1. ΟΙ ΦΥΣΙΚΟΙ, ΟΙ ΑΚΕΡΑΙΟΙ ΚΑΙ ΟΙ ΡΗΤΟΙ ΑΡΙΘΜΟΙ

1.1. Οι φυσικοί αριθμοί είναι οι 0, 1, 2, 3, 4, 5, ... Το σύνολο τους συμβολίζεται με $\mathcal{N}$. Γράφουμε λοιπόν $\mathcal{N}$={0, 1, 2, 3, ...}. Τα αποσιωπητικά υποδηλώνουν ότι οι αριθμοί συνεχίζονται επ΄ άπειρον. Το πλήθος των φυσικών αριθμών είναι άπειρο. Κάθε φυσικός αριθμός ν έχει και ένα επόμενο τον ν+1. Ο επόμενος του 2 είναι ο 3, ο επόμενος του 5 είναι ο 6. Κάθε φυσικός αριθμός εκτός από το 0 είναι και επόμενος κάποιου άλλου φυσικού αριθμού: Ο 56 είναι επόμενος του 55, ο 13 είναι επόμενος του 12. Κάθε φυσικός αριθμός είναι μικρότερος του επομένου του. Ο 0 είναι ο πιο μικρός φυσικός αριθμός. ΄Ομως δεν υπάρχει φυσικός αριθμός που να είναι πιο μεγάλος από τους άλλους φυσικούς αριθμούς. Μερικές φορές χρειάζεται να εργασθούμε με μη μηδενικούς φυσικούς αριθμούς. Το σύνολο τους το συμβολίζουμε με $\mathcal{N}^*$. Είναι δηλαδή $\mathcal{N}^*$ ={0, 1, 2, 3, ...}. Συνήθως (αλλά όχι και απαραιτήτως) χρησιμοποιούμε «ενδιάμεσα» γράμματα της αλφαβήτου για να συμβολίσουμε τους φυσικούς αριθμούς: κ, λ, μ, ν, k, m, n. Λέγοντας ο *«φυσικός αριθμός ν»* εννοούμε, αν δεν προσδιορίζεται κάτι διαφορετικό, ένα οποιοδήποτε αριθμό μικρό ή μεγάλο. ΄Ομως κάθε φορά πρόκειται για ένα αριθμό και όχι για το άπειρο. Για παράδειγμα το άθροισμα $\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+...+\frac{1}{\nu}$ είναι το άθροισμα όλων των κλασμάτων πού έχουν αριθμητή 1 και των οπίων ο παρονομαστής παίρνει όλες τις τιμές από 1 έως ν. Το άθροισμα αυτό δεν έχει βέβαια 4 προσθετέους επειδή φαίνονται μόνο 4 διότι αποσιωπώνται και κάποιοι προσθετέοι που η ύπαρξη τους εννοείται. Είναι άσκοπο (αλλά και ανέφικτο όταν ο ν είναι μεγάλος) να γραφούν όλοι. Το πλήθος των προσθετέων του αθροίσματος αυτού είναι ν. Το πλήθος είναι 4 όταν ο ν είναι 4. Το πλήθος είναι 1 όταν ο ν είναι 1. Σε καμία όμως περίπτωση το πλήθος δεν είναι άπειρο.

1.2. Να βρείτε το πλήθος των προσθετέων στα παρακάτω αθροίσματα

$$\frac{1}{2}+\frac{1}{5}+\frac{1}{10}+...+\frac{1}{\nu^2+1}$$

$$1+p+p^2+p^3+...+p^n$$

$$1+1\cdot 2+1\cdot 2\cdot 3+...+1\cdot 2\cdot 3\cdot ...\cdot n$$

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+...+\frac{1}{2^k+1}$$

1.3. Να βρείτε το πλήθος των παραγόντων στα παρακάτω γινόμενα

$$(1+1)(1+x)(1+x^2)...(1+x^\nu)$$

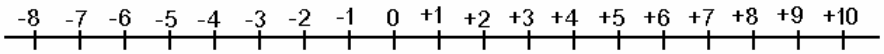
$$(1+1)(1+x)(1+x^2)(1+x^3)...(1+x^{2^\nu})$$

$$(1+1)(1+x^2)(1+x^4)...(1+x^{2^\nu})$$

1.4. Ο επόμενος του 3x-2 είναι ο 31. Ποιο είναι ο x;

1.5. Τίνων φυσικών αριθμών το τετράγωνο είναι 81;

1.6. Οι ακέραιοι αριθμοί είναι όπως απλά μπορούμε να πούμε οι φυσικοί αριθμοί και οι αντίθετοι τους δηλαδή οι 0, ±1, ±2, ±3, ... Το σύνολο των ακεραίων συμβολίζεται με $\mathbb{Z}$ δηλαδή $\mathbb{Z}$={0, ±1, ±2, ±3, ...}. Με $\mathbb{Z}^*$ συμβολίζουμε το σύνολο των μη μηδενικών ακεραίων δηλαδή $\mathbb{Z}^*$ ={ ±1, ±2, ±3, ...}. Οι ακέραιοι αριθμοί είναι και αυτοί άπειροι όπως οι φυσικοί αριθμοί όμως όχι μόνο δεν υπάρχει ακέραιος αριθμός που να είναι πιο μεγάλος από τους άλλους αλλά δεν υπάρχει ούτε ακέραιος αριθμός που να είναι πιο μικρός από τους άλλους. Αν παραστήσουμε τους ακέραιους αριθμούς στην ευθεία των πραγματικών αριθμών τότε οι ακέραιοι αριθμοί «εκτείνονται» και προς τα δύο μέρη της ευθείας:



1.7. Ποιοι ακέραιοι περιέχονται στο διάστημα [-1,5];

1.8. Ποιες ακέραιες τιμές παίρνει η συνάρτηση συνx;

1.9. Πόσοι ακέραιοι περιέχονται στο διάστημα [-480, 1999];

1.10. Υπάρχουν άραγε ακέραιοι μεταξύ των αντιστρόφων δύο διαδοχικών φυσικών αριθμών;

1.11. Τίνων ακεραίων το τετράγωνο είναι ίσο με 81;

1.12. Οι ρητοί αριθμοί είναι όλα τα κλάσματα με αριθμητή και παρονομαστή ακεραίους. Εννοείται βέβαια ότι ο παρονομαστής δε μπορεί να είναι 0. Οι αριθμοί $\frac{2}{3}, \frac{-13}{18}, \frac{5}{-1}$ είναι ρητοί αριθμοί ενώ οι $\frac{\sqrt{2}}{3}, \sqrt{5}, \text{συν}1^\circ$ δεν είναι (οι πραγματικοί αριθμοί που δεν είναι ρητοί ονομάζονται *άρρητοι*). Το σύνολο των ρητών αριθμών το συμβολίζουμε με Q. Είναι λοιπόν

$$Q = \left\{ \frac{\mu}{\nu} \ / \ \mu \in Z, \nu \in Z^* \right\}.$$

Υπενθυμίζεται ότι δύο κλάσματα μπορεί να παριστούν τον ίδιο ρητό αριθμό λ.χ. $\frac{2}{3} = \frac{4}{6}$. Αν θέλουμε να συγκρίνουμε δύο ρητούς που εκφράζονται με τα κλάσματα $\frac{\kappa}{\lambda}, \frac{\mu}{\nu}$ των οποίων οι όροι κ, λ, μ, ν είναι θετικοί σχηματίζουμε τα δύο γινόμενα κν, μλ. Αν είναι ίσα οι ρητοί είναι ίσοι. Αν είναι μεγαλύτερο το πρώτο γινόμενο τότε

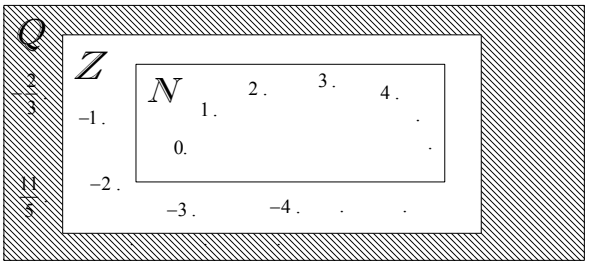
μεγαλύτερος είναι ο πρώτος ρητός και αν είναι το δεύτερο μεγαλύτερος είναι ο δεύτερος.

Και οι ρητοί αριθμοί αν παρασταθούν στην ευθεία των πραγματικών αριθμών εκτείνονται και προς τα δύο μέρη της αλλά έχουν και ένα επιπλέον χαρακτηριστικό: Είναι «διάσπαρτοι» στην ευθεία δηλαδή μεταξύ δύο οποιωνδήποτε πραγματικών αριθμών υπάρχει πάντοτε και ένας ρητός. Εντούτοις οι ρητοί αριθμοί δεν «καλύπτουν» όλα τα σημεία της πραγματικής ευθείας.

13. Να βρείτε δέκα ρητούς που ανήκουν στο διάστημα (0, 1).

14. Για ποια τιμή του φυσικού αριθμού x οι ρητοί $\frac{x}{3}, \frac{x+11}{12}$ είναι ίσοι;

15. Κάθε φυσικός αριθμός είναι και ακέραιος αριθμός και κάθε ακέραιος αριθμός είναι ρητός αριθμός. Λέμε ότι το σύνολο των φυσικών αριθμών είναι υποσύνολο του συνόλου των ακεραίων αριθμών και ότι το σύνολο των ακεραίων αριθμών είναι υποσύνολο του συνόλου των ρητών αριθμών. Γράφουμε συμβολικά $N \subseteq Z$ και $Z \subseteq Q$.



16. Για ποιες τιμές του ακεραίου x ο x+12 είναι φυσικός αριθμός;

17. Για ποιες ακέραιες τιμές του x ο ρητός αριθμός $\frac{18}{x}$ είναι ακέραιος; Ο $\frac{11}{x}$

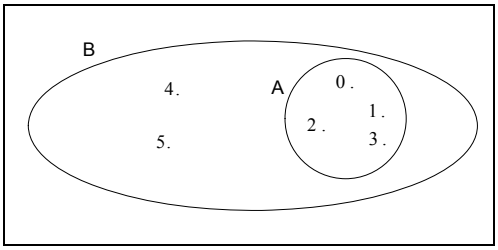
18. Υπενθυμίζεται ότι γενικά αν έχουμε δύο σύνολα Α και Β

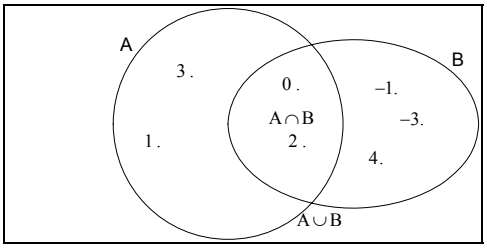
- τα Α και Β λέγονται *ίσα* (γράφουμε Α=Β) αν έχουν ακριβώς τα ίδια στοιχεία δηλαδή κάθε στοιχείο του Α είναι και στοιχείο του Β αλλά και κάθε στοιχείο του Β είναι και στοιχείο του Α.
- το Α λέγεται *υποσύνολο* του Β (γράφουμε $A\subseteq B$) αν κάθε στοιχείο του Α είναι και στοιχείο του Β.
- Η *τομή* των Α και Β (συμβολικά $A\cap B$) είναι το σύνολο που απαρτίζεται από τα *κοινά* στοιχεία των Α και Β δηλαδή εκείνα που ανήκουν και στο Α και στο Β.
- Η *ένωση* των Α και Β (συμβολικά $A\cup B$) είναι το σύνολο που απαρτίζεται από όλα τα στοιχεία των Α και Β κοινά και μη κοινά.
- Το σύνολο που δεν έχει καθόλου στοιχεία δηλαδή το { } συμβολίζεται με $\varnothing$ (*κενό σύνολο*)

Λ.χ. αν είναι Α={0, 1, 2, 3}, Β={0, 1, 2, 3, 4, 5} τότε $A\subseteq B$.

Αν είναι Α={0, 1, 2, 3}, Β={0, -1, 2, -3, 4, -5} τότε

$A\cap B=\{0, 2\}$ ενώ $A\cup B=\{0, 1, -1, 2, 3, -3, 4, -5\}$





1.19. Να βρείτε την τομή των συνόλων Α και Β όταν

- το Α έχει ως στοιχεία τους ακεραίους του διαστήματος $(-\sqrt{2},7)$
- το Β έχει ως στοιχεία τους ακεραίους του διαστήματος $(-\sqrt{5},\sqrt{7})$

1.20. Να βρείτε την ένωση των συνόλων Α και Β όταν

- το Α έχει ως στοιχεία τους ακεραίους του διαστήματος [-1, 5)
- το Β έχει ως στοιχεία τους ακεραίους του διαστήματος (-2, 4]

1.21. Μπορούμε να εκτελούμε τις τέσσερις πράξεις μεταξύ φυσικών, ακεραίων και των ρητών αριθμών αλλά ενδέχεται το αποτέλεσμα τους να μην ανήκει πάντοτε στο σύνολο από το οποίο προέρχονται οι αριθμοί λ.χ. η διαφορά 4-7 των φυσικών αριθμών 4 και 7 δεν είναι φυσικός αριθμός με άλλα λόγια για να βρούμε το αποτέλεσμα της πράξης αυτής χρειάζεται να «βγούμε» από το σύνολο των φυσικών αριθμών και να εργασθούμε στο «μεγαλύτερο» σύνολο των ακεραίων. Στον πίνακα που ακολουθεί φαίνεται ποιες πράξεις μπορούν να διεκπεραιωθούν μέσα στο σύνολο από το οποίο προέρχονται οι αριθμοί.

	Ανήκει πάντοτε το αποτέλεσμα της πράξης στο αντίστοιχο σύνολο ;		
Πράξη	$\mathcal{N}$	$\mathcal{Z}$	$\mathcal{Q}$
α+β	ΝΑΙ	ΝΑΙ	ΝΑΙ
α·β	ΝΑΙ	ΝΑΙ	ΝΑΙ
α-β	ΟΧΙ	ΝΑΙ	ΝΑΙ
α:β (β≠0)	ΟΧΙ	ΟΧΙ	ΝΑΙ

1.22. Οι α, β είναι ακέραιοι αριθμοί. Ποιοι από τους παρακάτω αριθμούς είναι βέβαιο ότι είναι ακέραιοι:

$$(\alpha+\beta)(\alpha-\beta),\quad \frac{\alpha+\beta}{\alpha-\beta},\quad \frac{\alpha+\beta}{\alpha\beta},\quad \frac{\alpha^2\beta+\alpha\beta^2}{\alpha\beta},\ \alpha^{\beta},\ \beta^{|\alpha|}$$

1.23. Ποιοι από τους ακέραιους 90, 100, 120, 130 είναι της μορφής ν^2-1, $\nu\in\mathcal{Z}$;

(Η έκφραση «είναι της μορφής» είναι πολύ συνηθισμένη στα Μαθηματικά: δίνεται ένας τύπος του οποίου οι μεταβλητές δηλαδή τα «γράμματα» μεταβάλλονται σε ένα σύνολο και τίθεται το ερώτημα ποιοι αριθμοί μπορούν ή δε μπορούν να προκύψουν από την εφαρμογή του τύπου δηλαδή να «παραχθούν» από τον τύπο).

1.24. Ποιοι από τους ακέραιους 90, 100, 120, 130 είναι της μορφής $20κ+30$, $κ\in Z$;

1.25. Ποιοι από τους ακέραιους 90, 100, 120, 130 είναι της μορφής $20κ^2+30$, $κ\in Z$;

1.26. Ποιοι από τους ακέραιους 90, 100, 120, 130 είναι της μορφής $κ^2+λ^2+1$, $κ,λ\in Z$;

1.27. Ποιος από τους αριθμούς 2^{2^n},$(2^2)^n$ (n φυσικός) είναι μεγαλύτερος;

1.28. Ποια είναι η μικρότερη τιμή που μπορεί να πάρει η απόλυτη τιμή ενός μη μηδενικού ακεραίου;

1.29. Αν οι αριθμοί α, β, γ είναι θετικοί ακέραιοι ποιος από τους παρακάτω αριθμούς είναι ο μεγαλύτερος από τους παρακάτω αριθμούς;

$(α+1)^2+(β+1)^2$ $(α+1)^3+(β+1)^2$ $α+β+2$

1.30. ***Γραμμικός συνδυασμός*** δύο ακεραίων α, β λέγεται κάθε ακέραιος της μορφής $κα+λβ$ με $κ,λ\in Z$. Οι κ, λ λέγονται *συντελεστές* του γραμμικού συνδυασμού $κα+λβ$ Οι αριθμοί $2α+3β$, $-5α+6β$, $12α+0β$, $0α+(-1)β$ είναι όλοι τους γραμμικοί συνδυασμοί των α, β. Ο $α^2+αβ$ είναι γραμμικός συνδυασμός των α, β αφού γράφεται $(α)α+α(β)$. Ο 5 δε μπορεί να γραφεί ως γραμμικός συνδυασμός των 2 και 8. (Γιατί;). Οι γραμμικοί συνδυασμοί ακεραίων συμπεριφέρονται γενικά όπως οι γραμμικοί συνδυασμοί διανυσμάτων με μία μόνο, αλλά σημαντική, διαφορά: *Μπορεί δύο γραμμικοί συνδυασμοί ακεραίων να είναι ίσοι χωρίς οι αντίστοιχοι συντελεστές τους να είναι ίσοι.* Λ.χ. $(-2)\cdot\mathbf{2}+1\cdot\mathbf{3}=(10)\cdot\mathbf{2}+(-7)\cdot\mathbf{3}$.

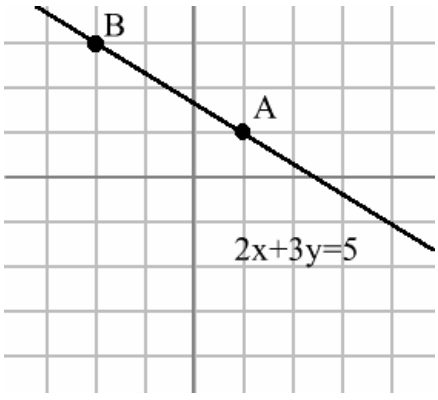
1.31. Να αποδείξετε ότι:

I. Αν οι ακέραιοι x, y είναι γραμμικοί συνδυασμοί των α, β τότε και το άθροισμα τους x-y και η διαφορά τους x-y είναι γραμμικός συνδυασμός των α, β. Δηλαδή να αποδείξετε ότι *το άθροισμα και η διαφορά γραμμικών συνδυασμών των α, β είναι γραμμικός συνδυασμός των α, β.*

II. Αν ο x είναι γραμμικός συνδυασμός των α, β τότε για κάθε ακέραιο λ ο λx είναι γραμμικός συνδυασμός των α, β. Δηλαδή *το γινόμενο επί ένα ακέραιο ενός γραμμικού συνδυασμού των α, β είναι γραμμικός συνδυασμός των α, β.*

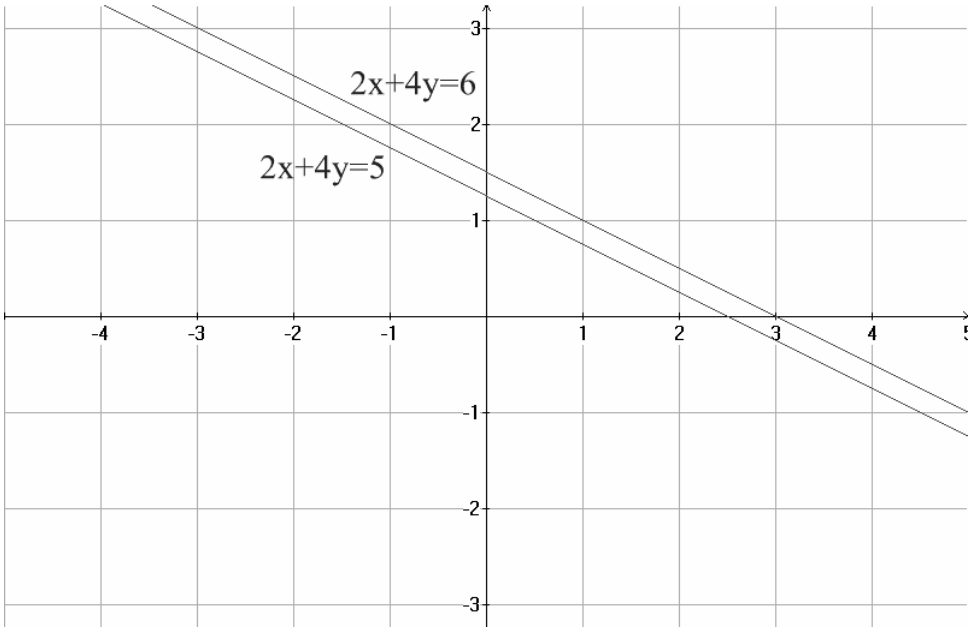
III. Αν ο x είναι γραμμικός συνδυασμός των β, γ και ο γ είναι γραμμικός συνδυασμός των α, β τότε ο x είναι γραμμικός συνδυασμός των α, β.

1.32. Ποιοι αριθμοί μπορούν να γραφούν ως γραμμικοί συνδυασμοί των α, β; Αυτό είναι ένα ερώτημα που θα το απαντήσουμε πλήρως στο τέλος αυτών των μαθημάτων. Εντούτοις μπορούμε να δούμε τι σημαίνει αυτό γεωμετρικά. Κατ΄ αρχήν αν α=β=0 μόνο ο 0 μπορεί να γραφεί ως γραμμικός συνδυασμός των α, β. Αν κάποιος από τους α, β είναι διάφορος του 0 τότε ο γ γράφεται ως γραμμικός συνδυασμός των α, β αν και μόνο αν υπάρχουν ακέραιοι x, y έτσι ώστε xα+yβ=γ δηλαδή αx+by=γ. Αυτό σημαίνει ότι θα πρέπει η ευθεία αx+by=γ να έχει ένα τουλάχιστον σημείο με ακέραιες συντεταγμένες. Τα σημεία του επιπέδου με ακέραιες συντεταγμένες ονομάζονται *συνδεσμικά σημεία*. Επομένως *ο γ είναι γραμμικός συνδυασμός των α, β αν και μόνο αν η ευθεία αx+by=γ διέρχεται από ένα τουλάχιστον συνδεσμικό σημείο*. Για παράδειγμα η ευθεία 2x+3y=5 διέρχεται από τα συνδεσμικά σημεία A(1,1) και B(-2, 3).



Απεναντίας δεν υπάρχουν ακέραιοι x, y έτσι ώστε 2x+4y=5 (αν υπήρχαν το πρώτο μέλος που είναι άρτιος θα ήταν ίσο με το δεύτερο μέλος που είναι περιττός πράγμα αδύνατο). άρα ο 5

δεν γράφεται ως γραμμικός συνδυασμός των 2 και 4. Αντιθέτως ο 6 γράφεται (1·2+1·4=6). Επομένως η ευθεία 2x+4y=5 δεν διέρχεται από κανένα συνδεσμικό σημείο ενώ η παράλληλη της 2x+4y=6 διέρχεται.



2. Η ΜΑΘΗΜΑΤΙΚΗ ΕΠΑΓΩΓΗ

2.1. Στις φυσικές επιστήμες η αλήθεια βρίσκεται κατ΄αρχήν με πειραματισμό. Αν μία υπόθεση επιβεβαιωθεί πολλές φορές αυτό μας είναι αρκετό για να την θεωρήσουμε ως «νόμο». Στα Μαθηματικά η κατάσταση είναι διαφορετική. Ο πειραματισμός μπορεί να μας δώσει ενδείξεις για την ισχύ μίας πρότασης αλλά ποτέ οριστική απόδειξη.

2.2. Για παράδειγμα ο μέγας Euler δοκιμάζοντας τιμές στην παράσταση $\nu^2+\nu+41$ (τριώνυμο του Euler) πίστεψε προς στιγμήν ότι η παράσταση αυτή μας δίνει πάντα πρώτους αριθμούς (πρώτοι αριθμοί λέγονται εκείνοι οι θετικοί ακέραιοι που είναι μεγαλύτεροι του 1 και έχουν μόνο δύο διαιρέτες: τον εαυτό τους και τη μονάδα). Πράγματι αν στο τριώνυμο του Euler θέσουμε όπου ν τις τιμές 1, 2, 3, ..., 39 θα βρούμε

ν	$ν^2+ν+41$	ν	$ν^2+ν+41$
1	43	21	503
2	47	22	547
3	53	23	593
4	61	24	641
5	71	25	691
6	83	26	743
7	97	27	797
8	113	28	853
9	131	29	911
10	151	30	971
11	173	31	1033
12	197	32	1097
13	223	33	1163
14	251	34	1231
15	281	35	1301
16	313	36	1373
17	347	37	1447
18	383	38	1523
19	421	39	1601
20	461		

Αν όμως θέσουμε ν=40 θα βρούμε:

$40^2+40+41=40(40+1)+41=40\cdot 41+41=41\cdot(40+1)=41^2$

Βρήκαμε δηλαδή ένα αριθμό που έχει διαιρέτη τον 41 και επομένως δεν είναι πρώτος.

2.3. Όταν εργαζόμαστε με δοκιμές δοκιμάζουμε πεπερασμένο πλήθος αριθμών αφήνοντας απέξω άπειρους αριθμούς. Ένα χαρακτηριστικό παράδειγμα είναι το ακόλουθο: Στην δεκαετία του 30 στην τότε Σοβιετική Ένωση οι μαθηματικοί προσπαθούσαν να λύσουν ένα πρόβλημα του Τσεμποτάρεφ. Συγκεκριμένα να εξετασθεί αν όταν αναλύσουμε το κυκλοτομικό πολυώνυμο $x^ν-1$ σε γινόμενο πρώτων παραγόντων θα βρούμε πολυώνυμα των οποίων όλοι οι συντελεστές είναι +1 ή -1.

Ας δούμε τι συμβαίνει με μικρές τιμές του ν:

ν	$x^ν-1$	Ανάλυση του $x^ν-1$ σε γινόμενο πρώτων παραγόντων.
1	x^1-1	$x-1$
2	x^2-1	$(x-1)(x+1)$
3	x^3-1	$(x-1)(x^2+x+1)$
4	x^4-1	$(x-1)(x+1)(x^2+1)$
5	x^5-1	$(x-1)(x^4+x^3+x^2+x+1)$

Γνωρίζουμε πόσο επίπονη είναι η διαδικασία της παραγοντοποίησης. Ο Ιβάνωφ το 1941 με τα περιορισμένα υπολογιστικά μέσα της εποχής απέδειξε ότι για ν=105 είναι

$x^{105}-1=(x-1)\ (x^6+x^5+x^4+x^3+x^2+x+1)(x^4+x^3+x^2+x+1)$

$(1-x+x^5-x^6+x^7-x^8+x^{10}-x^{11}+x^{12}-x^{13}+x^{14}-x^{16}+x^{17}-x^{18}+x^{19}-x^{23}+x^{24})$

$(x^2+x+1)(1-x+x^3-x^4+x^6-x^8+x^9-x^{11}+x^{12})$

$(1-x+x^3-x^4+x^5-x^7+x^8)$

$(1+x-x^{43}+x^{46}+x^{47}+x^{34}+x^{35}+x^{36}-x^{39}-x^{40}-2x^{41}-x^{42}-x^{22}-x^{26}-x^{28}+x^{31}+x^{32}+x^{33}-x^{20}+x^{15}+x^{48}-x^6-x^5+x^2-2x^7-x^{24}+x^{12}-x^8+x^{13}+x^{14}+x^{16}+x^{17}-x^9)$

Προσέξτε ότι στον τελευταίο παράγοντα εμφανίζονται οι συντελεστές 2. Επομένως δεν είναι σωστό ότι όλοι οι ανάγωγοι παράγοντες του x^v-1 έχουν συντελεστές ± 1 παρά το ότι αυτό ισχύει για $v\leq 104$.

2.4. Ένα άλλο παράδειγμα είναι η εικασία του Goldbach. Σύμφωνα με αυτή κάθε άρτιος αριθμός που είναι μεγαλύτερος του 4 μπορεί να γραφεί ως άθροισμα δύο περιττών πρώτων (ο μόνος άρτιος πρώτος είναι ο 2)

Πράγματι αν δοκιμάσουμε τιμές έχουμε

Άρτιος αριθμός	Γράφεται ως άθροισμα
6	3+3
8	5+3
10	5+5
12	7+5
14	7+7 αλλά και 11+3
16	5+11
18	15+3

Η ισχύς της εικασίας του Goldbach έχει δοκιμασθεί με την βοήθεια υπολογιστών για πολύ μεγάλους αριθμούς και σε κάθε μεμονωμένη περίπτωση έχει επιβεβαιωθεί. Πράγμα που σημαίνει ότι αν ξοδέψουμε όλη τη ζωή μας σε μεμονωμένες δοκιμές πάντα θα βλέπουμε την εικασία να επιβεβαιώνεται. Είναι τούτοις με τις δοκιμές δεν θα έχουμε αποδείξει την εικασία. Διότι ενδέχεται κάποιος μεγάλος αριθμός που δεν έχουμε δοκιμάσει να μη την επαληθεύει.

Η εικασία του Goldbach είναι ένα από τα *άλυτα* προβλήματα [1] των Μαθηματικών.

2.5. 🕮 Πόσο είναι το άθροισμα των ν πρώτων θετικών ακεραίων δηλαδή το άθροισμα 1+2+3+...+ν;

Το άθροισμα που ζητάμε έχει ν προσθετέους. Αυτό που ζητάμε είναι ένας γενικός τύπος γι'αυτό το άθροισμα. Ας δούμε μερικές τιμές του αθροίσματος

1=**1**

1+2=**3**

1+2+3=(1+2)+3=3+3=**6**

1+2+3+4=(1+2+3)+4=6+4=**10**

1+2+3+4+5=(1+2+3+4)+5=10+5=**15**

1+2+3+4+5+6=(1+2+3+4+5)+6=15+6=**21**

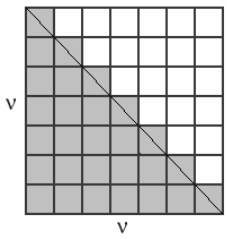
1+2+3+4+5+6+7=(1+2+3+4+5+6)+7=21+6=**27**

.....

.....

Μπορούμε άραγε εξετάζοντας τα τελικά αποτελέσματα 1, 3, 6, 10, 15, 21, 27 ... να βρούμε ένα τρόπο δηλαδή ένα κανόνα με τον οποίο προκύπτουν; Αν όχι ας βοηθήσουμε την παρατηρητικότητα μας με ένα σχήμα:

Ας παραστήσουμε κάθε μονάδα με ένα μικρό τετραγωνάκι. Ζητάμε να μάθουμε πόσα τετραγωνάκια θα έχουμε αν παραθέσουμε 1, 2, 3, 4, ... , ν τετραγωνάκια. Το πλήθος θα είναι 1+2+3+...+ν. (Στο σχήμα που ακολουθεί έχουμε πάρει ν=7)



[1] Πρόκειται για προβλήματα που κανείς δεν έχει λύσει ή τουλάχιστον δεν είναι γνωστό αν κάποιος τα έχει λύσει. Ασφαλώς δεν πρόκειται για «άλυτες ασκήσεις»

Αν κάθε τετραγωνάκι έχει πλευρά 1 τότε το άθροισμα που ζητάμε είναι το εμβαδόν του γραμμοσκιασμένου χωρίου. Το χωρίο αυτό απαρτίζεται από ένα ορθογώνιο τρίγωνο που έχει εμβαδόν ίσο με το εμβαδόν του τετραγώνου που σχηματίζεται δηλαδή $\frac{1}{2}\nu^2$ συν το εμβαδόν των ν μικρών τριγώνων που βρίσκονται πάνω από την διαγώνιο δηλαδή συν $\frac{1}{2}\nu$. Επομένως

$$1+2+3+...+\nu=\frac{1}{2}\nu^2+\frac{1}{2}\nu=\frac{1}{2}(\nu^2+\nu)=\frac{1}{2}\nu(\nu+1)$$

άρα

$$\mathbf{1+2+3+...+\nu=\frac{\nu(\nu+1)}{2}}$$

Ας ξαναγυρίσουμε στους αρχικούς μας υπολογισμούς ξέροντας τώρα το αποτέλεσμα. Εκ των υστέρων ίσως δούμε ότι θα μπορούσαμε αν έχουμε παρατηρήσει ότι

1=**1=1·2/2**

1+2=**3=1·1/2**

1+2+3=**6=3·4/2**

1+2+3+4=**10=4·5/2**

1+2+3+4+5=**15=5·6/2**

1+2+3+4+5+6=**21=6·7/2**

1+2+3+4+5+6+7=**27=7·8/2**

.....

.....

Ας υποθέσουμε ότι κάποιος κατόρθωνε να κάνει αυτή την παρατήρηση. Θα μπορούσε να υποθέσει ότι 1+2+3+...+ν=ν(ν+1)/2. Πρόκειται όμως απλώς για *μία υπόθεση* που πρέπει να επικυρωθεί από απόδειξη. Η υπόθεση αυτή επιβεβαιώνεται για τους

πρώτους 7 θετικούς ακεραίους αλλά αυτοί δεν είναι τίποτε μπροστά στους άπειρους που ακολουθούν.

Ξέρουμε (έχει επιβεβαιωθεί) ότι $1+2+3+...+7=\frac{1}{2}7(7+1)$.

Το γεγονός αυτό μας επιτρέπει να επιβεβαιώσουμε την υπόθεση για ν=8. Πράγματι

$$1+2+3+...+7+8=(1+2+3+...+7)+8=$$
$$\frac{1}{2}7\cdot 8+8=\frac{1}{2}7\cdot 8+8=\left(\frac{1}{2}7+1\right)8=\frac{9}{2}\cdot 8=\frac{1}{2}8(8+1).$$ Έτσι

επεκτείναμε την ισχύ της υπόθεσης μας για ν=8. Πόσο μακριά μπορούμε να φθάσουμε; Δεν έχει σημασία έτσι κι΄αλλιώς δεν επαρκεί η μικρή ζωή μας για να καλύψουμε όλους τους θετικούς ακεραίους. Ας πούμε ότι κατορθώσαμε να επιβεβαιώσουμε την ισχύ της υπόθεσης μας για ν=k δηλαδή ότι κατορθώσαμε να φθάσουμε έως τον k.

Φθάνοντας έως τον k ξέρουμε ότι $1+2+3+...+k=\frac{1}{2}k(k+1)$

Τότε μπορούμε να επαληθεύσουμε την ισχύ της υπόθεσης μας για ν=k+1. Πράγματι:

$$1+2+3+...+k+(k+1)=\left(1+2+3+...+k\right)+(k+1)=$$

$$=\frac{1}{2}k(k+1)+(k+1)=\left(\frac{1}{2}k+1\right)(k+1)=\frac{1}{2}(k+1)(k+2)$$

Βλέπουμε λοιπόν ότι κάθε φορά μπορούμε να επεκτείνουμε την ισχύ της υπόθεσης μας κατά 1 δηλαδή ξέροντας ότι ισχύει για ν=k να αποδείξουμε ότι ισχύει και για ν=k+1. Είναι λοιπόν καθαρά θέμα «χρόνου» να κάνουμε την απόδειξη για όλους τους φυσικούς αριθμούς. Απλώς ξέρουμε πως θα το πετύχουμε αλλά δεν μπορούμε γιατί οι φυσικοί αριθμοί είναι άπειροι. Αυτή την αδυναμία έρχεται να καλύψει η αρχή της μαθηματικής επαγωγής η οποία μας λέει ότι αν ξέρουμε πώς να κάνουμε μία απόδειξη «διατρέχοντας» τους θετικούς ακεραίους είναι σαν να την έχουμε κάνει.

2.6. Μία αρχή για να επαληθεύονται προτάσεις που έχουν να κάνουν με φυσικούς αριθμούς είναι η αρχή της **μαθηματικής επαγωγής** ή όπως αλλιώς λέγεται της *τέλειας επαγωγής*:

Έστω ένας ισχυρισμός που αναφέρεται στους θετικούς ακεραίους.

Αν

- ο ισχυρισμός είναι αληθής για 1.
- όταν ο ισχυρισμός αληθεύει για ν=k τότε είναι βέβαιο ότι αληθεύει και για ν=k+1.

Τότε

- ο ισχυρισμός αληθεύει για όλους τους θετικούς ακεραίους ν.

2.7. 🕮 Για όλους τους θετικούς ακεραίους ν με $\nu \geq 2$ και για όλους τους πραγματικούς α με $\alpha \neq 0$ και $\alpha > -1$ ισχύει: $(1+\alpha)^{\nu} > 1+\nu\alpha$. (Ανισότητα του Bernoulli)

2.8. Η ανισότητα του Bernoulli είναι προφανής όταν α>0 και δεν χρειάζεται επαγωγή για να αποδειχθεί. Αρκεί να παρατηρήσουμε ότι

$$(1+a)^{\nu} = \underbrace{(1+a)(1+a)...(1+a)}_{\nu \text{ παράγοντες}}$$

Ας εκτελέσουμε νοερά τους πολλαπλασιασμούς του β΄ μέλους. Αρκεί κάθε φορά να παίρνουμε ένα παράγοντα από κάθε παρένθεση και να πολλαπλασιάσουμε τους παράγοντες. Αν διαλέξουμε από όλες τις παρενθέσεις το 1 θα έχουμε γινόμενο 1. Αν διαλέξουμε από μία παρένθεση το α και από όλες τις υπόλοιπες παρενθέσεις το 1 θα βρούμε γινόμενο α. Το β΄ μέλος -που θα είναι τελικά ένα άθροισμα γινομένων που θα διαθέτει ένα παράγοντα από κάθε παρένθεση-θα έχει ως προσθετέο το 1, θα έχει ν προσθετέους ίσους με α και θα έχει και άλλους προσθετέους που αντιστοιχούν σε

άλλες επιλογές (λ.χ. να διαλέξουμε από τις δύο πρώτες παρενθέσεις το 1 και από τις υπόλοιπες το α οπότε θα πάρουμε ως προσθετέο το $\alpha^{\nu-2}$). ΄Αρα το β΄ μέλος είναι κάτι παραπάνω από $1+\underbrace{a+a...a}_{\text{ν προσθετέοι}}$. Αυτό σημαίνει ότι $(1+a)^{\nu}>1+\nu a$. ΄Αρα η ενδιαφέρουσα περίπτωση της ανισότητας του Ανισότητα του Bernoulli είναι όταν $-1<a\le 0$ Αυτή διατυπώνεται και με την μορφή

$$\theta^{\nu}\ge 1-\nu(1-\theta)\quad 0<\theta\le 1$$

Να αποδείξετε την ανισότητα αυτή α) Αυτοτελώς με επαγωγή β) Στηριζόμενοι στην προηγούμενη μορφή της ανισότητας του Bernoulli.

2.9. ☐🕮 Να αποδείξετε ότι για κάθε θετικό ακέραιο *ν* ισχύει

I. $1^2+2^2+3^2+...+\nu^2=\dfrac{\nu(\nu+1)(2\nu+1)}{6}$

II. $1^3+2^3+3^3+...+\nu^3=\left(\dfrac{\nu(\nu+1)}{2}\right)^2$

III. $1\cdot 2+2\cdot 3+3\cdot 4+...+\nu(\nu+1)=\dfrac{\nu(\nu+1)(\nu+2)}{3}$

IV. $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}+\dfrac{1}{3\cdot 4}+...+\dfrac{1}{\nu(\nu+1)}=\dfrac{\nu}{\nu+1}$.

2.10. ☐🕮 Να αποδείξετε ότι για κάθε θετικό ακέραιο *ν* ισχύει

$$1+x+x^2+...+x^{\nu-1}=\frac{x^{\nu}-1}{x-1},\qquad \text{εφόσον}\quad x\ne 1.$$

2.11. ☐ Η μαθηματική επαγωγή δεν είναι ασφαλώς ούτε ο μόνος ούτε ο καλύτερος τρόπος για να αποδεικνύουμε προτάσεις που εξαρτώνται από φυσικούς αριθμούς. Αποδείξτε την ισότητα του προηγουμένου παραδείγματος εκτελώντας απλώς τον πολλαπλασιασμό

$$(x-1)(x^{\nu-1}+....+x^2+x+1)$$

2.12. Να αποδείξετε ότι:

I. $\nu^2 > 2\nu + 1$ για κάθε ακέραιο $\nu \geq 3$

II. $\left(\frac{4}{3}\right)^{\nu} > \nu$ για κάθε ακέραιο $\nu \geq 7$

III. $5^{\nu} > 5\nu - 1$ για κάθε θετικό ακέραιο ν.

2.13. Να λυθεί η ανισότητα $x^2 > 2x + 1$. Στη συνέχεια να βρείτε τις ακέραιες λύσεις της. Θα έχετε έτσι μία απόδειξη για το ερώτημα I της προηγούμενης άσκησης χωρίς να έχετε χρησιμοποιήσει επαγωγή.

2.14. Να αποδείξετε ότι για κάθε θετικό ακέραιο $\nu \geq 4$ ισχύει

$$\nu! > 2^{\nu}, \quad \text{όπου } \nu! = 1 \cdot 2 \cdot 3 \ldots \nu .$$

2.15. Να αποδείξετε ότι για κάθε θετικό ακέραιο ν ισχύει

$$\frac{1}{1^2} + \frac{1}{2^2} + \ldots + \frac{1}{\nu^2} \leq 2 - \frac{1}{\nu}.$$

2.16. Να αποδείξετε ότι για κάθε θετικό ακέραιο $\nu \geq 3$ ισχύει

$$\nu^{\nu+1} > (\nu+1)^{\nu}.$$

2.17. Να αποδείξετε με την βοήθεια της μαθηματικής επαγωγής ότι

I. $|a_1 + \ldots + a_{\nu}| \leq |a_1| + \ldots + |a_{\nu}|$

II. $|\vec{a}_1 + \ldots + \vec{a}_{\nu}| \leq |\vec{a}_1| + \ldots + |\vec{a}_{\nu}|$

Η πρώτη ανισότητα αναφέρεται σε απόλυτες τιμές ενώ η δεύτερη σε μέτρα διανυσμάτων. Να χρησιμοποιήσετε και στις δύο περιπτώσεις-ως δεδομένη- την τριγωνική ανισότητα.

2.18. Για μία συνάρτηση φ είναι γνωστό ότι για κάθε ζεύγος αριθμών x, y ισχύει $\varphi(x+y) \leq \varphi(x) + \varphi(y)$. Υπάρχουν πολλές τέτοιες συναρτήσεις. Ανάμεσα τους

η φ(x)=αx, η φ(x)=|x| κ.α. Να αποδειχθεί ότι αν $x_1, x_2, ..., x_v$ είναι ν οποιοιδήποτε πραγματικοί αριθμοί τότε ισχύει

$$\varphi(x_1 + x_2 + ... + x_v) \le \varphi(x_1) + \varphi(x_2) + ... + \varphi(x_v)$$

2.19. ☐ Να αποδείξετε ότι κάθε πεπερασμένο υποσύνολο των πραγματικών αριθμών έχει μέγιστο και ελάχιστο στοιχείο. Με άλλα λόγια να αποδειχθεί ότι αν

$$X = \{x_1, x_2, ..., x_v\}$$

είναι ένα υποσύνολο του R με ν στοιχεία τότε υπάρχουν δύο στοιχεία μ, M του X τέτοια ώστε για κάθε στοιχείο x του X να ισχύει $\mu \le x \le M$.

2.20. ☐ Υπάρχουν υποσύνολα του R τα οποία δεν έχουν ελάχιστο στοιχείο. Για παράδειγμα το ανοικτό διάστημα (0, 1) δεν έχει ελάχιστο στοιχείο δηλαδή δεν υπάρχει κάποιο στοιχείο του που να είναι πιο μικρό από τα υπόλοιπα στοιχεία του. Λόγω της **2.19.** ένα τέτοιο σύνολο δε μπορεί να είναι πεπερασμένο. Να αποδειχθεί όμως ότι κάθε μη κενό υποσύνολο (πεπερασμένο ή όχι) του συνόλου των θετικών ακεραίων έχει ελάχιστο στοιχείο. Για την απόδειξη εργασθείτε ως εξής: Έστω S ένα υποσύνολο των θετικών ακεραίων. Ας υποθέσουμε ότι το S δεν έχει ελάχιστο στοιχείο. Τότε $1 \notin S$. Έστω T το σύνολο όλων των θετικών ακεραίων που δεν ανήκουν στο S. Προφανώς $1 \in T$. Δείξτε τώρα με επαγωγή ότι κάθε θετικός ακέραιος ανήκει στο T. Όταν τελειώσετε θα έχετε καταλήξει στο άτοπο συμπέρασμα ότι το S δεν έχει στοιχεία.

2.21. ☐ Αν έχουμε ένα σύνολο X μεταξύ των υποσυνόλων του συγκαταλέγονται το ίδιο το X και το κενό σύνολο ∅ που δεν έχει καθόλου στοιχεία. Ας πούμε ότι X={α}. Τότε το X έχει δύο μόνο υποσύνολα τα ∅ και X. Αν X={α, β} τότε τα

υποσύνολα του Χ είναι 4: Τα ∅, {α}, {β}, Χ. Αν Χ={α, β, γ} τότε το Χ έχει 8 υποσύνολα: Τα ∅, {α}, {β}, {γ}, {α, β}, {α, γ}, {β, γ}, Χ.

Πόσα άραγε υποσύνολα έχει ένα σύνολο με ν στοιχεία; Προσπαθήστε να αποδείξετε το συμπέρασμα σας με επαγωγή.

2.22. ☐ Με ν! (διαβάζεται «νι παραγοντικό») συμβολίζουμε το γινόμενο $1\cdot 2\cdot 3\cdot ...\cdot \nu$. Είναι 1!=1, 2!=2, 3!=6, 4!=24 κ.ο.κ. Επίσης δεχόμαστε ότι 0!=1

I. Να αποδειχθεί ότι ισχύει (ν+1) !=ν!· (ν+1)

II. Το ν! αυξάνει πολύ γρήγορα, γρηγορότερα από τις δυνάμεις οποιουδήποτε αριθμού. Έστω m ένας θετικός ακέραιος. Να αποδείξετε ότι για κάθε ν≥m+1 ισχύει $\nu!\geq m^{\nu}$.

2.23. Έστω k ένας θετικός ακέραιος. Να αποδείξετε ότι κάθε σύνολο με ν στοιχεία (ν≥k) έχει

$$\frac{\nu\cdot(\nu-1)\cdot...\cdot(\nu-k+1)}{k!}$$

υποσύνολα με k στοιχεία.

Ο αριθμός $\frac{\nu\cdot(\nu-1)\cdot...\cdot(\nu-k+1)}{k!}$ συμβολίζεται με $\binom{\nu}{k}$.

Δεχόμαστε ότι $\binom{\nu}{0}=1$

Επειδή αν θέλουμε από ν αντικείμενα να διαλέξουμε k δηλαδή να *συνδυάσουμε* k αντικείμενα που διαλέγουμε από ν λέμε ότι το πλήθος των **συνδυασμών ν αντικειμένων ανά k** είναι

$$\binom{\nu}{k}=\frac{\nu\cdot(\nu-1)\cdot...\cdot(\nu-k+1)}{k!}.$$

2.24. ☐ Δείξτε ότι το $(\alpha+\beta)^{\nu}$ δηλαδή το γινόμενο

$$\underbrace{(\alpha+\beta)(\alpha+\beta)(\alpha+\beta)...(\alpha+\beta)}_{\nu\ \text{φορές}}$$

είναι ίσο με

$$\binom{\nu}{0}\alpha^{\nu}+\binom{\nu}{1}\alpha^{\nu-1}\beta^{1}+\binom{\nu}{2}\alpha^{\nu-2}\beta^{2}+\binom{\nu}{3}\alpha^{\nu-3}\beta^{3}+...+\binom{\nu}{\nu-1}\alpha^{1}\beta^{\nu-1}+\binom{\nu}{\nu}\beta^{\nu}$$

(Newton)

3. ΕΥΚΛΕΙΔΕΙΑ ΔΙΑΙΡΕΣΗ

3.1. Η ταυτότητα της Ευκλείδειας διαίρεσης.

3.1.1. Ξέρουμε ότι όταν διαιρούμε ένα φυσικό αριθμό (διαιρετέο) με ένα μικρότερο του (διαιρέτη) θα βρούμε ένα πηλίκο και ένα υπόλοιπο. Το υπόλοιπο που μπορεί (όταν η διαίρεση είναι τέλεια) να είναι και 0 είναι σε κάθε περίπτωση μικρότερο από τον διαιρέτη. Επιπροσθέτως *ο διαιρετέος είναι ίσος με το πηλίκο επί τον διαιρέτη συν το υπόλοιπο*. Πρόκειται για την γνωστή ταυτότητα της Ευκλείδειας διαίρεσης Δ=πδ+υ με υ<δ. ΄Ετσι η διαίρεση 25:4 έχει πηλίκο 6 και υπόλοιπο 1 είναι δε 25=6·24+1 ενώ η διαίρεση 120:100 έχει πηλίκο 1 και υπόλοιπο 20 είναι δε 120=1·100+20. Μπορούμε να διαιρέσουμε ένα φυσικό και με ένα μεγαλύτερο του αριθμό. Τότε το πηλίκο είναι 0 και ο διαιρετέος είναι ταυτοχρόνως και υπόλοιπο. Η διαίρεση 100:120 έχει πηλίκο 0 και αφήνει υπόλοιπο 100 δηλαδή 100=0·120+100.

3.1.2. *Αν α και β είναι φυσικοί αριθμοί με $\beta \neq 0$, τότε υπάρχουν μοναδικοί φυσικοί π και υ, τέτοιοι, ώστε*

$$\alpha=\pi\beta+\upsilon,\ \beta>\upsilon\geq 0.$$

Το θεώρημα αυτό που έχουμε μάθει να χρησιμοποιούμε από το Δημοτικό μπορεί να αποδειχθεί με την βοήθεια της μαθηματικής επαγωγής:

Απόδειξη ΄Εστω β≠0. Αποδεικνύουμε ότι για κάθε φυσικό αριθμό α υπάρχουν φυσικοί αριθμοί π και υ τέτοιοι ώστε α=πβ+υ και β>υ. ΄Οταν εξασφαλίσουμε την ύπαρξη των κ, υ θα δείξουμε ότι είναι και οι μοναδικοί. Αν α=0 αρκεί να πάρουμε π=0 και υ=0.

Αν α=1 διακρίνουμε τις περιπτώσεις

I. β=1 οπότε παίρνουμε π=1 και υ=0

II. β>1 οπότε παίρνουμε π=0 και υ=1

΄Εστω ότι το αποδεικτέο ισχύει για α=k. Δηλαδή υπάρχουν π, υ έτσι ώστε k =βπ+υ β>υ≥0

΄Εστω ότι α= k +1. Τότε προσθέτοντας και στα δύο μέλη της k =βπ+υ το 1 βρίσκουμε k +1=βπ+υ+1. Διακρίνουμε πάλι δύο περιπτώσεις

I. Αν το β εξακολουθεί να είναι μεγαλύτερο του υ+1 τότε το πηλίκο της διαίρεσης k +1:β είναι π και το υπόλοιπο υ+1

II. Αν το β είναι ίσο με το υ+1 τότε το πηλίκο της διαίρεσης k +1:β είναι π+1 και το υπόλοιπο 0.

Σε κάθε περίπτωση έχουμε εξασφαλίσει ότι υπάρχουν π, υ έτσι ώστε k+1=πβ+υ και β>υ≥0

Θα αποδείξουμε τώρα ότι οι φυσικοί αριθμοί π και υ είναι μοναδικοί. Ας υποθέσουμε ότι για δύο φυσικούς π΄ και υ΄ ξέρουμε ότι

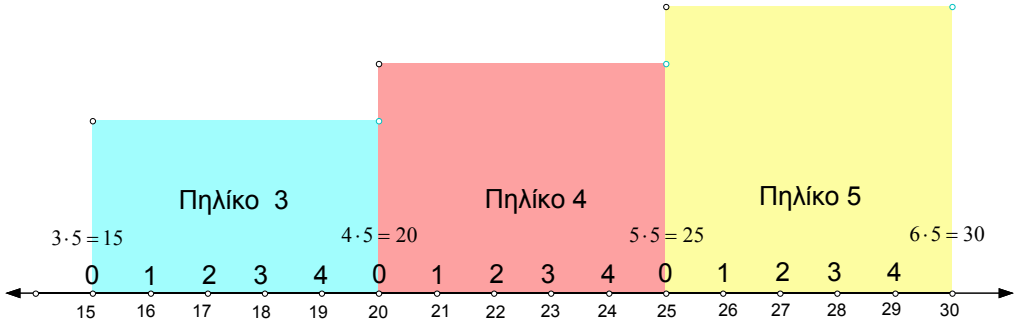
$$\alpha=\pi'\beta+\upsilon' \text{ και } \beta>\upsilon'\geq 0$$

Ασφαλώς ισχύει

$$\alpha=\pi\beta+\upsilon \text{ και } \beta>\upsilon\geq 0$$

Αν μεν υ=υ΄ καλώς αν όχι τότε κάποιος από τους υ, υ΄ είναι μεγαλύτερος του άλλου. Ας πούμε ότι είναι ο υ. Αφαιρώντας κατά μέλη βρίσκουμε (π-π΄)β+(υ-υ΄)=0 δηλαδή (υ-υ΄)=(π΄-π)β. ΄Ομως ο π΄-π είναι θετικός ακέραιος και επομένως π΄-π≥1 πράγμα που σημαίνει ότι (π΄-π)β≥β. Άρα υ-υ΄≥β και επομένως υ≥β+υ΄. Από την τελευταία σχέση συμπεραίνουμε ότι υ≥β πράγμα άτοπο διότι έχουμε υποθέσει ότι β>υ. Καταλήξαμε σε άτοπο υποθέτοντας ότι τα υ, υ΄ είναι διάφορα. ΄Αρα είναι ίσα. Αυτό σημαίνει ότι είναι ίσα και ότι υ-υ΄=0. Τότε από την σχέση (π-π΄)β+(υ-υ΄)=0 βρίσκουμε ότι (π-π΄)β=0 και επειδή β≠ 0 συμπεραίνουμε ότι και τα π, π΄ είναι ίσα. ΄Αρα το ζεύγος π, υ είναι το μοναδικό με την ιδιότητα α=πβ+υ και β>υ≥0.■

3.1.3. Ας δούμε με ποια λογική βρίσκουμε το πηλίκο και το υπόλοιπο της διαίρεσης ενός αριθμού λ.χ. δια 5



Ας φαντασθούμε τα θετικά πολλαπλάσια του 5 τοποθετημένα σε μία γραμμή. Ένας φυσικός αριθμός ή θα είναι πολλαπλάσιο του 5 ή θα βρίσκεται μεταξύ δύο διαδοχικών πολλαπλασίων του 5. Για παράδειγμα ο 17 βρίσκεται μεταξύ των πολλαπλασίων 15 και 20. Ο 15=3·5 είναι το μεγαλύτερο πολλαπλάσιο του 5 που «χωράει» στο 17. Το πηλίκο της διαίρεσης 17:5 είναι 3. Για να μεταβούμε από το 15 στο 17 χρειάζεται να προσθέσουμε 2. Ο 2 είναι το υπόλοιπο του 17:5.

Μπορούμε να φαντασθούμε τους φυσικούς αριθμούς «οργανωμένους» σε πεντάδες. Οι αριθμοί κάθε πεντάδας αφήνουν όλοι το ίδιο πηλίκο διαιρούμενοι δια 17 αλλά τα υπόλοιπα είναι 0, 1, 2, 3, 4. Στην επόμενη πεντάδα το πηλίκο αυξάνεται κατά 1 αλλά τα υπόλοιπα επαναλαμβάνονται: 1, 2, 3, 4. Αν λοιπόν για ένα αριθμό α είναι $5k \le a < 5(k+1)$ τότε ο k είναι το πηλίκο της διαίρεσης α:5. Το υπόλοιπο είναι ο αριθμός $a-5k$. Πιο γενικά αν θέλουμε να βρούμε το πηλίκο της διαίρεσης α:β βρίσκουμε δύο διαδοχικά πολλαπλάσια βk, $\beta(k+1)$ του β έτσι ώστε $\beta k \le a < \beta(k+1)$ Το πηλίκο της διαίρεσης α:β θα είναι k το δε υπόλοιπο ο a-βk. Την ίδια λογική ακολουθούμε αν έχουμε αρνητικό διαιρετέο. Λ.χ. ο -16 βρίσκεται μεταξύ των διαδοχικών πολλαπλασίων $(-4)\cdot 5 = -20$ και $(-3)\cdot 5 = -15$ δηλαδή $(-4)\cdot 5 \le -16 < (-3)\cdot 5$. Μπορούμε λοιπόν να θεωρήσουμε ότι το πηλίκο της διαίρεσης -

16:5 είναι -4 και το υπόλοιπο -16-(-4)·5=4. Σημειώστε ότι το πηλίκο εδώ είναι αρνητικό αλλά το υπόλοιπο είναι θετικό.

3.1.4. Γενικότερα αν έχουμε τον αρνητικό -α και θέλουμε να βρούμε πηλίκο και υπόλοιπο της διαίρεσης -α:β (β θετικός) τότε παίρνουμε τον αντίθετο α του -α. Ας πούμε ότι είναι $\beta k \le -a < \beta(k+1)$. Τότε $-\beta(k+1) < -a \le -\beta k$. Από την τελευταία σχέση συνάγουμε ότι

$$\text{πηλίκο της διαίρεσης } -\alpha:\beta = \begin{cases} -(k+1) & \text{αν } -a < -\beta k \\ -k & \text{αν } -a = -\beta k \end{cases}$$

$$\text{υπόλοιπο της διαίρεσης } -\alpha:\beta = \begin{cases} -\alpha+(k+1)\beta & \text{αν } -a < -\beta k \\ 0 & \text{αν } -a = -\beta k \end{cases}$$

Δεν είναι δύσκολο να δούμε ότι σε κάθε περίπτωση για το υπόλοιπο υ ισχύει $0 \le \upsilon < \beta$. Ανάλογους συλλογισμούς μπορούμε να κάνουμε όταν έχουμε β<0.

Φροντίζουμε να βρούμε δύο διαδοχικά πολλαπλάσια $\beta k, \beta(k+1)$ του β έτσι ώστε $\beta k \le a < \beta(k+1)$ (Αδιάφορο αν ο α είναι θετικός ή αρνητικός). Το πηλίκο της διαίρεσης α:β θα είναι k ενώ το υπόλοιπο ο $a-\beta k$.

3.1.5. Το προηγούμενο θεώρημα λοιπόν ισχύει όχι μόνο για φυσικούς αριθμούς αλλά και για ακεραίους αριθμούς. Συγκεκριμένα:

Αν α και β είναι ακέραιοι αριθμοί με $\beta \neq 0$, τότε υπάρχουν μοναδικοί ακέραιοι αριθμοί π (πηλίκο) και υ (υπόλοιπο), τέτοιοι, ώστε

$$\alpha = \pi\beta + \upsilon,\ |\beta| > \upsilon \ge 0.$$

3.1.6. Η προηγούμενη ταυτότητα λέγεται **ταυτότητα της Ευκλείδειας διαίρεσης** α:β. Με την βοήθεια της μπορούμε να παρατηρήσουμε ότι:

- Κάθε αριθμός διαιρούμενος δια 2 αφήνει υπόλοιπο 0 (**άρτιος**) ή 1 (**περιττός**) οπότε είναι της μορφής $2k$ ή $2k+1$.

- Κάθε αριθμός διαιρούμενος δια 3 αφήνει υπόλοιπο 0 , 1 ή 2. Οπότε είναι της μορφής $3k$ ή $3k+1$ ή $3k+2$.
- Κάθε αριθμός διαιρούμενος δια 4 αφήνει υπόλοιπο 0 , 1 ή 2 ή 3. ΄Αρα κάθε αριθμός έχει μία από τις ακόλουθες μορφές $4k$, $4k+1$, $4k+2$, $4k+3$.
- Γενικά κάθε αριθμός διαιρούμενος δια του m>0 αφήνει υπόλοιπο 0 ή 1 ή 2 ή .... ή m-1 και επομένως έχει μία από τις μορφές km, km+1, km+2, ..., km+(m-1).
- Αν για ένα m>0 και ένα οποιοδήποτε α πετύχουμε να γράψουμε α=m·(ένας οποιοσδήποτε ακέραιος)+υ και συμβαίνει ο υ να είναι μή αρνητικός και μικρότερος του m τότε είναι βέβαιο έχουμε γράψει την ταυτότητα της Ευκλείδειας διαίρεσης του α δια του m και ότι ο υ είναι το υπόλοιπο της διαίρεσης α:m.

Για παράδειγμα ο $1999^{1981}+10$ μπορεί να γραφεί $(1999^{1981}-1)+11$ και με χρήση της γνωστής ταυτότητας

$$x^{\nu}-y^{\nu}=(x-y)(x^{\nu-1}+x^{\nu-2}y+....+y^{\nu-1})$$

έχουμε $99^{1981}+10=(1999-1)(1999^{1980}+1999^{1979}+...+1999+1)+11$ δηλαδή

$$99^{1981}+10=1998\cdot\underbrace{(1999^{1980}+1999^{1979}+...+1999+1)}_{x}+11$$

3.1.7. Αν ένας αριθμός α διαιρούμενος δια του β (β≠0) αφήνει υπόλοιπο 0 λέμε ότι **διαιρείται** από το β και ότι η διαίρεση α:β είναι **τέλεια**. Επίσης λέμε ότι ο β είναι διαιρέτης του α. Επομένως ο α διαιρείται από το β αν υπάρχει ακέραιος k έτσι ώστε $a=k\beta$. Αν ο β διαιρεί τον α τότε συμβολικά γράφουμε β|α. Αν ο β δεν διαιρεί τον α τότε γράφουμε $\beta\nmid\alpha$. Επομένως $\beta\nmid\alpha$ αν και μόνο αν για κάθε ακέραιο k είναι $a\neq k\beta$. Οι συμβολισμοί β|α, $\beta\nmid\alpha$ θα αναφέρονται μόνο σε ακέραιους αριθμούς α, β με β≠0. Αν $\beta\nmid\alpha$ τότε δεν υπάρχει ακέραιος k έτσι ώστε $a=k\beta$. Στην περίπτωση που ο α διαιρεί τον β λέμε ότι ο α είναι **πολλαπλάσιο** του β. Γράφουμε συμβολικά α=πολβ. Λ.χ. 2|4, $4\nmid 2$, 6|18, 15|-30, -5|40, $5\nmid -8$, 50=πολ5, 60≠πολ7.

3.1.8. ☐ Δείξτε ότι αν οι αριθμοί x, y διαιρούμενοι δια του 3 αφήνουν υπόλοιπα 1 και 2 τότε το άθροισμα τους διαιρούμενο δια του 3 αφήνει υπόλοιπο 0.

3.1.9. ☐ Δείξτε ότι αν οι αριθμοί x, y διαιρούμενοι δια του 5 αφήνουν υπόλοιπα 1 και 2 τότε το άθροισμα τους διαιρούμενο δια του 5 αφήνει υπόλοιπο 3.

3.1.10. ☐ Δείξτε ότι αν οι αριθμοί x, y διαιρούμενοι δια του 15 αφήνουν υπόλοιπα 9 και 12 τότε το άθροισμα τους διαιρούμενο δια του 15 αφήνει υπόλοιπο 6.

3.1.11. ☐ Να βρείτε όλους τους αριθμούς που είναι μικρότεροι του 100 και διαιρούμενοι δια 7 και 9 αφήνουν αντιστοίχως υπόλοιπα 2 και 4.

3.1.12. ☐🕮 Αν ο α είναι ακέραιος, τότε και ο $\dfrac{\alpha(\alpha^2+2)}{3}$ είναι ακέραιος.

3.1.13. ☐🕮 Να αποδειχτεί ότι:

(i) Το γινόμενο δύο διαδοχικών ακεραίων είναι άρτιος αριθμός.

(ii) Το τετράγωνο κάθε περιττού ακεραίου είναι της μορφής $\mathbf{8\lambda+1}$, $\lambda\in\mathbb{Z}$.

3.1.14. ☐🕮 Να βρείτε το πηλίκο και το υπόλοιπο της ευκλείδειας διαίρεσης του α με τον β σε καθεμιά από τις παρακάτω περιπτώσεις:

1) $\alpha=83$ και $\beta=11$

2) $\alpha=-83$ και $\beta=11$

3) $\alpha=83$ και $\beta=-11$

4) $\alpha=-83$ και $\beta=-11$.

3.1.15. ☐🕮 Να αποδείξετε ότι:

1) Το τετράγωνο ενός ακεραίου α παίρνει τη μορφή $\alpha^2=3\kappa$, $\kappa\in\mathbf{Z}$ ή $\alpha^2=3\kappa+1$, $\kappa\in\mathbf{Z}$.

2) Κάθε ακέραιος α της μορφής $\alpha = 6\kappa + 5$, $\kappa \in \mathbf{Z}$ μπορεί να πάρει τη μορφή $\alpha = 3\lambda + 2$, $\lambda \in \mathbf{Z}$. Ισχύει το αντίστροφο;

3.1.16. ☐ Οι αριθμοί διαιρούμενοι δια του 3 αφήνουν υπόλοιπα 0, 1, 2 και όπως διατρέχουμε τους ακεραίους τα υπόλοιπα εναλλάσσονται με την ίδια σειρά. Οι αριθμοί που είναι τετράγωνα ακεραίων (τα **τέλεια τετράγωνα** ή οι **τετράγωνοι αριθμοί** όπως αλλιώς λέγονται) δηλαδή οι αριθμοί της μορφής k^2 είναι «σπανιότεροι». Επειδή $(\nu+1)^2 - \nu^2 = 2\nu+1$ αν φθάσουμε το νι-οστό τετράγωνο αριθμό θα χρειασθεί να συναντήσουμε 2ν+1 μη τετράγωνους αριθμούς έως ότου φθάσουμε στον επόμενο τετράγωνο. Λ.χ. μετά τον 100^0 τετράγωνο αριθμό που είναι ο 10000 ο επόμενος τετράγωνος είναι ο $10000+2\cdot100+1=10201=101^2$. Δείξτε ότι οι τετράγωνοι αριθμοί διαιρούμενοι δια του 3 αφήνουν πάντα υπόλοιπο 0 ή 1. Δηλαδή «αποφεύγουν» τους αριθμούς $3k+2$. (Ένας στους τρεις αριθμούς είναι της μορφής $3k$+2).

3.1.17. ☐🕮 Αν α είναι ένας περιττός ακέραιος, να αποδείξετε ότι

$$\frac{\alpha^2 + (\alpha+2)^2 + (\alpha+4)^2 + 1}{12} \in \mathbf{Z}.$$

3.1.18. ☐🕮 Μπορεί ο αριθμός 25 να γραφεί ως άθροισμα 10 προσθετέων, καθένας από τους οποίους να είναι ίσος με 1 ή 3 ή 5;

3.1.19. ☐🕮 Για ποιες τιμές του θετικού ακεραίου β το πηλίκο της διαίρεσης του 660 με τον β είναι ίσο με 17; Ποιο είναι το υπόλοιπο της διαίρεσης αυτής σε καθεμιά περίπτωση;

3.1.20. ☐🕮Αν α, β, γ είναι περιττοί ακέραιοι, να αποδείξετε ότι η εξίσωση $\alpha x^2 + \beta x + \gamma = 0$ δεν έχει ακέραιες λύσεις.

3.1.21. ☐🕮Έχει ακέραιες λύσεις η εξίσωση $x^2 + 3^{1997}x + 2001 = 0$;

3.1.22. ☐🕮 Αν α,β είναι δύο περιττοί ακέραιοι, να αποδείξετε ότι

(i) $\frac{\alpha^2-\beta^2}{8}\in\mathbf{Z}$ και (ii) $\frac{\alpha^4+\beta^4-2}{16}\in\mathbf{Z}$.

3.1.23. ☐🕮 Για ποιες τιμές του ακεραίου κ ο αριθμός $\frac{3\kappa+4}{5}$ είναι ακέραιος;

3.1.24. ☐🕮 Να αποδείξετε ότι:

1) Το τετράγωνο ενός άρτιου είναι της μορφής $\alpha^2=4\lambda$, $\lambda\in\mathbf{Z}$, ενώ το τετράγωνο ενός περιττού είναι της μορφής $\alpha^2=4\lambda+1$, $\lambda\in\mathbf{Z}$.
2) Αν α,β είναι περιττοί ακέραιοι, τότε η εξίσωση $x^2=\alpha^2+\beta^2$ δεν έχει ακέραιες ρίζες.
3) Κανένας από τους όρους της αριθμητικής προόδου: 6,10,14,18,22,... δεν είναι τετράγωνο φυσικού αριθμού.

3.2. Ισότιμοι ή ισοϋπόλοιποι ακέραιοι

3.2.1. Οι αριθμοί μπορούν να διακριθούν μεταξύ τους κατά πολλούς τρόπους:

- θετικοί- αρνητικοί
- αριθμοί που κάνουν την παράσταση x^2-3x+2 θετική, αρνητική ή 0
- αριθμοί που είναι της μορφής x^2-3x+2 ή όχι. κ.α.

Μία διάκριση που καθιέρωσε και επεξεργάσθηκε ο μεγάλος Γερμανός μαθηματικός του περασμένου αιώνα Γκάους (Carl Friedrich Gauss, 1777 -1855) είναι εκείνη που γίνεται με βάση το υπόλοιπο που αφήνουν οι διάφοροι αριθμοί όταν διαιρούνται δια του ίδιου κάθε φορά θετικού ακεραίου. Στους πίνακες που ακολουθούν βλέπουμε την κατάταξη των ακεραίων ανάλογα με τα υπόλοιπα που αφήνουν διαιρούμενοι δια 2 και δια 3.

Υπόλοιπα διαιρέσεων δια 2	
0	1
v=2k	v=2k+1
.....	.....
-10	-9
-8	-7
-6	-5
-4	-3
-2	-1
0	1
2	3
4	5
6	7
8	9
10	11
12	13
14	15
16	17
....	....

Υπόλοιπα διαιρέσεων δια 3		
0	1	2
v=3k	v=3k+1	v=3k+2
....	....	....
-18	-17	-16
-15	-14	-13
-12	-11	-10
-9	-8	-7
-6	-5	-4
-3	-2	-1
0	1	2
3	4	5
6	7	8
9	10	11
12	13	14
15	16	17
18	19	20
....	....	....

Ο 10 για παράδειγμα «ως προς 2» ανήκει στην κατηγορία 0 δηλαδή στην κατηγορία των αριθμών που διαιρούμενοι δια 2 αφήνουν υπόλοιπο 0. Ο ίδιος αριθμός δηλαδή ο 10 «ως προς 3» ανήκει στην κατηγορία 1 δηλαδή διαιρούμενος δια 3 αφήνει υπόλοιπο 1. Όλοι οι αριθμοί που «ως προς 2» αφήνουν το ίδιο υπόλοιπο δηλαδή ή όλοι οι αριθμοί της κατηγορίας 1 ή όλοι οι αριθμοί της κατηγορίας 2 λέγονται ισοϋπόλοιποι «ως προς 2» ή ισότιμοι «ως προς 2». Ο 2 είναι εν προκειμένω είναι ένα κριτήριο ένα «μέτρο» για την κατάταξη των αριθμών. Ο 3 είναι ένα άλλο «μέτρο».

Ο Gauss στο θεμελιώδες έργο του Disquisitiones Arithmeticae (Αριθμητικές Έρευνες) όρισε ότι δύο αριθμοί α, β θα λέγονται **ισότιμοι** ως προς το *modulus* (*μέτρο*, *γνώμονα*) m>0 αν οι α, β διαιρούμενοι δια του m αφήνουν το ίδιο υπόλοιπο. Έγραψε $\alpha \equiv \beta(\mathrm{mod}\, m)$ (διαβάζεται «ο α είναι ισότιμος με τον β μόντουλο m»). Αν οι α, β δεν είναι ισότιμοι ή ισοϋπόλοιποι όπως αλλιώς λέμε ως προς m γράφουμε $\alpha \not\equiv \beta(\mathrm{mod}\, m)$. Με αυτό τον συμβολισμό είναι:

$3 \equiv 13 \pmod 2$ $3 \not\equiv 12 \pmod 2$

$11 \equiv 34 \pmod 3$ $-5 \equiv 4 \pmod 3$

$3 \not\equiv 13 \pmod 3$ $3 \equiv (12 \bmod 2)$

3.2.2. Ποιες από τις παρακάτω σχέσεις είναι αληθείς;

$11 \equiv 12 \pmod 2$ $-3 \not\equiv 12 \pmod 2$

$101 \equiv -4 \pmod 3$ $11 \equiv 4 \pmod 3$

$3 \not\equiv -33 \pmod 3$ $30 \equiv -12 \pmod 2$

3.2.3. Να συμπληρώσετε τα κενά με ένα από τους αριθμούς 1 ή 0.

Αν $\alpha \equiv 1 \pmod 2$ τότε $2+\alpha \equiv \ldots \pmod 2$

Αν $\alpha \equiv 0 \pmod 2$ τότε $2+\alpha \equiv \ldots \pmod 2$

Αν $\alpha \equiv 0 \pmod 2$ τότε $-\alpha \equiv \ldots \pmod 2$

Αν $\alpha \equiv 1 \pmod 2$ τότε $-\alpha \equiv \ldots \pmod 2$

Αν $\alpha \equiv 0 \pmod 2$ τότε $\alpha+3 \equiv \ldots \pmod 2$

Αν $\alpha \equiv 1 \pmod 2$ τότε $\alpha+3 \equiv \ldots \pmod 2$

Αν $\alpha \equiv 0 \pmod 2$ τότε $\alpha^2 \equiv \ldots \pmod 2$

Αν $\alpha \equiv 1 \pmod 2$ τότε $\alpha^2 \equiv \ldots \pmod 2$

3.2.4. Να συμπληρώσετε τα κενά με ένα από τους αριθμούς 0, 1 ή 2.

Αν $\alpha \equiv 1 \pmod 3$ τότε $2+\alpha \equiv \ldots \pmod 3$

Αν $\alpha \equiv 0 \pmod 3$ τότε $2+\alpha \equiv \ldots \pmod 3$

Αν $\alpha \equiv 1 \pmod 3$ τότε $-\alpha \equiv \ldots \pmod 3$

Αν $\alpha \equiv 1 \pmod 3$ τότε $-\alpha \equiv \ldots \pmod 3$

Αν $\alpha \equiv 0 \pmod 3$ τότε $2\alpha \equiv \ldots \pmod 3$

Αν $\alpha \equiv 1 \pmod 3$ τότε $\alpha^2 \equiv \ldots \pmod 3$

Αν $\alpha \equiv 2 \pmod 3$ τότε $4\alpha \equiv ... \pmod 3$

Αν $\alpha \equiv 2 \pmod 3$ τότε $3\alpha^2 \equiv ... \pmod 3$

3.2.5. Στον πίνακα που ακολουθεί υπάρχουν οι αριθμοί κατανεμημένοι mod 5.

Υπόλοιπα διαιρέσεων δια 5				
0	1	2	3	4
v=5k	v=5k+1	v=5k+2	v=5k+3	v=5k+4
....	....	....	....	....
-50	-49	-48	-47	-46
-45	-44	-43	-42	-41
-40	-39	-38	-37	-36
-35	-34	-33	-32	-31
-30	-29	-28	-27	-26
-25	-24	-23	-22	-21
-20	-19	-18	-17	-16
-15	-14	-13	-12	-11
-10	-9	-8	-7	-6
-5	-4	-3	-2	-1
0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19
20	21	22	23	24
25	26	27	28	29
....	....	....	....	....

1. Σε ποια στήλη ανήκουν οι αριθμοί 299, -35, 121, -389;
2. Σε ποια στήλη ανήκουν οι αριθμοί $5k^2+1$, 5k-1, 25k-8;
3. Διαλέξτε ένα αριθμό της πρώτης στήλης και ένα αριθμό της δεύτερης. Σε ποια στήλη ανήκει το άθροισμα τους. Να δοκιμάσετε δύο άλλους αριθμούς. Μπορούμε να έχουμε κάποιο γενικό συμπέρασμα; μπορείτε να αποδείξετε το συμπέρασμα αυτό;
4. Διαλέξτε ένα αριθμό της στήλης 2 και προσθέστε τον σε ένα οποιοδήποτε αριθμό της στήλης 4. Δοκιμάστε δύο αριθμούς πάλι από τις στήλες 2 και 4. Τι συμπέρασμα βγάζετε. Ας υποθέσουμε ότι κάνουμε την εξής «πρόσθεση» μεταξύ στηλών: *Για να προσθέσουμε δύο στήλες διαλέγουμε ένα αριθμό από κάθε στήλη τους προσθέτουμε και κοιτάμε σε ποια στήλη ανήκει το αποτέλεσμα. Σαν άθροισμα των στηλών γράφουμε την στήλη αυτή.* Πόσο είναι το 2+4, το 3+3, το 3+2;

5. Εργασθείτε αυτή τη φορά με τον πολλαπλασιασμό δοκιμάζοντας διάφορους αριθμούς. Πόσο θα είναι το $2\cdot4$, το $3\cdot3$, το $3\cdot2$;

4. ΔΙΑΙΡΕΤΟΤΗΤΑ

4.1. Στην προηγούμενη παράγραφο γνωρίσαμε την έννοια της διαιρετότητας: *Ο β διαιρεί το α αν και μόνο αν υπάρχει ακέραιος k έτσι ώστε $a=k\beta$.* Το γεγονός αυτό συμβολίζεται με β|α. (Σχέση του διαιρείν).

4.2. Κάθε ακέραιος α διαιρείται από τον 1 διότι $a=1\cdot a$. Με άλλα λόγια ο 1 είναι διαιρέτης κάθε ακεραίου.

4.3. Κάθε ακέραιος β διαιρεί το 0 διότι $0=0\cdot\beta$ δηλαδή ο 0 έχει διαιρέτη κάθε ακέραιο.

4.4. *Ο β διαιρεί τον α αν και μόνο αν ο α διαιρεί τον -β.*

Απόδειξη: Αν $\beta|a$ τότε υπάρχει ακέραιος k έτσι ώστε $a=k\beta$. Η σχέση αυτή γράφεται και $a=(-k)(-\beta)$ με άλλα λόγια υπάρχει ο ακέραιος $-k$ που πολλαπλασιαζόμενος με τον β μας δίνει τον α. Αν πάλι ξέρουμε ότι $-\beta|a$ τότε ξέρουμε ότι και ο αντίθετος του -β δηλαδή ο β διαιρεί τον α. Επομένως: $\beta|a\Leftrightarrow-\beta|a$. Ανάλογα συμπεραίνουμε ότι αν $\beta|a$ τότε και $\beta|-a$ Επομένως $\beta|a\Leftrightarrow\pm\beta|\pm a$. ■

4.5. *Αν ο β διαιρεί τον α τότε β διαιρεί κάθε πολλαπλάσιο λα του α.*

Απόδειξη: Αν $\beta|a$ τότε υπάρχει ακέραιος k έτσι ώστε $a=k\beta$. Πολλαπλασιάζοντας την ισότητα αυτή επί λ βρίσκουμε ότι Η σχέση αυτή γράφεται και $\lambda a=\lambda k\beta$ με άλλα λόγια υπάρχει ο ακέραιος λk που πολλαπλασιαζόμενος με τον β μας δίνει τον λα. ΄Αρα β|λα. ■

4.6. *Αν $\lambda\neq0$ τότε ο β διαιρεί τον α αν και μόνο αν ο $\lambda\beta$ διαιρεί τον λα.*

Απόδειξη: Αν $\beta \mid \alpha$ τότε υπάρχει ακέραιος k έτσι ώστε $a = k\beta$. Έστω λ ένας ακέραιος με λ≠0. Πολλαπλασιάζοντας την τελευταία σχέση με λ βρίσκουμε ότι $\lambda a = (\lambda k)\beta$ πράγμα που σημαίνει ότι $\lambda a = k(\lambda\beta)$ δηλαδή $\lambda\beta \mid \lambda a$. Αλλά και αντιστρόφως αν $\lambda\beta \mid \lambda a$ τότε υπάρχει ακέραιος k έτσι ώστε $\lambda a = k(\lambda\beta)$. Απλοποιώντας το λ καταλήγουμε στο συμπέρασμα ότι $\beta \mid \alpha$. Δηλαδή για λ≠0 ισχύει η ισοδυναμία $\beta \mid a \Leftrightarrow \lambda\beta \mid \lambda a$. ■

4.7. Από το προηγούμενο βλέπουμε ότι η σχέση του διαιρείν συμπεριφέρεται όπως η ισότητα: Μπορούμε να πολλαπλασιάζουμε κατά μέλη με τον ίδιο μη μηδενικό ακέραιο ή να διαγράφουμε τον ίδιο παράγοντα· προκύπτει πάλι σχέση του διαιρείν. Ανάλογη ιδιότητα δεν ισχύει για το άθροισμα δηλαδή η σχέση $\beta \mid \alpha$ δεν συνεπάγεται την $\lambda+\beta \mid \lambda+a$. Λ.χ. 2|4 αλλά 5+2 ⁄ 5+4.

4.8. *Αν α≠0 και β|α τότε* $|\beta| \le |a|$.

Απόδειξη: Αφού β|α υπάρχει ακέραιος k έτσι ώστε $a = k\beta$. Θα είναι $k \neq 0$. Αν πάρουμε τις απόλυτες τιμές και των δύο μελών έχουμε $|a| = |k\beta|$ και επομένως $|a| = |k||\beta|$. Ο $|k|$ είναι μη μηδενικός φυσικός αριθμός και επομένως $|k| \ge 1$. Άρα $|k||\beta| \ge |\beta|$ και επομένως $|a\| \ge |\beta|$.

4.9. Είδαμε ότι $\beta \mid a \Rightarrow |\beta| \le |a|$. Με άλλα λόγια η απόλυτη τιμή ενός διαιρέτη του α≠0 δεν υπερβαίνει την απόλυτη τιμή του α. Συνέπεια τούτου είναι $\beta \mid a \Rightarrow -|a| \le \beta \le |a|$. Το πλήθος λοιπόν των διαιρετών του α δε μπορεί να υπερβεί (στην πραγματικότητα είναι κατά πολύ μικρότερο) το πλήθος των ακεραίων του διαστήματος $[-|a|, |a|]$ δηλαδή τον αριθμό $2|a|+1$. Σημειώστε ότι μπορεί να ισχύει $|\beta| \le |a|$ χωρίς να ισχύει β|α. Λ.χ. είναι |3|<|5| αλλά 3 ⁄ 5

4.10. *Αν x|y και y|z τότε x|z. (μεταβατική ιδιότητα του διαιρείν)*

Απόδειξη: Αφού x|y θα υπάρχει ακέραιος k έτσι ώστε $y = kx$. Επίσης αφού y|z θα υπάρχει ακέραιος t έτσι ώστε $z = ty$. Αντικαθιστώντας το $y = kx$ στην $z = ty$ βρίσκουμε ότι υπάρχει ο ακέραιος tk έτσι ώστε $z = (tk)x$ δηλαδή x|z. ■

4.11. *Αν ο δ διαιρεί τους x, y τότε διαιρεί και το άθροισμα τους x+y.*

Απόδειξη: Αφού δ|x, δ|y θα υπάρχουν ακέραιοι k_1, k_2 έτσι ώστε $x = k_1\delta$, $y = k_2\delta$. Προσθέτοντας κατά μέλη βρίσκουμε ότι $x + y = k_1\delta + k_2\delta$ δηλαδή $x + y = (k_1 + k_2)\delta$. Επειδή και ο $k_1 + k_2$ είναι ακέραιος συμπεραίνουμε δ|x+y. ■

4.12. *Αν ο δ διαιρεί τους x, y τότε διαιρεί και κάθε γραμμικό συνδυασμό τους $px+qy$. Ιδιαιτέρως διαιρεί την διαφορά τους x-y.*

Απόδειξη: Ο δ διαιρεί τους x, y και επομένως τα πολλαπλάσια τους px, qy, άρα και το άθροισμα τους px+qy. Θέτοντας p=1, q=-1 έχουμε ότι δ|x-y. □

4.13. *Αν ο δ διαιρεί οποιουσδήποτε δύο από τους αριθμούς x, y, x+y τότε διαιρεί και τον τρίτο.*

Απόδειξη: Έχουμε να εξετάσουμε τρεις περιπτώσεις ανάλογα με το ποια είναι η δυάδα των αριθμών που διαιρεί ο δ. Αν διαιρεί τους x, y τότε όπως έχουμε δει διαιρεί και το άθροισμα τους x+y Αν δ|x, δ|x+y τότε δ|(x+y)-x δηλαδή δ|y. Όμοια και για την τρίτη περίπτωση. □

4.14. *Αν είναι α=kβ+γ τότε ο δ διαιρεί τους α, β αν και μόνο αν διαιρεί τους β, γ.*

Απόδειξη: υποθέτουμε πρώτα ότι ο δ διαιρεί τους α, β. Τότε διαιρεί και τον γραμμικό συνδυασμό τους γ=α-kβ. Αν πάλι διαιρεί τους β, υ διαιρεί και τον γραμμικό συνδυασμό τους α=kβ+γ. □

4.15. Είναι χρήσιμο να θυμόμαστε δύο βασικούς χειρισμούς που έχουν να κάνουν με τη σχέση του διαιρείν:

- Αν δ|α τότε δ|κα

- Αν δ|α, δ|β τότε δ|κα+β.

Με τον συμβολισμό του πολλαπλασίου αυτές γράφονται

- α=πολδ⇒κα=πολδ
- α=πολδ, β=πολδ⇒κα+β=πολδ

Με άλλα λόγια αν έχουμε δύο στοιχεία του συνόλου των πολλαπλασίων του δ τότε οι ακόλουθοι δύο χειρισμοί μας επιτρέπουν να παραμείνουμε στο σύνολο των πολλαπλασίων του δ

- Πολλαπλασιασμός ενός πολλαπλασίου του δ με ένα αριθμό.
- Πολλαπλασιασμός ενός πολλαπλασίου του δ με ένα αριθμό και πρόσθεση σε ένα άλλο πολλαπλάσιο του δ.

4.16. ☐ Ποιες από τις παρακάτω σχέσεις είναι σωστές και ποιες λάθος;

$$2|22,\ 22|2,\ 4\nmid 12;\ ,\ 12\nmid 4$$

4.17. ☐ Διαιρεί άραγε ο α τον 5α; Ο α τον α^2; Ο αβ τον $\alpha\beta^2$; Ο 4 τον 4444; Ο 5 τον 505050;

4.18. ☐ *Κάθε ταυτότητα που έχουμε μάθει στην Άλγεβρα η οποία αναφέρεται σε ισότητα πολυωνύμων με ακεραίους συντελεστές μας οδηγεί αυτομάτως και σε μία σχέση του διαιρείν*. Χρησιμοποιώντας ήδη γνωστά πράγματα να εξηγήσετε γιατί ισχύουν τα επόμενα. (Οι α, β, γ είναι ασφαλώς ακέραιοι)

$$\alpha+\beta|\alpha^2-\beta^2$$

$$\alpha-\beta|\alpha^2-\beta^2$$

$$\alpha-\beta|\alpha^2+\alpha\beta+\beta^2$$

$$\alpha+\beta|\alpha^2-\alpha\beta+\beta^2$$

$$\alpha+\beta+\gamma|\alpha^3+\beta^3+\gamma^3-3\alpha\beta\gamma$$

$$\alpha+\beta|\alpha^4-\beta^4$$

4.19. ☐ Για ποιες τιμές του φυσικού αριθμού α ισχύει α|12;

4.20. ☐ Να βρείτε όλα τα ζεύγη φυσικών αριθμών α, β για τα οποία ισχύει α|36 και β|α.

4.21. ☐ Να λύσετε το «σύστημα»:

$$\left.\begin{array}{l} x+y|20 \\ x|y \\ x>0 \\ y>0 \end{array}\right\}$$

4.22. ☐ Να συμπληρώσετε τον παρακάτω πίνακα σημειώνοντας ένα x στο αντίστοιχο τετραγωνάκι στην περίπτωση που ο αριθμός που βρίσκεται «οριζοντίως» διαιρεί τον αριθμό «καθέτως» :

	87	22	52	18	90	60	30	35	38
82									
69									
78									
21									
61									
2					x				
55									
86									
6									
1									
7								x	
53									
76									
68									

4.23. ☐ Να γράψετε όλους τους διαιρέτες του 24. Ποιοι από αυτούς είναι διαιρέτες του 18;

4.24. ☐ Να αποδείξετε ότι αν $\delta|x_1,\delta|x_2,...,\delta|x_v$ τότε για οποιουσδήποτε ακεραίους $k_1,k_2,...,k_v$ ισχύει

$$\delta | k_1x_1 + k_2x_2 + ... + k_vx_v$$

4.25. ☐ Στην ΄Αλγεβρα έχουμε μάθει το θεώρημα *«Αν ένα πολυώνυμο με ακέραιους συντελεστές έχει ακέραια ρίζα ρ τότε ο ρ είναι διαιρέτης του σταθερού όρου του πολυωνύμου.»*

I. Να αποδείξετε το θεώρημα. *Υπόδειξη*: Αν το πολυώνυμο είναι το $f(x)= a_vx^v + a_{v-1}x^{v-1} + ... + a_1x + a_0$ από την σχέση $f(\rho)= 0$ να συμπεράνετε ότι $\rho(a_v\rho^{v-1} + a_{v-1}\rho^{v-2} + ... + a_1) = -a_0$ και $\rho | a_0$.

II. Το θεώρημα αυτό μας επιτρέπει να συντάξουμε ένα κατάλογο των πιθανών ακεραίων ριζών του πολυωνύμου. ΄Οταν ο σταθερός όρος είναι 0 (οπότε το πολυώνυμο έχει την προφανή ρίζα 0 ο κατάλογος αυτός είναι πολύ μεγάλος: περιλαμβάνει όλους τους ακεραίους και επομένως δεν μας προσφέρει καμία πληροφορία. Υπάρχει άραγε κάποιος «μικρότερος» κατάλογος πιθανών ακεραίων ριζών;

4.26. ☐ Να αποδειχθεί ότι αν $\alpha|\beta$ τότε $\alpha|\alpha^3+\beta^3$.

4.27. ☐ Να αποδειχθεί ότι αν $\alpha|\beta$ και $\beta|\gamma$ τότε $\alpha|\alpha^2+\beta^3+\gamma^4$.

4.28. ☐ Να αποδειχθεί ότι αν $x|y+z$, $y|z+x$, $z|x+y$ τότε $xyz|(x+y+z)^3$.

4.29. ☐ Να αποδειχθεί ότι αν ο α διαιρεί τους αριθμούς που βρίσκονται σε μία γραμμή ή μία στήλη της ορίζουσας $D = \begin{vmatrix} x & y \\ z & w \end{vmatrix}$ τότε ο α διαιρεί την D.

4.30. ☐ Στο σύστημα $\left.\begin{matrix} \alpha x + \beta y = \gamma \\ \alpha' x + \beta' y = \gamma' \end{matrix}\right\} (\Sigma)$ οι συντελεστές του είναι ακέραιοι αριθμοί. Υποθέτουμε ότι το (Σ) έχει μία μόνο λύση (x, y) με $x, y \in \mathbb{Z}$.

I. Να αποδείξετε ότι $D|D_x$, $D|D_y$

II. Να αποδείξετε ότι αν $\delta|x$, $\delta|y$ τότε $D\delta|D_x$, $D\delta|D_y$.

4.31. Αν α,δ ακέραιοι με $\delta\,|\,(2\alpha+1)$ και $\delta\,|\,(3\alpha-1)$, να βρεθούν οι πιθανές θετικές τιμές του δ.

4.32. Να αποδειχτεί ότι $9^{\nu+1}-8\nu-9=$ πολ64 , για κάθε $\nu\in\mathrm{N}^*$.

4.33. Να αποδειχτεί ότι ο 3 διαιρεί τους ακεραίους α και β, αν και μόνο αν ο 3 διαιρεί το άθροισμα $\alpha^2+\beta^2$.

4.34. Να βρείτε το πλήθος των θετικών ακεραίων που δεν υπερβαίνουν τον 1000 και διαιρούνται με:

(i) τον 5, (ii) τον 25,

(iii) τον 125, (iv) τον 625.

4.35. Αν $\alpha\,|\,\beta$ και $\gamma\,|\,\delta$, να αποδείξετε ότι $\alpha\gamma\,|\,\beta\delta$.

4.36. Αν $11\,|\,(\alpha+2)$ και $11\,|\,(35-\beta)$, να αποδείξετε ότι $11|(a+\beta)$.

4.37. Αν η διαφορά δύο ακεραίων είναι άρτιος αριθμός, να αποδείξετε ότι η διαφορά των τετραγώνων τους είναι πολλαπλάσιο του 4.

4.38. Αν $m\,|\,\alpha$ και $m>1$, να αποδείξετε ότι $m\nmid\alpha+1$.

4.39. Να αποδείξετε ότι $2|(\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)$ για όλους τους ακέραιους α,β,γ.

4.40. Έστω α ένας περιττός ακέραιος. Να αποδείξετε ότι

I. Το τετράγωνο του α είναι της μορφής $\alpha^2=4\lambda+1,\ \lambda\in\mathbf{Z}$

II. $32\,|\,(\alpha^2+3)(\alpha^2+7)$

4.41. Να αποδείξετε ότι $4\nmid(\alpha^2+2)$, για κάθε $a\in\mathbf{Z}$.

4.42. Να αποδείξετε ότι δεν υπάρχουν διαδοχικοί θετικοί ακέραιοι που να είναι και οι δύο τετράγωνα ακεραίων.

4.43. ☐🕮 Αν $\beta|a$ να αποδείξετε ότι $(2^{\beta}-1)|(2^{\alpha}-1)$.

4.44. ☐🕮 Να αποδείξετε ότι

(i) Το γινόμενο τριών διαδοχικών ακεραίων διαιρείται με το 6.

(ii) $6 \mid \alpha(\alpha+1)(2\alpha+1)$ για κάθε $a \in \mathbf{Z}$

(iii) $6 \mid (\alpha^3+3\alpha^2-4\alpha)$ για κάθε $a \in \mathbf{Z}$.

4.45. ☐🕮 Να αποδείξετε ότι

(i) $3 \mid (\nu^3+2\nu)$ για κάθε $\nu \in \mathbf{N}$

(ii) $64 \mid (9^{\nu+1}-8\nu-9)$ για κάθε $\nu \in \mathbf{N}$

(iii) $5 \mid (3\cdot 27^{\nu}+2\cdot 2^{\nu})$ για κάθε $\nu \in \mathbf{N}$

(iv) $14 \mid (3^{4\nu+2}+5^{2\nu+1})$ για κάθε $\nu \in \mathbf{N}$

4.46. ☐🕮 Έστω $\alpha,\beta,\kappa,\lambda \in \mathbf{Z}$ με $\kappa \neq \lambda$. Αν $(\kappa-\lambda)|(\kappa\alpha+\lambda\beta)$, να αποδείξετε ότι $(\kappa-\lambda)|(\lambda\alpha+\kappa\beta)$.

4.47. ☐ Να αποδειχθεί ότι αν μία αριθμητική πρόοδος έχει τον πρώτο όρο α_1 και την διαφορά ω ακεραίους αριθμούς και $x|\alpha_1$, $x|\omega$ τότε ο x διαιρεί όλους τους όρους της προόδου.

4.48. ☐ Έστω κ, λ, α, β σταθεροί ακέραιοι. Έστω η ακολουθία $x_{\nu}=\kappa\alpha^{\nu}+\lambda\beta^{\nu}$, ν=1, 2, 3, ... Να αποδείξετε ότι αν κάποιος ακέραιος δ διαιρεί τους δύο πρώτους όρους της x_{ν} τότε τους διαιρεί όλους.

4.49. ☐ Χρησιμοποιείστε αυτά που ξέρετε για τα πολυώνυμα για να αποδείξετε ότι:

I. Για κάθε θετικό ακέραιο ν ισχύει $\nu+1 \mid 2\nu^3+2\nu^2-\nu-1$

II. Για κάθε ζεύγος θετικών ακεραίων ν, k ισχύει $(\nu-1)^2 \mid k\nu^{k+1}-(k+1)\nu^k+1$

4.50. ¨ Να αποδειχθεί ότι αν κ|λ τότε $\alpha^{\kappa}-\beta^{\kappa}|\alpha^{\lambda}-\beta^{\lambda}$.

4.51. ¨ Να αποδείξετε ότι το γινόμενο οσωνδήποτε διαδοχικών θετικών ακεραίων διαιρείται από το πλήθος τους.

4.52. ¨ Να αποδείξετε ότι το γινόμενο ν διαδοχικών θετικών ακεραίων διαιρείται από το ν!.

5. ΜΕΓΙΣΤΟΣ ΚΟΙΝΟΣ ΔΙΑΙΡΕΤΗΣ - ΕΛΑΧΙΣΤΟ ΚΟΙΝΟ ΠΟΛΛΑΠΛΑΣΙΟ

5.1.Βασικές έννοιες.

5.1.1. Κάθε ακέραιος αριθμός έχει και ένα σύνολο διαιρετών που είναι πάντοτε πεπερασμένο σύνολο εκτός αν πρόκειται για τον 0 που διαιρείται από όλους τους ακεραίους και επομένως έχει άπειρους το πλήθος διαιρέτες.

5.1.2. ¨ Να βρείτε όλους τους διαιρέτες του 36. Να κάνετε το ίδιο για τον -20.

5.1.3. Αν ένας αριθμός διαιρείται από τον δ τότε διαιρείται και από τον -δ. Επομένως αν γνωρίζουμε τους θετικούς διαιρέτες του γνωρίζουμε όλους τους διαιρέτες.

5.1.4. ¨ Ένας αριθμός έχει διαιρέτες μόνο τους ±1, ±3, ±7, ±21. Ποιος μπορεί να είναι ο αριθμός;

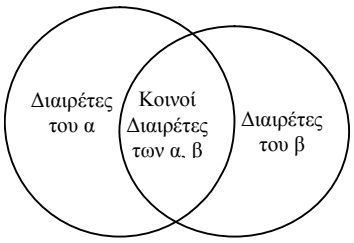
5.1.5. Στον παρακάτω πίνακα παρουσιάζονται οι θετικοί διαιρέτες των αριθμών από 1 έως 70.

1	{1}
2	{1,2}
3	{1,3}
4	{1,2,4}
5	{1,5}
6	{1,2,3,6}
7	{1,7}
8	{1,2,4,8}
9	{1,3,9}
10	{1,2,5,10}
11	{1,11}
12	{1,2,3,4,6,12}
13	{1,13}
14	{1,2,7,14}
15	{1,3,5,15}
16	{1,2,4,8,16}
17	{1,17}
18	{1,2,3,6,9,18}
19	{1,19}
20	{1,2,4,5,10,20}
21	{1,3,7,21}
22	{1,2,11,22}
23	{1,23}
24	{1,2,3,4,6,8,12,24}
25	{1,5,25}

26	{1,2,13,26}
27	{1,3,9,27}
28	{1,2,4,7,14,28}
29	{1,29}
30	{1,2,3,5,6,10,15,30}
31	{1,31}
32	{1,2,4,8,16,32}
33	{1,3,11,33}
34	{1,2,17,34}
35	{1,5,7,35}
36	{1,2,3,4,6,9,12,18,36}
37	{1,37}
38	{1,2,19,38}
39	{1,3,13,39}
40	{1,2,4,5,8,10,20,40}
41	{1,41}
42	{1,2,3,6,7,14,21,42}
43	{1,43}
44	{1,2,4,11,22,44}
45	{1,3,5,9,15,45}
46	{1,2,23,46}
47	{1,47}
48	{1,2,3,4,6,8,12,16,24,48}
49	{1,7,49}
50	{1,2,5,10,25,50}

51	{1,3,17,51}
52	{1,2,4,13,26,52}
53	{1,53}
54	{1,2,3,6,9,18,27,54}
55	{1,5,11,55}
56	{1,2,4,7,8,14,28,56}
57	{1,3,19,57}
58	{1,2,29,58}
59	{1,59}
60	{1,2,3,4,5,6,10,12,15,20,30,60}
61	{1,61}
62	{1,2,31,62}
63	{1,3,7,9,21,63}
64	{1,2,4,8,16,32,64}
65	{1,5,13,65}
66	{1,2,3,6,11,22,33,66}
67	{1,67}
68	{1,2,4,17,34,68}
69	{1,3,23,69}
70	{1,2,5,7,10,14,35,70}
71	{1,71}
72	{1,2,3,4,6,8,9,12,18,24,36,72}
73	{1,73}
74	{1,2,37,74}

5.1.6. Αν διαλέξουμε δύο οποιουσδήποτε αριθμούς α, β στον προηγούμενο βλέπουμε ότι υπάρχουν θα υπάρχουν αριθμοί που θα είναι διαιρέτες **και** των δύο. Σίγουρα ένας τέτοιος είναι ο 1 . Επίσης αν θεωρήσουμε και τους αρνητικούς διαιρέτες είναι και ο -1. Οι διαιρέτες αυτοί λέγονται **κοινοί διαιρέτες** των α, β



Το σύνολο τους δεν είναι άλλο από την τομή των συνόλων των διαιρετών τους. Επίσης το σύνολο των θετικών κοινών διαιρετών των α, β είναι οι τομή των συνόλων των θετικών διαιρετών των α, β.

Λ.χ. το σύνολο τω κοινών θετικών διαιρετών των 55, 70 είναι το

$$\{\mathbf{1}, \mathbf{5}, 11, 55\} \cap \{\mathbf{1}, 2, \mathbf{5}, 7, 10, 14, 35, 70\}$$

δηλαδή το

$$\{1, 5\}$$

Το σύνολο τω κοινών θετικών διαιρετών των 63, 74 είναι το

$$\{\mathbf{1}, 3, 7, 9, 21, 63\}\cap\{\mathbf{1}, 2, 37, 74\}$$

δηλαδή το

$$\{1\}$$

5.1.7. Να βρείτε τους κοινούς διαιρέτες των αριθμών α, β στις ακόλουθες περιπτώσεις

I. $\alpha=100, \beta=50$

II. $\alpha=2^5$, $\beta=2^6$

5.1.8. Να αποδείξετε ότι αν $\alpha|\beta$ τότε οι κοινοί διαιρέτες των α, β είναι οι διαιρέτες του β.

5.1.9. Να αποδείξετε ότι αν $\mu<\nu$ τότε οι κοινοί διαιρέτες των α^ν, α^μ είναι οι διαιρέτες του α^μ.

5.1.10. Κάθε αριθμός εκτός από διαιρέτες έχει και πολλαπλάσια. Το 0 έχει μόνο ένα πολλαπλάσιο· τον εαυτό του. Όλοι οι άλλοι ακέραιοι έχουν άπειρα πολλαπλάσια. Όπως και με τους διαιρέτες αν ένας αριθμός m είναι πολλαπλάσιο του α και ο αντίθετος του -m είναι πολλαπλάσιο του α. Διότι αφού $m=k\alpha$ είναι $-m=(-k)\alpha$. Επομένως αν γνωρίζουμε τα θετικά πολλαπλάσια ενός $\alpha\neq0$ γνωρίζουμε όλα τα πολλαπλάσια.

5.1.11. Να γράψετε όλα τα πολλαπλάσια του 4 που ανήκουν στο διάστημα $[-31, -1]$.

5.1.12. Ένας αριθμός $\alpha\neq0, \pm1$ που έχει μόνο δύο θετικούς διαιρέτες (και επομένως 4 διαιρέτες αν μετρήσουμε και τους αρνητικούς) δηλαδή τους 1 και $|\alpha|$ λέγεται **πρώτος**. Διαφορετικά λέγεται **σύνθετος**. Στον πίνακα των διαιρετών βλέπουμε ότι ο αριθμός 7 (επομένως και ο -7) είναι πρώτος. Ο 18 είναι σύνθετος. Δύο αριθμοί που έχουν μόνο ένα κοινό θετικό διαιρέτη λέγονται **σχετικά πρώτοι** δηλαδή πρώτοι ο

ένας σε σχέση με τον άλλο. Δύο σχετικά πρώτοι αριθμοί λέγονται και **πρώτοι προς αλλήλους**.

5.1.13. ¨ Ποια ζεύγη από τους αριθμούς 1,11, 21, 31, 41, 51, 61, 61, 91 είναι ζεύγη σχετικά πρώτων αριθμών;

5.1.14. ¨ Ποια από τα παρακάτω ζεύγη αριθμών είναι αριθμοί σχετικά πρώτοι;

α) 11, 33 β) 12, 34

γ) 13, 35 δ) 15, 45

5.1.15. ¨ Να αποδείξετε ότι αν οι α, β είναι σχετικά πρώτοι και γ|β τότε και οι α, γ είναι σχετικά πρώτοι.

5.1.16. ¨Με φ(ν) (*Συνάρτηση φι του Euler*) συμβολίζουμε το πλήθος των θετικών ακεραίων που είναι δεν υπερβαίνουν τον θετικό ακέραιο ν και είναι σχετικά πρώτοι προς αυτόν. Λ.χ. είναι φ(10)=4 διότι οι από του; αριθμούς 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 σχετικά πρώτοι προς το 10 είναι οι εξής 4: 1, 3, 7, 9.

I. Να υπολογίσετε την παράσταση φ(20)+φ(30)+φ(40)

II. Να κάνετε την γραφική παράσταση τη φ για $1\le\nu\le20$. Επειδή η φ είναι ακολουθία θα έχετε μεμονωμένα σημεία.

5.1.17. Σε αντίθεση με την εύρεση των θετικών διαιρετών ενός αριθμού α (που γενικά είναι επίπονη διαδικασία˙ υπάρχουν αριθμοί που δεν είναι γνωστοί οι διαιρέτες τους) το να βρούμε τα θετικά πολλαπλάσια του $\alpha\neq0$ είναι εύκολη δουλειά και μπορεί να γίνει μόνο κάνοντας πρόσθεση. Τα θετικά πολλαπλάσια του α είναι τα:

|α| |α|+|α| |α|+|α|+|α| |α|+|α|+|α|+|α| ....

Αποτελούν μία αριθμητική πρόοδο με πρώτο όρο τον |α| και διαφορά τον |α| και επομένως το νι-οστό θετικό πολλαπλάσιο του α είναι ο ν|α|.

5.1.18. Στον πίνακα που ακολουθεί φαίνονται τα σύνολα των θετικών πολλαπλασίων των αριθμών 1-19.

Αριθμός	Σύνολο θετικών πολλαπλασίων
1	{1,2,3,4,5,6,7,8,9,10,...}
2	{2,4,6,8,10,12,14,16,18,20,...}
3	{3,6,9,12,15,18,21,24,27,30,...}
4	{4,8,12,16,20,24,28,32,36,40,...}
5	{5,10,15,20,25,30,35,40,45,50,...}
6	{6,12,18,24,30,36,42,48,54,60,...}
7	{7,14,21,28,35,42,49,56,63,70,...}
8	{8,16,24,32,40,48,56,64,72,80,...}
9	{9,18,27,36,45,54,63,72,81,90,...}
10	{10,20,30,40,50,60,70,80,90,100,...}
11	{11,22,33,44,55,66,77,88,99,110,...}
12	{12,24,36,48,60,72,84,96,108,120,...}
13	{13,26,39,52,65,78,91,104,117,130,...}
14	{14,28,42,56,70,84,98,112,126,140,...}
15	{15,30,45,60,75,90,105,120,135,150,...}
16	{16,32,48,64,80,96,112,128,144,160,...}
17	{17,34,51,68,85,102,119,136,153,170,...}
18	{18,36,54,72,90,108,126,144,162,180,...}
19	{19,38,57,76,95,114,133,152,171,190,...}

5.1.19. Είδαμε ότι το σύνολο των διαιρετών ενός $\alpha\neq 0$ είναι πεπερασμένο. Φυσικά και το σύνολο των θετικών διαιρετών του α είναι και αυτό πεπερασμένο. Αν $\beta\neq 0$ τότε και το σύνολο των κοινών διαιρετών των α, β είναι πεπερασμένο. Επομένως (βλ. **2.19.**) θα έχει κάποιο στοιχείο που θα είναι **μέγιστο** δηλαδή μεγαλύτερο ή ίσο από όλα τα υπόλοιπα. Ο αριθμός αυτός είναι ο μεγαλύτερος από τους κοινούς διαιρέτες που έχουν οι α, β και θα είναι θετικός αριθμός, ονομάζεται **μέγιστος κοινός διαιρέτης** των α, β συμβολίζεται[2] δε με (α, β).

Για παράδειγμα οι κοινοί διαιρέτες των 22, 18 είναι οι ±1, ±2 και ο μεγαλύτερος από αυτούς είναι ο 2. Επομένως (12, 22)=2.

5.1.20. *Είναι* $(\alpha, \beta)=(\beta,\alpha)$.

Απόδειξη. Είτε θεωρήσουμε τους κοινούς διαιρέτες των α, β είτε τους κοινούς διαιρέτες των β, α αναφερόμαστε στους ίδιους αριθμούς. Επομένως και οι μέγιστοι από αυτούς συμπίπτουν.

[2] **Προσοχή** χρησιμοποιείται ο ίδιος συμβολισμός με εκείνον του διατεταγμένου ζεύγους, του διανύσματος , του σημείου και του ανοικτού διαστήματος. Από τα συμφραζόμενα καταλαβαίνουμε περί τίνος πρόκειται

5.1.21. ¨ Να βρείτε τον μέγιστο κοινό διαιρέτη των αριθμών 34, 45.

5.1.22. Ποιός είναι ο μέγιστος κοινός διαιρέτης των αριθμών 12 και -3;

5.1.23. ¨ Να βρείτε την τιμή της παράστασης

(2, 12)+(-24,45)+1

5.1.24. ¨ Να λύσετε τις εξισώσεις

(3, 4)=x (x, 3)=3 (x, 4)=3

5.1.25. Ανάλογα με τους κοινούς διαιρέτες δύο αριθμών ορίζονται και τα κοινά πολλαπλάσια. Δοθέντων δύο αριθμών α, β υπάρχουν αριθμοί όπως λ.χ. το γινόμενο τους αβ που είναι πολλαπλάσια **και** του α **και** του β. Οι αριθμοί αυτοί λέγονται **κοινά πολλαπλάσια των** α, β. Το σύνολο των κοινών πολλαπλασίων των α, β δεν είναι άλλο από την τομή του συνόλου των πολλαπλασίων του α με το σύνολο των πολλαπλασίων του β. Λ.χ. το σύνολο των πολλαπλασίων του 6 είναι το

$$\{\pm 6, \pm 12, \pm 18, \mathbf{\pm 24}, \pm 30, \pm 36, \pm 42, \mathbf{\pm 48}, \pm 54, \pm 60, ...\}$$

ενώ του -8 το

$$\{\pm 8, \pm 16, \mathbf{\pm 24}, \pm 32, \pm 40, \mathbf{\pm 48}, \pm 56, \pm 64, \mathbf{\pm 72}, \pm 80, ...\}$$

Το σύνολο των κοινών πολλαπλασίων των 6 και -8 είναι η τομή των δύο αυτών συνόλων δηλαδή το

$$\{\pm 24, \pm 48, \pm 73, ...\}$$

Το σύνολο των κοινών πολλαπλασίων δύο μη μηδενικών αριθμών α, β περιέχει οπωσδήποτε και τον θετικό αριθμό |α||β|. Επομένως δύο μη μηδενικοί αριθμοί έχουν και θετικά κοινά πολλαπλάσια. Το σύνολο των θετικών κοινών πολλαπλασίων των α, β είναι ένα υποσύνολο των θετικών ακεραίων και επομένως (παράδειγμα 2.19.) θα έχει ένα στοιχείο που θα είναι μικρότερο ή ίσο από άλλα δηλαδή ένα **ελάχιστο** στοιχείο. Το ελάχιστο αυτό κοινό θετικό πολλαπλάσιο των α, β ονομάζεται **ελάχιστο**

κοινό πολλαπλάσιο των α, β και συμβολίζεται[3] με [α, β]. Για παράδειγμα το σύνολα των θετικών πολλαπλασίων των αριθμών -9, -6 είναι αντιστοίχως τα:

$$\{9,\mathbf{18},27,\mathbf{36},45,\mathbf{54},63,\mathbf{72},81,\mathbf{90},...\}$$

$$\{6,12,\mathbf{18},24,30,\mathbf{36},42,48,\mathbf{54},60,...\}$$

και το σύνολο των θετικών κοινών πολλαπλασίων, δηλαδή η τομή τους, είναι το

$$\{18,36,54,72,90,...\}$$

Το ελάχιστο στοιχείο του συνόλου αυτού είναι το 18. Επομένως το ελάχιστο κοινό πολλαπλάσιο των -9, -6 είναι το 18 δηλαδή [-9, -6]=18.

5.1.26. Είναι [α, β]=[β,α]

Απόδειξη. Δείτε την απόδειξη της αντίστοιχης ιδιότητας για τον μέγιστο κοινό διαιρέτη. ■

5.1.27. Να βρείτε το [34, 12].

5.1.28. Να βρείτε τον x όταν είναι γνωστό ότι [x, 10]=20

5.1.29. Να λύσετε το «σύστημα»

$$[x,10]= 40$$
$$(x,12)= 4$$

5.2. Οι βασικές προτάσεις στον μέγιστο κοινό διαιρέτη και στο ελάχιστο κοινό πολλαπλάσιο.

5.2.1. *Ισχύει*

$$(\alpha, \beta)=(-\alpha, \beta)=(\alpha, -\beta)=(-\alpha, -\beta)=(|\alpha|, |\beta|)$$

$$[\alpha, \beta]=[-\alpha, \beta]=[\alpha, -\beta]=[-\alpha, -\beta]=[|\alpha|, |\beta|]$$

[3] Ισχύει ανάλογη επισήμανση με εκείνη που κάναμε για τον μέγιστο κοινό διαιρέτη. Δεν πρέπει να συγχέουμε το ελάχιστο κοινό πολλαπλάσιο [α, β] με το κλειστό διάστημα [α, β].

Απόδειξη. Οι αριθμοί -α, και α έχουν τους ίδιους διαιρέτες. Επίσης και οι β, β έχουν τους ίδιους διαιρέτες. Επομένως τα ζεύγη

$$\alpha, \beta \quad -\alpha, \beta \quad \alpha, -\beta \quad -\alpha, \beta$$

έχουν τους ίδιους κοινούς διαιρέτες. Αυτό σημαίνει ότι έχουν και τους ίδιους θετικούς κοινούς διαιρέτες άρα και τον ίδιο μέγιστο κοινό διαιρέτη.

Συνεπώς $(\alpha, \beta)=(-\alpha, \beta)=(\alpha, -\beta)=(-\alpha, -\beta)$

Τέλος ο $(|\alpha|, |\beta|)$ είναι κάποιος από τους παραπάνω τέσσερις αριθμούς και επομένως είναι ίσος με αυτούς.

Ακριβώς τον ίδιο συλλογισμό μπορούμε να κάνουμε και για το ελάχιστο κοινό πολλαπλάσιο. Η απόδειξη θα είναι ίδια με την προηγούμενη αρκεί η λέξη «διαιρέτης» να αντικατασταθεί με την λέξη «πολλαπλάσιο» ■

5.2.2. *Αν $\alpha=k\beta+\gamma$ τότε οι κοινοί διαιρέτες των α, β συμπίπτουν με τους κοινούς διαιρέτες των β, γ.*

Απόδειξη: Είδαμε ότι ο δ διαιρεί τους α, β αν και μόνο αν διαιρεί τους β, γ. Επομένως κάθε κοινός διαιρέτης των α, β είναι και κοινός διαιρέτης των β, γ και κάθε κοινός διαιρέτης των β, γ είναι και κοινός διαιρέτης των α, β. ΄Αρα οι κοινοί διαιρέτες των α, β συμπίπτουν με τους κοινούς διαιρέτες των α, γ. ■

5.2.3. *Αν $\alpha=k\beta+\gamma$ τότε ο μέγιστος κοινός διαιρέτης των α, β είναι ίσος με τον μέγιστο κοινό διαιρέτη των β, γ. Δηλαδή $(\alpha, \beta)=(\beta, \gamma)$.*

Απόδειξη: Διότι αφού οι κοινοί διαιρέτες των α, β και β, γ συμπίπτουν και οι μέγιστοι εξ΄αυτών συμπίπτουν.

5.2.4. *Αν προσθέσουμε στον α ένα πολλαπλάσιο του β τότε ο μέγιστος κοινός διαιρέτης δεν αλλάζει. Δηλαδή $(\alpha, \beta)=(\alpha+ k\beta, \beta)$.*

Ειδικά αν προσθέσουμε ή αφαιρέσουμε από τον α τον β ο μέγιστος κοινός διαιρέτης δεν αλλάζει δηλαδή $(\alpha, \beta)=(\alpha-\beta, \beta)=(\alpha+\beta, \beta)$

Απόδειξη: Το πρώτο σκέλος είναι συνέπεια του προηγουμένου αν πάρουμε γ=α+(-k)β.

Το δεύτερο είναι συνέπεια του πρώτου αν πάρουμε k=±1. ■

5.2.5. *Αν υ είναι το υπόλοιπο της διαίρεσης α:β τότε* $(\alpha, \beta)=(\beta, \upsilon)$

Απόδειξη: Αρκεί να παρατηρήσουμε ότι α=πβ+υ. ■

5.2.6. Ας βρούμε τον μέγιστο κοινό διαιρέτη των ν+1, ν. έχουμε:

(ν+1, ν)=(αφαιρούμε από το ν+1 το ν)

=(ν, 1)=(οι κοινοί διαιρέτες των ν και 1 είναι οι ±1) =1

5.2.7. Ας βρούμε τον μέγιστο κοινό διαιρέτη των 3ν+1, 2ν-1. Έχουμε:

(3ν+1, 2ν-1)=(αφαιρούμε από το 3ν+1 το 2ν-1)

=(ν+2, 2ν-1)=(προσθέτουμε στο 2ν-1 το (-2)(ν+2))

=(ν+2, -5)= (προσθέτουμε στο ν+2 το -5)

=(ν-3, -5)= (στη θέση του -5 γράφουμε το 5)

=(ν-3, 5)

5.2.8. Έστω οι αριθμοί α=123, β=33. Διαιρώντας το α:β βρίσκουμε

$$\mathbf{\alpha}=3\cdot\mathbf{33}+\mathbf{24}$$

Διαιρώντας τον διαιρέτη της προηγούμενης διαίρεσης β=33 με το υπόλοιπο της 24 βρίσκουμε

$$\mathbf{33}=1\cdot\mathbf{24}+\mathbf{9}$$

Διαιρώντας τον διαιρέτη 24 της προηγούμενης διαίρεσης με το υπόλοιπο της 9 βρίσκουμε

$$\mathbf{24}=2\cdot\mathbf{9}+\mathbf{6}$$

Διαιρώντας τον διαιρέτη 9 της προηγούμενης διαίρεσης με το υπόλοιπο της 6 βρίσκουμε

$$\mathbf{9}=1\cdot\mathbf{6}+\mathbf{3}$$

Διαιρώντας τον διαιρέτη 6 της προηγούμενης διαίρεσης με το υπόλοιπο της 3 βρίσκουμε

$$\mathbf{9}=2\cdot\mathbf{3}+\mathbf{0}$$

Είναι (123, 33)=(33, 24)=(24, 9)=(9, 6)=(6, 3)=3

5.2.9. *Αν η διαίρεση α:β αφήνει υπόλοιπο $υ_1$, η διαίρεση β:$υ_1$ αφήνει υπόλοιπο $υ_2$, η διαίρεση β:$υ_1$ αφήνει υπόλοιπο $υ_3$, κ.ο.κ τότε κάποια από τις διαιρέσεις αυτές είναι τέλεια και ο διαιρέτης αυτής της διαίρεσης είναι ο μέγιστος κοινός διαιρέτης των α, β.*

Απόδειξη: Εκτελούμε την διαίρεση α:β. Αν βρούμε υπόλοιπο 0 τότε ο β είναι διαιρέτης του α και ο μέγιστος κοινός διαιρέτης των α, β είναι ο β. Αν όχι θα βρούμε κάποιο μη μηδενικό υπόλοιπο $υ_1$ το οποίο θα είναι μικρότερο του β. ΄Ο μέγιστος κοινός διαιρέτης των α, β είναι ταυτοχρόνως ο μέγιστος κοινός διαιρέτης των β, $υ_1$. Διαιρούμε τον α με τον $υ_1$. Θα βρούμε κάποιο υπόλοιπο $υ_2$. Αν συμβαίνει το υπόλοιπο αυτό να είναι 0 τότε ο $υ_1$ είναι διαιρέτης του β και επομένως ο μέγιστος κοινός διαιρέτης των β, $υ_1$ που με την σειρά του είναι ο μέγιστος κοινός διαιρέτης των α, β. Αν ο $υ_2$ είναι διάφορος του μηδενός θα είναι οπωσδήποτε μικρότερος του διαιρέτη της διαίρεσης από την οποία έχει προέλθει δηλαδή του $υ_1$ που με την σειρά του είναι μικρότερος του β. Συνεχίζουμε αυτή την διαδικασία όσες φορές χρειασθεί έως ότου βρούμε υπόλοιπο 0. Το αμέσως προηγούμενο υπόλοιπο-που θα είναι διάφορο του μηδενός- είναι ο μέγιστος κοινός διαιρέτης των α, β. Λέμε όσες φορές χρειασθεί εννοώντας ότι κάποτε αυτή η διαδικασία θα τερματισθεί. Και έτσι είναι διότι κάθε φορά τα υπόλοιπα που βρίσκουμε είναι μικρότερα αλλά ως υπόλοιπα δε μπορεί να είναι μικρότερα από το 0. Στην πρώτη διαίρεση τα δυνατά υπόλοιπα είναι 0, 1, 2, ...,

β-1 στην επόμενη είναι κατά ένα λιγότερα και οι επιλογές λιγοστεύουν μετά από κάθε διαίρεση. Επομένως το πολύ μετά από β βήματα θα βρούμε μηδενικό υπόλοιπο. ■

5.2.10. *Ο μέγιστος κοινός διαιρέτης των θετικών ακεραίων α, β γράφεται ως γραμμικός συνδυασμός των α, β.*

***Απόδειξη*:** Ας πούμε ότι α≥β. Διαιρώντας το α με το β, το β με το υπόλοιπο της διαίρεσης αυτής κ.ο.κ θα καταλήξουμε στον (α, β) που θα είναι το τελευταίο μη μηδενικό υπόλοιπο που συναντάμε σε αυτή την αλληλουχία διαιρέσεων. Ξέρουμε το υπόλοιπο μίας διαίρεσης είναι γραμμικός συνδυασμός του διαιρέτη και του διαιρετέου. ΄Αρα ο (α, β) είναι γραμμικός συνδυασμός του διαιρέτη και του διαιρετέου της διαίρεσης από την οποία προκύπτει. Αλλά ο διαιρέτης αυτής της διαίρεσης είναι γραμμικός συνδυασμός του διαιρέτη και του διαιρετέου της αμέσως προηγούμενης διαίρεσης. Δηλαδή ο (α, β) είναι γραμμικός συνδυασμός όχι μόνο διαιρέτη-διαιρετέου της διαίρεσης από την οποία προκύπτει αλλά και γραμμικός συνδυασμός του διαιρέτη-διαιρετέου της αμέσως προηγούμενης διαίρεσης. Προχωρώντας βήμα-βήμα συμπεραίνουμε ότι ο (α, β) είναι συνδυασμός των α, β. ■

5.2.11. Ας εκφράσουμε τον μέγιστος κοινό διαιρέτη των α=123, β=33 ως γραμμικό συνδυασμό τους. ΄Εχουμε τις ισότητες

Ισότητα που προκύπτει από την διαίρεση	΄Εκφραση του υπολοίπου ως γραμμικού συνδυασμού διαιρετέου-διαιρέτη
$123=3\cdot 33+24$	$24=123-3\cdot 33$
$33=1\cdot 24+9$	$9=33-1\cdot 24$
$24=2\cdot 9+6$	$6=24-2\cdot 9$
$9=1\cdot 6+3$	$3=9-1\cdot 6$
$9=3\cdot 3+0$	(123, 33)=3

Είναι

$3=9-1\cdot 6=9-1\cdot(24-2\cdot 9)=3\cdot 9-1\cdot 24=3\cdot(33-1\cdot 24)-1\cdot 24=$

$3\cdot 33-4\cdot 24=3\cdot 33-4\cdot(123-3\cdot 33)=-4\cdot 123+15\cdot 33$

Επομένως είναι (α, β)=-4α+15β.

5.2.12. Ο μέγιστος κοινός διαιρέτης δύο αριθμών γράφεται μεν ως γραμμικός συνδυασμός τους αλλά οι συντελεστές αυτού του γραμμικού συνδυασμού δεν είναι μοναδικοί. Λ.χ. όπως είδαμε πριν είναι με α=123, β=33 είναι

(α, β)=3=-4α+15β. Αλλά υπάρχουν και άλλοι συντελεστές εκτός από τους -4, 15 με τους οποίους επιτυγχάνεται το ίδιο αποτέλεσμα. Δεν είναι δύσκολο να διαπιστώσετε ότι (α, β)=194α-723β.

5.2.13. ☐ *Οι α, β είναι σχετικά πρώτοι αν και μόνο αν υπάρχουν κ, λ έτσι ώστε*

κα+λβ=1

Απόδειξη. Αν οι α, β είναι σχετικά πρώτοι τότε ο μέγιστος κοινός διαιρέτης τους αφενός είναι 1 και αφετέρου όπως κάθε μέγιστος κοινός διαιρέτης δύο αριθμών είναι ένας θετικός γραμμικός συνδυασμός τους κα+λβ. ΄Αρα υπάρχουν κ, λ έτσι ώστε κα+λβ=1. Αντιστρόφως αν υπάρχουν κ, λ έτσι ώστε κα+λβ=1 και δ είναι ένας κοινός διαιρέτης των α, β τότε ο δ διαιρεί τους α, β και επομένως τον γραμμικός συνδυασμός τους κα+λβ. ΄Αρα δ|1. Ο δ λοιπόν είναι ±1. Συνεπώς οι κοινοί διαιρέτες των α, β είναι οι +1, -1 και ο μέγιστος από αυτούς είναι ο 1 δηλαδή (α, β)=1. ■

5.2.14. ☐ *Για κάθε ζεύγος ακεραίων α, β με β*≠0 *ο (α,β) είναι θετικός γραμμικός συνδυασμός των α, β.*

Απόδειξη. Είναι (α, β)=(|α|, |β|). Αν είναι α=0 τότε

(α, β)=|β| και |β|=1α+(±1)β. (Το + αν β>0 και το - αν β<0).

Αν α≠0 τότε υπάρχουν κ, λ έτσι ώστε

(α, β)=(|α|, |β|)=κ|α|+λ|β|= (±κ)α+(±λ)β

5.2.15. ☐ *Ο (α,β) είναι ο ελάχιστος θετικός γραμμικός συνδυασμός των α, β.*

Απόδειξη. Ο (α, β) ασφαλώς είναι ένας θετικός γραμμικός συνδυασμός των α, β. Πρέπει να δείξουμε ότι είναι μικρότερος ή ίσος από κάθε θετικό γραμμικό συνδυασμό των α, β. Έστω δ=(α, β). Έστω x=κα+λβ ένας θετικός γραμμικός συνδυασμός των α, β. Είναι x>0. Επειδή δ|α, δ|β συμπεραίνουμε ότι δ| κα+λβ δηλαδή δ|x. Οι δ, x είναι θετικοί ακέραιοι και επομένως δ≤x.

5.2.16. *Αν ένας αριθμός x διαιρεί τους α, β διαιρεί και τον μέγιστο κοινό διαιρέτη* (α,β) *των α, β.*

Απόδειξη. Αφού ο x διαιρεί τους α, β διαιρεί και κάθε γραμμικό συνδυασμό τους επομένως και τον (α,β).

5.2.17. *Αν ν≥2 και* $a_1,a_2,...,a_v$ *είναι ν ακέραιοι διάφοροι του μηδενός τότε:*

I. Ο μέγιστος κοινός διαιρέτης τους $(a_1,a_2,...,a_v)$ *είναι γραμμικός συνδυασμός τους.*

II. Κάθε κοινός διαιρέτης των $a_1,a_2,...,a_v$ *διαιρεί τον* $(a_1,a_2,...,a_v)$.

III.Ο $(a_1,a_2,...,a_v)$ *είναι ο ελάχιστος θετικός γραμμικός συνδυασμός των* $a_1,a_2,...,a_v$

Απόδειξη.

I. Θα αποδείξουμε ότι ο $(a_1,a_2,...,a_v)$ *είναι* γραμμικός συνδυασμός των $a_1,a_2,...,a_v$ με επαγωγή στο ν. Αν ν=2 το αποδεικτέο ισχύει. Έστω ότι ισχύει για ν=k δηλαδή έστω ότι ο μέγιστος κοινός διαιρέτης k αριθμών είναι γραμμικός συνδυασμός αυτών των αριθμών. Θα δείξουμε ότι το αποδεικτέο ισχύει και για ν=k+1 συγκεκριμένα θα δείξουμε ότι ο μέγιστος κοινός διαιρέτης k+1 αριθμών $a_1,a_2,...,a_k,a_{k+1}$ είναι γραμμικός συνδυασμός αυτών των αριθμών. Ισχύει $(a_1,a_2,...,a_k,a_{k+1})=((a_1,a_2,...,a_k),a_{k+1})$. Όμως ο μέγιστος κοινός διαιρέτης των αριθμών $(a_1,a_2,...,a_k)$, a_{k+1} είναι γραμμικός συνδυασμός τους δηλαδή υπάρχουν x, y έτσι ώστε

$$((a_1,a_2,...,a_k),a_{k+1})=x(a_1,a_2,...,a_k)+ya_{k+1} \quad \textbf{(1)}$$

Από την υπόθεση της επαγωγής και ο $(a_1,a_2,...,a_k)$ είναι γραμμικός συνδυασμός των $a_1,a_2,...,a_k$ δηλαδή υπάρχουν $x_1,x_2,...,x_k$ έτσι ώστε

$$(a_1,a_2,...,a_k)= x_1a_1 + x_2a_2 +...+x_ka_k \qquad \textbf{(2)}$$

Αντικαθιστούμε το $(a_1,a_2,...,a_k)$ από την (2) στην (1) και έχουμε $((a_1,a_2,...,a_k),a_{k+1})= x(x_1a_1 + x_2a_2 +...+x_ka_k)+ya_{k+1}$ Κάνοντας τις πράξεις βρίσκουμε ότι $(a_1,a_2,...,a_k,a_{k+1})=(xx_1)a_1 +(xx_2)a_2 +...+(xx_k)a_k + ya_{k+1}$ Επομένως ο $(a_1,a_2,...,a_k,a_{k+1})$ είναι γραμμικός συνδυασμός των $a_1,a_2,...,a_k,a_{k+1}$.

II. Ας υποθέσουμε τώρα ότι ο δ είναι κοινός διαιρέτης των $a_1,a_2,...,a_v$. Ο μέγιστος κοινός διαιρέτης τους $(a_1,a_2,...,a_v)$ γράφεται ως γραμμικός συνδυασμός τους δηλαδή υπάρχουν $x_1,x_2,...,x_v$ έτσι ώστε $(a_1,a_2,...,a_v)= x_1a_1 + x_2a_2 +...+x_va_v$. Ο δ διαιρεί κάθε ένα από τους $a_1,a_2,...,a_v$ επομένως και τα πολλαπλάσια τους $x_1a_1, x_2a_2, ..., x_va_v$ άρα και το άθροισμα τους $x_1a_1 + x_2a_2 +...+x_va_v$. Επομένως $\delta|(a_1,a_2,...,a_v)$.

III.Ο $(a_1,a_2,...,a_v)$ είναι κάποιος γραμμικός συνδυασμός $x_1a_1 + x_2a_2 +...+x_va_v$ των $a_1,a_2,...,a_v$. Θα είναι $x_1a_1 + x_2a_2 +...+x_va_v > 0$ διότι $(a_1,a_2,...,a_v)> 0$. Αν τώρα $y_1a_1 + y_2a_2 +...+y_va_v$ είναι ένας οποιοσδήποτε θετικός γραμμικός συνδυασμός των $a_1,a_2,...,a_v$ τότε αφού ο $(a_1,a_2,...,a_v)$ είναι διαιρέτης των $a_1,a_2,...,a_v$ θα είναι διαιρέτης και του $y_1a_1 + y_2a_2 +...+y_va_v$. ΄Αρα επειδή πρόκειται για θετικούς αριθμούς θα είναι

$$(a_1,a_2,...,a_v)\le y_1a_1 + y_2a_2 +...+y_va_v$$

πράγμα που σημαίνει ότι $x_1a_1 + x_2a_2 +...+x_va_v\le y_1a_1 + y_2a_2 +...+y_va_v$

Επομένως ο μέγιστος κοινός διαιρέτης των $a_1,a_2,...,a_v$ είναι ο πιο μικρός θετικός γραμμικός συνδυασμός των $a_1,a_2,...,a_v$. ■

Αν οι α, β είναι σχετικά πρώτοι και α|βx τότε α|x.

Απόδειξη. Αφού οι α, β είναι σχετικά πρώτοι υπάρχουν κ, λ έτσι ώστε κα+λβ=1. Πολλαπλασιάζοντας την σχέση αυτή με x βρίσκουμε ότι καx+λβx=x. Στην σχέση αυτή α διαιρεί και τους δύο προσθετέους του πρώτου μέλους της επομένως και το δεύτερο. ■

5.2.18. Προσέξτε ότι το συμπέρασμα στην παραπάνω ιδιότητα παύει να ισχύει όταν οι α, β δεν είναι σχετικά πρώτοι. Π.χ. με α=9, β=3, x=12 είναι α|βx αλλά α ∤ x.

5.2.19. *Αν οι α, β είναι σχετικά πρώτοι και α|γ, β|γ τότε αβ|γ.*

Απόδειξη. Ξέρουμε ότι β|γ. Επομένως υπάρχει k έτσι ώστε γ=xβ. Αφού α|γ είναι α|xβ. Όμως οι α, β είναι σχετικά πρώτοι επομένως α|x. Άρα δηλαδή αβ|γ. ■

5.2.20. *Αν δ=(α, β) τότε ο δ διαιρεί τους α, β και τα πηλίκα των διαιρέσεων α:δ, β:δ είναι αριθμοί σχετικά πρώτοι.*

Απόδειξη. Το ότι ο δ διαιρεί τους α, β έχει ήδη αποδειχθεί. Έστω ότι δ=κα+λβ. Τότε διαιρώντας δια δ έχουμε $\frac{\delta}{\delta}=\kappa\frac{\alpha}{\delta}+\lambda\frac{\beta}{\delta}$ δηλαδή $\kappa\frac{\alpha}{\delta}+\lambda\frac{\beta}{\delta}=1$. Από την τελευταία σχέση συμπεραίνουμε ότι οι ακέραιοι αριθμοί $\frac{\alpha}{\delta},\frac{\beta}{\delta}$ είναι σχετικά πρώτοι. ■

5.2.21. *Είναι* $[\alpha, \beta](\alpha, \beta)=\alpha\beta$

Απόδειξη. Έστω δ=(α, β). Είναι α=α΄δ, β=β΄δ και οι α΄, β΄ είναι σχετικά πρώτοι. Έστω τώρα x ένα θετικό κοινό πολλαπλάσιο των α, β. Αφού το ο x είναι πολλαπλάσιο του α υπάρχει y έτσι ώστε

$$x=y\alpha$$

Αντικαθιστώντας στην θέση του α το α=α΄δ έχουμε ότι

$$x=y\,\alpha'\delta$$

Ο β διαιρεί τον x επομένως β΄δ| y α΄δ . Απλοποιώντας το δ βρίσκουμε β΄ | y α΄. ΄Ομως οι α΄, β΄ είναι σχετικά πρώτοι και αναγκαστικά β΄ | y . ΄Αρα υπάρχει z έτσι ώστε

$$y=z\beta$$

Συνοψίζοντας έχουμε ότι

$$x=y\alpha=y\alpha=y\alpha'\delta=z\beta\alpha'\delta=z\alpha'\beta'\delta$$

Κάθε λοιπόν θετικό πολλαπλάσιο των α, β είναι της μορφής zα΄β΄δ, z>0 και κάθε αριθμός της μορφής zα΄β΄δ με z>0 είναι ένα θετικό πολλαπλάσιο των α, β. Με άλλα λόγια τα θετικά πολλαπλάσια των α, β είναι ακριβώς οι αριθμοί της μορφής

$$z\alpha'\beta'\delta \text{ με } z>0$$

Επειδή οι α΄, β΄, δ είναι δεδομένοι το πολλαπλάσιο zα΄β΄δ είναι ελάχιστο όταν z=1. ΄Αρα

$$[\alpha, \beta]=\alpha'\beta'\delta$$

Πολλαπλασιάζοντας και διαιρώντας το α΄β΄δ με δ βρίσκουμε ότι

$$[\alpha, \beta]=\frac{\alpha'\delta\beta'\delta}{\delta}=\frac{\alpha\beta}{\delta} \text{ άρα } [\alpha, \beta](\alpha, \beta)=\alpha\beta \quad \blacksquare$$

5.2.22. ☐ *Αν α|x και β|x τότε* $[\alpha, \beta] \mid x$ *δηλαδή κάθε κοινό πολλαπλάσιο των α, β είναι και πολλαπλάσιο του ελάχιστου κοινού πολλαπλασίου των α, β.*

Απόδειξη. Αν δ=(α, β) τότε α=α΄δ, β=β΄δ και οι α΄, β΄ είναι σχετικά πρώτοι. Αφού α|x, β|x υπάρχουν ακέραιοι y, z έτσι ώστε

$$x=y\alpha,\ x=z\beta$$

και επομένως

$$x=y\alpha'\delta,\ x=z\beta'\delta \quad \textbf{(1)}$$

Εξισώνοντας έχουμε

$$y\alpha'\delta=z\beta'\delta$$

και απλοποιώντας το δ έχουμε

$$yα΄=zβ΄$$

Από την ισότητα αυτή συμπεραίνουμε ότι

$$α΄|zβ΄, β΄|yα΄$$

Επειδή οι α΄, β΄ είναι σχετικά πρώτοι έχουμε ότι

$$α΄|z \text{ και } β΄|y$$

Επομένως υπάρχουν z΄, y΄ έτσι ώστε

$$z=z΄α΄ \text{ και } y=y΄β΄ \quad \textbf{(2)}$$

Αντικαθιστώντας στην πρώτη σχέση από τις (1) το y από την (2) βρίσκουμε ότι

$$x= y΄β΄α΄δ= y΄β΄α΄δ=\frac{α΄δβ΄δ}{δ} = y΄[α, β]$$

Επομένως το x διαιρείται από το [α, β]. ■

5.3. Μέγιστος κοινός διαιρέτης και ελάχιστο κοινό πολλαπλάσιο περισσοτέρων ακεραίων.

5.3.1. Γενικότερα αν έχουμε περισσότερους αριθμούς α, β, γ, δ, ... κοινοί διαιρέτες τους λέγονται οι αριθμοί που είναι διαιρέτες όλων των α, β, γ, δ, ... και ο μέγιστος τους λέγεται **μέγιστος κοινός διαιρέτης** των α, β, γ, δ, ... συμβολίζεται δε με $(α, β, γ, δ, ...)$. Για παράδειγμα οι αριθμοί 16, 24, -36 έχουν κοινούς διαιρέτες τους ±1, ±2, ±4 και επομένως $(16, 24, 36)=4$.

5.3.2. ΄Οπως και για δύο αριθμούς η σειρά με την οποία λαμβάνεται ο μέγιστος κοινός διαιρέτης δεν έχει σημασία. Αυτό συμβαίνει διότι όταν αναφερόμαστε στο μέγιστο κοινό διαιρέτη κάποιων ακεραίων αναφερόμαστε στο σύνολο των ακεραίων αυτών.

΄Ετσι

(α, β, γ)=(α, γ, β)=(γ, α, β) ή (x, y, z, w)=(w, y, x, z) κ.τ.λ. Ανάλογη παρατήρηση ισχύει για περισσότερους αριθμούς.

5.3.3. ☐ Να βρείτε τους κοινούς διαιρέτες των αριθμών α, β, γ στις ακόλουθες περιπτώσεις

I. α=100, β=50, γ=80

II. $\alpha=2^5$, $\beta=2^6$, $\beta=2^7$

5.3.4. ☐ Να βρείτε την τιμή της παράστασης

(-36, (72, 63))

5.3.5. ☐ Να βρείτε την τιμή της παράστασης

(1, (2, (3, (4, (5, (6, (7, (8, (9, 10)))))))))

5.3.6. Οι αριθμοί α, β, γ, .., λέγονται **σχετικά πρώτοι** αν οι μόνοι κοινοί διαιρέτες τους είναι οι ±1. ΄Οταν ελέγχουμε κατά πόσο κάποιοι αριθμοί είναι σχετικά πρώτοι κοιτάμε τους κοινούς διαιρέτες που διαθέτουν *όλοι μαζί* και όχι κάποιοι μεμονωμένοι από αυτούς. Λ.χ. οι αριθμοί 6, 15, 10 είναι σχετικά πρώτοι. Εν τούτοις τα ζεύγη 6, 15 ή 6, 10 ή 10, 6 δεν είναι ζεύγη σχετικά πρώτων αριθμών.

5.3.7. Αν έχουμε περισσότερους μη μηδενικούς αριθμούς α, β, γ, δ, ... *κοινά πολλαπλάσια* τους λέγονται οι αριθμοί που είναι πολλαπλάσια όλων των α, β, γ, δ, ... Πάντοτε υπάρχουν και θετικά κοινά πολλαπλάσια και το πιο μικρό από αυτά ονομάζεται ελάχιστο κοινό πολλαπλάσιο των α, β, γ, δ, ... και συμβολίζεται με $[\alpha, \beta, \gamma, \delta, ...]$. Για παράδειγμα οι αριθμοί 16, -24, -36 έχουν θετικά πολλαπλάσια αντιστοίχως τους αριθμούς

- 16, 32, 48, 64, 80, 96, 112, 128, **144**, 160, 176, 192, 208, 224, 240, 256, 272, **288**,...

- 24, 48, 72, 96, 120, **144**, 168, 192, 216, 240, 264, **288**, 312, 336, 360, 384, 408,...
- 36, 72, 108, **144**, 180, 216, 252, **288**, 324, 360, 396, **432**, 468, 504, 540, 576, 612,...

Το ελάχιστο κοινό πολλαπλάσιο είναι ο 144 δηλαδή

[16, -24, -36]=144

5.3.8. Η σειρά με την οποία γράφουμε τους αριθμούς στο σύμβολο του ελάχιστου κοινού πολλαπλασίου τους δεν παίζει κανένα ρόλο. Λ.χ. ισχύει

$$[\alpha, \beta, \gamma]=[\beta, \gamma, \alpha], \qquad [\alpha, \beta, \gamma, \delta]=[\gamma, \delta, \alpha, \beta] \text{ κ.τ.λ.}$$

5.3.9. Να βρείτε το ελάχιστο κοινό πολλαπλάσιο των αριθμών 12, 16, 20.

5.3.10. Να βρείτε τα [1,2,3], [1,2,3,4].

5.3.11. Ποιο είναι το $[\alpha^2,\alpha^4,\alpha^6]$;

5.3.12. ☐ *Ισχύει* $(\alpha, (\beta, \gamma))=((\alpha, \beta), \gamma)=(\alpha, \beta, \gamma)$

Απόδειξη. Αρκεί να δείξουμε ότι τα ζεύγη αριθμών

α, (β, γ) και (α, β), γ έχουν τους ίδιους διαιρέτες και ότι αυτοί συμπίπτουν με τους κοινούς διαιρέτες των αριθμών α, β, γ.

$$\left.\begin{matrix}\delta|\alpha \\ \delta|(\beta,\gamma)\end{matrix}\right\} \Rightarrow \left.\begin{matrix}\delta|\alpha \\ \delta|\beta \\ \delta|\gamma\end{matrix}\right\}$$ ΄Αρα ο δ είναι κοινός διαιρέτης των α, β, γ.

Επίσης $\left.\begin{matrix}\delta|(\alpha,\beta) \\ \delta|\gamma\end{matrix}\right\} \Rightarrow \left.\begin{matrix}\delta|\alpha \\ \delta|\beta \\ \delta|\gamma\end{matrix}\right\}$ ΄Αρα ο δ είναι κοινός διαιρέτης των α, β, γ. ■

5.3.13. ☐ *Ισχύει* $[\alpha, \beta, \gamma]= [\alpha, [\beta, \gamma]]= [[\alpha, \beta], \gamma]$.

Απόδειξη. Θα αποδείξουμε την ισότητα

$$[\alpha, \beta, \gamma]= [\alpha, [\beta, \gamma]] \quad (1)$$

Η ισότητα

$$[\alpha, \beta, \gamma]=[[\alpha, \beta], \gamma] \quad (2)$$

αποδεικνύεται με όμοιο τρόπο.

Ας ονομάσουμε x=[α, β, γ] και y=[α, [β, γ]]

Το x είναι το ελάχιστο κοινό πολλαπλάσιο των α, β, γ. Ιδιαιτέρως είναι

- πολλαπλάσιο του α
- κοινό πολλαπλάσιο των β, γ

Ως κοινό πολλαπλάσιο των β, γ είναι και πολλαπλάσιο του [β, γ]. Επομένως το x είναι:

- πολλαπλάσιο του α
- πολλαπλάσιο του [β, γ]

΄Αρα το x είναι κοινό πολλαπλάσιο των α, [β, γ] και ως τέτοιο είναι και πολλαπλάσιο του ελάχιστου κοινού πολλαπλασίου τους [α, [β, γ]] δηλαδή του y. ΄Αρα y|x και επειδή πρόκειται για θετικούς ακεραίους συνάγουμε ότι y≤x.

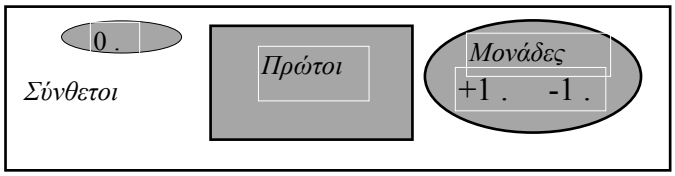
Ας δούμε τώρα τι συμβαίνει με το y. Το y είναι το ελάχιστο κοινό πολλαπλάσιο των α, [β, γ]. Ως πολλαπλάσιο του [β, γ] είναι και πολλαπλάσιο των β, γ. Επομένως το y είναι κοινό πολλαπλάσιο των α, β, γ. Αυτό σημαίνει ότι είναι μεγαλύτερο ή ίσο από το ελάχιστο κοινό πολλαπλάσιο τους [α, β, γ]. ΄Αρα y≥x.

Συνοψίζοντας έχουμε ότι y≤x και y≥x άρα x=y. ■

6. ΟΙ ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ

6.1. ΄Οπως έχουμε δει ένας αριθμός α λέγεται πρώτος αν είναι διάφορος των ±1 και έχει μόνο 4 διαιρέτες τους ±1, ±α. Επομένως ένας θετικός αριθμός είναι πρώτος αν είναι μεγαλύτερος του 1 και δεν έχει άλλους διαιρέτες εκτός από τον εαυτό του και τον 1. ΄Οσοι αριθμοί είναι διάφοροι των ±1 και δεν είναι πρώτοι λέγονται σύνθετοι. Οι σύνθετοι έχουν πάντα περισσότερους από 4 διαιρέτες. Είναι προφανές ότι ο α είναι

πρώτος αν και μόνο αν ο -α είναι πρώτος. Επίσης προφανές είναι ότι ένας αριθμός α είναι σύνθετος αν και μόνο αν ο -α είναι σύνθετος. Οι ακέραιοι λοιπόν χωρίζονται σε 4 ξένα ανά δύο υποσύνολα: το μονοσύνολο που περιέχει το 0, τις μονάδες ±1, τους σύνθετους και τους πρώτους. Κάθε ένα από αυτά αν περιέχει ένα αριθμό περιέχει και τον αντίθετο του.



Επομένως αν γνωρίζουμε τους θετικούς πρώτους γνωρίζουμε όλους τους πρώτους. Αν γνωρίζουμε τους θετικούς σύνθετους γνωρίζουμε όλους τους σύνθετους. Για τον λόγο αυτό θα περιορισθούμε μόνο στους θετικούς πρώτους και στους θετικούς σύνθετους. ΄Οταν λοιπόν στα επόμενα λέμε «πρώτος αριθμός» θα εννοούμε θετικό πρώτο. Επίσης λέγοντας «σύνθετος αριθμός» θα εννοούμε θετικός σύνθετος.

6.2. Οι πρώτοι διαδραματίζουν ένα σημαντικό ρόλο στην θεωρία αριθμών ανάλογο με εκείνο που παίζουν τα άτομα στην Χημεία.

6.3. *Κάθε σύνθετος αριθμός διαιρείται από κάποιος πρώτο.*

Απόδειξη. ΄Εστω α ένας σύνθετος αριθμός. Ο α θα έχει τουλάχιστον τρεις θετικούς διαιρέτες. Εκτός λοιπόν από τους 1 και α θα έχει και κάποιο θετικό διαιρέτη β με $1<\beta<\alpha$. Αν ο β είναι πρώτος η απόδειξη έχει τελειώσει. Βρήκαμε ένα πρώτο διαιρέτη τον β. Αν ο β είναι σύνθετος θα έχει ένα διαιρέτη γ με $1<\gamma<\beta$. Αν ο γ είναι πρώτος πάλι η απόδειξη έχει τελειώσει διότι ο πρώτος γ διαιρεί τον β ο οποίος με την σειρά του διαιρεί τον α άρα $\gamma|\alpha$. Δε μπορεί σε αυτή τη διαδικασία να βρίσκουμε συνέχεια σύνθετους αριθμούς διότι τότε θα υπάρχουν άπειροι (σύνθετοι) αριθμοί β, γ, δ, .. με $1<...<\delta<\gamma<\beta$. ΄Αρα διαδικασία αυτή θα τερματισθεί μετά από πεπερασμένο πλήθος βημάτων με την εύρεση ενός πρώτου διαιρέτη p του α. ■

6.4. *Έστω p, q δύο πρώτοι. Αν ισχύει μία από τις παρακάτω συνθήκες ισχύουν και οι υπόλοιπες*

1) $p \neq q$ 2) $p \nmid q$ 3) $(p,q)=1$

Απόδειξη. **1)⇒2)** Αν p≠q τότε ο p δε μπορεί να είναι διαιρέτης του q διότι δεν είναι ίσος με κανένα από τους θετικούς διαιρέτες του q που είναι οι 1, q. Άρα $p \nmid q$.

2)⇒3) Αν $p \nmid q$ τότε οι p, q έχουν ως μόνο θετικό κοινό διαιρέτη τον 1. Επομένως (p, q)=1.

3)⇒1) Αν (p, q)=1 τότε δε μπορεί p=q διότι τότε θα είχαμε (p, q)=(p, p)=p>1. Άρα p=q. ■

6.5. *Έστω p ένας πρώτος αριθμός και α ένας οποιοσδήποτε αριθμός. Οι παρακάτω συνθήκες είναι ισοδύναμες:*

1) $p \mid x$ 2) $(p, x)=1$

Απόδειξη. **1)⇒2)** Οι κοινοί θετικοί διαιρέτες των p, x δε μπορεί παρά να είναι διαιρέτες του p. Άρα (p, x)=1 ή

(p, x)=p. Η δεύτερη περίπτωση αποκλείεται διότι τότε θα είχαμε p|x. Άρα ισχύει η πρώτη δηλαδή (p, x)=1.

2)⇒1) Ας πούμε ότι (p, x)=1. Αν συνέβαινε p|x τότε θα ήταν (p, x)=p>1. ■

Η προηγούμενη πρόταση μας λέει ότι ένας πρώτος ή είναι σχετικά πρώτος προς ένα ακέραιο ή τον διαιρεί. Συνέπεια της είναι η επόμενη:

6.6. *Αν ο p είναι πρώτος και $p \mid xy$ τότε $p \mid x$ ή $p \mid y$.*

Απόδειξη. Αν $p \nmid x$ τότε (p, x)=1 και επομένως p|y. ■

6.7. Ένα τρόπο για να βρίσκουμε πρώτους αριθμούς μας προσφέρει το **κόσκινο του Ερατοσθένη**. Λέγεται έτσι γιατί λειτουργεί όπως ακριβώς το κόσκινο που χρησιμοποιείται στο αλεύρι. Μετά από κάθε «κοσκίνισμα» αποχωρίζονται από τους

αριθμούς με τους οποίους εργαζόμαστε κάποιοι σύνθετοι αριθμοί. Μετά από αρκετά «κοσκινίσματα» παραμένουν μόνο πρώτοι αριθμοί. Ας δούμε πως δουλεύει το κόσκινο του Ερατοσθένη για την εύρεση των πρώτων φυσικών αριθμών που δεν υπερβαίνουν τον 110.

Διαγράφουμε τους 0 και 1 που δεν είναι πρώτοι.

110	111	112	113	114	115	116	117	118	119
100	101	102	103	104	105	106	107	108	109
90	91	92	93	94	95	96	97	98	99
80	81	82	83	84	85	86	87	88	89
70	71	72	73	74	75	76	77	78	79
60	61	62	63	64	65	66	67	68	69
50	51	52	53	54	55	56	57	58	59
40	41	42	43	44	45	46	47	48	49
30	31	32	33	34	35	36	37	38	39
20	21	22	23	24	25	26	27	28	29
10	11	12	13	14	15	16	17	18	19
0	1	2	3	4	5	6	7	8	9

Ο 2 είναι πρώτος αλλά όλα τα υπόλοιπα πολλαπλάσια του δηλαδή οι άρτιοι που είναι μεγαλύτεροι του 2 είναι σύνθετοι. Τους διαγράφουμε:

110	111	112	113	114	115	116	117	118	119
100	101	102	103	104	105	106	107	108	109
90	91	92	93	94	95	96	97	98	99
80	81	82	83	84	85	86	87	88	89
70	71	72	73	74	75	76	77	78	79
60	61	62	63	64	65	66	67	68	69
50	51	52	53	54	55	56	57	58	59
40	41	42	43	44	45	46	47	48	49
30	31	32	33	34	35	36	37	38	39
20	21	22	23	24	25	26	27	28	29
10	11	12	13	14	15	16	17	18	19
0	1	2	3	4	5	6	7	8	9

Ο 3 είναι πρώτος. Αυτό είναι κάτι που το ξέρουμε. Ωστόσο το ότι είναι πρώτος προκύπτει και από ένα άλλο επιχείρημα που θα μας χρειασθεί παρακάτω: Αν ήταν σύνθετος θα είχε ένα μικρότερο από αυτόν πρώτο διαιρέτη. Ο μόνος μικρότερος από τον 3 πρώτος είναι ο 2 και τα πολλαπλάσια του τα έχουμε ήδη διαγράψει χωρίς όμως να διαγραφεί ο 3.΄Αρα ο 3 είναι πρώτος. ΄Ομως τα πολλαπλάσια του είναι σύνθετοι. Τα διαγράφουμε.

110	111	112	113	114	115	116	117	118	119
100	101	102	103	104	105	106	107	108	109
90	91	92	93	94	95	96	97	98	99
80	81	82	83	84	85	86	87	88	89
70	71	72	73	74	75	76	77	78	79
60	61	62	63	64	65	66	67	68	69
50	51	52	53	54	55	56	57	58	59
40	41	42	43	44	45	46	47	48	49
30	31	32	33	34	35	36	37	38	39
20	21	22	23	24	25	26	27	28	29
10	11	12	13	14	15	16	17	18	19
0	1	2	3	4	5	6	7	8	9

Ο 5 είναι πρώτος διότι δεν διαιρείται από κανένα μικρότερο του πρώτο. Τα πολλαπλάσια του 5 που είναι μεγαλύτερα του 5 είναι αριθμοί σύνθετοι τους οποίους και διαγράφουμε:

110	111	112	113	114	115	116	117	118	119
100	101	102	103	104	105	106	107	108	109
90	91	92	93	94	95	96	97	98	99
80	81	82	83	84	85	86	87	88	89
70	71	72	73	74	75	76	77	78	79
60	61	62	63	64	65	66	67	68	69
50	51	52	53	54	55	56	57	58	59
40	41	42	43	44	45	46	47	48	49
30	31	32	33	34	35	36	37	38	39
20	21	22	23	24	25	26	27	28	29
10	11	12	13	14	15	16	17	18	19
0	1	2	3	4	5	6	7	8	9

Ο 7 είναι πρώτος. Διαγράφουμε τα πολλαπλάσια του:

110	111	112	113	114	115	116	117	118	119
100	101	102	103	104	105	106	107	108	109
90	91	92	93	94	95	96	97	98	99
80	81	82	83	84	85	86	87	88	89
70	71	72	73	74	75	76	77	78	79
60	61	62	63	64	65	66	67	68	69
50	51	52	53	54	55	56	57	58	59
40	41	42	43	44	45	46	47	48	49
30	31	32	33	34	35	36	37	38	39
20	21	22	23	24	25	26	27	28	29
10	11	12	13	14	15	16	17	18	19
0	1	2	3	4	5	6	7	8	9

Ο 11 είναι πρώτος διαγράφουμε τα πολλαπλάσια του εκτός από τον ίδιο κ.ο.κ. Τελικά μετά τις διαγραφές θα έχουμε την ακόλουθη εικόνα:

110	111	112	113	114	115	116	117	118	119
100	101	102	103	104	105	106	107	108	109
90	91	92	93	94	95	96	97	98	99
80	81	82	83	84	85	86	87	88	89
70	71	72	73	74	75	76	77	78	79
60	61	62	63	64	65	66	67	68	69
50	51	52	53	54	55	56	57	58	59
40	41	42	43	44	45	46	47	48	49
30	31	32	33	34	35	36	37	38	39
20	21	22	23	24	25	26	27	28	29
10	11	12	13	14	15	16	17	18	19
0	1	2	3	4	5	6	7	8	9

Οι αριθμοί που δεν έχουν διαγραφεί είναι πρώτοι.

6.8. Στους 109 πρώτους στη σειρά θετικούς ακεραίους οι 30 είναι πρώτοι δηλαδή ένα ποσοστό 36%. ΄Ομως όταν πάρουμε περισσότερους αριθμούς το ποσοστό αυτό ελαττώνεται δραματικά: Οι πρώτοι αριθμοί που δεν υπερβαίνουν το 1000 είναι 168 δηλαδή το ποσοστό των πρώτων πέφτει περίπου στο 17% και γίνεται 12% στις 10.000. Οι πρώτοι αριθμοί που δεν υπερβαίνουν το 1.000.000 είναι 78.498 δηλαδή περίπου 8%. ΄Οσο μεγαλώνουν οι αριθμοί το ποσοστό αυτό μικραίνει. Τίθεται το ερώτημα: Μήπως από ένα σημείο και πέρα οι πρώτοι αριθμοί θα εξαφανισθούν εντελώς δηλαδή μήπως οι πρώτοι αριθμοί κάποτε τελειώνουν ή αλλιώς μήπως είναι πεπερασμένοι το πλήθος. Η απάντηση είναι αρνητική και την έδωσε ο Ευκλείδης:

6.9. *Υπάρχουν άπειροι πρώτοι.*

Απόδειξη. Η απόδειξη θα γίνει με απαγωγή στο άτοπο. Ας υποθέσουμε ότι οι πρώτοι δεν είναι άπειροι αλλά πεπερασμένοι. Ας πούμε ότι το πλήθος τους είναι ν. Τότε μπορούμε να τους αριθμήσουμε κατά αύξουσα σειρά και έστω ότι είναι οι $p_1 = 2, p_2 = 3, ..., p_\nu$. ΄Εστω x ο αριθμός $1 + p_1 p_2 .... p_\nu$. Ο αριθμός αυτός είναι μεγαλύτερος από όλους τους $p_1, p_2, ..., p_\nu$ και επομένως είναι διάφορος από όλους αυτούς. Δεν είναι λοιπόν πρώτος διότι οι πρώτοι είναι όλοι κι΄ όλοι οι $p_1, p_2, ..., p_\nu$.

Επομένως είναι σύνθετος. Ως σύνθετος πρέπει να διαιρείται από κάποιον πρώτο δηλαδή από κάποιον από τους $p_1,p_2,....,p_v$. Ας πούμε ότι είναι εκείνος που έχει i θέση στην σειρά των πρώτων $p_1,p_2,....,p_v$ δηλαδή είναι ο p_i. Τότε $p_i|x$ και ασφαλώς $p_i|p_1p_2....p_v$ αφού στους παράγοντες του γινομένου συγκαταλέγεται και ο p_i. Επομένως $p_i|1$. (΄Ατοπο). Καταλήξαμε σε άτοπο διότι δεχθήκαμε ότι οι πρώτοι είναι πεπερασμένοι. Επομένως είναι άπειροι. ■

6.10. Στην προηγούμενη απόδειξη ο Ευκλείδης χρησιμοποιεί αριστοτεχνικά την μέθοδο της απαγωγής στο άτοπο προκειμένου να αποδειχθεί ότι υπάρχουν άπειροι πρώτοι. Το θεώρημα δεν μας λέει πως θα βρούμε αυτούς τους άπειρους πρώτους. Πρόκειται για ένα **θεώρημα ύπαρξης**. Με το κόσκινο του Ερατοσθένη μπορούμε να βρούμε όλους τους πρώτους που υπάρχουν σε ένα διάστημα [1, ν] αλλά δε μπορούμε να βρούμε όλους τους πρώτους ούτε είναι δυνατόν να έχουμε ένα «τύπο» που να μας δίνει τον νι-οστό πρώτο όπως λ.χ. έχουμε τον 2ν για τον νιοστό θετικό άρτιο ή τον 2ν-1 για τον νι-οστό θετικό περιττό. Το πλήθος των πρώτων που ανήκουν στο διάστημα [1, x] συμβολίζεται με π(x). Η π(x) είναι μία αύξουσα συνάρτηση (όχι γνησίως) αλλά ο λόγος $\frac{\pi(x)}{x}$ που εκφράζει το ποσοστό των πρώτων στο διάστημα [1, x] είναι συνάρτηση φθίνουσα. Δεν υπάρχει ακριβής τύπος για την συνάρτηση $\frac{\pi(x)}{x}$ και πολλοί μαθηματικοί του 19ου αιώνα μεταξύ των οποίων και οι Γκάους (Gauss) και Τσέμπσεβ (Chebyshev) είχαν διατυπώσει την εικασία ότι είναι «περίπου» $\frac{x}{\ln x}$ με άλλα λόγια ότι για μεγάλα x, δηλαδή όταν το x τείνει στο άπειρο, το κλάσμα $\frac{\frac{\pi(x)}{x}}{\ln x}$ πλησιάζει στη μονάδα. Χρειάσθηκε να περάσουν αρκετά χρόνια έως ότου ο Βέλγος Ντε λα Βαλέ Πουσέν (De la Vallée Poussin) και ο Γάλλος Ζακ Ανταμάρ

(Jacques Hadamard) το 1901 ο κατορθώσουν ο ένας ανεξάρτητα από τον άλλο να αποδείξουν ότι πράγματι αυτό ισχύει. Το θεώρημα αυτό που λέγεται και **θεώρημα του πρώτου αριθμού** μας λέει ότι για μεγάλα x το π(x) είναι περίπου $\frac{x}{\ln x}$.

6.11. Οι πρώτοι αριθμοί έχουν μία ακανόνιστη συμπεριφορά στην εμφάνιση τους. ΄Ολοι οι πρώτοι αριθμοί που είναι μεγαλύτεροι του 2 είναι περιττοί αλλά ασφαλώς δεν είναι όλοι οι περιττοί πρώτοι. Πόσο συχνά μπορούν να εμφανίζονται οι πρώτοι αριθμοί; Η πιο συχνή εμφάνιση είναι να έχουμε ένα πρώτο μετά ένα άρτιο και μετά πάλι πρώτο. Δηλαδή να έχουμε ένα ζεύγος πρώτων p, p+2. Αυτά τα ζεύγη πρώτων λέγονται από την αρχαιότητα **δίδυμοι πρώτοι**. Τα ζεύγη 17, 19 και 41, 43 είναι ζεύγη διδύμων πρώτων. Υπάρχουν άπειρα ή πεπερασμένα ζεύγη διδύμων πρώτων; (*πρόβλημα των διδύμων*). Η απάντηση μας είναι άγνωστη δηλαδή πρόκειται για ένα άλυτο πρόβλημα. Πόσο σπάνια μπορούν να εμφανίζονται οι πρώτοι αριθμοί; Για παράδειγμα οι συνεχόμενοι αριθμοί 90, 91, 92, 93, 94, 95, 96 είναι όλοι σύνθετοι. Μπορούμε να έχουμε οσοδήποτε μεγάλου μήκους σειρές με σύνθετους αριθμούς; Η απάντηση είναι «ναι» όπως προκύπτει από το επόμενο:

6.12. *Δοθέντος ενός οποιουδήποτε αριθμού ν υπάρχουν ν διαδοχικοί σύνθετοι αριθμοί.*

Απόδειξη. Η απόδειξη χρησιμοποιεί την ιδέα της απόδειξης του Ευκλείδη. Αφού οι πρώτοι είναι άπειροι υπάρχουν οσοδήποτε μεγάλοι πρώτοι. ΄Εστω p ένας πρώτος που είναι μεγαλύτερος του ν. Γράφουμε όλους τους πρώτους έως τον p:

$$2, 3, 5, ..., p$$

Κάθε αριθμός έως τον p είναι ή πρώτος δηλαδή κάποιος από τους 2, 3, 5, ..., p ή είναι σύνθετος οπότε διαιρείται από κάποιον πρώτο του καταλόγου 2, 3, 5, ..., p . Σε κάθε περίπτωση οποιοσδήποτε αριθμός από 2 έως p διαιρείται από κάποιον από τους 2, 3, 5, ..., p . Σχηματίζουμε το γινόμενο $2\cdot 3\cdot 5\cdot ...\cdot p$ των πρώτων 2, 3, 5, ..., p. Το

γινόμενο αυτό διαιρείται από όλους τους αριθμούς 2, 3, 5, ..., p. Στη συνέχεια προσθέτουμε κάθε φορά στο γινόμενο αυτό τους αριθμούς 2, 3, 4, 5, 6, ..., p-1, p δηλαδή σχηματίζουμε τους αριθμούς:

$$(2\cdot 3\cdot 5\cdot \ldots \cdot p)+2$$

$$(2\cdot 3\cdot 5\cdot \ldots \cdot p)+3$$

$$(2\cdot 3\cdot 5\cdot \ldots \cdot p)+4$$

$$(2\cdot 3\cdot 5\cdot \ldots \cdot p)+5$$

$$(2\cdot 3\cdot 5\cdot \ldots \cdot p)+6$$

.....

$$(2\cdot 3\cdot 5\cdot \ldots \cdot p)+(p-1)$$

$$(2\cdot 3\cdot 5\cdot \ldots \cdot p)+p$$

Το πλήθος τους είναι p-1 και επειδή είναι $p>\nu$ είναι $p-1\geq\nu$ δηλαδή το πλήθος τους είναι τουλάχιστον ν. Όλοι τους είναι σύνθετοι διότι κάθε ένας από αυτούς είναι άθροισμα του $2\cdot 3\cdot 5\cdot \ldots \cdot p$ που διαιρείται από όλους τους 2, 3, 5, ..., p και ενός αριθμού που διαιρείται από κάποιον από τους 2, 3, 5, ..., p. Επομένως υπάρχουν ν διαδοχικοί σύνθετοι αριθμοί. ■

6.1. Το θεμελιώδες θεώρημα της Αριθμητικής.

6.1.1. Είδαμε ότι κάθε αριθμός $\alpha>1$ διαιρείται από ένα πρώτο. Ας πούμε ότι ο α διαιρείται από τον p. Τότε ο α γράφεται $\alpha=px$. Είναι $\alpha>x\geq 1$. Αν συμβαίνει $x>1$ τότε και ο x διαιρείται από κάποιο πρώτο. Ας τον ονομάσουμε q. Ο q μπορεί να είναι ο ίδιος με τον p η διάφορος του p. Σε κάθε περίπτωση όμως είναι $\alpha=pqy$ και είναι $\alpha>x>y\geq 1$. Επαναλαμβάνουμε τον προηγούμενο συλλογισμό: Αν είναι $y>1$ ο y με την σειρά του διαιρείται από κάποιο πρώτο έστω r, θα είναι $\alpha=pqrz$ και $\alpha>x>y>z\geq 1$. Είναι φανερό ότι δε μπορεί επ΄ άπειρον να βρίσκουμε πηλίκα μεγαλύτερα του 1 και ότι

κάποτε η διαδικασία θα τελειώσει με την εξ΄ ολοκλήρου μετατροπή του α σε γινόμενο πρώτων αριθμών.

6.1.2. Πρόκειται για μία διαδικασία που μας είναι γνωστή από το Γυμνάσιο όπου μάθαμε να μετατρέπουμε τους αριθμούς σε γινόμενο πρώτων παραγόντων. Ας θυμηθούμε πως γίνεται αυτό για τον αριθμό 1512

1512	2
756	2
378	2
189	3
63	3
21	3
7	7
1	

Ο 1512 λοιπόν γράφεται ως γινόμενο πρώτων αριθμών $1512 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7$.

Θα μπορούσαμε να κάνουμε το ίδιο με τον αριθμό 1512 αλλά δοκιμάζοντας πρώτους διαιρέτες με διαφορετική σειρά:

1512	3
504	3
168	2
84	3
28	7
4	2
2	2
1	

Βρίσκουμε τότε $1512 = 3 \cdot 3 \cdot 2 \cdot 3 \cdot 7 \cdot 2 \cdot 2$ Βρίσκουμε τους ίδιους με πριν πρώτους παράγοντες αλλά με διαφορετική σειρά. ΄Ομως επειδή η πράξη του πολλαπλασιασμού είναι αντιμεταθετική η σειρά δεν παίζει κανένα ρόλο.

6.1.3. Κατ΄ αρχήν έχουμε αποδείξει ότι.

Κάθε αριθμός α μεγαλύτερος του 1 *είναι γινόμενο πρώτων αριθμών.* ■

Προσέξτε ότι ο όρος «γινόμενο πρώτων παραγόντων» χρησιμοποιείται διαφορετικά απ΄ ότι έχουμε συνηθίσει: καλύπτει και την περίπτωση ενός μόνο πρώτου παράγοντα δηλαδή ενός γινομένου με ένα παράγοντα. Οι πρώτοι αυτοί αριθμοί λέγονται **πρώτοι παράγοντες** του α. Το ποιοι πρώτοι παράγοντες θα εμφανισθούν και πόσες φορές ο κάθε ένας είναι εξαρτάται αποκλειστικά από τον α. Δηλαδή αν ο ίδιος αριθμός γραφεί ως γινόμενο πρώτων παραγόντων κατά δύο τρόπους τα δύο γινόμενα θα περιέχουν ακριβώς τους ίδιους πρώτους, και οι φορές που ο ίδιος πρώτος εμφανίζεται στα δύο γινόμενα είναι ίδιες. Θα αποδείξουμε λοιπόν κάτι περισσότερο:

6.1.4. *Κάθε αριθμός α μεγαλύτερος του* 1 *γράφεται ως γινόμενο πρώτων αριθμών κατά μοναδικό τρόπο.*

Απόδειξη. ΄Εστω α>1. ΄Εχουμε αποδείξει ήδη ότι ο α γράφεται ως γινόμενο πρώτων παραγόντων. Απομένει να δείξουμε ότι αυτό γίνεται κατά μοναδικό τρόπο. Ας πούμε ότι έχουμε εκφράσει τον α ως γινόμενο πρώτων παραγόντων με δύο γινόμενα Γ_1, Γ_2 δηλαδή $\alpha=\Gamma_1$, $\alpha=\Gamma_2$. Είναι

$$\Gamma_1=\Gamma_2 \quad (1)$$

Ας πούμε ότι στο Γ_1 εμφανίζεται ο πρώτος p. Τότε ο p διαιρεί το Γ_2. Επομένως εμφανίζεται και στο Γ_2. Απλοποιώντας τον p στην (1) θα βρούμε μία ισότητα

$$\Gamma_1'=\Gamma_2' \quad (2)$$

Στην (2) δύο πράγματα μπορεί να συμβαίνουν. ΄Η και τα δύο μέλη της είναι 1 ή εξακολουθούν να υπάρχουν πρώτοι αριθμοί. Στην πρώτη περίπτωση η απόδειξη έχει ολοκληρωθεί και ο p είναι ο μοναδικός πρώτος παράγοντας του α. Στην δεύτερη περίπτωση διαλέγουμε ένα πρώτο παράγοντα από κάποιο γινόμενο έστω q (σημειώστε ότι ενδέχεται να είναι p=q). Αυτός θα υπάρχει αναγκαστικά και στο άλλο γινόμενο και επομένως μπορεί να απλοποιηθεί. Τον απλοποιούμε. Θα βρούμε έτσι μία ισότητα

$$\Gamma_1'' = \Gamma_2'' \quad (3)$$

Συνεχίζοντας με τον ίδιο τρόπο «διώχνουμε» ένα-ένα τους πρώτους παράγοντες έως ότου βρούμε 1=1. Αυτό που *έμεινε* δεν μας λέει τίποτα αλλά ας θυμηθούμε τι *έφυγε* ΄Εφυγαν οι ίδιοι πρώτοι παράγοντες και από τα δύο μέλη. ΄Αρα υπήρχαν οι ίδιοι πρώτοι παράγοντες και στα δύο μέλη. Αν δε κάποιος έφυγε 2, 3, .. φορές έφυγε γιατί και στα δύο μέλη υπήρχε τις ίδιες φορές. ■

6.1.5. Για την γραφή παραγόντων που επαναλαμβάνονται έχουμε τον «οικονομικό» συμβολισμό των δυνάμεων. ΄Ετσι είναι βολικό να γράψουμε $1512 = 2^3 \cdot 3^3 \cdot 7$ ή ακόμη και $1512 = 2^3 \cdot 3^3 \cdot 7^1$ αντί για $1512 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7$. Επομένως *κατά την γραφή ενός αριθμού σε γινόμενο πρώτων παραγόντων μπορούμε να γράφουμε τους τυχόν επαναλαμβανόμενους πρώτους υπό μορφή δυνάμεων*. Συνοψίζοντας τις δύο προηγούμενες προτάσεις και την τελευταία παρατήρηση έχουμε το

Θεμελιώδες Θεώρημα της Αριθμητικής. *Κάθε αριθμός μεγαλύτερος του 1 μπορεί να γραφεί ως γινόμενο δυνάμεων διαφορετικών ανά δύο πρώτων αριθμών κατά μοναδικό τρόπο. Δηλαδή οι βάσεις και οι εκθέτες αυτών των δυνάμεων είναι μονοσήμαντως ορισμένες.* ■

Σύμφωνα με το θεμελιώδες θεώρημα της αριθμητικής κάθε αριθμός α>1 γράφεται κατά μοναδικό τρόπο ως γινόμενο της μορφής $a = p_1^{x_1} p_2^{x_2} \ldots p_r^{x_r}$ όπου

- $p_1, p_2, \ldots, p_r$ είναι οι διαφορετικοί πρώτοι παράγοντες του α
- r είναι το πλήθος τους,
- οι εκθέτες $x_1, x_2, \ldots, x_r$ είναι θετικοί ακέραιοι που δείχνουν πόσες φορές οι αριθμοί $p_1, p_2, \ldots, p_r$ εμφανίζονται στην ανάλυση του α.

Η γραφή $a = p_1^{x_1} p_2^{x_2} \ldots p_r^{x_r}$ ονομάζεται **κανονική μορφή** του α. Σημειώστε ότι:

- *αν στην κανονική μορφή του α ο p εμφανίζεται με εκθέτη x τότε ο x είναι ο μεγαλύτερος εκθέτης στον οποίο υψούμενος ο p διαιρεί τον α.*

αλλά και αντιστρόφως

- *αν $x\geq 1$ είναι ο μεγαλύτερος εκθέτης στον οποίο υψούμενος ο p διαιρεί τον α τότε ο p εμφανίζεται στην ανάλυση του α με εκθέτη x.*

6.1.6. *Έστω ότι x είναι ο μεγαλύτερος εκθέτης στον οποίο υψούμενος ο p διαιρεί τον α και y είναι ο μεγαλύτερος εκθέτης στον οποίο υψούμενος ο p διαιρεί τον β. Τότε ο μεγαλύτερος εκθέτης στον οποίο υψούμενος ο p διαιρεί τον αβ είναι x+y.*

Απόδειξη. Υπάρχουν αριθμοί t, k έτσι ώστε $\alpha=tp^x$, $\beta=kp^y$. Ο t δεν διαιρείται από τον p διότι διαφορετικά ο α θα διαιρείτο από τον p υψούμενο σε μεγαλύτερο εκθέτη από τον x. Για τον ίδιο λόγο ο k δεν διαιρείται από τον p. Είναι $\alpha\beta= tp^xp^y=tkp^{x+y}$. Επειδή ο tk δεν διαιρείται από τον p η μεγαλύτερη δύναμη του p που διαιρεί το γινόμενο tkp^{x+y} είναι η p^{x+y} με άλλα λόγια ο x+y είναι ο μεγαλύτερος εκθέτης στον οποίο υψούμενος ο p διαιρεί τον tkp^{x+y} και επομένως τον αβ. ■

6.1.7. Ο αριθμός 2000 μπορεί να γραφεί στις ακόλουθες μορφές:

$2000 = 20^2 \cdot 5$ $\quad$ $2000 = 2^2 \cdot 2^2 \cdot 5$ $\quad$ $2000 = 2^4 \cdot 5^3$

$2000 = 2^8 \cdot 2^{-4} \cdot 5$ $\quad$ $2000 = 5 \cdot 2^4$

Μόνο όμως η μορφές $2000 = 2^4 \cdot 5^3$, $2000 = 5 \cdot 2^4$ είναι κανονικές διότι η $2000 = 20^2 \cdot 5$ δεν έχει πρώτους όλους τους παράγοντες, η $2000 = 2^2 \cdot 2^2 \cdot 5$ έχει τους παράγοντες πρώτους αλλά όχι διαφορετικούς και η $2000 = 2^8 \cdot 2^{-4} \cdot 5$ έχει όλους τους παράγοντες πρώτους αλλά όχι σε θετικούς εκθέτες.

6.1.8. Στον παρακάτω πίνακα εμφανίζονται οι αναλύσεις σε γινόμενο πρώτων παραγόντων των αριθμών από 2 έως 75.

		26	$2\cdot13$	51	$3\cdot17$
2	2	27	3^3	52	$2^2\cdot13$
3	3	28	$2^2\cdot7$	53	53
4	2^2	29	29	54	$2\cdot3^3$
5	5	30	$2\cdot3\cdot5$	55	$5\cdot11$
6	$2\cdot3$	31	31	56	$2^3\cdot7$
7	7	32	2^5	57	$3\cdot19$
8	2^3	33	$3\cdot11$	58	$2\cdot29$
9	3^2	34	$2\cdot17$	59	59
10	$2\cdot5$	35	$5\cdot7$	60	$2^2\cdot3\cdot5$
11	11	36	$2^2\cdot3^2$	61	61
12	$2\cdot^2 3$	37	37	62	$2\cdot31$
13	13	38	$2\cdot19$	63	$3^2\cdot7$
14	$2\cdot7$	39	$3\cdot13$	64	2^6
15	$3\cdot5$	40	$2^3\cdot5$	65	$5\cdot13$
16	2^4	41	41	66	$2\cdot3\cdot11$
17	17	42	$2\cdot3\cdot7$	67	67
18	$2\cdot3^2$	43	43	68	$2^2\cdot17$
19	19	44	$2^2\cdot11$	69	$3\cdot23$
20	$2^2\cdot5$	45	$3^2\cdot5$	70	$2\cdot5\cdot7$
21	$3\cdot7$	46	$2\cdot23$	71	71
22	$2\cdot11$	47	47	72	$2^2\cdot3^2$
23	23	48	$2^4\cdot3$	73	73
24	$2^3\cdot3$	49	7^2	74	$2\cdot37$
25	5^2	50	$2\cdot5^2$	75	$3\cdot5^2$

6.1.9. Οι πρώτοι αριθμοί είναι το «υλικό» που αν συνδεθεί με την πράξη του πολλαπλασιασμού μπορεί να φτιάξει όλους τους αριθμούς. Ο ρόλος τους είναι ανάλογος με εκείνο των ατόμων στην Χημεία. Όπως λ.χ. για να περιγράψουμε το νιτρικό οξύ γράφουμε HNO_3 και εννοούμε ότι ένα μόριο νιτρικού οξέος απαρτίζεται από ένα μόριο υδρογόνου, ένα αζώτου και τρία οξυγόνου έτσι γράφουμε $60=2^2\cdot3\cdot5$ για να δηλώσουμε ότι ο 60 φτιάχνεται πολλαπλασιάζοντας δύο 2, ένα 3 και ένα 5. Όπως και στη Χημεία οποιαδήποτε ανάλυση και να υποστεί το μόριο του νιτρικού οξέος θα οδηγήσει σε αυτή την δοσολογία μορίων το ίδιο συμβαίνει και με την αριθμητική: Όπως και να αναλύσει κάποιος σε γινόμενο πρώτων παραγόντων το 60 θα καταλήξει στο ίδιο συμπέρασμα.

6.2. Διαιρέτες και πολλαπλάσια αριθμού σε κανονική μορφή.

6.2.1. *Έστω ότι $\alpha|\beta$ και p ένας πρώτος αριθμός. Έστω x, y οι μεγαλύτεροι εκθέτες στους οποίους υψούμενος ο p διαιρεί τους α και β αντιστοίχως. Τότε $x\leq y$.*

Απόδειξη. Επειδή α|β θα είναι

β=λα (1)

Ας ονομάσουμε z τον μεγαλύτερο εκθέτη στον οποίο υψούμενος ο p διαιρεί τον λ. Τότε η μεγαλύτερη δύναμη του p διαιρεί το πρώτο μέλος της (1) είναι p^y, ενώ η μεγαλύτερη δύναμη του p που διαιρεί το δεύτερο μέλος της (1) είναι η p^{z+x}. ΄Αρα y=z+x και επομένως y≥x. ■

6.2.2. *Αν* $\beta= p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$ *είναι η κανονική μορφή του β τότε ένας αριθμός είναι διαιρέτης του β αν και μόνο αν είναι της μορφής* $p_1^{x_1} p_2^{x_2} \ldots p_r^{x_r}$ *με* $0 \le x_1 \le \beta_1$, $0 \le x_2 \le \beta_2$, ..., $0 \le x_r \le \beta_r$.

Απόδειξη. ΄Εστω α ένας διαιρέτης του β. Κάθε πρώτος παράγοντας που εμφανίζεται στην ανάλυση του α σε γινόμενο πρώτων παραγόντων θα είναι κάποιος από τους $p_1, p_2, \ldots p_r$ και επιπλέον θα εμφανίζεται σε εκθέτη μικρότερο ή ίσο του αντίστοιχου εκθέτη με τον οποίο εμφανίζεται στην ανάλυση του β. Μπορεί κάποιος πρώτος παράγοντας p_i του β να μην είναι και πρώτος παράγοντας του α. Τότε μπορούμε να τότε να τον συμπεριλάβουμε στο γινόμενο που δίνει την ανάλυση του α γράφοντας απλώς $p_i^0 = 1$. ΄Αρα κάθε διαιρέτης α του β είναι της μορφής:

$a = p_1^{x_1} p_2^{x_2} \ldots p_r^{x_r}$ με $0 \le x_1 \le \beta_1, 0 \le x_2 \le \beta_2, \ldots, 0 \le x_r \le \beta_r$ (1)

Αντιστρόφως τώρα κάθε αριθμός της μορφής (1) είναι διαιρέτης του β διότι ο β μπορεί να γραφεί $\beta= \left(p_1^{\beta_1 - x_1} p_2^{\beta_2 - x_2} \ldots p_r^{\beta_r - x_r}\right)\left(p_1^{x_1} p_2^{x_2} \ldots p_r^{x_r}\right)$.

Επομένως οι διαιρέτες του β είναι ακριβώς οι αριθμοί (2). ■

6.2.3. Ας βρούμε όλους τους διαιρέτες του α=320. Αναλύοντας το 320 σε γινόμενο πρώτων παραγόντων βρίσκουμε ότι $320 = 2^3 \cdot 3^2 \cdot 5^1$. Επομένως οι διαιρέτες του 320 είναι οι αριθμοί της μορφής $2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3}$ όπου $0 \le \alpha_1 \le 3$, $0 \le \alpha_2 \le 2$,

$0 \le \alpha_3 \le 1$. Παίρνοντας όλες τις δυνατές περιπτώσεις των εκθετών βρίσκουμε ότι οι διαιρέτες του 360 είναι:

α_1	α_2	α_3	Διαιρέτης	Τιμή του διαιρέτη
0	0	0	$2^0 3^0 5^0$	1
0	0	1	$2^0 3^0 5^1$	5
0	1	0	$2^0 3^1 5^0$	3
0	1	1	$2^0 3^1 5^1$	15
0	2	0	$2^0 3^2 5^0$	9
0	2	1	$2^0 3^2 5^1$	45
1	0	0	$2^1 3^0 5^0$	2
1	0	1	$2^1 3^0 5^1$	10
1	1	0	$2^1 3^1 5^0$	6
1	1	1	$2^1 3^1 5^1$	30
1	2	0	$2^1 3^2 5^0$	18
1	2	1	$2^1 3^2 5^1$	90
2	0	0	$2^2 3^0 5^0$	4
2	0	1	$2^2 3^0 5^1$	20
2	1	0	$2^2 3^1 5^0$	12
2	1	1	$2^2 3^1 5^1$	60
2	2	0	$2^2 3^2 5^0$	36
2	2	1	$2^2 3^2 5^1$	180
3	0	0	$2^3 3^0 5^0$	8
3	0	1	$2^3 3^0 5^1$	40
3	1	0	$2^3 3^1 5^0$	24
3	1	1	$2^3 3^1 5^1$	120
3	2	0	$2^3 3^2 5^0$	72
3	2	1	$2^3 3^2 5^1$	360

6.2.4. Να γράψετε όλους τους διαιρέτες του p^2q^3 όπου p, q είναι δύο διαφορετικοί πρώτοι.

6.2.5. Να γράψετε όλους τους διαιρέτες του 2^v.

6.2.6. Να αποδείξετε ότι αν $\beta = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$ είναι η κανονική μορφή του β τότε το πλήθος των διαιρετών του είναι $(\beta_1+1)(\beta_2+1)\ldots(\beta_r+1)$.

6.2.7. Να βρείτε το άθροισμα των διαιρετών του αριθμού β αν είναι γνωστό ότι η κανονική μορφή του είναι $\beta = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$.

Υπόδειξη: Δείξτε πρώτα ότι το άθροισμα των διαιρετών του β είναι ίσο με το γινόμενο:

$$(1 + p_1^1 + p_1^2 + \ldots + p_1^{\beta_1})(1 + p_2^1 + p_2^2 + \ldots + p_2^{\beta_2}) \ldots (1 + p_r^1 + p_r^2 + \ldots + p_r^{\beta_r})$$

6.2.8. Να βρείτε το γινόμενο των διαιρετών του αριθμού β αν είναι γνωστό ότι η κανονική μορφή του είναι $\beta = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$.

6.2.9. Έστω ότι p, q, s είναι τρεις διαφορετικοί πρώτοι και $\alpha=p^2q$ και $\beta=q^3s^5$. Ας βρούμε τον (α, β) και τον [α, β].

Για τον (*α, β*).Οι διαιρέτες του α είναι όλοι οι αριθμοί της μορφής p^xq^y με $0\le x\le 2$ και $0\le y\le 1$. Οι διαιρέτες του β είναι της μορφής p^zs^u με $0\le z\le 3$ και $0\le u\le 5$. Ένας κοινός διαιρέτης των α, β δε μπορεί να έχει παράγοντα τον p αλλά ούτε και τον s. Ο μόνος πρώτος παράγοντας που μπορεί να έχει είναι ο q. Άρα ένας κοινός διαιρέτης των α, β δε μπορεί παρά να είναι δύναμη του q. Όχι όμως σε οποιοδήποτε εκθέτη διότι ο εκθέτης του δε μπορεί αφενός να υπερβεί το 1 και αφετέρου το 2. Τελικά δε μπορεί να υπερβεί το 1. Άρα οι μόνοι κοινοί διαιρέτες των α, β είναι οι $q^0=1$, $q^1=q$. Ο μεγαλύτερος από αυτούς δηλαδή ο μέγιστος κοινός διαιρέτης των α, β είναι ο q.

Για τον [α, β]. Ένα πολλαπλάσιο του α θα πρέπει οπωσδήποτε στην κανονική του μορφή να περιλαμβάνει τους παράγοντες p, q και σε εκθέτες x, y με $x\ge 2$, $y\ge 1$. Όμοια ένα πολλαπλάσιο του β στην κανονική του μορφή θα περιλαμβάνει τους q, s με εκθέτες z, u όπου $z\ge 3$, $u\ge 5$. Ένα κοινό πολλαπλάσιο των α, β πρέπει επομένως να περιλαμβάνει στην κανονική του μορφή του p, q, r με εκθέτες κ, λ, μ όπου το κ δε μπορεί να είναι μικρότερο του 2, το λ ούτε του 1 ούτε του 3, και το μ του 5. Τελικά κάθε κοινό πολλαπλάσιο των α, β θα είναι της μορφής $\xi p^{\kappa}q^{\lambda}s^{\mu}$, όπου ο ξ θα είναι αριθμός που δεν θα έχει παράγοντες τους p, q, s και για τους κ, λ, μ θα είναι $\kappa\ge 2$, $\lambda\ge 3$, $\mu\ge 5$. Από όλα αυτά τα κοινά πολλαπλάσια το πιο μικρό προκύπτει αν φροντίσουμε να έχουμε και τους τέσσερις αριθμούς ξ, p^{κ}, q^{λ}, s^{μ} όσο γίνεται πιο μικρούς. Με δεδομένους τους περιορισμούς $\kappa\ge 2$, $\lambda\ge 3$, $\mu\ge 5$ αυτό επιτυγχάνεται αν πάρουμε $\xi=1$, $\kappa=2$, $\lambda=3$, $\mu=5$. Επομένως $[\alpha, \beta]= p^2q^3s^5$.

6.2.10. Με βάση τα προηγούμενα μπορούμε να βρούμε τον μέγιστο κοινό διαιρέτη και το ελάχιστο κοινό πολλαπλάσιο δύο αριθμών α, β των οποίων ξέρουμε την κανονική μορφή. Έστω δ ένας κοινός διαιρέτης των α, β. Αν ο δ δεν είναι 1 τότε θα έχει πρώτους παράγοντες. Ένα πρώτος παράγοντας p του δ πρέπει να είναι πρώτος παράγοντας αφενός του α και αφετέρου του β δηλαδή πρέπει ο p να είναι κοινός πρώτος παράγοντας των α και β. Ο εκθέτης με τον οποίο εμφανίζεται ο p στην κανονική μορφή του δ δεν μπορεί να υπερβεί ούτε τον εκθέτη στον οποίο εμφανίζεται στην κανονική μορφή του α ούτε σε εκείνη του β. Με άλλα λόγια δεν μπορεί να υπερβεί τον ελάχιστο από τους εκθέτες με τους οποίους εμφανίζεται στις κανονικές μορφές των α, β. Αν τώρα θέλουμε ο δ να είναι και μέγιστος κοινός διαιρέτης ένας τρόπος υπάρχει να το πετύχουμε: Να φροντίσουμε ο δ να έχει όσο γίνεται περισσότερους πρώτους παράγοντες (επομένως να έχει όλους τους κοινούς πρώτους παράγοντες των α, β) και τον κάθε πρώτο παράγοντα να τον έχει σε όσο -επιτρέπεται- μεγαλύτερο εκθέτη. Συμπεραίνουμε λοιπόν ότι:

Η κανονική μορφή του (α, β) θα περιλαμβάνει όλους τους κοινούς πρώτους παράγοντες των α, β και μόνο αυτούς τον κάθε ένα δε υψωμένο στον πιο μικρό από τους εκθέτες που εμφανίζονται στις κανονικές μορφές των α, β. Αν δεν υπάρχουν κοινοί πρώτοι παράγοντες των α, β τότε (α, β)=1. ■

Ένα κοινό πολλαπλάσιο m των α, β θα έχει μεταξύ των πρώτων παραγόντων του σίγουρα και τους πρώτους παράγοντες των α, β. Έστω p είναι ένας πρώτος παράγοντας του m. Ας πούμε ότι p^x, p^y, p^z, είναι οι μεγαλύτερες δυνάμεις του p που διαιρούν τους α, β, m. Επειδή α|m, β|m συνάγουμε ότι x≤z, y≤z. Άρα ο z θα είναι μεγαλύτερος ή ίσος από τον μέγιστο των x, y. Αν τώρα θέλουμε το m να είναι όχι απλώς πολλαπλάσιο των α, β αλλά το ελάχιστο κοινό πολλαπλάσιο των α, β θα πρέπει να πάρουμε όσο γίνεται λιγότερους πρώτους παράγοντες. Δηλαδή μόνο τους

«υποχρεωτικούς» που δεν είναι άλλοι από τους πρώτους παράγοντες που εμφανίζονται στο α ή στο β. Επίσης κάθε παράγοντα που παίρνουμε πρέπει να είναι υψωμένος σε όσο γίνεται μικρότερο εκθέτη πράγμα που σημαίνει ότι πρέπει αν είναι υψωμένος στον μέγιστο από τους εκθέτες που εμφανίζεται στην ανάλυση των α, β. Συμπεραίνουμε λοιπόν ότι:

Το [*α, β*] *στην κανονική του μορφή θα έχει ως πρώτους παράγοντες εκείνους των α ή β κοινούς και μη κοινούς και τον κάθε ένα υψωμένο στον μέγιστο των εκθετών που εμφανίζονται στην κανονική μορφή των α, β. τότε ο p θα πρέπει να εμφανίζεται στην κανονική ανάλυση του m σε εκθέτη που θα είναι μεγαλύτερος ή ίσος από τον εκθέτη με τον οποίο εμφανίζεται στην ανάλυση του α ή του β.* ■

7. ΓΡΑΜΜΙΚΕΣ ΔΙΟΦΑΝΤΙΚΕΣ ΕΞΙΣΩΣΕΙΣ

7.1. Μπορούμε να πληρώσουμε ένα λογαριασμό 5700 δραχμών χρησιμοποιώντας μόνο χιλιάρικα και πεντακοσάρικα χωρίς να χρειασθεί να πάρουμε ρέστα; Η απάντηση είναι προφανώς «όχι». Μπορούμε να κάνουμε το ίδιο χρησιμοποιώντας μόνο χιλιάρικα και κατοστάρικα; ; Η απάντηση είναι προφανώς «ναι». Κατά πόσους διαφορετικούς τρόπους μπορεί να γίνει αυτό; Ας πούμε ότι χρησιμοποιούμε x χιλιάρικα και y κατοστάρικα. Τότε πρέπει $1000x+100y=5700$. Απλοποιώντας τα μηδενικά βρίσκουμε $10x+y=57$. Πρέπει $x\geq 0$, $y\geq 0$. Επομένως αφού το x είναι ακέραιος δε μπορεί να υπερβεί το 5. Οι δυνατές τιμές του x είναι 0, 1, 2, 3, 4, 5 και οι αντίστοιχες με αυτές τιμές του y είναι $y=57-10x$ δηλαδή 57, 47, 37, 27, 17, 7.

7.2. Μόλις λύσαμε την εξίσωση $10x+y=57$ αναζητώντας όχι όλες τις λύσεις της που είναι άπειρα ζεύγη αριθμών

$(x, 57-10x)$ αλλά μόνο εκείνες που απαρτίζονται από μη αρνητικούς ακέραιους αριθμούς. Στην αναζήτηση μας αυτή, η λύση $(5{,}6 , 1)$ μολονότι είναι λύση της

10x+y=57 δε μας ενδιαφέρει. Μία πολυωνυμική εξίσωση με ένα ή περισσότερους αγνώστους λέγεται Διοφαντική αν οι συντελεστές και οι άγνωστοι της είναι ακέραιοι αριθμοί. Ο όρος προέρχεται από τον αρχαίο Έλληνα μαθηματικό **Διόφαντο** που έζησε στην Αλεξάνδρεια περί το 250 μ.Χ. Ο Διόφαντος έγραψε τα «*Αριθμητικά*» όπου πραγματεύονται μεταξύ άλλων προβλήματα με αγνώστους ακέραιους αριθμούς. Παραδείγματα Διοφαντικών εξισώσεων είναι με δύο αγνώστους είναι οι:

$$x^2 + y^2 = z^2$$

$$x^2 - ky^2 = 1$$

$$x^n + y^n = z^n \quad \text{n>2}$$

$$\alpha x+\beta y=\gamma$$

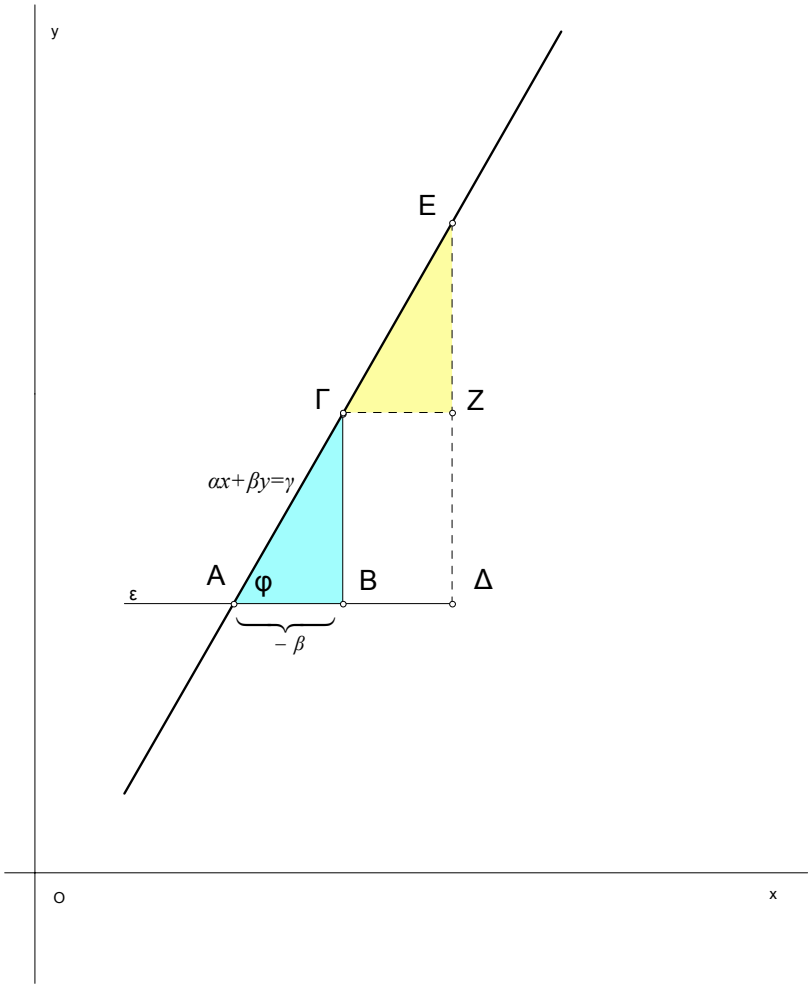
Στα επόμενα θα ασχοληθούμε με την τελευταία εξίσωση που λέγεται **γραμμική Διοφαντική εξίσωση**. Η ονομασία οφείλεται στο γεγονός ότι οι λύσεις της εφόσον υπάρχουν βρίσκονται όλες σε μία ευθεία γραμμή.

7.3. Έστω η γραμμική Διοφαντική εξίσωση

$$\alpha x+\beta y=\gamma \qquad \textbf{(1)}$$

Μπορούμε να υποθέσουμε ότι α>0 (Αν α<0 πολλαπλασιάζουμε και τα δύο μέλη με -1. Υπάρχουν δύο περιπτώσεις για το β μία να είναι αρνητικό και μία να είναι θετικό. Λύση της (1) είναι κάθε ζεύγος ακεραίων (x, y) που την επαληθεύει. Η (1) λοιπόν έχει λύση αν και μόνο αν το γ είναι γραμμικός συνδυασμός των α, β. Αυτό, όπως έχουμε δει, γεωμετρικά σημαίνει ότι η ευθεία με εξίσωση **(1)** διέρχεται από ένα τουλάχιστον συνδεσμικό σημείο δηλαδή ένα σημείο του οποίου οι συντεταγμένες είναι ακέραιοι αριθμοί. Έχουμε δει ότι ενδέχεται η ευθεία $\alpha x+\beta y=\gamma$ να μην διέρχεται από κανένα συνδεσμικό σημείο και επομένως ενδέχεται η (1) να μην έχει λύση. Ένα παράδειγμα αποτελεί η εξίσωση 2x+4y=5. Ας υποθέσουμε ότι β<0 (Στην περίπτωση όπου β>0

εργαζόμαστε ανάλογα) Ας δούμε τι συμβαίνει όταν η $\alpha x+\beta y=\gamma$ διέρχεται από κάποιο συνδεσμικό σημείο $A(x_0,y_0)$.



Από το σημείο Α φέρνουμε παράλληλη ε στον άξονα xx΄. Η παράλληλη αυτή σχηματίζει με την $\alpha x+\beta y=\gamma$ την γωνία φ. Η εφαπτομένη της φ είναι ο συντελεστής διευθύνσεως της $\alpha x+\beta y=\gamma$. Δηλαδή $\varepsilon\varphi\varphi=\frac{\alpha}{-\beta}$. Αν κινηθούμε στην ε δεξιά και σε απόσταση -β. Θα βρεθούμε στο σημείο Β. Η τετμημένη x του Β θα είναι $x=x_0+(-\beta)$ ενώ η τεταγμένη θα είναι η ίδια με του Α δηλαδή y_0. Είναι ΑΒ=-β. Φέρνουμε κάθετη στην ε στο Β η οποία τέμνει την $\alpha x+\beta y=\gamma$ στο Γ. Η τετμημένη του Γ είναι η ίδια με του Β δηλαδή $x=x_0+(-\beta)$

Ας πούμε ότι η τεταγμένη του Γ είναι y. Ας υπολογίσουμε το y. Παρατηρούμε ότι το μήκος του ΒΓ είναι $y - y_0$. Από το ορθογώνιο ΑΒΓ έχουμε ΒΓ=ΑΒεφφ δηλαδή $y - y_0 = -\beta\frac{\alpha}{-\beta}$. Επομένως

$$y = y_0 + \alpha$$

Το σημείο Γ λοιπόν ανήκει στην $\alpha x+\beta y=\gamma$ και έχει ακέραιες συντεταγμένες. ΄Αρα η **(1)** έχει άλλη μία λύση την $(x_0 +(-\beta), y_0 +\alpha)$. Μπορούμε να επαναλάβουμε την ίδια διαδικασία ξεκινώντας με την λύση $(x_0 +(-\beta), y_0 +\alpha)$ και να σχηματίσουμε το τρίγωνο ΓΕΖ. Θα καταλήξουμε στο συμπέρασμα ότι το Γ έχει ακέραιες συντεταγμένες $x_0 + 2(-\beta), y_0 + 2\alpha$ και ότι το ζεύγος $(x_0 + 2(-\beta), y_0 + 2\alpha)$ είναι επίσης λύση της **(1)**. Γενικά κινούμενοι προς τα πάνω θα βρούμε ότι όλα τα ζεύγη

$$(x_0 +(-\beta), y_0 +\alpha)$$

$$(x_0 + 2(-\beta), y_0 + 2\alpha)$$

$$(x_0 + 3(-\beta), y_0 + 3\alpha)$$

.....

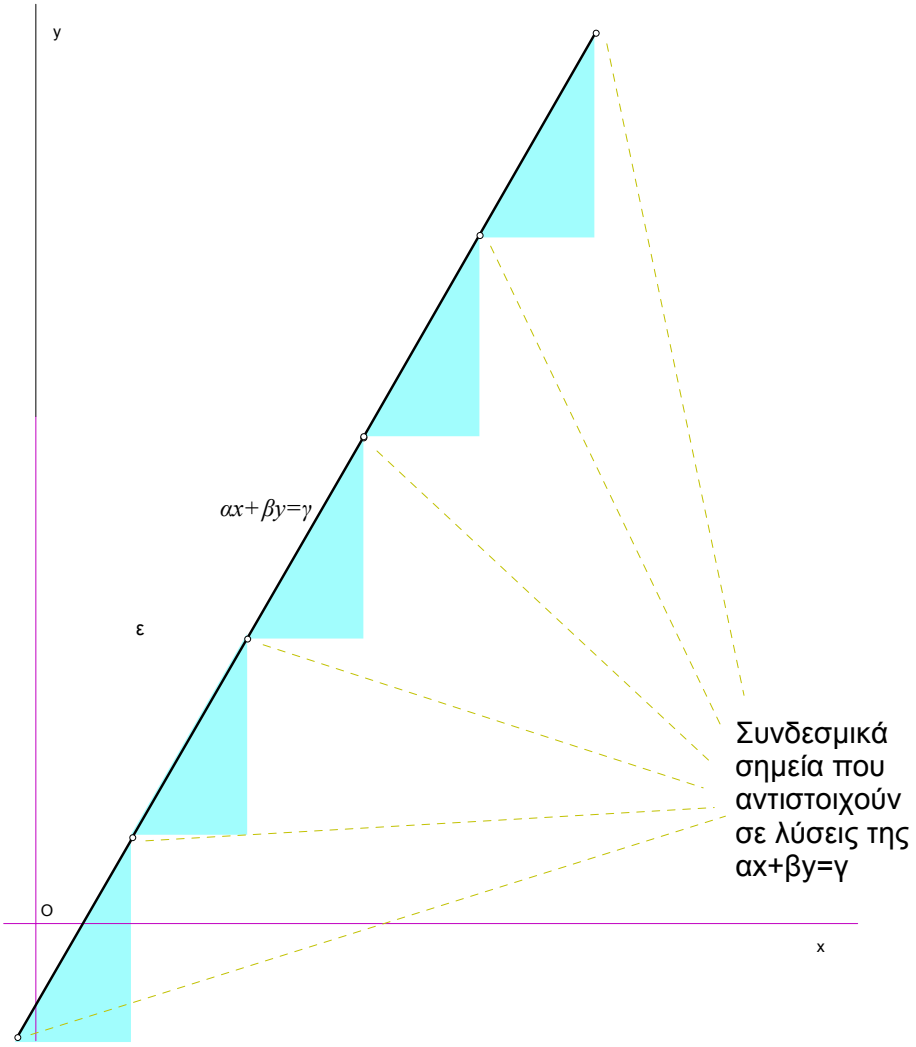
είναι λύσεις της **(1)**. Μπορούμε όμως να κινηθούμε προς τα κάτω και τότε θα βρούμε τις λύσεις

$$(x_0 -(-\beta), y_0 -\alpha)$$

$$(x_0 - 2(-\beta), y_0 - 2\alpha)$$

$$(x_0 - 3(-\beta), y_0 - 3\alpha)$$

.....



΄Ολες *αυτές* οι λύσεις εκφράζονται με ένα και μόνο τύπο όπως γίνεται και με τις λύσεις τριγωνομετρικών εξισώσεων:

$$(x_0 + k(-\beta), y_0 + k\alpha)\ k \in \mathbb{Z} \quad \textbf{(2)}$$

Εργασθήκαμε με την προϋπόθεση ότι η **(1)** έχει λύση. Πότε όμως συμβαίνει αυτό; Παρατηρούμε ότι αν υπάρχουν ακέραιοι x_0, y_0 που επαληθεύουν την **(1)** δηλαδή $\alpha x_0 + \beta y_0 = \gamma$ τότε τυχόν κάθε κοινός διαιρέτης των α, β θα διαιρεί τον $\alpha x_0 + \beta y_0$ και επομένως τον γ. Ιδιαιτέρως ο (α, β) *θα διαιρεί τον* γ. Αλλά και αντιστρόφως αν ο (α, β) διαιρεί τον γ τότε αφενός

(α, β)=κα+λβ για κάποιους κ, λ

και αφετέρου

γ=μ(α, β) για κάποιον μ

οπότε γ=μ(α, β)=μ(κα+λβ)=α(μκ)+β(μλ)δηλαδή το ζεύγος x_0=κα, y_0=λβ είναι λύση της **(1).** Βρήκαμε λοιπόν την συνθήκη ώστε η **(1)** να έχει λύση:

Η **(1)** *έχει λύση αν και μόνο αν ο μέγιστος κοινός διαιρέτης* (*α, β*) *των α, β διαιρεί τον γ.*

Βρήκαμε ότι αν η **(1)** έχει λύση (x_0,y_0) τότε θα έχει και τις άπειρες λύσεις **(2)**. Θα έχει όμως άλλες λύσεις εκτός των **(2)**; Ας πούμε ότι το ζεύγος (x_0',y_0') είναι λύση της **(1).** Τότε θα ισχύει

$$\alpha x_0+\beta y_0=\gamma, \qquad \alpha x_0'+\beta x_0'=\gamma$$

Συνδυάζοντας τις δύο αυτές ισότητες βρίσκουμε ότι

$$\alpha x_0+\beta y_0=\alpha x_0'+\beta y_0'$$

και επομένως $\beta(y_0'-y_0)=\alpha(x_0-x_0')$. Αυτό σημαίνει ότι $\beta|\alpha(x_0-x_0')$ και επειδή (α, β)=1 έχουμε ότι $\beta|(x_0-x_0')$. Αυτό σημαίνει ότι $x_0'-x_0=k\beta$ για κάποιο k και επομένως $x_0-x_0'=k\beta$ δηλαδή

$$x_0'=x_0+k(-\beta)$$

Αντικαθιστώντας στην $\alpha x_0+\beta y_0=\alpha x_0'+\beta y_0'$ το x_0' βρίσκουμε ότι $\alpha x_0+\beta y_0=\alpha(x_0+k(-\beta))+\beta y_0'$ από την οποία αν κάνουμε τις πράξεις προκύπτει ότι $\beta y_0=\alpha k(-\beta)+\beta y_0'$ δηλαδή y_0=-$\alpha k+y_0'$ και

$$y_0' = y_0+k\alpha$$

Επομένως η λύση (x_0',y_0') είναι της μορφής **(2)**.

Συνοψίζοντας όλα τα προηγούμενα έχουμε την πρόταση:

7.4. *Η γραμμική Διοφαντική εξίσωση* $\alpha x+\beta y=\gamma$ *έχει λύση αν και μόνο αν* $(\alpha,\beta)|\gamma$**.** *Στην περίπτωση που έχει λύση* (x_0, y_0) *τότε όλες οι λύσεις της είναι οι*

$$(x_0+k(-\beta), y_0+k\alpha)\ k\in Z \blacksquare$$

7.5. Ας λύσουμε την εξίσωση 18x+13y=31. Μία προφανής λύση της είναι το ζεύγος (1, 1). Τότε όλες οι λύσεις της είναι τα ζεύγη

(1-13k, 1+18k) με k τυχόντα ακέραιο. Για παράδειγμα θέτοντας k=2 βρίσκουμε την λύση (-25, 37).