

Εισαγωγή στη Θεωρία των Αριθμών

Μια προσέγγιση ελαφρώς υπολογιστική

Τυπογραφικά

Τελευταία ενημέρωση 16-9-2026

Η εντόπιση των παρακάτω τυπογραφικών αβλεψιών οφείλεται, σχεδόν αποκλειστικά, στον Μάριο Βεληβασάκη, ο οποίος διάβασε πολύ προσεκτικά το βιβλίο. Πριν από κάποια χρόνια ευτύχησα να έχω τον Μάριο προπτυχιακό και μεταπτυχιακό φοιτητή· τώρα ευτύχησα να τον έχω ασυνήθιστα προσεκτικό αναγνώστη! Είμαι ευγνώμων για τη μέριμνα και τον κόπο του.

Νίκος Γ. Τζανάκης

- σελ. 56, γραμμή 12: προέρχεται από το **ΑΥ** $\rightarrow$ προέρχεται από το **ΕΡ**
- σελ. 58, υποσημείωση 6: διατύπω~~ση~~ $\rightarrow$ διατύπω~~ση~~
- σελ. 64, γραμμή 3: έ~~χ~~ει $\rightarrow$ έ~~χ~~ει
- σελ. 64, γραμμή 10 της παραγράφου 2.6.1: είναι $\rightarrow$ είναι~~ι~~
- σελ. 64, υποσημείωση 7: πίνακα $\rightarrow$ πίνακα~~ς~~ (δύο φορές)
- σελ. 65, γραμμή 20: τους $a = 2, 3, \dots, B,$. $\rightarrow$ τους $a = 2, 3, \dots, B$. (χωρίς το κόμμα)
- σελ. 65, γραμμή 21: και **A** = 201 $\rightarrow$ και **B** = 201
- σελ. 74, υποσημείωση 10: **m** : **n** $\rightarrow$ και **n** : **m**
- σελ. 108, γραμμή 4 από το τέλος: περίπτωση **2** $\rightarrow$ περίπτωση **3**
- σελ. 122, προτελευταία γραμμή, δεύτερη ισότητα: $(-1)^{p-1} \left(\frac{p}{7} \right) \rightarrow (-1)^{2(p-1)} \left(\frac{p}{7} \right)$
- σελ. 126, πρώτη γραμμή του υπολογισμού: **jac21811** $\left(\frac{527}{1811} \right) \rightarrow \left(\frac{2}{1811} \right) \left(\frac{527}{1811} \right)$
- σελ. 128, γραμμή 2: αυτή η **η** συνθήκη $\rightarrow$ αυτή η συνθήκη
- σελ. 130, γραμμή 3: θετικού ακεραίου n είναι εξής $\rightarrow$ θετικού ακεραίου n είναι **η** εξής
- σελ. 142, γραμμή 5: (mod **m**) $\rightarrow$ (mod **r**)
- σελ. 142, Θεώρημα 6.1.4(2), γραμμή 2: $(k, \mathbf{m}) = 1 \rightarrow (k, \phi(\mathbf{m})) = 1$
- σελ. 143, τελευταία γραμμή: Κεφαλαίου 1) ότι $\rightarrow$ Κεφαλαίου 1) (χωρίς το ότι)
- σελ. 143, τελευταία γραμμή: Είναι $\rightarrow$ Εί~~ν~~αι

- σελ. 147, γραμμή 2: το μόνο που μένει ν'αποδειχθεί **είναι** ότι $\rightarrow$ το μόνο που μένει **για** ν'αποδειχθεί ότι
- σελ. 153, γραμμή 13: $a^x \equiv b \pmod{m} \rightarrow a^x \equiv b \pmod{p}$
- σελ. 155, σχέση (6.7): $b^{q^{e-1}} \equiv a^{kq^{e-1}} \rightarrow b^{q^{e-1}} \equiv a^{xq^{e-1}}$ (δεν είναι μαθηματικό λάθος, διότι $b \equiv a^k \pmod{p}$, απλώς ίσως είναι πιο κατανοητό με το x λόγω των υπολογισμών που έγιναν ακριβώς πριν από τη σχέση (6.7).)
- σελ. 175, παράδειγμα 7.2.8(1), στήλη των a_i : $a_3 = 3, a_4 = 2 \rightarrow a_3 = 7, a_4 = 1$
- σελ. 175, παράδειγμα 7.2.8(2), στήλη των a_i : $a_2 = 4 \rightarrow a_2 = 1$
- σελ. 181, γραμμή 2 της τελευταίας παραγράφου: $a \square_k \rightarrow a'_k$
- σελ. 182, γραμμή 6: $\langle a_0, a_1, \dots, a_1, a_k, a'_{k+1} \rangle \rightarrow \langle a_0, a_1, \dots, a_{k-1}, a_k, a'_{k+1} \rangle$
- σελ. 182, γραμμή 15: $\langle a_0, a_1, \dots, a_n \rangle - \theta \rightarrow |\langle a_0, a_1, \dots, a_n \rangle - \theta|$
- σελ. 196, γραμμή 10: ολοκληρώσαμε **τ** την $\rightarrow$ ολοκληρώσαμε την
- σελ. 198, γραμμή 9: $p_2\alpha + p_1/q_2\alpha + q_1 = 9\alpha + 4/7\alpha + 3 \rightarrow (p_2\alpha + p_1)/(q_2\alpha + q_1) = (9\alpha + 4)/(7\alpha + 3)$
- σελ. 198, γραμμή 6 του παραδείγματος 7.5.6(4): $P_2\alpha + P_1/Q_2\alpha + Q_1 = \alpha + 1/2\alpha + 1 = 10 + \sqrt{37}/13 + 2\sqrt{37} \rightarrow (P_2\alpha + P_1)/(Q_2\alpha + Q_1) = (\alpha + 1)/(2\alpha + 1) = (10 + \sqrt{37})/(13 + 2\sqrt{37})$
- σελ. 207, γραμμή 1: ο συζυγής του **α** είναι $\bar{\alpha} = \dots \rightarrow$ ο συζυγής του **α_1** είναι $\bar{\alpha}_1 = \dots$
- σελ. 207, γραμμή 5: και ο συζυγής του είναι $\bar{\alpha} = \dots \rightarrow$ και ο συζυγής του είναι $\bar{\alpha}_2 = \dots$
- σελ. 214, σχέση (7.61): $a_{m-1} = [2\sqrt{d}] \rightarrow c_{m-1} = [2\sqrt{d}]$
- σελ. 218, γραμμή 17:
 $((x_1 + y_1\sqrt{d})(x_1 + y_1\sqrt{d})^m((x_1 + y_1\sqrt{d})) \rightarrow ((x_1 + y_1\sqrt{d})(x_1 - y_1\sqrt{d})^m(x_1 + y_1\sqrt{d}))$
- σελ. 225, γραμμή 7: $\begin{pmatrix} 5 & 2 \\ 3 & I \end{pmatrix} \rightarrow \begin{pmatrix} 5 & 2 \\ 3 & 1 \end{pmatrix}$
- σελ. 225, γραμμή 9 της παραγράφου 7.7.1: είναι $\rightarrow$ είναι
- σελ. 226, γραμμή 8 της απόδειξης: και το **το** αντίστροφο $\rightarrow$ και το αντίστροφο
- σελ. 229, σχέση (7.93): $m_1, m_2 \in \mathbb{N}_0$ ²³ λείπει η υποσημείωση 23, η οποία είναι «Αν $k = 1$ (αντιστ. $l = 1$), πρέπει $m_1 \geq 1$ (αντιστ. $m_2 \geq 1$).»
- σελ. 244, γραμμή 2 μετά το τέλος της απόδειξης του λήμματος: η **g** περιέχεται στην **f** μέσω... $\rightarrow$ η **f** περιέχεται στην **g** μέσω...

- σελ. 246, γραμμή 13 της απόδειξης: δίνει $d \equiv (2auv' + bv')^2 \pmod{B}$. $\rightarrow$ δίνει $d \equiv (2auv' + b)^2 \pmod{B}$.
- σελ. 251, γραμμή 9 της απόδειξης του παραδείγματος 8.2.7: είναι τετράγωνο $\pmod{4p}$ $\rightarrow$ είναι τετράγωνο $\pmod{4p}$
- σελ. 253, γραμμή 3: $P^{-1} = \begin{pmatrix} s & -r \\ -q & p \end{pmatrix} \rightarrow \epsilon \begin{pmatrix} s & -r \\ -q & p \end{pmatrix}$
 (δεν υπάρχει κάποιο λάθος στην συνέχεια της απόδειξης διότι η έκφραση $\frac{\epsilon s p - \epsilon r}{-\epsilon q p + \epsilon p}$ είναι ίση, έπειτα από απλοποίηση του ϵ , με την έκφραση $\frac{s p - r}{-q p + p}$ η οποία χρησιμοποιείται στην απόδειξη)
- σελ. 258, γραμμή 4 της απόδειξης του πορίσματος: Είναι $\alpha p = -b + \sqrt{d} > 0$, $\rightarrow$ Είναι $2\alpha p = -b + \sqrt{d} > 0$,
- σελ. 268, ακριβώς μετά τη σχέση (8.22): $\langle c_0, c_{n-1}, c_n, \dots \rangle$ αλυσιδωτό $\rightarrow$ $\langle c_0, c_1, \dots, c_{n-1}, c_n, \dots \rangle$ αλυσιδωτό