Επώνυμοι Ακέραιοι, Αποδείξεις υπάρξεως άπειρων πρώτων και το Θεώρημα του Dirichlet

Χριστίνα Ιατράκη

Επιβλέπων καθηγητής
Ιωάννης Αντωνιάδης

Μεταπτυχιακή Εργασία

Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών
Πανεπιστήμιο Κρήτης
Ηράκλειο
Οκτώβριος 2015

Η παρούσα μεταπτυχιακή εργασία κατατέθηκε στο τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών του Πανεπιστημίου Κρήτης τον Οκτώβριο του 2015 στα πλαίσια του μεταπτυχιακού προγράμματος «Μαθηματικά και Εφαρμογές τους» στην κατεύθυνση «Μαθηματικά για την Εκπαίδευση». Την επιτροπή αξιολόγησης αποτέλεσαν οι:

Ιωάννης Αντωνιάδης, (επιβλέπων),
Νικόλαος Τζανάκης,
Χρήστος Κουρουνιώτης,

τους οποίους ευχαριστώ για την συμμετοχή τους στην επιτροπή αυτή.
Ιδιαίτερα ευχαριστώ τον κ. Αντωνιάδη για την καθοδήγησή του, τις συμβουλές, την υπομονή και το χρόνο που μου προσέφερε και να τονίσω πως χωρίς την συμβολή του δεν θα ήταν δυνατή η άρτια ολοκλήρωση αυτής της εργασίας.
Τέλος, θα ήθελα να ευχαριστήσω τον κ. Μιχάλη Παπαδημητράκη για όλη του την βοήθεια κατά την διάρκεια των μεταπτυχιακών αλλά και προπτυχιακών σπουδών μου .

Στους γονείς μου, Βασίλη και Μαρία

Περιεχόμενα

Εισαγωγή

Στην παρούσα μεταπτυχιακή εργασία μελετώνται οι επώνυμοι ακέραιοι αριθμοί, αποδείξεις υπάρξεως άπειρου πλήθους πρώτων αριθμών και το Θεώρημα του Dirichlet .

Στο πρώτο κεφάλαιο μελετώνται καταρχήν οι φίλοι αριθμοί. Πρόκειται για ζευγάρια ακεραίων των οποίων το άθροισμα των διαιρετών του ενός συμπίπτει με το άθροισμα των διαιρετών του άλλου. Στη συνέχεια θεωρούμε τους τέλειους αριθμούς. Αναφέρουμε τις εικασίες του Νικόμαχου του Γερασηνού και εξετάζουμε ποιες από αυτές έχουν αποδειχθεί μέχρι σήμερα. Αποδεικνύουμε την πρόταση του Euler : *Αν ο άρτιος φυσικός m είναι τέλειος τότε έχει κατ' ανάγκη τη μορφή $m = 2^{n-1}(2^n - 1)$, όπου ο $2^n - 1$ είναι πρώτος για κάποιο $n \geq 2$.* Έπειτα, αποδεικνύουμε μια σειρά αποτελεσμάτων για τους περιττούς τέλειους, παρόλο που δεν γνωρίζουμε ως σήμερα αν υπάρχει κάποιος τέτοιος αριθμός. Ορίζουμε τους πρώτους αριθμούς Mersenne που είναι της μορφής $2^p - 1$ και παραθέτουμε έναν πίνακα με τους 48 πρώτους Mersenne και άρα με τους 48 μέχρι σήμερα γνωστούς άρτιους τέλειους. Επίσης, ορίζουμε τους αριθμούς Fermat που είναι της μορφής $2^{2^n}+1$. Τέλος, ορίζουμε τους αριθμούς Fibonacci και εξετάζουμε κάποιες αριθμοθεωρητικές ιδιότητές τους.

Στο δεύτερο κεφάλαιο μελετούμε μερικές αντιπροσωπευτικές αποδείξεις για την ύπαρξη άπειρων πρώτων, τις οποίες εμείς και κατηγοριοποιούμε. Στην πρώτη κατηγορία ανήκουν αυτές που βασίζονται στην ιδέα του Ευκλείδη. Οι αποδείξεις αυτές ακολουθούν την μέθοδο της εις άτοπον απαγωγής. Τέτοιες είναι οι αποδείξεις του Hermite, του Kummer, του Stieltjes, του Braun και του Métrod . Στην δεύτερη κατηγορία μελετούμε αποδείξεις οι οποίες στηρίζονται στο γεγονός ότι κάθε μη πεπερασμένη ακολουθία ακέραιων αριθμών, της οποίας δύο οποιοιδήποτε διαδοχικοί όροι είναι πρώτοι μεταξύ τους οδηγεί στην απόδειξη του θεωρήματος του Ευκλείδη. Σε αυτήν την κατηγορία ανήκουν οι αποδείξεις του Goldbach, του Schorn, του Filip Saidak και κάποιες παραλλαγές αυτών. Στην τρίτη κατηγορία ανήκουν αποδείξεις που βασίζονται στην Αλγεβρική Θεωρία Αριθμών, όπως είναι αυτή του Larry Washington. Στην τέταρτη κατηγορία μελετούμε μερικές συνδυαστικές αποδείξεις που περιέχουν απλά επιχειρήματα αριθμητικής. Τέτοιες αποδείξεις είναι του Perott, του Thue και του Auric . Στην πέμπτη κατηγορία μελετούμε την τοπολογική απόδειξη του Furstenberg και μια παραλλαγή της. Στην έκτη και τελευταία κατηγορία ανήκουν οι αποδείξεις που βασίζονται στην απόδειξη του Euler , όπως είναι αυτή του Erdos .

Στο τρίτο και τελευταίο κεφάλαιο αρχικά εξετάζουμε ότι υπάρχουν άπειροι αριθμοί των μορφών $4n+1$, $4n+3$, $6n+1$ και $6n+5$. Βασιζόμενοι σε μεθόδους της Αλγεβρικής Θεωρίας Αριθμών και ιδιαίτερα σε ιδιότητες των κυκλοτομικών πολυωνύμων αποδεικνύουμε ότι για κάθε φυσικό $n \geq 2$ υπάρχει άπειρο πλήθος πρώτων p τέτοιοι ώστε $p \equiv 1 \pmod{n}$. Έπειτα, δίνουμε των ορισμό των χαρακτήρων πεπερασμένων αβελιανών ομάδων και μελετάμε κάποιες ιδιότητες τους. Στη συνέχεια ορίζουμε τις L-σειρές του Dirichlet και μελετάμε τις ιδιότητες τους. Τέλος, αποδεικνύουμε το θεώρημα του Dirichlet για αριθμητικές προόδους, δηλαδή ότι σε κάθε αριθμητική πρόοδο $\{a+kn | (a,n)=1, k \in \mathbb{Z}\}$ υπάρχουν άπειροι πρώτοι.

Κεφάλαιο 1

Επώνυμοι ακέραιοι

1.1 Φίλοι αριθμοί

Για κάθε θετικό ακέραιο n, ορίζουμε μια συνάρτηση $\sigma(n)$, το άθροισμα των θετικών διαιρετών του n.
Έτσι, $\sigma(1) = 1, \sigma(2) = 1 + 2 = 3, \sigma(3) = 1 + 3 = 4, \sigma(4) = 1 + 2 + 4 = 7$.
Για κάθε $n \geq 2$, ισχύει $\sigma(n) \geq n + 1$. Αν $n = \prod_{p|n} p^{\vartheta_p(n)}$ η (μονοσήμαντη) ανάλυση του n σε γινόμενο πρώτων παραγόντων, τότε κάθε θετικός διαιρέτης $d \mid n$ θα έχει την μορφή

$$d = \prod_{p|n} p^{a_p}, \qquad \text{όπου } 0 \leq a_p \leq \vartheta_p(n)$$

για κάθε $p \in \mathbb{P}, p \mid n$. Επομένως,

$$\sigma(n) = \sum_{d|n} d = \prod_{p|n} \sum_{a_p=0}^{\vartheta_p(n)} p^{a_p}$$

Το εσωτερικό άθροισμα, είναι άθροισμα όρων γεωμετρικής προόδου και συνεπώς

$$\sum_{a_p=0}^{\vartheta_p(n)} p^{a_p} = \frac{p^{\vartheta_p(n)+1} - 1}{p - 1}.$$

Άρα,

$$\sigma(n) = \prod_{p|n} \frac{p^{\vartheta_p(n)+1} - 1}{p - 1}.$$

Πρόταση 1.1.1. *Αν n, m θετικοί ακέραιοι και $(m, n) = 1$, τότε $\sigma(nm) = \sigma(n)\sigma(m)$.*

Απόδειξη. Είναι:

$$\sigma(nm) = \prod_{p|nm} \frac{p^{\vartheta_p(nm)+1} - 1}{p-1}$$

Επειδή $(n, m) = 1$ έπεται ότι,

$$\prod_{p|nm} \frac{p^{\vartheta_p(nm)+1} - 1}{p-1} = \prod_{p|n} \frac{p^{\vartheta_p(nm)+1} - 1}{p-1} \prod_{p|m} \frac{p^{\vartheta_p(nm)+1} - 1}{p-1}.$$

Όταν το p διαιρεί το n, τότε το p δεν διαιρεί το m, αφού $(n, m) = 1$. Δηλαδή, $\vartheta_p(m) = 0$. Επομένως, $\vartheta_p(nm) = \vartheta_p(n) + \vartheta_p(m) = \vartheta_p(n)$. Ανάλογα, όταν το p διαιρεί τον m, τότε το p δεν διαιρεί το n, οπότε $\vartheta_p(nm) = \vartheta_p(m)$. Συνεπώς,

$$\prod_{p|n} \frac{p^{\vartheta_p(nm)+1} - 1}{p-1} \prod_{p|m} \frac{p^{\vartheta_p(nm)+1} - 1}{p-1} = \prod_{p|n} \frac{p^{\vartheta_p(n)+1} - 1}{p-1} \prod_{p|m} \frac{p^{\vartheta_p(m)+1} - 1}{p-1} = \sigma(n)\sigma(m).$$

Άρα, $\sigma(nm) = \sigma(n)\sigma(m)$. □

Ορισμός 1.1.1. *Δυο θετικοί αριθμοί m, n θα λέγονται φίλοι όταν*

$$\sigma(m) - m = n$$

και

$$\sigma(n) - n = m$$

δηλαδή όταν $\sigma(m) = m + n = \sigma(n)$.

Το μικρότερο ζευγάρι γνωστών φίλων αριθμών αναφέρεται στο έργο του Ιάμβλιχου « Περί τῆς Νικομάχου Αριθμητικῆς Εἰσαγωγῆς» και είναι το $(220, 284)$. Αποδίδεται μάλιστα στον Πυθαγόρα και στους μαθητές του. Ονομάστηκαν έτσι επειδή έχουν τη «δύναμη» ο ένας να παράγει τον άλλο και αντιστρόφως, κάτι που συμβολίζει την «αμοιβαία αρμονία» , την «τέλεια φιλία». Όταν κάποτε ο Πυθαγόρας ρωτήθηκε « Τί εστί φίλος·», απάντησε «Έτερος εγώ».

Μερικά άλλα ζευγάρια φίλων είναι: $(1184, 1210), (2620, 2924), (5020, 5564), (6232, 6368), (10744, 10856), (12285, 14595), (17296, 18416)$.

Το 1636 ο Fermat βρήκε το $(17296, 18416)$ και το 1638 ο Descartes βρήκε το $(9363584, 9437056)$. Τα δύο τελευταία αποτελέσματα ήταν ήδη γνωστά στους Άραβες. Ο Euler ανακάλυψε το 1747 30 νέα ζευγάρια φίλων αριθμών και στη συνέχεια επεξέτεινε τα αποτελέσματά τους σε 64 ζευγάρια (δύο από τα οποία ήταν λάθος).Αξιοσημείωτο είναι ότι το ζευγάρι $(1184, 1210)$ διέλαθε την προσοχή όλων, ακόμη και του Euler και πρωτοανακαλύφθηκε από τον 16χρονο Nicolo Papagini στα 1866. Με χρήση ηλεκτρονικού υπολογιστή ο αριθμός των φίλων το 1946 έφτανε τα 390 ζευγάρια. Σήμερα (αποτελέσματα Σεπτ. του 2005) είναι γνωστοί 8.846.881 ζευγάρια.

Το ερώτημα αν υπάρχει κάποιος κανόνας υπολογισμού ζευγαριών φίλων αριθμών απαντήθηκε θετικά κατά τον 9ο μ.Χ. αιώνα από τον Άραβα μαθηματικό Thabit ibn Kuwah (ή, κατ΄ άλλους Qurra).

Πρόταση 1.1.2. *Αν $n > 1$ και οι αριθμοί $p = 3 \cdot 2^{n-1} - 1, q = 3 \cdot 2^n - 1$ και $r = 9 \cdot 2^{2n-1} - 1$ είναι πρώτοι τότε οι $2^n \cdot p \cdot q$ και $2^n \cdot r$ είναι φίλοι.*

Απόδειξη. Πράγματι,

$$\begin{aligned}\sigma(2^n \cdot p \cdot q) &= \sigma(2^n)\sigma(p)\sigma(q) = \frac{2^{n+1}-1}{2-1} \cdot \frac{p^2-1}{p-1} \cdot \frac{q^2-1}{q-1} = (2^{n+1}-1) \cdot (p+1) \cdot (q+1) \\ &= (2^{n+1}-1) \cdot 3 \cdot 2^n \cdot 3 \cdot 2^{n-1} = (2^{n+1}-1) \cdot 9 \cdot 2^{2n-1}.\end{aligned}$$

Επίσης,

$$\sigma(2^n \cdot r) = \sigma(2^n)\sigma(r) = (2^{n+1}-1) \cdot (r+1) = (2^{n+1}-1) \cdot 9 \cdot 2^{2n-1}.$$

Επομένως, οι $2^n \cdot p \cdot q$ και $2^n \cdot r$ είναι φίλοι. □

Παραδείγματα.

1. *Για $n = 2$ οι $p = 5, q = 11$ και $r = 71$ είναι πρώτοι κι έχουμε το ζευγάρι φίλων $2^2 \cdot 5 \cdot 11 = 220$ και $2^2 \cdot 71 = 284$.*

2. *Το ζευγάρι φίλων του Fermat προκύπτει από το θεώρημα για $n = 4$, οι $p = 23, q = 47$ και $r = 1151$ είναι πρώτοι, ενώ το ζευγάρι φίλων του Descartes για $n = 7$, οι $p = 191, q = 383$ και $r = 73727$ είναι επίσης πρώτοι.*

Δυστυχώς δεν προκύπτουν όλα τα ζευγάρια φίλων κατ΄ αυτόν τον τρόπο, π.χ. το ζευγάρι $(6232, 6368)$.

Παρατηρήσεις.

1. *Δεν υπάρχει γνωστό ζευγάρι φίλων στο οποίο ένας τουλάχιστον να είναι τέλειο τετράγωνο.*

2. *Υπάρχουν ζευγάρια φίλων οι οποίοι να έχουν ίσα αθροίσματα ψηφίων, π.χ.* $(69615, 87633)$. *Στα πρώτα 5000 427 είναι τέτοια.*
   Υπάρχουν ζευγάρια φίλων στα οποία κάθε φίλος διαιρείται με το άθροισμα των ψηφίων του, π.χ. $(2620, 2924)$.

3. *Σε όλα τα γνωστά ζευγάρια φίλων μέχρι τη δεκαετία του 60 οι περιττοί φίλοι αριθμοί διαιρούνται με 3. Έτσι, οι Bratley και Mc Kay (1968) διατύπωσαν την εικασία ότι αυτό ισχύει για όλα τα ζευγάρια περιττών φίλων. Η εικασία*

αυτή αποδείχθηκε λανθασμένη 20 χρόνια αργότερα από τους Battiato και Borho (1988). Το αντιπαράδειγμα με τους πιο μικρούς φίλους οι οποίοι δεν διαιρουνται με 3 είναι

$$(42262694537514864075544955198125, 42405817271188606697466971841875)$$

οι οποίοι είναι αριθμοί με 32 ψηφία.

1.2 Τέλειοι αριθμοί

Ορισμός 1.2.1. *Ο θετικός ακέραιος $n, n > 1$ θα λέγεται*

1. *Υπερτέλειος (abundant) , όταν $\sigma(n) > 2n$*
2. *Τέλειος (perfect) , όταν $\sigma(n) = 2n$*
3. *Ελλιπής (deficient) , όταν $\sigma(n) < 2n$*

Η ταξινόμηση αυτή ανάγεται στους Πυθαγόρειους.

Οι 4 πρώτοι (μικρότεροι) τέλειοι αριθμοί είναι :

- $6 = 1 + 2 + 3$
- $28 = 1 + 2 + 4 + 7 + 14$
- $496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$ *και*
- $8128 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064.$

Και οι 4 ήταν γνωστοί στον Νικόμαχο τον Γερασηνό και αναφέρονται στο έργο του «Αριθμητική Εισαγωγή».

Πρόταση 1.2.1. *(Ευκλείδη). Αν ο $2^n - 1$ είναι πρώτος αριθμός, τότε ο $2^{n-1}(2^n - 1)$ είναι τέλειος.*

Απόδειξη. Αφού $2^n - 1$ είναι πρώτος, έπεται ότι $\sigma(2^n - 1) = 1 + (2^n - 1) = 2^n$. Έστω $m := 2^{n-1}(2^n - 1)$. Επίσης, $(2^{n-1}, 2^n - 1) = 1$, επομένως $\sigma(m) = \sigma(2^{n-1}(2^n - 1)) = \sigma(2^{n-1})\sigma(2^n - 1) = 2^n \sum_{k=0}^{n-1} 2^k = 2^n(2^n - 1) = 2m$. Συνεπώς, ο m είναι τέλειος.

□

Παρατήρηση.*Η παραπάνω πρόταση εμπεριέχεται στα «Στοιχεία» του Ευκλείδη. (Βιβλίο IX, πρόταση 36)*

«Ε᾽αν ἀπό μονάδος ὁποσοιῶν ἀριθμοί ἐξῆς ἐκτεθῶσιν ἐν τῇ διπλασίονη ἀναλογία, ἕως οὗ σύμπας συντεθῆς πρῶτος γένηται, καί ὁ σύμπας ἐπί τον ἔσχατον πολλαπλασιασθείς ποιή τίνα, ὁ γενόμενος τέλειος ἔσται».

Δηλαδή, Αν το άθροισμα ενός δοσμένου πλήθους αριθμών που βρίσκονται σε συνεχή αναλογία η οποία ξεκινά από την μονάδα και έχει λόγο τον 2, είναι πρώτος αριθμός, τότε το γινόμενο του αθροίσματος με τον τελευταίο αριθμό της συνεχούς αναλογίας θα είναι τέλειος αριθμός.

(Αν $1+2+2^2+\cdots+2^{n-1}$ *είναι πρώτος αριθμός τότε ο* $2^{n-1}(1+2+2^2+\cdots+2^{n-1})$ *είναι τέλειος.)*

Παραδείγματα.

1. $1+2=3\in\mathbb{P}$. *Άρα, ο* $2\cdot 3=6$ *είναι τέλειος.*

2. $1+2+4=7\in\mathbb{P}$. *Συνεπώς, ο* $4\cdot 7=28$ *είναι τέλειος.*

3. $1+2+4+8+16=31\in\mathbb{P}$. *Οπότε, ο* $16\cdot 31=496$ *είναι τέλειος.*

4. $1+2+4+8+16+32=127\in\mathbb{P}$. *Επομένως, ο* $64\cdot 127=8128$ *είναι τέλειος.*

Έχοντας ως βάση τη γνώση αυτών των τεσσάρων τέλειων αριθμών ο Νικόμαχος ο Γερασηνός, διατύπωσε πέντε εικασίες. Στο έργο του Νικόμαχου αναφέρονται ως «αποτελέσματα» χωρίς την παραμικρή αναφορά σε αποδείξεις.

1. *Ο n-οστός τέλειος έχει n ψηφία.*

2. *Όλοι οι τέλειοι είναι άρτιοι.*

3. *Οι τέλειοι αριθμοί έχουν ψηφίο μονάδων 6 ή 8 και μάλιστα εναλλάξ.*

4. *Η πρόταση του Ευκλείδη (πρόταση 1.2.1) μας δίνει όλους τους τέλειους αριθμούς.*

5. *Υπάρχουν άπειροι τέλειοι αριθμοί.*

Στη συνέχεια θα εξετάσουμε τί είναι μέχρι σήμερα γνωστό σχετικά με τις εικασίες του Νικόμαχου.

Το 1747 ο Euler απέδειξε ότι ισχύει και το αντίστροφο της πρότασης του Ευκλείδη με τον περιορισμό όμως στους άρτιους αριθμούς. Συγκεκριμένα:

Πρόταση 1.2.2. *(Euler). Αν ο άρτιος φυσικός αριθμός m είναι τέλειος, τότε έχει κατ΄ ανάγκη τη μορφή $m = 2^{n-1}(2^n - 1)$, όπου ο $(2^n - 1)$ είναι πρώτος για κάποιο φυσικό αριθμό $n \geq 2$.*

Απόδειξη. Αφού ο m είναι άρτιος, γράφεται στη μορφή $m = 2^{n-1} \cdot l$, όπου $n > 1$ και l περιττός. Συνεπώς $(2^{n-1}, l) = 1$, οπότε

$$\sigma(m) = \sigma(2^{n-1} \cdot l) = \sigma(2^{n-1})\sigma(l) = (2^n - 1)\sigma(l).$$

Ο m όμως είναι τέλειος, συνεπώς

$$\sigma(m) = 2m = 2^n \cdot l$$

Επομένως, $2^n l = (2^n - 1)\sigma(l)$, δηλαδή $(2^n - 1) \mid 2^n l$ και επειδή $(2^n - 1, 2^n) = 1$, έχουμε $(2^n - 1) \mid l, l = (2^n - 1)t$, για κάποιο $t \in \mathbb{Z}$.
Αντικαθιστούμε το l στην προηγούμενη σχέση και απλοποιώντας, με το $2^n - 1$ βρίσκουμε

$$2^n \cdot t = \sigma(l).$$

Αλλά το l και το t είναι διαιρέτες του $l, (t < l)$. Επομένως, $l + t \leq \sigma(l) = 2^n \cdot t$. Επίσης, $l + t = (2^n - 1)t + t = 2^n \cdot t$, άρα $\sigma(l) = l + t$. Αυτό μας δείχνει ότι ο l έχει ακριβώς δύο διαιρέτες, τους l και t. Άρα, θα πρέπει ο l να είναι πρώτος $(l \in \mathbb{P})$ και ο $t = 1$. Καταλήξαμε στο συμπέρασμα ότι $l = (2^n - 1) \in \mathbb{P}$, δηλαδή ότι $m = 2^{n-1}(2^n - 1)$. □

Παρατήρηση. *Άμεσα προκύπτει από την πρόταση 1.2.2 ότι η εικασία (4) είναι σωστή αν δεχθούμε την ορθότητα της εικασίας (2).*

Ενδιαφέρον έχει να ελέγξουμε πότε ένας φυσικός αριθμός της μορφής $2^n - 1$, $n \geq 2$ είναι πρώτος.

Αρχικά όμως, ας εξετάσουμε πότε ένας ακέραιος της μορφής $a^n - 1, a > 1, n > 1$ είναι πρώτος.

Πρόταση 1.2.3. *Αν ο $a^n - 1, a > 1, n > 1$ είναι πρώτος, τότε κατ΄ ανάγκη $a = 2$ και n πρώτος αριθμός.*

Απόδειξη. Είναι γνωστή η παραγοντοποίηση

$$(a^n - 1) = (a - 1)(a^{n-1} + a^{n-2} + \cdots + a + 1).$$

Ο δεύτερος παράγοντας είναι μεγαλύτερος του 1. Επειδή $a^n - 1$, πρώτος, έπεται ότι $a - 1 = 1$, δηλαδή $a = 2$.
Αν τώρα ο n είναι σύνθετος, $n = m \cdot l, m > 1, l > 1$ τότε

$$2^n - 1 = 2^{ml} - 1 = (2^m)^l - 1 = (2^m - 1)((2^m)^{l-1} + \cdots + 2^m + 1).$$

Οι παράγοντες του δεξιού μέλους είναι και οι δύο μεγαλύτεροι του 1, δηλαδή ο $2^n - 1$ είναι σύνθετος. Συνεπώς, θα πρέπει ο n να είναι πρώτος. □

Παρατήρηση. *Όπως, βλέπουμε από την παραπάνω πρόταση (1.2.3) για να είναι ένας αριθμός της μορφής $2^n - 1$ πρώτος, η αναγκαία συνθήκη είναι να είναι ο n πρώτος. Προφανώς το αντίστροφο δεν ισχύει π.χ. για $n = 11 \in \mathbb{P}$ ο $2^n - 1 = 2^{11} - 1 = 2047 = 23 \cdot 89$ δεν είναι πρώτος.*
Έτσι, για να βρούμε όλους τους τέλειους άρτιους αριθμούς θα πρέπει να γνωρίζουμε όλους τους πρώτους της μορφής $2^p - 1, p \in \mathbb{P}$.

Ας γυρίσουμε, όμως, πίσω στην ιστορία ανακάλυψης τέλειων αριθμών. Σε ένα χειρόγραφο που χρονολογείται στα μέσα του 15ου αιώνα αποδεικνύεται ότι ο $2^{13} - 1$ είναι πρώτος και συνεπώς ο $2^{12}(2^{13} - 1) = 33550336$ είναι ο πέμπτος τέλειος αριθμός. Επομένως, η πρώτη εικασία του Νικόμαχου είναι λάθος (ο 5ος τέλειος αριθμός έχει 8 ψηφία).

Το 1555 ο Schebyl και το 1588 ο Piedro Antonio Cataldi , ένας μαθηματικός από τη Μπολόνια, απέδειξαν ότι οι $2^{17} - 1 = 131071$ και $2^{19} - 1 = 524287$ είναι πρώτοι και έτσι ανακάλυψαν τους επόμενους δύο τέλειους αριθμούς 8589869056, 137438691328. Οπότε, οι διαδοχικοί τέλειοι 5ος και 6ος τελειώνουν και οι δύο σε 6. Άρα, δεν ισχύει το εναλλάξ στην εικασία (3). Το υπόλοιπο της εικασίας (3) όμως είναι σωστό. Αποδείχθηκε από τον Euler .

Πρόταση 1.2.4. *Το ψηφίο των μονάδων ενός άρτιου τέλειου φυσικού αριθμού m είναι 6 ή 8.*

Απόδειξη. Σύμφωνα με την πρόταση 1.2.2 ο $m = 2^{n-1}(2^n - 1)$ και ο $2^n - 1 =: p$ είναι πρώτος.
Σύμφωνα με την πρόταση 1.2.3 , θα πρέπει ο $n =: q \in \mathbb{P}$. Αν $q = 2$, τότε $m = 2 \cdot 3 = 6$, που ισχύει.
Έστω τώρα $q > 2$. Ξεχωρίζουμε δύο περιπτώσεις:
Περίπτωση 1: Ο q είναι της μορφής $4l + 1$. Στην περίπτωση αυτή ο m γράφεται

$$m = 2^{4l}(2^{4l+1} - 1) = 2^{8l+1} - 2^{4l} = 2 \cdot 16^{2l} - 16^l$$

Επαγωγικά αποδεικνύεται ότι ο 16^l γράφεται πάντα στη μορφή $10s + 6, s \in \mathbb{Z}$.
Πραγματικά, για $l = 1$ ισχύει. Έστω ότι ισχύει για $l = k$, δηλαδή ότι $16^k = 10s + 6$.

Για $l = k+1 : 16^{k+1} = 16 \cdot 16^k = 16(10s+6) = 160s+96 = 10t+6$, όπου $t = 16s+9$. Επομένως, ο

$$m = 2(10s_1 + 6) - (10s_2 + 6) = 10(2s_1 - s_2) + 6$$

Περίπτωση 2: Ο q είναι της μορφής $4l + 3$. Τότε $m = 2^{4l+2}(2^{4l+3} - 1) = 2^{8l+5} - 2^{4l+2} = 2 \cdot 16^{2l+1} - 4 \cdot 16^l = 2(10t_1 + 6) - 4(10t_2 + 6) = 10(2t_1 - 4t_2) - 12 = 10(2t_1 - 4t_2 - 2) + 8$. □

Παρατήρηση. *Μπορούμε μάλιστα να αποδείξουμε ότι τα τελικά ψηφία άρτιου τέλειου αριθμού είναι το 6 ή 28 και θα το αποδείξουμε ευθύς αμέσως.*

Αφού ένας ακέραιος είναι ισότιμος $\pmod{100}$ *με τα 2 τελευταία του ψηφία, αρκεί να αποδείξουμε ότι αν ο n είναι της μορφής $4l + 3$,τότε $m \equiv 28 \pmod{100}$. Για να το δούμε αυτό παρατηρούμε ότι:*

$$2^{n-1} = 2^{4l+2} = 16^l \cdot 4 \equiv 6 \cdot 4 \equiv 4 \pmod{10}$$

Επιπλέον, για $n > 2$ έχουμε ότι $4 \mid 2^{n-1}$ και ο αριθμός που προκύπτει από τα δύο τελευταία ψηφία του 2^{n-1} διαιρείται από το 4. Οπότε έχουμε ότι το τελευταίο ψηφίο του 2^{n-1} είναι 4, ενώ το 4 διαιρεί τα δύο τελευταία του ψηφία. Στο modulo 100, οι διάφορες επιλογές είναι

$$2^{n-1} \equiv 4, 24, 44, 64 \text{ ή } 84$$

Αλλά αυτό συνεπάγεται ότι

$$2^n - 1 = 2 \cdot 2^{n-1} - 1 \equiv 7, 47, 87, 27 \text{ ή } 67 \pmod{100}$$

άρα

$$m = 2^{n-1}(2^n - 1) \equiv 4 \cdot 7, 24 \cdot 47, 44 \cdot 87, 64 \cdot 27 \text{ ή } 84 \cdot 67 \pmod{100}.$$

Καθένα από τα παραπάνω γινόμενα είναι ισότιμο με 28 modulo 100.

Είναι άγνωστο αν υπάρχουν περιττοί τέλειοι αριθμοί. Υπάρχει ωστόσο μια σειρά αποτελέσματα χωρίς όμως οι μαθηματικοί να έχουν φτάσει στην απάντηση της ερώτησης αν υπάρχουν ή όχι.

Θεώρημα 1.2.1. *(Euler). Αν ο n είναι ένας περιττός τέλειος αριθμός, τότε $n = p_1^{k_1} p_2^{2j_2} \cdots p_r^{2j_r}$, όπου τα p_i είναι διαφορετικοί μεταξύ τους πρώτοι αριθμοί και $p_1 \equiv k_1 \equiv 1 \pmod{4}$*

Απόδειξη. Έστω $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ η ανάλυση του n σε πρώτους. Αφού ο n είναι τέλειος μπορούμε να γράψουμε

$$2n = \sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2})\cdots\sigma(p_r^{k_r})$$

Αφού ο n είναι περιττός ακέραιος θα είναι $n \equiv 1 \pmod 4$ ή $n \equiv 3 \pmod 4$. Σε κάθε περίπτωση $2n \equiv 2 \pmod 4$. Άρα, $\sigma(n) = 2n$ διαιρείται από το 2 αλλά όχι από το 4. Το συμπέρασμα είναι ότι ένας από τους $\sigma(p_i^{k_i})$, έστω ο $\sigma(p_1^{k_1})$, πρέπει να είναι άρτιος ακέραιος (που δεν διαιρείται με το 4), ενώ όλοι οι υπόλοιποι $\sigma(p_i^{k_i})$ είναι περιττοί ακέραιοι. Τώρα για κάθε τέτοιο δοσμένο p_i υπάρχουν δύο περιπτώσεις: $p_i \equiv 1 \pmod 4$ ή $p_i \equiv 3 \pmod 4$.
Αν $p_i \equiv 3 \equiv -1 \pmod 4$ θα έχουμε

$$\sigma(p_i^{k_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{k_i} \equiv 1 + (-1) + (-1)^2 + \cdots + (-1)^{k_i} \pmod 4$$

$$= \begin{cases} 0 \pmod 4, \text{ αν } k_i \text{ είναι περιττός} \\ 1 \pmod 4, \text{ αν } k_i \text{ είναι άρτιος} \end{cases}$$

Αφού $\sigma(p_1)^{k_1} \equiv 2 \pmod 4$ συμπεραίνουμε ότι $p_1 \equiv 1 \pmod 4$. Επιπλέον, η συνθήκη $\sigma(p_i^{k_i}) \equiv 0 \pmod 4$ δείχνει ότι το 4 διαιρεί το $\sigma(p_i^{k_i})$ το οποίο είναι αδύνατο. Συνεπώς, αν $p_i \equiv 3 \pmod 4$, όπου $i = 2, \ldots, r$ τότε ο εκθέτης του k_i είναι άρτιος ακέραιος.
Αν $p_i \equiv 1 \pmod 4$ (το οποίο σίγουρα αληθεύει για $i = 1$) τότε:

$$\sigma(p_i^{k_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{k_i} \equiv 1 + 1 + 1^2 + \cdots + 1^{k_i} \pmod 4 \equiv k_i + 1 \pmod 4$$

Η συνθήκη $\sigma(p_1^{k_1}) = 2 \pmod 4$ οδηγείται στην $k_1 \equiv 1 \pmod 4$. Για τις άλλες τιμές του i , εμείς ξέρουμε ότι $\sigma(p_i^{k_i}) \equiv 1$ ή $3 \pmod 4$ και επιπλέον $k_i \equiv 0$ ή $2 \pmod 4$. Σε κάθε περίπτωση k_i είναι άρτιος ακέραιος. Οπότε είτε $p_i \equiv 1 \pmod 4$ είτε $p_i \equiv 3 \pmod 4$, το k_i είναι πάντα άρτιος για $i \neq 1$. □

Πόρισμα 1.2.1. *Εάν n είναι περιττός τέλειος αριθμός, τότε ο n είναι της μορφής $n = p^k m^2$, όπου p είναι πρώτος, p δεν διαιρεί τον m και $p \equiv k \equiv 1 \pmod 4$ συγκεκριμένα $n \equiv 1 \pmod 4$*

Απόδειξη. Μόνο ο τελευταίος ισχυρισμός δεν είναι προφανής. Διότι από $p \equiv 1 \pmod 4$ έπεται ότι $p^k \equiv 1 \pmod 4$. Σημειώνουμε ότι το m πρέπει να είναι περιττός, άρα $m \equiv 1$ ή $3 \pmod 4$ και επιπλέον $m^2 \equiv 1 \pmod 4$. Επομένως, ότι $n = p^k m^2 \equiv 1 \cdot 1 \equiv 1 \pmod 4$ δημιουργώντας τον περιορισμό μας. □

Τα μέχρι σήμερα γνωστά αποτελέσματα μας λένε ότι κάθε περιττός τέλειος αριθμός n πρέπει να είναι της μορφής $12m + 1$ ή $36m + 9$ και να ικανοποιεί τις ακόλουθες ιδιότητες:

- *Στην παραγοντοποίηση του n στο Θεώρημα 1.2.1 ο r είναι τουλάχιστον 9, και ο r είναι τουλάχιστον 12 αν το 3 δεν διαιρεί το n (Nielsen 2006).*
- *Στην παραγοντοποίηση του n στο Θεώρημα 1.2.1, ένας τουλάχιστον από τους $j_2, \cdots, j_r$ είναι μεγαλύτερος από 1. (Steuerwald 1937)*
- *Ο μεγαλύτερος πρώτος που διαιρεί το n είναι μεγαλύτερος από 10^8 (Takeshi Goto and Yasuo Ohno , 2006).*
- *Ο δεύτερος μεγαλύτερος πρώτος που διαιρεί το n είναι μεγαλύτερος από 10^4 , και ο τρίτος μεγαλύτερος πρώτος είναι μεγαλύτερος από 100 (Iannucci 1999, 2000).*
- *Ο n έχει τουλάχιστον 75 πρώτους στην παραγοντοποίησή του, υπολογίζοντας κάθε μια από τις $2j_r$ επαναλήψεις του p_r χωριστά (Kevin Hare 2005).*
- *Ο n είναι μικρότερος από 2^{4^r} όπου r είναι ο αριθμός των διακεκριμένων πρώτων που τον διαιρούν (οπότε $k = r + 1$ όπου όπως r πριν) (Nielsen 2003).*

Αν υπάρχει περιττός τέλειος τότε θα είναι μεγαλύτερος από 10^{500}.

1.3 Πρώτοι αριθμοί Mersenne και Fermat

Ορισμός 1.3.1. *Οι πρώτοι αριθμοί της μορφής $2^p - 1$, όπου p πρώτος, λέγονται πρώτοι αριθμοί του Mersenne .*

Σήμερα είναι γνωστοί 48 πρώτοι της μορφής $2^p - 1$ και άρα 48 τέλειοι άρτιοι αριθμοί. Ο $2^{88}(2^{89} - 1)$ είναι ο τελευταίος που υπολογίστηκε με το χέρι το 1911, όλοι οι άλλοι έχουν βρεθεί με την βοήθεια υπολογιστή. Ο μεγαλύτερος από αυτούς - ο 48ος - αποτελείται από 17.425.170 ψηφία. Δεν είναι γνωστό αν υπάρχουν άπειροι πρώτοι της μορφής $2^p - 1$, επομένως και άπειροι άρτιοι τέλειοι.

Στον παρακάτω πίνακα παρατήθενται πληροφορίες για τους πρώτους Mersenne που είναι γνωστοί μέχρι σήμερα.

Πίνακας Πρώτων Mersenne

#	Πρώτος p	Ψηφία του M_p	Ψηφία του P_p [1]	Χρονολογία	Ανακαλύφθηκε από:
1	2	1	1	430 π.Χ.	Αρχαίοι Έλληνες Μαθηματικοί
2	3	1	2	430 π.Χ.	Αρχαίοι Έλληνες Μαθηματικοί
3	5	2	3	300 π.Χ	Αρχαίοι Έλληνες Μαθηματικοί

[1] Με P_p συβολίζουμε τον τέλειο αριθμό που προκύπτει από τον αντίστοιχο Mersenne

#	Πρώτος p	Ψηφία του M_p	Ψηφία του P_p	Χρονολογία	Ανακαλύφθηκε από:
4	7	3	4	300 π.Χ.	Αρχαίοι Έλληνες Μαθηματικοί
5	13	4	8	1456	Άγνωστος
6	17	6	10	1588	Cataldi
7	19	6	12	1588	Cataldi
8	31	10	19	1772	Euler
9	61	19	37	1883	Pervushin
10	89	27	54	1911	Powers
11	107	33	65	1914	Powers
12	127	39	77	1876	Lucas
13	521	157	314	1952	Robinson
14	607	183	366	1952	Robinson
15	1279	386	770	1952	Robinson
16	2203	664	1327	1952	Robinson
17	2281	687	1373	1952	Robinson
18	3217	969	1937	1957	Riesel
19	4253	1281	2561	1961	Hurwitz
20	4423	1332	2663	1961	Hurwitz
21	9689	2917	5834	1963	Gillies
22	9941	2993	5985	1963	Gillies
23	11213	3376	6751	1963	Gillies
24	19937	6002	12003	1971	Tuckerman
25	21701	6533	13066	1978	Noll, Nickel
26	23209	6987	13973	1979	Noll
27	44497	13395	26790	1979	Nelson, Slowinski
28	86243	25962	51924	1982	Slowinski
29	110503	33265	66530	1988	Colquitt, Welsh
30	132049	39751	79502	1983	Slowinski
31	216091	65050	130100	1985	Slowinski
32	756839	227832	455663	1992	Slowinski, Gage
33	859433	258716	517430	1994	Slowinski, Gage
34	1257787	378632	757263	1996	Slowinski, Gage
35	1398269	420921	841842	1996	GIMPS /Armengaud
36	2976221	895932	1791864	1997	GIMPS / Spence
37	3021377	909526	1819050	1998	GIMPS /Clarkson
38	6972593	2098960	4197919	1999	GIMPS / Hajratwala
39	13466917	4053946	8107892	2001	GIMPS / Cameron
40	20996011	6320430	12640858	2003	GIMPS /Shafer
41	24036583	7235733	14471465	2004	GIMPS / Findley
42	25964951	7816230	15632458	2005	GIMPS /Nowak
43	30402457	9152052	18304103	2005	GIMPS / Cooper & Boone
44⋆	32582657	9808358	19616714	2006	GIMPS / Cooper & Boone
45⋆	37156667	11185272	22370543	2008	GIMPS / Elvenich
46⋆	42643801	12837064	25674127	2009	GIMPS / Strindmo
47⋆	43112609	12978189	25956377	2008	GIMPS / Smith
48⋆	57885161	17425170	34850339	2013	GIMPS / Cooper

Τα τελευταία πέντε στοιχεία είναι με αστερίσκο διότι δεν έχει αποδειχθεί ακόμη ότι δεν υπάρχουν πρώτοι Mersenne ανάμεσά τους.

Θεώρημα 1.3.1. *Αν ο αριθμός $a^n + 1$ είναι πρώτος, $a > 1$ και $n > 0$ τότε ο a είναι άρτιος και $n = 2^r$ για κάποιο ακέραιο r.*

Απόδειξη. Αν ο a ήταν περιττός, τότε ο $a^n+1 \geq 4$ θα ήταν άρτιος, δηλαδή όχι πρώτος, άτοπο.
Αν ο n δεν ήταν δύναμη του 2 θα είχε κάποιο περιττό πρώτο παράγοντα, έστω q, $n = mq$. Τότε, όμως, θα είχαμε

$$a^n + 1 = a^{mq} + 1 = (a^m + 1)(a^{m(q-1)} - a^{m(q-2)} + \cdots - a^m + 1).$$

Επειδή το $q \geq 3$ οι παράγοντες του δεξιού μέλους είναι και οι δυο μεγαλύτεροι του 1 και άρα ο $a^n + 1$ δεν είναι πρώτος. Συνεπώς $n = 2^r, r \in \mathbb{N}$. □

Ο Fermat θεώρησε την ειδική περίπτωση που $a = 2$, δηλαδή αριθμούς της μορφής $2^{2^n} + 1$. Για $n = 0, 1, 2, 3, 4$ οι αριθμοί αυτοί είναι πρώτοι. Πράγματι, $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$.

Η εικασία του ήταν ότι όλοι οι αριθμοί αυτής της μορφής είναι πρώτοι. Εδώ, όμως, ο Fermat στάθηκε άτυχος. Αν είχε κάνει ένα βήμα ακόμη θα είχε διαπιστώσει το λάθος του. Πράγματι, ο F_5 διαιρείται από το 641 ($F_5 = 4294967297 = 641 \cdot 6700417$). Βέβαια η διαπίστωση έγινε έναν αιώνα αργότερα από τον Euler .

Ορισμός 1.3.2. *Οι πρώτοι αριθμοί της μορφής $2^{2^n} + 1$ λέγονται πρώτοι αριθμοί του Fermat .*

1.4 Οι αριθμοί Fibonacci και οι αριθμοθεωρητικές ιδιότητες τους

Ο Leonardo Pisano Bigollo (1170-1250 μ.Χ.), γνωστός επίσης και ως Λεονάρδος της Πίζας (Leonardo Pisano) , ή Leonardo Bonacci , ή Leonardo Fibonacci , ή απλούστερα Fibonacci , ήταν ένας Ιταλός μαθηματικός που από πολλούς θεωρείται ως ο πιο προικισμένος μαθηματικός της Δύσης, κατά τον Μεσαίωνα. Έμεινε στην ιστορία για την εισαγωγή στην Ευρώπη του δεκαδικού συστήματος αρίθμησης και άλλων σπουδαίων καινοτομιών (ιδιαίτερα σε μια τόσο σκοτεινή εποχή για την Ευρώπη), αλλά κυρίως για την περίφημη ακολουθία του, την ακολουθία Fibonacci .

Ήταν γιος του Ιταλού διπλωμάτη Guglielmo Bonaccio (Bonaccio σημαίνει απλός), γι΄ αυτό και το πατρώνυμό του είναι το Φιμπονάτσι, δηλαδή γιος του Bonacci (filius Bonacci). Το 1202 σε ηλικία 32 ετών συνέγραψε το έργο Liber Abacci (βιβλίο των

υπολογισμών), με το οποίο συνέβαλε στην καθιέρωση των αραβικών αριθμών στην Ευρώπη και παρουσίασε ένα «νέο» πρόβλημα από το οποίο οδηγήθηκε στην περίφημη ακολουθία για την οποία είναι γνωστός. Το πρόβλημα αυτό είναι το εξής:

Κάποιος τοποθέτησε σε έναν αποκλεισμένο τόπο ένα ζευγάρι κουνελιών. Τα κουνέλια αυτά αναπαράγονται με ρυθμό ένα νέο ζευγάρι το μήνα και κάθε νέο ζευγάρι γίνεται γόνιμο δύο μήνες μετά κι αναπαράγεται με τον ίδιο ρυθμό. Πόσα ζευγάρια κουνελιών έχουν παραχθεί σε έναν χρόνο από το αρχικό ζεύγος;

Το αποτέλεσμα είναι η ακολουθία 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, 10946 ... (ο Φιμπονάτσι παρέλειψε τον πρώτο όρο στο Liber abaci). Εδώ λοιπόν κάθε νέος όρος είναι το άθροισμα των δύο προηγουμένων όρων. Οι όροι της ακολουθίας αυτής ονομάζονται αριθμοί Fibonacci . Η ακολουθία αναδρομικά δίνεται από τον τύπο:

$$F_0 = 0, F_1 = 1, F_{n+1} = F_n + F_{n-1} \quad \text{για κάθε} \quad n \geq 1$$

Πρόκειται για μια αρκετά ενδιαφέρουσα ακολουθία με πολλές εφαρμογές η οποία βρίσκεται μέχρι σήμερα στο κέντρο της ερευνητικής δραστηριότητας. Μάλιστα έχει ιδρυθεί η Fibonacci Assosiation η οποία εκδίδει και περιοδικό με τίτλο The Fibonacci Quarterly .

Παρακάτω θα εξετάσουμε μερικές αριθμοθεωρητικές ιδιότητες των αριθμών Fibonacci .

Πρόταση 1.4.1. *Για κάθε φυσικό αριθμό $n \geq 1$ ισχύει*

$$F_{n+m} = F_{n-1}F_m + F_nF_{m+1}$$

Απόδειξη. Θα κάνουμε επαγωγή ως προς m. Για $m = 0$, προφανώς ισχύει. Υποθέτουμε ότι ισχύει για όλα τα $m, m \leq k+1$. Επομένως, ισχύουν $F_{n+k} = F_{n-1}F_k + F_nF_{k+1}$ και $F_{n+k+1} = F_{n-1}F_{k+1} + F_nF_{k+2}$. Προσθέτουμε κατά μέλη και έχουμε

$$F_{n+k} + F_{n+k+1} = F_{n-1}F_k + F_nF_{k+1} + F_{n-1}F_{k+1} + F_nF_{k+2}$$

Δηλαδή,

$$F_{n+k+2} = F_{n-1}(F_k + F_{k+1}) + F_n(F_{k+1} + F_{k+2})$$

Οπότε, προκύπτει ότι $F_{n+k+2} = F_{n-1}F_{k+2} + F_nF_{k+3}$, δηλαδή ισχύει και για $k + 2$ και επομένως για κάθε φυσικό αριθμό m. □

Πρόταση 1.4.2. *Για κάθε $m, n \in \mathbb{N}$ ισχύουν:*

1. *Αν $m \mid n$ τότε $F_m \mid F_n$*
2. *Μ.Κ.Δ.(F_n, F_{n+1})= 1*

3. *Μ.Κ.Δ.*(F_n, F_m)= $F_{Μ.Κ.Δ.(n,m)}$

Απόδειξη. 1. Επειδή $m \mid n$ έπεται ότι $n = mm_1$ για κάποιο $m_1 \in \mathbb{N}$. Εφαρμόζουμε μαθηματική επαγωγή ως προς m_1. Για $m_1 = 0$, έχουμε $n = 0$, δηλαδή $F_0 = 0$ ο οποίος διαιρείται από κάθε F_m. (Αν $m_1 = 1$ τότε $m = n$ οπότε και $F_m = F_n \mid F_n$.) Υποθέτουμε ότι η πρόταση ισχύει για τον m_1, δηλαδή ότι $F_m \mid F_{mm_1}$.Θα αποδείξουμε ότι ισχύει και για $m_1 + 1$. Πράγματι, από την Πρόταση 1.4.1

$$F_{m(m_1+1)} = F_{mm_1+m} = F_{mm_1-1}F_m + F_{mm_1}F_{m+1}.$$

Συνεπώς, $F_m \mid F_{m(m_1+1)}$.

2. Υποθέτουμε ότι $(F_n, F_{n+1}) = d > 1$. Επομένως, $d \mid F_{n-1} = F_{n+1} - F_n$. Όμοια συμπεραίνουμε ότι $d \mid F_{n-2}$ και, συνεχίζοντας επαγωγικά, τελικά καταλήγουμε ότι θα πρέπει $d \mid F_1 = 1$, άτοπο. Άρα, $d = 1$.

3. Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $m > n$. Εφαρμόζουμε διαδοχικά τον ευκλείδειο αλγόριθμο :

$$\begin{gathered} m = nq_0 + r_1, \text{ όπου } 0 \le r_1 < n, \\ n = r_1q_1 + r_2, \text{ όπου } 0 \le r_2 < r_1, \\ r_1 = r_2q_2 + r_3, \text{ όπου } 0 \le r_3 < r_2, \\ \vdots \\ r_{t-2} = r_{t-1}q_{t-1} + r_t, \text{ όπου } 0 \le r_t < r_{t-1} \\ r_{t-1} = r_tq_t \text{ και } r_t = (m, n). \end{gathered}$$

Επομένως, για τους αντίστοιχους αριθμούς Fibonacci έχουμε

$$(F_m, F_n) = (F_{nq_0+r_1}, F_n) = (F_{nq_0-1}F_{r_1}+F_{nq_0}F_{r_1+1}, F_n) = (F_{nq_0-1}F_{r_1}, F_n) = (F_{r_1}, F_n),$$

διότι, λόγω της 2.,

$$(F_n, F_{nq_0-1}) \mid (F_{nq_0}, F_{nq_0-1}) = 1.$$

Όμοια αποδεικνύεται ότι:

$$\begin{gathered} (F_{r_1}, F_n) = (F_{r_2}, F_n), \\ (F_{r_2}, F_{r_1}) = (F_{r_3}, F_{r_2}), \\ \vdots \\ (F_{r_{t-1}}, F_{r_{t-2}}) = (F_{r_t}, F_{r_{t-1}}). \end{gathered}$$

Λόγω της ιδιότητας 1., επειδή $F_{r_t} \mid F_{r_{t-1}}$ έπεται ότι $(F_{r_t}, F_{r_{t-1}}) = F_{r_t}$. Άρα,

$$(F_m, F_n) = (F_{r_t}, F_{r_{t-1}}) = F_{r_t} = F_{(m,n)}$$

□

Κεφάλαιο 2

Η ύπαρξη άπειρων πρώτων

2.1 Αποδείξεις για την ύπαρξη άπειρων πρώτων

2.1.1 Εισαγωγή

Η απάντηση στην ερώτηση «πόσοι πρώτοι αριθμοί υπάρχουν;» δίνεται από το Θεμελιώδες Θεώρημα:

Θεώρημα 2.1.1. *Το σύνολο των πρώτων αριθμών $\mathbb{P}$ είναι άπειρο.*

Σε αυτό το κεφάλαιο θα δούμε διάφορες αποδείξεις αυτού του θεωρήματος από διάσημους, αλλά επίσης και από ξεχασμένους , μαθηματικούς. Μερικές αποδείξεις προτείνουν ενδιαφέροντα αναπτύγματα, άλλες είναι απλά έξυπνες ή περίεργες. Υπάρχουν, φυσικά, πολύ περισσότερες αποδείξεις της ύπαρξης άπειρων πρώτων αριθμών από αυτές που θα παρουσιάσουμε σε αυτό το κεφάλαιο. Θα παρουσιάσουμε όμως μερικές αντιπροσωπευτικές από αυτές.

2.1.2 Αποδείξεις που βασίζονται στην ιδέα του Ευκλείδη

Πρώτος ο Ευκλείδης από την Αλεξάνδρεια γύρω στο 300 π.Χ. απέδειξε ότι το πλήθος των πρώτων αριθμών είναι άπειρο.

1η απόδειξη (του Ευκλείδη (300 π.Χ.))

Έστω $\mathbb{P}$ πεπερασμένο, $\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$.Θεωρούμε τον φυσικό αριθμό $N = p_1 p_2 \cdots p_n + 1$. Αφού $N > 1$, υπάρχει κάποιος πρώτος p τέτοιος ώστε $p \mid N$. Αλλά, ο p είναι διάφορος των $p_1, p_2, \ldots, p_n$ διότι αλλιώς $p \mid N - p_1 p_2 \cdots p_n = 1$, άτοπο. Άρα, το $\mathbb{P}$ είναι άπειρο. □

Υπάρχουν διάφορες παραλλαγές της απόδειξης του Ευκλείδη. Η πιο απλή από αυτές είναι η απόδειξη του Hermite (1915), η οποία προκύπτει από το γεγονός ότι ο μικρότερος πρώτος διαιρέτης του $n!+1$ είναι μεγαλύτερος από το n. Συγκεκριμένα:

2η απόδειξη (του Hermite)

Αφού $n!+1 = 1\cdot2\cdot3\cdot4\cdots(n-1)\cdot n+1 > 1$ υπάρχει πρώτος p τέτοιος ώστε $p \mid (n!+1)$. Ο p είναι μεγαλύτερος από το n αφού αν $p \leq n$ τότε $p \mid [(n!+1)-(1\cdot2\cdot3\cdots(n-1)n)] = 1$, άτοπο. Άρα, υπάρχει $p > n$ τέτοιος ώστε $p \mid (n!+1)$ για κάθε φυσικό αριθμό n. Επομένως, υπάρχουν άπειροι πρώτοι. □

Άλλη μια τέτοια απόδειξη είναι αυτή του Kummer (1878/9) , η οποία στην πραγματικότητα είναι μια κομψή παραλλαγή της απόδειξης του Ευκλείδη.

3η απόδειξη (του Kummer (1878))

Έστω ότι υπάρχουν πεπερασμένου πλήθους πρώτοι αριθμοί, οι οποίοι (διατεταγμένοι) είναι οι: $p_1 < p_2 < \cdots < p_n$. Προφανώς $n \geq 2$ αφού $p_1 = 2$ και $p_2 = 3$ πρώτοι. Αφού κάθε ακέραιος μεγαλύτερος του 1 έχει πρώτο παράγοντα κάποιον p_i, ο μόνος αριθμός που θα είναι πρώτος ως προς τον $D = p_1p_2\cdots p_n$ θα είναι ο 1. Παίρνουμε τον $D-1$, είναι φυσικός μεγαλύτερος του 1. Αν, λοιπόν, $p_i \mid D-1$ τότε $p_i \mid (D-1, D)$ γιατί και $p_i \mid D$. Άτοπο, διότι $(D-1, D) = 1$. Επομένως, ο $D-1$ διαιρείται από κάποιον $p, p \neq p_i \forall i = 1, 2, \cdots n$ και συνεπώς υπάρχουν άπειροι πρώτοι. □

Επίσης, άλλες τέτοιες αποδείξεις είναι του T.J.Stieltjes (1890) του Braun (1899) και του Metrod (1917).

4η απόδειξη (του T.J.Stieltjes (1890))

Έστω p_n ο μεγαλύτερος πρώτος. Γράφουμε το γινόμενο των υπαρχόντων πρώτων $p_1, p_2, \ldots, p_n$ σαν γινόμενο $A \cdot B$ καθ' όλους τους δυνατούς τρόπους. Αφού ο καθένας από τους $p_1, p_2, \ldots, p_n$ διαιρεί τον A ή τον B αλλά όχι συγχρόνως και τους δυο, τότε ο αριθμός $A+B$ δεν διαιρείται από κανένα από τα $p_1, p_2, \ldots, p_n$. Όμως, επειδή $A+B > 1$ έπεται ότι υπάρχει πρώτος $p \neq p_i, i = 1, 2, \ldots, n$ τέτοιος ώστε $p \mid (A+B)$. Δηλαδή υπάρχει κάποιος μεγαλύτερος του p_n. Άτοπο. Άρα, υπάρχει άπειρο πλήθος πρώτων αριθμών. □

5η απόδειξη (του Braun (1899))

Έστω p_n ο μεγαλύτερος πρώτος, $p_1 < p_2 < \cdots < p_n$. Αφού το 5 είναι πρώτος θα

έχουμε ότι $p_n \geq 5$. *Τώρα* $\frac{1}{p_1}+\frac{1}{p_2}+\cdots+\frac{1}{p_n} = \frac{N}{D}$, *όπου* $N = p_2p_3\cdots p_n + p_1p_3\cdots p_n + \cdots + p_1p_2\cdots p_n$ *και* $D = p_1p_2\cdots p_n$. *Αφού* $\frac{1}{2}+\frac{1}{3}+\frac{1}{5} > 1 \Rightarrow \frac{N}{D} > 1 \Rightarrow N > D > 1$, *οπότε προκύπτει ότι υπάρχει πρώτος* p *τέτοιος ώστε* $p \mid N$. *Όμως, κανένας από τους* $p_1, p_2, \ldots, p_n$ *δεν διαιρεί τον* N, *διότι λείπει σε έναν ακριβώς προσθετέο του* N, *οπότε* $p > p_n$. *Άτοπο. Άρα, υπάρχει άπειρο πλήθος πρώτων αριθμών.* □

6η απόδειξη (του Metrod (1917))

Υποθέτουμε ότι υπάρχουν ακριβώς r *στο πλήθος πρώτοι αριθμοί, δηλαδή* $p_1, p_2, \ldots, p_r$. *Έστω* $N = p_1p_2\cdots p_r$ *και για κάθε* $i = 1, 2, \ldots, r$ *έστω* $Q_i = N/p_i$. *Σημειώνουμε ότι το* p_i *δεν διαιρεί το* Q_i *για κάθε* i , *ενώ* p_i *διαιρεί το* Q_j *για κάθε* $i \neq j$. *Έστω* $S = \sum_{i=1}^{r} Q_i$. *Αν* q *είναι ένας οποιοσδήποτε πρώτος που διαιρεί το* S , *τότε* $q \neq p_i$, *διότι το* p_i *διαιρεί τα* Q_j *(για* $i \neq j$*) αλλά* p_i *δεν διαιρεί το* Q_i. *Άρα υπάρχει ένας ακόμη πρώτος!* □

2.1.3 Αποδείξεις που βασίζονται στην ιδέα του Goldbach για τους σχετικά πρώτους αριθμούς

Η ιδέα του Goldbach στηρίζεται στο γεγονός ότι κάθε μη πεπερασμένη ακολουθία ακεραίων οι οποίοι είναι ανά δύο πρώτοι μεταξύ τους οδηγεί στην απόδειξη του θεωρήματος του Ευκλείδη. Ειδικότερα, η απόδειξη του Goldbach είναι η εξής:

7η απόδειξη (του Goldbach)

Έχουμε τους αριθμούς Fermat $F_n = 2^{2^n} + 1$ *για* $n = 0, 1, 2, \ldots$. *Θα δείξουμε ότι δυο οποιοιδήποτε αριθμοί Fermat είναι πρώτοι μεταξύ τους, άρα πρέπει να υπάρχουν άπειροι στο πλήθος πρώτοι αριθμοί. Θα αποδείξουμε επαγωγικά τη σχέση:*

$$\prod_{k=0}^{n-1} F_k = F_n - 2, \quad n \geq 1$$

την οποία θα χρησιμοποιήσουμε για την απόδειξή μας.
Για $n = 1$*: έχουμε* $F_0 = 3$ *και* $F_1 - 2 = 5 - 2 = 3$
Επαγωγική υπόθεση: Έστω ότι ισχύει για n, *δηλαδή ότι*

$$\prod_{k=0}^{n-1} F_k = F_n - 2$$

Επαγωγικό βήμα: Θα δείξουμε ότι ισχύει για $n+1$.

$$\prod_{k=1}^{n} F_k = \Big(\prod_{k=0}^{n-1} F_k\Big) \cdot F_n = (F_n - 2)F_n = (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2$$

Έστω m *κοινός διαιρέτης των* F_k *και* F_n, $(k < n)$. *Ο* $m \mid \prod_{k=0}^{n-1} F_k$, *αφού διαιρεί έναν παράγοντα (τον* $F_k, k < n$*). Άρα από τη σχέση που δείξαμε* $m \mid (F_n - 2)$ *και* $m \mid F_n$. *Επομένως,* $m \mid 2$ *άρα* $m = 1$ *ή* 2. *Όλοι οι αριθμοί Fermat είναι περιττοί, οπότε δεν διαιρούνται με το 2.*

Άρα, $m = 1$. *Οπότε* $(F_k, F_n) = 1$. *Έτσι, έχουμε μια άπειρη ακολουθία αριθμών Fermat που έχουν διαφορετικούς μεταξύ τους πρώτους διαιρέτες. Άρα, υπάρχουν άπειροι στο πλήθος πρώτοι αριθμοί.* □

Μια παραλλαγή της απόδειξης αυτής είναι :

Έστω ότι F_n *και* F_{n+k}, *όπου* $k > 0$ *είναι δύο αριθμοί Fermat και έστω ότι έχουν κάποιο κοινό διαιρέτη* m.
Αν $x = 2^{2^n}$, *έχουμε:*

$$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \cdots - 1$$

και έτσι $F_n \mid F_{n+k} - 2$. *Άρα,*

$$m \mid F_{n+k} \quad \text{και} \quad m \mid F_{n+k} - 2$$

και έτσι $m \mid 2$. *Αφού,* F_n *είναι περιττός,* $m = 1$. *Οπότε,* $(F_n, F_{n+k}) = 1$.

Η απόδειξη του Schorn είναι,όπως θα δούμε, μια από τις αποδείξεις που ανήκουν σε αυτή την κατηγορία.

8η απόδειξη (Schorn)

Πρώτα απ΄ όλα, σημειώνουμε ότι αν $1 \le i < j \le n$ *τότε ο*

$$M.K.\Delta.((n!)i + 1, (n!)j + 1) = 1$$

Πράγματι, γράφοντας $j = i + d$, *τότε* $1 \le d \le n$, *έτσι :*

$M.K.\Delta.((n!)i + 1, (n!)j + 1) = M.K.\Delta.\ ((n!)i + 1, (n!)d) = 1,$
διότι κάθε πρώτος p *που διαιρεί το* $(n!)d$ *είναι το πολύ ίσος με* n *και οι παράγοντες αυτοί δεν διαιρούν το* $(n!)i + 1$.

Τώρα, αν το πλήθος των πρώτων αριθμών ήταν m, παίρνοντας $n = m+1$, το παραπάνω σχόλιο συνεπάγεται ότι οι $m+1$ ακέραιοι $(m+1)! + 1 (1 \leq i \leq m+1)$ είναι ανά δύο πρώτοι μεταξύ τους. Έτσι, υπάρχουν τουλάχιστον $(m+1)$ διαφορετικοί πρώτοι. Άτοπο. □

Επίσης, σε αυτή την κατηγορία ανήκουν και οι επόμενες δύο:

9η απόδειξη(Filip Saidak [5])

Έστω n φυσικός αριθμός μεγαλύτερος του 1. Οι αριθμοί n και $n+1$ δεν έχουν κοινό παράγοντα, γιατί αν είχαν θα ήταν παράγοντας και της διαφοράς τους $(n+1-n=1)$, δηλαδή θα υπήρχε πρώτος που θα διαιρούσε το 1. Άτοπο. Επομένως, ο αριθμός $N_2 := n(n+1)$ έχει τουλάχιστον δυο διαφορετικούς μεταξύ τους πρώτους παράγοντες. Όμοια, και οι φυσικοί αριθμοί $n(n+1)$ και $n(n+1)+1$ δεν έχουν κοινό πρώτο παράγοντα. Επομένως, ο $N_3 = n(n+1)[n(n+1)+1]$ θα έχει τουλάχιστον τρεις διαφορετικούς μεταξύ τους πρώτους παράγοντες. Η διαδικασία αυτή μπορεί να συνεχιστεί επ΄ άπειρον, δηλαδή το πλήθος των πρώτων είναι άπειρο. □

10η απόδειξη
Μία μέθοδος για την απόδειξη της απειρίας των πρώτων είναι η εξής:
Έστω $a_1 < a_2 < a_3 < \cdots$ μία ακολουθία θετικών ακεραίων με την ιδιότητα

$$Αν\ M.K.Δ.(i,j) = 1\ τότε\ M.K.Δ.(a_i, a_j) = 1$$

Επιπλέον υποθέτουμε ότι για κάποιο πρώτο p ο ακέραιος a_p έχει τουλάχιστον δυο διαφορετικούς πρώτους παράγοντες. Τότε αν $p_1, p_2, \cdots, p_k$ είναι όλοι οι πρώτοι, ο ακέραιος $a_{p_1} a_{p_2} \cdots a_{p_k}$ θα έχει τουλάχιστον $k+1$ πρώτους παράγοντες. Πράγματι, κάθε παράγοντας είναι μεγαλύτερος από 1, οι παράγοντες είναι ανά δύο πρώτοι μεταξύ τους και κάποιος από αυτούς διαιρείται από δύο διαφορετικούς πρώτους. Άρα, υπάρχουν $k+1 > k$ πρώτοι. Άτοπο.
Μία τέτοια ακολουθία είναι η $a_n = 2^n - 1$. Είναι εύκολο να αποδειχθεί ότι
$(2^n - 1, 2^m - 1) = 2^{(n,m)} - 1$. Άρα, αν $(m,n) = 1$ τότε $(2^n - 1, 2^m - 1) = 1$. Επίσης, ο όρος $a_{11} = 23 \cdot 89$ διαιρείται από δύο διαφορετικούς πρώτους. □

Επιπλέον, η ύπαρξη άπειρων πρώτων συνεπάγεται από το ότι η ακολουθία $Fibonacci$ περιέχει μία μη πεπερασμένη αύξουσα υπακολουθία όρων τέτοια ώστε ανά δύο οι όροι της να είναι πρώτοι μεταξύ τους. Αυτό σημαίνει ότι το σύνολο των πρώτων διαιρετών της ακολουθίας $Fibonacci$ είναι άπειρο. Ας δούμε αναλυτικότερα αυτήν την απόδειξη, η οποία οφείλεται στον A.Rotkiewicz :

11η απόδειξη

Αν F_n είναι ο n-ιοστός όρος της ακολουθίας Fibonacci και αν m, n είναι θετικοί ακέραιοι, τότε από πρόταση 1.4.2 $(F_m, F_n) = F_{(m,n)}$. Αφού $F_1 = 1$, βλέπουμε ότι αν p_k είναι ο k-οστός διαδοχικός πρώτος, τότε κάθε δύο όροι της αύξουσας μη πεπερασμένης ακολουθίας $F_{p_1}, F_{p_2}, \cdots$ είναι πρώτοι μεταξύ τους , αφού $(F_{p_i}, F_{p_j}) = F_{(p_i,p_j)} = F_1 = 1$. Άρα, υπάρχει άπειρο πλήθος πρώτων αριθμών. □

2.1.4 Αποδείξεις που βασίζονται στην Αλγεβρική Θεωρία Αριθμών

Η απόδειξη του Larry Washington (1980) μέσω της αντιμεταθετικής άλγεβρας, βασίζεται στις περιοχές μονοσήμαντης ανάλυσης. Αρχικά, θα αναφέρουμε κάποια βασικά στοιχεία της Αλγεβρικής Θεωρίας Αριθμών που θα χρειαστούμε για την απόδειξη :

1. *Σε κάθε σώμα αριθμών (πεπερασμένου βαθμού) ο δακτύλιος των αλγεβρικών ακεραίων είναι μία περιοχή Dedekind : κάθε μη μηδενικό ιδεώδες είναι, κατά μοναδικό τρόπο, γινόμενο πρώτων ιδεωδών.*

2. *Σε κάθε σώμα αριθμών (πεπερασμένου βαθμού) υπάρχουν πεπερασμένου πλήθους πρώτα ιδεώδη που διαιρούν οποιοδήποτε δοσμένο πρώτο αριθμό p.*

3. *Μία περιοχή Dedekind με πεπερασμένου πλήθους πρώτα ιδεώδη είναι περιοχή κυρίων ιδεωδών. Έτσι κάθε μη μηδενικό στοιχείο του (εκτός τις μονάδες) αναλύεται μονοσήμαντα σε γινόμενο πρώτων στοιχείων.*

12η απόδειξη (του Larry Washington)

Θεωρούμε το σώμα όλων των αριθμών της μορφής $a+b\sqrt{-5}$ όπου $a, b \in \mathbb{Q}$. Ο δακτύλιος των αλγεβρικών ακεραίων αυτού του σώματος περιέχει αριθμούς της παραπάνω μορφής , με $a, b \in \mathbb{Z}$. Είναι εύκολο να δούμε ότι τα 2, 3, $1+\sqrt{-5}, 1-\sqrt{-5}$ είναι πρώτα στοιχεία του δακτυλίου αυτού, αφού δεν μπορούν να αναλυθούν σε παράγοντες που είναι αλγεβρικοί ακέραιοι εκτός αν ένας από τους παράγοντες είναι η μονάδα. Σημειώνουμε, επίσης, ότι $(1 - \sqrt{-5})(1 + \sqrt{-5}) = 2 \cdot 3$ η ανάλυση του 6 σε γινόμενο πρώτων δεν είναι μοναδική. Έτσι, ο δακτύλιος δεν είναι περιοχή ιδεωδών μονοσήμαντης ανάλυσης, άρα δεν είναι περιοχή κυρίων ιδεωδών. Έτσι, πρέπει να έχει άπειρα πρώτα ιδεώδη (από το στοιχείο 3 παραπάνω) και (από το στοιχείο 2 παραπάνω) εκεί υπάρχουν άπειροι στο πλήθος πρώτοι αριθμοί. □

Επίσης, μια , όχι και τόσο γνωστή, απόδειξη που ανήκει σε αυτήν την κατηγορία είναι η παρακάτω η οποία είναι βασισμένη στο Θεώρημα Lagrange και στους αριθμούς Mersenne .

13η απόδειξη

Έστω ότι το σύνολο των πρώτων $\mathbb{P}$ είναι πεπερασμένο κι ότι ο p είναι ο μεγαλύτερος πρώτος. Θεωρούμε τον αριθμό Mersenne 2^p-1 και θα δείξουμε ότι οποιοσδήποτε πρώτος παράγοντας του 2^p-1 είναι μεγαλύτερος από p. Έστω q να είναι ένας πρώτος διαιρέτης του 2^p-1 τότε $2^p \equiv 1 \pmod q$. Αφού p είναι πρώτος αυτό σημαίνει ότι το στοιχείο 2 έχει τάξη p στην πολλαπλασιαστική ομάδα $\mathbb{Z}_q^* = \mathbb{Z}_q \setminus \{0\}$ του σώματος $\mathbb{Z}_q$. Αυτή η ομάδα έχει $q-1$ στοιχεία. Από το θεώρημα Lagrange ξέρουμε ότι η τάξη κάθε στοιχείου διαιρεί την τάξη της ομάδας, δηλαδή $p \mid q-1$ και άρα $p < q-1 < q$. Άτοπο, αφού το p είναι ο μεγαλύτερος πρώτος. □

2.1.5 Αποδείξεις που βασίζονται σε επιχειρήματα υπολογισιμοτητας

Μερικές συνδυαστικές αποδείξεις περιέχουν απλά επιχειρήματα αριθμητικής. Τέτοιες αποδείξεις είναι του Perott (1881), του Thue (1897) και του Auric (1915), τις οποίες θα δούμε παρακάτω.

14η αποδειξη (του Perott)

$$\sum_{n=1}^{\infty} \frac{1}{n^2} < \sum_{n=1}^{\infty} \frac{1}{n(n+1)} = 1 + \sum_{n=1}^{\infty} \Big(\frac{1}{n} - \frac{1}{n+1}\Big) = 1 + 1 = 2$$

Υποθέτουμε ότι υπάρχουν ακριβώς r στο πλήθος πρώτοι αριθμοί οι $p_1, p_2, \ldots, p_r$ και έστω N ακέραιος τέτοιος ώστε $p_1 p_2 \cdots p_r < N$. Το πλήθος των ακεραίων $m \leq N$ που δεν διαιρούνται από ένα τετράγωνο είναι 2^r (είναι ο αριθμός όλων των πιθανών συνδυασμών από διαφορετικούς πρώτους), διότι κάθε ακέραιος είναι μονοσήμαντα γινόμενο πρώτων. Ο αριθμός των ακεραίων $m \leq N$ που διαιρούνται από p_i^2 είναι το πολύ $[N/p_i^2]$,έτσι ο αριθμός των ακεραίων $m \leq N$ που διαιρούνται από κάποιο τετράγωνο είναι το πολύ $\sum_{i=1}^{n}(N/p_i^2)$. Άρα,

$$N \leq 2^r + \sum_{i=1}^{r} \frac{N}{p_i^2} < 2^r + N(\sum_{i=1}^{\infty} \frac{1}{n^2} - 1) = 2^r + N(1-\delta)$$

, όπου $\delta > 0$ (αφού $\sum_{i=1}^{n} \frac{1}{n^2} - 1 < 1$). Επομένως, $N\delta < 2^r$. Διαλέγοντας N τέτοιο

ώστε $N\delta \geq 2^r$ έχουμε αντίφαση. □

15η απόδειξη (του Thue)

Έστω $n, k \geq 1$ ακέραιοι τέτοιοι ώστε $(1+n)^k < 2^n$ και έστω $p_1 = 2, p_2 = 3, \ldots p_r$ όλοι οι πρώτοι που ικανοποιούν τη σχέση $p_i \leq 2^n$ για $i = 1, 2, \ldots, r$. Υποθέτουμε ότι $r \leq k$. Κάθε ακέραιος m, με $1 \leq m \leq 2^n$ μπορεί να γραφεί με μοναδικό τρόπο στη μορφή:

$$m = 2^{e_1} \cdot 3^{e_2} \cdots p_r^{e_r},$$

όπου $0 \leq e_i \leq n$, για $i = 1, \ldots, r$.

Αν θέσουμε στους εκθέτες όλες τις τιμές των e_i για τα οποία ισχύει $0 \leq e_i \leq n$ τότε παίρνουμε όχι μόνο όλους τους φυσικούς αριθμούς που είναι μικρότεροι του 2^n αλλά παίρνουμε κι άλλους πολλούς μεγαλύτερους του 2^n. Δηλαδή , όλοι οι αριθμοί της παραπάνω μορφής δεν είναι όλοι μικρότεροι του 2^n. Για παράδειγμα, $n = 3, 2^3 = 8$ και $m = 2^{e_1}3^{e_2}5^{e_3}7^{e_4}$, αν $e_2 = 3$ τότε $3^3 \leq 8, 5^3 \leq 8, 7^3 \leq 8$. Οπότε $2^n \leq (n+1)n^r$.

Υπολογίζοντας, λοιπόν, όλες τις πιθανότητες, έπεται ότι: $2^n \leq (n+1)^r \leq (n+1)^k < 2^n$, άτοπο. Έτσι, $r \geq k+1$. Διαλέγουμε $n = 2k^2$. Από την $1 + 2k^2 < 2^{2k}$ για κάθε $k \geq 1$, έπεται ότι: $(1+2k^2)^k \leq 2^{2k^2} = 4k^2$. Άρα, υπάρχουν τουλάχιστον $k+1$ πρώτοι p τέτοιοι ώστε $p < 4^{k^2}$. Αφού το k μπορεί να είναι αυθαίρετα μεγάλο, υπάρχουν άπειροι στο πλήθος πρώτοι. □

16η απόδειξη (του Auric (1915))

Υποθέτουμε ότι υπάρχουν r στο πλήθος πρώτοι, $p_1 < p_2 < \ldots < p_r$. Έστω $t \geq 1$ ένας ακέραιος και $N = p_r^t$. Από την μονοσήμαντη ανάλυση σε πρώτους παράγοντες έχουμε ότι κάθε ακέραιος m, με $1 \leq m \leq N$ γράφεται $m = p_1^{f_1}p_2^{f_2}\cdots p_r^{f_r}$ και η ακολουθία $(f_1, f_2, \ldots, f_r)$ με κάθε $f_i \geq 0$ είναι μοναδικά ορισμένη. Επίσης, $p_1^{f_i} \leq p_i^{f_i} \leq m \leq N = p_r^t$. Τότε για $i = 1, 2, \ldots, r$ έχουμε $f_i \leq tE$, όπου $E = (\log p_r)/(\log p_1)$. Άρα, ο αριθμός N είναι ο αριθμός που αντιστοιχεί στην ακολουθία $(f_1, f_2, \ldots, f_r)$. Οπότε $p_r^t = N < (tE+1)^r < t^r(E+1)^r$. Αν το t είναι αυθαίρετα μεγάλο, η ανισότητα δεν ισχύει κι αυτό μας δείχνει ότι το πλήθος των πρώτων πρέπει να είναι άπειρο. □

2.1.6 Η τοπολογική απόδειξη του Furstenberg

Σε αυτήν την κατηγορία θα δούμε την απόδειξη του Furstenberg και μια παραλλαγή της.

Ορισμός 2.1.1. *Έστω X ένα σύνολο $X \neq \emptyset$. Αν $\tau \subseteq \mathcal{P}(X)$ τέτοιο ώστε:*

1. *Το $\emptyset$ και το $X \in \tau$*

2. *Αν $O_{i,i\in I}$ είναι μία οποιαδήποτε οικογένεια στοιχείων του τ τότε και η ένωση $\bigcup_{i\in I} O_i \in \tau$.*

3. *Κάθε πεπερασμένη τομή στοιχείων του τ, ανήκει επίσης στο τ.*
Τότε το ζευγάρι (X,τ) λέγεται τοπολογικός χώρος.

Τα στοιχεία του τ λέγονται ανοιχτά σύνολα του τοπολογικού χώρου.

17η απόδειξη (του Furstenberg 1955)

Θεωρούμε την ακόλουθη τοπολογία στο σύνολο $\mathbb{Z}$ των ακεραίων Για κάθε $a,b \in \mathbb{Z}, b>0$ θέτουμε

$$N_{a,b} = \{a+nb : n \in \mathbb{Z}\}$$

Κάθε σύνολο $N_{a,b}$, είναι μια άπειρη αριθμητική πρόοδος που εκτείνεται και στους θετικούς και στους αρνητικούς ακεραίους. Καλούμε ένα σύνολο $O \subseteq \mathbb{Z}$ ανοικτό αν είτε το O είναι κενό, ή αν για κάθε $a \in O$ υπάρχει κάποιο $b>0$ με $N_{a,b} \subseteq O$. Έστω $(O_i)_{i\in}$ οικογένεια ανοικτών συνόλων.Θα δείξω ότι $bigcup_{i\in I} O_i$ είναι ανοικτό σύνολο. Πράγματι, $\forall a \in \bigcup_{i\in I} O_i \; \exists\, i \in I$ τέτοιο ώστε $a \in O_i$. Αφού O_i ανοικτό συνεπάγεται ότι υπάρχει $b>0$ τέτοιο ώστε $N_{a,b} \subseteq O_i \subseteq \bigcup_{i\in I} O_i$. Άρα, $\bigcup_{i\in I} O_i$ ανοικτό. Δηλαδή, η ένωση οποιασδήποτε οικογένειας ανοικτών συνόλων του είναι επίσης ανοικτό σύνολο του .

Αν O_1, O_2 είναι ανοικτά και $a \in O_1 \cap O_2$ με $N_{a,b_1} \subseteq O_1$ και $N_{a,b_2} \subseteq O_2$, τότε $a \in N_{a,b_1 b_2} \subseteq O_1 \cap O_2$. Έτσι καταλήγουμε ότι κάθε πεπερασμένη τομή ανοικτών συνόλων είναι ανοικτό σύνολο.
Έτσι αυτή η οικογένεια ανοικτών συνόλων επάγει μια καλώς ορισμένη τοπολογία στο $\mathbb{Z}$. Εδώ σημειώνουμε δύο δεδομένα:
(A) Ένα μη κενό ανοικτό σύνολο είναι άπειρο.
(B) Κάθε σύνολο $N_{a,b}$ είναι κλειστό.
Πράγματι, το (A) έπεται από τον ορισμό. Για το (B) παρατηρούμε ότι

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$$

το οποίο αποδεικνύει ότι το $N_{a,b}$ είναι συμπλήρωμα ενός ανοικτού συνόλου και άρα κλειστό. Αφού τώρα, κάθε ακέραιος αριθμός $n \neq \pm 1$ έχει έναν πρώτο διαιρέτη p και άρα περιέχεται στο $N_{0,p}$ καταλήγουμε ότι

$$\mathbb{Z} \setminus \{1,-1\} = \bigcup_{p\in\mathbb{P}} N_{0,p}$$

Τώρα αν το $\mathbb{P}$ ήταν πεπερασμένο, τότε η $\bigcup_{p\in\mathbb{P}} N_{0,p}$ θα ήταν μία πεπερασμένη ένωση κλειστών συνόλων (από το (B)) και άρα κλειστό. Συνεπώς, το σύνολο {1,-1} θα ήταν

ανοικτό κατά παράβαση του (A). □

Ως μικρή παραλλαγή της $17^{ης}$ *απόδειξης αναφέρεται και η*

18η απόδειξη

Έστω το σύνολο $A = \bigcup A_p$, *όπου το* A_p *έχει ως στοιχεία του όλα τα πολλαπλάσια του* p *και το* p *τρέχει στο σύνολο των πρώτων* ≥ 2. *Οι μόνοι αριθμοί που δεν ανήκουν στο A είναι οι -1 και 1 και αφού το σύνολο {-1,1} είναι ξεκάθαρα ένα μη ανοιχτό σύνολο, το A δεν μπορεί να είναι κλειστό. Άρα, το A δεν είναι μια πεπερασμένη ένωση κλειστών συνόλων, που αποδεικνύει ότι υπάρχει μία απειρία πρώτων.* □

2.1.7 Η απόδειξη του Euler και αποδείξεις που βασίζονται σε αυτήν

19η απόδειξη (Euler)

Έστω ότι υπάρχουν πεπερασμένου πλήθους πρώτοι, οι $p_1, \cdots, p_r$. *Θεωρούμε το γινόμενο:*

$$X = \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right)^{-1}$$

Το γινόμενο είναι πεπερασμένο αφού υπάρχουν μόνο πεπερασμένου πλήθους πρώτοι. Τώρα αναπτύσσουμε κάθε παράγοντα σε μία συγκλίνουσα γεωμετρική σειρά:

$$\frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots .$$

Για οποιοδήποτε σταθερό K, *συμπεραίνουμε ότι:*

$$\frac{1}{1 - \frac{1}{p}} \geq 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots + \frac{1}{p^K}.$$

Επομένως, ισχύει:

$$\begin{aligned} X &\geq \left(1+\frac{1}{2}+\frac{1}{2^2}+\cdots+\frac{1}{2^K}\right)\cdot\left(1+\frac{1}{3}+\frac{1}{3^2}+\cdots+\frac{1}{3^K}\right) \\ &\quad \cdot\left(1+\frac{1}{5}+\frac{1}{5^2}+\cdots+\frac{1}{5^K}\right)\cdots\left(1+\frac{1}{p_r}+\frac{1}{{p_r}^2}+\cdots+\frac{1}{{p_r}^K}\right) \\ &= 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots \\ &= \sum_{n\in\mathcal{N}(K)}\frac{1}{n}, \end{aligned} \tag{2.1}$$

(2.2)

όπου

$$\mathcal{N}(K)=\{n\in\mathbb{N}|n={p_1}^{e_1}\cdots{p_r}^{e_r}, e_i\leq K\ \forall\ i\}$$

είναι το σύνολο όλων των φυσικών αριθμών με την ιδιότητα ότι κάθε πρώτος παράγοντας δεν εμφανίζεται παραπάνω από K φορές. Σημειώνουμε ότι η σχέση (2.1) απαιτεί το Θεμελιώδες Θεώρημα της Αριθμητικής. Για κάθε δοσμένο αριθμό $n\in\mathbb{N}$, αν το K είναι αρκετά μεγάλο, τότε $n\in\mathcal{N}(K)$, έτσι συμπεραίνουμε ότι

$$X\geq\sum_{n=1}^{\infty}\frac{1}{n}.$$

Η σειρά στο δεξί μέλος (ως αρμονική) αποκλίνει στο άπειρο, ενώ το X είναι πεπερασμένο. Οπότε καταλήξαμε σε άτοπο. Συνεπώς υπάρχουν άπειροι στο πλήθος πρώτοι αριθμοί. □

Η παρακάτω απόδειξη βασίζεται στην απόδειξη του Euler .

20η απόδειξη (Erdós)

Έστω $p_1,p_2,p_3,\ldots$ η ακολουθία πρώτων αριθμών σε αύξουσα σειρά και υποθέτουμε ότι η σειρά $\sum_{p_i\in\mathbb{P}}\frac{1}{p_i}$ συγκλίνει. Τότε πρέπει να υπάρχει ένας φυσικός αριθμός k τέτοιος ώστε $\sum_{i\geq k+1}\frac{1}{p_i}<\frac{1}{2}$. Ας ονομάσουμε τους $p_1,p_2,\ldots,p_k$ μικρούς πρώτους και τους $p_{k+1},p_{k+2},\ldots$ μεγάλους πρώτους. Για κάθε $N\in\mathbb{N}$ έχουμε:

$$\sum_{i\geq k+1}\frac{N}{p_i}<\frac{N}{2} \tag{1}$$

Έστω N_b να είναι το πλήθος των θετικών ακεραίων $n\leq N$, οι οποίοι διαιρούνται τουλάχιστον από ένα μεγάλο πρώτο και N_s το πλήθος των θετικών ακέραιων $n\leq N$

οι οποίοι διαιρούνται μόνο από μικρούς πρώτους. Προφανώς, $N_b + N_s = N$. *Εμείς θα δείξουμε ότι για κατάλληλο* N *έχουμε* $N_b + N_s < N$ *και έτσι θα καταλήξουμε σε άτοπο.*

Για να εκτιμήσουμε το N_b *σημειώνουμε ότι το* $\left[\frac{N}{p_i}\right]$ *μετράει το πλήθος των θετικών ακεραίων* N *οι οποίοι είναι πολλαπλάσια του* p_i. *Άρα, από την (1):*

$$N_b \leq \sum_{i+1} \left[\frac{N}{p_i}\right] < \frac{N}{2} \tag{2}$$

Ας κοιτάξουμε τώρα το N_s. *Γράφουμε κάθε* $n \leq N$ *, που έχει μόνο μικρούς πρώτους διαιρέτες στη μορφή* $n = a_n \cdot b_n^2$, *όπου* a_n *είναι το ελεύθερο από τετράγωνα μέρος. Κάθε* a_n *είναι ένα γινόμενο διαφορετικών μικρών πρώτων και συμπεραίνουμε ότι υπάρχουν ακριβώς* 2^k *διαφορετικά μέρη ελεύθερα τετραγώνων. Επιπλέον, αφού* $b_n^2 \leq a_n b_n^2 = n \Rightarrow b_n \leq \sqrt{n} \leq \sqrt{N}$ *βρίσκουμε ότι υπάρχουν το πολύ* $\sqrt{N}$ *μέρη στο τετράγωνο, και έτσι* $N_s \leq 2^k\sqrt{N}$. *Αφού η (2) ισχύει για κάθε* N, *μένει να βρούμε ένα* N *ώστε* $2^k\sqrt{N} \leq \frac{N}{2}$ *ή* $2^{k+1} \leq \sqrt{N}$ *και ένα τέτοιο* N *είναι το* $N = 2^{2k+2}$. $\square$

Κεφάλαιο 3

Το Θεώρημα του Dirichlet

3.1 Εισαγωγικά παραδείγματα

Πρόταση 3.1.1. *Υπάρχουν άπειροι πρώτοι της μορφής* $4m+1, m \in \mathbb{N}$.

Απόδειξη. Αν $n \in \mathbb{N}, n \geq 1$ ορίζουμε τον $N := (n!)^2 + 1$. Ο N είναι φυσικός μεγαλύτερος του 1, οπότε θα έχει κάποιον πρώτο διαιρέτη p, $p \mid N$. Ο p είναι μεγαλύτερος από τον n , διότι αν $p \leq n$ θα είχαμε $p \mid N$ και $p \mid n!$, δηλαδή $p \mid 1$. Άτοπο!

Αφού $p \mid N$ έπεται ότι $(n!)^2 \equiv -1 \pmod{p}$. Αυτό σημαίνει ότι η ισοτιμία $x^2 \equiv -1 \pmod{p}$ έχει λύση, δηλαδή ισχύει $\left(\frac{-1}{p}\right) = 1$, που σημαίνει ότι $p \equiv 1 \pmod{4}$.

Έχουμε αποδείξει ότι για κάθε φυσικό n υπάρχει πρώτος p, $p > n$ με $p \equiv 1 \pmod{4}$. Συνεπώς υπάρχουν άπειροι πρώτοι της μορφής $4m+1$. □

Πρόταση 3.1.2. *Υπάρχουν άπειροι πρώτοι της μορφής* $4n+3, n \in \mathbb{N}$.

Απόδειξη. Έστω ότι υπάρχουν πεπερασμένου πλήθους πρώτοι της μορφής $4n+3$ και έστω ότι αυτοί είναι $p_1, p_2, \cdots, p_k$. Θεωρούμε τον αριθμό $N = 4p_1 \cdots p_k - 1$. Ο N είναι μεγαλύτερος του 1 οπότε γράφεται ως γινόμενο πρώτων. Ο N είναι περιττός, οπότε ο 2 δεν είναι πρώτος παράγων του N. Άρα, κάθε πρώτος παράγων του N είναι είτε της μορφής $4n+1$ είτε της μορφής $4n+3$. Αν καθένας από τους πρώτους παράγοντες του N είναι της μορφής $4n+1$, τότε και ο N ως γινόμενο πρώτων της μορφής $4n+1$ θα ήταν επίσης της μορφής $4n+1$. Αυτό, όμως, είναι άτοπο, διότι $N = 4(p_1 \cdots p_k - 1) + 3$. Άρα, ένας τουλάχιστον πρώτος διαιρέτης του N είναι της μορφής $4n+3$. Αυτός ο διαιρέτης πρέπει να είναι ένας από τους $p_1, \cdots, p_k$ έστω ότι είναι ο p_i οπότε $p_i \mid N, p_i \mid 4p_1 \cdots p_k$, άρα $p_i \mid 4p_1 \cdots p_k - N = 1$ και καταλήγουμε σε άτοπο. □

Παρατήρηση. *Όλοι οι πρώτοι $p > 3$ είναι της μορφής $6n+1$ ή $6n+5, n \in \mathbb{Z}$. Ας δούμε γιατί ισχύει αυτό. Κάθε φυσικός αριθμός είναι είτε της μορφής $6n$ είτε της μορφής $6n+1$ είτε της μορφής $6n+2$ είτε της μορφής $6n+3$ είτε της μορφής $6n+4$ είτε της μορφής $6n+5$. Τώρα, ένας πρώτος δεν μπορεί να είναι της μορφής $6n$, διότι δεν είναι πολλαπλάσιο του 6. Αν ένας πρώτος είναι της μορφής $6n+2$ τότε είναι πολλαπλάσιο του 2, οπότε είναι ο 2. Αν ένας πρώτος είναι της μορφής $6n+3$, τότε είναι πολλαπλάσιο του 3, άρα είναι ο 3. Τέλος, αν ένας πρώτος είναι της μορφής $6n+4$, τότε είναι πολλαπλάσιο του 2 , οπότε είναι ο 2 και έχουμε άτοπο διότι ο 2 δεν είναι της μορφής $6n+4$. Το συμπέρασμα είναι ότι ένας πρώτος μεγαλύτερος του 3 είναι είτε της μορφής $6n+1$ είτε της μορφής $6n+5$.*

Πρόταση 3.1.3. *Υπάρχουν άπειροι πρώτοι της μορφής $6n+5, n \in \mathbb{N}$.*

Απόδειξη. Ας υποθέσουμε ότι υπάρχουν πεπερασμένου πλήθους πρώτοι της μορφής $6n+5$ και ας υποθέσουμε ότι όλοι οι πρώτοι της μορφής $6n+5$ είναι οι $p_1, \cdots, p_m$. Θεωρούμε τον αριθμό $N := 6p_1p_2\cdots p_m - 1$. Παραδείγματα πρώτων της μορφής $6n+5$ είναι οι 5, 11, 17. Άρα $N > 1$, οπότε ο N έχει τουλάχιστον έναν πρώτο παράγοντα. Έστω, λοιπόν, p ένας πρώτος παράγων του N. Αν ο p είναι ένας από τους $2, 3, p_1, \cdots, p_m$ τότε $p \mid N, p \mid 6p_1\cdots p_m \Rightarrow p \mid 1$, το οποίο είναι αδύνατο. Άρα, ο p είναι πρώτος μεγαλύτερος του 3 και διαφορετικός από όλους τους πρώτους της μορφής $6n+5$. Βάσει της αμέσως προηγούμενης πρότασης ο p είναι της μορφής $6n+1$. Δείξαμε, λοιπόν, ότι κάθε πρώτος παράγων του N είναι της μορφής $6n+1$ και επειδή ο N είναι ίσος με το γινόμενο των πρώτων παραγόντων του, συμπεραίνουμε ότι ο N είναι ίσος με το γινόμενο αριθμών της μορφής $6n+1$. Όμως, αυτό συνεπάγεται ότι ο N είναι της μορφής $6n+1$. Πράγματι το γινόμενο δυο αριθμών της μορφής $6n+1$ είναι της μορφής $6n+1$ διότι $(6n'+1)(6n''+1) = 6(6n'n''+n'+n'')+1 = 6n+1$. Αυτό επεκτείνεται με επαγωγή για το γινόμενο περισσότερων των δύο αριθμών. Όμως το ότι το N είναι της μορφής $6n+1$ είναι άτοπο, αφού ο N είναι της μορφής $N = 6(p_1\cdots p_m - 1) + 5 = 6n+5$. □

Πρόταση 3.1.4. *Υπάρχουν άπειροι πρώτοι της μορφής $6k+1, k \in \mathbb{N}$.*

Απόδειξη. Έστω P το πεπερασμένο σύνολο των πρώτων της μορφής $6k+1$, δηλαδή $P = \{p_1, p_2, \cdots, p_n\}$. Θεωρούμε τον φυσικό αριθμό $N = 6p_1p_2\cdots p_n$. Είναι φανερό ότι N διαιρείται από όλους τους πρώτους αριθμούς που ανήκουν στο P. Έστω p ένας πρώτος διαιρέτης του $N^2 - N + 1$. Σημειώνουμε ότι $(N^2 - N + 1)(N + 1) = N^3 + 1$, έτσι ο p διαιρεί το $N^3 + 1$, δηλαδή $N^3 \equiv -1 \pmod p$ και έτσι $N^6 \equiv 1 \pmod p$. Υπενθυμίζουμε ότι η τάξη του $N \bmod p$ είναι ο ελάχιστος θετικός k, έτσι ώστε $N^k \equiv 1 \pmod p$. Η τάξη πρέπει να διαιρεί το 6, έτσι $k = 1, 2, 3$ ή 6. Αλλά $N^3 \equiv -1 \pmod p$, έτσι η τάξη δεν μπορεί να είναι 3 ούτε 1. Μπορεί η τάξη να είναι 2; Αν $N^2 \equiv 1 \pmod p$ και $N^3 \equiv -1 \pmod p$ τότε $N \equiv -1 \pmod p$. Αλλά τότε ο p θα διαιρούσε και το $N+1$ και το $N^2 - N + 1$, όμως Μ.Κ.Δ. $(N+1, N^2 - N + 1) =$ Μ.Κ.Δ.$(N+1, N(N+1) - 2N + 1) =$ Μ.Κ.Δ$(N+1, -2(N+1) + 3) =$

Μ.Κ.Δ. $(N+1,3) < p$, άτοπο. Άρα, το N έχει τάξη 6 $(\mathrm{mod}\ p)$ και η ομάδα των μονάδων $modp$ έχει τάξη $p-1$, έτσι το 6 διαιρεί το $p-1$ το οποίο σημαίνει ότι το p έχει τη μορφή $6k+1$. Άρα, το σύνολο P δεν περιέχει όλους τους πρώτους της μορφής $6k+1$. Έτσι, το σύνολο των πρώτων αυτής της μορφής είναι άπειρο. □

Θεώρημα 3.1.1. *Αν $n > 1$ υπάρχει άπειρο πλήθος πρώτων p τέτοιο ώστε* $p \equiv 1 \pmod{n}$.

Για την απόδειξη θα χρειαστούμε το ακόλουθο

Λήμμα 3.1.1. *Έστω $a \in \mathbb{Z}$ και $p \in \mathbb{P}$. Αν $n \in \mathbb{N}$ τέτοιος ώστε $p \nmid n$, τότε οι ακόλουθες προτάσεις είναι μεταξύ τους ισοδύναμες.*
(i) $\Phi_n(a) \equiv 0 \pmod{p}$
(ii) n είναι η τάξη της κλάσης a .

Απόδειξη. Ας υποθέσουμε ότι ο a είναι ρίζα του πολυωνύμου $\Phi_n(X) mod p$. Από τη σχέση $X^n - 1 = \prod_{d|n} \Phi_d(X)$ έχουμε ότι $\bar{a}^n = [a]^n = 1 \in \mathbb{Z}/p\mathbb{Z}$. Επομένως, $ord(\bar{a}) \mid n$. Αν η τάξη της κλάσης $k := a \pmod{p}$ ήταν $k < n$ τότε από την $X^k - 1 = \prod_{d|k} \Phi_d(X)$ θα είχαμε ότι το a θα ήταν ρίζα $modp$ και ενός ακόμη κυκλοτομικού πολυωνύμου $\Phi_{d_0}(X)$, με $d_0 \mid n, d_0 \neq n$. Έστω $g(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ ο Μ.Κ.Δ.$(\Phi_{d_0}(X), \Phi_n(X))$, όπου τα πολυώνυμα $\Phi_{d_0}(X)$ και $\Phi_n(X)$ τα θεωρούμε ως πολυώνυμα με συντελεστές από το $\mathbb{Z}/p\mathbb{Z}$. Ως γνωστό το πολυώνυμο $g(X) = f_1(X)\Phi_{d_0}(X) + f_2(X)\Phi_n(X)$ όπου $f_i(X) \in \mathbb{Z}/p\mathbb{Z}[X]$. Επομένως, το $g(X)$ έχει σαν ρίζα του την $\bar{a} := amodp$. Αυτό σημαίνει ότι $g(X) \not\equiv 0$. Επομένως, στην ανάλυση του $X^n - 1$ στον $\mathbb{Z}/p\mathbb{Z}[X]$ εμφανίζεται τουλάχιστον ένας παράγοντας (ο $(x-\bar{a})$) με πολλαπλότητα > 1. Αυτό όμως είναι άτοπο επειδή το πολυώνυμο $X^n - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$ είναι διαχωρίσιμο. Επομένως, $n = ord(a \bmod p)$.

Αντίστροφα, έστω $n = ord(\bar{a}), \bar{a} := a \bmod p$, οπότε $\bar{a}^n - 1 = 0$ στο $F_p = \mathbb{Z}/p\mathbb{Z}$ και επομένως αφού $X^n - 1 = \prod_{d|n} \Phi_d(X)$, έπεται ότι το a είναι ρίζα ενός πολυωνύμου $\Phi_d(X) \bmod p$ για κάποιο $d \mid n$. Αν ίσχυε $\Phi_d(\bar{a}) = 0$ για κάποιο $d \mid n, d < n$ θα είχαμε $\bar{a}^d - 1 = 0$, άτοπο αφού $ord(\bar{a}) = n$. Επομένως, κατ΄ ανάγκη, ισχύει $\Phi_n(\bar{a}) = 0$. □

Πόρισμα 3.1.1. *Αν $p \nmid n$ τότε οι ακόλουθες προτάσεις είναι μεταξύ τους ισοδύναμες.*
(i) $\Phi_n(a) \equiv 0 \pmod{p}$ *για κάποιο* $a \in \mathbb{Z}$.
(ii) $p \equiv 1 \pmod{n}$

Απόδειξη. Αν το a είναι ρίζα του $\Phi_n(X) \bmod p$ τότε από το Λήμμα 3.1.1 $ord(\bar{a}) = n$. Επομένως, $n \mid (p-1)$, δηλαδή $p \equiv 1 \pmod{n}$.

Αντίστροφα, αν $p \equiv 1 \pmod{n}$. Είναι γνωστό ότι υπάρχουν πρωταρχικές ρίζες $modp$, δηλαδή ένα τουλάχιστο στοιχείο $\bar{a} := a \pmod{p}$ τάξης n στην ομάδα $(\mathbb{Z}/p\mathbb{Z})^\star$. Σύμφωνα με το λήμμα έχουμε $\Phi_n(\bar{a}) = 0$, στο $(\mathbb{Z}/p\mathbb{Z})$.

□

Απόδειξη. (Θεωρήματος) Υποθέτουμε ότι υπάρχει μόνο πεπερασμένο πλήθος πρώτων τέτοιων ώστε $p \equiv 1 \pmod{n}$. Έστω P το γινόμενο αυτών. Έστω r αυθαίρετος φυσικός αριθμός
Ισχυρισμός: Ο αριθμός $\Phi_n(nrP)$ έχει μόνο πρώτους παράγοντες της μορφής $1 \pmod{n}$.
Δεχόμαστε προς το παρόν, τον ισχυρισμό και έχουμε : το $\Phi_n(X)$ είναι ένα μονικό πολυώνυμο, επομένως $\Phi_n(rnP) \to \infty$, όταν $r \to \infty$. Ιδιαίτερα, ισχύει $\Phi_n(rnP) > 1$ για αρκετά μεγάλο r. Αν τώρα $p \in \mathbb{P}$ τέτοιο ώστε $p \mid \Phi_n(rnP)$ τότε (ισχυρισμός) $p \equiv 1 \pmod{n}$. Επομένως $p \mid P$. Συνεπώς ο p διαιρεί και τον σταθερό όρο του πολυωνύμου $\Phi_n(X)$. Επειδή όμως η σταθερά αυτή είναι ± 1 καταλήξαμε σε άτοπο. □

Απόδειξη. (Ισχυρισμού). Έστω $p \mid \Phi_n(nrP)$ τότε ο αριθμός (nrP) είναι ρίζα του $\Phi_n(X) \bmod p$.
Αν $p \not\equiv 1 \pmod{n}$ από πόρισμα θα είχαμε $p \mid n$. Ο σταθερός όρος του $\Phi_n(X)$ είναι $\prod_{\substack{\zeta^n=1 \\ \zeta \text{πρωταρχική}}} (-\zeta)$ και συνεπώς μία ρίζα της μονάδος. Όμως, ως γνωστό $\Phi_n(X) \in \mathbb{Z}[X]$ άρα ο σταθερός όρος $\in \mathbb{Z}$ και συνεπώς είναι ± 1. Επειδή $p \mid n$, έπεται ότι
$\Phi_n(nrP) \equiv \pm 1 \pmod{p}$, άτοπο αφού (nrP)-ρίζα του $\Phi_n \pmod{p}$.

□

3.2 Χαρακτήρες πεπερασμένων αβελιανών ομάδων

Ορισμός 3.2.1. . *Έστω G μια πεπερασμένη αβελιανή ομάδα. Κάθε ομομορφισμός ομάδων*

$$\chi : G \to \mathbb{C}^*$$

θα λέγεται χαρακτήρας της G.

Το γινόμενο δύο χαρακτήρων χ και χ' της G ορίζεται ως εξής:

$$(\chi \cdot \chi')(g) := \chi(g)\chi'(g) \quad \text{για κάθε στοιχείο } g \text{ της } G$$

Ο ομομορφισμός $\chi_0(g) = 1$ για κάθε $g \in G$ επαληθεύει την ιδιότητα
$(\chi \cdot \chi_0)(g) = (\chi_0 \cdot \chi)(g) = \chi(g)$ *για κάθε $g \in G$ και κάθε χαρακτήρα χ της G.*
Ο αντίστροφος ενός χαρακτήρα χ της ομάδας G ορίζεται

$$\chi^{-1}(g) := \chi(g)^{-1} \quad \text{για κάθε στοιχείο } g \text{ της } G$$

Θεωρούμε το σύνολο

$$\widehat{G} = \{\chi / \chi \text{ χαρακτήρας της } G\}$$

.

Προφανώς το σύνολο $\widehat{G}$ αποτελεί ομάδα με πράξη τον πολλαπλασιασμό των χαρακτήρων. Ισχύει ότι αν G πεπερασμένη αβελιανή ομάδα, τότε η ομάδα $\hat{G}$ των χαρακτήρων της G είναι ισόμορφη με την ομάδα G. Συνεπώς, η τάξη της $\hat{G}$ είναι ίση με την τάξη της G.

Παρατήρηση: *Αν G πεπερασμένη τότε $\chi(g)$ είναι ρίζα της μονάδας, δηλαδή για κάθε $g \in G$ έχουμε ότι $|\chi(g)| = 1 \Rightarrow \chi(g)\overline{\chi(g)} = 1$, οπότε μπορούμε να ορίσουμε τον συζυγή χαρακτήρα $\overline{\chi}$ του χ ως εξής:*

$$\overline{\chi}(g) := \overline{\chi(g)}\ \forall g \in G.$$

Ορισμός 3.2.2. . *Έστω $N > 2$. Κάθε χαρακτήρας της $\mathbb{Z}_N^* = \{n \pmod N | (n, N) = 1\}$ θα λέγεται χαρακτήρας Dirichlet mod N .*

Από τον ορισμό έχουμε ότι ο χ ορίζεται μόνο στα n για τα οποία ισχύει $(n, N) = 1$. Επεκτείνουμε λοιπόν τον ορισμό ως εξής:

$$\chi(n) := \begin{cases} \chi(n \pmod N), & \text{όταν } (n, N) = 1 \\ 0, & \text{όταν } (n, N) > 1 \end{cases}$$

και θα το ονομάζουμε και πάλι χαρακτήρα του Dirichlet .

Ο κύριος χαρακτήρας $\bmod N$ ορίζεται ως εξής:

$$\chi_0(n) := \begin{cases} 1, & \text{όταν } (n, N) = 1 \\ 0, & \text{όταν } (n, N) > 1 \end{cases}$$

Ώστε χαρακτήρας του Dirichlet mod N είναι μια συνάρτηση $\chi : \mathbb{Z} \to \mathbb{C}$ με τις εξής ιδιότητες:

1. $\chi(n) = 0 \iff (n, N) > 1$
2. *χ πλήρως πολλαπλασιαστική, δηλαδή $\chi(mn) = \chi(m)\chi(n)\ \forall m, n \in \mathbb{Z}$*
3. *$\chi(n)$ εξαρτάται μόνο από την κλάση του $(n \bmod N)$*

Ως γνωστό η τάξη της πολλαπλασιαστικής ομάδας $\mathbb{Z}_N^*$ είναι

$$\varphi(N) = N \prod_{p|N} \Big(1 - \frac{1}{p}\Big).$$

Επομένως και η τάξη της ομάδας των χαρακτήρων Dirichlet $\pmod N$ είναι επίσης $\varphi(N)$.

Παραδείγματα.

1. *Για* $N = 2$ *έχουμε* $\varphi(N) = 1$, *συνεπώς ο* χ_0 *είναι μοναδικός χαρακτήρας* mod2.

2. *Για* $N = 3, 4, 6$ *έχουμε ότι* $\varphi(N) = 2$ *οπότε υπάρχει ακόμη ένας εκτός του κύριου π.χ.*
   για $N = 3$

n	0	1	2	3	4	5	6	$\cdots$
$\varepsilon_3(n)$	0	1	-1	0	1	-1	0	$\cdots$

   για $N = 4$

n	0	1	2	3	4	5	6	$\cdots$
$\varepsilon_4(n)$	0	1	0	-1	0	1	0	$\cdots$

3. *για* $N = 5$, $\varphi(N) = 5\Big(1 - \frac{1}{5}\Big) = 4$ *υπάρχουν ακόμα 3 χαρακτήρες έκτος από τον κύριο.*

$n \pmod 5$	0	1	2	3	4
	0	1	i	$-i$	-1
$\chi(n)$	0	1	-1	-1	1
	0	1	$-i$	i	-1

Θεώρημα 3.2.1. *Αν* χ *χαρακτήρας Dirichlet mod* N *τότε ισχύει η*

$$S := \sum_{n(\bmod N)} \chi(n) = \begin{cases} \varphi(N), & \text{για } \chi = \chi_0 \\ 0, & \text{για } \chi \neq \chi_0 \end{cases}$$

Απόδειξη. Αν $\chi = \chi_0$, προφανώς $S = \varphi(N)$. Αν $\chi \neq \chi_0$ τότε $\exists\, n_0 \pmod N, (n_0, N) = 1$, τέτοιο ώστε $\chi(n_0) \neq 1$. Όταν το n διατρέχει ένα πλήρες σύστημα αντιπροσώπων πρώτων κλάσεων υπολοίπων $modN$ το ίδιο κάνει και το nn_0 (δηλαδή $(n, N) = 1 \Leftrightarrow (nn_0, N) = 1$). Συνεπώς

$$S = \sum_{n(modN)} \chi(nn_0) = \chi(n_0)S$$

άρα επειδή $\chi(n_0) \neq 1$, έχουμε ότι $S = 0$. □

Πόρισμα 3.2.1. *Αν* χ_1, χ_2 *είναι χαρακτήρες Dirichlet mod* N *τότε*

$$\frac{1}{\varphi(N)} \sum_{n(modN)} \chi_1(n)\overline{\chi_2}(n) = \begin{cases} 1, & \text{όταν } \chi_1 = \chi_2 \\ 0, & \text{όταν } \chi_1 \neq \chi_2 \end{cases}$$

Απόδειξη. Εφαρμόζουμε το θεώρημα για τον χαρακτήρα $\chi := \chi_1\overline{\chi}_2$. □

Εάν τώρα αθροίσουμε ως προς τους χαρακτήρες, έχουμε το επόμενο θεώρημα.

Θεώρημα 3.2.2. *Για κάθε ακέραιο n ισχύει*

$$\sum_{\chi} \chi(n) = \begin{cases} \varphi(N), & \text{όταν } n \equiv 1 \pmod N \\ 0, & \text{όταν } n \not\equiv 1 \pmod N \end{cases}$$

όπου το χ στην άθροιση διατρέχει όλους τους χαρακτήρες Dirichlet mod N

Απόδειξη. Αν $n \equiv 1 \pmod N$ τότε για όλους τους χαρακτήρες Dirichlet mod N χ ισχύει ότι $\chi(n) = 1$.Το πλήθος αυτών είναι $\varphi(N)$. Επομένως, όταν $n \equiv 1 \pmod N$ έχουμε το ζητούμενο.
Αν τώρα $(n, N) > 1$ το θεώρημα ισχύει γιατί για όλους τους χαρακτήρες Dirichlet mod N θα ισχύει $\chi(n) = 0$. Έστω, λοιπόν, $n \not\equiv 1 \pmod N, (n, N) = 1$ και χ_1 ένας χαρακτήρας Dirichlet mod N τέτοιος ώστε $\chi_1(n) \neq 1$. Υπάρχει τέτοιος χαρακτήρας διότι οι χαρακτήρες χ με $\chi(n) = 1$ είναι χαρακτήρες της ομάδας πηλίκων $(\mathbb{Z}/N\mathbb{Z})^*/ < n >$ της οποίας η τάξη είναι μικρότερη της τάξης της $(\mathbb{Z}/N\mathbb{Z})^*$. Έχουμε λοιπόν:

$$(1 - \chi_1(n)) \sum_{\chi} \chi(n) = \sum_{\chi} [\chi(n) - (\chi_1\chi)(n)] = \sum_{\chi} \chi(n) - \sum_{\chi} \chi(n) = 0$$

Λόγω τη σχέσης $\chi_1(n) \neq 1$ έπεται ότι $\sum_\chi \chi(n) = 0$. □

Πόρισμα 3.2.2. *Αν $a, b \in \mathbb{Z}, (b, N) = 1$, τότε ισχύει:*

$$\frac{1}{\varphi(N)} \sum_{\chi} \chi(a)\overline{\chi}(b) = \begin{cases} 1, & \text{όταν } a \equiv b \pmod N \\ 0, & \text{όταν } a \not\equiv b \pmod N \end{cases}$$

Απόδειξη. Εφαρμόζουμε το θεώρημα για $n, nb \equiv a \pmod N$. Η ισοτιμία $bx \equiv a \pmod N$ έχει λύση αφού $(b, N) = 1$. □

Ενδιαφερόμαστε προπαντός για πραγματικούς χαρακτήρες ($\chi = \bar{\chi}$) δηλαδή τέτοιους που παίρνουν τιμές πραγματικούς αριθμούς. Επειδή οι τιμές τους είναι ρίζες της μονάδος ή μηδέν οι χαρακτήρες αυτοί παίρνουν τιμές $0, -1, +1$. Το επόμενο θεώρημα θα μας δώσει όλους τους πρωταρχικούς πραγματικούς χαρακτήρες. Πρώτα όμως δίνουμε τον παρακάτω ορισμό.

Ορισμός 3.2.3. *Έστω D ακέραιος. Ο D θα λέγεται θεμελιώδης διακρίνουσα όταν ισχύουν:*

- *ο* $D \equiv 1 \pmod 4$ *και δεν διαιρείται με το τετράγωνο ακεραίου μεγαλύτερου του ένα (square free), ή*

- *ο* $D \equiv 0 \pmod 4$, *ο* $\dfrac{D}{4}$ *είναι square free και* $\dfrac{D}{4} \equiv 2$ *ή* $3 \pmod 4$.

Έστω D *θεμελιώδης διακρίνουσα. Ορίζουμε τη συνάρτηση* $\chi_D : \mathbb{N} \to \mathbb{Z}$ *ως εξής:*

1. $\chi_D(p) = \left(\dfrac{D}{p}\right)$, *όπου* $p \in \mathbb{P} \setminus \{2\}$

2. $$\chi_D(2) = \begin{cases} 0, & \text{όταν } D \equiv 0 \pmod 4 \\ 1, & \text{όταν } D \equiv 1 \pmod 8 \\ -1, & \text{όταν } D \equiv 5 \pmod 8 \end{cases}$$

3. $\chi_D(p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}) = \chi_D(p_1)^{n_1} \chi_D(p_2)^{n_2} \cdots \chi_D(p_k)^{n_k}$

Ισχύει λοιπόν το ακόλουθο

Θεώρημα 3.2.3. *Έστω* D *θεμελιώδης διακρίνουσα. Η συνάρτηση*

$$n \mapsto \chi_D(n)$$

είναι περιοδική $\bmod |D|$ *και ορίζει έναν πρωταρχικό χαρακτήρα του Dirichlet* $\bmod |D|$, *όπου*

$$\chi_D(-1) = \begin{cases} 1, & \text{όταν } D > 0 \\ -1, & \text{όταν } D < 0 \end{cases}$$

Κάθε πρωταρχικός πραγματικός χαρακτήρας του Dirichlet είναι χαρακτήρας της μορφής χ_D.

3.3 Σειρές του Dirichlet (γενικά)

Οι σειρές του Dirichlet παίζουν στην αναλυτική θεωρία αριθμών, τόσο σημαντικό ρόλο όσο οι δυναμοσειρές στη θεωρία των μιγαδικών συναρτήσεων. Στη θεωρία των δυναμοσειρών παίρνει κανείς την συνάρτηση $z \mapsto z^n (n \in \mathbb{N})$ *και προσπαθεί οποιαδήποτε άλλη συνάρτηση να την παραστήσει σαν άπειρο γραμμικό συνδυασμό τέτοιων. Στις σειρές Dirichlet παίρνουμε την εκθετική συνάρτηση*

$$z \longmapsto e^{-\lambda z} (\lambda \in \mathbb{R})$$

και, αφού το $\mathbb{R}$ *είναι υπεραριθμήσιμο, περιοριζόμαστε σε μία ακολουθία*

$$\{z \to e^{-\lambda_n z}\}_{n \in \mathbb{N}}$$

όπου λ_n *ακολουθία πραγματικών αριθμών με* $\lambda_1 < \lambda_2 < \cdots < \lambda_n \to \infty$. *Η μιγαδική μεταβλητή θα συμβολίζεται με* $s = \sigma + it$, *όπου* $\sigma, t \in \mathbb{R}$.

Ορισμός 3.3.1. *Μια σειρά Dirichlet είναι μια σειρά της μορφής*

$$\sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$$

όπου $\{\lambda_n\}$ *είναι ακολουθία πραγματικών αριθμών με* $\lambda_1 < \lambda_2 < \cdots < \lambda_n \to \infty, a_n$ *αυθαίρετοι μιγαδικοί αριθμοί και* $s = \sigma + it \in \mathbb{C}$.

Παραδείγματα:

1. *Έστω* $\{\lambda_n = n\}$ *για κάθε φυσικό αριθμό* n. *Σε αυτήν την περίπτωση δεν οδηγούμαστε σε καμία καινούργια θεωρία διότι η αντικατάσταση* $z = e^{-s}$ *μας δίνει την μορφή* $\sum a_n z^n$ *δηλαδή σε αυτήν την περίπτωση, η θεωρία των σειρών Dirichlet ταυτίζεται με τη θεωρία των δυναμοσειρών.*

2. *Έστω* $\lambda_n = \log n$ *οπότε η σειρά γράφεται* $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$. *Με αυτή τη μορφή θα ασχοληθούμε παρακάτω. Από εδώ και πέρα θα τη λέμε συνήθη σειρά Dirichlet .*

Το πρώτο πρόβλημα που θα εξετάσουμε, είναι το πού και πότε συγκλίνει μία σειρά Dirichlet .
Για τις δυναμοσειρές γνωρίζουμε το θεώρημα του Abel ([3] σελίδα 38) σύμφωνα με το οποίο υπάρχει ένας μη αρνητικός πραγματικός αριθμός R*(η ακτίνα σύγκλισης της δυναμοσειράς) έτσι ώστε η δυναμοσειρά να συγκλίνει απόλυτα για κάθε* $z \in \mathbb{C}$ *με* $|z| < R$ *και να αποκλίνει για* $|z| > R$. *(Εννοείται ότι για* $R = 0$ *η σειρά αποκλίνει παντού, ενώ για* $R = \infty$ *συγκλίνει παντού.)*

Συγκεκριμένα, στο παράδειγμα (1) , για $\lambda_n = n$ *και* $z = e^{-s}$, *αν* R *είναι η ακτίνα σύγκλισης της δυναμοσειράς* $\sum_{n=1}^{\infty} a_n z^n$, *τότε αυτό συνεπάγεται την ύπαρξη ενός πραγματικού αριθμού* $\sigma_0 := \log\left(\frac{1}{R}\right)$ *έτσι ώστε η σειρά του Dirichlet* $\sum_{n=1}^{\infty} a_n e^{-ns}$ *να συγκλίνει για κάθε* $s = \sigma + it \in \mathbb{C}$ *με* $\sigma > \sigma_0$, *αποκλίνει για κάθε* $s \in \mathbb{C}$ *,με* $\sigma < \sigma_0$ *ενώ δεν μπορούμε να πούμε τίποτα για* $\sigma = \sigma_0$. *Σκοπός μας τώρα είναι να το αποδείξουμε για όλες τις σειρές του Dirichlet . Αν και η απόδειξη είναι ίδια στη γενική περίπτωση εμείς εδώ θα περιοριστούμε, από εδώ και κάτω, στις συνήθεις σειρές Dirichlet .*

Θεώρημα 3.3.1. *Αν η σειρά Dirichlet* $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *συγκλίνει για* $s = s_0$, *τότε συγκλίνει για όλα τα* s *με* $Re(s) > Re(s_0)$ *και μάλιστα ομοιόμορφα σε συμπαγή υποσύνολα του ημιεπιπέδου* $Re(s) > Re(s_0)$.

Απόδειξη. Θα αποδείξουμε κάτι γενικότερο, ότι δηλαδή σε κάθε τόπο της μορφής

$$\arg(s - s_0) \leq \frac{\pi}{2} - \theta < \frac{\pi}{2}$$

έχουμε ομοιόμορφη σύγκλιση, οπότε τελειώνουμε αφού κάθε συμπαγές υποσύνολο του ημιεπιπέδου $Re(s) > Re(s_0)$ περιέχεται σε κάποιο τέτοιο τόπο. Κατ΄ αρχήν, χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $s_0 = 0$.
$\Big(\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \sum_{n=1}^{\infty} \frac{a_n}{n^{s_0}} \cdot \frac{1}{n^{s-s_0}} = \sum_{n=1}^{\infty} \frac{b_n}{n^{s-s_0}}$ οπότε σύγκλιση της αρχικής σειράς για $s = s_0$ είναι ισοδύναμη με τη σύγκλιση της τελευταίας για $s - s_0 = 0\Big)$.
Αφού λοιπόν εξ υποθέσεως συγκλίνει για $s_0 = 0$, έχουμε ότι η σειρά $\sum_{n=1}^{\infty} a_n$ συγκλίνει, δηλαδή

$$\forall \varepsilon > 0 \quad \exists\, N_0 \in \mathbb{N} \text{ τέτοιος ώστε } A(M,N) \le \varepsilon \text{ για όλα τα } N > M \ge N_0$$

όπου

$$A(M,N) := \sum_{n=M}^{N} a_n, \quad A(N) := \sum_{n=1}^{N} a_n \quad \text{και} \quad A(M, M-1) := 0$$

Επομένως για $N > M \ge N_0$ ισχύει

$$\begin{aligned}
\sum_{n=M}^{N} a_n e^{-\lambda_n s} &= \sum_{n=M}^{N} \Big[A(M,n) - A(M,n-1) \Big] e^{-\lambda_n s} \\
&= A(M,M)e^{-\lambda_M s} - A(M,M)e^{-\lambda_{M+1} s} \\
&\quad + A(M,M+1)e^{-\lambda_{M+1} s} - A(M,M+1)e^{-\lambda_{M+2} s} \\
&\quad \vdots \\
&\quad + A(M,N-1)e^{-\lambda_{N-1} s} - A(M,N-1)e^{-\lambda_N s} \\
&\quad + A(M,N)e^{\lambda_N s} \\
&= \sum_{n=M}^{N-1} A(M,n) \Big[e^{-\lambda_n s} - e^{\lambda_{n+1} s} \Big] + A(M,N)e^{-\lambda_N s}.
\end{aligned}$$

Η παραπάνω διαδικασία είναι το λεγόμενο λήμμα του Abel (π.χ [6], σελίδα 26, άσκηση 13). Τώρα

$$\begin{aligned}
\left| e^{-\lambda_n s} - e^{\lambda_{n+1} s} \right| &= \left| s \int_{\lambda_n}^{\lambda_{n+1}} e^{-su} du \right| \\
\le |s| \int_{\lambda_n}^{\lambda_{n+1}} |e^{-su}| du &= |s| \int_{\lambda_n}^{\lambda_{n+1}} e^{-\sigma u} du \\
&= \frac{|s|}{\sigma} \Big(e^{-\lambda_n \sigma} - e^{-\lambda_{n+1} \sigma} \Big).
\end{aligned}$$

Για s μέσα στην περιοχή που ορίσαμε, έχουμε:

$$\frac{|s|}{\sigma} = \frac{1}{\cos|\arg s|} \le \frac{1}{\cos(\frac{\pi}{2} - \theta)} = \frac{1}{\sin\theta}$$

οπότε για $\sigma > 0$, ισχύει :

$$\left|\sum_{n=M}^{N} a_n e^{-\lambda_n s}\right| \leq \sum_{n=M}^{N-1} |A(M,n)| \cdot \left|e^{-\lambda_n s} - e^{-\lambda_{n+1} s}\right| + |A(M,N)| \cdot \left|e^{-\lambda_N s}\right|$$

$$\leq \frac{1}{\sin\theta}\varepsilon \sum_{n=M}^{N-1} (e^{-\lambda_n \sigma} - e^{-\lambda_{n+1}\sigma}) + \varepsilon e^{-\lambda_N \sigma}$$

$$\leq \frac{1}{\sin\theta}\varepsilon e^{-\lambda_M \sigma} + \varepsilon e^{-\lambda_N \sigma} < \Big(\frac{1}{\sin\theta} + 1\Big) e^{-\lambda_{N_0}\sigma}\varepsilon,$$

δηλαδή αποδείξαμε την αλήθεια του θεωρήματος. □

Το θεώρημα αυτό μάς δίνει ότι μια σειρά Dirichlet συγκλίνει σε κάποιο ημιεπίπεδο. Πράγματι αν
$U = \left\{\sigma \in \mathbb{R} \left| \sum_{n=1}^{\infty} \frac{a_n}{n^s} \text{ συγκλίνει} \right.\right\}$ *και*
$L = \left\{\sigma \in \mathbb{R} \left| \sum_{n=1}^{\infty} \frac{a_n}{n^s} \text{ αποκλίνει} \right.\right\}$
τότε κάθε στοιχείο του U είναι μεγαλύτερο από κάθε στοιχείο του L και η ταξινόμηση αυτή ορίζει ένα πραγματικό σ_0 τέτοιο ώστε να έχουμε σύγκλιση για κάθε $\sigma > \sigma_0$ και απόκλιση για κάθε $\sigma < \sigma_0$.
Αν $U = \emptyset$ τότε $\sigma_0 = +\infty$.
Αν $L = \emptyset$ τότε $\sigma_0 = -\infty$.

Ορισμός 3.3.2. . *Το σημείο σ_0 θα λέγεται σημείο αρχής της σύγκλισης. Η ευθεία $\sigma = \sigma_0$ είναι η γραμμή σύγκλισης και το ημιεπίπεδο $\sigma > \sigma_0$ είναι το ημιεπίπεδο σύγκλισης της σειράς Dirichlet .*

Συνδυάζοντας το θεώρημα 3.2.1 και το γνωστό θεώρημα του Weierstrass ([3] σελίδα 176) για σειρές συναρτήσεων παίρνουμε το εξής θεώρημα.

Θεώρημα 3.3.2. *Κάθε σειρά Dirichlet παριστά στο ημιεπίπεδο σύγκλισής της μία ολόμορφη συνάρτηση του s της οποίας οι διαδοχικές παράγωγοι λαμβάνονται παραγωγίζοντας τη σειρά κατά όρους.*

Φυσιολογικά τίθεται το ερώτημα στη συνέχεια για την εύρεση του σ_0 και τη συμπεριφορά της συνάρτησης (όριο σύγκλισης της σειράς Dirichlet στο $\sigma > \sigma_0$) στη γραμμή σύγκλισης $\sigma = \sigma_0$. Έχουμε το ανάλογο της ακτίνας σύγκλισης των δυναμοσειρων; Θα αποδείξουμε το ακόλουθο:

Θεώρημα 3.3.3. *Έστω $\sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$ μία σειρά Dirichlet και έστω ότι η σειρά $\sum_{n=1}^{\infty} a_n$ αποκλίνει. Τότε*

$$\sigma_0 = \limsup_{N\to\infty} \frac{\log|A(N)|}{\lambda_N}$$

όπου $A(N) := \sum_{n=1}^{N} a_n$.

Παρατήρηση: *Αν $\sum_{n=1}^{\infty} a_n$ συγκλίνει τότε το θεώρημα ισχύει και πάλι αρκεί να αντικαταστήσουμε το $A(N)$ με το $\sum_{n=N}^{\infty} a_n$. Επίσης, μπορούμε πάντα να μεταφέρουμε τη σειρά έτσι ώστε $\sigma_0 > 0$, δηλαδή η σειρά $\sum_{n=1}^{\infty} a_n$ να αποκλίνει.*

Απόδειξη. Για λόγους ευκολίας θα αποδείξουμε το θεώρημα για συνήθεις σειρές Dirichlet , δηλαδή για $\lambda_N = \log N$. Για την απόδειξη της γενικής περίπτωσης παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στο [5], σελίδα 161. Θα πρέπει λοιπόν να δείξουμε ότι

$$\sigma_0 = \gamma := \limsup_{N\to\infty} \frac{\log|A(N)|}{\log N} = \inf\{\alpha\,|\alpha > 0, A(N) = O(N^{\alpha})\}$$

(Ο συμβολισμός $A(N) = O(N^{\alpha})$ σημαίνει ότι υπάρχει $B > 0$ τέτοιο ώστε $|A(N)| \leq BN^{\alpha}$ για όλα τα N). Έστω $\sigma > \sigma_0$. Τότε η σειρά $\sum a_n n^{-\sigma}$ συγκλίνει. Άρα θα έχουμε ότι

$$\left|\sum_{n=1}^{N} a_n n^{-\sigma}\right| < C$$

για όλα τα $N \in \mathbb{N}$ και κατάλληλη σταθερά C. Όπως και πιο πριν, κάνοντας χρήση του λήμματος Abel , έχουμε

$$\begin{aligned}
|A(N)| &= \left|\sum_{n=1}^{N}(a_n n^{-\sigma})n^{\sigma}\right| \\
&= \left|\sum_{n=1}^{N-1}\Big(\sum_{m=1}^{n} a_m m^{-\sigma}\Big)\big(n^{\sigma}-(n+1)^{\sigma}\big) + \Big(\sum_{n=1}^{N} a_n n^{-\sigma}\Big)N^{\sigma}\right| \\
&\overset{(\sigma>0)}{\leq} \sum_{n=1}^{N-1}\left|\sum_{m=1}^{n} a_m m^{-\sigma}\right|\big((n+1)^{\sigma}-n^{\sigma}\big) + \left|\sum_{n=1}^{N} a_n n^{-\sigma}\Big)\right| N^{\sigma} \\
&< C\sum_{n=1}^{N-1}\big((n+1)^{\sigma}-n^{\sigma}\big) + CN^{\sigma} < 2CN^{\sigma}.
\end{aligned}$$

Συνεπώς, $|A(N)| = O(N^{\sigma})$. Αν τώρα $\gamma := \inf\{\alpha|\exists N_0 \in \mathbb{N}$ τ.ω $\forall N \geq N_0 \frac{\log|A(N)|}{\log N} < \alpha\}$ τότε ο γ θα είναι εξ ορισμού, μικρότερος ή ίσος προς τον σ και, αφού αυτό θα ισχύει

για όλα τα σ , με $\sigma > \sigma_0$, θα έχουμε ότι $\gamma \leq \sigma_0$. Έστω τώρα $\sigma > \gamma$. Εφαρμόζοντας ξανά το λήμμα του Abel βρίσκουμε ότι

$$\sum_{n=1}^{N} a_n n^{-\sigma} = \sum_{n=1}^{N-1} A(n)\big(n^{-\sigma} - (n+1)^{-\sigma}\big) + A(N)N^{-\sigma} \tag{1.3}$$

Διαλέγουμε α με $\gamma < \alpha < \sigma$ και μία σταθερά C με $|A(N)| \leq CN^{\alpha}$ για κάθε N, οπότε έχουμε:

$$\begin{aligned} \big|A(n)\big(n^{-\sigma} - (n+1)^{-\sigma}\big)\big| &\overset{(\sigma>0)}{\leq} Cn^{\alpha}\big(n^{-\sigma} - (n+1)^{-\sigma}\big) \\ &= Cn^{\alpha}\sigma \int_{n}^{n+1} x^{-\sigma-1}dx \\ &< C\sigma n^{\alpha-\sigma-1}. \end{aligned}$$

και $|A(N)N^{-\sigma}| \leq CN^{\alpha-\sigma} \to 0$ καθώς $N \to \infty$. Η σύγκλιση της σειράς $\sum_{n=1}^{\infty} n^{\alpha-\sigma-1}$ μας δίνει ένα πεπερασμένο όριο καθώς $N \to \infty$. Επομένως το δεξί μέλος της (1.3) συγκλίνει, όταν $N \to \infty$, οπότε και η σειρά $\sum_{n=1}^{\infty} a_n n^{-\sigma}$ συγκλίνει άρα $\sigma \geq \sigma_0$ και αφού ισχύει για κάθε $\sigma > \gamma$ έπεται ότι $\gamma \geq \sigma_0$, δηλαδή τελικά $\gamma = \sigma_0$ □

Παραδείγματα:

1. *Έστω* $\zeta(s) = \sum_{n=1}^{\infty} \dfrac{1}{n^s}$ *η περίφημη ζήτα συνάρτηση του Riemann . Έχουμε*

$$a_n = 1 \text{ και } A(N) = N \Longrightarrow \sigma_0 = \gamma = 1$$

δηλαδή η σειρά συγκλίνει για $\sigma > 1$.

2. *Έστω τώρα η* $\psi(s) := 1 - \dfrac{1}{2^s} + \dfrac{1}{3^s} - \cdots$ *εδώ*

$$a_n = (-1)^{n-1}, A(N) := \begin{cases} 1, & \text{όταν } N \text{ είναι περιττός} \\ 0, & \text{όταν } N \text{ είναι άρτιος} \end{cases}$$

συνεπώς $\sigma_0 = \gamma = 0$ *δηλαδή η σειρά συγκλίνει για* $\sigma > 0$ *και ορίζεται στο ημιεπίπεδο αυτό μία ολόμορφη συνάρτηση. Για* $\sigma > 1$ *όμως είναι προφανές ότι*

$$\psi(s) = \zeta(s) - 2\Big(\frac{1}{2^s} + \frac{1}{4^s} + \cdots\Big) = (1 - 2^{1-s})\zeta(s),$$

δηλαδή έχουμε μία μέθοδο να επεκτείνουμε την $\zeta(s)$ *μερόμορφα στο ημιεπίπεδο* $\sigma > 0$, *όπου οι πιθανοί πόλοι βρίσκονται το πολύ στα σημεία*

$$s = 1, 1 \pm \frac{2\pi i}{\log 2}, 1 \pm \frac{4\pi i}{\log 2}, \cdots$$

όπου μηδενίζεται ο $1 - 2^{1-s}$.

Σημαντική διαφορά από τις δυναμοσειρές.
Ο τύπος $R = \liminf_{n\to\infty} |a_n|^{-\frac{1}{n}}$ *δίνει αμέσως ότι οι* $\sum a_n z^n$ *και* $\sum |a_n| z^n$ *έχουν την ίδια ακτίνα σύγκλισης και μάλιστα όπου συγκλίνει η σειρά μέσα στον ανοικτό δίσκο σύγκλισης εκεί συγκλίνει και απόλυτα.*
Στο παράδειγμά μας όμως η $\psi(s)$ *συγκλίνει για* $\sigma > 0$, *ενώ συγκλίνει απόλυτα για* $\sigma > 1$.

Στην περίπτωση της συνήθους σειράς Dirichlet ισχύει το

Θεώρημα 3.3.4. *Έστω ότι η σειρά Dirichlet* $\sum_{n=1}^{\infty} a_n n^{-s}$ *έχει σημείο αρχής σύγκλισης το* σ_0 *ενώ η* $\sum_{n=1}^{\infty} |a_n| n^{-s}$ *το* σ_1. *Τότε ισχύει:*

$$\sigma_1 \leq \sigma_0 + 1, \text{ δηλαδή } 0 \leq \sigma_1 - \sigma_0 \leq 1.$$

Παρατήρηση: *Το θεώρημα 3.2.4 ισχύει μόνο για συνήθεις σειρές Dirichlet και όχι γενικά για κάθε σειρά Dirichlet .*

Απόδειξη. Αρκεί να δείξουμε ότι αν η $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ συγκλίνει για κάποια τιμή s_0 με $Re(s_0) = \sigma_0$, τότε θα συγκλίνει απόλυτα για όλα τα s με $\sigma > \sigma_0 + 1$. Έστω A ένα άνω φράγμα των αριθμών $\left|\frac{a_n}{n^{s_0}}\right|$. (Υπάρχει τέτοιο αφού εξ υποθέσεως για $s = s_0$ η σειρά $\sum \frac{a_n}{n^{s_0}}$ συγκλίνει). Επομένως

$$\left|\frac{a_n}{n^s}\right| = \left|\frac{a_n}{n^{s_0}}\right| \cdot \left|\frac{1}{n^{s-s_0}}\right| \leq \frac{A}{n^{\sigma-\sigma_0}}$$

για $\sigma > \sigma_0 + 1 \Longrightarrow \sigma - \sigma_0 > 1 \Longrightarrow \sum \frac{1}{n^{\sigma-\sigma_0}}$ συγκλίνει, άρα και η σειρά $\sum \left|\frac{a_n}{n^s}\right|$ συγκλίνει. □

Υπάρχει και άλλη πολύ πιο σπουδαία διαφορά των σειρών Dirichlet από αυτή των δυναμοσειρών.
Στις δυναμοσειρές, αν η $\sum_{n=1}^{\infty} a_n z^n$ *παριστά μια συνάρτηση η οποία επεκτείνεται ολόμορφα στον ανοικτό δίσκο* $|z| < r$ *τότε αυτή συγκλίνει σε αυτόν τον δίσκο. Αυτό δεν ισχύει για σειρές Dirichlet (μπορεί να δει κανείς ότι η* $\psi(s)$ *η οποία ορίζεται για* $\sigma > 0$ *επεκτείνεται ολόμορφα σ΄ όλο το μιγαδικό επίπεδο, αλλά η σειρά* $\psi(s) = \sum_{n=0}^{\infty} (-1)^n \frac{1}{n^s}$ *συγκλίνει μόνο για* $\sigma > 0$.*)*
Ισχύει όμως, σαν ειδική περίπτωση, το παρακάτω θεώρημα.

Θεώρημα 3.3.5. ***(Θεώρημα του Landau)*** *Έστω* $\sigma_0 \in \mathbb{R}$ *το αρχικό σημείο σύγκλισης της σειράς* $\sum_{n=1}^{\infty} a_n n^{-s}$ *και έστω ότι* $a_n \in \mathbb{R}$ *για κάθε* $n \in \mathbb{N}$ *και* $a_n \geq 0$.

Τότε η συνάρτηση $f(s)$ που ορίζεται από τη σειρά Dirichlet

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \text{ για } \sigma > \sigma_0$$

έχει ανωμαλία στο $\sigma = \sigma_0$.

Απόδειξη. Αφού $a_n \geq 0$ έχουμε ότι $\sigma_1 = \sigma_0$ (για τον ορισμό του σ_1 δες το αμέσως προηγούμενο θεώρημα 3.2.4). Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $\sigma_0 = 0$. Αν $f(s)$ ολόμορφη στο $s = 0$ τότε αυτή θα ήταν ολόμορφη σε κάποιο δίσκο $|s| < \varepsilon$ και αφού για $\sigma > \sigma_0 = 0$ είναι ολόμορφη (δες θεώρημα 3.2.2) το ανάπτυγμα Taylor της $f(s)$ στο σημείο $s = 1$ θα είχε ακτίνα σύγκλισης $R > 1$. Θα υπήρχε λοιπόν ένα $s \in \mathbb{R}, s < 0$ για το οποίο το ανάπτυγμα Taylor

$$\sum_{\nu=0}^{\infty} \frac{(s-1)^\nu}{\nu!} f^{(\nu)}(1)$$

θα συνέκλινε. Αλλά για $\sigma > 0$, $f(s) = \sum_{n=1}^{\infty} a_n e^{-s \log n}$, οπότε από θεώρημα 3.2.2, έχουμε

$$f^{(\nu)}(s) = \sum_{n=1}^{\infty} a_n \frac{(-\log n)^\nu}{n^s}$$

και για $s = 1$

$$f^{\nu}(1) = \sum_{n=1}^{\infty} a_n \frac{(-\log n)^\nu}{n}$$

Το ανάπτυγμα Taylor λοιπόν της f για $s = 1$ είναι :

$$\sum_{\nu=0}^{\infty} \frac{(s-1)^\nu}{\nu!} \sum_{n=1}^{\infty} a_n \frac{(-\log n)^\nu}{n} = \sum_{\nu=0}^{\infty} \frac{(1-s)^\nu}{\nu!} \sum_{n=1}^{\infty} \frac{a_n (\log n)^\nu}{n}$$

Όλοι οι όροι της διπλοσειράς είναι μη αρνητικοί, αν $s < 0$ (έχουμε δηλαδή απόλυτη σύγκλιση) οπότε μπορούμε να αλλάξουμε τη σειρά της πρόσθεσης συνεπώς η προηγούμενη σχέση μπορεί να πάρει τη μορφή

$$\sum_{n=1}^{\infty} \frac{a_n}{n} \sum_{\nu=0}^{\infty} \frac{(1-s)^\nu (\log n)^\nu}{\nu!}$$

Έχουμε λοιπόν σύγκλιση της σειράς αυτής για κάποιο $s < 0$. Επίσης έχουμε ότι

$$\sum_{\nu=0}^{\infty} \frac{(1-s)^\nu (\log n)^\nu}{\nu!} = e^{(1-s)\log n} = n^{1-s}$$

Επομένως, η σειρά $\sum_{n=1}^{\infty} a_n n^{-s}$ συγκλίνει για κάποιο $s < 0$ το οποίο είναι άτοπο, διότι $\sigma_0 = 0$, δηλαδή θα πρέπει η $f(s)$ να έχει ανωμαλία στο $s = 0$. □

Θα κλείσουμε αυτήν την παράγραφο με ένα θεώρημα μοναδικότητας των συντελεστών μιας σειράς Dirichlet . Συγκεκριμένα θα αποδείξουμε το

Θεώρημα 3.3.6. *Αν οι σειρές Dirichlet*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} \quad \text{και} \quad \sum_{n=1}^{\infty} \frac{b_n}{n^s}$$

συγκλίνουν σε κάποιο κοινό ημιεπίπεδο και οι συναρτήσεις που ορίζουν, έστω $f_1(s)$ και $f_2(s)$, συμπίπτουν σε κάποιο μη κενό, ανοικτό σύνολο που περιέχεται στο ημιεπίπεδο κοινής σύγκλισης, τότε $a_n = b_n$ για όλα $n \geq 1$.

Απόδειξη. Θεωρούμε τη σειρά Dirichlet

$$\sum_{n=1}^{\infty} \frac{(a_n - b_n)}{n^s}$$

Αυτή συγκλίνει στο ημιεπίπεδο $\sigma > \sigma_0$ όπου και ορίζει ολόμορφη συνάρτηση, έστω $f(s)$. Η συνάρτηση αυτή μηδενίζεται σε κάποιο ανοικτό σύνολο που περιέχεται στο ημιεπίπεδο $\sigma > \sigma_0$. Επομένως $f(s) \equiv 0$ στο $\sigma > \sigma_0$. Έστω M ο ελάχιστος φυσικός αριθμός τέτοιος ώστε $a_M \neq b_M$ και έστω $c_n = a_n - b_n$. Για $\sigma > \sigma_0$ έχουμε λοιπόν

$$\sum_{n=1}^{\infty} \frac{c_n}{n^\sigma} = \sum_{n=M}^{\infty} \frac{c_n}{n^\sigma} = 0 \quad \text{ή} \quad \frac{c_M}{M^\sigma} = -\sum_{n=M+1}^{\infty} \frac{c_n}{n^\sigma}.$$

Επομένως

$$|c_M| \leq \sum_{n=M+1}^{\infty} |c_n| \left(\frac{M}{n}\right)^\sigma, \quad \sigma > \sigma_0 + 1$$

Αν τώρα πάρουμε το s τέτοιο ώστε $\sigma > \sigma_0 + 2$, τότε λόγω ομοιόμορφης σύγκλισης, αν $\sigma \to \infty$ έπεται ότι $c_M = 0$ το οποίο είναι άτοπο. Συνεπώς δεν υπάρχει τέτοιο M και επομένως ισχύει $a_n = b_n$ για κάθε $n \geq 1$.

□

3.4 Σειρές του Dirichlet (τυπικές ιδιότητες)

Η πρόσθεση σειρών του Dirichlet ορίζεται τελείως φυσιολογικά ως η σειρά που έχει συντελεστές το άθροισμα των αντίστοιχων συντελεστών. Τί γίνεται όμως με το γινόμενο; Έστω

$$f(s) = \sum_{n=1}^{\infty} a_n n^{-s} \text{ και } g(s) = \sum_{m=1}^{\infty} b_m m^{-s}$$

δύο συναρτήσεις οι οποίες ορίζονται σε κάποιο ανοικτό σύνολο U μέσω της απόλυτης σύγκλισης των σειρών Dirichlet που τις ορίζουν. Στο U λοιπόν έχουμε

$$\begin{aligned} f(s)g(s) &= \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} a_n b_m n^{-s} m^{-s} \\ &= \sum_{n,m=1}^{\infty} a_n b_m (nm)^{-s} = \sum_{k=1}^{\infty} c_k k^{-s} \end{aligned}$$

$$\text{όπου } c_k = \sum_{n,m\geq 1, mn=k} a_n b_m = \sum_{n|k} a_n b_{\frac{k}{n}}$$

Σημαντική παρατήρηση: *Η παραπάνω έκφραση των συντελεστών c_k που είναι πολλαπλασιαστική, σε αντίθεση με τις δυναμοσειρές που είναι προσθετική, είναι αυτή για την οποία οι σειρές Dirichlet αποκτούν εξαιρετική σημασία για τη Θεωρία Αριθμών.*
Εύκολα αποδεικνύεται ότι η σειρά $\sum_{k=1}^{\infty} c_k k^{-s}$ συγκλίνει όταν τουλάχιστον μία από αυτές συγκλίνει απλά και η άλλη απόλυτα.

Παραδείγματα:

1. *Έστω $d(n)$ το πλήθος των θετικών διαιρετών του φυσικού αριθμού n. Τότε, για $\sigma > 1$,*
$$\sum_{n=1}^{\infty} \frac{d(n)}{n^s} = \zeta(s)^2 \text{ διότι } d(n) = \sum_{d|n} 1 \times 1$$

2. *Έστω $\tau(n)$ το άθροισμα των θετικών διαιρετών του n ή γενικότερα*
$$\sigma_k(n) = \sum_{d|n} d^k = 1 \times d^k$$
τότε ισχύει
$$\sum_{n=1}^{\infty} \frac{\sigma_k(n)}{n^s} = \zeta(s)\zeta(s-k) \quad (\sigma > k+1)$$

Και στα δύο παραδείγματα οι συναρτήσεις μέσω των οποίων ορίζονται οι συντελεστές των σειρών είναι πολλαπλασιαστικές. Ξαναθυμίζουμε τον ορισμό.

Ορισμός 3.4.1. . *Η συνάρτηση $f : \mathbb{N} \to \mathbb{C}$ θα λέγεται πολλαπλασιαστική συνάρτηση όταν*
$$f(mn) = f(m)f(n)$$

για όλους τους φυσικούς m, n πρώτους μεταξύ τους και υπάρχει τουλάχιστον ένας φυσικός n_0 τέτοιος ώστε $f(n_0) \neq 0$. Επιπλέον θα λέγεται πλήρως πολλαπλασιαστική συνάρτηση όταν απαλείψουμε τον περιορισμό $(m, n) = 1$
Στα 1737 ο Euler ανακάλυψε και απέδειξε το παρακάτω θεώρημα.

Θεώρημα 3.4.1. ***(Γινόμενο Euler)*** *Αν f πολλαπλασιαστική και $\sum_{n=1}^{\infty} f(n)$ απολύτως συγκλίνουσα τότε*

$$\sum_{n=1}^{\infty} f(n) = \prod_{p \in \mathbb{P}} \{1 + f(p) + f(p^2) + \cdots\}$$

και το απειρογινόμενο συγκλίνει απόλυτα. Αν f πλήρως πολλαπλασιαστική τότε

$$\sum_{n=1}^{\infty} f(n) = \prod_{p \in \mathbb{P}} \frac{1}{1 - f(p)}.$$

Απόδειξη. Κατ' αρχήν ορίζουμε

$$P(x) := \prod_{p \leq x} \{1 + f(p) + f(p^2) + \cdots\}.$$

Το $P(x)$ είναι πεπερασμένο γινόμενο απόλυτα συγκλινουσών σειρών, συνεπώς μπορούμε να πολλαπλασιάσουμε ή να αλλάξουμε τη σειρά των όρων, χωρίς να αλλάξει το άθροισμα. Θα έχουμε δηλαδή γινόμενα της μορφής

$$f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_\nu^{\alpha_\nu}) = f(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\nu^{\alpha_\nu}) \quad p_i \neq p_j, \text{ για κάθε } i \neq j$$

Το θεμελιώδες θεώρημα της αριθμητικής μας δίνει

$$P(x) = \sum_{n \in A} f(n)$$

όπου $A = \{n \in \mathbb{N} \,|\, \text{οι πρώτοι παράγοντες του } n \text{ είναι όλοι} \leq x\}$. Επομένως

$$\sum_{n=1}^{\infty} f(n) - P(x) = \sum_{n \in B} f(n)$$

όπου $B = \{n \in \mathbb{N} \,|\, \exists p \in \mathbb{P}, p \mid n, \text{ τέτοιος ώστε } p > x\}$. Άρα,

$$\left| \sum_{n=1}^{\infty} f(n) - P(x) \right| \leq \sum_{n \in B} |f(n)| \leq \sum_{n > x} |f(n)|.$$

Τώρα αφού η $\sum_{n=1}^{\infty}|f(n)|$ συγκλίνει, έπεται ότι για $x\to\infty$ το $\sum_{n>x}^{\infty}|f(n)|\to 0$. Επίσης είναι γνωστό ότι το απειρογινόμενο $\prod_{n=1}^{\infty}(1+a_n)$ συγκλίνει απόλυτα τότε και μόνο τότε όταν η σειρά $\sum_{n=1}^{\infty}|a_n|$ συγκλίνει. ([8], σελίδα 192.) Επίσης έχουμε ότι:

$$\sum_{p\le x}\big|f(p)+f(p^2)+\cdots\big|\le\sum_{p\le x}\Big(|f(p)|+\big|f(p^2)\big|+\cdots\Big)\le\sum_{n=2}^{\infty}|f(n)|$$

Αφού όλα τα μερικά αθροίσματα είναι πεπερασμένα, η σειρά θετικών όρων

$$\sum_{p\in\mathbb{P}}\big|f(p)+f(p^2)+\cdots\big|$$

συγκλίνει, οπότε και το αντίστοιχο απειρογινόμενο συγκλίνει απόλυτα. Τώρα αν η f είναι πλήρως πολλαπλασιαστική τότε $f(p^n)=f(p)^n$ για κάθε πρώτο p και έχουμε γεωμετρικές σειρές με άθροισμα $\dfrac{1}{1-f(p)}$. □

Θεώρημα 3.4.2. *Αν υποθέσουμε ότι η σειρά Dirichlet $\sum_{n=1}^{\infty}\frac{f(n)}{n^s}$ συγκλίνει απόλυτα για $\sigma>\sigma_0$, όπου f πολλαπλασιαστική συνάρτηση, τότε*

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s}=\prod_{p\in\mathbb{P}}\Big\{1+\frac{f(p)}{p^s}+\frac{f(p^{2)}}{p^{2s}}+\cdots\Big\},\qquad \text{για } \sigma>\sigma_0.$$

Αν f πλήρως πολλαπλασιαστική συνάρτηση, τότε

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s}=\prod_{p\in\mathbb{P}}\frac{1}{1-f(p)p^{-s}},\qquad \text{για } \sigma>\sigma_0$$

Το παραπάνω θεώρημα είναι άμεση συνέπεια του θεωρήματος 3.3.2 για $g(n)=\dfrac{f(n)}{n^s}$. Αρκεί να παρατηρήσουμε ότι όταν η $f(n)$ είναι πολλαπλασιαστική, το ίδιο ισχύει και για την $g(n)=\dfrac{f(n)}{n^s}$.

Παραδείγματα:

1. $\zeta(s)=\sum_{n=1}^{\infty}\dfrac{1}{n^s}=\prod_{p\in\mathbb{P}}\dfrac{1}{1-p^{-s}}$, για $\sigma>1$

2. $\sum_{n=1}^{\infty}\dfrac{d(n)}{n^s}=\zeta(s)^2=\prod_{p\in\mathbb{P}}(1-p^{-s})^{-2}$, για $\sigma>1$.

3.5 Οι L-σειρές του Dirichlet

Στη συνέχεια θα συνδέσουμε τη θεωρία των σειρών του Dirichlet με τη θεωρία των χαρακτήρων πεπερασμένων ομάδων που αναπτύξαμε στη δεύτερη παράγραφο αυτού του κεφαλαίου.
Έστω $N \in \mathbb{N}$, $N \geq 2$ και χ ένας χαρακτήρας Dirichlet $\bmod N$*.Η L-σειρά Dirichlet ορίζεται ως εξής:*

$$L(s/\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \tag{3.1}$$

Αφού $|\chi(n)| \leq 1$ για κάθε φυσικό αριθμό n, συνεπάγεται ότι $\left|\frac{\chi(n)}{n^s}\right| \leq \frac{1}{n^\sigma}$, άρα η σειρά $L(s/\chi)$ συγκλίνει απόλυτα για $\sigma > 1$.

Αφού χ πολλαπλασιαστική συνάρτηση θα έχουμε ότι

$$L(s/\chi) = \prod_{p\in\mathbb{P}} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \cdots\right)$$

και μάλιστα αφού χ πλήρως πολλαπλασιαστική,

$$L(s/\chi) = \prod_{p\in\mathbb{P}} \frac{1}{1 - \frac{\chi(p)}{p^s}} \quad (\sigma > 1) \tag{3.2}$$

Ιδιαίτερα για $\chi = \chi_0$ ισχύει

$$L(s/\chi_0) = \prod_{p\in\mathbb{P}} (1 - \chi_0(p)p^{-s})^{-1}$$

Για $p \mid N$, ισχύει $\chi_0(p) = 0$ και συνεπώς $(1 - \chi_0(p)p^{-s})^{-1} = 1$. Για $p \nmid N$ ισχύει $\chi_0(p) = 1$. Επομένως,

$$\begin{aligned} L(s/\chi_0) &= \prod_{p\in\mathbb{P}} (1 - \chi_0(p)p^{-s})^{-1} \\ &= \prod_{\substack{p\in\mathbb{P} \\ p\nmid N}} (1 - p^{-s})^{-1} \\ &= \prod_{p\mid N} (1 - p^{-s}) \prod_{p\in\mathbb{P}} (1 - p^{-s})^{-1} \\ &= \zeta(s) \prod_{\substack{p\in\mathbb{P} \\ p\mid N}} (1 - p^{-s}), \end{aligned}$$

δηλαδή η L-σειρά Dirichlet για $\chi = \chi_0$ είναι ίση με τη ζήτα συνάρτηση του Riemann πολλαπλασιασμένη με σταθερά που εξαρτάται μόνο από το N.

Αν δεχτούμε σαν γνωστή την ιδιότητα της ζήτα συνάρτηση του Riemann , ότι επεκτείνεται μερόμορφα σ΄ όλο το μιγαδικό επίπεδο και μάλιστα έχει μοναδικό απλό πόλο στη θέση $s = 1$ και υπόλοιπο ίσο με 1, τότε το συμπέρασμα για την $L(s/\chi_0)$ είναι ότι επεκτείνεται μερόμορφα σ΄ όλο το μιγαδικό επίπεδο με μοναδικό πόλο στη θέση $s = 1$ και υπόλοιπο ίσο προς

$$\prod_{p|N}(1 - p^{-1}) = \frac{\varphi(N)}{N}.$$

Αν τώρα $\chi \neq \chi_0$ και $x \to \infty$ τότε

$$\begin{aligned}
\left|\sum_{n=1}^{x}\chi(n)\right| &= \left|\sum_{n=1}^{N\left[\frac{x}{N}\right]}\chi(n) + \sum_{n=N\left[\frac{x}{N}\right]+1}^{x}\chi(n)\right| \\
&= \left|\left[\frac{x}{N}\right]\sum_{n \pmod N}\chi(n) + \sum_{n=N\left[\frac{x}{N}\right]+1}^{x}\chi(n)\right| \\
&= \left|\sum_{n=N\left[\frac{x}{N}\right]+1}^{x}\chi(n)\right| \\
&\leq \left|x - N\left[\frac{x}{N}\right]\right| \leq N = O(1)
\end{aligned}$$

οπότε από το θεώρημα 3.1.1 έχουμε ότι $\sigma_0 \leq 0$. επειδή η σειρά αποκλίνει για $\sigma_0 < 0$ θα έχουμε κατ΄ ανάγκη $\sigma_0 = 0$.

Επομένως για $\chi \neq \chi_0$ και $\sigma > 0$ η $L(s/\chi)$ είναι μια ολόμορφη συνάρτηση. Για $\chi \neq \chi_0$ μπορεί να αποδειχθεί ότι η $L(s/\chi)$ επιδέχεται ολόμορφη επέκταση σ΄ όλο το μιγαδικό επίπεδο.

Η πιο σημαντική ίσως ιδιότητα των L-σειρών του Dirichlet περιέχεται στο επόμενο θεώρημα.

Θεώρημα 3.5.1. *Αν $\chi \neq \chi_0$ τότε*

$$L(1/\chi) \neq 0.$$

Απόδειξη. Έστω

$$F(s) := \prod_{\chi} L(s/\chi) \tag{3.3}$$

όπου το χ διατρέχει όλους τους χαρακτήρες Dirichlet mod N . Λόγω του γινομένου Euler για $\sigma > 1$ ισχύει :

$$\begin{aligned}
\log F(s) &= \log\big(\prod_{\chi} L(1/\chi)\big) \\
&= \sum_{\chi} \log L(s/\chi) \\
&= \sum_{\chi} \log\big[\prod_{p\in\mathbb{P}} (1-\chi(p)p^{-s})^{-1}\big] \\
&= \sum_{\chi}\sum_{p\in\mathbb{P}} \log[(1-x(p)p^{-s})^{-1}] \\
&= \sum_{\chi}\sum_{p\in\mathbb{P}}\sum_{r=1}^{\infty} \frac{1}{r}\frac{\chi(p)^r}{p^{rs}} \\
&= \sum_{p\in\mathbb{P}}\sum_{n=1}^{\infty} \frac{1}{rp^{rs}} \sum_{\chi} \chi(p^r) \\
&= \varphi(N) \sum_{\substack{p\in\mathbb{P}, \\ p^r\equiv 1 \pmod N}} \sum_{r=1}^{\infty} \frac{1}{rp^{rs}}
\end{aligned}$$

διότι

$$\sum_{\chi} \chi(n) := \begin{cases} \varphi(N), & \text{όταν } n \equiv 1 \pmod N \\ 0, & \text{όταν } n \not\equiv 1 \pmod N. \end{cases}$$

Ιδιαίτερα για $s \in \mathbb{R}$ και $s > 1$ ισχύει $\log F(s) \geq 0$. Δηλαδή,

$$\liminf_{\substack{s\to 1^+ \\ s\in\mathbb{R}}} F(s) \geq 1. \tag{3.4}$$

Το γινόμενο (3.3) περιέχει μόνο ένα απλό πόλο στη θέση $s = 1$ που προκύπτει από την $L(s/\chi_0)$. Υποθέτουμε τώρα ότι $L(1/\chi) = 0$ για δυο ή περισσότερους χαρακτήρες $\chi \neq \chi_0$, τότε ο απλός πόλος της στο θα αναιρούνταν από την μία $L(s/\chi)$ με $L(1/\chi) = 0$ οπότε η $F(s)$ θα ήταν ολόμορφη στη θέση $s = 1$ και θα έπαιρνε για $s = 1$ την τιμή 0 λόγω του μηδενισμού της άλλης L-σειράς, άτοπο λόγω της (3.4). Άρα το πολύ για ένα χαρακτήρα $\chi \neq \chi_0$ μπορεί να ισχύει $L(1/\chi) = 0$.
Έστω, λοιπόν, τώρα $L(1/\chi) = 0$ τότε

$$L(1/\bar{\chi}) = \sum_{n=1}^{\infty} \frac{\bar{\chi}(n)}{n} = \sum_{n=1}^{\infty} \frac{\overline{\chi(n)}}{n} = \overline{\sum_{n=1}^{\infty} \Big(\frac{\chi(n)}{n}\Big)} = \overline{L(1/\chi)} = 0.$$

Επομένως αν υπήρχε μοναδικός χαρακτήρας τέτοιος ώστε $L(1/\chi) = 0$ θα έπρεπε $\chi = \bar{\chi}$, δηλαδή ο χ να είναι πραγματικός χαρακτήρας. Έστω λοιπόν χ πραγματικός χαρακτήρας με $L(1/\chi) = 0$. Ορίζουμε

$$\psi(s) := L(s/\chi)\zeta(s) = \sum_{n=1}^{\infty} \frac{\rho(n)}{n^s}, \quad \text{όπου } \rho(n) = \sum_{d|n} \chi(d)$$

$$\begin{aligned}
\psi(s) &= \prod_{p\in\mathbb{P}} \frac{1}{(1-\chi(p)p^{-s})(1-p^{-s})} \\
&= \prod_{\chi(p)=1} \frac{1}{(1-p^{-s})^2} \prod_{\chi(p)=0} \frac{1}{1-p^{-s}} \prod_{\chi(p)=-1} \frac{1}{1-p^{-2s}} \\
&= \prod_{\chi(p)=0} \left(1+\frac{2}{p^s}+\frac{3}{p^{2s}}+\cdots\right) \prod_{\chi(p)=1} \left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\cdots\right) \prod_{\chi(p)=-1} \left(1+\frac{1}{p^{2s}}+\frac{1}{p^{4s}}+\cdots\right)
\end{aligned}$$

Επομένως, έχουμε απειρογινόμενα όλα με θετικούς συντελεστές, οπότε

$$\rho(n) \geq 0 \quad \forall n \in \mathbb{N} \text{ και μάλιστα } \rho(n^2) \geq 1.$$

Τώρα, λόγω της υπόθεσης ότι $L(1/\chi) = 0$ (και επειδή η $\zeta(s)$ έχει πόλο μόνο για $s = 1$ και μάλιστα τάξης 1), έπεται ότι η $\psi(s)$ δεν έχει ιδιάζον σημείο για $\sigma > 0$ και η (3.2) και το Θεώρημα Landau μας εξασφαλίζουν τη σύγκλιση της σειράς $\sum \rho(n)n^{-s}$ για $\sigma > 0$. Από την άλλη μεριά όμως,

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{\rho(n)}{n^{\frac{1}{2}}} &= \frac{\rho(1)}{1} + \frac{\rho(2)}{\sqrt{2}} + \frac{\rho(3)}{\sqrt{3}} + \frac{\rho(4)}{\sqrt{4}} + \cdots \\
&\geq \frac{\rho(1)}{1} + \frac{\rho(4)}{\sqrt{2}} + \cdots = \sum_{n=1}^{\infty} \frac{\rho(n^2)}{n} \\
&\geq \sum_{n=1}^{\infty} \frac{1}{n}
\end{aligned}$$

Ως γνωστό η σειρά $\sum_{n=1}^{\infty} \frac{1}{n}$ αποκλίνει.Συνεπώς και η σειρά $\sum_{n=1}^{\infty} \frac{\rho(n)}{n^{\frac{1}{2}}}$ αποκλίνει, άτοπο. Οπότε

$$L(1/\chi) \neq 0 \text{ για κάθε χαρακτήρα } \chi \neq \chi_0$$

□

Πόρισμα 3.5.1. ***(Θεώρημα του Dirichlet για αριθμητικές προόδους.)*** *Αν N φυσικός αριθμός και a ακέραιος πρώτος προς τον N, τότε η αριθμητική πρόοδος $\{Nk+a\}_{k\in\mathbb{N}}$ περιέχει άπειρο πλήθος πρώτων και μάλιστα η σειρά $\sum_{\substack{p\in\mathbb{P}\\ p\equiv a \pmod N}} \frac{1}{p}$ αποκλίνει.*

Απόδειξη. Για $\sigma > 1$

$$\begin{aligned}
\sum_{\substack{p\in\mathbb{P}\\ p^r\equiv a(modN)}} \sum_{r\geq 1} \frac{1}{rp^{rs}} &= \sum_{\substack{p\in\mathbb{P}\\ p^r\equiv a(modN)}} \sum_{r\geq 1} \frac{1}{\varphi(N)} \sum_{\chi} \bar{\chi}(a)\chi(p^r)\frac{1}{rp^{rs}} \\
&= \frac{1}{\varphi(N)} \sum_{\chi} \bar{\chi}(a) \sum_{\substack{p\in\mathbb{P}\\ p^r\equiv a(modN)}} \sum_{r=1}^{\infty} \frac{\chi(p)^r}{rp^{rs}} \\
&= \frac{1}{\varphi(N)} \sum_{\chi} \bar{\chi}(a) \log L(s/\chi) \\
&= \frac{1}{\varphi(N)} \left[\log L(s/\chi_0) + \sum_{\chi\neq\chi_0} \bar{\chi}(a) \log L(s/\chi) \right] \qquad (3.5)
\end{aligned}$$

Η εναλλαγή των $\sum_p$ και $\sum_\chi$ επιτρέπεται διότι οι σειρές συγκλίνουν απόλυτα (μάλιστα η $\sum_\chi$ είναι πεπερασμένο άθροισμα). Τα αθροίσματα διατρέχουν ως συνήθως όλους τους πρώτους αριθμούς και όλους τους χαρακτήρες $modN$ αντίστοιχα.
Η $\log L(s/\chi_0)$ για $s \to 1$ τείνει στο ∞ ενώ για $\chi \neq \chi_0$ η $\log L(s/\chi)$ είναι άνω φραγμένη λόγω του θεωρήματος 3.4.1 , άρα το δεξί μέλος της (3.5) για $s = 1$ αποκλίνει. Αλλά

$$\begin{aligned}
\sum_{\substack{p\in\mathbb{P}\\ p^r\equiv a(modN)}} \sum_{r>1} \frac{1}{rp^{rs}} &\leq \sum_{p\in\mathbb{P}} \sum_{r=2}^{\infty} \frac{1}{rp^r} \\
&\leq \sum_{p\in\mathbb{P}} \sum_{r=2}^{\infty} \frac{1}{2p^r} = \sum_{p} \frac{1}{2p(p-1)} \\
&\leq \sum_{n=2}^{\infty} \frac{1}{2n(n-1)} = \frac{1}{2}
\end{aligned}$$

δηλαδή η σειρά συγκλίνει για $r > 1$, συνεπώς αποκλίνει για $r = 1$, οπότε η σειρά $\sum_{\substack{p\in\mathbb{P}\\ p\equiv a(modN)}} \frac{1}{p}$ αποκλίνει. Επομένως υπάρχουν άπειροι πρώτοι $p \equiv a \pmod N$.

□

Βιβλιογραφία

[1] *Ι. Αντωνιάδης και Α. Κοντογεώργης, Θεωρία Αριθμών και Εφαρμογές, Πρόγραμμα Κάλλιπος, http://eclass.uoa.gr/modules/document/file.php/MATH443 , Ηράκλειο 2015.*

[2] *Γιάννη Α. Αντωνιάδη, Θεωρία Αριθμών ΙΙ , L-σειρές, Έκδοση ΕΠΕΑΕΚ «ΠΡΟΜΗΘΕΑΣ», Πανεπιστήμιο Κρήτης, Ηράκλειο 1999.*

[3] *Lars V. Ahlfors, Complex Analysis, McGraw-Hill, London 1979.*

[4] *Martin Aigner, Günter M. Ziegler, Proofs from THE BOOK, Springer, third edition, Berlin 2003.*

[5] *Tom M.Apostol, Modular Functions and Dirichlet Series in Number Theory, Springer-Verlag, New York 1976 .*

[6] *E. Freitag, R. Busam, Funktionenthorie, 2 Auflage, Springer-Verlag, Berlin 1995.*

[7] *Romeo Meštrović, Euclid's Theorem on the infitude of Primes: A historical survey of its Proofs (300 B.C. -2012),*
arXiv: 1202.3670v2 [math.HO] 5 Jun 2012.

[8] *P.Ribenboim, The Little Book of Bigger Primes, Springer, second edition, Berlin 2004.*

[9] *Filip Saidak, A New Proof of Euclid's Theorem, American Math.Monthly, 113 (2006), 937-938.*