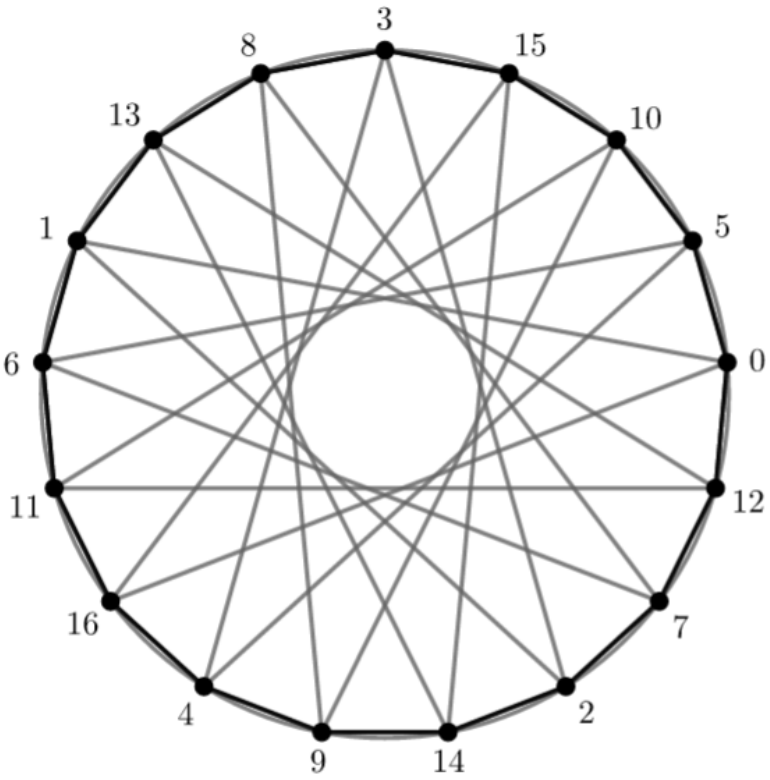
Η ΓΕΩΜΕΤΡΙΑ ΣΤΗΝ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών,
Αναστάσιος Φράγκος, 2^o προς 3^o εξάμηνο



Αύγουστος, 22/2020

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Μέχρι και τις αρχές $17^{ου}$ αιώνα, τα Μαθηματικά είχαν μια κατά βάση γεωμετρική αύρα. Τα περισσότερα μαθηματικά θεωρήματα των εποχών εκείνων είχαν γεωμετρική προέλευση και ισχυρή γεωμετρική ερμηνεία, ή σπανιώτερα για περιπλοκότερα και πιο αφηρημένα προβλήματα βρίσκοταν (ακόμη και αν η σύνδεση ήταν αχνή ή σύνθετη) μια γεωμετρική κατασκευή που τα ερμήνευε πλήρως. Κάθε πρόβλημα συνδέοταν με ένα σχήμα και κάθε σχήμα έκρυβε ένα τουλάχιστον πρόβλημα που περίμενε να λυθεί. Η αμφίδρομη σχέση αυτή ήταν πολύ δελεαστική για τους ανθρώπους της εποχής, καθώς έβλεπαν τον κόσμο τους να ξετυλίγεται μπροστά από τα μάτια τους, να τους λύνει τα προβλήματά τους και με την σειρά του ο ίδιος να αυτοερμηνεύεται.

Ο τρόπος όμως αυτός επίλυσης προβλημάτων έδινε όλο και δυσκολότερα απαντήσεις σε μαθηματικά προβλήματα, ιδίως καθώς προχορώντας στον χρόνο τα Μαθηματικά αποκτούσαν μια έννοια περισσότερο αφηρημένη και μία υπόσταση περισσότερο φιλοσοφική. Ήταν αναγκαίο, λοιπόν, η Γεωμετρία να εξεληχθεί, πράγμα που τελικά έγινε περί το 1637, όταν ο *Descartes* εισήγαγε την Αναλυτική Γεωμετρία στον χώρο των Μαθηματικών. Την αλγεβρικοποίηση της Γεωμετρίας ακολούθησαν ανακαλύψεις στον τομέα των Μαθηματικών και πρόοδος σε άλλες επιστήμες και κυριότερα στην Φυσική.

Είναι αδιαμφισβήτητο το γεγονός ότι η εισαγωγή της Άλγεβρας έφερε μια σειρά αλυσιδωτών αντιδράσεων, μια αναγέννηση στον χώρο των Μαθηματικών, και κατά συνέπεια, τεράστια πρόοδο σε όλες τις υπόλοιπες επιστήμες, όμως αυτό στο οποίο η Άλγεβρα υστερεί της Γεωμετρίας είναι η ικανότητα οπτικοποίησης των μαθηματικών εννοιών. Κύριο μέλημα της Άλγεβρας δεν είναι η γεωμετρικοποίηση, οπότε επόμενο είναι ο αλγεβρικός τρόπος σκέψης να μην προϋποθέτει (τουλάχιστον όχι πάντα) την (έστω νοητική) κατασκευή σχημάτων και, ως εκ τούτου, η σύνδεση των μαθηματικών εννοιών με τον περιβάλλοντα κόσμο γίνεται ολοένα και πιο αμυδρή. Κατα την γνώμη μου, έτσι χάνεται μια ολόκληρη σκοπιά, μια οπτική στον τρόπο που βιώνουμε τα Μαθηματικά. Διότι μέσω της Άλγεβρας είναι μεν

ευκολότερη (πολλές φορές) η επίλυση προβλημάτων, μέσω όμως της Γεωμετρίας ενδυναμώνεται η διαίσθηση και η συνδιαστική σκέψη.

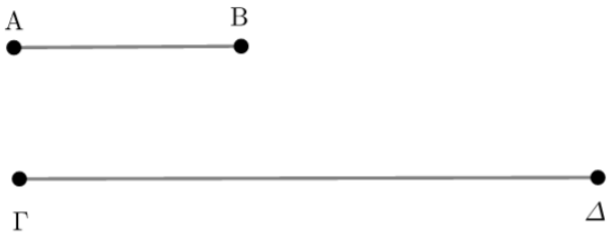
Όσον αφορά την Θεωρία των Αριθμών, κι αυτή όπως και πολλοί άλλοι μαθηματικοί κλάδοι, αρχικά βασίζοταν στην Γεωμετρία, ενώ τώρα πλέον, είναι σχεδόν εξ ολοκλήρου αλγεβρικοποιημένη. Σε αυτήν την εργασία, λοιπόν, θα επιχειρήσω να γεωμετρικοποιήσω μερικές έννοιες και μερικά θεωρήματα της στοιχειώδους Θεωρίας Αριθμών, ευελπιστώντας ότι μια ''νέα'' οπτική του πεδίου αυτού θα είναι οφέλιμη.

Κεφάλαιο 2

Γεωμετρική αναπαράσταση των θετικών πραγματικών αριθμών

2.1 Γραμμική αναπαράσταση των θετικών πραγματικών αριθμών

Ο πιο συνηθισμένος τρόπος να αναπαρίστανται αριθμοί σε γεωμετρικό επίπεδο, είναι με την χρήση ευθυγράμμων τμημάτων. Θεωρώντας ευθύγραμμο τμήμα AB να αντιπροσωπεύει την μονάδα, μπορούμε να μετρήσουμε οποιοδήποτε άλλο ευθύγραμμο τμήμα μας δοθεί, έστω $\Gamma\Delta$, θεωρώντας τον λόγο: $\frac{\Gamma\Delta}{AB}$ να αντιστοιχεί στο μήκος του ευθυγράμμου τμήματος $\Gamma\Delta$.



Σχήμα 2.1

Δεδομένου ότι ο προαναφερθείς λόγος μπορεί να είναι οποιοσδήποτε $\mathbb{R}_+^*$ αριθμός για τυχαία επιλογή του $\Gamma\Delta$, είναι εμφανές ότι με τον τρόπο αυτό, ουσιαστικά αντιστοιχούμε κάθε θετικό πραγματικό αριθμό σε ένα (τουλάχιστον) ευθύγραμμο

τμήμα. Αντίστροφα, κάθε ευθύγραμμο τμήμα με την σειρά του αντιστοιχεί σε έναν αριθμό. Ας θεωρήσουμε $\hat{\Delta}$ το σύνολο των ευθυγράμμων τμημάτων ενός ευκλείδειου επιπέδου. Δεν μας ενδιαφέρει, συνήθως, η αντιστοιχία $\mathbb{R}_+^* \to \hat{\Delta}$ να είναι συνάρτηση, ούτε (ισοδύναμα) η $\hat{\Delta} \to \mathbb{R}_+^*$ να είναι $1-1$. Στην περίπτωση όμως που χρειάζεται η αντιστοιχία $\mathbb{R}_+^* \to \hat{\Delta}$ να είναι αμφιμονοσήμαντη, θα τροποποιήσουμε κατάλληλα τον αρχικό αρισμό ώστε κάτι τέτοιο να επιτρέπεται.

Συγκεκριμένα, θεωρούμε την ημιευθεία $A\varepsilon$ που είναι παράλληλη της ε, με αρχή το σημείο A.

Σχήμα 2.2

Όπως και πριν, θεωρούμε το τμήμα AB να αντιπροσωπεύει την μονάδα. Θα αντιστοιχούμε έναν αριθμό $\gamma \in \mathbb{R}_+^*$ με το ευθύγραμμο τμήμα $A\Gamma$ της $A\varepsilon$, όπου $\dfrac{A\Gamma}{AB} = \gamma$. Αντίστροφα, για κάθε τμήμα της μορφής $A\Gamma \in A\varepsilon$, θεωρούμε τον λόγο $\dfrac{A\Gamma}{AB} = \gamma$. Το τμήμα $A\Gamma$ θα αντιστοιχίζεται στον αριθμό γ. Θεωρούμε το σύνολο $\bar{\Delta}$ να είναι το σύνολο όλων των ευθυγράμμων τμημάτων της $A\varepsilon$ με αρχή το A. Θα δείξουμε ότι η απεικόνηση $\bar{\Delta} \to \mathbb{R}_+^*$ είναι αμφιμονοσήμαντη συνάρτηση.

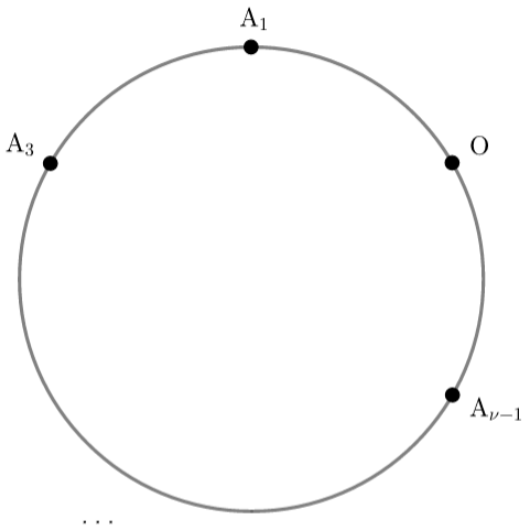
- Για αρχή, δείχνουμε ότι είναι συνάρτηση. Πράγματι, ο λόγος $\dfrac{A\Gamma}{AB}$ δεν μπορεί να παίρνει 2 διαφορετικές πραγματικές τιμές.
- Έπειτα, ότι είναι επί του $\mathbb{R}_+^*$. Εδώ, για οποιονδήποτε $\gamma \in \mathbb{R}_+^*$, παίρνοντας τμήμα $A\Gamma$ τέτοιο ώστε $A\Gamma = \gamma \cdot AB$, έπεται $\dfrac{A\Gamma}{AB} = \gamma$, το οποίο σημαίνει ότι $\forall \gamma \in \mathbb{R}, \exists A\Gamma \in \bar{\Delta} : A\Gamma \to \gamma$.
- Τέλος, ότι είναι $1-1$. Θεωρούμε τον αριθμό $\gamma \in \mathbb{R}_+^*$ καθώς επίσης και τον κύκλο (A, AP), όπου $AP = \gamma \cdot AB$. Ο κύκλος αυτός παριστά το σύνολο των σημείων X του επιπέδου για τα οποία ισχύει $AX = \gamma \cdot AB$. Εάν η απεικόνησή μας είναι $1-1$, θα πρέπει να υπάρχει μοναδικό Γ της $A\varepsilon$ τέτοιο

ώστε $A\Gamma = \gamma \cdot AB$. Αυτό όμως πράγματι συμβαίνει, αφού ο κύκλος μας έχει κέντρο την αρχή της ημιευθείας $A\varepsilon$, και συνεπώς το σημείο τομής του με την $A\varepsilon$ είναι μοναδικό.

Τον τρόπο αυτόν αναπαράστασης των αριθμών θα τον χρησιμοποιούμε για την γεωμετρική κατασκευή αριθμών στο επίπεδο, ή όταν δεν γνωρίζουμε σε ποιό διάστημα βρίσκονται οι αριθμοί που μας ενδιαφέρει να μελετήσουμε.

2.2 Κυκλική αναπαράσταση των θετικών πραγματικών αριθμών

Ακόμη ένας τρόπος αναπαράστασης των θετικών πραγματικών αριθμών είναι με την χρήση σημείων στην περιφέρεια ενός κύκλου. Ειδικά για την περίπτωση των μη αρνητικών ακέραιων αριθμών, εάν θέλουμε να αναπαραστήσουμε ν στο πλήθος διαδοχικούς $\mathbb{Z}_+$ αριθμούς ξεκινώντας από το 0, παίρνουμε πάνω στην περιφέρεια του κύκλου ν σημεία $(A_i | i \in [0, \nu-1] \cap \mathbb{Z}_+)$ τέτοια ώστε κάθε A_i σημείο να απέχει ίδια απόσταση από το A_{i-1} και το A_{i+1}, όπως στο παρακάτω σχήμα. Από τα ν σημεία αυτά επιλέγουμε το $A_0 \equiv O$ ως αρχή. Το τόξο $\widehat{OA_1}$ το ορίζουμε να έχει μήκος μονάδας.



Σχήμα 2.3

Μετρώντας αριστερόστροφα και από το O, παρατηρούμε ότι το τόξο $\widehat{OA_i}$ έχει μήκος $i \cdot \widehat{OA_1}$, για κάθε $i \in [0, \nu-1] \cap \mathbb{Z}_+$. Επομένως είναι εύλογο να ορίσουμε την απεικόνιση $[0, \nu-1] \cap \mathbb{Z}_+ \to \{A_i | i \in [0, \nu-1] \cap \mathbb{Z}_+\}$ έτσι ώστε κάθε αριθμός i να αντιστοιχίζεται στο σημείο A_i, για το οποίο συμβαίνει $\widehat{OA_i} = i \cdot \widehat{OA_1}$.

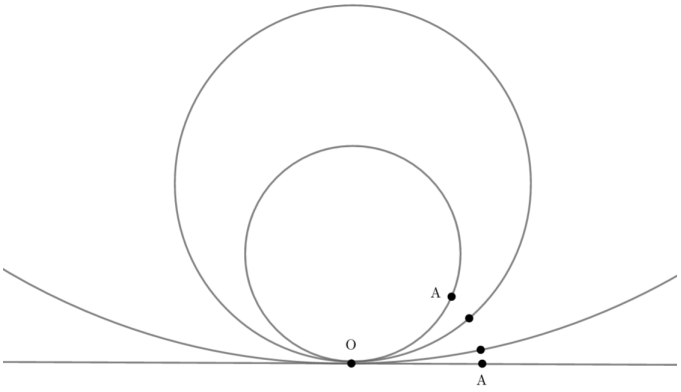
Εδώ, βέβαια, μπορούμε να επεκτείνουμε τον ορισμό αυτόν ώστε να περιέχει όλους τους θετικούς πραγματικούς αριθμούς γνήσια κάτω του ν, παίρνοντας επίσης τα υπόλοιπα σημεία που βρίσκονται μεταξύ των A_i.

Συγκεκριμένα, ένας τυχόν αριθμός $j \in [0, n) \cap \mathbb{R}_+$ θα αντιστοιχίζεται σε σημείο A_j, τέτοιο ώστε $\widehat{OA_j} = j \cdot \widehat{OA_1}$. Το A_j αυτό θα μπορεί να βρίσκεται οπουδήποτε

επί του κύκλου και όχι (απαραίτητα) να ταυτίζεται με κάποιο από τα προηγούμενα $\{A_i | i \in [0, \nu - 1] \cap \mathbb{Z}_+\}$.

Ο ορισμός αυτός είναι χρήσιμος όταν γνωρίζουμε ένα άνω φραγμένο διάστημα στο οποίο ανήκουν οι αριθμοί που μας ενδιαφέρει να μελετήσουμε. Επιπλέον η μελέτη των αριθμών με αυτό το σύστημα είναι ευκολότερη όταν ασχολούμαστε με μη αρνητικούς ακέραιους αριθμούς, γι΄ αυτό και θα το χρησιμοποιήσουμε σε περιπτώσεις όπως αυτήν της αριθμητικής υπολοίπων.

Αξίζει, επίσης, να σημειωθεί ότι εάν θεωρήσουμε κύκλο ακτίνας ρ και το τόξο $\widehat{OA}$ να αντιπροσωπεύει την μονάδα, εάν θέλουμε να παραστήσουμε το σύνολο των θετικών πραγματικών αριθμών με τον 2ο τρόπο, θα έπρεπε, κρατώντας το μήκος $\widehat{OA}$ αμετάβλητο, η ακτίνα να απειρίζεται. Τότε, κατά μια έννοια, οι 2 ορισμοί που αναφέρθηκαν συμπίπτουν, αφού ο κύκλος μας εκφυλίζεται σε ευθεία.



Σχήμα 2.4

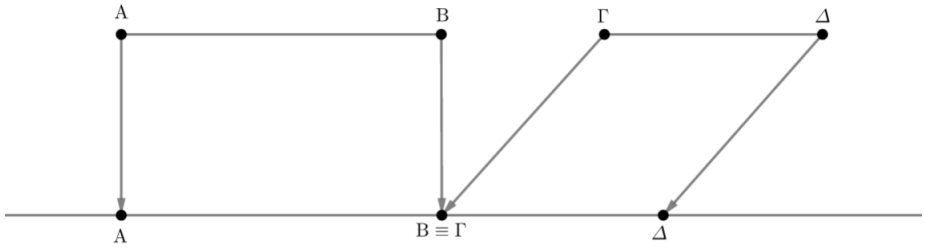
Κεφάλαιο 3

Πράξεις μεταξύ ευθυγράμμων τμημάτων

3.1 Πρόσθεση

Για τις διάφορες πράξεις θα χρησιμοποιήσουμε την γραμμική αναπαράσταση των αριθμών. Αυτό διότι θέλουμε να γενικεύσουμε τα αποτελέσματά μας, χωρίς (απαραίτητα) να γνωρίζουμε το μέγεθος των αριθμών. Συν το ότι στα ευθύγραμμα τμήματα είναι ευκολότερο απ΄ ότι στα τόξα κύκλων να γίνουν μαθηματικοί (αριθμητικοί) υπολογισμοί.

Όσον αφορά την πρόσθεση, υποθέτουμε ότι έχουμε τα ευθύγραμμα τμήματα $AB, \Gamma\Delta$. Για να προσθέσουμε τα τμήματα αυτά θέλουμε, ουσιαστικά, να κατασκευάσουμε ένα νέο ευθύγραμμο τμήμα του οποίου το μήκος θα ισούται με το άθροισμα των μηκών των 2 προηγούμενων. Για να καταφέρουμε κάτι τέτοιο θεωρούμε ευθεία



Σχήμα 3.1

ε του επιπέδου πάνω στην οποία τοποθετούμε αρχικά το AB. Στην συνέχεια, τοποθετείται το $\Gamma\Delta$ έτσι ώστε κάποιο από τα άκρα του να ταυτίζεται με κάποιο από τα άκρα του AB, ενώ ταυτόχρονα, πάνω στην ε, από αριστερά προς τα δεξιά, βρίσκουμε πρώτα τα 2 σημεία του $1^{ου}$ ευθύγραμμου τμήματος και μετά του $2^{ου}$, ή το συμμετρικό του, δηλαδή πρώτα τα 2 σημεία του $2^{ου}$ ευθύγραμμου τμήματος και μετά του $1^{ου}$. Το ίδιο πρέπει να συμβαίνει και από δεξιά προς τα αριστερά. Αυτό το κάνουμε για να αποφύγουμε περιπτώσεις όπως:

Σχήμα 3.2

Στις οποίες δεν δημιουργείται το επιθημητό ευθύγραμμο τμήμα. Τέλος διαλέγουμε το ευθύγραμμο τμήμα που ορίζεται από το αριστερότερο και το δεξιότερο σημείο. Αυτό το τμήμα θα είναι το $AB + \Gamma\Delta$.

3.2 Αφαίρεση

Η αφαίρεση θα γίνει με τρόπο παρόμοιο της πρόσθεσης, με την λογική της μεταφοράς των ευθυγράμμων τμημάτων σε ευθεία ε. Η ειδοποιώς διαφορά θα εντοπίζεται στην σειρά των σημείων των ευθυγράμμων τμημάτων πάνω στην ε.

Έστω AB, $\Gamma\Delta$ να είναι ευθύγραμμα τμήματα. Εάν το μήκος του AB υπερβαίνει το μήκος του $\Gamma\Delta$, θα βρούμε την διαφορά $AB - \Gamma\Delta$. Εάν συμβαίνει το αντίθετο, θα βρούμε την διαφορά $\Gamma\Delta - AB$. Δηλαδή, γενικά θα προσδιορίζουμε την τιμή $|AB - \Gamma\Delta|$. Αυτό διότι σε γεωμετρικό επίπεδο η αναπαράσταση των αρνητικών αριθμών δεν είναι εύκολο εγχείρημα. Συγκεκριμένα θα χρειάζοταν να οριστεί άξονας και προσανατολισμός στα ευθύγραμμα τμήματα (τα οποία θα έπρεπε να είναι παράλληλα του άξονα και με αρχή την αρχή του άξονα). Η αφαίρεση τότε θα μπορούσε να γίνει ως αφαίρεση διανυσμάτων.

Για αρχή, λοιπόν, τοποθετούμε ένα τμήμα από τα 2 επί της ευθείας ε. Στην συνέχεια θα τοποθετίσουμε το 2^o, έτσι ώστε κάποιο από τα άκρα του να ταυτίζεται με κάποιο από τα άκρα του προηγούμενου. Το άκρο που περισσεύει μπορεί να τοποθετηθεί σε 2 σημεία επί της ε, έτσι ώστε να διατηρείται το μήκος του ευθυγράμμου τμήματος αυτού (δηλαδή εκατέρωθεν του ταυτιζόμενου σημείου). Διαλέγουμε το σημείο που δεν δημιουργεί τμήμα $AB + \Gamma\Delta$.

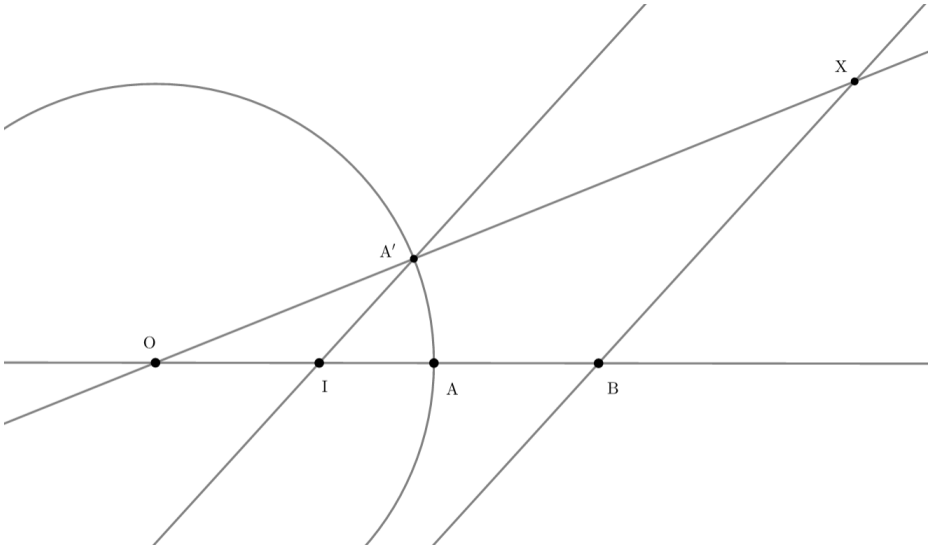
Σχήμα 3.3

Τέλος πάνω στην ε ψάχνουμε 2 διαδοχικά σημεία των ευθυγράμμων τμημάτων που να μην ανήκουν και τα 2 σε ένα από τα ευθύγραμμα τμήματα $AB, \Gamma\Delta$. Αυτά τα σημεία ορίζουν το ευθύγραμμο τμήμα $|AB - \Gamma\Delta|$.

3.3 Πολλαπλασιασμός

Ο πολλαπλασιασμός θα γίνει χρησιμοποιώντας, αυτήν την φορά, την 2^η εκδοχή της γραμμικής αναπαράστασης των αριθμών. Αντίθετα με ό,τι κάναμε προηγουμένως, στην περίπτωση αυτήν θα χρειαστεί βοηθητικά το τμήμα της μονάδας. Στην πρόσθεση, ανεξαρτήτως των προσθετέων, το άθροισμα έβγαινε μεγαλύτερο. Στην αφαίρεση η διαφορά ήταν πάντοτε μικρότερη του μειωτέου. Στον πολλαπλασιασμό δε, ανάλογα με το εάν οι τιμές που πολλαπλασιάζονται είναι μεγαλύτερες, μικρότερες ή ίσες του 1, το μέγεθος του αποτελέσματος μεταβάλλεται. Οπότε, χρειάζεται ένα μέτρο σύγκρισης, το μοναδιαίο τμήμα.

Θεωρούμε, λοιπόν, ευθεία ε, καθώς και τα σημεία της O, I, A, B. Το τμήμα OI θα αντιπροσωπεύει την μονάδα. Θα υπολογίσουμε το γινόμενο $OA \cdot OB$.



Σχήμα 3.4

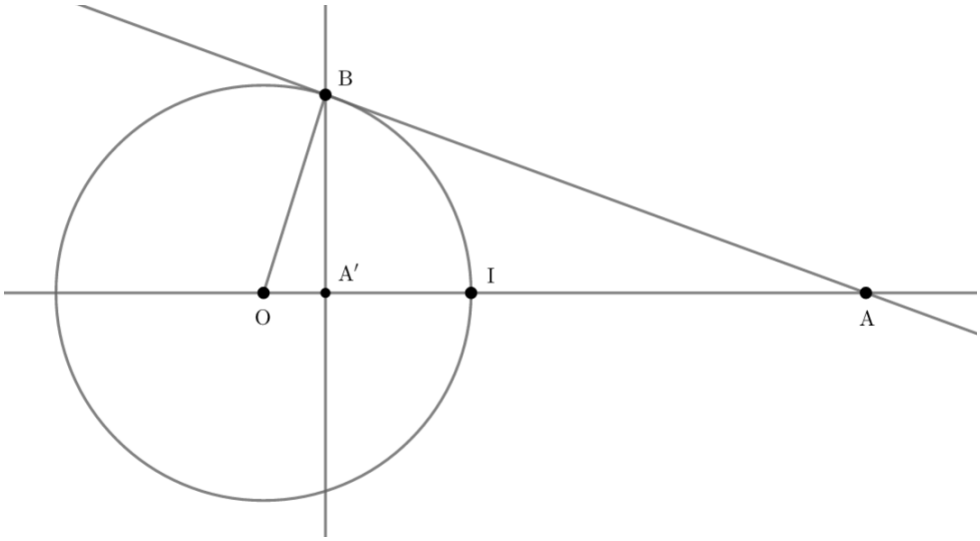
Από το O φέρουμε ευθεία ζ μη παράλληλη προς την ε και σχεδιάζουμε τον κύκλο (O, OA) που τέμνει την ζ στο A'. Από το A' και το I φέρουμε ευθεία η και από το B μια ευθεία $\theta \parallel \eta$, η οποία τέμνει την ζ στο X. Ισχυριζόμαστε ότι $OX = OA \cdot OB$.

Πράγματι, τα τρίγωνα $\overset{\triangle}{OIA'}$ και $\overset{\triangle}{OBX}$ είναι όμοια, αφού $\widehat{IOA'} = \widehat{BOX}$ (κοινή) και $\widehat{A'IO} = \widehat{XBO}$ ($\theta \parallel \eta$). Τότε θα ισχύουν οι αναλογίες των πλευρών: $\dfrac{OA'}{OI} = \dfrac{OX}{OB} \Rightarrow OX \cdot OI = OA' \cdot OB \Rightarrow OX = OA' \cdot OB$. Επειδή OA και OA' αποτελούν ακτίνες του ίδιου κύκλου, έχουμε $OA = OA'$, από το οποίο συνεπάγεται $OX = OA \cdot OB$.

3.4 Αντιστροφή

Πρίν προχωρίσουμε στην διαίρεση θα αναφέρουμε μια ακόμη σημαντική λειτουργία, αυτήν της αντιστροφής. Θεωρώντας ευθεία ε και επί αυτής σημεία O, I και A, όπου OI αντιπροσωπεύει την μονάδα, θα προσδιορίσουμε τον αριθμό $\dfrac{1}{OA}$.

Κατασκευάζουμε, λοιπόν, κύκλο κέντρου O και ακτίνας OI. Από το A φέρουμε εφαπτομένη στον κύκλο (O, OI), η οποία τον τέμνει στο B. Από το B φέρουμε κάθετο προς την ε, η οποία τέμνει την ε στο A'. Αυτό που θα δείξουμε είναι ότι $OA' = \dfrac{1}{OA}$.

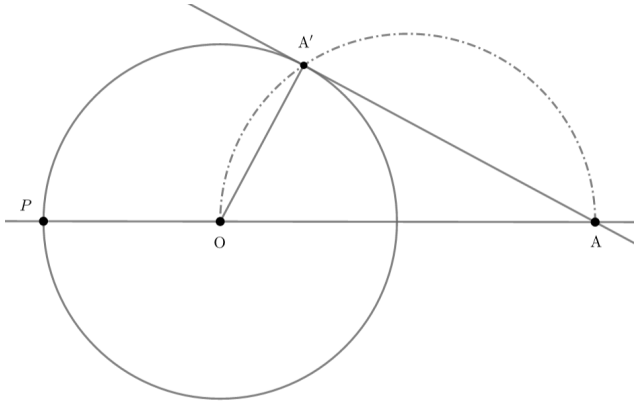


Σχήμα 3.5

Για αρχή παρατηρούμε ότι τα τρίγωνα $\overset{\triangle}{OBA}$ και $\overset{\triangle}{OBA'}$ είναι όμοια, καθώς είναι και τα 2 ορθογώνια $\left(\widehat{OBA} = \widehat{OA'B} = \dfrac{\pi}{2}\right)$ και επίσης έχουν κοινή την γωνία $\widehat{BOA}$.

Οπότε ισχύουν οι αναλογίες: $\dfrac{OB}{OA} = \dfrac{OA'}{OB}$. Επειδή OB, OI αποτελούν ακτίνες του ίδιου κύκλου (O, OI), έχουμε $OB = OI$. Από αυτά συμπαιρένουμε ότι $OA' = \dfrac{OB^2}{OA} \Rightarrow OA' = \dfrac{1}{OA}$, το οποίο αποδεικνύει το ζητούμενο.

Προηγουμένως, στην γεωμετρική κατασκευή του αντίστροφου, χρειάστηκε να φέρουμε εφαπτομένη σε κύκλο από εξωτερικό του σημείο (τετριμμένα, εάν ανήκει στον κύκλο). Δεν εξηγήθηκε όμως πως ακριβώς γίνεται η διαδικασία αυτή.



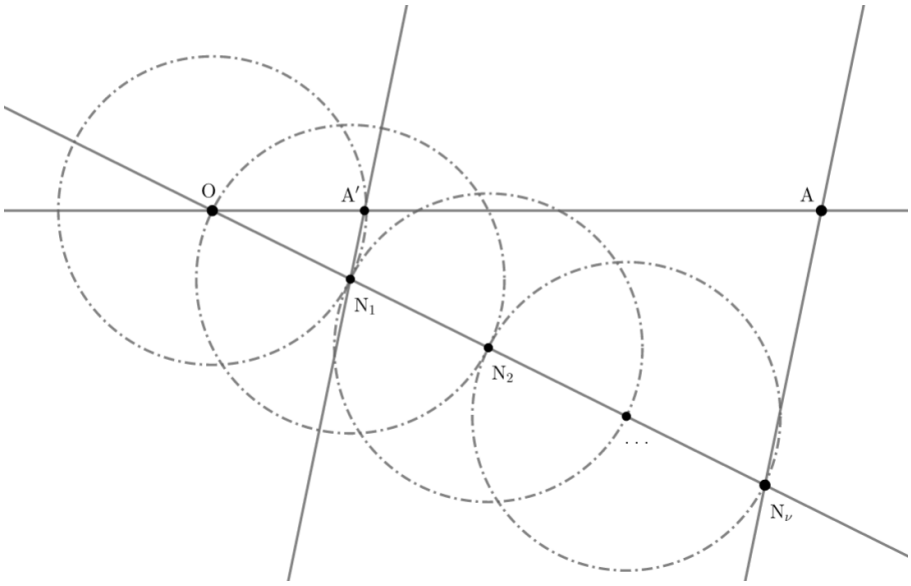
Σχήμα 3.6

Γενικά ας θεωρήσουμε κύκλο (O, OP) και τυχαίο σημείο A που να μην ανήκει σ΄ αυτόν (εάν ανήκει, η περίπτωση είναι τετριμμένη: Φέρνουμε κάθετο στην OA από το A). Ουσιαστικά θέλουμε να βρούμε ένα σημείο A' το οποίο ανήκει στον (O, OP) και επίσης $OA \perp AA'$. Όμως ο γεωμετρικός τόπος των A' για τα οποία συμβαίνει $OA \perp AA'$ είναι ο κύκλος διαμέτρου OA που διέρχεται από τα O και A. Τελικά το A' θα πρέπει να είναι η τομή των 2 κύκλων που αναφέρθηκαν προηγουμένως και συνεπώς η εφαπτομένη είναι η OA'.

3.5 Διαίρεση

Αρχικά θα αναφερθούμε στην διαίρεση με την πιο απλή της μορφή, δηλαδή διαίρεση οποιουδήποτε θετικού πραγματικού αριθμού α με φυσικό αριθμό ν. Σε αυτήν την περίπτωση θα προσπαθούμε, ουσιαστικά, να χωρίσουμε ευθύγραμμο τμήμα μήκους α σε ν ίσα τμήματα.

Ας θεωρήσουμε ότι ο αριθμός α αντιστοιχεί σε ευθύγραμμο τμήμα OA. Από τα O, A φέρουμε ευθεία ε και από το O μια τυχαία ευθεία $\zeta \nparallel \varepsilon$. Στην ζ, από το O, κατασκευάζουμε κύκλο ακτίνας ρ που τέμνει την ζ στο N_1. Από το N_1, κατασκευάζουμε κύκλο ακτίνας πάλι ρ, που τέμνει την ζ στο $N_2 \not\equiv O$. Από το N_2 κατασκευάζουμε κύκλο ακτίνας ρ, που τέμνει την ζ στο $N_3 \not\equiv N_1$.



Σχήμα 3.7

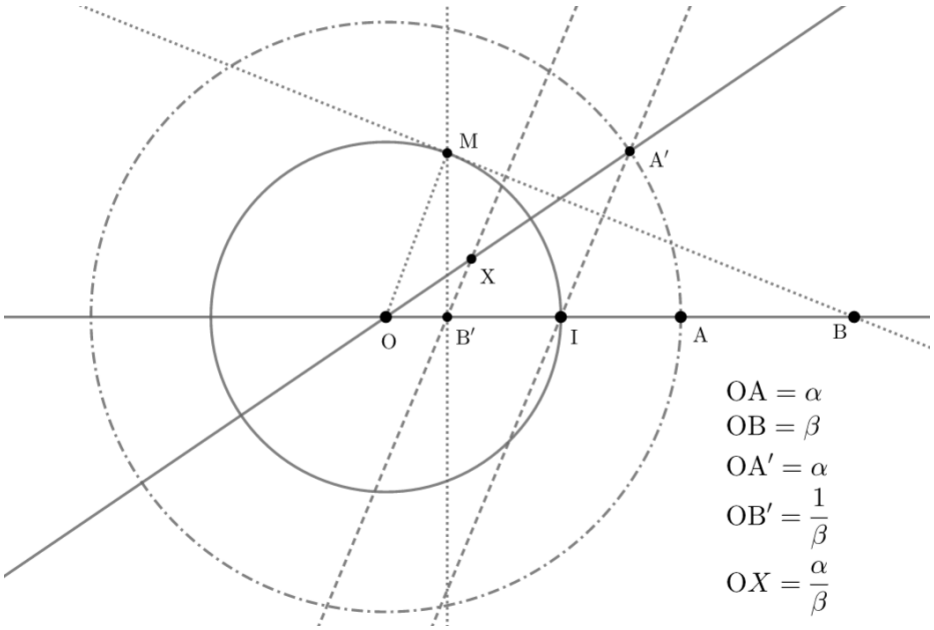
Συνεχίζουμε καθ' αυτόν τον τρόπο ώσπου επί της ζ να έχουμε δημιουργήσει στο πλήθος ν ίσα ευθύγραμμα τμήματα $ON_1 = N_1N_2 = \cdots = N_iN_{i+1} = \cdots = N_{\nu-1}N_\nu = \rho$. Τέλος φέρουμε την ευθεία η που διέρχεται από τα A, N_ν και σε αυτήν μια παράλληλη θ που να διέρχεται από το N_1. Υποθέτουμε ότι η θ τέμνει την ε στο A'. Θα δείξουμε ότι $OA' = \dfrac{OA}{\nu}$.

Πράγματι, ισχύει ότι τα τρίγωνα $\overset{\triangle}{OAN_\nu}$ και $\overset{\triangle}{OA'N_1}$ είναι όμοια, αφού έχουν την $\widehat{AON_\nu}$ κοινή και $\widehat{AN_\nu O} = \widehat{A'N_1O}$, λόγω της παραλληλίας των η και θ. Οπότε, ισχύουν οι αναλογίες των πλευρών: $\dfrac{OA'}{ON_1} = \dfrac{OA}{ON_\nu}$. Επειδή κατασκευάσαμε τα σημεία N_i με τρόπο τέτοιο ώστε $ON_1 = N_1N_2 = \cdots = N_iN_{i+1} = \cdots = N_{\nu-1}N_\nu =$

ρ, έχουμε ότι $ON_\nu = ON_1 + N_1N_2 + N_2N_3 + \cdots + N_{\nu-1}N_\nu = \nu \cdot \rho$. Οπότε, $\dfrac{OA'}{\rho} = \dfrac{OA}{\nu\rho} \Rightarrow OA' = \dfrac{OA}{\nu}$, που είναι το ζητούμενο.

Υπάρχει, βέβαια, και η περίπτωση που η διαίρεση του θετικού πραγματικού αριθμού α γίνεται από τυχαίο θετικό πραγματικό αριθμό β, ο οποίος δεν είναι απαραίτητα φυσικός. Σε αυτήν την περίπτωση, δεν μπορούμε να εφαρμόσουμε πάντοτε την προηγούμενη μέθοδο.

Εδώ θα βρίσκουμε με την βοήθεια της αντιστροφής το τμήμα $\dfrac{1}{\beta}$, το οποίο στην συνέχεια θα πολλαπλασιάζουμε με το α για να βρούμε τον $\dfrac{\alpha}{\beta}$. Συγκεκριμένα, εάν $OA = \alpha$, $OB = \beta$ και OI αντιπροσωπεύει την μονάδα, με O, I, A, B σημεία επί ευθείας ε, έχουμε:



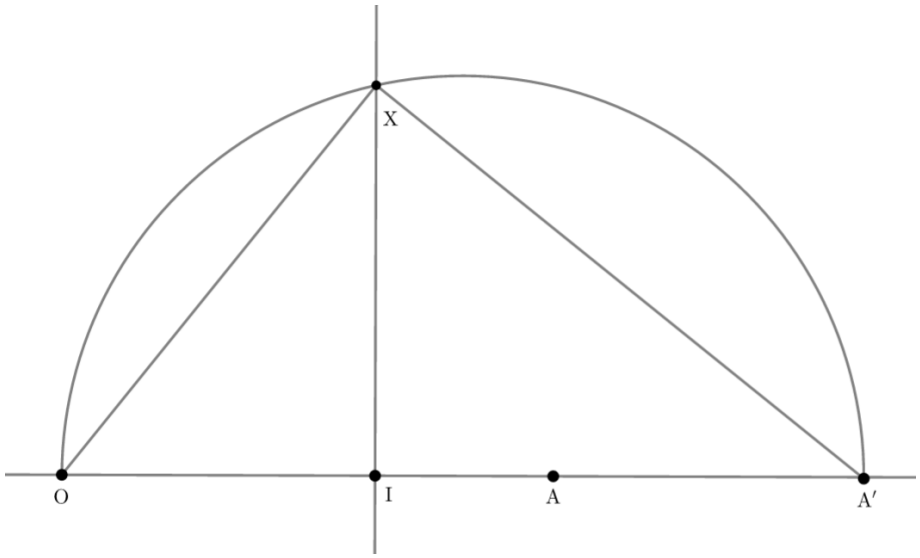
Σχήμα 3.8

Το τμήμα OX θα αντιπροσωπεύει το αποτέλεσμα $\dfrac{\alpha}{\beta}$

3.6 Τετραγωνική ρίζα αριθμού

Τέλος θα ασχοληθούμε με την κατασκευή της τετραγωνικής ρίζας ενός θετικού πραγματικού αριθμού. Ας θεωρήσουμε α έναν τυχαίο θετικό πραγματικό αριθμό. Θα προσδιορίσουμε την τιμή $\sqrt{\alpha}$.

Θεωρούμε σημεία O,I,A επί μιας ευθείας ε, με OI να αντιπροσωπεύει την μονάδα και $OA = \alpha$. Προσθέτουμε στο τμήμα OI το τμήμα OA προς σχηματισμό του $OI + OA = OA'$. Το τελευταίο βήμα είναι να κατασκευάσουμε ημικύκλιο διαμέτρου OA' και να φέρουμε την κάθετο ζ από το I στην ε που τέμνει το ημικύκλιο στο X. Θα δείξουμε ότι το τμήμα IX αντιστοιχεί στην ρίζα του α.



Σχήμα 3.9

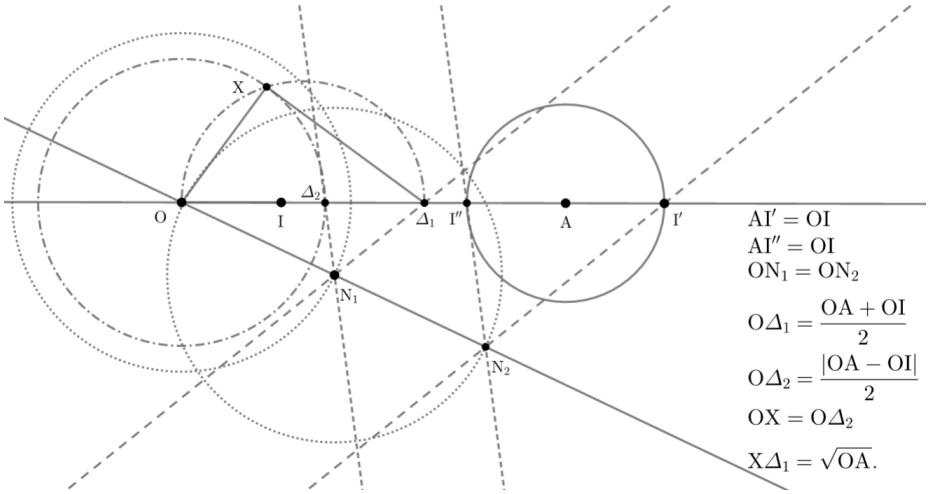
Καταρχάς, επειδή στο OI προσθέσαμε το OA για να κατασκευάσουμε το OA', συνεπάγεται ότι $IA' = OA$. Επειδή το τρίγωνο $\overset{\triangle}{OX}A'$ είναι εγγεγραμμένο σε ημικύκλιο, θα είναι ορθογώνιο. Οπότε: $\widehat{IXA'} + \widehat{OXI} = \dfrac{\pi}{2}$. Όμως, στο τρίγωνο $\overset{\triangle}{IX}A'$ ισχύει $\pi = \dfrac{\pi}{2} + \widehat{IXA'} + \widehat{IA'X} \Rightarrow \dfrac{\pi}{2} = \widehat{IXA'} + \widehat{IA'X}$, από το οποίο συνεπάγεται ότι: $\widehat{OXI} = \widehat{IA'X}$.

Λόγω αυτής της ισότητας των γωνιών και της καθετότητας της ζ στην ε $\Big($δηλαδή $\widehat{OIX} = \widehat{XIA'} = \dfrac{\pi}{2}\Big)$, τα τρίγωνα $\overset{\triangle}{OX}I$ και $\overset{\triangle}{IX}A'$ θα είναι όμοια. Από αυτό έπεται το ζητούμενο, καθώς: $\dfrac{IX}{OI} = \dfrac{IA'}{IX} \Rightarrow IX = \dfrac{OA}{IX} \Rightarrow IX^2 = OA$.

Υπάρχει άλλος ένας τρόπος υπολογισμού της ρίζας ενός θετικού πραγματικού αριθμού που βασίζεται, αυτήν την φορά, στο πυθαγόρειο θεώρημα. Συγκεκριμένα, εάν OA αντιστοιχεί στο α και OI στην μονάδα, αρκεί να παρατηρήσουμε ότι τα ευθύγραμμα τμήματα $\sqrt{OA}$, $\dfrac{|OA-OI|}{2}$, $\dfrac{OA+OI}{2}$, αποτελούν πλευρές ορθογωνίου τριγώνου, καθώς:

$$\sqrt{OA}^2+\Big(\frac{|OA-OI|}{2}\Big)^2 = OA+\frac{OA^2}{4}-OA\cdot\frac{OI}{2}+\frac{OI^2}{4} = OA+\frac{OA^2}{4}-\frac{OA}{2}+\frac{OI^2}{4} = \frac{OA^2}{4}+\frac{OA}{2}+\frac{OI^2}{4} = \frac{OA^2}{4}+OA\cdot\frac{OI}{2}+\frac{OI^2}{4} = \Big(\frac{OA+OI}{2}\Big)^2.$$

Οπότε για τον προσδιορισμό της ρίζας, αρκεί να κατασκευαστεί ορθογώνιο τρίγωνο με υποτείνουσα $\dfrac{OA+OI}{2}$ και κάθετη πλευρά $\dfrac{|OA-OI|}{2}$. Η υπολοιπόμενη κάθετος θα αντιστοιχεί στην $\sqrt{OA}$.



Σχήμα 3.10

Για την κατασκευή, λοιπόν, θεωρούμε ευθεία ε και επί αυτής O, I, A. Από το A προσθαφαιρούμε OI, σχηματίζοντας $OI' = OA+OI$, $OI'' = |OA-OI|$. Στην συνέχεια, διαιρούμε δια του 2 τα 2 προαναφερόμενα τμήματα. Αυτό το κάνουμε (όπως προηγουμένως) ως εξής: Από το O φέρουμε ευθεία $\zeta \nparallel \varepsilon$. Παίρνουμε επί της ζ σημεία N_1, N_2, τέτοια ώστε $ON_1 = N_1N_2$. Για την διαίρεση του OI', φέρουμε ευθεία η να διέρχεται από τα N_2, I' και $\theta \parallel \eta$ που διέρχεται από το N_1 και τέμνει την ε στο Δ_1. Το $O\Delta_1$ είναι το μισό του OI'. Αντίστοιχα, για την διαίρεση του OI'', φέρουμε ευθεία κ να διέρχεται από τα N_2, I'' και παράλληλη προς αυτήν λ που διέρχεται από το N_1 και τέμνει την ε στο Δ_2. Το $O\Delta_2$ είναι το μισό του OI''. Σκοπός μας είναι να δημιουργήσουμε, ουσιαστικά, ορθογώνιο τρίγωνο με υποτείνουσα $O\Delta_1$ και κάθετο $O\Delta_2$. Κρατούμε, λοιπόν, το $O\Delta_1$ σταθερό και παρατηρούμε ότι η πιθανή θέση του επιθυμητού τμήματος μήκους $O\Delta_2$ (Έστω

OX) γύρω του O δημιουργεί κύκλο. Επειδή επίσης θέλουμε το τρίγωνο που θα δημιουργηθεί να είναι ορθογώνιο, το X θα πρέπει να βρίσκεται επί του ημικυκλίου με διάμετρο $O\Delta_1$ που διέρχεται από τα O, Δ_1 †. Οπότε το X είναι η τομή του κύκλου $(O, O\Delta_2)$ και του ημικυκλίου διαμέτρου $O\Delta_1$ που διέρχεται από τα O, Δ_1.

Με αυτόν τον τρόπο έχουμε κατασκευάσει ορθογώνιο τρίγωνο $O\overset{\triangle}{\Delta_1}X$ με υποτείνουσα $O\Delta_1 = \dfrac{OA+OI}{2}$ και κάθετο $OX = O\Delta_2 = \dfrac{|OA-OI|}{2}$. Η δεύτερη κάθετη θα πρέπει, σύμφωνα με ό,τι έχουμε δείξει, να είναι $\Delta_1 X = \sqrt{OA}$.

† *Εδώ θα μπορούσαμε να είχαμε πάρει κύκλο αντί για ημικύκλιο. Το αποφεύγουμε διότι θα προέκυπταν 2 σημεία X από τα οποία χρειαζόμαστε μόνον το 1.*

Κεφάλαιο 4

Το σύνολο των κατασκευάσιμων αριθμών

Στο δεύτερο κεφάλαιο μελετήσαμε τρόπους αναπαράστασης των θετικών πραγματικών αριθμών και βρήκαμε 2 τρόπους να αναπαριστούμε καθέναν από τους αριθμούς αυτούς. Στο τρίτο κεφάλαιο, αναπαριστώντας τους θετικούς πραγματικούς αριθμούς γραμμικά, ασχοληθήκαμε με τις πράξεις που μπορούν να υπάρξουν μεταξύ ευθυγράμμων τμημάτων και προσδιορίσαμε την πρόσθεση, την αφαίρεση, τον πολλαπλασιασμό, την αντιστροφή, την διαίρεση και τον υπολογισμό της ρίζας. Αυτό που όμως δεν μελετήσαμε είναι ποιοί από τους θετικούς πραγματικούς αριθμούς μπορούν να κατασκευαστούν (και όχι απλώς να αναπαραστηθούν) με την χρήση των προηγούμενων πράξεων (πεπερασμένες στο πλήθος χρήσεις) με ως μόνο δεδομένο ευθύγραμμο τμήμα αυτό της μονάδας. Δηλαδή, εάν πάνω στο τμήμα της μονάδας δράσουμε με τις προηγούμενες πράξεις, θα θέλαμε να δούμε ποιούς από τους $\mathbb{R}_+$ αριθμούς μπορούμε να κατασκευάσουμε.

- Όσον αφορά τους $\mathbb{N}$: Κάθε $\nu \in \mathbb{N}$ μπορεί να κατασκευαστεί με πρόσθεση ν τμημάτων της μονάδας.

- Όσον αφορά τους $\mathbb{Q}_+$: Κάθε $\xi \in \mathbb{Q}_+$ μπορεί να κατασκευαστεί με διαίρεση. Συγκεκριμένα το ξ, ως ρητός, θα γράφεται στην μορφή $\frac{\alpha}{\beta}$, $\alpha, \beta \in \mathbb{N}$. Τα α, β είναι κατασκευάσιμα, όπως είδαμε προηγουμένως, οπότε, διαιρώντας το α με το β, παίρνουμε το ζητούμενο.

- Όσον αφορά τους $\mathbb{R}_+ - \mathbb{Q}$: Εδώ η κατάσταση είναι περιπλοκότερη.
  Για αρχή, κάθε ρίζα της μορφής $\sqrt{q}$ με $q \in \mathbb{N} \wedge q \neq \nu^2$ με $\nu \in \mathbb{N}$ είναι κατασκευάσιμη, όπως αναφέραμε στο προηγούμενο κεφάλαιο.
  Εάν αντί $q \in \mathbb{N}$ είχαμε $q \in \mathbb{Q}_+ - \mathbb{N}$ και πάλι η $\sqrt{q}$ θα είναι αριθμός κατασκευάσιμος.

  Προφανώς, οποιοσδήποτε συνδιασμός της μορφής $\overbrace{\sqrt{\sqrt{\dots\sqrt{q}}}}^{\nu\in\mathbb{N}} \in \mathbb{R} - \mathbb{Q}$,

$q \in \mathbb{Q}_+$ είναι κατασκευάσιμος, αφού όλες οι ρίζες είναι κατασκευάσιμες και q κατασκευάσιμος.

Γενικότερα, κάθε μορφή $\sqrt{a_1 + b_1\sqrt{a_2 + b_2\sqrt{\ldots\sqrt{a_\nu + b_\nu\sqrt{a_{\nu+1}}}}}} \in \mathbb{R} - \mathbb{Q}$ με $a_i, b_i \in \mathbb{Q}_+$, $\nu \in \mathbb{N}$ είναι κατασκευάσιμη, αφού $\sqrt{a_{\nu+1}}$ κατασκευάσιμος, $b_\nu\sqrt{a_{\nu+1}}$ κατασκευάσιμος, $a_\nu + b_\nu\sqrt{a_{\nu+1}}$ κατασκευάσιμος, $\ldots$, $\sqrt{a_1 + b_1\sqrt{a_2 + b_2\sqrt{\ldots\sqrt{a_\nu + b_\nu\sqrt{a_{\nu+1}}}}}}$ κατασκευάσιμος.

(*Στα προηγούμενα, εάν αλλάξουμε κάποια από τα $+$ σε $-$ και ο αριθμός εξακολουθεί να είναι άρρητος, τότε προφανώς κατασκευάζεται. Αυτό περιλαμβάνει και τα $+$ μπροστά από τα α_i.*)

Δηλαδή οποιοσδήποτε πεπερασμένος συνδιασμός των πράξεων που αναφέραμε σε έναν κατασκευάσιμο αριθμό δίδει άρρητο, είναι κατασκευάσιμος (αυτό μπορεί να προκύψει και από τον ορισμό της κατασκευασιμότητας). Από τον ορισμό της κατασκευασιμότητας, επίσης προκύπτει ότι ισχύει και το αντίστροφο· δηλαδή, ένας κατασκευάσιμος άρρητος θα είναι πάντοτε συνδιασμός των πράξεων που αναφέρθηκαν πάνω σε κάποιον κατασκευάσιμο αριθμό.

Προσδιορίσαμε, λοιπόν, ποιοί από τους $\mathbb{R}_+$ αριθμούς μπορούν να κατασκευαστούν γεωμετρικά. Αυτό που θα θέλαμε επίσης να κάνουμε είναι να βρούμε μια γενική μορφή, έναν γενικό τύπο, ο οποίος θα εκφράζει όλους τους κατασκευάσιμους αριθμούς. Αυτό θα γίνει με την βοήθεια μιας συνάρτησης, η οποία θα μπορεί, αναλόγως την είσοδο, να κάνει οποιαδήποτε από τις πράξεις αναφέραμε προηγουμένως πάνω σε έναν ή περισσότερους αριθμούς. Από την στιγμή που θα έχουμε στα χέρια μας μια τέτοια συνάρτηση, θα μπορούμε εν συνεχεία, να εκφράσουμε κάθε κατασκευάσιμο αριθμό με πεπερασμένο αριθμό συνθέσεων της συνάρτησής μας.

Συγκεκριμένα θεωρούμε $K : K(a, b, c, d) = \left|\frac{a}{b} + (-1)^c \cdot \sqrt{d}\right|$,
με $(a, b, d) \in \mathbb{K}^3$, $c \in \mathbb{N}$, όπου $\mathbb{K}$ το σύνολο των κατασκευάσιμων αριθμών.

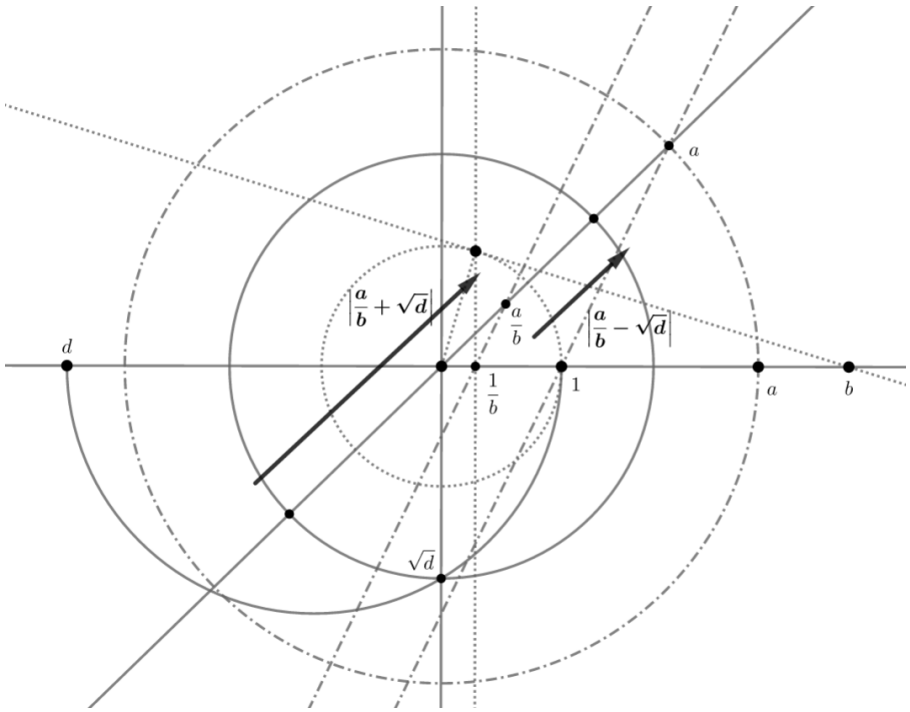
Η συνάρτηση αυτή μπορεί να κάνει όλες τις πράξεις που αναφέραμε στο προηγούμενο κεφάλαιο:

- Για την αντιστροφή ενός $x \in \mathbb{K}$, θεωρούμε $a = 1, b = x, c \in \mathbb{N}, d = 0$ και έχουμε:
  $K(1, x, c, 0) = \left|\frac{1}{x} + 0\right| = \frac{1}{x}$.
- Για την διαίρεση του x από y με $x, y \in \mathbb{K}^*$, θεωρούμε $a = x, b = y, c \in \mathbb{N}, d = 0$ και έχουμε:
  $K(x, y, c, 0) = \left|\frac{x}{y} + 0\right| = \frac{x}{y}$.
- Για τον πολλαπλασιασμό των $x, y \in \mathbb{K}$, θεωρούμε $a = y, b = K(1, x, c, 0), c \in \mathbb{N}, d = 0$ και έχουμε:

$$K(y, K(1, x, c, 0), c, 0) = \Big| \frac{y}{K(1, x, c, 0)} + 0 \Big| = \left| \frac{y}{\frac{1}{x}} \right| = x \cdot y.$$

- Για την πρόσθεση των $x, y \in \mathbb{K}$, θεωρούμε $a = x, b = 1, c \propto 2, d = K\big(y, K(1, y, c, 0), c, 0\big)$ και έχουμε:
  $K\Big(x, 1, c, K\big(y, K(1, y, c, 0), c, 0\big)\Big) = \Big| \frac{x}{1} + \sqrt{K\big(y, K(1, y, c, 0), c, 0\big)} \Big| = |x + \sqrt{y^2}| = |x + y| = x + y.$
- Για την αφαίρεση του x από y με $x, y \in \mathbb{K}$ και (χωρίς βλαβη της γενικότητας) $x \geq y$, θεωρούμε $a = x, b = 1, c \propto 2, d = K\big(y, K(1, y, c, 0), c, 0\big)$ και έχουμε:
  $K\Big(x, 1, c, K\big(y, K(1, y, c, 0), c, 0\big)\Big) = \Big| \frac{x}{1} - \sqrt{K\big(y, K(1, y, c, 0), c, 0\big)} \Big| = |x - \sqrt{y^2}| = |x - y| = x - y.$

Παρακάτω εικονίζεται η γεωμετρική αναπαράσταση της συνάρτησης K:



Σχήμα 4.1

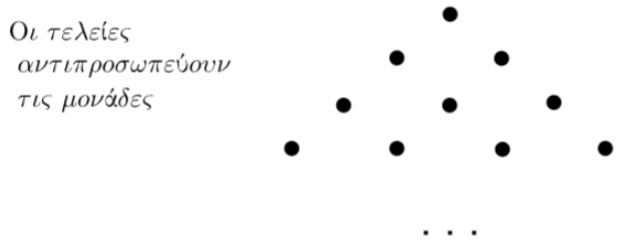
Κεφάλαιο 5

Ειδικές κατηγορίες κατασκευάσιμων αριθμών

5.1 Τρίγωνοι αριθμοί

Στο κεφάλαιο αυτό θα ασχοληθούμε με ορισμένες ενδιαφέρουσες κατηγορίες πραγματικών, κατασκευάσιμων αριθμών. Οι κατηγορίες αυτές έχουν μια ιδιαίτερη γεωμετρική εικόνα / γεωμετρική ερμηνεία, που αξίζει να παρουσιαστεί.

Ξεκινώντας από τους τρίγωνους αριθμούς· τρίγωνοι θα ονομάζονται οι φυσικοί αριθμοί που οι μονάδες τους μπορούν να σχηματίσουν μια τριγωνική διάταξη στο επίπεδο, στην οποίαν η πρώτη σειρά θα έχει μια μονάδα, η δεύτερη 2, ..., η $(\nu-1)$-οστή $\nu-1$, και η ν-οστή ν. Συγκεκριμένα οι τρίγωνοι αριθμοί παίρνουν την ακόλουθη μορφή:

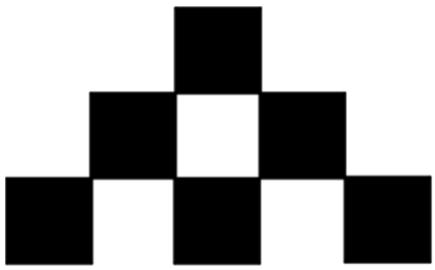


Σχήμα 5.1

Εμείς θα επιχειρήσουμε να μεταφράσουμε αυτήν την γεωμετρική εικόνα σε έναν

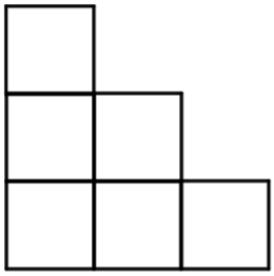
αλγεβρικό τύπο, από τον οποίον θα μπορούμε να βρούμε όποιον τρίγωνο αριθμό επιθυμούμε.

Για να πετύχουμε τον στόχο μας, αρχικά θα εκφράσουμε την γεωμετρική μορφή των τρίγωνων αριθμών με μια γεωμετρική πάλι μορφή που θα είναι βολικότερη για τους υπολογισμούς μας. Στο προηγούμενο σχήμα συμβολίζαμε με τελείες τις μονάδες. Οι μονάδες όμως μπορούν αλλιώς να αντιστοιχηθούν στο εμβαδόν τετραγώνων πλευράς μήκους 1. Πρακτικά αυτό σημαίνει ότι μπορούμε να αντιστοιχήσουμε τετράγωνα αντί τελείες στις μονάδες. Οπότε, εάν αντικαταστήσουμε τις τελείες με τετράγωνα στο αρχικό μας σχήμα, παίρνουμε την ακόλουθη μορφή:



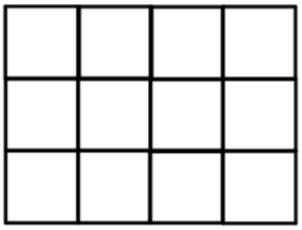
Σχήμα 5.2

Προφανώς, το εμβαδόν του σχήματος που προκύπτει θα αντιστοιχεί στο σύνολο των μονάδων, που δεν είναι τίποτε άλλο, με την σειρά του, από τον τρίγωνο αριθμό μας. Εν συνεχεία μεταφέρουμε τα τετράγωνα παράλληλα έτσι ώστε να δημιουργηθούν στήλες τετραγώνων, με την πρώτη να έχει ν τετράγωνα, την δευτερη$\to \nu-1$ ...την $\nu-1\to 2$ και την $\nu\to 1$.



Σχήμα 5.3

Διπλασιάζοντας το σχήμα του προέκυψε, το προσθέτουμε κατάλληλα στον εαυτό του δημιουργώντας, έτσι, ένα παραλληλόγραμμο.



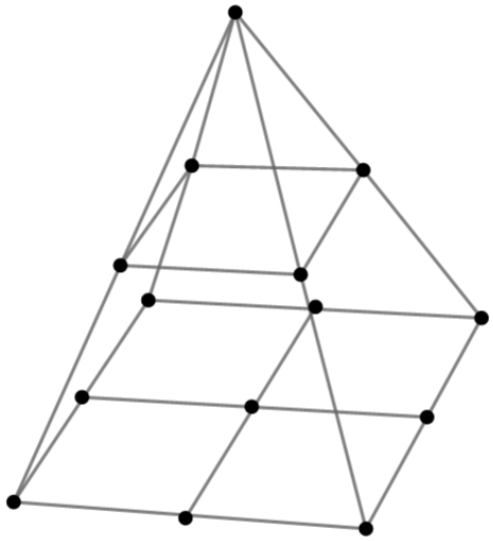
Σχήμα 5.4

Το παραλληλόγραμμο που προκύπτει θα έχει πλευρές ν και $\nu+1$. Επειδή το εμβαδόν του ισούται με 2 φορές τον τριγωνικό αριθμό, έπεται ότι ο τριγωνικός μας αριθμός έχει την μορφή: $\dfrac{\nu\cdot(\nu+1)}{2}$.

Πόρισμα: Το άθροισμα $\sum_{x=1}^{\nu} x$ ισούται με $\dfrac{\nu\cdot(\nu+1)}{2}$ για κάθε $\nu\in\mathbb{N}$.
Πράγματι, από το πρώτο σχήμα βλέπουμε ότι κάθε τριγωνικός αριθμός είναι της μορφής $\tau = 1+2+3+4+\cdots+\nu$ και επίσης αποδείξαμε ότι $\tau = \dfrac{\nu\cdot(\nu+1)}{2}$.
Οπότε, $1+2+3+4+\cdots+\nu = \dfrac{\nu\cdot(\nu+1)}{2}$, το οποίο είναι το ζητούμενο.

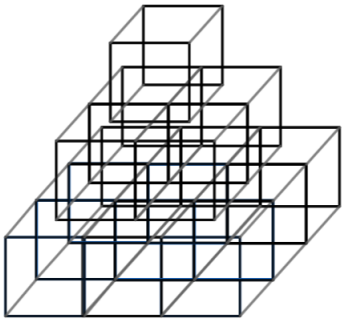
5.2 Πεντάεδροι αριθμοί

Ανάλογα με τους τρίγωνους αριθμούς, πεντάεδροι θα ονομάζονται οι φυσικοί αριθμοί που οι μονάδες τους μπορούν να σχηματίσουν μια πενταεδρική (πυραμιδοειδή) διάταξη στον χώρο, στην οποίαν το πρώτο επίπεδο θα έχει μια μονάδα, το δεύτερο 2^2, ..., το $(\nu-1)$-οστό $(\nu-1)^2$, και το ν-οστό ν^2. Συγκεκριμένα οι πεντάπλευροι αριθμοί παίρνουν την ακόλουθη μορφή:

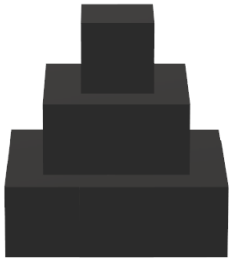


Σχήμα 5.5

Η λογική μας εδώ θα είναι ανάλογη αυτής των τρίγωνων αριθμών. Δηλαδή θα αναζητήσουμε ένα βολικό για τους υπολογισμούς μας, εν προκειμένω, γεωμετρικό στερεό, το οποίο στο πρώτο σχήμα θα αντικαταστήσει τις τελείες. Προφανώς θα διαλέξουμε τον κύβο όγκου 1.



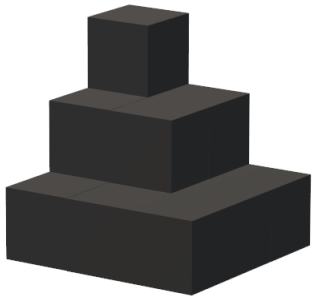
(α′)



(β′) *Ένα λιγότερα περίπλοκο σχήμα*

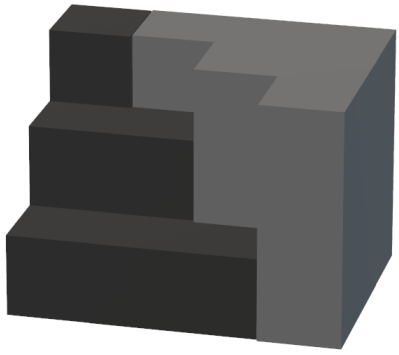
Ο όγκος του σχήματος που προκύπτει θα αντιστοιχεί στο σύνολο των μονάδων, που δεν είναι τίποτε άλλο, με την σειρά του, από τον πεντάεδρο αριθμό μας.

Στην συνέχεια θα μετακινήσουμε τους κύβους των διαφόρων επιπέδων με τρόπο τέτοιο ώστε να δημιουργηθεί ένας πύργος ύψους ν, γύρω από αυτόν και σε σχήμα Γ ένας δεύτερος πύργος ύψους $\nu - 1$, εφαπτόμενα του πύργου σχήματος Γ ένας τρίτος πύργος, επίσης σχήματος Γ και ύψους $\nu - 2$. Συνεχίζουμε καθ′ αυτόν τον τρόπο έως ότου η βάση του προκύπτωντος πυραμιδοειδούς να περιέχει ν^2 κύβους.



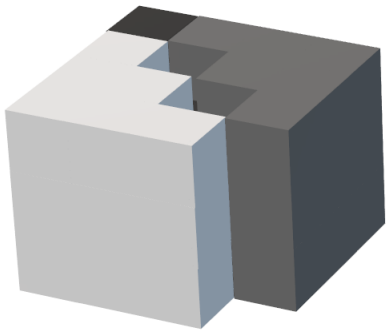
Σχήμα 5.7

Στην συνέχεια διπλασιάζουμε την δομή αυτή και περιστρέφουμε το αντίγραφο έτσι ώστε, για τις ακμές του παραλληλεπιπέδου της βάσης που απέχουν το μέγιστο από τον κορυφαίο κύβο, η μια μεγάλη ακμή να είναι κάθετη στο επίπεδο που περιέχει την μεγάλη έδρα του παραλληλεπιπέδου της βάσης, της αρχικής δομής ενώ η άλλη μεγάλη ακμή να απέχει απόσταση από το επίπεδο της βάσης μικρότερη της απόστασης που ορίζει η παράλληλή της ακμή στο επίπεδο των 2 μεγάλων ακμών με το επίπεδο της βάσης. Έπειτα μετακινούμε τις δύο δομές έτσι ώστε οι δύο κορυφαίοι κύβοι να εφάπτονται, η ανώτερη έδρα του ενός με μια πλάγια του άλλου, όπως στο ακόλουθο σχήμα:



Σχήμα 5.8

Τέλος, με παρόμοιο τρόπο, διπλασιάζουμε ξανά την αρχική δομή μας και περιστέφοντάς την κατάλληλα την τοποθετούμε συμμετρικά στην άλλη μη επίπεδη μεριά της αρχικής δομής.



Σχήμα 5.9

Με την κατασκευή αυτή βλέπουμε ότι προκύπτει ένα παραλληλεπίπεδο όγκου $\nu \cdot (\nu+1) \cdot (\nu+1) = \nu \cdot (\nu+1)^2$, από το οποίο, βέβαια, κάποια τμήματα λείπουν. Ο όγκος του παραλληλεπιπέδου αυτού πλην του όγκου των τμημάτων που λείπουν θα είναι, ουσιαστικά, το τριπλάσιο του πεντάεδρου αριθμού μας.

Στον πρώτο πύργο σχήματος Γ, προσθέσαμε στην κορυφή του δύο κύβους που κάλυψαν επιφάνεια $2 \cdot 1 = 2$. Οπότε αφού ο ίδιος είχε επιφάνεια $2 \cdot 1 + 1 = 3$, θα δημιουργήθηκε κενό ενός κύβου. Στον δεύτερο πύργο σχήματος Γ, προσθέσαμε στην κορυφή του δύο παραλληλεπίπεδα 2^2 κύβων με τετραγωνικές βάσεις. Οι μη τετραγωνικές βάσεις αυτών των παραλληλεπιπέδων κάλυψαν επιφάνεια $2 + 2 = 4$ στην κορυφή του πύργου. Όμως η συνολική επιφάνεια της κορυφής του πύργου είναι $2 \cdot 2 + 1 = 5$, το οποίο σημαίνει ότι δημιουργείται ένας $2 \cdot 1$ κενός πύργος. Συνεχίζοντας με ακριβώς ανάλογο τρόπο βρίσκουμε ότι τα κενά τμήματα που δημιουργούνται έχουν όγκους: $1, 2, 3, 4, \ldots, \nu-1, \nu$. Συνεπώς το άθροισμα των όγκων των κενών τμημάτων θα είναι $1 + 2 + 3 + \cdots + \nu$. Αυτός είναι ένας τριγωνικός αριθμός και, άρα, θα παίρνει την μορφή $\dfrac{\nu \cdot (\nu+1)}{2}$.

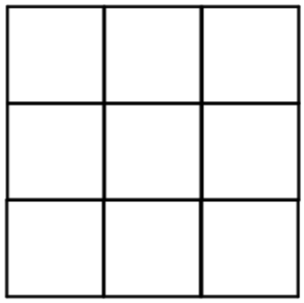
Τελικά ο όγκος της τριπλής αυτής δομής θα πρέπει να είναι: $\nu \cdot (\nu+1)^2 - \dfrac{\nu \cdot (\nu+1)}{2}$, το οποίο συνεπάγεται ότι το τριπλάσιο του πεντάεδρου αριθμού (ρ) θα είναι: $3\rho = \nu \cdot (\nu+1)^2 - \dfrac{\nu \cdot (\nu+1)}{2}$.

Πόρισμα: Το άθροισμα $\sum_{x=1}^{\nu} x^2$ ισούται με $\dfrac{\nu \cdot (\nu+1) \cdot (2\nu+1)}{6}$ για κάθε $\nu \in \mathbb{N}$.
Πράγματι, από το πρώτο σχήμα βλέπουμε ότι κάθε πεντάεδρος αριθμός είναι της μορφής $\rho = 1^2 + 2^2 + 3^2 + \cdots + \nu^2$ και επίσης αποδείξαμε ότι $3\rho = \nu \cdot (\nu+1)^2 - \dfrac{\nu \cdot (\nu+1)}{2}$. Οπότε, $1^2 + 2^2 + 3^2 + \cdots + \nu^2 = \rho = \dfrac{1}{3} \cdot \left(\nu \cdot (\nu+1)^2 - \dfrac{\nu \cdot (\nu+1)}{2} \right) =$

$$\frac{1}{3}\cdot\nu\cdot(\nu+1)\cdot\left(\nu+1-\frac{1}{2}\right)=\frac{\nu\cdot(\nu+1)\cdot(2\nu+1)}{6}.$$

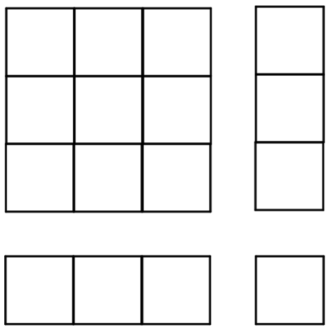
5.3 Τέλεια τετράγωνα

Τέλεια τετράγωνα θα ονομάζονται οι αριθμοί αυτοί $\alpha \in \mathbb{N}$ οι οποίοι μπορούν να γραφούν ως $\alpha = \nu^2$ για κάποιον $\nu \in \mathbb{N}$. Γεωμετρικά, για κάθε τέλειο τετράγωνο θα υπάρχει φυσικός ν τέτοιος ώστε το τέλειο τετράγωνο να είναι το εμβαδόν τετραγώνου πλευράς ν.



Σχήμα 5.10

Θα επιχειρήσουμε να προσδιορίσουμε μια εναλλακτική αλγεβρική μορφή (εκτός του ν^2 βέβαια) που παίρνουν τα τέλεια τετράγωνα. Για να καταφέρουμε κάτι τέτοιο θα ακολουθήσουμε μια διαδικασία πιο έμμεση. Συγκεκριμένα θα δούμε πως έχοντας ένα τέλειο τετράγωνο μπορούμε να κατασκευάσουμε το αμέσως μεγαλύτερο τέλειο τετράγωνο.



Σχήμα 5.11

Ας υποθέσουμε ότι ν^2 είναι ένα τέλειο τετράγωνο που αναπαρίσταται ως τετράγωνο πλευράς ν. Για να κατασκευάσουμε το αμέσως μεγαλύτερο τέλειο τετράγωνο

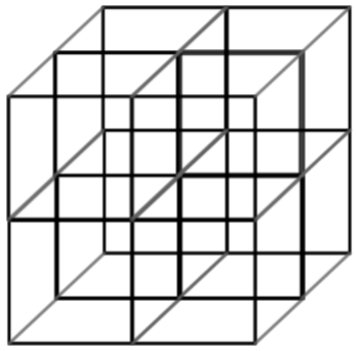
(το $(\nu+1)^2$) θα πρέπει να προσθέσουμε κατάλληλο αριθμό μοναδιαίων τετραγώνων έτσι ώστε να κατασκευάσουμε τετράγωνο πλευράς $\nu+1$. Αυτό το κάνουμε προθέτοντας δύο ορθογώνια παραλληλόγραμμα $\nu \cdot 1$ εφαπτόμενα στις πλευρές του τετραγώνου, το ένα στην μια πλευρά του και το άλλο σε μία κάθετή της και επίσης ένα μοναδιαίο τετράγωνο που να εφάπτεται και στα δύο προηγούμενα ορθογώνια παραλληλόγραμμα (προφανώς, τα σχήματά μας δεν θα πρέπει να επικαλύπτονται).

Οπότε, επειδή το 1 είναι τέλειο τετράγωνο, για να κατασκευάσουμε το ν^2 εφαρμόζουμε στο μοναδιαίο τετράγωνο την παραπάνω διαδικασία $\nu-1$ φορές και παίρνουμε: $\nu^2 = 1 + (2 \cdot 1 + 1) + (2 \cdot 2 + 1) + (2 \cdot 3 + 1) + \cdots + (2 \cdot (\nu-1) + 1)$.

Τελικά κάθε τέλειο τετράγωνο παίρνει την μορφή: $\nu^2 = \sum_{x=0}^{\nu-1} (2x+1)$

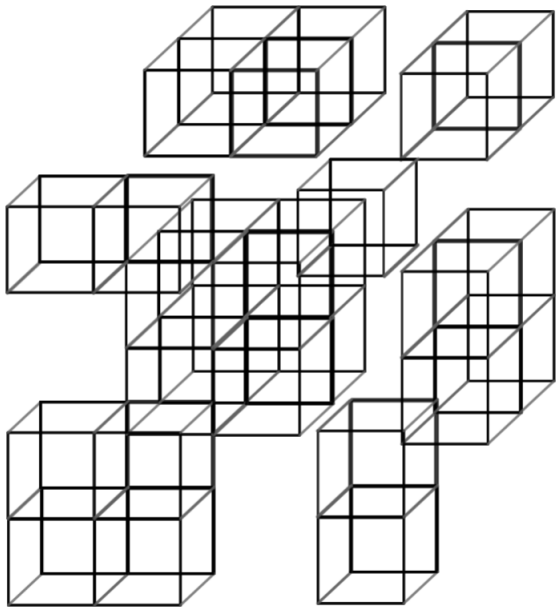
5.4 Τέλειοι κύβοι

Τέλειοι κύβοι θα ονομάζονται οι αριθμοί αυτοί $\alpha \in \mathbb{N}$ οι οποίοι μπορούν να γραφούν ως $\alpha = \nu^3$ για κάποιον $\nu \in \mathbb{N}$. Γεωμετρικά, για κάθε τέλειο κύβο θα υπάρχει φυσικός ν τέτοιος ώστε ο τέλειος κύβος να είναι ο όγκος κύβου πλευράς ν.



Σχήμα 5.12

Και πάλι θα επιχειρήσουμε να προσδιορίσουμε μια εναλλακτική αλγεβρική μορφή (εκτός του ν^3 βέβαια) που παίρνουν οι τέλειοι κύβοι. Για να καταφέρουμε κάτι τέτοιο θα ακολουθήσουμε μια διαδικασία πιο έμμεση, ανάλογη αυτής των τέλειων τετραγώνων. Συγκεκριμένα θα δούμε πως έχοντας έναν τέλειο κύβο, μπορούμε να κατασκευάσουμε τον αμέσως μεγαλύτερο τέλειο κύβο.



Σχήμα 5.13

Ας υποθέσουμε ότι ν^3 είναι ένας τέλειος κύβος που αναπαρίσταται ως κύβος πλευράς ν. Για να κατασκευάσουμε τον αμέσως μεγαλύτερο τέλειο κύβο (το $(\nu+1)^3$) θα πρέπει να προσθέσουμε κατάλληλο αριθμό μοναδιαίων κύβων έτσι ώστε να κατασκευάσουμε κύβο πλευράς $\nu+1$. Αυτό το κάνουμε (όπως στο σχήμα) ως εξής: Διαλέγουμε 3 έδρες με κοινή κορυφή και εφαπτόμενα σε αυτές τοποθετούμε (3) παραλληλεπίπεδα $\nu \cdot \nu \cdot 1$. Προσθέτουμε επίσης εφαπτόμενα στις μικρές έδρες των παραλληλεπιπέδων, (3) παραλληλεπίπεδα $\nu \cdot 1 \cdot 1$. Τέλος, εφαπτόμενα στα τελευταία παραλληλεπίπεδα, προσθέτουμε μοναδιαίο κύβο. Με αυτόν τον τρόπο δημιουργείται κύβος πλευράς $\nu+1$.

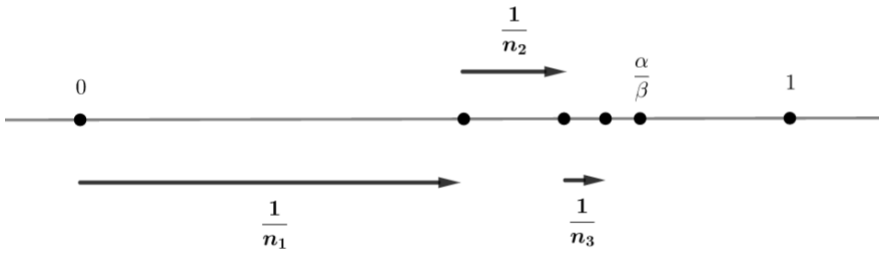
Επειδή το 1 είναι τέλειος κύβος, για να κατασκευάσουμε το ν^3 εφαρμόζουμε στον μοναδιαίο κύβο την παραπάνω διαδικασία $\nu-1$ φορές, και παίρνουμε: $\nu^3 = 1+(3\cdot 1^2+3\cdot 1+1)+(3\cdot 2^2+3\cdot 2+1)+\cdots+(3\cdot(\nu-1)^2+3\cdot(\nu-1)+1)$.

Τελικά, κάθε τέλειος κύβος παίρνει την μορφή: $\nu^3 = \sum_{x=0}^{\nu-1}(3x^2+3x+1)$

5.5 Αιγυπτιακά κλάσματα

Στην αρχαία Αίγυπτο ήταν γνωστοί οι αντίστροφοι των φυσικών αριθμών. Για τις εμπορικές συναλλαγές (συνήθως) οι αρχαίοι Αιγύπτιοι έκαναν τους υπολογισμούς τους - και συγκεκριμένα τις διαιρέσεις τους - γράφοντας τα κλάσματα ως άθροισμα αντιστρόφων φυσικών αριθμών. Αυτό βοηθούσε διότι κλάσματα όπως το: $\frac{9}{14}$ παίρνουν μια πολύ απλούστερη μορφή, που βοηθάει στο μοίρασμα· εν προκειμένω: $\frac{9}{14} = \frac{1}{2} + \frac{1}{7}$. Οπότε, προβλήματα όπως αυτό του *Rhind*, όπου ζητείται να μοιραστούν 6 φρατζόλες ψωμί σε 10 άνδρες, μπορούν να λυθούν εύκολα παρατηρώντας ότι $\frac{6}{10} = \frac{12}{20} = \frac{1}{2} + \frac{1}{10}$.

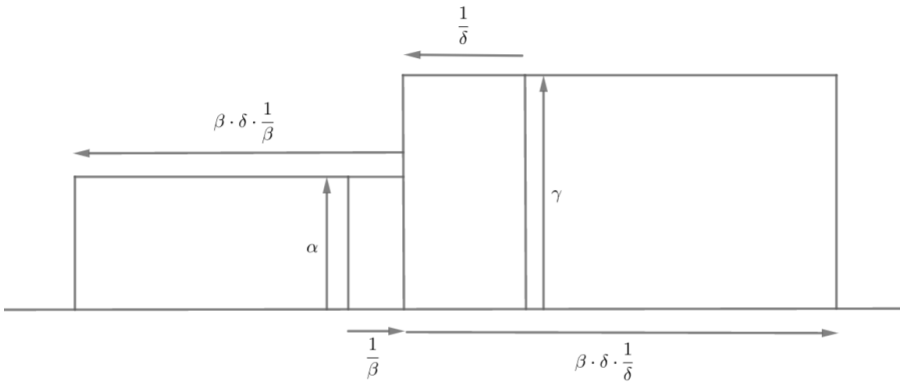
Οι αρχαίοι Αιγύπτιοι κατάφερναν και έκαναν εύκολα υπολογισμούς χρησιμοποιώντας αυτό το σπάσιμο των κλασμάτων, δεν απέδειξαν όμως ότι κάτι τέτοιο μπορεί να γίνεται πάντα, μιας και τα Μαθηματικά της εποχής βασίζοταν περισσότερο στην παρατήρηση και όχι στην απόδειξη ή διατύπωση θεωρημάτων. Εμείς θα επιχειρήσουμε να δείξουμε ότι ένα τέτοιο σπάσιμο μπορεί πάντα να γίνεται, για κάθε ρητό $\frac{\alpha}{\beta} < 1$.



Σχήμα 5.14

Θεωρούμε $\frac{1}{n_1}$ τον μέγιστο αντίστροφο για τον οποίο συμβαίνει: $\frac{1}{n_1} \leq \frac{\alpha}{\beta} < \frac{1}{n_1 - 1}$. Λέμε ότι ο αριθμητής της ρητής διαφοράς $\frac{\alpha}{\beta} - \frac{1}{n_1}$ θα είναι μικρότερος του α.

Πράγματι, αποδεικνύοντας την επόμενη πρόταση, θα δείξουμε το ζητούμενο:



Σχήμα 5.15

Έστω οι ρητοί $\frac{\alpha}{\beta}, \frac{\gamma}{\delta}$. Ισχύει ότι $\frac{\alpha}{\beta} + \frac{\gamma}{\delta} = \frac{\alpha\delta + \beta\gamma}{\beta\delta}$ και $\frac{\alpha}{\beta} - \frac{\gamma}{\delta} = \frac{\alpha\delta - \beta\gamma}{\beta\delta}$.

Κατασκευάζουμε παραλληλόγραμμα πλευρών $\alpha, \frac{1}{\beta}$ και $\gamma, \frac{1}{\delta}$, όπως στο σχήμα, με εμβαδά $\frac{\alpha}{\beta}$ και $\frac{\gamma}{\delta}$ αντίστοιχα. Την δομή των 2 παραλληλογράμμων την πολλαπλασιάζουμε β φορές και απομονώνουμε τα παραλληλόγραμμα εμβαδού $\frac{\alpha}{\beta}$ από τα υπόλοιπα. Το σύνολο των εμβαδών των παραλληλογράμμων εμβαδού $\frac{\alpha}{\beta}$ κατασκευάζει παραλληλόγραμμο εμβαδού α και τα υπόλοιπα κατασκευάζουν παραλληλόγραμμο εμβαδού $\frac{\beta\gamma}{\delta}$. Την νέα δομή των παραλληλογράμμων την πολλαπλασιάζουμε δ φορές και απομονώνουμε τα παραλληλόγραμμα εμβαδού $\frac{\beta\gamma}{\delta}$. Το σύνολο των εμβαδών των παραλληλογράμμων εμβαδού $\frac{\beta\gamma}{\delta}$ κατασκευάζει παραλληλόγραμμο εμβαδού $\beta\gamma$ και τα υπόλοιπα κατασκευάζουν παραλληλόγραμμο εμβαδού $\alpha\delta$. Εδώ σταματούμε καθώς τα εμβαδά έχουν πλέον μορφή ακέραιη και συνεπώς η πρόσθεση είναι διαδικασία τετριμμένη.

Επειδή πολλαπλασιάσαμε την δομή β και έπειτα δ φορές, έχουμε: $\beta \cdot \delta \left(\frac{\alpha}{\beta} + \frac{\gamma}{\delta} \right) = \alpha \cdot \delta + \beta \cdot \gamma$, απ΄ όπου προκύπτει το ζητούμενο.

Η αφαίρεση γίνεται με διαδικασία ανάλογη.

Οπότε από το αποτέλεσμα της πρότασης αυτής προκύπτει ότι $\frac{\alpha}{\beta} - \frac{1}{n_1}$ έχει αριθμητή $\alpha \cdot n_1 - \beta$. Επειδή όμως $\frac{\alpha}{\beta} < \frac{1}{n_1 - 1}$, έχουμε: $\frac{\alpha \cdot n_1 - \alpha - \beta}{\beta \cdot (n_1 - 1)} < 0 \Rightarrow \alpha \cdot n_1 - \beta - \alpha < 0 \Rightarrow \alpha \cdot n_1 - \beta < \alpha$.

Στην συνέχεια θεωρούμε τον μέγιστο αντίστροφο αυτόν για τον οποίον ισχύει $\frac{1}{n_2} \leq \frac{\alpha}{\beta} - \frac{1}{n_1} < \frac{1}{n_2 - 1}$. Όπως προηγουμένως, ο αριθμητής του $\frac{\alpha}{\beta} - \frac{1}{n_1} - \frac{1}{n_2}$ θα είναι μικρότερος από τον αριθμητή του $\frac{\alpha}{\beta} - \frac{1}{n_1}$. Οπότε, εάν $A(x)$ είναι ο αριθμητής του ρητού x, τότε έχουμε: $\alpha = A\Big(\frac{\alpha}{\beta}\Big) < A\Big(\frac{\alpha}{\beta} - \frac{1}{n_1}\Big) < A\Big(\frac{\alpha}{\beta} - \frac{1}{n_1} - \frac{1}{n_2}\Big) < A\Big(\frac{\alpha}{\beta} - \frac{1}{n_1} - \frac{1}{n_2} - \frac{1}{n_3}\Big) < \cdots < \frac{\alpha}{\beta} - \sum_{x=1}^{\nu} \frac{1}{n_x}$.

Επειδή δεν υπάρχουν άπειροι φυσικοί αριθμοί μικρότεροι του α, δύο περιπτώσεις μπορούν να ισχύουν:

1. Φτάνουμε σε αριθμό $\frac{\alpha}{\beta} - \sum_{x=1}^{\nu} \frac{1}{n_x}$ με αριθμητή 1.

2. Φτάνουμε σε αριθμό $\frac{\alpha}{\beta} - \sum_{x=1}^{\nu} \frac{1}{n_x}$ με αριθμητή $k > 1$ που δεν μπορεί να αναλυθεί σε άθροισμα αντιστρόφων.

Το 2. δεν μπορεί ισχύει, καθώς εάν το εν λόγω κλάσμα είναι $\frac{k}{m}$, τότε $\frac{1}{\lceil \frac{m}{k} \rceil} \leq \frac{k}{m} < \frac{1}{\lceil \frac{m}{k} \rceil - 1}$ και, συνεπώς, μπορεί να εφαρμοστεί η προηγούμενη διαδικασία, που, υπό την υπόθεση 2., θα πρέπει να καταλήξει ξανά σε ρητό που δεν γράφεται ως άθροισμα αντιστρόφων. Για αυτόν τον ρητό, όμως, μπορούμε να εφαρμόσουμε ξανά την ίδια διαδικασία. Συνεχίζοντας έτσι, παίρνουμε άθροισμα άπειρων κλασμάτων που ισούται του $\frac{\alpha}{\beta}$ με τους αριθμητές των κλασμάτων συνεχώς να φθίνουν, να είναι φυσικοί και μικρότεροι του α. Προφανώς κάτι τέτοιο είναι άτοπο.

Τελικά, ισχύει το 1. και κάθε ρητός $\frac{\alpha}{\beta}$ μπορεί να γραφεί ως: $\frac{\alpha}{\beta} = \sum_{x=1}^{\nu} \frac{1}{n_x}$ για κάποιο $\nu \in \mathbb{N}$ και $n_x \in \mathbb{N}$.

Κεφάλαιο 6

Στοιχεία από τον απειροστικό λογισμό

6.1 Αρχή της άπειρης καθόδου

Στο προηγούμενο κεφάλαιο, στα Αιγυπτιακά κλάσματα, αναφέραμε ότι οι φυσικοί αριθμοί που είναι μικρότεροι ενός $\alpha \in \mathbb{N}$ είναι πεπερασμένοι στο πλήθος. Αυτό είναι αποτέλεσμα των ισοδύναμων αρχών του ελαχίστου και της άπειρης καθόδου.

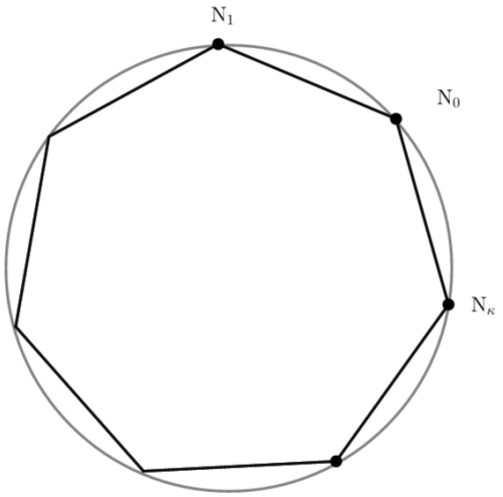
Σύμφωνα με την αρχή ελαχίστου, κάθε υποσύνολο των φυσικών αριθμών έχει ελάχιστο.

Σύμφωνα με την αρχή της άπειρης καθόδου, δεν υπάρχει γνησίως φθίνουσα ακολουθία φυσικών αριθμών.

Δείχνουμε ότι πράγματι αυτές οι προτάσεις είναι ισοδύναμες:

1. Ισχύει: αρχή ελαχίστου $\Rightarrow$ αρχή άπειρης καθόδου:

Θεωρούμε το σύνολο $A = \{\nu_i | i \in [0, \kappa] \cap \mathbb{Z}\} \subset \mathbb{N}$ με $\nu_i < \nu_j, \forall i < j$. Θα αναπαραστήσουμε τα στοιχεία αυτού του συνόλου ως σημεία (της οικογένειας N_i και $\nu_i \to N_i$) με κατεύθυνση αριστερόστροφη στην περιφέρεια ενός κύκλου. Ας υποθέσουμε επίσης ότι υπάρχει γνησίως φθίνουσα ακολουθία α_i στοιχείων του A. Η ακολουθία αυτή θα ξεκινάει από έναν αριθμό ν_j του A και, ως φθίνουσα, θα συνεχίσει σε αριθμό $\nu_i < \nu_j$. Στον κύκλο η ακολουθία θα αναπαρίσταται ως μια γραμμή εντός του, από ευθύγραμμα τμήματα που ενώνουν σημεία τα οποία αντιστοιχούν σε διαδοχικές τιμές της ακολουθίας, ενώ ταυτόχρονα η ίδια η γραμμή θα ξεκινάει από ένα N_j και συνεχίζοντας δεξιόστροφα θα περνά από το N_0, το οποίο θα αντιστοιχεί στο ελάχιστο στοιχείο του A.

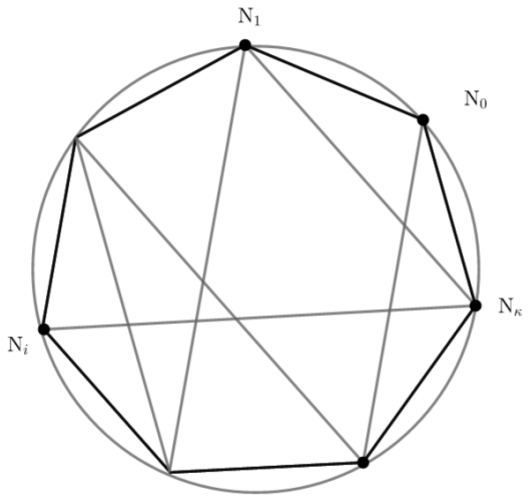


Σχήμα 6.1

Εάν η ακολουθία είναι γνησίως φθίνουσα, η διαδρομή μετά του N_0 θα συνεχίζει σε σημείο N_τ με N_τ να είναι δεξιότερα του N_0 και να μην ταυτίζεται αυτού, αφού όσο κινούμαστε προς τα αριστερά οι αριθμοί μεγαλώνουν· επειδή επίσης N_0 ελάχιστο, το N_τ αριστερότερα του N_0. Από αυτό παίρνουμε το άτοπο και συνεπώς το ζητούμενο.

2. Ισχύει: αρχή άπειρης καθόδου $\Rightarrow$ αρχή ελαχίστου:

Εδώ ας θεωρήσουμε το σύνολο $A = \{\nu_i | i \in [0, \kappa] \cap \mathbb{Z}\} \subset \mathbb{N}$, όπως προηγουμένως, του οποίου τα στοιχεία αναπαριστούμε ως σημεία (της οικογένειας N_i και $\nu_i \to N_i$) με κατεύθυνση αριστερόστροφη στην περιφέρεια ενός κύκλου. Επίσης ας θεωρήσουμε την φθίνουσα ακολουθία $(\nu_p, \nu_r, \ldots, \nu_q)$, η οποία αναπαρίσταται ως γραμμή ευθυγράμμων τμημάτων εντός του κύκλου μας. Επειδή ισχύει η αρχή της άπειρης καθόδου, η γραμμή έχει τέλος σε κάποιο N_i. Επειδή η ακολουθία είναι φθίνουσα και η γραμμή περνά από όλα τα N_j που αντιστοιχούν στα στοιχεία του A, το ν_i θα είναι το ελάχιστο του A.

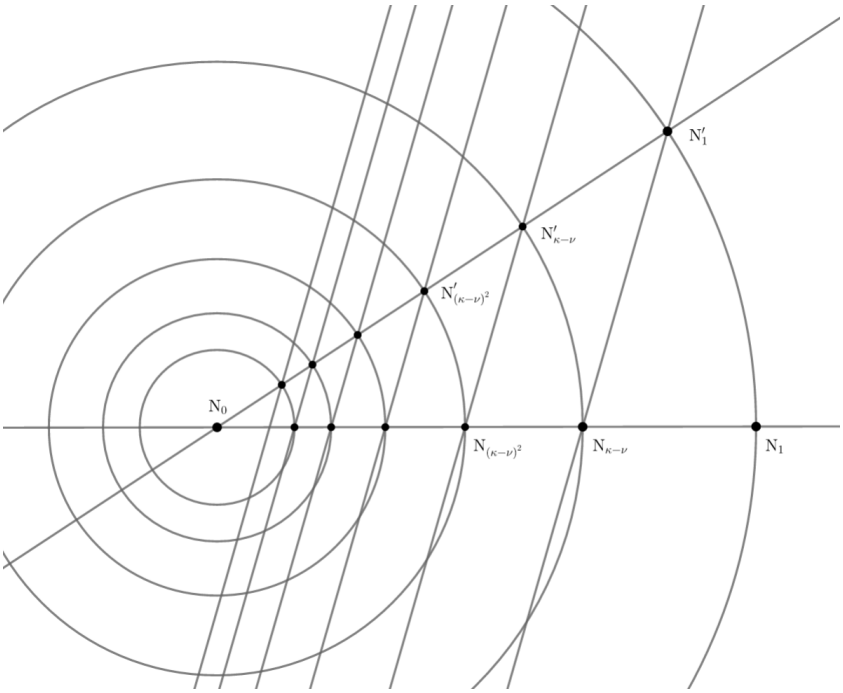


Σχήμα 6.2

Οπότε καταλήγουμε στο συμπέρασμα ότι οι 2 αυτές αρχές είναι ισοδύναμες. Εμείς για τους υπολογισμούς μας και για τις αποδείξεις μας συνήθως θα χρησιμοποιούμε την αρχή της άπειρης καθόδου, μιας και γεωμετρικά βολεύει περισσότερο.

Πόρισμα: Μεταξύ 2 φυσικών αριθμών που απέχουν μονάδα, δεν υπάρχει τρίτος.

Πράγματι, ας υποθέσουμε $\nu < \kappa < \nu + 1$ φυσικοί αριθμοί. Επειδή κ, ν φυσικοί, ο αριθμός $\kappa - \nu$ είναι φυσικός. Μάλιστα, από την προηγούμενη ανισότητα, $0 < \kappa - \nu < 1$. Θεωρούμε σημείο N_0 και ευθεία ε που διέρχεται του N_0. Επίσης θεωρούμε $\zeta \nparallel \varepsilon$ που διέρχεται από το N_0 και έναν κύκλο $(N_0, 1)$ που τέμνει τις ε, ζ στα N_1 και N_1' αντίστοιχα. Πάνω στην ε θεωρούμε $N_{\kappa-\nu}$ τέτοιο ώστε το τμήμα $N_0N_{\kappa-\nu}$ να αντιστοιχεί στο $\kappa - \nu$. Έπειτα φέρουμε κύκλο $(N_0, N_0N_{\kappa-\nu})$ που τέμνει την ζ στο $N'_{\kappa-\nu}$. Από τα $N_{\kappa-\nu}$ και N_1 φέρουμε ευθεία η_1 και σε αυτήν παράλληλη η_2 που διέρχεται από το $N'_{\kappa-\nu}$ και τέμνει την ε στο $N_{(\kappa-\nu)^2}$. Όπως είπαμε στο 3^o κεφάλαιο, το τμήμα $N_0N_{(\kappa-\nu)^2}$ θα αντιστοιχεί στο $N_0N_{(\kappa-\nu)^2} = N_0N_{(\kappa-\nu)} \cdot N_0N'_{(\kappa-\nu)} = (\kappa - \nu) \cdot (\kappa - \nu) = (\kappa - \nu)^2$.



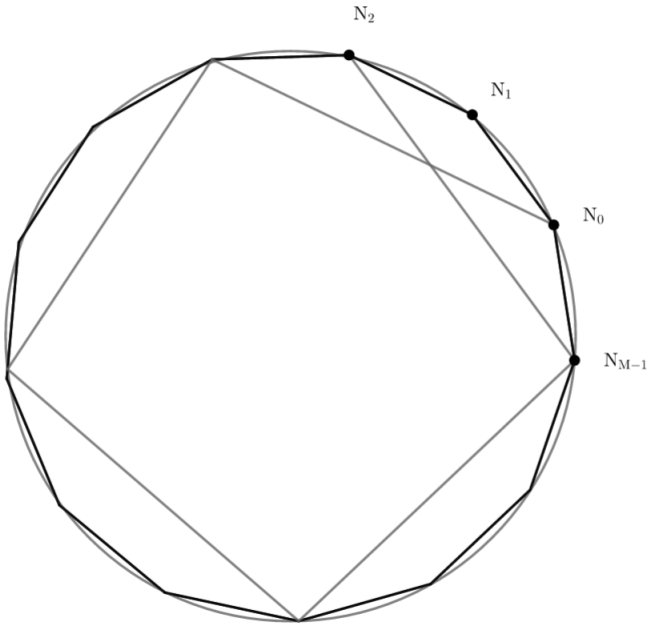
Σχήμα 6.3

Προφανώς, τα τρίγωνα $\overset{\triangle}{N_1'N_{\kappa-\nu}N_0}$ και $\overset{\triangle}{N'_{\kappa-\nu}N_{(\kappa-\nu)^2}N_0}$ είναι όμοια αφού έχουν όλες τους τις πλευρές παράλληλες. Οπότε, επειδή $N_0N_1' = N_0N_1 > N_0N_{\kappa-\nu}$, έχουμε $N_0N'_{\kappa-\nu} = N_0N_{\kappa-\nu} > N_0N(\kappa - \nu)^2$. Συνεχίζοντας με τον ίδιο τρόπο, παίρνουμε την άπειρη ακολουθία φυσικών αριθμών: $N_0N_1 > N_0N_{\kappa-\nu} > N_0N_{(\kappa-\nu)^2} > \cdots > N_0N_{(\kappa-\nu)^n} > \ldots$, το οποίο είναι άτοπο. Από αυτό παίρνουμε το ζητούμενο.

6.2 Αρχιμήδεια ιδιότητα

Σύμφωνα με την Αρχιμήδεια ιδιότητα για κάθε 2 φυσικούς αριθμούς M και Λ υπάρχει ένας $\kappa \in \mathbb{N}$ τέτοιος ώστε, για $\Lambda < M$ να ισχύει: $\kappa \cdot \Lambda > M$.

Εδώ θα αναπαραστήσουμε τους φυσικούς αριθμούς έως το M ως σημεία στην περιφέρεια ενός κύκλου, αριθμώντας αριστερόστροφα και ξεκινώντας από σημείο N_0.



Σχήμα 6.4

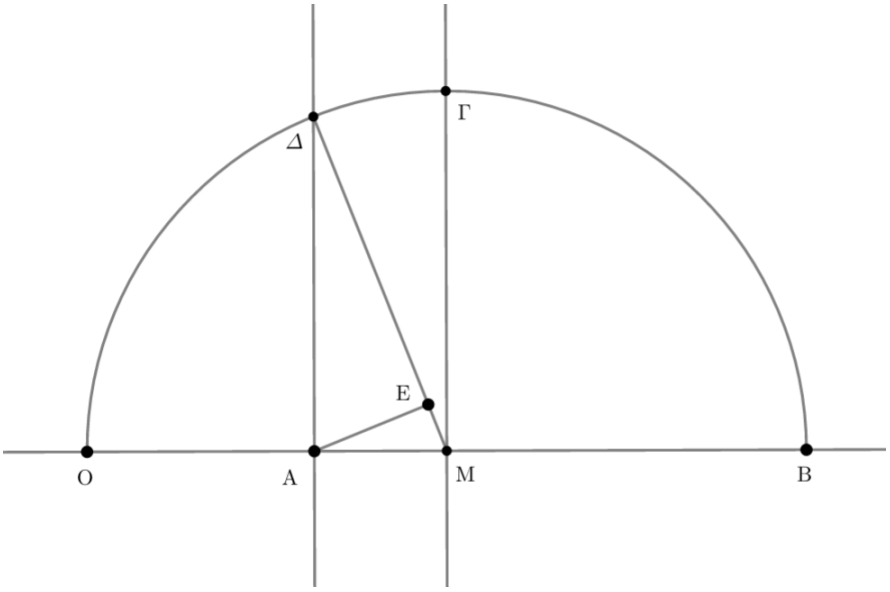
Στην συνέχεια κατασκευάζουμε την ακολουθία $(\Lambda, 2\Lambda, 3\Lambda, \dots)$ η οποία απεικονίζεται εντός του κύκλου ως γραμμή ευθυγράμμων τμημάτων. Υποθέτουμε ότι δεν περνά ποτέ το N_{M-1}, που αντιστοιχεί στο M. Επειδή η μέγιστη γραμμή τέτοιου είδους που μπορεί να επιτευχθεί στον κύκλο είναι αυτή που ξεκινά από το N_0 και, προχωρώντας ανά 1 σημείο την φορά, φθάνει στο N_{M-1} (δηλαδή, είναι το πολύγωνο $N_0N_1N_2 \dots N_{M-1}$ εκτός του ευθυγράμμου τμήματος N_0N_{M-1}), η προαναφερθήσα ακολουθία δεν μπορεί να έχει παραπάνω από $M+1$ πρώτες τιμές της μικρότερες του M (η αιτιολόγιση μπορεί να γίνει χρησιμοποιώντας το ότι η συντομότερη διαδρομή μεταξύ 2 σημείων είναι ευθύγραμμο τμήμα). Με αυτό δείχνουμε το ζητούμενο. Αλλιώς, θα μπορούσαμε να αντιστοιχίσουμε τα N_i στα $M - i\Lambda$. Έτσι η γραμμή μας θα αντιστοιχούσε σε γνησίως φθίνουσα ακολουθία, που είναι άτοπο.

6.3 Αρμονικός - Γεωμετρικός - Αριθμητικός Μέσος

Η έννοια του μέσου όρου είναι ίσως το χρησιμότερο μέτρο της στατιστικής. Δείχνοντας την σχετική θέση όσων αριθμών εξετάζονται, μπορεί και επάγει μια γενίκευση στους υπολογισμούς που είναι, συνήθως, αρκετά αντιπροσωπευτική του δείγματος.

Εμείς θα μελετήσουμε 3 διαφορετικά είδη μέσων όρων 2 αριθμών $\alpha, \beta \in \mathbb{R}_+^*$:

1. Ο αριθμητικός μέσος όρος των α, β ορίζεται ως: $\bar{A} = \dfrac{\alpha+\beta}{2}$.
2. Ο γεωμετρικός μέσος όρος των α, β ορίζεται ως: $\bar{\Gamma} = \sqrt{\alpha \cdot \beta}$.
3. Ο αρμονικός μέσος όρος των α, β ορίζεται ως: $\bar{H} = \dfrac{2}{\frac{1}{\alpha}+\frac{1}{\beta}}$.



Σχήμα 6.5

Για την γεωμετρική αναπαράσταση των $3^{\omega\nu}$ αυτών μέσων, θεωρούμε O, A, B επί ευθείας ε, με το OA να αντιστοιχεί στο α και το AB στο β. Στην συνέχεια κατασκευάζουμε ημικύκλιο διαμέτρου $\alpha+\beta$ που να διέρχεται από τα O, B και έχει κέντρο το M. Η ακτίνα του ημικυκλίου αυτού θα είναι $\dfrac{\alpha+\beta}{2}$, δηλαδή ο αριθμητικός μέσος. Έπειτα, φέρουμε από το A κάθετο προς την ε που τέμνει το ημικύκλιο στο Δ. Τα τρίγωνα $O\overset{\triangle}{\Delta}A$ και $A\overset{\triangle}{\Delta}B$ είναι όμοια, αφού είναι και τα 2

ορθογώνια και επίσης $\widehat{O\Delta A} = \pi - \frac{\pi}{2} - \widehat{\Delta OA} = \widehat{OB\Delta}$. Από αυτό παίρνουμε: $\frac{A\Delta}{OA} = \frac{AB}{A\Delta} \Rightarrow A\Delta = \sqrt{OA \cdot AB} = \sqrt{\alpha \cdot \beta}$, δηλαδή, το $A\Delta$ είναι ο γεωμετρικός μέσος των α, β. Τέλος από το A φέρνουμε κάθετη προς την $M\Delta$, που την τέμνει στο E. Η $M\Delta$ αποτελεί ακτίνα του ημικυκλίου, οπότε ισούται με $\frac{\alpha+\beta}{2}$. Τα τρίγωνα $\overset{\triangle}{AM}\Delta$ και $\overset{\triangle}{AE}\Delta$ είναι όμοια, αφού είναι και τα 2 ορθογώνια και $\widehat{A\Delta M}$ είναι κοινή γωνία. Οπότε, $\frac{A\Delta}{M\Delta} = \frac{\Delta E}{A\Delta} \Rightarrow \Delta E = \frac{A\Delta^2}{M\Delta} = \frac{\alpha\beta}{\frac{\alpha+\beta}{2}} = \frac{2}{\frac{1}{\alpha}+\frac{1}{\beta}}$, δηλαδή η ΔE είναι ο αρμονικός μέσος των α, β.

Πρόταση: Για κάθε $\alpha, \beta \in \mathbb{R}_+^*$ ισχύει: $\frac{2}{\frac{1}{\alpha}+\frac{1}{\beta}} \leq \sqrt{\alpha \cdot \beta} \leq \frac{\alpha+\beta}{2}$.

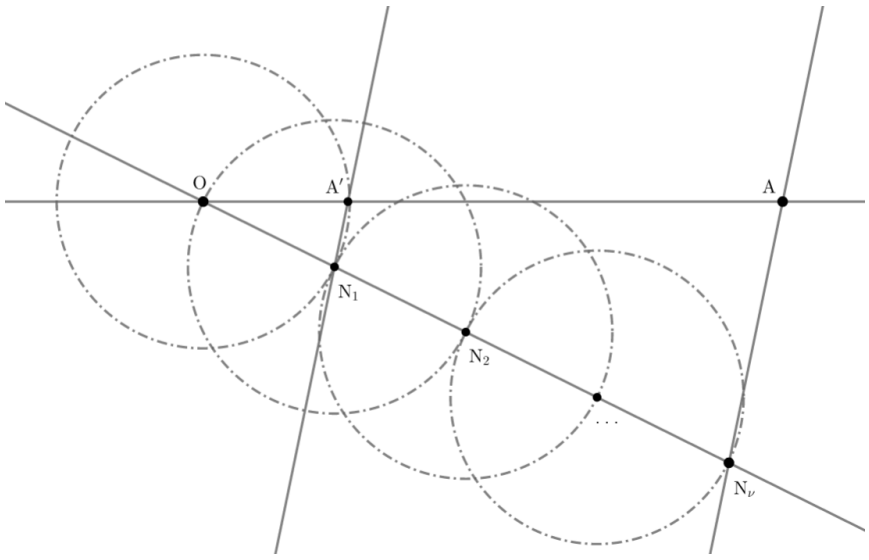
Πράγματι, στο ορθογώνιο τρίγωνο $\overset{\triangle}{AM}\Delta$ η $M\Delta$ είναι υποτείνουσα και η $A\Delta$ κάθετη, οπότε: $A\Delta \leq M\Delta$. Επίσης, στο ορθογώνιο τρίγωνο $\overset{\triangle}{AE}\Delta$ η $A\Delta$ είναι υποτείνουσα και η ΔE κάθετη, οπότε $\Delta E \leq A\Delta$. Συνδυάζοντας αυτές τις 2 ανισότητες παίρνουμε: $\Delta E \leq A\Delta \leq M\Delta \Rightarrow \frac{2}{\frac{1}{\alpha}+\frac{1}{\beta}} \leq \sqrt{\alpha \cdot \beta} \leq \frac{\alpha+\beta}{2}$.

Κεφάλαιο 7

Το σύνολο των πρώτων αριθμών

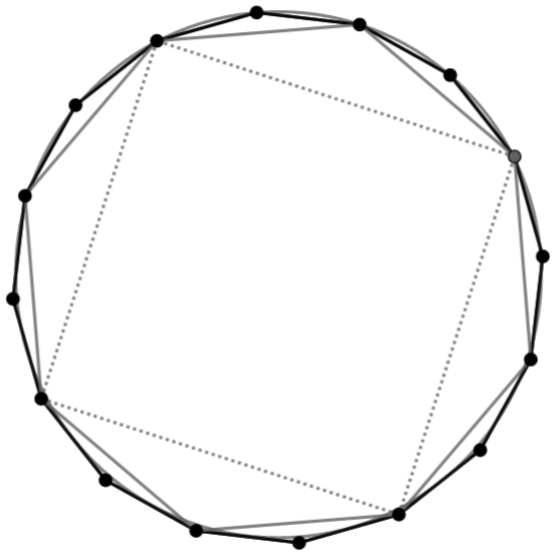
7.1 Γενικά

Γενικά για τους πρώτους αριθμούς, πρώτοι αριθμοί θα ονομάζονται οι αριθμοί εκείνοι α για τους οποίους δεν υπάρχει φυσικός $1 < \nu < \alpha$ τέτοιος ώστε να τους διαιρεί σε φυσικούς αριθμούς. Γεωμετρικά και χρησιμοποιώντας την γραμμική αναπαράσταση των αριθμών, η διαίρεση του $OA = \alpha$ με οποιοδήποτε $\nu \in \mathbb{N} - \{1\}$ δίδει τμήμα $OA' = \dfrac{OA}{\nu}$ που δεν σύγκειται από μονάδες.

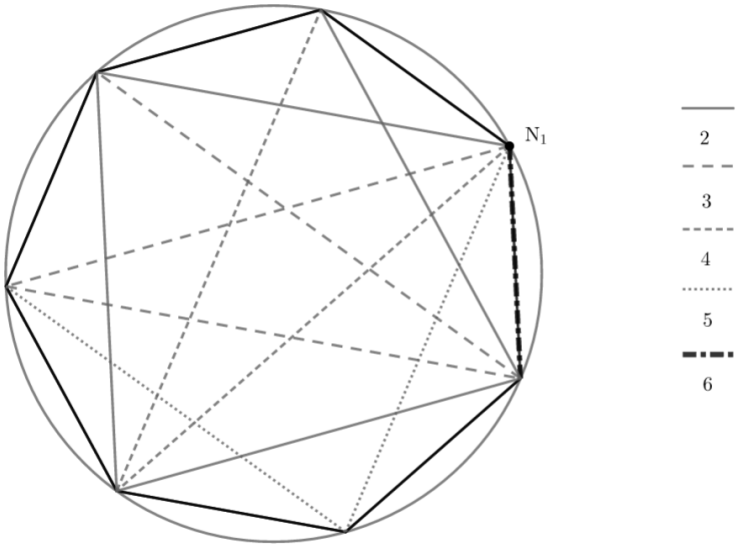


Σχήμα 7.1

Χρησιμοποιώντας την κυκλική αναπαράσταση των αριθμών, ας θεωρήσουμε κύκλο με α σημεία στην περιφέρειά του $N_i, i \in [1, \alpha] \cap \mathbb{N}$ (τα $\widehat{N_iN_{i+1}} = \widehat{N_{i+1}N_{i+2}}$). Στον κύκλο προχωρούμε ανά ν σημεία (με βήμα ν) και κατασκευάζουμε μια διαδρομή από ευθύγραμμα τμήματα. Εάν η διαδρομή δημιουργεί κανονικό πολύγωνο, δηλαδή ξεκινά από ένα σημείο και τελειώνει στο ίδιο χωρίς να περάσει πέρα από αυτό το σημείο έστω και 1 φορά (κανονικό και όχι αστρικό πολύγωνο), τότε το ν διαιρεί τον α σε αριθμό φυσικό. Διαφορετικά, ο ν δεν διαιρεί τον α. Εάν, λοιπόν, για οποιαδήποτε διαδρομή βήματος ν δεν κατασκευάζεται κανονικό πολύγωνο, ο αριθμός α είναι πρώτος.



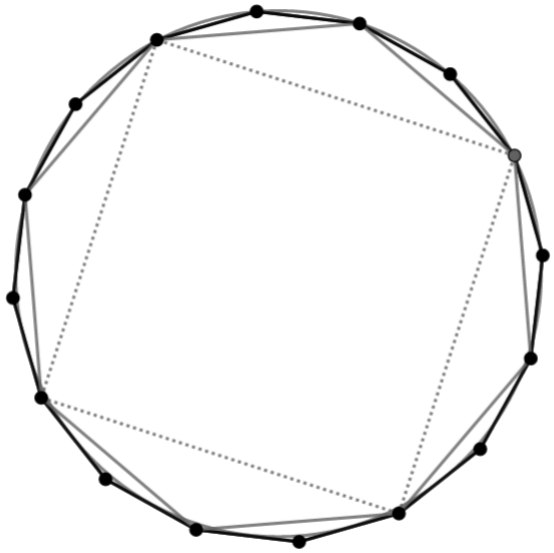
Σχήμα 7.2: *Η διαίρεση του* 16 *με το* 2 *και το* 4



Σχήμα 7.3: *Η περίπτωση του* 7 *όταν διαιρείται με φυσικούς μικρότερούς του, εκτός του* 1

7.2 Διαδρομές και πρώτοι αριθμοί

Από τον δεύτερο τρόπο αναπαράστασης των πρώτων αριθμών μπορούμε να παρατηρήσουμε ότι κάθε πολυγωνική διαδρομή εντός ενός κύκλου α σημείων αντιστοιχεί σε διαιρέτη του α. Συγκεκριμένα, το βήμα της διαδρομής θα είναι διαιρέτης του αριθμού α. Επίσης, εάν συνεχίσουμε να κατασκευάζουμε την πολυγωνική διαδρομή προχωρώντας ανά το βήμα της, η διαδρομή αυτή ποτέ της δεν θα περάσει από κάθε σημείο του κύκλου, διότι τα σημεία του κύκλου μεταξύ 2 διαδοχικών σημείων της διαδρομής δεν θα πιάνονται ποτέ. Αυτό συμβαίνει γιατί μετά από κάθε περιστροφή φτάνουμε να ξεκινούμε από το ίδιο σημείο από το οποίο ξεκινήσαμε· προχωρώντας με το ίδιο βήμα, η συνέχεια της διαδρομής ταυτίζεται με την διαδρομή προ της περιστροφής.

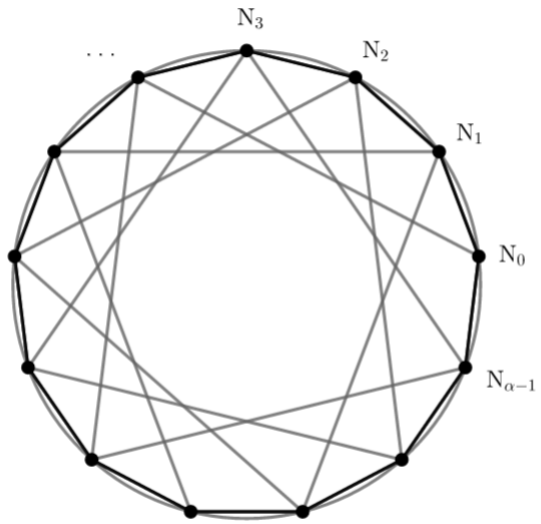


Σχήμα 7.4: *Η συνέχεια των πολυγωνικών διαδρομών με βήματα* 2 *ή* 4 *στον κύκλο* 16 *σημείων ταυτίζεται με την αρχική διαδρομή*

Όμως στην περιπτωση που δεν υπάρχουν διαιρέτες του πλήθους α των σημείων του κύκλου (δηλαδή το α είναι πρώτος) πολυγωνικές διαδρομές δεν δημιουργούνται. Οπότε υποψιαζόμαστε ότι, ίσως, αν συνεχίσουμε μια μη πολυγωνική διαδρομή βήματος ν στον κύκλο α σημείων, αυτή θα περνάει από κάθε σημείο του κύκλου. Γενικότερα, εάν δεν υπάρχει, εκτός του 1, κοινός διαιρέτης του βήματος ν της μη πολυγωνικής διαδρομής και του πλήθους α των σημείων, υποψιαζόμαστε ότι η συνέχεια της διαδρομής περνά από κάθε σημείο του κύκλου.

Πράγματι, αυτό συμβαίνει, όπως αποδεικνύουμε στην επόμενη πρόταση:

Πρόταση: Θεωρούμε κύκλο και στην περιφέρεια αυτού α στο πλήθος σημεία της οικογένειας N_i με $\widehat{N_iN_{i+1}} = \widehat{N_{i+1}N_{i+2}}$. Επίσης θεωρούμε την διαδρομή εντός του, βήματος ν. Εάν δεν υπάρχει, εκτός του 1, κοινός διαιρέτης του α και του ν, τότε η διαδρομή βήματος ν περνάει από κάθε N_i της περιφέρειας του κύκλου.



Σχήμα 7.5

Πράγματι, αποδεικνύουμε ότι η διαδρομή ξεκινώντας από το N_0 φθάνει στο N_1:

Λόγω της Αρχιμήδειας ιδιότητας, θα υπάρχει κ_1 τέτοιο ώστε $\kappa_1 \cdot \nu > \alpha$. Μάλιστα, για το ελάχιστο κ_1 για το οποίο ισχύει η προαναφερθήσα ανισότητα, το επόμενο αληθεύει: $\kappa_1 \cdot \nu = \alpha + \lambda_1$ με $0 < \lambda_1 < \nu$, καθώς αν $\lambda_1 > \nu$, τότε $\lambda_1 = \kappa_2 \cdot \nu + \lambda_2$ και συνεπώς $\kappa_1 \cdot \nu = \alpha + \kappa_2 \cdot \nu + \lambda_2 \Rightarrow (\kappa_1 - \kappa_2) \cdot \nu = \alpha + \lambda_2 \rightarrow$ Άτοπο διότι $\kappa_1 - \kappa_2 < \kappa_1$ και κ_1 είναι ελάχιστο. Το $\lambda_1 \neq \nu$, διότι αν $\lambda_1 = \nu$, $(\kappa_1 - 1) \cdot \nu = \alpha \Rightarrow$ ο ν διαιρεί τον α. Το $\lambda_1 \neq 0$ διότι αν $\lambda_1 = 0$, το ν διαιρεί τον α. Το γιατί το λ_1 είναι μη αρνητικό είναι προφανές. Οπότε, προχωρώντας κ_1 φορές με βήμα ν, φθάνουμε σε σημείο N_{λ_1} μεταξύ των N_0 και N_ν.

Εάν υποθέσουμε επίσης, ότι κ_2 είναι ο ελάχιστος φυσικός για τον οποίον ισχύει $\kappa_2 \cdot \lambda_1 > \alpha$, επαναλαμβάνοντας την προηγούμενη διαδρομή κ_2 φορές, παίρνουμε: $\kappa_2 \cdot \kappa_1 \cdot \nu = \kappa_2 \cdot \alpha + \kappa_2 \cdot \lambda_1 \Rightarrow \kappa_2 \cdot \kappa_1 \cdot \nu = \kappa_2 \cdot \alpha + \alpha + \lambda_2 \Rightarrow \kappa_2 \cdot \kappa_1 \cdot \nu = (\kappa_2 + 1) \cdot \alpha + \lambda_2$. Ισχυριζόμαστε ότι: $0 < \lambda_2 < \lambda_1$. Πράγματι, εάν $\lambda_2 > \lambda_1$, όπως προηγουμένως,

θα πρέπει να καταλήξουμε σε άτοπο. Εάν $\lambda_1 = \lambda_2$, τότε $(\kappa_2 - 1) \cdot \lambda_1 = \alpha \rightarrow$ το λ_1 διαιρεί τον α. Επιπροσθέτως, επειδή $\kappa_1 \cdot \nu = \alpha + \lambda_1$, $\kappa_2 \cdot \lambda_1 = \alpha + \lambda_2$ και $\lambda_1 = \lambda_2$, έχουμε: $\kappa_1 \cdot \nu = \kappa_2 \cdot \lambda_1 \Rightarrow \dfrac{\nu}{\kappa_2} = \dfrac{\lambda_1}{\kappa_1}$. Από αυτό συνάγουμε ότι, επειδή $\lambda_1 < \nu$, ισχύει $\nu = \varphi_1 \cdot \lambda_1$ και $\kappa_2 = \varphi_1 \cdot \kappa_1$. Έτσι, λ_1 διαιρεί τον $\nu \rightarrow$ ο λ_1 κοινός διαιρέτης των α και $\nu \rightarrow$ Άτοπο. Τέλος, το $\lambda_2 \neq 0$, καθώς αν $\lambda_2 = 0$, θα είχαμε $\kappa_2 \cdot \lambda_1 = \alpha$ και $\kappa_1 \cdot \nu = \alpha + \lambda_1$, από το οποίο προκύπτει $\kappa_1 \cdot \nu = (\kappa_2 + 1) \cdot \lambda_1 \Rightarrow \dfrac{\nu}{\kappa_2 + 1} = \dfrac{\lambda_1}{\kappa_1}$. Με συλλογισμούς παρόμοιους της περίπτωσης $\lambda_1 = \lambda_2$ καταλήγουμε σε άτοπο. Το ότι το λ_2 είναι μη αρνητικό είναι προφανές. Οπότε, η διαδρομή μας φθάνει σε σημείο N_{λ_2} μεταξύ των N_{λ_1} και N_0.

Συνεχίζοντας με ακριβώς ανάλογο τρόπο την διαδρομή, παίρνουμε:

1. λ_1 τέτοιο ώστε: $\kappa_1 \cdot \nu = \alpha + \lambda_1$
2. λ_2 τέτοιο ώστε: $\kappa_2 \cdot \kappa_1 \cdot \nu = (\kappa_2 + 1) \cdot \alpha + \lambda_2$ με $\lambda_2 < \lambda_1$
3. λ_3 τέτοιο ώστε: $\kappa_3 \cdot \kappa_2 \cdot \kappa_1 \cdot \nu = (\kappa_3 \cdot (\kappa_2 + 1) + 1) \cdot \alpha + \lambda_3$ με $\lambda_3 < \lambda_2$

... ...

n. λ_n τέτοιο ώστε: $\prod_{i=1}^{n} \kappa_i \cdot \nu = \Big(1 + \kappa_n \cdot \big(1 + \kappa_{n-1} \cdot (1 + \ldots)\big)\Big) + \lambda_n$ με $\lambda_n < \lambda_{n-1}$.

Παρατηρούμε ότι η διαδρομή $N_{\lambda_1} \rightarrow N_{\lambda_2} \rightarrow \cdots \rightarrow N_{\lambda_n}$ δεν είναι άπειρη, αφού αντιστοιχεί στην φθίνουσα ακολουθία φυσικών αριθμών $(\lambda_1, \lambda_2, \ldots, \lambda_n)$. Άρα θα υπάρχει τελικό N_n αυτής της ακολουθίας και, μάλιστα, αυτό θα είναι το N_1. Τούτο διότι αν τελειώνει σε N_n μεταξύ των N_1 και N_ν, θα βρίσκαμε τον ελάχιστο κ_{n+1}, για τον οποίον ισχύει: $\kappa_{n+1} \cdot \lambda_n > \alpha \Rightarrow \kappa_{n+1} \cdot \lambda_n = \alpha + \lambda_{n+1}$. Εάν N_n ελάχιστο, θα πρέπει $\lambda_{n+1} \geq \lambda_n \Rightarrow \lambda_{n+1} = \sigma \cdot \lambda_n + \lambda'_n$, από το οποίο $(\kappa_{n+1} - \sigma) \cdot \lambda_n = \alpha + \lambda'_n \rightarrow$ Άτοπο, καθώς κ_{n+1} είναι ελάχιστο (εάν $\lambda'_n = 0$, στην θέση του βάζουμε ένα από τα λ_n). Οπότε η διαδικασία μπορεί να συνεχιστεί και το τέλος της διαδρομής δεν είναι το N_n, αλλά κάποιο N'_n κοντύτερα του N_1. Προφανώς, αυτό το N'_n θα πρέπει να ταυτίζεται του N_1.

Ας θεωρήσουμε, τώρα, τυχαίο N_i επί του κύκλου. Παίρνουμε την προηγούμενη διαδρομή βήματος ν εντός του κύκλου α σημείων, που ξεκινάει από το N_0 και τελειώνει στο N_1, και την επαναλαμβάνουμε $i - 1$ φορές. Δηλαδή, στην διαδρομή που ξεκινά από το N_0 και τελειώνει στο N_1, θεωρώντας ως αρχή το N_1, επαναλαμβάνουμε την διαδρομή και φθάνουμε στο N_2· από το N_2, με τον ίδιο τρόπο, φθάνουμε στο N_3· από το N_3 στο N_4 και ούτω καθεξής. Με τον τρόπο αυτόν μπορούμε να φτάσουμε στο N_i, καθώς $\overbrace{1 + 1 + \ldots}^{i-1} + 1 = i$.

Με αυτό η απόδειξη ολοκληρώνεται.

7.3 Θεώρημα του Ουήλσον

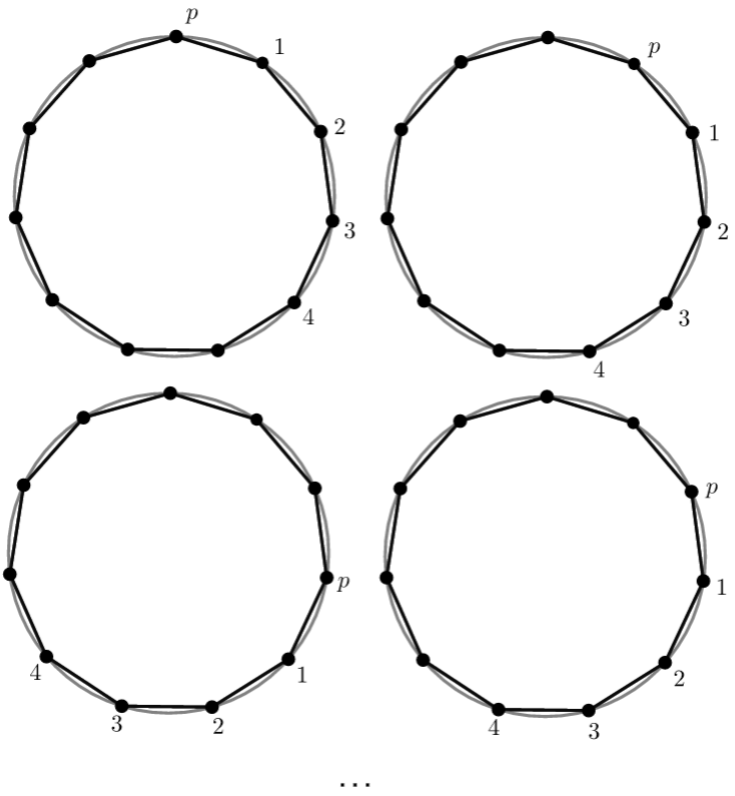
Όπως αναφέραμε στα προηγούμενα υποκεφάλαια, πρώτοι είναι οι αριθμοί οι οποίοι δεν διαιρούνται από κανέναν από τους φυσικούς αριθμούς που είναι μικρότεροί τους. Γεωμετρικά, ένας αριθμός είναι πρώτος εάν το αντίστοιχο ευθύγραμμο τμήμα, όταν διαιρεθεί σε οποιοδήποτε ακέραιο πλήθος τμημάτων, κάθε ένα από τα προκύπτοντα τμήματα δεν σύγκειται από μονάδες ή όταν κάθε διαδρομή - εντός ενός κύκλου τόσων σημείων όσος και ο αριθμός μας - ξεκινώντας από κάποιο αρχικό σημείο, χωρίς καμμία φορά να περάσει πέρα από αυτό, δεν φτάνει ποτέ σε αυτό (δηλαδή δεν δημιουργείται μη αστρική πολυγωνική διαδρομή). Και τα 2 αυτά χαρακτηριστικά των πρώτων αριθμών μας επιτρέπουν να βρούμε εάν ένας αριθμός είναι πρώτος ή όχι· μόνο προϋποτίθενται περισσότεροι από έναν έλεγχοι για τον προσδιορισμό αυτό. Παρακάτω θα περιγράψουμε έναν τρόπο που με έναν μόνον έλεγχο μπορούμε να προσδιορίσουμε εάν ένας αριθμός είναι πρώτος ή όχι †.

Θεώρημα του Ουήλσον (*Wilson*)**:** Έστω $p \geq 2$ αριθμός πρώτος. Ο αριθμός $(p-2)!-1$ διαιρείται από τον p. Αντίστροφα, εάν ο p διαιρεί τον $(p-2)!-1$, τότε ο p είναι πρώτος.

Θεωρούμε $N_i | i \in [1,p] \cap \mathbb{N}$ σημεία ομοιόμορφα κατανεμημένα στην περιφέρεια ενός κύκλου έτσι ώστε $\widehat{N_iN_{i+1}} = \widehat{N_{i+1}N_{i+2}}$. Για αρχή θα προσδιορίσουμε πόσα πολύγωνα, χρησιμοποιώντας όλα τα σημεία N_i, μπορούν να κατασκευαστούν εντός του κύκλου (p-γωνα). Κατασκευάζουμε το πολύγωνο $N_1N_2N_3 \dots N_p$ και σε αυτό επιδρούμε με μετάθεση $\tau \neq id$ κατασκευάζοντας έτσι πολύγωνο $N_{\tau(1)}N_{\tau(2)}N_{\tau(3)} \dots N_{\tau(p)}$. Άπαξ η τιμή $\tau(1)$ προσδιοριστεί να είναι κάποια από τις $N_1, N_2, \dots N_p$ (p δυνατές επιλογές), η επόμενη τιμή $\tau(2)$ μπορεί να είναι οποιαδήποτε από τις $N_1, N_2, \dots N_p$ εκτός της $\tau(1)$ ($p-1$ δυνατές επιλογές). Για την τιμή $\tau(3)$, οι δυνατές επιλογές είναι $N_1, N_2, \dots N_p$ εκτός των $\tau(1), \tau(2)$ ($p-2$ δυνατές επιλογές). Οπότε, συνεχίζοντας ομοίως, βρίσκουμε ότι: $\#\tau(1) = p$, $\#\tau(2) = p-1$, $\#\tau(3) = p-2$, $\dots$, $\#\tau(i) = p-i+1$, $\dots$, $\#\tau(p) = 1$. Από αυτό βλέπουμε ότι το συνολικό πλήθος των πολυγώνων που δημιουργούνται θα πρέπει να είναι: $\prod_{i=1}^{p} \#\tau(i) = \prod_{i=1}^{p} \#\tau(p-i+1) = 1 \cdot 2 \cdot \dots \cdot p = p!$

Από αυτά τα $p!$ πολύγωνα κάποια θα ταυτίζονται, λόγω συμμετρίας. Αρχικά παρατηρούμε ότι ένα πολύγωνο $N_{\tau(1)}N_{\tau(2)}N_{\tau(3)} \dots N_{\tau(p)}$ δεν αλλάζει μορφή εάν ξεκινήσουμε την αρίθμηση από διαφορετικό σημείο αλλά κρατήσουμε τις συνδέσεις των σημείων ίδιες. Δηλαδή, το $N_{\tau(1)}N_{\tau(2)}N_{\tau(3)} \dots N_{\tau(p)}$ ταυτίζεται του $N_{\tau(2)}N_{\tau(3)} \dots N_{\tau(p)}N_{\tau(1)}$ και αυτό, με την σειρά του, του $N_{\tau(3)} \dots N_{\tau(p)}N_{\tau(1)}N_{\tau(2)}$ κ.ο.κ., όπως εικονίζεται παρακάτω:

† *Η απόδειξη που δίνουμε είναι η απόδειξη του J.Peterson (Dickson [1], vol. I) τροποποιημένη (τροποποιημένη ώστε να ταιριάζει με όσα έχουν αναφερθεί στα προηγούμενα κεφάλαια αυτής της εργασίας).*



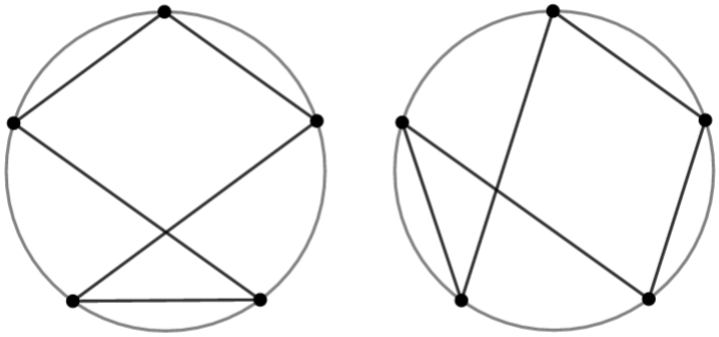
Σχήμα 7.6

Άρα, επειδή υπάρχουν p διαφορετικά σημεία που μπορούν να αποτελέσουν αρχή των πολυγώνων, το πλήθος των πολυγώνων που δεν εμφανίζουν την συμμετρία αυτή είναι: $\frac{p!}{p} = (p-1)!$. Για αυτά τα πολύγωνα δεν βλάπτει να υποθέσουμε ότι όλα έχουν αρχή το σημείο N_1.

Επιπλέον, επειδή η αρίθμηση των κορυφών ενός πολυγώνου μπορεί να γίνει είτε δεξιόστροφα είτε αριστερόστροφα, το πλήθος των πολυγώνων που δεν εμφανίζουν μεταξύ τους και τις 2 συμμετρίες αυτές, θα είναι: $\frac{(p-1)!}{2}$.

Υπάρχει άλλο ένα τελευταίο είδος συμμετρίας, το οποίο είναι λίγο περιπλοκότερο από τα προηγούμενα. Εάν πάρουμε ένα πολύγωνο το οποίο δεν είναι κανονικό, περιστρέφοντάς το κατά πολλαπλάσια του $\frac{2\pi}{p}$, παίρνουμε ένα πολύγωνο από τα $\frac{(p-1)!}{2}$, το οποίο δεν του αρχικού (προ περιστροφής) πολυγώνου. Στα κανονικά

πολύγωνα εμφανίζεται μια συμμετρία, αφού αν περιστέψουμε ένα κανονικό πολύγωνο κατά πολλαπλάσια του $\frac{2\pi}{p}$ προκύπτει ακριβώς το ίδιο (προ περιστροφής) πολύγωνο. Υπάρχει, δηλαδή, μια περιστροφική συμμετρία, την οποία δεν έχουμε λάβει υπόψην.



Σχήμα 7.7

Στην συνέχεια θα προσδιορίσουμε το πλήθος των κανονικών πολυγώνων. Λόγω της πρότασης που αναφέραμε στην αρχή του κεφαλαίου, επειδή p πρώτος, ξεκινώντας από το N_1, με οποιοδήποτε από τα βήματα $1, 2, 3, \ldots, p-1$ μπορεί να κατασκευαστεί πολυγωνική διαδρομή. Προφανώς, κάθε πολλαπλάσιο του p δεν κατασκευάζει πολύγωνο, αφού με βήμα πολλαπλάσιο του p, μόνον το N_1 μπορεί να αποτελεί σημείο της διαδρομής. Κάθε άλλος αριθμός $q > p$ μπορεί να γραφεί ως $q = \kappa \cdot p + \delta$, με $\delta \in \{1, 2, 3, \ldots, p-1\}$, $\kappa \in \mathbb{N}$, οπότε, ουσιαστικά, το βήμα q είναι βήμα δ. Τέλος, για τα $\delta < \frac{p}{2}$, παρατηρούμε ότι το πολύγωνο βήματος δ ταυτίζεται του πολυγώνου βήματος $p - \delta$, μιας και το δεύτερο είναι το πρώτο εάν φτιαχθεί με αντίθετη κατεύθυνση (δηλαδή αντί αριστερόστροφα, δεξιόστροφα ή το αντίστροφο). Οπότε το σύνολο των κανονικών πολυγώνων θα πρέπει να είναι $\frac{p-1}{2}$.

Συνεπώς, λαμβάνοντας υπόψην και την τελευταία συμμετρία, τα πολύγωνα που δεν την εμφανίζουν είναι στον αριθμό: $\frac{(p-1)!}{2} - \frac{p-1}{2} = (p-1) \cdot \frac{(p-2)!-1}{2} = \frac{p-1}{2} \cdot \Big((p-2)!-1\Big)$. Κάθε πολύγωνο από τα $\frac{p-1}{2} \cdot \Big((p-2)!-1\Big)$ μπορεί να περιστραφεί $p-1$ φορές, δίνοντας, έτσι, μαζί με τον εαυτό του, p στο πλήθος πολύγωνα· δηλαδή, τα $\frac{p-1}{2} \cdot \Big((p-2)!-1\Big)$ πολύγωνα που απέμειναν ομαδοποιούνται

ανά p. Αυτό σημαίνει ότι το πλήθος $\frac{p-1}{2} \cdot \Big((p-2)! - 1\Big)$ διαιρείται από το p. Επειδή $\mathbb{N} \ni \frac{p-1}{2} < p$, το p δεν διαιρεί τον $\frac{p-1}{2}$ (επειδή, ακόμη, p πρώτος) $\rightarrow$ ο p διαιρεί τον $(p-2)! - 1$.

Αντίστροφα, εάν ο p ήταν σύνθετος, θα είχε τους διαιρέτες του δ και $\frac{p}{\delta}$ μικρότερους ή ίσους του $\frac{p}{2}$, μιας και το 2 είναι ο μικρότερος πρώτος που μπορεί να διαιρεί τον p. Επειδή εάν $\frac{p}{2} > p-2 \Rightarrow p < 4$ προκύπτει άτοπο, διότι 2,3 πρώτοι, θα ισχύει $\frac{p}{2} < p-2$. Από αυτό συνάγουμε τα εξής: Εάν $\delta \neq \frac{p}{\delta}$, τότε και οι 2 διαιρέτες αποτελούν παράγοντες του παραγοντικού $(p-2)!$, οπότε ο p διαιρεί το $(p-2)! \rightarrow$ ο p δεν διαιρεί τον $(p-2)! - 1$. Εάν $\delta = \frac{p}{\delta} \Rightarrow p = \delta^2$, τότε πάλι ισχυριζόμαστε ότι ο p δεν διαιρεί τον $(p-2)! - 1$. Πράγματι, εάν $2\delta \leq \frac{p}{2}$, τότε το δ^2 είναι παράγοντας του $(p-2)! \rightarrow$ ο p διαιρεί τον $(p-2)!$. Εάν $2\delta \geq \frac{p}{2} \Rightarrow 4\delta > p$, επειδή $\delta^2 = p$, θα πρέπει $\delta < 4 \Rightarrow \delta \in \{2, 3\}$. Εάν $\delta = 2 \Rightarrow p = 4$ και τότε $(4-2)! - 1 = 2! - 1 = 1$, που δεν διαιρείται από το 4. Εάν $\delta = 3 \Rightarrow p = 9$ και τότε $(9-2)! - 1 = 7! - 1 = 5039$. Επειδή $5 + 0 + 3 + 9 = 17$ δεν διαιρείται από το 9, ο 5039 δεν διαιρείται από το 9.

Με αυτό η απόδειξη ολοκληρώνεται.

Κεφάλαιο 8

Μέγιστος κοινός διαιρέτης (Μ.Κ.Δ.) και ελάχιστο κοινό πολλαπλάσιο (Ε.Κ.Π.)

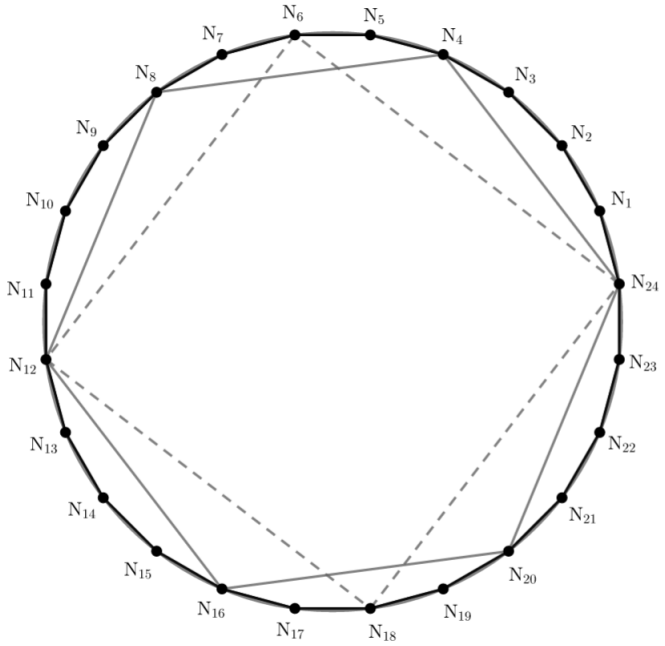
8.1 Μέγιστος κοινός διαιρέτης

Έστω α, β αριθμοί φυσικοί. Επειδή οι διαιρέτες των α, β θα είναι πάντοτε μικρότεροι των α, β και το πλήθος των φυσικών έως τα α, β είναι πεπερασμένο, το πλήθος των διαιρετών θα είναι κι αυτό πεπερασμένο. Οπότε τα σύνολα $A = \{x \in \mathbb{N} \mid x \text{ διαιρεί τον } \alpha\}$ και $B = \{x \in \mathbb{N} \mid x \text{ διαιρεί τον } \beta\}$ είναι πεπερασμένα. Είναι και μη κενά, αφού $1 \in A, B$. Επίσης θεωρούμε $\Delta = A \cap B$. Το Δ δεν είναι κενό, καθώς $A \cap B \supseteq \{1\} \neq \emptyset$. Θα ονομάζουμε μέγιστο κοινό διαιρέτη δ των α, β το μέγιστο στοιχείο του Δ (υπάρχει μέγιστο στοιχείο, διότι το Δ είναι υποσύνολο των φυσικών και πεπερασμένο).

Ο αριθμός δ θα διαιρείται από κάθε στοιχείο του Δ, διότι, εάν υπήρχε $\nu \in \Delta$ που να μην διαιρούσε τον δ, θα είχαμε: $\delta \in \Delta \Rightarrow \alpha = \kappa_1 \cdot \delta, \beta = \kappa_2 \cdot \delta \cdot$ επειδή $\nu \in \Delta$ με ν να μην διαιρεί τον δ, το ν διαιρεί τους κ_1, κ_2. Από αυτό, $\kappa_1 = \lambda_1 \cdot \nu$ και $\kappa_2 = \lambda_2 \cdot \nu \Rightarrow \alpha = \lambda_1 \cdot \nu \cdot \delta$ και $\beta = \lambda_2 \cdot \nu \cdot \delta \Rightarrow \delta < \nu \cdot \delta \in \Delta \Rightarrow$ το δ δεν είναι μέγιστο του $\Delta \rightarrow$ Άτοπο. Αντίστροφα μπορούμε να δούμε ότι εάν $\delta \in \Delta$ και δ διαιρείται από κάθε x του Δ, το Δ είναι το μέγιστο του $\Delta \rightarrow$ το δ είναι ο μέγιστος κοινός διαιρέτης των α, β.

Για να εκφράσουμε τον μέγιστο κοινό διαιρέτη των α, β γεωμετρικά, θεωρούμε $N_i \mid i \in [1, \alpha \cdot \beta] \cap \mathbb{N}$ σημεία ομοιόμορφα κατανεμημένα στην περιφέρεια ενός κύκλου έτσι ώστε $\widehat{N_i N_{i+1}} = \widehat{N_{i+1} N_{i+2}}$. Κατασκευάζοντας τις πολυγωνικές διαδρομές

βημάτων α και β, παρατηρούμε ότι είναι κανονικά πολύγωνα, αφού $\alpha \cdot \beta \propto \alpha, \beta$. Θα δείξουμε ότι η ελάχιστη φυσική απόσταση (στην περιφέρεια του κύκλου) των κορυφών των 2 αυτών πολυγώνων αντιστοιχεί στον μέγιστο κοινό διαιρέτη των α, β.



Σχήμα 8.1: *Εντός του* 24*γωνου* $(4 \cdot 6 = 24)$*, το* 4*γωνο (ο αριθμός* 6*) και το* 6*γωνο (ο αριθμός* 4*) απέχουν ελάχιστη απόσταση* $\widehat{N_6 N_8} = 2$*. Οπότε,* $\mu\kappa\delta(4, 6) = 2$.

Πράγματι, θεωρούμε δ τον μέγιστο κοινό διαιρέτη των α, β. Εάν $\alpha = \kappa \cdot \delta$, το β θα έχει την μορφή $\beta = \lambda \cdot \delta^{\mu}$, με $\mu\kappa\delta(\kappa, \lambda) = 1$. Αυτό διότι εάν $\mu\kappa\delta(\kappa, \lambda) = \sigma$, θα είχαμε $\alpha = \dfrac{\kappa}{\sigma} \cdot \sigma \cdot \delta$ και $\beta = \dfrac{\lambda}{\sigma} \cdot \sigma \cdot \delta \rightarrow$ το $\sigma \cdot \delta > \delta$ κοινός διαιρέτης των α, β. Επιπλέον ισχύει ότι $\mu\kappa\delta(\kappa, \delta) = 1$, διότι: εάν $\mu\kappa\delta(\kappa, \delta) = \tau$, θα είχαμε $\alpha = \dfrac{\kappa}{\tau} \cdot \tau \cdot \delta$ και $\beta = \lambda \cdot \dfrac{\delta}{\tau} \cdot \tau \cdot \delta^{\mu-1}$. Για $\mu \geq 2$, $\tau \cdot \delta > \delta$ κοινός διαιρέτης των α, β. Για $\mu = 1$, το $\tau \leq \delta$ είναι ο μέγιστος κοινός διαιρέτης των α, β (το $\tau < \delta$ είναι προφανές γιατί απορρίπτεται. Εάν τ=δ, θα είχαμε $\alpha = \dfrac{\kappa}{\delta} \cdot \delta^2$ και $\beta = \lambda \cdot \delta$. Εναλλάσσοντας τους ρόλους των α και β, μπορούμε να πάρουμε τα αντίστοιχα κ και λ όπως χρειάζονται).

Οπότε μπορούμε να συμπεράνουμε ότι $\mu\kappa\delta\Big(\dfrac{\alpha}{\delta}, \beta\Big) = 1$, αφού $\dfrac{\alpha}{\delta} = \kappa$, $\beta = \lambda \cdot \delta^{\mu}$

και $\mu\kappa\delta(\kappa,\lambda)=\mu\kappa\delta(\kappa,\delta)=1$. Επειδή κάθε κοινός διαιρέτης των $\frac{\alpha}{\delta},\beta$ διαιρεί τον $\mu\kappa\delta\left(\frac{\alpha}{\delta},\beta\right)=1$, οι αριθμοί $\frac{\alpha}{\delta},\beta$ δεν έχουν διαιρέτη μεγαλύτερο του 2.

Από την πρόταση στην αρχή του κεφαλαίου, θεωρώντας κύκλο β σημείων, η διαδρομή με βήμα $\frac{\alpha}{\delta}$ περνά από κάθε σημείο του κύκλου. Ειδικότερα, μπορούμε να βρούμε $\mu,\nu\in\mathbb{N}$ τέτοια ώστε: $\mu\cdot\frac{\alpha}{\delta}=\nu\cdot\beta+1\Rightarrow\frac{\alpha\mu}{\delta}\cdot\alpha=\nu\cdot\alpha\beta+\alpha\Rightarrow\frac{\alpha\mu^2}{\delta}\cdot\alpha=\mu\nu\cdot\alpha\beta+\mu\cdot\alpha\Rightarrow\frac{\alpha\mu^2}{\delta}\cdot\alpha=\mu\nu\cdot\alpha\beta+\nu\delta\cdot\beta+\delta\Rightarrow\frac{\alpha\mu^2}{\delta}\cdot\alpha-\nu\delta\cdot\beta=\mu\nu\cdot\alpha\beta+\delta$.

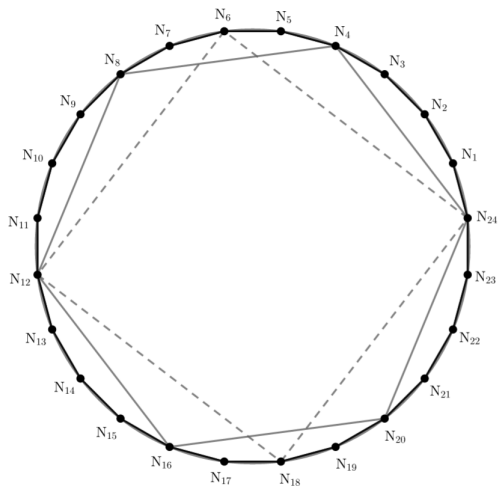
Στην προηγούμενη ισότητα θέτουμε: $x=\frac{\alpha\mu^2}{\delta}$, $y=\nu\delta$, $z=\mu\nu$ και παίρνουμε: $x\cdot\alpha+y\cdot\beta=z\cdot\alpha\beta+\delta$. Αυτή η νέα ισότητα, ουσιαστικά, μας πληροφορεί ότι υπάρχουν 2 σημεία των διαδρομών βημάτων α και β αντίστοιχα εντός του κύκλου των $\alpha\beta$ σημείων που απέχουν μεταξύ τους απόσταση δ. Η απόσταση αυτή θα είναι η ελάχιστη, καθώς εάν υπάρχουν $\zeta,\eta,\theta\in\mathbb{N}$ τέτοια ώστε $\zeta\cdot\alpha-\eta\cdot\beta=\theta\cdot\alpha\beta+\upsilon$, με $\upsilon<\delta$, επειδή δ διαιρεί τα α,β, το δ θα διαιρεί το $\upsilon\rightarrow$ Άτοπο.

8.2 Ελάχιστο κοινό πολλαπλάσιο

Ας υποθέσουμε ότι $\alpha, \beta \in \mathbb{N}$. Θεωρούμε $A = \{x \in \mathbb{N} \mid x \propto \alpha\}$ να είναι το σύνολο των αριθμητικών πολλαπλασίων του α και αντίστοιχα $B = \{x \in \mathbb{N} \mid x \propto \beta\}$ να είναι το σύνολο των αριθμητικών πολλαπλασίων του β. Το σύνολο $E = A \cap B$ δεν είναι κενό και επίσης είναι κάτω φραγμένο, αφού $\alpha \cdot \beta \in E$ και $\forall x \in E, x \geq max\{\alpha, \beta\}$. Ως μη κενό και κάτω φραγμένο υποσύνολο των φυσικών, το E θα έχει ελάχιστο στοιχείο· αυτό το ελάχιστο στοιχείο ε το ονομάζουμε ελάχιστο κοινό πολλαπλάσιο των α, β.

Το ε έχει την ιδιότητα να διαιρεί οποιοδήποτε άλλο πολλαπλάσιο των α και β, αφού εάν υπήρχε $x \in E$ με το ε να μην διαιρούσε το x, θα είχαμε $x = \kappa \cdot \varepsilon + \upsilon$. Εάν α, β διαιρούν το x, επειδή διαιρούν και το ε, θα διαιρούν το υ. Τότε όμως το υ θα ήταν πολλαπλάσιο των α, β μικρότερο του $\varepsilon \rightarrow$ Άτοπο.

Για να εκφράσουμε το ελάχιστο κοινό πολλαπλάσιο των α, β γεωμετρικά, θεωρούμε $N_i \mid i \in [1, \alpha \cdot \beta] \cap \mathbb{N}$ σημεία ομοιόμορφα κατανεμημένα στην περιφέρεια ενός κύκλου έτσι ώστε $\widehat{N_i N_{i+1}} = \widehat{N_{i+1} N_{i+2}}$. Κατασκευάζοντας τις πολυγωνικές διαδρομές βημάτων α και β, παρατηρούμε ότι είναι κανονικά πολύγωνα, αφού $\alpha \cdot \beta \propto \alpha, \beta$. Θα δείξουμε η απόσταση (στην περιφέρεια του κύκλου) της αρχής των διαδρομών με το πρώτο σημείο τομής των διαδρομών επί του κύκλου αντιστοιχεί στο ελάχιστο κοινό πολλαπλάσιο των α, β.



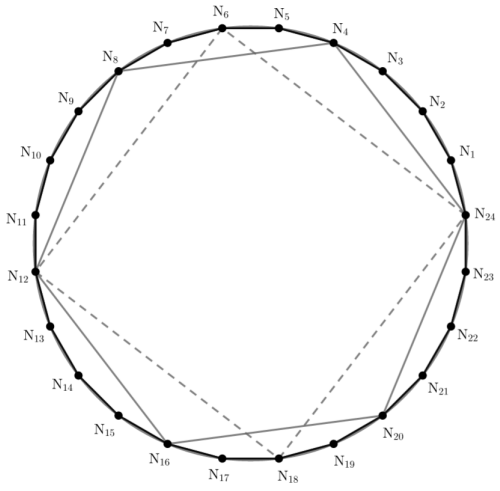
Σχήμα 8.2: *Εντός του* 24*γωνου* $(4 \cdot 6 = 24)$*, το* 4*γωνο (ο αριθμός* 6*) και το* 6*γωνο (ο αριθμός* 4*) τέμνονται στο* N_{12}*. Επειδή* $\widehat{N_{24} N_{12}} = 12$*,* $\varepsilon\kappa\pi(4, 6) = 12$*.*

Τα σημεία τομής των 2 διαδρομών (έστω N_j που αντιστοιχεί στον αριθμό j) θα αντιστοιχούν σε πολλαπλάσια των αριθμών α και β, αφού σε αυτά ισχύει: $\exists\ \kappa, \lambda \in \mathbb{N} : \kappa \cdot \alpha = \lambda \cdot \beta = j \propto \alpha, \beta$. Προφανώς, από αυτά τα σημεία, αυτό το N_μ που ορίζει ελάχιστη απόσταση $\widehat{N_{\alpha\beta}N_\mu} = \mu$ θα αντιστοιχεί στο ελάχιστο κοινό πολαπλάσιο $\varepsilon\kappa\pi(\alpha, \beta) = \mu$.

8.3 Σχέση μεταξύ Ε.Κ.Π. και Μ.Κ.Δ.

Το ελάχιστο κοινό πολλαπλάσιο και ο μέγιστος κοινός διαιρέτης 2 φυσικών αριθμών α, β είναι έννοιες αλληλοεξερτόμενες. Συγκεκριμένα, εάν δ είναι ο $\mu\kappa\delta(\alpha, \beta)$ και ε είναι το $\varepsilon\kappa\pi(\alpha, \beta)$, οι αριθμοί δ και ε είναι αντιστρόφως ανάλογοι· μάλιστα, ισχύει: $\delta \cdot \varepsilon = \alpha \cdot \beta$.

Θεωρούμε κύκλο $\alpha \cdot \beta$ σημείων και εντός αυτού τις διαδρομές βημάτων α και β αντίστοιχα. Για να αποδείξουμε την προηγούμενη σχέση ισχυριζόμαστε ότι και οι 2 διαδρομές διέρχονται από το $\dfrac{\alpha\beta}{\delta}$ και δεν τέμνονται σε κανένα άλλο σημείο προ αυτού $\left(\text{δηλαδή } \dfrac{\alpha\beta}{\delta} = \varepsilon\kappa\pi(\alpha, \beta)\right)$. Πράγματι, για αρχή παρατηρούμε ότι $\dfrac{\alpha\beta}{\delta} \propto \alpha, \beta$, οπότε, $\dfrac{\alpha\beta}{\delta}$ ανήκει στο σύνολο των πολλαπλασίων των α και β. Εάν $\dfrac{\alpha\beta}{\delta} \neq \varepsilon$, θα υπάρχει σημείο $\varepsilon = \varepsilon\kappa\pi(\alpha, \beta)$ μεταξύ της αρχής και του $\dfrac{\alpha\beta}{\delta}$. Από την Αρχημίδεια ιδιότητα, θα υπάρχει ελάχιστος μ τέτοιος ώστε $\mu\cdot\varepsilon > \dfrac{\alpha\beta}{\delta} \Rightarrow (\mu-1)\cdot\varepsilon \leq \dfrac{\alpha\beta}{\delta}$. Θεωρώντας την διαφορά $\dfrac{\alpha\beta}{\delta} - (\mu-1)\cdot\varepsilon$, παρατηρούμε ότι ισχύει: $0 \leq \dfrac{\alpha\beta}{\delta} - (\mu-1)\cdot\varepsilon < \varepsilon$, οπότε, επειδή επιπλέον $\dfrac{\alpha\beta}{\delta}, \varepsilon \propto \alpha, \beta$, η διαφορά είναι πολλαπλάσιο των α, β. Από αυτό παίρνουμε άτοπο, καθώς τότε θα υπήρχε πολλαπλάσιο των α, β μικρότερο του ελαχίστου.



Σχήμα 8.3: *Ο μέγιστος κοινός διαιρέτης των* $4, 6$ *(το* 2*) χωρίζει το* 24*γωνο σε* 2 *τμήματα μήκους* 12 *στα οποία οι διαδρομές βημάτων* 4 *και* 6 *δεν τέμνονται.*

Τελικά, $\frac{\alpha\beta}{\delta} = \varepsilon \Rightarrow \delta \cdot \varepsilon = \alpha \cdot \beta$, το οποίο σημαίνει ότι ο δ ορίζει στον κύκλο κανονική πολυγωνική διαδρομή βήματος ε.

Δηλαδή, εάν τέμνουμε τον κύκλο σε τόσα τμήματα όση και η ελάχιστη απόσταση μεταξύ των πολυγωνικών διαδρομών βήματος α και β αντίστοιχα επί κύκλου $\alpha \cdot \beta$ σημείων, δημιουργείται πολυγωνική διαδρομή βήματος $\varepsilon = \varepsilon\kappa\pi(\alpha, \beta)$, που διέρχεται από σημεία που αντιστοιχούν στα πολλαπλάσια των α και β, στα οποία οι 2 πολυγωνικές διαδρομές των α και β τέμνονται (μάλιστα όλα τα πολλαπλάσια έως του $\alpha \cdot \beta$ πιάνονται).

Κεφάλαιο 9

Γραμμική διοφαντική εξίσωση

Ένα πόρισμα των όσων είπαμε περι διαδρομών, είναι ο προσδιορισμός της ύπαρξης λύσεων $(x, y) \in \mathbb{Z}^2$ της εξίσωσης $\alpha \cdot x - \beta \cdot y = \gamma$, για τις διάφορες τιμές των $\alpha, \beta, \gamma \in \mathbb{N}$.

Συγκεκριμένα, αρχικά εάν υποθέσουμε ότι $\alpha, \beta, \gamma \in \mathbb{N}$ με $\delta = \mu\kappa\delta(\alpha, \beta)$ να μην διαιρεί τον γ, η εξίσωση $\alpha \cdot x - \beta \cdot y = \gamma$ δεν έχει λύσεις $(x, y) \in \mathbb{Z}^2$. Πράγματι, εάν υπάρχουν $(x, y) \in \mathbb{Z}^2$ τέτοια ώστε $\alpha \cdot x - \beta \cdot y = \gamma$, θα πρέπει δ να διαιρεί τον γ, αφού διαιρεί τους α και β. Αυτό, όμως, είναι άτοπο από την υπόθεση.

Εάν υποθέσουμε ότι α, β, γ είναι φυσικοί αριθμοί με $\delta = \mu\kappa\delta(\alpha, \beta)$ να διαιρεί τον γ, η εξίσωση $\alpha \cdot x - \beta \cdot y = \gamma$ έχει λύσεις $(x, y) \in \mathbb{Z}^2$. Πράγματι, η εξίσωση $\alpha \cdot x - \beta \cdot y = \gamma$ θα είναι ισοδύναμη με την $\frac{\alpha}{\delta} \cdot x - \frac{\beta}{\delta} \cdot y = \frac{\gamma}{\delta}$. Επειδή $\mu\kappa\delta\left(\frac{\alpha}{\delta}, \frac{\beta}{\delta}\right) = 1 < 2$, οι διαδρομές βημάτων $\frac{\alpha}{\delta}, \frac{\beta}{\delta}$ εντός κύκλου $\frac{\alpha}{\delta} \cdot \frac{\beta}{\delta}$ σημείων θα έχουν 2 σημεία που η μεταξύ τους απόσταση επί του κύκλου θα είναι $\frac{\gamma}{\delta}$. Αυτό διότι στον κύκλο $\frac{\beta}{\delta}$ σημείων η διαδρομή βήματος $\frac{\alpha}{\delta}$ περνάει από το $w + \frac{\gamma}{\delta} \in \mathbb{N}$, άρα υπάρχουν p_1, q_1 φυσικοί για τους οποίους ισχύει: $\frac{\alpha}{\delta} \cdot p_1 = \frac{\beta}{\delta} \cdot q_1 + w + \frac{\gamma}{\delta}$ και αντίστοιχα, η διαδρομή βήματος $\frac{\beta}{\delta}$ στον κύκλο $\frac{\alpha}{\delta}$ σημείων διέρχεται από το $\frac{\gamma}{\delta}$, άρα υπάρχουν p_2, q_2 φυσικοί για τους οποίους ισχύει: $\frac{\beta}{\delta} \cdot q_2 = \frac{\alpha}{\delta} \cdot p_2 + w$· συνδυάζοντας τις 2 ισότητες παίρνουμε: $\frac{\alpha}{\delta} \cdot (p_1 + p_2) = \frac{\beta}{\delta} \cdot (q_1 + q_2) + \frac{\gamma}{\delta}$. Οπότε θα υπάρχουν $p = p_1 + p_2, q = q_1 + q_2$ φυσικοί για τους οποίους θα ισχύει $\frac{\alpha}{\delta} \cdot p - \frac{\beta}{\delta} \cdot q = \frac{\gamma}{\delta}$. Θέτωντας $x = p$ και $y = q$, παίρνουμε μια λύση $(x, y) \in \mathbb{Z}^2$ της εξίσωσής μας.

Κεφάλαιο 10

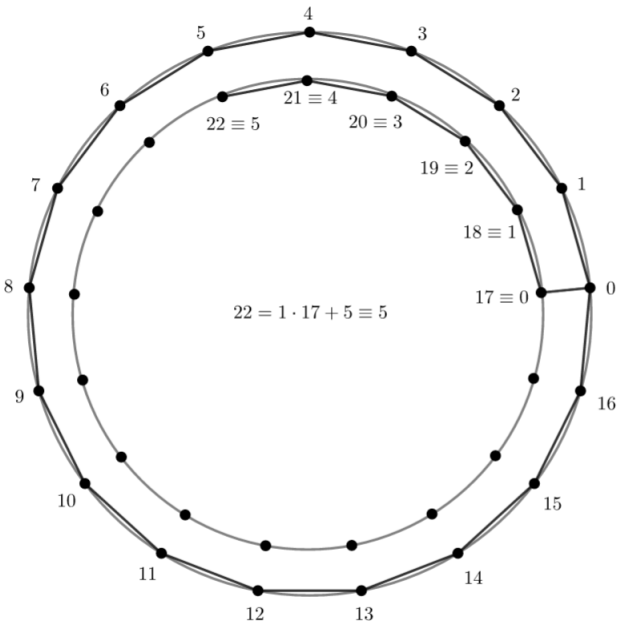
Αριθμητική υπολοίπων

10.1 Γενικά

Ας αναπαριστήσουμε έναν φυσικό αριθμό α χρησιμοποιώντας την κυκλική αναπαράσταση των αριθμών σε κύκλο $\beta > \alpha$ σημείων. Ξεκινώντας με βήμα γ τέτοιο ώστε $\mu\kappa\delta(\beta, \gamma) = 1 < 2$, κατασκευάζουμε μια διαδρομή η οποία, κατά τα προηγούμενα, θα διέλθει από το α. Επειδή θα διέλευθει από το α, θα υπάρχουν $\kappa, \lambda \in \mathbb{N}$ τέτοιοι ώστε $\kappa \cdot \gamma = \lambda \cdot \beta + \alpha$. Εάν πάρουμε την ειδική περίπτωση όπου $\gamma = 1$, τότε $\mu\kappa\delta(1, \beta) = 1 < 2$ και $\kappa = \lambda \cdot \beta + \alpha$.

Έτσι, λοιπόν, βλέπουμε ότι μπορούμε να αντιστοιχίσουμε παραπάνω από έναν αριθμούς σε ένα σημείο του κύκλου, και οι αριθμοί που αντιστοιχούνται στο σημείο αυτό είναι σημεία στα οποία η διαδρομή βήματος 1 φτάνει μετά από λ πλήρεις περιστροφές και α επιπλέον βήματα. Συγκεκριμένα, εάν ο κύκλος είναι β σημείων, στο α μπορούμε να αντιστοιχίσουμε όλους τους αριθμούς της μορφής $\lambda \cdot \beta + \alpha$.

Προφανώς, κάθε αριθμός $\kappa \leq \beta$ μπορεί να αντιστοιχηθεί σε ένα σημείο του κύκλου β σημείων, επειδή ακριβώς $\kappa \leq \beta$. Εάν $\kappa > \beta$, θα δείξουμε ότι, αρχικά υπάρχουν λ, α τέτοια ώστε $\kappa = \lambda \cdot \beta + \alpha$ με $\alpha < \beta$ και, κατά δεύτερον, ότι αυτά τα λ, α είναι μοναδικά· τότε, ο αριθμός κ θα αντιστοιχίζεται στο σημείο α (αυτό είναι κάτι που στα προηγούμενα κεφάλαια χρησιμοποιούσαμε, χωρίς όμως να το έχουμε αποδείξει). Πράγματι, λοιπόν, από Αρχημίδεια ιδιότητα θα υπάρχει ένας ελάχιστος $\lambda + 1$ τέτοιος ώστε $(\lambda + 1) \cdot \beta > \kappa \Rightarrow \lambda \cdot \beta \leq \kappa$. Θεωρούμε $\alpha = \kappa - \lambda \cdot \beta$ και παίρνουμε: $\kappa = \lambda \cdot \beta + \alpha$. Λόγω των προηγούμενων ανισοτήτων, μπορούμε να δούμε ότι $0 \leq \alpha = \kappa - \lambda \cdot \beta < \beta$, οπότε το α πληροί την προϋπόθεση $\alpha < \beta$. Εάν τώρα υπήρχαν λ, α και λ', α' (διαφορετικά μεταξύ τους, με $\alpha, \alpha' < \beta$) τέτοια ώστε: $\kappa = \lambda \cdot \beta + \alpha = \lambda' \cdot \beta + \alpha'$, θα ίσχυε $\alpha' - \alpha = \kappa - \lambda' \cdot \beta - \kappa + \lambda \cdot \beta = (\lambda - \lambda') \cdot \beta \propto \beta$. Οπότε, ουσιαστικά, στον κύκλο β σημείων, τα α, α' ταυτίζονται $\rightarrow \alpha = \mu \cdot \beta + \alpha'$. Επειδή το α πληροί την προϋπόθεση $\alpha < \beta$, τότε, $\mu = 0 \Rightarrow \alpha = \alpha'$. Από το τελευταίο προκύπτει ότι $(\lambda - \lambda') \cdot \beta = 0 \Rightarrow \lambda = \lambda'$.



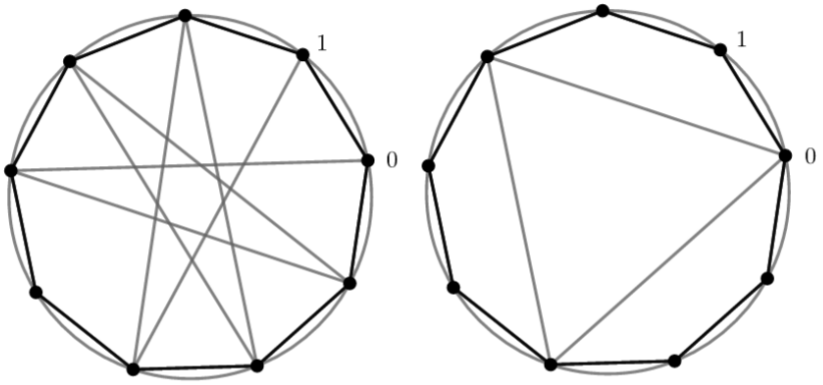
Σχήμα 10.1

Για παράδειγμα, στον κύκλο 17 σημείων, η διαδρομή βήματος 1, μετά από 22 βήματα, φθάνει στον αριθμό 5, αφού $22 = 1 \cdot 17 + 5$. Σε αυτήν την περίπτωση θα λέμε ότι το 22 ταυτίζεται του 5 στον κύκλο των 17 σημείων. Για ευκολία στην διατύπωση, όταν ένας αριθμός x στον κύκλο n σημείων ταυτίζεται ενός αριθμού y, θα γράφω $x\mathbb{O}n = y$ (εδώ $22\mathbb{O}17 = 5$).

Τέλος, αξίζει να παρατηρήσουμε ότι:
$(x + y)\mathbb{O}n = (k_x \cdot n + a_x + k_y \cdot n + a_y)\mathbb{O}n = a_x + a_y = x\mathbb{O}n + y\mathbb{O}n$
και
$(x \cdot y)\mathbb{O}n = \big[(k_x \cdot n + a_x) \cdot (k_y \cdot n + a_y)\big]\mathbb{O}n = (k_x \cdot k_y \cdot n^2 + k_x \cdot a_y \cdot n + k_y \cdot a_y \cdot n + a_x \cdot a_y)\mathbb{O}n = a_x \cdot a_y = x\mathbb{O}n \cdot y\mathbb{O}n.$

10.2 Αντίστροφοι αριθμοί στην αριθμητική υπολοίπων

Έστω x είναι ένας φυσικός αριθμός και ένας κύκλος n σημείων. Ισχυριζόμαστε ότι εάν x και n δεν έχουν κοινό διαιρέτη μεγαλύτερο της μονάδας, υπάρχει ένας τουλάχιστον $y \in \mathbb{N}$ τέτοιος ώστε ο αριθμός $x \cdot y$ εντός του κύκλου n σημείων, να ταυτίζεται του 1. Δηλαδή, $\forall x \in \mathbb{N}$ με $\mu\kappa\delta(x, n) < 2$, $\exists y \in \mathbb{N}$: $(x \cdot y)\mathbb{O}n = 1$.



Σχήμα 10.2: *Στον κύκλο των* 9 *σημείων η διαδρομή βήματος* 4 *(*$\mu\kappa\delta(4, 9) = 1$*) φθάνει στο* 1*, ενώ η διαδρομή βήματος* 3 *(*$\mu\kappa\delta(3, 9) = 3$*) δεν φθάνει στο* 1

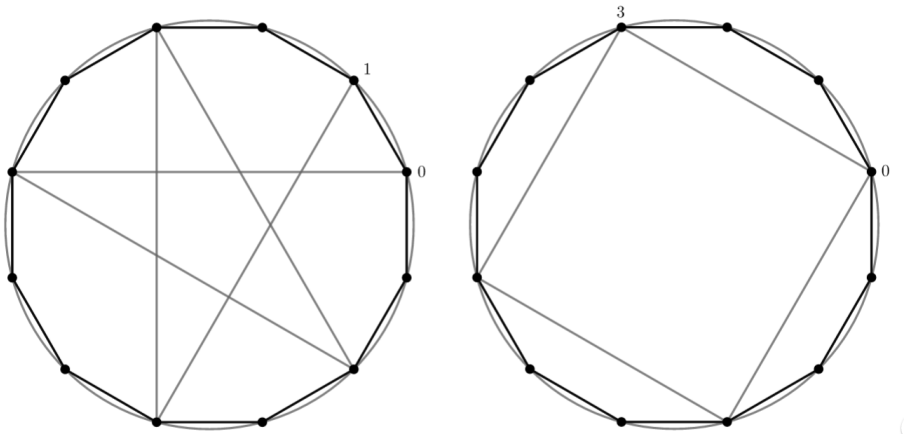
Θεωρούμε κύκλο n σημείων και εντός αυτού την διαδρομή βήματος x. Επειδή $\mu\kappa\delta(x, n) < 2$, σύμφωνα με την πρόταση περί διαδρομών, η διαδρομή βήματος x θα φθάσει στο 1. Συγκεκριμένα, θα υπάρχουν $y, z \in \mathbb{N}$ τέτοια ώστε $x \cdot y = z \cdot n + 1$. Από το τελευταίο παίρνουμε ότι $(x \cdot y)\mathbb{O}n = (z \cdot n + 1)\mathbb{O}n = 1$, που είναι το ζητούμενο.

Επίσης, εάν $\delta = \mu\kappa\delta(x, n) \geq 2$, δεν υπάρχει $y \in \mathbb{N}$: $(x \cdot y)\mathbb{O}n = 1$. Αυτό διότι εάν θεωρήσουμε κύκλο $x \cdot n$ σημείων και εντός αυτού τις διαδρομές βημάτων x και n αντίστοιχα, επειδή $(x \cdot y)\mathbb{O}n = 1 \Rightarrow x \cdot y = z \cdot n + 1 \Rightarrow x \cdot y - z \cdot n = 1 < 2$, θα υπήρχαν 2 σημεία των διαδρομών που θα απείχαν απόσταση μικρότερη του δ. Αυτό, προφανώς, είναι άτοπο.

10.3 Γραμμικές ισοτιμίες

Έχοντας αναλύσει την περίπτωση των αντιστρόφων τις αριθμητικής υπολοίπων, μπορούμε να δούμε ότι η εξίσωση $(\alpha \cdot x)\mathbb{O}n = 1$, $\alpha \in \mathbb{N}$, έχει λύσεις $x \in \mathbb{N}$ όταν $\mu\kappa\delta(\alpha, n) = 1 < 2$. Εδώ, γενικεύουμε κάπως το προηγούμενο αποτέλεσμα δείχνοντας ότι, εάν $\delta = \mu\kappa\delta(\alpha, n)$, η εξίσωση $(\alpha \cdot x)\mathbb{O}n = \delta$ έχει λύσεις $x \in \mathbb{N}$.

Πράγματι, εφόσον $\delta = \mu\kappa\delta(\alpha, n)$, εντός του κύκλου $\alpha \cdot n$ σημείων, οι διαδρομές βημάτων α και n έχουν 2 σημεία τα οποία απέχουν μεταξύ τους απόσταση δ επί τις περιφέρειας του κύκλου. Συγκεκριμένα, θα υπάρχουν $x, y, z \in \mathbb{N}$ τέτοια ώστε: $\alpha \cdot x - y \cdot n = z \cdot \alpha \cdot n + \delta$. Από το τελευταίο παίρνουμε το ζητούμενο, καθώς $(\alpha \cdot x - y \cdot n)\mathbb{O}n = (z \cdot \alpha \cdot n + \delta)\mathbb{O}n \Rightarrow (\alpha \cdot x)\mathbb{O}n - (y \cdot n)\mathbb{O}n = (z \cdot \alpha \cdot n + \delta)\mathbb{O}n \Rightarrow (\alpha \cdot x)\mathbb{O}n = \delta$.



Σχήμα 10.3: *Στον κύκλο των* 12 *σημείων, η διαδρομή βήματος* 5 *(*$\mu\kappa\delta(5, 12) = 1$*) περνάει από το* 1. *Αντίστοιχα, η διαδρομή βήματος* 3 *(*$\mu\kappa\delta(3, 12) = 3$*) περνάει από το* 3

Έχοντας αποδείξει ότι η εξίσωση $(\alpha \cdot x)\mathbb{O}n = \delta$ έχει λύσεις $x \in \mathbb{N}$, μπορούμε να δείξουμε ότι η εξίσωση $(\alpha \cdot x)\mathbb{O}n = \kappa \cdot \delta$ έχει λύσεις για κάθε $\kappa \in \mathbb{N}$. Εφόσον $(\alpha \cdot x)\mathbb{O}n = \delta$ έχει λύσεις, η διαδρομή βήματος α στον κύκλο των n σημείων διέρχεται από το δ. Επιλέγουμε το τμήμα της διαδρομής που ξεκινά από το 0 και τελειώνει στο δ. Επαναλαμβάνοντάς το $\kappa - 1$ φορές, κατασκευάζουμε μια νέα διαδρομή που ξεκινάει από το 0 και τελειώνει στο $\kappa \cdot \delta$. Δηλαδή, στο τμήμα της διαδρομής που ξεκινά από το 0 και τελειώνει στο δ, θεωρώντας ως αρχή το δ, επαναλαμβάνουμε το τμήμα της διαδρομής και φθάνουμε στο $2 \cdot \delta$· από το $2 \cdot \delta$, με τον ίδιο τρόπο, φτάνουμε στο $3 \cdot \delta$ κ.ο.κ.. Με την διαδικασία αυτή μπορούμε

να φτάσουμε στο $\kappa \cdot \delta$, αφού $\overbrace{\delta + \delta + \delta + \ldots}^{\kappa-1} + \delta = \kappa \cdot \delta$. Οπότε, η διαδρομή βήματος α διέρχεται από το $\kappa \cdot \delta$. Ισοδύναμα, υπάρχουν $x, z \in \mathbb{N}$ τέτοια ώστε $\alpha \cdot x = z \cdot n + \kappa \cdot \delta \Rightarrow (\alpha \cdot x)\mathbb{O}n = (z \cdot n + \kappa \cdot \delta)\mathbb{O}n = \kappa \cdot \delta \Rightarrow (\alpha \cdot x)\mathbb{O}n = \kappa \cdot \delta$.

Τέλος, θα δείξουμε ότι η εξίσωση $(\alpha \cdot x)\mathbb{O}n = \gamma$ δεν έχει λύσεις όταν $\gamma \not\propto \delta$. Πράγματι, ας υποθέσουμε ότι η $(\alpha \cdot x)\mathbb{O}n = \gamma$ έχει λύση $x = p$ με $\gamma \not\propto \delta$. Επειδή $\gamma \not\propto \delta$, θα υπάρχουν $\kappa, \kappa+1 \in \mathbb{N}$ τέτοια ώστε $\kappa \cdot \delta < \gamma < (\kappa+1) \cdot \delta$. Προηγουμένως δείξαμε ότι η $(\alpha \cdot x)\mathbb{O}n = \kappa \cdot \delta = \kappa \cdot \mu\kappa\delta(\alpha, n)$ έχει λύση q, οπότε: $(\alpha \cdot p)\mathbb{O}n = \gamma$ και $(\alpha \cdot q)\mathbb{O}n = \kappa \cdot \delta \Rightarrow (\alpha \cdot p)\mathbb{O}n - (\alpha \cdot q)\mathbb{O}n = \gamma - \kappa \cdot \delta \Rightarrow \big(\alpha \cdot (p - q)\big)\mathbb{O}n = \gamma - \kappa \cdot \delta \Rightarrow \alpha \cdot (p - q) = w \cdot n + \gamma - \kappa \cdot \delta \Rightarrow \alpha \cdot (p - q) - w \cdot n = \gamma - \kappa \cdot \delta < \delta$. Η τελευταία ισότητα μας πληροφορεί ότι εντός του κύκλου $\alpha \cdot n$ σημείων οι διαδρομές βημάτων α και n απέχουν μεταξύ τους απόσταση $0 < \gamma - \kappa \cdot \delta < \delta$. Αυτό είναι άτοπο, καθώς δ είναι ο $\mu\kappa\delta(\alpha, n)$.

10.4 Κινέζικο θεώρημα υπολοίπων

Έχοντας αναλύσει την περίπτωση των γραμμικών ισοτιμιών, μπορούμε να συνεχίσουμε στην επίλυση γραμμικών συστημάτων της αριθμητικής υπολοίπων. Αρχικά θα ασχοληθούμε με την απλούστερη περίπτωση συστήματος 2 εξισώσεων.

Ας υποθέσουμε $\eta, \theta, \kappa, \lambda, n, m \in \mathbb{N}$ και το σύστημα εξισώσεων:

$$(\eta \cdot x)\mathbb{O}n = \kappa$$
$$(\theta \cdot x)\mathbb{O}m = \lambda$$

Για να έχει λύσεις το σύστημα, θα πρέπει, αρχικά, καθεμία από τις επιμέρους εξισώσεις να έχει λύση. Σύμφωνα με τα προηγούμενα, η $(\eta \cdot x)\mathbb{O}n = \kappa$ θα έχει λύση όταν $\kappa \propto \mu\kappa\delta(\eta, n)$ και η $(\theta \cdot x)\mathbb{O}m = \lambda$ θα έχει λύση όταν $\lambda \propto \mu\kappa\delta(\theta, m)$. Έστω $\alpha\mathbb{O}n$, $\beta\mathbb{O}m$ είναι λύσεις των εξισώσεων $(\eta \cdot x)\mathbb{O}n = \kappa$, $(\theta \cdot x)\mathbb{O}m = \lambda$. Τότε οι λύσεις του συστήματος αυτών των εξισώσεων θα ταυτίζονται με τις λύσεις του συστήματος:

$$x\mathbb{O}n = \alpha$$
$$x\mathbb{O}m = \beta$$

Τώρα, εάν y είναι μια λύση της εξίσωσης $x\mathbb{O}n = \alpha$, η y θα παίρνει την μορφή $y = p \cdot n + \alpha$. Εάν, επίσης, είναι λύση της $x\mathbb{O}m = \beta$, θα πρέπει $(p \cdot n + \alpha)\mathbb{O}m = \beta \Rightarrow (p \cdot n)\mathbb{O}m = \beta - \alpha \Rightarrow p \cdot n - q \cdot m = \beta - \alpha$. Από την τελευταία ισότητα βλέπουμε ότι θα πρέπει $\mu\kappa\delta(m, n)$ να διαιρεί τον $\beta - \alpha$ (σημειωτέον, χωρίς βλάβη της γενικότητας, μπορούμε να θεωρήσουμε $\beta - \alpha \geq 0$).

Εάν αντιστρόφως $\mu\kappa\delta(m, n)$ διαιρεί τον $\beta - \alpha$, προφανώς η $p \cdot n - q \cdot m = \beta - \alpha$ έχει λύσεις φυσικές και, συνεπώς, η ισοδύναμή της $(p \cdot n + \alpha)\mathbb{O}m = \beta$ έχει κι αυτή λύσεις. Οπότε, έτσι μπορεί να βρεθεί λύση x του συστήματος των εξισώσεων που αναφέραμε.

Η λύση x που βρίσκουμε είναι μοναδική στον κύκλο των $\varepsilon\kappa\pi(n, m)$ σημείων. Αυτό διότι εάν x, z δύο λύσεις του συστήματος, θα ισχύει:

$$x\mathbb{O}n = \alpha \text{ και } z\mathbb{O}n = \alpha$$
$$x\mathbb{O}m = \beta \text{ και } z\mathbb{O}m = \beta$$

Οπότε $x\mathbb{O}n - z\mathbb{O}n = 0 \Rightarrow (x - z)\mathbb{O}n = 0 \Rightarrow$ το n διαιρεί τον $x - z$. Ομοίως, $x\mathbb{O}m - z\mathbb{O}m = 0 \Rightarrow (x - z)\mathbb{O}m = 0 \Rightarrow$ το m διαιρεί τον $x - z$. Από τα 2 προηγούμενα μπορούμε να συνάγουμε ότι $\varepsilon\kappa\pi(n, m)$ διαιρεί τον $x - z \Rightarrow (x - z)\mathbb{O}\varepsilon\kappa\pi(n, m) = 0 \Rightarrow x\mathbb{O}\varepsilon\kappa\pi(n, m) = z \rightarrow$ η λύση z ταυτίζεται της x στον κύκλο των $\varepsilon\kappa\pi(n, m)$ σημείων.

Για συστήματα περισσότερων των 2 εξισώσεων, λύνουμε ανά 2 τις εξισώσεις έως ότου να φτάσουμε σε κοινή λύση.

$$\left\{ \begin{array}{l} \left\{ \begin{array}{l} x\mathbb{O}n_1 = \kappa_1 \\ x\mathbb{O}n_2 = \kappa_2 \end{array} \right\} \\ x\mathbb{O}n_3 = \kappa_3 \\ \dots \\ x\mathbb{O}n_c = \kappa_c \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} \left\{ \begin{array}{l} x\mathbb{O}\varepsilon\kappa\pi(n_1, n_2) = \kappa_{1,2} \\ x\mathbb{O}n_3 = \kappa_3 \end{array} \right\} \\ x\mathbb{O}n_4 = \kappa_4 \\ \dots \\ x\mathbb{O}n_c = \kappa_c \end{array} \right\} \Rightarrow \dots$$

Μια ειδική περίπτωση συστήματος γραμμικών ισοτιμιών είναι αυτή όπου όλοι οι κύκλοι έχουν πλήθος σημείων αριθμούς που ανά 2 δεν έχουν κοινό διαιρέτη μεγαλύτερο ή ίσο του 2. Συγκεκριμένα, τα συστήματα γραμμικών ισοτιμιών της μορφής:

$$\begin{array}{c} x\mathbb{O}n_1 = \kappa_1 \\ x\mathbb{O}n_2 = \kappa_2 \\ \dots \\ x\mathbb{O}n_c = \kappa_c \end{array}$$

Όπου $\mu\kappa\delta(n_i, n_j) < 2$ για κάθε $i \neq j$. Σε αυτήν την περίπτωση θα δείξουμε ότι η μοναδική λύση στον κύκλο των $\prod\limits_{i\in[c]} n_i$ σημείων είναι η $X = \sum\limits_{j\in[c]} \Big(\frac{x_j}{n_j} \prod\limits_{i\in[c]} n_i\Big)$, όπου x_j λύση της $\dfrac{x}{n_j} \prod\limits_{i\in[c]} n_i \mathbb{O} n_j = k_j$.

Στο προηγούμενο σύστημα εξισώσεων, επειδή n_i δεν έχουν ανά 2 κοινό διαιρέτη μεγαλύτερο του 2, αντικαθιστώντας το x της $j-$οστής εξίσωσης με $\dfrac{x}{n_j} \prod\limits_{i\in[c]} n_i$, προκύπτει νέα εξίσωση η οποία έχει λύσεις. Έστω x_j να είναι λύση της νέας εξίσωσης· η $\dfrac{x_j}{n_j} \prod\limits_{i\in[c]} n_i$ θα είναι λύση της $x\mathbb{O}n_j = \kappa_j$. Επειδή $\forall w \in [c]-\{j\}$ ισχύει $\dfrac{x_j}{n_j} \prod\limits_{i\in[c]} n_i \propto n_w$, θα πρέπει $\Big(\dfrac{x_j}{n_j} \prod\limits_{i\in[c]} n_i\Big)\mathbb{O}n_w = 0$. Από το τελευταίο μπορούμε να παρατηρήσουμε ότι η $X = \dfrac{x_1}{n_1} \prod\limits_{i\in[c]} n_i + \dfrac{x_2}{n_2} \prod\limits_{i\in[c]} n_i + \dots + \dfrac{x_c}{n_c} \prod\limits_{i\in[c]} n_i = \sum\limits_{j\in[c]} \Big(\dfrac{x_j}{n_j} \prod\limits_{i\in[c]} n_i\Big)$ είναι λύση του αρχικού μας συστήματος. Επειδή n_i, n_j για κάθε $i \neq j$ δεν έχουν κοινό διαιρέτη μεγαλύτερο του 2, ισχύει $\varepsilon\kappa\pi(n_c, \varepsilon\kappa\pi(n_{c-1}, \varepsilon\kappa\pi(\dots \varepsilon\kappa\pi(n_3, \varepsilon\kappa\pi(n_2, n_1)) \dots))) = \prod\limits_{i\in[c]} n_i$ και, συνεπώς, η $X = \sum\limits_{j\in[c]} \Big(\dfrac{x_j}{n_j} \prod\limits_{i\in[c]} n_i\Big)$ είναι μοναδική λύση του συστήματος στον κύκλο των $\prod\limits_{i\in[c]} n_i$ σημείων.

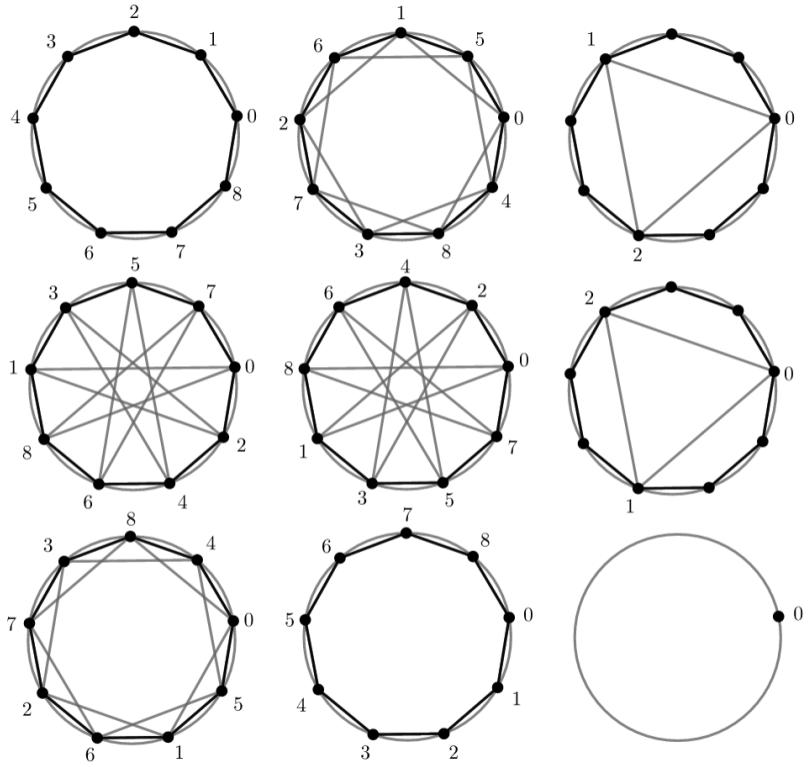
Κεφάλαιο 11

Η συνάρτηση Φ

11.1 Η συνάρτηση Φ στους πρώτους αριθμούς

Η συνάρτηση Φ είναι μια συνάρτηση που με είσοδο έναν φυσικό αριθμό α μας δίδει το πλήθος των αριθμών κάτω του α που δεν έχουν με το α κοινό διαιρέτη μεγαλύτερο ή ίσο του 2.

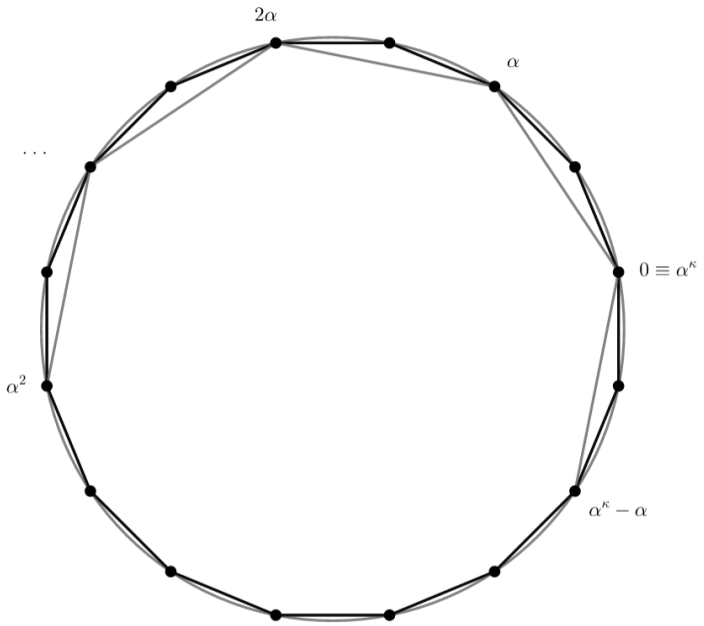
Για να εκφράσουμε γεωμετρικά την συνάρτηση Φ, αρχικά παρατηρούμε ότι σε έναν κύκλο α σημείων, η διαδρομή βήματος ν, όπου ν τέτοιο ώστε $\delta = \mu\kappa\delta(\nu, \alpha) \geq 2$, δεν διέρχεται από όλα τα σημεία του κύκλου. Αυτό διότι εάν διέρχοταν από τα $\kappa \cdot \delta + \gamma$ με $0 < \gamma < \delta$, επειδή διέρχεται από τα $\kappa \cdot \delta$, θα υπήρχαν αριθμοί $p, q \in \mathbb{N}$ τέτοιοι ώστε $(p \cdot \nu)\mathbb{O}\alpha = \kappa \cdot \delta + \gamma$ και $(q \cdot \nu)\mathbb{O}\alpha = \kappa \cdot \delta \Rightarrow (p \cdot \nu)\mathbb{O}\alpha - (q \cdot \nu)\mathbb{O}\alpha = \gamma \Rightarrow \big((p - q) \cdot \nu\big)\mathbb{O}\alpha = \gamma \Rightarrow (p - q) \cdot \nu - w \cdot \alpha = \gamma < \delta$. Από το τελευταίο παίρνουμε άτοπο, αφού οι διαδρομές βημάτων α και ν, εντός του κύκλου των $\alpha \cdot \nu$ σημείων, θα απείχαν απόσταση $\gamma < \delta = \mu\kappa\delta(\alpha, \nu)$. Συμβαίνει επίσης οι διαδρομές βημάτων ν, όπου ν τέτοιο ώστε $\mu\kappa\delta(\alpha, \nu) < 2$, εντός του κύκλου των α σημείων, να διέρχονται από κάθε σημείο του κύκλου, όπως αναλύσαμε στα προηγούμενα κεφάλαια. Οπότε η συνάρτηση Φ σε μία τιμή α, ουσιαστικά, μας δείχνει με πόσα διαφορετικά βήματα μπορούν να κατασκευαστούν διαδρομές εντός ενός κύκλου α σημείων, ώστε αυτές να διέρχονται από κάθε σημείο του κύκλου.



Σχήμα 11.1: *Στον κύκλο των* 9 *σημείων μπορούν* 6 *διαδρομές να κατασκευαστούν που να διέρχονται από κάθε σημείο του κύκλου· αυτές των βημάτων* $1, 2, 4, 5, 7$ *και* 8. *Συνεπώς,* $\Phi(9) = 6$.

Όσον αφορά την περίπτωση των πρώτων αριθμών, σε προηγούμενη πρόταση έχουμε δείξει ότι, εάν α είναι πρώτος αριθμός, με οποιοδήποτε βήμα μη πολλαπλάσιο του α κατασκευάζονται διαδρομές που διέρχονται από κάθε σημείο τού κύκλου των α σημείων. Οπότε για κάθε ένα από τα βήματα $1, 2, 3, \ldots, \alpha - 1$ μπορούν να κατασκευαστούν διαδρομές που διέχονται από κάθε σημείο του κύκλου των α σημείων, ενώ για το βήμα α μόνο το αρχικό σημείο μπορεί να αποτελεί σημείο της διαδρομής $\rightarrow \Phi(\alpha) = \alpha - 1$.

Θα αναλύσουμε ακόμη μία περίπτωση· αυτήν των αριθμών α^κ, όταν α είναι αριθμός πρώτος. Εδώ κασκευάζουμε κύκλο α^κ σημείων και εντός του τις διαδρομές βημάτων ν. Επειδή το α είναι πρώτος, ξεκινώντας την διαδρομή με βήμα κάποιον αριθμό ανάμεσα του $\lambda \cdot \alpha$ και του $(\lambda + 1) \cdot \alpha$, κατασκευάζουμε διαδρομή που διέρχεται από κάθε σημείο του κύκλου. Αυτό διότι $0 < \nu - \lambda \cdot \alpha < \alpha$· ο $\nu - \lambda \cdot \alpha$ ως αριθμός μικρότερος του α δεν θα έχει κοινό διαιρέτη με τον α μεγαλύτερο ή ίσο του 2 και, επειδή επιπλέον $\lambda \cdot \alpha \propto \alpha$, το ν δεν έχει με τον α κοινό διαιρέτη μεγαλύτερο ή ίσο του $2 \rightarrow \mu\kappa\delta(\nu, \alpha^\kappa) < 2$.



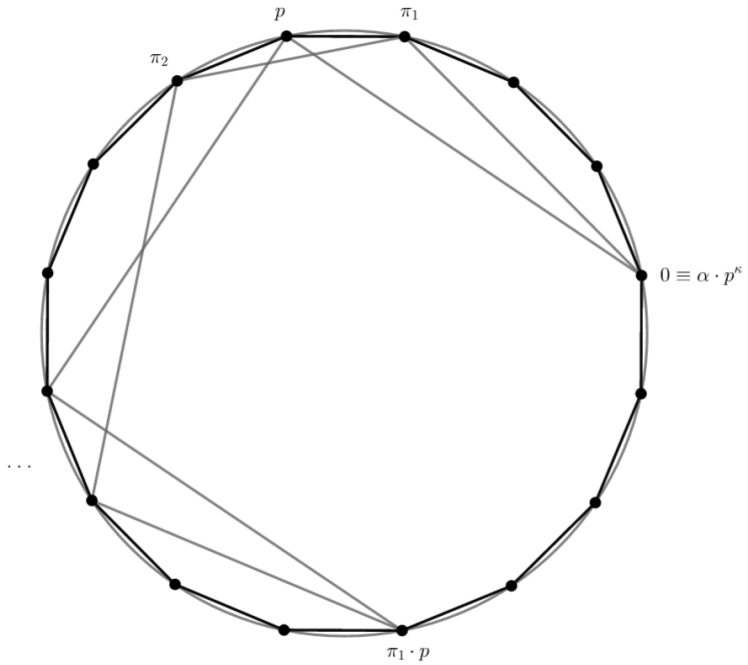
Σχήμα 11.2

Έτσι, λοιπόν, τα βήματα που δεν δημιουργούν διαδρομή που διέρχεται από όλα τα σημεία του κύκλου είναι τα πολλαπλάσια του α. Στον κύκλο των α^κ σημείων, ξεκινώντας με βήμα α μπορούμε να κατασκευάσουμε πολύγωνο που θα διατρέχει όλα τα πολλαπλάσια του α έως το α^κ, και το οποίο θα έχει πλήθος κορυφών $\dfrac{\alpha^\kappa}{\alpha} = \alpha^{\kappa-1}$, μιας και κάθε α σημεία του κύκλου αντιστοιχούν σε μια κορυφή του πολυγώνου. Έτσι, αφού το πολύγωνο έχει $\alpha^{\kappa-1}$ κορυφές, τα πολλαπλάσια του α έως το α^κ είναι στο πλήθος $\#(\lambda \cdot \alpha) = \alpha^{\kappa-1}$ και η συνάρτηση Φ στο α^κ θα είναι $\Phi(\alpha^\kappa) = \alpha^\kappa - \#(\lambda \cdot \alpha) \Rightarrow \Phi(\alpha^\kappa) = \alpha^\kappa - \alpha^{\kappa-1}$.

11.2 Η πολλαπλασιαστικότητα και ο τύπος της συνάρτησης Φ

Για να προσδιορίσουμε τον γενικό τύπο της συνάρτησης Φ πρώτα θα αποδείξουμε την πολλαπλασιαστικότητα της συνάρτησης Φ. Δηλαδή, θα δείξουμε ότι εάν $\alpha, \beta \in \mathbb{N}$ με $\mu\kappa\delta(\alpha, \beta) < 2$, τότε $\Phi(\alpha \cdot \beta) = \Phi(\alpha) \cdot \Phi(\beta)$.

Ξεκινώντας, ας θεωρίσουμε $\alpha \in \mathbb{N}$ και p ένας αριθμός πρώτος με $\mu\kappa\delta(\alpha, p) < 2$. Για $\kappa \in \mathbb{N}$, θα αποδείξουμε ότι $\Phi(\alpha \cdot p^{\kappa}) = \Phi(\alpha) \cdot \Phi(p^{\kappa})$.

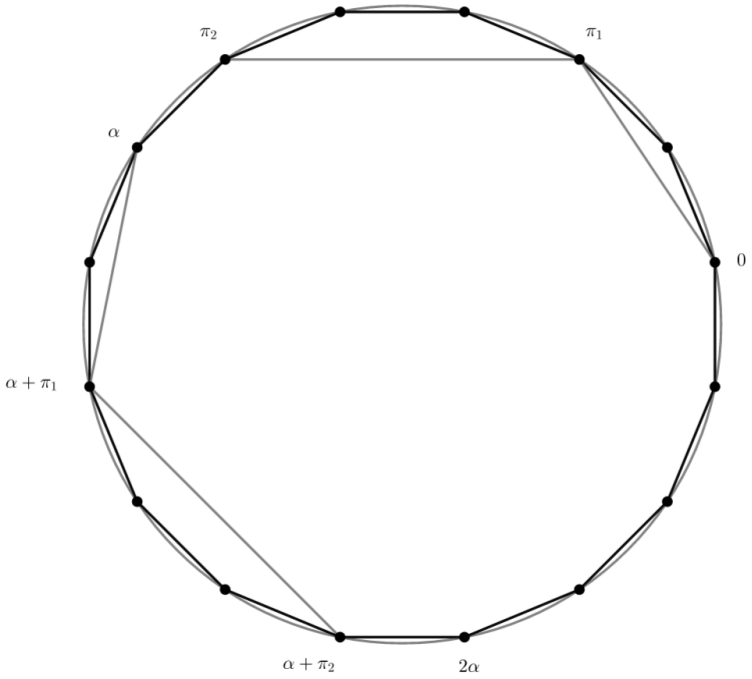


Σχήμα 11.3

Θεωρούμε π_i την οικογένεια των αριθμών που είναι μικρότεροι του α και που με το α έχουν κοινό διαιρέτη μεγαλύτερο ή ίσο του 2 και επίσης την διαδρομή που διέρχεται από καθένα από αυτά τα π_i καθώς και από τα αριθμητικά τους πολλαπλάσια επί ενός κύκλου $\alpha \cdot p^{\kappa}$ σημείων. Στον ίδιο κύκλο θεωρούμε ακόμη την διαδρομή που διέρχεται των πολλαπλασίων του πρώτου αριθμού p. Και οι 2 διαδρομές αυτές διέρχονται από αριθμούς που με τον $\alpha \cdot p^{\kappa}$ έχουν μεγαλύτερου του 1 κοινό διαιρέτη.

Το πλήθος των σημείων από τα οποία η 1^{η} διαδρομή διέρχεται ισχυριζόμαστε ότι είναι $\#(\pi_i) \cdot p^{\kappa}$. Πράγματι, επειδή το πλήθος των σημείων επί του κύκλου είναι $\alpha \cdot p^{\kappa}$, ο κύκλος μπορεί να χωριστεί σε p^{κ} τμήματα α σημείων το καθένα. Σε κάθε ένα από αυτά τα τμήματα βρίσκονται $\#(\pi_i)$ αριθμοί που με το $\alpha \cdot p^{\kappa}$ έχουν

κοινό διαιρέτη μεγαλύτερο του 1. Αυτό διότι για κάθε q τέτοιο ώστε $q = \lambda \cdot \pi_j$ ισχύει $q = \mu \cdot \alpha + w$ με $0 \leq w < \alpha$ και $\mu\kappa\delta(q, \alpha)$ διαιρεί το $w \to$ το w ανήκει στην οικογένεια των π_i· αντιστρόφως, κάθε αριθμός της μορφής $\mu \cdot \alpha + \pi_j$, είναι πολλαπλάσιο κάποιου π_i, αφού $\mu \cdot \alpha + \pi_j = \left(\mu \cdot \dfrac{\alpha}{\mu\kappa\delta(\alpha, \pi_j)} + \dfrac{\pi_j}{\mu\kappa\delta(\alpha, \pi_j)}\right) \cdot \mu\kappa\delta(\alpha, \pi_j)$ και προφανώς ο $\mu\kappa\delta(\alpha, \pi_j)$ ανήκει στην οικογένεια των π_i. Οπότε, αφού σε κάθε τμήμα α σημείων βρίσκονται $\#(\pi_i)$ αριθμοί της $1^{\eta\varsigma}$ διαδρομής, σε όλα τα p^κ τμήματα θα βρίσκονται $\#(\pi_i) \cdot p^\kappa$ σημεία της διαδρομής μας.



Σχήμα 11.4

Η 2^η διαδρομή που διέρχεται από όλα τα πολλαπλάσια του p εντός του κύκλου $\alpha \cdot p^\kappa$ σημείων είναι (κανονικό) πολύγωνο, αφού $\alpha \cdot p^\kappa \propto p$. Το πλήθος των σημείων αυτής της διαδρομής ισούται με το πλήθος των κορυφών του πολυγώνου και αυτό, με την σειρά του, ισούται με $\dfrac{\alpha \cdot p^\kappa}{p} = \alpha \cdot p^{\kappa-1}$, μιας και κάθε p σημεία αντιστοιχούν σε μία κορυφή.

Οπότε, λοιπόν, ίσως κανείς έλεγε ότι η συνάρτηση Φ στον $\alpha \cdot p^\kappa$ παίρνει τιμή $\alpha \cdot p^\kappa - \#(\pi_i) \cdot p^\kappa - \alpha \cdot p^{\kappa-1}$, αφού από το σύνολο των $\alpha \cdot p^\kappa$ αριθμών αφαιρούμε όλους τους αριθμούς που με τον $\alpha \cdot p^\kappa$ έχουν κοινό διαιρέτη μεγαλύτερο του 1. Αυτό όμως είναι λάθος, αφού δεν συνυπολογίσαμε ότι κάποιοι αριθμοί της $1^{\eta\varsigma}$ διαδρομής μπορεί να ταυτίζονται με αριθμούς της $2^{\eta\varsigma}$ διαδρομής.

Λαμβάνοντας και αυτήν την περίπτωση υπόψην, υπολογίζουμε το πλήθος των σημείων τομής της $1^{\eta\varsigma}$ και $2^{\eta\varsigma}$ διαδρομής. Από τους $\#(\pi_i)\cdot p^\kappa$ αριθμούς της $1^{\eta\varsigma}$ διαδρομής, ισχυριζόμαστε ότι $\#(\pi_i)\cdot p^{\kappa-1}$ αριθμοί ανήκουν στην 2^η διαδρομή. Πράγματι, εάν θεωρίσουμε $\lambda\cdot\pi_i\cdot p$ ένα πολλαπλάσιο των π_i και του p, επειδή $\lambda\cdot\pi_i=\mu\cdot\alpha+\pi_j$, έχουμε: $\lambda\cdot\pi_i\cdot p=\mu\cdot\alpha\cdot p+\pi_j\cdot p$. Επιπλέον, εφόσον $0\le\mu\cdot\alpha\cdot p\le\alpha\cdot p^\kappa\Rightarrow 0\le\mu\le p^{\kappa-1}\Rightarrow\#\mu=p^{\kappa-1}+1$. Από αυτό, επειδή στην ποσότητα $\mu\cdot\alpha\cdot p+\pi_j\cdot p$ για $0\le\mu\le p^{\kappa-1}-1$ (όχι $\mu=p^{\kappa-1}$, διότι τότε η προηγούμενη ποσότητα θα ξεπερνούσε το $\alpha\cdot p^\kappa$) τα π_j μπορούν να πάρουν $\#(\pi_i)$ τιμές για κάθε τιμή του μ, το συνολικό πλήθος των αριθμών που είναι πολλαπλάσια των π_i και του p είναι $\#(\pi_i)\cdot(p^{k-1}-1+1)=\#(\pi_i)\cdot p^{k-1}$.

Τελικά, μπορούμε να δούμε ότι $\Phi(\alpha\cdot p^\kappa)=\alpha\cdot p^\kappa-\#(\pi_i)\cdot p^\kappa-\alpha\cdot p^{\kappa-1}+\#(\pi_i)\cdot p^{\kappa-1}=\big(\alpha-\#(\pi_i)\big)\cdot\big(p^\kappa-p^{\kappa-1}\big)$.

Έχοντας υπόψην το προηγούμενο υποκεφάλαιο, παρατηρούμε ότι $p^\kappa-p^{\kappa-1}=\Phi(p^\kappa)$. Επειδή στην ποσότητα $\alpha-\#(\pi_i)$ από το σύνολο α αφαιρούμε το πλήθος των αριθμών που με το α έχουν κοινό διαιρέτη μεγαλύτερο του 1, θα πρέπει να ισχύει: $\Phi(\alpha)=\alpha-\#(\pi_i)$.

Ο ακόλουθος τύπος, λοιπόν, ισχύει όταν $\alpha\in\mathbb{N}$ και p πρώτος με $\mu\kappa\delta(\alpha,p)<2$:

$$\Phi(\alpha\cdot p^\kappa)=\Phi(\alpha)\cdot\Phi(p^\kappa)$$

Από τον τελευταίο τύπο προκύπτει η πολλαπλασιαστικότητα της Φ, αφού εάν

$$\alpha=\prod_{i\in[n]}p_i^{k_i},\beta=\prod_{i\in[m]\cap(n,\infty)}p_i^{k_i}$$

με $\mu\kappa\delta(\alpha,\beta)<2$, ισχύει ότι:

$$\Phi(\alpha)=\Phi\Big(\prod_{i\in[n]}p_i^{k_i}\Big)=\Phi\Big(\prod_{i\in[n-1]}p_i^{k_i}\cdot p_n^{k_n}\Big)=\Phi\Big(\prod_{i\in[n-1]}p_i^{k_i}\Big)\cdot\Phi(p_n^{k_n})=$$

$$\Phi\Big(\prod_{i\in[n-2]}p_i^{k_i}\cdot p_{n-1}^{k_{n-1}}\Big)\cdot\Phi(p_n^{k_n})=\Phi\Big(\prod_{i\in[n-2]}p_i^{k_i}\Big)\cdot\Phi(p_{n-1}^{k_{n-1}})\cdot\Phi(p_n^{k_n})=\cdots=\prod_{i\in[n]}\Phi(p_i^{k_i})$$

$$\Rightarrow\Phi(\alpha)=\prod_{i\in[n]}\Phi(p_i^{k_i})$$

και ομοίως:

$$\Phi(\beta)=\Phi\Big(\prod_{i\in[m]\cap(n,\infty)}p_i^{k_i}\Big)=\Phi\Big(\prod_{i\in[m-1]\cap(n,\infty)}p_i^{k_i}\cdot p_m^{k_m}\Big)=$$

$$\Phi\Big(\prod_{i\in[m-1]\cap(n,\infty)}p_i^{k_i}\Big)\cdot\Phi(p_m^{k_m})=\Phi\Big(\prod_{i\in[m-2]\cap(n,\infty)}p_i^{k_i}\cdot p_{m-1}^{k_{m-1}}\Big)\cdot\Phi(p_m^{k_m})=$$

$$\Phi\Big(\prod_{i\in[m-2]\cap(n,\infty)} p_i^{k_i}\Big)\cdot\Phi(p_{m-1}^{k_{m-1}})\cdot\Phi(p_m^{k_m}) = \cdots = \prod_{i\in[m]\cap(n,\infty)}\Phi(p_i^{k_i})$$

$$\Rightarrow \Phi(\beta) = \prod_{i\in[m]\cap(n,\infty)}\Phi(p_i^{k_i})$$

Οπότε:

$$\Phi(\alpha\cdot\beta) = \Phi\Big(\prod_{i\in[n]} p_i^{k_i}\cdot\prod_{i\in[m]\cap(n,\infty)} p_i^{k_i}\Big) = \Phi\Big(\prod_{i\in[m]} p_i^{k_i}\Big) = \Phi\Big(\prod_{i\in[m-1]} p_i^{k_i}\cdot p_m^{k_m}\Big) =$$

$$\Phi\Big(\prod_{i\in[m-1]} p_i^{k_i}\Big)\cdot\Phi(p_m^{k_m}) = \Phi\Big(\prod_{i\in[m-2]} p_i^{k_i}\cdot p_{m-1}^{k_{m-1}}\Big)\cdot\Phi(p_m^{k_m}) =$$

$$\Phi\Big(\prod_{i\in[m-2]} p_i^{k_i}\Big)\cdot\Phi(p_{m-1}^{k_{m-1}})\cdot\Phi(p_m^{k_m}) = \cdots = \prod_{i\in[m]}\Phi(p_i^{k_i}) \Rightarrow$$

$$\Phi(\alpha\cdot\beta) = \overbrace{\prod_{i\in[n]}\Phi(p_i^{k_i})}^{\Phi(\alpha)}\cdot\overbrace{\prod_{i\in[m]\cap(n,\infty)}\Phi(p_i^{k_i})}^{\Phi(\beta)} = \Phi(\alpha)\cdot\Phi(\beta)$$

Τέλος, χρησιμοποιώντας την πολλαπλασιαστικότητα της Φ, με ακριβώς ανάλογη μέθοδο, είναι δυνατόν να δείξουμε ότι για κάθε $x\in\mathbb{N}$ με:

$$x = \prod_{i\in[n]} p_i^{k_i}$$

ισχύει:

$$\Phi(x) = \prod_{i\in[n]}(p_i^{k_i} - p_i^{k_i-1})$$

Πράγματι:

$$\Phi(x) = \Phi\Big(\prod_{i\in[n]} p_i^{k_i}\Big) = \Phi\Big(\prod_{i\in[n-1]} p_i^{k_i}\cdot p_n^{k_n}\Big) = \Phi\Big(\prod_{i\in[n-1]} p_i^{k_i}\Big)\cdot\Phi(p_n^{k_n}) =$$

$$\Phi\Big(\prod_{i\in[n-2]} p_i^{k_i}\cdot p_{n-1}^{k_{n-1}}\Big)\cdot\Phi(p_n^{k_n}) = \Phi\Big(\prod_{i\in[n-2]} p_i^{k_i}\Big)\cdot\Phi(p_{n-1}^{k_{n-1}})\cdot\Phi(p_n^{k_n}) = \cdots = \prod_{i\in[n]}\Phi(p_i^{k_i})$$

$$\Rightarrow \Phi(x) = \prod_{i\in[n]}\Phi(p_i^{k_i}) = \prod_{i\in[n]}(p_i^{k_i} - p_i^{k_i-1})$$

.

Κεφάλαιο 12

Διωνυμικό ανάπτυγμα

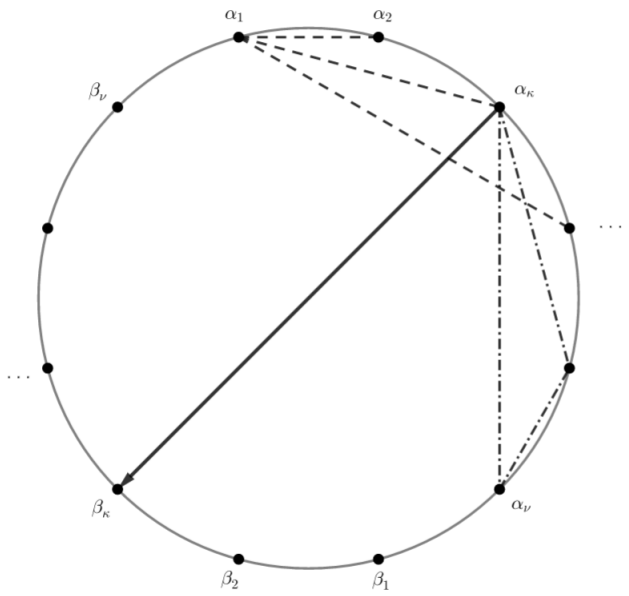
12.1 Ο τύπος του διωνυμικού αναπτύγματος

Στο κεφάλαιο αυτό θα προσδιορίσουμε τον τύπο του αναπτύγματος $(\alpha+\beta)^\nu$ όταν $\nu \in \mathbb{N}$. Συγκεκριμένα, θα αποδείξουμε ότι εάν $A = (\alpha+\beta)^\nu$, τότε $A = \sum_{i\in[\nu]\cup\{0\}} \frac{\nu!}{i!\cdot(\nu-i)!}\cdot\alpha^i\cdot\beta^{\nu-i}$.

Πριν προχωρίσουμε στην γεωμετρική απόδειξη, θα παραστήσουμε ισοδύναμα το A ως $A = \overbrace{(\alpha+\beta)\cdot(\alpha+\beta)\cdot\cdots\cdot(\alpha+\beta)}^{\nu}$ και θα παρατηρίσουμε ότι λόγω του επιμερισμού του πολλαπλασιασμού, κάθε στοιχείο εντός μιας παρενθέσεως θα πολλαπλασιαστεί με κάθε άλλο στοιχείο κάθε άλλης παρένθεσης (όχι ταυτόχρονα, βέβαια), στο σύνολο των όρων του αναπτύγματος. Δηλαδή, θα υπάρχουν όροι του αναπτύγματος στους οποίους θα μπορεί να βρεθεί το α της κ παρένθεσης πολλαπλασιασμένο με το β της $\lambda \neq \kappa$ παρένθεσης, ή με το α της $\mu \neq \kappa, \lambda$ παρένθεσης. Επίσης, επειδή κατά την κατασκευή των όρων του αναπτύγματος διαλέγουμε ένα στοιχείο από κάθε παρένθεση και τα πολλαπλασιάζουμε μεταξύ τους, και ακόμη το πλήθος των παρενθέσεων είναι ν, κάθε όρος του αναπτύγματος αποτελείται ακριβώς ν όρους α και β. Αυτό σημαίνει ότι εάν $\alpha^\kappa\cdot\beta^\lambda$ είναι ένας όρος του αναπτύγματος, θα πρέπει $\kappa+\lambda=\nu \Rightarrow \lambda = \nu-\kappa$.

Έχοντας, λοιπόν, αυτά υπόψην, ξεκινούμε την απόδειξη.

Κατασκευάζουμε έναν κύκλο και επί αυτού σε ένα ημικύκλιό του τοποθετούμε ν στο πλήθος σημεία που αντιστοιχούν στα α των ν παρενθέσεων. Τα σημεία αυτά συμβολίζουμε με α_i και θεωρούμε ότι κάθε σημείο α_i αντιστοιχεί στο α της $i-$οστής παρενθέσεως. Αντιδιαμετρικά κάθε α_i σημείου τοποθετούμε σημεία β_i που ομοίως αντιστοιχούν στα β των παρενθέσεων.



Σχήμα 12.1

Αφού κάθε παρένθεση έχει εντός της ένα α και ένα β, εάν κατά τους πολλαπλασιασμούς μας δεν επιλέξουμε από μία παρένθεση το α, επιλέγουμε οποσδήποτε το β. Στον κύκλο, εάν δεν επιλέξουμε κάποιο α_κ σημείο, οποσδήποτε διαλέγουμε το αντιδιαμετρικό του β_κ. Για την μελέτη, λοιπόν, των όρων, αρκεί να μελετήσουμε το πλήθος των α κάθε όρου του αναπτύγματος.

Εάν υποθέσουμε ότι από τις παρενθέσεις διαλέγουμε μόνο έαν α, ο όρος του αναπτύγματός μας είναι $\alpha \cdot \beta^{\nu-1}$. Για να κατασκευάσουμε, όμως, αυτόν τον όρο, μπορούμε να διαλέξουμε οποιοδήποτε α από τις ν παρενθέσεις, το οποίο σημαίνει ότι ν στο πλήθος όροι $\alpha \cdot \beta^{\nu-1}$ μπορούν να κατασκευαστούν στο ανάπτυγμα. Ισοδύναμα, από την περιφέρεια του κύκλου, μπορούμε να διαλέξουμε οποιοδήποτε από τα ν στο πλήθος α_i για να κατασκευάσουμε τον $\alpha \cdot \beta^{\nu-1}$· το πλήθος των σημείων αντιστοιχεί στο πλήθος των όρων με ένα α.

Εάν διαλέξουμε, εν συνεχεία, δύο α, είναι σαν να επιλέγουμε 2 σημεία α_i επί του κύκλου. Οπότε, το πλήθος των διαφορετικών ευθυγράμμων τμημάτων που μπορούν να κατασκευαστούν με άκρα α_i αντιστοιχεί στο πλήθος των όρων με δύο α. Ας υποθέσουμε ότι $\alpha_1\alpha_j$ είναι ένα ευθύγραμμο τμήμα. Κρατώντας το α_1 σταθερό, το α_j μπορεί να βρίσκεται σε $\nu - 1$ θέσεις. Συνεχίζοντας σε ευθύγραμμο τμήμα $\alpha_2\alpha_j$, το α_j πάλι μπορεί να βρίσκεται σε $\nu - 1$ θέσεις, όμως η διαφορά εδώ είναι ότι το ευθύγραμμο τμήμα $\alpha_1\alpha_2$ καλύφθηκε στην προηγούμενη περίπτωση. Οπότε, δημιουργούνται $\nu - 2$ διαφορετικά ευθύγραμμα τμήματα. Με ακριβώς ανάλογο τρόπο μπορούμε να δείξουμε ότι το σύνολο των ευθυγράμμων τμημάτων είναι $(\nu - 1) + (\nu - 2) + (\nu - 3) + \cdots + 1$. Ο αριθμός αυτός είναι τρίγωνος και,

συνεπώς, παίρνει την μορφή $\dfrac{\nu \cdot (\nu-1)}{2}$.

Στην περίπτωση των τριών α, επιλέγουμε επί του κύκλου 3 σημεία. Οπότε, το πλήθος των διαφορετικών τριγώνων που μπορούν να κατασκευαστούν με κορυφές α_i αντιστοιχεί στο πλήθος των όρων με τρία α. Εδώ παρατηρούμε ότι επειδή κάθε τρίγωνο αποτελείται από 3 κορυφές $\alpha_i, \alpha_j, \alpha_w$, θεωρώντας $\alpha_i\alpha_j$ να είναι σταθερό ευθύγραμμο τμήμα, το α_w μπορεί να κινηθεί σε $\nu-2$ θέσεις. Οπότε, κανείς ίσως έλεγε ότι επειδή το πλήθος των ευθυγράμμων τμημάτων είναι $\dfrac{\nu \cdot (\nu-1)}{2}$, το πλήθος των τριγώνων είναι $\dfrac{\nu \cdot (\nu-1) \cdot (\nu-2)}{2}$. Αυτό όμως δεν είναι σωστό, μιας και κάθε τρίγωνο $\alpha_i\alpha_j\alpha_w$ μπορεί να κατασκευαστεί θεωρώντας ως σταθερά ευθύγραμμα τμήματα τα $\alpha_i\alpha_j$ ή $\alpha_i\alpha_w$ ή $\alpha_j\alpha_w$, οπότε, ουσιαστικά, δημιουργείται με τον προηγούμενο τρόπο, τριπλάσιος αριθμός τριγώνων. Διαιρώντας, λοιπόν, με το 3, παίρνουμε το πραγματικό πλήθος $\dfrac{\nu \cdot (\nu-1) \cdot (\nu-2)}{2 \cdot 3}$.

> *Εδώ να διευκρινήσουμε τα πολύγωνα που μελετούμε είναι όλα της μορφής* $\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_\kappa}$ *με* $i_1 < i_2 < \cdots < i_\kappa$. *Μελετούμε μόνο τέτοια πολύγωνα, διότι, διαφορετικά, πολύγωνα όπως τα* $\alpha_1\alpha_2\alpha_3\alpha_4$ *και* $\alpha_1\alpha_3\alpha_2\alpha_4$, *παρόλο που αντιστοιχούν στον ίδιο όρο του αναπτύγματος, δεν ταυτίζονται. Οπότε τελικά το πλήθος των όρων θα έβγαινε μεγαλύτερο του πραγματικού. Ουσιαστικά, κάθε πολύγωνο καθορίζεται από τις κορυφές του και όχι από τις συνδέσεις μεταξύ των κορυφών του.*

Συνεχίζοντας με τον ίδιο τρόπο, βρίσκουμε ότι:

1. Το πλήθος των σημείων = Το πλήθος των όρων $\alpha \cdot \beta^{\nu-1} = \nu$
2. Το πλήθος των ευθυγράμμων τμημάτων = Το πλήθος των όρων $\alpha^2 \cdot \beta^{\nu-2} = \dfrac{\nu \cdot (\nu-1)}{2}$
3. Το πλήθος των τριγώνων = Το πλήθος των όρων $\alpha^3 \cdot \beta^{\nu-3} = \dfrac{\nu \cdot (\nu-1) \cdot (\nu-2)}{2 \cdot 3}$
4. Το πλήθος των τετραγώνων = Το πλήθος των όρων $\alpha^4 \cdot \beta^{\nu-4} = \dfrac{\nu \cdot (\nu-1) \cdot (\nu-2) \cdot (\nu-3)}{2 \cdot 3 \cdot 4}$

... ...

κ. Το πλήθος των $\kappa-$γώνων = Το πλήθος των όρων $\alpha^\kappa \cdot \beta^{\nu-\kappa} = \dfrac{\nu!}{\kappa! \cdot (\nu-\kappa)!}$

... ...

ν. Πλήθος των $\nu-$γώνων = Το πλήθος των όρων $\alpha^\nu = 1$

0. Προφανώς, το πλήθος των όρων που δεν έχουν α = Το πλήθος των όρων $\beta^\nu = 1$, μιας και υπάρχει μοναδικό $\nu-$γωνο με κορυφές β_i, επειδή το πλήθος των β_i είναι ν.

Συνεπώς, το ανάπτυγμα του A θα πρέπει να είναι:

$$A = (\alpha+\beta)^{\nu} = \beta^{\nu} + \nu\cdot\alpha\cdot\beta^{\nu-1} + \frac{\nu\cdot(\nu-1)}{2}\cdot\alpha^2\cdot\beta^{\nu-2} + \dots$$

$$+\frac{\nu!}{\kappa!\cdot(\nu-\kappa)!}\cdot\alpha^{\kappa}\cdot\beta^{\nu-\kappa} + \dots + \alpha^{\nu} = \sum_{i\in[\nu]\cup\{0\}} \frac{\nu!}{i!\cdot(\nu-i)!}\cdot\alpha^{i}\cdot\beta^{\nu-i}$$

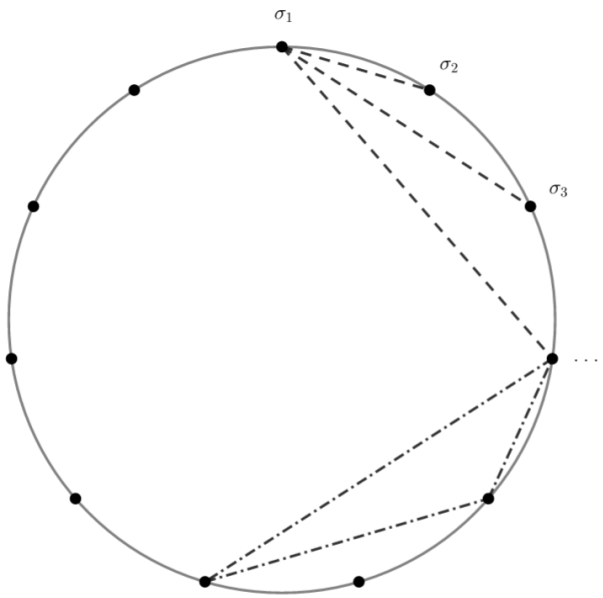
$$\Rightarrow A = (\alpha+\beta)^{\nu} = \sum_{i\in[\nu]\cup\{0\}} \frac{\nu!}{i!\cdot(\nu-i)!}\cdot\alpha^{i}\cdot\beta^{\nu-i}$$

12.2 Εφαρμογή του διωνυμικού αναπτύγματος στα δυναμοσύνολα

Έστω Σ ένα σύνολο $\Sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_\nu\}$. Θα καλούμε δυναμοσύνολο $\mathcal{P}(\Sigma)$ του Σ το σύνολο αυτό που περιέχει όλα τα δυνατά υποσύνολα του Σ. Δηλαδή, $\forall A \subseteq \Sigma$, $A \in \mathcal{P}(\Sigma)$.

Εμείς χρησιμοποιώντας τον τύπο του διωνυμικού αναπτύγματος που αποδείξαμε στο προηγούμενο κεφάλαιο, θα δείξουμε ότι $|\mathcal{P}(\Sigma)| = 2^{|\Sigma|}$.

Θεωρούμε ότι $\Sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_\nu\}$ έχει ν στοιχεία ($|\Sigma| = \nu$). Στην περιφέρεια ενός κύκλου τοποθετούμε ν σημεία που αντιστοιχούν στα σ_i του συνόλου Σ.



Σχήμα 12.2

Τα υποσύνολα του Σ που είναι μονοσύνολα, επειδή περιέχουν ένα στοιχείο μόνον το καθένα, θα αντιστοιχούν σε ένα σημείο του κύκλου. Το πλήθος, συνεπώς, των διαφορετικών μονοσυνόλων θα είναι όσο το πλήθος των σημείων· δηλαδή ν.

Τα υποσύνολα του Σ που είναι δισύνολα, επειδή περιέχουν δύο στοιχεία το καθένα, θα αντιστοιχούν σε ένα ευθύγραμμο τμήμα του κύκλου. Όπως και στην περίπτωση του διωνυμικού αναπτύγματος, μπορούμε να δείξουμε ότι το πλήθος των ευθυγράμμων τμημάτων εντός του κύκλου είναι $\dfrac{\nu \cdot (\nu - 1)}{2}$.

Αντίστοιχα, τα υποσύνολα του Σ που είναι τρισύνολα, επειδή περιέχουν τρία στοιχεία το καθένα, θα αντιστοιχούν σε ένα τρίγωνο του κύκλου. Όμοια πάλι με την περίπτωση του διωνυμικού αναπτύγματος, μπορούμε να δείξουμε ότι το πλήθος των τριγώνων είναι $\dfrac{\nu \cdot (\nu-1) \cdot (\nu-2)}{2 \cdot 3}$.

Γενικά για τα υποσύνολα του Σ που είναι $\kappa-$σύνολα, επειδή περιέχουν $\kappa-$στοιχεία το καθένα, θα αντιστοιχούν σε $\kappa-$γωνα του κύκλου. Οπότε, το πλήθος τους θα είναι $\dfrac{\nu!}{\kappa! \cdot (\nu-\kappa)!}$.

Προσθέτωντας τα πλήθη των διαφορετικών μη κενών υποσυνόλων του Σ βρίσκουμε ότι ο συνολικός αριθμός τους είναι:

$$\nu + \frac{\nu \cdot (\nu-1)}{2} + \frac{\nu \cdot (\nu-1) \cdot (\nu-2)}{2 \cdot 3} + \cdots + \frac{\nu!}{\kappa! \cdot (\nu-\kappa)!} + \cdots + 1 =$$

$$\left(1 + \nu + \frac{\nu \cdot (\nu-1)}{2} + \frac{\nu \cdot (\nu-1) \cdot (\nu-2)}{2 \cdot 3} + \cdots + \frac{\nu!}{\kappa! \cdot (\nu-\kappa)!} + \cdots + 1\right) - 1$$

Όμως από τον τύπο του διωνυμικού αναπτύγματος μπορούμε να δούμε ότι:

$$2^\nu = (1+1)^\nu = 1^\nu + \nu \cdot 1^\nu \cdot 1^{\nu-1} + \cdots + \frac{\nu!}{\kappa! \cdot (\nu-\kappa)!} \cdot 1^\kappa \cdot 1^{\nu-\kappa} + \cdots + 1^\nu =$$

$$1 + \nu + \frac{\nu \cdot (\nu-1)}{2} + \frac{\nu \cdot (\nu-1) \cdot (\nu-2)}{2 \cdot 3} + \cdots + \frac{\nu!}{\kappa! \cdot (\nu-\kappa)!} + \cdots + 1$$

Συνεπώς:

$$\left(1 + \nu + \frac{\nu \cdot (\nu-1)}{2} + \frac{\nu \cdot (\nu-1) \cdot (\nu-2)}{2 \cdot 3} + \cdots + \frac{\nu!}{\kappa! \cdot (\nu-\kappa)!} + \cdots + 1\right) - 1 =$$

$$2^\nu - 1$$

Οπότε, όλα τα μη κενά υποσύνολα του Σ είναι στον αριθμό $2^\nu - 1$. Επειδή όμως και το κενό σύνολο είναι υποσύνολο του Σ, τελικά παίρνουμε:

$$|\mathcal{P}(\Sigma)| = 2^\nu - 1 + 1 = 2^\nu = 2^{|\Sigma|}$$

Κεφάλαιο 13

Μικρό θεώρημα του Φερμά

Το τελευταίο θεώρημα με το οποίο θα ασχοληθούμε στα πλάισια αυτής της εργασίας είναι το Μικρό θεώρημα του $Fermat$. Σύμφωνα με αυτό το θεώρημα, εάν p είναι αριθμός πρώτος και $\alpha \not\propto p$ είναι φυσικός αριθμός, ισχύει ότι:

$$\alpha^{p-1}\mathbb{O}p = 1$$

Για το θεώρημα αυτό θα δώσουμε μια απόδειξη και μια γενίκευση. Αρχικά, χρησιμοποιώντας τον τύπο του διωνυμικού αναπτύγματος που αποδείξαμε προηγουμένως, αποδεικνύουμε το θεώρημα αυτό καθαυτό.

Θεωρούμε το ανάπτυγμα του $(\alpha - 1)^p$:

$$(\alpha + (-1))^p = \alpha^p - p \cdot \alpha^{p-1} + \frac{p \cdot (p-1)}{2} \cdot \alpha^{p-2} + \cdots - 1$$

Επειδή ο γενικός όρος $\dfrac{p!}{\kappa! \cdot (p-\kappa)!}$ είναι πάντοτε πολλαπλάσιο του p, όταν $\kappa \neq 0, p$, για την προηγούμενη ποσότητα ισχύει: $(\alpha - 1)^p\mathbb{O}p = \alpha^p - 1$.

Για την περίπτωση $\beta = \alpha - 1$:
Εάν θεωρίσουμε $\beta = \alpha - 1$ και εφαρμόσουμε την προηγούμενη ισοτιμία για β, παίρνουμε:

$$(\alpha - 2)^p\mathbb{O}p = (\alpha - 1)^p - 1$$

Όμως, σύμφωνα με ό,τι δείξαμε:

$$(\alpha - 2)^p\mathbb{O}p = ((\alpha - 1)^p - 1)\mathbb{O}p = \alpha^p - 1 - 1 = \alpha^p - 2$$

Για την περίπτωση $\beta = \alpha - 2$:
Συνεχίζοντας με $\beta = \alpha - 2$ χρησιμοποιώντας την πρώτη ισοτιμία, παίρνουμε:

$$(\alpha - 3)^p\mathbb{O}p = (\alpha - 2)^p - 1$$

Εφαρμόζοντας στο προηγούμενο την τρίτη ισοτιμία:

$$(\alpha-3)^p \mathbb{O} p = ((\alpha-2)^p - 1)\mathbb{O}p = \alpha^p - 2 - 1 = \alpha^p - 3 \Rightarrow$$

$$(\alpha-3)^p \mathbb{O} p = \alpha^p - 3$$

Για την περίπτωση $\beta = \alpha - (\alpha-1) = 1$**:**
Συνεχίζοντας με ακριβώς ανάλογο τρόπο την διαδικασία, μπορούμε να βρούμε ότι, για την περίπτωση $\beta = \alpha - (\alpha-1) = 1$, ισχύει:

$$(\alpha-(\alpha-1))^p \mathbb{O} p = \alpha^p - (\alpha-1) \Rightarrow 1^p \mathbb{O} p = \alpha^p - \alpha + 1 \Rightarrow (\alpha^p - \alpha + 1)\mathbb{O}p = 1 \Rightarrow$$

$$\alpha^p \mathbb{O} p = \alpha$$

Επειδή υποθέσαμε ότι $\alpha \not\propto p$ και p πρώτος, μεταξύ των α και p δεν υπάρχει κοινός διαιρέτης μεγαλύτερος του 1. Έτσι, θα υπάρχει $\alpha' \in \mathbb{N}$ τέτοιος ώστε $(\alpha \cdot \alpha')\mathbb{O}p = 1$. Οπότε:

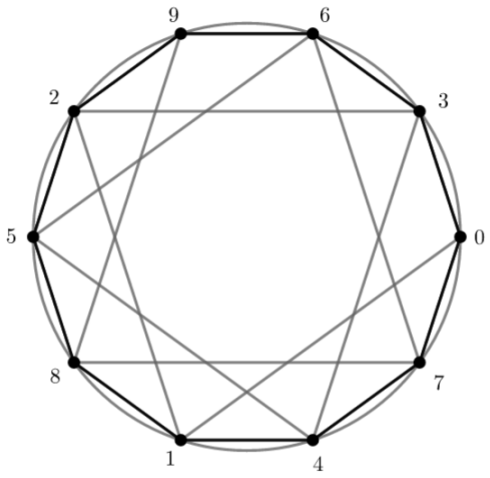
$$\alpha^p \mathbb{O} p = \alpha \Rightarrow (\alpha^p \cdot \alpha')\mathbb{O}p = \alpha \cdot \alpha' \Rightarrow \alpha^{p-1}\mathbb{O}p = 1$$

Το θεώρημα αυτό του $Fermat$ θα το γενικεύσουμε αποδεικνύοντας ότι για φυσικούς α, n που μεταξύ τους δεν έχουν κοινό διαιρέτη μεγαλύτερο της μονάδας ισχύει: $\alpha^{\Phi(n)}\mathbb{O}n = 1$. Ειδικά για την περίπτωση όπου n πρώτος, $\Phi(n) = n-1 \Rightarrow \alpha^{n-1}\mathbb{O}n = 1$, όπως άλλωστε αποδείξαμε.

Αρχικά, όπως δείξαμε στο κεφάλαιο της συνάρτησης Φ, εάν n είναι φυσικός αριθμός, ο αριθμός $\Phi(n)$ μας δείχνει με πόσα διαφορετικά βήματα μπορούν, εντός ενός κύκλου n σημείων, να φτιαχθούν διαδρομές που διέρχονται από κάθε σημείο του κύκλου. Ας υποθέσουμε κ_i είναι η οικογένεια των βημάτων που κατασκευάζουν τέτοιες διαδρομές. Ισχύει ότι, εάν α, n μεταξύ τους δεν έχουν κοινό διαιρέτη μεγαλύτερο της μονάδας, η οικογένεια $\alpha \cdot \kappa_i$ και η οικογένεια κ_i ταυτίζονται.

Πράγματι, εάν $\mu\kappa\delta(\alpha, n) < 2$, το $\alpha \cdot \kappa_i$ δεν έχει με το n κοινό διαιρέτη μεγαλύτερο της μονάδας, οπότε η διαδρομή με βήμα $\alpha \cdot \kappa_i$ διέρχεται από όλα τα σημεία του κύκλου n σημείων $\rightarrow$ το $\alpha \cdot \kappa_i$ ανήκει στην οικογένεια των κ_i. Επίσης, εάν για $i \neq j$ ισχύει $(\alpha \cdot \kappa_i)\mathbb{O}n = \alpha \cdot \kappa_j$, επειδή $\mu\kappa\delta(\alpha, n) < 2$, υπάρχει $\alpha' : \alpha' \cdot \alpha \mathbb{O} n = 1 \rightarrow \kappa_i \mathbb{O} n = \kappa_j$. Αυτό είναι άτοπο, αφού η οικογένεια κ_i περιέχει διαφορετικά βήματα στον κύκλο των n σημείων.

Συνεπώς η οικογένεια $\alpha \cdot \kappa_i$ έχει στοιχεία που ανήκουν όλα τους στην οικογένεια κ_i. Επειδή τα στοιχεία της $\alpha \cdot \kappa_i$ είναι διαφορετικά ανά 2, η οικογένεια αυτή έχει τόσα στοιχεία όσα έχει η κ_i. Οπότε, οι $\alpha \cdot \kappa_i$ και κ_i ταυτίζονται.



Σχήμα 13.1: *Στον κύκλο των* 10 *σημείων, η διαδρομή με βήμα* $27 = 9 \cdot 3$ *ταυτίζεται της διαδρομής βήματος* 7

Από αυτό παίρνουμε το ζητούμενο, αφού:

$$\Big(\prod_{i\in[\Phi(n)]} \alpha\cdot\kappa_i\Big)\mathbb{O}n = \prod_{i\in[\Phi(n)]} \kappa_i \Rightarrow \Big(\alpha^{\Phi(n)}\cdot \prod_{i\in[\Phi(n)]} \kappa_i\Big)\mathbb{O}n = \prod_{i\in[\Phi(n)]} \kappa_i$$

Επειδή καθένα από τα κ_i με τον n δεν έχει κοινό διαιρέτη μεγαλύτερο του 1, θα ισχύει $\mu\kappa\delta\Big(\prod_{i\in[\Phi(n)]} \kappa_i, n\Big) < 2$. Οπότε, υπάρχει $\kappa : \Big(\kappa\cdot \prod_{i\in[\Phi(n)]} \kappa_i\Big)\mathbb{O}n = 1$. Άρα,

$$\Big(\alpha^{\Phi(n)}\cdot\kappa\cdot \prod_{i\in[\Phi(n)]} \kappa_i\Big)\mathbb{O}n = \kappa\cdot \prod_{i\in[\Phi(n)]} \kappa_i \Rightarrow \alpha^{\Phi(n)}\mathbb{O}n = 1$$

Κεφάλαιο 14

Επίλογος

Με την τεράστια πρόοδο της Φυσικής και της Πληροφορικής τον 20-21^ο αιώνα, έγινε πλέον πασιφανές ότι η θέση των θεωριτικών Μαθηματικών είναι αδιαμφισβήτητης σημασίας στον χώρο της επιστήμης. Τα θεωρητικά Μαθηματικά όχι μόνον μπορούν και παρέχουν Μαθηματικές λύσεις και αφηρημένα Μαθηματικά μοντέλα για προβλήματα πέρα των Μαθηματικών, αλλά επίσης δύνανται να γενικεύσουν έννοιες / ερευνητικά αποτελέσματα από άλλες επιστήμες σε Μαθηματικές αρχές, από τις οποίες, εν συνεχεία, μπορεί να κτιστεί ένα νέο Μαθηματικό δημιούργημα. Η σχέση, λοιπόν, θεωρίας και εφαρμογής είναι ισχυρότατη στον χώρο της επιστήμης και για την επιστημονική πρόοδο χρειάζεται συνδιασμός και των δύο. Γι΄ αυτό θεωρώ σφάλμα οι ασχολούμενοι με τα θεωρητικά Μαθηματικά να αποκτούν νοοτροπία ''μέγιστης αποδοτικότητας'', βρίσκοντας πάντα τον ευκολότερο (ή συντομότερο, αν και αυτό δεν είναι πάντα εύκολο) τρόπο επίλυσης προβλημάτων. Στα θεωρητικά μαθηματικά, επειδή ακριβώς από την φύση τους είναι αρκετά αφηρημένα, κατα την γνώμη μου, κάθε έννοια πρέπει να ερμηνεύεται με τον ελκυστικότερο δυνατό τρόπο, ακόμη κι αν είναι δυσκολότερος ή περιπλοκότερος ενός άλλου γνωστού τρόπου, είτε χρησιμοποιώντας μέσα οπτικής, όπως είναι η γεωμετρία, είτε με συνδιασμό πολλών Μαθηματικών κλάδων. Αυτό για 2 λόγους: πρώτον, τα Μαθηματικά δεν πρόκειται να εξελιχθούν εάν δεν υπάρχει κανείς να ασχοληθεί για να τα εξελίξει και δεύτερον, εάν οι εκπρόσωποι του θεωρητικού και εφαρμοσμένου τμήματος της επιστήμης σκέφτονται με τον ίδιο ακριβώς τρόπο, δεν θα υπάρχει σφαιρικότητα στην αντίληψη των μαθηματικών εννοιών και συνεπώς η πρόοδος της επιστήμης θα επιβραδύνει.

Βιβλιογραφία

[1] *L.E. Dickson. History of the Theory of Numbers. Chelsea*, Νέα Υόρκη, 1984.

[2] Δημήτρης Ι. Δεριζιώτης. *Μια εισαγωγή στην Θεωρία αριθμών, Β΄ Έκδοση*. Εκδόσεις Σοφία, Θεσσαλονίκη, 2012.

[3] Εγώ.