент биде $a - qb$ и нека го означиме со $r$ (односно $r = a - qb$). Ако важи $0 \leq r < b$, тогаш постоењето на броевите $q$ и $r$ е докажано. Ако важи $r \geq b$, тогаш бројот $a - (q + 1)b$ е исто така ненегативен (бидејќи $r - b$ е ненегативен), што значи дека $a - (q + 1)b$ припаѓа во $T$, а воедно е помал од $r$, што е во контрадикција со претпоставката дека $r$ е минималниот елемент на $T$.

$a - qb - b = a - (q+1)b = r - b \geq 0$

# Делење со остаток

$q_1 - q = 0 \quad (q_1 - q)b = 0$

$a, b \in \mathbb{Z}$

$q, r \in$

Понатаму, да докажеме дека тие се единствени. Да претпоставиме дека за $a, b$ важи $a = qb + r$ за $q, r \in \mathbb{N}^0$ кои ги исполнуваат условите на теоремата, но и $a = q_1 b + r_1$ за $q_1, r_1 \in \mathbb{N}^0$ и без губење на општоста (БГО) да претпоставиме дека $r \leq r_1$. Изедначувајќи ги двата израза за $a$ добиваме $qb + r = q_1 b + r_1$, односно после префрлање

$b|$

$$0 = (q_1 - q)b + (r_1 - r) \qquad (1)$$

$\cancel{b = k} \cdot b$

$b|0 \qquad b| \qquad 0$

Од $0 = 0 \cdot b$ имаме дека $0$ е делив со $b$, а очигледно $(q_1 - q)b$ е делив со $b$, што според Последицата од Својство 4 значи дека $r_1 - r$ е делив со $b$. Но, знаеме дека $0 \leq r \leq r_1 < b$, та $b > r_1 - r \geq 0$, а како $r_1 - r$ се дели со $b$, тоа знажи дека $r_1 - r = 0$, односно $r_1 = r$. Со замена на добиеново равенство во (1) добиваме $(q_1 - q)b = 0$, а како $b \neq 0$, имаме $q_1 = q$.

$b - 1 - 0$

$=$

$b - 1$

$(q_1 - q)b = k \cdot b$

## Најголем заеднички делител

$2 | 14 \quad 2 | 22$

$-14 = (-7) \cdot 2 \quad 2 | -14 \quad 2 | 22$

Нека $a, b \in \mathbb{Z}$. Ако важи $d|a$ и $d|b$ за природен број $d$, тогаш бројот $d$ го нарекуваме заеднички делител на броевите $a$ и $b$. 1

Ако за бројот $d$ важи дека е заеднички делител на $a$ и $b$ и притоа за секој друг заеднички делител $d_1$ на $a$ и $b$ важи $d_1 \leq d$, бројот $d$ го нарекуваме најголемиот заеднички делител на броевите $a$ и $b$.

Најголемиот заеднички делител на $a$ и $b$ се означува со НЗД$(a, b)$ или некогаш со $NZD(a, b)$. $GCD(a, b)$

$(a, b)$

Бидејќи станува збор за истите броеви, важи $NZD(a, b) = NZD(b, a)$.

$(1, 0)$

$2 | -2 \qquad |-2| = |2| = 2$

$\frac{5}{1}$

## Најголем заеднички делител

$a = q_1^{u} q_2^{u} \dots q_s^{u}$

$b = r_1^{u} \dots r_t^{u}$

Барање на НЗД: За природните броеви $a$ и $b$ со канонични облици $a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ и $b = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$, каде $p_1, p_2, \dots, p_k$ е унијата на простите делители на $a$ и $b$, односно некои од степените $a_1, a_2, \dots, a_k, b_1, b_2, \dots b_k$ можат да бидат 0 (во случај основата на степенот кој е 0 да не го дели бројот во чиј каноничен запис се наоѓа). Тогаш

$$NZD(a,b) = p_1^{min\{a_1,b_1\}} p_2^{min\{a_2,b_2\}} \dots p_k^{min\{a_k,b_k\}}$$

24

$a = 2^3 \cdot 3 = 2^3 \cdot 3^1 \cdot 5^0$ $\quad NZD(a,b) = 2^0 \cdot 3^1 \cdot 5^0 =$

$b = 3^2 \cdot 5 = 2^0 \cdot 3^2 \cdot 5^1$ $\quad = 3$

45

## Најголем заеднички делител

$p \mid NZD$ и $NZD \mid a$

$p \mid a$

Доказ: Очигледно, сите прости делители на $NZD(a, b)$ се делители и на $a$ и на $b$. Затоа, можеме $NZD(a, b)$ да го запишеме во облик

$c_1 \leq a_1$

$c_1 \leq b_1$

$p_1^{c_1} \mid a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$

$$NZD(a, b) = p_1^{c_1} p_2^{c_2} \dots p_k^{c_k}$$

каде $c_1, c_2, \dots, c_k$ се ненегативни цели броеви. За $c_1$ имаме дека $p_1^{c_1} | p_1^{a_1}$ и $p_1^{c_1} | p_1^{b_1}$, та $c_1 \leq min\{a_1, b_1\}$ (во спротивно би имале дека или $a$ или $b$ се дели со поголем степен на $p_1$ отколку што има во каноничниот запис, што не е можно). Ако $c_1 < min\{a_1, b_1\}$, тогаш бројот $p_1 \cdot NZD(a, b)$ е заеднички делител на $a$ и $b$ и е поголем од $NZD(a, b)$, што не е можно. Затоа $c_1 = min\{a_1, b_1\}$. На ист начин, имаме $c_2 = min\{a_2, b_2\}$, ..., $c_k = min\{a_k, b_k\}$, што и требаше да докажеме.

$p_1 NZD = p_1^{c_1+1} \dots$ $c_1 + 1 \leq min\{a_1, b_1\}$

# Најголем заеднички делител

$a | b \quad a | c \quad NZD(a, b, c) = a$

Својство 5: Ако $a|b$ за $a, b \in \mathbb{Z}$, тогаш важи $NZD(a, b) = a$.

$a | a$

Доказ: Од Својство 1 имаме $b|b$, што заедно со $a|b$ ни дава дека $a$ е заеднички делител на $a$ и $b$. Ако постои $d > a$ така што $d$ е заеднички делител на $a$ и $b$, имаме $a = k \cdot d$, односно $|a| \geq d$, што е контрадикција со претпоставката $d > a$. Со тоа е докажано бараното.

$|-1 \cdot d| = d \geq d$

$|-2 \cdot d| = 2d \geq d$

$|2 \cdot d|$

## Најголем заеднички делител

$n = a + b$

$a+b, b$ $k|$ $k|$ $k|$ $k|$

Својство 6: Важи $NZD(a,b) = NZD(a, a+b) = NZD(a, a-b)$.

$+(-b)$

Доказ: Нека $n = a - b$. Од Својство 4 имаме дека ако $m$ е заеднички делител на $a$ и $b$, тогаш $m$ е делител и на $n$. Тоа значи дека сите заеднички делители на $a$ и $b$ се делители и на $n$. Од друга страна, $a = n + b$, та повторно со примена на Својство 4 ни следува дека сите заеднички делители на $a$ и $n$ се делители и на $b$. Оттука следува дека множеството делители на $a$ и $b$ е исто со множеството делители на $a$ и $n$, та $NZD(a,b) = NZD(a, a-b)$. Од докажаното следува

$$NZD(a, a+b) = NZD(a, (a+b) - a) = NZD(a, b)$$

та со тоа ни е докажано својството.

## Најголем заеднички делител

$$\overset{7}{}\quad\overset{3}{}$$
$$NZD(15, 32) = 1$$

За броевите $a$ и $b$ велиме дека се заемно прости ако важи $NZD(a, b) = 1$.

Својство 7: Броевите $n$ и $n+1$ се заемно прости.

Доказ: Според Својство 6 имаме $NZD(n, n+1) = NZD(n, (n+1) - n) = NZD(n, 1) = 1$, при што последната еднаквост следува од Својство 5.

## Најголем заеднички делител

$a = k \cdot d$
$b = l \cdot d$

Својство 8: Нека за броевите $a$, $b$ и $d$ важи $d = NZD(a, b)$. Тогаш $NZD(\frac{a}{d}, \frac{b}{d}) = 1$.

Доказ: Од тоа дека $d$ е најголем заеднички делител на броевите $a$ и $b$ следи дека $d$ е делител на тие броеви, односно дека постојат $k, m \in \mathbb{Z}$ за кои важи $a = kd$ и $b = md$, односно важи $\frac{a}{d} = k$ и $\frac{b}{d} = m$. Значи, треба да докажеме дека $NZD(k, m) = 1$. Нека $t = NZD(k, m)$. Исто како претходно, имаме дека $k = lt$ и $m = nt$. Оттука следува $a = kd = ltd = l \cdot (td)$ и $b = md = ntd = n \cdot (td)$, односно $td$ е заеднички делител на $a$ и $b$, та како за $t \geq 2$ важи $|td| \geq |2d| > d$, односно $td > NZD(a, b)$, следува $t = 1$, т.е. $NZD(k, m) = 1$.

$td \geq 2d > d \quad t = 1$

## Бесконечен број на прости броеви

$A = q_1^{c_1} \cdot \ldots q_r^{c_r}$

Евклид: Има бесконечно многу прости броеви. $c_1 = 1$ $r = 1$

$A = q_1$

Доказ: Да го претпоставиме спротивното, нека има конечно многу прости броеви и нека $S = \{p_1, p_2, ..., p_k\}$ е множеството од сите нив. Да го дефинираме бројот $A = p_1 p_2 ... p_k + 1$. Според ОТА, имаме дека бројот $A$, кој е поголем од 1, има прост делител, кој ќе го крстиме $q$. Имаме $q | p_1 p_2 ... p_k + 1$, што според Својство 5 значи дека $NZD(q, p_1 p_2 ... p_k + 1) = q > 1$. Бидејќи $q$ е прост број, а според нашата претпоставка такви броеви ги има конечно многу, следува дека $q = p_i$ за некое $1 \leq i \leq k$. Оттука $NZD(q, p_1 p_2 ... p_k + 1) = NZD(p_i, p_1 p_2 ... p_k + 1) = NZD(p_i, p_1 p_2 ... p_k + 1 - p_i) = NZD(p_i, p_1 p_2 ... p_k + 1 - 2p_i) = ... = NZD(p, p_1 p_2 ... p_k + 1 - (p_1 p_2 ... p_{i-1} p_{i+1} ... p_k) \cdot p_i) = NZD(p_i, p_1 p_2 ... p_k + 1 - p_1 p_2 ... p_k) = NZD(p_i, 1) = 1$ според Својство 7. Оттука следи $q = 1$, што не е можно бидејќи $q$ е прост број. Од добиената контрадикција следи својството.

## Најмал заеднички содржател

$s \geq \max\{a, b\}$

$a | s \quad b | s \quad s, 2s, 3s, \ldots$

Нека $a, b \in \mathbb{Z}$. Ако важи ~~$s|a$ и $s|b$~~ за природен број $s$, тогаш бројот $s$ го нарекуваме заеднички содржател на броевите $a$ и $b$.

Ако за бројот $s$ важи дека е заеднички содржател на $a$ и $b$ и притоа за секој друг заеднички содржател $s_1$ на $a$ и $b$ важи $s \leq s_1$, бројот $s$ го нарекуваме најмалиот заеднички содржател на броевите $a$ и $b$.

$a < b$

$\leq$

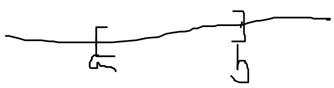
$<$

Најмалиот заеднички содржател на $a$ и $b$ се означува со НЗС$(a, b)$ или некогаш со $NZS(a, b)$.

$LCM(a, b)$

Бидејќи станува збор за истите броеви, важи $NZS(a, b) = NZS(b, a)$.

$[a, b]$



# Најмал заеднички содржател

Барање на НЗС: За природните броеви $a$ и $b$ со канонични облици $a = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$ и $b = p_1^{b_1} p_2^{b_2} ... p_k^{b_k}$, каде $p_1, p_2, ..., p_k$ е унијата на простите делители на $a$ и $b$, односно некои од степените $a_1, a_2, ..., a_k, b_1, b_2, ... b_k$ можат да бидат 0 (во случај основата на степенот кој е 0 да не го дели бројот во чиј каноничен запис се наоѓа). Тогаш

$$NZS(a, b) = p_1^{max\{a_1, b_1\}} p_2^{max\{a_2, b_2\}} ... p_k^{max\{a_k, b_k\}}$$

Доказ: За домашна.

$a = 2^3 \cdot 3 \cdot 7 = 168$ $\quad NZS(168, 550) = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^1 \cdot 11^1$

$b = 2 \cdot 5^2 \cdot 11 = 550$

$a = 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^0$ $\quad b = 2^1 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^1$

# Најмал заеднички содржател

$\mathbb{N}$ $NZD = a$

Својство 9: Ако за $a, b \in \mathbb{Z}$ важи $a|b$, тогаш $NZS(a, b) = b$.

Доказ: Од $a|b$ следува $b = ka$ за некое $k \in \mathbb{Z}$. Од $b|b$ и $a|b$ следува дека $\underline{b}$ е заеднички содржател на $a$ и $b$. Ако постои заеднички содржател на $a$ и $b$ $t$ така што $t < b$, тогаш $t = lb$ за $l \in \mathbb{Z}$, та $|t| = |lb| \geq |b|$, што е во контрадикција со претпоставката за $t$. Оттука следува бараното својство.

$l \geq 1$ $t \geq b$

# Најмал заеднички содржател

Својство 10: Нека $a, b \in \mathbb{Z}$. Важи

$$NZD(a,b) \cdot NZS(a,b) = ab$$

Доказ: Нека $a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ и $b = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$ се каноничните облици на $a$ и $b$. Според „Барање на НЗД" и „Барање на НЗС" имаме дека

$$NZD(a,b) = p_1^{min\{a_1,b_1\}} p_2^{min\{a_2,b_2\}} \dots p_k^{min\{a_k,b_k\}}$$

$$NZS(a,b) = p_1^{max\{a_1,b_1\}} p_2^{max\{a_2,b_2\}} \dots p_k^{max\{a_k,b_k\}}$$

# Најмал заеднички содржател

та со приметување дека $a+b=\overset{a}{min\{a+b\}}+\overset{b}{max\{a+b\}}$ (БГО можеме да претпоставиме дека $a \leq b$, та имаме $min\{a+b\}=a$ и $max\{a+b\}=b$), добиваме

$$NZD(a,b)\cdot NZS(a,b)=$$

$$=p_1^{min\{a_1,b_1\}}p_2^{min\{a_2,b_2\}}...p_k^{min\{a_k,b_k\}}\cdot p_1^{max\{a_1,b_1\}}p_2^{max\{a_2,b_2\}}...p_k^{max\{a_k,b_k\}}=$$

$$=p_1^{min\{a_1,b_1\}+max\{a_1,b_1\}}p_2^{min\{a_2,b_2\}+max\{a_2,b_2\}}...p_k^{min\{a_k,b_k\}+max\{a_k,b_k\}}=$$

$$=p_1^{a_1+b_1}p_2^{a_2+b_2}...p_k^{a_k+b_k}=\underbrace{p_1^{a_1}p_2^{a_2}...p_k^{a_k}}_{a}\cdot\underbrace{p_1^{b_1}p_2^{b_2}...p_k^{b_k}}_{b}=ab$$

# Евклидов алгоритам

Својство 11: Ако за $a, b \in \mathbb{Z}$ важи $a = qb + r$ ($q \in \mathbb{Z}$, $0 \leq r < b$), тогаш $NZD(a, b) = NZD(b, r)$.

Доказ: Со примена на Својство 6 $q$ пати, добиваме

$$NZD(a, b) = NZD(b, a) = NZD(b, qb + r) =$$

$$= NZD(b, qb + r - b) = NZD(b, (q - 1)b + r) =$$

$$= NZD(b, (q - 1)b + r - b) = NZD(b, (q - 2)b + r) = \ldots =$$

$$= NZD(b, b + r) = NZD(b, \cancel{b} + r - \cancel{b}) = NZD(b, r)$$

# Евклидов алгоритам

Евклидов алгоритам: Нека

$$a = qb + r \qquad 0 \leq r < b \qquad r \leq b-1$$
$$b = q_1 r + r_1 \qquad 0 \leq r_1 < r \qquad r_1 \leq r-1 \leq b-2$$
$$r = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1 \qquad r_2 \leq b-3$$
$$r_1 = q_3 r_2 + r_3 \qquad 0 \leq r_3 < r_2$$
$$r_{k-2} = q_k r_{k-1} + r_k$$
$$\vdots$$
$$r_{k-1} = q_{k+1} r_k + r_{k+1} \qquad 0 \quad r_{k+2} \leq 0 = b - b$$
$$r_k = q_{k+2} r_{k+1} + \cancel{r_{k+2}}$$

$a \mid b$

$NZD = a$

Според Својство 11 имаме $NZD(a, b) = NZD(b, r) = NZD(r, r_1) = ... = NZD(r_k, r(k+1)) = r_{k+1}$, каде последната еднаквост следува од Својство 5. Овој алгоритам ни овозможува лесно пресметување на НЗД на два броја.

## Евклидов алгоритам

$\underset{a}{122}$ $\underset{b}{46}$

Д: $NZD(144, 16)$

$122 = \underline{2} \cdot 46 + \underline{30} \quad 0 \le r < 46$

$46 = \underline{1} \cdot 30 + 16 \quad 0 \le r_1 < 30$

$30 = \underline{1} \cdot 16 + \underline{14} \quad 0 \le r_2 < 16$

$16 = 1 \cdot 14 + 2$

$14 = 7 \cdot \underline{2}$

$NZD(\underline{122}, \underline{46}) = 2$

# Теорема на Безу

Теорема на Безу: Важат $d|a$, $d|b$ и $d = ax + by$ за цели броеви $x$ и $y$ ако и само ако $d = NZD(a, b)$.

$$\cancel{ax + by = d}$$

$$r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$$

Доказ: Според Евклидовиот алгоритам имаме
$d = r_{k+1} = r_{k-1} - q_{k+1} r_k = r_{k-1} - q_{k+1}(r_{k-2} - q_k r_{k-1}) =$
$(r_{k-3} - q_{k-1} r_{k-2}) - q_{k+1}(r_{k-2} - q_k(r_{k-3} - q_{k-1} r_{k-2})) = \ldots$
продолжувајќи вака ќе го изразиме $r_{k-2}$ преку $r_{k-3}$ и $r_{k-4}$, па $r_{k-3}$ преку $r_{k-4}$ и $r_{k-5}$ итн. се додека не стигнеме до изразување на $r$ преку $a$ и $b$, при што ќе добиеме израз од обликот $d = ax + by$.

# Теорема на Безу

За другата насока приметувама дека од првата насока ни следува $NZD(a,b) = au + bv$ за некои цели броеви $u$ и $v$, а од $d|a$ и $d|b$ имаме $a = kd$ и $b = md$ за $k, m \in \mathbb{Z}$, та $NZD(a,b) = au + bv = (kd)u + (md)v = d(ku + mv)$, што имплицира $d|NZD(a,b)$. Од $NZD(a,b)|a$ и $NZD(a,b)|b$ имаме $a = a_0 NZD(a,b)$ и $b = b_0 NZD(a,b)$, та $d = ax + by = (a_0 NZD(a,b))x + (b_0 NZD(a,b))y = NZD(a,b)(a_0 x + b_0 y)$, односно $NZD(a,b)|d$. Последнава деливост во комбинација со $d|NZD(a,b)$, според Својство 2 ни дава $d = NZD(a,b)$.

$NZD = w \cdot d$

$a|b$ $b|a$

# Теорема на Безу

$a = 6 \quad b = 16 \quad NZD(6,16) = 2$

$2 = 6x + 16y \qquad 3x + 2y = 1$

$1 = 3x + 8y \qquad x = 1$

$y = -1$

$\underline{x = -5} \quad \underline{y = 2}$

$8y + 3x = 16 - 15 = 1$

## Најголем заеднички делител

Својство 12: Ако $a|bc$ и $NZD(a,c) = 1$, тогаш $a|b$.

Доказ: Од $NZD(a,c) = 1$ според Теоремата на Безу имаме дека постојат $x, y \in \mathbb{Z}$ за кои важи $ax + cy = 1$, та
$\underline{a} \cdot bx + \underline{(bc)} \cdot y = \underline{b}$, но како $a|a$ и $a|bc$, според Својство 4 имаме дека $\underline{a|b}$.

Д: Преку Кан. запис!

## Најголем заеднички делител

Својство 13: За цели броеви $a, b$ и $k$ важи

$$NZD(ka, kb) = k \cdot NZD(a, b)$$

Доказ: Ако $d = NZD(a, b)$ според Теоремата на Безу имаме $d = ax + by$ за некои цели броеви $x$ и $y$, та $kd = (ka)x + (kb)y$, што повторно според Теоремата на Безу (другата насока), бидејќи $kd|ka$ и $kd|kb$, важи $kNZD(a, b) = kd = NZD(ka, kb)$.

## Најголем заеднички делител

$b_1 = 2a_1 \Leftarrow q_1^{b_1} = p_i^{2a_i}$

Својство 14: Ако за броевите $a$ и $c$ имаме $NZD(a, c) = 1$ и $ac = b^2$, тогаш постојат цели броеви $x$ и $y$ така што важи $a = x^2$ и $c = y^2$.

$q_1 = p_i$

Доказ: Ако $b = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ е бројот $b$ во каноничен запис, тогаш $b^2 = p_1^{2a_1} p_2^{2a_2} \dots p_k^{2a_k}$, та сите степени на простите делители на $b$ се парни (во каноничен облик). Со оглед на тоа дека $a$ и $c$ немаат заеднички делители а нивниот производ е $b^2$, следува дека степените на простите делители на $a$ и $c$ во каноничен запис се парни, односно дека самите $a$ и $c$ се квадрати на некои цели броеви. Оттука следи бараното.

$ac = b^2$

$s + t = k$

$a = q_1^{b_1} \dots q_s^{b_s}$

$c = r_1^{c_1} \dots r_t^{c_t}$

$p, q, r \quad p_i, q_i, r_i$

а) $NZD(n, n+2)$

$$NZD(n, n+2) = NZD(n, n+2-n) =$$
$$= NZD(n, 2) = d$$

$d \mid n$ $\qquad$ $d \mid 2$ $\qquad$ или $d = 1$ ← или

$n$ е парно $\qquad$ или $\underline{d = 2}$ $\qquad$ $n$ е непарно

$n \equiv 0 \pmod 2$

$n \equiv_2 0$

$n \overset{2}{\equiv} 0$

b) $NZD(n, n+3)$

$$NZD(n, n+3) = NZD(n, n+3-n) =$$
$$= NZD(n, 3) = d$$

$d \mid 3$ или $d = 1$ или $d = 3$

3 го дели $n \Rightarrow d = 3$

3 не го дели $n \Rightarrow d = 1$

$n \equiv_3 0 \Rightarrow d = 3$ $n \equiv_3 1$ или $n \equiv_3 2$

$d = 1$

c) $NZD(n, n+24)$

$$NZD(n, n+24) = NZD(n, n+24-n) =$$

$$= NZD(n, 24) = d \qquad d \in \{1, 2, 3, 4, 6, 8, 12, 24\}$$

$$NZD(216, 24) = NZD(2^3 \cdot 3^3, 2^3 \cdot 3) =$$

$$= 2^3 \cdot 3^1 = 24$$

# Page 41

сабота, 21 мај 2022 01:21

# Page 42

субота, 21 мај 2022 01:21

## Домашна

1. Докажи ги својствата 2 и 3 за цели броеви $a, b, c$ така што ниеден од нив не е еднаков на 0.

2. Најди $NZD(n, n+2), NZD(n, n+3)$ и $NZD(n, n+24)$.
Помош: Вредностите зависат од $n$.

3. Докажи го Својство 8 преку доказ со контрадикција!
4. Секој заеднички делител на $a$ и $b$ е делител на $NZD(a, b)$. Докажи.

5. Секој заеднички содржател на $a$ и $b$ се дели со $NZS(a, b)$.

6. Докажи дека под истите услови како во „Барање на НЗД“, $NZS(a, b)$ може да се најде со промена на минимумите во максимуми. Помош: Доказот е аналоген.