ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΥΠΟΛΟΓΙΣΤΙΚΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ ΜΕ ΕΦΑΡΜΟΓΕΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΜΙΧΑΗΛ Θ. ΡΑΣΣΙΑΣ

Τριμελής Επιτροπή:
Βασίλης Παπανικολάου, Καθηγητής ΣΕΜΦΕ, ΕΜΠ
Αλέξανδρος Παπαϊωάννου, Αν. Καθηγητής ΣΕΜΦΕ, ΕΜΠ (Επιβλέπων)
Κωνσταντίνος Παπαοδυσσεύς, Αν. Καθηγητής ΣΗΜΜΥ, ΕΜΠ

Αθήνα, Νοέμβριος 2009

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΥΠΟΛΟΓΙΣΤΙΚΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ ΜΕ ΕΦΑΡΜΟΓΕΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΜΙΧΑΗΛ Θ. ΡΑΣΣΙΑΣ

Τριμελής Επιτροπή:
Βασίλης Παπανικολάου, Καθηγητής ΣΕΜΦΕ, ΕΜΠ
Αλέξανδρος Παπαϊωάννου, Αν. Καθηγητής ΣΕΜΦΕ, ΕΜΠ (Επιβλέπων)
Κωνσταντίνος Παπαοδυσσεύς, Αν. Καθηγητής ΣΗΜΜΥ, ΕΜΠ

Αθήνα, Νοέμβριος 2009

.....

Μιχαήλ Θ. Ρασσιάς

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

ΠΡΟΛΟΓΟΣ

Ο σκοπός αυτής της διπλωματικής εργασίας είναι μια συνοπτική παρουσίαση της Στοιχειώδους και Αναλυτικής Θεωρίας Αριθμών με εφαρμογές στην Κρυπτογραφία.

Ειδικότερα, στην Θεωρία Αριθμών, έμφαση δίνεται: στο Θεμελιώδες θεώρημα της Αριθμητικής, στις βασικότερες αριθμητικές συναρτήσεις (συνάρτηση Möbius μ(n), συνάρτηση Euler φ(n), συνάρτηση σ(n) και συνάρτηση τ(n)), σε ιδιότητές τους καθώς και σε θεωρήματα τα οποία σχετίζονται με αυτές, στους τέλειους αριθμούς, στους αριθμούς Fermat, στις ισοτιμίες, στα τετραγωνικά υπόλοιπα (όπου παρουσιάζουμε βασικά θεωρήματα με κυριότερο αυτό της τετραγωνικής αντιστροφής του Gauss), στις συναρτήσεις π(x), li(x) και στη συνάρτηση ζ(s) του Riemann. Τέλος, παρουσιάζονται παραδείγματα και εφαρμογές της θεωρίας στην επίλυση προβλημάτων.

Ακολούθως, στην Κρυπτογραφία, παρουσιάζουμε: θεμελιώδεις μεθόδους και βασικούς αλγορίθμους που αφορούν την Πιστοποίηση Πρώτων Αριθμών (όπως τους αλγορίθμους Fermat, Miller-Rabin και Solovay–Strassen), την Παραγοντοποίηση Ακεραίων σε Πρώτους Παράγοντες (όπως τον αλγόριθμο p – 1 του Pollard) και το πρόβλημα του Διακριτού Λογαρίθμου (όπως την μέθοδο ανταλλαγής κλειδιού Diffie–Hellman, τους αλγορίθμους Shanks, Pohlig–Hellman, Index Calculus και τις μεθόδους ρ και λ του Pollard).

ABSTRACT

In this diploma thesis entitled “Computational Number Theory with Applications”, we provide an introduction to Elementary and Analytic Number Theory along with applications to Cryptography.

More specifically, in Number Theory, we give emphasis to: the fundamental theorem of Arithmetic, the basic arithmetic functions (the Möbius function $\mu(n)$, the Euler function $\varphi(n)$, the function $\sigma(n)$ and the function $\tau(n)$) and characteristic properties along with theorems which are related to these, perfect numbers, Fermat numbers, congruences, quadratic residues, where we present some fundamental theorems proving Gauss’ Quadratic Reciprocity Law, the functions $\pi(x)$, $\mathrm{li}(x)$ and the Riemann $\zeta(s)$ function with some of their characteristic properties along with relevant open problems. Finally, we give examples and applications of the theory in the solution of some problems.

Furthermore, in Cryptography, we present: fundamental methods and basic algorithms concerning Primality Testing (the Fermat, Miller–Rabin and Solovay–Strassen algorithms), factorization of integers (the $p-1$ Pollard algorithm) and the Discrete Logarithm Problem (the Diffie–Hellman key exchange method, the Shanks, Pohlig–Hellman, Index Calculus algorithms and the ρ, λ Pollard methods).

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή της διπλωματικής αυτής εργασίας, Αναπ. Καθηγητή κ. Αλέξανδρο Παπαϊωάννου για το μεγάλο ενδιαφέρον του, την ενθάρρυνση και την ουσιώδη βοήθεια και καθοδήγηση που μου προσέφερε κατά την διάρκεια των φοιτητικών μου σπουδών στο ΕΜΠ.

Επίσης, θα ήθελα να εκφράσω τις ευχαριστίες μου στον Αναπ. Καθηγητή κ. Ιωάννη Σαραντόπουλο για τις πολύτιμες παρατηρήσεις του κατά την διάρκεια της συγγραφής της εργασίας αυτής καθώς και για το πολύ χρήσιμο μάθημά του που παρακολούθησα στην Μιγαδική Ανάλυση.

Ευχαριστώ ακόμα τον Επικ. Καθηγητή κ. Γεώργιο Φικιώρη, που οι συζητήσεις μας στα Μαθηματικά αποτέλεσαν έρεισμα για βαθύτερη μελέτη.

Ιδιαίτερες ευχαριστίες εκφράζω στον Καθηγητή κ. Βασίλη Παπανικολάου και τον Αναπ. Καθηγητή κ. Κωνσταντίνο Παπαοδυσσέα για τις σημαντικές επιστημονικές συμβουλές και το αμέριστο ενδιαφέρον τους να μου μεταλαμπαδεύσουν πολύτιμη γνώση.

Μιχαήλ Θ. Ρασσιάς

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Η Θεωρία Αριθμών είναι ένας από τους αρχαιότερους και πιο ενεργούς κλάδους των καθαρών Μαθηματικών, ενώ τα τελευταία χρόνια βρίσκει σημαντική εφαρμογή στην Θεωρητική Πληροφορική. Ασχολείται κατά κύριο λόγο με τη μελέτη των ακέραιων και των ρητών αριθμών.

Αρχίζουμε με κάποιους βασικούς ορισμούς.

Ορισμός

Ονομάζουμε **πρώτο αριθμό** (prime number) κάθε θετικό ακέραιο μεγαλύτερο της μονάδας, ο οποίος δεν έχει άλλους διαιρέτες εκτός από τον εαυτό του και την μονάδα.

Έτσι, για παράδειγμα οι ακέραιοι 2, 3, 13, 17 είναι όλοι *πρώτοι αριθμοί*, ενώ οι ακέραιοι 4, 8, 12, 15, 18, 21 δεν είναι πρώτοι αριθμοί.

Ο αριθμός 1 δεν θεωρείται πρώτος αριθμός.

Ορισμός

Οι ακέραιοι οι οποίοι δεν είναι πρώτοι αριθμοί και είναι μεγαλύτεροι της μονάδας, ονομάζονται **σύνθετοι αριθμοί** (composite numbers).

Ορισμός

Δύο ακέραιοι αριθμοί a και b ονομάζονται **πρώτοι μεταξύ τους** (relatively prime) αν δεν υπάρχει φυσικός αριθμός c μεγαλύτερος της μονάδας, τέτοιος ώστε να διαιρεί ταυτόχρονα τους a και b.

Για παράδειγμα, οι ακέραιοι αριθμοί 12 και 17 είναι πρώτοι μεταξύ τους.

Οι πρώτοι αριθμοί αποτελούν τους θεμελιώδεις λίθους κατασκευής όλων των ακεραίων. Κάθε θετικός ακέραιος γράφεται σαν γινόμενο δυνάμεων πρώτων παραγόντων, όπως θα δούμε στην απόδειξη του *θεμελιώδους θεωρήματος της Αριθμητικής*.

Ο Ευκλείδης, αξιοποιώντας το θεώρημα αυτό, απέδειξε ότι οι πρώτοι αριθμοί είναι άπειροι στο πλήθος.

Θα ξεκινήσουμε παρουσιάζοντας την απόδειξη της απειρίας του πλήθους των πρώτων αριθμών. Η απόδειξη οφείλεται στον Ευκλείδη και είναι μια από τις πιο στοιχειώδεις αποδείξεις του θεωρήματος αυτού.

Θεώρημα
Οι πρώτοι αριθμοί είναι άπειροι στο πλήθος.

ΑΠΟΔΕΙΞΗ

Ας υποθέσουμε πως το πλήθος των πρώτων αριθμών είναι πεπερασμένο και ότι ο p είναι ο μεγαλύτερος πρώτος αριθμός.

Θεωρούμε τον αριθμό

$$Q = p!+1 \ .$$

Τότε, αν ο Q ήταν πρώτος αριθμός θα ήταν μεγαλύτερος του p. Αυτό, όμως, είναι αδύνατον λόγω της ιδιότητας του p. Αν ο Q δεν είναι πρώτος αριθμός τότε προφανώς θα έχει πρώτους διαιρέτες. Αλλά, κάθε πρώτος αριθμός μικρότερος του p δεν μπορεί να διαιρεί τον Q, διότι θα

αφήνει πάντα υπόλοιπο 1. Επομένως οι πρώτοι διαιρέτες του Q είναι όλοι μεγαλύτεροι του p. Άτοπο.

Συνεπώς, η υπόθεση ότι οι πρώτοι αριθμοί είναι πεπερασμένοι στο πλήθος καταλήγει σε άτοπο. Άρα, οι πρώτοι αριθμοί είναι άπειροι.

■

ΠΑΡΑΔΕΙΓΜΑ

Οι πρώτοι αριθμοί της μορφής $4n+3$, όπου $n \in \mathbb{N}$, είναι άπειροι στο πλήθος.

ΑΠΟΔΕΙΞΗ

Θα εφαρμόσουμε παρόμοια αποδεικτική διαδικασία με αυτή για το θεώρημα του Ευκλείδη για την απειρία των πρώτων αριθμών. Έστω ότι οι πρώτοι αριθμοί της μορφής $4n+3$ είναι πεπερασμένοι στο πλήθος, και ο p είναι ο τελευταίος και μεγαλύτερος από τους αριθμούς αυτούς.

Θεωρούμε τον ακέραιο αριθμό q, όπου

$$q = 2^2 \cdot 3 \cdot 5 \cdots p - 1$$

Ο αριθμός q είναι της μορφής $4n+3$, $n \in \mathbb{N}$, διότι:

$$q = 2^2 \cdot 3 \cdot 5 \ldots p - 1 = 4\kappa - 1, \text{ όπου } \kappa = 3 \cdot 5 \cdots p \in \mathbb{Z}.$$

Άρα

$$q = 4\kappa + 3 - 4 = 4(\kappa - 1) + 3, \quad \kappa \in \mathbb{N}.$$

Ο αριθμός q είναι πρώτος ή μπορεί να αναπαρασταθεί ως γινόμενο δυνάμεων πρώτων αριθμών.

- Αν ο αριθμός q είναι πρώτος, τότε έχουμε έναν πρώτο της μορφής $4n+3$ ο οποίος είναι μεγαλύτερος του p. Άτοπο (το γεγονός ότι $q > p$ αποδεικνύεται εύκολα με Μαθηματική επαγωγή).

Συνεπώς, οι πρώτοι αριθμοί της μορφής $4n+3$ είναι άπειροι στο πλήθος.

- Αν ο αριθμός q δεν είναι πρώτος, τότε αναπαρίσταται ως γινόμενο δυνάμεων πρώτων παραγόντων. Οι πρώτοι αυτοί παράγοντες μπορούν να λάβουν την μορφή $4n+1$ ή $4n+3$ (αφού οι $4n, 4n+2$ δεν είναι πρώτοι).

Όμως, δεν μπορούν όλοι οι πρώτοι παράγοντες να λάβουν την μορφή $4n+1$, διότι τότε ο q θα έπρεπε να λαμβάνει την μορφή $4n+1$. Αυτό συμβαίνει, διότι το γινόμενο δύο αριθμών της μορφής $4n+1$ δίνει επίσης αριθμό της μορφής $4n+1$.

Επομένως, ένας τουλάχιστον από τους πρώτους παράγοντες του ακεραίου αριθμού q θα είναι της μορφής $4n+3$.

Όμως, κανένας από τους πρώτους αριθμούς μέχρι τον p δεν διαιρεί τον q. Έτσι, ο οποιοσδήποτε πρώτος παράγοντας του q ο οποίος έχει την μορφή $4n+3$ θα είναι μεγαλύτερος από τον p. Άτοπο.

Συνεπώς, και σ' αυτήν την περίπτωση αποδεικνύεται πως οι πρώτοι αριθμοί της μορφής $4n+3$ είναι άπειροι στο πλήθος.

■

1. Το θεμελιώδες θεώρημα της Αριθμητικής

Θα παρουσιάσουμε το θεώρημα, το οποίο είναι γνωστό ως **Λήμμα του Bezout** ή ως **επεκτεταμένος Ευκλείδειος Αλγόριθμος** (extended Euclidean algorithm), όπως επεκράτησε στον κλάδο της Θεωρητικής Πληροφορικής.

Θεώρημα *(ΛΗΜΜΑ ΤΟΥ BEZOUT)*
Έστω $a,b\in\mathbb{Z}$, *όπου τουλάχιστον ένας από τους δύο ακεραίους είναι διάφορος του μηδενός. Αν* d *είναι ο μεγαλύτερος θετικός ακέραιος με την ιδιότητα* $d|a$ *και* $d|b$, *τότε υπάρχουν* $x,y\in\mathbb{Z}$ *τέτοιοι ώστε* $d=ax+by$.

ΑΠΟΔΕΙΞΗ

Θεωρούμε το μη κενό σύνολο

$$A=\{ax+by \mid a,b,x,y\in\mathbb{Z},\ \text{όπου}\ \ ax+by>0\}.$$

Θα αποδείξουμε ότι ο ακέραιος d είναι το ελάχιστο στοιχείο του A.

Έστω d' το ελάχιστο στοιχείο του A. Τότε, υπάρχουν ακέραιοι q,r (q=το πηλίκο, r=το υπόλοιπο), τέτοιοι ώστε

$$a=d'q+r\ ,\ 0\le r<d\ .$$

Θα αποδείξουμε ότι $d'|a$. Δηλαδή, θα αποδείξουμε ότι $r=0$.

Έστω $r\neq 0$. Τότε,

$$r=a-d'q=a-(ax_1+by_1)q,$$

για κάποιους ακεραίους αριθμούς x_1, y_1.

Άρα,

$$r=a(1-x_1q)+b(-y_1q).$$

Όμως, έχουμε υποθέσει ότι $r\neq 0$. Συνεπώς, αναγκαστικά θα ισχύει ότι $r>0$ και $r=ax_2+by_2$, όπου $x_2=1-x_1q$, $y_2=-y_1q\in\mathbb{Z}$. Αυτό, όμως, είναι αδύνατον διότι έχουμε υποθέσει πως ο ακέραιος αριθμός d' είναι το ελάχιστο στοιχείο του A. Επομένως, $r=0$.

Για τον λόγο αυτό $d'\mid a$. Με ακριβώς τον ίδιο τρόπο αποδεικνύεται ότι $d'\mid b$.

Συνεπώς, έχουμε αποδείξει ότι ο ακέραιος αριθμός d' είναι κοινός διαιρέτης των a και b. Θα δείξουμε τώρα πως ο d' είναι ο μεγαλύτερος θετικός ακέραιος με την ιδιότητα αυτή.

Έστω β ένας κοινός διαιρέτης των a,b. Τότε, $\beta\mid ax+by$. Άρα, $b\mid d'$ και συνεπώς $\beta\le d'$.

Επομένως, σύμφωνα με τα παραπάνω συνεπάγεται ότι

$$d'=d=ax+by,\ \text{για}\ x,y\in\mathbb{Z}.$$

■

Παρατήρηση
Ο αριθμός d *είναι μοναδικός ακέραιος με την ιδιότητα του θεωρήματος. Αυτό αληθεύει διότι αν υπήρχαν δύο ακέραιοι* d_1,d_2 *με την ιδιότητα που ορίζει το θεώρημα, τότε θα ίσχυε* $d_1\le d_2$ *και* $d_2\le d_1$. *Επομένως,* $d_1=d_2$.

Από το παραπάνω θεώρημα προκύπτει πως για οποιονδήποτε ακέραιο αριθμό e με την ιδιότητα $e \mid a$ και $e \mid b$, θα ισχύει ότι $e \mid d$.

Στη συνέχεια θα δώσουμε τον ορισμό του μέγιστου κοινού διαιρέτη δύο ακεραίων αριθμών.

Ορισμός

Έστω $a, b \in \mathbb{Z}$, όπου τουλάχιστον ένας από τους δύο ακεραίους αριθμούς είναι διάφορος του μηδενός. Ονομάζουμε **μέγιστο κοινό διαιρέτη** (greatest common divisor) **των *a* και *b*** τον ακέραιο αριθμό d για τον οποίο ισχύει ότι $d \mid a$ και $d \mid b$ και για όποιονδήποτε ακέραιο αριθμό $e \in \mathbb{Z}$ με την ιδιότητα $e \mid a$ και $e \mid b$ να συνεπάγεται ότι $e \mid d$.

Συμβολίζουμε τον μέγιστο κοινό διαιρέτη των ακεραίων αριθμών a, b με (a, b).

Θεώρημα

Αν $(a_1, a_2, \cdots, a_n) = d$ *είναι ο μέγιστος κοινός διαιρέτης των ακεραίων αριθμών* $a_1, a_2, ..., a_n$, *τότε*

$$\left(\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_n}{d}\right) = 1.$$

ΑΠΟΔΕΙΞΗ

Ισχύει ότι

$$d \mid a_1,\ d \mid a_2,\ \cdots,\ d \mid a_n\ .$$

Άρα

$$a_1 = \kappa_1 d,\ a_2 = \kappa_2 d,\ \cdots,\ a_n = \kappa_n d \tag{1}$$

όπου $\kappa_i \in \mathbb{Z}$ για $i = 1, 2, \cdots, n$.

Έστω

$$\left(\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_n}{d}\right) = d' > 1.$$

Τότε, ομοίως ισχύει

$$d' \left| \frac{a_1}{d},\ d' \right| \frac{a_2}{d},\ \cdots,\ d' \left| \frac{a_n}{d}, \right.$$

δηλαδή

$$\frac{a_1}{d} = \kappa_1' d',\ \frac{a_2}{d} = \kappa_2' d',\ \cdots,\ \frac{a_n}{d} = \kappa_n' d' \tag{2}$$

όπου $\kappa_i' \in \mathbb{Z}$ για $i = 1, 2, \cdots, n$

Συνεπώς, από τις σχέσεις (1), (2) προκύπτει ότι

$$a_1 = \kappa_1' d' d,\ a_2 = \kappa_2' d' d,\ \cdots,\ a_n = \kappa_n' d' d\ .$$

Έτσι

$$d'd \mid a_1,\ \ d'd \mid a_2,\ \ \cdots,\ \ d'd \mid a_n .$$

Άρα

$$dd' \mid d ,$$

το οποίο είναι αδύνατον αφού $d' > 1$. Συνεπώς $d' = 1$.
Αυτό ολοκληρώνει την απόδειξη του θεωρήματος.

■

Θεώρημα

Έστω $a, b, c \in \mathbb{Z}$ *με* $a \mid bc$. *Αν* $(a,b) = 1$, *τότε* $a \mid c$ *ενώ αν* $(a,c) = 1$, *τότε* $a \mid b$.

ΑΠΟΔΕΙΞΗ

- Αν $(a,b) = 1$, τότε

$$1 = ax + by, \text{ όπου } x, y \in \mathbb{Z} .$$

Συνεπώς

$$c = acx + bcy .$$

Όμως, $a \mid acx$ και $a \mid bcy$. Άρα $a \mid c$.

- Ομοίως, αποδεικνύεται πως αν $a \mid bc$ και $(a,c) = 1$, τότε $a \mid b$.

■

Δύο βασικοί τρόποι για τον προσδιορισμό του μέγιστου κοινού διαιρέτη δύο ακεραίων.
Ο ένας τρόπος είναι ο υπολογισμός του ελαχίστου στοιχείου του συνόλου

$$A = \{ ax + by \mid a, b, x, y \in \mathbb{Z}, \text{ όπου } ax + by > 0 \}.$$

Ο δεύτερος τρόπος, που είναι περισσότερο αποδοτικός, είναι ο αλγόριθμος του Ευκλείδη.

Αλγόριθμος του Ευκλείδη

Έστω πως επιθυμούμε να βρούμε τον μέγιστο κοινό διαιρέτη των ακεραίων a, b. Θεωρούμε, χωρίς βλάβη της γενικότητας, ότι $b \le a$.

Τότε $(a,b) = (b,r)$, όπου r είναι το υπόλοιπο της διαίρεσης του a με το b. Δηλαδή

$$a = bq + r .$$

Αυτό ισχύει διότι: $(a,b) \mid b$ και $(a,b) \mid r$, αφού $r = a - bq$. Έτσι, $(a,b) \mid (b,r)$ από τον ορισμό του μέγιστου κοινού διαιρέτη. Ομοίως, $(b,r) \mid b$ και $(b,r) \mid a$, αφού $a = bq + r$. Άρα, $(b,r) \mid (a,b)$.

Λόγω του γεγονότος ότι $(a,b) \mid (b,r)$ και $(b,r) \mid (a,b)$ προκύπτει ότι $(a,b) = (b,r)$.

Αν $b = a$, τότε $(a,b) = (a,0) = (b,0) = a = b$ και ο αλγόριθμος σταματά στο πρώτο βήμα.

Γενικά ισχύει

$$(a,b) = (b,r_1) = (r_1,r_2) = \cdots = (r_{n-1},r_n) = (r_n,0) = r_n ,$$

όταν

$$a = bq_1 + r_1, \text{ αφού } b \le a$$
$$b = r_1 q_2 + r_2, \text{ αφού } 0 \le r_1 < b$$
$$r_1 = r_2 q_3 + r_3, \text{ αφού } 0 \le r_2 < r_1$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_n + r_n, \text{ αφού } 0 \le r_{n-1} < r_n$$
$$r_{n-1} = r_n q_{n+1} + 0, \text{ αφού } 0 \le r_n < r_{n-1}.$$

Θα παρουσιάσουμε τώρα τον Αλγόριθμο του Ευκλείδη γραμμένο σε γλώσσα Pascal και C αντίστοιχα, για την υλοποίησή του με την βοήθεια ηλεκτρονικών υπολογιστών.

Ο αλγόριθμος του Ευκλείδη σε γλώσσα Pascal

```
i:= a;   j:= b;
while (i > 0) and (j > 0) do
if (i > j) then i := i mod j  else  j := j mod i;
write ln(i + j).
```

Ο αλγόριθμος του Ευκλείδη σε γλώσσα *C*

```
i = a;
j = b;
 while (i > 0) && (j > 0)
{
if (i > j)
    i = i% j;
else
    j = j%i;
 }
print f(i + j) .
```

Η Μέθοδος του Blankinship

Η Μέθοδος του Blankinship αποτελεί έναν πρακτικό τρόπο για τον υπολογισμό του μέγιστου κοινού διαιρέτη δύο θετικών ακεραίων a, b.

Αν, χωρίς βλάβη της γενικότητας, θεωρήσουμε πως $a > b > 0$ τότε, ξεκινώντας από τον πίνακα

$$\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

κάνοντας γραμμοπράξεις με ακέραια πολλαπλάσια των γραμμών προσπαθούμε να δημιουργήσουμε έναν πίνακα της μορφής

$$\begin{bmatrix} d & x & y \\ 0 & x' & y' \end{bmatrix}$$

ή

$$\begin{bmatrix} 0 & x' & y' \\ d & x & y \end{bmatrix}$$

δηλαδή προσπαθούμε να δημιουργήσουμε ένα μηδενικό στοιχείο στην πρώτη στήλη του πίνακα.

Τότε, ο ζητούμενος μέγιστος κοινός διαιρέτης είναι το στοιχείο d της πρώτης στήλης του πίνακα στον οποίο καταλήξαμε και ειδικότερα

$$d = ax + by\,.$$

Επομένως, η μέθοδος του Blankinship δεν υπολογίζει μόνο τον μέγιστο κοινό διαιρέτη των a, b αλλά και τους συντελεστές x, y του Λήμματος του Bezout.

ΠΑΡΑΔΕΙΓΜΑ

Να υπολογιστεί ο μέγιστος κοινός διαιρέτης των ακεραίων αριθμών 78 και 513.

ΛΥΣΗ

Θεωρούμε τον πίνακα

$$\begin{bmatrix} 513 & 1 & 0 \\ 78 & 0 & 1 \end{bmatrix}$$

Τότε

$$\begin{bmatrix} 513 & 1 & 0 \\ 78 & 0 & 1 \end{bmatrix} \Gamma_1 \leftarrow \Gamma_1 - 6\Gamma_2 \begin{bmatrix} 45 & 1 & -6 \\ 78 & 0 & 1 \end{bmatrix} \Gamma_2 \leftarrow \Gamma_2 - \Gamma_1 \begin{bmatrix} 45 & 1 & -6 \\ 33 & -1 & 7 \end{bmatrix}$$

$$\Gamma_1 \leftarrow \Gamma_1 - \Gamma_2 \begin{bmatrix} 12 & 2 & -13 \\ 33 & -1 & 7 \end{bmatrix} \Gamma_2 \leftarrow \Gamma_2 - 2\Gamma_1 \begin{bmatrix} 12 & 2 & -13 \\ 9 & -5 & 33 \end{bmatrix}$$

$$\Gamma_1 \leftarrow \Gamma_1 - \Gamma_2 \begin{bmatrix} 3 & 7 & -46 \\ 9 & -5 & 33 \end{bmatrix} \Gamma_2 \leftarrow \Gamma_2 - 3\Gamma_1 \begin{bmatrix} 3 & 7 & -46 \\ 0 & -26 & 171 \end{bmatrix}$$

Έτσι, προκύπτει ότι $(513,78) = d = 3$ και μάλιστα $3 = 513 \cdot 7 + 78(-46)$.

■

Θεώρημα *(ΤΟ ΠΡΩΤΟ ΘΕΩΡΗΜΑ ΤΟΥ ΕΥΚΛΕΙΔΗ)*

Έστω p ενας πρώτος αριθμός και $a, b \in \mathbb{Z}$. Αν $p \mid ab$, τότε

$$p \mid a \text{ ή } p \mid b\,.$$

ΑΠΟΔΕΙΞΗ

Έστω ότι $p \nmid a$. Τότε $(a, p) = 1$ και σύμφωνα με την ιδιότητα του μέγιστου κοινού διαιρέτη, που έχουμε ήδη αποδείξει, θα ισχύει

$$1 = ax + py, \text{ όπου } x,y \in \mathbb{Z} \Leftrightarrow b = abx + pby, \text{ όπου } x,y \in \mathbb{Z}\,.$$

Όμως, $p \mid abx$ και $p \mid pby$. Άρα, $p \mid b$.

Ομοίως, αν $p \nmid b$ αποδεικνύεται ότι $p \mid a$. Συνεπώς, $p \mid a$ ή $p \mid b$.

■

Θεώρημα *(ΤΟ ΘΕΜΕΛΙΩΔΕΣ ΘΕΩΡΗΜΑ ΤΗΣ ΑΡΙΘΜΗΤΙΚΗΣ)*
Κάθε θετικός ακέραιος μπορεί να αναπαρασταθεί ως γινόμενο δυνάμεων πρώτων παραγόντων κατά μοναδικό τρόπο.

ΑΠΟΔΕΙΞΗ

• **Θα αποδείξουμε ότι κάθε θετικός ακέραιος μπορεί να αναπαρασταθεί ως γινόμενο πρώτων παραγόντων.**

Κάθε θετικός ακέραιος αριθμός n, έχει διαιρέτες τους ακέραιους αριθμούς d, τέτοιους ώστε $1 < d \le n$. Στην περίπτωση όπου ο n είναι πρώτος αριθμός θα ισχύει ότι $n = d^1$. Σε κάθε άλλη περίπτωση είναι $1 < d < n$.

Στη συνέχεια θα εξετάσουμε την περίπτωση όπου ο n είναι σύνθετος. Στην περίπτωση αυτή, ισχύει ότι $1 < d < n$. Ο ελάχιστος διαιρέτης d, θα είναι αναγκαστικά πρώτος. Αυτό συμβαίνει διότι, αν υπήρχε ένας ακέραιος αριθμός d_0, όπου $d_0 \mid d$ με $d_0 \neq d$ τότε, $d_0 < d$. Αυτό, όμως, αντιβαίνει στην επιλογή του d ως ελάχιστου διαιρέτη.

Έστω d_1 ο ελάχιστος αυτός διαιρέτης. Τότε

$$n = d_1 n_1, \text{ όπου } n_1 \in \mathbb{N}.$$

Ομοίως, ο θετικός ακέραιος n_1 έχει έναν ελάχιστο διαιρέτη d_2, που είναι πρώτος αριθμός. Έτσι προκύπτει,

$$n = d_1 d_2 n_2, \ n_2 \in \mathbb{N}.$$

Συνεχίζοντας αυτήν την διαδικασία, συνεπάγεται ότι ο θετικός ακέραιος n μπορεί να αναπαρασταθεί ως γινόμενο πρώτων παραγόντων.

Λόγω του γεγονότος ότι κάποιοι πρώτοι παράγοντες μπορεί να παρουσιάζονται περισσότερες από μία φορά στο παραπάνω γινόμενο, μπορούμε να το εκφράσουμε το γινόμενο αυτό σαν γινόμενο δυνάμεων πρώτων παραγόντων.

Έτσι,

$$n = p_1^{a_1} p_2^{a_2} \ldots p_\kappa^{a_\kappa}, \ \textit{όπου } \kappa \in \mathbb{N}.$$

Τότε, ο θετικός ακέραιος αριθμός n έχει αναπαρασταθεί σε **κανονική μορφή** (canonical form).

• **Θα αποδείξουμε ότι η αναπαράσταση αυτή είναι και μοναδική.**

Ας υποθέσουμε ότι ο θετικός ακέραιος αριθμός n έχει αναπαρασταθεί ως γινόμενο δυνάμεων πρώτων παραγόντων κατά δύο τρόπους.

Τότε ισχύει

$$p_1^{a_1} p_2^{a_2} \ldots p_\kappa^{a_\kappa} = q_1^{b_1} q_2^{b_2} \ldots q_\lambda^{b_\lambda}, \text{ όπου } \kappa, \lambda \in \mathbb{N}.$$

Από το πρώτο θεώρημα του Ευκλείδη θα έχουμε

$$p_i \mid p_1^{a_1} p_2^{a_2} \ldots p_\kappa^{a_\kappa} \Rightarrow p_i \mid q_1^{b_1} q_2^{b_2} \ldots q_\lambda^{b_\lambda} \Rightarrow p_i \mid q_j,$$

για κάθε i, j, όπου $i = 1,2,\ldots,\kappa$ και $j = 1,2,\ldots,\lambda$.

Άρα, κάθε p_i είναι ίσο με ένα q_j. Άρα, $\kappa = \lambda$.

Αρκεί να δείξουμε ότι

$$a_i = b_i, \text{ για κάθε } i, \text{ όπου } i = 1,2,...,\kappa = \lambda .$$

Έστω $a_i \neq b_i$. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $a_i > b_i$. Τότε

$$\begin{aligned} p_1^{a_1} p_2^{a_2} ... p_i^{a_i} ... p_\kappa^{a_\kappa} &= q_1^{b_1} q_2^{b_2} ... q_i^{b_i} ... q_\kappa^{b_\kappa} \\ &= p_1^{b_1} p_2^{b_2} ... p_i^{b_i} ... p_\kappa^{b_\kappa} \\ \Leftrightarrow p_1^{\alpha_1} p_2^{\alpha_2} ... p_i^{\alpha_i - b_i} ... p_\kappa^{\alpha_\kappa} &= p_1^{b_1} p_2^{b_2} ... p_{i-1}^{b_{i-1}} p_{i+1}^{b_{i+1}} ... p_\kappa^{b_\kappa} \end{aligned} \quad (1)$$

Αφού $a_i - b_i \geq 1$, από την ισότητα (1) προκύπτει ότι

$$p_i \mid p_1^{a_1} p_2^{a_2} ... p_\kappa^{a_\kappa} \text{ αλλά } p_i \nmid p_1^{b_1} p_2^{b_2} ... p_\kappa^{b_\kappa},$$

το οποίο είναι αδύνατον.

Όμως, καταλήγουμε σε άτοπο στην περίπτωση όπου $a_i < b_i$. Άρα, αναγκαστικά θα ισχύει ότι $a_i = b_i$, για κάθε $i = 1,2,...,\kappa$.

Αυτό ολοκληρώνει την απόδειξη του θεωρήματος.

■

Λήμμα

Κάθε θετικός ακέραιος n μπορεί να αναπαρασταθεί κατά μοναδικό τρόπο, ως το γινόμενο $a^2 b$ δύο ακεραίων αριθμών a,b, όπου ο θετικός ακέραιος b έχει την ιδιότητα να μη μπορεί να διαιρεθεί από κανένα τετράγωνο πρώτου αριθμού (b is a squarefree integer).

ΑΠΟΔΕΙΞΗ

Από το θεμελιώδες θεώρημα της Αριθμητικής γνωρίζουμε ότι κάθε θετικός ακέραιος μπορεί να αναπαρασταθεί, κατά μοναδικό τρόπο, ως γινόμενο δυνάμεων πρώτων παραγόντων.

Έτσι, λαμβάνουμε ότι:

$$n = p_1^{q_1} p_2^{q_2} ... p_\kappa^{q_\kappa}, \text{ όπου } n \in \mathbb{N}.$$

Θεωρούμε το σύνολο $A = \{q_1, q_2, ..., q_\kappa\}$. Έστω m_i οι ακέραιοι αριθμοί που ανήκουν στο σύνολο A και είναι άρτιοι και h_j οι ακέραιοι αριθμοί που ανήκουν στο σύνολο A και είναι περιττοί.

Τότε

$$\begin{aligned} n &= \left(p_{i_1}^{m_1} p_{i_2}^{m_2} ... p_{i_\lambda}^{m_\lambda}\right) \cdot \left(p_{j_1}^{h_1} p_{j_2}^{h_2} ... p_{j_\mu}^{h_\mu}\right) \\ &= \left(p_{i_1}^{2e_1} p_{i_2}^{2e_2} ... p_{i_\lambda}^{2e_\lambda}\right) \cdot \left(p_{j_1}^{2f_1+1} p_{j_2}^{2f_2+1} ... p_{j_\mu}^{2f_\mu+1}\right) \\ &= \left(p_{i_1}^{e_1} p_{i_2}^{e_2} ... p_{i_\lambda}^{e_\lambda} \cdot p_{j_1}^{f_1} p_{j_2}^{f_2} ... p_{j_\mu}^{f_\mu}\right)^2 \cdot \left(p_{j_1} ... p_{j_\mu}\right) \\ &= a^2 \cdot b \end{aligned}$$

Οι ακέραιοι a,b είναι μοναδικοί διότι οι ακέραιοι p_i, q_i είναι μοναδικοί και συνεπώς οι m_i, h_j είναι μοναδικοί.

■

2. Αριθμητικές συναρτήσεις

Αριθμητική συνάρτηση ονομάζεται μια συνάρτηση $f:\mathbb{N}\to\mathbb{C}$, η οποία έχει ως πεδίο ορισμού το σύνολο των φυσικών αριθμών $\mathbb{N}$ και τιμές στο σύνολο των μιγαδικών αριθμών $\mathbb{C}$.

Η συνάρτηση f καλείται *αθροιστική* (additive function) όταν ισχύει

$$f(mn)=f(m)+f(n) \tag{1}$$

για όλους τους ακεραίους m,n οι οποίοι είναι πρώτοι μεταξύ τους.

Στην περίπτωση όπου η συνθήκη (1) ικανοποιείται για οποιουσδήποτε ακέραιους m,n, οι οποίοι δεν είναι αναγκαστικά πρώτοι μεταξύ τους, τότε η συνάρτηση f ονομάζεται *πλήρως αθροιστική*.

Η συνάρτηση f ονομάζεται *πολλαπλασιαστική* όταν αληθεύει

$$f(1)=1 \text{ και } f(mn)=f(m)f(n) \tag{2}$$

για όλους τους ακεραίους m,n οι οποίοι είναι πρώτοι μεταξύ τους.

Στην περίπτωση όπου οι συνθήκες (2) ικανοποιούνται για οποιουσδήποτε ακέραιους m,n, οι οποίοι δεν είναι αναγκαστικά πρώτοι μεταξύ τους, τότε η συνάρτηση f ονομάζεται *πλήρως πολλαπλασιαστική*.

Η συνάρτηση Möbius μ(n)

Η συνάρτηση Möbius ορίζεται από τον παρακάτω τύπο

$$\mu(n)=\begin{cases}1, & \alpha\nu \quad n=1\\ (-1)^{\kappa}, & \alpha\nu \quad n=p_1^{a_1}\ldots p_\kappa^{a_\kappa} \quad \mu\varepsilon\ a_i=1\ (i=1,2,\ldots,\kappa)\\ 0, & \acute{o}\varepsilon\ \kappa\acute{a}\grave{\varepsilon}\ \acute{a}\lambda\lambda\eta\ \pi\varepsilon\rho\acute{\imath}\pi\tau\omega\acute{o}\eta\end{cases}$$

> ***Σχόλιο***
>
> *Στην παραπάνω αναπαράσταση του n στη μορφή $p_1^{a_1}\ldots p_\kappa^{a_\kappa}$ με $p_1,\ldots,p_\kappa$ **δεν** συμβολίζουμε αναγκαστικά τον πρώτο, ..., τον κ-οστό πρώτο αριθμό στην ακολουθία των πρώτων αριθμών (π.χ. μπορεί να είναι $p_1\neq 2$).*

Έτσι, για **παράδειγμα** ισχύει

$$\mu(2)=-1,\ \mu(3)=-1,\ \mu(4)=0,\ \mu(5)=-1,\ \mu(6)=1.$$

- Η συνάρτηση Möbius είναι πολλαπλασιαστική, διότι ισχύει ότι

$$\mu(1)=1 \text{ και } \mu(mn)=\mu(m)\mu(n)$$

για όλους τους ακέραιους m,n με $(m,n)=1$.

> ***Παρατήρηση***
>
> *Η συνάρτηση Μφbius **δεν** είναι **πλήρως πολλαπλασιαστική** αφού*
> *μ(4)=0 και μ(2)μ(2)=(–1)(–1)=1.*

Θεώρημα

$$\sum_{d|n}\mu(d)=1,\ \alpha\nu\ n=1\quad \kappa\alpha\iota\quad \sum_{d|n}\mu(d)=0,\ \alpha\nu\ n>1$$

ΑΠΟΔΕΙΞΗ

• Η περίπτωση $n=1$ είναι προφανής διότι $\mu(1)=1,$ από τον ορισμό της συνάρτησης Möbius.

• Για $n>1$ λαμβάνουμε ότι

$$n=p_1^{a_1}p_2^{a_2}\ldots p_\kappa^{a_\kappa}$$

΄Αρα

$$\sum_{d|n}\mu(d)=\mu(1)+\sum_{1\le i\le\kappa}\mu(p_i)+\sum_{\substack{i\ne j\\ 1\le i,j\le\kappa}}\mu(p_ip_j)+\cdots+\mu(p_1p_2\ldots p_\kappa),$$

όπου το τυχαίο άθροισμα

$$\sum_{i_1\ne i_2\ne\ldots\ne i_\lambda}\mu(p_{i_1}p_{i_2}\cdots p_{i_\lambda})$$

εκτείνεται σ' όλους τους δυνατούς συνδιασμούς λ διαφορετικών μεταξύ τους πρώτων παραγόντων του n. Από τον ορισμό προκύπτει πως στην περίπτωση όπου οι πρώτοι αριθμοί δεν είναι όλοι διάφοροι μεταξύ τους, τότε η συνάρτηση Möbius μηδενίζεται.

Από τον διωνυμικό τύπο συνεπάγεται

$$\sum_{d|n}\mu(d)=1+\binom{\kappa}{1}(-1)+\binom{\kappa}{2}(-1)^2+\ldots+\binom{\kappa}{\kappa}(-1)^\kappa$$

$$=(1-1)^\kappa=0\,.$$

Επομένως

$$\sum_{d|n}\mu(d)=0,\ \alpha\nu\ n>1\ .$$

Αυτό, ολοκληρώνει την απόδειξη του θεωρήματος. ■

Παρατήρηση

Η παραπάνω απόδειξη για την συνάρτηση Mφbius $\mu(n)$, καθώς και η τέταρτη απόδειξη στην παράγραφο για την συνάρτηση Euler $\varphi(n)$, που θα δούμε παρακάτω, βασίζεται στην Αρχή Εγκλεισμού – Αποκλεισμού (Inclusion – Exclusion).

Θεώρημα *(ΤΥΠΟΣ ΑΝΤΙΣΤΡΟΦΗΣ ΜΟBIUS – The Mφbius inversion formula).*
Αν ισχύει ότι

$$g(n)=\sum_{d|n}f(d),$$

τότε

$$f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)g(d)$$

και αντιστρόφως.

ΑΠΟΔΕΙΞΗ

● **Θα αποδείξουμε πρώτα το ευθύ.**

Γενικά, για κάθε αριθμητική συνάρτηση $m(n)$, ισχύει ότι

$$\sum_{d|n} m(d) = \sum_{d|n} m\left(\frac{n}{d}\right), \text{ αφού } \frac{n}{d} = d',$$

όπου d' είναι ένας διαιρέτης του n.
Ακολουθώντας την ίδια ιδέα προκύπτει ότι

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right). \tag{1}$$

΄Ομως

$$\sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right) = \sum_{d|n} \left(\mu(d) \cdot \sum_{\lambda \left| \frac{n}{d} \right.} f(\lambda) \right). \tag{2}$$

Θα εκφράσουμε το δεξί μέλος της σχέσης (2) έτσι ώστε να περιλαμβάνει ένα μόνο άθροισμα. Για να το κάνουμε αυτό πρέπει να βρούμε μια κοινή συνθήκη για τα αθροίσματα

$$\sum_{d|n} \quad \text{και} \quad \sum_{\lambda \left| \frac{n}{d} \right.} .$$

Η συνθήκη αυτή είναι η

$$\lambda d \mid n .$$

Άρα

$$\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{\lambda d|n} \mu(d) \cdot f(\lambda)$$

Ομοίως μπορούμε να γράψουμε

$$\sum_{\lambda|n} \left(f(\lambda) \sum_{d \left| \frac{n}{\lambda} \right.} \mu(d) \right) = \sum_{\lambda d|n} \mu(d) \cdot f(\lambda)$$

Συνεπώς

$$\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{\lambda|n} \left(f(\lambda) \sum_{d \left| \frac{n}{\lambda} \right.} \mu(d) \right). \tag{3}$$

Αλλά, από το θεώρημα που αποδείξαμε προηγουμένως συνεπάγεται ότι

$$\sum_{d \left| \frac{n}{\lambda} \right.} \mu(d) = 1 \text{ αν και μόνο αν } \frac{n}{\lambda} = 1, \text{ δηλαδή } n = \lambda$$

(σε κάθε άλλη περίπτωση το άθροισμα μηδενίζεται).

Στην περίπτωση, όμως, όπου $n=\lambda$ προκύπτει

$$\sum_{\lambda \mid n}\left(f(\lambda)\sum_{d\mid \frac{n}{\lambda}}\mu(d)\right)=f(n). \tag{4}$$

Από τις σχέσεις (1), (3) και (4) προκύπτει ότι

$$\text{αν } g(n)=\sum_{d\mid n}f(d) \text{ τότε } f(n)=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)g(d) \ .$$

• **Για το αντίστροφο, ακολουθούμε παρόμοια μέθοδο.**

Θα αποδείξουμε ότι αν

$$f(n)=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)g(d)\ ,$$

τότε

$$g(n)=\sum_{d\mid n}f\ (d).$$

Θα ξεκινήσουμε από το δεύτερο μέλος για να φτάσουμε στο πρώτο μέλος:

$$\sum_{d\mid n}f\ (d)=\sum_{d\mid n}f\left(\frac{n}{d}\right),$$

$$=\sum_{d\mid n}\sum_{\lambda\mid \frac{n}{d}}\mu\left(\frac{n}{\lambda d}\right)g(\lambda),$$

$$=\sum_{d\lambda\mid n}\mu\left(\frac{n}{\lambda d}\right)g(\lambda)$$

$$=\sum_{\lambda\mid n}\left(g(\lambda)\sum_{d\mid \frac{n}{\lambda}}\mu\left(\frac{n}{\lambda d}\right)\right),$$

όπως ακριβώς κάνουμε και στο ευθύ.

Το άθροισμα

$$\sum_{d\mid \frac{n}{\lambda}}\mu\left(\frac{n}{\lambda d}\right) \text{ είναι ίσο με 1 αν και μόνο αν } n=\lambda$$

(σε κάθε άλλη περίπτωση το άθροισμα μηδενίζεται).

Έτσι, για $n=\lambda$ λαμβάνουμε ότι

$$\sum_{d\mid n}f(d)=g(n).$$

Αυτό, ολοκληρώνει την απόδειξη του θεωρήματος.

■

ΕΦΑΡΜΟΓΗ

Έστω f *μια πολλαπλασιαστική συνάρτηση και*

$$n = p_1^{a_1} p_2^{a_2} \ldots p_\kappa^{a_\kappa},\ \text{όπου}\ \kappa \in \mathbb{N}$$

η κανονική μορφή του θετικού ακεραίου n.

Να δειχθεί ότι

$$\sum_{d \mid n} \mu(d) f(d) = \prod_{i=1}^{\kappa} (1 - f(p_i)),$$

όπου το άθροισμα εκτείνεται σ' όλους τους διαιρέτες του n.

ΑΠΟΔΕΙΞΗ

Οι μη-μηδενικοί όροι του αθροίσματος

$$\sum_{d \mid n} \mu(d) f(d)$$

αντιστοιχούν σε διαιρέτες d, όπου

$$d = p_1^{q_1} p_2^{q_2} \ldots p_\kappa^{q_\kappa},\ \text{για}\ q_i = 0\ \text{ή}\ 1\ \text{και}\ 1 \le i \le \kappa.$$

΄Αρα

$$\sum_{d \mid n} \mu(d) f(d) = \sum_{q_i = 0\ \text{ή}\ 1} (-1)^\kappa f\left(p_1^{q_1} \ldots p_\kappa^{q_\kappa}\right), \qquad (1)$$

όπου το άθροισμα στο δεξί μέλος της σχέσης (1) εκτείνεται σ' όλους τους δυνατούς συνδυασμούς γινομένων πρώτων παραγόντων του n σε δυνάμεις 0 ή 1.

Όμως, αν εκτελέσουμε τις πράξεις στο γινόμενο

$$(1 - f(p_1))\,(1 - f(p_2)) \ldots (1 - f(p_\kappa))$$

προκύπτει ένα άθροισμα της μορφής

$$\sum (-1)^\kappa f\left(p_1^{q_1}\right) f\left(p_2^{q_2}\right) \ldots f\left(p_\kappa^{q_\kappa}\right),$$

$$= \sum (-1)^\kappa f\left(p_1^{q_1} p_2^{q_2} \ldots p_\kappa^{q_\kappa}\right),$$

όπου $q_i = 0$ ή 1 και $1 \le i \le \kappa$

Δηλαδή ισχύει

$$\prod_{i=1}^{\kappa} (1 - f(p_i)) = \sum (-1)^\kappa f\left(p_1^{q_1} \ldots p_\kappa^{q_\kappa}\right)$$

$$\overset{(1)}{=} \sum_{d \mid n} \mu(d) f(d).$$

Αυτό ολοκληρώνει την απόδειξη.

■

Σχόλιο

Στην ειδική περίπτωση όπου $f(d) = 1$ *για κάθε διαιρέτη* d *του* n*, τότε:*

$$\sum_{d \mid n} \mu(d) f(d) = \sum_{d \mid n} \mu(d) = \prod_{i=1}^{\kappa} (1 - 1) = \left\lfloor \frac{1}{n} \right\rfloor,$$

το οποίο είναι ακριβώς το θεώρημα που αποδείξαμε στην ενότητα για την συνάρτηση Μφbius.

Η συνάρτηση του Euler $\phi(n)$

Η συνάρτηση $\phi(n)$ του Euler εκφράζει το πλήθος των φυσικών αριθμών, οι οποίοι είναι **μικρότεροι ή το πολύ ίσοι με n και πρώτοι προς το n.**

— Συμβολικά, μπορούμε να εκφράσουμε την συνάρτηση $\phi(n)$ ως εξής:

$$\phi(n)=\sum_{m=1}^{n}\left\lfloor \frac{1}{(n,m)} \right\rfloor$$

(άθροισμα ακεραίων μερών)
Είναι

$$\phi(1)=1, \phi(2)=1,\ \phi(3)=2,\ \phi(6)=2,\ \phi(9)=6\ .$$

— Δύο βασικές ιδιότητες της συνάρτησης ϕ, τις οποίες θα γενικεύσουμε παρακάτω, είναι οι εξής:

- Για κάθε πρώτο αριθμό p ισχύει ότι

$$\phi(p^{\kappa})=p^{\kappa}-p^{\kappa-1}\ .$$

ΑΠΟΔΕΙΞΗ

Οι μοναδικοί θετικοί ακέραιοι, οι οποίοι λαμβάνουν τιμή το πολύ p^{κ} και δεν είναι πρώτοι πρός τον αριθμό p^{κ} είναι οι αριθμοί

$$p, 2p,\ 3p, ...,\ p^{\kappa-1}\ p\ .$$

Το πλήθος των αριθμών αυτών είναι $p^{\kappa-1}$.

Συνεπώς, το πλήθος των θετικών ακεραίων οι οποίοι δεν υπερβαίνουν τον p^{κ} και είναι πρώτοι προς αυτόν, είναι

$$p^{\kappa}-p^{\kappa-1}.$$

Αυτό ολοκληρώνει την απόδειξη της ιδιότητας.

■

- Η συνάρτηση $\phi(n)$ είναι πολλαπλασιαστική, δηλαδή ισχύει ότι

$$\phi(mn)=\phi(m)\phi(n),\ \alpha\nu\ (m,n)=1.$$

Θα παρουσιάσουμε την απόδειξη αυτού του θεωρήματος αφού πρώτα αποδείξουμε κάποια άλλα βασικά θεωρήματα.

Θεώρημα
Για κάθε φυσικό αριθμό n ισχύει ότι

$$\phi(n)=\sum_{d\mid n}\mu(d)\frac{n}{d}$$

ΑΠΟΔΕΙΞΗ

Έχουμε αποδείξει προηγούμενα πως το άθροισμα $\sum_{d|n}\mu(d)$ είναι ίσο με 1 για $n=1$ ενώ είναι ίσο με 0 σε κάθε άλλη περίπτωση. Έτσι, μπορούμε να γράψουμε

$$\sum_{d|n}\mu(d)=\left\lfloor\frac{1}{n}\right\rfloor.$$

Λόγω του γεγονότος αυτού λαμβάνουμε

$$\phi(n)=\sum_{m=1}^{n}\left\lfloor\frac{1}{(n,m)}\right\rfloor=\sum_{m=1}^{n}\sum_{d|(n,m)}\mu(d). \tag{1}$$

Οι συνθήκες που έχουμε στα παραπάνω αθροίσματα είναι

$$1\le m\le n$$

$$d\mid n$$

και

$$d\mid m\,.$$

Δηλαδή $1\le \lambda d\le n$, για κάποιο $\lambda\in\mathbb{N}$

ή

$$1\le\lambda\le\frac{n}{d}\ \text{ και }\ d\mid n\,.$$

Επομένως, μπορούμε να γράψουμε

$$\sum_{m=1}^{n}\sum_{d|(n,m)}\mu(d)=\sum_{d|n}\sum_{\lambda=1}^{n/d}\mu(d)=\sum_{d|n}\frac{n}{d}\mu(d)\,. \tag{2}$$

Άρα από τις σχέσεις (1), (2) προκύπτει ότι

$$\phi(n)=\sum_{d|n}\mu(d)\frac{n}{d}.$$

■

Θεώρημα

Για κάθε φυσικό αριθμό n ισχύει ότι

$$\sum_{d|n}\phi(d)=n$$

ΑΠΟΔΕΙΞΗ

Όλοι οι θετικοί ακέραιοι κ οι οποίοι δεν υπερβαίνουν τον φυσικό αριθμό n έχουν κάποια σχέση διαιρετότητας με τον n. Δηλαδή, είτε θα είναι πρώτοι ως προς τον n είτε $(n,\kappa)=d>1$.

Γενικά αν $(n,\kappa)=d$, τότε $\left(\frac{n}{d},\frac{\kappa}{d}\right)=1$. Οπότε, το πλήθος των θετικών ακεραίων για τους οποίους ισχύει ότι $(n,\kappa)=d$ είναι $\phi\left(\frac{n}{d}\right)$.

Όμως, το πλήθος των θετικών ακεραίων κ, όπου $\kappa\le n$ είναι, προφανώς, ίσο με n.

Άρα

$$\sum_{d|n}\phi\left(\frac{n}{d}\right)=n.$$

Αλλά

$$\sum_{d|n}\phi\left(\frac{n}{d}\right)=\sum_{d|n}\phi(d),$$

συνεπώς

$$\sum_{d|n}\phi(d)=n.$$

■

Σχόλιο

Μιά άλλη απόδειξη του θεωρήματος μπορεί να δοθεί με τον τύπο ανιστροφής του Μφbius.

Θεώρημα

Για κάθε φυσικό αριθμό n *με* $n=p_1^{a_1}p_2^{a_2}...p_\kappa^{a_\kappa}$ *ισχύει ότι*

$$\phi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_\kappa}\right)$$

και επομένως για οποιουσδήποτε φυσικούς αριθμούς n_1, n_2 *ισχύει ότι*

$$\phi(n_1n_2)=\phi(n_1)\ \phi(n_2)\ \frac{d}{\phi(d)}$$

όπου $d=(n_1,n_2)$.

ΑΠΟΔΕΙΞΗ

Είναι

$$\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_\kappa}\right)$$
$$=1+\sum\frac{(-1)^\lambda}{p_{m_1}p_{m_2}\cdots p_{m_\lambda}},$$

όπου $m_i=1,2,..,\kappa$

και το άθροισμα εκτείνεται σ' όλους τους δυνατούς συνδυασμούς γινομένων $p_{m_1}p_{m_2}...p_{m_\lambda}$.

Όμως, έχουμε

$$\mu\left(p_{m_1}p_{m_2}...p_{m_\lambda}\right)=(-1)^\lambda,\ \text{όπου}\ \mu(1)=1$$

και $\mu(d)=0$, αν ο d διαιρείται από το τετράγωνο ενός από τους πρώτους παράγοντες $p_1, p_2,..., p_\kappa$. Επομένως

$$\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_\kappa}\right)=\sum_{d|n}\frac{m(d)}{d}$$
$$=\frac{\phi(n)}{n}.$$

Άρα

$$\phi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_\kappa}\right).$$

Για να αποδείξουμε τώρα ότι

$$\phi(n_1n_2)=\phi(n_1)\phi(n_2)\frac{d}{\phi(d)}$$

έχουμε

$$\phi(n_1n_2)=(n_1n_2)\prod_{p|n_1n_2}\left(1-\frac{1}{p}\right).$$

Όμως, αν $n_1n_2 = p_1^{q_1} p_2^{q_2} ... p_m^{q_m}$, τότε στο γινόμενο

$$\prod_{p|n_1n_2}\left(1-\frac{1}{p}\right)$$

οι αριθμοί $p_1, p_2, ..., p_m$ παρουσιάζονται από μια μόνο φορά σε έναν από τους παράγοντες

$$1-\frac{1}{p}.$$

Αντιθέτως, αν θεωρήσουμε το γινόμενο

$$\prod_{p|n_1}\left(1-\frac{1}{p}\right)\cdot\prod_{p|n_2}\left(1-\frac{1}{p}\right),$$

τότε αυτοί οι πρώτοι παράγοντες από τους $p_1, p_2, ..., p_m$ οι οποίοι διαιρούν ταυτοχρόνως τον n_1 και τον n_2, παρουσιάζονται δύο φορές. Δηλαδή εμφανίζονται σε δύο παράγοντες $\left(1-\frac{1}{p}\right)$ του γινομένου.

Συνεπώς

$$\prod_{p|n_1n_2}\left(1-\frac{1}{p}\right)=\frac{\prod_{p|n_1}\left(1-\frac{1}{p}\right)\cdot\prod_{p|n_2}\left(1-\frac{1}{p}\right)}{\prod_{\substack{p|n_1\\p|n_2}}\left(1-\frac{1}{p}\right)}$$

Άρα

$$\phi(n_1n_2)=\frac{n_1\prod_{p|n_1}\left(1-\frac{1}{p}\right)\cdot n_2\prod_{p|n_2}\left(1-\frac{1}{p}\right)}{\prod_{\substack{p|n_1\\p|n_2}}\left(1-\frac{1}{p}\right)}$$

$$=\frac{\phi(n_1)\ \phi(n_2)}{\prod_{p|d}\left(1-\frac{1}{p}\right)}$$

$$= \frac{\phi(n_1)\phi(n_2)}{\frac{\phi(d)}{d}}$$

$$= \phi(n_1)\phi(n_2)\frac{d}{\phi(d)}.$$

Επομένως

$$\phi(n_1 n_2) = \phi(n_1)\ \phi(n_2)\ \frac{d}{\phi(d)}\ .$$

Αυτό, ολοκληρώνει την απόδειξη.

■

> ***Σχόλιο***
> *Για περισσότερες πληροφορίες πάνω στις συναρτήσεις Μφbius και Euler ο αναγνώστης παραπέμπεται σε βιβλία Συνδιαστικής, για παράδειγμα στο βιβλίο του* Laszlo Lovαsz, Combinatorial Problems and Exercises, North Holland Publishing Co., 1979.

Η συνάρτηση $\tau(n)$

Η συνάρτηση $\tau(n)$ είναι μία αριθμητική συνάρτηση που εκφράζει **το πλήθος των θετικών διαιρετών του φυσικού αριθμού** n**.**

- Συμβολικά γράφουμε

$$\tau(n) = \sum_{\substack{d \mid n \\ d \geq 1}} 1,$$

όπου το άθροισμα εκτείνεται σ' όλους τους θετικούς διαιρέτες του n.

- Η συνάρτηση $\tau(n)$ είναι πολλαπλασιαστική, δηλαδή αν $(m,n)=1$ τότε ισχύει

$$\tau(mn) = \tau(m)\tau(n).$$

Η ιδιότητα αυτή είναι πολύ χρήσιμη για τον υπολογισμό του πλήθους των διαιρετών μεγάλων ακεραίων αριθμών.

Θεώρημα

Αν $n = p_1^{a_1} p_2^{a_2} \ldots p_\kappa^{a_\kappa}$ *είναι η κανονική μορφή του θετικού ακεραίου αριθμού* n*, τότε ισχύει η σχέση*

$$\tau(n) = (a_1+1)\ (a_2+1)\ \cdots\ (a_\kappa+1)\ .$$

ΑΠΟΔΕΙΞΗ

Θα χρησιμοποιήσουμε την Μέθοδο της Μαθηματικής Επαγωγής.

Για $\kappa = 1$ αληθεύει

$$\tau(n) = \tau\left(p_1^{a_1}\right).$$

Όμως οι διαιρέτες του *n,* όπου $n = p_1^{a_1}$ είναι οι φυσικοί αριθμοί $1, p_1, p_1^2, \ldots, p_1^{\alpha_1}$.

Δηλαδή ισχύει

$$\tau\ (n) = a_1 + 1.$$

Θέτουμε, $m = p_1^{\alpha_1} \ldots p_{\kappa-1}^{\alpha_{\kappa-1}}$ και υποθέτουμε ότι

$$\tau(m) = (\alpha_1 + 1)\ (\alpha_2 + 1)\ \cdots\ (\alpha_{\kappa-1} + 1). \qquad (1)$$

Όμως, οι διαιρέτες του θετικού ακεραίου αριθμού n, όπου $n = p_1^{a_1} p_2^{a_2} \ldots p_{\kappa}^{a_{\kappa}}$ προκύπτουν από τους διαιρέτες του θετικού ακεραίου m αν πολλαπλασιασθούν αντίστοιχα με τις δυνάμεις του παράγοντα p_{κ}, äηλ. $\left(p_{\kappa}^0, p_{\kappa}^1, p_{\kappa}^2, \ldots, p_{\kappa}^{a_{\kappa}}\right)$.

Συνεπώς, αν συμβολίσουμε με d_n και d_m τους θετικούς διαιρέτες των n και m αντίστοιχα, τότε

$$\tau(n) = \sum_{d_n \mid n} 1 \ = \sum_{d_m \mid m} 1 + \sum_{d_m p_{\kappa} \mid n} 1 + \sum_{d_m p_{\kappa}^2 \mid n} 1 + \cdots + \sum_{d_m p_{\kappa}^{\alpha_{\kappa}} \mid n} 1$$

και επειδή το πλήθος των διαιρετών d_m είναι $\tau(m)$, λαμβάνουμε ότι

$$\begin{aligned} \tau(n) &= \tau(m) + \tau(m) + \tau(m) + \ldots + \tau(m) \quad (a_{\kappa} + 1 \text{ öορές}) \qquad (2) \\ &= \tau(\mu)(a_{\kappa} + 1). \end{aligned}$$

Από τις σχέσεις (1) και (2) προκύπτει ότι

$$\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_{\kappa-1} + 1)(a_{\kappa} + 1).$$

Αυτό ολοκληρώνει την απόδειξη του θεωρήματος.

■

Παρατήρηση

Για την συνάρτηση $\tau(n)$ αληθεύει η σχέση

$$\tau(n) = \tau(p_1^{a_1})\ \tau(p_2^{a_2})\ \ldots\ \tau(p_{\kappa}^{a_{\kappa}}),$$

όπου $n = p_1^{a_1} p_2^{a_2} \ldots p_{\kappa}^{a_{\kappa}}$.

ΠΑΡΑΔΕΙΓΜΑΤΑ

- $\tau(60) = \tau\left(2^2 \cdot 3 \cdot 5\right) = (2+1)(1+1)(1+1) = 12$
- $\tau(120) = \tau\left(2^3 \cdot 3 \cdot 5\right) = (3+1)(1+1)(1+1) = 16$
- $\tau(3528) = \tau\left(2^3 \cdot 3^2 \cdot 7^2\right) = (3+1)(2+1)(2+1) = 36$.

Η συνάρτηση $\sigma_a(n)$

Η $ó_a(n)$ είναι μια αριθμητική συνάρτηση που εκφράζει το **άθροισμα των a – οστών δυνάμεων των θετικών διαιρετών του φυσικού αριθμού** n, όπου ο a μπορεί να λάβει οποιαδήποτε μιγαδική τιμή.

Έτσι, συμβολικά γράφουμε

$$\sigma_a(n) = \sum_{\substack{d \mid n \\ d \geq 1}} d^a \ ,$$

όπου το άθροισμα εκτείνεται σ' όλους τους θετικούς διαιρέτες του n.

- Στην περίπτωση όπου $\kappa = 0$ προκύπτει η συνάρτηση $\tau(n)$, δηλαδή

$$\tau(n) = \sigma_0(n).$$

- Η συνάρτηση $\sigma_a(n)$ είναι πολλαπλασιαστική, δηλαδή αν $(m,n)=1$ τότε ισχύει

$$\sigma_a(mn) = \sigma_a(m)\sigma_a(n).$$

Θεώρημα

Αν $n = p_1^{a_1} p_2^{a_2} \dots p_\kappa^{a_\kappa}$ είναι η κανονική μορφή του θετικού ακεραίου αριθμού n, τότε ισχύει ότι:

$$\sigma_1(n) = \frac{p_1^{a_1+1}-1}{p_1-1} \cdot \frac{p_2^{a_2+1}-1}{p_2-1} \dots \frac{p_\kappa^{a_\kappa+1}-1}{p_\kappa-1}$$

ΑΠΟΔΕΙΞΗ

Θα κάνουμε χρήση της Μεθόδου της Μαθηματικής Επαγωγής για τον ακέραιο αριθμό κ.

- Για $\kappa = 1$ ισχύει

$$\sigma_1(n) = \sigma_1\left(p_1^{a_1}\right).$$

Όμως οι διαιρέτες του n, όπου $n = p_1^{\alpha_1}$ είναι οι θετικοί ακέραιοι $1, p_1, p_1^2, \dots, p_1^{a_1}$ και επομένως

$$\sigma_1(n) = 1 + p_1 + p_1^2 + \dots + p_1^{a_1} = \frac{p_1^{a_1+1}-1}{p_1-1}.$$

- Όπως και στην περίπτωση του θεωρήματος για την συνάρτηση $\tau(n)$, θέτουμε $m = p_1^{a_1} \dots p_{\kappa-1}^{a_{\kappa-1}}$ και υποθέτουμε ότι ισχύει

$$\sigma_1(m) = \frac{p_1^{a_1+1}-1}{p_1-1} \cdot \frac{p_2^{a_2+1}-1}{p_2-1} \dots \frac{p_{\kappa-1}^{a_{\kappa-1}}-1}{p_{\kappa-1}-1}. \tag{3}$$

Ακολουθούμε την ίδια λογική που ακολουθήσαμε και στο προηγούμενο θεώρημα. Έτσι, αν d_n και d_m είναι οι θετικοί διαιρέτες των n, m αντίστοιχα, όπου $n = p_1^{a_1} p_2^{a_2} \dots p_\kappa^{a_\kappa}$, τότε ισχύει

$$\begin{aligned}
\sigma_1(n) &= \sum_{d_n \mid n} d_n \\
&= \sum_{d_m \mid m} d_m + \sum_{d_m \mid m} d_m p_\kappa + \sum_{d_m \mid m} d_m p_\kappa^2 + \dots + \sum_{d_m \mid m} d_m p_\kappa^{a_\kappa} \\
&= 1 \cdot \sum_{d_m \mid m} d_m + p_\kappa \sum_{d_m \mid m} d_m + p_\kappa^2 \sum_{d_m \mid m} d_m + \dots + p_\kappa^{a_\kappa} \sum_{d_m \mid m} d_m \\
&= \left(1 + p_\kappa + p_\kappa^2 + \dots + p_\kappa^{a_\kappa}\right) \sum_{d_m \mid m} d_m = \frac{p_\kappa^{a_\kappa+1}-1}{p_\kappa-1} \cdot \sigma_1(m)
\end{aligned} \tag{4}$$

Επομένως, από τις σχέσεις (3), (4) προκύπτει

$$\sigma_1(n)=\frac{p_1^{a_1+1}-1}{p_1-1}\cdot\frac{p_2^{a_2+1}-1}{p_2-1}\cdots\frac{p_{\kappa-1}^{a_{\kappa-1}+1}-1}{p_{\kappa-1}-1}\cdot\frac{p_\kappa^{a_\kappa+1}-1}{p_\kappa-1}.$$

Αυτό ολοκληρώνει την απόδειξη του θεωρήματος.

■

Παρατηρήσεις

Για την συνάρτηση $\sigma_a(n)$ *ισχύουν οι ιδιότητες:*

- $$\sigma_a(n)=\prod_{i=1}^{\kappa}\frac{p_i^{(a_i+1)a}-1}{p_i^a-1}\ .$$
- $$\sigma_a\left(p_1^{a_1}\cdots p_\kappa^{a_\kappa}\right)=\sigma_a\left(p_1^{a_1}\right)\sigma_a\left(p_2^{a_2}\right)\cdots\sigma_a\left(p_\kappa^{a_\kappa}\right).$$

ΠΑΡΑΔΕΙΓΜΑΤΑ

- $\sigma_1(60)=\sigma_1\left(2^2\cdot3\cdot5\right)=\frac{2^3-1}{2-1}\cdot\frac{3^2-1}{3-1}\cdot\frac{5^2-1}{5-1}=168$
- $\sigma_1(120)=\sigma_1\left(2^3\cdot3\cdot5\right)=\frac{2^4-1}{2-1}\cdot\frac{3^2-1}{3-1}\cdot\frac{5^2-1}{5-1}=360$
- $\sigma_1(3528)=\sigma_1\left(2^3\cdot3^2\cdot7^2\right)=\frac{2^4-1}{2-1}\cdot\frac{3^3-1}{3-1}\cdot\frac{7^3-1}{7-1}=11115$.

3. Τέλειοι αριθμοί, αριθμοί Fermat

Τέλειοι Αριθμοί

Ένας θετικός ακέραιος αριθμός n ονομάζεται **τέλειος** (perfect number) όταν ο αριθμός αυτός είναι **ίσος με το άθροισμα των διαιρετών του χωρίς φυσικά να συμπεριλαμβάνουμε τον n στην άθροιση.**

Με σύμβολα μπορούμε να γράψουμε πως ο n είναι τέλειος αριθμός αν και μόνον αν ισχύει

$$\sigma_1(n)=2n\,.$$

Ο πρώτος τέλειος αριθμός είναι ο 6 διότι 6=1+2+3. Ο δεύτερος τέλειος αριθμός είναι ο 28, διότι 28=1+2+4+7+14, κ.λ.π.

Η έρευνα για τους τέλειους αριθμούς ξεκίνησε από τα αρχαία χρόνια και ειδικότερα από τους αρχαίους Έλληνες, αφού ο Ευκλείδης στα *Στοιχεία* παρουσίασε ένα από τα βασικότερα θεωρήματα που αφορούν τους τέλειους αριθμούς.

Θεώρημα *(ΘΕΩΡΗΜΑ ΤΟΥ ΕΥΚΛΕΙΔΗ)*

Για οποιονδήποτε φυσικό αριθμό n για τον οποίο ο αριθμός 2^n-1 είναι πρώτος, ο $2^{n-1}\left(2^n-1\right)$ είναι τέλειος αριθμός.

ΑΠΟΔΕΙΞΗ

Αρκεί να αποδείξουμε ότι $\sigma_1\left(2^{n-1}(2^n-1)\right)=2^n\left(2^n-1\right)$. Γι' αυτό το σκοπό είναι αρκετό να προσδιορίσουμε τους διαιρέτες του αριθμού $2^{n-1}\cdot p$, όπου $p=2^n-1$.

Οι διαιρέτες του αριθμού αυτού είναι οι ακέραιοι

$$1,2,\ 2^2,\ \ldots,2^{n-1},p,2p,2^2p,\ldots,2^{n-1}p\,.$$

Συνεπώς

$$\begin{aligned}\sigma_1\left(2^{n-1}p\right)&=1+2+2^2+\cdots+2^{n-1}+p+2p+2^2p+\ldots+2^{n-1}p\\&=(p+1)\left(1+2+2^2+\ldots+2^{n-1}\right)\\&=(p+1)\left(2^n-1\right)\\&=2^n\left(2^n-1\right).\end{aligned}$$

δηλαδή

$$\sigma_1\left(2^{n-1}p\right)=2^n\left(2^n-1\right).$$

Αυτό, ολοκληρώνει την απόδειξη του θεωρήματος.

■

Θεώρημα *(ΘΕΩΡΗΜΑ ΤΟΥ EULER)*

Κάθε άρτιος τέλειος αριθμός μπορεί να αναπαρασταθεί στην μορφή $2^{n-1}\left(2^n-1\right)$ όταν $n\in\mathbb{N}$, όπου 2^n-1 είναι πρώτος αριθμός.

ΑΠΟΔΕΙΞΗ

Έστω κ ένας τέλειος αριθμός.

Τότε ισχύει

$$\sigma_1(\kappa)=2\kappa\,.$$

Υποθέτουμε ότι ο φυσικός αριθμός $n-1$ είναι η μεγαλύτερη δύναμη του 2 που διαιρεί τον αριθμό κ. Συνεπώς

$\kappa=2^{n-1}\lambda$, όπου λ ένας περιττός ακέραιος αριθμός.

Έτσι

$$\begin{aligned}2\kappa=\sigma_1(\kappa)&=\sigma_1\left(2^{n-1}\lambda\right)\\&=\sigma_1\left(2^{n-1}\right)\sigma_1(\lambda),\end{aligned}$$

αφού οι ακέραιοι 2^{n-1} και λ είναι πρώτοι μεταξύ τους.

Όμως,

$$\sigma_1\left(p^{\kappa}\right)=\frac{p^{\kappa+1}-1}{p-1},$$

αν p είναι ένας πρώτος αριθμός,

επομένως

$$2\kappa=\left(2^n-1\right)\sigma_1(\lambda)$$

ή

$$2^n\lambda=\left(2^n-1\right)\sigma_1(\lambda) \qquad (1)$$

ή

$$\frac{\lambda}{\sigma_1(\lambda)}=\frac{2^n-1}{2^n}\ .$$

Προφανώς, το κλάσμα $\dfrac{2^n-1}{2^n}$ είναι ανάγωγο, αφού $\left(2^n-1,2^n\right)=1$.

Συνεπώς $\lambda=m\left(2^n-1\right)$ και $\sigma_1(\lambda)=m2^n$, για κάποιον αριθμό $m\in\mathbb{N}$. Θα αποδείξουμε ότι $m=1$.

Υποθέτουμε ότι $m\neq 1$, τότε

$$\sigma_1(\lambda)\geq\lambda+m+1,$$

καθώς ο λ θα έχει τουλάχιστον τους ακεραίους $\lambda, m, 1$ ως διαιρέτες.

Δηλαδή

$$\sigma_1(\lambda)\geq m\left(2^n-1\right)+m+1=2^n m+1>\sigma_1(\lambda),$$

αφού $\sigma_1(\lambda)=m2^n$. Άτοπο.

Έτσι, ισχύει ότι $m=1$ και συνεπώς $\lambda=2^n-1$ και επειδή $\kappa=2^{n-1}\lambda$ λαμβάνουμε ότι

$$\kappa=2^{n-1}\left(2^n-1\right).$$

Αρκεί να αποδείξουμε, ότι ο 2^n-1 είναι πρώτος αριθμός.

Από την σχέση (1) προκύπτει ότι

$$\left(2^n-1\right)\sigma_1\left(2^n-1\right)=2^n\left(2^n-1\right)$$

ή

$$\sigma_1\left(2^n-1\right)=2^n=\left(2^n-1\right)+1.$$

Επομένως, οι μοναδικοί διαιρέτες του 2^n-1 είναι ο εαυτός του και η μονάδα. Συνεπώς, ο θετικός ακέραιος 2^n-1 είναι πρώτος αριθμός. Αυτό, ολοκληρώνει την απόδειξη του θεωρήματος.

■

Ανοιχτά Προβλήματα

- Παρατηρούμε ότι το θεώρημα του Euler αναφέρεται μόνο σε άρτιους τέλειους αριθμούς και έτσι γεννάται το **ερώτημα**: «*Υπάρχουν περιττοί τέλειοι αριθμοί;*»

Το παραπάνω ερώτημα είναι ένα από τα αρχαιότερα ανοιχτά προβλήματα της Θεωρίας Αριθμών και ίσως των Μαθηματικών.

Οι R. Brent, G. Cohen και H. te Riele στην εργασία τους: *Improved techniques for lower bounds for odd perfect numbers, Math. Comp., 61(1993), 857 – 868,* απέδειξαν πως αν υπάρχουν περιττοί τέλειοι αριθμοί *n*, τότε πρέπει να ισχύει

$$n>10^{300}.$$

- Ένα ακόμη πολύ σπουδαίο **ανοιχτό πρόβλημα** που αφορά τους τέλειους αριθμούς είναι το εξής:

«Είναι οι άρτιοι τέλειοι αριθμοί άπειροι το πλήθος;»

Σημειώνουμε ότι στα δύο προηγούμενα θεωρήματα αναφερθήκαμε στον αριθμό 2^n-1 στην περίπτωση που αυτός είναι πρώτος αριθμός.

Τούς πρώτους αριθμούς αυτής της μορφής τους μελέτησε ο Marin Mersenne και γι' αυτό ονομάζονται *πρώτοι του Mersenne.*

Ο Mersenne διατηρούσε αλληλογραφία με τον Pierre de Fermat (1601 – 1665). Έτσι ο Fermat εξετάζοντας τους πρώτους αριθμούς της μορφής 2^n-1 κατέληξε σ' αυτό το θεώρημα που είναι γνωστό ως **«Μικρό Θεώρημα του Fermat»**.

- Το έτος 1644 ο Mersenne διατύπωσε την **εικασία** ότι ο ακέραιος αριθμός M_p, όπου

$$M_p=2^p-1$$

είναι πρώτος για $p=2,3,5,7,13,17,19,31,67,127,257$ και σύνθετος αριθμός για τους υπόλοιπους πρώτους οι οποίοι είναι μικρότεροι του αριθμού 257.

Αυτό όμως δεν ισχύει. Το πρώτο αντιπαράδειγμα στην εικασία του Mersenne δόθηκε το έτος 1886 από τους Pervusin και Seelhoff οι οποίοι απέδειξαν ότι για $p=61$, ο ακέραιος 2^p-1 είναι πρώτος.

Αριθμοί Fermat

Ως **αριθμούς Fermat** ορίζουμε τους αριθμούς F_n που εκφράζονται από τον ακόλουθο τύπο:

$$F_n=2^{2^n}+1, \quad \text{όπου} \quad n=0,1,2,...$$

Συνεπώς, ισχύει ότι:

$$F_0=3, \quad F_1=5, \quad F_2=17, \quad F_3=257, \quad F_4=65537.$$

Ο Fermat υπέθεσε πως όλοι οι αριθμοί της μορφής

$$2^{2^n}+1$$

είναι πρώτοι. Όμως ο Leonhard Euler (1707 – 1783) απέδειξε το έτος 1732 πως ο ακέραιος

$$F_5 = 2^{2^5}+1$$

είναι σύνθετος αριθμός.
(Η απόδειξη του Euler παρουσιάζεται στη συνέχεια της εργασίας).

ΧΑΡΑΚΤΗΡΙΣΤΙΚΕΣ ΙΔΙΟΤΗΤΕΣ

1) ***Να δειχθεί ότι για τους αριθμούς Fermat ισχύει ότι:***

$$\boldsymbol{F_m - 2 = F_0F_1\cdots F_{m-1}} \text{ } \boldsymbol{\text{για } m \geq 1} \text{ με } \boldsymbol{m \in \mathbb{Z}}.$$

ΑΠΟΔΕΙΞΗ

• Για m=1 λαμβάνουμε ότι

$$F_1 - 2 = F_0 \Leftrightarrow F_0 = 3,$$

το οποίο ισχύει.

• Υποθέτουμε πως για κάποιο $\kappa \in \mathbb{Z}$ με $\kappa > 1$ ισχύει ότι

$$F_\kappa - 2 = F_0F_1\cdots F_{\kappa-1}.$$

• Αρκεί να δείξουμε ότι

$$F_{\kappa+1} - 2 = F_0F_1\cdots F_\kappa.$$

Όμως

$$\left(F_0F_1\cdots F_{\kappa-1}\right)F_\kappa = \left(F_\kappa - 2\right)F_\kappa = (2^{2^\kappa}-1)(2^{2^\kappa}+1)$$

$$\Leftrightarrow F_0F_1\cdots F_\kappa = \left(2^{2^\kappa}\right)^2 - 1 = 2^{2^\kappa}\cdot 2^{2^\kappa} - 1 = 2^{2\cdot 2^\kappa} - 1 = 2^{2^{\kappa+1}} - 1$$

$$\Leftrightarrow F_0F_1\cdots F_\kappa = F_{\kappa+1} - 2.$$

Άρα, σύμφωνα με την Αρχή της Μαθηματικής Επαγωγής αποδείχθηκε η ζητούμενη ιδιότητα. ■

2) ***Να δειχθεί ότι για τους αριθμούς Fermat F_n, όπου $F_n = 2^{2^n}+1$ ισχύει ότι $F_n \mid 2^{F_n} - 2$, όπου $n = 0,1,2,\ldots$.***

ΑΠΟΔΕΙΞΗ

Από την παραπάνω ιδιότητα έχουμε:

$$F_m - 2 = F_0F_1\ldots F_{m-1}.$$

Θεωρούμε ότι $m > n$. Τότε ο F_n είναι ένας από τους αριθμούς $F_0, F_1, \ldots, F_{m-1}$.

• Ισχύει ότι

$$2^n \geq n+1.$$

Πράγματι

Για n=1 , $2 \geq 2$, που ισχύει.

Έστω ότι $2^n \geq n+1$ για τυχαίο θετικό ακέραιοαριθμό n. Αρκεί να δείξουμε ότι

$$2^{n+1} \geq n+2 .$$

Όμως

$$2 \cdot 2^n \geq 2(n+1) = 2n+2 \geq n+2 \Leftrightarrow 2^{n+1} \geq n+2 .$$

Συνεπώς σύμφωνα με την Αρχή της Μαθηματικής Επαγωγής ισχύει η σχέση

$$2^n \geq n+1 .$$

• Επομένως, μπορούμε να θέσουμε όπου m το 2^n, με το F_n να είναι πάλι ένας από τους αριθμούς

$$F_0, F_1, \cdots, F_{m-1} .$$

Τότε λαμβάνουμε ότι:

$$F_{2^n} - 2 = F_0 \cdot F_1 \cdots F_{2^n-1} .$$

Επομένως

$$F_n \mid F_{2^n} - 2 .$$

Όμως

$$F_{2^n} = 2^{2^{2^n}} + 1 = 2^{F_n - 1} + 1$$

΄Αρα

$$F_n \mid \left(2^{F_n - 1} - 1\right)$$

΄και συνεπώς

$$F_n \mid 2\left(2^{F_n - 1} - 1\right), \text{äçëî.}\ F_n \mid \left(2^{F_n} - 2\right).$$

■

Σχόλιο

Ο G. Pólya (1887 –1985) αξιοποίησε την πρώτη χαρακτηριστική ιδιότητα για να δώσει μια άλλη απόδειξη του γεγονότος ότι το πλήθος των πρώτων αριθμών είναι άπειρο.

3) ***Να δειχθεί ότι οι πρώτοι αριθμοί είναι άπειροι στο πλήθος.***

ΑΠΟΔΕΙΞΗ

Ο G. Pólya σκέφτηκε πως για να αποδείξει ότι οι πρώτοι αριθμοί είναι άπειροι στο πλήθος αρκεί να βρει μια άπειρη ακολουθία φυσικών αριθμών οι οποίοι να είναι ανά δύο πρώτοι μεταξύ τους. Τότε, αν ο πρώτος αριθμός p_κ διαιρεί τον κ–οστό όρο της ακολουθίας (α_κ), δεν θα μπορεί να διαιρεί κανέναν άλλο όρο της ακολουθίας. Επομένως, τους όρους $a_{\kappa+1}, a_{\kappa+2}, \ldots$ θα τους διαιρούν άλλοι πρώτοι αριθμοί που είναι διάφοροι του p_κ και διακεκριμένοι μεταξύ τους.

Όμως, οι όροι της ακολουθίας είναι άπειροι στο πλήθος, άρα και οι διαφορετικοί μεταξύ τους πρώτοι αριθμοί είναι άπειροι στο πλήθος.

Θα δείξουμε πως μια τέτοια ακολουθία δημιουργείται από τους αριθμούς Fermat.

Έστω ότι οι αριθμοί Fermat δεν είναι ανά δύο πρώτοι μεταξύ τους. Τότε υπάρχει πρώτος αριθμός p τέτοιος ώστε:

$$p \mid F_m, \quad p \mid F_n \text{ , για } n < m .$$

Λόγω της πρώτης ιδιότητας λαμβάνουμε ότι

$$F_n \mid F_m - 2 \Rightarrow p \mid F_m - 2.$$

Άρα

$$p \mid F_m \text{ και } p \mid F_m - 2 .$$

Συνεπώς

$$p \mid F_m - (F_m - 2) \Rightarrow p \mid 2 \Rightarrow p = 2 .$$

Άτοπο, διότι οι αριθμοί Fermat είναι περιττοί και συνεπώς δεν διαιρούνται από το 2.

Σύμφωνα με τα παραπάνω προκύπτει πως οι πρώτοι αριθμοί είναι άπειροι στο πλήθος.

■

Όπως έχει προαναφερθεί, ο Euler απέδειξε το έτος 1732 ότι ο αριθμός Fermat

$$F_5 = 2^{2^5} + 1$$

δεν είναι πρώτος. Είναι πραγματικά εντυπωσιακό το γεγονός ότι ο Euler έκανε την απόδειξη αυτή παρόλο που ήταν πλέον τελείως τυφλός.

Η απόδειξή του είναι η ακόλουθη:

$$F_5 = 2^{2^5} + 1 = 641 \cdot 6700417$$

που είναι σύνθετος αριθμός. Βέβαια, για να αποδείξει ο Euler ότι ο F_5 είναι σύνθετος αριθμός δεν παρέθεσε απλώς το παραπάνω γινόμενο. Απέδειξε το γεγονός ότι ο αριθμός 641 διαιρεί τον F_5.

Αυτό ισχύει διότι

$$\begin{aligned} 641 &= 5^4 + 2^4 = 5 \cdot 5^3 + 16 = 5 \cdot 125 + 15 + 1 \\ &= 5(125 + 3) + 1 = 5 \cdot 128 + 1 = 5 \cdot 2^7 + 1, \end{aligned}$$

δηλαδή

$$641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1. \tag{1}$$

Όμως , αληθεύει ότι

$$\begin{aligned} \left(5^4 + 2^4\right)\left(2^7\right)^4 &= 5^4\left(2^7\right)^4 + 2^4\left(2^7\right)^4 = \left(5 \cdot 2^7\right)^4 + \left(2 \cdot 2^7\right)^4 \\ &= 5^4 \cdot 2^{28} + 2^{32}, \end{aligned}$$

δηλαδή

$$641 \mid 5^4 \cdot 2^{28} + 2^{32}$$

λόγω της (1).

Επίσης, ισχύει ότι $5^4 \cdot 2^{28} - 1 = 5^2 \cdot 2^{14} \cdot 5^2 \cdot 2^{14} - 1$

$$\begin{aligned} &= \left(5^2 \cdot 2^{14}\right)^2 - 1 \\ &= \left(5^2 \cdot 2^{14} - 1\right)\left(5^2 \cdot 2^{14} + 1\right) \\ &= \left(5 \cdot 2^7 - 1\right)\left(5 \cdot 2^7 + 1\right)\left(5^2 \cdot 2^{14} + 1\right) \end{aligned}$$

Οπότε, προκύπτει ότι

$$641 \mid 5^4 \cdot 2^{28} - 1 \quad \text{λόγω της (1).}$$

Συνεπώς

$$641 \mid \left(5^4 \cdot 2^{28} + 2^{32}\right) - \left(5^4 \cdot 2^{28} - 1\right)$$

ή

$$641 \mid 2^{32} + 1,$$

δηλαδή

$$641 \mid 2^{2^5} + 1, \text{ όπου } 2^{2^5} + 1 = F_5.$$

Άρα

$$641 \mid F_5,$$

που σημαίνει ότι ο F_5 δεν μπορεί να είναι πρώτος αριθμός.

■

Σχόλιο

Είναι σημαντικό να αναφέρουμε ότι 148 χρόνια μετά τον Euler, ο Landau απέδειξε ότι ούτε ο F_6 είναι πρώτος αριθμός. Από τότε, έχουν βρεθεί πολλοί αριθμοί Fermat οι οποίοι είναι σύνθετοι, αντιβαίνοντας στην εικασία του Fermat ότι όλοι οι ακέραιοι της μορφής

$$2^{2^n} + 1$$

είναι πρώτοι για κάθε $n \in \mathbb{N}$.

4. Ισοδυναμίες (ή Ισοτιμίες)

Ορισμός

Δύο ακέραιοι αριθμοί *a, b* λέγονται **ισοδύναμοι** ή **ισότιμοι** (ή **ισοϋπόλοιποι**) **modulo** ***m***, όπου *m* ένας ακέραιος αριθμός, αν ο *m* διαιρεί τη διαφορά $a-b$ και συμβολίζουμε

$$a \equiv b \,(\mathrm{mod}\, m).$$

Στην περίπτωση όπου η διαφορά $a-b$ δεν διαιρείται με τον *m*, τότε συμβολίζουμε

$$a \not\equiv b \,(\mathrm{mod}\, m).$$

Θεώρημα *(ΤΟ ΜΙΚΡΟ ΘΕΩΡΗΜΑ ΤΟΥ FERMAT)*

Αν p *είναι ένας πρώτος αριθμός και* $a \in \mathbb{Z}$ *με* $(a, p)=1$*, τότε* $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

ΑΠΟΔΕΙΞΗ

Αρχικά, θα αποδείξουμε ότι $a^p \equiv a \bmod p$. Στη συνέχεια, χρησιμοποιώντας την ιδιότητα $(a, p)=1$ θα καταλήξουμε στο επιθυμητό αποτέλεσμα.

– Θεωρούμε πρώτα την περίπτωση όπου $a \in \mathbb{N}$. Τότε, για $a=1$ ισχύει ότι $a^p \equiv a (\mathrm{mod}\, p)$ για οποιονδήποτε πρώτο αριθμό p.

Υποθέτουμε ότι η σχέση $a^p \equiv a (\mathrm{mod}\, p)$ ικανοποιείται και θα αποδείξουμε ότι $(a+1)^p \equiv (a+1) (\mathrm{mod}\, p)$.

Από το διώνυμο του Νεύτωνα έχουμε

$$(a+1)^p = \binom{p}{0} a^p + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a + \binom{p}{p}$$

$$= a^p + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a + 1.$$

Όμως, ο p διαιρεί καθέναν από τους ακεραίους

$$\binom{p}{1}, \binom{p}{2}, \ \cdots \ , \binom{p}{p-1}.$$

Συνεπώς, από την παραπάνω σχέση προκύπτει ότι

$$(a+1)^p \equiv a^p + 1 (\mathrm{mod}\, p). \qquad (1)$$

Αλλά, γνωρίζουμε ότι $a^p \equiv a (\mathrm{mod}\, p)$. Έτσι, η σχέση (1) γίνεται

$$(a+1)^p \equiv a + 1 (\mathrm{mod}\, p).$$

Επομένως, σύμφωνα με την Αρχή της Μαθηματικής επαγωγής αποδείξαμε πως $a^p \equiv a (\mathrm{mod}\, p)$, για $a \in \mathbb{N}$.

– Θα αποδείξουμε την ίδια σχέση στην περίπτωση όπου $a \in \mathbb{Z}$, με $a \le 0$.

Για $a=0$, είναι προφανές ότι $a^p \equiv a(\mathrm{mod}\, p)$.

Για $a<0$, έχουμε:

- Αν $p=2$, τότε $a^2=(-a)^2 \equiv (-a)(\mathrm{mod}\, 2)$ καθώς $-a \in \mathbb{N}$. Δηλαδή, $2 \mid a^2+a$. Όμως, $2 \mid 2a$ και συνεπώς $2 \mid a^2+a-2a$. Άρα, $2 \mid a^2-a$. Επομένως, $a^2 \equiv a(\mathrm{mod}\, 2)$.

- Αν $p \neq 2$, δηλαδή ο p είναι περιττός, προκύπτει
  $a^p = -(-a)^p \equiv -(-a)(\mathrm{mod}\, p)$ καθώς $-a \in \mathbb{N}$.
  Έτσι, $a^p \equiv a(\mathrm{mod}\, p)$.

  Αφού δείξαμε ότι $a^p \equiv a(\mathrm{mod}\, p)$, για κάθε $a \in \mathbb{Z}$, θα προχωρήσουμε στην απόδειξη του θεωρήματος.

  Ισχύει ότι $p \mid a^p - a$, δηλαδή $p \mid a(a^{p-1}-1)$.

  Όμως, $(a,p)=1$. Άρα, ο p αναγκαστικά διαιρεί τον ακέραιο $a^{p-1}-1$. Συνεπώς $a^{p-1} \equiv 1(\mathrm{mod}\, p)$.

■

Θεώρημα *(ΤΟ ΘΕΩΡΗΜΑ FERMAT – EULER)*
Αν $a, m \in \mathbb{Z}$ *και* $(a,m)=1$, *τότε*

$$a^{\phi(m)} \equiv 1(\mathrm{mod}\, m)$$

(όπου $\phi(m)$ *είναι η συνάρτηση του Euler).*

ΑΠΟΔΕΙΞΗ

Θα αποδείξουμε, αρχικά, το θεώρημα στη περίπτωση όπου ο ακέραιος αριθμός m είναι τέλεια δύναμη ενός πρώτου αριθμού. Έστω, λοιπόν, ότι $m=p^\kappa$, όπου p πρώτος αριθμός και $\kappa \in \mathbb{N}$. Για $\kappa=1$, ισχύει

$$a^{\phi(p)} = a^{p-1} \equiv 1(\mathrm{mod}\, p),$$

δηλαδή

$$a^{\phi(m)} \equiv 1(\mathrm{mod}\, m).$$

Παρατηρούμε, δηλαδή, πως για $\kappa=1$ έχουμε ακριβώς το Μικρό Θεώρημα του Fermat. Υποθέτουμε πως ισχύει ότι

$$a^{\phi(p^\kappa)} \equiv 1(\mathrm{mod}\, p^\kappa)$$

και θα δείξουμε πως

$$a^{\phi(p^{\kappa+1})} \equiv 1(\mathrm{mod}\, p^{\kappa+1}).$$

Έτσι, λαμβάνουμε

$$a^{\phi(p^\kappa)} - 1 = \lambda p^\kappa, \text{ για κάποιο } \lambda \in \mathbb{Z}$$

ή

$$a^{p^\kappa - p^{\kappa-1}} = 1 + \lambda p^\kappa$$

ή $$a^{p^{\kappa+1}-p^{\kappa}} = \left(1+\lambda p^{\kappa}\right)^{p}$$

ή $$a^{\phi\left(p^{\kappa+1}\right)} = \left(1+\lambda p^{\kappa}\right)^{p}. \qquad (1)$$

Όμως,

$$\left(1+\lambda p^{\kappa}\right)^{p} = 1+\binom{p}{1}\lambda p^{\kappa}+\cdots+\binom{p}{p-1}\left(\lambda p^{\kappa}\right)^{p-1}+\left(\lambda p^{\kappa}\right)^{p}.$$

Αλλά, ο πρώτος αριθμός p διαιρεί καθέναν από τους ακεραίους αριθμούς

$$\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}.$$

Άρα,

$$\left(1+\lambda p^{\kappa}\right)^{p} = 1+\lambda' p^{\kappa+1}, \text{ για κάποιο } \lambda' \in \mathbb{Z}.$$

Συνεπώς, από την σχέση (1) λαμβάνουμε ότι:

$$a^{\phi\left(p^{\kappa+1}\right)} = 1+\lambda' p^{\kappa+1},$$

δηλαδή

$$a^{\phi\left(p^{\kappa+1}\right)} \equiv 1\left(\mathrm{mod}\ p^{\kappa+1}\right).$$

Επομένως, για κάθε $\kappa \in \mathbb{N}$ ισχύει ότι

$$a^{\phi\left(p^{\kappa}\right)} \equiv 1\left(\mathrm{mod}\ p^{\kappa}\right).$$

Από το θεμελιώδες θεώρημα της Αριθμητικής θα έχουμε ότι

$$m = p_1^{\kappa_1} p_2^{\kappa_2} \ldots p_n^{\kappa_n}, \text{ όπου } n \in \mathbb{N},$$

ενώ γνωρίζουμε, επίσης, πως η συνάρτηση ϕ είναι πολλαπλασιαστική για ακεραίους που είναι ανά δύο πρώτοι μεταξύ τους.

Συνεπώς, σύμφωνα με τα παραπάνω θα ισχύει

$$\left(\left(\left(a^{\phi\left(p_1^{\kappa_1}\right)}\right)^{\phi\left(p_2^{\kappa_2}\right)}\right)^{\cdot^{\cdot}}\right)^{\phi\left(p_n^{\kappa_n}\right)} \equiv \left(\left(\left(1^{\phi\left(p_1^{\kappa_1}\right)}\right)^{\phi\left(p_2^{\kappa_2}\right)}\right)^{\cdot^{\cdot}}\right)^{\phi\left(p_n^{\kappa_n}\right)} \left(\mathrm{mod}\ p_1^{\kappa_1}\right)$$

ή

$$a^{\phi\left(p_1^{\kappa_1} p_2^{\kappa_2} \ldots p_n^{\kappa_n}\right)} \equiv 1\left(\mathrm{mod}\ p_1^{\kappa_1}\right)$$

ή

$$a^{\phi(m)} \equiv 1\left(\mathrm{mod}\ p_1^{\kappa_1}\right).$$

Ομοίως, έχουμε

$$a^{\phi(m)} \equiv 1\left(\mathrm{mod}\ p_2^{\kappa_2}\right), \ldots, a^{\phi(m)} \equiv 1\left(\mathrm{mod}\ p_n^{\kappa_n}\right).$$

Ακολούθως, γνωρίζουμε πως αν $a \mid c$ και $b \mid c$ με $(a,b)=1$, τότε $ab \mid c$. Έτσι, εφαρμόζοντας αυτήν την ιδιότητα στην παραπάνω περίπτωση, λαμβάνουμε

$$p_1^{\kappa_1} \mid a^{\phi(m)}-1,\ p_2^{\kappa_2} \mid a^{\phi(m)}-1,\ \ldots,\ p_n^{\kappa_n} \mid a^{\phi(m)}-1$$

με

$$\left(p_1^{\kappa_1}, p_2^{\kappa_2}, \ \dots \ , p_n^{\kappa_n}\right) = 1 .$$

Άρα, $$p_1^{\kappa_1} \cdot p_2^{\kappa_2} \cdot \ \cdots \cdot p_n^{\kappa_n} \mid a^{\varphi(m)} - 1 ,$$

δηλαδή $$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$$

■

> ***Παρατήρηση***
> *Το θεώρημα Fermat–Euler απέδειξε ο Leonhard Euler το έτος 1758. Το θεώρημα αυτό αποτελεί γενίκευση του Μικρού Θεωρήματος του Fermat .*

Θεώρημα

Έστω οι ακέραιοι αριθμοί a, b, c *με τουλάχιστον έναν από τους* α, b *διάφορο του μηδενός.*

Αν $d = (a,b)$ *και* $d \mid c$, *τότε η διοφαντική εξίσωση*

$$ax + by = c$$

έχει άπειρες λύσεις της μορφής

$$x = x_0 + \frac{b}{d} n \ , \ y = y_0 - \frac{a}{d} n \ , \ \ n \in \mathbb{Z}$$

όπου (x_0, y_0) *είναι μία λύση της εξίσωσης αυτής.*

Στην περίπτωση όπου $d \nmid c$, *η διοφαντική εξίσωση*

$$ax + by = c$$

δεν έχει λύσεις.

ΑΠΟΔΕΙΞΗ

- Αν $d \mid c$, τότε είναι $c = \kappa d$, για κάποιον ακέραιο αριθμό κ .

Όμως, λόγω του γεγονότος ότι ο d έχει την ιδιότητα να είναι ο μέγιστος κοινός διαιρέτης των a, b, θα υπάρχουν ακέραιοι κ_1, κ_2 τέτοιοι ώστε

$$d = \kappa_1 a + \kappa_2 b .$$

Άρα

$$c = \kappa\kappa_1 a + \kappa\kappa_2 b .$$

Επομένως, μία λύση της διοφαντικής εξίσωσης είναι η $x_0 = \kappa\kappa_1, y_0 = \kappa\kappa_2$. Δείξαμε, λοιπόν, την ύπαρξη μιας τουλάχιστον λύσης της διοφαντικής εξίσωσης.

Για να αποδείξουμε πως υπάρχουν άπειρες λύσεις της διοφαντικής εξίσωσης και μάλιστα της μορφής

$$x = x_0 + \frac{b}{d} n, \ \ y = y_0 - \frac{a}{d} n$$

θεωρούμε ότι η (x, y) είναι μία τυχαία λύση της διοφαντικής εξίσωσης.

Τότε ισχύει

$$ax + by = c$$
$$ax_0 + by_0 = c\,.$$

Άρα

$$a(x - x_0) + b(y - y_0) = 0$$
$$\Leftrightarrow a(x - x_0) = b(y_0 - y)$$

$$\Leftrightarrow \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y) \qquad (1)$$

Δηλαδή

$$\frac{b}{d} \Big| \frac{a}{d}(x - x_0),$$

όμως

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1\,,$$

άρα

$$\frac{b}{d} \Big| (x - x_0).$$

Συνεπώς, υπάρχει $n \in \mathbb{Z}$ τέτοιος, ώστε

$$x = x_0 + n\ \frac{b}{d}\cdot$$

Θεωρούμε, χωρίς βλάβη της γενικότητας, ότι $b \neq 0$. Τότε, από την σχέση (1) λαμβάνουμε ότι

$$\frac{a}{d} \cdot n\frac{b}{d} = \frac{b}{d}(y_0 - y)$$
$$\Rightarrow \frac{a}{d} \cdot n = y_0 - y$$

$$\Rightarrow y = y_0 - \frac{a}{d}n\,.$$

Αν θεωρήσουμε πως $a \neq 0$, εκτελούμε ακριβώς την ίδια διαδικασία και καταλήγουμε στην ίδια λύση.

Άρα, για κάποιον συγκεκριμένο ακέραιο αριθμό n προκύπτει ότι η

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n$$

είναι λύση της διοφαντικής εξίσωσης $ax + by = c$. Όμως, αν θεωρήσουμε έναν τυχαίο ακέραιο αριθμό *t,* τότε για

$$x = x_0 + \frac{b}{d}t \ \text{ και } \ y = y_0 - \frac{a}{d}t$$

λαμβάνουμε ότι

$$c = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right)$$

$$= ax_0 + \frac{ab}{d}t + by_0 - \frac{ba}{d}t$$

$$= ax_0 + by_0,$$

που ισχύει

Συνεπώς, η διοφαντική εξίσωση $ax + by = c$ έχει άπειρες λύσεις οι οποίες εκφράζονται στην μορφή

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n, \text{ για } n \in \mathbb{Z}.$$

- Αν $d \nmid c$, τότε προκύπτει:

$$d \mid a \text{ και } d \mid b.$$

Άρα

$$d \mid (ax + by).$$

Δηλαδή $d \mid c$. Άτοπο.

Συνεπώς, στην περίπτωση αυτή, η διοφαντική εξίσωση

$$ax + by = c$$

δεν δέχεται καμία λύση.

■

Θεώρημα

Έστω οι ακέραιοι αριθμοί a,b και ο φυσικός αριθμός m. Αν $d = (a,m)$ και $d \mid b$, τότε η γραμμική ισοδυναμία

$$ax \equiv b(\mathrm{mod}\, m)$$

έχει d, ανά δύο διαφορετικές μεταξύ τους, λύσεις modulo m.

Στην περίπτωση όπου $d \nmid b$, η γραμμική ισοδυναμία δεν έχει λύσεις.

Παρατήρηση: Οι λύσεις x_1, x_2 θεωρούνται διαφορετικές, αν $x_1 \not\equiv x_2 (\mathrm{mod}\, m)$.

ΑΠΟΔΕΙΞΗ

- Αν $d \mid b$ τότε, για να έχει η γραμμική ισοδυναμία $ax \equiv b(\mathrm{mod}\, m)$ λύση πρέπει , ισοδύναμα, η διοφαντική εξίσωση

$$ax - my = b$$

να έχει λύση.

Η διοφαντική εξίσωση $ax - my = b$ δέχεται άπειρες λύσεις με

$$x = x_0 - \frac{m}{d}n,$$

όπου (x_0, y_0) είναι μια λύση της $ax - my = b$.

Θα αποδείξουμε πως από την απειρία των λύσεων της γραμμικής ισοδυναμίας

$$ax \equiv b(\mathrm{mod}\, m),$$

μόνο d λύσεις είναι ανά δύο διαφορετικές μεταξύ τους.

Παρατηρούμε πως οι αριθμοί

$$x_0,\ \ x_0 - \frac{m}{d},\ \ x_0 - 2\frac{m}{d}\ ,\ ...,\ \ x_0 - (d-1)\frac{m}{d}$$

είναι όλες λύσεις της γραμμικής ισοδυναμίας $ax \equiv b(\mathrm{mod}\, m)$. Οι λύσεις αυτές είναι ανά δύο διαφορετικές μεταξύ τους καθώς αν

$$x_0 - n_1\frac{m}{d} \equiv x_0 - n_2\frac{m}{d}(\mathrm{mod}\, m)$$

για κάποιους ακεραίους n_1, n_2 με $1 \le n_1, n_2 \le d-1$, τότε

$$n_1\frac{m}{d} \equiv n_2\frac{m}{d}(\mathrm{mod}\, m)$$

δηλαδή

$$m \mid (n_1 - n_2)\frac{m}{d}.$$

Άρα

$$m \mid (n_1 - n_2) \ \text{ ή } \ m \left| \frac{m}{d}. \right.$$

Όμως, είναι προφανές ότι $m \nmid \frac{m}{d}$. Συνεπώς, πρέπει να ισχύει ότι

$$m \mid (n_1 - n_2).$$

Αλλά $d \mid m$ και έτσι πρέπει

$$d \mid (n_1 - n_2).$$

Άτοπο, καθώς

$$1 \le n_1, n_2 \le d-1.$$

Επομένως, οι λύσεις

$$x_0, x_0 - \frac{m}{d}, x_0 - 2\frac{m}{d}, ..., x_0 - (d-1)\frac{m}{d}$$

είναι ανά δύο διαφορετικές μεταξύ τους.

Θα δείξουμε πως δεν μπορούν να υπάρξουν άλλες λύσεις της γραμμικής ισοδυναμίας

$$ax \equiv b(\mathrm{mod}\, m)$$

ώστε όλες οι λύσεις να παραμένουν ανά δύο διαφορετικές μεταξύ τους.

Έστω, λοιπόν, $\kappa \in \mathbb{Z}$ μια διαφορετική λύση.

Τότε, λαμβάνουμε ότι η

$$ax \equiv b(\mathrm{mod}\, m)$$

μπορεί να λάβει την μορφή

$$a\kappa \equiv b(\mathrm{mod}\, m)$$

ενώ γνωρίζουμε ότι $ax_0 \equiv b(\mathrm{mod}\, m)$.

Έτσι

$$a\kappa \equiv ax_0 (\mathrm{mod}\, m). \qquad (1)$$

Όμως, γνωρίζουμε ότι $(a,m)=d$. Συνεπώς, μπορούμε να θέσουμε $a=\lambda_1 d,\ m=\lambda_2 d$, για $\lambda_1,\lambda_2 \in \mathbb{Z}$ με $(\lambda_1,\lambda_2)=1$.

Αντικαθιστώντας στην σχέση (1) προκύπτει:

$$\lambda_1 d\kappa \equiv \lambda_1 dx_0 (\mathrm{mod}\, m),$$

δηλαδή

$$m \mid \lambda_1 d(\kappa - x_0)$$

Αλλά $m=\lambda_2 d$, οπότε προκύπτει ότι

$$\lambda_2 d \mid \lambda_1 d(\kappa - x_0),$$

δηλαδή

$$\lambda_2 \mid \lambda_1 (\kappa - x_0).$$

Όμως, για τους λ_1,λ_2 ισχύει ότι $(\lambda_1,\lambda_2)=1$. Επομένως

$$\lambda_2 \mid (\kappa - x_0).$$

Άρα, υπάρχει ακέραιος αριθμός ν τέτοιος, ώστε:

$$\kappa = x_0 + \nu\lambda_2 .$$

Διαιρώντας τον ακέραιο ν με d , συνεπάγεται

$$\nu = d\pi + \upsilon \text{, όπου } \pi,\upsilon \in \mathbb{Z} \text{ με } 0 \le \upsilon < d .$$

Έτσι

$$\kappa = x_0 + (d\pi + \upsilon)\lambda_2$$

$$\Leftrightarrow \kappa = x_0 + d\lambda_2\pi + \lambda_2\upsilon .$$

$$\Leftrightarrow \kappa = x_0 + m\pi + \frac{m}{d}\upsilon$$

$$\Leftrightarrow m\pi = \kappa - \left(x_0 + \frac{m}{d}\upsilon \right).$$

Δηλαδή,

$$\kappa \equiv x_0 + \frac{m}{d}\upsilon (\mathrm{mod}\, m), \text{ όπου } 0 \le \upsilon \le d-1 .$$

Άρα, η κ δεν αποτελεί διαφορετική λύση. Αυτό ολοκληρώνει την απόδειξη στην περίπτωση όπου $d \mid b$.

- Αν $d \nmid b$, τότε η διοφαντική εξίσωση

$$ax - my = b$$

δεν λαμβάνει καμμία λύση. Άρα και η γραμμική ισοδυναμία

$$ax \equiv b (\mathrm{mod}\, m)$$

δεν θα λαμβάνει καμία λύση.

■

Παρατήρηση:

Στην περίπτωση όπου $(a,m)=1$, *προκύπτει ότι η γραμμική ισοδυναμία* $ax \equiv b(\mathrm{mod}\, m)$ *λαμβάνει μοναδική λύση.*

Θεώρημα *(ΘΕΩΡΗΜΑ ΤΟΥ LAGRANGE)*

Έστω το πολυώνυμο $f(x)=a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, *όπου* $a_0, a_1, \ldots, a_{n-1}, a_n \in \mathbb{Z}$ *και* $a_n \neq 0$. *Αν* p *είναι ένας πρώτος αριθμός και* $a_n \not\equiv 0(\mathrm{mod}\, p)$, *τότε η πολυωνυμική ισοδυναμία*

$$f(x) = 0(\mathrm{mod}\, p)$$

έχει το πολύ n *λύσεις.*

ΑΠΟΔΕΙΞΗ

• Για $n=1$ έχουμε $f(x)=a_1x+a_0$. Η πολυωνυμική ισοδυναμία $a_1x+a_0 \equiv 0(\mathrm{mod}\, p)$ λαμβάνει ακριβώς μία λύση. Έτσι, στην περίπτωση όπου $n=1$, το θεώρημα ικανοποιείται.

• Υποθέτουμε πως ο υσχυρισμός του θεωρήματος ικανοποιείται για πολυώνυμα έως και βαθμού $n-1$.

• Έστω πως η πολυωνυμική ισοδυναμία

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0(\mathrm{mod}\, p)$$

δεν έχει το πολύ n λύσεις, αλλά έχει τουλάχιστον $n+1$ λύσεις

$$x_0, x_1, \ldots, x_n.$$

Τότε

$$\begin{aligned}
&\left(a_n x_i^n + a_{n-1}x_i^{n-1} + \cdots + a_1 x_i + a_0\right) - \left(a_n x_0^n + a_{n-1}x_0^{n-1} + \cdots + a_1 x_0 + a_0\right) \\
&= a_n\left(x_i^n - x_0^n\right) + a_{n-1}\left(x_i^{n-1} - x_0^{n-1}\right) + \cdots + a_1\left(x_i - x_0\right) \\
&= \left(x_i - x_0\right)p\left(x_i\right),\ i=1,2,\ldots,n,
\end{aligned}$$

όπου $p(x)$ είναι ένα πολυώνυμο $n-1$ βαθμού με ακέραιους συντελεστές.

Ισχύει ότι

$$p \mid \left(\alpha_n x_i^n + \cdots + \alpha_1 x_i + \alpha_0\right) \text{ και } p \mid \left(\alpha_n x_0^n + \cdots + \alpha_1 x_0 + \alpha_0\right).$$

Άρα

$$p \mid \left(x_i - x_0\right)p\left(x_i\right),\ i=1,2,\ldots,n.$$

Οι αριθμοί x_i, x_0 είναι διαφορετικές λύσεις. Επομένως, από τον ορισμό της διαφορετικότητας των λύσεων θα είναι

$$x_i \not\equiv x_0(\mathrm{mod}\, p).$$

Επομένως

$$p \mid p\left(x_i\right), i=1,2,\ldots,n.$$

Δηλαδή, για το πολυώνυμο $p(x)$, το οποίο είναι βαθμού $n-1$, λαμβάνουμε n λύσεις της πολυωνυμικής ισοδυναμίας

$$p(x)\equiv 0(\mathrm{mod}\, p).$$

Αυτό είναι αδύνατον, καθώς έχουμε υποθέσει πως το θεώρημα ικανοποιείται για πολυώνυμα έως και βαθμού $n-1$.

Συνεπώς, σύμφωνα με την Αρχή της Μαθηματικής Επαγωγής προκύπτει ότι η πολυωνυμική ισοδυναμία

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0(\mathrm{mod}\, p)$$

έχει το πολύ n λύσεις, όταν $a_n \not\equiv 0(\mathrm{mod}\, p)$.

■

Θεώρημα (συντελεστών πολυωνύμου)

Θεωρούμε το πολυώνυμο $f(x)=a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, *όπου* $a_0, a_1, \ldots, a_{n-1}, a_n \in \mathbb{Z}$ *και* $a_n \neq 0$. *Αν* p *είναι ένας πρώτος αριθμός και η πολυωνυμική ισοδυναμία* $f(x)\equiv 0(\mathrm{mod}\, p)$ *έχει περισσότερες από* n *λύσεις, τότε ο αριθμός* p *διαιρεί καθέναν από τους συντελεστές του πολυωνύμου. Δηλαδή,*

$$p \mid a_0,\ p \mid a_1,\ p \mid a_2,\ \ldots,\ p \mid a_{n-1},\ \text{και}\ \ p \mid a_n .$$

ΑΠΟΔΕΙΞΗ

Λόγω του γεγονότος ότι η πολυωνυμική ισοδυναμία $f(x)\equiv 0(\mathrm{mod}\, p)$ λαμβάνει περισσότερες από n λύσεις, προκύπτει ότι $p \mid a_n$. Αυτό συμβαίνει διότι, αν $a_n \not\equiv 0(\mathrm{mod}\, p)$ τότε, η ισοδυναμία $f(x)\equiv 0(\mathrm{mod}\, p)$ θα είχε το πολύ n λύσεις. Αδύνατον, λόγω της υπόθεσης.

Επομένως, για κάθε λύση x_0 της ισοδυναμίας $f(x)\equiv 0(\mathrm{mod}\, p)$ θα ισχύει αναγκαστικά ότι

$$p \mid a_{n-1}x_0^{n-1} + \cdots + a_1 x_0 + a_0 .$$

Άρα, η πολυωνυμική ισοδυναμία

$$a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0(\mathrm{mod}\, p)$$

έχει περισσότερες από n (και συνεπώς περισσότερες από $n-1$) λύσεις.

Ομοίως, λοιπόν, θα ισχύει ότι $p \mid a_{n-1}$.

Ακολουθώντας αυτήν την διαδικασία προκύπτει ότι για κάθε $\lambda \leq n$ η πολυωνυμική ισοδυναμία

$$a_\lambda x^\lambda + a_{\lambda-1}x^{\lambda-1} + \cdots + a_1 x + a_0 \equiv 0(\mathrm{mod}\, p)$$

έχει περισσότερες από λ λύσεις. Άρα $p \mid a_\lambda$, για κάθε $\lambda = 0,1,2,\ldots,n$.

■

Θεώρημα *(ΚΙΝΕΖΙΚΟ ΘΕΩΡΗΜΑ ΥΠΟΛΟΙΠΩΝ)*

Έστω $m_1, m_2, ..., m_\kappa, a_1, a_2, ..., a_\kappa$ *ακέραιοι αριθμοί τέτοιοι ώστε* $(m_i, m_j) = 1$, *για* $i \neq j$ *και* $(a_i, m_i) = 1$, *για κάθε* i, *όπου* $1 \leq i, j \leq \kappa$.

Αν $m = m_1 m_2 ... m_\kappa$, *τότε το σύστημα των γραμμικών ισοδυναμιών*

$$a_1 x \equiv b_1 (\mathrm{mod}\, m_1)$$
$$a_2 x \equiv b_2 (\mathrm{mod}\, m_2)$$
$$\vdots$$
$$a_\kappa x \equiv b_\kappa (\mathrm{mod}\, m_\kappa)$$

έχει μοναδική λύση modulo m.

ΑΠΟΔΕΙΞΗ

Θα αποδείξουμε πως το σύστημα έχει μια κοινή λύση modulo m και στη συνέχεια, θα αποδείξουμε την μοναδικότητα της λύσης αυτής.

Θέτουμε $r_i = \dfrac{m}{m_i}$. Είναι προφανές ότι $(r_i, m_i) = 1$.

Συνεπώς, η γραμμική ισοδυναμία $r_i x \equiv 1 (\mathrm{mod}\, m_i)$ λαμβάνει μοναδική λύση. Έστω r_i' να είναι η λύση αυτή.

Τότε

$$r_i r_i' \equiv 1 (\mathrm{mod}\, m_i), \text{ για } i = 1,2,...,\kappa .$$

Θα δείξουμε ότι ο ακέραιος αριθμός

$$x_0 = \sum_{i=1}^{\kappa} x_i r_i r_i'$$

όπου x_i είναι η μοναδική λύση $\mathrm{mod}\, m_i$ της γραμμικής ισοδυναμίας $a_i x \equiv b_i (\mathrm{mod}\, m_i)$, για $i = 1,2,...,\kappa$, αποτελεί λύση modulo m του συστήματος.

Ισχύει ότι

$$a_i x_0 = a_i x_1 r_1 r_1' + a_i x_2 r_2 r_2' + \cdots + a_i x_i r_i r_i' \cdots + a_i x_\kappa r_\kappa r_\kappa',$$

για κάθε τιμή του i, όπου $i = 1,2,...,\kappa$.

Όμως, η γραμμική ισοδυναμία $a_i x \equiv b_i (\mathrm{mod}\, m_i)$ λαμβάνει μοναδική λύση καθώς $(a_i, m_i) = 1$. Έστω, λοιπόν, x_i να είναι η αντίστοιχη λύση.

Τότε

$$a_i x_i \equiv b_i (\mathrm{mod}\, m_i)$$

και

$$r_i r_i' \equiv 1 (\mathrm{mod}\, m_i).$$

Επομένως

$$a_i x_i r_i r_i' \equiv b_i (\mathrm{mod}\, m_i). \quad (1)$$

Επίσης, στην περίπτωση όπου $i \neq j$ είναι προφανές ότι $m_i | r_j$.

Συνεπώς, ισχύει ότι

$$m_i \mid a_i x_j r_j r_j', \text{ για κάθε } i \neq j. \tag{2}$$

Αλλά

$$a_i x_0 - b_i = a_i x_1 r_1 r_1' + a_i x_2 r_2 r_2' + \cdots + (a_i x_i r_i r_i' - b_i) + \cdots$$
$$\cdots + a_i x_\kappa r_\kappa r_\kappa', \quad i = 1,2,...,\kappa.$$

Επομένως, από τις σχέσεις (1) και (2) προκύπτει ότι

$$m_i | (a_i x_0 - b_i), \text{ για κάθε } i = 1,2,...,\kappa,$$

δηλαδή $a_i x_0 \equiv b_i (\mathrm{mod}\, m_i)$, για κάθε $i = 1,2,...,\kappa$.

Γνωρίζουμε ότι οι ακέραιοι αριθμοί $m_1, m_2, ..., m_\kappa$ είναι πρώτοι μεταξύ τους. Άρα

$$a_i x_0 \equiv b_i \bmod(m_1 m_2 ... m_\kappa)$$

ή

$$a_i x_0 \equiv b_i (\mathrm{mod}\, m),$$

για κάθε $i = 1,2,...,\kappa$.

Αρκεί, λοιπόν, να δείξουμε πως η κοινή λύση x_0 του συστήματος είναι και μοναδική modulo m. Έστω πως υπάρχει μία ακόμη κοινή λύση του συστήματος modulo m. Αν ονομάσουμε x_0' την λύση αυτή, τότε

$$m | (a_i x_0' - b_i), \text{ για κάθε } i = 1,2,...,\kappa.$$

Άρα, είναι προφανές ότι

$$m_i | (a_i x_0' - b_i), \text{ για κάθε } i = 1,2,...,\kappa.$$

Όμως, $m_i | (a_i x_0 - b_i)$, για κάθε $i = 1,2,..,\kappa$.

Δηλαδή

$$m_i | a_i (x_0' - x_0), \text{ για κάθε } i = 1,2,..,\kappa.$$

Γνωρίζουμε πως $(a_i, m_i) = 1$. Έτσι

$$x_0' \equiv x_0 (\mathrm{mod}\, m_i).$$

Αλλά οι $m_1, m_2, ..., m_\kappa$ είναι πρώτοι μεταξύ τους.

Συνεπώς

$$x_0' \equiv x_0 (\mathrm{mod}\, m).$$

Δηλαδή οι λύσεις x_0', x_0 δεν είναι διαφορετικές μεταξύ τους. Αυτό σημαίνει πως η x_0 είναι μοναδική λύση και έτσι ολοκληρώνεται η απόδειξη του θεωρήματος.

■

5. Τετραγωνικά υπόλοιπα (ή κατάλοιπα) και ο νόμος της τετραγωνικής αντιστροφής (ή αμοιβαιότητας)

Τετραγωνικά υπόλοιπα (ή κατάλοιπα)

Ορισμός

Ο ακέραιος αριθμός a είναι τετραγωνικό υπόλοιπο (quadratic residue) του θετικού ακεραίου c, αν $(a,c)=1$ και η ισοτιμία $x^2 \equiv a(\mathrm{mod}\, c)$ έχει λύση.

Έτσι, για παράδειγμα έχουμε

$$3^2 \equiv 1(\mathrm{mod}\, 4), \quad 6^2 \equiv 11(\mathrm{mod}\, 5).$$

Θα παρουσιάσουμε κάποια βασικά θεωρήματα που αφορούν τα τετραγωνικά υπόλοιπα.

Θεώρημα

Έστω p περιττός πρώτος αριθμός και a ένας ακέραιος αριθμός τέτοιος ώστε $(a,p)=1$. Τότε, η

$$x^2 \equiv a(\mathrm{mod}\, p) \qquad (1)$$

είτε δεν θα έχει καμμία λύση ή θα έχει δύο διαφορετικές λύσεις.

(Υπενθυμίζουμε ότι με τον όρο διαφορετικές λύσεις εννοούμε πως οι λύσεις αυτές είναι μη - ισοδύναμες mod p).

ΑΠΟΔΕΙΞΗ

Στην περίπτωση όπου η $x^2 \equiv a(\mathrm{mod}\, p)$ έχει λύση, θεωρούμε πως

$$x_0^2 \equiv a(\mathrm{mod}\, p).$$

Τότε, είναι προφανές ότι

$$(-x_0)^2 \equiv a(\mathrm{mod}\, p).$$

Δηλαδή, αν x_0 είναι μία λύση της (1) , τότε και η $-x_0$ είναι λύση της (1) και μάλιστα ισχύει ότι

$$x_0 \not\equiv -x_0(\mathrm{mod}\, p).$$

Αυτό προκύπτει διότι αν $x_0 \equiv -x_0(\mathrm{mod}\, p)$, τότε $p|2x_0$ δηλαδή, $p|x_0$.

Όμως, ισχύει ότι $p|(x_0^2 - a)$ και $p \nmid a$ άρα δεν μπορεί να αληθεύει ότι $p|x_0$.

Θα αποδείξουμε ότι δεν μπορούν να υπάρξουν άλλες, διαφορετικές μεταξύ τους, λύσεις. (Αυτό είναι άμεση συνέπεια του θεωρήματος συντελεστών πολυωνύμου, που έχουμε αποδείξει). Μπορεί αυτό επίσης να δειχθεί ως ακολούθως:

Έστω ότι η x_0' είναι μια άλλη λύση, διαφορετική από τις παραπάνω.

Τότε

$$x_0^2 \equiv a(\text{mod}\, p),$$
$$(x_0')^2 \equiv a(\text{mod}\, p).$$

Συνεπώς

$$p \mid x_0^2 - (x_0')^2$$

ή

$$p \mid (x_0 - x_0')(x_0 + x_0')$$

δηλαδή

$$p \mid (x_0 - x_0') \text{ ή } p \mid (x_0 + x_0'),$$

το οποίο σημαίνει πως

$$x_0 \equiv x_0'(\text{mod}\, p) \text{ ή } -x_0 \equiv x_0'(\text{mod}\, p).$$

Επομένως,η λύση x_0' δεν είναι διαφορετική των x_0, $-x_0'$. Άτοπο.

Αυτό ολοκληρώνει την απόδειξη του θεωρήματος.

■

Θεώρημα

Έστω p περιττός πρώτος αριθμός, τότε υπάρχουν ακριβώς $\frac{p-1}{2}$ τετραγωνικά υπόλοιπα και $\frac{p-1}{2}$ τετραγωνικά μη υπόλοιπα $\text{mod}\, p$.

ΑΠΟΔΕΙΞΗ

Παρατηρούμε ότι

$$p-1 \equiv -1(\text{mod}\, p)$$
$$p-2 \equiv -2(\text{mod}\, p)$$
$$\vdots$$
$$p-\frac{p-1}{2} \equiv -\frac{p-1}{2}(\text{mod}\, p).$$

Επομένως

$$(p-1)^2 \equiv 1^2(\text{mod}\, p)$$
$$(p-2)^2 \equiv 2^2(\text{mod}\, p)$$
$$\vdots$$
$$\left(p-\frac{p-1}{2}\right)^2 \equiv \left(\frac{p-1}{2}\right)^2(\text{mod}\, p).$$

Συνεπώς, οι ακέραιοι αριθμοί $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$ είναι όλοι τετραγωνικά υπόλοιπα $\text{mod}\, p$.

Θα αποδείξουμε, τώρα, πως είναι και ανά δύο μή – ισοδύναμοι $\text{mod}\, p$.

Έστω

$$x_1, x_2 \in \left\{1,2,...,\frac{p-1}{2}\right\}.$$

Τότε

$$1 < x_1 + x_2 < p\,. \tag{1}$$

Συνεπώς αν $x_1^2 \equiv x_2^2 (\mathrm{mod}\, p)$ με $x_1 \neq x_2$, τότε $p \mid (x_1 - x_2)(x_1 + x_2)$, δηλαδή $p|(x_1 - x_2)$ ή $p|(x_1 + x_2)$. Λόγω της ανισότητας (1) προκύπτει ότι

$$p|(x_1 - x_2).$$

Αλλά, ισχύει ότι

$$|x_1 - x_2| < p\,.$$

Άρα, πρέπει να αληθεύει ότι $x_1 = x_2$. Άτοπο.

Επομένως, σύμφωνα με τα παραπάνω, προκύπτει πως υπάρχουν $\frac{p-1}{2}$ τετραγωνικά υπόλοιπα και $\frac{p-1}{2}$ τετραγωνικά μη-υπόλοιπα του p.

Τα τετραγωνικά υπόλοιπα είναι οι αριθμοί

$$1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2.$$

■

Θεώρημα *(ΘΕΩΡΗΜΑ ΤΟΥ DIRICHLET)*
Έστω p πρώτος αριθμός και a ένας ακέραιος αριθμός τέτοιος, ώστε $1 \le a \le p-1$. Αν η $x^2 \equiv a(\mathrm{mod}\, p)$ δεν έχει λύσεις,
τότε

$$p|(p-1)! - a^{(p-1)/2},$$

ενώ αν η $x^2 \equiv a(\mathrm{mod}\, p)$ έχει λύσεις,
τότε

$$p|(p-1)! + a^{(p-1)/2}.$$

ΑΠΟΔΕΙΞΗ

- Αν ο πρώτος αριθμός p είναι άρτιος, δηλαδή $p = 2$, ο ισχυρισμός του θεωρήματος είναι προφανής.
- Θα εξετάσουμε, λοιπόν, την περίπτωση όταν ο p είναι περιττός αριθμός.

Θεωρούμε την

$$a_1 x \equiv a(\mathrm{mod}\, p) \tag{1}$$

με $1 \le a_1 \le p-1$.

Τότε, η (1) έχει μοναδική λύση. Σύμφωνα με τις αρχές που διέπουν τις λύσεις των γραμμικών ισοδυναμιών, προκύπτει ότι τις τιμές του x τις αναζητούμε στο σύνολο

$$\{0,1,...,p-1\}$$

ή στο σύνολο

$$\left\{-\frac{p-1}{2},...,-2,-1,0,1,2,...,\frac{p-1}{2}\right\}.$$

Στην περίπτωσή μας , θα θεωρήσουμε χωρίς βλάβη της γενικότητας ότι $x\in\{1,2,...,p-1\}$. Είναι προφανές πως η περίπτωση $x=0$ απορρίπτεται καθώς $(a,p)=1$.

Έστω πως b είναι η μοναδική λύση της (1).

Τότε

$$a_1 b\equiv a(\mathrm{mod}\, p).$$

Έτσι, αν η ισοδυναμία $x^2\equiv a(\mathrm{mod}\, p)$ δεν έχει λύσεις προκύπτει ότι $a_1\neq b$ (ενώ ταυτόχρονα $a_1,b\in\{1,2,...,p-1\}$).

Συνεπώς, μπορούμε να διαμερίσουμε το σύνολο $\{1,2,...,p-1\}$σε $\frac{p-1}{2}$ διαφορετικά ζεύγη (a_1,b), με $a_1\neq b$.

Πολλαπλασιάζοντας κατά μέλη όλες τις γραμμικές ισοδυναμίες που θα προκύψουν από τα ζεύγη αυτά, θα έχουμε:

$$(p-1)!\equiv a^{\frac{p-1}{2}}(\mathrm{mod}\, p)\ .$$

Άρα

$$p\big|(p-1)!-a^{\frac{p-1}{2}}\ .$$

Αν η $x^2\equiv a\ (\mathrm{mod}\, p)$ έχει λύσεις, τότε θα έχει ακριβώς δύο λύσεις.

Θα περιοριστούμε πάλι στο σύνολο $\{1,2,...,p-1\}$ για τις λύσεις της ισοδυναμίας αυτής. Έστω κ η μία από τις δύο λύσεις. Τότε παρατηρούμε πως και ο ακέραιος $p-\kappa$ αποτελεί λύση της ισοδυναμίας. Όμως, μπορούμε να έχουμε δύο το πολύ λύσεις. Άρα, οι μοναδικές λύσεις είναι οι ακέραιοι

$$\kappa, p-\kappa\in\{1,2,...,p-1\}.$$

Αφαιρώντας τους ακέραιους $\kappa,\ p-\kappa$ από το σύνολο $\{1,2,...,p-1\}$, θα παραμείνουν $p-3$, στο πλήθος, ακέραιοι τους οποίους μπορούμε να διαμερίσουμε σε $\frac{p-3}{2}$ διαφορετικά ζεύγη (a_1,b), με $a_1\neq b$ και

$$a_1 b\equiv a\ (\mathrm{mod}\, p)$$

(όπως στην πρώτη περίπτωση).

Ομοίως, πολλαπλασιάζοντας κατά μέλη όλες τις γραμμικές ισοδυναμίες που θα προκύψουν από τα ζεύγη, λαμβάνουμε ότι

$$A \equiv a^{\frac{p-3}{2}} \pmod{p}, \text{ όπου } A \in \mathbb{N}.$$

Άρα

$$A = \frac{(p-1)!}{\kappa \cdot (p-\kappa)}$$

Όμως,

$$\kappa \cdot (p-\kappa) = \kappa\, p - \kappa^2 \equiv -a \pmod{p}.$$

Έτσι

$$A \cdot \kappa \cdot (p-\kappa) \equiv a^{\frac{p-3}{2}} (-a) \bmod p,$$

δηλαδή

$$(p-1)! \equiv -a^{\frac{p-1}{2}} \pmod{p}\cdot$$

Άρα

$$p \mid (p-1)! + a^{\frac{p-1}{2}}.$$

Αυτό ολοκληρώνει την απόδειξη του θεωρήματος.

■

Θεώρημα *(ΤΟ ΘΕΩΡΗΜΑ ΤΟΥ WILSON)*
Έστω p ένας πρώτος αριθμός. Τότε, ο αριθμός p διαιρεί τον

$$(p-1)!+1$$

και αντιστρόφως.

ΑΠΟΔΕΙΞΗ

1ος τρόπος

• **Για να αποδείξουμε το ευθύ του θεωρήματος** του Wilson θα αξιοποιήσουμε το θεώρημα του Dirichlet.

Θεωρούμε την ισοδυναμία

$$x^2 \equiv 1 \pmod{p},$$

η οποία έχει αναγκαστικά λύση, αφού μπορούμε να επιλέξουμε κατάλληλο x, τέτοιο ώστε $p \mid (x-1)(x+1)$ (για παράδειγμα $x = p-1$).

Αν στο θεώρημα Dirichlet, που αποδείξαμε προηγούμενα, θεωρήσουμε την τιμή του a να είναι $a = 1$, τότε πρέπει

$$p \mid (p-1)! + 1^{\frac{p-1}{2}},$$

δηλαδή $p \mid (p-1)!+1$.

● **Για την απόδειξη του αντιστρόφου** θα εργαστούμε ως εξής:

Έστω

$$p \mid (p-1)!+1,$$

χωρίς να γνωρίζουμε πως ο p είναι πρώτος αριθμός.

Παρατηρούμε ότι κανένας των ακεραίων αριθμών 2, 3, ..., $p-1$ δεν διαιρεί τον $(p-1)!+1$. Έτσι, ο μικρότερος διαιρέτης του $(p-1)!+1$ είναι ο p. Όμως, ο μικρότερος διαιρέτης κάθε ακεραίου αριθμού είναι πάντα πρώτος. Άρα, ο p είναι αναγκαστικά πρώτος αριθμός.

■

2ος τρόπος (*Η απόδειξη οφείλεται στον Lagrange*).

Θεωρούμε το πολυώνυμο

$$f(x) = (x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1}-1),$$

όπου $x = 1, 2, ..., p-1$ και p πρώτος αριθμός.

Αφού $x = 1, 2, ..., p-1$, προκύπτει ότι $(x, p) = 1$ και ένας από τους ακεραίους

$$x-1, x-2, ..., x-(p-1)$$

είναι ίσος με μηδέν.

Από το γεγονός ότι $(x, p) = 1$, συνεπάγεται ότι

$$x^{p-1} \equiv 1 (\mathrm{mod}\ p)$$

(*Μικρό Θεώρημα του Fermat*),
ενώ

$$p \mid (x-1)(x-2)\cdots(x-(p-1)),$$

αφού $p \mid 0$.

Άρα, η ισοδυναμία

$$f(x) \equiv 0 (\mathrm{mod}\ p)$$

έχει $p-1$ λύσεις. Όμως, το πολυώνυμο $f(x)$ είναι βαθμού $p-2$. Επομένως, σύμφωνα με το θεώρημα συντελεστών πολυωνύμου, που αποδείξαμε προηγούμενα, αν

$$f(x) = a_{p-2}x^{p-2} + \cdots + a_1 x + a_0$$

θα ισχύει ότι

$$p \mid a_0, p \mid a_1, ..., p \mid a_{p-2}.$$

Αλλά $a_0 = (p-1)!+1$ και αφού $p \mid a_0$, προκύπτει ότι

$$p \mid (p-1)!+1.$$

Έτσι, **αποδείξαμε το ευθύ του θεωρήματος του Wilson.** Για το *αντίστροφο* ακολουθούμε τον προηγούμενο τρόπο.

■

Το σύμβολο του Legendre

Ορισμός

Έστω p ένας περιττός πρώτος αριθμός και a ένας ακέραιος αριθμός τέτοιος ώστε $(a,p)=1$. Τότε, ορίζουμε **το σύμβολο του Legendre**

$$\left(\frac{a}{p}\right)$$

ως εξής:

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{αν ο ακέραιος } a \text{ είναι δευτεροβάθμιο τετραγωνικό υπόλοιπο mod } p\\ -1, & \text{αν ο ακέραιος } a \text{ δεν είναι δευτεροβάθμιο τετραγωνικό υπόλοιπο mod } p\end{cases}$$

Το σύμβολο του Legendre γενικεύεται και στην περίπτωση όπου $p \mid a$ λαμβάνοντας μηδενική τιμή. Δηλαδή

$$\left(\frac{a}{p}\right)=0, \text{ αν } p \mid a.$$

Έτσι, για παράδειγμα είναι

$$\left(\frac{11}{7}\right)=1,\ \left(\frac{6}{13}\right)=-1,\ \left(\frac{15}{5}\right)=0 \ .$$

Θα αποδείξουμε κάποιες βασικές ιδιότητες και θεωρήματα που αφορούν το σύμβολο του Legendre.

Θεώρημα *(ΤΟ ΚΡΙΤΗΡΙΟ ΤΟΥ EULER)*

Έστω p περιττός πρώτος αριθμός και a ακέραιος αριθμός, τέτοιος ώστε $(a,p)=1$. *Τότε, ισχύει ότι*

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p.$$

ΑΠΟΔΕΙΞΗ

Γνωρίζουμε ότι $(a,p)=1$. Άρα, αποκλείεται η περίπτωση $\left(\frac{a}{p}\right)=0$. Δηλαδή

$$\left(\frac{a}{p}\right)=\pm 1.$$

- Αν $\left(\frac{a}{p}\right)=1$, τότε ο ακέραιος αριθμός a είναι τετραγωνικό υπόλοιπο του p και συνεπώς υπάρχει ακέραιος αριθμός x_0 τέτοιος, ώστε

$$x_0^2 \equiv a \pmod p.$$

Συνεπώς

$$\left(x_0^2\right)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod p$$

ή

$$\left(x_0^{p-1}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

ή $$\left(a^{\frac{p-1}{2}}\right)\equiv x_0^{p-1}\pmod p. \qquad (1)$$

Όμως, γνωρίζουμε ότι $(x_0,p)=1$ αφού $p\left|\left(x_0^2-a\right)\right.$ και $(a,p)=1$. Επομένως, από το Μικρό Θεώρημα του Fermat προκύπτει

$$x_0^{p-1}\equiv 1\pmod p. \qquad (2)$$

Άρα, από τις σχέσεις (1) και (2) προκύπτει

$$a^{\frac{p-1}{2}}\equiv 1\pmod p$$

ή $$1\equiv a^{\frac{p-1}{2}}\pmod p.$$

Δηλαδή

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}\pmod p.$$

- Αν $\left(\frac{a}{p}\right)=-1$, τότε ο ακέραιος αριθμός a είναι τετραγωνικό

μη-υπόλοιπο του p. Δηλαδή η $x^2\equiv a\pmod p$ δεν έχει καμμία λύση. Σ' αυτήν την περίπτωση, όμως, από το θεώρημα του Dirichlet γνωρίζουμε ότι

$$p\,|\,(p-1)!-a^{\frac{p-1}{2}},$$

δηλαδή

$$a^{\frac{p-1}{2}}\equiv (p-1)!\pmod p. \qquad (3)$$

Αλλά, από το θεώρημα του Wilson αληθεύει

$$(p-1)!\equiv -1\pmod p \qquad (4)$$

και επομένως, από τις σχέσεις (3) και (4) λαμβάνουμε ότι

$$a^{\frac{p-1}{2}}\equiv -1\pmod p$$

$$\Leftrightarrow -1\equiv a^{\frac{p-1}{2}}\pmod p.$$

Συνεπώς

$$\left(\frac{\alpha}{p}\right)\equiv \alpha^{\frac{p-1}{2}}\pmod p.$$

Αυτό ολοκληρώνει την απόδειξη του κριτηρίου Euler.

■

Θεώρημα

Έστω p περιττός πρώτος αριθμός και a ακέραιος αριθμός, τέτοιος ώστε $(a,p)=1$. Αν $a\equiv b(\mathrm{mod}\, p)$, τότε

$$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right).$$

ΑΠΟΔΕΙΞΗ

Είναι προφανές ότι $(b,p)=1$, διότι αν $p|b$ τότε $p|a$, το οποίο είναι αδύνατον. Συνεπώς, αφού $a\equiv b(\mathrm{mod}\, p)$ προκύπτει ότι ο a είναι τετραγωνικό υπόλοιπο (αντίστοιχα μη-υπόλοιπο) του p αν και μόνο αν ο b είναι τετραγωνικό υπόλοιπο (αντίστοιχα μη-υπόλοιπο). Έτσι, από τον ορισμό του συμβόλου του Legendre, έχουμε

$$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right).$$

■

Θεώρημα

Έστω p περιττός πρώτος και a,b ακέραιοι αριθμοί , τέτοιοι ώστε $(ab,p)=1$. Τότε, ισχύει ότι

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

δηλαδή το σύμβολο του Legendre είναι μια πλήρης πολλαπλασιαστική συνάρτηση.

ΑΠΟΔΕΙΞΗ

Από το κριτήριο του Euler λαμβάνουμε ότι

$$\left(\frac{ab}{p}\right)\equiv (ab)^{\frac{p-1}{2}}(\mathrm{mod}\, p),$$

το οποίο είναι ισοδύναμο με

$$\left(\frac{ab}{p}\right)\equiv a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}(\mathrm{mod}\, p)$$

$$\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(\mathrm{mod}\, p).$$

Άρα

$$p\left|\left(\frac{ab}{p}\right)-\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right.$$

Όμως,

$$\left(\frac{ab}{p}\right), \left(\frac{a}{p}\right) \text{και} \left(\frac{b}{p}\right)$$

λαμβάνουν τις τιμές –1, 1. Δηλαδή

$$(ab|p)-(a|p)(b|p)=0 \text{ ή } 2 \text{ ή } -2$$

ενώ ο p είναι περιττός αριθμός. Συνεπώς, αναγκαστικά θα ισχύει ότι

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Αυτό ολοκληρώνει την απόδειξη του θεωρήματος. ■

Λήμμα 1
Έστω p περιττός πρώτος αριθμός. Τότε ισχύει ότι

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}.$$

ΑΠΟΔΕΙΞΗ

Από το κριτήριο του Euler προκύπτει ότι

$$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}}(\text{mod } p).$$

Όμως,

$$\left(-\frac{1}{p}\right) \text{και } (-1)^{\frac{p-1}{2}}$$

μπορούν να λάβουν μόνο τις τιμές –1 και 1. Συνεπώς, αφού

$$p\left|\left(\frac{-1}{p}\right)-(-1)^{\frac{p-1}{2}}\right.$$

και ο p είναι περιττός αριθμός, αναγκαστικά θα ισχύει ότι

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}.$$

■

Λήμμα 2
Έστω p περιττός πρώτος αριθμός. Τότε ισχύει ότι

$$\left(-\frac{1}{p}\right)=\begin{cases} 1, & \text{αν } p\equiv 1(\text{mod}\,4) \\ -1, & \text{αν } p\equiv 3(\text{mod}\,4) \end{cases}$$

ΑΠΟΔΕΙΞΗ

Ο πρώτος αριθμός p μπορεί να λάβει την μορφή $4n+1$ ή την μορφή $4n+3$, όπου $n \in \mathbb{N}$.

- Αν $p = 4n+1$, τότε από το Λήμμα 1 προκύπτει

$$\left(-\frac{1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{2n} = 1.$$

- Αν $p = 4n+3$, τότε από το Λήμμα 1 συνεπάγεται

$$\left(-\frac{1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{2n+1} = -1 .$$

■

Θεώρημα

Έστω p περιττός πρώτος. Τότε ισχύει ότι

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{αν } p \equiv \pm 1 \pmod 8 \\ -1, & \text{αν } p \equiv \pm 3 \pmod 8 \end{cases}$$

ΑΠΟΔΕΙΞΗ

Θεωρούμε τις παρακάτω $\frac{p-1}{2}$ το πλήθος ισοδυναμίες:

$$\begin{aligned} p-1 &\equiv 1\cdot(-1)^1 \pmod p \\ 2 &\equiv 2\cdot(-1)^2 \pmod p \\ p-3 &\equiv 3\cdot(-1)^3 \pmod p \\ 4 &\equiv 4\cdot(-1)^4 \pmod p \\ &\vdots \\ \kappa &\equiv \frac{p-1}{2}\cdot(-1)^{\frac{p-1}{2}} \pmod p, \end{aligned}$$

όπου

$$\kappa = \begin{cases} \frac{p-1}{2}, & \text{αν ο ακέραιος } (p-1)/2 \text{ είναι άρτιος} \\ p-\frac{p-1}{2}, & \text{αν ο ακέραιος } (p-1)/2 \text{ είναι περιττός.} \end{cases}$$

Πολλαπλασιάζοντας τις παραπάνω ισοδυναμίες κατά μέλη, προκύπτει ότι

$$2\cdot 4\cdot 6\cdots(p-1) \equiv \left(\frac{p-1}{2}\right)!(-1)^{\frac{p^2-1}{8}} \pmod p . \qquad (1)$$

Όμως, ισχύει ότι

$$2\cdot 4\cdot 6\cdots(p-1) \equiv (2\cdot 1)\cdot(2\cdot 2)\cdot(2\cdot 3)\cdots\left(2\cdot\frac{p-1}{2}\right)$$

$$= 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!.$$

Άρα, η σχέση (1) λαμβάνει την μορφή

$$2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\equiv\left(\frac{p-1}{2}\right)!(-1)^{\frac{p^2-1}{8}}(\mathrm{mod}\,p). \tag{2}$$

Όμως, είναι προφανές πως ο p δεν διαιρεί τον ακέραιο $\left(\frac{p-1}{2}\right)!$.

Συνεπώς, από τη (2) προκύπτει ότι

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}}(\mathrm{mod}\,p). \tag{3}$$

Από το κριτήριο του Euler λαμβάνουμε

$$\left(\frac{2}{p}\right)\equiv 2^{\frac{p-1}{2}}(\mathrm{mod}\,p)\ . \tag{4}$$

Από τις σχέσεις (3) και (4) συνεπάγεται ότι

$$\left(\frac{2}{p}\right)\equiv(-1)^{\frac{p^2-1}{8}}(\mathrm{mod}\,p).$$

Αλλά τα

$$(2|p) \text{ και } (-1)^{\frac{p^2-1}{8}}$$

μπορούν να λάβουν μόνο τις τιμές –1 και 1.

Συνεπώς, θα ισχύει ότι

$$(2|p)-(-1)^{(p^2-1)/8}=0 \text{ ή } 2 \text{ ή } -2,$$

ενώ

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

Ο πρώτος αριθμός p μπορεί να λάβει την μορφή

$$8n+1 \text{ ή } 8n+3 \text{ ή } 8n-3 \text{ ή } 8n-1, \text{ όπου } n\in\mathbb{N}.$$

Στην περίπτωση όπου $p=8n\pm1$ λαμβάνουμε ότι

$$\frac{p^2-1}{8}=8n^2\pm2n,$$

που είναι άρτιος αριθμός.

Στην περίπτωση όπου $p=8n\pm3$ συνεπάγεται ότι

$$\frac{p^2-1}{8}=8n^2\pm6n+1,$$

που είναι περιττός αριθμός.

Έτσι, συνοψίζοντας, μπορούμε να γράψουμε ότι

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, & \text{αν } p\equiv\pm1(\mathrm{mod}\,8)\\ -1, & \text{αν } p\equiv\pm3(\mathrm{mod}\,8).\end{cases}$$

■

Θεώρημα *(ΤΟ ΛΗΜΜΑ ΤΟΥ GAUSS)*

Έστω p *περιττός πρώτος αριθμός και* a *ακέραιος αριθμός, τέτοιοι ώστε* $(a,p)=1$. *Θεωρούμε τα ελάχιστα θετικά υπόλοιπα των ακεραίων*

$$a, 2a, 3a, ..., \frac{p-1}{2}a .$$

Τότε, αν υποθέσουμε ότι ο ακέραιος αριθμός s *συμβολίζει το πλήθος των υπολοίπων αυτών, που είναι μεγαλύτερα από τον πραγματικό αριθμό* $\frac{p}{2}$, *ισχύει ότι*

$$\left(\frac{a}{p}\right)=(-1)^s .$$

ΑΠΟΔΕΙΞΗ

Είναι προφανές ότι καθένας από τους αριθμούς της μορφής $m\alpha$, όπου $m=1,2,...,\frac{p-1}{2}$ διαιρούμενος από τον p, δίνει ένα μη – μηδενικό υπόλοιπο. Αυτό αληθεύει, διότι

$$(a,p)=1 \text{ και } (m,p)=1, \text{ για κάθε } m.$$

Θεωρώντας τα ελάχιστα από τα $\frac{p-1}{2}$ θετικά υπόλοιπα τα κατανέμουμε σε δύο σύνολα ως εξής:

$$S_1=\{r_1,r_2,...,r_\lambda\}, \text{ αν } r_i<\frac{p}{2}, \text{ με } i=1,2,...,\lambda$$

και

$$S_2=\{e_1,e_2,...,e_s\}, \text{ αν } e_i>\frac{p}{2}, \text{ με } i=1,2,...,s .$$

Είναι προφανές πως ισχύει ότι $s+\lambda=(p-1)/2$, καθώς $S_1\cap S_2=\varnothing$.

Θα προσπαθήσουμε, τώρα, αξιοποιώντας τα στοιχεία του συνόλου S_2 να δημιουργήσουμε ένα τρίτο σύνολο S_3, τέτοιο ώστε

$$S_1\cup S_3=\{1,2,...,(p-1)/2\}.$$

Παρατηρούμε ότι οποιοδήποτε στοιχείο $r_i\in S_1$ είναι διαφορετικό από κάθε ακέραιο αριθμό w_j, $w_j=p-e_j$, όπου $e_j\in S_2$, δηλαδή, για οποιοδήποτε ζεύγος (i,j) με $i=1,2,...,\lambda$ και $j=1,2,...,s$, ισχύει ότι $w_j\neq r_i$. Αυτό συμβαίνει, διότι αν υπήρχαν i,j τέτοια ώστε $w_j=r_i$, τότε $p=r_i+e_j$. Όμως, από τον ορισμό των r_i, e_j λαμβάνουμε ότι

$$\kappa a=\kappa_i p+r_i, \text{ όπου } 1\le\kappa\le\frac{p-1}{2}, \text{ με } i=1,2,...,\lambda , \quad (1)$$

και

$$\nu a=\nu_j p+e_j, \text{ όπου } 1\le\nu\le\frac{p-1}{2}, \text{ με } j=1,2,...,s . \quad (2)$$

Άρα

$$\begin{aligned}(\kappa+\nu)a&=(\kappa_i+\nu_j)p+(r_i+e_j)\\&=(\kappa_i+\nu_j)p+p\end{aligned}$$

και επειδή $(a, p)=1$, θα έχουμε ότι

$$\kappa+\nu \equiv 0(\mathrm{mod}\, p).$$

Άτοπο, επειδή

$$2 \le \kappa+\nu \le p-1.$$

Συνεπώς, από τα παραπάνω προκύπτει ότι τα σύνολα S_1 και $\{w_1, w_2, ..., w_s\}$ είναι ξένα μεταξύ τους.

Αλλά γνωρίζουμε ότι $w_j \in \left\{1, 2, ..., \frac{p-1}{2}\right\}$, για κάθε $j=1, 2, ..., s$ καθώς

$$w_j = p - e_j \text{ και } e_j > \frac{p}{2}.$$

Επομένως, το σύνολο S_3 που αναζητούσαμε είναι ακριβώς το σύνολο $\{w_1, w_2, ..., w_s\}$. Άρα

$$S_1 \cup S_3 = \left\{1, 2, ..., \frac{p-1}{2}\right\}.$$

Το γινόμενο των στοιχείων του συνόλου $S_1 \cup S_3$ δίνει

$$r_1 r_2 \ \cdots \ r_\lambda \cdot w_1 w_2 \ \cdots \ w_s = 1 \cdot 2 \cdot 3 \ \cdots \ \frac{p-1}{2},$$

το οποίο ισοδύναμα γράφεται

$$r_1 r_2 \ \cdots \ r_\lambda (p-e_1)\ (p-e_2)\ \cdots\ (p-e_s) = \left(\frac{p-1}{2}\right)!.$$

Όμως

$$r_1 r_2 \ \cdots \ r_\lambda (p-e_1)(p-e_2)\ \cdots\ (p-e_s) = c\ p - r_1 r_2 \cdots\ r_\lambda (-1)^s e_1 e_2 \cdots\ e_s,$$

για κάποιον ακέραιο αριθμό c.

Αλλά

$$p \mid r_1 r_2 \ \cdots \ r_\lambda (p-e_1)(p-e_2) \cdots\ (p-e_s) - \left(\frac{p-1}{2}\right)! = 0,$$

συνεπώς

$$p \mid cp - r_1 r_2 \ \cdots \ r_\lambda (-1)^s e_1 e_2 \cdots\ e_s - \left(\frac{p-1}{2}\right)!$$

και επομένως

$$p \mid (-1)^s r_1 r_2 \cdots\ r_\lambda \cdot e_1 e_2 \ldots e_s - \left(\frac{p-1}{2}\right)! \qquad (3)$$

Από τις σχέσεις (1) και (2) λαμβάνουμε

$$r_i = \kappa a - \kappa_i p, \quad 1 \le \kappa \le \frac{p-1}{2} \ \text{ με } i = 1,2,...,\lambda$$

και

$$e_j = \nu a - \nu_j p, \quad 1 \le \nu \le \frac{p-1}{2} \ \text{ με } \ j = 1,2,...,s.$$

Άρα

$$r_1 r_2 \cdots r_\lambda \cdot e_1 e_2 \cdots e_s \equiv a(2a)(3a) \cdots \left(\frac{p-1}{2}a\right) (\mathrm{mod}\, p). \qquad (4)$$

Από τις σχέσεις (3) και (4) προκύπτει ότι

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^s a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \ (\mathrm{mod}\, p).$$

Βέβαια, από το κριτήριο του Euler, έχουμε

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\mathrm{mod}\, p).$$

Συνεπώς

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^s \left(\frac{a}{p}\right) \left(\frac{p-1}{2}\right)! \ (\mathrm{mod}\, p)$$

$$\Leftrightarrow 1 \equiv (-1)^s \left(\frac{a}{p}\right) (\mathrm{mod}\, p)$$

$$\Leftrightarrow \left(\frac{a}{p}\right) \equiv \left(\frac{a}{p}\right) (-1)^s \left(\frac{a}{p}\right) (\mathrm{mod}\, p)$$

$$\Leftrightarrow \left(\frac{a}{p}\right) \equiv (-1)^s (\mathrm{mod}\, p)$$

και επειδή

$$\left(\frac{a}{p}\right) - (-1)^s = 0 \text{ ή } 2 \text{ ή } -2,$$

προκύπτει ότι

$$\left(\frac{a}{p}\right) = (-1)^s.$$

■

Θεώρημα *(ΝΟΜΟΣ ΤΕΤΡΑΓΩΝΙΚΗΣ ΑΝΤΙΣΤΡΟΦΗΣ ή ΑΜΟΙΒΑΙΟΤΗΤΑΣ)*
Έστω p, q δύο διαφορετικοί περιττοί πρώτοι αριθμοί. Τότε, ισχύει ότι

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

ΑΠΟΔΕΙΞΗ

Από το λήμμα του Gauss που αποδείξαμε προηγούμενα, έχουμε

$$\left(\frac{p}{q}\right) = (-1)^{s_1} \text{ και } \left(\frac{q}{p}\right) = (-1)^{s_2},$$

όπου s_1, s_2 συμβολίζουν τα πλήθη των θετικών υπολοίπων που προκύπτουν από την διαίρεση των αριθμών

$$p, 2p, 3p, ..., \frac{q-1}{2}p, \text{ διά του } q$$

και

$$q, 2q, 3q, ..., \frac{p-1}{2}q, \text{ διά του } p$$

και είναι μεγαλύτερα από $\frac{q}{2}, \frac{p}{2}$, αντίστοιχα.

Άρα

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{s_1+s_2}.$$

***Βήμα 1*:** Θα αποδείξουμε ότι

$$s_1 = \sum_{m_1=1}^{(q-1)/2} \left\lfloor \frac{m_1 p}{q} \right\rfloor (\mathrm{mod}\, 2) \quad \text{και} \quad s_2 = \sum_{m_2=1}^{(p-1)/2} \left\lfloor \frac{m_2 q}{p} \right\rfloor (\mathrm{mod}\, 2).$$

Γι' αυτό το σκοπό αρκεί να δείξουμε πως για το πλήθος s που έχουμε θεωρήσει στο λήμμα του Gauss, ισχύει ότι

$$s \equiv (a-1)\frac{p^2-1}{8} + \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor (\mathrm{mod}\, 2).$$

Έτσι, συνεπάγεται

$$\sum_{m=1}^{(p-1)/2} m = \sum_{i=1}^{\lambda} r_i + \sum_{j=1}^{s} w_i = \sum_{i=1}^{\lambda} r_i + \sum_{j=1}^{s} (p - e_j)$$

$$= \sum_{i=1}^{\lambda} r_i + s \cdot p - \sum_{j=1}^{s} e_j . \tag{1}$$

Επίσης ισχύει

$$\frac{ma}{p} = \left\lfloor \frac{ma}{p} \right\rfloor + \upsilon_m, \text{ όπου } 0 < \upsilon_m < 1,$$

το οποίο ισοδύναμα γράφεται

$$ma = \left\lfloor \frac{ma}{p} \right\rfloor p + \upsilon_m p . \tag{2}$$

Θέτουμε $h_m = \upsilon_m p$. Άρα, θα ισχύει ότι $0 < h_m < p$. Είναι προφανές ότι το h_m είναι το ελάχιστο θετικό υπόλοιπο της διαίρεσης του ma δια p.

Συνεπώς

$$\sum_{i=1}^{\lambda} r_i + \sum_{j=1}^{s} e_j = \sum_{m=1}^{(p-1)/2} h_m$$

και λόγω της (2) προκύπτει ότι

$$a\sum_{m=1}^{(p-1)/2} m - p\sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor = \sum_{i=1}^{\lambda} r_i + \sum_{j=1}^{s} e_j \ . \tag{3}$$

Προσθέτοντας κατά μέλη τις σχέσεις (1) και (3) λαμβάνουμε ότι

$$(a+1)\sum_{m=1}^{(p-1)/2} m - p\sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor = 2\sum_{i=1}^{\lambda} r_i + s\cdot p \tag{4}$$

Όμως, γνωρίζουμε ότι $p \equiv 1 (\mathrm{mod}\, 2)$. Από την σχέση αυτή προκύπτουν οι ισοδυναμίες

$$sp \equiv s (\mathrm{mod}\, 2)$$

και

$$p\sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor \equiv \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor (\mathrm{mod}\, 2) \ .$$

Επίσης γνωρίζουμε ότι $a+1 \equiv a-1 (\mathrm{mod}\, 2)$.

Άρα

$$(a+1)\sum_{m=1}^{(p-1)/2} m \equiv (a-1)\sum_{m=1}^{(p-1)/2} m (\mathrm{mod}\, 2) \ .$$

Συνεπώς, από τις τρεις παραπάνω σχέσεις προκύπτει

$$s + p\sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor + (a+1)\sum_{m=1}^{(p-1)/2} m \equiv sp + \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor + (a-1)\sum_{m=1}^{(p-1)/2} m \ (\mathrm{mod}\, 2).$$

και λόγω της σχέσης (4) λαμβάνουμε

$$s + 2\sum_{i=1}^{\lambda} r_i + sp + 2p\sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor$$

$$\equiv sp + \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor + (a-1)\sum_{m=1}^{(p-1)/2} m (\mathrm{mod}\, 2).$$

Άρα

$$s \equiv \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor + (a-1)\sum_{m=1}^{(p-1)/2} m (\mathrm{mod}\, 2) \ .$$

Επομένως

$$s \equiv \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor + (a-1)\frac{p^2-1}{8} (\mathrm{mod}\, 2).$$

Αυτό ολοκληρώνει την απόδειξη του πρώτου βήματος.΄Αρα έχουμε αποδείξει ότι

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{s_1+s_2},$$

όπου

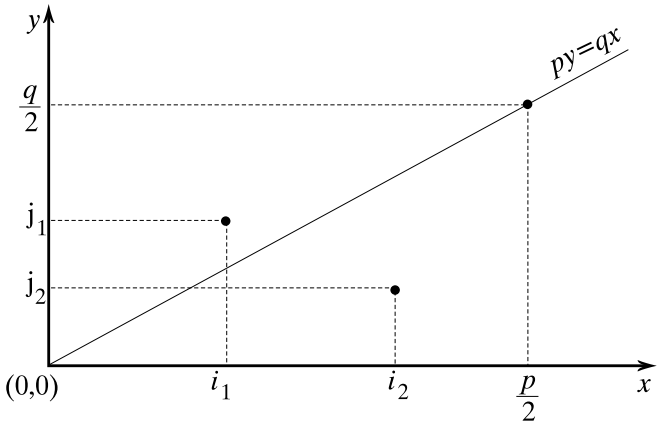
$$s_1+s_2\equiv\sum_{m_1=1}^{(q-1)/2}\left\lfloor\frac{m_1p}{q}\right\rfloor+\sum_{m_2=1}^{(p-1)/2}\left\lfloor\frac{m_2q}{p}\right\rfloor(\mathrm{mod}\,2).$$

Βήμα 2: Θα αποδείξουμε ότι

$$\sum_{m_1=1}^{(q-1)/2}\left\lfloor\frac{m_1p}{q}\right\rfloor+\sum_{m_2=1}^{(p-1)/2}\left\lfloor\frac{m_2q}{p}\right\rfloor=\frac{p-1}{2}\cdot\frac{q-1}{2}$$

Θεωρούμε στο καρτεσιανό επίπεδο τα **συνδεσμικά σημεία** (lattice points) (m_2,m_1), όπου $1\le m_1\le\frac{q-1}{2}$ και $1\le m_2\le\frac{p-1}{2}$, με $(m_1,m_2)\in\mathbb{N}$.

Η ευθεία με εξίσωση $py=qx$ δεν διέρχεται από κανένα συνδεσμικό σημείο (m_2,m_1).



Αυτό συμβαίνει, διότι αν υπήρχε έστω και ένα ζεύγος (m_2,m_1), τέτοιο ώστε $pm_2=qm_1$, τότε θα έπρεπε $qm_1\equiv 0(\mathrm{mod}\,p)$, το οποίο είναι αδύνατον καθώς $(q,p)=1$ και $1\le m_1\le(q-1)/2$.

Συνεπώς, κάθε συνδεσμικό σημείο (m_2,m_1) θα βρίσκεται είτε πάνω είτε κάτω από την ευθεία με εξίσωση $py=qx$.

Θα θεωρήσουμε δύο περιπτώσεις.

1η περίπτωση: Αν το συνδεσμικό σημείο (m_2,m_1) βρίσκεται πάνω από την ευθεία με εξίσωση $py=qx$, τότε ισχύει

$$pm_1>qm_2$$

και επομένως

$$m_2<\frac{pm_1}{q}.$$

Άρα, για κάθε σταθερή τιμή του m_1 υπάρχουν $\left\lfloor\frac{pm_1}{q}\right\rfloor$ συνδεσμικά σημεία τα οποία βρίσκονται πάνω από την ευθεία με εξίσωση $py=qx$.

Συνεπώς, το συνολικό πλήθος των συνδεσμικών σημείων που βρίσκονται πάνω από την ευθεία είναι

$$\sum_{m_1=1}^{(q-1)/2} \left\lfloor \frac{m_1 p}{q} \right\rfloor .$$

2η περίπτωση: Αν το συνδεσμικό σημείο (m_2, m_1) βρίσκεται κάτω από την ευθεία με εξίσωση $py = qx$, τότε ισχύει

$$pm_1 < qm_2$$

και συνεπώς

$$m_1 < \frac{qm_2}{p} .$$

Έτσι, ακολουθώντας την ίδια επιχειρηματολογία με την προηγούμενη περίπτωση, λαμβάνουμε ότι το πλήθος των συνδεσμικών σημείων που βρίσκονται κάτω από την ευθεία είναι

$$\sum_{m_2=1}^{(p-1)/2} \left\lfloor \frac{m_2 q}{p} \right\rfloor .$$

Επομένως, το συνολικό πλήθος των συνδεσμικών σημείων που βρίσκονται πάνω και κάτω από την ευθεία με εξίσωση $py = qx$ είναι

$$\sum_{m_1=1}^{(q-1)/2} \left\lfloor \frac{m_1 p}{q} \right\rfloor + \sum_{m_2=1}^{(p-1)/2} \left\lfloor \frac{m_2 q}{p} \right\rfloor .$$

Όμως, γενικά, το πλήθος των συνδεσμικών σημείων (m_2, m_1) είναι $\frac{p-1}{2} \cdot \frac{q-1}{2}$ και καθώς κανένα συνδεσμικό σημείο δεν βρίσκεται πάνω στην ευθεία με εξίσωση $py = qx$, είναι προφανές ότι

$$\sum_{m_1=1}^{(q-1)/2} \left\lfloor \frac{m_1 p}{q} \right\rfloor + \sum_{m_2=1}^{(p-1)/2} \left\lfloor \frac{m_2 q}{p} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2} .$$

Συνεπώς, από τα αποτελέσματα των βημάτων 1 και 2 προκύπτει ότι

$$s_1 + s_2 \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2,$$

δηλαδή

$$s_1 + s_2 - \frac{p-1}{2} \cdot \frac{q-1}{2} = 2\kappa, \quad \text{όπου } \kappa \in \mathbb{Z} .$$

Άρα

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{s_1+s_2} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} (-1)^{2\kappa}$$

$$= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} .$$

Αυτό ολοκληρώνει την απόδειξη του *νόμου της τετραγωνικής αντιστροφής (ή αμοιβαιότητας)*.

■

Σχόλιο

Ο νόμος της ***τετραγωνικής αντιστροφής*** *(ή* ***αμοιβαιότητας****) συσχετίζει την επιλυσιμότητα της ισοσυναμίας*

$$x^2 \equiv p \pmod{q} \qquad (*)$$

με την επιλυσιμότητα της ισοδυναμίας

$$x^2 \equiv q \pmod{p}. \qquad (**)$$

Έτσι, υπάρχουν δύο βασικές περιπτώσεις

1η περίπτωση: *Αν* $p \equiv 1 \pmod 4$ *ή* $q \equiv 1 \pmod 4$*, τότε*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1.$$

Αυτό σημαίνει ότι η ισοδυναμία $(*)$ *έχει λύση αν και μόνο αν η ισοδυναμία* $(**)$ *έχει λύση.*

2η περίπτωση: *Αν* $p \equiv 3 \pmod 4$ *και* $q \equiv 3 \pmod 4$*, τότε*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1.$$

Αυτό σημαίνει ότι η ισοδυναμία $(*)$ *έχει λύση αν και μόνο αν η ισοδυναμία* $(**)$ *δεν έχει λύση.*

ΠΑΡΑΔΕΙΓΜΑΤΑ

- Ισχύει ότι $6^2 \equiv 5 \pmod{31}$, δηλαδή, αληθεύει ότι $\left(\frac{5}{31}\right) = 1$. Όμως, από τον *νόμο της τετραγωνικής αντιστροφής* λαμβάνουμε ότι

$$\left(\frac{31}{5}\right)\left(\frac{5}{31}\right) = (-1)^{\frac{31-1}{2}\cdot\frac{5-1}{2}} = (-1)^{15\cdot 2} = 1.$$

Άρα

$$\left(\frac{31}{5}\right) = 1$$

και συνεπώς ο αριθμός 31 είναι τετραγωνικό υπόλοιπο $\bmod 5$.

- Ισχύει ότι $\left(\frac{29}{17}\right) = -1$. Έτσι, από τον *νόμο της τετραγωνικής αντιστροφής* προκύπτει ότι

$$\left(\frac{29}{17}\right)\left(\frac{17}{29}\right) = (-1)^{\frac{29-1}{2}\cdot\frac{17-1}{2}} = (-1)^{14\cdot 8} = 1.$$

Άρα

$$\left(\frac{17}{29}\right) = -1$$

και συνεπώς ο αριθμός 17 είναι τετραγωνικό μη –υπόλοιπο $\bmod 29$.

- Από τον νόμο της τετραγωνικής αντιστροφής έχουμε

$$\left(\frac{7}{29}\right)\left(\frac{29}{7}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{29-1}{2}} = (-1)^{3\cdot 14} = 1.$$

Συνεπώς, η εξίσωση $x^2 \equiv 7 \pmod{29}$ έχει λύση αν και μόνο αν η εξίσωση $x^2 \equiv 29 \pmod 7$

έχει λύση. Αλλά, ισχύει ότι $6^2 \equiv 7 \pmod{29}$. Συνεπώς $\left(\frac{7}{29}\right)=\left(\frac{29}{7}\right)=1$, καθώς και οι δύο ισοτιμίες έχουν λύσεις.

Το σύμβολο του Jacobi

Το σύμβολο του Jacobi [που ονομάστηκε έτσι προς τιμήν του Carl Gustav Jacobi (1804 – 1851), ο οποίος το παρουσίασε το έτος 1846] αποτελεί μια γενίκευση του συμβόλου του Legendre που παρουσιάσαμε προηγούμενα. Το σύμβολο του Legendre αναφέρεται στην επιλυσιμότητα της ισοτιμίας $x^2 \equiv a \pmod{p}$ αν ο p είναι πρώτος αριθμός και $(a,p)=1$. Στο σύμβολο του Jacobi δεν μελετάμε μόνο πρώτο αριθμό p αλλά οποιονδήποτε περιττό θετικό ακέραιο P και το αποτέλεσμα που επιστρέφει το σύμβολο αυτό δεν μας πληροφορεί για το αν η ισοτιμία $x^2 \equiv a \pmod{P}$, όπου $(a,P)=1$, έχει λύσεις *(βλέπε σχόλιο).* **Στην περίπτωση, όμως, που ο P είναι πρώτος αριθμός τα σύμβολα Legendre και Jacobi ταυτίζονται.**

Ορισμός

Έστω P περιττός θετικός ακέραιος και a ένας ακέραιος αριθμός, τέτοιος ώστε $(a,P)=1$.

Τότε, ορίζουμε το **σύμβολο του Jacobi**

$$\left(\frac{\boldsymbol{a}}{\boldsymbol{P}}\right)$$

ως εξής

$$\left(\frac{a}{P}\right)=1, \text{ αν } P=1$$

και

$$\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)^{m_1}\left(\frac{a}{p_2}\right)^{m_2}\cdots\left(\frac{a}{p_\kappa}\right)^{m_\kappa}, \text{ αν } P=p_1^{m_1}p_2^{m_2}\ldots p_\kappa^{m_\kappa}$$

όπου $\left(\frac{a}{p_i}\right)$ είναι το σύμβολο του Legendre.

Παρατήρηση

Πολλές φορές το σύμβολο του Jacobi γενικεύεται και στην περίπτωση όπου $P|a$ λαμβάνοντας μηδενική τιμή. Δηλαδή $\left(\frac{a}{P}\right)=0$, αν $P|a$.

ΠΑΡΑΔΕΙΓΜΑΤΑ

- $$\left(\frac{14}{17081}\right)=\left(\frac{14}{19\cdot 29\cdot 31}\right)=\left(\frac{14}{19}\right)\left(\frac{14}{29}\right)\left(\frac{14}{31}\right)$$

$$= (-1)\cdot(-1)\cdot 1 = 1$$

- $$\left(\frac{14}{324539}\right) = \left(\frac{14}{19^2 \cdot 29 \cdot 31}\right) = \left(\frac{14}{19}\right)^2 \left(\frac{14}{29}\right)\left(\frac{14}{31}\right)$$
$$= (-1)^2 \cdot (-1)\cdot 1 = -1$$
- $$\left(\frac{27}{9}\right) = 0 \ .$$

Σχόλιο

Όπως αναφέραμε παραπάνω, η τιμή του συμβόλου του Jacobi $\left(\frac{a}{P}\right)$ *δεν μας πληροφορεί για το αν ο ακέραιος αριθμός* a *είναι τετραγωνικό υπόλοιπο του* P*. Αυτό συμβαίνει διότι, αν υποθέσουμε ότι*

$$P = p_1 p_2 \cdots p_\kappa \text{, όπου } \kappa = 2\lambda \text{, } \lambda \in \mathbb{N}$$

(χωρίς αναγκαστικά να ισχύει ότι οι πρώτοι $p_1, p_2, ..., p_\kappa$ *είναι διάφοροι μεταξύ τους)*

και $\left(\frac{a}{p_i}\right) = -1$ *, για κάθε* $i = 1, 2, ..., \kappa$ *, τότε*

$$\left(\frac{a}{P}\right) = (-1)^\kappa = 1 \ .$$

Αλλά, προφανώς, η ισοτιμία $x^2 \equiv a \pmod P$ *δεν έχει λύσεις διότι αν είχε λύσεις, τότε κάθε μια από τις ισοτιμίες* $x^2 \equiv a \pmod{p_i}$ *θα είχε λύση. Δηλαδή, θα ίσχυε ότι* $\left(\frac{a}{p_i}\right) = 1$*, για κάθε* $i = 1, 2, ..., \kappa$*. Άτοπο, λόγω της υπόθεσης.*

Όμως, αν ο ακέραιος αριθμός a *είναι τετραγωνικό υπόλοιπο του* P*, τότε (όμοια με παραπάνω) θα ισχύει ότι* $\left(\frac{a}{p_i}\right) = 1$*, για κάθε πρώτο διαιρέτη* p_i *του* P *και συνεπώς γνωρίζουμε πως το σύμβολο του Jacobi επιστρέφει την τιμή 1.*

Στην περίπτωση όπου $\left(\frac{a}{P}\right) = -1$*, γνωρίζουμε ότι ο* a *δεν είναι τετραγωνικό υπόλοιπο του* P*. Αν αυτό συνέβαινε, τότε κάθε ισοτιμία*

$$x^2 \equiv a \pmod{p_i},$$

όπου p_i *οι πρώτοι διαιρέτες του* P*, θα είχε λύση και τότε, προφανώς, θα είχαμε* $\left(\frac{a}{P}\right) = 1$*. Άτοπο.*

Έτσι, συγκεντρωτικά έχουμε

- *Αν* $\left(\frac{a}{P}\right) = 1$*, δεν μπορούμε να αποφανθούμε για το αν ο* a *είναι τετραγωνικό υπόλοιπο του* P*.*

- *Αν ο a είναι τετραγωνικό υπόλοιπο του P, τότε* $\left(\frac{a}{P}\right)=1$.
- *Αν* $\left(\frac{a}{P}\right)=-1$, *τότε ο a δεν είναι τετραγωνικό υπόλοιπο του P.*

Θεώρημα

Έστω a οποιοσδήποτε ακέραιος αριθμός που είναι πρώτος προς τους περιττούς θετικούς ακεραίους P,Q. Τότε ισχύει

$$\left(\frac{a}{PQ}\right)=\left(\frac{a}{P}\right)\left(\frac{a}{Q}\right).$$

ΑΠΟΔΕΙΞΗ

Έστω $P=p_1^{m_1}p_2^{m_2}...p_\kappa^{m_\kappa}$ και $Q=q_1^{b_1}q_2^{b_2}...q_\lambda^{b_\lambda}$, όπου $\kappa,\lambda\in\mathbb{N}$ οι κανονικές μορφές των P,Q, αντίστοιχα.

Τότε, από τον ορισμό του συμβόλου του Jacobi, λαμβάνουμε

$$\left(\frac{a}{PQ}\right)=\left(\frac{a}{p_1^{m_1}p_2^{m_2}...p_\kappa^{m_\kappa}q_1^{b_1}q_2^{b_2}...q_\lambda^{b_\lambda}}\right)$$

$$=\left(\frac{a}{p_1}\right)^{m_1}\left(\frac{a}{p_2}\right)^{m_2}...\left(\frac{a}{p_\kappa}\right)^{m_\kappa}\left(\frac{a}{q_1}\right)^{b_1}\left(\frac{a}{q_2}\right)^{b_2}...\left(\frac{a}{q_\lambda}\right)^{b_\lambda}$$

$$=\left(\frac{a}{P}\right)\left(\frac{a}{Q}\right).$$

■

Θεώρημα

Έστω a,b ακέραιοι αριθμοί που είναι πρώτοι προς τον θετικό περιττό ακέραιο αριθμό P. Τότε ισχύει

$$\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)=\left(\frac{ab}{P}\right).$$

ΑΠΟΔΕΙΞΗ

Έστω $P=p_1^{m_1}p_2^{m_2}...p_\kappa^{m_\kappa}$, $\kappa\in\mathbb{N}$, η κανονική μορφή του περιττού θετικού ακεραίου αριθμού P.

Τότε

$$\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)=\left(\frac{a}{p_1^{m_1}p_2^{m_2}...p_\kappa^{m_\kappa}}\right)\left(\frac{b}{p_1^{m_1}p_2^{m_2}...p_\kappa^{m_\kappa}}\right)$$

$$= \left(\frac{a}{p_1}\right)^{m_1}\left(\frac{a}{p_2}\right)^{m_2}\cdots\left(\frac{a}{p_\kappa}\right)^{m_\kappa}\left(\frac{b}{p_1}\right)^{m_1}\left(\frac{b}{p_2}\right)^{m_2}\cdots\left(\frac{b}{p_\kappa}\right)^{m_\kappa}$$

$$= \left[\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\right]^{m_1}\cdot\left[\left(\frac{a}{p_2}\right)\left(\frac{b}{p_2}\right)\right]^{m_2}\cdots\left[\left(\frac{a}{p_\kappa}\right)\left(\frac{b}{p_\kappa}\right)\right]^{m_\kappa}. \qquad (1)$$

Όμως, στην παράγραφο αναφορικά με το σύμβολο του Legendre αποδείξαμε πως αν p είναι ένας πρώτος αριθμός και a,b είναι ακέραιοι αριθμοί, τέτοιοι ώστε $(ab,p)=1$, τότε

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Έτσι, από τη σχέση (1) λαμβάνουμε ότι

$$\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)=\left(\frac{ab}{p_1}\right)^{m_1}\left(\frac{ab}{p_2}\right)^{m_2}\cdots\left(\frac{ab}{p_\kappa}\right)^{m_\kappa}$$

$$=\left(\frac{ab}{P}\right).$$

■

Πόρισμα

Έστω a ακέραιος αριθμός που είναι πρώτος προς τον περιττό θετικό ακέραιο P. Τότε ισχύει

$$\left(\frac{a^2}{P}\right)\left(\frac{a}{P^2}\right)=1\ .$$

ΑΠΟΔΕΙΞΗ

Από τα δύο παραπάνω θεωρήματα, που αποδείξαμε, προκύπτει ότι

$$\left(\frac{a}{P^2}\right)=\left(\frac{a}{P}\right)\left(\frac{a}{P}\right)$$

και

$$\left(\frac{a^2}{P}\right)=\left(\frac{a}{P}\right)\left(\frac{a}{P}\right).$$

Αλλά, είναι προφανές ότι $\left(\frac{a}{P}\right)\left(\frac{a}{P}\right)=1$ και επομένως

$$\left(\frac{a^2}{P}\right)=\left(\frac{a}{P^2}\right)=1\ .$$

■

Θεώρημα

Έστω a,b ακέραιοι αριθμοί, όπου ο a είναι πρώτος προς τον περιττό θετικό ακέραιο αριθμό P. Αν $a \equiv b(\mathrm{mod}\, P)$, τότε ισχύει

$$\left(\frac{a}{P}\right)=\left(\frac{b}{P}\right).$$

ΑΠΟΔΕΙΞΗ

Αν υποθέσουμε πως $P = p_1^{m_1} p_2^{m_2} ... p_\kappa^{m_\kappa}$, $\kappa \in \mathbb{N}$, είναι η κανονική μορφή του αριθμού P, τότε θα ισχύει ότι

$$a \equiv b(\mathrm{mod}\, p_i), \text{ για κάθε } i = 1, 2, ..., \kappa .$$

Όμως, στην παράγραφο που αναφέρεται στο σύμβολο του Legendre αποδείξαμε πως αν p είναι ένας πρώτος αριθμός, a ακέραιος αριθμός, τέτοιος ώστε $(a, p)=1$ και $a \equiv b(\mathrm{mod}\, p)$, τότε

$$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right).$$

Συνεπώς, σύμφωνα με τα παραπάνω, προκύπτει

$$\left(\frac{a}{p_i}\right)=\left(\frac{b}{p_i}\right), \text{ για κάθε } i = 1, 2, ..., \kappa .$$

Άρα

$$\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)^{m_1}\left(\frac{a}{p_2}\right)^{m_2} ... \left(\frac{a}{p_\kappa}\right)^{m_\kappa}$$

$$=\left(\frac{b}{p_1}\right)^{m_1}\left(\frac{b}{p_2}\right)^{m_2} ... \left(\frac{b}{p_\kappa}\right)^{m_\kappa} =\left(\frac{b}{P}\right).$$

Αυτό ολοκληρώνει την απόδειξη του θεωρήματος. ■

Θεώρημα

Έστω P περιττός θετικός ακέραιος. Τότε ισχύει

$$\left(-\frac{1}{P}\right)=(-1)^{\frac{P-1}{2}}.$$

ΑΠΟΔΕΙΞΗ

Έστω

$$P = p_1^{m_1} p_2^{m_2} ... p_\kappa^{m_\kappa}, \ \kappa \in \mathbb{N},$$

είναι η κανονική μορφή του περιττού θετικού ακεραίου P. Τότε, από τον ορισμό του συμβόλου του Jacobi έχουμε

$$\left(-\frac{1}{P}\right)=\left(\frac{-1}{p_1}\right)^{m_1}\left(\frac{-1}{p_2}\right)^{m_2}\cdots\left(\frac{-1}{p_\kappa}\right)^{m_\kappa} \tag{1}$$

Όμως, από το κριτήριο του Euler προκύπτει άμεσα ότι

$$\left(\frac{-1}{p_i}\right)=(-1)^{\frac{p_i-1}{2}},\ \text{για κάθε } i=1,2,...,\kappa,$$

καθώς καθένας από τους p_i είναι περιττός και συνεπώς μεγαλύτερος του 2.

Άρα, από τη σχέση (1) λαμβάνουμε ότι

$$\left(\frac{-1}{P}\right)=(-1)^{\sum_{i=1}^{\kappa}(p_i-1)m_i/2}$$

Έστω

$$p_1^{m_1}p_2^{m_2}\cdots p_\kappa^{m_\kappa}=q_1q_2\cdots q_\lambda,$$

όπου

$$\lambda=m_1+m_2+\cdots+m_\kappa \quad \text{και } q_1,q_2,...,q_\lambda\in\{p_1,p_2,...,p_\kappa\}$$

Τότε

$$\left(-\frac{1}{P}\right)=(-1)^{\sum_{j=1}^{\lambda}\left(q_j-1\right)/2}. \tag{2}$$

Όμως, ισχύει ότι

$$P=\prod_{j=1}^{\lambda}q_j=\prod_{j=1}^{\lambda}\left[1+(q_j-1)\right]$$

$$=1+\sum_{j=1}^{\lambda}(q_j-1)+4r,\ r\in\mathbb{N},$$

καθώς κάθε όρος q_j-1 είναι άρτιος αριθμός.

Συνεπώς

$$\frac{1}{2}(P-1)=\frac{1}{2}\sum_{j=1}^{\lambda}(q_j-1)+2r.$$

Επομένως, η σχέση (2) λαμβάνει την μορφή

$$\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}(-1)^{-2r}=(-1)^{\frac{P-1}{2}}.$$

Αυτό ολοκληρώνει την απόδειξη του θεωρήματος.

■

Θεώρημα

Έστω P περιττός θετικός ακέραιος. Τότε ισχύει

$$\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}.$$

ΑΠΟΔΕΙΞΗ

Ας υποθέσουμε, όπως στην προηγούμενη απόδειξη, ότι

$$P = p_1^{m_1} p_2^{m_2} \ldots p_\kappa^{m_\kappa} = q_1 q_2 \cdots q_\lambda ,$$

όπου

$$\lambda = m_1 + m_2 + \cdots + m_\kappa$$

και

$$q_1, q_2, \ldots, q_\lambda \in \{p_1, p_2, \ldots, p_\kappa\}.$$

Τότε

$$\left(\frac{2}{P}\right) = \left(\frac{2}{q_1}\right)\left(\frac{2}{q_2}\right) \ldots \left(\frac{2}{q_\lambda}\right). \tag{1}$$

Όμως, στην παράγραφο που αναφερθήκαμε στο σύμβολο του Legendre αποδείξαμε ότι αν ο p είναι περιττός πρώτος αριθμός, τότε

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} .$$

Έτσι, η σχέση (1) γίνεται

$$\left(\frac{2}{P}\right) = (-1)^{\sum_{i=1}^{\lambda} (q_i^2-1)/8} . \tag{2}$$

Αλλά

$$\frac{P^2-1}{8} = \frac{q_1^2 q_2^2 \ldots q_\lambda^2 - 1}{8}$$

$$= \frac{\left(1+8\cdot\frac{q_1^2-1}{8}\right)\left(1+8\cdot\frac{q_2^2-1}{8}\right)\ldots\left(1+8\cdot\frac{q_\lambda^2-1}{8}\right)-1}{8}. \tag{3}$$

Ο αριθμητής γράφεται ισοδύναμα στη μορφή

$$\left(1+8\cdot\frac{q_1^2-1}{8}\right)\left(1+8\cdot\frac{q_2^2-1}{8}\right)\ldots\left(1+8\cdot\frac{q_\lambda^2-1}{8}\right)-1$$

$$= 1 + \sum_{i=1}^{\lambda} \frac{8(q_i^2-1)}{8} + \left(\sum_{i\neq j} \frac{8(q_i^2-1)}{8} \cdot \frac{8(q_j^2-1)}{8} \right.$$

$$\left. + \sum_{i\neq j\neq\kappa} \frac{8(q_i^2-1)}{8} \cdot \frac{8(q_j^2-1)}{8} \cdot \frac{8(q_\kappa^2-1)}{8} + \cdots \right) - 1$$

$$= \sum_{i=1}^{\lambda} (q_i^2-1) + \left(\sum_{i\neq j} 8v_i \cdot 8v_j + \sum_{i\neq j\neq\kappa} 8v_i \cdot 8v_j \cdot 8v_\kappa + \cdots \right) \tag{4}$$

καθώς $q_i^2 = 8v_i + 1$, για κάποια τιμή του $v_i \in \mathbb{N}$.

Συνεπώς, η σχέση (3) μέσω της (4) λαμβάνει την ισοδύναμη μορφή

$$\frac{P^2-1}{8} = \sum_{i=1}^{\lambda} \frac{1}{8}(q_i^2-1) + 2r, \text{ για κάποιον } r \in \mathbb{N}$$

Επομένως, η σχέση (2) γίνεται

$$\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}(-1)^{-2r}=(-1)^{\frac{P^2-1}{8}}.$$

Αυτό ολοκληρώνει την απόδειξη του θεωρήματος.

■

Θεώρημα *(ΝΟΜΟΣ ΤΕΤΡΑΓΩΝΙΚΗΣ ΑΝΤΙΣΤΡΟΦΗΣ ΓΙΑ ΣΥΜΒΟΛΑ JACOBI)*
Έστω P,Q *περιττοί θετικοί ακέραιοι για τους οποίους ισχύει ότι* $(P,Q)=1$. *Τότε*

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

ΑΠΟΔΕΙΞΗ

Ας υποθέσουμε ότι $P=p_1p_2\cdots p_\lambda$, $\lambda\in\mathbb{N}$ (όπου οι πρώτοι αριθμοί $p_1,p_2,...,p_\lambda$ δεν είναι αναγκαστικά διάφοροι μεταξύ τους) και $Q=q_1q_2\cdots q_m$, $m\in\mathbb{N}$ (όπου οι πρώτοι αριθμοί $q_1,q_2,...,q_m$ δεν είναι αναγκαστικά διάφοροι μεταξύ τους).

Τότε ισχύει

$$\left(\frac{P}{Q}\right)=\prod_{i=1}^{m}\left(\frac{P}{q_i}\right)=\prod_{i=1}^{m}\prod_{j=1}^{\lambda}\left(\frac{p_j}{q_i}\right).$$

Ομοίως αληθεύει

$$\left(\frac{Q}{P}\right)=\prod_{j=1}^{\lambda}\left(\frac{Q}{p_j}\right)=\prod_{j=1}^{\lambda}\prod_{i=1}^{m}\left(\frac{q_i}{p_j}\right).$$

Συνεπώς

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=\prod_{j=1}^{\lambda}\prod_{i=1}^{m}\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right). \tag{1}$$

Όμως, από τον νόμο της τετραγωνικής αντιστροφής (για σύμβολα Legendre) γνωρίζουμε ότι

$$\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right)=(-1)^{\frac{p_j-1}{2}\cdot\frac{q_i-1}{2}}$$

Άρα, από την σχέση (1) προκύπτει

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=(-1)^{\sum_{j=1}^{\lambda}\sum_{i=1}^{m}\frac{1}{2}(p_j-1)\frac{1}{2}(q_i-1)}$$

$$=(-1)^{\sum_{j=1}^{\lambda}\frac{1}{2}(p_j-1)\sum_{i=1}^{m}\frac{1}{2}(q_i-1)} \tag{2}$$

Αλλά, κατά την απόδειξη του θεωρήματος

$$\left(-\frac{1}{P}\right)=(-1)^{\frac{P-1}{2}}$$

δείξαμε ότι

$$\frac{1}{2}(P-1)=\frac{1}{2}\sum_{j=1}^{\lambda}(p_j-1)+2r_1,\quad r_1\in\mathbb{N}.$$

Ομοίως, προκύπτει ότι

$$\frac{1}{2}(Q-1)=\frac{1}{2}\sum_{i=1}^{m}(q_i-1)+2r_2,\quad r_2\in\mathbb{N}.$$

Επομένως, η σχέση (2) γράφεται

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=(-1)^{-2r_1}(-1)^{-2r_2}(-1)^{\frac{1}{2}(P-1)\cdot\frac{1}{2}(Q-1)}$$

$$=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Αυτό ολοκληρώνει την απόδειξη του θεωρήματος.

■

6. Οι συναρτήσεις $\pi(x)$ και $li(x)$

Η συνάρτηση $\pi(x)$

Η συνάρτηση $\pi(x)$ εκφράζει το πλήθος των πρώτων αριθμών που δεν υπερβαίνουν τον πραγματικό αριθμό x.

Δεν υπάρχει ένας γνωστός τύπος που να προσδιορίζει την συνάρτηση $\pi(x)$. Αυτό συμβαίνει διότι, δεν έχουμε πλήρη γνώση για τον τρόπο με τον οποίο είναι κατανεμημένοι οι πρώτοι αριθμοί μέσα στους ακεραίους.

Είναι δυνατόν να αποδείξουμε, πως τα κενά μεταξύ διαδοχικών πρώτων αριθμών μπορεί να είναι οσοδήποτε μεγάλα. Κι αυτό γιατί, οποιονδήποτε φυσικό αριθμό n και αν θεωρήσουμε, πάντα θα υπάρχουν n στο πλήθος διαδοχικοί σύνθετοι αριθμοί.

Ας θεωρήσουμε την ακολουθία των διαδοχικών φυσικών αριθμών:

$$(n+1)!+2,(n+1)!+3,...,(n+1)!+n,(n+1)!+(n+1).$$

Κανένας από τους παραπάνω n διαδοχικούς φυσικούς αριθμούς δεν είναι πρώτος αφού

$$2\,|\,(n+1)!+2,3\,|\,(n+1)!+3,...,n\,|\,(n+1)!+n,(n+1)\,|\,(n+1)!+(n+1).$$

Έτσι αρχίζουμε να αντιλαμβανόμαστε ότι το πρόβλημα της κατανομής των πρώτων αριθμών είναι ένα πραγματικά σύνθετο ερώτημα και κατ' επέκταση ότι ο προσδιορισμός της $\pi(x)$ είναι πολύπλοκος.

Στην συνάρτηση αυτή βασίζεται ένα από τα πλέον φημισμένα θεωρήματα της Θεωρίας Αριθμών, το **Θεώρημα των Πρώτων Αριθμών** *(The Prime Number Theorem).*

Σύμφωνα με το θεώρημα αυτό, η συνάρτηση $\pi(x)$ είναι ασυμπτωτικά ίση προς την συνάρτηση $x/\log x$, δηλαδή

$$\pi(x)\sim\frac{x}{\log x}\quad(x\to\infty).$$

Μια συνεπαγωγή του Θεωρήματος των Πρώτων Αριθμών είναι το ακόλουθο θεώρημα:

Οποιουσδήποτε θετικούς πραγματικούς αριθμούς a,b και αν θεωρήσουμε, όπου $a<b$, θα υπάρχει τουλάχιστον ένας πρώτος αριθμός μεταξύ των ac και bc, για κατάλληλα μεγάλες τιμές του c.

Η συνάρτηση $li(x)$

Όπως αναφέραμε προηγούμενα, ένας προσεγγιστικός τύπος της $\pi(x)$ είναι ο

$$\pi(x)\sim\frac{x}{\log x}\quad(\textit{Θεώρημα των Πρώτων Αριθμών}).$$

Όμως, η συνάρτηση $\pi(x)$ μπορεί να προσεγγιστεί ακόμη καλύτερα από την συνάρτηση που ορίζεται ως εξής

$$\ell i(x)=\int_2^x\frac{dt}{\log t},$$

καθώς το πηλίκο $\pi(x)/\ell i(x)$ τείνει στο 1 πιο γρήγορα από το πηλίκο $\pi(x)\ell og(x)/x$.

Παρατήρηση

Στη βιβλιογραφία χρησιμοποιούνται επίσης οι συμβολισμοί

$$Li(x)=\int_2^x \frac{dt}{\log t}\ ,\quad \ell i(x)=\int_0^x \frac{dt}{\log t}\ .$$

Ο P. Chebyshev είχε αποδείξει πως αν το όριο $\lim\limits_{x\to\infty}\dfrac{\pi(x)}{x/\log x}$ υπάρχει, τότε θα είναι αναγκαστικά ίσο με 1. Όταν οι J. Hadamard και C. J. de la Vallée – Poussin ολοκλήρωσαν την απόδειξη, έδειξαν πως για κάποιον θετικό αριθμό *C* ισχύει ότι:

$$\pi(x)=li(x)+O\left(xe^{-C\sqrt{\log x}}\right)\ .$$

Από την σχέση αυτή προκύπτει ότι:

$$\left|\pi(x)-li(x)\right|=O\left(\frac{x}{\log^m x}\right),\ \text{για κάθε}\ m>0\ .$$

Άλλες χρήσιμες ιδιότητες της $li(x)$ είναι οι εξής:

$$li(x)\sim\frac{x}{\log x}\quad \text{(εφαρμόζοντας τον κανόνα του L' Hôpital),}$$

$$li(x)=\frac{x}{\log x}+\frac{x}{\log^2 x}+O\left(\frac{x}{\log^3 x}\right).$$

Κατόπιν αριθμητικών υπολογισμών, η $li(x)$ παρουσιάζεται στην αρχή σαν μια "υπερεκτίμηση" της $\pi(x)$, όπως φαίνεται στον πίνακα παρακάτω.

x	$\pi(x)$	$li(x)-\pi(x)$
10^8	5761455	753
10^9	50847534	1700
10^{10}	455052511	3103
10^{11}	4118054813	11587
10^{12}	37607912018	38262
10^{13}	346065536839	108970
10^{14}	3204941750802	314889
10^{15}	29844570422669	1052618
10^{16}	279238341033925	3214631
10^{17}	2623557157654233	7956588
10^{18}	24739954287740860	21949554
10^{19}	234057667276344607	99877774
10^{20}	2220819602560918840	222744643

Όμως, το έτος 1914 ο J.E. Littlewood απέδειξε πως η διαφορά $\pi(x)-li(x)$ αλλάζει πρόσημο

άπειρες φορές. Αργότερα, το έτος 1933, ένας από τους μαθητές του Littlewood, ο Skewes, απέδειξε πως η πρώτη αλλαγή προσήμου πρέπει αναγκαστικά να συμβαίνει για

$$x < 10^{10^{10^{79}}}.$$

Αυτό το άνω φράγμα έχει ελαττωθεί αισθητά από έρευνες που ακολούθησαν, αλλά ακόμα βρίσκεται στην περιοχή του 10^{316}.

x	$\pi(x)$	$x/\log x$	$\pi(x)/\frac{x}{\log x}$	$li(x)$	$\pi(x)/li(x)$
10^3	168	144.8	1.160	178	0.9438202
10^4	1229	1085.7	1.132	1246	0.9863563
10^5	9592	8685.9	1.104	9630	0.9960540
10^6	78498	72382.4	1.085	78628	0.9983466
10^7	664579	620420.7	1.071	664918	0.9998944
10^8	5761455	5428681.0	1.061	5762209	0.9998691
10^9	50847534	48254942.4	1.054	50849235	0.9999665
10^{10}	455052512	434294481.9	1.048	455055614	0.9999932
10^{11}	4118054813	3948131663.7	1.043	4118165401	0.9999731
10^{12}	37607912018	36191206825.3	1.039	37607950281	0.9999990

Εικασία

Για κάθε πρώτο αριθμό p μεγαλύτερο του δύο, υπάρχουν δύο πρώτοι αριθμοί $p_1, p_2 (p_1 < p_2)$, τέτοιοι, ώστε

$$p = \frac{p_1 + p_2 + 1}{p_1} \quad .$$

Η εικασία μπορεί επίσης να διατυπωθεί ως εξής:

Για κάθε πρώτο αριθμό p μεγαλύτερο του δύο, υπάρχουν δύο πρώτοι αριθμοί $p_1, p_2 (p_1 < p_2)$ τέτοιοι, ώστε οι αριθμοί $(p-1)p_1, p_2$ να είναι διαδοχικοί ακέραιοι
(Μιχαήλ Θ. Ρασσιάς, *Octogon Mathematical Magazine 13 (1B) (2005), σελ. 885.*
Βλέπε, επίσης, Problem 25, Newsletter, European Mathematical Society, 65 (2007), σελ. 47).

7. Η συνάρτηση ζήτα του Riemann

Η **συνάρτηση ζήτα** ορίζεται ως

$$\zeta(s)=\sum_{n=1}^{+\infty}\frac{1}{n^s}$$

για πραγματικές τιμές του s, $s>1$.

Η συνάρτηση ορίστηκε για πρώτη φορά το έτος 1737 από τον Leonhard Euler (1707 – 1783). Το έτος 1859, ο Georg Bernhard Riemann (1826 – 1866) χρησιμοποίησε την συνάρτηση αυτή στην προσπάθειά του να αποδείξει το Θεώρημα των Πρώτων Αριθμών. Θεώρησε μιγαδικές τιμές του s και απέδειξε κάποιες βασικές ιδιότητες της $\zeta(s)$. Ο Riemann παρουσίασε έξι υποθέσεις στην εργασία του .

Αξιοποιώντας τις υποθέσεις αυτές, απέδειξε τό Θεώρημα των Πρώτων Αριθμών. Όμως, μέχρι σήμερα, μόνο οι πέντε από αυτές τις υποθέσεις έχουν αποδειχθεί. Η έκτη παραμένει ανοικτό πρόβλημα και είναι γνωστή ως υπόθεση του Riemann (Riemann hypothesis).

Η διατύπωση της υπόθεσης αυτής είναι η εξής:

«*Οι μη–τετριμμένες ρίζες της συνάρτησης* $\zeta(s)$*, όπου* $s\in\mathbb{C}$ *, έχουν πραγματικό μέρος ίσο με 1/2 (δηλ.* $\mathrm{Re}(s)=1/2$ *»**.

Με τον όρο «τετριμμένες ρίζες» εννοούμε τους αρνητικούς άρτιους ακεραίους.

Θα παρουσιάσουμε τώρα τα βασικά βήματα της εργασίας του Riemann, ώστε να γίνει κατανοητή η σχέση της συνάρτησης $\zeta(s)$ με την κατανομή των πρώτων αριθμών.

Αρχικά, ο Riemann έθεσε

$$J(x)=\sum_{\kappa=1}^{+\infty}\frac{1}{\kappa}\pi\left(x^{1/\kappa}\right)$$

(οι όροι της παραπάνω σειράς μηδενίζονται για κάθε $\kappa\geq\kappa_0$, για κάποια θετική ακέραια τιμή του κ_0, διότι $\pi(x)=0$ για κάθε $x<2$).

Στην συνέχεια, απέδειξε πως

$$\pi(x)=\sum_{\kappa=1}^{+\infty}\frac{1}{\kappa}\mu(\kappa)J\left(x^{1/\kappa}\right), \tag{1}$$

όπου $\mu(\kappa)$ είναι η γνωστή συνάρτηση του Möbius.

Όμως

$$J(x)=li(x)-\sum_{\rho}li(x^{\rho})-\log 2+\int_x^{+\infty}\frac{dt}{t(t^2-1)\log t} \tag{2}$$

---

* Στην εργασία του ο Riemann θεώρησε την συνάρτηση

$\xi(t)=\frac{1}{2}s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$, όπου $s=\frac{1}{2}+it$ και $\Gamma(s)$ η γνωστή συνάρτηση Γάμμα. Υπέθεσε πως όλες οι ρίζες της συνάρτησης $\xi(t)$ είναι πραγματικές. Αυτή είναι η υπόθεση του Riemann με ισοδύναμη διατύπωση αυτή που παρουσιάσαμε παραπάνω.

όπου το άθροισμα

$$\sum_{\rho} li\left(x^{\rho}\right)$$

εκτείνεται σ' όλες τις μη–τετριμμένες ρίζες της συνάρτησης $\zeta(s)$.

Συγκρίνοντας, λοιπόν, τις σχέσεις (1) και (2) καταλαβαίνουμε ότι μπορεί να προκύψει ένας τύπος για την $\pi(x)$ που να εξαρτάται από σαφώς καθορισμένες συναρτήσεις και τις μη–τετριμμένες ρίζες της $\zeta(s)$. Εδώ μπορεί να δει κανείς την πολύ μεγάλη «πρακτική» σημασία της υπόθεσης Riemann.

ΒΑΣΙΚΕΣ ΙΔΙΟΤΗΤΕΣ ΤΗΣ ΣΥΝΑΡΤΗΣΗΣ $\zeta(s)$

Θα αποδείξουμε τώρα κάποιες βασικές ιδιότητες της συνάρτησης ζήτα για πραγματικές τιμές της μεταβλητής s.

- ΤΑΥΤΟΤΗΤΑ EULER

$$\zeta(s)=\prod_{p}\frac{1}{1-p^{-s}},\ \ s>1,$$

όπου το γινόμενο εκτείνεται σε όλους τους πρώτους αριθμούς p.

Η ιδέα για την απόδειξη της παραπάνω ταυτότητας είναι:

$$\prod_{p}\frac{1}{1-p^{-s}}=\frac{1}{1-p_1^{-s}}\cdot\frac{1}{1-p_2^{-s}}\cdots\frac{1}{1-p_{\kappa}^{-s}}\cdots$$

$$=\left(1+\frac{1}{p_1^{s}}+\frac{1}{p_1^{2s}}+\cdots\right)\cdot\left(1+\frac{1}{p_2^{s}}+\frac{1}{p_2^{2s}}+\cdots\right)\cdots\left(1+\frac{1}{p_{\kappa}^{s}}+\frac{1}{p_{\kappa}^{2s}}+\cdots\right)\cdots,\kappa\in\mathbb{N}$$

Παρατηρούμε, όμως, ότι κάνοντας τις πράξεις στο παραπάνω γινομενο, θα εμφανιστούν όροι της μορφής:

$$\frac{1}{\left(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_{\lambda}^{\alpha_{\lambda}}\right)^{s}},\ \text{όπου}\ \lambda\in\mathbb{N}$$

από μια φορά ο καθένας.

Βέβαια, από το *θεμελιώδες θεώρημα της Αριθμητικής* γνωρίζουμε ότι κάθε θετικός ακέραιος μπορεί να αναπαρασταθεί ως γινόμενο δυνάμεων πρώτων παραγόντων κατά μοναδικό τρόπο.

Έτσι, προκύπτει ότι

$$\prod_{p}\frac{1}{1-p^{-s}}=\sum_{n\geq 1}\frac{1}{n^{s}}\ ,\ \mathrm{s}>1$$

ή

$$\zeta(s)=\prod_{p}\frac{1}{1-p^{-s}},\ \mathrm{s}>1\ .$$

■

Σχόλιο

Η παραπάνω ταυτότητα παρουσιάστηκε για πρώτη φορά στο βιβλίο του Euler, «Introductio in Analysin Infinitorum», *το οποίο δημοσιεύτηκε το έτος 1748. Εφαρμόζοντας την ταυτότητα αυτή προκύπτει άμεσα ότι*

$$\frac{\zeta(2s)}{\zeta(s)} = \prod_p \frac{1}{1+p^{-s}} \ .$$

- ***Ισχύει ότι***

$$\frac{1}{s-1} = \int_1^{+\infty} \frac{1}{x^s}\,dx \le \zeta(s) \le 1 + \int_1^{+\infty} \frac{1}{x^s}\,dx = 1 + \frac{1}{s-1}$$

και άρα η συνάρτηση $\zeta(s)$ συγκλίνει σε πραγματικό αριθμό, για $s>1$.

ΑΠΟΔΕΙΞΗ

Αρχικά, θα αποδείξουμε πως για μια μη αρνητική, συνεχή και φθίνουσα συνάρτηση f, της ανεξαρτήτου μεταβλητής x, που ορίζεται στο διάστημα $[1,+\infty)$, ισχύει ότι

$$\int_1^{+\infty} f(x)\,dx \le S \le a_1 + \int_1^{+\infty} f(x)\,dx \ ,$$

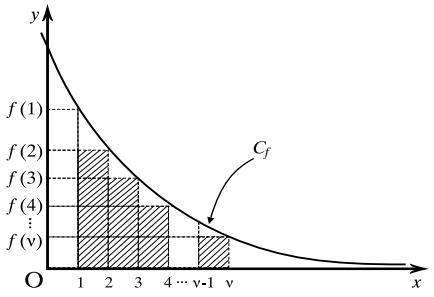
όπου

$$a_\nu = f(\nu)$$

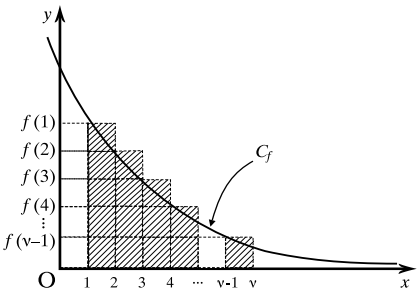
και

$$S = \lim_{\nu\to+\infty} S_\nu = \lim_{\nu\to+\infty} \left(f(1)+f(2)+\cdots+f(\nu)\right), \text{ για } \nu\in\mathbb{N}.$$

Γι'αυτό το σκοπό, θεωρούμε μια υποδιαίρεση του διαστήματος $[1,\nu]$ όπως φαίνεται στα δύο παρακάτω σχήματα.



Σχ. 1



Σχ. 2

Παρατηρούμε ότι στο Σχ. 1 σχηματίζεται ένα σύνολο εγγεγραμμένων ορθογώνιων παραλληλογράμμων. Έτσι, το εμβαδόν του γραμμοσκιασμένου χωρίου στο Σχ. 1 είναι ίσο με

$$\sum_{\kappa=2}^{\nu} f(\kappa).$$

Ομοίως, στο Σχ. 2 σχηματίζεται ένα σύνολο περιγεγραμμένων ορθογωνίων παραλληλογράμμων.

Συνεπώς, το εμβαδόν του γραμμοσκιασμένου χωρίου στο Σχ. 2 είναι ίσο με

$$\sum_{\kappa=1}^{\nu-1} f(\kappa).$$

Όπως συμπεραίνουμε από τα Σχήματα 1 και 2 είναι προφανές ότι

$$\sum_{\kappa=2}^{\nu} f(\kappa) \le \int_1^{\nu} f(x)\,dx \le \sum_{\kappa=1}^{\nu-1} f(\kappa) \ .$$

Όμως,

$$S_\nu = f(1)+f(2)+\cdots+f(\nu) \ .$$

Άρα,

$$S_\nu - f(1) \le \int_1^{\nu} f(x)\,dx \ \le \ S_{\nu-1}$$

ή

$$\lim_{\nu\to+\infty}\left(S_\nu - f(1)\right) \le \lim_{\nu\to+\infty}\int_1^{\nu} f\,(x)dx \le \lim_{\nu\to+\infty} S_{\nu-1}$$

ή

$$S - f(1) \le \int_1^{+\infty} f(x)\,dx \le S \ .$$

Επομένως

$$\int_1^{+\infty} f(x)\,dx \le S \le f(1)+\int_1^{+\infty} f(x)\,dx \ .$$

Δηλαδή

$$\int_1^{+\infty} f(x)\,dx \le S \le a_1+\int_1^{+\infty} f(x)\,dx \ .$$

Έτσι, για την περίπτωση της συνάρτησης $\zeta(s)$ ισχύει

$$\int_1^{+\infty} \frac{1}{x^s}\,dx \le \lim_{\nu\to+\infty}\left(\frac{1}{1^s}+\frac{1}{2^s}+\cdots+\frac{1}{\nu^s}\right) \le \frac{1}{1^s}+\int_1^{+\infty}\frac{1}{x^s}\,dx$$

Αλλά

$$\int_1^{+\infty}\frac{1}{x^s}dx = \frac{1}{s-1}$$

και

$$\lim_{\nu\to+\infty}\left(\frac{1}{1^s}+\frac{1}{2^s}+\cdots+\frac{1}{\nu^s}\right) = \sum_{\nu\ge1}\frac{1}{\nu^s} \ .$$

Συνεπώς,

$$\frac{1}{s-1} = \int_1^{+\infty}\frac{1}{x^s}dx \le \zeta(s) \le 1+\int_1^{+\infty}\frac{1}{x^s}\,dx = 1+\frac{1}{s-1} \ .$$

■

• ***Η σειρά*** $\sum_{n\geq 1}\frac{1}{n^2}$ ***συγκλίνει στο*** $\mathbb{R}$ ***και μάλιστα ισχύει ότι***

$$\zeta(2)=\frac{\pi^2}{6}\,.$$

(Αυτή η σχέση είναι γνωστή και σαν *πρόβλημα της Basel).*

ΑΠΟΔΕΙΞΗ

– Αρχικά θα αποδείξουμε πως η σειρά

$$\sum_{n\geq 1}\frac{1}{n^2}$$

συγκλίνει στο $\mathbb{R}$.

Είναι

$$\sum_{n\geq 1}\frac{1}{n^2}<1+\sum_{n\geq 2}\frac{1}{(n-1)n}=1+\sum_{n\geq 2}\left(\frac{1}{n-1}-\frac{1}{n}\right)=2\,.$$

Επομένως

$$\sum_{n\geq 1}\frac{1}{n^2}<2\,.$$

Άρα , η σειρά

$$\sum_{n\geq 1}\frac{1}{n^2}$$

συγκλίνει στο $\mathbb{R}$.

– Θα αποδείξουμε ότι

$$\zeta(2)=\frac{\pi^2}{6}\,.$$

Ο σκοπός μας είναι να κατασκευάσουμε τη σειρά $\sum_{n\geq 1}\frac{1}{n^2}$ και να την φράξουμε από κάτω και από πάνω από το ίδιο όριο. Για να το κάνουμε αυτό, θα αξιοποιήσουμε την γνωστή ανισότητα

$$\cot^2 x<\frac{1}{x^2}<\csc^2 x\,,\ \text{για}\ 0<x<\frac{\pi}{2}\,.$$

Η ανισότητα αυτή ισχύει καθώς

(i) $$|\sin x|<|x|\Rightarrow \sin^2 x<x^2\Rightarrow \frac{1}{\sin^2 x}>\frac{1}{x^2}\,.$$

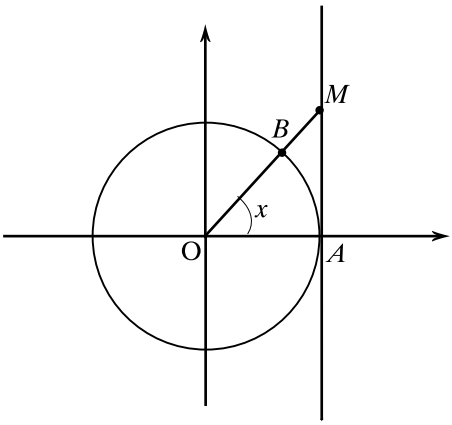
Άρα

$$\csc^2 x>\frac{1}{x^2}\,.$$

(ii) Είναι

$$x<\tan x\ \ \text{για}\ \ 0<x<\frac{\pi}{2}$$

διότι αν θεωρήσουμε τον μοναδιαίο τριγωνομετρικό κύκλο έχουμε:



Το εμβαδόν του κυκλικού τομέα OAB είναι μικρότερο από το εμβαδόν του τριγώνου OAM. Επομένως

$$\frac{1}{2}(OA)x < \frac{1}{2}(OA)(AM).$$

Άρα

$$x < (AM).$$

Όμως, $(AM) = \tan x$. Δηλαδή $x < \tan x$, για $0 < x < \frac{\pi}{2}$.

Επομένως, από τα (i) και (ii) συνεπάγεται

$$\cot^2 x < \frac{1}{x^2} < \csc^2 x, \text{ για } 0 < x < \frac{\pi}{2}. \tag{1}$$

Αλλά

$$\frac{\cos(nx) + i\sin(nx)}{(\sin x)^n} = \frac{(\cos x + i\sin x)^n}{(\sin x)^n} \text{ (από τον τύπο του De Moivre)}$$

$$= (\cot x + i)^n = \binom{n}{0}\cot^n x + \binom{n}{1}\cot^{n-1} x \cdot i + \binom{n}{2}\cot^{n-2} x \cdot i^2$$

$$+ \binom{n}{3}\cot^{n-3} x \cdot i^3 + \cdots + \binom{n}{n-1}\cot x \cdot i^{n-1} + \binom{n}{n} i^n$$

$$= \left[\binom{n}{0}\cot^n x - \binom{n}{2}\cot^{n-2} x + \cdots\right] + i\left[\binom{n}{1}\cot^{n-1} x - \binom{n}{3}\cot^{n-3} x + \cdots\right]$$

Άρα,

$$\frac{\sin(nx)}{(\sin x)^n} = \left[\binom{n}{1}\cot^{n-1} x - \binom{n}{3}\cot^{n-3} x + \cdots\right].$$

Θέτουμε

$$n = 2m+1 \text{ και } x = \frac{r\pi}{2m+1} \text{ με } r = 1,2,...,m.$$

Τότε $nx = r\pi$. Δηλαδή, $\dfrac{\sin(nx)}{(\sin x)^n} = 0$ για όλες αυτές τις τιμές του x.

Έτσι

$$\binom{2m+1}{1}\cot^{2m} x - \binom{2m+1}{3}\cot^{2m-2} x + \cdots = 0.$$

Επομένως

$$\binom{2m+1}{1}\left(\cot^2 x\right)^m - \binom{2m+1}{3}\left(\cot^2 x\right)^{m-1} + \cdots = 0$$

για κάθε τιμή του x με $x = \dfrac{r\pi}{2m+1}$, όπου $r = 1,\ 2,\ ...,m$.

Συνεπώς, το πολυώνυμο

$$p(t) = \binom{2m+1}{1}t^m - \binom{2m+1}{3}t^{m-1} + \cdots,$$

έχει ως m ρίζες τις $\cot^2 x$, για τις διάφορες τιμές του x (που είναι m στο πλήθος, καθώς $r = 1,2,...,m$).

Επομένως, από τις σχέσεις ριζών και συντελεστών πολυωνύμου (τύποι Viète), προκύπτει:

$$\cot^2\left(\frac{\pi}{2m+1}\right) + \cot^2\left(\frac{2\pi}{2m+1}\right) + \cdots + \cot^2\left(\frac{m\pi}{2m+1}\right) = \frac{\binom{2m+1}{3}}{\binom{2m+1}{1}}$$

$$= \frac{(2m+1)!}{3!(2m-2)!}\frac{(2m)!}{(2m+1)!} = \frac{2m(2m-1)}{6}$$

$$\Leftrightarrow \cot^2\left(\frac{\pi}{2m+1}\right) + \cot^2\left(\frac{2\pi}{2m+1}\right) + \cdots + \cot^2\left(\frac{m\pi}{2m+1}\right) = \frac{2m(2m-1)}{6} \quad . \tag{2}$$

Αλλά $\csc^2 x = \cot^2 x + 1$, συνεπώς, από την σχέση (2) λαμβάνουμε ότι:

$$\csc^2\left(\frac{\pi}{2m+1}\right) + \csc^2\left(\frac{2\pi}{2m+1}\right) + \cdots + \csc^2\left(\frac{m\pi}{2m+1}\right) - m = \frac{2m(2m-1)}{6}$$

$$\Leftrightarrow \csc^2\left(\frac{\pi}{2m+1}\right) + \csc^2\left(\frac{2\pi}{2m+1}\right) + \cdots + \csc^2\left(\frac{m\pi}{2m+1}\right) = \frac{2m(2m-1)}{6} + \frac{2\cdot 3m}{6}$$

$$= \frac{2m(2m+2)}{6}.$$

Οπότε, τελικά έχουμε

$$\csc^2\left(\frac{\pi}{2m+1}\right) + \csc^2\left(\frac{2\pi}{2m+1}\right) + \cdots + \csc^2\left(\frac{m\pi}{2m+1}\right) = \frac{2m(2m+2)}{6} \tag{3}$$

Από τις σχέσεις (2), (3) και την ανισότητα (1) συνεπάγεται

$$\cot^2\left(\frac{\pi}{2m+1}\right)+\cot^2\left(\frac{2\pi}{2m+1}\right)+\cdots+\cot^2\left(\frac{m\pi}{2m+1}\right)$$

$$<\frac{(2m+1)^2}{\pi^2}+\frac{(2m+1)^2}{2^2\pi^2}+\cdots+\frac{(2m+1)^2}{m^2\pi^2}$$

$$<\csc^2\left(\frac{\pi}{2m+1}\right)+\csc^2\left(\frac{2\pi}{2m+1}\right)+\cdots+\csc^2\left(\frac{m\pi}{2m+1}\right).$$

Άρα

$$\frac{2m(2m-1)}{6}<\frac{(2m+1)^2}{\pi^2}\sum_{n=1}^{m}\frac{1}{n^2}<\frac{2m(2m+2)}{6}.$$

Συνεπώς

$$\frac{\pi^2}{6}\frac{2m(2m-1)}{(2m+1)^2}<\sum_{n=1}^{m}\frac{1}{n^2}<\frac{\pi^2}{6}\frac{2m(2m+2)}{(2m+1)^2}.$$

Επομένως

$$\frac{\pi^2}{6}\lim_{m\to+\infty}\frac{2m(2m-1)}{(2m+1)^2}\le\sum_{n=1}^{+\infty}\frac{1}{n^2}\le\frac{\pi^2}{6}\lim_{m\to+\infty}\frac{2m(2m+2)}{(2m+1)^2},$$

δηλαδή

$$\frac{\pi^2}{6}\lim_{m\to+\infty}\frac{4m^2}{4m^2}\le\zeta(2)\le\frac{\pi^2}{6}\lim_{m\to+\infty}\frac{4m^2}{4m^2}$$

ή

$$\frac{\pi^2}{6}\le\zeta(2)\le\frac{\pi^2}{6}$$

Άρα

$$\zeta(2)=\frac{\pi^2}{6}.$$

■

Σχόλια

— Η παραπάνω απόδειξη οφείλεται στον Ιωάννη Παπαδημητρίου και αποτελεί μια από τις πλέον στοιχειώδεις αποδείξεις του θεωρήματος αυτού.

Το πρόβλημα υπολογισμού της $\zeta(2)$ τέθηκε για πρώτη φορά το 1644 από τον Pietro Mengoli. Ο πρώτος μαθηματικός που παρουσίασε λύση του παραπάνω προβλήματος ήταν ο Euler το 1735 (σε ηλικία 28 ετών). Ορισμένες ιδέες του Euler σχετικά με κάποιες γενικεύσεις του προβλήματος αυτού αξιοποιήθηκαν αργότερα από τον Riemann στην εργασία που δημοσίευσε το 1859.

Η ονομασία «το πρόβλημα της Basel» *προέρχεται από την Βασιλεία, τόπο γέννησης του Euler.*

— Ο Euler έλυσε το πρόβλημα θεωρώντας την σχέση

$$\frac{\sin x}{x}=\frac{x-\frac{x^3}{3!}+\frac{x^5}{5!}+\cdots}{x}=1-\frac{x^2}{3!}+\frac{x^4}{5!}-\cdots,$$

οπότε ο συντελεστής του x^2 *είναι ο αριθμός* $-\frac{1}{6}$*.Οι ρίζες της συνάρτησης* $\frac{\sin x}{x}$ *είναι οι αριθμοί* $\pm\pi,\ \pm 2\pi,\ \pm 3\pi, \ldots$.

Ο Euler αντιμετώπισε την συνάρτηση $\frac{\sin x}{x}$ *ως πολυώνυμο και έγραψε*

$$\frac{\sin x}{x} = \left(1-\frac{x}{\pi}\right)\left(1+\frac{x}{\pi}\right)\left(1-\frac{x}{2\pi}\right)\left(1+\frac{x}{2\pi}\right)\left(1-\frac{x}{3\pi}\right)\left(1+\frac{x}{3\pi}\right)\cdots$$

$$= \left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{2^2\pi^2}\right)\left(1-\frac{x^2}{3^2\pi^2}\right)\cdots$$

Αν εκτελέσουμε τις πράξεις, προκύπτει ότι ο συντελεστής του x^2 *είναι ο αριθμός*

$$-\frac{1}{\pi^2}\left(1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots\right).$$

Άρα

$$-\frac{1}{\pi^2}\left(1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots\right)=-\frac{1}{6}\ .$$

Επομένως

$$\zeta(2)=\frac{\pi^2}{6}\cdot$$

- Ένα σημαντικό συμπέρασμα είναι πως η συνάρτηση $\zeta(s)$ συγκλίνει σε ρητό πολλαπλάσιο του π^s, για κάθε άρτιο αριθμό $s \geq 2$. Ο Euler απέδειξε ότι

$$\zeta(2n)=\sum_{\kappa=1}^{+\infty}\frac{1}{\kappa^{2n}}=(-1)^{n-1}\frac{(2\pi)^{2n}\cdot B_{2n}}{2(2n)!},$$

όπου με B_n συμβολίζουμε τους **αριθμούς Bernoulli,** οι οποίοι μπορούν να οριστούν από τον αναδρομικό τύπο:

$$B_0=1,\quad B_n=\sum_{s=0}^{n}\binom{n}{s}B_s,\ \text{για}\ n\geq 2$$

$$(B_0=1, B_1=-1/2, B_2=1/6\ , B_4=-1/30, B_6=1/42, B_8=-1/30,\ B_{10}=5/66,\ldots)$$

Έτσι

$$\zeta(2)=\frac{\pi^2}{6}$$

$$\zeta(4)=\frac{\pi^4}{90}$$

$$\zeta(6)=\frac{\pi^6}{945}$$

$$\zeta(8)=\frac{\pi^8}{9450}$$

$$\zeta(10)=\frac{\pi^{10}}{93555}$$
$$\vdots$$

Το έτος 1979, ο Roger Apéry απέδειξε πως ο αριθμός $\zeta(3)$ είναι άρρητος.

Ανοιχτό Πρόβλημα

Να εξεταστεί αν υπάρχουν άλλοι περιττοί ακέραιοι s, όπου $s \geq 5$, τέτοιοι ώστε η σειρά $\zeta(s)$ να συγκλίνει σε άρρητο αριθμό.

Είναι

$$\zeta(3)=1{,}202056903\cdots$$
$$\zeta(5)=1{,}036927755\cdots$$
$$\zeta(7)=1{,}008349277\cdots$$
$$\zeta(9)=1{,}002008392\cdots$$

ΕΦΑΡΜΟΓΕΣ

1) ***Κάνοντας χρήση της συνάρτησης*** $\zeta(s)$***, να δειχθεί ότι υπάρχουν άπειροι πρώτοι αριθμοί.***

ΑΠΟΔΕΙΞΗ

Έστω πως οι πρώτοι αριθμοί είναι πεπερασμένοι στο πλήθος. Τότε, το γινόμενο

$$\prod_p \frac{1}{1-\frac{1}{p^s}},$$

το οποίο εκτείνεται σ' όλους τους πρώτους αριθμούς *p,* θα συγκλίνει σε πραγματικό αριθμό. Άρα και στην περίπτωση όπου $s \to 1^+$, το γινόμενο θα συγκλίνει σε πραγματικό αριθμό.

Όμως, από την ταυτότητα του Euler προκύπτει:

$$\lim_{s\to 1^+}\prod_p \frac{1}{1-p^{-s}} = \lim_{s\to 1^+}\sum_{n=1}^{+\infty}\frac{1}{n^s} = +\infty,$$

το οποίο είναι άτοπο.

■

2) ***Κάνοντας χρήση της συνάρτησης*** $\zeta(s)$***, να δειχθεί ότι η σειρά*** $\sum_p \frac{1}{p}$ ***,***

η οποία εκτείνεται σ' όλους τους πρώτους αριθμούς p ***, αποκλίνει, δηλ. απειρίζεται θετικά.***

Υπόδειξη: Ισχύει ότι

$$\log\frac{1}{1-p^{-s}} = \sum_{n=1}^{+\infty}\frac{1}{np^{ns}},\ \text{όπου}\ s>1.$$

ΑΠΟΔΕΙΞΗ

Γνωρίζουμε ότι $\lim\limits_{s\to 1^+}\zeta(s)=+\infty$. Άρα, θα ισχύει, επίσης, ότι:

$$\lim_{s\to 1^+}(\log\zeta(s))=+\infty .$$

Όμως,

$$\log\zeta(s)=\log\left(\sum_{n\geq 1}\frac{1}{n^s}\right)=\log\left(\prod_p\frac{1}{1-p^{-s}}\right)$$

$$=\sum_p\log\frac{1}{1-p^{-s}}$$

$$=\sum_p\sum_{n=1}^{+\infty}\frac{1}{np^{ns}}=\sum_p\left(\frac{1}{p^s}+\sum_{n=2}^{+\infty}\frac{1}{np^{ns}}\right).$$

Άρα,

$$\log\zeta(s)=\sum_p\frac{1}{p^s}+\sum_p\sum_{n=2}^{+\infty}\frac{1}{np^{ns}}.$$

Συνεπώς,

$$\log\zeta(s)<\sum_p\frac{1}{p^s}+\sum_p\sum_{n=2}^{+\infty}\frac{1}{p^{ns}}.$$

Αλλά, η σειρά

$$\sum_{n=2}^{+\infty}\frac{1}{p^{ns}}$$

αποτελεί άθροισμα φθίνουσας γεωμετρικής προόδου απείρων όρων με πρώτο όρο $\frac{1}{p^{2s}}$ και λόγο $\frac{1}{p^s}$.

Επομένως,

$$\log\zeta(s)<\sum_p\frac{1}{p^s}+\sum_p\frac{\frac{1}{p^{2s}}}{1-\frac{1}{p^s}}$$

$$=\sum_p\frac{1}{p^s}+\sum_p\frac{1}{p^{2s}-p^s}$$

$$=\sum_p\frac{1}{p^s}+\sum_p\frac{1}{p^s(p^s-1)}$$

$$<\sum_p\frac{1}{p^s}+\sum_{n=2}^{+\infty}\frac{1}{n^s(n^s-1)}$$

$$< \sum_p \frac{1}{p^s} + \sum_{n=2}^{+\infty} \frac{1}{n(n-1)}, \text{ διότι } s>1$$

$$< \sum_p \frac{1}{p^s} + \sum_{n=2}^{+\infty} \frac{1}{(n-1)^2}.$$

Άρα,

$$\lim_{s\to 1^+}(\log\zeta(s)) \le \lim_{s\to 1^+}\left(\sum_p \frac{1}{p^s} + \sum_{n=2}^{+\infty}\frac{1}{(n-1)^2}\right).$$

Επομένως

$$\lim_{s\to 1^+}\left(\sum_p \frac{1}{p^s} + \sum_{n=2}^{+\infty}\frac{1}{(n-1)^2}\right) = +\infty,$$

αφού

$$\lim_{s\to 1^+}(\log\zeta(s)) = +\infty.$$

Όμως η σειρά

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

συγκλίνει σε πραγματικό αριθμό, συνεπώς

$$\lim_{s\to 1+}\sum_p \frac{1}{p^s} = +\infty.$$

Επομένως, συνεπάγεται ότι

$$\sum_p \frac{1}{p} = +\infty \quad .$$

■

3) ***Να δειχθεί ότι***

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{+\infty}\frac{\mu(n)}{n^s}.$$

Η ιδέα για την απόδειξη είναι η ακόλουθη:

Από την ταυτότητα του Euler λαμβάνουμε ότι

$$\frac{1}{\zeta(s)} = \frac{1}{\prod_p \frac{1}{1-p^{-s}}} = \prod_p\left(1-\frac{1}{p^s}\right)$$

$$= \left(1-\frac{1}{p_1^s}\right)\left(1-\frac{1}{p_2^s}\right)\cdots$$

Όμως, εκτελώντας τις πράξεις στο παραπάνω γινόμενο, θα προκύψει ένα άθροισμα όρων της μορφής

$$\frac{(-1)^{\kappa}}{(p_1^{a_1}p_2^{a_2}...p_{\kappa}^{a_{\kappa}})^{s}},$$

όπου $a_i = 0$ ή 1 για $i = 1,2,...,\kappa$ χωρίς να μηδενίζονται όλοι οι εκθέτες ταυτόχρονα, αυξημένο κατά μια μονάδα.

Στους παρανομαστές των παραπάνω όρων παρουσιάζονται όλα τα δυνατά γινόμενα πρώτων παραγόντων με εκθέτες 0 ή 1.

Συνεπώς

$$\frac{1}{\zeta(s)} = 1 + \sum \frac{(-1)^{\kappa}}{(p_1^{a_1}p_2^{a_2}...p_{\kappa}^{a_{\kappa}})^{s}}$$

$$= \frac{\mu(1)}{1} + \sum \frac{\mu(p_1^{a_1}p_2^{a_2}...p_{\kappa}^{a_{\kappa}})}{(p_1^{a_1}p_2^{a_2}...p_{\kappa}^{a_{\kappa}})^{s}} + 0$$

Όμως, μπορούμε να γράψουμε

$$0 = \sum \frac{\mu(p_1^{q_1}p_2^{q_2}...p_{\lambda}^{q_{\lambda}})}{(p_1^{q_1}p_2^{q_2}...p_{\lambda}^{q_{\lambda}})^{s}},$$

όπου στους παρονομαστές του παραπάνω αθροίσματος παρουσιάζονται όλοι οι δυνατοί συνδυασμοί γινομένων πρώτων παραγόντων με $q_i \geq 2, i = 1, 2, ..., \lambda$.

Έτσι

$$\frac{1}{\zeta(s)} = \frac{\mu(1)}{1} + \sum \frac{\mu(p_1^{a_1}p_2^{a_2}...p_{\kappa}^{a_{\kappa}})}{(p_1^{a_1}p_2^{a_2}...p_{\kappa}^{a_{\kappa}})^{s}} + \sum \frac{\mu(p_1^{q_1}p_2^{q_2}...p_{\lambda}^{q_{\lambda}})}{(p_1^{q_1}p_2^{q_2}...p_{\lambda}^{q_{\lambda}})^{s}}.$$

Άρα, προκύπτει ότι με τους όρους $p_1^{a_1}p_2^{a_2}...p_{\kappa}^{a_{\kappa}}$ και $p_1^{q_1}p_2^{q_2}...p_{\lambda}^{q_{\lambda}}$ μπορούν να αναπαρασταθούν, όλοι οι θετικοί ακέραιοι $n > 1$.

Δηλαδή ισχύει

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^{s}}.$$

■

4) ***Έστω η συνάρτηση***

$$\boldsymbol{\zeta(s,a) = \sum_{n=0}^{+\infty} \frac{1}{(n+a)^{s}}}$$

για πραγματικές τιμές των s ***και*** a***, όπου*** $s > 1$ ***και*** $0 < a \leq 1$***.***
Να δειχθεί ότι

$$\boldsymbol{\Gamma(s)\zeta(s,a) = \int_0^{+\infty} \frac{x^{s-1}e^{-ax}}{1-e^{-x}}dx}$$

(η συνάρτηση $\zeta(s,a)$ ***είναι γνωστή ως συνάρτηση ζήτα του Hurwitz).***

Η ιδέα για την απόδειξη είναι η ακόλουθη:

Από τον ορισμό της συνάρτησης Γάμμα έχουμε

$$\Gamma(s) = \int_0^{+\infty} e^{-t}t^{s-1}dt \ .$$

Θέτουμε $t = (n+a)x,$ *όπου* $n \in \mathbb{N} \cup \{0\}.$

Άρα, $dt=(n+a)\,dx$. Έτσι, προκύπτει ότι

$$\Gamma(s)=(n+\alpha)^{s-1}(n+\alpha)\int_0^{+\infty}e^{-(n+\alpha)x}x^{s-1}dx=(n+\alpha)^s\int_0^{+\infty}e^{-nx}e^{-\alpha x}x^{s-1}dx$$

Επομένως,

$$\frac{1}{(n+a)^s}\Gamma(s)=\int_0^{+\infty}e^{-nx}e^{-\alpha x}x^{s-1}dx \tag{1}$$

Συνεπώς, προκειμένου να δημιουργήσουμε το γινόμενο $\Gamma(s)\ \zeta(s,a)$ αρκεί να αθροίσουμε κατά μέλη όλες τις σχέσεις της μορφής (1), για κάθε $n\geq 0$.

Επομένως, μετά την άθροιση έχουμε

$$\Gamma(s)\sum_{n=0}^{+\infty}\frac{1}{(n+a)^s}=\sum_{n=0}^{+\infty}\int_0^{+\infty}e^{-nx}e^{-ax}x^{s-1}dx$$

ή

$$\Gamma(s)\ \zeta(s,a)=\sum_{n=0}^{+\infty}\int_0^{+\infty}e^{-nx}e^{-ax}x^{s-1}dx.$$

Για να μπορέσουμε να υπολογίσουμε το απειροάθροισμα

$$\sum_{n=0}^{+\infty}\int_0^{+\infty}e^{-nx}e^{-\alpha x}x^{s-1}dx,$$

θα εξετάσουμε αν

$$\sum_{n=0}^{+\infty}\int_0^{+\infty}e^{-nx}e^{-\alpha x}x^{s-1}dx=\int_0^{+\infty}\sum_{n=0}^{+\infty}e^{-nx}e^{-\alpha x}x^{s-1}dx \tag{2}$$

Αυτό όμως είναι άμεση συνέπεια του θεωρήματος του Tonelli.

Άρα,

$$\Gamma(s)\ \zeta(s,\alpha)=\sum_{n=0}^{+\infty}\int_0^{+\infty}e^{-nx}e^{-\alpha x}x^{s-1}dx=\int_0^{+\infty}\sum_{n=0}^{+\infty}e^{-nx}e^{-\alpha x}x^{s-1}dx$$

$$=\int_0^{+\infty}e^{-\alpha x}x^{s-1}\sum_{n=0}^{+\infty}e^{-nx}dx.$$

Η σειρά

$$\sum_{n=0}^{+\infty}e^{-nx}$$

αποτελεί άθροισμα απείρων όρων φθίνουσας γεωμετρικής προόδου.

Συνεπώς,

$$\sum_{n=0}^{+\infty}e^{-nx}=\frac{1}{1-e^{-x}}\quad .$$

Επομένως,

$$\Gamma(s)\ \zeta(s,\alpha)=\int_0^{+\infty}\frac{e^{-\alpha x}x^{s-1}}{1-e^{-x}}dx.$$

Σχόλια

α) *Στην περίπτωση όπου* $\alpha = 1$, *ισχύει:* $\zeta(s,1) = \zeta(s)$ *καθώς*

$$\sum_{n=1}^{+\infty} \frac{1}{n^s} = \sum_{n=0}^{+\infty} \frac{1}{(n+1)^s}.$$

Επομένως,

$$\Gamma(s)\zeta(s) = \int_0^{+\infty} \frac{e^{-x}x^{s-1}}{1-e^{-x}}\,dx.$$

β) *Η παραπάνω απόδειξη δόθηκε για πραγματικές τιμές του* s. *Αποδεικνύεται επίσης πως*

$$\Gamma(s)\zeta(s) = \int_0^{+\infty} \frac{e^{-x}x^{s-1}}{1-e^{-x}}\,dx$$

και στην περίπτωση όπου $s = a + bi$, *με* $a > 1$.

γ) *Μια άλλη χρήσιμη σχέση μεταξύ της συνάρτησης* $\zeta(s)$ *και της συνάρτησης* $\Gamma(s)$ *είναι η ακόλουθη:*

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \frac{1}{s(s-1)} + \int_1^{+\infty} W(x)\left(x^{s/2} + x^{(1-s)/2}\right)\frac{dx}{x},$$

όπου

$$W(x) = \frac{w(x)-1}{2},\quad w(y) = \vartheta(iy) \quad \mu\varepsilon \quad \theta(z) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 z}.$$

Δύο διασκεδαστικές παρατηρήσεις που απαιτούν Μαθηματική θεμελίωση

Α. ΤΟ ΠΡΟΒΛΗΜΑ ΤΟΥ CHEBYSHEV

Η «πιθανότητα» Q ***ώστε δύο «τυχαίοι» ακέραιοι αριθμοί*** x, y ***να είναι πρώτοι μεταξύ τους, δηλ.*** $Q = P\{(x,y) = 1\}$***, είναι***

$$Q = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

Έχουμε

$$(x,y) = 1 \Leftrightarrow \begin{cases} p \nmid x \\ \text{ή} \\ p \nmid y \end{cases}, \text{για όλους τους πρώτους αριθμούς } p.$$

Όμως, τα «ενδεχόμενα» που αντιστοιχούν σε κάθε πρώτο αριθμό p ξεχωριστά, θεωρούνται «ανεξάρτητα».

Έτσι:

$$\begin{aligned} Q = P\{(x,y)=1\} &= P\{p_1 \nmid x \text{ ή } p_1 \nmid y\}\cdot P\{p_2 \nmid x \text{ ή } p_2 \nmid y\}\cdots \\ &= \prod_p P\{p \nmid x \text{ ή } p \nmid y\} \\ &= \prod_p P\left\{\left(p \mid x \text{ και } p \mid y\right)'\right\} \end{aligned}$$

$$= \prod_p \left(1 - P\{p \mid x \text{ και } p \mid y\}\right).$$

Όμως, τα «ενδεχόμενα»

$$A = \{p \mid x\}, \quad B = \{p \mid y\}$$

είναι ανεξάρτητα.
Άρα

$$P(AB) = P(A)P(B) \ .$$

Συνεπώς

$$Q = P\{(x,y) = 1\} = \prod_p \left(1 - P\{p \mid x\} \cdot P\{p \mid y\}\right) = \prod_p \left(1 - \frac{1}{p} \cdot \frac{1}{p}\right)$$

$$= \prod_p \left(1 - \frac{1}{p^2}\right) = \frac{1}{\prod_p \frac{1}{1 - p^{-2}}} = \frac{1}{\zeta(2)} \ .$$

Δηλαδή

$$Q = \frac{1}{\zeta(2)} .$$

■

Β. ***Θεωρούμε στο Καρτεσιανό επίπεδο όλα τα συνδεσμικά σημεία (lattice points)*** (x, y) ***με*** $x, y \in \mathbb{N}$. ***Αν υποθέσουμε πως σε κάθε σημείο*** (x, y) ***κάθεται ένας μαθητής και στο σημείο*** $O(0,0)$ ***βρίσκεται η έδρα του καθηγητή, τότε να υπολογιστεί η «πιθανότητα» ο καθηγητής να έχει πλήρη ορατότητα (χωρίς να υπάρχουν ενδιάμεσα άλλοι μαθητές) προς έναν «τυχαίο» μαθητή που βρίσκεται στην θέση*** (x, y).

Είναι φανερό ότι ο καθηγητής θα έχει πλήρη ορατότητα προς έναν τυχαίο μαθητή που βρίσκεται στην θέση (x, y), αν και μόνο αν οι ακέραιοι αριθμοί x, y είναι πρώτοι μεταξύ τους.

Αν ήταν $(x, y) = d > 1$, τότε στην θέση $\left(\frac{x}{d}, \frac{y}{d}\right)$ θα υπήρχε άλλος ένας μαθητής που θα εμπόδιζε την ορατότητα του καθηγητή.

Συνεπώς, η ζητούμενη «πιθανότητα», είναι ίση με την «πιθανότητα» δύο «τυχαίοι» φυσικοί αριθμοί x, y να είναι πρώτοι μεταξύ τους. Όμως, στο *πρόβλημα του Chebyshev* είδαμε ότι η «πιθανότητα» αυτή είναι ίση με

$$\frac{1}{\zeta(2)} = \frac{6}{\pi^2} .$$

■

ΔΥΟ ΕΙΚΑΣΙΕΣ ΣΧΕΤΙΚΕΣ ΜΕ ΤΟΥΣ ΠΡΩΤΟΥΣ ΑΡΙΘΜΟΥΣ

I. Εικασία Goldbach

Κάθε άρτιος φυσικός αριθμός μεγαλύτερος του δύο, μπορεί να εκφραστεί ως άθροισμα δύο πρώτων αριθμών.

> ***Σχόλιο***
> *Η παραπάνω εικασία διατυπώθηκε από τον Christian Goldbach (1690 –1764) σε επιστολή του προς τον Leonhard Euler (1707 – 1783) στις 7 Ιουνίου 1742.*

II. Εικασία Andrica

Έστω P_n ο n-οστός πρώτος αριθμός. Αν θεωρήσουμε την ακολουθία $(A_n)_{n\geq 1}$ που ορίζεται από τον τύπο

$$A_n = \sqrt{P_{n+1}} - \sqrt{P_n}$$

τότε

$$A_n < 1$$

για κάθε θετικό ακέραιο n.

(Dorin Andrica, *Problem 34, Newsletter, European Mathematical Society,* 67(2008), σελ.44).

8. Παραδείγματα – Εφαρμογές

1) ***Έστω n θετικός ακέραιος αριθμός. Ένας ακέραιος αριθμός A αποτελείται από 2n ψηφία καθένα των οποίων είναι το 4, ενώ ένας άλλος ακέραιος B αποτελείται από n ψηφία καθένα των οποίων είναι το 8. Να αποδειχθεί ότι ο ακέραιος αριθμός***

$$A + 2B + 4$$

είναι τέλειο τετράγωνο ακεραίου αριθμού.

(7η Βαλκανική Μαθηματική Ολυμπιάδα).

ΑΠΟΔΕΙΞΗ

Είναι

$$A = \underbrace{444...4}_{2n} = \underbrace{444...4}_{n}\underbrace{00...0}_{n} + \underbrace{44...4}_{n}$$

$$= \underbrace{444...4}_{n} \cdot \left(10^n - 1\right) + \underbrace{88...8}_{n}$$

$$= \underbrace{444...4}_{n} \cdot \left(10^n - 1\right) + B .$$

Επομένως

$$A = 4 \cdot \underbrace{111...1}_{n} \cdot \underbrace{999...9}_{n} + B = 4 \cdot \underbrace{111...1}_{n} \cdot 9 \cdot \underbrace{111...1}_{n} + B$$

$$= 6 \cdot \underbrace{111...1}_{n} \cdot 6 \cdot \underbrace{111...1}_{n} + B = (\underbrace{666...6}_{n})^2 + B$$

$$= \left(3 \cdot 222...2\right)^2 + B = \left(\frac{3}{4} \cdot 888...8\right)^2 + B = \left(\frac{3}{4} \cdot B\right)^2 + B .$$

Έτσι, λαμβάνουμε ότι:

$$A + 2B + 4 = \left(\frac{3}{4} \cdot B\right)^2 + B + 2B + 4$$

$$= \left(\frac{3}{4} \cdot B\right)^2 + 2 \cdot \frac{3}{4} B \cdot 2 + 2^2$$

$$= \left(\frac{3}{4} B + 2\right)^2 = \left(\frac{3}{4} \underbrace{888...8}_{n} + 2\right)^2$$

$$= \left(3 \cdot \underbrace{222...2}_{n} + 2\right)^2 = \underbrace{666...6}_{n-1}8^2 ,$$

που είναι τέλειο τετράγωνο ακέραιου αριθμού.

■

2) ***Να βρεθούν οι τρεις μικρότεροι φυσικοί διαδοχικοί αριθμοί των οποίων το άθροισμα είναι τέλειο τετράγωνο και τέλειος κύβος φυσικού αριθμού.***

(Μ. Θ. Ρασσιάς, Προτεινομενο πρόβλημα #94, Ευκλείδης Β΄, Ελληνική Μαθηματική Εταιρεία, Τεύχος 62, 2006, σελ. 80).

ΛΥΣΗ

΄Εστω, οι τρεις διαδοχικοί φυσικοί αριθμοί $n-1, n, n+1$, όπου $n \in \mathbb{N} - \{1\}$. Τότε, λαμβάνουμε

$$(n-1)+n+(n+1)=3n.$$

Άρα, πρέπει ο φυσικός αριθμός $3n$ να είναι τέλειο τετράγωνο και τέλειος κύβος φυσικού αριθμού. Δηλαδή,

$$3n=a^2 \text{ και } 3n=b^3, \text{ όπου } a,b \in \mathbb{N}.$$

Έτσι,

$$3 \mid a^2 \text{ και } 3 \mid b^3, \text{ οπότε } 3 \mid a \text{ και } 3 \mid b$$

(αφού ο 3 είναι πρώτος αριθμός).

Από το θεμελιώδες θεώρημα της αριθμητικής προκύπτει

$$a = p_1^{a_1} 3^{a_2} \cdots p_\kappa^{a_\kappa} \text{ και } b = p_1^{b_1} 3^{b_2} \cdots p_\kappa^{b_\kappa},$$

όπου $p_1,...,p_\kappa$ είναι πρώτοι αριθμοί.

Άρα,

$$p_1^{2a_1} 3^{2a_2} \cdots p_\kappa^{2a_\kappa} = p_1^{3b_1} 3^{3b_2} \cdots p_\kappa^{3b_\kappa}$$

Συνεπώς,

$$2a_2 = 3b_2. \tag{1}$$

Δηλαδή, όταν αναπαρασταθεί ο φυσικός αριθμος $3n$ σε κανονική μορφή ο εκθέτης του 3 θα είναι ταυτόχρονα πολλαπλάσιο και του 2 και του 3. Για την εύρεση των μικρότερων φυσικών αριθμών με την ζητούμενη ιδιότητα, ο $3n$ πρέπει να είναι ο ελάχιστος δυνατός.

Αυτό θα συμβαίνει όταν:

$$3n = 3^\kappa,$$

όπου κ ο ελάχιστος δυνατός εκθέτης του 3.

Από την σχέση (1) προκύπτει ότι ο κ είναι το ελάχιστο κοινό πολλαπλάσιο των αριθμών 2 και 3.

Συνεπώς,

$$3n = 3^6 \Leftrightarrow n = 3^5.$$

Άρα, οι ζητούμενοι φυσικοί αριθμοί είναι οι

$$3^5-1,\ 3^5,\ 3^5+1.$$

Πράγματι

$$\left(3^5-1\right)+3^5+\left(3^5+1\right)=3\cdot 3^5=3^6=\left(3^3\right)^2=\left(3^2\right)^3.$$

■

3) ***Έστω n ένας θετικός ακέραιος αριθμός, τέτοιος ώστε $(n,6)=1$. Να αποδειχθεί ότι το άθροισμα n τετραγώνων διαδοχικών ακεραίων είναι πολλαπλάσιο του n.***

ΑΠΟΔΕΙΞΗ

Έστω

$$\kappa = a^2 + (a+1)^2 + (a+2)^2 + \ldots + (a+n-1)^2 .$$

Τότε λαμβάνουμε ότι:

$$\kappa = a^2 + (a^2 + 2a + 1) + (a^2 + 2\cdot 2a + 2^2) + \ldots + \left[a^2 + 2(n-1)a + (n-1)^2\right]$$

$$= na^2 + 2\frac{(n-1)n}{2}a + \frac{(n-1)n(2n-1)}{6}$$

$$= na^2 + an(n-1) + n\frac{(n-1)(2n-1)}{6}.$$

Για να αποδείξουμε το ζητούμενο αρκεί να δείξουμε ότι ο αριθμός $\dfrac{(n-1)(2n-1)}{6}$ είναι ακέραιος.

Γνωρίζουμε ότι $(n,6)=1$ δηλαδή, ο ακέραιος n είναι περιττός και έτσι ο $n-1$ είναι άρτιος. Αφού $(n,6)=1$ προκύπτει, επίσης, ότι:

$$n = 3\lambda + 1 \text{ ή } n = 3\lambda - 1, \text{ όπου } \lambda \in \mathbb{Z},$$

διότι ο n δεν μπορεί να είναι πολλαπλάσιο του 3.

- Αν $n = 3\lambda + 1$, τότε $n - 1 = 3\lambda$ ενώ ο $n-1$ είναι ταυτόχρονα άρτιος αριθμός. Άρα

$$n - 1 = 0 \bmod 6 \text{ και έτσι, } (n-1)(2n-1) \equiv 0 \pmod 6 .$$

- Αν $n = 3\lambda - 1$, τότε $2n - 1 = 3(2\lambda - 1) \equiv 0 \pmod 3$, ενώ ταυτόχρονα

$$n - 1 \equiv 0 \pmod 2 .$$

Έτσι,

$$(n-1)(2n-1) \equiv 0 \pmod 6 .$$

Συνεπώς

$$\frac{(n-1)(2n-1)}{6} \in \mathbb{Z}$$

και επομένως ο ακέραιος αριθμός κ είναι πολλαπλάσιο του n, το οποίο αποδεικνύει το ζητούμενο.

■

4) ***Έστω δύο περιττοί πρώτοι αριθμοί*** p_1, p_2 ***και*** a, n ***ακέραιοι αριθμοί με*** $a > 1$ ***και*** $n > 1$***. Αν η εξίσωση***

$$\left(\frac{p_2 - 1}{2}\right)^{p_1} + \left(\frac{p_2 + 1}{2}\right)^{p_1} = a^n$$

δεν έχει ακέραιες λύσεις στην περίπτωση $p_1 = p_2$***, τότε δεν έχει ακέραιες λύσεις και στην περίπτωση*** $p_1 \neq p_2$**.**

(Μ. Θ. Ρασσιάς, Προτεινόμενο πρόβλημα #110, Ευκλείδης Β΄, Ελληνική Μαθηματική Εταιρεία, τεύχος 65, 2007, σελ. 75 – 76).

ΑΠΟΔΕΙΞΗ

Από τα δεδομένα αποκλείονται οι περιπτώσεις $p_1 = 2$ και $p_2 = 2$, οπότε θεωρούμε

$$p_2 = 2x + 1,\ x \in \mathbb{N}.$$

Υποθέτουμε, τώρα, ότι η εξίσωση δέχεται τουλάχιστον μια ακέραια λύση. Τότε, η εξίσωση

$$\left(\frac{p_2 - 1}{2}\right)^{p_1} + \left(\frac{p_2 + 1}{2}\right)^{p_1} = a^n$$

λαμβάνει τη μορφή:

$$x^{p_1} + (x+1)^{p_1} = a^n. \tag{1}$$

Επειδή ο p_1 είναι περιττός αριθμός, προκύπτει ότι:

$$a^n = x^{p_1} + (x+1)^{p_1} = (x + x + 1)A = (2x+1)A,\ A \in \mathbb{N}.$$

Άρα

$$(2x+1) \mid a^n.$$

Επειδή, ο $2x+1$ είναι πρώτος αριθμός προκύπτει ότι:

$$(2x+1) \mid a.$$

Άρα,

$$(2x+1)^2 \mid a^2.$$

΄Ομως $n > 1$, οπότε

$$(2x+1)^2 \mid a^n \ \text{ ή } \ (2x+1)^2 \mid x^{p_1} + (x+1)^{p_1} \tag{2}$$

Επομένως,

$$\begin{aligned} x^{p_1} + (x+1)^{p_1} &= x^{p_1} + \left[(2x+1) - x\right]^{p_1} \\ &= x^{p_1} + (2x+1)^{p_1} + \binom{p_1}{1}(2x+1)^{p_1 - 1}(-x) + \cdots \\ &\quad + \binom{p_1}{p_1 - 1}(2x+1)(-x)^{p_1 - 1} + (-x)^{p_1} \end{aligned}$$

$$= x^{p_1} + (2x+1)^2 B + \binom{p_1}{p_1 - 1}(2x+1)x^{p_1-1} - x^{p_1}$$

$$= \binom{p_1}{p_1 - 1}(2x+1)x^{p_1-1} + (2x+1)^2 B, \text{ όπου } B \in \mathbb{Z}.$$

Οπότε

$$x^{p_1} + (x+1)^{p_1} = \binom{p_1}{p_1 - 1}(2x+1)x^{p_1-1} + (2x+1)^2 B.$$

Από την σχέση (2) προκύπτει ότι:

$$(2x+1)^2 \left| \binom{p_1}{p_1 - 1}(2x+1)\, x^{p_1-1} \right.$$

ή

$$(2x+1) \left| \binom{p_1}{p_1 - 1} x^{p_1-1} \right.$$

ή

$$(2x+1) \mid p_1 x^{p_1-1}$$

Επειδή ο αριθμός $2x+1$ είναι πρώτος, ισχύει ότι

$$(2x+1) \mid p_1 \text{ ή } (2x+1) \mid x.$$

Η δεύτερη περίπτωση αποκλείεται αφού

$$2x+1 > x \text{ και } (2x+1, x) = 1.$$

Τελικά $(2x+1) \mid p_1$, δηλαδή

$$p_1 = 2x+1, \text{ αφού ο } p_1 \text{ είναι πρώτος αριθμός.}$$

Άρα

$$p_1 = p_2.$$

Όμως, σύμφωνα με την υπόθεση, η εξίσωση δεν επιδέχεται λύση για $p_1 = p_2$, συνεπώς, η εξίσωση (1) και επομένως η εξίσωση

$$\left(\frac{p_2 - 1}{2}\right)^{p_1} + \left(\frac{p_2 + 1}{2}\right)^{p_1} = a^n$$

δεν έχει ακέραιες λύσεις.

■

5) ***Να δειχθεί ότι η εξίσωση***

$$x^4 + y^4 = z^4$$

δεν έχει μη–μηδενικές ακέραιες λύσεις.

ΑΠΟΔΕΙΞΗ

Το παραπάνω πρόβλημα αποτελεί την πλέον απλή (όσον αφορά την απόδειξη) περίπτωση του τελευταίου θεωρήματος του Fermat.

Θα αποδείξουμε ότι η εξίσωση $x^n + y^n = z^n$ δεν έχει μη μηδενικές ακέραιες λύσεις για $n = 4 > 2$.

Αρκεί να δείξουμε ότι η εξίσωση $x^4 + y^4 = z^2$ δεν έχει μη μηδενικές ακέραιες λύσεις. Αυτό συμβαίνει διότι, αν η εξίσωση $x^4 + y^4 = z^4$ είχε έστω και μία λύση $(x_\kappa, y_\kappa, z_\kappa)$ στο σύνολο των μη μηδενικών ακεραίων, τότε και η εξίσωση $x^4 + y^4 = z^2$ θα είχε μια λύση την $(x_\kappa, y_\kappa, z_\kappa^2)$. Άρα, αποδεικνύοντας την ανυπαρξία μη μηδενικών ακέραιων λύσεων της $x^4 + y^4 = z^2$ αποδεικνύουμε ταυτοχρόνως και την ανυπαρξία μη μηδενικών ακέραιων λύσεων της $x^4 + y^4 = z^4$. Θα ακολουθήσουμε την ***μέθοδο της καθόδου***.

Υποθέτουμε ότι η εξίσωση $x^4 + y^4 = z^2$ έχει τουλάχιστον μια μη μηδενική λύση (x, y, z) στο σύνολο των ακεραίων αριθμών.

Θεωρούμε έναν ακέραιο αριθμό S τέτοιον ώστε:

$$S = xyz\ .$$

Από το σύνολο όλων των ακέραιων αριθμών S που προκύπτουν από τις διάφορες λύσεις (x, y, z), θα υπάρχει ένα S το οποίο θα έχει την ελάχιστη τιμή.

Έστω, ο $S_0 = x_0 y_0 z_0$ ο μικρότερος ακέραιος από όλα τα δυνατά S.

Θα δείξουμε τώρα ότι για τον μέγιστο κοινό διαιρέτη των x_0, y_0, z_0 ισχύει $(x_0, y_0, z_0) = 1$. Αρκεί να δείξουμε ότι $(x_0, y_0) = 1$ διότι, αν υπήρχε έστω και ένας πρώτος αριθμός p τέτοιος ώστε $p|x_0$, $p|y_0$ και $p|z_0$, τότε προφανώς θα ήταν $(x_0, y_0) \neq 1$.

Υποθέτουμε, λοιπόν, ότι υπάρχει ένας πρώτος αριθμός p τέτοιος ώστε $p|x_0$ και $p|y_0$.

Όμως, έχουμε υποθέσει πως η εξίσωση $x^4 + y^4 = z^2$ έχει τουλάχιστον μια μη μηδενική λύση (x, y, z) στο σύνολο των ακεραίων.

Άρα

$$x_0^4 + y_0^4 = z_0^2 \Leftrightarrow \left(\frac{x_0}{p}\right)^4 + \left(\frac{y_0}{p}\right)^4 = \left(\frac{z_0}{p^2}\right)^2 \in \mathbb{Z}\ .$$

Συνεπώς $p^2|z_0$. Θέτουμε

$$x_1 = \frac{x_0}{p},\ y_1 = \frac{y_0}{p},\ z_1 = \frac{z_0}{p^2}\ .$$

Επομένως, λαμβάνουμε ότι:

$$S_1 = x_1 y_1 z_1 = \frac{x_0}{p}\frac{y_0}{p}\frac{z_0}{p^2} < x_0 y_0 z_0 = S_0\ .$$

Άρα

$$S_1 < S_0,$$

το οποίο είναι αδύνατον από τον ορισμό του S_0.

Σύμφωνα με τα παραπάνω προκύπτει ότι για τον μέγιστο κοινό διαιρέτη των x_0, y_0, z_0 ισχύει

$$(x_0, y_0, z_0) = 1$$

και από αυτό προκύπτει επίσης ότι:

$$(x_0^2, y_0^2, z_0) = 1,$$

διότι αν υπήρχε πρώτος αριθμός p τέτοιος ώστε

$$p \mid x_0^2,\ p \mid y_0^2,\ p \mid z_0,$$

τότε θα ίσχυε ότι $p \mid x_0$, $p \mid y_0$, $p \mid z_0$, το οποίο είναι άτοπο.

Η τριάδα (x_0^2, y_0^2, z_0) είναι μια Πυθαγόρεια τριάδα διότι

$$(x_0^2)^2 + (y_0^2)^2 = z_0^2 .$$

Όμως, έχουμε ήδη αποδείξει ότι οι ακέραιες λύσεις της εξίσωσης $x^2 + y^2 = z^2$ μπορούν να εκφραστούν στη μορφή

$$x = 2a\beta,\ y = \beta^2 - a^2,\ z = \beta^2 + a^2, \text{ όπου } \beta > a \text{ και } (a, \beta) = 1.$$

Έτσι, αν υποθέσουμε ότι ο x_0^2 είναι άρτιος (καθώς ένας από τους x_0^2, y_0^2 αναγκαστικά πρέπει να είναι άρτιος) θα ισχύει:

$$x_0^2 = 2\gamma\delta,\ y_0^2 = \delta^2 - \gamma^2,\ z_0 = \delta^2 + \gamma^2,$$

όπου $\delta > \gamma$ και $(\gamma, \delta) = 1$.

Άρα, λαμβάνουμε ότι:

$$\delta^2 = y_0^2 + \gamma^2, \text{ όπου } (\delta, y_0, \gamma) = 1 \text{ αφού } (\gamma, \delta) = 1.$$

Συνεπώς η τριάδα (δ, y_0, γ) είναι μια Πυθαγόρεια τριάδα. Έχουμε υποθέσει πως ο x_0^2 είναι άρτιος. Για τον λόγο αυτό πρέπει ο y_0^2 να είναι περιττός και συνεπώς ο y_0 να είναι περιττός.

Άρα, ο αριθμός γ είναι άρτιος.

Έτσι

$$\gamma = 2cd,\ y_0 = d^2 - c^2,\ \delta = d^2 + c^2,$$

όπου $d > c$ και $(c, d) = 1$.

Όμως, έχουμε αποδείξει ότι

$$x_0^2 = 2\gamma\delta .$$

Συνεπώς

$$x_0^2 = 2(2cd)(d^2 + c^2).$$

Άρα

$$\left(\frac{x_0}{2}\right)^2 = cd\,(d^2 + c^2).$$

Προφανώς $\frac{x_0}{2} \in \mathbb{Z}$ αφού ο x_0 είναι άρτιος αριθμός.

Άρα, ο αριθμός

$$\left(\frac{x_0}{2}\right)^2$$

είναι τέλειο τετράγωνο. Οι ακέραιοι αριθμοί $c, d, d^2 + c^2$ είναι ανά δύο πρώτοι μεταξύ τους διότι

- αν υπήρχε πρώτος αριθμός p_1, τέτοιος ώστε $p_1 | c$ και $p_1 \mid \left(d^2 + c^2\right)$, τότε θα ίσχυε $p_1 | c^2$ και $p_1 \mid \left(d^2 + c^2\right)$, δηλαδή $p_1 | d^2$ και επομένως $p_1 | d$, το οποίο είναι αδύνατο αφού $(c, d) = 1$.
- αν υπήρχε πρώτος αριθμός p_2, τέτοιος ώστε $p_2 | d$ και $p_2 \mid \left(d^2 + c^2\right)$, ομοίως θα ίσχυε ότι $p_2 | d^2$ και $p_2 \mid \left(d^2 + c^2\right)$ και άρα $p_2 | c$, το οποίο είναι αδύνατον.

Έτσι, θα ισχύει ότι:

$$c = x_m^2,\ d = y_m^2,\ d^2 + c^2 = z_m^2,$$

δηλαδή

$$x_m^4 + y_m^4 = z_m^2.$$

Επομένως, η τριάδα $\left(x_m, y_m, z_m\right)$ αποτελεί λύση της εξίσωσης

$$x^4 + y^4 = z^2$$

στο σύνολο των ακέραιων αριθμών.

Τότε,

$$S_m = x_m y_m z_m = \sqrt{x_m^2 y_m^2 z_m^2} = \sqrt{cd\left(d^2 + c^2\right)}$$

$$= \frac{x_0}{2} < x_0 y_0 z_0 = S_0,$$

δηλαδή

$$S_m < S_0,$$

το οποίο είναι αδύνατο.

Άρα, η υπόθεση ότι η εξίσωση $x^4 + y^4 = z^2$ έχει τουλάχιστον μια λύση στο σύνολο των μηδενικών ακεραίων αριθμών καταλήγει σε άτοπο. Συνεπώς, ούτε η εξίσωση $x^4 + y^4 = z^4$ μπορεί να έχει μη μηδενικές ακέραιες λύσεις.

■

Σχόλιο

Η παραπάνω απόδειξη οφείλεται στον Γερμανό μαθηματικό Ernst Eduard Kummer (1810 – 1893).

6) ***Να αποδειχθεί ότι δεν μπορούν να βρεθούν ακέραιες τιμές των μεταβλητών*** x, y, z ***με*** x ***της μορφής*** $4\kappa+3$, $\kappa\in\mathbb{Z}$, ***τέτοιες ώστε να ικανοποιείται η εξίσωση***

$$x^n = y^n + z^n \quad \textit{για } n\in\mathbb{N}-\{1\}.$$

ΑΠΟΔΕΙΞΗ

Σύμφωνα με το Τελευταίο Θεώρημα του Fermat (Fermat's Last Theorem) η διοφαντική εξίσωση $x^n = y^n + z^n$ δεν έχει μη–μηδενικές ακέραιες λύσεις x, y, z για $n \geq 3$.

Συνεπώς, αρκεί να δείξουμε ότι για $n = 2$ η εξίσωση $x^n = y^n + z^n$ δεν ικανοποιείται, αν ο x είναι της μορφής $4\kappa+3$, $\kappa\in\mathbb{Z}$.

Όμως αν η εξίσωση $x^2 = y^2 + z^2$ έχει λύση, τότε προκύπτει ότι και η εξίσωση $x = y^2 + z^2$ έχει λύση. Αυτό συμβαίνει διότι, αν x_0, y_0, z_0 είναι μια λύση της εξίσωσης $x^2 = y^2 + z^2$, τότε η (x_0^2, y_0, z_0) είναι λύση της εξίσωσης $x = y^2 + z^2$.

Όμως, αν ο x είναι της μορφής $4\kappa+3$, τότε η εξίσωση $x = y^2 + z^2$ δεν μπορεί να έχει λύση αφού κανένας ακέραιος της μορφής $4\kappa+3$ δεν μπορεί να εκφραστεί ως άθροισμα δύο τετραγώνων ακεραίων αριθμών.

Η απόδειξη του παραπάνω ισχυρισμού είναι η εξής:

Έστω $x = y^2 + z^2$ με $x = 4\kappa+3$, τότε ισχύει ότι:

$$y^2 + z^2 \equiv 3 (\mathrm{mod}\, 4).$$

Όμως, γενικά για τα τετράγωνα ακεραίων ισχύει:

$$a^2 \equiv 0 \text{ ή } 1 (\mathrm{mod}\, 4)$$

διότι

- αν ο ακέραιος a είναι άρτιος τότε $a^2 = 4\lambda,\ \lambda\in\mathbb{Z}$ και επομένως

$$a^2 \equiv 0 (\mathrm{mod}\, 4).$$

- αν ο ακέραιος a είναι περιττός τότε $a^2 = 8\lambda+1,\ \lambda\in\mathbb{Z}$ και επομένως

$$a^2 \equiv 1 (\mathrm{mod}\, 4).$$

Συνεπώς, για το άθροισμα δύο τετραγώνων ακεραίων αριθμών ισχύει:

$$a^2 + b^2 \equiv 0 \text{ ή } 1 \text{ ή } 2 (\mathrm{mod}\, 4)$$

και δεν ισχύει ποτέ

$$a^2 + b^2 \equiv 3 (\mathrm{mod}\, 4).$$

Άρα, ο ισχυρισμός:

$$\text{αν } x = y^2 + z^2 \text{ τότε } y^2 + z^2 \equiv 3 (\mathrm{mod}\, 4)$$

καταλήγει σε άτοπο.

Συνεπώς στο σύνολο των ακεραίων αριθμών, η εξίσωση

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

δεν έχει λύση και άρα και η εξίσωση

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

δεν έχει λύση και συνεπώς ούτε και η εξίσωση

$$x^n = y^n + z^n$$

έχει λύση στο $\mathbb{Z}$ αν ο x είναι της μορφής $4\kappa + 3$, $\kappa \in \mathbb{Z}$.

■

7) ***Να αποδειχθεί ότι***

$$\boldsymbol{\pi(x) \geq \log\log x},$$

για $\boldsymbol{x \geq 2}$ ***με την βοήθεια της ανισότητας***

$$\boldsymbol{p_n < 2^{2^n}}$$

($\boldsymbol{p_n}$ ***είναι ο*** $\boldsymbol{n}$***–οστός πρώτος αριθμός) .***

ΑΠΟΔΕΙΞΗ

Παρατηρούμε ότι στην ανισότητα που θέλουμε να αποδείξουμε παρουσιάζεται "διπλός" λογάριθμος. Για τον λόγο αυτόν θα φράξουμε τον αριθμό x μεταξύ δυνάμεων της μορφής

$$e^{e^n}, \text{ όπου } n \in \mathbb{N}.$$

Έτσι, θεωρούμε

$$e^{e^{n-1}} < x \leq e^{e^n}, \text{ όπου } n \geq 4 \qquad (1)$$

(την περίπτωση $n < 4$ θα την εξετάσουμε μεμονωμένα).

• Σύμφωνα με την υπόδειξη της εκφώνησης, θα αποδείξουμε πρώτα την ανισότητα

$$p_n < 2^{2^n}.$$

Για $n = 1$ ισχύει $2 < 2^2$. Υποθέτοντας ότι $p_n < 2^{2^n}$ αρκεί να δείξουμε ότι

$$p_{n+1} < 2^{2^{n+1}}.$$

Είναι γνωστό ότι

$$p_{n+1} \leq p_1 p_2 \ldots p_n + 1.$$

Η απόδειξη της πρότασης αυτής είναι προφανής καθώς κανένας από τους πρώτους αριθμούς $p_1, p_2, \ldots, p_n$ δεν διαιρεί τον ακέραιο $p_1 p_2 \ldots p_n + 1$. Άρα, ο p_{n+1} είναι ο μικρότερος από τους πιθανούς πρώτους παράγοντές του. Επομένως,

$$p_{n+1} \leq p_1 p_2 \ldots p_n + 1 < 2^{2^1 + 2^2 + \cdots + 2^n} + 1$$

$$= 2^{2(2^n - 1)} + 2^2 < 2^{2(2^n - 1)} \cdot 2^2 = 2^{2^{n+1}},$$

δηλαδή

$$p_{n+1} < 2^{2^{n+1}}.$$

Άρα επαγωγικά δείξαμε πως

$$p_n < 2^{2^n}, \text{ για κάθε } n \in \mathbb{N}.$$

• Θα αποδείξουμε και πάλι κάνοντας χρήση της Μεθόδου της Μαθηματικής Επαγωγής ότι

$$e^{n-1} > 2^n \text{ για κάθε } n \in \mathbb{N} \text{ με } n \geq 4.$$

Για $n=4$ ισχύει ότι $e^3 > 2^4$, (διότι $e > 2.7$).

Υποθέτουμε ότι $e^{n-1} > 2^n$ και θα δείξουμε ότι $e^n > 2^{n+1}$.
Είναι:

$$e^n = e^{n-1}e > 2^n e > 2^n 2 = 2^{n+1}.$$

Συνεπώς,

$$e^{n-1} > 2^n, \text{ για κάθε } n \geq 4 .$$

Έτσι,

$$e^{e^{n-1}} > 2^{2^n}.$$

• Από την παραπάνω ανίσωση και την (1) συνεπάγεται ότι:

$$\pi(x) \geq \pi\left(e^{e^{n-1}}\right) \geq \pi\left(2^{2^n}\right).$$

Όμως,

$$p_n < 2^{2^n} \text{ και } \pi(p_n) = n,$$

δηλαδή

$$\pi\left(2^{2^n}\right) \geq n. \tag{2}$$

Άρα,

$$\pi(x) \geq n.$$

Βέβαια, λόγω της (1) ισχύει ότι

$$\log\log x \leq n. \tag{3}$$

Από τις (2) και (3) προκύπτει ότι

$$\pi(x) \geq \log\log x, \text{ για } x > e^{e^3}.$$

Αρκεί να αποδείξουμε ότι

$$\pi(x) \geq \log\log x \text{ για } 2 \leq x \leq e^{e^3} \text{ (δηλαδή για } n < 4).$$

Για $5 \leq x \leq e^{e^3}$ η απόδειξη είναι προφανής καθώς

$$\log\log x \leq 3 \text{ και } \pi(x) \geq \pi(5) = 3.$$

Για $2 \leq x \leq 5$ είναι $\log\log x \leq \log\log 5 < 0.48$ και $\pi(x) \geq \pi(2) = 1$. Άρα

$$\pi(x) > \log\log x.$$

Συνεπώς, γενικά ισχύει ότι:

$$\pi(x) \geq \log\log x, \text{ για } x \geq 2.$$

■

Παρατήρηση

Το συμπέρασμα του παραπάνω θεωρήματος είναι "πολύ αδύναμο" καθώς οι τιμές της συνάρτησης π(x) αυξάνονται με εξαιρετικά πιο γρήγορους ρυθμούς από τη συνάρτηση $\log\log x$.

Για παράδειγμα όταν $x = 10^{12}$ *η ανισότητα δίνει:*

$$\pi(10^{12}) \geq 3.318\cdots,$$

αλλά

$$\pi(10^{12}) = 37607912018.$$

9. Εφαρμογές στην κρυπτογραφία

Πιστοποίηση πρώτων

Η **πιστοποίηση πρώτων αριθμών** είναι η διαδικασία με την οποία εξετάζουμε αν ένας θετικός ακέραιος είναι πρώτος αριθμός ή όχι.

Γενικά, υπάρχουν δύο είδη διαδικασιών πιστοποίησης πρώτων αριθμών, οι ντετερμινιστικές και οι πιθανοτικές διαδικασίες (ντετερμινιστικοί ή πιθανοτικοί αλγόριθμοι).

Οι ντετερμινιστικοί αλγόριθμοι πιστοποίησης πρώτων αριθμών είναι εκείνοι που αποφαίνονται με απόλυτη βεβαιότητα για το αν ένας θετικός ακέραιος είναι πρώτος ή σύνθετος.

Παράδειγμα τέτοιου είδους αλγορίθμου πιστοποίησης πρώτων, είναι ο **αλγόριθμος Lucas – Lehmer (Lucas – Lehmer test).** Αντιθέτως, πιθανοτικοί είναι οι αλγόριθμοι εκείνοι που αποφαίνονται με μεγάλη πιθανότητα για το αν ένας θετικός ακέραιος είναι πρώτος. Δηλαδή, υπάρχει μια μικρή πιθανότητα να αναγνωρίσουν έναν σύνθετο ακέραιο ως πρώτο (το αντίστροφο όμως δεν συμβαίνει ποτέ). Στην περίπτωση που συμβεί αυτό, τότε ονομάζουμε τον σύνθετο αυτόν ακέραιο ως **ψευδοπρώτο.** Για παράδειγμα, ένας σύνθετος θετικός ακέραιος που ικανοποιεί το Μικρό Θεώρημα του Fermat (το οποίο αποτελεί μια πιθανοτική διαδικασία πιστοποίησης πρώτων), ονομάζεται **ψευδοπρώτος του Fermat** ή **Fermat ψευδοπρώτος**.

Συνήθως, οι πιθανοτικοί αλγόριθμοι πιστοποίησης πρώτων αριθμών είναι αρκετά πιο γρήγοροι από τους ντετερμινιστικούς. Ένα παράδειγμα πολύ αποδοτικού και γρήγορου τέτοιου πιθανοτικού αλγορίθμου είναι το ισχυρό Rabin – Miller test (Rabin – Miller strong pseudoprime test).

Το 2004, ανακαλύφθηκε ένας ντετερμινιστικός αλγόριθμος πιστοποίησης πρώτων αριθμών, ο οποίος δεν είναι απλώς αποδοτικός, αλλά αποδεικνύει επίσης, όντας πολυωνυμικός, πως το πρόβλημα της πιστοποίησης πρώτων αριθμών ανήκει στο P. Δηλαδή, είναι πρόβλημα πολυωνυμικού χρονου. Ο αλγόριθμος αυτός ανακαλυφθηκε από τους Ινδούς μαθηματικούς Manindra Agrawal, Neeraj Kayal και Nitin Saxena, οι οποίοι τον δημοσίευσαν στις 6 Αυγούστου του 2004 στην εργασία τους με τίτλο PRIMES is in P, *Annals of Mathematics 160 (2004), No.2, pp.781–793* Ο αλγόριθμος αυτός είναι πλέον γνωστός ως αλγόριθμος AKS.

Θα προχωρήσουμε, τώρα, στην παρουσίαση κάποιων βασικών συμπερασμάτων και ορισμένων από τους σημαντικότερους αλγορίθμους πιστοποίησης πρώτων.

Αλγόριθμος Fermat (Fermat Primality test)

Από το μικρό θεώρημα του Fermat, γνωρίζουμε ότι αν ο p είναι πρώτος αριθμός, τότε

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p),$$

για κάθε ακέραιο α.

Επομένως, είναι προφανές πως αν για κάποιον ακέραιο β ισχύει ότι

$$\beta^{p-1} \not\equiv 1 (\mathrm{mod}\ p)$$

τότε ο p δεν μπορεί να είναι πρώτος αριθμός.

Έτσι, τα βήματα του στοιχειώδους πιθανοτικού αλγορίθμου πιστοποίησης πρώτων που προκύπτει είναι τα ακόλουθα:

1. Επιλέγουμε έναν θετικό ακέραιο $n \geq 3$ που θέλουμε να εξετάσουμε αν είναι πρώτος.

2. Θεωρούμε το σύνολο $A = \{2, 3, ..., n-2\}$ και επιλέγουμε τυχαία έναν ακέραιο $a \in A$.

3. Υπολογίζουμε το $a^{n-1} (\mathrm{mod}\ n)$.

Αν το αποτέλεσμα του υπολογισμού είναι διαφορετικό του 1, τότε ο n είναι σύνθετος αριθμός, αλλιώς ο n είναι πιθανόν πρώτος αριθμός.

Όπως αντιλαμβανόμαστε από τα βήματα του παραπάνω αλγορίθμου, το κριτήριο του Fermat αποφαίνεται με βεβαιότητα μόνο όταν ο ακέραιος που εξετάζουμε είναι σύνθετος. Αυτό συμβαίνει, διότι υπάρχουν πολλά παραδείγματα σύνθετων φυσικών αριθμών *n* που ικανοποιούν την ισοδυναμία

$$a^{n-1} \equiv 1(mod\, n).$$

Γενικά, αν ο φυσικός αριθμός *n* είναι σύνθετος περιττός και ισχύει $a^n \equiv a(\mathrm{mod}\, n)$, για κάποιον ακέραιο *α,* τότε ο *n* ονομάζεται **ψευδοπρώτος ως προς την βάση *a*** και ο *a* ονομάζεται **Fermat ψεύτης.** Ενώ, αν ισχύει ότι

$$a^{n-1}(\mathrm{mod}\, n) \not\equiv 1 \text{ με } 1 \le a < n,$$

τότε ο *a* ονομάζεται **Fermat μάρτυρας.**

Παράδειγμα

Ο ακέραιος $645 = 3 \cdot 5 \cdot 43$ είναι παράδειγμα ψευδοπρώτου ως προς την βάση 2, καθώς ισχύει ότι

$$2^{645} \equiv 2(\mathrm{mod}\, 645)$$

Θεώρημα

Υπάρχουν άπειροι ψευδοπρώτοι ως προς την βάση 2.

Απόδειξη

Αρκεί να μπορέσουμε να κατασκευάσουμε μια άπειρη ακολουθία διαφορετικών μεταξύ τους ψευδοπρώτων ως προς την βάση 2.

Αν n_0 είναι ένας ψευδοπρώτος ως προς την βάση δύο, μπορούμε να αποδείξουμε πως και ο ακέραιος n_1, με $n_1 = 2^{n_0} - 1 > n_0$ είναι ψευδοπρώτος ως προς την ίδια βάση. Η απόδειξη αυτού του ισχυρισμού παρουσιάζεται παρακάτω:

Ισχύει ότι $n_0 = q_1 \cdot q_2$, για κάποιους ακεραίους q_1, q_2 (αφού ο n_0 είναι σύνθετος) και

$$2^{n_0-1} \equiv 1(\mathrm{mod}\, n)$$

(αφού είναι ψευδοπρώτος ως προς 2).

Όμως, τότε ισχύει ότι $2^{q_1} - 1 \mid 2^{n_0} - 1$, διότι αν θέσουμε $\omega = 2^{q_1}$ ισχύει

$$\omega^{q_2} - 1 = (\omega - 1)\ (\omega^{q_2-1} + \omega^{q_2-2} + ... + 1)$$

Άρα

$$2^{q_1 q_2} - 1 = (2^{q_1} - 1)\ (2^{q_1(q_2-1)} + ... + 1)$$

$$\Leftrightarrow 2^{n_0} - 1 = (2^{q_1} - 1)\ (2^{q_1(q_2-1)} + ... + 1)$$

οπότε, είναι προφανές ότι $2^{q_1} - 1 \mid 2^{n_0} - 1 = n_1$. Δηλαδή, ο ακέραιος αριθμός n_1 είναι σύνθετος.

Επίσης, λόγω του γεγονότος ότι ο n_0 είναι ψευδοπρώτος ως προς την βάση 2, ισχύει ότι

$$2^{n_0} \equiv 2(\mathrm{mod}\, n_0)$$

Επομένως, υπάρχει ακέραιος m τέτοιος ώστε $2^{n_0}-2=mn_0$.

Όμως, τότε λαμβάνουμε

$$2^{n_1-1}=2^{2^{n_0}-2}=2^{mn_0}$$

ή

$$2^{n_1-1}-1=2^{mn_0}-1 \tag{1}$$

Ακολούθως, επειδή ισχύει $n_0 \mid mn_0$ προκύπτει ότι $2^{n_0}-1 \mid 2^{mn_0}-1$ (η απόδειξη είναι όμοια με αυτήν που παρουσιάσαμε παραπάνω). Συνεπώς, μέσω της σχέσης (1) λαμβάνουμε ότι

$$n_1=2^{n_0}-1 \mid 2^{n_1-1}-1$$

ή

$$2^{n_1-1}\equiv 1(\mathrm{mod}\, n_1)$$

Επομένως, ο ακέραιος αριθμός $n_1=2^{n_0}-1$ ικανοποιεί το κριτήριο του Fermat ενώ είναι σύνθετος αριθμός. Άρα, αποτελεί ψευδοπρώτο ως προς την βάση 2.

Από την παραπάνω επιχειρηματολογία, προκύπτει άμεσα πως αν ο n_k είναι ψευδοπρώτος ως προς την βάση 2, τότε και ο

$$n_{k+1}=2^{n_k}-1$$

είναι ψευδοπρώτος ως προς την βάση 2.

Επειδή η ακολουθία n_k είναι γνωσίως αύξουσα και περιλαμβάνει άπειρους όρους, προκύπτει ότι υπάρχουν άπειροι το πλήθος ψευδοπρώτοι ως προς την βάση 2.

Αυτό ολοκληρώνει την απόδειξη του θεωρήματος.

■

Αλγόριθμος Miller – Rabin

Θα παρουσιάσουμε αρχικά κάποιες βασικές ιδιότητες.

Λήμμα

Έστω οι ακέραιοι x, y, n για τους οποίους ισχύει

$$x^2\equiv y^2(\mathrm{mod}\, n),$$

ενώ ταυτόχρονα $x \not\equiv \pm y(\mathrm{mod}\, n)$. Τότε, ο ακέραιος n είναι σύνθετος και μάλιστα ο (x–y, n) είναι ένας μη – τετριμμένος παράγοντάς του.

Απόδειξη

Θέτουμε $d=(x-y,n)$. Αρκεί να αποδείξουμε ότι $d\neq 1,n$.

- Αν $d=1$, προκύπτει ότι $n \nmid (x-y)$. Όμως, γνωρίζουμε ότι $n \mid (x-y)(x+y)$. Συνεπώς, $n \mid (x+y)$. Αλλά, αυτό είναι άτοπο, διότι από τα δεδομένα γνωρίζουμε ότι $x \not\equiv -y(\mathrm{mod}\, n)$

- Αν $d = n$, τότε $n \mid (x - y)$. Άτοπο, αφού $x \not\equiv +\, y (\mathrm{mod}\, n)$.

  Συνεπώς, ο d είναι μη–τετριμμένος διαιρέτης του n και επομένως ο n είναι σύνθετος.

■

Έστω p ένας περιττός πρώτος αριθμός. Τότε, ο $p-1$ είναι άρτιος και μπορούμε να τον αναπαραστήσουμε ως

$$p - 1 = 2^m k,$$

όπου m είναι η μέγιστη δύναμη του 2 που διαιρεί τον $p-1$.

Στην διεθνή βιβλιογραφία, ο ακέραιος αριθμός k αναφέρεται ως squarefree integer (ακέραιος "ελεύθερος τετραγώνου").

Από το μικρό θεώρημα του Fermat γνωρίζουμε ότι

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p)$$

Υπολογίζοντας διαδοχικά τις τετραγωνικές ρίζες του a^{p-1} θα προκύπτει πάντα ένας ακέραιος που θα είναι ίσος με 1 ή $-1 \pmod p$. Οι δύο δυνατές περιπτώσεις που λαμβάνουμε είναι

$$a^{2^q k} \equiv -1 (\mathrm{mod}\, p), \text{ για κάποιον } q \text{ με } 0 \le q \le m-1 \quad (1)$$

ή

$$a^k \equiv 1 (\mathrm{mod}\, p). \quad (2)$$

Ο αλγόριθμος των Miller και Rabin βασίζεται στην παραπάνω ιδιότητα. Η κεντρική ιδέα του αλγορίθμου αυτού είναι πως αν $a^k \not\equiv 1 (\mathrm{mod}\, p)$ και $a^{2^{q_k}} \not\equiv -1 (mod\ p)$, για κάθε q, με $0 \le q \le m-1$, τότε ο ακέραιος αριθμός $n = 2^m k$ είναι σύνθετος.

Πριν παρουσιάσουμε τα βήματα του αλγορίθμου, θα παραθέσουμε κάποιους σχετικούς ορισμούς.

Ορισμοί

Έστω n περιττός σύνθετος ακέραιος με $n - 1 = 2^m k$, όπου m η μέγιστη δύναμη του 2 που διαιρεί τον $n-1$. Αν α είναι ένας ακέραιος με $1 \le a \le n-1$, για τον οποίο ισχύει ότι:

(i) $a^k \not\equiv 1 (\mathrm{mod}\, n)$ και $a^{2^q k} \not\equiv -1 (\mathrm{mod}\, n)$, για κάθε q, με $0 \le q \le m-1$, τότε ο αριθμός a ονομάζεται **ισχυρός μάρτυρας** για τον n.

(ii) Αν $a^k \equiv 1 (\mathrm{mod}\, n)$ ή $a^{2^q k} \equiv -1 (\mathrm{mod}\, n)$, για κάποιον q, με $0 \le q \le m-1$, τότε ο αριθμός n ονομάζεται **ισχυρός ψευδοπρώτος ως προς την βάση *a*** και ο a ονομάζεται *ισχυρός ψεύτης* για τον n.

Προχωρούμε τώρα στην παρουσίαση του αλγορίθμου:

1. Θεωρούμε τον θετικό περιττό ακέραιο $n > 1$ που ενδιαφερόμαστε να εξετάσουμε αν είναι πρώτος.

2. Εκφράζουμε τον $n - 1$ στην μορφή $2^m k$, όπου m η μεγαλύτερη δύναμη του 2 που διαιρεί τον $n - 1$.

3. Επιλέγουμε έναν τυχαίο ακέραιο a στο διάστημα $(0,n)$.

4. Υπολογίζουμε το x_0 τέτοιο ώστε $x_0 \equiv a^k (\mathrm{mod}\, n)$.

Αν $x_0 \equiv \pm 1(\mathrm{mod}\, n)$ τότε ο n είναι πιθανόν πρώτος και ο αλγόριθμος σταματά σ' αυτό το βήμα.

Αλλιώς

4.1 Θέτουμε $x_1 \equiv x_0^2 (\mathrm{mod}\, n)$

Αν $x_1 \equiv 1(\mathrm{mod}\, n)$ τότε ο n είναι σύνθετος αριθμός και μάλιστα ο $(x_0 - 1, n)$ είναι ένας μη – τετριμμένος διαιρέτης του.

Αλλιώς αν $x_1 \equiv -1(\mathrm{mod}\, n)$, τότε ο n είναι πιθανόν πρώτος αριθμός και ο αλγόριθμος σταματά σ΄αυτό το βήμα.

Αλλιώς

4.2 Θέτουμε $x_2 \equiv x_1^2 (\mathrm{mod}\, n)$

Αν $x_2 \equiv 1(\mathrm{mod}\, n)$, τότε ο αριθμός n είναι σύνθετος

Αλλιώς αν $x_2 \equiv -1(\mathrm{mod}\, n)$, τότε ο n είναι πιθανόν πρώτος αριθμός και ο αλγόριθμος σταματά σ΄αυτό το βήμα.

Αλλιώς ο αλγόριθμος ακολουθεί την ίδια διαδικασία ώσπου να οδηγηθεί σε πιθανό πρώτο ή μέχρι να φτάσει στο επίπεδο x_{k-1} .

Αν $x_{k-1} \not\equiv -1(\mathrm{mod}\, n)$, τότε ο αριθμός n είναι σύνθετος.

Παράδειγμα

Για $n = 561$ λαμβάνουμε $n - 1 = 560 = 16 \cdot 35 = 2^4 \cdot 35$. Δηλαδή, $m = 4$ και $k = 35$.

Για $a = 2$, ο αλγόριθμος Miller – Rabin επιστρέφει τα εξής:

$$x_0 \equiv 2^{35} \equiv 263(\mathrm{mod}\, 561)$$

$$x_1 \equiv x_0^2 \equiv 166$$

$$x_2 \equiv x_1^2 \equiv 67$$

$$x_3 \equiv x_2^2 \equiv 1$$

Επομένως από την τελευταία ισοδυναμία προκύπτει ότι ο αριθμός 561 είναι σύνθετος (και το αποτέλεσμα αυτό είναι μαθηματικώς βέβαιο). Πράγματι είναι $561 = 3 \times 11 \times 17$.

Ιστορική Παρατήρηση

Ο Garry Lee Miller είναι σήμερα καθηγητής θεωρητικής πληροφορικής στο Πανεπιστήμιο Carnegie Mellon των ΗΠΑ. Είναι περισσότερο γνωστός για την ανακάλυψη, σε συνεργασία με τον Rabin, του αποδοτικού αλγορίθμου πιστοποίησης πρώτων που αναφέρεται πλέον ως Miller – Rabin primality test. Γι' αυτό του το επίτευγμα, το 2003 του απονεμήθει το βραβείο ACM Paris Kanellakis, ενώ από το 2002 είχε ανακηρυχθεί ως ACM Fellow.

Ο Miller έλαβε το διδακτορικό του από το Πανεπιστήμιο της California, στο Berkeley το 1975. Στη διδακτορική του διατριβή με τίτλο *Riemann's Hypothesis and Tests for Primality* παρουσίασε δύο αλγορίθμους πιστοποίησης πρώτων. Ο ένας αλγόριθμος απαιτούσε $O(n/7)$ βήματα για να δώσει απάντηση, ενώ ο δεύτερος απαιτούσε $O(\log^4 n)$ βήματα. Όμως, ο δεύτερος αυτός αλγόριθμος βασιζόταν στην ορθότητα της Επεκτεταμένης Υπόθεσης Riemann.

Τα πεδία ερεύνης του Miller δεν περιορίζονται μόνο στην Υπολογιστική Θεωρία Αριθμών και την πιστοποίηση πρώτων αριθμών. Έχει διεξάγει έρευνα και στις περιοχές της Υπολογιστικής Γεωμετρίας, των παράλληλων αλγορίθμων και των randomized algorithms.

Αλγόριθμος Solovay – Strassen

Εδώ θα παρουσιάσουμε έναν άλλο διαδεδομένο αλγόριθμο πιστοποίησης πρώτων, ο οποίος ανακαλύφθηκε από τους Robert M. Solovay και Volker Strassen. Παραθέτουμε αυτόν τον αλγόριθμο κυρίως για λόγους ιστορικής πληρότητας, καθώς η μέθοδος των Miller και Rabin είναι πιο αποδοτική (αν και οι δύο αλγόριθμοι απαιτούν πλήθος πράξεων της ίδιας τάξης μεγέθους). Και οι δύο αυτοί πιθανοτικοί αλγόριθμοι παρουσιάστηκαν στις αρχές της δεκαετίας του 1980.

Αρχικά, υπενθυμίζουμε το κριτήριο του Euler.

Θεώρημα *(ΚΡΙΤΗΡΙΟ ΤΟΥ EULER)*

Έστω p περιττός πρώτος αριθμός και a ακέραιος, τέτοιος ώστε $(a, p) = 1$. *Τότε*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\, p).$$

Γενικά, όπου $\left(\frac{a}{n}\right)$ *είναι το σύμβολο του Jacobi.*

Πριν προχωρήσουμε στην παρουσίαση των βημάτων του αλγορίθμου, θα παραθέσουμε κάποιους σχετικούς βασικούς ορισμούς.

Ορισμοί

Έστω n περιττός σύνθετος ακέραιος και a ακέραιος για τον οποίο ισχύει ότι $1 \le a \le n-1$. Τότε

(i) Αν

$$(a,n) > 1 \text{ ή } a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) (mod\ n),$$

ο αριθμός a ονομάζεται **Euler μάρτυρας** για τον ακέραιο *n.*

(ii) Αν

$$(a,n) = 1 \text{ και } a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) (mod\ n),$$

ο *n* ονομάζεται **Euler ψευδοπρώτος** ως προς την βάση *a* και ο ακέραιος *α* ονομάζεται **Euler ψεύτης.**

Ο αλγόριθμος Solovay - Strassen αποτελείται από τα εξής βήματα:

1. Θεωρούμε τον περιττό θετικό ακέραιο $n \ge 3$ που θέλουμε να εξετάσουμε αν είναι πρώτος.

2. Επιλέγουμε τυχαία έναν ακέραιο στο διάστημα $(1, n-1)$.

3. Υπολογίζουμε το $x \equiv a^{(n-1)/2} (\mathrm{mod}\, n)$.

Αν $x \neq 1$ και $x \neq n-1$, τότε ο ακέραιος αριθμός n είναι σύνθετος και ο αλγόριθμος σταματά σ' αυτό το βήμα.

Αλλιώς

3.1 Υπολογίζουμε το σύμβολο Jacobi

$$j = \left(\frac{a}{n}\right).$$

Αν $x \not\equiv j \pmod{n}$, τότε ο ακέραιος αριθμός n είναι σύνθετος και ο αλγόριθμος σταματά σ' αυτό το βήμα.

4. Αν τα παραπάνω βήματα ξεπεραστούν για διάφορες επιλογές του a, τότε ο n είναι πιθανόν πρώτος αριθμός .

Σύμφωνα με τα βήματα του αλγορίθμου αυτού, η μοναδική περίπτωση όπου υπάρχει πιθανότητα να οδηγηθούμε σε λανθασμένο συμπέρασμα, είναι όταν ο n είναι σύνθετος και η αλγοριθμική διαδικασία μας λέει πως ο n είναι πρώτος. Το πλήθος των Euler ψευτών είναι το πολύ

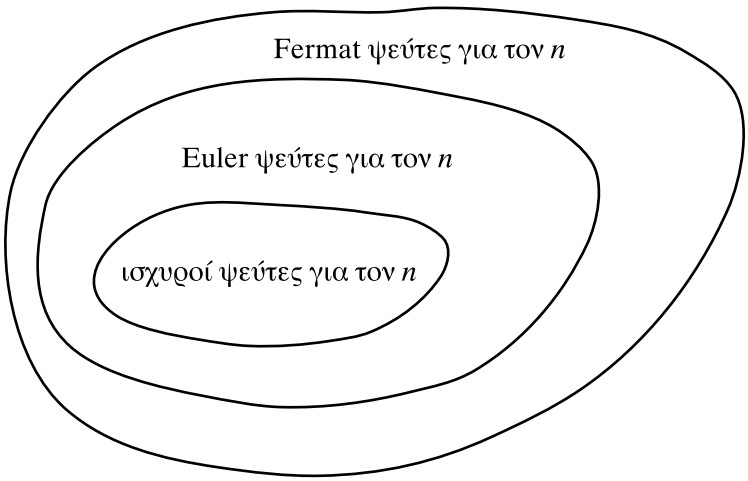
$$\phi(n)/2 < (n-1)/2 .$$

Άρα, η πιθανότητα να προκύψει Euler ψεύτης είναι μικρότερη του 1/2.

Παρατήρηση

- *Αν ο αλγόριθμος επιστρέψει ως αποτέλεσμα πως ο n είναι σύνθετος, τότε αυτό είναι απολύτως βέβαιο. Επίσης, αν ο n είναι πρώτος, τότε πάλι ο αλγόριθμος αποφαίνεται πως ο n είναι πρώτος.*
- *Έχοντας παρουσιάσει τους ορισμούς των Euler ψεύτη, Fermat ψεύτη και ισχυρού ψεύτη για τον n, μπορούμε να παραθέσουμε κάποια γενικά συμπεράσματα:*
  (Α) Αν ο ακέραιος α είναι Euler ψεύτης για τον n, τότε είναι και Fermat ψεύτης για τον n.
  (Β) Αν ο ακέραιος α είναι ισχυρός ψεύτης για τον n, τότε είναι και Euler ψεύτης για τον n.

Τα παραπάνω συμπεράσματα μπορούν να αναπαρασταθούν γραφικά ως εξής:



Παραγοντοποίηση Ακεραίων σε ΠρώτουςΠαράγοντες

Η παραγοντοποίηση ακεραίων σε πρώτους παράγοντες απασχολεί τους μαθηματικούς από την αρχαιότητα έως και στις μέρες μας.

Στην σύγχρονη Θεωρία Αριθμών, η εύρεση πρώτων παραγόντων μεγάλων ακέραιων αριθμών αποτελεί ένα από τα δυσκολότερα και σημαντικότερα προβλήματα λόγω και των εφαρμογών που βρίσκει στην Κρυπτογραφία. Έτσι, έχουν ανακαλυφθεί διάφορες μέθοδοι για την επίλυση αυτού του προβλήματος. Βέβαια, η μέχρι σήμερα έλλειψη ενός πολυωνυμικού αλγορίθμου για την επίλυσή του, έπαιξε πολύ σημαντικό ρόλο στην ανακάλυψη του κρυπτοσυστήματος RSA, η ασφάλεια του οποίου βασίζεται στην δυσκολία παραγοντοποίησης ενός ακεραίου αριθμού $n = p \cdot q$, όπου p, q είναι μεγάλοι πρώτοι αριθμοί.

Φυσικά, ένας ακόμα λόγος που αιτιολογεί την σπουδαιότητα της εύρεσης των πρώτων παραγόντων ενός ακεραίου είναι η ιδιότητα των ακεραίων να αναπαρίστανται σε κανονική μορφή κατά μοναδικό τρόπο.

Σ' αυτό το σημείο πρέπει να παρατηρήσουμε πως κάποια σύνολα αριθμών έχουν την ιδιότητα αυτή, ενώ κάποια άλλα όχι. Για παράδειγμα στο σύνολο των ακεραίων του Gauss $\mathbb{Z}[i]$ η ιδιότητα αυτή ισχύει, ακριβώς όπως συμβαίνει και στο σύνολο των ακεραίων. Αντιθέτως, όμως, θα παρουσιάσουμε παρακάτω ένα δακτύλιο που δεν υπακούει στήν ιδιότητα αυτήν.

Θεωρούμε το σύνολο

$$A = \{ a + bk \text{ , όπου } a, b \in \mathbb{Z} \text{ και } k \text{ συμβολίζει την τετραγωνική ρίζα του } -5 \}.$$

Τότε λαμβάνουμε

$$2 \cdot 3 = 6 = 1 + 5 = 1 - k^2 = (1-k)(1+k).$$

Όμως, οι αριθμοί 2,3, $1-k$, $1+k \in A$ δεν μπορούν να παραγοντοποιηθούν στο σύνολο A. Επομένως, εντοπίσαμε ένα στοιχείο του συνόλου αυτού που επιδέχεται περισσότερες από μία παραγοντοποιήσεις.

Θα ασχοληθούμε με την παραγοντοποίηση στο σύνολο των ακεραίων αριθμών, στο οποίο η κανονική αναπαράσταση είναι μοναδική.

Θα παρουσιάσουμε κάποιους από τους βασικότερους αλγορίθμους που έχουν ως σκοπό την επίλυση του προβλήματος αυτού.

Ο αρχαιότερος και πλέον στοιχειώδης τέτοιος αλγόριθμος είναι αυτός των διαδοχικών διαιρέσεων. Ο αλγόριθμος βασίζεται στο ακόλουθο λήμμα, γνωστό από την εποχή του Ερατοσθένη.

Λήμμα

Αν n είναι ένας σύνθετος θετικός ακέραιος, τότε έχει πρώτο διαιρέτη p, όπου $p \le \sqrt{n}$.

Απόδειξη

Αναπαριστούμε τον n στην κανονική του μορφή. Τότε

$$n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}, \quad \text{όπου} \quad k \ge 2 .$$

Αν κανένας από τους πρώτους παράγοντες $p_1, p_2, \ldots, p_k$ του n δεν ήταν μικρότερος ή το πολύ ίσος προς n, τότε προφανώς θα ίσχυε

$$n = \sqrt{n}\sqrt{n} < p_i p_j \le p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} = n ,$$

όπου $1 \le i, j \le k$ με $i \ne j$, που είναι άτοπο.

Επομένως, πρέπει να υπάρχει τουλάχιστον ένας πρώτος διαιρέτης p του n, για τον οποίο να ισχύει ότι $p \le \sqrt{n}$.

■

Έτσι, προκειμένου να παραγοντοποιήσουμε έναν θετικό ακέραιο n, αναζητούμε έναν από τους πρώτους παράγοντές του p_1, ανάμεσα στους ακεραίους που ανήκουν στο διάστημα $[2, \sqrt{n}]$.

Όταν εντοπίσουμε τον p_1, διεξάγουμε την ίδια διαδικασία αναζητώντας έναν πρώτο διαιρέτη p_2 του ακεραίου $n|p_1$. Συνεχίζοντας με τον ίδιο τρόπο προσδιορίζουμε πρώτους διαιρέτες, ώσπου να φτάσουμε στο στάδιο για το οποίο ισχύει η

$$n \left| p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} = 1. \right.$$

Η μέθοδος αυτή είναι γνωστή ως το **Κόσκινο του Ερατοσθένη**.

Βέβαια, όπως γίνεται εύκολα κατανοητό, αν ο n είναι κατασκευασμένος από μεγάλους πρώτους αριθμούς, τότε η μέθοδος αυτή δεν είναι καθόλου αποτελεσματική. Συνεπως, η ασφάλεια ενός κρυπτοσυστήματος όπως το RSA που βασίζεται στην δυσκολία παραγοντοποίησης ενός θετικού ακεραίου $n = p \cdot q$, όπου p, q δύο μεγάλοι πρώτοι αριθμοί, δεν επηρεάζεται καθόλου από τον αλγόριθμο αυτόν.

Ιστορική Παρατήρηση

Ο Ερατοσθένης ο Κυρηναίος (ή Ερατοσθένης ο Πένταθλος), γεννήθηκε το 276 π.Χ., στην Κυρήνη (σημερινή Λιβύη) και πέθανε το 194 π.Χ. στην Αλεξάνδρεια.

Ήταν Έλληνας μαθηματικός, αστρονόμος, αθλητής, ποιητής και γεωγράφος. Σπούδασε στην Αλεξάνδρεια και το 236 π.Χ, ο Πτολεμαίος Γ΄ ο Ευεργέτης, του παραχώρησε την θέση του Αρχηβιβλιοθηκάριου της βιβλιοθήκης της Αλεξάνδρειας. Έτσι, έγινε ο τρίτος βιβλιοθηκάριος, διαδεχόμενος τον Ζηνόδοτο.

Συνέβαλε καθοριστικά με σημαντικές ανακαλύψεις, όπως το κόσκινο για την παραγοντοποίηση ακεραίων σε πρώτους παράγοντες, τον υπολογισμό της περιφέρειας της Γης με αξιοθαύμαστη ακρίβεια (περίπου το 240 π.Χ.), την ανακάλυψη συστήματος παράλληλων και μεσημβρινών, την ανακάλυψη του σφαιρικού αστρολάβου (περίπου το 255 π.Χ.) και την δημιουργία ενός χάρτη του κόσμου βασιζόμενος στην υπάρχουσα γεωγραφική γνώση της εποχής. Φημολογείται, πως είχε επίσης υπολογίσει την απόσταση μεταξύ Γης και Ήλιου.

> ***Παρατήρηση***
>
> *Στην περίπτωση που γνωρίζουμε την τιμή της συνάρτησης του Euler $\phi(n)$, για κάποιον ακέραιο $n = p \cdot q$, όπου p,q είναι πρώτοι αριθμοί, τότε μπορούμε πολύ εύκολα να προσδιορίσουμε τους πρώτους παράγοντες p,q του n, όπως θα δείξουμε παρακάτω. Σε μια τέτοια περίπτωση, η ασφάλεια ενός κρυπτοσυστήματος όπως το RSA θα κατέρεε. Όμως, ο προσδιορισμός της τιμής της $\phi(n)$ για κάποιον τυχαίο θετικό ακέραιο n είναι εξίσου δύσκολος με την παραγοντοποίηση του n.*
>
> *Έστω πως γνωρίζουμε την τιμή της $\phi(n)$. Τότε, έχουμε*
>
> $$n = p \cdot q$$
>
> και
>
> $$\phi(n) = (p-1)(q-1)$$
>
> *Θέτουμε όπου q το n/p. Τότε, λαμβάνουμε*

$$\phi(n) = n - p - \frac{n}{p} + 1$$

$$\Leftrightarrow p\phi(n) = p(n+1) - p^2 - n$$

$$\Leftrightarrow p^2 + (\phi(n) - n - 1)p + n = 0$$

Επομένως, λύνοντας την παραπάνω δευτεροβάθμια εξίσωση ως προς p υπολογίζουμε τον πρώτο παράγοντα του n. Ο υπολογισμός και του q είναι πλέον πολύ εύκολος.
Μία ακόμη στοιχειώδης μέθοδος για την παραγοντοποίηση ενός θετικού ακέραιου n είναι η ***μέθοδος του Fermat*** *(Fermat factorization method)****.***
Η κεντρική ιδέα της μεθόδου είναι να εκφράσουμε τον ακέραιο n ως διαφορά δύο τετραγώνων ακέραιων αριθμών.
Τότε

$$n = a^2 - b^2 = (a-b)(a+b)$$

Οπότε, έχουμε μια αρχική παραγοντοποίηση του n. Συνεχίζοντας την ίδια διαδικασία για τους ακέραιους παράγοντες που προκύπτουν, τελικά ο n θα αναλυθεί σε πρώτους παράγοντες.

Η διαδικασία προκειμένου να βρούμε δύο ακεραίους a, b *για τους οποίους* $n = a^2 - b^2$ *είναι η εξής:*

Υπολογίζουμε τις τιμές των ακεραίων $n+1^2,\ n+2^2,\ n+3^2, \ldots$ *έως ότου το αποτέλεσμα που θα προκύψει να αποτελεί τέλειο τετράγωνο ακεραίου. (Αν ο n αποτελεί το γινόμενο δύο πρώτων αριθμών* p, q *τότε απαιτούνται* $|p-q|/2$ *βήματα προκειμένου να τους εντοπίσει ο αλγόριθμος).*

Παράδειγμα

Είναι

$$424983 + 11^2 = 425104 = 652^2$$

Έτσι

$$424983 = (652-11)(652+11) = 641 \cdot 663$$

Ο αριθμός 641 είναι πρώτος και ο 663 εύκολα παραγοντοποιείται.

$$663 = 3 \cdot 221 = 3 \cdot 13 \cdot 17$$

Συνεπώς, λαμβάνουμε

$$424983 = 3 \cdot 13 \cdot 17 \cdot 641$$

■

Θα προχωρήσουμε τώρα, στην παρουσίαση ενός πιο αποδοτικού αλγορίθμου παραγοντοποίησης.

Αλγόριθμος *p* – 1 του Pollard

ο Αλγόριθμος αυτός προτάθηκε το 1974 από τον John Pollard και είναι αποδοτικός για την παραγοντοποίηση ακεραίων που οι παράγοντές τους έχουν συγκεκριμμένες ιδιότητες (στην διεθνή βιβλιογραφία, τέτοιου είδους αλγόριθμοι καλούνται special – purpose algorithms).

Πριν προχωρήσουμε στην καταγραφή των βημάτων του αλγορίθμου θα παρουσιάσουμε την κεντρική ιδέα στην οποία αυτός βασίζεται.

Έστω n ο σύνθετος αριθμός που επιθυμούμε να παραγοντοποιήσουμε και p ένας πρώτος

παράγοντάς του. Ας υποθέσουμε πως B είναι ένας ακέραιος αριθμός, για τον οποίο κάθε δύναμη p^m για την οποία ισχύει ότι $p^m \mid p-1$, είναι μικρότερη ή το πολύ ίση με το B.

Θέτουμε, τώρα,

$$\lambda = \prod_{q \le B} q^{\lfloor \log_q B \rfloor},$$

όπου το γινόμενο εκτείνεται στους πρώτους αριθμούς $q \le B$. Τότε, από το μικρό θεώρημα του Fermat, εύκολα προκύπτει ότι

$$a^{\lambda} \equiv 1 (\mathrm{mod}\ p) \ .$$

Συνεπώς, ισχύει ότι $(a^{\lambda}-1, n) \ge p > 1$. Επομένως, αν $(a^{\lambda}-1, n) \ne n$ τότε ο μέγιστος κοινός διαιρέτης των $a^{\lambda}-1$, n είναι ένας μη τετριμμένος παράγοντας του n.

Ακολουθεί η αναλυτική περιγραφή των βημάτων του αλγορίθμου:

1. Επιλέγουμε έναν θετικό ακέραιο B (σχετικά μικρό π.χ. B = 20) και στην συνέχεια υπολογίζουμε το λ τέτοιο ώστε

$$\lambda = \prod_{q \le B} q^{\lfloor \log_q B \rfloor},$$

όπου το γινόμενο εκτείνεται στους πρώτους αριθμούς $q \le B$.

2. Επιλέγουμε τυχαία έναν ακέραιο αριθμό a για τον οποίο ισχύει ότι $1 < a < n$ και υπολογίζουμε το (a, n).

2.1 Αν $(a,n) > 1$ τότε ο μέγιστος κοινός διαιρέτης των (a,n) είναι ένας μη τετριμμένος παράγοντας του n.

αλλιώς

2.2 Υπολογίζουμε το $(a^{\lambda}-1, n)$.

2.3 Αν $(a^{\lambda}-1, n) > 1$ και $(a^{\lambda}-1, n) \ne n$ τότε ο μέγιστος κοινός διαιρέτης των $a^{\lambda}-1$, n είναι ένας μη τετριμμένος παράγοντας του n.

αλλιώς

2.4 Επιλέγουμε έναν διαφορετικό ακέραιο αριθμό a και επιστρέφουμε στο βήμα 2.1 του αλγορίθμου.

Παράδειγμα

Θα παρουσιάσουμε τώρα ένα παράδειγμα εκτέλεσης του αλγορίθμου αυτού. Επιθυμούμε να παραγοντοποιήσουμε τον ακέραιο $n = 1241143$.

Όπως υπαγορεύει το πρώτο βήμα, επιλέγουμε μια βάση παραγόντων B, σχετικά μικρή. Έστω, λοιπόν, B =13. Στην συνέχεια υπολογίζουμε το λ που εδώ προκύπτει ότι είναι

$$\lambda = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$$

Επιλέγουμε, τώρα, τυχαία έναν ακέραιο αριθμό a, με $1 < a < n$. Έστω a = 2. Τότε, ισχύει ότι

$$(2, 1241143) = 1 .$$

Συνεπώς, σύμφωνα με όσα υπαγορεύει ο αλγόριθμος, θα προχωρήσουμε στον υπολογισμό του

$$a^{\lambda} - 1 = 2^{32760} - 1 .$$

Όμως, παρατηρούμε (με χρήση του αλγορίθμου του Ευκλείδη για τον υπολογισμό του μέγιστου κοινού διαιρέτη) πως

$$(2^{32760}-1, 1241143) = 547 > 1$$

και $547 \neq 1241143$.

Επομένως, ο αριθμός 547 αποτελεί μη τετριμμένο παράγοντα του αριθμού 1241143 και μάλιστα είναι πρώτος παράγοντας.

Έτσι, μετά από μια διαίρεση προκύπτει

$$1241143 = 2269 \cdot 547,$$

όπου ο φυσικός αριθμός 2269 είναι και αυτός πρώτος. Άρα, εδώ ολοκληρώθηκε η διαδικασία παραγοντοποίησης του αριθμού n = 1241143.

Το πρόβλημα του Διακριτού Λογαρίθμου

Έστω η πεπερασμένη πολλαπλασιαστική ομάδα $(G, \cdot)$. Αν $a \in G$ και $<\alpha>$ είναι η κυκλική υποομάδα τάξης n που παράγεται από το α, τότε για κάθε $\beta \in < a >$ υπάρχει μοναδικός ακέραιος x, με $0 \leq x \leq n-1$, τέτοιος ώστε $\beta = a^x$.

Το πρόβλημα της εύρεσης του x, για δοσμένους ακεραίους a, β (που ανήκουν στο $\mathbb{Z}_n$ ή γενικά στην πολλαπλασιαστική ομάδα G στην οποία αναφερόμαστε) είναι γνωστό ως το **πρόβλημα του διακριτού λογαρίθμου** και ο ακέραιος αριθμός x ονομάζεται ο διακριτός λογάριθμος του β ως προς την βάση α.

Για παράδειγμα, αν θέσουμε $\alpha = 2$, $x = 17$ και $p = 13$, τότε επειδή

$$2^{17} = 131072 = 10082 \cdot 13 + 6,$$

προκύπτει ότι $6 \equiv 2^{17} (\mathrm{mod}\, 13)$.

Επομένως, ο διακριτός λογάριθμος του 6 με βάση το 2 είναι ο 17.

Στο παραπάνω παράδειγμα, αν στα δεδομένα είχαμε $p = 13$, $a = 2, \beta = 6$, η εύρεση του x δεν θα αποτελούσε δύσκολο πρόβλημα επειδή τυχαίνει η τιμή που ικανοποιεί την ισοδυναμία $\beta \equiv \alpha^x (\mathrm{mod}\ p)$ να είναι σχετικά μικρή. Οπότε, μια διαδικασία όπως η μέθοδος απαρίθμησης (square – and – multiply)* θα μας έδινε απάντηση στο πρόβλημα σε σύντομο χρονικό διάστημα.

Όμως, αν το πρόβλημα ήταν ο υπολογισμός του διακριτού λογαρίθμου για $a = 2199$, $\beta = 1907$, και $p = 2633$, τότε η διαδικασία γίνεται αρκετά πολύπλοκη και η μέθοδος απαρίθμησης δεν είναι αποδοτική (ισχύει ότι $1907 \equiv 2199^{2269} (\mathrm{mod}\, 2633)$).

Συνήθως, η διαδικασία υπολογισμού του διακριτού λογαρίθμου είναι πολύ δύσκολη. Για τον λόγο αυτό έχουν γίνει πολλές προσπάθειες για την κατασκευή αλγορίθμων υπολογισμού του.

(*) Η μέθοδος απαρίθμησης (square – and – multiply) είναι μέθοδος ύψωσης σε δύναμη. Υπολογίζει την τιμή του a^κ από τα a και κ, όπου

$$\kappa = \sum_{i=0}^{m-1} b_i 2^i \quad \text{καί} \quad \alpha^\kappa = \prod_{i=0}^{m-1} \left(a^{2^i}\right)^{b_i}, \quad \text{όπου } b_i \in \{0,1\}$$

Όμως, δεν έχει ανακαλυφθεί ακόμα αλγόριθμος που δίνει απάντηση στο πρόβλημα σε πολυωνυμικό χρόνο.

Λόγω της μεγάλης δυσκολίας που έγκειται, στην πλειοψηφία των περιπτώσεων, στην εύρεση του ακεραίου x που ικανοποιεί την ισοδυναμία $a^x \equiv \beta (\mathrm{mod}\ p)$, το πρόβλημα του διακριτού λογαρίθμου εφαρμόζεται ιδιαίτερα στον κλάδο της Κρυπτογραφίας.

Θα προχωρήσουμε τώρα στην παρουσίαση διάφορων μεθόδων και αλγορίθμων προσδιορισμού του διακριτού λογαρίθμου.

Σημείωση: Οι χαρακτήρες a, β, x θα χρησιμοποιούνται σ' αυτήν την ενότητα αντιπροσωπεύοντας τα στοιχεία που επαληθεύουν το πρόβλημα του διακριτού λογαρίθμου

$$x = log_a \beta \ \Leftrightarrow \ \beta = a^x .$$

Λήμμα
Έστω p πρώτος αριθμός. Τότε

$$\beta^{(p-1)/2} \equiv \begin{cases} +1, & \text{αν } o\ x \text{ είναι άρτιος αριθμός} \\ -1, & \text{αν } o\ x \text{ είναι περιττός αριθμός} \end{cases}$$

Σημείωση: Σύμφωνα με το Λήμμα, στο $\mathbb{Z}_p^*$ το τελευταίο bit του διακριτού λογαρίθμου είναι άχρηστο. Επίσης, για $G = < g >$, $|< g >| = n$ και $n = 2^r \cdot m$, όπου m είναι περιττός φυσικός αριθμός, ισχύει ότι τα r τελευταία bits του διακριτού λογαρίθμου είναι άχρηστα.

Απόδειξη
Ισχύει ότι

$$a^x \equiv \beta (\mathrm{mod}\ p),\ 0 \le x \le p-1 \qquad (1)$$

Από το μικρό θεώρημα του Fermat γνωρίζουμε ότι

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p) \Leftrightarrow (a^{\frac{p-1}{2}})^2 \equiv 1 (\mathrm{mod}\ p) \qquad (2)$$

Όμως, γενικά, οι μοναδικές λύσεις της ισοδυναμίας $y^2 \equiv 1 (\mathrm{mod}\ p)$ είναι οι $y \equiv \pm 1 (\mathrm{mod}\ p)$. Αυτό ισχύει διότι $p \mid y^2 - 1$ δηλαδή $p \mid (y-1)(y+1)$. Συνεπώς, από το πρώτο θεώρημα του Ευκλείδη προκύπτει ότι $p \mid y-1$ ή $p \mid y+1$.

Επομένως, από την σχέση (2) λαμβάνουμε

$$a^{\frac{p-1}{2}} \equiv \pm 1 (\mathrm{mod}\ p)$$

Αλλά,

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p)$$

και ο εκθέτης $p-1$ είναι ο μικρότερος φυσικός αριθμός που έχει την ιδιότητα αυτή. Άρα

$$a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\ p) .$$

Από την παραπάνω σχέση και από την σχέση (1) λαμβάνουμε

$$\beta^{\frac{p-1}{2}} \equiv a^{x\cdot\frac{p-1}{2}} \equiv (-1)^x (\text{mod } p)\,.$$

Άρα

$$\beta^{\frac{p-1}{2}} \equiv (-1)^x (mod\ p)\,,$$

δηλαδή

$$\beta^{\frac{p-1}{2}} \equiv 1(\text{mod } p)\,,\ \text{αν ο } x \text{ είναι άρτιος}$$

ή

$$\beta^{\frac{p-1}{2}} \equiv -1(\text{mod } p)\,,\ \text{αν ο } x \text{ είναι περιττός}\,.$$

■

Ανταλλαγή κλειδού Diffie - Hellman

Η μέθοδος ανταλλαγής κλειδιού Diffie – Hellman ή το πρωτόκολλο Diffie – Hellman, αξιοποιείται προκειμένου να επιτευχθεί η ασφαλής ανταλλαγή κλειδιού κάποιου κρυπτοσυστήματος μέσω ενός μη ασφαλούς διαύλου επικοινωνίας.

Υποθέτουμε πως η Kim και ο Russell θέλουν να ανταλλάξουν ένα κλειδί. Επιλέγουν, έναν μεγάλο πρώτο αριθμό p και μια πρωταρχική ρίζα α, όπου $2 \le a \le p-2$, χωρίς να ενδιαφέρονται αν κάποιος παρακολουθεί την συνομιλία τους.

Ακολούθως, η Kim επιλέγει έναν ακέραιο αριθμό k με $0 \le k \le p-2$, τον οποίο θα κρατήσει κρυφό και υπολογίζει έναν ακέραιο c, τέτοιον ώστε

$$c \equiv a^k (\text{mod } p)\,,\ \text{όπου } 1 \le c \le p-1\,. \qquad (1)$$

Η Kim αποστέλλει στον Russel την τιμή του ακεραίου c μέσω κάποιου διαύλου επικοινωνίας.

Ο Russel, ακολουθεί την αντίστοιχη διαδικασία επιλέγοντας έναν ακέραιο r με $0 \le r \le p-2$, τον οποίο κρατά κρυφό και υπολογίζει έναν ακέραιο e τέτοιον ώστε

$$e \equiv a^r (\text{mod } p)\,,\ \text{όπου } 1 \le e \le p-1\,. \qquad (2)$$

Ο Russel με την σειρά του αποστέλλει στην Kim την τιμή του ακεραίου e.

Στην συνέχεια, η Kim και ο Russel με τα στοιχεία που έχουν κατασκευάζουν ένα κοινό κλειδί S.

Η διαδικασία κατασκευής είναι η ακόλουθη:

Η Kim υπολογίζει

$$S \equiv e^k (\text{mod } p)$$

και ο Russel υπολογίζει

$$S \equiv c^r (\text{mod } p)\,.$$

Από τους παραπάνω υπολογισμούς προκύπτει κοινό κλειδί S, διότι από τις σχέσεις (1), (2) έχουμε

$$e^k \equiv a^{kr} (\text{mod } p)$$

και

$$c^r \equiv a^{kr} (\text{mod } p)\,.$$

Η ασφάλεια της μεθόδου αυτής βασίζεται στην μεγάλη δυσκολία υπολογισμού του διακριτού λογαρίθμου. Αυτό γίνεται κατανοητό, διότι οι ακέραιοι αριθμοί p, α, c, e αποστέλονται μέσω ενός μη ασφαλούς διαύλου και επομένως είναι πιθανόν να γίνουν γνωστοί σ' ένα άλλο άτομο, τον Bill, στον οποίο η Kim και ο Russel δεν επιθυμούν να γνωστοποιήσουν το κλειδί. Ο μοναδικός τρόπος, ώστε ο Bill να ανακαλύψει το κλειδί γνωρίζοντας μόνο τους p, α, c, e είναι να υπολογίσει τον διακριτό λογάριθμο $k = \log_a c$ και ακολούθως το κλειδί $S \equiv e^k \pmod p$ ή να υπολογίσει το διακριτό λογάριθμο $r = \log_a e$ και ακολούθως το κλειδί $S \equiv c^r \pmod p$.

Λόγω του γεγονότος ότι οι αλγόριθμοι που γνωρίζουμε, ως σήμερα, δεν είναι αρκετά αποδοτικοί ώστε να υπολογίζουν σχετικά σύντομα τον διακριτό λογάριθμο, όταν γίνει κατάλληλη επιλογή της πολλαπλασιαστικής ομάδας G, και του γεννήτορα α της κυκλικής υποομάδας $<\alpha>$, η μέθοδος Diffie – Hellman θεωρείται ασφαλής. Σήμαρα οι αριθμοί με περισσότερα από 120 ψηφία θεωρούναι ασφαλείς για το DLP.

Ιστορική Παρατήρηση

Η μέθοδος Diffie – Hellman δημοσιεύτηκε για πρώτη φορά το 1976 από τους Whitfield Diffie και Martin Hellman. Όμως, είχε ανακαλυφθεί λίγα χρόνια νωρίτερα από τον Malcolm J. Williamson της Βρεττανικής υπηρεσίας πληροφοριών σημάτων και είχε παραμείνει απόρρητο, μέχρι το έτος 1997.

Θεωρείται πως είναι η πρώτη μέθοδος για την πραγματοποίηση μιας ασφαλούς ανταλλαγής ενός κρυφού κλειδιού μέσω ενός μη ασφαλούς διαύλου επικοινωνίας. Πρέπει να τονιστεί πως στην μέθοδο αυτήν ο ασφαλής δίαυλος περιττεύει, πράγμα που δεν ισχύει στα συμμετρικά κρυπτοσυστήματα.

Οι Diffie και Hellman βασίστηκαν στο έργο του Ralph Merkle και για τον λόγο αυτόν ο Hellman, το 2002, πρότεινε να μετονομαστεί η μέθοδος από Diffie – Hellman σε Diffie – Hellman Merkle.

Σημείωση: Από τους αλγορίθμους που θα παρουσιάσουμε παρακάτω, οι αλγόριθμοι του Shanks, του Pohlig – Hellman και οι μέθοδοι του Pollard δεν απαιτούν η ομάδα να είναι υποομάδα της πολλαπλασιαστικής ομάδας κάποιου πεπερασμένου σώματος. Δουλεύουν στην οποιαδήποτε κυκλική ομάδα και κατά συνέπεια, οι προσθετικοί συμβολισμοί που χρησιμοποιούνται στις ελλειπτικές καμπύλες δεν δημιουργούν πρόβλημα.

Αλγόριθμος Baby step – Giant step (ή Αλγόριθμος του Shanks).

Ο Αλγόριθμος που θα παρουσιάσουμε, οφείλεται στον D. Shanks* και σκοπό έχει τον υπολογισμό του διακριτού λογαρίθμου $\log_a \beta \pmod p$, ως προς έναν πρώτο αριθμό p.

Πριν προχωρήσουμε στην καταγραφή των βημάτων του αλγορίθμου, θα παραθέσουμε την λογική διεργασία που οδηγεί στην κατασκευή του.

Επιθυμούμε να υπολογίσουμε τον ακέραιο x τέτοιον ώστε $a^x \equiv \beta \pmod p$. Όμως, είναι γνωστό πως μπορούμε να εκφράσουμε τον x ως $ln+q$, όπου $0 \le q \le n-1$, $0 \le l < p/n$, για

*D. Shanks. Class number, a theory of factorization and genera. 1969 Number Theory Institute, Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, NY, p.p. 415 - 440, 1969.

κάποιον ακέραιο αριθμό $n = \lceil \sqrt{p-1} \rceil$.

Έτσι, έχουμε ότι

$$a^{ln+q} \equiv \beta (mod\ p)$$

ή $$a^{ln} a^{q} \equiv \beta (mod\ p)$$

ή $$a^{ln} \equiv \beta a^{-q} (mod\ p) \quad (1)$$

όπου ο n είναι σταθερός, ενώ οι l, q μπορούν να λαμβάνουν διάφορες ακέραιες τιμές στα διαστήματα $[0, n-1]$ και $[0, p/n)$ αντίστοιχα.

Συνεπώς, ο σκοπός μας είναι να εντοπίσουμε εκείνες τις τιμές των *l, q* που ικανοποιούν την σχέση (1). Η πιθανότητα εύρεσης τέτοιου ζεύγους είναι ικανοποιητική.

Επομένως, τα βήματα του αλγορίθμου είναι τα εξής:

1. Θέτουμε $n = \lceil \sqrt{p-1} \rceil$

2. Υπολογίζουμε το $a^{ln} (mod\ p)$, για κάθε διαφορετική τιμή του *l,* με $0 \le l < p/n$.

3. Ταξινομούμε όλα τα ζεύγη $(l, a^{ln} (mod\ p))$ που προκύπτουν, σε αύξουσα σειρά ως προς την τεταγμένη $a^{ln} (mod\ p)$. Έτσι, δημιουργείται μια αύξουσα ακολουθία S_1.

4. Υπολογίζουμε το $\beta\alpha^{-q} (\mathrm{mod}\ p)$, για κάθε διαφορετική τιμή του q με $0 \le q \le n-1$.

5. Όμοια, ταξινομούμε όλα τα ζεύγη $(q, \beta a^{-q} (mod\ p))$, σε αύξουσα σειρά ως προς την τεταγμένη $\beta a^{-q} (mod\ p)$. Έτσι, δημιουργείται μια αύξουσα ακολουθία S_2.

6. Ελέγχουμε τις αύξουσες ακολουθίες που έχουν προκύψει από τα βήματα (3), (5) ώστε να βρούμε δύο ζεύγη (l, ω) και (q, ω) τέτοια ώστε $\omega \in S_1$ και $\omega \in S_2$.

7. Τότε, θα ισχύει $a^{nl} \equiv \omega \equiv \beta a^{-q} (\mathrm{mod}\ p)$ και επομένως ο διακριτός λογάριθμος x που αναζητούμε θα είναι ο ακέραιος αριθμός $ln+q$, για τις συγκεκριμένες τιμές των l, q που εντοπίσαμε στο βήμα (6).

Ο αλγόριθμος του Shanks μπορεί να διατυπωθεί και σ' ένα γενικότερο πλαίσιο, χωρίς οι υπολογισμοί να γίνονται $\mathrm{mod}\ p$, όπου p είναι πρώτος αριθμός.

Θεωρούμε την προσθετική ομάδα G τάξης *n* και τα στοιχεία $P, Q \in G$. Θεωρούμε επίσης πως το στοιχείο *P* είναι γεννήτορας της *G.* Τότε, τα βήματα μπορούν να γραφούν ως εξής:

1. Επιλέγουμε κάποιον φυσικό αριθμό $m \ge \sqrt{n}$.

2. Υπολογίζουμε το $R = mP$.

3. Υπολογίζουμε τις τιμές qP για $0 \le q < m$ και τις αποθηκεύουμε σε μια λίστα L.

Αυτό το βήμα αποτελεί το Baby step.

4. Υπολογίζουμε τις τιμές $Q - lR$, για $0 \le l < m$, μέχρι να βρούμε μια τιμή που να ταυτίζεται με κάποιο στοιχείο της λίστας *L.* (Αυτό το βήμα αποτελεί το Giant step).

5. Έχοντας ξεπεράσει το βήμα (4) επιτυχώς, υπολογίζουμε τον διακριτό λογάριθμο $x = lm + q (\mathrm{mod}\, n)$ για τις τιμές των l, q που εντοπίσαμε στα βήματα 3 και 4.

Παράδειγμα

Θα παρουσιάσουμε τώρα μια εφαρμογή του αλγορίθμου του Shanks στην περίπτωση όπου οι υπολογισμοί γίνονται mod p, όπου p είναι πρώτος αριθμός.

Επιθυμούμε να υπολογίσουμε τον διακριτό λογάριθμο x του 525 με βάση 3, ως προς τον πρώτο αριθμό $p = 809$. Άρα θέλουμε να επιλύσουμε το DLP

$$3^x = 525 \pmod{809}.$$

Αρχικά, έχουμε ότι $n = \left\lceil \sqrt{809-1} \right\rceil = 29$. Στην συνέχεια, υπολογίζουμε όλα τα ζεύγη $(l, 3^l (mod\ 809))$, για $0 \le l < 29$.

Έτσι λαμβάνουμε:

(0,1)	(1,99)	(2,93)	(3,308)	(4,559)
(5,329)	(6,211)	(7,664)	(8,207)	(9,268)
(10,644)	(11,654)	(12,26)	(13,147)	(14,800)
(15,727)	(16,781)	(17,464)	(18,632)	(19,275)
(20,528)	(21,496)	(22,564)	(23,15)	(24,676)
(25,586)	(26,575)	(27,295)	(28,81)	

Ταξινομώντας τα ζεύγη που προέκυψαν, ως προς την δεύτερη συνιστώσα, λαμβάνουμε την αύξουσα ακολουθία S_1.

Όμοια, προχωρούμε στον υπολογισμό των ζευγών $\left(q,\ 525 \cdot 3^{-q} (mod\ 809)\right)$, για $0 \le q < 29$. Επομένως, έχουμε

(0,525)	(1,175)	(2,328)	(3,379)	(4,396)
(5,132)	(6,44)	(7,554)	(8,724)	(9,511)
(10,440)	(11,686)	(12,768)	(13,256)	(14,355)
(15,388)	(16,399)	(17,133)	(18,314)	(19,644)
(20,754)	(21,521)	(22,713)	(23,777)	(24,259)
(25,356)	(26,658)	(27,489)	(28,163)	

Ταξινομώντας τα ζεύγη αυτά ως προς την δεύτερη συνιστώσα, προκύπτει η αύξουσα ακολουθία S_2.

Τώρα, όπως υπαγορεύει το Βήμα 6 του αλγορίθμου, αναζητούμε δύο ζεύγη (l, ω) και (q, ω), τέτοια ώστε $\omega \in S_1$ και $\omega \in S_2$.

Όμως, παρατηρούμε ότι

$$(10, 644) \in S_1 \text{ και } (19, 644) \in S_2 .$$

Συνεπώς, μπορούμε τώρα να υπολογίσουμε

$$x = log_3 525 = (29 \cdot 10 + 19)\ (mod\ 808)$$
$$= 309 (\text{mod}\, 808) .$$

Παρατήρηση

Όταν βρούμε το πρώτο ταίριασμα δεν χρειάζεται να συνεχιστεί η κατασκευή της ακολουθίας S_2.

Ο Αλγόριθμος των Pohlig - Hellman

Ο Αλγόριθμος αυτός έχει σκοπό τον υπολογισμό του διακριτού λογαρίθμου $x = \log_a \beta$, ως προς έναν πρώτο αριθμό *p*.

Η αποδοτικότητά του είναι ικανοποιητική μόνο όταν οι πρώτοι παράγοντες του ακέραιου αριθμού $p-1$ είναι σχετικά μικροί.

Υποθέτουμε, λοιπόν, πως έχουμε επιλέξει έναν κατάλληλο πρώτο αριθμό *p*.

Έστω

$$p-1 = q_1^{r_1} q_2^{r_2} \ldots q_k^{r_k}$$

η αναπαράσταση του $p-1$ σε κανονική μορφή.

Λόγω του γεγονότος ότι $\left(q_i^{r_i}, q_j^{r_j}\right) = 1$, για $i \neq j$ και $i, j = 1,2,\ldots,k$ μπορούμε να υπολογίσουμε τον διακριτό λογάριθμο $\log_\alpha \beta$ ως προς $q_i^{r_i}$ για κάθε $i = 1,2,\ldots k$ και στην συνέχεια να συνθέσουμε την λύση $\bmod(p-1)$ αξιοποιώντας το Κινέζικο Θεώρημα Υπολοίπων.

Ο αλγόριθμος Pohlig – Hellman αφορά την εύρεση του x ως προς την μέγιστη δύναμη *r* ενός τυχαίου πρώτου παράγοντα *q,* του ακεραίου $p-1$, όπου $\alpha^x \equiv \beta (\bmod q^r)$.

Η διαδικασία είναι η ακόλουθη:

Αρχικά, αναπαριστούμε τον x ως προς την βάση q.

Έτσι, έχουμε

$$x = x_0 + x_1 q + x_2 q^2 + \ldots + x_{r-1} q^{r-1}, \text{ με } 0 \le x_i \le q-1, \tag{1}$$

$i = 0,1,\ldots,r-1$.

Ο σκοπός μας, προφανώς, είναι να υπολογίσουμε τους συντελεστές $x_0, x_1, \ldots, x_{r-1}$.

Από την σχέση (1) λαμβάνουμε

$$\frac{x}{q} = \frac{x_0}{q} + x_1 + x_2 q + \ldots + x_{r-1} q^{r-2}$$

$$\Leftrightarrow \frac{x(p-1)}{q} = \frac{x_0 (p-1)}{q} + (p-1)\left(x_1 + x_2 q + \ldots + x_{r-1} q^{r-2}\right)$$

$$= \frac{x_0 (p-1)}{q} + (p-1)m,$$

για κάποιον $m \in \mathbb{N}$.

Επομένως, από την παραπάνω σχέση και από την ισοδυναμία

$$a^x \equiv \beta (\bmod p)$$

προκύπτει

$$\begin{aligned} \beta^{\frac{p-1}{q}} &\equiv a^{x\frac{p-1}{q}} (\bmod p) \\ &\equiv a^{x_0 (p-1)/q} a^{(p-1)m} (\bmod p) \\ &\equiv a^{x_0 (p-1)/q} (\bmod p), \end{aligned} \tag{2}$$

αφού από το μικρό θεώρημα του Fermat γνωρίζουμε ότι $a^{p-1} \equiv 1 (\text{mod } p)$. Σε αυτό το σημείο, πρέπει να παρατηρήσουμε πως όλες οι πράξεις εκθετών που θα κάνουμε από εδώ και στο εξής θα γίνονται $(\text{mod } p-1)$, διότι κάθε όρος της μορφής $a^{k(p-1)}$ αναιρείται λόγω του συμπεράσματος του μικρού θεωρήματος του Fermat.

Από την σχέση (2) προκύπτει ότι, για να βρούμε τον συντελεστή x_0 αρκεί να υπολογίσουμε τις δυνάμεις

$$a^{n(p-1)/q} (mod\ p), \quad \text{για } n = 0,1,..., q-1$$

μέχρι να βρούμε τον κατάλληλο *n* για τον οποίο

$$a^{n(p-1)/q} \equiv \beta^{(p-1)/q} (\text{mod } p) .$$

Η τιμή αυτή του *n* αποτελεί και τον επιθυμητό συντελεστή x_0.

Προκειμένου να υπολογίσουμε τον συντελεστή x_1 γράφουμε:

$$\begin{aligned} \beta &\equiv a^x (\text{mod } p) \\ &\equiv a^{x_0} a^{q(x_1 + x_2 q + ... + x_{r-1} q^{r-2})} (\text{mod } p) \end{aligned}$$

Δηλαδή

$$c_1 \equiv a^{q(x_1 + x_2 q + ... + x_{r-1} q^{r-2})} (\text{mod } p) \text{, όπου } c_1 = \beta a^{-x_0}$$

Υψώνουμε και τα δύο μέλη της παραπάνω ισοδυναμίας στην δύναμη $(p-1)/q^2$.

Τότε

$$\begin{aligned} c_1^{(p-1)/q^2} &\equiv a^{\frac{(p-1)}{q} \cdot (x_1 + x_2 q + ... + x_{r-1} q^{r-2})} \\ &\equiv a^{x_1 (p-1)/q} \cdot a^{(p-1)(x_2 + ... + x_{r-1} q^{r-3})} \\ &\equiv a^{x_1 (p-1)/q} (\text{mod } p) . \end{aligned}$$

Οπότε, όπως εργαστήκαμε και για τον προσδιορισμό του x_0, θα υπολογίσουμε τις δυνάμεις

$$a^{n(p-1)/q} (mod\ q) \text{, για } n = 0, 1, ..., q-1$$

μέχρι να βρούμε το κατάλληλο *n* για το οποίο ισχύει

$$a^{n(p-1)/q} \equiv c_1^{(p-1)/q} (\text{mod } p) \ .$$

Η τιμή του *n* που θα εντοπίσουμε αποτελεί τον επιθυμητό συντελεστή x_1.

Θέτουμε, τώρα, $c_2 = c_1 a^{-x_1 q}$ και εργαζόμαστε όμοια, υψώνοντας στην δύναμη $(p-1)/q^3$. Έτσι, βρίσκουμε τον συντελεστή x_3.

Για να προσδιορίσουμε τον τυχαίο συντελεστή x_k εκτελούμε την ίδια διαδικασία θέτοντας

$$c_k = c_{k-1} a^{-x_{k-1} q^{k-1}}$$

και υψώνοντας στην δύναμη $(p-1)/q^{k+1}$, όπου $0 \le k \le r-1$.

Η παραπάνω διαδικασία θα γίνει πιο κατανοητή με μια αριθμητική εφαρμογή.

Εφαρμογή

Έστω ο πρώτος αριθμός $p = 8101$, ο γεννήτορας $\alpha = 6$ και $\beta = 7531$.

Η εύρεση του διακριτού λογαρίθμου $x = \log_a \beta$ αξιοποιώντας τον αλγόριθμο Pohlig – Hellman γίνεται ως εξής:

$$p - 1 = 8100 = 2^2 \cdot 3^4 \cdot 5^2 \ .$$

Αρχικά, θα εφαρμόσουμε την μέθοδο ώστε να υπολογίσουμε τους ακεραίους b_1, b_2, b_3 για τους οποίους ισχύει ότι

$$b_1 \equiv x(\mathrm{mod}\, 2^2)$$

$$b_2 \equiv x(\mathrm{mod}\, 3^4)$$

$$b_3 \equiv x(\mathrm{mod}\, 5^2) \ .$$

Εύρεση του b_1

Αναπαριστούμε τον b_1 με βάση το 2. Άρα, έχουμε

$$b_1 = x_0 + x_1 \cdot 2 \text{, με } x_0, x_1 = 0 \text{ ή } 1.$$

Ισχύει ότι

$$7531^{(p-1)/2} \equiv 7531^{4050} \equiv (-1)\ (mod\ p) .$$

Όμως

$$a^{(p-1)/2} \equiv 6^{4050} \equiv (-1)\ (\mathrm{mod}\ p) .$$

Άρα, $x_0 = 1$.

Θέτουμε, τώρα, $c_1 = 7531 a^{-x_0} = 7531 \cdot 6^{-1} \equiv 8006(\mathrm{mod}\ p)$.

Όμως

$$8006^{(p-1)/2^2} \equiv 8006^{2025} \equiv 1(\mathrm{mod}\ p) .$$

Έτσι, είναι προφανές ότι $x_1 = 0$. Επομένως $b_1 = 1$.

Εύρεση b_2

Όμοια, έχουμε

$$b_2 = x_0 + x_1 \cdot 3 + x_2 \cdot 3^2 + x_3 \cdot 3^3, \text{ με } x_0, x_1, x_2, x_3 = 0 \text{ ή } 1 \text{ ή } 2 .$$

Έτσι, λαμβάνουμε

$$7531^{(p-1)/3} \equiv 2217(\mathrm{mod}\ p) .$$

Αλλά

$$a^{2(p-1)/3} \equiv 2217(mod\ p) \ .$$

Άρα $x_0 = 2$.

Θέτουμε $c_1 = 7531 a^{-x_0} = 7531 \cdot 6^{-2} \equiv 6735(\mathrm{mod}\ p)$.

Όμως

$$6735^{(p-1)/3^2} \equiv 1(\mathrm{mod}\ p) \ .$$

Επομένως είναι $x_1 = 0$.

Θέτουμε $c_2 = 6735 \cdot a^{-3x_1} = 6735 \equiv 6735 (\mathrm{mod}\ p)$.
Όμως

$$6735^{(p-1)/3^3} \equiv 2217 (\mathrm{mod}\ p)$$

Αλλά

$$a^{2(p-1)/3} \equiv 2217 (\mathrm{mod}\ p).$$

Άρα $x_2 = 2$.

Θέτουμε, τώρα, $c_3 = 6735 a^{-3^2 x_2} = 6735 a^{-18} \equiv 6992 (\mathrm{mod}\ p)$.
Όμως

$$6992^{(p-1)/3^4} \equiv 5883 (\mathrm{mod}\ p).$$

Αλλά

$$a^{(p-1)/3} \equiv 5883 (mod\ p).$$

Άρα $x_3 = 1$.
Επομένως

$$b_2 = 2 + 0 \cdot 3 + 2 \cdot 3^2 + 1 \cdot 3^3 = 47.$$

Εύρεση b_3
Εδώ έχουμε

$$b_3 = x_0 + x_1 \cdot 5 \text{, με } x_0, x_1 = 0,1,2,3,4.$$

Ισχύει ότι

$$7531^{(p-1)/5} \equiv 5221 (\mathrm{mod}\ p)\ .$$

Όμως

$$a^{4(p-1)/5} \equiv 5221 (mod\ p)\ .$$

Άρα $x_0 = 4$.
Θέτουμε

$$c_1 = 7531 a^{-x_0} \equiv 7613 (\mathrm{mod}\ p).$$

Όμως

$$7613^{(p-1)/5^2} \equiv 356 (\mathrm{mod}\ p).$$

Αλλά

$$a^{2(p-1)/5} \equiv 356 (\mathrm{mod}\ p).$$

Άρα $x_1 = 2$.
Επομένως

$$b_3 = 4 + 2 \cdot 5 = 14.$$

Έχοντας υπολογίσει τους ακεραίους b_1, b_2, b_3 προκύπτει

$$x \equiv 1 (\mathrm{mod}\ 4) \quad (1)$$

$$x \equiv 47 (\mathrm{mod}\ 81) \quad (2)$$

$$x \equiv 14 (\mathrm{mod}\ 25) \quad (3)$$

Από το Κινέζικο Θεώρημα Υπολοίπων, γνωρίζουμε ότι το παραπάνω σύστημα ισοδυναμιών έχει μοναδική λύση modulo $(4 \cdot 81 \cdot 25)$.

Η λύση αυτή x προσδιορίζεται από τον παρακάτω τύπο:

$$x = x_1 r_1 r_1' + x_2 r_2 r_2' + x_3 r_3 r_3', \tag{4}$$

όπου x_i είναι λύση της ισοδυναμίας (i) για i=1, 2, 3:

$$r_1 = \frac{4 \cdot 81 \cdot 25}{4} = 2025, \quad r_2 = \frac{4 \cdot 81 \cdot 25}{81} = 100, \quad r_3 = \frac{4 \cdot 81 \cdot 25}{25} = 324$$

και

$$r_1 r_1' \equiv 1 (\mathrm{mod}\, 4)$$
$$r_2 r_2' \equiv 1 (\mathrm{mod}\, 81)$$
$$r_3 r_3' \equiv 1 (\mathrm{mod}\, 25)$$

Εύκολα προκύπτει ότι $x_1 = 1$, $x_2 = 47$, $x_3 = 14$, $r_1' = 1$, $r_2' = 64$, $r_3' = 24$.

Συνεπώς, αντικαθιστώντας στον τύπο (4) λαμβάνουμε ότι

$$x \equiv 6689 \,(mod\ 8100)$$

Αυτός είναι ο διακριτός λογάριθμος $\log_6 7531 (\mathrm{mod}\ 8101)$.

Αλγόριθμος Index Calculus

Ο αλγόριθμος αυτός έχει ως σκοπό τον υπολογισμό του διακριτού λογαρίθμου $x = \log_a \beta$, ως προς έναν πρώτο p, όταν ο α αποτελεί πρωταρχική ρίζα $\mathrm{mod}\ p$.

Πριν παρουσιάσουμε την διαδικασία του αλγορίθμου, θα παραθέσουμε μια ιδιότητα κεντρικής σημασίας για την διεξαγωγή του.

Έστω

$$a^x \equiv \beta (\mathrm{mod}\ p).$$

Αν συμβολίσουμε $x = \log_a \beta$, τότε είναι

$$a^{\log_a \beta} \equiv \beta (mod\ p)$$

Όμως, αν θέσουμε όπου β το γινόμενο $\beta_1 \beta_2$, όπου β_1 και β_2 ακέραιοι για τους οποίους ισχύει ότι

$$a^{\log_a \beta_1} \equiv \beta_1 (mod\ p)$$

και

$$a^{\log_a \beta_2} \equiv \beta_2 (mod\ p)$$

λαμβάνουμε ότι

$$\begin{aligned} a^{\log_a (\beta_1 \beta_2)} &\equiv \beta_1 \beta_2 (mod\ p) \\ &\equiv a^{\log_a \beta_1} a^{\log_a \beta_2} (mod\ p) \\ &\equiv a^{\log_a \beta_1 + \log_a \beta_2} (mod\ p)\ . \end{aligned}$$

Επομένως

$$log_a (\beta_1 \beta_2) \equiv log_a\, \beta_1 + log_a\, \beta_2\ (mod\ p-1). \tag{1}$$

Δηλαδή, ο διακριτός λογάριθμος γινομένου διασπάται σε άθροισμα διακριτών λογαρίθμων, όπως ακριβώς συμβαίνει και με τους κλασσικούς λογαρίθμους που γνωρίζουμε από την ΄Αλγεβρα.

Ακολουθεί, η διαδικασία του αλγορίθμου Index Calculus.

Αρχικά, επιλέγουμε έναν σχετικά μικρό ακέραιο και στην συνέχεια θεωρούμε το σύνολο των πρώτων αριθμών $p_1, p_2, ..., p_k$ που είναι μικρότεροί του. Το σύνολο $B = \{p_1, p_2, ..., p_k\}$ ονομάζεται **βάση παραγόντων** (factor base). Στην συνέχεια, για διάφορες τιμές ενός ακεραίου *m*, υπολογίζουμε το $a^m \pmod p$ προσπαθώντας να εντοπίσουμε εκείνες τις τιμές *m* για τις οποίες, όλοι οι πρώτοι παράγοντες του $a^m \pmod p$ ανήκουν στην βάση παραγόντων *B*.

Έστω m_0 μια τέτοια επιθυμητή τιμή. Τότε

$$a^{m_0} \equiv p_1^{e_1} p_2^{e_2} ... p_k^{e_k} (mod\ p), \text{ για } e_i \in \mathbb{N} \cup \{0\}.$$

Συνεπώς, σύμφωνα με την ιδιότητα (1) προκύπτει

$$m_0 \equiv e_1 log_a\ p_1 + ... + e_k log_a\ p_k (mod\ p-1). \quad (2)$$

Ο σκοπός μας είναι να εντοπίσουμε αρκετές τέτοιες τιμές του ακεραίου *m,* ώστε να μπορούμε να σχηματίσουμε επαρκείς στο πλήθος σχέσεις της μορφής (2) προκειμένου να υπολογίσουμε τις τιμές των $\log_a p_i$, για κάθε $i = 1,2,...,k$, μέσω γραμμικού συστήματος.

Ακολούθως, επιχειρούμε να εντοπίσουμε κάποιον ακέραιο *n,* για τον οποίο οι πρώτοι παράγοντες του

$$a^n \beta \pmod p$$

να ανήκουν στο σύνολο *B*.

Έτσι, όπως και πριν, αν υπολογίσουμε μια τέτοια τιμή του *n,* θα ισχύει

$$a^n \beta \equiv p_1^{\lambda_1} p_2^{\lambda_2} ... p_k^{\lambda_k} \pmod p \quad \text{για } \lambda_i \in \mathbb{N} \cup \{0\}.$$

Δηλαδή

$$n + \log_a \beta \equiv \lambda_1 \log_a p_1 + ... + \lambda_k \log_a p_k \pmod{p-1}$$

$$\Leftrightarrow \log_a \beta \equiv -n + \lambda_1 \log_a p_1 + ... + \lambda_k \log_a p_k \pmod{p-1}. \quad (3)$$

Συνεπώς, από την παραπάνω σχέση, υπολογίζουμε τον διακριτό λογάριθμο του $\beta \pmod p$.

Η αποδοτικότητα του αλγορίθμου αυτού, εξαρτάται άμεσα από την επιλογή της βάσης παραγόντων *B*. Αν το σύνολο αυτό περιλαμβάνει πολλούς πρώτους αριθμούς, τότε η εύρεση των κατάλληλων σχέσεων της μορφής (2), θα είναι εύκολη αλλά η διαδικασία επίλυσης του συστήματος που προκύπτει θα είναι πολύ δύσκολη. Αντιστρόφως, αν το σύνολο *B* περιλαμβάνει πολύ λίγους πρώτους αριθμούς, τότε θα είναι δύσκολο να σχηματίσουμε τις σχέσεις της μορφής (2).

Γενικά, ο προβλεπόμενος χρόνος που απαιτεί ο αλγόριθμος αυτός ώστε να υπολογίσει τον διακριτό λογάριθμο είναι $O(e^{\sqrt{2 ln\, p\, ln ln\, p}})$.

Ο Index Calculus θεωρείται υπο–εκθετικός (subexponetial) και μη–καθολικός (non–generic) αλγόριθμος (δεν εφαρμόζεται σε οποιαδήποτε ομάδα).

Εφαρμογή

Επιθυμούμε να υπολογίσουμε τον διακριτό λογάριθμο $\log_3 37$, ως προς τον πρώτο αριθμό p= 1217, αξιοποιώντας τον αλγόριθμο Index Calculus.

Επιλέγουμε, αρχικά, την βάση παραγόντων $B=\{2,3,5,7,11,13\}$ και επιχειρούμε να εντοπίσουμε κατάλληλους εκθέτες *m*.

Παρατηρούμε ότι

$$\left.\begin{aligned} 3^1 &\equiv 3(\mathrm{mod}1217)\\ 3^{24} &\equiv -2^2\cdot 7\cdot 13\\ 3^{25} &\equiv 5^3\\ 3^{30} &\equiv -2\cdot 5^2\\ 3^{54} &\equiv -5\cdot 11\\ 3^{87} &\equiv 13 \end{aligned}\right\} \qquad (A)$$

Είμαστε σίγουροι πως το γραμμικό σύστημα έχει λύση αφού έχουμε 6+1 εξισώσεις στο σύστημα. Θα μπορούσαμε ίσως να το λύσουμε και με λιγότερες εξισώσεις.

Από τις παραπάνω εξισώσεις, παρατηρούμε πως θα χρειαστούμε στους υπολογισμούς μας την τιμή του $\log_3(-1)$. Όμως,

$$\left(3^{\frac{p-1}{2}}\right)^2 \equiv 1(mod\, p).$$

Άρα

$$3^{\frac{p-1}{2}} \equiv \pm 1(mod\ p).$$

Αλλά, ο $p-1$ είναι ο μικρότερος εκθέτης για τον οποίο ισχύει ότι $3^{(p-1)} \equiv 1(\mathrm{mod}\ p)$.

Επομένως

$$3^{\frac{p-1}{2}} \equiv -1(mod\ p).$$

Δηλαδή

$$\log_3(-1) \equiv \frac{p-1}{2} \equiv 608(\mathrm{mod}1216)$$

Συνεπώς, από τις σχέσεις (Α) προκύπτει

$$\begin{aligned} 1 &\equiv \log_3 3(\mathrm{mod}1216)\\ 24 &\equiv 608+2\log_3 2+\log_3 7+\log_3 13\\ 25 &\equiv 3\log_3 5\\ 30 &\equiv 608+\log_3 2+2\log_3 5\\ 54 &\equiv 608+\log_3 5+\log_3 11\\ 87 &\equiv \log_3 13\,. \end{aligned}$$

Θα εκτελέσουμε τις πράξεις $(\mathrm{mod}1216)$ σταδιακά.

Ισχύει ότι

$$\log_3 3 \equiv 1, \log_3 5 \equiv 819, \log_3 13 \equiv 87$$

Ακολούθως, βρίσκουμε

$$\log_3 2 \equiv 30 - 608 - 2 \cdot 819 \equiv 216$$

$$\log_3 11 \equiv 54 - 608 - 819 \equiv 1059$$

$$\log_3 7 \equiv 24 - 608 - 2 \cdot 216 - 87 \equiv 113$$

Έχοντας υπολογίσει τους διακριτούς λογαρίθμους όλων των στοιχείων της βάσης, αυτό που απομένει είναι να εντοπίσουμε έναν ακέραιο αριθμό n για τον οποίο οι πρώτοι παράγοντες του αριθμού $3^n \cdot 37 (\mathrm{mod} 1217)$ ανήκουν στο σύνολο *B*.

Παρατηρούμε, όμως, ότι

$$3^{16} \cdot 37 \equiv 2^3 \cdot 7 \cdot 11 (\mathrm{mod} 1217) .$$

Επομένως

$$16 log_3 3 + log_3 37 \equiv 3 log_3 2 + log_3 7 + log_3 11 (mod\, 1216),$$

δηλαδή

$$log_3 37 \equiv 3 log_3 2 + log_3 7 + log_3 11 - 16 log_3 3 (mod\, 1216) .$$

Αντικαθιστώντας τις τιμές των λογαρίθμων, που υπολογίσαμε στην παραπάνω σχέση, προκύπτει ότι

$$\log_3 37 \equiv 588 (\mathrm{mod} 1216) .$$

■

Μέθοδοι ρ και λ του Pollard

Σε αυτές τις μεθόδους, εργαζόμαστε ανάλογα με την γενική περίπτωση του αλγορίθμου του Shanks. Δηλαδή, θεωρούμε την πεπερασμένη προσθετική ομάδα *G* τάξης *n* και τα στοιχεία $P, Q \in G$. Θεωρούμε επίσης πως το στοιχείο *P* είναι γεννήτορας της *G* και προσπαθούμε να προσδιορίσουμε έναν κατάλληλο φυσικό αριθμό ω για τον οποίο ισχύει ότι $Q = \omega P$.

Ένα από τα βασικότερα μειονεκτήματα του αλγορίθμου του Shanks είναι πως δεσμεύει μεγάλο τμήμα μνήμης ενός υπολογιστή προκειμένου να αποθηκεύει τα απαραίτητα στοιχεία για την διεξαγωγή του. Αντιθέτως οι μέθοδοι που ανέπτυξε ο J. Pollard στην εργασία του:
Monte Carlo methods for index computation (modp), Mathematics of Computation, 32(143) (1978), 918 – 924, ξεπερνά αυτό το πρόβλημα. Όμως, με τις μεθόδους αυτές δεν είναι μαθηματικώς βέβαιο πως θα δοθεί απάντηση στο πρόβλημα του διακριτού λογαρίθμου σε συγκεκριμένο χρόνο, παρόλο που η πιθανότητα επιτυχίας είναι πολύ μεγάλη. Ως προς αυτό το θέμα, ο αλγόριθμος του Shanks υπερτερεί καθώς είναι ντετερμινιστικός και γνωρίζουμε πως βρίσκει απάντηση σε χρόνο $O(\sqrt{n})$.

Αρχικά, θα παρουσιάσουμε την μέθοδο ρ και στην συνέχεια θα περιγράψουμε μια γενίκευσή της που αποτελεί την μέθοδο λ.

Θεωρούμε μια συνάρτηση $f : G \to G$, η οποία παρουσιάζει σχετικά τυχαία συμπεριφορά (στην συνέχεια θα παραθέσουμε ένα παράδειγμα τέτοιας συνάρτησης) και θέτουμε $P_{k+1} = f(P_k)$, όπου P_0 ένα τυχαίο αρχικό στοιχείο της *G*.

Λόγω του γεγονότος ότι η ομάδα *G* είναι πεπερασμένη και κυκλική, είναι βέβαιο πως μπορούμε να εντοπίσουμε δύο στοιχεία P_{k_0}, P_{m_0} για τα οποία να ισχύει $P_{k_0} = P_{m_0}$. Όμως, τότε προκύπτει

ότι

$$f(P_{k_0}) = f(P_{m_0}).$$

Δηλαδή

$$P_{k_0+1} = P_{m_0+1}\ .$$

Ακολουθώντας την ίδια διαδικασία λαμβάνουμε ότι

$$P_{k_0+T} = P_{m_0+T}\text{, για κάθε } T \in \mathbb{N} \cup \{0\}.$$

Η παραπάνω σχέση υποδηλώνει πως η ακολουθία των στοιχείων P_k είναι περιοδική, με περίοδο έναν διαιρέτη του ακεραίου $k_0 - m_0$. Η ιδιότητα της περιοδικότητας είναι το χαρακτηριστικό που ξεπερνά το πρόβλημα της μεγάλης δέσμευσης μνήμης.

Υπάρχουν διάφοροι τρόποι να εκμεταλλευτούμε την ιδιότητα αυτή, προκειμένου να εντοπίσουμε ένα ζεύγος P_{k_0}, P_{m_0} για το οποίο $P_{k_0} = P_{m_0}$. Τα ζεύγη αυτά θα τα ονομάζουμε ταιριαστά ζεύγη (matches). Ένας από τους τρόπους αυτούς περιγράφεται παρακάτω.

Επιλέγουμε και αποθηκεύουμε ένα από κάθε 2^{ω} στοιχεία. Συλλέγουμε όλα τα στοιχεία που επιλέξαμε και επιχειρούμε να βρούμε ταιριαστά ζεύγη μεταξύ τους.

Απομένει, να σχηματίσουμε μια συνάρτηση f με σχετικά τυχαία συμπεριφορά. Μια τέτοια συνάρτηση περιγράφεται παρακάτω.

Διαμερίζουμε την ομάδα G σε ξένα μεταξύ τους υποσύνολα $C_1, C_2, ..., C_r$ τέτοια ώστε να έχουν περίπου το ίδιο πλήθος στοιχείων (ακριβώς ίδιο αν είναι εφικτό) και άρα να ισχύει $G = \bigcup_{i=1}^{r} C_i$. Ακολούθως, επιλέγουμε r το πλήθος τυχαία ζεύγη $(s_i, t_i)\ mod\ n$.

Θεωρούμε την συνάρτηση

$$f(a) = a + R_i\text{, για } a \in C_i\text{,}$$

όπου

$$R_i = s_i P + t_i Q\ .$$

Η συνάρτηση αυτή συμπεριφέρεται επαρκώς τυχαία.

Επίσης, όπως ορίσαμε αρχικά, ισχύει ότι $P_{k+1} = f(P_k)$.

Συνεπώς, προκειμένου να αρχίσει ο υπολογισμός των τιμών P_k, αρκεί να θεωρήσουμε ένα αρχικό σημείο P_0. Επιλέγουμε, λοιπόν, δύο τυχαίους ακεραίους s_0, t_0 και θέτουμε

$$P_0 = s_0 P + t_0 Q\ .$$

Τότε, για το τυχαίο στοιχείο P_k ισχύει

$$P_k = v_k P + \xi_k Q$$

και ταυτοχρόνως

$$P_{k+1} = f(P_k) = P_k + R_i$$
$$= (v_k + s_i)P + (\xi_k + t_i)Q\ .$$

Όμως

$$P_{k+1} = v_{k+1} P + \xi_{k+1} Q\ .$$

Άρα

$$v_{k+1} = v_k + s_i \quad \text{και} \quad \xi_{k+1} = \xi_k + t_i$$

Ακολουθώντας αυτή την διαδικασία, θα εντοπίσουμε τελικά ένα ταιριαστό ζεύγος P_{k_0}, P_{m_0}. Επομένως, θα ισχύει ότι

$$v_{k_0} P + \xi_{k_0} Q = v_{m_0} P + \xi_{m_0} Q \ .$$

Συνεπώς

$$\left(v_{k_0} - v_{m_0}\right) P = \left(\xi_{m_0} - \xi_{k_0}\right) Q \ .$$

Τότε, η ισοδυναμία

$$\left(\xi_{m_0} - \xi_{k_0}\right) \omega \equiv \left(v_{k_0} - v_{m_0}\right) (mod\ n) \ ,$$

όπου

$$d = (\xi_{m_0} - \xi_{k_0}, n)$$

λαμβάνει *d* λύσεις ως προς *ω*.

Δοκιμάζοντας όλες τις δυνατές περιπτώσεις βρίσκουμε τελικά έναν φυσικό αριθμό *ω*, τέτοιο ώστε $Q = \omega P$.

Η μέθοδος *λ* του Pollard είναι όμοια με την μέθοδο *ρ,* με την διαφορά ότι χρησιμοποιούμε περισσότερα από ένα τυχαία αρχικά σημεία P_0.

Έστω $P_0^1, P_0^2, ..., P_0^v$ τα σημεία αυτά. Τότε, θέτουμε

$$P_{k+1}^m = f(P_k^m), \text{ για } m = 1, 2, ..., v$$

και εφαρμόζουμε την μέθοδο *ρ* για κάθε μια από τις *v* ακολουθίες.

Πίνακας Συμβόλων

$\mathbb{N}$: Το σύνολο των φυσικών αριθμών 1, 2, 3,4,...,ν,...

$\mathbb{N}_0$: Το σύνολο των φυσικών αριθμών και του μηδενός.

$\mathbb{Z}$: Το σύνολο των ακεραίων αριθμών.

$\mathbb{Z}^+$: Το σύνολο των μη αρνητικών ακεραίων.

$\mathbb{Z}^-$: Το σύνολο των μη θετικών ακεραίων.

$\mathbb{Q}$: Το σύνολο των ρητών αριθμών.

$\mathbb{Q}^+$: Το σύνολο των μη αρνητικών ρητών αριθμών.

$\mathbb{Q}^-$: Το σύνολο των μη θετικών ρητών αριθμών.

$\mathbb{R}$: Το σύνολο των πραγματικών αριθμών.

$\mathbb{R}^+$: Το σύνολο των μη αρνητικών πραγματικών αριθμών.

$\mathbb{R}^-$: Το σύνολο των μη θετικών πραγματικών αριθμών.

$\nu!$ $= 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \nu$, αν ν φυσικός αριθμός, 0! = 1.

$a \in A$: Το a είναι στοιχείο του συνόλου Α.

$a \notin A$: Το a δεν ανήκει στο σύνολο Α.

$A \cup B$: Ένωση των συνόλων Α και Β.

$A \cap B$: Τομή των συνόλων Α και Β.

$A - B$: Διαφορά του συνόλου Β από το σύνολο Α.

$C_A(B)$: Συμπλήρωμα του συνόλου Β ως προς το σύνολο Α.

$A \times B$: Το καρτεσιανό γινόμενο του συνόλου Α με το σύνολο Β.
Το σύνολο όλων των διατεταγμένων ζευγών (α,β) τέτοιων, ώστε $\alpha \in A$ και $\beta \in B$.

A^2 : Το καρτεσιανό γινόμενο του συνόλου Α με το Α (δηλαδή $A^2 = A \times A$).

$\{\}$: Άγγιστρα συνόλου.

$\varnothing$: Το κενό σύνολο.

$\subseteq$: Είναι υποσύνολο του ...

$\not\subseteq$: Δεν είναι υποσύνολο του ...

$\subset$: Είναι γνήσιο υποσύνολο του ...

$\not\subset$: Δεν είναι γνήσιο υποσύνολο του ...

$\supseteq$: Είναι υπερσύνολο του ...

$\not\supseteq$: Δεν είναι υπερσύνολο του ...

$\supset$: Είναι γνήσιο υπερσύνολο του ...

$\not\supset$: Δεν είναι γνήσιο υπερσύνολο του ...

(α, β) : Διατεταγμένο ζεύγος με πρώτο στοιχείο το α και δεύτερο στοιχείο το β.

$|\cdot|$: Απόλυτη τιμή πραγματικού αριθμού.

d : Απόσταση, μετρική.

$\Rightarrow$: Σύμβολο συνεπαγωγής.

$\Leftrightarrow$: Σύμβολο ισοδυναμίας.

$\forall$: Για κάθε.

$\exists$: Υπάρχει ένα τουλάχιστον.

$f : A \to B$: Συνάρτηση f με πεδίο (σύνολο) ορισμού το A (ή υποσύνολο του A) και πεδίο (σύνολο) τιμών το B (ή υποσύνολο του B).

$f(x)$: Συνάρτηση της μεταβλητής x.

$f \equiv g$: Οι συναρτήσεις f και g της μεταβλητής x είναι εκ ταυτότητος ίσες, δηλ. $f(x) = g(x)$ για κάθε x στο κοινό πεδίο ορισμού τους.

$\sim$: Είναι ισοδύναμο του ...

$\simeq$: Είναι κατά προσέγγιση ίσο με ...

$f(A)$ ή $f[A]$: Εικόνα του συνόλου A μέσω της συνάρτησης f.

$f^{-1}(B)$ ή $f^{-1}[B]$: Εικόνα του συνόλου B μέσω της συνάρτησης f^{-1}.

f^{-1} : Αντίστροφη της συνάρτησης f.

$$\sum_{\kappa=1}^{v} \alpha_\kappa = \alpha_1 + \alpha_2 + ... + \alpha_v$$

$$\prod_{\kappa=1}^{v} \alpha_\kappa = \alpha_1 \cdot \alpha_2 \cdot \alpha_3 ... \cdot \alpha_v$$

■ : Τέλος λύσης ή απόδειξης.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. A. Adler and J. E. Coury, *The Theory of Numbers,* Jones and Bartlett Publishers, Boston, London, 1995.
2. M. Aigner and G. M. Ziegler, *Proofs from the BOOK,* Springer – Verlag, New York, 1999.
3. G. L. Alexanderson, L. F. Klosinski and L. C. Larson, *The William Lowell Putnam Mathematical Competition, Problems and Solutions, 1965 - 1984.* The Mathematical Accociation of America, New York, Washington, 1985.
4. T. Andreescu and D. Andrica, *An Introduction to Diophantine Equations,* Gil Publishing House, Romania, 2002.
5. T. Andreescu and D. Andrica, *Number Theory: Structures, Examples, and Problems,* Birkhäuser, Boston, Basel, Berlin, 2009.
6. T. Apostol, *Introduction to Analytic Number Theory,* Springer – Verlag, New York, 1984.
7. E. J. Barbeau, *Power Play,* The Mathematical Association of America, New York, Washington, 1997.
8. Δ. Βάρσος, Δ. Δεριζιώτης, Γ. Εμμανουήλ, Μ. Μαλιάκας, Ο. Ταλέλλη, *Μια Εισαγωγή στην Άλγεβρα,* Εκδόσεις Σοφία, Θεσσαλονίκη, 2005.
9. A. Bremner, R. J. Stroeker and N. Tzanakis, On sums of consecutive squares, J. Number Theory 62(1) (1997), 39 – 70
10. T. T. Bell, *Men of Mathematics, 1986.*
11. B. Bollobas, *The Art of Mathematics – Coffee Time in Memphis,* Cambridge University Press, Cambridge, New York, Melbourne, 2006.
12. D. M. Burton, *Elementary Number Theory,* Allyn and Bacon, Inc., 1980.
13. H. Cohn, *Advanced Number Theory,* Dover Publications, Inc., New York, 1962.
14. R. Crandall and C. Pomerance, *Prime Numbers – A Computational Perspective,* Springer – Verlag, New York, 2005.
15. J. B. Dence and T. P. Dence, *Elements of the Theory of Numbers,* Harcourt Academic Press, London, Boston, New York, 1999.
16. Δ. Δεριζιώτης, *Μια Εισαγωγή στη Θεωρία Αριθμών,* Εκδόσεις Σοφία, Θεσσαλονίκη, 2007.
17. D. Djukic, V. Jankovic, I. Matic and N. Petrovic, *The IMO Compendium.* Springer – Verlag, New York, 2006.
18. P. Erdős and J. Surányi, *Topics in the Theory of Numbers,* Springer – Verlag, New York, 2003.
19. G. Everst and T. Ward, *An Introduction to Number Theory*, Springer – Verlag, New York, 2005.
20. B. Fine and G. Rosenberger, *Number Theory: An Introduction via the Distribution of Primes,* Birkhäuser, Boston, Basel, Berlin, 2007.
21. C. F. Gauss, *Disquisitiones Arithmeticae,* Leipzig, 11801 (English translation: A. F. Clarke, Yale University Press, Yale, New Haven, 1966)
22. A. M. Gleason, R. E. Greenwood and L. M. Kelly, *The William Lowell Putnam Mathematical Competition Problems and Solutions, 1938 - 1964.* The Mathematical Association of America, New York, Washington, 1980.
23. J. R. Goldman, *The Queen of Mathematics, A Historically Motivated Guide to Number Theory,* A. K. Peters, Natick, Massachusetts, 2004.
24. R. K. Guy, *Unsolved Problems in Number Theory,* 2nd edition, Springer – Verlag, New York, Berlin, 1994.
25. G. H. Hardy and E. W. Wright, *An Introduction to the Theory of Numbers,* 5th edition, Clarendon Press, Oxford, 1979.

26. A. Hurwitz, *Μαθήματα Αριθμοθεωρίας,* Έκδοση Γ. Α. Πνευματικού, Αθήνα, 1981.
27. K. S. Kedlaya, B. Poonen and R. Vakil, *The William Lowell Putnam Mathematical Competition, 1985 – 2000.* The Mathematical Accociation of America, New York, Washington, 2002.
28. N. Koblitz, *A Course in Number Theory and Cryptography,* Springer – Verlag, New York, 1994.
29. Χ. Κουκουβίνος και Α. Παπαϊωάννου, *Κρυπτογραφία,* Εκδόσεις Ε.Μ.Π., Αθήνα 2005.
30. M. Křižek, F. Luca and L. Somer, *17 Lectures on Fermat Numbers: From Number Theory to Geometry,* Springer – Verlag, New York, 2001.
31. E. Landau, *Elementary Number Theory,* 2nd edition, Chelsea*, New York, 1966.*
32. L. C. Larson, *Problem - Solving Through Problems, Springer – Verlag, New York, Berlin, 1983.*
33. S. B. Malik, *Basic Number Theory,* Vikas, New Delhi, 1995.
34. C. J. Moreno and S.S.Wagstaff, *Sums of Squares of Integers,* Chapmand & Hall / CRC, London, New York, 2006.
35. M. R. Murty, *Problems in Analytic Number Theory,* Springer – Verlag, New York, 2001.
36. I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers,* John Wiley & Sons, Inc, Toronto, 1991.
37. Oystein Ore, *Number Theory and its History,* Mc Graw – Hill, New York, 1948.
38. Δ. Μ. Πουλάκης, *Θεωρία Αριθμών,* Εκδόσεις Ζήτη, Θεσσαλονίκη, 2001.
39. P. Ribenboim, *The Little Book of Big Primes,* Springer – Verlag, New York, 1991.
40. K. H. Rosen, *Elementary Number Theory and its Applications,* 3rd edition, Addison – Wesley Publishing Company, Reading, Massachusetts, New York, 1993.
41. D. Shanks, *Solved and Unsolved Problems in Number Theory,* AMS Chelsea, Rhode, Island, 2001.
42. W. Sierpinski, *250 Problèmes de Théorie Élémentaire des Nombres,* Panstwoew Wydawnictwo, Warsaw, 1970.
43. J. H. Silverman, *A Friendly Introduction to Number Theory,* 3rd edition, Pearson Prentice Hall, Upper Saddle River, New Jersey, 2006.
44. D. R. Stinson, *Cryptography Theory and Practice,* Chapman & Hall / CRC, London, New York, 2006.
45. D. J. Struik, *A. Concise History of Mathematics,* Dover Publications, Inc., New York, 1987.
46. Π. Γ. Τσαγκάρης, *Θεωρία Αριθμών,* Εκδόσεις Συμμετρία, Αθήνα, 2005.
47. H. N. Wright, *First Course in Theory of Numbers,* John Wiley and Sons, London, 1939.
48. I. M. Vinogradov, *Elements of Number Theory,* Dover Publications, New York, 1954.
49. Ε. Ζάχος, *Εισαγωγή στη Θεωρία Αριθμών και την Κρυπτολογία,* Εκδόσεις Ε.Μ.Π., Αθήνα 2005.
50. Ε. Ζάχος, *Αλγόριθμοι καί Πολυπλοκότητα,* Εκδόσεις Ε.Μ.Π., Αθήνα 2003.