Αναλυτική Θεωρία Αριθμών

Σημειώσεις από τις Διαλέξεις

Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών
Πανεπιστήμιο Κρήτης
Ηράκλειο, 2026

Περιεχόμενα

1 Η πρώτη αναγωγή

1.1 Άθροιση κατά Abel

Θεώρημα 1.1 (Άθροιση κατά Abel). *Έστω $0 < y < x$ πραγματικοί αριθμοί και $f : [y, x] \to \mathbb{R}$ συνεχώς παραγωγίσιμη. Θεωρούμε την ακολουθία μιγαδικών αριθμών $(a_n)_{n \geq 1}$ και για κάθε*

$t > 0$ *ορίζουμε*

$$A(t) := \sum_{n \le t} a_n.$$

Τότε ισχύει

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

Θεώρημα 1.2 (Τύπος άθροισης Euler). *Έστω $0 < y < x$ πραγματικοί αριθμοί και $f : [y, x] \to \mathbb{R}$ με συνεχή παράγωγο f' στο $[y, x]$. Τότε*

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

όπου $\{t\} = t - \lfloor t \rfloor$ είναι το κλασματικό μέρος.

Οι παρακάτω δύο εφαρμογές είναι χαρακτηριστικές για το πώς χρησιμοποιούμε τον τύπο άθροισης.

Θεώρημα 1.3. *Για $x \ge 1$ ισχύει*

$$\sum_{n \le x} \frac{1}{n} = \log x + \gamma + \mathcal{O}\left(\frac{1}{x}\right), \tag{1}$$

όπου γ είναι η σταθερά του Euler, οριζόμενη από

$$\gamma = 1 - \int_1^\infty \frac{\{t\}}{t^2}\, dt.$$

Επιπλέον,

$$\gamma = \lim_{x \to \infty} \left(\sum_{n \le x} \frac{1}{n} - \log x \right).$$

Απόδειξη. Εφαρμόζουμε το Θεώρημα 1.2 για την συνάρτηση $f(t) = 1/t$ και $y = 1$. Τότε $\{1\} = 0$ και $f'(t) = -1/t^2$, άρα

$$\sum_{1 < n \le x} \frac{1}{n} = \int_1^x \frac{1}{t}\, dt + \int_1^x \{t\} \left(-\frac{1}{t^2}\right) dt - \{x\}\, \frac{1}{x}.$$

Επομένως

$$\sum_{n \le x} \frac{1}{n} = 1 + \log x - \int_1^x \frac{\{t\}}{t^2}\, dt - \frac{\{x\}}{x}.$$

Προσθέτουμε και αφαιρούμε $\int_1^\infty \frac{\{t\}}{t^2} dt$:

$$\sum_{n \le x} \frac{1}{n} = \log x + \left(1 - \int_1^\infty \frac{\{t\}}{t^2}\, dt\right) + \int_x^\infty \frac{\{t\}}{t^2}\, dt - \frac{\{x\}}{x}.$$

Ορίζοντας $\gamma = 1 - \int_1^\infty \frac{\{t\}}{t^2}\, dt$ παίρνουμε

$$\sum_{n \le x} \frac{1}{n} = \log x + \gamma + \int_x^\infty \frac{\{t\}}{t^2}\, dt - \frac{\{x\}}{x}.$$

Τώρα $0 \le \{t\} \le 1$, άρα

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

Άρα το υπόλοιπο είναι $\mathcal{O}(1/x)$ και προκύπτει η (1). Τέλος, καθώς $x \to \infty$ το $\mathcal{O}(1/x)$ τείνει στο 0, οπότε

$$\sum_{n \le x} \frac{1}{n} - \log x \to \gamma,$$

δηλαδή $\gamma = \lim_{x\to\infty} \left(\sum_{n\le x} \frac{1}{n} - \log x\right)$. □

Ορισμοί

Για $x \ge 0$ θέτουμε:

$$\pi(x) := \#\{p \le x : \ p \text{ πρώτος}\}, \qquad \theta(x) := \sum_{p \le x} \log p,$$

και

$$\psi(x) := \sum_{n \le x} \Lambda(n) = \sum_{p^k \le x} \log p,$$

όπου Λ είναι η συνάρτηση von Mangoldt: $\Lambda(n) = \log p$ αν $n = p^k$ για κάποιον πρώτο p και $k \ge 1$, και $\Lambda(n) = 0$ αλλιώς.

Θεώρημα 1.4. *Για κάθε $x \ge 2$ ισχύουν οι ταυτότητες*

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

και

$$\pi(x) = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t(\log t)^2}\,dt.$$

Απόδειξη. Εφαρμόζουμε το Θεώρημα 1.1 με $y = 2$,

$$a_n = \mathbf{1}_{\{n \text{ πρώτος}\}}, \qquad f(t) = \log t, \qquad A(t) = \sum_{n \le t} a_n = \pi(t).$$

Τότε

$$\sum_{2 < n \le x} a_n f(n) = \sum_{2 < p \le x} \log p = \theta(x) - \log 2.$$

Το Θεώρημα 1.1 δίνει

$$\theta(x) - \log 2 = \pi(x)\log x - \pi(2)\log 2 - \int_2^x \pi(t)\,\frac{dt}{t}.$$

Επειδή $\pi(2) = 1$, οι όροι $\log 2$ απαλείφονται, και παίρνουμε

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

Εφαρμόζουμε πάλι το Θεώρημα 1.1 με $y = 2$,

$$a_n = (\log n)\,\mathbf{1}_{\{n \text{ πρώτος}\}}, \qquad f(t) = \frac{1}{\log t}, \qquad A(t) = \sum_{n \le t} a_n = \theta(t).$$

Τότε

$$\sum_{2<n\le x} a_n f(n) = \sum_{2<p\le x} \frac{\log p}{\log p} = \pi(x) - 1,$$

επομένως

$$\pi(x) - 1 = \theta(x)\frac{1}{\log x} - \theta(2)\frac{1}{\log 2} - \int_2^x \theta(t)\, f'(t)\, dt.$$

Επειδή $\theta(2) = \log 2$, ο όρος $\theta(2)/\log 2$ είναι 1 και απαλείφεται με το -1 αριστερά. Επίσης

$$f'(t) = \left(\frac{1}{\log t}\right)' = -\frac{1}{t(\log t)^2}.$$

Άρα

$$\pi(x) = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t(\log t)^2}\, dt.$$

□

Θεώρημα 1.5. *Για κάθε $x \ge 1$ ισχύει*

$$0 \le \psi(x) - \theta(x) \le \frac{\sqrt{x}(\log x)^2}{2\log 2}. \tag{2}$$

Ειδικότερα, για $x \ge 2$ έχουμε

$$\psi(x) = \theta(x) + O\big(\sqrt{x}(\log x)^2\big).$$

Απόδειξη. Η ανισότητα $\psi(x) - \theta(x) \ge 0$ είναι άμεση, αφού η ψ περιλαμβάνει όλους τους όρους της θ και επιπλέον τις συνεισφορές από πρώτες δυνάμεις p^k με $k \ge 2$.

Για το άνω φράγμα, ξεκινάμε από τον ορισμό

$$\psi(x) = \sum_{n\le x} \Lambda(n) = \sum_{p^k \le x} \Lambda(p^k).$$

Ομαδοποιώντας ως προς τον εκθέτη k παίρνουμε

$$\psi(x) = \sum_{k\ge 1} \sum_{p \le x^{1/k}} \log p = \sum_{k\ge 1} \theta\big(x^{1/k}\big).$$

Το άθροισμα ως προς k είναι στην πράξη πεπερασμένο, διότι $\theta(y) = 0$ όταν $y < 2$ (δεν υπάρχουν πρώτοι ≤ 1). Άρα $\theta(x^{1/k}) = 0$ για $x^{1/k} < 2$, δηλαδή για

$$k > \frac{\log x}{\log 2}.$$

Συνεπώς

$$\psi(x) - \theta(x) = \sum_{k\ge 2} \theta(x^{1/k}) = \sum_{2 \le k \le \log x/\log 2} \theta(x^{1/k}).$$

Για $k \ge 2$ έχουμε $x^{1/k} \le \sqrt{x}$, άρα (μονοτονία της θ)

$$\theta(x^{1/k}) \le \theta(\sqrt{x}) \quad \text{για κάθε } k \ge 2.$$

Επομένως

$$\psi(x) - \theta(x) \le \theta(\sqrt{x}) \cdot \frac{\log x}{\log 2}.$$

Τέλος,

$$\theta(\sqrt{x}) = \sum_{p \le \sqrt{x}} \log p \le \sum_{p \le \sqrt{x}} \log \sqrt{x} \le \sqrt{x} \log \sqrt{x}.$$

Άρα

$$\psi(x) - \theta(x) \le \sqrt{x} \log \sqrt{x} \cdot \frac{\log x}{\log 2} = \sqrt{x} \cdot \frac{(\log x)^2}{2 \log 2},$$

που είναι ακριβώς το (2). □

Λήμμα 1.6. *Για $x \ge 3$ ισχύει*

$$\int_2^x \frac{dt}{\log t} \le \frac{C_1 x}{\log x}, \qquad \int_2^x \frac{dt}{(\log t)^2} \le \frac{C_2 x}{(\log x)^2}.$$

Απόδειξη. Θέτουμε $u = \sqrt{x}$. Για $t \in [u, x]$ έχουμε $\log t \ge \log u = \frac{1}{2} \log x$. Άρα

$$\int_2^x \frac{dt}{\log t} = \int_2^u \frac{dt}{\log t} + \int_u^x \frac{dt}{\log t} \le \frac{u-2}{\log 2} + \frac{x-u}{\frac{1}{2}\log x} = \mathcal{O}\left(\sqrt{x} + \frac{x}{\log x}\right) = \mathcal{O}\left(\frac{x}{\log x}\right).$$

Ομοίως,

$$\int_2^x \frac{dt}{(\log t)^2} \le u + \frac{x-u}{(\frac{1}{2}\log x)^2} \ll \sqrt{x} + \frac{x}{(\log x)^2} \ll \frac{x}{(\log x)^2}.$$

□

Θεώρημα 1.7. *Οι παρακάτω προτάσεις είναι ισοδύναμες:*

$$\pi(x) \sim \frac{x}{\log x}, \tag{3}$$

$$\theta(x) \sim x, \tag{4}$$

$$\psi(x) \sim x. \tag{5}$$

Απόδειξη. Από το Θεώρημα 1.4 έχουμε, για $x \ge 2$,

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

Διαιρώντας με x και γράφοντας $\frac{\pi(x)\log x}{x} = \frac{\pi(x)}{x/\log x}$ παίρνουμε

$$\frac{\theta(x)}{x} = \frac{\pi(x)}{x/\log x} - \frac{1}{x}\int_2^x \frac{\pi(t)}{t}\, dt. \tag{6}$$

(3) $\implies$ (4). Υποθέτουμε ότι $\pi(x) \sim x/\log x$. Τότε υπάρχει σταθερά $C > 0$ ώστε για t μεγάλα

$$\pi(t) \le C\frac{t}{\log t}.$$

Άρα

$$\frac{1}{x}\int_2^x \frac{\pi(t)}{t}\, dt \ll \frac{1}{x}\int_2^x \frac{dt}{\log t} \ll \frac{1}{\log x}.$$

Συνεπώς

$$\frac{1}{x}\int_2^x \frac{\pi(t)}{t}\, dt \longrightarrow 0 \qquad (x \to \infty).$$

Επιστρέφοντας στην (6) και χρησιμοποιώντας ότι $\frac{\pi(x)}{x/\log x} \to 1$, παίρνουμε $\frac{\theta(x)}{x} \to 1$, δηλαδή $\theta(x) \sim x$.

(4) $\Longrightarrow$ (3). Από το Θεώρημα 1.4έχουμε επίσης

$$\pi(x) = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t(\log t)^2}\, dt,$$

άρα

$$\frac{\pi(x)}{x/\log x} = \frac{\theta(x)}{x} + \frac{\log x}{x}\int_2^x \frac{\theta(t)}{t(\log t)^2}\, dt. \tag{7}$$

Υποθέτουμε $\theta(x) \sim x$. Τότε υπάρχει σταθερά $C > 0$ ώστε για t μεγάλα $\theta(t) \le Ct$. Έτσι

$$\frac{\log x}{x}\int_2^x \frac{\theta(t)}{t(\log t)^2}\, dt \ll \frac{\log x}{x}\int_2^x \frac{dt}{(\log t)^2} \ll \frac{1}{\log x}.$$

Στην (7) λοιπόν, ο δεύτερος όρος τείνει στο 0 και ο πρώτος τείνει στο 1, οπότε $\frac{\pi(x)}{x/\log x} \to 1$, δηλαδή $\pi(x) \sim x/\log x$.

(5) $\Longleftrightarrow$ (4). Από το Θεώρημα 1.5 ισχύει $0 \le \psi(x) - \theta(x) \le C\sqrt{x}(\log x)^2$ για $x \ge 2$. Διαιρώντας με x παίρνουμε

$$\lim_{x\to\infty}\left(\frac{\psi(x)}{x} - \frac{\theta(x)}{x}\right) = 0.$$

Άρα $\theta(x) \sim x$ αν και μόνο αν $\psi(x) \sim x$.

Συμπεραίνουμε ότι (3), (4), (5) είναι ισοδύναμες. □

Εφόσον θέλουμε να αποδείξουμε ότι $\psi(x) \sim x$, κάνουμε την πρώτη βασική αναγωγή, με βάση το παρακάτω Θεώρημα.

Θεώρημα 1.8 (Korevaar–Zagier). *Έστω $(a_n)_{n\ge1}$ ακολουθία με $a_n \ge 0$ και ορίζουμε, για $x \ge 1$,*

$$A(x) := \sum_{n\le x} a_n.$$

Αν το γενικευμένο ολοκλήρωμα

$$\int_1^\infty \frac{A(x) - x}{x^2}\, dx$$

συγκλίνει, τότε $A(x) \sim x$, καθώς $x \to \infty$.

Απόδειξη. Θέτουμε

$$I(y) = \int_y^\infty \frac{A(t) - t}{t^2}\, dt.$$

Η υπόθεση ότι $\int_1^\infty \frac{A(t)-t}{t^2}\, dt$ συγκλίνει ισοδυναμεί με $I(y) \to 0$. Θα αποδείξουμε ότι $A(x)/x \to 1$.

Υποθέτουμε, προς άτοπο, ότι $\limsup_{x\to\infty} A(x)/x > 1$. Τότε υπάρχει $\lambda > 1$ και άπειρα x με $A(x) \ge \lambda x$. Για τέτοιο x και κάθε $t \in [x, \lambda x]$ ισχύει $A(t) \ge A(x) \ge \lambda x$, άρα

$$I(x) - I(\lambda x) = \int_x^{\lambda x} \frac{A(t) - t}{t^2}\, dt \ge \int_x^{\lambda x} \frac{\lambda x - t}{t^2}\, dt.$$

Με την αλλαγή μεταβλητής $t = vx$ παίρνουμε

$$\int_x^{\lambda x} \frac{\lambda x - t}{t^2}\, dt = \int_1^\lambda \frac{\lambda - v}{v^2}\, dv = \lambda - 1 - \log\lambda > 0.$$

Όμως $I(x) \to 0$ και $I(\lambda x) \to 0$, άρα $I(x) - I(\lambda x) \to 0$, άτοπο. Ανάλογα αποκλείεται και η σχέση $\liminf_{x\to\infty} A(x)/x < 1$. Άρα $A(x)/x \to 1$. □

1.2 Ένα φυσικό αντικείμενο: Mellin–τύπου ολοκλήρωμα

Για $\sigma > 1$ ορίζουμε

$$F(\sigma) := \int_1^\infty \frac{\psi(x) - x}{x^{\sigma+1}}\, dx. \tag{8}$$

Τυπικά,

$$F(1) = \int_1^\infty \frac{\psi(x) - x}{x^2}\, dx,$$

άρα το ερώτημα είναι αν το $F(\sigma)$ μπορεί να «κατέβει» μέχρι $\sigma = 1$ με πεπερασμένη τιμή. Προς το παρόν εργαζόμαστε μόνο στο $\sigma > 1$, όπου όλα είναι απολύτως νόμιμα.

1.3 Η σύνδεση με την συνάρτηση Mangoldt

Λήμμα 1.9. *Για κάθε $\sigma > 1$ ισχύει*

$$\int_1^\infty \frac{\psi(x)}{x^{\sigma+1}}\, dx = \frac{1}{\sigma} \sum_{n=1}^\infty \frac{\Lambda(n)}{n^\sigma}.$$

Απόδειξη. Από τον ορισμό $\psi(x) = \sum_{n \le x} \Lambda(n)$ και επειδή $\Lambda(n) \ge 0$, μπορούμε να εφαρμόσουμε Tonelli και να ανταλλάξουμε άθροισμα–ολοκλήρωμα:

$$\begin{aligned}\int_1^\infty \frac{\psi(x)}{x^{\sigma+1}}\, dx &= \int_1^\infty \left(\sum_{n \le x} \Lambda(n) \right) x^{-\sigma-1}\, dx \\ &= \sum_{n=1}^\infty \Lambda(n) \int_1^\infty \mathbf{1}_{\{n \le x\}}\, x^{-\sigma-1}\, dx = \sum_{n=1}^\infty \Lambda(n) \int_n^\infty x^{-\sigma-1}\, dx.\end{aligned}$$

Για $\sigma > 0$ έχουμε

$$\int_n^\infty x^{-\sigma-1}\, dx = \frac{1}{\sigma} n^{-\sigma},$$

οπότε παίρνουμε το ζητούμενο. □

Επιπλέον για κάθε $\sigma > 1$ ισχύει

$$\int_1^\infty \frac{x}{x^{\sigma+1}}\, dx = \int_1^\infty x^{-\sigma}\, dx = \frac{1}{\sigma - 1},$$

επομένως παίρνουμε την ακόλουθη ισότητα.

Πρόταση 1.10. *Για κάθε $\sigma > 1$ ισχύει*

$$F(\sigma) = \frac{1}{\sigma} \sum_{n=1}^\infty \frac{\Lambda(n)}{n^\sigma} - \frac{1}{\sigma - 1}. \tag{9}$$

Άρα το πρόβλημά μας μεταφέρθηκε φυσικά στη μελέτη της σειράς Dirichlet

$$\sum_{n=1}^\infty \frac{\Lambda(n)}{n^\sigma}.$$

1.4 Σύνδεση με την συνάρτηση ζ

Εισάγουμε την συνάρτηση ζ ως σειρά Dirichlet:

$$\zeta(\sigma) := \sum_{n=1}^{\infty} \frac{1}{n^\sigma} \qquad (\sigma > 1). \tag{10}$$

Λήμμα 1.11 (Παραγώγιση της ζ για $\sigma > 1$). *Για κάθε $\sigma > 1$ ισχύει*

$$\zeta'(\sigma) = -\sum_{n=1}^{\infty} \frac{\log n}{n^\sigma}.$$

Απόδειξη. Για κάθε $\varepsilon > 0$ η σειρά $\sum_{n\geq 1} \frac{\log n}{n^{1+\varepsilon}}$ συγκλίνει, οπότε η σειρά των παραγώγων συγκλίνει ομοιόμορφα στο $[1+\varepsilon, \infty)$ (Weierstrass M–test). Άρα επιτρέπεται η παραγώγιση της (10) για $\sigma > 1$. □

Το κρίσιμο αριθμητικό γεγονός είναι μια ταυτότητα για τη von Mangoldt συνάρτηση.

Λήμμα 1.12 (Ταυτότητα διαιρετών για Λ). *Για κάθε ακέραιο $n \geq 1$ ισχύει*

$$\log n = \sum_{d|n} \Lambda(d). \tag{11}$$

Απόδειξη. Αν $n = \prod_{j=1}^{m} p_j^{\alpha_j}$, τότε $\log n = \sum_{j=1}^{m} \alpha_j \log p_j$. Οι διαιρέτες d του n με $\Lambda(d) \neq 0$ είναι ακριβώς οι δυνάμεις p_j^k με $1 \leq k \leq \alpha_j$, άρα

$$\sum_{d|n} \Lambda(d) = \sum_{j=1}^{m} \sum_{k=1}^{\alpha_j} \log p_j = \sum_{j=1}^{m} \alpha_j \log p_j = \log n.$$

□

Λήμμα 1.13. *Για κάθε $\sigma > 1$ η σειρά $\displaystyle\sum_{n\geq 1} \frac{\Lambda(n)}{n^\sigma}$ συγκλίνει απολύτως.*

Απόδειξη. Ισχύει $\Lambda(n) \leq \log n$, άρα

$$\sum_{n=1}^{\infty} \frac{|\Lambda(n)|}{n^\sigma} \leq \sum_{n=1}^{\infty} \frac{\log n}{n^\sigma} < \infty \qquad (\sigma > 1).$$

□

Θεώρημα 1.14. *Για κάθε $\sigma > 1$ ισχύει*

$$-\frac{\zeta'(\sigma)}{\zeta(\sigma)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^\sigma}. \tag{12}$$

Απόδειξη. Από το Λήμμα 1.11 έχουμε

$$-\zeta'(\sigma) = \sum_{n=1}^{\infty} \frac{\log n}{n^\sigma}.$$

Χρησιμοποιούμε την ταυτότητα (11):

$$-\zeta'(\sigma) = \sum_{n=1}^{\infty} \frac{1}{n^\sigma} \sum_{d|n} \Lambda(d).$$

Για $\sigma > 1$ όλοι οι όροι είναι μη αρνητικοί, οπότε (Tonelli) αναδιατάσσουμε:

$$-\zeta'(\sigma) = \sum_{d=1}^{\infty} \Lambda(d) \sum_{\substack{n \geq 1 \\ d \mid n}} \frac{1}{n^\sigma} = \sum_{d=1}^{\infty} \Lambda(d) \sum_{m=1}^{\infty} \frac{1}{(dm)^\sigma}$$
$$= \left(\sum_{d=1}^{\infty} \frac{\Lambda(d)}{d^\sigma} \right) \left(\sum_{m=1}^{\infty} \frac{1}{m^\sigma} \right) = \left(\sum_{d=1}^{\infty} \frac{\Lambda(d)}{d^\sigma} \right) \zeta(\sigma).$$

Επειδή $\zeta(\sigma) > 0$ για $\sigma > 1$, διαιρούμε και παίρνουμε την (12). □

1.5 Συμπέρασμα

Συνδυάζοντας την Πρόταση 1.10 με το Θεώρημα 1.14 παίρνουμε, για κάθε $\sigma > 1$,

$$F(\sigma) = -\frac{1}{\sigma} \frac{\zeta'(\sigma)}{\zeta(\sigma)} - \frac{1}{\sigma - 1}. \tag{13}$$

Ξεκινήσαμε από τη ψ και το κριτήριο Korevaar–Zagier, και φτάσαμε στο ότι η μελέτη της σύγκλισης του (??) ισοδυναμεί με το να καταλάβουμε τη συμπεριφορά του δεξιού μέλους του (13) καθώς $\sigma \downarrow 1$.

Γιατί *αναγκαστικά* θα περάσουμε σε μιγαδική ανάλυση.

Παρατήρηση 1.15 (Γιατί δεν αρκεί να μείνουμε στο $\sigma \in \mathbb{R}$). Μέχρι εδώ δουλέψαμε μόνο με πραγματικά $\sigma > 1$. Το επόμενο βήμα θα ήταν να περάσουμε στο

$$F(1) = \int_1^{\infty} \frac{\psi(x) - x}{x^2}\, dx,$$

αλλά αυτό *δεν* προκύπτει μόνο από τη γνώση του $F(\sigma)$ για $\sigma > 1$. Πράγματι, αν πάρουμε

$$E(x) := x \sin(\log x), \qquad F_E(\sigma) := \int_1^{\infty} \frac{E(x)}{x^{\sigma+1}}\, dx = \int_1^{\infty} \frac{\sin(\log x)}{x^\sigma}\, dx,$$

με την αλλαγή μεταβλητής $u = \log x$ προκύπτει

$$F_E(\sigma) = \int_0^{\infty} e^{-(\sigma-1)u} \sin u\, du = \frac{1}{(\sigma-1)^2 + 1},$$

άρα $\lim_{\sigma \downarrow 1} F_E(\sigma) = 1$. Πράγματι, ένας γρήγορος τρόπος για τον τελευταίο υπολογισμό είναι

$$\int_0^{\infty} e^{-(\sigma-1)u} \sin u\, du = \Im \int_0^{\infty} e^{-(\sigma-1)u} e^{iu}\, du = \Im \int_0^{\infty} e^{-(\sigma-1-i)u}\, du.$$

Για $\sigma > 1$ έχουμε $\Re(\sigma - 1 - i) = \sigma - 1 > 0$, άρα

$$\int_0^{\infty} e^{-(\sigma-1-i)u}\, du = \frac{1}{\sigma - 1 - i}.$$

Επομένως

$$\int_0^{\infty} e^{-(\sigma-1)u} \sin u\, du = \Im \frac{1}{\sigma - 1 - i} = \Im \left(\frac{\sigma - 1 + i}{(\sigma-1)^2 + 1} \right) = \frac{1}{(\sigma-1)^2 + 1}.$$

Ωστόσο

$$F_E(1) = \int_1^{\infty} \frac{\sin(\log x)}{x}\, dx = \int_0^{\infty} \sin u\, du,$$

που δεν συγκλίνει. Δηλαδή: ακόμη και πολύ καλή συμπεριφορά για όλα τα $\sigma > 1$ (και μάλιστα ύπαρξη ορίου στο $\sigma \downarrow 1$) δεν εγγυάται σύγκλιση στο $\sigma = 1$.

Η σωστή πρόσθετη πληροφορία είναι να ελέγξουμε την *οριακή ευθεία* $\Re(s) = 1$, δηλαδή τι συμβαίνει για $s = \sigma + it$. Στο παραπάνω παράδειγμα, ο αντίστοιχος μετασχηματισμός είναι

$$F_E(s) = \frac{1}{(s-1)^2 + 1},$$

που έχει πόλους στα $s = 1 \pm i$, δηλαδή πάνω στην $\Re(s) = 1$. Αυτές οι ανωμαλίες αντιστοιχούν σε ταλαντώσεις και είναι ακριβώς αυτό που πρέπει να αποκλείσουμε στην περίπτωση της ζ.

2 Επέκταση του Ορισμού της συνάρτησης ζ

Λήμμα 2.1. *Έστω $(a_n)_{n\geq 1}$ με $a_n \in \mathbb{C}$ και έστω*

$$F(s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \qquad s = \sigma + it.$$

Αν υπάρχει $\sigma_0 \in \mathbb{R}$ τέτοιο ώστε $\sum_{n=1}^{\infty} \frac{|a_n|}{n^{\sigma_0}} < \infty$, τότε για κάθε $\sigma_1 > \sigma_0$ η σειρά συγκλίνει απολύτως και ομοιόμορφα στο ημιεπίπεδο $\Re(s) \geq \sigma_1$. Επιπλέον, η F είναι ολόμορφη στο $\Re(s) > \sigma_0$ και

$$F'(s) = -\sum_{n=1}^{\infty} \frac{a_n \log n}{n^s},$$

με ομοιόμορφη σύγκλιση σε κάθε $\Re(s) \geq \sigma_1 > \sigma_0$.

Απόδειξη. Για s με $\Re(s) = \sigma \geq \sigma_1$ έχουμε

$$\left|\frac{a_n}{n^s}\right| = \frac{|a_n|}{n^{\sigma}} \leq \frac{|a_n|}{n^{\sigma_1}}.$$

Επειδή $\sum_{n\geq 1} \frac{|a_n|}{n^{\sigma_1}} < \infty$, το M-κριτήριο του Weierstrass δίνει ομοιόμορφη σύγκλιση στο $\Re(s) \geq \sigma_1$. Άρα η F είναι συνεχής εκεί.

Για την ολομορφία, παρατηρούμε ότι κάθε όρος $s \mapsto a_n n^{-s} = a_n e^{-s\log n}$ είναι ολόμορφη και για $\sigma \geq \sigma_1$ ισχύει

$$\left|\frac{a_n \log n}{n^s}\right| = \frac{|a_n| \log n}{n^{\sigma}} \leq \frac{|a_n| \log n}{n^{\sigma_1}}.$$

Αλλά για κάθε $\varepsilon > 0$ ισχύει $\log n \leq n^{\varepsilon}$ για n αρκετά μεγάλο, οπότε (π.χ. παίρνοντας $\varepsilon = (\sigma_1 - \sigma_0)/2$) η $\sum \frac{|a_n| \log n}{n^{\sigma_1}}$ συγκλίνει. Άρα η σειρά των παραγώγων συγκλίνει ομοιόμορφα όταν $\Re(s) \geq \sigma_1$. Από το Θεώρημα ?? συμπεραίνουμε ότι F είναι ολόμορφη και ότι επιτρέπεται παραγωγίση όρο-όρο. □

Πρόταση 2.2. *Για $\Re(s) > 1$ ορίζουμε*

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

Τότε η σειρά συγκλίνει απολύτως για $\Re(s) > 1$, ορίζει ολόμορφη συνάρτηση στο $\{s : \Re(s) > 1\}$, και για κάθε $\Re(s) > 1$ ισχύει

$$\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\log n}{n^s},$$

με ομοιόμορφη σύγκλιση σε κάθε ημιεπίπεδο $\Re(s) \geq 1 + \delta$ $(\delta > 0)$.

Απόδειξη. Εφαρμόζουμε το Λήμμα 2.1 με $a_n \equiv 1$ και $\sigma_0 = 1$. □

Παρατήρηση 2.3. Θέτουμε $H_1 := \{s \in \mathbb{C} : \Re(s) > 1\}$. Η σειρά

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

δεν συγκλίνει ομοιόμορφα στο H_1.

Πράγματι, έστω προς άτοπο ότι συγκλίνει ομοιόμορφα στο H_1. Τότε, από το κριτήριο Cauchy για ομοιόμορφη σύγκλιση, για $\varepsilon = 1$ υπάρχει $N \in \mathbb{N}$ τέτοιο ώστε για κάθε $\ell > k \geq N$ και κάθε $s \in H_1$ να ισχύει

$$\left| \sum_{n=k}^{\ell} \frac{1}{n^s} \right| < 1.$$

Ειδικότερα, αυτό ισχύει για κάθε *πραγματικό* $s > 1$ (αφού $(1, \infty) \subset H_1$). Για πραγματικό $s > 1$ όλοι οι όροι είναι θετικοί, άρα

$$\sum_{n=k}^{\ell} \frac{1}{n^s} < 1 \qquad (\ell > k \geq N,\ s > 1).$$

Αφήνοντας τώρα $s \to 1^+$, και χρησιμοποιώντας ότι για κάθε σταθερά ℓ, k έχουμε $\frac{1}{n^s} \to \frac{1}{n}$, παίρνουμε

$$\sum_{n=k}^{\ell} \frac{1}{n} \leq 1 \qquad (\ell > k \geq N).$$

Τέλος, αφήνοντας $\ell \to \infty$ καταλήγουμε ότι

$$\sum_{n=k}^{\infty} \frac{1}{n} \leq 1 \qquad (k \geq N),$$

άτοπο, επειδή η αρμονική σειρά αποκλίνει. Άρα η αρχική υπόθεση είναι ψευδής.

Πρόταση 2.4. *Θέτουμε*

$$F(s) := \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

Τότε η F είναι καλά ορισμένη και ολόμορφη στο $\Re(s) > 1$, και

$$F'(s) = -\sum_{n=1}^{\infty} \frac{\Lambda(n) \log n}{n^s},$$

με ομοιόμορφη σύγκλιση σε κάθε $\Re(s) \geq 1 + \delta$.

Απόδειξη. Χρησιμοποιούμε ότι $0 \leq \Lambda(n) \leq \log n$ για κάθε $n \geq 2$. Για $\sigma > 1$ έχουμε

$$\sum_{n=2}^{\infty} \frac{|\Lambda(n)|}{n^\sigma} \leq \sum_{n=2}^{\infty} \frac{\log n}{n^\sigma} < \infty,$$

άρα εφαρμόζουμε το Λήμμα 2.1 με $\sigma_0 = 1$. □

Πρόταση 2.5. *Θεωρούμε το ημιεπίπεδο $\Omega := \{s \in \mathbb{C} : \Re(s) > 1\}$. Υποθέτουμε ότι για κάθε πραγματικό $s > 1$ έχει ήδη αποδειχθεί η ταυτότητα*

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

Τότε η ίδια ταυτότητα ισχύει για κάθε μιγαδικό $s \in \Omega$.

Απόδειξη. Από την Πρόταση 2.2 η ζ και η ζ' είναι ολόμορφες στο Ω. Από την Πρόταση 2.4 η

$$F(s) := \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$$

είναι ολόμορφη στο Ω. Άρα και το γινόμενο $\zeta(s)F(s)$ είναι ολόμορφη συνάρτηση στο Ω.

Ορίζουμε την ολόμορφη συνάρτηση

$$H(s) := -\zeta'(s) - \zeta(s)F(s) \qquad (s \in \Omega).$$

Από την υπόθεση, για κάθε πραγματικό $s > 1$ ισχύει $H(s) = 0$. Το σύνολο $(1, \infty) \subset \Omega$ έχει σημείο συσσώρευσης *εντός* του Ω (π.χ. στο $s = 2$), άρα από την Αρχή Αναλυτικής Συνέχισης (Identity Theorem) συμπεραίνουμε ότι $H \equiv 0$ σε όλο το Ω. Δηλαδή

$$-\zeta'(s) = \zeta(s) \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s},$$

για κάθε $s \in \Omega$.

□

Λήμμα 2.6. *Έστω $\Omega \subset \mathbb{C}$ ανοικτό, $s_0 \in \Omega$ και $f : \Omega \to \mathbb{C}$ ολόμορφη. Υποθέτουμε ότι $f \not\equiv 0$ και ότι $f(s_0) = 0$. Τότε υπάρχει ακέραιος $m \geq 1$ και ολόμορφη συνάρτηση h σε κάποια γειτονιά του s_0 με $h(s_0) \neq 0$ τέτοια ώστε*

$$f(s) = (s - s_0)^m h(s)$$

για s κοντά στο s_0. Ο m είναι μοναδικός και λέγεται τάξη (ή πολλαπλότητα) του μηδενικού στο s_0.

Απόδειξη. Επειδή f είναι ολόμορφη, υπάρχει $r > 0$ και ανάπτυγμα Taylor

$$f(s) = \sum_{n=0}^{\infty} a_n (s - s_0)^n \qquad (|s - s_0| < r).$$

Από $f(s_0) = 0$ παίρνουμε $a_0 = 0$. Επειδή $f \not\equiv 0$, δεν είναι όλοι οι συντελεστές μηδέν, άρα υπάρχει ελάχιστος $m \geq 1$ με $a_m \neq 0$. Τότε

$$f(s) = \sum_{n=m}^{\infty} a_n (s - s_0)^n = (s - s_0)^m \sum_{k=0}^{\infty} a_{m+k} (s - s_0)^k.$$

Θέτουμε

$$h(s) := \sum_{k=0}^{\infty} a_{m+k} (s - s_0)^k.$$

Η h είναι ολόμορφη στο $|s - s_0| < r$ και $h(s_0) = a_m \neq 0$. Η μοναδικότητα του m προκύπτει από τη μοναδικότητα του Taylor αναπτύγματος. □

Θεώρημα 2.7. *Για κάθε s με $\Re(s) > 1$ ισχύει $\zeta(s) \neq 0$.*

Απόδειξη. Έστω προς άτοπο ότι υπάρχει s_0 με $\Re(s_0) > 1$ και $\zeta(s_0) = 0$. Η ζ είναι ολόμορφη στο $\Re(s) > 1$, άρα το s_0 είναι μηδενικό κάποιας τάξης $m \geq 1$, δηλαδή υπάρχει ολόμορφη h κοντά στο s_0 με $h(s_0) \neq 0$ ώστε

$$\zeta(s) = (s - s_0)^m h(s).$$

Τότε

$$\zeta'(s) = m(s-s_0)^{m-1}h(s) + (s-s_0)^m h'(s),$$

οπότε η $\zeta'(s)$ έχει μηδενικό ακριβώς τάξης $m-1$ στο s_0. Ισοδύναμα, $-\zeta'(s)$ έχει μηδενικό ακριβώς τάξης $m-1$ στο s_0.

Από την Πρόταση 2.5 έχουμε στο $\Re(s) > 1$ την ταυτότητα

$$-\zeta'(s) = \zeta(s)\,F(s), \qquad F(s) := \sum_{n\geq 1} \frac{\Lambda(n)}{n^s}.$$

Η F είναι ολόμορφη στο $\Re(s) > 1$ (από απόλυτη σύγκλιση), άρα κοντά στο s_0 είναι πεπερασμένη. Επομένως το γινόμενο $\zeta(s)F(s)$ έχει μηδενικό τάξης *τουλάχιστον* m στο s_0, αφού η ζ έχει τάξη m εκεί.

Άρα το αριστερό μέλος $-\zeta'(s)$ θα έπρεπε να έχει μηδενικό τάξης $\geq m$ στο s_0, που αντιφάσκει με το ότι έχει τάξη ακριβώς $m-1$. Άτοπο. Συνεπώς $\zeta(s) \neq 0$ για $\Re(s) > 1$. □

2.1 Μερομορφική συνέχεια της $\zeta(s)$ στο $\Re(s) > 0$

Θεώρημα 2.8. *Για $s \in \mathbb{C}$ με $\sigma = \mathrm{Re}(s) > 1$ ισχύει*

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

Απόδειξη. Απ τον τύπο αθροίσεως του Euler, παίρνουμε

$$\sum_{n\leq x} n^{-s} = 1 + \int_1^x t^{-s}\,dt + \int_1^x \{t\}\,(t^{-s})'\,dt - \frac{\{x\}}{x^s}.$$

Υπολογίζοντας τα παραπάνω ολοκληρώματα καταλήγουμε στην ισότητα

$$\sum_{n\leq x} n^{-s} = \frac{x^{1-s}}{1-s} + \frac{s}{s-1} - \frac{\{x\}}{x^s} - s\int_1^x \frac{\{t\}}{t^{s+1}}\,dt.$$

Περνώντας στο όριο $x \to \infty$ (και χρησιμοποιώντας ότι $\sigma > 1$ ώστε $x^{1-s} \to 0$ και $\{x\}/x^s \to 0$), παίρνουμε το ζητούμενο. □

Θεώρημα 2.9. *Η σχέση του Θεωρήματος 2.8 δίνει αναλυτική συνέχιση της $\zeta(s)$ στο ημιεπίπεδο $\sigma > 0$, με απλό πόλο στο $s = 1$ και υπόλοιπο 1.*

Απόδειξη. Εφόσον η συνάρτηση

$$s \longmapsto \frac{s}{s-1} = \frac{1}{s-1} + 1$$

είναι αναλυτική σε κάθε σημείο του $\sigma > 0$ εκτός από έναν απλό πόλο στο $s = 1$ με υπόλοιπο 1, αρκεί να δείξουμε ότι η συνάρτηση

$$f(s) = \int_1^\infty \frac{\{t\}}{t^{s+1}}\,dt$$

είναι αναλυτική στο $\sigma > 0$.

Για κάθε $m \in \mathbb{N}$ ορίζουμε

$$f_m(s) = \int_1^m \frac{\{t\}}{t^{s+1}}\,dt \qquad \text{για } s \in \mathbb{C} \text{ με } \sigma > 0.$$

Επειδή το ολοκληρωτέο είναι αναλυτική συνάρτηση του s, δεν είναι δύσκολο να δούμε ότι f_m είναι αναλυτική στο ημιεπίπεδο $\sigma > 0$.

Εναλλακτικά, γράφουμε το $f_m(s)$ ως δυναμοσειρά. Παρατηρούμε ότι

$$f_m(s) = \int_1^m \{t\}\, e^{-(s+1)\log t}\, dt = \int_1^m \sum_{n=0}^{\infty} \frac{\{t\}\,(-\log t)^n (s+1)^n}{n!}\, dt,$$

και ότι

$$\sum_{n=0}^{\infty} \left| \frac{\{t\}\,(-\log t)^n (s+1)^n}{n!} \right| \le \sum_{n=0}^{\infty} \frac{\big(|\log t|(|s|+1)\big)^n}{n!} = e^{|\log t|(|s|+1)}.$$

Άρα

$$\int_1^m \sum_{n=0}^{\infty} \left| \frac{\{t\}\,(-\log t)^n (s+1)^n}{n!} \right| dt \le \int_1^m t^{|s|+1}\, dt < \infty.$$

Με το θεώρημα Fubini, μπορούμε να αλλάξουμε τη σειρά ολοκλήρωσης και αθροίσεως και παίρνουμε

$$f_m(s) = \sum_{n=0}^{\infty} \frac{(s+1)^n}{n!} \int_1^m \{t\}\,(-\log t)^n\, dt,$$

που είναι δυναμοσειρά ως προς το s.

Για να δούμε ότι $f_m \to f$ ομοιόμορφα σε κάθε συμπαγές υποσύνολο του $\sigma > 0$, θεωρούμε το ημιεπίπεδο $\sigma \ge \delta$ και παίρνουμε

$$|f_m(s) - f(s)| \le \int_m^{\infty} \frac{1}{t^{\sigma+1}}\, dt \ll \frac{1}{\sigma m^{\sigma}} \le \frac{1}{\delta m^{\delta}}.$$

Άρα, αν $\varepsilon, \delta > 0$ δοθούν, μπορούμε να διαλέξουμε $M > 0$ που εξαρτάται από ε, δ αλλά όχι από το s (π.χ. $M = (\delta\varepsilon)^{-1/\delta}$) τέτοιο ώστε $|f_m(s) - f(s)| < \varepsilon$ για κάθε $m > M$ και κάθε $s \in \mathbb{C}$ με $\sigma \ge \delta$. Αυτό ολοκληρώνει την απόδειξη. □

2.2 Μη μηδενισμός της ζ στη γραμμή $\Re(s) = 1$

Λήμμα 2.10. *Για $\Re(s) > 1$ ισχύει*

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s},$$

και η σειρά συγκλίνει απολύτως και ομοιόμορφα σε κάθε ημιεπίπεδο $\Re(s) \ge 1 + \varepsilon$.

Απόδειξη. Προκύπτει άμεσα από τα παραπάνω. □

Λήμμα 2.11. *Για κάθε $\theta \in \mathbb{R}$ ισχύει*

$$P(\theta) := 3 + 4\cos\theta + \cos(2\theta) = 2(1 + \cos\theta)^2 \ge 0.$$

Λήμμα 2.12. *Έστω $t \in \mathbb{R} \setminus \{0\}$. Για $\sigma > 1$ θέτουμε*

$$G(\sigma) := \big|\zeta(\sigma)\big|^3 \big|\zeta(\sigma + it)\big|^4 \big|\zeta(\sigma + 2it)\big|.$$

Τότε:

1. *$G(\sigma) \ge 1$ για κάθε $\sigma > 1$.*

2. *Πιο συγκεκριμένα,*

$$-\frac{d}{d\sigma}\log G(\sigma) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^{\sigma}}\, P\big(t\log n\big) \;\geq\; 0,$$

όπου P είναι όπως στο Λήμμα 2.11.

Απόδειξη. Για $\sigma > 1$ έχουμε $\zeta(\sigma) \neq 0$, άρα οι ποσότητες ζ'/ζ ορίζονται και είναι ολόμορφες.

Βήμα 1: Παράγωγος του $\log G(\sigma)$. Για κάθε $u \in \mathbb{R}$ και $\sigma > 1$ ισχύει

$$\frac{d}{d\sigma}\log|\zeta(\sigma+iu)| = \Re\left(\frac{\zeta'}{\zeta}(\sigma+iu)\right).$$

Πράγματι, γράφουμε

$$\zeta(\sigma+it) = u(\sigma,t) + iv(\sigma,t), \qquad u, v : \Omega \to \mathbb{R},$$

και υποθέτουμε ότι $\zeta(\sigma+it) \neq 0$. Τότε

$$\log|\zeta(\sigma+it)| = \frac{1}{2}\log\big(u(\sigma,t)^2 + v(\sigma,t)^2\big),$$

οπότε, για t σταθερό,

$$\frac{\partial}{\partial\sigma}\log|\zeta(\sigma+it)| = \frac{u\,u_\sigma + v\,v_\sigma}{u^2+v^2}.$$

Από την άλλη, επειδή η ζ είναι ολόμορφη, έχουμε

$$\zeta'(\sigma+it) = u_\sigma(\sigma,t) + i\,v_\sigma(\sigma,t),$$

άρα

$$\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)} = \frac{u_\sigma + iv_\sigma}{u+iv} = \frac{(u_\sigma+iv_\sigma)(u-iv)}{u^2+v^2} = \frac{u\,u_\sigma + v\,v_\sigma}{u^2+v^2} + i\,\frac{u\,v_\sigma - v\,u_\sigma}{u^2+v^2}.$$

Συνεπώς

$$\mathrm{Re}\left(\frac{\zeta'(\sigma+it)}{\zeta(\sigma+it)}\right) = \frac{u\,u_\sigma + v\,v_\sigma}{u^2+v^2} = \frac{\partial}{\partial\sigma}\log|\zeta(\sigma+it)|.$$

Επειδή $\big(\log\zeta\big)' = \zeta'/\zeta$ όπου $\zeta \neq 0$, καταλήγουμε

$$\frac{\partial}{\partial\sigma}\log|\zeta(\sigma+it)| = \mathrm{Re}\big((\log\zeta)'(\sigma+it)\big).$$

Άρα

$$\frac{d}{d\sigma}\log G(\sigma) = 3\,\Re\left(\frac{\zeta'}{\zeta}(\sigma)\right) + 4\,\Re\left(\frac{\zeta'}{\zeta}(\sigma+it)\right) + \Re\left(\frac{\zeta'}{\zeta}(\sigma+2it)\right).$$

Επομένως

$$-\frac{d}{d\sigma}\log G(\sigma) = 3\,\Re\left(-\frac{\zeta'}{\zeta}(\sigma)\right) + 4\,\Re\left(-\frac{\zeta'}{\zeta}(\sigma+it)\right) + \Re\left(-\frac{\zeta'}{\zeta}(\sigma+2it)\right).$$

Βήμα 2: Χρήση της Dirichlet σειράς (Λήμμα 2.10). Για $\sigma > 1$ έχουμε

$$-\frac{\zeta'}{\zeta}(\sigma+iu) = \sum_{n\geq 1}\frac{\Lambda(n)}{n^{\sigma+iu}} = \sum_{n\geq 1}\frac{\Lambda(n)}{n^{\sigma}}\,e^{-iu\log n},$$

και επειδή η σύγκλιση είναι απόλυτη, παίρνουμε πραγματικά μέρη όρο-όρο:

$$\Re\left(-\frac{\zeta'}{\zeta}(\sigma+iu)\right)=\sum_{n\geq 1}\frac{\Lambda(n)}{n^{\sigma}}\cos(u\log n).$$

Άρα

$$-\frac{d}{d\sigma}\log G(\sigma)=\sum_{n\geq 1}\frac{\Lambda(n)}{n^{\sigma}}\Big(3+4\cos(t\log n)+\cos(2t\log n)\Big)=\sum_{n\geq 1}\frac{\Lambda(n)}{n^{\sigma}}\,P\big(t\log n\big).$$

Με το Λήμμα 2.11 έχουμε $P(\cdot)\geq 0$ και με $\Lambda(n)\geq 0$ παίρνουμε

$$-\frac{d}{d\sigma}\log G(\sigma)\geq 0.$$

Άρα $\frac{d}{d\sigma}\log G(\sigma)\leq 0$, δηλαδή η $\log G$ είναι φθίνουσα ως προς σ.

Βήμα 3: Πέρασμα στο όριο $\sigma\to\infty$**.** Για κάθε σταθερό u έχουμε

$$\zeta(\sigma+iu)=1+\sum_{n\geq 2}n^{-(\sigma+iu)}\quad\Rightarrow\quad\big|\zeta(\sigma+iu)-1\big|\leq\sum_{n\geq 2}n^{-\sigma}\xrightarrow[\sigma\to\infty]{}0.$$

Άρα $\zeta(\sigma+iu)\to 1$, οπότε $G(\sigma)\to 1$ όταν $\sigma\to\infty$. Επειδή $\log G$ είναι φθίνουσα στο σ, έχουμε για κάθε $\sigma>1$:

$$\log G(\sigma)\geq\lim_{\sigma\to\infty}\log G(\sigma)=0,$$

δηλαδή $G(\sigma)\geq 1$. □

Θεώρημα 2.13. *Ισχύει $\zeta(s)\neq 0$ για κάθε $s\in\mathbb{C}$ με $\Re(s)=1$.*

Απόδειξη. Θα δείξουμε ότι $\zeta(1+it)\neq 0$ για κάθε $t\in\mathbb{R}$. Υποθέτουμε, προς άτοπο, ότι

$$\zeta(1+it)=0.$$

Από το Θεώρημα 2.9, η $\zeta(s)$ είναι αναλυτική σε κάθε σημείο της ευθείας $\Re(s)=1$ εκτός από ένα απλό πόλο στο $s=1$. Άρα $\zeta^3(\sigma)$ έχει πόλο τάξης 3 στο $\sigma=1$ και επίσης $\zeta^4(\sigma+it)$ έχει μηδενικό τάξης τουλάχιστον 4 στο $\sigma=1$ (δηλαδή στο σημείο $s=1+it$). Συνεπώς

$$\lim_{\sigma\to 1^+}\zeta^4(\sigma+it)\,\zeta^3(\sigma)=0.$$

Επιπλέον, επειδή ζ είναι αναλυτική στο σημείο $1+2it$ (αφού $t\neq 0$), είναι και συνεχής εκεί, οπότε

$$\lim_{\sigma\to 1^+}\zeta(\sigma+2it)=\zeta(1+2it).$$

Άρα

$$\lim_{\sigma\to 1^+}\zeta^4(\sigma+it)\,\zeta^3(\sigma)\,\zeta(\sigma+2it)=0.$$

Όμως, από το Λήμμα 2.12 ισχύει ότι για κάθε $\sigma>1$,

$$\big|\zeta^4(\sigma+it)\,\zeta^3(\sigma)\,\zeta(\sigma+2it)\big|\geq 1.$$

Επομένως το όριο καθώς $\sigma\to 1^+$ δεν μπορεί να είναι 0, που είναι άτοπο. Άρα η υπόθεση $\zeta(1+it)=0$ είναι ψευδής, και συνεπώς $\zeta(1+it)\neq 0$ για κάθε $t\neq 0$. Μαζί με το $t=0$ (όπου υπάρχει πόλος), παίρνουμε ότι $\zeta(s)\neq 0$ για κάθε s με $\Re(s)=1$. □

Παρατήρηση 2.14. Γιατί επιλέξαμε *αυτές* τις δυνάμεις; Το τρικ βασίζεται σε δύο *ταυτόχρονες* απαιτήσεις:

(i) Θέλουμε μη αρνητικότητα. Θέλουμε ένα τριγωνομετρικό πολυώνυμο $P(\theta)$ τέτοιο ώστε

$$P(\theta) = a_0 + a_1 \cos\theta + a_2 \cos(2\theta) \geq 0 \quad \forall \theta,$$

για να συμπεράνουμε ότι

$$-\frac{d}{d\sigma} \log G(\sigma) = \sum_{n \geq 1} \frac{\Lambda(n)}{n^\sigma} P(t \log n) \geq 0.$$

Το απλούστερο "τετράγωνο" που δίνει πολυώνυμο μέχρι βαθμό 2 είναι

$$(1 + \cos\theta)^2 = \frac{1}{2}\Big(3 + 4\cos\theta + \cos(2\theta)\Big).$$

Για να πάρουμε *ακέραιους* συντελεστές (ώστε να αντιστοιχούν σε *ακέραιες* δυνάμεις της ζ), πολλαπλασιάζουμε επί 2 και παίρνουμε ακριβώς

$$P(\theta) = 3 + 4\cos\theta + \cos(2\theta) = 2(1 + \cos\theta)^2 \geq 0.$$

Αυτό εξηγεί το σχήμα των δυνάμεων $3, 4, 1$.

(ii) Θέλουμε το μηδενικό να "νικάει" τον πόλο στο 1. Κοντά στο $\sigma = 1$ έχουμε $|\zeta(\sigma)| \asymp (\sigma - 1)^{-1}$ (πόλος τάξης 1), ενώ αν υπήρχε μηδενικό στο $1 + it$ τάξης $m \geq 1$ τότε $|\zeta(\sigma + it)| \ll (\sigma - 1)^m$. Άρα, αν πάρεις

$$|\zeta(\sigma)|^{a_0} \, |\zeta(\sigma + it)|^{a_1}$$

με *ίδιους* εκθέτες $a_0 = a_1$ (όπως θα προέκυπτε από το πολυώνυμο $1 + \cos\theta$ ή $2 + 2\cos\theta$), τότε για απλό μηδενικό ($m = 1$) θα έχεις εκθέτη

$$-(a_0) + a_1 m = -a_0 + a_0 \cdot 1 = 0,$$

δηλαδή το γινόμενο *δεν* τείνει αναγκαστικά στο 0 όταν $\sigma \downarrow 1$, άρα δεν παίρνεις αντίφαση από το $G(\sigma) \geq 1$.

Στο δικό μας $G(\sigma)$ οι εκθέτες είναι $a_0 = 3$ για τον πόλο στο $s = 1$ και $a_1 = 4$ για το υποτιθέμενο μηδενικό στο $1 + it$. Τότε για $m = 1$ παίρνεις

$$-3 + 4 \cdot 1 = 1 > 0,$$

οπότε *αναγκαστικά* $G(\sigma) \to 0$ αν υπήρχε μηδενικό, και έτσι κλείνει η αντίφαση. Γι' αυτό οι "συγκεκριμένες" δυνάμεις είναι ακριβώς αυτές που χρειάζονται: προέρχονται από *τετράγωνο* (άρα μη αρνητικότητα) και ταυτόχρονα έχουν $4 > 3$ (άρα το μηδενικό υπερισχύει του πόλου).

3 Το «μιγαδικό» Korevaar–Zagier

Θεώρημα 3.1 (Korevaar–Zagier). *Έστω $f : [0, \infty) \to \mathbb{C}$ φραγμένη και ολοκληρώσιμη σε κάθε κλειστό φραγμένο υποδιάστημα του $[0, \infty)$. Θέτουμε*

$$g(s) := \int_0^\infty f(x) e^{-sx} \, dx \qquad (\mathrm{Re}(s) > 0).$$

Υποθέτουμε ότι υπάρχει ανοικτό σύνολο $G \subset \mathbb{C}$ με $\{\, \mathrm{Re}(s) \geq 0 \,\} \subset G$ και ολόμορφη επέκταση της g στο G (την οποία συμβολίζουμε πάλι με g). Τότε το αόριστο ολοκλήρωμα

$$\int_0^\infty f(x) \, dx$$

συγκλίνει και ισχύει

$$\int_0^\infty f(x) \, dx = g(0).$$

Απόδειξη. Θέτουμε $M := \sup_{x\ge 0} |f(x)| < \infty$. Για $T > 0$ ορίζουμε

$$g_T(s) := \int_0^T f(x) e^{-sx}\, dx \qquad (s \in \mathbb{C}).$$

1) Το g_T είναι ολόμορφο (entire). Για κάθε $s \in \mathbb{C}$ το $x \mapsto f(x)e^{-sx}$ είναι ολοκληρώσιμο στο $[0,T]$, άρα το $g_T(s)$ ορίζεται. Επιπλέον, για $h \neq 0$ γράφουμε

$$\frac{g_T(s+h) - g_T(s)}{h} = \int_0^T f(x) e^{-sx}\, \frac{e^{-hx} - 1}{h}\, dx.$$

Για σταθερό s και για h μικρό, ισχύει (με το θεώρημα μέσης τιμής στην πραγματική μεταβλητή)

$$\left| \frac{e^{-hx} - 1}{h} \right| \le x\, e^{|h|x} \le x\, e^{x} \qquad (0 \le x \le T),$$

οπότε το ολοκληρωτέο κυριαρχείται από την ολοκληρώσιμη συνάρτηση $M\, x\, e^x e^{|s|x}$, όπου $M = \sup_{[0,T]} |f|$. Άρα, από το θεώρημα κυριαρχημένης σύγκλισης, μπορούμε να περάσουμε στο όριο $h \to 0$ μέσα στο ολοκλήρωμα και παίρνουμε

$$g_T'(s) = \int_0^T f(x) e^{-sx} \lim_{h\to 0} \frac{e^{-hx} - 1}{h}\, dx = -\int_0^T x f(x) e^{-sx}\, dx.$$

Επομένως g_T είναι μιγαδικά παραγωγίσιμη σε κάθε $s \in \mathbb{C}$, άρα ολόμορφη στο $\mathbb{C}$.
2) Στόχος. Αρκεί να δείξουμε ότι $g_T(0) \to g(0)$ όταν $T \to \infty$. Πράγματι, $g_T(0) = \int_0^T f(x)\, dx$, άρα το $\int_0^\infty f$ συγκλίνει και ισούται με $g(0)$.
3) Επιλογή καμπύλης ολοκλήρωσης γύρω από το 0. Σταθεροποιούμε $R > 0$. Θέτουμε

$$L_R := \{\, it : \ |t| \le 2R \,\} \subset \{\, \mathrm{Re}(s) = 0 \,\} \subset G.$$

Για κάθε σημείο $z \in L_R$ υπάρχει ανοικτός δίσκος $B(z, r_z) \subset G$ (επειδή το G είναι ανοικτό). Από συμπάγεια του L_R (Heine–Borel) παίρνουμε πεπερασμένη υποκάλυψη, άρα υπάρχει $\delta = \delta(R) > 0$ τέτοια ώστε

$$D := \{\, z \in \mathbb{C} : \ |z| < 2R,\ \mathrm{Re}(z) > -2\delta \,\} \subset G.$$

Τότε επίσης η κλειστή καμπύλη

$$C := \partial\{\, z \in \mathbb{C} : \ |z| \le R,\ \mathrm{Re}(z) \ge -\delta \,\}$$

βρίσκεται μέσα στο D και περικλείει το 0. (Γεωμετρικά: είναι *τόξο* του κύκλου $|z| = R$ για $\mathrm{Re}(z) \ge -\delta$ μαζί με τη *χορδή* $\mathrm{Re}(z) = -\delta$.)
4) Τύπος Cauchy για $g - g_T$ και «κόλπο» Carleman. Η συνάρτηση $h_T(z) := g(z) - g_T(z)$ είναι ολόμορφη στο D (ως διαφορά δύο ολόμορφων). Άρα από τον τύπο του Cauchy στο 0 παίρνουμε

$$g(0) - g_T(0) = \frac{1}{2\pi i} \int_C \frac{g(z) - g_T(z)}{z}\, dz. \tag{14}$$

Παρατηρούμε τώρα ότι:

- Η $(g - g_T)(z) e^{z^T}$ είναι ολόμορφη στο D και στο $z = 0$ έχει την ίδια τιμή με $g - g_T$.
- Η $(g - g_T)(z) e^{z^T} \cdot \dfrac{z}{R^2}$ είναι επίσης ολόμορφη στο D, άρα το ολοκλήρωμά της πάνω στο C είναι 0.

Συνεπώς, προσθέτοντας το μηδέν στο (14), παίρνουμε την ισοδυναμία

$$g(0) - g_T(0) = \frac{1}{2\pi i} \int_C (g(z) - g_T(z))\, e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z}. \tag{15}$$

5) Διάσπαση $C = C_+ \cup C_-$. Θέτουμε

$$C_+ := C \cap \{\, \mathrm{Re}(z) \geq 0 \,\}, \qquad C_- := C \cap \{\, \mathrm{Re}(z) \leq 0 \,\}.$$

(Τα σημεία με $\mathrm{Re}(z) = 0$ είναι πεπερασμένα και δεν παίζουν ρόλο.)

6) Εκτίμηση στο C_+. Για $z \in C_+$ ισχύει $|z| = R$ και $\mathrm{Re}(z) > 0$, οπότε

$$g(z) - g_T(z) = \int_T^\infty f(t) e^{-zt}\, dt, \qquad \Rightarrow \qquad |g(z) - g_T(z)| \leq M \int_T^\infty e^{-(\mathrm{Re}\, z)\, t} dt = \frac{M e^{-(\mathrm{Re}\, z)T}}{\mathrm{Re}\, z}.$$

Επιπλέον, για $|z| = R$ έχουμε

$$\left| \left(1 + \frac{z^2}{R^2}\right) \frac{1}{z} \right| = \frac{|1 + e^{2i\theta}|}{R} = \frac{2|\cos\theta|}{R} = \frac{2|\,\mathrm{Re}(z)|}{R^2},$$

όπου $z = Re^{i\theta}$. Άρα, στο C_+,

$$\left| (g - g_T)(z)\, e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{1}{z} \right| \leq \frac{M e^{-(\mathrm{Re}\, z)T}}{\mathrm{Re}\, z} \cdot e^{(\mathrm{Re}\, z)T} \cdot \frac{2\,\mathrm{Re}(z)}{R^2} = \frac{2M}{R^2}.$$

Επομένως

$$\left| \frac{1}{2\pi i} \int_{C_+} (g - g_T)(z) e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z} \right| \leq \frac{1}{2\pi} \cdot \frac{2M}{R^2} \cdot \mathrm{length}(C_+) \leq \frac{M}{R}, \tag{16}$$

αφού $\mathrm{length}(C_+) \leq \pi R$.

7) Εκτίμηση στο C_-**: διάσπαση σε** g **και** g_T. Από (15),

$$\int_{C_-} (g - g_T)(\cdot) = \int_{C_-} g(\cdot) \; - \; \int_{C_-} g_T(\cdot).$$

(i) Ο όρος με g_T. Η συνάρτηση

$$z \longmapsto g_T(z) e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{1}{z}$$

είναι ολόμορφη σε περιοχή που περιέχει τον «αριστερό θύλακα» που περικλείεται ανάμεσα στο C_- και στο αριστερό ημικύκλιο

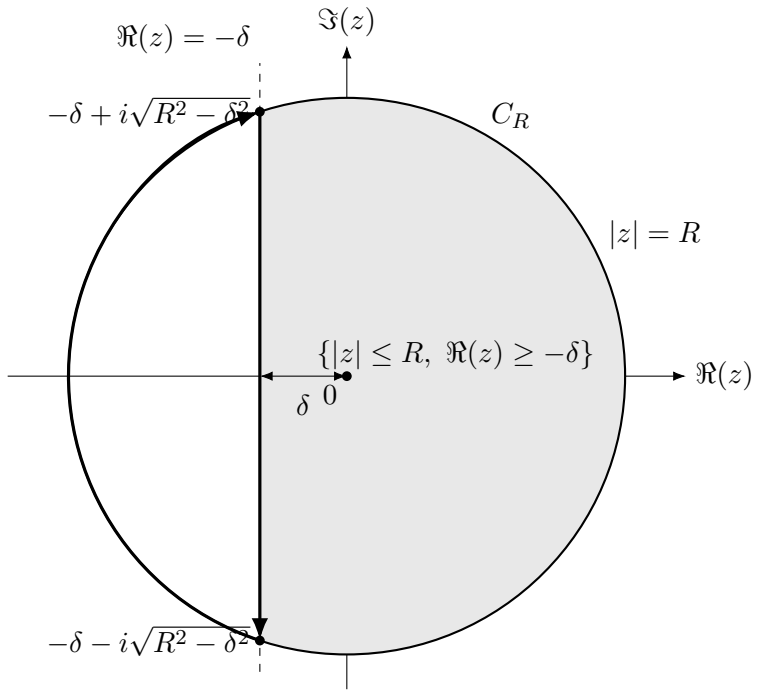
$$C'_- \; := \; \{\, |z| = R, \;\; \mathrm{Re}(z) < 0 \,\}$$

(εφόσον ο θύλακας αυτός δεν περιέχει το 0). Άρα, με παραμόρφωση καμπύλης (θεώρημα Cauchy),

$$\int_{C_-} g_T(z) e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z} = \int_{C'_-} g_T(z) e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z}.$$

Για $z \in C'_-$ έχουμε $\mathrm{Re}(z) < 0$ και

$$|g_T(z)| \leq \int_0^T |f(t)| e^{-(\mathrm{Re}\, z)t} dt \leq M \int_0^T e^{-(\mathrm{Re}\, z)t} dt \leq M\, \frac{e^{-(\mathrm{Re}\, z)T}}{|\,\mathrm{Re}\, z|}.$$



Σχήμα 1: Το χωρίο $\{|z| \le R,\ \Re(z) \ge -\delta\}$ (σκιασμένο) και το περίγραμμα C_R: η χορδή $\Re(z) = -\delta$ (κάθοδος) και το τόξο $|z| = R$ στο $\Re(z) \ge -\delta$ (άνοδος).

Άρα, όπως πριν (και πάλι $|z| = R$),

$$\left| g_T(z) e^{zT} \Big(1 + \frac{z^2}{R^2}\Big) \frac{1}{z} \right| \le \frac{M e^{-(\operatorname{Re} z)T}}{|\operatorname{Re} z|} \cdot e^{(\operatorname{Re} z)T} \cdot \frac{2|\operatorname{Re} z|}{R^2} = \frac{2M}{R^2}.$$

Έτσι παίρνουμε, ακριβώς όπως στο (16),

$$\left| \frac{1}{2\pi i} \int_{C_-} g_T(z) e^{zT} \Big(1 + \frac{z^2}{R^2}\Big) \frac{dz}{z} \right| \le \frac{M}{R}. \tag{17}$$

(ii) Ο όρος με g. Θέτουμε

$$H(z) := g(z) \Big(1 + \frac{z^2}{R^2}\Big) \frac{1}{z}.$$

Επειδή το C_- είναι συμπαγές, το $0 \notin C_-$ και η g είναι ολόμορφη (άρα συνεχής) σε γειτονιά του C_-, η H είναι συνεχής στο C_- και συνεπώς ομοιόμορφα φραγμένη εκεί:

$$B := \sup_{z \in C_-} |H(z)| < \infty.$$

Για κάθε $z \in C_-$ έχουμε $\operatorname{Re}(z) < 0$, άρα $e^{zT} \to 0$ καθώς $T \to \infty$ και επίσης

$$|e^{zT}| = e^{(\operatorname{Re} z)T} \le 1 \qquad (T > 0).$$

Επομένως

$$|H(z) e^{zT}| \le B \qquad (z \in C_-,\ T > 0),$$

και επειδή $H(z) e^{zT} \to 0$ σημειακά στο C_-, από το θεώρημα κυριαρχημένης σύγκλισης (με μέτρο μήκους πάνω στο C_-) παίρνουμε

$$\lim_{T \to \infty} \int_{C_-} H(z) e^{zT}\, dz = 0,$$

δηλαδή

$$\lim_{T\to\infty} \frac{1}{2\pi i} \int_{C_-} g(z) e^{zT} \Big(1 + \frac{z^2}{R^2}\Big) \frac{dz}{z} = 0. \tag{18}$$

8) Συμπέρασμα. Από (15) και τις (16), (17), (18) παίρνουμε: για κάθε σταθερό $R > 0$,

$$\limsup_{T\to\infty} |g(0) - g_T(0)| \le \frac{2M}{R}.$$

Δεδομένου $\varepsilon > 0$, επιλέγουμε R τόσο μεγάλο ώστε $2M/R \le \varepsilon/2$. Έπειτα, από (18) παίρνουμε T_0 τέτοιο ώστε για $T \ge T_0$ να ισχύει

$$\left| \frac{1}{2\pi i} \int_{C_-} g(z) e^{zT} \Big(1 + \frac{z^2}{R^2}\Big) \frac{dz}{z} \right| \le \varepsilon/2.$$

Τότε, για κάθε $T \ge T_0$, από (15) προκύπτει $|g(0) - g_T(0)| \le \varepsilon$. Άρα $g_T(0) \to g(0)$.

Τέλος, επειδή $g_T(0) = \int_0^T f(x)\,dx$, συμπεραίνουμε ότι $\int_0^\infty f(x)\,dx$ συγκλίνει και ισούται με $g(0)$. □

Παρατήρηση 3.2 (Γιατί εισάγουμε το βάρος $e^{zT}\Big(1 + \frac{z^2}{R^2}\Big)$). Το βάρος έχει διπλό ρόλο. Πρώτον, για $\mathrm{Re}(z) > 0$ έχουμε

$$(g - g_T)(z) = \int_T^\infty f(x) e^{-zx}\,dx, \qquad \Rightarrow \qquad (g - g_T)(z) e^{zT} = \int_0^\infty f(T+u) e^{-zu}\,du,$$

οπότε $|(g - g_T)(z) e^{zT}| \le M/\mathrm{Re}(z)$ (ομοιόμορφα ως προς T) και για $\mathrm{Re}(z) < 0$ το e^{zT} δίνει εκθετική απόσβεση καθώς $T \to \infty$. Δεύτερον, στον κύκλο $|z| = R$ ισχύει

$$\left| \Big(1 + \frac{z^2}{R^2}\Big) \frac{1}{z} \right| = \frac{2|\mathrm{Re}(z)|}{R^2},$$

οπότε ο παράγοντας $|\mathrm{Re}(z)|$ ακυρώνει το $1/\mathrm{Re}(z)$ που προκύπτει από την προηγούμενη εκτίμηση και το ολοκληρωτέο γίνεται τάξης $O(1/R^2)$ πάνω στο τόξο, άρα το ολοκλήρωμα πάνω σε τόξο μήκους $O(R)$ είναι $O(1/R)$. Τέλος, επειδή $e^{zT}\big(1 + \frac{z^2}{R^2}\big) = 1 + O(z)$ όταν $z \to 0$, το υπόλοιπο στο $z = 0$ δεν αλλάζει, οπότε η εισαγωγή του βάρους επιτρέπεται (θεώρημα Cauchy/υπολοίπων).

Παρατήρηση 3.3 (Γιατί παραμορφώνουμε από C_- σε C'_-.). Θέλουμε να εκτιμήσουμε

$$\int_{C_-} g_T(z) e^{zT} \Big(1 + \frac{z^2}{R^2}\Big) \frac{dz}{z}.$$

Το περίγραμμα C_- περιέχει τμήμα πάνω στη χορδή $\mathrm{Re}(z) = -\delta$. Εκεί μπορεί να ισχύει

$$|g_T(z)| = \left| \int_0^T f(t) e^{-zt}\,dt \right| \le M \int_0^T e^{\delta t}\,dt \asymp \frac{e^{\delta T}}{\delta},$$

οπότε ο παράγοντας e^{zT} απλώς ακυρώνει το $e^{\delta T}$ και μένει μέγεθος τάξης $1/\delta$, δηλαδή δεν παίρνουμε φθορά όταν $T \to \infty$.

Αντίθετα, στο αριστερό ημικύκλιο

$$C'_- := \{\, |z| = R,\ \mathrm{Re}(z) < 0 \,\}$$

έχουμε για $\mathrm{Re}(z) < 0$ την εκτίμηση

$$|g_T(z) e^{zT}| \le \frac{M}{|\mathrm{Re}(z)|},$$

ενώ πάνω στον κύκλο $|z| = R$ ισχύει

$$\left|\Big(1 + \frac{z^2}{R^2}\Big)\frac{1}{z}\right| = \frac{2|\operatorname{Re}(z)|}{R^2}.$$

Άρα το $1/|\operatorname{Re}(z)|$ ακυρώνεται και το ολοκληρωτέο φράσσεται ομοιόμορφα από $O(1/R^2)$, πράγμα που δίνει

$$\int_{C'_-} g_T(z)e^{zT}\Big(1 + \frac{z^2}{R^2}\Big)\frac{dz}{z} = O(1/R).$$

Η αντικατάσταση του C_- από το C'_- επιτρέπεται (παραμόρφωση καμπύλης / θεώρημα Cauchy), διότι η συνάρτηση $z \mapsto g_T(z)e^{zT}\big(1 + \frac{z^2}{R^2}\big)\frac{1}{z}$ είναι ολόμορφη στην περιοχή ανάμεσα στις C_- και C'_- (ο «αριστερός θύλακας»), η οποία δεν περιέχει το $z = 0$.

Πόρισμα 3.4 (Tauberian). *Έστω $f : [1, \infty) \to \mathbb{C}$ φραγμένη και ολοκληρώσιμη σε κάθε $[1, T]$. Για $\Re(s) > 0$ θέτουμε*

$$g(s) = \int_1^\infty f(x)\, x^{-s}\, \frac{dx}{x}.$$

Αν υπάρχει ανοικτό $U \subset \mathbb{C}$ με $\{\Re(s) \geq 0\} \subset U$ τέτοιο ώστε το g να έχει ολόμορφη επέκταση στο U, τότε το γενικευμένο ολοκλήρωμα $\int_1^\infty f(x)\,\frac{dx}{x}$ συγκλίνει και ισούται με $g(0)$.

Απόδειξη. Θέτουμε $F(t) = f(e^t)$ για $t \geq 0$. Τότε

$$g(s) = \int_0^\infty F(t)e^{-st}\, dt$$

(αλλαγή μεταβλητής $x = e^t$). Εφαρμόζουμε το Θεώρημα 9.3 στο F και παίρνουμε ότι $\int_0^\infty F(t)\, dt$ υπάρχει και ισούται με $g(0)$. Με την αντίστροφη αλλαγή μεταβλητής,

$$\int_0^\infty F(t)\, dt = \int_1^\infty f(x)\, \frac{dx}{x}.$$

□

3.1 Ένα βοηθητικό λήμμα: σύγκλιση $\int (A(x) - x)/x^2 \Rightarrow A(x) \sim x$

Λήμμα 3.5. *Έστω $A : [1, \infty) \to \mathbb{R}$ αύξουσα. Αν το γενικευμένο ολοκλήρωμα*

$$\int_1^\infty \frac{A(t) - t}{t^2}\, dt$$

συγκλίνει, τότε $A(x) \sim x$ όταν $x \to \infty$, δηλαδή $\frac{A(x)}{x} \to 1$.

Απόδειξη. Υποθέτουμε προς άτοπο ότι $\limsup_{x\to\infty} \frac{A(x)}{x} > \lambda > 1$. Τότε υπάρχουν άπειρα x με $A(x) \geq \lambda x$. Για ένα τέτοιο x και για κάθε $t \in [x, \lambda x]$, από την αύξηση παίρνουμε $A(t) \geq A(x) \geq \lambda x$, άρα

$$\int_x^{\lambda x} \frac{A(t) - t}{t^2}\, dt \geq \int_x^{\lambda x} \frac{\lambda x - t}{t^2}\, dt.$$

Με αλλαγή $t = ux$ (δηλαδή $dt = x\, du$) έχουμε

$$\int_x^{\lambda x} \frac{\lambda x - t}{t^2}\, dt = \int_1^\lambda \frac{\lambda - u}{u^2}\, du =: c(\lambda) > 0,$$

σταθερά που εξαρτάται μόνο από λ. Άρα, για άπειρα x ισχύει

$$\left|\int_x^\infty \frac{A(t) - t}{t^2}\, dt - \int_{\lambda x}^\infty \frac{A(t) - t}{t^2}\, dt\right| = \left|\int_x^{\lambda x} \frac{A(t) - t}{t^2}\, dt\right| \geq c(\lambda) > 0.$$

Όμως τα δύο αριστερά ολοκληρώματα είναι *ουρές* ενός συγκλίνοντος ολοκληρώματος, άρα καθώς $x \to \infty$ και τα δύο τείνουν στο 0 και η διαφορά τους πρέπει να τείνει στο 0, άτοπο. Άρα $\limsup_{x\to\infty} A(x)/x \le 1$.

Ομοίως, αν $\liminf_{x\to\infty} A(x)/x < \mu < 1$, τότε για άπειρα x έχουμε $A(x) \le \mu x$ και για $t \in [\mu x, x]$ παίρνουμε $A(t) \le A(x) \le \mu x$, άρα

$$\int_{\mu x}^{x} \frac{A(t)-t}{t^2}\,dt \le \int_{\mu x}^{x} \frac{\mu x - t}{t^2}\,dt = -\int_{\mu}^{1} \frac{u-\mu}{u^2}\,du =: -c'(\mu) < 0,$$

και ξανά παίρνουμε αντίφαση με τη σύγκλιση των ουρών. Άρα $\liminf_{x\to\infty} A(x)/x \ge 1$. Συνεπώς $\frac{A(x)}{x} \to 1$. □

Θεώρημα 3.6. *Έστω* $a_n \ge 0$ *και*

$$A(x) := \sum_{n\le x} a_n.$$

Υποθέτουμε ότι $A(x) = O(x)$. *Θέτουμε τη Dirichlet σειρά*

$$F(s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \qquad \Re(s) > 1.$$

Υποθέτουμε ότι η $F(s)$ *έχει αναλυτική συνέχεια στο* $\Re(s) \ge 1$ *εκτός από έναν απλό πόλο στο* $s = 1$ *με υπόλοιπο* 1. *Τότε*

$$A(x) \sim x \qquad (x \to \infty).$$

Απόδειξη. **Βήμα 1: Μερική άθροιση** Για $\Re(s) > 1$ ισχύει η ταυτότητα:

$$\sum_{n\le X} \frac{a_n}{n^s} = \frac{A(X)}{X^s} + s\int_1^X \frac{A(x)}{x^{s+1}}\,dx.$$

Επειδή $A(X) = O(X)$ και $\Re(s) > 1$, έχουμε $A(X)X^{-s} \to 0$ καθώς $X \to \infty$. Άρα, περνώντας στο όριο $X \to \infty$,

$$F(s) = s\int_1^{\infty} \frac{A(x)}{x^{s+1}}\,dx \qquad (\Re(s) > 1). \tag{19}$$

Βήμα 2: Αφαίρεση του πόλου στο $s = 1$ **και αναλυτική συνέχεια στο** $\Re(z) \ge 0$. Θέτουμε $s = 1 + z$ (οπότε $\Re(z) > 0$) και ορίζουμε

$$H(z) := \frac{F(1+z)}{1+z} - \frac{1}{z}.$$

Η υπόθεση "F έχει απλό πόλο στο $s = 1$ με υπόλοιπο 1" ισοδυναμεί με το ότι $F(1+z) = \frac{1}{z} + (\text{ολόμορφος όρος})$ κοντά στο $z = 0$. Άρα ο $H(z)$ είναι ολόμορφος σε γειτονιά του $z = 0$ και επιπλέον έχει αναλυτική συνέχεια στο $\Re(z) \ge 0$.

Βήμα 3: Αναπαράσταση του H. Από (19) με $s = 1 + z$ παίρνουμε, για $\Re(z) > 0$,

$$\frac{F(1+z)}{1+z} = \int_1^{\infty} \frac{A(x)}{x^{2+z}}\,dx = \int_1^{\infty} \frac{A(x)}{x}\,x^{-z}\,\frac{dx}{x}.$$

Επίσης για $\Re(z) > 0$ ισχύει

$$\frac{1}{z} = \int_1^{\infty} x^{-z}\,\frac{dx}{x}.$$

Άρα, για $\Re(z) > 0$,

$$H(z) = \int_1^{\infty} \left(\frac{A(x)}{x} - 1\right) x^{-z}\,\frac{dx}{x}. \tag{20}$$

Βήμα 4: Εφαρμογή του Θεωρήματος. Θέτουμε

$$f(x) := \frac{A(x)}{x} - 1.$$

Από $A(x) = O(x)$ έχουμε ότι f είναι φραγμένη στο $[1, \infty)$, και είναι ολοκληρώσιμη σε κάθε $[1, X]$. Η σχέση (20) λέει ότι για $\Re(z) > 0$ η Mellin μετασχηματισμένη της f είναι $H(z)$, η οποία (από το Βήμα 2) έχει αναλυτική συνέχεια στο $\Re(z) \geq 0$. Άρα, από το Θεώρημα 9.3, το ολοκλήρωμα

$$\int_1^\infty \left(\frac{A(x)}{x} - 1\right) \frac{dx}{x} = \int_1^\infty \frac{A(x) - x}{x^2}\, dx$$

συγκλίνει.

Βήμα 5: Συμπέρασμα $A(x) \sim x$. Η $A(x)$ είναι αύξουσα (επειδή $a_n \geq 0$). Επομένως, από το Λήμμα 3.5 συμπεραίνουμε $\frac{A(x)}{x} \to 1$, δηλαδή $A(x) \sim x$. □

Μένει να αποδείξουμε ότι τα παραπάνω μπορούμε να τα εφαρμόσουμε για την συνάρτηση ψ.

Θεώρημα 3.7 (Εκτίμηση Chebyshev). *Ορίζουμε τη συνάρτηση von Mangoldt*

$$\Lambda(n) := \begin{cases} \log p, & \text{αν } n = p^k \text{ για κάποιο πρώτο } p \text{ και } k \geq 1, \\ 0, & \text{διαφορετικά}, \end{cases}$$

και τη συνάρτηση Chebyshev

$$\psi(x) := \sum_{n \leq x} \Lambda(n) \qquad (x \geq 1).$$

Τότε ισχύει

$$\psi(x) \asymp x \qquad \text{ομοιόμορφα για } x \geq 2,$$

δηλαδή υπάρχουν σταθερές $c_1, c_2 > 0$ ώστε $c_1 x \leq \psi(x) \leq c_2 x$ για κάθε $x \geq 2$.

Απόδειξη. **1) Ένα λήμμα για εναλλασσόμενες σειρές.** Αν $(a_n)_{n \geq 1}$ είναι ακολουθία μη αρνητικών πραγματικών που φθίνει προς το 0, τότε η σειρά $\sum_{n=1}^\infty (-1)^{n-1} a_n$ συγκλίνει και ισχύει

$$a_1 - a_2 \;\leq\; \sum_{n=1}^{\infty} (-1)^{n-1} a_n \;\leq\; a_1 - a_2 + a_3. \tag{21}$$

Πράγματι, τα μερικά αθροίσματα γράφονται ως

$$(a_1 - a_2) + (a_3 - a_4) + \cdots \geq a_1 - a_2,$$

ενώ

$$(a_1 - a_2 + a_3) - (a_4 - a_5) - \cdots \leq a_1 - a_2 + a_3,$$

επειδή $a_{2j-1} - a_{2j} \geq 0$ και $a_{2j} - a_{2j+1} \geq 0$.

2) Ορισμός της $T(x)$ και ταύτιση με $\sum_{n \leq x} \log n$. Για $x \geq 1$ θέτουμε

$$T(x) := \sum_{n \leq x} \psi\Big(\frac{x}{n}\Big).$$

Θα δείξουμε ότι

$$T(x) = \sum_{n \leq x} \log n. \tag{22}$$

Χρησιμοποιούμε την κλασική ταυτότητα

$$\sum_{d\,|\,n}\Lambda(d)=\log n, \tag{23}$$

η οποία προκύπτει από την παραγοντοποίηση $n=\prod p^{\alpha_p}$: το άθροισμα στα $d|n$ με $\Lambda(d)\neq 0$ δίνει $\sum_p \alpha_p\log p=\log n$. Άρα

$$\sum_{n\le x}\log n=\sum_{n\le x}\sum_{d\,|\,n}\Lambda(d)=\sum_{d\le x}\Lambda(d)\sum_{\substack{n\le x\\ d|n}}1=\sum_{d\le x}\Lambda(d)\sum_{k\le x/d}1.$$

Αλλά

$$\sum_{d\le x}\Lambda(d)\sum_{k\le x/d}1=\sum_{k\le x}\sum_{d\le x/k}\Lambda(d)=\sum_{k\le x}\psi\Big(\frac{x}{k}\Big)=T(x),$$

οπότε ισχύει (22).

3) Ασύμπτωτη για $\sum_{n\le x}\log n$ και συνέπεια για $T(x)$. Για $x\ge 2$ έχουμε (σύγκριση αθροίσματος με ολοκλήρωμα)

$$\int_1^x \log t\,dt\ \le\ \sum_{n\le x}\log n\ \le\ \int_1^x \log t\,dt+\log x,$$

άρα

$$\sum_{n\le x}\log n=x\log x-x+\mathcal{O}(\log x)\qquad (x\ge 2). \tag{24}$$

Με (22) συμπεραίνουμε

$$T(x)=x\log x-x+\mathcal{O}(\log x)\qquad (x\ge 2). \tag{25}$$

Επομένως

$$T(x)-2T\Big(\frac{x}{2}\Big)=(\log 2)\,x+\mathcal{O}(\log x)\qquad (x\ge 2). \tag{26}$$

(Πράγματι, αντικαθιστώντας την (25) στα δύο μέλη και απλοποιώντας, παίρνουμε τον κύριο όρο $(\log 2)x$, ενώ τα σφάλματα παραμένουν $\mathcal{O}(\log x)$.)

4) Εναλλασσόμενο άθροισμα για $T(x)-2T(x/2)$. Από τον ορισμό,

$$T(x)-2T\Big(\frac{x}{2}\Big)=\sum_{n\le x}\psi\Big(\frac{x}{n}\Big)-2\sum_{n\le x/2}\psi\Big(\frac{x}{2n}\Big).$$

Επειδή $\psi(y)=0$ για $0<y<1$ (το άθροισμα είναι κενό), έχουμε $\psi(x/(2n))=0$ όταν $x/2<n\le x$, οπότε

$$\sum_{n\le x/2}\psi\Big(\frac{x}{2n}\Big)=\sum_{n\le x}\psi\Big(\frac{x}{2n}\Big).$$

Άρα

$$T(x)-2T\Big(\frac{x}{2}\Big)=\sum_{n\le x}\psi\Big(\frac{x}{n}\Big)-2\sum_{n\le x}\psi\Big(\frac{x}{2n}\Big). \tag{27}$$

Με αλλαγή δείκτη $m=2n$ έχουμε

$$2\sum_{n\le x}\psi\Big(\frac{x}{2n}\Big)=2\sum_{\substack{m\le x\\ 2|m}}\psi\Big(\frac{x}{m}\Big),$$

και έτσι το δεξί μέλος του (27) γράφεται ως

$$\sum_{\substack{m\le x\\ m\ \text{περιττός}}} \psi\Big(\frac{x}{m}\Big) - \sum_{\substack{m\le x\\ m\ \text{άρτιος}}} \psi\Big(\frac{x}{m}\Big) = \sum_{n\le x}(-1)^{n-1}\psi\Big(\frac{x}{n}\Big)\,.$$

Επιπλέον, αν $n > x$ τότε $x/n < 1$ και $\psi(x/n) = 0$, άρα

$$T(x) - 2T\Big(\frac{x}{2}\Big) = \sum_{n=1}^{\infty}(-1)^{n-1}\psi\Big(\frac{x}{n}\Big)\,. \tag{28}$$

5) Εφαρμογή του (21). Για σταθερό $x \ge 2$ θέτουμε $a_n := \psi(x/n)$. Επειδή η ψ είναι μη φθίνουσα ως συνάρτηση του ορίσματος και x/n φθίνει με το n, η ακολουθία (a_n) είναι μη αύξουσα. Επίσης $a_n = 0$ για $n > x$, άρα $a_n \to 0$. Επομένως μπορούμε να εφαρμόσουμε το (21) στη σειρά (28) και παίρνουμε

$$\psi(x) - \psi\Big(\frac{x}{2}\Big) \;\le\; \sum_{n=1}^{\infty}(-1)^{n-1}\psi\Big(\frac{x}{n}\Big) \;\le\; \psi(x) - \psi\Big(\frac{x}{2}\Big) + \psi\Big(\frac{x}{3}\Big)\,. \tag{29}$$

Συνδυάζοντας (26) και (28)–(29) παίρνουμε, για κάθε $x \ge 2$,

$$\psi(x) - \psi\Big(\frac{x}{2}\Big) \le (\log 2)\,x + \mathcal{O}(\log x), \tag{30}$$

$$\psi(x) - \psi\Big(\frac{x}{2}\Big) + \psi\Big(\frac{x}{3}\Big) \ge (\log 2)\,x + \mathcal{O}(\log x). \tag{31}$$

6) Άνω φράγμα $\psi(x) \ll x$. Θέτουμε r τον μέγιστο ακέραιο με $2^r < x$ (οπότε $x/2^{r+1} < 1$ και $\psi(x/2^{r+1}) = 0$). Γράφουμε τηλεσκοπικά

$$\psi(x) = \sum_{j=0}^{r}\Big(\psi\Big(\frac{x}{2^j}\Big) - \psi\Big(\frac{x}{2^{j+1}}\Big)\Big).$$

Εφαρμόζοντας την (30) στο $x/2^j$, παίρνουμε

$$\psi\Big(\frac{x}{2^j}\Big) - \psi\Big(\frac{x}{2^{j+1}}\Big) \le (\log 2)\,\frac{x}{2^j} + \mathcal{O}\big(\log(x/2^j)\big).$$

Αθροίζοντας για $j = 0, \dots, r$,

$$\psi(x) \le (\log 2)\,x\sum_{j=0}^{r}\frac{1}{2^j} + \mathcal{O}\left(\sum_{j=0}^{r}\log(x/2^j)\right).$$

Έχουμε $\sum_{j=0}^{r} 2^{-j} \le 2$ και

$$\sum_{j=0}^{r}\log(x/2^j) = (r+1)\log x - (\log 2)\sum_{j=0}^{r} j = \mathcal{O}\big((\log x)^2\big),$$

άρα

$$\psi(x) \le 2(\log 2)\,x + \mathcal{O}\big((\log x)^2\big) \ll x \qquad (x \ge 2). \tag{32}$$

7) Κάτω φράγμα $\psi(x) \gg x$. Από (31) και (32) (εφαρμοσμένη στο $x/3$) παίρνουμε

$$\psi(x) - \psi\Big(\frac{x}{2}\Big) \ge (\log 2)\,x - \psi\Big(\frac{x}{3}\Big) + \mathcal{O}(\log x) \ge (\log 2)\,x - \frac{2(\log 2)}{3}x + \mathcal{O}\big((\log x)^2\big),$$

δηλαδή

$$\psi(x) - \psi\Big(\frac{x}{2}\Big) \geq \frac{\log 2}{3}\, x + \mathcal{O}\big((\log x)^2\big). \tag{33}$$

Άρα υπάρχει $x_0 \geq 2$ τέτοιο ώστε για κάθε $x \geq x_0$ να ισχύει

$$\psi(x) - \psi\Big(\frac{x}{2}\Big) \geq \frac{\log 2}{6}\, x. \tag{34}$$

Τότε, για $x \geq x_0$, τηλεσκοπώντας όπως πριν και εφαρμόζοντας (34) στα $x/2^j$ όσο $x/2^j \geq x_0$, παίρνουμε

$$\psi(x) \geq \sum_{0\leq j\leq J} \Big(\psi\Big(\frac{x}{2^j}\Big) - \psi\Big(\frac{x}{2^{j+1}}\Big)\Big) \geq \frac{\log 2}{6} \sum_{0\leq j\leq J} \frac{x}{2^j} \geq \frac{\log 2}{6}\, x,$$

όπου J είναι ο μέγιστος ακέραιος με $x/2^J \geq x_0$ (οπότε $\sum_{j=0}^{J} 2^{-j} \geq 1$). Τέλος, αν θέσουμε

$$c_1 := \min\left\{ \frac{\log 2}{6},\ \min_{2\leq x\leq x_0} \frac{\psi(x)}{x} \right\} > 0,$$

τότε $c_1 x \leq \psi(x)$ για όλα τα $x \geq 2$.

Από (32) παίρνουμε επίσης $\psi(x) \leq c_2 x$ για κάποιο $c_2 > 0$ και για όλα τα $x \geq 2$. Άρα $\psi(x) \asymp x$ ομοιόμορφα για $x \geq 2$. □

Παρατήρηση 3.8 (Γιατί η ψ ικανοποιεί τις υποθέσεις του Θεωρήματος 3.6). Θέτουμε $a_n := \Lambda(n) \geq 0$ και

$$A(x) = \sum_{n\leq x} a_n = \sum_{n\leq x} \Lambda(n) = \psi(x).$$

Από την εκτίμηση Chebyshev, Θεώρημα 3.7, που αποδείξαμε προηγουμένως έχουμε $\psi(x) \ll x$, άρα $A(x) = O(x)$. Η αντίστοιχη Dirichlet σειρά είναι

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

Για $\Re(s) > 1$ γνωρίζουμε ότι

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s},$$

δηλαδή $F(s) = -\zeta'(s)/\zeta(s)$ στο ημιεπίπεδο $\Re(s) > 1$.

Από τη σχέση που αποδείχθηκε για τη ζ (αναλυτική συνέχιση της ζ στο $\Re(s) > 0$ με απλό πόλο στο $s = 1$ και υπόλοιπο 1), συμπεραίνουμε ότι:

- Η $\zeta(s)$ είναι ολόμορφη στο $\Re(s) \geq 1$ εκτός από απλό πόλο στο $s = 1$.
- Στο $\Re(s) \geq 1$ δεν υπάρχουν μηδενικά της ζ (η $\zeta(s) = \sum_{n\geq 1} n^{-s}$ έχει θετική πραγματική τιμή για $s > 1$, και η αναλυτική της συνέχεια στο $\Re(s) \geq 1$ δεν μπορεί να αποκτήσει μηδενικό πάνω στη γραμμή $\Re(s) = 1$ χωρίς να παραβιάζεται η γνωστή μορφή του πόλου στο 1).

Συνεπώς, η συνάρτηση $F(s) = -\zeta'(s)/\zeta(s)$ έχει αναλυτική συνέχεια στο $\Re(s) \geq 1$ εκτός από ενδεχόμενες ιδιομορφίες στα σημεία όπου $\zeta(s) = 0$ και στο $s = 1$. Στο $\Re(s) \geq 1$ όμως δεν έχουμε μηδενικά, άρα η μόνη ιδιομορφία προέρχεται από το $s = 1$.

Τέλος, επειδή κοντά στο $s = 1$ έχουμε

$$\zeta(s) = \frac{1}{s-1} + h(s) \qquad \text{με } h \text{ ολόμορφη κοντά στο } 1,$$

παίρνουμε

$$\zeta'(s) = -\frac{1}{(s-1)^2} + h'(s), \qquad -\frac{\zeta'(s)}{\zeta(s)} = \frac{1}{s-1} + (\text{ολόμορφος όρος κοντά στο } 1).$$

Άρα η $F(s) = -\zeta'(s)/\zeta(s)$ έχει *απλό πόλο* στο $s = 1$ με *υπόλοιπο* 1.

Με άλλα λόγια, για την ακολουθία $a_n = \Lambda(n)$ ισχύουν όλες οι υποθέσεις του Θεωρήματος 3.6.

4 Το Θεώρημα Dirichlet σε αριθμητικές προόδους

Θεωρούμε $q \geq 2$ και $(a, q) = 1$. Ορίζουμε τη συνάρτηση Chebyshev σε αριθμητική πρόοδο

$$\psi(x; q, a) := \sum_{\substack{n \leq x \\ n \equiv a \pmod q}} \Lambda(n).$$

Για $\mathrm{Re}(s) > 1$ ορίζουμε τη Dirichlet σειρά

$$F_{q,a}(s) := \sum_{\substack{n \geq 1 \\ n \equiv a \pmod q}} \frac{\Lambda(n)}{n^s}.$$

Επειδή $\Lambda(n) \geq 0$ και $\psi(x; q, a) \leq \psi(x)$, από το Chebyshev φράγμα για την ψ έχουμε $\psi(x; q, a) = O(x)$ και η $F_{q,a}(s)$ συγκλίνει για $\mathrm{Re}(s) > 1$.

Θεώρημα 4.1 (Θεώρημα Dirichlet για πρώτους σε αριθμητικές προόδους (αναλυτική μορφή)). *Έστω $q \geq 2$ και a με $(a, q) = 1$. Ορίζουμε*

$$\psi(x; q, a) := \sum_{\substack{n \leq x \\ n \equiv a \pmod q}} \Lambda(n), \qquad F_{q,a}(s) := \sum_{\substack{n \geq 1 \\ n \equiv a \pmod q}} \frac{\Lambda(n)}{n^s} \qquad (\mathrm{Re}(s) > 1).$$

Τότε:

1. *Η $F_{q,a}(s)$ επεκτείνεται μερομορφικά στο ημιεπίπεδο $\mathrm{Re}(s) \geq 1$ και έχει εκεί μοναδικό απλό πόλο στο $s = 1$, με υπόλοιπο*

$$\mathrm{Res}_{s=1} F_{q,a}(s) = \frac{1}{\varphi(q)}.$$

2. *Ισχύει η ασυμπτωτική*

$$\psi(x; q, a) \sim \frac{x}{\varphi(q)} \qquad (x \to \infty).$$

Ισοδύναμα, υπάρχουν άπειροι πρώτοι $p \equiv a \pmod q$.

Μερική άθροιση Θέτουμε $A(x) := \psi(x; q, a)$. Για $\mathrm{Re}(s) > 1$ ισχύει η κλασική ταυτότητα μερικής άθροισης

$$\sum_{\substack{n \leq X \\ n \equiv a \ (q)}} \frac{\Lambda(n)}{n^s} = \frac{A(X)}{X^s} + s \int_1^X \frac{A(x)}{x^{s+1}}\, dx.$$

Επειδή $A(X) = O(X)$ και $\mathrm{Re}(s) > 1$, έχουμε $A(X)X^{-s} \to 0$ όταν $X \to \infty$, οπότε περνώντας στο όριο

$$F_{q,a}(s) = s \int_1^\infty \frac{\psi(x; q, a)}{x^{s+1}}\, dx, \tag{35}$$

για $\mathrm{Re}(s) > 1$. Ακριβώς όπως στην απόδειξη του Θεωρήματος των Πρώτων, για να πάρουμε ασυμπτωτική της $\psi(x; q, a)$ χρειαζόμαστε πληροφορία για την αναλυτική επέκταση της $F_{q,a}(s)$ μέχρι την ευθεία $\mathrm{Re}(s) = 1$.

4.1 Ορθογωνιότητα χαρακτήρων και αναγωγή σε $-L'/L$

Λήμμα 4.2 (Ορθογωνιότητα). *Για $(a,q)=1$ και κάθε ακέραιο n ισχύει*

$$\mathbf{1}_{n\equiv a\ (q)} = \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \overline{\chi}(a)\,\chi(n),$$

όπου το άθροισμα τρέχει σε όλους τους Dirichlet χαρακτήρες modulo q (επεκτεινόμενους με $\chi(n)=0$ όταν $(n,q)>1$).

Απόδειξη. Αν $(n,q)>1$, τότε $\chi(n)=0$ για κάθε χ, ενώ $\mathbf{1}_{n\equiv a(q)}=0$ επειδή $(a,q)=1$. Αν $(n,q)=1$, τότε η ταυτότητα είναι ακριβώς η ορθογωνιότητα των χαρακτήρων της ομάδας $(\mathbb{Z}/q\mathbb{Z})^\times$:

$$\frac{1}{\varphi(q)}\sum_{\chi}\overline{\chi}(a)\chi(n) = \begin{cases} 1, & n\equiv a \pmod q,\\ 0, & n\not\equiv a \pmod q. \end{cases}$$

□

Για $\mathrm{Re}(s)>1$, από το Λήμμα 4.2 παίρνουμε

$$F_{q,a}(s) = \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \overline{\chi}(a) \sum_{n\ge 1} \frac{\Lambda(n)\chi(n)}{n^s}. \tag{36}$$

Ορισμός $L(s,\chi)$ (ως Dirichlet σειρά, χωρίς Euler προϊόν). Για κάθε χαρακτήρα χ ορίζουμε

$$L(s,\chi) := \sum_{n\ge 1} \frac{\chi(n)}{n^s}, \qquad \mathrm{Re}(s)>1,$$

και επίσης

$$F_\chi(s) := \sum_{n\ge 1} \frac{\Lambda(n)\chi(n)}{n^s}, \qquad \mathrm{Re}(s)>1.$$

Λήμμα 4.3. *Για κάθε $n\ge 1$ ισχύει $\sum_{d\mid n}\Lambda(d)=\log n$.*

Απόδειξη. (Όπως στο ΠΘΠ.) Αν $n=p^k$, τότε $\sum_{d\mid p^k}\Lambda(d)=\Lambda(p)+\cdots+\Lambda(p^k)=\log p=\log(p^k)/k$; αλλά μόνο το $d=p$ συμβάλλει, άρα $\sum_{d\mid p^k}\Lambda(d)=\log p^k=\log n$. Αν n δεν είναι δύναμη πρώτου, το άθροισμα είναι $0=\log n$; συνολικά παίρνουμε την ταυτότητα. □

Πρόταση 4.4. *Για $\mathrm{Re}(s)>1$ ισχύει η ταυτότητα*

$$-L'(s,\chi) = L(s,\chi)\,F_\chi(s). \tag{37}$$

Απόδειξη. (Ακριβώς όπως στο ΠΘΠ για την ζ, αλλά με χ.) Για $\sigma:=\mathrm{Re}(s)>1$ Για $\sigma:=\mathrm{Re}(s)>1$ οι σειρές

$$L(s,\chi)=\sum_{m\ge1}\frac{\chi(m)}{m^s}, \qquad F_\chi(s)=\sum_{n\ge1}\frac{\Lambda(n)\chi(n)}{n^s}$$

συγκλίνουν απολύτως, αφού

$$\sum_{m\ge1}\frac{|\chi(m)|}{m^\sigma}\le\sum_{m\ge1}\frac{1}{m^\sigma}<\infty, \qquad \sum_{n\ge1}\frac{|\Lambda(n)\chi(n)|}{n^\sigma}\le\sum_{n\ge1}\frac{\Lambda(n)}{n^\sigma}<\infty.$$

Επομένως μπορούμε να πολλαπλασιάσουμε τις δύο σειρές και να αναδιατάξουμε το διπλό άθροισμα (Tonelli/Fubini), οπότε παίρνουμε το Cauchy product:

$$L(s,\chi)F_\chi(s) = \left(\sum_{m\geq 1}\frac{\chi(m)}{m^s}\right)\left(\sum_{n\geq 1}\frac{\Lambda(n)\chi(n)}{n^s}\right)$$
$$= \sum_{m\geq 1}\sum_{n\geq 1}\frac{\chi(m)\Lambda(n)\chi(n)}{(mn)^s}.$$

Τώρα ομαδοποιούμε τους όρους ως προς $k = mn$: για σταθερό $k \geq 1$ οι λύσεις $mn = k$ αντιστοιχούν ακριβώς στους διαιρέτες $d \mid k$ θέτοντας $n = d$ και $m = k/d$. Άρα

$$\sum_{m\geq 1}\sum_{n\geq 1}\frac{\chi(m)\Lambda(n)\chi(n)}{(mn)^s} = \sum_{k\geq 1}\frac{1}{k^s}\sum_{d\mid k}\chi\left(\frac{k}{d}\right)\Lambda(d)\chi(d),$$

δηλαδή

$$L(s,\chi)F_\chi(s) = \sum_{k\geq 1}\frac{1}{k^s}\sum_{d\mid k}\chi\left(\frac{k}{d}\right)\chi(d)\Lambda(d).$$

Αν $(k,q) = 1$, τότε $\chi(k/d)\chi(d) = \chi(k)$ και

$$\sum_{d\mid k}\chi\left(\frac{k}{d}\right)\chi(d)\Lambda(d) = \chi(k)\sum_{d\mid k}\Lambda(d) = \chi(k)\log k$$

με το Λήμμα 4.3. Αν $(k,q) > 1$, τότε $\chi(k) = 0$ και κάθε όρος στο άθροισμα είναι 0 (επειδή τότε d ή k/d έχει κοινό διαιρέτη με q), άρα πάλι ο συντελεστής είναι $\chi(k)\log k = 0$. Συνεπώς

$$L(s,\chi)F_\chi(s) = \sum_{k\geq 1}\frac{\chi(k)\log k}{k^s}.$$

Τέλος,

$$L'(s,\chi) = \frac{d}{ds}\sum_{k\geq 1}\frac{\chi(k)}{k^s} = -\sum_{k\geq 1}\frac{\chi(k)\log k}{k^s},$$

οπότε παίρνουμε (37). □

Θεώρημα 4.5. *Για κάθε χαρακτήρα χ και κάθε s με $\mathrm{Re}(s) > 1$ ισχύει $L(s,\chi) \neq 0$.*

Απόδειξη. (Ιδια ακριβώς ιδέα με το Θεώρημα 2.7 στο ΠΘΠ.) Έστω προς άτοπο ότι $L(s_0,\chi) = 0$ για κάποιο s_0 με $\mathrm{Re}(s_0) > 1$, και έστω $m \geq 1$ η τάξη του μηδενικού. Τότε $-L'(s,\chi)$ έχει μηδενικό τάξης ακριβώς $m-1$ στο s_0. Όμως από την Πρόταση 4.4 έχουμε $-L'(s,\chi) = L(s,\chi)F_\chi(s)$, όπου F_χ είναι ολόμορφη στο $\mathrm{Re}(s) > 1$ (από απόλυτη σύγκλιση), άρα το δεξί μέλος έχει μηδενικό τάξης τουλάχιστον m στο s_0. Αντίφαση. Άρα $L(s,\chi) \neq 0$ στο $\mathrm{Re}(s) > 1$. □

Πόρισμα 4.6. *Στο $\mathrm{Re}(s) > 1$ ισχύει*

$$-\frac{L'}{L}(s,\chi) = \sum_{n\geq 1}\frac{\Lambda(n)\chi(n)}{n^s}.$$

Απόδειξη. Διαιρούμε την (37) με $L(s,\chi)$ (επιτρέπεται από το Θεώρημα 4.5). □

Άρα, από (36) και το Κορ. 4.6, παίρνουμε στο $\mathrm{Re}(s) > 1$:

$$F_{q,a}(s) = -\frac{1}{\varphi(q)}\sum_{\chi \pmod q}\overline{\chi}(a)\,\frac{L'}{L}(s,\chi). \tag{38}$$

4.2 Αναλυτική συνέχεια των $L(s,\chi)$ στο $\mathrm{Re}(s)>0$ (όπως για την ζ)

Λήμμα 4.7. *Αν χ είναι μη κύριος χαρακτήρας modulo q, τότε τα μερικά αθροίσματα*

$$S_\chi(x) := \sum_{n\le x} \chi(n)$$

είναι φραγμένα, δηλαδή $S_\chi(x) = O(1)$.

Απόδειξη. Εφόσον χ είναι μη κύριος, υπάρχει a με $(a,q)=1$ και $\chi(a)\neq 1$. Τότε, επειδή ο πολλαπλασιασμός με a μεταθέτει το πλήρες σύστημα υπολοίπων modulo q, έχουμε

$$\sum_{n=1}^{q}\chi(n) = \sum_{n=1}^{q}\chi(an) = \chi(a)\sum_{n=1}^{q}\chi(n),$$

άρα $\sum_{n=1}^{q}\chi(n)=0$. Γράφοντας $N = kq+r$ με $0\le r<q$ παίρνουμε

$$\sum_{n=1}^{N}\chi(n) = k\sum_{n=1}^{q}\chi(n) + \sum_{n=1}^{r}\chi(n) = \sum_{n=1}^{r}\chi(n),$$

οπότε $\left|\sum_{n=1}^{N}\chi(n)\right| \le \sum_{n=1}^{r}|\chi(n)| \le r \le q$. □

Πρόταση 4.8. *Αν χ είναι μη κύριος χαρακτήρας modulo q, τότε η $L(s,\chi)$ επεκτείνεται ως ολόμορφη συνάρτηση στο ημιεπίπεδο $\mathrm{Re}(s)>0$.*

Απόδειξη. (Όπως το Θεώρημα 2.9.) Για $\mathrm{Re}(s)>1$ εφαρμόζουμε μερική άθροιση στη Dirichlet σειρά του $L(s,\chi)$:

$$L(s,\chi) = \sum_{n\ge 1}\frac{\chi(n)}{n^s} = s\int_1^\infty \frac{S_\chi(x)}{x^{s+1}}\,dx.$$

Από το Λήμμα 4.7 έχουμε $S_\chi(x)=O(1)$, άρα το ολοκλήρωμα συγκλίνει για $\mathrm{Re}(s)>0$. Επιπλέον ο ολοκληρωτέος πυρήνας είναι ολόμορφος ως προς s και η σύγκλιση είναι ομοιόμορφη σε συμπαγή, οπότε η $L(s,\chi)$ είναι ολόμορφη στο $\mathrm{Re}(s)>0$. □

Πρόταση 4.9. *Για τον κύριο χαρακτήρα χ_0 modulo q ισχύει για $\mathrm{Re}(s)>1$ η ταυτότητα*

$$L(s,\chi_0) = \zeta(s)\sum_{d\mid q}\frac{\mu(d)}{d^s}.$$

Άρα η $L(s,\chi_0)$ έχει μερομορφική συνέχεια στο $\mathrm{Re}(s)>0$ με απλό πόλο στο $s=1$ και υπόλοιπο $\sum_{d\mid q}\mu(d)/d = \prod_{p\mid q}(1-1/p) = \varphi(q)/q$.

Απόδειξη. Χρησιμοποιούμε την ταυτότητα

$$\mathbf{1}_{(n,q)=1} = \sum_{d\mid (n,q)}\mu(d) = \sum_{d\mid q,\ d\mid n}\mu(d).$$

Τότε για $\mathrm{Re}(s)>1$,

$$L(s,\chi_0) = \sum_{(n,q)=1}\frac{1}{n^s} = \sum_{n\ge1}\frac{1}{n^s}\sum_{\substack{d\mid q\\ d\mid n}}\mu(d) = \sum_{d\mid q}\mu(d)\sum_{m\ge1}\frac{1}{(dm)^s} = \zeta(s)\sum_{d\mid q}\frac{\mu(d)}{d^s}.$$

Το συμπέρασμα για τον πόλο και το υπόλοιπο προκύπτει από το αντίστοιχο για την ζ. Πράγματι, θέτουμε

$$h(s) := \sum_{d\mid q}\frac{\mu(d)}{d^s}.$$

Επειδή το q είναι σταθερό, το άθροισμα είναι *πεπερασμένο* (τρέχει σε πεπερασμένο πλήθος διαιρετών d). Κάθε όρος $d^{-s} = e^{-s\log d}$ είναι ολόμορφος σε όλο το $\mathbb{C}$, άρα και το h είναι *ολόμορφο σε όλο το* $\mathbb{C}$.

Αν $\zeta(s)$ έχει απλό πόλο στο $s=1$ με υπόλοιπο 1 και h είναι ολόμορφη, τότε

$$\operatorname{Res}_{s=1}\big(\zeta(s)h(s)\big) = h(1)\ \operatorname{Res}_{s=1}\zeta(s) = h(1).$$

Επομένως, από $L(s,\chi_0) = \zeta(s)\,h(s)$ παίρνουμε

$$\operatorname{Res}_{s=1} L(s,\chi_0) = h(1) = \sum_{d\mid q}\frac{\mu(d)}{d} = \prod_{p\mid q}\left(1-\frac{1}{p}\right) = \frac{\varphi(q)}{q}.$$

□

4.3 Μη μηδενισμός στη γραμμή $\operatorname{Re}(s)=1$, $t\neq 0$

Θεώρημα 4.10. *Για κάθε Dirichlet χαρακτήρα χ και κάθε $t\neq 0$ ισχύει*

$$L(1+it,\chi)\neq 0.$$

Απόδειξη. (Όπως στο Θεώρημα των Πρώτων για τη $\zeta(1+it)\neq 0$, με το ίδιο τριγωνομετρικό πολυώνυμο.) Χρησιμοποιούμε την ανισότητα

$$3+4\cos\theta+\cos(2\theta) = 2(1+\cos\theta)^2 \geq 0.$$

Για $\sigma>1$ θέτουμε

$$\mathcal{G}(\sigma) := \zeta(\sigma)^3\,L(\sigma+it,\chi)^4\,L(\sigma+2it,\chi^2).$$

Για $\sigma>1$ όλα τα μέλη είναι μη μηδενικά (για ζ από το Θεώρημα 2.7 του ΠΘΠ, για L από το Θεώρημα 4.5), άρα η $\log|\mathcal{G}(\sigma)|$ είναι καλά ορισμένη.

Παραγωγίζοντας ως προς σ και χρησιμοποιώντας (α) την ταυτότητα $-\zeta'/\zeta = \sum\Lambda(n)n^{-s}$ από την απόδειξη του Θεωρήματος των Πρώτων, (β) το Πόρισμα 4.6 για $-L'/L$, παίρνουμε για $\sigma>1$:

$$-\frac{d}{d\sigma}\log|\mathcal{G}(\sigma)| = \sum_{n\geq 1}\frac{\Lambda(n)}{n^\sigma}\Big(3+4\ \operatorname{Re}(\chi(n)n^{-it}) + \operatorname{Re}(\chi(n)^2 n^{-2it})\Big)\ \geq\ 0.$$

Για να ελέγξουμε το

$$3+4\ \operatorname{Re}\big(\chi(n)n^{-it}\big) + \operatorname{Re}\big(\chi(n)^2 n^{-2it}\big),$$

αρκεί να το κάνουμε για n με $\Lambda(n)\neq 0$, δηλαδή για $n=p^k$. Αν $p\nmid q$, τότε $\chi(p)$ είναι ρίζα της μονάδας, άρα υπάρχει $\phi_p\in\mathbb{R}$ με $\chi(p)=e^{i\phi_p}$. Με πλήρη πολλαπλασιαστικότητα παίρνουμε

$$\chi(p^k) = \chi(p)^k = e^{ik\phi_p}, \qquad (p^k)^{-it} = e^{-it\log(p^k)} = e^{-ikt\log p}.$$

Θέτοντας

$$\theta_p := \phi_p - t\log p,$$

έχουμε

$$\chi(p^k)\,p^{-ikt} = e^{ik(\phi_p - t\log p)} = e^{ik\theta_p} \quad\Rightarrow\quad \operatorname{Re}\big(\chi(p^k)p^{-ikt}\big) = \operatorname{Re}(e^{ik\theta_p}) = \cos(k\theta_p),$$

και επίσης

$$\chi(p^k)^2\,p^{-i2kt} = e^{i2k\theta_p} \quad\Rightarrow\quad \operatorname{Re}\big(\chi(p^k)^2 p^{-i2kt}\big) = \cos(2k\theta_p).$$

Άρα, για $n=p^k$ με $p\nmid q$,

$$3+4\ \operatorname{Re}\big(\chi(n)n^{-it}\big) + \operatorname{Re}\big(\chi(n)^2 n^{-2it}\big) = 3+4\cos(k\theta_p)+\cos(2k\theta_p).$$

Αν $p \mid q$, τότε $\chi(p^k) = 0$ και οι δύο πραγματικοί όροι μηδενίζονται, οπότε μένει απλώς 3. Άρα $\frac{d}{d\sigma} \log|\mathcal{G}(\sigma)| \le 0$ και η $\log|\mathcal{G}(\sigma)|$ είναι μη αύξουσα στο $(1,\infty)$. Άρα για κάθε $1 < \sigma \le 2$ ισχύει

$$\log|\mathcal{G}(\sigma)| \ge \log|\mathcal{G}(2)|.$$

Επειδή $\mathcal{G}(2) \neq 0$ (όλες οι συναρτήσεις $\zeta(2)$, $L(2+it,\chi)$, $L(2+2it,\chi^2)$ είναι πεπερασμένες και μη μηδενικές), έχουμε $|\mathcal{G}(2)| > 0$. Θέτοντας

$$c := |\mathcal{G}(2)|,$$

παίρνουμε

$$|\mathcal{G}(\sigma)| \ge c \qquad (1 < \sigma \le 2).$$

Έστω προς άτοπο ότι $L(1+it,\chi) = 0$ για κάποιο $t \neq 0$. Επειδή η $L(s,\chi)$ είναι ολόμορφη σε γειτονιά του $1+it$, το $1+it$ είναι μηδενικό κάποιας τάξης $m \ge 1$, δηλαδή υπάρχει ολόμορφη h με $h(1+it) \neq 0$ ώστε

$$L(s,\chi) = (s-(1+it))^m h(s) \qquad (\text{για } s \text{ κοντά στο } 1+it).$$

Θέτοντας $s = \sigma + it$ και αφήνοντας $\sigma \downarrow 1$ παίρνουμε

$$|L(\sigma+it,\chi)| \asymp |\sigma-1|^m.$$

Επομένως, ο παράγοντας $L(\sigma+it,\chi)^4$ έχει μηδενικό τάξης $4m$ στο $\sigma = 1$.

Από την άλλη, η $\zeta(s)$ έχει απλό πόλο στο $s = 1$, άρα $\zeta(\sigma)^3$ έχει πόλο τάξης 3 στο $\sigma = 1$ και

$$|\zeta(\sigma)^3| \asymp (\sigma-1)^{-3} \qquad (\sigma \downarrow 1).$$

Τέλος, επειδή $2t \neq 0$, το σημείο $1+2it$ δεν είναι το 1, άρα ο παράγοντας $L(s,\chi^2)$ είναι ολόμορφος σε γειτονιά του $1+2it$ και συνεπώς φραγμένος και μη μηδενικός εκεί:

$$|L(\sigma+2it,\chi^2)| \asymp 1 \qquad (\sigma \downarrow 1).$$

Συνεπώς, για $\sigma \downarrow 1$,

$$|\mathcal{G}(\sigma)| = |\zeta(\sigma)|^3\,|L(\sigma+it,\chi)|^4\,|L(\sigma+2it,\chi^2)| \asymp (\sigma-1)^{-3}\cdot(\sigma-1)^{4m}\cdot 1 = (\sigma-1)^{4m-3}.$$

Επειδή $m \ge 1$, έχουμε $4m-3 \ge 1$, άρα $(\sigma-1)^{4m-3} \to 0$ όταν $\sigma \downarrow 1$. Δηλαδή $|\mathcal{G}(\sigma)| \to 0$ καθώς $\sigma \downarrow 1$, σε αντίφαση με το κάτω φράγμα $|\mathcal{G}(\sigma)| \ge c > 0$ για $1 < \sigma \le 2$. □

Παρατήρηση 4.11. Αν $t = 0$ και χ είναι *μη πραγματικός* μη κύριος χαρακτήρας, τότε $\chi^2 \neq \chi_0$ και η ίδια απόδειξη (με $t = 0$) δίνει $L(1,\chi) \neq 0$. Για πραγματικούς μη κυρίους χαρακτήρες έχουμε $\chi^2 = \chi_0$ και τότε εμφανίζεται πόλος στο $L(s,\chi^2)$ στο $s = 1$, οπότε το παραπάνω επιχείρημα δεν αρκεί. Εκεί χρειάζεται το κλασικό θεώρημα του Dirichlet $L(1,\chi) \neq 0$.

4.4 Μη μηδενισμός στο $s = 1$ για πραγματικούς μη κυρίους χαρακτήρες (μέθοδος Lambert)

Θα δώσουμε μια κλασική απόδειξη ότι $L(1,\chi) \neq 0$ όταν χ είναι *πραγματικός* μη κύριος χαρακτήρας. Η απόδειξη βασίζεται σε μια Lambert–σειρά και σε ένα απλό επιχείρημα «φραγμένο/άφραχτο» καθώς $x \to 1^-$.

Λήμμα 4.12. *Έστω χ μη κύριος Dirichlet χαρακτήρας modulo q. Η σειρά $\sum_{n\ge1} \chi(n)/n$ συγκλίνει και ορίζουμε*

$$L(1,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n}.$$

Απόδειξη. Εφαρμόζουμε μερική άθροιση:

$$\sum_{n\le N}\frac{\chi(n)}{n}=\frac{S_\chi(N)}{N}+\int_1^N\frac{S_\chi(x)}{x^2}\,dx.$$

Εφόσον $S_\chi(x)=O(1)$, το $\frac{S_\chi(N)}{N}\to 0$ και το ολοκλήρωμα $\int_1^\infty S_\chi(x)x^{-2}\,dx$ συγκλίνει απολύτως. Άρα η $\sum_{n\ge1}\chi(n)/n$ συγκλίνει. □

Θεώρημα 4.13. *Έστω χ πραγματικός και μη κύριος Dirichlet χαρακτήρας modulo q. Τότε*

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

Απόδειξη. **Βήμα 1: Ορισμός της Lambert–σειράς και απόλυτη σύγκλιση.** Για $x\in(0,1)$ ορίζουμε

$$f(x):=\sum_{n=1}^{\infty}\chi(n)\frac{x^n}{1-x^n}.$$

Για $0<x<1$ έχουμε $1-x^n\ge 1-x$, άρα

$$\left|\chi(n)\frac{x^n}{1-x^n}\right|\le\frac{x^n}{1-x}.$$

Επομένως η σειρά για το $f(x)$ συγκλίνει απολύτως (και ομοιόμορφα σε κάθε $[0,x_0]$ με $x_0<1$).

Βήμα 2: Ανάπτυγμα $f(x)=\sum_{m\ge1}c_mx^m$ με $c_m\ge0$. Για $0<x<1$ ισχύει

$$\frac{x^n}{1-x^n}=\sum_{j=1}^{\infty}x^{nj}.$$

Λόγω της απόλυτης σύγκλισης μπορούμε να αλλάξουμε τη σειρά αθροίσεως και παίρνουμε

$$f(x)=\sum_{n\ge1}\chi(n)\sum_{j\ge1}x^{nj}=\sum_{m\ge1}\left(\sum_{d\mid m}\chi(d)\right)x^m=:\sum_{m\ge1}c_mx^m,\qquad c_m=\sum_{d\mid m}\chi(d).$$

Θα αποδείξουμε ότι $c_m\ge0$ για κάθε m (εδώ χρησιμοποιούμε ότι χ είναι *πραγματικός*). Επειδή είναι πολλαπλασιαστική συνάρτηση, άρα αρκεί να υπολογίσουμε τα c_{p^k}.

- Αν $p\mid q$, τότε $\chi(p)=0$ και $\chi(p^j)=0$ για $j\ge1$, άρα

$$c_{p^k}=\sum_{j=0}^{k}\chi(p^j)=\chi(1)=1.$$

- Αν $p\nmid q$ και $\chi(p)=1$, τότε $\chi(p^j)=1$ και

$$c_{p^k}=\sum_{j=0}^{k}1=k+1\ge0.$$

- Αν $p\nmid q$ και $\chi(p)=-1$, τότε $\chi(p^j)=(-1)^j$ και

$$c_{p^k}=\sum_{j=0}^{k}(-1)^j=\begin{cases}1, & k\text{ άρτιος},\\ 0, & k\text{ περιττός},\end{cases}$$

  άρα πάλι $c_{p^k}\ge0$.

Άρα $c_m = \prod_p c_{p^{v_p(m)}} \geq 0$ για κάθε m.

Επιπλέον, επειδή $q \geq 2$, υπάρχει πρώτος $p \mid q$ και τότε, όπως είδαμε, $c_{p^k} = 1$ για κάθε $k \geq 1$. Άρα υπάρχουν *άπειροι* δείκτες m με $c_m \geq 1$.

Βήμα 3: Το $f(x)$ τείνει στο άπειρο καθώς $x \to 1^-$. Πάρε έναν πρώτο $p \mid q$. Για κάθε $K \geq 1$,

$$f(x) = \sum_{m \geq 1} c_m x^m \;\geq\; \sum_{k=1}^{K} c_{p^k} x^{p^k} \;=\; \sum_{k=1}^{K} x^{p^k}.$$

Δοθέντος $M > 0$, διάλεξε $K \geq 2M$. Επειδή $x^{p^K} \to 1$ όταν $x \to 1^-$, υπάρχει $x_0 \in (0,1)$ ώστε $x^{p^K} \geq \frac{1}{2}$ για κάθε $x \in [x_0, 1)$. Τότε για κάθε τέτοιο x και κάθε $1 \leq k \leq K$ ισχύει $x^{p^k} \geq x^{p^K} \geq \frac{1}{2}$, άρα

$$f(x) \geq \sum_{k=1}^{K} x^{p^k} \geq K \cdot \frac{1}{2} \geq M.$$

Άρα $f(x) \to +\infty$ κατά μήκος $x \to 1^-$, δηλαδή η f δεν είναι φραγμένη κοντά στο 1.

Βήμα 4: Αν $L(1,\chi) = 0$, τότε το $f(x)$ είναι φραγμένο κοντά στο 1 (αντίφαση). Για $n \geq 1$ και $x \in (0,1)$ ορίζουμε

$$b_n(x) := \frac{1}{n(1-x)} - \frac{x^n}{1-x^n}.$$

Παρατηρούμε πρώτα ότι $b_n(x) \geq 0$. Πράγματι, $b_n(x) \geq 0$ ισοδυναμεί με

$$\frac{1}{n(1-x)} \geq \frac{x^n}{1-x^n} \iff \frac{1-x^n}{1-x} \geq nx^n \iff (1 + x + \cdots + x^{n-1}) \geq nx^n,$$

και αυτό ισχύει επειδή για $0 < x < 1$ έχουμε $x^k \geq x^{n-1} \geq x^n$ για $k = 0, 1, \ldots, n-1$, άρα $1 + x + \cdots + x^{n-1} \geq nx^n$.

Θα χρειαστούμε επίσης ότι για κάθε σταθερό $x \in (0,1)$ η ακολουθία $n \mapsto b_n(x)$ είναι *φθίνουσα* και τείνει στο 0. Το $b_n(x) \to 0$ είναι άμεσο από

$$0 \leq b_n(x) \leq \frac{1}{n(1-x)} \xrightarrow[n\to\infty]{} 0.$$

Για τη μονοτονία, θέτουμε

$$A_n(x) := 1 + x + \cdots + x^{n-1}, \qquad B_n(x) := 1 + x + \cdots + x^n.$$

Τότε

$$\frac{x^n}{1-x^n} = \frac{x^n}{(1-x)A_n(x)}, \qquad \frac{x^{n+1}}{1-x^{n+1}} = \frac{x^{n+1}}{(1-x)B_n(x)},$$

και με απλή πράξη παίρνουμε

$$b_n(x) - b_{n+1}(x) = \frac{1}{1-x}\left(\frac{1}{n(n+1)} - \frac{x^n}{A_n(x)B_n(x)}\right).$$

Άρα αρκεί να δείξουμε ότι $A_n(x)B_n(x) \geq n(n+1)x^n$. Με AM–GM,

$$\frac{A_n(x)}{n} \geq \left(x^{0+1+\cdots+(n-1)}\right)^{1/n} = x^{(n-1)/2}, \qquad \frac{B_n(x)}{n+1} \geq \left(x^{0+1+\cdots+n}\right)^{1/(n+1)} = x^{n/2}.$$

Πολλαπλασιάζοντας,

$$A_n(x)B_n(x) \geq n(n+1)x^{(n-1)/2+n/2} = n(n+1)x^{n-1/2} \geq n(n+1)x^n$$

(επειδή $0 < x < 1$ και $x^{n-1/2} \geq x^n$). Άρα $b_n(x) - b_{n+1}(x) \geq 0$, δηλαδή $b_n(x)$ είναι φθίνουσα ως προς n.

Τώρα, για κάθε N έχουμε την ταυτότητα (απλώς από τον ορισμό του b_n)

$$\sum_{n\leq N} \chi(n)\frac{x^n}{1-x^n} = \frac{1}{1-x}\sum_{n\leq N}\frac{\chi(n)}{n} \; - \; \sum_{n\leq N}\chi(n)b_n(x).$$

Περνάμε στο όριο $N \to \infty$. Από το Λήμμα 4.12 το $\sum_{n\leq N}\chi(n)/n \to L(1,\chi)$. Επίσης, για σταθερό $x \in (0,1)$, η σειρά $\sum_{n\geq 1}\chi(n)b_n(x)$ συγκλίνει (Dirichlet test), επειδή τα μερικά αθροίσματα $S_\chi(N)$ είναι φραγμένα και η $b_n(x)$ είναι φθίνουσα προς το 0. Άρα

$$f(x) = \frac{L(1,\chi)}{1-x} - \sum_{n=1}^{\infty}\chi(n)b_n(x).$$

Υποθέτουμε προς άτοπο ότι $L(1,\chi) = 0$. Τότε

$$f(x) = -\sum_{n=1}^{\infty}\chi(n)b_n(x).$$

Θα δείξουμε ότι το δεξί μέλος είναι *ομοιόμορφα φραγμένο* ως προς $x \in (0,1)$. Θέτουμε $S_\chi(N) = \sum_{n\leq N}\chi(n)$ και $C := \sup_N |S_\chi(N)| < \infty$. Με άθροιση κατά μέρη, για κάθε N,

$$\sum_{n\leq N}\chi(n)b_n(x) = S_\chi(N)b_N(x) + \sum_{n=1}^{N-1} S_\chi(n)\big(b_n(x) - b_{n+1}(x)\big).$$

Παίρνοντας απόλυτες τιμές και χρησιμοποιώντας $|S_\chi(\cdot)| \leq C$ και $b_n(x) - b_{n+1}(x) \geq 0$, παίρνουμε

$$\left|\sum_{n\leq N}\chi(n)b_n(x)\right| \leq C\,b_N(x) + C\sum_{n=1}^{N-1}\big(b_n(x) - b_{n+1}(x)\big) = C\,b_N(x) + C\,(b_1(x) - b_N(x)) \leq C\,b_1(x).$$

Αλλά $b_1(x) = \frac{1}{1-x} - \frac{x}{1-x} = 1$ για κάθε $x \in (0,1)$. Άρα

$$\left|\sum_{n\leq N}\chi(n)b_n(x)\right| \leq C \qquad \text{για όλα τα } N \in \mathbb{N},\ x \in (0,1).$$

Περνώντας $N \to \infty$, παίρνουμε

$$|f(x)| \leq C \qquad \text{για όλα τα } x \in (0,1),$$

δηλαδή το f είναι φραγμένο κοντά στο 1.

Αυτό αντιφάσκει με το Βήμα 3, όπου δείξαμε ότι $f(x)$ είναι απεριόριστο καθώς $x \to 1^-$. Άρα η υπόθεση $L(1,\chi) = 0$ είναι άτοπη και συνεπώς $L(1,\chi) \neq 0$. □

5 Μη μηδενισμός στο $s = 1$ για πραγματικούς χαρακτήρες (μέθοδος Landau)

Λήμμα 5.1. *Έστω χ πραγματικός Dirichlet χαρακτήρας modulo q. Για $\mathrm{Re}(s) > 1$ ισχύει*

$$\zeta(s)L(s,\chi) = \sum_{n=1}^{\infty}\frac{a_n}{n^s}, \qquad a_n = \sum_{d\mid n}\chi(d).$$

Επιπλέον $a_n \geq 0$ για κάθε n και $a_{m^2} \geq 1$ για κάθε $m \in \mathbb{N}$.

Απόδειξη. (Χωρίς Euler προϊόν: μόνο Cauchy product.) Για $\mathrm{Re}(s) > 1$ οι σειρές $\zeta(s) = \sum_{n\ge1} n^{-s}$ και $L(s,\chi) = \sum_{n\ge1} \chi(n) n^{-s}$ συγκλίνουν απολύτως, άρα

$$\zeta(s)L(s,\chi) = \sum_{k\ge1} \frac{1}{k^s} \sum_{d\mid k} \chi(d),$$

οπότε $a_k = \sum_{d\mid k} \chi(d)$.

Η $a = 1 * \chi$ είναι πολλαπλασιαστική, άρα αρκεί να ελέγξουμε a_{p^k}. Αν $p \mid q$, τότε $\chi(p) = 0$ και $a_{p^k} = 1$. Αν $p \nmid q$ και $\chi(p) = 1$, τότε $a_{p^k} = k+1$. Αν $p \nmid q$ και $\chi(p) = -1$, τότε $a_{p^k} = 1$ για k άρτιο και $a_{p^k} = 0$ για k περιττό. Άρα $a_{p^k} \ge 0$ και για άρτιο εκθέτη $2k$ ισχύει $a_{p^{2k}} \ge 1$. Επομένως $a_n \ge 0$ και $a_{m^2} \ge 1$. □

5.1 Ολοκλήρωση της Απόδειξης με Tauberian

Από (38) βλέπουμε ότι η $F_{q,a}(s)$ γράφεται ως πεπερασμένο άθροισμα λογαριθμικών παραγώγων L-συναρτήσεων. Από την Πρόταση 4.9 ο όρος του κύριου χαρακτήρα χ_0 δίνει απλό πόλο στο $s = 1$, ενώ από τα Θεωρήματα 4.10 και ?? (και το Σχόλιο 4.11) παίρνουμε ότι για κάθε μη κύριο χ η $L(s,\chi)$ είναι ολόμορφη στο $\mathrm{Re}(s) > 0$ και δεν μηδενίζεται στη γραμμή $\mathrm{Re}(s) = 1$, άρα η $-L'/L(s,\chi)$ είναι ολόμορφη σε γειτονιά της $\mathrm{Re}(s) = 1$. Συνεπώς η $F_{q,a}(s)$ έχει μερομορφική συνέχιση στο $\mathrm{Re}(s) \ge 1$ με *μοναδικό* απλό πόλο στο $s = 1$ και υπόλοιπο $1/\varphi(q)$. Πράγματι, θυμίζουμε ότι για $\mathrm{Re}(s) > 1$ (και κατόπιν με αναλυτική συνέχιση) έχουμε την αναπαράσταση μέσω χαρακτήρων

$$F_{q,a}(s) = -\frac{1}{\varphi(q)} \sum_{\chi \pmod q} \overline{\chi}(a)\, \frac{L'}{L}(s,\chi).$$

Για κάθε *μη κύριο* χαρακτήρα $\chi \ne \chi_0$ έχουμε $L(1,\chi) \ne 0$, άρα η $L(s,\chi)$ είναι ολόμορφη και μη μηδενική σε γειτονιά του $s = 1$, οπότε $\frac{L'}{L}(s,\chi)$ είναι επίσης ολόμορφη εκεί. Συνεπώς αυτοί οι όροι δεν δίνουν πόλο στο $s = 1$.

Ο μοναδικός όρος που μπορεί να δώσει ανωμαλία είναι ο όρος του *κύριου* χαρακτήρα χ_0. Έχουμε (π.χ. από $L(s,\chi_0) = \zeta(s)\sum_{d\mid q} \mu(d) d^{-s}$) ότι $L(s,\chi_0)$ έχει απλό πόλο στο $s = 1$, άρα γράφεται κοντά στο 1 ως

$$L(s,\chi_0) = \frac{c}{s-1} + h(s), \qquad c \ne 0, \quad h \text{ ολόμορφη}.$$

Τότε

$$\frac{L'}{L}(s,\chi_0) = \frac{d}{ds}\log L(s,\chi_0) = -\frac{1}{s-1} + (\text{ολόμορφος όρος}),$$

άρα

$$\mathrm{Res}_{s=1} \frac{L'}{L}(s,\chi_0) = -1 \qquad \Big(\text{ισοδύναμα } \mathrm{Res}_{s=1}\Big(-\frac{L'}{L}(s,\chi_0)\Big) = 1\Big).$$

Επειδή $\overline{\chi_0}(a) = 1$, το υπόλοιπο της $F_{q,a}(s)$ στο $s = 1$ είναι μόνο η συνεισφορά του χ_0:

$$\mathrm{Res}_{s=1} F_{q,a}(s) = -\frac{1}{\varphi(q)}\,\overline{\chi_0}(a)\,\mathrm{Res}_{s=1}\frac{L'}{L}(s,\chi_0) = -\frac{1}{\varphi(q)}\cdot 1\cdot(-1) = \frac{1}{\varphi(q)}.$$

Άρα η $F_{q,a}(s)$ έχει *μοναδικό* απλό πόλο στο $s = 1$ και υπόλοιπο $1/\varphi(q)$. Εφαρμόζοντας τώρα το *ίδιο Tauberian θεώρημα* που χρησιμοποιήθηκε στο ΠΘΠ (Wiener–Ikehara) στην $F_{q,a}(s)$ και στο $A(x) = \psi(x;q,a)$ μέσω της Mellin αναπαράστασης (35), καταλήγουμε

$$\psi(x;q,a) \sim \frac{x}{\varphi(q)} \qquad (x \to \infty).$$

Πρόταση 5.2. *Έστω $q \geq 2$ και $(a,q)=1$. Αν ισχύει η ασυμπτωτική*

$$\psi(x;q,a) \sim \frac{x}{\varphi(q)} \qquad (x \to \infty),$$

τότε

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod q}} \frac{\log p}{p} = \frac{1}{\varphi(q)} \log x + O(1) \qquad (x \to \infty).$$

Απόδειξη. Θέτουμε

$$a_n := \Lambda(n)\, \mathbf{1}_{n \equiv a \pmod q}, \qquad A(t) := \sum_{n \leq t} a_n = \psi(t;q,a), \qquad f(t) := \frac{1}{t}.$$

Εφαρμόζοντας το Θεώρημα 1.1 στο διάστημα $[1,x]$ παίρνουμε

$$\sum_{1 < n \leq x} \frac{\Lambda(n) \mathbf{1}_{n \equiv a(q)}}{n} = \frac{\psi(x;q,a)}{x} - \psi(1;q,a) + \int_1^x \frac{\psi(t;q,a)}{t^2}\, dt. \tag{39}$$

Το αριστερό μέλος γράφεται ως

$$\sum_{\substack{n \leq x \\ n \equiv a(q)}} \frac{\Lambda(n)}{n} = \sum_{\substack{p \leq x \\ p \equiv a(q)}} \frac{\log p}{p} + \sum_{\substack{p^k \leq x \\ k \geq 2 \\ p^k \equiv a(q)}} \frac{\log p}{p^k}.$$

Ο δεύτερος όρος είναι $O(1)$, διότι

$$0 \leq \sum_{\substack{p^k \leq x \\ k \geq 2}} \frac{\log p}{p^k} \leq \sum_p \sum_{k \geq 2} \frac{\log p}{p^k} = \sum_p \frac{\log p}{p^2} \cdot \frac{1}{1 - 1/p} \ll \sum_p \frac{\log p}{p^2} < \infty.$$

Άρα από (39) προκύπτει

$$\sum_{\substack{p \leq x \\ p \equiv a(q)}} \frac{\log p}{p} = \frac{\psi(x;q,a)}{x} + \int_1^x \frac{\psi(t;q,a)}{t^2}\, dt + O(1). \tag{40}$$

Τώρα χρησιμοποιούμε την υπόθεση $\psi(t;q,a) \sim t/\varphi(q)$. Τότε $\psi(x;q,a)/x \to 1/\varphi(q)$ και, γράφοντας $\psi(t;q,a) = \frac{t}{\varphi(q)} + o(t)$, έχουμε

$$\int_1^x \frac{\psi(t;q,a)}{t^2}\, dt = \frac{1}{\varphi(q)} \int_1^x \frac{dt}{t} + \int_1^x o\left(\frac{1}{t}\right) dt = \frac{1}{\varphi(q)} \log x + o(\log x).$$

Επιστρέφοντας στο (40), παίρνουμε

$$\sum_{\substack{p \leq x \\ p \equiv a(q)}} \frac{\log p}{p} = \frac{1}{\varphi(q)} \log x + O(1),$$

όπως θέλαμε. □

Πρόταση 5.3. *Υπό τις ίδιες υποθέσεις, ισχύει*

$$\pi(x;q,a) \sim \frac{x}{\varphi(q) \log x} \qquad (x \to \infty),$$

όπου $\pi(x;q,a) = \#\{p \leq x : \ p \equiv a \pmod q\}$.

Απόδειξη. Το επιχείρημα είναι ακριβώς το ίδιο όπως στο Θεώρημα των Πρώτων, με αντικατάσταση

$$\psi(x) \rightsquigarrow \psi(x;q,a), \qquad \theta(x) \rightsquigarrow \theta(x;q,a), \qquad \pi(x) \rightsquigarrow \pi(x;q,a).$$

Πρώτα δείχνουμε ότι $\psi(x;q,a) \sim x/\varphi(q)$ συνεπάγεται $\theta(x;q,a) \sim x/\varphi(q)$, επειδή η διαφορά $\psi - \theta$ προέρχεται μόνο από δυνάμεις p^k με $k \geq 2$ και είναι $O(\sqrt{x}\log x)$. Έπειτα εφαρμόζουμε άθροιση κατά Abel στην ταυτότητα

$$\theta(x;q,a) = \sum_{\substack{p \leq x \\ p \equiv a(q)}} \log p$$

με $A(t) = \pi(t;q,a)$ και $f(t) = \log t$, και καταλήγουμε στο $\pi(x;q,a) \sim x/(\varphi(q)\log x)$ όπως στο κλασικό ΠΘΠ. □

Λήμμα 5.4 (Συνέπεια Dirichlet για $q = 4$)**.** *Ισχύει*

$$\sum_{\substack{p \leq x \\ p \equiv 3 \pmod 4}} \frac{\log p}{p} = \frac{1}{2}\log x + O(1), \qquad \sum_{\substack{p \leq x \\ p \equiv 1 \pmod 4}} \frac{\log p}{p} = \frac{1}{2}\log x + O(1).$$

Επίσης

$$\sum_{\substack{p \leq x \\ p \equiv 1 \ (4)}} \frac{\log p}{p-1} = \frac{1}{2}\log x + O(1).$$

Απόδειξη. Οι δύο πρώτες σχέσεις είναι η ειδική περίπτωση $q = 4$, $a = 3$ ή $a = 1$ της γενικής συνέπειας

$$\sum_{\substack{p \leq x \\ p \equiv a \ (q)}} \frac{\log p}{p} = \frac{1}{\varphi(q)}\log x + O(1) \qquad ((a,q) = 1).$$

Για την τρίτη, γράφουμε

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

Επειδή $\sum_p \frac{\log p}{p^2} < \infty$, το σφάλμα αθροίζει σε $O(1)$ και παίρνουμε

$$\sum_{\substack{p \leq x \\ p \equiv 1 \ (4)}} \frac{\log p}{p-1} = \sum_{\substack{p \leq x \\ p \equiv 1 \ (4)}} \frac{\log p}{p} + O(1) = \frac{1}{2}\log x + O(1).$$

□

Πρόταση 5.5. *Η εξίσωση*

$$x^8 = n! + 1$$

έχει μόνο πεπερασμένες λύσεις σε μη αρνητικούς ακεραίους (x,n)*.*

Απόδειξη. Έστω (x,n) λύση. Τότε

$$n! = x^8 - 1 = (x^2-1)(x^2+1)(x^4+1).$$

Επειδή $x^2+1 \geq x^2-1$ και $x^4+1 \geq (x^2-1)^2$, παίρνουμε

$$n! \ \geq \ (x^2-1)\,(x^2-1)\,(x^2-1)^2 = (x^2-1)^4,$$

άρα

$$x^2 - 1 \ \leq \ (n!)^{1/4}. \tag{41}$$

Θέτουμε

$$A_n := \{\, p \le n : \ p \text{ πρώτος και } p \equiv 3 \pmod 4 \,\}.$$

Από το Λήμμα ??, για κάθε $p \in A_n$ ισχύει $p \nmid (x^2+1)(x^4+1)$, άρα όλη η δύναμη του p μέσα στο $n!$ διαιρεί τον παράγοντα x^2-1:

$$p^{v_p(n!)} \mid (x^2-1) \qquad (p \in A_n).$$

Επομένως

$$x^2 - 1 \ \ge \ \prod_{p \in A_n} p^{v_p(n!)}.$$

Παίρνοντας λογαρίθμους και χρησιμοποιώντας την (41) παίρνουμε

$$\frac{1}{4}\log(n!) \ \ge \ \sum_{p \in A_n} v_p(n!)\log p.$$

Με το Λήμμα ?? έχουμε $v_p(n!) \ge n/p - 1$, άρα

$$\frac{1}{4}\log(n!) \ \ge \ \sum_{p \in A_n} \Big(\frac{n}{p} - 1\Big)\log p = n \sum_{p \in A_n} \frac{\log p}{p} \ - \ \sum_{p \in A_n} \log p.$$

Άρα

$$\sum_{p \in A_n} \frac{\log p}{p} \ \le \ \frac{1}{4n}\log(n!) \ + \ \frac{1}{n}\sum_{p \in A_n} \log p. \tag{42}$$

Όμως, $\log(n!) = n\log n + O(n)$, επομένως

$$\frac{1}{4n}\log(n!) = \frac{1}{4}\log n + O(1).$$

Επίσης από την εκτίμηση Chebyshev, Θεώρημα 3.7, παίρνουμε $\sum_{p \in A_n} \log p \le \sum_{p \le n} \log p = O(n)$, άρα ο δεύτερος όρος του (42) είναι $O(1)$. Συμπεραίνουμε

$$\sum_{\substack{p \le n \\ p \equiv 3 \ (4)}} \frac{\log p}{p} \ \le \ \frac{1}{4}\log n + O(1). \tag{43}$$

Όμως από το Λήμμα 5.4 έχουμε

$$\sum_{\substack{p \le n \\ p \equiv 3 \ (4)}} \frac{\log p}{p} = \frac{1}{2}\log n + O(1),$$

που αντιφάσκει με (43) για $n \to \infty$ (διότι $\frac{1}{2} > \frac{1}{4}$). Άρα τα n που επιτρέπουν λύση είναι φραγμένα, δηλαδή υπάρχουν μόνο πεπερασμένες λύσεις. □

Λήμμα 5.6. *Για* $P_n := \prod_{k=1}^{n}(k^2+1)$ *ισχύει*

$$v_2(P_n) = \#\{1 \le k \le n : \ k \text{ περιττός}\} = \Big\lfloor \frac{n+1}{2} \Big\rfloor.$$

Απόδειξη. Αν k είναι περιττός, τότε $k^2 \equiv 1 \pmod 4$, άρα $k^2+1 \equiv 2 \pmod 4$ και $v_2(k^2+1) = 1$. Αν k είναι άρτιος, τότε k^2+1 είναι περιττός και $v_2(k^2+1) = 0$. Άρα $v_2(P_n)$ ισούται με το πλήθος των περιττών $k \le n$. □

Λήμμα 5.7. *Θέτουμε* $P_n = \prod_{k=1}^{n}(k^2+1)$. *Για κάθε περιττό πρώτο* p *ισχύει*

$$v_p(P_n) \;\le\; 2\big\lfloor \log_p(n^2+1)\big\rfloor \;+\; \frac{2n}{p-1}.$$

Απόδειξη. Για $i \ge 1$ θέτουμε

$$n_i := \#\{1 \le k \le n :\; p^i \mid k^2+1\}.$$

Τότε (κλασικά)

$$v_p(P_n) = \sum_{k=1}^{n} v_p(k^2+1) = \sum_{i\ge 1} n_i,$$

και ο όρος n_i μηδενίζεται για $i > \log_p(n^2+1)$, διότι $p^i \le k^2+1 \le n^2+1$. Άρα

$$v_p(P_n) = \sum_{i=1}^{\lfloor \log_p(n^2+1)\rfloor} n_i.$$

Μένει να φράξουμε τα n_i. Για σταθερό i, η ισοτιμία $k^2 \equiv -1 \pmod{p^i}$ έχει *το πολύ* 2 λύσεις modulo p^i (αν $u^2 \equiv v^2 \equiv -1 \pmod{p^i}$ τότε $p^i \mid (u-v)(u+v)$ και επειδή p είναι περιττός, δεν μπορεί να διαιρεί ταυτόχρονα και τους δύο παράγοντες χωρίς να αναγκάζει $u \equiv \pm v \pmod{p^i}$). Άρα, στο διάστημα $\{1,2,\dots,n\}$, κάθε πλήρες σύστημα υπολοίπων modulo p^i δίνει το πολύ 2 λύσεις, οπότε

$$n_i \le 2\Big(\frac{n}{p^i}+1\Big) = \frac{2n}{p^i} + 2.$$

Συνεπώς

$$v_p(P_n) \le \sum_{i=1}^{\lfloor \log_p(n^2+1)\rfloor} \Big(\frac{2n}{p^i}+2\Big) \le \frac{2n}{p-1} + 2\big\lfloor \log_p(n^2+1)\big\rfloor.$$

□

Πρόταση 5.8. *Για κάθε* $c > 0$ *υπάρχουν άπειρα* m *τέτοια ώστε ο μέγιστος πρώτος διαιρέτης του* m^2+1 *ικανοποιεί*

$$P^+(m^2+1) > c\,m.$$

Απόδειξη. Θέτουμε

$$P_n := \prod_{k=1}^{n}(k^2+1), \qquad f(n) := P^+(P_n) \;\; (\text{ο μέγιστος πρώτος διαιρέτης του } P_n).$$

Θα δείξουμε ότι

$$\frac{f(n)}{n} \longrightarrow \infty. \tag{44}$$

Αυτό αρκεί: αν η (44) ισχύει, τότε για κάθε $c > 0$ υπάρχουν άπειρα n με $f(n) > cn$. Για τέτοιο n, ο πρώτος $f(n)$ διαιρεί κάποιον παράγοντα k^2+1 με $1 \le k \le n$, άρα $P^+(k^2+1) \ge f(n) > cn \ge ck$. Έτσι παίρνουμε άπειρα $m := k$.

1) Κάτω φράγμα για $\log P_n$. Επειδή $k^2+1 > k^2$, έχουμε

$$P_n = \prod_{k=1}^{n}(k^2+1) \;>\; \prod_{k=1}^{n} k^2 = (n!)^2,$$

άρα

$$\log P_n \;>\; 2\log(n!). \tag{45}$$

2) Ποιους πρώτους μπορεί να έχει το P_n. Αν p είναι περιττός πρώτος και $p \mid (k^2+1)$, τότε $k^2 \equiv -1 \pmod p$, άρα -1 είναι τετραγωνικό υπόλοιπο mod p, οπότε $p \equiv 1 \pmod 4$. Συνεπώς όλοι οι περιττοί πρώτοι διαιρέτες του P_n είναι $\equiv 1 \pmod 4$, και επιπλέον είναι $\le f(n)$ από τον ορισμό του $f(n)$.

Άρα, γράφοντας την παραγοντοποίηση,

$$\log P_n = v_2(P_n)\log 2 + \sum_{\substack{p \le f(n)\\ p\equiv 1 \pmod 4}} v_p(P_n)\,\log p.$$

3) Άνω φράγμα για $\log P_n$ μέσω των $v_p(P_n)$. Από το Λήμμα 5.6 έχουμε $v_2(P_n) = \lfloor (n+1)/2 \rfloor$, άρα $v_2(P_n)\log 2 = O(n)$.

Για κάθε περιττό p εφαρμόζουμε το Λήμμα 5.7:

$$v_p(P_n)\log p \le 2\big\lfloor \log_p(n^2+1)\big\rfloor \log p + \frac{2n}{p-1}\log p.$$

Αλλά $\lfloor \log_p(n^2+1)\rfloor \log p \le \log(n^2+1) \le 3\log n$ για $n \ge 2$. Άρα

$$\sum_{\substack{p \le f(n)\\ p\equiv 1 \pmod 4}} \big\lfloor \log_p(n^2+1)\big\rfloor \log p \le 3\log n \cdot \pi(f(n)),$$

όπου π είναι η συνάρτηση πλήθους πρώτων.

Συνεπώς, για $n \ge 2$,

$$\log P_n \le 6\log n \cdot \pi(f(n)) + 2n \sum_{\substack{p \le f(n)\\ p\equiv 1 \pmod 4}} \frac{\log p}{p-1} + O(n). \tag{46}$$

4) Χρήση των γνωστών εκτιμήσεων (Chebyshev + Dirichlet). Από την κλασική εκτίμηση Chebyshev ισχύει

$$\pi(x) \ll \frac{x}{\log x} \qquad (x \ge 2).$$

Επίσης, από το Λήμμα 5.4 έχουμε

$$\sum_{\substack{p \le y\\ p\equiv 1 \pmod 4}} \frac{\log p}{p-1} = \frac{1}{2}\log y + O(1).$$

Εφαρμόζοντας τα στο (46) (με $y = f(n)$) παίρνουμε

$$\log P_n \le 6\log n \cdot O\Big(\frac{f(n)}{\log f(n)}\Big) + 2n\Big(\frac{1}{2}\log f(n) + O(1)\Big) + O(n).$$

Δηλαδή

$$\log P_n \le O\Big(\frac{f(n)\log n}{\log f(n)}\Big) + n\log f(n) + O(n). \tag{47}$$

Συνδυάζοντας (45) και (47) και διαιρώντας με $n\log n$, χρησιμοποιώντας $\log(n!) = n\log n - n + O(\log n)$, παίρνουμε

$$2 \le O\Big(\frac{f(n)}{n\log f(n)}\Big) + \frac{\log f(n)}{\log n} + o(1).$$

5) Συμπέρασμα. Αν υπήρχε $C > 0$ ώστε $f(n) \le Cn$ για όλα τα μεγάλα n, τότε $\frac{\log f(n)}{\log n} \to 1$ και $\frac{f(n)}{n\log f(n)} = O(1/\log n) \to 0$, άρα από την προηγούμενη ανισότητα θα παίρναμε $2 \le 1$, άτοπο. Άρα το $f(n)/n$ δεν μπορεί να είναι φραγμένο, δηλαδή ισχύει (44), και συνεπώς ολοκληρώνεται η απόδειξη του ισχυρισμού. □

6 Ανασκόπηση των άπειρων γινομένων

Η έννοια των άπειρων γινομένων μπορεί να οριστεί με τρόπο παρόμοιο με εκείνον των άπειρων αθροισμάτων. Θεωρούμε το άπειρο γινόμενο

$$\prod_{n=1}^{\infty} x_n,$$

όπου (x_n) είναι ακολουθία μιγαδικών αριθμών. Για κάθε $k \in \mathbb{N}$, θέτουμε

$$P_k = \prod_{n=1}^{k} x_n = x_1 x_2 x_3 \cdots x_k,$$

το οποίο ονομάζεται *μερικό γινόμενο* του $\prod_{n=1}^{\infty} x_n$.

Ένας προφανής τρόπος να ορίσουμε τη σύγκλιση του άπειρου γινομένου $\prod_{n=1}^{\infty} x_n$ είναι να πούμε ότι η ακολουθία (P_k) των μερικών γινομένων συγκλίνει. Ωστόσο, για τεχνικούς λόγους, είναι χρησιμότερος ένας ελαφρώς διαφορετικός ορισμός.

Ορισμός 6.1. Λέμε ότι το άπειρο γινόμενο $\prod_{n=1}^{\infty} x_n$ *συγκλίνει* αν ισχύουν τα εξής:

(i) υπάρχει θετικός ακέραιος k τέτοιος ώστε $x_n \neq 0$ για κάθε $n \geq k$,

(ii) υπάρχει το όριο

$$\lim_{m\to\infty} \prod_{n=k}^{m} x_n$$

και είναι μη μηδενικό.

Αν το $\prod_{n=1}^{\infty} x_n$ συγκλίνει, ορίζουμε την τιμή του ως

$$\prod_{n=1}^{\infty} x_n = \left(\prod_{n=1}^{k-1} x_n\right)\left(\lim_{m\to\infty} \prod_{n=k}^{m} x_n\right).$$

Από τον παραπάνω ορισμό βλέπουμε ότι το $\prod_{n=1}^{\infty} x_n$ συγκλίνει στο 0 αν και μόνο αν υπάρχει τουλάχιστον ένας θετικός ακέραιος n τέτοιος ώστε $x_n = 0$, και υπάρχουν μόνο πεπερασμένοι τέτοιοι n. Για παράδειγμα, το άπειρο γινόμενο

$$(0)(1)(1)(1)(1)(1)\cdots$$

συγκλίνει στο 0, ενώ τα άπειρα γινόμενα

$$(0)(1)(0)(1)(0)(1)\cdots, \qquad (1)\left(\frac{1}{2}\right)(1)\left(\frac{1}{2}\right)(1)\left(\frac{1}{2}\right)\cdots, \qquad \text{και} \qquad (0)(1)(2)(3)(4)(5)\cdots$$

αποκλίνουν.

Για να δικαιολογήσουμε εύκολα τη σύγκλιση γινομένων όπως

$$\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{4^2}\right)\left(1-\frac{1}{5^2}\right)\cdots$$

και

$$\left(1+\frac{1}{2^2}\right)\left(1+\frac{1}{3^2}\right)\left(1+\frac{1}{4^2}\right)\left(1+\frac{1}{5^2}\right)\cdots, \tag{48}$$

είναι χρήσιμο να υπενθυμίσουμε τα ακόλουθα γνωστά αποτελέσματα.

Θεώρημα 6.2. *Αν το* $\prod_{n=1}^{\infty} x_n$ *συγκλίνει, τότε* $x_n \to 1$.

Απόδειξη. Έστω $N \in \mathbb{N}$ τέτοιος ώστε $x_n \neq 0$ για κάθε $n \geq N$. Τότε, για κάθε $n > N$, έχουμε

$$x_n = \frac{\prod_{i=N}^{n} x_i}{\prod_{i=N}^{n-1} x_i}.$$

Εφόσον τα $\prod_{i=N}^{n} x_i$ και $\prod_{i=N}^{n-1} x_i$ συγκλίνουν στο ίδιο μη μηδενικό όριο όταν $n \to \infty$, παίρνουμε $x_n \to 1$, όπως θέλαμε. □

Ως συνέπεια αυτού του θεωρήματος, είναι συνηθισμένο να γράφουμε άπειρα γινόμενα στην ειδική μορφή

$$\prod_{n=1}^{\infty}(1 + a_n)$$

και να θυμόμαστε ότι, σε ένα συγκλίνον γινόμενο, η ακολουθία (a_n) συγκλίνει στο 0. Επιπλέον, επιτρέπουμε να είναι $a_n = -1$ μόνο για πεπερασμένους δείκτες n. Η απόλυτη σύγκλιση είναι επίσης εύκολο να θυμόμαστε.

Ορισμός 6.3. Έστω (a_n) ακολουθία μιγαδικών αριθμών. Το άπειρο γινόμενο

$$\prod_{n=1}^{\infty}(1 + a_n)$$

λέγεται *απολύτως συγκλίνον* αν το

$$\prod_{n=1}^{\infty}(1 + |a_n|)$$

συγκλίνει.

Στη συνέχεια δίνουμε το κριτήριο Cauchy για άπειρα γινόμενα, το οποίο είναι ανάλογο με το κριτήριο Cauchy για άπειρα αθροίσματα. Στην πραγματικότητα, και οι δύο εκδοχές αποδεικνύονται με παρόμοιο τρόπο, όπως θα δούμε στο επόμενο θεώρημα.

Θεώρημα 6.4 (Κριτήριο Cauchy). *Υποθέτουμε ότι* $a_n \neq -1$ *για κάθε* n. *Τότε το άπειρο γινόμενο*

$$\prod_{n=1}^{\infty}(1 + a_n)$$

συγκλίνει αν και μόνο αν

$$\lim_{m,k\to\infty}\left(\prod_{n=k}^{m}(1 + a_n)\right) = 1,$$

δηλαδή αν για κάθε $\varepsilon > 0$ *υπάρχει* $N \in \mathbb{N}$ *τέτοιο ώστε για κάθε* $m \geq k \geq N$

$$\left|\prod_{n=k}^{m}(1 + a_n) - 1\right| < \varepsilon.$$

Απόδειξη. Θέτουμε

$$P_k = \prod_{n=1}^{k}(1 + a_n).$$

Υποθέτουμε πρώτα ότι το $\prod_{n=1}^{\infty}(1 + a_n)$ συγκλίνει. Τότε η ακολουθία (P_k) συγκλίνει σε κάποιον μη μηδενικό αριθμό x. Άρα υπάρχει $N_1 \in \mathbb{N}$ τέτοιο ώστε

$$|P_n| > \frac{|x|}{2} \qquad \text{για κάθε } n \geq N_1.$$

Έστω τώρα $\varepsilon > 0$. Επειδή η (P_k) είναι ακολουθία Cauchy, υπάρχει $N > N_1$ τέτοιο ώστε

$$|P_{k-1} - P_m| < \frac{\varepsilon|x|}{2} \qquad \text{για κάθε } m \geq k \geq N.$$

Τότε, για κάθε $m \geq k \geq N$, έχουμε

$$\frac{\varepsilon|x|}{2} > |P_{k-1} - P_m| = |P_{k-1}| \left| \frac{P_m}{P_{k-1}} - 1 \right| \geq \frac{|x|}{2} \left| \prod_{n=k}^{m} (1 + a_n) - 1 \right|,$$

οπότε

$$\left| \prod_{n=k}^{m} (1 + a_n) - 1 \right| < \varepsilon,$$

όπως θέλαμε.

Για την αντίστροφη κατεύθυνση, υποθέτουμε ότι

$$\prod_{n=k}^{m} (1 + a_n) = \frac{P_m}{P_{k-1}}$$

συγκλίνει στο 1 όταν $m, k \to \infty$ και $m \geq k$. Θα δείξουμε ότι η (P_k) συγκλίνει.

Θέτοντας $\varepsilon = 1$ και χρησιμοποιώντας το ίδιο επιχείρημα όπως στα άπειρα αθροίσματα, βλέπουμε ότι η (P_k) είναι φραγμένη. Άρα υπάρχει $M > 0$ τέτοιο ώστε

$$|P_k| \leq M \qquad \text{για κάθε } k \in \mathbb{N}.$$

Για να δείξουμε ότι η (P_k) συγκλίνει, έστω $\varepsilon > 0$. Τότε υπάρχει $N \in \mathbb{N}$ τέτοιο ώστε

$$\left| \frac{P_m}{P_{k-1}} - 1 \right| < \frac{\varepsilon}{M} \qquad \text{για κάθε } m \geq k \geq N.$$

Πολλαπλασιάζοντας και τις δύο πλευρές με $|P_{k-1}|$, παίρνουμε

$$|P_m - P_{k-1}| < \varepsilon \qquad \text{για κάθε } m \geq k \geq N.$$

Άρα η (P_k) είναι ακολουθία Cauchy και επομένως συγκλίνει.

Μένει να δείξουμε ότι το όριό της δεν είναι 0. Θέτουμε $\varepsilon = \frac{1}{2}$, οπότε υπάρχει $M \in \mathbb{N}$ τέτοιο ώστε

$$\left| \prod_{n=M}^{m} (1 + a_n) - 1 \right| < \frac{1}{2} \qquad \text{για κάθε } m \geq M.$$

Άρα, ειδικότερα,

$$\left| \prod_{n=M}^{m} (1 + a_n) \right| > \frac{1}{2} \qquad \text{για κάθε } m \geq M.$$

Θέτουμε

$$c := \prod_{n=1}^{M-1} (1 + a_n).$$

Τότε το c είναι μη μηδενική σταθερά και

$$\left| \prod_{n=1}^{m} (1 + a_n) \right| = |c| \left| \prod_{n=M}^{m} (1 + a_n) \right| > \frac{|c|}{2} \qquad \text{για κάθε } m \geq M.$$

Αυτό δείχνει ότι το όριο της (P_k) δεν μπορεί να είναι 0. □

Στη συνέχεια δίνουμε μια σύνδεση ανάμεσα στο

$$\prod_{n=1}^{\infty}(1+a_n) \qquad \text{και} \qquad \sum_{n=1}^{\infty} a_n.$$

Θα δούμε ότι η διάκριση ανάμεσα σε σύγκλιση και απόκλιση ενός άπειρου γινομένου μπορεί να γίνει εξετάζοντας το αντίστοιχο άπειρο άθροισμα. Ξεκινάμε με ένα λήμμα.

Λήμμα 6.5. *Αν $x \in [0,1]$, τότε*

$$1 + x \leq e^x \leq 1 + 2x.$$

Απόδειξη. Ορίζουμε τις συναρτήσεις $f, g : [0,1] \to \mathbb{R}$ με

$$f(x) = e^x - x - 1 \qquad \text{και} \qquad g(x) = 1 + 2x - e^x,$$

και εφαρμόζουμε τη συνηθισμένη τεχνική του απειροστικού λογισμού για να βρούμε τα απόλυτα ακρότατα των f και g. Έχουμε $f(x) \geq f(0)$ και $g(x) \geq g(0)$ για όλα τα $x \in [0,1]$, πράγμα που δίνει την επιθυμητή ανισότητα. □

Θεώρημα 6.6. *Έστω (a_n) ακολουθία μιγαδικών αριθμών. Τότε το άπειρο γινόμενο*

$$\prod_{n=1}^{\infty}(1+|a_n|)$$

συγκλίνει αν και μόνο αν η σειρά

$$\sum_{n=1}^{\infty} |a_n|$$

συγκλίνει.

Απόδειξη. Εφαρμόζοντας το προηγούμενο λήμμα, παίρνουμε

$$\prod_{n=N}^{m}(1+|a_n|) \leq \exp\left(\sum_{n=N}^{m}|a_n|\right),$$

και

$$\exp\left(\frac{1}{2}\sum_{n=N}^{m}|a_n|\right) \leq \prod_{n=N}^{m}(1+|a_n|),$$

όπου N είναι αρκετά μεγάλος ώστε $|a_n| \leq 1$ για όλα τα $n \geq N$. Έπειτα χρησιμοποιούμε το θεώρημα μονοτονικής σύγκλισης για να πάρουμε το ζητούμενο. Οι λεπτομέρειες αφήνονται στον αναγνώστη. □

Θεώρημα 6.7. *Αν το*

$$\prod_{n=1}^{\infty}(1+|a_n|)$$

συγκλίνει, τότε και το

$$\prod_{n=1}^{\infty}(1+a_n)$$

συγκλίνει. Με άλλα λόγια, αν το $\prod_{n=1}^{\infty}(1+a_n)$ συγκλίνει απολύτως, τότε συγκλίνει.

Απόδειξη. Υποθέτουμε ότι το

$$\prod_{n=1}^{\infty}(1+|a_n|)$$

συγκλίνει. Από το προηγούμενο θεώρημα έπεται ότι $|a_n| \to 0$, άρα υπάρχει $N \in \mathbb{N}$ τέτοιο ώστε $a_n \neq -1$ για όλα τα $n \geq N$. Άρα η πρώτη προϋπόθεση του ορισμού της σύγκλισης του $\prod_{n=1}^{\infty}(1+a_n)$ ικανοποιείται.

Θέτουμε

$$P_k = \prod_{n=N}^{k}(1+a_n) \qquad \text{και} \qquad Q_k = \prod_{n=N}^{k}(1+|a_n|) \qquad \text{για κάθε } k \geq N.$$

Παρατηρούμε πρώτα ότι

$$P_k = 1 + f,$$

όπου f είναι πολυώνυμο ως προς $a_N, a_{N+1}, \ldots, a_k$, ενώ

$$Q_k = 1 + f^*,$$

όπου κάθε όρος του f^* είναι η απόλυτη τιμή του αντίστοιχου όρου του f. Επομένως

$$|P_k - 1| = |f| \leq f^* = Q_k - 1 \qquad \text{για κάθε } k \geq N.$$

Γενικότερα, για οποιοδήποτε πεπερασμένο γινόμενο, ισχύει

$$\left|\prod(1+a_n) - 1\right| \leq \prod(1+|a_n|) - 1. \tag{49}$$

Τώρα, για $m > k \geq N$, από την (49) παίρνουμε

$$\left|\frac{P_m}{P_k} - 1\right| \leq \frac{Q_m}{Q_k} - 1,$$

και συνεπώς

$$\begin{aligned} |P_m - P_k| &= |P_k|\left|\frac{P_m}{P_k} - 1\right| \\ &\leq Q_k\left(\frac{Q_m}{Q_k} - 1\right) \\ &= Q_m - Q_k. \end{aligned}$$

Εφόσον η (Q_k) συγκλίνει, είναι ακολουθία Cauchy, άρα

$$Q_m - Q_k \to 0 \qquad \text{όταν } m, k \to \infty.$$

Άρα και η (P_k) είναι ακολουθία Cauchy, επομένως συγκλίνει. Μένει μόνο να παρατηρήσουμε ότι, όπως και πριν, το όριό της δεν μπορεί να είναι 0, επειδή τα μερικά ουραία γινόμενα είναι τελικά κοντά στο 1. Άρα το $\prod_{n=1}^{\infty}(1+a_n)$ συγκλίνει. □

Απόδειξη. Εφόσον η $(Q_k)_{k\geq N}$ συγκλίνει, η $(P_k)_{k\geq N}$ είναι επίσης συγκλίνουσα. Μένει να δείξουμε ότι

$$\lim_{k\to\infty} P_k \neq 0.$$

Από το κριτήριο Cauchy, υπάρχουν ακέραιοι $M > N > 0$ τέτοιοι ώστε

$$\left|\prod_{n=m}^{k}(1+|a_n|) - 1\right| < \frac{1}{2} \qquad \text{για κάθε } k > m \geq M.$$

Άρα, από την (49), παίρνουμε

$$\left|\prod_{n=m}^{k}(1+a_n)-1\right|<\frac{1}{2}\qquad \text{για κάθε } k>m\geq M.$$

Επομένως

$$\left|\prod_{n=m}^{k}(1+a_n)\right|>\frac{1}{2}\qquad \text{για κάθε } k>m\geq M.$$

Ειδικότερα,

$$\left|\prod_{n=M+1}^{k}(1+a_n)\right|>\frac{1}{2}\qquad \text{για κάθε } k>M+1.$$

Τότε

$$\begin{aligned}\lim_{k\to\infty}|P_k| &= \lim_{k\to\infty}\left|\prod_{n=N}^{k}(1+a_n)\right| \\ &= \lim_{k\to\infty}\left|\left(\prod_{n=N}^{M}(1+a_n)\right)\left(\prod_{n=M+1}^{k}(1+a_n)\right)\right| \\ &= \left|\prod_{n=N}^{M}(1+a_n)\right|\lim_{k\to\infty}\left|\prod_{n=M+1}^{k}(1+a_n)\right| \\ &\geq \frac{1}{2}\left|\prod_{n=N}^{M}(1+a_n)\right|>0.\end{aligned}$$

Αυτό ολοκληρώνει την απόδειξη. □

Πόρισμα 6.8. *Αν η σειρά*

$$\sum_{n=1}^{\infty}|a_n|$$

συγκλίνει, τότε το γινόμενο

$$\prod_{n=1}^{\infty}(1+a_n)$$

συγκλίνει.

Απόδειξη. Αυτό ακολουθεί αμέσως από τα προηγούμενα δύο θεωρήματα. □

Από το παραπάνω πόρισμα, είναι τώρα εύκολο να δούμε ότι τα άπειρα γινόμενα στο (48) συγκλίνουν.

7 Τύπος γινομένου του Euler

Είμαστε τώρα έτοιμοι να δώσουμε την απόδειξη του τύπου γινομένου του Euler, ο οποίος συνδέει ένα άπειρο άθροισμα μιας πολλαπλασιαστικής συνάρτησης με ένα άπειρο γινόμενο. Διαισθητικά, ο λόγος πίσω από αυτόν τον τύπο είναι το θεμελιώδες θεώρημα της αριθμητικής.

Θεώρημα 7.1 (Τύπος γινομένου του Euler). *Έστω f μια πολλαπλασιαστική συνάρτηση. Υποθέτουμε ότι η σειρά*

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

συγκλίνει απολύτως. Τότε

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \big(1 + f(p) + f(p^2) + \cdots\big),$$

όπου το γινόμενο λαμβάνεται πάνω σε όλους τους πρώτους αριθμούς και είναι απολύτως συγκλίνον. Αν, επιπλέον, η f είναι πλήρως πολλαπλασιαστική, τότε

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

Απόδειξη. Θυμόμαστε από τα προηγούμενα αποτελέσματα ότι το

$$\prod_{n=1}^{\infty} (1 + a_n)$$

συγκλίνει απολύτως αν το

$$\sum |a_n|$$

συγκλίνει.

Επομένως εξετάζουμε

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

Άρα το γινόμενο

$$\prod_{p} \big(1 + f(p) + f(p^2) + \cdots\big)$$

συγκλίνει απολύτως.

Θέτουμε τώρα

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

Για σταθερό x, ο αριθμός των παραγόντων του $P(x)$ είναι πεπερασμένος και κάθε παράγοντας είναι απολύτως συγκλίνουσα σειρά, αφού η $\sum |f(n)|$ συγκλίνει. Άρα, από το θεώρημα του Cauchy για γινόμενα σειρών, μπορούμε να πολλαπλασιάσουμε τους όρους και να τους αναδιατάξουμε με οποιονδήποτε τρόπο θέλουμε, και το αποτέλεσμα θα εξακολουθεί να συγκλίνει απολύτως.

Από την πολλαπλασιαστικότητα της f, ένας τυπικός όρος έχει τη μορφή

$$f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_k^{a_k}) = f(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}),$$

όπου

$$2 = p_1 < p_2 < \cdots < p_k \le x$$

είναι οι πρώτοι μικρότεροι ή ίσοι του x και οι $a_1, a_2, \ldots, a_k$ είναι μη αρνητικοί ακέραιοι. Εφόσον κάθε $n > 1$ γράφεται κατά μοναδικό τρόπο ως γινόμενο πρώτων, παίρνουμε

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

όπου A είναι το σύνολο όλων των θετικών ακεραίων των οποίων όλοι οι πρώτοι παράγοντες είναι μικρότεροι ή ίσοι του x.

Τότε

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

όπου B είναι το σύνολο όλων των θετικών ακεραίων που έχουν κάποιο πρώτο παράγοντα μεγαλύτερο του x. Επομένως

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

και το τελευταίο τείνει στο 0 όταν $x \to \infty$. Άρα

$$P(x) \longrightarrow \sum_{n=1}^{\infty} f(n) \qquad \text{όταν } x \to \infty.$$

Αν η f είναι πλήρως πολλαπλασιαστική, τότε

$$f(p^n) = f(p)^n \qquad \text{για κάθε } n \in \mathbb{N},$$

και το γινόμενο γράφεται

$$\prod_p \big(1 + f(p) + f(p)^2 + f(p)^3 + \cdots\big) = \prod_p (1 - f(p))^{-1}.$$

Παρατηρούμε ότι έχουμε ήδη εξασφαλίσει τη σύγκλιση της γεωμετρικής σειράς

$$1 + f(p) + f(p)^2 + f(p)^3 + \cdots .$$

Άρα $|f(p)| < 1$ και ο τύπος

$$\sum_{n=0}^{\infty} f(p)^n = (1 - f(p))^{-1}$$

που εφαρμόζουμε παραπάνω είναι έγκυρος. □

Εφαρμόζοντας τον τύπο γινομένου του Euler σε απολύτως συγκλίνουσες Dirichlet σειρές, παίρνουμε το ακόλουθο αποτέλεσμα.

Θεώρημα 7.2. *Υποθέτουμε ότι η σειρά*

$$\sum_{n=1}^{\infty} f(n) n^{-s}$$

συγκλίνει απολύτως για $\sigma > \sigma_a$. Αν η f είναι πολλαπλασιαστική και το $s \in \mathbb{C}$ έχει πραγματικό μέρος $\sigma > \sigma_a$, τότε

$$\sum_{n=1}^{\infty} f(n) n^{-s} = \prod_p \big(1 + f(p)p^{-s} + f(p^2)p^{-2s} + \cdots\big).$$

Επιπλέον, αν η f είναι πλήρως πολλαπλασιαστική, τότε

$$\sum_{n=1}^{\infty} f(n) n^{-s} = \prod_p (1 - f(p)p^{-s})^{-1} \qquad \text{για } \sigma > \sigma_a.$$

Επιπρόσθετα, κάθε ένα από αυτά τα γινόμενα συγκλίνει απολύτως για $\sigma > \sigma_a$.

Απόδειξη. Αυτό ακολουθεί αμέσως από το προηγούμενο θεώρημα. □

Αντικαθιστώντας στο προηγούμενο θεώρημα τις

$$f(n) = 1,\ \mu(n),\ \varphi(n),\ d(n),\ \sigma(n),\ \lambda(n),\ \chi(n),$$

παίρνουμε τους ακόλουθους τύπους.

Πόρισμα 7.3. *Για $s \in \mathbb{C}$ με πραγματικό μέρος σ, ισχύουν οι παρακάτω τύποι:*

(i)
$$\zeta(s) = \prod_p (1 - p^{-s})^{-1} \qquad \text{αν } \sigma > 1.$$

(ii)
$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_p (1 - p^{-s}) = \frac{1}{\zeta(s)} \qquad \text{αν } \sigma > 1.$$

(iii)
$$\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \prod_p (1 + p^{-s})^{-1} = \frac{\zeta(2s)}{\zeta(s)} \qquad \text{αν } \sigma > 1.$$

(iv)
$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p (1 - \chi(p)p^{-s})^{-1} \qquad \text{αν } \sigma > 1.$$

Επιπλέον, κάθε ένα από τα γινόμενα στα (i)–(iv) συγκλίνει απολύτως.

Απόδειξη. Θυμόμαστε ότι η
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$
συγκλίνει απολύτως για $\sigma > 1$. Άρα μπορούμε να εφαρμόσουμε το προηγούμενο θεώρημα στη ζ και να πάρουμε το (i).

Επίσης,
$$|\mu(n)n^{-s}| \le n^{-\sigma} \qquad \text{για κάθε } n \in \mathbb{N},$$
και η σειρά $\sum_{n=1}^{\infty} n^{-\sigma}$ συγκλίνει για $\sigma > 1$. Άρα η σειρά στο (ii) συγκλίνει απολύτως για $\sigma > 1$. Ομοίως, επειδή
$$|\lambda(n)| \le 1 \qquad \text{και} \qquad |\chi(n)| \le 1 \qquad \text{για κάθε } n \in \mathbb{N},$$
οι σειρές στα (iii) και (iv) συγκλίνουν επίσης απολύτως για $\sigma > 1$. Εφόσον οι συναρτήσεις λ και χ είναι πλήρως πολλαπλασιαστικές, παίρνουμε τα (ii), (iii) και (iv) από το προηγούμενο θεώρημα. Αυτό ολοκληρώνει την απόδειξη. □

Στη συνέχεια δίνουμε ένα ακόμη αποτέλεσμα που βοηθά στον υπολογισμό γινομένων Euler για Dirichlet σειρές.

Θεώρημα 7.4. *Υποθέτουμε ότι οι Dirichlet σειρές*
$$\sum_{n=1}^{\infty} f(n)n^{-s} \qquad \textit{και} \qquad \sum_{n=1}^{\infty} g(n)n^{-s}$$
συγκλίνουν απολύτως για $\sigma > a$ και $\sigma > b$, αντιστοίχως. Τότε για
$$\sigma > \max\{a, b\}$$
ισχύει
$$\left(\sum_{n=1}^{\infty} f(n)n^{-s}\right)\left(\sum_{n=1}^{\infty} g(n)n^{-s}\right) = \sum_{n=1}^{\infty} h(n)n^{-s},$$
όπου
$$h = f * g$$

είναι το γινόμενο Dirichlet των f και g, δηλαδή

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

Απόδειξη. Έστω $\sigma > \max\{a, b\}$. Εφόσον και οι δύο σειρές

$$\sum f(n)n^{-s} \qquad \text{και} \qquad \sum g(n)n^{-s}$$

συγκλίνουν απολύτως, μπορούμε να τις πολλαπλασιάσουμε και να αναδιατάξουμε τους όρους όπως θέλουμε. Έχουμε

$$\left(\sum_{n=1}^{\infty} f(n)n^{-s}\right)\left(\sum_{m=1}^{\infty} g(m)m^{-s}\right) = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} f(n)g(m)(nm)^{-s}.$$

Ομαδοποιώντας τώρα τους όρους για τους οποίους $nm = k$, η παραπάνω έκφραση γίνεται

$$\sum_{k=1}^{\infty}\left(\sum_{nm=k} f(n)g(m)\right)k^{-s} = \sum_{k=1}^{\infty} h(k)k^{-s},$$

όπου

$$h(k) = \sum_{nm=k} f(n)g(m) = \sum_{d|k} f(d)\, g\Big(\frac{k}{d}\Big)\,.$$

Αυτό ολοκληρώνει την απόδειξη. □

Πόρισμα 7.5. *Για $s \in \mathbb{C}$ με πραγματικό μέρος σ, ισχύουν οι ακόλουθοι τύποι:*

(i)

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)} = \prod_p (1-p^{-s})(1-p^{1-s})^{-1} \qquad \text{αν } \sigma > 2.$$

(ii)

$$\sum_{n=1}^{\infty} \frac{d(n)}{n^s} = \zeta^2(s) = \prod_p (1-p^{-s})^{-2} \qquad \text{αν } \sigma > 1.$$

(iii)

$$\sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s} = \zeta(s-1)\zeta(s) = \prod_p (1-p^{1-s})^{-1}(1-p^{-s})^{-1} \qquad \text{αν } \sigma > 2.$$

Απόδειξη. Εφόσον η συνάρτηση πλήθους διαιρετών ικανοποιεί

$$d = 1 * 1$$

και

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

παίρνουμε από το Θεώρημα ?? και το Πόρισμα ?? ότι

$$\sum_{n=1}^{\infty} d(n)n^{-s} = \zeta(s)\zeta(s) = \zeta^2(s) = \prod_p (1-p^{-s})^{-2} \qquad \text{για } \sigma > 1.$$

Άρα αποδείχθηκε το (ii).

Στη συνέχεια, επειδή

$$|\varphi(n)| \leq n,$$

έχουμε

$$|\varphi(n)n^{-s}| \leq n^{1-\sigma}.$$

Εφόσον η σειρά $\sum_{n=1}^{\infty} n^{1-\sigma}$ συγκλίνει για $\sigma > 2$, η σειρά

$$\sum_{n=1}^{\infty} \varphi(n)n^{-s}$$

συγκλίνει απολύτως όταν $\sigma > 2$.

Επιπλέον, αν $N(n) = n$ είναι η ταυτοτική αριθμητική συνάρτηση, τότε

$$1 * \varphi = N.$$

Άρα, από το Θεώρημα ??, παίρνουμε για $\sigma > 2$:

$$\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s}\right) = \sum_{n=1}^{\infty} \frac{N(n)}{n^s} = \sum_{n=1}^{\infty} \frac{n}{n^s} = \zeta(s-1).$$

Δηλαδή

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

και επομένως

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

Χρησιμοποιώντας τώρα το Πόρισμα ??, παίρνουμε

$$\frac{\zeta(s-1)}{\zeta(s)} = \frac{\prod_p (1-p^{1-s})^{-1}}{\prod_p (1-p^{-s})^{-1}} = \prod_p (1-p^{-s})(1-p^{1-s})^{-1},$$

οπότε αποδείχθηκε το (i).

Ομοίως, επειδή

$$\sigma = N * 1,$$

παίρνουμε από το Θεώρημα ?? ότι, για $\sigma > 2$,

$$\sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s} = \left(\sum_{n=1}^{\infty} \frac{N(n)}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right) = \zeta(s-1)\zeta(s).$$

Και πάλι, από το Πόρισμα ??,

$$\zeta(s-1)\zeta(s) = \prod_p (1-p^{1-s})^{-1}(1-p^{-s})^{-1}.$$

Άρα αποδείχθηκε και το (iii). □

Πόρισμα 7.6. *Για $s \in \mathbb{C}$ με $\sigma > 1$, ισχύουν:*

(i) $\zeta(s) \neq 0$,

(ii)

$$\log \zeta(s) = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n}\, n^{-s},$$

(iii)

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

Εδώ ο κλάδος του $\log \zeta(s)$ *επιλέγεται έτσι ώστε να είναι πραγματικός πάνω στον πραγματικό άξονα.*

Απόδειξη. Έστω $\sigma > 1$. Από το Πόρισμα ??, γνωρίζουμε ότι

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$$

και ότι το γινόμενο αυτό συγκλίνει απολύτως και δεν έχει κανέναν μηδενικό παράγοντα. Άρα

$$\zeta(s) \neq 0.$$

Αυτό αποδεικνύει το (i).

Έστω τώρα $s \in \mathbb{R}$ με $s > 1$. Παίρνοντας λογάριθμο και στις δύο πλευρές του γινομένου Euler για τη $\zeta(s)$, παίρνουμε

$$\log \zeta(s) = \sum_p \log(1 - p^{-s})^{-1}.$$

Για κάθε πρώτο p, επειδή $|p^{-s}| < 1$, έχουμε

$$\log(1 - p^{-s})^{-1} = \sum_{k=1}^{\infty} \frac{p^{-ks}}{k}.$$

Άρα

$$\log \zeta(s) = \sum_p \sum_{k=1}^{\infty} \frac{p^{-ks}}{k}.$$

Τώρα παρατηρούμε ότι ο όρος $\frac{p^{-ks}}{k}$ είναι ακριβώς

$$\frac{\Lambda(p^k)}{\log(p^k)} (p^k)^{-s},$$

αφού $\Lambda(p^k) = \log p$ και $\log(p^k) = k \log p$. Επομένως

$$\log \zeta(s) = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n}\, n^{-s}.$$

Έτσι αποδείχθηκε ο τύπος του (ii) για πραγματικά $s > 1$.

Παρατηρούμε τώρα ότι

$$\left| \frac{\Lambda(n)}{\log n} n^{-s} \right| \leq n^{-\sigma} \qquad (n \geq 2),$$

οπότε η δεξιά πλευρά του (ii) ορίζει αναλυτική συνάρτηση στο ημιεπίπεδο $\sigma > 1$. Και η αριστερή πλευρά, ως $\log \zeta(s)$ με τον επιλεγμένο κλάδο, είναι επίσης αναλυτική στο ίδιο ημιεπίπεδο, αφού από το (i) η $\zeta(s)$ δεν μηδενίζεται εκεί. Επειδή οι δύο αναλυτικές συναρτήσεις συμφωνούν για όλα τα πραγματικά $s > 1$, συμφωνούν παντού στο ημιεπίπεδο $\sigma > 1$. Άρα το (ii) ισχύει για κάθε s με $\sigma > 1$.

Για το (iii), θυμόμαστε την ταυτότητα

$$\Lambda * 1 = \log,$$

δηλαδή

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

Άρα, από το Θεώρημα ??, παίρνουμε

$$\left(\sum_{n=1}^{\infty} \Lambda(n) n^{-s}\right) \zeta(s) = \sum_{n=1}^{\infty} (\log n)\, n^{-s}.$$

Αλλά

$$\zeta'(s) = \frac{d}{ds} \sum_{n=1}^{\infty} n^{-s} = -\sum_{n=1}^{\infty} (\log n)\, n^{-s},$$

οπότε

$$\left(\sum_{n=1}^{\infty} \Lambda(n) n^{-s}\right) \zeta(s) = -\zeta'(s).$$

Διαιρώντας με $\zeta(s) \neq 0$, παίρνουμε

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \Lambda(n)\, n^{-s},$$

όπως θέλαμε.

Εναλλακτικά, μπορούμε να διαφορίσουμε τον τύπο του (ii) και να πάρουμε

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{p} \sum_{k=1}^{\infty} (\log p)\, p^{-ks} = -\sum_{n=1}^{\infty} \Lambda(n)\, n^{-s}.$$

Η απόδειξη ολοκληρώθηκε. □

8 Η εξίσωση του Pell

Ένα γεγονός που όλοι επιμένουν να σου λένε για την εξίσωση του Pell είναι ότι ο Pell δεν είχε καμία σχέση με αυτήν. Ο Euler, απ' ό,τι φαίνεται, έκανε το λάθος να αποδώσει το έργο του Brouckner στον Pell. Ωστόσο, το όνομα εξακολουθεί να χρησιμοποιείται για τη μελέτη των ακέραιων λύσεων (x, y) της εξίσωσης

$$x^2 - Ny^2 = 1$$

για διάφορους ακεραίους N. Αν το N είναι τέλειο τετράγωνο, ή αν $N < 0$, δεν είναι δύσκολο να δει κανείς ότι υπάρχουν μόνο οι τετριμμένες λύσεις $(\pm 1, 0)$. Η εξίσωση του Pell με $N = 8$ εμφανίστηκε στην Άσκηση 1.1.3, σε σχέση με το ερώτημα ποιοι τριγωνικοί αριθμοί είναι επίσης τετράγωνα.

Ο Fermat ήταν ο πρώτος μαθηματικός που διατύπωσε την εικασία ότι για $N > 0$, όταν το N δεν είναι τέλειο τετράγωνο, υπάρχουν άπειρες πολλές λύσεις. Έθεσε στους συναδέλφους του τις ειδικές περιπτώσεις $N = 61$ και $N = 109$, λέγοντας ότι είχε διαλέξει αρκετά μικρούς αριθμούς *pour ne vous donner pas trop de peine* ("ώστε να μη σας δώσει υπερβολικό κόπο"). Στην πραγματικότητα όμως επιδεικνυόταν, αφού οι ελάχιστες λύσεις είναι

$$1766319049^2 - 61 \cdot 226153980^2 = 1 \qquad \text{και} \qquad 158070671986249^2 - 109 \cdot 15140424455100^2 = 1.$$

Στην πραγματικότητα, η μελέτη των εξισώσεων του Pell είναι πολύ παλαιότερη. Ο Αρχιμήδης, στο έργο *Η μέτρηση του κύκλου*, χρησιμοποίησε το γεγονός ότι το $1351/780$ είναι μια πολύ καλή προσέγγιση του $\sqrt{3}$. Ο λόγος είναι ότι

$$1351^2 - 3 \cdot 780^2 = 1, \qquad \text{οπότε} \qquad \frac{1351^2}{780^2} - 3 = \frac{1}{780^2}.$$

Πόσα γνώριζε ο Αρχιμήδης για την εξίσωση του Pell; Το 1773 ανακαλύφθηκε ένα χειρόγραφο στη βιβλιοθήκη του Wolfenbüttel. Περιέγραφε ένα πρόβλημα που είχε θέσει ο Αρχιμήδης στους συναδέλφους του Ερατοσθένη και Απολλώνιο, γραμμένο ως ποίημα σε 22 δίστιχα:

> Αν είσαι επιμελής και σοφός, ω ξένε, υπολόγισε τον αριθμό των βοδιών του Ήλιου, τα οποία κάποτε έβοσκαν στα λιβάδια της Θρινακίας, χωρισμένα σε τέσσερα κοπάδια διαφορετικών χρωμάτων, το ένα γαλακτόλευκο, το άλλο στιλπνό μαύρο ...

Η Θρινακία είναι η Σικελία, το "τριγωνικό" νησί. Το πρόβλημα συνεχίζει περιγράφοντας τις σχέσεις ανάμεσα στα μεγέθη των κοπαδιών διαφορετικών χρωμάτων. Συνολικά, υπάρχουν επτά γραμμικές εξισώσεις και οκτώ άγνωστοι: ο αριθμός των αγελάδων και των ταύρων κάθε χρώματος. Μέχρι εδώ, πρόκειται για ένα απλό πρόβλημα γραμμικής άλγεβρας, αν και οι αριθμοί που εμφανίζονται είναι μεγάλοι. Η μικρότερη λύση είναι ένα κοπάδι από 50389082 ζώα. Ο Αρχιμήδης λέει ότι, αν μπορέσεις να λύσεις μέχρι εδώ, τότε

> ... δεν θα σε αποκαλέσουν αμαθή ή αδαή στους αριθμούς, αλλά ακόμη δεν θα συγκαταλεγείς ανάμεσα στους σοφούς.

Στη συνέχεια προσθέτει ακόμη δύο συνθήκες: ότι ο αριθμός των λευκών και των μαύρων ταύρων να είναι τετράγωνος αριθμός και ότι ο αριθμός των κίτρινων και των στικτών ταύρων να είναι τριγωνικός αριθμός.

> Αν είσαι ικανός, ω ξένε, να βρεις όλα αυτά ... τότε θα φύγεις στεφανωμένος με δόξα και γνωρίζοντας ότι έχεις κριθεί τέλειος σε αυτό το είδος σοφίας.

Ύστερα από κάποιους αλγεβρικούς μετασχηματισμούς, οι πρόσθετες συνθήκες απαιτούν τη λύση της εξίσωσης του Pell

$$x^2 - 4729494y^2 = 1,$$

με την πρόσθετη συνθήκη ότι το y να είναι διαιρετό από το 9314. Μια αναπαράσταση της λύση, που περιγράφεται παρακάτω, βρέθηκε από τον Amthor το 1880. Το μέγεθος του κοπαδιού είναι περίπου

$$7.76 \cdot 10^{206544}$$

ζώα. Το 1895, η Μαθηματική Λέσχη του Hillsboro, στο Illinois, έδωσε μια απάντηση με προσέγγιση έως 32 δεκαδικά ψηφία. Αφιέρωσαν τέσσερα χρόνια στον υπολογισμό και ανακοίνωσαν με περηφάνια (Bell, 1895) ότι η τελική απάντηση είχε μήκος μισό μίλι. Η ακριβής λύση βρέθηκε από τους Williams, German και Zarnke το 1965 (Williams, German, Zarnke, 1965), σε έναν IBM 7040 με μνήμη μόλις 32K. Για μια καλή συζήτηση του προβλήματος, βλ. Vardi (1998). Το βιβλίο του Weil (Weil, 1983) περιέχει περισσότερα για την ιστορία της εξίσωσης του Pell.

Αλγεβρική ερμηνεία των λύσεων

Οι λύσεις της εξίσωσης του Pell μπορούν να ιδωθούν γεωμετρικά ως σημεία πλέγματος πάνω σε μια υπερβολή. Όμως μια αλγεβρική ερμηνεία είναι επίσης πολύ χρήσιμη. Μπορούμε να παραγοντοποιήσουμε την εξίσωση του Pell ως

$$(x + \sqrt{N}\, y)(x - \sqrt{N}\, y) = 1.$$

Αυτό υποδεικνύει να εξετάσουμε αριθμούς της μορφής $x + \sqrt{N}\, y$, όπου x και y είναι ακέραιοι. Κατά κάποιον τρόπο, αυτοί μοιάζουν με μιγαδικούς αριθμούς, με το $\sqrt{N}$ να παίζει τον ρόλο του i. Μπορούμε να πολλαπλασιάζουμε τέτοιους αριθμούς με τον προφανή κανόνα:

$$(x + \sqrt{N}\, y) \cdot (a + \sqrt{N}\, b) = ax + \sqrt{N}\, ay + \sqrt{N}\, bx + Nby$$

$$= (ax + Nby) + \sqrt{N}\, (bx + ay).$$

Άσκηση Να δείξετε ότι αν (x, y) είναι μία λύση της εξίσωσης του Pell και αν (a, b) είναι μία άλλη, τότε ορίζοντας

$$(a, b) \cdot (x, y) = (ax + Nby,\ bx + ay)$$

παίρνουμε μια νέα λύση. Παρατηρήστε ότι η πράξη $\cdot$ είναι ένας νέος τρόπος συνδυασμού ζευγών σημείων.

Με αυτή την παρατήρηση, μπορούμε να πούμε ότι οι λύσεις της εξίσωσης του Pell σχηματίζουν μια ομάδα. Ο κανόνας πολλαπλασιασμού για τον συνδυασμό δύο λύσεων είναι αυτός που δόθηκε παραπάνω με το $\cdot$. Το ουδέτερο στοιχείο της ομάδας είναι η τετριμμένη λύση $(1, 0)$, που αντιστοιχεί στον αριθμό

$$1 = 1 + \sqrt{N}\, 0,$$

και το αντίστροφο της λύσης (x, y) είναι η λύση $(x, -y)$.

Λύσεις modulo p

Επειδή σε πρώτη φάση είναι δύσκολο να βρεθούν ακέραιες λύσεις της εξίσωσης του Pell, μπορούμε να αλλάξουμε το πρόβλημα σε ένα διαφορετικό αλλά συγγενικό. Αν σταθεροποιήσουμε έναν πρώτο αριθμό p, υπάρχουν λύσεις modulo p; Πιο ενδιαφέρον όμως είναι το ερώτημα πόσες λύσεις υπάρχουν modulo p.

Στην πραγματικότητα, σε αυτή την ενότητα θα αποδείξουμε το εξής:

Θεώρημα 8.1. *Αν p είναι περιττός πρώτος που δεν διαιρεί το N, τότε ο αριθμός των λύσεων της ισοτιμίας*

$$x^2 - Ny^2 \equiv 1 \pmod{p}$$

είναι

$$\#\{(x,y) \mid x^2 - Ny^2 \equiv 1 \pmod{p}\} = \begin{cases} p-1, & \text{αν υπάρχει } a \text{ με } a^2 \equiv N \pmod{p}, \\ p+1, & \text{διαφορετικά.} \end{cases}$$

Χρειαζόμαστε πρώτα ένα λήμμα.

Λήμμα 8.2. *Υπάρχουν $p-1$ λύσεις της εξίσωσης*

$$z^2 - w^2 \equiv N \pmod{p}.$$

Απόδειξη. Μπορούμε να εισαγάγουμε νέες μεταβλητές u και v, που συνδέονται με τα z και w με τις εξισώσεις (modulo p)

$$u = z - w, \qquad v = z + w \qquad \Longleftrightarrow \qquad z = \frac{u+v}{2}, \qquad w = \frac{u-v}{2}.$$

(Μπορούμε να διαιρέσουμε με το 2, επειδή το p είναι περιττό.) Τότε

$$u \cdot v \equiv N \pmod{p} \qquad \Longleftrightarrow \qquad z^2 - w^2 \equiv N \pmod{p}.$$

Όμως η εξίσωση ως προς u και v έχει ακριβώς $p-1$ λύσεις, διότι για κάθε κλάση υπολοίπων

$$u = 1, 2, \ldots, p-1$$

παίρνουμε μια λύση θέτοντας

$$v \equiv \frac{N}{u} \pmod{p}.$$

□

Απόδειξη του Θεωρήματος. Έστω πρώτα ότι

$$N \equiv a^2 \pmod{p}.$$

Από το λήμμα γνωρίζουμε ότι η εξίσωση

$$x^2 - w^2 \equiv 1 \pmod{p}$$

έχει ακριβώς $p-1$ λύσεις (x,w). (Εδώ ο αριθμός 1 παίζει τον ρόλο του N στο λήμμα.) Θέτοντας

$$y = \frac{w}{a},$$

παίρνουμε $p-1$ λύσεις (x,y) της εξίσωσης

$$x^2 - Ny^2 \equiv 1 \pmod{p}.$$

(Γνωρίζουμε ότι $a \not\equiv 0 \pmod{p}$, αφού το p δεν διαιρεί το N.) Αυτό αποδεικνύει την πρώτη περίπτωση.

Στη συνέχεια, ας υποθέσουμε ότι το N δεν είναι ισότιμο με κανένα τετράγωνο modulo p. Ξέρουμε από το λήμμα ότι υπάρχουν $p-1$ λύσεις (z,w) της εξίσωσης

$$z^2 - w^2 \equiv N \pmod{p}.$$

Επιπλέον, κανένα από τα w δεν είναι ισότιμο με 0 modulo p, γιατί διαφορετικά θα είχαμε

$$N \equiv z^2 \pmod{p}.$$

Γράφουμε την εξίσωση ως

$$\frac{z^2}{w^2} - \frac{N}{w^2} \equiv 1 \pmod{p}.$$

Με την αλλαγή μεταβλητών

$$x = \frac{z}{w}, \qquad y = \frac{1}{w},$$

παίρνουμε $p-1$ λύσεις της εξίσωσης

$$x^2 - Ny^2 \equiv \frac{z^2}{w^2} - \frac{N}{w^2} \equiv 1 \pmod{p}.$$

Επιπλέον, κανένα από τα y δεν είναι ίσο με 0, αφού είναι της μορφής $1/w$. Υπάρχουν ακριβώς δύο ακόμη λύσεις που έχουν

$$y \equiv 0 \pmod{p},$$

δηλαδή οι

$$(\pm 1, 0).$$

Άρα συνολικά υπάρχουν $p+1$ λύσεις. □

Θεώρημα 8.3 (Νόμος της τετραγωνικής αντιστροφής). *Έστω p, q δύο διαφορετικοί περιττοί πρώτοι. Τότε*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Το βασικό λήμμα του Eisenstein

Στο εξής, p θα είναι περιττός πρώτος και $a \in \mathbb{Z}$ με $p \nmid a$.

Λήμμα 8.4. *Ισχύει*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2ak}{p} \right\rfloor}.$$

Απόδειξη. Για κάθε άρτιο ακέραιο u με

$$1 \le u \le p-1,$$

έστω $r(u)$ το ελάχιστο θετικό υπόλοιπο του au modulo p. Άρα

$$r(u) \in \{1, 2, \ldots, p-1\} \qquad \text{και} \qquad r(u) \equiv au \pmod{p}.$$

Θεωρούμε τώρα τους αριθμούς

$$(-1)^{r(u)}\, r(u)$$

ως κλάσεις modulo p, γραμμένες πάλι με το ελάχιστο θετικό υπόλοιπό τους.

Ισχυρισμός 1: Οι αριθμοί αυτοί είναι όλοι άρτιοι.

Πράγματι, αν $r(u)$ είναι άρτιος, τότε

$$(-1)^{r(u)} r(u) = r(u)$$

είναι άρτιος. Αν $r(u)$ είναι περιττός, τότε

$$(-1)^{r(u)} r(u) \equiv -r(u) \equiv p - r(u) \pmod{p},$$

και ο $p - r(u)$ είναι άρτιος, αφού p και $r(u)$ είναι περιττοί.

Ισχυρισμός 2: Οι αριθμοί

$$(-1)^{r(u)} r(u)$$

είναι ανά δύο διαφορετικοί καθώς το u διατρέχει τους άρτιους αριθμούς $2, 4, \ldots, p-1$.

Έστω

$$(-1)^{r(u)} r(u) \equiv (-1)^{r(v)} r(v) \pmod{p}.$$

Τότε

$$r(u) \equiv \pm r(v) \pmod{p}.$$

Επειδή

$$r(u) \equiv au, \qquad r(v) \equiv av \pmod{p},$$

και a είναι αντιστρέψιμος modulo p, παίρνουμε

$$u \equiv \pm v \pmod{p}.$$

Αν ίσχυε $u \equiv -v \pmod{p}$, τότε

$$u + v \equiv 0 \pmod{p}.$$

Αλλά $u, v \in \{2, 4, \ldots, p-1\}$, άρα

$$2 \leq u + v \leq 2p - 2.$$

Η μόνη δυνατότητα για να είναι πολλαπλάσιο του p είναι

$$u + v = p,$$

πράγμα αδύνατο, αφού το αριστερό μέλος είναι άρτιο ενώ το δεξί περιττό. Άρα αναγκαστικά

$$u \equiv v \pmod{p}.$$

Επειδή $1 \leq u, v \leq p-1$, συμπεραίνουμε ότι $u = v$.

Υπάρχουν ακριβώς $(p-1)/2$ τέτοιοι άρτιοι αριθμοί, και βρήκαμε ότι οι

$$(-1)^{r(u)} r(u)$$

είναι $(p-1)/2$ διαφορετικοί άρτιοι αριθμοί modulo p. Άρα αποτελούν αναδιάταξη των άρτιων αριθμών

$$2, 4, 6, \ldots, p-1.$$

Επομένως, πολλαπλασιάζοντάς τους, παίρνουμε

$$\prod_{\substack{1 \leq u \leq p-1 \\ u \text{ άρτιος}}} (-1)^{r(u)} r(u) \equiv \prod_{\substack{1 \leq u \leq p-1 \\ u \text{ άρτιος}}} u \pmod{p}.$$

Δηλαδή

$$(-1)^{\sum r(u)} \prod r(u) \equiv \prod u \pmod{p}.$$

Επειδή $r(u) \equiv au \pmod{p}$, έχουμε

$$\prod r(u) \equiv a^{(p-1)/2} \prod u \pmod{p}.$$

Άρα

$$(-1)^{\sum r(u)} a^{(p-1)/2} \prod u \equiv \prod u \pmod{p}.$$

Κανένας από τους άρτιους u δεν διαιρείται από p, άρα μπορούμε να απλοποιήσουμε το γινόμενο $\prod u$, και παίρνουμε

$$a^{(p-1)/2} \equiv (-1)^{\sum r(u)} \pmod{p},$$

όπου το άθροισμα εκτείνεται σε όλα τα άρτια $u \in \{2, 4, \ldots, p-1\}$.

Από τον ορισμό του $r(u)$,

$$au = p\left\lfloor \frac{au}{p} \right\rfloor + r(u).$$

Επειδή ο u είναι άρτιος, το au είναι άρτιο. Επειδή ο p είναι περιττός, αν πάρουμε την παραπάνω σχέση modulo 2, παίρνουμε

$$0 \equiv \left\lfloor \frac{au}{p} \right\rfloor + r(u) \pmod{2}.$$

Άρα

$$r(u) \equiv \left\lfloor \frac{au}{p} \right\rfloor \pmod{2}.$$

Συνεπώς

$$\sum r(u) \equiv \sum \left\lfloor \frac{au}{p} \right\rfloor \pmod{2}.$$

Θέτοντας $u = 2k$, $k = 1, \ldots, (p-1)/2$, βρίσκουμε

$$a^{(p-1)/2} \equiv (-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2ak}{p} \right\rfloor} \pmod{p}.$$

Τώρα, από το κριτήριο του Euler,

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

Και τα δύο μέλη είναι ίσα με ± 1, άρα η σύγκριση modulo p συνεπάγεται ισότητα:

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2ak}{p} \right\rfloor}.$$

□

Πόρισμα 8.5. *Για κάθε περιττό πρώτο p,*

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

Απόδειξη. Θέτουμε

$$a = \frac{p+1}{2}.$$

Τότε a είναι ακέραιος και

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

Επειδή ένας αριθμός είναι τετραγωνικό υπόλοιπο modulo p αν και μόνον αν το αντίστροφό του είναι τετραγωνικό υπόλοιπο, έχουμε

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right).$$

Από το Λήμμα 8.4,

$$\left(\frac{2}{p}\right) = \left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2ak}{p} \right\rfloor}.$$

Αλλά

$$2a = p + 1,$$

άρα

$$\left\lfloor \frac{2ak}{p} \right\rfloor = \left\lfloor \frac{(p+1)k}{p} \right\rfloor = \left\lfloor k + \frac{k}{p} \right\rfloor = k,$$

διότι $1 \leq k \leq (p-1)/2 < p$. Επομένως

$$\left(\frac{2}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} k} = (-1)^{\frac{(p-1)/2\,((p-1)/2+1)}{2}} = (-1)^{\frac{p^2-1}{8}}.$$

□

3. Η βολική μορφή του Eisenstein για περιττό a

Πρόταση 8.6. *Έστω p περιττός πρώτος και a περιττός ακέραιος με $p \nmid a$. Τότε*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ak}{p} \right\rfloor}.$$

Απόδειξη. Θέτουμε

$$b = \frac{p+a}{2}.$$

Επειδή p και a είναι περιττοί, ο b είναι ακέραιος. Επιπλέον

$$b \equiv a \cdot 2^{-1} \pmod{p}.$$

Άρα

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

Και όπως πριν,

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

Έτσι

$$\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{2}{p}\right).$$

Από το Λήμμα 8.4,

$$\left(\frac{b}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2bk}{p} \right\rfloor}.$$

Επειδή

$$2b = p + a,$$

παίρνουμε

$$\left\lfloor \frac{2bk}{p} \right\rfloor = \left\lfloor \frac{(p+a)k}{p} \right\rfloor = \left\lfloor k + \frac{ak}{p} \right\rfloor = k + \left\lfloor \frac{ak}{p} \right\rfloor.$$

Άρα

$$\left(\frac{a}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} k}\,(-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ak}{p} \right\rfloor}.$$

Από το Πόρισμα 8.5,

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

Απλοποιώντας τον κοινό παράγοντα $\left(\frac{2}{p}\right)$, καταλήγουμε

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ak}{p} \right\rfloor}.$$

□

4. Η ταυτότητα των lattice points

Πρόταση 8.7. *Αν p, q είναι διαφορετικοί περιττοί πρώτοι, τότε*

$$\sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor + \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor = \frac{(p-1)(q-1)}{4}.$$

Απόδειξη. Θεωρούμε το σύνολο

$$R = \left\{ (x,y) \in \mathbb{Z}^2 : 1 \le x \le \frac{p-1}{2},\ 1 \le y \le \frac{q-1}{2} \right\}.$$

Είναι φανερό ότι

$$|R| = \frac{p-1}{2} \cdot \frac{q-1}{2} = \frac{(p-1)(q-1)}{4}.$$

Θεωρούμε επίσης την ευθεία

$$L:\ y = \frac{q}{p}x.$$

Θα δείξουμε ότι κανένα lattice point του R δεν ανήκει στην L. Πράγματι, αν $(x,y) \in R$ ικανοποιούσε

$$y = \frac{q}{p}x,$$

τότε

$$py = qx.$$

Επειδή p, q είναι πρώτοι και διαφορετικοί, θα είχαμε $p \mid x$ και $q \mid y$, κάτι αδύνατο αφού

$$1 \le x \le \frac{p-1}{2} < p, \qquad 1 \le y \le \frac{q-1}{2} < q.$$

Άρα κάθε σημείο του R είναι είτε αυστηρά κάτω είτε αυστηρά πάνω από την L.
Για κάθε σταθερό $x \in \{1, \dots, (p-1)/2\}$, ο αριθμός των ακεραίων y με

$$1 \le y < \frac{qx}{p}$$

είναι ακριβώς

$$\left\lfloor \frac{qx}{p} \right\rfloor.$$

Άρα ο συνολικός αριθμός των σημείων του R κάτω από την L είναι

$$\sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor.$$

Αντίστοιχα, για κάθε σταθερό $y \in \{1, \dots, (q-1)/2\}$, ο αριθμός των ακεραίων x με

$$1 \le x < \frac{py}{q}$$

είναι

$$\left\lfloor \frac{py}{q} \right\rfloor.$$

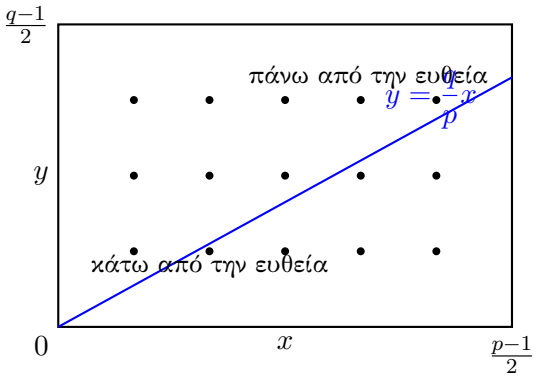
Αυτός είναι ο αριθμός των σημείων του R πάνω από την L στη συγκεκριμένη οριζόντια γραμμή. Άρα ο συνολικός αριθμός των σημείων του R πάνω από την L είναι

$$\sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor.$$

Προσθέτοντας τους δύο αριθμούς, παίρνουμε όλο το R. Επομένως

$$\sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor + \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor = |R| = \frac{(p-1)(q-1)}{4}.$$

□



Σχήμα 2: Η ταυτότητα των lattice points στην απόδειξη του Eisenstein.

Θεώρημα 8.8 (Νόμος της τετραγωνικής αντιστροφής). *Έστω p, q διαφορετικοί περιττοί πρώτοι. Τότε*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Απόδειξη. Από την Πρόταση 8.6, επειδή ο q είναι περιττός,

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor}.$$

Αντίστοιχα,

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor}.$$

Πολλαπλασιάζοντας,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor + \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor}.$$

Τώρα εφαρμόζουμε την Πρόταση 8.7:

$$\sum_{x=1}^{(p-1)/2} \left\lfloor \frac{qx}{p} \right\rfloor + \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{py}{q} \right\rfloor = \frac{(p-1)(q-1)}{4}.$$

Άρα

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

□

Παράδειγμα $(N = 2)$. Ορίζουμε μια συνάρτηση $\chi_8(n)$ ως εξής:

$$\chi_8(n) = \begin{cases} +1, & \text{αν } n \equiv 1 \text{ ή } 7 \pmod 8, \\ -1, & \text{αν } n \equiv 3 \text{ ή } 5 \pmod 8, \\ 0, & \text{διαφορετικά.} \end{cases} \tag{50}$$

Τότε, για κάθε περιττό πρώτο p, η εξίσωση του Pell

$$x^2 - 2y^2 \equiv 1 \pmod p$$

έχει

$$p - \chi_8(p)$$

λύσεις modulo p, σύμφωνα με τον νόμο της τετραγωνικής αντιστροφής.

Απόδειξη. Από το Θεώρημα 8.1, ο αριθμός των λύσεων της ισοτιμίας

$$x^2 - 2y^2 \equiv 1 \pmod p$$

είναι

$$\begin{cases} p - 1, & \text{αν το 2 είναι τετράγωνο modulo } p, \\ p + 1, & \text{αν το 2 δεν είναι τετράγωνο modulo } p. \end{cases}$$

Άρα αρκεί να καταλάβουμε πότε το 2 είναι τετραγωνικό υπόλοιπο modulo p.

Ο συμπληρωματικός νόμος για το 2 λέει ότι, για κάθε περιττό πρώτο p,

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

Επομένως,

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{αν } p \equiv 1 \text{ ή } 7 \pmod 8, \\ -1, & \text{αν } p \equiv 3 \text{ ή } 5 \pmod 8. \end{cases}$$

Δηλαδή το 2 είναι τετράγωνο modulo p ακριβώς όταν $p \equiv 1, 7 \pmod 8$, και δεν είναι τετράγωνο όταν $p \equiv 3, 5 \pmod 8$.

Άρα:

$$\#\{(x, y) \mid x^2 - 2y^2 \equiv 1 \pmod p\} = \begin{cases} p - 1, & \text{αν } p \equiv 1, 7 \pmod 8, \\ p + 1, & \text{αν } p \equiv 3, 5 \pmod 8, \end{cases}$$

που είναι ακριβώς

$$p - \chi_8(p).$$

□

Παράδειγμα $(N = 3)$. Ορίζουμε μια συνάρτηση $\chi_{12}(n)$ ως εξής:

$$\chi_{12}(n) = \begin{cases} +1, & \text{αν } n \equiv 1 \text{ ή } 11 \pmod{12}, \\ -1, & \text{αν } n \equiv 5 \text{ ή } 7 \pmod{12}, \\ 0, & \text{διαφορετικά.} \end{cases} \tag{11.3}$$

Τότε, για κάθε πρώτο $p \neq 3$, η εξίσωση του Pell

$$x^2 - 3y^2 \equiv 1 \pmod p$$

έχει

$$p - \chi_{12}(p)$$

λύσεις modulo p.

Απόδειξη. Για $p = 2$, έχουμε ορίσει $\chi_{12}(2) = 0$. Επιπλέον,

$$x^2 - 3y^2 \equiv x^2 + y^2 \pmod 2.$$

Η σύγκριση

$$x^2 + y^2 \equiv 1 \pmod 2$$

έχει ακριβώς δύο λύσεις, δηλαδή τις $(1, 0)$ και $(0, 1)$. Άρα και η περίπτωση $p = 2$ είναι σύμφωνη με τον τύπο, αφού

$$p - \chi_{12}(p) = 2 - 0 = 2.$$

Ας υποθέσουμε τώρα ότι p είναι περιττός πρώτος με $p \neq 3$. Θα χρησιμοποιήσουμε τον νόμο της τετραγωνικής αντιστροφής. Πρώτα παρατηρούμε ότι modulo 3 ισχύει

$$1^2 \equiv 1 \pmod 3, \qquad 2^2 \equiv 1 \pmod 3.$$

Άρα το 1 είναι τετράγωνο modulo 3, ενώ το 2 δεν είναι.

Σύμφωνα με το Θεώρημα (11.1), υπάρχουν $p - 1$ λύσεις ακριβώς όταν το 3 είναι τετράγωνο modulo p, δηλαδή όταν

$$\left(\frac{3}{p}\right) = 1.$$

Με τον νόμο της τετραγωνικής αμοιβαιότητας,

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{(3-1)(p-1)}{4}} = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}.$$

Τώρα εξετάζουμε τις δυνατές κλάσεις του p modulo 12.

Περίπτωση 1: $p \equiv 1 \pmod 3$ και $p \equiv 1 \pmod 4$.

Τότε

$$\left(\frac{p}{3}\right) = 1 \qquad \text{και} \qquad (-1)^{\frac{p-1}{2}} = 1,$$

οπότε

$$\left(\frac{3}{p}\right) = 1.$$

Με το Κινεζικό Θεώρημα Υπολοίπων αυτό ισοδυναμεί με

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

Περίπτωση 2: $p \equiv 2 \pmod 3$ και $p \equiv 3 \pmod 4$.

Τότε

$$\left(\frac{p}{3}\right) = -1 \qquad \text{και} \qquad (-1)^{\frac{p-1}{2}} = -1,$$

οπότε πάλι

$$\left(\frac{3}{p}\right) = 1.$$

Αυτό συμβαίνει ακριβώς όταν

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

Άρα το 3 είναι τετράγωνο modulo p ακριβώς όταν

$$p \equiv 1 \text{ ή } 11 \pmod{12}.$$

Στις άλλες δύο περιπτώσεις το 3 δεν είναι τετράγωνο modulo p.

Αν

$$p \equiv 2 \pmod 3 \qquad \text{και} \qquad p \equiv 1 \pmod 4,$$

τότε

$$\left(\frac{p}{3}\right) = -1, \qquad (-1)^{\frac{p-1}{2}} = 1,$$

άρα

$$\left(\frac{3}{p}\right) = -1.$$

Αυτό αντιστοιχεί στην κλάση

$$p \equiv 5 \pmod{12}.$$

Αν

$$p \equiv 1 \pmod 3 \qquad \text{και} \qquad p \equiv 3 \pmod 4,$$

τότε

$$\left(\frac{p}{3}\right) = 1, \qquad (-1)^{\frac{p-1}{2}} = -1,$$

οπότε

$$\left(\frac{3}{p}\right) = -1.$$

Αυτό αντιστοιχεί στην κλάση

$$p \equiv 7 \pmod{12}.$$

Συνοψίζοντας, έχουμε

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{αν } p \equiv 1 \text{ ή } 11 \pmod{12}, \\ -1, & \text{αν } p \equiv 5 \text{ ή } 7 \pmod{12}. \end{cases}$$

Άρα, από το (11.1),

$$\#\{(x,y) \mid x^2 - 3y^2 \equiv 1 \pmod p\} = \begin{cases} p-1, & \text{αν } p \equiv 1, 11 \pmod{12}, \\ p+1, & \text{αν } p \equiv 5, 7 \pmod{12}, \end{cases}$$

που είναι ακριβώς

$$p - \chi_{12}(p).$$

□

11.4. Συναρτήσεις Dirichlet L

Αυτή η ενότητα θα συνεχίσει να εξετάζει τις ειδικές περιπτώσεις $N = 3$ και $N = 2$, αλλά μεγάλο μέρος από όσα ακολουθούν ισχύουν γενικότερα. Μπορούμε να πάρουμε τη συνάρτηση χ_{12}, που ορίστηκε νωρίτερα, και να τη χρησιμοποιήσουμε για να ορίσουμε ένα γινόμενο Euler:

$$L(s, \chi_{12}) = \prod_{p \text{ πρώτος}} \left(1 - \chi_{12}(p) p^{-s}\right)^{-1}.$$

Για $\Re(s) > 1$ και για κάθε πρώτο p, γνωρίζουμε ότι

$$\left|\chi_{12}(p) p^{-s}\right| < 1.$$

Καθώς

$$\chi_{12}(n)\chi_{12}(m) = \chi_{12}(nm),$$

παίρνουμε ότι

$$L(s,\chi_{12}) = \sum_{n=1}^{\infty} \frac{\chi_{12}(n)}{n^s}$$

$$= 1 - \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} - \frac{1}{17^s} - \frac{1}{19^s} + \frac{1}{23^s} \cdots .$$

Χρησιμοποιώντας το κριτήριο σύγκρισης με τη $\zeta(s)$, μπορούμε να δείξουμε ότι η $L(s,\chi_{12})$ συγκλίνει απολύτως για $\Re(s) > 1$. Και, όπως έχουμε δει η $L(s,\chi_{12})$ συγκλίνει (με άθροισμα κατά Abel) και για

$$0 < \Re(s) \leq 1.$$

Αυτό υποδεικνύει ότι κάτι ενδιαφέρον συμβαίνει στο $s = 1$. Πώς μοιάζει το γινόμενο Euler όταν $s = 1$; Τυπικά, αν θέσουμε $s = 1$, παίρνουμε

$$L(1,\chi_{12}) = \prod_{p \text{ πρώτος}} \frac{1}{1 - \chi_{12}(p)/p} = \prod_{p \text{ πρώτος}} \frac{p}{p - \chi_{12}(p)}.$$

Οι όροι στον παρονομαστή είναι ακριβώς ο αριθμός των λύσεων της εξίσωσης του Pell modulo p. Αυτό δεν είναι τόσο θαυμαστό· λίγο-πολύ ορίσαμε τη $L(s,\chi_{12})$ έτσι ώστε να συμβαίνει αυτό. Το εντυπωσιακό είναι ότι αυτός ο αριθμός δίνει μια λύση της αρχικής, ακέραιας εξίσωσης του Pell.

Θεώρημα 8.9. *Ισχύει*

$$L(1,\chi_{12}) = \frac{\log(7 + 4\sqrt{3})}{\sqrt{12}} = \frac{\log\big((2+\sqrt{3})^2\big)}{\sqrt{12}}.$$

Παρατηρήστε ότι

$$1 = 7^2 - 3 \cdot 4^2.$$

Απόδειξη. Θέλουμε να υπολογίσουμε τη σειρά

$$1 - \frac{1}{5} - \frac{1}{7} + \frac{1}{11} + \frac{1}{13} - \frac{1}{17} - \frac{1}{19} + \frac{1}{23} \cdots ,$$

χρησιμοποιώντας τα θεωρήματα του Abel. Αφενός, τα μερικά αθροίσματα της σειράς

$$\sum_{n} \chi_{12}(n)$$

είναι πάντοτε ίσα με 1, 0 ή -1, επειδή η χ_{12} είναι περιοδική, άρα η σειρά

$$L(1,\chi_{12})$$

συγκλίνει.

Τώρα θέλουμε να χρησιμοποιήσουμε το Θεώρημα του Abel για τις δυναμοσειρές. Δηλαδή, ορίζουμε για $|x| < 1$ τη σειρά Taylor

$$f_{12}(x) = \sum_{n=1}^{\infty} \frac{\chi_{12}(n)}{n} x^n$$

$$= x - \frac{x^5}{5} - \frac{x^7}{7} + \frac{x^{11}}{11} + \frac{x^{13}}{13} - \frac{x^{17}}{17} - \frac{x^{19}}{19} + \frac{x^{23}}{23} \cdots .$$

Αν μπορέσουμε να βρούμε μια κλειστή μορφή για τη $f_{12}(x)$ η οποία να είναι συνεχής στο $x = 1$, τότε η σειρά που μας ενδιαφέρει είναι απλώς η τιμή $f_{12}(1)$. Επειδή η $\chi_{12}(n)$ έχει περίοδο 12, μπορούμε να γράψουμε τη $f_{12}(x)$ ως

$$\sum_{k=0}^{\infty} \left\{ \frac{x^{12k+1}}{12k+1} - \frac{x^{12k+5}}{12k+5} - \frac{x^{12k+7}}{12k+7} + \frac{x^{12k+11}}{12k+11} \right\}.$$

Η συνάρτηση $f_{12}(x)$ είναι κάπως περίπλοκη. Γι' αυτό παίρνουμε παράγωγο και βρίσκουμε ότι

$$\begin{aligned} f'_{12}(x) &= \sum_{k=0}^{\infty} \left\{ x^{12k} - x^{12k+4} - x^{12k+6} + x^{12k+10} \right\} \\ &= \left(1 - x^4 - x^6 + x^{10}\right) \sum_{k=0}^{\infty} x^{12k} \\ &= \frac{1 - x^4 - x^6 + x^{10}}{1 - x^{12}} \\ &= \frac{(1-x)(1+x)}{1 - x^2 + x^4}. \end{aligned}$$

Εδώ, στο τελευταίο βήμα, χρησιμοποιήσαμε ότι

$$1 - x^4 - x^6 + x^{10} = (1-x)(1+x)(1 - x^2 + x^6 + x^8)$$

και

$$1 - x^{12} = (1 - x^2 + x^4)(1 - x^2 + x^6 + x^8).$$

Η συνάρτηση $f_{12}(x)$ που αναζητούμε είναι λοιπόν μια παράγουσα της

$$\frac{(1-x)(1+x)}{1 - x^2 + x^4}$$

η οποία είναι ίση με 0 στο $x = 0$ (επειδή ο σταθερός όρος της σειράς Taylor της $f_{12}(x)$ είναι 0).

Ο παρονομαστής παραγοντοποιείται ως

$$1 - x^2 + x^4 = (1 + \sqrt{3}\, x + x^2)(1 - \sqrt{3}\, x + x^2).$$

Άρα το ολοκλήρωμα μπορεί να υπολογιστεί με μερικά κλάσματα. Βρίσκουμε ότι

$$\frac{(1-x)(1+x)}{1 - x^2 + x^4} = \frac{1}{\sqrt{12}} \left\{ \frac{2x + \sqrt{3}}{1 + \sqrt{3}\, x + x^2} - \frac{2x - \sqrt{3}}{1 - \sqrt{3}\, x + x^2} \right\}.$$

Άρα

$$f_{12}(x) = \frac{1}{\sqrt{12}} \left\{ \int \frac{2x + \sqrt{3}}{1 + \sqrt{3}\, x + x^2}\, dx - \int \frac{2x - \sqrt{3}}{1 - \sqrt{3}\, x + x^2}\, dx \right\}.$$

Αυτό τώρα είναι ένα εύκολο ολοκλήρωμα με αντικατάσταση. Βρίσκουμε ότι

$$\begin{aligned} f_{12}(x) &= \frac{1}{\sqrt{12}} \left\{ \log(1 + \sqrt{3}\, x + x^2) - \log(1 - \sqrt{3}\, x + x^2) \right\} \\ &= \frac{1}{\sqrt{12}} \log\left(\frac{1 + \sqrt{3}\, x + x^2}{1 - \sqrt{3}\, x + x^2} \right). \end{aligned}$$

Όλα αυτά, μέχρι στιγμής, είναι έγκυρα για $|x| < 1$. Όμως το δεξί μέλος παραπάνω είναι ορισμένο και συνεχές στο $x = 1$. Άρα το άθροισμα της σειράς είναι

$$f_{12}(1) = \frac{1}{\sqrt{12}} \log\left(\frac{2+\sqrt{3}}{2-\sqrt{3}}\right)$$

$$= \frac{1}{\sqrt{12}} \log\big((2+\sqrt{3})^2\big).$$

□

Μπορούμε να ορίσουμε μια παρόμοια συνάρτηση L για $N = 2$:

$$L(s, \chi_8) = \prod_{p \text{ πρώτος}} \big(1 - \chi_8(p)p^{-s}\big)^{-1}$$

$$= \sum_{n=1}^{\infty} \frac{\chi_8(n)}{n^s}$$

$$= 1 - \frac{1}{3^s} - \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} - \frac{1}{11^s} - \frac{1}{13^s} + \frac{1}{15^s} \cdots .$$

Πάλι,

$$L(1, \chi_8) = \prod_{p \text{ πρώτος}} \frac{p}{p - \chi_8(p)}$$

είναι ένα άπειρο γινόμενο που μετρά τον αριθμό των λύσεων της σύγκρισης

$$x^2 - 2y^2 \equiv 1 \pmod{p}.$$

Θεώρημα 8.10. *Ισχύει*

$$L(1, \chi_8) = \frac{\log(3 + 2\sqrt{2})}{\sqrt{8}}.$$

Και

$$1 = (3 - 2\sqrt{2})(3 + 2\sqrt{2}) = 3^2 - 2 \cdot 2^2.$$

Άρα η τιμή της L-συνάρτησης κωδικοποιεί μια λύση της εξίσωσης του Pell.

Η formula του Dirichlet για το class number
στην περίπτωση αρνητικής περιττής θεμελιώδους διακρίνουσας

9 Εισαγωγή: από την εξίσωση του Pell στις τετραγωνικές μορφές σε δύο μεταβλητές

Ένα από τα πιο κλασικά διοφαντικά προβλήματα είναι η εξίσωση του Pell

$$x^2 - dy^2 = 1,$$

όπου $d > 1$ είναι ακέραιος που δεν είναι τέλειο τετράγωνο. Το πρόβλημα αυτό έχει δύο όψεις.

Η πρώτη είναι η *πολλαπλασιαστική* όψη. Αν

$$x^2 - dy^2 = 1 \quad \text{και} \quad u^2 - dv^2 = 1,$$

τότε

$$(xu + dyv)^2 - d(xv + yu)^2 = 1.$$

Ισοδύναμα, αν γράψουμε

$$\alpha = x + y\sqrt{d}, \qquad \beta = u + v\sqrt{d},$$

τότε

$$N(\alpha) = x^2 - dy^2 = 1, \qquad N(\beta) = u^2 - dv^2 = 1,$$

και

$$N(\alpha\beta) = N(\alpha)N(\beta) = 1.$$

Άρα οι λύσεις της Pell συνδυάζονται πολλαπλασιαστικά.

Η δεύτερη είναι η *τετραγωνική* όψη. Η εξίσωση του Pell μπορεί να γραφτεί ως

$$f(x, y) = 1, \qquad \text{όπου} \qquad f(x, y) = x^2 - dy^2.$$

Δηλαδή η Pell είναι μια εξίσωση της μορφής

$$ax^2 + bxy + cy^2 = n,$$

όπου τώρα

$$a = 1, \qquad b = 0, \qquad c = -d.$$

Αυτό οδηγεί φυσικά στη γενική έννοια της τετραγωνικής μορφής σε δύο μεταβλητές.

Ορισμός 9.1. Μια *τετραγωνική μορφή σε δύο μεταβλητές* είναι μια παράσταση

$$f(x, y) = ax^2 + bxy + cy^2,$$

όπου $a, b, c \in \mathbb{Z}$. Θα τη συμβολίζουμε και με

$$f = [a, b, c].$$

Η *διακρίνουσα* της f είναι ο ακέραιος

$$\Delta(f) = b^2 - 4ac.$$

Για παράδειγμα, η μορφή της Pell,

$$f(x, y) = x^2 - dy^2 = [1, 0, -d],$$

έχει διακρίνουσα

$$\Delta(f) = 0^2 - 4 \cdot 1 \cdot (-d) = 4d.$$

Άρα η Pell ανήκει στη θεωρία των μορφών με *θετική* διακρίνουσα. Αντίθετα, όταν

$$\Delta(f) < 0,$$

η μορφή είναι, υπό κατάλληλες υποθέσεις, θετικά ορισμένη, και τότε η γεωμετρία της είναι πολύ διαφορετική: οι καμπύλες

$$f(x, y) = n$$

είναι ελλείψεις και όχι υπερβολές.

Ορισμός 9.2. Η μορφή $f = [a, b, c]$ λέγεται *primitive* αν

$$\gcd(a, b, c) = 1.$$

Ορισμός 9.3. Η μορφή $f = [a, b, c]$ λέγεται *θετικά ορισμένη* αν

$$f(x, y) > 0 \qquad \text{για κάθε } (x, y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}.$$

Ισοδύναμα, για μια μορφή $f = [a, b, c]$, αυτό συμβαίνει ακριβώς όταν

$$a > 0 \qquad \text{και} \qquad \Delta(f) < 0.$$

Το βασικό ερώτημα στη θεωρία αυτή είναι: πότε δύο μορφές πρέπει να θεωρούνται «ίδιες» από αριθμητική άποψη; Η σωστή απάντηση είναι ότι επιτρέπουμε αλλαγές μεταβλητών με ακέραιους συντελεστές και ορίζουσα ± 1, διότι τέτοιες αλλαγές είναι αντιστρέψιμες πάνω στο $\mathbb{Z}^2$ και άρα διατηρούν το σύνολο των ακεραίων που παριστάνονται.

Ορισμός 9.4. Δύο τετραγωνικές μορφές f και g λέγονται *ισοδύναμες* αν υπάρχει πίνακας

$$M = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in GL_2(\mathbb{Z}), \qquad \det M = \pm 1,$$

τέτοιος ώστε

$$g(x, y) = f(px + qy, rx + sy).$$

Αν απαιτήσουμε επιπλέον $\det M = 1$, παίρνουμε μια πιο λεπτή έννοια ισοδυναμίας.

Ορισμός 9.5. Δύο τετραγωνικές μορφές f και g λέγονται *γνησίως ισοδύναμες* αν υπάρχει

$$M = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$$

τέτοιος ώστε

$$g(x, y) = f(px + qy, rx + sy).$$

Ορισμός 9.6. Η *γνήσια κλάση* μιας τετραγωνικής μορφής f είναι το σύνολο όλων των μορφών που είναι γνήσια ισοδύναμες με την f.

Η γνήσια ισοδυναμία είναι η σωστή σχέση για τη σύνδεση με τις αναπαραστάσεις ακεραίων και, τελικά, με τον αριθμό κλάσεων. Πράγματι, αν δύο μορφές είναι γνησίως ισοδύναμες, τότε μία παριστάνει έναν ακέραιο n αν και μόνον αν και η άλλη τον παριστάνει, επειδή η αλλαγή μεταβλητών δίνει αμφιμονοσήμαντη αντιστοιχία ανάμεσα στα ακέραια ζεύγη (x, y).

Στην περίπτωση $\Delta < 0$, οι πρωταρχικές θετικά ορισμένες μορφές με δεδομένη διακρίνουσα Δ διαμερίζονται σε πεπερασμένο αριθμό από γνήσιες κλάσεις. Αυτό είναι το πρώτο ουσιαστικό σημείο της θεωρίας. Το πλήθος αυτών των γνησίων κλάσεων συμβολίζεται συνήθως με

$$h(\Delta)$$

και λέγεται *αριθμός κλάσεων* της διακρίνουσας Δ. Στην περίπτωση αρνητικής διακρίνουσας, η θεωρία των γνησίων κλάσεων γίνεται αποτελεσματική χάρη στην έννοια της ανάγωγης μορφής.

Ορισμός 9.7. Έστω

$$f(x, y) = ax^2 + bxy + cy^2 = [a, b, c]$$

πρωταρχική θετικά ορισμένη τετραγωνική μορφή σε δύο μεταβλητές με διακρίνουσα

$$\Delta = b^2 - 4ac < 0.$$

Η μορφή f λέγεται *ανάγωγη* αν ισχύουν

$$|b| \le a \le c,$$

και επιπλέον, αν συμβαίνει μία από τις ισότητες

$$|b| = a \qquad \text{ή} \qquad a = c,$$

τότε απαιτούμε

$$b \ge 0.$$

Η σημασία του ορισμού αυτού είναι ότι κάθε γνήσια κλάση περιέχει ακριβώς έναν τέτοιο «κανονικό» εκπρόσωπο.

Θεώρημα 9.8 (Θεώρημα αναγωγής για $\Delta < 0$). *Έστω $\Delta < 0$. Τότε κάθε πρωταρχική γνήσια κλάση θετικά ορισμένων τετραγωνικών μορφών σε δύο μεταβλητές με διακρίνουσα Δ περιέχει ακριβώς μία ανάγωγη μορφή.*

Δεν θα αποδείξουμε εδώ το θεώρημα αυτό· θα το χρησιμοποιήσουμε ως κλασικό αποτέλεσμα της θεωρίας των τετραγωνικών μορφών. Η συνέπειά του είναι ότι ο αριθμός των proper classes μπορεί να υπολογιστεί με το χέρι, αρκεί να βρούμε όλες τις reduced primitive μορφές με τη δοσμένη διακρίνουσα.

Πόρισμα 9.9. *Για κάθε αρνητική διακρίνουσα $\Delta < 0$, ο αριθμός κλάσεων $h(\Delta)$ είναι ίσος με το πλήθος των πρωταρχικών αναγώγων θετικά ορισμένων μορφών με διακρίνουσα Δ.*

Υπάρχουν μόνο πεπερασμένες τέτοιες reduced μορφές. Πράγματι, αν

$$[a, b, c]$$

είναι reduced και έχει διακρίνουσα $\Delta < 0$, τότε από τις ανισότητες

$$|b| \leq a \leq c$$

παίρνουμε

$$|\Delta| = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2.$$

Άρα

$$a \leq \sqrt{\frac{|\Delta|}{3}}.$$

Επομένως υπάρχουν μόνο πεπερασμένες δυνατές τιμές για το a, και για κάθε τέτοιο a μόνο πεπερασμένες δυνατές τιμές για το b, ενώ τότε το c καθορίζεται από τη σχέση

$$c = \frac{b^2 - \Delta}{4a}.$$

Άρα οι ανάγωγες μορφές με διακρίνουσα Δ είναι πεπερασμένες.

Παρατήρηση 9.10. Στην πράξη, για να υπολογίσουμε τον αριθμό κλάσεων $h(\Delta)$ για μικρή αρνητική διακρίνουσα Δ, αρκεί:

1. να βρούμε όλες τις ακέραιες τριάδες (a, b, c) με
$$b^2 - 4ac = \Delta,$$
2. να επιβάλουμε τις συνθήκες
$$|b| \leq a \leq c,$$
και αν $|b| = a$ ή $a = c$, τότε $b \geq 0$,
3. να κρατήσουμε μόνο τις πρωταρχικές μορφές, δηλαδή εκείνες με
$$\gcd(a, b, c) = 1.$$

Το πλήθος των μορφών που απομένουν είναι ακριβώς το $h(\Delta)$.

Παράδειγμα 9.11. Ας υπολογίσουμε το πλήθος των κλάσεων για τη διακρίνουσα $\Delta = -15$.

Οι ανάγωγες πρωταρχικές θετικά ορισμένες μορφές $[a, b, c]$ με διακρίνουσα -15 ικανοποιούν

$$|b| \leq a \leq c \qquad \text{και} \qquad a \leq \sqrt{\frac{15}{3}} < 3.$$

Άρα $a = 1$ ή $a = 2$.

Αν $a = 1$, τότε επειδή $b^2 - 4ac = -15$, ο b πρέπει να είναι περιττός και $|b| \leq 1$, άρα $b = \pm 1$. Επειδή $|b| = a$, για ανάγωγη μορφή πρέπει $b \geq 0$, οπότε $b = 1$. Τότε

$$c = \frac{b^2 + 15}{4a} = \frac{1 + 15}{4} = 4,$$

και παίρνουμε τη μορφή

$$[1, 1, 4].$$

Αν $a = 2$, τότε πάλι b είναι περιττός και $|b| \leq 2$, άρα $b = \pm 1$. Για $b = 1$,

$$c = \frac{1 + 15}{8} = 2,$$

οπότε παίρνουμε τη μορφή

$$[2, 1, 2].$$

Η μορφή $[2, -1, 2]$ δεν είναι ανάγωγη, επειδή εδώ $a = c$ και άρα πρέπει να έχουμε $b \geq 0$.

Άρα υπάρχουν ακριβώς δύο ανάγωγες πρωταρχικές μορφές που αντιστοιχούν στην διακρίνουσα -15, δηλαδή

$$[1, 1, 4], \qquad [2, 1, 2].$$

Συνεπώς

$$h(-15) = 2.$$

Μέχρι τώρα ορίσαμε τον αριθμό κλάσεων $h(\Delta)$ ως το πλήθος των γνήσιων κλάσεων των πρωταρχικών θετικά ορισμένων τετραγωνικών μορφών σε δύο μεταβλητές με διακρίνουσα $\Delta < 0$. Ο ορισμός αυτός είναι καθαρά διακριτός. Για να συνδεθεί όμως με μια L-συνάρτηση, πρέπει να τον συσχετίσουμε με το πλήθος λύσεων διοφαντικών εξισώσεων.

Αν

$$f(x, y) = ax^2 + bxy + cy^2$$

είναι μια πρωταρχική θετικά ορισμένη μορφή, ορίζουμε για κάθε $n \geq 1$

$$r_f(n) := \#\{(x, y) \in \mathbb{Z}^2 : \ f(x, y) = n\}.$$

Με άλλα λόγια, το $r_f(n)$ είναι το πλήθος των ακεραίων λύσεων της εξίσωσης

$$ax^2 + bxy + cy^2 = n.$$

Γενικά, το $r_f(n)$ εξαρτάται από τη συγκεκριμένη μορφή f, και δεν υπάρχει απλός ρητός τύπος μόνο με διαιρέτες του n. Έστω

$$f_1, \ldots, f_{h(\Delta)}$$

ένα πλήρες σύστημα εκπροσώπων των γνήσιων κλάσεων πρωταρχικών θετικά ορισμένων μορφών με διακρίνουσα Δ. Ορίζουμε

$$r_\Delta(n) := \sum_{j=1}^{h(\Delta)} r_{f_j}(n).$$

Με άλλα λόγια, το $r_\Delta(n)$ είναι το συνολικό πλήθος αναπαραστάσεων του n από όλες τις γνήσιες κλάσεις με διακρίνουσα Δ.

Το βασικό αριθμητικό γεγονός είναι ότι το $r_\Delta(n)$, σε αντίθεση με το μεμονωμένο $r_f(n)$, έχει κλειστό τύπο. Αν $\Delta < 0$ είναι θεμελιώδης διακρίνουσα, τότε

$$r_\Delta(n) = w_\Delta \sum_{d|n} \chi_\Delta(d),$$

όπου

$$\chi_\Delta(d) = \left(\frac{\Delta}{d}\right)$$

είναι ο αντίστοιχος πραγματικός χαρακτήρας Dirichlet και

$$w_\Delta = \begin{cases} 6, & \Delta = -3, \\ 4, & \Delta = -4, \\ 2, & \Delta < -4. \end{cases}$$

Στην ειδική περίπτωση που εξετάζουμε εδώ, δηλαδή όταν $\Delta < 0$ είναι περιττή θεμελιώδης διακρίνουσα, έχουμε πάντοτε

$$w_\Delta = \begin{cases} 6, & \Delta = -3, \\ 2, & \Delta < -3, \end{cases}$$

οπότε, για $\Delta < -3$,

$$r_\Delta(n) = 2 \sum_{d|n} \chi_\Delta(d).$$

Άρα ο αριθμός κλάσεων δεν ελέγχει το πλήθος λύσεων μιας *συγκεκριμένης* μορφής, αλλά το συνολικό πλήθος λύσεων όταν αθροίσουμε πάνω σε όλες τις proper classes της ίδιας διακρίνουσας.

Παράδειγμα 9.12. Για $\Delta = -15$ είδαμε ότι υπάρχουν ακριβώς δύο reduced primitive θετικά ορισμένες μορφές:

$$[1, 1, 4] \qquad \text{και} \qquad [2, 1, 2].$$

Άρα

$$h(-15) = 2.$$

Οι αντίστοιχες εξισώσεις είναι

$$x^2 + xy + 4y^2 = n \qquad \text{και} \qquad 2x^2 + xy + 2y^2 = n.$$

Επομένως

$$r_{-15}(n) = r_{[1,1,4]}(n) + r_{[2,1,2]}(n).$$

Ο γενικός τύπος δίνει

$$r_{-15}(n) = 2 \sum_{d|n} \chi_{-15}(d).$$

Δηλαδή,

$$r_{[1,1,4]}(n) + r_{[2,1,2]}(n) = 2 \sum_{d|n} \left(\frac{-15}{d}\right).$$

Για παράδειγμα, όταν $n = 1$, έχουμε

$$\sum_{d|1} \chi_{-15}(d) = \chi_{-15}(1) = 1,$$

άρα

$$r_{[1,1,4]}(1) + r_{[2,1,2]}(1) = 2.$$

Πράγματι,

$$x^2 + xy + 4y^2 = 1$$

έχει ακριβώς τις δύο λύσεις

$$(1,0), \quad (-1,0),$$

ενώ η εξίσωση

$$2x^2 + xy + 2y^2 = 1$$

δεν έχει ακέραιες λύσεις. Άρα συνολικά υπάρχουν 2 λύσεις, όπως προβλέπει ο τύπος.

Όταν $n = 2$, έχουμε

$$\sum_{d|2} \chi_{-15}(d) = \chi_{-15}(1) + \chi_{-15}(2) = 1 + 1 = 2,$$

οπότε

$$r_{[1,1,4]}(2) + r_{[2,1,2]}(2) = 4.$$

Και πράγματι, η εξίσωση

$$2x^2 + xy + 2y^2 = 2$$

έχει τις τέσσερις λύσεις

$$(1,0),\ (-1,0),\ (0,1),\ (0,-1),$$

ενώ η

$$x^2 + xy + 4y^2 = 2$$

δεν έχει ακέραιες λύσεις.

Η σημασία του τύπου αυτού είναι ότι, όταν αθροίσουμε ως προς $n \leq X$, το αριστερό μέλος μπορεί να υπολογιστεί γεωμετρικά με μέτρηση ακέραιων σημείων σε ελλείψεις, ενώ το δεξί μέλος υπολογίζεται αναλυτικά μέσω της L-συνάρτησης

$$L(s, \chi_\Delta) = \sum_{n=1}^{\infty} \frac{\chi_\Delta(n)}{n^s}.$$

Η ταύτιση των δύο κύριων όρων είναι ακριβώς η formula του Dirichlet class number. Το επόμενο βήμα είναι να συνδέσουμε αυτή τη θεωρία με τις τετραγωνικές μορφές modulo πρώτους. Αν Δ είναι ένας ακέραιος με

$$\Delta \equiv 0 \text{ ή } 1 \pmod 4,$$

τότε για κάθε περιττό πρώτο $p \nmid \Delta$ το σύμβολο Legendre

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

μας λέει αν η διακρίνουσα Δ είναι ή όχι τετράγωνο modulo p. Όταν η Δ είναι *θεμελιώδης διακρίνουσα*, δηλαδή δεν προκύπτει από μικρότερη διακρίνουσα με αφαίρεση τετραγωνικού παράγοντα, το σύμβολο αυτό επεκτείνεται σε έναν πρωταρχικό πραγματικό χαρακτήρα Dirichlet

$$\chi_\Delta(n) = \left(\frac{\Delta}{n}\right).$$

Για τις αρνητικές θεμελιώδεις διακρίνουσες, η αντίστοιχη σειρά Dirichlet

$$L(s, \chi_\Delta) = \sum_{n=1}^{\infty} \frac{\chi_\Delta(n)}{n^s}$$

κρύβει μέσα της τον αριθμό κλάσεων $h(\Delta)$. Ο στόχος μας είναι να αποδείξουμε ότι για $\Delta < 0$ περιττή θεμελιώδη διακρίνουσα ισχύει

$$L(1, \chi_\Delta) = \frac{2\pi}{w_\Delta \sqrt{|\Delta|}}\, h(\Delta),$$

όπου w_Δ είναι ο $w_\Delta = 6$ όταν $\Delta = -3$, $w_\Delta = 4$ όταν $\Delta = -4$ και $w_\Delta = 2$ όταν $\Delta < -4$.

Με άλλα λόγια, μια ειδική τιμή μιας αναλυτικής συνάρτησης, της $L(s, \chi_\Delta)$, μετρά έναν καθαρά διακριτό αριθμητικό αναλλοίωτο, δηλαδή το πλήθος των γνησίων κλάσεων τετραγωνικών μορφών σε δύο μεταβλητές με διακρίνουσα Δ.

Ορισμός 9.13. Θέτουμε

$$w_D = \begin{cases} 6, & D = -3, \\ 4, & D = -4 \\ 2, & D < -4 \end{cases}$$

Ο στόχος είναι να αποδειχθεί το εξής.

Θεώρημα 9.14 (Dirichlet class number formula: αρνητική περιττή περίπτωση). *Έστω $D < 0$ περιττή θεμελιώδης διακρίνουσα. Τότε*

$$L(1, \chi_D) = \frac{2\pi}{w_D \sqrt{|D|}}\, h(D).$$

10 Αυτομορφισμοί θετικά ορισμένων μορφών

Ο πρώτος λεπτός αριθμητικός όρος που θα χρειαστούμε είναι ο αριθμός γνήσιων αυτομορφισμών μιας πρωταρχικής θετικά ορισμένης μορφής με διακρίνουσα D.

Ορισμός 10.1. Για μια μορφή $f = [a, b, c]$, ορίζουμε

$$\mathrm{Aut}^+(f) = \{M \in \mathrm{SL}_2(\mathbb{Z}) : f^M = f\},$$

όπου

$$f^M(x, y) := f(px + qy, rx + sy), \qquad M = \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

Λήμμα 10.2. *Έστω $f = [a, b, c]$ πρωταρχική θετικά ορισμένη μορφή με διακρίνουσα $D < 0$. Θέτουμε*

$$S_f = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}, \qquad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad A_f = JS_f = \begin{pmatrix} -b & -2c \\ 2a & b \end{pmatrix}.$$

Τότε:

1. $A_f^2 = D\, I_2$.
2. *Αν $U \in \mathrm{Aut}^+(f)$, τότε U αντιμετατίθεται με το A_f.*
3. *Κάθε $U \in \mathrm{Aut}^+(f)$ γράφεται μοναδικά με τη μορφή*

$$U = \begin{pmatrix} \dfrac{t - bu}{2} & -cu \\ au & \dfrac{t + bu}{2} \end{pmatrix}$$

για κάποιους ακεραίους t, u που ικανοποιούν

$$t^2 - Du^2 = 4.$$

Αντίστροφα, κάθε τέτοιος πίνακας ανήκει στην $\mathrm{Aut}^+(f)$.

Απόδειξη. Πρώτα,

$$A_f^2 = \begin{pmatrix} -b & -2c \\ 2a & b \end{pmatrix}^2 = \begin{pmatrix} b^2 - 4ac & 0 \\ 0 & b^2 - 4ac \end{pmatrix} = D\, I_2.$$

Τώρα έστω $U \in \mathrm{Aut}^+(f)$. Η συνθήκη $f^U = f$ ισοδυναμεί με

$$U^T S_f U = S_f.$$

Πράγματι, αν

$$S_f = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}, \qquad X = \begin{pmatrix} x \\ y \end{pmatrix},$$

τότε

$$2f(x, y) = X^T S_f X.$$

Άρα

$$2f^U(x, y) = (UX)^T S_f (UX) = X^T U^T S_f U\, X.$$

Επομένως η συνθήκη $f^U = f$ ισοδυναμεί με

$$U^T S_f U = S_f.$$

Άρα

$$S_f U = U^{-T} S_f.$$

Επειδή $\det(U) = 1$,

$$U^{-T} = \begin{pmatrix} s & -r \\ -q & p \end{pmatrix},$$

οπότε, για

$$J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

υπολογίζουμε άμεσα ότι

$$J\, U^{-T} = \begin{pmatrix} q & -p \\ s & -r \end{pmatrix} = U\, J.$$

Πολλαπλασιάζοντας την $S_f U = U^{-T} S_f$ από αριστερά με J, παίρνουμε

$$J S_f U = J U^{-T} S_f = U J S_f.$$

Δηλαδή

$$A_f U = U A_f.$$

Επειδή $D < 0$ και άρα D δεν είναι τετράγωνο στο $\mathbb{Q}$, το ελάχιστο πολυώνυμο του A_f πάνω από το $\mathbb{Q}$ είναι το

$$X^2 - D.$$

Επειδή το ελάχιστο πολυώνυμο του A_f είναι το $X^2 - D$, έχει βαθμό 2. Άρα υπάρχει διάνυσμα v τέτοιο ώστε τα $v, A_f v$ να αποτελούν βάση του $\mathbb{Q}^2$. Αν U αντιμετατίθεται με τον A_f, τότε ο U καθορίζεται από το $U(v)$, και αν

$$U(v) = xv + yA_f v,$$

τότε, από τη σχέση $UA_f = A_f U$, παίρνουμε επίσης

$$U(A_f v) = A_f U(v) = xA_f v + yA_f^2 v.$$

Άρα ο U συμφωνεί στη βάση $(v, A_f v)$ με τον πίνακα $xI + yA_f$. Επομένως

$$U = xI + yA_f.$$

Συνεπώς το σύνολο των πινάκων που αντιμετατίθενται με τον A_f είναι ακριβώς

$$\mathbb{Q}[A_f] = \{xI + yA_f : \ x, y \in \mathbb{Q}\}.$$

Επομένως υπάρχουν μοναδικοί $x, y \in \mathbb{Q}$ με

$$U = xI_2 + yA_f = \begin{pmatrix} x - by & -2cy \\ 2ay & x + by \end{pmatrix}.$$

Θέτουμε

$$t = 2x, \qquad u = 2y.$$

Τότε

$$U = \begin{pmatrix} \dfrac{t - bu}{2} & -cu \\ au & \dfrac{t + bu}{2} \end{pmatrix}.$$

Επειδή ο U έχει ακέραια στοιχεία, συμπεραίνουμε ότι $t, u \in \mathbb{Z}$.

Από την εξίσωση $A_f^2 = DI_2$ παίρνουμε

$$U = (xI_2 + yA_f) \quad \Longrightarrow \quad \det(U) = x^2 - Dy^2.$$

Πράγματι, από τις σχέσεις

$$\operatorname{tr}(A_f) = 0 \qquad \text{και} \qquad \det(A_f) = -D$$

και το γεγονός ότι για κάθε 2×2 πίνακα A ισχύει

$$\det(xI_2 + yA) = x^2 + xy \operatorname{tr}(A) + y^2 \det(A),$$

παίρνουμε

$$\det(xI_2 + yA_f) = x^2 - Dy^2.$$

Επειδή $\det(U) = 1$, παίρνουμε

$$x^2 - Dy^2 = 1 \qquad \Longleftrightarrow \qquad t^2 - Du^2 = 4.$$

Αντίστροφα, αν

$$U = xI_2 + yA_f \qquad \text{με} \qquad x^2 - Dy^2 = 1,$$

τότε

$$U^T S_f U = (xI_2 + yA_f)^T S_f (xI_2 + yA_f).$$

Επειδή $A_f = JS_f$, έχουμε

$$A_f^T S_f = -S_f A_f.$$

Άρα

$$U^T S_f U = x^2 S_f + xy(A_f^T S_f + S_f A_f) + y^2 A_f^T S_f A_f = x^2 S_f - y^2 S_f A_f^2.$$

Εφόσον $A_f^2 = DI_2$, παίρνουμε

$$U^T S_f U = (x^2 - Dy^2) S_f = S_f.$$

Άρα $U \in \operatorname{Aut}^+(f)$. Το λήμμα αποδείχθηκε. □

Πόρισμα 10.3. *Έστω f πρωταρχική θετικά ορισμένη μορφή με περιττή θεμελιώδη διακρίνουσα $D < 0$. Τότε*

$$|\operatorname{Aut}^+(f)| = w_D = \begin{cases} 6, & D = -3, \\ 2, & D < -4 \end{cases}$$

Απόδειξη. Από το προηγούμενο λήμμα, οι proper αυτομορφισμοί του f αντιστοιχούν στις ακέραιες λύσεις της Pell–τύπου εξίσωσης

$$t^2 - Du^2 = 4.$$

Επειδή $D < 0$, αυτό γράφεται

$$t^2 + |D|u^2 = 4.$$

Αν $D < -4$, τότε $|D| \geq 7$, άρα η μόνη δυνατότητα είναι $u = 0$, οπότε $t = \pm 2$. Αυτό δίνει ακριβώς τους δύο αυτομορφισμούς I_2 και $-I_2$.

Αν $D = -3$, η εξίσωση είναι

$$t^2 + 3u^2 = 4.$$

Πέρα από τις λύσεις $(t, u) = (\pm 2, 0)$, έχουμε και τις τέσσερις λύσεις

$$(t, u) = (1, 1),\ (1, -1),\ (-1, 1),\ (-1, -1).$$

Συνολικά παίρνουμε 6 proper αυτομορφισμούς. Άρα

$$|\operatorname{Aut}^+(f)| = w_D.$$

□

11 Primitive αναπαραστάσεις και ρίζες της $b^2 \equiv D \pmod{4n}$

Ορισμός 11.1. Για $n \geq 1$, ορίζουμε

$$r_D(n) := \sum_{j=1}^{h(D)} \#\{(x, y) \in \mathbb{Z}^2 : f_j(x, y) = n\},$$

και

$$r_D^*(n) := \sum_{j=1}^{h(D)} \#\{(x, y) \in \mathbb{Z}^2 :\ f_j(x, y) = n,\ \gcd(x, y) = 1\}.$$

Ορισμός 11.2. Για $n \geq 1$, θέτουμε

$$\rho_D(n) := \#\{\beta \pmod{2n} :\ \beta^2 \equiv D \pmod{4n}\}.$$

Λήμμα 11.3. *Για κάθε $n \geq 1$,*

$$r_D^*(n) = w_D\, \rho_D(n).$$

Απόδειξη. Για κάθε j, θέτουμε

$$\mathcal{R}_j^*(n) := \{(x, y) \in \mathbb{Z}^2 :\ f_j(x, y) = n,\ \gcd(x, y) = 1\}.$$

Για κάθε j, η ομάδα $\operatorname{Aut}^+(f_j)$ δρα στο $\mathcal{R}_j^*(n)$ με

$$T \cdot v := Tv.$$

Έστω $v \in \mathcal{R}_j^*(n)$. Θα δείξουμε ότι ο σταθεροποιητής του v είναι τετριμμένος.

Πράγματι, αν $T \in \mathrm{Aut}^+(f_j)$ και $Tv = v$, γράφουμε $v = (x, y)$ και επιλέγουμε

$$M = \begin{pmatrix} x & u \\ y & v' \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Επειδή η πρώτη στήλη του M είναι το $v = (x, y)$, έχουμε

$$f_j^M(X, 0) = f_j(xX, yX) = X^2 f_j(x, y) = nX^2.$$

Άρα ο συντελεστής του X^2 στη μορφή f_j^M είναι ίσος με n, και επομένως

$$g = [n, B, C]$$

για κάποιους ακεραίους B, C. Θέτουμε

$$g := f_j^M = [n, B, C] \qquad \text{και} \qquad U := M^{-1}TM \in \mathrm{Aut}^+(g).$$

Επειδή $Me_1 = v$ και $Tv = v$, έχουμε

$$Ue_1 = e_1.$$

Άρα ο U έχει τη μορφή

$$U = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$

για κάποιο $t \in \mathbb{Z}$.

Τώρα

$$g(X, Y) = nX^2 + BXY + CY^2,$$

οπότε

$$g^U(X, Y) = g(X + tY, Y) = nX^2 + (2nt + B)XY + (nt^2 + Bt + C)Y^2.$$

Εφόσον $U \in \mathrm{Aut}^+(g)$, έχουμε $g^U = g$. Συγκρίνοντας τον συντελεστή του XY, παίρνουμε

$$2nt + B = B,$$

άρα $t = 0$. Επομένως $U = I$, και συνεπώς $T = I$.

Άρα ο σταθεροποιητής κάθε $v \in \mathcal{R}_j^*(n)$ είναι τετριμμένος. Από το θεώρημα τροχιάς–σταθεροποιητή,

$$|\,\mathrm{Aut}^+(f_j) \cdot v| = \frac{|\,\mathrm{Aut}^+(f_j)|}{|\mathrm{Stab}_{\mathrm{Aut}^+(f_j)}(v)|} = |\,\mathrm{Aut}^+(f_j)| = w_D.$$

Συνεπώς κάθε τροχιά έχει ακριβώς w_D στοιχεία.

Θα δείξουμε ότι το σύνολο

$$\bigsqcup_{j=1}^{h(D)} \mathcal{R}_j^*(n)/\,\mathrm{Aut}^+(f_j)$$

είναι σε αμφιμονοσήμαντη αντιστοιχία με το σύνολο

$$\{\beta \pmod{2n} :\ \beta^2 \equiv D \pmod{4n}\}.$$

Θέτουμε

$$\widetilde{\mathcal{R}}^*(n) := \bigsqcup_{j=1}^{h(D)} \mathcal{R}_j^*(n)/\,\mathrm{Aut}^+(f_j).$$

Θα ορίσουμε μια απεικόνιση

$$\Phi : \widetilde{\mathcal{R}}^*(n) \longrightarrow \{\beta \pmod{2n} : \ \beta^2 \equiv D \pmod{4n}\}$$

και θα δείξουμε ότι είναι αμφιμονοσήμαντη.

Ορισμός της Φ**.** Έστω $[v] \in \widetilde{\mathcal{R}}^*(n)$, όπου

$$v = (x, y) \in \mathcal{R}_j^*(n)$$

για κάποιο j. Επειδή $\gcd(x, y) = 1$, υπάρχει

$$M = \begin{pmatrix} x & u \\ y & v' \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Γράφουμε

$$f_j^M = [n, B, C].$$

Τότε

$$B^2 - 4nC = D,$$

άρα

$$B^2 \equiv D \pmod{4n}.$$

Ορίζουμε

$$\Phi([v]) = B \pmod{2n}.$$

Η Φ είναι καλά ορισμένη. Πράγματι, αν αλλάξουμε τη δεύτερη στήλη του M σε $(u, v')+t(x, y)$, τότε αντικαθιστούμε τον M με

$$M \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix},$$

και ο μεσαίος συντελεστής αλλάζει από B σε $B + 2nt$, άρα η κλάση modulo $2n$ δεν αλλάζει. Επίσης, αν αντικαταστήσουμε το v με Tv, όπου $T \in \mathrm{Aut}^+(f_j)$, και το M με TM, τότε

$$f_j^{TM} = f_j^M,$$

οπότε η κλάση $B \pmod{2n}$ μένει ίδια. Άρα η Φ εξαρτάται μόνο από την τροχιά $[v]$.

Η Φ **είναι επί.** Έστω

$$\beta \pmod{2n}, \qquad \beta^2 \equiv D \pmod{4n}.$$

Επιλέγουμε έναν ακέραιο εκπρόσωπο B της β και θέτουμε

$$C := \frac{B^2 - D}{4n}.$$

Τότε η μορφή

$$g = [n, B, C]$$

έχει διακρίνουσα D. Είναι πρωταρχική: αν κάποιος πρώτος p διαιρούσε ταυτόχρονα τα n, B, C, τότε από

$$D = B^2 - 4nC$$

θα είχαμε $p^2 \mid D$, άτοπο αφού ο D είναι περιττή θεμελιώδης διακρίνουσα. Επίσης, επειδή $D < 0$ και ο πρώτος συντελεστής της g είναι $n > 0$, η g είναι θετικά ορισμένη.

Άρα η g ανήκει σε μοναδική γνήσια κλάση από τις $f_1, \ldots, f_{h(D)}$. Έστω ότι

$$g = f_j^M$$

για κάποιο j και κάποιο

$$M = \begin{pmatrix} x & u \\ y & v' \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Τότε η πρώτη στήλη $v = (x, y)$ του M ικανοποιεί

$$f_j(x, y) = n \qquad \text{και} \qquad \gcd(x, y) = 1,$$

δηλαδή

$$v \in \mathcal{R}_j^*(n).$$

Από τον ορισμό της Φ, παίρνουμε

$$\Phi([v]) = B \pmod{2n} = \beta.$$

Άρα η Φ είναι επί.

Η Φ είναι 1-1. Έστω

$$\Phi([v_1]) = \Phi([v_2]).$$

Έστω

$$v_i \in \mathcal{R}_{j_i}^*(n) \qquad (i = 1, 2),$$

και διαλέγουμε πίνακες

$$M_i = \begin{pmatrix} x_i & u_i \\ y_i & v_i' \end{pmatrix} \in SL_2(\mathbb{Z})$$

με πρώτη στήλη το v_i, έτσι ώστε

$$f_{j_i}^{M_i} = [n, B_i, C_i].$$

Η ισότητα

$$\Phi([v_1]) = \Phi([v_2])$$

σημαίνει ότι

$$B_1 \equiv B_2 \pmod{2n}.$$

Άρα υπάρχει $t \in \mathbb{Z}$ με

$$B_2 = B_1 + 2nt.$$

Αντικαθιστούμε τον M_2 με

$$M_2' := M_2 \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix}.$$

Η πρώτη στήλη του M_2' είναι πάλι το v_2, ενώ η μορφή $f_{j_2}^{M_2'}$ έχει πρώτο συντελεστή n και μεσαίο συντελεστή B_1. Επειδή η διακρίνουσα είναι D, ο τρίτος συντελεστής καθορίζεται αναγκαστικά από

$$C = \frac{B_1^2 - D}{4n}.$$

Άρα

$$f_{j_1}^{M_1} = f_{j_2}^{M_2'} = [n, B_1, C].$$

Επομένως οι f_{j_1} και f_{j_2} είναι γνήσια ισοδύναμες. Εφόσον οι

$$f_1, \ldots, f_{h(D)}$$

είναι εκπρόσωποι διαφορετικών γνησίων κλάσεων, συμπεραίνουμε ότι

$$j_1 = j_2 =: j.$$

Τότε

$$f_j^{M_1} = f_j^{M_2'},$$

άρα

$$M_2' M_1^{-1} \in \mathrm{Aut}^+(f_j).$$

Επομένως οι πρώτες στήλες των M_1 και M_2', δηλαδή τα v_1 και v_2, ανήκουν στην ίδια $\mathrm{Aut}^+(f_j)$-τροχιά. Άρα

$$[v_1] = [v_2].$$

Αυτό δείχνει ότι η Φ είναι 1-1.

Συνεπώς η Φ είναι αμφιμονοσήμαντη, και άρα

$$\left|\widetilde{\mathcal{R}}^*(n)\right| = \#\{\beta \pmod{2n} : \ \beta^2 \equiv D \pmod{4n}\} = \rho_D(n).$$

και επομένως δίνουν αμφιμονοσήμαντη αντιστοιχία

$$\bigsqcup_{j=1}^{h(D)} \mathcal{R}_j^*(n)/\,\mathrm{Aut}^+(f_j) \ \longleftrightarrow\ \{\beta \pmod{2n} : \ \beta^2 \equiv D \pmod{4n}\}.$$

Άρα

$$\#\left(\bigsqcup_{j=1}^{h(D)} \mathcal{R}_j^*(n)/\,\mathrm{Aut}^+(f_j)\right) = \rho_D(n).$$

Τώρα, για κάθε j, το σύνολο $\mathcal{R}_j^*(n)$ γράφεται ως ξένη ένωση των τροχιών της $\mathrm{Aut}^+(f_j)$. Επειδή κάθε τέτοια τροχιά έχει ακριβώς w_D στοιχεία, παίρνουμε

$$|\mathcal{R}_j^*(n)| = w_D\, |\mathcal{R}_j^*(n)/\,\mathrm{Aut}^+(f_j)|.$$

Αθροίζοντας ως προς $j = 1, \ldots, h(D)$, βρίσκουμε

$$r_D^*(n) = \sum_{j=1}^{h(D)} |\mathcal{R}_j^*(n)| = w_D \sum_{j=1}^{h(D)} |\mathcal{R}_j^*(n)/\,\mathrm{Aut}^+(f_j)|.$$

Επειδή η ένωση

$$\bigsqcup_{j=1}^{h(D)} \mathcal{R}_j^*(n)/\,\mathrm{Aut}^+(f_j)$$

είναι ξένη, αυτό γράφεται

$$r_D^*(n) = w_D \left|\bigsqcup_{j=1}^{h(D)} \mathcal{R}_j^*(n)/\,\mathrm{Aut}^+(f_j)\right|.$$

Από την αμφιμονοσήμαντη αντιστοιχία που δείξαμε παραπάνω, το τελευταίο πλήθος είναι ίσο με $\rho_D(n)$. Άρα

$$r_D^*(n) = w_D\, \rho_D(n).$$

Τέλος, κάθε $\mathrm{Aut}^+(f_j)$-τροχιά έχει ακριβώς w_D στοιχεία, επειδή η δράση είναι ελεύθερη και

$$|\,\mathrm{Aut}^+(f_j)| = w_D.$$

Άρα

$$r_D^*(n) = w_D\, \rho_D(n).$$

□

Λήμμα 11.4. *Για κάθε $n \geq 1$,*

$$r_D(n) = \sum_{g^2 | n} r_D^*\left(\frac{n}{g^2}\right).$$

Απόδειξη. Έστω $f = [a, b, c]$ πρωταρχική μορφή και

$$f(x, y) = n.$$

Αν θέσουμε

$$g = \gcd(x, y), \qquad x = gx_0, \qquad y = gy_0,$$

τότε $\gcd(x_0, y_0) = 1$ και, επειδή η f είναι ομογενής βαθμού 2,

$$n = f(x, y) = g^2 f(x_0, y_0).$$

Άρα κάθε αναπαράσταση του n προκύπτει μοναδικά από μια πρωταρχική αναπαράσταση του n/g^2, για κάποιο $g^2 \mid n$. Αθροίζοντας πάνω σε όλα τα f_j, παίρνουμε ακριβώς τον ζητούμενο τύπο. □

Λήμμα 11.5. *Η συνάρτηση ρ_D είναι πολλαπλασιαστική.*

Απόδειξη. Αν $(m, n) = 1$, τότε από το Κινεζικό Θεώρημα Υπολοίπων, η ισοτιμία

$$\beta^2 \equiv D \pmod{4mn}$$

είναι ισοδύναμη με το σύστημα

$$\beta^2 \equiv D \pmod{4m}, \qquad \beta^2 \equiv D \pmod{4n},$$

και οι κλάσεις modulo $2mn$ αντιστοιχούν ακριβώς σε ζεύγη κλάσεων modulo $2m$ και modulo $2n$. Άρα

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

□

Λήμμα 11.6. *Έστω p περιττός πρώτος με $p \nmid D$. Τότε, για κάθε $\alpha \geq 1$,*

$$\rho_D(p^\alpha) = 1 + \chi_D(p).$$

Απόδειξη. Επειδή D είναι περιττός, κάθε λύση της

$$\beta^2 \equiv D \pmod{4p^\alpha}$$

είναι περιττή. Άρα η $\beta \pmod{2p^\alpha}$ καθορίζεται μονοσήμαντα από τη ρίζα της modulo p^α. Επομένως αρκεί να μετρήσουμε τις ρίζες της

$$x^2 \equiv D \pmod{p^\alpha}.$$

Αν $\chi_D(p) = -1$, τότε η $x^2 \equiv D \pmod{p}$ δεν έχει λύσεις, άρα ούτε modulo p^α. Συνεπώς

$$\rho_D(p^\alpha) = 0 = 1 + \chi_D(p).$$

Αν $\chi_D(p) = 1$, τότε η $x^2 \equiv D \pmod{p}$ έχει ακριβώς δύο ρίζες modulo p. Καθεμία «ανεβαίνει» μοναδικά σε ρίζα modulo p^α. Πράγματι, αν u_k ικανοποιεί

$$u_k^2 \equiv D \pmod{p^k},$$

ζητούμε έναν $t \pmod p$ ώστε

$$u_{k+1} := u_k + tp^k$$

να ικανοποιεί

$$u_{k+1}^2 \equiv D \pmod{p^{k+1}}.$$

Αναπτύσσοντας,

$$u_k^2 + 2u_k tp^k \equiv D \pmod{p^{k+1}}.$$

Αν γράψουμε

$$u_k^2 - D = p^k m,$$

η παραπάνω συνθήκη γίνεται

$$m + 2u_k t \equiv 0 \pmod p.$$

Επειδή $p \nmid u_k$, ο t καθορίζεται μοναδικά modulo p. Άρα κάθε ρίζα modulo p^k ανεβαίνει μοναδικά σε ρίζα modulo p^{k+1}. Συνεπώς υπάρχουν ακριβώς δύο ρίζες modulo p^α, και άρα

$$\rho_D(p^\alpha) = 2 = 1 + \chi_D(p).$$

□

Λήμμα 11.7. *Έστω p περιττός πρώτος με $p \mid D$. Τότε*

$$\rho_D(p) = 1, \qquad \rho_D(p^\alpha) = 0 \quad (\alpha \geq 2).$$

Απόδειξη. Επειδή D είναι τετραγωνοελεύθερος, κάθε περιττός πρώτος που διαιρεί το D το διαιρεί ακριβώς μία φορά.

Για $\alpha = 1$, ζητούμε τις κλάσεις $\beta \pmod{2p}$ με

$$\beta^2 \equiv D \pmod{4p}.$$

Modulo p, αυτό δίνει

$$\beta^2 \equiv 0 \pmod p,$$

άρα $p \mid \beta$. Επειδή $D \equiv 1 \pmod 4$, κάθε λύση είναι περιττή. Στο $\mathbb{Z}/2p\mathbb{Z}$, η μοναδική κλάση που είναι ταυτόχρονα $0 \pmod p$ και περιττή είναι η

$$\beta \equiv p \pmod{2p}.$$

Άρα $\rho_D(p) = 1$.

Αν $\alpha \geq 2$ και υπήρχε λύση της

$$\beta^2 \equiv D \pmod{4p^\alpha},$$

τότε πάλι $p \mid \beta$, άρα $p^2 \mid \beta^2$. Από τη σύγκριση θα παίρναμε τότε $p^2 \mid D$, άτοπο. Άρα

$$\rho_D(p^\alpha) = 0 \qquad (\alpha \geq 2).$$

□

Λήμμα 11.8. *Για κάθε $\alpha \geq 1$,*

$$\rho_D(2^\alpha) = 1 + \chi_D(2).$$

Απόδειξη. Θυμίζουμε ότι $\rho_D(2^\alpha)$ είναι ο αριθμός των κλάσεων

$$\beta \pmod{2^{\alpha+1}} \qquad \text{με} \qquad \beta^2 \equiv D \pmod{2^{\alpha+2}}.$$

Περίπτωση 1: $D \equiv 5 \pmod 8$. Κάθε περιττό τετράγωνο είναι ίσο με $1 \pmod 8$. Άρα η ισοτιμία

$$\beta^2 \equiv D \pmod 8$$

δεν έχει λύσεις. Επομένως

$$\rho_D(2^\alpha) = 0 \qquad (\alpha \geq 1).$$

Επειδή τώρα $\chi_D(2) = -1$, παίρνουμε

$$\rho_D(2^\alpha) = 0 = 1 + \chi_D(2).$$

Περίπτωση 2: $D \equiv 1 \pmod 8$. Θα δείξουμε ότι

$$\rho_D(2^\alpha) = 2 \qquad (\alpha \geq 1).$$

Για $\alpha = 1$, οι λύσεις της

$$\beta^2 \equiv D \pmod 8$$

είναι ακριβώς οι δύο περιττές κλάσεις modulo 4, δηλαδή

$$\beta \equiv 1,\ 3 \pmod 4.$$

Άρα $\rho_D(2) = 2$.

Θέτουμε γενικότερα, για $m \geq 3$,

$$N_m := \#\{x \pmod{2^{m-1}} :\ x^2 \equiv D \pmod{2^m}\}.$$

Τότε $\rho_D(2^\alpha) = N_{\alpha+2}$. Έχουμε ήδη $N_3 = 2$. Θα δείξουμε ότι

$$N_{m+1} = N_m \qquad (m \geq 3).$$

Έστω $x \pmod{2^{m-1}}$ με

$$x^2 \equiv D \pmod{2^m}.$$

Οι δύο δυνατές ανυψώσεις της κλάσης $x \pmod{2^{m-1}}$ σε κλάσεις modulo 2^m είναι οι

$$x, \qquad x + 2^{m-1}.$$

Υπολογίζουμε

$$(x + 2^{m-1})^2 - x^2 = 2^m x + 2^{2m-2}.$$

Επειδή κάθε λύση είναι περιττή, x είναι περιττός, άρα

$$2^m x + 2^{2m-2} \equiv 2^m \pmod{2^{m+1}}.$$

Άρα ακριβώς μία από τις δύο κλάσεις x και $x + 2^{m-1}$ ικανοποιεί την ισοτιμία modulo 2^{m+1}. Επομένως κάθε λύση modulo 2^m ανυψώνεται μοναδικά σε λύση modulo 2^{m+1}, και έτσι $N_{m+1} = N_m$.

Άρα επαγωγικά $N_m = 2$ για όλα τα $m \geq 3$, δηλαδή

$$\rho_D(2^\alpha) = 2 \qquad (\alpha \geq 1).$$

Επειδή τώρα $\chi_D(2) = 1$, παίρνουμε

$$\rho_D(2^\alpha) = 2 = 1 + \chi_D(2).$$

Το λήμμα αποδείχθηκε. □

Πρόταση 11.9. *Για κάθε* $n \geq 1$,

$$r_D(n) = w_D \sum_{d|n} \chi_D(d).$$

Απόδειξη. Από το Λήμμα 11.4 και το Λήμμα 11.3, έχουμε

$$r_D(n) = \sum_{g^2|n} r_D^*\left(\frac{n}{g^2}\right) = w_D \sum_{g^2|n} \rho_D\left(\frac{n}{g^2}\right).$$

Θέτουμε λοιπόν

$$a_D(n) := \sum_{g^2|n} \rho_D\left(\frac{n}{g^2}\right).$$

Αρκεί να δείξουμε ότι

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

Η a_D είναι πολλαπλασιαστική, επειδή η ρ_D είναι πολλαπλασιαστική (Λήμμα 11.5). Άρα αρκεί να υπολογίσουμε τις τιμές της σε πρώτες δυνάμεις.

(i) Έστω $p \nmid D$, p **περιττός.** Από το Λήμμα 11.6,

$$\rho_D(p^\alpha) = 1 + \chi_D(p) \qquad (\alpha \geq 1).$$

Αν $\chi_D(p) = 1$, τότε $\rho_D(p^\alpha) = 2$ για κάθε $\alpha \geq 1$, και έτσι

$$a_D(p^\alpha) = \begin{cases} 1, & \alpha = 0, \\ 2 + 1 = 3, & \alpha = 2, \\ \alpha + 1, & \text{γενικά}, \end{cases}$$

καθώς

$$a_D(p^\alpha) = \sum_{\nu=0}^{\lfloor \alpha/2 \rfloor} \rho_D(p^{\alpha-2\nu}) = 1 + 2\lfloor \alpha/2 \rfloor + \begin{cases} 1, & \alpha \text{ περιττός}, \\ 0, & \alpha \text{ άρτιος}, \end{cases} = \alpha + 1.$$

Από την άλλη,

$$\sum_{j=0}^{\alpha} \chi_D(p)^j = \sum_{j=0}^{\alpha} 1 = \alpha + 1.$$

Αν $\chi_D(p) = -1$, τότε $\rho_D(p^\alpha) = 0$ για κάθε $\alpha \geq 1$, άρα

$$a_D(p^\alpha) = \sum_{\nu=0}^{\lfloor \alpha/2 \rfloor} \rho_D(p^{\alpha-2\nu}) = \begin{cases} 1, & \alpha \text{ άρτιος}, \\ 0, & \alpha \text{ περιττός}. \end{cases}$$

Αλλά

$$\sum_{j=0}^{\alpha} (-1)^j = \begin{cases} 1, & \alpha \text{ άρτιος}, \\ 0, & \alpha \text{ περιττός}. \end{cases}$$

Άρα και πάλι

$$a_D(p^\alpha) = \sum_{j=0}^{\alpha} \chi_D(p)^j.$$

(ii) Έστω $p \mid D$, p **περιττός.** Από το Λήμμα 11.7,

$$\rho_D(p) = 1, \qquad \rho_D(p^\alpha) = 0 \quad (\alpha \geq 2).$$

Άρα για κάθε $\alpha \geq 0$,

$$a_D(p^\alpha) = 1.$$

Από την άλλη, $\chi_D(p) = 0$, οπότε

$$\sum_{j=0}^{\alpha} \chi_D(p)^j = 1.$$

Άρα

$$a_D(p^\alpha) = \sum_{j=0}^{\alpha} \chi_D(p)^j.$$

(iii) Η περίπτωση $p = 2$. Από το Λήμμα 11.8,

$$\rho_D(2^\alpha) = 1 + \chi_D(2) \qquad (\alpha \geq 1).$$

Ακριβώς με την ίδια ανάλυση όπως στο (i), παίρνουμε

$$a_D(2^\alpha) = \sum_{j=0}^{\alpha} \chi_D(2)^j.$$

Επομένως, για κάθε πρώτο p και κάθε $\alpha \geq 0$,

$$a_D(p^\alpha) = \sum_{j=0}^{\alpha} \chi_D(p)^j.$$

Επειδή και οι δύο συναρτήσεις είναι πολλαπλασιαστικές, συμπεραίνουμε ότι για κάθε n,

$$a_D(n) = \prod_{p^\alpha \| n} \left(\sum_{j=0}^{\alpha} \chi_D(p)^j \right) = \sum_{d|n} \chi_D(d).$$

Άρα

$$r_D(n) = w_D a_D(n) = w_D \sum_{d|n} \chi_D(d).$$

□

12 Η αναλυτική ασυμπτωτική

Λήμμα 12.1. *Αν*

$$A_D(x) := \sum_{n \leq x} \chi_D(n),$$

τότε

$$A_D(x) = O_D(1).$$

Συνεπώς η σειρά

$$L(1, \chi_D) = \sum_{n=1}^{\infty} \frac{\chi_D(n)}{n}$$

συγκλίνει.

Απόδειξη. Επειδή χ_D είναι μη κύριος Dirichlet χαρακτήρας modulo $|D|$, έχουμε

$$\sum_{a=1}^{|D|} \chi_D(a) = 0.$$

Πράγματι, αν u είναι μια ακέραια κλάση modulo $|D|$ με $\chi_D(u) \neq 1$, τότε

$$\sum_{a \bmod |D|} \chi_D(a) = \sum_{a \bmod |D|} \chi_D(ua) = \chi_D(u) \sum_{a \bmod |D|} \chi_D(a),$$

οπότε το άθροισμα είναι 0.

Άρα πάνω σε κάθε πλήρη περίοδο μήκους $|D|$, το άθροισμα της χ_D είναι μηδέν, και από αυτό αμέσως έπεται ότι

$$A_D(x) = O_D(1).$$

Για τη σύγκλιση του $L(1, \chi_D)$, εφαρμόζουμε μερική ολοκλήρωση (summation by parts):

$$\sum_{n \leq X} \frac{\chi_D(n)}{n} = \frac{A_D(X)}{X} + \int_1^X \frac{A_D(t)}{t^2}\, dt.$$

Επειδή $A_D(t) = O_D(1)$, το δεξί μέλος συγκλίνει όταν $X \to \infty$. Άρα η σειρά $L(1, \chi_D)$ συγκλίνει. □

Πρόταση 12.2. *Ισχύει*

$$\sum_{n \leq X} r_D(n) = w_D\, L(1, \chi_D)\, X + O_D(\sqrt{X}).$$

Απόδειξη. Από την Πρόταση 11.9,

$$\sum_{n \leq X} r_D(n) = w_D \sum_{n \leq X} \sum_{d \mid n} \chi_D(d).$$

Θέτουμε

$$a_D(n) := \sum_{d \mid n} \chi_D(d), \qquad S_D(X) := \sum_{n \leq X} a_D(n).$$

Τότε

$$\sum_{n \leq X} r_D(n) = w_D S_D(X).$$

Άρα αρκεί να δείξουμε ότι

$$S_D(X) = L(1, \chi_D)\, X + O_D(\sqrt{X}).$$

Γράφουμε

$$S_D(X) = \sum_{dm \leq X} \chi_D(d).$$

Θέτουμε $Y = \lfloor \sqrt{X} \rfloor$ και θα χρησιμοποιήσουμε την μέθοδο της υπερβολής του Dirichlet. Χωρίζουμε τα ζεύγη (d, m) με $dm \leq X$ σε εκείνα με $d \leq Y$ και σε εκείνα με $d > Y$. Έτσι

$$S_D(X) = \sum_{\substack{dm \leq X \\ d \leq Y}} \chi_D(d) + \sum_{\substack{dm \leq X \\ d > Y}} \chi_D(d).$$

Ο πρώτος όρος γράφεται αμέσως

$$\sum_{\substack{dm\le X\\ d\le Y}}\chi_D(d)=\sum_{d\le Y}\chi_D(d)\Big\lfloor\frac{X}{d}\Big\rfloor.$$

Για τον δεύτερο όρο, από τις ανισότητες $d>Y$ και $dm\le X$ έπεται ότι $m<X/Y$, οπότε

$$\sum_{\substack{dm\le X\\ d>Y}}\chi_D(d)=\sum_{m<X/Y}\ \sum_{Y<d\le X/m}\chi_D(d).$$

Αν γράψουμε

$$A_D(t):=\sum_{n\le t}\chi_D(n),$$

τότε

$$\sum_{Y<d\le X/m}\chi_D(d)=A_D\Big(\frac{X}{m}\Big)-A_D(Y),$$

και έτσι

$$S_D(X)=\sum_{d\le Y}\chi_D(d)\Big\lfloor\frac{X}{d}\Big\rfloor+\sum_{m<X/Y}A_D\Big(\frac{X}{m}\Big)-A_D(Y)\Big\lfloor\frac{X}{Y}\Big\rfloor.$$

Στη συνέχεια χρησιμοποιούμε τη μέθοδο άθροισης του Abel για να συγκρίνουμε το

$$\sum_{d\le Y}\frac{\chi_D(d)}{d}$$

με τη σειρά

$$L(1,\chi_D)=\sum_{n=1}^{\infty}\frac{\chi_D(n)}{n}.$$

Εφόσον $A_D(t)=O_D(1)$, για κάθε $Z>Y$ έχουμε

$$\sum_{Y<n\le Z}\frac{\chi_D(n)}{n}=\frac{A_D(Z)}{Z}-\frac{A_D(Y)}{Y}+\int_Y^Z\frac{A_D(t)}{t^2}\,dt.$$

Αφήνοντας $Z\to\infty$, παίρνουμε

$$\sum_{n>Y}\frac{\chi_D(n)}{n}=-\frac{A_D(Y)}{Y}+\int_Y^{\infty}\frac{A_D(t)}{t^2}\,dt.$$

Επειδή $A_D(t)=O_D(1)$, το δεξί μέλος είναι

$$O_D\Big(\frac{1}{Y}\Big).$$

Άρα

$$\sum_{d\le Y}\frac{\chi_D(d)}{d}=L(1,\chi_D)+O_D\Big(\frac{1}{Y}\Big).$$

Με $Y=\lfloor\sqrt{X}\rfloor$, αυτό γίνεται

$$\sum_{d\le Y}\frac{\chi_D(d)}{d}=L(1,\chi_D)+O_D\Big(\frac{1}{\sqrt{X}}\Big).$$

Βάζοντας το στην προηγούμενη σχέση, παίρνουμε

$$S_D(X) = L(1,\chi_D)\,X + O_D(\sqrt{X}).$$

Πολλαπλασιάζοντας με w_D, καταλήγουμε

$$\sum_{n\le X} r_D(n) = w_D\,L(1,\chi_D)\,X + O_D(\sqrt{X}).$$

□

13 Η γεωμετρική ασυμπτωτική

Λήμμα 13.1. *Για κάθε $t>0$ υπάρχει σταθερά $C_t>0$ τέτοια ώστε για κάθε φραγμένο κυρτό σύνολο $\Omega\subset\mathbb{R}^2$ να ισχύει*

$$\text{area}\big(\{x\in\mathbb{R}^2 : \text{dist}(x,\partial\Omega)\le t\}\big) \le C_t\big(L(\partial\Omega)+1\big).$$

Μάλιστα, μπορεί κανείς να πάρει

$$\text{area}\big(\{x : \text{dist}(x,\partial\Omega)\le t\}\big) \le 2t\,L(\partial\Omega)+\pi t^2.$$

Απόδειξη. Θα δώσουμε πρώτα την απόδειξη όταν $\Omega=P$ είναι κυρτό πολύγωνο με πλευρές μήκους

$$\ell_1,\dots,\ell_m, \qquad L(\partial P)=\ell_1+\cdots+\ell_m.$$

Εξωτερική ζώνη. Το σύνολο

$$\{x\notin P : \text{dist}(x,P)\le t\}$$

αποτελείται από:

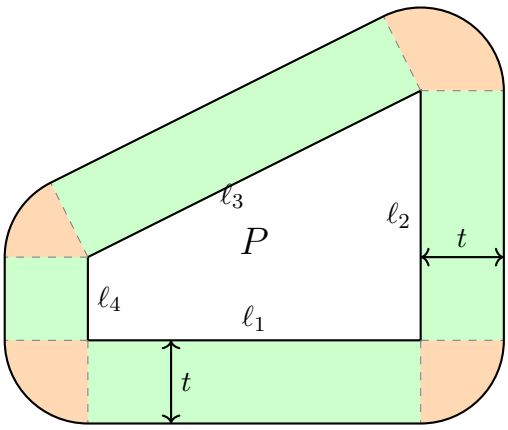
- ορθογώνιες λωρίδες πλάτους t κατά μήκος κάθε πλευράς, συνολικού εμβαδού
$$t(\ell_1+\cdots+\ell_m)=t\,L(\partial P),$$
- και κυκλικούς τομείς ακτίνας t γύρω από τις κορυφές.

Επειδή το άθροισμα των εξωτερικών γωνιών ενός κυρτού πολυγώνου είναι 2π, το συνολικό εμβαδόν των τομέων είναι

$$\frac{2\pi}{2}t^2=\pi t^2.$$

Άρα

$$\text{area}\big(\{x\notin P : \text{dist}(x,P)\le t\}\big) \le t\,L(\partial P)+\pi t^2.$$



Σχήμα 1: Εξωτερική ζώνη (Ορθογώνιες λωρίδες & Κυκλικοί τομείς)

Εσωτερική ζώνη. Το σύνολο

$$\{x \in P : \operatorname{dist}(x, \partial P) \le t\}$$

περιέχεται στην ένωση των εσωτερικών λωρίδων πλάτους t κατά μήκος των πλευρών του P. Το άθροισμα των εμβαδών αυτών των λωρίδων είναι

$$t(\ell_1 + \cdots + \ell_m) = t\, L(\partial P).$$

Άρα

$$\operatorname{area}\big(\{x \in P : \operatorname{dist}(x, \partial P) \le t\}\big) \le t\, L(\partial P).$$

Προσθέτοντας τις δύο εκτιμήσεις, παίρνουμε

$$\operatorname{area}\big(\{x : \operatorname{dist}(x, \partial P) \le t\}\big) \le 2t\, L(\partial P) + \pi t^2.$$

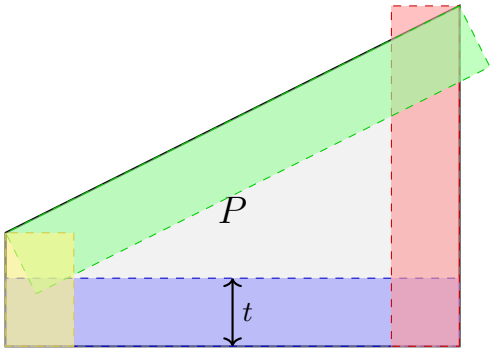
Για γενικό φραγμένο κυρτό Ω, παίρνουμε μια ακολουθία κυρτών πολυγώνων P_ν που συγκλίνουν στον Ω κατά Hausdorff και τέτοια ώστε

$$L(\partial P_\nu) \to L(\partial \Omega), \qquad \operatorname{area}(P_\nu) \to \operatorname{area}(\Omega).$$

Περνώντας στο όριο στην παραπάνω ανισότητα για τα P_ν, παίρνουμε

$$\operatorname{area}\big(\{x : \operatorname{dist}(x, \partial \Omega) \le t\}\big) \le 2t\, L(\partial \Omega) + \pi t^2.$$

Αυτό ολοκληρώνει την απόδειξη. □



Σχήμα 2: Εσωτερική ζώνη (Επικάλυψη εσωτερικών λωρίδων)

Λήμμα 13.2. *Υπάρχει απόλυτη σταθερά $C > 0$ τέτοια ώστε για κάθε φραγμένο κυρτό σύνολο $\Omega \subset \mathbb{R}^2$ να ισχύει*

$$\big|\#(\Omega \cap \mathbb{Z}^2) - \operatorname{area}(\Omega)\big| \le C\big(L(\partial \Omega) + 1\big).$$

Απόδειξη. Θέτουμε

$$Q = \left[-\frac{1}{2}, \frac{1}{2}\right]^2.$$

Άνω φράγμα. Για κάθε $z \in \Omega \cap \mathbb{Z}^2$, το τετράγωνο $z + Q$ έχει εμβαδόν 1, και τα τετράγωνα αυτά είναι ξένα. Επίσης

$$z + Q \subset \Omega + Q.$$

Άρα

$$\#(\Omega \cap \mathbb{Z}^2) \le \operatorname{area}(\Omega + Q).$$

Τώρα, κάθε σημείο του $(\Omega + Q) \setminus \Omega$ απέχει από το $\partial\Omega$ το πολύ $\sqrt{2}/2$, αφού

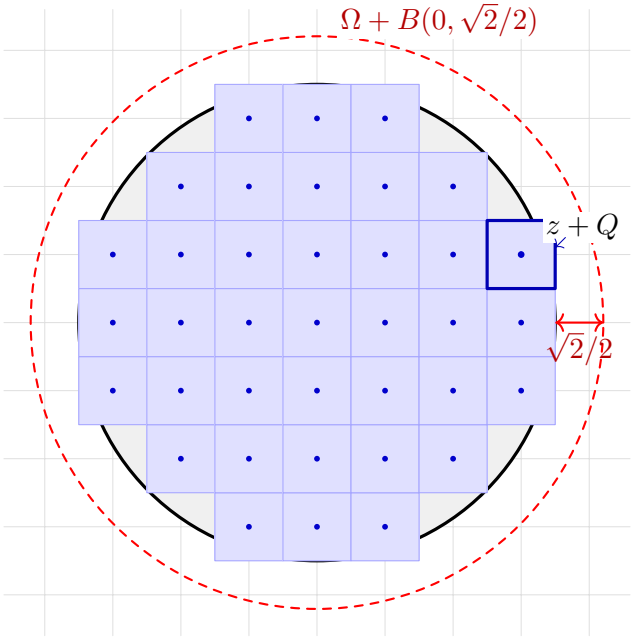
$$Q \subset B(0, \sqrt{2}/2).$$

Επομένως

$$\text{area}(\Omega + Q) \leq \text{area}(\Omega) + \text{area}\big(\{x : \text{dist}(x, \partial\Omega) \leq \sqrt{2}/2\}\big).$$

Από το Λήμμα 13.1, παίρνουμε

$$\#(\Omega \cap \mathbb{Z}^2) \leq \text{area}(\Omega) + C_1\big(L(\partial\Omega) + 1\big).$$



Σχήμα 3: Για κάθε $z \in \Omega \cap \mathbb{Z}^2$, το τετράγωνο $z+Q$ περιέχεται στο $\Omega+Q$. Επειδή $Q \subset B(0, \sqrt{2}/2)$, έχουμε $\Omega + Q \subset \Omega + B(0, \sqrt{2}/2)$.

Κάτω φράγμα. Θέτουμε

$$\Omega^\circ_{\sqrt{2}} := \{x \in \Omega : \text{dist}(x, \partial\Omega) > \sqrt{2}\}.$$

Θα δείξουμε ότι

$$\text{area}(\Omega^\circ_{\sqrt{2}}) \leq \#(\Omega \cap \mathbb{Z}^2).$$

Πράγματι, εκτός από τα σημεία που ανήκουν στα σύνορα των τετραγώνων του πλέγματος (σύνολο μέτρου μηδέν), κάθε σημείο $x \in \mathbb{R}^2$ ανήκει σε μοναδικό τετράγωνο της μορφής $z + Q$, με $z \in \mathbb{Z}^2$. Αν τώρα $x \in \Omega^\circ_{\sqrt{2}}$ και $x \in z + Q$, τότε για κάθε $y \in z + Q$ έχουμε

$$|y - x| \leq \sqrt{2},$$

επειδή η διάμετρος του Q είναι $\sqrt{2}$. Άρα

$$y \in \Omega.$$

Επομένως

$$z + Q \subset \Omega.$$

Άρα τα σημεία του $\Omega^\circ_{\sqrt{2}}$ καλύπτονται από τετράγωνα $z + Q$ με $z \in \Omega \cap \mathbb{Z}^2$. Τα τετράγωνα αυτά είναι ξένα και έχουν εμβαδόν 1, οπότε

$$\text{area}(\Omega^\circ_{\sqrt{2}}) \leq \#(\Omega \cap \mathbb{Z}^2).$$

Από την άλλη,

$$\Omega \setminus \Omega^{\circ}_{\sqrt{2}} \subset \{x : \operatorname{dist}(x, \partial\Omega) \leq \sqrt{2}\},$$

οπότε, με το Λήμμα 13.1,

$$\operatorname{area}(\Omega) - \operatorname{area}(\Omega^{\circ}_{\sqrt{2}}) \leq C_2\big(L(\partial\Omega) + 1\big).$$

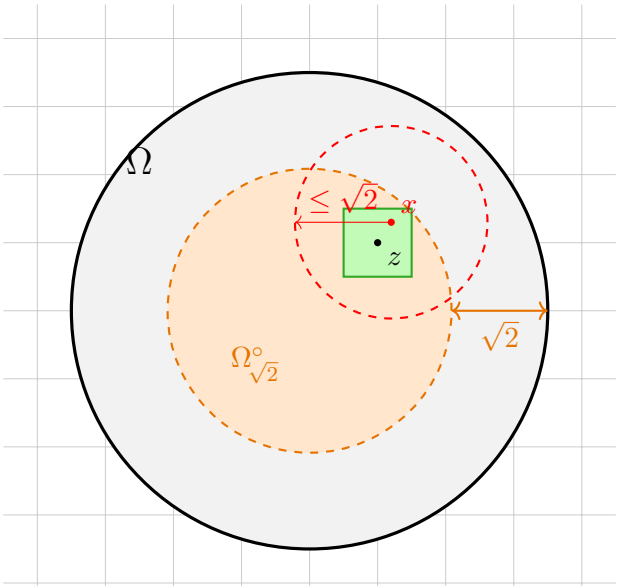
Άρα

$$\#(\Omega \cap \mathbb{Z}^2) \geq \operatorname{area}(\Omega) - C_2\big(L(\partial\Omega) + 1\big).$$

Συνδυάζοντας τα δύο φράγματα, παίρνουμε

$$\big|\#(\Omega \cap \mathbb{Z}^2) - \operatorname{area}(\Omega)\big| \leq C\big(L(\partial\Omega) + 1\big),$$

για κάποια απόλυτη σταθερά C. □



Σχήμα 2: Αν $x \in \Omega^{\circ}_{\sqrt{2}}$, ολόκληρο το $z + Q$ περιέχεται στο Ω

Πόρισμα 13.3. *Για τις ελλείψεις*

$$E_j(X) := \{(x, y) \in \mathbb{R}^2 : \ f_j(x, y) \leq X\},$$

ισχύει

$$\#\big(E_j(X) \cap \mathbb{Z}^2\big) = \operatorname{area}(E_j(X)) + O_D(\sqrt{X}).$$

Απόδειξη. Το $E_j(X)$ είναι έλλειψη. Από τον τύπο του εμβαδού ξέρουμε ότι

$$\operatorname{area}(E_j(X)) = \frac{2\pi}{\sqrt{|D|}}\, X.$$

Επιπλέον, επειδή το $E_j(X)$ είναι ομοιόθετο του $E_j(1)$ με λόγο $\sqrt{X}$, το μήκος του συνόρου του ικανοποιεί

$$L(\partial E_j(X)) = O_D(\sqrt{X}).$$

Εφαρμόζοντας το Λήμμα 13.2 με $\Omega = E_j(X)$, παίρνουμε

$$\#\big(E_j(X) \cap \mathbb{Z}^2\big) = \operatorname{area}(E_j(X)) + O_D(\sqrt{X}).$$

□

Λήμμα 13.4. *Για κάθε j,*

$$\operatorname{area}(E_j(X)) = \frac{2\pi}{\sqrt{|D|}}\, X.$$

Απόδειξη. Η μορφή f_j γράφεται ως

$$f_j(x,y) = \begin{pmatrix} x & y \end{pmatrix} Q_j \begin{pmatrix} x \\ y \end{pmatrix}, \qquad Q_j = \begin{pmatrix} a_j & b_j/2 \\ b_j/2 & c_j \end{pmatrix}.$$

Εφόσον f_j είναι θετικά ορισμένη, ο Q_j είναι συμμετρικός θετικά ορισμένος. Επιπλέον

$$\det(Q_j) = a_j c_j - \frac{b_j^2}{4} = \frac{4a_jc_j - b_j^2}{4} = \frac{|D|}{4}.$$

Η περιοχή

$$E_j(X) = \{v \in \mathbb{R}^2 :\ v^T Q_j v \le X\}$$

είναι η εικόνα του ευκλείδειου δίσκου ακτίνας $\sqrt{X}$ μέσω της γραμμικής απεικόνισης $Q_j^{-1/2}$. Άρα

$$\operatorname{area}(E_j(X)) = \frac{\pi X}{\sqrt{\det(Q_j)}} = \frac{\pi X}{\sqrt{|D|/4}} = \frac{2\pi}{\sqrt{|D|}}\, X.$$

□

Πρόταση 13.5. *Ισχύει*

$$\sum_{n \le X} r_D(n) = \frac{2\pi h(D)}{\sqrt{|D|}}\, X + O_D(\sqrt{X}).$$

Απόδειξη. Για κάθε j, θέτουμε

$$N_j(X) := \#\big(E_j(X) \cap \mathbb{Z}^2\big).$$

Τότε

$$N_j(X) = 1 + \sum_{1 \le n \le X} \#\{(x,y) \in \mathbb{Z}^2 :\ f_j(x,y) = n\},$$

διότι το σημείο $(0,0)$ συμβάλλει ακριβώς μία φορά και δίνει την τιμή 0. Αθροίζοντας ως προς j, παίρνουμε

$$\sum_{j=1}^{h(D)} N_j(X) = h(D) + \sum_{n \le X} r_D(n).$$

Άρα

$$\sum_{n \le X} r_D(n) = \sum_{j=1}^{h(D)} N_j(X) - h(D).$$

Από το Λήμμα ?? και το Λήμμα 13.4,

$$N_j(X) = \frac{2\pi}{\sqrt{|D|}}\, X + O_D(\sqrt{X}).$$

Αθροίζοντας για $j = 1, \dots, h(D)$, παίρνουμε

$$\sum_{j=1}^{h(D)} N_j(X) = \frac{2\pi h(D)}{\sqrt{|D|}}\, X + O_D(\sqrt{X}),$$

διότι $h(D)$ είναι σταθερός ως προς X. Επομένως

$$\sum_{n \le X} r_D(n) = \frac{2\pi h(D)}{\sqrt{|D|}}\, X + O_D(\sqrt{X}).$$

□

14 Απόδειξη της formula του Dirichlet

Απόδειξη του Θεωρήματος 9.14. Από την αναλυτική ασυμπτωτική της Πρότασης 12.2, έχουμε

$$\sum_{n \le X} r_D(n) = w_D \, L(1, \chi_D) \, X + O_D(\sqrt{X}).$$

Από τη γεωμετρική ασυμπτωτική της Πρότασης 13.5, έχουμε επίσης

$$\sum_{n \le X} r_D(n) = \frac{2\pi h(D)}{\sqrt{|D|}} \, X + O_D(\sqrt{X}).$$

Αφαιρώντας τις δύο σχέσεις, παίρνουμε

$$\left(w_D \, L(1, \chi_D) - \frac{2\pi h(D)}{\sqrt{|D|}} \right) X = O_D(\sqrt{X}).$$

Διαιρώντας με X και αφήνοντας $X \to \infty$, καταλήγουμε

$$w_D \, L(1, \chi_D) = \frac{2\pi h(D)}{\sqrt{|D|}}.$$

Άρα

$$L(1, \chi_D) = \frac{2\pi}{w_D \sqrt{|D|}} \, h(D).$$

Αυτό ακριβώς είναι η formula του Dirichlet class number για αρνητική περιττή θεμελιώδη διακρίνουσα. □

Ορισμός 14.1. Έστω $D > 0$ θεμελιώδης διακρίνουσα. Γράφουμε $h(D)$ για τον αριθμό των proper κλάσεων πρωταρχικών αόριστων δυαδικών τετραγωνικών μορφών διακρίνουσας D. Από κάθε proper κλάση διαλέγουμε έναν reduced αντιπρόσωπο

$$f_j = [a_j, b_j, c_j], \qquad b_j^2 - 4a_j c_j = D, \qquad a_j > 0 > c_j, \qquad j = 1, \dots, h(D).$$

Για μια τέτοια μορφή $f = [a, b, c]$, θέτουμε

$$\alpha = \frac{-b + \sqrt{D}}{2a}, \qquad \beta = \frac{-b - \sqrt{D}}{2a},$$

ώστε

$$f(x, y) = a(x - \alpha y)(x - \beta y).$$

Λήμμα 14.2. *Έστω $f = [a, b, c]$ πρωταρχική αόριστη μορφή διακρίνουσας $D > 0$. Θέτουμε*

$$S_f = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}, \qquad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad A_f = J S_f = \begin{pmatrix} -b & -2c \\ 2a & b \end{pmatrix}.$$

Τότε:

1. $A_f^2 = D \, I_2$.
2. *Αν $U \in \mathrm{Aut}^+(f)$, τότε U αντιμετατίθεται με το A_f.*

3. Κάθε $U \in \mathrm{Aut}^+(f)$ *γράφεται μοναδικά με τη μορφή*

$$U = \begin{pmatrix} \dfrac{t-bu}{2} & -cu \\ au & \dfrac{t+bu}{2} \end{pmatrix}$$

για κάποιους ακεραίους t, u *που ικανοποιούν*

$$t^2 - Du^2 = 4.$$

Αντίστροφα, κάθε τέτοιος πίνακας ανήκει στην $\mathrm{Aut}^+(f)$.

Επιπλέον, αν $U_f \neq I_2$ *είναι ο proper αυτομορφισμός της* f *με το ελάχιστο ίχνος* > 2*, τότε*

$$U_f = \begin{pmatrix} \dfrac{t_0-bu_0}{2} & -cu_0 \\ au_0 & \dfrac{t_0+bu_0}{2} \end{pmatrix}$$

για κάποιους ακεραίους t_0, u_0 *με* $u_0 > 0$*, και αν θέσουμε*

$$\varepsilon_D := \frac{t_0 + u_0\sqrt{D}}{2} > 1,$$

τότε οι ιδιοτιμές του U_f *είναι* ε_D *και* ε_D^{-1}.

Απόδειξη. Οι αποδείξεις των (1), (2), (3) είναι ακριβώς οι ίδιες όπως στην ορισμένη περίπτωση $D < 0$, αφού χρησιμοποιούν μόνο την ταυτότητα

$$f(x,y) = \frac{1}{2}(x,y)S_f\begin{pmatrix} x \\ y \end{pmatrix},$$

τη σχέση $U^t S_f U = S_f$, και το γεγονός ότι κάθε ακέραιος πίνακας που αντιμετατίθεται με το A_f είναι της μορφής $xI_2 + yA_f$.

Για την τελευταία πρόταση, έστω

$$U_f = \begin{pmatrix} \dfrac{t_0-bu_0}{2} & -cu_0 \\ au_0 & \dfrac{t_0+bu_0}{2} \end{pmatrix}$$

ο proper αυτομορφισμός με το μικρότερο ίχνος > 2. Εφόσον $\det U_f = 1$, οι ιδιοτιμές του U_f είναι οι ρίζες του

$$\lambda^2 - t_0\lambda + 1 = 0.$$

Χρησιμοποιώντας ότι $t_0^2 - Du_0^2 = 4$, παίρνουμε

$$\lambda = \frac{t_0 \pm \sqrt{t_0^2 - 4}}{2} = \frac{t_0 \pm u_0\sqrt{D}}{2}.$$

Άρα η μεγαλύτερη ιδιοτιμή είναι

$$\varepsilon_D = \frac{t_0 + u_0\sqrt{D}}{2} > 1,$$

και η άλλη είναι ε_D^{-1}. □

Λήμμα 14.3. *Έστω $f = [a, b, c]$ reduced πρωταρχική αόριστη μορφή διακρίνουσας $D > 0$, και*

$$\alpha = \frac{-b + \sqrt{D}}{2a}, \qquad \beta = \frac{-b - \sqrt{D}}{2a}.$$

Θέτουμε

$$\xi = x - \alpha y, \qquad \eta = x - \beta y.$$

Τότε ο θεμελιώδης proper αυτομορφισμός U_f δρα ως

$$(\xi, \eta) \longmapsto \big(\varepsilon_D^{-1}\xi,\ \varepsilon_D\,\eta\big).$$

Συνεπώς,

$$\frac{\eta}{\xi} \longmapsto \varepsilon_D^2 \frac{\eta}{\xi}.$$

Απόδειξη. Γράφουμε

$$U_f = \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} \dfrac{t_0 - bu_0}{2} & -cu_0 \\ au_0 & \dfrac{t_0 + bu_0}{2} \end{pmatrix}.$$

Αν

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = U_f \begin{pmatrix} x \\ y \end{pmatrix},$$

τότε

$$x' - \alpha y' = (p - \alpha r)x + (q - \alpha s)y.$$

Επειδή η α είναι ρίζα της

$$aX^2 + bX + c = 0,$$

έχουμε

$$q - \alpha s = -\alpha(p - \alpha r),$$

οπότε

$$x' - \alpha y' = (p - \alpha r)(x - \alpha y).$$

Τώρα

$$p - \alpha r = \frac{t_0 - bu_0}{2} - au_0 \frac{-b + \sqrt{D}}{2a} = \frac{t_0 - u_0\sqrt{D}}{2} = \varepsilon_D^{-1}.$$

Άρα

$$\xi' = \varepsilon_D^{-1}\xi.$$

Ομοίως,

$$\eta' = \varepsilon_D \eta.$$

Ο μετασχηματισμός του η/ξ ακολουθεί αμέσως. □

Ορισμός 14.4. Έστω $f = [a, b, c]$ reduced πρωταρχική αόριστη μορφή διακρίνουσας $D > 0$, και

$$\alpha = \frac{-b + \sqrt{D}}{2a}, \qquad \beta = \frac{-b - \sqrt{D}}{2a}.$$

Μια λύση $(x, y) \in \mathbb{Z}^2$ της εξίσωσης $f(x, y) = n > 0$ λέγεται *κύρια αναπαράσταση* αν

$$x - \alpha y > 0$$

και

$$1 \le \frac{x - \beta y}{x - \alpha y} < \varepsilon_D^2.$$

Λήμμα 14.5. *Έστω $f = [a, b, c]$ reduced πρωταρχική αόριστη μορφή διακρίνουσας $D > 0$, και $n \geq 1$. Τότε κάθε proper $\mathrm{Aut}^+(f)$-τροχιά στο*

$$\{(x, y) \in \mathbb{Z}^2 : \ f(x, y) = n\}$$

περιέχει ακριβώς ένα κύριο στοιχείο. Το ίδιο ισχύει και αν περιοριστούμε στις primitive λύσεις.

Απόδειξη. Έστω (x, y) με $f(x, y) = n > 0$, και θέτουμε

$$\xi = x - \alpha y, \qquad \eta = x - \beta y.$$

Αφού

$$f(x, y) = a\,\xi\eta > 0,$$

οι ξ, η έχουν το ίδιο πρόσημο. Επειδή $-I_2 \in \mathrm{Aut}^+(f)$, αντικαθιστώντας αν χρειάζεται το (x, y) με $(-x, -y)$, μπορούμε να υποθέσουμε ότι $\xi > 0$, άρα και $\eta > 0$.

Θέτουμε

$$r = \frac{\eta}{\xi} > 0.$$

Από το Λήμμα 14.3, η δράση του U_f στέλνει το r στο $\varepsilon_D^2 r$. Επομένως υπάρχει μοναδικός ακέραιος m τέτοιος ώστε

$$1 \leq \varepsilon_D^{2m} r < \varepsilon_D^2.$$

Τότε το $U_f^m(x, y)$ είναι κύριο.

Για τη μοναδικότητα, αν και τα δύο $U_f^m(x, y)$, $U_f^{m'}(x, y)$ είναι κύρια, τότε

$$\varepsilon_D^{2m} r, \ \varepsilon_D^{2m'} r \in [1, \varepsilon_D^2).$$

Διαιρώντας, παίρνουμε

$$\varepsilon_D^{2(m-m')} \in (\varepsilon_D^{-2}, \varepsilon_D^2).$$

Η μόνη ακέραια δύναμη του ε_D^2 μέσα σε αυτό το διάστημα είναι το 1, άρα $m = m'$.

Η τελευταία πρόταση ακολουθεί επειδή κάθε proper αυτομορφισμός έχει ορίζουσα 1, άρα διατηρεί το $\gcd(x, y)$. □

Ορισμός 14.6. Για $n \geq 1$, ορίζουμε

$$r_D(n) := \sum_{j=1}^{h(D)} \#\{(x, y) \in \mathbb{Z}^2 : \ f_j(x, y) = n, \ (x, y) \text{ είναι κύριο}\},$$

και

$$r_D^*(n) := \sum_{j=1}^{h(D)} \#\{(x, y) \in \mathbb{Z}^2 : \ f_j(x, y) = n, \ \gcd(x, y) = 1, \ (x, y) \text{ είναι κύριο}\}.$$

Ορισμός 14.7. Για $n \geq 1$, θέτουμε

$$\rho_D(n) := \#\{\beta \pmod{2n} : \ \beta^2 \equiv D \pmod{4n}\}.$$

Λήμμα 14.8. *Για κάθε $n \geq 1$,*

$$r_D^*(n) = \rho_D(n).$$

Απόδειξη. Το αλγεβρικό μέρος της αντιστοιχίας ανάμεσα σε primitive αναπαραστάσεις και ρίζες της

$$\beta^2 \equiv D \pmod{4n}$$

είναι ακριβώς το ίδιο όπως στην περίπτωση $D < 0$, οπότε θυμίζουμε μόνο τα ουσιώδη σημεία.

Αν (x, y) είναι primitive λύση της $f_j(x, y) = n$, επιλέγουμε $\gamma, \delta \in \mathbb{Z}$ με

$$x\delta - y\gamma = 1,$$

και θέτουμε

$$M = \begin{pmatrix} x & \gamma \\ y & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Τότε

$$f_j \circ M = [n, \beta, \gamma']$$

για κάποιους ακεραίους β, γ', και επειδή η διακρίνουσα διατηρείται,

$$\beta^2 \equiv D \pmod{4n}.$$

Επιπλέον, η κλάση του $\beta \pmod{2n}$ εξαρτάται μόνο από την proper κλάση της primitive αναπαράστασης.

Αντίστροφα, αν

$$\beta^2 \equiv D \pmod{4n},$$

τότε

$$[n, \beta, \tfrac{\beta^2 - D}{4n}]$$

είναι πρωταρχική μορφή διακρίνουσας D. Περνώντας στην reduced proper κλάση της, παίρνουμε μια primitive proper τροχιά λύσεων της $f_j(x, y) = n$.

Στην αρνητική περίπτωση $D < 0$, κάθε proper τροχιά συνεισφέρει w_D primitive αναπαραστάσεις. Στην παρούσα αόριστη περίπτωση, από το Λήμμα 14.5, κάθε primitive proper τροχιά περιέχει ακριβώς έναν κύριο εκπρόσωπο. Άρα η παραπάνω αντιστοιχία είναι μία προς μία, και συνεπώς

$$r_D^*(n) = \rho_D(n).$$

□

Λήμμα 14.9. *Η συνάρτηση ρ_D είναι πολλαπλασιαστική.*

Απόδειξη. Ακριβώς όπως για $D < 0$, αυτό ακολουθεί από το Κινέζικο Θεώρημα Υπολοίπων. □

Πρόταση 14.10. *Για κάθε $n \geq 1$,*

$$r_D(n) = \sum_{d \mid n} \chi_D(d).$$

Απόδειξη. Η απόδειξη είναι η ίδια όπως για $D < 0$, με μόνη διαφορά ότι το Λήμμα 14.8 δίνει

$$r_D^*(n) = \rho_D(n)$$

αντί για

$$r_D^*(n) = w_D\, \rho_D(n).$$

Άρα ο παράγοντας w_D εξαφανίζεται σε όλη τη συνέχεια του επιχειρήματος, και παίρνουμε

$$r_D(n) = \sum_{d \mid n} \chi_D(d).$$

□

Πρόταση 14.11. *Ισχύει*

$$\sum_{n\le X} r_D(n) = L(1,\chi_D)\,X + O_D(\sqrt{X}).$$

Απόδειξη. Αυτό αποδεικνύεται ακριβώς όπως στην περίπτωση $D<0$, ξεκινώντας από τον τύπο

$$r_D(n) = \sum_{d\mid n} \chi_D(d),$$

και αθροίζοντας για $n \le X$. □

Λήμμα 14.12. *Υπάρχει απόλυτη σταθερά $C>0$ τέτοια ώστε για κάθε φραγμένο χωρίο $\Omega\subset\mathbb{R}^2$ του οποίου το σύνορο είναι ένωση πεπερασμένου πλήθους ευθυγράμμων τμημάτων και C^1-τόξων να ισχύει*

$$\big|\#(\Omega\cap\mathbb{Z}^2) - \mathrm{area}(\Omega)\big| \le C\big(L(\partial\Omega)+1\big).$$

Απόδειξη. Θέτουμε

$$Q = \left[-\frac{1}{2},\frac{1}{2}\right]^2.$$

Όπως και στην κυρτή περίπτωση, η ένωση των lattice squares $z+Q$, όπου $z\in\Omega\cap\mathbb{Z}^2$, περιέχεται στο $\Omega+Q$, και τα τετράγωνα αυτά είναι ξένα και όλα έχουν εμβαδόν 1. Ομοίως, κάθε lattice square που τέμνει και το Ω και το συμπλήρωμά του περιέχεται στη 1-γειτονιά του $\partial\Omega$. Άρα η διαφορά

$$\big|\#(\Omega\cap\mathbb{Z}^2) - \mathrm{area}(\Omega)\big|$$

φράσσεται από σταθερά επί το εμβαδόν της 1-γειτονιάς του $\partial\Omega$.

Τώρα, η 1-γειτονιά ενός ευθυγράμμου τμήματος μήκους ℓ έχει εμβαδόν $\ll \ell+1$, και το ίδιο ισχύει και για ένα C^1-τόξο μήκους ℓ. Επειδή το $\partial\Omega$ είναι ένωση πεπερασμένου πλήθους τέτοιων κομματιών, το συνολικό εμβαδόν της 1-γειτονιάς του $\partial\Omega$ είναι

$$\ll L(\partial\Omega)+1.$$

Αυτό δίνει το ζητούμενο. □

Πρόταση 14.13. *Ισχύει*

$$\sum_{n\le X} r_D(n) = \frac{h(D)\log(\varepsilon_D)}{\sqrt{D}}\,X + O_D(\sqrt{X}).$$

Απόδειξη. Για κάθε reduced αντιπρόσωπο

$$f_j = [a_j,b_j,c_j],$$

θέτουμε

$$\alpha_j = \frac{-b_j+\sqrt{D}}{2a_j}, \qquad \beta_j = \frac{-b_j-\sqrt{D}}{2a_j},$$

και ορίζουμε το χωρίο

$$\Omega_j(X) := \Big\{(x,y)\in\mathbb{R}^2 : 0<f_j(x,y)\le X,\ x-\alpha_j y>0,\ 1\le \frac{x-\beta_j y}{x-\alpha_j y} < \varepsilon_D^2\Big\}.$$

Από τον ορισμό των κύριων αναπαραστάσεων, τα lattice points της $\Omega_j(X)$ είναι ακριβώς οι κύριες αναπαραστάσεις όλων των ακεραίων $n\le X$ από τη μορφή f_j. Επομένως

$$\sum_{n\le X} r_D(n) = \sum_{j=1}^{h(D)} \#(\Omega_j(X)\cap\mathbb{Z}^2).$$

Θα δείξουμε ότι, ομοιόμορφα ως προς j,

$$\#(\Omega_j(X)\cap\mathbb{Z}^2)=\frac{\log(\varepsilon_D)}{\sqrt{D}}\,X+O_D(\sqrt{X}).$$

Αθροίζοντας ως προς j, θα αποδείξουμε την πρόταση.

Θέτουμε

$$\xi=x-\alpha_j y,\qquad \eta=x-\beta_j y.$$

Τότε

$$f_j(x,y)=a_j\xi\eta.$$

Ο Ιακωβιανός της αλλαγής μεταβλητών $(x,y)\mapsto(\xi,\eta)$ είναι

$$\left|\det\frac{\partial(\xi,\eta)}{\partial(x,y)}\right|=\alpha_j-\beta_j=\frac{\sqrt{D}}{a_j},$$

οπότε

$$dx\,dy=\frac{a_j}{\sqrt{D}}\,d\xi\,d\eta.$$

Στο επίπεδο (ξ,η), το χωρίο $\Omega_j(X)$ γράφεται

$$R_j(X):=\Big\{(\xi,\eta):0<a_j\xi\eta\le X,\ \xi>0,\ 1\le\eta/\xi<\varepsilon_D^2\Big\}.$$

Θέτουμε

$$r=\frac{\eta}{\xi},\qquad \text{ώστε}\qquad \eta=r\xi.$$

Τότε

$$0<a_j\xi\eta\le X\qquad\Longleftrightarrow\qquad 0<a_jr\xi^2\le X,$$

δηλαδή

$$0<\xi\le\sqrt{\frac{X}{a_jr}}.$$

Επίσης,

$$d\eta=\xi\,dr+r\,d\xi,$$

άρα

$$d\xi\,d\eta=\xi\,d\xi\,dr.$$

Έτσι

$$\text{area}(\Omega_j(X))=\frac{a_j}{\sqrt{D}}\int_1^{\varepsilon_D^2}\int_0^{\sqrt{X/(a_jr)}}\xi\,d\xi\,dr.$$

Το εσωτερικό ολοκλήρωμα είναι

$$\int_0^{\sqrt{X/(a_jr)}}\xi\,d\xi=\frac{X}{2a_jr},$$

οπότε

$$\text{area}(\Omega_j(X))=\frac{a_j}{\sqrt{D}}\int_1^{\varepsilon_D^2}\frac{X}{2a_jr}\,dr=\frac{X}{2\sqrt{D}}\int_1^{\varepsilon_D^2}\frac{dr}{r}=\frac{\log(\varepsilon_D)}{\sqrt{D}}\,X.$$

Μένει να ελέγξουμε το μήκος του συνόρου. Το σύνορο του $R_j(X)$ αποτελείται από δύο ευθύγραμμα τμήματα που βρίσκονται πάνω στις ημιευθείες

$$\eta=\xi\qquad\text{και}\qquad\eta=\varepsilon_D^2\xi,$$

καθώς και από ένα τόξο της υπερβολής

$$a_j \xi \eta = X.$$

Τα δύο ευθύγραμμα τμήματα έχουν προφανώς μήκος $O_D(\sqrt{X})$. Για το υπερβολικό τόξο, γράφουμε

$$\eta = \frac{X}{a_j \xi}, \qquad \sqrt{\frac{X}{a_j \varepsilon_D^2}} \le \xi \le \sqrt{\frac{X}{a_j}}.$$

Το μήκος του είναι λοιπόν

$$\int \sqrt{1 + \left(\frac{d\eta}{d\xi}\right)^2}\, d\xi = \int \sqrt{1 + \frac{X^2}{a_j^2 \xi^4}}\, d\xi \ll_D \sqrt{X}.$$

Άρα

$$L(\partial R_j(X)) \ll_D \sqrt{X}.$$

Η γραμμική αλλαγή μεταβλητών από (ξ, η) σε (x, y) εξαρτάται μόνο από τη μορφή f_j. Επειδή, για σταθερό D, υπάρχουν μόνο πεπερασμένες reduced κλάσεις, οι νόρμες των αντίστοιχων γραμμικών μετασχηματισμών φράσσονται μόνο ως προς το D. Επομένως

$$L(\partial \Omega_j(X)) \ll_D \sqrt{X}.$$

Εφαρμόζοντας το Λήμμα 14.12, παίρνουμε

$$\#(\Omega_j(X) \cap \mathbb{Z}^2) = \operatorname{area}(\Omega_j(X)) + O_D(\sqrt{X}) = \frac{\log(\varepsilon_D)}{\sqrt{D}}\, X + O_D(\sqrt{X}).$$

Αθροίζοντας για $j = 1, \dots, h(D)$, καταλήγουμε στο

$$\sum_{n \le X} r_D(n) = \frac{h(D) \log(\varepsilon_D)}{\sqrt{D}}\, X + O_D(\sqrt{X}).$$

□

Θεώρημα 14.14. *Για κάθε θεμελιώδη διακρίνουσα $D > 0$,*

$$L(1, \chi_D) = \frac{h(D) \log(\varepsilon_D)}{\sqrt{D}}.$$

Απόδειξη. Συγκρίνουμε τις Προτάσεις 14.11 και 14.13. □

Πόρισμα 14.15. *Έστω $d > 1$ τετραγωνοελεύθερος, και D η θεμελιώδης διακρίνουσα του $\mathbb{Q}(\sqrt{d})$, δηλαδή*

$$D = \begin{cases} d, & d \equiv 1 \pmod 4, \\ 4d, & d \equiv 2, 3 \pmod 4. \end{cases}$$

Τότε η εξίσωση Pell

$$x^2 - dy^2 = 1$$

έχει μη τετριμμένη ακέραιη λύση.

Απόδειξη. Από το Θεώρημα 14.14,

$$L(1,\chi_D)=\frac{h(D)\log(\varepsilon_D)}{\sqrt{D}}.$$

Επειδή χ_D είναι πραγματικός μη κύριος χαρακτήρας, έχουμε

$$L(1,\chi_D)>0.$$

Επίσης $h(D)\geq 1$, άρα

$$\log(\varepsilon_D)>0, \qquad \text{οπότε} \qquad \varepsilon_D>1.$$

Από το Λήμμα 14.2, αν

$$\varepsilon_D=\frac{t_0+u_0\sqrt{D}}{2},$$

τότε

$$t_0^2-Du_0^2=4$$

με $u_0\neq 0$.

Αν $D=4d$, τότε

$$t_0^2-4du_0^2=4,$$

οπότε

$$\left(\frac{t_0}{2}\right)^2-du_0^2=1,$$

και $\left(\frac{t_0}{2},u_0\right)$ είναι μη τετριμμένη λύση.

Αν $D=d$, τότε

$$t_0^2-du_0^2=4.$$

Αν t_0,u_0 είναι και οι δύο άρτιοι, τότε

$$\left(\frac{t_0}{2}\right)^2-d\left(\frac{u_0}{2}\right)^2=1,$$

και τελειώσαμε.

Υποθέτουμε τώρα ότι t_0,u_0 είναι και οι δύο περιττοί, και θέτουμε

$$\alpha=\frac{t_0+u_0\sqrt{d}}{2}.$$

Τότε

$$\alpha\cdot\frac{t_0-u_0\sqrt{d}}{2}=1,$$

άρα

$$\alpha^{-1}=\frac{t_0-u_0\sqrt{d}}{2}, \qquad \alpha+\alpha^{-1}=t_0.$$

Συνεπώς

$$\alpha^3+\alpha^{-3}=t_0^3-3t_0,$$

και

$$\alpha^3-\alpha^{-3}=(\alpha-\alpha^{-1})(\alpha^2+1+\alpha^{-2})=u_0\sqrt{d}\,(t_0^2-1).$$

Άρα

$$\alpha^3=\frac{t_0^3-3t_0}{2}+\frac{u_0(t_0^2-1)}{2}\sqrt{d}.$$

Επειδή t_0, u_0 είναι περιττοί, και οι δύο συντελεστές είναι ακέραιοι. Επομένως

$$\alpha^3 = x + y\sqrt{d}$$

για κάποιους ακεραίους x, y. Παίρνοντας νόρμες, παίρνουμε

$$x^2 - dy^2 = 1.$$

Εφόσον $\alpha > 1$, έχουμε $\alpha^3 > 1$, άρα $y \neq 0$. Επομένως αυτό δίνει μη τετριμμένη λύση της εξίσωσης Pell. □

15 Το Θεώρημα Vinogradov

Στόχος σε αυτή την παράγραφο είναι το ακόλουθο θεώρημα.

Θεώρημα 15.1 (Vinogradov). *Κάθε αρκετά μεγάλος περιττός ακέραιος γράφεται ως άθροισμα τριών πρώτων.*

Θέτουμε

$$r(n) = \sum_{k_1+k_2+k_3=n} \Lambda(k_1)\Lambda(k_2)\Lambda(k_3).$$

Η ποσότητα $r(n)$ μετρά, με βάρη, τις αναπαραστάσεις του n ως αθροίσματος τριών αριθμών, όπου καθένας είναι είτε πρώτος είτε δύναμη πρώτου.

Θεωρούμε τώρα έναν ακέραιο $N \geq 1$. Ορίζουμε τη συνάρτηση

$$S : \mathbb{R} \to \mathbb{C}, \qquad S(\alpha) = \sum_{k \leq N} \Lambda(k) e^{2\pi i k\alpha}.$$

Η S είναι 1-περιοδική, διότι για κάθε $\alpha \in \mathbb{R}$ έχουμε

$$S(\alpha+1) = \sum_{k \leq N} \Lambda(k) e^{2\pi i k(\alpha+1)} = \sum_{k \leq N} \Lambda(k) e^{2\pi i k\alpha} e^{2\pi i k} = S(\alpha).$$

Επομένως αρκεί να τη μελετούμε στο διάστημα $[0, 1]$.

Υψώνοντας στην τρίτη δύναμη, παίρνουμε

$$S(\alpha)^3 = \sum_{k_1,k_2,k_3 \leq N} \Lambda(k_1)\Lambda(k_2)\Lambda(k_3) e^{2\pi i(k_1+k_2+k_3)\alpha}.$$

Ομαδοποιώντας τους όρους ως προς το άθροισμα $n = k_1 + k_2 + k_3$, γράφουμε

$$S(\alpha)^3 = \sum_n \left(\sum_{\substack{k_1+k_2+k_3=n \\ k_1,k_2,k_3 \leq N}} \Lambda(k_1)\Lambda(k_2)\Lambda(k_3) \right) e^{2\pi i n\alpha}.$$

Θέτουμε λοιπόν

$$r(n, N) = \sum_{\substack{k_1+k_2+k_3=n \\ k_1,k_2,k_3 \leq N}} \Lambda(k_1)\Lambda(k_2)\Lambda(k_3),$$

οπότε

$$S(\alpha)^3 = \sum_n r(n, N) e^{2\pi i n\alpha}.$$

Για $n \leq N$ έχουμε προφανώς $r(n, N) = r(n)$, αφού από τη σχέση $k_1 + k_2 + k_3 = n$ με $k_i \geq 1$ έπεται αυτόματα $k_i \leq n \leq N$.

Τώρα χρησιμοποιούμε την ορθογωνιότητα των εκθετικών συναρτήσεων στο $[0,1]$:

$$\int_0^1 e^{2\pi i(m-n)\alpha}\,d\alpha = \begin{cases} 1, & \text{αν } m = n, \\ 0, & \text{αν } m \neq n. \end{cases}$$

Πολλαπλασιάζοντας την ανάπτυξη του $S(\alpha)^3$ με $e^{-2\pi in\alpha}$ και ολοκληρώνοντας από 0 έως 1, απομονώνουμε τον συντελεστή $r(n,N)$. Έτσι παίρνουμε

$$r(n,N) = \int_0^1 S(\alpha)^3 e^{-2\pi in\alpha}\,d\alpha.$$

Αυτή είναι ακριβώς η ταυτότητα που θα χρησιμοποιήσουμε στη μέθοδο του κύκλου.

Ορισμός 15.2. Για σταθερές η και B, θέτουμε

$$P = \log^B(N) \qquad \text{και} \qquad Q = \frac{N}{\log^{2B}(N)}.$$

Επίσης, για κάθε πραγματικό x, γράφουμε

$$\|x\| := \min_{m\in\mathbb{Z}} |x-m|.$$

Τότε, για κάθε $q \le P$ και b τέτοιο ώστε $1 \le b \le q$ και $(b,q)=1$, θέτουμε

$$\mathfrak{M}(b,q) = \left\{ \alpha \in [0,1) : \left\| \alpha - \frac{b}{q} \right\| \le \frac{1}{Q} \right\}.$$

Επιπλέον, θέτουμε

$$\mathfrak{M} = \bigcup_{\substack{q\le P \\ 1\le b\le q \\ (b,q)=1}} \mathfrak{M}(b,q), \qquad \mathfrak{m} = [0,1) \setminus \mathfrak{M}.$$

Τα $\mathfrak{M}(b,q)$ τα ονομάζουμε *πρωτεύοντα τόξα*, ενώ τα διαστήματα του $\mathfrak{m}$ τα ονομάζουμε *ελάσσονα τόξα*.

Λήμμα 15.3. *Το $\mathfrak{m}$ είναι μη κενό.*

Απόδειξη. Κάθε δύο πρωτεύοντα τόξα είναι ξένα. Πράγματι, αν

$$\frac{b}{q} \neq \frac{b'}{q'}$$

όπως στον ορισμό, τότε για μεγάλο N ισχύει $Q > 2P^2$, και άρα

$$\left\| \frac{b}{q} - \frac{b'}{q'} \right\| \ge \frac{1}{qq'} > \frac{2}{Q}.$$

Επομένως τα τόξα $\mathfrak{M}(b,q)$ και $\mathfrak{M}(b',q')$ δεν τέμνονται.

Άρα το $\mathfrak{M}$, που είναι η πεπερασμένη ένωση ξένων κλειστών τόξων $\mathfrak{M}(b,q)$, δεν ισούται με όλο το $[0,1)$, και συνεπώς το $\mathfrak{m}$ είναι μη κενό. □

Στη συνέχεια της απόδειξης θα γράψουμε

$$r(N) = \int_0^1 S(\alpha)^3 e^{-2\pi iN\alpha}\,d\alpha = \int_{\mathfrak{M}} S(\alpha)^3 e^{-2\pi iN\alpha}\,d\alpha + \int_{\mathfrak{m}} S(\alpha)^3 e^{-2\pi iN\alpha}\,d\alpha$$

και θα φράξουμε καθένα από τα δύο ολοκληρώματα του αθροίσματος.

16 Πρωτεύοντα τόξα

Θεωρούμε το πρωτεύον τόξο $\mathfrak{M}(b,q)$. Για κάθε χαρακτήρα Dirichlet modulo q θεωρούμε το άθροισμα του Gauss

$$\tau(\chi) = \sum_{m\in\mathbb{Z}/q\mathbb{Z}} \chi(m)e^{\frac{2\pi im}{q}}.$$

Θεωρούμε επίσης το πεπερασμένο άθροισμα

$$\frac{1}{\phi(q)}\sum_{\chi \bmod q} \chi(n)\overline{\tau(\chi)},$$

όπου $\overline{\chi}$ είναι ο μιγαδικός συζυγής του χ, δηλαδή

$$\overline{\chi}(n) = \overline{\chi(n)} \qquad \forall n \in \mathbb{N}.$$

Αν $(n,q) > 1$, τότε $\chi(n) = 0$, άρα

$$\frac{1}{\phi(q)}\sum_{\chi \bmod q} \chi(n)\overline{\tau(\chi)} = 0.$$

Όμως για $(n,q) = 1$ έχουμε ότι

$$\frac{1}{\phi(q)}\sum_{\chi \bmod q} \chi(n)\overline{\tau(\chi)} = \frac{1}{\phi(q)}\sum_{\chi \bmod q}\sum_{m\in\mathbb{Z}/q\mathbb{Z}} \chi(n)\overline{\chi(m)}e^{\frac{2\pi im}{q}}.$$

Επειδή $(n,q) = 1$, για κάθε $m \in \mathbb{Z}/q\mathbb{Z}$ υπάρχει $h \in \mathbb{Z}/q\mathbb{Z}$ τέτοιο ώστε

$$m \equiv nh \pmod q,$$

και άρα καθώς το h διατρέχει το $\mathbb{Z}/q\mathbb{Z}$, το ίδιο κάνει και το m. Άρα

$$\begin{aligned}
\frac{1}{\phi(q)}\sum_{\chi \bmod q}\sum_{m\in\mathbb{Z}/q\mathbb{Z}} \chi(n)\overline{\chi(m)}e^{\frac{2\pi im}{q}} &= \frac{1}{\phi(q)}\sum_{\chi \bmod q}\sum_{h\in\mathbb{Z}/q\mathbb{Z}} \chi(n)\overline{\chi(nh)}e^{\frac{2\pi inh}{q}} \\
&= \frac{1}{\phi(q)}\sum_{\chi \bmod q}\sum_{h\in\mathbb{Z}/q\mathbb{Z}} \overline{\chi(h)}e^{\frac{2\pi inh}{q}} \\
&= \frac{1}{\phi(q)}\sum_{h\in\mathbb{Z}/q\mathbb{Z}} e^{\frac{2\pi inh}{q}}\sum_{\chi \bmod q}\overline{\chi(h)} \\
&= e^{\frac{2\pi in}{q}}.
\end{aligned}$$

Η τελευταία ισότητα ισχύει λόγω της πρότασης για την ορθογωνιότητα. Άρα έχουμε την

$$e^{\frac{2\pi in}{q}} = \frac{1}{\phi(q)}\sum_{\chi \bmod q} \chi(n)\overline{\tau(\chi)}. \tag{51}$$

Στη συνάρτηση $S(\alpha)$, επειδή δουλεύουμε για $\alpha \in \mathfrak{M}(b,q)$, γράφουμε

$$\alpha = \frac{b}{q} + c.$$

Τότε

$$S(\alpha) = \sum_{\substack{k\le N\\(k,q)=1}} \Lambda(k)e^{2\pi ik\left(\frac{b}{q}+c\right)} + O(\log^2 N).$$

Πράγματι, το σφάλμα προκύπτει αν αφαιρέσουμε από το $S(\alpha)$ τους όρους για τους οποίους $(k,q)>1$ ως εξής:

$$S(\alpha)-\sum_{\substack{k\le N\\(k,q)=1}}\Lambda(k)e^{2\pi ik\left(\frac{b}{q}+c\right)}=\sum_{\substack{k\le N\\(k,q)>1}}\Lambda(k)e^{2\pi ik\left(\frac{b}{q}+c\right)},$$

και συνεπώς, επειδή $|e^{2\pi ix}|=1$,

$$\left|S(\alpha)-\sum_{\substack{k\le N\\(k,q)=1}}\Lambda(k)e^{2\pi ik\left(\frac{b}{q}+c\right)}\right|\le\sum_{\substack{k\le N\\(k,q)>1}}\Lambda(k).$$

Τώρα, αν $\Lambda(k)\neq 0$, τότε $k=p^\nu$ για κάποιον πρώτο p και κάποιο $\nu\ge 1$, ενώ $\Lambda(k)=\log p$. Αν επιπλέον $(k,q)>1$, τότε αναγκαστικά $p\mid q$. Άρα

$$\sum_{\substack{k\le N\\(k,q)>1}}\Lambda(k)=\sum_{p\mid q}\sum_{\substack{\nu\ge 1\\p^\nu\le N}}\log p.$$

Για κάθε σταθερό πρώτο $p\mid q$, το πλήθος των εκθετών ν με $p^\nu\le N$ είναι το πολύ $\frac{\log N}{\log p}$, οπότε

$$\sum_{\substack{\nu\ge 1\\p^\nu\le N}}\log p\le\log p\cdot\frac{\log N}{\log p}=\log N.$$

Επομένως

$$\sum_{\substack{k\le N\\(k,q)>1}}\Lambda(k)\le\sum_{p\mid q}\log N\le(\log q)\log N\le\log^2 N,$$

αφού στα πρωτεύοντα τόξα έχουμε $q\le P=\log^B N$, και άρα $\log q\ll\log\log N\ll\log N$.

Συνεπώς

$$S(\alpha)=\sum_{\substack{k\le N\\(k,q)=1}}\Lambda(k)e^{2\pi ik\left(\frac{b}{q}+c\right)}+O(\log^2 N).$$

Αυτό το άθροισμα, με χρήση της (51) και του ότι

$$\chi(kb)=\chi(k)\chi(b)\qquad\text{για }(k,q)=1,$$

γίνεται

$$\begin{aligned}S(\alpha)&=\sum_{k\le N}\Lambda(k)\frac{1}{\phi(q)}\sum_{\chi\bmod q}\chi(kb)\overline{\tau(\chi)}\,e^{2\pi ikc}+O(\log^2 N)\\&=\frac{1}{\phi(q)}\sum_{\chi\bmod q}\tau(\overline{\chi})\chi(b)\sum_{k\le N}\chi(k)\Lambda(k)e^{2\pi ikc}+O(\log^2 N).\end{aligned}\tag{52}$$

Χρησιμοποιώντας άθροιση κατά μέρη παίρνουμε

$$\sum_{k\le N}\chi(k)\Lambda(k)e^{2\pi ikc}=e^{2\pi iNc}\sum_{n\le N}\chi(n)\Lambda(n)-2\pi ic\int_1^N e^{2\pi iuc}\sum_{n\le u}\chi(n)\Lambda(n)\,du.\tag{53}$$

Ορίζουμε τώρα

$$\psi(x,\chi)=\sum_{n\le x}\chi(n)\Lambda(n).$$

Άρα η (53) ξαναγράφεται ως

$$\sum_{k\le N}\chi(k)\Lambda(k)e^{2\pi ikc}=e^{2\pi iNc}\psi(N,\chi)-2\pi ic\int_1^N e^{2\pi iuc}\psi(u,\chi)\,du. \tag{54}$$

Θα χρησιμοποιήσουμε την ισχυρή μορφή του θεωρήματος των πρώτων για αριθμητικές προόδους στην ακόλουθη ομοιόμορφη διατύπωση.

Θεώρημα 16.1 (Ισχυρή ομοιόμορφη μορφή του θεωρήματος των πρώτων για αριθμητικές προόδους). *Για κάθε $M>0$ υπάρχει σταθερά $C(M)>0$ τέτοια ώστε, ομοιόμορφα ως προς*

$$2\le u\le N,\qquad q\le(\log N)^M,\qquad (a,q)=1,$$

να ισχύει

$$\psi(u;q,a)=\frac{u}{\varphi(q)}+O_M\left(Ne^{-C(M)\sqrt{\log N}}\right),$$

όπου

$$\psi(u;q,a):=\sum_{\substack{n\le u\\ n\equiv a\,(\mathrm{mod}\,q)}}\Lambda(n).$$

Η παραπάνω μορφή είναι ακριβώς αυτή που χρειαζόμαστε, διότι στη συνέχεια θα πρέπει να εκτιμήσουμε τη $\psi(u,\chi)$ ομοιόμορφα για όλα τα $u\in[1,N]$.

Λήμμα 16.2. *Θέτουμε*

$$\delta_\chi=\begin{cases}1, & \text{αν } \chi=\chi_0,\\ 0, & \text{αν } \chi\neq\chi_0,\end{cases}$$

όπου χ_0 είναι ο κύριος χαρακτήρας modulo q. Τότε, για κάθε χαρακτήρα Dirichlet $\chi\pmod q$, με

$$q\le(\log N)^M,$$

ισχύει ομοιόμορφα για $2\le u\le N$ ότι

$$\psi(u,\chi)=\delta_\chi\,u+O_M\left(Ne^{-C_1(M)\sqrt{\log N}}\right),$$

για κάποια θετική σταθερά $C_1(M)$, όπου

$$\psi(u,\chi):=\sum_{n\le u}\chi(n)\Lambda(n).$$

Απόδειξη. Εφόσον $\chi(n)=0$ όταν $(n,q)\neq1$, έχουμε

$$\psi(u,\chi)=\sum_{\substack{n\le u\\ (n,q)=1}}\chi(n)\Lambda(n).$$

Ομαδοποιώντας τώρα ως προς τις κλάσεις υπολοίπων modulo q, παίρνουμε

$$\psi(u,\chi)=\sum_{\substack{a\,(\mathrm{mod}\,q)\\ (a,q)=1}}\chi(a)\sum_{\substack{n\le u\\ n\equiv a\,(\mathrm{mod}\,q)}}\Lambda(n)=\sum_{\substack{a\,(\mathrm{mod}\,q)\\ (a,q)=1}}\chi(a)\,\psi(u;q,a).$$

Γράφουμε

$$\psi(u;q,a)=\frac{u}{\varphi(q)}+E_a(u),$$

όπου, από το Θεώρημα 16.1, ισχύει ομοιόμορφα ως προς a ότι

$$E_a(u) = O_M\left(Ne^{-C(M)\sqrt{\log N}}\right).$$

Τότε

$$\psi(u,\chi) = \sum_{\substack{a \,(\mathrm{mod}\, q)\\(a,q)=1}} \chi(a)\psi(u;q,a) = \sum_{\substack{a \,(\mathrm{mod}\, q)\\(a,q)=1}} \chi(a)\left(\frac{u}{\varphi(q)} + E_a(u)\right),$$

άρα

$$\psi(u,\chi) = \frac{u}{\varphi(q)} \sum_{\substack{a \,(\mathrm{mod}\, q)\\(a,q)=1}} \chi(a) + \sum_{\substack{a \,(\mathrm{mod}\, q)\\(a,q)=1}} \chi(a)E_a(u).$$

Για το δεύτερο άθροισμα, επειδή $|\chi(a)| = 1$ όταν $(a,q) = 1$, έχουμε

$$\left|\sum_{\substack{a \,(\mathrm{mod}\, q)\\(a,q)=1}} \chi(a)E_a(u)\right| \le \sum_{\substack{a \,(\mathrm{mod}\, q)\\(a,q)=1}} |E_a(u)|.$$

Υπάρχουν ακριβώς $\varphi(q)$ κλάσεις υπολοίπων $a \pmod q$ με $(a,q) = 1$, και καθεμιά από αυτές συνεισφέρει

$$O_M\left(Ne^{-C(M)\sqrt{\log N}}\right).$$

Επομένως

$$\sum_{\substack{a \,(\mathrm{mod}\, q)\\(a,q)=1}} \chi(a)E_a(u) = O_M\left(\varphi(q)\, Ne^{-C(M)\sqrt{\log N}}\right).$$

Άρα

$$\psi(u,\chi) = \frac{u}{\varphi(q)} \sum_{\substack{a \,(\mathrm{mod}\, q)\\(a,q)=1}} \chi(a) + O_M\left(\varphi(q)\, Ne^{-C(M)\sqrt{\log N}}\right).$$

Όμως

$$\sum_{\substack{a \,(\mathrm{mod}\, q)\\(a,q)=1}} \chi(a) = \begin{cases} \varphi(q), & \text{αν } \chi = \chi_0,\\ 0, & \text{αν } \chi \ne \chi_0. \end{cases}$$

Επομένως

$$\psi(u,\chi) = \delta_\chi\, u + O_M\left(\varphi(q)\, Ne^{-C(M)\sqrt{\log N}}\right).$$

Αφού

$$\varphi(q) \le q \le (\log N)^M,$$

ο πολυλογαριθμικός παράγοντας απορροφάται στην εκθετική, ίσως ελαττώνοντας τη σταθερά $C(M)$. Άρα

$$\psi(u,\chi) = \delta_\chi\, u + O_M\left(Ne^{-C_1(M)\sqrt{\log N}}\right),$$

όπως θέλαμε. □