УНИВЕРЗИТЕТ У БЕОГРАДУ
МАТЕМАТИЧКИ ФАКУЛТЕТ



**РАВИЋ АНА**

# Модуларна аритметика и примене

МАСТЕР РАД

**Ментор: др. Александар Липковски**

Београд 2015.

# Садржај :

# Увод

Мастер рад је посвећен модуларној аритметици и њеној примени у криптографији (науци која се бави методима очувања тајности информација ) и у визуалној уметности.

Шта је то модуларна аритметика?

Модуларна аритметика представља аритметички систем код кога се бројеви враћају у круг, након што достигну одређену вредност — модуло. Модуларну аритметику је увео Карл Фридрих Гаус у свом делу *Disquisitiones Arithmeticae (Аритметичка истраживања)*.

Општепозната примена модуларне аритметике је у 24-часовном мерењу времена: дан траје од поноћи до следеће поноћи, и подељен је на 24 часа, од 0 до 23. Ако је у одређеном тренутку 19:00 часова (седам увече), осам сати касније време не износи 27:00 (као код уобичајеног сабирања: 19 + 8 = 27), већ је тада 03:00 (наредног дана). Исто, ако је у одређеном тренутку подне (12:00), и од тог тренутка је протекао 21 час, сат ће показивати 09:00 наредног дана, а не 33:00 (као код уобичајеног сабирања). Како часови поново почињу од 00 након што прођу 24 сата, овде се ради о аритметици по модулу 24 — бројеви поново почињу од нуле након што достигну 24.

Модуларна аритметика се математички може посматрати увођењем релације конгруенције на скупу целих бројева.

# 1. Дељивост целих бројева

## 1.1. Основне особине

**Дефиниција 1.1.** Нека су a и b цели бројеви. Ако постоји цео број m такав да је b=m·a, тада кажемо да је a **делитељ** броја b и да је b **садржалац** броја a. То записујемо овако a|b.
На пример: 3|9, 5|30, 4|0 .
Ако је a|b, очигледно је и a|(-b), (-a)|b, (-a)|(-b). Зато се, при проучавању дељивости, најчешће ограничавамо на ненегативне целе бројеве.

**Дефиниција 1.2.** Број a називамо **прави делитељ** од b, ако је a|b и a≠b.

У следећој теореми дате су неке од најважнијих особина релације дељивости.

**Теорема 1.1.** Нека су a, b, c произвољни ненегативни цели бројеви. Тада важи:
а) ако је a≠0 тада важи следеће: a|a , a|0 и 1|a;
б) ако је a|b и b|c, тада је a|c ;
в) ако је a|b и b≠0, тада је $0 < a \leq b$ ;
г) ако је a|b и a|c, тада је, за произвољне целе бројеве x и y, a|(b·x+c·y) ;
д) ако је a|b и b|a, тада је a=b ;
ђ) ако је a|b и c≠0, тада је ac|bc ;
е) ако је ac|bc и c≠0, тада је a|b .

**Доказ:** а) Следи из следећих израза a=a·1, 0=0·a и a=1·a и дефиниције1.1. .
б) Ако је a|b и b|c, тада постоје цели бројеви m и n такви да је b=m·a и c=n·b. Тада је, c=n·m·a, а како је mn цео број, следи да је a|c.
в) Ако је a|b, тада постоји ненегативан цео број m такав да је b=m·a. Како је b>0, тада су и a и m позитивни бројеви, тј. $1 \leq a$ и $1 \leq m$. Из чега следи да је $b=a\cdot m \geq a\cdot 1= a > 0$.
г) Ако је a|b и a|c, тада постоје цели бројеви m и n такви да је b=m·a и c=n·a. Дакле, b·x+c·y= m·a·x + n·a·y = a(m·x + n·y) . Kako је m·x + n·y цео број, то је a|(b·x+c·y).
д) Претпоставимо да је a|b и b|a. Ако је b=0, тада је и a=0. Ако је b>0 тада из б) следи a=b.
ђ) Ако је a|b, тада постоји ненегативан цео број m такав да је b=m·a. Ако дату једначину помножимо са c , c≠0 добијамо b·c=m·(a·c) тј. ac|bc.
е) Ако је ac|bc, тада постоји ненегативан цео број m такав да је b·c=m·(a·c). Ако дату једначину поделимо са c , c≠0 добијамо b=m·a тј. a|b. ■

**Последица 1.1.** а) Ако су a, b, c произвољни ненегативни цели бројеви такви да је a|b и a|c и $n \in \mathbb{N}\setminus\{0\}$, тада је a|(b+c), a|(b-c), a|b·c и $a|b^n$.
б) Ако су у једнакости $a_1 + a_2 + \cdots + a_n = b_1 + b_2 + \cdots + b_s$ сви сабирци изузев једног дељиви са c, тада је и тај један дељив са c.

У теорији бројева важну улогу има следећа теорема јединствености о дељењу са остатком.

**Теорема 1.2. (Алгоритам дељивости)** Нека су a и b ненегативни цели бројеви и $b\neq 0$ . Тада су једнозначно одређени ненегативни цели бројеви q и r, такви да је $a=bq+r$, $0 \leq r < b$ .

**Доказ:** Заиста, такав један начин представљања броја a добија се ако узмемо да је bq највећи садржилац броја b који није већи од a.
Претпоставимо да постоји још један начин за представљање броја a.
$a=bq_1+r_1$ , $0 \leq r_1 < b$ .
Тада је $0 = b(q-q_1) + r - r_1$ , одакле следи да је $b|( r - r_1 )$ .
Како је $| r - r_1 | < b$, следи да је $r - r_1 =0$, тј $r = r_1$. Како је $b\neq 0$, следи да је $q=q_1$. ■

Број q назива се **количник**, а број r **остатак** при дељењу a са b.
Алгоритам дељења се користи у класификацији бројева. На пример за b=2, ако је r =1 (a=2q+1) тада кажемо да је a **непаран број**, а ако је r =0 (a=2q), тада је a **паран број**. Слична класификација се успоставља за b=3,4,..

Позитиван цео број p већи од 1 је **прост** ако су му једини позитивни делитељи бројеви 1 и p. За позитиван цео број већи од 1 који није прост, кажемо да је **сложен**. Сваки сложен број n, има делитеље различите од 1 и n.

## 1.2. Највећи заједнички делилац

**Дефиниција 1.3.** Нека су a и b ненегативни цели бројеви такви да је бар један већи од 0. За број к кажемо да је заједнички делитељ бројева a и b, ако је k|a и k|b.

**Дефиниција 1.4.** Највећи позитиван цео број који је делитељ и од a и од b, назива се **највећи заједнички делитељ** бројева a и b. Означавамо га са НЗД(a,b).

На пример: НЗД(4,16)=4, НЗД(0,5)=5, НЗД(30,50)=10, НЗД(8,15)=1.

Да бисмо доказали да је d=НЗД(a,b), треба доказати тачност следећих тврђења:
1) d|a и d|b
2) Ако k|a и k|b, тада је k|d.

**Теорема 1.3.** Највећи заједнички делитељ два цела броја, од којих је бар један различит од 0, је јединствен.

**Доказ:** Ако је d=НЗД(a,b) и d'=НЗД(a,b), тада је d|d' и d'|d, ако применимо теорему 1.1. д) следи да је d=d' . ■

**Теорема 1.4.** Нека су a и b ненегативни цели бројеви, при чему је бар један различит од нуле. Тада је НЗД(a,b) једнак најмањем целом броју који се може изразити као линеарна функција од a и b, тј. НЗД(a,b) је најмањи позитиван цео број који се може написати у облику ax+by, где су x и y цели бројеви.

**Доказ:** Нека је S скуп свих позитивних целих бројева облика ax+by , где су x и y цели бројеви. S је непразан, јер садржи број $a^2 + b^2$. Зато у S постоји најмањи елемент $d=ax_1+by_1$ .
Ако је a=0 или b=0, тврђење важи.
Претпоставимо да је a≠0 и b≠0, и нека су q и r цели бројеви, такви да је

$$a = qd+r \quad , 0 \le r < d$$

Тада је

$$r = a-qd = a-q(ax_1+by_1) = a(1-q\cdot x_1) + b(-q\cdot y_1) .$$

Дакле, r је линеарна функција од a и b. Међутим, r није у скупу S, јер је $0 \le r < d$ , а d је најмањи број у S. Зато је r=0 и a=qd, тј. d|a.
На исти начин доказује се да је d|b
Претпоставимо да је и d' заједнички делитељ од a и b. Тада је $d'|(ax_1+by_1)$ по теореми 1.1. г) , тј. d'|d. Према томе d=НЗД(a,b). ■

Очигледно је НЗД(a,a)= НЗД(0,a) = a, за a>0. За разлиите позитивне бројеве a и b, алгоритам за одређивање њиховог највећег заједничког делитеља заснива се на алгоритму дељења. То је познати **Еуклидов алгоритам** који се састоји у следећем.
Нека су a и b позитивни цели бројеви, a>b.Тада према алгоритму дељења, једнозначно су одређени бројеви $q_1$ и $r_1$, $1\le i \le k+1$ , такви да је

$a= q_1b + r_1$ , $0 < r_1 < b$ ;
$b= q_2 r_1 + r_2$ , $0 < r_2 < r_1$ ;
…
$r_{k-2}= q_k r_{k-1} + r_k$ , $0 < r_k< r_{k-1}$ ;
$r_{k-1}= q_{k+1} r_k + 0$ $(r_{k+1}=0)$ .

Низ $r_1, r_2 , r_3 , ... , r_{к-1}, r_k$ је опадајући низ природних бројева мањих од b , што значи да се горе описани поступак мора завршити после коначног броја корака.

**Теорема 1.5.** НЗД(a,b) = $r_k$ , где је $r_k$ последњи позитиван остатак добијен применом Еуклидовог алгоритма на природне бројеве a и b , a > b .

**Доказ:** Докажимо да важе следећа два тврђења:
1) $r_k|a$ и $r_k|b$
2) ако је d|a и d|b, тада је $d| r_k$ .

Из Еуклидовог алгоритма добијамо да је $r_k|r_{k-1}$ . На основу тога и последње једнакости, закључујемо да је $r_k|r_{k-2}$ . Настављајући тај поступак добија се да је $r_k|r_{k-3}$ , $r_k|r_{k-4}$, ... , $r_k|b$ , а онда из прве једнакости следи да је $r_k|a$ . Дакле услов 1) је задовољен.
Нека је d природан број такав да је d|a и d|b . Тада из прве једнакости Еуклидовог алгоритма добијамо да је $d|r_1$ , из друге да је $d|r_2$ , ... , и коначно из претпоследње да је $d| r_k$ . Тиме је доказано да важи 2). Дакле, $r_k$= НЗД(a,b) . ■

**Пример 1.1.** По Еулидовом алгоритму одредити НЗД(2541,588) .

$$2541 = 4\cdot 588 + 189$$
$$588 = 3\cdot 189 + 21$$
$$189 = 21\bullet 9$$

Дакле, НЗД(2541,588) = 21 . ◊

Претходни поступак можемо извести и користећи матрице. Уочимо матрицу

$$\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

где су a и b бројеви чији највећи заједнички делилац тражимо. Ову матрицу можемо трансформисати користећи следеће операције:
1. множење врсте целим бројем и додавање другој врсти;
2. множење врсте са -1;
3. замена места врстама.

На тај начин полазну матрицу можемо свести на облик

$$\begin{bmatrix} d & x & y \\ 0 & x' & y' \end{bmatrix}$$

где је d = НЗД(a,b), цели бројеви x и y су такви да ax+by = d, док нам x',y'$\in Z$ нису битни.

На пример, нека су a = 2541 и b = 588. Тада је

$$\begin{bmatrix} 2541 & 1 & 0 \\ 588 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 189 & 1 & -4 \\ 588 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 189 & 1 & -4 \\ 21 & -3 & 13 \end{bmatrix} \sim \begin{bmatrix} 0 & -26 & 113 \\ 21 & -3 & 13 \end{bmatrix} \sim \begin{bmatrix} 21 & -3 & 13 \\ 0 & -26 & 113 \end{bmatrix}$$

одакле видимо да је НЗД(2541,588) = 21 и 21 = (-3)·2541 + 13 ·588.

**Дефиниција 1.5.** Нека су $a_1, a_2, \dots, a_n$ ненегативни цели бројеви, при чему је бар један различит од 0. Највећи позитиван цео број d, који је делитељ свих тих бројева се назива највећи заједнички делитељ за бројеве $a_1, a_2, \dots, a_n$, и обележавамо га са d= НЗД($a_1, a_2, \dots, a_n$).

На пример НЗД(21, 12, 30) = 3.

Да бисмо доказали да је d =НЗД($a_1, a_2, \dots, a_n$) довољно је да докажемо:
1) $d|a_i$ за i=1,2, ... , n ;
2) ако је r|a за i=1,2, ... , n , тада је r|d.

**Теорема 1.6.** Ако су $a_1, a_2, \dots, a_n$ позитивни цели бројеви, n ≥ 3, тада је НЗД($a_1, a_2, \dots, a_n$) = НЗД(НЗД($a_1, a_2, \dots, a_{n-1}$), $a_n$) .

**Доказ:** Нека је d =НЗД($a_1, a_2, \dots, a_n$) и d'= НЗД(НЗД($a_1, a_2, \dots, a_{n-1}$), $a_n$) . Како је $d|a_i$ , за i=1,2, ... , n , добијамо да је d| НЗД($a_1, a_2, \dots, a_{n-1}$) и $d|a_n$ . Дакле, d|d' . Слично, из d'| НЗД($a_1, a_2, \dots, a_{n-1}$) и $d'|a_n$ следи $d'|a_i$ , за i=1,2, ... , n , па добијамо да је d'|d. Према томе, по теореми 1.1. д) следи d = d' . ■

На основу теореме 1.6. закључујемо да се вишеструком применом Еуклидовог алгоритма може добити највећи заједнички делитељ више целих бројева.

**Дефиниција 1.6.** Целе бројеве a и b, од којих је бар један различит од нуле, називамо **узајамно простим** ако је НЗД (a,b)=1.

На пример бројеви 11 и 13, 14 и 25, ... су узајамно прости.

**Дефиниција 1.7.** Нека су $a_1, a_2, \dots, a_n$ цели бројеви, при чему је бар један различит од нуле. Ако је НЗД($a_i$ , $a_j$)=1, за $1 \le i < j \le n$ , тада су бројеви $a_1, a_2, \dots, a_n$

**по паровима узајамно прости**. Ако је НЗД($a_1$, $a_2$, ... , $a_n$)=1 тада су бројеви $a_1$, $a_2$, ... , $a_n$ **узајамно прости.**

**Пример 1.2.** Бројеви 6, 10 и 15 су узајамно прости, а нису по паровима узајамно прости. Бројеви 18, 25, 77 су по паровима узајамно прости. ◊

**Дефиниција 1.8.** Најмањи позитиван број m који је заједнички садржалац бројева a и b назива се **најмањи заједнички садржалац** бројева a и b и обележавамо га са НЗС(a,b) .

Јасно је да је НЗС(a,b)= НЗС(-a,b)= НЗС(a,-b)= НЗС(-a,-b) .
Прецизније , m= НЗС(a,b) ако важи:
1) a|m и b|m
2) ако је a|к и b|к , тада је m|к .

Слично као за највећи заједнички делитељ дефинише се најмањи заједнички садржалац бројева $a_1$, $a_2$, ... , $a_n$ у ознаци НЗС($a_1$, $a_2$, ... , $a_n$) као најмањи позитиван број који је садржалац сваког од бројева $a_1$, $a_2$, ... , $a_n$.

## 1.3. Основна теорема аритметике

У овом делу доказаћемо да се сваки цео број може представити у облику производа простих фактора и да је такво представљање јединствено до на поредак фактора.

**Теорема 1.7.** Ако је n цео број већи од један, онда је n производ простих фактора.

**Доказ:** Ако је n прост број тврђење очигледно важи.
Претпоставимо да тврђење важи за сваки сложени број мањи од n. Ако је n сложен број тада постоји цео број d такав да је 1<d<n и d|n. Означимо са m најмањи такав број. Број m не може бити сложен јер би у том случају постојао цео број k такав да је 1<k<m и k|m, што повлачи да је k|n. То је међутим у контрадикцији са претпоставком да је m најмањи цео број већи од један који је делитељ од n. Дакле, m је прост број. Обележимо га са $p_1$. Следи да је $n=p_1 \cdot n_1$ , где је $1< n_1 < n$. По индукцијској претпоставци број $n_1$ се може представити у облику простих фактора, према томе, онда може и n . ■

Групишући једнаке просте факторе броја n, закључујемо да се сваки цео број већи од један може представити у облику

$$n = \prod_{i=1}^{k} {p_i}^{\alpha_i} \quad , \qquad (1)$$

где је $p_1< p_2 < \ldots < p_k$ и $\alpha_i > 0$, за i=1,2, … , k.

**Дефиниција 1.9.** Представљање броја n у облику (1) називамо **канонски облик** броја n.

**Теорема 1.8. (Основна теорема алгебре)** Сваки цео број већи од један има јединствен канонски облик.

**Доказ:** Канонско представљање постоји на основу теореме 1.7. Преостаје да докажемо да је то представљање јединствено.

Претпоставимо да постоји позитиван сложен број већи од један који се може на два различита начина представити у канонском облику. Нека је n најмањи такав број са представљањима

$$n= p_1p_2 \dots p_k = q_1q_2 \dots q_m .$$

Не постоји прост број p који се појављује у обе канонске репрезентације броја n, јер би у том случају и број $n' = \frac{n}{p}$ , који је мањи од n, имао две различите канонске репрезентације, што је у контрадикцији са претпоставком о минималности броја n.

Можемо да претпоставимо да је $p_1 \leq p_2 \leq \dots \leq p_k$ , $q_1 \leq q_2 \leq \dots \leq q_m$ .

За просте факторе $p_1$ и $q_1$ важи $p_1 \neq q_1$ , па можемо узети $p_1 < q_1$ . Нека је $N= p_1q_2 \dots q_m$ . Како је $p_1|N$ и $p_1|n$ , следи да је $p_1|(n-N)$ , где је $n-N=(q_1- p_1)q_2 \dots q_m > 1$ . Следи да се број n-N може написати у облику

$$n-N= p_1t_1 \dots t_h ,$$

где су $t_i$ прости бројеви за i=1,2, ... ,h . Са друге стране, ако је $q_1- p_1>1$ , онда се $q_1- p_1$ може написати као производ простих фактора, на пример $q_1 - p_1= r_1r_2 \dots r_s$ , па добијамо, на други начин, у облику производа простих фактора:

$$n-N= r_1r_2 \dots r_sq_2 \dots q_m .$$

Ова последња факторизација не садржи прост фактор $p_1$. Знамо да је $p_1 \neq q_i$ , за i=1,2,..., m; са друге стране $p_1 \neq r_j$ за j=1,2,..., s, јер $p_1$ није делитељ од $q_1- p_1$ . Дакле , број n-N има две различите факторизације, јер само једна од њих садржи прост фактор $p_1$. То важи и у случају када је $q_1 - p_1=1$ . Међутим, $1 < n-N < n$ што је у контрадикцији са претпоставком о минималности броја n да не постоји цео број већи од један, који се може представити на два начина у канонском облику. ■

**Теорема 1.9.** Нека су бројеви m и n дати у канонском облику

$$m = \prod_{i=1}^{k} p_i^{\alpha_i} \qquad , \qquad n = \prod_{i=1}^{k} p_i^{\beta_i}$$

Тада m|n ако и само ако је $0 \leq \alpha_i \leq \beta_i$ за i=1,2,..., k .

**Доказ:** Следи на основу тога што је n= md где је

$$d = \prod_{i=1}^{k} p_i^{\delta_i}$$

при чему је $\delta_i= \beta_i-\alpha_i$ . ■

**Последица 1.9.** Ако је

$$m = \prod_{i=1}^{k} p_i^{\alpha_i} \qquad , \qquad n = \prod_{i=1}^{k} p_i^{\beta_i} \quad .$$

Тада је

$$\text{НЗД}(m,n) = \prod_{i=1}^{k} p_i^{\min(\alpha_i-\beta_i)} \qquad , \qquad \text{НЗС}(m,n) = \prod_{i=1}^{k} p_i^{\max(\alpha_i-\beta_i)} \quad .$$

# 2. Модуларна аритметика

## 2.1. Дефиниција релације конгруенције

Конгруенција по модулу $m$, $m \in N$, $m \geq 2$ , целих бројева може да се дефинише на следећи начин.

**Дефиниција 2.1.** Нека је m природни број већи од 1. Кажемо да су бројеви a, b ∈ Z **конгруентни по модулу m** и пишемо $\mathbf{a \equiv b \pmod m}$ или $\mathbf{a \equiv_m b}$ ако је m|(a-b) .

Према дефиницији1.1. релација $a \equiv b \pmod m$ означава да m|(a-b), што значи да постоји цео број t такав да је a-b=mt, односно a = b+ mt.
На основу претходног излагања, релацију конгруенције можемо дефинисати на следећи начин:

**Дефиниција 2.2.** Број a је конгруентан броју b по модулу m ако постоји цео број t такав да је a = b + mt , t = 0, ± 1, ± 2, … .

**Теорема 2.1.** Бројеви a и b имају исте остатке при дељењу са m ако и само ако је $a \equiv b \pmod m$ .

**Доказ:** Ако је a ≡ b (mod m), тада постоји цео број t такав да је a = b + mt. За b и m ≠ 0 постоје једнозначно одређени цели бројеви q и r такви да је b = mq + r, 0 ≤ r < |m|, где је r остатак добијен при дељењу b са m. Одавде следи да је a = m (t + q) + r, 0 ≤ r <|m|.
Дакле и број a има исти остатак при дељењу са m.
Обратно, нека су a и b бројеви који при дељењу са m имају исте остатке. Тада се може записати да је $a = mq_1 + r$ и $b = mq_2 + r$ при чему је 0 ≤ r < |m|. Одавде следи да је $a - b = m (q_1 - q_2)$, па је a ≡ b (mod m). ■

С обзиром на доказану теорему релацију конгруенције можемо дефинисати на следећи начин:
Број a је конгруентан броју b по модулу m ако бројеви a и b имају исте остатке при дељењу са m (m ≠ 0)

## 2.2. Особине релације конгруенције

**Теорема 2.2.** Релација конгруенције по модулу је релација еквиваленције.

**Доказ:** Релација конгруенције је рефлексивна јер за цео број a важи a ≡ a (mod m) јер m|(a-a) тј. m|0.
Релација конгруенције је симетрична јер ако a ≡ b (mod m) тада је m|(a-b). А одатле је и m|-(a-b) тј. m|(b-a) одакле следи да је b ≡ a (mod m).
Ако је a ≡ b (mod m) и b ≡ c (mod m) тада постоје бројеви p и q такви да је a=b+ mp и b=c+ mq. Ако саберемо ове две једнакости добијамо a-c= m·(p+q) тј. a ≡ c (mod m).
На основу овога закључујемо да је релација конгруенције транзитивна. ■

**Теорема 2.3.** Нека су a,b,c,d и m≠0 цели бројеви. Ако је $a \equiv b \pmod m$ и $c \equiv d \pmod m$ тада је $a+c \equiv b+d \pmod m$ и $a-c \equiv b-d \pmod m$.

**Доказ:** Према дефиницији релације конгруенције постоје цели бројеви u и v такви да је $a=b+mu$ и $c=d+mv$. Сабирањем, односно одузимањем, претходне две једначине добијамо:

$$a+c \equiv b+d+m\cdot(u+v) \text{ и } a-c \equiv b-d+m\cdot(u-v)$$

а то је

$$a+c \equiv b+d \pmod m \text{ и } a-c \equiv b-d \pmod m \quad . \blacksquare$$

Претходно тврђење може да се уопшти.

**Теорема 2.4.** Ако су $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$ и $m \neq 0$ цели бројеви тада из релације $a_1 \equiv b_1, a_2 \equiv b_2, \dots, a_n \equiv b_n \pmod m$ следи

$$a_1+a_2+\dots+a_n \equiv b_1+b_2+\dots+b_n \pmod m \quad .$$

**Доказ:** У доказу ове теореме користићемо теорему 2.3. и принцип математичке индукције. Тврђење је тачно за n=2 јер на основу претходне теореме и релације $a_1 \equiv b_1$ и $a_2 \equiv b_2$ следи $a_1+a_2 \equiv b_1+b_2 \pmod m$ .
Нека је тврђење тачно за n-1, докажимо да важи и за n.
Пошто је тврђење тачно за n-1 следи да из $a_1 \equiv b_1, a_2 \equiv b_2, \dots, a_{n-1} \equiv b_{n-1} \pmod m$ следи $a_1+a_2+\dots+a_{n-1} \equiv b_1+b_2+\dots+b_{n-1} \pmod m$ .
Ако је поред тога $a_n \equiv b_n \pmod m$ из претходне две релације, на основу теореме 2.3. , следи да је $a_1+a_2+\dots+a_n \equiv b_1+b_2+\dots+b_n \pmod m$ . ■

**Теорема 2.5.** Ако су a,b,c и m≠0 цели бројеви, тада из релације $a \equiv b \pmod m$ следи $ac \equiv bc \pmod m$, а такође и $ac \equiv bc \pmod{mc}$ .

**Доказ:** Из релације $a \equiv b \pmod m$ следи да је $m \mid a-b$ . Одавде произилази да $m \mid (a-b)\cdot c$ тј. $m \mid ac-bc$ , а то је $ac \equiv bc \pmod m$ што је и требало доказати.
Из $m \mid a-b$ такође је $mc \mid ac-bc$ , а одатле $ac \equiv bc \pmod{mc}$ . ■

**Последица 2.5.** Ако је $a \equiv b \pmod m$ тада је $-a \equiv -b \pmod m$ .

**Теорема 2.6.** За целе бројеве a,b,c,d и m≠0 из релације $a \equiv b \pmod m$ и $c \equiv d \pmod m$ следи $a\cdot c \equiv b\cdot d \pmod m$ .

**Доказ:** На основу претходне теореме важи $a\cdot c \equiv b\cdot c \pmod m$ и $b\cdot c \equiv b\cdot d \pmod m$ , а одавде због транзитивности релације конгруенције добијамо $a\cdot c \equiv b\cdot d \pmod m$ . ■

И ово тврђење се може уопштити.

Ако су $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$ и $m \neq 0$ цели бројеви тада из релације $a_1 \equiv b_1, a_2 \equiv b_2, \dots, a_n \equiv b_n \pmod m$ следи

$$a_1\cdot a_2\cdot \dots \cdot a_n \equiv b_1\cdot b_2\cdot \dots \cdot b_n \pmod m \quad .$$

Тврђење се такође доказује математичком индукцијом и теоремом 2.6.

Као непосредну последицу овог тврђења добија се да из $a \equiv b \pmod m$ следи

$$a^n \equiv b^n \pmod m \quad ,$$

где је n природан број. Последња релација важи и за n=0 , јер је $1 \equiv 1 \pmod m$ .

**Пример 2.1.** Користећи претходно тврђење одредити остатак који се добија дељењем броја $3^{100}$ бројем 13.

Како је 3≡3 (mod 13) добија се $3^3 \equiv 27 \pmod{13}$.
Како је 27≡1 (mod 13) такође је $3^3 \equiv 1 \pmod{13}$
Одавде је $(3^3)^{33} \cdot 3 \equiv 1 \cdot 3 \pmod{13}$ тј. $3^{100} \equiv 3 \pmod{13}$ .
Пошто је $0 \leq 3 < 13$ закључујемо да је 3 остатак при дељењу броја $3^{100}$ бројем 13 . ◊

**Теорема 2.7.** Ако је $f(x)= c_0x^n + c_1x^{n-1}+ \dots + c_n$ полином са целим коефицијентима $c_i$ , i=1,2,…,n , тада из релације $a \equiv b \pmod{m}$ следи $f(a) \equiv f(b) \pmod{m}$ .

**Доказ:** Из $a \equiv b \pmod{m}$ следи $a^i \equiv b^i \pmod{m}$ и $c_ia^i \equiv c_ib^i \pmod{m}$ , i=1,2,…,n . Такође према теореми 2.4. следи $c_0a^n + c_1a^{n-1}+ \dots + c_n \equiv c_0b^n + c_1b^{n-1}+ \dots + c_n \pmod{m}$, тј. $f(a) \equiv f(b) \pmod{m}$ . ■

**Теорема 2.8.** Ако је $a \equiv b \pmod{m}$ и d|m тада је $a \equiv b \pmod{d}$ .

**Доказ:** Ако је $a \equiv b \pmod{m}$ тада је m|(a-b). Kako d|m из претходне релације следи да је d|(a-b) тј. $a \equiv b \pmod{d}$ . ■

**Теорема 2.9.** Ако је $a \equiv b \pmod{m}$ и ако c|a и c|b , тада је

$$\frac{a}{c} \equiv \frac{b}{c} \quad \left(mod\ \frac{m}{d}\right)$$

где је d=НЗД(c,m) .

**Доказ:** Из релације $a \equiv b \pmod{m}$ следи m|(a-b) , а исто тако и

$$\frac{m}{d} \mid \frac{c}{d} \cdot \frac{a-b}{c} \qquad (2)$$

Међутим, због d=НЗД(c,m) тада је $НЗД\left(\frac{c}{d}, \frac{m}{d}\right) = 1$ , Према томе из релације (2) следи да $\frac{m}{d} \mid \frac{a-b}{c}$ тј. $\frac{a}{c} \equiv \frac{b}{c} \quad \left(mod\ \frac{m}{d}\right)$ . ■

Ако је НЗД(c,m) =1, тада из $a \equiv b \pmod{m}$ следи $\frac{a}{c} \equiv \frac{b}{c} \quad (mod\ m)$ .
Прецизније речено ако је НЗД(c,m) =1 тада се из $c \cdot a \equiv c \cdot b \pmod{m}$ добија $a \equiv b \pmod{m}$ .
У случају да c|m тада је НЗД(c,m) =c па је . $\frac{a}{c} \equiv \frac{b}{c} \quad \left(mod\ \frac{m}{c}\right)$ .
Из претходног се види да "скраћивање" код конгруенција не може увек да се изведе.

**Пример 2.2**. Из релације $42 \equiv 84 \pmod{6}$ "скраћивањем" са 7 добија се $6 \equiv 12 \pmod{6}$ што је тачно. Међутим, ако би се извршило "скраћивање" са 14, добија се резултат $3 \equiv 6 \pmod{6}$ што је нетачно. Ово је последица чињенице да је НЗД(14,6)=2, па је тачно да је $3 \equiv 6 \pmod{3}$ . ◊

**Теорема 2.10.** Ако је : $a \equiv b \pmod{m_1}$ , $a \equiv b \pmod{m_2}$ , ... , $a \equiv b \pmod{m_к}$ тада је $a \equiv b \pmod{M}$ где је $M= НЗС(m_1, m_2, \dots , m_к)$ .

**Доказ:** Из услова теореме следи $m_1|(a-b)$ , $m_2|(a-b)$ , ... , $m_к|(a-b)$ , а одатле $НЗС(m_1, m_2, \dots , m_к) |(a-b)$ тј. $a \equiv b \pmod{M}$ што је и требало доказати. ■

## 2.3. Класе остатака по датом модулу

**Дефиниција 2.3.** Скуп свих бројева конгруентних броју a по модулу $m \neq 0$ назива се **класа по модулу m**. Ову класу обележаваћемо са $[a]_m$ .

**Теорема 2.11.** Класа $[a]_m$ представља скуп бројева $x = a + mt$, ($t = 0, \pm 1, \pm 2, \ldots$).

Ова чињеница се може изразити и овако:

$$[a]_m = \{\ldots, a - 2t, a - t, a, a + t, a + 2t, \ldots\}.$$

Како је релација конгруенције по модулу m релација еквиваленције, $[a]_m$ представља класу еквиваленције, коју називамо **класа конгруенције по модулу m**.

**Теорема 2.12.** Класе $[a]_m = [b]_m$ ако и само ако је $a \equiv b \pmod m$.

За свако $x \epsilon [a]_m$ важи да је $x \equiv a \pmod m$, а тада је $[x]_m = [a]_m$.

**Теорема 2.13.** Класе $[a]_m$ и $[b]_m$ су или једнаке или дисјунктне.
Увек важи или $a \equiv b \pmod m$ или $a \not\equiv b \pmod m$.

**Теорема 2.14.** Два цела броја имају исти остатак при дељењу са m, ако и само ако припадају истој класи по модулу m.

**Доказ:** Према теореми 2.1 два цела броја a и b имају исте остатке при дељењу са m ако и само ако је $a \equiv b \pmod m$. Међутим, ова релација важи ако и само ако a и b припадају истој класи конгруенције по модулу m. Дакле бројеви a и b имају исте остатке при дељењу са m ако и само ако припадају истој класи. ■

**Теорема 2.15.** Остатак r, добијен дељењем a са m, је најмањи ненегативан број класе $[a]_m$ .

**Доказ:** Како је r остатак добијен дељењем a са m, то је $a \equiv r \pmod m$, одакле следи да је $r \epsilon [a]_m$ тј. $[r]_m = [a]_m$.

Дакле, елементи дате класе су у облику $x = r + mt$, $t = 0, \pm 1, \pm 2, \ldots$
Како је $m > 0$, следи x расте са t. Како је $0 \leq r < m$, лако се уочава да се најмања ненегативна вредност од x добија за $t = 0$, тј. најмањи ненегативан елемент ове класе је r. ■

**Теорема 2.16.** Релација конгруенције по модулу m дели скуп целих бројева на m дисјунктних класа по модулу m.

**Доказ:** Пошто је релација конгруенције по модулу m релација еквиваленције, скуп целих бројева је њом подељен на известан број дисјунктних класа. Како остатака при дељењу неког целог броја са m има тачно m, следи да је број класа тачно m: $[0]_m, [1]_m, \ldots, [m-1]_m$. ■

$$Z = \bigcup_{a=0}^{m-1} [a]_m$$

Ако је m = 1, тада постоји само једна класа конгруенције по модулу m, а то је скуп свих целих бројева.

Ако је m = 3, тада постоји три класа конгруенције по модулу m, и оне су :

$[0]_3 = \{\dots, -6, -3, 0, 3, 6, \dots\}$, $[1]_3 = \{\dots, -5, -2, 1, 4, 7, \dots\}$ $[2]_3 = \{\dots, -4, -1, 2, 5, 8, \dots\}$.

## 2.4. Модуларна аритметика

Теорема 2.3. и теорема 2.6. сугеришу начин на који ће бити погодно дефинисати аритметичке операције на количничком скупу $Z/\equiv_m$ :

- $[a]_m + [b]_m = [a+b]_m$
- $[a]_m - [b]_m = [a-b]_m$
- $[a]_m \cdot [b]_m = [a \bullet b]_m$

Дакле, за класе $[a]_m$ и $[b]_m$ збир је класа чији представник је остатак при дељењу a + b са m. Теорема 2.3. и теорема 2.6. гарантују да збир класа еквиваленције $([a]_m + [b]_m)$ не зависи од њихових представника, а слично је и у преостала два случаја, тако да су операције коректно дефнисане.

**Пример 2.3.** Нека је m=4 , тада је $Z/\equiv_4 = \{[0]. [1], [2], [3]\}$ . Према претходном је $[3] + [2] = [5]$ и како је $5 \equiv_4 1$ то је $[3] + [2] = [1]$. Слично, пошто је $[3] \cdot [2] = [6]$ и $6 \equiv_4 2$, онда је $[3] \cdot [2] = [2]$ . ◊

Имајући у виду све претходно речено, на даље ћемо скуп $Z/\equiv_m$ поистоветити са скупом $Z_m=\{0,1, \dots, m-1\}$. Није тешко проверити да је алгебарска структура $\langle Z_m, +, \cdot, -, 0, 1\rangle$ комутативни прстен са јединицом.

Ако m није прост број, јасно је да увек постоје природни бројеви x и y такви да важи :

1. $1 < x < m$ , $1 < y < m$
2. $x \cdot y = m$ , односно $x \cdot y \equiv_m 0$.

Дакле ако m није прост број, $Z_m$ има делиоце нуле. Тада $\langle Z_m, +, \cdot, -, 0, 1\rangle$ неће бити поље, јер претпоставка да уочени елемент x има инверз $x^{-1}$ доводи до следећег:

$x \cdot y \equiv_m 0$

$x^{-1} \cdot (x \cdot y) \equiv_m x^{-1} \cdot 0$

$(x^{-1} \cdot x) \cdot y \equiv_m 0$, због асоцијативности , па је супротно претпоставци

$1 \cdot y \equiv_m 0$ , односно $y \equiv_m 0$ .

Међутим ако је број, односно модул, m у односу на који се дефинише конгруенција прост број , претходно разматрање не пролази и $\langle Z_m, +, \cdot, -, 0, 1\rangle$ јесте поље. У доказивању овог тврђења користи се такозвана Мала Фермаова теорема.

**Теорема 2.17. (Мала Фермаова теорема)** Ако је p прост број и a природан број онда p дели $a^p$-a односно $\mathbf{a^p - a = к \cdot p}$ , за неки цео број к.

Приметимо да се теорема 2.17. може формулисати и на следећи начин за $0 < a < p$:

$$a^{p-1} - 1 = к \cdot p \quad \Rightarrow$$
$$a^{p-1} \equiv_p 1 \quad \Rightarrow$$
$$a \cdot a^{p-2} \equiv_p 1 \quad .$$

Према томе, за прост број p и произвољан природни број a, такав да је $0 < a < p$, $\mathbf{a^{-1} \equiv_p a^{p-2}}$ је инверз од a у $\langle Z_p, +, \cdot, -, 0, 1\rangle$, па је ова структура поље.

**Пример 2.4.** Инверзни елементи за 2, 3 и 4 у $Z_5$ су редом :

$$\mathbf{2^{-1} \equiv_5 3\ ,\ 3^{-1} \equiv_5 2 \ \text{ и } \ 4^{-1} \equiv_5 4\ ,}$$

јер је $2^{5-2} = 2^3 = 8$ и $8 \equiv_5 3$, $3^{5-2} = 3^3 = 27$ и $27 \equiv_5 2$ и $4^{5-2} = 4^3 = 64$ и $64 \equiv_5 4$. ◊

**Пример 2.5.** Следећим табелама

| $+_2$ | **0** | **1** |
|---|---|---|
| **0** | 0 | 1 |
| **1** | 1 | 0 |

| $\bullet_2$ | **0** | **1** |
|---|---|---|
| **0** | 0 | 0 |
| **1** | 0 | 1 |

дефинисане су операције $+_2$ и $\bullet_2$ у пољу $\langle Z_2, +_2, \cdot_2, -_2, 0, 1\rangle$.

За одузимање у овом пољу се лако види да је $x +_2 y = x -_2 y$.

Ако је y = 0, ово важи тривијално. Ако је y = 1, за x = 1 је очигледно $1 +_2 1 = 0 = 1 -_2 1$. Ако је x = 0, онда је $1 +_2 0 = 1$, док је 0 - 1 = -1 (као операција над целим бројевима), а пошто је $-1 \in [1]_2$, то је и $0 -_2 1 = 1$.

У овом случају је лако одредити и резултат дељења: дељење са 0 није дефнисано, док дељење са 1 не мења дељеник. ◊

Последица теореме 2.17. је да можемо одредити инверзе не-нултих елемената поља $Z_p$. Међутим, у општем случају и за разлику од примера 2.5. овај поступак, као и израчунавање резултата дељења, нису тривијални. Најпре, израчунавање p-2 степена броја може бити захтевно. Такође, иако је јасно да за $y \neq 0$ важи $\frac{x}{y} = z$ ако и само ако је $z \cdot y = x$ и да претрагом кроз скуп $Z_p$ увек можемо одредити z, у случајевима када је p велико овакав поступак није ефкасан. Показује се да се проблем дељења своди на проблем налажења инверза:

Нека се тражи вредност $z \equiv_p \frac{x}{y}$. Ако можемо наћи d такав да је $y \cdot d \equiv_p 1$, тј. $d = y^{-1}$, тада је $\frac{1}{y} \equiv_p d$ и $z \equiv_p \frac{x}{y} \equiv_p x \cdot \frac{1}{y} \equiv_p x \cdot d$.

Под посебним условима можемо да искорисимо Еуклидов алгоритам за израчунавање највећег заједничког делиоца у налажењу инверза . Он важи само када је p узајамно прост са y, где је p прост број и y природан број $0 < y < p$.

Како су p и y узајамно прости то је НЗД(p, y)=1 и према Еуклидовом алгоритму за израчунавање највећег заједничког делиоца постоје цели бројеви u и v такви да је $u \cdot y + v \cdot p = 1$ . Другим речима добија се u тако да је $u \cdot y \equiv_p 1$. Коначно, пошто не мора да буде u < p, инверз елемента y је $y^{-1} \equiv_p u$ .

**Пример 2.6.** Нека је p= 234527. Израчунати $2^{-1}$ у $Z_p$.

$$234527 = 117263 \cdot 2 + 1$$
$$-117263 \cdot 2 + 1 \cdot 234527 = 1$$
$$-117263 \equiv_{234527} 117264 .$$
$$\mathbf{2^{-1} \equiv_{234527} 117264.} \qquad ◊$$

Проста аналогија за дељење, какву смо применили на сабирање, одузимање и множење, на скуп $Z_m$ није могућа. То је последица чињенице да не важи, у општем случају, еквиваленција: $a \neq 0$ и $b \neq 0 \Rightarrow a \cdot b \neq 0$ .

Ако погледамо у табелу за множење у $Z_6$

| $\bullet_6$ | **0** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|
| **0** | 0 | 0 | 0 | 0 | 0 | 0 |
| **1** | 0 | 1 | 2 | 3 | 4 | 5 |
| **2** | 0 | 2 | 4 | 0 | 2 | 4 |
| **3** | 0 | 3 | 0 | 3 | 0 | 3 |
| **4** | 0 | 4 | 2 | 0 | 4 | 2 |
| **5** | 0 | 5 | 4 | 3 | 2 | 1 |

видимо да је 2·3=0 , 3·2=0, 3·4=0 и 4·3=0 , док су 2,3,4≠0 .

Због тога се дељење броја b бројем a, по модулу m, уводи на природан начин преко множења. Наиме, количник бројева b и a у $Z_m$ је цео број x који задовољава једначину $\boldsymbol{ax \equiv b \pmod m}$.

Питамо се под којим условима постоји решење једначине $ax \equiv b \,(mod\, m)$ и колико их има.

Постоји решење једначине $ax \equiv b \,(mod\, m)$ акко m|(ax-b) ; за неко x
акко ax-b=m· (-y); за неко x и y
акко једначина ax+my=b има решење
акко НЗД(a,m) | b.

Нека је d= НЗД(a,m) . Ако је d | b, одредимо решење ове једначине.
Нека је $(x_0, y_0)$ решење једначине ax+my= d одређено помоћу Еуклидовог алгоритма. Тада је $x_1 = x_0 \cdot \frac{b}{d}$ једно решење полазне једначине $ax \equiv b \,(mod\, m)$.
Ако је d = 1, онда су сва решења облика $x_1 + mt$, за $t \in Z$.
Нека је d > 1. Докажимо да је x решење једначине $ax \equiv b \,(mod\, m)$ ако и само ако је решење једначине $a'x \equiv b' \,(mod\, m')$ , где су $a'=\frac{a}{d}$ , $b'=\frac{b}{d}$ и $m'=\frac{m}{d}$ .
Важи :
Ако је $ax \equiv b \,(mod\, m)$ онда m|(ax-b)
=> ax-b=m· (-y); за неко y
=> ax+my=b
=> ax+my=b /:d
=> $a'x+m'y=b'$
=> $a'x \equiv b' \pmod{m'}$ .
С друге стране
Ако је $a'x \equiv b' \,(mod\, m')$ онда $m'|(a'x-b')$
=> $a'x-b'=m' \cdot (-y)$; за неко y
=> $a'x+m'y=b'$
=> $a'x+m'y=b'$ /·d
=> ax+my=b
=> $ax \equiv b \pmod m$ .

Нека је $x_0$ најмањи позитиван број који је решење једначине $a'x \equiv b' \,(mod\, m')$.

Тада су: $x_0$, $x_0 + m'$, $x_0 + 2m'$, … , $x_0 + (d-1)m'$
различита решења једначине $ax \equiv b \ (mod\ m)$ , јер је m=m'·d .Како је НЗД(a′,b′)=1, према претходном делу сва решења једначине $ax \equiv b \ (mod\ m)$ су $x_0 + m't$ , за $t \in Z$.
Дакле **сва решења једначине $ax \equiv b \ (mod\ m)$** су $\mathbf{y_i = x_0 + im'}$ , за i∈{0,1, … , d-1}. Приметимо да их има d. Дакле, **опште решење** дате једначине је $\mathbf{y_i + mt}$ ,
за i∈{0,1, … , d-1} и $t \in Z$.

**Пример 2.7.** Испитати да ли следеће једначине имају решење и ако имају одредити га :

1. $4x \equiv_{14} 9$
2. $7x \equiv_{9} 1$
3. $8x \equiv_{28} 12$

1. Како је НЗД(4,14)=2 и 2∤9 , једначина нема решења.
2. Како је НЗД(7,9)=1 и 1|1, једначина има решења. Можемо закључити да је 4 једино решење једначине и без коришћења Еуклидовог алгоритма тако што ћемо заменити бројеве од 1 до 8 у једначину. Тако да је опште решење једначине 4+9t, за $t \in Z$.
3. Једначина има решење јер је НЗД(8,28)=4 и 4|12. Према претходном треба одредити решење једначине $2x \equiv_7 3$. Сва решења једначине су бројеви 5,12,19 и 24. ◊

**Теорема 2.18.(Вилсонова теорема)** Ако је p прост број тада је

$$(p-1)! \equiv -1 \ (mod\ m).$$

Важи и обрат Вилсонове теореме: Ако за неки природан број p>1 важи да $(p-1)! \equiv -1 \ (mod\ m)$ онда је p прост број.
Ово важи јер p|(p-1)!+1 па постоји к $\in Z$ тако да је pk=(p-1)!+1, тј. pk+ (-1)(p-1)!=1 .
Тада НЗД(p, (p-1)!) |1 , ра је НЗД(p, 1·2·...·p-1)=1 . Видимо да је за свако
i∈{0,1, … , p-1} број НЗД(i,p)=1, па је p прост.

**Теорема 2.19.(Кинеска теорема о остацима)** Систем конгруенција

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\dots$$
$$x \equiv a_k \pmod{m_k}$$

има решење ако НЗД($m_i$, $m_j$) | ($a_i$-$a_j$) за све i≠j. Ако је x′ неко решење тог система, онда је опште решење облика x=x′ + НЗС($m_1$, $m_2$,… , $m_k$)· t , где је $t \in Z$.

**Доказ:** Користићемо индукцију по броју конгруенција к. Ако је к=1 имамо једну конгруенцију $x \equiv a_1 \pmod{m_1}$. Решења су $x=a_1+mt$, за свако $t \in Z$ .
Претпоставимо да је тврђење тачно за к конгруенција . Докажимо да важи за к+1.
Нека је дат систем конгруенција

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\dots$$
$$x \equiv a_k \pmod{m_k}$$
$$x \equiv a_{k+1} \pmod{m_{k+1}}$$

тако да важи услов НЗД($m_i$, $m_j$) | ($a_i$-$a_j$) за све i≠j. Према индуктивној хипотези, првих к конгруенција има решење и опште решење је облика
$x=x_0$ + НЗС($m_1$, $m_2$,…, $m_k$)· $y$ , где је $x_0$ једно изабрано решење и $y \in Z$. Проверимо да ли ово решење задовољава и последњу конгруенцију, то јест да ли једначина
$x_0$ + НЗС($m_1$, $m_2$,…, $m_k$)$y \equiv a_{к+1} \pmod{m_{k+1}}$ има решење.
Дакле, тражимо $y \in Z$ тако да НЗС($m_1$, $m_2$,…, $m_k$)$y \equiv a_{к+1} - x_0 \pmod{m_{k+1}}$ . Решење ове једначине постоји ако НЗД(НЗС($m_1$, $m_2$,…, $m_k$), $m_{k+1}$) | ($a_{к+1} - x_0$) . Како је НЗД(НЗС($m_1$, $m_2$,…, $m_k$), $m_{k+1}$)=НЗС(НЗД($m_1$,$m_{k+1}$), НЗД($m_2$,$m_{k+1}$), … , НЗД($m_k$,$m_{k+1}$)) довољно је показати да НЗД($m_i$, $m_{k+1}$)| ($a_{к+1} - x_0$) , за свако i∈{1, … , к}. Важи $a_{к+1} - x_0 = (a_{к+1} - a_i) + (a_i - x_0)$. Према претпоставци је НЗД($m_i$,$m_{k+1}$)|($a_{к+1} - a_i$).
Такође, $x_0 \equiv a_i \pmod{m_i}$ , за свако i∈{1, … , к}, тј. $m_i$| ($a_i - x_0$) , па је онда и НЗД($m_i$, $m_{k+1}$)| ($a_i - x_0$) . Самим тим НЗД($m_i$, $m_{k+1}$) | $(a_{к+1} - a_i) + (a_i - x_0)$ . Тиме смо доказали да систем од к+1 конгруенције има решење.
Треба одредити како изгледа опште решење система конгруенције. Нека је $x'$ једно решење система, а x произвољно. Тада је :

$x' \equiv a_1 \pmod{m_1}$ $\quad$ $x \equiv a_1 \pmod{m_1}$
$x' \equiv a_2 \pmod{m_2}$ $\quad$ $x \equiv a_2 \pmod{m_2}$
… $\quad$ …
$x' \equiv a_k \pmod{m_k}$ $\quad$ $x \equiv a_k \pmod{m_k}$

а тиме и $\quad x' \equiv x \pmod{m_1}$
$x' \equiv x \pmod{m_2}$
…
$x' \equiv x \pmod{m_k}$ .

Следи да $m_i$|(x-x′) , за свако i∈{1, … , к}, То значи да НЗС($m_i$, $m_k$) |(x-x′) , тј. да је x-x′=НЗС($m_i$, $m_k$) ·t , за неко $t \in Z$ . Такође, сваки број облика x′+НЗС($m_i$, $m_k$) · t , за $t \in Z$ јесте решење датог система конгруенција, пошто је НЗС($m_i$, $m_k$)≡0 (mod $m_i$) , за свако i∈{1, … , к}, ■

Ако су бројеви $m_i$, $m_j$ међусобно узајамно прости за i≠j, онда важи да наведени систем конгруенција има решење за све $a_i$.

**Пример 2.8.** Решити систем конгруенција

$x \equiv_3 2$
$x \equiv_4 3$
$x \equiv_5 1$ .

Приметимо да су 3,4 и 5 међусобно узајамно прости па дати систем има решење. Из прве једначине је 3|(x-2) , па је решење облика x=3y+2 , за неко y∈Z . Заменимо то у другу једначину : 3y+2≡$_4$ 3 , тј. 3y≡$_4$ 1 . Пошто је НЗД(3,4)=1 и 1|1 последња једначина има решење које је облика y=3+4z , за z∈Z . Тада је

x=3y+2=3(3+4z)+2=11+12z .

Заменимо ову једнакост у трећу једначину датог система: 11+12z≡$_5$ 1 , тј. 12z≡$_5$ 0 , па је 5|12z . Како је НЗД(5,12)=1 следи да је 5|z тј. z=5t . за $t \in Z$. Дакле, x=11+12z=11+60 t , $t \in Z$ је опште решење полазног система. Приметимо да 11 јесте једно специјално решење система, као и да НЗС(3,4,5)=60, па се добијени резултат поклапа са тврђењем теореме. ◊

**Дефиниција 2.4.** Нека је n>1 природан број. Са $\boldsymbol{\varphi(n)}$ означавамо број природних бројева m тако да 1≤ m < n и НЗД(m,n)=1. Функција φ се назива **Ојлерова функција**.

**Теорема 2.20.** Нека су m,n>1 природани бројеви такви да НЗД(m,n)=1. Тада је

$$\varphi(mn) = \varphi(m) \cdot \varphi(n) .$$

**Теорема 2.21.(Ојлерова теорема)** Нека су a и n позитивни природни бројеви, такви да НЗД(a,n)=1. Тада важи $a^{\varphi(n)} \equiv 1 \ (mod\ n)$ .

**Последица 2.21.** Ако је НЗД(a,n)=1 тада је

$$x \equiv b a^{\varphi(n)-1} \ (mod\ n)$$

решење конгруенције ax≡b (mod n) .

**Доказ:** Према Ојлеровој теореми $a^{\varphi(n)} \equiv 1 \ (mod\ n)$ одакле је

$$a^{\varphi(n)} b \equiv b \ (mod\ n)$$

Уврставајући $a^{\varphi(n)} b$ уместо b у једначину добијамо

$$ax \equiv b a^{\varphi(n)} \ (mod\ n)$$

из чега следи

$$x \equiv b a^{\varphi(n)-1} \ (mod\ n)$$

је решење конгруенције ax≡b (mod n) . ■

Ова последица нам указује још један начин за решавање конгруенције ax≡b (mod n), а самим тим и налажења количника два броја по датом модулу.

**Пример 2.9.** Одредити решење једначине $3x \equiv_{35} 20$.
Како је НЗД(3,35)=1 можемо применити последицу 2.21.

$$x \equiv_{35} 20 \cdot 3^{\varphi(35)-1}$$
$$x \equiv_{35} 20 \cdot 3^{23}$$
$$x \equiv_{35} 30 \qquad . \Diamond$$

# 3. Криптографија

**Fysis kriptesthai filei**
(Природа воли да се скрива - Heraklit)

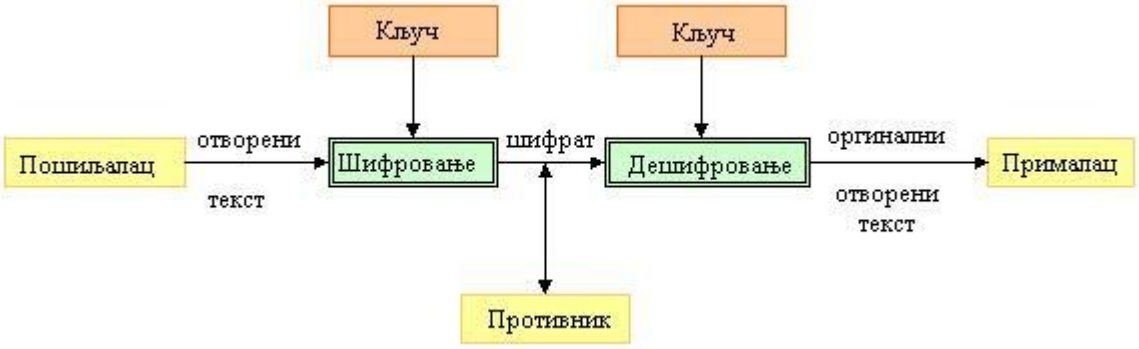
Криптографија има велики потенцијал којим може обогатити наставу математике. Може јој дати узбудљивост, драматичност, динамичност, а код ученика пробудити знатижељу и креативност. Управо то тако често недостаје у настави математике у којој се по плану и програму све сервира "здраво за готово" па због тога ученици мисле да се у математици више ништа ново не може открити. Многи примери из криптографије нам могу послужити да "разбијемо" стереотип као нпр. да је сваки математички проблем решив уз помоћ праве формуле или доброг рачунара. Наиме, сигурност шифровања лежи управо у нашој немогућности да брзо и ефикасно решимо одговарајући проблем из подручја алгебре, теорије бројева или комбинаторике. Занимљиве методе шифровања и проналажење метода за дешифровање омогућују ученицима да осете сву снагу и лепоту математике.

## 3.1. Општи појмови у криптографији

Криптографија (од грчког kryptós (скривен) и gráfo (писати)) је наука која се бави методима очувања тајности информација. Она се бави проналаском методе за чување информација у оној форми која ће бити читљива само онима којима је информација намењена док ће за остале бити неупотребљива.
Када се личне, финансијске, војне или информације државне безбедности преносе са места на место, оне постају рањиве на прислушкивачке тактике. Овакви проблеми се могу избећи криптовањем (шифровањем) информација које их чини недоступним нежељеној страни.

Шифра и дигитални потпис су криптографске технике које се користе да би се имплементирали безбедносни сервиси. Основни елемент који се користи назива се шифарски систем или алгоритам шифровања. Сваки шифарски систем обухвата пар трансформација података, које се називају шифровање и дешифровање. Шифровање је процедура која трансформише оригиналну информацију (отворени текст) у шифроване податке (шифрат). Обрнут процес, дешифровање, реконструише отворени текст на основу шифрата.

Приликом шифровања, поред отвореног текста, користи се једна независна вредност која се назива кључ шифровања. Слично, трансформација за дешифровање користи кључ дешифровања. Број симбола који представљају кључ (дужина кључа) зависи од шифарског система и представља један од параметара сигурности тог система.




Упоредо са развојем криптографије развила се и криптоанализа (од грчког kryptós (скривено) и analýein (размрсити) ). Криптоанализа је наука која се бави разбијањем шифри, односно откривањем садржаја отвореног текста на основу шифрата, а без познавања кључа. У ширем смислу, криптоанализа обухвата и проучавање слабости криптографских елемената, као што су, на пример, хеш функције или протоколи аутентификације. Различите технике криптоанализе називају се напади.

Иако је циљ одувек исти, методе и технике криптоанализе су се током историје криптографије драстично промениле, прилагођавајући се повећаној комплексности криптографије, почев од метода који су подразумевали папир и оловку, преко машина као што је Енигма током Другог светског рата, до рачунарски базираних напада данашњице. Методи за разбијање криптосистема су сада другачије него раније, и обично подразумевају решавање пажљиво конструисаних проблема из чисте математике, међу којима је најпознатија факторизација целих бројева.

## 3.2. Кратак историјски преглед криптографије

Када је писмо постало средство комуникације, појавила се потреба да се нека писма сачувају од туђих погледа. Тада је и криптографија угледала светлост дана. Урезивање хијероглифа на споменицима Старог царства у Египту (пре више од 4500 година) узима се за најранији доказ криптографије. Од самог почетка, енкрипција података користила се првенствено у војне сврхе. У старој Грчкој су спартански војници користили нарочит штап за одгонетање, скитал. Херодот још помиње јавке на таблама, прекривене воском и писање на главама робова (прво тетовирање) што би касније покрила коса. Један од првих великих војсковођа који је користио шифроване поруке био је Јулије Цезар. Наиме, када је Цезар слао поруке својим војсковођама, он је те поруке шифровао тако што су сва или поједина слова у тексту била померана за три, четри или више места у абецеди. Такву поруку могли су да дешифрују само они који су познавали правило за померање. Позната Цезарова изјава приликом преласка Рубикона у шифрираном дописивању гласила би: ***fqkf ofhzf kyz***. Помицањем сваког слова за шест места у абецеди лако се може прочитати прави смисао поруке: ***Alea iacta est*** (коцка је бачена).

Прву познату расправу о криптографији написао је на 25 страница италијански архитекта Леоне Батиста Алберти 1467. године. Он је такође творац такозваног шифарског круга и неких других решења двоструког прикривања текста која су у XIX веку прихватили и усавршавали немачки, енглески и француски шифрантски бирои.

Пола века након тога објављено је у пет свезака дело Јоханеса Тритхемуса прва књига из подручја криптографије. У 16. веку значајан допринос дају милански доктор Ђироламо Кардано, математичар Батисто Порта и француски дипломата Блез де Вижнер.

Све до Другог светског рата шифроване поруке могле су се колико-толико и дешифровати. На немачкој страни појавила се машина која је шифровала поруке на до тада још невиђен начин. Немци су машину назвали Енигма. Међутим, ма колико је она у то време била револуциона, савезници су успели да разбију поруке шифроване Енигмом.

После Другог светског рата и појавом првих рачунара отворила су се нова врата криптографији. Рачунари су временом постајали све бржи и бржи, радећи и по неколико стотина, а касније и милиона операција у секунди. Новом брзином рада је омогућено пробијање шифри за све мање времена. Упоредо с тим, радило се и на измишљању нових, сигурнијих и компликованијих алгоритама за шифровање.

## 3.3. Класична криптографија - Супституционе и транспозиционе шифре

Пре појаве рачунара, криптографија се састојала од алгоритама заснованих на словима. Различити криптографски алгоритми су или замењивали слова једно другим или су премештали слова. Бољи алгоритми су радили обе операције.

Ситуација је данас сложенија али је филозофија остала иста. Основна разлика је што данас алгоритми раде са битовима, а не са словима. То је у ствари само промена величине абецеде; у енглеском језику са 26 на 2 елемента, а код нас са 30 на 2 елемента. Многи добри алгоритми још увек комбинују елементе супституције и транспозиције и то је управо мост између класичних и савремених шифара.

### 3.3.1. Супституционе шифре

Супституциона шифра (шифра замене) свако слово у отвореном тексту замењује другим словом у шифрату. Прималац обрће супституцију у шифрату да би реконструисао отворени текст.

У класичној криптографији постоје четири врсте супституционих шифара:

1. Обична супституциона шифра или моноалфабетска шифра, јесте шифра у којој је свако слово отвореног текста замењено одговарајућим словом у шифрату. Криптограми у новинама су обичне супституционе шифре.
2. Хомофонична супституциона шифра слична је обичној супституционој шифри; разлика је само у томе што једно слово из отвореног текста може бити замењено једним или са неколико слова у шифрату. На пример, "А" може да одговара броју 5, 13, 25 или 56, "Б" може одговарати броју 7, 19, 31 или 42 и тако даље.
3. Полиграмска супституциона шифра шифрује блокове знакова у групама. На пример, "АБА" може одговарати "РТМ", "АББ" може одговарати "СЛЛ", и тако даље.

4. Полиалфабетска супституциона шифра састоји се од више обичних супституционих шифара из различитих абецеда. На пример, може се употребити пет различитих обичних супституционих шифара, а абецеда се мења на произвољним местима у отвореном тексту.

### 3.3.2. Транспозиционе шифре

У транспозиционој шифри (шифри премештања) елементи отвореног текста остају исти али им се мења распоред. У једноставној стубичној транспозиционој шифри отворени текст је написан хоризонтално на парчету папира с квадратићима фиксне ширине, а шифрат се чита вертикално. При дешифровању се шифрат пише вертикално, на папиру с квадратићима исте ширине, а затим се отворени текст чита хоризонтално.

Пошто су слова у шифрату иста као и у отвореном тексту, анализом учесталости шифрата откриће се да је вероватноћа појаве сваког слова приближно једнака као у енглеском језику. То даје веома добар траг криптоаналитичару, који онда може да искористи разне технике како би одредио прави поредак слова и тако добио отворени текст. Обрада шифрата другом транспозиционом шифром у великој мери повећава сигурност. Постоје још компликованије шифре, али је све њих могуће провалити помоћу рачунара.

Иако многи савремени алгоритми користе транспозицију, то је незгодно јер је за њу потребно много меморије и понекад мора да буде ограничена дужина поруке. Супституција се користи много чешће.

### 3.3.3. Примери супституционих и транспозиционих шифара

У овом делу описаћу неке примере супституционих и транспозиционих шифара које користе модуларну аритметику. Њих могу користити и они који немају велико математичко предзнање тако да су јако згодни за популаризацију математике код ученика у вишим разредима основне и ученика у средњој школи.

#### 3.3.3.1. Цезарова шифра

У криптографији Цезарова шифра је један од најпростијих и најраспрострањенијих начина шифровања. То је тип шифре замењивања у коме се свако слово отвореног текста мења одговарајућим словом азбуке, помереним за одређени број места. На пример, са помаком 3, А се замењује словом Г, Б са Д итд. Овај метод је добио име по Јулију Цезару, који га је користио за размену порука са својим генералима.

Цезарова шифра се често користи као корак у креирању сложенијих начина шифровања, као што је Вижнерова шифра, а има и модерну употребу у систему *ROT13*.

Као и све остале шифре простог азбучног замењивања Цезарова шифра се лако разбија и у пракси не пружа никакву сигурност у комуникацији.

Претварање може да се представи поравнавањем две азбуке једне испод друге; азбука за шифровање је обична азбука ротирана лево или десно за одређени број места. На пример, овде је Цезарова шифра која користи леву ротацију од три места (параметар помак, у овом примеру 3, се користи као кључ):

| **отворено:** | **а** | **б** | **в** | **г** | **д** | **ђ** | **е** | **ж** | **з** | **и** | **ј** | **к** | **л** | **љ** | **м** | **н** | **њ** | **о** | **п** | **р** | **с** | **т** | **ћ** | **у** | **ф** | **х** | **ц** | **ч** | **џ** | **ш** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **шифрат:** | **Г** | **Д** | **Ђ** | **Е** | **Ж** | **З** | **И** | **Ј** | **К** | **Л** | **Љ** | **М** | **Н** | **Њ** | **О** | **П** | **Р** | **С** | **Т** | **Ћ** | **У** | **Ф** | **Х** | **Ц** | **Ч** | **Џ** | **Ш** | **А** | **Б** | **В** |

За шифровање поруке једноставно се записује слово из линије „Шифрат“ које се налази испод одговарајућег слова у линији „Отворено“. За дешифровање поступак је обрнут.

Отворено: Чик погоди шта пише
Шифрат: АЛМ ТСЕСЖЛ ВФГ ТЛВИ

Цезарово шифровање се такође може представити коришћењем модуларне аритметике тако што се прво слова претворе у бројеве, по шеми А=0, Б=1, ..., Ш=29.

| **отворено:** | **а** | **б** | **в** | **г** | **д** | **ђ** | **е** | **ж** | **з** | **и** | **ј** | **к** | **л** | **љ** | **м** | **н** | **њ** | **о** | **п** | **р** | **с** | **т** | **ћ** | **у** | **ф** | **х** | **ц** | **ч** | **џ** | **ш** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **шифрат:** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** | **25** | **26** | **27** | **28** | **29** |

Шифровање слова x са помаком n може математички да се опише као

$$E_n(x) = (x + n) \pmod{30}$$

Сличне се изводи и дешифровање

$$D_n(x) = (x - n) \pmod{30}$$

Према наведеном, резултат је у опсегу од 0 до 29. Ако резултат x+n или x-n није у опсегу од 0 до 29, треба додати или одузети 30.

Нпр. џ у шифранту са помаком 3 је 28 +3= 31, а $31 \equiv 1 \pmod{30}$ дакле џ је б.

Замена је иста за целу поруку, тако да је ово шифровање класификовано као тип моноалфабетске шифре, насупрот типу полиалфабетске шифре и за њено разбијање је довољан само шифрат.

Вишеструка шифровања не омогућавају додатну сигурност. То је зато што ће два шифровања са рецимо помаком *A* и помаком *B* бити еквивалентна једном шифровању са помаком *A* + *B*.

Није познато колико је Цезарова шифра била ефикасна у то време, али је вероватно била релативно сигурна, не само због тога што је мало Цезарових непријатеља знало латински или уопште било упознато са писаним језиком, већ и због немогућности примене криптоанализе. Под претпоставком да је нападач могао да прочита поруку, не постоје записи из тог времена о било каквој техници за решавање шифара просте замене. Најстарији записи са открићем фреквентне анализе датирају из 9. века са арапског подручја.

У 19. веку, лични огласи у новинама су коришћени за размену шифрованих порука коришћењем простих шема шифровања. Дејвид Кан (1867) у Тајмсу описује случајеве тајне комуникације љубавника шифроване Цезаровом шифром. Чак и касније, 1915, коришћена је Цезарова шифра: Руска војска је користила као замену за много компликованије шифре које су се код њихових трупа показале као сувише тешке за савладавање; Немачки и Аустријски криптоаналитичари нису имали муке да декриптују њихове поруке.

Данас се Цезарова шифра може наћи у дечијим играма. Цезаров помак од 13 се такође користи у ROT13 алгоритму, прост метод да се неки текст учини непрепознатљивим који се користи на неким Интернет форумима (да се сакрије спојлер), али не као метод шифровања.

Априла 2006. мафијашки бос Бернардо Провенцано је ухваћен на Сицилији делимично захваљујући криптоанализи његових порука писаних у варијанти Цезарове шифре. Провенцанова шифра је користила бројеве, тако да је "А" писано као "4", "Б" као "5" итд.

Рачунар у филму " Одисеја у свемиру 2001" се зове HAL што уопше није случајно. Ако се мало боље погледа види се да ће Цезарова шифра са помаком један превести HAL у IBM.

### 3.3.3.2. Вижнерова шифра

Вижнерова шифра је метод шифровања азбучног текста коришћењем серије Цезарових шифара, заснованих на словима кључа. Ово је прости облик шифре полиалфабетске замене.

Вижнерова шифра је откривана више пута. Метод је први описао Ђован Батиста Белазо. Међутим, касније, у 19. веку је та шема погрешно приписана Блезу де Вижнеру, тако да је сад позната као „Вижнерова шифра“.

Шифра је добро позната зато што, иако је лака за разумевање и примену, почетницима изгледа као непробојна; тако је и добила епитет непробојна шифра. Стога су многи покушавали да примене шеме шифровања, које су у основи Вижнерова шифра.

Код Цезарове шифре, свако слово алфабета се помера за неки број места; на пример, са помаком 3, слово *A* постаје *D*, *B* постаје *E* итд. Вижнерова шифра се састоји од низа неколико Цезарових шифара са различитим помацима. Овде користимо енглески алфабет.

Вижнерова таблица, такође позната и као *tabula recta*, може да се користи за шифровање и дешифровање.

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

Вижнерова таблица или Вижнеров квадрат састоји се од алфабета написаног 26 пута (овде је реч о енглеској абецеди) у новом реду, сваки ред ротиран улево у односу на претходни, одговара свим могућим комбинацијама Цезарове шифре. У појединој тачки процеса шифровања, шифра користи други алфабет из једног од редова. Који ће се ред користити зависи од понављајућег кључа.

На пример, рецимо да је отворени текст који треба да се шифрује:

ATTACKATDAWN

Особа која шаље поруку бира кључ и понавља га онолико пута колико је потребно да одговара дужини отвореног текста, нпр, кључ LEMON:

LEMONLEMONLE

Прво слово отвореног текста A се шифрује користећи алфабет из реда L, које је прво слово кључа. То се ради тако што се тражи слово у реду L и колони A Вижнерове таблице, односно тражено слово је L. За следеће слово отвореног текста се користи следеће слово кључа, слово у пресеку реда E и колоне T је тражено слово X. По том систему се наставља до краја отвореног текста:

| Отворени текст: | A | T | T | A | C | K | A | T | D | A | W | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Кључ: | L | E | M | O | N | L | E | M | O | N | L | E |
| Шифрат: | L | X | F | O | P | V | E | F | R | N | H | R |

Дешифровање се врши тражењем места шифрованог слова у реду табеле, а као слово отвореног текста се узима наслов колоне. На пример, у реду L, шифровано L се налази у колони са насловом A, који се узима као прво слово отвореног текста. Следеће слово се дешифрује тражењем слова X у реду E - оно се налази у колони T и то је тражено слово отвореног текста.

Вижнерова шифра може да се представи и алгебарски. Ако се словима азбуке А до Ш (овде је реч о српској ћирилици) доделе вредности 0 до 29 и изврши сабирање по модулу 30, шифровање може да се напише као $S_i \equiv O_i + K_i \pmod{30}$ , а дешифровање као $O_i \equiv S_i - K_i \pmod{30}$ где је

O - отворени текст, S - шифрат, а K – кључ.

Пример шифровања поруке Вижнеровом шифром на српском ћириличном писму

| порука | с | к | р | и | в | е | н | а | п | о | р | у | к | а |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| код поруке | 20 | 11 | 19 | 9 | 2 | 6 | 15 | 0 | 18 | 17 | 19 | 23 | 11 | 0 |
| кључ | к | љ | у | ч | к | љ | у | ч | к | љ | у | ч | к | љ |
| код кључа | 11 | 13 | 23 | 27 | 11 | 13 | 23 | 27 | 11 | 13 | 23 | 27 | 11 | 13 |
| код шифрата | 1 | 24 | 12 | 6 | 13 | 19 | 8 | 27 | 29 | 0 | 12 | 20 | 22 | 13 |
| шифрат | Б | Ф | Л | Е | Љ | Р | З | Ч | Ш | А | Л | С | Ћ | Љ |

Вижнерова шифра је ефикасна јер маскира карактерситичну фреквенцију слова отвореног текста, али одређени узорак ипак остаје.

Снага Вижнерове шифре, као и свих полиалфабетских шифара, је њена способност отежавања фреквентне анализе. Фреквентна анализа је вештина декриптовања поруке бројањем фреквенције слова шифрата и упоређивање са фреквенцијом слова нормалног текста. На пример, ако се слово K јавља највећи број пута у шифрату чији је отворени текст на српском, може се претпоставити да K одговара слову A, јер је слово A најчешће у српском језику. Коришћењем Вижнерове шифре, слово A ће се

замењивати различитим словима алфабета на различитим местима у поруци и тако онемогућити просту фреквентну анализу.
Основна слабост Вижнерове шифре је њен релативно кратак и понављајући кључ. Ако криптоаналитичар открије дужину кључа, онда шифрат може да се посматра као серија Цезарових шифара, које се затим појединачно једноставно разбијају.

## 3.4. Савремени алгоритми за шифровање

Појавом рачунарских мрежа криптографија нагло добија на значају. Нарочито је битно обезбедити заштиту важних података (нпр. финансијских) који се преносе мрежом.

Криптовање података подразумева коришћење разних криптографских алгоритама којима се врши криптовање.

Алгоритми за криптовање се могу поделити у две групе:

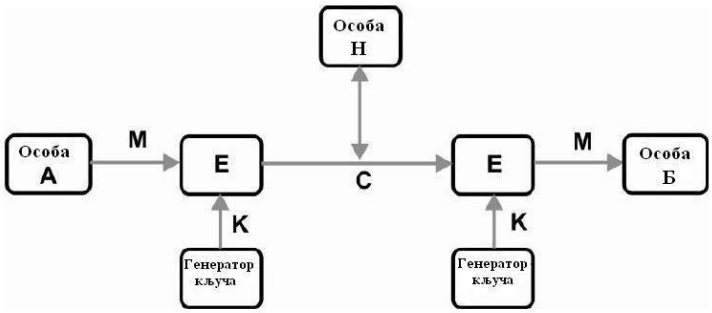
1. Тајни алгоритми : безбедност се заснива на тајности алгоритма (историјски интересантни).
2. Алгоритми засновани на кључу : безбедност се заснива на кључевима, а не на детаљима алгоритма који се могу публиковати и анализирати. Овде је алгоритам јавно познат, а кључ се чува у тајности.

Данас се највише користе алгоритми за криптовање засновани на кључу. Они се могу класификовати у три групе :

1. Симетрични, код којих се користи један кључ.
2. Асиметрични, код којих постоје два кључа.
3. Хибридни, који су комбинација претходна два.

### 3.4.1. Симетрична криптографија

Основна особина симетричних криптосистема или криптосистема са тајним кључем (*Symetric-Key* ili *Secret-key Criptosystems*) је да се за криптовање/декриптовање порука користи исти кључ.




На слици је приказан принцип рада симетричног криптосистема. Особа *А* има за циљ слање поруке *М* особи *Б* преко незаштићеног комуникационог канала. Особа *А*

најпре генерише поруку *M* (изворни текст) која се упућује у блок за шифровање *E*. У овом блоку се врши криптовање поруке *M* уз коришћење кључа *K* добијеног уз помоћ генератора кључа. На тај начин се креира криптована порука *C*. Потом се тако добијена порука комуникационим каналом шаље до особе *Б* .

Поступак декриптовања се обавља инверзним поступком од криптовања у блоку за декриптовање. Декриптовање поруке *C* се врши помоћу истог кључа *K* који је коришћен приликом криптовања. Након декриптовања се добија изворна порука *M*.

Уколико на каналу за пренос постоји особа *H* (нападач) може да пресретне криптовану поруку и уколико дође у посед кључа може прочитати или злоупотребити изворну поруку. Да би се избегле манипулације, обе стране морају држати кључ у тајности, односно кључ се не сме преносити незаштићеним комуникационим каналом. За разлику од кључа, криптована порука може да се шаље и по незаштићеном каналу с обзиром на то да садржај изворне поруке може да протумачи само онај корисник који има кључ. Пример слања кључа различитим комуникационим каналом је када се ПИН (eng. *Personal Identification Number*) код за приступ заштићеним Интернет сајтовима (нпр. Банке за увид стања на рачуну) достављају корисницима поштом, а не Интернетом.

Најпознатији алгоритми симетричних криптосистема који се данас користе су: DES, 3DES, DES-CBC, IDEA, RC5, RC6, AES и други.

Алгоритми који користе симетрични кључ за криптовање одликују се високом ефикасношћу, што се огледа у кратком времену криптовања порука. Разлог кратког времена криптовања је употреба кратких кључева. Из тих разлога се ова врста алгоритама користи за криптовање/декриптовање порука велике дужине.

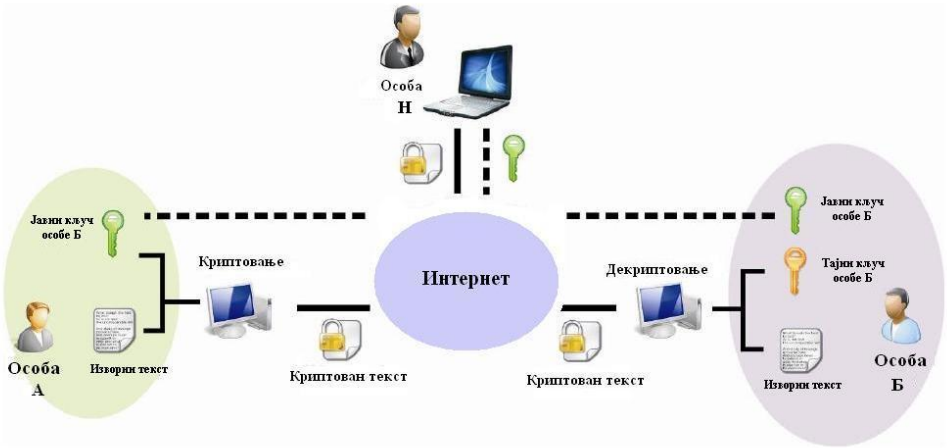
Симетрично криптовање има два основна недостатка. Оба корисника (особа *A* и особа *Б*) морају поседовати јединствени симетрични кључ, те се јавља проблем дистрибуције кључева. Наиме, корисници који желе да размене поруку претходно морају да се договоре о кључу. Једини поуздан начин је да се оба корисника физички сретну и изврше размену кључа. Међутим, често су корисници физички раздвојени и не могу да дођу у непосредан контакт, зато морају да користе неки заштићен канал да би сигурно разменили кључеве. Проблем је то што заштићен канал практично не постоји. Други проблем који се јавља код симетричних криптосистема је велики број потребних кључева. Ако имамо *n* људи који желе да користе ову методу криптовања, то захтева $n(n - 1)/2$ симетричних кључева. На пример за 1 милион људи потребно је 500 милијарди симетричних кључева. Ради добијања толико великог броја различитих кључева морају се користити кључеви веће дужине. Тако на пример, дужина кључа од 56 бита је данас на граници довољног с обзиром на то да савремени рачунари могу релативно брзо да открију кључ те дужине.

## 3.4.2. Асиметрична криптографија

Творци асиметричне криптографије су Whitefield Diffie и Martin Hellman који су 1976. године описали идеју криптографије која се темељи на два кључа, приватном (или често званим тајним) и јавном кључу. У литератури појам асиметричног криптовања се поистовећује са термином asymmetric-key или public-key криптовањем.

Разлика између симетричних и асиметричних алгоритама је у томе што симетрични алгоритми користе исти кључ за криптовање и декриптовање док асиметрични алгоритми користе различите кључеве за криптовање односно декриптовање. Информације које су криптоване јавним кључем могу се декриптовати само тајним кључем односно то може само особа која је власник тајног асиметричног кључа. Оба кључа морају бити повезана помоћу јединствене једносмерне функције. Односно не сме се израчунати тајни кључ из јавног кључа или се барем не сме израчунати у разумном времену.

Алгоритми асиметричних криптосистема заснивају се на одређеним својствима бројева. При криптовању се изворни текст третира као низ природних бројева који се одабраном функцијом криптовања и кључем Ке прерачунавају у криптовани низ текста. Функција криптовања мора бити таква да се из криптованог текста не може одредити изворни текст, чак ако је познат и кључ за криптовање. Међутим, уколико се зна кључ декриптовања Kd могуће је лако рачунање изворног текста. Асиметрично криптовање представља јако сложен вид заштите података. За његову реализацију сваки од саговорника мора поседовати два кључа (јавни и тајни). Иако су различити, кључеви су међусобно повезани одређеним трансформацијама. На следећој слици је приказан пример асиметричног криптовања.




Ради једноставније анализе рада користићемо симболе *А, Б* и *Н*. *А* је особа која жели да пошаље изворни текст, *Б* представља особу која би требала да прими послати текст, а *Н* је особа која неовлашћено жели да дође до сигурних података које особа *А* шаље особи *Б*.

Сценарио асиметричног криптовања би изгледао овако: Особа *А* кодира поруку ради слања особи *Б* употребом јавног кључа особе *Б* који је свима доступан (чак и особи *Н*). Особа *А* је јавни кључ могла добити путем email-а, преузети са *Web* сајта и сл. Међутим особа *Н* или било ко и поред тога што познаје јавни кључ не може открити садржај поруке. Поруку може дешифровати само особа *Б* коришћењем свог тајног кључа. На овај начин порука је заштићена од трећег лица. Основни недостатак овог начина криптовања је његова спорост и неприкладност за криптовање великих количина података. Такође, остаје отворено питање аутентичности поруке, односно

како да особа *Б* буде сигурна да је поруку коју је примила уистину послала особа *А*. Најчешће се користе следећи асиметрични алгоритми: RSA (eng. Rivest-Shamir-Adleman), Diffie-Hellman, ElGamal, Eliptic Curves, Rabin и други.

Криптовање/декриптовање помоћу асиметричног кључа има две предности: Прво, решава недостатаке дељења кључа код симетричних алгоритама приликом комуникације између две особе (*А* и *Б*). Код симетричног криптовања кључ се размењује између две особе и не може се користити уколико једна од две особе жели комуницирати са трећом особом. Код асиметричних криптосиситема свака особа креира по два кључа, један је тајни који особа чува, а други је јавни који се размењује са другима. Сваки од ентитета је независтан и свој пар кључева може користити у комуникацији са било киме. Друга предност се огледа у веома великом смањењу броја укупно потребних кључева. У систему у коме комуницира милион корисника, потребно је само 2 милиона кључева, док би у случају коришћења симетричног криптовања било потребно бар 500 милијарди кључева.

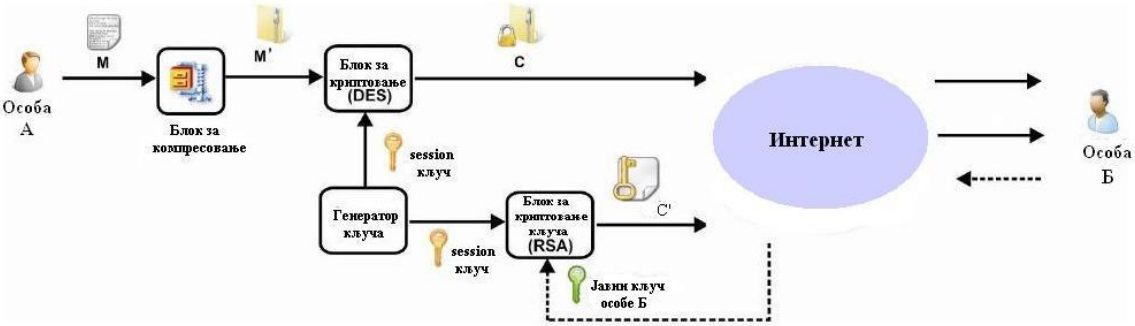
Симетрични алгоритми, такође, имају два недостатка. Највећи недостатак је комплексност алгоритама који се користе приликом криптовања. Ако се жели ефектно криптовање то повлачи да алгоритам користи огромне кључеве приликом рада. Оперисање са огромним бројевима захтева много времена. Због тога асиметрични алгоритми нису препоручљиви за рад са великим изворним подацима. Може се рећи да су асиметрични алгоритми много ефикаснији у раду са кратким порукама. Исто тако, ова врста алгоритама због своје сложености нису погодни за хардверску имплементацију. Други недостатак је тај што се комуникација између две стране и јавни кључ морају верификовати. Како особа *А* шаље свој јавни кључ особи *Б* путем електронске поште, особа *Б* на неки начин мора бити сигурна да је добијени кључ управо послат од стране особе *А*. Ово је нарочито важно уколико се ради о коришћењу асиметричног криптовања приликом идентификације корисника на неки систем.

### 3.4.3. Хибридни криптосистеми

Имајући у виду да употреба симетричне или асиметричне криптографије пати од извесних недостатака јавља се потреба за системима који комбинују најбоље појединачне карактеристике оба система. Тако су настали хибридни криптосистеми. Принцип рада ових система се огледа у следећем: Изворни текст се прво криптује употребом кључа (понекад назван и session кључ), а затим се тај кључ заједно са криптованом поруком пакује и поново криптује са јавним кључем особе којој се шаље порука. Поступак декрипције целе поруке се остварује обрнутим редоследом операција: Особа која је примила поруку прво декриптује исту са својим тајним кључем, проналази запаковани session кључ и користи га да би прочитала изворну поруку.

За генерисање session кључа користи се генератор псеудо-случајног броја у комбинацији са разним корисниковим уносима у току процеса генерисања. На овај начин се постижу завидне перформансе система за криптовање, јер се асиметрично криптује само кратак симетрични кључ, а не цела, велика порука. Знамо да асиметрично криптовање није погодно за поруке велике дужине.

Пример успешног хибридног криптосистема је PGP (eng. Pretty Good Privacy) програмски пакет за криптовање података који је формирао Phill Zimmerman 1991. године. Принцип рада PGP алгоритма је приказан на следећој слици.




Особа *А* пре слања поруке *М* особи *Б* прво изврши компресију помоћу неке од метода за компресију података (нпр. ZIP). Компресовањем поруке се убрзава време слања поруке, а истовремено и добија на заштити поруке. Тако компресована порука *M′* се криптује помоћу неког од симетричних алгоритама (DES, 3DES, IDEA или слично) и session кључа. На тај начин се добија криптована порука *С*. Затим се врши криптовање session кључа помоћу неког од асиметричних алгоритама (RSA, ElGamal или Diffie-Hellman) и јавног кључа особе *Б*. Тако настаје криптована порука *C′* која се шаље особи *Б* заједно са поруком *С* .

Процес декриптовања се обавља обрнутим редоследом радњи од процеса криптовања. Када прими криптовану поруку особа *Б* употребљава свој тајни кључ и декриптује поруку која садржи session кључ. Коришћењем session кључа особа ***Б*** декриптује криптовану поруку, а касније је и декомпресује у циљу добијања изворне поруке.

PGP програм нуди неколико степени заштите: ниски, високи и војни. Први користи 512-битни кључ, други 768-битни, а војни користи 1024-битни кључ. Осим генерисања пара кључева, PGP алгоритам нуди још доста сигурносних мера типа: за генерисање кључева се не користи генератор кључева већ алгоритам тражи од корисника да унесе неке податке помоћу тастатуре, а за то време мери размаке између времена удараца и на основу њих генерише кључеве. Исто тако PGP нуди потписивање послатих докумената у циљу доказивања аутентичности.

### 3.4.4. Примери савремених алгоритама за шифровање

У овом делу нећу описивати сваки од алгоритама за шифровање већ ћу само поменути оне који користе модуларну аритметику и кратко описати где је користе. Разлог томе је што су савремени алгоритми доста сложенији од класичних алгоритама (што се може видети из њихових уопштених шема) и јер је за њих потребно доста знања како из математике тако и из информатике.

### 3.4.4.1. RC5 алгоритам

RC5 алгоритам формирао је Ronald Rivest са Massachusetts института за технологију 1994. године. RC5 припада симетричним шифарским блоковима погодан како за софтверску тако и за хардверску реализацију. RC5 представља алгоритам са промењивом величином блока улазних података, промењивим бројем корака извршавања и промењивим дужинама кључа. На овај начин RC5 обезбеђује велику флексибилност у перформансама и нивоима сигурности података.

RC5 алгоритам карактеришу следећи параметри RC5 - *w/r/b*. Где је *w* број битова у речи, *r* представља број корака RC5 алгоритма, а *b* је дужина кључа изражена у бајтовима. Различитим избором параметара добијају се различити RC5 алгоритми. Стандардну реч чини 32 бита, док су могуће и вредности 16 бита и 64 бита. RC5 криптовање користи блокове од две речи (2*w*) изворног или криптованог текста. Могуће вредности параметра *r* су 0,1,…,255. Број бајтова који чине кључ *b* креће се од 0 до 255. Тајни кључ K се често пре употребе проширi и на тај начин се формира такозвана проширена табела кључева S .

RC5 алгоритам чине три компоненте: алгоритам за проширење кључа, алгоритам за криптовање и алгоритам за декриптовање.

Сва три алгоритма користе следеће једноставне операције:

- $\boxplus$ Аритметичко сабирање по модулу $2^w$ ,
- $\oplus$ Бит по бит XOR ( Искључива дисјункција (бинарна логичка операција која је тачна само ако се операнди разликују). У математици,искључивој дисјункцији одговара сабирање по модулу 2. )
- <<< Ротација улево за одређени број битова.

Због једноставности операција RC5 је лак за имплементацију. Уз то износ помака у операцијама ротирања није фиксан, већ зависи од улазног податка.
Декриптовање имају одређену сличност која се огледа у обрнутом редоследу операција.

### 3.4.4.2. RC6 алгоритам

RC6 алгоритам се појавио као унапређење RC5 алгоритма 1998. године, наравно са строжијим захтевима по питању сигурности и бољим перформансама. Као и код RC5 и овај алгоритам користи ротације са променљивим помаком. Ново је једино то што RC6 користи четири уместо два блока речи (радна регистра). RC6 подржава блокове података од по 128 битова и користи кључеве величине 128, 192 и 256 бита.

RC6 алгоритам карактеришу следећи параметри RC6 - *w/r/b* где је *w* величина речи у битовима, *r* представља број корака алгоритма и *b* је дужина кључа у бајтовима.

Операције које се користе приликом криптовања су:

- $a + b$ Целобројно сабирање по модулу $2^w$
- $a - b$ Целобројно одузимање по модулу $2^w$
- $a \oplus b$ Бит по бит XOR над *w*-бит речима
- $a \times b$ Целобројно множење по модулу $2^w$
- $a <<< b$ Ротација *w*-битне речи *a* улево за b бита
- $a >>> b$ Ротација *w*-битне речи *a* удесно за b бита

### 3.4.4.3. RSA алгоритам

Најпопуларнији асиметрични метод за криптовање података је RSA алгоритам. RSA је скраћеница од почетних слова научника Rivest, Shamir и Adleman који су први јавно описали алгоритам 1977. године. Clifford Cocks, енглески математичар, развио је еквивалентан систем 1973. годиине, али је он био класификован највећим степеном тајности све до 1997. године.

За генерисање јавног и тајног кључа се користе прости бројеви. Тајни кључ представља уређени пар *(N,d)*, а јавни кључ уређени пар (*N,e*). Треба уочити да је број N заједнички за оба кључа. Особа која шаље поруку врши криптовање помоћу следеће једначине :

$$C = P^e \ (mod\ N)$$

где је P изворни текст који је приказан у облику броја; C број који представља криптован текст; бројеви e и N су компоненте јавног кључа. Када се порука прими потребно је дешифровати помоћу следеће једначине: $P = C^d \ (mod\ N)$

где су P и C исте као и у претходној формули, а N и d представљају компоненте тајног кључа.

Основни проблем код RSA алгоритма је како извршити избор бројева N, d и e (веома велике вредности дужине од 1024 до 2048), а да уједно задовољавају формуле алгоритма.

Заправо RSA користи теорију простих бројева и следећу процедуру :

- Изабрати два проста броја p и q .
- Израчунати N = p x q .
- Изабрати e (мора бити мањи од N) тако да e и производ (p - 1)(q - 1) буду узајамно прости .
- Одредити број d тако да задовољава једначину (e x d) = 1 ( mod [(p - 1)(q - 1)] ) .

Одређивање оригиналне поруке на основу криптоване поруке и јавног кључа еквивалентно је факторизацији производа два велика проста броја. Уколико би нека особа факторисала број N и из тога пронашла производ (p-1)(q-1)=$\varphi(N)$ ( $\varphi$ је Ојлерова функција) она не може доћи у посед броја e зато што он нема заједничког делитеља са (p-1)(q-1) . Ако се деси да на неки начин сазна број e, да би дошао до тајног кључа d мора да факторише број N. Пошто је број N веома велики и до 309 децималних цифара, факторизација је скоро немогућа.

Велики прости бројеви који се користе у RSA алгоритму намећу више проблема практичне природе. Да би се множили ови бројеви морају се користити посебни алгоритми за множење, за које је потребно више времена, самим тим се повећава време извршења алгоритма за криптовање. Сем тога алгоритми за факторизацију су из дана у дан све бољи и бољи, па је данас 512-битни RSA алгоритам недовољан за безбедно криптовање порука. Међутим претпоставља се да ће 1024-битни RSA бити безбедан још петнаестак година.

### 3.4.4.4. Diffie-Hellman-ов протокол за размену кључева

Diffie и Hellman су 1976. године предложили први алгоритам за размену кључева преко несигурног канала, чија је сигурност заснована на налажењу дискретног логаритма. Ово је практична метода за јавну размену тајних кључева и коришћен је у великом броју комерцијалних производа. Овај алгоритам се не може користити за размену порука већ се користи да се успостави заједнички тајни кључ који знају само учесници у комуникацији. Данас је познато да је James Ellis предложио исти концепт у тајности 1970. године.

Претпоставимо да се две особе (Ана и Бане) морају договорити о кључу за шифровање преко неког несигурног комуникационог канала. Такође, претпоставимо да су те две особе изабрале велики прост број $n$ и број $g$, такав да је G={0, 1, ..., n-1} циклична мултипликативна група, а $g$ њен генератор. Бројеви $g$ и $n$ нису тајна, што значи да их може користити већи број особа које међусобно комуницирају.

Diffie-Hellman-ов протокол за размену кључева обухвата следеће кораке :

- **Ана бира случајан велики број $x$ ($0 \le x \le n-2$) и шаље Банету $X = g^x \pmod n$,**
- **Бане бира случајан велики број $y$ ($0 \le y \le n-2$) и шаље Ани $Y = g^y \pmod n$,**
- **Ана одређује $k = Y^x \pmod n$,**
- **Бане одређује $k' = X^y \pmod n$.**

Вредности $k$ и $k'$ су једнаке $g^{xy} \pmod n$ и не може их израчунати неко ко прислушкује канал. То значи да нападач може доћи до вредности $n$, $g$, $X$, і $Y$, али да би добио вредност $k$ мора израчунати дискретни логаритам ( $x = log_g X \ (mod\ n)$). Дакле, к је тајни кључ који Ана и Бане независно рачунају.

**Пример.** Особе А и Б су договориле параметре **n** и **g** за размену кључева Diffie-Hellman-овим протоколом : **n = 5, g = 3.** Особа А је за свој приватни кључ изабрала **x = 3,** а особа Б је изабрала **y = 2.** Проверити да ли се кључеви који се добијају овим начином размене подударају, тј. да ли је $k=k'$.

| | |
|---|---|
| **Особа А: x = 3**<br>**$X = g^x \bmod n$**<br>$X = 3^3 \bmod 5$<br>$X = 27 \bmod 5$<br>$X = 2$<br><br>Особа А је особи Б послала **X = 2**<br><br>**Одређивање приватног кључа**<br>**$k = Y^x \bmod n$**<br>$k = 4^3 \bmod 5$<br>$k = 64 \bmod 5$<br>**k = 4** | **Особа Б: y = 2**<br>**$Y = g^y \bmod n$**<br>$Y = 3^2 \bmod 5$<br>$Y = 9 \bmod 5$<br>$Y = 4$<br><br>Особа Б је особи А послала **Y = 4**<br><br>**Одређивање приватног кључа**<br>**$k' = X^y \bmod n$**<br>$k' = 2^2 \bmod 5$<br>$k' = 4 \bmod 5$<br>**k' = 4** |

Из овог примера се види да су и особа А и особа Б добили идентичне кључеве па ће и поступак дешифровања бити успешан.

**Пример.** Ако је познато да је $3^n = 81$ релативно је лако доћи до решења n=4. Ако је $3^n(mod\ 7) = 1$ како доћи до решења?

Направићемо табелу и видети за које n је резултат 1.

| n | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $3^n$ | 3 | 9 | 27 | 81 | 243 | 729 |
| $3^n\ (mod\ 7)$ | 3 | 2 | 6 | 4 | 5 | 1 |

Ово је добро решење за мале бројеве али шта би радили да смо требали да рачунамо за $328^n(mod\ 23713)$. Овим путем би било тешко изводљиво. Сигурност Diffie-Hellman размене кључева лежи управо у чињеници да иако је релативно лако наћи експоненте по модулу примарног броја, јако је тешко наћи дискретне логаритме.

# 4. Модуларност у уметности

Модуларност у уметности можемо сагледати као генерализацију симетрије, али и као могућност стварања различитих структура помоћу једног или више базичних елемената - модула.

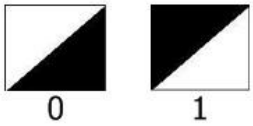
У науци принцип модуларности је трагање за основним елементима различитих геометријских структура, док у уметности различити модули (на пример цигле у орнаменталном зидарству) представљају основу модуларних структура.

У различитим областима математике проблем је препознати скуп основних елемената, правила конструкције и извођење различитих, тако изведених структура.

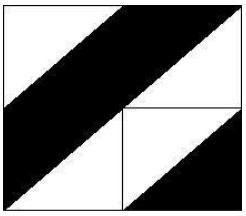
У визуелној уметности модуларна аритметика се може користити за прављење уметничких шара базираних на таблицама множења и сабирања по модулу n.

Најједноставнији пример је коришћење таблице за сабирање по модулу 2 и две основне црно-беле слике.

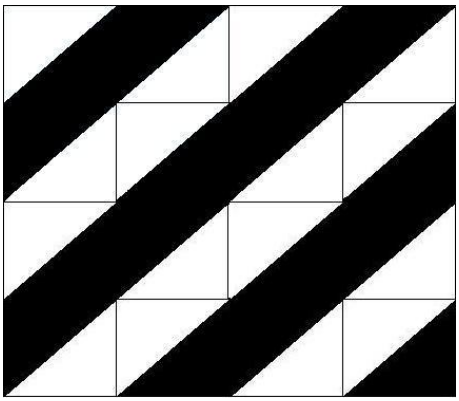
| + | **0** | **1** |
|---|---|---|
| **0** | 0 | 1 |
| **1** | 1 | 0 |




Заменом слика уместо бројева 0 и 1 у тамнијем делу табеле добијамо следећу шару



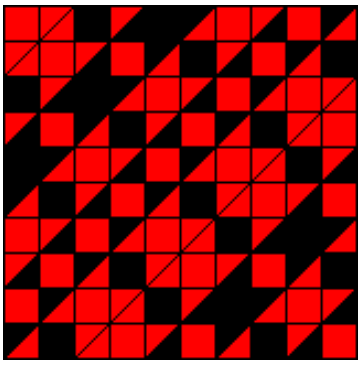
Ако добијену шару ставим у сва четири квадранта табеле 2x2 добићу следећу шару



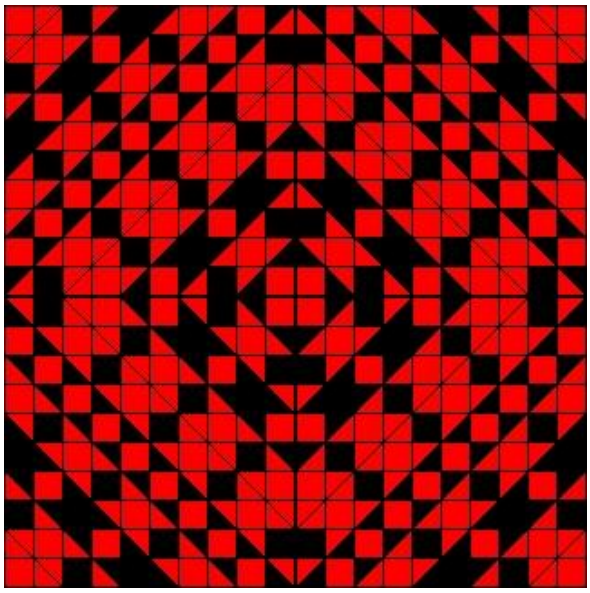
Овде ћу користити таблицу за сабирања по модулу 5 и пет основних слика.

| + | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| **0** | 0 | 1 | 2 | 3 | 4 |
| **1** | 1 | 2 | 3 | 4 | 0 |
| **2** | 2 | 3 | 4 | 0 | 1 |
| **3** | 3 | 4 | 0 | 1 | 2 |
| **4** | 4 | 0 | 1 | 2 | 3 |


Заменом слика уместо бројева 0, 1, 2, 3, 4, у таблици за сабирање, у тамнијем делу табеле добијамо следећу шару

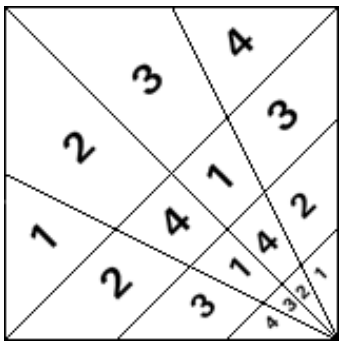


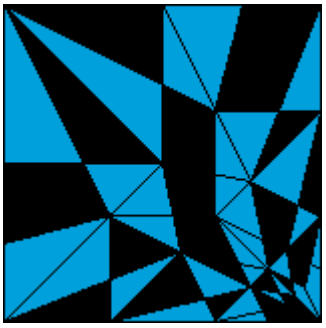
Ако добијену шару ставим у горњи леви угао табеле 2x2, а у остале квадранте сместим њој осно симетричне слике у односу на унутрашње странице табеле добићу следећу шару

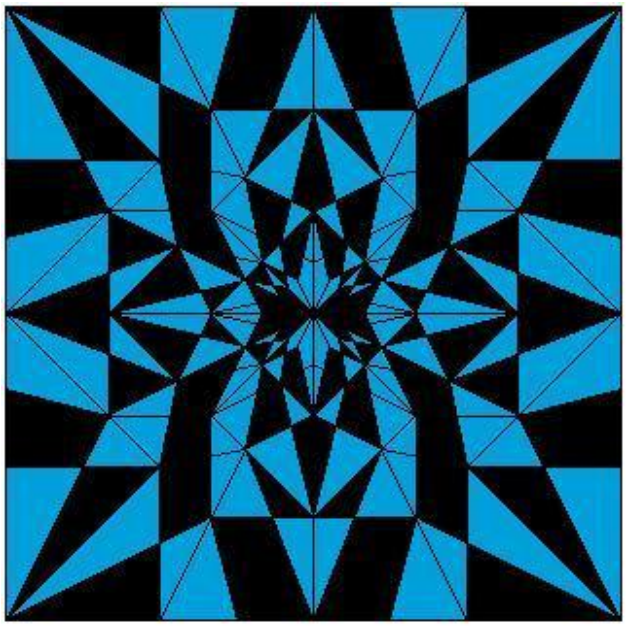


Слично као у претходном случају, ако искористим таблицу за множења по модулу 5 у мало измењеном облику и следеће основне елементе добићу

| • | **0** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|---|
| **0** | 0 | 0 | 0 | 0 | 0 |
| **1** | 0 | 1 | 2 | 3 | 4 |
| **2** | 0 | 2 | 4 | 1 | 3 |
| **3** | 0 | 3 | 1 | 4 | 2 |
| **4** | 0 | 4 | 3 | 2 | 1 |





# 5. Johann Carl Friedrich Gauß

Велики математичар, физичар и астроном Карл Фридрих Гаус, написао је преко осамдесет обимних научних расправа, које представљају основу развоја теоријске и примењене математике. Као човек велике интуиције са ненадмашним осећајем и смислом за логичку прецизност у математичком расуђивању, свој живот је посветио истраживањима закона природе, како је сам истицао: „Природо, ти си моје божанство. Истраживањима твојих закона живот мој је посвећен“.

Генијално вешт да као посматрач феномена природе податке посматрања претвори у математичка средства, стварао је методе и теорије да би помоћу њих откривао законе. Допринео је да се заснује теорија функције комплексне променљиве и у вези са тим теорија елиптичних функција. Гаусова расправа о хипергеометријским редовима је од великог значаја за развитак теорије бесконачних редова. У теорији вероватноће и њеним применама познат је Гаусов закон расподеле вероватноћа, Гаусов алгоритам у линеарној алгебри, као теоријско и практично средство решавања система линеарних алгебарских једначина, а Гаусова метода најмањих квадрата теоријска је подлога у многим практичним применама математике. Писао је споро и концизно зато што је волео да својим радовима да такво савршенство да им се не може ништа додати и одузети и да на што мањем простору што више каже.

Гаус је рођен у Браунсвишком војводству (данас Немачка), у скромној породици, 30. априла 1777. године. Таленат за математику испољио је у детињству, али његов отац за то није имао разумевања. Већ као дете поседовао је чудесну моћ рачунања. У школи, Карлу је све било лако па се досађивао. Учитељ Бутнер је одлучио да га умири на дуже па му је задао да сабере све бројеве од 1 до 100. Али, Карло који је тада имао 7 година, одмах је одговорио да је то 5050, без да је то написао на папир. Посматрајући низ 1, 2, 3, ..., 98, 99, 100, уочио је законитост: када сабере 1 и 100, 2 и 99, 3 и 98 итд, увек добије збир 101. Таквих парова има 50 па је тражени збир једнак 5050. Овај поступак назван је *„Гаусов поступак“*.

Као средњошколац читао је Њутна, Ојлера и Лагранжа. Проучавајући њихове радове Гаус је сматрао да је Њутн од свих највећи. Војвода његовог родног града, наградио га је стипендијом за колеџ *Carolinum*, који је похађао од 1792. до 1795. године. По завршетку школовања у Брунсвику, где се већ у младим данима показао као надарен математичар откривши, истина већ познате, законитости попут биномне теореме или закона квадратног реципроцитета, Гаус 1795. прелази у Гетинген. И поред исказаног талента за математику, дуго се двоумио између математике и филологије. Желео је да се бави класичном филологијом. Свиђала му се помисао да напише коментар Вергилија, посебно силазак Енеја у подземље. С друге стране желео је да реши питање шта је број. Од 1795. године Гаус је размишљао да напише рад о бројевима. 1796. је показао да се сваки правилни полигон, чији су непарни фактори различити Фермаови прости бројеви, може конструисати помоћу лењира и шестара. Ово откриће било је веома важно на пољу математике: такви конструкциони проблеми окупирали су математичаре још у време старе Грчке. И сам Гаус је био толико задовољан што је успео да реши овај комплексан проблем, да је затражио да му се на надгробни споменик уграви ра правилни 17-тоугао. Погребник, ипак, није прихватио његов захтев због још несавршене технике гравирања.

Прекретница у његовом двоумљењу између математике и филологије настала је 1797. године, када почиње да води свој математички дневник, који данас за многе представља највеличанственији математички документ ***Disquisitiones Arithmeticae*** (Аритметичке расправе), ремек дело аритметике, штампано 1801. године. Обимом невелика ова бележница садржи 146 веома сажетих белешки, од којих свака представља једно поглавље у математици, које није лако протумачити. Том бележницом Гаус је показао да је за њега математика била усавршавање властитог бића и ништа више. Ово дело је камен темељац за заснивање теорије бројева као посебне математичке дисциплине, а дао јој је облик који и данас има. У њој је увео релацију конгруенције, што је олакшало решавање многих проблема. Француски математичар Луј Лагранж сматрао је да последње поглавље о једначинама, помоћу којих се дефинише подела круга, садржи најлепше аналитичко откриће које одавно није постигнуто. Ту је Гаус одредио правилно полигоне који се могу уписати у кружницу употребом лењира и шестара и тако је коначно решио један проблем који је поставила математика антике. Дирихле, један од најдаровитијих Гаусових ученика и врло истакнути математичар, посебно у теорији бројева, успео је да проучи, стваралачки усвоји и даље унапреди дубоке идеје које садржи Гаусово дело. Он је био први који је то дело разумео и открио га другима. Гаусова докторска дисертација (1799. године под менторством професора Пфафа) је нов допринос проучавању алгебарских једначина, у њој је доказ тзв. основне теореме алгебре која гласи: Сваки полином , над пољем комплексних бројева, степена већег или једнаког један има бар једну нулу у том пољу. Ова теорема има и другачију интерпретацију која гласи: сваки не-нула полином једне променљиве, са комплексним коефицијентима, има тачно онолико комплексних коренова колики му је степен, уколико се поновљени

корени рачунају у свом мултиплицитету. Математичари пре Гауса су само претпостављали да је то истина, али је он то и доказао. У току свог живота, дао је 4 потпуно различита доказа за ту теорему.

У двадесет трећој години постао је члан Петроградске академије наука, а убрзо и академија наука широм Европе. У двадесет петој години тачно је одредио путању планетоида Церес, побивши тврдњу филозофа Хегела да на небу не може бити више од седам планета. Путања једне звезде није било какво кретање већ нужни резултат деловања свих тела на једно појединачно у простору. Из веома скромних астрономских података успео је математичким путем, на основу закона гравитације, да одреди путању планетоида Церес који се био изгубио из вида астрономима. У Бремену је, у сарадњи са Беселом, сређивао Јупитерове табеле.

Немачки природњак Александар Хумболт писао је 1805. године владару Немачке Фридриху Вилхелму III: „Једини човек који Берлинској академији наука може дати нови сјај зове се Карл Фридрих Гаус“. Захваљујући својом научној активности изабран је за професора математике и астрономије на Универзитету Георг-Аугуст у Гетингену, као и за директора Гетингешке астрономске опсерваторије.

Године 1809. објављује другу књигу под називом *Theoria motus corporum coelestium in sectionibus conicis ambientium*, дводелну расправу о небеским телима. У првом делу расправља о диференцијалним једначинама и елиптичким путањама, а у другом делу објашњава како проценити, а након тога и тачно одредити путању планета. Теоријском астрономијом бавио се до 1817. године када се окреће геодетској проблематици. Гаус је 1813. године писао да се „У теорији паралелних линија није напредовало даље од Еуклида“ и да је то нечасни део математике који мора добити сасвим други облик. Исказ да се две паралеле не додирују никада није могао да се докаже и није очигледан. Простор допушта да ако човек има једну линију и једну тачку поред ње може бескрајно много паралела да се провуче кроз ту једну тачку. Проучавањем његове заоставштине констатовано је да је имао јасну слику о могућности да се изгради геометрија логички непротивречна и независна од петог Еуклидовог постулата.

Универзитет у Копенхагену га награђује 1822. године за дело *Theoria attractionis*. Рад *Theoria combinatuonis observationum erroribus minimis obnoxiae* (1823.) посвећен је математичкој статистици, посебно методи најмањих квадрата, према којој је најпогоднија вредност мерне величине за коју је збир квадрата погрешака најмањи. Године 1827. објавио је своје велико дело „Општа истраживања кривих површи“ којим је засновао диференцијалну геометрију као посебну дисциплину теоријске математике. Према „Славној теореми“, тако ју је Гаус назвао, при ма каквој деформацији површине која настаје без раскидања и растезања у било којој тачки површине не мења се вредност потпуне кривине површине. Допринео је теорији функције комплексне променљиве и у вези са тим теорији елиптичних функција. Гаусова расправа о хипергеометријским редовима је од великог значаја за развој теорије бесконачних редова. У теорији вероватноће и њеним применама познат је Гаусов закон расподеле вероватноћа до којег је дошао у својој теорији грешака, подстакнут теоријским и практичним проблемима којима се бавио у геодезији и астрономији. Познат је и Гаусов алгоритам у линеарној алгебри, као теоријско и практично средство решавања система линеарних алгебарских једначина.

У Гетингену је основао магнетску опсерваторију, а 1833. године конструисао је први магнетски телеграф, којим је била успостављена веза између магнетске и астрономске опсерваторије, коју је користио са својим пријатељем Вилхелмом Вебером. Земљино магнетно поље Гаус је измерио 1835. године новом математичком методом коју је развио управо за ту потребу и израчуната је вредност

магнетног момента (M). У теорији магнетизма Гаусово име остало је трајно обележено тако што је јединица за мерење магнетне индукције названа по њему.
Неколико распарава из више геодезије, које је објавио од 1843. до 1846. године, нашле су широку примену у геодезији. Гаус је одбацио елипсоид, односно сфероид као облик површине Земље и на основу астрономских и гравиметријских метода усвојио геоид као облик површине Земље. Занимала га је и картографија, посебно проблем да се у равни нацрта слика чији ће довољно мали делови бити слични одговарајућим деловима површине Земље. Гаус је развио основну теорију, а радне формуле извео је немачки геодета Л. Кригер. Гаус није публиковао свој метод директног пресликавања елипсоида на раван, који је први пут искоришћен за обраду резултата Хановерске триангулације у периоду 1820-1830. година. Теорију пресликавања Гаус је прво приказао својим студентима више геодезије, који су као официри радили на пословима триангулације Хановера, а његов асистент Голдшмит тада записује њене коначне формуле. Ове формуле такође се помињу у Гаусовим писмима познатом геодети тог времена Шумахеру, који их је објавио 1825. године у свом астрономском часопису. Касније је обраду Гаусових формула за пресликавање елипсоида на раван наставио тадашњи капетан, касније генерал и вишегодишњи шеф пруског државног премера др Оскар Шрајбер. Након Гаусове смрти научно друштво из Гетингена поверило је професору др Л. Кригеру да прегледа његову заоставштину. Л. Кригер је обрадио метод директног пресликавања елипсоида на раван и своје радове публиковао 1912. године у Потсдаму. С обзиром на допринос Л. Кригера пројекција добија назив Гаус-Кригерова.
Гаус је волео миран породичан живот, тако да бурна политичка и друштвена збивања изазвана Наполеоновим ратним походима, нису имала утицаја на његов рад. Гауса је тешко погодила Наполеонова окупација. Наполеон је одредио високе порезе, па је Гаус, као професор, морао плаћати 2000 франака, што је била велика сума. Многи су слали помоћ Гаусу, међу којима и Лаплас, али је Гаус презирао милосрђе и одбијао је сваку новчану помоћ. Аритметичке преокупације, наука, породица и дописивање са драгим пријатељима, су га чиниле срећним и ублажавале му бол у времену када је око себе видео само беду и очај.
Језици су му били притајена страст. Био је велики познавалац грчког и латинског. Толико је волео латински да је све своје радове објавио на том језику. Читао је Шекспира, Бајрона, Шилера, а у шездесетој години, за две године, научио је руски толико да је класике читао у оригиналу. Имао је врло критичке ставове према неким филозофима свог времена, који су се бавили филозофијом математике.
Иако велики геније живео је скромно, не напуштајући универзитет и астрономску опсерваторију у Гетингену. Био је необично нежан према мајци, која је слепа доживела дубоку старост. Први пут се оженио 1805. године Јоханом Остхоф са којом је имао троје деце. После њене смрти оженио се њеном пријатељицом Мином, са којом је имао двоје деце. Децом није био срећан, посебно са синовима. Једино је Јозеф био надарен за рачунање, док су остали имали авантуристичке склоности и расули се по свету. Његов пријатељ Сарториј Валтерсхаузен записао је у својим сећањима: „Какав је био у младости, такав је остао до старости и до последњих дана, непромењен и једноставан. Мала радна соба, мали радни сто са зеленим чаршавом, табла обојена бело, уски диван и после његових седамдест година наслоњача, засењена светиљка, неугрејани кревет, скромно јело, кућни капут и баршунаста капица, то су биле тако уобичајене све његове потребе“. Последње године живота провео је болестан, имао је проблема са срцем. Умро је 23.2.1855. године у Гетингену, који је припадао независном ханзеатском граду Хамбургу, данас Немачка .

Поводом Гаусове смрти краљ Хановера Џорџ V наложио је да се искује новац посвећен Гаусу као Краљу математичара. Истакнути немачки математичар Леополд Кронекер истиче да је скоро све што је математика 19. века постигла у својим научним идејама везано за Гауса.



# Литература


[1] Александар Липковски, “Линеарна алгебра и аналитичка геометрија“, Завод за уџбенике, Београд, 2007.
[2] Гојко Калајџић, “ Алгебра“, Математички факултет, Београд, 2004.
[3] Жарко Мијајловић, Зоран Петровић, Маја Рославцев, “ Дискретне структуре 1“, http://poincare.matf.bg.ac.rs/~zoranp/2014-15/DS1.pdf
[4] Зоран Огњеновић, “Скрипта предмета дискретна математика“, Математички факултет, Београд, 2010-2011.
[5] Prof. Bernhard Esslinger (co-author and editor) and the CrypTool Development Team, The CrypTool Script: “Cryptography, Mathematics, and More ", 1998-2010 Frankfurt am Main, Germany.
[6] N. Koblitz, “Cryptograpy as a teaching tool", Cryptologia 21 (1997) 317–326. http://www.math.washington.edu/~koblitz/crlogia.html
[7] William Stalings, “Cryptography and Network Security Principles and Practices", Book Prentice Hall, ISBN 100131873164, 4th edition, London, Nov. 2005, pp. 298
[8] Драган Спасић, “Криптозаштита података у рачунарским мрежама применом симетричних и асиметричних криптосистема “, Дирекција за поштански саобраћај.
[9] Славик Јаблан, Љиљана Радовић , “Визуелна комуникација кроз визуелну математику“ ,Часопис Филомат, 23:2 (2009), пп. 56-67
[10] Jill Britton , “Modular art ", http://britton.disted.camosun.bc.ca
[11] Милан Божић, “Преглед историје и филозофије математике“ “, Завод за уџбенике, Београд, 2010.