ΚΕΦΑΛΑΙΟ Ι

ΟΙ ΦΥΣΙΚΟΙ ΑΡΙΘΜΟΙ

ΕΙΣΑΓΩΓΗ

Ο αριθμός είναι η βάση των σύγχρονων μαθηματικών. Τι είναι όμως αριθμός; Τι σημαίνει ότι $\frac{1}{2} + \frac{1}{2} = 1$, $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$, και $(-1)(-1) = 1$; Αν και στο σχολείο διδασκόμαστε τις μηχανικές διαδικασίες του χειρισμού κλασμάτων και αρνητικών αριθμών, για μια πραγματική κατανόηση του συστήματος αριθμών θα πρέπει να αναχθούμε σε απλούστερα στοιχεία. Ενώ οι Έλληνες επέλεξαν ως βάση των μαθηματικών τους τις γεωμετρικές έννοιες του σημείου και της ευθείας, η σύγχρονη καθοδηγητική αρχή είναι πλέον ότι όλες οι μαθηματικές προτάσεις θα πρέπει να μπορούν τελικά να αναχθούν σε προτάσεις σχετικά με τους *φυσικούς αριθμούς*, $1, 2, 3, \ldots$. «Ο Θεός δημιούργησε τους φυσικούς αριθμούς· όλα τα άλλα είναι έργο των χειρών του ανθρώπου». Με αυτά τα λόγια ο Leopold Kronecker (1823-1891) επισήμανε το ασφαλές έδαφος πάνω στο οποίο μπορεί να συγκροτηθεί η δομή των μαθηματικών.

Δημιουργημένοι από τον ανθρώπινο νου για την καταμέτρηση των αντικειμένων διαφόρων συλλογών, οι αριθμοί δεν συνδέονται καθόλου με τα ιδιαίτερα χαρακτηριστικά των καταμετρούμενων αντικειμένων. Ο αριθμός έξι συνιστά μια αφαίρεση από όλες τις πραγματικές συλλογές που περιλαμβάνουν έξι πράγματα· δεν εξαρτάται από καμία συγκεκριμένη ποιότητα αυτών των πραγμάτων, ούτε από τα σύμβολα που χρησιμοποιούνται. Ο αφηρημένος χαρακτήρας της έννοιας του αριθμού γίνεται σαφής μόνο σε ένα αρκετά προχωρημένο στάδιο διανοητικής ανάπτυξης. Για τα παιδιά, οι αριθμοί παραμένουν πάντα συνδεδεμένοι με απτά αντικείμενα όπως τα δάχτυλα ή οι χάντρες, και οι πρωτόγονες γλώσσες χαρακτηρίζονται από μια συγκεκριμένη αίσθηση του αριθμού, καθώς παρέχουν διαφορετικά σύνολα από λέξεις αριθμών για τους διαφορετικούς τύπους αντικειμένων.

Ευτυχώς, ο καθαυτό μαθηματικός δεν χρειάζεται να ασχοληθεί με τη φιλοσοφική φύση της μετάβασης από τις συλλογές συγκεκριμένων αντικειμένων στην αφηρημένη έννοια του αριθμού. Ως εκ τούτου, θα αποδεχθούμε τους φυ-

σικούς αριθμούς ως δεδομένους, μαζί με τις δύο θεμελιώδεις πράξεις, την πρόσθεση και τον πολλαπλασιασμό, με τις οποίες αυτοί μπορούν να συνδυαστούν μεταξύ τους.

§1. ΥΠΟΛΟΓΙΣΜΟΣ ΜΕ ΑΚΕΡΑΙΟΥΣ

1. Οι νόμοι της αριθμητικής

Η μαθηματική θεωρία των φυσικών αριθμών, ή αλλιώς των *θετικών ακεραίων*, ονομάζεται *αριθμητική*. Βασίζεται στο γεγονός ότι η πρόσθεση και ο πολλαπλασιασμός ακεραίων διέπονται από ορισμένους νόμους. Για να διατυπώσουμε αυτούς τους νόμους στην πλήρη γενικότητά τους, δεν μπορούμε να χρησιμοποιήσουμε σύμβολα όπως τα $1, 2, 3$ τα οποία αναφέρονται σε συγκεκριμένους ακεραίους. Η πρόταση

$$1 + 2 = 2 + 1$$

είναι μόνο ένα συγκεκριμένο «στιγμιότυπο» του γενικού νόμου ότι το άθροισμα δύο ακεραίων είναι το ίδιο ανεξάρτητα από τη σειρά με την οποία θεωρούμε αυτούς τους ακεραίους. Συνεπώς, όταν θέλουμε να εκφράσουμε το γεγονός ότι μια ορισμένη σχέση ανάμεσα σε ακεραίους ισχύει ανεξάρτητα από τις τιμές των συγκεκριμένων ακεραίων που υπεισέρχονται, θα δηλώνουμε τους ακεραίους συμβολικά με τα γράμματα $a, b, c, \ldots$. Με αυτή τη συμφωνία, μπορούμε να διατυπώσουμε πέντε θεμελιώδεις νόμους της αριθμητικής οι οποίοι είναι γνωστοί στον αναγνώστη:

$$\begin{aligned} &(1)\ \ a + b = b + a, && (2)\ \ ab = ba,\\ &(3)\ \ a + (b + c) = (a + b) + c, && (4)\ \ a(bc) = (ab)c,\\ &&(5)\ \ a(b + c) = ab + ac. \end{aligned}$$

Οι δύο πρώτοι από αυτούς, ο *αντιμεταθετικός* νόμος της πρόσθεσης και του πολλαπλασιασμού, ορίζουν ότι μπορούμε να εναλλάξουμε τη σειρά των στοιχείων που υπεισέρχονται στην πρόσθεση ή τον πολλαπλασιασμό. Ο τρίτος, ο *προσεταιριστικός* νόμος της πρόσθεσης, ορίζει ότι η πρόσθεση τριών αριθμών δίνει το ίδιο αποτέλεσμα είτε προσθέσουμε στον πρώτο το άθροισμα του δεύτερου και του τρίτου, είτε προσθέσουμε στον τρίτο το άθροισμα του πρώτου και του δεύτερου. Ο τέταρτος είναι ο προσεταιριστικός νόμος του πολλαπλασιασμού. Ο τελευταίος, ο *επιμεριστικός* νόμος, εκφράζει το γεγονός ότι για να πολλαπλασιάσουμε ένα άθροισμα με έναν ακέραιο μπορούμε να πολλαπλασιάσουμε κάθε όρο του αθροίσματος με αυτό τον ακέραιο και κατόπιν να προσθέσουμε τα γινόμενα.

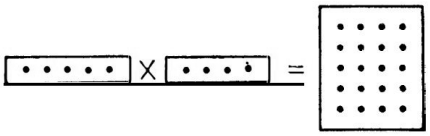
Αυτοί οι νόμοι της αριθμητικής είναι πολύ απλοί, και ίσως να φαίνονται προφανείς. Αλλά πιθανόν να μην ισχύουν για οντότητες διαφορετικές από τους

ακέραιους αριθμούς. Αν τα a και b δεν συμβολίζουν ακεραίους αλλά χημικές ουσίες, και αν η λέξη «πρόσθεση» χρησιμοποιείται με την καθημερινή της σημασία, είναι εμφανές ότι ο αντιμεταθετικός νόμος δεν θα ισχύει πάντα. Για παράδειγμα, αν προστεθεί θειικό οξύ σε νερό, θα προκύψει ένα αραιό διάλυμα, ενώ ή πρόσθεση νερού σε καθαρό θειικό οξύ μπορεί να καταλήξει σε καταστροφή για τον πειραματιζόμενο. Με αντίστοιχα παραδείγματα μπορεί να δειχθεί ότι σε αυτού του είδους τη χημική «αριθμητική» πιθανόν να μην ισχύουν επίσης ο προσεταιριστικός και ο επιμεριστικός νόμος της πρόσθεσης. Επομένως, μπορεί κανείς να φανταστεί είδη αριθμητικής στα οποία ένας ή περισσότεροι από τους νόμους (1)-(5) δεν ισχύουν. Τέτοια συστήματα έχουν στην πραγματικότητα μελετηθεί στα σύγχρονα μαθηματικά.

Το διαισθητικό θεμέλιο στο οποίο βασίζονται οι νόμοι (1)-(5) μπορεί να καταδειχθεί με ένα «χειροπιαστό» μοντέλο για την αφηρημένη έννοια του ακεραίου. Αντί για τα συνήθη σύμβολα $1, 2, 3$, κ.λπ., των αριθμών, ας συμβολίσουμε τον ακέραιο που δίνει το πλήθος των αντικειμένων σε μια δεδομένη συλλογή (λόγου χάριν, στη συλλογή των μήλων σε ένα συγκεκριμένο δέντρο) με ένα σύνολο από κουκκίδες τοποθετημένες μέσα σε ένα παραλληλόγραμμο κουτί, μία κουκκίδα για κάθε αντικείμενο. Κάνοντας πράξεις με αυτά τα κουτιά, μπορούμε να διερευνήσουμε τους νόμους της αριθμητικής των ακεραίων. Για να προσθέσουμε δύο ακεραίους a και b, τοποθετούμε τα αντίστοιχα κουτιά το ένα «κολλητά» στο άλλο, και αφαιρούμε τη διαχωριστική γραμμή.

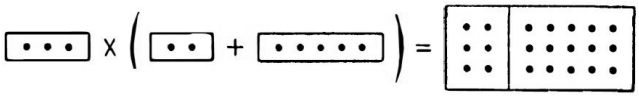
Σχήμα 1. Πρόσθεση.

Για να πολλαπλασιάσουμε τους a και b, διατάσσουμε τις κουκκίδες των δύο κουτιών σε γραμμές, και σχηματίζουμε ένα νέο κουτί με a γραμμές και b στήλες από κουκκίδες. Είναι πλέον φανερό ότι οι κανόνες (1)-(5) αντιστοιχούν σε διαισθητικά προφανείς ιδιότητες αυτών των πράξεων με κουτιά.



Σχήμα 2. Πολλαπλασιασμός.

Με βάση τον ορισμό της πρόσθεσης δύο ακεραίων, μπορούμε να ορίσουμε τη σχέση της *ανισότητας*. Καθεμία από τις ισοδύναμες προτάσεις $a < b$ (που διαβάζεται, «το a είναι μικρότερο του b») και $b > a$ (που διαβάζεται, «το b είναι μεγαλύτερο του a») σημαίνει ότι το κουτί b μπορεί να προκύψει από το



Σχήμα 3. Ο επιμεριστικός νόμος.

κουτί a με την πρόσθεση ενός κατάλληλα επιλεγμένου τρίτου κουτιού c, έτσι ώστε $b = a + c$. Όταν ισχύει αυτό, γράφουμε τη σχέση

$$c = b - a,$$

η οποία ορίζει την πράξη της *αφαίρεσης*.

Σχήμα 4. Αφαίρεση.

Λέμε ότι η πρόσθεση και η αφαίρεση είναι *αντίστροφες πράξεις*, διότι αν η πρόσθεση του ακεραίου d στον ακέραιο a ακολουθηθεί από την αφαίρεση του ακεραίου d, το αποτέλεσμα είναι ο αρχικός ακέραιος a:

$$(a + d) - d = a.$$

Να σημειωθεί ότι ο ακέραιος $b - a$ έχει οριστεί μόνο όταν $b > a$. Η ερμηνεία του συμβόλου $b - a$ ως *αρνητικού αριθμού* όταν $b < a$ θα εξεταστεί παρακάτω (σελ. 60 κ.ε.).

Συχνά μας διευκολύνει να χρησιμοποιούμε μία από τις εκφράσεις $b \geq a$ (που διαβάζεται «το b είναι μεγαλύτερο ή ίσο του a») ή $a \leq b$ (που διαβάζεται «το a είναι μικρότερο ή ίσο του b»), για να εκφράσουμε την άρνηση της πρότασης $a > b$. Επομένως, $2 \geq 2$ και $3 \geq 2$.

Μπορούμε να επεκτείνουμε ελαφρά την επικράτεια των θετικών ακεραίων, που αναπαριστώνται από κουτιά με κουκκίδες, εισάγοντας τον ακέραιο *μηδέν*, που αναπαριστάται από ένα εντελώς άδειο κουτί. Αν συμβολίσουμε το άδειο κουτί με το συνηθισμένο σύμβολο 0, τότε, σύμφωνα με τον ορισμό μας για την πρόσθεση και τον πολλαπλασιασμό,

$$\begin{aligned} a + 0 &= a, \\ a \cdot 0 &= 0, \end{aligned}$$

για κάθε ακέραιο a. Διότι το $a + 0$ συμβολίζει την πρόσθεση ενός άδειου κουτιού στο κουτί a, ενώ το $a \cdot 0$ συμβολίζει ένα κουτί χωρίς καμία στήλη· δηλαδή, ένα άδειο κουτί. Είναι λοιπόν φυσικό να επεκτείνουμε τον ορισμό της αφαίρεσης θέτοντας

$$a - a = 0$$

για κάθε ακέραιο a. Αυτές είναι οι χαρακτηριστικές αριθμητικές ιδιότητες του μηδενός.

Γεωμετρικά μοντέλα σαν αυτά τα κουτιά με τις κουκκίδες, όπως ο αρχαίος άβακας, χρησιμοποιούνταν ευρέως για αριθμητικούς υπολογισμούς μέχρι τα τέλη του Μεσαίωνα, οπότε άρχισαν να αντικαθίστανται σταδιακά από πολύ ανώτερες συμβολικές μεθόδους με βάση το δεκαδικό σύστημα.

2. Η αναπαράσταση των ακεραίων

Θα πρέπει να διακρίνουμε προσεκτικά ανάμεσα σε έναν ακέραιο και το σύμβολο, 5, V, …, κ.λπ., που χρησιμοποιείται για να αναπαρασταθεί αυτός ο ακέραιος. Στο δεκαδικό σύστημα, χρησιμοποιούνται τα δέκα σύμβολα ψηφίων $0, 1, 2, 3, \ldots, 9$ για το μηδέν και τους πρώτους εννέα θετικούς ακεραίους. Ένας μεγαλύτερος αριθμός, όπως το «τριακόσια εβδομήντα δύο», μπορεί να εκφραστεί στη μορφή

$$300 + 70 + 2 = 3 \cdot 10^2 + 7 \cdot 10 + 2,$$

και συμβολίζεται στο δεκαδικό σύστημα με το σύμβολο 372. Το σημαντικό εδώ είναι ότι το νόημα των συμβόλων ψηφίων $3, 7, 2$ εξαρτάται από τη *θέση* τους, δηλαδή από το αν βρίσκονται στη θέση των μονάδων, των δεκάδων ή των εκατοντάδων. Με αυτό τον «θεσιακό συμβολισμό» μπορούμε να αναπαραστήσουμε οποιονδήποτε ακέραιο χρησιμοποιώντας μόνο τα δέκα σύμβολα ψηφίων σε διάφορους συνδυασμούς. Ο γενικός κανόνας είναι ότι εκφράζουμε έναν ακέραιο στη μορφή

$$z = a \cdot 10^3 + b \cdot 10^2 + c \cdot 10 + d,$$

όπου τα ψηφία a, b, c, d είναι ακέραιοι από το μηδέν μέχρι το εννέα. Επομένως, ο ακέραιος z αναπαριστάται από τη συντομογραφική έκφραση

$$abcd.$$

Ειρήσθω εν παρόδω ότι οι συντελεστές d, c, b, a είναι τα υπόλοιπα που απομένουν μετά από διαδοχικές διαιρέσεις του z με το 10. Συνεπώς,

372	10	Υπόλοιπο
37	10	2
3	10	7
0		3

Η συγκεκριμένη έκφραση που παραθέσαμε παραπάνω για το z μπορεί να αναπαραστήσει μόνο ακεραίους μικρότερους από τις δέκα χιλιάδες, αφού οι μεγαλύτεροι ακέραιοι θα απαιτούν πέντε ή περισσότερα σύμβολα ψηφίων. Αν ο z είναι ένας ακέραιος ανάμεσα στις δέκα χιλιάδες και στις εκατό χιλιάδες, μπορούμε να τον εκφράσουμε στη μορφή

$$z = a \cdot 10^4 + b \cdot 10^3 + c \cdot 10^2 + d \cdot 10 + e,$$

και να τον αναπαραστήσουμε με την έκφραση $abcde$. Μια αντίστοιχη πρόταση ισχύει για τους ακεραίους που βρίσκονται ανάμεσα στις εκατό χιλιάδες και στο ένα εκατομμύριο, κ.ο.κ. Είναι πολύ χρήσιμο να έχουμε έναν τρόπο να υποδεικνύουμε το αποτέλεσμα σε πλήρη γενικότητα με έναν μόνο τύπο. Για να το κάνουμε αυτό, μπορούμε να συμβολίσουμε όλους τους διαφορετικούς συντελεστές $e, d, c, ...$ μόνο με το γράμμα a με διαφορετικούς «κάτω δείκτες», $a_0, a_1, a_2, a_3, ...$, και να εκφράσουμε το γεγονός ότι οι δυνάμεις του δέκα μπορούν να είναι όσο μεγάλες απαιτείται συμβολίζοντας την ανώτατη δύναμη όχι με 10^3 ή 10^4 όπως στα παραπάνω παραδείγματα, αλλά με 10^n, όπου το n θεωρείται ότι συμβολίζει έναν τυχόντα ακέραιο. Επομένως, η γενική μέθοδος για την αναπαράσταση ενός ακεραίου z στο δεκαδικό σύστημα είναι να εκφράσουμε τον z στη μορφή

$$z = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0, \tag{1}$$

και να τον αναπαραστήσουμε με την έκφραση

$$a_n a_{n-1} a_{n-2} \cdots a_1 a_0.$$

Όπως και στην ειδική περίπτωση παραπάνω, βλέπουμε ότι τα ψηφία $a_0, a_1, a_2, \ldots, a_n$ είναι απλά τα διαδοχικά υπόλοιπα της επανειλημμένης διαίρεσης του z με το 10.

Στο δεκαδικό σύστημα, ο αριθμός δέκα έχει επιλεγεί για να λειτουργεί ως βάση. Ο μη εξοικειωμένος με τα μαθηματικά αναγνώστης ίσως να μη συνειδητοποιεί ότι η επιλογή του δέκα δεν είναι ουσιώδης, και ότι οποιοσδήποτε ακέραιος μεγαλύτερος του ένα θα μπορούσε να εξυπηρετήσει τον ίδιο σκοπό. Για παράδειγμα, θα μπορούσε να χρησιμοποιηθεί ένα *επταδικό* σύστημα (με βάση το 7). Σε ένα τέτοιο σύστημα, ένας ακέραιος θα εκφραζόταν ως

$$b_n \cdot 7^n + b_{n-1} \cdot 7^{n-1} + \cdots + b_1 \cdot 7 + b_0, \tag{2}$$

όπου τα b είναι ψηφία από το μηδέν μέχρι το έξι, και θα συμβολιζόταν με την έκφραση

$$b_n b_{n-1} \cdots b_1 b_0.$$

Συνεπώς, το «εκατόν εννέα» θα συμβολιζόταν στο επταδικό σύστημα με την έκφραση 214, η οποία σημαίνει

$$2 \cdot 7^2 + 1 \cdot 7 + 4.$$

Ο αναγνώστης μπορεί να αποδείξει ως άσκηση πως ο γενικός κανόνας για να περνάμε από τη βάση δέκα σε οποιαδήποτε άλλη βάση B είναι ότι εκτελούμε διαδοχικές διαιρέσεις του αριθμού z με το B· τα υπόλοιπα των διαιρέσεων θα είναι τα ψηφία του αριθμού στο σύστημα με βάση B. Για παράδειγμα:

109	7	Υπόλοιπο
15	7	4
2	7	1
0		2

$$109 \text{ (δεκαδικό σύστημα)} = 214 \text{ (επταδικό σύστημα)}.$$

Είναι φυσικό να αναρωτιέται κανείς αν κάποια συγκεκριμένη επιλογή βάσης θα ήταν πιο επιθυμητή από τις άλλες. Όπως θα δούμε, μια πολύ μικρή βάση έχει μειονεκτήματα, ενώ μια μεγάλη βάση απαιτεί την απομνημόνευση πολλών συμβόλων ψηφίων, και έναν εκτενή πίνακα πολλαπλασιασμού. Κάποιοι έχουν υποστηρίξει την επιλογή του δώδεκα ως βάσης, διότι το δώδεκα διαιρείται ακριβώς με το δύο, το τρία, το τέσσερα και το έξι, και ως εκ τούτου οι εργασίες που περιλαμβάνουν διαίρεση και κλάσματα συχνά θα απλοποιούνταν. Για να γράψουμε οποιονδήποτε ακέραιο στη βάση δώδεκα (στο δωδεκαδικό σύστημα), χρειαζόμαστε δύο νέα σύμβολα ψηφίων για το δέκα και για το έντεκα. Ας συμβολίσουμε με α το δέκα και με β το δώδεκα. Τότε, στο δωδεκαδικό σύστημα το «δώδεκα» θα γραφόταν 10, το «είκοσι δύο» θα ήταν 1α, το «είκοσι τρία» θα ήταν 1β, και το «εκατόν τριάντα ένα» θα ήταν $\alpha\beta$.

Η επινόηση του θεσιακού συμβολισμού, ο οποίος αποδίδεται στους Σουμέριους ή Βαβυλώνιους και εξελίχθηκε από τους Ινδούς, είχε τεράστια σημασία για τον πολιτισμό. Τα πρώιμα συστήματα αρίθμησης βασίζονταν σε μια αμιγώς προσθετική αρχή. Στον συμβολισμό των Ρωμαίων, για παράδειγμα, χρησιμοποιούνταν εκφράσεις του τύπου

$$\text{CXVIII} = \text{εκατό} + \text{δέκα} + \text{πέντε} + \text{ένα} + \text{ένα} + \text{ένα}.$$

Τα συστήματα αρίθμησης των Αιγυπτίων, των Εβραίων και των Ελλήνων ήταν στο ίδιο επίπεδο. Ένα μειονέκτημα οποιουδήποτε αμιγώς προσθετικού συμβολισμού είναι ότι καθώς οι αριθμοί γίνονται μεγαλύτεροι απαιτούνται ολοένα

και περισσότερα νέα σύμβολα. (Βέβαια, οι φυσικοί επιστήμονες των παλαιών εποχών δεν είχαν να αντιμετωπίσουν τα σημερινά αστρονομικά ή ατομικά μεγέθη.) Αλλά το κύριο ελάττωμα των αρχαίων συστημάτων, όπως αυτού των Ρωμαίων, ήταν ότι οι υπολογισμοί με αριθμούς ήταν τόσο δύσκολοι που οποιοδήποτε πρόβλημα εκτός από τα πολύ απλά μπορούσαν να το χειριστούν μόνο οι ειδήμονες. Με το θεσιακό σύστημα των Ινδών που χρησιμοποιείται σήμερα, η κατάσταση είναι εντελώς διαφορετική. Το σύστημα αυτό το εισήγαγαν στη μεσαιωνική Ευρώπη οι έμποροι της Ιταλίας, που το έμαθαν από τους Μουσουλμάνους. Το θεσιακό σύστημα έχει την ευπρόσδεκτη ιδιότητα ότι όλοι οι αριθμοί, οσοδήποτε μεγάλοι ή μικροί, μπορούν να αναπαρασταθούν μέσω ενός μικρού συνόλου από διαφορετικά σύμβολα ψηφίων (στο δεκαδικό σύστημα, τα ψηφία αυτά είναι οι «αραβικοί αριθμοί» $0, 1, 2, \ldots, 9$). Από την ιδιότητα αυτή απορρέει το πιο σημαντικό πλεονέκτημα της ευκολίας των υπολογισμών. Οι κανόνες υπολογισμών με αριθμούς που αναπαριστώνται σε θεσιακό συμβολισμό μπορούν να διατυπωθούν με τη μορφή πινάκων πρόσθεσης και πολλαπλασιασμού για τα ψηφία οι οποίοι μπορούν να απομνημονευθούν άπαξ και δια παντός. Η αρχαία τέχνη του υπολογισμού, που κάποτε ήταν προνόμιο λίγων ειδημόνων, τώρα διδάσκεται στο δημοτικό σχολείο. Δεν υπάρχουν πολλές περιπτώσεις όπου η επιστημονική πρόοδος έχει επηρεάσει και διευκολύνει τόσο βαθιά την καθημερινή ζωή.

3. Υπολογισμοί σε συστήματα διαφορετικά από το δεκαδικό

Η χρήση του δέκα ως βάσης ανάγεται στην απαρχή του πολιτισμού, και οφείλεται αναμφίβολα στο γεγονός ότι έχουμε δέκα δάχτυλα με τα οποία μπορούμε να μετράμε. Αλλά στις ονομασίες των αριθμών σε πολλές γλώσσες υπάρχουν απομεινάρια της χρήσης άλλων βάσεων, ιδιαίτερα του δώδεκα και του είκοσι. Στα αγγλικά και στα γερμανικά, οι λέξεις για το 11 και το 12 δεν κατασκευάζονται σύμφωνα με τη δεκαδική αρχή του συνδυασμού του 10 με τα ψηφία, όπως οι λέξεις με κατάληξη «teen», αλλά είναι γλωσσικά ανεξάρτητες από τις λέξεις για το 10. Στα γαλλικά, οι λέξεις «vingt» και «quatrevingt» για το 20 και για το 80 υποδεικνύουν ότι για κάποιους σκοπούς ίσως να έχει χρησιμοποιηθεί ένα σύστημα με βάση το 20. Στα δανέζικα, η λέξη για το 70, «halvfirsindstyve», σημαίνει το μέσον (από το τριπλάσιο) μέχρι το τετραπλάσιο του είκοσι. Οι Βαβυλώνιοι αστρονόμοι είχαν ένα σύστημα συμβολισμού που ήταν εν μέρει εξηκονταδικό (βάση 60), και πιστεύεται ότι σε αυτό οφείλεται η καθιερωμένη διαίρεση της ώρας και της μοίρας σε 60 λεπτά.

Σε ένα σύστημα διαφορετικό από το δεκαδικό, οι κανόνες της αριθμητικής είναι οι ίδιοι, αλλά θα πρέπει να χρησιμοποιεί κανείς διαφορετικούς πίνακες για την πρόσθεση και τον πολλαπλασιασμό ψηφίων. Καθώς είμαστε συνηθισμένοι στο δεκαδικό σύστημα και συνδεδεμένοι με αυτό μέσω των λέξεων

της γλώσσας μας για τους αριθμούς, αυτό ίσως να μας μπερδέψει αρχικά. Ας δοκιμάσουμε ένα παράδειγμα πολλαπλασιασμού στο επταδικό σύστημα. Πριν προχωρήσουμε, θα ήταν σκόπιμο να παραθέσουμε τους πίνακες που θα πρέπει να χρησιμοποιήσουμε.

Πρόσθεση

	1	2	3	4	5	6
1	2	3	4	5	6	10
2	3	4	5	6	10	11
3	4	5	6	10	11	12
4	5	6	10	11	12	13
5	6	10	11	12	13	14
6	10	11	12	13	14	15

Πολλαπλασιασμός

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	11	13	15
3	3	6	12	15	21	24
4	4	11	15	22	26	33
5	5	13	21	26	34	42
6	6	15	24	33	42	51

Ας πολλαπλασιάσουμε τώρα το 265 επί 24, όπου αυτές οι αριθμητικές εκφράσεις είναι γραμμένες στο επταδικό σύστημα. (Στο δεκαδικό σύστημα, αυτό θα ήταν ισοδύναμο με το να πολλαπλασιάσουμε το 145 επί 18.) Οι κανόνες του πολλαπλασιασμού είναι οι ίδιοι όπως και στο δεκαδικό σύστημα. Αρχικά πολλαπλασιάζουμε 5 επί 4, που μας κάνει 26, όπως βλέπουμε στον πίνακα του πολλαπλασιασμού.

$$\begin{array}{r} 265 \\ \times\ \ 24 \\ \hline 1456 \\ 563 \\ \hline 10416 \end{array}$$

Γράφουμε το 6 στη θέση των μονάδων, και έχουμε «κρατούμενο» 2 για την επόμενη θέση. Κατόπιν βρίσκουμε $4 \cdot 6 = 33$, και $33 + 2 = 35$. Γράφουμε το 5 και συνεχίζουμε με τον ίδιο τρόπο μέχρι να τα πολλαπλασιάσουμε όλα. Προσθέτοντας $1456 + 5630$, παίρνουμε $6 + 0 = 6$ στη θέση των μονάδων, $5 + 3 = 11$ στη θέση των επτάδων. Και πάλι γράφουμε 1 και κρατάμε 1 για τη θέση των σαρανταεννιάδων, όπου έχουμε $1+6+4 = 14$. Το τελικό αποτέλεσμα είναι $265 \cdot 24 = 10.416$.

Για να ελέγξουμε αυτό το αποτέλεσμα μπορούμε να πολλαπλασιάσουμε τους ίδιους αριθμούς στο δεκαδικό σύστημα. Το 10.416 (στο επταδικό σύστημα) μπορεί να γραφτεί στο δεκαδικό σύστημα αν βρούμε τις δυνάμεις του 7 μέχρι και την τέταρτη: $7^2 = 49$, $7^3 = 343$, $7^4 = 2401$. Επομένως, $10.416 = 2401 + 4 \cdot 49 + 7 + 6$, όπου αυτός ο υπολογισμός είναι στο δεκαδικό σύστημα. Προσθέτοντας αυτούς τους αριθμούς βρίσκουμε ότι το 10.416 στο επταδικό σύστημα ισούται με το 2610 στο δεκαδικό σύστημα. Κατόπιν πολλαπλασιά-

ζουμε το 145 με το 18 στο δεκαδικό σύστημα· το αποτέλεσμα είναι 2610, οπότε οι υπολογισμοί έχουν επαληθευτεί.

Ασκήσεις: 1) Καταστρώστε τους πίνακες της πρόσθεσης και του πολλαπλασιασμού στο δωδεκαδικό σύστημα και εργαστείτε με κάποια παραδείγματα του ίδιου τύπου.

2) Εκφράστε το «τριάντα» και το «εκατόν τριάντα τρία» στα συστήματα με βάσεις $5, 7, 11, 12$.

3) Τι σημαίνουν οι εκφράσεις 11111 και 21212 σε αυτά τα συστήματα;

4) Καταστρώστε τους πίνακες της πρόσθεσης και του πολλαπλασιασμού για τις βάσεις $5, 11, 13$.

Από θεωρητικής σκοπιάς, το θεσιακό σύστημα με βάση το 2 ξεχωρίζει ως το σύστημα με την ελάχιστη δυνατή βάση. Τα μοναδικά ψηφία σε αυτό το *δυαδικό σύστημα* είναι το 0 και το 1· κάθε άλλος αριθμός z αναπαριστάται από μια αλληλουχία αυτών των συμβόλων. Οι πίνακες της πρόσθεσης και του πολλαπλασιασμού συνίστανται απλώς στους κανόνες $1+1=10$ και $1\cdot 1=1$. Αλλά το μειονέκτημα του συστήματος αυτού είναι προφανές: για να αναπαρασταθούν ακόμα και μικροί αριθμοί απαιτούνται μακροσκελείς εκφράσεις. Έτσι, το εβδομήντα εννέα, που μπορεί να εκφραστεί ως $1\cdot 2^6+0\cdot 2^5+0\cdot 2^4+1\cdot 2^3+1\cdot 2^2+1\cdot 2+1$ γράφεται στο δυαδικό σύστημα ως 1.001.111.

Για να καταδείξουμε την απλότητα του πολλαπλασιασμού στο δυαδικό σύστημα, θα πολλαπλασιάσουμε το επτά με το πέντε, τα οποία είναι αντίστοιχα 111 και 101. Υπενθυμίζοντας ότι $1+1=10$ σε αυτό το σύστημα, έχουμε ότι

$$\begin{array}{r} 111 \\ \times\ 101 \\ \hline 111 \\ 111 \\ \hline 100011 \end{array} = 2^5+2+1$$

που είναι τριάντα πέντε, όπως έπρεπε.

Ο Gottfried Wilhelm Leibniz (1646-1716), ένας από τους μεγαλύτερους στοχαστές της εποχής του, ήταν λάτρης του δυαδικού συστήματος. Σύμφωνα με τον Laplace: «Ο Leibniz έβλεπε στη δυαδική αριθμητική του την εικόνα της δημιουργίας. Φανταζόταν ότι η Μονάδα αντιπροσώπευε τον Θεό, και το μηδέν το κενό· ότι το Ανώτατο Ον εξήγαγε όλα τα όντα από το κενό, ακριβώς όπως η μονάδα και το μηδέν εκφράζουν όλους τους αριθμούς στο σύστημα αρίθμησής του.»

Άσκηση: Θεωρήστε το ερώτημα της αναπαράστασης ακεραίων με βάση a. Για να ονοματίσουμε τους ακεραίους σε αυτό το σύστημα, χρειαζόμαστε λέξεις για τα ψηφία $0, 1, \ldots, a-1$ και για τις διάφορες δυνάμεις του a: $a, a^2, a^3, \ldots$. Πόσες διαφορετικές λέξεις για αριθμούς χρειάζονται για να ονοματίσουμε όλους τους αριθμούς από το μηδέν μέχρι το χίλια, για $a=2, 3, 4, 5, \ldots, 15$; Ποια βάση απαιτεί τις ελάχιστες τέτοιες

λέξεις; (Παραδείγματα: Αν $a = 10$, χρειαζόμαστε δέκα λέξεις για τα ψηφία, συν λέξεις για το 10, το 100 και το 1000, δηλαδή συνολικά 13 λέξεις. Για $a = 20$, χρειαζόμαστε είκοσι λέξεις για τα ψηφία, συν λέξεις για το 20 και για το 400, δηλαδή συνολικά 22. Αν $a = 100$, χρειαζόμαστε 100 συν 1 λέξεις.)

*§2. Η ΑΠΕΙΡΙΑ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΑΡΙΘΜΩΝ. ΜΑΘΗΜΑΤΙΚΗ ΕΠΑΓΩΓΗ.

1. Η αρχή της μαθηματικής επαγωγής

Η ακολουθία των ακεραίων $1, 2, 3, 4, \ldots$ δεν έχει τέλος· διότι όταν έχουμε φτάσει σε οποιονδήποτε ακέραιο n, μπορούμε να γράψουμε τον επόμενο ακέραιο, $n + 1$. Εκφράζουμε αυτή την ιδιότητα της ακολουθίας των ακεραίων λέγοντας ότι υπάρχουν *άπειροι το πλήθος* ακέραιοι. Η ακολουθία των ακεραίων αντιπροσωπεύει το απλούστερο και πιο φυσικό παράδειγμα του μαθηματικού απείρου, το οποίο παίζει κυρίαρχο ρόλο στα σύγχρονα μαθηματικά. Παντού σε αυτό το βιβλίο θα έχουμε να πραγματευτούμε συλλογές ή «σύνολα» που περιέχουν άπειρα το πλήθος μαθηματικά αντικείμενα, όπως το σύνολο όλων των σημείων σε μια ευθεία ή το σύνολο όλων των τριγώνων σε ένα επίπεδο. Η άπειρη ακολουθία των ακεραίων είναι το απλούστερο δυνατό παράδειγμα άπειρου συνόλου.

Η βήμα προς βήμα διαδικασία του περάσματος από το n στο $n + 1$ η οποία παράγει την άπειρη ακολουθία των ακεραίων αποτελεί επίσης τη βάση ενός από τα πιο θεμελιώδη μοτίβα μαθηματικής συλλογιστικής, της αρχής της μαθηματικής επαγωγής. Η «εμπειρική επαγωγή» στις φυσικές επιστήμες προχωρά από μια συγκεκριμένη σειρά παρατηρήσεων ενός ορισμένου φαινομένου στη διατύπωση ενός γενικού νόμου που διέπει όλες τις εμφανίσεις αυτού του φαινομένου. Ο βαθμός βεβαιότητας με τον οποίο ο νόμος τεκμηριώνεται με αυτό τον τρόπο εξαρτάται από το πλήθος των μεμονωμένων παρατηρήσεων και επιβεβαιώσεων. Αυτού του είδους ο επαγωγικός συλλογισμός είναι συχνά απόλυτα πειστικός· η πρόβλεψη ότι ο Ήλιος θα ανατείλει αύριο στην ανατολή έχει τη μέγιστη δυνατή βεβαιότητα, αλλά ο χαρακτήρας αυτής της πρότασης δεν είναι ίδιος με εκείνον ενός θεωρήματος που έχει αποδειχθεί με αυστηρό λογικό ή μαθηματικό σκεπτικό.

Με έναν πολύ διαφορετικό τρόπο, η *μαθηματική επαγωγή* χρησιμοποιείται για να τεκμηριωθεί η ισχύς ενός μαθηματικού θεωρήματος για μια άπειρη ακολουθία περιπτώσεων, την πρώτη, τη δεύτερη, την τρίτη, κ.ο.κ. χωρίς εξαίρεση. Ας συμβολίσουμε με A μια πρόταση που περιλαμβάνει έναν τυχόντα αριθμό n. Για παράδειγμα, η A μπορεί να είναι η πρόταση «Το άθροισμα των γωνιών ενός κυρτού πολυγώνου με $n + 2$ πλευρές είναι n επί 180 μοίρες».

Ή η A' μπορεί να είναι ο ισχυρισμός, «Φέροντας n ευθείες σε ένα επίπεδο, δεν μπορούμε να χωρίσουμε το επίπεδο σε περισσότερα από 2^n μέρη». Για να αποδείξουμε ένα τέτοιο θεώρημα για *κάθε* ακέραιο n δεν αρκεί να το αποδείξουμε ξεχωριστά για τις πρώτες 10 ή 100 ή ακόμα και 1000 τιμές του n. Αυτό στην πραγματικότητα θα αντιστοιχούσε στην αντίληψη της εμπειρικής επαγωγής. Αντ' αυτού, θα πρέπει να χρησιμοποιήσουμε μια μέθοδο αυστηρά μαθηματικού και μη εμπειρικού συλλογισμού της οποίας ο χαρακτήρας θα καταδειχθεί από τις παρακάτω αποδείξεις για τα συγκεκριμένα παραδείγματα A και A'. Στην περίπτωση A, ξέρουμε ότι για $n = 1$ το πολύγωνο είναι τρίγωνο, και από τη στοιχειώδη γεωμετρία γνωρίζουμε ότι το άθροισμα των γωνιών είναι $1 \cdot 180^\circ$. Για ένα τετράπλευρο, $n = 2$, φέρουμε μια διαγώνιο που χωρίζει το τετράπλευρο σε δύο τρίγωνα. Με τον τρόπο αυτό φαίνεται αμέσως ότι το άθροισμα των γωνιών του τετραπλεύρου ισούται με το άθροισμα των γωνιών των δύο τριγώνων, το οποίο είναι $180^\circ + 180^\circ = 2 \cdot 180^\circ$. Προχωρώντας στην περίπτωση ενός πενταγώνου με 5 πλευρές, $n = 3$, το αναλύουμε σε ένα τρίγωνο συν ένα τετράπλευρο. Δεδομένου ότι το τελευταίο έχει άθροισμα γωνιών $2 \cdot 180^\circ$, όπως έχουμε μόλις αποδείξει, και δεδομένου ότι το τρίγωνο έχει άθροισμα γωνιών 180°, παίρνουμε $3 \cdot 180$ μοίρες για το 5-γωνο. Είναι πλέον φανερό ότι μπορούμε να συνεχίσουμε με τον ίδιο τρόπο επ' αόριστον, αποδεικνύοντας το θεώρημα για $n = 4$, κατόπιν για $n = 5$, και ούτω καθεξής. Κάθε πρόταση έπεται με τον ίδιο τρόπο από την προηγούμενη, οπότε το γενικό θεώρημα A μπορεί να αποδειχθεί για όλα τα n.

Ομοίως μπορούμε να αποδείξουμε το θεώρημα A'. Για $n = 1$ ισχύει κατά προφανή τρόπο, αφού μία μόνο ευθεία χωρίζει το επίπεδο σε 2 μέρη. Κατόπιν προσθέτουμε μια δεύτερη ευθεία. Καθένα από τα προηγούμενα μέρη θα χωριστεί σε δύο νέα μέρη, εκτός αν η νέα ευθεία είναι παράλληλη στην πρώτη. Σε κάθε περίπτωση, για $n = 2$ έχουμε το πολύ $4 = 2^2$ μέρη. Κατόπιν προσθέτουμε μια τρίτη ευθεία. Καθεμία από τις προηγούμενες περιοχές είτε θα χωριστεί σε δύο μέρη είτε θα μείνει ανέπαφη. Συνεπώς, το άθροισμα των μερών δεν είναι μεγαλύτερο από $2^2 \cdot 2 = 2^3$. Γνωρίζοντας ότι ισχύει αυτό, μπορούμε να αποδείξουμε με τον ίδιο τρόπο την επόμενη περίπτωση, και ούτω καθεξής επ' αόριστον.

Η ουσιαστική ιδέα στα προηγούμενα επιχειρήματα είναι να αποδείξουμε ένα γενικό θεώρημα A για όλες τις τιμές του n αποδεικνύοντας διαδοχικά μια ακολουθία ειδικών περιπτώσεων $A_1, A_2, \ldots$. Η δυνατότητα να το κάνουμε αυτό βασίζεται σε δύο πράγματα: (α) Υπάρχει μια γενική μέθοδος για να δείξουμε ότι *αν* ισχύει οποιαδήποτε πρόταση A_r τότε θα ισχύει *επίσης* η επόμενη πρόταση, A_{r+1}. (β) *Ξέρουμε* ότι η πρώτη πρόταση A_1 ισχύει. Το ότι οι δύο αυτές συνθήκες είναι ικανές για να αποδειχθεί η ισχύς *όλων* των προτάσεων $A_1, A_2, A_3, \ldots$ είναι μια λογική αρχή εξίσου θεμελιώδης για τα μαθηματικά

με τους κλασικούς κανόνες της αριστοτελικής λογικής. Τη διατυπώνουμε ως εξής:

Έστω ότι θέλουμε να αποδείξουμε μια άπειρη ακολουθία μαθηματικών προτάσεων

$$A_1, A_2, A_3, ...$$

οι οποίες συνιστούν από κοινού τη γενική πρόταση A. *Έστω ότι* (α) *μέσω κάποιου μαθηματικού επιχειρήματος δείχνουμε ότι* ***αν*** r *είναι οποιοσδήποτε ακέραιος και* ***αν*** *γνωρίζουμε ότι ισχύει ο ισχυρισμός* A_r, ***τότε*** *έπεται ότι ισχύει ο ισχυρισμός* A_{r+1}, *και ότι* (β) ***γνωρίζουμε*** *ότι η πρώτη πρόταση* A_1 *ισχύει. Τότε, όλες οι προτάσεις της ακολουθίας πρέπει να ισχύουν, και η* A *έχει αποδειχθεί.*[*]

Δεν θα διστάσουμε να αποδεχθούμε το παραπάνω, ακριβώς όπως αποδεχόμαστε τους απλούς κανόνες της συνήθους λογικής, ως μια βασική αρχή του μαθηματικού συλλογισμού. Διότι μπορούμε να αποδείξουμε την ισχύ κάθε πρότασης A_n, ξεκινώντας από τον δεδομένο ισχυρισμό (β) ότι η A_1 ισχύει, και προχωρώντας με επανειλημμένη χρήση του ισχυρισμού (α) ώστε να αποδείξουμε διαδοχικά την ισχύ των A_2, A_3, A_4, και ούτω καθεξής μέχρι να φτάσουμε στην πρόταση A_n. Συνεπώς, η αρχή της μαθηματικής επαγωγής βασίζεται στο γεγονός ότι μετά από κάθε ακέραιο r υπάρχει ένας επόμενος, $r+1$, και ότι μπορούμε να φτάσουμε σε οποιονδήποτε επιθυμητό ακέραιο n με πεπερασμένο πλήθος τέτοιων βημάτων, ξεκινώντας από τον ακέραιο 1.

Συχνά, η αρχή της μαθηματικής επαγωγής εφαρμόζεται χωρίς ρητή αναφορά, ή απλά υποδεικνύεται από ένα πρόχειρο «κ.λπ.» ή «και ούτω καθεξής». Αυτό συμβαίνει ιδιαίτερα συχνά στη στοιχειώδη επαγωγή. Αλλά η ρητή χρήση ενός επαγωγικού σκεπτικού είναι αναντικατάστατη σε πιο περίτεχνες αποδείξεις. Ας δούμε μερικά παραδείγματα απλού αλλά όχι εντελώς τετριμμένου χαρακτήρα.

2. Η αριθμητική πρόοδος

Για κάθε τιμή του n, *το άθροισμα* $1 + 2 + 3 + \cdots + n$ *των πρώτων* n *ακεραίων ισούται με* $\dfrac{n(n+1)}{2}$. Για να αποδείξουμε αυτό το θεώρημα με μαθηματική επαγωγή, θα πρέπει να δείξουμε ότι για κάθε n ο ισχυρισμός A_n:

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \tag{1}$$

[*] Σ.τ.Ε.: Η μαθηματική επαγωγή παρομοιάζεται διαισθητικά με ένα παιχνίδι ντόμινο. Αν ρίξουμε το πρώτο ντόμινο (πρόταση A_1), και αν κάθε ντόμινο ρίχνει το επόμενο (η ισχύς της πρότασης A_r οδηγεί στην ισχύ της A_{r+1}, τότε όλα τα ντόμινο θα καταλήξουν πεσμένα (όλες οι προτάσεις θα ισχύουν).

ισχύει. (α) Παρατηρούμε ότι αν r είναι ένας ακέραιος και αν γνωρίζουμε ότι ισχύει η πρόταση A_r, δηλαδή αν γνωρίζουμε ότι

$$1 + 2 + 3 + \cdots + r = \frac{r(r+1)}{2},$$

τότε προσθέτοντας τον αριθμό $(r+1)$ και στα δύο μέλη αυτής της εξίσωσης παίρνουμε την εξίσωση

$$\begin{aligned} 1 + 2 + 3 + \cdots + r + (r+1) &= \frac{r(r+1)}{2} + (r+1) \\ &= \frac{r(r+1) + 2(r+1)}{2} = \frac{(r+1)(r+2)}{2}, \end{aligned}$$

που είναι ακριβώς η πρόταση A_{r+1}. (β) Η πρόταση A_1 ισχύει κατά προφανή τρόπο, διότι $1 = \dfrac{1 \cdot 2}{2}$. Συνεπώς, βάσει της αρχής της μαθηματικής επαγωγής, η πρόταση A_n ισχύει για κάθε n, όπως θέλαμε να αποδείξουμε.

Συνήθως για να αποδειχθεί αυτό γράφουμε το άθροισμα $1 + 2 + 3 + \cdots + n$ σε δύο μορφές:

$$S_n = 1 + 2 + \cdots + (n-1) + n$$

και

$$S_n = n + (n-1) + \cdots + 2 + 1.$$

Προσθέτοντας, βλέπουμε ότι κάθε ζεύγος αριθμών στην ίδια στήλη δίνει άθροισμα $n + 1$, και δεδομένου ότι υπάρχουν συνολικά n στήλες, έπεται ότι

$$2S_n = n(n+1),$$

οπότε το ζητούμενο αποτέλεσμα έχει αποδειχθεί.

Από την (1) μπορούμε να συναγάγουμε αμέσως τον τύπο για το άθροισμα των πρώτων $(n+1)$ όρων οποιασδήποτε *αριθμητικής προόδου*,

$$P_n = a + (a+d) + (a+2d) + \cdots + (a+nd) = \frac{(n+1)(2a+nd)}{2}. \quad (2)$$

Διότι

$$\begin{aligned} P_n = (n+1)a + (1 + 2 + \cdots + n)d &= (n+1)a + \frac{n(n+1)d}{2} \\ &= \frac{2(n+1)a + n(n+1)d}{2} = \frac{(n+1)(2a+nd)}{2}. \end{aligned}$$

Για την περίπτωση $a = 0$, $d = 1$, αυτό είναι ισοδύναμο της (1).

3. Η γεωμετρική πρόοδος

Με παρόμοιο τρόπο μπορούμε να πραγματευτούμε τη γενική γεωμετρική πρόοδο. Θα αποδείξουμε ότι για κάθε τιμή του n

$$G_n = a + aq + aq^2 + \cdots + aq^n = a\frac{1-q^{n+1}}{1-q}. \tag{3}$$

(Υποθέτουμε ότι $q \neq 1$, διότι διαφορετικά το δεξί μέλος της (3) δεν έχει νόημα.)

Ο ισχυρισμός ισχύει σίγουρα για $n = 1$, διότι σε αυτή την περίπτωση δηλώνει ότι

$$G_1 = a + aq = \frac{a(1-q^2)}{1-q} = \frac{a(1+q)(1-q)}{(1-q)} = a(1+q).$$

Και *αν* δεχθούμε ότι

$$G_r = a + aq + \cdots + aq^r = a\frac{1-q^{r+1}}{1-q},$$

τότε βρίσκουμε ως επακόλουθο ότι

$$\begin{aligned} G_{r+1} &= (a + aq + \cdots + aq^r) + aq^{r+1} = G_r + aq^{r+1} = a\frac{1-q^{r+1}}{1-q} + aq^{r+1} \\ &= a\frac{(1-q^{r+1}) + q^{r+1}(1-q)}{1-q} = a\frac{1-q^{r+1}+q^{r+1}-q^{r+2}}{1-q} = a\frac{1-q^{r+2}}{1-q}, \end{aligned}$$

το οποίο όμως είναι ακριβώς ο ισχυρισμός (3) για την περίπτωση $n = r+1$, οπότε η απόδειξη έχει ολοκληρωθεί.

Στα εισαγωγικά εγχειρίδια, η συνήθης απόδειξη έχει ως εξής. Θέτουμε

$$G_n = a + aq + \cdots + aq^n,$$

και πολλαπλασιάζουμε και τα δύο μέλη αυτής της εξίσωσης επί q, οπότε προκύπτει ότι

$$qG_n = aq + aq^2 + \cdots + aq^{n+1}.$$

Στη συνέχεια αφαιρούμε κατά μέλη αυτή την εξίσωση από την προηγούμενη, οπότε προκύπτει ότι

$$\begin{aligned} G_n - qG_n &= a - aq^{n+1}, \\ (1-q)G_n &= a(1-q^{n+1}), \\ G_n &= a\frac{1-q^{n+1}}{1-q}. \end{aligned}$$

4. Το άθροισμα των πρώτων n τετραγώνων

Μια ακόμα ενδιαφέρουσα εφαρμογή της αρχής της μαθηματικής επαγωγής αφορά το άθροισμα των πρώτων n τετραγώνων. Με απευθείας δοκιμή, μπορεί κανείς να διαπιστώσει ότι, τουλάχιστον για μικρές τιμές του n,

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}, \tag{4}$$

και θα μπορούσε ίσως να *εικάσει* ότι αυτός ο αξιοσημείωτος τύπος ισχύει για *όλους τους ακεραίους* n. Για να το *αποδείξουμε* αυτό, θα χρησιμοποιήσουμε και πάλι την αρχή της μαθηματικής επαγωγής. Ξεκινάμε παρατηρώντας ότι *αν* ο ισχυρισμός A_n, ο οποίος στην προκειμένη περίπτωση είναι η εξίσωση (4), ισχύει για την περίπτωση $n = r$, οπότε

$$1^2 + 2^2 + 3^2 + \cdots + r^2 = \frac{r(r+1)(2r+1)}{6},$$

τότε προσθέτοντας και στα δύο μέλη αυτής της εξίσωσης το $(r+1)^2$ βρίσκουμε ότι

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \cdots + r^2 + (r+1)^2 &= \frac{r(r+1)(2r+1)}{6} + (r+1)^2 \\ &= \frac{r(r+1)(2r+1) + 6(r+1)^2}{6} = \frac{(r+1)[r(2r+1) + 6(r+1)]}{6} \\ &= \frac{(r+1)(2r^2+7r+6)}{6} = \frac{(r+1)(r+2)(2r+3)}{6}, \end{aligned}$$

που είναι ακριβώς ο ισχυρισμός A_{r+1} σε αυτή την περίπτωση, διότι προκύπτει με αντικατάσταση του n με $r+1$ στην (4). Για να ολοκληρώσουμε την απόδειξη, αρκεί να παρατηρήσουμε ότι ο ισχυρισμός A_1, δηλαδή στην προκειμένη περίπτωση η εξίσωση

$$1^2 = \frac{1(1+1)(2+1)}{6},$$

ισχύει κατά προφανή τρόπο. Συνεπώς, η εξίσωση (4) ισχύει για κάθε n.

Παρόμοιοι τύποι μπορούν να βρεθούν για ανώτερες δυνάμεις των ακεραίων, $1^k + 2^k + 3^k + \cdots + n^k$, όπου k είναι οποιοσδήποτε θετικός ακέραιος. Ο αναγνώστης μπορεί να αποδείξει με μαθηματική επαγωγή ως άσκηση ότι

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2. \tag{5}$$

Θα πρέπει να σημειωθεί ότι παρότι η αρχή της μαθηματικής επαγωγής αρκεί για να *αποδειχθεί* ο τύπος (5) άπαξ και έχουμε αυτό τον τύπο σε γραπτή μορφή,

η απόδειξη δεν μας δίνει καμία ένδειξη για το πώς φτάσαμε κατ' αρχάς σε αυτό τον τύπο· για ποιον ακριβώς λόγο θα έπρεπε να εικάσουμε ως έκφραση για το άθροισμα των πρώτων n κύβων την $[n(n+1)/2]^2$, αντί της $[n(n+1)/3]^2$ ή της $(19n^2-41n+24)/2$ ή οποιασδήποτε από τις απειράριθμες εκφράσεις τέτοιου είδους που θα μπορούσαμε να έχουμε θεωρήσει. Το γεγονός ότι η απόδειξη ενός θεωρήματος συνίσταται στην εφαρμογή ορισμένων απλών κανόνων λογικής δεν εξαλείφει το δημιουργικό στοιχείο στα μαθηματικά, το οποίο έγκειται στην επιλογή των δυνατοτήτων που πρέπει να εξεταστούν. Το ερώτημα περί της προέλευσης της *υπόθεσης* (5) ανήκει σε μια επικράτεια για την οποία δεν μπορεί να δοθεί κανένας πολύ γενικός κανόνας· ο πειραματισμός, η αναλογία, και η εποικοδομητική διαίσθηση παίζουν τον ρόλο τους εδώ. Άπαξ όμως και διατυπωθεί η σωστή υπόθεση, η αρχή της μαθηματικής επαγωγής συχνά αρκεί για να δώσει την απόδειξη. Επειδή μια τέτοια απόδειξη δεν μας δίνει κανένα ίχνος σχετικά με την πράξη της ανακάλυψης, θα μπορούσε να αποκαλείται πιο εύστοχα *επαλήθευση*.

*5. Μια σημαντική ανισότητα

Σε ένα από τα επόμενα κεφάλαια, θα μας φανεί χρήσιμη η ανισότητα

$$(1+p)^n \geq 1+np, \tag{6}$$

η οποία ισχύει για κάθε αριθμό $p > -1$ και για κάθε θετικό ακέραιο n. (Χάριν της γενικότητας, προεξοφλούμε εδώ τη χρήση αρνητικών και μη ακέραιων αριθμών επιτρέποντας στο p να είναι οποιοσδήποτε αριθμός μεγαλύτερος του -1. Η απόδειξη για τη γενική περίπτωση είναι ακριβώς η ίδια με την περίπτωση όπου το p είναι θετικός ακέραιος.) Θα χρησιμοποιήσουμε και πάλι μαθηματική επαγωγή.

(α) *Αν* ισχύει ότι $(1+p)^r \geq 1+rp$, τότε πολλαπλασιάζοντας και τα δύο μέλη αυτής της ανισότητας με τον θετικό αριθμό $1+p$, έχουμε ότι

$$(1+p)^{r+1} \geq 1+rp+p+rp^2.$$

Αν παραλείψουμε τον θετικό όρο rp^2 η ανισότητα αυτή μπορεί μόνο να ενισχυθεί, οπότε

$$(1+p)^{r+1} \geq 1+(r+1)p,$$

πράγμα που δείχνει ότι η ανισότητα (6) θα ισχύει επίσης για τον επόμενο ακέραιο, $r+1$. (β) Ισχύει κατά προφανή τρόπο ότι $(1+p)^1 \geq 1+p$. Επομένως, η απόδειξη ότι η (6) ισχύει για κάθε n έχει ολοκληρωθεί. Ο περιορισμός σε αριθμούς $p > -1$ είναι απαραίτητος. Αν $p < -1$, τότε το $1+p$ είναι αρνητικό και το σκεπτικό στο σκέλος (α) καταρρέει, διότι αν και τα δύο μέλη μιας ανισότητας πολλαπλασιαστούν με μια αρνητική ποσότητα, η φορά της ανισότητας

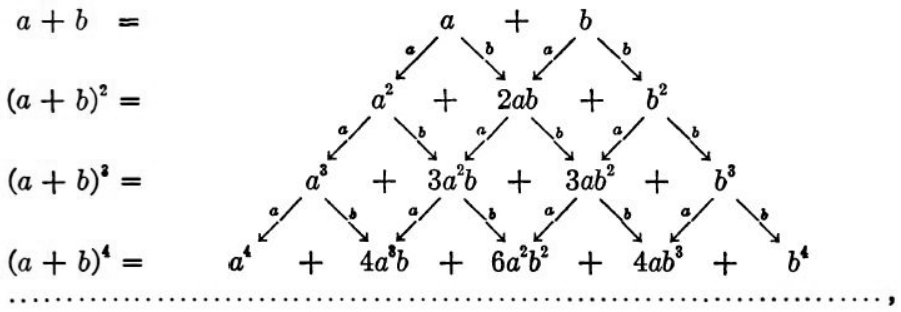
αντιστρέφεται. (Για παράδειγμα, αν πολλαπλασιάσουμε και τα δύο μέλη της ανισότητας $3 > 2$ επί -1, παίρνουμε $-3 > -2$, το οποίο είναι ψευδές.)

*6. Το διωνυμικό θεώρημα

Συχνά είναι σημαντικό να έχουμε μια συγκεκριμένη έκφραση για την n-οστή δύναμη ενός διωνύμου, $(a+b)^n$. Με απευθείας υπολογισμό βρίσκουμε ότι

$$\begin{aligned}
&\text{για } n=1,\ (a+b)^1 = a+b,\\
&\text{για } n=2,\ (a+b)^2 = (a+b)(a+b) = a(a+b)+b(a+b)\\
&\qquad\qquad = a^2+2ab+b^2,\\
&\text{για } n=3,\ (a+b)^3 = (a+b)(a+b)^2 = a(a^2+2ab+b^2)\\
&\qquad\qquad + b(a^2+2ab+b^2) = a^3+3a^2b+3ab^2+b^3,
\end{aligned}$$

και ούτω καθεξής. Ποιος γενικός νόμος σχηματισμού βρίσκεται πίσω από τις λέξεις «και ούτω καθεξής»; Ας εξετάσουμε τη διαδικασία με την οποία υπολογίστηκε η δύναμη $(a+b)^2$. Δεδομένου ότι $(a+b)^2 = (a+b)(a+b)$, για να πάρουμε την έκφραση για το $(a+b)^2$ πολλαπλασιάσαμε κάθε όρο στην έκφραση $a+b$ με το a, κατόπιν με το b, και προσθέσαμε. Την ίδια διαδικασία χρησιμοποιήσαμε για να υπολογίσουμε το $(a+b)^3 = (a+b)(a+b)^2$. Συνεχίζοντας με τον ίδιο τρόπο μπορούμε να υπολογίσουμε το $(a+b)^4$, το $(a+b)^5$, και ούτω καθεξής επ' αόριστον. Για να πάρουμε την έκφραση για το $(a+b)^n$ θα πολλαπλασιάσουμε κάθε όρο της σχέσης που έχει προκύψει προηγουμένως για το $(a+b)^{n-1}$ με το a, κατόπιν με το b, και θα προσθέσουμε. Με τον τρόπο αυτό προκύπτει το ακόλουθο διάγραμμα:



το οποίο μας δίνει αμέσως τον γενικό κανόνα για τον σχηματισμό των συντελεστών στο ανάπτυγμα για το $(a+b)^n$. Κατασκευάζουμε έναν τριγωνικό πίνακα αριθμών, ξεκινώντας από τους συντελεστές 1, 1 του $a+b$, για τον οποίο ισχύει ότι κάθε αριθμός στο τρίγωνο είναι το άθροισμα των δύο αριθμών σε καθεμία από τις πλευρές του στην προηγούμενη γραμμή. Ο πίνακας αυτός είναι γνωστός ως *τρίγωνο του Pascal*.

$$
\begin{array}{ccccccccccccccc}
 & & & & & & 1 & & 1 & & & & & & \\
 & & & & & 1 & & 2 & & 1 & & & & & \\
 & & & & 1 & & 3 & & 3 & & 1 & & & & \\
 & & & 1 & & 4 & & 6 & & 4 & & 1 & & & \\
 & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & \\
1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1
\end{array}
$$

.....

Η n-οστή γραμμή αυτού του πίνακα δίνει τους συντελεστές στο ανάπτυγμα του $(a+b)^n$ κατά φθίνουσες δυνάμεις του a και αύξουσες δυνάμεις του b· συνεπώς,

$$(a+b)^7 = a^7 + 7a^6b + 21a^5b^2 + 35a^4b^3 + 35a^3b^4 + 21a^2b^5 + 7ab^6 + b^7.$$

Χρησιμοποιώντας έναν συνοπτικό συμβολισμό με κάτω και άνω δείκτες, μπορούμε να γράφουμε τους αριθμούς στην n-οστή γραμμή του τριγώνου του Pascal ως εξής:

$$C_0^n = 1, C_1^n, C_2^n, C_3^n, \cdots, C_{n-1}^n, C_n^n = 1.$$

Συνεπώς, ο γενικός τύπος για το $(a+b)^n$ μπορεί να γραφτεί στη μορφή

$$(a+b)^n = a^n + C_1^n a^{n-1}b + C_2^n a^{n-2}b^2 + \cdots + C_{n-1}^n ab^{n-1} + b^n. \qquad (7)$$

Σύμφωνα με τον νόμο του σχηματισμού του τριγώνου του Pascal, έχουμε

$$C_i^n = C_{i-1}^{n-1} + C_i^{n-1}. \qquad (8)$$

Ως άσκηση, ο έμπειρος αναγνώστης μπορεί χρησιμοποιώντας αυτή τη σχέση, σε συνδυασμό με το γεγονός ότι $C_0^1 = C_1^1 = 1$, να δείξει με μαθηματική επαγωγή ότι

$$C_i^n = \frac{n(n-1)(n-2)\cdots(n-i+1)}{1\cdot 2\cdot 3\cdots i} = \frac{n!}{i!(n-i)!}. \qquad (9)$$

(Για κάθε θετικό ακέραιο n, το σύμβολο $n!$ (που διαβάζεται «n παραγοντικό») δηλώνει το γινόμενο των πρώτων n ακεραίων: $n! = 1\cdot 2\cdot 3\cdots n$. Μας διευκολύνει επίσης να ορίσουμε $0! = 1$, οπότε η (9) ισχύει για $i = 0$ και για $i = n$.) Αυτός ο συγκεκριμένος τύπος για τους συντελεστές στο διωνυμικό ανάπτυγμα ονομάζεται μερικές φορές *διωνυμικό θεώρημα*. (Βλ. επίσης σελ. 516.)

Ασκήσεις: Αποδείξτε με μαθηματική επαγωγή:

1) $\dfrac{1}{1\cdot 2} + \dfrac{1}{2\cdot 3} + \cdots + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1}$.

2) $\dfrac{1}{2} + \dfrac{2}{2^2} + \dfrac{3}{2^3} + \cdots + \dfrac{n}{2^n} = 2 - \dfrac{n+2}{2^n}$.

*3) $1 + 2q + 3q^2 + \cdots + nq^{n-1} = \dfrac{1 - (n+1)q^n + nq^{n+1}}{(1-q)^2}$.

*4) $(1+q)(1+q^2)(1+q^4)\cdots(1+q^{2^n}) = \dfrac{1-q^{2^{n+1}}}{1-q}$.

Βρείτε το άθροισμα των παρακάτω γεωμετρικών προόδων:

5) $\dfrac{1}{1+x^2} + \dfrac{1}{(1+x^2)^2} + \cdots + \dfrac{1}{(1+x^2)^n}$.

6) $1 + \dfrac{x}{1+x^2} + \dfrac{x^2}{(1+x^2)^2} + \cdots + \dfrac{x^n}{(1+x^2)^n}$.

7) $\dfrac{x^2-y^2}{x^2+y^2} + \left(\dfrac{x^2-y^2}{x^2+y^2}\right)^2 + \cdots + \left(\dfrac{x^2-y^2}{x^2+y^2}\right)^n$.

Χρησιμοποιώντας τους τύπους (4) και (5) αποδείξτε τα εξής:

*8) $1^2 + 3^2 + \cdots + (2n+1)^2 = \dfrac{(n+1)(2n+1)(2n+3)}{3}$.

*9) $1^3 + 3^3 + \cdots + (2n+1)^3 = (n+1)^2(2n^2+4n+1)$.

10) Αποδείξτε τα ίδια αποτελέσματα απευθείας με μαθηματική επαγωγή.

*7. Επιπλέον σχόλια για τη μαθηματική επαγωγή

Η αρχή της μαθηματικής επαγωγής μπορεί να γενικευτεί ελαφρά ως εξής: «Αν δοθεί μια ακολουθία προτάσεων $A_s, A_{s+1}, A_{s+2}, \ldots$, όπου s είναι κάποιος θετικός ακέραιος, και αν

(α) για κάθε τιμή του $r \geq s$, η ισχύς της A_{r+1} έπεται από την ισχύ της A_r, και

(β) γνωρίζουμε ότι η A_s ισχύει,

τότε όλες οι προτάσεις $A_s, A_{s+1}, A_{s+2}, \ldots$ ισχύουν· δηλαδή, η A_n ισχύει για όλα τα $n \geq s$.» Στην περίπτωση αυτή ισχύει ακριβώς το ίδιο σκεπτικό που χρησιμοποιήσαμε για να αποδείξουμε την ισχύ της συνήθους αρχής της μαθηματικής επαγωγής, όπου η ακολουθία $1, 2, 3 \ldots$ έχει αντικατασταθεί από την παρόμοια ακολουθία $s, s+1, s+2, s+3, \ldots$. Χρησιμοποιώντας την αρχή σε αυτή τη μορφή, μπορούμε να ενισχύσουμε κάπως την ανισότητα της σελ. 17 διαγράφοντας τη δυνατότητα του συμβόλου «=». Λέμε λοιπόν ότι: *Για κάθε $p \neq 0$ και > -1 και για κάθε ακέραιο $n \geq 2$,*

$$(1+p)^n > 1 + np. \tag{10}$$

Η απόδειξη αφήνεται για τον αναγνώστη.

Στενά συνδεδεμένη με την αρχή της μαθηματικής επαγωγής είναι η «αρχή του ελάχιστου ακεραίου», σύμφωνα με την οποία *κάθε μη κενό σύνολο C θετικών ακεραίων έχει ένα ελάχιστο μέλος.* Ένα σύνολο είναι κενό αν δεν έχει κανένα μέλος, π.χ., το σύνολο των ευθύγραμμων κύκλων ή το σύνολο των ακεραίων n για τους οποίους ισχύει ότι $n > n$. Για προφανείς λόγους, εξαιρούμε τέτοια σύνολα στη διατύπωση της αρχής. Το σύνολο C μπορεί να είναι πεπερασμένο, όπως το σύνολο $1, 2, 3, 4, 5$, ή άπειρο, όπως το σύνολο όλων των άρτιων αριθμών $2, 4, 6, 8, 10, \ldots$. Κάθε μη κενό σύνολο C θα πρέπει να περιέχει τουλάχιστον έναν ακέραιο, έστω n, και ο μικρότερος από τους ακεραίους $1, 2, 3, \ldots, n$ που ανήκει στο C θα είναι ο ελάχιστος ακέραιος στο C.

Ο μόνος τρόπος να συνειδητοποιήσουμε τη σημασία αυτής της αρχής είναι να παρατηρήσουμε ότι *δεν* ισχύει για κάθε σύνολο C αριθμών που δεν είναι ακέραιοι· για παράδειγμα, το σύνολο των θετικών κλασμάτων $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$ δεν περιέχει ένα ελάχιστο μέλος.

Από τη σκοπιά της λογικής, είναι ενδιαφέρον να παρατηρήσουμε ότι η αρχή του ελάχιστου ακεραίου μπορεί να χρησιμοποιηθεί για να *αποδειχθεί* η αρχή της μαθηματικής επαγωγής ως θεώρημα. Για τον σκοπό αυτό, ας θεωρήσουμε οποιαδήποτε ακολουθία προτάσεων $A_1, A_2, A_3, \ldots$ για την οποία ισχύει ότι

(α) Για κάθε θετικό ακέραιο r, η ισχύς της A_{r+1} έπεται από εκείνη της A_r.

(β) Γνωρίζουμε ότι η A_1 ισχύει.

Θα δείξουμε πως η υπόθεση ότι οποιαδήποτε από τις A δεν ισχύει είναι αβάσιμη. Διότι αν έστω και μία από τις A δεν ίσχυε, το σύνολο C *όλων* των θετικών ακεραίων n για τους οποίους η A_n δεν ισχύει θα ήταν μη κενό. Βάσει της αρχής του ελάχιστου ακεραίου, το C θα περιείχε έναν ελάχιστο ακέραιο, p, ο οποίος θα πρέπει να είναι > 1 λόγω του (β). Επομένως, η A_p δεν θα ίσχυε, αλλά η A_{p-1} θα ίσχυε. Αυτό αντιβαίνει προς το (α).

Για άλλη μια φορά υπογραμμίζουμε ότι η αρχή της μαθηματικής επαγωγής είναι εντελώς διαφορετική από την εμπειρική επαγωγή στις φυσικές επιστήμες. Η επιβεβαίωση ενός γενικού νόμου σε οποιοδήποτε πεπερασμένο πλήθος περιπτώσεων, οσοδήποτε μεγάλο, δεν μπορεί να αποτελέσει μια απόδειξη για τον νόμο με την αυστηρή μαθηματική έννοια του όρου, ακόμα κι αν αυτή τη στιγμή δεν υπάρχει καμία γνωστή εξαίρεση. Ένας τέτοιος νόμος θα παρέμενε απλά μια πολύ εύλογη *υπόθεση*, υποκείμενη σε τροποποίηση βάσει των αποτελεσμάτων της μελλοντικής εμπειρίας. Στα μαθηματικά, ένας νόμος ή ένα θεώρημα αποδεικνύεται μόνο αν μπορεί να δειχθεί ότι αποτελεί αναγκαία λογική συνέπεια ορισμένων παραδοχών οι οποίες αναγνωρίζονται ως έγκυρες. Υπάρχουν πολλά παραδείγματα μαθηματικών προτάσεων που έχουν επαληθευτεί σε κάθε συγκεκριμένη περίπτωση που έχει εξεταστεί μέχρι στιγμής, αλλά που δεν έχει ακόμα αποδειχθεί ότι ισχύουν εν γένει (βλ. σελ. 33 για ένα παράδειγμα). Ίσως κανείς να *υποψιάζεται* ότι ένα θεώρημα ισχύει σε πλήρη γενικότητα παρατηρώντας την ισχύ του σε κάποιον αριθμό παραδειγμάτων· στην περίπτωση αυτή μπορεί να επιχειρήσει να το *αποδείξει* μέσω μαθηματικής επαγωγής. Αν η απόπειρα τελεσφορήσει, αποδεικνύεται ότι το θεώρημα ισχύει· αν η προσπάθεια αποτύχει, το θεώρημα μπορεί να ισχύει ή να μην ισχύει, και ίσως κάποια μέρα να αποδειχθεί ή να καταρριφθεί με άλλες μεθόδους.

Όταν χρησιμοποιεί κανείς την αρχή της μαθηματικής επαγωγής, θα πρέπει να είναι πάντοτε σίγουρος ότι οι συνθήκες (α) και (β) πραγματικά ικανοποιούνται. Αν αμεληθεί αυτή η προφύλαξη, είναι πιθανόν να οδηγηθεί κανείς σε παραλογισμούς όπως ο παρακάτω, για τον οποίο ο αναγνώστης καλείται να ανακαλύψει την ανακολουθία. Θα «αποδείξουμε» ότι *οποιοιδήποτε δύο θετικοί ακέραιοι είναι ίσοι*· για παράδειγμα, ότι $5 = 10$.

Αρχικά ένας ορισμός: αν a και b είναι δύο άνισοι θετικοί ακέραιοι, ορίζουμε ότι

το $\max(a, b)$ είναι το μεγαλύτερο μεταξύ των a και b· αν $a = b$ θέτουμε $\max(a, b) = a = b$. Επομένως, $\max(3, 5) = \max(5, 3) = 5$, ενώ $\max(4, 4) = 4$. Τώρα έστω A_n η πρόταση, «Αν a και b είναι οποιοιδήποτε δύο θετικοί ακέραιοι τέτοιοι ώστε $\max(a, b) = n$, τότε $a = b$».

(α) Ας υποθέσουμε ότι η A_r ισχύει. Έστω a και b οποιοιδήποτε δύο θετικοί ακέραιοι τέτοιοι ώστε $\max(a, b) = r + 1$. Αν θεωρήσουμε τους δύο ακεραίους

$$\alpha = a - 1$$
$$\beta = b - 1,$$

τότε $\max(\alpha, \beta) = r$. Επομένως, $\alpha = \beta$, διότι υποθέτουμε ότι η A_r ισχύει. Έπεται ότι $a = b$· συνεπώς, η A_{r+1} ισχύει.

(β) Η A_1 ισχύει κατά προφανή τρόπο, διότι αν $\max(a, b) = 1$, τότε δεδομένου ότι τα a και b είναι εξ υποθέσεως θετικοί ακέραιοι, θα πρέπει να είναι αμφότερα ίσα με 1. Επομένως, βάσει της μαθηματικής επαγωγής, η A_n ισχύει για κάθε n.

Τώρα, αν a και b είναι οποιοιδήποτε δύο θετικοί ακέραιοι, συμβολίζουμε το $\max(a, b)$ με r. Δεδομένου ότι έχουμε δείξει πως η A_n ισχύει για κάθε n, εν προκειμένω η A_r ισχύει. Συνεπώς, $a = b$.

ΣΥΜΠΛΗΡΩΜΑ ΣΤΟ ΚΕΦΑΛΑΙΟ Ι

Η ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

ΕΙΣΑΓΩΓΗ

Αν και οι ακέραιοι έχουν σταδιακά χάσει τη σύνδεσή τους με τη δεισιδαιμονία και τον μυστικισμό, το ενδιαφέρον των ανθρώπων των μαθηματικών για αυτούς δεν έχει υποχωρήσει ποτέ. Ο Ευκλείδης (περί το 300 π.Χ.), του οποίου η φήμη οφείλεται στο τμήμα των *Στοιχείων* του το οποίο αποτελεί το θεμέλιο της γεωμετρίας που διδάσκεται στο γυμνάσιο και στο λύκειο, φαίνεται πως έχει κάνει πρωτότυπες συνεισφορές στη θεωρία αριθμών, ενώ η γεωμετρία του ήταν εν πολλοίς μια σύνθεση προγενέστερων αποτελεσμάτων. Ο Διόφαντος ο Αλεξανδρεύς (περί το 275 μ.Χ.), ένας από τους πρώτους αλγεβριστές, άφησε το σημάδι του στη θεωρία αριθμών. Ο Pierre de Fermat (1601-1665), δικαστής από την Τουλούζη, και ένας από τους μεγαλύτερους μαθηματικούς της εποχής του, εγκαινίασε τη σύγχρονη εργασία σε αυτό το πεδίο. Ο Euler (1707-1783), ο πιο παραγωγικός μαθηματικός όλων των εποχών, συμπεριέλαβε στις έρευνές του σημαντικό έργο πάνω στη θεωρία αριθμών. Στη λίστα αυτή μπορούν να προστεθούν πολλά εξέχοντα ονόματα στα χρονικά των μαθηματικών – Legendre, Dirichlet, Riemann. Ο Gauss (1777-1855), ο κορυφαίος μαθηματικός της σύγχρονης εποχής, ο οποίος μελέτησε πολλούς διαφορετικούς κλάδους των μαθηματικών, λέγεται ότι είχε εκφράσει τη γνώμη του για τη θεωρία αριθμών με το εξής σχόλιο: «Τα μαθηματικά είναι η βασίλισσα των επιστημών, και η θεωρία αριθμών είναι η βασίλισσα των μαθηματικών».

§1. ΟΙ ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ

1. Θεμελιώδη στοιχεία

Οι περισσότερες προτάσεις στη θεωρία αριθμών, όπως και στα μαθηματικά ως σύνολο, δεν αφορούν ένα μόνο αντικείμενο –τον αριθμό 5 ή τον αριθμό 32–, αλλά μια ολόκληρη κλάση αντικειμένων που έχουν κάποια κοινή ιδιότητα, όπως την κλάση όλων των άρτιων ακεραίων,

$$2, 4, 6, 8, \dots ,$$

ή τη κλάση όλων των ακεραίων που διαιρούνται με το 3,

$$3, 6, 9, 12, \dots,$$

ή την κλάση όλων των τετραγώνων ακεραίων,

$$1, 4, 9, 16, \dots,$$

και ούτω καθεξής.

Θεμελιώδους σημασίας στη θεωρία αριθμών είναι η κλάση όλων των *πρώτων αριθμών*. Οι περισσότεροι ακέραιοι μπορούν να αναλυθούν σε μικρότερους παράγοντες: $10 = 2 \cdot 5$, $111 = 3 \cdot 37$, $144 = 3 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2$, κ.λπ. Οι αριθμοί που δεν μπορούν να αναλυθούν με αυτό τον τρόπο ονομάζονται πρώτοι αριθμοί, ή απλά πρώτοι. Ακριβέστερα, *πρώτος αριθμός είναι ένας ακέραιος p, μεγαλύτερος του ένα, που δεν έχει κανέναν παράγοντα εκτός από τον εαυτό του και το ένα*. (Λέμε ότι ένας *ακέραιος* a είναι *παράγοντας* ή *διαιρέτης* ενός *ακεραίου* b αν υπάρχει κάποιος *ακέραιος* c τέτοιος ώστε $b = ac$.) Οι αριθμοί $2, 3, 5, 7, 11, 13, 17, \dots$ είναι πρώτοι, ενώ ο 12, για παράδειγμα, δεν είναι, διότι $12 = 3 \cdot 4$. Η σημασία της κλάσης των πρώτων οφείλεται στο γεγονός ότι *κάθε* ακέραιος μπορεί να εκφραστεί ως *γινόμενο πρώτων*: αν ένας αριθμός δεν είναι ο ίδιος πρώτος, μπορεί να παραγοντοποιηθεί διαδοχικά μέχρις ότου όλοι οι παράγοντες να είναι πρώτοι· συνεπώς, $360 = 3 \cdot 120 = 3 \cdot 30 \cdot 4 = 3 \cdot 3 \cdot 10 \cdot 2 \cdot 2 = 3 \cdot 3 \cdot 5 \cdot 2 \cdot 2 \cdot 2 = 2^3 \cdot 3^2 \cdot 5$. Ένας ακέραιος (διάφορος του 0 ή του 1) ο οποίος δεν είναι πρώτος χαρακτηρίζεται ως *σύνθετος*.

Ένα από τα πρώτα ερωτήματα που ανακύπτουν όσον αφορά την κλάση των πρώτων είναι αν υπάρχει μόνο ένα πεπερασμένο πλήθος διαφορετικών πρώτων ή αν η κλάση των πρώτων περιλαμβάνει άπειρα το πλήθος μέλη, όπως η κλάση όλων των ακεραίων, της οποίας αποτελεί τμήμα. Η απάντηση είναι: *Υπάρχουν άπειροι το πλήθος πρώτοι*.

Η απόδειξη της απειρίας της κλάσης των πρώτων από τον Ευκλείδη παραμένει υπόδειγμα μαθηματικής συλλογιστικής. Ακολουθεί την «έμμεση μέθοδο». Ξεκινάμε με τη δοκιμαστική παραδοχή ότι το θεώρημα δεν ισχύει. Αυτό σημαίνει ότι θα υπήρχε μόνο πεπερασμένο πλήθος πρώτων, ίσως ένα τεράστιο πλήθος –λόγου χάριν, ένα δισεκατομμύριο– ή, εκπεφρασμένο με γενικό και μη δεσμευτικό τρόπο, n. Χρησιμοποιώντας τον συμβολισμό με κάτω δείκτες, μπορούμε να συμβολίσουμε αυτούς τους πρώτους με $p_1, p_2, \dots, p_n$. Κάθε άλλος αριθμός θα είναι σύνθετος, και θα πρέπει να διαιρείται από έναν τουλάχιστον από τους πρώτους $p_1, p_2, \dots, p_n$. Στη συνέχεια παράγουμε ένα άτοπο (μια αντίφαση) κατασκευάζοντας έναν αριθμό A ο οποίος διαφέρει από καθέναν από τους πρώτους $p_1, p_2, \dots, p_n$ διότι είναι μεγαλύτερος από καθέναν από αυτούς, και ο οποίος εντούτοις δεν διαιρείται από κανέναν από αυτούς. Ο αριθμός αυτός είναι ο

$$A = p_1 p_2 \dots p_n + 1,$$

δηλαδή, 1 συν το γινόμενο των αριθμών που υποτίθεται ότι είναι όλοι οι πρώτοι. Ο αριθμός A είναι μεγαλύτερος από καθέναν από τους p και επομένως θα πρέπει να είναι σύνθετος. Αλλά όταν το A διαιρεθεί με τον p_1, ή με τον p_2, κ.λπ., αφήνει πάντα υπόλοιπο 1· επομένως, ο A δεν έχει ως διαιρέτη κανέναν από τους p. Δεδομένου ότι η αρχική μας παραδοχή ότι υπάρχει μόνο πεπερασμένο πλήθος πρώτων οδηγεί σε αυτό το άτοπο, βλέπουμε ότι η παραδοχή αυτή είναι άτοπη, και συνεπώς θα πρέπει να ισχύει το αντίθετο. Επομένως, το θεώρημα έχει αποδειχθεί.

Παρότι η απόδειξη αυτή είναι έμμεση, μπορεί να τροποποιηθεί εύκολα ώστε να δώσει μια μέθοδο για την κατασκευή, τουλάχιστον στη θεωρία, μιας άπειρης ακολουθίας πρώτων. Ξεκινώντας από οποιονδήποτε πρώτο αριθμό, όπως τον $p_1 = 2$, ας υποθέσουμε ότι έχουμε βρει n πρώτους $p_1, p_2, \ldots, p_n$· κατόπιν παρατηρούμε ότι ο αριθμός $p_1 p_2 \ldots p_n + 1$ είτε είναι και ο ίδιος πρώτος, είτε περιλαμβάνει ως παράγοντα έναν πρώτο ο οποίος διαφέρει από εκείνους που έχουμε ήδη βρει. Δεδομένου ότι ο παράγοντας αυτός μπορεί πάντα να βρεθεί με απευθείας δοκιμή, είμαστε σίγουροι σε κάθε περίπτωση ότι θα βρούμε τουλάχιστον έναν νέο πρώτο p_{n+1}· προχωρώντας με αυτό τον τρόπο βλέπουμε ότι η ακολουθία κατασκευάσιμων πρώτων δεν μπορεί να τελειώσει ποτέ.

Άσκηση: Εφαρμόστε αυτή την κατασκευή ξεκινώντας από τους $p_1 = 2$, $p_2 = 3$, και βρείτε 5 ακόμα πρώτους.

Όταν ένας αριθμός έχει εκφραστεί ως γινόμενο πρώτων, μπορούμε να διατάξουμε αυτούς τους πρώτους παράγοντες με οποιαδήποτε σειρά. Με λίγη εμπειρία καταλαβαίνουμε ότι, αν εξαιρέσουμε αυτή την αυθαιρεσία στη σειρά, η ανάλυση ενός αριθμού N σε πρώτους είναι μοναδική: *Κάθε ακέραιος N μεγαλύτερος από το 1 μπορεί να παραγοντοποιηθεί σε γινόμενο πρώτων με έναν μόνο τρόπο*. Εκ πρώτης όψεως, η πρόταση αυτή φαίνεται τόσο προφανής που ο μη μαθηματικός τείνει να τη θεωρεί δεδομένη. Ωστόσο, δεν είναι επ' ουδενί τετριμμένη, και η απόδειξη, παρότι απόλυτα στοιχειώδης, απαιτεί κάποια περίτεχνη συλλογιστική. Η κλασική απόδειξη αυτού του «θεμελιώδους θεωρήματος της αριθμητικής» η οποία έχει διατυπωθεί από τον Ευκλείδη βασίζεται σε μια μέθοδο, ή αλλιώς «αλγόριθμο», για την εύρεση του μέγιστου κοινού διαιρέτη δύο αριθμών. Θα την εξετάσουμε στην σελ. 48. Εδώ θα παραθέσουμε αντ' αυτής μια απόδειξη πιο πρόσφατης εσοδείας, κάπως πιο συνοπτική και ίσως πιο εκλεπτυσμένη από αυτή του Ευκλείδη. Αποτελεί τυπικό παράδειγμα έμμεσης απόδειξης. Θα δεχθούμε την ύπαρξη ενός ακεραίου που επιδέχεται δύο ουσιωδώς διαφορετικές αναλύσεις σε πρώτους παράγοντες, και από την παραδοχή αυτή θα καταλήξουμε σε άτοπο. Το άτοπο αυτό θα δείξει ότι η υπόθεση πως υπάρχει ακέραιος με δύο ουσιωδώς διαφορετικές αναλύσεις σε πρώτους αριθμούς είναι αβάσιμη, και συνεπώς ότι η ανάλυση κάθε ακεραίου σε πρώτους είναι μοναδική.

*Αν υπάρχει θετικός ακέραιος που επιδέχεται ανάλυση σε δύο ουσιωδώς

διαφορετικά γινόμενα πρώτων, τότε θα υπάρχει *ελάχιστος* τέτοιος αριθμός (βλ. σελ. 20),

$$m = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s, \tag{1}$$

όπου οι p και οι q είναι πρώτοι. Αναδιατάσσοντας τη σειρά των p και των q αν αυτό είναι απαραίτητο, μπορούμε να υποθέσουμε ότι

$$p_1 \le p_2 \le \cdots \le p_r, \qquad q_1 \le q_2 \le \cdots \le q_s.$$

Τώρα, ο p_1 δεν μπορεί να είναι ίσος με τον q_1, διότι αν ήταν θα μπορούσαμε να απαλείψουμε τον πρώτο παράγοντα από το κάθε μέλος της εξίσωσης (1) και να πάρουμε δύο ουσιωδώς διαφορετικές αναλύσεις σε πρώτους ενός ακεραίου μικρότερου από τον m, πράγμα που θα αντέβαινε προς την επιλογή του m ως *ελάχιστου* ακεραίου για τον οποίο αυτό είναι δυνατόν. Επομένως, είτε $p_1 < q_1$ είτε $q_1 < p_1$. Έστω ότι $p_1 < q_1$. (Αν $q_1 < p_1$, απλά εναλλάσσουμε τα γράμματα p και q σε ό,τι ακολουθεί.) Σχηματίζουμε τον ακέραιο

$$m' = m - (p_1 q_2 q_3 \dots q_s). \tag{2}$$

Αντικαθιστώντας το m με τις δύο εκφράσεις της εξίσωσης (1) μπορούμε να γράψουμε τον ακέραιο m' σε καθεμία από τις δύο μορφές

$$m' = (p_1 p_2 \dots p_r) - (p_1 q_2 \dots q_s) = p_1(p_2 p_3 \dots p_r - q_2 q_3 \dots q_s) \tag{3}$$

$$m' = (q_1 q_2 \dots q_s) - (p_1 q_2 \dots q_s) = (q_1 - p_1)(q_2 q_3 \dots q_s) \tag{4}$$

Δεδομένου ότι $p_1 < q_1$, έπεται από την (4) ότι ο m' είναι θετικός ακέραιος, ενώ από τη (2) έπεται ότι ο m' είναι μικρότερος του m. Συνεπώς, η ανάλυση του m' σε πρώτους θα πρέπει να είναι *μοναδική*, πέρα από τη σειρά των παραγόντων. Αλλά από την (3) φαίνεται ότι ο πρώτος p_1 είναι παράγοντας του m', και άρα βάσει της (4) ο p_1 θα πρέπει να εμφανίζεται ως παράγοντας είτε του $(q_1 - p_1)$ είτε του $(q_2 q_3 \dots q_s)$. (Αυτό έπεται από την υποτεθείσα μοναδικότητα της ανάλυσης του m' σε πρώτους· βλ. το σκεπτικό στην επόμενη παράγραφο.) Το τελευταίο είναι αδύνατο, διότι όλοι οι q είναι μεγαλύτεροι του p_1. Επομένως, ο p_1 θα πρέπει να είναι παράγοντας του $q_1 - p_1$, και άρα για κάποιον ακέραιο h,

$$q_1 - p_1 = p_1 \cdot h \qquad \text{ή} \qquad q_1 = p_1(h+1).$$

Αλλά αυτό σημαίνει ότι ο p_1 είναι παράγοντας του q_1, που αντιβαίνει προς το γεγονός ότι ο q_1 είναι πρώτος. Αυτό το άτοπο δείχνει ότι η αρχική παραδοχή μας είναι αβάσιμη, και επομένως ολοκληρώνει την απόδειξη του θεμελιώδους θεωρήματος της αριθμητικής.

Ένα σημαντικό πόρισμα του θεμελιώδους θεωρήματος είναι το εξής; *Αν ένας πρώτος p είναι παράγοντας του γινομένου ab, τότε ο p θα πρέπει να είναι*

παράγοντας είτε του a είτε του b. Διότι αν ο p δεν ήταν παράγοντας ούτε του a ούτε του b, τότε το γινόμενο των αναλύσεων των a και b σε πρώτους θα έδινε μια ανάλυση του ακεραίου ab σε πρώτους *που δεν θα περιείχε τον p*. Από την άλλη πλευρά, δεδομένου ότι έχουμε υποθέσει πως ο p είναι παράγοντας του ab, υπάρχει ακέραιος t τέτοιος ώστε

$$ab = pt.$$

Συνεπώς, το γινόμενο του p και μιας ανάλυσης του t σε πρώτους θα έδινε μια ανάλυση του ακεραίου ab σε πρώτους *η οποία θα περιείχε τον p*, σε αντίθεση προς το γεγονός ότι η ανάλυση του ab σε πρώτους είναι μοναδική.

Παραδείγματα: Αν έχει κανείς επιβεβαιώσει το γεγονός ότι το 13 είναι παράγοντας του 2652 και το γεγονός ότι $2652 = 6 \cdot 442$, μπορεί να συμπεράνει ότι το 13 είναι παράγοντας του 442. Από την άλλη πλευρά, το 6 είναι παράγοντας του 240, και $240 = 15 \cdot 16$, αλλά το 6 δεν είναι παράγοντας ούτε του 15 ούτε του 16. Αυτό δείχνει πως η παραδοχή ότι ο p είναι *πρώτος* είναι ουσιώδης.

Άσκηση: Προκειμένου να βρούμε όλους τους διαιρέτες οποιουδήποτε αριθμού a, αρκεί να αναλύσουμε τον a σε ένα γινόμενο

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

όπου οι p είναι διαφορετικοί πρώτοι, καθένας υψωμένος σε κάποια δύναμη. *Όλοι* οι διαιρέτες του a είναι οι αριθμοί

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_r^{\beta_r},$$

όπου οι αριθμοί β είναι οποιοιδήποτε ακέραιοι που ικανοποιούν τις ανισότητες

$$0 \le \beta_1 \le \alpha_1, \quad 0 \le \beta_2 \le \alpha_2, \quad \dots, \quad 0 \le \beta_r \le \alpha_r.$$

Αποδείξτε αυτή την πρόταση. Δείξτε, ως επακόλουθο, ότι το πλήθος των διαφορετικών διαιρετών του a (συμπεριλαμβανομένων των διαιρετών a και 1) δίνεται από το γινόμενο

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1).$$

Για παράδειγμα, το

$$144 = 2^4 \cdot 3^2$$

έχει $5 \cdot 3$ διαιρέτες. Είναι οι $1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 9, 18, 36, 72, 144$.

2. Η κατανομή των πρώτων

Για να καταστρώσουμε μια λίστα όλων των πρώτων μέχρι οποιονδήποτε δεδομένο ακέραιο N, μπορούμε να γράψουμε κατά σειρά όλους τους ακεραίους που είναι μικρότεροι του N, να διαγράψουμε εκείνους που είναι πολλαπλάσια

του 2, κατόπιν όλους τους εναπομείναντες ακεραίους που είναι πολλαπλάσια του 3, και ούτω καθεξής μέχρις ότου να διαγραφούν όλοι οι σύνθετοι αριθμοί. Η διαδικασία αυτή, γνωστή ως «κόσκινο του Ερατοσθένη», θα πιάσει στα δίχτυα της τους πρώτους αριθμούς μέχρι τον N. Με εκλεπτυσμένες εκδοχές αυτής της μεθόδου, έχουν σταδιακά συνταχθεί πίνακες πρώτων αριθμών μέχρι το $10.000.000$ περίπου, οι οποίοι μας παρέχουν μια τεράστια ποσότητα εμπειρικών δεδομένων σχετικά με την κατανομή και τις ιδιότητες των πρώτων. Με βάση αυτούς τους πίνακες, μπορούμε να κάνουμε πολλές εξαιρετικά εύλογες εικασίες (σαν να ήταν η θεωρία αριθμών μια πειραματική επιστήμη) οι οποίες συχνά είναι ιδιαίτερα δύσκολο να αποδειχθούν.

α. Τύποι που παράγουν πρώτους αριθμούς

Έχουν γίνει προσπάθειες να βρεθούν απλοί αριθμητικοί τύποι οι οποίοι δίνουν μόνο πρώτους αριθμούς, παρότι ίσως να μην δίνουν όλους αυτούς τους αριθμούς. Ο Fermat διατύπωσε την περίφημη εικασία (η οποία όμως δεν ήταν ρητός ισχυρισμός) ότι όλοι οι αριθμοί της μορφής

$$F(n) = 2^{2^n} + 1$$

είναι πρώτοι. Πράγματι, για $n = 1, 2, 3, 4$ παίρνουμε

$$\begin{aligned} F(1) &= 2^2 + 1 = 5, \\ F(2) &= 2^{2^2} + 1 = 2^4 + 1 = 17, \\ F(3) &= 2^{2^3} + 1 = 2^8 + 1 = 257, \\ F(4) &= 2^{2^4} + 1 = 2^{16} + 1 = 65.537, \end{aligned}$$

που είναι όλοι τους πρώτοι αριθμοί. Αλλά το 1732, ο Euler ανακάλυψε την παραγοντοποίηση $2^{2^5} + 1 = 641 \cdot 6.700.417$· συνεπώς, ο $F(5)$ δεν είναι πρώτος. Αργότερα, διαπιστώθηκε ότι και άλλοι από αυτούς τους «αριθμούς Fermat» είναι σύνθετοι, με κάθε τέτοια περίπτωση να απαιτεί βαθύτερες αριθμοθεωρητικές μεθόδους, λόγω των ανυπέρβλητων δυσκολιών της απευθείας δοκιμής. Μάλιστα, μέχρι σήμερα δεν έχει αποδειχθεί για κανέναν από τους αριθμούς $F(n)$ με $n > 4$ ότι είναι πρώτος.

Μια άλλη αξιοσημείωτη και απλή έκφραση που παράγει πολλούς πρώτους είναι η

$$f(n) = n^2 - n + 41.$$

Για $n = 1, 2, 3, \ldots, 40$, ο αριθμός $f(n)$ είναι πρώτος· αλλά για $n = 41$, έχουμε $f(n) = 41^2$, ο οποίος δεν είναι πλέον πρώτος.

Η έκφραση

$$n^2 - 79n + 1601$$

δίνει πρώτους για όλα τα n μέχρι το 79, αλλά αποτυγχάνει όταν $n = 80$. Συνολικά, η αναζήτηση εκφράσεων απλής μορφής οι οποίες να δίνουν μόνο πρώτους έχει αποδειχθεί άκαρπη. Ακόμα λιγότερο υποσχόμενη είναι η προσπάθεια να βρεθεί ένας αλγεβρικός τύπος ο οποίος θα δίνει *όλους* τους πρώτους.*

β. Πρώτοι αριθμοί σε αριθμητικές προόδους

Ενώ ήταν εύκολο να αποδείξουμε ότι υπάρχουν άπειροι το πλήθος πρώτοι στην ακολουθία όλων των ακεραίων $1, 2, 3, 4, \ldots$,, το βήμα σε ακολουθίες όπως η $1, 4, 7, 10, 13, \ldots$ ή η $3, 7, 11, 15, 19, \ldots$ ή, γενικότερα, σε οποιαδήποτε αριθμητική πρόοδο, $a, a+d, a+2d, \ldots, a+nd, \ldots$, όπου τα a και d δεν έχουν κανέναν κοινό παράγοντα, ήταν πολύ πιο δύσκολο. Όλες οι παρατηρήσεις υποδείκνυαν ότι *σε κάθε τέτοια ακολουθία υπάρχουν άπειροι το πλήθος πρώτοι*, όπως στην απλούστερη δυνατή περίπτωση $1, 2, 3, \ldots$. Απαιτήθηκε τεράστια προσπάθεια για να αποδειχθεί αυτό το γενικό θεώρημα. Ο Lejeune Dirichlet (1805-1859), ένας από τους κορυφαίους μαθηματικούς του δέκατου ένατου αιώνα, κατήγαγε πλήρη επιτυχία εφαρμόζοντας τα πιο προηγμένα εργαλεία μαθηματικής ανάλυσης που ήταν γνωστά στην εποχή του. Τα αρχικά του άρθρα πάνω στο αντικείμενο συγκαταλέγονται ακόμα και σήμερα ανάμεσα στα εξαιρετικά επιτεύγματα των μαθηματικών, και εκατό χρόνια μετά η απόδειξη δεν έχει ακόμα απλοποιηθεί αρκετά ώστε να βρίσκεται εντός της γνωστικής εμβέλειας μαθητών που δεν είναι καλά εκπαιδευμένοι στην τεχνική του απειροστικού λογισμού και της θεωρίας συναρτήσεων.

Αν και δεν μπορούμε να επιχειρήσουμε να αποδείξουμε το γενικό θεώρημα του Dirichlet, είναι εύκολο να γενικεύσουμε την απόδειξη του Ευκλείδη για την απειρία των πρώτων ώστε να καλύψουμε κάποιες *ειδικές* αριθμητικές προόδους όπως την $4n + 3$ και την $6n + 5$. Για να πραγματευτούμε την πρώτη από αυτές, παρατηρούμε ότι κάθε πρώτος αριθμός μεγαλύτερος του 2 είναι περιττός (αφού διαφορετικά θα διαιρούνταν με το 2) και επομένως είναι της μορφής $4n + 1$ ή $4n + 3$, για κάποιον ακέραιο n. Επιπλέον, το γινόμενο δύο αριθμών της μορφής $4n + 1$ είναι και πάλι αυτής της μορφής, διότι

$$(4a + 1)(4b + 1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1.$$

Ας υποθέσουμε τώρα ότι υπήρχε πεπερασμένο πλήθος πρώτων, $p_1, p_2, \ldots, p_n$, της μορφής $4n + 3$, και ας θεωρήσουμε τον αριθμό

$$N = 4(p_1 p_2 \cdots p_n) - 1 = 4(p_1 \cdots p_n - 1) + 3.$$

Είτε ο ίδιος ο N είναι πρώτος, είτε μπορεί να αναλυθεί σε γινόμενο πρώτων, κανένας από τους οποίους δεν μπορεί να είναι ένας από τους $p_1, \ldots, p_n$, διότι

*Σ.τ.Ε.: Για νεότερες εξελίξεις σε αυτό το θέμα βλ. Κεφ. IX.

οι αριθμοί αυτοί διαιρούν τον N με υπόλοιπο -1. Επιπλέον, οι πρώτοι παράγοντες του N δεν μπορούν να είναι όλοι της μορφής $4n+1$, διότι ο N δεν είναι αυτής της μορφής και, όπως είδαμε, το γινόμενο αριθμών της μορφής $4n+1$ είναι και πάλι αυτής της μορφής. Συνεπώς, τουλάχιστον ένας πρώτος παράγοντας θα πρέπει να είναι της μορφής $4n+3$, πράγμα αδύνατον, διότι είδαμε ότι κανένας από τους p, για τους οποίους υποθέσαμε ότι είναι *όλοι* οι πρώτοι της μορφής $4n+3$, δεν μπορεί να είναι παράγοντας του N. Επομένως, η παραδοχή ότι το πλήθος των πρώτων της μορφής $4n+3$ είναι πεπερασμένο μας έχει οδηγήσει σε άτοπο, και συνεπώς το πλήθος αυτού του είδους των πρώτων θα πρέπει να είναι άπειρο.

Άσκηση: Αποδείξτε το αντίστοιχο θεώρημα για την πρόοδο $6n+5$.

γ. Το θεώρημα των πρώτων αριθμών

Στην αναζήτηση ενός νόμου που διέπει την κατανομή των πρώτων αριθμών, το καθοριστικό βήμα έγινε όταν οι μαθηματικοί εγκατέλειψαν τις άκαρπες προσπάθειες να βρουν έναν απλό μαθηματικό τύπο που να δίνει όλους τους πρώτους ή που να δίνει το ακριβές πλήθος των πρώτων που περιέχονται ανάμεσα στους πρώτους n ακεραίους, και αναζήτησαν αντ' αυτού πληροφορίες σχετικά με τη *μέση* κατανομή των πρώτων ανάμεσα στους ακεραίους.

Για κάθε ακέραιο n, ας συμβολίσουμε με A_n το πλήθος των πρώτων ανάμεσα στους ακεραίους $1, 2, 3, \cdots, n$. Αν υπογραμμίσουμε τους πρώτους στην ακολουθία που αποτελείται από τους λίγους πρώτους ακεραίους, $1\,\underline{2}\,\underline{3}\,4\,\underline{5}\,6\,\underline{7}\,8\,9\,10\,\underline{11}\,12\,\underline{13}\,14\,15\,16\,\underline{17}\,18\,\underline{19}\,...$, μπορούμε να υπολογίσουμε τις λίγες πρώτες τιμές του A_n:
$A_1 = 0, A_2 = 1, A_3 = A_4 = 2, A_5 = A_6 = 3, A_7 = A_8 = A_9 = A_{10} = 4,$
$A_{11} = A_{12} = 5, A_{13} = A_{14} = A_{15} = A_{16} = 6, A_{17} = A_{18} = 7, A_{19} = 8,$
κ.λπ.

Αν πάρουμε τώρα οποιαδήποτε ακολουθία τιμών για το n η οποία αυξάνεται χωρίς όριο, λόγου χάριν

$$n = 10, 10^2, 10^3, 10^4, \dots,$$

τότε οι αντίστοιχες τιμές του A_n,

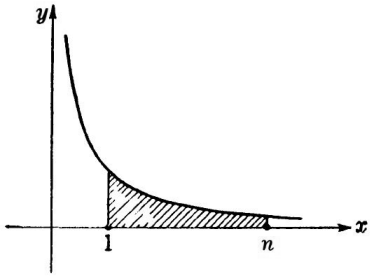
$$A_{10}, A_{10^2}, A_{10^3}, A_{10^4}, \dots,$$

θα αυξάνονται επίσης χωρίς όριο (αν και βραδύτερα). Διότι ξέρουμε ότι υπάρχουν άπειροι το πλήθος πρώτοι, και επομένως οι τιμές του A_n αργά ή γρήγορα θα υπερβούν οποιονδήποτε πεπερασμένο αριθμό. Η «πυκνότητα» των πρώτων ανάμεσα στους n μικρότερους ακεραίους δίνεται από τον λόγο A_n/n, και από έναν πίνακα πρώτων αριθμών μπορούν να υπολογιστούν εμπειρικά οι τιμές του A_n/n για αρκετά μεγάλες τιμές του n.

n	A_n/n
10^3	0,168
10^6	0,078498
10^9	0,050847478
.....	.....

Το τελευταίο στοιχείο αυτού του πίνακα μπορεί να θεωρηθεί ότι δίνει την πιθανότητα ένας ακέραιος που επιλέγεται τυχαία ανάμεσα στους πρώτους 10^9 ακεραίους να είναι πρώτος, αφού υπάρχουν 10^9 δυνατές επιλογές, από τις οποίες οι A_{10^9} είναι πρώτοι αριθμοί.

Η κατανομή των μεμονωμένων πρώτων ανάμεσα στους ακεραίους είναι εξαιρετικά ανομοιόμορφη. Αλλά αυτή η ανομοιομορφία «στα μικρά» εξαφανίζεται αν επικεντρώσουμε την προσοχή μας στη μέση κατανομή των πρώτων όπως δίνεται από τον λόγο A_n/n. Ο απλός νόμος που διέπει τη συμπεριφορά αυτού του λόγου είναι μία από τις πιο αξιοσημείωτες ανακαλύψεις σε όλο το πεδίο των μαθηματικών. Προκειμένου να διατυπώσουμε το *θεώρημα των πρώτων αριθμών*, θα πρέπει να ορίσουμε τον «φυσικό λογάριθμο» ενός ακεραίου n. Για τον σκοπό αυτό, παίρνουμε δύο κάθετους άξονες σε ένα επίπεδο, και θεωρούμε τον γεωμετρικό τόπο όλων των σημείων του επιπέδου για τα οποία ισχύει ότι το γινόμενο το αποστάσεών τους x και y από αυτούς τους άξονες ισούται με ένα. Συναρτήσει των συντεταγμένων x και y, ο γεωμετρικός αυτός τόπος, μια ισόπλευρη υπερβολή, ορίζεται μέσω της εξίσωσης $xy = 1$. Στη συνέχεια ορίζουμε ως $\log n$ το *εμβαδόν* στο Σχήμα 5 το οποίο οριοθετείται από την υπερβολή, τον άξονα x, και τις δύο κατακόρυφες ευθείες $x = 1$ και $x = n$. (Μια λεπτομερέστερη παρουσίαση του λογαρίθμου παρατίθεται στο Κεφάλαιο VIII.) Από μια εμπειρική μελέτη των πινάκων πρώτων αριθμών, ο Gauss παρατήρησε ότι ο λόγος A_n/n ισούται κατά προσέγγιση με $1/\log n$, και ότι η προσέγγιση αυτή φαίνεται να βελτιώνεται καθώς το n αυξάνεται. Η ποιότητα της προσέγγισης δίνεται από τον λόγο $\dfrac{A_n/n}{1/\log n}$, του οποίου οι τιμές για



Σχήμα 5. Το εμβαδόν της σκιασμένης περιοχής κάτω από την υπερβολή ορίζει το $\log n$.

$n = 1000, 1.000.000, 1.000.000.000$ παρουσιάζονται στον παρακάτω πίνακα.

n	A_n/n	$1/\log n$	$\dfrac{A_n/n}{1/\log n}$
10^3	0,168	0,145	1,159
10^6	0,078498	0,072382	1,084
10^9	0,050847478	0,048254942	1,053
.....	.....	.....	.....

Βάσει τέτοιων εμπειρικών δεδομένων, ο Gauss έκανε την εικασία ότι ο λόγος A_n/n είναι «ασυμπτωτικά ίσος» με $1/\log n$. Η φράση αυτή σημαίνει ότι αν πάρουμε μια ακολουθία ολοένα και μεγαλύτερων τιμών του n, λόγου χάριν για n ίσο με

$$10, 10^2, 10^3, 10^4, ...$$

όπως πριν, τότε ο λόγος του A_n/n προς το $1/\log n$,

$$\frac{A_n/n}{1/\log n},$$

που υπολογίζεται για αυτές τις διαδοχικές τιμές του n, θα πλησιάζει ολοένα και περισσότερο την τιμή 1, και ότι η διαφορά αυτού του λόγου από το 1 μπορεί να γίνει όσο μικρή θέλουμε αν περιοριστούμε σε επαρκώς μεγάλες τιμές του n. Ο ισχυρισμός αυτός εκφράζεται συμβολικά μέσω του συμβόλου $\sim$:

$\dfrac{A_n}{n} \sim \dfrac{1}{\log n}$ σημαίνει ότι το $\dfrac{A_n/n}{1/\log n}$ τείνει προς το 1 καθώς αυξάνεται το n.

Το ότι το $\sim$ δεν μπορεί να αντικατασταθεί από το σύνηθες σύμβολο $=$ της ισότητας είναι εμφανές από το γεγονός ότι ενώ το A_n είναι πάντα ακέραιος αριθμός, ο λόγος $n/\log n$ δεν είναι.

Το γεγονός ότι η μέση συμπεριφορά της κατανομής των πρώτων αριθμών μπορεί να περιγραφεί από τη λογαριθμική συνάρτηση είναι μια πολύ αξιοσημείωτη ανακάλυψη, διότι είναι αναπάντεχο δύο μαθηματικές έννοιες που φαίνονται τόσο ασύνδετες μεταξύ τους να είναι στην πραγματικότητα τόσο στενά συνδεδεμένες.

Παρότι η διατύπωση της εικασίας του Gauss είναι απλή και εύληπτη, μια αυστηρή μαθηματική απόδειξη υπερέβαινε κατά πολύ τις δυνατότητες της μαθηματικής επιστήμης την εποχή του Gauss. Για να αποδειχθεί αυτό το θεώρημα, το οποίο αφορά μόνο τις πιο στοιχειώδεις έννοιες, είναι απαραίτητο να εφαρμόσουμε τις πιο ισχυρές μεθόδους των σύγχρονων μαθηματικών. Χρειάστηκαν σχεδόν εκατό χρόνια μέχρι η ανάλυση να αναπτυχθεί σε τέτοιο σημείο ώστε ο Hadamard (1896) στο Παρίσι και ο de la Vallée Poussin (1896)

στη Λουβαίν να μπορέσουν να δώσουν μια πλήρη απόδειξη του θεωρήματος των πρώτων αριθμών. Στη συνέχεια, οι v. Mangoldt και Landau προέβησαν σε απλοποιήσεις και σημαντικές τροποποιήσεις. Πολύ πριν από τον Hadamard, καθοριστική πρωτοποριακή εργασία πάνω στο συγκεκριμένο θέμα είχε γίνει από τον Riemann (1826-1866) σε ένα περίφημο άρθρο όπου χαράχτηκαν οι στρατηγικές κατευθυντήριες γραμμές για την επίθεση. Πρόσφατα,* ο Αμερικανός μαθηματικός Norbert Wiener κατάφερε τροποποιώντας την απόδειξη να αποφύγει τη χρήση μιγαδικών αριθμών ως σημαντικό βήμα του σκεπτικού. Ωστόσο, η απόδειξη του θεωρήματος των πρώτων αριθμών παραμένει αρκετά απαιτητικό θέμα ακόμα και για έναν προχωρημένο φοιτητή. Θα επανέλθουμε στο ζήτημα αυτό στη σελ. 524 κ.ε.

δ. Δύο άλυτα προβλήματα σχετικά με τους πρώτους αριθμούς

Ενώ το πρόβλημα της μέσης κατανομής των πρώτων έχει επιλυθεί ικανοποιητικά, υπάρχουν πολλές άλλες εικασίες που υποστηρίζονται από όλα τα διαθέσιμα εμπειρικά δεδομένα αλλά που ακόμα δεν έχει αποδειχθεί ότι ισχύουν.

Μία από αυτές είναι η περίφημη *εικασία του Goldbach*. Ο Christian Goldbach (1690-1764) δεν έχει αφήσει κανένα άλλο στίγμα στην ιστορία των μαθηματικών πέρα από αυτό το πρόβλημα, το οποίο πρότεινε το 1742 σε μια επιστολή στον Euler. Όπως παρατήρησε σε όλες τις περιπτώσεις που δοκίμασε, κάθε άρτιος αριθμός (εκτός από το 2, που είναι και το ίδιο πρώτος αριθμός) μπορούσε να αναπαρασταθεί ως άθροισμα δύο πρώτων. Για παράδειγμα:

$4 = 2 + 2, 6 = 3 + 3, 8 = 5 + 3, 10 = 5 + 5, 12 = 5 + 7, 14 = 7 + 7, 16 = 13 + 3, 18 = 11 + 7, 20 = 13 + 7, \ldots, 48 = 29 + 19, \ldots, 100 = 97 + 3,$ κ.λπ.

Ο Goldbach ρώτησε αν ο Euler μπορούσε να αποδείξει ότι αυτό ισχύει για *όλους* τους άρτιους αριθμούς, ή αν μπορούσε να βρει ένα παράδειγμα που να το καταρρίπτει. Ο Euler δεν βρήκε ποτέ την απάντηση σε αυτό το ερώτημα, ούτε έχει δοθεί απάντηση μέχρι σήμερα. Τα εμπειρικά δεδομένα υπέρ της πρότασης ότι κάθε άρτιος αριθμός μπορεί να αναπαρασταθεί με αυτό τον τρόπο είναι απολύτως πειστικά,† όπως μπορεί να επιβεβαιώσει ο καθένας δοκιμάζοντας μερικά παραδείγματα. Η πηγή της δυσκολίας έγκειται στο ότι οι πρώτοι ορίζονται μέσω του *πολλαπλασιασμού*, ενώ το πρόβλημα περιλαμβάνει *πρόσθεση*. Γενικά μιλώντας, είναι δύσκολο να αποδειχθούν συνδέσεις ανάμεσα στις πολλαπλασιαστικές και τις προσθετικές ιδιότητες των ακεραίων.

---

*Σ.τ.Ε.: Η απλοποιημένη απόδειξη χαρακτηρίζεται πρόσφατη σε σχέση με την αρχική έκδοση του βιβλίου *What is Mathematics* (1941). Ο Norbert Wiener δημοσίευσε την εν λόγω απόδειξη μόλις το 1932. Έκτοτε, έχουν δοθεί και άλλες αποδείξεις (στοιχειώδεις και μη) από τους Selberg, Erdös και Newmann.

†Σ.τ.Ε.: Με χρήση υπολογιστών, η εικασία έχει επαληθευτεί για όλους τους άρτιους μικρότερους του $4 \cdot 10^{18}$.

Μέχρι πρόσφατα, μια απόδειξη της εικασίας του Goldbach φαινόταν εντελώς απρόσιτη. Σήμερα μια λύση δεν φαίνεται πλέον απροσπέλαστη. Μια σημαντική επιτυχία, πολύ αναπάντεχη και εκπληκτική από κάθε πλευρά, κατήγαγε το 1931 ένας άγνωστος τότε νεαρός Ρώσος μαθηματικός, ο Schnirelmann (1905-1938), ο οποίος απέδειξε ότι *κάθε θετικός ακέραιος μπορεί να αναπαρασταθεί ως άθροισμα το πολύ* 300.000 *πρώτων*. Αν και το αποτέλεσμα αυτό φαίνεται κωμικό σε σύγκριση με τον αρχικό στόχο της απόδειξης της εικασίας του Goldbach, ωστόσο ήταν ένα πρώτο βήμα σε αυτή την κατεύθυνση. Η απόδειξη είναι άμεση, κατασκευαστική, αν και δεν παρέχει καμία πρακτική μέθοδο για την εύρεση της ανάλυσης ενός τυχόντος ακεραίου σε πρώτους αριθμούς. Πιο πρόσφατα, ο Ρώσος μαθηματικός Vinogradoff, χρησιμοποιώντας μεθόδους που οφείλονται στον Hardy, τον Littlewood και τον μεγάλο Ινδό συνεργάτη τους Ramanujan, έχει πετύχει να μειώσει το πλήθος από 300.000 σε 4. Το αποτέλεσμα αυτό είναι πολύ πλησιέστερο σε μια λύση στο πρόβλημα του Goldbach. Ωστόσο, ανάμεσα στο αποτέλεσμα του Schnirelmann και σε αυτό του Vinogradoff υπάρχει μια καίρια διαφορά, ίσως πιο σημαντική από τη διαφορά ανάμεσα στο 300.000 και το 4. Το θεώρημα του Vinogradoff αποδείχθηκε μόνο για όλους τους «επαρκώς μεγάλους» ακεραίους· ακριβέστερα, ο Vinogradoff απέδειξε ότι *υπάρχει* ακέραιος N για τον οποίο ισχύει ότι κάθε ακέραιος $n > N$ μπορεί να αναπαρασταθεί ως άθροισμα το πολύ 4 πρώτων. Η απόδειξη του Vinogradoff δεν μας επιτρέπει να εκτιμήσουμε ποσοτικά τον N· σε αντίθεση με το θεώρημα του Schnirelmann, είναι ουσιαστικά έμμεση και μη κατασκευαστική. Αυτό που απέδειξε στην πραγματικότητα ο Vinogradoff είναι ότι η παραδοχή πως άπειροι το πλήθος ακέραιοι δεν μπορούν να αναλυθούν σε 4 το πολύ πρώτους προσθετέους οδηγεί σε άτοπο. Εδώ έχουμε ένα καλό παράδειγμα της θεμελιώδους διαφοράς ανάμεσα στα δύο είδη αποδείξεων, την άμεση και την έμμεση. (Βλ. τη γενική παρουσίαση στη σελ. 93.)

Για το ακόλουθο ακόμα πιο εντυπωσιακό πρόβλημα από εκείνο του Goldbach δεν έχει υπάρξει καμία απολύτως πρόοδος όσον αφορά τη λύση του. Έχει παρατηρηθεί ότι οι πρώτοι απαντούν συχνά σε ζεύγη της μορφής p και $p+2$. Τέτοια ζεύγη είναι τα 3 και 5, 11 και 13, 29 και 31, κ.λπ. Η πρόταση ότι υπάρχουν άπειρα το πλήθος τέτοια ζεύγη πιστεύεται ότι είναι ορθή, αλλά μέχρι στιγμής δεν έχει γίνει ούτε το ελάχιστο συγκεκριμένο βήμα προς μια απόδειξη.[*]

[*] Σ.τ.Ε.: Στα χρόνια που μεσολάβησαν από την αρχική έκδοση του βιβλίου, έχει γίνει μεγάλη πρόοδος όσον αφορά τα παραπάνω ζητήματα. Κάποια σημαντικά επιτεύγματα αναφέρονται στο Κεφ. IX, το οποίο γράφτηκε μεταγενέστερα από τον Ian Stewart.

§2. ΙΣΟΫΠΟΛΟΙΠΙΚΕΣ ΣΧΕΣΕΙΣ

1. Γενικές έννοιες

Οποτεδήποτε ανακύπτει το ζήτημα της διαιρετότητας ακεραίων με έναν καθορισμένο ακέραιο d, η πραγμάτευση μπορεί να αποσαφηνιστεί και να απλοποιηθεί με χρήση της έννοιας και του συμβολισμού των «ισοϋπόλοιπων» αριθμών (που οφείλονται στον Gauss).

Για να εισαγάγουμε αυτή την έννοια, ας εξετάσουμε τα υπόλοιπα που απομένουν όταν διαιρούμε ακεραίους με τον αριθμό 5. Έχουμε

$$\begin{array}{lll}
0 = 0\cdot 5 + 0 & 7 = 1\cdot 5 + 2 & -1 = -1\cdot 5 + 4 \\
1 = 0\cdot 5 + 1 & 8 = 1\cdot 5 + 3 & -2 = -1\cdot 5 + 3 \\
2 = 0\cdot 5 + 2 & 9 = 1\cdot 5 + 4 & -3 = -1\cdot 5 + 2 \\
3 = 0\cdot 5 + 3 & 10 = 2\cdot 5 + 0 & -4 = -1\cdot 5 + 1 \\
4 = 0\cdot 5 + 4 & 11 = 2\cdot 5 + 1 & -5 = -1\cdot 5 + 0 \\
5 = 1\cdot 5 + 0 & 12 = 2\cdot 5 + 2 & -6 = -2\cdot 5 + 4 \\
6 = 1\cdot 5 + 1 & \text{κ.λπ.} & \text{κ.λπ.}
\end{array}$$

Παρατηρούμε ότι το υπόλοιπο που απομένει όταν οποιοσδήποτε ακέραιος διαιρείται με το 5 είναι ένας από τους πέντε ακεραίους $0, 1, 2, 3, 4$. Λέμε ότι δύο ακέραιοι a και b είναι «ισοϋπόλοιποι modulo 5» αν αφήνουν το *ίδιο υπόλοιπο* όταν διαιρούνται με το 5. Συνεπώς, οι $2, 7, 12, 17, 22, \ldots, -3, -8, -13, -18, \ldots$ είναι όλοι τους ισοϋπόλοιποι modulo 5, αφού αφήνουν υπόλοιπο 2. Εν γένει, λέμε ότι δύο ακέραιοι a και b είναι *ισοϋπόλοιποι modulo* d, όπου το d είναι ένας καθορισμένος ακέραιος, αν οι a και b αφήνουν το ίδιο υπόλοιπο όταν διαιρούνται με τον d, δηλαδή αν υπάρχει ακέραιος n τέτοιος ώστε $a - b = nd$. Για παράδειγμα, το 27 και το 15 είναι ισοϋπόλοιποι modulo 4, διότι

$$27 = 6\cdot 4 + 3, \quad 15 = 3\cdot 4 + 3.$$

Η έννοια των ισοϋπόλοιπων αριθμών είναι τόσο χρήσιμη που μας διευκολύνει να έχουμε έναν συνοπτικό συμβολισμό για αυτήν. Γράφουμε

$$a \equiv b \qquad (\text{mod } d)$$

για να εκφράσουμε το γεγονός ότι οι a και b είναι ισοϋπόλοιποι modulo d. Αν είναι προφανές ποιο είναι το modulus, η έκφραση $(\text{mod } d)$ του τύπου μπορεί να παραλειφθεί. (Αν ο a δεν είναι ισοϋπόλοιπος του b modulo d, γράφουμε $a \not\equiv b \ (\text{mod } d)$).

Ισοϋπολοιπικές σχέσεις απαντούν συχνά στην καθημερινή ζωή. Για παράδειγμα, οι δείκτες ενός ρολογιού δείχνουν την ώρα modulo 12, και ο οδοδείκτης

ενός αυτοκινήτου δίνει τα συνολικά χιλιόμετρα που έχουν διανυθεί modulo 100.000.

Προτού προχωρήσουμε στη λεπτομερή πραγμάτευση των ισοϋπολοιπικών σχέσεων, ο αναγνώστης θα πρέπει να παρατηρήσει ότι οι παρακάτω προτάσεις είναι όλες ισοδύναμες:

1. Ο a είναι ισοϋπόλοιπος του b modulo d.
2. $a = b + nd$ για κάποιον ακέραιο n.
3. Το d διαιρεί το $a - b$.

Η χρησιμότητα του ισοϋπολοιπικού συμβολισμού του Gauss έγκειται στο γεγονός ότι η ιδιότητα του ίσου υπολοίπου ως προς ένα καθορισμένο modulus έχει πολλές από τις τυπικές ιδιότητες της συνήθους ισότητας. Οι πιο σημαντικές τυπικές ιδιότητες της σχέσης $a = b$ είναι οι εξής:

(1) Πάντα $a = a$.

(2) Αν $a = b$, τότε $b = a$.

(3) Αν $a = b$ και $b = c$, τότε $a = c$.

Επιπλέον, αν $a = a'$ και $b = b'$, τότε

(4) $a + b = a' + b'$.

(5) $a - b = a' - b'$.

(6) $ab = a'b'$.

Οι ιδιότητες αυτές εξακολουθούν να ισχύουν όταν η σχέση $a = b$ αντικατασταθεί από την ισοϋπολοιπική σχέση $a \equiv b \pmod{d}$. Επομένως,

(1′) Πάντα $a \equiv a \pmod{d}$.

(2′) Αν $a \equiv b \pmod{d}$, τότε $b \equiv a \pmod{d}$.

(3′) Αν $a \equiv b \pmod{d}$ και $b \equiv c \pmod{d}$, τότε $a \equiv c \pmod{d}$.

Η τετριμμένη επαλήθευση των παραπάνω αφήνεται για τον αναγνώστη.

Επιπλέον, αν $a \equiv a' \pmod{d}$ και $b \equiv b' \pmod{d}$, τότε

(4′) $a + b \equiv a' + b' \pmod{d}$.

(5′) $a - b \equiv a' - b' \pmod{d}$.

(6′) $ab \equiv a'b' \pmod{d}$.

Επομένως, *οι ισοϋπολοιπικές σχέσεις ως προς το ίδιο modulus μπορούν να προστεθούν, να αφαιρεθούν και να πολλαπλασιαστούν*. Για να αποδείξουμε αυτές τις τρεις προτάσεις, αρκεί να παρατηρήσουμε ότι αν

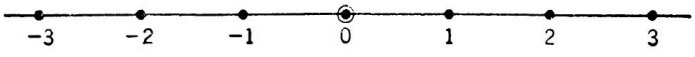
$$a = a' + rd, \qquad b = b' + sd,$$

τότε

$$\begin{aligned} a + b &= a' + b' + (r + s)d, \\ a - b &= a' - b' + (r - s)d, \\ ab &= a'b' + (a's + b'r + rsd)d, \end{aligned}$$

από τις οποίες έπονται τα ζητούμενα συμπεράσματα.

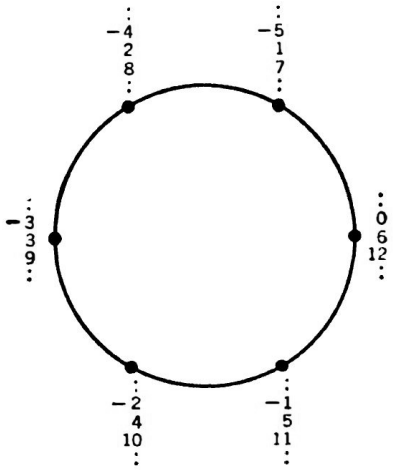
Η έννοια του ίσου υπολοίπου έχει μια διαφωτιστική γεωμετρική ερμηνεία. Συνήθως, αν θέλουμε να αναπαραστήσουμε τους ακεραίους γεωμετρικά, επιλέγουμε ένα τμήμα μοναδιαίου μήκους και το επεκτείνουμε κατά πολλαπλάσια του μήκους του και προς τις δύο κατευθύνσεις. Με αυτό τον τρόπο, μπορούμε να βρούμε ένα σημείο στην ευθεία που να αντιστοιχεί σε κάθε ακέραιο, όπως στο Σχήμα 6. Όταν όμως πραγματευόμαστε τους ακεραίους modulo d, οποιοιδήποτε δύο ισοϋπόλοιποι αριθμοί θεωρούνται ίδιοι όσον αφορά τη συμπεριφορά τους στη διαίρεση με τον d, καθώς αφήνουν το ίδιο υπόλοιπο. Για να δείξουμε αυτό το γεγονός γεωμετρικά, χρησιμοποιούμε έναν κύκλο χωρισμένο σε d ίσα μέρη. Κάθε ακέραιος, όταν διαιρείται με τον d αφήνει ως υπόλοιπο έναν από τους d αριθμούς $0, 1, \ldots, d-1$, οι οποίοι τοποθετούνται σε ίσα διαστήματα επάνω στην περιφέρεια του κύκλου. Κάθε ακέραιος είναι ισοϋπόλοιπος modulo d με έναν από αυτούς τους αριθμούς, και συνεπώς αναπαριστάται γεωμετρικά από ένα από αυτά τα σημεία· δύο αριθμοί είναι ισοϋπόλοιποι αν αναπαριστώνται από το ίδιο σημείο. Το Σχήμα 7 αντιπροσωπεύει την περίπτωση $d = 6$. Ένα άλλο παράδειγμα από την καθημερινή ζωή είναι η πλάκα ενός ρολογιού.



Σχήμα 6. Γεωμετρική αναπαράσταση των ακεραίων.

Ως ένα παράδειγμα της χρήσης της πολλαπλασιαστικής ιδιότητας (6′) των ισοϋπολοιπικών σχέσεων, μπορούμε να προσδιορίσουμε τα υπόλοιπα που απομένουν όταν διαιρούνται με έναν δεδομένο αριθμό δυνάμεις του 10. Λόγου χάριν,

$$10 \equiv -1 \qquad (\text{mod } 11),$$



Σχήμα 7. Γεωμετρική αναπαράσταση των ακεραίων modulo 6.

διότι $10 = -1 + 11$. Πολλαπλασιάζοντας διαδοχικά αυτή την ισοϋπολοιπική σχέση με την εαυτό της, βρίσκουμε ότι

$$\begin{aligned} 10^2 &\equiv (-1)(-1) = 1 \pmod{11}, \\ 10^3 &\equiv -1 \pmod{11}, \\ 10^4 &\equiv 1 \pmod{11}, \text{ κ.λπ.} \end{aligned}$$

Από αυτό μπορούμε να δείξουμε ότι κάθε ακέραιος

$$z = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n,$$

εκπεφρασμένος στο δεκαδικό σύστημα, αφήνει όταν διαιρείται με το 11 το ίδιο υπόλοιπο με το άθροισμα των ψηφίων του, με εναλλασσόμενα πρόσημα,

$$t = a_0 - a_1 + a_2 - a_3 + \cdots.$$

Διότι μπορούμε να γράψουμε

$$z - t = a_1 \cdot 11 + a_2(10^2 - 1) + a_3(10^3 + 1) + a_4(10^4 - 1) + \cdots.$$

Δεδομένου ότι όλοι οι αριθμοί $11, 10^2 - 1, 10^3 + 1, \ldots$ είναι ισοϋπόλοιποι με το 0 modulo 11, το ίδιο ισχύει και για τον $z - t$, και επομένως ο z αφήνει όταν διαιρείται με το 11 το ίδιο υπόλοιπο με το t. Έπεται συγκεκριμένα ότι ένας αριθμός διαιρείται με το 11 (δηλαδή αφήνει υπόλοιπο 0) αν και μόνο αν το εναλλασσόμενο άθροισμα των ψηφίων του διαιρείται με το 11. Για παράδειγμα, δεδομένου ότι $3-1+6-2+8-1+9 = 22$, ο αριθμός $z = 3162819$

διαιρείται με το 11. Το να βρούμε έναν κανόνα διαιρετότητας με το 3 ή με το 9 είναι ακόμα πιο απλό, διότι $10 \equiv 1 \pmod{3 \text{ ή } 9}$, και επομένως $10^n \equiv 1 \pmod{3 \text{ ή } 9}$ για κάθε n. Έπεται ότι ένας αριθμός z διαιρείται με το 3 ή με το 9 αν και μόνο αν το άθροισμα των ψηφίων του

$$s = a_0 + a_1 + a_2 + \cdots + a_n$$

διαιρείται ομοίως με το 3 ή με το 9, αντίστοιχα.

Για ισοϋπολοιπικές σχέσεις modulo 7, έχουμε

$$10 \equiv 3, \quad 10^2 \equiv 2, \quad 10^3 \equiv -1, \quad 10^4 \equiv -3, \quad 10^5 \equiv -2, \quad 10^6 \equiv 1.$$

Στη συνέχεια τα διαδοχικά υπόλοιπα επαναλαμβάνονται. Συνεπώς, ο z διαιρείται με το 7 αν και μόνο αν η έκφραση

$$r = a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + \cdots$$

διαιρείται με το 7.

Άσκηση: Βρείτε έναν παρόμοιο νόμο για διαιρετότητα με το 13.

Όταν προσθέτουμε ή πολλαπλασιάζουμε ισοϋπολοιπικές σχέσεις ως προς ένα καθορισμένο modulus, λόγου χάριν $d = 5$, μπορούμε να αποφύγουμε οι αριθμοί που υπεισέρχονται να γίνουν υπερβολικά μεγάλοι αντικαθιστώντας πάντοτε κάθε αριθμό a με τον αριθμό από το σύνολο

$$0, \quad 1, \quad 2, \quad 3, \quad 4$$

με τον οποίο είναι ισοϋπόλοιπος. Συνεπώς, για να υπολογίσουμε αθροίσματα και γινόμενα ακεραίων modulo 5, αρκεί να χρησιμοποιήσουμε τους παρακάτω πίνακες πρόσθεσης και πολλαπλασιασμού.

$a + b$

$a \equiv$	$b \equiv$	0	1	2	3	4
	0	0	1	2	3	4
	1	1	2	3	4	0
	2	2	3	4	0	1
	3	3	4	0	1	2
	4	4	0	1	2	3

$a \cdot b$

$a \equiv$	$b \equiv$	0	1	2	3	4
	0	0	0	0	0	0
	1	0	1	2	3	4
	2	0	2	4	1	3
	3	0	3	1	4	2
	4	0	4	3	2	1

Από τον δεύτερο από αυτούς τους πίνακες, φαίνεται ότι ένα γινόμενο ab είναι ισοϋπόλοιπο με το $0 \pmod 5$ μόνο αν το a ή το b είναι $\equiv 0 \pmod 5$. Αυτό υποδεικνύει τον γενικό νόμο

(7) $ab \equiv 0 \pmod d$ μόνο αν είτε $a \equiv 0$ είτε $b \equiv 0 \pmod d$,

που είναι μια επέκταση του συνήθους νόμου για ακεραίους, σύμφωνα με τον οποίο $ab = 0$ μόνο αν $a = 0$ ή $b = 0$. *Ο νόμος* (7) *ισχύει μόνο όταν το modulus* d *είναι πρώτος αριθμός*. Διότι η ισοϋπολοιπική σχέση

$$ab \equiv 0 \qquad (\text{mod } d)$$

σημαίνει ότι ο d διαιρεί το ab, και όπως έχουμε δει ένας πρώτος αριθμός d διαιρεί ένα γινόμενο ab μόνο αν διαιρεί τον a ή τον b· δηλαδή, μόνο αν

$$a \equiv 0 \qquad (\text{mod } d) \quad \text{ή} \quad b \equiv 0 \qquad (\text{mod } d).$$

Αν ο d δεν είναι πρώτος, ο νόμος δεν ισχύει απαραίτητα· διότι μπορούμε να γράψουμε $d = r \cdot s$, όπου οι r και s είναι μικρότεροι του d, οπότε

$$r \not\equiv 0 \qquad (\text{mod } d), \qquad s \not\equiv 0 \qquad (\text{mod } d),$$

αλλά

$$rs = d \equiv 0 \qquad (\text{mod } d).$$

Για παράδειγμα, $2 \not\equiv 0 \pmod 6$ και $3 \not\equiv 0 \pmod 6$, αλλά $2 \cdot 3 = 6 \equiv 0 \pmod 6$.

Άσκηση: Δείξτε ότι ο ακόλουθος *νόμος απαλοιφής* ισχύει για ισοϋπολοιπικές σχέσεις ως προς ένα modulus που είναι πρώτος αριθμός:

Αν $ab \equiv ac$ και $a \not\equiv 0$, τότε $b \equiv c$.

Ασκήσεις: 1) Με ποιον αριθμό μεταξύ του 0 και του 6 (συμπεριλαμβανομένων αυτών των δύο) είναι το γινόμενο $11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19$ ισοϋπόλοιπο modulo 7;

2) Με ποιον αριθμό μεταξύ του 0 και του 12 (συμπεριλαμβανομένων αυτών των δύο) είναι το $3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 113$ ισοϋπόλοιπο modulo 13;

3) Με ποιον αριθμό μεταξύ του 0 και του 4 (συμπεριλαμβανομένων αυτών των δύο) είναι το άθροισμα $1 + 2 + 2^2 + \cdots + 2^{19}$ ισοϋπόλοιπο modulo 5;

2. Θεώρημα του Fermat

Τον δέκατο έβδομο αιώνα, ο Fermat, ο θεμελιωτής της σύγχρονης θεωρίας αριθμών, ανακάλυψε ένα σημαντικότατο θεώρημα: *Αν* p *είναι οποιοσδήποτε πρώτος ο οποίος δεν διαιρεί τον ακέραιο* a*, τότε*

$$a^{p-1} \equiv 1 \qquad (\text{mod } p).$$

Αυτό σημαίνει ότι η $(p-1)$-οστή δύναμη του a αφήνει υπόλοιπο 1 όταν διαιρείται με τον p.

Κάποιοι από τους προηγούμενους υπολογισμούς μας επιβεβαιώνουν αυτό το θεώρημα· π.χ., βρήκαμε ότι $10^6 \equiv 1 \pmod 7$, $10^2 \equiv 1 \pmod 3$ και

$10^{10} \equiv 1 \pmod{11}$. Αντίστοιχα μπορούμε να δείξουμε ότι $2^{12} \equiv 1 \pmod{13}$ και $5^{10} \equiv 1 \pmod{11}$. Για να ελέγξουμε τις τελευταίες ισοϋπολοιπικές σχέσεις δεν χρειάζεται να υπολογίσουμε πραγματικά τόσο υψηλές δυνάμεις, διότι μπορούμε να εκμεταλλευτούμε την πολλαπλασιαστική ιδιότητα αυτών των σχέσεων:

$$\begin{aligned} &2^4 = 16 \equiv 3 && \pmod{13}, \\ &2^8 \equiv 9 \equiv -4 && \pmod{13}, \\ &2^{12} \equiv -4 \cdot 3 = -12 \equiv 1 && \pmod{13}. \end{aligned} \qquad \begin{aligned} &5^2 \equiv 3 && \pmod{11}, \\ &5^4 \equiv 9 \equiv -2 && \pmod{11}, \\ &5^8 \equiv 4 && \pmod{11}, \\ &5^{10} \equiv 3 \cdot 4 = 12 \equiv 1 && \pmod{11}. \end{aligned}$$

Για να αποδείξουμε το θεώρημα του Fermat, θεωρούμε τα πολλαπλάσια του a:

$$m_1 = a, \quad m_2 = 2a, \quad m_3 = 3a, \quad \dots, \quad m_{p-1} = (p-1)a.$$

Κανένα ζεύγος αυτών των ακεραίων δεν μπορεί να είναι ισοϋπόλοιποι modulo p, διότι τότε το p θα ήταν παράγοντας του $m_r - m_s = (r-s)a$ για κάποιο ζεύγος ακεραίων r, s με $1 \leq r < s \leq (p-1)$. Αλλά σύμφωνα με τον νόμο (7) αυτό δεν μπορεί να συμβαίνει· διότι αφού το $s-r$ είναι μικρότερο του p, το p δεν είναι παράγοντας του $s-r$, ενώ εξ υποθέσεως το p δεν είναι παράγοντας του a. Ομοίως, κανένας από αυτούς τους αριθμούς δεν μπορεί να είναι ισοϋπόλοιπος με το 0. Επομένως, οι αριθμοί $m_1, m_2, \dots, m_{p-1}$ θα πρέπει να είναι αντίστοιχα ισοϋπόλοιποι με τους αριθμούς $1, 2, 3, \dots, p-1$, με κάποια διάταξη. Έπεται ότι

$$m_1 m_2 \cdots m_{p-1} = 1 \cdot 2 \cdot 3 \cdots (p-1) a^{p-1} \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p},$$

ή, αν συμβολίσουμε χάριν συντομίας με K το γινόμενο $1 \cdot 2 \cdot 3 \cdots (p-1)$,

$$K(a^{p-1} - 1) \equiv 0 \pmod{p}.$$

Αλλά το K δεν διαιρείται με το p, διότι δεν διαιρείται κανένας από τους παράγοντές του· συνεπώς, βάσει του νόμου (7), το $(a^{p-1}-1)$ θα πρέπει να διαιρείται με το p, δηλαδή

$$a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Αυτό είναι το θεώρημα του Fermat.

Για να ελέγξουμε το θεώρημα ακόμα μία φορά, ας πάρουμε $p = 23$ και $a = 5$. Τότε έχουμε, παντού modulo 23, ότι $5^2 \equiv 2$, $5^4 \equiv 4$, $5^8 \equiv 16 \equiv -7$, $5^{16} \equiv 49 \equiv 3$, $5^{20} \equiv 12$, $5^{22} \equiv 24 \equiv 1$. Με $a = 4$ αντί για 5, παίρνουμε, και πάλι modulo 23, $4^2 \equiv -7$, $4^3 \equiv -28 \equiv -5$, $4^4 \equiv -20 \equiv 3$, $4^8 \equiv 9$, $4^{11} \equiv -45 \equiv 1$, $4^{22} \equiv 1$.

Στο παραπάνω παράδειγμα με $a = 4, p = 23$, και σε άλλα, παρατηρούμε ότι όχι μόνο η $(p-1)$-οστή δύναμη του a, αλλά και μια μικρότερη δύναμη μπορεί να είναι ισοϋπόλοιπη του 1. Ισχύει πάντα ότι η μικρότερη τέτοια δύναμη, στην προκειμένη περίπτωση η 11, είναι διαιρέτης του $p - 1$. (Βλ. την παρακάτω Άσκηση 3.)

Ασκήσεις: 1) Δείξτε με παρόμοιο υπολογισμό ότι $2^8 \equiv 1 \pmod{17}$, $3^8 \equiv -1 \pmod{17}$, $3^{14} \equiv -1 \pmod{29}$, $2^{14} \equiv -1 \pmod{29}$, $4^{14} \equiv 1 \pmod{29}$, $5^{14} \equiv 1 \pmod{29}$.

2) Ελέγξτε το θεώρημα του Fermat για $p = 5, 7, 11, 17$ και 23 με διαφορετικές τιμές του a.

3) Αποδείξτε το γενικό θεώρημα: Ο μικρότερος θετικός ακέραιος e για τον οποίο $a^e \equiv 1 \pmod{p}$ θα πρέπει να είναι διαιρέτης του $p - 1$. (Υπόδειξη: Διαιρώντας το $p - 1$ με e, παίρνουμε

$$p - 1 = ke + r,$$

όπου $0 \leq r < e$, και χρησιμοποιούμε το γεγονός ότι $a^{p-1} \equiv a^e \equiv 1 \pmod{p}$).

3. Τετραγωνικά υπόλοιπα

Ανατρέχοντας στα παραδείγματα για το θεώρημα του Fermat, βρίσκουμε ότι όχι μόνο $a^{p-1} \equiv 1 \pmod{p}$ πάντα, αλλά (αν ο p είναι πρώτος αριθμός διάφορος του 2, και επομένως περιττός και της μορφής $p = 2p' + 1$) ότι για κάποιες τιμές του a ισχύει ότι $a^{p'} = a^{(p-1)/2} \equiv 1 \pmod{p}$. Το γεγονός αυτό υποδεικνύει μια αλυσίδα από ενδιαφέρουσες διερευνήσεις. Μπορούμε να γράψουμε το θεώρημα στην εξής μορφή:

$$a^{p-1} - 1 = a^{2p'} - 1 = (a^{p'} - 1)(a^{p'} + 1) \equiv 0 \pmod{p}.$$

Δεδομένου ότι ένα γινόμενο διαιρείται με p μόνο αν διαιρείται ένας από τους παράγοντές του, φαίνεται αμέσως ότι είτε το $a^{p'} - 1$ είτε το $a^{p'} + 1$ θα πρέπει να διαιρείται με τον p, οπότε για κάθε πρώτο $p > 2$ και για κάθε αριθμό a που δεν διαιρείται με τον p, είτε

$$a^{(p-1)/2} \equiv 1 \quad \text{είτε} \quad a^{(p-1)/2} \equiv -1 \pmod{p}.$$

Από τις απαρχές της σύγχρονης θεωρίας αριθμών, οι μαθηματικοί έχουν ενδιαφερθεί να προσδιορίσουν για ποιους αριθμούς a έχουμε την πρώτη περίπτωση και για ποιους τη δεύτερη. Έστω ότι ο a είναι ισοϋπόλοιπος modulo p με το τετράγωνο κάποιου αριθμού x,

$$a \equiv x^2 \pmod{p}.$$

Τότε, $a^{(p-1)/2} \equiv x^{p-1}$, το οποίο σύμφωνα με το θεώρημα του Fermat είναι ισοϋπόλοιπο με το 1 modulo p. Ένας αριθμός a, όχι πολλαπλάσιο του p, που

είναι ισοϋπόλοιπος modulo p με το τετράγωνο κάποιου αριθμού ονομάζεται *τετραγωνικό υπόλοιπο* του p, ενώ ένας αριθμός b, όχι πολλαπλάσιο του p, που δεν είναι ισοϋπόλοιπος με κανένα τετράγωνο ονομάζεται *τετραγωνικό μη υπόλοιπο* του p. Όπως μόλις είδαμε, κάθε τετραγωνικό υπόλοιπο a του p ικανοποιεί την ισοϋπολοιπική σχέση $a^{(p-1)/2} \equiv 1 \pmod{p}$. Μπορεί να αποδειχθεί χωρίς ιδιαίτερη δυσκολία ότι για κάθε μη υπόλοιπο b ισχύει η ισοϋπολοιπική σχέση $b^{(p-1)/2} \equiv -1 \pmod{p}$. Επιπλέον, θα δείξουμε τώρα ότι ανάμεσα στους αριθμούς $1, 2, 3, \ldots, p-1$ υπάρχουν ακριβώς $(p-1)/2$ τετραγωνικά υπόλοιπα και $(p-1)/2$ μη υπόλοιπα.

Αν και οι απευθείας υπολογισμοί έδωσαν τη δυνατότητα να συγκεντρωθούν άφθονα εμπειρικά δεδομένα, αρχικά δεν ήταν εύκολο να ανακαλυφθούν γενικοί νόμοι που διέπουν την κατανομή των τετραγωνικών υπολοίπων και των μη υπολοίπων. Η πρώτη βαθιά ιδιότητα αυτών των υπολοίπων παρατηρήθηκε από τον Legendre (1752-1833), και ονομάστηκε αργότερα από τον Gauss *νόμος της τετραγωνικής αμοιβαιότητας*. Ο νόμος αυτός αφορά τη συμπεριφορά δύο διαφορετικών πρώτων p και q, και ορίζει ότι ο q είναι τετραγωνικό υπόλοιπο του p αν και μόνο αν ο p είναι τετραγωνικό υπόλοιπο του q, υπό την προϋπόθεση ότι το γινόμενο $\left(\dfrac{p-1}{2} \cdot \dfrac{q-1}{2}\right)$ είναι *άρτιο*. Στην περίπτωση που το γινόμενο αυτό είναι *περιττό*, η κατάσταση αντιστρέφεται, οπότε ο p είναι υπόλοιπο του q αν και μόνο αν ο q είναι *μη υπόλοιπο* του p. Ένα από τα επιτεύγματα του νεαρού Gauss ήταν ότι έδωσε την πρώτη αυστηρή απόδειξη αυτού του αξιοσημείωτου θεωρήματος, που για πολύ καιρό αποτελούσε πρόκληση για τους μαθηματικούς. Η πρώτη απόδειξη του Gauss δεν ήταν επ' ουδενί απλή, και ακόμα και σήμερα ο νόμος της αμοιβαιότητας δεν είναι τόσο εύκολο να αποδειχθεί, παρότι έχουν δημοσιευτεί πολλές διαφορετικές αποδείξεις. Η πραγματική σπουδαιότητα του νόμου αναδείχθηκε μόνο πρόσφατα, σε σύνδεση με σύγχρονες εξελίξεις στην αλγεβρική θεωρία αριθμών.*

Ως ένα παράδειγμα που καταδεικνύει την κατανομή των τετραγωνικών υπολοίπων, ας επιλέξουμε $p = 7$. Τότε, δεδομένου ότι

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 2, \quad 4^2 \equiv 2, \quad 5^2 \equiv 4, \quad 6^2 \equiv 1,$$

όλα modulo 7, και δεδομένου ότι τα υπόλοιπα τετράγωνα επαναλαμβάνουν αυτή την ακολουθία, τα τετραγωνικά υπόλοιπα του 7 είναι οι αριθμοί που είναι ισοϋπόλοιποι με τα 1, 2 ή 4, ενώ τα μη υπόλοιπα είναι ισοϋπόλοιπα με τα 3, 5 ή 6. Στη γενική περίπτωση, τα τετραγωνικά υπόλοιπα του p συνίστανται στους αριθμούς που είναι ισοϋπόλοιποι με τους $1^2, 2^2, \ldots, (p-1)^2$. Αλλά αυτοί είναι

*Σ.τ.Ε.: Το 9ο πρόβλημα του Hilbert αφορά την αναζήτηση μιας γενίκευσης του νόμου αμοιβαιότητας για τη μη αβελιανή θεωρία κλάσεων σωμάτων, και παραμένει άλυτο μέχρι σήμερα.

ισοϋπόλοιποι κατά ζεύγη, διότι

$$x^2 \equiv (p-x)^2 \pmod{p} \quad (\text{π.χ., } 2^2 \equiv 5^2 \pmod{7}),$$

αφού $(p-x)^2 = p^2 - 2px + x^2 \equiv x^2 \pmod{p}$. Επομένως, οι μισοί από τους αριθμούς $1, 2, \ldots, p-1$ είναι τετραγωνικά υπόλοιπα του p και οι μισοί είναι τετραγωνικά μη υπόλοιπα.

Για να δώσουμε ένα παράδειγμα του νόμου της τετραγωνικής αμοιβαιότητας, έστω $p = 5$, $q = 11$. Δεδομένου ότι $11 \equiv 1^2 \pmod{5}$, το 11 είναι τετραγωνικό υπόλοιπο $\pmod{5}$· δεδομένου ότι το γινόμενο $[(5-1)/2][(11-1)/2]$ είναι άρτιο, από τον νόμο αμοιβαιότητας έχουμε ότι το 5 είναι τετραγωνικό υπόλοιπο $\pmod{11}$. Προς επιβεβαίωση αυτού, παρατηρούμε ότι $5 \equiv 4^2 \pmod{11}$. Από την άλλη πλευρά, αν $p = 7$, $q = 11$, τότε το γινόμενο $[(7-1)/2][(11-1)/2]$ είναι περιττό, και όντως το 11 είναι υπόλοιπο $\pmod{7}$ (δεδομένου ότι $11 \equiv 2^2 \pmod{7}$), ενώ το 7 είναι μη υπόλοιπο $\pmod{11}$.

Ασκήσεις: 1) $6^2 = 36 \equiv 13 \pmod{23}$. Είναι το 23 τετραγωνικό υπόλοιπο $\pmod{13}$;

2) Έχουμε δει ότι $x^2 \equiv (p-x)^2 \pmod{p}$. Δείξτε ότι αυτές είναι οι *μόνες* ισοϋπολοιπικές σχέσεις ανάμεσα στους αριθμούς $1^2, 2^2, 3^2, \ldots, (p-1)^2$.

§3. ΠΥΘΑΓΟΡΕΙΟΙ ΑΡΙΘΜΟΙ ΚΑΙ ΤΟ ΤΕΛΕΥΤΑΙΟ ΘΕΩΡΗΜΑ ΤΟΥ FERMAT

Ένα ενδιαφέρον ερώτημα στη θεωρία αριθμών συνδέεται με το πυθαγόρειο θεώρημα. Οι Έλληνες γνώριζαν ότι ένα τρίγωνο με πλευρές $3, 4, 5$ είναι ορθογώνιο. Το γεγονός αυτό υποδεικνύει το εξής γενικό ερώτημα: Ποια άλλα ορθογώνια τρίγωνα έχουν πλευρές των όποιων τα μήκη είναι ακέραια πολλαπλάσια ενός μοναδιαίου μήκους; Το πυθαγόρειο θεώρημα εκφράζεται αλγεβρικά μέσω της εξίσωσης

$$a^2 + b^2 = c^2, \tag{1}$$

όπου a και b είναι τα μήκη των κάθετων πλευρών ενός ορθογώνιου τριγώνου και c είναι το μήκος της υποτείνουσας. Επομένως, το πρόβλημα της εύρεσης *όλων* των ορθογώνιων τριγώνων με πλευρές ακέραιου μήκους είναι ισοδύναμο με το πρόβλημα της εύρεσης όλων των ακέραιων λύσεων (a, b, c) της εξίσωσης (1). Κάθε τέτοια τριάδα αριθμών ονομάζεται *πυθαγόρεια τριάδα αριθμών*.

Το πρόβλημα της εύρεσης όλων των πυθαγόρειων τριάδων αριθμών μπορεί να λυθεί πολύ απλά. Αν τα a, b και c αποτελούν μια πυθαγόρεια τριάδα αριθμών, οπότε $a^2 + b^2 = c^2$, τότε θέτουμε, χάριν συντομογραφίας, $a/c = x$, $b/c = y$. Τα x και y είναι ρητοί αριθμοί για τους οποίους ισχύει ότι $x^2 + y^2 = 1$. Επομένως, έχουμε $y^2 = (1-x)(1+x)$, ή $y/(1+x) = (1-x)/y$. Η κοινή τιμή των δύο μελών αυτής της ισότητας είναι ένας αριθμός t ο οποίος μπορεί

να εκφραστεί ως πηλίκο δύο ακεραίων, u/v. Μπορούμε τώρα να γράψουμε $y = t(1 + x)$ και $(1 - x) = ty$, ή

$$tx - y = -t, \quad x + ty = 1.$$

Από αυτό το σύστημα εξισώσεων, βρίσκουμε αμέσως ότι

$$x = \frac{1 - t^2}{1 + t^2}, \quad y = \frac{2t}{1 + t^2}.$$

Αντικαθιστώντας τα x, y και t, έχουμε ότι

$$\frac{a}{c} = \frac{v^2 - u^2}{u^2 + v^2}, \quad \frac{b}{c} = \frac{2uv}{u^2 + v^2}.$$

Επομένως,

$$\begin{aligned} a &= (v^2 - u^2)r, \\ b &= (2uv)r, \\ c &= (u^2 + v^2)r, \end{aligned} \tag{2}$$

για κάποιον ρητό παράγοντα αναλογίας r. Από αυτό βλέπουμε ότι αν (a, b, c) είναι μια πυθαγόρεια τριάδα αριθμών, τότε τα a, b, c είναι ανάλογα των $v^2 - u^2$, $2uv$, $u^2 + v^2$, αντίστοιχα. Αντιστρόφως, είναι εύκολο να δούμε ότι κάθε τριάδα (a, b, c) που ορίζεται μέσω των (2) είναι μια πυθαγόρεια τριάδα, διότι από τις (2) βρίσκουμε ότι

$$\begin{aligned} a^2 &= (u^4 - 2u^2v^2 + v^4)r^2, \\ b^2 &= (4u^2v^2)r^2, \\ c^2 &= (u^4 + 2u^2v^2 + v^4)r^2, \end{aligned}$$

οπότε $a^2 + b^2 = c^2$.

Το αποτέλεσμα αυτό μπορεί να απλοποιηθεί κάπως. Από κάθε πυθαγόρεια τριάδα αριθμών (a, b, c) μπορούμε να πάρουμε άπειρες το πλήθος άλλες πυθαγόρειες τριάδες αριθμών (sa, sb, sc) για κάθε θετικό ακέραιο s. Επομένως, από την $(3, 4, 5)$ παίρνουμε τις $(6, 8, 10)$, $(9, 12, 15)$, κ.λπ. Τέτοιες τριάδες δεν είναι ουσιωδώς διαφορετικές μεταξύ τους, διότι αντιστοιχούν σε όμοια ορθογώνια τρίγωνα. Για τον λόγο αυτό, ορίζουμε ως *πρωταρχική* πυθαγόρεια τριάδα αριθμών μια τριάδα στην οποία τα a, b και c δεν έχουν κοινό παράγοντα. Μπορεί τότε να δειχθεί ότι *οι τύποι*

$$\begin{aligned} a &= v^2 - u^2, \\ b &= 2uv, \\ c &= u^2 + v^2, \end{aligned}$$

για οποιουσδήποτε θετικούς ακεραίους u και v με $v > u$, όπου οι u και v δεν έχουν κοινό παράγοντα και δεν είναι αμφότεροι περιττοί, δίνουν όλες τις πρωταρχικές πυθαγόρειες τριάδες αριθμών.

**Άσκηση:* Αποδείξτε την τελευταία πρόταση.

Κάποια παραδείγματα πρωταρχικών πυθαγόρειων τριάδων αριθμών είναι τα εξής: $u = 2, v = 1 : (3, 4, 5)$, $u = 3, v = 2 : (5, 12, 13)$, $u = 4, v = 3 : (7, 24, 25)$, …, $u = 10, v = 7 : (51, 140, 149)$, κ.λπ.

Από το αποτέλεσμα αυτό σχετικά με τους πυθαγόρειους αριθμούς ανακύπτει φυσιολογικά το ερώτημα αν μπορούν να βρεθούν ακέραιοι a, b, c για τους οποίους $a^3 + b^3 = c^3$ ή $a^4 + b^4 = c^4$, ή, εν γένει, αν για έναν δεδομένο θετικό ακέραιο εκθέτη $n > 2$, η εξίσωση

$$a^n + b^n = c^n \tag{3}$$

μπορεί να λυθεί με θετικούς ακεραίους a, b, c. Μια απάντηση στο ερώτημα αυτό έδωσε ο Fermat με έναν εντυπωσιακό τρόπο. Ο Fermat είχε μελετήσει το έργο του Διόφαντου, του αρχαίου μαθηματικού που είχε συνεισφέρει στη θεωρία αριθμών, και συνήθιζε να προσθέτει σχόλια στο περιθώριο του αντιτύπου του. Παρότι διατύπωσε πολλά θεωρήματα εκεί χωρίς να μπει στον κόπο να παρουσιάσει αποδείξεις, όλα αυτά τα θεωρήματα έχουν στη συνέχεια αποδειχθεί, με μία σημαντική εξαίρεση. Στα σχόλιά του σχετικά με τους πυθαγόρειους αριθμούς, ο Fermat ανέφερε ότι *η εξίσωση (3) δεν μπορεί να λυθεί στους ακεραίους για κανένα $n > 2$*, αλλά ότι η κομψή απόδειξη που είχε βρει ήταν δυστυχώς πολύ μακροσκελής για το περιθώριο στο οποίο έγραφε.

Η γενική πρόταση του Fermat δεν έχει ποτέ αποδειχθεί ούτε καταρριφθεί,[*] παρά τις προσπάθειες κάποιων από τους μεγαλύτερους μαθηματικούς από την εποχή του και έπειτα. Μάλιστα, το θεώρημα έχει αποδειχθεί για πολλές τιμές του n, και συγκεκριμένα για όλα τα $n < 619$, αλλά όχι για όλα τα n, παρότι δεν έχει παρουσιαστεί ποτέ κάποιο αντιπαράδειγμα. Αν και το θεώρημα καθ' εαυτό δεν είναι τόσο σημαντικό από μαθηματικής πλευράς, οι προσπάθειες απόδειξής του έχουν αποτελέσει το έναυσμα για πολλές σημαντικές διερευνήσεις στη θεωρία αριθμών. Το πρόβλημα έχει επίσης εξάψει μεγάλο ενδιαφέρον σε μη μαθηματικούς κύκλους, εν μέρει λόγω ενός βραβείου 100.000 μάρκων που είχε προσφερθεί για εκείνον που θα βρει πρώτος μια λύση, και το οποίο τηρούνταν ως καταπίστευμα στη Βασιλική Ακαδημία του Γκαίττινγκεν. Μέχρις ότου ο μεταπολεμικός πληθωρισμός στη Γερμανία να εξανεμίσει τη νομισματική αξία αυτού του βραβείου, υποβάλλονταν κάθε χρόνο στους διαχειριστές του καταπιστεύματος πολλές λανθασμένες «λύσεις». Ακόμα και σοβαροί μαθηματικοί είχε συμβεί να αυταπατηθούν και να παρουσιάσουν σε συναδέλφους τους

[*] Σ.τ.Ε.: Αντίστοιχα και εδώ έχει σημειωθεί σημαντική πρόοδος στα χρόνια που μεσολάβησαν. Ο Ian Stewart απαριθμεί κάποια από τα σημαντικότερα αποτελέσματα στο Κεφ. IX.

ή να δημοσιεύσουν αποδείξεις οι οποίες κατέρρευσαν όταν ανακαλύφθηκε σε αυτές κάποιο επιπόλαιο σφάλμα. Το γενικό ενδιαφέρον για το ζήτημα φαίνεται να έχει ατονήσει από την υποτίμηση του μάρκου και ύστερα, παρότι περιστασιακά εμφανίζεται στα ΜΜΕ μια ανακοίνωση ότι το πρόβλημα έχει επιλυθεί από κάποιον μέχρι τούδε άγνωστο ιδιοφυή μελετητή.

§4. Ο ΕΥΚΛΕΙΔΕΙΟΣ ΑΛΓΟΡΙΘΜΟΣ

1. Γενική θεωρία

Ο αναγνώστης είναι εξοικειωμένος με τη συνήθη διαδικασία της μακράς διαίρεσης ενός ακεραίου a με έναν άλλο ακέραιο b και γνωρίζει ότι η συγκεκριμένη διαδικασία μπορεί να εκτελεστεί μέχρις ότου το υπόλοιπο να γίνει μικρότερο από τον διαιρέτη. Συνεπώς, αν $a = 648$ και $b = 7$, έχουμε πηλίκο $q = 92$ και υπόλοιπο $r = 4$.

$$\begin{array}{r|l} 648 & 7 \\ \underline{63} & \hline 92 \\ 18 & \\ \underline{14} & \\ 4 & \end{array} \qquad 648 = 7 \cdot 92 + 4.$$

Αυτό μπορεί να διατυπωθεί ως γενικό θεώρημα: *Αν a είναι οποιοσδήποτε ακέραιος και b είναι οποιοσδήποτε ακέραιος μεγαλύτερος από το 0, τότε μπορούμε πάντα να βρούμε έναν ακέραιο q τέτοιον ώστε*

$$a = b \cdot q + r, \tag{1}$$

όπου r είναι ένας ακέραιος που ικανοποιεί την ανισότητα $0 \leq r < b$.

Για να αποδείξουμε αυτή την πρόταση χωρίς να χρησιμοποιήσουμε τη διαδικασία της μακράς διαίρεσης, αρκεί να παρατηρήσουμε ότι οποιοσδήποτε ακέραιος a είναι είτε ο ίδιος πολλαπλάσιο του b,

$$a = bq,$$

είτε βρίσκεται ανάμεσα σε δύο διαδοχικά πολλαπλάσια του b,

$$bq < a < b(q + 1) = bq + b.$$

Στην πρώτη περίπτωση, η εξίσωση (1) ισχύει με $r = 0$. Στη δεύτερη περίπτωση έχουμε, από την πρώτη από τις παραπάνω ανισότητες,

$$a - bq = r > 0,$$

ενώ από τη δεύτερη ανισότητα έχουμε

$$a - bq = r < b,$$

οπότε $0 < r < b$, όπως απαιτείται από την (1).

Από αυτό το απλό γεγονός θα συναγάγουμε μια ποικιλία από σημαντικά επακόλουθα. Το πρώτο από αυτά είναι μια μέθοδος για την εύρεση του μέγιστου κοινού διαιρέτη δύο ακεραίων.

Έστω a και b δύο οποιοιδήποτε ακέραιοι, όχι αμφότεροι ίσοι με 0, και ας θεωρήσουμε το σύνολο όλων των θετικών ακεραίων που διαιρούν αμφότερους τους a και b. Το σύνολο αυτό είναι σίγουρα πεπερασμένο, διότι αν ο a, για παράδειγμα, είναι $\neq 0$, τότε κανένας ακέραιος μεγαλύτερος σε μέγεθος από τον a δεν μπορεί να είναι διαιρέτης του a, για να μην πούμε τίποτα για τον b. Συνεπώς, δεν μπορεί παρά να υπάρχει πεπερασμένο πλήθος κοινών διαιρετών των a και b, και έστω d ο μεγαλύτερος από αυτούς. Ο ακέραιος d ονομάζεται *μέγιστος κοινός διαιρέτης* των a και b, και γράφεται $d = (a, b)$. Συνεπώς, για $a = 8$ και $b = 12$ βρίσκουμε με απευθείας δοκιμή ότι $(8, 12) = 4$, ενώ για $a = 5$ και $b = 9$ βρίσκουμε ότι $(5, 9) = 1$. Όταν οι a και b είναι μεγάλοι, λόγου χάριν $a = 1804$ και $b = 328$, η προσπάθεια να βρούμε τον (a, b) με δοκιμή και σφάλμα θα ήταν αρκετά επίπονη. Μια σύντομη και σίγουρη μέθοδο μας παρέχει ο *ευκλείδειος αλγόριθμος*. (Ένας αλγόριθμος είναι μια συστηματική μέθοδος υπολογισμού.) Βασίζεται στο γεγονός ότι από οποιαδήποτε σχέση της μορφής

$$a = b \cdot q + r \tag{2}$$

έπεται ότι

$$(a, b) = (b, r). \tag{3}$$

Διότι κάθε αριθμός u ο οποίος διαιρεί αμφότερους τους a και b,

$$a = su, \quad b = tu,$$

διαιρεί επίσης τον r, αφού $r = a - bq = su - qtu = (s - qt)u$· και αντιστρόφως, κάθε αριθμός v που διαιρεί τους b και r,

$$b = s'v, \quad r = t'v,$$

διαιρεί επίσης τον a, αφού $a = bq + r = s'vq + t'v = (s'q + t')v$. Συνεπώς *κάθε* κοινός διαιρέτης των a και b είναι ταυτόχρονα κοινός διαιρέτης των b και r, και αντιστρόφως. Δεδομένου, επομένως, ότι το σύνολο *όλων* των κοινών διαιρετών των a και b συμπίπτει με το σύνολο όλων των κοινών διαιρετών των b και r, ο *μέγιστος* κοινός διαιρέτης των a και b θα πρέπει να είναι ίσος με τον μέγιστο κοινό διαιρέτη των b και r, οπότε η (3) έχει αποδειχθεί. Η χρησιμότητα αυτής της σχέσης θα γίνει αντιληπτή αμέσως παρακάτω.

Ας επανέλθουμε στο ζήτημα της εύρεσης του μέγιστου κοινού διαιρέτη του 1804 και του 328. Με συνήθη μακρά διαίρεση

$$\begin{array}{r|l} 1804 & 328 \\ \underline{1640} & 5 \\ 164 & \end{array}$$

βρίσκουμε ότι

$$1804 = 5 \cdot 328 + 164.$$

Συνεπώς, από την (3) συμπεραίνουμε ότι

$$(1804, 328) = (328, 164).$$

Παρατηρούμε ότι το πρόβλημα της εύρεσης του $(1804, 328)$ έχει αντικατασταθεί από ένα πρόβλημα που περιλαμβάνει μικρότερους αριθμούς. Μπορούμε να συνεχίσουμε αυτή τη διαδικασία. Δεδομένου ότι

$$\begin{array}{r|l} 328 & 164 \\ \underline{328} & 2 \\ \mathbf{0} & \end{array}$$

έχουμε ότι $328 = 2 \cdot 164 + 0$, οπότε $(328, 164) = (164, 0) = 164$. Άρα, $(1804, 328) = (328, 164) = (164, 0) = 164$, που είναι το ζητούμενο αποτέλεσμα.

Αυτή η διαδικασία για την εύρεση του μέγιστου κοινού διαιρέτη δύο αριθμών παρουσιάζεται σε γεωμετρική μορφή στα *Στοιχεία* του Ευκλείδη. Για τυχόντες ακεραίους a και b, όχι αμφότερους ίσους με 0, μπορεί να περιγραφεί αλγεβρικά ως εξής.

Μπορούμε να υποθέσουμε ότι $b \neq 0$, δεδομένου ότι $(a, 0) = a$. Τότε, με διαδοχική διαίρεση μπορούμε να γράψουμε

$$\begin{array}{ll} a = bq_1 + r_1 & (0 < r_1 < b) \\ b = r_1 q_2 + r_2 & (0 < r_2 < r_1) \\ r_1 = r_2 q_3 + r_3 & (0 < r_3 < r_2) \\ r_2 = r_3 q_4 + r_4 & (0 < r_4 < r_3) \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots \end{array} \tag{4}$$

για όσο τα υπόλοιπα $r_1, r_2, r_3, \ldots$ είναι διάφορα του 0. Από τις ανισότητες στα δεξιά, βλέπουμε ότι τα διαδοχικά υπόλοιπα σχηματίζουν μια συνεχώς φθίνουσα ακολουθία θετικών αριθμών:

$$b > r_1 > r_2 > r_3 > r_4 > \ldots > 0. \tag{5}$$

Συνεπώς, μετά από b το πολύ βήματα (συχνά πολύ λιγότερα, καθώς η διαφορά ανάμεσα σε δύο διαδοχικά r είναι συνήθως μεγαλύτερη από 1) θα πρέπει να εμφανιστεί το υπόλοιπο 0:

$$\begin{aligned} r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1} + 0. \end{aligned}$$

Όταν συμβεί αυτό, ξέρουμε ότι

$$(a, b) = r_n.$$

με άλλα λόγια, ο (a, b) *είναι το τελευταίο θετικό υπόλοιπο στην ακολουθία (5)*. Αυτό έπεται από τη διαδοχική εφαρμογή της ισότητας (3) στις εξισώσεις (4), διότι από τις διαδοχικές γραμμές της (4) έχουμε

$$\begin{aligned}(a, b) = (b, r_1), \qquad (b, r_1) = (r_1, r_2), \qquad (r_1, r_2) = (r_2, r_3),\\ (r_2, r_3) = (r_3, r_4), \qquad \dots, \qquad (r_{n-1}, r_n) = (r_n, 0) = r_n.\end{aligned}$$

Άσκηση: Εκτελέστε τον ευκλείδειο αλγόριθμο για να βρείτε τον μέγιστο κοινό διαιρέτη των (α) 188, 77. (β) 105, 385. (γ) 245, 193.

Από τις εξισώσεις (4) μπορεί να συναχθεί μια εξαιρετικά σημαντική ιδιότητα του (a, b). *Αν $d = (a, b)$, τότε μπορούν να βρεθούν θετικοί ή αρνητικοί ακέραιοι k και l τέτοιοι ώστε*

$$d = ka + lb. \tag{6}$$

Για να το αποδείξουμε, ας θεωρήσουμε την ακολουθία (5) των διαδοχικών υπολοίπων. Από την πρώτη εξίσωση στην (4), έχουμε

$$r_1 = a - q_1 b,$$

και επομένως το r_1 μπορεί να γραφτεί στη μορφή $k_1 a + l_1 b$ (στην περίπτωση αυτή, $k_1 = 1, l_1 = -q_1$). Από την επόμενη εξίσωση, έχουμε

$$\begin{aligned}r_2 = b - q_2 r_1 &= b - q_2(k_1 a + l_1 b)\\ &= (-q_2 k_1)a + (1 - q_2 l_1)b = k_2 a + l_2 b.\end{aligned}$$

Είναι προφανές πως η διαδικασία αυτή μπορεί να συνεχιστεί στα διαδοχικά υπόλοιπα $r_3, r_4, \dots$, μέχρι να φτάσουμε σε μια αναπαράσταση

$$r_n = ka + lb,$$

όπως ήταν το ζητούμενο.

Για παράδειγμα, ας θεωρήσουμε τον ευκλείδειο αλγόριθμο για την εύρεση του $(61, 24)$· ο μέγιστος κοινός διαιρέτης είναι 1 και η ζητούμενη αναπαράσταση για το 1 μπορεί να υπολογιστεί από τις εξισώσεις

$$\begin{gathered}61 = 2 \cdot 24 + 13, \quad 24 = 1 \cdot 13 + 11, \quad 13 = 1 \cdot 11 + 2,\\ 11 = 5 \cdot 2 + 1, \quad 2 = 2 \cdot 1 + 0.\end{gathered}$$

Από την πρώτη από αυτές τις εξισώσεις έχουμε

$$13 = 61 - 2 \cdot 24,$$

από τη δεύτερη έχουμε

$$11 = 24 - 13 = 24 - (61 - 2 \cdot 24) = -61 + 3 \cdot 24,$$

από την τρίτη έχουμε

$$2 = 13 - 11 = (61 - 2 \cdot 24) - (-61 + 3 \cdot 24) = 2 \cdot 61 - 5 \cdot 24,$$

και από την τέταρτη έχουμε

$$1 = 11 - 5 \cdot 2 = (-61 + 3 \cdot 24) - 5(2 \cdot 61 - 5 \cdot 24) = -11 \cdot 61 + 28 \cdot 24.$$

2. Εφαρμογή στο θεμελιώδες θεώρημα της αριθμητικής

Το γεγονός ότι ο $d = (a, b)$ μπορεί πάντα να γραφτεί στη μορφή $d = ka + lb$ μπορεί να χρησιμοποιηθεί για να δοθεί μια απόδειξη του θεμελιώδους θεωρήματος της αριθμητικής ανεξάρτητη από την απόδειξη που δώσαμε στη σελ. 25. Αρχικά θα αποδείξουμε, ως λήμμα, το πόρισμα της σελ. 26, και κατόπιν από αυτό το λήμμα θα συναγάγουμε το θεμελιώδες θεώρημα, αντιστρέφοντας με αυτό τον τρόπο την προηγούμενη σειρά της απόδειξης.

Λήμμα: Αν ένας πρώτος p διαιρεί ένα γινόμενο ab, τότε ο p θα πρέπει να διαιρεί τον a ή τον b.

Αν ένας πρώτος p δεν διαιρεί τον ακέραιο a, τότε $(a, p) = 1$, διότι οι μόνοι διαιρέτες του p είναι το p και το 1. Επομένως, μπορούμε να βρούμε ακεραίους k και l τέτοιους ώστε

$$1 = ka + lp.$$

Πολλαπλασιάζοντας και τα δύο μέλη αυτής της εξίσωσης με b παίρνουμε

$$b = kab + lpb.$$

Τώρα αν ο p διαιρεί το ab μπορούμε να γράψουμε

$$ab = pr,$$

οπότε

$$b = kpr + lpb = p(kr + lb),$$

απ' όπου είναι προφανές ότι ο p διαιρεί τον b. Συνεπώς, έχουμε δείξει ότι αν ο p διαιρεί το ab αλλά δεν διαιρεί τον a τότε θα πρέπει να διαιρεί τον b, οπότε σε κάθε περίπτωση ο p θα πρέπει να διαιρεί τον a ή τον b αν διαιρεί το ab.

Η επέκταση σε γινόμενα περισσότερων από δύο ακεραίους είναι άμεση. Για παράδειγμα, αν ο p διαιρεί το γινόμενο abc, τότε εφαρμόζοντας δύο φορές το λήμμα μπορούμε να δείξουμε ότι ο p θα πρέπει να διαιρεί τουλάχιστον έναν από τους ακεραίους a, b και c. Διότι αν ο p δεν διαιρεί κανέναν από τους a, b και c, τότε δεν μπορεί να διαιρεί το ab και άρα δεν μπορεί να διαιρεί το $(ab)c = abc$.

Άσκηση: Η επέκταση αυτού του σκεπτικού σε γινόμενα με οποιοδήποτε πλήθος n ακεραίων απαιτεί την άμεση ή έμμεση χρήση της αρχής της μαθηματικής επαγωγής. Συμπληρώστε τις λεπτομέρειες αυτού του σκεπτικού.

Από το αποτέλεσμα αυτό, το θεμελιώδες θεώρημα της αριθμητικής έπεται άμεσα. Ας υποθέσουμε ότι μας δίνονται οποιεσδήποτε δύο αναλύσεις ενός θετικού ακεραίου N σε πρώτους:

$$N = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

Δεδομένου ότι ο p_1 διαιρεί το αριστερό μέλος αυτής της εξίσωσης, θα πρέπει να διαιρεί και το δεξί μέλος, και συνεπώς, βάσει της προηγούμενης άσκησης, θα πρέπει να διαιρεί έναν από τους παράγοντες q_k. Αλλά ο q_k είναι πρώτος, και άρα ο p_1 θα πρέπει να ισούται με αυτόν τον q_k. Αφού απαλείψουμε από την εξίσωση αυτούς τους ίσους παράγοντες, έπεται ότι ο p_2 θα πρέπει να διαιρεί έναν από τους εναπομένοντες παράγοντες q_t, και άρα θα πρέπει να είναι ίσος με αυτόν. Απαλείφοντας τους p_2 και q_t, προχωράμε ομοίως με τους $p_3, \ldots, p_r$. Στο τέλος αυτής της διαδικασίας, όλοι οι p θα έχουν απαλειφθεί, αφήνοντας στο αριστερό μέλος μόνο το 1. Στο δεξί μέλος δεν είναι δυνατόν να παραμένει κανένας παράγοντας q, διότι όλοι οι q είναι μεγαλύτεροι από ένα. Άρα, οι p και οι q θα έχουν συνταιριαστεί σε ζεύγη ίσων αριθμών, γεγονός που αποδεικνύει ότι, εκτός ίσως από τη σειρά των παραγόντων, οι δύο αναλύσεις ήταν πανομοιότυπες.

3. Η συνάρτηση φ του Euler. Το θεώρημα του Fermat ξανά

Λέμε ότι δύο ακέραιοι a και b είναι *σχετικά πρώτοι* αν ο μέγιστος κοινός διαιρέτης τους είναι το 1:

$$(a, b) = 1.$$

Για παράδειγμα, οι αριθμοί 24 και 35 είναι σχετικά πρώτοι, ενώ οι 12 και 18 δεν είναι. *Αν οι a και b είναι σχετικά πρώτοι, τότε για κατάλληλα επιλεγμένους θετικούς ή αρνητικούς ακεραίους k και l μπορούμε να γράψουμε*

$$ka + lb = 1.$$

Αυτό έπεται από την ιδιότητα του (a, b) που αναφέρθηκε στη σελ. 50.

Άσκηση: Αποδείξτε το θεώρημα: *Αν ένας ακέραιος r διαιρεί ένα γινόμενο ab και είναι σχετικά πρώτος με τον a, τότε ο r θα πρέπει να διαιρεί τον b.* (Υπόδειξη: αν ο r είναι σχετικά πρώτος με τον a τότε μπορούμε να βρούμε ακεραίους k και l τέτοιους ώστε

$$kr + la = 1.$$

Πολλαπλασιάστε και τα δύο μέλη αυτής της εξίσωσης επί b.) Το θεώρημα αυτό περιλαμβάνει το λήμμα της σελ. 51 ως ειδική περίπτωση, αφού ένας πρώτος p είναι σχετικά πρώτος με έναν ακέραιο a αν και μόνο αν ο p δεν διαιρεί τον a.

Για κάθε θετικό ακέραιο n, έστω $\varphi(n)$ το *πλήθος των ακεραίων από το* 1 *μέχρι τον n οι οποίοι είναι σχετικά πρώτοι με τον n*. Η συνάρτηση $\varphi(n)$, την οποία εισήγαγε ο Euler, είναι μια «αριθμοθεωρητική συνάρτηση» μεγάλης σημασίας. Οι τιμές της $\varphi(n)$ για τις μικρότερες τιμές του n υπολογίζονται εύκολα:

$\varphi(1) = 1$ διότι ο 1 είναι σχετικά πρώτος με τον 1,
$\varphi(2) = 1$ διότι ο 1 είναι σχετικά πρώτος με τον 2,
$\varphi(3) = 2$ διότι οι 1 και 2 είναι σχετικά πρώτοι με τον 3,
$\varphi(4) = 2$ διότι οι 1 και 3 είναι σχετικά πρώτοι με τον 4,
$\varphi(5) = 4$ διότι οι $1, 2, 3, 4$ είναι σχετικά πρώτοι με τον 5,
$\varphi(6) = 2$ διότι οι $1, 5$ είναι σχετικά πρώτοι με τον 6,
$\varphi(7) = 6$ διότι οι $1, 2, 3, 4, 5, 6$ είναι σχετικά πρώτοι με τον 7,
$\varphi(8) = 4$ διότι οι $1, 3, 5, 7$ είναι σχετικά πρώτοι με τον 8,
$\varphi(9) = 6$ διότι οι $1, 2, 4, 5, 7, 8$ είναι σχετικά πρώτοι με τον 9,
$\varphi(10) = 4$ διότι οι $1, 3, 7, 9$ είναι σχετικά πρώτοι με τον 10,
κ.λπ.

Παρατηρούμε ότι $\varphi(p) = p - 1$ αν ο p είναι πρώτος· διότι ένας πρώτος p δεν έχει άλλους διαιρέτες εκτός από τον εαυτό του και το 1, και συνεπώς είναι σχετικά πρώτος με όλους τους ακεραίους $1, 2, 3, \ldots, p - 1$. Αν ο n είναι σύνθετος, και έχει ανάλυση σε πρώτους αριθμούς

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

όπου τα p αναπαριστούν διαφορετικούς πρώτους, καθέναν υψωμένο σε μια ορισμένη δύναμη, τότε

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Για παράδειγμα, αφού $12 = 2^2 \cdot 3$,

$$\varphi(12) = 12(1 - \tfrac{1}{2})(1 - \tfrac{1}{3}) = 12(\tfrac{1}{2})(\tfrac{2}{3}) = 4,$$

όπως έπρεπε. Η απόδειξη είναι μάλλον στοιχειώδης, αλλά δεν θα την παρουσιάσουμε εδώ.

**Άσκηση:* Χρησιμοποιώντας τη συνάρτηση φ του Euler, γενικεύστε το θεώρημα του Fermat, σελ. 40. Το γενικό θεώρημα έχει ως εξής: *Αν n είναι οποιοσδήποτε ακέραιος, και ο a είναι σχετικά πρώτος με τον n, τότε*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

4. Συνεχή κλάσματα. Διοφαντικές εξισώσεις

Ο ευκλείδειος αλγόριθμος για την εύρεση του μέγιστου κοινού διαιρέτη δύο ακεραίων οδηγεί αμέσως σε μια σημαντική μέθοδο για την αναπαράσταση του πηλίκου δύο ακεραίων υπό τη μορφή σύνθετου κλάσματος.

Αν εφαρμοστεί, για παράδειγμα, στους αριθμούς 840 και 611, ο ευκλείδειος αλγόριθμος δίνει τη σειρά εξισώσεων

$$\begin{aligned} 840 &= 1 \cdot 611 + 229, & 611 &= 2 \cdot 229 + 153, \\ 229 &= 1 \cdot 153 + 76, & 153 &= 2 \cdot 76 + 1, \end{aligned}$$

απ' όπου, παρεμπιπτόντως, προκύπτει ότι $(840, 611) = 1$. Από αυτές τις εξισώσεις μπορούμε να συναγάγουμε τις εξής εκφράσεις:

$$\frac{840}{611} = 1 + \frac{229}{611} = 1 + \frac{1}{611/229},$$

$$\frac{611}{229} = 2 + \frac{153}{229} = 2 + \frac{1}{229/153},$$

$$\frac{229}{153} = 1 + \frac{76}{153} = 1 + \frac{1}{153/76},$$

$$\frac{153}{76} = 2 + \frac{1}{76}.$$

Συνδυάζοντας αυτές τις εξισώσεις, παίρνουμε την ανάπτυξη του ρητού αριθμού $\dfrac{840}{611}$ στη μορφή

$$\frac{840}{611} = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{76}}}}.$$

Μια έκφραση της μορφής

$$a = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}, \tag{7}$$

όπου τα a είναι θετικοί ακέραιοι, ονομάζεται *συνεχές κλάσμα*. Ο ευκλείδειος αλγόριθμος μας δίνει μια μέθοδο για να εκφράζουμε οποιονδήποτε ρητό αριθμό σε αυτή τη μορφή.

Άσκηση: Βρείτε τις αναπτύξεις σε συνεχή κλάσματα των

$$\frac{2}{5}, \frac{43}{30}, \frac{169}{70}.$$

*Τα συνεχή κλάσματα είναι πολύ σημαντικά στον κλάδο των ανώτερων μαθηματικών που ονομάζεται διοφαντική ανάλυση. Μια *διοφαντική εξίσωση* είναι μια αλγεβρική εξίσωση με έναν ή περισσότερους αγνώστους με *ακέραιους* συντελεστές, για την οποία αναζητούνται *ακέραιες* λύσεις. Μια τέτοια εξίσωση ενδέχεται να μην έχει καμία λύση, να έχει πεπερασμένο πλήθος λύσεων, ή άπειρο πλήθος λύσεων. Η απλούστερη περίπτωση είναι η *γραμμική* διοφαντική εξίσωση με δύο αγνώστους,

$$ax + by = c, \tag{8}$$

όπου a, b και c είναι δεδομένοι ακέραιοι, και ζητούνται ακέραιες λύσεις x, y. Η πλήρης λύση μιας εξίσωσης αυτής της μορφής μπορεί να βρεθεί μέσω του ευκλείδειου αλγορίθμου.

Κατ' αρχάς, ας βρούμε τον $d = (a, b)$ μέσω του ευκλείδειου αλγορίθμου· τότε για κατάλληλη επιλογή των ακεραίων k και l,

$$ak + bl = d. \tag{9}$$

Συνεπώς, η εξίσωση (8) έχει τη συγκεκριμένη λύση $x = k$, $y = l$ για την περίπτωση $c = d$. Γενικότερα, αν c είναι οποιοδήποτε πολλαπλάσιο του d:

$$c = d \cdot q,$$

τότε από την (9) παίρνουμε

$$a(kq) = b(lq) = dq = c,$$

οπότε η (8) έχει τη συγκεκριμένη λύση $x = x^\star = kq, y = y^\star = lq$. Αντιστρόφως, αν η (8) έχει οποιαδήποτε λύση x, y για δεδομένο c, τότε το c θα πρέπει να είναι πολλαπλάσιο του $d = (a, b)$· διότι το d διαιρεί αμφότερα τα a και b, συνεπώς θα πρέπει να διαιρεί και το c. Επομένως, έχουμε αποδείξει ότι η εξίσωση (8) έχει λύση αν και μόνο αν το c είναι πολλαπλάσιο του (a, b).

Για να προσδιορίσουμε τις άλλες λύσεις της (8), παρατηρούμε ότι αν $x = x'$, $y = y'$ είναι οποιαδήποτε λύση εκτός από εκείνη, $x = x^\star$, $y = y^\star$, που βρήκαμε παραπάνω μέσω του ευκλείδειου αλγορίθμου, τότε η $x = x' - x^\star$, $y = y' - y^\star$ είναι μια λύση της «ομογενούς» εξίσωσης

$$ax + by = 0. \tag{10}$$

Διότι αν

$$ax' + by' = c \quad \text{και} \quad ax^\star + by^\star = c,$$

τότε αφαιρώντας τη δεύτερη εξίσωση από την πρώτη βρίσκουμε ότι

$$a(x' - x^\star) + b(y' - y^\star) = 0.$$

Τώρα η πιο γενική λύση της εξίσωσης (10) είναι $x = rb/(a,b), y = -ra/(a,b)$, όπου r οποιοσδήποτε ακέραιος. (Αφήνουμε την απόδειξη ως άσκηση για τον αναγνώστη. Υπόδειξη: Διαιρέστε με (a,b) και χρησιμοποιήστε την Άσκηση στη σελ. 53.) Έπεται αμέσως ότι

$$x = x^\star + rb/(a,b), \quad y = y^\star - ra/(a,b).$$

Για να συνοψίσουμε: Η γραμμική διοφαντική εξίσωση $ax + by = c$, όπου a, b και c είναι ακέραιοι, έχει λύση στους ακεραίους αν και μόνο αν το c είναι πολλαπλάσιο του (a,b). Στην τελευταία αυτή περίπτωση, μπορεί να βρεθεί μια συγκεκριμένη λύση $x = x^\star, y = y^\star$ μέσω του ευκλείδειου αλγορίθμου, και η πιο γενική λύση είναι της μορφής

$$x = x^\star + rb/(a,b), \quad y = y^\star - ra/(a,b),$$

όπου r οποιοσδήποτε ακέραιος.

Παραδείγματα: Η εξίσωση $3x + 6y = 22$ δεν έχει ακέραιη λύση, διότι $(3,6) = 3$, που δεν διαιρεί το 22.

Η εξίσωση $7x + 11y = 13$ έχει τη συγκεκριμένη λύση $x = -39, y = 26$, που βρίσκεται ως εξής:

$$11 = 1 \cdot 7 + 4, \quad 7 = 1 \cdot 4 + 3, \quad 4 = 1 \cdot 3 + 1, \quad (7,11) = 1.$$
$$1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2(11 - 7) - 7 = 2 \cdot 11 - 3 \cdot 7.$$

Συνεπώς,

$$7 \cdot (-3) + 11(2) = 1,$$
$$7 \cdot (-39) + 11(26) = 13.$$

Οι άλλες λύσεις δίνονται από τις σχέσεις

$$x = -39 + 11r, \quad y = 26 - 7r,$$

όπου r οποιοσδήποτε ακέραιος.

Άσκηση: Λύστε τις διοφαντικές εξισώσεις (α) $3x - 4y = 29$, (β) $11x + 12y = 58$, (γ) $153x - 34y = 51$.