ΑΚΕΡΑΙΟΙ ΑΡΙΘΜΟΙ

1. Εσωτερικές πράξεις ορισμοί. (Βλέπε και [ZK], σελ. 36).
Μία απεικόνιση f: $A\times A \to A$ ($A \neq \varnothing$) καλείται ***εσωτερική πράξη*** επί του Α. Αντί να σημειώνουμε με το f(α,β) την εικόνα του στοιχείου $(\alpha,\beta)\in A$, γράφουμε αfβ. Στην γραφή αυτή, αντί του συμβόλου f, που δηλώνει την πράξη μας, χρησιμοποιούμε σύμβολα, ως τα "+" (πρόσθεση), "$\circ$" (πολλαπλασιασμός), ή "$*$". Συνήθως, το πολλαπλασιαστικό σύμβολο ανάμεσα σε δύο στοιχεία του Α, παραλείπεται. Το $(A,*)$ καλείται ***δομή μιάς εσωτερικής πράξεως***.
Μία εσωτερική πράξη λέγεται ***προσεταιριστική***, αν και μόνον αν, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ οπότε γράφουμε απλά αβγ, για κάθε $\alpha,\beta,\gamma\in A$.

Ομαδοειδές καλείται μία δομή μιάς εσωτερικής πράξεως.

Ημιομάδα καλείται μία δομή μιάς προσεταιριστική εσωτερικής πράξεως.

Ένα στοιχείο $e\in A$, αν υπάρχει, για το οποίο ισχύει ότι $\forall\alpha\in A$, $e\alpha = \alpha$, καλείται ***αριστερά μοναδιαίο στοιχείο*** του Α. Φανερός είναι ο ορισμός του ***δεξιά μοναδιαίου στοιχείου***. ***Ουδέτερο*** στοιχείο του Α είναι το $e\in A$, αν και μόνον αν είναι ταυτόχρονα αριστερά και δεξιά μοναδιαίο στοιχείο. Συμβολίζουμε το e με το 1, όταν βέβαια δεν υπάρχει η πιθανότητα συγχύσεως του ουδετέρου στοιχείου e με τον αριθμό 1. Μία ημιομάδα με ουδέτερο στοιχείο, την καλούμε επίσης και ***ημιομάδα με μονάδα***. ***Αριστερά αντίστροφο*** στοιχείο, του τυχόντος στοιχείου α μιάς ημιομάδας με ουδέτερο στοιχείο, καλείται το στοιχείο α^{-1} για το οποίο ισχύει ότι, $\alpha^{-1}\alpha = e$. Ανάλογα ορίζεται το ***δεξιά αντίστροφο*** στοιχείο. Στην περίπτωση, που το α^{-1} είναι και αριστερά και δεξιά αντίστροφο στοιχείο του α, καλείται απλά ***αντίστροφο*** στοιχείο του α. Θέτουμε $\alpha^n = \alpha\alpha^{n-1}$. Ισχύει ότι, $\alpha^n\alpha^m = \alpha^{n+m} = \alpha^m\alpha^n$.

Μορφισμοί ή ***ομομορφισμοί*** καλούνται γενικώς, οι συναρτήσεις, που διατηρούν την δομή του πεδίου ορισμού τους. ***Επιμορφισμοί***, λέγονται οι μορφισμοί $f : A \to B$, που είναι επί, δηλαδή, f(A) = B. ***Ενδομορφισμοί***, οι μορφισμοί f, που είναι εντός, δηλαδή, $f(A) \subset B$. ***Μονομορφισμοί***, καλούνται οι μορφισμοί, που είναι ένα-ένα απεικονίσεις. ***Ισομορφισμοί***, καλούνται οι επιμορφισμοί που, είναι επιπλέον και μονομορφισμοί (είναι δηλαδή, bijective).

2. Ορισμός ομάδος. ***Ομάδα*** G, καλείται μία ημιομάδα με μονάδα μέσα στην οποία, για δοσμένα $\alpha,\beta\in G$ οι εξισώσεις $\alpha x = \beta$ και $y\alpha = \beta$, έχουν μοναδική λύση $x, y\in G$.

Πορίσματα. i) $\alpha\beta_1 = \alpha\beta_2 \to \beta_1 = \beta_2$ και $\beta_1\alpha = \beta_2\alpha \to \beta_1 = \beta_2$. Τούτο έπεται από την μοναδικότητα των λύσεων $x, y\in G$. ii) Αν στις εξισώσεις $\alpha x = \beta$ και $y\alpha = \beta$ λάβουμε $\beta = e$, συμπεραίνουμε ότι, κάθε $\alpha\in G$ έχει αριστερά και δεξιά αντίστροφο στοιχείο.

Πρόταση. Η μονάδα μιάς ομάδας είναι μοναδική.
Απόδειξη. Από τον ορισμό της ομάδας έχουμε ότι, η εξίσωση $\alpha e_\alpha = \alpha$ έχει την μοναδική λύση e_α. Θα δείξουμε κατ' αρχήν, ότι το στοιχείο e_α δεν εξαρτάται από το συγκεκριμένο $\alpha\in G$. Προς τούτο, αν $\beta\in G$ και y το μοναδικό στοιχείο της G για το οποίο είναι $y\alpha = \beta$, τότε έχουμε και ότι, $\beta e_\alpha = (y\alpha)\, e_\alpha = y(\alpha e_\alpha) = y\alpha = \beta$. Αν το e_α είναι, λοιπόν, δεξιά μοναδιαίο στοιχείο για το $\alpha\in G$, είναι τότε και δεξιά μοναδιαίο στοιχείο για το $\beta\in G$. (Ίδια ισχύουν και για ένα αριστερά μοναδιαίο στοιχείο). Έστω, τώρα, τα μοναδικά e_1 και e_2, για τα οποία ισχύει για όλα τα $\alpha\in G$ ότι, $\alpha e_1 = \alpha$ και $e_2\alpha = \alpha$. Λαβαίνουμε ως α το γινόμενο $e_1 e_2$.
Είναι, τότε, $(e_1 e_2)e_1 = e_1 e_2$ και $e_2(e_1 e_2) = e_1 e_2$. Άρα και, $(e_1 e_2)e_1 = e_2(e_1 e_2)$.
Ή $(e_1 e_2)e_2 = e_1(e_1 e_2)$. Ή $e_2 e_2 = e_1$, e_1 ή $e_1 = e_2$.

Πρόταση. Κάθε στοιχείο $\alpha \in G$ έχει ένα και μόνον αντίστροφο στοιχείο α^{-1}.
Απόδειξη. Θα δείξουμε ότι, $\forall \alpha \in G, \exists!\ \alpha^{-1} \in G: \alpha\alpha^{-1} = \alpha^{-1}\alpha = e$. Από τον ορισμό της ομάδας, γνωρίζουμε ότι υπάρχουν μοναδικά α΄ και α΄΄∈G τέτοια ώστε, αα΄ = e και α΄΄α = e. Είναι, όμως, α΄΄αα΄= α΄΄(αα΄) = α΄΄e = α΄΄ και α΄΄αα΄ = (α΄΄α)α΄ = eα΄ = α΄. Άρα α΄ = α΄΄.

Πόρισμα. α) $\left(\alpha^{-1}\right)^{-1} = \alpha$. β) $e^{-1} = e$. γ) $(\alpha_1\alpha_2 \cdots \alpha_n)^{-1} = \alpha^{-1} \cdots \alpha_n{}^{-1}$ δ) Η αντιστοιχεία $\alpha \mapsto \alpha^{-1}$ είναι ένα-ένα και επί.

Παράδειγμα. Θεωρούμε το σύνολο των αυτομορφισμών ενός συνόλου U. Φανερά, η σύνθεση δύο αυτομορφισμών του U είναι πάντοτε δυνατή. Ορίζεται λοιπόν μέσα στο σύνολο αυτό, μία εσωτερική πράξη, ο πολλαπλασιασμός δύο στοιχείων του. Μέσα στο σύνολο των αυτομορφισμών του U, συγκαταλέγεται και η ταυτοτική απεικόνιση $1_U : U \to U$, που ορίζεται από την σχέση, $\forall x \in U, 1_U(x) = x$. Στην περίπτωση, που ο αυτομορφισμός είναι μετάθεση f, υπάρχει και η αντίστροφή της f^{-1}. Το σύνολο συνεπώς των μεταθέσεων του U, με πράξη την σύνθεση, αποτελεί ομάδα.

Υποομάδα Η της G, είναι ένα υποσύνολο της G, τέτοιο ώστε, $\forall \alpha, \beta \in H$, $\alpha\beta \in H$ και $\forall \alpha \in H$, $\alpha^{-1} \in H$. ***Αντιμεταθετική*** ή ***Αβελιανή*** λέγεται η ομάς G, αν και μόνον αν, οι μοναδικές λύσεις x, y∈G είναι και ίσες. Στην περίπτωση αυτή, ∀α, β∈G, ισχύει ότι, αβ = βα.

Σημειώσει επί του συμβολισμού. Στην περίπτωση Αβελιανής ομάδας, σημειώνουμε πάντα την πράξη με το "+", το ουδέτερο στοιχείο με το "0" (μηδέν), και το αντίστροφο στοιχείο του α με το "–α" (αντίθετο). Γράφουμε α–β αντί του (σωστού) α+(–β). Αυτό είναι η μοναδική λύση x∈R της εξίσωσης α+x = β. Φανερά, λόγω της αντιμεταθετικότητας της προσθέσεως, ισχύει ότι, $\alpha - (\beta_1 + \beta_2) = \alpha - \beta_1 - \beta_2$.

Ομάς μεταθέσεων. Μία ***διάταξης,*** είναι η εικόνα μιάς μεταθέσεως. Θεωρούμε το σύνολο S_p των μεταθέσεων επί του S. Ορίζουμε το γινόμενο δύο διατάξεων από την παρακάτω σχέση. $\forall p_1, p_2 \in S_p$, $p_2 p_1 = p$, όπου p η μετάθεση του S, που ορίζεται από την σχέση,
$\forall x \in S, p(x) = p_1(p_2(x))$. Η πράξη "γινόμενο" που ορίσαμε, καθιστά το S_p ομάδα.
Ουδέτερο στοιχείο της ομάδας αυτής, είναι η ταυτοτική μετάθεση, για την οποία ισχύει ότι $\forall x \in S,\ p_i(x) = x$.

Στην περίπτωση, που το σύνολο S είναι ένα πεπερασμένο σύνολο με n το πλήθος στοιχεία $x_1, x_2, \cdots x_n$, όταν αυτό χρησιμοποιείται ως πεδίον ορισμού της p, το θέτουμε πάντα στην μορφή S = {1, 2, . . . , n}. Το σύνολο τιμών είναι τότε, το σύνολο
p(S) = {p(1), p(2), . . . , p(n)} όπου το p(i) = j, με i, j∈S. για να δηλώσουμε την μετάθεση p, χρησιμοποιούμε και τον συμβολισμό

$$p = \begin{pmatrix} 1 & 2 & \cdots & n \\ p(1) & p(2) & \cdots & p(n) \end{pmatrix}.$$

Το σύνολο p(S) καλείται και διάταξη του S. Φανερά, το σύνολο των διατάξεων, βρίσκεται σε αντιστοιχία ένα-ένα και επί, με το σύνολο των μεταθέσεων. Το σύνολο συνεπώς S_p έχει τόσα στοιχεία, όσες είναι οι διατάξεις των n αντικειμένων 1, 2, . . . , n. Το πλήθος αυτό, βρίσκεται ως εξής: Μία διάταξη προκύπτει, αν θεωρήσουμε ότι έχουμε n θέσεις, οι οποίες γεμίζονται μία προς μία από τα στοιχεία 1, 2, κλπ, ένα στοιχείο σε κάθε θέση. Η πρώτη θέση πληρούται κατά n

διαφορετικούς τρόπους, η δεύτερη κατά n−1, κοκ, η n-στη κατά ένα τρόπο. Το πλήθος, λοιπόν, των διαφορετικών τρόπων με τους οποίους γεμίζουν οι n θέσεις είναι n(n−1) … 1 και συμβολίζεται με n!.
Κάνοντας χρήση του παραπάνω συμβολισμού για την μετάθεση p, μπορούμε πολύ εύκολα να βρούμε το γινόμενο δύο μεταθέσεων. για παράδειγμα, αν έχουμε να βρούμε το p_1p_2, όπου

$$p_1=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\quad p_2=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad \text{γράφουμε,}$$

$$p_1p_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}3&1&2\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}.$$

3. Δακτύλιοι - ακέραιες περιοχές. Ένας ***Δακτύλιος,*** είναι μία δομή δύο εσωτερικών πράξεων: Τον πολλαπλασιασμό, και την πρόσθεση. Ως προς τον πολλαπλασιασμό, η δομή R είναι ομαδοειδές. Ως προς την πρόσθεση η R είναι αβελιανή ομάδα. Οι δύο αυτές πράξεις συνδέονται με τους ***επιμεριστικούς νόμους,*** που είναι οι:

$$\forall\alpha,\beta,\gamma\in R,\ \alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma \ \text{ και } \ (\beta+\gamma)\alpha=\beta\alpha+\beta\gamma.$$

Συνήθως, αντί για ομαδοειδές λαβαίνουμε ημιομάδα. Τότε έχουμε έναν ***προσεταιριστικό δακτύλιο***. Αν επιπλέον η ημιομάδα είναι και αντιμεταθετική, τότε έχουμε έναν ***προσεταιριστικό-αντιμεταθετικό δακτύλιο***. Αν αντί για ημιομάδα έχουμε ομάδα (με πράξη τον πολλαπλασιασμό) τότε λέμε, ότι έχουμε δακτύλιο με μονάδα, η οποία βέβαια είναι και μοναδική, και συμβολίζεται, συνήθως, με το 1. Στην περίπτωση ημιομάδας, τα αντίστροφα στοιχεία καλούνται ***μονάδες.***

Πόρισμα. Συνέπεια της ισότητας γ+β−γ = β είναι οι σχέσεις α(β−γ) = αβ−αγ
και (β−γ)α = βγ−γα.

Κάθε αβελιανή ομάδα G είναι δυνατόν να θεωρηθεί ότι αποτελεί την αβελιανή ομάδα του δακτυλίου R, που ορίζεται ως εξής:
α) Τα στοιχεία του R είναι ακριβώς αυτά της G.
β) Το ομαδοειδές του R ορίζεται από την σχέση: $\forall\alpha,\beta\in R,\ \alpha\beta=0$.
Αυτός ο δακτύλιος R, καλείται ***μηδενικός δακτύλιος***.

Πρόταση. α) $\forall\alpha\in R,\ \alpha0=0\alpha=0$. β)$\forall\alpha\in R,\ (-1)\alpha=-\alpha$.
Απόδειξη. α) Αν $x\in R$, $0=x-x$. Άρα και, $\alpha0=\alpha(x-x)=\alpha x-\alpha x=0$.
β) $1\alpha+(-1)\alpha=(1-1)\alpha=0\alpha=0$. Το $(-1)\alpha$ είναι, λοιπόν, ένα αντίθετο στοιχείο του $\alpha\in R$. Το αντίθετο στοιχείο του α είναι όμως μοναδικό. Άρα $(-1)\alpha=-\alpha$.

Πρόταση. Σε κάθε προσεταιριστικό δακτύλιο ισχύει ότι, $\forall\alpha,\beta\in R,\ (-\alpha)(-\beta)=\alpha\beta$.
Απόδειξη. Είναι, $\alpha\beta+(-\alpha)\beta+(-\alpha)(-\beta)=(\alpha-\alpha)\beta+(-\alpha)(-\beta)=(-\alpha)(-\beta)$ και
$\alpha\beta+(-\alpha)\beta+(-\alpha)(-\beta)=\alpha\beta+(-\alpha)(\beta-\beta)=\alpha\beta$.

Έστω ότι μας δίδεται ένας προσεταιριστικός δακτύλιος R (και από εδώ και εξής, όταν λέμε "δακτύλιος" θα εννοούμε "προσεταιριστικός δακτύλιος"). Μπορούμε τότε, πάνω σ' αυτόν να κατασκευάσουμε έναν άλλο, ως εξής: α) Διατηρούμε την δομή (R,+) ως έχει, και ορίζουμε έναν νέο πολλαπλασιασμό "$\circ$", θέτοντας $\alpha\circ\beta=\alpha\beta-\beta\alpha$. Η δομή $(R,+,\circ)$ που λαβαίνουμε κατ' αυτόν τον τρόπο, καλείται ***δακτύλιος Lie*** R^-.
β) Διατηρούμε την δομή (R,+) ως έχει, και ορίζουμε έναν νέο πολλαπλασιασμό "$\bullet$", θέτοντας $\alpha\bullet\beta=\alpha\beta+\beta\alpha$. Η δομή $(R,+,\bullet)$ που λαβαίνουμε κατ' αυτόν τον τρόπο, καλείται ***δακτύλιος Jordan*** R^+. Μέσα σε ένα δακτύλιο του Lie ισχύουν οι ταυτότητες:
i) $\forall\alpha,\beta\in R^-,\ \alpha\circ\beta=-\beta\alpha$. ii) $(\alpha\circ\beta)\circ\gamma+(\beta\circ\gamma)\circ\alpha+(\gamma\circ\alpha)\circ\beta=0$ (ταυτότητα του Jacobi).
Μέσα σε ένα δακτύλιο του Jordan ισχύουν οι ταυτότητες:

i) $\forall \alpha,\beta \in R^+$, $\alpha \bullet \beta = \beta \bullet \alpha$. ii) $[(\alpha \bullet \alpha) \bullet \beta] \bullet \alpha = (\alpha \bullet \alpha) \bullet (\beta \bullet \alpha)$.

Θέτουμε $\alpha^0 = 1$. για n όρους α, γράφουμε, $\alpha + \ \ldots \ + \alpha = n\alpha$. Γράφουμε, ακόμα,

$$\alpha_1 + \ \ldots \ + \alpha_n = \sum_{i=1}^{n} \alpha_i .$$

Ισχύει ότι $(\alpha_1 + \ \ldots \ + \alpha_n)(\beta_1 + \ \ldots \ + \beta_n) = \left(\sum_{i=1}^{n} \alpha_i \right) \left(\sum_{j=1}^{m} \beta_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_i \beta_j$, συνολικά mn όρους.

Πρόταση. Σε κάθε δακτύλιο, αν ένας από τους παράγοντες ενός γινομένου είναι ο 0, τότε το γινόμενο ισούται με 0.
Απόδειξη. Πράγματι είναι, $\alpha 0 = \alpha(x - x) = \alpha x - \alpha x = 0$.

Το αντίστροφο δεν ισχύει πάντα. Μπορούμε, δηλαδή, μέσα σε ένα δακτύλιο να έχουμε ότι $\alpha \neq 0$, $\beta \neq 0$, αλλά $\alpha\beta = 0$. Λέμε στην περίπτωση αυτή, ότι έχουμε ***διαιρέτες του μηδενός***. για παράδειγμα, το σύνολο των πραγματικών συναρτήσεων, που ορίζεται επί ενός συνόλου Α, και το οποίο γίνεται δακτύλιος αν ορίσουμε την πρόσθεση και τον πολλαπλασιασμό θέτοντας, $\forall x \in A$, $(f+g)(x) = f(x)+g(x)$ και $(fg)(x) = f(x)g(x)$, έχει διαιρέτες του μηδενός. Ουδέτερο στοιχείο, εδώ, για την πρόσθεση, είναι η f_0, για την οποία, $\forall x \in A$, $f_0(x) = 0$. για να βρούμε διαιρέτες του μηδενός μέσα σ' αυτόν τον δακτύλιο, αρκεί να λάβουμε έναν ***μερισμό*** του Α σε δύο υποσύνολά του Φ και Γ, (είναι, δηλαδή, $\Phi \cap \Gamma = \varnothing$ και $\Phi \cup \Gamma = A$) και να θεωρήσουμε την f έτσι ώστε, $\forall x \in \Phi$, $f(x) = 0$ ενώ $\forall x \in \Gamma$, $f(x) \neq 0$ και την g έτσι ώστε, $\forall x \in \Gamma$, $g(x) = 0$ ενώ $\forall x \in \Phi$, $g(x) \neq 0$. Φανερά, έχουμε τότε, $f, g \neq f_0$, ενώ $fg = f_0$.

Μέσα σε έναν ***αντιμεταθετικό δακτύλιο με μονάδα*** Δ, ισχύουν συνεπώς οι ιδιότητες:
1) $\forall\ \alpha, \beta \in \Delta$ $\alpha+\beta$ και $\alpha\beta \in \Delta$ (κλειστότητα των πράξεων).
2) Αν $\alpha' = \alpha$ και $\beta' = \beta$, τότε και $\alpha+\beta = \alpha'+\beta'$ και $\alpha\alpha' = \beta\beta'$ (οι πράξεις είναι καλά ορισμένες).
3) $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$ και $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ (προσεταιρισμός).
4) $\alpha+\beta = \beta+\alpha$ και $\alpha\beta = \beta\alpha$ (αντιμετάθεση).
5) $\alpha(\beta+\gamma) = \alpha\beta+\alpha\gamma$ (επιμερισμός).
6) $\exists\ 0 \in \Delta$, με $\alpha+0 = 0+\alpha\ \forall \alpha \in \Delta$.
7) $\exists\ 1 \neq 0\ \in \Delta$, με $1\alpha = \alpha 1$, $\forall \alpha \in \Delta$.
8) $\exists\ x \in \Delta$: $\forall \alpha \in \Delta$, $x+\alpha = 0$.

Οι παραπάνω ιδιότητες, είναι αρκετές για να μας εξασφαλίσουν τον λογισμό μέσα στον δακτύλιο Δ.

Ένας αντιμεταθετικός δακτύλιος καθίσταται ***ακεραία περιοχή*** D (integral Domain) ανν μέσα σ' αυτόν ισχύει ***ο νόμος της διαγραφής***: $\alpha\gamma = \alpha\beta \rightarrow \gamma = \beta$. Ο νόμος της διαγραφής, είναι ισοδύναμος με την πρόταση: Αν $\alpha\beta = 0$, τότε είτε $\alpha = 0$, είτε $\beta = 0$. (**Απόδειξη.** α) Ισχύει ο νόμος της διαγραφής. Τον εφαρμόζουμε στην σχέση $\alpha\beta = 0 = \alpha 0$, $\alpha \neq 0$. Προκύπτει ότι $\beta = 0$.
β) Ισχύει ότι η $\alpha\beta = 0 \rightarrow$ είτε $\alpha = 0$ είτε $\beta = 0$. Τότε, η $\alpha\beta = \alpha\gamma \rightarrow \alpha(\beta-\gamma) = 0$. Άρα για $\alpha \neq 0$, $(\beta-\gamma) = 0$, δηλαδή, $\beta = \gamma$). Μέσα σε μία ακέραια περιοχή, δεν έχουμε συνεπώς ***διαιρέτες του μηδενός***.

Μία δομή Δ με δύο πράξεις, μπορούμε να την διατάξουμε ολικά, αν επιλέξουμε μέσα σ' αυτήν, το σύνολο των θετικών της στοιχείων P (ο ***θετικός κώνος*** P, βλέπε, [ZK], σελ. 137).
$P = \{x \in \Delta \mid \alpha)$ Το άθροισμα (αντ. γινόμενο) δύο στοιχείων του P, είναι στοιχείο του P. β) είτε $x \in P$, είτε $-x \in P$, είτε $x = 0\}$. Ορίζουμε στην συνέχεια την διάταξη "$\leq$ " από την σχέση, $\alpha \leq \beta$ ανν είτε $\alpha = \beta$ είτε $\beta - \alpha \in P$. Η διάταξη αυτή, έτσι όπως ορίστηκε, είναι συμβατή με τις

εσωτερικές πράξεις της δομής. Το σύνολο P, δεν είναι κενό, μια και περιέχει το τετράγωνο παντός στοιχείου της Δ.

Υποθέτουμε τώρα επιπλέον, ότι η ακέραια περιοχή D, είναι "***καλά***" διατεταγμένη. Τούτο σημαίνει ότι, το τυχόν μη κενό υποσύνολο του P, έχει ελάχιστο στοιχείο.

4. Το σύνολο $\mathbb{N}$ των φυσικών αριθμών.

Ιστορική σημείωση. Οι ***φυσικοί αριθμοί*** προέκυψαν από την ανάγκη του ανθρώπου να απαριθμήσει αντικείμενα. Ο πρώτος που κατέγραψε τις ιδιότητες εκείνες των φυσικών αριθμών, οι οποίες είναι αρκετές για να τους ορίσουν, ήταν ο Peano. Γεννήθηκε στις 27 Αυγούστου του 1858 στο Cuneo, Sardinia και πέθανε 20 Απριλίου 1932 στο Τουρίνο, Ιταλία. Γνωστός για την συμβολή του στην Μαθηματική Λογική.

Αξιώματα του Peano.

P1. Υπάρχει ένα σύνολο μη κενό $\mathbb{N}$, το οποίο θα καλούμε σύνολο των φυσικών αριθμών.

P2. Ορίζεται η αντιστοιχία ένα - ένα και εντός $+ : \mathbb{N} \to \mathbb{N}$. Αν $a \in \mathbb{N}$, το $+(a)$ θα το συμβολίζουμε με a^+, και θα το καλούμε επόμενο στοιχείο του a, το οποίο θα καλείται προηγούμενο του a^+.

P3. Η εικόνα Im(+) της +, είναι γνήσιο υποσύνολο του $\mathbb{N}$.

P4. ***Αρχή της επαγωγής.*** Κάθε σύνολο του $\mathbb{N}$ που περιέχει ένα στοιχείο, το οποίο δεν έπεται κανενός και περιέχει το επόμενο στοιχείο οιουδήποτε στοιχείου του, ταυτίζεται με το σύνολο $\mathbb{N}$. [Το $\mathbb{N}$ είναι, λοιπόν, όπως αποδεικνύεται παρακάτω, σύνολο ***καλά διατεταγμένο.***]

Το P4. είναι η βάση της αποδεικτικής μεθόδου, που καλείται ***επαγωγική μέθοδος.*** Αυτή χρησιμοποιείται για να ορίζουμε έννοιες και να αποδεικνύουμε προτάσεις.

Η μέθοδος αυτή συνοψίζεται στα εξής: Έστω ότι για κάποιο φυσικό n έχουμε την λογική πρόταση $\varphi(n)$ και θέλουμε να μάθουμε αν αυτή αληθεύει για κάθε n. Προς τούτο, ελέγχουμε την $\varphi(1)$, και αν αληθεύει, υποθέτουμε ότι η $\varphi(n)$ αληθεύει, και αποδεικνύουμε (ή ορίζουμε ότι) και η $\varphi(n+1)$ αληθεύει. Η πρόταση, τότε, ισχύει για κάθε φυσικό αριθμό n.

Επειδή $\mathrm{Im}(+) \subset \mathbb{N}$ έπεται ότι υπάρχουν στοιχεία $x \in \mathbb{N}$, με $x \notin \mathrm{Im}(+)$. Άρα το x δεν έπεται κανενός στοιχείου του $\mathbb{N}$. Έστω ότι υπάρχει και ένα άλλο στοιχείο $y \in \mathbb{N}$ με την ίδια ιδιότητα. Θεωρούμε, τότε, τα δύο σύνολα $\{x\} \cup \mathrm{Im}(+)$ και $\{y\} \cup \mathrm{Im}(+)$. Και τα δύο πληρούν το P4, άρα συμπίπτουν. **Συμπέρασμα.** Το στοιχείο εκείνο του $\mathbb{N}$ που δεν έπεται κανενός άλλου στοιχείου του $\mathbb{N}$ είναι μονοσημάντως ορισμένο. Το μοναδικό αυτό στοιχείο, το συμβολίζουν με 1. Το 1^+ λόγω του P2 είναι μοναδικό, και συμβολίζεται με 2, κ.ο.κ. Το σύνολο {1, 2, . . . } πληροί το P4, και συνεπώς συμπίπτει με το $\mathbb{N}$.

Ορίζουμε τις πράξεις "+" και "·" εν $\mathbb{N}$ ως εξής:

α) $+(1, y) = y^+$. Γράφουμε και $1 + y = y^+$, για κάθε $y \in \mathbb{N}$.

β) $+(x^+, y) = (x + y)^+$. Γράφουμε και $x^+ + y = (x + y)^+$, για κάθε $x, y \in \mathbb{N}$.

γ) $\cdot(1, y) = y$. Γράφουμε και $1 \cdot y = y$, για κάθε $y \in \mathbb{N}$.

δ) $\cdot(x^+, y) = \cdot(x, y) + \cdot(1, y)$. Γράφουμε και $(x + 1) \cdot y = xy + y$, για κάθε $x, y \in \mathbb{N}$.

Το "·" συνήθως παραλείπεται κατά την αναγραφή των σχέσεων.

Ισχύουν οι ιδιότητες για κάθε $x, y, z \in \mathbb{N}$:

$(x + y) + z = x + (y + z)$ και $(xy)z = x(yz)$. Προσεταιριστικός νόμος.

$x + y = y + x$ και $xy = yx$. Αντιμεταθετικός νόμος.

$x + z = y + z \to x = y$ και $xz = yz \to x = y$. Νόμος της διαγραφής.

$(x+y)z = xz + yz$. Επιμερισμός του πολλαπλασιασμού ως προς την πρόσθεση. Το αντίστροφο δεν ισχύει.
Οι φυσικοί αριθμοί, αποτελούν αντιμεταθετική ημιομάδα και ως προς την "+" και ως προς τον "·". Έχουν επιπλέον και μοναδιαίο στοιχείο, το 1.

για να αποδειχθεί ο νόμος της διαγραφής, είναι αναγκαίο να εισαχθεί η έννοια της διατάξεως μέσα στους φυσικούς αριθμούς, ως εξής: $x < y \leftrightarrow \exists z \in \mathbb{N}$, με $y = x + z$ (ημιδιάταξη) και $x \le y \leftrightarrow$ είτε $x < y$ είτε $x = y$. Χρησιμοποιούμε και τις " $>$ " και " $\ge$ " με το προφανές νόημα. Υποθέτουμε, τώρα, ότι $x < y$. Είναι, τότε, και $x = y + z$ και λόγω του μονοσήμαντου της προσθέσεως, $x^+ = (y+z)^+ = 1 + (y+z) = (1+y) + z = y^+ + z$.

Άρα, $x < y \rightarrow x^+ < y^+$ (1).
Εξ' άλλου, $\forall x \in \mathbb{N}$, $x \neq 1$, $1 < x$. Άρα, λόγω του P4, η " $<$ " επεκτείνεται σε ολόκληρο το $\mathbb{N}$. Το $\mathbb{N}$ είναι συνεπώς ολικά διατεταγμένο σύνολο.

για κάθε $x, y, z \in \mathbb{N}$, ισχύουν οι σχέσεις:
Δ1. Η $x > y$, αποκλείει την $x \le y$.
Δ2 $x \le y$ και $y \le x \rightarrow x = y$.
Δ3. $\forall (x, y) \in \mathbb{N} \times \mathbb{N}$, μία και μόνον από τις $x < y$, $x = y$, $x > y$ ισχύει.
Δ4. $x + z \le y \rightarrow x \le y$.
Δ5. Επαγωγικά, λόγω της (1), έχουμε, $x \le y \rightarrow x + z \le y + z$ και $x \le y \rightarrow xz \le yz$. Λέμε ότι οι πράξεις είναι συμβατές με την διάταξη.
Δ6. Η $x < y$ αποκλείει την $x^+ > y$.
Δ7. $x < y \rightarrow x^+ \le y$.

Αρχή της καλής διάταξης. Κάθε μη κενό υποσύνολο Κ των φυσικών αριθμών, περιέχει ελάχιστο στοιχείο.
Απόδειξη. Έστω $\varnothing \neq K \cap \mathbb{N}$ και $\forall x \in K$, $M = \{y \in \mathbb{N}, \text{ με } y \le x\}$. Φανερά, $1 \in M$. Αν $x \in K$, τότε και $x^+ > x$, και, συνεπώς, $x^+ \notin M$. Είναι, λοιπόν, $M \neq \mathbb{N}$, και συνεπώς, υπάρχει $m \in M$, με $m^+ \notin M$, διότι άλλως θα έπρεπε λόγω P4 να είναι, $M = \mathbb{N}$. Θα δείξουμε ότι, το m είναι το ελάχιστο στοιχείο του Κ. Πράγματι, $m \in M \rightarrow \forall x \in K$, $m \le x$. Παρατηρούμε, τώρα, ότι οι σχέσεις $m < x$, και $m > x$ αποκλείονται, μιά και $m \le x$, και αν $m < x$, τότε και $m^+ \le x$, οπότε και $m^+ \in M$, άτοπον. Άρα $x = m$ για κάποιον $x \in K$. Άρα $m \in K$. Το m είναι, λοιπόν, το ελάχιστο στοιχείο του Κ. Συγχρόνως δείξαμε και ότι $M \cap K = \{m\}$.

Δεύτερη αρχή της επαγωγής. Έστω ότι για κάποιο φυσικό αριθμό n ισχύει η πρόταση $\varphi(n)$. Αν $\exists m \in \mathbb{N}$, τέτοιος ώστε, η υπόθεση ότι η $\varphi(k)$ είναι αληθείς $\forall k \in \mathbb{N}$, $k < m$, συνεπάγεται ότι η $\varphi(k)$ είναι αληθείς, τότε η $\varphi(n)$ είναι αληθείς για κάθε φυσικό αριθμό n.
Απόδειξη. Έστω S το σύνολο των φυσικών, για τους οποίους η $\varphi(n)$ είναι ψευδής. Αν $S \neq \varnothing$, τότε το S έχει ελάχιστο στοιχείο m. για κάθε $k \in \mathbb{N}$, $k < n$, η $\varphi(k)$ είναι αληθής. Άρα και η $\varphi(n)$ αληθής, άτοπον. Η υπόθεση $S \neq \varnothing$ οδηγεί σε άτοπον. Άρα, $S = \varnothing$. και συνεπώς η $\varphi(n)$ ισχύει για κάθε n. Παρατηρούμε ότι, για m = 1, το σύνολο $\{k \in \mathbb{N}, k < m\} = \varnothing$. Η $\varphi(1)$ θα πρέπει συνεπώς, να αποδεικνύεται χωριστά.

Υπενθυμίζουμε ότι, η αρχή της καλής διάταξης, η αρχή της επαγωγής, και η αρχή της επιλογής, είναι προτάσεις ισοδύναμες.

Παράδειγμα. Με την μέθοδο της επαγωγής, αποδεικνύεται ότι:

α) $1+2+\ \ldots\ +n=\dfrac{n(n+1)}{2}$

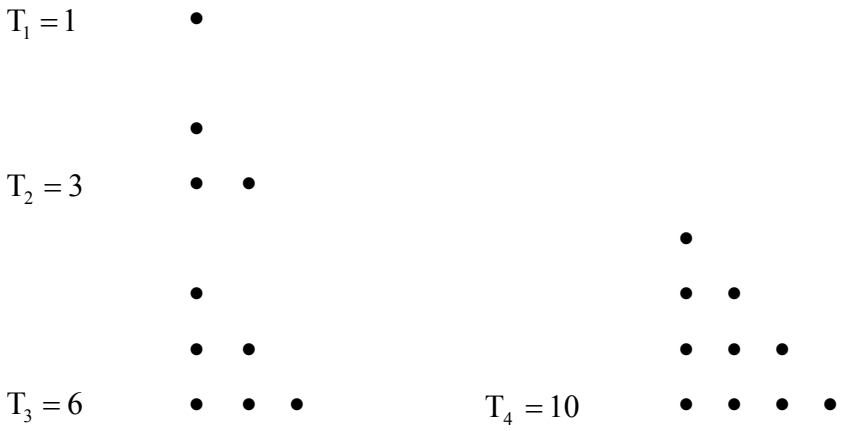
β) $1+4+\ \ldots\ +n^2=\dfrac{n(n+1)(2n+1)}{6}$

γ) $1+8+\ \ldots\ +n^3=\left(\dfrac{n(n+1)}{2}\right)^2$

δ) $1\cdot 2+2\cdot 3+\ \ldots\ +n\cdot(n+1)=\dfrac{n(n+1)(n+2)}{3}$

Η συνάρτηση n! ορίζεται επαγωγικά από τις σχέσεις 0! = 1 και $(n+1)!=n!(n+1)$.

Τριγωνικοί αριθμοί. Ο επαγωγικός ορισμός των τριγωνικών αριθμών περιγράφεται από το παρακάτω σχήμα:



Παρατηρούμε ότι, $T_{n+1}=T_n+(n+1)$ όπου $T_1=1$.

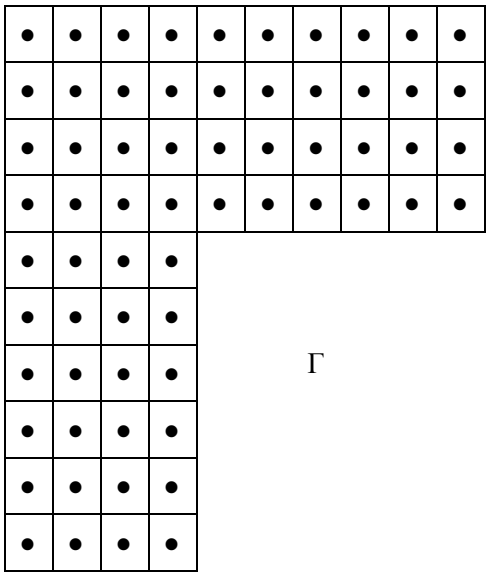
Θέλουμε να υπολογίσουμε τον T_n χωρίς πρώτα, να έχουμε υπολογίσει τον προηγούμενό του T_{n-1}. Αρκεί προς τούτο να σκεφτούμε, ότι ο T_n παριστά το εμβαδόν του n-στού τριγώνου εκπεφρασμένο σε κουκίδες.

Είναι, λοιπόν, $T_n=\dfrac{1}{2}\,\beta\acute{\alpha}\sigma\eta\times\acute{\upsilon}\psi o\varsigma=\dfrac{1}{2}n(n+1)$

Με την μέθοδο των κουκίδων, θα δείξουμε
και την σχέση $T_n^2-T_{n-1}^2=n^3$.

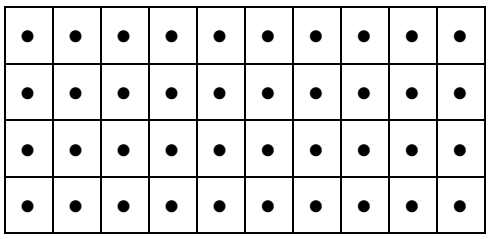
Είναι:

Τ =

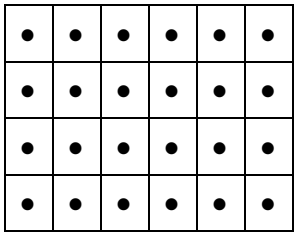


Γ

Β =



Α =



Είναι, εμβαδόν Τ = εμβαδόν Α + εμβαδόν Β+ εμβαδόν Γ. Όμως $T = T_n^2$, $\Gamma = T_{n-1}^2$, $B = nT_n$ και $A = nT_{n-1}$.

Άρα εμβαδόν Τ – εμβαδόν Γ = εμβαδόν Α + εμβαδόν Β.

Συνεπώς: $T_n^2 - T_{n-1}^2 = nT_n + nT_{n-1} = n(T_n + T_{n-1})$

Όμως, $T_n + T_{n-1} = \frac{1}{2}n(n+1) + \frac{1}{2}(n-1)n = \frac{1}{2}n(n+1+n-1) = n^2$

Άρα, $T_n^2 - T_{n-1}^2 = n^3$.

Πυθαγόρεια Τρίγωνα. Έτσι καλούνται τα ορθογώνια τρίγωνα, των οποίων οι πλευρές έχουν μήκη ακεραίους θετικούς αριθμούς. Παράδειγμα πυθαγορείου τριγώνου είναι το ορθογώνιο τρίγωνο με πλευρές 1, 2, 3. Η εύρεση όλων των πυθαγορείων τριγώνων ισοδυναμεί με την εύρεση όλων των ακεραίων και θετικών αριθμών που πληρούν την ισότητα $x^2 + y^2 = z^2$. Ο Πυθαγόρας βρήκε ότι οι τριάδες των φυσικών $\frac{n^2-1}{2}$, n, $\frac{n^2+1}{2}$, $n > 1, n = 2\kappa + 1$ σχηματίζουν πυθαγόρεια τρίγωνα. Όμως αυτές δεν είναι οι μόνες. Σχετικά ισχύει η πρόταση: (Στοιχεία Ευκλείδου, Βιβλίο X, Λήμμα 1 στην πρόταση 29). **Πρόταση.** Οι πλευρές όλων των Πυθαγορείων τριγώνων δίδονται από τους τύπους $a = m^2 - n^2,\ b = 2mn,\ c = m^2 + n^2$ όπου $(m,n) = 1,\ m > n$ και όπου όταν ο m άρτιος, ο n περιττός (βλέπε Π.Γ. Τσαγκάρη Θεωρία Αριθμών, Εκδόσεις Συμμετρία Αθήνα 2005).

5. Το σύνολο $\mathbb{Z}$ των ακεραίων. Η κατασκευή του συστήματος των ***ακεραίων*** γίνεται με τέτοιο τρόπο, ώστε η εξίσωση $a + x = b,\ a,b \in \mathbb{N}$ να έχει πάντα λύση μέσα σ' αυτό.

Θεωρούμε το σύνολο $\mathbb{N} \times \mathbb{N}$ και εισάγουμε την εξής σχέση ισοδυναμίας $R \subseteq (\mathbb{N} \times \mathbb{N})^2$: $((a,b),(c,d)) \in R \leftrightarrow a + d = b + c$. Το σύνολο $\mathbb{N} \times \mathbb{N} / R$ το καλούμε σύνολο των ακεραίων $\mathbb{Z}$. Ένας ακέραιος αριθμός, ένα στοιχείο του $\mathbb{Z}$ δηλαδή, είναι μία τάξη ισοδυναμίας $C_{(a,b)}$ που περιέχει όλα τα ζεύγη $(c,d) \in \mathbb{N} \times \mathbb{N}$, για τα οποία ισχύει ότι, $a + d = b + c$. Στην περίπτωση, που $a = b = 0$, η τάξη $C_{(0,0)}$ ταυτίζεται με την διαγώνιο του $\mathbb{N} \times \mathbb{N}$.

Οι πράξεις " + " και "·" μεταφέρονται στο σύνολο $\mathbb{Z}$, αν ορίσουμε ότι,

$C_{(a,b)} + C_{(c,d)} = C_{(a+c,b+d)}$ για την πρόσθεση, και

$C_{(a,b)} \cdot C_{(c,d)} = C_{(ac+bd,ad+bc)}$ για τον πολλαπλασιασμό.

Η τάξη $C_{(0,0)}$ δρα ως ουδέτερο στοιχείο για την πρόσθεση.

Πράγματι, $(x,x) + (a,b) = (a + x, b + x)$ και $(a + x, b + x) \in C_{(a,b)}$, μιά και $a + x + b = b + x + a$.

Η τάξη $C_{(b,a)}$ δρα ως αντίθετο στοιχείο του στοιχείου $C_{(a,b)}$.

Πράγματι, $(b,a) + (a,b) = (b + a, a + b) \in C_{(0,0)}$.

Ο πολλαπλασιασμός, όπως ορίσθηκε, καθιστά το $\mathbb{Z}$ ημιομάδα με μονάδα. Τον ρόλο της μονάδος εν $\mathbb{Z}$, τον παίζει η τάξη $C_{(1,0)}$.

Εύκολα αποδεικνύεται, ότι η πρόσθεση και ο πολλαπλασιασμός όπως ορίσθηκαν, καθιστούν το σύνολο $\mathbb{Z}$ ακέραια περιοχή.

Η ακέραια αυτή περιοχή, διατάσσεται ολικά, αν θέσουμε $C_{(a,b)} \le C_{(c,d)} \leftrightarrow a + d \le b + c$.

για την διάταξη στους ακεραίους, παρατηρούμε ότι, ισχύουν και γι' αυτήν τα Δ1, Δ2, Δ3 και Δ4. Η Δ5 ισχύει τροποποιημένη ως εξής: Δ5. Αν $z > 0$, τότε και $x \le y \leftrightarrow xz \le yz$.

Εύκολα δείχνεται ότι, Αν $x < y \to -x > -y$. Το σύνολο $P = \{x \in \mathbb{Z},\ 0 < x\}$ καλείται σύνολο των ***ακεραίων θετικών*** αριθμών. Το σύνολο P των θετικών στοιχείων του $\mathbb{Z}$, ταυτίζεται με το σύνολο $\mathbb{N}$ των φυσικών αριθμών, το οποίο είναι σύνολο καλά διατεταγμένο. Το σύνολο των ακεραίων, που δεν είναι θετικοί ή μηδέν, καλείται σύνολο των ***αρνητικών*** ακεραίων –P. Ένας ακέραιος είναι δυνατόν να είναι είτε θετικός, είτε αρνητικός, είτε μηδέν. Η απεικόνιση $x \mapsto -x,\ x \ne 0$, είναι μία bijection του P επί το –P. (Βλέπε και §12).

Πρόταση. Ανάμεσα στον 0 και τον 1 δεν υπάρχει κανείς ακέραιος.
Απόδειξη. Ας υποθέσουμε ότι, το σύνολο S των μεταξύ 0 και 1 ακεραίων είναι μη κενό. Τούτο είναι υποσύνολο του P. Έχει λοιπόν, ελάχιστο στοιχείο m.

Έχουμε, $0 < m < 1$. Άρα και, $0 < m^2 < m < 1$. Άρα $m^2 \in S$, άτοπο, μια και το m είναι το ελάχιστο στοιχείο του S.

Πρόταση. Το τετράγωνο παντός ακεραίου, είναι θετικός αριθμός. Βλέπε και [ΖΚ], σελ. 139.

6 Αρχές συνδυαστικής. Η απαρίθμηση των συμβάντων, (αντικειμένων, γεγονότων, καταστάσεων, . . .), βασίζεται στους εξής δύο νόμους, που αποτελούν και την βάση της ***συνδυαστικής.***
Νόμος της προσθέσεως. Αν ένα γεγονός είναι δυνατόν να συμβεί με m διαφορετικούς τρόπους και κάποιο άλλο γεγονός με n διαφορετικούς τρόπους, το σύνθετο γεγονός, που αποτελείται είτε από το ένα είτε από το άλλο, συμβαίνει κατά $m + n$ διαφορετικούς τρόπους.
Νόμος του πολλαπλασιασμού. Αν ένα γεγονός είναι δυνατόν να συμβεί με m διαφορετικούς τρόπους και κάθε ένας από αυτούς τους m διαφορετικούς τρόπους, παράγει κάποιο άλλο γεγονός με n διαφορετικούς τρόπους, τότε, τα δεύτερα γεγονότα, συμβαίνουν με $m \cdot n$ διαφορετικούς τρόπους.

Μιά εφαρμογή του νόμου του πολλαπλασιασμού, κάναμε ήδη κατά τον υπολογισμό του αριθμού των μεταθέσεων των n αντικειμένων (βλέπε §11). Μερικές ακόμα, χρήσιμες εφαρμογές, θα κάνουμε αμέσως, τώρα.

α) Έστω ότι έχουμε n αντικείμενα, τα οποία θέλουμε να τοποθετήσουμε σε r διαφορετικές θέσεις, $r \le n$. Ζητάμε να βρούμε τους διαφορετικούς τρόπους $P(n,r)$ με τους οποίους είναι δυνατόν να γίνουν αυτές οι τοποθετήσεις. Κάθε διαφορετική τοποθέτηση, αποτελεί και μία διάταξη των n αντικειμένων σε r θέσεις. Παρατηρούμε ότι, η πρώτη θέσης γεμίζει με n ($n = n - $ αριθμός θέσεως $+ 1$) διαφορετικούς τρόπους. Η δεύτερη, με $n-1$, κ.λ.π. η n-στή θέσης κατά $n - r + 1$ διαφορετικούς τρόπους.

Άρα, $P(n,r) = n \cdot (n-1) \cdot \ \ldots \ \cdot (n-r+1) = \dfrac{n!}{(n-r)!}$.

β) Συμβολίζουμε με $C(n,r)$ τους διαφορετικούς τρόπους, με τους οποίους μπορούμε να εκλέξουμε r αντικείμενα, από ένα σύνολο n αντικειμένων. Έτσι, για παράδειγμα, $C(n,n) = 1$.

Παρατηρούμε, τώρα, ότι για να πληρώσουμε τις r θέσεις στο α) πιο πάνω, θα πρέπει πρώτα να εκλέξουμε αυτά τα r αντικείμενα, από τα n που διαθέτουμε, και μετά, να τοποθετήσουμε αυτά, στις r θέσεις. Κάθε τοποθέτησης, είναι και μία διάταξης αυτών. Το πλήθος αυτό των διατάξεων, είναι, $P(r,r) = r!$. Άρα είναι και $P(n,r) = P(r,r) \cdot C(n,r)$. Από την σχέση αυτή, λαβαίνουμε και την $C(n,r) = \dfrac{P(n,r)}{P(r,r)} = \dfrac{(n-r+1)!}{r!} = \dfrac{n!}{r!(n-r)!}$.

Γράφουμε και $\binom{n}{r} = \dfrac{n!}{r!(n-r)!}$. Φανερά, $C(n,r) = C(n,n-r)$.

γ) Έστω ότι θέλουμε να εκλέξουμε r αντικείμενα, από ένα σύνολο n αντικειμένων. Ας υποθέσουμε ακόμα, ότι ένα από αυτά τα n αντικείμενα, είναι σημαδεμένο. Κάθε εκλογή μας, τότε, είτε θα περιέχει, είτε δεν θα περιέχει το σημαδεμένο αντικείμενο. Στην πρώτη περίπτωση, οι διαφορετικές επιλογές είναι $C(n-1,r-1)$. Στην δεύτερη, $C(n-1,r)$. Ισχύει συνεπώς η σχέση $C(n,r) = C(n-1,r-1) + C(n-1,r)$.

Γράφουμε και $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$.

δ) Με πόσους διαφορετικούς τρόπους, είναι δυνατόν να καθίσουν n άτομα γύρω από ένα στρογγυλό τραπέζι; Παρατηρούμε εδώ, ότι η ίδια διάταξη των n ατόμων, προκύπτει κατά n διαφορετικούς τρόπους, μιά και δεν έχουμε προσδιορίσει μιά θέση σαν πρώτη θέση, και συνεπώς ως πρώτη, θα μπορούσαμε να λάβουμε οιαδήποτε θέση. Άρα η λύση στο ερώτημά μας είναι ο αριθμός $n!/n = (n-1)!$

Διώνυμο του Newton. Έστω ότι θέλουμε να υπολογίσουμε το $(a+b)^n$, δηλαδή, το $(a+b)\ \cdots\ (a+b)$, n παράγοντες. Το αποτέλεσμα είναι ένα άθροισμα 2^n όρων, όπου κάθε όρος είναι ένα γινόμενο n παραγόντων, με κάθε παράγοντα να είναι το a ή το b. Ας υποθέσουμε, τώρα, ότι τα a και b είναι φυσικοί αριθμοί. Λόγω αντιμεταθετικότητας του πολλαπλασιασμού, όροι της μορφής $ab\cdots b$, $ba\cdots b$, $bb\cdots a$ είναι ίσοι προς ab^{n-1} και έχουμε $C(n,1)$ τέτοιους όρους. Έχουμε, τώρα, $C(n,2)$ όρους της μορφής a^2b^{n-2}, και γενικά έχουμε $C(n,r)$ όρους της μορφής a^rb^{n-r}. Θα πρέπει ακόμα να θεωρήσουμε και τους μοναδικούς όρους της μορφής $aa\cdots a = C(n,n)a^nb^0$ και $bb\cdots b = C(n,0)a^0b^n$.
Είναι, λοιπόν,

$$(a+b)^n = C(n,0)a^nb^0 + C(n,1)a^{n-1}b^1 + \ \dots\ + C(n,r)a^{n-r}b^r + \ \dots\ + C(n,n)a^0b^n$$
$$= \sum_{r=0}^{n} C(n,r)a^{n-r}b^r \qquad \text{ή} \qquad (a+b)^n = \sum_{r=0}^{n}\binom{n}{r}a^{n-r}b^r \ .$$

Καταμέτρηση των στοιχείων ενός συνόλου. Επειδή τα στοιχεία ενός συνόλου S θεωρούνται όλα διαφορετικά, η αντιστοιχία $S \ni s \mapsto n \in \mathbb{N}$ είναι ένα προς ένα. Η απεικόνιση, λοιπόν $n(S) = n$, μου ορίζει το πλήθος των στοιχείων του S. Στην περίπτωση συνόλου που είναι η ένωση δύο άλλων συνόλων, $S = S_1 \cup S_2$, επειδή τα στοιχεία της τομής των συνόλων καταμετρούνται από μία φορά και στα δύο σύνολα, ισχύει φανερά ότι, $n(S) = n(S_1) + n(S_2) - n(S_1 \cap S_2)$. Ερχόμαστε, τώρα, στην περίπτωση της ενώσεως τριών συνόλων, και έστω $S = S_1 \cup S_2 \cup S_3$. Είναι,

$$n(S) = n\{(S_1 \cup S_2) \cup S_3\} = n(S_1 \cup S_2) + n(S_3) - n\{(S_1 \cup S_2) \cap S_3\}$$
$$= n(S_1) + n(S_2) + n(S_3) - n(S_1 \cap S_2) - n\{(S_1 \cap S_3) \cup (S_2 \cap S_3)\}$$
$$= n(S_1) + n(S_2) + n(S_3) - n(S_1 \cap S_2) - n(S_1 \cap S_3) - n(S_2 \cap S_3) + n(S_1 \cap S_2 \cap S_3)$$

Επαγωγικά έχουμε ότι

$$n(S_1 \cup S_2 \cup \cdots \cup S_k) =$$
$$= \sum_{C(k,1)} n(S_i) - \sum_{C(k,2)} n(S_i \cap S_j) + \cdots + (-1)^k \sum_{C(k,k)} n(S_1 \cap S_2 \cap \cdots \cap S_k)$$

7. Η συνδυαστική άποψη. Αν το σύμβολο του πολλαπλασιασμού το ταυτίσουμε με το λογικό σύμβολο "$\wedge$" = "και" (σύζευξη) και το σύμβολο της προσθέσεως με το "$\vee$" = "είτε" (διάζευξη), η ύψωση, τότε, σε κάποια δύναμη n, (το a^n δηλαδή) διαβάζεται, «λαμβάνουμε n αντικείμενα a» ενώ το $a+b$ διαβάζεται «λαμβάνουμε είτε το a είτε το b». Το a^0, διαβάζεται δεν λαμβάνουμε κανένα αντικείμενο a».

Παρατηρούμε, τώρα, ότι ο συντελεστής $C(n,r)$ του $a^{n-r}b^r$ μετρά ακριβώς τους τρόπους με τους οποίους μπορούμε να "λάβουμε" (ή καλλίτερα, να χαρακτηρίσουμε) από n αντικείμενα, $n-r$ ως a, και r ως b.

Η "μετάφραση" αυτή των μαθηματικών σχέσεων έχει νόημα. Για παράδειγμα, αν μας έχουν δοθεί τρία αντικείμενα, τα a, b, c η έκφραση τότε $(a+b+c)x$ "μεταφράζεται" ως εξής: «Με τρείς τρόπους λαβαίνουμε ένα από αυτά. Μπορούμε, δηλαδή, να λάβουμε, είτε το a , είτε το b, είτε το c». Η έκφραση $(ab+bc+ca)x^2$ "μεταφράζεται" ως εξής: «Με τρεις τρόπους λαβαίνουμε δύο απ' αυτά. Μπορούμε, δηλαδή, να λάβουμε είτε το ab είτε το bc είτε το ca». Τέλος, η έκφραση $(abc)x^3$ μου λεει ότι, «με ένα τρόπο λαβαίνουμε και τα τρία αντικείμενα. Ο

τρόπος αυτός, είναι ο abc». Η έκφραση, τώρα, $x^0 + ax = 1 + ax$ διαβάζεται «δεν εκλέγω το αντικείμενο, είτε εκλέγω αντικείμενο a».

Κατ' αυτόν τον τρόπο, μπορούμε να μεταφράσουμε και πολυπλοκότερες σχέσεις. Για παράδειγμα, η ισότητα $(1+ax)(1+bx) = 1 + (a+b)x + abx^2$ διαβάζεται ως εξής: Εκλέγω ή όχι το a και εκλέγω ή όχι το b είναι ισοδύναμο με το να μη εκλέξω κανένα, είτε να εκλέξω ένα απ' αυτά, είτε να εκλέξω και τα δύο.

Εκφράσεις τέτοιου τύπου, είναι οι ***γεννήτριες συναρτήσεις.*** Θεωρούμε, λοιπόν, "πολυωνυμικές" εκφράσεις, όπου η "μεταβλητή" μεταφράζεται «επέλεξε», η δύναμη, στην οποία εμφανίζεται η μεταβλητή δείχνει το πλήθος των αντικειμένων που επιλέγονται ενώ, τέλος, ο συντελεστής της μεταβλητής καταδεικνύει το πλήθος των συγκεκριμένων επιλογών. Λέμε ότι η $F(x) = (1+ax)(1+bx)$ είναι η γεννήτρια συνάρτηση των επιλογών των συγκεκριμένων δύο αντικειμένων a και b. Από την στιγμή που δεν ενδιαφερόμεθα για επιλογή συγκεκριμένων αντικειμένων, αλλά μόνον για το πλήθος των δυνατών επιλογών, η $F(x)$ λαβαίνει την μορφή $F(x) = (1+x)(1+x) = (1+x)^2$.

Η γεννήτρια συνάρτηση $F(x) = (1+x)^n$ μου δίδει το πλήθος των επιλογών, κανενός, ενός, δύο, τριών, . . . n-αντικειμένων. Είναι, βέβαια,

$$(1+x)^n = 1 + nx + \frac{n(n-1)}{2!}x^2 + \ \dots\ + \frac{n(n-1)\ \cdots\ (n-r+1)}{r!}x^r + \ \dots\ + x^n = \sum_{r=0}^{n} C(n,r)x^r$$

Παραδείγματα. 1. Αν στην προηγούμενη ισότητα θέσουμε $x = 1$, λαβαίνουμε την σχέση $2^n = \sum_{r=0}^{n} C(n,r)$. Η "μετάφραση" αυτής της ισότητας είναι η: «Η διαφορετικοί τρόποι, με τους οποίους είναι δυνατόν να εκλέξουμε από n αντικείμενα κανένα, είτε 1, είτε 2, είτε . . . είτε n (όλα, δηλαδή) αντικείμενα, είναι 2^n το πλήθος. Το σύνολο, δηλαδή, των υποσυνόλων ενός συνόλου n αντικειμένων, είναι 2^n το πλήθος.

2. Αν θέσουμε $x = -1$, λαβαίνουμε $\sum_{r=0}^{n} (-1)^r C(n,r) = 0$. Από την ισότητα αυτή συμπεραίνουμε ότι, το πλήθος των επιλογών αρτίου πλήθους αντικειμένων, από ένα σύνολο n αντικειμένων, ισούται ακριβώς, με το πλήθος των επιλογών περιττού πλήθους αντικειμένων.

3. Έστω ότι, από ένα πλήθος 2n αντικειμένων, έχουμε να διαλέξουμε n αντικείμενα. Προς τούτο, αν τα 2n αντικείμενα τα χωρίσουμε σε δύο τμήματα από n αντικείμενα το κάθε τμήμα, και επιλέγουμε k αντικείμενα από το ένα τμήμα και $n-k$ αντικείμενα από το άλλο τμήμα, με $0 \le k \le n$, τότε, οι επιλογές μας είναι $\sum_{k=0}^{n} C(n,k)C(n,n-k)$. Ισχύει, λοιπόν, η ισότητα,

$$C(2n,n) = \sum_{k=0}^{n} C(n,k)C(n,n-k).$$

Τέλος, επειδή είναι $C(n,k) = C(n,n-k)$, $C(2n,n) = \sum_{k=0}^{n} C(n,k)^2$.

4. Για να βρούμε τον συντελεστή του όρου x^{23}, στο ανάπτυγμα του $(1+x^5+x^9)^{100}$, σκεπτόμεθα ως εξής: Επειδή η παραγωγή του x^{23} από τα x^5 και x^9 έχει την μοναδική έκφραση $x^5x^9x^9$, και επειδή το x^9 επιλέγεται με $C(100,2)$ τρόπους και το x^5 με $C(98,1)$ τρόπους, έχουμε συντελεστή, τον $C(100,2)C(98,1)$.

Επιλέξαμε πρώτα τον x^9, και μετά τον x^5. Αν ενεργούσαμε αντίστροφα, θα υπολογίζαμε ως συντελεστή του x^{23} τον $C(100,1)C(99,2)$. Είναι όμως,

$$C(100,1)C(99,2) = 100 \times \frac{99 \times 98}{2} = \frac{100 \times 99}{2} \times 98 = C(100,2)C(98,1)$$

Ας υποθέσουμε, τώρα, ότι έχουμε τα δύο αντικείμενα a, b, όμως, όταν κάνω τις επιλογές μου, μου επιτρέπεται να επιλέξω το a, μέχρι και δύο φορές. Η γεννήτρια συνάρτηση όλων των ζητουμένων δυνατών επιλογών, σύμφωνα με ότι έχουμε πει, είναι η $(1+ax+a^2x^2)(1+bx)$. Αν δεν μας ενδιαφέρουν τα συγκεκριμένα αντικείμενα a και b, η γεννήτρια συνάρτηση F(x), όπου $F(x) = (1+x+x^2)(1+x)$ μου δίδει όλους τους τρόπους, με τους οποίους μπορούμε να εκλέξουμε δύο αντικείμενα, όταν επιτρέπεται η επανεκλογή του ενός αντικειμένου, μέχρι και δύο φορές. Είναι, βέβαια, $F(x) = 1+2x+2x^2+x^3$. Αν θέλουμε, λοιπόν, να γνωρίζουμε, τους διαφορετικούς τρόπους, με τους οποίους είναι δυνατόν να έχουμε π.χ. επιλογή ενός αντικειμένου, είναι 2. (Ο συντελεστής του x^1. Αν ενδιαφερόμεθα για τα συγκεκριμένα αντικείμενα a και b, ο συντελεστής αυτός, θα ήταν ο $a+b$). Αν θέλουμε, να γνωρίζουμε, τους διαφορετικούς τρόπους, με τους οποίους είναι δυνατόν να έχουμε επιλογή δύο αντικειμένων, επιτρέποντας επανάληψη της επιλογής του ενός ακόμα μιά φορά, θα κοιτάξουμε τον συντελεστή του x^2, που είναι 2. (Για τα συγκεκριμένα αντικείμενα a και b, ο συντελεστής αυτός, θα ήταν ο $ab+a^2$).

5. Την έκφραση $(1+x)(1+x)^2$ την "μεταφράζουμε" ως εξής :

$1 = x^0 \rightarrow$ δεν εκλέγω το x.

$x = x^1 \rightarrow$ εκλέγω το x μία φορά.

$x^2 \rightarrow$ εκλέγω το xx μία φορά.

Είναι, λοιπόν, $(1+x)(1+x)^2 \rightarrow$ [είτε δεν εκλέγω το x είτε εκλέγω το x μία φορά] και [είτε δεν εκλέγω το x είτε εκλέγω το xx μία αφορά]. Η πρόταση αυτή, όμως, είναι ισοδύναμος με την : [δεν εκλέγω το x] είτε [εκλέγω το x μία φορά] είτε [εκλέγω το xx μία φορά] είτε [εκλέγω το x μία φορά και το xx μία φορά]. Έχουμε, συνεπώς, την ισότητα, $(1+x)(1+x)^2 = 1+x+x^2+x^3$

Γενίκευση της ταυτότητος αυτής, είναι η $(1+x)(1+x)^2 \cdots (1+x)^{2n} = 1+x+x^2+\ldots+x^{2n+1}$

Εφαρμογή. Το θεώρημα του Vandermonde. Όπως είδαμε, το πλήθος των διατάξεων r αντικειμένων, που λαμβάνονται από n αντικείμενα, είναι $P(n,r) = P(r,r) \cdot C(n,r)$. Αν, τώρα, αντί για n αντικείμενα είχαμε $m+n$ αντικείμενα, τότε, το πλήθος $P(m+n,r)$, $0 \le r \le m \le n$ βρίσκεται, αν σκεφτούμε ως εξής: Αν οι διατάξεις γίνουν μόνον από τα m αντκείμενα, έχουμε τότε, $C(r,0)P(m,r)$ διατάξεις. Αν λάβουμε $r-1$ αντικείμενα από τα m και 1 αντικείμενο από τα n, τότε θα έχουμε $C(r,1)P(m,r-1)P(n,1)$. Στην γενική περίπτωση, θα έχουμε λάβει k αντικείμενα από τα m, $n-k$ αντικείμενα από τα m, και όλες οι διατάξεις θα είναι $C(r,k)P(m,r-k)P(n,k)$. Έχουμε συνεπώς τελικά ότι,

$$P(m+n,r) = \sum_{k=0}^{r} C(r,k)P(m,r-k)P(n,k)$$

Βιβλιογραφία. C.L. Liu, Introduction to Combinatorial Mathematics. McGraw-Hill.

8. Γεννήτριες συναρτήσεις. Έτσι ονομάζουμε μια πολυωνυμική συνάρτηση, που έχει συντελεστές τους όρους μιάς δοσμένης ακολουθίας (ακεραίων) αριθμών.

Παράδειγμα 1. Έστω ότι δίδεται η ακολουθία $a_0, a_1, \ldots$ (1) όπου $a_{n+1} = 2a_n + 1$, με $n \geq 0$ και $a_0 = 0$. Ζητάμε να βρούμε ένα πολυώνυμο $A(x)$, που να έχει για συντελεστές τους όρους της ακολουθίας (1). Ζητάμε, δηλαδή, το $A(x) = a_0 x^0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$. Γνωρίζουμε βέβαια ότι, $a_0 = 0$, $a_1 = 1$, $a_2 = 3$, … , όμως, για να υπολογίσουμε τον συντελεστή a_n, θα πρέπει να έχουμε πρώτα υπολογίσει τον συντελεστή a_{n-1}. Μήπως υπάρχει άλλος τρόπος γι' αυτόν τον υπολογισμό;

Λύση. Από την (1) έχουμε ότι, $a_{n+1}x^n = 2a_n x^n + x^n$, οπότε, $\sum_{n\geq 0} a_{n+1}x^n = \sum_{n\geq 0}(2a_n x^n + x^n)$

Είναι, $\sum_{n\geq 0} a_{n+1}x^n = a_1 + a_2 x + \ldots + a_{n+1}x^n = \left\{(a_0 + a_1 x + \ldots + a_n x^n)x - a_0 x\right\} \Big/ x = A(x) \Big/ x$.

Εξ' άλλου, $\sum_{n\geq 0}(2a_n + 1)x^n = 2A(x) + \sum_{n\geq 0} x^n$. Εργαζόμαστε, τώρα, για τιμές του x, τέτοιες ώστε $|x| < 1$. Είναι, τότε, ως γνωστόν, $\sum_{n\to\infty} x^n = \frac{1}{1-x}$. Άρα, τελικά, λαβαίνουμε την σχέση $\sum_{n\geq 0}(2a_n + 1)x^n = 2A(x) + \frac{1}{1-x}$. Είναι, λοιπόν, $\frac{A(x)}{x} = 2A(x) + \frac{1}{1-x}$, απ' όπου υπολογίζουμε το $A(x) = \frac{x}{(1-x)(1-2x)} = x\left\{\frac{2}{1-2x} - \frac{1}{1-x}\right\}$, ή ακόμα και,

$$A(x) = (2x + 4x^2 + 8x^3 + \ldots) - (x + x^2 + x^3 + \ldots) = (2-1)x + (2^2 - 1)x^2 + (2^3 - 1)x + \ldots$$

Μπορούμε, λοιπόν, πιά, από την σχέση $a_n = 2^n - 1$, να υπολογίσουμε απ' ευθείας τον n-στο όρο της ακολουθίας (1).

Βιβλιογραφία. Herbert Wilf generatingfunctionology. Διατίθεται από το site του H. Wilf.

9. Αναγωγικές σχέσεις. Εξισώσεις διαφορών. Έστω ότι έχουμε μία ακολουθία ακεραίων αριθμών, οι όροι της οποίας παρουσιάζουν κάποια κανονικότητα. Για παράδειγμα:

α) 1, 2, 3, 4, . . . , n, . . .

β) 2, 4, 8, 16, . . . , 2^n, . . .

γ) 1, 1, 2, 3, 5, 8, 13, . . .

Στην α) περίπτωση, έχουμε ότι, η διαφορά δύο διαδοχικών όρων ισούται με 1. Γράφουμε και $a_r - a_{r-1} = 1$, $1 < r \leq n$, $\forall n \in \mathbb{N}$, όπου, ο πρώτος όρος a_1 είναι γνωστός .

Στην β) περίπτωση, ο λόγος δύο διαδοχικών όρων ισούται με 2. Γράφουμε και $\frac{a_r}{a_{r-1}} = 2$, $1 < r \leq n$, $\forall n \in \mathbb{N}$, όπου, ο πρώτος όρος a_1 είναι γνωστός. Στην Τρίτη περίπτωση, τέλος, είναι, $a_r = a_{r-1} + a_{r-2}$, $2 < r \leq n$, $\forall n \in \mathbb{N}$, όπου, οι δύο πρώτοι όροι a_1 και a_2 δίδονται.

Οι σχέσεις αυτές καλούνται ***αναγωγικές σχέσεις*** ενώ οι ισότητες που τις παριστούν καλούνται ***εξισώσεις διαφορών.*** Ο όρος a_r είναι ο ***γενικός όρος*** της ακολουθίας. Οι συνθήκες που προσδιορίζουν τους αρχικούς όρους καλούνται ***αρχικές συνθήκες.*** Με $a: a_1, a_2, \ldots, a_n, \ldots$ θα συμβολίζουμε την τυχούσα ακολουθία ακεραίων.

Τα ερωτήμα που θα εξετάσουμε, σχετικά με ακολουθίες της παραπάνω μορφής, είναι τα εξής δύο: 1) Να ευρεθεί ο n-στός όρος της ακολουθίας, χωρίς να υπολογίσουμε όλους τους προηγούμενους όρους. 2) Να υπολογισθεί το άθροισμα των n πρώτων όρων της ακολουθίας, χωρίς να έχουμε υπολογίσει το άθροισμα των $n-1$ πρώτων όρων της.

Ας εξετάσουμε, πρώτα, την περίπτωση α). Η γενική περίπτωση είναι να έχουμε $a_r - a_{r-1} = d$, όπου $1 \le r \le n$, οπότε λέμε ότι, η ακολουθία μας είναι μία ***αριθμητική πρόοδος.***
Παρατηρούμε ότι, εδώ, $a_r = a_1 + (a_2 - a_1) + (a_3 - a_2) + \ \dots \ + (a_r - a_{r-1}) = a_1 + (r-1)d$. Όμοια είναι και $a_{n-r+1} = a_1 + (a_2 - a_1) + (a_3 - a_2) + \ \dots \ + (a_{n-r+1} - a_{n-r}) = a_1 + (n-r)d$. Το άθροισμα των δεικτών των δύο αυτών όρων είναι n+1. Το άθροισμα των όρων αυτών είναι,
$a_r + a_{n-r+1} = 2a_1 + (n-1)d$, $1 \le r \le n$.
Για να υπολογίσουμε το άθροισμα των n πρώτων όρων, γράφουμε:

$$2S(n) = a_1 + a_2 + \ \dots \ + a_r + \ \dots \ + \quad a_n +$$
$$a_n + a_{n-1} + \ \dots \ + a_{n-r+1} + \ \dots \ + a_1$$

ή $$2S(n) = \sum_{r=1}^{n} a_r + a_{n-r} = n(2a_1 + (n-1)d) = n(a_1 + (a_1 + a_{n-1})),$$

δηλαδή, $S(n) = \dfrac{n(a_1 + a_n)}{2}$. Το $S(n)$ ισούται, δηλαδή, με n φορές τον μέσο όρο του πρώτου και του τελευταίου όρου. **Εφαρμογή.** Για την ακολουθία α), που έχει γενικό όρο $a_r = r$ είναι,

$S_1(n) = \dfrac{n(n+1)}{2}$. (Βλέπε και §13).

Ας αθροίσουμε, τώρα, τους n όρους των ακολουθιών με γενικό όρο $a_r = r^k$, k = 1,2, 3, ...
(Η περίπτωση k = 1 είναι, βέβαια, η προηγούμενη εφαρμογή).
Για να υπολογίσουμε, το $S_m(n) = 1^m + 2^m + \cdots + n^m$, χρησιμοποιούμε την ταυτότητα

$$(x+1)^{m+1} - x^{m+1} = 1 + C(m+1,1)x + C(m+1,2)x^2 + \cdots + C(m+1,m)x^m$$

Ως εξής:
Για $m = 1$. Ξεκινάμε από την ταυτότητα $(x+1)^2 - x^2 = 2x + 1$, και στη συνέχεια, προσθέτουμε κατά μέλη τις ισότητες που προκύπτουν για $x = n, n-1, \ \dots \ ,1$.
Έχουμε, λοιπόν, $(n+1)^2 - n^2 = 2 \times n + 1$

. . . . . .
$(3+1)^2 - 3^2 = 2 \times 3 + 1$
$(2+1)^2 - 2^2 = 2 \times 2 + 1$
$(1+1)^2 - 1^2 = 2 \times 1 + 1$

Άρα, και $(n+1)^2 - 1^2 = 2(1 + 2 + \ \dots \ + n) + n$, ή $(n+1)^2 - 1^2 = 2S_1(n) + n$, οπότε και,

$$S_1(n) = \frac{n^2 + 2n - n}{2} = \frac{n(n+1)}{2}$$

Για $m = 2$. Ξεκινάμε από την ταυτότητα $(x+1)^3 - x^3 = 3x^2 + 3x + 1$, και στη συνέχεια, προσθέτουμε κατά μέλη τις ισότητες που προκύπτουν για $x = n, n-1, \ \dots \ ,1$, οπότε λαβαίνουμε την ισότητα $(n+1)^3 - 1 = 3S_2(n) + 3S_1(n) + n$.

Άρα και, $S_2(n) = \dfrac{n(n-1)(2n-1)}{6}$.

Με τον ίδιο τρόπο, υπολογίζουμε τα αθροίσματα $S_3(n) = \dfrac{n^2(n+1)^2}{4}$, κ.ο.κ.

Παρατηρούμε, τώρα, ότι: $(n+1)^2 - (n+1) = 2S_1(n)$

$$(n+1)^3-(n+1)=3S_2(n)+3S_1(n)$$
$$(n+1)^4-(n+1)=4S_3(n)+6S_2(n)+4S_1(n)$$
$$(n+1)^5-(n+1)=5S_4(n)+10S_3(n)+10S_2(n)+5S_1(n)$$

κ.ο.κ.

Αν συμπληρώσουμε τον πίνακα των συντελεστών των $S_m(n)$ με τις ελλείπουσες μονάδες, λαβαίνουμε τον πίνακα: 1

1 2 1

1 3 3 1

1 4 6 4 1 κ.ο.κ., (τρίγωνο του Pascal, βλέπε [ΖΚ], σελ. 28) που είναι οι συντελεστές του διωνύμου του Newton. (Βλέπε §13). Βλέπε και παρακάτω, αριθμοί Bernoulli.

Ας εξετάσουμε, τώρα, την περίπτωση β). Εδώ, δύο διαδοχικοί όροι της ακολουθίας, έχουν λόγο σταθερό: $\frac{a_{r+1}}{a_r}=\omega$, $1\le r\le n$. Ονομάζουμε, τότε, την ακολουθία μας ***γεωμετρική πρόοδο.*** Οι όροι μιας γεωμετρικής προόδου είναι, λοιπόν, οι $a_1, a_1\omega, \ldots, a_1\omega^{r-1}, \ldots, a_1\omega^{n-1}$. Το άθροισμα $S=a_1+a_1\omega+\ldots+a_1\omega^{n-1}$ βρίσκεται, αν πολλαπλασιάσουμε και τα δύο σκέλη της προηγούμενης ισότητας επί $1-\omega$, $\omega\ne 1$, οπότε και έχουμε,

$(1-\omega)S=a_1+a_1\omega+\ldots+a_1\omega^{n-1}-(a_1\omega+a_1\omega^2+\ldots+a_1\omega^n)$, δηλαδή, $S=\frac{a_1(1-\omega^n)}{1-\omega}$. Και, επειδή ο n-στός όρος $a_n=a_1\omega^{n-1}$, $S=\frac{a_1-a_n\omega}{1-\omega}$.

Θα εξετάσουμε, τώρα, ακολουθίες a όπου $a_r=(a+br)\omega^r$. Όπως θα έχει διαπιστώσει ο παρατηρητικός αναγνώστης, για να αθροίσουμε τους n πρώτους όρους της ακολουθίας που μας δίδεται, προσπαθούμε να γράψουμε τον a_r όρο, ως διαφορά $a_r=u_r-v_r$, τέτοια ώστε $u_{r+1}=v_r$, οπότε, κατά την άθροιση οι ενδιάμεσοι όροι μηδενίζονται.

Για την συγγεκριμένη ακολουθία είναι,

$$S=(a+b)\omega+(a+2b)\omega^2+\ldots+(a+rb)\omega^r+\ldots+(a+nb)\omega^n$$

οπότε, αν πολλαπλασιάσουμε και τα δύο μέλη της προηγούμενης ισότητας επί $1-\omega$ λαβαίνουμε, $(1-\omega)S=(a+b)\omega+\sum_{r=2}^{n}(a+rb)\omega^r-\sum_{r=2}^{n}\big(a+(r-1)b\big)\omega^r+(a+nb)\omega^{n+1}$, άρα και,

$$(1-\omega)S=(a+b)\omega+b\sum_{r=2}^{n}r\omega^r+(a+nb)\omega^{n+1}$$

και ο μεσαίος όρος είναι γεωμετρική πρόοδος, η οποία αθροίζεται, αν πολλαπλασιάσουμε άλλη μία φορά επί $1-\omega$.

Γενικά, αν $a_r=f(r)\omega^r$, όπου $f(r)=p_0r^k+p_1r^{k-1}+\ldots+p_k$, οι n πρώτοι όροι της ακολουθίας αθροίζονται, αν πολλαπλασιάσουμε, όπως προηγουμένως, επί $(1-\omega)^{k+1}$.

Πριν εξετάσουμε περιπτώσεις που περιλαμβάνουν και την ακολουθία γ), θα ασχοληθούμε, λίγο, με την μέθοδο ***των πεπερασμένων διαφορών*** του Newton.

Ξεκινάμε από την ακολουθία a: $a_1, a_2, \ldots, a_n, \ldots$. Θεωρούμε το σύνολο $\mathcal{A}$ των ακολουθιών αυτών, και ορίζουμε ότι, $\forall(a,b)\in\mathcal{A}\times\mathcal{A}$, $a+b=c\in\mathcal{A}$, όπου $c_r=a_r+b_r$, και

$$\forall a\in\mathcal{A},\ \lambda a=c\in\mathcal{A},\ \text{όπου}\ c_r=\lambda a_r,\ \lambda\in\mathbb{Z}.$$

Εισάγουμε, τώρα, την απεικόνιση (λέμε, τον "τελεστή") $\Delta : \mathcal{A} \to \mathcal{A}$, η οποία ορίζεται από την σχέση $\Delta a_n = a_{n+1} - a_n$, $1 \le n$. Παρατηρούμε ότι, αν με "0" συμβολίσουμε την ακολουθία εκείνη, της οποίας όλοι οι όροι είναι μηδενικά, τότε έχουμε ότι, $\Delta a = 0$, ανν, $a_{r+1} = a_r$, $1 \le r \le n$. Ισχύει εξ' άλλου ότι, $\Delta(\lambda a + \mu b) = \lambda \Delta a + \mu \Delta b$ (λέμε ότι, ο Δ είναι ένας ***γραμμικός τελεστής***). Συνέπεια της γραμμικότητας του Δ είναι ότι, $\Delta(a_{n+1} - a_n) = \Delta a_{n+1} - \Delta a_n$.
Εφαρμόζουμε τον Δ στην ακολουθία $a' = \Delta a$.
Είναι $\Delta a' = \Delta(\Delta(a)) = \Delta^2(a)$, με, $\Delta^2 a_n = \Delta(a_{n+1} - a_n) = \Delta a_{n+1} - \Delta a_n = a_{n+2} - 2a_{n+1} + a_n$.
Εφαρμόζουμε πάλι τον τελεστή Δ στην προκύπτουσα ακολουθία, και έχουμε,

$$\Delta^3 a_n = \Delta(a_{n+2} - 2a_{n+1} + a_n) = a_{n+3} - 3a_{n+2} + 3a_{n+1} - a_n .$$

Επαγωγικά, αποδυκνείεται η σχέση, $\Delta^k a_n = \sum_{i=0}^{k} (-1)^i C(k,i) a_{n+k-i}$.

Εξ' ορισμού θέτουμε, βέβαια, $\Delta^0 a_n = a_n$ και $\Delta^1 a_n = \Delta a_n$. Δ^0 είναι, λοιπόν, η ταυτοτική απεικόνιση. Την συμβολίζουμε και με το 1.
Αποδεικνύεται, ακόμα, και ότι $\Delta^m(\Delta^n) = \Delta^{m+n} = \Delta^n(\Delta^m)$.

Παράδειγμα. Αν,

τότε	a:	1		4		9		16		25	. . .
	Δa:		3		5		7		9	. . .	
	Δ^2a:			2		2		2	. . .		
	Δ^3a:				0		0	. . .			

Ορισμός. Ορίζουμε τον ***τελεστή*** $\sum_{i=0}^{p} \lambda_i \Delta^i : a \to a'$, από την σχέση

$$\left(\sum_{i=0}^{p} \lambda_i \Delta^i \right) a_n = \sum_{i=0}^{p} \lambda_i \Delta^i a_n .$$

Για $r \ge 1$, ορίζουμε επαγωγικά ότι, $(1+\Delta)^r = (1+\Delta)(1+\Delta)^{r-1}$.

Ισχύει ότι, $(1+\Delta)^r a_n = \sum_{i=0}^{r} C(r,i) \Delta^i a_n$. Παρατηρούμε ότι, $a_{n+1} = a_n + (a_{n+1} - a_n) = a_n + \Delta a_n$.

Άρα και, $a_{n+1} = (1+\Delta) a_n = (1+\Delta)^2 a_{n-1} = \ \ldots \ = (1+\Delta)^n a_1$, συνεπώς, και

$$a_{n+1} = (1+\Delta)^n a_1 = \sum_{k=0}^{n} C(n,k) \Delta^k a_1 .$$

Η προηγούμενη ισότητα λέγεται ***τύπος διαφοράς του Newton.***

Για κάθε ακολουθία a, μπορούμε να βρούμε μία ακολουθία b, τέτοια ώστε, $\Delta b = a$. Πράγματι, ως ακολουθία b αρκεί να λάβουμε αυτήν, που έχει γενικό όρο τον $b_r = a_1 + a_2 + \ \ldots \ + a_{r-1}$, $2 \le r \le n$, $b_1 = 0$. Τότε, για την b έχουμε ότι, $\Delta b = \{b_{r+1} - b_r\} = \{a_r\} = a$. Αν, τώρα, είχαμε βρει και μίαν άλλη ακολουθία c, με την ίδια ιδιότητα, δηλαδή, $\Delta c = a$, τότε, θα είχαμε και ότι $\Delta c = \Delta b$, οπότε η ακολουθία $\Delta(c - b)$ θα ήταν η μηδενική ακολουθία. Οι όροι δηλαδή της $c - b$, είναι, όλοι ίσοι, και συνεπώς, δεν εξαρτώνται από τον συγκεκριμένο δείκτη n του όρου.

Ένα ***μερικό άθροισμα*** της ακολουθίας a, έχει την μορφή $s_r = s_{r-1} + a_r$, $0 \le r \le n$, με $s_0 = 0$.

Έστω, τώρα, b μιά ακολουθία τέτοια ώστε, $\Delta b = a$, και s_n ένα μερικό άθροισμα της ακολουθίας a. Έχουμε ότι, $\Delta s_n = a_{n+1} = (1+\Delta)^n a_1 = (1+\Delta)^n \Delta b_1 = \Delta(1+\Delta)^n b_1$. Άρα, η ακολουθία
$\Delta s_n - \Delta(1+\Delta)^n b_1 = \Delta(s_n - (1+\Delta)^n b_1)$ είναι η μηδενική ακολουθία. Συνεπώς, οι όροι της $s_n - (1+\Delta)^n b_1$, είναι όλοι ίσοι, προς $s_1 - (1+\Delta)b_1 = a_1 - b_1 - \Delta b_1 = a_1 - b_1 - a_1 = -b_1$. Είναι, λοιπόν, και $s_n = (1+\Delta)^n b_1 - b_1 = \{(1+\Delta)^n - 1\}b_1$

$$= \sum_{r=1}^{n} C(n,k)\Delta^r b_1 = C(n,1)a_1 + C(n,2)\Delta a_1 + \ \dots \ + C(n,r)\Delta^{r-1}a_1 + \ \dots \ + \Delta^{n-1}a_1 .$$

Παράδειγμα. Έστω a η ακολουθία του προηγουμένου παραδείγματος. Εφαρμόζουμε τον προηγούμενο τύπο, για την εύρεση του αθροίσματος των n πρώτων όρων της ακολουθίας αυτής παρατηρώντας ότι, για $r \geq 3$, $\Delta^r a = 0$. Είναι,

$$s_n = \sum_{r=1}^{n} C(n,k)\Delta^r b_1 = C(n,1)a_1 + C(n,2)\Delta a_1 + C(n,3)\Delta^2 a_1, \quad \text{ή}$$
$$s_n = C(n,1)\times 1 + C(n,2)\times 3 + C(n,3)\times 2 \qquad \text{άρα και,}$$
$$s_n = n + \frac{3}{2}(n-1) + \frac{1}{3}n(n-1)(n-2) = \frac{1}{6}n(n+1)(2n+1)$$

όπως το υπολογίσαμε παραπάνω.

Ορισμός. Μία σχέση της μορφής $c_0 a_{n+r} + c_1 a_{n+r-1} + \ \dots \ + c_r a_n = f(n)$, όπου a_i, $n \leq i \leq n+r$ είναι όροι μιάς ακολουθίας $a \in \mathcal{A}$ και οι συντελεστές c είναι δοσμένοι σταθεροί ακέραιοι αριθμοί, καλείται ***γραμμική εξίσωση διαφοράς*** (διαφοροεξίσωση) με σταθερούς συντελεστές.

Αν γνωρίζουμε τις r αρχικές συνθήκες, που προσδιορίζουν τους a_i, $1 \leq i \leq r$ πρώτους όρους τις ακολουθίας a, μπορούμε να προσδιορίσουμε με την βοήθεια της παραπάνω ισότητας τον a_{1+r} όρο της ακολουθίας. Στην συνέχεια, υπολογίζουμε τους επόμενους διαδοχικούς όρους της.
Το ερώτημα που τίθεται, είναι αν μπορούμε να υπολογίσουμε τον τυχόντα a_n όρο, $n > r$, χωρίς να είμαστε υποχρεωμένοι να υπολογίσουμε όλους τους προηγούμενους όρους της ακολουθίας. Η σχέση που μου δίδει τον a_n μόνο από τις αρχικές συνθήκες και τους συντελεστές c, καλείται ***λύσις*** της διαφοροεξίσωσις.

Ως γνωστόν, η λύση μιάς γραμμικής εξισώσεως ισούται πάντα, με την γενική λύση της ομογενούς της, συν μιάς ειδικής λύσης της.
Ας δούμε λοιπόν, πως είναι δυνατόν να βρούμε την γενική λύση της ομογενούς. Για τον σκοπό αυτό, θα θεωρούμε εκτός της ομογενούς $c_0 a_{n+r} + c_1 a_{n+r-1} + \ \dots \ + c_r a_n = 0$ (1), και την ***βοηθητική*** ή ***χαρακτηριστική*** της εξίσωση $c_0 x^r + c_1 x^{r-1} + \ \dots \ + c_r = 0$ (2). Ισχύει, σχετικά, το

Θεώρημα. Στην περίπτωση, που οι ρίζες της (2) είναι όλες διαφορετικές, τότε η γενική λύση της (1) έχει την μορφή $a_n = \Gamma_1 \rho_r^n + \Gamma_2 \rho_{r-1}^n + \ \dots \ + \Gamma_r \rho_1^n$ (3), όπου ρ_i οι r διαφορετικές ρίζες της (2), και Γ_i συντελεστές, που προσδιορίζονται από τις αρχικές συνθήκες. Στην περίπτωση πολλαπλής ρίζας ρ_j πολλαπλότητας k, στο άθροισμα (3) εμφανίζονται όροι της μορφής $\left(\sum_{i=1}^{k} B_i n^{i-1} \right) \rho_j^n$.

Θα αποδείξουμε το θεώρημα για την περίπτωση $r=2$. Η γενική περίπτωση έχει παρόμοια απόδειξη.
Ξεκινάμε, λοιπόν, από την εξίσωση $a_{n+2}+c_1a_{n+1}+c_2a_n=0$. Η χαρακτηριστική εξίσωση αυτής, είναι η $x^2+c_1x+c_2=0$, με ρίζες τις $\rho_1\neq\rho_2$. Θεωρούμε και την ακολουθία b, που ορίζεται από την σχέση $b_{n+2}=a_{n+2}-\rho_1a_{n+1}$. Τότε, $b_{n+2}-\rho_2b_{n+1}=(a_{n+2}-\rho_1a_{n+1})-\rho_2(a_{n+1}-\rho_1a_n)$

$$=a_{n+2}-(\rho_1+\rho_2)a_{n+1}+\rho_1\rho_2a_n$$
$$=a_{n+2}+c_1a_{n+1}+c_2a_n=0.$$

Άρα, $b_{n+2}=\rho_2b_n=\rho_2^2b_{n-1}=\ \dots\ =\rho_2^nb_1$, οπότε και, $a_{n+1}-\rho_1a_n=\rho_2^nb_1$. Με τον ίδιο τρόπο, θεορώντας την ακολουθία b΄ που ορίζεται από την σχέση $b'_{n+2}=a_{n+2}-\rho_2a_{n+1}$, λαβαίνουμε και την ισότητα $a_{n+1}-\rho_2a_n=\rho_1^nb'_1$. Άρα και, $(\rho_1-\rho_2)a_n=\rho_1^nb'_1-\rho_2^nb_1$. Είναι, λοιπόν,

$$a_n=\frac{\rho_1^nb'_1-\rho_2^nb_1}{\rho_1-\rho_2}.$$

Παράδειγμα. 1) Θα υπολογίσουμε τον n όρο της ακολουθίας γ) του ***Fibonacci.*** Έχουμε αρχικές συνθήκες $a_1=1,\ a_2=1$, και αναγωγική σχέση, την $a_{n+2}-a_{n+1}-a_n=0$. Η χαρακτηριστική εξίσωση είναι η $x^2-x-1=0$ με ρίζες $\rho_1=\frac{1+\sqrt{5}}{2}$ και $\rho_2=\frac{1-\sqrt{5}}{2}$.

Άρα και, $a_n=\frac{\rho_1^nb'_1-\rho_2^nb_1}{\rho_1-\rho_2}$. Για τα b_1, b'_1, έχουμε, εξ' ορισμού, ότι, $b_1=a_2-\rho_1a_1$ και $b'_1=a_2-\rho_2a_1$. Είναι, λοιπόν, $a_n=\frac{1}{\sqrt{5}}\left\{\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right\}$.

2) Θα λύσουμε την διαφοροεξίσωση $a_{n+3}+6a_{n+2}+12a_{n+1}+8a_n=0$, με αρχικές συνθήκες τις $a_1=1,\ a_2=-2,\ a_3=8$. Η χαρακτηριστική εξίσωση, είναι η $x^3+6x^2+12x+8=0$, η οποία έχει τριπλή ρίζα $\rho=-2$. Άρα είναι, $a_n=(B_1+B_2n+B_3n^2)\rho^n$. Οι αρχικές συνθήκες, δίδουν για τα B τις τιμές $B_1=1,\ B_2=-1/2,\ B_3=1/2$.

3) Να λυθεί η διαφοροεξίσωση $a_{n+2}=a_{n+1}-a_n$, με αρχικές συνθήκες $a_1=1$ και $a_2=0$.
Η χαρακτηριστική εξίσωση είναι η $x^2-x+1=0$, με μιγαδικές ρίζες $\rho=\frac{1\pm i\sqrt{3}}{2}$, οπότε έχουμε ότι, $a_n=\Gamma_1\cos\frac{n\pi}{3}+\Gamma_2\sin\frac{n\pi}{3}$, όπου $\Gamma_1=1$ και $\Gamma_2=\frac{1}{\sqrt{3}}$.

Στην περίπτωση, που έχουμε να λύσουμε μη ομογενή διαφοροεξίσωση, στην γενική λύση της ομογενούς θα πρέπει να προσθέσουμε και μιά κάποια λύση (η ειδική λύση) αυτής. Η ειδική λύση βρίσκεται με δοκιμές. Συνήθως, αυτή έχει την μορφή $a_n=\alpha n+\beta$, όπου α και β κατάλληλες σταθερές.

Παράδειγμα. 1) Να λυθεί η διαφοροεξίσωση $a_{n+1}+2a_n=n+3$ με αρχικές συνθήκες $a_1=3$.
Η ρίζα της χαρακτηριστικής $x+2=0$ είναι η $\rho=-2$, οπότε η λύση της ομογενούς είναι η $a_n=\Gamma(-2)^n$. Για ειδική λύση δοκιμάζουμε μία της μορφής $a_n=\alpha n+\beta$.

Είναι, $\alpha n+\beta+2\left[(\alpha(n-1)+\beta\right]=n+3$, ή $3\alpha n-2\alpha+3\beta=n+3$. Η ισότητα αυτή ισχύει βέβαια για κάθε $n\geq 1$. Άρα, $3\alpha=1$ και $-2\alpha+3\beta=3$, απ' όπου, $\alpha=\frac{1}{3}$ και $\beta=\frac{11}{9}$. Η γενική λύση της διαφοροεξίσωσης, είναι, λοιπόν, η $a_n=\Gamma(-2)^n+\frac{n}{3}+\frac{11}{9}$. Για $n=1$, η αρχική συνθήκη δίδει την τιμή $\Gamma=\frac{16}{9}$.

Παράδειγμα. 2) **Οι Πύργοι του Ανόϊ.** Σε ένα στέλεχος Α υποθέτουμε ότι έχουμε περάσει τέσσερις δίσκους, τους 1, 2, 3, 4 των οποίων οι διάμετροι βρίσκονται στην σχέση:
διάμετρος του δίσκου 1 < διάμετρος του δίσκου 2 . . . < διάμετρος του δίσκου 4.
Θέλουμε να μεταφέρουμε τους δίσκους από το στέλεχος Α στο στέλεχος Γ έτσι ώστε και στο στέλεχος Γ να έχουν την ίδια διάταξη.
Επιτρέπεται να χρησιμοποιήσουμε ένα και μόνον βοηθητικό στέλεχος Β. Επιτρέπεται να κινούμε ένα και μόνον δίσκο κάθε φορά, και να τον θέτουμε σε στέλεχος το οποίο περιέχει δίσκο με διάμετρο μεγαλύτερη απ' αυτήν του μετακινούμενου, είτε, δεν περιέχει απολύτως κανένα δίσκο.
Η μετακίνηση των δίσκων επιτυγχάνεται αν εκτελέσουμε διαδοχικά τις παρακάτω κινήσεις, όπως αυτές περιγράφονται στον παρακάτω πίνακα:

Παρατήρηση. Οι τέσσερις δίσκοι τοποθετήθηκαν στο στέλεχος Γ μετά από 15 κινήσεις. Παρατηρούμε ότι οι 3 δίσκοι έχουν τοποθετηθεί στο στέλεχος Β μετά από 7 κινήσεις και τέλος, οι δύο δίσκοι έχουν τοποθετηθεί στο στέλεχος Γ μετά από 3 κινήσεις. Όμως, $15 = 2\times7+1$, $7 = 2\times3+1$ και, τέλος, $3 = 2\times1+1$

$0^{η}$ Κίνηση:	Α	Β	Γ		$8^{η}$ Κίνηση:	Α	Β	Γ
	1						1	
	2						2	
	3						3	
	4							4
$1^{η}$ Κίνηση:	Α	Β	Γ		$9^{η}$ Κίνηση:	Α	Β	Γ
		1						1
	2						2	
	3						3	
	4							4
$2^{η}$ Κίνηση:	Α	Β	Γ		$10^{η}$ Κίνηση:	Α	Β	Γ
		1						1
			2			2		
	3						3	
	4							4
$3^{η}$ Κίνηση:	Α	Β	Γ		$11^{η}$ Κίνηση:	Α	Β	Γ
			1			1		
			2			2		
	3						3	
	4							4
$4^{η}$ Κίνηση:	Α	Β	Γ		$12^{η}$ Κίνηση:	Α	Β	Γ
			1			1		
			2			2		
		3						3
	4							4
$5^{η}$ Κίνηση:	Α	Β	Γ		$13^{η}$ Κίνηση:	Α	Β	Γ
	1						1	
			2			2		
		3						3
	4							4
$6^{η}$ Κίνηση:	Α	Β	Γ		$14^{η}$ Κίνηση:	Α	Β	Γ
	1						1	
		2						2
		3						3
	4							4
$7^{η}$ Κίνηση:	Α	Β	Γ		$15^{η}$ Κίνηση:	Α	Β	Γ
		1						1
		2						2
		3						3
	4							4

Οι σχέσεις αυτές οδηγούν στον αναγωγικό τύπο $T_n = 2T_{n-1} + 1$, όπου T_n είναι ο αριθμός των κινήσεων που απαιτούνται για την μετακίνηση n δίσκων.

Ζητάμε να βρούμε την τιμή του T_n, χωρίς προηγουμένως να έχουμε υπολογίσει την τιμή του T_{n-1} (αυτό λέγεται «λύση του αναγωγικού τύπου»). Σκεφτόμαστε ως εξής: Αν x είναι μία φορά λύση του αναγωγικού τύπου, τότε x^n είναι (αρχή του πολλαπλασιασμού) η λύση του αναγωγικού τύπου μετά την εφαρμογή του n φορές. Η $T_n = 2T_{n-1} + 1$ (1) μετατρέπεται, λοιπόν, στην $x^n = 2x^{n-1} + 1$ (χαρακτηριστική εξίσωση). Θεωρούμαι την ομογενή εξίσωση της (1), με χαρακτηριστική εξίσωση την $x^n - 2x^{n-1} = x^{n-1}(x-2) = 0$. Η γενική λύση της (1) είναι, λοιπόν, $T_n = 2^n - 1$.

Πράγματι, για $n = 4$, $T_4 = 2^4 - 1 = 15$. Το -1 προέρχεται, βέβαια, από την αρχική τιμή $T_0 = 0$.

Παράδειγμα. 3) **Οι αριθμοί του Bernoulli.** Υπολογίσαμε παραπάνω τα αθροίσματα $S_m(n)$. Παρατηρούμε ότι, κάθε τέτοιο άθροισμα των m δυνάμεων των n διαδοχικών ακεραίων, είναι ένα πολυώνυμο του n, βαθμού $m+1$. Ο Jakob Bernoulli στο **Ars Conjectandi** (1713), υπολόγισε τους συντελεστές των πολυωνύμων αυτών, οι οποίοι και φέρουν το όνομά του.

Ορισμός. Η ακολουθία των αριθμών Bernoulli ορίζεται επαγωγικά, ως εξής:

$B_0 = 1$ και αν $B_0, B_1, \ldots, B_{m-1}$ έχουν υπολογιστεί, τότε $(m+1)B_m = -\sum_{k=0}^{m-1} C(m+1,k)B_k$.

Για $m = 0$ έχουμε ότι $B_0 = 1$

Για $m = 1$ έχουμε ότι $2B_1 = -\sum_{k=0}^{1-1} C(2,0)B_0 = -1$, απ' όπου $2B_1 = -1$

Για $m = 2$ έχουμε ότι $3B_2 = -C(3,0)B_0 - C(3,1)B_1 = 1 - 3B_1$, κ.λ.π.

Οι αριθμοί Bernoulli θα μπορούσαν, συνεπώς, να ορισθούν και ως λύσεις του συστήματος

$$\begin{aligned} 1 + 2B_1 &= 0 \\ 1 + 3B_1 + 3B_2 &= 0 \\ 1 + 4B_1 + 6B_2 + 4B_3 &= 0 \\ \ldots \quad & \ldots \quad \ldots \end{aligned}$$

(Τρίγωνο του Pascal)

10. Διαιρετότης εν $\mathbb{Z}$. Ιδεώδη. Θα λέμε ότι ο b διαιρεί τον a, και γράφουμε b | a, ανν a = qb. Οι q και b λέγονται παράγοντες ή διαιρέτες του a. Η σχέση " | " είναι αυτοπαθής και μεταβατική. Είναι συνεπώς, μια σχέση μερικής διατάξεως εν $\mathbb{Z}$.

Από το γεγονός ότι, μεταξύ του 0 και του 1 δεν περιέχεται κανείς ακέραιος, έπεται ότι, οι μοναδικές μονάδες του $\mathbb{Z}$ είναι οι +1 και −1. Πόρισμα του γεγονότος αυτού, είναι ότι, αν a | b και b | a, τότε και a = ±b.

Ορισμός. Ο $p \in Z$ καλείται πρώτος, αν $p \neq 0$, $p \neq \pm 1$, και αν ο p διαιρείται μόνον από το ±1 και το ±p.

Θεώρημα. ***Αλγόριθμος του Ευκλείδη.*** Δοθέντων των a και b, a > b > 0, υπάρχουν ακέραιοι r και q, τέτοιοι ώστε, a = bq+r με r < b.

Απόδειξη. Θεωρούμε το σύνολο $S = \{a - bx \mid x \in Z\}$. Το σύνολο των θετικών στοιχείων του S είναι μη κενό, μια και για x = 0, $a \in S$. Έστω r το ελάχιστο στοιχείο του συνόλου αυτού. Θα δείξουμε ότι, r ≤ b. Πράγματι, αν r > b, τότε, a−b(q+1) = a−bq−b ή επειδή r = a−bq, a−b(q+1) = r−b > 0. Το r−b έχει την μορφή a−xb, άρα $r - b \in S$, και είναι θετικό. Άρα πρέπει να είναι μεγαλύτερο από το ελάχιστο στοιχείο r. Άτοπον

Θα δείξουμε, τώρα, ότι οι αριθμοί q και r είναι μοναδικοί. Πράγματι, αν είχαμε και την a = bq′+r′, με r′ < b, τότε και, b(q−q′) = r′−r > 0, μια και r = ελάχιστο. Άρα q−q′ > 0, μια και b > 0. Τότε όμως, r′ = kb+r, δηλαδή, r′ > b. Άτοπον.

Θεώρημα. Κάθε μη κενό σύνολο ακεραίων S, κλειστό ως προς την πρόσθεση (και την αφαίρεση), περιέχει ένα ελάχιστο θετικό στοιχείο d, τέτοιο ώστε, κάθε στοιχείο, που ανήκει στο S, να γράφεται ως πολλαπλάσιο rd του d, με $r \in Z$.

Απόδειξη. Το S περιέχει και θετικά στοιχεία. Πράγματι, αν $a \neq 0$, $a \in S$, τότε και το $0 = a - a \in S$, οπότε και το $0 - a = -a \in S$. Έχουμε λοιπόν, ένα ελάχιστο θετικό στοιχείο $d \in S$.

α) Κάθε rd = d+ . . . +d r φορές, ανήκει συνεπώς στο S. β) Θα δείξουμε, τώρα, ότι το S περιέχει μόνο στοιχεία της μορφής αυτής. Προς τούτο, έστω το $b \in S$, b > 0, $b \neq rd$.

Είναι, b > d. Άρα και b = qd+ρ, ρ < d. Άρα, $\rho = b - qd \in S$. Άτοπον.

Ορισμοί. Κάθε υποσύνολο I ενός αντιμεταθετικού δακτυλίου Δ, το οποίο είναι κλειστό ως προς την πρόσθεση (και τη αφαίρεση) του Δ, και το οποίο έχει την ιδιότητα, με το τυχόν $a \in I$ να περιέχει και κάθε πολλαπλάσιό του ra, $r \in \Delta$, καλείται ***ιδεώδες*** (Ideal) του Δ. Ένα ιδεώδες I που έχει την ιδιότητα, να περιέχει κάποιο στοιχείο d, τέτοιο ώστε, $\forall r \in \Delta$, $rd \in I$, και μόνον αυτά,

καλείται ***κύριο ιδεώδες*** (principal Ideal). Ένα κύριο ιδεώδες συμβολίζεται και (d). Το (d) είναι το ελάχιστο ιδεώδες, που περιέχει το d, με την έννοια ότι, κάθε άλλο ιδεώδες που περιέχει το d, θα περιέχει και κάθε πολλαπλάσιό του, και συνεπώς, θα περιέχει το (d). Ένα ιδεώδες M του Δ θα καλείται ***μέγιστο ιδεώδες*** του Δ, ανν δεν υπάρχει ιδεώδες I του Δ τέτοιο ώστε $M \subset I \subset \Delta$. Βλέπε και [ZK], σελ. 41, 53. Αν το Δ είναι σώμα, τότε περιέχει μόνον κύρια ιδεώδη, μια και το $1 \in I$, επειδή αν $a \in I$, $\exists a^{-1} \in \Delta$ με $a^{-1}a = 1$. Μέσα σε έναν αντιμεταθετικό δακτύλιο Δ, ένα ιδεώδες του $I \subset \Delta$ θα καλείται ***πρώτο ιδεώδες*** ανν $ab \in I \rightarrow a \in I$ είτε $b \in I$, $\forall a, b \in \Delta$.

Παραδείγματα. α) Τα σύνολα I = (0) και I = Δ αποτελούν ιδεώδη του Δ. Αυτά καλούνται και ***τετριμμένα*** ιδεώδη του Δ.

β) Έστω $m \in \mathbb{Z}$ και $I = \{\lambda m \mid \lambda \in \mathbb{Z}\}$. Το I είναι ιδεώδες.

Ισχύει ότι, $m_1 \mid m_2 \rightarrow (m_2) \subseteq (m_1)$

Πόρισμα. Το $\mathbb{Z}$ είναι ακέραια περιοχή κυρίων Ιδεωδών (δηλαδή, κάθε ιδεώδες του $\mathbb{Z}$ είναι κύριο ιδεώδες).

Μία απεικόνιση $f : \Delta \rightarrow \Delta'$ είναι ένας μορφισμός, αν και μόνον αν, είναι μορφισμός ως προς κάθε μία πράξη, που ορίζεται εν Δ και Δ΄. (Βλέπε §10). Αν η f δεν είναι ισομορφισμός, θα ονομάζουμε αυτήν ***ομομορφισμό. Πυρήνας*** K του ομομορφισμού f είναι το σύνολο των στοιχείων του Δ, που απεικονίζονται δια της f στο $0' \in \Delta'$. Πάντοτε $K \neq \varnothing$, μιά και $0 \in K$ αφού, όπως εύκολα βλέπουμε, $f(0) = 0'$. Εξ' άλλου, $\forall x, y \in K$, $\lambda x + \xi y \in K$, $\lambda, \xi \in \Delta$. Ο K είναι, λοιπόν, ιδεώδες του Δ. Η f είναι ισομορφισμός, αν και μόνον αν, $K = \{0\}$.

Ορισμός-Παρατηρήσεις. Η σχέση $\Delta \times \Delta \supset R \ni (x, y)$ ανν $x - y \in I$, I ιδεώδες του Δ, ορίζει μια σχέση ισοδυναμίας επί του Δ. Γράφουμε $x = y(I)$ για να συμβολίσουμε την σχέση αυτή. Πράγματι, είναι α) $x = x(I)$, μια και $\Delta \ni 0 = 0x = 0 \in I$, β) $x = y(I) \rightarrow y = x(I)$, μια και η $x - y \in I$ δίδει την $x = y + h$, $h \in I$, άρα και $y = x - h$ και το $-h \in I$ μια και το I είναι κλειστό ως προς την πρόσθεση, και $h + (-h) = 0 \in I$. γ) ανάλογα αποδεικνύεται και η απομένουσα μεταβατική ιδιότης. Το σύνολο των ισοδυνάμων του a στοιχείων x του Δ το συμβολίζουμε με $[a]$. Επειδή όμως είναι για $x \in [a]$, $x = a + h$, $h \in I$, γράφουμε και $[a] = a + I$. Οι πράξεις του δακτυλίου Δ μεταφέρονται στο σύνολο πηλίκο (βλέπε ενότητα σύνολα, §4 και §5) $\Delta / I = \{[a],\ a \in \Delta\}$, αν τις ορίσουμε ως εξής: $[a] + [b] = [a + b]$ και $[a][b] = [ab]$. Το Δ / I αποκτά συνεπώς και αυτό την δομή του δακτυλίου. Μπορούμε όμως να έχουμε κάτι παραπάνω, όπως θα δούμε παρακάτω.

Θεώρημα. Έστω Δ αντιμεταθετικός δακτύλιος με μονάδα. Το M είναι μέγιστο ιδεώδες του Δ, ανν το Δ / M είναι σώμα.

Απόδειξη. Εύκολα φαίνεται ότι και ο δακτύλιος Δ / M είναι αντιμεταθετικός δακτύλιος με μονάδα. Έστω $[a] = a + M$ το τυχόν στοιχείο του Δ / M, $a \notin M$. Θα δείξουμε ότι το στοιχείο αυτό έχει αντίστροφο. Προς τούτο, θεωρούμε το σύνολο $N = \{ra + m\}$, όπου $r \in \Delta$ και $m \in M$. Εύκολα αποδεικνύεται ότι το N είναι ιδεώδες του Δ. Επειδή $a = 1a + 0$, $a \in N$, και για $m \in M$, η ταυτότης $m = 0m + m$ δείχνει ότι, $M \subseteq N$. Όμως το M μέγιστο ιδεώδες του Δ. Άρα είτε $M = N$, είτε $N = \Delta$. Η πρώτη ισότης αποκλείεται μια και το N περιέχει το a, το οποίο από υπόθεση $a \notin M$. Άρα $N = \Delta$. Ιδιαίτερα, $1 \in N$. Συνεπώς, ως εκ του ορισμού του N υπάρχουν $b \in \Delta$ και $m \in M$ τέτοια ώστε $1 = ba + m$.

Άρα, $1 + M = ba + M = (b + M)(a + M)$.

Αντίστροφα, έστω ότι το Δ/M είναι σώμα. Τότε κάθε ιδεώδες του είναι κύριο, άρα και μέγιστο.

Πόρισμα. Έστω Δ αντιμεταθετικός δακτύλιος με μονάδα. Τότε κάθε μέγιστο ιδεώδες είναι και πρώτο ιδεώδες. Και αντίστροφα.
Απόδειξη. Αν το M μέγιστο, το Δ/M σώμα. Μέσα στο Δ/M δεν έχουμε, λοιπόν, διαιρέτες του μηδενός. Το μηδενικό στοιχείο όμως του Δ/M είναι το $[0] = 0 + M = M$. Η σχέση συνεπώς $(a + M)(b + M) = M$ συνεπάγεται είτε την $a + M = M$ είτε την $b + M = M$.

Ορισμός. Ο d καλείται μ.κ.δ. (μέγιστος κοινός διαιρέτης) των ακεραίων a και b, αν d | a, d | b και για κάθε άλλο $c\in\mathbb{Z}$ με c | a και c | b, είναι και c | d. Τον μ.κ.δ. των αριθμών a και b των συμβολίζουμε με το (a,b).

Πρόταση Bezout. Δύο οιαδήποτε ακέραιοι a και b έχουν θετικό μ.κ.δ. d = sa+tb.
Απόδειξη. Θεωρούμε το σύνολο S = {sa+tb | s, t∈**Z**}. Το S είναι φανερά, κλειστό ως προς την πρόσθεση (και την αφαίρεση). Άρα περιέχει ένα ελάχιστο θετικό στοιχείο d = sa+tb, τέτοιο ώστε, κάθε άλλο στοιχείο του S να είναι πολλαπλάσιο του d. Είναι d = (a,b). Πράγματι, τα a και b∈S, και άρα d | a και d | b. Εξ' άλλου, αν το c | a, και c | b, δηλαδή, αν
a = λc, b = μc, τότε και d = λsc+μtc = κc, δηλαδή, c | d.

Τον μ.κ.δ. των αριθμών a και b τον ευρίσκουμε, αν εφαρμόσουμε τον αλγόριθμο της διαιρέσεως. Είναι πράγματι,

$$\begin{aligned}
a &= bq_1 + r_1 && \text{με} && 0 \le r_1 < b\\
b &= r_1q_2 + r_2 && && r_2 < r_1\\
r_1 &= r_2q_3 + r_3 && && r_3 < r_2\\
&\ldots && \ldots && \ldots\\
r_{k-2} &= r_{k-1}q_k + r_k && && r_{k-1} < r_k\\
r_{k-1} &= r_kq_{k+1} && \text{μια και για κάποια τιμή του k,} && r_{k+1} = 0.
\end{aligned}$$

Λαβαίνουμε $d = r_k$. Είναι, $d = (r_k, r_{k-1}) = \ldots = (a,b)$.

Πρόταση. Αν p πρώτος και p | AB, τότε είτε p | a είτε p | b.
Απόδειξη. Έστω ότι ο p δεν διαιρεί τον a. Τότε (pa) = 1. Άρα και spυta = 1, οπότε και bsp+bta = b. Όμως, από υπόθεση, ab = λp. Άρα bsp+λtp = b ή κp = b, ή p | b.

Οι a και b θα λέγονται ***μεταξύ τους πρώτοι***, ανν ο μ.κ.δ. d = 1. Γι' αυτούς ισχύει η ***ταυτότητα του*** Bezout, αα+ββ = 1. Ένα ***κοινό πολλαπλάσιο*** των a και b είναι ο ακέραιος z, που έχει τους a και b παράγοντες. Αν είναι d = (a, b), a = λd, b = κd και (λ, κ) = 1, τότε, το ***ελάχιστο κοινό πολλαπλάσιο*** (ε.κ.π.) των a και b είναι λκd.

Παράδειγμα. Έστω a = 365 και b = 1876. Εφαρμόζουμε τον αλγόριθμο του Ευκλείδη:

$$\begin{aligned}
1876 &= 365\times5+51\\
365 &= 51\times7+8\\
51 &= 8\times6+3\\
8 &= 3\times2+2\\
3 &= 2\times1+1\,. \qquad \text{Άρα, } (1876,\ 365) = 1\,.
\end{aligned}$$

Στην συνέχεια, λύνουμε τις παραπάνω ισότητες ως προς τα διαδοχικά υπόλοιπα, και αντικαθιστούμε αυτά, διαδοχικά, αρχίζοντας από την τελευταία ισότητα:

$$\begin{aligned}
1 &= 3-2 = 3-(8-3\times2) = 3\times3-8 = 3\times(51-8\times6)-8 = 3\times51-8\times19\\
&= 3\times51-19\times(365-51\times7) = 136\times51-19\times365
\end{aligned}$$

$= 136\times(1876-5\times365)-19\times365$

$1 = 136\times1876-699\times365$, που είναι η ταυτότητα του Bezout.

Πόρισμα. Μέσα σε μία περιοχή κυρίων ιδεωδών, για τα μη μηδενικά στοιχεία της, ισχύει ότι:

α) Υπάρχει ο μ.κ.δ. d αυτών.

β) Αν $a_i \in \{D\setminus\{0\}\}$, $i = 1, \ldots, n$, τότε $\exists\ \lambda_i \neq 0$, έτσι ώστε, $\sum_{i=1}^{n}\lambda_i a_i = d$.

Πορίσματα. α) Αν $(c,a) = 1$ και $c \mid ab$, τότε και $c \mid b$.

β) Αν $(c,a) = 1$ και $a \mid m$, $c \mid m$, τότε και $ac \mid m$.

γ) Αν $a \mid b$ και $a \mid c$, τότε και, $a \mid (\beta b + \gamma c)$, $\forall \beta,\gamma \in \mathbb{Z}$.

δ) $(a,b) = (a, b+\alpha a)$, $\forall \alpha \in \mathbb{Z}$. ε) $m(a,b) = (ma, mb)$.

στ) Αν $(a,r) = d$ και $(b,r) = 1$, τότε και $(ab,r) = d$.

η) Αν $d = (a,b)$ και $\alpha a + \beta b = d$, τότε και $(\alpha,\beta) = 1$.

θ) Αν $d = (a,b)$, τότε και, $(d) = \{\gamma d \text{ με } \gamma \in \mathbb{Z}\} = \{\alpha a + \beta b \text{ με } \alpha,\beta \in \mathbb{Z}\}$.

Παράδειγμα. Ισχύει ότι, $10^\nu = 1 + \text{πολλαπλάσιο του } 9$. Άρα και, $\lambda 10^\nu = \lambda + \kappa 9$.

Πράγματι, $10^\nu = (1+9)^\nu = \sum_{r=0}^{\nu} C(\nu,r) 1^r 9^{\nu-r} = 1 + \kappa 9$. **Εφαρμογή.** Αν ο $9 \mid$ το άθροισμα των ψηφίων του ακεραίου α, τότε και $9 \mid \alpha$. Αρκεί να γράψουμε τον $\alpha = \sum_{r=0}^{\nu}\lambda_r 10^r = \kappa 9 + \sum_{r=0}^{\nu}\lambda_r$.

Θεμελιώδες Θεώρημα της Αριθμητικής. Κάθε ακέραιος εκφράζεται (±) ως γινόμενο (πεπερασμένου πλήθους) πρώτων θετικών παραγόντων, κατά μοναδικό τρόπο.

Απόδειξη. Με επαγωγή. Έστω P(a) η πρότασης: Ο ακέραιος a είναι δυνατόν να γραφεί ως γινόμενο πεπερασμένου πλήθους παραγόντων. Η P(a) ισχύει προφανώς για a = 1, ή a = p (p πρώτος). Στην περίπτωση, που ο a δεν είναι ο 1 ή πρώτος, έχει έναν θετικό διαιρέτη b έτσι ώστε,

a = bc με b < a, c < a. Από την αρχή της επαγωγής έχουμε ότι, η P(b) και η P(c) ισχύουν. Εκφράζονται συνεπώς οι b και c ως γινόμενα $b = p_1 p_2 \cdots p_k$ και $c = q_1 q_2 \cdots q_m$. Άρα και $a = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_m$.

Η μοναδικότητα της εκφράσεως του a ως γινομένου πρώτων παραγόντων έπεται από το γεγονός ότι αν $a = (\pm)p_1 p_2 \cdots p_k = (\pm)q_1 q_2 \cdots q_m$, (1) τότε και ο p_1 πρέπει να διαιρεί τουλάχιστον έναν παράγοντα q_j. Από την $p_1 \mid q_j$ και το γεγονός ότι οι p_1 και q_j είναι πρώτοι θετικοί, έπεται ότι, $p_1 = q_j$. Μπορούμε συνεπώς να τους διαγράψουμε, και να λάβουμε μία σχέση της μορφής (1) με κατά ένα λιγότερους παράγοντες. Όμως γι' αυτήν ισχύει η υπόθεση της επαγωγής.

Πόρισμα. Κάθε ακέραιος a γράφεται ως γινόμενο $a = (\pm)p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ κατά ένα και μόνο τρόπο.

Παρατήρηση. Έστω $n = ab$, με $a \le b$. Τότε, $a \le \sqrt{n}$. Συμπέρασμα: Αν $n = ab$, τότε οι a και b, δεν είναι δυνατόν να είναι αμφότεροι $> \sqrt{n}$. Άρα, αν p πρώτος παράγων του n, $p \le \sqrt{n}$.

Θεώρημα. Το σύνολο P των πρώτων αριθμών, δεν έχει μέγιστο στοιχείο.

Απόδειξη (του Ευκλείδη). Έστω ότι το σύνολο των πρώτων αριθμών είχε μέγιστο στοιχείο p_n. Τότε, $P = \{p_1 \ \dots \ p_n\}$. Θα δείξουμε ότι, ο $p_1 \cdots p_n + 1 \notin P$, και όμως περιέχει πρώτο παράγοντα $p_m > p_n$. Πράγματι, αν ο $p_1 \cdots p_n + 1$ δεν είναι πρώτος, θα έχει κάποιο πρώτο διαιρέτη $q \in P$. Όμως, $q \mid p_1 \cdots p_n$. Άρα $q \mid (p_1 \cdots p_n + 1 - p_1 \cdots p_n) = 1$, άτοπον.

Σημείωση. Ο αριθμός $N = p_1 p_2 \cdots p_n + 1$ δεν είναι κατ' ανάγκη πρώτος. Παράδειγμα, ο αριθμός $N = 30031 = 30030 + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 509$, ο οποίος, όμως, περιέχει πρώτο παράγοντα μεγαλύτερο του 13.

11. Ορισμός Ισοϋπολοίπων αριθμών. Θεωρούμε το σύνολο των ακεραίων $\mathbb{Z}$. Εισάγουμε στο $\mathbb{Z}$ την εξής διμελή σχέση R: $(\alpha,\beta) \in R$, ανν $\beta - \alpha$ = πολλαπλάσιο του 3. Η R είναι σχέση ισοδυναμίας. Πράγματι: 1) $(\alpha,\alpha) \in R$, μιά και $\alpha - \alpha = 0$, και $0 = 0 \cdot 3$. 2) Αν $(\alpha,\beta) \in R$, τότε και $(\beta,\alpha) \in R$, μιά και η $\beta - \alpha = 3\lambda$, δίδει και την $\alpha - \beta = 3(-\lambda)$, δηλαδή, την $(\beta,\alpha) \in R$. 3) Τέλος, αν $(\alpha,\beta) \in R$ και $(\beta,\gamma) \in R$, δηλαδή, $\beta - \alpha = 3\lambda_1$ και $\gamma - \beta = 3\lambda_2$, τότε οι $\beta = 3\lambda_2 - \gamma$, και $\beta = 3\lambda_1 - \alpha$ δίδουν την
$3\lambda_2 - \gamma = 3\lambda_1 - \alpha$, δηλαδή, την $\gamma - \alpha = 3(\lambda_1 - \lambda_2)$, που είναι η $(\alpha,\gamma) \in R$.
Ας δούμε τώρα, ποίες είναι οι κλάσεις ισοδυναμίας, που μερίζουν το σύνολο $\mathbb{Z}$. Προς τούτο, ας λάβουμε το $1 \in \mathbb{Z}$. Η C_1 περιέχει όλους τους ακεραίους, που διαφέρουν από τον 1, κατά πολλαπλάσιο του 3. Άρα $x \in C_1$ ανν $x = 1+3\lambda$. Οι ακέραιοι αυτοί, είναι εκείνοι, οι οποίοι διαιρούμενοι με το 3, δίδουν υπόλοιπο 1. Είναι λοιπόν, $C_1 = \{\pm 1, \pm 4, \pm 7, \dots\} = [1]_3$.
Επειδή ο $2 \notin C_1$, ας σχηματίσουμε την C_2.
Είναι, με τον ίδιο τρόπο σκεπτόμενοι, $C_2 = \{\pm 2, \pm 5, \pm 8, \dots\} = [2]_3$. Φανερά, μία ακόμα κλάση υπάρχει. Η $C_0 = \{0, \pm 3, \pm 6, \dots\} = [0]_3$, που περιέχει όλα τα πολλαπλάσια του 3.

Γενικεύουμε τα παραπάνω εισάγοντας στο $\mathbb{Z}$ την διμελή σχέση ισοδυναμίας R:
$(\alpha,\beta) \in R$, ανν $\beta - \alpha = \lambda m$. Το σύνολο πηλίκο $\mathbb{Z}/\approx$, που το συμβολίζουμε και με $\mathbb{Z}/(m)$ ή $\mathbb{Z}_m$ αποτελείται από τις κλάσεις $[0]_m$, $[1]_m$, … ,$[m-1]_m$, όπου $\alpha \in [a]_m$, ανν το υπόλοιπο της διαιρέσεως του α από τον n είναι a $(a = 1, \ \dots \ , m-1)$, μιά και τότε, $\alpha = \lambda m + a$, δηλαδή,
$\alpha - a = \lambda m$. Λέμε ότι, οι ακέραιοι $0, 1, \dots, m-1$, αποτελούν ένα ***πλήρες σύστημα καταλοίπων.***

Συμβολισμοί. Αν $\alpha \in C_a = [a]_m$, γράφουμε $\alpha \equiv a (\mathrm{mod}\, m)$, ή και $\alpha \equiv a (m)$. Η σχέση αυτή, ονομάζεται ***ισοτιμία.*** Κάθε κλάση ισοδυναμίας, έχει ελάχιστο θετικό (ή μέγιστο αρνητικό) στοιχείο. Αυτό και χρησιμοποιούμε ως αντιπρόσωπο της κλάσεως, την οποία και συμβολίζουμε, όπως είδαμε, με $[a]_m = \{a + \lambda m \mid \lambda \in \mathbb{Z}\}$, a ο αντιπρόσωπός της..
Παρατήρηση. Οι ακέραιοι που αποτελούν μία κλάση, ευρίσκονται σε αριθμητική πρόοδο. m ακέραιοι, που ανα δύο δεν είναι ισότιμοι, αποτελούν ένα πλήρες σύστημα καταλοίπων.

Το $\mathbb{Z}_m$ καθίσταται αντιμεταθετικός δακτύλιος, αν ορίσουμε μία πρόσθεση "+" και έναν πολλαπλασιασμό "∘" μέσα σ' αυτό, ως εξής: $[a]_m + [b]_m = [a+b]_m$ και $[a]_m \circ [b]_m = [ab]_m$.
Εν $\mathbb{Z}_3 = \{[0]_3, [1]_3 [2]_3\}$ έχουμε, λοιπόν, ότι $[1]_3 + [2]_3 = [0]_3$.
Η $[0]_m$ περιέχει όλα τα πολλαπλάσια του m. Στην περίπτωση, που ο m δεν είναι αριθμός πρώτος, π.χ. $m = \alpha\beta$, $[0]_m = [\alpha\beta]_m = [\alpha]_m [\beta]_m$. Έχουμε, λοιπόν, εν $\mathbb{Z}_m$ διαιρέτες του μηδενός, εκτός και αν ο m πρώτος p. Ο νόμος της διαγραφής δεν ισχύει συνεπώς εν $\mathbb{Z}_m$, όταν ο m δεν είναι πρώτος.

Παράδειγμα. Δίδουμε τον πίνακα για τις πράξεις «+» και «◦», όταν $\mathbb{Z}_m = \mathbb{Z}_5$:

+	**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

◦	**1**	**2**	**3**	**4**	**0**
1	1	2	3	4	0
2	2	4	1	3	0
3	3	1	4	2	0
4	4	3	2	1	0
0	0	0	0	0	0

Για λόγους προφανείς, το μοναδιαίο στοιχείο της πράξης «+» συμβολίζεται με το [0], ενώ το μοναδιαίο στοιχείο της πράξης «◦» με το [1]. Είναι, βέβαια, $[0] = [5]$.

Παρατήρηση. Ο πολλαπλασιασμός των στοιχείων $\{[1]_p, [2]_p, \ldots, [p-1]_p\}$ επί την κλάση $[a]_p$ όπου $1 < a < p-1$ μας παρέχει μία νέα αναδιάταξη των κλάσεων. Για κάθε κλάση $[a]_p$, όταν $1 < a < p-1$, υπάρχει, λοιπόν, ένα $b \neq a$ τέτοιο ώστε, $[a]_p[b]_p = [1]_p$. Το σύνολο, λοιπόν, των κλάσεων $\{[2]_p, [3]_p, \ldots, [p-2]_p\}$ είναι δυνατόν να χωρισθεί σε ζεύγει έτσι ώστε, για $b \neq a$ να είναι $[a]_p[b]_p = [1]_p$. Φυσικά, για τα ακραία στοιχεία έχουμε $[1]_p[1]_p = [1]_p$ και, $[p-1]_p[p-1]_p = [1]_p$, όπως διακρίνεται και από τον παραπάνω πίνακα.

Πρόταση. Αν $(\gamma, m) = 1$, τότε $[\gamma]_m[\alpha]_m = [\gamma]_m[\beta]_m \rightarrow [\alpha]_m = [\beta]_m$.
Πράγματι, η $[\gamma]_m[\alpha]_m = [\gamma]_m[\beta]_m \rightarrow [\gamma\alpha]_m = [\gamma\beta]_m \rightarrow [\gamma(\alpha-\beta)]_m = 0$,
δηλαδή ότι ο $\gamma(\alpha-\beta) = \lambda m$. Επειδή όμως, από υπόθεση ο m δεν διαιρεί τον γ, ο m πρέπει να διαιρεί τον $\alpha-\beta$. Άρα, $\alpha-\beta \equiv 0(\mathrm{mod}\, m)$, οπότε και, $\alpha \equiv \beta(\mathrm{mod}\, m)$.

Στο σημείο αυτό συγκεντρώνουμε τις ιδιότητες τις σχέσεως "$\equiv$".

α) $a - c \equiv b(m) \rightarrow a \equiv b + c(m)$

β) $a \equiv b(m) \wedge b \equiv c(m) \rightarrow a \equiv c(m)$ (μεταβατική ιδιότης)

γ) $a \equiv b(m) \wedge a' \equiv b'(m) \rightarrow a + a' \equiv b + b'(m)$ (πρόσθεση ισοτιμιών)

Άρα και, $a \equiv b(m) \rightarrow ka \equiv kb(m)$, $k \in \mathbb{Z}$

δ) $a \equiv b(m) \wedge a' \equiv b'(m) \rightarrow aa' = bb'(m)$ (πολλαπλασιασμός ισοτιμιών)

Άρα και, $a \equiv b(m) \rightarrow a^v \equiv b^v(m)$, $v \in \mathbb{N}$

ε) $a \equiv b(m) \wedge d \mid m \rightarrow a \equiv b(d)$ (αλλαγή του modulus)

στ) $a \equiv b(m) \wedge a \equiv b(n) \rightarrow a \equiv b(mn)$

ζ) $\lambda a \equiv \lambda b(m) \rightarrow a \equiv b\left(\dfrac{m}{(\lambda, m)}\right)$ (νόμος της διαγραφής για ισοτιμίες)

η) $a \equiv b(m) \rightarrow ak \equiv bk(mk)$ και

$a = a_1 d \wedge b = b_1 d \wedge m = m_1 d \wedge a \equiv b(m) \rightarrow a_1 \equiv b_1(m_1)$

θ) $d \mid a \wedge a \equiv b(m) \rightarrow d \mid b$

ζ) Αν $(\lambda.m) = 1$ και b_i, $1 \leq i \leq m$ ένα πλήρες σύστημα καταλοίπων modulo m, τότε και

το $\lambda b_i + \kappa$, $\kappa \in \mathbb{Z}$ αποτελεί πλήρες σύστημα καταλοίπων modulo m. Δηλαδή, αν $\mathbb{Z}_m = \{[0]_m, [1]_m, \ \ldots \ , [m-1]_m\}$, τότε και

$\mathbb{Z}_m = \{[\kappa]_m,\ [\lambda+\kappa]_m,\ \ldots,[\lambda(m-1)+\kappa]_m\}$, όπου $(\lambda, m) = 1$.

Απόδειξη. Κατ' αρχήν παρατηρούμε ότι, $i \neq j \to \lambda b_i + \kappa \neq \lambda b_j + \kappa$. Έχουμε, λοιπόν, m το πλήθος ακεραίους της μορφής $\lambda b_i + \kappa$. Αρκεί να δείξουμε ότι, ανα δύο δεν είναι ισότιμοι. Πράγματι, αν $i \neq j \to \lambda b_i + \kappa(\mathrm{mod}\, m) \equiv \lambda b_j + \kappa(\mathrm{mod}\, m) \to \lambda b_i(\mathrm{mod}\, m) \equiv \lambda b_j(\mathrm{mod}\, m)$, και επειδή $(\lambda, m) = 1$, $b_i(\mathrm{mod}\, m) \equiv b_j(\mathrm{mod}\, m)$, πράγμα αδύνατον για $b_i \neq b_j$.

Όταν, λοιπόν, το x διατρέχει ένα πλήρες σύστημα καταλοίπων mod m, και το $\lambda x + \kappa$, όπου $(\lambda, m) = 1$ και $\kappa \in \mathbb{Z}$, διατρέχει το ίδιο σύστημα καταλοίπων mod m.

ι) $a \equiv b(m) \to (a, m) = (b, m)$. Το αντίστροφο δεν ισχύει. Π.χ., ενώ είναι $(1,4) = (3,4)$,

$[0]_m,\ [1]_m,\ \ldots,[m-1]_m$ δεν είναι $1 \equiv 3(4)$.

Κόσκινο του Ερατοσθένη. Ζητάμε να βρούμε όλους τους πρώτους αριθμούς, που είναι > 1 και < n. Αρκεί να προσδιορίσουμε όλους τους πρώτους που είναι > 1 και $< \sqrt{n}$, μιά και αν $x^2 = n$, ο x δεν είναι πρώτος. Προς τούτο, γράφουμε την ακολουθία 2, 3, . . . , n, και στην συνέχεια διαγράφουμε όλα τα πολλαπλάσια των πρώτων που το τετράγωνό τους είναι < n. Για παράδειγμα, αν θέλουμε να βρούμε όλους τους πρώτους τους μεταξύ 1 και 100, γράφουμε την ακολουθία 2, 3, . . . , 100, και στην συνέχεια διαγράφουμε όλα τα πολλαπλάσια των 2, 3, 5, 7 μιά και το τετράγωνο του επόμενου πρώτου 11, είναι > 100.

Ορισμός. Η συνάρτηση $\varphi(m)$ του ***Euler*** ορίζεται ως εξής: Δοθέντος του θετικού ακεραίου m, ευρίσκουμε όλους τους $1 \le a < m$, για τους οποίους ισχύει ότι, $(a, m) = 1$. Το πλήθος αυτών, ορίζει την τιμή της συναρτήσεως $\varphi(m)$. Με Φ_m θα συμβολίζουμε το σύνολο των θετικών ακεραίων a, $1 \le a < m$, των πρώτων προς τον m.

Για να βρούμε την τιμή $\varphi(m)$, χρησιμοποιούμε το κόσκινο του ***Ερατοσθένη.*** Έστω π.χ. ότι $m = 28$. Γράφουμε όλους τους ακεραίους a τους $0 \le a < 28$, σημειώνουμε τους πρώτους διαιρέτες του 28, και στην συνέχεια, διαγράφουμε όλα τα πολλαπλάσιά τους. Ότι απομένει, είναι οι ακέραιοι a, που είναι πρώτοι προς τον 24. Το πλήθος τους, δίδει την τιμή $\varphi(28)$: Είναι, $28 = 2^2 \times 7$

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	

Είναι, $\varphi(28) = 12$, και $\Phi_{28} = \{1,\ 3,\ 5,\ 9,\ 11,\ 13,\ 15,\ 17,\ 19,\ 23,\ 25,\ 27\}$.
Φανερά, αν $m = p$ αριθμός πρώτος, τότε $\varphi(p) = p - 1$.

Ορισμός. Το υποσύνολο του $\mathbb{Z}_m^a$, που αποτελείται από εκείνες τις κλάσεις του $\mathbb{Z}_m$ με αντιπρόσωπο εν Φ_m, καλείται ***περιορισμένο*** ή ***ανηγμένο*** σύστημα καταλοίπων mod m.

Πορίσματα. α) Κάθε ακέραιος πρώτος προς τον m, ανήκει σε μία και μόνον κλάση του $\mathbb{Z}_m^a$.

β) Οι αντιπρόσωποι του $\mathbb{Z}_m^a$ είναι ανά δύο μεταξύ τους πρώτοι.

γ) Αν $\mathbb{Z}_m^a = \{[b_i]_m \mid b_i \in \Phi_m\}$ και $(\lambda_i, m) = 1$, τότε και, $\mathbb{Z}_m^a = \{[\lambda_i b_i]_m \mid b_i \in \Phi_m\}$.

Θεώρημα του Euler Αν $(a, m) = 1$, τότε και $a^{\varphi(m)} = 1(m)$. Βλέπε και [ZK], σελ. 131, 132.

Απόδειξη. Θεωρούμε το $\mathbb{Z}_m^a = \{[\lambda_i b_i]_m \mid b_i \in \Phi_m\}$, από το οποίο για $\lambda_i = a$ λαβαίνουμε τις $\varphi(m)$ σχέσεις ισοδυναμίας $ab_i \equiv b_i(m)$. Πολλαπλασιάζουμε τις ισοδυναμίες αυτές κατά μέλη, και εκτελούμε τις επιτρεπόμενες διαγραφές. Προκύπτει τότε η προς απόδειξη σχέση.

Θεώρημα του Fermat (1636). Για κάθε πρώτο p και κάθε ακέραιο a, ισχύει ότι, $a^p \equiv a(\mathrm{mod}\, p)$.

Απόδειξη α). Είναι πόρισμα του θεωρήματος του Euler μιά και έχουμε ότι $(a,p)=1$ και $\varphi(p) = p-1$. Άρα και $a^{p-1} \equiv 1(p)$, δηλαδή, $a^p \equiv a(p)$

β). Πρέπει να δείξουμε ότι, $a^p - a = \lambda p$. Με επαγωγή επί του a. Για κάποιον συγκεκριμένο p, έστω φ(a) η πρόταση $a^p = a(p)$. Οι προτάσεις φ(0) και φ(1) ισχύουν φανερά. Θεωρούμε τον $(a+1)^p$. Λόγω του διωνύμου του Newton,

$(a+1)^p = a^p + \text{πολλαπλάσια του } p + 1$. Άρα $(a+1)^p = (a^p+1)(p)$.

Η $a^p = a(\mathrm{mod}\, p) \rightarrow (a+1)^p = (a^p+1)(\mathrm{mod}\, p)$. Άρα η φ(a) ισχύει $\forall\, a \in \mathbb{N}$.

12. Ο δακτύλιος $\mathbb{Z}_m$. Ορισμός. Εν $\mathbb{Z}_m$, τα στοιχεία εκείνα, (που είναι βέβαια κλάσεις ισοδυναμίας), που είναι αντιστρέψιμα, καλούνται ***ενάδες*** (unit elements). Βλέπε και [ZK], σελ. 93.

Για να βρούμε τις ενάδες του $\mathbb{Z}_m$ σκεπτόμεθα ως εξής: Η συνθήκη, για να είναι η κλάση $[a]_m$ ενάδα, είναι να υπάρχει κλάση $[b]_m$, τέτοια ώστε $[a]_m[b]_m = [ab]_m = [1]_m$. Η τελευταία ισότητα, είναι ισοδύναμος της $\alpha\beta = 1 + \lambda m$, όπου $\alpha \in [a]_m$ και $\beta \in [b]_m$. Έχουμε, λοιπόν, την ισότητα, $\beta\alpha - \lambda m = 1$, την οποία, αν την διαβάσουμε σαν ταυτότητα του Bezout, μας λεει ότι $(\alpha, m) = 1$. Με ποιόν τρόπο βρίσκουμε τους συντελεστές β και λ, το είδαμε στην §15.

Πόρισμα. Όλα τα στοιχεία του $\mathbb{Z}_p$ είναι ενάδες (δηλαδή, αντιστρέψιμα). Όλες οι ενάδες του $\mathbb{Z}_m$, είναι $\varphi(m)$ το πλήθος. Το γινόμενο δύο ενάδων, είναι και αυτό ενάδα. Εν $\mathbb{Z}_m$, αν $[a_1]_m$ και $[a_2]_m$ δύο ενάδες, τότε, $\alpha_1 = 1 + \lambda_1 m$, $\alpha_1 \in [a_1]_m$ και $\alpha_2 = 1 + \lambda_2 m$, $\alpha_2 \in [a_2]_m$. Άρα και, $\alpha_1\alpha_2 = 1 + \lambda m$, δηλαδή, η $[a_1a_2]_m = [a_1]_m[a_2]_m$ είναι ενάδα.

Σημείωση. Αν εν $\mathbb{Z}_p$, πολλαπλασιάσουμε τις

Πόρισμα. Το $\mathbb{Z}_m^a$ αποτελεί υποομάδα ως προς τον πολλαπλασιασμό, της $\mathbb{Z}_m$.

Παράδειγμα. Εν $\mathbb{Z}_{13}$, θέλουμε να βρούμε το αντίστροφο στοιχείο του $[9]_{13}$. Εφαρμόζουμε τον αλγόριθμο του Ευκλείδη: $13 = 9 + 4$, $9 = 2\times 4 + 1$. Άρα και, $1 = 9 - 8$, $4 = 13 - 9$, άρα και $1 = 9 - 2\times 13 + 2\times 9 = 3\times 9 - 2\times 13$. Το ζητούμενο στοιχείο, είναι λοιπόν, το $[3]_{13}$. Πράγματι, $[9]_{13}[3]_{13} = [27]_{13} = [1]_{13}$.

Πρόβλημα 1. Να λυθεί η ισοτιμία $ax \equiv b(\mathrm{mod}\, m)$ (1). Ζητάμε να βρούμε μιά κλάση ισοδυναμίας $[b]_m$, από τις m κλάσεις ενός πλήρους συστήματος καταλοίπων $[b_i]_m$ mod m, η οποία να περιέχει το πολλαπλάσιο ax του a. Στην περίπτωση, που $(a,m) = d = 1$, όπως είδαμε στη προηγούμενη παράγραφο όταν το x διατρέχει ένα πλήρες σύστημα καταλοίπων mod m, και

το ax θα διατρέχει το ίδιο σύστημα. Η ισοτιμία $ax \equiv b(\mathrm{mod}\, m)$, έχει λοιπόν μοναδική λύση, λαμβανομένη από το $[b_i]_m$.

Παράδειγμα 1. Να λυθεί η ισοτιμία $35x \equiv 8(\mathrm{mod}\, 41)$. **Λύση.** Παρατηρούμε ότι $d = (35,41) = 1$. Άρα έχουμε μοναδική λύση. Από την σχέση του Bezout έχουμε $1 = 41 \times 6 - 35 \times 7$, άρα και $8 = 41 \times 48 - 35 \times 56$. Η δοσμένη ισοδυναμία γράφεται

$$35x \equiv 41 \times 48 - 35 \times 56(\mathrm{mod}\, 4) \equiv 48 \times 41 - 35 \times 56(\mathrm{mod}\, 41) = -35 \times 15(\mathrm{mod}\, 41)$$

και επειδή $(35,4) = 1$, έχουμε και την $x \equiv -15(\mathrm{mod}\, 41) \equiv 26(\mathrm{mod}\, 41)$.

Ερχόμαστε, τώρα, στην περίπτωση, που $(a,m) = d > 1$. Για να είναι δυνατή η ισοτιμία (1) πρέπει ο $d \mid b$ μιά και άλλως, η (1) είναι αδύνατος για κάθε πολλαπλάσιο του a. Θέτουμε, λοιπόν, $b = db_1$, $a = da_1$ και $m = dm_1$, οπότε η (1) είναι ισοδύναμος της $a_1 x = b_1(\mathrm{mod}\, m_1)$ με $(a_1, m_1) = 1$, οπότε γι αυτήν έχουμε μοναδική λύση $x_1(\mathrm{mod}\, m)$. Τότε, κάθε $x \equiv x_1(m_1)$, είναι λύση της (1). Όμως, modulo m, οι ακέραιοι x δεν αποτελούν μοναδική λύση της (1). Για να βρούμε όλες τις λύσεις της (1), παρατηρούμε ότι, σε κάποια κλάση του συστήματος $[0]_m$, $[1]_m$, … ,$[m-1]_m$ των κλάσεων modulo m, περιέχονται και οι ακέραιοι της μορφής x_1, $x_1 + m_1$, … , $x_1 + (d-1)m_1$, οι οποίοι λαμβανόμενοι modulo m_1, δίδουν την λύση της (1).

Παράδειγμα 2. Να λυθεί η ισοτιμία $6x \equiv 3(\mathrm{mod}\, 21)$. **Λύση.** Παρατηρούμε ότι $d = (6,21) = 3$. Άρα έχουμε τρεις λύσεις. της μορφής $x_1 + \lambda \times 21$, όπου x_1 η λύση της $2x_1 \equiv 1(\mathrm{mod}\, 7)$, και το λ είναι το 0, ή το 1, ή το 2. Έχουμε ότι, $x_1 \equiv 4(\mathrm{mod}\, 7)$. Οι τρεις λύσεις μου είναι συνεπώς, οι

$$x \equiv 4,\ 11,\ 18(\mathrm{mod}\, 7)$$

Πρόβλημα 2. Να λυθεί το σύστημα $x = b_1(m_1)$, $x = b_2(m_2)$, . . . , $x = b_n(m_n)$, όπου $(m_i, m_j) = 1$, $1 \le i,\ j \le n$. Για κάθε $1 \le i \le n$, λύνουμε το σύστημα που προκύπτει από το προηγούμενο αν θέσουμε $b_i = 1$ και $b_j = 0,\ \forall j \ne i$. Προς τούτο θεωρούμε τον $k_i = \prod_{j \ne i} m_j$, οπότε είναι $(m_i, k_i) = 1$, και έχουμε την ταυτότητα του Bezout $\alpha m_i + \beta k_i = 1$. Άρα, $\beta k_i = 0(\mathrm{mod}\, k_i)$ και $\beta k_i = 1(\mathrm{mod}\, m_i)$. Εξ άλλου, $\forall j \ne i$, $m_j \mid k_i$ και συνεπώς, ο $x_i = \beta k_i$ είναι λύση του συστήματος $x_i = \delta_{i,j}(m_j)$, με $1 \le i,\ j \le n$ και για $j = i$, $\delta_{i,j} = 1$, ενώ για $j \ne i$, $\delta_{i,j} = 0$. Θεωρούμε, τώρα, τον ακέραιο $x = \sum_{i=1}^{n} b_i x_i$. Ο x φανερά, είναι λύση του αρχικού μας συστήματος.. Λύση όμως, αποτελεί και κάθε άλλος x της μορφής $x + \kappa \prod_{i=1}^{n} m_i$, $\kappa \in \mathbb{Z}$.

Παράδειγμα. Να λυθεί το σύστημα $x = 3(\mathrm{mod}\, 11),\ x = 6(\mathrm{mod}\, 8),\ x = -1(\mathrm{mod}\, 15)$. Είναι, $k_1 = 8 \times 15 = 120$, $k_2 = 11 \times 15 = 165$ και $k_3 = 11 \times 8 = 88$. Η ταυτότητα του Bezout γράφεται κατά περίπτωση, $-1(120) + 11(11) = 1,\ -3(165) + 62(8) = 1$ και, $7(88) - 41(15) = 1$. Άρα έχουμε, $x_1 = 120 \times (-1) = -120$, $x_2 = 165 \times -3) = -495$ και, $x_3 = 88 \times 7 = 616$. Μία λύση, λοιπόν, του συστήματος είναι η $x = 3(-120) + 6(-495) + (-1)(616) = -3946$. Όλες οι λύσεις του δίδονται από την έκφραση $x = -3946 + \kappa(11 \times 8 \times 15) = -3946 + \kappa 1320$. Η μικρότερη θετική λύση λαβαίνετε για $\kappa = 3$, και είναι η $x = 14$.

Ορισμός. Έστω α τυχόν στοιχείο δακτυλίου Δ. Ορίζουμε την πράξη $\mathbb{N}\times\ni(n,\alpha)\mapsto n\alpha\in\Delta$ επαγωγικά ως εξής: $1\alpha=\alpha$ και $n\alpha=\alpha+(n-1)\alpha$. Τέλος, ορίζουμε και το $(-n\alpha)=-n\alpha$ το αντίθετο στοιχείο του nα. Έχουμε, τότε εν Δ τον συνηθισμένο λογισμό εν Δ. Υπάρχει περίπτωση να έχουμε $\forall\alpha\in\Delta,\ n\alpha=0$ για κάποιο $n>1$. Έστω m ο ελάχιστος τέτοιος φυσικός αριθμός. Τότε, $n=mq+r$ με $1\le q$, $0\le r<m$. Είναι, $r\alpha=(n-m)\alpha=n\alpha-q(m\alpha)=0$ και, συνεπώς, $m\,|\,n$. Ο m καλείται ***χαρακτηριστική*** του δακτυλίου Δ. **Παράδειγμα.** Η χαρακτηριστική του $\mathbb{Z}_p$, p πρώτος, είναι p.

Θεώρημα του Wilson (1770). Ο p είναι πρώτος, αν και μόνον αν $(p-1)!\equiv-1(p)$. (Ο $(p-1)!+1$ είναι πολλαπλάσιο του p).
Απόδειξη. Έστω ο p πρώτος. Όπως παρατηρήσαμε παραπάνω, το σύνολο των κλάσεων $S=\{[2]_p,[3]_p,\ldots,[p-2]_p\}$ είναι δυνατόν να μερισθεί σε ζεύγη με την ιδιότητα $[a]_p[b]_p=[1]$. Άρα και $[1]_p[2]_p\cdots[p-2]_p[p-1]_p=[1]_p[p-1]_p=[p-1]_p$. Την ισότητα αυτή, μπορούμε να την γράφουμε και $(p-1)!=-1(p)$, που είναι το θεώρημα του Wilson. Παρατηρούμε ότι, αν $a\in S$, τότε και $(a,p)=1$ ως επίσης και $(p-1,p)=1$, μια και ο p από υπόθεση είναι πρώτος.
Αντίστροφα, έστω ότι ο p δεν είναι πρώτος, αλλά είναι ο σύνθετος αριθμός q. Όλοι, τότε, οι θετικοί διαιρέτες του ευρίσκονται στο σύνολο $1,2,3,\cdots,(q-1)$. Άρα ο μ.κ.δ. του $(q-1)!$ και του q είναι $\neq1$. Ο q συνεπώς, είναι αδύνατον να διαιρεί τον $(q-1)!+1$.

13. Σημείωση. Μερικοί συγγραφείς καλούν ότι εμείς θα ορίσουμε "σώμα", "αντιμεταθετικό σώμα" και καλούν "σώμα", ότι εμείς θα ορίσουμε αμέσως τώρα, "δακτύλιο διαιρετότητας" (Division Ring). **Ορισμός.** Ένας δακτύλιος Δ καλείται ***δακτύλιος διαιρετότητας,*** ανν έχει περισσότερα από ένα στοιχεία, και γιά κάθε μη μηδενικό στοιχείο του a, η εξίσωση $ax=b$ έχει λύση εν Δ.

Λήμμα. Ένας δακτύλιος διαιρετότητας Δ, δεν έχει διαιρέτες του μηδενός. Πράγματι, εξ ορισμού, έχουμε λύσεις για τις εξισώσεις $ax=b$ και $by=x$ (με $a,b\neq0$).
Άρα και, $a(by)=(ab)y=b\neq0$. Άρα, και, $ab\neq0$.

Πόρισμα. Μέσα στον Δ ισχύει ο νόμος της διαγραφής.

Λήμμα. Ο Δ έχει μοναδιαίο στοιχείο e.
Απόδειξη. Εν Δ θεωρούμε την εξίσωση $ae=a$, από την οποία προκύπτει και η $ae^2=ae$, και επειδή ισχύει ο νόμος της διαγραφής, η $e^2=e$. Αν, τώρα, t τυχόν στοιχείο του Δ, έχουμε ότι, $(t-te)e=0$ και $e(t-et)=0$. Άρα και, $te=et=t$.

Αφού ο Δ έχει μοναδιαίο στοιχείο, αυτό είναι και μοναδικό, και, όπως είδαμε κάθε μη μηδενικό στοιχείο του Δ έχει αντίστροφο στοιχείο. Άρα, έχουμε την,

Πρόταση. Μέσα σε έναν δακτύλιο διαιρετότητας, και η εξίσωση $ya=b,\ a\neq0$, έχει μοναδική λύση, την $y=ba^{-1}$.

Πόρισμα. Η χαρακτηριστική ενός δακτυλίου διαιρετότητας, με πεπερασμένο το πλήθος στοιχεία. Είναι αριθμός πρώτος p.
Απόδειξη. Έστω γ η χαρακτηριστική του δακτυλίου Δ.

Αν $\gamma = \alpha\beta$, τότε και, $\gamma e = (\alpha e)(\beta e) = 0$, με $0 < \alpha, \beta < \gamma$. Ο Δ έχει, λοιπόν, διαιρέτες του μηδενός. Άτοπον.

Ορισμός σώματος. Ένα ***σώμα*** F, είναι μία ακέραια περιοχή D, στην οποία η εξίσωση $\alpha x = \beta,\ \alpha \neq 0$, έχει πάντα λύση μέσα σ' αυτήν. Η διαίρεσης συνεπώς με κάθε μη μηδενικό στοιχείο είναι δυνατή, και το πηλίκο της διαιρέσεως είναι μοναδικό εν F. Ένα υποσύνολο S του σώματος F είναι ***υπόσωμα*** του F, ανν είναι και αυτό σώμα, ως προς τις πράξεις πρόσθεση και πολλαπλασιασμό, που καθιστούν το F σώμα. Το S είναι, λοιπόν κλειστό ως προς τις πράξεις του F, περιέχει τα δύο ουδέτερα στοιχεία 0 και 1 του F, και $\forall \alpha \in S,\ \alpha^{-1} \in S$.

Παραδείγματα. α) Το $\mathbb{Z}_m$ είναι σώμα, ανν ο m πρώτος αριθμός p. Μιά και σε αντίθετη περίπτωση, το $\mathbb{Z}_m$ περιέχει διαιρέτες του μηδενός, και συνεπώς δεν είναι ακέραια περιοχή.

β) Το σύνολο των πραγματικών αριθμών της μορφής $\alpha + \beta\sqrt{2},\ \alpha, \beta \in \mathbb{R}$ αποτελεί υπόσωμα του σώματος των πραγματικών αριθμών.

Πρόταση. Αν ένα σώμα F έχει n το πλήθος στοιχεία, τότε το $n = p^m$, όπου p πρώτος αριθμός, η χαρακτηριστική του σώματος, και $m \in \mathbb{N}$.

Απόδειξη. Έστω ότι το F έχει n το πλήθος στοιχεία, και, έστω, e η μονάδα του F. Παρατηρούμε ότι τα $n+1$ το πλήθος στοιχεία $e, 2e, 3e, \ldots, (n+1)e$ δεν είναι δυνατόν να είναι όλα διαφορετικά. Υπάρχουν συνεπώς οι ακέραιοι και θετικοί l_1, l_2, τέτοιοι ώστε, $l_1 e = l_2 e$, ή $(l_1 - l_2)e = 0$. Ο αριθμός, λοιπόν, $l_1 - l_2$, ισούται με την χαρακτηριστική του σώματος. Άρα, το F περιέχει ke $k = 0,1,2,\ldots,(p-1)$ διαφορετικά στοιχεία, και κάθε ακέραιο πολλαπλάσιο των στοιχείων αυτών. Η πρόταση συνεπώς, εδείχθη γιά $m = 1$.

Έστω, τώρα, ότι το F περιέχει και κάποιο στοιχείο a, το οποίο δεν είναι ακέραιο πολλαπλάσιο των ke στοιχείων. Θα δείξουμε, τότε, ότι τα p^2 στοιχεία της μορφής $k_1 e + k_2 a$, όπου οι $0 \leq k_1, k_2 \leq p-1$ είναι όλα διαφορετικά στοιχεία του F. Πράγματι, αν είχαμε την σχέση $k_1 e + k_2 a = k_1^* e + k_2^* a$, με $k_2 > k_2^*$, θα είχαμε και, $(k_2 - k_2^*)a = (k_1^* - k_1)e$. Όμως, έχουμε ότι, $0 < k_2 - k_2^* < p$, και συνεπώς (αλγόριθμος της διαιρέσεως) υπάρχουν ακέραιοι r και s, τέτοιοι ώστε, $r(k_2 - k_2^*) = 1 + sp$ Έχουμε και την $r(k_2 - k_2^*)a = r(k_1^* - k_1)e$. Άρα, και την $(1+sp)a = r(k_1^* - k_1)e$, και επειδή $sp = 0$, την $a = r(k_1^* - k_1)e$. Το στοιχείο a είναι πολλαπλάσιο του e. Άτοπο. Άρα αναγκαστικά, $k_2 = k_2^*$, δηλαδή, $(k_1^* - k_1)e = 0$, και επειδή οι $k_1, k_1^* < p$, $k_1 = k_1^*$, δηλαδή όλα p^2 στοιχεία που θεωρήσαμε είναι όλα διαφορετικά μεταξύ τους. Αν δεν έχουμε εξαντλήσει τα στοιχεία του F, συνεχίζουμε με την ίδια διαδικασία, μέχρις ότου τα εξαντλήσουμε.

Ισχύει ακόμα και το εξής. Αν p τυχόν αριθμός και $m \in \mathbb{N}$, υπάρχει τότε σώμα με p^m το πλήθος στοιχεία. Αναφέρουμε ακόμα σχετικά, το ***θεώρημα του Wedderburn*** το οποίο αποδεικνύει ότι, κάθε πεπερασμένος δακτύλιος διαιρετότητας είναι σώμα.

Ορισμός. Ένα σώμα F λέγεται ***πρώτο*** αν και μόνον αν δεν περιέχει υπόσωμα $K \subset F$.

14. Κατασκευή των ρητών αριθμών. Κάθε φορά που δίδεται μία ακεραία περιοχή D, μπορούμε να κατασκευάσουμε πάνω σ' αυτήν ένα αντιμεταθετικό σώμα $\mathbb{Q}(D)$, το οποίο να περιέχει την D και το οποίο καλείται ***σώμα των ρητών,*** ως εξής: Θεωρούμε το σύνολο $\mathbb{Q} = D \times D$ και

εισάγουμε σ' αυτό την σχέση R θέτοντας $((\alpha_1,\beta_1),(\alpha_2,\beta_2)) \in R \subseteq \mathbb{Q}^2$, ανν $\alpha_1\beta_2 = \alpha_2\beta_1$. Το σύνολο πηλίκο $\mathbb{Q}/R$ αποτελείται από τις κλάσεις ισοδυναμίας $C_{(p,q)} = \left[\frac{p}{q}\right]$, όπου $(\alpha,\beta) \in C_{(p,q)}$ ανν $q\alpha = p\beta$. Ένας αντιπρόσωπος συνεπώς της κλάσεως $C_{(p,q)}$ είναι ο (p,q), όπου $(p,q) = 1$. Την $C_{(p,q)}$ την συμβολίζουμε απλά $\frac{p}{q}$ ή, τέλος p/q. Λέμε την κλάση p/q ρητό αριθμό με αριθμητή p και παρονομαστή q. Κάθε άλλο στοιχείο της τάξης αυτής, έχει την μορφή λp/λq, $\lambda \in \mathbb{Z}$.

Το Q καθίσταται αντιμεταθετικό σώμα, αν ορίσουμε μέσα σ' αυτό μιά πρόσθεση "+" και έναν πολλαπλασιασμό "·" ως εξής:

$(\alpha_1,\beta_1) + (\alpha_2,\beta_2) = (\alpha_1\beta_2 + \alpha_2\beta_1, \beta_1\beta_2)$ και $(\alpha_1,\beta_1)\cdot(\alpha_2,\beta_2) = (\alpha_1\alpha_2, \beta_1\beta_2)$.

Η κλάση 0/1 είναι το στοιχείο "0" του σώματος, η 1/1 το "1" αυτού, και μπορούμε να ταυτίσουμε τα στοιχεία του $\mathbb{Z}$ με τις κλάσεις της μορφής α/1, $\alpha \in \mathbb{Z}$.

Μέσα σε ένα σώμα, ισχύει η σχέση $\alpha^{-1} - (1+\alpha)^{-1} = \alpha^{-1}(1+\alpha)^{-1}$.

Πράγματι, είναι $1 = (\alpha+1)(1+\alpha)^{-1}$ ή $1 = \alpha(1+\alpha)^{-1} + (1+\alpha)^{-1}$ ή $1 - \alpha(1+\alpha)^{-1} = (1+\alpha)^{-1}$ ή $\alpha\alpha^{-1} - \alpha(1+\alpha)^{-1} = (1+\alpha)^{-1}$ ή $\alpha\{\alpha^{-1} - (1+\alpha)^{-1}\} = (1+\alpha)^{-1}$ ή τέλος, $\alpha^{-1} - (1+\alpha)^{-1} = \alpha^{-1}(1+\alpha)^{-1}$

Θεώρημα. Δ αντιμεταθετικός δακτύλιος με μονάδα. Το Δ είναι σώμα, ανν τα μοναδικά ιδεώδη που περιέχει, είναι τα τετριμμένα ιδεώδη.

Απόδειξη. α) Έστω Δ σώμα και I ιδεώδες του. Αν $I \neq (0)$, έστω το $\alpha \neq 0$, $\alpha \in I$. Επειδή το Δ σώμα, $\exists\ \alpha^{-1} \in \Delta$ με $\alpha\,\alpha^{-1} = 1 \in I$. Άρα και κάθε $x \in \Delta$ είναι και $x \in I$, μιά και $x = 1x$. β) Έστω ότι το Δ δεν έχει άλλα ιδεώδη, εκτός από τα τετριμμένα. Θεωρούμε το $\alpha \in \Delta$, $\alpha \neq 0$, και το (α). Από υπόθεση,

(α) = Δ (μιά και αποκλείεται να είναι (α) = (0). Όμως, το Δ περιέχει την μονάδα. Άρα $1 = \alpha\alpha'$.

Θεώρημα. Κάθε αντιμεταθετικό σώμα F περιέχει ένα και μόνον πρώτο υπόσωμα P, το οποίο είναι ισόμορφο είτε του $\mathbb{Q}$ είτε του $\mathbb{Z}_p$, για κάποιο πρώτο αριθμό p.

Απόδειξη. Φανερά, η τομή του P με κάθε άλλο υπόσωμα του F είναι το P. Το P είναι επίσης το μοναδικό υπόσωμα του F με αυτήν την ιδιότητα. Έχουμε εξ' άλλου και ότι $1 \in P$. Άρα και $n \cdot 1 \in P$. Συνεπώς, για δύο τυχόντες ακεραίους $s,t \in \mathbb{Z}$, έχουμε και $s\cdot 1 + t\cdot 1 = (s+t)\cdot 1 \in P$. Η απεικόνιση συνεπώς, $f : \mathbb{Z} \to P$, που ορίζεται από την σχέση $\forall n \in \mathbb{Z},\ f(n) = n\cdot 1 \in P$ είναι ομομορφισμός. Ο πυρήνας Kerf του ομομορφισμού αυτού, που είναι ένα ιδεώδες του $\mathbb{Z}$, είναι της μορφής $m\mathbb{Z}$ (βλέπε §15). Στην περίπτωση, που $m = 0$, η f είναι ισομορφισμός, και τα στοιχεία $s\cdot 1/t\cdot 1$, που έχουν νόημα εν F, σχηματίζουν ένα υπόσωμα P ισόμορφο του $\mathbb{Q}$. Αν $m > 0$, η απεικόνιση $\mathbb{Z}_m \ni C_k \mapsto k \in P$ είναι ισομορφισμός, αν και μόνον αν m πρώτος.

Ορισμός. Λέμε ότι ένα αντιμεταθετικό σώμα F έχει χαρακτηριστική μηδέν, αν το υπόσωμά του P είναι ισόμορφο του $\mathbb{Q}$. Στην περίπτωση, που το P είναι ισόμορφο του $\mathbb{Z}_p$, λέμε ότι, έχει χαρακτηριστική p. Τα σώματα αυτά, καλούνται και ***σώματα του Galois.*** Βλέπε και [ZK], σελ. 75.

Για την πλήρωση του σώματος $\mathbb{Q}$ και την κατασκευή του $\mathbb{R}$ (= σώμα των πραγματικών αριθμών), βλέπε [ZK], σελ.162, και την ενότητά μας Πραγματικοί αριθμοί.

14. Κλασικές ανισότητες εν $\mathbb{R}$**.** 1. Ξεκινάμε από την προφανή ανισότητα $(x_1 - x_2)^2 \geq 0$, από την οποία λαβαίνουμε την $x_1^2 + x_2^2 \geq 2x_1x_2$. Γενικεύουμε την ανισότητα αυτή, ως εξής: Έστω $0 \leq x_i$, $1 \leq i \leq n$, n θετικοί πραγματικοί αριθμοί. Ισχύει τότε η $\prod_{i=1}^{n} x_i = 1 \rightarrow \sum_{i=1}^{n} x_i \geq n$ (1).

Απόδειξη. Με επαγωγή. Για $n = 2$ και $x_1 = \sqrt{x}$, $x_2 = \frac{1}{\sqrt{x}}$, η (1) ισχύει. Υποθέτουμε την (1) για $n = k$. Θεωρούμε, τώρα, $k+1$ θετικούς x_i, των οποίων το γινόμενο είναι ίσο με 1. Στηνη περίπτωση, που $\forall i,\ 1 \leq i \leq k+1,\ x_i = 1$, $\sum_{i=1}^{k+1} x_i = k+1$ και συνεπώς η ανισότητα πληρούται. Αν, τώρα, δεν είναι όλοι η $k+1$ $x_i = 1$, τότε, αν, έστω ο $x_{k+1} > 1$, ο, έστω, $x_k < 1$. Γράφουμε, τότε το γινόμενο των $k+1$ x_i ως $x_1x_2 \cdots x_{k-1}(x_kx_{k+1}) = 1$, και το θεωρούμε ως γινόμενο k το πλήθος x_i, για το οποίο εφαρμόζουμε την υπόθεση της επαγωγής, και λαβαίνουμε την ανισότητα,

$$x_1 + x_2 + \cdots + x_{k-1} + (x_kx_{k+1}) \geq k.$$

Άρα, και $x_1 + x_2 + \ldots + x_{k-1} + x_k + x_{k+1} \geq k + x_k + x_{k+1} - x_kx_{k+1} = k + 1 + (x_k - 1)(1 - x_{k+1}) > k+1$ μιά και $(x_k - 1)(1 - x_{k+1}) < 0$.

2. Ο αριθμητικός μέσος $n \geq 2$ θετικών αριθμών, είναι $\geq$ του γεωμετρικού μέσου. Είναι, δηλαδή,

$$\frac{x_1 + x_2 + \ldots + x_n}{n} \geq \sqrt[n]{x_1x_2 \cdots x_n} \quad (2).$$

Απόδειξη. Προκύπτει από την (1) ως εξής: Θέτουμε $c = \sqrt[n]{x_1x_2 \cdots x_n}$ και $y_i = \frac{x_i}{c}$. Τότε είναι, $\prod_{i=1}^{n} y_i = 1 \rightarrow \sum_{i=1}^{n} y_i \geq n$, που είναι η προς απόδειξη ανισότητα (2). **Εφαρμογή 1.** Αν στην (2) θέσουμε $x_i = i$, λαβαίνουμε την $\frac{1 + 2 + \ldots + n}{n} \geq \sqrt[n]{n!}$, συνεπώς και την $\left(\frac{n+1}{2}\right)^n \geq n!$.

Εφαρμογή 2. Στην (2) θέτουμε, $x_1 = x_2 = \ldots = x_k = a$ και $x_{k+1} = x_{k+2} = \ldots = x_n = b$ οπότε λαβαίνουμε την $ka + (n-k)b \geq n\sqrt[n]{a^k b^{n-k}}$, $1 \leq k \leq n$, ή για $r = \frac{k}{n}$, $ra + (1-r)b \geq a^r b^{1-r}$. Η ανισότητα αυτή, ισχύει $\forall a, b > 0$ και $0 < r < 1$. Αν λάβουμε $r = \frac{1}{p}$, $p > 0$, και $q = \frac{p}{p-1}$ έτσι ώστε $\frac{1}{p} + \frac{1}{q} = 1$, τότε η προηγούμενη ανισότητα γράφεται $\frac{a}{p} + \frac{b}{q} \geq a^{1/p}b^{1/q}$, ή ακόμα και, $\frac{a^p}{p} + \frac{b^q}{q} \geq ab$.

3. Η ταυτότητα του Lagrange $\left(\sum_{i=1}^{n} x_i^2\right)\left(\sum_{i=1}^{n} y_i^2\right)-\left(\sum_{i=1}^{n} x_i y_i\right)^2=\sum_{i<j}(x_i y_j - x_j y_i)^2$ αποδεικνύεται ως εξής: Παρατηρούμε ότι, το γινόμενο $\left(\sum_{i=1}^{n} x_i^2\right)\left(\sum_{i=1}^{n} y_i^2\right)$ αποτελείται από $n\times n$ όρους της μορφής $x_i^2 y_j^2$, $1\le i,j\le n$. Οι όροι με δείκτες $i=j$, μηδενίζονται από τους αντίστοιχους όρους, που λαβαίνουμε από το ανάπτυγμα του $\left(\sum_{i=1}^{n} x_i y_i\right)^2$. Συνεπώς, ότι απομένει από το αριστερό σκέλος της παραπάνω ισότητας, είναι όροι της μορφής $x_i^2 y_j^2 - 2x_i y_j x_j y_i$ με $i<j$. Το άθροισμα όμως αυτό, δεν είναι παρά το ανάπτυγμα του δεξιού σκέλους της ταυτότητας του Lagrange.

Εφαρμογή 1. Πραφανώς, $\left(\sum_{i=1}^{n} x_i^2\right)\left(\sum_{i=1}^{n} y_i^2\right)-\left(\sum_{i=1}^{n} x_i y_i\right)^2=\sum_{i<j}(x_i y_j - x_j y_i)^2\ge 0$. Άρα ίσχύει η ανισότητα των ***Cauchy – Schwartz:*** $\left(\sum_{i=1}^{n} x_i y_i\right)^2\le\left(\sum_{i=1}^{n} x_i^2\right)\left(\sum_{i=1}^{n} y_i^2\right)$.

Εφαρμογή 2. Η ***τριγωνική ανισότητα*** $\sqrt{\sum_{i=1}^{n}(x_i-y_i)^2}\le\sqrt{\sum_{i=1}^{n}(x_i-z_i)^2}+\sqrt{\sum_{i=1}^{n}(z_i-y_i)^2}$ προκύπτει με την βοήθεια της προηγούμενης ανισότητας, ως εξής: Είναι,

$$\left\{\sqrt{\left(\sum_{i=1}^{n}(x_i-z_i)^2\right)}+\sqrt{\left(\sum_{i=1}^{n}(z_i-y_i)^2\right)}\right\}^2=$$

$$\left(\sum_{i=1}^{n}(x_i-z_i)^2\right)+\left(\sum_{i=1}^{n}(z_i-y_i)^2\right)+2\sqrt{\left(\sum_{i=1}^{n}(x_i-z_i)^2\right)}\sqrt{\left(\sum_{i=1}^{n}(z_i-y_i)^2\right)}\ge$$

$$\left(\sum_{i=1}^{n}(x_i-z_i)^2\right)+\left(\sum_{i=1}^{n}(z_i-y_i)^2\right)+2\left(\sum_{i=1}^{n}(x_i-z_i)(z_i-y_i)\right)=$$

$$\sum_{i=1}^{n}\left\{(x_i-z_i)^2+(z_i-y_i)^2+2(x_i-z_i)(z_i-y_i)\right\}=\sum_{i=1}^{n}(x_i-y_i)^2$$

4. Η ανισότητα του Cauchy γενικεύεται από την ανισότητα του Hlder.

$$\left(\sum_{i=1}^{n} x_i^p\right)^{1/p}\left(\sum_{i=1}^{n} y_i^q\right)^{1/q}\ge\sum_{i=1}^{n} x_i y_i\ ,\ \text{με}\ \frac{1}{p}+\frac{1}{q}=1,\ p>1.$$

Για $p=q=2$, η παραπάνω ανισότητα δίδει την ανισότητα του Cauchy. **Απόδειξη.** Ξεκινάμε από την $\frac{a^p}{p}+\frac{b^q}{q}\ge ab$, που δείξαμε στο 3, εφαρμογή 2. Θέτουμε $a=\frac{x_i}{\left(\sum_{i=1}^{n} x_i^p\right)^{1/p}}$ και

$b=\frac{y_i}{\left(\sum_{i=1}^{n} x_i^q\right)^{1/q}}$ και λαβαίνουμε την $\frac{x_i^p}{p\left(\sum_{i=1}^{n} x_i^p\right)}+\frac{y_i^q}{q\left(\sum_{i=1}^{n} x_i^q\right)}\geq\frac{x_i y_i}{\left(\sum_{i=1}^{n} x_i^p\right)^{1/p}\left(\sum_{i=1}^{n} x_i^q\right)^{1/q}}$. Για $1\leq i\leq n$, προσθέτουμε κατά μέλη όλες τις λαμβανόμενες ανισότητες, και έχουμε την, $\frac{1}{p}+\frac{1}{q}\geq\frac{\sum_{i=1}^{n} x_i y_i}{\left(\sum_{i=1}^{n} x_i^p\right)^{1/p}\left(\sum_{i=1}^{n} x_i^q\right)^{1/q}}$ και επειδή $\frac{1}{p}+\frac{1}{q}=1$, η προηγούμενη ανισότητα, δίδει την ανισότητα του H¬lder.

Εφαρμογή. Όπως λάβαμε την τριγωνική ανισότητα από την ανισότητα του Cauchy, λαβαίνουμε την ***ανισότητα του Minkowski*** από την ανισότητα του H¬lder:

$$\sqrt[p]{\sum_{i=1}^{n}(x_i-y_i)^p}\leq\sqrt[p]{\sum_{i=1}^{n}(x_i-z_i)^p}+\sqrt[p]{\sum_{i=1}^{n}(z_i-y_i)^p}\ .$$

5. Ανισότητα του ***Weierstrass.*** Με επαγωγή, αποδεικνύεται ότι, $\prod_{i=1}^{n}(1+x_i)\geq 1+\sum_{i=1}^{n} x_i$, με $x_i\geq 0$

6. Ανισότητα του ***Tchebychef.*** Αν $x_1\leq x_2\leq\ \ldots\ \leq x_n$ και $y_1\leq y_2\leq\ \ldots\ \leq y_n$, τότε και,

$$n\sum_{i=1}^{n} x_i y_i\geq\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} y_i\right)\qquad(3).$$

Απόδειξη. Παρατηρούμε ότι, $\forall i\neq j$, $(x_i-x_j)(y_i-y_j)\geq 0$. Ισχύει, δηλαδή, η

$$x_i y_i+x_j y_j\geq x_i y_j+x_j y_i\qquad(4).$$

Όλα τα δυνατά ζεύξη δεικτών (i, j) είναι $C(n,2)=\frac{n(n-1)}{2}$ το πλήθος. Άρα έχουμε τόσες ανισότητες (4), τις οποίες και προσθέτουμε κατά μέλη, και λαβαίνουμε την (3)

.