ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Στοιχειώδης απόδειξη του θεωρήματος πρώτων αριθμών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΝΙΚΗΤΑΣ ΓΕΩΡΓΑΚΗΣ

Επιβλέπων:Ι.Σαραντόπουλος
Καθηγητής ΕΜΠ

Αθήνα,Δεκέμβριος 2014

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Στοιχειώδης απόδειξη του θεωρήματος πρώτων αριθμών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΝΙΚΗΤΑΣ ΓΕΩΡΓΑΚΗΣ

Επιβλέπων:Ι.Σαραντόπουλος
Καθηγητής ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την …… 2014

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
……	……	……..
Ιωάννης Σαραντόπουλος	Ιωάννης Σπηλιώτης	Άρης Παγουρτζής
Καθηγητής ΕΜΠ	Αν.Καθηγητής Ε.Μ.Π.	Επ.Καθηγητής Ε.Μ.Π.

Αθήνα, Δεκέμβριος 2014

(Υπογραφή)

.....

Νικήτας Γεωργάκης

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

Ευχαριστίες

Αρχικά θα ήθελα να ευχαριστήσω τον καθηγητή και επιβλέποντα κ. Ιωάννη Σαραντόπουλο, για τις σημαντικές γνώσεις που αποκόμισα τόσο μέσα από τη συνεργασία μας όσο και από την παρακολούθηση των προπτυχιακών του διαλέξεων,καθώς και για την ευκαιρία που μου έδωσε να μελετήσω ένα σημαντικό κομμάτι των μαθηματικών.Επιπρόσθετα οφείλω να ευχαριστήσω τον κ.Ιωάννη Σπηλιώτη Αν.Καθηγητή της ΣΕΜΦΕ και τον κ.Άρη Παγουρτζή Επ.Καθηγητή της ΣΗΜΜΥ που δέχτηκαν να συμμετάσχουν στην τριμελή επιτροπή.Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου για την αμέριστη ηθική και υλική υποστήριξη που μου παρέχει όλα αυτά τα χρόνια.

Περίληψη

Σε αυτή τη διπλωματική εργασία παρουσιάζουμε την στοιχειώδη απόδειξη του Θεωρήματος των Πρώτων Αριθμών. Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή σε βασικές έννοιες της θεωρίας αριθμών όπως ο μέγιστος κοινός διαρέτης,η ανάλυση σε γινόμενο πρώτων καθώς και η απειρία των πρώτων αριθμών.Στο δεύτερο κεφάλαιο μελετώνται κύριες αριθμητικές συναρτήσεις και συνάγονται ορισμένα αποτελέσματα για τις πολλαπλασιαστικές συναρτήσεις.Στο τρίτο κεφάλαιο αποδεικνύονται κάποιες ισοδυναμίες του Θεωρήματος των Πρώτων Αριθμών (κάνοντας χρήση των συναρτήσεων $\theta(x)$ και $\psi(x)$) και τέλος στο τέταρτο κεφάλαιο παρατίθεται η απόδειξη του Θεωρήματος των Πρώτων Αριθμών.Στα παραρτήματα παρατίθενται οι ορισμοί των ασυμτωτικών συμβολισμών του Landau,η θεωρία των γενικευμένων συνελίξεων και κατόπιν αποδεικνύεται ο ασυμτωτικός τύπος του Selberg.

Λέξεις κλειδιά

πρώτοι αριθμοί,θεώρημα πρώτων αριθμών,στοχειώδης απόδειξη θεωρήματος πρώτων αριθμών,$\pi(x)$,$\psi(x)$,$\theta(x)$,γενικευμένες συνελίξεις,ταυτότητα Abel

Abstract

In this diploma thesis we present an elementary proof of the Prime Number Theorem. In the first chapter the basic concepts of the number theory are introduced such as the greatest common divisor, the prime factorization and the infinitude of primes. In the second chapter we have studied the main arithmetic functions and we have derived some results for the multiplicative functions. In the third chapter we prove some equivalences of the Prime Number Theorem (by using the functions $\theta(x)$ and $\psi(x)$) and finally in the fourth chapter we give a proof of the Prime Number Theorem. In the appendices we give the definitions of Landau's asymptotic notations, the generalized convolution theory and as an application we give a proof of Selberg's asymptotic formula.

Key words

prime numbers,prime number theorem,elementary proof of the prime number theorem, $\pi(x)$,$\psi(x)$,$\theta(x)$,generalized convolutions,Abel's identity

Πρόλογος

Η παρούσα διπλωματική εργασία έχει ως αντικείμενο την αναλυτική θεωρία αριθμών και συγκεκριμένα την στοιχειώδη απόδειξη του θεωρήματος των πρώτων αριθμών,η οποία δόθηκε το 1949 από τους Atle Selberg και Paul Erdos κάνοντας χρήση στοιχειώδους απειροστικού λογισμού.Το ερέθισμα για να διατυπωθεί και ν' αποδειχτεί το θεώρημα των πρώτων αριθμών δηλ. $\pi(x)\sim x/logx$ ήταν η εικασία των Gauss και Legendre.Αμφότεροι δεν κατάφεραν να δώσουν απάντηση στο ερώτημα και το πρόβλημα της αποφάνσεως για το αληθές ή μη της παραπάνω εικασίας προσέλκυσε εξέχοντες μαθηματικούς για σχεδόν 100 χρόνια,μέχρι το 1851 που ο Ρώσος μαθηματικός Chebyshev έκανε ένα σημαντικό βήμα δείχνοντας πως αν ο παραπάνω λόγος έτεινε σε κάποιο όριο τότε αυτό θα έπρεπε να είναι 1,χωρίς να καταφέρει να το αποδείξει.Το 1859 ο Riemann συνέδεσε την κατανομή των πρώτων με τις ιδιότητες της συνάρτησης ζ(s) χωρίς όμως να καταλήξει στην απόδειξη η οποία δόθηκε το 1896 από τους J.Hadamard και C.J. de la Valle Poussin ανεξάρτητα ο ένας απ' τον άλλο,ανοίγοντας τον δρόμο και για άλλες αποδείξεις όπως π.χ. αυτή του Newman.Η διπλωματική εργασία διαρθρώνεται σε 4 κεφάλαια και 2 παραρτήματα.Στο $1^{ο}$ κεφάλαιο γίνεται μια εισαγωγή σε βασικές έννοιες της θεωρίας αριθμών όπως ο μέγιστος κοινός διαρέτης,η ανάλυση σε γινόμενο πρώτων καθώς και η απειρία των πρώτων αριθμών.Στο $2^{ο}$ κεφάλαιο μελετώνται κύριες αριθμητικές συναρτήσεις και συνάγονται ορισμένα αποτελέσματα για τις πολλαπλασιαστικές συναρτήσεις.Στο κεφάλαιο 3 αποδεικνύονται κάποιες ισοδυναμίες του θεωρήματος των πρώτων αριθμών με εκφράσεις που περιέχουν τις συναρτήσεις ψ(x) και θ(x) και τέλος στο $4^{ο}$ κεφάλαιο παρατίθεται η απόδειξη του θεωρήματος των πρώτων αριθμών.Τέλος αξίζει να αναφερθεί η ύπαρξη διαφορετικών τρόπων προσέγγισης ενός προβλήματος στην θεωρία αριθμών όπως για παράδειγμα η χρήση ανάλυσης ή αλγεβρικών εργαλείων και ότι η στοιχειώδης απόδειξη ανεμενόταν ως η πιο «φυσική».

ΠΕΡΙΕΧΟΜΕΝΑ

1 Εισαγωγή

1.1 Το σύνολο των ακεραίων αριθμών

Η στοιχειώδης θεωρία αριθμών ασχολείται με την μελέτη των ιδιοτήτων του συνόλου $\boldsymbol{N}=\{1,2,3\ldots.\}$ των φυσικών αριθμών.Η αυστηρή θεμελίωση του συνόλου αυτού γίνεται μέσω των αξιωμάτων του Peano όπου η πρόσθεση και ο πολλαπλασιασμός ορίζονται με τέτοιο τρόπο ώστε να ικανοποιούνται η αντιμεταθετικότητα,η προσεταιριστικότητα,η επιμεριστικότητα και η αρχή της μαθηματικής επαγωγής.Θα χρειαστεί να βλέπουμε το $\boldsymbol{N}$ σαν υποσύνολο του συνόλου $\boldsymbol{Z=N\cup\{0\}\cup\{-N\}=\{0,1,2,...\}}$ ή ακόμα και του συνόλου $\boldsymbol{Q=\{p/q,\ \forall\ p\in Z,\ \forall q\in Z^{*}\}}$.Σε αυτή την παράγραφο θα αναφερθούμε σε μερικές βασικές αρχές.

Θεώρημα 1.1.1(Αρχή του ελαχίστου):Κάθε μη κενό σύνολο S μη αρνητικών ακεραίων έχει ελάχιστο στοιχείο,δηλαδή υπάρχει $\alpha\in S$ με την ιδιότητα $\alpha\leq b$ για κάθε $b\in S$.

Παρατήρηση:Η αρχή του ελαχίστου έχει ως συνέπεια την εξής πρόταση:Δεν υπάρχει γνησίως φθίνουσα ακολουθία μη αρνητικών ακεραίων.
Πράγματι ας υποθέσουμε ότι υπάρχει μια ακολουθία $n_1>n_2\ldots>n_k$ στο $\boldsymbol{Z}^{+}$.Από την αρχή του ελαχίστου,το σύνολο $S=\{n_k:k\in\boldsymbol{N}\}$ έχει ελάχιστο στοιχείο n_m για κάποιο $m\in\boldsymbol{N}$.Ομως, $n_{m+1}<n_m$ το οποίο είναι άτοπο.
Η αρχή του ελαχίστου διαδραματίζει σημαντικό ρόλο γι' αυτό δίνουμε κάποια παραδείγματα εφαρμογής της.

Θεώρημα 1.1.2(Αρχιμήδεια ιδιότητα):Αν α,b είναι δύο φυσικοί αριθμοί,υπάρχει φυσικός n τέτοιος ώστε $n>\alpha b$.
Απόδειξη:Αν υποθέσουμε ότι το θεώρημα δεν ισχύει,υπάρχουν $\alpha,b\in\boldsymbol{N}$ τέτοιοι ώστε $n\alpha<b$ για κάθε n.Αυτό σημαίνει ότι το σύνολο $S=\{b-n\alpha|n\in\boldsymbol{N}\}$ αποτελείται απο θετικούς ακεραίους και σύμφωνα με την αρχή του ελαχίστου,το S έχει ελάχιστο στοιχείο που γράφεται στη μορφή b-mα για κάποιον φυσικό m.Παρατηρούμε ότι ο $b-(m+1)\alpha\in S$ και $b-(m+1)\alpha=b-m\alpha-\alpha<b-m\alpha$,το οποίο είναι άτοπο.#

Θεώρημα 1.1.3(Αρχή της μαθηματικής επαγωγής):Έστω S ένα σύνολο θετικών ακεραίων με τις εξής ιδιότητες:
1.Ο 1 ανήκει στο S.
2.Αν $\kappa\in S$ τότε $\kappa+1\in S$.
Τότε το S είναι το σύνολο των φυσικών αριθμών.

Απόδειξη:Θέτουμε $T=\boldsymbol{N}\backslash S$ και υποθέτουμε ότι το T είναι μη κενό.Από την αρχή του ελαχίστου το T έχει ελάχιστο στοιχείο έστω α.Αφού $1\in S$ αναγκαστικά έχουμε ότι $\alpha>1$ οπότε $\alpha-1\in\boldsymbol{N}$.Αφού ο α ήταν το ελάχιστο στοιχείο του T,έχουμε $\alpha-1\in S$.Από την υπόθεση 2
$\alpha=(\alpha-1)+1\in S$.Καταλήξαμε σε άτοπο και άρα το T είναι το κενό σύνολο,επομένως $S=\boldsymbol{N}$.#

Η αρχή της μαθηματικής επαγωγής μας επιτρέπει να αποδεικνύουμε ότι κάποια πρόταση P(n) που αφορά τους φυσικούς αριθμούς ισχύει για κάθε $n\in\boldsymbol{N}$.Αρκεί να ελέγξουμε ότι η P(1) είναι αλήθης και να αποδείξουμε τη συνεπαγωγή $P(k)\Rightarrow P(k+1)$.(επαγωγικό βήμα)
Στη συνέχεια θα παραθέσουμε χωρίς απόδειξη δύο παραλλαγές του θεωρήματος 1.1.3.

Θεώρημα1.1.4.Εστω $m\in\boldsymbol{Z}$ και S ένα σύνολο ακεραίων με τις εξής ιδιότητες:$m\in S$ και αν $k\in S$ τότε $k+1\in S$.Τότε, $S\supseteq\{n\in\boldsymbol{Z}:\boldsymbol{n\geq m}\}=\{\boldsymbol{m,m+1...}\}$.
Θεώρημα1.1.5.Εστω S ένα σύνολο θετικών ακεραίων με τις εξής ιδιότητες:$1\in S$ και αν $1,.....,k\in S$ τότε $k+1\in S$.Τότε,$S=\boldsymbol{N}$.

1.2 Διαιρετότητα

Έστω $\alpha,\beta\in\boldsymbol{Z}$,λέμε ότι ο α διαιρεί τον β και γράφουμε $\alpha|\beta$,αν υπάρχει $x\in\boldsymbol{Z}$ τέτοιος ώστε $\beta=\alpha x$.Σε αυτήν την περίπτωση θα λέμε ότι ο α είναι διαιρέτης του β ή ότι ο β είναι πολλαπλάσιο του α.Απλές συνέπειες του ορισμού είναι οι εξής:
1.$\alpha|\alpha$ για κάθε $\alpha\in\boldsymbol{Z}$.
2.$\alpha|0$ για κάθε $\alpha\in\boldsymbol{Z}$.
3.$1|\alpha$ για κάθε $\alpha\in\boldsymbol{Z}$.
4.$0|\alpha$ αν και μόνο αν $\alpha=0$.
5.Αν $\alpha|\beta$ και $\beta|\gamma$ τότε $\alpha|\gamma$.
6.Αν $\alpha|\beta$ και $\alpha|\gamma$ τότε $\alpha|\beta x+\gamma\mu$ για κάθε $x,\mu\in\boldsymbol{Z}$.
7.Αν $\alpha,\beta\in\boldsymbol{Z}\backslash\{0\}$ και $\alpha|\beta$ τότε $|\alpha|\leq|\beta|$
8.$\alpha|\pm1$ αν και μόνο αν $\alpha=\pm1$.

Θεώρημα 1.2.1(Ταυτότητα της διαίρεσης):Υποθέτουμε ότι $\alpha\in\boldsymbol{N}$ και $\beta\in\boldsymbol{Z}$.Τότε υπάρχουν μοναδικοί $q,r\in\boldsymbol{Z}$ τέτοιοι ώστε $\beta=\alpha q+r$ με $0\leq r<a$.
Απόδειξη:Αποδεικνύουμε πρώτα την ύπαρξη αριθμών q,r που ικανοποιούν το ζητούμενο.Θεωρούμε το σύνολο $A=\{\beta-\alpha\lambda:\lambda\in\boldsymbol{Z}\}\cap\boldsymbol{Z}^{+}$.Δεν είναι δύσκολο να διαπιστώουμε πως το A είναι μη κενό διότι αν $\beta\geq0$,τότε $(\beta-\alpha)\cdot0\in A$.Αν $\beta<0$,θεωρούμε ακεραίους s της μορφής $-\alpha\cdot n$ όπου $n\in\boldsymbol{N}$.Τότε $\beta-\alpha s=\beta+\alpha^2n$ και από την αρχιμήδεια ιδιότητα υπάρχει $n\in\boldsymbol{N}$ τέτοιος ώστε $\alpha^2n\geq(-\beta)$.Από την αρχή του ελαχίστου το A έχει ελάχιστο στοιχείο το οποίο συμβολίζουμε με r.Από τον ορισμό του A έχουμε $r\geq0$ και υπάρχει $q\in\boldsymbol{Z}$ τέτοιος ώστε

β−αq=r.Απομένει να δείξουμε ότι r<α.Ας υποθέσουμε ότι r≥α,τότε β−α(q+1)=β−αq−α=r−α≥0,δηλαδή β−α(q+1) ∈Α.Όμως β−α(q+1)=r−α<r,το οποίο είναι άτοπο αφού ο r ήταν το ελάχιστο στοιχείο του Α.
Αποδεικνύουμε τώρα τη μοναδικότητα των q,r.Ας υποθέσουμε ότι β=αq+r=αq*+r*,όπου 0≤r,r*<α.Τότε, |r−r*|=α|q−q*|.Αν q≠q*,α|q−q*|≥**α** ενώ |r−r*|<α.Έχουμε αντίφαση,άρα q=q* και από 1.2.3 έπεται ότι r=r*.#

1.3 Μέγιστος κοινός διαιρέτης

Έστω α,β δύο φυσικοί αριθμοί.Οι α,β έχουν τουλάχιστον έναν κοινό διαιρέτη τον 1.Σ' αυτό το κεφάλαιο θα αποδείξουμε πως υπάρχει μέγιστος κοινός διαιρέτης των α,β τον οποίο θα συμβολίσουμε d,όπου ο d είναι φυσικός αριθμός.Η ιδέα πίσω από την απόδειξη που θα δώσουμε είναι να θεωρήσουμε το σύνολο I όλων των θετικών ακεραίων συνδυασμών αu+βv των α,β,όπου u,v∈***Z***.Τέτοιοι θετικοί συνδυασμοί υπάρχουν,για παράδειγμα α=α·1+β·0.Η βασική παρατήρηση είναι ότι κάθε κοινός διαιρέτης των α,β διαιρεί κάθε στοιχείο του I(σύμφωνα με την ιδιότητα 6 της διαιρετότητας),άρα δεν ξεπερνάει το ελάχιστο στοιχείο του I.Αν δείξουμε ότι το ελάχιστο στοιχείο του I είναι κοινός διαρέτης των α,β τότε θα είναι και ο μέγιστος κοινός διαιρέτης τους.

Θεώρημα1.3.1 Έστω α,β∈***N***.Υπάρχει d∈***N*** ο οποίος ικανοποιεί τα εξής:
1.d|α και d|β
2.Αν για κάποιον k∈***N*** έχουμε k|α και k|β,τότε k|d.Ειδικότερα,k≤d.
Επιπλέον, υπάρχουν x,y∈***Z*** τέτοιοι ώστε d=αx+βy.
Απόδειξη:Θεωρούμε το σύνολο,I={αu+βv: u,v ∈***Z***}∩***N***.
Είναι φανερό ότι το I είναι μη κενό(για παράδειγμα τα α,β ανήκουν στο I).Από την αρχή του ελαχίστου,το I έχει ελάχιστο στοιχείο d το οποίο γράφεται στη μορφή d=αx+βy για κάποια x,y∈***Z***.Θα δείξουμε ότι ο d διαιρεί κάθε στοιχείο του I.Ας υποθέσουμε ότι z=dq+r.Παρατηρούμε ότι,
r=z−dq=αu+βv−(αx+βy)q=α(u−xq)+β(v−yq) ∈I.
Αν ήταν 0<r<d τότε ο r θα ήταν στοιχείο του I μικρότερο απο το d,άτοπο από τον τρόπο ορισμού του d.Αρα r=0,το οποίο αποδεικνύει ότι ο d διαιρεί τον z.
Αφού α,β∈I,ο d διαιρεί τους α,β.Αυτός είναι ο πρώτος ισχυρισμός του θεωρήματος.Για τον δεύτερο παρατηρούμε ότι αν κ|α και κ|β τότε κ|αx+βy=d.
Για τη μοναδικότητα του d παρατηρούμε ότι αν οι φυσικοί d_1,d_2 ικανοποιούν τα 1,2 του θεωρήματος τότεd_1 $|d_2$ και $d_2|d_1$,συνεπώς $d_2 \leq d_1, d_1 \leq d_2$ και άρα $d_1=d_2$.#

Ο αριθμός d που ορίζεται από το παραπάνω θεώρημα λέγεται μέγιστος κονός διαιρέτης (μκδ) των α,β και συμβολίζεται ως d=(α,β) ή d=gcd(α,β).Οταν για τους α,β ισχύει (α,β)=1 τότε οι α,β λέγονται σχετικά πρώτοι.
Για την εύρεση του μκδ(μέγιστου κοινού διαιρέτη) ο αλγόριθμος του ευκλείδη που στηρίζεται στην εξής ιδιότητα:αν α>β (α,β)=(β,αmodβ) μας δίνει έναν αποδοτικό αλγόριθμο πολυπλοκότητας O(loga) και ο επεκτεταμένος ευκλείδιος αλγόριθμος μας δίνει την δυνατότητα υπολογισμού των x,y d=αx+βy.
Αλγόριθμος:
function gcd(a,b: integer);
if b = 0 then gcd ← a else gcd ← gcd(b, a mod b).

1.4 Ανάλυση σε γινόμενο πρώτων παραγόντων

Έστω α>1 ένας φυσικός αριθμός,θα λέμε ότι ο α είναι πρώτος αν έχει ακριβώς δύο θετικούς διαιρέτες,το 1 και τον α.Αν ο α δεν είναι πρώτος θα λέγεται σύνθετος.Το 1 δεν κατατάσσεται σε καμία κατηγορία ενώ ο μόνος πρώτος που είναι άρτιος είναι το 2.Στην πορεία με το σύμβολο p θα συμβολίζουμε κάποιον πρώτο αριθμό.Στη συνέχεια παραθέτουμε κάποια στοιχειώδη θεωρήματα.
Θεώρημα 1.4.1 Έστω α,β∈***N*** και p ένας πρώτος.Αν p|αβ τότε είτε p|α ή p|β.
Απόδειξη:Έστω ότι ο p δεν διαιρεί τον α.Αφού οι μόνοι διαιρέτες του p είναι ο 1 και ο p έχουμε ότι (α,p)=1,άρα υπάρχουν κ,λ∈***Z*** τέτοιοι ώστε ακ+λp=1.Αρα, β=αβκ+pβλ και αφού p|αβ έπεται ότι p|β.#
Με επαγωγή παίρνουμε την εξής πρόταση:Έστω $\alpha_1,\alpha_2,.....,\alpha_k$ και $p|\alpha_1....\alpha_k$ τότε $p|\alpha_j$ για κάποιο j∈{1,2,....,k}.
Θεώρημα1.4.2(Το θεμελιώδες θεώρημα της αριθμητικής)Κάθε φυσικός αριθμός n>1 αναπαρίσταται σαν γινόμενο πρώτων αριθμών.Η αναπαράσταση αυτή είναι μοναδική αν αγνοήσουμε τη διάταξη των παραγόντων του γινομένου.
Απόδειξη:Θα χρησιμοποιήσουμε την αρχή της επαγωγής.Για n=2 ισχύει τετριμμένα.Έστω πως ισχύει για κάθε m∈***N*** με 2<m<n.Τώρα θα δείξουμε πως ισχύει για το n.Αν ο n είναι πρώτος ισχύει πάλι τετριμμένα,οπότε υποθέτουμε πως ο n είναι σύνθετος και άρα n=st με 2≤s,t<n και από την επαγωγική υπόθεση οι s,t αναλύονται σε γινόμενο πρώτων αριθμών οπότε το ίδιο ισχύει και για το n.
Δείχνουμε τώρα τη μοναδικότητα.Ας υποθέσουμε ότι $n=p_1....p_r=q_1....q_s$
όπου οι $p_1....p_r$ και $q_1....q_s$ είναι πρώτοι.Αφού $p_1|q_1....q_s$ έχουμε ότι $p_1|q_j$ για κάποιο j≤s.Αφού οι p_1,q_j είναι πρώτοι τότε $p_1=q_j$.Ομοίως $q_1|p_1....p_r$ υπάρχει i≤r τέτοιος ώστε $q_1|p_i$ $q_1=p_i$.Παρατηρούμε ότι, $p_1=q_jq_1=p_ip_1$,
άρα $p_1=q_1$,

οπότε έχουμε $q_2....q_s= p_2....p_r$ και επαναλαμβάνοντας την διαδικασία συμπεραίνουμε ότι r=s και τα p,q ταυτίζονται.#
Αν πάρουμε κατά ομάδες τους ίσους πρώτους που εμφανίζονται στην αναπαράσταση στο προηγούμενο θεώρημα τότε συνάγουμε το εξής:
Θεώρημα1.4.3 Κάθε φυσικός n≥2 αναπαρίσταται μοναδικά στην μορφή,
$n=p_1^{a1}....p_r^{ar}$ όπου $p_1<....<p_r$ πρώτοι και τα $k_i \in \boldsymbol{N}$

1.5 Η απειρία των πρώτων αριθμών και το θεώρημα των πρώτων αριθμών

Η πρώτη σημαντική συνέπεια του θεμελιώδους θεωρήματος της αριθμητικής είναι το θεώρημα του Ευκλείδη για την απειρία των πρώτων αριθμών.

Θεώρημα 1.5.1 Υπάρχουν άπειροι πρώτοι αριθμοί.
Θα δώσουμε 4 διαφορετικές αποδείξεις για το παραπάνω θεώρημα διότι κατ' αρχάς θέλουμε να καταδείξουμε τους διαφορετικούς τρόπους προσέγγισης ενός προβλήματος της θεωρίας αριθμών και κατά δεύτερον οι πιο σύγχρονες αποδείξεις δίνουν περαιτέρω πληροφορίες για την άπειρη ακολουθία των πρώτων.
Η πρώτη απόδειξη που θα δώσουμε είναι αυτή του Ευκλείδη που αποτελεί την παλαιότερη και απλούστερη απόδειξη.
1η Απόδειξη:Ας υποθέσουμε ότι οι πρώτοι αριθμοί έχουν πεπερασμένο πλήθος έστω $p_1<....<p_r$.
Αν θεωρήσουμε τον φυσικό αριθμό:$n=p_1....p_r+1$,τότε ο n>1 και άρα έχει πρώτο διαιρέτη.
Αφού το $\{p_1,....,p_r\}$ είναι το σύνολο όλων των πρώτων θα υπάρχει ένα j≤r τέτοιο ώστε $p_j|n$,δηλ.
$p_j|p_1....p_rp_j|n-p_1....p_rp_j|1$,άτοπο άρα υπάρχουν άπειροι πρώτοι.#

2η Απόδειξη:Για κάθε n=0,1,2... ορίζουμε $F_n=2^{2^n}+1$,αυτοί οι αριθμοί λέγονται αριθμοί Fermat.Αφού $F_n\geq 2$ για κάθε n κάθε F_n έχει τουλάχιστον έναν πρώτο διαιρέτη q_n.Θα δείξουμε οτι $n\neq m \Rightarrow (F_n,F_m)=1$.(σχέση 1)
Οποιοιδήποτε 2 αριθμοί Fermat είναι σχετικά πρώτοι,άρα $n\neq m \Rightarrow q_n\neq q_m$(αν είχαμε $q_n=q_m$ τότε οι $(F_n,F_m)\neq 1$).Έπεται ότι οι $q_n,n\geq 0$,είναι διαφορετικοί πρώτοι,το οποίο δείχνει την απειρία των πρώτων αριθμών.
Για την απόδειξη της σχέσης 1 δείχνουμε πρώτα με επαγωγή το εξής,αν n≥1,τότε $\prod_{j=0}^{n-1} F_j = F_n-2$.
Η παραπάνω σχέση ισχύει αν $n=1,F_0=3=5-2=F_i-2$.Αν δεχτούμε ότι ισχύει για n=k τότε,

$\prod_{j=0}^{k} F_j=(\prod_{j=0}^{k-1} F_j)*F_k=(F_k-2)*F_k=(2^{(2^k)}-1)(2^{(2^k)}+1)=2^{(2^{k+1})}-1=F_{k+1}-2$,
δηλαδή ισχύει για n=k+1.
Έστω τώρα 0≤m<n και έστω d ενας κοινός θετικός διαιρέτης των F_m και F_n.Τότε $d|F_m|\prod_{j=0}^{n-1} F_j=F_n-2$, άρα $d|F_n$ και $d|F_n-2$,οπότε ο d διαιρεί το 2 άρα θα πρέπει να ισούται με 1 ή 2 κι επειδή οι αριθμοί Fermat είναι περιττοί ο d=1 και άρα $(F_n,F_m)=1$.#
Κοιτάζοντας την παραπάνω απόδειξη παρατηρούμε ότι αν $p_1<...<p_n<....$είναι η άπειρη ακολουθία πρώτων αριθμών τότε $p_n\leq F_{n-1}=2^{2^{n-1}}+1$ για κάθε n∈N.Πράγματι οι $F_0,F_1,...F_{n-1}$ έχουν n διακεκριμένους πρώτους διαιρέτες $p_{k_1}\ldots,p_{k_n}$,άρα

$$p_n \leq \max\{p_{k_1},\ldots, p_{k_n}\}\leq \max\{F_o,F_1,...F_{n-1}\}=F_{n-1}.$$

Η παρατήρηση αυτή μας οδηγεί στον ορισμό της π(x)=πλήθος των πρώτων μικρότερων του x.Η π είναι αύξουσα και βέβαια π(x)=0 αν x<2.Παρατηρούμε ότι αν x≥2 και n=n(x) είναι ο μεγαλύτερος μη αρνητικός ακέραιος για τον οποίο $2^{(2^v+1)}\leq x$ τότε $\pi(x)\geq\pi(2^{2n}+1)\geq n+1$.Από την άλλη πλευρά $2^{2n+1}\geq x$ άρα $log_2(log_2 x)\leq n+1$.Έχουμε λοιπόν το εξής κάτω φράγμα για την π(x):
$\pi(x)\geq log_2(log_2 x)$ για κάθε πραγματικό x≥2,ειδικότερα αν $\pi(x)\to+\infty$ καθώς το $x\to+\infty$,άρα υπάρχουν άπειροι πρώτοι.
Αυτό το φράγμα θα βελτιωθεί όταν θα κάνουμε την τρίτη απόδειξη.

3η Απόδειξη:(με π(x) συμβολίζουμε το πλήθος των πρώτων μικρότερων ή ίσων του x):Θεωρούμε την πεπερασμένη ακολουθία των πρώτων αριθμών σε αύξουσα διάταξη $p_1<p_2<....<p_k<....$Αν f(t)=1/t,τότε για κάθε n≥2 και για κάθε $n\leq x<n+1$ έχουμε :

$$ln x=\int_1^x \frac{1}{t}dt \leq \int_1^2 \frac{1}{t}dt + \ldots. + \int_n^{n+1} \frac{1}{t}dt \leq 1+1/2+.....+1/n\leq \sum_{m\in A(x)} 1/m,$$

όπου A(x) είναι το σύνολο όλων των φυσικών αριθμών που όλοι οι πρώτοι διαιρέτες τους είναι μικρότεροι ή ίσοι από x.Το σύνολο A(x) περιγράφεται με τη βοήθεια του θεμελιώδους θεωρήματος της αριθμητικής:
$A(x)=\{n=\prod_{k=1}^{\pi(x)} p_k^{r_k}$,όπου $r_k\geq 0\}$,παρατηρούμε πως ο 1 προκύπτει αν πάρουμε όλους τους εκθέτες ίσους με 0.Χρησιμοποιώντας την επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση ελέγχουμε ότι $\sum_{m\in A(x)} 1/m=\prod_{k=1}^{\pi(x)}(\sum_{s=0}^{\infty}\frac{1}{p_k^s})$.Στην παρένθεση έχουμε μια γεωμετρική σειρά με λόγο $1/p_k$,άρα $\sum_{s=0}^{\infty}\frac{1}{p_k^s}=\frac{1}{1-\frac{1}{p_k}}=\frac{p_k}{p_k-1}$.Έπεται ότι $ln x\leq\prod_{k=1}^{\pi(x)}\frac{p_k}{p_k-1}$ και χρησιμοποιώντας τη σχέση $p_k\geq k+1$ έχουμε ότι $\frac{p_k}{p_k-1}=1+\frac{1}{p_k-1}\leq 1+1/k=\frac{k+1}{k}$.Τελικά προκύπτει ότι $ln x\leq\prod_{k=1}^{\pi(x)}\frac{k+1}{k}=\pi(x)+1$,δηλαδή έχουμε αποδείξει ότι για x≥2 ισχύει ότι $\pi(x)\geq ln x-1$ και παίρνοντας όριο για $x\to\infty$ έχουμε $\pi(x)\to\infty$,άρα έχουμε άπειρους πρώτους.#

Σημείωση:Με [x] συμβολίζουμε το ακέραιο μέρος ενός αριθμού x,για το οποίο προφανώς ισχύει $[x]\leq x$.

4η Απόδειξη:Έστω P={p_1,p_2,p_3....} το σύνολο των πρώτων αριθμών τους οποίους θεωρούμε σε αύξουσα διάταξη.Ας υποθέσουμε ότι η σειρά $\sum_{i\geq 1} 1/p_i$ συγκλίνει.Τότε,υπάρχει φυσικός αριθμός k με ιδιότητα $\sum_{i\geq k} 1/p_i$.Θα λέμε ότι οι p_1,....p_k είναι οι μικροί πρώτοι ενώ οι p_{k+1}... είναι οι μεγάλοι πρώτοι.Για κάθε φυσικό αριθμό N έχουμε $\sum_{i\geq k} N/p_i$<N/2 (1).

Γράφουμε N_b για το πλήθος των φυσικών n≤Nπου έχουν τουλάχιστον έναν μεγάλο πρώτο διαιρέτη και N_a για το πλήθος των φυσικών που όλοι οι πρώτοι διαιρέτες τους είναι μικροί.Από τον ορισμό των N_a,N_b έχουμε ότι N_α+N_b=N.

Παρατηρούμε ότι το πλήθος των φυσικών n≤N που είναι πολλαπλασια κάποιου πρώτου p_i ισούται με [N/p_i].Άρα,χρησιμοποιώντας την (1) παίρνουμε:

$$N_b \leq \sum_{i\geq k}[\frac{N}{p_i}] \leq \sum_{i\geq k} N/p_i < N/2.$$

Ας δούμε τώρα πως μπορεί κανείς να φράξει τον N_a.Κάθε φυσικός n≤N που έχει μόνο μικρούς πρώτους διαιρέτες γράφεται στη μορφή $n=a_n b_n^2$,οπου ο a_n είναι γινόμενο διακεκριμένων πρώτων.Αφού αυτοί οι πρώτοι είναι κάποιοι απ' τους p_1,p_2,...,p_k έχουμε το πολύ 2^k επιλογές για τον a_n.Επιπλέον b_n^2 ≤n≤N,άρα $b_n \leq \sqrt{N}$.Δηλαδή έχουμε το πολύ $\sqrt{N}$ επιλογές για τον b_n.Έπεται ότι,

$N_a \leq 2^k\sqrt{N}$.

Από τις προηγούμενες σχέσεις παίρνουμε $N=N_a+N_b \leq N/2+2^k\sqrt{N} \Rightarrow \sqrt{N} \leq 2^{k+1}$.Αυτό όμως δεν μπορεί να ισχύει για κάθε φυσικό αριθμό N:τότε το N θα ήταν άνω φραγμένο,άτοπο.Άρα η σειρά $\sum_{i\geq 1} 1/p_i$ αποκλίνει και συνεπώς υπάρχουν άπειροι πρώτοι.#

2 Αριθμητικές συναρτήσεις

Εισαγωγή

Μια συνάρτηση ορισμένη πάνω στο σύνολο των θετικών ακεραίων και με τις τιμές τις πραγματικές ή μιγαδικές λέγεται αριθμητική συνάρτηση.Σ΄αυτό το κεφάλαιο θα αναφερθούμε σε αρκετές αριθμητικές συναρτήσεις που παίζουν σημαντικό ρόλο στη μελέτη των ιδιοτήτων διαιρετότητας,καθώς και στην κατανομή των πρώτων αριθμών.Επιπρόσθετα,θα ορίσουμε τον κατά Dirichlet πολλαπλασιασμό,τις πολλαπλασιαστικές και πλήρως πολλαπλασιαστικές συναρτήσεις και τέλος την αντίστροφη μιας πολλαπλασιαστικής συνάρτησης.

2.1 Η συνάρτηση Mobius

Θα ξεκινήσουμε την αναφορά στις αριθμητικές συναρτήσεις με τον ορισμό μιας πολύ βασικής συνάρτησης της συνάρτησης Mobius,που ορίζεται ως εξής:

Ορισμός:

- $\mu(1)=1$

εάν n>1 και $n=p_1^{a1}\cdot \ldots p_k^{ak}$:

- $\mu(n)=(-1)^k$,αν $\alpha_1=\alpha_2=\ldots=1$
- $\mu(n)=0$,σε κάθε άλλη περίπτωση

Θεώρημα 2.1 Αν n>1,τότε ισχύει

$$\sum_{d|n}\mu(d)=\left[\frac{1}{n}\right]=\begin{cases}1, \alpha\nu\ n=1\\ 0, \alpha\nu\ n>1\end{cases}$$

Απόδειξη:Ο τύπος είναι φανερά αληθής για n=1.Ας υποθέσουμε λοιπόν ότι n>1.Έστω $n=p_1^{a1}\cdot \ldots p_k^{ak}$ η ανάλυση του n σε γινόμενο πρώτων παραγόντων.Στο άθροισμα $\sum_{d|n}\mu(d)$ οι

μόνοι μη μηδενκοί όροι προέρχονται από τον d=1 και από εκείνους τους διαιρέτες του n που είναι γινόμενα διαφορετικών πρώτων.Έτσι θα έιναι:

$\sum_{d|n}\mu(d)=\mu(1)+\mu(p_1)+....+\mu(p_1p_2)+....+\mu(p_{k-1}p_k)+....+\mu(p_1p_2...p_k)=1+\binom{k}{1}(-1)+\binom{k}{2}(-1)^2+....+\binom{k}{k}(-1)^k=(1-1)^k=0$#.

2.2 Η συνάρτηση Euler φ(n)

Ορισμός:Αν n≥ 1 τότε η συνάρτηση του Euler φ(n) ορίζεται ως το πλήθος των θετικών ακεραίων που δεν υπερβαίνουν τον n και είναι σχετικά πρώτοι με τον n.Έτσι $\varphi(n)=\sum_{\substack{k=1\\(k,n)=1}}^{n}1$.Όπως στην περίπτωση της μ έτσι και για την φ υπάρχει ένας αντίστοιχος τύπος.

Θεώρημα 2.2 Αν n>1 τότε ισχύει

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

Απόδειξη:Έστω ότι S συμβολίζουμε το σύνολο {1,2,....,n}.Κατανέμουμε τα στοιχεία του S σε ξένα σύνολα ως εξής,για κάθε διαρέτη d του n,έστω

$A(d)=\{k:(k,n)=d,1\leq k\leq n\}$

Έτσι το A(d) αποτελείται από εκείνα τα στοιχεία του S που έχουν με τον n σαν μκδ τον d.Τα σύνολα A(d) είναι ανά δύο ξένα ενώ η ένωσή τους είναι το S.Συνεπώς αν $f(d)$ συμβολίσουμε το πλήθος των στοιχείων του A(d) τότε θα είναι

$$\sum_{d|n}f(d)=n. \quad (1)$$

Όμως είναι (k,n)=d αν και μόνο αν $(\frac{k}{d},\frac{n}{d})=1$.Επίσης είναι $0\leq k\leq n$ αν και μόνο αν

$0\leq\frac{k}{d}\leq\frac{n}{d}$.Άρα αν τεθεί $q=\frac{k}{d}$ τότε υπάρχει αμφιμονοσήμαντη αντιστοιχία μεταξύ των στοιχείων του A(d) και των ακεραίων q με τις εξής ιδιότητες $0\leq q\leq\frac{n}{d}$ και $(q,\frac{n}{d})=1$.Το πλήθος αυτών των q είναι $\varphi(\frac{n}{d})$.Επομένως $f(d)=\varphi(\frac{n}{d})$,συνεπώς η (1) γίνεται

$$\sum_{d|n}\varphi(\frac{n}{d})=n$$

Όμως αυτή είναι ισοδύναμη με την $\sum_{d|n}\varphi(d)=n$,διότι όταν το d διατρέχει το σύνολο των διαρετών του n τότε το ίδιο συμβαίνει και για το $\frac{n}{d}$.#

Παρακάτω θα αποδείξουμε μία σχέση που συνδέει τις φ,μ.

Θεώρημα 2.3 Αν n≥ 1 τότε ισχύει

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

Απόδειξη:Το άθροισμα που ορίζει την φ μπορεί να γραφεί στη μορφή

$\varphi(n)=\sum_{k=1}^{n}\left[\frac{1}{(n,k)}\right]$,όπου το k διατρέχει όλους τους «$\leq n$»

ακεραίους.Εφαρμόζουμε τώρα το θεώρημα 2.1 όπου το n αντικαθίσταται από το (n,k) κι έτσι προκύπτει

$\varphi(n)=\sum_{k=1}^{n}\sum_{d|n}\mu(d)=\sum_{k=1}^{n}\sum_{d|n,d|k}\mu(d)$

Η ισότητα αυτή σημαίνει ότι για ένα συγκεκριμένο διαιρέτη d του n η άθροιση πρέπει να γίνει για όλους τους ακεραίους k με $1\leq k\leq n$,που είναι πολλαπλάσια του d.Αν γράψουμε k=qd τότε θα είναι $1\leq k\leq n$ αν και μόνο αν $1\leq q\leq n/d$.Επομένως το προηγούμενο διπλό άθροισμα για το φ(n) μπορεί να γραφεί ως εξής:

$\varphi(n)=\sum_{d|n}\sum_{q=1}^{n/d}\mu(d)=\sum_{d|n}\mu(d)\sum_{q=1}^{n/d}1=\sum_{d|n}\mu(d)\frac{n}{d}$.#

Το άθροισμα στο θεώρημα 2.3 μπορεί να εκφραστεί σαν ένα γινόμενο πάνω στους διάφορους πρώτους διαρέτες του n.

Θεώρημα 2.4 Για κάθε ακέραιο n≥1 ισχύει

$$\varphi(n)=n\cdot\prod_{p|n}\left(1-\frac{1}{p}\right)$$

Απόδειξη:Για n=1 το γινόμενο είναι κενό επειδή δεν υπάρχουν πρώτοι που διαιρούν τον 1.Στην περίπτωση αυτή εννοείται πως στο γινόμενο θα δοθεί η τιμή 1.Ας υποθέσουμε ότι n>1 και έστω $p_1,\ldots,p_r$ οι διαφορετικοί πρώτοι διαιρέτες του n.Το γινόμενο μπορεί να γραφεί ως εξής:

$$\prod_{p|n}\left(1-\frac{1}{p}\right)=\prod_{i=1}^{r}\left(1-\frac{1}{pi}\right)=1-\sum\frac{1}{pi}+\sum\frac{1}{pipj}-\sum\frac{1}{pipjpk}+\ldots.+\frac{(-1)^r}{p_1p_2\ldots.p_r}$$

Στο δεξί μέλος αυτής της ισότητας σε έναν όρο όπως στον $\sum\frac{1}{pipjpk}$ εννοείται ότι θεωρούμε όλα τα δυνατά γινόμενα $p_ip_jp_k$ διαφορετικών πρώτων παραγόντων του n που τους παίρνουμε ανά τρεις.Πρέπει να παρατηρήσουμε ότι κάθε όρος στο δεξί μέλος είναι της μορφής $\pm$1/d όπου d είναι ένας διαρέτης του n που είναι 1 ή γινόμενο από διαφόρους πρώτους.Ο αριθμητής $\pm$1 είναι ίσος με μ(d).Επειδή είναι μ(d)=0 όταν ο d διαιρείται από το τετράγωνο οποιουδήποτε p_i,είναι φανερό ότι το συνολικό άθροισμα είναι ίσο με

$\sum_{d|n}\mu(d)$/d,αυτό όμως αποδεικνύει το θεώρημα.#

Θα αναφέρουμε ενδεικτικά κάποιες ιδιότητες της φ(n) χωρίς απόδειξη προς οικονομία χώρου.

Θεώρημα 2.5 Η συνάρτηση φ(n) έχει τις παρακάτω ιδιότητες:

1.$\varphi(p^a)= p^a-p^{a-1}$ για κάθε p πρώτο και $a\geq 1$

2.φ(mn)=φ(m)φ(n)(d/φ(d)) όπου d=(m,n)

3.φ(mn)=φ(m)φ(n) αν (m,n)=1

4.a|b συνεπάγεται φ(a)|φ(b)

5.ο φ(n) είναι άρτιος για $n\geq 3$,επιπλέον αν ο n έχει r διαφορετικούς περιττούς πρώτους παράγοντες τότε $2^r|\varphi(n)$.#

2.3 Το κατά Dirichlet γινόμενο αριθμητικών συναρτήσεων

Στο θεώρημα 2.3 απεδείχθη ότι φ(n)= $\sum_{d|n}\mu(d)\frac{n}{d}$

Το άθροισμα στο δεξί μέλος αυτής της σχέσης είναι του τύπου $\sum_{d|n}f(d)g(\frac{n}{d})$,με f,g αριθμητικές συναρτήσεις.Τέτοια αθροίσματα εμφανίζονται πολύ συχνά στην θεωρία αριθμών και ως εκ τούτου χρήζουν ιδιαίτερης μελέτης.

Ορισμός:Αν f,g είναι δύο αριθμητικές συναρτήσεις ορίζουμε το κατά Dirichlet γινόμενό τους (ή συνέλιξη Dirichlet) ως την αριθμητική συνάρτηση h που ορίζεται ως εξής:

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

Ισοδύναμα γράφουμε h(n)=f(n) $*$g(n) (h=f $*$g)

φ=μ $*$N,όπου N(n)=n.

Θεώρημα 2.6 Ο κατά Dirichlet πολλαπλασιασμός είναι αντιμεταθετικός και προσεταιριτικός,δηλαδή για οποιεσδήποτε f,g,k έχουμε

f $*$g=g$*$ f

(f $*$g) $*$k=f $*$ (g$*$k)

Η απόδειξη του παραπάνω θεωρήματος παραλείπεται σκοπίμως.

Ορισμός:Η αριθμητική συνάρτηση I που ορίζεται από τον παρακάτω τύπο

$$I(n)=\left[\frac{1}{n}\right]=\begin{cases}1, \alpha\nu\ n=1\\ 0, \alpha\nu\ n>1\end{cases}$$

ονομάζεται ταυτοτική συνάρτηση.

Θεώρημα 2.7 Για κάθε f ισχύει $I*f=f*I=f$.

Απόδειξη:Έχουμε $(f*I)(n)=\sum_{d|n} f(d)I(\frac{n}{d})=\sum_{d|n} f(d)\left[\frac{d}{n}\right]=f(n)$,διότι [d/n]=0 για d<n.#

2.4 Αντίστροφες κατά Dirichlet συναρτήσεις και ο τύπος αντιστροφής του Mobius

Θεώρημα 2.8 Έστω f αριθμητική συνάρτηση με $f(1)\neq 0$.Τότε υπάρχει μοναδική αριθμητική συνάρτηση f^{-1} (η κατά Dirichlet αντίστροφη) τέτοια ώστε $f*f^{-1}=f^{-1}*f=I$.Ακόμη, η f^{-1}προσδιορίζεται από τους εξής αναγωγικούς τύπους:

$f^{-1}(1)=\frac{1}{f(1)}$, $f^{-1}(n)=\frac{-1}{f(1)}\sum_{\substack{d|n\\ d<n}} f(\frac{n}{d})f^{-1}(d)$ για n>1.

Απόδειξη:Αν δοθεί η f θα αποδειχθεί ότι η εξίσωση $(f*f^{-1})(n)=I(n)$ έχει μία μοναδική λύση για τις συναρτησιακές τιμές $f^{-1}(n)$.Για n=1 έχουμε να λύσουμε την εξίσωση

$(f*f^{-1})(1)=I(1)$ η οποία ανάγεται στην $f(1)f^{-1}(1)=1$.

Από την υπόθεση έχουμε ότι $f(1)\neq 0$ έπεται ότι υπάρχει μοναδική λύση,η $f^{-1}(1)=\frac{1}{f(1)}$.Ας υποθέσουμε τώρα ότι n>1 και ότι οι τιμές $f^{-1}(k)$ έχουν προσδιορισθεί μονοσήμαντα για κάθε k<n.Τότε έχουμε να λύσουμε την εξίσωση $(f*f^{-1})(n)=I(n)$,δηλ.

την $\sum_{d|n} f(\frac{n}{d})f^{-1}(d)=0$ η οποία μπορεί να γραφεί ως,

$f(1)f^{-1}(n)+\sum_{\substack{d|n\\ d<n}} f(\frac{n}{d})f^{-1}(d)=0$

Αν οι τιμές $f^{-1}(d)$ είναι γνωστές για κάθε διαιρέτη του n με d<n,τότε υπάρχει μία μονοσήμαντα προσδιοριζόμενη τιμή $f^{-1}(n)$,η

$$f^{-1}(n)=\frac{-1}{f(1)}\sum_{\substack{d|n\\ d<n}} f(\frac{n}{d})f^{-1}(d).$$

Αυτή η ισότητα και η $f^{-1}(1)=\frac{1}{f(1)}$ αποδεικνύουν επαγωγικά την ύπαρξη και το μονοσήμαντο της f^{-1}.#

Ορισμός:Ορίζουμε την μοναδιαία συνάρτηση u ως την αριθμητική συνάρτηση με u(n)=1 για κάθε n.

Θεώρημα 2.9 Τύπος αντιστροφής του Mobius.Η εξίσωση

$$f(n)=\sum_{d|n} g(d) \quad (1)$$

συνεπάγεται

$$g(n)=\sum_{d|n} f(d)\mu(\frac{n}{d}) \quad (2)$$ και αντιστρόφως.

Απόδειξη:Η εξίσωση (1) σημαίνει ότι $f=g*u$.Ο πολλαπλασιασμός αυτής της ισότητας με την μ μας δίνει $f*\mu=(g*u)*\mu=g*I=g$ δηλαδή $f*\mu=g$ που είναι η (2).Αντίστροφα,η (2) σημαίνει ότι $f*\mu=g$.Ο πολλαπλασιασμός των μελών της ισότητας επί u μας δίνει

$g*u=(f*\mu)*u=f*(\mu*u)=f*I=f$,δηλ $g*u=f$ που είναι η (1).#

2.5 Η συνάρτηση (von) Mangoldt Λ(n)

Σε αυτή την παράγραφο θα ορίσουμε την συνάρτηηση Λ(n) που παίζει κεντρικό ρόλο στην κατανομή των πρώτων αριθμών.

Ορισμός:Για κάθε ακέραιο $n\geq 1$ ορίζουμε

$$\Lambda(n)=\begin{cases} log p, \text{όταν } n=p^m \text{ για κάποιον πρώτο } p \text{ και } m\geq 1 \\ 0, \text{σε κάθε άλλη περίπτωση} \end{cases}$$

Θεώρημα 2.10 Για κάθε $n\geq 1$ ισχύει

$$log\, n=\sum_{d|n}\Lambda(n).$$

Απόδειξη:Το θεώρημα αληθεύει για n=1 επειδή και τα δύο μέλη της παραπάνω σχέσης είναι μηδέν.Επομένως υποθέτουμε n>1 και έστω ότι ο n γράφεται ως εξής:

$n=p_1^{a1}\cdot \ldots \cdot p_r^{ar}$,παίρνοντας λογαρίθμους έχουμε $log\, n=\sum_{k=1}^{r} a_k log p_k$.

Τώρα ας θεωρήσουμε το άθροισμα $\sum_{d|n} \Lambda(d)$,στο άθροισμα αυτό οι μόνοι μη μηδενικοί όροι προέρχονται από τους διαιρέτες d της μορφής p_k^m για m=1,2,…,a_k και k=1,2,…,r.Επομένως,

$\sum_{d|n} \Lambda(d)=\sum_{k=1}^{r} \sum_{m=1}^{a_k} \Lambda(p_k^m)=\sum_{k=1}^{r} \sum_{m=1}^{a_k} logp_k=\sum_{k=1}^{r} a_k logp_k=log$n.#

Ακολουθεί ένα θεώρημα(χωρίς απόδειξη) που κάνει χρήση της αντιστροφής κατά Mobius για να εκφραστεί η Λ(n) μέσω του λογαρίθμου.

Θεώρημα 2.11 $\Lambda(n)=\sum_{d|n} \mu(d)\log(\frac{n}{d})= -\sum_{d|n} \mu(d)\log(d)$.

2.6 Πολλαπλασιαστικές συναρτήσεις

Ορισμός:Μία αριθμητική συνάρτηση f λέγεται πολλαπλασιαστική,αν η f δεν είναι ταυτοτικά μηδέν και αν ισχύει:

$f(mn)=f(m)f(n)$ για (m,n)=1

Μία πολλαπλασιαστική συνάρτηση λέγεται πλήρως πολλαπλασιαστική αν δεν χρειάζεται οι m,n να είναι σχετικά πρώτοι.

Στη συνέχεια θα δώσουμε δύο παραδείγματα πολλαπλασιαστικών συναρτήσεων.

Παράδειγμα 1:Η συνάρτηση φ είναι πολλαπλασιαστική,όμως δεν είναι πλήρως πολλαπλασιαστική διότι φ(4)=2 και φ(2)φ(2)=1.

Παράδειγμα 2:Το σύνηθες γινόμενο δύο αριθμητικών συναρτήσεων f,g ορίζεται από τον τύπο $(fg)(n)=f(n)g(n)$ και το πηλίκο f/g ορίζεται από τον τύπο $(f/g)(n)=f(n)/g(n)$.Αν οι f,g είναι πλήρως πολλαπλασιαστικές τότε το γινόμενο και το πηλίκο είναι πλήρως πολλαπλασιαστικές.

Θεώρημα 2.12 Αν η f είναι πολλαπλασιαστική τότε $f(1)=1$.

Απόδειξη:Από το γεγονός (n,1)=1 για κάθε n έπεται ότι $f(n)=f(1)f(n)$ για κάθε n.Επειδή η f δεν είναι ταυτοτικά μηδέν θα ισχύει $f(n) \neq 0$ για κάποιο n,άρα $f(1)=1$.#

Θεώρημα 2.13 Αν οι f,g είναι πολλαπλασιαστικές,τότε το ίδιο ισχύει και για το κατά Dirichlet γινόμενό τους $f * g$.

Απόδειξη:Έστω h=$f * g$ και m,n φυσικοί σχετικά πρώτοι,τότε

$h(mn)=\sum_{c|mn} f(c)g(\frac{mn}{c})$

Κάθε διαρέτης c του mn μπορεί να εκφρασθεί στην μορφή c=ab όπου a|m,b|n.Ακόμη ισχύει (a,b)=1 και (m/a,n/b)=1 και συνεπώς υπάρχει μια αμφιμονοσήμαντη αντιστοιχία μεταξύ του συνόλου των γινομένων ab και του συνόλου των διαιρετών c του mn.

Επομένως,

h(mn)=$\sum_{\substack{a|m\\b|n}} f(ab)g(\frac{mn}{ab})=\sum_{\substack{a|m\\b|n}} f(a)f(b)g\left(\frac{m}{a}\right)g(\frac{n}{b})=\sum_{a|m} f(a)g(\frac{m}{a})\sum_{b|n} f(b)g(\frac{n}{b})=$
h(m)h(n).#

Παρατήρηση: Το κατά Dirichlet γινόμενο δύο πλήρως πολλαπλασιαστικών συναρτήσεων δεν είναι πλήρως πολλαπλασιαστική συνάρτηση.

Θεώρημα 2.14 Αν οι g και οι $f*$g είναι πολλαπλασιαστικές τότε και η f είναι πολλαπλασιαστική.

Απόδειξη:Θα υποθέσουμε ότι η f δεν είναι πολλαπλασιαστική και θα συνάγουμε ότι η $f*$g δεν είναι πολλαπλασιαστική.Έστω h=$f*$g,από το ότι η f έχει υποτεθεί μη πολλαπλασιαστική τότε υπάρχουν m,n με (m,n)=1 τέτοιοι ώστε

f(mn)≠ f(m)f(n) (*)

Εκλέγουμε ένα ζεύγος m,n με την ιδιότητα (*) τέτοιο ώστε το γινόμενο mn να είναι το ελάχιστο δυνατό.

Αν mn=1 τότε $f(1) \neq f(1)f(1)$ και τότε $f(1) \neq 1$.Επειδή h(1)=f(1)g(1)=$f(1) \neq 1$ η h δεν είναι πολλαπλασιαστική.

Αν mn>1,τότε έχουμε f(ab)=f(a)f(b) για όλους τους φυσικούς a,b με (a,b)=1 και ab<mn.Τώρα παρόμοια με το προηγούμενο θεώρημα με την εξαίρεση ότι στο άθροισμα που ορίζει το h(mn),απομακρύνουμε τον όρο που αντισοιχεί σε a=m,b=n.Έτσι έχουμε

h(mn)=$\sum_{\substack{a|m\\b|n\\ab<mn}} f(ab)g\left(\frac{mn}{ab}\right)+f$(mn)g(1)= $\sum_{\substack{a|m\\b|n\\ab<mn}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right)+f$(mn)=

$\sum_{a|m} f(a)g(\frac{m}{a})\sum_{b|n} f(b)g(\frac{n}{b}) - f(m)f$(n) +$f$(mn)=h(m)h(n)−$f(m)f$(n)+$f$(mn).

Αφού f(mn) ≠ f(m)f(n) δείχνει ότι h(mn) ≠h(m)h(n) και άρα η h δεν έιναι πολλαπλασιαστική,άτοπο.#

Θεώρημα 2.15 Αν η g είναι πολλαπλασιαστική τότε το ίδιο ισχύει και για την g^{-1},την κατά Dirichlet αντίστροφή της.

Απόδειξη:Από το προηγούμενο θεώρημα επειδή οι g και $g*g^{-1}$=I είναι και οι δύο πολλαπλασιαστικές.#

2.7 Η αντίστροφη μιας πλήρως πολλαπλασιαστικής συνάρτησης

Η κατά Dirichlet αντίστροφη μιας πλήρως πολλαπλασιαστικής συνάρτησης είναι ιδιαιτέρως εύκολο να προσδιορισθεί.Αυτό γίνεται εμφανές στο παρακάτω θεώρημα.

Θεώρημα 2.16 Έστω ότι η f είναι πολλαπλασιαστική.Τότε η f είναι πλήρως πολλαπλασιαστική αν και μόνο αν

$f^{-1}(n)=\mu(n)f(n)$ για κάθε $n \geq 1$.

Απόδειξη:Έστω $g(n)=\mu(n)f(n)$.Αν η f είναι πλήρως πολλαπλασιαστική τότε ισχύει

$(g*f)(n)=\sum_{d|n}\mu(d)f(d)f(\frac{n}{d})=f(n)\sum_{d|n}\mu(d)=f(n)I(n)$ διότι $f(1)=1$ και $I(n)=0$ για $n>1$.Επομένως $g=f^{-1}$.

Αντίστροφα,ας υποτεθεί ότι έχουμε $f^{-1}(n)=\mu(n)f(n)$.Για να αποδειχθεί ότι η f είναι πλήρως πολλαπλασιαστική,αρκεί ν' αποδειχθεί ότι ισχύει $f(p^a)=f(p)^a$ για δυνάμεις πρώτων p^a.Πράγματι, η εξίσωση $f^{-1}(n)=\mu(n)f(n)$ συνεπάγεται ότι

$\sum_{d|n}\mu(d)f(d)f(\frac{n}{d})=0$ για κάθε $n>1$.

Επομένως αν ληφθεί $n=p^a$,τότε θα είναι:

$\mu(1)f(1)\,f(p^a)+\mu(p)f(p)f(p^{a-1})=0$,

απ' όπου προκύπτει ότι $f(p^a)=f(p)\,f(p^{a-1})$.Αυτό συνεπάγεται με επαγωγή στον a ότι είναι $f(p^a)=f(p)^a$ συνεπώς η f είναι πλήρως πολλαπλασιαστική.#

2.8 Οι συναρτήσεις d(n),λ(n),σ(n),r(n)

Σ’ αυτή την ενότητα θα παρουσιάσουμε κάποιες βασικές πολλαπλασιαστικές συναρτήσεις αρχίζοντας από την d(n).

Ορισμός:Η συνάρτηση d(n) ορίζεται ως εξής:

d(n)=$\sum_{k|n} 1=\sum_{k|n} u(k)$,άρα η d είναι πολλαπλασιαστική αφού και η u είναι πολλαπλασιαστική.

Ορισμός:Η συνάρτηση σ ορίζεται ως εξής:

σ(n)= $\sum_{k|n} k=\sum_{k|n} I(k)$,άρα η σ είναι πολλαπλασιαστική αφού η I είναι πολλαπλασιαστική.

Ορισμός:Η συνάρτηση λ(n) ορίζεται ως εξής:

$$\lambda(n)=\begin{cases} 1, \alpha\nu\ n=1 \\ (-1)^{a_1+a_2+\cdots+a_k}, \alpha\nu\ n=p_1^{a1}\cdot \ldots \cdot p_k^{ak} \end{cases}$$

Από τον ορισμό είναι προφανές πως η λ(n) είναι πλήρως πολλαπλασιαστική συνάρτηση.

Ορισμός:Η συνάρτηση r(n) ορίζεται ως εξής:

Ορίζουμε r(n) τον αριθμό των διαφορετικών αναπαραστάσεων του n στη μορφή $n=A^2+B^2$,όπου τα A,B είναι ακέραιοι.Υπολογίζουμε τις διαφορετικές αναπαραστάσεις ακόμα και όταν αυτές διαφέρουν στο πρόσημο ή ακόμα και στη σειρά,π.χ.

$0=0^2+0^2$, r(0)=1

$1=(\pm 1)^2+0^2=0^2+(\pm 1)^2$, r(1)=4

$5=(\pm 2)^2+(\pm 1)^2=(\pm 1)^2+(\pm 2)^2$, r(5)=8

Αναφέρουμε ότι r(n)=8 όταν ο n είναι πρώτος της μορφής 4λ+1 και r(n)=0 όταν ο n είναι της μορφής 4λ+3.

3 Μέσοι όροι αριθμητικών συναρτήσεων και μερικά στοιχειώδη θεωρήματα για την κατανομή των πρώτων

3.1 Εισαγωγή

Στο προηγούμενο κεφάλαιο εξετάστηκαν διάφορες αριθμητικές συναρτήσεις καθώς και κάποες σχέσεις που ικανοποιούν.Στο παρόν κεφάλαιο θα μελετηθεί η συμπεριφορά αριθμητικών συναρτήσεων για μεγάλες τιμές του n.Ως παράδειγμα ας θεωρήσουμε την d(n) όπως αυτή ορίστικε στο κεφάλαιο 2,αυτή η συνάρτηση παίρνει την τιμή 2 άπειρες φορές όταν ο n είναι πρώτος και παίρνει αυθαίρετα μεγάλες τιμές όταν ο n έχει μεγάλο πλήθος διαρετών,π.χ.$d(p^m)=m+1$ για p πρώτο,έτσι γίνεται φανερό ότι οι τιμές της d διακυμαίνονται αισθητά καθώς ο n μεταβάλλεται.Επειδή αρκετές συναρτήσεις παρουσιάζουν τέτοιες διακυμάνσεις είναι χρήσιμο να μελετάται ο μέσος όρος τους,δηλ.

$\tilde{f}(n)=\frac{1}{n}\sum_{k=1}^{n} f(k)$.

Οι μέσοι όροι εξομαλύνουν τις διακυμάνσεις οπότε οι $\tilde{f}(n)$ παρουσιάζουν μία κανονικότητα.Για τη μελέτη του μέσου όρου θα χρησιμοποιήσουμε τα μερικά αθροίσματα της $f, \sum_{k=1}^{n} f(k)$ τα οποία μπορούν να θεωρηθούν και ως εξής:$\sum_{k\leq x} f(k)$ για κάποιο θετικό πραγματικό x.Εδώ ο δείκτης k μεταβάλλεται απο 1 έως [x].Θεωρώντας τα παραπάνω αθροίσματα ως συναρτήσεις του x στόχος μας είναι να προσδιορίσουμε τη συμπεριφορά αυτών των συναρτήσεων για μεγάλα x.Τέλος θα κάνουμε χρήση ορισμένων συμβλόλων όπως π.χ. O,~ των οποίων τις επεξηγήσεις δίνουμε στο παράρτημα.

3.2 Αθροιστικός τύπος του Euler

Στην παρούσα ενότητα θα ορίσουμε τον αθροιστικό τύπο του Euler και θα αποδείξουμε κάποιους ασυμτωτικούς τύπους.Η ασυμπτωτική τιμή[1] ενός μερικού αθροίσματος μπορεί να προκύψει από τη συγκρισή του μ' ένα ολοκλήρωμα και ο τύπος του Euler δίνει μία έκφραση για το σφάλμα που προκύπτει σε μία τέτοια προσέγγιση.

Θεώρημα 3.2.1(Αθροιστικός τύπος του Euler).Αν η f έχει συνεχή παράγωγο στο διάστημα [y,x] όπου 0<y<x τότε

$$\sum_{y<n\leq x} f(n)=\int_y^x f(t) +\int_y^x (t-[t])f'(t)dt +f(\mathrm{x})([\mathrm{x}]-\mathrm{x}) -f(\mathrm{y})([\mathrm{y}]-\mathrm{y}).$$

Απόδειξη:Έστω m=[y],k=[x],για ακέραιους n και n−1 στο [y,x] ισχύει:

$\int_{n-1}^{n}[t]f'(t)dt=\int_{n-1}^{n}(n-1)f'(t)dt=(\mathrm{n}-1)\{f(\mathrm{n})-f(\mathrm{n}-1)\}=\{\mathrm{n}f(\mathrm{n})-(\mathrm{n}-1)f(\mathrm{n}-1)\}-f(\mathrm{n})$

Αθροίζοντας από n=m+1 έως n=k βρίσκουμε:

$\int_m^k[t]f'(t)dt=\sum_{n=m+1}^{k}\{nf(n)-(n-1)f(n-1)\}-\sum_{y<n\leq x}f(n)=$

$\mathrm{k}f(\mathrm{k})-\mathrm{m}f(\mathrm{m})-\sum_{y<n\leq x}f(n)$

επομένως

$\sum_{y<n\leq x}f(n)=-\int_m^k[t]f'(t)dt+\mathrm{k}f(\mathrm{k})-\mathrm{m}f(\mathrm{m})=-\int_y^x[t]f'(t)dt+\mathrm{k}f(\mathrm{x})-\mathrm{m}f(\mathrm{y})$

$\int_y^x f(t)=\mathrm{x}f(\mathrm{x})-\mathrm{y}f(\mathrm{y})-\int_y^x tf'(t)dt$,που σε συνδυασμό με την παραπάνω σχέση δίνει το ζητούμενο.

Παρακάτω θ' αποδείξουμε ορισμένους ασυμπτωτικούς τύπους βάσει του τύπου του Euler.

Θεώρημα 3.2.2 Αν x≥ 1 τότε ισχύουν:

a) $\sum_{n\leq x}1/n=\log\mathrm{x}+C+O(1/\mathrm{x})$,όπου $C=\lim_{n\to\infty}(1+\frac{1}{2}+\cdots.+\frac{1}{n}-logn)$,σταθερά του Euler

b) $\sum_{n\leq x}\frac{1}{n^s}=\frac{x^{1-s}}{1-s}+\zeta(\mathrm{s})+O(\mathrm{x}^{-\mathrm{s})}$ αν s>0,≠ 1

c) $\sum_{n>x}\frac{1}{n^s}=O(\mathrm{x}^{1-\mathrm{s}})$,s>1

d) $\sum_{n\leq x}n^a=\frac{x^{a+1}}{a+1}+O(\mathrm{x}^{\mathrm{a}})$ αν a≥ 0

Όπου στο b η ζ(s) είναι η συνάρτηση του Riemann που ορίζεται για s>1

[1] Βλέπε παράρτημα ασυμπτωτική συμπεριφορά

$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}$

και για 0<s<1

$\zeta(s)=\lim_{n\to\infty}(\sum_{n\le x}\frac{1}{n^s}-\frac{x^{1-s}}{1-s})$

Απόδειξη:

a)Έστω $f(t)=1/t$ στον αθροστικό τύπο του Euler οπότε προκύπτει:

$\sum_{n\le x}\frac{1}{n}=\int_1^x\frac{dt}{t}-\int_1^x\frac{t-[t]}{t^2}dt+1-\frac{x-[x]}{x}=log x-\int_1^x\frac{t-[t]}{t^2}dt+1+O(1/x)=log x+1-\int_1^{\infty}\frac{t-[t]}{t^2}dt+\int_x^{\infty}\frac{t-[t]}{t^2}dt$

Τα γενικευμένα ολοκληρώματα υπάρχουν διότι υπάρχουν τα $\int_1^{\infty}\frac{1}{t^2}dt$ και $\int_x^{\infty}\frac{1}{t^2}dt$ και ισχύει $\frac{t-[t]}{t^2}<\frac{1}{t^2}$,εξ' άλλου είναι

$0\le\int_x^{\infty}\frac{t-[t]}{t^2}dt\le\int_x^{\infty}\frac{1}{t^2}dt=1/x$

Οπότε έχουμε $\sum_{n\le x}\frac{1}{n}=log x+1-\int_1^{\infty}\frac{t-[t]}{t^2}dt+O(1/x)$,οπότε με $C=1-\int_1^{\infty}\frac{t-[t]}{t^2}dt$ έχουμε το a.

b)Για την απόδειξη του b χρησιμοποιούμε ανάλογους συλλογισμούς με $f(x)=x^{-s}$ με $s>0,\neq 1$.Ο αθροιστικός τύπος του Euler δίνει,

$\sum_{n\le x}\frac{1}{n^s}=\int_1^x\frac{dt}{t^s}-s\int_1^x\frac{t-[t]}{t^{s+1}}dt+1-\frac{x-[x]}{x^s}=\frac{x^{1-s}}{1-s}-\frac{1}{1-s}+1-s\int_1^{\infty}\frac{t-[t]}{t^{s+1}}dt+O(\psi)$

που δίνει το b με $C=-\frac{1}{1-s}+1-s\int_1^{\infty}\frac{t-[t]}{t^{s+1}}dt$

Αν s>1 τότε τα $\frac{x-[x]}{x^s},\frac{x^{1-s}}{1-s}$ τείνουν στο μηδέν για x να τείνει στο μηδέν και άρα C=ζ(s).

Αν s<1 το x^{-s} τείνει στο μηδέν για x τείνει στο άπειρο $\lim_{x\to\infty}(\sum_{n\le x}\frac{1}{n^s}-\frac{x^{1-s}}{1-s})=C$ άρα και πάλι ζ(s)=C

c)Για την απόδειξη του c χρησιμοποιούμε το b με s>1 οπότε έχουμε:

$\sum_{n>x}\frac{1}{n^s}=\zeta(s)-\sum_{n\le x}\frac{1}{n^s}=\frac{x^{1-s}}{1-s}+O(x^{-s})=O(x^{1-s})$,διότι $x^{-s}\le x^{1-s}$

d)Για την απόδειξη του d χρησιμοποιούμε τον αθροιστικό τύπο του Euler με $f(t)=t^a$ και έχουμε:

$\sum_{n\le x}n^a=\int_1^x t^a\,dt+a\int_1^x t^{a-1}(1-[t])dt+1-(x-[x])x^a=\frac{x^{a+1}}{a+1}-\frac{1}{a+1}+O(a\int_1^x t^{a-1}dt)+O(x^a)=\frac{x^{a+1}}{a+1}+O(x^a)$.#

Στη συνέχεια θα παραθέσουμε χωρίς απόδειξη τα μέσα μεγέθη των d(n),σ(n),φ(n),μ(n) και Λ(n).

$\sum_{n\le x}d(n)=xlogx+(2C-1)x+O(\sqrt{x})$,όπου C η σταθερά του Euler.

$\sum_{n\le x}\sigma(n)=\frac{1}{2}\zeta(2)x^2+O(xlogx)$.

$\sum_{n\le x}\varphi(n)=\frac{3}{\pi^2}x^2+O(x\log x)$.

και

$\lim_{x\to\infty}\frac{1}{x}\sum_{n\le x}\mu(n)=0$.

$\lim_{x\to\infty}\frac{1}{x}\sum_{n\le x}\Lambda(n)=1$.

Για τις μ,Λ ο προσδιορισμός των μερικών αθροισμάτων είναι αρκετά δύσκολος.Τα δύο αυτά αποτελέσματα είναι ισοδύναμα με το θεώρημα των πρώτων αριθμών,δηλαδή $\lim_{x\to\infty}\frac{\pi(x)\log x}{x}=1$.

Θεώρημα 3.2.3 Αν $h=f*g$,έστω

$H(x)=\sum_{n\le x}h(n)$ $F(x)=\sum_{n\le x}f(n)$ και $G(x)=\sum_{n\le x}g(n)$.

Τότε είναι:

$H(x)=\sum_{n\le x}f(n)\,G\left(\frac{x}{n}\right)=\sum_{n\le x}g(n)\,F(\frac{x}{n})$.

Απόδειξη:Χρησιμοποιούμε τον επιμεριστικό νόμο (βλ. Παράρτημα) που συνδέει τις πράξεις $\circ$ και $*$.Έστω

$U(x)=\begin{cases}0 & \alpha\nu\ 0<x<1\\ 1 & \alpha\nu\ x\ge 1\end{cases}$

Τότε είναι:$F=f\circ U$,$G=g\circ U$,οπότε:

$f\circ G=f\circ(g\circ U)=(f*g)\circ U=H$

$g\circ F=g\circ(f\circ U)=(g*f)\circ U=H$.#

Θεώρημα 3.2.3 Αν $F(x)=\sum_{n\le x}f(n)$,τότε ισχύει:

$\sum_{n\le x}\sum_{d|n}f(d)=\sum_{n\le x}f(n)\,[\frac{x}{n}]=\sum_{n\le x}F(\frac{x}{n})$.

3.3 Οι συναρτήσεις θ(x) και ψ(x)

Σ΄αυτή την ενότητα θα ορίσουμε τις συναρτήσεις ψ(x) και θ(x) για να δώσουμε στη συνέχεια ισοδύναμες μορφές του θεωρήματος πρώτων αριθμών βάσει αυτών των συναρτήσεων.Σε επόμενη ενότητα θα δειχθεί ότι

$\sum_{n\le x}\Lambda(n)\sim x$ (1)

όταν το x τείνει στο άπειρο.

Ορισμός:Για x>0 ορίζουμε την ψ συνάρτηση του Chebyshev ως εξής:

ψ(x)=$\sum_{n\le x}\Lambda(n)$

οπότε ισοδύναμα η (1) γράφεται $\lim_{x\to\infty}\frac{\psi(x)}{x}$ =1.

Από το ότι $\Lambda(n)$=0 όταν ο n δεν είναι δύναμη πρώτου ενώ $\Lambda(p^m)=logp$ έπεται ότι ο ορισμός της ψ μπορεί να διατυπωθεί ως εξής

ψ(x)= $\sum_{n\le x}\Lambda(n)=\sum_{\substack{m=1\\ p^m\le x}}^{\infty}\sum_p\Lambda(p^m)=\sum_{m=1}^{\infty}\sum_{p\le x^{1/m}}logp$,όπου το άθροισμα με δείκτη m είναι στην πραγματικότητα πεπερασμένο.

Επιπλέον το άθροισμα με δείκτη p είναι κενό όταν $x^{1/m}$<2 δηλαδή όταν (1/m)logx<log2 ή ισοδύναμα m>$\frac{logx}{log2}=log_2x$,οπότε έχουμε

ψ(x)=$\sum_{m\le log_2x}\sum_{p\le x^{1/m}}logp$.

Μέσω της εισαγωγής της συνάρτησης θ(x) η παραπάνω έκφραση μπορεί να γραφεί και ως ψ(x)=$\sum_{m\le log_2x}\theta(x^{\frac{1}{m}})$ (2), με θ(x) να ορίζεται ως εξής,

θ(x)=$\sum_{p\le x}logp$.

Θεώρημα 3.3.1 Για x>0 ισχύει

$0\le\frac{\psi(x)}{x}-\frac{\theta(x)}{x}\le\frac{(logx)^2}{2log2\sqrt{x}}$

$\lim_{x\to\infty}(\frac{\psi(x)}{x}-\frac{\theta(x)}{x})$ =0,το οποίο σημαίνει ότι τα $\frac{\psi(x)}{x},\frac{\theta(x)}{x}$ έχουν ίσα όρια.

Απόδειξη:Από την (2) προκύπτει ότι

0≤ψ(x)−θ(x)=$\sum_{2\le m\le log_2x}\theta(x^{\frac{1}{m}})$,αλλά από τον αριθμό της θ(x) έχουμε την τετριμμένη ανισότητα θ(x)≤ $\sum_{p\le x}logx\le xlogx$.

Επομένως θα είναι:

$0 \le \psi(x) - \theta(x) \le \sum_{2 \le m \le log_2 x} x^{\frac{1}{m}} \log(x^{\frac{1}{m}}) \le (log_2 x)\sqrt{x} log(\sqrt{x}) = \frac{logx}{log2}\frac{\sqrt{x}}{2} logx = \frac{\sqrt{x}(logx)^2}{2log2}$

Και τώρα η διαίρεση με x συμπληρώνει την απόδειξη.#

Θεώρημα 3.3.2(Ταυτότητα του Abel).Για κάθε αριθμητική συνάρτηση a(n) έστω

$A(x) = \sum_{n \le x} a(n)$

Όπου A(x)=0 για x<1.Ας υποθέσουμε ότι η συνάρτηση f έχει συνεχή παράγωγο στο διάστημα [y,x] με 0<y<x.Τότε ισχύει:

$\sum_{y < n \le x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$ (3)

Απόδειξη:Έστω k=[x],m=[y],οπότε A(x)=A(k) και A(y)=A(m).

Τότε: $\sum_{y < n \le x} a(n)f(n) = \sum_{n=m+1}^{k} a(n)f(n) = \sum_{n=m+1}^{k} \{A(n) - A(n-1)\}f(n) = \sum_{n=m+1}^{k} A(n)f(n) - \sum_{n=m}^{k-1} A(n)f(n+1)$

$= \sum_{n=m+1}^{k-1} A(n)\{f(n) - f(n+1)\} + A(k)f(k) - A(m)f(m+1)$

$= -\sum_{n=m+1}^{k-1} A(n) \int_n^{n+1} f'(t)dt + A(k)f(k) - A(m)f(m+1)$

$= -\sum_{n=m+1}^{k-1} \int_n^{n+1} A(t)f'(t)dt + A(k)f(k) - A(m)f(m+1)$

$= -\int_{m+1}^{k} A(t)f'(t)dt + A(x)f(x) - \int_k^x A(t)f'(t)dt - A(y)f(y) - \int_y^{m+1} A(t)f'(t)dt$

$= A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$#

Χρησιμοποιούμε την (3) για να εκφράσουμε (συνδέσουμε) τις θ,ψ.

Θεώρημα 3.3.3. Για $x \ge 2$ έχουμε:

$\theta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t} dt$ (4)

$\pi(x) = \frac{\theta(x)}{logx} + \int_2^x \frac{\theta(t)}{tlog^2 t} dt$ (5)

Απόδειξη:Έστω ότι a(n) συμβολίζει την χαρακτηριστική συνάρτηση των πρώτων αριθμών,δηλ.

a(n)=1,αν ο n είναι πρώτος διαφορετικά είναι 0.

Τότε έχουμε:

$\pi(x) = \sum_{p \le x} 1 = \sum_{1 < n \le x} a(n)$

$\theta(x) = \sum_{p\le x} logp = \sum_{1<n\le x} a(n)logn.$

Παίρνοντας f(x)=logx στην (3) με y=1 συνάγουμε ότι

$\theta(x)=\sum_{1<n\le x} a(n)logn =$ π(x)logx−π(1)log1− $\int_2^x \frac{\pi(t)}{t} dt$ που αποδεικνύει την (4) διότι π(t)=0 για t<2.

Κατόπιν έστω b(n)=a(n)logn οπότε

π(x) =$\sum_{\frac{3}{2}<n\le x} b(n)\frac{1}{logn}$, $\theta(x) = \sum_{n\le x} b(n)$

Αν ληφθεί f(x)=1/logx τότε η (3) με y=3/2 δίνει

π(x) = $\frac{\theta(x)}{logx} - \frac{\theta(\frac{3}{2})}{log3/2} + \int_{3/2}^{x} \frac{\theta(t)}{tlog^2 t}$dt,που αποδεικνύει την (5) διότι θ(t)=0 για t<2.#

Στη συνέχεια θ' αναφέρουμε τρεις προτάσεις ισοδύναμες με το θεώρημα των πρώτων αριθμών.

Θεώρημα 3.3.4. Οι ακόλουθες προτάσεις είναι λογικά ισοδύναμες:

(6) $\lim_{x\to\infty} \frac{\pi(x)logx}{x} = 1$

(7) $\lim_{x\to\infty} \frac{\theta(x)}{x} = 1$

(8) $\lim_{x\to\infty} \frac{\psi(x)}{x} = 1$

Απόδειξη:Από τις (4),(5) προκύπτουν αντίστοιχα,

$\frac{\theta(x)}{x} = \frac{\pi(x)logx}{x} - \frac{1}{x}\int_2^x \frac{\pi(t)dt}{t}$

και $\frac{\pi(x)logx}{x} = \frac{\theta(x)}{x} + \frac{logx}{x}\int_2^x \frac{\theta(t)dt}{tlog^2 t}$.

Για ν' αποδειχθεί ότι η (6) συνεπάγεται την (7) απαιτείται μόνο να αποδειχθεί ότι η (6) συνεπάγεται την εξής:

$\lim_{x\to\infty} \frac{1}{x}\int_2^x \frac{\pi(t)dt}{t}$ =0.

Αλλά η (6) συνεπάγεται ότι ισχύει :

$\frac{\pi(t)}{t}$ =O($\frac{1}{logt}$) για t≥ 2 οπότε $\frac{1}{x}\int_2^x \frac{\pi(t)dt}{t}$ =O($\frac{1}{x}\int_2^x \frac{dt}{logt}$)

$\int_2^x \frac{dt}{logt} = \int_2^{\sqrt{x}} \frac{dt}{logt} + \int_{\sqrt{x}}^x \frac{dt}{logt} \leq \frac{\sqrt{x}}{log2} + \frac{x-\sqrt{x}}{log\sqrt{x}}$

οπότε $\frac{1}{x}\int_2^x \frac{dt}{logt} \to 0$ για x$\to \infty$

Αυτό δείχνει ότι η (6) συνεπάγεται την (7).

Για ν'αποδειχθεί ότι η (7) συνεπάγεται την (6) απαιτείται μόνο ν'αποδειχθεί ότι η (7) συνεπάγεται την εξής:

$\lim_{x\to\infty} \frac{logx}{x} \int_2^x \frac{\theta(t)dt}{tlog^2t} = 0$

Αλλά η (7) συνεπάγεται ότι θ(t)=O(t) οπότε

$\frac{logx}{x} \int_2^x \frac{\theta(t)dt}{tlog^2t} = O(\frac{logx}{x} \int_2^x \frac{dt}{tlog^2t})$.

$\int_2^x \frac{1dt}{tlog^2t} = \int_2^{\sqrt{x}} \frac{dt}{log^2t} + \int_{\sqrt{x}}^x \frac{dt}{log^2t} \leq \frac{\sqrt{x}}{log^2 2} + \frac{x-\sqrt{x}}{log^2\sqrt{x}}$ οπότε

$\frac{logx}{x} \int_2^x \frac{dt}{tlog^2t} \to 0 \; για \; x \to \infty.$

Αυτό αποδεικνύει ότι η (7) συνεπάγεται την (6) οπότε αυτές είναι ισοδύναμες.

Γνωρίζουμε ήδη από το θεώρημα 3.3.1 ότι οι (7),(8) είναι ισοδύναμες.#

Το επόμενο θεώρημα συσχετίζει το θεώρημα των πρώτων αριθμών με την ασυμπτωτική τιμή του n-οστού πρώτου αριθμού.

Θεώρημα 3.3.5. Έστω ότι p_n συμβολίζει τον n-οστό πρώτο αριθμό.Τότε οι ακόλουθες ασυμτωτικές σχέσεις είναι ισοδύναμες(παραλείπουμε την απόδειξη)

(9) $lim_{x\to\infty} \frac{\pi(x)logx}{x} = 1$

(10) $lim_{x\to\infty} \frac{\pi(x)\log\pi(x)}{x} = 1$

(11) $lim_{x\to\infty} \frac{p_n}{nlogn} = 1$

Θεώρημα 3.3.6. Για κάθε ακέραιο n≥ 2 ισχύει

$$\frac{1}{6}\frac{n}{logn} < \pi(n) < \frac{n}{logn} \qquad (12)$$

Απόδειξη:Αρχίζουμε με τις ανισότητες:

$2^n \leq \binom{2n}{n} < 4^n$

Η δεξιά ανισότητα προκύπτει από τη σχέση

$4^n=(1+1)^{2n}=\sum_{k=0}^{2n}\binom{2n}{k}>\binom{2n}{n}$,ενώ η άλλη ανισότητα προκύπτει με επαγωγή.Παίρνοντας λογαρίθμους έχουμε

$n\log 2 \leq \log(2n)! - 2\log n! < n\log 4$ (13)

αλλά απο την ταυτότητα του Legendre(για κάθε x≥ 1 [x]!=$\prod_{p\leq x} p^{a(p)}$ και a(p)=$\sum_{m=1}^{\infty}[\frac{x}{p^m}]$)

συνεπάγεται ότι $\log n! = \sum_{p\leq n} a(p)\log p$,με a(p)=$\sum_{m=1}^{[\frac{\log n}{\log p}]}[\frac{n}{p^m}]$.

Συνεπώς,

$$\log(2n)! - 2\log n! = \sum_{p\leq 2n}\sum_{m=1}^{[\frac{\log 2n}{\log p}]}\{[2\frac{n}{p^m}] - 2[\frac{n}{p^m}]\}\log p$$

Επιδή η διαφορά [2x]−2[x] είναι μηδέν ή 1,έπεται ότι η αριστερή ανισότητα στη (13) συνεπάγεται:

$$n\log 2 \leq \sum_{p\leq 2n}(\sum_{m=1}^{[\frac{\log 2n}{\log p}]} 1)\log p \leq \sum_{p\leq 2n}\log 2n = \pi(2n)\log 2n.$$

Αυτή μας δίνει:

$\pi(2n) \geq \frac{n\log 2}{\log 2n} = \frac{2n}{\log 2n}\frac{\log 2}{2} > \frac{1}{4}\frac{2n}{\log 2n}$,διότι $\log 2 > 1/2$ (14).

Για περιττούς ακεραίους έχουμε:

$\pi(2n+1) \geq \pi(2n) > \frac{1}{4}\frac{2n}{\log 2n} > \frac{1}{4}\frac{2n}{2n+1}\frac{2n+1}{\log(2n+1)} \geq \frac{1}{6}\frac{2n+1}{\log(2n+1)}$, διότι $2n/(2n+1) \geq \frac{2}{3}$.

Αυτή μαζί με τη (14) μας δίνει $\pi(n) > \frac{1}{6}\frac{n}{\log n}$ για κάθε n ≥ 2 που αποδεικνύει το αριστερό μέλος της (12).

Για την δεξιά ανισότητα ξαναγυρίζουμε στην :

$$\log(2n)! - 2\log n! = \sum_{p\leq 2n}\sum_{m=1}^{[\frac{\log 2n}{\log p}]}\{[2\frac{n}{p^m}] - 2[\frac{n}{p^m}]\}\log p$$

και εξάγουμε τον όρο που αντιστοιχεί στο m=1.

Οι υπόλοιποι όροι είναι μη αρνητικοί οπότε έχουμε:

$$\log(2n)! - 2\log n! \geq \sum_{n<p\leq 2n}\log p = \theta(2n) - \theta(n)$$

επομένως $\theta(2n) - \theta(n) < n\log 4$.

Ειδικά αν ο n είναι δύναμη του 2 αυτή δίνει:

$\theta(2^{r+1})-\theta(2^r)< 2^r\, log4=2^{r+1}log2$.

Αθροίζοντας για r=0,1,…,k επειδή το από τα αριστερά άθροσιμα είνα τηλεσκοπικό βρίσκουμε ότι ισχύει : $\theta(k)<2^{k+2}log2$.

Εκλέγοντας k έτσι ώστε να είναι $2^k\leq n<2^{k+1}$ έχουμε

$\theta(n)\leq\theta(2^{k+1})< 2^{k+2}log2\leq 4nlog2$,

αλλά όταν $0<\alpha<1$ τότε έχουμε,

$(\pi(n)-\pi(n^a))\log n^a< \sum_{n^a<p\leq n} logp \leq \theta(n) < 4nlog2$.

Κατά συνέπεια

$\pi(n)< \frac{4nlog2}{alogn} + \pi(n^a)< \frac{4nlog2}{alogn} + n^a= \frac{n}{logn}(\frac{4log2}{a} + \frac{logn}{n^{1-a}})$.

Τώρα αν $c>0, x\geq 1$ τότε η συνάρτηση $f(x)=x^{-c}logx$ παίρνει την μέγιστη τιμή της στο $x=e^{1/c}$,οπότε $n^{-c}logn\leq 1/(ce)$ για $n\geq 1$.Παίρνοντας $\alpha=2/3$ στην τελευταία ανισότητα για το $\pi(n)$ βρίσκουμε

$\pi(n)< \frac{n}{logn}(6log2+3/e)<6\frac{n}{logn}$.#

Θεώρημα 3.3.7 Για $n\geq 1$ ο n-οστός πρώτος ικανοποιεί την εξής διπλή ανισότητα:

$\frac{1}{6}nlogn <p_n< 12(nlogn +nlog\frac{12}{e})$.

Απόδειξη: Αν $k=p_n$,τότε $k\geq 2$ και $n=\pi(k)$.Από την (12) έχουμε:

$n=\pi(k)<6\frac{k}{logk} = 6\frac{p_n}{logp_n}$,επομένως

$p_n> \frac{1}{6} log\ p_n> \frac{1}{6}nlogn$.

Για το άνω φράγμα του θεωρήματος χρησιμοποιούμε πάλι την (12) και έχουμε:

$n=\pi(k)> \frac{1}{6}\frac{k}{logk} = \frac{1}{6}\frac{p_n}{logp_n}$,από την οποία βρίσκουμε $p_n<6nlog\ p_n$.

Από το ότι $logx\leq(2/e)\sqrt{x}$ για $x\geq 1$,έπεται ότι $log\ p_n\leq(2/e)\sqrt{p_n}$ οπότε έχουμε,

$\sqrt{p_n}<12n/e$.

Συνεπώς προκύπτει η ανισότητα,

$\frac{1}{2} log\ p_n<logn + log\frac{12}{e}$ η οποία σε συνδυασμό με την ($p_n<6nlog\ p_n$)

μας δίνει $p_n<6n(2logn +2log\frac{12}{e})$,η οποία μας δίνει το ζητούμενο.#

Το άνω φράγμα του προηγούμενου θεωρήματος μας δείχνει πως η σειρά

$\sum_{n=1}^{\infty} \frac{1}{p_n}$ αποκλίνει.Αυτό συμπεραίνεται από το γεγονός ότι $\frac{1}{6}$nlogn <p_n και ότι η

$\sum_{n=2}^{\infty} \frac{1}{nlogn}$ αποκλίνει.

3.4 Το θεώρημα τύπου Tauber του Shapiro

Έχουμε αναφέρει ότι το θεώρημα των πρώτων αριθμών είναι ισοδύναμο με τον ασυμπτωτικό τύπο

$\frac{1}{x}\sum_{n\leq x} \Lambda(n) \sim 1$ για x$\to \infty$.

Επίσης ισχύει $\sum_{n\leq x} \Lambda(n)[\frac{x}{n}]$=x$log$x – x +O($log$x).

Και τα δύο αθροίσματα στις παραπάνω σχέσεις είναι μέσοι όροι με βάρη της Λ(n).Στην πρώτη σχέση κάθε όρος πολλαπλασιάζεται επί 1/x ενώ στην δεύτερη επί [x/n].

Τα θεωρήματα που συσχετίζουν μέσους όρους με βάρη λέγονται θεωρήματα τύπου Tauber.Εξετάζουμε έπειτα ένα τέτοιο θεώρημα που αποδείχτηκε απο τον Shapiro.

Θεώρημα 3.4.1 Έστω a(n) μια μη αρνητική ακολουθία τέτοια ώστε

$\sum_{n\leq x} \alpha(n)[\frac{x}{n}] = xlogx + O(x)$ για κάθε x$\geq$ 1 (15)

Τότε ισχύουν τα εξής:

α)Για x$\geq$ 1 έχουμε:

$\sum_{n\leq x} \frac{a(n)}{n}$ = logx +O(1).

b)Υπάρχει μια σταθερά B>0 τέτοια ώστε

$\sum_{n\leq x} \alpha(n) \leq$Bx για κάθε x$\geq$ 1.

c)Υπάρχει μια σταθερά A>0 και ένα x_o>0 τέτοια ώστε

$\sum_{n\leq x} \alpha(n) \geq Ax$ για κάθε $x \geq x_o$.

Απόδειξη:Εστω

S(x)= $\sum_{n\le x}\alpha(n)$,T(x)= $\sum_{n\le x}\alpha(n)[\frac{x}{n}]$

Αποδεικνύουμε πρώτα την b).Για το σκοπό αυτό αποδεικνύουμε ότι

S(x) – S($x/2$) ≤T(x) – T(x/2) (16)

Αυτή αποδεικνύεται ως εξής:

T(x) – 2T(x/2)= $\sum_{n\le x}\alpha(n)[\frac{x}{n}]-2\sum_{n\le x/2}\alpha(n)[\frac{x}{2n}]$=

$\sum_{n\le x/2}\alpha(n)\{\left[\frac{x}{n}\right]-\left[\frac{x}{2n}\right]\}+\sum_{\frac{x}{2}<n\le x}\left[\frac{x}{n}\right]a(n)$

Από το ότι η διαφορά [2x]-2[x] είναι ή μηδέν ή 1,έπεται ότι το πρώτο άθροισμα είναι μη αρνητικό οπότε προκύπτει ότι:

T(x) – 2T(x/2)≥ $\sum_{\frac{x}{2}<n\le x}\left[\frac{x}{n}\right]a(n)=\sum_{\frac{x}{2}<n\le x}a(n)$= S(x) – S($\frac{x}{2}$).

Αυτό αποδεικνύει την (16).Αλλά η (14) συνεπάγεται ότι :

T(x) – 2T(x/2)=xlogx +O(x) – 2($\frac{x}{2}log\frac{x}{2}$+O(x))=O(x).

Επομένως η (15) συνεπάγεται S(x) – S($\frac{x}{2}$)=O(x).Αυτό σημαίνει ότι υπάρχει κάποια σταθερά K>0 ώστε S(x) – S($\frac{x}{2}$) ≤Kx για κάθε x≥ 1.

Αντικαθιστώντας στην ανισότητα αυτή το x διαδοχικά με x/2,x/4….έχουμε:

S($\frac{x}{2}$) – S($\frac{x}{4}$)≤ $Kx/2$

S($\frac{x}{4}$) – S($\frac{x}{8}$)≤ $Kx/4$ κλπ.

Ας σημειωθεί ότι S($\frac{x}{2^n}$)=0 όταν 2^n>x.Με πρόσθεση κατά μέλη αυτών των ανισοτήτων παίρνουμε:

S(x)≤Kx(1+1/2+1/4…)=2Kx.Αυτό αποδεικνύει την b) με B=2K.

Κατόπιν αποδεικνύουμε την a).Γράφουμε [x/n]=(x/n) +O(1) κι έχουμε:

T(x)= $\sum_{n\le x}\alpha(n)[\frac{x}{n}]=\sum_{n\le x}(O(1)+\frac{x}{n})$a(n)=x$\sum_{n\le x}\frac{a(n)}{n}$ + O($\sum_{n\le x}a(n)$)=x$\sum_{n\le x}\frac{a(n)}{n}$ + O(x).βάσει του b).

Συνεπώς $\sum_{n\le x}\frac{a(n)}{n}$ =T(x)/x +O(1)=logx +O(1).Αυτό αποδεικνύει την a).

Τέλος αποδεικνύουμε την c)Έστω,

A(x)= $\sum_{n\le x}\frac{a(n)}{n}$.Τότε η a) μπορεί να γραφεί ως εξής

A(x)=logx +R(x),όπου R(x) είναι ο όρος σφάλματος.Από το ότι R(x)=O(1) έπεται ότι |R(x)|≤M για κάποιο M>0.

Αν εκλέξουμε α,με 0<α<1(το α θα το καθορίσουμε ακριβέστερα αμέσως μετά) και αν θεωρήσουμε τη διαφορά

A(x)− A(ax)=$\sum_{ax<n\le x}\frac{a(n)}{n}=\sum_{n\le x}\frac{a(n)}{n}-\sum_{n\le ax}\frac{a(n)}{n}$

Αν x≥ 1 και $ax\ge 1$ τότε μπορούμε να εφαρμόσουμε τον ασυμπτωτικό τύπο για το A(x) για να γράψουμε

A(x)− A(ax)=logx +R(x)−(logax+R(x))= $-log$a +R(x) – R(ax)≥ $-log$a−|R(x)|−|R(ax)|

≥ $-log$a −2M.

Τώρα αν εκλέξουμε a έτσι ώστε να είναι –loga−2M=1.Αυτό απαιτεί loga=−2M−1 άρα a=e^{-2M-1}.Ας σημειωθεί ότι 0<a<1.Ακόμη γι'αυτόν τον a ισχύει η ανισότητα A(x)− A(ax) ≥1 αν x≥1/α.

Όμως είναι A(x)− A(ax)= $\sum_{ax<n\le x}\frac{a(n)}{n}\le\frac{1}{ax}\sum_{n\le x}\alpha(n)$=S(x)/ax.

Επομένως S(x)/ax ≥1 αν $x\ge 1/\alpha$

Κατά συνέπεια θα είναι S(x) ≥ax για x≥1/α που αποδεικνύει την c) με A=a,x_o=1/a.#

Θεώρημα 3.4.2 Για κάθε x≥1 ισχύει

$\sum_{n\le x}\Lambda(n)[\frac{x}{n}]=log$x +O(1). (17)

Επίσης υπάρχουν θετικές σταθερές c_1,c_2 τέτοιες ώστε

ψ(x)≤c_1x, για x≥ 1

και

ψ(x) ≥ c_2x, για όλους τους αρκετά μεγάλους x.

Θεώρημα 3.4.3 Για κάθε x≥ 1 ισχύει

$\sum_{p\le x}\frac{\log p}{p}=log$x +O(1)

Επίσης υπάρχουν θετικές σταθερές c_1,c_2 τέτοιες ώστε

θ(x))≤c_1x για x≥ 1

και $\theta(x) \geq c_2 x$ για όλους τους αρκετά μεγάλους x.

Θεώρημα 3.4.4 Για κάθε x≥ 1 ισχύει $\sum_{n\leq x} \psi(\frac{x}{n})$=x$log$x – x +O($log$x)

και $\sum_{n\leq x} \theta(\frac{x}{n})$=x$log$x +O(x).

Θεώρημα 3.4.5(Ένας ασυμτωτικός τύπος για τα μερικά αθροίσματα $\sum_{p\leq x}(\frac{1}{p})$).

Υπάρχει σταθερά A,τέτοια ώστε

$\sum_{p\leq x}(\frac{1}{p})$=$loglog$x +A +O(1/$log$x) για κάθε x≥2.

Απόδειξη:Έστω A(x)= $\sum_{p\leq x}(\frac{logp}{p})$ και έστω

a(n)=$\begin{cases} 1, αν\ o\ n\ είναι\ πρώτος \\ 0, αλλιώς \end{cases}$

Τότε:

$\sum_{p\leq x}(\frac{1}{p})$=$\sum_{n\leq x} \frac{a(n)}{n}$ και A(x)= $\sum_{n\leq x} \frac{a(n)}{n} logn$

Επομένως αν ληφθεί f(t)=1/logt στην ταυτότητα του Abel επειδή A(t)=0 για t<2 προκύπτει:

$\sum_{p\leq x}(\frac{1}{p}) = \frac{A(x)}{logx} + \int_2^x \frac{A(t)}{tlog^2 t} dt$.Από το θεώρημα 3.4.3 έχουμε A(x)= logx +R(x), R(x)=O(1).Έτσι:

$\sum_{p\leq x}(\frac{1}{p}) = \frac{logx+O(1)}{logx} +\int_2^x \frac{logt+R(t)}{tlog^2 t} dt$=1+ O($\frac{1}{logx}$) +$\int_2^x \frac{1}{tlogt} dt$ +$\int_2^x \frac{R(t)}{tlog^2 t} dt$. (18)

Όμως, $\int_2^x \frac{1}{tlogt} dt$=$log(logx) – log(log2)$

και

$\int_2^x \frac{R(t)}{tlog^2 t} dt$=$\int_2^\infty \frac{R(t)}{tlog^2 t} dt - \int_x^\infty \frac{R(t)}{tlog^2 t} dt$,όπου η ύπαρξη των ολοκληρωμάτων εξασφαλίζεται από τη συνθήκη R(t)=O(1).

$\int_x^\infty \frac{R(t)}{tlog^2 t} dt$=O($\int_x^\infty \frac{R(t)}{tlog^2 t} dt$)= O($\frac{1}{logx}$).

Οπότε η (18) μπορεί να γραφτεί ως εξής:

$\sum_{p\leq x}(\frac{1}{p}) = log(logx) + 1 - log(log2) + \int_2^\infty \frac{R(t)}{tlog^2 t} dt$ + O($\frac{1}{logx}$).

Αυτό όμως αποδεικνύει το θεώρημα με A=1$-log(log2)$ + $\int_2^\infty \frac{R(t)}{tlog^2 t} dt$.#

3.5 Τα μερικά αθροίσματα της συνάρτησης Mobius

Ορισμός: Αν x≥1,ορίζουμε,

$$M(x)=\sum_{n\le x}\mu(n).$$

Σε αυτήν την παράγραφο θα αποδείξουμε ότι $\lim_{x\to\infty}\frac{M(x)}{x}=0$ είναι ισοδύναμη με το θεώρημα των πρώτων αριθμών.Αρχικά θα συσχετίσουμε με έναν άλλο μέσο όρο της μ(n) με βάρος.

Ορισμός: Αν x≥ 1,ορίζουμε

$$H(x)=\sum_{n\le x}\mu(n)\log n.$$

Το επόμενο θεώρημα αποδεικνύει ότι η ασυμπτωτική συμπεριφορά της M(x)/x προσδιορίζεται από εκείνη της H(x)/x$\log$x.

Θεώρημα 3.5.1. Ισχύει:

$$\lim_{x\to\infty}\left(\frac{M(x)}{x}-\frac{H(x)}{x\log x}\right)=0. \quad (19)$$

Απόδειξη: Αν ληφθεί f(t)=1/logt στην ταυτότητα,τότε προκύπτει

$$H(x)=\sum_{n\le x}\mu(n)\log n = M(x)\log x-\int_1^x\frac{M(t)}{t}dt.$$

Επομένως αν x>1 θα είναι :

$$\frac{M(x)}{x}-\frac{H(x)}{x\log x}=\frac{1}{x\log x}\int_1^x\frac{M(t)}{t}dt.$$

Άρα,για ν' αποδειχθεί το θεώρημα πρέπει ν' αποδειχθεί ότι

$$\lim_{x\to\infty}\frac{1}{x\log x}\int_1^x\frac{M(t)}{t}dt=0. \quad (20)$$

Όμως έχουμε την τεριμμένη εκτίμηση ότι M(x)=O(x),οπότε

$$\int_1^x\frac{M(t)}{t}dt=O\left(\int_1^x dt\right)=O(x)$$

Απ' όπου προκύπτει η (20) και επομένως η (19).#

Θεώρημα 3.5.2. Το θεώρημα των πρώτων αριθμών συνεπάγεται

$\lim_{x\to\infty} \frac{M(x)}{x} = 0$.

Απόδειξη:Χρησιμοποιούμε το θεώρημα των πρώτων αριθμών με την ισοδύναμη μορφή ψ(x)~x και αποδεικνύουμε ότι H(x)/xlogx→ 0 για x→ ∞.Για τον σκοπό αυτό απαιτείται η ταυτότητα

$-H(x) = -\sum_{n\le x} \mu(n) log n = \sum_{n\le x} \mu(n)\psi(\frac{x}{n})$. (21)

Για ν'αποδείξουμε την (21) αρχίζουμε με το θεώρημα (2.11) που αναφέρει ότι

$\Lambda(n)=\sum_{d|n} \mu(d) log(\frac{n}{d})$ και εφαρμόζουμε αντιστροφή κατά Mobius οπότε έχουμε,

$-\mu(n) log n = \sum_{d|n} \mu(d)\Lambda(\frac{n}{d})$

Αθροίζοντας πάνω σε όλους τους n≤x και χρησιμοποιώντας το θεώρημα 3.2.3 με $f=\mu$,g=Λ συνάγουμε την (21).

Από το ότι ψ(x)~x έπεται ότι αν δοθεί ε>0 τότε υπάρχει μια σταθερά A>0 τέτοια ώστε:

$|\frac{\psi(x)}{x} - 1| <$ε όταν x≥A.

Ισοδύναμα, $|\psi(x) - x| < \varepsilon x$ όταν x≥A. (22)

Αν εκλεγεί x>A και διαχωρίσουμε το άθροισμα στο δεξί μέλος της (21) σε δύο μέρη

$\sum_{n\le y}$ + $\sum_{y<n\le x}$,όπου y=[x/A].

Στο πρώτο άθροισμα έχουμε n≤y οπότε n ≤x/A και επομένως x/n≥A.Συνεπώς μπορούμε να χρησιμοποιήσουμε την (22) για να γράψουμε:

$\left|\psi\left(\frac{x}{n}\right) - \frac{x}{n}\right| < \varepsilon\frac{x}{n}$ αν n≤y.

Έτσι έχουμε:

$\sum_{n\le y} \mu(n)\psi(\frac{x}{n}) = \sum_{n\le y} \mu(n)(\frac{x}{n} + \psi(\frac{x}{n}) - \frac{x}{n}) =$ x$\sum_{n\le y} \frac{\mu(n)}{n} + \sum_{n\le y} \mu(n)(\psi(\frac{x}{n}) - \frac{x}{n})$,

οπότε

$|\sum_{n\le y} \mu(n)\psi(\frac{x}{n})| \le$x$|\sum_{n\le y} \frac{\mu(n)}{n}| + \sum_{n\le y} |(\psi(\frac{x}{n}) - \frac{x}{n})|$

<x + ε$\sum_{n\le y} \frac{x}{n}$ <x +εx(1+logy)<x+ εx +εxlogx.

Στο δεύτερο άθροισμα $\sum_{y<n\leq x}\mu(n)\psi(\frac{x}{n})$ έχουμε:y<n≤x οπότε n≥y+1.

Άρα,

$$\frac{x}{n}\leq\frac{x}{y+1}<A$$

διότι y ≤ $\frac{x}{A}$<y+1.

Η ανισότητα (x/n)<A συνεπάγεται ψ(x/n) ≤ ψ(A).Επομένως το δεύτερο αυτό άθροισμα είναι απόλυτα μικρότερο από το xψ(A).Κατά συνέπεια,το πλήρες άθροισμα της (21) είναι απόλυτα μικρότερο από το

(1+ε)x +εxlogx +xψ(A)<(2+ψ(A))x +εxlogx όταν ε<1.

Με άλλα λόγια αν δοθεί ε με ε<1 τότε ισχύει,

|H(x)|<(2+ψ(A))x +εxlogx αν x>A,δηλαδή

$$\frac{|H(x)|}{xlogx}<\frac{2+\psi(A)}{logx}+\varepsilon$$

Τώρα αν επιλέξουμε B>A,έτσι ώστε η x>B να συνεπάγεται (2+ψ(A))/logx<ε.Τότε για x>B είναι:

$$\frac{|H(x)|}{xlogx}<2\varepsilon,$$

που αποδεικνύει ότι H(x)/xlogx→ 0 για x→ ∞,οπότε βάσει του θεωρήματος 3.5.1 η απόδειξη συμπληρώνεται.#

4 Στοιχειώδης απόδειξη του θεωρήματος των πρώτων αριθμών

Σε αυτό το κεφάλαιο θα δώσουμε τη στοιχειώση απόδειξη του θεωρήματος των πρώτων αριθμών που οφείλεται στους A.Selberg και P.Erdos.

4.1 Εισαγωγή

Θα αποδείξουμε το θεώρημα των πρώτων αριθμών στην ισοδύναμη μορφή του

$\lim_{x\to\infty} \frac{\theta(x)}{x} = 1$ (1.1),όπου $\theta(x) = \sum_{p\le x} logp.$ (1.2)

Η βασική καινούρια 'ιδέα' που θα εισάγουμε για την απόδειξη αυτή είναι η εξής σχέση

$\theta(x)logx + \sum_{p\le x} logp\theta(\frac{x}{p}) = 2xlogx + O(x)$ (1.3).

Απ΄αυτήν την έκφραση υπάρχουν αρκετοί τρόποι να συμπεράνουμε το ζητούμενο.Ο πρώτος τρόπος που είναι ο πιο στοιχειώδης παρουσιάζεται στις παραγράφους 2,4.Η αρχική απόδειξη είναι αρκετά διαφορετική και χρησιμοποιεί το εξής αποτέλεσμα που οφείλεται στον Erdos:

Για ένα αυθαίρετο θετικό σταθερό δ,υπάρχει $K(\delta)>0$ και ένα $x_o=x_o(\delta)$ τέτοιο ώστε για κάθε $x>x_o$ να υπάρχουν

$\frac{K(\delta)x}{logx}$ πρώτοι στο διάστημα της μορφής $x+\delta x$.

Η αρχική απόδειξη έχει ως εξής:

Εισάγουμε τους συμβολισμούς: $\overline{lim}(\frac{\theta(x)}{x})=A$, $\underline{lim}(\frac{\theta(x)}{x})=a$.

Χρησιμοποιώντας το γνωστό αποτέλεσμα ότι $\sum_{p\le x} \frac{logp}{x} = logx + O(1)$ (1.4)

μπορεί εύκολα να συναχθεί ότι $A+a=2$. (1.5)

Έπειτα θεωρώντας το x ως 'μεγάλο' και με $\theta(x)=ax+o(x)$ μπορούμε να συμπεράνουμε από την (3) την τροποποιημένη μορφή:

(θ(x)−ax)logx +$\sum_{p\le x} logp(\theta(\frac{x}{p}) - A\frac{x}{p})$=O(x) (1.6).

Επομένως για ένα σταθερό θετικό δ έχουμε

$\theta\left(\frac{x}{p}\right)$>(A−δ)$\frac{x}{p}$ (1.7) εκτός από ένα σύνολο πρώτων «≤ x» με $\sum\frac{logp}{p}$ =o(logx).

Οπότε εύκολα συμπεραίνεται ότι υπάρχει x' με $\sqrt{x}$<x' <x και θ(x')=Ax' +o(x').

Οπότε πάλι από την (1.6) εναλλάσοντας τα a,A και αντί για x βάλουμε x',έχουμε:

θ($\frac{x'}{p}$)<(α+δ)$\frac{x'}{p}$ (1.8) εκτός από ένα σύνολο πρώτων «≤ x» με $\sum\frac{logp}{p}$ =o(logx).

Από το αποτέλεσμα του Erdos είναι φανερό πως μπορούν να επιλεγούν p και p' σε κάποια από τα εξαιρούμενα σύνολα με

$\frac{x}{p}$<$\frac{x'}{p'}$<(1+δ)$\frac{x}{p}$

Από τις (1.7),(1.8) παίρνουμε ότι

(A−δ)$\frac{x}{p}$<θ($\frac{x}{p}$) ≤θ($\frac{x'}{p'}$)<(α+δ)$\frac{x'}{p'}$<(α+δ)(1+δ)$\frac{x}{p}$

Συνεπώς

(A−δ) <(α+δ)(1+δ) και παίρνοντας δ να τείνει στο μηδέν A≤α.

Αφού A≥α και A+α=2 τότε α=A=1,που αποδεικνύει το θεώρημα.

Για τη συνέχεια θα θεωρήσουμε p,q,r πρώτους,c σταθερές και K θετικές σταθερές,μ(n) θα είναι η συνάρτηση Mobius και τ(n) το πλήθος διαιρετών του n.

4.2 Βασικές σχέσεις

Για x,d θετικούς ακεραίους γράφουμε:

λ_d=$\lambda_{d,x}$ =μ(d)$log^2\frac{x}{d}$ (2.1)

και αν n είναι θετικός ακέραιος

θ_n=$\theta_{n,x}$=$\sum_{d|n}\lambda_d$. (2.2)

Τότε έχουμε,

$$\theta_n=\begin{cases} log^2 x, \gamma\iota\alpha\ n=1 \\ logplog(\frac{x^2}{p}), \gamma\iota\alpha\ n=p^a, a\geq 1 \\ 2logplogq, \gamma\iota\alpha\ n=p^a q^\beta, \alpha\geq 1, \beta\geq 1 \\ 0, \gamma\iota\alpha\ \kappa\acute{\alpha}\theta\varepsilon\ \acute{\alpha}\lambda\lambda\eta\ \pi\varepsilon\rho\acute{\iota}\pi\tau\omega\sigma\eta \end{cases} \quad (2.3)$$

- Για n=1 έχουμε $\sum_{d|1}\lambda_d=\mu(1)log^2\frac{x}{1}=log^2 x$
- Για n=p^a οι μόνοι μη μηδενικοί όροι στο άθροισμα των λ_d είναι αυτοί που αντιστοιχούν σε d=1,p οπότε,

  $\theta_n=log^2 x-\ log^2\frac{x}{p}=log^2 x-(logx-logp)^2=$ logp $log(\frac{x^2}{p})$

- Για n=$p^a q^\beta$ $\theta_n=log^2 x-log^2\frac{x}{p}-log^2\frac{x}{q}-log^2\frac{x}{pq}$ =2log(p)log(q)
- Από τον ορισμό της θ_n προκύπτει $\theta_n=\theta_{n/pk,x}-\theta_{n/pk,x/}$pk.Τώρα θεωρώντας n=$p_1\ldots.p_k$(αλλιώς η μ(d)=0) και με επαγωγή προκύπτει το ζητούμενο.

Έπειτα θεωρούμε τον n ελεύθερο τετραγώνων δηλ.n=$p_1\ldots.p_k$ και παίρνουμε

$\theta_{n,x}=\theta_{n/pk,x}-\theta_{n/pk,x/pk}$.

Ας θεωρήσουμε την παρακάτω σχέση:

$\sum_{n\leq x}\theta_n=\sum_{n\leq x}\sum_{d|n}\lambda_d=\sum_{d\leq x}\lambda_d[\frac{x}{d}]=x\sum_{d\leq x}\lambda_d/d$ + $O(\sum_{d\leq x}|\lambda_d|)=$

$x\sum_{d\leq x}(\mu(d)/d)log^2\frac{x}{d}+O(\sum_{d\leq x}log^2\frac{x}{d})=x\sum_{d\leq x}(\mu(d)/d)log^2\frac{x}{d}+O(x)$. (2.4)

Επιπλέον,

$\sum_{n\leq x}\theta_n=log^2 x+\sum_{p^a\leq x}logplog\frac{x^2}{p}+2\sum_{\substack{p^a q^\beta\leq x\\ p<q}}logplogq=\sum_{p\leq x}log^2 p$

$+\sum_{pq\leq x}logplogq+O(\sum_{p\leq x}logplog\frac{x}{p})$

$+O(\sum_{\substack{p^a\leq x\\ a>1}}log^2 x)+O(\sum_{\substack{p^a q^\beta\leq x\\ a>1}}logplogq)$

$+log^2 x=\sum_{p\leq x}log^2 p+\sum_{pq\leq x}logplogq+O(x)$. (2.5)

Από(4) και (5) συνάγουμε

$\sum_{p\leq x}log^2 p+\sum_{pq\leq x}logplogq=x\sum_{d\leq x}(\mu(d)/d)log^2\frac{x}{d}+O(x)$. (2.6)

Τώρα απομένει να υπολογίσουμε το δεξιό άθροισμα στην (6).Γι' αυτόν τον σκοπό χρειαζόμαστε τον τύπο:

$\sum_{\nu\le z}\frac{1}{\nu}=logz+c_1+O(z^{-1/4})$ (2.7)

και

$\sum_{\nu\le z}\frac{\tau(\nu)}{\nu}=\frac{1}{2}log^2z+c_2logz+c_3+O(z^{1/4})$ (2.7')

Η (2.7') προκύπτει εύκολα απο το γνωστό αποτέλεσμα:

$\sum_{\nu\le z}\tau(\nu)=zlogz+c_4z+O(\sqrt{z})$

Από τις παραπάνω σχέσεις παίρνουμε:

$log^2z=2\sum_{\nu\le z}\frac{\tau(\nu)}{\nu}+c_5\sum_{\nu\le z}\frac{1}{\nu}+c_6+O(z^{1/4})$.

Παίρνοντας z=x/d προκύπτει:

$\sum_{d\le x}(\mu(d)/d)log^2\frac{x}{d}=2\sum_{d\le x}(\mu(d)/d)\sum_{\nu\le x/d}\frac{\tau(\nu)}{\nu}+c_5\sum_{d\le x}(\mu(d)/d)\sum_{\nu\le x/d}\frac{1}{\nu}$

$+c_6\sum_{d\le x}(\mu(d)/d)+O(x^{-1}\sum_{d\le x}d^{\frac{-3}{4}})=2\sum_{d\nu\le x}\frac{\mu(d)\tau(\nu)}{d\nu}$

$+c_5\sum_{d\nu\le x}\frac{\mu(d)}{d\nu}+c_6\sum_{d\le x}(\mu(d)/d)+O(1)$

$=2\sum_{n\le x}\frac{1}{n}\sum_{d|n}\mu(d)\tau(\frac{n}{d})+c_5\sum_{n\le x}\frac{1}{n}\sum_{d|n}\mu(d)+O(1)$

$=2\sum_{n\le x}\frac{1}{n}+c_5+O(1)=2logx+O(1)$.

Χρησιμοποιήσαμε ότι $\sum_{d|n}\mu(d)\tau(\frac{n}{d})=1$ και ότι $\sum_{d\le x}(\mu(d)/d)=O(1)$

Τώρα η (2.6) οδηγεί:

$\sum_{p\le x}log^2p+\sum_{pq\le x}logplogq=2xlogx+O(x)$ (2.8)

Η οποία μπορεί να γραφεί και ως εξής:

$\theta(x)logx+\sum_{p\le x}logp\theta(\frac{x}{p})=2xlogx+O(x)$ (2.9)

Παρατηρώντας ότι, $\sum_{p\le x}log^2p=\theta(x)logx+O(x)$ κι έτσι παίρνουμε

$\sum_{p\le x}logp+\sum_{pq\le x}logplogq\,/logpq=2x+O(\frac{x}{logx})$ (2.10)

Η (2.10) δίνει,

$\sum_{pq\le x}logplogq=\sum_{p\le x}logp\sum_{q\le x/p}logq=2x\sum_{p\le x}logp\,/p-$

$\sum_{p\le x}logp\sum_{qr\le x/p}\frac{logqlogr}{logqr}+O(\sum_{p\le x}\frac{logp}{p(1+log\frac{x}{p})})$

$=2x\log x - \sum_{qr\le x}\frac{\log q\log r}{\log qr}\theta(\frac{x}{qr}) + O(x\log\log x)$.

Χρησιμοποιώντας το παραπάνω στην (2.8) έχουμε:

$\theta(x)\log x=\sum_{pq\le x}\frac{\log p\log q}{\log pq}\theta(\frac{x}{pq}) + O(x\log\log x)$. (2.11)

Γράφοντας τώρα,$\theta(x)=x+R(x)$,η (2.9) μας δίνει

$R(x)\log x= -\sum_{p\le x}\log p\, R\left(\frac{x}{p}\right) + O(x)$. (2.12)

Και με τον ίδιο τρόπο από την (11) προκύπτει,

$R(x)\log x=\sum_{pq\le x}\frac{\log p\log q}{\log pq}R(\frac{x}{pq}) + O(x\log\log x)$. (2.13)

Αφού $\sum_{pq\le x}\frac{\log p\log q}{pq\log pq} = \log x + O(\log\log x)$ το οποίο συνεπάγεται από την

$\sum_{pq\le x}\frac{\log p\log q}{\log pq} = \frac{1}{2}\log^2 x + O(\log x)$ η οποία εύκολα συνάγεται απο την (1.4).

Από τις (2.12),(2.13) προκύπτει,

$2|R(x)|\log x\le \sum_{p\le x}\log p\left|R\left(\frac{x}{p}\right)\right| + \sum_{pq\le x}\frac{\log p\log q}{\log pq}\left|R\left(\frac{x}{pq}\right)\right| + O(x\log\log x)$

Από την παραπάνω σχέση και την (10) παίρνουμε,

$2|R(x)|\log x\le 2\sum_{n\le x}n\{|R(\frac{x}{n}) - \left|R\left(\frac{x}{n+1}\right)\right|\} + O(\sum_{n\le x}\frac{n}{1+\log n}|R(\frac{x}{n}) - \left|R\left(\frac{x}{n+1}\right)\right|) + O(x\log\log x)$

$=2\sum_{n\le x}|R(\frac{x}{n})| + O(\sum_{n\le x}\frac{n}{1+\log n}\{|\theta\left(\frac{x}{n}\right| - \left|\theta\left(\frac{x}{n+1}\right)\right|\}) + O(x\sum_{n\le x}\frac{1}{n(1+\log n)}) + O(x\log\log x)$

$=2\sum_{n\le x}|R(\frac{x}{n})| + O(\sum_{n\le x}\frac{1}{1+\log n}\theta(\frac{x}{n})) + O(x\log\log x)$

$=2\sum_{n\le x}|R(\frac{x}{n})| + O(x\log\log x)$

Άρα, $|R(x)|\le \frac{1}{\log x}\sum_{n\le x}|R(\frac{x}{n})| + O(\frac{x\log\log x}{\log x})$. (2.14)

4.3 Μερικές ιδιότητες της R(x)

Από την (1.4) με μερική άθροιση παίρνουμε:

$$\sum_{n\le x}\frac{\theta(n)}{n^2} = log\text{x} + \text{O}(1) \quad \text{ή} \quad \sum_{n\le x}\frac{R(n)}{n^2} = \text{O}(1)$$

Αυτό σημαίνει ότι υπάρχει θετική σταθερά K_1 τέτοια ώστε για όλα τα x>4 και x'>x να είναι:

$$\left|\sum_{x\le n\le x'}\frac{R(n)}{n^2}\right| < K_1. \quad (3.1)$$

Αν το R(n) δεν μεταβάλλει το πρόσημό του ανάμεσα στο x και το x' τότε υπάρχει ένα y στο διάστημα $[x, x']$ τέτοιο ώστε:

$$\left|\frac{R(y)}{y}\right| < \frac{K_2}{log\frac{x'}{x}},\ K_2 \ge 1. \quad (3.2)$$

Είναι εύκολο να συμπεράνουμε ότι αν το R(n) μεταβάλλει το πρόσημό του διότι τότε θα υπάρχει y ώστε : $|R(y)|<logy$.

Έτσι,για ένα αυθαίρετα εκλεγμένο δ<1 και x>4 θα υπάρχει ένα y στο διάστημα $x \le y \le e^{K_2/\delta}x$,με $|R(y)| < \delta y$. (3.3)

Από την (2.10) βλέπουμε ότι για $y < y'$,

$$0 \le \sum_{y<p\le y'} logp \le 2(y' - y) + \text{O}\left(\frac{y'}{logy'}\right),$$

Από το οποίο συνεπάγεται

$$|R(y') - R(y)| \le y' - y + \text{O}\left(\frac{y'}{logy'}\right)$$

Ως εκ τούτου,αν $y/2 \le y' \le 2y, y > 4$,

$$|R(y') - R(y)| \le |y' - y| + \text{O}\left(\frac{y'}{logy'}\right)$$

ή

$$|R(y')| \le |R(y)| + |y' - y| + \text{O}\left(\frac{y'}{logy'}\right).$$

Τώρα αν θεωρήσουμε ένα διάστημα $(x, e^{K_2/\delta}x)$,σύμφωνα με την (3.3) υπάρχει ένα y σ' αυτό το διάστημα με,

$$|R(y)|<\delta y$$

Έτσι για κάθε y' για το οποίο ισχύει $y/2 \leq y' \leq 2y$ έχουμε:

$|R(y')| \leq \delta y + |y' - y| + \frac{K_3 y'}{\log x}$

ή $\left|\frac{R(y')}{y'}\right| < 2\delta + \left|1 - \frac{y'}{y}\right| + \frac{K_3}{\log x}$.

Αν $x > e^{K_2/\delta}$ και $e^{-\delta/2} cy'/y \leq e^{\delta/2}$ παίρνουμε:

$\left|\frac{R(y')}{y'}\right| < 2\delta + (e^{\delta/2} - 1) + \delta < 4\delta$.

Οπότε για $x > e^{K_2/\delta}$ το διάστημα $(x, e^{K_2/\delta}x)$ θα περιέχει ένα υποδιάστημα $(y_1, e^{\delta/2}y_1)$,ώστε $|R(z)| < 4\delta z$ αν το z ανήκει σ' αυτό το υποδιάστημα.

4.4 Απόδειξη του θεωρήματος των πρώτων αριθμών

Σ' αυτήν την παράγραφο θ' αποδείξουμε ότι :

$$\lim_{x\to\infty} \frac{\theta(x)}{x} = 1 .$$

Η παραπάνω σχέση είναι ισοδύναμη με την,

$$\lim_{x\to\infty} \frac{R(x)}{x} = 0. \quad (4.1)$$

Ξέρουμε ότι $\psi(x)=O(x)$.Αυτό σημαίνει πως για $x > 1$, $|R(x)| < K_4 x$ (4.2)

Υποθέτουμε τώρα ότι για κάποιον θετικό $a<8$ $|R(x)| < ax$ (4.3)

το οποίο αληθεύει για $x > x_0 > e^{K_2/\delta}$.Θέτοντας τώρα $\delta = a/8$ έχουμε από την προηγούμενη παράγραφο ότι τα διαστήματα της μορφής $(x, e^{K_2/\delta}x)$ περιέχουν ένα διάστημα $(y, e^{\delta/2} y)$ με,

$|R(z)| < az/2$ (4.4) για $y \leq z \leq e^{\delta/2} y$.

Η ανισότητα (2.14) χρησιμοποιώντας την (4.2) δίνει:

$$|R(x)| \leq \frac{1}{\log x}\sum_{n\leq x} \left|R\left(\frac{x}{n}\right)\right| + O\left(\frac{x}{\sqrt{\log x}}\right)$$

$$< K_4 \frac{x}{\log x}\sum_{\left(\frac{x}{x_0}\right)<n\leq x} \frac{1}{n} + \frac{x}{\log x}\sum_{n\leq\left(\frac{x}{x_0}\right)} \frac{1}{n}\left|\frac{n}{x} R\left(\frac{x}{n}\right)\right| + O\left(\frac{x}{\sqrt{\log x}}\right).$$

Γράφοντας τώρα ρ=$e^{K_2/\delta}$ και χρησιμοποιώντας τις (4.3) και (4.4.)

| R(x) | <$\frac{ax}{logx}\sum_{n\le(\frac{x}{xo})}\frac{1}{n}-\frac{ax}{2logx}\sum_{1\le v\le(\log(\frac{x}{xo})/log\rho)}\sum_{\substack{y_v\le n\le y_v e^{\frac{\delta}{2}}\\ \rho^{v-1}<y_v\le\rho^v e^{-(\frac{\delta}{2})}}}\frac{1}{n}$ + O($\frac{x}{\sqrt{logx}}$)=ax –

$\frac{ax}{2logx}\sum_{1\le v\le(\log(\frac{x}{xo})/log\rho)}\delta/2$ + O($\frac{x}{\sqrt{logx}}$)=$ax-\frac{a\delta}{4log\rho}$x + O($\frac{x}{\sqrt{logx}}$)=

$a(1-\frac{a^2}{256K_2})$ + O($\frac{x}{\sqrt{logx}}$) < $a(1-\frac{a^2}{300K_2})x$,για x>x_1.

Επαναλαμβάνοντας τη διαδικασία παίρνουμε:

a_{n+1}=$a_n(1-\frac{a_n^2}{300K_2})$.

Προφανώς αυτή η ακολουθία συγκλίνει στο μηδέν αν για παράδειγμα έχουμε a_1=4 (εύκολα δείχνουμε πως a_n<$K_5\sqrt{n}$).Αυτό αποδεικνύει το (4.1) και συνεπώς το ζητούμενο.

Σχόλιο:Είναι φανερό πως δεν έχουμε χρησιμοποιήσει την πλήρη έκφραση της (2.8).Θα μπορούσαμε να έχουμε χρησιμοποιήσει αντί για O(x) το o($xlog$x).#

Παράρτημα

A) Ο συμβλισμός Landau

Στο Α) μέρος του παραρτήματος θα αναφέρουμε σύντομα τον ορισμό και τις ιδιότητες των συμβόλων «Ο» και «ο» που ονομάζοντα αντίστοιχα με μεγάλο και μικρό όμικρον του Landau.

Α1) Το μεγάλο Ο του Landau

Έστω a ένας οποιοσδήποτε πραγματικός αριθμός(ακόμα και τα $\pm\infty$).Έστω συναρτήσεις $f(x)$,g(x) που ορίζονται σε κάποια γειτονιά του a και θεωρούμε ότι η g(x) είναι θετική συνάρτηση.Λέμε ότι η f(x) είναι το μεγάλο Ο της g(x) και γράφουμε:

$f(x)=O(g(x))$, αν υπάρχει σταθερά K>0 και μια γειτονιά του N(a) του a τέτοια ώστε,

$|f(x)| \leq Kg(x)$, $\forall x \in N(a)$.

Με τον όρο γειτονιά του a εννοούμε κάθε σύνολο N(a) που περιέχει ένα ανοικτό διάστημα (a-ε,a+ε).Με τον όρο γειτονιά του +∞ εννοούμε κάθε σύνολο N(+∞) που περιέχει ένα διάστημα (M, +∞) και τέλος με τον όρο γειτονιά του -∞ εννοούμε κάθε σύνολο N(-∞) που περιέχει ένα διάστημα της μορφής $(-\infty, -m)$.

Παραδείγματα:

i) Έστω a=0,τότε

$\sin x=O(x)$, $x^3=O(x^2)$

ii) Έστω a=+∞,τότε

$\sin x=O(1)$, $x=O(x^2)$

Ιδιότητες:

i)Αν $f_i(x)=O(g_i(x))$,τότε

$$f_1(x) + f_2(x) = O(g_1(x) + g_2(x))$$

$$f_1(x)f_2(x) = O(g_1(x)g_2(x))$$

ii)Αν c είναι μια σταθερά και $f(x)=O(g(x))$ τότε $c f(x)=O(g(x))$.

Απόδειξη: i)

$$|f_1(x) + f_2(x)| \leq |f_1(x)| + |f_2(x)| \leq K_1 g_1(x) + K_2 g_2(x)$$

ii) $|c f(x)| \leq kcg(x) \leq Kg(x)$

Η παράσταση αυτή μπορεί να χρησιμοποιηθεί επίσης γι' ακολουθίες που μπορεί να είναι ακολουθίες είτε πραγματικές είτε μιγαδικές.Για παράδειγμα η σχέση $f(n)\in O(g(n))$ δηλώνει ότι υπάρχει μια σταθερά K κι ένας N_o τέτοια ώστε,αν $n>N_o$:

$$|f(n)| \leq Kg(n).$$

Πολλές φορές συμβολίζουμε το $f(n)\in O(g(n))$ ως $f(n)=O(g(n))$,π.χ. $10n^3 + 10^{-5}n^3 log n = O(n^3 log n)=O(n^4)$.

Α2) Το μικρό ο του Landau

Έστω συναρτήσεις $f(x)$,g(x) που ορίζονται σε κάποια γειτονιά του a και θεωρούμε ότι η g(x) είναι θετική συνάρτηση.Λέμε ότι η $f(x)$ είναι το μικρό ο της g(x) και γράφουμε:

$$f(x)=o(g(x)) \quad \text{αν } \lim_{n\to\infty} \frac{f(n)}{g(n)} = 0.$$

Εύκολα αποδεικνύεται πως αν $f_i(x)=o(g_i(x))$,τότε

$$f_1(x)f_2(x)=o(g_1(x)g_2(x))$$

Α3) Ο ασυμπτωτικός συμβολισμός "∼"

Έστω δύο συναρτήσεις f(x),g(x) θα λέμε πως η f είναι ασυμπτωτική στη g και γράφουμε:

$$f \sim \text{g (όταν το } x \to \infty) \text{ , αν } \lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$$

Ο ορσιμός εφαρμόζεται σε συναρτήσεις πραγματικής ή μιγαδικής μεταβλητής καθώς και σε ακολουθίες.Η σχέση είναι συμμετρική και μεταβατική.

Β) Γενικευμένες συνελίξεις

Σε αυτό το μέρος του παραρτήματος θα αναφερθούμε σύντομα στις γενικευμένες συνελίξεις.Θα συμβολίζουμε με F μια συνάρτηση με πραγματικές ή μιγαδικές μεταβλητές τιμές,που είναι ορισμένη πάνω στο θετικό πραγματικό άξονα (0,∞) και με την ιδιότητα F(x)=0,για 0<x<1.Στα αθροίσματα της μορφής

$\sum_{n\le x} a(n)F(\frac{x}{n})$,θεωρούμε πως το a είνα οποιαδήποτε αριθμητική συνάρτηση.Το προηγούμενο άθροισμα ορίζει πάνω στο (0,∞) μια νέα συνάρτηση G που επίσης μηδενίζεται για 0<x<1.Αυτή τη συνάρτηση G θα τη συμβολίζουμε με a ∘ F.Έτσι,

(a ∘ F)(x)= $\sum_{n\le x} a(n)F(\frac{x}{n})$.

Αν F(x)=0 για κάθε μη ακέραιο x,τότε ο περιορισμός της F πάνω στους ακεραίους είναι μια αριθμητική συνάρτηση και ισχύει:

(a ∘ F)(m)=(a∗F)(m) για κάθε ακέραιο m≥1,συνεπώς η πράξη ∘ μπορεί να θεωρηθεί σαν μία γενίκευση της κατά Dirichlet συνέλιξης ∗.

Η πράξη ∘ γενικά δεν είναι ούτε μεταθετική ούτε προσεταιριστική.Όμως το ακόλουθο θεώρημα χρησιμεύει σαν «υποκατάστατο» του προσεταιριστικού νόμου.

Θεώρημα Β1:Για οποιεσδήποτε αριθμητικές συναρτήσεις α,β ισχύει:

α ∘ (β ∘ F)=(α∗β) ∘ F.

Απόδειξη: Για x>0 είναι :

{ α ∘ (β ∘ F)}(x)= $\sum_{n\le x} a(n) \sum_{m\le x/n} \beta(m)F(\frac{x}{mn})=\sum_{mn\le x} a(n)\beta(m)F(\frac{x}{mn})=$

$\sum_{k\le x}(\sum_{n|k} a(n)\beta(\frac{k}{n}))F(\frac{x}{k})=\sum_{k\le x}(a*\beta)(k)F(\frac{x}{k})=$

{(α∗β) ∘ F}(x).#

Έπειτα παρατηρούμε ότι η ταυτοτική συνάρτηση I(n)=[1/n] για την κατά Dirichlet συνέλιξη είναι,επίσης, μια από τ' αριστερά «μονάδα» για την πράξη ∘ ,δηλαδή ισχύει

(I ∘ F)(x)=$\sum_{n\le x}\left[\frac{1}{n}\right]F\left(\frac{x}{n}\right)=F(x)$ για κάθε x.

Αν χρησιμοποιήσουμε αυτό το γεγονός μαζί με την προσεταιριστική ιδιότητα μπορούμε ν'αποδείξουμε τον ακόλουθο τύπο αντιστροφής.

Θεώρημα Β2 (Γενικευμένος τύπος αντιστροφής):Αν η α έχει κατά Dirichlet αντίστροφη α^{-1},τότε η εξίσωση

G(x)= $\sum_{n\le x} a(n)F\left(\frac{x}{n}\right)$ (1)

συνεπάγεται την

F(x)= $\sum_{n\le x} a^{-1}(n)G\left(\frac{x}{n}\right)$ (2)

και αντίστροφα.

Απόδειξη: Αν G=α ∘ F,τότε

α^{-1} ∘ G= α^{-1} ∘ (α ∘ F)=(α^{-1} ∗α) ∘ F=I ∘ F=F.

Έτσι η (1) συνεπάγεται την (2) και με παρόμοιο τρόπο λαμβάνουμε και το αντίστροφο.

Θεώρημα Β3 (Γενικευμένος τύπος αντιστροφής του Mobius): Αν η α είναι πλήρως πολλαπλασιαστική τότε έχουμε,

G(x)= $\sum_{n\le x} a(n)F\left(\frac{x}{n}\right)$

αν και μόνο αν

F(x)= $\sum_{n\le x} \mu(n)a(n)G\left(\frac{x}{n}\right)$

Απόδειξη: Αν στην σχέση (2) του θεωρήματος Β2) το α^{-1}(n) το αντικαταστήσουμε με $\mu(n)a(n)$ προκύπτει το ζητούμενο.

Γ)Ο ασυμτωτικός τύπος του Selberg

Έστω F μια συνάρτηση με πραγματικές τιμές ορισμένη πάνω στο διάστημα $(0,\infty)$ και έστω G(x)=logx$\sum_{n\le x} F(x/n)$.Τότε ισχύει,

F(x)logx + $\sum_{n\le x} F(x/n)\,\Lambda(n)$=$\sum_{d\le x}\mu(d)G(x/d)$.

Απόδειξη:Κατ' αρχήν γράφουμε την F(x)logx ως άθροισμα,δηλ.

F(x)logx=$\sum_{n\le x}[\frac{1}{n}]F(\frac{x}{n})log\frac{x}{n}=\sum_{n\le x}F(\frac{x}{n})log\frac{x}{n}\sum_{d|n}\mu(d)$. (*)

Τώρα χρησιμοποιώντας το θεώρημα (2.11) έχουμε:

$\sum_{n\le x} F(x/n)\,\Lambda(n) = \sum_{n\le x} F(\frac{x}{n})\sum_{d|n}\mu(d)\,log(n/d)$ (**).

Με πρόσθεση των (*) και (**) προκύπτει,

F(x)logx +$\sum_{n\le x} F(x/n)\,\Lambda(n) = \sum_{n\le x} F(\frac{x}{n})\sum_{d|n}\mu(d)\{log(n/d) + log(x/n)\}$=

$\sum_{n\le x}\ \sum_{d|n} F(\frac{x}{n})\mu(d)log\frac{x}{d}$.

Στο παραπάνω άθροισμα παίρνοντας n=qd προκύπτει:

$\sum_{n\le x}\ \sum_{d|n} F(\frac{x}{n})\mu(d)log\frac{x}{d}=\sum_{d|n}\mu(d)\,log(x/d)\sum_{q\le x/d}F(\frac{x}{qd})=\sum_{d\le x}\mu(d)G(x/d)$.#

Εφαρμόζοντας το παραπάνω για την F_1(x)=ψ(x) και έπειτα για την F_2(x)=x−C−1,όπου C είναι η σταθερά του Euler έχουμε για την F_1(x),

G_1(x)=logx$\sum_{n\le x}\psi(\frac{x}{n})$=x$log^2$x –x$log$x +O($log^2$x) και αντίστοιχα

G_2(x)=logx$\sum_{n\le x}(\frac{x}{n}-C-1)$=x$log$x$\sum_{n\le x}\frac{1}{n}-(C+1)logx\sum_{n\le x}1$=

xlogx(logx +C+O(1/x)) − (C+1)logx(x+O(1))=xlog^2x – xlogx+O(logx).

Όμως G_1(x)−G_2(x)=O(log^2x).Στην πραγματικότητα θα χρησιμοποιήσουμε την ασθενέστερη εκτίμηση O($\sqrt{x}$).

Τώρα εφαρμόζοντας το 1ο θεώρημα στις F_1(x), F_2(x) η διαφορά των δεξιών μελών δίνει:

$\sum_{d\le x}\mu(d)\{G_1(\frac{x}{d})-G_2(\frac{x}{d})\}$=O($\sum_{d\le x}\sqrt{\frac{x}{d}}$)=O($\sqrt{x}\sum_{d\le x}\frac{1}{\sqrt{d}}$)=O(x).Οπότε έχουμε,

{ψ(x)−(x−C−1)}logx +$\sum_{n\le x}\{\psi(\frac{x}{n})-(\frac{x}{n}-C-1)\}\Lambda$(n)=O(x),και με βάση τη σχέση $\sum_{n\le x}\frac{\Lambda(n)}{n}=log$x =O(1)

προκύπτει,

$\psi(x)log x + \sum_{n\leq x}\psi(\frac{x}{n})\Lambda(n) = (x-C-1)log x + \sum_{n\leq x}(\frac{x}{n}-C-1)\Lambda(n) + O(x) = 2x log x + O(x)$.

Βιβλιογραφία

[1] Tom M. Apostol,*Introduction to analytic number theory,*Springer-Verlag.

[2] G.H.Hardy,Edward M. Wright,*An introduction to the theory of numbers,*Oxford University Press.

[3] Victor Shoup,*Μια υπολογιστική εισαγωγή στη θεωρία αριθμών και την άλγεβρα,*Κλειδάριθμος.

[4] Liang-Shin Hahn,Bernard Epstein,*Classical Complex Analysis*,Jones and Bartlett Publishers.

[5] J.Bak,D.J.Newman,*Complex analysis*,Springer-Verlag

[6] Atle Selberg, *An Elementary Proof of the Prime-Number Theorem*, Annals of Mathematics, Second Series, Vol. 50, No. 2 (Apr., 1949), pp. 305-313
[7] Theodore J. Yoder, *An Introduction to the Riemann Hypothesis*.

[8] Tom M. Apostol,*What is the most surprising*,Math Horizons February 1997,page 26-31.

[9] D. Goldfeld,*The elementary proof of the prime number theorem: An historical perspective.*

[10] Jerome Baltzersen, *Hardy's theorem and the prime number theorem*, Thesis for Bachelor of Science in Mathematics. Department of Mathematical Sciences, University of Copenhagen.

[11] Jake Koenig,*An elementary proof of the prime number theorem,* http://math.uchicago.edu/~may/REU2013/REUPapers/Koenig.pdf

[12] A Primer of Analytic Number Theory: From Pythagoras to Riemann,*Jeffrey Stopple*,Cambridge University Press

[13] Στάθης Ζάχος,*Υπολογιστική Θεωρία Αριθμών και Κρυπτογραφία*

[14] Παναγιώτης Τσαγκάρης,*Θεωρία Αριθμών,*Εκδόσεις Συμμετρία
[15] Stephen Lucas,*A direct proof of the Prime Number Theorem*,James Madison University