Αναλυτική Θεωρία Αριθμών

Πρόχειρες Σημειώσεις

Τμήμα Μαθηματικών
Πανεπιστήμιο Αθηνών
Αθήνα, 2022

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1

Το θεμελιώδες θεώρημα της Αριθμητικής

1.1 Αρχή του ελαχίστου και μαθηματική επαγωγή

Συμβολίζουμε με

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$$

το σύνολο των ακεραίων και με

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

το σύνολο των θετικών ακεραίων (των φυσικών αριθμών). Γράφουμε επίσης $\mathbb{Z}^+ = \mathbb{N} \cup \{0\}$ για το σύνολο των μη αρνητικών ακεραίων. Η αρχή του ελαχίστου, γνωστή και ως αρχή της καλής διάταξης, ισχυρίζεται ότι υπάρχει κάποιος ελάχιστος ακέραιος σε κάθε μη κενό υποσύνολο των μη αρνητικών ακεραίων. Μας βοηθάει να αποδείξουμε το ακόλουθο αποτέλεσμα.

Θεώρημα 1.1.1. *Έστω $S(1), S(2), \ldots, S(n), \ldots$ προτάσεις, μία για κάθε ακέραιο $n \geqslant 1$. Αν κάποια από τις προτάσεις είναι ψευδής, τότε υπάρχει κάποια ψευδής πρόταση που είναι η πρώτη με αυτήν την ιδιότητα.*

Απόδειξη. Ορίζουμε

$$T = \{k \in \mathbb{N} : \text{ η } S(k) \text{ είναι ψευδής}\}.$$

Αφού τουλάχιστον μία από τις προτάσεις είναι ψευδής, το T είναι μη κενό. Από την αρχή του ελαχίστου, υπάρχει ένας ελάχιστος ακέραιος n στο T. Αυτό σημαίνει ότι η $S(n)$ είναι η πρώτη ψευδής πρόταση. □

Από το Θεώρημα 1.1.1 παίρνουμε την αρχή της μαθηματικής επαγωγής.

Θεώρημα 1.1.2. *Έστω $S(n)$ προτάσεις, μία για κάθε $n \geqslant 1$. Υποθέτουμε ότι οι παρακάτω συνθήκες ικανοποιούνται από τις $S(n)$:*

(α) *Η πρόταση $S(1)$ είναι αληθής.*

(β) *Αν η $S(n)$ είναι αληθής, τότε η $S(n+1)$ είναι αληθής.*

Τότε η $S(n)$ είναι αληθής για όλους τους ακεραίους $n \geqslant 1$.

Απόδειξη. Υποθέτουμε ότι η $S(n)$ δεν είναι αληθής για όλους τους ακεραίους $n \geqslant 1$. Τότε, υπάρχει κάποιος θετικός ακέραιος $k \geqslant 1$ τέτοιος ώστε η $S(k)$ να είναι ψευδής. Από το Θεώρημα 1.1.1 υπάρχει κάποια πρώτη ψευδής πρόταση, ας πούμε η $S(m)$. Από το γεγονός ότι η $S(1)$ ισχύει, συμπεραίνουμε ότι $m \neq 1$. Επιπλέον, από το γεγονός ότι ο m είναι ελάχιστος, παρατηρούμε ότι η $S(j)$ αληθεύει για $1 \leqslant j \leqslant m-1$. Τώρα, από το (β), αφού η $S(m-1)$ είναι αληθής έχουμε ότι η $S(m)$ είναι αληθής. Αυτό έρχεται σε αντίφαση με την υπόθεση ότι η $S(m)$ είναι ψευδής, και συμπεραίνουμε ότι η $S(n)$ είναι αληθής για κάθε θετικό ακέραιο $n \geqslant 1$. □

Στο Θεώρημα 1.1.2 (α) μπορούμε να αντικαταστήσουμε τον 1 με οποιονδήποτε ακέραιο m. Με άλλα λόγια, μπορούμε να τροποποιήσουμε το Θεώρημα 1.1.2 ως εξής:

Θεώρημα 1.1.3. *Έστω m ένας ακέραιος. Έστω $S(n)$ προτάσεις, μία για κάθε $n \geqslant m$. Υποθέτουμε ότι οι παρακάτω συνθήκες ικανοποιούνται από τις $S(n)$:*

(α) *Η πρόταση $S(m)$ είναι αληθής.*

(β) *Αν $n \geqslant m$ και η $S(n)$ είναι αληθής, τότε η $S(n+1)$ είναι αληθής.*

Τότε η $S(n)$ είναι αληθής για όλους τους ακεραίους $n \geqslant m$.

Ολοκληρώνουμε αυτήν την ενότητα με μία ακόμα εκδοχή της αρχής της μαθηματικής επαγωγής. Η απόδειξη αυτής της εκδοχής είναι όμοια με την απόδειξη του Θεωρήματος 1.1.2 και την αφήνουμε ως άσκηση για τους αναγνώστες.

Θεώρημα 1.1.4. *Έστω m ένας ακέραιος. Έστω $S(n)$ προτάσεις, μία για κάθε $n \geqslant m$. Υποθέτουμε ότι οι παρακάτω συνθήκες ικανοποιούνται από τις $S(n)$:*

(α) *Η πρόταση $S(m)$ είναι αληθής.*

(β) *Αν $n \geqslant m$ και η $S(k)$ είναι αληθής για κάθε $m \leqslant k \leqslant n$, τότε η $S(n+1)$ είναι αληθής.*

Τότε η $S(n)$ είναι αληθής για όλους τους ακεραίους $n \geqslant m$.

1.2 Αλγόριθμος της διαίρεσης

Θεώρημα 1.2.1 (αλγόριθμος της διαίρεσης)**.** *Έστω a και b ακέραιοι τέτοιοι ώστε $b > 0$. Τότε υπάρχουν μοναδικοί ακέραιοι q και r τέτοιοι ώστε*

$$a = bq + r \quad \textit{και} \quad 0 \leqslant r < b.$$

Απόδειξη. Ορίζουμε

$$S = \{y : y = a - bx,\ \ x \in \mathbb{Z} \text{ και } y \geqslant 0\}.$$

Παρατηρώντας ότι

$$a - b(-|a|) = a + b|a| \geqslant 0,$$

βλέπουμε ότι

$$a + b|a| \in S,$$

και συμπεραίνουμε ότι το S είναι μη κενό. Από την αρχή του ελαχίστου, το S περιέχει έναν ελάχιστο μη αρνητικό ακέραιο, τον οποίο συμβολίζουμε με r. Παρατηρούμε ότι, αφού $r \in S$,

$$r = a - bq,$$

για κάποιον ακέραιο q. Συνεπώς, έχουμε ότι

$$a = bq + r \quad \text{και} \quad r \geqslant 0.$$

Δείχνουμε τώρα ότι $r < b$. Ας υποθέσουμε ότι $r \geqslant b$. Τότε

$$r - b \geqslant 0 \quad \text{και} \quad r - b = a - b(q + 1).$$

Αυτό συνεπάγεται ότι

$$r - b \in S.$$

Από την υπόθεση, $b > 0$ και συνεπώς $r - b < r$. Άρα, έχουμε βρει έναν μη αρνητικό ακέραιο $r - b$ ο οποίος ανήκει στο S και είναι μικρότερος από τον r. Αυτό έρχεται σε αντίφαση με το γεγονός ότι ο r ήταν ελάχιστος. Έτσι συμπεραίνουμε ότι $r < b$.

Τέλος, δείχνουμε ότι οι ακέραιοι q και r είναι μοναδικοί. Θεωρούμε τυχούσα αναπαράσταση της μορφής $a = bq' + r'$, όπου $q', r' \in \mathbb{Z}$ και $0 \leqslant r' < b$, και θα δείξουμε ότι $q = q'$ και $r = r'$. Έστω ότι $q \neq q'$. Τότε $|q - q'| \geqslant 1$ και από την

$$b(q' - q) = r - r' \tag{1.2.1}$$

συμπεραίνουμε ότι $|r - r'| = b|q - q'| \geqslant b$. Από την άλλη πλευρά, έχουμε $r, r' \in [0, b)$, συνεπώς $|r - r'| < b$, το οποίο είναι άτοπο. Με άλλα λόγια, $q = q'$ και από την (1.2.1), $r = r'$. □

Παρατήρηση 1.2.2. Κατάλληλη εκδοχή του αλγόριθμου της διαίρεσης του Θεωρήματος 1.2.1 ισχύει επίσης όταν $b < 0$. Για παράδειγμα, αποδείξτε ότι αν $a, b \in \mathbb{Z}$ και $b \neq 0$ τότε υπάρχουν μοναδικοί ακέραιοι q και r τέτοιοι ώστε $a = bq + r$ και $0 \leqslant r < |b|$.

Όταν $r = 0$ στο Θεώρημα 1.2.1, τότε έχουμε $a = bq$ και λέμε ότι ο b διαιρεί τον a.

Ορισμός 1.2.3. Αν ένας ακέραιος b διαιρεί τον a, λέμε ότι ο b είναι διαιρέτης του a και ότι ο a είναι πολλαπλάσιο του b. Ο συμβολισμός για την πρόταση «ο b διαιρεί τον a» είναι

$$b \mid a.$$

Αν ο b δεν διαιρεί τον a τότε γράφουμε $b \nmid a$.

Ορισμός 1.2.4. Λέμε ότι ένας θετικός ακέραιος $p > 1$ είναι πρώτος αν έχει ακριβώς δύο θετικούς διαιρέτες, τον 1 και τον εαυτό του.

Διατυπώνουμε τώρα κάποιες στοιχειώδεις ιδιότητες της διαιρετότητας.

Θεώρημα 1.2.5. *Έστω a, b, d, k, m και n ακέραιοι, οι οποίοι μπορεί να είναι θετικοί, αρνητικοί ή μηδέν. Τότε ισχύουν τα ακόλουθα:*

(α) *Αν* $k \neq 0$ *τότε* $k \mid k$.

(β) *Αν* $d \mid n$ *και* $n \mid m$, *τότε* $d \mid m$.

(γ) *Αν* $d \mid n$ *και* $d \mid m$, *τότε* $d \mid (an + bm)$.

(δ) *Αν* $d \mid n$, *τότε* $ad \mid an$.

(ε) *Αν* $ad \mid an$ *και* $a \neq 0$, *τότε* $d \mid n$.

(στ) *Για κάθε ακέραιο* k *ισχύει* $1 \mid k$.

(ζ) *Για κάθε ακέραιο* k *ισχύει* $k \mid 0$. *Αν* $0 \mid k$ *τότε* $k = 0$.

(η) *Αν* $n \neq 0$ *και* $d \mid n$ *τότε* $|d| \leqslant |n|$.

(ϑ) *Αν* $d \mid n$ *και* $n \mid d$, *τότε* $|d| = |n|$.

(ι) *Αν* $d \neq 0$ *και* $d \mid n$, *τότε* $\frac{n}{d} \mid n$.

Απόδειξη. Θα αποδείξουμε το (γ) και θα αφήσουμε την απόδειξη των υπόλοιπων ισχυρισμών ως άσκηση. Αφού $d \mid n$, έχουμε ότι $n = ds$ για κάποιον ακέραιο s. Όμοια, η $d \mid m$ συνεπάγεται ότι $m = dt$ για κάποιον ακέραιο t. Τώρα,

$$an + bm = ads + bdt = d(as + bt).$$

Αυτό δείχνει ότι $d \mid (an + bm)$ για κάθε ζεύγος ακεραίων a και b. □

Από το Θεώρημα 1.2.5 (ι) βλέπουμε ότι αν ο $d \neq 0$ είναι διαιρέτης του n τότε ο n/d είναι επίσης διαιρέτης του n. Ο διαιρέτης n/d λέγεται συζυγής διαιρέτης του d.

1.3 Μέγιστος κοινός διαιρέτης

Ορισμός 1.3.1. Κοινός διαιρέτης των ακεραίων a και b είναι κάθε ακέραιος c τέτοιος ώστε $c \mid a$ και $c \mid b$.

Ορισμός 1.3.2. Μέγιστος κοινός διαιρέτης των ακεραίων a και b είναι ένας ακέραιος d με τις ακόλουθες ιδιότητες:

(α) Ο d είναι μη αρνητικός.

(β) Ο d είναι κοινός διαιρέτης των a και b.

(γ) Αν e είναι ένας κοινός διαιρέτης των a και b, τότε $e \mid d$.

Σημειώνουμε ότι αν οι d και d' είναι και οι δύο μέγιστοι κοινοί διαιρέτες των a και b, τότε ο d είναι κοινός διαιρέτης των a και b και ο d' είναι μέγιστος κοινός διαιρέτης των a και b, άρα $d' \mid d$ από τον Ορισμό 1.3.2 (γ). Όμοια, αφού ο d' είναι κοινός διαιρέτης των a και b και ο d είναι μέγιστος κοινός διαιρέτης των a και b, έχουμε $d \mid d'$. Από το Θεώρημα 1.2.5 (ϑ) έχουμε $|d| = |d'|$, και από τον Ορισμό 1.3.2 (α) συμπεραίνουμε ότι $d = d'$. Αυτό δείχνει ότι, αν υπάρχει, ο μέγιστος κοινός διαιρέτης των a και b ορίζεται μονοσήμαντα.

Ο συμβολισμός για τον μέγιστο κοινό διαιρέτη των a και b είναι

$$(a, b).$$

Παρατήρηση 1.3.3. Όταν οι a και b είναι ίσοι με 0, τότε $(0, 0) = 0$ (παρατηρήστε ότι ο 0 ικανοποιεί τα (α), (β) και (γ) του ορισμού που δώσαμε). Αν $a = 0$ και ο b είναι μη μηδενικός, τότε $(0, b) = (b, 0) = |b|$.

Στη συνέχεια δείχνουμε ότι ο μέγιστος κοινός διαιρέτης δύο ακεραίων υπάρχει. Από την Παρατήρηση 1.3.3, αρκεί να θεωρήσουμε την περίπτωση που οι a και b είναι και οι δύο μη μηδενικοί.

Θεώρημα 1.3.4. *Έστω a και b μη μηδενικοί ακέραιοι. Τότε, ο μικρότερος θετικός ακέραιος στο σύνολο*

$$P := \{sa + tb : s, t \in \mathbb{Z} \text{ και } sa + tb > 0\}$$

είναι ο (a, b).

Απόδειξη. Αν ο a είναι θετικός, τότε $a \in P$ αφού

$$a = 1 \cdot a + 0 \cdot b.$$

Όμοια, αν ο b είναι θετικός, τότε $b \in P$. Υποθέτουμε ότι οι a και b είναι και οι δύο αρνητικοί. Τότε $0 \cdot a + (-1) \cdot b \in P$. Άρα το P είναι μη κενό. Από την αρχή του ελαχίστου, υπάρχει κάποιος ελάχιστος θετικός ακέραιος, ας τον πούμε d, στο P. Στόχος μας είναι να δείξουμε ότι

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

Αφού $d \in P$, έχουμε

$$d = xa + yb \tag{1.3.1}$$

για κάποιους ακεραίους $x, y \in \mathbb{Z}$. Δείχνουμε πρώτα ότι ο d είναι κοινός διαιρέτης των a και b.

Από το Θεώρημα 1.2.1, μπορούμε να υποθέσουμε ότι

$$a = dq + r, \qquad 0 \leqslant r < d.$$

Έστω ότι $r > 0$. Τότε, αφού

$$r = a - dq = a - (xaq + ybq) = a(1 - xq) + b(-yq)$$

έχουμε $r \in P$ και ο r είναι μικρότερος από τον d. Όμως ο d είναι ο μικρότερος ακέραιος στο P, δηλαδή καταλήγουμε σε άτοπο. Άρα, $r = 0$. Με άλλα λόγια, $d \mid a$. Με παρόμοιο επιχείρημα, αντικαθιστώντας τον a με τον b, συμπεραίνουμε ότι $d \mid b$. Αυτό δείχνει ότι ο d είναι κοινός διαιρέτης των a και b.

Τώρα, παρατηρούμε ότι αφού $d \in P$ έχουμε $d > 0$. Επιπλέον, αν $c \mid a$ και $c \mid b$ τότε $a = cu$ και $b = cv$. Αυτό συνεπάγεται, από την (1.3.1), ότι

$$d = xa + yb = c(ux + vy),$$

άρα $c \mid d$. Αυτό δείχνει ότι ο d ικανοποιεί τις συνθήκες στον Ορισμό 1.3.2 και συμπεραίνουμε ότι $d = (a, b)$. □

Η ταυτότητα (1.3.1) θα χρησιμοποιείται συχνά και την καταγράφουμε ως εξής.

Πόρισμα 1.3.5. *Έστω a και b ακέραιοι. Τότε, υπάρχουν ακέραιοι x και y τέτοιοι ώστε*

$$(a, b) = ax + by.$$

Ορισμός 1.3.6. Λέμε ότι δύο ακέραιοι a και b είναι σχετικώς πρώτοι αν

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

Θεώρημα 1.3.7. *Έστω a και b μη μηδενικοί ακέραιοι. Τότε, $(a, b) = 1$ αν και μόνο αν $1 = ax+by$ για κάποιους ακεραίους x και y.*

Απόδειξη. Παρατηρούμε ότι αν $(a, b) = 1$ τότε, από το Πόρισμα 1.3.5,

$$1 = ax + by$$

για κάποιους ακεραίους x και y.

Αντίστροφα, αν

$$1 = ax + by,$$

τότε $(a, b) \mid a$ και $(a, b) \mid b$, συνεπώς $(a, b) \mid 1$. Αυτό συνεπάγεται ότι $(a, b) = 1$. □

Καταγράφουμε τώρα κάποιες βασικές ιδιότητες του μέγιστου κοινού διαιρέτη δύο ακεραίων.

Θεώρημα 1.3.8. *Έστω a, b και c μη μηδενικοί ακέραιοι. Τότε:*

(α) $(a, b) = (b, a)$.

(β) $(a, (b, c)) = ((a, b), c)$.

(γ) $(ac, bc) = |c|(a, b)$.

Απόδειξη. Θα αποδείξουμε μόνο το (γ) και θα αφήσουμε την απόδειξη των υπόλοιπων ισχυρισμών ως άσκηση. Θέτουμε $d = (ac, bc)$ και $d' = |c|(a, b)$. Από το Πόρισμα 1.3.5,

$$d = acx + bcy$$

για κάποιους ακεραίους x και y. Άρα,

$$d = \frac{c}{|c|}(a \cdot |c| \cdot x + b \cdot |c| \cdot y). \tag{1.3.2}$$

Τώρα, $d' = |c|(a, b)$ και αφού $(a, b) \mid a$ και $(a, b) \mid b$ βλέπουμε ότι ο d' είναι κοινός διαιρέτης των $a \cdot |c|$ και $b \cdot |c|$. Συνεπώς, από την (1.3.2) βλέπουμε ότι $d' \mid d$.

Στη συνέχεια, αφού $d'/|c| = (a, b)$, από το Πόρισμα 1.3.5,

$$\frac{d'}{|c|} = au + bv$$

για κάποιους ακεραίους u και v. Αυτό συνεπάγεται ότι

$$d' = a \cdot |c| \cdot u + b \cdot |c| \cdot v = \frac{|c|}{c}(acu + bcv).$$

Όμως, ο d είναι κοινός διαιρέτης των ac και bc, άρα $d \mid d'$. Αφού $d' \mid d$ και $d \mid d'$, συμπεραίνουμε από το Θεώρημα 1.2.5 (ι) ότι $|d| = |d'|$. Αφού οι d και d' είναι και οι δύο μη αρνητικοί, συμπεραίνουμε ότι $d = d'$. □

1.4 Ο Ευκλείδειος αλγόριθμος

Σε αυτή την ενότητα, αποδεικνύουμε ένα αποτέλεσμα που μας επιτρέπει να υπολογίζουμε τον μέγιστο κοινό διαιρέτη δύο ακεραίων. Πρώτα, χρειαζόμαστε ένα λήμμα.

Λήμμα 1.4.1. *Έστω a, b ακέραιοι όχι και οι δύο μηδέν, και εστω q και r ακέραιοι τέτοιοι ώστε*

$$a = bq + r.$$

Τότε,

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

Απόδειξη. Παρατηρήστε ότι οι b, r δεν είναι και οι δύο μηδέν, αλλιώς θα είχαμε και $a = 0$. Έστω $d = (a, b)$ και $d' = (b, r)$. Παρατηρούμε ότι, αφού $d \mid a$ και $d \mid b$, έχουμε $d \mid (a - bq)$ από το Θεώρημα 1.2.5 (γ). Άρα, $d \mid r$ και ο d είναι κοινός διαιρέτης των b και r. Από τον Ορισμό 1.3.2 (γ), $d \mid d'$ αφού $d' = (b, r)$. Όμοια, $d' \mid b$ και $d' \mid r$, άρα $d' \mid (bq + r)$ από το Θεώρημα 1.2.5 (γ) και έπεται ότι $d' \mid a$. Από τον Ορισμό 1.3.2 (γ), $d' \mid d$ αφού $d = (a, b)$. Συνεπώς, από το Θεώρημα 1.2.5 (ι), $d = d'$. □

Θεώρημα 1.4.2 (ο Ευκλείδειος αλγόριθμος)**.** *Έστω a και b θετικοί ακέραιοι με $b \nmid a$. Θέτουμε $r_0 = a$, $r_1 = b$, και εφαρμόζουμε τον αλγόριθμο της διαίρεσης διαδοχικά, παίρνοντας ένα σύνολο υπολοίπων $r_2, r_3, \ldots, r_n, r_{n+1}$ που ορίζονται από τις σχέσεις*

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 & 0 &< r_2 < r_1 \\
r_1 &= r_2 q_2 + r_3 & 0 &< r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 &< r_n < r_{n-1} \\
r_{n-1} &= r_n q_n + r_{n+1} & r_{n+1} &= 0.
\end{aligned}$$

Τότε, ο r_n, το τελευταίο μη μηδενικό υπόλοιπο σε αυτή τη διαδικασία, είναι ο (a, b), ο μέγιστος κοινός διαιρέτης των a και b.

Απόδειξη. Σε κάποιο βήμα της διαδικασίας πρέπει να έχουμε $r_{n+1} = 0$, διότι οι r_i είναι μη αρνητικοί και φθίνουν γνησίως. Στη συνέχεια, εφαρμόζοντας το Λήμμα 1.4.1, βλέπουμε ότι

$$(a, b) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_n, r_{n+1}) = (r_n, 0) = r_n.$$

Αυτό ολοκληρώνει την απόδειξη του Θεωρήματος 1.4.2. □

Παράδειγμα 1.4.3. Υπολογίστε τον $(196884, 576)$.

Λύση. Έχουμε

$$\begin{aligned}
196884 &= 341 \cdot 576 + 468 \\
576 &= 1 \cdot 468 + 108 \\
468 &= 4 \cdot 108 + 36 \\
108 &= 3 \cdot 36 + 0.
\end{aligned}$$

Συνεπώς, $(196884, 576) = 36$.

1.5 Ισοτιμίες

Έστω $n \in \mathbb{N}$ και $a, b \in \mathbb{Z}$. Λέμε ότι ο a είναι ισότιμος με τον b ως προς n όταν $n \mid (a-b)$. Ο συμβολισμός είναι

$$a \equiv b \,(\operatorname{mod} n).$$

Θεώρημα 1.5.1 (βασικές ιδιότητες των ισοτιμιών)**.** *Έστω a, b, c, d, n ακέραιοι με $n > 0$. Τότε*

(i) *Για κάθε ακέραιο k, $k \equiv k \,(\operatorname{mod} n)$.*

(ii) *Αν $a \equiv b \,(\operatorname{mod} n)$ τότε $b \equiv a \,(\operatorname{mod} n)$.*

(iii) *Αν $a \equiv b \,(\operatorname{mod} n)$ και $b \equiv c \,(\operatorname{mod} n)$ τότε $a \equiv c \,(\operatorname{mod} n)$.*

(iv) *Αν $a \equiv b \,(\operatorname{mod} n)$ και $c \equiv d \,(\operatorname{mod} n)$ τότε $a + c \equiv b + d \,(\operatorname{mod} n)$ και $ac \equiv bd \,(\operatorname{mod} n)$.*

Η απόδειξη του Θεωρήματος 1.5.1 είναι άμεση, με εφαρμογή του ορισμού, και αφήνεται ως άσκηση.

Γνωρίζουμε ότι αν $c \neq 0$ τότε η $ca = cb$ συνεπάγεται ότι $a = b$. Αυτή η συνεπαγωγή είναι γνωστή ως ο νόμος της διαγραφής για την ισότητα. Ο νόμος αυτός δεν ισχύει γενικά αν αντικαταστήσουμε το «$=$» με «$\equiv$». Για παράδειγμα, $15 \equiv 3 \,(\operatorname{mod} 12)$ αλλά $5 \not\equiv 1 \,(\operatorname{mod} 12)$. Το επόμενο αποτέλεσμα δείχνει ότι ο νόμος της διαγραφής ισχύει αν επιβάλουμε μια συνθήκη στον ακέραιο c.

Θεώρημα 1.5.2. *Έστω a, b, c ακέραιοι και n φυσικός αριθμός. Αν $ca \equiv cb \,(\operatorname{mod} n)$ και $(c, n) = 1$, τότε $a \equiv b \,(\operatorname{mod} n)$.*

Απόδειξη. Θυμηθείτε από το Πόρισμα 1.3.5 ότι αν $(c, n) = 1$ τότε υπάρχουν ακέραιοι x και y τέτοιοι ώστε $cx + ny = 1$. Πολλαπλασιάζοντας με a και b παίρνουμε

$$acx + any = a$$

και

$$bcx + bny = b,$$

αντίστοιχα. Αφού $ac \equiv bc \,(\operatorname{mod} n)$, συμπεραίνουμε ότι $a - b \equiv (ac - bc)x \equiv 0 \,(\operatorname{mod} n)$, άρα

$$a \equiv b \,(\operatorname{mod} n).$$

□

Χρησιμοποιώντας το Θεώρημα 1.5.2 μπορούμε να αποδείξουμε το ακόλουθο αποτέλεσμα του Ευκλείδη.

Πόρισμα 1.5.3 (το Λήμμα του Ευκλείδη)**.** *Έστω a και b ακέραιοι και έστω p πρώτος. Αν $p \mid (ab)$ τότε είτε $p \mid a$ ή $p \mid b$.*

Απόδειξη. Ο p έχει μόνο δύο θετικούς διαιρέτες, τον 1 και τον p. Άρα, για κάθε ακέραιο n έχουμε $(n, p) = 1$ ή p.

Ας υποθέσουμε ότι $p \nmid a$. Τότε $(p, a) = 1$. Από το Θεώρημα 1.5.2, η σχέση

$$ab \equiv 0 \,(\operatorname{mod} p)$$

συνεπάγεται τότε ότι
$$b \equiv 0 \pmod p.$$
□

Με επαγωγή παίρνουμε το ακόλουθο:

Πόρισμα 1.5.4. *Έστω $a_1, a_2, \ldots, a_m$ ακέραιοι και έστω p πρώτος. Αν $p \mid (a_1 a_2 \cdots a_m)$ τότε $p \mid a_k$ για κάποιον k.*

1.6 Θεμελιώδες θεώρημα της Αριθμητικής

Θεώρημα 1.6.1 (Θεμελιώδες θεώρημα της Αριθμητικής)**.** *Κάθε θετικός ακέραιος $n > 1$ αναπαρίσταται ως γινόμενο πρώτων. Αυτή η αναπαράσταση είναι μοναδική αν εξαιρέσουμε τη σειρά με την οποία εμφανίζονται οι πρώτοι παράγοντες.*

Απόδειξη. Δείχνουμε πρώτα ότι ο n είναι πρώτος ή γράφεται ως γινόμενο πρώτων. Χρησιμοποιούμε επαγωγή ως προς n. Ο ισχυρισμός προφανώς αληθεύει για τον $n = 2$ διότι ο 2 είναι πρώτος. Έστω ότι ο m είναι πρώτος ή γινόμενο πρώτων για κάθε $2 \leqslant m \leqslant n-1$. Αν ο n είναι πρώτος τότε έχουμε τελειώσει. Υποθέτουμε ότι ο n είναι σύνθετος, και τότε $n = ab$, όπου $1 < a, b < n$. Από την επαγωγική υπόθεση καθένας από τους a και b είναι είτε πρώτος ή γινόμενο πρώτων. Άρα, ο $n = ab$ είναι γινόμενο πρώτων. Από το Θεώρημα 1.1.4 έπεται ότι κάθε θετικός ακέραιος $n > 1$ είναι πρώτος ή γινόμενο πρώτων.

Για να δείξουμε τη μοναδικότητα, χρησιμοποιούμε πάλι επαγωγή ως προς n. Αν $n = 2$ τότε η αναπαράσταση του n στη μορφή γινομένου πρώτων είναι προφανώς μοναδική. Υποθέτουμε ότι αυτό αληθεύει για όλους τους ακεραίους που είναι μεγαλύτεροι από 1 και μικρότεροι από n. Θα αποδείξουμε ότι το ίδιο ισχύει για τον n. Αν ο n είναι πρώτος, τότε δεν έχουμε τίποτα να δείξουμε. Υποθέτουμε λοιπόν ότι ο n είναι σύνθετος και έχει δύο παραγοντοποιήσεις, ας πούμε

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t. \tag{1.6.1}$$

Αφού ο p_1 διαιρεί το γινόμενο $q_1 q_2 \cdots q_t$, πρέπει να διαιρεί τουλάχιστον έναν παράγοντα από το Πόρισμα 1.5.4. Αλλάζοντας αν χρειαστεί ονόματα στους $q_1, q_2, \ldots, q_t$ μπορούμε να υποθέσουμε ότι $p_1 \mid q_1$. Τότε $p_1 = q_1$ αφού οι p_1 και q_1 είναι και οι δύο πρώτοι. Μπορούμε τότε στην (1.6.1) να διαγράψουμε τον p_1 από τα δύο μέλη της ισότητας, και παίρνουμε

$$n/p_1 = p_2 \cdots p_s = q_2 \cdots q_t.$$

Τώρα, από την επαγωγική υπόθεση έπεται ότι οι δύο παραγοντοποιήσεις του n/p_1 πρέπει να ταυτίζονται, αν εξαιρέσουμε τη σειρά με την οποία εμφανίζονται οι παράγοντες. Συνεπώς, $s = t$ και οι παραγοντοποιήσεις στην (1.6.1) ταυτίζονται, αν εξαιρέσουμε τη σειρά εμφάνισης των παραγόντων. Αυτό ολοκληρώνει την απόδειξη. □

Στα επόμενα κεφάλαια, όποτε γράφουμε

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

εννοούμε ότι $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ είναι η ανάλυση του n σε γινόμενο δυνάμεων πρώτων, η οποία είναι μοναδική με την εξαίρεση μιας αναδιάταξης των παραγόντων. Όταν γράφουμε

$$n=\prod_{k=1}^{r} p_k^{\alpha_k}$$

εννοούμε ότι $\alpha_j \geqslant 1$ για κάθε $1\leqslant j\leqslant r$. Όταν γράφουμε

$$n=\prod_{p} p^{\alpha_p},$$

εννοούμε ότι το γινόμενο είναι πάνω από όλους τους πρώτους και ότι μόνο πεπερασμένοι το πλήθος από τους εκθέτες α_p είναι μη-μηδενικοί.

1.7 Η απειρία των πρώτων αριθμών

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

Θεώρημα 1.7.1. *Υπάρχουν άπειροι πρώτοι αριθμοί.*

Θα δώσουμε τέσσερεις διαφορετικές αποδείξεις αυτού του θεωρήματος. Οι τρεις τελευταίες εξασφαλίζουν την απειρία των πρώτων, δίνουν όμως και περισσότερες πληροφορίες για την *άπειρη ακολουθία* των πρώτων αριθμών.

Πρώτη απόδειξη. Το επιχείρημα είναι αυτό που χρησιμοποίησε ο Ευκλείδης. Ας υποθέσουμε ότι υπάρχουν πεπερασμένοι το πλήθος πρώτοι αριθμοί, οι $p_1<\cdots<p_r$. Θεωρούμε τον φυσικό αριθμό

$$n=p_1\cdots p_r+1.$$

Ο n είναι μεγαλύτερος από 1, άρα έχει τουλάχιστον έναν πρώτο διαιρέτη. Αφού το $\{p_1,\dots,p_r\}$ είναι το σύνολο *όλων* των πρώτων αριθμών, υπάρχει $j\leqslant r$ τέτοιος ώστε $p_j \mid n$. Όμως $p_j \mid p_1\cdots p_r$, άρα

$$p_j \mid (n-p_1\cdots p_r) \text{ δηλαδή } p_j \mid 1.$$

Αυτό είναι άτοπο, άρα υπάρχουν άπειροι πρώτοι. □

Η επόμενη απόδειξη χρησιμοποιεί τους *αριθμούς του Fermat.*

Δεύτερη απόδειξη. Για κάθε $n=0,1,2,\dots$ ορίζουμε

$$F_n=2^{2^n}+1.$$

Οι αριθμοί F_n λέγονται αριθμοί του Fermat. Αφού $F_n\geqslant 2$ για κάθε $n\geqslant 0$, κάθε F_n έχει τουλάχιστον έναν πρώτο διαιρέτη q_n. Θα δείξουμε ότι

$$n\neq m \Longrightarrow (F_n,F_m)=1. \tag{1.7.1}$$

Οποιοιδήποτε δύο αριθμοί του Fermat είναι σχετικά πρώτοι, άρα (εξηγήστε γιατί)

$$n \neq m \Longrightarrow q_n \neq q_m.$$

Έπεται ότι οι q_n, $n \geqslant 0$, είναι διακεκριμένοι πρώτοι, το οποίο δείχνει την απειρία των πρώτων αριθμών.

Για την απόδειξη της (1.7.1) δείχνουμε πρώτα με επαγωγή το εξής: αν $n \geqslant 1$, τότε

$$\prod_{j=0}^{n-1} F_j = F_n - 2. \tag{1.7.2}$$

Η (1.7.2) ισχύει αν $n = 1$: $F_0 = 3 = 5 - 2 = F_1 - 2$. Αν δεχτούμε ότι ισχύει για $n = k$, τότε

$$\begin{aligned}\prod_{j=0}^{k} F_j &= \left(\prod_{j=0}^{k-1} F_j\right) \cdot F_k = (F_k - 2) \cdot F_k = (2^{2^k} - 1)(2^{2^k} + 1) = 2^{2^{k+1}} - 1 \\ &= F_{k+1} - 2,\end{aligned}$$

δηλαδή η (1.7.2) ισχύει για $n = k + 1$. Έστω τώρα $0 \leqslant m < n$ και έστω d ένας κοινός θετικός διαιρέτης των F_m και F_n. Τότε

$$d \mid F_m \quad \Longrightarrow \quad d \mid \prod_{j=0}^{n-1} F_j = F_n - 2,$$

άρα $d \mid F_n$ και $d \mid (F_n - 2)$. Έπεται ότι $d \mid 2$, άρα $d = 1$ ή $d = 2$. Αφού όλοι οι αριθμοί του Fermat είναι περιττοί, ο d δεν μπορεί να ισούται με 2. Άρα $(F_n, F_m) = 1$. $\square$

Η πρώτη απόδειξη (του Ευκλείδη) είναι πολύ πιο σύντομη και κομψή. Κοιτάζοντας όμως τη δεύτερη απόδειξη παρατηρούμε το εξής: αν $p_1 < p_2 < \cdots < p_n < p_{n+1} < \cdots$ είναι η άπειρη ακολουθία των πρώτων αριθμών, τότε

$$p_n \leqslant F_{n-1} = 2^{2^{n-1}} + 1$$

για κάθε $n \in \mathbb{N}$. Πράγματι, οι $F_0, F_1, \ldots, F_{n-1}$ έχουν n διακεκριμένους πρώτους διαιρέτες $p_{k_1}, \ldots, p_{k_n}$, άρα

$$p_n \leqslant \max\{p_{k_1}, \ldots, p_{k_n}\} \leqslant \max\{F_0, F_1, \ldots, F_{n-1}\} = F_{n-1}.$$

Η παρατήρηση αυτή μας οδηγεί στον ορισμό μιας συνάρτησης $\pi : \mathbb{R} \to \mathbb{R}$, με

$$\pi(x) = \text{ το πλήθος των πρώτων αριθμών } p \leqslant x. \tag{1.7.3}$$

Η π είναι αύξουσα, και βέβαια $\pi(x) = 0$ αν $x < 2$, $\pi(x) = 1$ αν $2 \leqslant x < 3$. Παρατηρούμε ότι αν $x \geqslant 3$ και αν $n = n(x)$ είναι ο μεγαλύτερος μη αρνητικός ακέραιος για τον οποίο $2^{2^n} + 1 \leqslant x$, τότε

$$\pi(x) \geqslant \pi\big(2^{2^n} + 1\big) \geqslant n + 1.$$

Από την άλλη πλευρά, $2^{2^{n+1}} \geqslant 2^{2^n} + 2 \geqslant x$ άρα $\log_2(\log_2 x) \leqslant n + 1$. Έχουμε λοιπόν το εξής κάτω φράγμα για την $\pi(x)$.

Πρόταση 1.7.2. *Για κάθε πραγματικό αριθμό $x \geqslant 2$ ισχύει η ανισότητα*

$$\pi(x) \geqslant \log_2(\log_2 x).$$

Ειδικότερα, $\pi(x) \to +\infty$ καθώς το $x \to +\infty$, άρα υπάρχουν άπειροι πρώτοι.

Με άλλα λόγια, η δεύτερη απόδειξη μας δίνει επιπλέον πληροφορίες για το πλήθος των πρώτων αριθμών σε ένα διάστημα της μορφής $[0, x]$, όπου x είναι ένας «μεγάλος» θετικός πραγματικός αριθμός. Η επόμενη απόδειξη που θα δώσουμε δίνει ακόμα καλύτερο κάτω φράγμα για τη συνάρτηση $\pi(x)$.

Τρίτη απόδειξη. Θεωρούμε την (ενδεχομένως πεπερασμένη) ακολουθία των πρώτων αριθμών σε αύξουσα διάταξη: $p_1 < p_2 < \cdots < p_k < \cdots$. Αν $f(t) = 1/t$, τότε για κάθε $n \geqslant 2$ και για κάθε $n \leqslant x < n+1$ έχουμε

$$\begin{aligned} \ln x &= \int_1^x \frac{1}{t}dt \leqslant \int_1^2 \frac{1}{t}dt + \int_2^3 \frac{1}{t}dt + \cdots + \int_n^{n+1} \frac{1}{t}dt \\ &\leqslant 1 + \frac{1}{2} + \cdots + \frac{1}{n} \leqslant \sum_{m \in A(x)} \frac{1}{m}, \end{aligned} \tag{1.7.4}$$

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:

$$A(x) = \left\{ n = \prod_{k=1}^{\pi(x)} p_k^{r_k} : r_k \geqslant 0 \right\}.$$

Παρατηρήστε ότι ο 1 προκύπτει αν πάρουμε όλους τους εκθέτες r_k ίσους με 0. Χρησιμοποιώντας την επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση ελέγχουμε ότι

$$\sum_{m \in A(x)} \frac{1}{m} = \prod_{k=1}^{\pi(x)} \left(\sum_{s=0}^{\infty} \frac{1}{p_k^s} \right).$$

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

$$\ln x \leqslant \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}.$$

Από την προφανή ανισότητα $p_k \geqslant k+1$ βλέπουμε ότι

$$\frac{p_k}{p_k + 1} = 1 + \frac{1}{p_k - 1} \leqslant 1 + \frac{1}{k} = \frac{k+1}{k}.$$

Επιστρέφοντας στην (1.7.4) παίρνουμε

$$\ln x \leqslant \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1.$$

Δηλαδή, έχουμε αποδείξει την εξής βελτίωση της Πρότασης 1.7.2. $\square$

Πρόταση 1.7.3. *Για κάθε πραγματικό αριθμό $x \geqslant 2$ ισχύει η ανισότητα*

$$\pi(x) \geqslant \ln x - 1.$$

Ειδικότερα, $\pi(x) \to +\infty$ καθώς το $x \to +\infty$, άρα υπάρχουν άπειροι πρώτοι.

Η τελευταία απόδειξη που θα δώσουμε εξασφαλίζει την απειρία των πρώτων με τον εξής τρόπο: η σειρά

$$\sum_{p \in P} \frac{1}{p}$$

αποκλίνει (P είναι το σύνολο των πρώτων αριθμών). Επομένως, το πλήθος των προσθετέων (δηλαδή, το πλήθος των πρώτων αριθμών) αποκλείεται να είναι πεπερασμένο. Η πρώτη απόδειξη αυτού του αποτελέσματος δόθηκε από τον Euler. Επί τη ευκαιρία, υπενθυμίζουμε τον ορισμό και τις βασικές ιδιότητες της συνάρτησης του ακεραίου μέρους.

Ορισμός 1.7.4. Έστω $x \in \mathbb{R}$. Το *ακέραιο μέρος* $[x]$ του x είναι ο μοναδικός ακέραιος m που ικανοποιεί τις ανισότητες $m \leqslant x < m+1$. Η απεικόνιση $x \mapsto [x]$ καλείται *συνάρτηση του ακεραίου μέρους.*

Πρόταση 1.7.5. *Για κάθε $x, y \in \mathbb{R}$ ισχύουν τα εξής.*

(i) $x - 1 < [x] \leqslant x$ *και* $0 \leqslant x - [x] < 1$.

(ii) *Αν $x \geqslant 0$, τότε ο $[x]$ ισούται με το πλήθος των φυσικών που δεν ξεπερνούν τον x. Δηλαδή*

$$[x] = \sum_{1 \leqslant n \leqslant x} 1.$$

(iii) *Για κάθε $k \in \mathbb{Z}$ έχουμε $[x+k] = [x] + k$.*

(iv) $[x] + [y] \leqslant [x+y] \leqslant [x] + [y] + 1$.

(v) *Αν $x \in \mathbb{Z}$ τότε $[x] + [-x] = 0$, ενώ αν $x \notin \mathbb{Z}$ τότε $[x] + [-x] = -1$.*

(vi) *Αν $x > 0$ και $k \in \mathbb{N}$, τότε $[x/k]$ είναι το πλήθος των πολλαπλασίων του k που δεν ξεπερνούν τον x.*

Η απόδειξη αυτών των ιδιοτήτων είναι απλή και αφήνεται ως άσκηση για τον αναγνώστη.

Τέταρτη απόδειξη, Erdős. Έστω $P = \{p_1, p_2, \ldots\}$ το σύνολο των πρώτων αριθμών, τους οποίους θεωρούμε σε αύξουσα διάταξη. Ας υποθέσουμε ότι η σειρά $\sum_{i \geqslant 1} \frac{1}{p_i}$ συγκλίνει. Τότε υπάρχει φυσικός αριθμός k με την ιδιότητα

$$\sum_{i \geqslant k+1} \frac{1}{p_i} < \frac{1}{2}. \tag{1.7.5}$$

Θα λέμε ότι οι $p_1, \ldots, p_k$ είναι οι *μικροί* πρώτοι, ενώ οι $p_{k+1}, \ldots$ είναι οι *μεγάλοι* πρώτοι. Για κάθε φυσικό αριθμό N έχουμε

$$\sum_{i \geqslant k+1} \frac{N}{p_i} < \frac{N}{2}.$$

Γράφουμε N_b για το πλήθος των φυσικών $n \leqslant N$ που έχουν τουλάχιστον έναν μεγάλο πρώτο διαιρέτη, και N_s για το πλήθος των φυσικών $n \leqslant N$ που όλοι οι πρώτοι διαιρέτες τους είναι μικροί. Από τον ορισμό των N_b και N_s έχουμε

$$N_b + N_s = N.$$

Παρατηρούμε ότι το πλήθος των φυσικών $n \leqslant N$ που είναι πολλαπλάσια κάποιου πρώτου p_i ισούται με $[N/p_i]$. Άρα χρησιμοποιώντας και την (1.7.5) παίρνουμε

$$N_b \leqslant \sum_{i \geqslant k+1} \left[\frac{N}{p_i}\right] \leqslant \sum_{i \geqslant k+1} \frac{N}{p_i} < \frac{N}{2}.$$

Ας δούμε τώρα πώς μπορεί κανείς να φράξει τον N_s. Κάθε φυσικός n γράφεται στη μορφή $n = a_n b_n^2$, όπου ο a_n είναι γινόμενο διακεκριμένων πρώτων ή 1 (άσκηση). Αν λοιπόν ο $n \leqslant N$ έχει μόνο μικρούς πρώτους διαιρέτες, τότε αφού αυτοί οι πρώτοι είναι κάποιοι από τους $p_1, \ldots, p_k$, έχουμε το πολύ 2^k επιλογές για τον a_n. Επιπλέον $b_n^2 \leqslant n \leqslant N$, άρα $b_n \leqslant \sqrt{N}$. Δηλαδή έχουμε το πολύ $\sqrt{N}$ επιλογές για τον b_n. Έπεται ότι

$$N_s \leqslant 2^k \sqrt{N}.$$

Από τις προηγούμενες τρείς σχέσεις παίρνουμε

$$N = N_b + N_s \leqslant \frac{N}{2} + 2^k \sqrt{N},$$

δηλαδή

$$\sqrt{N} \leqslant 2^{k+1}.$$

Αυτό όμως δεν μπορεί να ισχύει για κάθε φυσικό αριθμό N: τότε το $\mathbb{N}$ θα ήταν άνω φραγμένο. Καταλήξαμε σε άτοπο, άρα η σειρά $\sum_{i \geqslant 1} \frac{1}{p_i}$ αποκλίνει. Ειδικότερα, υπάρχουν άπειροι πρώτοι. □

Το πρόβλημα της ασυμπτωτικής συμπεριφοράς της συνάρτησης $\pi(x)$ καθώς το $x \to +\infty$ απασχόλησε έντονα τους μαθηματικούς κατά τον 19ο αιώνα. Ο Legendre (1798) έκανε την εικασία ότι για μεγάλα x ο αριθμός $\pi(x)$ είναι περίπου ίσος με

$$\pi(x) \simeq \frac{x}{\ln x - A}, \tag{1.7.6}$$

όπου $A \simeq 1.08366$. Ο Gauss πρότεινε την προσέγγιση

$$\pi(x) \sim \int_2^x \frac{1}{\ln t} dt. \tag{1.7.7}$$

Το ολοκλήρωμα στο δεξιό μέλος είναι ουσιαστικά ίσο με $x/\ln x$ για μεγάλα x, οπότε μια ισχυρή εικασία που προκύπτει από την (1.7.7) είναι η

$$\lim_{x \to \infty} \frac{\pi(x) \ln x}{x} = 1. \tag{1.7.8}$$

Ο Chebyshev (1848) έδειξε ότι αν το όριο στην (1.7.8) υπάρχει, τότε θα είναι υποχρεωτικά ίσο με 1. Λίγο αργότερα (1850) έδειξε ότι υπάρχουν δύο θετικές σταθερές c_1 και c_2 τέτοιες ώστε

$$c_1 \frac{x}{\ln x} \leqslant \pi(x) \leqslant c_2 \frac{x}{\ln x}$$

για κάθε $x \geqslant 2$. Δηλαδή, η σωστή τάξη μεγέθους του $\pi(x)$ είναι $x/\ln x$ (συγκρίνετε με το πολύ ασθενέστερο κάτω φράγμα $\ln x - 1$ που δίνει η Πρόταση 1.7.3).

Πολύ νωρίτερα, ο Euler (1740) είχε εισαγάγει τη συνάρτηση

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

για πραγματικές τιμές της μεταβλητής s και είχε παρατηρήσει ότι αναπαρίσταται σαν απειρογινόμενο:

$$\zeta(s) = \prod_{p\in P} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Ο Riemann (1860) παρατήρησε ότι αυτή η ταυτότητα θα μπορούσε να οδηγήσει σε χρήσιμα συμπεράσματα για την κατανομή των πρώτων αριθμών αν θεωρούσε κανείς τη συνάρτηση ζ σαν συνάρτηση μιας μιγαδικής μεταβλητής s και χρησιμοποιούσε τις μεθόδους της μιγαδικής ανάλυσης. Ο συμβολισμός $\zeta(s)$ οφείλεται στον Riemann, και η συνάρτηση αυτή είναι γνωστή με το όνομα «συνάρτηση ζήτα του Riemann».

Το 1896, οι Hadamard και de la Vallée Poussin έδειξαν ανεξάρτητα και σχεδόν ταυτόχρονα ότι το όριο στην (1.7.8) υπάρχει και είναι ίσο με 1. Το αποτέλεσμα αυτό είναι γνωστό ως το «θεώρημα των πρώτων αριθμών». Από τη δουλειά του de la Vallée Poussin έπεται ότι το ολοκλήρωμα (1.7.7) που πρότεινε ο Gauss δίνει καλύτερη προσέγγιση για την τιμή του $\pi(x)$ απ' ότι δίνει η (1.7.6), όποια τιμή κι αν δοκιμάσει κανείς για τη σταθερά A.

1.8 Ασκήσεις

1.1. Ολοκληρώστε τις αποδείξεις των Θεωρημάτων 1.2.5, 1.3.8 και 1.5.1.

1.2. Αποδείξτε την εξής μορφή της ταυτότητας της διαίρεσης: αν $a, b \in \mathbb{Z}$ και $b \neq 0$, υπάρχουν μοναδικοί ακέραιοι q και r τέτοιοι ώστε $a = bq + r$ και $-|b|/2 < r \leqslant |b|/2$.

1.3. Ο ορισμός του μέγιστου κοινού διαιρέτη γενικεύεται ως εξής: αν $k \geqslant 2$ και $a_1, \ldots, a_k \in \mathbb{Z}$ και τουλάχιστον ένας από τους $a_1, \ldots, a_k$ δεν είναι μηδέν, ορίζουμε $(a_1, \ldots, a_k)$ εκείνον τον θετικό ακέραιο d που ικανοποιεί τα εξής:

(i) $d \mid a_j$ για κάθε $j = 1, \ldots, k$.

(ii) Αν $s \in \mathbb{Z}$ και $s \mid a_j$ για κάθε j, τότε $s \leqslant d$.

(α) Αποδείξτε ότι $(a_1, \ldots, a_k) = (|a_1|, \ldots, |a_k|)$ και ότι υπάρχουν ακέραιοι $x_1, \ldots, x_k$ τέτοιοι ώστε $(a_1, \ldots, a_k) = a_1x_1 + \cdots + a_kx_k$.

(β) Αποδείξτε ότι $((a_1, \ldots, a_{k-1}), a_k) = (a_1, \ldots, a_k)$.

1.4. Αποδείξτε τα ακόλουθα:

(α) Αν a, b και c είναι μη μηδενικοί ακέραιοι και $(a, b) = (a, c) = 1$ τότε $(a, bc) = 1$.

(β) Αν $a, b \in \mathbb{N}$ και $d = (a, b)$ τότε έχουμε $a = du$ και $b = dv$ για ακεραίους $u, v \in \mathbb{N}$ με $(u, v) = 1$.

(γ) Αν $r_1, r_2 \in \mathbb{N}$ με $(r_1, r_2) = 1$ και $r_1 \mid r_2m$ για κάποιον $m \in \mathbb{N}$, τότε $r_1 \mid m$.

(δ) Αν $r_1, r_2 \in \mathbb{N}$ με $(r_1, r_2) = 1$ και $r_1 \mid m$, $r_2 \mid m$ για κάποιον $m \in \mathbb{N}$, τότε $r_1r_2 \mid m$.

(ε) Αν $a, b, w \in \mathbb{N}$ με $(a, b) = 1$ και $w \mid ab$ τότε υπάρχουν μοναδικοί φυσικοί u, v τέτοιοι ώστε $w = uv$ και $u \mid a$, $v \mid b$. Επιπλέον έχουμε $(u, v) = 1$.

1.5. Έστω a, b, x, y μη μηδενικοί ακέραιοι και έστω n ένας θετικός ακέραιος. Αποδείξτε ότι αν $(a, b) = 1$ και $ab = c^n$, τότε $a = x^n$ και $b = y^n$ για κάποιους x και y.

1.6. Το ελάχιστο κοινό πολλαπλάσιο δύο μη μηδενικών ακεραίων a, b ορίζεται μέσω της

$$[a, b] = |ab|/(a, b).$$

Αποδείξτε ότι

$$(a, [b, c]) = [(a, b), (a, c)].$$

1.7. Έστω a, b ακέραιοι. Αποδείξτε ότι αν $(a, b) = 1$ τότε ο $(a + b, a^2 - ab + b^2)$ είναι ίσος με 1 ή 3.

1.8. Έστω m και n θετικοί ακέραιοι και $m \neq n$. Να βρείτε τον (A_m, A_n) όπου $A_m = a^{2^m} + 1$.

1.9. Έστω n και k θετικοί ακέραιοι. Αποδείξτε ότι αν $(n - 1)^2 \mid (n^k - 1)$ τότε $(n - 1) \mid k$. Από αυτό, ή με άλλον τρόπο, αποδείξτε ότι αν ο p είναι πρώτος τότε οι ακόλουθες προτάσεις είναι ισοδύναμες:

(α) Ο $(p - 1)! + 1$ είναι δύναμη του p.

(β) $p = 2, 3$ και 5.

1.10. Για κάθε $n \in \mathbb{N}$ και $0 \leqslant k \leqslant n$, ορίζουμε τον διωνυμικό συντελεστή

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}.$$

(α) Συμφωνούμε ότι $0! = 1$ και $\binom{0}{0} = 1$. Αποδείξτε ότι, για κάθε $n \in \mathbb{N}$,

$$\binom{n}{0} = \binom{n}{n} = 1$$

και

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

για κάθε $1 \leqslant k \leqslant n - 1$.

(β) Αποδείξτε ότι το γινόμενο k διαδοχικών φυσικών διαιρείται με $k!$. *Υπόδειξη:* Αποδείξτε με επαγωγή ότι ο $\binom{n}{k}$ είναι ακέραιος.

1.11. (α) Αν ο n είναι πρώτος και ο k είναι ακέραιος με $1 \leqslant k \leqslant n - 1$ αποδείξτε ότι

$$n \mid \binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

(β) Ισχύει το (α) χωρίς να υποθέσουμε ότι ο n είναι πρώτος;

1.12. Έστω $a, m, n \in \mathbb{N}$ με $a > 1$. Αποδείξτε ότι $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

1.13. Αποδείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $4n-1$. *Υπόδειξη:* Μιμηθείτε το επιχείρημα του Ευκλείδη.

1.14. Υποθέτουμε ότι ο 2^n+1 είναι πρώτος για κάποιον $n \geqslant 2$ (οι πρώτοι αυτής της μορφής λέγονται πρώτοι του Fermat). Αποδείξτε ότι ο n είναι δύναμη του 2.

1.15. Υποθέτουμε ότι ο 2^n-1 είναι πρώτος για κάποιον $n \in \mathbb{N}$ (οι πρώτοι αυτής της μορφής λέγονται πρώτοι του Mersenne). Αποδείξτε ότι ο n είναι πρώτος.

1.16. Έστω p ένας πρώτος αριθμός. Αποδείξτε ότι ο $\sqrt{p}$ είναι άρρητος.

1.17. Αποδείξτε ότι δεν υπάρχει πολυώνυμο $f(x) = a_0 + a_2 x + \cdots + a_k x^k$, $k \geqslant 1$, $a_k \neq 0$, με συντελεστές ακεραίους, για το οποίο όλοι οι αριθμοί $|f(n)|$, $n \geqslant 0$ να είναι πρώτοι.

1.18. Έστω $n \geqslant 2$. Αποδείξτε ότι ο $(n+1)! + k$ είναι σύνθετος για κάθε $k = 2, \ldots, n+1$. Αυτό αποδεικνύει ότι υπάρχουν οσοδήποτε μακριά διαστήματα διαδοχικών σύνθετων αριθμών.

1.19. Έστω $n \geqslant 2$. Αποδείξτε ότι ο $n!$ δεν είναι τέλειο τετράγωνο: δεν υπάρχει $m \in \mathbb{N}$ τέτοιος ώστε $n! = m^2$.

1.20. Αν $n \geqslant 2$ αποδείξτε ότι το άθροισμα

$$\sum_{k=1}^{n} \frac{1}{k}$$

δεν είναι ακέραιος.

ΚΕΦΑΛΑΙΟ 2

Αριθμητικές συναρτήσεις και γινόμενο Dirichlet

2.1 Η συνάρτηση Möbius

Ορισμός 2.1.1. Μια πραγματική ή μιγαδική συνάρτηση ορισμένη στο σύνολο των θετικών ακεραίων ονομάζεται αριθμητική συνάρτηση.

Οι αριθμητικές συναρτήσεις παίζουν σημαντικό ρόλο στη μελέτη των αριθμών. Εισάγουμε τώρα μία από τις πιο σημαντικές αριθμητικές συναρτήσεις, τη συνάρτηση του Möbius $\mu(n)$.

Ορισμός 2.1.2. Θέτουμε $\mu(1) = 1$ και αν $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ τότε ορίζουμε

$$\mu(n) = \begin{cases} (-1)^k & , \text{ αν } \alpha_1 = \alpha_2 = \cdots = \alpha_k = 1 \\ 0 & , \text{ αλλιώς} \end{cases}.$$

Η συνάρτηση $\mu(n)$ είναι γνωστή ως συνάρτηση του Möbius.

Παρατηρήστε ότι με βάση αυτόν τον ορισμό, η συνάρτηση Möbius $\mu(n)$ παίρνει την τιμή 0 αν και μόνο αν ο n έχει κάποιον τετραγωνικό παράγοντα μεγαλύτερο από 1.

Ορισμός 2.1.3. Γράφουμε

$$\sum_{d|n} f(d)$$

για να συμβολίσουμε το άθροισμα των τιμών της f πάνω από τους θετικούς διαιρέτες d του n.

Παρατήρηση 2.1.4. Αν $d_1, d_2, \ldots, d_k$ είναι οι διαιρέτες του n, τότε

$$\sum_{d|n} f(d) = f(d_1) + f(d_2) + \cdots + f(d_k).$$

Τώρα, η απεικόνιση $d \mapsto n/d$ είναι 1-1 και επί από το σύνολο των θετικών διαιρετών του n στον εαυτό του: κάθε d_j γράφεται στη μορφή n/d'_j, όπου d'_j είναι ο συζυγής διαιρέτης του d_j. Άρα,

$$\sum_{d|n} f(d) = f\left(\frac{n}{d'_1}\right) + f\left(\frac{n}{d'_2}\right) + \cdots + f\left(\frac{n}{d'_k}\right) = \sum_{d'|n} f\left(\frac{n}{d'}\right).$$

Συνεπώς,

$$\sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right). \tag{2.1.1}$$

Θεώρημα 2.1.5. *Έστω n ένας θετικός ακέραιος και έστω $[x]$ το ακέραιο μέρος ενός πραγματικού αριθμού x. Έχουμε*

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

Απόδειξη. Η ισότητα ισχύει για τον $n = 1$. Υποθέτουμε ότι $n > 1$ και

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$

Στο άθροισμα

$$\sum_{d|n} \mu(d)$$

οι όροι είναι μη μηδενικοί όταν $d = 1$ ή όταν οι διαιρέτες του n είναι γινόμενα διακεκριμένων πρώτων. Έτσι βλέπουμε ότι

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{d|(p_1 p_2 \cdots p_k)} \mu(d) \\ &= \mu(1) + [\mu(p_1) + \cdots + \mu(p_k)] + [\mu(p_1 p_2) + \cdots + \mu(p_{k-1} p_k)] + \cdots + \mu(p_1 \cdots p_k). \end{aligned} \tag{2.1.2}$$

Αφού υπάρχουν $\binom{k}{j}$ τρόποι για να επιλέξουμε j πρώτους από ένα σύνολο k πρώτων, συμπεραίνουμε από την (2.1.2) ότι

$$\sum_{d|n} \mu(d) = 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k = (1-1)^k = 0.$$

□

Ορισμός 2.1.6. Για κάθε θετικό ακέραιο $n \geqslant 1$ ορίζουμε

$$I(n) = \left[\frac{1}{n}\right].$$

Με βάση τον Ορισμό 2.1.6 μπορούμε να ξαναγράψουμε το Θεώρημα 2.1.5 στη μορφή

$$\sum_{d|n} \mu(d) = I(n). \tag{2.1.3}$$

2.2 Η συνάρτηση του Euler

Ορισμός 2.2.1. Η συνάρτηση του Euler $\varphi(n)$ ορίζεται να είναι το πλήθος των θετικών ακεραίων που είναι το πολύ ίσοι με n και είναι σχετικά πρώτοι (δείτε τον Ορισμό 1.3.6) προς τον n.

Μερικές φορές είναι βολικό να γράφουμε τον $\varphi(n)$ ως

$$\varphi(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} \mathbf{1}. \tag{2.2.1}$$

Το πρώτο σημαντικό αποτέλεσμα για την $\varphi(n)$ είναι το ακόλουθο θεώρημα.

Θεώρημα 2.2.2. *Έστω n ένας θετικός ακέραιος. Τότε,*

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

Απόδειξη. Θέτουμε

$$S = \{1, \dots, n\}$$

και για κάθε $d \mid n$, $d > 0$ ορίζουμε

$$A(d) = \{k \in \mathbb{Z} : (k,n) = d, 1 \leqslant k \leqslant n\}.$$

Αφού κάθε ακέραιος $k \leqslant n$ δίνει έναν μοναδικό (k,n), συμπεραίνουμε ότι το S είναι η ξένη ένωση των συνόλων $A(d)$, άρα

$$\sum_{d|n} f(d) = n, \tag{2.2.2}$$

όπου $f(d)$ είναι το πλήθος των στοιχείων του $A(d)$.

Ορίζουμε

$$B(d) = \{1 \leqslant q \leqslant n/d : (q, n/d) = 1\}.$$

Ισχυριζόμαστε ότι υπάρχει μία ένα προς ένα αντιστοιχία ανάμεσα στα στοιχεία των $A(d)$ και $B(d)$. Αν $k \in A(d)$, τότε ο k/d είναι φυσικός διότι $d \mid k$ και $k/d \in B(d)$ αφού $k/d \leqslant n/d$ και

$$(k/d, n/d) = 1$$

από το Θεώρημα 1.3.8 (γ). Αντίστροφα, αν $q \in B(d)$, θέτουμε $k = qd$ και έχουμε $k \leqslant n$ και $(k,n) = \left(qd, \frac{n}{d}d\right) = d(q, n/d) = d$, δηλαδή $k \in A(d)$.

Τώρα, το πλήθος των στοιχείων του $B(d)$ είναι $\varphi(n/d)$. Άρα, από την (2.2.2) και το γεγονός ότι

$$|A(d)| = |B(d)|,$$

όπου $|U|$ είναι το πλήθος των στοιχείων ενός συνόλου U, βλέπουμε ότι $f(d) = \varphi(n/d)$. Συνεπώς,

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

Όμως, από την (2.1.1), αυτό είναι ισοδύναμο με την

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

□

Στη συνέχεια αποδεικνύουμε μια ταυτότητα που συνδέει τις συναρτήσεις $\varphi(n)$ και $\mu(n)$.

Θεώρημα 2.2.3. *Έστω n ένας θετικός ακέραιος. Τότε,*

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

Απόδειξη. Παρατηρούμε αρχικά ότι

$$I(j) = \begin{cases} 1 & , \text{ αν } j = 1 \\ 0 & , \text{ αν } j > 1 \end{cases}.$$

Συνεπώς, αν $g(k)$ είναι μια αριθμητική συνάρτηση, τότε

$$\sum_{\substack{k=1 \\ (k,n)=1}}^{n} g(k) = \sum_{k=1}^{n} g(k) I((k,n)).$$

Θέτοντας $g(k) = 1$ βλέπουμε ότι

$$\varphi(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} \mathbf{1} = \sum_{k=1}^{n} I((k,n)).$$

Από την (2.1.3) συμπεραίνουμε ότι

$$\begin{aligned} \varphi(n) &= \sum_{k=1}^{n} I((k,n)) = \sum_{k=1}^{n} \sum_{d|(k,n)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|k \\ d|n}} \mu(d) \\ &= \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} \mathbf{1} = \sum_{d|n} \mu(d) \frac{n}{d}. \end{aligned}$$

Το πέρασμα στην προτελευταία ισότητα δικαιολογείται από το γεγονός ότι στο προηγούμενο άθροισμα για κάθε $d \mid n$ έχουμε το $\mu(d)$ τόσες φορές όσα είναι τα πολλαπλάσια k του d έως το n, δηλαδή n/d φορές. Αυτό ολοκληρώνει την απόδειξη του θεωρήματος. □

Για κάθε θετικό ακέραιο n, μπορούμε πάντοτε να υπολογίσουμε την $\varphi(n)$ απευθείας, μετρώντας το πλήθος των ακεραίων $k \leqslant n$ που είναι σχετικά πρώτοι προς τον n. Όμως, αυτή η ευθεία μέθοδος είναι πολύ κοπιαστική εκτός από τις περιπτώσεις όπου ο n είναι πρώτος ή δύναμη πρώτου.

Αν ο p είναι πρώτος, τότε όλοι οι θετικοί ακέραιοι που είναι μικρότεροι από τον p είναι σχετικώς πρώτοι προς τον p και συμπεραίνουμε ότι

$$\varphi(p) = p - 1. \tag{2.2.3}$$

Αν $n = p^\alpha$ τότε οι μόνοι θετικοί ακέραιοι που είναι μικρότεροι από p^α και δεν είναι σχετικά πρώτοι προς τον p^α είναι τα πολλαπλάσια του p. Υπάρχουν ακριβώς $p^{\alpha-1}$ τέτοιοι ακέραιοι, άρα

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}. \tag{2.2.4}$$

Όταν ο n δεν είναι πρώτος ή δύναμη πρώτου, ο υπολογισμός της $\varphi(n)$ δίνεται από το επόμενο θεώρημα. Σημειώνουμε ότι ο τύπος που δίνει την $\varphi(n)$ είναι χρήσιμος μόνον όταν γνωρίζουμε την ανάλυση του n σε γινόμενο πρώτων παραγόντων.

Θεώρημα 2.2.4. *Έστω n ένας θετικός ακέραιος με ανάλυση*

$$n = \prod_{j=1}^{k} p_j^{\alpha_j}$$

σε γινόμενο πρώτων παραγόντων. Τότε

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

Απόδειξη. Από το Θεώρημα 2.2.3 βλέπουμε ότι

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d} = n \sum_{d|p_1^{\alpha_1}\cdots p_k^{\alpha_k}} \frac{\mu(d)}{d} = n \sum_{d|p_1\cdots p_k} \frac{\mu(d)}{d}. \tag{2.2.5}$$

Η τελευταία ισότητα στην (2.2.5) προκύπτει από το γεγονός ότι η $\mu(d)$ είναι μη μηδενική αν και μόνο αν ο d είναι 1 ή ελεύθερος τετραγώνων διαιρέτης του n. Άρα,

$$\begin{aligned}\varphi(n) &= n\left(1 + \sum_i \frac{\mu(p_i)}{p_i} + \sum_{i\neq j} \frac{\mu(p_ip_j)}{p_ip_j} + \cdots + \frac{\mu(p_1\cdots p_k)}{p_1\cdots p_k}\right)\\ &= n\left(1 - \sum_i \frac{1}{p_i} + \sum_{i\neq j}\frac{1}{p_ip_j} - \cdots + \frac{(-1)^k}{p_1\cdots p_k}\right).\end{aligned}$$

Στη συνέχεια, χρησιμοποιούμε το γεγονός ότι αν οι $a_1, \ldots, a_k$ είναι διακεκριμένοι, τότε

$$(u-a_1)(u-a_2)\cdots(u-a_k) = u^k - \sum_i a_i u^{k-1} + \sum_{i\neq j} a_ia_j u^{k-2} + \cdots + (-1)^k a_1a_2\cdots a_k.$$

Θέτοντας $u = 1$ και $a_j = 1/p_j$ συμπεραίνουμε ότι

$$\begin{aligned}\varphi(n) &= n\left(1 - \sum_i \frac{1}{p_i} + \sum_{i\neq j}\frac{1}{p_ip_j} - \cdots + \frac{(-1)^k}{p_1\cdots p_k}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\\ &= n\prod_{j=1}^{k}\left(1-\frac{1}{p_j}\right).\end{aligned}$$

Παρατηρώντας ότι

$$\prod_{j=1}^{k}\left(1-\frac{1}{p_j}\right)=\prod_{p\mid n}\left(1-\frac{1}{p}\right),$$

ολοκληρώνουμε την απόδειξη του θεωρήματος. □

Αρκετές ιδιότητες της $\varphi(n)$ προκύπτουν αμέσως από το Θεώρημα 2.2.4.

Πόρισμα 2.2.5. (α) *Έστω p ένας πρώτος αριθμός και α ένας θετικός ακέραιος. Τότε*

$$\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}.$$

(β) *Αν m και n είναι θετικοί ακέραιοι τέτοιοι ώστε $(m,n)=d>1$, τότε*

$$\varphi(mn)=\varphi(m)\varphi(n)\frac{d}{\varphi(d)}.$$

(γ) *Αν οι m και n είναι σχετικώς πρώτοι, τότε $\varphi(mn)=\varphi(m)\varphi(n)$.*

Απόδειξη. (α) Παρατηρήστε ότι η ζητούμενη ισότητα είναι η (2.2.4) την οποία έχουμε ήδη αποδείξει. Αυτή η ταυτότητα έπεται άμεσα από το Θεώρημα 2.2.4 αν θέσουμε $n=p^\alpha$.

(β) Έστω m και n θετικοί ακέραιοι και έστω $d=(m,n)$. Γράφουμε $m=m'd_1$ και $n=n'd_2$, όπου d_1 και d_2 είναι τα γινόμενα όλων των δυνάμεων πρώτων που διαιρούν τον d στην ανάλυση των m και n αντίστοιχα. Από την επιλογή του d_1,

$$(m',d_1)=1. \tag{2.2.6}$$

Αν $(m',n')>1$, τότε ένας πρώτος p που διαιρεί τον (m',n') πρέπει να διαιρεί και τον $(m,n)=d$. Αυτό συνεπάγεται ότι $p\mid d_1$. Όμως $p\mid m'$, άρα $(m',d_1)\neq 1$, το οποίο έρχεται σε αντίφαση με την (2.2.6). Άρα, συμπεραίνουμε ότι $(m',n')=1$. Από την επιλογή των d_1 και d_2 συμπεραίνουμε ότι

$$\prod_{p\mid d}\left(1-\frac{1}{p}\right)=\prod_{p\mid d_1}\left(1-\frac{1}{p}\right)=\prod_{p\mid d_2}\left(1-\frac{1}{p}\right)=\prod_{p\mid d_1d_2}\left(1-\frac{1}{p}\right). \tag{2.2.7}$$

Αυτό συνεπάγεται ότι

$$\begin{aligned}\varphi(mn)&=mn\prod_{p\mid(mn)}\left(1-\frac{1}{p}\right)\\&=mn\prod_{p\mid(m'n'd_1d_2)}\left(1-\frac{1}{p}\right)\\&=mn\prod_{p\mid m'}\left(1-\frac{1}{p}\right)\prod_{p\mid n'}\left(1-\frac{1}{p}\right)\prod_{p\mid d}\left(1-\frac{1}{p}\right)\end{aligned}$$

από την (2.2.7). Άρα,

$$\begin{aligned}
\varphi(mn) &= mn \prod_{p|m'}\left(1-\frac{1}{p}\right)\prod_{p|n'}\left(1-\frac{1}{p}\right)\prod_{p|d}\left(1-\frac{1}{p}\right)\frac{\prod_{p|d}\left(1-\frac{1}{p}\right)}{\prod_{p|d}\left(1-\frac{1}{p}\right)} \\
&= mn\frac{\prod_{p|m'}\left(1-\frac{1}{p}\right)\prod_{p|n'}\left(1-\frac{1}{p}\right)\prod_{p|d_1}\left(1-\frac{1}{p}\right)\prod_{p|d_2}\left(1-\frac{1}{p}\right)}{\prod_{p|d}\left(1-\frac{1}{p}\right)} \\
&= mn\frac{\prod_{p|m}\left(1-\frac{1}{p}\right)\prod_{p|n}\left(1-\frac{1}{p}\right)}{\prod_{p|d}\left(1-\frac{1}{p}\right)} \\
&= \varphi(m)\varphi(n)\frac{d}{\varphi(d)}
\end{aligned}$$

από την (2.2.7).

(γ) Αν $m=1$ ή $n=1$ τότε το ζητούμενο ισχύει, μπορούμε λοιπόν να υποθέσουμε ότι $m,n>1$. Παρατηρούμε ότι αν $(m,n)=1$ τότε τα σύνολα των πρώτων διαιρετών των m και n είναι ξένα, και η ένωσή τους είναι το σύνολο των πρώτων διαιρετών του mn. Άρα,

$$\prod_{p|mn}\left(1-\frac{1}{p}\right) = \prod_{p|m}\left(1-\frac{1}{p}\right)\prod_{p|n}\left(1-\frac{1}{p}\right).$$

Έπεται ότι

$$\begin{aligned}
\varphi(mn) &= mn\prod_{p|mn}\left(1-\frac{1}{p}\right) = mn\prod_{p|m}\left(1-\frac{1}{p}\right)\prod_{p|n}\left(1-\frac{1}{p}\right) \\
&= m\prod_{p|m}\left(1-\frac{1}{p}\right) n\prod_{p|n}\left(1-\frac{1}{p}\right) = \varphi(m)\varphi(n).
\end{aligned}$$

□

Ορισμός 2.2.6. Μια αριθμητική συνάρτηση f λέγεται πολλαπλασιαστική αν

$$f(1)=1$$

και

$$f(mn)=f(m)f(n) \quad \text{εάν} \quad (m,n)=1.$$

Το Πόρισμα 2.2.5 (γ) δείχνει ότι η συνάρτηση φ του Euler είναι πολλαπλασιαστική. Άλλα παραδείγματα πολλαπλασιαστικών συναρτήσεων μας δίνουν η συνάρτηση Möbius $\mu(n)$ και η $I(n)$. Αφήνουμε την επαλήθευση αυτού του ισχυρισμού ως άσκηση.

Έστω $n>1$ ένας ακέραιος που γράφεται στη μορφή

$$n=\prod_{i=1}^{k} p_i^{\alpha_i}.$$

Αν f είναι μια πολλαπλασιαστική συνάρτηση, τότε

$$f(n) = f\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) = \prod_{i=1}^{k} f(p_i^{\alpha_i}).$$

Αυτό δείχνει ότι αν η f είναι πολλαπλασιαστική τότε η τιμή της σε κάθε θετικό ακέραιο προσδιορίζεται από τις τιμές της στις δυνάμεις πρώτων.

2.3 Γινόμενο Dirichlet αριθμητικών συναρτήσεων και πολλαπλασιαστικές συναρτήσεις

Ορισμός 2.3.1. Έστω f και g δύο αριθμητικές συναρτήσεις. Ορίζουμε το γινόμενο Dirichlet των f και g, το οποίο συμβολίζουμε με $f * g$, ως εξής:

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

Συχνά θα γράφουμε $f * g$ για τη συνάρτηση $(f * g)(n)$, παραλείποντας το n.

Ορισμός 2.3.2. Έστω n ένας θετικός ακέραιος. Η αριθμητική συνάρτηση $N(n)$ ορίζεται μέσω της

$$N(n) = n.$$

Χρησιμοποιώντας αυτόν τον συμβολισμό και τους Ορισμούς 2.3.1 και 2.3.2, μπορούμε να διατυπώσουμε το Θεώρημα 2.2.3 ως εξής:

$$\varphi = \mu * N.$$

Θεώρημα 2.3.3. *Το γινόμενο Dirichlet είναι μεταθετικό και προσεταιριστικό, δηλαδή, αν f, g, h είναι αριθμητικές συναρτήσεις τότε έχουμε*

$$f * g = g * f$$

και

$$(f * g) * h = f * (g * h).$$

Απόδειξη. Το γινόμενο Dirichlet των f και g δίνεται από την

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

Έστω $d_1 = n/d$ ο συζυγής διαιρέτης του d. Όταν ο d διατρέχει όλους τους διαιρέτες του n, το ίδιο κάνει και ο d_1. Από την (2.1.1),

$$(f * g)(n) = \sum_{d_1|n} f\left(\frac{n}{d_1}\right) g(d_1) = (g * f)(n).$$

Για να δείξουμε την προσεταιριστική ιδιότητα, θέτουμε $A = g * h$. Τότε

$$\begin{aligned}(f * A)(n) &= \sum_{a|n} f(a) A\left(\frac{n}{a}\right) = \sum_{a \cdot d = n} f(a) A(d) \\ &= \sum_{a \cdot d = n} f(a) \sum_{b \cdot c = d} g(b) h(c) \\ &= \sum_{a \cdot b \cdot c = n} f(a) g(b) h(c).\end{aligned}$$

Όμοια, αν θέσουμε $B = f * g$, τότε

$$\begin{aligned}(B * h)(n) &= \sum_{d \cdot c = n} B(d) h(c) \\ &= \sum_{d \cdot c = n} \sum_{a \cdot b = d} f(a) g(b) h(c) \\ &= \sum_{a \cdot b \cdot c = n} f(a) g(b) h(c).\end{aligned}$$

Συνεπώς,

$$(f * (g * h))(n) = ((f * g) * h)(n).$$

□

Θεώρημα 2.3.4. *Έστω $I(n)$ η συνάρτηση που ορίστηκε στον Ορισμό 2.1.6. Η συνάρτηση I είναι το ταυτοτικό στοιχείο για την $*$, δηλαδή $I * f = f * I = f$ για κάθε αριθμητική συνάρτηση f.*

Απόδειξη. Από τον ορισμό της I βλέπουμε ότι

$$(I * f)(n) = \sum_{d|n} I(d) f\left(\frac{n}{d}\right) = I(1) f(n) = f(n).$$

Από τη μεταθετική ιδιότητα του Θεωρήματος 2.3.3 συμπεραίνουμε ότι

$$f * I = f.$$

□

2.4 Αντίστροφες Dirichlet και ο τύπος αντιστροφής του Möbius

Θεώρημα 2.4.1. *Έστω f μια αριθμητική συνάρτηση. Αν $f(1) \neq 0$ τότε υπάρχει μοναδική συνάρτηση g τέτοια ώστε*

$$f * g = I. \tag{2.4.1}$$

Απόδειξη. Δείχνουμε με επαγωγή ως προς m ότι η (2.4.1) έχει μοναδική λύση $g(m)$. Για να ισχύει η (2.4.1), πρέπει η συνάρτηση $g(n)$ να ικανοποιεί την

$$f(1) g(1) = 1.$$

Αφού $f(1) \neq 0$, βλέπουμε ότι

$$g(1) = \frac{1}{f(1)},$$

δηλαδή η τιμή $g(1)$ προσδιορίζεται μονοσήμαντα. Θεωρούμε $m > 1$ και υποθέτουμε ότι οι τιμές $g(k)$ έχουν προσδιοριστεί για $1 \leqslant k \leqslant m-1$. Από την (2.4.1) βλέπουμε ότι

$$f(1)g(m) + \sum_{\substack{d|m \\ d>1}} f(d) g\left(\frac{m}{d}\right) = 0.$$

Συνεπώς,

$$g(m) = \frac{1}{f(1)} \left(-\sum_{\substack{d|m \\ d>1}} f(d) g\left(\frac{m}{d}\right) \right)$$

και η $g(m)$ προσδιορίζεται μονοσήμαντα. Από την αρχή της επαγωγής, υπάρχει μοναδική συνάρτηση $g(n)$ τέτοια ώστε

$$f * g = I.$$

□

Ορισμός 2.4.2. Έστω f αριθμητική συνάρτηση τέτοια ώστε $f(1) \neq 0$. Η μοναδική συνάρτηση g που ικανοποιεί την $f*g = I$ λέγεται αντίστροφη Dirichlet της f. Ο συμβολισμός για την αντίστροφη Dirichlet της f είναι f^{-1}.

Στη συνέχεια εισάγουμε άλλη μία αριθμητική συνάρτηση.

Ορισμός 2.4.3. Έστω n ένας θετικός ακέραιος. Η αριθμητική συνάρτηση u ορίζεται μέσω της

$$u(n) = 1.$$

Με αυτόν τον συμβολισμό, το Θεώρημα 2.1.5 διατυπώνεται ως εξής:

$$\mu * u = I.$$

Συνεπώς, έχουμε $u = \mu^{-1}$ και $\mu = u^{-1}$. Με άλλα λόγια, έχουμε:

Θεώρημα 2.4.4. *Η αντίστροφη Dirichlet της u είναι η μ.*

Θεώρημα 2.4.5 (τύπος αντιστροφής του Möbius)**.** *Αν $f = g * u$, τότε $g = f * \mu$. Αντίστροφα, αν $g = f * \mu$ τότε $f = g * u$.*

Απόδειξη. Υποθέτουμε ότι $f = g * u$. Τότε, από το Θεώρημα 2.4.4,

$$f * \mu = (g * u) * \mu = g * (u * \mu) = g * I = g.$$

Αντίστροφα, αν $g = f * \mu$ τότε

$$g * u = (f * \mu) * u = f * (\mu * u) = f * I = f.$$

□

Τα Θεωρήματα 2.2.2 και 2.2.3 είναι ειδικές περιπτώσεις του τύπου αντιστροφής του Möbius. Με άλλα λόγια,

$$N = \varphi * u \quad \text{και ισοδύναμα} \quad N * \mu = \varphi.$$

2.5 Πολλαπλασιαστικές συναρτήσεις και γινόμενα Dirichlet

Από την κατασκευή της f^{-1} στο Θεώρημα 2.4.1, δεν είναι σαφές ότι η αντίστροφη Dirichlet μιας πολλαπλασιαστικής συνάρτησης f είναι πολλαπλασιαστική. Τα αποτελέσματα που ακολουθούν δείχνουν ότι αυτό όντως ισχύει.

Θεώρημα 2.5.1. *Αν f και g είναι πολλαπλασιαστικές συναρτήσεις, τότε το ίδιο ισχύει και για το γινόμενο Dirichlet $f * g$.*

Απόδειξη. Έστω $h = f * g$. Παρατηρούμε ότι

$$h(1) = f(1)g(1) = 1.$$

Στη συνέχεια θεωρούμε την παράσταση

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

Αν υποθέσουμε ότι $(m, n) = 1$, μπορούμε να γράψουμε τους διαιρέτες του mn ως $c = ab$, όπου οι a, b διατρέχουν τα σύνολα των διαιρετών των m και n αντίστοιχα. Επομένως, συμπεραίνουμε ότι

$$\begin{aligned} h(mn) &= \sum_{a|m}\sum_{b|n} f(ab)g\left(\frac{m}{a}\frac{n}{b}\right) \\ &= \sum_{a|m}\sum_{b|n} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right), \end{aligned}$$

αφού $(m/a, n/b) = 1$ για κάθε $a \mid m$ και $b \mid n$, και οι f και g είναι και οι δύο πολλαπλασιαστικές. Από αυτή τη σχέση έπεται ότι

$$\begin{aligned} h(mn) &= \left(\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\right)\left(\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\right) \\ &= h(m)h(n). \end{aligned}$$

□

Θεώρημα 2.5.2. *Αν οι g και $f * g$ είναι και οι δύο πολλαπλασιαστικές, τότε η f είναι επίσης πολλαπλασιαστική.*

Απόδειξη. Αποδεικνύουμε το θεώρημα με απαγωγή σε άτοπο. Έστω ότι η f δεν είναι πολλαπλασιαστική. Θέτουμε

$$h = f * g.$$

Αφού η f δεν είναι πολλαπλασιαστική, υπάρχουν δύο σχετικώς πρώτοι ακέραιοι m και n τέτοιοι ώστε

$$f(mn) \neq f(m)f(n).$$

Επιλέγουμε τους m και n έτσι ώστε ο mn να είναι ο μικρότερος δυνατός. Αν $mn = 1$, τότε

$$f(1) \neq f(1)f(1)$$

και $f(1) \neq 1$. Αφού $h(1) = f(1)g(1) = f(1) \neq 1$, συμπεραίνουμε ότι η h δεν είναι πολλαπλασιαστική, το οποίο οδηγεί σε αντίφαση. Άρα, $mn \neq 1$.

Αν $mn > 1$, τότε
$$f(ab) = f(a)f(b)$$
για κάθε $1 \leqslant ab < mn$ με $(a,b) = 1$. Τώρα,
$$\begin{aligned} h(mn) &= f(mn)g(1) + \sum_{\substack{a|m, b|n \\ ab<mn}} f(ab) g\left(\frac{mn}{ab}\right) \\ &= f(mn) + \sum_{\substack{a|m, b|n \\ ab<mn}} f(a)f(b) g\left(\frac{m}{a}\right) g\left(\frac{n}{b}\right) \\ &= f(mn) - f(m)f(n) + h(m)h(n). \end{aligned}$$

Με άλλα λόγια,
$$h(mn) - h(m)h(n) = f(mn) - f(m)f(n).$$
Αφού $f(mn) \neq f(m)f(n)$, βλέπουμε ότι $h(mn) \neq h(m)h(n)$. Έπεται ότι η h δεν είναι πολλαπλασιαστική, το οποίο έρχεται σε αντίφαση με την υπόθεσή μας ότι η $f*g = h$ είναι πολλαπλασιαστική. □

Θεώρημα 2.5.3. *Αν η g είναι πολλαπλασιαστική τότε η αντίστροφη Dirichlet g^{-1} είναι επίσης πολλαπλασιαστική.*

Απόδειξη. Οι συναρτήσεις g και $g * g^{-1} = I$ είναι πολλαπλασιαστικές. Από το Θεώρημα 2.5.2 η g^{-1} είναι πολλαπλασιαστική. □

Παρατήρηση 2.5.4. Τα προηγούμενα αποτελέσματα δείχνουν ότι το σύνολο των πολλαπλασιαστικών αριθμητικών συναρτήσεων σχηματίζει αβελιανή ομάδα με το γινόμενο Dirichlet $*$, και ταυτοτικό στοιχείο την I.

2.6 Παράγωγος αριθμητικής συνάρτησης

Ορισμός 2.6.1. Για κάθε αριθμητική συνάρτηση f ορίζουμε την παράγωγό της f' να είναι η αριθμητική συνάρτηση που ορίζεται από την
$$f'(n) = f(n)\ln n, \qquad n \in \mathbb{N}.$$

Παραδείγματα 2.6.2. Αφού $I(n)\ln n = 0$ για κάθε $n \in \mathbb{N}$, έχουμε $I' \equiv 0$. Αφού $u(n) = 1$ για κάθε $n \in \mathbb{N}$, έχουμε $u'(n) = \ln n$. Έπεται ότι για τη συνάρτηση $\Lambda(n)$ του von Mangoldt (βλέπε Άσκηση 2.1), η σχέση
$$\sum_{d|n} \Lambda(d) = \ln n$$
γράφεται ισοδύναμα

$$\Lambda * u = u'. \tag{2.6.1}$$

Το επόμενο θεώρημα δείχνει ότι αυτή η έννοια παραγώγου έχει αρκετές από τις ιδιότητες της συνήθους παραγώγου που συζητάμε στον απειροστικό λογισμό. Ισχύουν οι γνωστοί «κανόνες παραγώγισης» αν ως γινόμενο θεωρήσουμε το γινόμενο Dirichlet.

Θεώρημα 2.6.3. *Αν f και g είναι αριθμητικές συναρτήσεις, τότε:*

(α) $(f+g)' = f' + g'$.

(β) $(f*g)' = f'*g + f*g'$.

(γ) $(f^{-1})' = -f' * (f*f)^{-1}$.

Απόδειξη. Η απόδειξη του (α) είναι άμεση: για κάθε $n \in \mathbb{N}$ έχουμε

$$(f+g)'(n) = (f+g)(n)\ln n = f(n)\ln n + g(n)\ln n = f'(n) + g'(n).$$

Για να αποδείξουμε το (β) χρησιμοποιούμε την ισότητα $\ln n = \ln d + \ln(n/d)$ και γράφουμε

$$\begin{aligned}(f*g)'(n) &= \sum_{d|n} f(d) g\left(\frac{n}{d}\right)\ln n \\ &= \sum_{d|n} f(d)\ln d \cdot g\left(\frac{n}{d}\right) + \sum_{d|n} f(d)\cdot g\left(\frac{n}{d}\right)\ln\left(\frac{n}{d}\right) \\ &= \sum_{d|n} f'(d) g\left(\frac{n}{d}\right) + \sum_{d|n} f(d) g'\left(\frac{n}{d}\right) \\ &= (f'*g)(n) + (f*g')(n).\end{aligned}$$

Για να αποδείξουμε το (γ) εφαρμόζουμε το (β) στην $I' = 0$, παίρνοντας υπόψιν μας την $I = f*f^{-1}$. Έχουμε

$$0 = (f*f^{-1})' = f'*f^{-1} + f*(f^{-1})',$$

άρα

$$f*(f^{-1})' = -f'*f^{-1}.$$

Πολλαπλασιάζοντας επί f^{-1} παίρνουμε

$$(f^{-1})' = -(f'*f^{-1})*f^{-1} = -f'*(f^{-1}*f^{-1}).$$

Όμως, $f^{-1}*f^{-1} = (f*f)^{-1}$, άρα έχουμε το (γ). □

Ως εφαρμογή της παραγώγου δίνουμε μια σύντομη απόδειξη μιας ταυτότητας του Selberg η οποία μερικές φορές χρησιμοποιείται ως αφετηρία για μια στοιχειώδη απόδειξη του θεωρήματος των πρώτων αριθμών.

Θεώρημα 2.6.4 (ταυτότητα του Selberg)**.** *Για κάθε $n \in \mathbb{N}$ ισχύει ότι*

$$\Lambda(n)\ln n + \sum_{d|n}\Lambda(d)\Lambda\left(\frac{n}{d}\right) = \sum_{d|n}\mu(d)\ln^2\left(\frac{n}{d}\right).$$

Απόδειξη. Από την (2.6.1) έχουμε ότι $\Lambda * u = u'$. Παραγωγίζοντας αυτή την ισότητα παίρνουμε

$$\Lambda' * u + \Lambda * u' = u'',$$

που λόγω της $u' = \Lambda * u$ γράφεται ως

$$\Lambda' * u + \Lambda * (\Lambda * u) = u''.$$

Πολλαπλασιάζοντας τα δύο μέλη της τελευταίας ισότητας επί $\mu = u^{-1}$ παίρνουμε

$$\Lambda' + \Lambda * \Lambda = u'' * \mu.$$

Παρατηρώντας ότι $\Lambda'(n) = \Lambda(n) \ln n$ και $u''(n) = \ln^2 n$ έχουμε το ζητούμενο. □

2.7 Ασκήσεις

2.1. (Η συνάρτηση $\Lambda(n)$ του von Mangoldt). Για κάθε ακέραιο $n \geqslant 1$ ορίζουμε

$$\Lambda(n) = \begin{cases} \ln p & , \text{ αν } n = p^m \text{ για κάποιον } p \text{ και κάποιον } m \geqslant 1 \\ 0 & , \text{ αλλιώς} \end{cases}.$$

(α) Είναι η $\Lambda(n)$ πολλαπλασιαστική;

(β) Αποδείξτε ότι για κάθε θετικό ακέραιο n,

$$\ln n = \sum_{d|n} \Lambda(d). \tag{2.7.1}$$

2.2. Μια αριθμητική συνάρτηση $f(n)$ λέγεται πλήρως πολλαπλασιαστική αν $f(1) = 1$ και για οποιουσδήποτε θετικούς ακεραίους m και n,

$$f(mn) = f(m)f(n).$$

(α) Αποδείξτε ότι αν η $f(n)$ είναι πλήρως πολλαπλασιαστική συνάρτηση, τότε η Dirichlet αντίστροφη της $f(n)$ είναι η $\mu(n)f(n)$.

(β) Αποδείξτε ότι αν η $f(n)$ είναι πολλαπλασιαστική συνάρτηση και $f^{-1}(n) = \mu(n)f(n)$ για κάθε θετικό ακέραιο n, τότε η $f(n)$ είναι πλήρως πολλαπλασιαστική.

2.3. Αποδείξτε ότι

$$\frac{n}{\varphi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)}$$

για κάθε $n \in \mathbb{N}$.

2.4. Αποδείξτε ότι για κάθε θετικό ακέραιο n,

$$\sum_{d^2|n} \mu(d) = \mu^2(n).$$

2.5. (Άθροισμα Ramanujan). Το άθροισμα Ramanujan ορίζεται μέσω της

$$c_q(n) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e^{2\pi i \frac{a}{q} n}.$$

(α) Αποδείξτε ότι
$$c_q(n) = \sum_{d|(q,n)} d\mu\left(\frac{q}{d}\right).$$

(β) Να βρείτε τη συνάρτηση $c_q(n)$ όταν $n = 0$.

(γ) Να βρείτε τη συνάρτηση $c_q(n)$ όταν $q = 1$.

2.6. Για πραγματικό ή μιγαδικό α και για κάθε θετικό ακέραιο n, ορίζουμε
$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha,$$
το άθροισμα των α-οστών δυνάμεων των διαιρετών του n.

(α) Αποδείξτε ότι η $\sigma_\alpha(n)$ είναι πολλαπλασιαστική.

(β) Αποδείξτε ότι
$$\sigma_\alpha(p^k) = \begin{cases} \frac{p^{\alpha(k+1)}-1}{p^\alpha - 1} & , \text{ αν } \alpha \neq 0 \\ k+1 & , \text{ αν } \alpha = 0 \end{cases}.$$

(γ) Να βρείτε την Dirichlet αντίστροφη της $\sigma_\alpha(n)$.

(δ) Ένας θετικός ακέραιος n λέγεται τέλειος αν ισούται με το άθροισμα των θετικών διαιρετών του που είναι μικρότεροι από n. Με άλλα λόγια, ο n είναι τέλειος αν
$$\sigma(n) := \sigma_1(n) = 2n.$$
Αποδείξτε ότι αν ο $2^p - 1$ είναι πρώτος, τότε ο $n = 2^{p-1}(2^p - 1)$ είναι τέλειος.

(ε) Αποδείξτε ότι αν ο n είναι άρτιος τέλειος αριθμός, τότε ο n πρέπει να είναι της μορφής
$$2^{k-1}(2^k - 1),$$
όπου ο $2^k - 1$ είναι πρώτος.

2.7. (Η συνάρτηση $\lambda(n)$ του Liouville). Έστω $\lambda(1) = 1$. Έστω n τυχών θετικός ακέραιος που δίνεται από την $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Ορίζουμε
$$\lambda(n) = (-1)^{\alpha_1 + \cdots + \alpha_k}.$$
Αποδείξτε ότι η λ είναι πλήρως πολλαπλασιαστική και ότι για κάθε $n \geqslant 1$,
$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & , \text{ αν ο } n \text{ είναι τέλειο τετράγωνο} \\ 0 & , \text{ αλλιώς} \end{cases}.$$
Χρησιμοποιώντας το γεγονός ότι η λ είναι πλήρως πολλαπλασιαστική, να βρείτε την λ^{-1}.

2.8. Έστω $d(n)$ το πλήθος των θετικών διαιρετών του n. Με άλλα λόγια,
$$d(n) = \sum_{d|n} 1 = (u * u)(n).$$
Αποδείξτε ότι
$$\prod_{t|n} t = n^{d(n)/2}.$$

2.9. Αποδείξτε ότι
$$\sum_{k|n} d(k)^3 = \left(\sum_{k|n} d(k)\right)^2.$$

2.10. (α) Αποδείξτε ότι ο $d(n)$ είναι περιττός αν και μόνο αν ο n είναι τέλειο τετράγωνο.

(β) Αποδείξτε ότι $d(n) \leqslant d(2^n - 1)$ για κάθε φυσικό n.

(γ) Αποδείξτε ότι $d(n) < 2\sqrt{n}$ για κάθε $n \in \mathbb{N}$.

(ε) Βρείτε όλους τους θετικούς ακεραίους n για τους οποίους ισχύει $d(2n) = n$.

2.11. Αποδείξτε ότι
$$\sum_{k|n} \mu(k) d\left(\frac{n}{k}\right) = 1 \qquad \text{και} \qquad \sum_{k|n} \mu(k) \sigma\left(\frac{n}{k}\right) = n$$
για κάθε $n \in \mathbb{N}$.

2.12. Αποδείξτε ότι η συνάρτηση $f(n) = (-1)^{n-1}$ είναι πολλαπλασιαστική και υπολογίστε το άθροισμα
$$h(n) = \sum_{k|n} (-1)^{k-1} \mu\left(\frac{n}{k}\right)$$
για κάθε $n \in \mathbb{N}$.

2.13. Να βρείτε μια αριθμητική συνάρτηση $f(n)$ τέτοια ώστε, για κάθε θετικό ακέραιο n,
$$\frac{1}{\varphi(n)} = \sum_{d|n} \frac{1}{d} f\left(\frac{n}{d}\right).$$

2.14. Αποδείξτε ότι
$$\sum_{\substack{k=1 \\ (k,n)=1}}^{n} k = \frac{n\varphi(n)}{2}$$
για κάθε $n \geqslant 2$.

2.15. Αποδείξτε ότι $\varphi(n)d(n) \geqslant n$ για $n \in \mathbb{N}$.

2.16. Έστω $n \in \mathbb{N}$ με την ιδιότητα $\varphi(n) \mid n$. Αποδείξτε ότι $n = 2^a 3^b$ για κάποιους $a, b \in \mathbb{Z}^+$.

2.17. Υποθέτουμε ότι $p_1 < p_2 < \cdots < p_N$ είναι όλοι οι πρώτοι αριθμοί. Αποδείξτε ότι $\varphi(p_1 p_2 \cdots p_N) = 1$ και καταλήξτε σε άτοπο (έτσι, παίρνετε άλλη μια απόδειξη για την απειρία των πρώτων αριθμών).

2.18. Αποδείξτε ότι
$$\sum_{k|n} \sigma(k) \varphi\left(\frac{n}{k}\right) = nd(n)$$
για κάθε $n \in \mathbb{N}$.

2.19. Έστω $f : \mathbb{N} \to \mathbb{C}$ πολλαπλασιαστική αριθμητική συνάρτηση. Αν $m, n \in \mathbb{N}$, $d = (m, n)$ και $D = mn/d$ αποδείξτε ότι
$$f(m)f(n) = f(d)f(D).$$

Υπόδειξη: θεωρήστε την κανονική αναπαράσταση των m, n.

2.20. Ορίζουμε $\nu(1) = 0$ και για $n > 1$ ορίζουμε $\nu(n)$ να είναι το πλήθος των διακεκριμένων πρώτων παραγόντων του n. Αποδείξτε ότι αν $f = \mu * \nu$ τότε $f(n) = 0$ ή $f(n) = 1$ για κάθε $n \in \mathbb{N}$.

2.21. Για κάθε $x \in \mathbb{R}$, $x > 0$ ορίζουμε $\varphi(x, n)$ να είναι το πλήθος των θετικών ακεραίων $k \leqslant x$ που είναι σχετικώς πρώτοι προς τον n. Παρατηρήστε ότι $\varphi(n, n) = \varphi(n)$. Αποδείξτε ότι

$$\varphi(x,n) = \sum_{d|n} \mu(d) \left[\frac{x}{d}\right] \qquad \text{και} \qquad \sum_{d|n} \varphi\left(\frac{x}{d}, \frac{n}{d}\right) = [x].$$

2.22. Αν $f(n), g(n) > 0$ για κάθε n και $a(n) \in \mathbb{R}$, $a(1) \neq 0$, αποδείξτε ότι

$$g(n) = \prod_{d|n} f(d)^{a(n/d)} \qquad \text{αν και μόνο αν} \qquad f(n) = \prod_{d|n} g(d)^{b(n/d)},$$

όπου $b = a^{-1}$ είναι η αντίστροφη Dirichlet της a.

2.23. Έστω $P(n)$ το γινόμενο των θετικών ακεραίων που είναι μικρότεροι ή ίσοι από n και σχετικώς πρώτοι προς τον n. Αποδείξτε ότι

$$P(n) = n^{\varphi(n)} \prod_{d|n} \left(\frac{d!}{d^d}\right)^{\mu(n/d)}.$$

2.24. Η συνάρτηση J_k του Jordan γενικεύει τη συνάρτηση φ του Euler και ορίζεται από την

$$J_k(n) = n^k \prod_{p|n} \left(1 - \frac{1}{p^k}\right).$$

Αποδείξτε ότι

$$J_k(n) = \sum_{d|n} \mu(d) \left(\frac{n}{d}\right)^k \qquad \text{και} \qquad n^k = \sum_{d|n} J_k(d).$$

2.25. Έστω $f(n)$ πολλαπλασιαστική συνάρτηση. Αποδείξτε ότι

$$f^{-1}(p^2) = f(p)^2 - f(p^2)$$

για κάθε πρώτο p. Αποδείξτε επίσης ότι η f είναι πλήρως πολλαπλασιαστική αν και μόνο αν $f^{-1}(p^k) = 0$ για κάθε πρώτο p και κάθε ακέραιο $k \geqslant 2$.

2.26. (α) Έστω $f \neq 0$ πλήρως πολλαπλασιαστική συνάρτηση. Αποδείξτε ότι

$$(*) \qquad (f \cdot g)^{-1} = f \cdot g^{-1}$$

για κάθε αριθμητική συνάρτηση g με $g(1) \neq 0$.

(β) Αποδείξτε ότι αν η f είναι πολλαπλασιαστική και η $(*)$ ισχύει για την $g = \mu^{-1}$, τότε η f είναι πλήρως πολλαπλασιαστική.

2.27. Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει η ανισότητα

$$\sigma(n) \leqslant n(1 + \ln n).$$

2.28. Αποδείξτε ότι για κάθε φυσικό αριθμό n ισχύουν οι ανισότητες

$$\frac{1}{2} < \frac{\varphi(n)\sigma(n)}{n^2} \leqslant 1.$$

Αποδείξτε επίσης ότι για κάθε $n \in \mathbb{N}$ ισχύει η ανισότητα

$$\varphi(n) > \frac{n}{2(1+\ln n)}.$$

2.29. Αποδείξτε ότι για κάθε $k \in \mathbb{N}$ και κάθε $C > 0$ υπάρχει $n \in \mathbb{N}$ τέτοιος ώστε

$$d(n) > C(\ln n)^k.$$

2.30. Αποδείξτε ότι για κάθε $\varepsilon > 0$ υπάρχει σταθερά $C(\varepsilon) > 0$ τέτοια ώστε

$$d(n) \leqslant C(\varepsilon)n^{\varepsilon}$$

για κάθε $n \in \mathbb{N}$. Δηλαδή, το πλήθος των διαιρετών του n «φράσσεται» από n^{ε}.

ΚΕΦΑΛΑΙΟ 3

Μέσοι όροι αριθμητικών συναρτήσεων

3.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα μελετήσουμε τους μέσους όρους μιας αριθμητικής συνάρτησης f. Αυτοί ορίζονται από τη σχέση
$$\overline{f}(n) = \frac{1}{n}\sum_{k=1}^{n} f(k).$$
Ο λόγος για τον οποίο μελετάμε τους αριθμητικούς μέσους $\overline{f}(n)$ είναι γιατί, γενικά, η ακολουθία $\overline{f}(n)$ συμπεριφέρεται πιο ομαλά από την $f(n)$ όταν το n είναι μεγάλο.

Για να μελετήσουμε τους αριθμητικούς μέσους οποιασδήποτε συνάρτησης f, χρειάζεται να μελετήσουμε τα μερικά αθροίσματα
$$\sum_{k=1}^{n} f(k).$$
Μερικές φορές είναι βολικό να αντικαταστήσουμε τον άνω δείκτη n με τυχόντα θετικό πραγματικό αριθμό x και αντί για τα μερικά αθροίσματα να θεωρήσουμε αθροίσματα της μορφής
$$\sum_{k\leqslant x} f(k).$$
Σε αυτό το άθροισμα καταλαβαίνουμε ότι ο δείκτης k μεταβάλλεται από 1 έως $[x]$, όπου $[x]$ είναι ο μεγαλύτερος ακέραιος που είναι μικρότερος ή ίσος από x. Αν $0 < x < 1$ τότε το άθροισμα είναι κενό και του αντιστοιχίζουμε την τιμή 0. Στόχος μας είναι να προσδιορίσουμε τη συμπεριφορά αυτού του αθροίσματος, βλέποντάς το ως συνάρτηση του x, ιδιαίτερα όταν ο x είναι μεγάλος.

Ολοκληρώνουμε αυτήν την εισαγωγή με τους ακόλουθους ορισμούς.

Ορισμός 3.1.1. Έστω a πραγματικός αριθμός και $g(x)$ μια πραγματική συνάρτηση τέτοια ώστε $g(x) > 0$ αν $x \geqslant a$. Γράφοντας
$$f(x) = O(g(x))$$

εννοούμε ότι ο λόγος $f(x)/g(x)$ είναι φραγμένος για $x \geqslant a$. Δηλαδή, υπάρχει μια σταθερά $M > 0$ τέτοια ώστε

$$|f(x)| \leqslant Mg(x) \quad \text{για κάθε } x \geqslant a.$$

Μερικές φορές χρησιμοποιούμε επίσης τον συμβολισμό

$$f(x) \ll g(x)$$

εννοώντας ότι $f(x) = O(g(x))$.

Παράδειγμα 3.1.2. Η συνάρτηση $x^2 = O(x^3)$ όταν ο x είναι μεγάλος. Η συνάρτηση $x^n = O(e^x)$ για κάθε θετικό ακέραιο n.

Ορισμός 3.1.3. Αν

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1,$$

τότε λέμε ότι η $f(x)$ είναι ασυμπτωτική προς την $g(x)$ όταν $x \to \infty$, και γράφουμε

$$f(x) \sim g(x) \quad \text{όταν } x \to \infty.$$

3.2 Άθροιση κατά μέρη και ο τύπος άθροισης Euler-Maclaurin

Θεώρημα 3.2.1. *Έστω $a(n)$ μια αριθμητική συνάρτηση και έστω*

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

Έστω $0 \leqslant y < x$ πραγματικοί αριθμοί και f μια πραγματική συνάρτηση με συνεχή παράγωγο στο $[y, x]$. Τότε

$$\sum_{y<n\leqslant x} a(n)f(n) = f(x)A(x) - f(y)A(y) - \int_y^x A(t)f'(t)dt. \tag{3.2.1}$$

Απόδειξη. Παρατηρούμε ότι

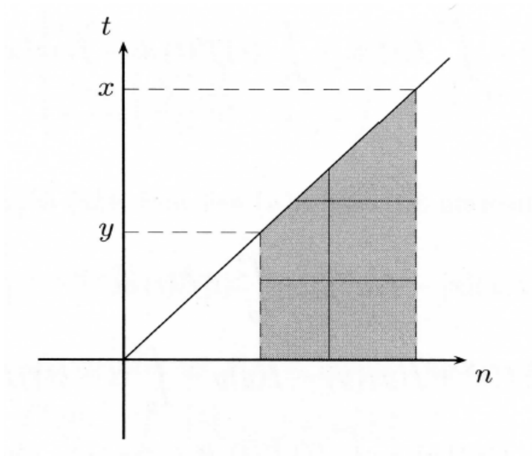
$$\begin{aligned}
\int_y^x A(t)f'(t)dt &= \int_y^x \sum_{n\leqslant t} a(n)f'(t)dt \\
&= \int_y^x \sum_{n\leqslant x} \mathbf{1}_{\{n\leqslant t\}}(n,t)a(n)f'(t)dt \\
&= \sum_{n\leqslant x} a(n) \int_y^x \mathbf{1}_{\{n\leqslant t\}}(n,t)f'(t)dt \\
&= \sum_{n\leqslant y} a(n) \int_y^x f'(t)dt + \sum_{y<n\leqslant x} a(n) \int_n^x f'(t)dt \\
&= \left(\sum_{n\leqslant y} a(n)\right)(f(x) - f(y)) + \left(\sum_{y<n\leqslant x} a(n)\right)(f(x) - f(n)) \\
&= \left(\sum_{n\leqslant x} a(n)\right) f(x) - \left(\sum_{n\leqslant y} a(n)\right) f(y) - \sum_{n<y\leqslant x} a(n)f(n).
\end{aligned} \tag{3.2.2}$$

Συνεπώς,

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

που είναι το ζητούμενο. □

Παρατήρηση 3.2.2. Μια ερμηνεία για την εναλλαγή του ολοκληρώματος και του αθροίσματος δίνεται από το παρακάτω σχήμα. Παρατηρήστε ότι για σταθερό t, το άθροισμα είναι πάνω από όλους τους $n \leqslant t$ (θεωρήστε την κατακόρυφη ευθεία). Για σταθερό n, ολοκληρώνουμε από το y ως το x αν $n < y$ και από το n ως το x αν $n \geqslant y$ (κοιτάξτε τις δύο οριζόντιες ευθείες στο σκιασμένο χωρίο).



Σχήμα 3.1: Διάγραμμα για τα όρια της ολοκλήρωσης στην (3.2.2)

Όταν $y = 1$, έχουμε

$$\sum_{1<n\leqslant x} a(n)f(n) = A(x)f(x) - A(1)f(1) - \int_1^x A(t)f'(t)dt.$$

Όμως

$$\begin{aligned}\sum_{1<n\leqslant x} a(n)f(n) + A(1)f(1) &= \sum_{1<n\leqslant x} a(n)f(n) + a(1)f(1)\\ &= \sum_{n\leqslant x} a(n)f(n).\end{aligned}$$

Συνεπώς, έχουμε την ακόλουθη ειδική περίπτωση:

Πόρισμα 3.2.3. *Έστω $a(n)$ μια αριθμητική συνάρτηση και έστω*

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

Έστω $x > 1$ και f μια πραγματική συνάρτηση με συνεχή παράγωγο στο $[1, x]$. Τότε,

$$\sum_{n \leqslant x} a(n)f(n) = A(x)f(x) - \int_1^x A(t)f'(t)dt. \tag{3.2.3}$$

Θεωρούμε τώρα την ειδική περίπτωση όπου $a(n) = u(n) = 1$.

Θεώρημα 3.2.4 (ο τύπος άθροισης Euler-Maclaurin)**.** *Έστω x και y πραγματικοί αριθμοί τέτοιοι ώστε $0 < y < x$ και $f(x)$ μια πραγματική συνάρτηση με συνεχή παράγωγο στο $[y, x]$. Τότε*

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

Απόδειξη. Από το Θεώρημα 3.2.1 με $a(n) = 1$ και $A(x) = [x]$, βλέπουμε ότι

$$\begin{aligned}
\sum_{y < n \leqslant x} f(n) &= f(x)[x] - f(y)[y] - \int_y^x [t]f'(t)dt \\
&= f(x)x - \{x\}f(x) + \{y\}f(y) - f(y)y - \int_y^x (t - \{t\})f'(t)dt \\
&= -\{x\}f(x) + \{y\}f(y) + \int_y^x \{t\}f'(t)dt + f(x)x - f(y)y - \int_y^x tf'(t)dt \\
&= \{x\}f(x) + \{y\}f(y) + \int_y^x \{t\}f'(t)dt + \int_y^x f(t)dt.
\end{aligned}$$

□

Πόρισμα 3.2.5. *Έστω f μια πραγματική συνάρτηση με συνεχή παράγωγο στο $[1, x]$. Τότε,*

$$\sum_{n \leqslant x} f(n) = \int_1^x f(t)dt + \int_1^x \{t\}f'(t)dt + f(1) - f(x)\{x\}.$$

Απόδειξη. Θέτουμε $y = 1$ στο Θεώρημα 3.2.4 και έχουμε

$$\sum_{1 < n \leqslant x} f(n) = \int_1^x f(t)dt + \int_1^x \{t\}f'(t)dt - f(x)\{x\}.$$

Προσθέτοντας τον $f(1)$ και στα δύο μέλη αυτής της ισότητας έχουμε το ζητούμενο, αφού

$$\sum_{n \leqslant x} f(n) = f(1) + \sum_{1 < n \leqslant x} f(n).$$

□

3.3 Κάποιοι στοιχειώδεις ασυμπτωτικοί τύποι

Ορισμός 3.3.1. Για κάθε πραγματικό αριθμό $s > 1$, ορίζουμε τη συνάρτηση ζήτα του Riemann ως εξής:

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

Ορισμός 3.3.2. Η σταθερά του Euler γ ορίζεται από την

$$\gamma := \lim_{n\to\infty}\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}-\ln n\right).$$

Θεώρημα 3.3.3. *Αν $x \geqslant 1$, τότε:*

(α) $\sum\limits_{n\leqslant x}\frac{1}{n} = \ln x+\gamma+O\left(\frac{1}{x}\right)$.

(β) *Αν $s>0$ και $s\neq 1$ τότε*

$$\sum_{n\leqslant x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s}+C(s)+O(x^{-s}),$$

όπου

$$C(s)=\begin{cases}\zeta(s) & ,\ \textit{αν } s>1\\ \lim_{x\to\infty}\left(\sum_{n\leqslant x}\frac{1}{n^s}-\frac{x^{1-s}}{1-s}\right) & ,\ \textit{αν } 0<s<1\end{cases}.$$

(γ) *Αν $s>1$ τότε*

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

(δ) *Αν $\alpha\geqslant 0$ τότε*

$$\sum_{n\leqslant x}n^\alpha = \frac{x^{\alpha+1}}{\alpha+1}+O(x^\alpha).$$

Απόδειξη. Για να αποδείξουμε το (α) θέτουμε αρχικά $f(t)=1/t$ στο Πόρισμα 3.2.5 και έχουμε

$$\begin{aligned}\sum_{n\leqslant x}\frac{1}{n} &= \int_1^x\frac{dt}{t}-\int_1^x\frac{\{t\}}{t^2}dt+1-\frac{\{x\}}{x}\\ &=\ln x-\int_1^x\frac{\{t\}}{t^2}dt+1+O\left(\frac{1}{x}\right)\\ &=\ln x+1-\int_1^\infty\frac{\{t\}}{t^2}+\int_x^\infty\frac{\{t\}}{t^2}dt+O\left(\frac{1}{x}\right).\end{aligned}$$

Το γενικευμένο ολοκλήρωμα

$$\int_1^\infty\frac{\{t\}}{t^2}dt$$

υπάρχει διότι φράσσεται από το

$$\int_1^\infty\frac{1}{t^2}dt.$$

Επιπλέον,

$$0\leqslant\int_x^\infty\frac{\{t\}}{t^2}dt\leqslant\int_x^\infty\frac{1}{t^2}dt=\frac{1}{x},$$

άρα η τελευταία ισότητα παίρνει τη μορφή

$$\sum_{n\leqslant x}\frac{1}{n}=\ln x+C+O\left(\frac{1}{x}\right),$$

όπου

$$C := 1 - \int_1^{\infty} \frac{\{t\}}{t^2} dt.$$

Αφήνοντας το $x \to \infty$ βλέπουμε ότι

$$C = \lim_{x\to\infty} \left(\sum_{n\leqslant x} \frac{1}{n} - \ln x \right)$$

και ειδικότερα

$$C = \lim_{N\to\infty} \left(\sum_{n\leqslant N} \frac{1}{n} - \ln N \right) = \gamma,$$

οπότε έχουμε αποδείξει το (α).

Για να αποδείξουμε το (β), χρησιμοποιούμε το ίδιο επιχείρημα με την

$$f(x) = x^{-s},$$

όπου $s > 0$, $s \neq 1$. Ο τύπος άθροισης Euler-Maclaurin μας δίνει ότι

$$\sum_{n\leqslant x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} - \frac{1}{1-s} + 1 - s \int_1^{\infty} \frac{\{t\}}{t^{s+1}} dt + O(x^{-s}).$$

Συνεπώς,

$$\sum_{n\leqslant x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + C(s) + O(x^{-s}), \tag{3.3.1}$$

όπου

$$C(s) = 1 - \frac{1}{1-s} - s \int_1^{\infty} \frac{\{t\}}{t^{s+1}} dt.$$

Αν $s > 1$ τότε το αριστερό μέλος της (3.3.1) συγκλίνει στον $\zeta(s)$ καθώς το x συγκλίνει στο ∞ και οι x^{1-s} και x^{-s} συγκλίνουν στο 0. Άρα

$$C(s) = \zeta(s)$$

αν $s > 1$. Αν $0 < s < 1$ τότε

$$\lim_{x\to\infty} \frac{1}{x^s} = 0$$

και η (3.3.1) δείχνει ότι

$$C(s) = \lim_{x\to\infty} \left(\sum_{n\leqslant x} \frac{1}{n^s} - \frac{x^{1-s}}{1-s} \right)$$

το οποίο ολοκληρώνει την απόδειξη του (β).

Για να δείξουμε το (γ), χρησιμοποιούμε το (β) με $s > 1$ και παίρνουμε

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

αφού $x^{-s} \leqslant x^{1-s}$.

Τέλος, για να δείξουμε το (δ), χρησιμοποιούμε τον τύπο άθροισης Euler-Maclaurin με $f(t) = t^\alpha$ και παίρνουμε

$$\begin{aligned}\sum_{n\leqslant x} n^\alpha &= \int_1^x t^\alpha dt + \alpha\int_1^x t^{\alpha-1}\{t\}dt + 1 - \{x\}x^\alpha \\ &= \frac{x^{\alpha+1}}{\alpha+1} - \frac{1}{\alpha+1} + O\left(\alpha\int_1^x t^{\alpha-1}dt\right) + O(x^\alpha) \\ &= \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha).\end{aligned}$$

□

3.4 Η συνάρτηση διαιρετών και η μέθοδος της υπερβολής του Dirichlet

Ορισμός 3.4.1. Θέτουμε $d(1) = 1$ και για κάθε θετικό ακέραιο $n > 1$ ορίζουμε $d(n)$ να είναι το πλήθος των διαιρετών του n.

Σημειώνουμε ότι

$$d(n) = \sum_{d|n} \mathbf{1}$$

άρα

$$d = u * u, \tag{3.4.1}$$

όπου u η συνάρτηση που ορίστηκε στον Ορισμό 2.4.3. Σε αυτή την παράγραφο αποδεικνύουμε τον ασυμπτωτικό τύπο του Dirichlet για τα μερικά αθροίσματα της συνάρτησης διαιρετών $d(n)$.

Θα βασιστούμε στον γενικό τύπο του ακόλουθου θεωρήματος.

Θεώρημα 3.4.2. *Έστω f και g δύο αριθμητικές συναρτήσεις. Ορίζουμε*

$$F(x) = \sum_{n\leqslant x} f(n) \quad \text{και} \quad G(x) = \sum_{n\leqslant x} g(n).$$

Τότε, για κάθε $1 \leqslant y \leqslant x$ έχουμε

$$\sum_{n\leqslant x}(f*g)(n) = \sum_{d\leqslant y} g(d)F\left(\frac{x}{d}\right) + \sum_{m\leqslant \frac{x}{y}} f(m)G\left(\frac{x}{m}\right) - F\left(\frac{x}{y}\right)G(y).$$

Απόδειξη. Αρχικά παρατηρούμε ότι

$$\sum_{n\leqslant x}(f*g)(n) = \sum_{md\leqslant x} f(m)g(d).$$

Στη συνέχεια, για $y \leqslant x$, βλέπουμε ότι

$$\begin{aligned}\sum_{md\leqslant x} f(m)g(d) &= \sum_{\substack{md\leqslant x\\ d\leqslant y}} f(m)g(d) + \sum_{\substack{md\leqslant x\\ d>y}} f(m)g(d)\\ &= \sum_{d\leqslant y} g(d)\sum_{m\leqslant \frac{x}{d}} f(m) + \sum_{m\leqslant \frac{x}{y}} f(m)\sum_{y<d\leqslant \frac{x}{m}} g(d)\\ &= \sum_{d\leqslant y} g(d)F\left(\frac{x}{d}\right) + \sum_{m\leqslant \frac{x}{y}} f(m)\left[G\left(\frac{x}{m}\right) - G(y)\right]\\ &= \sum_{d\leqslant y} g(d)F\left(\frac{x}{d}\right) + \sum_{m\leqslant \frac{x}{y}} f(m)G\left(\frac{x}{m}\right) - \left(\sum_{m\leqslant \frac{x}{y}} f(m)\right)G(y)\\ &= \sum_{d\leqslant y} g(d)F\left(\frac{x}{d}\right) + \sum_{m\leqslant \frac{x}{y}} f(m)G\left(\frac{x}{m}\right) - F\left(\frac{x}{y}\right)G(y).\end{aligned}$$

Αυτό αποδεικνύει το ζητούμενο. □

Τώρα θέτουμε $f = g = u$. Τότε

$$f * g = u * u = d$$

από την (3.4.1). Παρατηρούμε ότι $F(x) = [x] = G(x)$. Έστω $y = \sqrt{x}$. Τότε, από το Θεώρημα 3.4.2,

$$\begin{aligned}\sum_{n\leqslant x} d(n) &= \sum_{d\leqslant \sqrt{x}} F\left(\frac{x}{d}\right) + \sum_{m\leqslant \sqrt{x}} G\left(\frac{x}{m}\right) - [\sqrt{x}]^2\\ &= 2\sum_{n\leqslant \sqrt{x}} \left[\frac{x}{n}\right] - [\sqrt{x}]^2\\ &= 2x\sum_{n\leqslant \sqrt{x}} \frac{1}{n} - 2\sum_{n\leqslant \sqrt{x}} \left\{\frac{x}{n}\right\} - (\sqrt{x} - \{\sqrt{x}\})^2\\ &= 2x\sum_{n\leqslant \sqrt{x}} \frac{1}{n} - x + O(\sqrt{x})\end{aligned}$$

Χρησιμοποιώντας το Θεώρημα 3.3.3 (α), συμπεραίνουμε ότι

$$\begin{aligned}\sum_{n\leqslant x} d(n) &= 2x\left(\ln(\sqrt{x}) + \gamma + O\left(\frac{1}{\sqrt{x}}\right)\right) - x + O(\sqrt{x})\\ &= x\ln x + (2\gamma - 1)x + O(\sqrt{x}).\end{aligned}$$

Δηλαδή, έχουμε αποδείξει το εξής.

Θεώρημα 3.4.3. *Για κάθε $x \geqslant 1$,*

$$\sum_{n\leqslant x} d(n) = x\ln x + (2\gamma - 1)x + O(\sqrt{x}),$$

όπου γ είναι η σταθερά του Euler.

Ως πόρισμα, παίρνουμε ότι

$$\overline{d}(n) \sim \ln n. \tag{3.4.2}$$

Με άλλα λόγια, η μέση τάξη μεγέθους της $d(n)$ είναι $\ln n$.

Μπορούμε να δείξουμε την ασυμπτωτική εκτίμηση (3.4.2) χωρίς να χρησιμοποιήσουμε τη μέθοδο της υπερβολής του Dirichlet. Όμως, η εκτίμηση που θα παίρναμε για το σφάλμα θα ήταν $O(x)$ αντί για $O(\sqrt{x})$ (δείτε το Πρόβλημα 2 της Άσκησης 3.6).

Παρατήρηση 3.4.4. Η εκτίμηση του σφάλματος στο Θεώρημα 3.4.3 μπορεί να βελτιωθεί. Το 1903 ο Voronoi απέδειξε το φράγμα $O(x^{1/3}\ln x)$. Το 1928, ο J. G. van der Corput βελτίωσε την εκτίμηση του σφάλματος σε $O(x^{27/82})$ χρησιμοποιώντας τη μέθοδο των εκθετικών αθροισμάτων. Το 1988, οι H. Iwaniec και C. J. Mozzochi έδειξαν ότι το σφάλμα είναι $O(x^{7/22})$. Το καλύτερο γνωστό φράγμα για το σφάλμα οφείλεται στον M. N. Huxley, ο οποίος απέδειξε το 2003 ότι το σφάλμα είναι $O(x^{131/416}(\ln x)^{26947/8320})$.

Μια χρήσιμη ειδική περίπτωση του Θεωρήματος 3.4.2 είναι η ακόλουθη.

Θεώρημα 3.4.5. *Έστω f και g δύο αριθμητικές συναρτήσεις. Ορίζουμε*

$$F(x) = \sum_{n\leqslant x} f(n) \quad \textit{και} \quad G(x) = \sum_{n\leqslant x} g(n).$$

Τότε, για κάθε $x \geqslant 1$ έχουμε

$$\sum_{n\leqslant x}(f*g)(n) = \sum_{d\leqslant x} g(d)F\left(\frac{x}{d}\right) = \sum_{m\leqslant x} f(m)G\left(\frac{x}{m}\right).$$

Απόδειξη. Θυμηθείτε ότι, για κάθε $1 \leqslant y \leqslant x$,

$$\sum_{n\leqslant x}(f*g)(n) = \sum_{d\leqslant y} g(d)F\left(\frac{x}{d}\right) + \sum_{m\leqslant \frac{x}{y}} f(m)G\left(\frac{x}{m}\right) - F\left(\frac{x}{y}\right)G(y)$$

από το Θεώρημα 3.4.2. Επιλέγοντας $y = x$ και παρατηρώντας ότι $f(1)G(x) - F(1)G(x) = 0$ παίρνουμε την

$$\sum_{n\leqslant x}(f*g)(n) = \sum_{d\leqslant x} g(d)F\left(\frac{x}{d}\right).$$

Επιλέγοντας $y = 1$ και παρατηρώντας ότι $g(1)F(x) - F(x)G(1) = 0$ παίρνουμε την

$$\sum_{n\leqslant x}(f*g)(n) = \sum_{m\leqslant x} f(m)G\left(\frac{x}{m}\right).$$

Αυτό δείχνει το θεώρημα. □

Τώρα επιλέγουμε $g(n) = 1$ στο Θεώρημα 3.4.5. Τότε $(f*g)(n) = \sum_{d|n} f(d)$ και $G(x) = [x]$, άρα παίρνουμε αμέσως το εξής.

Θεώρημα 3.4.6. *Έστω f μια αριθμητική συνάρτηση και $F(x) = \sum_{n\leqslant x} f(n)$. Για κάθε $x \geqslant 1$ έχουμε*

$$\sum_{n\leqslant x}\sum_{d|n} f(d) = \sum_{n\leqslant x} f(n)\left[\frac{x}{n}\right] = \sum_{n\leqslant x} F\left(\frac{x}{n}\right).$$

Παίρνοντας $f(n) = \mu(n)$ και $f(n) = |lambda(n)$ στο Θεώρημα 3.4.6 έχουμε τους ακόλουθους τύπους.

Θεώρημα 3.4.7. *Για κάθε* $x \geqslant 1$ *ισχύουν οι*

$$\sum_{n\leqslant x} \mu(n) \left[\frac{x}{n}\right] = 1 \tag{3.4.3}$$

και

$$\sum_{n\leqslant x} \Lambda(n) \left[\frac{x}{n}\right] = \ln([x]!). \tag{3.4.4}$$

Απόδειξη. Από το Θεώρημα 3.4.6 έχουμε

$$\sum_{n\leqslant x} \mu(n) \left[\frac{x}{n}\right] = \sum_{n\leqslant x} \sum_{d|n} \mu(d) = \sum_{n\leqslant x} \left[\frac{1}{n}\right] = 1$$

και

$$\sum_{n\leqslant x} \Lambda(n) \left[\frac{x}{n}\right] = \sum_{n\leqslant x} \sum_{d|n} \Lambda(d) = \sum_{n\leqslant x} \ln n = \ln([x]!).$$

□

Χρησιμοποιώντας τον τύπο της άθροισης κατά μέρη μπορούμε να βρούμε την ασυμπτωτική συμπεριφορά του $\ln([x]!)$.

Θεώρημα 3.4.8. *Αν* $x \geqslant 2$ *τότε*

$$\ln([x]!) = x\ln x - x + O(\ln x). \tag{3.4.5}$$

Συνεπώς,

$$\sum_{n\leqslant x} \Lambda(n) \left[\frac{x}{n}\right] = x\ln x - x + O(\ln x). \tag{3.4.6}$$

Απόδειξη. Παίρνοντας $f(t) = \ln t$ στο Πόρισμα 3.2.5 έχουμε

$$\begin{aligned}\sum_{n\leqslant x} \ln n &= \int_1^x \ln t\, dt + \int_1^x \frac{t-[t]}{t}\, dt - (x-[x])\ln x\\ &= x\ln x - x + 1 + \int_1^x \frac{t-[t]}{t}\, dt + O(\ln x).\end{aligned}$$

Αυτό αποδεικνύει την (3.4.5) αφού

$$\int_1^x \frac{t-[t]}{t}\, dt = O\left(\int_1^x \frac{1}{t}\, dt\right) = O(\ln x),$$

και η (3.4.6) έπεται από την (3.4.4). □

Από τις (3.4.3) και (3.4.4) προκύπτουν δύο ενδιαφέρουσες εφαρμογές.

Θεώρημα 3.4.9. *Για κάθε $x \geqslant 1$ έχουμε*

$$\left|\sum_{n\leqslant x}\frac{\mu(n)}{n}\right| \leqslant 1 \tag{3.4.7}$$

με ισότητα μόνο αν $x < 2$.

Απόδειξη. Αν $x < 2$ τότε έχουμε μόνο έναν όρο στο άθροισμα, $\mu(1) = 1$. Υποθέτουμε λοιπόν ότι $x \geqslant 2$. Από την (3.4.3) έχουμε

$$1 = \sum_{n\leqslant x}\mu(n)\left[\frac{x}{n}\right] = \sum_{n\leqslant x}\left(\frac{x}{n} - \left\{\frac{x}{n}\right\}\right) = x\sum_{n\leqslant x}\frac{\mu(n)}{n} - \sum_{n\leqslant x}\mu(n)\left\{\frac{x}{n}\right\}.$$

Αφού $0 \leqslant \{y\} < 1$, συμπεραίνουμε ότι

$$\begin{aligned} x\left|\sum_{n\leqslant x}\frac{\mu(n)}{n}\right| &= \left|1 + \sum_{n\leqslant x}\mu(n)\left\{\frac{x}{n}\right\}\right| \leqslant 1 + \sum_{n\leqslant x}\left\{\frac{x}{n}\right\} \\ &= 1 + \{x\} + \sum_{2\leqslant n\leqslant x}\left\{\frac{x}{n}\right\} < 1 + \{x\} + [x] - 1 = x. \end{aligned}$$

Διαιρώντας με x παίρνουμε την (3.4.7) με γνήσια ανισότητα. □

Σημείωση. Όπως θα δούμε αργότερα το θεώρημα των πρώτων αριθμών προκύπτει από τον ισχυρισμό ότι η σειρά

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

συγκλίνει και έχει άθροισμα 0. Το Θεώρημα 3.4.9 δείχνει ότι η παραπάνω σειρά έχει φραγμένα μερικά αθροίσματα.

Θεώρημα 3.4.10 (ταυτότητα του Legendre)**.** *Για κάθε $x \geqslant 1$ ισχύει ότι*

$$[x]! = \prod_{p\leqslant x} p^{\alpha(p)}, \tag{3.4.8}$$

όπου το γινόμενο είναι πάνω από όλους τους πρώτους $p \leqslant x$ και

$$\alpha(p) = \sum_{m=1}^{\infty}\left[\frac{x}{p^m}\right]. \tag{3.4.9}$$

Σημείωση. Το άθροισμα $\sum_{m=1}^{\infty}\left[\frac{x}{p^m}\right]$ είναι πεπερασμένο αφού $[x/p^m] = 0$ αν $p^m > x$.

Απόδειξη. Αφού $\Lambda(n) = 0$ αν ο n δεν είναι δύναμη πρώτου και $\Lambda(p^m) = \ln p$, απότην (3.4.4) παίρνουμε

$$\ln([x]!) = \sum_{n\leqslant x}\Lambda(n)\left[\frac{x}{n}\right] = \sum_{p\leqslant x}\sum_{m=1}^{\infty}\left[\frac{x}{p^m}\right]\ln p = \sum_{p\leqslant x}\alpha(p)\ln p,$$

και έπεται η (3.4.9). □

3.5 Μια εφαρμογή της μεθόδου της υπερβολής

Σε αυτή την ενότητα συζητάμε το ακόλουθο ενδιαφέρον ερώτημα:

> «Αν επιλέξουμε τυχαία δύο θετικούς ακεραίους, ποια είναι η πιθανότητα να είναι σχετικώς πρώτοι;»

Για να απαντήσουμε αυτό το ερώτημα, αποδεικνύουμε πρώτα το εξής αποτέλεσμα:

Θεώρημα 3.5.1. *Έστω $\varphi(n)$ η συνάρτηση φ του Euler. Για κάθε $x>1$,*

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

Απόδειξη. Υπενθυμίζουμε ότι $\varphi=\mu*N$. Εφαρμόζοντας το Θεώρημα 3.4.2 με $f=N$ και $g=\mu$, βλέπουμε ότι, για κάθε $1\leqslant y\leqslant x$,

$$\sum_{n\leqslant x}\varphi(n)=\sum_{n\leqslant x}(\mu*N)(n)=\sum_{n\leqslant y}\mu(n)F\left(\frac{x}{n}\right)+\sum_{m\leqslant \frac{x}{y}}N(m)G\left(\frac{x}{m}\right)-F\left(\frac{x}{y}\right)G(y),$$

όπου

$$F(x)=\sum_{n\leqslant x}N(n)=\frac{x^2}{2}+O(x)$$

και

$$G(x)=\sum_{n\leqslant x}\mu(n)=O(x).$$

Συνεπώς,

$$\sum_{n\leqslant x}\varphi(n)=\frac{1}{2}\sum_{n\leqslant y}\mu(n)\left(\frac{x}{n}\right)^2+O\left(\left|\sum_{n\leqslant y}\mu(n)\right|x\right)+O\left(\sum_{m\leqslant\frac{x}{y}}m\frac{x}{m}\right)+O\left(\left(\frac{x}{y}\right)^2y\right).$$

Θέτοντας $y=\sqrt{x}$ και χρησιμοποιώντας τα απλά φράγματα

$$\left|\sum_{n\leqslant\sqrt{x}}\mu(n)\right|\leqslant\sqrt{x}\qquad\text{και}\qquad\sum_{m\leqslant\sqrt{x}}m\frac{x}{m}\leqslant x^{3/2},$$

συμπεραίνουμε ότι

$$\sum_{n\leqslant x}\varphi(n)=\frac{x^2}{2}\sum_{n\leqslant\sqrt{x}}\frac{\mu(n)}{n^2}+O(x^{3/2}).\tag{3.5.1}$$

Στο Θεώρημα 6.3.1 θα δείξουμε ότι

$$\zeta(2)\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}=1.$$

Αυτό συνεπάγεται ότι

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}=\frac{6}{\pi^2},$$

αφού $\zeta(2) = \pi^2/6$. Θεωρώντας γνωστή αυτή την ταυτότητα, βλέπουμε ότι

$$\begin{aligned}\sum_{n \leqslant \sqrt{x}} \frac{\mu(n)}{n^2} &= \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} - \sum_{n > \sqrt{x}} \frac{\mu(n)}{n^2} \\ &= \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} + O\left(\sum_{n > \sqrt{x}} \frac{1}{n^2} \right) \\ &= \frac{6}{\pi^2} + O(x^{-1/2}),\end{aligned}$$

όπου η τελευταία ισότητα έπεται από το Θεώρημα 3.3.3 (γ). Αντικαθιστώντας αυτή την ισότητα στην (3.5.1), ολοκληρώνουμε την απόδειξη του θεωρήματος. □

Τώρα, έστω T ένας θετικός ακέραιος και

$$S_T = \{(m,n) : 1 \leqslant m \leqslant T, 1 \leqslant n \leqslant T\}.$$

Τότε, το συνολικό πλήθος N_T των στοιχείων του S_T που ικανοποιούν την $(m,n) = 1$ δίνεται από την

$$\begin{aligned}\sum_{\substack{n \leqslant T, m \leqslant T \\ (m,n)=1}} \mathbf{1} &= 1 + 2 \sum_{\substack{m \leqslant T, n < m \\ (m,n)=1}} \mathbf{1} \\ &= 1 + 2 \sum_{m \leqslant T} \varphi(m) = \frac{6}{\pi^2} T^2 + O(T^{3/2}).\end{aligned}$$

Αυτό αποδεικνύει ότι η πιθανότητα να είναι σχετικώς πρώτοι δύο θετικοί ακέραιοι που επιλέγονται τυχαία είναι ίση με

$$\lim_{T \to \infty} \frac{N_T}{T^2} = \frac{6}{\pi^2}.$$

3.6 Ασκήσεις

3.1. Χρησιμοποιώντας τον τύπο άθροισης Euler-Maclaurin αποδείξτε ότι για κάθε $x \geqslant 3$,

$$\sum_{n \leqslant x} (\ln n)^2 = x(\ln x)^2 - 2x \ln x + 2x + O((\ln x)^2).$$

3.2. Χρησιμοποιώντας τον τύπο άθροισης Euler-Maclaurin αποδείξτε ότι για κάθε $x \geqslant 2$,

$$\sum_{n \leqslant x} \frac{\ln n}{n} = \frac{1}{2}(\ln x)^2 + A + O\left(\frac{\ln x}{x}\right)$$

όπου A είναι μια σταθερά, και

$$\sum_{n \leqslant x} \frac{1}{n \ln n} = \ln(\ln x) + B + O\left(\frac{1}{x \ln x}\right)$$

όπου B είναι μια σταθερά.

3.3. Αποδείξτε ότι για κάθε αριθμητική συνάρτηση $f(n)$,

$$\sum_{n\leqslant x}\sum_{d|n} f(d) = \sum_{d\leqslant x} f(d)\left[\frac{x}{d}\right]. \tag{3.6.1}$$

Συμπεράνατε ότι

$$\sum_{n\leqslant x} d(n) = x\ln x + O(x).$$

3.4. Χρησιμοποιήστε τον τύπο άθροισης κατά μέρη για να δείξετε ότι

$$\sum_{n\leqslant x}\frac{d(n)}{n} = \frac{1}{2}(\ln x)^2 + 2\gamma(\ln x) + O(1)$$

όπου γ είναι η σταθερά του Euler.

3.5. Αν $x\geqslant 2$ και $\alpha>1$, αποδείξτε ότι

$$\sum_{n\leqslant x}\frac{d(n)}{n^\alpha} = \frac{x^{1-\alpha}\ln x}{1-\alpha} + \zeta(\alpha)^2 + O(x^{1-\alpha}).$$

3.6. Έστω n ένας θετικός ακέραιος. Συμβολίζουμε με $\omega(n)$ το πλήθος των διακεκριμένων πρώτων διαιρετών του n. Πιο συγκεκριμένα,

$$\omega(n) = \begin{cases} 0 & ,\ \text{αν } n=1 \\ k & ,\ \text{αν } n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k} \end{cases}.$$

Αποδείξτε ότι, για κάθε $x\geqslant 3$,

$$\sum_{n\leqslant x} 2^{\omega(n)} = \frac{6}{\pi^2}x\ln x + O(x).$$

3.7. Αν $x\geqslant 2$ αποδείξτε ότι

$$\sum_{n\leqslant x}\mu(n)\left[\frac{x}{n}\right]^2 = \frac{x^2}{\zeta(2)} + O(x\ln x)$$

και

$$\sum_{n\leqslant x}\frac{\mu(n)}{n}\left[\frac{x}{n}\right] = \frac{x}{\zeta(2)} + O(\ln x).$$

3.8. Έστω $x\geqslant 1$. Αποδείξτε ότι

$$\sum_{n\leqslant x}\varphi(n) = \frac{1}{2}\sum_{n\leqslant x}\mu(n)\left[\frac{x}{n}\right]^2 + \frac{1}{2}.$$

Από αυτή τη σχέση συμπεράνατε ότι για κάθε $x\geqslant 2$

$$\sum_{n\leqslant x}\varphi(n) = \frac{1}{2}\frac{x^2}{\zeta(2)} + O(x\ln x).$$

3.9. Έστω $x\geqslant 1$. Αποδείξτε ότι

$$\sum_{n\leqslant x}\frac{\varphi(n)}{n} = \sum_{n\leqslant x}\frac{\mu(n)}{n}\left[\frac{x}{n}\right].$$

Από αυτή τη σχέση συμπεράνατε ότι για κάθε $x \geqslant 2$

$$\sum_{n \leqslant x} \frac{\varphi(n)}{n} = \frac{x}{\zeta(2)} + O(\ln x).$$

3.10 Αν $x \geqslant 2$ αποδείξτε ότι

$$\sum_{n \leqslant x} \frac{\varphi(n)}{n^2} = \frac{1}{\zeta(2)} \ln x + \frac{\gamma}{\zeta(2)} - A + O\left(\frac{\ln x}{x}\right),$$

όπου γ είναι η σταθερά του Euler και

$$A = \sum_{n=1}^{\infty} \frac{\mu(n) \ln n}{n^2}.$$

3.11. Έστω n τυχών θετικός ακέραιος και

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

Υποθέτουμε γνωστή την

$$\zeta(2) = \pi^2/6.$$

(α) Αποδείξτε ότι αν $n \geqslant 2$ τότε

$$\frac{\sigma(n)}{n} < \frac{n}{\varphi(n)} < \frac{\pi^2}{6} \frac{\sigma(n)}{n}.$$

(β) Έστω $x \geqslant 2$. Αποδείξτε ότι

$$\sum_{n \leqslant x} \frac{n}{\varphi(n)} = O(x).$$

3.12. Αποδείξτε ότι

$$\sum_{n \leqslant x} \sigma(n) \sim c_1 x^2$$

για κάποια σταθερά $c_1 > 0$.

3.13. Αν $x \geqslant 2$ αποδείξτε ότι

$$\sum_{n \leqslant x} \frac{1}{\varphi(n)} = O(\ln x).$$

3.14. Έστω $k \in \mathbb{N}$. Αποδείξτε ότι

$$\sum_{\substack{n \leqslant x \\ (n,k)=1}} \frac{1}{n} \sim \frac{\varphi(k)}{k} \ln x.$$

Γενικότερα, αν $s > 0$ να βρείτε ασυμπτωτικό τύπο για τα μερικά αθροίσματα

$$\sum_{\substack{n \leqslant x \\ (n,k)=1}} \frac{1}{n^s}.$$

3.15. Αποδείξτε ότι

$$\sum_{\substack{n \leqslant x \\ (n,k)=1}} n = \frac{\varphi(k)}{2k} x^2 + O(d(k)x),$$

όπου $d(k)$ είναι το πλήθος των θετικών διαιρετών του k.

3.16. Αποδείξτε ότι
$$\sum_{n\leqslant x}\lambda(n)\left[\frac{x}{n}\right]=[\sqrt{x}].$$

3.17. Έστω $k\geqslant 2$. Ορίζουμε $q_k(n)=1$ αν ο n δεν διαιρείται με k-οστή δύναμη πρώτου και $q_k(n)=0$ αλλιώς. Αποδείξτε ότι
$$\sum_{n\leqslant x}q_k(n)=c_kx+O(x^{1/k}),$$
όπου
$$c_k=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^k}.$$

3.18. Ορίζουμε $M(x)=\sum_{n\leqslant x}\mu(n)$. Αποδείξτε ότι
$$\sum_{n\leqslant x}M\left(\frac{x}{n}\right)=1.$$

3.19. Αποδείξτε ότι, για κάθε $x\geqslant 2$,
$$\sum_{p\leqslant x}\left[\frac{x}{p}\right]\ln p=x\ln x+O(x).$$

3.20. Έστω $(a_n)_{n=1}^{\infty}$ ακολουθία μιγαδικών αριθμών. Ορίζουμε
$$M(x)=\frac{1}{x}\sum_{n\leqslant x}a_n\qquad\text{και}\qquad L(x)=\frac{1}{\ln x}\sum_{n\leqslant x}\frac{a_n}{n}.$$

(α) Αν υπάρχει το $\lim_{x\to\infty}M(x)=\ell$, αποδείξτε ότι υπάρχει και το $\lim_{x\to\infty}L(x)$ και είναι επίσης ίσο με ℓ.

(β) Δώστε παράδειγμα ακολουθίας $a_n\in[0,1]$ για την οποία υπάρχει το $\lim_{x\to\infty}L(x)$ αλλά δεν υπάρχει το $\lim_{x\to\infty}M(x)$.

ΚΕΦΑΛΑΙΟ 4

Στοιχειώδη αποτελέσματα για την κατανομή των πρώτων

4.1 Εισαγωγή

Ορισμός 4.1.1. Για κάθε πραγματικό αριθμό $x > 0$ συμβολίζουμε με $\pi(x)$ το πλήθος των πρώτων αριθμών που δεν ξεπερνούν τον x.

Η συμπεριφορά της $\pi(x)$ ως συνάρτησης του x έχει μελετηθεί από πολλούς μαθηματικούς ήδη από τον δέκατο όγδοο αιώνα. Εξετάζοντας πίνακες πρώτων αριθμών, οι Gauss (1792) και Legendre (1798) οδηγήθηκαν στην εικασία ότι

$$\pi(x) \sim \frac{x}{\ln x}. \tag{4.1.1}$$

Η εικασία αυτή αποδείχθηκε για πρώτη φορά, ανεξάρτητα, από τους Hadamard και de la Vallée Poussin το 1896, και είναι τώρα γνωστή ως το *θεώρημα των πρώτων αριθμών*. Διατυπώνουμε το θεώρημα ως εξής:

Θεώρημα 4.1.2 (θεώρημα των πρώτων αριθμών)**.** *Έστω x ένας θετικός πραγματικός αριθμός και $\pi(x)$ το πλήθος των πρώτων που είναι μικρότεροι από x. Τότε*

$$\pi(x) \sim \frac{x}{\ln x}.$$

Οι αποδείξεις που έχουν δοθεί για το θεώρημα των πρώτων αριθμών συχνά ταξινομούνται ως στοιχειώδεις ή αναλυτικές. Οι αποδείξεις των Hadamard και de la Vallée Poussin είναι αναλυτικές, αφού χρησιμοποιούν τη θεωρία των μιγαδικών συναρτήσεων και ιδιότητες της ζήτα συνάρτησης του Riemann $\zeta(s)$ (δείτε τον Ορισμό 3.1.1 για τον ορισμό του $\zeta(s)$ όταν $s \in \mathbb{R}$ και $s > 1$). Στοιχειώδεις αποδείξεις ανακαλύφθηκαν γύρω στο 1949 από τους Selberg και Erdős. Σε αυτές τις αποδείξεις δεν εμπλέκονται η $\zeta(s)$ και η θεωρία μιγαδικών συναρτήσεων, και αυτός είναι ο λόγος για τον χαρακτηρισμό «στοιχειώδεις».

Υπάρχουν κι άλλες στοιχειώδεις αποδείξεις του θεωρήματος των πρώτων αριθμών, μεταγενέστερες αυτών που έδωσαν οι Selberg και Erdős, μία από τις οποίες οφείλεται στον Hildebrand. Η απόδειξη αυτή (1986) βασίζεται στην απόδειξη μιας πρότασης ισοδύναμης με το θεώρημα των πρώτων αριθμών που σχετίζεται με τη μέση τιμή της $\mu(n)$. Θα αποδείξουμε αυτή την ισοδύναμη διατύπωση του θεωρήματος των πρώτων αριθμών στην Παράγραφο 4.5.

Σε αυτό το κεφάλαιο αποδεικνύουμε κάποιες βασικές ιδιότητες της $\pi(x)$ και παρουσιάζουμε κάποιες προτάσεις που είναι ισοδύναμες με το θεώρημα των πρώτων αριθμών. Χρησιμοποιούμε επίσης τα αποτελέσματα που συζητάμε σε αυτό το κεφάλαιο για να μελετήσουμε το αίτημα του Bertrand, το οποίο ισχυρίζεται ότι για κάθε $n \geqslant 2$ υπάρχει πρώτος ανάμεσα στους n και $2n$.

4.2 Η συνάρτηση $\psi(x)$

Υπενθυμίζουμε τον ορισμό της συνάρτησης του Mangoldt (δείτε την Άσκηση 2.1).

Ορισμός 4.2.1. Για κάθε ακέραιο $n \geqslant 1$ ορίζουμε

$$\Lambda(n) = \begin{cases} \ln p & , \text{ αν } n = p^m \text{ για κάποιον } p \text{ και κάποιον } m \geqslant 1 \\ 0 & , \text{ αλλιώς} \end{cases}.$$

Ορισμός 4.2.2. Για κάθε πραγματικό αριθμό $x \geqslant 1$ ορίζουμε

$$\psi(x) = \sum_{n \leqslant x} \Lambda(n) = \sum_{p^m \leqslant x} \ln p.$$

Θεώρημα 4.2.3. *Υπάρχουν απόλυτες θετικές σταθερές c_1 και c_2 τέτοιες ώστε*

$$c_1 x \leqslant \psi(x) \leqslant c_2 x.$$

Απόδειξη. Για κάθε $x \geqslant 4$ θέτουμε

$$S = \sum_{n \leqslant x} \ln n - 2 \sum_{n \leqslant x/2} \ln n.$$

Από το Θεωρημα 3.2.4 με $f(n) = \ln n$, βλέπουμε ότι

$$\sum_{n \leqslant x} \ln n = \int_1^x \ln t \, dt + \int_1^x \{t\} \frac{1}{t} dt - \{x\} \ln x + \{y\} \ln y \tag{4.2.1}$$

$$= x \ln x - x + O(\ln x). \tag{4.2.2}$$

Από αυτή τη σχέση έπεται ότι

$$S = x \ln 2 + O(\ln x).$$

Συνεπώς, υπάρχει $x_0 \geqslant 4$ τέτοιος ώστε

$$\frac{x}{2} \leqslant S \leqslant x \tag{4.2.3}$$

για κάθε $x \geqslant x_0 \geqslant 4$. Τώρα, αφού (δείτε την Άσκηση 2.1)

$$\ln n = \sum_{d \mid n} \Lambda(d),$$

βλέπουμε ότι

$$\begin{aligned} S &= \sum_{n\leqslant x}\sum_{d|n}\Lambda(d) - 2\sum_{n\leqslant x/2}\sum_{d|n}\Lambda(d) \\ &= \sum_{d\leqslant x}\Lambda(d)\left[\frac{x}{d}\right] - 2\sum_{d\leqslant x/2}\Lambda(d)\left[\frac{x}{2d}\right] \\ &= \sum_{d\leqslant x/2}\Lambda(d)\left\{\left[\frac{x}{d}\right] - 2\left[\frac{x}{2d}\right]\right\} + \sum_{x/2<d\leqslant x}\Lambda(d)\left[\frac{x}{d}\right]. \end{aligned}$$

Άρα,

$$S = \sum_{d\leqslant x/2}\Lambda(d)\varrho_d + \sum_{x/2<d\leqslant x}\Lambda(d)\left[\frac{x}{d}\right],$$

όπου

$$\varrho_d = \left[\frac{x}{d}\right] - 2\left[\frac{x}{2d}\right]. \tag{4.2.4}$$

Τώρα, εάν

$$\frac{x}{2} < d \leqslant x,$$

έχουμε

$$\left[\frac{x}{d}\right] = 1.$$

Συνεπώς, μπορούμε να απλοποιήσουμε τον δεύτερο όρο στο δεξιό μέλος της (4.2.4) και προκύπτει ότι

$$S = \sum_{d\leqslant x/2}\Lambda(d)\varrho_d + \sum_{x/2<d\leqslant x}\Lambda(d). \tag{4.2.5}$$

Παρατηρούμε τώρα ότι $\varrho_d = 0$ ή 1, αφού

$$[y] - 2[y/2] = 0 \ \text{ ή } \ 1.$$

Χρησιμοποιώντας την (4.2.5) συμπεραίνουμε ότι

$$S \leqslant \sum_{d\leqslant x/2}\Lambda(d) + \sum_{x/2<d\leqslant x}\Lambda(d) = \sum_{d\leqslant x}\Lambda(d) = \psi(x) \tag{4.2.6}$$

και

$$S \geqslant \sum_{x/2<d\leqslant x}\Lambda(d) = \psi(x) - \psi(x/2). \tag{4.2.7}$$

Από τις (4.2.3) και (4.2.6) έχουμε

$$\psi(x) \geqslant S \geqslant \frac{x}{2}, \qquad x \geqslant x_0.$$

Άρα,

$$\psi(x) \geqslant c_1 x.$$

Για να πάρουμε άνω φράγμα για την $\psi(x)$, αρχικά παρατηρούμε ότι, από τις (4.2.3) και (4.2.7),

$$\psi(x) - \psi(x/2) \leqslant S \leqslant x.$$

Συνεπώς,

$$\begin{aligned}
\psi(x) &\leqslant x + \psi\left(\frac{x}{2}\right), \qquad x \geqslant x_0 \\
&\leqslant x + \frac{x}{2} + \psi\left(\frac{x}{4}\right), \qquad x \geqslant 2x_0 \\
&\vdots \\
&\leqslant x + \frac{x}{2} + \cdots + \frac{x}{2^k} + \psi\left(\frac{x}{2^{k+1}}\right), \qquad \frac{x}{2^{k+1}} < x_0 \leqslant \frac{x}{2^k}.
\end{aligned}$$

Αυτό συνεπάγεται ότι

$$\psi(x) \leqslant 2x + \psi(x_0) \leqslant c_2 x$$

για κάποια θετική πραγματική σταθερά c_2. □

4.3 Οι συναρτήσεις $\vartheta(x)$ και $\pi(x)$

Ορισμός 4.3.1. Για κάθε πραγματικό αριθμό $x \geqslant 1$, ορίζουμε

$$\vartheta(x) = \sum_{p \leqslant x} \ln p.$$

Θεώρημα 4.3.2. *Για κάθε πραγματικό αριθμό $x \geqslant 1$ ισχύει ότι*

$$\vartheta(x) = \psi(x) + O(\sqrt{x}).$$

Απόδειξη. Αρχικά παρατηρούμε ότι η διαφορά των $\psi(x)$ και $\vartheta(x)$ είναι ίση με

$$\begin{aligned}
\psi(x) - \vartheta(x) &= \sum_{\substack{p^m \leqslant x \\ m \leqslant 2}} \ln p \\
&= \sum_{\substack{p^m \leqslant \sqrt{x} \\ m \leqslant 2}} \ln p + \sum_{p \leqslant x^{1/3}} \ln p \sum_{3 \leqslant m \leqslant \frac{\ln x}{\ln p}} \mathbf{1}.
\end{aligned}$$

Συνεπώς,

$$\begin{aligned}
\psi(x) - \vartheta(x) &\leqslant \psi(\sqrt{x}) + \sum_{p \leqslant x^{1/3}} \ln p \, \frac{\ln x}{\ln p} \\
&\ll \sqrt{x} + x^{1/3} \ln x \ll \sqrt{x},
\end{aligned}$$

όπου $f(x) \ll g(x)$ σημαίνει ακριβώς το ίδιο με την $f(x) = O(g(x))$ (δείτε τον Ορισμό 3.1.1). □

Χρησιμοποιώντας τα Θεωρήματα 4.2.3 και 4.3.2, παίρνουμε το ακόλουθο πόρισμα.

Πόρισμα 4.3.3. *Υπάρχουν θετικές πραγματικές σταθερές c_1 και c_2 τέτοιες ώστε, για κάθε $x \geqslant 4$,*

$$c_1 x \leqslant \vartheta(x) \leqslant c_2 x.$$

Μπορούμε τώρα να συγκρίνουμε τις $\vartheta(x)$ και $\pi(x)$, όπου η $\pi(x)$ ορίστηκε στον Ορισμό 4.1.1.

Θεώρημα 4.3.4. *Για κάθε θετικό πραγματικό αριθμό $x \geqslant 4$,*

$$\frac{c_1 x}{\ln x} \leqslant \pi(x) \leqslant \frac{c_2 x}{\ln x}.$$

Απόδειξη. Λόγω του Θεωρήματος 4.3.2 αρκεί να αποδείξουμε ότι

$$\pi(x) = \frac{1}{\ln x}\vartheta(x) + O\left(\frac{x}{\ln^2 x}\right).$$

Παρατηρούμε ότι

$$\pi(x) - \frac{\vartheta(x)}{\ln x} = \sum_{p \leqslant x}\left(1 - \frac{\ln p}{\ln x}\right) = \sum_{p \leqslant x} \ln p \left(\frac{1}{\ln p} - \frac{1}{\ln x}\right). \tag{4.3.1}$$

Αν

$$a(n) = \begin{cases} \ln p & , \text{αν ο } n \text{ είναι κάποιος πρώτος } p \\ 0 & , \text{αλλιώς} \end{cases},$$

τότε από το Πόρισμα 4.3.3,

$$A(t) = \sum_{n \leqslant t} a(n) = \vartheta(t) \ll t.$$

Η τελευταία παράσταση στην (4.3.1) είναι ίση με

$$\begin{aligned} \vartheta(x)\left(\frac{1}{\ln x} - \frac{1}{\ln x}\right) - \int_2^x \vartheta(t)\left(\frac{1}{\ln t} - \frac{1}{\ln x}\right)' dt \\ = \int_2^x \frac{\vartheta(t)}{t \ln^2 t} dt \ll \int_2^x \frac{dt}{\ln^2 t} \\ = \int_2^{\sqrt{x}} \frac{dt}{\ln^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\ln^2 t} \\ \ll \sqrt{x} + \int_{\sqrt{x}}^x \frac{dt}{\ln^2 x} \ll \frac{x}{\ln^2 x}. \end{aligned}$$

□

Ως πορίσματα των Θεωρημάτων 4.3.2 και 4.3.4 έχουμε τα ακόλουθα αποτελέσματα, τις αποδείξεις των οποίων αφήνουμε για τον αναγνώστη.

Πόρισμα 4.3.5. *Το θεώρημα των πρώτων αριθμών*

$$\pi(x) \sim \frac{x}{\ln x}$$

είναι ισοδύναμο με κάθε μία από τις παρακάτω σχέσεις:

(α) $\vartheta(x) \sim x$, *και*

(β) $\psi(x) \sim x$.

Η επόμενη πρόταση συνδέει το θεώρημα των πρώτων αριθμών με την ασυμπτωτική τιμή του n-οστού πρώτου.

Πρόταση 4.3.6. *Έστω p_n ο n-οστός πρώτος αριθμός. Οι ακόλουθες ασυμπτωτικές σχέσεις είναι ισοδύναμες:*

$$\lim_{x\to\infty} \frac{\pi(x)\ln x}{x} = 1. \tag{4.3.2}$$

$$\lim_{x\to\infty} \frac{\pi(x)\ln \pi(x)}{x} = 1. \tag{4.3.3}$$

$$\lim_{x\to\infty} \frac{p_n}{n\ln n} = 1. \tag{4.3.4}$$

Απόδειξη. Υποθέτουμε αρχικά ότι ισχύει η (4.3.2) και θα δείξουμε την (4.3.3). Παίρνοντας λογαρίθμους στην (4.3.2) έχουμε

$$\lim_{x\to\infty} \Big(\ln \pi(x) + \ln\ln x - \ln x\Big) = 0,$$

δηλαδή

$$\lim_{x\to\infty} \Big[\ln x\Big(\frac{\ln \pi(x)}{\ln x} + \frac{\ln\ln x}{\ln x} - 1\Big)\Big] = 0.$$

Αφού $\ln x \to \infty$ όταν $x \to \infty$, έπεται ότι

$$\lim_{x\to\infty} \Big(\frac{\ln \pi(x)}{\ln x} + \frac{\ln\ln x}{\ln x} - 1\Big) = 0,$$

απ' όπου συμπεραίνουμε ότι

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

Συνδυάζοντας με την (4.3.2) παίρνουμε

$$\frac{\pi(x)\ln \pi(x)}{x} = \frac{\pi(x)\ln x}{x} \cdot \frac{\ln \pi(x)}{\ln x} \longrightarrow 1$$

όταν $x \to \infty$.

Υποθέτουμε τώρα ότι ισχύει η (4.3.3). Αν $x = p_n$ τότε $\pi(x) = n$ και

$$\pi(x)\ln \pi(x) = n\ln n.$$

Αφού $p_n \to \infty$, από την (4.3.3) βλέπουμε ότι

$$\lim_{n\to\infty} \frac{n\ln n}{p_n} = \lim_{n\to\infty} \frac{\pi(p_n)\ln \pi(p_n)}{p_n} = 1,$$

δηλαδή ισχύει η (4.3.4).

Ας υποθέσουμε τώρα ότι ισχύει η (4.3.4). Για $x \geqslant 2$ θεωρούμε τον μοναδικό $n \geqslant 1$ για τον οποίο

$$p_n \leqslant x < p_{n+1}.$$

Τότε, $\pi(x) = n$. Διαιρώντας με $n \ln n$ παίρνουμε

$$\frac{p_n}{n \ln n} \leqslant \frac{x}{n \ln n} < \frac{p_{n+1}}{n \ln n} = \frac{p_{n+1}}{(n+1)\ln(n+1)} \cdot \frac{(n+1)\ln(n+1)}{n \ln n}.$$

Αφήνοντας το $n \to \infty$ και χρησιμοποιώντας την (4.3.4) και την $\pi(x) = n$, παίρνουμε

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

Δηλαδή ισχύει η (4.3.3).

Τέλος δείχνουμε ότι η (4.3.3) συνεπάγεται την (4.3.2). Παίρνοντας λογαρίθμους στην (4.3.3) έχουμε

$$\lim_{x\to\infty} \Big(\ln \pi(x) + \ln \ln \pi(x) - \ln x \Big) = 0,$$

δηλαδή

$$\lim_{x\to\infty} \Big[\ln \pi(x) \Big(1 + \frac{\ln \ln \pi(x)}{\ln \pi(x)} - \frac{\ln x}{\ln \pi(x)} \Big) \Big] = 0.$$

Αφού $\ln \pi(x) \to \infty$ όταν $x \to \infty$, έπεται ότι

$$\lim_{x\to\infty} \Big(1 + \frac{\ln \ln \pi(x)}{\ln \pi(x)} - \frac{\ln x}{\ln \pi(x)} \Big) = 0,$$

απ' όπου συμπεραίνουμε ότι

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

Συνδυάζοντας με την (4.3.3) παίρνουμε

$$\frac{\pi(x) \ln x}{x} = \frac{\pi(x) \ln \pi(x)}{x} \cdot \frac{\ln x}{\ln \pi(x)} \longrightarrow 1$$

όταν $x \to \infty$. □

Κλείνουμε αυτή την παράγραφο με μια δεύτερη απόδειξη των εκτιμήσεων του Chebyshev. Η διπλή ανισότητα του Θεωρήματος 4.3.4 είναι ουσιαστικά ισοδύναμη με τον ισχυρισμό ότι υπάρχουν σταθερές $c_1, c_2 > 0$ τέτοιες ώστε, για κάθε $n \geqslant 2$,

$$\frac{c_1 n}{\ln n} \leqslant \pi(n) \leqslant \frac{c_2 n}{\ln n}.$$

Θα αποδείξουμε αυτή την ανισότητα με $c_1 = 1/6$ και $c_2 = 6$.

Θεώρημα 4.3.7. *Για κάθε φυσικό $n \geqslant 2$ έχουμε*

$$\frac{1}{6}\frac{n}{\ln n} < \pi(n) < 6\frac{n}{\ln n}. \tag{4.3.5}$$

Απόδειξη. Αποδεικνύουμε αρχικά ότι, για κάθε $n \geqslant 1$,

$$2^n \leqslant \binom{2n}{n} < 4^n. \tag{4.3.6}$$

Η δεξιά ανισότητα προκύπτει από την παρατήρηση ότι

$$4^n = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} > \binom{2n}{n}.$$

Η αριστερή ανισότητα αποδεικνύεται εύκολα με επαγωγή. Αν υποθέσουμε ότι $\binom{2n}{n} \geqslant 2^n$ τότε

$$\binom{2n+2}{n+1} = \binom{2n}{n} \cdot \frac{(2n+1)(2n+2)}{(n+1)^2} \geqslant 2^n \cdot \frac{2(2n+1)}{n+1} \geqslant 2^n \cdot 2 = 2^{n+1}.$$

Παίρνοντας λογαρίθμους στην (4.3.6) έχουμε την

$$n(\ln 2) < \ln(2n)! - 2\ln n! < n(\ln 4). \tag{4.3.7}$$

Από την ταυτότητα του Legendre (Θεώρημα 3.4.10) έχουμε

$$\ln n! = \sum_{p \leqslant n} \alpha(p) \ln p$$

όπου το άθροισμα είναι πάνω από τους πρώτους που δεν ξεπερνούν τον n και

$$\alpha(p) = \sum_{m=1}^{\left[\frac{\ln n}{\ln p}\right]} \left[\frac{n}{p^m}\right].$$

Έπεται ότι

$$\ln(2n)! - 2\ln n! = \sum_{p \leqslant 2n} \sum_{m=1}^{\left[\frac{\ln 2n}{\ln p}\right]} \left(\left[\frac{2n}{p^m}\right] - 2\left[\frac{n}{p^m}\right] \right) \ln p. \tag{4.3.8}$$

Αφού $[2y] - 2[y] = 0$ ή 1, από την αριστερή ανισότητα στην (4.3.7) παίρνουμε

$$n(\ln 2) \leqslant \sum_{p \leqslant 2n} \left(\sum_{m=1}^{\left[\frac{\ln 2n}{\ln p}\right]} \mathbf{1} \right) \ln p \leqslant \sum_{p \leqslant 2n} \ln(2n) = \pi(2n)\ln(2n).$$

Συνεπώς,

$$\pi(2n) \geqslant \frac{n(\ln 2)}{\ln(2n)} = \frac{2n}{\ln(2n)} \frac{\ln 2}{2} > \frac{1}{4} \frac{2n}{\ln(2n)}, \tag{4.3.9}$$

αφού $\ln 2 > 1/2$. Για τους περιττούς φυσικούς έχουμε

$$\pi(2n+1) \geqslant \pi(2n) > \frac{1}{4} \frac{2n}{\ln(2n)} > \frac{1}{4} \frac{2n}{2n+1} \frac{2n+1}{\ln(2n+1)} \geqslant \frac{1}{6} \frac{2n+1}{\ln(2n+1)},$$

αφού $\frac{2n}{2n+1} \geqslant \frac{2}{3}$. Συνδυάζοντας με την (4.3.9) παίρνουμε

$$\pi(n) > \frac{1}{6} \frac{n}{\ln n}$$

για κάθε $n \geqslant 2$, έχουμε δηλαδή αποδείξει την αριστερή ανισότητα στην (4.3.5).

Για να αποδείξουμε τη δεξιά ανισότητα, επιστρέφουμε στην (4.3.8) και κρατάμε μόνο τον όρο που αντιστοιχεί στον $m = 1$. Οι υπόλοιποι όροι είναι μη αρνητικοί, άρα παίρνουμε

$$\ln(2n)! - 2\ln n! \geqslant \sum_{p\leqslant 2n}\left(\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]\right)\ln p.$$

Για τους πρώτους p που ικανοποιούν την $n < p \leqslant 2n$ έχουμε $[2n/p] - 2[n/p] = 1$, άρα

$$\ln(2n)! - 2\ln n! \geqslant \sum_{n<p\leqslant 2n}\ln p = \vartheta(2n) - \vartheta(n).$$

Άρα, η (4.3.7) μας δίνει

$$\vartheta(2n) - \vartheta(n) < n(\ln 4).$$

Ειδικότερα, αν ο n είναι δύναμη του 2, δηλαδή $n = 2^r$, έχουμε

$$\vartheta(2^{r+1}) - \vartheta(2^r) < 2^r(\ln 4) = 2^{r+1}(\ln 2).$$

Θεωρώντας αυτές τις ανισότητες για $r = 0, 1, \ldots, k$ και προσθέτοντας, στο αριστερό μέλος έχουμε τηλεσκοπικό άθροισμα ενώ στο δεξιό έχουμε γεωμετρική σειρά, και έτσι παίρνουμε

$$\vartheta(2^{k+1}) < 2^{k+2}(\ln 2).$$

Αν, για δοσμένο n, επιλέξουμε k έτσι ώστε $2^k \leqslant n < 2^{k+1}$, τότε παίρνουμε

$$\vartheta(n) \leqslant \vartheta(2^{k+1}) < 2^{k+2}(\ln 2) = (4\ln 2)n.$$

Σταθεροποιούμε $0 < \alpha < 1$ και γράφουμε

$$(\pi(n) - \pi(n^\alpha))\ln(n^\alpha) < \sum_{n^\alpha<p\leqslant n}\ln p \leqslant \vartheta(n) < (4\ln 2)n.$$

Έπεται ότι

$$\begin{aligned}\pi(n) &< \frac{(4\ln 2)n}{\alpha\ln n} + \pi(n^\alpha) < \frac{(4\ln 2)n}{\alpha\ln n} + n^\alpha\\ &= \frac{n}{\ln n}\left(\frac{4\ln 2}{\alpha} + \frac{\ln n}{n^{1-\alpha}}\right).\end{aligned}$$

Παρατηρούμε τώρα ότι η συνάρτηση $f(x) = \ln x/x^{1-\alpha}$ παίρνει τη μέγιστη ιμή της στο $x = e^{\frac{1}{1-\alpha}}$ και αυτή η μέγιστη τιμή είναι ίση με $\frac{1}{e(1-\alpha)}$. Επιλέγοντας $\alpha = 2/3$ και επιστρέφοντας στο τελευταίο μας άνω φράγμα για τον $\pi(n)$, παίρνουμε

$$\pi(n) < \frac{n}{\ln n}\left(6\ln 2 + \frac{\ln n}{n^{1/3}}\right) \leqslant \frac{n}{\ln n}\left(6\ln 2 + \frac{3}{e}\right) < 6\frac{n}{\ln n},$$

δηλαδή έχουμε δείξει και τη δεξιά ανισότητα στην (4.3.5). □

Από το Θεώρημα 4.3.7 μπορούμε να πάρουμε άνω και κάτω φράγματα για το μέγεθος του n-οστού πρώτου.

Θεώρημα 4.3.8. *Για κάθε $n \geqslant 1$, ο n-οστός πρώτος p_n ικανοποιεί τις ανισότητες*

$$\frac{1}{6}n\ln n < p_n < 12\,(n\ln n + \ln(12/e)n)\,. \tag{4.3.10}$$

Απόδειξη. Αν $k = p_n$ τότε $k \geqslant 2$ και $\pi(k) = n$. Από την (4.3.5) έχουμε

$$n = \pi(k) < 6\frac{k}{\ln k} = 6\frac{p_n}{\ln p_n}.$$

Άρα,

$$p_n > \frac{1}{6}n\ln p_n > \frac{1}{6}n\ln n,$$

και έχουμε το κάτω φράγμα στην (4.3.10).

Για το άνω φράγμα, ξεκινάμε πάλι από την (4.3.5) και γράφουμε

$$n = \pi(k) > \frac{1}{6}\frac{k}{\ln k} = \frac{1}{6}\frac{p_n}{\ln p_n},$$

απ' όπου βλέπουμε ότι

$$p_n < 6n\ln p_n. \tag{4.3.11}$$

Χρησιμοποιώντας την $x \leqslant (2/e)\sqrt{x}$, η οποία ισχύει για κάθε $x \geqslant 1$, έχουμε $\ln p_n \leqslant (2/e)\sqrt{p_n}$, άρα η (4.3.11) μας δίνει

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

Έπεται ότι

$$\frac{1}{2}\ln p_n < \ln n + \ln(12/e),$$

και εισάγοντας αυτή την ανισότητα στην (4.3.11) παίρνουμε

$$p_n < 12\,(n\ln n + \ln(12/e)n)\,,$$

που είναι το άνω φράγμα στην (4.3.10). □

Σημείωση. Από το άνω φράγμα της (4.3.10) και το γεγονός ότι η σειρά $\sum_{n=2}^{\infty}\frac{1}{n\ln n}$ αποκλίνει, συμπεραίνουμε και πάλι ότι η σειρά $\sum_{n=1}^{\infty}\frac{1}{p_n}$ αποκλίνει.

4.4 Οι εκτιμήσεις του Mertens

Σε αυτή την παράγραφο αποδεικνύουμε ότι υπάρχουν άπειροι πρώτοι αποδεικνύοντας ότι η $\sum\limits_{p\leqslant x}\frac{1}{p}$ αποκλίνει.

Θεώρημα 4.4.1 (οι εκτιμήσεις του Mertens)**.** *Έστω x ένας θετικός πραγματικός αριθμός μεγαλύτερος από 1. Έχουμε*

(α) $\sum\limits_{n\leqslant x}\frac{\Lambda(n)}{n} = \ln x + O(1)$, (β) $\sum_{p\leqslant x} \frac{\ln p}{p} = \ln x + O(1)$,

(γ) $\sum_{p\leqslant x} \frac{1}{p} = \ln\ln x + A + O\left(\frac{1}{\ln x}\right)$, *και*

(δ) (Θεώρημα του Mertens) $\prod_{p\leqslant x}\left(1-\frac{1}{p}\right) = \frac{e^{-A}}{\ln x}\left(1+O\left(\frac{1}{\ln x}\right)\right)$, *όπου* A *είναι μια σταθερά.*

Απόδειξη. (α) Αρχικά γράφουμε

$$\begin{aligned}\sum_{n\leqslant x}\frac{\Lambda(n)}{n} &= \sum_{n\leqslant x}\left\{\Lambda(n)\frac{1}{x}\left(\left[\frac{x}{n}\right]+O(1)\right)\right\}\\ &= \frac{1}{x}\sum_{n\leqslant x}\Lambda(n)\left[\frac{x}{n}\right] + O\left(\frac{1}{x}\sum_{n\leqslant x}\Lambda(n)\right).\end{aligned}$$

Από την (3.6.1) βλέπουμε ότι

$$\sum_{n\leqslant x}\Lambda(n)\left[\frac{x}{n}\right] = \sum_{n\leqslant x}(\Lambda * u)(n).$$

Άρα, χρησιμοποιώντας τις (2.7.1) και (4.2.1) συμπεραίνουμε ότι

$$\begin{aligned}\sum_{n\leqslant x}\frac{\Lambda(n)}{n} &= \frac{1}{x}\sum_{n\leqslant x}(\Lambda * u)(n) + O(1)\\ &= \frac{1}{x}\sum_{n\leqslant x}\ln n + O(1)\\ &= \ln x + O(1).\end{aligned}$$

(β) Παρατηρούμε ότι

$$\begin{aligned}0 \leqslant \sum_{n\leqslant x}\frac{\Lambda(n)}{n} - \sum_{p\leqslant x}\frac{\ln p}{p} &= \sum_{p\leqslant\sqrt{x}}\ln p\sum_{2\leqslant m\leqslant\frac{\ln x}{\ln p}}\frac{1}{p^m}\\ &\ll \sum_{p\leqslant\sqrt{x}}\frac{\ln p}{p^2} \ll 1.\end{aligned}$$

Άρα,

$$\sum_{p\leqslant x}\frac{\ln p}{p} = \ln x + O(1).$$

(γ) Θέτουμε

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

όπου

$$a(n) = \begin{cases}\frac{\ln p}{p} & , \text{ αν ο } n \text{ είναι κάποιος πρώτος } p\\ 0 & , \text{ αλλιώς}\end{cases}.$$

Τότε, έχουμε ότι

$$\sum_{p\leqslant x}\frac{1}{p}=\sum_{p\leqslant x}\left(\frac{\ln p}{p}\right)\left(\frac{1}{\ln p}\right) \tag{4.4.1}$$
$$=A(x)\frac{1}{\ln x}-\int_2^x A(t)\left(\frac{1}{\ln t}\right)'dt$$
$$=\frac{A(x)}{\ln x}+\int_2^x\frac{A(t)}{t\ln^2 t}dt.$$

Από το Θεώρημα 4.4.1 (β) βλέπουμε ότι

$$A(t)=\ln t+R(t),$$

με

$$R(t)\ll 1,\qquad t\geqslant 2. \tag{4.4.2}$$

Χρησιμοποιώντας την (4.4.2) στον τελευταίο όρο της (4.4.1) συμπεραίνουμε ότι

$$\int_2^x\frac{\ln t+R(t)}{t\ln^2 t}dt=\int_2^x\frac{dt}{t\ln t}+\int_2^x\frac{R(t)}{t\ln^2 t}dt \tag{4.4.3}$$
$$=\ln\ln x-\ln\ln 2+\int_2^\infty\frac{R(t)}{t\ln^2 t}dt-\int_x^\infty\frac{R(t)}{t\ln^2 t}dt$$
$$=\ln\ln x-\ln\ln 2+A''+O\left(\frac{1}{\ln x}\right).$$

Αντικαθιστώντας την (4.4.3) στην (4.4.1) ολοκληρώνουμε την απόδειξη του (γ).

(δ) Παρατηρούμε ότι

$$\ln\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)=\sum_{p\leqslant x}\ln\left(1-\frac{1}{p}\right)=\sum_{p\leqslant x}\left(-\frac{1}{p}+r_p\right),$$

όπου

$$r_p=\ln\left(1-\frac{1}{p}\right)+\frac{1}{p}.$$

Άρα,

$$\ln\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)=\sum_{p\leqslant x}r_p-\sum_{p\leqslant x}\frac{1}{p} \tag{4.4.4}$$
$$=-\ln\ln x+A+O\left(\frac{1}{\ln x}\right)+\sum_p r_p-\sum_{p>x}r_p.$$

Τώρα,

$$r_p=-\sum_{m=2}^\infty\frac{1}{mp^m}=O\left(\frac{1}{p^2}\right), \tag{4.4.5}$$

αφού για $m\geqslant 1$ και $p\geqslant 2$ ισχύει ότι

$$mp^m\geqslant 2^m.$$

Χρησιμοποιώντας την (4.4.5) στην (4.4.4), συμπεραίνουμε ότι

$$\begin{aligned}\ln\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)&=-\ln\ln x+A'+O\left(\frac{1}{\ln x}\right)+O\left(\sum_{p>x}\frac{1}{p^2}\right)\\&=-\ln\ln x+A'+O\left(\frac{1}{\ln x}\right)+O\left(\frac{1}{x-1}\right)\\&=-\ln\ln x+A'+O\left(\frac{1}{\ln x}\right).\end{aligned}$$

Άρα,

$$\ln\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)=-\ln\ln x+A'+O\left(\frac{1}{\ln x}\right). \tag{4.4.6}$$

Συνθέτοντας με την εκθετική συνάρτηση τα δύο μέλη της (4.4.6), καταλήγουμε στην

$$\begin{aligned}\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)&=\exp\left(-\ln\ln x+A'+O\left(\frac{1}{\ln x}\right)\right)\\&=\frac{e^{A'}}{\ln x}\exp\left(O\left(\frac{1}{\ln x}\right)\right)\\&=\frac{e^{A'}}{\ln x}\left(1+O\left(\frac{1}{\ln x}\right)\right),\end{aligned}$$

διότι $e^t=1+O(t)$ καθώς το $t\to 0^+$. □

Ως εφαρμογή των εκτιμήσεων του Mertens αποδεικνύουμε το επόμενο θεώρημα, που έχει ως πόρισμα το αποτέλεσμα του Chebyshev ότι αν το

$$\lim_{x\to\infty}\frac{\pi(x)\ln x}{x}$$

υπάρχει τότε αναγκαστικά θα είναι ίσο με 1.

Θεώρημα 4.4.2. *Ισχύει ότι*

$$\liminf_{x\to\infty}\frac{\pi(x)\ln x}{x}\leqslant 1\leqslant\limsup_{x\to\infty}\frac{\pi(x)\ln x}{x}.$$

Απόδειξη. Δείχνουμε την αριστερή ανισότητα, η δεξιά αποδεικνύεται με τον ίδιο τρόπο. Θέτουμε

$$\ell:=\liminf_{x\to\infty}\frac{\pi(x)\ln x}{x}.$$

Για τυχόν $0<\varepsilon<\ell$ υπάρχει $x_0=x_0(\varepsilon)\geqslant 2$ τέτοιος ώστε, για κάθε $x\geqslant x_0$,

$$\pi(x)\geqslant(\ell-\varepsilon)\frac{x}{\ln x}.$$

Θεωρούμε την αριθμητική συνάρτηση $a(n)$ με $a(n)=1$ αν ο n είναι πρώτος και $a(n)=0$ αλλιώς. Παρατηρήστε ότι $A(x)=\sum_{n\leqslant x}a(n)=\pi(x)$. Για $x>x_0$ γράφουμε

$$\begin{aligned}\sum_{p\leqslant x}\frac{1}{p} &\geqslant \sum_{x_0<n\leqslant x}a(n)\frac{1}{n}\\ &= \frac{A(x)}{x}-\frac{A(x_0)}{x_0}+\int_{x_0}^{x}A(t)\frac{1}{t^2}dt\\ &= \frac{\pi(x)}{x}-\frac{\pi(x_0)}{x_0}+\int_{x_0}^{x}\pi(t)\frac{1}{t^2}dt\\ &\geqslant \frac{\pi(x)}{x}-\frac{\pi(x_0)}{x_0}+(\ell-\varepsilon)\int_{x_0}^{x}\frac{1}{t\ln t}dt\\ &= O(1/\ln x)-\frac{\pi(x_0)}{x_0}+(\ell-\varepsilon)(\ln\ln x-\ln\ln x_0),\end{aligned}$$

αφού $\pi(x)/x=O(1/\ln x)$ από το Θεώρημα 4.3.4. Από το Θεώρημα 4.4.1 (γ) έχουμε

$$\sum_{p\leqslant x}\frac{1}{p}=\ln\ln x+A+O\left(\frac{1}{\ln x}\right).$$

Συνδυάζοντας τα παραπάνω παίρνουμε

$$\lim_{x\to\infty}\left(\ln\ln x+A-(\ell-\varepsilon)(\ln\ln x-\ln\ln x_0)+\frac{\pi(x_0)}{x_0}\right)\geqslant 0,$$

και διαιρώντας με $\ln\ln x$ έχουμε

$$\lim_{x\to\infty}\left(1+\frac{A}{\ln\ln x}-(\ell-\varepsilon)\left(1-\frac{\ln\ln x_0}{\ln\ln x}\right)+\frac{\pi(x_0)}{x_0\ln\ln x}\right)\geqslant 0,$$

δηλαδή

$$1-(\ell-\varepsilon)\geqslant 0.$$

Αφήνοντας το $\varepsilon\to 0^+$ συμπεραίνουμε ότι $\ell\leqslant 1$. □

Κλείνουμε αυτή την παράγραφο με ένα γενικό «Tauberian θεώρημα» του Shapiro που συνδέει αθροίσματα της μορφής $\sum_{n\leqslant x}a(n)$ με αθροίσματα της μορφής $\sum_{n\leqslant x}a(n)[x/n]$ για τυχούσα μη αρνητική αριθμητική συνάρτηση $a(n)$.

Θεώρημα 4.4.3. *Έστω $a(n)$ μη αρνητική αριθμητική συνάρτηση τέτοια ώστε*

(4.4.7) $$\sum_{n\leqslant x}a(n)\left[\frac{x}{n}\right]=x\ln x+O(x),\qquad x\geqslant 1.$$

Τότε:

(α) *Για κάθε $x\geqslant 1$ ισχύει*

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

(β) *Υπάρχει σταθερά $c_1 > 0$ τέτοια ώστε, για κάθε $x \geqslant 1$,*

$$\sum_{n \leqslant x} a(n) \leqslant c_1 x.$$

(γ) *Υπάρχουν σταθερά $c_2 > 0$ και $x_0 > 0$ τέτοια ώστε, για κάθε $x \geqslant x_0$,*

$$\sum_{n \leqslant x} a(n) \geqslant c_2 x.$$

Σημείωση. Έχουμε ήδη συναντήσει αυτή την κατάσταση με την $\Lambda(n)$. Γνωρίζουμε ότι

$$\sum_{n \leqslant x} \Lambda(n) \left[\frac{x}{n}\right] = \sum_{n \leqslant x} \sum_{d|n} \Lambda(d) = \sum_{n \leqslant x} \ln n = x \ln x - x + O(\ln x),$$

και δείξαμε ότι η

$$\psi(x) = \sum_{n \leqslant x} \Lambda(n)$$

ικανοποιεί την

$$c_2 x \leqslant \psi(x) \leqslant c_1 x$$

για $x \geqslant 1$, όπου $c_1, c_2 > 0$ είναι θετικές σταθερές. Το Θεώρημα 4.4.3 δείχνει ότι υπάρχει ένα πιο γενικό επιχείρημα που συνδέει αυτά τα αποτελέσματα.

Απόδειξη του Θεωρήματος 4.4.3. Θέτουμε

$$S(x) = \sum_{n \leqslant x} a(n) \qquad \text{και} \qquad T(x) = \sum_{n \leqslant x} a(n) \left[\frac{x}{n}\right].$$

Αποδεικνύουμε πρώτα το (β). Για το σκοπό αυτό θα δείξουμε ότι

$$S(x) - S(x/2) \leqslant T(x) - 2T(x/2). \tag{4.4.8}$$

Πράγματι,

$$\begin{aligned} T(x) - 2T(x/2) &= \sum_{n \leqslant x} a(n) \left[\frac{x}{n}\right] - \sum_{n \leqslant x/2} a(n) \cdot 2 \left[\frac{x}{2n}\right] \\ &= \sum_{n \leqslant x/2} a(n) \left(\left[\frac{x}{n}\right] - 2\left[\frac{x}{2n}\right]\right) + \sum_{x/2 < n \leqslant x} a(n) \left[\frac{x}{n}\right]. \end{aligned}$$

Αφού $[2y] - 2[y] = 0$ ή 1 και $a(n) \geqslant 0$, το πρώτο άθροισμα είναι μη αρνητικό, άρα

$$T(x) - 2T(x/2) \geqslant \sum_{x/2 < n \leqslant x} a(n) \left[\frac{x}{n}\right] = \sum_{x/2 < n \leqslant x} a(n) = S(x) - S(x/2),$$

όπου χρησιμοποιήσαμε και το γεγονός ότι $[x/n] = 1$ αν $x/2 < n \leqslant x$. Αυτό αποδεικνύει την (4.4.8). Έχουμε υποθέσει την (4.4.7), άρα

$$T(x) - 2T(x/2) = x \ln x + O(x) - 2\left(\frac{x}{2} \ln \frac{x}{2} + O(x)\right) = O(x).$$

Συνδυάζοντας με την (4.4.8) βλέπουμε ότι υπάρχει σταθερά $K>0$ τέτοια ώστε

$$S(x)-S(x/2)\leqslant Kx$$

για κάθε $x\geqslant 1$. Αντικαθιστώντας το x με $x/2, x/2^2,\ldots$ παίρνουμε τις

$$\begin{aligned}S(x/2)-S(x/2^2)&\leqslant K\frac{x}{2},\\ S(x/2^2)-S(x/2^3)&\leqslant K\frac{x}{2^2},\end{aligned}$$

και ούτω καθεξής. Παρατηρήστε ότι αν $2^n>x$ τότε $x/2^n<1$ άρα $S(x/2^n)=0$. Προσθέτοντας λοιπόν όλες αυτές τις ανισότητες παίρνουμε

$$S(x)\leqslant K\left(x+\frac{x}{2}+\frac{x}{2^2}+\cdots\right)=2Kx.$$

Έτσι έχουμε αποδείξει το (β) με $c_1=2K$.

Αποδεικνύουμε τώρα το (α). Αν γράψουμε $[x/n]=x/n+O(1)$, έχουμε

$$\begin{aligned}T(x)&=\sum_{n\leqslant x}a(n)\left[\frac{x}{n}\right]=\sum_{n\leqslant x}a(n)\left(\frac{x}{n}+O(1)\right)=x\sum_{n\leqslant x}\frac{a(n)}{n}+O\left(\sum_{n\leqslant x}a(n)\right)\\ &=x\sum_{n\leqslant x}\frac{a(n)}{n}+O(x)\end{aligned}$$

από το (β). Συνεπώς,

$$\sum_{n\leqslant x}\frac{a(n)}{n}=\frac{1}{x}T(x)+O(1)=\ln x+O(1).$$

Αυτό αποδεικνύει το (α).

Τέλος, αποδεικνύουμε το (γ). Ορίζουμε

$$A(x)=\sum_{n\leqslant x}\frac{a(n)}{n}.$$

Τότε, από το (α) έχουμε

$$A(x)=\ln x+R(x),$$

και $R(x)=O(1)$, δηλαδή υπάρχει σταθερά $M>0$ τέτοια ώστε $|R(x)|\leqslant M$.

Σταθεροποιούμε $0<\delta<1$ και θεωρούμε τη διαφορά

$$A(x)-A(\delta x)=\sum_{\delta x<n\leqslant x}\frac{a(n)}{n}=\sum_{n\leqslant x}\frac{a(n)}{n}-\sum_{n\leqslant\delta x}\frac{a(n)}{n}.$$

Αν $x\geqslant 1$ και $\delta x\geqslant 1$, τότε εφαρμόζοντας τον ασυμπτωτικό τύπο για την $A(x)$ γράφουμε

$$\begin{aligned}A(x)-A(\delta x)&=\ln x+R(x)-(\ln(\delta x)+R(\delta x))\\ &=\ln\frac{1}{\delta}+R(x)-R(\delta x)\\ &\geqslant\ln\frac{1}{\delta}-|R(x)|-|R(\delta x)|\geqslant\ln\frac{1}{\delta}-2M.\end{aligned}$$

Επιλέγουμε τον δ έτσι ώστε να ικανοποιείται η $\ln\frac{1}{\delta} - 2M = 1$. Δηλαδή, ορίζουμε $\delta = 1/e^{2M+1}$. Τότε, για κάθε $x \geqslant x_0 = \frac{1}{\delta}$ έχουμε

$$A(x) - A(\delta x) \geqslant 1.$$

Παρατηρήστε ότι

$$1 \leqslant A(x) - A(\delta x) = \sum_{\delta x < n \leqslant x} \frac{a(n)}{n} \leqslant \frac{1}{\delta x} \sum_{\delta x < n \leqslant x} a(n) \leqslant \frac{1}{\delta x} \sum_{n \leqslant x} a(n).$$

Άρα,

$$\sum_{n \leqslant x} a(n) \geqslant \delta x$$

για κάθε $x \geqslant 1/\delta$. Δηλαδή, ισχύει το (γ) με $c_2 = \delta$ και $x_0 = 1/\delta$. □

4.5 Το θεώρημα των πρώτων αριθμών και η $M(\mu)$

Ορισμός 4.5.1. Έστω f μια αριθμητική συνάρτηση. Ορίζουμε

$$M(f) = \lim_{x \to \infty} \frac{1}{x} \sum_{n \leqslant x} f(n)$$

αν το όριο στο δεξιό μέλος υπάρχει.

Όπως αναφέραμε στην εισαγωγή, υπάρχουν αρκετές στοιχειώδεις αποδείξεις του θεωρήματος των πρώτων αριθμών. Μία από αυτές τις αποδείξεις βασίζεται στο να δείξουμε ότι $M(\mu) = 0$. Σε αυτήν την παράγραφο θα δείξουμε ότι αν $M(\mu) = 0$ τότε το θεώρημα των πρώτων αριθμών αληθεύει. Αντίστροφα, από το θεώρημα των πρώτων αριθμών έπεται ότι $M(\mu) = 0$.

Θεώρημα 4.5.2. *Το θεώρημα των πρώτων αριθμών είναι ισοδύναμο με τη σχέση*

$$M(\mu) = 0.$$

Απόδειξη. Θα δείξουμε πρώτα ότι το θεώρημα των πρώτων αριθμών συνεπάγεται την $M(\mu) = 0$.

Ορίζουμε

$$M_1(\mu) = \lim_{x \to \infty} \left(\frac{1}{x \ln x} \sum_{n \leqslant x} \mu(n) \ln n \right).$$

Παρατηρούμε ότι

$$M(\mu) = 0 \;\text{ αν και μόνο αν }\; M_1(\mu) = 0, \tag{4.5.1}$$

διότι

$$\frac{1}{x} \sum_{n \leqslant x} \left| \frac{\ln n}{\ln x} - 1 \right| \ll \frac{1}{\ln x}.$$

Υποθέτουμε ότι το θεώρημα των πρώτων αριθμών ισχύει στη μορφή $\vartheta(x) \sim x$.

Παρατηρούμε ότι

$$\sum_{n\leqslant x}\mu(n)\ln n=\sum_{n\leqslant x}\mu(n)\sum_{d|n}\Lambda(d)=\sum_{n\leqslant x}\mu(n)\sum_{p|n}\ln p,$$

όπου χρησιμοποιήσαμε το γεγονός ότι οι όροι που αντιστοιχούν σε n που δεν είναι ελεύθερος τετραγώνων ισούνται με 0. Επιπλέον, η τιμή $\Lambda(d)$ είναι μη μηδενική μόνο όταν ο d είναι δύναμη πρώτου. Όμως, αφού ο n είναι ελεύθερος τετραγώνων, οι διαιρέτες $d \mid n$ που είναι δυνάμεις πρώτων είναι απλώς πρώτοι. Συνεπώς,

$$\sum_{n\leqslant x}\mu(n)\ln n=\sum_{p\leqslant x}\ln p\sum_{\substack{n\leqslant x\\ p|n}}\mu(n)=-\sum_{p\leqslant x}\ln p\sum_{\substack{n'\leqslant x/p\\ p\nmid n'}}(\mu(n')),$$

όπου έχουμε γράψει $n=pn'$. Στη συνέχεια, παρατηρούμε ότι

$$\begin{aligned}\sum_{n\leqslant x}\mu(n)\ln n&=-\sum_{p\leqslant x}\ln p\sum_{n\leqslant x/p}\mu(n)+O\left(\sum_{p\leqslant x}\ln p\sum_{\substack{n\leqslant x/p\\ p|n}}\mathbf{1}\right)\\&=-\sum_{p\leqslant x}\ln p\sum_{n\leqslant x/p}\mu(n)+O\left(x\sum_{p\leqslant x}\frac{\ln p}{p^2}\right)\\&=-\sum_{n\leqslant x}\mu(n)\sum_{p\leqslant x/n}\ln p+O(x)\\&=-\sum_{n\leqslant x}\mu(n)\vartheta\left(\frac{x}{n}\right)+O(x).\end{aligned}$$

Τώρα, γράφουμε

$$\sum_{n\leqslant x}\mu(n)\ln n=-x\sum_{n\leqslant x}\frac{\mu(n)}{n}-\sum_{n\leqslant x}\mu(n)R\left(\frac{x}{n}\right)+O(x),\tag{4.5.2}$$

όπου

$$R(y)=\vartheta(y)-y.$$

Αφού

$$1=\sum_{n\leqslant x}\sum_{d|n}\mu(d)=\sum_{n\leqslant x}\mu(n)\left[\frac{x}{n}\right]=x\sum_{n\leqslant x}\frac{\mu(n)}{n}+O(x),$$

βλέπουμε ότι

$$x\sum_{n\leqslant x}\frac{\mu(n)}{n}=O(x).$$

Συνεπώς, η (4.5.2) γράφεται στη μορφή

$$\sum_{n\leqslant x}\mu(n)\ln n=-\sum_{n\leqslant x}\mu(n)R\left(\frac{x}{n}\right)+O(x).$$

Έπεται ότι

$$\frac{1}{x\ln x}\left|\sum_{n\leqslant x}\mu(n)\ln n\right|\leqslant\frac{1}{x\ln x}\sum_{n\leqslant x}\left|R\left(\frac{x}{n}\right)\right|+O\left(\frac{1}{\ln x}\right).$$

Έστω $\varepsilon > 0$. Από το θεώρημα των πρώτων αριθμών,

$$\lim_{y\to\infty} \frac{R(y)}{y} = 0.$$

Συνεπώς, υπάρχει y_0 τέτοιος ώστε

$$|R(y)| \leqslant \varepsilon y, \qquad y \geqslant y_0.$$

Για $x \geqslant y_0$,

$$\begin{aligned}\sum_{n\leqslant x} \left| R\left(\frac{x}{n}\right)\right| &\leqslant \sum_{n\leqslant x/y_0} \varepsilon \frac{x}{n} + \sum_{x/y_0<n\leqslant x} \max_{y\leqslant y_0} |R(y)| \\ &\leqslant \varepsilon x \ln x + O_\varepsilon(x).\end{aligned}$$

Άρα,

$$\limsup \frac{1}{x\ln x}\left(\sum_{n\leqslant x}\left|R\left(\frac{x}{n}\right)\right|\right) \leqslant \varepsilon.$$

Αυτό αποδεικνύεί ότι το θεώρημα των πρώτων αριθμών συνεπάγεται ότι $M_1(\mu) = 0$. Από την (4.5.1) συμπεραίνουμε ότι $M(\mu) = 0$.

Για να αποδείξουμε το αντίστροφο, γράφουμε

$$\ln n = d(n) - 2C + r(n)$$

όπου $r(n)$ είναι μια αριθμητική συνάρτηση. Έστω $y \geqslant 1$. Από την (4.2.1),

$$\begin{aligned}\sum_{n\leqslant y} r(n) &= \sum_{n\leqslant y}\ln n - \sum_{n\leqslant y} d(n) + 2Cy + O(1) \\ &= y(\ln y - 1) + O(\ln y) - (y\ln y + (2C-1)y + O(\sqrt{y})) + 2Cy + O(1) \\ &= O(\sqrt{y}).\end{aligned} \tag{4.5.3}$$

Κατόπιν, αφού

$$\Lambda = \ln * \mu,$$

συμπεραίνουμε ότι

$$\begin{aligned}\sum_{n\leqslant x}\Lambda(n) &= \sum_{n\leqslant x}(\mu * \ln)(n) \\ &= \sum_{n\leqslant x}(\mu * d) - 2C\left(\sum_{n\leqslant x}\mu * u\right) + \sum_{n\leqslant x}(\mu * r) \\ &= [x] - 2C + \sum_{n\leqslant x}(\mu * r)(n).\end{aligned}$$

Η τελευταία ισότητα ισχύει λόγω της

$$\sum_{n\leqslant x} \mu * u * u = [x].$$

Έτσι, το θεώρημα των πρώτων αριθμών θα προκύψει από την $\psi(x) \sim x$ (δείτε το Πόρισμα 4.3.5) αν δείξουμε ότι

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

Σταθεροποιούμε $y \geqslant 1$ και θεωρούμε $x > y$. Από το Θεώρημα 3.4.2,

$$\begin{aligned} \sum_{n\leqslant x} \mu * r(n) &= \sum_{n\leqslant x} \sum_{d_1 d_2 = n} \mu(d_1) r(d_2) \\ &= \sum_{d_1\leqslant x} \sum_{\substack{d_2\leqslant x \\ d_1 d_2 \leqslant x}} \mu(d_1) r(d_2) \\ &= S_1(x) + S_2(x) - S_3(x), \end{aligned}$$

όπου

$$\begin{aligned} S_1(x) &= \sum_{d_2\leqslant y} \sum_{d_1\leqslant x/d_2} \mu(d_1) r(d_2) \\ S_2(x) &= \sum_{d_1\leqslant x/y} \sum_{d_2\leqslant x/d_1} \mu(d_1) r(d_2) \\ S_3(x) &= \sum_{d_1\leqslant x/y} \sum_{d_2\leqslant y} \mu(d_1) r(d_2). \end{aligned}$$

Έχουμε

$$|S_1(x)| \leqslant \sum_{d_2\leqslant y} |r(d_2)| \left| \sum_{d_1\leqslant x/d_2} \mu(d_1) \right|.$$

Τώρα, χρησιμοποιώντας την υπόθεση ότι

$$M(\mu) = 0,$$

βλέπουμε ότι για κάθε $d_2 \leqslant y$ ισχύει

$$\lim_{x\to\infty} \left| \frac{1}{x} \sum_{d_1\leqslant x/d_2} \mu(d_1) \right| = 0.$$

Από το γεγονός ότι το y είναι σταθερό, άρα το πλήθος των $d_2 \leqslant y$ είναι σταθερό, συμπεραίνουμε ότι

$$\lim_{x\to\infty} S_1(x) = 0.$$

Στη συνέχεια, χρησιμοποιώντας την (4.5.3), βλέπουμε ότι

$$\begin{aligned} |S_2(x)| &\leqslant \sum_{d_1\leqslant x/y} \left| \sum_{d_2\leqslant x/d_1} r(d_2) \right| \leqslant c \sum_{d_1\leqslant x/y} \sqrt{\frac{x}{d_1}} \\ &\leqslant c\sqrt{x} \sum_{d_1\leqslant x/y} \frac{1}{\sqrt{d_1}} \leqslant c\sqrt{x} \left(1 + \int_1^{x/y} \frac{dt}{\sqrt{t}} \right) \leqslant c_1 \frac{x}{\sqrt{y}}. \end{aligned}$$

Τέλος, χρησιμοποιώντας την (4.5.3), βλέπουμε ότι

$$|S_3(x)| \leqslant \frac{x}{y}\left|\sum_{d_2\leqslant y} r(d_2)\right| \leqslant \frac{x}{y}c_2\sqrt{y} = c_2\frac{x}{\sqrt{y}}.$$

Άρα,

$$\limsup_{x\to\infty}\frac{1}{x}\left|\sum_{n\leqslant x}(\mu * r)(n)\right| \leqslant 0 + \frac{c_1}{\sqrt{y}} + \frac{c_2}{\sqrt{y}}.$$

Αφού το y ήταν τυχόν,

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

□

4.6 Το αίτημα του Bertrand

Σε αυτή την παράγραφο θα χρησιμοποιήσουμε τις ιδιότητες των συναρτήσεων $\vartheta(x)$ και $\psi(x)$ για να δώσουμε μια απόδειξη του διάσημου αιτήματος του Bertrand.

Θεώρημα 4.6.1 (αίτημα του Bertrand)**.** *Για κάθε φυσικό $n \geqslant 2$ υπάρχει πρώτος ανάμεσα στον n και τον $2n$.*

Τα περισσότερα βιβλία που συζητούν το Θεώρημα 4.6.1 αποδεικνύουν το αποτέλεσμα ακολουθώντας την προσέγγιση του Erdős. Θα παρουσιάσουμε εδώ αρχικά την απόδειξη του Ramanujan και στη συνέχεια την απόδειξη του Erdős.

Η απόδειξη του Ramanujan μνημονεύεται σε ένα άρθρο του Erdős με τίτλο "Ramanujan and I". Η απόδειξη που έδωσε ο Erdős για το Θεώρημα 4.6.1 δημοσιεύτηκε το 1932 και η πρώτη φορά που ο Erdős άκουσε για τον Ramanujan ήταν όταν ο Kalmar του ζήτησε να κοιτάξει την απόδειξη του Ramanujan γι' αυτό το θεώρημα.

Από τον ορισμό των $\psi(x)$ και $\vartheta(x)$ παρατηρούμε ότι:

Λήμμα 4.6.2. *Για κάθε θετικό πραγματικό αριθμό x,*

$$\psi(x) = \vartheta(x) + \vartheta(\sqrt{x}) + \vartheta(\sqrt[3]{x}) + \cdots . \tag{4.6.1}$$

Στη συνέχεια θα δείξουμε ότι:

Λήμμα 4.6.3.

$$\ln([x]!) = \psi(x) + \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \cdots . \tag{4.6.2}$$

Απόδειξη. Έχουμε

$$\psi(x) = \sum_{n\leqslant x}\Lambda(n),$$

όπου $\Lambda(n)$ είναι η συνάρτηση von Mangoldt. Άρα,

$$\begin{aligned}\sum_{k=1}^{\infty}\psi\left(\frac{x}{k}\right) &= \sum_{k=1}^{\infty}\sum_{n\leqslant\frac{x}{k}}\Lambda(n) = \sum_{\substack{kn\leqslant x\\ k\geqslant 1}}\Lambda(n)\\ &= \sum_{n\leqslant x}\sum_{k\leqslant\frac{x}{n}}\Lambda(n) = \sum_{n\leqslant x}\left[\frac{x}{n}\right]\Lambda(n)\\ &= \sum_{n\leqslant x}\sum_{d|n}\Lambda(d) = \ln[x]!,\end{aligned}$$

όπου οι τελευταίες δύο ισότητες προκύπτουν από την (3.6.1) και την Άσκηση 2.1 (β). □

Στη συνέχεια αποδεικνύουμε κάποιες ισότητες και ανισότητες.

Λήμμα 4.6.4. *Για κάθε θετικό πραγματικό αριθμό x έχουμε*

(4.6.3) $$\psi(x) - 2\psi(\sqrt{x}) = \vartheta(x) - \vartheta(\sqrt{x}) + \vartheta(\sqrt[3]{x}) - \cdots,$$

(4.6.4) $$\ln[x]! - 2\ln[x/2]! = \psi(x) - \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) - \cdots,$$

(4.6.5) $$\psi(x) - 2\psi(\sqrt{x}) \leqslant \vartheta(x) \leqslant \psi(x)$$

και

(4.6.6) $$\psi(x) - \psi\left(\frac{x}{2}\right) \leqslant \ln[x]! - 2\ln[x/2]! \leqslant \psi(x) - \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right).$$

Απόδειξη της (4.6.3). Είναι άμεση συνέπεια της (4.6.1). Ακριβέστερα,

$$\psi(x) - 2\psi(\sqrt{x}) = \sum_{k=1}^{\infty}\vartheta(\sqrt[k]{x}) - 2\sum_{k=1}^{\infty}\vartheta(\sqrt[2k]{x}).$$

Απόδειξη της (4.6.4). Προκύπτει από την (4.6.2). Έχουμε

$$\ln[x]! - 2\ln[x/2]! = \sum_{k=1}^{\infty}\psi\left(\frac{x}{k}\right) - 2\sum_{k=1}^{\infty}\psi\left(\frac{x}{2k}\right).$$

Απόδειξη της (4.6.5). Παρατηρούμε ότι η $\vartheta(x)$ είναι αύξουσα. Συνεπώς, από την (4.6.3),

$$\psi(x) - 2\psi(\sqrt{x}) \leqslant \vartheta(x).$$

Επίσης, από την (4.6.1),

$$\psi(x) \geqslant \vartheta(x).$$

Απόδειξη της (4.6.6). Είναι άμεση συνέπεια της (4.6.4).

Λήμμα 4.6.5. *Έστω x ένας πραγματικός αριθμός. Τότε,*

$$\ln[x]! - 2\ln[x/2]! > \frac{2x}{3} \quad \text{αν } x > 750, \tag{4.6.7}$$

$$\ln[x]! - 2\ln[x/2]! < \frac{3x}{4} \quad \text{αν } x > 0, \tag{4.6.8}$$

$$\psi(x) - \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) > \frac{2x}{3} \quad \text{αν } x > 750, \tag{4.6.9}$$

και

$$\psi(x) - \psi\left(\frac{x}{2}\right) < \frac{3x}{4} \quad \text{αν } x > 0. \tag{4.6.10}$$

Απόδειξη της (4.6.7). Για κάθε πραγματικό αριθμό z ισχύει ότι

$$\Gamma(z) = \lim_{n\to\infty} \frac{(n-1)!n^z}{z(z+1)\cdots(z+n-1)}.$$

Η συνάρτηση $\Gamma(z)$ ικανοποιεί τον γνωστό τύπο του Stirling

$$\ln\Gamma(x) = \ln\sqrt{2\pi} + \left(x - \frac{1}{2}\right)\ln x - x + \frac{\varrho_x}{12x}, \qquad 0 < \varrho_x < 1. \tag{4.6.11}$$

Αφού η $\Gamma(x)$ είναι αύξουσα για $x > 3$, συμπεραίνουμε ότι

$$\ln[x]! - 2\ln[x/2]! \geqslant \ln\Gamma(x) - 2\ln\Gamma\left(\frac{x}{2} + 1\right).$$

Για να αποδείξουμε την (4.6.7), αρκεί να δείξουμε ότι για $x > 750$ ισχύει

$$\ln\Gamma(x) - 2\ln\Gamma\left(\frac{x}{2} + 1\right) > \frac{2x}{3}. \tag{4.6.12}$$

Από την (4.6.11) βλέπουμε ότι

$$\begin{aligned}\ln\Gamma(x) - 2\ln\Gamma\left(\frac{x}{2} + 1\right) &= \ln\sqrt{2\pi} - \left(x - \frac{1}{2}\right)\ln x - x + \frac{\varrho_1}{12x} - 2\ln\sqrt{2\pi} \\ &\quad - 2\left(\frac{x}{2} + \frac{1}{2}\right)\ln\left(\frac{x}{2} + 1\right) + 2\left(\frac{x}{2} + 1\right) - \frac{\varrho_2}{3x+6},\end{aligned}$$

όπου οι ϱ_1, ϱ_2 ανήκουν στο διάστημα $(0,1)$. Απλοποιώντας την παραπάνω ανισότητα, συμπεραίνουμε ότι

$$\ln\Gamma(x) - 2\ln\Gamma\left(\frac{x}{2} + 1\right) > x\ln\left(\frac{2x}{x+2}\right) - 2\ln x.$$

Για $x > 750$ έχουμε

$$x\ln\left(\frac{2x}{x+2}\right) - 2\ln x > \frac{2x}{3}.$$

Αυτό ολοκληρώνει την απόδειξη της (4.6.12).

Απόδειξη της (4.6.8). Η απόδειξη είναι όμοια με αυτήν της (4.6.7). Χρησιμοποιούμε την ανισότητα

$$\ln[x]! - 2\ln[x/2]! \leqslant \ln\Gamma(x+1) - 2\ln\Gamma\left(\frac{x+1}{2}\right)$$

και τον τύπο του Stirling για να συμπεράνουμε ότι (δείτε την Άσκηση 4.8)

$$\ln[x]! - 2\ln[x/2]! \leqslant \frac{3x}{4}$$

για κάθε $x > 0$.

Απόδειξη των (4.6.9) και (4.6.10). Αυτές οι δύο ανισότητες προκύπτουν άμεσα από τις (4.6.6)–(4.6.8).

Λήμμα 4.6.6. *Για κάθε θετικό πραγματικό αριθμό x έχουμε*

$$\psi(x) < \frac{3x}{2} \quad \textit{αν } x > 0 \tag{4.6.13}$$

και

$$\begin{aligned}\psi(x) - \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) &\leqslant \vartheta(x) + 2\psi(\sqrt{x}) - \vartheta\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right)\\ &< \vartheta(x) - \vartheta\left(\frac{x}{2}\right) + \frac{x}{2} + 3\sqrt{x}.\end{aligned} \tag{4.6.14}$$

Απόδειξη της (4.6.13). Για να αποδείξουμε την (4.6.13) χρησιμοποιούμε την (4.6.10) διαδοχικά, αντικαθιστώντας τον x με $x/2, x/4, \ldots$ και προσθέτουμε τα αποτελέσματα. Έτσι βλέπουμε ότι

$$\psi(x) \leqslant \frac{3x}{4}\left(1 + \frac{1}{2} + \cdots\right) < \frac{3x}{2}.$$

Απόδειξη της (4.6.14). Από την (4.6.5) έχουμε ότι

$$\psi(x) - 2\psi(\sqrt{x}) \leqslant \vartheta(x).$$

Άρα,

$$\psi(x) \leqslant \vartheta(x) + 2\psi(\sqrt{x}).$$

Στη συνέχεια, από την (4.6.5),

$$\vartheta(x/2) \leqslant \psi(x/2).$$

Χρησιμοποιώντας τις παραπάνω ανισότητες, συμπεραίνουμε ότι

$$\psi(x) - \psi(x/2) + \psi(x/3) \leqslant \vartheta(x) + 2\psi(\sqrt{x}) - \vartheta(x/2) + \psi(x/3).$$

Για τη δεύτερη ανισότητα, από την (4.6.13) παίρνουμε

$$2\psi(\sqrt{x}) + \psi(x/3) \leqslant 3\sqrt{x} + x/2.$$

Μπορούμε τώρα να αποδείξουμε το αίτημα του Bertrand. Από την (4.6.9),

$$\psi(x) - \psi(x/2) + \psi(x/3) \geqslant \frac{2x}{3}$$

για $x > 750$. Συνεπώς, από την (4.6.14) βλέπουμε ότι

$$\vartheta(x) - \vartheta(x/2) \geqslant \frac{2x}{3} - \frac{x}{2} - 3\sqrt{x},$$

το οποίο σημαίνει ότι υπάρχει πρώτος ανάμεσα στον x και τον $2x$ εάν $x > 750$.

Απομένει τώρα να επαληθεύσουμε ότι το αίτημα του Bertrand ισχύει για $x \leqslant 750$. Αυτό είναι άμεσο και το αφήνουμε ως άσκηση.

Παράδειγμα 4.6.7. Ας υποθέσουμε ότι S είναι ένα σύνολο διαδοχικών ακεραίων το οποίο περιέχει κάποιον πρώτο. Αποδείξτε ότι υπάρχει ακέραιος στο S που είναι σχετικά πρώτος προς όλους τους άλλους ακεραίους στο S. Αντίστροφα, αποδείξτε ότι αν κάθε πεπερασμένο σύνολο διαδοχικών ακεραίων που περιέχει τουλάχιστον έναν πρώτο περιέχει αριθμό που είναι σχετικά πρώτος προς τους υπόλοιπους, τότε το αίτημα του Bertrand ισχύει.

Απόδειξη. Έστω $S := \{n, n+1, \dots, n+k\}$ τυχόν σύνολο διαδοχικών ακεραίων που περιέχει τουλάχιστον έναν πρώτο. Έστω p ο μεγαλύτερος πρώτος στο σύνολο S. Αν $2p \leqslant n+k$, τότε από το αίτημα του Bertrand υπάρχει κάποιος άλλος πρώτος q τέτοιος ώστε $p < q < 2p$ και αυτό αντιφάσκει προς την υπόθεση ότι ο p είναι ο μεγαλύτερος πρώτος στο σύνολο S. Άρα $2p > n+k$ και έπεται ότι ο p είναι σχετικά πρώτος προς όλους τους υπόλοιπους ακεραίους στο S.

Αντίστροφα, έστω $n > 1$ και ας θεωρήσουμε το σύνολο $T = \{2, 3, \dots, 2n\}$. Προφανώς υπάρχει τουλάχιστον ένας πρώτος στο T, άρα από την υπόθεση υπάρχει ακέραιος q που είναι σχετικά πρώτος προς όλους τους ακεραίους στο T. Αυτό συνεπάγεται ότι $2q > 2n$, γιατί αν $2q < 2n$ τότε ο q δεν είναι σχετικά πρώτος προς τον $2q$. Άρα, $n < q < 2n$. Για να αποδείξουμε ότι ο q είναι πρώτος, υποθέτουμε ότι $a \mid q$ και $a \neq 1$. Τότε $a \in T$ και ο a δεν είναι σχετικά πρώτος προς τον q. Αυτό έρχεται σε αντίφαση με την επιλογή του q. Επομένως, ο q πρέπει να είναι πρώτος. Αυτό σημαίνει ότι υπάρχει πρώτος ανάμεσα στον n και τον $2n$, και αφού ο $n > 1$ ήταν τυχών έχουμε αποδείξει το αίτημα του Bertrand. □

Η απόδειξη του Erdős

Συγκεντρώνουμε πρώτα διάφορα βοηθητικά αποτελέσματα που χρησιμοποιούνται στο επιχείρημα του Erdős. Το πρώτο μας λήμμα δίνει κάτω φράγμα για τους κεντρικούς διωνυμικούς συντελεστές.

Λήμμα 4.6.8. *Για κάθε φυσικό αριθμό $n \geqslant 1$ ισχύει η ανισότητα*

$$\frac{4^n}{2n} \leqslant \binom{2n}{n}.$$

Απόδειξη. Από το διωνυμικό ανάπτυγμα έχουμε

$$4^n = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} = 2 + \sum_{k=1}^{2n-1} \binom{2n}{k} \leqslant 2n\binom{2n}{n},$$

διότι ο $\binom{2n}{n}$ είναι ο μεγαλύτερος προσθετέος στο δεξιό μέλος, και το άθροισμα έχει $2n$ προσθετέους. □

Το δεύτερο λήμμα δίνει άνω φράγμα για τις δυνάμεις πρώτων που διαιρούν τους κεντρικούς διωνυμικούς συντελεστές.

Λήμμα 4.6.9. *Για κάθε πρώτο p ορίζουμε $r(p,n)$ τον μεγαλύτερο φυσικό αριθμό r για τον οποίο ο p^r διαιρεί τον $\binom{2n}{n}$. Τότε,*

$$p^{r(p,n)} \leqslant 2n.$$

Απόδειξη. Από την ταυτότητα του Legendre, ο εκθέτης του p στην ανάλυση του $n!$ σε γινόμενο πρώτων παραγόντων ισούται με

$$\sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor,$$

άρα

$$r(p,2n) = \sum_{j=1}^{\infty} \left\lfloor \frac{2n}{p^j} \right\rfloor - 2\sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor = \sum_{j=1}^{\infty} \left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2\left\lfloor \frac{n}{p^j} \right\rfloor \right).$$

Όμως, έχουμε δει ότι κάθε όρος στο τελευταίο άθροισμα είναι είτε ίσος με μηδέν ή 1, και όλοι οι όροι για $j > \log_p(2n)$ μηδενίζονται. Συνεπώς,

$$r(p,n) \leqslant \log_p(2n),$$

και

$$p^{r(p,n)} \leqslant p^{\log_p 2n} = 2n.$$

Αυτό αποδεικνύει το λήμμα. □

Μια βασική ιδέα του Erdös (όπως ισχυρίζεται ο ίδιος) είναι ότι οι πρώτοι p που ικανοποιούν την $\frac{2n}{3} < p \leqslant n$ δεν διαιρούν τον $\binom{2n}{n}$.

Λήμμα 4.6.10. *Αν ο p είναι περιττός και $\frac{2n}{3} < p \leqslant n$ τότε $r(p,n) = 0$.*

Απόδειξη. Υπάρχουν ακριβώς δύο παράγοντες του p στον αριθμητή του κλάσματος $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$, οι οποίοι προέρχονται από τους δύο όρους p και $2p$ στο $(2n)!$, και ομοίως υπάρχουν δύο παράγοντες του p στον παρονομαστή, οι οποίοι οφείλονται στα δύο αντίτυπα του όρου p στο $n!$. Οι παράγοντες αυτοί διαγράφονται, και έτσι δεν υπάρχουν παράγοντες του p στον $\binom{2n}{n}$.

Η υπόθεση $p \geqslant \frac{2n}{3}$ εξασφαλίζει ότι $3p > 2n$ και έτσι ο $3p$ δεν είναι όρος του αριθμητή, και η υπόθεση ότι ο p είναι περιττός εξασφαλίζει ότι ο $2p$ συνεισφέρει μόνο έναν παράγοντα του p στον αριθμητή. □

Στη συνέχεια δίνουμε άνω φράγμα για τη συνάρτηση

$$G(x) = \prod_{p \leqslant x} p,$$

όπου το γινόμενο είναι πάνω από όλους τους πρώτους $p \in \mathbb{P}$ που είναι μικρότεροι ή ισοι από τον πραγματικό αριθμό x.

Λήμμα 4.6.11. *Για κάθε πραγματικό αριθμό x ισχύει*

$$G(x) < 2^{2x-3}.$$

Απόδειξη. Αφού $G(x) = G(\lfloor x \rfloor)$ και $2^{2\lfloor x \rfloor - 3} \leqslant 2^{2x-3}$, αρκεί να αποδείξουμε το ζητούμενο κάνοντας την υπόθεση ότι ο $x = m$ είναι φυσικός, και $m \geqslant 3$. Αφού ο $\binom{2m-1}{m}$ είναι φυσικός και όλοι οι πρώτοι $m+1 \leqslant p \leqslant 2m-1$ εμφανίζονται στον αριθμητή του αλλά δεν εμφανίζονται στον παρονομαστή του, έχουμε

$$\frac{G(2m-1)}{G(m)} \leqslant \binom{2m-1}{m} = \frac{1}{2}\left(\binom{2m-1}{m-1} + \binom{2m-1}{m}\right) < \frac{1}{2}(1+1)^{2m-1} = 2^{2m-2}.$$

Συνεχίζουμε την απόδειξη με επαγωγή ως προς n.

(i) Αν $n = 3$, τότε $G(n) = 6 < 8 = 2^{2n-3}$.

(ii) Αν $n = 4$, τότε $G(n) = 6 < 32 = 2^{2n-3}$.

(iii) Αν ο $n \geqslant 5$ είναι περιττός, δηλαδή $n = 2m-1$, τότε από την προηγούμενη ανισότητα και την επαγωγική υπόθεση, αφού $m \geqslant 3$ και $m < n$ παίρνουμε

$$G(n) = G(2m-1) < G(m) \cdot 2^{2m-2} < 2^{2m-3} 2^{2m-2} = 2^{4m-5} = 2^{2n-3}.$$

(iv) Αν ο $n = 2m$ είναι άρτιος και $n \geqslant 6$, τότε από την προηγούμενη ανισότητα και την επαγωγική υπόθεση, αφού $m \geqslant 3$ και $n-1 < n$ παίρνουμε

$$G(n) = G(2m) = G(2m-1) = G(n-1) < 2^{2(n-1)-3} < 2^{2n-3}.$$

Έτσι, έχουμε το λήμμα. □

Δεύτερη απόδειξη του Θεωρήματος 4.6.1. Υποθέτουμε ότι για κάποιον φυσικό $n \geqslant 2$ δεν υπάρχουν πρώτοι που να ικανοποιούν την $n < p \leqslant 2n$. Με βάση τη συζήτηση της προηγούμενης παραγράφου έχουμε ότι δεν υπάρχουν πρώτοι παράγοντες p του $\binom{2n}{n}$ τέτοιοι ώστε:

- $2n < p$, διότι κάθε τέτοιος παράγοντας πρέπει να διαιρεί τον $(2n)!$.
- $p = 2n$, διότι ο $2n$ δεν είναιπρώτος.
- $n < p < 2n$, διότι υποθέσαμε ότι δεν υπάρχουν τέτοιοι πρώτοι αριθμοί.
- $\frac{2n}{3} < p \leqslant n$, λόγω του Λήμματος 4.6.10.

Συνεπώς, κάθε πρώτος παράγοντας p του $\binom{2n}{n}$ ικανοποιεί την

$$p \leqslant \frac{2n}{3}.$$

Παρατηρούμε τώρα ότι αν $p > \sqrt{2n}$ τότε ο φυσικός $\binom{2n}{n}$ έχει το πολύ έναν παράγοντα p. Από το Λήμμα 4.6.9, για κάθε πρώτο p έχουμε $p^{r(p,n)} \leqslant 2n$, άρα το γινόμενο των $p^{r(p,n)}$ πάνω από τους πρώτους που είναι μικρότεροι ή ίσοι από $\sqrt{2n}$ είναι το πολύ ίσο με $(2n)^{\sqrt{2n}}$.

Ξεκινώντας τότε από το Λήμμα 4.6.8 και αναλύοντας το δεξιό μέλος σε γινόμενο πρώτων παραγόντων, και κατόπιν χρησιμοποιώντας το Λήμμα 4.6.11, από τα παραπάνω βλέπουμε ότι

$$\begin{aligned}\frac{4^n}{2n} &\leqslant \binom{2n}{n} = \Bigg(\prod_{p\leqslant\sqrt{2n}} p^{r(p,n)}\Bigg)\Bigg(\prod_{\sqrt{2n}<p\leqslant\frac{2n}{3}} p^{r(p,n)}\Bigg) < (2n)^{\sqrt{2n}} \prod_{1<p\leqslant\frac{2n}{3}} p \\ &= (2n)^{\sqrt{2n}} G\Big(\frac{2n}{3}\Big) \leqslant (2n)^{\sqrt{2n}} 4^{2n/3}.\end{aligned}$$

Παίρνοντας λογαρίθμους καταλήγουμε στην

$$\frac{\ln 4}{3} n \leqslant (\sqrt{2n}+1)\ln(2n).$$

Αφού το δεξιό μέλος είναι κοίλη συνάρτηση του n, η τελευταία αυτή ανισότητα ισχύει σε κάποιο διάστημα τιμών του n. Εύκολα ελέγχουμε ότι ισχύει για $n = 467$ και δεν ισχύει για $n = 468$. Έτσι, έχουμε δείξει ότι $n < 468$.

Τώρα όμως μπορούμε να αποκλείσουμε και αυτό το ενδεχόμενο, χρησιμοποιώντας το «τέχνασμα του Landau». Για οποιονδήποτε $2 \leqslant n < 468$, επιλέγοντας ως p κάποιον από τους πρώτους αριθμούς $3, 5, 7, 13, 23, 43, 83, 163, 317, 631$ (καθένας από τους οποίους είναι μικρότερος από το διπλάσιο του προηγούμενου του) μπορούμε να έχουμε $n < p < 2n$.

Άρα δεν υπάρχει αντιπαράδειγμα στο αίτημα του Bertrand. □

4.7 Ασκήσεις

4.1. Αποδείξτε ότι το ελάχιστο κοινό πολλαπλάσιο $[1, 2, \dots, n]$ των $1, 2, \dots n$ είναι ίσο με

$$[1, 2, \dots, n] = e^{\psi(n)}.$$

4.2. Αποδείξτε ότι οι παρακάτω δύο σχέσεις είναι ισοδύναμες.

(α) $\pi(x) = \frac{x}{\ln x} + O\left(\frac{x}{\ln^2 x}\right)$.

(β) $\vartheta(x) = x + O\left(\frac{x}{\ln x}\right)$.

4.3. Θεωρώντας γνωστό το θεώρημα των πρώτων αριθμών αποδείξτε τα ακόλουθα:

(α) Αν $a > 0$ και $b > 0$ τότε $\frac{\pi(ax)}{\pi(bx)} \sim \frac{a}{b}$ καθώς το $x \to \infty$.

(β) Αν $0 < a < b$ τότε υπάρχει x_0 τέτοιος ώστε $\pi(ax) < \pi(bx)$ για κάθε $x \geqslant x_0$.

(γ) Αν $0 < a < b$ τότε υπάρχει x_0 τέτοιος ώστε για κάθε $x \geqslant x_0$ υπάρχει τουλάχιστον ένας πρώτος ανάμεσα στον ax και τον bx.

(δ) Κάθε διάστημα $[a, b]$ με $0 < a < b$ περιέχει ρητό αριθμό της μορφής p/q όπου οι p και q είναι πρώτοι.

4.4. Ορίζουμε $P(x) = \prod_{p\leqslant x} p$. Αποδείξτε ότι το θεώρημα των πρώτων αριθμών είναι ισοδύναμο με την

$$\lim_{x\to\infty} P(x)^{1/x} = e.$$

4.5. Έστω $a(n)$ φθίνουσα ακολουθία θετικών αριθμών. Αποδείξτε ότι η σειρά $\sum_p a(p)$ συγκλίνει αν και μόνο αν η σειρά $\sum_{n=2}^{\infty} \frac{a(n)}{\ln n}$ συγκλίνει.

4.6. Για $x \geqslant 2$ ορίζουμε

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\ln t}.$$

(α) Αποδείξτε ότι

$$\mathrm{Li}(x) = \frac{x}{\ln x} + \int_2^x \frac{dt}{(\ln t)^2} - \frac{2}{\ln 2}.$$

Πιο γενικά, αποδείξτε ότι

$$\mathrm{Li}(x) = \frac{x}{\ln x}\left(1 + \sum_{k=1}^{n-1} \frac{k!}{(\ln x)^k}\right) + n! \int_2^x \frac{dt}{(\ln t)^{n+1}} + C_n,$$

όπου C_n είναι μια σταθερά ανεξάρτητη από το x.

(β) Για $x \geqslant 2$ αποδείξτε ότι

$$\int_2^x \frac{dt}{(\ln t)^n} = O\left(\frac{x}{(\ln x)^n}\right).$$

4.7. Έστω $f(n)$ μια αριθμητική συνάρτηση τέτοια ώστε

$$\sum_{p \leqslant x} f(p) \ln p = (ax + b) \ln x + cx + O(1)$$

για $x \geqslant 2$. Αποδείξτε ότι υπάρχει μια σταθερά A, που εξαρτάται από την f, τέτοια ώστε, για $x \geqslant 2$,

$$\sum_{p \leqslant x} f(p) = ax + (a + c)\left(\frac{x}{\ln x} + \int_2^x \frac{dt}{(\ln t)^2}\right) + b \ln \ln x + A + O\left(\frac{1}{\ln x}\right).$$

4.8. Έστω $S(x)$ και $T(x)$ πραγματικές συναρτήσεις τέτοιες ώστε

$$T(x) = \sum_{n \leqslant x} S\left(\frac{x}{n}\right)$$

για κάθε $x \geqslant 1$. Αν $S(x) = O(x)$ και c είναι μια θετική σταθερά, αποδείξτε ότι η σχέση

$$S(x) \sim cx \ \text{ καθώς το } x \to \infty$$

συνεπάγεται την

$$T(x) \sim cx \ln x \ \text{ καθώς το } x \to \infty.$$

4.9. Έστω $f(n)$ αριθμητική συνάρτηση και

$$S(x) = \sum_{n \leqslant x} f(n).$$

Αποδείξτε ότι αν

$$\lim_{x \to \infty} \frac{S(x)}{x} = \ell,$$

τότε

$$\sum_{n \leqslant x} \frac{f(n)}{n} = \ell \ln x + o(\ln x).$$

[*Σημείωση.* $g(x) = o(\ln x)$ σημαίνει $\lim_{x \to \infty} \frac{g(x)}{\ln x} = 0$.]

4.10. Αποδείξτε ότι αν οι p, q είναι πρώτοι, τότε

$$\sum_{pq \leqslant x} \frac{1}{pq} = (\ln \ln x)^2 + O(\ln \ln x).$$

4.11. Έστω $\omega(n)$ η συνάρτηση που ορίστηκε στην Άσκηση 3.6. Αποδείξτε ότι

$$\sum_{n \leqslant x} \omega(n) = x \ln \ln x + O(x).$$

4.12. Αποδείξτε ότι, για κάθε $x \geqslant 2$,

$$\sum_{n \leqslant x} \psi\left(\frac{x}{n}\right) = x \ln x + O(x).$$

4.13. Αποδείξτε ότι, για κάθε $x \geqslant 1$,

$$\sum_{n \leqslant x} \frac{\vartheta(n)}{n^2} = \ln x + O(1).$$

4.14. Αποδείξτε ότι

$$\sum_{p \leqslant x} \frac{\ln p}{p-1} = \ln x + O(1).$$

4.15. Έστω x ένας θετικός πραγματικός αριθμός. Χρησιμοποιώντας τον τύπο του Stirling επαληθεύστε ότι

$$\ln[x]! - 2\ln[x/2]! < \frac{3x}{4} \qquad \text{αν } x > 0.$$

4.16. Συμπληρώστε την απόδειξη του αιτήματος του Bertrand που έδωσε ο Erdős εξηγώντας τα ακόλουθα βήματα:

(α) Έστω $r(p)$ τέτοιος ώστε

$$p^{r(p)} \leqslant 2n < p^{r(p)+1}.$$

Αποδείξτε ότι

$$\binom{2n}{n} \Bigm| \prod_{p \leqslant 2n} p^{r(p)}.$$

(β) Αποδείξτε ότι αν $p > 2$ και $\frac{2n}{3} < p \leqslant n$ τότε

$$p \nmid \binom{2n}{n}.$$

(γ) Αποδείξτε ότι

$$\prod_{p \leqslant n} p < 4^n.$$

(δ) Χρησιμοποιώντας τα προηγούμενα αποτελέσματα αποδείξτε το αίτημα του Bertrand.

4.17. Αποδείξτε ότι αν n είναι οποιοσδήποτε θετικός ακέραιος μεγαλύτερος από 1, τότε ο $n!$ δεν είναι ποτέ τέλειο τετράγωνο.

4.18. Έστω n ένας θετικός ακέραιος. Υποθέτουμε ότι για κάθε $m > 20$ υπάρχει πρώτος ανάμεσα στον $m/2$ και τον $m - 6$. Αποδείξτε ότι ο n μπορεί να γραφεί ως άθροισμα διακεκριμένων πρώτων όταν $n > 6$. (Πρόκληση: Προσπαθήστε να αποδείξετε αυτό το αποτέλεσμα χωρίς να κάνετε την πρώτη υπόθεση.)

4.19. Χρησιμοποιώντας το αίτημα του Bertrand αποδείξτε ότι για κάθε θετικό ακέραιο n, ο αριθμός

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

δεν είναι ποτέ ακέραιος.

4.20. Χρησιμοποιώντας επαγωγή και το αίτημα του Bertrand αποδείξτε ότι, συμβολίζοντας με p_n τον n-οστό πρώτο, για κάθε $n > 3$,

$$p_n < p_1 + p_2 + \cdots + p_{n-1}.$$

4.21. Ξεκινώντας από την

$$1 = \sum_{n=1}^{\infty} \frac{I(n)}{n^2} = \sum_{n=1}^{\infty} \frac{1}{n^2} \sum_{d|n} \mu(d)$$

αποδείξτε ότι

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)}.$$

4.22. (α) Έστω f, f_0, g αριθμητικές συναρτήσεις τέτοιες ώστε $f = f_0 * g$. Αν $F(x) = \sum_{n \leqslant x} f(n)$ και $F_0(x) = \sum_{n \leqslant x} f_0(n)$, αποδείξτε ότι

$$F(x) = \sum_{d \leqslant x} g(d) F_0(x/d).$$

(β) Γράφοντας $\mu^2 = u * (\mu^2 * \mu)$ και χρησιμοποιώντας το (α) αποδείξτε ότι

$$\sum_{n \leqslant x} \mu^2(n) = \frac{6}{\pi^2} x + O(\sqrt{x}).$$

Με την υπόθεση ότι ισχύει το θεώρημα των πρώτων αριθμών, αποδείξτε ότι

$$\sum_{n \leqslant x} \mu^2(n) = \frac{6}{\pi^2} x + o(\sqrt{x}).$$

ΚΕΦΑΛΑΙΟ 5

Το θεώρημα των πρώτων αριθμών

5.1 Το θεώρημα των πρώτων αριθμών

Στο Κεφάλαιο 4, Πόρισμα 4.3.5, αποδείξαμε ότι το θεώρημα των πρώτων αριθμών είναι ισοδύναμο με την πρόταση

$$\psi(x) \sim x. \tag{5.1.1}$$

Σε αυτό το κεφάλαιο, θα αποδείξουμε το ακόλουθο θεώρημα.

Θεώρημα 5.1.1. *Για κάθε θετικό πραγματικό αριθμό x έχουμε*

$$\psi(x) = x + O\left(x\exp(-c\sqrt[10]{\ln x})\right),$$

όπου $c > 0$ είναι μια σταθερά ανεξάρτητη από τον x.

Παρατηρήστε ότι η (5.1.1) προκύπτει άμεσα από το Θεώρημα 5.1.1.

Το Θεώρημα 5.1.1 είναι ασθενέστερο από το αποτέλεσμα που αποδείχθηκε ανεξάρτητα από τους J. Hadamard και de la Vallée Poussin, το οποίο ισχυρίζεται ότι

$$\psi(x) = x + O\left(x\exp(-c\sqrt{\ln x})\right).$$

Η απόδειξη όμως που θα δώσουμε εδώ μας επιτρέπει να εκτιμήσουμε την αναλυτική μέθοδο που χρησιμοποιείται στις αποδείξεις του θεωρήματος των πρώτων αριθμών και απαιτεί λιγότερα τεχνικά βήματα.

5.2 Η συνάρτηση ζήτα του Riemann

Στο Κεφάλαιο 3, στον Ορισμό 3.3.1, συναντήσαμε τη συνάρτηση ζήτα του Riemann για πραγματικό $s > 1$. Δίνουμε τώρα τον ορισμό της συνάρτησης όταν ο s είναι μιγαδικός αριθμός. Σε ό,τι ακολουθεί γράφουμε κάθε $s \in \mathbb{C}$ ως $s = \sigma + it$, όπου σ είναι το πραγματικό και t το φανταστικό μέρος του s. Επίσης, για κάθε $a \in \mathbb{R}$ ορίζουμε

$$H_a := \{s = \sigma + it \in \mathbb{C} : \sigma > a\}.$$

Ορισμός 5.2.1. Έστω $s = \sigma + it \in \mathbb{C}$ με $\sigma > 1$. Ορίζουμε

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

Θεώρημα 5.2.2. *Η συνάρτηση ζήτα του Riemann $\zeta(s)$ είναι αναλυτική συνάρτηση στο ημιεπίπεδο H_1.*

Απόδειξη. Παρατηρούμε ότι αν $\sigma \geqslant \sigma_0 > 1$, τότε

$$\sum_{n=m}^{M} \left|\frac{1}{n^s}\right| \leqslant \sum_{n=m}^{M} \frac{1}{n^{\sigma}} \leqslant \sum_{n=m}^{M} \frac{1}{n^{\sigma_0}}.$$

Τώρα, για κάθε $\varepsilon > 0$, υπάρχει $N_\varepsilon > 0$ τέτοιος ώστε

$$\sum_{n=m}^{M} \frac{1}{n^{\sigma_0}} < \varepsilon$$

για $M > m > N_\varepsilon$. Άρα, συμπεραίνουμε ότι

$$\sum_{n=m}^{M} \left|\frac{1}{n^s}\right| < \varepsilon$$

για $M > m > N_\varepsilon$. Συνεπώς, από το M-κριτήριο του Weierstrass (Θεώρημα A.1.2) η σειρά

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

είναι απολύτως και ομοιόμορφα συγκλίνουσα σε κάθε ημιεπίπεδο H_{σ_0}, όπου $\sigma_0 > 1$.

Έστω τώρα K συμπαγές υποσύνολο του H_1. Παρατηρούμε ότι υπάρχει $\sigma_0 > 1$ ώστε $K \subseteq H_{\sigma_0}$. Άρα, η σειρά $\sum_{n=1}^{\infty} \frac{1}{n^s}$ συγκλίνει ομοιόμορφα στο K. Αφού για κάθε $n \in \mathbb{N}$ η συνάρτηση $s \mapsto 1/n^s$ είναι αναλυτική στο $\mathbb{C}$, από το Θεώρημα A.1.2 έπεται ότι η συνάρτηση ζήτα του Riemann $\zeta(s)$ είναι αναλυτική συνάρτηση στο ημιεπίπεδο H_1. □

Παρατήρηση 5.2.3. Η σειρά $\sum_{n=1}^{\infty} \frac{1}{n^s}$ δεν συγκλίνει ομοιόρφα στο H_1. Αυτό μπορούμε να το δούμε με απαγωγή σε άτοπο: αν έχουμε ομοιόμορφη σύγκλιση στο H_1 τότε για $\varepsilon = 1$ μπορούμε να βρούμε $n_0 \in \mathbb{N}$ τέτοιο ώστε, αν $\ell > k \geqslant n_0$ τότε για κάθε $s \in H_1$

$$\left|\sum_{n=k}^{\ell} \frac{1}{n^s}\right| \leqslant 1.$$

Αφήνοντας το $s \to 1$ (μέσα από το H_1) παίρνουμε

$$\left|\sum_{n=k}^{\ell} \frac{1}{n}\right| \leqslant 1$$

και ααφήνοντας το $\ell \to \infty$ έχουμε ότι $\sum_{n=k}^{\infty} \frac{1}{n} \leqslant 1$, το οποίο είναι άτοπο αφού η αρμονική σειρά αποκλίνει.

5.3 Το γινόμενο του Euler και η αναπαράσταση της $\zeta(s)$ σε γινόμενο

Σε αυτή την ενότητα αποδεικνύουμε ότι η ζ αναπαρίσταται ως απειρογινόμενο στο H_1.

Θεώρημα 5.3.1. *Για κάθε $s \in H_1$,*

$$\zeta(s) = \prod_{k=1}^{\infty} \left(1 - \frac{1}{p_k^s}\right)^{-1},$$

όπου (p_k) είναι η ακολουθία των πρώτων, διατεταγμένων σε αύξουσα διάταξη.

Η σχέση αυτή είναι άμεση συνέπεια του επόμενου θεωρήματος.

Θεώρημα 5.3.2. *Έστω $f : \mathbb{N} \to \mathbb{C}$ πολλαπλασιαστική αριθμητική συνάρτηση τέτοια ώστε*

$$\sum_{n=1}^{\infty} |f(n)| < +\infty.$$

Τότε το άθροισμα της σειράς εκφράζεται ως απολύτως συγκλίνον άπειρο γινόμενο, δηλαδή,

$$\sum_{n=1}^{\infty} f(n) = \prod_{i=1}^{\infty} \left(1 + f(p_i) + f(p_i^2) + \cdots\right), \tag{5.3.1}$$

όπου $\{p_i : i \in \mathbb{N}$ είναι η ακολουθία των πρώτων σε αύξουσα διάταξη. Αν επιπλέον η f είναι πλήρως πολλαπλασιαστική, τότε

$$\sum_{n=1}^{\infty} f(n) = \prod_{i=1}^{\infty} \frac{1}{1 - f(p_i)}.$$

Το γινόμενο του παραπάνω θεωρήματος ονομάζεται γινόμενο Euler της σειράς.

Απόδειξη. Έστω $N \in \mathbb{N}$ τέτοιος ώστε $p_k \leqslant N < p_{k+1}$, και $m \in \mathbb{N}$ τέτοιος ώστε $2^m \geqslant N$. Τότε,

$$\prod_{i=1}^{k}(1 + f(p_i) + \cdots + f(p_i^m)) = \sum_{0 \leqslant i_1, \ldots, i_k \leqslant m} f(p_1^{i_1}) \cdots f(p_k^{i_k}) = \sum_{0 \leqslant i_1, \ldots, i_k \leqslant m} f(p_1^{i_1} \cdots p_k^{i_k}).$$

Παρατηρούμε ότι αν $1 \leqslant \ell \leqslant N$ τότε ο ℓ δεν έχει πρώτο διαιρέτη μεγαλύτερο από τον p_k, άρα γράφεται ως $\ell = p_1^{i_1} \cdots p_k^{i_k}$ και

$$2^{i_1 + \cdots + i_k} \leqslant p_1^{i_1} \cdots p_k^{i_k} = \ell \leqslant N \leqslant 2^m,$$

άρα $0 \leqslant i_1, \ldots, i_k \leqslant m$. Αυτό αποδεικνύει ότι $\{1, \ldots, N\} \subseteq \{p_1^{i_1} \cdots p_k^{i_k} : 0 \leqslant i_1, \ldots, i_k \leqslant m\}$, απ' όπου έπεται ότι

$$\left| \prod_{i=1}^{k}(1 + f(p_i) + \cdots + f(p_i^m)) - \sum_{n=1}^{N} f(n) \right| \leqslant \sum_{n=N+1}^{\infty} |f(n)|.$$

Αφού $\sum_{n=1}^{\infty} |f(n)| < +\infty$, για κάθε $i \in \mathbb{N}$ έχουμε ότι η σειρά $\sum_{j=0}^{\infty} f(p_i^j)$ συγκλίνει, συνεπώς αφήνοντας το $m \to \infty$ στην προηγούμενη ανισότητα παίρνουμε

$$\left| \prod_{i=1}^{k}(1 + f(p_i) + \cdots) - \sum_{n=1}^{N} f(n) \right| \leqslant \sum_{n=N+1}^{\infty} |f(n)|.$$

Επιλέγουμε $N = p_k$ και αφήνουμε το $k \to \infty$. Έχουμε $\sum_{n=p_k+1}^{\infty} |f(n)| \to 0$ όταν το $k]to\infty$ και $\sum_{n=1}^{p_k} f(n) \to \sum_{n=1}^{\infty} f(n)$, άρα υπάρχει το

$$\lim_{k\to\infty} \prod_{i=1}^{k} (1 + f(p_i) + \cdots) \quad \text{και είναι ίσο με} \quad \sum_{n=1}^{\infty} f(n).$$

Δηλαδή,

$$\sum_{n=1}^{\infty} f(n) = \prod_{k=1}^{\infty} \left(1 + f(p_k) + f(p_k^2) + \cdots\right).$$

Στην περίπτωση που η f είναι πλήρως πολλαπλασιαστική, για κάθε $i \in \mathbb{N}$ έχουμε ότι

$$1 + f(p_k) + f(p_k^2) + \cdots = \sum_{j=0}^{\infty} f(p_i)^j,$$

και αφού αυτή η σειρά συγκλίνει, βλέπουμε ότι $|f(p_i)| < 1$ και

$$1 + f(p_k) + f(p_k^2) + \cdots = \frac{1}{1 - f(p_i)}.$$

Αυτό αποδεικνύει τον δεύτερο ισχυρισμό του θεωρήματος. □

Εφαρμόζοντας το Θεώρημα 5.3.2 για την πλήρως πολλαπλασιαστική συνάρτηση

$$f(n) = \frac{1}{n^s},$$

παίρνουμε το Θεώρημα 5.3.1.

Παρατήρηση 5.3.3. Χρησιμοποιώντας το Θεώρημα 5.3.1 μπορούμε να δούμε ότι $\zeta(s) \neq 0$ για κάθε $s \in H_1$. Πράγματι, αν $s = \sigma + it$ όπου $\sigma > 1$, τότε γράφοντας $\frac{1}{1-p_k^{-s}} = 1 + a_k$, έχουμε $a_k = \frac{1}{1-p_k^{-s}} \frac{1}{p_k^s}$, άρα $|a_k| \leqslant \frac{1}{2p_k^\sigma}$ και έπεται ότι η σειρά $\sum_{k=1}^{\infty} |a_k|$ συγκλίνει. Έπεται ότι υπάρχει $N \in \mathbb{N}$ τέτοιος ώστε

$$\sum_{k=N+1}^{\infty} |a_k| < 1$$

και από την απόδειξη του Θεωρήματος A.2.2 έχουμε ότι

$$\prod_{k=N+1}^{\infty} (1 + a_k) = \prod_{k=N+1}^{\infty} \left(1 - p_k^{-s}\right)^{-1} \neq 0.$$

Αφού έχουμε επίσης $\left(1 - p_k^{-s}\right)^{-1} \neq 0$ για κάθε $k = 1, \ldots, N$, παίρνοντας υπόψη μας και το Θεώρημα 5.3.1 συμπεραίνουμε ότι

$$\zeta(s) = \prod_{k=1}^{\infty} \left(1 - p_k^{-s}\right)^{-1} = \prod_{k=1}^{N} \left(1 - p_k^{-s}\right)^{-1} \prod_{k=N+1}^{\infty} \left(1 - p_k^{-s}\right)^{-1} \neq 0.$$

5.4 Αναλυτική επέκταση της $\zeta(s)$ για $\sigma > 0$

Δείχνουμε τώρα ότι η $\zeta(s)$ μπορεί να επεκταθεί σε αναλυτική συνάρτηση στο $H_0 \setminus \{1\}$.

Θεώρημα 5.4.1. *Η συνάρτηση ζήτα του Riemann $\zeta(s)$ επεκτείνεται σε μια συνάρτηση που είναι αναλυτική στο ημιεπίπεδο H_0, εκτός από το $s = 1$ στο οποίο έχει απλό πόλο με υπόλοιπο 1.*

Απόδειξη. Θυμηθείτε από το Θεώρημα 3.2.4 ότι

$$\sum_{n\leqslant x} f(n) = f(1) + \int_1^x f(t)dt + \int_1^x f'(t)\{t\}dt - \{x\}f(x).$$

Για s πραγματικό,

$$x = N \in \mathbb{N} \quad \text{και} \quad f(n) = \frac{1}{n^s},$$

έχουμε

$$\sum_{n=1}^{N} \frac{1}{n^s} = 1 + \int_1^N \frac{d\eta}{\eta^s} - \int_1^N \frac{s\{\eta\}}{\eta^{s+1}} d\eta.$$

Δεδομένου ότι το αριστερό και το δεξιό μέλος ορίζουν αναλυτικές συναρτήσεις στο H_1 (εδώ χρησιμοποιείται και το Θεώρημα A.4.2), από την αρχή της αναλυτικής συνέχισης (Θεώρημα A.3.2) αυτή η ταυτότητα εξακολουθεί να ισχύει για κάθε $s \in H_1$.

Παρατηρούμε ότι, για κάθε $s \in H_1$,

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

και

$$\lim_{N\to\infty} \int_1^N \frac{d\eta}{\eta^s} = \int_1^\infty \frac{d\eta}{\eta^s} = \frac{1}{s-1}.$$

Επίσης, υπάρχει το

$$\lim_{N\to\infty} \int_1^N \frac{\{\eta\}}{\eta^{s+1}} d\eta = \int_1^\infty \frac{\{\eta\}}{\eta^{s+1}} d\eta =: \Phi(s).$$

Άρα,

$$\zeta(s) = \frac{s}{s-1} - s\Phi(s), \qquad s \in H_1. \tag{5.4.1}$$

Τώρα χρησιμοποιούμε την ακόλουθη πρόταση:

Πρόταση 5.4.2. *Το ολοκλήρωμα*

$$\Phi(s) := \int_1^\infty \frac{\{t\}}{t^{s+1}} dt$$

συγκλίνει για κάθε $s \in H_0$ και ορίζει αναλυτική συνάρτηση στο H_0.

Έχοντας αποδείξει την Πρόταση 5.4.2, μπορούμε να ορίσουμε μια συνάρτηση G στο $H_0 \setminus \{1\}$ με

$$G(s) := \frac{s}{s-1} - s\Phi(s).$$

Παρατηρήστε ότι αυτή η συνάρτηση είναι μερόμορφη στο H_0 με μοναδικό πόλο στο $s = 1$ και $\mathrm{Res}(G; 1) = 1$. Από την (5.4.1) βλέπουμε ότι η G είναι η επέκταση της ζ που ζητούσαμε. Στη συνέχεια θα συμβολίζουμε την G πάλι με ζ. $\square$

Απόδειξη της Πρότασης 5.4.2. Αν $s = \sigma + it \in H_0$ τότε $\sigma > 0$, άρα

$$\int_1^\infty \left| \frac{\{t\}}{t^{s+1}} \right| dt \leqslant \int +1^\infty \frac{1}{t^{\sigma+1}} dt < \infty.$$

Έπεται ότιη $\Phi(s)$ ορίζεται καλά. Τώρα, για κάθε $k \in \mathbb{N}$ ορίζουμε $F_k : \mathbb{C} \to \mathbb{C}$ με

$$F_k(s) = \int_k^{k+1} \frac{\{t\}}{t^{s+1}} dt = \int_k^{k+1} \frac{t-k}{t^{k+1}} dt.$$

Από το Θεώρημα A.4.2 βλέπουμε ότι όλες οι F_k είναι αναλυτικές στο $\mathbb{C}$. Επίσης έχουμε

$$\Phi = \sum_{k=1}^\infty F_k.$$

Έστω τώρα $K \subseteq H_0$ συμπαγές. Υπάρχει $\sigma_0 > 0$ τέτοιος ώστε $K \subset H_{\sigma_0}$. Για κάθε $s \in K$ έχουμε

$$|F_k(s)| \leqslant \int_k^{k+1} \frac{1}{t^{\sigma_0+1}} dt = \frac{1}{\sigma_0} \left(\frac{1}{k^{\sigma_0}} - \frac{1}{(k+1)^{\sigma_0}} \right),$$

και

$$\frac{1}{\sigma_0} \sum_{k=1}^\infty \left(\frac{1}{k^{\sigma_0}} - \frac{1}{(k+1)^{\sigma_0}} \right) = \frac{1}{\sigma_0} < \infty.$$

Εφαρμόζοντας το κριτήριο του Weierstrass (Θεώρημα A.1.3) έχουμε ότι η $\sum_{k=1}^\infty F_k$ συγκλίνει ομοιόμορφα στο K, και από το Θεώρημα A.1.2 συμπεραίνουμε ότι η $\Phi = \sum_{k=1}^\infty F_k$ είναι αναλυτική στο H_0. □

5.5 Μη μηδενισμός της $\zeta(1 + it)$

Σε αυτήν την ενότητα δείχνουμε ότι η $\zeta(s)$ δεν μηδενίζεται στην κατακόρυφη ευθεία $\sigma = 1$.

Θεώρημα 5.5.1. *Για κάθε πραγματικό αριθμό $t \neq 0$ ισχύει ότι*

$$\zeta(1 + it) \neq 0.$$

Αποδεικνύουμε πρώτα μερικά απλά λήμματα.

Λήμμα 5.5.2. *Για κάθε $\vartheta \in \mathbb{R}$,*

$$3 + 4\cos\vartheta + \cos 2\vartheta \geqslant 0.$$

Απόδειξη. Αυτή η ανισότητα προκύπτει άμεσα από τον υπολογισμό

$$\begin{aligned} 3 + 4\cos\vartheta + 2\cos^2\vartheta - 1 &= 2\cos^2\vartheta + 4\cos\vartheta + 2 \\ &= 2(\cos^2\vartheta + 2\cos\vartheta + 1) \\ &= 2(\cos\vartheta + 1)^2 \geqslant 0, \end{aligned}$$

και τη γνωστή ταυτότητα $\cos 2\vartheta = 2\cos^2\vartheta - 1$. □

Λήμμα 5.5.3. *Για $\sigma > 1$ ισχύει*
$$\zeta(s) = e^{G(s)},$$
όπου
$$G(s) = \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}}.$$

Απόδειξη. Χρησιμοποιώντας την αναπαράσταση της $\zeta(s)$ μέσω του γινομένου Euler, βλέπουμε ότι
$$\begin{aligned}\zeta(s) &= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \\ &= \exp\left(-\sum_p \ln\left(1-\frac{1}{p^s}\right)\right) \\ &= \exp\left(\sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{sm}}\right) = \exp(G(s)).\end{aligned}$$
□

Λήμμα 5.5.4. *Για $\sigma > 1$ και για κάθε $t \in \mathbb{R}$,*
$$|\zeta(\sigma)|^3 |\zeta(\sigma+it)|^4 |\zeta(\sigma+2it)| \geqslant 1.$$

Απόδειξη. Από το Λήμμα 5.5.3 έχουμε, για $\sigma > 1$,
$$\begin{aligned}\zeta(s) &= \exp\left(\sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}}\right) \\ &= \exp\left(\sum_p \sum_{m=1}^{\infty} \frac{1}{m} \exp\{-(\ln p)ms\}\right) \\ &= \exp\left(\sum_p \sum_{m=1}^{\infty} \frac{1}{m} \exp\{-m\sigma \ln p - itm \ln p\}\right),\end{aligned}$$
αφού $s = \sigma + it$. Άρα,
$$\zeta(s) = \exp\left(\sum_p \sum_{m=1}^{\infty} \frac{1}{m} \frac{1}{p^{\sigma m}} \{\cos(tm \ln p) - i \sin(tm \ln p)\}\right).$$
Συνεπώς,
$$|\zeta(s)| = \exp\left(\sum_p \sum_{m=1}^{\infty} \frac{1}{m} \frac{1}{p^{\sigma m}} \cos(tm \ln p)\right).$$
Αυτό συνεπάγεται ότι
$$\begin{aligned}|\zeta(\sigma)|^3 |\zeta(\sigma+it)|^4 |\zeta(\sigma+2it)| &= \exp\left(\sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{\sigma m}} (3 + 4\cos(tm \ln p) + \cos(2tm \ln p))\right) \\ &\geqslant \exp(0) = 1,\end{aligned}$$
όπου στο τέλος χρησιμοποιούμε το Λήμμα 5.5.2. □

Απόδειξη του Θεωρήματος 5.5.1. Υποθέτουμε ότι $\zeta(1+it_0)=0$ για κάποιον $t_0\neq 0$. Από το Λήμμα 5.5.4, συμπεραίνουμε ότι για $\sigma>1$,

$$|\zeta(\sigma)(\sigma-1)|^3\left|\frac{\zeta(\sigma+it_0)}{\sigma-1}\right|^4|\zeta(\sigma+2it_0)|\geqslant\frac{1}{\sigma-1}. \tag{5.5.1}$$

Τώρα, αφού η $\zeta(\sigma)$ έχει απλό πόλο με υπόλοιπο 1 στο $\sigma=1$, βλέπουμε ότι

$$\lim_{\sigma\to 1^+}\zeta(\sigma)(\sigma-1)=1. \tag{5.5.2}$$

Τώρα,

$$\zeta(\sigma+it_0)=\zeta(1+it_0)+(\sigma-1)\zeta'(1+it_0)+O((\sigma-1)^2).$$

Αυτό συνεπάγεται ότι

$$\lim_{\sigma\to 1^+}\frac{\zeta(\sigma+it_0)}{\sigma-1}=\zeta'(1+it_0). \tag{5.5.3}$$

Είναι επίσης φανερό ότι

$$\zeta(\sigma+2it_0)\to\zeta(1+2it_0). \tag{5.5.4}$$

Συνδυάζοντας τις (5.5.2)–(5.5.4) βλέπουμε ότι όταν το σ πλησιάζει το 1 από τα δεξιά, το δεξιό μέλος της (5.5.1) τείνει στο ∞ και το αριστερό μέλος της (5.5.1) έχει πεπερασμένο όριο. Αυτό οδηγεί σε αντίφαση και συμπεραίνουμε ότι

$$\zeta(1+it)\neq 0$$

για κάθε μη μηδενικό πραγματικό t. □

5.6 Άνω φράγματα για τα $|\zeta(s)|$ και $|\zeta'(s)|$ κοντά στο $\sigma=1$

Για την απόδειξη του θεωρήματος των πρώτων αριθμών θα χρειαστούμε τα παρακάτω άνω φράγματα για τα μέτρα $|\zeta(s)|$ και $|\zeta'(s)|$.

Θεώρημα 5.6.1. (α) *Αν $|t|\geqslant 2$, $\frac{1}{2}\leqslant\sigma_0<1$ και $\sigma\geqslant\sigma_0$, τότε*

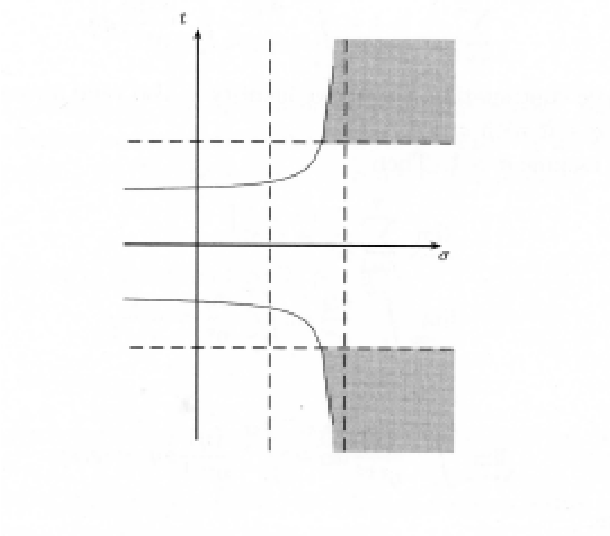
$$|\zeta(s)|\leqslant 4\frac{|t|^{1-\sigma_0}}{1-\sigma_0}. \tag{5.6.1}$$

(β) *Αν $|t|\geqslant 2$ και $\sigma\geqslant 1-\frac{1}{4\ln|t|}$ τότε*

$$|\zeta(s)|\leqslant A_1\ln|t|. \tag{5.6.2}$$

(γ) *Αν $|t|\geqslant 2$ και $\sigma\geqslant 1-\frac{1}{12\ln|t|}$ τότε*

$$|\zeta'(s)|\leqslant A_2\ln^2|t|. \tag{5.6.3}$$



Σχήμα 5.1: Τα σκιασμένα χωρία είναι αυτά στα οποία ισχύουν οι (5.6.2) και (5.6.3).

Θα χρησιμοποιήσουμε τα παρακάτω λήμματα.

Λήμμα 5.6.2. *Αν $\sigma > 0$ και $N \in \mathbb{N}$ τότε*

$$\zeta(s) = \sum_{n=1}^{N} \frac{1}{n^s} - \frac{N^{1-s}}{1-s} - s\int_N^\infty \frac{\{t\}}{t^{s+1}}dt. \tag{5.6.4}$$

Απόδειξη. Έστω $s \in \mathbb{R}$, $s > 1$. Από την

$$\sum_{n \leqslant x} f(n) = \int_1^x f(t)dt + \int_1^x \{t\}f'(t)dt + f(1) - f(x)\{x\}$$

για την $f(n) = n^{-s}$ και με $x = N$ παίρνουμε

$$\begin{aligned}\sum_{n=1}^{N} \frac{1}{n^s} &= 1 + \int_1^N \frac{dt}{t^s} - s\int_1^N \frac{\{t\}}{s+1}dt \\ &= 1 + \frac{N^{1-s}-1}{1-s} - s\int_1^\infty \frac{\{t\}}{t^{s+1}}dt + s\int_N^\infty \frac{\{t\}}{t^{s+1}}dt \\ &= \zeta(s) + \frac{N^{1-s}}{1-s} + s\int_N^\infty \frac{\{t\}}{t^{s+1}}dt,\end{aligned}$$

δηλαδή η (5.6.4) ισχύει στην ημιευθεία $s \in \mathbb{R}$, $s > 1$. Αφού το αριστερό και το δεξιό μέλος της (5.6.4) είναι και τα δύο αναλυτικές συναρτήσεις στο ανοικτό και συνεκτικό σύνολο $H_0 \setminus \{1\}$, το λήμμα έπεται από την αρχή αναλυτικής συνέχισης (Θεώρημα A.3.2). □

Λήμμα 5.6.3. *Αν $\sigma > 0$, $t \neq 0$ και $N \in \mathbb{N}$ τότε*

$$|\zeta(s)| \leqslant \sum_{n=1}^{N} \frac{1}{n^\sigma} + \frac{N^{1-\sigma}}{|t|} + \frac{|s|}{\sigma}\frac{1}{N^\sigma}. \tag{5.6.5}$$

Απόδειξη. Χρησιμοποιώντας το προηγούμενο λήμμα γράφουμε

$$\begin{aligned}|\zeta(s)| &\leqslant \sum_{n=1}^{N}\left|\frac{1}{n^s}\right| + \frac{|N^{1-s}|}{|1-s|} + |s|\int_N^\infty \frac{1}{|t^{s+1}|}dt\\ &= \sum_{n=1}^{N}\frac{1}{n^\sigma} + \frac{N^{1-\sigma}}{|1-s|} + |s|\int_N^\infty \frac{1}{t^{\sigma+1}}dt\\ &= \sum_{n=1}^{N}\frac{1}{n^\sigma} + \frac{N^{1-\sigma}}{|1-s|} + \frac{|s|}{\sigma}\frac{1}{N^\sigma},\end{aligned}$$

και τέλος παρατηρούμε ότι $|1-s| \geqslant |t|$. □

Λήμμα 5.6.4. *Αν* $\frac{1}{2} < \sigma_0 < 1$, $\sigma \geqslant \sigma_0$, $t \neq 0$ *και* $N \in \mathbb{N}$ *τότε*

$$|\zeta(s)| \leqslant \frac{N^{1-\sigma_0}}{1-\sigma_0} + \frac{N^{1-\sigma_0}}{|t|} + \left(1+\frac{|t|}{\sigma_0}\right)\frac{1}{N^{\sigma_0}}. \tag{5.6.6}$$

Απόδειξη. Παρατηρούμε ότι

$$\sum_{n=1}^{N}\frac{1}{n^\sigma} \leqslant \sum_{n=1}^{N}\frac{1}{n^{\sigma_0}} \leqslant 1 + \int_1^N \frac{1}{t^{\sigma_0}}dt = 1 + \frac{N^{1-\sigma_0}-1}{1-\sigma_0} \leqslant \frac{N^{1-\sigma_0}}{1-\sigma_0},$$

όπου χρησιμοποιήσαμε την υπόθεση ότι $\sigma \geqslant \sigma_0$ και για την τελευταία ανισότητα το γεγονός ότι $1-\frac{1}{1-\sigma_0} < 0$. Παρατηρούμε επίσης ότι

$$\frac{N^{1-\sigma}}{|t|} \leqslant \frac{N^{1-\sigma_0}}{|t|}$$

και

$$\frac{|s|}{\sigma}\frac{1}{N^\sigma} \leqslant \frac{|s|}{\sigma}\frac{1}{N^{\sigma_0}} \leqslant \frac{\sigma+|t|}{\sigma}\frac{1}{N^{\sigma_0}} = \left(1+\frac{|t|}{\sigma_0}\right)\frac{1}{N^{\sigma_0}}.$$

Τώρα το ζητούμενο προκύπτει από το Λήμμα 5.6.3. □

Απόδειξη του Θεωρήματος 5.4.1. (α) Από το Λήμμα 5.6.4 με $N = [|t|]$ έχουμε

$$\begin{aligned}|\zeta(s)| &\leqslant \frac{|t|^{1-\sigma_0}}{1-\sigma_0} + \frac{|t|^{1-\sigma_0}}{|t|} + \left(1+\frac{|t|}{\sigma_0}\right)\frac{|t|^{1-\sigma_0}}{[|t|]}\\ &= \frac{|t|^{1-\sigma_0}}{1-\sigma_0}\left(1+\frac{1-\sigma_0}{|t|} + \left(1+\frac{|t|}{\sigma_0}\right)\frac{1-\sigma_0}{[|t|]}\right).\end{aligned}$$

Από τις υποθέσεις μας έχουμε $\frac{1-\sigma_0}{|t|} \leqslant \frac{1}{2|t|} \leqslant \frac{1}{4}$ και

$$\left(1+\frac{|t|}{\sigma_0}\right)\frac{1-\sigma_0}{[|t|]} = \left(\frac{1}{|t|}+\frac{1}{\sigma_0}\right)\frac{|t|}{[|t|]}(1-\sigma_0) \leqslant \left(\frac{1}{2}+2\right)\cdot\frac{3}{2}\cdot\frac{1}{2} = \frac{15}{8}$$

(διότι $|t| \leqslant [|t|]+1 \leqslant 3[|t|]/2$). Άρα,

$$1+\frac{1-\sigma_0}{|t|} + \left(1+\frac{|t|}{\sigma_0}\right)\frac{1-\sigma_0}{[|t|]} \leqslant 1+\frac{1}{4}+\frac{15}{8} \leqslant 4,$$

και έχουμε το ζητούμενο.

(β) Είναι άμεση συνέπεια του (α). Με την υπόθεση ότι $\sigma \geqslant 1 - \frac{1}{4\ln|t|}$ παρατηρούμε ότι έχουμε επίσης $\sigma_0 \geqslant 1 - \frac{1}{4\ln 2} > \frac{1}{2}$. Εφαρμόζοντας το (α) παίρνουμε

$$|\zeta(s)| \leqslant 4\frac{|t|^{\frac{1}{4\ln|t|}}}{\frac{1}{4\ln|t|}} = 16e^{1/4}\ln|t|,$$

δηλαδή το ζητούμενο με $A_1 = 16e^{1/4}$.

(γ) Αν $\sigma \geqslant 2$ τότε από την $\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\ln n}{n^s}$ βλέπουμε ότι

$$|\zeta'(s)| \leqslant \sum_{n=1}^{\infty} \frac{\ln n}{n^{\sigma}} \leqslant \sum_{n=1}^{\infty} \frac{\ln n}{n^2} =: C_1$$

Αφού $|t| \geqslant 2$ έπεται προφανώς ότι $C_1 \leqslant A\ln^2|t|$, όπου $A := C_1/(\ln 2)^2$.

Στην ένωση των δύο ορθογωνίων $\frac{1}{2} \leqslant \sigma \leqslant 2$, $2 \leqslant |t| \leqslant 3$ η $\zeta'(s)$ είναι αναλυτική, άρα συνεχής. Λόγω συμπάγειας έχουμε $|\zeta'(s)| \leqslant C_2$ για κάποια σταθερά $C_2 > 0$, άρα όπως πριν παίρνουμε $|\zeta'(s)| \leqslant A\ln^2|t|$ αν επιλέξουμε κατάλληλα την απόλυτη σταθερά $A > 0$.

Ζητάμε λοιπόν την ανισότητα $|\zeta'(s)| \leqslant A_2\ln^2|t|$ για κάποια απόλυτη σταθερά $A_2 > 0$, με τις υποθέσεις

$$1 - \frac{1}{12\ln|t|} \leqslant \sigma \leqslant 2 \quad \text{και} \quad |t| \geqslant 3.$$

Έστω $s = \sigma + it$ που ικανοποιεί αυτές τις υποθέσεις. Θέτουμε $\delta = \frac{1}{12\ln|t|}$ και παρατηρούμε ότι για κάθε $s_1 = \sigma_1 + it_1$ στον κύκλο $C(s,\delta) = \{s_1 \in \mathbb{C} : |s - s_1| = \delta\}$ ισχύουν τα εξής:

- $|t_1| \leqslant |t| - \delta \geqslant 3 - 1 = 3$, και
- $|t_1| \leqslant |t| + \delta \leqslant |t| + \frac{1}{12\ln e} \leqslant |t| + \frac{1}{12}|t| = \frac{13}{12}|t| \leqslant |t|^{3/2}$, διότι $|t| \geqslant 2 \geqslant (13/12)^2$, άρα

$$|\sigma_1| \geqslant |\sigma| - \frac{1}{12\ln|t|} \geqslant 1 - \frac{1}{5\ln|t|} \geqslant 1 - \frac{1}{4\ln|t_1|}.$$

Δηλαδή, για κάθε $s \in C(s,\delta)$ ικανοποιούνται οι υποθέσεις του (β), και συνεπώς,

$$|\zeta(s_1)| \leqslant A_1\ln|t_1|.$$

Τώρα, από τον τύπο του Cauchy παίρνουμε

$$\begin{aligned}|\zeta'(s)| &= \left|\frac{1}{2\pi i}\int_{C(s,\delta)} \frac{\zeta'(s_1)}{(s_1 - s)^2} ds_1\right| \leqslant \delta \cdot \frac{1}{\delta^2} A_1 \max_{s_1 \in C(s,\delta)} \ln|t_1| \\ &= 12A_1\ln|t| \cdot \frac{3}{2}\ln|t| = 18A_1\ln^2|t|,\end{aligned}$$

και έχουμε το ζητούμενο με $A := 18A_1$. Συνδυάζοντας τις τρεις περιπτώσεις που εξετάσουμε παραπάνω, επιλέγουμε κατάλληλα τη σταθερά $A_2 > 0$ ώστε το φράγμα να ισχύει για όλους τους s που θεωρήσαμε. $\square$

5.7 Κάτω φράγμα για το $|\zeta(s)|$ κοντά στο $\sigma = 1$

Χρησιμοποιώντας τα αποτελέσματα των δύο προηγουμένων ενοτήτων δίνουμε τώρα και τα ακόλουθα κάτω φράγματα για το μέτρο $|\zeta(s)|$.

Θεώρημα 5.7.1. (α) *Υπάρχουν $c_1 > 0$ και $A_3 > 0$ ώστε: αν $\sigma \geqslant 1 - c_1$ και $|t| \leqslant 2$ τότε*

$$\left|\frac{1}{\zeta(s)}\right| \leqslant A_3.$$

(β) *Υπάρχουν $c_2 > 0$ και $A_4 > 0$ ώστε: αν $\sigma > 1 - \frac{c_2}{(\ln|t|)^9}$ και $|t| \geqslant 2$, τότε*

$$\left|\frac{1}{\zeta(s)}\right| \leqslant A_4(\ln|t|)^7.$$

Απόδειξη. (α) Αν $\sigma \geqslant 2$ τότε

$$|\zeta(s)| = \left|\sum_{n=1}^{\infty}\frac{1}{n^s}\right| \geqslant 1 - \left|\sum_{n=2}^{\infty}\frac{1}{n^s}\right| \geqslant 1 - \sum_{n=2}^{\infty}\frac{1}{n^2} = 2 - \frac{\pi^2}{6} > \frac{1}{4}.$$

Συνεπώς, έχουμε το ζητούμενο με $A_3 = 4$. Στα δύο ορθογώνια $1 \leqslant \sigma \leqslant 2$, $|t| \leqslant 2$ η $\zeta(s)$ δεν μηδενίζεται και η $\frac{1}{\zeta(s)}$ είναι αναλυτική, άρα είναι φραγμένη. Λόγω συμπάγειας, μπορούμε να δούμε ότι εξακολουθεί να είναι φραγμένη σε μια μικρή περιοχή αυτού του ορθογωνίου, άρα υπάρχουν $c_1 > 0$ (κατάλληλα μικρό) και $A_3 > 0$ ώστε: αν $\sigma \geqslant 1 - c_1$ και $|t| \leqslant 2$ τότε $|1/\zeta(s)| \leqslant A_3$.
(β) Για $\sigma \geqslant 2$, όπως πριν βλέπουμε ότι $|1/\zeta(s)| \leqslant 4 \leqslant A_4(\ln|t|)^7$ αν $A_4 \geqslant \frac{(\ln 2)^7}{4}$.

Υποθέτουμε λοιπόν ότι $\sigma \leqslant 2$. Σταθεροποιούμε $\alpha > 0$, το οποίο θα επιλεγεί κατάλληλα, και υποθέτουμε ότι

$$1 + \frac{\alpha}{(\ln|t|)^9} \leqslant \sigma \leqslant 2 \quad \text{και} \quad |t| \geqslant 2.$$

Από το Λήμμα 5.5.4 βλέπουμε ότι

$$|\zeta(\sigma + it)| \geqslant \frac{1}{|\zeta(\sigma)|^{3/4}|\zeta(\sigma + 2it)|^{1/4}}.$$

Αφού $\sigma \leqslant 2$, έχουμε

$$\zeta(\sigma) = \sum_{n=1}^{\infty}\frac{1}{n^\sigma} \leqslant 1 + \int_1^{\infty}\frac{1}{x^\sigma}dx = 1 + \frac{1}{\sigma - 1} \leqslant \frac{2}{\sigma - 1}.$$

Από το Θεώρημα 5.6.1 έχουμε

$$|\zeta(\sigma + 2it)| \leqslant A_1 \ln|2t| \leqslant 2A_1 \ln|t|$$

διότι $\ln|2t| \leqslant \ln(|t|^2) = 2\ln|t|$ αφού $|t| \geqslant 2$. Συνδυάζοντας τα παραπάνω βλέπουμε ότι

$$\begin{aligned} |\zeta(\sigma + it)| &\geqslant \frac{1}{2^{3/4}}\frac{1}{(2A_1)^{1/4}}(\sigma - 1)^{3/4}\frac{1}{(\ln|t|)^{1/4}} \\ &\geqslant c_0\frac{\alpha^{3/4}}{(\ln|t|)^{27/4}}\frac{1}{(\ln|t|)^{1/4}} = \frac{c_0\alpha^{3/4}}{(\ln|t|)^7}. \end{aligned} \tag{5.7.1}$$

Θα δείξουμε ότι παρόμοιο κάτω φράγμα ισχύει και για το χωρίο

$$\sigma_1 := 1 - \frac{\alpha}{(\ln|t|)^9} \leqslant \sigma \leqslant 1 + \frac{\alpha}{(\ln|t|)^9}, \quad |t| \geqslant 2.$$

Παρατηρούμε ότι αν $\sigma_1 \leqslant \sigma \leqslant \sigma_2$ τότε

$$\begin{aligned} |\zeta(\sigma+it)| &= \left|\zeta(\sigma_2+it) - \int_\sigma^{\sigma_2} \zeta'(u+it)du\right| \\ &\geqslant |\zeta(\sigma_2+it)| - (\sigma_2-\sigma_1)\max_{\sigma_1\leqslant u\leqslant\sigma_2}|\zeta'(u+it)| \\ &\geqslant \frac{c_0\alpha^{3/4}}{(\ln|t|)^7} - \frac{2\alpha}{(\ln|t|)^9}\cdot A_2(\ln|t|)^2) \\ &\geqslant \alpha^{3/4}(c_0 - 2A_2\alpha^{1/4})\frac{1}{(\ln|t|)^7} \\ &= \frac{c_0\alpha^{3/4}}{2(\ln|t|)^7}, \end{aligned} \tag{5.7.2}$$

αν επιλέξουμε $\alpha = \left(\frac{c_0}{4A_2}\right)^4$. Συνδυάζοντας τα κάτω φράγματα των (5.7.1) και (5.7.2) γι' αυτήν την τιμή του α έχουμε το ζητούμενο. □

Συνδυάζοντας το Θεώρημα 5.7.1 με το Θεώρημα 5.4.1 έχουμε το εξής.

Θεώρημα 5.7.2. *Υπάρχουν σταθερές $0 < c_1 < \frac{1}{2}$ και $A_5 > 0$ τέτοιες ώστε:*

(α) *Αν $\sigma \geqslant 1 - \frac{c_1}{(\ln|t|)^9}$ και $|t| \geqslant 2$ τότε*

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \leqslant A_5(\ln|t|)^9.$$

(β) *Αν $\sigma \geqslant 1 - c_1$, $|t| \leqslant 2$ και $s \neq 1$, τότε*

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \leqslant A_5 \max\left\{1, \frac{1}{|\sigma-1|}\right\}.$$

Απόδειξη. (α) Παρατηρούμε ότι αν η σταθερά c_1 επιλεγεί αρκετά μικρή τότε ικανοποιούνται οι υποθέσεις του Θεωρήματος 5.7.1 και του Θεωρήματος 5.4.1, άρα

$$|\zeta'(s)| \leqslant A_2(\ln|t|)^2 \quad \text{και} \quad \left|\frac{1}{\zeta(s)}\right| \leqslant A_4(\ln|t|)^7.$$

Έπεται τώρα άμεσα το συμπέρασμα.

(β) Παρατηρούμε ότι η $(s-1)\zeta'(s)/\zeta(s)$ είναι αναλυτική στο ημιεπίπεδο $\{z \in \mathbb{C} : \sigma \geqslant 1\}$ και ειδικότερα στο ορθογώνιο $1 \leqslant \sigma \leqslant 2$, $|t| \leqslant 2$. Λόγω συμπάγειας μπορούμε να επεκτείνουμε την αναλυτικότητα στο $1 - c_1 \leqslant \sigma \leqslant 2$, $|t| \leqslant 2$ αν επιλέξουμε τη σταθερά $c_1 > 0$ αρκετά μικρή. Δηλαδή,

$$|s-1|\cdot\left|\frac{\zeta'(s)}{\zeta(s)}\right| \leqslant A_5'$$

σε αυτό το ορθογώνιο. Από την άλλη πλευρά, για $\sigma \geqslant 2$ έχουμε

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| = \left|-\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}\right| \leqslant \sum_{n=1}^{\infty}\frac{\ln n}{n^2} = A_5''.$$

Έπεται ότι, αν $\sigma \geqslant 1 - c_1$, $|t| \leqslant 2$ και $s \neq 1$, τότε

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \leqslant A_5 \max\left\{1, \frac{1}{|\sigma - 1|}\right\},$$

όπου $A_5 = \max\{A_5', A_5''\}$. □

5.8 Ο τύπος του Perron

Η απόδειξη του θεωρήματος των πρώτων αριθμών θα βασιστεί στις προηγούμενες εκτιμήσεις, έχοντας ως αφετηρία τον τύπο του Perron.

Θεώρημα 5.8.1. *Έστω x ένας ημι-ακέραιος. Τότε για κάθε $b \in (1,3]$ και κάθε $T \geqslant 1$,*

$$\psi(x) = \frac{1}{2\pi i}\int_{b-iT}^{b+iT}\left(-\frac{\zeta'}{\zeta}(s)\frac{x^s}{s}\right) ds + O\left(\frac{x^b}{T(b-1)} + x\frac{\ln^2 x}{T}\right).$$

Αρχικά αποδεικνύουμε διάφορα λήμματα.

Λήμμα 5.8.2. *Για $\sigma > 1$,*

$$\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s} = -\frac{\zeta'}{\zeta}(s).$$

Απόδειξη. Η απόδειξη είναι άμεση αν χρησιμοποιήσουμε τον τύπο

$$\Lambda = \mu * \ln$$

και το γεγονός ότι (δείτε το Κεφάλαιο 6, Θεώρημα 6.3.1)

$$\sum_{n=1}^{\infty}\frac{(f*g)(n)}{n^s} = \sum_{n=1}^{\infty}\frac{f(n)}{n^s}\sum_{n=1}^{\infty}\frac{g(n)}{n^s}.$$

Έχουμε $I = \mu * u$, άρα

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

και

$$\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s} = \sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}\sum_{n=1}^{\infty}\frac{\ln n}{n^s}.$$

Συνδυάζοντας τα παραπάνω με την $\zeta'(s) = -\sum_{n=1}^{\infty}\frac{\ln n}{n^s}$ παίρνουμε το λήμμα. □

Λήμμα 5.8.3. *Για $\sigma > 1$,*

$$\left|\frac{\zeta'}{\zeta}(s)\right| \ll \frac{1}{\sigma - 1} + 1.$$

Απόδειξη. Για $1 < \sigma \leqslant 2$,

$$\begin{aligned}\left|\frac{\zeta'}{\zeta}(s)\right| &\leqslant \sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^{\sigma}} = \sigma\int_1^{\infty}\sum_{n\leqslant t}\Lambda(n)\frac{dt}{t^{\sigma+1}}\\ &\leqslant \sigma\int_1^{\infty}\frac{ct}{t^{\sigma+1}}dt \qquad \text{(από το Θεώρημα 4.2.3)}\\ &= c\frac{\sigma}{\sigma-1} \ll 1+\frac{1}{\sigma-1}.\end{aligned}$$

□

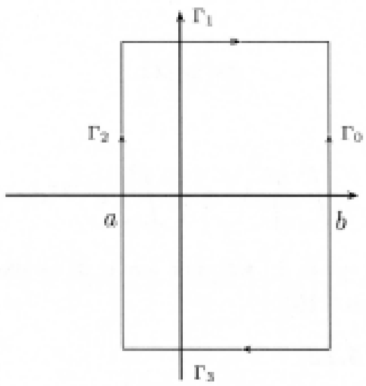
Λήμμα 5.8.4. *Για $b > 0$, $T \geqslant 1$ και $y > 0, y \neq 1$, έχουμε*

$$\frac{1}{2\pi i}\int_{b-iT}^{b+iT}\frac{y^s}{s}ds = 1 + O\left(\frac{y^b}{T|\ln y|}\right)$$

αν $y > 1$, και

$$\frac{1}{2\pi i}\int_{b-iT}^{b+iT}\frac{y^s}{s}ds = O\left(\frac{y^b}{T|\ln y|}\right)$$

αν $0 < y < 1$.



Σχήμα 5.2: Οι καμπύλες που χρησιμοποιούνται για την απόδειξη του Λήμματος 5.8.4.

Απόδειξη. Θα αποδείξουμε το αποτέλεσμα μόνο στην περίπτωση που $y > 1$. Από το θεώρημα των υπολοίπων,

$$\frac{1}{2\pi i}\int_{b-iT}^{b+iT}\frac{y^s}{s}ds = \frac{1}{2\pi i}\int_{\Gamma_0}\frac{y^s}{s}ds = 1 + \frac{1}{2\pi i}\sum_{j=1}^{3}\int_{\Gamma_j}\frac{y^s}{s}ds.$$

Αρκεί λοιπόν να δείξουμε ότι αν το $-a$ είναι αρκετά μεγάλο,

$$\left|\int_{\Gamma_j}\frac{y^s}{s}ds\right| \ll \frac{y^b}{T|\ln y|},$$

για $j = 1, 2, 3$.

Στην Γ_2,

$$\left|\frac{y^s}{s}\right| = \frac{y^a}{|s|} \leqslant y^a,$$

αν $a \leqslant -1$. Αυτό συνεπάγεται ότι

$$\left|\int_{\Gamma_2} \frac{y^s}{s} ds\right| \leqslant y^a 2T.$$

Αφήνοντας το $a \to -\infty$ συμπεραίνουμε ότι το παραπάνω ολοκλήρωμα τείνει στο 0.

Στις Γ_1 και Γ_3,

$$\left|\frac{y^s}{s}\right| = \frac{y^\sigma}{|s|} \leqslant \frac{y^\sigma}{T},$$

διότι

$$|s| > |T|.$$

Άρα, για $j = 1$ ή 3,

$$\left|\int_{\Gamma_j} \frac{y^s}{s} ds\right| \leqslant \int_a^b \frac{y^\sigma}{T} d\sigma \leqslant \frac{1}{T} \int_{-\infty}^b e^{\sigma \ln y} d\sigma \ll \frac{y^b}{T|\ln y|}.$$

Αφήνουμε την περίπτωση $0 < y < 1$ ως άσκηση για τον αναγνώστη (δείτε την Άσκηση 5.3). □

Απόδειξη του Θεωρήματος 5.8.1. Ορίζουμε

$$I = \frac{1}{2\pi i} \int_{b-iT}^{b+iT} \left(-\frac{\zeta'}{\zeta}(s)\right) \frac{x^s}{s} ds. \tag{5.8.1}$$

Από τα Λήμματα 5.8.2 και 5.8.4 βλέπουμε ότι

$$\begin{aligned}
I &= \frac{1}{2\pi i} \int_{b-iT}^{b+iT} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \frac{x^s}{s} ds \\
&= \sum_{n=1}^{\infty} \Lambda(n) \frac{1}{2\pi i} \int_{b-iT}^{b+iT} \frac{1}{s} \left(\frac{x}{n}\right)^s ds \\
&= \sum_{n \leqslant x} \Lambda(n) + \sum_{n=1}^{\infty} \Lambda(n) O\left(\frac{(x/n)^b}{T|\ln(x/n)|}\right) \\
&= \psi(x) + O\left(\frac{x^b}{T} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^b |\ln(x/n)|}\right).
\end{aligned}$$

Θέτουμε

$$R = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^b |\ln(x/n)|}.$$

Τότε,

$$R = \sum_{\frac{x}{2} \leqslant n \leqslant 2x} \frac{\Lambda(n)}{n^b |\ln(x/n)|} + \sum_{n \notin [x/2, 2x]} \frac{\Lambda(n)}{n^b |\ln(x/n)|} = R_1 + R_2.$$

Παρατηρούμε ότι αν $n > 2x$ ή $n < x/2$ τότε $|\ln(x/n)| \geqslant \ln 2$. Επιπλέον, αφού $1 < b \leqslant 3$, από τα Λήμματα 5.8.2 και 5.8.3,

$$R_2 \leqslant \frac{1}{\ln 2}\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^b} \leqslant 1 + \frac{1}{b-1} \leqslant \frac{1}{b-1} + \frac{2}{3-1} \ll \frac{1}{b-1}.$$

Τώρα, αν

$$-\frac{1}{2} \leqslant t < 1,$$

τότε

$$|\ln(1+t)| \geqslant \frac{|t|}{2}$$

και συμπεραίνουμε ότι

$$\left|\ln\frac{x}{n}\right| = \left|\ln\left(1 + \frac{x-n}{n}\right)\right| \gg \left|\frac{x-n}{n}\right|. \tag{5.8.2}$$

Επιπλέον, αφού

$$\Lambda(n) \leqslant \ln x \tag{5.8.3}$$

και

$$\frac{1}{n^b} \leqslant \frac{2^b}{x^b} \tag{5.8.4}$$

για $x/2 < n$, χρησιμοποιώντας τις (5.8.2)–(5.8.4) βλέπουμε ότι

$$R_1 = \sum_{\frac{x}{2}\leqslant n\leqslant 2x}\frac{\Lambda(n)}{n^b|\ln(x/n)|} \ll \frac{\ln x}{x^b}\sum_{\frac{x}{2}\leqslant n\leqslant 2x}\left|\frac{x}{x-n}\right|. \tag{5.8.5}$$

Αφού ο x είναι ημι-ακέραιος, ο παρονομαστής στο άθροισμα

$$\sum_{\frac{x}{2}\leqslant n\leqslant 2x}\left|\frac{x}{x-n}\right|$$

δεν μηδενίζεται και βλέπουμε ότι

$$\sum_{\frac{x}{2}\leqslant n\leqslant 2x}\left|\frac{x}{x-n}\right| \ll x\ln x. \tag{5.8.6}$$

Αντικαθιστώντας την (5.8.6) στην (5.8.5) συμπεραίνουμε ότι

$$R_1 \ll 2^b\frac{\ln^2 x}{x^b}x \ll \frac{\ln^2 x}{x^b}x,$$

όπου χρησιμοποιήσαμε το γεγονός ότι

$$2^b \leqslant 2^3$$

αν

$$b \leqslant 3.$$

Άρα, ό όρος του σφάλματος για το I, που δίνεται από την (5.8.1), είναι

$$O\left(\frac{x^b}{T(b-1)} + x\frac{\ln^2 T}{T}\right).$$

$\square$

5.9 Απόδειξη του θεωρήματος των πρώτων αριθμών

Βήμα 1. Εφαρμόζουμε τον τύπο του Perron. Έστω

$$T \geqslant 1, \quad x = N + \frac{1}{2} \geqslant 2 \quad \text{και} \quad b = 1 + \frac{1}{\ln x}.$$

Τότε,

$$\frac{x^b}{T(b-1)} = \frac{x \cdot x^{\frac{1}{\ln x}}}{T \cdot \frac{1}{\ln x}} = \frac{ex \ln x}{T},$$

άρα

$$O\left(\frac{x^b}{T(b-1)} + \frac{x \ln^2 x}{T}\right) = O\left(\frac{x \ln^2 x}{T}\right)$$

και ο τύπος του Perron μας δίνει

$$\psi(x) = \frac{1}{2\pi i} \int_{b-iT}^{b+iT} \left(-\frac{\zeta'}{\zeta}(s)\right) \frac{x^s}{s} ds + O\left(\frac{x \ln^2 x}{T}\right).$$

Βήμα 2. Μετατοπίζουμε τη διαδρομή ολοκλήρωσης. Επιλέγουμε a αρκετά κοντά στο 1 ώστε

$$\zeta(s) \neq 0$$

για κάθε $\sigma \geqslant a$, $|t| \leqslant T$. Παρατηρούμε ότι η ολοκληρωτέα ποσότητα

$$\left(-\frac{\zeta'}{\zeta}(s)\right) \frac{x^s}{s}$$

είναι αναλυτική στο χωρίο που περιβάλλεται από την παλιά και τη νέα διαδρομή με την εξαίρεση ενός πόλου στο $s = 1$, με υπόλοιπο x. Από το θεώρημα των υπολοίπων,

$$\frac{1}{2\pi i} \int_{b-iT}^{b+iT} \left(-\frac{\zeta'}{\zeta}(s)\right) \frac{x^s}{s} ds = x + \sum_{j=1}^{3} \frac{1}{2\pi i} \int_{\Gamma_j} \left(-\frac{\zeta'}{\zeta}(s)\right) \frac{x^s}{s} ds.$$

Βήμα 3. Υπολογίζουμε το

$$\int_{\Gamma_j} \left(-\frac{\zeta'}{\zeta}(s)\right) \frac{x^s}{s} ds.$$

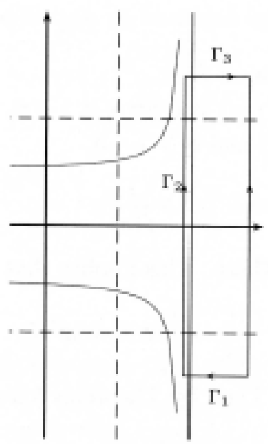
Ορίζουμε

$$B = \max_{s \in \Gamma_1, \Gamma_2, \Gamma_3} \left|\frac{\zeta'}{\zeta}(s)\right|.$$

Ο αριθμός B εξαρτάται από το T και θα τον εκτιμήσουμε στο Βήμα 4.

Τώρα, για $T \geqslant 2$,

$$\left|\int_{\Gamma_2} \left(-\frac{\zeta'}{\zeta}(s)\right) \frac{x^s}{s} ds\right| \leqslant x^a B \int_{a-iT}^{a+iT} \frac{|ds|}{|s|} = 2x^a B \int_0^T \frac{dt}{|a+it|} \ll B x^a \ln T. \tag{5.9.1}$$



Σχήμα 5.3: Οι καμπύλες που χρησιμοποιούνται για την απόδειξη του θεωρήματος των πρώτων αριθμών.

Η τελευταία ανισότητα προκύπτει από το γεγονός ότι για $T \geqslant 2$,

$$\int_0^T \frac{dt}{|a+it|} \leqslant \int_1^T \frac{dt}{t} + \int_0^1 \frac{dt}{a} \leqslant \ln T + 2 \ll \ln T.$$

Τώρα θα εκτιμήσουμε το ολοκλήρωμα στην Γ_3. Η εκτίμηση για το ολοκλήρωμα στην Γ_1 είναι όμοια. Αφού

$$b = 1 + \frac{1}{\ln x},$$

βλέπουμε ότι

$$\left| \int_{\Gamma_3} \left(-\frac{\zeta'}{\zeta}(s) \right) \frac{x^s}{s} ds \right| \leqslant B \int_{a+iT}^{b+iT} \left| \frac{x^s}{s} \right| ds \leqslant \frac{B}{T} \int_a^b x^\sigma d\sigma \tag{5.9.2}$$
$$\ll \frac{Bx^b}{T} \ll \frac{Bx}{T}.$$

Συμπεραίνουμε λοιπόν από τις (5.9.1) και (5.9.2) ότι

$$\psi(x) = x + O\left(\frac{Bx}{T}\right) + O(Bx^a \ln T) + O\left(\frac{x \ln^2 x}{T}\right).$$

Παρατηρήστε ότι τα παραπάνω ισχύουν για $T \geqslant 2$ και για κατάλληλη επιλογή του a.

Βήμα 4. Επιλογή του a και εκτίμηση για το B. Για $|t| \leqslant 2$, παρατηρούμε ότι $\zeta(s) \neq 0$ για $s = 1 + it$. Άρα, υπάρχει $\delta > 0$ τέτοιος ώστε για $|t| \leqslant 2$ και $\sigma > 1 - \delta$, η

$$\frac{1}{\zeta(s)}$$

είναι αναλυτική και φραγμένη. Αυτό συνεπάγεται ότι

$$\left|\frac{\zeta'}{\zeta}(s)\right| \ll 1 \ll (\ln T)^9. \tag{5.9.3}$$

Υποθέτουμε ότι $2 \leqslant |t| \leqslant T$. Τότε από τα Θεωρήματα 5.6.1 και 5.5.1, υπάρχουν σταθερές c και d τέτοιες ώστε

$$|\zeta(s)| \geqslant \frac{d}{(\ln|t|)^7} \quad \text{και} \quad |\zeta'(s)| \ll (\ln|t|)^2$$

στο χωρίο

$$\sigma \geqslant 1 - \frac{c}{(\ln|t|)^9}.$$

Παρατηρήστε ότι πρέπει να επιλέξουμε το c έτσι ώστε

$$c < \delta(\ln 2)^9. \tag{5.9.4}$$

Η πρόσθετη συνθήκη που επιβάλλουμε στο c είναι αναγκαία για να ισχύει η (5.9.3). Κατόπιν, με $2 \leqslant |t| \leqslant T$ και

$$a = 1 - \frac{c}{(\ln|T|)^9},$$

συμπεραίνουμε ότι

$$\left|\frac{\zeta'}{\zeta}(s)\right| \ll 1 \ll (\ln T)^9.$$

Συνδυάζοντας με την (5.9.3) βλέπουμε ότι

$$B = \max_{s\in\Gamma_1,\Gamma_2,\Gamma_3}\left|\frac{\zeta'}{\zeta}(s)\right| \ll 1 \ll (\ln T)^9.$$

Συνεπώς,

$$\psi(x) = x + O\left(x\frac{(\ln T)^9}{T}\right) + O\left(\frac{x\ln^2 x}{T}\right) + O\left(x(\ln T)^{10}\exp\left(-c\frac{\ln x}{(\ln T)^9}\right)\right).$$

Τώρα, οι πρώτοι δύο όροι σφάλματος φράσσονται από

$$O\left(x\frac{(\ln x)^{10}}{T}\right).$$

Άρα,

$$\psi(x)) = x + O\left(x\frac{(\ln x)^{10}}{T}\right) + O\left(x(\ln T)^{10}\exp\left(-c\frac{\ln x}{(\ln T)^9}\right)\right).$$

Βήμα 5. Επιλογή του T. Υποθέτουμε ότι $2 \leqslant T \leqslant x$. Η παράσταση στον όρο του σφάλματος ελαχιστοποιείται αν

$$\frac{1}{T} = \exp\left\{-\frac{c\ln x}{(\ln T)^9}\right\}.$$

Συνεπώς, επιλέγουμε

$$T = \exp\{(c_3\ln x)^{1/10}\}.$$

Με αυτή την επιλογή του T έχουμε για αρκετά μεγάλο $x \geqslant x_0$ και $2 \leqslant T \leqslant x$,

$$\psi(x) = x + O\left(x \frac{(\ln x)^{10}}{\exp((c \ln x)^{1/10})}\right).$$

Αφού για κάθε $\varepsilon > 0$

$$(\ln x)^{10} \ll \exp\left(\varepsilon (\ln x)^{1/10}\right),$$

συμπεραίνουμε ότι

$$\psi(x) = x + O(x \exp(-c'(\ln x)^{1/10}))$$

για κατάλληλη επιλογή της σταθεράς $c' > 0$. Για $2 \leqslant x \leqslant x_0$, έχουμε

$$\psi(x) = x + O(x \exp(-c'(\ln x)^{1/10})).$$

Αυτό ολοκληρώνει την απόδειξη του θεωρήματος των πρώτων αριθμών.

Παρατήρηση 5.9.1. Οι ισοδύναμες διατυπώσεις των παραπάνω για τις $\vartheta(x)$ και $\pi(x)$ είναι

$$\vartheta(x) = x + O(x \exp(-c(\ln x)^{1/10})), \qquad x \geqslant 2$$

και

$$\pi(x) = \mathrm{Li}(x) + O(x \exp(-c(\ln x)^{1/10})), \qquad x \geqslant 2,$$

όπου

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\ln t}.$$

5.10 Ασκήσεις

5.1. Για δοσμένο $A > 0$ αποδείξτε ότι υπάρχει σταθερά M τέτοια ώστε: για $|t| \geqslant 2$, $\sigma \geqslant \max\left(\frac{1}{2}, 1 - \frac{A}{\ln |t|}\right)$,

$$|\zeta'(s)| \leqslant M \ln^2 |t|.$$

5.2. Γράφοντας $b(x) = \{x\} - \frac{1}{2}$, αποδείξτε ότι

$$\zeta(s) = \frac{s}{s-1} - \frac{1}{2} - s \int_1^\infty \frac{b(x)}{x^{s+1}} dx.$$

Συμπεράνατε ότι το δεξιό μέλος είναι μια αναλυτική συνέχιση της $\zeta(s)$ στο $\sigma > -1$ και ότι

$$\zeta(0) = -\frac{1}{2}.$$

5.3. Έστω $b > 0$, $T \geqslant 1$ και $0 < y < 1$. Αποδείξτε ότι

$$\frac{1}{2\pi i} \int_{b-iT}^{b+iT} \frac{y^s}{s} ds = O\left(\frac{y^b}{T |\ln y|}\right).$$

5.4. Αποδείξτε ότι

$$\lim_{s \to 1} (1-s) \frac{\zeta'(s)}{\zeta(s)} = 1.$$

5.5. Αποδείξτε ότι για $0 < \sigma < 1$,
$$-\frac{1}{1-\sigma} < \zeta(\sigma) < 0.$$

5.6. Αποδείξτε ότι για $\sigma > 1$,
$$-\frac{\zeta'(s)}{\zeta(s)} = s\int_1^\infty \frac{\psi(x)}{x^{s+1}}dx.$$

ΚΕΦΑΛΑΙΟ 6

Σειρές Dirichlet

6.1 Απόλυτη σύγκλιση σειρών Dirichlet

Σειρά Dirichlet είναι μια σειρά της μορφής

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \qquad s = \sigma + it,$$

όπου $f(n)$ είναι μια αριθμητική συνάρτηση.

Παρατηρήστε ότι αν $\sigma \geqslant a$ τότε $|n^s| \geqslant n^a$. Συνεπώς,

$$\left| \frac{f(n)}{n^s} \right| \leqslant \frac{|f(n)|}{n^a}.$$

Έπεται ότι αν μια σειρά Dirichlet συγκλίνει απολύτως για κάποιον $s = a + ib$, τότε από το κριτήριο σύγκρισης συγκλίνει επίσης απολύτως για κάθε s με $\sigma \geqslant a$. Από αυτή την παρατήρηση παίρνουμε το ακόλουθο θεώρημα.

Θεώρημα 6.1.1. *Έστω ότι η σειρά*

$$\sum_{n=1}^{\infty} \left| \frac{f(n)}{n^s} \right|$$

δεν συγκλίνει για όλους τους s ή αποκλίνει για κάθε s. Τότε υπάρχει ένας πραγματικός αριθμός σ_a που λέγεται τετμημένη της απόλυτης σύγκλισης, τέτοιος ώστε η σειρά

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

να συγκλίνει απολύτως αν $\sigma > \sigma_a$ αλλά να μην συγκλίνει απολύτως αν $\sigma < \sigma_a$.

Απόδειξη. Έστω D το σύνολο όλων των πραγματικών σ για τους οποίους η σειρά

$$\sum_{n=1}^{\infty} \left| \frac{f(n)}{n^s} \right|$$

αποκλίνει. Τότε το D είναι μη κενό, διότι η σειρά δεν συγκλίνει για κάθε s. Το σύνολο D είναι άνω φραγμένο αφού η σειρά δεν αποκλίνει για κάθε s. Άρα, το D έχει ελάχιστο άνω φράγμα το οποίο ονομάζουμε σ_a. Αν $\sigma < \sigma_a$ τότε $\sigma \in D$, αλλιώς το σ θα ήταν άνω φράγμα για το D, μικρότερο από το ελάχιστο άνω φράγμα του. Αν $\sigma > \sigma_a$ τότε $\sigma \notin D$ αφού το σ_a είναι άνω φράγμα του D. Αυτό αποδεικνύει το θεώρημα. □

6.2 Το θεώρημα μοναδικότητας

Θεώρημα 6.2.1. *Έστω ότι οι σειρές*

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \textit{και} \quad G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$$

συγκλίνουν απολύτως για $\sigma \geqslant \sigma_0$. *Αν* $F(s) = G(s)$ *για κάθε* s *που είναι όρς μιας άπειρης ακολουθίας* $\{s_k\}$ *τέτοιας ώστε* $\sigma_k \to \infty$ *καθώς* $k \to \infty$, *τότε* $f(n) = g(n)$ *για κάθε* n.

Απόδειξη. Θέτουμε $h(n) = f(n) - g(n)$ και $H(s) = F(s) - G(s)$. Τότε $H(s_k) = 0$ για κάθε k. Για να δείξουμε ότι $h(n) = 0$ για κάθε n υποθέτουμε ότι $h(n) \neq 0$ για κάποιον n και θα καταλήξουμε σε αντίφαση.

Έστω N ο μικρότερος ακέραιος n για τον οποίο

$$h(n) \neq 0. \tag{6.2.1}$$

Τότε

$$H(s) = \sum_{n=N}^{\infty} \frac{h(n)}{n^s} = \frac{h(N)}{n^s} + \sum_{n=N+1}^{\infty} \frac{h(n)}{n^s}.$$

Άρα,

$$h(N) = N^s H(s) - N^s \sum_{n=N+1}^{\infty} \frac{h(n)}{n^s}.$$

Θέτοντας $s = s_k$ έχουμε $H(s_k) = 0$, άρα

$$h(N) = -N^{s_k} \sum_{n=N+1}^{\infty} \frac{h(n)}{n^{s_k}}.$$

Επιλέγουμε k έτσι ώστε $\sigma_k > c$ όπου $c > \sigma_a$. Τότε,

$$|h(N)| \leqslant N^{\sigma_k} (N+1)^{-(\sigma_k - c)} \sum_{n=N+1}^{\infty} |h(n)| n^{-c} = \left(\frac{N}{N+1} \right)^{\sigma_k} A,$$

όπου η σταθερά A είναι ανεξάρτητη από το k. Αφήνοντας το $k \to \infty$ βλέπουμε ότι

$$\left(\frac{N}{N+1} \right)^{\sigma_k} \to 0.$$

Άρα, $h(N) = 0$, το οποίο αντιφάσκει προς την (6.2.1). Έπεται ότι $h(n) = 0$ για όλους τους θετικούς ακεραίους n. □

Αυτό το αποτέλεσμα είναι πολύ χρήσιμο. Για παράδειγμα, έστω $f(n)$ μια πλήρως πολλαπλασιαστική συνάρτηση. Ας υποθέσουμε ότι οι

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

και

$$G(s) = \sum_{n=1}^{\infty} \frac{f^{-1}(n)}{n^s}$$

συγκλίνουν απολύτως για $\sigma \geqslant \sigma_0$. Τότε γνωρίζουμε ότι

$$G(s) = \frac{1}{F(s)} = \prod_p \left(1 - \frac{f(p)}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)f(s)}{n^s}.$$

Από το Θεώρημα 6.2.1, αυτό δείχνει ότι

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

6.3 Πολλαπλασιασμός σειρών Dirichlet

Το επόμενο θεώρημα συνδέει το γινόμενο δύο σειρών Dirichlet με τη συνέλιξη Dirichlet των συντελεστών τους.

Θεώρημα 6.3.1. *Έστω $F(s)$ και $G(s)$ δύο συναρτήσεις που αναπαρίστανται από τις σειρές Dirichlet*

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \text{για } \sigma > a$$

και

$$G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \quad \text{για } \sigma > b.$$

Τότε, στο ημιεπίπεδο στο οποίο και οι δύο σειρές συγκλίνουν απολύτως, έχουμε

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{(f]astg)(n)}{n^s}.$$

Αν

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{\alpha(n)}{n^s}$$

για κάθε s που είναι όρς μιας άπειρης ακολουθίας $\{s_k\}$ τέτοιας ώστε $\sigma_k \to \infty$ καθώς $k \to \infty$, τότε $\alpha = f * g$.

Απόδειξη. Για κάθε s για τον οποίο και οι δύο σειρές συγκλίνουν απολύτως, έχουμε

$$F(s)G(s) = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{f(n)g(m)}{(nm)^s}.$$

Λόγω της απόλυτης σύγκλισης, μπορούμε να πολλαπλασιάσουμε αυτές τις σειρές μαζί και να διατάξουμε τους όρους με όποιον τρόπο θέλουμε χωρίς να μεταβληθεί το άθροισμα. Παίρνουμε μαζί εκείνους τους όρους για τους οποίους το γινόμενο mn είναι σταθερό, ας πούμε $mn = k$. Οι τιμές που μπορεί να πάρει το k είναι $1, 2, \ldots$, άρα

$$F(s)G(s) = \sum_{k=1}^{\infty} \frac{1}{k^s} \left(\sum_{mn=k} f(n)g(m) \right) = \sum_{k=1}^{\infty} \frac{h(k)}{k^s},$$

όπου

$$h(k) = \sum_{mn=k} f(n)g(m) = (f * g)(k).$$

Αυτό αποδεικνύει τον πρώτο ισχυρισμό. Ο δεύτερος ισχυρισμός προκύπτει από το Θεώρημα 6.2.1.

□

6.4 Σύγκλιση υπό συνθήκη σειρών Dirichlet

Θεώρημα 6.4.1. *Για κάθε σειρά Dirichlet υπάρχει $\sigma_c \in [-\infty, \infty]$ τέτοιος ώστε η σειρά να συγκλίνει (υπό συνθήκη) για κάθε s με $\sigma > \sigma_c$ και να αποκλίνει για κάθε s με $\sigma < \sigma_c$. Επιπλέον,*

$$\sigma_c \leqslant \sigma_a \leqslant \sigma_c + 1.$$

Απόδειξη. Θα αποδείξουμε ότι αν η

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

συγκλίνει για $s = s_1$, τότε συγκλίνει επίσης για κάθε s με $\sigma > \sigma_1$.

Αφού η

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

συγκλίνει στο $s = s_1$, συμπεραίνουμε ότι υπάρχει θετικός ακέραιος N_0 τέτοιος ώστε

$$\left| \sum_{x<n\leqslant y} \frac{f(n)}{n^{s_1}} \right| \leqslant 1$$

για κάθε $x, y > N_0$. Τώρα, έστω s με $\sigma > \sigma_1$ και έστω $y \geqslant x \geqslant N_0$. Έστω επίσης $\varepsilon > 0$. Τότε

$$\begin{aligned} \sum_{x<n\leqslant y} \frac{f(n)}{n^s} &= \sum_{x<n\leqslant y} \frac{f(n)}{n^{s_1}} n^{s_1-s} \\ &= \sum_{x<n\leqslant y} \frac{f(n)}{n^{s_1}} y^{s_1-s} - \int_x^y \sum_{x<n\leqslant t} \frac{f(n)}{n^{\sigma_1}} t^{s_1-s-1}(s_1-s)dt. \end{aligned}$$

Συνεπώς,

$$\left|\sum_{x<n\leqslant y}\frac{f(n)}{n^s}\right| \leqslant x^{\sigma_1-\sigma}+\int_x^y |s_1-s|t^{\sigma_1-\sigma-1}dt \tag{6.4.1}$$
$$\leqslant x^{\sigma_1-\sigma}\left(1+\frac{|s_1-s|}{\sigma-\sigma_1}\right)$$
$$<\varepsilon$$

αν υποθέσουμε ότι

$$x\geqslant\left\{\left(1+\frac{|s_1-s|}{\sigma-\sigma_1}\right)\varepsilon\right\}^{-1/(\sigma-\sigma_1)}.$$

Έχουμε λοιπόν δείξει ότι για κάθε $\varepsilon>0$ και για σταθερό s με $\sigma>\sigma_1$

$$\left|\sum_{x<n\leqslant y}\frac{f(n)}{n^s}\right|<\varepsilon$$

αν υποθέσουμε ότι

$$y\geqslant x\geqslant\min\left(N_0,\left\{\left(1+\frac{|s_1-s|}{\sigma-\sigma_1}\right)\varepsilon\right\}^{-1/(\sigma-\sigma_1)}\right).$$

Αυτό αποδεικνύει τη σύγκλιση της σειράς Dirichlet στο s.

Τώρα, έστω

$$\sigma_c:=\inf\left\{\mathrm{Re}s:\ \text{η σειρά }\sum_{n=1}^{\infty}\frac{f(n)}{n^s}\text{ συγκλίνει}\right\}. \tag{6.4.2}$$

Αν $\sigma>\sigma_a$ τότε από το προηγούμενο επιχείρημα συμπεραίνουμε ότι η $F(s)$ συγκλίνει αν $\sigma=\sigma_a+\delta$, $\delta>0$. Συνεπώς, συμπεραίνουμε ότι $\sigma_a\geqslant\sigma_c$.

Μένει να δείξουμε ότι $\sigma_a\leqslant\sigma_c+1$. Δείχνουμε πρώτα ότι αν η

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

σσυγκλίνει στο $s=s_1$ τότε συγκλίνει απολύτως σε κάθε s με $\sigma\geqslant\sigma_1+1$. Η σύγκλιση της σειράς

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^{s_1}}$$

συνεπάγεται ότι $f(n)n^{-s_1}\to 0$ καθώς $n\to\infty$, άρα

$$\left|\frac{f(n)}{n^{s_1}}\right|\leqslant C$$

για κάθε $n\in\mathbb{N}$ και κάποια θετική σταθερά C. Αν μας δώσουν s με $\sigma>\sigma_1+1$, τότε

$$\left|\frac{f(n)}{n^s}\right|=\left|\frac{f(n)}{n^{s_1}}\right|\frac{1}{n^{\sigma-\sigma_1}}\leqslant\frac{C}{n^{\sigma-\sigma_1}},$$

και $\sigma - \sigma_1 > 1$. Συνεπώς, για κάθε θετικό ακέραιο m,

$$\sum_{n=1}^{m} \left| \frac{f(n)}{n^s} \right| \leqslant \sum_{n=1}^{m} \frac{C}{n^{\sigma-\sigma_1}} < \infty.$$

Αφού $\sigma - \sigma_1 > 1$, η σειρά

$$\sum_{n=1}^{\infty} \frac{1}{n^{\sigma-\sigma_1}}$$

συγκλίνει. Από το κριτήριο σύγκρισης, συμπεραίνουμε ότι η

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

συγκλίνει απολύτως.

Τώρα, έχουμε αποδείξει ότι αν η

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

συγκλίνει στο $\sigma > \sigma_1 + 1$, τότε η $\sum\limits_{n=1}^{\infty} \frac{f(n)}{n^s}$ συγκλίνει απολύτως. Αυτό σημαίνει ότι ο $\sigma_1 + 1$ είναι άνω φράγμα για το σύνολο των πραγματικών αριθμών για τους οποίους η σειρά Dirichlet συγκλίνει απολύτως, άρα $\sigma_1 + 1 \geqslant \sigma_a$ αφού ο σ_a είναι το ελάχιστο άνω φράγμα. Όμως $\sigma_1 = \sigma_c + \delta$ για τυχόν $\delta > 0$, άρα

$$\sigma_c + 1 \geqslant \sigma_a.$$

□

6.5 Το θεώρημα του Landau για τις σειρές Dirichlet

Θεώρημα 6.5.1. *Η σειρά Dirichlet*

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

είναι αναλυτική στο ημιεπίπεδο $\sigma > \sigma_c$, όπου η σ_c ορίζεται από την (6.4.2).

Η απόδειξη αυτού του αποτελέσματος προκύπτει από το [1, σελ. 176, Θεώρημα 1], την ανισότητα (6.4.1) και το γεγονός ότι σε ένα συμπαγές σύνολο μπορούμε να φράξουμε τα $\sigma - \sigma_1$ και $|s_1 - s|$ από ποσότητες που δεν εξαρτώνται από το s. Για περισσότερες λεπτομέρειες της απόδειξης παραπέμπουμε στο [2, Θεώρημα 11.11].

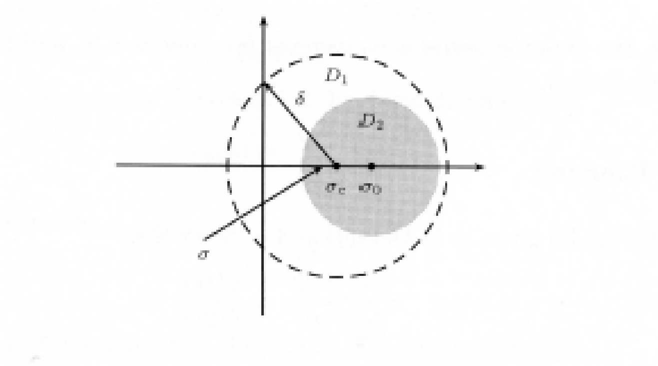
Ερχόμαστε τώρα στο κύριο θεώρημα αυτού του κεφαλαίου.

Θεώρημα 6.5.2. *Έστω*

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

μια σειρά Dirichlet με $f(n) \geqslant 0$ για κάθε $n \in \mathbb{N}$ και $\sigma_c < \infty$. Τότε η συνάρτηση $F(s)$ έχει ανωμαλία στο $s = \sigma_c$.

Απόδειξη. Υποθέτουμε ότι η $F(s)$ είναι αναλυτική στο σ_c. Τότε υπάρχει $\delta > 0$ τέτοιος ώστε η $F(s)$ να είναι αναλυτική στον δίσκο $D_1 := \{s : |s - \sigma_c| < \delta\}$. Σταθεροποιούμε ένα σημείο στον πραγματικό άξονα, ας πούμε $\sigma_0 > \sigma_c$, που περιέχεται σε αυτόν τον δίσκο και $\varepsilon > 0$ τέτοιον ώστε ολόκληρος ο δίσκος $D_2 := \{s : |s-\sigma_0| < \varepsilon\}$ να περιέχεται στον D_1 και $\sigma_c \in D_2$ (δείτε το παρακάτω σχήμα).



Σχήμα 6.1: Διάγραμμα που χρησιμοποιείται για να περιγράψει την επιλογή των δίσκων D_1 και D_2.

Αφού η $F(s)$ είναι αναλυτική στον D_2, έχουμε το ανάπτυγμα

$$F(s) = \sum_{n=0}^{\infty} \frac{F^{(n)}(\sigma_0)}{n!}(s - \sigma_0)^n.$$

Τώρα, $\sigma_0 > \sigma_c$, άρα η $F(s)$ δίνεται από την

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

Αφού η $F(s)$ είναι αναλυτική στο σ_0, μπορούμε βα παραγωγίσουμε αυτή τη σχέση όρο προς όρο, και παίρνουμε

$$F^{(\nu)}(\sigma_0) = \sum_{n=1}^{\infty} (-1)^{\nu} \frac{f(n) \ln^{\nu} n}{n^{\sigma_0}}.$$

Αντικαθιστώντας στο ανάπτυγμα Taylor βλέπουμε ότι

$$F(s) = \sum_{\nu=0}^{\infty} \frac{(\sigma_0 - s)^{\nu}}{\nu!} \sum_{n=1}^{\infty} \left(\frac{f(n) \ln^{\nu} n}{n^{\sigma_0}} \right).$$

Τώρα, θεωρώντας τον s πραγματικό, ας πούμε με $\sigma_0 - \varepsilon < s = \sigma < \sigma_0$, έχουμε

$$\begin{aligned}F(\sigma) &= \sum_{\nu=0}^{\infty} \frac{(\sigma_0 - \sigma)^\nu}{\nu!} \sum_{n=1}^{\infty} \left(\frac{f(n) \ln^\nu n}{n^{\sigma_0}} \right) \\ &= \sum_{n=1}^{\infty} \frac{f(n)}{n^{\sigma_0}} \sum_{\nu=0} \frac{(\sigma_0 - \sigma)^\nu \ln^\nu n}{\nu!} \\ &= \sum_{n=1}^{\infty} \frac{f(n)}{n^{\sigma_0}} \exp((\sigma_0 - \sigma) \ln n)) \\ &= \sum_{n=1}^{\infty} \frac{f(n)}{n^{\sigma_0}} n^{\sigma_0 - \sigma} = \sum_{n=1}^{\infty} \frac{f(n)}{n^{\sigma}}.\end{aligned}$$

Άρα, η σειρά Dirichlet συγκλίνει για κάποιο $\sigma < \sigma_c$ και αυτό οδηγεί σε αντίφαση. □

6.6 Ασκήσεις

6.1. Έστω $\omega(n)$ η συνάρτηση που ορίστηκε στην Άσκηση 3.4. Αποδείξτε ότι

$$\sum_{n=1}^{\infty} \frac{2^{\omega(n)}}{n^s} = \frac{\zeta^2(s)}{\zeta(2s)}.$$

6.2. Αποδείξτε ότι

$$\sum_{(m,n)=1} \frac{1}{m^2 n^2} = \frac{\zeta^2(2)}{\zeta(4)}.$$

6.3. Αποδείξτε ότι αν $\kappa(1) = 1$ και $\kappa(n) = \alpha_1 \alpha_2 \cdots \alpha_k$ όταν $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, τότε για $s > 1$,

$$\sum_{n=1}^{\infty} \frac{\kappa(n)}{n^s} = \frac{\zeta(s)\zeta(2s)\zeta(3s)}{\zeta(6s)}.$$

6.4. Έστω f μια πλήρως πολλαπλασιαστική συνάρτηση τέτοια ώστε $f(p) = f(p)^2$ για κάθε πρώτο p. Αν η σειρά

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

συγκλίνει απολύτως για $\sigma > \sigma_a$ και έχει άθροισμα $F(s)$, αποδείξτε ότι

$$\sum_{n=1}^{\infty} \frac{f(n)\lambda(n)}{n^s} = \frac{F(2s)}{F(s)} \quad \text{αν } \sigma > \sigma_a,$$

και $F(s) \neq 0$.

6.5. Ορίζουμε

$$F(\sigma, t) = 3\frac{\zeta'}{\zeta}(\sigma) + 4\frac{\zeta'}{\zeta}(\sigma + it) + \frac{\zeta'}{\zeta}(\sigma + 2it).$$

Αν $\sigma > 1$, αποδείξτε ότι η $F(\sigma, t)$ έχει πραγματικό μέρος ίσο με

$$-\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^\sigma} \mathrm{Re}\{3 + 4n^{-it} + n^{-2it}\}$$

και συμπεράνατε ότι

$$\mathrm{Re}F(\sigma, t) \leqslant 0.$$

6.6. Έστω $c_q(n)$ η συνάρτηση που ορίστηκε στην Άσκηση 2.3. Αποδείξτε ότι

$$c_q(n) = \sum_{d|(n,q)} d\mu\left(\frac{q}{d}\right),$$

και συμπεράνατε ότι

$$\frac{\sigma(n)}{n} = \frac{\pi^2}{6}\sum_{q=1}^{\infty}\frac{c_q(n)}{q^2}.$$

6.7. Αποδείξτε ότι για $\sigma > \sigma_a$,

$$\sum_{n=1}^{\infty}\frac{d(n^2)}{n^s} = \frac{\zeta^3(s)}{\zeta(2s)}.$$

Από αυτή τη σχέση ή με οποιονδήποτε άλλο τρόπο, δείξτε ότι

$$\mu^2 * d = \mu * d^2.$$

6.8. Αποδείξτε ότι για $\sigma > 1$,

$$\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{1}{[m,n]^\sigma} = \frac{\zeta^3(\sigma)}{\zeta(2\sigma)}.$$

6.9. Αποδείξτε ότι για $\sigma > 1$,

$$\sum_{n=1}^{\infty}\frac{2^{\omega(n)}\lambda(n)}{n^\sigma} = \frac{\zeta(2\sigma)}{\zeta^2(\sigma)}.$$

ΚΕΦΑΛΑΙΟ 7

Πρώτοι σε αριθμητικές προόδους

7.1 Εισαγωγή

Στο Κεφάλαιο 4 αποδείξαμε ότι υπάρχουν άπειροι πρώτοι αριθμοί δείχνοντας ότι (δείτε το Θεώρημα 4.4.1 (γ))

$$\sum_{p\leqslant x}\frac{1}{p}=\ln\ln x+O(1). \tag{7.1.1}$$

Το θεώρημα του Dirichlet για τους πρώτους σε αριθμητικές προόδους ισχυρίζεται ότι αν $(k,\ell)=1$ τότε υπάρχουν άπειροι πρώτοι της μορφής $kn+\ell$. Αν μπορούσαμε να αποδείξουμε ένα αποτέλεσμα παρόμοιο με την (7.1.1), με το άθροισμα πάνω από τους πρώτους p να αντικαθίσταται από άθροισμα πάνω από τους πρώτους της μορφής $kn+\ell$, τότε θα είχαμε ως συνέπεια το θεώρημα του Dirichlet. Αυτή η στρατηγική μας οδηγεί στο επόμενο θεώρημα.

Θεώρημα 7.1.1. *Έστω $k>1$ και ℓ θετικοί ακέραιοι τέτοιοι ώστε $(k,\ell)=1$. Τότε*

$$\sum_{\substack{p\leqslant x\\ p\equiv \ell \pmod k}}\frac{1}{p}=\frac{\ln\ln x}{\varphi(k)}+O(1).$$

Από το Θεώρημα 7.1.1 παίρνουμε άμεσα το θεώρημα του Dirichlet για τους πρώτους σε αριθμητικές προόδους.

Θεώρημα 7.1.2 (το θεώρημα του Dirichlet για τους πρώτους σε αριθμητικές προόδους)**.** *Αν k και ℓ είναι θετικοί ακέραιοι τέτοιοι ώστε $(k,\ell)=1$, τότε υπάρχουν άπειροι πρώτοι της μορφής $kn+\ell$.*

7.2 Χαρακτήρες Dirichlet

Ορισμός 7.2.1. Χαρακτήρας Dirichlet $(\mathrm{mod}\ k)$ είναι μια αριθμητική συνάρτηση

$$\chi:\mathbb{N}\to\mathbb{C}$$

που ικανοποιεί τα ακόλουθα:

(α) $\chi(mn) = \chi(m)\chi(n)$ για κάθε $m, n \in \mathbb{N}$.

(β) $|\chi(n)| = \begin{cases} 1 & , \text{ αν } (n,k) = 1 \\ 0 & , \text{ αλλιώς} \end{cases}$.

(γ) $\chi(n + km) = \chi(n)$ για κάθε $n, m \in \mathbb{N}$.

(δ) $\chi^{\varphi(k)}(n) = 1$, $(n, k) = 1$.

Παρατήρηση 7.2.2. (i) Οι τιμές του χ είναι 0 ή $\varphi(k)$-οστές ρίζες της μονάδας. Αυτό προκύπτει από το (α).

(ii) Υπάρχουν πεπερασμένοι το πλήθος χαρακτήρες $(\bmod\ k)$. Αυτό προκύπτει από το γεγονός ότι ο χ ορίζεται σε $\varphi(k)$ τιμές j με $1 \leqslant j \leqslant k$ και $(j, k) = 1$. Άρα, από το (δ), βλέπουμε ότι για κάθε k υπάρχουν $\varphi(k)$ τιμές που μπορούμε να δώσουμε στο $\chi(j)$. Αυτό δείχνει ότι υπάρχουν το πολύ $\varphi(k)^{\varphi(k)}$ χαρακτήρες.

(iii) Αν χ_1 και χ_2 είναι δύο χαρακτήρες $(\bmod\ k)$ τότε η $\chi_1\chi_2$ είναι επίσης χαρακτήρας.

(iv) Κάθε χαρακτήρας χ $(\bmod\ k)$ προκύπτει από έναν ομομορφισμό

$$\tilde{\chi} : (\mathbb{Z}/k\mathbb{Z})^* \to \{z \in \mathbb{C} : |z| = 1\}$$

όπου $(\mathbb{Z}/k\mathbb{Z})^*$ είναι η πολλαπλασιαστική ομάδα των κλάσεων υπολοίπων

$$(\{[n]_k : (n, k) = 1\}, \cdot),$$

με τον πολλαπλασιασμό $\cdot$ ως πράξη της ομάδας. Για κάθε χαρακτήρα $\tilde{\chi}$, ορίζουμε

$$\chi(n) = \begin{cases} \tilde{\chi}([n]_k) & , \text{ αν } (n,k) = 1 \\ 0 & , \text{ αλλιώς} \end{cases}.$$

Αντίστροφα, αν μας δοθεί ο χ, μπορούμε να ορίσουμε έναν ομομορφισμό $\tilde{\chi}$ μέσω της

$$\tilde{\chi}([n]_k) = \chi(n).$$

Αυτό δείχνει ότι υπάρχει ένα προς ένα αντιστοιχία ανάμεσα στους χαρακτήρες Dirichlet $(\bmod\ k)$ και τους ομομορφισμούς από την $(\mathbb{Z}/k\mathbb{Z})^*$ στον $\{z \in \mathbb{C} : |z| = 1\}$.

Θεώρημα 7.2.3. *Υπάρχουν ακριβώς $\varphi(k)$ χαρακτήρες* $(\bmod\ k)$.

Απόδειξη. Από την Παρατήρηση 7.2.2 (δ), αρκεί να δείξουμε ότι υπάρχουν ακριβώς $\varphi(k)$ ομομορφισμοί από την $(\mathbb{Z}/k\mathbb{Z})^*$ στον $\{z \in \mathbb{C} : |z| = 1\}$,

Από το θεώρημα δομής των αβελιανών ομάδων (βλέπε [8, Θεώρημα 8.2]) γνωρίζουμε ότι η $(\mathbb{Z}/k\mathbb{Z})^*$ γράφεται ως ευθύ άθροισμα κυκλικών ομάδων με τάξη δύναμη πρώτου, δηλαδή,

$$(\mathbb{Z}/k\mathbb{Z})^* = C_{h_1} \times \cdots \times C_{h_r},$$

όπου οι h_i είναι δυνάμεις πρώτων και γράφουμε C_m για μια κυκλική ομάδα τάξης m.

Έστω $[a_i]_k$ ένας γεννήτορας της C_{h_i}, $1 \leqslant i \leqslant r$. Εαν τα $w_1, \ldots, w_r$ ικανοποιούν την

$$w_i^{h_i} = 1,$$

θέτουμε

$$\tilde{\chi}([a_i]_k) = w_i, \qquad 1 \leqslant i \leqslant r.$$

Αν

$$[n]_k = \prod_i [a_i]_k^{\alpha_i},$$

τότε ορίζουμε

$$\tilde{\chi}([n]_k) = \prod_i \tilde{\chi}([a_i]_k)^{\alpha_i}.$$

Παρατηρούμε ότι η $\tilde{\chi}$ είναι ομομορφισμός από την $(\mathbb{Z}/k\mathbb{Z})^*$ στον $\{z \in \mathbb{C} : |z| = 1\}$. Συνεπώς, έχουμε τουλάχιστον

$$h_1 \cdots h_r = \varphi(k)$$

τέτοιους ομομορφισμούς.

Τώρα, έστω $[a]_k \in (\mathbb{Z}/k\mathbb{Z})^*$. Τότε

$$[a]_k = [a_1]_k^{\alpha_1} \cdots [a_r]_k^{\alpha_r}$$

όπου

$$0 \leqslant \alpha_i \leqslant h_i - 1.$$

Τώρα, αν $\tilde{\chi}$ είναι ένας ομομορφισμός από την $(\mathbb{Z}/k\mathbb{Z})^*$ στον $\{z \in \mathbb{C} : |z| = 1\}$, έχουμε

$$\tilde{\chi}([a]_k) = \prod_i \tilde{\chi}([a_i]_k)^{\alpha_i}.$$

Η τιμή $\tilde{\chi}([a]_k)$ εξαρτάται από τις τιμές $\tilde{\chi}([a_i]_k)$, $1 \leqslant i \leqslant r$. Το πλήθος των τιμών που μπορεί να πάρει η $\tilde{\chi}([a_i]_k)$ είναι h_i, $1 \leqslant i \leqslant r$. Συνεπώς, υπάρχουν το πολύ $h_1 h_2 \cdots h_r = \varphi(k)$ χαρακτήρες. Από τα παραπάνω συμπεραίνουμε ότι υπάρχουν ακριβώς $\varphi(k)$ χαρακτήρες $(\mathrm{mod}\ k)$. $\square$

Ο χαρακτήρας χ_0 θα είναι σε ό,τι ακολουθεί ο κύριος χαρακτήρας $(\mathrm{mod}\ k)$, ο οποίος ορίζεται ως εξής:

$$\chi_0(n) = \begin{cases} 1 & , \text{ αν } (n,k) = 1 \\ 0 & , \text{ αλλιώς} \end{cases}.$$

Με το σύμβολο $\overline{\chi}$ θα εννοούμε τον αντίστροφο του χ, δηλαδή, $\chi \cdot \overline{\chi} = \chi_0$.

7.3 Οι σχέσεις ορθογωνιότητας

Θεώρημα 7.3.1. (α) *Έστω χ_1, χ_2 δύο χαρακτήρες Dirichlet* modulo k. *Τότε*

$$\sum_{a=1}^{k} \chi_1(a)\overline{\chi_2(a)} = \begin{cases} \varphi(k) & , \textit{ αν } \chi_1 = \chi_2 \\ 0 & , \textit{ αλλιώς} \end{cases}.$$

(β) *Έστω a_1, a_2 ακέραιοι με $(a_i, k) = 1$. Τότε*

$$\sum_{\chi \pmod{k}} \chi(a_1)\overline{\chi(a_2)} = \begin{cases} \varphi(k) & , \text{ αν } a_1 \equiv a_2 \pmod{k} \\ 0 & , \text{ αλλιώς} \end{cases}.$$

Απόδειξη. (α) Θα αποδείξουμε αρχικά το ακόλουθο:

$$\sum_{a=1}^{k} \chi(a) = \begin{cases} \varphi(k) & , \text{ αν } \chi = \chi_0 \\ 0 & , \text{ αλλιώς} \end{cases}. \tag{7.3.1}$$

Παρατηρούμε πρώτα ότι, αφού $\chi(\ell) = 0$ οποτεδήποτε $(\ell, k) \neq 1$, πρέπει να έχουμε

$$\sum_{a=1}^{k} \chi(a) = \sum_{\substack{a=1 \\ (a,k)=1}}^{k} \chi(a).$$

Αν $\chi = \chi_0$, τότε για $(a, k) = 1$ έχουμε $\chi(a) = 1$ και

$$\sum_{z=1}^{k} \chi(a) = \sum_{\substack{a=1 \\ (a,k)=1}}^{k} \chi(a) = \sum_{\substack{a=1 \\ (a,k)=1}}^{k} \mathbf{1} = \varphi(k).$$

Αν $\chi \neq \chi_0$, τότε υπάρχει κάποιος a_0 σχετικά πρώτος προς τον k τέτοιος ώστε $\chi(a_0) \neq 1$. Έχουμε

$$\begin{aligned} \chi(a_0) \sum_{i=1}^{k} \chi(a) &= \tilde{\chi}([a_0]_k) \sum_{[a]_k \in (\mathbb{Z}/k\mathbb{Z})^*} \tilde{\chi}([a]_k) \\ &= \sum_{[a]_k \in (\mathbb{Z}/k\mathbb{Z})^*} \tilde{\chi}([a_0]_k [a]_k). \end{aligned}$$

Τώρα, ο πολλαπλασιασμός των στοιχείων της $(\mathbb{Z}/k\mathbb{Z})^*$ με $[a_0]_k$ εταθέτει τα στοιχεία της $(\mathbb{Z}/k\mathbb{Z})^*$. Άρα,

$$\sum_{[a]_k \in (\mathbb{Z}/k\mathbb{Z})^*} \tilde{\chi}([a_0]_k [a]_k) = \sum_{[a]_k \in (\mathbb{Z}/k\mathbb{Z})^*} \tilde{\chi}([a]_k) = \sum_{a=1}^{k} \chi(a).$$

Άρα, συμπεραίνουμε ότι

$$\sum_{i=1}^{k} \chi(a) = 0.$$

Τώρα, θέτοντας $\chi = \chi_1 \overline{\chi_2}$ στην (7.3.1) ολοκληρώνουμε την απόδειξη του (α).

(β) Θα αποδείξουμε αρχικά το ακόλουθο:

$$\sum_{\chi \pmod{k}} \chi(a) = \begin{cases} \varphi(k) & , \text{ αν } a \equiv 1 \pmod{k} \\ 0 & , \text{ αλλιώς} \end{cases}. \tag{7.3.2}$$

Αν $a \equiv 1 \pmod{k}$ τότε $\chi(a) = 1$ για όλους τους χαρακτήρες χ. Αφού υπάρχουν ακριβώς $\varphi(k)$ τέτοιοι χαρακτήρες, συμπεραίνουμε ότι

$$\sum_{\chi \pmod{k}} \chi(a) = \varphi(k).$$

Ας υποθέσουμε τώρα ότι $a \neq 1 \pmod{k}$. Τότε υπάρχει ένας χαρακτήρας χ^* τέτοιος ώστε $\chi^*(a) \neq 1$. Άρα,

$$\chi^*(a) \sum_{\chi \ (\mathrm{mod}\ k)} \chi(a) = \sum_{\chi \ (\mathrm{mod}\ k)} (\chi^* \chi)(a) = \sum_{\chi \ (\mathrm{mod}\ k)} \chi(a),$$

όπου χρησιμοποιήσαμε το γεγονός ότι πολλαπλασιάζοντας τα στοιχεία του συνόλου των χαρακτήρων με τον χ^* μεταθέτουμε τα στοιχεία του συνόλου. Έπεται ότι

$$\sum_{\chi \ (\mathrm{mod}\ k)} \chi(a) = 0.$$

Τώρα, για να αποδείξουμε το (β), απλώς βλέπουμε τον χ ως $\tilde{\chi}$ και θέτουμε $[a]_k = [a_1]_k \overline{[a_2]}_k$ όπου $\overline{[a]}_k$ είναι ο αντίστροφος του $[a]_k$ στην ομάδα $(\mathbb{Z}/k\mathbb{Z})^*$, και παρατηρούμε ότι

$$\chi(a_1)\overline{\chi(a_2)} = \tilde{\chi}([a_1]_k)\tilde{\chi}(\overline{[a_2]}_k).$$

□

7.4 Οι L-σειρές του Dirichlet

Ορισμός 7.4.1. Η L-σειρά του Dirichlet ορίζεται ως εξής:

$$L(s,\chi) = \sum_{n \geqslant 1} \frac{\chi(n)}{n^s}, \qquad \sigma > 1.$$

Θεώρημα 7.4.2. (α) *Αν $\chi = \chi_0$ τότε η $L(s,\chi)$ έχει αναλυτική συνέχιση στο ημιεπίπεδο $\sigma > 0$, με την εξαίρεση του σημείου $s = 1$ όπου έχει απλό πόλο με υπόλοιπο $\varphi(k)/k$.*

(β) *Αν ο χ δεν είναι ο κύριος χαρακτήρας $\pmod{k}$, τότε η $L(s,\chi)$ έχει αναλυτική συνέχιση στο $\sigma > 0$.*

Απόδειξη. (α) Για $\sigma > 1$, από το Θεώρημα 5.3.2 έχουμε

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Συνεπώς,

$$\begin{aligned} L(s,\chi_0) &= \prod_{p \nmid k} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p \mid k} \left(1 - \frac{1}{p^s}\right) \\ &= \frac{\varphi(k)}{k} \prod_p \left(1 - \frac{1}{p^s}\right). \end{aligned}$$

Η συνάρτηση $\zeta(s)$ έχει αναλυτική συνέχιση με υπόλοιπο 1 στο $s = 1$. Συνεπώς, το υπόλοιπο της $L(s,\chi_0)$ στο $s = 1$ είναι ίσο με $\varphi(k)/k$.

(β) Αν $\chi \neq \chi_0$, τότε

$$\sum_{k=1}^{n} \chi(n) = 0.$$

Συνεπώς,

$$\left|\sum_{n\leqslant x}\chi(n)\right|\leqslant k$$

για $x\geqslant 1$. Συνεπώς, για κάθε $\varepsilon>0$,

$$\left|\sum_{y\leqslant n\leqslant x}\frac{\chi(n)}{n^s}\right|\leqslant\frac{1}{|y^s|}\left|\sum_{y\leqslant n\leqslant x}\chi(n)\right|<\frac{k}{|y|^\sigma}<\varepsilon,$$

αν υποθέσουμε ότι

$$|y|>\left(\frac{k}{\varepsilon}\right)^{1/\sigma}.$$

Αυτό συνεπάγεται ότι η L-σειρά συγκλίνει για $\sigma>0$. □

7.5 Απόδειξη του θεωρήματος του Dirichlet

Βήμα 1. Αρκεί να δείξουμε ότι αν $x\geqslant 3$ και

$$\sigma=1+\frac{1}{\ln x},$$

τότε

$$\sum_{p:p\equiv\ell\ (\mathrm{mod}\ k)}\frac{1}{p^\sigma}=\frac{1}{\varphi(k)}\ln\left(\frac{1}{\sigma-1}\right)+O(1).$$

Θέτουμε

$$\Sigma_1=\sum_{p\equiv\ell\ (\mathrm{mod}\ k)}\frac{1}{p^\sigma}\quad\text{και}\quad\Sigma_2=\sum_{\substack{p\leqslant x\\ p\equiv\ell\ (\mathrm{mod}\ k)}}\frac{1}{p},$$

που

$$\sigma=1+\frac{1}{\ln x}.$$

Τότε

$$|\Sigma_1-\Sigma_2|\leqslant\Sigma_3+\Sigma_4:=\sum_{p\leqslant x}\left(\frac{1}{p}-\frac{1}{p^\sigma}\right)+\sum_{p>x}\frac{1}{p^\sigma}.$$

Τώρα,

$$\begin{aligned}\Sigma_3&=\sum_{p\leqslant x}\frac{1-e^{-(\sigma-1)\ln p}}{p}\leqslant\sum_{p\leqslant x}\frac{(\sigma-1)\ln p}{p}\\&=\frac{1}{\ln x}\sum_{p\leqslant x}\frac{\ln p}{p}=O(1),\end{aligned}$$

και

$$\begin{aligned}
\Sigma_4 &= \lim_{y\to\infty} \sum_{x\leqslant p\leqslant y} \frac{1}{p^\sigma} \\
&= \lim_{y\to\infty} \left(\frac{1}{y^\sigma} \sum_{p\leqslant y} \mathbf{1} - \frac{1}{x^\sigma} \sum_{p\leqslant x} \mathbf{1} - \int_x^y \sum_{p\leqslant t} \mathbf{1} \left(-\frac{\sigma}{t^{\sigma+1}} \right) dt \right) \\
&= O(1) + \int_x^\infty O\left(\frac{t}{\ln t} \right) \frac{dt}{t^{\sigma+1}} \\
&= O(1) + O\left(\int_x^\infty \frac{dt}{t^\sigma \ln t} \right) \\
&= O(1) + O\left(\frac{1}{\ln x} \int_x^\infty \frac{dt}{t^\sigma} \right) = O(1).
\end{aligned}$$

Άρα, αν

$$\sigma = 1 + \frac{1}{\ln x},$$

τότε

$$\sum_{p:p\equiv \ell \pmod k} \frac{1}{p^\sigma} = \frac{1}{\varphi(k)} \ln \frac{1}{\sigma - 1} + O(1)$$

και το θεώρημα του Dirichlet ισχύει.

Βήμα 2. Παρατηρούμε ότι για $\sigma > 1$,

$$\begin{aligned}
\sum_{p:p\equiv \ell \pmod k} \frac{1}{p^\sigma} &= \sum_p \frac{1}{p^\sigma} \left(\frac{1}{\varphi(k)} \sum_{\chi \pmod k} \overline{\chi(\ell)} \chi(p) \right) \\
&= \frac{1}{\varphi(k)} \sum_{\chi \pmod k} \overline{\chi(\ell)} S(\sigma, \chi),
\end{aligned}$$

όπου

$$S(\sigma, \chi) = \sum_p \frac{\chi(p)}{p}.$$

Τώρα,

$$\sum_p \sum_{m\geqslant 1} \frac{1}{mp^{m\sigma}} - \sum_p \frac{1}{p^\sigma} = -\ln\left(1 - \frac{1}{p^\sigma}\right) - \sum_p \frac{1}{p^\sigma} = O(1),$$

αφού

$$\sum_p \sum_{m\geqslant 2} \frac{1}{mp^{m\sigma}} \leqslant \frac{1}{2} \sum_p \sum_{m\geqslant 2} \frac{1}{p^{m\sigma}} = \frac{1}{2} \sum_p \frac{1}{p^\sigma (p^\sigma - 1)} = O(1).$$

Συνεπώς,

$$\begin{aligned}
S(\sigma, \chi_0) &= \sum_p \sum_{m \geqslant 1} \frac{1}{mp^{m\sigma}} - \sum_{p|k} \sum_{m \geqslant 1} \frac{1}{mp^{m\sigma}} \\
&= -\sum_p \ln\left(1 - \frac{1}{p^\sigma}\right) + O(1) \\
&= \ln \prod_p \left(1 - \frac{1}{p^\sigma}\right)^{-1} + O(1) \\
&= \ln \zeta(\sigma) + O(1) \\
&= \ln\left(\frac{1}{\sigma - 1}\right) + O(1).
\end{aligned}$$

Η τελευταία ισότητα προοκύπτει από το γεγονός ότι για σ κοντά στο 1 έχουμε

$$\zeta(\sigma) = \frac{1}{\sigma - 1} + g(\sigma),$$

όπου $g(\sigma)$ είναι μια συνάρτηση αναλυτική στο 1. Συμπεραίνουμε έτσι ότι ο κύριος όρος προέρχεται από τον κύριο χαρακτήρα χ_0. Άρα, μένει να δείξουμε ότι

$$S(\sigma, \chi) = O(1)$$

για $\sigma > 1$ και για όλους τους μη-κύριους χαρακτήρες $\chi \pmod{k}$.

Βήμα 3. Χρησιμοποιώντας υπολογισμούς παρόμοιους με αυτούς του Βήματος 2, βλέπουμε ότι

$$\begin{aligned}
S(\sigma, \chi) = \sum_p \frac{\chi(p)}{p^\sigma} &= \sum_p \sum_{m \geqslant 1} \frac{\chi(p)^m}{mp^{m\sigma}} + O(1) \\
&= -\sum_p \ln\left(1 - \frac{\chi(p)}{p^\sigma}\right)^{-1} + O(1) \\
&= \ln(L(\sigma, \chi)) + O(1).
\end{aligned}$$

Τώρα, αν $\chi \neq \chi_0$ τότε η $L(s, \chi)$ είναι αναλυτική στο ημιεπίπεδο $\sigma > 0$. Άρα, η $L(\sigma, x)$ είναι συνεχής στο $\sigma > 1$ και

$$\lim_{\sigma \to 1} L(\sigma, \chi) = L(1, \chi).$$

Αν $L(1, \chi) \neq 0$, έχουμε τελειώσει. Απομένει λοιπόν να δείξουμε ότι $L(1, \chi) \neq 0$.

Βήμα 4. Αποδεικνύουμε πρώτα ότι αν $\chi \neq \chi_0$ είναι ένας μιγαδικός χαρακτήρας $\pmod{k}$, τότε

$$L(1, \chi) \neq 0.$$

Θεωρούμε την παράσταση

$$P(\sigma) = \prod_{\chi \pmod{k}} L(\sigma, \chi).$$

Βλέπουμε ότι για $\sigma > 1$,

$$\begin{aligned}\ln P(\sigma) &= \sum_{\chi \ (\mathrm{mod}\ k)} \ln L(\sigma,\chi) \\ &= \sum_{\chi \ (\mathrm{mod}\ k)} \sum_p \sum_{m\geqslant 1} \frac{\chi(p^m)}{mp^{m\sigma}} \\ &= \sum_p \sum_{m\geqslant 1} \frac{1}{mp^{m\sigma}} \sum_{\chi \ (\mathrm{mod}\ k)} \chi(p^m)\overline{\chi(1)} \\ &= \sum_p \sum_{\substack{m\geqslant 1 \\ p^m\equiv 1 \ (\mathrm{mod}\ k)}} \frac{1}{mp^{m\sigma}} \geqslant 0.\end{aligned}$$

Άρα, για $\sigma > 1$,

$$P(\sigma) \geqslant 1. \tag{7.5.1}$$

Ας υποθέσουμε ότι $L(1,\chi) = 0$ για κάποιον χ. Τότε $L(1,\overline{\chi}) = 0$. Άρα, η $P(s)$ έχει δύο ρίζες στο $s = 1$. Όμως η $L(s,\chi_0)$ έχει απλό πόλο στο $s = 1$, το οποίο σημαίνει ότι $P(1) = 0$. Αυτό έρχεται σε αντίφαση με την (7.5.1).

Βήμα 5. Σε αυτό το τελευταίο βήμα,αποδεικνύουμε ότι για πραγματικό χαρακτήρα $\chi \neq \chi_0$ ισχύει $L(1,\chi) \neq 0$. Θεωρούμε τη συνάρτηση $f = \chi * u$. Η f είναι πολλαπλασιαστική από το Θεώρημα 2.5.1. Παρατηρούμε ότι

$$\sum_{\ell=0}^{m} \chi_1(p^\ell) = \begin{cases} 1 & ,\ \text{αν } p \mid k \\ \geqslant 1 & ,\ \text{αν } p \nmid k,\ m \text{ άρτιος} \\ \geqslant 0 & ,\ \text{αν } p \nmid k,\ m \text{ περιττός} \end{cases}.$$

Άρα, $f(n) \geqslant 0$ για κάθε n και $f(n) \geqslant 1$ όταν ο n είναι τέλειο τετράγωνο. Συνεπώς,

$$F(\sigma) = \sum_{n\geqslant 1} \frac{f(n)}{n^\sigma} \geqslant \sum_{n\geqslant 1} \frac{1}{n^{2\sigma}} = \zeta(2\sigma).$$

Ειδικότερα, η $F(\sigma)$ αποκλίνει στο $\sigma = 1/2$, άρα $\sigma_c \geqslant 1/2$. Από το Θεώρημα 6.5.2, η $F(s)$ πρέπει να έχει ανωμαλία στο $s = \sigma_c \geqslant 1/2$.

Από την άλλη πλευρά, για $\sigma > 1$,

$$F(s) = L(s,\chi)\zeta(s).$$

Αν ίσχυε ότι $L(1,\chi) = 0$, τότε η $F(s)$ θα ήταν αναλυτική στο $\sigma > 0$, άρα και στο $\sigma = \sigma_c$. Αυτό έρχεται σε αντίφαση με την προηγούμενη παρατήρηση ότι η $F(s)$ έχει ανωμαλία στο σ_c, άρα πρέπει να έχουμε $L(1,\chi) \neq 0$.

Παρατήρηση 7.5.1. Αν ο p είναι πρώτος τέτοιος ώστε ο $p+2$ να είναι επίσης πρώτος, τότε ονομάζουμε τον p δίδυμο πρώτο. Η εικασία των δίδυμων πρώτων ισχυρίζεται ότι υπάρχουν άπειροι δίδυμοι πρώτοι. Αυτός ο ισχυρισμός παραμένει ανοικτό πρόβλημα.

Παρακινούμενοι από τις εκτιμήσεις του Mertens και την απόδειξη του θεωρήματος του Dirichlet για τους πρώτους σε αριθμητικές προόδους, είναι φυσιολογικό να θεωρήσουμε το άθροισμα

$$\sum_{p\leqslant x, p\in T} \frac{1}{p}$$

όπου T είναι το σύνολο των δίδυμων πρώτων. Αν μπορούσαμε να αποδείξουμε ότι αυτό το άθροισμα αποκλίνει, τότε θα ξέραμε ότι υπάρχουν άπειροι δίδυμοι πρώτοι. Δυστυχώς, αποδεικνύεται ότι αυτό το άθροισμα συγκλίνει (με τη μέθοδο του κόσκινου). Συνεπώς, αυτή η προσέγγιση δεν μπορεί να προσφέρει μια απόδειξη της εικασίας των δίδυμων πρώτων.

7.6 Ασκήσεις

7.1. Αποδείξτε ότι κάθε αριθμητική συνάρτηση f που είναι περιοδική $\pmod k$ και ικανοποιεί την $f(n) = 0$ αν $(n, k) > 1$ εκφράζεται ως γραμμικός συνδυασμός χαρακτήρων $\pmod k$.

7.2. Έστω $k > 1$ ένας ακέραιος. Έστω χ ένας όχι-κύριος χαρακτήρας $\pmod k$. Αποδείξτε ότι για οποιουσδήποτε ακεραίους $a < b$ έχουμε

$$\left|\sum_{n=a}^{b} \chi(n)\right| \leqslant \frac{\varphi(k)}{2}.$$

7.3. Κατασκευάστε ένα άπειρο σύνολο S πρώτων με την ακόλουθη ιδιότητα: Αν $p \in S$ και $q \in S$ τότε

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

7.4. Έστω $c_q(n)$ η συνάρτηση που ορίστηκε στην Άσκηση 2.3. Ορίζουμε

$$\langle f, g\rangle = \lim_{x\to\infty} \sum_{n\leqslant x} f(n)\overline{g(n)}.$$

Χρησιμοποιώντας την Άσκηση 2.3, αποδείξτε ότι

$$\langle c_q, c_{q'}\rangle = \begin{cases} \varphi(q) & , \text{ αν } q = q' \\ 0 & , \text{ αλλιώς} \end{cases}.$$

7.5. (α) Έστω $f(x)$ ένα πολυώνυμο βαθμού $n \geqslant 1$ με ακέραιους συντελεστές και ας υποθέσουμε ότι για κάθε πρώτο p, υπάρχουν ακέραιος m και πρώτος q τέτοιοι ώστε $f(p) = q^m$. Αποδείξτε ότι για κάθε ακέραιο t,

$$q^{m+1} \mid (f(p + tq^{m+1}) - f(p)).$$

(β) Συμπεράνατε από το (α) ότι αν $p \neq q$ και ο $p + tq^{m+1}$ είναι πρώτος, τότε

$$f(p + tq^{m+1}) = q^m.$$

(γ) Καταλήξτε σε άτοπο από το (β) χρησιμοποιώντας το θεώρημα του Dirichlet για τους πρώτους σε αριθμητικές προόδους και συμπεράνατε ότι $p = q$, ή ισοδύναμα ότι για κάθε πρώτο p υπάρχει ακέραιος m_p τέτοιος ώστε

$$f(p) = p^{m_p}.$$

7.6. (α) Έστω m και k θετικοί ακέραιοι και f ένας χαρακτήρας Dirichlet $(\text{mod } k)$. Λέμε ότι ο m είναι περίοδος της f αν $f(n+m) = f(n)$ για κάθε θετικό ακέραιο n. Αν ο k είναι ελεύθερος τετραγώνων, αποδείξτε ότι ο k είναι η μικρότερη θετική περίοδος της f.

(β) Δώστε παράδειγμα ενός χαρακτήρα Dirichlet $(\text{mod } k)$ για τον οποίο ο k δεν είναι η μικρότερη θετική περίοδος της f.

ΠΑΡΑΡΤΗΜΑ A

Αποτελέσματα από τη Μιγαδική Ανάλυση

A.1 Ακολουθίες αναλυτικών συναρτήσεων

Το βασικό θεώρημα αυτής της ενότητας μας επιτρέπει να αποδεικνύουμε ότι, κάτω από κάποιες προϋποθέσεις, συναρτήσεις που ορίζονται ως αθροίσματα σειρών αναλυτικών συναρτήσεων είναι αναλυτικές συναρτήσεις.

Θεώρημα A.1.1. *Έστω $\Omega \subseteq \mathbb{C}$ ανοικτό και $\{f_n\}_{n=1}^{\infty}$ ακολουθία αναλυτικών συναρτήσεων στο Ω. Υποθέτουμε ότι υπάρχει $f : \Omega \to \mathbb{C}$ τέτοια ώστε $f_n \to f$ ομοιόμορφα σε κάθε συμπαγές υποσύνολο K του Ω. Τότε, η f είναι αναλυτική στο Ω και για κάθε $k \in \mathbb{N}$ ισχύει ότι $f_n^{(k)} \to f^{(k)}$ ομοιόμορφα σε κάθε συμπαγές υποσύνολο K του Ω, όπου $g^{k)}$ είναι η παράγωγος τάξης k μιας αναλυτικής συνάρτησης g.*

Απόδειξη. Έστω $s \in \Omega$. Αφού το Ω είναι ανοικτό, υπάρχει $\delta > 0$ τέτοιο ώστε $\overline{\Delta(s,\delta)} \subseteq \Omega$. Οι f_n είναι συνεχείς στο Ω, άρα και στον κλειστό δίσκο $\overline{\Delta(s,\delta)}$. Αφού $f_n \to f$ ομοιόμορφα στον $\overline{\Delta(s,\delta)}$, έπεται ότι η f είναι συνεχής στον $\overline{\Delta(s,\delta)}$. Ειδικότερα, η f είναι συνεχής στο s. Συμπεραίνουμε έτσι ότι η f είναι συνεχής στο Ω.

Έστω τώρα γ τριγωνική καμπύλη τέτοια ώστε η εικόνα της γ^* καθώς και το εσωτερικό της τρίγωνο $T(\gamma^*)$ να περιέχονται στο Ω. Αφού κάθε f_n είναι αναλυτική στο Ω, για κάθε $n \in \mathbb{N}$ έχουμε $\int_\gamma f_n(s)ds = 0$. Αφού $f_n \to f$ ομοιόμορφα στο συμπαγές σύνολο γ^*, έχουμε

$$\left|\int_\gamma f_n(s)ds - \int_\gamma f(s)ds\right| \leqslant \max_{s\in\gamma^*} |f_n(s) - f(s)| \cdot \ell(\gamma) \longrightarrow 0$$

(όπου $\ell(\gamma)$ είναι το μήκος της γ). Συνεπώς,

$$\int_\gamma f(s)ds = 0.$$

Αφού η f είναι και συνεχής στο Ω, από το θεώρημα Morera βλέπουμε ότι η f είναι αναλυτική στο Ω.

Έστω τώρα $k \geqslant 1$, $\Delta(s_0,\delta_0)$ ανοικτός δίσκος ώστε $\overline{\Delta(s_0,\delta_0)} \subseteq \Omega$ και έστω $C(s_0,\delta_0)$ η περιφέρεια του δίσκου. Από τον τύπο του Cauchy έχουμε

$$f_n^{(k)}(s) = \frac{k!}{2\pi i}\int_{C(s_0,\delta_0)} \frac{f_n(z)}{(z-s)^{k+1}}dz$$

για κάθε $s \in \Delta(s_0,\delta_0)$, και

$$f^{(k)}(s) = \frac{k!}{2\pi i}\int_{C(s_0,\delta_0)} \frac{f(z)}{(z-s)^{k+1}}dz$$

για κάθε $s \in \Delta(s_0,\delta_0)$. Παρατηρούμε ότι αν $s \in \Delta(s_0,\delta_0/2)$ τότε

$$|f_n^{(k)}(s) - f^{(k)}(s)| \leqslant \frac{k!}{(\delta_0/2)^{k+1}} \max_{z\in C(s_0,\delta_0)} |f_n(z) - f(z)| \cdot \ell(C(s_0,\delta_0)) \longrightarrow 0$$

καθώς το $n \to \infty$. Έτσι έχουμε αποδείξει ότι για κάθε $s \in \Omega$ υπάρχει $\delta = \delta(s) > 0$ τέτοιος ώστε $f_n^{(k)} \to f^{(k)}$ ομοιόμορφα στον $\Delta(s,\delta)$.

Έστω τώρα K συμπαγές υποσύνολο του Ω. Θεωρώντας την ανοικτή κάλυψη του K από δίσκους $\Delta(s,\delta(s))$, $s \in \Omega$ όπως παραπάνω και περνώντας σε πεπερασμένη υποκάλυψη, βρίσκουμε $s_1,\dots,s_N \in \Omega$ και $\delta_1,\dots,\delta_N > 0$ ώστε $K \subseteq \Delta(s_1,\delta_1)\cup\cdots\cup\Delta(s_N,\delta_N)$ και $f_n^{(k)} \to f^{(k)}$ ομοιόμορφα σε κάθε $\Delta(s_i,\delta_i)$. Αφού το πλήθος αυτών των δίσκων είναι πεπερασμένο, είναι απλό να συμπεράνουμε ότι $f_n^{(k)} \to f^{(k)}$ ομοιόμορφα στο K. Αφού ο $k \in \mathbb{N}$ ήταν τυχών, η απόδειξη είναι πλήρης. $\square$

Προκύπτει τώρα άμεσα το ανάλογο του Θεωρήματος A.1.1 για σειρές αναλυτικών συναρτήσεων.

Θεώρημα A.1.2. *Έστω $\Omega \subseteq \mathbb{C}$ ανοικτό και $\{f_n\}_{n=1}^{\infty}$ ακολουθία αναλυτικών συναρτήσεων στο Ω. Υποθέτουμε ότι υπάρχει $f:\Omega\to\mathbb{C}$ τέτοια ώστε η σειρά $\sum_{n=1}^{\infty} f_n$ να συγκλίνει στην f ομοιόμορφα σε κάθε συμπαγές υποσύνολο K του Ω. Τότε, η f είναι αναλυτική στο Ω και για κάθε $k \in \mathbb{N}$ ισχύει ότι η σειρά $\sum_{n=1}^{\infty} f_n^{(k)}$ συγκλίνει στην $f^{(k)}$ ομοιόμορφα σε κάθε συμπαγές υποσύνολο K του Ω.*

Απόδειξη. Για κάθε $n \in \mathbb{N}$ ορίζουμε $s_n = f_1+\cdots+f_n$. Κάθε s_n είναι αναλυτική στο Ω και $s_n \to f$ ομοιόμορφα σε κάθε συμπαγές $K \subseteq \Omega$. Από το Θεώρημα A.1.1 η f είναι αναλυτική στο Ω και για κάθε $k \in \mathbb{N}$ έχουμε $s_n^{(k)} \to f^{(k)}$ ομοιόμορφα σε κάθε συμπαγές $K \subseteq \Omega$. Αφού $s_n^{(k)} = f_1^{(k)}+\cdots+f_n^{(k)}$ έπεται ότι η σειρά $\sum_{n=1}^{\infty} f_n^{(k)}$ συγκλίνει ομοιόμορφα στην $f^{(k)}$ σε κάθε συμπαγές $K \subseteq \Omega$. $\square$

Πολύ συχνά εφαρμόζουμε το Θεώρημα A.1.2 σε συνδυασμό με το ακόλουθο κλασικό M-κριτήριο του Weierstrass.

Θεώρημα A.1.3. *Έστω $f_n : A \to \mathbb{C}$ μιγαδικές συναρτήσεις και $M_n \geqslant 0$ ώστε, για κάθε $n \in \mathbb{N}$ ισχύει ότι $|f_n(s)| \leqslant M_n$ για κάθε $s \in A$. Αν $\sum_{n=1}^{\infty} M_n < +\infty$ τότε υπάρχει $f : A \to \mathbb{C}$ τέτοια ώστε η σειρά $\sum_{n=1}^{\infty} f_n$ να συγκλίνει στην f ομοιόμορφα στο A.*

Α.2 Απειρογινόμενα

Έστω $\{z_n\}_{n=1}^{\infty}$ ακολουθία μιγαδικών αριθμών. Ονομάζουμε απειρογινόμενο των z_n το σύμβολο

$$\prod_{n=1}^{\infty} z_n \quad \text{ή} \quad z_1 z_2 \cdots z_n \cdots .$$

Λέμε ότι το απειρογινόμενο $\prod_{n=1}^{\infty} z_n$ συγκλίνει αν υπάρχει $N \in \mathbb{N}$ τέτοιος ώστε $z_n \neq 0$ για κάθε $n \geqslant N$ και η ακολουθία $b_M := \prod_{n=N}^{M} z_n = z_N \cdots z_M$, $M \geqslant N$ συγκλίνει σε κάποιον $w \neq 0$ ή ∞. Τότε λέμε ότι το $\prod_{n=1}^{\infty} z_n$ συγκλίνει στον $z = z_1 \cdots z_{N-1} w$ και γράφουμε

$$z = \prod_{n=1}^{\infty} z_n.$$

Παρατήρηση Α.2.1. Αν υπάρχει $N \in \mathbb{N}$ τέτοιος ώστε $z_n \neq 0$ για κάθε $n \geqslant N$ και η ακολουθία $b_M := \prod_{n=N}^{M} z_n = z_N \cdots z_M$, $M \geqslant N$ συγκλίνει στο 0 ή το ∞ τότε λέμε ότι το απειρογινόμενο αποκλίνει στο 0 ή το ∞ αντίστοιχα.

Παρατηρήστε επίσης ότι αν το απειρογινόμενο συγκλίνει σε αριθμό διαφορετικό από το 0 τότε $z_n \neq 0$ για κάθε $n \in \mathbb{N}$. Αντίστροφα, αν το απειρογινόμενο συγκλίνει και $z_n \neq 0$ για κάθε $n \in \mathbb{N}$ τότε το όριοείναι διάφορο του μηδενός.

Θεώρημα Α.2.2. *Έστω $\{z_n\}_{n=1}^{\infty}$ ακολουθία μιγαδικών αριθμών. Για κάθε $n \in \mathbb{N}$ γράφουμε $z_n = 1 + a_n$.*

α) *Αν το $\prod_{n=1}^{\infty} z_n = \prod_{n=1}^{\infty}(1 + a_n)$ συγκλίνει, τότε $a_n \to 0$. Δηλαδή, $z_n \to 1$.*

(β) *Αν η σειρά $\sum_{n=1}^{\infty} a_n$ συγκλίνει απολύτως, τότε το απειρογινόμενο $\prod_{n=1}^{\infty}(1 + a_n)$ συγκλίνει.*

Απόδειξη. (α) Υποθέτουμε ότι $z_n = 1 + a_n \neq 0$ για κάθε $n \geqslant N$ και η ακολουθία $b_M := \prod_{n=N}^{M} z_n = z_N \cdots z_M$, $M \geqslant N$ συγκλίνει σε κάποιον $w \neq 0$ ή ∞. Τότε, για κάθε $n > N$ έχουμε

$$z_n = \frac{b_n}{b_{n-1}} \to \frac{w}{w} = 1,$$

δηλαδή $a_n \to 0$.

(β) Αφού η σειρά $\sum_{n=1}^{\infty} |a_n|$ συγκλίνει, έχουμε $a_n \to 0$ επομένως υπάρχει $N \in \mathbb{N}$ ώστε $|a_n| < 1$ για κάθε $n \geqslant N$, και αυτό σημαίνει ότι $1 + a_n \neq 0$ για κάθε $n \geqslant N$.

Διακρίνουμε δύο περιπτώσεις:

(i) Έστω ότι $\sum_{n=1}^{\infty} |a_n| = \vartheta < 1$. Τότε $|a_n| < 1$ και συνεπώς $1 + a_n \neq 0$ για κάθε $n \in \mathbb{N}$. Θεωρούμε την ακολουθία $b_n = (1 + a_1) \cdots (1 + a_n)$. Τότε,

$$|b_n| \leqslant (1 + |a_1|) \cdots (1 + |a_n|) \leqslant e^{|a_1| + \cdots + |a_n|} \leqslant e,$$

άρα

$$|b_{n+1} - b_n| = |b_n| \cdot |a_{n+1}| \leqslant e|a_{n+1}|$$

και τότε για κάθε $n > m$ έχουμε

$$|b_n - b_m| \leqslant e(|a_{m+1}| + \cdots + |a_n|).$$

Από τη σύγκλιση της σειράς $\sum_{n=1}^{\infty}|a_n|$ υμπεραίνουμε ότι η (b_n) είναι βασική, άρα υπάρχει $b \in \mathbb{C}$ ώστε $b_n \to b$. Όμως,

$$|b_n| \geqslant (1-|a_1|)\cdots(1-|a_n|) \geqslant 1-(|a_1|+\cdots+|a_n|) \geqslant 1-\vartheta > 0$$

για κάθε $n \in \mathbb{N}$, άρα $|b| = \lim|b_n| \geqslant \vartheta > 0$, και ειδικότερα $b \neq 0$. Με βάση τον ορισμό, το απειρογινόμενο $\prod_{n=1}^{\infty}(1+a_n)$ συγκλίνει στον b.

(ii) Έστω ότι $1 \leqslant \sum_{n=1}^{\infty}|a_n| < \infty$. Τότε, υπάρχει $N \in \mathbb{N}$ τέτοιος ώστε $\sum_{n=N}^{\infty}|a_n| < 1$. Από την προηγούμενη περίπτωση έχουμε $1+a_n \neq 0$ για κάθε $n \geqslant N$ και το απειρογινόμενο $\prod_{n=N}^{\infty}(1+a_n)$ συγκλίνει σε κάποιον $b \neq 0$. Με βάση τον ορισμό συμπεραίνουμε ότι το απειρογινόμενο $\prod_{n=1}^{\infty}(1+a_n)$ συγκλίνει στον $b(1+a_1)\cdots(1+a_{N-1})$. □

A.3 Αναλυτική συνέχιση

Η αρχή της αναλυτικής συνέχισης εξασφαλίζει ότι αν f είναι μια αναλυτική συνάρτηση σε ένα ανοικτό και συνεκτικό $\Omega \subseteq \mathbb{C}$ και το σύνολο των ριζών της f έχει σημείο συσσώρευσης στο Ω, τότε $f \equiv 0$ στο Ω.

Θεώρημα A.3.1. *Έστω Ω ανοικτό και συνεκτικό υποσύνολο του $\mathbb{C}$ και $f : \Omega \to \mathbb{C}$ αναλυτική συνάρτηση. Υποθέτουμε ότι υπάρχουν $s \in \Omega$ και ακολουθία $\{s_n\}_{n=1}^{\infty}$ στο Ω με $s_n \neq s$ για κάθε $n \in \mathbb{N}$, $f(s_n) = 0$ για κάθε $n \in \mathbb{N}$ και $s_n \to s$. Τότε, η f είναι ταυτοτικά μηδέν στο Ω.*

Απόδειξη. Έστω $s \in \Omega$ με την εξής ιδιότητα: «υπάρχει ακολουθία (s_n) στο Ω με $s_n \neq s$, $s_n \to s$ και $f(s_n) = 0$.» Παίρνουμε $\delta > 0$ ώστε $\Delta(s,\delta) \subseteq \Omega$ και θεωρούμε τη σειρά Taylor της f

$$f(z) = a_0 + a_1(z-s) + a_2(z-s)^2 + \cdots$$

με κέντρο s στον δίσκο $\Delta(s,\delta)$. Ας υποθέσουμε ότι υπάρχει ελάχιστος $N \in \mathbb{N}$ με $a_N \neq 0$. Τότε,

$$f(z) = (z-s)^N(a_N + a_{N+1}(z-s) + \cdots) = (z-s)^N g(z)$$

και η $f(z) = a_N + a_{N+1}(z-s) + \cdots$ είναι αναλυτική στον $\Delta(s,\delta)$. Αφού $s_n \to s$, για μεγάλα n έχουμε $s_n \in \Delta(s,\delta)$, άρα

$$0 = f(s_n) = (s_n - s)^N g(s_n)$$

απ' όπου έπεται ότι $g(s_n) = 0$ αφού $s_n \neq 0$. Τότε,

$$0 = g(s_n) \to g(s) = a_N,$$

το οποίο είναι άτοπο. Άρα, $a_n = 0$ για κάθε $n \in \mathbb{N}$, δηλαδή $f \equiv 0$ στον $\Delta(s,\delta)$.

Ορίζουμε $A = \{s \in \Omega : f \equiv 0$ σε κάποιον δίσκο $\Delta(s,\delta) \subseteq \Omega\}$ και $B = \Omega \setminus A$. Ελέγχουμε εύκολα ότι το A είναι ανοικτό σύνολο. Έστω ότι το B δεν είναι ανοικτό. Τότε υπάρχει $s \in B$ με την εξής ιδιότητα: κανένας δίσκος $\Delta(s,\delta)$ δεν περιέχεται στο B. Αφού για $\delta > 0$ αρκετά μικρό έχουμε $\Delta(s,\delta) \subseteq \Omega$, βλέπουμε ότι όλοι οι δίσκοι $\Delta(s,\delta)$ με μικρή ακτίνα τέμνουν το A, καί συνεπώς *για κάθε* $\delta > 0$ ισχύει $\Delta(s,\delta) \cap A \neq \varnothing$. Μπορούμε λοιπόν να βρούμε ακολουθία (s_n) στο A τέτοια ώστε $s_n \to s$. Αφού $s \in B$ έχουμε $s_n \neq s$ για κάθε $n \in \mathbb{N}$, και αφού $s_n \in A$ έχουμε $f(s_n) = 0$

για κάθε $n \in \mathbb{N}$. Όμως με αυτές τις υποθέσεις δείξαμε ότι υπάρχει $\delta > 0$ ώστε $f \equiv 0$ στον $\Delta(s, \delta)$. Συνεπώς, $s \in A$ και έχουμε καταλήξει σε άτοπο.

Από την υπόθεση του θεωρήματος έχουμε $A \neq \varnothing$. Αφού τα A, B είναι ανοικτά και το $\Omega = A \cup B$ είναι συνεκτικό, έπεται ότι $\Omega = A$. Ειδικότερα, $f \equiv 0$ στο Ω. □

Το Θεώρημα Α.3.1 χρησιμοποιείται συχνά στην ακόλουθη μορφή, η οποία είναι άμεσο πόρισμα.

Θεώρημα Α.3.2. *Έστω Ω ανοικτό και συνεκτικό υποσύνολο του $\mathbb{C}$ και $f : \Omega \to \mathbb{C}$ αναλυτική συνάρτηση. Αν η f μηδενίζεται σε κάθε σημείο ενός ευθύγραμμου τμήματος ή ενός ανοικτού δίσκου στο Ω τότε $f \equiv 0$ στο Ω.*

Α.4 Αναλυτικές συναρτήσεις που ορίζονται από ολοκληρώματα

Θεώρημα Α.4.1. *Έστω Ω ανοικτό υποσύνολο του $\mathbb{C}$ και $f : [a, b] \times \Omega \to \mathbb{C}$ συνεχής συνάρτηση. Τότε η $F : \Omega \to \mathbb{C}$ με*

$$F(s) := \int_a^b f(t, s)\, dt$$

ορίζεται καλά και είναι συνεχής.

Απόδειξη. Αρχικά παρατηρούμε ότι το ολοκλήρωμα που δίνει την τιμή $F(s)$ είναι καλά ορισμένο, αφού η $t \mapsto f(t, s)$ είναι συνεχής στο $[a, b]$ για κάθε $s \in \Omega$.

Έστω $s_0 \in \Omega$ και $\delta_0 > 0$ ώστε $\overline{\Delta(s_0,]delta_0)} \subseteq \Omega$. Η f είναι ομοιόμορφα συνεχής στο $[a, b] \times \overline{\Delta(s_0, \delta_0)}$, άρα για τυχόν $\varepsilon > 0$ υπάρχει $\delta > 0$ ώστε αν τα $t_1, t_2 \in [a, b]$ και $s_1, s_2 \in \overline{\Delta(s_0, \delta_0)}$ ικανοποιούν τις $|t_1 - t_2| < \delta$ και $|s_1 - s_2| < \delta$ τότε $|f(t_1, s_1) - f(t_2, s_2)| < \varepsilon$.

Τότε, για κάθε $s_1 \in \overline{\Delta(s_0, \delta_0)}$ με $|s_0 - s_1| < \delta$ έχουμε

$$\begin{aligned} |F(s_0) - F(s_1)| &= \left| \int_a^b (f(t, s_0) - f(t, s_1)) dt \right| \leqslant \int_a^b |f(t, s_0) - f(t, s_1)| dt \\ &\leqslant (b - a)\varepsilon. \end{aligned}$$

Έπεται ότι η F είναισυνεχής στο s_0, και αφού το $s_0 \in \Omega$ ήταν τυχόν συμπεραίνουμε ότι η F είναι συνεχής στο Ω. □

Θεώρημα Α.4.2. *Έστω Ω ανοικτό υποσύνολο του $\mathbb{C}$ και $f : [a, b] \times \Omega \to \mathbb{C}$ συνάρτηση με τις ακόλουθες ιδιότητες:*

- *η f είναι συνεχής στο $[a, b] \times \Omega$,*
- *για κάθε $t \in [a, b]$ η $s \mapsto f(t, s)$ είναι αναλυτική στο Ω, και*
- *η μιγαδική παράγωγος f_s είναι συνεχής στο $[a, b] \times \Omega$.*

Τότε, η $F : \Omega \to \mathbb{C}$ με $F(s) := \int_a^b f(t, s)\, dt$ είναι αναλυτική στο Ω και

$$F'(s) = \int_a^b f_s(t, s)\, dt$$

για κάθε $s \in \Omega$.

Απόδειξη. Θεωρούμε τυχόν $s_0 \in \Omega$. Θα δείξουμε ότι η F ίναι αναλυτική στο s_0 και ότι

$$F'(s_0) = \int_a^b f_s(t, s_0)dt.$$

Θεωρούμε τη συνάρτηση $g : [a, b] \times \Omega \to \mathbb{C}$ με $g(t, s_0) = f_s(t, s_0)$ και

$$g(t, s) = \frac{f(t, s) - f(t, s_0)}{s - s_0} \quad \text{αν } s \neq a_0.$$

Για κάθε (t_1, s_1) με $s_1 \neq s_0$ από τη συνέχεια της f βλέπουμε ότι

$$\lim_{(t,s)\to(t_1,s_1)} g(t, s) = \lim_{(t,s)\to(t_1,s_1)} \frac{f(t, s) - f(t, s_0)}{s - s_0} = \frac{f(t_1, s_1) - f(t_1, s_0)}{s_1 - s_0} = g(t_1, s_1).$$

Έστω τώρα τυχόν $(t_0, s_0) \in [a, b] \times \Omega$. Θα δείξουμε ότι, πάλι,

$$\lim_{(t,s)\to(t_0,s_0)} g(t, s) = g(t_0, s_0).$$

Γράφουμε $f = u + iv$ και $s = \sigma + i\tau$. Από τις εξισώσεις Cauchy-Riemann έχουμε

$$f_s(t, s) = u_\sigma(t, s) + iv_\sigma(t, s) = v_\tau(t, s) - iu_\tau(t, s).$$

Συνεπώς,

$$\begin{aligned}
|g(t, s) - g(t_0, s_0)| &\leqslant |g(t, s) - g(t, s_0)| + |g(t, s_0) - g(t_0, s_0)| \\
&= \frac{1}{|s - s_0|}|f(t, s) - f(t, s_0) - f_s(t, s_0)(s - s_0)| + |f_s(t, s_0) - f_s(t_0, s_0)| \\
&= \frac{1}{|s - s_0|}\Big|[u(t, s) - u(t, s_0)] + i[v(t, s) - v(t, s_0)] \\
&\quad - f_s(t, s_0)[(\sigma - \sigma_0) + i(\tau - \tau_0)]\Big| \\
&\quad + |f_s(t, s_0) - f_s(t_0, s_0)|.
\end{aligned}$$

Από το θεώρημα μέσης τιμής έχουμε ότι για κάποια $s_1, s_2 \in [s_0, s]$ ισχύουν οι

$$u(t, s) - u(t, s_0) = u_\sigma(t, s_1)(\sigma - \sigma_0) + u_\tau(t, s_1)(\tau - \tau_0)$$

και

$$v(t, s) - v(t, s_0) = v_\sigma(t, s_2)(\sigma - \sigma_0) + v_\tau(t, s_2)(\tau - \tau_0).$$

Συνδυάζοντας τις προηγούμενες σχέσεις με τις εξισώσεις Cauchy-Riemann βλέπουμε ότι

$$\begin{aligned}
|g(t, s) - g(t_0, s_0)| \leqslant \frac{1}{|s - s_0|}\Big|&[(u_\sigma(t, s_1) - u_\sigma(t, s_0))(\sigma - \sigma_0) + (u_\tau(t, s_1) - u_\tau(t, s_0))(\tau - \tau_0)] \\
&+ i[(v_\sigma(t, s_2) - v_\sigma(t, s_0))(\sigma - \sigma_0) + (v_\tau(t, s_2) - v_\tau(t, s_0))(\tau - \tau_0)]\Big| \\
&+ |f_s(t, s_0) - f_s(t_0, s_0)| \\
&\leqslant |u_\sigma(t, s_1) - u_\sigma(t, s_0)| + |u_\tau(t, s_1) - u_\tau(t, s_0)| \\
&+ |v_\sigma(t, s_2) - v_\sigma(t, s_0)| + |v_\tau(t, s_2) - v_\tau(t, s_0)| + |f_s(t, s_0) - f_s(t_0, s_0)|.
\end{aligned}$$

Αφού η f_s είναι συνεχής, οι $u_\sigma, u_\tau, v_\sigma, v_\tau$ είναι συνεχείς, και αφού $s_1 \to s_0$ και $s_2 \to s_0$ όταν $s \to s_0$, βλέπουμε ότι

$$\lim_{(t,s)\to(t_0,s_0)} g(t,s) = g(t_0,s_0).$$

Αυτό αποδεικνύει ότι η g είναι συνεχής σε κάθε $(t,s) \in [a,b] \times \Omega$ τόσο στην περίπτωση $s = s_0$ όσο και στην περίπτωση $s \neq s_0$. Αφού η g είναι συνεχής στο $[a,b] \times \Omega$, από το Θεώρημα Α.4.1 έχουμε ότι η συνάρτηση $g : \Omega \to \mathbb{C}$ με

$$G(s) = \int_a^b g(t,s)dt$$

είναι συνεχής. Έπεται ότι

$$\begin{aligned}\lim_{s\to s_0} \frac{F(s)-F(s_0)}{s-s_0} &= \lim_{s\to s_0} \int_a^b g(t,s)dt = \lim_{s\to s_0} G(s)\\ &= G(s_0) = \int_a^b g(t,s_0)dt = \int_a^n f_s(t,s_0)dt,\end{aligned}$$

και αυτό ολοκληρώνει την απόδειξη. □

Βιβλιογραφία

[1] Alfhors, L., Complex Analysis, 3rd edn., McGraw–Hill, New York, 1996.

[2] Apostol, T., Introduction to Analytic Number Theory, 3rd edn., Springer–Verlag, New York, 1986.

[3] Erdős, P., Ramanujan and I, in Number Theory, Madras 1987, Proceedings of the International Ramanujan Centenary Conference held at Anna University, Madras, India, Dec.21, 1987, edited by K. Alladi, Lecture Notes in Mathematics (1395), Springer–Verlag, Berlin, 1989.

[4] Hildebrand, A., The Prime Number Theorem via the Large Sieve, Mathematika 33 (1986) 23–30.

[5] Hildebrand, A., Notes on Analytic Number Theory, University of Illinois at Urbana–Champaign, 1991.

[6] Huxley, H., Exponential sums of lattice points iii, Proc. London Math. Soc. 87 (2003) 591–609.

[7] Iwaniec, H. and Mozzochi, C., On the divisor and circle problems, J. Number Theory 29, 1 (1988) 60–93.

[8] Lang, S., Algebra, 3rd edn., Addison Wesley, 1993.

[9] Ramanujan, S., A proof of Bertrand's postulate, J. Indian Math. Soc. 11 (1919) 181–182.

[10] Rotman, J., A First Course in Abstract Algebra with Applications, 3rd edn., Pearson Prentice Hall, 2006.

[11] Tenenbaum, G., Introduction to Analytic and Probabilistic Number Theory, Cambridge University Press, 1995.

[12] van der Corput, J., Zum teilerproblem, Math. Ann. 98, 1 (1928) 697–716.

[13] Voronoi, G., Sur une problème du calcul des fonctions asymptotique, J. Reine Angew. Math. 126 (1903) 241–282.

[14] Whittaker, E. and Watson, G., A Course of Modern Analysis, 4th edn., Cambridge University Press, 1992.