ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
Τ.Ε.Ι. ΠΑΤΡΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ: *ΕΝΑΣ ΠΡΩΤΟΣ ΠΕΡΙΠΑΤΟΣ ΣΤΗ ΘΕΩΡΙΑ ΤΩΝ ΑΡΙΘΜΩΝ*

ΣΠΟΥΔΑΣΤΕΣ:

ΚΑΡΤΑΝΟΣ ΣΤΕΦΑΝΟΣ
ΠΑΝΑΓΟΥΛΙΑΣ ΠΡΟΚΟΠΙΟΣ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ:

ΤΣΑΓΚΑΝΟΣ ΑΘΑΝΑΣΙΟΣ

ΠΑΤΡΑ 2011

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

"Τα μαθηματικά είναι η βασίλισσα των επιστημών και η θεωρία αριθμών η βασίλισσα των μαθηματικών".

Carl Friedrich Gauss (1777 – 1855)

Θεωρία των Αριθμών είναι ο κλάδος των Θεωρητικών μαθηματικών που ασχολείται με τις ιδιότητες των ακεραίων αριθμών, καθώς και με προβλήματα που προκύπτουν από τη μελέτη αυτή. Είναι ένας εξαιρετικά ελκυστικός και γοητευτικός κλάδος συνυφασμένος με την εξέλιξη της μαθηματικής επιστήμης αλλά ταυτόχρονα και με τα επιτεύγματα και τις αποτυχίες πολλών ερευνητών μαθηματικών.

Η Θεωρία των Αριθμών, από τη σκοπιά του ευρύτερου κλάδου της Άλγεβρας, συχνά αποκαλείται ως Αριθμητική. Ανάλογα από το είδος των προβλημάτων και από τις μεθόδους επίλυσης τους η Θεωρία Αριθμών χωρίζεται σε επιμέρους κλάδους όπως:

Η Αλγεβρική Θεωρία Αριθμών, η Αναλυτική Θεωρία Αριθμών, η Γεωμετρική Θεωρία Αριθμών, η Υπολογιστική Θεωρία Αριθμών και η Πιθανοθεωρητική Θεωρία Αριθμών.

Η Θεωρία των Αριθμών είναι η "ρίζα" του δένδρου της Μαθηματικής Επιστήμης. Από το 800 π.Χ. μαθηματικοί στην Ινδία προσπαθούσαν να βρουν τις ακέραιες λύσεις Διοφαντικών Εξισώσεων, δηλαδή εξισώσεων με ένα ή περισσότερους αγνώστους και ακέραιους συντελεστές.

Η Στοιχειώδης Θεωρία των Αριθμών ασχολείται με τη μελέτη του δακτυλίου των ακεραίων αριθμών και επεκτάσεων του χωρίς όμως τη χρήση εργαλείων από άλλους κλάδους των μαθηματικών.

Βασικό αντικείμενο μελέτης της θεωρίας των αριθμών είναι οι πρώτοι αριθμοί (όπου θα αναλύσουμε παρακάτω).

Η θεωρία αριθμών βρίσκει ευρεία εφαρμογή στην Κρυπτογραφία καθώς οι πιο γνωστές, σύγχρονες εφαρμογές της θεωρίας Αριθμών αφορούν στα Κρυπτογραφικά Συστήματα. Αυτά επιτρέπουν σε τράπεζες, οργανισμούς και διάφορες άλλες κρατικές και μη υπηρεσίες να ανταλλάσσουν κωδικοποιημένες πληροφορίες με ασφάλεια. Πολλοί επιστήμονες και ιδίως οι ασχολούμενοι με τις επιστήμες των ηλεκτρονικών υπολογιστών διαπιστώνουν καθημερινά το πόσο απαραίτητη είναι γνώση, στοιχείων τουλάχιστον, της θεωρίας Αριθμών στη δουλειά τους.

Οι έννοιες της Θεωρίας Αριθμών είναι εύκολα κατανοητές, αφού τα μόνα προαπαιτούμενα είναι η ευχέρεια στις αλγεβρικές πράξεις.

ΕΙΣΑΓΩΓΗ

1.1 ΙΣΤΟΡΙΑ

Η θεωρία αριθμών είναι ένας κλάδος των μαθηματικών που ασχολείται με τους φυσικούς αριθμούς,

1, 2, 3, …..,

που συχνά ονομάζονται και *θετικοί ακέραιοι*.

Η αρχαιολογία και η ιστορία μας διδάσκουν ότι ο άνθρωπος ξεκίνησε να μετρά νωρίς. Έμαθε να προσθέτει αριθμούς και πολύ αργότερα να τους πολλαπλασιάζει και να τους αφαιρεί. Η διαίρεση αριθμών ήταν απαραίτητη ούτως ώστε να μοιράζουν ισόποσα π.χ. έναν σωρό μήλα ή μια ψαριά. Αυτές οι πράξεις (λειτουργίες) επάνω στους αριθμούς ονομάζονται υπολογισμοί.

Αμέσως μόλις οι άνθρωποι έμαθαν να κάνουν κάποιους υπολογισμούς, αυτό έγινε μια πολύ ευχάριστη ασχολία, ένα παιχνίδι, για πολλά θεωρητικά μυαλά..

Εμπειρίες με αριθμούς συσσωρεύτηκαν ανά τους αιώνες με, ας πούμε, σύνθετο ενδιαφέρον έτσι που τώρα έχουμε ένα επιβλητικό οικοδόμημα στα σύγχρονα μαθηματικά γνωστό ως θεωρία αριθμών. Κάποια κομμάτια του αποτελούνται από απλό παιχνίδι με τους αριθμούς, αλλά κομμάτια του όμως ανήκουν στα πιο δύσκολα και περίπλοκα κεφάλαια των μαθηματικών.

1.2 ΑΡΙΘΜΟΛΟΓΙΑ

Μερικά από τα πρώτα ίχνη των εικασιών επάνω στους αριθμούς μπορούν ασφαλώς να εντοπιστούν σε προκαταλήψεις που αφορούν τους αριθμούς. Προκαταλήψεις που μπορούν να βρεθούν μεταξύ όλων των λαών. Υπάρχουν ‘τυχεροί’ αριθμοί προτιμητέοι και προσφιλείς στους λαούς, και υπάρχουν και ‘άτυχοι’ αριθμοί που τους αποφεύγουν σαν το κακό το μάτι (όπως ο διάολος το λιβάνι!!). Έχουμε αρκετές πληροφορίες για την αριθμολογία των Ελλήνων κλασσικών, τις σκέψεις και τις προκαταλήψεις τους, δηλαδή, όσον αφορά την συμβολική σημασία διαφόρων αριθμών. Παραδείγματος χάριν, ένας μονός αριθμός μεγαλύτερος του ενός συμβόλιζε τον άντρα, ενώ οι ζυγοί αριθμοί συμβόλιζαν την γυναίκα...έτσι, ο αριθμός 5, το άθροισμα του πρώτου αρσενικού και του πρώτου θηλυκού αριθμού, συμβόλιζαν τον γάμο ή την ένωση.

Οποιοσδήποτε επιθυμεί παραδείγματα πιο προχωρημένης αριθμολογίας μπορεί να διαβάσει το Βιβλίο 8 της Δημοκρατίας του Πλάτωνα. Παρά το ότι αυτή η αριθμολογία δεν αντιπροσωπεύει ιδιαίτερα τις μαθηματικές ‘ιδέες’ , εντούτοις περιλαμβάνει επιδέξιους χειρισμούς των αριθμών και των ιδιοτήτων τους. Μάλιστα, κάποια αξιοσημείωτα προβλήματα που ακόμη απασχολούν μαθηματικούς προέρχονται από την Ελληνική αριθμολογία.

Όσον αφορά τις προκαταλήψεις στους αριθμούς, δεν έχουμε κανέναν λόγο να νιώθουμε ανώτεροι. Όλοι γνωρίζουμε οικοδέσποινες που με τίποτα δεν θα δέχονταν να έχουν 13 καλεσμένους στο τραπέζι, και υπάρχουν πολύ λίγα ξενοδοχεία τα οποία έχουν αριθμό διαμερίσματος ή ορόφου το 13. Πραγματικά δεν γνωρίζουμε γιατί έχουν δημιουργηθεί τέτοια ‘ταμπού’ στους αριθμούς. Υπάρχουν πολλές εύλογες εξηγήσεις, αλλά οι περισσότερες είναι τελείως αβάσιμες` π.χ. υπήρχαν 13εις άνθρωποι στον Μυστικό Δείπνο, ο 13ος φυσικά ήταν ο Ιούδας. Ίσως, η παρατήρηση ότι πολλά πράγματα μετριούνται σε δωδεκάδες, ενώ σε δεκατριάδες έχουμε 12 και μας μένει ένα επιπλέον, να είναι πιο ρεαλιστική.

Στην Βίβλο, ιδιαίτερα στην Παλαιά Διαθήκη, ο αριθμός 7 παίζει σημαντικό ρόλο, στην γερμανική παράδοση επαναλαμβάνονται συχνά οι αριθμοί 3 και 9, και στην ινδική μυθολογία ο αριθμός 10 είναι πολύ αγαπητός.

1.3 ΤΟ ΠΥΘΑΓΟΡΕΙΟ ΠΡΟΒΛΗΜΑ

Σαν παράδειγμα πρώιμης θεωρίας αριθμών μπορούμε να αναφέρουμε το Πυθαγόρειο πρόβλημα. Όπως γνωρίζουμε, σε ένα ορθογώνιο τρίγωνο τα μήκη των πλευρών ικανοποιούν την Πυθαγόρεια σχέση

$$\zeta^2 = \chi^2 + \psi^2 ,$$

όπου ζ το μήκος της υποτείνουσας. Αυτό καθιστά δυνατό τον υπολογισμό του μήκους της μίας πλευράς όταν είναι γνωστές οι άλλες δύο. Βέβαια, το ότι αυτό το θεώρημα πήρε το όνομα του από τον Έλληνα φιλόσοφο Πυθαγόρα είναι ακατάλληλο, μιας και ήταν ήδη γνωστό στους Βαβυλώνιους κοντά 2000 χρόνια πριν από την εποχή του.

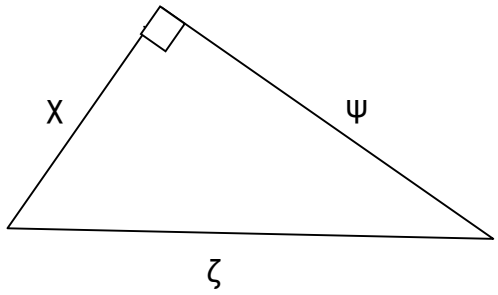
Κάποιες φορές όλα τα μήκη των πλευρών είναι ακέραιοι αριθμοί. Η πιο απλή περίπτωση,

$$\chi = 3, \qquad \psi = 4, \qquad \zeta = 5,$$

έχει βρεθεί σε Βαβυλωνιακούς δίσκους. Αυτό μπορεί να μεταφραστεί ως εξής.

Ας υποθέσουμε πως έχουμε ένα στεφάνι από σχοινί με σημάδια και κόμπους που το χωρίζουν σε 12 ίσα διαστήματα.. Ύστερα, τεντώνοντας το σχοινί σε τρία σημεία στο έδαφος δημιουργείται ένα τρίγωνο με πλευρές 3 και 4, η τρίτη πλευρά έχει μήκος 5 και η απέναντι γωνία είναι ορθή.

Συχνά διαβάζουμε σε ιστορίες μαθηματικών ότι αυτή την μέθοδο χρησιμοποιούσαν οι Αιγύπτιοι τοπογράφοι και αρπεδονάπτες για να επανακαθορίσουν τα όρια των χωραφιών μετά τις πλημμύρες του Νείλου. Φυσικά, αυτός μπορεί να είναι και ένας από τους πολλούς μύθους στην ιστορία της επιστήμης, μιας και δεν έχουμε σύγχρονα στοιχεία που να το υποστηρίζουν.



Υπάρχουν πολλές περιπτώσεις ακέραιων λύσεων στην Πυθαγόρεια εξίσωση, π.χ. ,

$\chi = 5, \quad \psi = 12, \quad \zeta = 13,$

$\chi = 7, \quad \psi = 24, \quad \zeta = 25,$

$\chi = 8, \quad \psi = 15, \quad \zeta = 17.$

Οι Έλληνες γνώριζαν πώς να υπολογίσουν τις λύσεις, και πιθανόν και οι Βαβυλώνιοι επίσης.

Όταν δίνονται δύο ακέραιοι χ και ψ, τότε πάντα μπορεί να βρεθεί ένας αντίστοιχος ζ που θα ικανοποιεί την εξίσωση $\zeta^2 = \chi^2 + \psi^2$, αλλά το ζ μπορεί κάλλιστα να είναι άρρητος.

Όταν απαιτείται και οι τρείς αριθμοί να είναι ακέραιοι, τότε οι πιθανότητες περιορίζονται σοβαρά. Ο Έλληνας μαθηματικός Διόφαντος της Αλεξάνδρειας (περί το 200 μ.Χ.) έγραψε το βιβλίο *Arithmetica* το οποίο ασχολείται με αυτού του είδους τα προβλήματα. Από την εποχή του το ζήτημα της εύρεσης ακέραιων ή ρητών λύσεων των εξισώσεων ονομάζεται Διοφαντικό πρόβλημα, και η Διοφαντική ανάλυση είναι ένα σημαντικό μέρος της θεωρίας αριθμών της σημερινής εποχής.

1.4 ΣΧΗΜΑΤΙΚΟΙ ΑΡΙΘΜΟΙ

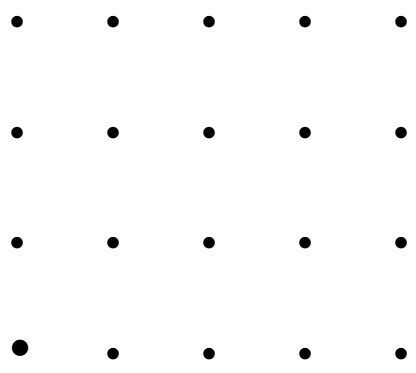
Στην θεωρία αριθμών συναντάμε συχνά τετραγωνικούς αριθμούς όπως

$$3^2 = 9, \qquad 7^2 = 49, \qquad 10^2 = 100$$

και, παρομοίως, κυβικούς αριθμούς όπως οι

$$2^3 = 8, \qquad 3^3 = 27, \qquad 5^3 = 125.$$

Αυτή η γεωμετρική μέθοδος έκφρασης είναι μια από τις πολλές κληρονομιές της Ελληνικής μαθηματικής σκέψης. Οι Έλληνες προτιμούσαν να σκέφτονται τους αριθμούς, μαζί με τους ακεραίους, ως γεωμετρικές ποσότητες. Κατά συνέπεια, ένα γινόμενο $\gamma = \alpha \times \beta$ θεωρούταν ως η περιοχή γ ενός τετραγώνου με πλευρές α και β. Μπορεί, επίσης, το $\alpha \times \beta$ να θεωρηθεί ως ο αριθμός των κουκίδων σε έναν ορθογώνιο πίνακα με α κουκίδες στη μια πλευρά και β κουκίδες στην άλλη. Παραδείγματος χάρη, το $20 = 4 \times 5$ είναι οι αριθμοί των κουκίδων στον ορθογώνιο πίνακα 1.4.1.



Σχήμα 1.4.1

Κάθε ακέραιος προϊόν δυο ακεραίων θα μπορούσε να ονομάζεται ορθογώνιος αριθμός. Όταν οι δυο πλευρές ενός ορθογωνίου έχουν το ίδιο μήκος, ο αριθμός είναι τετράγωνος. Κάποιοι αριθμοί δεν μπορούν να εκπροσωπηθούν ως ορθογώνιοι εκτός της τετριμμένης περίπτωσης όπου δημιουργούνται σημεία σε μια σειρά. Για παράδειγμα το 5 μπορεί να εκπροσωπηθεί ως ορθογώνιος αριθμός μόνο αν πάρουμε την μία πλευρά ως 1 και την άλλη ως 5 (Σχήμα 1.4.2). Τέτοιους αριθμούς οι αρχαίοι τους ονόμαζαν πρώτους αριθμούς. Ένα μοναδικό σημείο συνήθως δεν θεωρούταν αριθμός. Η μονάδα 1 ήταν η βάση, η πλίνθος από την οποία όλοι οι αριθμοί «χτίστηκαν».

Άρα το 1 δεν ήταν, και δεν είναι, πρώτος αριθμός.

● ● ● ● ●

Σχήμα 1.4.2

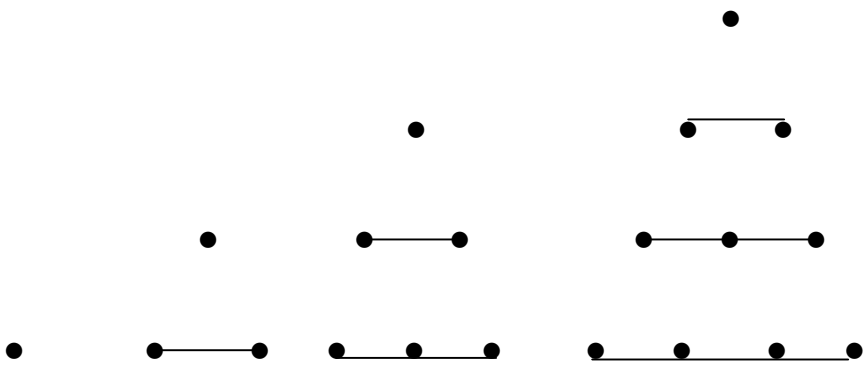
Αντί για ορθογώνια και τετράγωνα θα μπορούσαμε να εξετάσουμε σημεία τακτικά τοποθετημένα μέσα σε άλλα γεωμετρικά σχήματα. Στο Σχήμα 1.4.3 παρουσιάζουμε διαδοχικούς τριγωνικούς αριθμούς.

Γενικώς, ο ν-οστός τριγωνικός αριθμός δίνεται από τον τύπο

(1.4.1) $$T_v = \frac{1}{2}v(v+1), \quad v = 1, 2, 3, \ldots$$

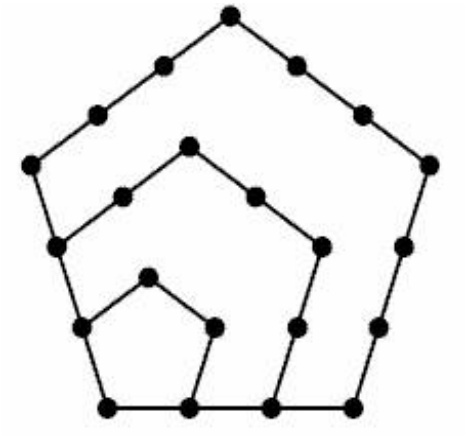
Οι αριθμοί αυτοί έχουν ποικιλία ιδιοτήτων, παραδείγματος χάρη, το άθροισμα δυο διαδοχικών τριγωνικών αριθμών είναι ένα τετράγωνο:

(1.4.2) $1 + 3 = 4, \quad 3 + 6 = 9, \quad 6 + 10 = 16, \quad$ κλπ.



Σχήμα 1.4.3

Οι τριγωνικοί και τετραγωνικοί αριθμοί γενικοποιήθηκαν σε μεγαλύτερους πολυγωνικούς αριθμούς. Ας το δούμε αυτό με πενταγωνικούς αριθμούς στο Σχήμα 1.4.4.



Σχήμα 1.4.4

Βλέπουμε ότι οι πρώτοι πενταγωνικοί αριθμοί είναι

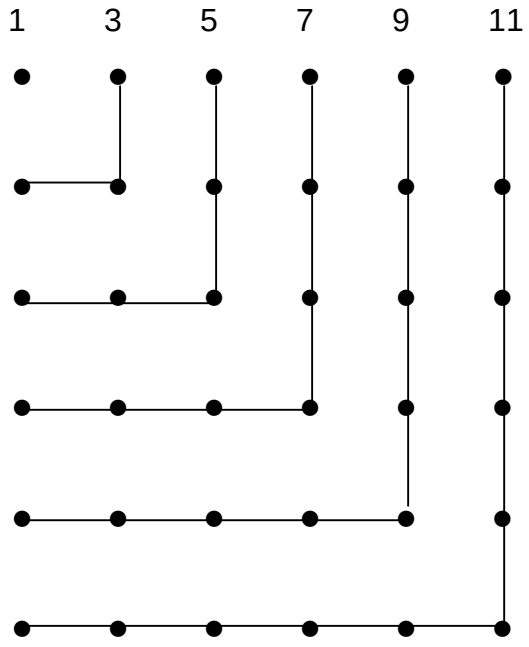
(1.4.3) 1, 5, 12, 22.

Μπορούμε να δείξουμε ότι ο ν-οστός πενταγωνικός αριθμός π_v δίνεται από τον τύπο

$$\pi_v = \frac{1}{2}(3v^2 - v). \qquad (1.4.4)$$

Οι εξαγωνικοί αριθμοί, και γενικότερα οι ν-γωνικοί αριθμοί που ορίζονται από ένα κανονικό πολύγωνο με *v* πλευρές, αποκτώνται αναλόγως.

Οι σχηματικοί αριθμοί, και ιδιαίτερα οι τριγωνικοί, υπήρξαν πολύ δημοφιλείς στις μελέτες των αριθμών στα τέλη της Αναγέννησης, αφότου η Ελληνική θεωρία αριθμών είχε έρθει στην Δυτική Ευρώπη. Περιστασιακά εμφανίζονται ακόμη σε μελέτες επάνω στην θεωρία αριθμών.



Σχήμα 1.4.5

Αρκετές απλές αριθμητικές σχέσεις μπορούν να συναχθούν από τέτοιες γεωμετρικές αναλύσεις. Ας υποδείξουμε μόνο ένα γεγονός. Νωρίς ανακαλύφθηκε πως η πρόσθεση περιττών αριθμών έως ένα σημείο έδινε ως αποτέλεσμα πάντα τετράγωνο. Παράδειγμα,

$$1 + 3 = 4,\ \ 1 + 3 + 5 = 9,\ \ 1 + 3 + 5 + 7 = 16,\ \ \text{κλπ.}$$

Για να αποδειχθεί αυτή η σχέση αρκεί απλώς μια ματιά στο διάγραμμα των ενθέτων τετραγώνων που δημιουργήσαμε στο Σχήμα 1.4.5.

1.5 ΜΑΓΙΚΑ ΤΕΤΡΑΓΩΝΑ

2	**9**	**4**
7	**5**	**3**
6	**1**	**8**

Σχήμα 1.5.1

Σε κάθε σειρά, σε κάθε στήλη, και σε κάθε μια από τις διαγωνίους το άθροισμα των αριθμών είναι το ίδιο, 15.

Γενικώς, ένα μαγικό τετράγωνο είναι η διευθέτηση των ακεραίων από το 1 έως το v^2 σε ένα τετράγωνο σχέδιο όπου οι αριθμοί σε κάθε σειρά, στήλη και διαγώνιο να δίνουν το ίδιο άθροισμα σ, το μαγικό άθροισμα. Ως μαγικό τετράγωνο στο 42 = 16 αριθμούς θα πάρουμε το σχήμα 1.5.2. Εδώ το μαγικό άθροισμα είναι 34.

1	**8**	**15**	**10**
12	**13**	**6**	**3**
14	**11**	**4**	**5**
7	**2**	**9**	**16**

Σχήμα 1.5.2

Για κάθε *v* υπάρχει μόνο ένα μαγικό άθροισμα *σ*, και είναι εύκολο να δούμε τι πρέπει να είναι: Το άθροισμα των αριθμών σε κάθε στήλη είναι *σ*, αφού υπάρχουν *v* στήλες τότε το άθροισμα όλων των αριθμών του μαγικού τετραγώνου είναι $v \times \sigma$. Αλλά το άθροισμα όλων των αριθμών από το 1 ως το v^2 είναι

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

όπως βλέπει κανείς από την έκφραση του αθροίσματος των αριθμών σε μια αριθμητική πρόοδο.
Αφού

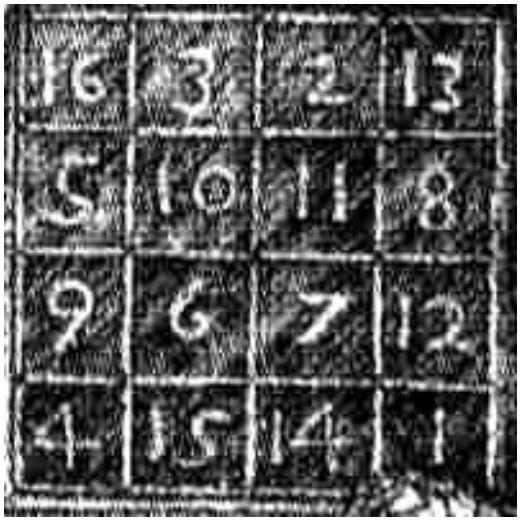
$$v\sigma = \frac{1}{2}(v^2 + 1)\, v^2 ,$$

άρα

$$(1.5.1) \qquad \sigma = \frac{1}{2} v(v^2 + 1)$$

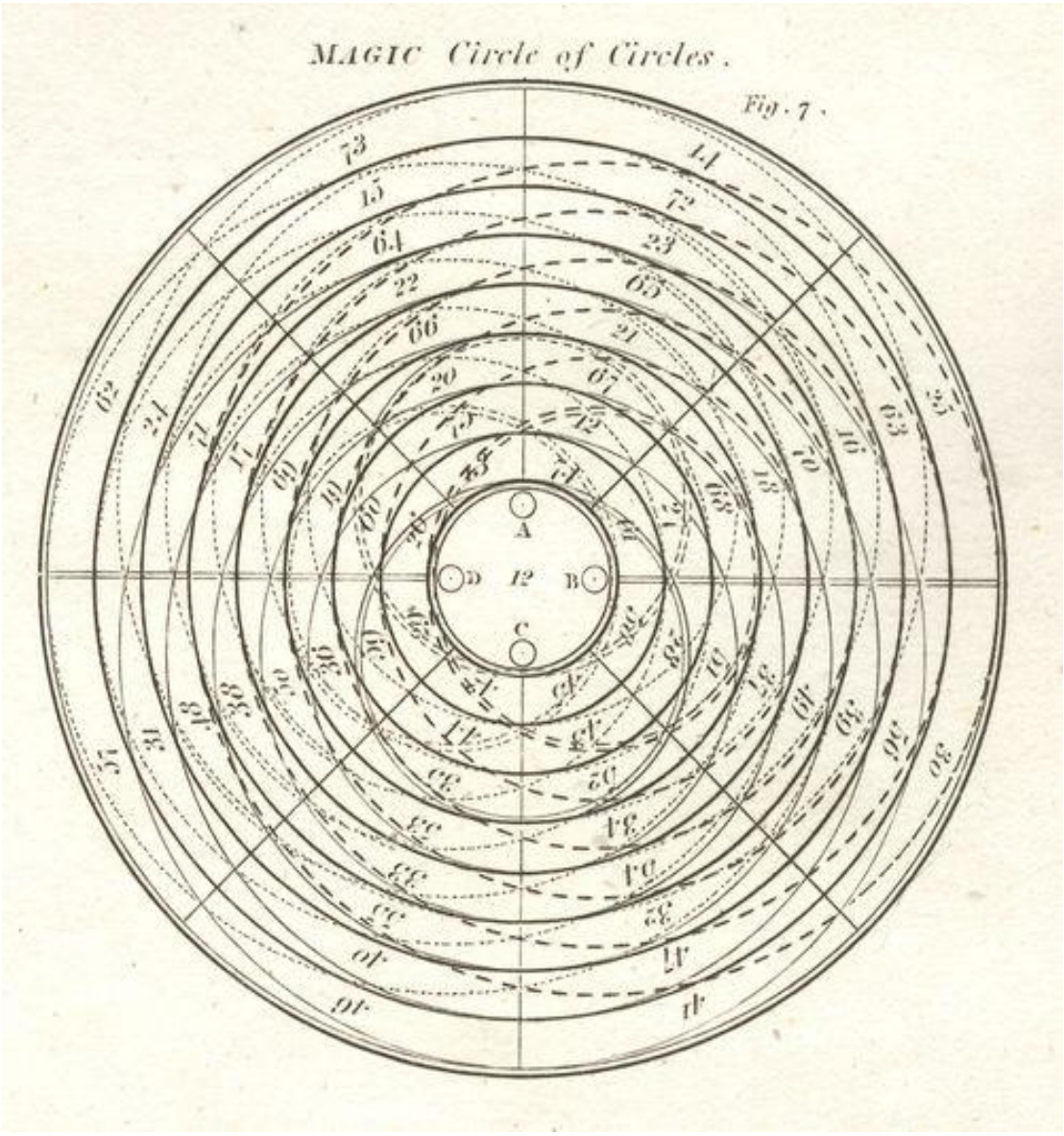
ώστε με δεδομένο το *v*, το *σ* προσδιορίζεται. Μαγικά τετράγωνα μπορούν να κατασκευαστούν για όλα τα *v* μεγαλύτερα του 2, είναι άλλωστε εύκολη η επαλήθευση πως δεν υπάρχει κανένα για $v = 2$.

Οι παράξενες ιδιότητες αυτών των τετραγώνων θεωρούνταν μαγικές τον Μεσαίωνα κι έτσι τα τετράγωνα χρησιμοποιούνταν ως φυλαχτά, προστατεύοντας αυτόν που το φορούσε από πολλά κακά. Ένα συχνά αναπαραγόμενο μαγικό τετράγωνο είναι το διάσημο χαρακτικό Melancholia του Albrecht Dürer (βλ. τελευταία σελίδα). Διακρίνεται με μεγαλύτερη λεπτομέρεια στο Σχήμα 1.5.3.
Οι μεσαίοι αριθμοί στην τελευταία σειρά αντιπροσωπεύουν το έτος 1514, κατά το οποίο δημιουργήθηκε το διάσημο χαρακτικό του Dürer. Πιθανότατα ξεκίνησε από αυτούς τους δυο αριθμούς και βρήκε τους υπόλοιπους εμπειρικά.



Σχήμα 1.5.3

Για ν μεγαλύτερα του 3 μπορούν να κατασκευαστούν πολλά μαγικά τετράγωνα. Κατά τον 16ο με 17ο αιώνα, αλλά και αργότερα, η δημιουργία μαγικών τετραγώνων άνθισε, παρόμοια με την σημερινή εποχή και την κατασκευή σταυρόλεξων και φυσικά των πασίγνωστων πια Sudoku. Ο Βενιαμίν Φραγκλίνος ήταν σφοδρός θαυμαστής των μαγικών τετραγώνων. Εξομολογήθηκε μάλιστα, κάποτε, ότι όταν ήταν υπάλληλος στο Pennsylvania Assembly και ήθελε να αποδιώξει την ανία της εργασίας του συμπλήρωνε κάτι περίεργα μαγικά τετράγωνα ή ακόμη και μαγικούς κύκλους που αποτελούνταν από περιπεπλεγμένους κύκλους αριθμών των οποίων το άθροισμα σε κάθε κύκλο ήταν το ίδιο (Σχήμα 1.5.4).



Σχήμα 1.5.4.

ΠΡΩΤΟΙ

2.1 ΠΡΩΤΟΙ ΚΑΙ ΣΥΝΘΕΤΟΙ ΑΡΙΘΜΟΙ

Πρέπει να είναι από τις πρώτες ιδιότητες που ανακαλύφθηκαν, ότι κάποιοι αριθμοί μπορούν να παραγοντοποιηθούν σε δύο ή περισσότερους μικρότερους παράγοντες. Για παράδειγμα:

$$6 = 2 \times 3, \quad 9 = 3 \times 3, \quad 30 = 2 \times 15 = 3 \times 10$$

ενώ κάποιοι άλλοι όπως:

$$3,\ 7,\ 13,\ 17$$

δεν μπορούν να παραγοντοποιηθούν. Ας θυμηθούμε πως όταν

$$\gamma = \alpha \times \beta \tag{2.1.1}$$

είναι προϊόν δυο αριθμών α και β, τότε ονομάζουμε τα α, β παράγοντες ή διαιρέτες του γ. Κάθε αριθμός έχει τετριμμένη παραγοντοποίηση

$$\gamma = 1 \times \gamma \tag{2.1.2}$$

Αντίστοιχα ονομάζουμε το 1 και το γ τετριμμένους διαιρέτες του γ.

Όποιος αριθμός $\gamma > 1$ έχει μη τετριμμένη παραγοντοποίηση ονομάζεται **σύνθετος**. Όταν ο γ έχει μόνο την τετριμμένη παραγοντοποίηση (2.1.2) ονομάζεται **πρώτος.** Μεταξύ των πρώτων 100 αριθμών οι παρακάτω 25 είναι πρώτοι:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,
43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

Όλοι οι υπόλοιποι εκτός του 1 είναι σύνθετοι. Σημειώνουμε ότι:

Θεώρημα 2.1.1 Κάθε ακέραιος αριθμός γ > 1 είναι είτε πρώτος είτε έχει πρώτο διαιρέτη.

Απόδειξη: Αν ο γ δεν είναι πρώτος έχει έναν μικρότερο μη τετριμμένο παράγοντα π . Τότε ο π είναι πρώτος γιατί αν ο π ήταν σύνθετος, ο γ θα είχε έναν ακόμη μικρότερο διαιρέτη.

Σε αυτό το σημείο είναι που εμφανίζεται το πρώτο σημαντικό πρόβλημα στη θεωρία των αριθμών: Πώς αποφασίζουμε αν ένας αριθμός είναι πρώτος ή όχι; Και στην περίπτωση που είναι σύνθετος πως μπορεί να βρεθεί ένας μη τετριμμένος διαιρέτης;

Μία άμεση αλλά μη ικανοποιητική απάντηση είναι ότι θα μπορούσαμε να διαιρέσουμε τον συγκεκριμένο αριθμό γ με όλους τους αριθμούς που είναι μικρότεροι από αυτόν. Σύμφωνα με το θεώρημα (2.1.1.) αρκεί να τον διαιρέσουμε με όλους τους πρώτους που είναι μικρότεροι του γ. Αλλά μπορούμε να μειώσουμε το έργο αυτό ουσιαστικά με την παρατήρηση ότι σε μία παραγοντοποίηση (2.1.1.) δεν μπορούν και οι δυο διαιρέτες α και β , να είναι μεγαλύτεροι του $\sqrt{g}$. Αν ίσχυε αυτή η περίπτωση τότε θα είχαμε:

$$\alpha \times \beta > \sqrt{g} \times \sqrt{g} = \gamma$$

που είναι αδύνατον. Έτσι για να βρούμε αν ο αριθμός γ έχει διαιρέτη αρκεί να εξετάσουμε μόνο εάν οποιοσδήποτε από τους πρώτους, μικρότεροι ή ίσοι του $\sqrt{g}$, διαιρεί τον γ.

Παράδειγμα 1. Αν γ = 91 τότε $\sqrt{g}$ = 9, ...

Δοκιμάζοντας τους πρώτους 2, 3, 5, 7 φαίνεται ότι 91 = 7 × 13.

Παράδειγμα 2. Αν γ = 1973 βρίσκουμε $\sqrt{g}$ = 44, ...

Αφού κανένας από τους πρώτους έως το 43 δεν διαιρεί το γ , τότε ο αριθμός είναι πρώτος.

Διαπιστώνουμε γρήγορα ότι για μεγάλους αριθμούς αυτή η μέθοδος ίσως δεν είναι αρκετά πρακτική. Ωστόσο, όπως εδώ, έτσι και σε πολλούς άλλους υπολογισμούς της θεωρίας των αριθμών μπορούμε να στηριχτούμε σε μοντέρνες τεχνικές. Είναι απλός ο προγραμματισμός ενός υπολογιστή ώστε να διαιρεί έναν συγκεκριμένο αριθμό γ με όλους τους ακέραιους έως το $\sqrt{g}$ και να εκτυπώσει αυτούς που δεν δίνουν υπόλοιπο, δηλαδή αυτούς που διαιρούν τον αριθμό γ.

Μια άλλη πολύ απλή μέθοδος είναι να στηριχτούμε πάνω στους πίνακες των πρώτων οι οποίοι έχουν διερευνηθεί και καταγραφεί από άλλους. Ο πιο εκτενής, διαθέσιμος πίνακας καταρτίστηκε από τον D.N.Lehmer ο οποίος μας δίνει όλους τους πρώτους μέχρι τα 10.000.000.

Μάλιστα μερικοί ενθουσιώδεις ερασιτέχνες μαθηματικοί προετοίμασαν πίνακες πρώτων πέραν των 10.000.000. Ωστόσο δεν φαίνεται να υπάρχει ιδιαίτερο νόημα να εκτυπωθούν λόγω των σημαντικότατων δαπανών. Επιπλέον, πολύ σπάνια ένας μαθηματικός, ακόμα και ειδικός στη Θεωρία των Αριθμών, μπορεί να χρειαστεί να υπολογίσει εάν ένας πολύ μεγάλος αριθμός είναι σύνθετος ή πρώτος. Οι αριθμοί που επιθυμεί συνήθως να εξετάζει εμφανίζονται σε ειδικά μαθηματικά προβλήματα οπότε και έχουν πολύ εξειδικευμένες μορφές.

ΠΙΝΑΚΑΣ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ ΜΕΧΡΙ ΤΟ 1.000

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101 , 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223 , 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 859, 869, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997

2.2 ΠΡΩΤΟΙ MERSENNE

Για πολλούς αιώνες και με διάφορες μεθόδους πολλοί μαθηματικοί έχουν ανταγωνιστεί μεταξύ τους για μια θέση στην Ιστορία των Μαθηματικών λόγω της εύρεσης του μεγαλύτερου πρώτου αριθμού. Μία απλή μέθοδος είναι η συγκέντρωση πολύ μεγάλων αριθμών που δεν έχουν τους προφανείς διαιρέτες 2, 3, 5, 7 και να δοκιμάσει αν είναι πρώτοι. Όπως αντιλαμβανόμαστε γρήγορα όμως, αυτή δεν είναι πολύ αποτελεσματική λύση. Έτσι πολλές μέθοδοι έχουν πια αποκλειστεί και ακολουθείται μία οδός, η οποία έχει αποδειχθεί η πιο επιτυχημένη.

Οι πρώτοι Mersenne είναι οι πρώτοι που δίνονται από τον ειδικό τύπο:

$$M_\pi = 2^\pi - 1 \qquad (2.2.1.)$$

όπου ο π είναι ένας άλλος πρώτος. Αυτοί οι αριθμοί τέθηκαν στα μαθηματικά νωρίς και εμφανίστηκαν στην συζήτηση του *Ευκλείδη* για τους τέλειους αριθμούς, τους οποίους θα συναντήσουμε αργότερα. Οι αριθμοί Mersenne πήραν το όνομά τους από τον Γάλλο μοναχό Marin Mersenne (1588 -1648) ο οποίος υπολόγισε έναν αρκετά μεγάλο αριθμό τέλειων αριθμών.

Όταν ξεκινάμε τον υπολογισμό των αριθμών (2.2.1.) για διάφορους πρώτους π παρατηρούμε πως δεν είναι όλοι πρώτοι, για παράδειγμα:

$$M_2 = 2^2 - 1 = 3 = \text{πρώτος}$$
$$M_3 = 2^3 - 1 = 7 = \text{πρώτος}$$
$$M_5 = 2^5 - 1 = 31 = \text{πρώτος}$$
$$M_7 = 2^7 - 1 = 127 = \text{πρώτος}$$
$$M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$$

Η γενική μέθοδος για την εύρεση μεγάλων πρώτων με τον τύπο του Mersenne είναι να εξετάσει κανείς όλους τους αριθμούς M_π για τους διάφορους πρώτους *π*.

Οι αριθμοί αυξάνονται πολύ γρήγορα και αυτό συνεπάγεται περισσότερη εργασία. Ο λόγος για τον οποίο η εργασία είναι διαχειρίσιμη ακόμα και για αρκετά μεγάλους αριθμούς είναι διότι υπάρχουν πολλοί αποτελεσματικοί τρόποι για να μάθουμε αν αυτοί οι αριθμοί είναι πρώτοι.

Υπήρξε μια περίοδος κατά την οποία η εξέταση των πρώτων Mersenne κορυφώθηκε όταν, το 1750 ο Ελβετός μαθηματικός Euler θέσπισε ότι ο M_{31} είναι πρώτος. Έως εκείνη την στιγμή 8 πρώτοι αριθμοί Mersenne είχαν ανακαλυφθεί οι οποίοι αριθμοί είναι:

π = 2,	π = 3,	π = 5,	π = 7,
π = 13,	π = 17,	π = 19,	π = 31

Ο αριθμός M_{31} του Euler παρέμεινε ο μεγαλύτερος πρώτος για πάνω από έναν αιώνα. Το 1876 ο Γάλλος μαθηματικός Lukas ανακάλυψε ότι ο τεράστιος αριθμός:

$$M_{127} = 170141183460469231731687303715884105727$$

είναι πρώτος.

Ο αριθμός αυτός έχει 39 ψηφία! Οι πρώτοι Mersenne μικρότεροι από αυτόν δίνονται από τις τιμές του *π* που αναφέρονται παραπάνω, όπως και από τους:

π = 61, π = 89, π = 107.

Αυτοί οι 12 πρώτοι Mersenne είχαν υπολογιστεί με πένα και χαρτί και για μερικούς από τους επόμενους με μηχανικές αριθμομηχανές γραφείου. Η εισαγωγή των ηλεκτρικά τροφοδοτούμενων αριθμομηχανών έδωσε την δυνατότητα να συνεχιστεί η έρευνα μέχρι το π = 257, αλλά τα αποτελέσματα ήταν απογοητευτικά. Δεν βρέθηκαν άλλοι πρώτοι Mersenne.

Αυτή η κατάσταση υπήρχε όταν ανέλαβαν οι υπολογιστές. Η ανάπτυξη των μηχανημάτων μεγαλύτερης ικανότητας κατέστησε δυνατό η έρευνα των πρώτων Mersenne να αναρριχηθεί σε όλο και υψηλότερα επίπεδα.
Ο D.H.Lehmer όρισε ότι οι τιμές:

$$\pi = 521, \quad \pi = 607, \quad \pi = 1279, \quad \pi = 2203, \quad \pi = 2281$$

αποδίδουν πρώτους Mersenne M_π. Αργότερα σημειώθηκε μεγαλύτερη πρόοδος. Ο Riesel (1958) έδειξε ότι ο:

$$\pi = 3217$$

αποδίδει έναν πρώτο Mersenne, και ο Hurwitz (1962) βρήκε τις δύο αξίες:

$$\pi = 4253, \qquad \pi = 4423.$$

Τεράστια πρόοδο σημείωσε ο Gillies (1964) ο οποίος βρήκε τους πρώτους Mersenne που αντιστοιχούν στους:

$$\pi = 9689, \quad \pi = 9941, \quad \pi = 11213.$$

Έτσι έχουμε μία συνολική συγκομιδή 23 πρώτων Mersenne και όσο οι ικανότητες των μηχανημάτων αυξάνονται ελπίζουμε για όλο και περισσότερους. Ο πρώτος M_{127} του Lukas , όπως αναφέραμε, έχει 39 ψηφία. Ο υπολογισμός μεγάλων πρώτων Mersenne απαιτεί πολύ εργασία και δεν έχει νόημα να αναπτυχθεί εδώ. Ωστόσο θα είχε ενδιαφέρον να μάθουμε πόσα ψηφία περιέχουν. Αυτό μπορούμε να το κάνουμε ως ακολούθως χωρίς πράγματι να υπολογίσουμε τον αριθμό.

Αντί να βρούμε τον αριθμό των ψηφίων στον τύπο $M_\pi = 2^\pi - 1$, ας πάρουμε τον ακόλουθο αριθμό:

$$M_\pi + 1 = 2^\pi$$

Αυτοί οι δύο αριθμοί πρέπει να έχουν τον ίδιο αριθμό ψηφίων έτσι ώστε, αν ο $M_π + 1$ είχε ένα ακόμα ψηφίο, αυτός θα έπρεπε να είναι ένας αριθμός ο οποίος λήγει σε 0. Όμως αυτό δεν είναι εφικτό για καμία δύναμη του 2, όπως προκύπτει από την σειρά:

$$2,\ 4,\ 8,\ 16,\ 32,\ 64,\ 128,\ 256, \ldots$$

στην οποία το τελευταίο ψηφίο μπορεί να είναι μόνο ένας από τους αριθμούς

$$2,\ 4,\ 8,\ 6.$$

Για την εύρεση του αριθμού των ψηφίων στο $2^π$ υπενθυμίζουμε ότι $\log 2^π = p \times \log 2$.
Από πίνακα βρίσκουμε ότι log 2 ισούται περίπου με .30103, οπότε:

$$\log 2^π = π \times \log 2 = π \times .30103$$

Σε περίπτωση που έχουμε π = 11213, μας δίνει:

$$\log 2^{11213} = 3375.449\ldots$$

και από το χαρακτηριστικό 3375, συμπεραίνουμε ότι ο αριθμός $2^π$ έχει 3376 ψηφία. Οπότε μπορούμε να πούμε ότι:

Ο πρώτος Mersenne M_{11213} έχει 3376 ψηφία. Ο συγκεκριμένος πρώτος Mersenne υπολογίστηκε στο Πανεπιστήμιο του Illinois όπου, μάλιστα, το τμήμα των μαθηματικών ήταν τόσο περήφανο για το κατόρθωμά του, που αποφάσισε να τον εκτυπώνει (τον M_{11213}) σε όλα τα γραμματόσημα του για να το θαυμάζει όλος ο κόσμος.

Μέχρι την ημέρα που γράφεται το παρών κείμενο γνωρίζουμε πως υπάρχουν 47 πρώτοι Mersenne (άρα και 47 τέλειοι αριθμοί). Από τον 35ο έως και τον 47ο οι πρώτοι Mersenne έχουν ανακαλυφθεί από έναν εκ των δυνατότερων υπολογιστών στον κόσμο ονόματι GIMPS (Great Internet Mersenne Prime Search Primenet). Ο GIMPS στις 11 Ιουλίου 2010 κάνοντας διπλό έλεγχο σε όλους τους προηγούμενους πρώτους απέδειξε

πως ο $M_{20.996.011}$ είναι ο 40ος πρώτος Mersenne. Από τον 41ο έως και τον 47ο δεν έχει ελεγχθεί ακόμη αν υπάρχουν ενδιάμεσα τους και άλλοι πρώτοι Mersenne.

Σε μια προσπάθεια οπτικοποίησης του μεγέθους του 47ου γνωστού πρώτου Mersenne, υπολογίζεται πως θα χρειάζονταν 3.461 σελίδες για να παρουσιάσουμε τον αριθμό, βάσεως 10, με 75 ψηφία ανά σειρά και 50 σειρές ανά σελίδα.

2.3 ΠΡΩΤΟΙ FERMAT

Υπάρχει και ένας άλλος τύπος πρώτων με μακρά και ενδιαφέρουσα ιστορία: *οι πρώτοι Fermat.* Εισήχθησαν αρχικά από τον Pierre de Fermat (1601-1665), έναν Γάλλο δικαστή, ο οποίος παράλληλα ήταν διακεκριμένος Μαθηματικός. Οι πρώτοι πέντε *πρώτοι Fermat* είναι οι εξής:

$$F_0 = 2^{2^0} + 1 = 3, \qquad F_1 = 2^{2^1} + 1 = 5, \qquad F_2 = 2^{2^2} + 1 = 17,$$

$$F_3 = 2^{2^3} + 1 = 257, \qquad F_4 = 2^{2^4} + 1 = 65537$$

Σύμφωνα με αυτή την ακολουθία ο γενικός τύπος για τους *πρώτους Fermat* θα είναι:

$$\Phi_v = 2^{2^v} + 1 \qquad (2.3.1)$$

Ο Fermat ήταν πεπεισμένος ότι όλοι οι αριθμοί αυτού του είδους ήταν πρώτοι παρόλα αυτά δεν προέβη σε υπολογισμούς πέρα από αυτούς τους πέντε που δίνονται παραπάνω. Η εικασία αυτή «πετάχτηκε έξω από το παράθυρο» όταν ο Ελβετός Μαθηματικός Euler έκανε ένα βήμα παραπάνω, και απέδειξε ότι ο επόμενος πρώτος Fermat

$$\Phi_5 = 4294967297 = 641 \times 6700417,$$

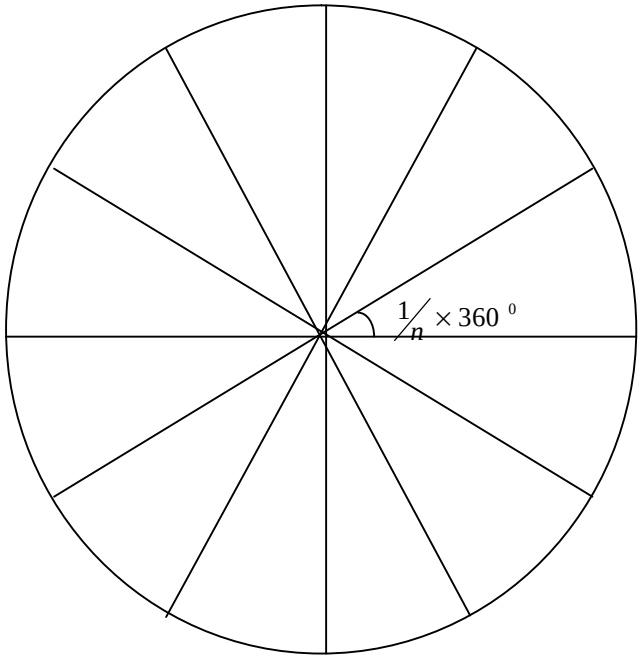
δεν είναι πρώτος, όπως φαίνεται. Αυτό θα μπορούσε να είναι το τέλος της ιστορίας αν δεν είχαν ανακύψει οι αριθμοί Fermat σε ένα διαφορετικό πρόβλημα, στην κατασκευή κανονικών πολυγώνων με κανόνα και διαβήτη.

Ένα κανονικό πολύγωνο είναι ένα πολύγωνο του οποίου οι κορυφές βρίσκονται σε ίσες αποστάσεις η μία από την άλλη σε κύκλο (Σχήμα 2.3.1). Αν ένα κανονικό πολύγωνο έχει v κορυφές, τότε το ονομάζουμε κανονικό *v-γωνο*. Οι v γραμμές από τις κορυφές μέχρι το κέντρο του κύκλου

δημιουργούν *v* γωνίες, το μέγεθος της κάθε μίας:

$$1/n \times 360^0$$

Αν μπορεί κανείς να κατασκευάσει μια γωνία αυτού του μεγέθους, μπορεί επίσης, να κατασκευάσει ένα ν-γωνο.



Σχήμα 2.3.1.

Οι αρχαίοι Έλληνες ενδιαφέρονταν πολύ για την εύρεση μεθόδων για την κατασκευή κανονικών πολυγώνων με κανόνα και διαβήτη. Οι απλούστερες περιπτώσεις που μπορούσαν, φυσικά, να κατασκευάσουν ήταν του ισοσκελούς τριγώνου ή τετραγώνου. Παίρνοντας επανειλημμένα το μισό της κεντρικής γωνίας μπορούσαν να κατασκευάσουν κανονικά πολύγωνα με

4, 8, 16, 32, …,

3, 6, 12, 24, …

κορυφές. Επιπλέον, μπορούσαν να κατασκευάσουν κανονικό πεντάγωνο, άρα και κανονικά πολύγωνα με

5, 10, 20, 40,…

κορυφές. Ένας ακόμη τύπος κανονικών πολυγώνων ήταν δυνατόν να επιτευχθεί. Η κεντρική γωνία σε ένα 15-γωνο ισούται με

$$\frac{1}{15}\times 360^0 = 24^0$$

και αυτό προκύπτει από την γωνία 72^o στο πεντάγωνο και η γωνία 120^o στο τρίγωνο: παίρνοντας την πρώτη γωνία δυο φορές και αφαιρώντας τη δεύτερη. Ως εκ τούτου μπορεί κανείς να κατασκευάσει κανονικά πολύγωνα με 15, 30, 60, 120, … πλευρές.

Αυτή ήταν η κατάσταση των πραγμάτων μέχρι το 1801, όταν ο νεαρός Γερμανός Μαθηματικός C.F.Gauss (1777-1855) δημοσίευσε μια κοσμοϊστορική εργασία στη Θεωρία των Αριθμών, την *Disquisitiones Arithmeticae.* Ο Gauss υπερέβη τους Έλληνες γεωμέτρες, φτιάχνοντας με κανόνα και διαβήτη ένα κανονικό 17-γωνο, αλλά προχώρησε ακόμα περισσότερο. Προσδιόρισε για όλα τα v , ποια v-γωνα μπορούν να κατασκευαστούν και ποια όχι. Μπορούμε να περιγράψουμε τα αποτελέσματα του Gauss παρακάτω.

Παρατηρήσαμε ότι από κανονικό ν-γωνο μπορεί να παραχθεί ένα 2ν-γωνο διαιρώντας κάθε κεντρική γωνία στη μέση. Από την άλλη μεριά, από ένα 2ν-γωνο μπορεί να κατασκευαστεί ένα ν-γωνο χρησιμοποιώντας απλώς κάθε δεύτερη κορυφή. Αυτό δείχνει ότι για να καθοριστεί ποια κανονικά πολύγωνα μπορούν να κατασκευαστούν, αρκεί να εξεταστούν μόνο τα
ν-γωνα με περιττό ν. Για κάθε ν ο Gauss απέδειξε ότι: *Ένα κανονικό πολύγωνο με ν κορυφές μπορεί να κατασκευαστεί με κανόνα και διαβήτη αν, και μόνο αν, ο αριθμός ν είναι πρώτος Fermat ή γινόμενο διακριτών πρώτων Fermat.*

Ας εξετάσουμε τις μικρότερες τιμές του *ν* . Μπορεί κανείς να αντιληφθεί ότι ένα 3-γωνο και ένα 5-γωνο μπορεί να κατασκευαστεί, ενώ ένα 7-γωνο όχι, καθώς το 7 δεν είναι πρώτος του Fermat. Ένα 9-γωνο δεν μπορεί να κατασκευαστεί καθώς το $9 = 3 \times 3$ είναι το γινόμενο δύο ίσων πρώτων Fermat. Για $n = 11$ ή $n = 13$ το πολύγωνο δεν μπορεί να κατασκευαστεί , αλλά μπορεί για $n = 15 = 3 \times 5$ και $v = 17$.

Η ανακάλυψη του Gauss φυσικά δημιούργησε νέο ενδιαφέρον στους αριθμούς του Fermat (2.3.1). Τον προηγούμενο αιώνα αρκετοί ηρωικοί υπολογισμοί έγιναν, χωρίς βοήθεια από μηχανές, για να βρεθούν νέοι πρώτοι του Fermat. Προς το παρόν αυτοί οι υπολογισμοί συνεχίζονται με έναν επιταχυνόμενο ρυθμό μέσα από τους υπολογιστές. Μέχρι στιγμής τα αποτελέσματα είναι αρνητικά. Κανένας καινούργιος πρώτος αριθμός του Fermat δεν έχει ανακαλυφθεί και πολλοί Μαθηματικοί έχουν φτάσει στο σημείο να δεχτούν ότι δεν υπάρχουν άλλοι, επιπλέον από τους ήδη γνωστούς.

2.4 ΤΟ ΚΟΣΚΙΝΟ ΤΟΥ ΕΡΑΤΟΣΘΕΝΗ

Όπως έχουμε αναφέρει, υπάρχουν πίνακες πρώτων μέχρι και αρκετά μεγάλους αριθμούς. Πως όμως θα κατασκευάσει πραγματικά ένα τέτοιο πίνακα; Αυτό το πρόβλημα λύθηκε, κατά κάποιο τρόπο, από τον Αλεξανδρινό Μαθηματικό, τον Ερατοσθένη (περί το 200 π.Χ.). Ο τρόπος του εκτελείται ως ακολούθως:

1. Γράφουμε μια ακολουθία όλων των ακεραίων από το 1 και προς τα άνω μέχρι οποιοδήποτε σημείο θέλουμε να φτάσουμε:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
			_		_		_	_	_		_		_	_
			2		2		2	3	2		2		2	3

2. Παίρνουμε τον πρώτο 2.Αποκλείουμε κάθε δεύτερο αριθμό μετά το 2 με μια παύλα από κάτω.
3. Μετά ο πρώτος "ασημάδευτος" αριθμός είναι ο 3.Είναι πρώτος αφού δεν διαιρείται με το 2.Οπότε σημαδεύουμε με την παύλα κάθε τρίτο αριθμό μετά το 3,χωρίς όμως να ξανασημαδεύουμε τους ήδη "σημαδεμένους" αριθμούς.
4. Κάνουμε την ίδια διαδικασία με το 5.τον επόμενο "ασημάδευτο" και πρώτο αριθμό (αφού δεν διαιρείται ούτε με το 2 ούτε με το 3). Μετά με το 7 και πάει λέγοντας.

Αυτή η μέθοδος «κοσκινίσματος» των αριθμών είναι γνωστή ως το «κόσκινο του Ερατοσθένη». Όλοι οι πίνακες πρώτων έχουν δημιουργηθεί με την αρχή του «κόσκινου του Ερατοσθένη». Πράγματι κάποιος μπορεί να προχωρήσει αυτή την μέθοδο και με μεγαλύτερους αριθμούς χρησιμοποιώντας την μνήμη ενός υπολογιστή. Στο επιστημονικό εργαστήριο του Λος Άλαμος όλοι οι πρώτοι άνω του 100.000.000 έχουν αποθηκευτεί με αυτόν τον τρόπο.

Μέσα από μια μικρή διακύμανση της μεθόδου του «κόσκινου» έχουμε επίσης την εξής πληροφορία σας κέρδος: Γράφοντας τον αριθμό που αποκλείει κάθε "σημαδεμένο" αριθμό αποκτούμε τον μικρότερο πρώτο που τον διαιρεί. Τότε αν πάρουμε για παράδειγμα, το 15 και το 35 θα έχουμε:

15	35
–	–
3	5

Μια τέτοια ακολουθία αριθμών ονομάζεται *πίνακας παραγόντων.* Ένας πίνακας παραγόντων είναι πιο σύνθετος από έναν πίνακα πρώτων. Ο μεγαλύτερος πίνακας παραγόντων που έχουμε υπολογίστηκε από τον D.N.Lehmer και εκτείνεται σε όλους τους αριθμούς μέχρι και το 10.000.000.

Το κόσκινο του Ερατοσθένη μπορεί να χρησιμοποιηθεί για την κατασκευή πινάκων των πρώτων και πινάκων παραγόντων όπως είδαμε. Αλλά μπορεί επίσης να χρησιμοποιηθεί για θεωρητικούς σκοπούς, και πολλά σημαντικά αποτελέσματα στη μοντέρνα Θεωρία έχουν προέρθει μέσα από τη μέθοδο αυτού του «κοσκινίσματος». Όπως μας επισημαίνει και ο Ευκλείδης μέσα από ένα ήδη γνωστό γεγονός: «*Υπάρχει άπειρος αριθμός πρώτων*»

Απόδειξη: Υποθέτουμε ότι υπάρχουν κ πρώτοι:

$$2,\ 3,\ 5,\ .....,\ \pi_\kappa\ .$$

Άρα στο κόσκινο δεν θα υπάρχουν "ασημάδευτοι" αριθμοί μετά το π_κ .
Αυτό όμως είναι αδύνατο. Γιατί:

$$\Pi = 2\times3\times5\times.....\times \pi_\kappa$$

θα αποκλειστεί κ φορές, μία για κάθε πρώτο, άρα ο επόμενος αριθμός
$\Pi + 1$ δεν θα σημαδευτεί από κανέναν τους.

ΔΙΑΙΡΕΤΕΣ ΑΡΙΘΜΩΝ

3.1 ΘΕΜΕΛΙΩΔΕΣ ΘΕΩΡΗΜΑ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ

Ένας σύνθετος αριθμός γ μπορεί να γραφεί ως γινόμενο $\gamma = \alpha \times \beta$, όπου κανείς εκ των παραγόντων δεν είναι 1 και οι δυο είναι μικρότεροι του γ. Για παράδειγμα,

$$72 = 8 \times 9, \qquad 150 = 10 \times 15.$$

Στην παραγοντοποίηση του γ, ο ένας ή και οι δυο παράγοντες μπορεί να είναι σύνθετοι. Αν ο α είναι σύνθετος, μπορεί να παραγοντοποιηθεί περαιτέρω:

$$\alpha = \alpha_1 \times \alpha_2, \qquad \gamma = \alpha_1 \times \alpha_2 \times \beta.$$

Στα ανωτέρω παραδείγματα έχουμε,

$$72 = 2 \times 4 \times 9, \qquad 150 = 2 \times 5 \times 15.$$

Μπορούμε να συνεχίσουμε την διαδικασία της παραγοντοποίησης μέχρι να σταματήσει. Σταματάει, μάλιστα, γιατί οι παράγοντες γίνονται όλο και μικρότεροι, αλλά δεν μπορούν να γίνουν 1. Όταν δεν μπορούμε να παραγοντοποιήσουμε παραπάνω τότε κάθε παράγοντας είναι πρώτος. Έτσι αποδείξαμε πως:

Κάθε παράγοντας μεγαλύτερος του 1 είναι είτε πρώτος είτε γινόμενο πρώτων.

Η σταδιακή παραγοντοποίηση ενός αριθμού μπορεί να επιτευχθεί με πολλούς τρόπους. Είναι γεγονός όμως, ότι ανεξάρτητα από τον τρόπο με τον οποίο γίνεται η παραγοντοποίηση πρώτων, το αποτέλεσμα είναι πάντα το ίδιο εκτός από την διάταξη των παραγόντων, δηλαδή, σε κάθε δυο παραγοντοποιήσεις οι πρώτοι είναι ίδιοι και ο καθένας εμφανίζεται τις ίδιες φορές. Αυτό συνοπτικά σημαίνει πως:

Η παραγοντοποίηση πρώτων ενός αριθμού είναι μοναδική.

Το θεώρημα αυτό, θεμελιώδες θεώρημα των μαθηματικών μάλιστα, μπορεί να αποδειχθεί με πολλούς τρόπους, κανένας τους όμως δεν είναι τετριμμένος. Εδώ θα χρησιμοποιήσουμε μια αποδεικτική μέθοδο η οποία στα Λατινικά ονομάζεται: reductio ad absurdum δηλαδή: εις άτοπον απαγωγή όπου υποθέτουμε πως το θεώρημα προς απόδειξη είναι εσφαλμένο και αποδεικνύουμε πως το αποτέλεσμα στο οποίο καταλήξαμε είναι παράλογο, άτοπο.

Απόδειξη. Υποθέτουμε πως το θεώρημα της μοναδικής παραγοντοποίησης είναι λάθος. Άρα υπάρχουν αριθμοί με περισσότερες από μια παραγοντοποιήσεις πρώτων.
Αναμεταξύ τους θα πρέπει να υπάρχει και ο μικρότερος όλων τον οποίο θα ονομάσουμε γ_0. Το θεώρημα ισχύει για μικρούς ακεραίους, μέχρι το 10, όπως μπορούμε να δούμε με έναν έλεγχο. Ο αριθμός γ_0 έχει τον μικρότερο πρώτο παράγοντα π_0, οπότε γράφουμε

$$\gamma_0 = \pi_0 \times \delta_0.$$

Αφού $\delta_0 < \gamma_0$, υπάρχει μοναδική παραγοντοποίηση πρώτων του δ_0, που σημαίνει πως η παραγοντοποίηση πρώτων του γ_0 για π_0 είναι μοναδική.

Αφού από υπόθεση υπάρχουν τουλάχιστον δυο παραγοντοποιήσεις πρώτων του γ_0, θα πρέπει να υπάρχει και μια στην οποία δεν θα εμφανίζεται το π_0.

Εδώ τον μικρότερο πρώτο θα τον ονομάσουμε π_1 και θα γράψουμε

(3.1.1.) $\gamma_0 = \pi_1 \times \delta_1$.

Αφού $\pi_1 > \pi_0$, έχουμε $\delta_1 < \delta_0$ άρα και $\pi_0\delta_1 < \gamma_0$. Ας εξετάσουμε τώρα τον αριθμό

(3.1.2.) $\gamma_0' = \gamma_0 - \pi_0\delta_1 = (\pi_1 - \pi_0)\delta_1$.

Εφόσον αυτός είναι μικρότερος αριθμός από το γ_0, θα πρέπει να έχει μοναδική παραγοντοποίηση, και οι πρώτοι παράγοντες του γ_0' θα απαρτίζονται από τους πρώτους παράγοντες του $\pi_1 - \pi_0$ και του δ_1. Αλλά οι πρώτοι παράγοντες στο δ_1 είναι μεγαλύτεροι από το π_0 αφού το π_1 ήταν ο μικρότερος πρώτος στο (3.1.1.). Οπότε η μόνη άλλη πιθανότητα είναι το π_0 να διαιρεί το $\pi_1 - \pi_0$, άρα να διαιρεί το π_1. Όμως αυτό είναι άτοπο, αφού ένας πρώτος π_1 δεν μπορεί να διαιρείται από έναν άλλον πρώτο π_0.

3.2 ΔΙΑΙΡΕΤΕΣ

Ας παραγοντοποιήσουμε έναν αριθμό, ας πούμε το 3600. Η παραγοντοποίηση του

$$3600 = 2 \times 2 \times 2 \times 2 \times 3 \times 3 \times 5 \times 5$$

μπορεί να γραφτεί και

$$3600 = 24 \times 32 \times 52.$$

Ομοίως, γενικότερα, όταν παραγοντοποιούμε έναν αριθμό v μπορούμε να συγκεντρώσουμε όλους τους ίσους πρώτους παράγοντες σε δυνάμεις και να γράψουμε

(3.2.1.) $$v = \pi_1\alpha_1 \times \pi_2\alpha_2 \times \ldots \times \pi_\rho\alpha_\rho,$$

όπου $\pi_1, \pi_2, \ldots, \pi_\rho$ είναι οι διαφορετικοί πρώτοι παράγοντες του v, και ο π_1 εμφανίζεται α_1 φορές, ο π_2 εμφανίζεται α_2 φορές και τα λοιπά. Όταν γνωρίζουμε την μορφή (3.2.1.) ενός αριθμού, μπορούμε να απαντήσουμε αρκετές ερωτήσεις γι' αυτόν τον αριθμό.

Για παράδειγμα, μπορεί να θέλουμε να ξέρουμε ποιοι αριθμοί διαιρούν τον v. Ας πάρουμε σαν παράδειγμα τον αριθμό 3600 που προαναφέραμε. Υποθέτουμε πως ο δ είναι ένας από τους διαιρέτες του, ώστε

$$3600 = \delta \times \delta_1.$$

Η παραγοντοποίηση πρώτων δείχνει ότι οι μόνοι πρώτοι που πιθανόν να μπορούν να παρουσιαστούν ως παράγοντες του δ είναι οι 2, 3 ,5. Επιπλέον, το 2 μπορεί να εμφανιστεί ως παράγοντας το πολύ τέσσερις φορές ενώ το 3 και το 5 το πολύ δυο. Οπότε βλέπουμε πως οι πιθανοί

παράγοντες του 3600 είναι:

$$\delta = 2\delta_1 \times 3\delta_2 \times 5\delta_3$$

όπου έχουμε τις επιλογές

$$\delta_1 = 0, 1, 2, 3, 4 \qquad \delta_2 = 0, 1, 2 \qquad \delta_3 = 0, 1, 2$$

για τους εκθέτες.

Αφού αυτές οι επιλογές μπορούν να συνδυαστούν με όλους τους πιθανούς τρόπους, ο αριθμός των διαιρετών είναι

$$(4 + 1) \times (2 + 1) \times (2 + 1) = 5 \times 3 \times 3 = 45.$$

Η κατάσταση για κάθε αριθμό v με παραγοντοποίηση πρώτων (3.2.1.) είναι ακριβώς η ίδια. Όταν ο δ είναι διαιρέτης του v, δηλαδή

$$v = \delta \times \delta_1$$

τότε οι μόνοι πρώτοι που μπορούν να διαιρέσουν τον δ είναι αυτοί που διαιρούν τον v, δηλαδή οι $\pi_1, \ldots, \pi_\rho$. Οπότε μπορούμε να γράψουμε την παραγοντοποίηση πρώτων του δ με τη μορφή

(3.2.2.) $$\delta = \pi_1\delta_1 \times \pi_2\delta_2 \ldots \pi_\rho\delta_\rho.$$

Ο πρώτος π_1 μπορεί να εμφανιστεί το πολύ α_1 φορές, όπως στο v, και παρομοίως για το π_2 και τους άλλους πρώτους. Αυτό σημαίνει πως για δ_1 έχουμε $\alpha_1 + 1$ επιλογές

$$\delta_1 = 0, 1, \ldots, \alpha_1$$

και παρομοίως για τους υπόλοιπους πρώτους. Αφού κάθε μια από τις $\alpha_1 + 1$ επιλογές για το δ_1 μπορεί να συνδυαστεί με τις $\alpha_2 + 1$ πιθανές αξίες

για το δ_2, και πάει λέγοντας, βλέπουμε ότι ο συνολικός αριθμός ρ(ν) των διαιρετών του *ν* δίνεται από τον τύπο

(3.2.3.) $$\rho(\nu) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_\rho + 1).$$

3.3 ΠΡΟΒΛΗΜΑΤΑ ΜΕ ΔΙΑΙΡΕΤΕΣ

Ο μόνος αριθμός με έναν μόνο διαιρέτη είναι ο $v = 1$. Οι αριθμοί με ακριβώς δυο διαιρέτες είναι οι πρώτοι $v = π$, αφού είναι διαιρέσιμοι από το 1 και το π. Άρα ο μικρότερος αριθμός με δυο διαιρέτες είναι ο $π = 2$.

Ας εξετάσουμε τώρα τους αριθμούς με ακριβώς τρείς διαιρέτες. Σύμφωνα με το (3.2.3.) έχουμε

$$3 = (α_1 + 1)(α_2 + 1) \ldots (α_ρ + 1).$$

Αφού ο 3 είναι πρώτος, μπορεί να υπάρχει μόνο ένας παράγοντας $\neq 1$ στα δεξιά, οπότε $ρ = 1$ και $α_1 = 2$. Επομένως

$$v = π_1^2.$$

Ο μικρότερος αριθμός με τρείς διαιρέτες είναι ο $v = 22 = 4$. Αυτό το επιχείρημα εφαρμόζεται σε κάθε περίπτωση όπου ο αριθμός των διαιρετών είναι ένας πρώτος τ, και βρίσκουμε

$$τ = α_1 + 1, \quad \text{ώστε} \quad α_1 = τ - 1 \quad \text{και} \quad v = π_1^{τ-1},$$

και ο μικρότερος τέτοιος αριθμός είναι ο

$$v = 2^{τ-1}.$$

Ας σκεφτούμε ύστερα την περίπτωση όπου υπάρχουν τέσσερις διαιρέτες. Τότε το

$$4 = (α_1 + 1)(α_2 + 1)$$

είναι πιθανό μόνο όταν

$$\alpha_1 = 3, \quad \alpha_2 = 0, \quad \text{ή} \quad \alpha_1 = \alpha_2 = 1.$$

Αυτό οδηγεί σε δυο εναλλακτικές

$$v = \pi_1^3, \qquad v = \pi_1 \times \pi_2,$$

και ο μικρότερος αριθμός με τέσσερις διαιρέτες είναι ο $v = 6$.

Όταν έχουμε έξι διαιρέτες τότε

$$6 = (\alpha_1 + 1)(\alpha_2 + 1),$$

το οποίο είναι δυνατό μόνο όταν

$$\alpha_1 = 5, \quad \alpha_2 = 0, \quad \text{ή} \quad \alpha_1 = 2, \quad \alpha_2 = 1.$$

Αυτό μας δίνει τις εναλλακτικές

$$v = \pi_1^5, \qquad v = \pi_1^2 \times \pi_2,$$

και η μικρότερη αξία εμφανίζεται στην τελευταία περίπτωση όταν

$$\pi_1 = 2, \quad \pi_2 = 3, \quad v = 12.$$

Η μέθοδος αυτή μπορεί να χρησιμοποιηθεί για τον υπολογισμό του μικρότερου ακεραίου με οποιονδήποτε αριθμό διαιρετών.

Υπάρχουν πίνακες των αριθμών των διαιρετών για τους διάφορους αριθμούς. Ξεκινούν ως εξής:

$v = 1 \;\; 2 \;\; 3 \;\; 4 \;\; 5 \;\; 6 \;\; 7 \;\; 8 \;\; 9 \;\; 10 \;\; 11 \;\; 12$

$v = 1 \;\; 2 \;\; 2 \;\; 3 \;\; 2 \;\; 4 \;\; 2 \;\; 4 \;\; 3 \;\; 4 \;\; 2 \;\; 6$

Ας αναφέρουμε εδώ πως κάθε ακέραιος v είναι υψηλά σύνθετος όταν όλοι οι αριθμοί μικρότεροι του v έχουν λιγότερους διαιρέτες από ότι ο v. Κοιτάζοντας τον πίνακα που έχουμε βλέπουμε πως οι

$$1,\ \ 2,\ \ 4,\ \ 6,\ \ 12$$

είναι οι πρώτοι μεταξύ των υψηλά σύνθετων αριθμών. Για τις ιδιότητες αυτών των αριθμών γνωρίζουμε πολύ λίγα.

3.4 ΤΕΛΕΙΟΙ ΑΡΙΘΜΟΙ

Οι αρχαίοι Έλληνες ήταν λάτρεις της αριθμολογίας ή γεματρίας, όπως αλλιώς την ονομάζουν. Ένας φυσικός λόγος για αυτό ήταν ότι οι Ελληνικοί αριθμοί εκφράζονταν με γράμματα της ελληνικής αλφαβήτου έτσι που κάθε γραμμένη λέξη, κάθε όνομα, ήταν συνδεδεμένο με έναν αριθμό. Δυο άντρες μπορούσαν να συγκρίνουν τις ιδιότητες των αριθμών των ονομάτων τους.

Οι διαιρέτες ή ομαλοί διαιρέτες ενός αριθμού ήταν πολύ σημαντικοί στην αριθμολογία. Ιδανικότεροι, για την ακρίβεια, τέλειοι, ήταν αυτοί οι αριθμοί οι οποίοι απαρτίζονταν μόνο από τους ομαλούς διαιρέτες τους, δηλαδή, όταν το άθροισμα των διαιρετών του ήταν ίσο με τον αριθμό. Εδώ πρέπει να σημειωθεί ότι οι Έλληνες δεν θεωρούσαν τον ίδιο τον αριθμό ως διαιρέτη.

Ο μικρότερος τέλειος αριθμός είναι ο

$$6 = 1 + 2 + 3.$$

Ο επόμενος είναι ο

$$28 = 1 + 2 + 4 + 7 + 14,$$

και ο επόμενος ο

$$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248.$$

Συχνά ένας μαθηματικός που έχει μια ή περισσότερες ειδικές λύσεις για ένα πρόβλημα θα «παίξει» με αυτά μήπως βρει κάποια τακτικότητα η οποία θα δίνει κάποιο στοιχείο που να οδηγεί στην γενική λύση.

Για τους τέλειους αριθμούς έχουμε

$$6 = 2 \times 3 = 2(2^2 - 1),$$

$$28 = 2^2 \times 7 = 2^2(2^3 - 1),$$

$$496 = 2^4 \times 31 = 2^4(2^5 - 1).$$

Αυτό μας οδηγεί να πούμε πως:

Ένας αριθμός είναι τέλειος όταν είναι της μορφής

(3.4.1.) $$\Pi = 2^{\pi-1}(2^{\pi} - 1) = 2^{\pi-1}\tau$$

όπου

$$\tau = 2^{\pi} - 1$$

που είναι πρώτος Mersenne.

Το αποτέλεσμα αυτό, μάλιστα, ήταν γνωστό στους Έλληνες και δεν είναι δύσκολο να αποδειχθεί. Οι διαιρέτες του αριθμού Π συμπεριλαμβανομένου και του ίδιου του Π φαίνεται να είναι

$$1,\ 2,\ 2^2,\ \ldots\ ,\ 2^{\pi-1},$$

$$\tau,\ 2\tau,\ 2^2\tau,\ \ldots\ ,\ 2^{\pi-1}\tau.$$

Το άθροισμα αυτών των διαιρετών είναι

$$1 + 2 + \ldots + 2^{\pi-1} + \tau(1 + 2 + \ldots + 2^{\pi-1})$$

το οποίο ισούται με

$$(1 + 2 + \ldots + 2^{\pi-1})(\tau + 1) = (1 + 2 + \ldots + 2^{\pi-1})2^{\pi}.$$

Σε περίπτωση που δεν θυμόμαστε το άθροισμα της γεωμετρικής σειράς

$$\Sigma = 1 + 2 + \ldots + 2^{\pi-1},$$

πολλαπλασιάζουμε με 2

$$2\Sigma = 2 + 2^2 + \ldots + 2^{\pi-1} + 2^{\pi}$$

και αφαιρούμε το Σ οπότε έχουμε

$$\Sigma = 2^{\pi} - 1 = \tau.$$

Άρα το άθροισμα όλων των διαιρετών του Π είναι

$$2^{\pi}\tau = 2 \times 2^{\pi-1}\tau,$$

και το άθροισμα όλων των διαιρετών εξαιρώντας το $\Pi = 2^{\pi-1}\tau$ είναι

$$2 \times 2^{\pi-1}\tau - 2^{\pi-1}\tau = 2^{\pi-1}\tau = \Pi,$$

άρα ο αριθμός μας είναι τέλειος.

Το αποτέλεσμα αυτό δείχνει ότι κάθε πρώτος Mersenne δημιουργεί έναν τέλειο αριθμό. Όμως, υπάρχουν άλλες μορφές τέλειων αριθμών; Όλοι οι τέλειοι αριθμοί της μορφής (3.4.1.) είναι άρτιοι και είναι δυνατό να αποδείξουμε ότι αν ένας τέλειος αριθμός είναι άρτιος τότε είναι της μορφής (3.4.1.). Αυτό μας οδηγεί στην ερώτηση: Υπάρχουν περιττοί τέλειοι αριθμοί; Μέχρι σήμερα δεν γνωρίζουμε κανέναν και, μάλιστα, είναι ένας από τους σημαντικότερους γρίφους της θεωρίας αριθμών εάν υπάρχει περιττός τέλειος αριθμός.

3.5 ΦΙΛΙΚΟΙ ΑΡΙΘΜΟΙ

Άλλο ένα κληροδότημα της Ελληνικής αριθμολογίας είναι οι φιλικοί αριθμοί.

Όταν δυο άντρες είχαν ονόματα των οποίων οι αριθμητικές αξίες ήταν τόσο συσχετισμένες ώστε το άθροισμα των διαιρετών του ενός να είναι ίσο με την αριθμητική αξία του άλλου και αντίστροφα, τότε εθεωρείτο ως σημάδι στενής σχέσης μεταξύ των δυο. Στην πραγματικότητα οι Έλληνες γνώριζαν μόνο ένα ζευγάρι τέτοιων αριθμών, δηλαδή τους

$$220 = 2^2 \times 5 \times 11, \qquad 284 = 2^2 \times 71$$

Τα αθροίσματα των διαιρετών τους είναι αντίστοιχα

$$1 + 2 + 4 + 5 + 10 + 20 + 11 + 22 + 44 + 55 + 110 = 284$$

$$1 + 2 + 4 + 71 + 142 = 220.$$

Ο Fermat επέκτεινε, έστω και λίγο, την θεωρία των φιλικών αριθμών βρίσκοντας το ζευγάρι

$$17296 = 2^4 \times 23 \times 47, \qquad 18416 = 2^4 \times 1151.$$

Για τις ιδιότητες των αριθμών αυτών γνωρίζουμε πολύ λίγα πράγματα, βασιζόμενοι, όμως, σε πίνακα (http://amicable.homepage.dk/knwnc2.htm) μπορούμε να κάνουμε κάποιες εικασίες. Παραδείγματος χάρη, φαίνεται πως το πηλίκο των δυο αριθμών πρέπει να φτάνει όλο και πιο κοντά στο 1 όσο αυξάνονται. Επίσης, μπορούμε να δούμε πως και οι δυο αριθμοί πρέπει να είναι είτε άρτιοι είτε περιττοί, αλλά δεν έχει βρεθεί ακόμη περίπτωση όπου ο ένας να είναι άρτιος και ο άλλος περιττός. Η έρευνα για φιλικούς αριθμούς αποκάλυψε πως έως τις 28 Σεπτεμβρίου 2007 είχαν βρεθεί 11.994.387 ζευγάρια.

ΜΕΓΙΣΤΟΣ ΚΟΙΝΟΣ ΔΙΑΙΡΕΤΗΣ ΚΑΙ ΕΛΑΧΙΣΤΟ ΚΟΙΝΟ ΠΟΛΛΑΠΛΑΣΙΟ

4.1 ΜΕΓΙΣΤΟΣ ΚΟΙΝΟΣ ΔΙΑΙΡΕΤΗΣ

Το κεφάλαιο αυτό ασχολείται με έννοιες οι οποίες ήταν από τις πρώτες τις οποίες διδαχθήκαμε στο σχολείο όταν μαθαίναμε να κάνουμε υπολογισμούς με κλάσματα. Ο μόνος λόγος για τον οποίο το συμπεριλαμβάνουμε είναι για να υπενθυμίσουμε κάποιες από αυτές τις βασικές έννοιες έτσι ώστε η υπόλοιπη παρουσίαση να γίνει πιο εύκολα κατανοητή.

Ας πάρουμε ένα κλάσμα α/β, το πηλίκο δυο ακεραίων α και β. Συνήθως προσπαθούμε να το μειώσουμε στους μικρότερους όρους του, δηλαδή, να απαλείψουμε παράγοντες κοινούς στο α και το β. Με αυτό τον τρόπο δεν αλλάζουμε την αξία του κλάσματος. Για παράδειγμα,

$$\frac{24}{36} = \frac{8}{12} = \frac{2}{3}$$

Ένας κοινός διαιρέτης δύο ακεραίων α και β είναι ένας ακέραιος δ ο οποίος είναι παράγοντας και του α και του β. Αυτό σημαίνει

$$\alpha = \delta \times \alpha_1 , \qquad \beta = \delta \times \beta_1.$$

Αφού το δ είναι κοινός διαιρέτης των α και β, τότε επίσης διαιρεί τους αριθμούς $\alpha + \beta$ και $\alpha - \beta$ αφού

$$\alpha + \beta = \delta \times \alpha_1 + \delta \times \beta_1 = \delta(\alpha_1 + \beta_1),$$

$$\alpha - \beta = \delta \times \alpha_1 - \delta \times \beta_1 = \delta(\alpha_1 - \beta_1).$$

Όταν γνωρίζουμε τους πρώτους παράγοντες του α και του β δεν είναι δύσκολο να βρούμε όλους τους κοινούς διαιρέτες. Γράφουμε τις δύο παραγοντοποιήσεις πρώτων ως εξής:

(4.1.1.) $\alpha = \pi_1\alpha_1 \dots \pi_\rho\alpha_\rho, \quad \beta = \pi_1\beta_1 \dots \pi_\rho\beta_\rho.$

Εδώ γράφουμε τις παραγοντοποιήσεις ως ο α και ο β να έχουν τους ίδιους πρώτους παράγοντες

$$\pi_1, \ \pi_2, \ \dots, \pi_\rho,$$

συμπεριλαμβανομένης και της περίπτωσης να χρησιμοποιηθούν εκθέτες που είναι μηδέν (0). Για παράδειγμα, αν το π_1 διαιρεί τον α αλλά όχι τον β, θέτουμε $\beta_1 = 0$ στο (4.1.1.).
Έτσι, αν

(4.1.2.) $\alpha = 140, \quad \beta = 110,$

γράφουμε

(4.1.3.) $\alpha = 22 \times 51 \times 71 \times 110, \quad \beta = 21 \times 51 \times 70 \times 111.$

Στο (4.1.1.) ένας διαιρέτης δ του α μπορεί να έχει ως πρώτους παράγοντες μόνο τους π_τ που υπάρχουν στον α, και ο καθένας με εκθέτη δ_τ όχι μεγαλύτερο από το αντίστοιχο α_τ στον α. Ανάλογες συνθήκες ισχύουν για κάθε διαιρέτη δ του β. Συνεπώς, ένας κοινός διαιρέτης δ των α και β μπορεί να έχει ως πρώτους παράγοντες μόνο τους π_τ που εμφανίζονται και στον α και στον β. Ο εκθέτης δ_τ του π_τ στον δ δεν μπορεί να υπερβαίνει τον μικρότερο από τους δύο εκθέτες α_τ και β_τ.
Από αυτό καταλήγουμε ότι:

Κάθε δύο ακέραιοι α και β έχουν έναν μέγιστο κοινό διαιρέτη δ_0. Οι πρώτοι παράγοντες π_τ του δ_0 είναι αυτοί οι οποίοι εμφανίζονται και στον

α και στον β, και ο εκθέτης του π_τ στο δ_0 είναι ο μικρότερος από τους δυο αριθμούς α_τ και β_τ.

Παράδειγμα. Ας πάρουμε τους αριθμούς του (4.1.2.) με τις παραγοντοποιήσεις πρώτων (4.1.3.). Βλέπουμε ότι

$$\delta_0 = 21 \times 51 = 10.$$

Αφού ο εκθέτης ενός πρώτου π_τ στον μέγιστο κοινό διαιρέτη είναι τουλάχιστον όσο μεγάλος όσο σε κάθε άλλο κοινό διαιρέτη έχουμε την χαρακτηριστική ιδιότητα:

Κάθε κοινός διαιρέτης δ διαιρεί τον μέγιστο κοινό διαιρέτη δ_0.

Ο μ.κ.δ. δύο αριθμών είναι τόσο σημαντικός που υπάρχει ειδική σημειογραφία:

(4.1.4.) $\delta_0 = (\alpha, \beta)$.

4.2 ΣΧΕΤΙΚΑ ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ

Ο αριθμός 1 είναι κοινός διαιρέτης κάθε ζεύγους αριθμών α και β. Μπορεί να συμβεί μάλιστα ώστε να είναι και ο μοναδικός κοινός παράγοντας, έτσι ώστε

(4.2.1.) $\delta_o = (\alpha, \beta) = 1.$

Σε αυτή την περίπτωση λέμε πως οι α και β είναι *σχετικά πρώτοι*.

Παράδειγμα : (39, 22) = 1.

Εάν οι αριθμοί έχουν κοινό διαιρέτη μεγαλύτερο του 1, τότε έχουν επίσης έναν κοινό πρώτο διαιρέτη. Οπότε δύο αριθμοί μπορούν να είναι σχετικά πρώτοι μόνο όταν δεν έχουν κοινούς πρώτους παράγοντες. Η συνθήκη (4.2.1.), λοιπόν, σημαίνει ότι το α και το β δεν έχουν κοινούς πρώτους, δηλαδή, όλοι οι πρώτοι παράγοντες τους είναι διαφορετικοί.

Επιστρέφοντας στην αρχή του κεφαλαίου, επιθυμούμε να μειώσουμε το κλάσμα α/β στους χαμηλότερους όρους του. Εάν το δ_o είναι ο μ.κ.δ. του α και του β μπορούμε να γράψουμε

(4.2.2.) $\alpha = \alpha_o \delta_o , \quad \beta = \beta_o \delta_o.$

Επίσης έχουμε

(4.2.3.) $\frac{a}{b} = \alpha_o \delta_o / \beta_o \delta_o = \alpha_o / \beta_o.$

Στο (4.2.2.) δεν μπορεί να υπάρξει κοινός πρώτος παράγοντας για τα α_o και β_o, διότι αλλιώς θα υπήρχε κοινός παράγοντας για τα α και β μεγαλύτερος του δ_o. Συμπεραίνουμε ότι

(4.2.4.) $(\alpha_o, \beta_o) = 1.$

Αυτό σημαίνει ότι το δεύτερο κλάσμα στο (4.2.3.) είναι στους χαμηλότερους όρους του και δεν μπορεί να γίνει περαιτέρω μείωση.

Μια ιδιότητα των σχετικά πρώτων αριθμών εμφανίζεται αρκετά συχνά:

Κανόνας διαίρεσης: Εάν ένα γινόμενο $\alpha\beta$ διαιρείται από αριθμό γ ο οποίος είναι σχετικά πρώτος με τον β, τότε και ο α διαιρείται από τον γ.

Απόδειξη: Αφού ο γ διαιρεί το $\alpha\beta$, οι πρώτοι παράγοντες του γ βρίσκονται μεταξύ εκείνων του α και του β. Αλλά αφού $(\beta, \gamma) = 1$, δεν μπορεί να υπάρχουν στον β. Άρα όλοι οι πρώτοι παράγοντες του γ διαιρούν τον α αλλά όχι τον β, και εμφανίζονται στον α σε δυνάμεις που δεν είναι μικρότερες στον γ αφού ο γ διαιρεί το $\alpha\beta$.

Αργότερα θα χρησιμοποιήσουμε και ένα άλλο γεγονός:

Εάν το γινόμενο δύο σχετικά πρώτων αριθμών είναι τετραγωνικός αριθμός,

(4.2.5.) $\alpha\beta = \gamma^2$, $(\alpha, \beta) = 1$,

τότε και ο α και ο β είναι τετραγωνικοί:

(4.2.6.) $\alpha = \alpha_1^2$, $\beta = \beta_1^2$.

Απόδειξη: Για να είναι τετραγωνικός ένας αριθμός είναι απαραίτητο και επαρκές όλοι οι εκθέτες στην παραγοντοποίηση πρώτων να είναι άρτιοι. Αφού ο α και ο β είναι σχετικά πρώτοι στο (4.2.5.) κάθε πρώτος παράγοντας του γ^2 βρίσκεται στο α ή στο β, αλλά όχι και στους δύο. Άρα οι πρώτοι παράγοντες του α και του β πρέπει να έχουν άρτιους εκθέτες.

4.3 Ο ΑΛΓΟΡΙΘΜΟΣ ΤΟΥ ΕΥΚΛΕΙΔΗ

Επιστρέφουμε στα κλάσματα α/β ξανά. Αν $\alpha > \beta$, τότε το κλάσμα είναι αριθμός μεγαλύτερος του 1, και συχνά το διαχωρίζουμε σε ένα ακέραιο μέρος και σε ένα κλάσμα που είναι μικρότερο του 1.

Γενικώς, για να το κάνουμε αυτό, κάνουμε χρήση της (ατελούς) διαίρεσης δύο ακεραίων $\alpha \geq \beta$, οπότε:

(4.3.1.) $\alpha = \pi\beta + \upsilon$ όπου $0 \leq \upsilon \leq \beta - 1$

Το υ είναι το *υπόλοιπο* της διαίρεσης (4.3.1.) και το π το *(ατελές) πηλίκο*. Το πηλίκο π μάλιστα εμφανίζεται τόσο συχνά που υπάρχει και ειδικό σύμβολο,

$$\pi = [\alpha/\beta]$$

Το σύμβολο αυτό υποδηλώνει τον **μεγαλύτερο ακέραιο που περιέχεται στο α/β**.

Στο 4.1 εξετάσαμε τον μέγιστο κοινό διαιρέτη,

(4.3.2.) $\delta_o = (\alpha, \beta)$

δύο ακεραίων α και β. Για να βρούμε τον δ_o υποθέσαμε πως γνωρίζαμε την παραγοντοποίηση πρώτων του α και του β. Για να τους καθορίσουμε, όμως, για μεγάλους αριθμούς αποδεικνύεται τεράστιο έργο. Υπάρχει μια σημαντική, αρκετά διαφορετική μέθοδος για την εύρεση του μ.κ.δ. η οποία δεν εξαρτάται στην παραγοντοποίηση. Βασίζεται επάνω στο εξής επιχείρημα:

Αν $\alpha = \pi\beta + \upsilon$ όπου $0 \leq \upsilon \leq \beta - 1$, τότε

(4.3.3.) $(\alpha, \beta) = \delta = (\upsilon, \beta)$

Απόδειξη: Έστω $\delta_o = (\alpha, \beta)$, $\delta_1 = (\upsilon, \beta)$

οπότε για να αποδειχθεί η σχέση (4.3.3.) πρέπει $\delta_o = \delta_1$. Κάθε κοινός διαιρέτης του α και του β επίσης διαιρεί και

$$\upsilon = \alpha - \pi\beta$$

συνεπώς το δ_o διαιρεί το υ. Αφού το δ_o είναι διαιρέτης του υ και του β, πρέπει να διαιρεί και $\delta_1 = (\upsilon, \beta)$, έτσι ώστε $\delta_1 \geq \delta_o$. Από την άλλη, σύμφωνα με το (4.3.1.) κάθε κοινός διαιρέτης του υ και του β διαιρεί το α, οπότε το δ_1 διαιρεί το α. Αφού το δ_1 είναι διαιρέτης και του β θα πρέπει να διαιρεί και $\delta_o = (\alpha, \beta)$. Επομένως $\delta_o \geq \delta_1$. Συμπεραίνουμε λοιπόν ότι $\delta_o = \delta_1$.

Παράδειγμα. $1066 = 5 \times 200 + 66$, άρα $(1066, 200) = (66, 200)$.

Το αποτέλεσμα που εκφράζεται στον κανόνα (4.3.3.) μας δίνει μια απλή μέθοδο για τον υπολογισμό του μ.κ.δ. δύο αριθμών. Αντί να ψάχνουμε τον μ.κ.δ. των α και β αρκεί να ψάξουμε τον μ.κ.δ. των υ και β. Έτσι απλοποιείται η αναζήτηση μιας και ο υ είναι μικρότερος και από τον α και από τον β. Για να βρούμε τον μ.κ.δ. των υ και β , χρησιμοποιούμε την ίδια μέθοδο και διαιρούμε το β με το υ:

$$\beta = \pi_1\upsilon + \upsilon_1 ,$$

όπου το υ_1 είναι μικρότερο και από το β και από το υ. Λόγω του κανόνα (4.3.3.) έχουμε :

$$\delta_o = (\alpha, \beta) = (\beta, \upsilon) = (\upsilon, \upsilon_1).$$

Ύστερα, κάνουμε το ίδιο με υ και υ_1 και ούτω καθεξής. Το αποτέλεσμα είναι μια σειρά ζευγαριών αριθμών, όπου το καθένα έχει τον ίδιο μέγιστο κοινό διαιρέτη:

(4.3.4.) $$\delta_o = (\alpha, \beta) = (\beta, \upsilon) = (\upsilon, \upsilon_1) = (\upsilon_1, \upsilon_2) = \ldots$$

Εφόσον τα υπόλοιπα μειώνονται σταθερά η σειρά θα τελειώσει φτάνοντας σε ένα υπόλοιπο $\upsilon_{\kappa+1} = 0$. Αυτό συμβαίνει στην διαίρεση

$$\upsilon_{\kappa-1} = \pi_{\kappa+1}\upsilon_\kappa + 0,$$

άρα το υ_κ διαιρεί το $\upsilon_{\kappa-1}$. Έτσι

$$(\upsilon_{\kappa-1}, \upsilon_\kappa) = \upsilon_\kappa ,$$

και το (4.3.4.) μας δείχνει ότι

$$\delta_o = (\alpha, \beta) = \upsilon_\kappa .$$

Με άλλα λόγια, το δ_o είναι ίσο με το πρώτο υ_κ που διαιρεί το προηγούμενο υπόλοιπο του.

Παράδειγμα. Θα βρούμε τον μ.κ.δ. των αριθμών 1970 και 1066.
Όταν διαιρέσουμε τον έναν αριθμό με τον άλλο όπως παραπάνω, έχουμε:

$$\begin{aligned}
1970 &= 1 \times 1066 + 904 \\
1066 &= 1 \times 904 + 162 \\
904 &= 5 \times 162 + 94 \\
162 &= 1 \times 94 + 68 \\
94 &= 1 \times 68 + 26 \\
68 &= 2 \times 26 + 16 \\
26 &= 1 \times 16 + 10 \\
16 &= 1 \times 10 + 6 \\
10 &= 1 \times 6 + 4 \\
6 &= 1 \times 4 + 2 \\
4 &= 2 \times 2 + 0.
\end{aligned}$$

Επομένως $(1970, 1066) = 2$.

Αυτή η μέθοδος για την εύρεση του μ.κ.δ. δύο αριθμών ονομάζεται *Ευκλείδειος αλγόριθμος*, αφού η πρώτη περιγραφή της εμφανίζεται στα *Στοιχεία* του Ευκλείδη. Είναι εξαιρετικά ταιριαστή για μηχανιστικούς υπολογισμούς.

4.4 ΕΛΑΧΙΣΤΟ ΚΟΙΝΟ ΠΟΛΛΑΠΛΑΣΙΟ

Επιστρέφοντας στα κλάσματα, κατά την πρόσθεση (ή αφαίρεση) δύο κλασμάτων $\frac{g}{a}$, $\frac{d}{b}$, τα φέρνουμε σε κοινό παρονομαστή και ύστερα προσθέτουμε (ή αφαιρούμε) τους αριθμητές.

Γενικώς, για να δημιουργήσουμε το άθροισμα $\frac{g}{a} + \frac{d}{b}$ πρέπει να βρούμε έναν κοινό παρονομαστή του α και του β. Ένας τέτοιος αριθμός είναι προφανής, ήτοι, το γινόμενο τους $\mu = \alpha\beta$. Έτσι έχουμε το άθροισμα των κλασμάτων:

$$\frac{g}{a} + \frac{d}{b} = \frac{gb}{ab} + \frac{da}{ab} = \frac{gb + da}{ab}.$$

Όμως υπάρχουν άπειρα άλλα κοινά πολλαπλάσια των α και β. Ας υποθέσουμε πάλι πως γνωρίζουμε τους πρώτους παράγοντες των δύο αριθμών:

(4.4.1.) $\alpha = \theta_1^{\alpha_1} \ldots \theta_\kappa^{\alpha_\kappa}, \quad \beta = \theta_1^{\beta_1} \ldots \theta_\kappa^{\beta_\kappa}.$

Ένας αριθμός μ που διαιρείται και από το α και από το β πρέπει να διαιρείται και από κάθε πρώτο θ_χ του α και του β σε δυνάμεις με εκθέτη ν_χ όχι μικρότερο από τον μεγαλύτερο των δυο εκθετών α_χ και β_χ. Έτσι, μεταξύ των κοινών πολλαπλασίων μ υπάρχει τουλάχιστον ένα

(4.4.2.) $\mu_0 = \theta_1^{\mu_1} \ldots \theta_\kappa^{\mu_\kappa},$

όπου κάθε εκθέτης μ_χ είναι ίσος με τον μεγαλύτερο των α_χ και β_χ. Αυτό δείχνει ότι το μ_0 είναι το ελάχιστο κοινό πολλαπλάσιο (ε.κ.π.), και κάθε άλλο κοινό πολλαπλάσιο του α και του β διαιρείται από το μ_0. Για αυτό το ε.κ.π. υπάρχει ειδική σημειογραφία:

(4.4.3.) $\mu_0 = [\alpha, \beta].$

Παράδειγμα.

$$\alpha = 140, \qquad \beta = 110.$$

Η παραγοντοποίηση αυτών των αριθμών είναι:

$$\alpha = 2^2 \times 5^1 \times 7^1 \times 11^0 \text{ και } \beta = 2^1 \times 5^1 \times 7^0 \times 11^1.$$

Άρα:

$$[\alpha, \beta] = 2^2 \times 5^1 \times 7^1 \times 11^1 = 1540.$$

Υπάρχει μια απλή σχέση μεταξύ του μ.κ.δ. και του ε.κ.π.:

(4.4.4.) $$\alpha\beta = (\alpha, \beta) \times [\alpha,\beta]$$

Απόδειξη: Όταν πολλαπλασιάζουμε τους δύο αριθμούς (4.4.1.) παίρνουμε

(4.4.5.) $$\alpha\beta = \theta_1^{\alpha_1+\beta_1} \ldots \theta_\kappa^{\alpha_\kappa+\beta_\kappa}.$$

Όπως παρατηρήσαμε, ο εκθέτης ενός πρώτου θ_χ στο (α, β) είναι ο μικρότερος των δύο αριθμών α_χ και β_χ. Στο [α, β] είναι ο μεγαλύτερος. Ας υποθέσουμε, για παράδειγμα, ότι $\alpha_\chi \leq \beta_\chi$. Τότε ο εκθέτης του θ_χ στο (α, β) είναι ο α_χ , και στο [α, β] είναι ο β_χ.

Άρα στο γινόμενο

$$(\alpha, \beta) \times [\alpha,\beta]$$

είναι $\alpha_\chi + \beta_\chi$, το οποίο είναι ακριβώς όπως στο γινόμενο (4.4.5.). Αυτό δείχνει ότι η σχέση (4.4.4.) ισχύει.

Παράδειγμα.

$$\alpha = 140\ , \quad \beta = 110\ , \quad (\alpha, \beta) = 10\ , \quad [\alpha, \beta] = 1540$$
$$\alpha\beta = 140 \times 110 = 10 \times 1540 = (\alpha, \beta) \times [\alpha, \beta].$$

Από τον κανόνα (4.4.4.) βλέπουμε ότι εάν το α και το β είναι σχετικά πρώτοι, τότε το γινόμενο τους ισούται με το ε.κ.π. τους, όπου, σε αυτή την περίπτωση $(\alpha, \beta) = 1$ άρα

$$\alpha\beta = [\alpha, \beta].$$

ΤΟ ΠΥΘΑΓΟΡΕΙΟ ΠΡΟΒΛΗΜΑ

5.1 ΠΡΟΚΑΤΑΡΚΤΙΚΑ

Στο Κεφάλαιο 1.3 αναφέρθηκε ένα από τα αρχαιότερα των αριθμητικών θεωρητικών προβλημάτων: Η εύρεση όλων των ορθογώνιων τριγώνων με ακέραιες πλευρές, δηλαδή, την εύρεση όλων των ακέραιων λύσεων της εξίσωσης

(5.1.1.) $$\zeta^2 = \chi^2 + \psi^2 .$$

Το πρόβλημα αυτό μπορεί να λυθεί με απλές ιδιότητες αριθμών, όμως πριν εξάγουμε αποτέλεσμα θα κάνουμε μερικές προκαταρκτικές παρατηρήσεις. Μια σειρά τριών ακεραίων

(5.1.2.) $$(\chi, \psi, \zeta)$$

που να ικανοποιεί την (5.1.1.) ονομάζεται *Πυθαγόρεια τριάδα*. Παραβλέπουμε την τετριμμένη περίπτωση όπου η μια από τις πλευρές του τριγώνου είναι μηδέν.

Είναι προφανές ότι εάν το (5.1.2.) είναι Πυθαγόρεια τριάδα, τότε κάθε τριάδα

(5.1.3.) $$(\kappa\chi, \kappa\psi, \kappa\zeta)$$

που λαμβάνεται από τον πολλαπλασιασμό κάθε αριθμού με έναν ακέραιο κ είναι επίσης Πυθαγόρεια, και αντιστρόφως. Έτσι, στην αναζήτηση για τις λύσεις, αρκεί να βρούμε τα *πρωταρχικά τρίγωνα*, όπου οι πλευρές δεν έχουν κοινό παράγοντα $\kappa > 1$ όπως στο (5.1.3.).

Παραδείγματος χάριν, τα

$$(6, 8, 10), \qquad (15, 20, 25)$$

είναι Πυθαγόρειες τριάδες οι οποίες προκύπτουν από την πρωταρχική λύση (3, 4, 5).

Σε μια *πρωταρχική τριάδα* (χ, ψ, ζ) δεν υπάρχει κοινός παράγοντας και για τους τρείς αριθμούς. Στην πραγματικότητα, μπορεί να γίνει και πιο ισχυρή δήλωση: *Δεν υπάρχουν δύο αριθμοί μιας πρωταρχικής τριάδας που να έχουν κοινό παράγοντα*, δηλαδή,

(5.1.4.) $$(\chi, \psi) = 1, \quad (\chi, \zeta) = 1, \quad (\psi, \zeta) = 1.$$

Για να το αποδείξουμε αυτό ας υποθέσουμε ότι ο χ και ο ψ έχουν κοινό παράγοντα. Άρα έχουν κοινό πρώτο διαιρέτη π. Σύμφωνα με το (5.1.1.) ο π πρέπει να διαιρεί και τον ζ, άρα το (χ, ψ, ζ) δεν είναι πρωταρχική τριάδα. Το ίδιο επιχείρημα εφαρμόζεται και στις υπόλοιπες συνθήκες του (5.1.4.).

Μπορεί να ειπωθεί ακόμη κάτι για τους αριθμούς σε μια πρωταρχική τριάδα. Μόλις μάθαμε πως ο χ και ο ψ *δεν μπορούν και οι δύο να είναι ζυγοί*. Όμως μπορούμε επίσης να δείξουμε ότι ο χ και ο ψ *δεν μπορούν να είναι ταυτόχρονα μονοί.* Ας υποθέσουμε, λοιπόν, ότι

$$\chi = 2\alpha + 1, \qquad \psi = 2\beta + 1.$$

Όταν τετραγωνίσουμε αυτούς τους αριθμούς και τους προσθέσουμε, παίρνουμε

$$\chi^2 + \psi^2 = (2\alpha + 1)^2 + (2\beta + 1)^2$$

$$= 2 + 4\alpha + 4\alpha^2 + 4\beta + 4\beta^2$$

$$= 2 + 4(\alpha + \alpha^2 + \beta + \beta^2),$$

ένας αριθμός ο οποίος διαιρείται από το 2 αλλά όχι από το 4. Σύμφωνα με το (5.1.1.) αυτό σημαίνει πως το ζ^2 διαιρείται από το 2 αλλά όχι από το 4. Αλλά αυτό δεν είναι δυνατό, αφού, εάν το ζ^2 διαιρείται από το 2, τότε το ζ διαιρείται από το 2 άρα και το ζ^2 διαιρείται από το 4.

Αφού ο ένας εκ των χ, ψ είναι ζυγός και ο άλλος μονός, τότε και ο ζ είναι επίσης μονός. *Θα υποθέσουμε στην σημειογραφία μας ότι ο* χ *είναι ζυγός και ο* ψ *μονός.*

5.2 ΛΥΣΕΙΣ ΤΗΣ ΠΥΘΑΓΟΡΕΙΑΣ ΕΞΙΣΩΣΗΣ

Για την εύρεση των πρωταρχικών λύσεων στην Πυθαγόρεια εξίσωση (5.1.1.), την γράφουμε με την μορφή

(5.2.1.) $\chi^2 = \zeta^2 - \psi^2 = (\zeta + \psi)(\zeta - \psi)$.

Υπενθυμίζουμε ότι ο χ είναι ζυγός όταν οι ζ και ψ είναι μονοί. Οπότε οι τρεις αριθμοί

$$\chi, \quad \zeta + \psi, \quad \zeta - \psi$$

είναι ζυγοί. Έπειτα μπορούμε να διαιρέσουμε και τις δυο πλευρές του (5.2.1.) με το 4 και να πάρουμε

(5.2.2.) $$(\frac{1}{2}\chi)^2 = \frac{1}{2}(\zeta + \psi) \times \frac{1}{2}(\zeta - \psi).$$

Θέτουμε

(5.2.3.) $$\mu_1 = \frac{1}{2}(\zeta + \psi), \quad v_1 = \frac{1}{2}(\zeta - \psi)$$

Οπότε το (5.2.2) γίνεται

(5.2.4.) $$(\frac{1}{2}\chi)^2 = \mu_1 v_1.$$

Οι αριθμοί μ_1 και v_1 στο (5.2.3) είναι σχετικά πρώτοι. Για να το δούμε αυτό, ας υποθέσουμε ότι ο

$$\delta = (\mu_1, v_1)$$

είναι ο *μ.κ.δ.* των μ_1 και v_1. Ύστερα, όπως αναφέραμε στο 4.1, ο αριθμός δ πρέπει να διαιρεί και τους δύο ακεραίους

$$\mu_1 + v_1 = \zeta, \qquad \mu_1 - v_1 = \psi.$$

Αλλά ο μόνος κοινός διαιρέτης των ζ και ψ σε μια πρωταρχική τριάδα είναι το 1, οπότε

$$\delta = (\mu_1, v_1) = 1$$

Αφού το γινόμενο (5.2.4.) αυτών των δυο σχετικά πρώτων αριθμών είναι τετράγωνο, μπορούμε να χρησιμοποιήσουμε το αποτέλεσμα στο τέλος του 4.2 για να καταλήξουμε ότι οι ακέραιοι μ_1 και v_1 είναι τετράγωνα:

(5.2.6.) $$\mu_1 = \mu^2, \; v_1 = v^2, \; (\mu, v) = 1.$$

Εδώ μπορούμε να πάρουμε $\mu > 0$, $v > 0$ χωρίς απώλεια της γενικότητας. Τώρα αντικαθιστούμε μ^2 και v^2 για μ_1 και v_1, αντίστοιχα, στις εξισώσεις (5.2.3.) και (5.2.4.) και έχουμε

$$\mu^2 = \frac{1}{2}\zeta + \frac{1}{2}\psi, \quad v^2 = \frac{1}{2}\zeta - \frac{1}{2}\psi, \quad \mu^2 v^2 = \frac{1}{4}\chi^2,$$

οπότε

(5.2.7.) $$\chi = 2\mu v, \quad \psi = \mu^2 - v^2, \quad \zeta = \mu^2 + v^2.$$

Ένας έλεγχος δείχνει ότι αυτοί οι τρείς αριθμοί πάντα ικανοποιούν την Πυθαγόρεια σχέση $\zeta^2 = \chi^2 + \psi^2$.

Απομένει να προσδιοριστούν ποιοι θετικοί ακέραιοι μ και ν όντως αντιστοιχούν σε πρωταρχικά τρίγωνα. Θα αποδείξουμε ότι οι τρείς ακόλουθες συνθήκες για το μ και το ν είναι απαραίτητες και επαρκείς.

(5.2.8.)

1. $(\mu, \nu) = 1$
2. $\mu > \nu$
3. Ένας εκ των αριθμών μ και ν είναι *ζυγός*, ο άλλος είναι *μονός*.

Απόδειξη: Πρώτα θα αποδείξουμε ότι, εάν οι χ, ψ, ζ δημιουργούν μια πρωταρχική τριάδα, οι συνθήκες (5.2.8.) ευσταθούν. Έχουμε ήδη δείξει ότι η συνθήκη 1. είναι συνέπεια των χ, ψ, ζ, που είναι σχετικά πρώτοι. Η συνθήκη 2. ακολουθείται από το γεγονός ότι οι χ, ψ, ζ, είναι θετικοί αριθμοί. Για να δούμε εάν η συνθήκη 3. είναι απαραίτητη, σημειώνουμε ότι εάν οι μ και ν ήταν και οι δυο περιττοί, τότε σύμφωνα με το (5.2.7.) οι ψ και ζ θα ήταν και οι δύο άρτιοι, αντίθετα με τα συμπεράσματα που βγάλαμε στο τέλος του προηγούμενου τμήματος.

Αντιστρόφως, εάν πληρούνται οι συνθήκες (5.2.8.), τότε το (5.2.7.) καθορίζει μια πρωταρχική τριάδα: η συνθήκη 2. μας διαβεβαιώνει ότι οι χ, ψ, ζ, είναι θετικοί.

Το ερώτημα είναι αν μπορούν οι δύο από τους τρεις να έχουν κοινό πρώτο παράγοντα π. Ένας τέτοιος πρώτος π ο οποίος διαιρεί και τους δύο αριθμούς θα πρέπει επίσης να διαιρεί και τον τρίτο αφού ικανοποιούν την εξίσωση:

$$\zeta^2 = \chi^2 + \psi^2.$$

Εάν ο π διαιρεί τον χ τότε θα πρέπει να διαιρεί και το $2\nu\mu$ σύμφωνα με το (5.2.7.). Ο π δεν μπορεί να είναι 2 γιατί οι ψ και ζ είναι μονοί σύμφωνα με την συνθήκη 3. και το (5.2.7.). Ας υποθέσουμε ότι π *διάφορο του 0* είναι περιττός πρώτος που διαιρεί το μ. Άρα η συνθήκη 1. και το (5.2.7.) δείχνουν ότι ο π δεν μπορεί να διαιρέσει τους ψ και ζ, και το ίδιο ισχύει στην περίπτωση όπου το π διαιρεί το ν.

Έχοντας βρει τις απαραίτητες και αναγκαίες συνθήκες (5.2.8.) ώστε οι μ και ν να δίνουν πρωταρχικό τρίγωνο, μπορούμε πια να υπολογίσουμε κάθε τέτοιο τρίγωνο από τις εκφράσεις του (5.2.7.).
Παραδείγματος χάρη, παίρνουμε

$$\mu = 11, \qquad \nu = 8$$

Οι συνθήκες μας ικανοποιούνται, οπότε βρίσκουμε

$$\chi = 176, \quad \psi = 57, \quad \zeta = 185.$$

5.3 ΠΡΟΒΛΗΜΑΤΑ ΣΧΕΤΙΖΟΜΕΝΑ ΜΕ ΤΑ ΠΥΘΑΓΟΡΕΙΑ ΤΡΙΓΩΝΑ

Λύσαμε το πρόβλημα εύρεσης όλων των Πυθαγόρειων τριγώνων. Έτσι, ως συνήθως στα μαθηματικά, η λύση ενός προβλήματος οδηγεί σε μια ποικιλία άλλων προβλημάτων. Συχνά, μάλιστα, οι ερωτήσεις που δημιουργούνται είναι σημαντικά δυσκολότερες από τις αρχικές.

Μια φυσική ερώτηση σχετικά με τα πρωταρχικά τρίγωνα είναι η εξής:

Όταν η μια πλευρά σε ένα ορθογώνιο τρίγωνο δίνεται, πως υπολογίζονται οι άλλες;

Ας πάρουμε πρώτα την περίπτωση όπου δίνεται η πλευρά ψ.

Σύμφωνα με το (5.2.7.) έχουμε,

$$\psi = \mu^2 - \nu^2 = (\mu + \nu)(\mu - \nu), \tag{5.3.1.}$$

όπου μ και ν αριθμοί που ικανοποιούν τις συνθήκες (5.2.8.). Στο (5.3.1.) οι δύο παράγοντες $(\mu + \nu)$ και $(\mu - \nu)$ είναι σχετικά πρώτοι αριθμοί. Για να το δούμε αυτό παρατηρούμε ότι οι παράγοντες

$$\alpha = \mu + \nu, \quad \beta = \mu - \nu, \tag{5.3.2.}$$

είναι και οι δύο περιττοί εφόσον ο ένας εκ των μ, ν είναι περιττός και ο άλλος άρτιος. Αν οι α και β είχαν κοινό πρώτο περιττό παράγοντα π, τότε ο π θα έπρεπε να διαιρεί και τους δύο αριθμούς

$$\alpha + \beta = \mu + \nu + (\mu - \nu) = 2\mu$$

και

$$\alpha - \beta = \mu + \nu - (\mu - \nu) = 2\nu$$

οπότε ο π θα έπρεπε να διαιρεί και τον μ και τον ν. Αλλά αυτό είναι αδύνατο αφού $(\mu, \nu) = 1$.

Ας υποθέσουμε τώρα ότι έχουμε την εξής παραγοντοποίηση του γνωστού περιττού αριθμού ψ σε δύο παράγοντες

(5.3.3.) $$\psi = \alpha\beta, \quad \alpha > \beta, \quad (\alpha, \beta) = 1$$

Από το (5.3.2.) έχουμε

(5.3.4.) $$\mu = \frac{1}{2}(\alpha + \beta), \quad \nu = \frac{1}{2}(\alpha - \beta).$$

Αυτοί οι δυο αριθμοί είναι επίσης σχετικά πρώτοι, διότι κάθε κοινός παράγοντας θα διαιρούσε το $\alpha = \mu + \nu$ και $\beta = \mu - \nu$. Επιπλέον, οι μ και ν δεν μπορούν να είναι περιττοί, διότι τότε και ο α και ο β θα διαιρούνταν με το 2. Καταλήγουμε ότι οι μ και ν ικανοποιούν τις συνθήκες (5.2.8.) και άρα προσδιορίζουν ένα πρωταρχικό τρίγωνο του οποίου η μια πλευρά είναι $\psi = \mu^2 - \nu^2$.

Παράδειγμα. Έστω $\psi = 15$. Έχουμε δυο παραγοντοποιήσεις (5.3.3.), όπου

$$\psi = 15 = 15 \times 1 = 5 \times 3$$

Το πρώτο δίνει

$$\mu = 8, \quad \nu = 7, \quad \chi = 112, \quad \psi = 15, \quad \zeta = 113,$$

ενώ το δεύτερο δίνει

$$\mu = 4, \quad \nu = 1, \quad \chi = 8, \quad \psi = 15, \quad \zeta = 17.$$

Έπειτα, ας υποθέσουμε ότι μας δίνεται η πλευρά χ. Μιας και ούτε το μ ούτε το v διαιρούνται από το 2, βλέπουμε από το $\chi = 2\mu v$ ότι ο χ πρέπει να διαιρείται με το 4. Αν παραγοντοποιηθεί ο $\frac{1}{2}\chi$ σε δυο σχετικά πρώτους παράγοντες μπορούμε να πάρουμε τον μεγαλύτερο ως μ, και τον μικρότερο ως v.

Παράδειγμα. Έστω $\chi = 24$, με

$$\frac{1}{2}\chi = 24 = 12 \times 1 = 4 \times 3$$

Η πρώτη παραγοντοποίηση δίνει

$$\mu = 12,\ \ v = 1,\ \ \chi = 24,\ \ \psi = 143,\ \ \zeta = 145$$

και η δεύτερη δίνει

$$\mu = 4,\ \ v = 3,\ \ \chi = 24,\ \ \psi = 7,\ \ \zeta = 25.$$

Η τρίτη και τελευταία περίπτωση μας φέρνει σε επαφή με μερικά σημαντικά προβλήματα στην θεωρία αριθμών. Εάν το ζ είναι η υποτείνουσα ενός πρωταρχικού Πυθαγόρειου τριγώνου, τότε, σύμφωνα με το (5.2.7.),

(5.3.5.) $$\zeta = \mu^2 + v^2.$$

όπου, ο ζ είναι το άθροισμα των τετραγώνων των αριθμών μ και v που ικανοποιούν τις συνθήκες (5.2.8.).

Αυτό μας οδηγεί να θέσουμε ένα ερώτημα το οποίο έχει ήδη απαντηθεί από τον Fermat: Πότε μπορεί ένας ακέραιος να γραφεί ως το άθροισμα δυο τετραγώνων;

(5.3.6.) $$\zeta = \alpha^2 + \beta^2;$$

Για την ώρα θα αφήσουμε όλους τους περιορισμούς στους α και β. Μπορεί να έχουν κοινό παράγοντα και ο ένας ή και οι δύο να είναι μηδέν. Μεταξύ των ακεραίων έως το 10 αθροίσματα δύο τετραγώνων είναι οι ακόλουθοι αριθμοί:

$$0 = 0^2 + 0^2,\quad 1 = 1^2 + 0^2,\quad 2 = 1^2 + 1^2,\quad 4 = 2^2 + 0^2,$$
$$5 = 2^2 + 1^2,\quad 8 = 2^2 + 2^2,\quad 9 = 3^2 + 0^2,\quad 10 = 3^2 + 1^2.$$

Οι εναπομείναντες αριθμοί, 3, 6, 7 δεν αναπαρίστανται ως αθροίσματα δύο τετραγώνων.

Θα περιγράψουμε τώρα πως μπορεί να αποφασιστεί αν ένας αριθμός είναι άθροισμα δύο τετραγώνων. Δυστυχώς, οι αποδείξεις δεν είναι απλές και θα πρέπει εδώ να τις παραλείψουμε.

Αρχικά θα εξετάσουμε τους πρώτους αριθμούς. Κάθε πρώτος της μορφής

$\pi = 4v + 1$ είναι το άθροισμα δύο τετραγώνων. Για παράδειγμα,

$$5 = 2^2 + 1^2,\quad 13 = 3^2 + 2^2,\quad 17 = 4^2 + 1^2,\quad 29 = 5^2 + 2^2.$$

Ένα αξιοσημείωτο γεγονός είναι πως αυτή η αντιπροσώπευση μπορεί να γίνει με έναν μοναδικό τρόπο.

Οι υπόλοιποι περιττοί πρώτοι είναι της μορφής $\varphi = 4v + 3$, άρα

$$\varphi = 3,\quad 7,\quad 11,\quad 19,\quad 23,\quad 31,\quad \ldots$$

Κανείς από αυτούς τους πρώτους δεν είναι το άθροισμα δύο τετραγώνων. Για την ακρίβεια, κανένας αριθμός της μορφής $\varphi = 4v + 3$ δεν είναι άθροισμα δύο τετραγώνων. Για γίνει κατανοητό αυτό, παρατηρούμε ότι όταν δύο ακέραιοι α και β είναι άρτιοι, τότε οι α^2 και β^2 διαιρούνται με το 4, άρα και ο $\alpha^2 + \beta^2$ διαιρείται με το 4.

Αν οι α και β είναι περιττοί, παραδείγματος χάρη $\alpha = 2\kappa + 1$, $\beta = 2\lambda + 1$ τότε

$$\alpha^2 + \beta^2 = 4\kappa^2 + 4\kappa + 1 + 4\lambda^2 + 4\lambda + 1$$
$$= 4(\kappa^2 + \lambda^2 + \kappa + \lambda) + 2,$$

άρα ο $\alpha^2 + \beta^2$ έχει υπόλοιπο 2 μετά την διαίρεση με το 4. Τέλος, αν ένας εκ των δύο ακεραίων α, β είναι άρτιος και ο άλλος περιττός, έστω $\alpha = 2\kappa + 1$, $\beta = 2\lambda$, τότε ο

$$\alpha^2 + \beta^2 = 4\kappa^2 + 4\kappa + 1 + 4\lambda^2$$

έχει υπόλοιπο 1 ύστερα από την διαίρεση με το 4. Αφού αυτό εξαντλεί όλες τις πιθανότητες, καταλήγουμε ότι το άθροισμα δυο τετραγώνων δεν είναι ποτέ της μορφής $4v + 3$.

Για να ολοκληρώσουμε την εξέταση των πρώτων παρατηρούμε ότι

$$2 = 1^2 + 1^2.$$

Η εξέταση του εάν ένας σύνθετος αριθμός ζ είναι ή όχι το άθροισμα δύο τετραγώνων γίνεται ως εξής: Έστω ότι η παραγοντοποίηση πρώτων του ζ είναι:

(5.3.7.) $$\zeta = \pi_1^{\alpha_1} \pi_2^{\alpha_2} \ldots$$

Οπότε, το ζ είναι άθροισμα δύο τετραγώνων μόνο και μόνο αν κάθε π_κ της μορφής $4v + 3$ εμφανίζεται με ζυγό εκθέτη.

Παραδείγματα.

Ο $\zeta = 198 = 2 \times 3^2 \times 11$

δεν είναι άθροισμα δύο τετραγώνων αφού ο 11 είναι της μορφής $4v + 3$ και εμφανίζεται στην πρώτη δύναμη.

Ο $\zeta = 194 = 2 \times 97$

είναι άθροισμα δύο τετραγώνων, αφού κανείς εκ των πρώτων παραγόντων του είναι της μορφής $4v + 3$. Βρίσκουμε και

$$\zeta = 13^2 + 5^2 .$$

Επιστρέφοντας στο αρχικό μας πρόβλημα: τον καθορισμό όλων των αριθμών ζ που μπορούν να είναι οι υποτείνουσες των πρωταρχικών Πυθαγόρειων τριγώνων. Ένας τέτοιος αριθμός ζ πρέπει να εκπροσωπείται ως $\zeta = \mu^2 + v^2$, όπου οι αριθμοί μ και v ικανοποιούν τις συνθήκες (5.2.8.).

Ξανά θα παραλείψουμε τις αποδείξεις, αλλά μπορεί να αποδειχθεί ότι μια αναγκαία και επαρκής προϋπόθεση για να ισχύει αυτό είναι: όλοι οι πρώτοι παράγοντες του ζ να είναι της μορφής $\pi = 4v + 1$.

Παράδειγμα.

1) $\zeta = 41$.

Εδώ βρίσκουμε την μοναδική αντιπροσώπευση ως άθροισμα δυο τετραγώνων του επιθυμητού είδους,

$$\zeta = 5^2 + 4^2,$$

άρα

$$\mu = 5, \quad v = 4 \qquad \chi = 40, \quad \psi = 9, \quad \zeta = 41.$$

Όπως βλέπουμε είναι το αντίστοιχο τρίγωνο.

Μια ποικιλία προβλημάτων σχετικά με τα Πυθαγόρεια τρίγωνα μπορεί να λυθεί μέσω των τύπων (5.2.7.),

$$\chi = 2\mu v, \quad \psi = \mu 2 - v2, \quad \zeta = \mu 2 + v2.$$

Έχοντας λύσει ένα μεγάλο μέρος του προβλήματος κατασκευής όλων των Πυθαγόρειων τριγώνων, οδηγούμαστε στην εξερεύνηση πιο γενικών προβλημάτων. Μια φυσική επέκταση είναι προς τα *τρίγωνα του Ήρωνος*, που ανέπτυξε ο Έλληνας μηχανικός και γεωμέτρης Ήρων ο Αλεξανδρεύς. Σε αυτά τα τρίγωνα απαιτείται, όπως πριν, οι πλευρές χ, ψ, ζ να είναι ακέραιοι αριθμοί, όμως δεν έχουμε την προϋπόθεση η μια γωνία να είναι 90^o αλλά το εμβαδόν του τριγώνου να είναι, επίσης, ακέραιος αριθμός. Τα Πυθαγόρεια τρίγωνα εμπίπτουν ξεκάθαρα σε αυτή την κατηγορία.

Για να ελέγξουμε αν ένα δεδομένο τρίγωνο είναι *του Ήρωνος*, είναι απλούστερο να χρησιμοποιήσουμε τον τύπο του Ήρωνος για το εμβαδό ενός τριγώνου,

$$A = \sqrt{g/2(g/2-c)(g/2-y)(g/2-z)}$$

όπου *γ* η περίμετρος ενός τριγώνου.

(Η περίμετρος ενός τριγώνου είναι:

(5.3.9.) $\gamma = \chi + \psi + \zeta$

Για ένα πρωταρχικό τρίγωνο είναι

$$\gamma = 2\mu\nu + (\mu^2 - \nu^2) + (\mu^2 + \nu^2) = 2\mu(\mu + \nu).)$$

Αν και γνωρίζουμε έναν σημαντικό αριθμό τριγώνων του Ήρωνος, δεν έχουμε έναν γενικό τύπο που να τα δίνει όλα. Αυτά είναι μερικά από τα πρώτα (μη-ορθογώνια) παραδείγματα:

$\chi = 7,$	$\psi = 15,$	$\zeta = 20$
9	10	17
13	14	15
39	41	50

Τέλος, δεν μπορούμε να κλείσουμε το κεφάλαιο των Πυθαγόρειων τριγώνων χωρίς να αναφερθούμε σε ένα από τα πιο διάσημα προβλήματα των μαθηματικών, την εικασία του Fermat:

« Δεν υπάρχουν **ακέραιοι χ, ψ, ζ** που να ικανοποιούν την εξίσωση

$$\zeta^{\kappa} = \chi^{\kappa} + \psi^{\kappa} \quad \text{για} \quad \kappa > 2$$ »

(Αντίθετα με την περίπτωση κ = 2 που οι λύσεις της είναι οι προαναφερθείσες Πυθαγόρειες τριάδες.)

Η ιδέα ήρθε στον Fermat όσο μελετούσε την μετάφραση από τα ελληνικά της πραγματείας του Διόφαντου *Arithmetica (φωτογραφία εξώφυλλου)*. Το έργο αυτό ασχολείται κυρίως με προβλήματα στα οποία εφαρμόζονται οι τύποι για τα Πυθαγόρεια τρίγωνα, και ο Fermat έκανε τα σχόλια του στο περιθώριο. Συγκεκριμένα, έγραψε: « Έχω βρει μια εκπληκτική απόδειξη αυτής της πρότασης , την οποία το περιθώριο αυτού εδώ του βιβλίου είναι πολύ μικρό για να χωρέσει ».

Ο Fermat έγραψε και άλλα τέτοια εξοργιστικά σημειώματα και μετά το θάνατό του ο γιος του εξέδωσε μια έκδοση του *Arithmetica* η οποία περιείχε όλα αυτά τα πειραχτικά προς τους μαθηματικούς σχόλια. Τελικά αυτό που συνέβη στην πράξη ήταν να αποδειχθούν και τα συνθετότερα των θεωρημάτων και ένα μόνο να μείνει άλυτο: **το τελευταίο θεώρημα του Fermat**.

Πολλοί μαθηματικοί πολέμησαν κατά καιρούς να βρουν κάποια απόδειξη , όμως τελικά αποτύγχαναν. Ενδεικτικά, αναφέρουμε τους:

Leonhard Euler, Kausler, Legendre, Lamé, Peter Guthrie Tait, Gambioli, Krey, Rychlík, Stockhaus, Axel Thue, Duarte, Carl Friedrich Gauss, Lebesgue, Guy Terjanian, Niels Henrik Abel, Peter Barlow, Sophie Germain, Frénicle de Bessy, David Hilbert, Leopold Kronecker, Hancock, Vrănceanu.

Το 1742 ο Leonard Euler , ο μεγαλύτερος θεωρητικός της θεωρίας των αριθμών του 18ου αιώνα , απογοητεύτηκε τόσο από την ανικανότητά του να επιλύσει το πρόβλημα , που ζήτησε από ένα φίλο του να ψάξει το σπίτι του Fermat μήπως και τυχόν έβρισκε κάποιο μυστικό παραπεταμένο σημείωμα που θα βοηθούσε στην προσπάθεια επίλυσης(!).

Τον 19ο αιώνα η Sophie Germain – η οποία λόγω προκατάληψης προς τις γυναίκες μαθηματικούς χρησιμοποιούσε τον ανδρικό τίτλο Monsieur Leblanc – έκανε το πρώτο μικρό αλλά αποφασιστικό βήμα. Η Germain απέδειξε ένα γενικό θεώρημα το οποίο επιχειρούσε να βοηθήσει στην εύρεση λύσεων για την εξίσωση Fermat για τιμές του κ > 2 που είναι πρώτοι αριθμοί έτσι ώστε και ο αριθμός 2κ+1 να είναι επίσης πρώτος. Αλλά μια πλήρης απόδειξη για ύπαρξη τέτοιου είδους εκθετών που δίνουν λύσεις παρέμεινε έξω από τις δυνατότητές της .

Στην αρχή του 20ού αιώνα, ο Paul Wolfskehl , ένας Γερμανός βιομήχανος κληροδότησε 100.000 μάρκα σε όποιον θα αντιμετώπιζε επιτυχώς την πρόκληση του Fermat. Σύμφωνα με κάποιους ιστορικούς, ο Wolfskehl βρισκόταν σε κάποια περίοδο στα πρόθυρα αυτοκτονίας , αλλά απέκτησε τόσο πάθος στην προσπάθεια να βρει τη λύση στο πρόβλημα που είχε θέσει ο Fermat που σύντομα εγκατέλειψε την ιδέα περί αυτοκτονίας. Επηρεασμένος από αυτήν την τροπή που είχαν πάρει τα πράγματα ο Wolfskehl ξαναέγραψε την διαθήκη του . Το βραβείο που όρισε ήταν κάτι σαν χρέος στον γρίφο που του είχε σώσει την ζωή.
Παραδόξως , παρόλο που το βραβείο Wolfskehl ωθούσε τους χομπίστες μαθηματικούς να βρουν τη λύση , οι επαγγελματίες έχαναν κάθε ελπίδα. Γενικά μέχρι εκείνη την εποχή η απόδειξη του τελευταίου θεωρήματος του Fermat αποτελούσε ένα ρομαντικό και απραγματοποίητο όνειρο από το παρελθόν και τίποτα παραπάνω.

Για περίπου τρεισήμισι αιώνες , το τελευταίο θεώρημα του Fermat ήταν ένα μεμονωμένο πρόβλημα , ένας μυστηριώδης και αποκλεισμένος γρίφος των μαθηματικών. Το 1986, ο Kenneth Alan Ribet (Αμερικανός καθηγητής στο πανεπιστήμιο του Berkeley, California) δουλεύοντας πάνω στο δρόμο που είχε ανοίξει ο Γερμανός συνάδελφος του Gerhard Frey (Καθηγητής θεωρίας αριθμών στο Πανεπιστήμιο του Duisburg-Essen) , είχε πετύχει να αναδείξει για τα καλά το πρόβλημα και αναζωπυρώσει το ενδιαφέρον για την επίλυσή του.

Εδώ εμφανίζεται ο Βρετανός καθηγητής Andrew John Wiles (καθηγητής του Πανεπιστημίου Princeton, New Jersey και χρισμένος Sir πλέον), ο οποίος, γοητευμένος με το τελευταίο θεώρημα του Fermat από τα 10 του χρόνια, αποφασίζει, βασιζόμενος στην δουλειά των Frey και Ribet να αποδείξει την ορθότητα του θεωρήματος. Για έξι χρόνια ο Wiles εργάζεται με απόλυτη μυστικότητα. Πρέπει, για να πετύχει το εγχείρημά του, να καταφέρει να αξιοποιήσει και να συνδυάσει τις μέχρι τότε γνωστές μεθόδους από την θεωρία των αριθμών. Όταν οι θεωρίες αυτές αποδεικνύονται ανεπαρκείς , αναγκάζεται να επινοεί και να χρησιμοποιεί νέες δικές του μεθόδους.

Τελικά, στις 23 Ιουνίου του 1993 ο Wiles περιχαρής ανακοινώνει την συνολική του μελέτη σε ένα συνέδριο στο Πανεπιστήμιο του Cambridge και εκπλήσσει όλη τη μαθηματική κοινότητα.

Ωστόσο δεν αργούν και πολύ να εμφανιστούν τα πρώτα σημάδια που θέτουν σε αμφισβήτηση το κύρος της μελέτης του Wiles. Και αυτό συμβαίνει όταν ο καθηγητής Nicholas Katz από το Princeton εντοπίζει μια ατέλεια στην αποδεικτική διαδικασία που είχε ακολουθηθεί. Στην επαγωγική του μέθοδο ο Wiles είχε δανειστεί την μέθοδο Kolyvagin-Flach από δύο διαφορετικούς καθηγητές αμερικανικών Πανεπιστημίων. Όμως οι μέθοδοι αυτές φαινόταν ότι δεν μπορούσαν να εφαρμοστούν για συγκεκριμένους λόγους στην προκειμένη περίπτωση και έτσι καθιστούσαν την όλη απόδειξη ανεπαρκή.

Για τους επόμενους 14 μήνες ο Wiles αποσύρεται από τα φώτα της δημοσιότητας και συζητά το όλο θέμα μόνο με ένα παλιό μαθητή του , τον Richard Taylor . Μαζί προσπαθούν να βρουν λύση στο πρόβλημα , διατηρώντας τη μέθοδο που είχε χρησιμοποιήσει ο Wiles και τροποποιώντας την κατάλληλα ούτως ώστε να δίνει ικανοποιητικά αποτελέσματα. Έχουν αρχίσει να χάνουν κάθε ελπίδα όταν τελικά το Σεπτέμβριο του 1994 βρίσκουν την ζωτική λύση. Ο Wiles διαπιστώνει ότι μια επιμέρους μέθοδος που είχε απορρίψει στο παρελθόν μπορεί να πετύχει ακριβώς για τον ίδιο λόγο που αποτύγχανε η μέθοδος Kolyvagin-Flach, για την οποία είχε γίνει όλη η φασαρία και του είχε δημιουργήσει πονοκέφαλο.

Έτσι, 358 χρόνια μετά την διάσημη εικασία του Fermat κατά τα λεγόμενα του Wiles: « Η οδύσσεια φτάνει στο τέλος της ».

Για άλλους μαθηματικούς όμως, αρκετά μεγάλα ερωτήματα είναι ακόμα ανοιχτά. Συγκεκριμένα όλοι συμφωνούν στο ότι η απόδειξη που έδωσε ο Wiles είναι τελικά αρκετά πολύπλοκη και μοντέρνα ώστε να προσεγγίζει αυτό που είχε στο μυαλό του ο Fermat όταν έγραψε το περίφημο σημείωμα στο *Arithmetica*. Συνεπώς, είτε ο Fermat έκανε λάθος και η απόδειξή του – αν ποτέ υπήρξε – ήταν ανεπαρκής, είτε μια απλή και αφοπλιστική απόδειξη περιμένει την ανακάλυψή της.

ΑΝΑΛΟΓΙΕΣ

6.1 ΟΡΙΣΜΟΣ ΑΝΑΛΟΓΙΩΝ

Η θεωρία αριθμών έχει την δική της άλγεβρα, γνωστή ως *θεωρία αναλογιών*. Η κοινή άλγεβρα αρχικά αναπτύχθηκε ως στενογραφία για τις λειτουργίες της αριθμητικής. Παρομοίως, οι αναλογίες αντιπροσωπεύουν μια συμβολική γλώσσα για την διαιρετότητα, την βασική έννοια της θεωρίας αριθμών. Πρώτος ο Gauss εισήγαγε την ιδέα των αναλογιών.

Προτού στραφούμε στις αναλογίες θα κάνουμε ένα σχόλιο σχετικά με τους αριθμούς τους οποίους θα μελετήσουμε σε αυτό το κεφάλαιο. Στην αρχή της εργασίας αυτής αναφέραμε ότι θα μας απασχολήσουν οι θετικοί ακέραιοι 1, 2, 3, …, και σε προηγούμενα κεφάλαια περιοριστήκαμε σε αυτούς και στον επιπρόσθετο αριθμό 0. Έχουμε φτάσει πλέον στο σημείο όπου είναι επωφελές να διευρύνουμε το πεδίο μας ώστε να συμπεριληφθούν όλοι οι ακέραιοι, θετικοί και αρνητικοί,

$$0, \quad \pm 1, \quad \pm 2, \quad \pm 3, \quad \ldots$$

Αυτό δεν επηρεάζει με κανέναν τρόπο τις προηγούμενες έννοιες μας. Εν συνεχεία, όταν θα μιλάμε για πρώτους, διαιρέτες, μέγιστους κοινούς διαιρέτες και τα συναφή, θα συνεχίσουμε να τους λαμβάνουμε ως θετικούς ακεραίους.

Ας επιστρέψουμε τώρα στην γλώσσα των αναλογιών. Αν α και β είναι δύο ακέραιοι και η διαφορά τους $\alpha - \beta$ διαιρείται από μ, το εκφράζουμε γραπτώς ως εξής:

(6.1.1.) $$\alpha \equiv \beta \ (mod\ \mu)$$

Και διαβάζεται

$$\alpha \text{ ανάλογο του } \beta, \text{ modulo } \mu.$$

Υποθέτουμε πως ο διαιρέτης μ είναι θετικός και ονομάζεται *modulus* της αναλογίας.

Οι δηλώσεις (6.1.1.) σημαίνουν

(6.1.2.) $\alpha - \beta \equiv \mu\kappa$, όπου κ ακέραιος.

Παραδείγματα.

1) $23 \equiv 8 \pmod 5$ αφού $23 - 8 = 15 = 5 \times 3$

2) $47 \equiv 11 \pmod 9$ αφού $47 - 11 = 36 = 9 \times 4$

3) $-11 \equiv 5 \pmod 8$ αφού $-11 - 5 = -16 = 8 \times (-2)$

4) $81 \equiv 0 \pmod{27}$ αφού $81 - 0 = 81 = 27 \times 3$.

Το τελευταίο παράδειγμα δείχνει ότι, γενικώς, αντί να πούμε ότι ένας αριθμός α είναι διαιρέσιμος από τον αριθμό μ μπορούμε να γράψουμε

$$\alpha \equiv 0 \pmod{\mu}$$

αφού αυτό σημαίνει

$$\alpha - 0 = \alpha = \mu\kappa$$

όπου κ κάποιος ακέραιος. Για παράδειγμα, αντί να πούμε πως ο α είναι ζυγός αριθμός μπορούμε να γράψουμε

$$\alpha \equiv 0 \pmod 2.$$

Με τον ίδιο τρόπο βλέπουμε πως και ένας περιττός αριθμός είναι ένας αριθμός που ικανοποιεί το

$$\alpha \equiv 1 \pmod 2.$$

Αυτή η, κατά κάποιον τρόπο, “αλλόκοτη” ορολογία είναι αρκετά κοινή στα μαθηματικά γραπτά.

6.2 ΙΔΙΟΤΗΤΕΣ ΑΝΑΛΟΓΙΩΝ

Ο τρόπος με τον οποίο γράφουμε τις αναλογίες μας θυμίζει τις εξισώσεις, και, πράγματι, οι αναλογίες και οι αλγεβρικές εξισώσεις έχουν αρκετές κοινές ιδιότητες. Οι απλούστερες είναι οι ακόλουθες τρείς:

(6.2.1.) $\alpha \equiv \alpha \pmod{\mu}$

το οποίο είναι συνέπεια του $\alpha - \alpha = 0 = \mu \times 0$

(6.2.2.) $\alpha \equiv \beta \pmod{\mu}$ που υποδηλώνει $\beta \equiv \alpha \pmod{\mu}$.

Αυτό προέρχεται από $\beta - \alpha = -(\alpha - \beta) = \mu(-\kappa)$.

(6.2.3.) $\alpha \equiv \beta \pmod{\mu}$, και $\beta \equiv \gamma \pmod{\mu}$

υποδηλώνουν

$$\alpha \equiv \gamma \pmod{\mu},$$

διότι οι δύο πρώτες δηλώσεις σημαίνουν

$$\alpha - \beta = \mu\kappa, \qquad \beta - \gamma = \mu\lambda,$$

έτσι ώστε

$$\alpha - \gamma = (\alpha - \beta) + (\beta - \gamma) = \mu(\kappa + \lambda).$$

Παράδειγμα. Από

$$13 \equiv 35 \pmod{11}, \quad 35 \equiv -9 \pmod{11}$$

Συνεπάγεται πως

$$13 \equiv -9 \pmod{11}$$

Είπαμε πως οι αναλογίες μοιάζουν με ισότητες στις ιδιότητες τους. Στην πραγματικότητα μπορούμε να θεωρήσουμε μια ισότητα ότι είναι τύπος αναλογίας, συγκεκριμένα, της αναλογίας *modulo* 0. Εξ ορισμού

$$\alpha \equiv \beta \pmod{0}$$

το οποίο σημαίνει

$$\alpha - \beta = 0 \times \kappa = 0 \qquad \text{ή} \qquad \alpha = \beta.$$

Η αλήθεια είναι πως αυτή την αναλογικού τύπου γραφή εξισώσεων δεν θα την συναντήσουμε σχεδόν ποτέ στην μαθηματική φιλολογία. Όμως, υπάρχει μια άλλη αναλογία, προφανώς αρκετά τετριμμένη, η οποία χρησιμοποιείται ενίοτε. Όταν το *modulus* είναι $\mu = 1$, τότε έχουμε

(6.2.4.) $$\alpha \equiv \beta \pmod{1}$$

για κάθε ζεύγος ακεραίων α και β, αφού αυτό σημαίνει ότι ο

(6.2.5.) $$\alpha - \beta = 1 \times \kappa = \kappa$$

είναι ακέραιος. Ας υποθέσουμε τώρα, για λίγο, πως οι α και β είναι αυθαίρετοι πραγματικοί αριθμοί και όχι απαραίτητα ακέραιοι. Άρα το γεγονός πως είναι ανάλογοι (mod 1) σημαίνει πως η διαφορά τους είναι ακέραιος, και αυτό, διότι έχουν το ίδιο κλασματικό μέρος (ή δεκαδικό μέρος εάν είναι γραμμένοι ως δεκαδικοί).

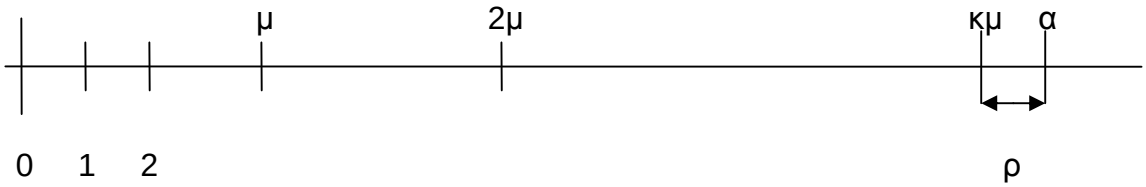
Παράδειγμα. $8\frac{1}{3} = 1\frac{1}{3} \pmod 1$

ή

$8.333\ldots = 1.333\ldots \pmod 1$.

Ας επιστρέψουμε στις ιδιότητες των συνηθισμένων αναλογιών ακεραίων. Από εδώ και στο εξής θα υποθέτουμε πάντα πως το *modulus* είναι ακέραιος $\mu \geq 2$.

Μπορούμε να διαιρέσουμε έναν άξονα αριθμών, από την αρχή προς τις δυο κατευθύνσεις, σε διαστήματα μήκους μ όπως στο σχήμα 6.2.1.



Σχήμα 6.2.1.

Έτσι, κάθε ακέραιος α, θετικός ή αρνητικός, θα εμπίπτει σε κάποιο από αυτά τα διαστήματα ή σε κάποια από τις γραμμές που τον διαιρούν, οπότε μπορούμε να γράψουμε

(6.2.6.) $$\alpha = \kappa\mu + \rho,$$

όπου κ κάποιος ακέραιος και ρ ένας από τους αριθμούς

(6.2.7.) $$0, 1, 2, \ldots, \mu - 1.$$

Αυτή είναι μια μικρή γενίκευση της διαίρεσης των θετικών ακεραίων στο κεφάλαιο 4.3. Επίσης, εδώ καλούμε το ρ στο (6.2.6.) το *υπόλοιπο* του α όταν διαιρείται με το μ, ή *υπόλοιπο* (mod μ).

Παραδείγματα.

1) $\alpha = 11, \quad \mu = 7, \quad 11 = 7 \times 1 + 4$

2) $\alpha = -11, \quad \mu = 7, \quad -11 = 7 \times (-2) + 3$

Η διαίρεση (6.2.6.) μπορεί επίσης να γραφτεί ως αναλογία

(6.2.8.) $$\alpha \equiv \rho \ (\text{mod } \mu),$$

ώστε κάθε αριθμός να είναι ανάλογος του υπολοίπου του (mod μ). Στα παραπάνω παραδείγματα έχουμε

$$11 \equiv 4 \ (\text{mod } 7), \quad -11 \equiv 3 \ (\text{mod } 7).$$

Δεν υπάρχουν δυο εκ των υπολοίπων του (6.2.7.) που να είναι ανάλογα (mod μ), διότι η διαφορά μεταξύ οποιονδήποτε δυο είναι μικρότερη του μ. Επομένως, δυο αριθμοί δυσανάλογοι (μη ανάλογοι) (mod μ) πρέπει να έχουν διαφορετικά υπόλοιπα. Άρα συμπεραίνουμε:

Μια αναλογία $\alpha \equiv \beta \ (\text{mod } \mu)$ ισχύει **μόνο και μόνο αν** οι α και β είναι αριθμοί που έχουν το ίδιο υπόλοιπο όταν διαιρούνται από το μ.

6.3 Η ΑΛΓΕΒΡΑ ΤΩΝ ΑΝΑΛΟΓΙΩΝ

Θυμόμαστε από την άλγεβρα ότι οι εξισώσεις μπορούν να προστεθούν, αφαιρεθούν, πολλαπλασιαστούν. Ακριβώς οι ίδιοι κανόνες ισχύουν στις αναλογίες. Ας υποθέσουμε ότι έχουμε τις αναλογίες

(6.3.1.) $\alpha \equiv \beta \pmod{\mu}, \quad \gamma \equiv \delta \pmod{\mu},$

Εξ ορισμού αυτό σημαίνει πως

(6.3.2.) $\alpha = \beta + \mu\kappa, \quad \gamma = \delta + \mu\lambda,$

όπου κ και λ ακέραιοι. Ας προσθέσουμε τώρα τις εξισώσεις (6.3.2.). Το αποτέλεσμα είναι

$$\alpha + \gamma = \beta + \delta + \mu(\kappa + \lambda)$$

το οποίο μπορεί να γραφεί και

(6.3.3.) $\alpha + \gamma \equiv \beta + \delta \pmod{\mu}$

Με άλλα λόγια, δυο αναλογίες μπορούν να προστεθούν. Με τον ίδιο τρόπο μπορούμε να δείξουμε ότι μια αναλογία μπορεί να αφαιρεθεί από μια άλλη, δηλαδή

(6.3.4.) $\alpha - \gamma \equiv \beta - \delta \pmod{\mu}.$

Παράδειγμα.

(6.3.5.) $11 \equiv -5 \pmod{8}, \quad \text{και} \quad 7 \equiv -9 \pmod{8}.$

Προσθέτοντας τις παίρνουμε

$$18 \equiv -14 \pmod 8$$

και αφαιρώντας τις,

$$4 \equiv 4 \pmod 8.$$

Και οι δυο είναι κανονικές αναλογίες.

Μπορούμε επίσης να πολλαπλασιάσουμε δυο αναλογίες. Από (6.3.1.) και (6.3.2.) έχουμε

$$\alpha\gamma = \beta\delta + \mu(\kappa\delta + \beta\lambda + \mu\kappa\lambda),$$

ώστε

(6.3.6.) $$\alpha\gamma \equiv \beta\delta \pmod \mu.$$

Παράδειγμα. Πολλαπλασιάζοντας τις δυο αναλογίες του (6.3.5.) παίρνουμε

$$77 \equiv 45 \pmod 8$$

Μια αναλογία $\alpha \equiv \beta \pmod \mu$ μπορεί να πολλαπλασιαστεί με οποιονδήποτε ακέραιο γ για να έχουμε

(6.3.7.) $$\alpha\gamma \equiv \beta\gamma \pmod \mu.$$

Αυτή η αναλογία μπορεί να λάβει υπόψη μια ιδιαίτερη περίπτωση του πολλαπλασιασμού (6.3.6.) για $\gamma = \delta$. Ή προκύπτει άμεσα από τον ορισμό των αναλογιών.

Παράδειγμα. Πολλαπλασιάζοντας την πρώτη αναλογία του (6.3.5.) με τον αριθμό 3 αποκτούμε

$$33 \equiv -15 \pmod 8.$$

Είναι λογική απορία να ρωτήσουμε πότε, σε μια αναλογία (6.3.7.), μπορούμε να απαλείψουμε τον κοινό παράγοντα γ και έτσι να αποκτήσουμε μια 'σωστή' αναλογία

$$\alpha \equiv \beta \pmod \mu.$$

Σε αυτό το σημείο οι αναλογίες διαφέρουν από τις εξισώσεις. Παραδείγματος χάρη, έχουμε

$$22 \equiv -2 \pmod 8,$$

αλλά η απαλοιφή του παράγοντα 2 θα μας έδινε

$$11 \equiv -1 \pmod 8$$

το οποίο δεν είναι αληθές.

Υπάρχει, όμως, μια σημαντική περίπτωση κατά την οποία η απαλοιφή επιτρέπεται:

Αν $\alpha\gamma \equiv \beta\gamma \pmod \mu$, τότε $\alpha \equiv \beta \pmod \mu$ **μόνο και μόνο αν** οι μ και γ είναι σχετικά πρώτοι.

Απόδειξη: Η πρώτη αναλογία σημαίνει

$$\alpha\gamma - \beta\gamma = (\alpha - \beta)\gamma = \mu\kappa.$$

Αν $(\mu, \gamma) = 1$, συνεπάγεται ότι το $\alpha - \beta$ διαιρείται με το μ σύμφωνα με το αποτέλεσμα που αποδείξαμε στο κεφάλαιο 4.2 .

Παράδειγμα. Στην αναλογία

$$4 \equiv 48 \pmod{11}$$

μπορούμε να απαλείψουμε τον παράγοντα 4, αφού $(11, 4) = 1$. Αυτό μας αποφέρει

$$1 \equiv 12 \pmod{11}.$$

6.4 ΔΥΝΑΜΕΙΣ ΑΝΑΛΟΓΙΩΝ

Ας υποθέσουμε πάλι πως έχουμε μια αναλογία

$$\alpha \equiv \beta \pmod{\mu}.$$

Όπως μόλις είδαμε, μπορούμε να πολλαπλασιάσουμε αυτή την αναλογία με τον εαυτό της και έτσι να έχουμε

$$\alpha^2 \equiv \beta^2 \pmod{\mu}.$$

Γενικότερα, μπορούμε να πολλαπλασιάσουμε την αναλογία με τον εαυτό της τόσες φορές μέχρι να έχουμε

$$\alpha^{\nu} \equiv \beta^{\nu} \pmod{\mu}$$

για κάθε θετικό ακέραιο *ν*.

Παράδειγμα. Από

$$8 \equiv -3 \pmod{11}$$

ακολουθεί, με τετραγωνισμό,

$$64 \equiv 9 \pmod{11},$$

και, υψώνοντας στην τρίτη,

$$512 \equiv -27 \pmod{11}.$$

Πολλά από τα αποτελέσματα στις αναλογίες ασχολούνται με την εύρεση των υπολοίπων των υψηλών δυνάμεων ενός αριθμού. Ας δείξουμε τώρα πως μπορούμε να προχωρήσουμε. Ας υποθέσουμε, για παράδειγμα, πως θέλουμε να βρούμε το υπόλοιπο του $3^{89} \pmod 7$.
Ένας τρόπος να το βρούμε είναι με επαναλαμβανόμενους τετραγωνισμούς.

Βρίσκουμε λοιπόν

$$\begin{aligned} 9 = 3^2 &\equiv 2 \pmod 7 \\ 3^4 &\equiv 4 \\ 3^8 &\equiv 16 = 2 \\ 3^{16} &\equiv 4 \\ 3^{32} &\equiv 16 = 2 \\ 3^{64} &\equiv 4 \pmod 7 \end{aligned}$$

Αφού

$$89 = 64 + 16 + 8 + 1 = 2^6 + 2^4 + 2^3 + 1,$$

εν συνεχεία,

$$3^{89} = 3^{64} \times 3^{16} \times 3^8 \times 3 = 4 \times 4 \times 2 \times 3 \equiv 5 \pmod 7.$$

Επομένως το υπόλοιπο (mod 7) είναι 5.

Στην πραγματικότητα αυτό που κάναμε για να βρούμε το υπόλοιπο ήταν να γράψουμε τον εκθέτη

$$89 = 2^6 + 2^4 + 2^3 + 1 = (1, 0, 1, 1, 0, 0, 1)_2$$

σε δυαδικό αριθμητικό σύστημα. Με συνεχείς τετραγωνισμούς βρίσκουμε τα υπόλοιπα (mod 7) των διαφόρων δυαδικών δυνάμεων

$$1,\ 2,\ 4,\ 8,\ 16,\ 32,\ 64.$$

Μια αντίστοιχη μέθοδος μπορεί πάντα να χρησιμοποιηθεί. Αλλά ειδικές περιπτώσεις μπορούμε συχνά να τις χειριστούμε με «πονηρές» παρατηρήσεις. Παραδείγματος χάρη, στην ανωτέρω περίπτωση παρατηρούμε ότι

$$3^8 \equiv -1 \pmod 7,$$
$$3^6 \equiv 1 \pmod 7,$$

οπότε καταλήγουμε ότι

$$3^{84} = (3^6)^{14} \equiv 1 \pmod 7.$$

Επομένως

$$3^{89} = 3^{84} \times 3^3 \times 3^2 = 1 \times (-1) \times 2 = -2 \equiv 5 \pmod 7$$

όπως πριν.

Ως άλλη απεικόνιση μπορούμε να λάβουμε υπόψη τους αριθμούς Fermat τους οποίους παρουσιάσαμε στο κεφάλαιο 2.3:

$$\Phi_\tau = 2^{2^\tau} + 1.$$

Τα πρώτα είναι

$$\Phi_0 = 3, \quad \Phi_1 = 5, \quad \Phi_2 = 17, \quad \Phi_3 = 257, \quad \Phi_4 = 65537.$$

Αυτό φαίνεται να υποδηλώνει ότι:

Οι δεκαδικοί αριθμοί για όλους τους αριθμούς Fermat εκτός των Φ_0 και Φ_1 τελειώνουν στο ψηφίο 7.

Ας αποδείξουμε με αναλογίες ότι αυτό ισχύει. Προφανώς είναι το ίδιο με το να πούμε πως οι αριθμοί 2^{2^τ}, $\tau = 2, 3, \ldots$ τελειώνουν στο ψηφίο 6.

Αυτό το αποδεικνύουμε μέσω της επαγωγής. Παρατηρούμε ότι

$$2^{2^2} = 16 \equiv 6 \pmod{10}$$
$$2^{2^3} = 256 \equiv 6 \pmod{10}$$
$$2^{2^4} = 65536 \equiv 6 \pmod{10}.$$

Επιπλέον, εάν τετραγωνίσουμε 2^{2^K} το αποτέλεσμα είναι

$$(2^{2^K})^2 = 2^{2 \times 2^K} = 2^{2^{K+1}}.$$

Ας υποθέσουμε ότι για κάθε τ

$$2^{2^T} \equiv 6 \pmod{10}$$

τετραγωνίζοντας αυτή την αναλογία βρίσκουμε

$$2^{2^{T+1}} = 36 \equiv 6 \pmod{10}$$

όπως επιθυμούσαμε.

6.5 Η ΑΝΑΛΟΓΙΑ FERMAT

Από την άλγεβρα θυμόμαστε τον διωνυμικό νόμο

$$\chi + \psi = \chi + \psi$$

$$(\chi + \psi)^2 = \chi^2 + 2\chi\psi + \psi^2$$

(6.5.1.) $$(\chi + \psi)^3 = \chi^3 + 3\chi^2\psi + 3\chi\psi^2 + \psi^3$$

$$(\chi + \psi)^4 = \chi^4 + 4\chi^3\psi + 6\chi^2\psi^2 + 4\chi\psi^3 + \psi^4,$$

και γενικώς

(6.5.2.) $$(\chi + \psi)^\pi = \chi^\pi + \binom{p}{1}\chi^{\pi-1}\psi + \binom{p}{2}\chi^{\pi-2}\psi^2 + \ldots + \psi^\pi.$$

Εδώ ο πρώτος και ο τελευταίος συντελεστής είναι μονάδες. Οι μεσαίοι διωνυμικοί συντελεστές είναι

$$\binom{p}{1} = \frac{p}{1}, \qquad \binom{p}{2} = \frac{p(p-1)}{1\times 2},$$

(6.5.3.) $$\binom{p}{3} = \frac{p(p-1)(p-2)}{1\times 2\times 3}, \qquad \ldots,$$

και γενικότερα

(6.5.4.) $$\binom{p}{r} = \frac{p(p-1)(p-2)\ldots(p-k+1)}{1\times 2\ldots\times r},$$

όπου $\rho = 1, 2, \ldots, \rho - 1.$

Αφού αυτοί οι συντελεστές αποκτώνται με τους συνεχείς πολλαπλασιασμούς με $\chi + \psi$ όπως υποδεικνύεται στο (6.5.1.), είναι προφανές πως είναι ακέραιοι.

Ας υποθέσουμε από εδώ και στο εξής πως ο π είναι πρώτος. Για να γράψουμε τους ακεραίους (6.5.4.) σε ακέραια μορφή πρέπει να απαλείψουμε όλους τους κοινούς παράγοντες του παρονομαστή

$$1 \times 2 \ldots \times \rho$$

και του αριθμητή

$$\pi(\pi - 1) \ldots (\pi - \rho + 1).$$

Όμως ο παρονομαστής δεν συμπεριλαμβάνει τον πρώτο παράγοντα π, όποτε μετά την απαλοιφή, ο π υπάρχει ακόμη στον αριθμητή. Έτσι καταλήγουμε:

Όλοι οι διωνυμικοί συντελεστές (εκτός του πρώτου και του τελευταίου) στο (6.5.2.) διαιρούνται με π αν το π είναι πρώτος.

Τώρα, έστω οι χ και ψ στο (6.5.2.) να είναι ακέραιοι. Εάν γράψουμε το (6.5.2.) ως αναλογία (mod π), καταλήγουμε ότι:

Για ακεραίους χ και ψ και για κάθε πρώτο π,

(6.5.5.) $$(\chi + \psi)^{\pi} = \chi^{\pi} + \psi^{\pi} \pmod{\pi}.$$

Ας πάρουμε σαν παράδειγμα το $\pi = 5$, ώστε

$$(\chi + \psi)^5 = \chi^5 + 5\chi^4\psi + 10\chi^3\psi^2 + 10\chi^2\psi^3 + 5\chi\psi^4 + \psi^5.$$

Αφού όλοι οι μεσαίοι συντελεστές διαιρούνται με 5, βρίσκουμε

$$(\chi + \psi)^5 \equiv \chi^5 + \psi^5 \pmod{5}$$

όπως στο (6.5.5.).

Μπορούμε να εξάγουμε σημαντικά συμπεράσματα από την αναλογία (6.5.5.). Ας το εφαρμόσουμε πρώτα στην περίπτωση $\chi = \psi = 1$. Αυτό μας δίνει

$$2^{\pi} = (1 + 1)^{\pi} = 1^{\pi} + 1^{\pi} \equiv 2 \pmod{\pi}.$$

Έπειτα παίρνουμε $\chi = 2$, $\psi = 1$ και βρίσκουμε

$$3^{\pi} = (2 + 1)^{\pi} = 2^{\pi} + 1^{\pi}$$

μετά χρησιμοποιούμε το προηγούμενο αποτέλεσμα $2^{\pi} \equiv 2 \pmod{\pi}$ και έχουμε

$$2^{\pi} + 1^{\pi} = 2 + 1 \equiv 3 \pmod{\pi}, \quad \text{άρα } 3^{\pi} \equiv 3 \pmod{\pi}.$$

Ύστερα, για $\chi = 3$, $\psi = 1$, παίρνουμε

$$4^{\pi} = 4 \pmod{\pi}.$$

Χρησιμοποιώντας αυτή τη μέθοδο, μπορούμε να αποδείξουμε με επαγωγή πως $\alpha^{\pi} \equiv \alpha \pmod{\pi}$ για κάθε τιμή

(6.5.6.) $$\alpha = 0, 1, \ldots, \pi - 1.$$

οι ειδικές περιπτώσεις $\alpha = 0$ και $\alpha = 1$ είναι αυταπόδεικτες. Αφού κάθε αριθμός είναι ανάλογος (mod π) προς ένα από τα υπόλοιπα στο (6.5.6.) καταλήγουμε ότι

Για κάθε ακέραιο α και κάθε πρώτο π ,

(6.5.7.) $$\alpha^{\pi} \equiv \alpha \pmod{\pi}.$$

Αυτός ο νόμος των αναλογιών ονομάζεται κοινώς και θεώρημα του Fermat, ωστόσο κάποιοι συγγραφείς το ονομάζουν *μικρό* θεώρημα του Fermat για να το ξεχωρίζουν από το τελευταίο θεώρημα του Fermat ή εικασία του Fermat την οποία αναφέραμε στο κεφάλαιο 5.3.

Παράδειγμα. Για $\pi = 13$ και $\alpha = 2$ βρίσκουμε $13 = 8 + 4 + 1$, άρα

$$2^{13} = 2^{8+4+1} = 2^8 \times 2^4 \times 2^1.$$

Οπότε αφού

$$2^4 = 16 \equiv 3 \pmod{13}, \qquad 2^8 \equiv 9 \pmod{13},$$

παίρνουμε

$$2^{13} = 2^8 \times 2^4 \times 2^1 = 9 \times 3 \times 2 \equiv 2 \pmod{13}$$

όπως ορίζεται από την αναλογία του Fermat.

Σύμφωνα με τον νόμο της απαλοιφής που αναφέραμε στο τέλος του κεφαλαίου 6.3, μπορούμε να απαλείψουμε τον κοινό παράγοντα α και στις δυο πλευρές της αναλογίας Fermat (6.5.7.), αρκεί το α να είναι σχετικά πρώτος με το modulus π. Αυτό μας δίνει το αποτέλεσμα:

Αν α ακέραιος μη διαιρέσιμος από πρώτο π, τότε

(6.5.8.) $$\alpha^{\pi-1} \equiv 1 \pmod{\pi}.$$

Αυτό το αποτέλεσμα είναι επίσης γνωστό και ως *θεώρημα Fermat*.

ΕΦΑΡΜΟΓΕΣ ΑΝΑΛΟΓΙΩΝ

7.1 ΕΛΕΓΧΟΙ ΥΠΟΛΟΓΙΣΜΩΝ

Όπως έχουμε αναφέρει, ο δημιουργός της θεωρίας των αναλογιών ήταν ο Γερμανός μαθηματικός *Carl Friedrich Gauss*. Η διάσημη εργασία του πάνω στη θεωρία των αριθμών, *Disquisitiones Arithmeticae*, εμφανίστηκε το 1801 όταν ήταν σε ηλικία 24 ετών.

Ας μην παραλείψουμε να αναφέρουμε εδώ ότι υπάρχουν ίχνη της θεωρίας των αναλογιών αρκετούς αιώνες πριν από τον Gauss. Κάποια από αυτά εμφανίστηκαν σε αρχαίους κανόνες ελέγχου για αριθμητικούς υπολογισμούς. Αποτέλεσαν αναπόσπαστο μέρος της διδασκαλίας της αριθμητικής στην περίοδο της Αναγέννησης. Μερικά από αυτά χρησιμοποιούνται ακόμα, και από όσα γνωρίζουμε για την καταγωγή τους θα μπορούσαν να έχουν τις ρίζες τους στην αρχαιότητα.

Δεν ξέρουμε πως αρχικά εισήχθησαν, αλλά ας δείξουμε έναν εύλογο τρόπο με τον οποίον μάλλον ανακαλύφθηκαν. Θα προχωρήσουμε πίσω στο χρόνο των υπολογιστικών πινάκων. Σε έναν τέτοιον άβακα κάθε ψηφίο του αριθμού που απαιτείται για τους υπολογισμούς θα ορίζεται μέσω μετρητών ή πετρών ή ράβδων ή ξηρών καρπών, όπου και κάθε ομάδα θα ορίζει των αριθμό των μονάδων, δεκάδων, εκατοντάδων και λοιπά, ανάλογα με την θέση του. Ένας αριθμός στο δεκαδικό μας σύστημα:

$$(7.1.1.) \quad N = \alpha_v \times 10^v + \alpha_{v-1} \times 10^{v-1} + \ldots + \alpha_2 \times 10^2 + \alpha_1 \times 10^1 + \alpha_0$$

$$= (\alpha_v,\ \alpha_{v-1},\ \ldots\ ,\ \alpha_2,\ \alpha_1,\ \alpha_0)_{10}$$

θα απαιτούσε ένα σύνολο

(7.1.2.) $$\Sigma_N = \alpha_v + \alpha_{v-1} + \ldots + \alpha_2 + \alpha_1 + \alpha_0$$

μετρητών. Αυτό τον αριθμό τον ονομάζουμε άθροισμα ψηφίων του N.

Ας υποθέσουμε τώρα ότι θέλουμε να εκτελέσουμε μια απλή πράξη στον πίνακα, όπως: να προσθέσουμε δύο αριθμούς N και M. Όπου ο δεύτερος αριθμός:

$$M = (\beta_\mu, \beta_{\mu-1}, \ldots, \beta_2, \beta_1, \beta_0)_{10}$$

Έτσι έχουμε επιπλέον μετρητές στις ίδιες γραμμές:

$$\Sigma_M = \beta_\mu + \beta_{\mu-1} + \ldots + \beta_2 + \beta_1 + \beta_0$$

Σε μερικές γραμμές ίσως να υπάρχουν πλέον περισσότεροι από 9 μετρητές. Η λειτουργία που απαιτείται για να βρούμε το N + M συνίσταται στην αντικατάσταση δέκα μονάδων μιας γραμμής από έναν μετρητή της επόμενης γραμμής, και συνεχίζεται μέχρι να μην μπορούν να γίνουν περαιτέρω μειώσεις. Σε κάθε βήμα μία μονάδα αντικαθιστά δέκα μετρητές, οπότε είναι φανερή η απώλεια των άλλων εννέα μετρητών. Έτσι βλέπουμε ότι εάν η πρόσθεση γίνει σωστά, ο αριθμός των μετρητών που παραμένουν πρέπει να πληρούν:

(7.1.3) $$\Sigma_{N+M} \equiv \Sigma_N + \Sigma_M \pmod 9$$

όπου, ο αριθμός των μετρητών που υπάρχουν ακόμη στον πίνακα πρέπει να διαφέρουν από το αρχικό σύνολο κατά ένα πολλαπλάσιο του 9. Ο έλεγχος αυτός (7.1.3.) είναι ακόμη γνωστός με το παλιό του όνομα: *casting out nines* (απαλοιφή των εννιαριών).

Αφού ανακαλύφθηκε αυτός ο κανόνας, δεν πέρασε πολύς καιρός ώστε να παρατηρήσουμε ότι αυτό ισχύει και σε αρκετές προσθαφαιρέσεις, σε διαφορές και σε γινόμενα.

Στην τελευταία υπόθεση έχουμε:

(7.1.4.) $\Sigma_N \times \Sigma_M \equiv \Sigma_{MN} \pmod 9$.

Για να αποδείξουμε αυτούς τους κανόνες θεωρητικά, είναι εύκολο όταν χρησιμοποιούμε τις αναλογίες. Είναι προφανές ότι:

(7.1.5.) $1 \equiv 1,\ 10 \equiv 1,\ 10^2 \equiv 1,\ 10^3 \equiv 1,\ \ldots \pmod 9$,

έτσι από (8.1.1.) και (8.1.2.) καταλήγουμε πως:

(7.1.6.) $N \equiv \Sigma_N \pmod 9$.

Ως εκ τούτου, από τους κανόνες των αναλογιών που αποδείξαμε στο κεφάλαιο 6.3, είναι φανερό ότι:

$$\Sigma_N \pm \Sigma_M \equiv N \pm M \equiv \Sigma_{N \pm M},\quad \Sigma_N \times \Sigma_M \equiv N \times M \equiv \Sigma_{N \times M} \pmod 9.$$

Το *casting out of nines* χρησιμοποιείται ως επί το πλείστον στους πολλαπλασιασμούς.
Ας πάρουμε για παράδειγμα τους αριθμούς:

(7.1.7.) $M = 3119,\quad N = 3724$

και το γινόμενο τους

$$M \times N = 116141156$$

Αυτός ο υπολογισμός δεν μπορεί να είναι σωστός γιατί:

$$M \equiv \Sigma_M \equiv 3 + 1 + 1 + 9 \equiv 5 \pmod 9,$$

$$N \equiv \Sigma_N \equiv 3 + 7 + 2 + 4 \equiv 7 \pmod 9,$$

και

$$MN \equiv \Sigma_{MN} \equiv 1 + 1 + 6 + 1 + 4 + 1 + 5 + 6 \equiv 7 \pmod 9.$$

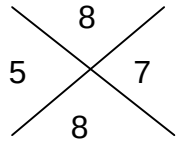
Αλλά

$$5 \times 7 = 35 \equiv 8 \neq 7 \pmod 9.$$

Στη πραγματικότητα το αποτέλεσμα έπρεπε να είναι:

$$M \times N = 11615156.$$

Στα μεσαιωνικά σχολεία, οι μαθητές είχαν αυστηρή οδηγία να συμπεριλαμβάνουν τον έλεγχο στις ασκήσεις τους, δηλαδή να κάνουν επαλήθευση. Έτσι στα χειρόγραφα εκείνης της εποχής βρίσκει κανείς ένα πρόσθετο μέρος με cross-bones που στο παράδειγμά μας (7.1.7.) θα φαίνεται έτσι:



Εικόνα 7.1.1.

Εδώ οι αριθμοί 5 και 7 στα πλάγια κενά εκπροσωπούν τα υπόλοιπα των M και N (mod 9) και ο αριθμός 8 που βρίσκεται στην πάνω πλευρά είναι το υπόλοιπο του αποτελέσματος $M \times N$. Αυτό πρέπει να επαληθεύεται με το γινόμενο των υπολοίπων στην κάτω πλευρά, όπου:

$$5 \times 7 = 35 \equiv 8 \pmod 9.$$

Αυτές οι επαληθεύσεις cross-bone εμφανίζονται αρκετά συχνά σε πρώιμα τυπωμένα αριθμητικά κείμενα, όπως, για παράδειγμα, σε Αγγλικά κείμενα του 17ου και 18ου αιώνα. Είναι, φυσικά, πιθανό ένας υπολογισμός να

περιέχει ένα λάθος το οποίο να μην διακρίνεται με τη μέθοδο *casting out nines*. Αλλά έτσι θα ξέρουμε ότι το λάθος θα είναι «σφάλμα modulo 9».

Είναι προφανές πως με άλλες βάσεις παρόμοιες επαληθεύσεις θα μπορούσαν να χρησιμοποιηθούν. Για έναν αριθμό

$$M = \mu_v \beta^v + \mu_{v-1} \beta^{v-1} + \ \dots \ + \mu_2 \beta^2 + \mu_1 \beta + \mu_0$$

με βάση β έχουμε, όπως στο (7.1.5.),

$$1 \equiv 1, \quad \beta \equiv 1, \quad \beta^2 \equiv 1, \quad \dots \pmod{\beta - 1}$$

έτσι, όπως και πριν,

$$M \equiv \Sigma_M = \mu_v + \mu_{v-1} + \ \dots \ + \mu_2 + \mu_1 + \mu_0 \pmod{\beta - 1},$$

και οι επαληθευτικοί κανόνες είναι ίδιοι.

Αυτή η φαινομενικά τετριμμένη παρατήρηση έχει εφαρμογές ακόμη και στο συνηθισμένο μας δεκαδικό σύστημα. Αναφέραμε και στο κεφάλαιο 6.5 πως αν διαιρέσουμε τα ψηφία ενός δεκαδικού αριθμού σε ομάδες των τριών, τότε αυτή η ομαδοποίηση μπορεί να γίνει κατανοητή ως επέκταση του αριθμού

$$\beta = 10^3 = 1000.$$

Παρομοίως, αν ομαδοποιήσουμε τα ψηφία σε ζεύγη, αυτό αντιστοιχεί σε επέκταση με βάση

$$\beta = 10^2 = 100.$$

Παίρνοντας τους αριθμούς 3119 και 3724 ως παράδειγμα πάλι, και γράφοντας

$$M = 31\ 19, \qquad N = 37\ 24$$

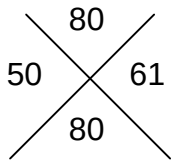
$$M \times N = 11\ \ 61\ \ 51\ \ 56,$$

βρίσκουμε

$$M \equiv 31 + 19 \equiv 50 \pmod{99}, \qquad N \equiv 37 + 24 \equiv 61 \pmod{99},$$

$$M \times N = 11 + 61 + 51 + 56 = 179 \equiv 80 \pmod{99}.$$

Εδώ η επαλήθευση cross-bone είναι



διότι, όπως βλέπουμε,

$$50 \times 61 \equiv 80 \pmod{99}.$$

Αυτή η επαλήθευση είναι πιο αποτελεσματική από την μέθοδο *casting out nines* γιατί το modulus είναι μεγαλύτερο, και έτσι η πιθανότητα η απάντηση να είναι σωστή είναι αντίστοιχα μεγαλύτερη. Με άλλα λόγια, ένα «σφάλμα modulo 99» είναι λιγότερο πιθανό από ότι ένα «σφάλμα modulo 9».

7.2 ΠΡΟΓΡΑΜΜΑ ΤΟΥΡΝΟΥΑ

Ας χρησιμοποιήσουμε τώρα την θεωρία αναλογιών για να δούμε την εφαρμογή της στην κατάρτιση του προγράμματος των τουρνουά. Τα προγράμματα αυτά χρησιμοποιούνται σε όλα τα αθλήματα, από το σκάκι μέχρι το ποδόσφαιρο.

Ας υποθέσουμε τώρα πως υπάρχουν N συμμετέχοντες ή ομάδες. Όταν το N είναι περιττός αριθμός, δεν μπορούμε να βάλουμε σε ζευγάρια όλες τις ομάδες σε κάθε γύρο, πάντα θα υπάρχει μια ομάδα που δεν θα έχει αντίπαλο. Μπορούμε όμως να εξαλείψουμε αυτή την δυσκολία με την πρόσθεση μιας φανταστικής ομάδας T_0 και να δημιουργήσουμε ένα πρόγραμμα για $N + 1$ ομάδες, συμπεριλαμβάνοντας την T_0. Σε κάθε γύρο η ομάδα η οποία θα πρόκειται να παίξει με την T_0 θα παίρνει 'ρεπό' σε αυτόν τον γύρο.

Μπορούμε, επομένως, να υποθέσουμε πως έχουμε άρτιο αριθμό ομάδων N. Δίνουμε τώρα στην κάθε ομάδα έναν αριθμό

$$\chi = 1,\ 2,\ \ldots\ N-1,\ N.$$

Ο συνολικός αριθμός των γύρων που θα παίζει κάθε ομάδα είναι $N - 1$.

Ας υποθέσουμε τώρα πως η χ ανήκει στην σειρά

(7.2.1.) $$1,\ 2,\ \ldots\ N-1.$$

Ως αντίπαλο της χ στον ν-οστό γύρο τοποθετούμε την ομάδα ψ_v από την σειρά (7.2.1.), όπου ψ_v είναι ο αριθμός που καθορίζεται από την αναλογία

(7.2.2.) $$\chi + \psi_v \equiv v \pmod{N-1}.$$

Για να δούμε ότι τα διαφορετικά χ θα έχουν διαφορετικούς ψ αντιπάλους, σημειώνουμε ότι

$$\chi + \psi_v \equiv v \equiv \chi' + \psi_v \pmod{N-1}$$

που σημαίνει

$$\chi \equiv \chi' \pmod{N-1}$$

ή $\chi = \chi'$ αφού αυτοί οι αριθμοί ανήκουν στο (7.2.1.).

Η μονή επιπλοκή παρουσιάζεται στην περίπτωση που $\chi = \psi_v$, οπότε στο (7.2.2.) έχουμε

(7.2.3.) $$2\chi \equiv v \pmod{N-1}.$$

Υπάρχει μόνο ένα χ στο (7.2.1.) για το οποίο μπορεί να συμβεί αυτό, διότι αν

$$2\chi \equiv v \equiv 2\chi' \pmod{N-1},$$

συνάγεται ότι

$$2(\chi - \chi') \equiv 0 \pmod{N-1},$$

ή

$$\chi \equiv \chi' \pmod{N-1}$$

αφού το N – 1 είναι περιττός. Υπάρχει πάντα μια λύση στο (7.2.3.) από το (7.2.1.), δηλαδή

$\chi = \frac{n}{2}$ όταν ο v είναι άρτιος,

$\chi = \frac{n+N-1}{2}$ όταν ο v είναι περιττός.

Μέσω της σχέσης (7.2.2.) αναθέσαμε έναν αντίπαλο στον ν-οστό γύρο για κάθε χ στο (7.2.1.) με την εξαίρεση του χ_0 που ικανοποιεί το (7.2.3.). Αυτό το χ_0 το ταιριάζουμε με την Ν-οστή ομάδα.

Απομένει να δείξουμε ότι με αυτά τα ταιριάσματα κάθε ομάδα παίζει με διαφορετικό αντίπαλο σε κάθε γύρο $\nu = 1, \dots, N-1$. Το επαληθεύουμε πρώτα με την Ν-οστή ομάδα. Στον ν-οστό γύρο παίζει με την χ_0 η οποία καθορίστηκε από το (7.2.3.). Ας υποθέσουμε πως $\varphi \neq \nu$, οπότε στον φ-οστό γύρο Ν παίζει η ομάδα χ_0' η οποία ικανοποιεί το

$$2\chi_0' \equiv \varphi \pmod{N-1}.$$

Δεν μπορούμε να έχουμε $\chi_0 = \chi_0'$ διότι θα οδηγούσε στο

$$2\chi_0 = 2\chi_0' \equiv \nu \equiv \varphi \pmod{N-1},$$

άρα και $\varphi = \nu$.

Ας εξετάσουμε τους διάφορους αντιπάλους της ομάδας χ στο (7.2.1.). Θα παίξει με την Ν-οστή ομάδα μια φορά, δηλαδή, για το ν_0 που καθορίζεται από το

$$2\chi = \nu_0 \pmod{N-1}.$$

Ας υποθέσουμε τώρα ότι $\nu \neq \nu_0$ και $\varphi \neq \nu_0$. Έτσι οι αντίπαλοι της ομάδας χ στους ν-οστό και φ-οστό γύρους θα καθοριστούν από (7.2.2.):

$$\chi + \psi_\nu \equiv \nu \pmod{N-1} \quad \text{και} \quad \chi + \psi_0 \equiv \varphi \pmod{N-1}.$$

Ξανά, το $\psi_\nu = \psi_0$ θα οδηγούσε στο $\varphi = \nu$ όπως πριν, οπότε συμπεραίνουμε πως $\psi_\nu \neq \psi_0$.

Ας φτιάξουμε έναν πίνακα για N = 6 ομάδες μέσω της μεθόδου που μόλις εξηγήσαμε. Μερικοί απλοί υπολογισμοί δίνουν το αποτέλεσμα που φαίνεται παρακάτω. Η είσοδος στην ν-οστή σειρά, χ-οστή στήλη δίνει τον αντίπαλο της ομάδας χ στον ν-οστό γύρο.

χ	1	2	3	4	5	6
ν						
1	5	4	6	2	1	3
2	6	5	4	3	2	1
3	2	1	5	6	3	4
4	3	6	1	5	4	2
5	4	3	2	1	6	5

7.3 ΠΡΩΤΟΣ Ή ΣΥΝΘΕΤΟΣ;

Ως τελευταία εφαρμογή των αναλογιών θα παραθέσουμε μια μέθοδο εξέτασης εάν ένας αριθμός είναι πρώτος ή σύνθετος. Είναι μια πολύ αποτελεσματική μέθοδος, η καλύτερη γενική μέθοδος που έχουμε όταν πρέπει να διερευνήσουμε έναν συγκεκριμένο αριθμό τον οποίο διαλέξαμε τυχαία. Βασίζεται στην αναλογία του Fermat (6.5.8.).

Έστω N ο αριθμός τον οποίο θέλουμε να εξετάσουμε. Επιλέγουμε α ως κάποιο μικρό αριθμό σχετικά πρώτο με N. Συχνά είναι βολικό να παίρνουμε *α* ως μικρό πρώτο που δεν διαιρεί τον *N*, για παράδειγμα, α = 2 ή 3 ή 5. Αν ο *N* ήταν πρώτος θα υπάκουε στο

(7.3.1.) $$\alpha^{N-1} = 1 \pmod N$$

σύμφωνα με την αναλογία Fermat. Συνεπώς αν ελέγξουμε αυτή την αναλογία και βρούμε πως δεν ισχύει, θα ξέρουμε πως ο *N* είναι σύνθετος.

Παράδειγμα. Έστω N = 91, και ας επιλέξουμε α = 2. Τότε

$$\alpha^{N-1} = 2^{90} = 2^{64} \times 2^{16} \times 2^{8} \times 2^{2}.$$

Επιπλέον,

$$2^{8} = 256 \equiv -17 \pmod{91},$$

$$2^{16} = (2^{8})^{2} \equiv (-17)^{2} = 289 \equiv 16 \pmod{91},$$

$$2^{32} = (2^{16})^{2} \equiv (16)^{2} = 256 \equiv -17 \pmod{91},$$

$$2^{64} = (2^{32})^{2} \equiv (-17)^{2} = 289 \equiv 16 \pmod{91},$$

έτσι ώστε

$$2^{90} = 2^{64} \times 2^{16} \times 2^{8} \times 2^{2}$$

$$\equiv 16 \times 16 \times (-17) \times 4 \equiv 64 \neq 1 \pmod{91}.$$

Συμπεραίνουμε ότι ο *N* είναι σύνθετος. Συγκεκριμένα, $91 = 7 \times 13$.

Το παράδειγμα μας είναι πολύ απλό για να δείξει την πραγματική δύναμη της μεθόδου. Με τον κατάλληλο προγραμματισμό σε υπολογιστή είναι δυνατό να αποδείξουμε ότι συγκεκριμένοι μεγάλοι αριθμοί είναι σύνθετοι. Δυστυχώς, όμως, αυτή η μέθοδος δεν δίνει καμία ένδειξη στο ποιοι είναι οι παράγοντες. Έτσι, σε πολλές περιπτώσεις γνωρίζουμε ότι ένας αριθμός είναι πρώτος αλλά δεν γίνεται καμία νύξη στο ποιοι είναι οι παράγοντες του.

Αυτό εφαρμόζεται περισσότερο στους αριθμούς Fermat

$$\Phi_v = 2^{2^v} + 1$$

που αναφέραμε στο κεφάλαιο 2.3. Οι αριθμοί αυτοί είναι πρώτοι για $v = 0, 1, 2, 3, 4$, όπως παρατηρήσαμε. Για να εξετάσουμε τον αριθμό

$$\Phi_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297$$

με την αναλογία Fermat, μπορούμε να πάρουμε $\alpha = 3$. Αν το Φ_5 είναι πρώτος θα έπρεπε να είχαμε

(7.3.2.) $$3^{2^{32}} \equiv 1 \pmod{\Phi_5}.$$

Για να υπολογίσουμε το υπόλοιπο της δύναμης στο αριστερό μέρος πρέπει να τετραγωνίσουμε 32 φορές και σε κάθε βήμα να μειώνουμε το αποτέλεσμα (mod Φ_5). Δεν θα παρουσιάσουμε τις πράξεις τώρα. Αποδεικνύεται πάντως πως η αναλογία (7.3.2.) δεν ισχύει, οπότε, ο Φ_5 είναι σύνθετος. Ο γνωστός παράγοντας 641 έχει βρεθεί με δοκιμές. Η ίδια μέθοδος έχει χρησιμοποιηθεί για να δείξουμε ότι αρκετοί μεγαλύτεροι

αριθμοί δεν είναι πρώτοι. Για κάποιους εξ αυτών γνωρίζουμε παράγοντες, για κάποιους όχι.

Εάν η αναλογία (7.3.1.) ισχύει για κάποιο α σχετικά πρώτο με N, ο αριθμός N μπορεί να είναι ή να μην είναι πρώτος. Οι περιπτώσεις στις οποίες ισχύει για σύνθετο αριθμό N είναι εξαιρέσεις, οπότε συνήθως θα υποθέταμε πως ο N είναι πρώτος. Παρολαυτά, στις περισσότερες περιπτώσεις θέλουμε να γνωρίζουμε σίγουρα. Σε αυτή την περίπτωση μπορούμε να το επιτύχουμε βασιζόμενοι στην παρατήρηση ότι ο N είναι πρώτος στην περίπτωση που το (7.3.1.) ισχύει για εκθέτη $N - 1$ αλλά για κανέναν διαιρέτη του $N - 1$.

Υπάρχει και μια άλλη προσέγγιση, αποτελεσματική για αριθμούς N που δεν είναι πολύ μεγάλοι. Παίρνουμε $\alpha = 2$. Οι Poulet και Lehmer είχαν υπολογίσει όλες τις αξίες του $N \leq 100.000$ που εξαιρούνται, υπό την έννοια ότι

$$2^{N-1} \equiv 1 \pmod{N}, \tag{7.3.3.}$$

αλλά ο N είναι σύνθετος. Οι αριθμοί αυτοί συχνά ονομάζονται ψεύδοπρώτοι. Για κάθε έναν από αυτούς τους αριθμούς N έχουν δοθεί επίσης οι μεγαλύτεροι πρώτοι παράγοντες.

Μέσω των πινάκων των Poulet και Lehmer μπορούμε να καθορίσουμε αν είναι πρώτος οποιοσδήποτε αριθμός $N \leq 100.000.000$ κατ' αυτόν τον τρόπο: Ελέγχουμε πρώτα αν η αναλογία (7.3.3.) ισχύει.
Εάν δεν ισχύει, ο N είναι σύνθετος. Αν η αναλογία ισχύει και ο N είναι στους πίνακες, πάλι είναι σύνθετος, και μπορούμε να διαβάσουμε και έναν πρώτο παράγοντα από τους πίνακες. Τέλος, αν το (7.3.3.) ισχύει και ο N δεν είναι στους πίνακες, τότε είναι πρώτος.

Ο μικρότερος σύνθετος αριθμός N που ικανοποιεί το (7.3.3.) είναι ο

$$N = 341 = 11 \times 31.$$

Κάτω από το 1000 υπάρχουν άλλοι δυο, οι

$$N = 561 = 3 \times 11 \times 17,$$

$$N = 645 = 3 \times 5 \times 43.$$

Ο αριθμός 541 είναι αξιοσημείωτος, διότι εδώ η αναλογία (7.3.1.) ισχύει για κάθε ακέραιο *α* σχετικά πρώτο με τον *N*. Τέτοιοι ιδιόμορφοι αριθμοί, λέμε πως έχουν την ιδιότητα Fermat. Έχει γίνει πολλή έρευνα πάνω σε αυτούς τους αριθμούς. Μπορείτε να «κατεβάσετε» ηλεκτρονικά τον πίνακα των ψευδοπρώτων < 1015 από την ηλεκτρονική διεύθυνση http://www.cecm.sfu.ca/Pseudoprimes/ .

ΕΠΙΛΟΓΟΣ

Η βιβλιογραφία που αφορά την θεωρία αριθμών κατά κύριο λόγο απευθύνεται σε επιστήμονες του συγκεκριμένου κλάδου και δεν υπάρχουν πολλά βιβλία τα οποία να μπορούν να μελετηθούν από το ευρύ κοινό. Οι πηγές για την εξεύρεση των απαραίτητων για την εργασία στοιχείων δεν ήταν πολλές.

Στηριχθήκαμε κυρίως σε συγκεκριμένα συγγράμματα ξένων συγγραφέων τα οποία επιλέχθηκαν ώστε να είναι πιο κατανοητή, ενδιαφέρουσα και «εύπεπτη» η ανάγνωση.
Το βάρος που δίδεται στους μαθηματικούς όρους σε τέτοιου είδους βιβλία είναι προφανώς μεγάλο. Παρόλα αυτά καταβλήθηκε μεγάλη προσπάθεια για να γίνει η εργασία αυτή εύκολα αναγνώσιμη και από ένα μη εξειδικευμένο κοινό.

Το φάσμα των πηγών ήταν αρκετά περιορισμένο και βασίστηκε κυρίως σε μερικά συγγράμματα και σε άρθρα και εργασίες - ερασιτεχνών και μη - μαθηματικών τα οποία δημοσιεύθηκαν στο Διαδίκτυο.

Η ενασχόληση με την εργασία αυτή δεν ήταν εύκολη, λόγω της μη εξοικείωσης των γραφόντων με τα Μαθηματικά και κατά συνέπεια με την θεωρία αριθμών. Τελικά όμως, υπήρξε μια ευχάριστη και δημιουργική διαδρομή στον διαρκώς εξελισσόμενο κόσμο των Μαθηματικών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Α. ΒΙΒΛΙΑ

- Oystein Ore, 1967, Invitation to number theory, Εκδόσεις Random House, Inc., Νέα Υόρκη.

- Τσαγκάρης Π. Γ., 2η έκδοση 2005, Θεωρία αριθμών, Εκδόσεις Συμμετρία, Αθήνα.

- Oystein Ore, 1948, Number theory and its history, Εκδόσεις McGraw-Hill Book Company Inc, Νέα Υόρκη.

Β. ΠΑΓΚΟΣΜΙΟΣ ΙΣΤΟΣ

- http://www.math.niu.edu/~rusin/known-math/index/11-XX.html

- http://www.numbertheory.org/ntw/number_theory.html

- http://primes.utm.edu/mersenne/

- http://www.mersenne.org/report_milestones/

- http://en.wikipedia.org/wiki/Fermat%27s_Last_Theorem

- http://danaos.cslab.ntua.gr/~ekall/Science/Other_docs/fermat_last_theorem.htm

- http://www.uh.edu/engines/epi833.htm

- http://www.hbmeyer.de/eratosiv.htm

- http://www.math.uoc.gr/~jplatis/pythagoras.pdf

- http://www-sop.inria.fr/members/Angelos.Mantzaflaris/down/FLT.pdf