ΚΕΦΑΛΑΙΟ 1

ΘΕΩΡΙΑ ΔΙΑΙΡΕΤΟΤΗΤΑΣ

§1. Βασικές άρχές καί θεωρήματα.

α) Ἡ θεωρία τῶν ἀριθμῶν ἀσχολεῖται μέ τή μελέτη τῶν ἰδιοτήτων τῶν ἀκεραίων. Λέγοντας ἀκέραιοι, δέν ἐννοοῦμε μόνο τούς ἀριθμούς τῆς ἀκολουθίας τῶν φυσικῶν 1,2,3,... (θετικοί ἀκέραιοι)· ἀλλά καί τό μηδέν καί τούς ἀρνητικούς ἀκεραίους $-1,-2,-3,\ldots$

Κατά κανόνα, στή παρουσίαση τῆς θεωρίας, θά χρησιμοποιοῦμε γράμματα μόνο γιά τό συμβολισμό τῶν ἀκεραίων. Στίς περιπτώσεις πού τά γράμματα πιθανόν νά μήν συμβολίζουν ἀκεραίους, ἄν αὐτό δέ γίνεται φανερό ἀπό μόνο του, θά τό ἀναφέρομε εἰδικώτερα.

Τό ἄθροισμα, ἡ διαφορά καί τό γινόμενο δυό ἀκεραίων a καί b εἶναι ἐπίσης ἀκέραιος, ἀλλά τό πηλίκο πού προκύπτει ἀπ' τή διαίρεση τοῦ a μέ τόν b (ἄν ὁ b δέν εἶναι μηδέν) μπορεῖ νά εἶναι ἀκέραιος μπορεῖ ὅμως καί νά μήν εἶναι.

β) Στήν περίπτωση κατά τήν ὁποία τό πηλίκο πού προκύπτει ἀπ' τή διαίρεση τοῦ a μέ τόν b εἶναι ἕνας ἀκέραιος, ἄς τόν συμβολίσουμε μέ q, ἔχομε $a=bq$, δηλ. ὁ a εἶναι ἴσος μέ τό γινόμενο τοῦ b ἐπί ἕνα ἀκέραιο. Τότε λέμε ὅτι ὁ a εἶναι διαιρετός ἀπό τόν b ἤ ὅτι ὁ b διαιρεῖ τόν a. Ἐδῶ χαρακτηρίζεται ὁ a πολλαπλάσιο τοῦ b καί ὁ b διαιρέτης τοῦ a. Τό ὅτι ὁ b διαιρεῖ τόν a συμβολίζεται μέ $b|a$.

Ἰσχύουν τά ἑξῆς δύο θεωρήματα:

1. <u>Ἄν ὁ a εἶναι πολλαπλάσιο τοῦ m καί ὁ m εἶναι πολλαπλάσιο τοῦ b, τότε ὁ a εἶναι πολλαπλάσιο τοῦ b.</u>

Πραγματικά, ἀπ' τίς σχέσεις $a=a_1m$ καί $m=m_1b$ ἕπεται ὅτι $a=a_1m_1b$ ὅπου ὁ a_1m_1 εἶναι ἀκέραιος. Ἀλλ' αὐτό ἀποδεικνύει τό θεώρημα.

2. <u>Ἄν εἶναι γνωστό γιά ὅλους τούς ὅρους, ἐκτός ἀπό ἕνα, μιᾶς ἐξίσωσης τῆς μορφῆς $k+\ldots+n=p+q+\ldots+s$ ὅτι εἶναι πολλαπλάσιο τοῦ b, τότε καί αὐτός ὁ ὑπόλοιπος ὅρος εἶναι ἐπίσης πολλαπλάσιο τοῦ b.</u>

Πραγματικά, ἔστω ὅτι ὁ ὅρος πού ἐξαιρέσαμε εἶναι ὁ k. Τότε ἔχομε

$$l=l_1b,\ldots,n=n_1b,\ p=p_1b,\ q=q_1b,\ldots,s=s_1b,$$

$$k=p+q+\ldots+s-l-\ldots-n=$$

$$=(p_1+q_1+\ldots+s_1-l_1-\ldots-n_1)b$$

ἀποδεικνύοντας ἔτσι τό θεώρημά μας.

γ) Στή γενική περίπτωση, πού περιλαμβάνει καί τήν εἰδικώτερη στήν ὁποία ὁ a εἶναι διαιρετός ἀπ' τόν b ἔχομε τό θεώρημα:

<u>Κάθε ἀκέραιος a μπορεῖ νά παρασταθεῖ κατά ἕνα καί μοναδικό τρόπο συναρτήσει τοῦ θετικοῦ ἀκεραίου b μέ τή μορφή:</u>

$$a=bq+r\ ,\quad 0\leq r<b$$

Πραγματικά, μιά τέτοια παράσταση τοῦ a παίρνομε ἄν θεωρήσομε τόν bq νά εἶναι ἴσος μέ τό μεγαλύτερο πολλαπλάσιο τοῦ b , πού δέν ξεπερνᾶ τόν a . Ὑποθέτοντας ὅτι ἔχομε, ἐπίσης, καί $a=bq_1+r_1$, $0\leq r_1<b$, βρίσκομε ὅτι $0=b(q-q_1)+r-r_1$ ἀπ'ὅπου ἕπεται (2,b) ὅτι ὁ $r-r_1$ εἶναι πολλαπλάσιο τοῦ b . Ἀλλά μιά καί $|r-r_1|<b$, τό τελευταῖο συμπέρασμα εἶναι δυνατόν μόνο ἄν $r-r_1=0$, δηλ. ἄν $r=r_1$. ἀπ'ὅπου ἕπεται, ἐπίσης, ὅτι καί $q=q_1$.
Ὁ ἀριθμός q λέγεται τό μερικό πηλίκο καί ὁ ἀριθμός r τό ὑπόλοιπο, πού προκύπτει ἀπ'τή διαίρεση τοῦ a μέ τόν b.
Παραδείγματα: Ἔστω $b=14$." Ἔχομε:

$$177=14.12+9\ ,\quad 0<9<14$$
$$-64=14(-5)+6\ ,\quad 0<6<14$$
$$154=14.11+0\ ,\quad 0=0<14$$

§ 2. Ὁ μέγιστος κοινός διαιρέτης.

a) Στά ἑπόμενα θά θεωροῦμε μονάχα τούς θετικούς διαιρέτες τῶν ἀριθμῶν. Κάθε ἀκέραιος πού διαιρεῖ ὅλους τούς ἀκεραίους a,b,...,l λέγεται <u>κοινός διαιρέτης</u> τῶν ἀριθμῶν αὐτῶν. Ὁ μεγαλύτερος ἀπ'αὐτούς τούς κοινούς διαιρέτες λέγεται <u>μέγιστος κοινός διαιρέτης</u> καί συμβολίζεται μέ (a,b,...,l). Μιά καί οἱ κοινοί διαιρέτες εἶναι πεπερασμένοι τό πλῆθος, ἡ ὕπαρξη τοῦ μέγιστου κοινοῦ διαιρέτη γίνεται φανερή. "Αν $(a,b,\dots,l)=1$ τότε οἱ a,b,...,l χαρακτηρίζονται σάν <u>πρῶτοι μεταξύ τους</u>." Αν δύο ὁποιοιδήποτε ἀπό τούς ἀριθμούς a,b,...,l εἶναι πρῶτοι μεταξύ τους, τότε οἱ a,b,...,l χαρακτηρίζονται σάν <u>ἀνά ζεύγη πρῶτοι</u>. Εἶναι φανερό ὅτι ἕνα πλῆθος ἀριθμῶν πού εἶναι ἀνά ζεύγη πρῶτοι, θά εἶναι καί μεταξύ τους πρῶτοι· στήν περίπτωση δυό ἀριθμῶν, οἱ ἔννοιες "ἀνά ζεύγη πρῶτοι" καί "πρῶτοι μεταξύ τους" συμπίπτουν.
Παραδείγματα: Οἱ ἀριθμοί 6,10,15 εἶναι πρῶτοι μεταξύ τους γιατί $(6,10,15)=1$ Οἱ ἀριθμοί 9,13,21 εἶναι ἀνά ζεύγη πρῶτοι γιατί $(9,13)=(9,21)=(13,21)=1$.

b) Πρῶτα θεωροῦμε τούς κοινούς διαιρέτες δύο ἀριθμῶν.
1. "<u>Αν ὁ a εἶναι πολλαπλάσιο τοῦ b , τότε τό σύνολο τῶν κοινῶν διαιρετῶν τῶν ἀριθμῶν a καί b συμπίπτει μέ τό σύνολο τῶν διαιρετῶν τοῦ b</u>· εἰδικώτερα, $(a,b)=b$.
Πραγματικά, κάθε κοινός διαιρέτης τῶν ἀριθμῶν a καί b εἶναι διαιρέτης τοῦ b . Ἀντίστροφα, ἄν ὁ a εἶναι πολλαπλάσιο τοῦ b τότε (1,b,§1) κάθε διαιρέτης τοῦ ἀριθμοῦ b εἶναι, ἐπίσης, διαιρέτης τοῦ ἀριθμοῦ a δηλ. εἶναι κοινός διαιρέτης τῶν ἀριθμῶν a καί b ." Ἅρα τό σύνολο τῶν κοινῶν διαιρετῶν τῶν ἀριθμῶν a καί b συμπίπτει μέ τό σύνολο τῶν διαιρετῶν τοῦ b , ἀλλά μιά καί ὁ μεγαλύτερος διαιρέτης τοῦ ἀριθμοῦ b εἶναι ὁ ἴδιος ὁ b , θά ἔχομε $(a,b)=b$.

2. Αν $a = bq + c$

τότε τό σύνολο τῶν κοινῶν διαιρετῶν τῶν ἀριθμῶν a καί b συμπίπτει μέ τό σύνολο τῶν κοινῶν διαιρετῶν τῶν ἀριθμῶν b καί c . Ειδικώτερα $(a,b)=(b,c)$. Πραγματικά, ἡ παραπάνω ἰσότητα δείχνει ὅτι κάθε κοινός διαιρέτης τῶν ἀριθμῶν a καί b διαιρεῖ τόν c (§1), ἄρα εἶναι κοινός διαιρέτης τῶν b καί c . Ἀντίστροφα, ἡ ἴδια ἰσότητα δείχνει ὅτι κάθε κοινός διαιρέτης τῶν ἀριθμῶν b καί c διαιρεῖ τόν a καί, κατά συνέπεια, εἶναι κοινός διαιρέτης τῶν ἀριθμῶν a καί b . Ἄρα οἱ κοινοί διαιρέτες τῶν ἀριθμῶν a καί b εἶναι ἐκεῖνοι ἀκριβῶς οἱ ἀριθμοί, πού εἶναι ἐπίσης κοινοί διαιρέτες τῶν ἀριθμῶν b καί c . Ειδικώτερα οἱ μεγαλύτεροι ἀπ' αὐτούς τούς διαιρέτες πρέπει, ἐπίσης, νά ταυτίζονται, δηλ. $(a,b)=(b,c)$

c) Προκειμένου νά βροῦμε τό μέγιστο κοινό διαιρέτη ἁλλά καί νά συνάγομε τίς πιό σπουδαῖες ἰδιότητές του, ἐφαρμόζομε τόν Εὐκλείδιο ἀλγόριθμο. Αὐτός συνίσταται στήν ἑξῆς διαδικασία:
Ἔστω ὅτι οἱ a καί b εἶναι θετικοί ἀκέραιοι. Ἀπ' τό §1 βρίσκομε τήν ἀκολουθία τῶν ἰσοτήτων,

$$(1)\quad \begin{cases} a = bq_1 + r_2 & , \ 0 < r_2 < b \\ b = r_2 q_3 + r_3 & , \ 0 < r_3 < r_2 \\ r_2 = r_3 q_4 + r_4 & , \ 0 < r_4 < r_3 \\ \cdots\cdots\cdots\cdots & \\ r_{n-2} = r_{n-1} q_n + r_n & , \ 0 < r_n < r_{n-1} \\ r_{n-1} = r_n q_{n+1} & \end{cases}$$

ἡ ὁποία σταματᾶ ὅταν βροῦμε κάποιο $r_{n+1}=0$. Αὐτό τό τελευταῖο πρέπει καθότε νά συμβεῖ, ἀφοῦ ἡ ἀκολουθία $b, r_2, r_3, \ldots$ σάν φθίνουσα ἀκολουθία ἀκεραίων δέν μπορεῖ νά περιέχει περισσότερους ἀπό b τό πλῆθος θετικούς ἀκεραίους.

d) Θεωρώντας τίς ἰσότητες (1), προχωρῶντας ἀπό πάνω πρός τά κάτω, ἔχομε σύμφωνα μέ τό (b) ὅτι οἱ κοινοί διαιρέτες τῶν ἀριθμῶν a καί b ταυτίζονται μέ τούς κοινούς διαιρέτες τῶν ἀριθμῶν b καί r_2, καί ἀκόμη μέ τούς κοινούς διαιρέτες τῶν ἀριθμῶν r_2 καί r_3, τῶν ἀριθμῶν r_3 καί r_4, ..., τῶν ἀριθμῶν r_{n-1} καί r_n καί, τελικά, μέ τούς διαιρέτες τοῦ ἀριθμοῦ r_n . Σύμφωνα μ' αὐτά ἔχομε:

$$(a,b)=(b,r_2)=(r_2,r_3)=\cdots=(r_{n-1},r_n)=r_n$$

φτάνομε ἔτσι στά ἑπόμενα ἀποτελέσματα:

1. Τό σύνολο τῶν κοινῶν διαιρετῶν τῶν ἀριθμῶν a καί b συμπίπτει μέ τό σύνολο τῶν διαιρετῶν τοῦ μεγίστου κοινοῦ διαιρέτη τους.

2. Αὐτός ὁ μέγιστος κοινός διαιρέτης τους εἶναι ἴσος μέ τόν r_n, δηλ. τό ἐλάχιστο μή μηδενικό ὑπόλοιπο στόν Εὐκλείδιον ἀλγόριθμο.

Παράδειγμα. Εφαρμόζομε τόν Ευκλείδιον αλγόριθμο στόν υπολογισμό του (525,231). Βρίσκομε (οι βοηθητικοί υπολογισμοί δίνονται αριστερά)

525 | 231 / 462 | 2		$525 = 231\cdot 2 + 63$
231 | 63 / 189 | 3		$231 = 63\cdot 3 + 42$
63 | 42 / 42 | 1		$63 = 42\cdot 1 + 21$
42 | 21 / 42 | 2		$42 = 21\cdot 2$
0		

Εδώ το ελάχιστο θετικό υπόλοιπο είναι $r_4 = 21$. Αυτό σημαίνει ότι $(525,231) = 21$.

e) 1. "Αν ο m είναι οποιοσδήποτε θετικός ακέραιος, τότε $(am,bm) = (a,b)m$.

2. "Αν δ είναι οποιοσδήποτε κοινός διαιρέτης των αριθμών a και b, τότε $\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a,b)}{\delta}$ ειδικώτερα $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$, δηλ. τα πηλίκα που προκύπτουν απ' τη διαίρεση δύο αριθμών με το μέγιστο κοινό διαιρέτη τους είναι αριθμοί πρώτοι μεταξύ τους.

Πραγματικά, ας πολλαπλασιάσουμε καθένα απ' τούς όρους των ισοτήτων (1) μέ τόν m. Παίρνομε τότε νέες ισότητες, όπου οι $a,b,r_2,\dots,r_n$ αντικαθίστανται απ' τούς $am, bm, r_2m, \dots, r_nm$. Τότε $(am,bm) = r_nm$, δείχνοντας έτσι ότι η πρόταση 1. αληθεύει.

Εφαρμόζοντας την πρόταση 1. βρίσκομε ότι

$$(a,b) = \left(\frac{a}{\delta}\delta, \frac{b}{\delta}\delta\right) = \left(\frac{a}{\delta}, \frac{b}{\delta}\right)\delta$$

και έτσι αποδεικνύομε και τήν πρόταση 2.

f) 1. "Αν $(a,b)=1$ τότε $(ac,b)=(c,b)$

Πραγματικά, ο αριθμός (ac,b) διαιρεί τούς ac και bc, γεγονός πού συνεπάγεται $(1,d)$ ότι επίσης διαιρεί τόν (ac,bc), ο όποιος είναι ίσος μέ c, σύμφωνα μέ τό 1.e. Αλλά ο (ac,b) διαιρεί επίσης και τόν b, άρα διαιρεί και τόν (c,b). Αντίστροφα, ο (c,b) διαιρεί τόν ac και τόν b άρα διαιρεί και τόν (ac,b). Έτσι οι (ac,b) και (c,b) διαιρούν ο ένας τόν άλλο άρα είναι ίσοι μεταξύ τους.

2. "Αν $(a,b)=1$ και ο ac είναι διαιρετός απ' τόν b, τότε ο c διαιρείται απ' τόν b.

Πραγματικά, άφού $(a,b)=1$, θά έχομε $(ac,b)=(c,b)$. Αλλά άν ο ac είναι πολλαπλάσιο τού b, τότε $(1,b)$ θά έχομε $(ac,b)=b$, πού σημαίνει ότι $(c,b)=b$, δηλ. ο c είναι πολλαπλάσιο τού b.

3. "Αν καθένας απ' τούς $a_1,a_2,\dots,a_m$ είναι πρώτος πρός καθέναν απ' τούς $b_1,b_2,\dots,b_n$ τότε τά γινόμενα $a_1a_2\dots a_m$ και $b_1b_2\dots b_n$ είναι αριθμοί πρώτοι μεταξύ τους.

Πραγματικά (θεώρημα 1.) έχομε:

$$(a_1,a_2\dots a_m,b_k) = (a_2a_3\dots a_m,b_k) = (a_3\dots a_m,b_k) = \dots = (a_m,b_k) = 1$$

καί, ἐπιπλέον, ἄν θέσωμε $a_1a_2\cdots a_n=A$, μέ τόν ἴδιο τρόπο βρίσκομε
$(b_1b_2\cdots b_n,A)=(b_2b_3\cdots b_n,A)=(b_3\cdots b_n,A)=\cdots=(b_n,A)=1$

g) Τό πρόβλημα τῆς εὑρεσης τοῦ μέγιστου κοινοῦ διαιρέτη περισσοτέρων ἀπό δύο ἀριθμῶν ἀνάγεται στό ἴδιο πρόβλημα γιά δύο ἀριθμούς. Πραγματικά, γιά νά βροῦμε τό μέγιστο κοινό διαιρέτη τῶν ἀριθμῶν $a_1,a_2,\cdots a_n$ σχηματίζομε τήν ἀκολουθία τῶν ἀριθμῶν:
$(a_1,a_2)=d_2$, $(d_2,a_3)=d_3$, $(d_3,a_4)=d_4,\ldots,(d_{n-1},a_n)=d_n$
Ὁ ἀριθμός d_n εἶναι, ἐπίσης, ὁ μέγιστος κοινός διαιρέτης ὅλων τῶν δοσμένων ἀριθμῶν.
Πραγματικά $(1,d)$, οἱ κοινοί διαιρέτες τῶν ἀριθμῶν a_1 καί a_2 συμπίπτουν μέ τούς διαιρέτες τοῦ d_2. Γι' αὐτό οἱ κοινοί διαιρέτες τῶν ἀριθμῶν a_1,a_2 καί a_3 συμπίπτουν μέ τούς κοινούς διαιρέτες τῶν ἀριθμῶν d_2 καί a_3, δηλ. συμπίπτουν μέ τούς διαιρέτες τοῦ d_3. Ἀκόμη, μποροῦμε νά ἐπαληθεύσουμε ὅτι οἱ κοινοί διαιρέτες τῶν ἀριθμῶν a_1,a_2,a_3,a_4 συμπίπτουν μέ τούς διαιρέτες τοῦ d_4 κ.ὁ.κ. καί τελικά, ὅτι οἱ κοινοί διαιρέτες τῶν ἀριθμῶν $a_1,a_2,\ldots,a_n$ συμπίπτουν μέ τούς διαιρέτες τοῦ d_n. Ἀλλά μιά καί ὁ μέγιστος διαιρέτης τοῦ d_n εἶναι ὁ ἴδιος ὁ d_n, αὐτός θά εἶναι καί ὁ μέγιστος κοινός διαιρέτης τῶν ἀριθμῶν $a_1,a_2,\ldots,a_n$.
Θεωρώντας τήν παραπάνω ἀπόδειξη, μποροῦμε νά δοῦμε ὅτι τό θεώρημα $1,d$ ἀληθεύει καί γιά περισσότερους ἀπό δυό ἀριθμούς, ἐπίσης. Τά θεωρήματα $1,e$ καί $2,e$ ἀληθεύουν, ἐπίσης, ἐπειδή ὁ πολλαπλασιασμός μέ τόν m ἤ ἡ διαίρεση μέ τόν δ ὅλων τῶν ἀριθμῶν $a_1,a_2,\ldots,a_n$ κάνει ὅλους τούς ἀριθμούς $d_1,d_2,\ldots,d_n$ νά πολλαπλασιάζονται μέ τόν m ἤ νά διαιροῦνται μέ τόν δ.

§3. Τό ἐλάχιστο κοινό πολλαπλάσιο

a) Ἕνας ἀκέραιος πού εἶναι πολλαπλάσια καθενός ἀπ' τούς ἀριθμούς ἑνός δοσμένου συνόλου, χαρακτηρίζεται σάν <u>κοινό πολλαπλάσιο</u> αὐτῶν τῶν ἀριθμῶν.

b) Πρῶτα θεωροῦμε τό <u>ἐλάχιστο κοινό πολλαπλάσιο</u> δυό ἀριθμῶν. Ἔστω ὅτι ὁ M εἶναι ἕνα ὁποιοδήποτε κοινό πολλαπλάσιο τῶν ἀριθμῶν a καί b. Μιά κάί ὁ M εἶναι πολλαπλάσιο τοῦ a, $M=aK$, ὅπου ὁ K εἶναι κάποιος ἀκέραιος. Ἀλλά ὁ M εἶναι ἐπίσης πολλαπλάσιο τοῦ b, ἄρα ὁ $\frac{aK}{b}$ πρέπει νά εἶναι ἐπίσης ἀκέραιος, ὁ ὁποῖος, ἄν θέσωμε $(a,b)=d$, $a=a_1d$, $b=b_1d$ μπορεῖ νά παρασταθεῖ μέ τή μορφή $\frac{a_1K}{b_1}$, ὅπου $(a_1,b_1)=1$ $(2,e,\S2)$. Τότε ὅμως $(2,f,\S2)$ ὁ K πρέπει νά εἶναι διαιρετός ἀπ' τόν b_1, $K=b_1t=\frac{b}{d}t$, ὅπου ὁ t εἶναι κάποιος ἀκέραιος. Ἔτσι

$$M=\frac{ab}{d}t$$

Αντίστροφα, είναι σαφές ότι κάθε Μ αύτής της μορφής είναι πολλαπλάσιο του a καθώς και του b , άρα, αύτή η μορφή δίνει όλα τά κοινά πολλαπλάσια των αριθμών a και b . Το μικρότερο θετικό απ' αύτά τά πολλαπλάσια, δηλ. το ελάχιστο κοινό πολλαπλάσιο, παίρνομε για t=1 . Αύτό είναι

$$m = \frac{ab}{d}$$

Εισάγοντας το m , μπορούμε να γράφομε τον τύπο πού πήραμε για το M σάν

$$M = m \cdot t$$

Οι δυό τελευταίες ισότητες μάς οδηγούν στά θεωρήματα:

1) <u>Τά κοινά πολλαπλάσια δυό αριθμών ταυτίζονται με τά πολλαπλάσια του ελάχιστου κοινού πολλαπλασίου τους.</u>

2) <u>Το ελάχιστο κοινό πολλαπλάσιο δυό αριθμών είναι ίσο με το γινόμενό τους διαιρεμένο με το μέγιστο κοινό διαιρέτη τους.</u>

c) Ας υποθέσουμε τώρα ότι χρειάζεται να βρούμε το ελάχιστο κοινό πολλαπλάσιο περισσοτέρων από δύο αριθμών $a_1, a_2, \dots, a_n$. Αν υποτεθεί ότι το σύμβολο $m(a,b)$ συμβολίζει το ελάχιστο κοινό πολλαπλάσιο των αριθμών a και b σχηματίζομε την ακολουθία των αριθμών:

$$m(a_1,a_2)=m_2 \ , \ m(m_2,a_3)=m_3 \ , \ \dots \ , \ m(m_{n-1},a_n)=m_n$$

Ο m_n πού παίρνομε μ' αύτό τον τρόπο είναι το ελάχιστο κοινό πολλαπλάσιο όλων των δοσμένων αριθμών.

Πραγματικά (1,b), τά κοινά πολλαπλάσια των αριθμών a_1 και a_2 συμπίπτουν με τά πολλαπλάσια του m_2, άρα τά κοινά πολλαπλάσια των αριθμών a_1, a_2 και a_3 συμπίπτουν με τά κοινά πολλαπλάσια των m_2 και a_3, δηλ. συμπίπτουν με τά πολλαπλάσια του m_3. Είναι φανερό τότε ότι τά κοινά πολλαπλάσια των αριθμών a_1, a_2, a_3, a_4 συμπίπτουν με τά πολλαπλάσια του m_4 κ.ό.κ. και, τελικά, τά κοινά πολλαπλάσια των αριθμών $a_1, a_2, \dots, a_n$ συμπίπτουν με τά πολλαπλάσια του m_n και αφού το ελάχιστο θετικό πολλαπλάσιο του m_n είναι ο ίδιος ο m_n, θα' είναι επίσης και το ελάχιστο κοινό πολλαπλάσιο των αριθμών $a_1, a_2, \dots, a_n$. Παρατηρώντας την παραπάνω απόδειξη, βλέπομε ότι το θεώρημα 1,b αληθεύει επίσης και για περισσότερους από δύο αριθμούς. Επιπλέον αποδείξαμε και την ισχύ του εξής θεωρήματος:

<u>Το ελάχιστο κοινό πολλαπλάσιο αριθμών πού είναι ανά ζεύγη πρώτοι, είναι ίσο με το γινόμενό τους.</u>

§4. Σχέση Ευκλείδιου Αλγορίθμου και Συνεχών Κλασμάτων

a) Έστω α ένας οποιοσδήποτε πραγματικός αριθμός. Έστω q_1 ο μεγαλύτερος ακέραιος πού δέν υπερβαίνει τον α. Αν το α δέν είναι ακέραιος θά έχομε:

$$\alpha = q_1 + \frac{1}{\alpha_2} \quad , \ \alpha_2 > 1$$

Με όμοιο τρόπο, αν οι $\alpha_2, \dots, \alpha_{n-1}$ δέν είναι ακέραιοι, θά έχομε:

$$\alpha_2 = q_2 + \frac{1}{\alpha_3} \quad , \quad \alpha_3 > 1$$

. . . .

$$\alpha_{s-1} = q_{s-1} + \frac{1}{\alpha_s} \quad , \quad \alpha_s > 1$$

ἀπ'ὅπου παίρνομε τήν παρακάτω <u>ἀνάπτυξη τοῦ α σέ συνεχές κλάσμα:</u>

$$(1) \qquad \alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \ddots \cfrac{1}{q_{s-1} + \cfrac{1}{q_s}}}}}$$

Ἄν ὁ α εἶναι ἄρρητος, τότε εἶναι φανερό ὅτι δέν μπορεῖ νά ὑπάρξουν ἀκέραιοι στήν ἀκολουθία $\alpha_1, \alpha_2, \ldots$ καί ἡ παραπάνω διαδικασία μπορεῖ νά συνεχίζεται ἀτέρμονα.

Ἄν ὁ α εἶναι ρητός, τότε, ὅπως θά δοῦμε παρακάτω (b), θά ὑπάρξει κάποια στιγμή ἕνας ἀκέραιος στήν ἀκολουθία $\alpha_1, \alpha_2, \ldots$ καί ἡ παραπάνω διαδικασία θά σταματήσει.

b) Ἄν ὁ α εἶναι ἀνάγωγο ρητό κλάσμα, τότε ἡ ἀνάπτυξη τοῦ α σέ συνεχές κλάσμα συνδέεται στενά μέ τόν Εὐκλείδιο ἀλγόριθμο. Πραγματικά, ἔχομε:

$$a = bq_1 + r_2 \quad , \quad \frac{a}{b} = q_1 + \frac{r_2}{b}$$
$$b = r_2 q_2 + r_3 \quad , \quad \frac{b}{r_2} = q_2 + \frac{r_3}{r_2}$$
$$r_2 = r_3 q_3 + r_4 \quad , \quad \frac{r_2}{r_3} = q_3 + \frac{r_4}{r_3}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n \quad , \quad \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{r_n}{r_{n-1}}$$
$$r_{n-1} = r_n q_n \quad , \quad \frac{r_{n-1}}{r_n} = q_n$$

ἀπ'ὅπου βρίσκομε:

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \ddots + \cfrac{1}{q_n}}}}$$

c) Οἱ ἀριθμοί $q_1, q_2, \ldots$ πού ἐμφανίζονται κατά τήν ἀνάπτυξη τοῦ ἀριθμοῦ α σέ συνεχές κλάσμα, λέγονται <u>μερικά πηλῖκα</u> (γιά τήν περίπτωση ρητοῦ α, αὐτά εἶναι, σύμφωνα μέ τό b, τά μερικά πηλῖκα τῶν διαδοχικῶν διαιρέσεων τοῦ Εὐκλείδιου ἀλγόριθμου) καί τά κλάσματα,

$$\delta_1 = q_1 \quad , \quad \delta_2 = q_1 + \frac{1}{q_2} \quad , \quad \delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}} \quad , \ldots$$

λέγονται <u>ἀναγωγήματα</u>.

d) Ὁ πολύ ἁπλός τρόπος γιά τό σχηματισμό τῶν ἀναγωγημάτων συνάγεται ἄν παρατηρήσομε ὅτι τό δ_s $(s>1)$ μποροῦμε νά τό πάρομε ἀπ'τό δ_{s-1}

Ἂν ἀντικαταστήσωμε τό q_{s-1} στήν ἔκφραση τοῦ δ_{s-1} μέ τό $q_{s-1}+\frac{1}{q_s}$. Πραγματικά, ἂν γιά χάρη τῆς ὁμοιομορφίας θέσωμε $P_0=1$, $Q_0=0$, μποροῦμε τότε νά παραστήσωμε ἀναδρομικά τά ἀναγωγήματα μέ τόν ἑξῆς τρόπο (ὅταν ἐδῶ γράφωμε τήν ἰσότητα $\frac{A}{B}=\frac{P_s}{Q_s}$, θά ἐννοοῦμε ὅτι ὁ A παριστάνεται ἀπ' τό σύμβολο P_s καί ὁ B ἀπ' τό σύμβολο Q_s):

$$\delta_1=\frac{q_1}{1}=\frac{P_1}{Q_1}\quad,\quad \delta_2=\frac{q_1+\frac{1}{q_2}}{1}=\frac{q_2q_1+1}{q_2\cdot 1+0}=\frac{q_2P_1+P_0}{q_2Q_1+Q_0}=\frac{P_2}{Q_2}$$

$$\delta_3=\frac{(q_2+\frac{1}{q_3})P_1+P_0}{(q_2+\frac{1}{q_3})Q_1+Q_0}=\frac{q_3P_2+P_1}{q_3Q_2+Q_1}=\frac{P_3}{Q_3}$$

κ.λ.π. καί γενικά

$$\delta_s=\frac{q_sP_{s-1}+P_{s-2}}{q_sQ_{s-1}+Q_{s-2}}=\frac{P_s}{Q_s}$$

Ἔτσι οἱ ἀριθμητές κάι οἱ παρανομαστές τῶν ἀναγωγημάτων μποροῦν νά ὑπολογιστοῦν ἀναδρομικά μέ τή βοήθεια τῶν τύπων:

$$(2)\quad \begin{cases} P_s=q_sP_{s-1}+P_{s-2} \\ Q_s=q_sQ_{s-1}+Q_{s-2} \end{cases} \text{ γιά } s\geqslant 2\ ,\ \text{ὅπου } \begin{matrix} P_0=1\ ,\ Q_0=0 \\ P_1=q_1\ ,\ Q_1=1 \end{matrix}$$

Οἱ ὑπολογισμοί μποροῦν νά γίνουν εὔκολα μέ τή βοήθεια τοῦ παρακάτω σχήματος:

q_s		q_1	q_2	...	q_{s-2}	q_{s-1}	q_s	...	q_{n-1}	q_n
P_s	1	q_1	P_2	...	P_{s-2}	P_{s-1}	P_s	...	P_{n-1}	$P_n=a$
Q_s	0	1	Q_2	...	Q_{s-2}	Q_{s-1}	Q_s	...	Q_{n-1}	$Q_n=b$

Παράδειγμα: Ν' ἀναπτυχθεῖ ὁ ἀριθμός $\frac{105}{38}$ σέ συνεχές κλάσμα.

105 | 38 | 2
76
38 | 29 | 1
29 | 9 | 3
27
9 | 2 | 4
8
2 | 1 | 2
2 | 2
0

$$\frac{105}{38}=2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{4+\frac{1}{2}}}}$$

Ἄρα τό σχῆμα γιά τό ὁποῖο κάναμε λόγο προηγουμένως δίνει:

q_s	0	2	1	3	4	2
P_s	1	2	3	11	47	105
Q_s	0	1	1	4	17	38

e) Τώρα θεωρούμε τή διαφορά $\delta_s - \delta_{s-1}$ διαδοχικών ἀναγωγημάτων.
Γιά $s>1$ βρίσκομε:

$$\delta_s - \delta_{s-1} = \frac{P_s}{Q_s} - \frac{P_{s-1}}{Q_{s-1}} = \frac{h_s}{Q_s Q_{s-1}}$$

ὅπου $h_s = P_s Q_{s-1} - Q_s P_{s-1}$. Ἀντικαθιστώντας τά P_s καί Q_s ἀπ' τίς ἐκφράσεις τους στήν (2) καί κάνοντας τίς προφανεῖς ἁπλοποιήσεις, βρίσκομε ὅτι $h_s = -h_{s-1}$. Ἡ τελευταία ἰσότητα σέ συνδυασμό μέ τήν $h_1 = q_1 \cdot 0 - 1 \cdot 1 = -1$ δίνει $h_s = (-1)^s$. Ἔτσι

$$(3) \qquad P_s Q_{s-1} - Q_s P_{s-1} = (-1)^s \qquad (s>0)$$

$$(4) \qquad \delta_s - \delta_{s-1} = \frac{(-1)^s}{Q_s Q_{s-1}} \qquad (s>1)$$

Παράδειγμα: Στόν πίνακα τοῦ παραδείγματος πού δώσαμε στό d, ἔχομε

$$105 \cdot 17 - 38 \cdot 47 = (-1)^5 = -1$$

f) Ἀπό τήν (3) ἕπεται ὅτι ὁ (P_s, Q_s) διαιρεῖ τόν $(-1)^s = \pm 1$, $(\forall s, b, \S 1)$. Ἄρα $(P_s, Q_s) = 1$, δηλ. τά ἀναγνώσματα $\frac{P_s}{Q_s}$ εἶναι ἀνάγωγα.

g) Τώρα θά ἐρευνήσομε τό πρόσημο τῆς διαφορᾶς $\delta_s - \alpha$ γιά ἐκεῖνα τά δ_s πού εἶναι διαφορετικά ἀπ' τό α. (δηλ. ἐξαιροῦμε τήν περίπτωση στήν ὁποία τό δ_s εἶναι τό τελευταῖο ἀναγώγημα γιά τό ρητόν ἀριθμό α). Εἶναι φανερό ὅτι παίρνομε τό δ_s ἄν ἀντικαταστήσομε τόν α_s ἀπ' τόν q_s στήν ἔκφραση (1) τοῦ α. Ἀλλά εἶναι φανερό ἀπ' τό α, ὅτι σάν ἀποτέλεσμα αὐτῆς τῆς ἀντικατάστασης εἶναι

ὁ α_s νά ἐλαττώνεται
ὁ α_{s-1} νά αὐξάνει
ὁ α_{s-2} νά ἐλαττώνεται
. . . . . .
ὁ α → νά ἐλαττώνεται γιά περιττό s
ὁ α → νά αὐξάνει γιά ἄρτιο s

Ἄρα $\delta_s - \alpha < 0$ γιά περιττό s καί $\delta_s - \alpha > 0$ γιά ἄρτιο s, καί κατά συνέπεια, τό πρόσημο τοῦ $\delta_s - \alpha$ εἶναι ἐκεῖνο τοῦ $(-1)^s$

h) Ἔχομε:

$$|\alpha - \delta_{s-1}| \leqq \frac{1}{Q_s Q_{s-1}}$$

Πραγματικά, ὁ ἰσχυρισμός ἕπεται γιά $\delta_s = \alpha$ (μέ τό σύμβολο τῆς ἰσότητας) ἀπ' τήν (4). Γιά δ_s διάφορο τοῦ α ἕπεται (μέ τό σύμβολο τῆς ἀνισότητας) ἀπ' τήν (4) σέ συνδυασμό καί μέ τό γεγονός ὅτι οἱ $\delta_s - \alpha$ καί $\delta_{s-1} - \alpha$ ἔχουν διαφορετικά πρόσημα, ἐξ αἰτίας τοῦ g.

§ 5. Πρῶτοι ἀριθμοί

a) Ὁ ἀριθμός 1 ἔχει μόνον ἕνα θετικό διαιρέτη, συγκεκριμένα τόν 1. Ἐξ αἰτίας αὐτοῦ τοῦ γεγονότος ὁ ἀριθμός 1 κατέχει μοναδική θέση στήν ἀκολουθία τῶν φυσικῶν ἀριθμῶν.
Κάθε ἀκέραιος, μεγαλύτερος ἀπ' τόν 1, ἔχει τουλάχιστον δυό διαιρέτες τόν 1 καί τόν ἑαυτό του. Ἄν αὐτοί οἱ διαιρέτες εἶναι ὅλοι κι ὅλοι οἱ θετικοί διαιρέτες ἑνός ἀκεραίου, τότε αὐτός λέγεται <u>πρῶτος</u>.
Ἕνας ἀκέραιος >1 πού ἔχει κι ἄλλους θετικούς διαιρέτες ἐκτός ἀπ' τό 1 καί τόν ἑαυτό του λέμε ὅτι εἶναι <u>σύνθετος</u>.

b) <u>Ὁ ἐλάχιστος διάφορος τοῦ ἕνα, διαιρέτης ἑνός ἀκεραίου μεγαλυτέρου τοῦ ἕνα, εἶναι πρῶτος ἀριθμός.</u>
Πραγματικά, ἔστω ὅτι q εἶναι ὁ μικρότερος διαιρέτης, διάφορος τοῦ 1, ἑνός ἀκεραίου $a>1$. Ἄν ὁ q ἦταν σύνθετος, τότε θά εἶχε κάποιο διαιρέτη q_1 τέτοιον ὥστε $1<q_1<q$. Ἀλλά μιά καί ὁ a εἶναι διαιρετός ἀπ' τόν q, θά εἶναι ἐπίσης διαιρετός ἀπ' τόν q_1 $(1,b,\S1)$ καί αὐτό ἔρχεται σέ ἀντίθεση μέ τήν ὑπόθεσή μας σχετικά μέ τόν q.

c) <u>Ὁ ἐλάχιστος, διάφορος τοῦ ἕνα, διαιρέτης ἑνός συνθέτου ἀριθμοῦ a (ἀπ' τό b αὐτός θά εἶναι πρῶτος) δέν ὑπερβαίνει τόν $\sqrt{a}$.</u>
Πραγματικά, ἔστω q αὐτός ὁ διαιρέτης· τότε $a=qa_1$, $a_1\geqslant q$, ἀπ' ὅπου πολλαπλασιάζοντας μέ q, παίρνομε $a\geqslant q^2$, $q\leqslant\sqrt{a}$.

d) <u>Τό πλῆθος τῶν πρώτων εἶναι ἄπειρο.</u>
Ἡ ἰσχύς αὐτοῦ τοῦ θεωρήματος ἕπεται ἀπ' τό γεγονός ὅτι ὁποιουσδήποτε διαφορετικούς πρώτους $P_1,P_2,\dots,P_k$ κι ἄν θεωρήσουμε, μποροῦμε νά πάρομε ἕνα νέο πρῶτο πού δέν συμπεριλαμβάνεται ἀναμεσά τους. Ἕνας τέτοιος πρῶτος εἶναι ὁ ὁποιοσδήποτε πρῶτος διαιρέτης τοῦ ἀθροίσματος $P_1P_2\cdots P_k+1$, ὁ ὁποῖος μέ τό νά διαιρεῖ ὅλο τό ἄθροισμα, δέ μπορεῖ νά ταυτίζεται μέ κανέναν ἀπ' τούς πρώτους $P_1,P_2,\dots,P_k$ $(2,b,\S1)$.

e) Ὑπάρχει μιά ἁπλή μέθοδος πού ὀνομάζεται <u>κόσκινο τοῦ Ἐρατοσθένη</u>, γιά τό σχηματισμό ἑνός πίνακα τῶν πρώτων πού δέν ὑπερβαίνουν ἕνα δοσμένο N. Συνίσταται στό ἑξῆς:
Καταγράφουμε τούς ἀριθμούς
(1) $\qquad 1,2,\dots,N$
Ὁ πρῶτος ἀριθμός αὐτῆς τῆς ἀκολουθίας πού εἶναι μεγαλύτερος ἀπ' τόν 1 εἶναι ὁ 2· αὐτός διαιρεῖται μόνον ἀπ' τόν 1 καί τόν ἑαυτό του, ἄρα εἶναι πρῶτος, διαγράφομε ἀπ' τήν ἀκολουθία (1) (μιά πού εἶναι σύνθετοι ἀριθμοί) ὅλους τούς ἀριθμούς πού εἶναι πολλαπλάσια τοῦ 2 ἐκτός ἀπ' τόν ἴδιο τόν 2.

Ὁ ἀμέσως ἑπόμενος ἀριθμός μετά τό 2 πού δέν διαγράφτηκε εἶναι ὁ 3 . δέν διαιρεῖται ἀπ' τόν 2 (γιατί ἀλλοιῶς θά εἶχε διαγραφεῖ) ἀπότε ὁ 3 διαιρεῖται μόνον ἀπ' τόν 1 καί τόν ἑαυτό του, ὅρα εἶναι ἐπίσης πρῶτος. Διαγράφομε ἀπ' τήν ἀκολουθία (1) ὅλους τούς ἀριθμούς πού εἶναι πολλαπλάσια τοῦ 3 , ἐκτός ἀπ' τόν ἴδιο τόν 3 . Ὁ ἀμέσως ἑπόμενος ἀριθμός μετά τόν 3 πού δέν ἔχει διαγραφτεῖ εἶναι ὁ 5 . δέν διαιρεῖται οὔτε ἀπ' τόν 2 οὔτε ἀπ' τόν 3 (ἀλλοιῶς θά εἶχε διαγραφτεῖ), ὁπότε διαιρεῖται μόνο ἀπ' τόν 1 καί τόν ἑαυτό του καί γι' αὐτό -εἶναι ἐπίσης πρῶτος κ.ὅ.κ. Ὅταν μ' αὐτή τή διαδικασία ἔχουν διαγραφτεῖ ὅλοι οἱ ἀριθμοί πού εἶναι πολλαπλάσια πρώτων μικροτέρων ἀπ' τόν πρῶτο p , τότε ὅλοι οἱ ἀριθμοί πού παραμένουν κάί εἶναι μικρότεροι ἀπ' τόν p^2 , εἶναι πρῶτοι. Πραγματικά, κάθε σύνθετος ἀριθμός a , μικρότερος ἀπ' τόν p^2 ἔχει ἤδη διαγραφτεῖ ἀφοῦ εἶναι πολλαπλάσιο τοῦ μικροτέρου πρώτου διαιρέτη του, ὁ ὁποῖος εἶναι $\leq \sqrt{a} < p$. Αὐτό συνεπάγεται:

1. Στή διαδικασία τῆς διαγραφῆς τῶν πολλαπλασίων τοῦ πρώτου p , αὐτό τό σύνολο τῶν διαγραφομένων ἀριθμῶν πρέπει ν' ἀρχίζει μέ τόν p^2;
2. Ὁ σχηματισμός τοῦ πίνακα τῶν πρώτων τῶν $\leq N$ εἶναι πλήρης ἅπαξ καί διαγράφομε ὅλους τούς σύνθετους, πού εἶναι πολλαπλάσια πρώτων τά ὁποῖα δέν ὑπερβαίνουν τόν $\sqrt{N}$.

§ 6. Τό μονότροπο τῆς ἀνάλυσης σέ πρώτους παράγοντες

a) Κάθε ἀκέραιος a εἶναι εἴτε πρῶτος πρός ἕνα δοσμένο πρῶτο p , ἤ διαιρεῖται ἀπ' τόν p.

Πραγματικά, $d(a,p)$ εἶναι διαιρέτης τοῦ p ἄρα θά εἶναι εἴτε ὁ 1 , εἴτε ὁ p . Στήν πρώτη περίπτωση, ὁ a εἶναι πρῶτος πρός τόν p , καί στή δεύτερη, ὁ a διαιρεῖται ἀπ' τόν p .

b) Ἄν τό γινόμενο μερικῶν παραγόντων εἶναι διαιρετό ἀπ' τόν p τότε τουλάχιστόν ἕνας ἀπ' τούς παράγοντες εἶναι διαιρετός ἀπ' τόν p .

Πραγματικά (a), κάθε ὅρος εἴτε διαιρεῖται ἀπ' τόν p , εἴτε εἶναι πρῶτος πρός τόν p . Ἄν ὅλοι οἱ ὅροι ἦταν πρῶτοι πρός τόν p , τότε τό γινόμενό τους (3, f, § 2) θά ἦταν πρῶτο πρός τόν p . Ὅρα ἕνας τουλάχιστον ὅρος εἶναι διαιρετός ἀπ' τόν p .

c) Κάθε ἀκέραιος μεγαλύτερος ἀπ' τόν ἕνα μπορεῖ νά ἀναλυθεῖ σέ γινόμενο πρώτων παραγόντων καί, μάλιστα, κατά μοναδικό τρόπο, ἄν παραβλέψομε τή σειρά τῶν παραγόντων.

Πραγματικά, ἔστω a ἕνας ἀκέραιος μεγαλύτερος ἀπ' τή μονάδα· ἄν p_1 εἶναι ὁ ἐλάχιστος πρῶτος διαιρέτης του, θά ἔχομε $a=p_1a_1$. Ἄν $a_1>1$ καί p_2 εἶναι ὁ ἐλάχιστος πρῶτος διαιρέτης του, θά ἔχομε $a_1=p_2a_2$. Ἄν $a_2>1$, τότε, ἀκριβῶς μέ τόν ἴδιο τρόπο βρίσκομε $a_2=p_3a_3$ κ.λ.π. μέχρι νά φτάσομε σέ κά-

ποιο q_n ίσο μέ ένα. Τότε $q_{n-1}=p_1$. Πολλαπλασιάζοντας όλες αυτές τις εξισώσεις και απλοποιώντας, παίρνομε τήν παρακάτω ανάλυση τού a σέ πρώτους παράγοντες:

$$a=p_1p_2\cdots p_n$$

Ας υποθέσομε ότι υπάρχει μιά δεύτερη ανάλυση τού ίδιου a σέ πρώτους παράγοντες, $a=q_1q_2\cdots q_s$. Τότε

$$p_1p_2\cdots p_n=q_1q_2\cdots q_s$$

Τό δεξιό μέλος αύτής τής ισότητας είναι διαιρετό άπ' τόν q_1. Άρα (b), τουλάχιστον ένας άπ' τούς παράγοντες τού αριστερού μέλους πρέπει νά είναι διαιρετός άπ' τόν q_1. Π.χ. Έστω ότι ό p_1 είναι διαιρετός άπ' τόν q_1, τότε $p_1=q_1$ (γιατί ό p_1 είναι διαιρετός μόνο άπ' τόν p_1 άν εξαιρέσομε τόν 1). Διαιρώντας και τά δύο μέλη τής ισότητας μέ $p_1=q_1$, έχομε $p_2p_3\cdots p_n=q_2q_3\cdots q_s$. Επαναλαμβάνοντας τήν προηγούμενη επιχειρηματολογία γι' αύτή τήν ισότητα, βρίσκομε $p_2\cdots p_n=q_3\cdots q_s$, κ.λ.π. μέχρι πού βρίσκομε τελικά ότι όλοι οί παράγοντες τού ενός μέλους, τού αριστερού άς πούμε, διαγράφονται μέ τις διαδοχικές διαιρέσεις. Άλλά όλοι οί παράγοντες τού δεξιού μέλους πρέπει νά έχουν συγχρόνως διαγραφτεί μιά κάι ή ισότητα $1=q_{n+1}\cdots q_s$, γιά $q_{n+1}\cdots q_s$ μεγαλύτερους άπό ένα είναι άδύνατη. Γι' αύτό ή δεύτερη ανάλυση σέ πρώτους παράγοντες ταυτίζεται μέ τήν πρώτη.

d) Στήν ανάλυση τού αριθμού a σέ πρώτους παράγοντες, μερικοί άπ' αύτούς μπορεί νά επαναλαμβάνονται. Άν $p_1,p_2,\cdots,p_k$ είναι οί διαφορετικοί πρώτοι και οί $\alpha_1,\alpha_2,\cdots,\alpha_k$ δείχνουν πόσες φορές εμφανίζεται ό αντίστοιχος πρώτος στήν ανάλυση τού a, παίρνομε τή λεγόμενη <u>κανονική ανάλυση τού a σέ παράγοντες</u>.

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

Παράδειγμα: Η κανονική ανάλυση τού αριθμού 588000 είναι: $588000=2^5\cdot3\cdot5^3\cdot7^2$

e) Έστω $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ ή κανονική ανάλυση τού αριθμού a. Τότε όλοι οί διαιρέτες τού a είναι έκείνοι άκριβώς οί αριθμοί τής μορφής:

$$d=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k} \qquad (1)$$

$$0\leq\beta_1\leq\alpha_1,\ 0\leq\beta_2\leq\alpha_2,\ \ldots,\ 0\leq\beta_k\leq\alpha_k$$

Πραγματικά, έστω ότι ό d διαιρεί τόν a. Τότε (b, §1) $a=dq$, άρα, όλοι οί πρώτοι διαιρέτες τού d εμφανίζονται στήν κανονική ανάλυση τού a μέ εκθέτες όχι μικρότερους άπό έκείνους μέ τούς οποίους εμφανίζονται στήν κανονική ανάλυση τού d. Άρα ό d έχει τή μορφή (1). Αντίστροφα, κάθε d τής μορφής (1), προφανώς διαιρεί τόν a.

Παράδειγμα: Μπορούμε νά πάρουμε όλους τούς διαιρέτες τοῦ ἀριθμοῦ $720=2^4 3^2 5$, ἄν θεωρήσουμε ὅτι οἱ b_1,b_2,b_3 στόν $2^{b_1}3^{b_2}5^{b_3}$ διατρέχουν, ἀνεξάρτητα ὁ ἕνας ἀπ' τόν ἄλλο, τίς τιμές $b_1=0,1,2,3,4$; $b_2=0,1,2$ * $b_3=0,1$
Ἄρα αὐτοί οἱ διαιρέτες εἶναι: 1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 9, 18, 36, 72, 144, 5, 10, 20, 40, 80, 15, 30, 60, 120, 240, 45, 90, 180, 360, 720

Οἱ παραπάνω σελίδες εἶναι μετάφραση [redacted] τοῦ βιβλίου τοῦ I.M. VINOGRADOV "Στοιχεῖα τῆς Θεωρίας τῶν Ἀριθμῶν" (Ἀγγλική ἔκδοση) Κεφ. I

ΚΕΦΑΛΑΙΟ ΙΙ

ΣΗΜΑΝΤΙΚΕΣ ΑΡΙΘΜΟΘΕΩΡΗΤΙΚΕΣ ΣΥΝΑΡΤΗΣΕΙΣ

Του Σ.Κ. Πηχωρίδη

Μετάφραση από: I.M. VINOGRADOV, ELEMENTS OF NUMBER THEORY, DOVER 1954, σελ. 21-28

§1. Οι συναρτήσεις $[\chi]$, $\{\chi\}$.

α. Η συναρτηση $[\chi]$ παίζει σημαντικό ρόλο στή θεωρία τῶν ἀριθμῶν· ὁρίζεται γιά ὅλους τούς πραγματικούς ἀριθμούς χ καί εἶναι ὁ μεγαλύτερος ἀκέραιος πού δέν ξεπερνᾶ τό χ. Η συνάρτηση αὐτή ὀνομάζεται τό ἀκέραιο μέρος τοῦ χ.

Παραδείγματα.

$[7]=7$, $[2,6]=2$, $[-4,75]=-5$.

Η συνάρτηση $\{\chi\}=\chi-[\chi]$ καλεῖται τό κλασματικό μέρος τοῦ χ. Καί αὐτή ἡ συνάρτηση συναντιέται μερικές φορές στή θεωρία τῶν ἀριθμῶν.

Παραδείγματα.

$\{7\}=0$, $\{2,6\}=0,6$, $\{-4,75\}=0,25$.

β. Γιά νά δοῦμε ὅτι πραγματικά εἶναι χρήσιμες αὐτές οἱ συναρτήσεις, δείχνουμε τό ἑξῆς θεώρημα:

Η δύναμη μέ τήν ὁποία ἕνας πρῶτος p ἐμφανίζεται στήν ἀνάλυση τοῦ γινομένου $n!$ ἰσοῦται μέ

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\dots$$

Πραγματικά, ὁ ἀριθμός τῶν παραγόντων τοῦ $n!$ πού εἶναι πολλαπλάσια τοῦ p εἶναι $\left[\frac{n}{p}\right]$. Ἀπό αὐτούς τά πολλαπλάσια τοῦ p^2 εἶναι $\left[\frac{n}{p^2}\right]$, ἀπό αὐτά τά πολλαπλάσια [illegible] τοῦ p^3 εἶναι $\left[\frac{n}{p^3}\right]$ κ.ο.κ. Τό ἄθροισμα τῶν ἀριθμῶν αὐτῶν δίνει τήν ζητουμένη δύναμη, διότι ἄν p^μ εἶναι ἡ μεγαλύτερη δύναμη τοῦ p πού διαιρεῖ ἕνα παράγοντα κ τοῦ n. (Ἐκεῖνον), τότε ὁ κ ἔχει μετρηθεῖ μ φορές ἀκριβῶς (σάν πολλαπλάσιο τοῦ p, τοῦ p^2, ..., τοῦ p^μ).

Παράδειγμα. Η μεγαλύτερη δύναμη τοῦ 3 πού διαιρεῖ τό $40!$ εἶναι

$$\left[\frac{40}{3}\right]+\left[\frac{40}{9}\right]+\left[\frac{40}{27}\right]=13+4+1=18 .$$

§2. Ἀθροίσματα πάνω στούς διαιρέτες ἑνός ἀριθμοῦ.

α. Οἱ πολλαπλασιαστικές συναρτήσεις παίζουν σημαντικό ρόλο στή θεωρία τῶν ἀριθμῶν. Μία συνάρτηση θ(α) λέγεται πολλαπλασιαστική ἄν ἱκανοποιοῦνται οἱ ἑξῆς συνθῆκες:

1. Ἡ συνάρτηση θ(α) ὁρίζεται γιά ὅλους τούς θετικούς ἀκεραίους α καί γιά μία τοὐλάχιστον τιμή τοῦ α εἶναι διάφορη τοῦ μηδενός.

2. Γιά ὁποιουσδήποτε σχετικά πρώτους θετικούς ἀκεραίους α_1 καί α_2 ἔχουμε:

$$\theta(\alpha_1\alpha_2)=\theta(\alpha_1)\theta(\alpha_2) .$$

Παράδειγμα. Εἶναι εὔκολο νά δοῦμε ὅτι ἡ συνάρτηση $\theta(\alpha)=\alpha^s$, ὅπου s τυχαῖος πραγματικός ἤ μιγαδικός ἀριθμός, εἶναι πολλαπλασιαστική.

β. Ἀπό τίς παραπάνω ἰδιότητες τῆς συνάρτησης θ(α) προκύπτει εἰδικώτερα ὅτι θ(1)=1. Πραγματικά, ἄν $\theta(\alpha_0)\neq 0$, τότε $\theta(\alpha_0)=\theta(1.\alpha_0)=$ $=\theta(1)\theta(\alpha_0)$, δηλ. θ(1)=1. Ἐπιπλέον ἔχουμε τήν ἑξῆς σημαντική ἰδιότητα: Ἄν $\theta_1(\alpha)$ καί $\theta_2(\alpha)$ εἶναι πολλαπλασιαστικές συναρτήσεις, τότε ἡ $\theta_0(\alpha)=\theta_1(\alpha)\theta_2(\alpha)$ εἶναι ἐπίσης πολλαπλασιαστική συνάρτηση. Πραγματικά ἔχουμε $\theta_0(1)=\theta_1(1)\theta_2(1)=1$. Ἀκόμα, γιά $(\alpha_1,\alpha_2)=1$, βρίσκουμε

$$\theta_0(\alpha_1\alpha_2)=\theta_1(\alpha_1\alpha_2)\theta_2(\alpha_1\alpha_2)=\theta_1(\alpha_1)\theta_1(\alpha_2)\theta_2(\alpha_1)\theta_2(\alpha_2)=$$
$$=\theta_1(\alpha_1)\theta_2(\alpha_1)\theta_1(\alpha_2)\theta_2(\alpha_2)=\theta_0(\alpha_1)\theta_0(\alpha_2) .$$

γ. Ἔστω θ(α) μία πολλαπλασιαστική συνάρτηση καί ἔστω $\alpha=\rho_1^{\alpha_1}\rho_2^{\alpha_2}\dots\rho_\kappa^{\alpha_\kappa}$ ἡ κανονική ἀνάλυση τοῦ ἀριθμοῦ α. Τότε, σημειώνοντας μέ τό σύμβολο $\sum_{\delta/\alpha}$ τό ἄθροισμα πού ἐκτείνεται πάνω σέ ὅλους τούς διαιρέτες δ τοῦ ἀκεραίου α, ἔχουμε

$$\sum_{\delta/\alpha}\theta(\delta)=(1+\theta(\rho_1)+\theta(\rho_1^2)+\dots+\theta(\rho_1^{\alpha_1}))\dots(1+\theta(\rho_\kappa)+\theta(\rho_\kappa^2)+\dots+\theta(\rho_\kappa^{\alpha_\kappa}))$$

(ἄν α=1, τό δεξιό μέλος θεωρεῖται ἴσο μέ 1).

Γιά νά δείξουμε αὐτή τήν ταυτότητα, ἐκτελοῦμε τούς πολλαπλασιασμούς στό δεξιό μέλος, ὁπότε βρίσκουμε ἕνα ἄθροισμα ὅρων τῆς μορφῆς

$$\theta(\rho_1^{\beta_1})\theta(\rho_2^{\beta_2})\dots\theta(\rho_\kappa^{\beta_\kappa})=\theta(\rho_1^{\beta_1}\rho_2^{\beta_2}\dots\rho_\kappa^{\beta_\kappa}),\quad 0\leq\beta_1\leq\alpha_1,\ 0\leq\beta_2\leq\alpha_2,\dots,0\leq\beta_\kappa\leq\alpha_\kappa,$$

Παίρνουμε μέλιστα ὅλους τοὺς ὅρους ποὺ ἀντιστοιχοῦν στὶς παραπάνω ἀνισότητες ἀκριβῶς μία φορὰ τὸν καθένα. Σύμφωνα λοιπὸν μὲ ὅτι μάθαμε στὴν ἀρχὴ τοῦ προηγουμένου κεφαλαίου, τὸ δεξιὸ μέλος συμπίπτει μὲ τὸ ἀριστερό.

δ. Γιὰ $\theta(a)=a^c$ ἡ ταυτότητα τῆς ὑποπαραγράφου 2γ παίρνει τὴν μορφὴ

$$(I)\quad \sum_{\delta/a} \delta^c=(I+p_I^c+p_I^{2c}+\ldots+p_I^{\alpha_I c})\ldots(I+p_\kappa^c+p_\kappa^{2c}+\ldots+p_\kappa^{\alpha_\kappa c}).$$

Εἰδικώτερα γιὰ $c=I$, τὸ ἀριστερὸ μέλος τῆς (I) παριστάνει τὸ ἄθροισμα τῶν διαιρετῶν $S(a)$ τοῦ ἀριθμοῦ a. Ἀθροίζοντας τὶς γεωμετρικὲς προόδους στὸ δεξιὸ μέλος βρίσκουμε

$$S(a)=\frac{p_I^{\alpha_I+I}-I}{p_I-I}\cdot\frac{p_2^{\alpha_2+I}-I}{p_2-I}\cdot\ldots\cdot\frac{p_\kappa^{\alpha_\kappa+I}-I}{p_\kappa-I}.$$

Παράδειγμα.

$$S(720)=\frac{2^{4+I}-I}{2-I}\cdot\frac{3^{2+I}-I}{3-I}\cdot\frac{5^{I+I}-I}{5-I}=2418.$$

Γιὰ $c=0$, τὸ ἀριστερὸ μέλος τῆς (I) παριστάνει τὸ πλῆθος τῶν διαιρετῶν $\gamma(a)$ τοῦ ἀριθμοῦ a καὶ ἔχουμε

$$\gamma(a)=(\alpha_I+I)(\alpha_2+I)\ldots(\alpha_\kappa+I).$$

Παράδειγμα.

$$\gamma(720)=(4+I)(2+I)(I+I)=30.$$

§3. Ἡ συνάρτηση τοῦ MÖBIUS.

α. Ἡ συναρτηση $\mu(a)$ τοῦ MÖBIUS ὁρίζεται γιὰ ὅλους τοὺς θετικοὺς ἀκεραίους a. Δίνεται ἀπὸ τὶς ἐξισώσεις: $\mu(a)=0$, ἂν ὁ a διαιρεῖται μὲ ἕνα τετράγωνο $\neq I$: $\mu(a)=(-I)^\kappa$, ἂν ὁ a δὲν διαιρεῖται μὲ τετράγωνο $\neq I$, ὅπου κ συμβολίζει τὸ πλῆθος τῶν πρώτων διαιρετῶν τοῦ a. Εἰδικώτερα, γιὰ $a=I$, παίρνουμε $\kappa=0$ καὶ ἑπομένως $\mu(I)=I$.

Παραδείγματα.

$\mu(I)=I$, $\mu(2)=-I$, $\mu(3)=-I$, $\mu(4)=0$, $\mu(5)=-I$, $\mu(6)=I$, $\mu(7)=-I$, $\mu(8)=0$, $\mu(9)=0$, $\mu(10)=I$, $\mu(11)=-I$, $\mu(12)=0$.

β. Έστω $\theta(\alpha)$ μία πολλαπλασιαστική συνάρτηση καί έστω ότι $\alpha=\rho_1^{\alpha_1}\rho_2^{\alpha_2}\dots\rho_\kappa^{\alpha_\kappa}$ είναι ή κανονική άνάλυση τού άριθμού α. Τότε

$$\sum_{\delta/\alpha}\mu(\delta)\theta(\delta)=(1-\theta(\rho_1))(1-\theta(\rho_2))\dots(1-\theta(\rho_\kappa)).$$

(Έάν $\alpha=1$, τό δεξιό μέλος θεωρείται ίσο μέ 1).

Πραγματικά είναι προφανές ότι ή μ είναι πολλαπλασιαστική. Συνάγουμε ότι ή συνάρτηση $\theta_1(\alpha)=\theta(\alpha)\mu(\alpha)$ είναι έπίσης πολλαπλασιαστική. Έφαρμόζοντας τήν ταυτότητα τής ύποπαραγράφου 2γ καί παρατηρώντας ότι $\theta_1(\rho)=-\theta(\rho)$, $\theta_1(\rho^\varsigma)=0$, γιά $\varsigma>1$, συμπληρώνουμε τήν άπόδειξη.

γ. Είδικότερα, θέτοντας $\theta(\alpha)=1$, παίρνουμε

$$\sum_{\delta/\alpha}\mu(\delta)=\begin{cases}0, & \text{έάν } \alpha>1\\ 1, & \text{έάν } \alpha=1\end{cases}$$

θέτοντας $\theta(\delta)=\frac{1}{\delta}$, βρίσκουμε

$$\sum_{\delta/\alpha}\frac{\mu(\delta)}{\delta}=\begin{cases}(1-\frac{1}{\rho_1})(1-\frac{1}{\rho_2})\dots(1-\frac{1}{\rho_\kappa}), & \text{έάν } \alpha>1\\ 1, & \text{έάν } \alpha=1\end{cases}.$$

δ. Δίνονται ν θετικοί άκέραιοι $\delta_1,\delta_2,\dots,\delta_\nu$ καί οί πραγματικοί (ή μιγαδικοί) άριθμοί $\lambda_1,\lambda_2,\dots,\lambda_\nu$. Γράφουμε S' γιά τό άθροισμα τών λ_κ γιά τούς δείκτες $\kappa=1$ καί S_δ γιά τό άθροισμα τών λ_κ γιά τούς δείκτες τό δ_κ είναι πολλαπλάσιο τού δ. Τότε έχουμε

$$S'=\sum\mu(\delta)S_\delta,$$

όπου τό άθροισμα έκτείνεται πάνω σέ όλους τούς θετικούς άκεραίους πού διαιροῦν τουλάχιστον ένα άπό τούς άριθμούς $\delta_1,\delta_2,\dots,\delta_\nu$.

Πραγματικά, σύμφωνα μέ ότι δείξαμε στήν §3γ, θά έχουμε

$$S'=\lambda_1\sum_{\delta/\delta_1}\mu(\delta)+\lambda_2\sum_{\delta/\delta_2}\mu(\delta)+\dots+\lambda_\nu\sum_{\delta/\delta_\nu}\mu(\delta).$$

Έστω τώρα δ ένας θετικός άκέραιος πού διαιρεί κάποιον άπό τούς $\delta_1,\delta_2,\dots,\delta_\nu$. Ό όρος $\mu(\delta)$ θά έμφανίσθεί στά άθροίσματα $\sum_{\delta/\delta_\kappa}\mu(\delta)$ γιά τά δείκτα δ/δ_κ καί έπομένως ή συνεισφορά του στό S' θά είναι $S_\delta\mu(\delta)$. Ή παρατήρηση αύτή άποδεικνύει τή ζητουμένη ίσότητα.

§4. Η συνάρτηση του EULER.

α. Η συνάρτηση του EULER $\varphi(\alpha)$ ορίζεται για όλους τους θετικούς ακεραίους α και παριστάνει το πλήθος των αριθμών της πεπερασμένης ακολουθίας

(I) $0,1,\dots,\alpha-1$

που είναι πρώτοι προς τον α.

Παραδείγματα.

$\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$.

β. Έστω

(2) $\alpha=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_\kappa^{\alpha_\kappa}$

η κανονική ανάλυση του αριθμού α. Τότε

(3) $\varphi(\alpha)=\alpha(1-\frac{1}{p_1})(1-\frac{1}{p_2})\dots(1-\frac{1}{p_\kappa})$,

ή ακόμα

(4) $\varphi(\alpha)=(p_1^{\alpha_1}-p_1^{\alpha_1-1})(p_2^{\alpha_2}-p_2^{\alpha_2-1})\dots(p_\kappa^{\alpha_\kappa}-p_\kappa^{\alpha_\kappa-1})$.

Ειδικώτερα

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

Πραγματικά αρκεί να εφαρμόσουμε το θεώρημα της υποπαραγράφου 3δ. Εδώ οι αριθμοί δ και λ ορίζονται ως εξής: Σε κάθε χ της ακολουθίας (I) αντιστοιχούμε τους αριθμούς $\delta_\chi=(\chi,\alpha)$, $\chi=1,2,\dots,\alpha-1$, και $\lambda=1$. Τότε το s'είναι το πλήθος των χ για τα οποία $\delta_\chi=1$, δηλ. $s=\varphi(\alpha)$. Το s_δ είναι το πλήθος των χ για τα οποία το δ_χ είναι πολλαπλάσιο του δ. Παρατηρούμε τώρα ότι αν το $\delta_\chi=(\chi,\alpha)$ είναι πολλαπλάσιο του δ, τότε αναγκαστικά το δ είναι διαιρέτης του α και το s_δ είναι το πλήθος των όρων της (I) που είναι πολλαπλάσια του δ, δηλ. $s_\delta=\frac{\alpha}{\delta}$. Συνάγουμε λοιπόν ότι

$$\varphi(\alpha)=\sum_{\delta/\alpha}\mu(\delta)\frac{\alpha}{\delta},$$

οπότε ο τελευταίος τύπος της υποπαραγράφου 3γ δίνει την (3). Η (4) είναι άμεση συνέπεια των (2) και (3).

Παραδείγματα.

$\varphi(60)=60(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})=16$

$\varphi(81)=81-27=54$

$\varphi(5)=5-1=4.$

γ. Η συνάρτηση $\varphi(\alpha)$ είναι πολλαπλασιαστική.

Πραγματικά άν $(\alpha_1,\alpha_2)=1$, τότε ή (3) δίνει άμεσα

$\varphi(\alpha_1\alpha_2)=\varphi(\alpha_1)\varphi(\alpha_2)$.

Παράδειγμα.

$\varphi(405)=\varphi(81)\varphi(5)=54.4=216.$

δ. $\sum_{\delta/\alpha}\varphi(\delta)=\alpha.$

Για νά δείξουμε αύτό τόν τύπο έφαρμόζουμε τήν ταυτότητα τής ύποπαραγράφου 2γ, ή όποία γιά $\theta(\alpha)=\varphi(\alpha)$ δίνει

$$\sum_{\delta/\alpha}\varphi(\delta)=(1+\varphi(p_1)+\ldots+\varphi(p_1^{\alpha_1}))\ldots(1+\varphi(p_\kappa)+\ldots+\varphi(p_\kappa^{\alpha_\kappa})).$$

Χρησιμοποιώντας τήν (5) βρίσκουμε ότι τό δεξιό μέλος ίσούται μέ

$$(1+(p_1-1)+(p_1^2-p_1)+\ldots+(p_1^{\alpha_1}-p_1^{\alpha_1-1}))\ldots(1+(p_\kappa-1)-\ldots+(p_\kappa^{\alpha_\kappa}-p_\kappa^{\alpha_\kappa-1})).$$

Η τελευταία παράσταση μετά τίς άπλοποιήσεις δίνει $p_1^{\alpha_1}\ldots p_\kappa^{\alpha_\kappa}=\alpha.$

Παράδειγμα. Θέτοντας $\alpha=12$, βρίσκουμε

$\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12)=1+1+2+2+2+4=12.$

ΚΕΦΑΛΑΙΟ ΙΙΙ
Ι Σ Ο Τ Ι Μ Ι Ε Σ

§1. Β α σ ι κ έ ς ά ρ χ έ ς.

a. Θά θεωρούμε τούς ἀκεραίους σέ σχέση μέ τά ὑπόλοιπα πού προκύπτουν ἀπ' τή διαίρεσή τους μ' ἕνα δοσμένο θετικό ἀκέραιο m, τόν ὁποῖο θά ὀνομάζουμε μέτρο. Σέ κάθε ἀκέραιο ἀντιστοιχεῖ ἕνα μοναδικό ὑπόλοιπο, πού προκύπτει ἀπ' τή διαίρεσή του μέ τόν m $(c, §1, Κεφ. I)^*$. Ἄν τό ἴδιο ὑπόλοιπο r ἀντιστοιχεῖ σέ δυό ἀκεραίους a καί b, τότε θά λέμε ὅτι αὐτοί οἱ ἀκέραιοι εἶναι ἰσότιμοι ὡς πρός μέτρο m.

b. Ἡ ἰσοτιμία τῶν ἀριθμῶν a καί b ὡς πρός μέτρο m γράφεται

$$a \equiv b \pmod m$$

καί διαβάζεται: Ὁ a εἶναι ἰσότιμος πρός τόν b ὡς πρός μέτρο m.

c. Ἡ ἰσοτιμία τῶν ἀριθμῶν a καί b ὡς πρός μέτρο m, εἶναι ἰσοδύναμη μέ:

1. Τή δυνατότητα νά παραστήσουμε τόν a μέ τή μορφή $a=b+mt$, ὅπου t εἶναι ἀκέραιος.
2. Τή διαιρετότητα τοῦ $a-b$ ἀπ' τόν m.

Πραγματικά, ἀπ' τή σχέση $a \equiv b \pmod m$ ἕπεται ὅτι

$$a = mq + r \quad , \quad b = mq_1 + r \quad , \quad 0 \leq r < m$$

ἀπ' ὅπου

$$a - b = m(q - q_1) \quad , \quad a = b + mt \quad , \quad t = q - q_1$$

Ἀντίστροφα, ἀπ' τή σχέση $a=b+mt$, ἄν παραστήσουμε τό b μέ τή μορφή

$$b = mq_1 + r \quad , \quad 0 \leq r < m$$

συνάγομε

$$a = mq + r \quad , \quad q = q_1 + t$$

δηλ.

$$a \equiv b \pmod m$$

ἀποδεικνύοντας ἔτσι τόν ἰσχυρισμό 1.

Ὁ ἰσχυρισμός 2. προκύπτει ἀμέσως ἀπ' τόν ἰσχυρισμό 1.

§2. Ἰδιότητες τῶν ἰσοτιμιῶν ὅμοιες μ' ἐκεῖνες τῶν ἐξισώσεων

a. Δυό ἀριθμοί πού εἶναι ἰσότιμοι μ' ἕνα τρίτο εἶναι καί μεταξύ τους ἰσότιμοι. Λύνω ἕπεται ἀπ' τό $a, §1$

b. Οἱ ἰσοτιμίες μποροῦν νά προστεθοῦν κατά μέλη

Πραγματικά, ἔστω

(1) $a_1 \equiv b_1 (\mathrm{mod} m)$, $a_2 \equiv b_2 (\mathrm{mod} m)$, ... , $a_\kappa \equiv b_\kappa (\mathrm{mod} m)$

δότε $(1, c, \S 1)$

(2) $a_1 = b_1 + mt_1$, $a_2 = b_2 + mt_2$, ... , $a_\kappa = b_\kappa + mt_\kappa$

ἄρα

$$a_1 + a_2 + \cdots + a_\kappa = b_1 + b_2 + \cdots + b_\kappa + m(t_1 + t_2 + \cdots + t_\kappa)$$

ἢ $(1, c, \S 1)$

$$a_1 + a_2 + \cdots + a_\kappa \equiv b_1 + b_2 + \cdots + b_\kappa (\mathrm{mod} m)$$

• Ἕνας προσθετέος σέ κάποιο μέλος μιᾶς ἰσοτιμίας μπορεῖ νά μεταφερθεῖ στό ἄλλο μέλος μέ ἀλλαγμένο τό πρόσημο.

Πράγματικά, προσθέτοντας τήν ἰσοτιμία $a + b \equiv c (\mathrm{mod} m)$ στήν προφανῆ ἰσοτιμία $-b \equiv -b (\mathrm{mod} m)$, βρίσκουμε $a \equiv c - b (\mathrm{mod} m)$

Κάθε ἀριθμός πού εἶναι πολλαπλάσιο τοῦ μέτρου μπορεῖ νά προστεθεῖ σέ (ἢ νά ἀφαιρεθεῖ ἀπό) ὁποιοδήποτε μέλος μιᾶς ἰσοτιμίας.

Πράγματικά, προσθέτοντας τήν ἰσοτιμία $a \equiv b (\mathrm{mod} m)$ στήν προφανῆ ἰσοτιμία $mk \equiv 0 (\mathrm{mod} m)$ παίρνουμε $a + mk \equiv b (\mathrm{mod} m)$

β. Οἱ ἰσοτιμίες μποροῦν νά πολλαπλασιαστοῦν κατά μέλη.

Πραγματικά, θεωροῦμε ξανά τίς ἰσοτιμίες (1), ἀπ' τίς ὁποῖες συνάγουμε τίς ἐξισώσεις (2). Πολλαπλασιάζοντας τίς ἐξισώσεις (2) κατά μέλη βρίσκουμε

$$a_1 a_2 \cdots a_\kappa = b_1 b_2 \cdots b_\kappa + mN$$

ὅπου ὁ N εἶναι ἕνας ἀκέραιος. Κατά συνέπεια $(1, c, \S 1)$

$$a_1 a_2 \cdots a_\kappa \equiv b_1 b_2 \cdots b_\kappa (\mathrm{mod} m)$$

Καί τά δύο μέλη μιᾶς ἰσοτιμίας μποροῦν νά ὑψωθοῦν στήν ἴδια δύναμη

Αὐτό προκύπτει ἀπ' τό προηγούμενο θεώρημα.

Καί τό δυό μέλη μιᾶς ἰσοτιμίας μποροῦν νά πολλαπλασιαστοῦν μέ τόν ἴδιον ἀκέραιο

Πραγματικά, πολλαπλασιάζοντας τήν ἰσοτιμία $a \equiv b (\mathrm{mod} m)$ μέ τήν προφανῆ ἰσοτιμία $\kappa \equiv \kappa (\mathrm{mod} m)$, βρίσκουμε $a\kappa \equiv b\kappa (\mathrm{mod} m)$.

δ. Οἱ ἰδιότητες **β.** καί **γ.** (πρόσθεση καί πολλαπλασιασμός τῶν ἰσοτιμιῶν) μποροῦν νά γενικευθοῦν στό ἑξῆς θεώρημα:

Ἄν ἀντικαταστήσουμε τό $A_1 x_1, y_2, \ldots, x_\kappa$ στήν ἔκφραση μιᾶς ἀκεραίας ρητῆς συνάρτησης $S = \sum A x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_\kappa^{\alpha_\kappa}$ μέ ἀκεραίους συντελεστές, ἀπ' τούς ἀριθμούς $B_1 y_1 y_2 \cdots y_\kappa$, οἱ ὁποῖοι εἶναι, ἀντιστοίχως, ἰσότιμοι πρός τούς προηγούμενους ὡς πρός τό μέτρο m, τότε ἡ νέα ἔκφραση S θά εἶναι ἰσότιμη μέ τήν παλιά ὡς πρός μέτρο m.

Πραγματικά, ἀπ' τίς σχέσεις

$$A\equiv B(\mathrm{mod}m),\quad x_1\equiv y_1(\mathrm{mod}m),\ x_2\equiv y_2(\mathrm{mod}m),\ \dots,\ x_k\equiv y_k(\mathrm{mod}m)$$

βρίσκομε (c)

$$A\equiv B(\mathrm{mod}m)\ ,\ x_1^{\alpha_1}\equiv y_1^{\alpha_1}(\mathrm{mod}m),\ x_2^{\alpha_2}\equiv y_2^{\alpha_2}(\mathrm{mod}m),\ \dots,\ x_k^{\alpha_k}\equiv y_k^{\alpha_k}(\mathrm{mod}m)$$

$$Ax_1^{\alpha_1}x_2^{\alpha_2}\dots x_k^{\alpha_k}\equiv By_1^{\alpha_1}y_2^{\alpha_2}\dots y_k^{\alpha_k}\ (\mathrm{mod}m)$$

ἀπ' τίς ὁποῖες, προσθέτοντας, βρίσκομε

$$\sum Ax_1^{\alpha_1}x_2^{\alpha_2}\dots x_k^{\alpha_k}\equiv\sum By_1^{\alpha_1}y_2^{\alpha_2}\dots y_k^{\alpha_k}\ (\mathrm{mod}m)$$

Ἄν

$$a\equiv b(\mathrm{mod}m)\ ,\ a_1\equiv b_1(\mathrm{mod}m),\ \dots,\ a_n\equiv b_n(\mathrm{mod}m)\ ,\ x\equiv x_1(\mathrm{mod}m)$$

τότε

$$ax^n+a_1x^{n-1}+\dots+a_n\equiv bx_1^n+b_1x_1^{n-1}+\dots+b_n\ (\mathrm{mod}m)$$

Αὐτό τό ἀποτέλεσμα εἶναι εἰδική περίπτωση τοῦ προηγούμενου

ε. *Καί τά δυό μέλη μιᾶς ἰσοτιμίας μποροῦν νά διαιρεθοῦν μέ κάποιο κοινό διαιρέτη τους ἄν αὐτός εἶναι πρῶτος πρός τό μέτρο τῆς ἰσοτιμίας*

Πραγματικά, ἀπ' τίς σχέσεις $a\equiv b(\mathrm{mod}m), a=a_1d,\ b=b_1d\ ,\ (d,m)=1$ ἕπεται ὅτι ἡ διαφορά $a-b$, πού εἶναι ἴση μέ $(a_1-b_1)d$ εἶναι διαιρετή ἀπ' τόν m. πρῶτε ὅμως (Ἀ.Γ., §2, Κεφ. I) ὁ a_1-b_1 εἶναι διαιρετός ἀπ' τόν m. δηλ. $a_1\equiv b_1(\mathrm{mod}m)$.

§3. Ἄλλες ἰδιότητες τῶν ἰσοτιμιῶν

α. *Καί τά δυό μέλη μιᾶς ἰσοτιμίας καθώς καί τό μέτρο μποροῦν νά πολλαπλασιαστοῦν μέ τόν ἴδιο ἀκέραιο.*

Πραγματικά ἀπ' τήν $a\equiv b(\mathrm{mod}m)$ ἕπεται ὅτι

$$a=b+mt\ ,\ ak=bk+mkt$$

ἄρα $ak\equiv bk(\mathrm{mod}mk)$

β. *Καί τά δυό μέλη μιᾶς ἰσοτιμίας καθώς καί τό μέτρο μποροῦν νά διαιρεθοῦν μέ ὁποιονδήποτε ἀπ' τούς κοινούς διαιρέτες τους*

Πραγματικά, ἔστω

$$a\equiv b(\mathrm{mod}m)\ ,\ a=a_1d\ ,\ b=b_1d\ ,\ m=m_1d$$

Ἔχομε

$$a=b+mt\ ,\ a_1d=b_1d+m_1dt\ ,\ a_1=b_1+m_1t$$

ἄρα $a_1\equiv b_1(\mathrm{mod}m_1)$.

γ. *Ἄν ἡ ἰσοτιμία $a\equiv b$ ἰσχύει μέ περισσότερα μέτρα, τότε ἰσχύει ἐπίσης μέ μέτρο τό ἐλάχιστο κοινό πολλαπλάσιο αὐτῶν τῶν μέτρων.*

Πραγματικά, ἀπ' τίς $a\equiv b(\mathrm{mod}m_1)\ ,\ a\equiv b(\mathrm{mod}m_2),\ \dots,\ a\equiv b(\mathrm{mod}m_n)$ ἕπεται ὅτι ἡ διαφορά $a-b$ εἶναι διαιρετή ἀπ' ὅλα τά μέτρα $m_1, m_2, \dots, m_n$. Ἄρα (Ἀ.Γ., §3, Κεφ. I) πρέπει νά εἶναι διαιρετή καί μέ τό ἐλάχιστο κοινό πολλαπλάσιο m αὐτῶν τῶν μέτρων, δηλ. $a\equiv b(\mathrm{mod}m)$.

d. "Αν μιά ἰσοτιμία ἰσχύει μέ μέτρο m , τότε ἰσχύει ἐπίσης καί μέ μέτρο d , ὅπου d εἶναι ἕνας ὁποιοσδήποτε διαιρέτης τοῦ m.
Πραγματικά, ἀπ' τήν $a \equiv b \pmod m$ ἕπεται ὅτι ἡ διαφορά $a-b$ πρέπει νά διαιρεῖται ἀπ' τόν m · τότε (1,b, §1, Κεφ I) πρέπει νά διαιρεῖται ἀπό ὁποιοδήποτε διαιρέτη d τοῦ ἀριθμοῦ m , δηλ. $a \equiv b \pmod d$

e. "Αν τό ἕνα μέλος μιᾶς ἰσοτιμίας καί τό μέτρο εἶναι διαιρετά ἀπό κάποιον ἀριθμό, τότε καί τό ἄλλο μέλος τῆς ἰσοτιμίας πρέπει νά εἶναι διαιρετό ἀπ' τόν ἴδιο ἀριθμό.
Πραγματικά, ἀπ' τήν $a \equiv b \pmod m$ ἕπεται ὅτι $a = b + mt$ καί ἄν οἱ a καί m εἶναι πολλαπλάσια τοῦ d , τότε (2,b, §1, Κεφ I) καί ὁ b πρέπει νά εἶναι πολλαπλάσιο τοῦ d , πρᾶγμα πού θέλαμε ν' ἀποδείξομε.

f. "Αν $a \equiv b \pmod m$, τότε $(a,m) = (b,m)$
Πραγματικά αὐτό ἕπεται ἀπό τή σχέση $a = b + mt$, λόγω τοῦ 2,b, §2, Κεφ I.

§4. Πλήρη συστήματα ὑπολοίπων

a. "Ολοι οἱ ἀριθμοί πού εἶναι μεταξύ τους ἰσότιμοι ὡς πρός μέτρο m ἀποτελοῦν μιά κλάση ἰσοδυναμίας ὡς πρός μέτρο m.
Ἀπ' αὐτό τόν ὁρισμό ἕπεται ὅτι ὅλοι οἱ ἀριθμοί μιᾶς κλάσης ἰσοδυναμίας ἔχουν τό ἴδιο ὑπόλοιπο r καθώς καί ὅτι παίρνομε ὅλους τούς ἀριθμούς μιᾶς κλάσης ἰσοδυναμίας ἄν θεωρήσομε ὅτι τό q στήν παράσταση $mq+r$ διατρέχει ὅλους τούς ἀκεραίους.
Ἀντίστοιχες στίς m τό πλῆθος τιμές τοῦ r , ἔχομε καί m τό πλῆθος κλάσεις ἰσοδυναμίας ἀριθμῶν, ὡς πρός μέτρο m.

b. Κάθε ἀριθμός μιᾶς κλάσης ἰσοδυναμίας χαρακτηρίζεται ἀπό ὑπόλοιπο, ὡς πρός μέτρο m . Τό ὑπόλοιπο πού παίρνομε γιά $q=0$ εἶναι ἴσο μέ τόν ἴδιο τόν r καί χαρακτηρίζεται τό ἐλάχιστο μή ἀρνητικό ὑπόλοιπο.
Τό ὑπόλοιπο ρ μέ τή μικρότερη ἀπόλυτη τιμή χαρακτηρίζεται τό ἀπολύτως ἐλάχιστο ὑπόλοιπο.
Εἶναι φανερό ὅτι ἔχομε $\rho = r$ γιά $r < \frac{m}{2}$ · γιά $r > \frac{m}{2}$ ἔχομε $\rho = r - m$ · τέλος, ἄν ὁ m εἶναι ἄρτιος καί $r = \frac{m}{2}$, τότε μποροῦμε νά πάρομε γιά ρ ὁποιοδήποτε ἀπ' τούς δυό ἀριθμούς $\frac{m}{2}$ καί $\frac{m}{2} - m = -\frac{m}{2}$.
Παίρνοντας ἕνα ὑπόλοιπο ἀπό κάθε κλάση ἰσοδυναμίας, παίρνομε ἕνα πλῆρες σύστημα ὑπολοίπων ὡς πρός μέτρο m . Συχνά, σάν πλῆρες σύστημα ὑπολοίπων χρησιμοποιοῦμε τά ἐλάχιστα μή ἀρνητικά ὑπόλοιπα $0, 1, 2, \ldots, m-1$ ἤ

τά ἀπολύτως ἐλάχιστα ὑπόλοιπα· τά τελευταῖα, καθώς προκύπτει ἀπ' τήν παραπάνω ἀνάλυση, περιστάνονται, στήν περίπτωση περιττοῦ m ἀπ' τήν ἀκολουθία

$$-\frac{m-1}{2}, \dots, -1, 0, 1, \dots, \frac{m-1}{2}$$

καί στήν περίπτωση ἄρτιου m ἀπό μιά ἀπ' τίς δυό ἀκολουθίες

$$-\frac{m}{2}+1, \dots, -1, 0, 1, \dots, \frac{m}{2}$$

$$-\frac{m}{2}, \dots, -1, 0, 1, \dots, \frac{m}{2}-1$$

<u>Ε.</u> <u>Κάθε m τό πλῆθος ἀκέραιοι πού εἶναι ἀνά δύο ἀνισότιμοι ὡς πρός μέτρο m συνιστοῦν ἕνα πλῆρες σύστημα ὑπολοίπων ὡς πρός μέτρο m.</u> Πραγματικά, μιά καί εἶναι ἀνισότιμοι, αὐτοί οἱ ἀκέραιοι πρέπει νά ἀνήκουν σέ διαφορετικές κλάσεις ἰσοϋπολοιπίας καί ἀφοῦ ὑπάρχουν m ἀπ' αὐτούς, δηλ. τόσοι ὅσες εἶναι καί οἱ κλάσεις, ἕπεται ὅτι ἕνας ἀκέραιος ἀντιστοιχεῖ σέ κάθε μιά κλάση.

<u>Ϛ.</u> <u>Ἄν $(a,m)=1$ καί ὁ x διατρέχει ἕνα πλῆρες σύστημα ὑπολοίπων ὡς πρός μέτρο m, τότε καί ὁ $ax+b$, ὅπου ὁ b εἶναι ὁποιοσδήποτε ἀκέραιος, διατρέχει ἕνα πλῆρες σύστημα ὑπολοίπων ὡς πρός μέτρο m.</u> Πραγματικά, ὑπάρχουν τόσοι ἀκέραιοι $ax+b$ ὅσοι εἶναι καί οἱ ἀκέραιοι x δηλ. m. Μένει, λοιπόν, ν' ἀποδείξουμε ὅτι ὁποιοιδήποτε ἀκέραιοι ax_1+b καί ax_2+b πού ἀντιστοιχοῦν σέ ἀνισότιμους x_1 καί x_2, θά εἶναι ἐπίσης ἀνισότιμοι ὡς πρός μέτρο m.

Ἀλλά, ὑποθέτοντας ὅτι $ax_1+b \equiv ax_2+b \pmod m$, φτάνουμε στήν ἰσοτιμία $ax_1 \equiv ax_2 \pmod m$, ἀπ' τήν ὁποία παίρνουμε $x_1 \equiv x_2 \pmod m$, σά συνέπεια τῆς $(a,m)=1$, καί αὐτό ἔρχεται σέ ἀντίφαση μέ τήν ὑπόθεση τῆς ἀνισοτιμίας τῶν ἀκεραίων x_1 καί x_2.

§5. Περιωρισμένα συστήματα ὑπολοίπων.

<u>Α.</u> Ἀπ' τό §3 οἱ ἀκέραιοι μιᾶς κλάσης ἰσοτιμίας ὡς πρός μέτρο m ἔχουν ὅλοι τόν ἴδιο μέγιστο κοινό διαιρέτη σέ σχέση μέ τό μέτρο. Ἰδιαίτερα σημαντικές εἶναι οἱ κλάσεις ἰσοδυναμίας γιά τίς ὁποῖες αὐτός ὁ διαιρέτης εἶναι ἴσος μέ τή μονάδα, δηλ. οἱ κλάσεις μέ ἀκεραίους πρώτους πρός τό μέτρο. Παίρνοντας ἕνα ὑπόλοιπο ἀπό κάθε μιά τέτοια κλάση σχηματίζουμε ἕνα <u>περιωρισμένο σύστημα ὑπολοίπων ὡς πρός μέτρο m</u>. Ἄρα, <u>ἕνα περιωρισμένο σύστημα ὑπολοίπων ἀποτελεῖται ἀπό ἐκείνους τούς ἀκεραίους ἑνός πλήρους συστήματος, οἱ ὁποῖοι εἶναι πρῶτοι πρός τό μέτρο.</u>

Συνήθως ένα περιορισμένο σύστημα υπολοίπων επιλέγεται μέσα από το σύστημα των ελαχίστων μη αρνητικών υπολοίπων $0,1,\dots,m-1$. Μιά και το πλήθος αυτών των αριθμών που είναι πρώτοι προς τον m είναι $\varphi(m)$, το πλήθος των αριθμών ενός περιορισμένου συστήματος, που είναι ίσο με το πλήθος των κλάσεων ισοδυναμίας οι όποτες περιέχουν αριθμούς πρώτους προς το μέτρο, είναι $\varphi(m)$.

Παράδειγμα: Ένα περιορισμένο σύστημα υπολοίπων ως προς μέτρο 42 είναι 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.

b. Οποιοιδήποτε $\varphi(m)$ το πλήθος αριθμοί, που είναι ανά δύο ανισότιμοι ως προς μέτρο m και πρώτοι προς το μέτρο αποτελούν ένα περιορισμένο σύστημα υπολοίπων ως προς μέτρο m.

Πραγματικά, με το να είναι ανισότιμοι και σχετικά πρώτοι προς το μέτρο αύτοι οι αριθμοί ανήκουν σε διαφορετικές κλάσεις ισοδυναμίας από εκείνες που περιέχουν αριθμούς πρώτους προς το μέτρο, και μιά και υπάρχουν $\varphi(m)$ απ' αυτούς, έπεται ότι ένας αριθμός υπάρχει από κάθε μιά κλάση.

Σ "Αν $(a,m)=1$ και ο x διατρέχει ένα περιορισμένο σύστημα υπολοίπων ως προς μέτρο m, τότε και ο ax διατρέχει ένα περιορισμένο σύστημα υπολοίπων ως προς μέτρο m.

Πραγματικά, υπάρχουν τόσοι αριθμοί ax όσοι και αριθμοί x δηλ. $\varphi(m)$. Απ' το b μένει ακόμη να δείξομε ότι οι αριθμοί ax είναι ανά δύο ανισότιμοι ως προς μέτρο m και πρώτοι προς το μέτρο. Αλλά το πρώτο αποδείχτηκε στο d, §4 για τους αριθμούς της γενικώτερης μορφής $ax+b$ και το δεύτερο έπεται απ' τις $(a,m)=1$ & $(x,m)=1$.

§6. Τα θεωρήματα των EULER και FERMAT

a. Για $m>1$ και $(a,m)=1$ έχομε (θεώρημα του Euler)

$$a^{\varphi(m)} \equiv 1 \pmod m$$

Πραγματικά, αν το x διατρέχει ένα περιορισμένο σύστημα υπολοίπων

$$x = r_1, r_2, \dots, r_c \quad , \quad c = \varphi(m)$$

το όποίο αποτελείται απ' τα ελάχιστα μη αρνητικά υπόλοιπα, τότε τα ελάχιστα μη αρνητικά υπόλοιπα $\rho_1, \rho_2, \dots \rho_c$ των αριθμών ax, θα διατρέχουν το ίδιο σύστημα, αλλά εν γένει με διαφορετική τάξη (c, §5).

Πολλαπλασιάζοντας τις ισοτιμίες

$$ar_1 \equiv \rho_1 \pmod m, \quad ar_2 \equiv \rho_2 \pmod m, \dots, ar_c \equiv \rho_c \pmod m$$

κατά μέλη, βρίσκομε:

$$a^c r_1 r_2 \dots r_c \equiv \rho_1 \rho_2 \dots \rho_c \pmod m$$

απ' όπου βρίσκομε

$$a^c \equiv 1 \pmod m$$

διαιρέντας καί τά δυό μέλη μέ τό γινόμενο $r_1 r_2 \cdots r_\kappa = \beta_1 \beta_2 \cdots \beta_\kappa$

b. Ἄν ὁ p εἶναι πρῶτος καί ὁ a δέν εἶναι διαιρετός ἀπ' τόν p τότε ἔχομε: (θεώρημα τοῦ Fermat)

$$a^{p-1} \equiv 1 \pmod{p}$$

Αὐτό τό θεώρημα εἶναι συνέπεια τοῦ θεωρήματος **a.** γιά $m = p$. Τό θεώρημα τοῦ Fermat μπορεῖ νά διατυπωθεῖ μέ πολλή πιό ἁπλή μορφή. Πραγματικά, πολλαπλασιάζοντας καί τά δυό μέλη τῆς ἰσοτιμίας (1) μέ τό a, παίρνομε τήν ἰσοτιμία

$$a^p \equiv a \pmod{p}$$

ἡ ὁποία ἰσχύει γιά ὅλους τούς ἀκεραίους a, μιά καί ἰσχύει γιά τούς ἀκεραίους a, πού εἶναι πολλαπλάσιο τοῦ p.

Οἱ προηγούμενες σελίδες ἀποτελοῦν μετάφραση τοῦ Κεφαλαίου III τοῦ βιβλίου Elements of Number Theory, I.M. Vinogradov (μετάφραση στ' ἀγγλική γλώσσα).

Κ ε φ ά λ α ι ο IV

Ἰ σ ο τ ι μ ί ε ς μ έ ν ἕ ν α ἄ γ ν ω σ τ ο.

§ 1. Βασικές ἀρχές.

Τό ἐπόμενό μας πρόβλημα εἶναι ἡ μελέτη τῶν ἰσοτιμιῶν τῆς γενικῆς μορφῆς:

(1) $f(x)\equiv 0 \pmod m$, $f(x)=a_0x^n+a_1x^{n-1}+\dots+a_n$

Ἄν ὁ a_0 δέν εἶναι διαιρετός ἀπ' τόν m, τότε ὁ n χαρακτηρίζεται βαθμός τῆς ἰσοτιμίας.

Νά λύσουμε μιά ἰσοτιμία σημαίνει νά βροῦμε ὅλες τίς τιμές τοῦ x πού τήν ἱκανοποιοῦν. Δυό ἰσοτιμίες πού ἱκανοποιοῦνται ἀπ' τίς ἴδιες τιμές τοῦ x λέγονται ἰσοδύναμες.

Ἄν ἡ ἰσοτιμία (1) ἱκανοποιεῖται ἀπό κάποιο $x=x_1$, τότε (d, §2, Κεφ. II) αὐτή ἡ ἰσοτιμία θά ἱκανοποιεῖται, ἐπίσης, ἀπ' ὅλους τούς ἀριθμούς πού εἶναι ἰσότιμοι πρός τόν x_1, ὡς πρός μέτρο m: $x\equiv x_1 \pmod m$. Ὅλη αὐτή ἡ κλάση τῶν ἀριθμῶν θεωρεῖται σά μιά λύση. Σύμφωνα μ' αὐτή τή σύμβαση, ἡ ἰσοτιμία (1) ἔχει τόσες λύσεις ὅσα εἶναι τά ὑπόλοιπα ἑνός πλήρους συστήματος πού τήν ἱκανοποιοῦν.

Παράδειγμα: Ἡ ἰσοτιμία

$$x^6+x+1\equiv 0 \pmod 7$$

ἱκανοποιεῖται ἀπ' τούς δυό ἀριθμούς $x=2$ καί $x=4$ ἀνάμεσα στούς ἀριθμούς $0,1,2,3,4,5,6$, πού ἀπαρτίζουν ἕνα πλῆρες σύστημα ὑπολοίπων ὡς πρός μέτρο 7. Γι' αὐτό ἡ παραπάνω ἰσοτιμία ἔχει τίς δυό λύσεις

$$x\equiv 2 \pmod 7 \quad , \quad x\equiv 4 \pmod 7.$$

§ 2. Ἰσοτιμίες πρώτου βαθμοῦ.

a. Μιά ἰσοτιμία πρώτου βαθμοῦ, τῆς ὁποίας ὁ σταθερός ὅρος βρίσκεται στό δεξιό μέλος (μέ ἀντίθετο πρόσημο) μπορεῖ νά τεθεῖ μέ τή μορφή:

(1) $$ax\equiv b \pmod m$$

b. Μελετώντας τό πλῆθος τῶν λύσεων, περιορίζομε πρῶτα τήν ἰσοτιμία μας στή συνθήκη $(a,m)=1$. Σύμφωνα μέ τήν §1, ἡ ἰσοτιμία μας ἔχει τόσες λύσεις ὅσα καί τά ὑπόλοιπα ἑνός πλήρους συστήματος, πού τήν ἱκανοποιοῦν. Ἀλλά καθώς ὁ x διατρέχει ἕνα πλῆρες σύστημα ὑπολοίπων ὡς πρός μέτρο m, ὁ ax διατρέχει, ἐπίσης, ἕνα πλῆρες σύστημα ὑπολοίπων (d, §4, Κεφ. II). Γι' αὐτό, εἰδικώτερα, ὁ ax θά εἶναι ἰσότιμος πρός τόν b γιά μιά, καί μόνο μιά, τιμή τοῦ x, παρμένη ἀπ' τό πλῆρες σύστημα ὑπολοίπων.

Ἄρα, ἡ ἰσοτιμία (1) ἔχει μιά λύση ὅταν $(a,m)=1$

c. Τώρα, ἔστω $(a,m)=d>1$. Τότε γιά νά ἔχει ἡ ἰσοτιμία (1) λύση, εἶναι ἀναγκαῖο (Θ. §3, Κεφ. II) ὁ b νά εἶναι διαιρετός ἀπ' τόν d , γιατί ἀλλοιῶς ἡ ἰσοτιμία (1) θά ἦταν ἀδύνατη γιά ὅλους τούς ἀκεραίους x. Θεωρώντας λοιπόν ὅτι ὁ b εἶναι πολλαπλάσιο τοῦ d , γράφομε $a=a_1 d$ $b=b_1 d$, $m=m_1 d$. Τότε ἡ ἰσοτιμία (1) εἶναι ἰσοδύναμη μέ τήν ἑξῆς (πού προκύπτει διαιρώντας μέ τόν d): $a_1 x \equiv b_1 \pmod{m_1}$, στήν ὁποία $(a_1, m_1)=1$, καί γι' αὐτό θά ἔχει μιά λύση ὡς πρός μέτρο m_1 . Ἔστω ὅτι x_1 εἶναι τό ἐλάχιστο μή ἀρνητικό ὑπόλοιπο αὐτῆς τῆς λύσης, ὡς πρός μέτρο m_1 · τότε ὅλοι οἱ ἀριθμοί x , πού εἶναι λύσεις αὐτῆς τῆς ἰσοτιμίας βρήκαμε ὅτι εἶναι τῆς μορφῆς

$$x \equiv x_1 \pmod{m_1} \qquad (2)$$

Ἀλλά ὡς πρός μέτρο m , οἱ ἀριθμοί πού ὁρίζονται ἀπ' τή σχέση (2) δέν σχηματίζουν μιά λύση, ἀλλά περισσότερες καί, συγκεκριμένα, τόσες λύσεις ὅσοι ἀριθμοί τῆς μορφῆς (2) περιέχονται στήν ἀκολουθία $0, 1, 2, \ldots, m-1$ τῶν ἐλάχιστων μή ἀρνητικῶν ὑπολοίπων ὡς πρός μέτρο m. Ἀλλά οἱ ἀριθμοί αὐτοί τῆς σχέσης (2) εἶναι οἱ ἑξῆς:

$$x_1 , \; x_1+m_1 , \; x_1+2m_1 , \ldots , \; x_1+(d-1)m_1$$

δηλ. d ἀριθμοί τῆς μορφῆς (2), ἀπ' ὅπου συμπεραίνομε ὅτι ἡ ἰσοτιμία (1) ἔχει d λύσεις.

d. Συγκεντρώνοντας τό συμπέρασμά μας, ἔχομε τό ἑξῆς θεώρημα:
Ἔστω $(a,m)=d$. Ἡ ἰσοτιμία $ax \equiv b \pmod{m}$ εἶναι ἀδύνατη ἄν ὁ b δέν εἶναι διαιρετός ἀπ' τόν d . Ἄν ὁ b εἶναι πολλαπλάσιο τοῦ d , ἡ ἰσοτιμία ἔχει d λύσεις.

e. Ἀναπτύσσοντας τίς λύσεις τῆς ἰσοτιμίας (1) , θά ἐφαρμόσομε μόνο μιά μέθοδο, πού βασίζεται στή θεωρία τῶν συνεχῶν κλασμάτων, καί ἀρκεῖ νά περιοριστοῦμε στήν περίπτωση πού $(a,m)=1$

Ἀναπτύσσοντας τό κλάσμα $\frac{m}{a}$ σέ συνεχές κλάσμα

$$\frac{m}{a} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots + \cfrac{1}{q_n}}}$$

καί θεωρώντας τά δύο τελευταῖα ἀναγωγήματα:

$$\frac{p_{n-1}}{q_{n-1}} \; \text{καί} \; \frac{p_n}{q_n} = \frac{m}{a}$$

Θά ἔχομε ἀπ' τίς ἰδιότητες τῶν συνεχῶν κλασμάτων (e, §4, Κεφ. I)

$$m\theta_{n-1} = aP_{n-1} = (-1)^n$$

$$aP_{n-1} \equiv (-1)^{n+1} \pmod m$$

$$a(-1)^{n-1}P_{n-1}b \equiv b \pmod m$$

Ἄρα, ἡ ἰσοτιμία μας ἔχει τή λύση

$$x \equiv (-1)^{n-1}P_{n-1}b \pmod m$$

γιά τόν ὑπολογισμό τῆς ὁποίας βρίσκει νά ὑπολογίσομε τόν P_{n-1} μέ τή μέθοδο πού περιγράψαμε στό d, §4, Κεφ. I

Παράδειγμα: Λύνομε τήν ἰσοτιμία

$$111x \equiv 75 \pmod{321} \tag{3}$$

Ἐδῶ $(111, 321) = 3$, ἐνῶ ὁ 75 εἶναι πολλαπλάσιο τοῦ 3. Ἄρα ἡ ἰσοτιμία ἔχει τρεῖς λύσεις.

Διαιρώντας καί τά δύο μέλη τῆς ἰσοτιμίας καθώς καί τό μέτρο μέ τόν 3 παίρνομε τήν ἰσοτιμία

$$37x \equiv 25 \pmod{107} \tag{4}$$

τήν ὁποία πρωτολύνομε. Ἔχομε

		107	37		
		74	2		
		37	33		
		33	1		
		33	4		
		32	8		
		4	1		
		4	4		
		0			

q_k		2	1	8	4
P_k	1	2	3	26	107

Ἐδῶ $n=4$, $P_{n-1}=26$, $b=25$, καί ἔχομε τή λύση τῆς ἰσοτιμίας (4) μέ τή μορφή

$$x \equiv -26 \cdot 25 \equiv 93 \pmod{107}$$

Μέ τή βοήθεια αὐτῆς τῆς λύσης μποροῦμε νά παραστήσομε τίς λύσεις τῆς ἰσοτιμίας (3) μέ τή μορφή:

$$\text{δηλ.} \quad \begin{matrix} x \equiv 93,\ 93+107,\ 93+2\cdot107 \pmod{321} \\ x \equiv 93,\ 200,\ 313 \pmod{321} \end{matrix}$$

§3. Συστήματα ἰσοτιμιῶν πρώτου βαθμοῦ.

a. Θά θεωρήσωμε μονάχα τό ἁπλούστερο σύστημα ἰσοτιμιῶν

(1) $x \equiv b_1 (\mathrm{mod} m_1)$, $x \equiv b_2 (\mathrm{mod} m_2)$, ... , $x \equiv b_k (\mathrm{mod} m_k)$

μέ ἕνα ἄγνωστο, ἀλλά μέ διαφορετικά καί ἀνά ζεύγη πρῶτα μεταξύ τους μέτρα.

b. Εἶναι δυνατόν νά λύσωμε τό σύστημα (1), δηλ. νά βροῦμε ὅλες τίς τιμές τοῦ x πού τό ἱκανοποιοῦν, ἐφαρμόζοντας τό ἑξῆς θεώρημα:

Ἔστω ὅτι οἱ ἀριθμοί M_s καί M'_s ὁρίζονται ἀπ' τίς συνθῆκες:

$$m_1 m_2 \cdots m_k = M_s m_s \quad , \quad M_s M'_s \equiv 1 (\mathrm{mod} m_s)$$

καί ἔστω

$$x_0 = M_1 M'_1 b_1 + M_2 M'_2 b_2 + \cdots + M_k M'_k b_k$$

τότε τό σύνολο τῶν τιμῶν τοῦ x, πού ἱκανοποιοῦν τό σύστημα (1) ὁρίζονται ἀπ' τήν ἰσοτιμία

(2) $$x \equiv x_0 (\mathrm{mod} m_1 m_2 \cdots m_k)$$

Πραγματικά, ἀφ' αἰτίας τοῦ γεγονότος ὅτι ὅλοι οἱ M_j πού εἶναι διαφορετικοί ἀπ' τόν M_s εἶναι διαιρετοί ἀπ' τόν m_s γιά κάθε $s = 1, 2, \ldots, k$, θά ἔχωμε $x_0 \equiv M_s M'_s b_s \equiv b_s (\mathrm{mod} m_s)$

Ἄρα τό σύστημα (1) ἱκανοποιεῖται γιά $x = x_0$. Ἀπ' αὐτό ἕπεται ἀμέσως ὅτι τό σύστημα (1) εἶναι ἰσοδύναμο μέ τό σύστημα

(3) $x \equiv x_0 (\mathrm{mod} m_1)$, $x \equiv x_0 (\mathrm{mod} m_2)$, ... , $x \equiv x_0 (\mathrm{mod} m_k)$

(δηλ. τά συστήματα (1) καί (3) ἱκανοποιοῦνται ἀπ' τίς ἴδιες τιμές τοῦ x)

Ἀλλά τό σύστημα (3), ἀπ' τά θεωρήματα τῶν §, §3, Κεφ. II καί §, §3, Κεφ. III, ἱκανοποιεῖται ἀπ' ἐκεῖνες καί μόνο ἐκεῖνες τίς τιμές τοῦ x πού ἱκανοποιοῦν τήν ἰσοτιμία (2)

c. Ἄν οἱ $b_1, b_2, \ldots, b_k$ διατρέχουν, ἀνεξάρτητα, πλήρη συστήματα ὑπολοίπων ὡς πρός μέτρα $m_1, m_2, \ldots, m_k$, τότε ὁ x_0 διατρέχει ἕνα πλῆρες σύστημα ὑπολοίπων ὡς πρός μέτρο $m_1 m_2 \cdots m_k$.

Πραγματικά, ὁ x_0 διατρέχει $m_1 m_2 \cdots m_k$ τό πλῆθος τιμές, πού εἶναι ἀνισότιμες ὡς πρός μέτρο $m_1 m_2 \cdots m_k$ (§, §3, Κεφ. III)

d. Παράδειγμα: Λύνομε τό σύστημα $x \equiv b_1 (\mathrm{mod} 4)$, $x \equiv b_2 (\mathrm{mod} 5)$, $x \equiv b_3 (\mathrm{mod} 7)$

Ἐδῶ $4.5.7 = 4.35 = 5.28 = 7.20$ ἐνῶ

$35.3 \equiv 1 (\mathrm{mod} 4)$, $28.2 \equiv 1 (\mathrm{mod} 5)$; $20.6 \equiv 1 (\mathrm{mod} 7)$.

Ἄρα

$$x = 35.3 b_1 + 28.2 b_2 + 20.6 b_3 = 105 b_1 + 56 b_2 + 120 b_3$$

ὁπότε τό σύνολο τῶν τιμῶν τοῦ x πού ἱκανοποιοῦν τό σύστημα

$$x \equiv 1 (\mathrm{mod} 4) , \quad x \equiv 3 (\mathrm{mod} 5) , \quad x \equiv 5 (\mathrm{mod} 7)$$

εἶναι

$$x \equiv 105.1 + 56.3 + 120.5 \equiv 93 (\mathrm{mod} 140) .$$

ἐνῶ τό σύνολο τῶν τιμῶν τοῦ x, πού ἱκανοποιοῦν τό σύστημα

$$x \equiv 3 \pmod 4, \quad x \equiv 2 \pmod 5, \quad x \equiv 6 \pmod 7$$

εἶναι

$$x \equiv 105\cdot 3 + 56\cdot 2 + 120\cdot 6 \equiv 27 \pmod{140}.$$

§4. Ἰσοτιμίες ὁποιουδήποτε βαθμοῦ μέ μέτρο πρῶτον ἀριθμό

a. Ἔστω p πρῶτος. Θ' ἀποδείξομε γενικά θεωρήματα σχετικά μέ τήν ἰσοτιμία τῆς μορφῆς:

$$(1) \quad f(x) \equiv 0 \pmod p, \quad f(x) = a x^{n} + a_1 x^{n-1} + \dots + a_n$$

b. Μιά ἰσοτιμία τῆς μορφῆς (1) εἶναι ἰσοδύναμη μέ μιά ἰσοτιμία βαθμοῦ ὄχι μεγαλυτέρου ἀπό $p-1$.

Πραγματικά, διαιρώντας τό $f(x)$ ἀπ' τό $x^p - x$ ἔχομε

$$f(x) = (x^p - x)Q(x) + R(x)$$

ὅπου ὁ βαθμός τοῦ $R(x)$ δέν εἶναι μεγαλύτερος ἀπό $p-1$. Ἀλλά ἡ σχέση $x^p - x \equiv 0 \pmod p$ συνεπάγεται τήν $f(x) \equiv R(x) \pmod p$ ἀπ' τήν ὁποία ἕπεται τό θεώρημά μας.

c. Ἄν ἡ ἰσοτιμία (1) ἔχει περισσότερες ἀπό n λύσεις, τότε ὅλοι οἱ συντελεστές τοῦ $f(x)$ εἶναι πολλαπλάσια τοῦ p.

Πραγματικά, ἔστω ὅτι ἡ ἰσοτιμία (1) ἔχει τοὐλάχιστον $n+1$ λύσεις. Ἄν παραστήσομε μέ $x_1, x_2, \dots, x_n, x_{n+1}$ τά ὑπόλοιπα αὐτῶν τῶν λύσεων, μποροῦμε νά παραστήσομε τό $f(x)$ μέ τή μορφή:

$$
\begin{aligned}
(2) \qquad f(x) = {} & a(x-x_1)(x-x_2)\cdots(x-x_{n-2})(x-x_{n-1})(x-x_n) + \\
& + b(x-x_1)(x-x_2)\cdots(x-x_{n-2})(x-x_{n-1}) + \\
& + c(x-x_1)(x-x_2)\cdots(x-x_{n-2}) + \\
& \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
& + k(x-x_1)(x-x_2) + \\
& + l(x-x_1) + \\
& + m
\end{aligned}
$$

Γι' αὐτό τό σκοπό, ἀναπτύσσομε τούς προσθετέους τοῦ δεξιοῦ μέλους σέ πολυώνυμα, καί ὕστερα ἐκλέγομε τόν b ἔτσι ὥστε τό ἄθροισμα τῶν συντελεστῶν τοῦ x^{n-1} στά δυό πρῶτα πολυώνυμα νά συμπίπτει μέ τό a_1. Ξέροντας τό b, ἐκλέγομε τό c ἔτσι ὥστε τό ἄθροισμα τῶν συντελεστῶν τοῦ x^{n-2} στά τρία πρῶτα πολυώνυμα νά συμπίπτει μέ τόν a_2 κ.λ.π. Ἄν θέσομε $x = x_1, x_2, \dots, x_n, x_{n+1}$ διαδοχικά στή (2), βρίσκομε ὅτι ὅλοι οἱ ἀριθμοί $m, l, k, \dots, c, b, a$ εἶναι πολλαπλάσια τοῦ p. Αὐτό σημαίνει ὅτι ὅλοι οἱ συντελεστές $a, a_1, \dots, a_n$ εἶναι πολλαπλάσια τοῦ p (ἀφοῦ εἶναι ἀθροίσματα ἀριθμῶν πού εἶναι πολλαπλάσια τοῦ p).

d. Γιά πρῶτο p ἔχομε τήν ἰσοτιμία (θεώρημα τοῦ WILSON)

(3) $1.2\cdots(p-1)+1 \equiv 0 \pmod p$

Πραγματικά, γιά $p=2$ τό θεώρημα εἶναι φανερό. Ἂν $p>2$, τότε θεωροῦμε τήν ἰσοτιμία

$$(x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1}-1) \equiv 0 \pmod p$$

Ὁ βαθμός της δέν εἶναι μεγαλύτερος ἀπό $p-2$ καί ἔχει $p-1$ λύσεις, συγκεκριμένα, τίς λύσεις μέ ὑπόλοιπα $1,2,\dots,p-1$. Ἄρα, ἀπ' τό θεώρημα c, ὅλοι οἱ συντελεστές της εἶναι πολλαπλάσια τοῦ p εἰδικώτερα ὁ σταθερός ὅρος εἶναι, ἐπίσης διαιρετός ἀπ' τόν p καί ὁ σταθερός ὅρος εἶναι, ἀκριβῶς, τό ἀριστερό μέλος τῆς ἰσοτιμίας (3).

Παράδειγμα: Ἔχομε $1.2.3.4.5.6+1 = 721 \equiv 0 \pmod 7$

§5. Ἰσοτιμίες ὁποιουδήποτε βαθμοῦ μέ μέτρο σύνθετον ἀριθμό.

a. Ἂν $m_1, m_2, \dots, m_k$ εἶναι ἀνά ζεύγη πρῶτοι τότε ἡ ἰσοτιμία

(1) $f(x) \equiv 0 \pmod{m_1 m_2 \cdots m_k}$

εἶναι ἰσοδύναμη μέ τό σύστημα

$$f(x) \equiv 0 \pmod{m_1}\ ,\ f(x) \equiv 0 \pmod{m_2},\ \dots,\ f(x) \equiv 0 \pmod{m_k}$$

Ἂν παραστήσωμε μέ $T_1, T_2, \dots, T_k$ τό πλῆθος τῶν λύσεων καθεμιᾶς ἰσοτιμίας τοῦ συστήματος, ὡς πρός τά ἀντίστοιχα μέτρα, καί μέ T τό πλῆθος τῶν λύσεων τῆς ἰσοτιμίας (1) θά ἔχομε $T = T_1 T_2 \cdots T_k$.

Πραγματικά, τό πρῶτο μέρος τοῦ θεωρήματος συνάγεται ἀπ' τά c καί d, §3, Κεφ. II. Τό δεύτερο μέρος ἕπεται ἀπό τό γεγονός ὅτι κάθε ἰσοτιμία

(2) $f(x) \equiv 0 \pmod{m_i}$

ἱκανοποιεῖται ἄν καί μόνο ἄν ἱκανοποιεῖται μιά ἀπ' τίς T_s τό πλῆθος ἰσοτιμίες τῆς μορφῆς $x \equiv b_s \pmod{m_s}$

ὅπου ὁ b_s διατρέχει τά ὑπόλοιπα τῶν λύσεων τῆς ἰσοτιμίας (2), ἐνῶ ὅλοι οἱ $T_1, T_2, \dots, T_k$ τό πλῆθος διαφορετικοί συνδυασμοί τῆς μορφῆς $x \equiv b_1 \pmod{m_1}\ ,\ x \equiv b_2 \pmod{m_2}\ ,\ \dots\ ,\ x \equiv b_k \pmod{m_k}$ εἶναι δυνατοί, καί ὁρίζουν (c, §3) διαφορετικές κλάσεις ὡς πρός μέτρο $m_1 m_2 \cdots m_k$.

Παράδειγμα: Ἡ ἰσοτιμία

(3) $f(x) \equiv 0 \pmod{35}$, $f(x) = x^4 + 2x^3 + 8x + 9$

εἶναι ἰσοδύναμη μέ τό σύστημα

$$f(x) \equiv 0 \pmod 5\ ,\ f(x) \equiv 0 \pmod 7$$

Εἶναι εὔκολο (§1) νά διαπιστώσει κανείς ὅτι ἡ πρώτη ἰσοτιμία αὐτοῦ τοῦ συστήματος ἔχει δυό λύσεις: $x \equiv 1, 4 \pmod 5$, καί ἡ δεύτερη ἰσοτιμία ἔχει τρεῖς λύσεις: $x \equiv 3, 5, 6 \pmod 7$. Ἄρα ἡ ἰσοτιμία (3) ἔχει $2.3 = 6$ λύσεις

Γιά νά βροῦμε αὐτές τίς ἕξη λύσεις, πρέπει νά λύσομε ἕξη συστήματα τῆς μορφῆς:

$$(4)\qquad x\equiv b_1 \pmod 5\ ,\ x\equiv b_2 \pmod 7$$

πού παίρνομε ἄν θεωρήσομε τό b_1 νά διατρέχει τίς τιμές $b_1\equiv 1,4 \pmod 5$ ἐνῶ τό b_2 νά διατρέχει τίς τιμές $b_2\equiv 3,5,6 \pmod 7$. Ἀλλά μιά καί

$$35=5\cdot 7=7\cdot 5,\quad 7\cdot 3\equiv 1 \pmod 5,\quad 5\cdot 3\equiv 1 \pmod 7$$

τό σύνολο τῶν τιμῶν τοῦ x, πού ἱκανοποιοῦν τό σύστημα (4) μπορεῖ νά παρασταθεῖ μέ τή μορφή (b, § 3)

$$x\equiv 21b_1+15b_2 \pmod{35}$$

Ἄρα οἱ λύσεις τῆς ἰσοτιμίας (3) εἶναι:

$$x\equiv 31, 26, 6, 24, 19, 34 \pmod{35}$$

β. Χάρη στό θεώρημα α, ἡ μελέτη καί λύση τῶν ἰσοτιμιῶν τῆς μορφῆς

$$f(x)\equiv 0 \pmod{p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}}$$

περιορίζεται στή μελέτη καί λύση ἰσοτιμιῶν τῆς μορφῆς

$$(5)\qquad f(x)\equiv 0 \pmod{p^\alpha}$$

κι αὐτή ἡ τελευταία ἰσοτιμία, πρόκειται σύντομα νά δοῦμε ὅτι περιορίζεται, γενικά, στήν ἰσοτιμία

$$(6)\qquad f(x)\equiv 0 \pmod p$$

Πραγματικά, κάθε x, πού ἱκανοποιεῖ τήν ἰσοτιμία (5) πρέπει, ἀναγκαστικά, νά ἱκανοποιεῖ τήν ἰσοτιμία (6). Ἔστω

$$x\equiv x_1 \pmod p$$

μιά ὁποιαδήποτε λύση τῆς ἰσοτιμίας (6). Τότε $x=x_1+pt_1$ ὅπου ὁ t_1 εἶναι κάποιος ἀκέραιος. Εἰσάγοντας αὐτή τήν τιμή τοῦ x στήν ἰσοτιμία $f(x)\equiv 0 \pmod{p^2}$ καί ἀναπτύσσοντας τό ἀριστερό μέλος μέ τή βοήθεια τοῦ τύπου τοῦ TAYLOR, βρίσκομε (παρατηρώντας ὅτι ὁ $\frac{1}{n!}f^{(n)}(x_1)$ εἶναι ἀκέραιος καί διαγράφοντας τούς ὅρους πού εἶναι πολλαπλάσια τοῦ p^2)

$$f(x_1)+pt_1f'(x_1)\equiv 0 \pmod{p^2},\quad \frac{f(x_1)}{p}+t_1f'(x_1)\equiv 0 \pmod p$$

Ἄν περιοριστοῦμε στήν περίπτωση πού ὁ $f'(x_1)$ δέν διαιρεῖται ἀπ' τόν p, θά ἔχομε μιά λύση

$$t_1\equiv t_1' \pmod p,\quad t_1=t_1'+pt_2$$

Ἡ ἔκφραση γιά τό x παίρνει τή μορφή

$$x=x_1+pt_1'+p^2t_2=x_2+p^2t_2$$

καί εἰσάγοντάς την στήν ἰσοτιμία

$$f(x)\equiv 0 \pmod{p^3}$$

βρίσκομε

$$f(x_2)+p^2t_2f'(x_2)\equiv 0 \pmod{p^3}$$

$$\frac{f(x_2)}{p^2}+t_2f'(x_2)\equiv 0 \pmod p$$

Έδω ὁ $f'(x_1)$ δέν διαιρεῖται ἀπ' τόν p, μιά καί

$$x_2 \equiv x_1 \pmod p$$
$$f'(x_2) \equiv f'(x_1) \pmod p$$

ἄρα ἡ τελευταία ἰσοτιμία ἔχει μιά λύση

$$t_2 \equiv t_2' \pmod p$$
$$t_2 = t_2' + pt_3$$

Ἡ ἔκφραση γιά τό x παίρνει τή μορφή

$$x = x_2 + p t_2' + p^2 t_3 = x_3 + p^2 t_3$$

κ.ὁ.κ. Μ' αὐτό τόν τρόπο, ἄν δοθεῖ μιά λύση τῆς ἰσοτιμίας (6), μποροῦμε νά βροῦμε μιά λύση τῆς ἰσοτιμίας (5) ἰσότιμη πρός αὐτή. Ἄρα ἄν ὁ $f'(x_1)$ δέν διαιρεῖται ἀπ' τόν p, κάθε λύση $x \equiv x_1 \pmod p$ τῆς ἰσοτιμίας (6) δίνει μιά λύση τῆς ἰσοτιμίας (5).

$$x = x_\alpha + p^\alpha t_\alpha$$
$$x \equiv x_\alpha \pmod{p^\alpha}$$

Παράδειγμα: Λύνομε τήν ἰσοτιμία

(7) $\quad f(x) \equiv 0 \pmod{27}$, $f(x) = x^4 + 7x + 4$

Ἡ ἰσοτιμία $f(x) \equiv 0 \pmod 3$ ἔχει μιά λυση $x \equiv 1 \pmod 3$. ἐδῶ $f'(1) \equiv 2 \pmod 3$ ἄρα ὁ $f'(1)$ δέν εἶναι διαιρετός ἀπ' τόν 3.

Βρίσκομε

$$x = 1 + 3t_1$$
$$f(1) + 3t_1 f'(1) \equiv 0 \pmod 9, \quad 3 + 3t_1 \cdot 2 \equiv 0 \pmod 9$$
$$2t_1 + 1 \equiv 0 \pmod 3, \quad t_1 \equiv 1 \pmod 3, \quad t_1 = 1 + 3t_2$$
$$x = 4 + 9t_2$$
$$f(4) + 9t_2 f'(4) \equiv 0 \pmod{27}, \quad 18 + 9t_2 \cdot 2 \equiv 0 \pmod{27}$$
$$2t_2 + 2 \equiv 0 \pmod 3, \quad t_2 \equiv 2 \pmod 3, \quad t_2 = 2 + 3t_3$$
$$x = 22 + 27t_3$$

Ἄρα ἡ ἰσοτιμία (7) ἔχει μιά λύση: $x \equiv 22 \pmod{27}$

Οἱ προηγούμενες σελίδες ἀποτελοῦν μετάφραση τοῦ Κεφ. IV τοῦ βιβλίου *Elements of Number Theory* I.M. Vinogradov (ἔκδοση σέ ἀγγλική γλώσσα).

Κεφάλαιο V

§1. Ισοτιμίες του δευτέρου βαθμού

α. Θά θεωρήσουμε μονάχα τίς άπλούστερες άπ' τίς ισοτιμίες βαθμού $n>1$, δηλ. τίς ισοτιμίες μέ δύο όρους:

(1) $$x^n \equiv a \pmod m \quad , \quad (a,m)=1$$

Άν ή ισοτιμία (1) έχει λύσεις, τότε ό α λέμε ότι είναι n-δύναμο ισοϋπόλοιπο, διαφορετικά ό α λέγεται n-δύναμο άνισοϋπόλοιπο. Εἰδικώτερα, γιά $n=2$ τά ισοϋπόλοιπα χαρακτηρίζονται τετραγωνικά, γιά $n=3$ κυβικά, γιά $n=4$ διτετραγωνικά.

β. Σ' αὐτό τό κεφάλαιο θά θεωρήσουμε τήν περίπτωση $n=2$ λεπτομερειακά, καί πρῶτα θά μελετήσουμε τίς ισοτιμίες δευτέρου βαθμοῦ, μέ δύο ὅρους πού τό μέτρο τους είναι περιττός πρῶτος p:

(2) $$x^2 \equiv a \pmod p \quad , \quad (a,p)=1$$

γ. Άν ὁ α είναι τετραγωνικό ισοϋπόλοιπο $\bmod p$, τότε ή ισοτιμία (2) έχει δύο λύσεις.

Πραγματικά, άν ὁ α είναι τετραγωνικό ισοϋπόλοιπο $\bmod p$, τότε ή ισοτιμία (2) έχει τουλάχιστον μιά λύση $x \equiv x_1 \pmod p$. Άλλά μιά καί $(-x_1)^2 = x_1^2$, ή ίδια ισοτιμία έχει τή δεύτερη λύση $x \equiv -x_1 \pmod p$. Αὐτή ή δεύτερη λύση είναι διαφορετική άπ' τήν πρώτη, γιατί ή $x_1 \equiv -x_1 \pmod p$, θά συνεπαγόταν τήν $2x_1 \equiv 0 \pmod p$, πού είναι άδύνατη άφοῦ $(2,p)=(x_1,p)=1$. Αὐτές οἱ δύο λύσεις έξαντλοῦν ὅλες τίς λύσεις τῆς ισοτιμίας (2) γιατί αὐτή μέ τό νά είναι δευτέρου βαθμοῦ, δέν μπορεῖ νά έχει παραπάνω άπό δυό λύσεις (c, §4, Κεφ. III).

δ. Ένα περιωρισμένο σύστημα $\bmod p$ άποτελεῖται άπό $\frac{p-1}{2}$ τετραγωνικά ισοϋπόλοιπα πού είναι ισότιμα πρός τούς άριθμούς.

(3) $$1^2, 2^2, \ldots, \left(\tfrac{p-1}{2}\right)^2$$

καί $\frac{p-1}{2}$ τετραγωνικά άνισοϋπόλοιπα.

Πραγματικά, ἀνάμεσα στά ὑπόλοιπα ἑνός περιωρισμένου συστήματος $\bmod p$, τά τετραγωνικά ισοϋπόλοιπα είναι ἀκριβῶς ἐκεῖνα πού είναι τετράγωνα τῶν ἀριθμῶν (περιορισμένου συστήματος ὑπολοίπων)

(4) $$-\tfrac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \tfrac{p-1}{2}$$

δηλ. οἱ ἀριθμοί (3). Ἐδῶ οἱ ἀριθμοί (3) είναι ἀνισότιμοι $\bmod p$, γιατί ἀπ' τή σχέση $k^2 \equiv l^2 \pmod p$, $0<k<l\leq\frac{p-1}{2}$ θά είχαμε ότι ή ισοτιμία $x^2 \equiv l^2 \pmod p$ ικανοποιεῖται ἀπ' τούς τέσσερεις ἀριθμούς $x \equiv -l, -k, k, l$ τοῦ συστήματος (4), πρᾶγμα πού ἔρχεται σέ ἀντίφαση μέ τό γ.

ε. Άν ὁ α είναι τετραγωνικό ισοϋπόλοιπο $\bmod p$ τότε

(5) $$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

ἐνῶ ἄν ὁ α είναι τετραγωνικό ἀνισοϋπόλοιπο $\bmod p$, τότε

(6) $$a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

Πραγματικά, άπ'τό θεώρημα τοῦ Fermat

$$a^{p-1}\equiv 1(\mathrm{mod}p)\ ,\quad (a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1)\equiv 0(\mathrm{mod}p)$$

Ἀκριβῶς ἕνας ἀπ'τούς παράγοντες τοῦ ἀριστεροῦ μέλους τῆς τελευταίας ἰσοτιμίας εἶναι διαιρετός ἀπ'τόν p (ἀποκλείεται νά εἶναι καί οἱ δυό γιατί αὐτοί θά συνεπαγόταν ὅτι ὁ 2 θά ἦταν διαιρετός ἀπ'τόν p).

Ἀλλά κάθε τετραγωνικό ἰσοϋπόλοιπο a ἱκανοποιεῖ τήν ἰσοτιμία.

$$a\equiv x^2(\mathrm{mod}p) \tag{7}$$

γιά κάποιο x καί γι'αὐτό ἱκανοποιεῖ καί τήν (6) πού μπορεῖ νά προκύψει ἄν ὑψώσομε καί τά δύο μέλη τῆς (7) στή δύναμη $\frac{p-1}{2}$. Ἐδῶ, τά τετραγωνικά ἰσοϋπόλοιπα ἐξαντλοῦν ὅλες τίς λύσεις τῆς ἰσοτιμίας (5) μιά καί αὐτή δέν εἶναι δυνατόν νά ἔχει περισσότερους ἀπό $\frac{p-1}{2}$ λύσεις, ἀφοῦ εἶναι ἰσοτιμία βαθμοῦ $\frac{p-1}{2}$.

Ἄρα τά τετραγωνικά ἀνισοϋπόλοιπα ἱκανοποιοῦν τήν ἰσοτιμία (6).

§2. Τό σύμβολο τοῦ Legendre

a. Τώρα θά θεωρήσομε τό σύμβολο τοῦ Legendre $\left(\frac{a}{p}\right)$ (πού διαβάζεται: τό σύμβολο τοῦ a ὡς πρός p. Τό σύμβολο αὐτό ὁρίζεται γιά ὅλους τούς a πού δέν εἶναι διαιρετοί ἀπ'τόν p· εἶναι ἴσο μέ 1 ἄν ὁ a εἶναι τετραγωνικό ἰσοϋπόλοιπο, καί ἴσο μέ -1 ἄν ὁ a εἶναι τετραγωνικό ἀνισοϋπόλοιπο. Ὁ ἀριθμός a λέγεται ἀριθμητής καί ὁ ἀριθμός p παρονομαστής τοῦ συμβόλου.

b. Ἀπ'τό e,§1, γίνεται φανερό ὅτι ἔχομε

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}(\mathrm{mod}p)$$

c. Ἐδῶ συνάγομε τίς πιό σπουδαῖες ἰδιότητες τοῦ συμβόλου Legendre καί στήν ἑπομένη παράγραφο, τίς ἰδιότητες τῆς γενίκευσης αὐτοῦ τοῦ συμβόλου, τοῦ Jacobi, τό ὁποῖο εἶναι χρήσιμο γιά τό γρήγορο ὑπολογισμό αὐτοῦ τοῦ συμβόλου καί, κατά συνέπεια, λύνει τό πρόβλημα τῆς δυνατότητας τῆς ἰσοτιμίας

$$x^2\equiv a(\mathrm{mod}p)$$

d. Ἄν $a\equiv a_1(\mathrm{mod}p)$, τότε $\left(\frac{a}{p}\right)=\left(\frac{a_1}{p}\right)$

Αὐτή ἡ ἰδιότητα προκύπτει ἀπ'τό γεγονός ὅτι ἀριθμοί μιᾶς κλάσης ἰσοτιμίας εἶναι ἤ ὅλοι τετραγωνικά ἰσοϋπόλοιπα ἤ ὅλοι τετραγωνικά ἀνισοϋπόλοιπα.

e. $\left(\frac{1}{p}\right)=1$

Πραγματικά, $1=1^2$ ἄρα ὁ 1 εἶναι τετραγωνικό ἰσοϋπόλοιπο.

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

Αὐτή ἡ ἰδιότητα ἔπεται ἀπ'τό b. γιά $a=-1$ Μιά καί ὁ $\frac{p-1}{2}$ εἶναι ἄρτιος γιά p τῆς μορφῆς $4m+1$ καί περιττός γιά p τῆς μορφῆς $4m+3$ ἐπειδή ὅτι ὁ -1 εἶναι τετραγωνικό ὑπόλοιπο τῶν πρώτων τῆς μορφῆς $4m+1$ καί τετραγωνικό ἀνισοϋπόλοιπο τῶν πρώτων τῆς μορφῆς $4m+3$.

g. $$\left(\frac{ab\cdots l}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\cdots\left(\frac{l}{p}\right)$$

Πραγματικά, ἔχομε

$$\left(\frac{ab\cdots l}{p}\right)\equiv(ab\cdots l)^{\frac{p-1}{2}}\equiv a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}\cdots l^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\cdots\left(\frac{l}{p}\right)\pmod p$$

ἀπ'ὅπου ἔπεται ὅτι ὁ ἰσχυρισμός μας ἀληθεύει. Μιά συνέπεια τοῦ ἀποτελέσματός μας εἶναι.

$$\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)$$

δηλ. μποροῦμε νά παραλείπομε ὁποιοδήποτε τετραγωνικό παράγοντα ἀπ' τόν ἀριθμητή ἑνός συμβόλου.

h. Προκειμένου νά συνάγομε περισσότερες ἰδιότητες τοῦ συμβόλου τοῦ Legendre, τοῦ δίνομε πρῶτα μιά διαφορετική ἑρμηνεία. Γράφοντας $\beta=\frac{p-1}{2}$, θεωροῦμε τίς ἰσότιμίες.

$$(1)\quad\begin{cases} a\cdot 1\equiv\varepsilon_1 r_1\pmod p\\ a\cdot 2\equiv\varepsilon_2 r_2\pmod p\\ \cdots\cdots\cdots\\ a\cdot\beta\equiv\varepsilon_\beta\cdot r_\beta\pmod p\end{cases}\qquad \beta=\frac{p-1}{2}$$

ὅπου $\varepsilon_x r_x$ εἶναι τό ἀπολύτως ἐλάχιστο ὑπόλοιπο τοῦ $a.x$, καί r_x εἶναι ἡ ἀπόλυτη τιμή αὐτοῦ τοῦ ὑπολοίπου, ἔτσι πού $\varepsilon_x=\pm 1$.
Οἱ ἀριθμοί $a.1, -a.1, a.2, -a.2, \ldots, a\beta, -a\beta$ σχηματίζουν ἕνα περιορισμένο σύστημα ὑπολοίπων mod p (ς, §6, Κεφ. II)· τά ἀπολύτως ἐλάχιστα ὑπόλοιπά τους εἶναι ἀκριβῶς τά $\varepsilon_1 r_1, -\varepsilon_1 r_1, \varepsilon_2 r_2, -\varepsilon_2 r_2, \ldots, \varepsilon_\beta r_\beta, -\varepsilon_\beta r_\beta$· τά θετικά ἀπ'αὐτά δηλ. τά $r_1, r_2, \ldots, r_\beta$ πρέπει νά συμπίπτουν μέ τούς ἀριθμούς $1, 2, \ldots, \beta$ (ὅ, §4, Κεφ. II)· Πολλαπλασιάζοντας κατά μέλη τίς (1) καί διαιρώντας μέ τόν $1.2\cdots\beta=r_1 r_2\cdots r_\beta$, βρίσκομε, $a^{\frac{p-1}{2}}\equiv\varepsilon_1\varepsilon_2\cdots\varepsilon_\beta\pmod p$, ἀπ'ὅπου ἔχομε (b)

$$(2)\qquad\left(\frac{a}{p}\right)=\varepsilon_1\varepsilon_2\cdots\varepsilon_\beta$$

i. Ἡ ἔκφραση τοῦ συμβόλου τοῦ Legendre πού βρήκαμε μπορεῖ νά τεθεῖ μέ πιό συμμετρική μορφή. Ἔχομε:

$$\left[\frac{2ax}{p}\right]=\left[2\left[\frac{ax}{p}\right]+2\left\{\frac{ax}{p}\right\}\right]=2\left[\frac{ax}{p}\right]+\left[2\left\{\frac{ax}{p}\right\}\right]$$

καί ὁ ἀριθμός αὐτός εἶναι ἄρτιος ἤ περιττός, ἀνάλογα μέ τό ἄν τό ἐλάχιστο θετικό ὑπόλοιπο τοῦ ἀριθμοῦ ax εἶναι μικρότερο ἤ μεγαλύτερο ἀπ'τό $\frac{p}{2}$ δηλ. ἀνάλογα μέ τό ἄν $\varepsilon_x=1$, ἤ $\varepsilon_x=-1$. Ἀπ'αὐτό γίνεται φανερό ὅτι

$$\varepsilon_x=(-1)^{\left[\frac{2ax}{p}\right]}$$

δπότε άπ'τή (2) έχομε:

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{\frac{p}{2}} \left[\frac{2ax}{p}\right]}$$

j. Υποθέτοντας τόν a περιττό μετασχηματίζομε τήν τελευταία έξίσωση. Έχομε (ό a+p είναι άρτιος)

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) = (-1)^{\sum_{x=1}^{\frac{p}{2}} \left[\frac{(a+p)x}{p}\right]} =$$

$$= (-1)^{\sum_{x=1}^{\frac{p}{2}} \left[\frac{ax}{p}\right] + \sum_{x=1}^{\frac{p}{2}} x}$$

άρα

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{\frac{p}{2}} \left[\frac{ax}{p}\right] + \frac{p^2-1}{8}} \qquad (3)$$

Ό τύπος (3) μάς έπιτρέπει νά συμπεράνομε δυό πολύ σημαντικές ίδιότητες τού συμβόλου τού Legendre.

K. $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Αύτό έπεται άπ'τόν τύπο (3) γιά a=1.

Έπιπλέον, μιά καί

$$\frac{(8m\pm1)^2-1}{8} = 8m^2 \pm 2m \quad , \text{άρτιος}$$

ένώ

$$\frac{(8m\pm3)^2-1}{8} = 8m^2 \pm 6m + 1 \quad , \text{περιττός},$$

έπεται ότι ό 2 είναι τετραγωνικό ίσοϋπόλοιπο τών πρώτων τής μορφής $8m\pm1$ $(8m+1,\ 8m+7)$, καί τετραγωνικό άνισοϋπόλοιπο τών πρώτων τής μορφής $8m\pm3$ $(8m+3,\ 8m+5)$

l. <u>Άν οί p, q είναι περιττοί πρώτοι, τότε (ό νόμος τής τετραγωνικής άντιστροφής)</u>

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

Άφού ό $\frac{p-1}{2}\cdot\frac{q-1}{2}$ είναι περιττός μονάχα στήν περίπτωση πού καί οί δυό άριθμοί p, q είναι τής μορφής $4m+3$, καί άρτιος άν ένας, τουλάχιστον άπ'αύτούς τούς άριθμούς είναι τής μορφής $4m+1$ ή παραπάνω ίδιότητα μπορεί νά διατυπωθεί ώς έξής:

"Αν καί οί δυό άριθμοί p καί q είναι τής μορφής $4m+3$, τότε

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)$$

ένῶ άν ένας, τουλάχιστον, είναι τής μορφής $4m+1$, τότε

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$$

Προκειμένου ν'άποδείξομε τό άποτέλεσμά μας, παρατηροῦμε ότι, ό τύπος (3) , λόγω τοῦ $k=\frac{p}{2}$ παίρνει τή μορφή

$$\left(\frac{q}{p}\right)=(-1)^{\sum_{x=1}^{\frac{p}{2}}\left[\frac{qx}{p}\right]} \qquad (4)$$

"Αν θέσομε $\frac{q-1}{2}=q_1$, θεωροῦμε τά p_1q_1 ζευγάρια τῶν άριθμῶν, πού παίρνομε όταν οί άριθμοί x καί y στίς έκφράσεις qx, py διατρέχουν τίς τιμές

$$x=1,2,\cdots,p_1\ ,\quad y=1,2,\cdots,q_1$$

άνεξάρτητα.

Δέν μπορεῖ ποτέ νά έχομε $qx=py$, γιατί τότε θά συμπεραίναμε άπ' αύτή τήν έξίσωση ότι ό py είναι πολλαπλάσιο τοῦ q , πράγμα άδύνατο, άφοῦ $(p,q)=(y,q)=1$ (γιατί $0<y<q$). "Αρα μποροῦμε νά θέσομε, $p_1q_1=S_1+S_2$, όπου S_1 είναι τό πλῆθος τῶν ζευγαριῶν μέ $qx<py$ καί S_2 τό πλῆθος τῶν ζευγαριῶν μέ $py<qx$.

Είναι φανερό ότι S_1 είναι, έπίσης, τό πλῆθος τῶν ζευγαριῶν μέ $x<\frac{p}{q}y$ Γιά δοσμένο y μποροῦμε νά πάρουμε $x=1,2,\cdots,\left[\frac{p}{q}y\right]$. (Μιά καί $\frac{p}{q}y\leq\frac{p}{q}q_1<\frac{p}{2}$, έχομε $\left[\frac{p}{q}y\right]\leq p_1$). Κατά συνέπεια,

$$S_1=\sum_{y=1}^{q_1}\left[\frac{p}{q}y\right]$$

'Ανάλογα, μποροῦμε ν'άποδείξομε ότι

$$S_2=\sum_{x=1}^{p_1}\left[\frac{q}{p}x\right]$$

"Αλλά τότε ή έξίσωση (4) δίνει.

$$\left(\frac{p}{q}\right)=(-1)^{S_1}\ ,\quad \left(\frac{q}{p}\right)=(-1)^{S_2}$$

άρα

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{S_1+S_2}=(-1)^{p_1q_1}$$

άπ'όπου έπεται ή ζητούμενη ίδιότητα.

§3. Τό σύμβολο τοῦ Jacobi

α. Προκειμένου νά ὑπολογίζομε πιό σύντομα τό σύμβολο τοῦ Legendre, θεωροῦμε τό πιό γενικό σύμβολο τοῦ Jacobi. "Εστω P ένας περιττός άριθμός μεγαλύτερος άπ'τή μονάδα, καί έστω $P=p_1p_2\cdots p_r$ ή άνάλυ-

σή του σέ πρώτους παράγοντες (μερικοί άπ' τούς όποίους μπορεί νά είναι ίσοι). Άκόμη, έστω ότι $(a,P)=1$. Τότε τό σύμβολο τοῦ Jacobi όρίζεται άπ' τήν έξίσωση:

$$\left(\frac{a}{P}\right)=\left(\frac{a}{P_1}\right)\left(\frac{a}{P_2}\right)\cdots\left(\frac{a}{P_r}\right)$$

Οί πολύ γνωστές ίδιότητες τοῦ συμβόλου τοῦ Legendre μᾶς έπιτρέπουν νά συμπεράνομε άνάλογες ίδιότητες γιά τό σύμβολο τοῦ Jacobi.

(b) Άν $a\equiv a_1 \pmod P$, τότε $\left(\frac{a}{P}\right)=\left(\frac{a_1}{P}\right)$

Πραγματικά,

$$\left(\frac{a}{P}\right)=\left(\frac{a}{P_1}\right)\left(\frac{a}{P_2}\right)\cdots\left(\frac{a}{P_r}\right)=\left(\frac{a_1}{P_1}\right)\left(\frac{a_1}{P_2}\right)\cdots\left(\frac{a_1}{P_r}\right)=\left(\frac{a_1}{P}\right)$$

γιατί ό a μέ τό νά είναι ίσότιμος πρός τόν $a_1 \pmod P$ είναι έπίσης ίσότιμος πρός τόν $a_1, \bmod p_1, \bmod p_2, \ldots \bmod p_r$ πού είναι διαιρέτες τοῦ P.

(c) $\left(\frac{1}{P}\right)=1$

Πραγματικά,

$$\left(\frac{1}{P}\right)=\left(\frac{1}{P_1}\right)\left(\frac{1}{P_2}\right)\cdots\left(\frac{1}{P_r}\right)=1$$

(d) $\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}$

Γιά νά τό άποδείξομε αύτό παρατηροῦμε ότι.

$$(1)\quad \left(\frac{-1}{P}\right)=\left(\frac{-1}{P_1}\right)\left(\frac{-1}{P_2}\right)\cdots\left(\frac{-1}{P_r}\right)=(-1)^{\frac{P_1-1}{2}+\frac{P_2-1}{2}+\cdots+\frac{P_r-1}{2}}$$

Άλλά $\frac{P-1}{2}=\frac{P_1P_2\cdots P_r-1}{2}=\frac{\left(1+2\frac{P_1-1}{2}\right)\left(1+2\frac{P_2-1}{2}\right)\cdots\left(1+2\frac{P_r-1}{2}\right)}{2}=$

$$=\frac{P_1-1}{2}+\frac{P_2-1}{2}+\cdots+\frac{P_r-1}{2}+2N$$

άρα, άπ' τόν τύπο (1) συμπεραίνομε

$$\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}$$

(e) $\left(\frac{ab\ldots\ell}{P}\right)=\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)\cdots\left(\frac{\ell}{P}\right)$

Πραγματικά,

$$\left(\frac{ab\ldots\ell}{P}\right)=\left(\frac{ab\ldots\ell}{P_1}\right)\left(\frac{ab\ldots\ell}{P_2}\right)\cdots\left(\frac{ab\ldots\ell}{P_r}\right)=\left(\frac{a}{P_1}\right)\left(\frac{b}{P_1}\right)\cdots\left(\frac{\ell}{P_1}\right)\cdots\left(\frac{a}{P_r}\right)\left(\frac{b}{P_r}\right)\cdots\left(\frac{\ell}{P_r}\right)$$

και πολλαπλασιάζοντας τα σύμβολα με τον ίδιο αριθμητή παίρνομε τη ζητούμενη ιδιότητα. Απ' αυτή παίρνομε το πόρισμα,

$$\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right)$$

(f) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$

Πραγματικά,

(2) $$\left(\frac{2}{p}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_r}\right)=(-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\cdots+\frac{p_r^2-1}{8}}$$

Αλλά $$\frac{p^2-1}{8}=\frac{p^2p_1^2\cdots p_r^2-1}{8}=\frac{\left(1+8\frac{p^2-1}{8}\right)\left(1+8\frac{p_1^2-1}{8}\right)\cdots\left(1+8\frac{p_r^2-1}{8}\right)}{8}=$$

$$=\frac{p^2-1}{8}+\frac{p_1^2-1}{8}+\cdots+\frac{p_r^2-1}{8}+2N$$

άρα, απ' τον τύπο (2) συνάγομε.

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$$

(g) Αν P, Q είναι θετικοί και πρώτοι μεταξύ τους περιττοί αριθμοί, τότε

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right)$$

!!!

Πραγματικά, έστω $Q=q_1q_2\cdots q_s$ η ανάλυση του Q σε πρώτους παράγοντες (μερικοί απ' τούς οποίους μπορεί να είναι ίσοι). Έχομε.

$$\left(\frac{Q}{P}\right)=\left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right)\cdots\left(\frac{Q}{p_r}\right)=\prod_{\alpha=1}^{r}\prod_{\beta=1}^{s}\left(\frac{q_\beta}{p_\alpha}\right)=(-1)^{\sum_{\alpha=1}^{r}\sum_{\beta=1}^{s}\frac{p_\alpha-1}{2}\cdot\frac{q_\beta-1}{2}}\cdot\prod_{\alpha=1}^{r}\prod_{\beta=1}^{s}\left(\frac{p_\alpha}{q_\beta}\right)$$

$$=(-1)^{\left(\sum_{\alpha=1}^{r}\frac{p_\alpha-1}{2}\right)\left(\sum_{\beta=1}^{s}\frac{q_\beta-1}{2}\right)}\cdot\left(\frac{P}{Q}\right)$$

Αλλά όπως στό d. βρίσκομε,

$$\frac{P-1}{2}=\sum_{\alpha=1}^{r}\frac{p_\alpha-1}{2}+2N\ ,\quad \frac{Q-1}{2}=\sum_{\beta=1}^{s}\frac{q_\beta-1}{2}+2N_1$$

άρα $$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right)$$

παράδειγμα: Σάν παράδειγμα ὑπολογισμοῦ τοῦ συμβόλου τοῦ Legendre (θά τό θεωρήσομε σάν εἰδική περίπτωση τοῦ συμβόλου τοῦ Jacobi) ἐξετάζομε τήν ἐπιλυσιμότητα τῆς ἰσοτιμίας

$$x^2 \equiv 219 \pmod{383}$$

Ἔχομε (ἐφαρμόζοντας μέ τή σειρά τίς ἰδιότητες g, b, τό πόρισμα 4, τοῦ c, g, b, e, f, g, b, d.):

$$\left(\frac{219}{383}\right) = -\left(\frac{383}{219}\right) = -\left(\frac{164}{219}\right) = -\left(\frac{41}{219}\right) = -\left(\frac{219}{41}\right) = -\left(\frac{19}{41}\right) =$$

$$= -\left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -\left(\frac{7}{41}\right) = -\left(\frac{41}{7}\right) = -\left(\frac{-1}{7}\right) = 1$$

ἄρα ἡ θεωρούμενη ἰσοτιμία ἔχει δυό λύσεις.

§4. Ἡ περίπτωση σύνθετων μέτρων

a. Οἱ ἰσοτιμίες δευτέρου βαθμοῦ μέ σύνθετα μέτρα ἐρευνοῦνται καί λύνονται σύμφωνα μέ τίς γενικές μεθόδους τῆς § 5, Κεφ. 3.

b. Ἀρχίζομε μέ μιά ἰσοτιμία τῆς μορφῆς

(1) $\quad x^2 \equiv a \pmod{p^\alpha}$, $\alpha > 0$, $(a,p)=1$

ὅπου ὁ p εἶναι περιττός πρῶτος.

Ἄν θέσομε $f(x) = x^2 - a$, ἔχομε $f'(x) = 2x$ καί ἄν $x \equiv x_1 \pmod{p}$ εἶναι μιά λύση τῆς ἰσοτιμίας

(2) $\quad x^2 \equiv a \pmod{p}$

τότε, μιά καί $(a,p)=1$ ἔχομε ἐπίσης $(x_1, p)=1$ καί ἀφοῦ ὁ p εἶναι περιττός, $(2x_1, p)=1$ δηλ. ὁ $f'(x_1)$ δέν εἶναι διαιρετός ἀπ' τόν p.

Ἄρα γιά νά βροῦμε τίς λύσεις τῆς ἰσοτιμίας (1) μποροῦμε νά ἐφαρμόσομε τούς συλλογισμούς τοῦ b, §5, Κεφ. III , ἐνῶ κάθε λύση τῆς ἰσοτιμίας (2) μᾶς δίνει μιά λύση τῆς ἰσοτιμίας (1) . Ἀπ' αὐτό ἕπεται ὅτι: Ἡ ἰσοτιμία (1) ἔχει δυό λύσεις ἤ καμιά ἀνάλογα μέ τό ἄν ὁ a εἶναι τετραγωνικό ὑπόλοιπο ἤ τετραγωνικό ἀνυπόλοιπο $\bmod p$

c. Τώρα θεωροῦμε τήν ἰσοτιμία (1): $x^2 \equiv a \pmod{2^\alpha}$, $\alpha > 0$, $(a,2)=1$

Ἐδῶ ὁ $f'(x_1) = 2x_1$ εἶναι διαιρετός ἀπ' τόν 2 καί κατά συνέπεια, οἱ συλλογισμοί τοῦ b, § 5, Κεφ. III, δέν ἐφαρμόζονται· μποροῦν ὅμως νά τροποποιηθοῦν ὡς ἑξῆς:

d. Ἄν ἡ ἰσοτιμία (3) λύνεται, τότε, μιά καί $(a,2)=1$, θά ἔχομε $(x,2)=1$, δηλ. $x = 1+2t$, ὅπου ὁ t εἶναι ἀκέραιος. Ἡ ἰσοτιμία (2) παίρνει τή μορφή

$$1 + 4t(t+1) \equiv a \pmod{2^\alpha}$$

Ἀλλά ἕνας ἀπ' τούς ἀριθμούς $t, t+1$ εἶναι ἄρτιος, ἄρα ὁ $4t(t+1)$ εἶναι πολλαπλάσιο τοῦ 8. Ἄρα γιά νά εἶναι δυνατή ἡ τελευταία ἰσοτιμία, καί μαζί μ' αὐτή ἡ ἰσοτιμία (3) εἶναι ἀναγκαῖο νά ἰσχύει.

(4) $\quad a \equiv 1 \pmod{4}$ γιά $\alpha = 2$, $a \equiv 1 \pmod{8}$ γιά $\alpha \geq 3$.

e. Σ' αὐτές τίς περιπτώσεις, πού ἡ συνθήκη (4) ἱκανοποιεῖται, μελετοῦμε

τό πρόβλημα τῆς εὑρεσης τῶν λύσεων καί τοῦ πλήθους τους.
Γιά $\alpha \leq 3$, ὅλοι οἱ περιττοί ἀριθμοί ἱκανοποιοῦν τήν ἰσοτιμία, λόγω τοῦ d. Ἄρα ἡ ἰσοτιμία $x^2 \equiv a \pmod 2$ ἔχει μιά λύση: $x \equiv 1 \pmod 2$, ἡ ἰσοτιμία $x^2 \equiv a \pmod 4$ ἔχει δυό λύσεις: $x \equiv 1, 3 \pmod 4$, ἡ ἰσοτιμία $x^2 \equiv a \pmod 8$ ἔχει τέσσερεις λύσεις $x \equiv 1, 3, 5, 7 \pmod 8$
Γιά νά μελετήσομε τίς περιπτώσεις $\alpha = 4, 5, \cdots$ ὅλοι οἱ περιττοί ἀριθμοί χωρίζονται σέ δυό ἀριθμητικές προόδους:

$$x = \pm (1 + 4t_3). \tag{5}$$

$$\left(1+4t_3 \equiv 1 \pmod 4 \, , \; -1-4t_3 \equiv -1 \equiv 3 \pmod 4 \right)$$

Τώρα ἀποφασίζομε ποιοί ἀπ' τούς παραπάνω ἀριθμούς ἱκανοποιοῦν τήν ἰσοτιμία $x^2 \equiv a \pmod{16}$. Βρίσκομε

$$(1+4t_3)^2 \equiv a \pmod{16} \, , \; t_3 \equiv \frac{a-1}{8} \pmod 2$$

$$t_3 = t_3' + 2t_4 \, , \quad x = \pm (1 + 4t_3' + 8t_4) = \pm (x_4 + 8t_4)$$

Τώρα ἀποφασίζομε ποιοί ἀπ' τούς τελευταίους ἀριθμούς ἱκανοποιοῦν τήν ἰσοτιμία $x^2 \equiv a \pmod{32}$. Βρίσκομε,

$$(x_4 + 8t_4)^2 \equiv a \pmod{32} \, , \; t_4 = t_4' + 2t_5 \, , \; x = \pm (x_5 + 16t_5)$$

κ.λ.π. Μ' αὐτόν τόν τρόπο βρίσκομε ὅτι οἱ τιμές τοῦ x πού ἱκανοποιοῦν τήν ἰσοτιμία (3) γιά $\alpha > 3$, παριστάνονται μέ τή μορφή

$$x = \pm (x_\alpha + 2^{\alpha-1} t_\alpha)$$

Αὐτές οἱ τιμές τοῦ x σχηματίζουν τέσσερεις διαφορετικές λύσεις τῆς ἰσοτιμίας (3)

$$x \equiv x_\alpha, \; x_\alpha + 2^{\alpha-1}, \; -x_\alpha, \; -x_\alpha - 2^{\alpha-1} \pmod{2^\alpha}$$

(ὡς πρός μέτρο 4 οἱ δυό πρῶτες εἶναι ἰσότιμες πρός τό 1 ἐνῶ οἱ δυό ἑπόμενες εἶναι ἰσότιμες πρός τό -1).

Παράδειγμα Ἡ ἰσοτιμία

$$x^2 \equiv 57 \pmod{64}$$

ἔχει τέσσερεις λύσεις, γιατί $57 \equiv 1 \pmod 8$. Παριστάνοντας τόν x μέ τή μορφή $x = \pm (1 + 4t_3)$ βρίσκομε

$$(1+4t_3)^2 \equiv 57 \pmod{16} \, , \; 8t_3 \equiv 56 \pmod{16} \, , \; t_3 \equiv 1 \pmod 2 \, , \; t_3 = 1 + 2t_4$$

$$x = \pm (5 + 8t_4)$$

$$(5+8t_4)^2 \equiv 57 \pmod{32} \, , \; 5.16 t_4 \equiv 32 \pmod{32} \, , \; t_4 \equiv 0 \pmod 2 \, , \; t_4 = 2t_5$$

$$x = \pm (5 + 16t_5)$$

$$(5+16t_5)^2 \equiv 57 \pmod{64} \, , \; 5.32 t_5 \equiv 32 \pmod{64} \, , \; t_5 \equiv 1 \pmod 2 \, , \; t_5 = 1 + 2t_6 \, ,$$

$$x = \pm (21 + 32t_6)$$

Ἄρα οἱ λύσεις τῆς ἰσοτιμίας (6) εἶναι:

$$x \equiv \pm 21, \pm 53 \pmod{64}$$

ε. Ἀπ' τά c, d. καί e ἕπεται ὅτι:

Οἱ ἀναγκαῖες συνθῆκες γιά τήν ἐπιλυσιμότητα τῆς ἰσοτιμίας

$$x^2 \equiv a \pmod{2^\alpha}$$

εἶναι: $a \equiv 1 \pmod 4$ γιά $\alpha = 2$, $a \equiv 1 \pmod 8$ γιά $\alpha \geq 3$. Ἄν αὐτές οἱ

συνθήκες ικανοποιοῦνται, τότε τό πλῆθος τῶν λύσεων εἶναι:
1 γιά $\alpha=1$, 2 γιά $\alpha=2$, 4 γιά $\alpha\geq 3$

g. Ἀπ' τά b, f καί τό a, §6, Κεφ. III, ἕπεται ὅτι:
οἱ ἀναγκαῖες συνθῆκες γιά τήν ἐπιλυσιμότητα τῶν ἰσοτιμιῶν τῆς μορφῆς

$$x^2\equiv a \pmod m, \quad m=2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}, \quad (a,m)=1$$

εἶναι:

$a\equiv 1 \pmod 4$ γιά $\alpha=2$, $a\equiv 1 \pmod 8$ γιά $\alpha\geq 3$,

$$\left(\frac{a}{p_1}\right)=1, \ \left(\frac{a}{p_2}\right)=1, \ \ldots, \ \left(\frac{a}{p_k}\right)=1$$

Ἂν ὅλες αὐτές οἱ συνθῆκες ικανοποιοῦνται, τό πλῆθος τῶν λύσεων εἶν
2^k γιά $\alpha=0$, καί $\alpha=1$; 2^{k+1} γιά $\alpha=2$, 2^{k+2} γιά $\alpha\geq 3$.

Οἱ προηγούμενες σελίδες ἀφορέλιων μετάγραψη τοῦ Κεφαλαίου V τοῦ βιβλίου *Elements of Number Theory* (I.M. Vinogradov).

Κεφάλαιο VI

Αρχικές ρίζες και δείκτες

§ 1. Γενικά θεωρήματα

a. Για (a,m)=1 υπάρχει θετικός γ τέτοιος ώστε $a^\gamma \equiv 1 \pmod m$, π.χ. (απ' το θεώρημα του Euler) ο $\gamma = \varphi(m)$. Ο ελάχιστος γ με αυτή την ιδιότητα καλείται <u>τάξη του a modulo m</u>.

b. Αν η τάξη του a mod m είναι δ, τότε οι αριθμοί $1 = a^0, a^1, \dots, a^{\delta-1}$ είναι ανισότιμοι mod m.

Πράγματι, σε αντίθετη περίπτωση θα είχαμε μια σχέση της μορφής

$a^l \equiv a^k \pmod m$, $0 \le k < l < \delta$, οπότε $a^{l-k} \equiv 1 \pmod m$, $0 < l-k < \delta$, που αντίκειται στον ορισμό του δ.

c. Αν η τάξη του a mod m είναι δ, τότε ισχύει $a^\gamma \equiv a^{\gamma'} \pmod m$ αν και μόνο αν $\gamma \equiv \gamma' \pmod \delta$· ειδικώτερα (για $\gamma' = 0$), ισχύει $a^\gamma \equiv 1 \pmod m$ αν και μόνο αν ο γ είναι διαιρετός απ' τον δ.

Πράγματι, ας είναι r και r_1 τα ελάχιστα μη αρνητικά υπόλοιπα των γ, γ' modulo δ. Τότε για κάποιους q και q_1 έχομε $\gamma = \delta q + r$, $\gamma' = \delta q_1 + r_1$. Απ' αυτές τις σχέσεις και την $a^0 \equiv 1 \pmod m$ έπεται ότι

$$a^\gamma \equiv (a^\delta)^q \cdot a^r = a^r \pmod m, \quad a^{\gamma'} \equiv (a^\delta)^{q_1} \cdot a^{r_1} \equiv a^{r_1} \pmod m.$$

Συνεπώς, $a^\gamma \equiv a^{\gamma'} \pmod m$ τότε και μόνο τότε αν $a^r \equiv a^{r_1} \pmod m$, δηλ. (b), όταν $r = r_1$.

d. Απ' τη σχέση $a^{\varphi(m)} \equiv 1 \pmod m$ και το **c** (για $\gamma' = 0$) έπεται ότι το $\varphi(m)$ διαιρείται απ' το δ. Άρα οι τάξεις των διαφόρων αριθμών modulo m είναι διαιρέτες του $\varphi(m)$. Ο μεγαλύτερος απ' αυτούς τους διαιρέτες είναι ο $\varphi(m)$. Οι αριθμοί των οποίων η τάξη mod m είναι $\varphi(m)$ (αν υπάρχουν τέτοιοι) καλούνται <u>αρχικές ρίζες mod m</u>.

§2. Αρχικές ρίζες modulo p^α και $2p^\alpha$.

a. Έστω p ένας περιττός πρώτος και $\alpha \geq 1$. Θα δείξωμε ότι υπάρχουν αρχικές ρίζες modulo p^α και $2p^\alpha$.

b. Αν η τάξη του x mod m είναι ab, τότε η τάξη του x^a είναι b.

Πράγματι, έστω ότι η τάξη του x^a είναι δ. Τότε $x^{a\delta} \equiv 1 \pmod m$, οπότε $(c, §1)$ το $a\delta$ διαιρείται από τον ab, δηλ. το δ διαιρείται από τον b. Αφ' ετέρου $x^{ab} \equiv 1 \pmod m$, από όπου $(x^a)^b \equiv 1 \pmod m$ και, συνεπώς $(c, §1)$, το b διαιρείται από τον δ. Άρα $\delta = b$.

c. Αν η τάξη του x mod m είναι a και η τάξη του y είναι b, όπου $(a,b)=1$, τότε η τάξη του xy είναι ab.

Πράγματι, έστω ότι η τάξη του xy είναι δ. Τότε $(xy)^\delta \equiv 1 \pmod m$. Από αυτήν έπεται ότι $x^{b\delta} y^{b\delta} \equiv 1 \pmod m$ και $(c, §1)$ $x^{b\delta} \equiv 1 \pmod m$. Άρα $(c, §1)$ το $b\delta$ διαιρείται από τον a και, λόγω της $(b,a)=1$, το δ διαιρείται από τον a. Ομοίως συμπεραίνομε ότι το δ διαιρείται από τον b και, λόγω της $(a,b)=1$, το δ διαιρείται και από τον ab. Αφ' ετέρου, από την $(xy)^{ab} \equiv 1 \pmod m$ έπεται $(c, §1)$ ότι το ab διαιρείται από τον δ. Άρα $\delta = ab$.

d. Υπάρχουν αρχικές ρίζες modulo p.

Πράγματι, έστω ότι $\delta_1, \delta_2, \ldots, \delta_r$ (1) είναι οι τάξεις των αριθμών $1, 2, \ldots, (p-1)$ modulo p. Έστω τ το ΕΚΠ αυτών των τάξεων και $\tau = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$ η κανονική του ανάλυση. Κάθε δύναμη $q_s^{\alpha_s}$ σ' αυτήν την ανάλυση διαιρεί ένα τουλάχιστον δ_j από τους αριθμούς (1), το οποίο, κατ' ανάγκη, μπορεί και παραπάνω με την μορφή $\delta_j = a q_s^{\alpha_s}$. Έστω ξ_j ένας από τους αριθμούς $1, 2, \ldots, p-1$, το οποίο έχει τάξη δ_j. Συμφώνα με το b, ο αριθμός $\eta_j = \xi_j^a$ έχει τάξη $q_s^{\alpha_s}$ και σύμφωνα με το c το γινόμενο $g = \eta_1 \ldots \eta_k$ έχει τάξη $q_1^{\alpha_1} \ldots q_k^{\alpha_k} = \tau$.

Άρα $(d, §1)$ το τ είναι διαιρέτης του $p-1$.

Αλλά μια και οι αριθμοί (1) διαιρούν τον τ, όλοι οι αριθμοί $1, 2, \ldots, p-1$ είναι λύσεις της ισοτιμίας $x^\tau \equiv 1 \pmod p$ $(c, §1)$.

Άρα, σύμφωνα με το c, §4 του κεφ. IV, θα έχομε $p-1 \leq \tau$. Συνεπώς, $\tau = p-1$, όπότε η g είναι αρχική ρίζα.

ε. Έστω g αρχική ρίζα mod p. Μπορούμε να επιλέξομε t κατάλληλα ώστε ο u, που ορίζεται απ' την ισότητα, $(g+pt)^{p-1} = 1 + pu$, να μη διαιρείται απ' τον p. Ο αντίστοιχος αριθμός $g+pt$ είναι αρχική ρίζα mod p^α για οποιοδήποτε $\alpha \geq 1$.

Πράγματι έχομε

$$\left.\begin{aligned} g^{p-1} &= 1 + pT_0 \\ (g+pt)^{p-1} &= 1 + p(T_0 - g^{p-2}t + pT_1) = 1 + pu, \end{aligned}\right\} \quad (2)$$

όπου ο u διατρέχει ένα πλήρες σύστημα υπολοίπων mod p καθώς ο t διατρέχει ένα τέτοιο σύστημα. Άρα μπορούμε να επιλέξομε τον t είς τρόπον ώστε ο u να μη διαιρείται απ' τον p. Για ένα τέτοιο t παίρνομε απ' τις (2)

$$\left.\begin{aligned} (g+pt)^{p(p-1)} &= (1+pu)^p = 1 + p^2 u_2, \\ (g+pt)^{p^2(p-1)} &= 1 + p^3 u_3 \\ &\cdots\cdots\cdots\cdots \\ (g+pt)^{p^{\alpha-1}(p-1)} &= 1 + p^\alpha u_\alpha, \end{aligned}\right\} \quad (3)$$

όπου όλοι οι $u_2, u_3, \ldots, u_\alpha$ είναι μη διαιρετοί απ' τον p. Έστω ότι η τάξη του $g+pt$ modulo p^α είναι δ. Τότε έχομε $(g+pt)^\delta \equiv 1 \pmod{p^\alpha}$ απ' όπου, κατά μείζονα λόγο, $g^\delta \equiv 1 \pmod p$. Άρα (c, §1) ο δ διαιρείται απ' τον $p-1$ και, όντας διαιρέτης του $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ (d, §1), πρέπει να είναι της μορφής $\delta = p^{r-1}(p-1)$, όπου ο r είναι ένας απ' τους αριθμούς $1, \ldots, \alpha$. Αλλά καθώς οι ισότητες (2) και (3) δείχνουν ότι η ισοτιμία

$$(g+pt)^{p^{r-1}(p-1)} \equiv 1 \pmod{p^\alpha}$$

αληθεύει μία $r = \alpha$ αλλά όχι μία $r < \alpha$, συμπεραίνομε (d, §1)

ὅτι $\delta = p^{\alpha-1}(p-1) = \phi(p^\alpha)$ καὶ ὁ ἀριθμὸς $g+p^\iota$ εἶναι ἀρχικὴ ρίζα $\bmod p^\alpha$.

β. Ἔστω $\alpha \geq 1$ καὶ g ἀρχικὴ ρίζα modulo p^α. Ἐκεῖνος ὁ g_0 ἀπὸ τοὺς ἀριθμοὺς g καὶ $g+p^\alpha$, ὁ ὁποῖος εἶναι περιττός, θὰ εἶναι ἀρχικὴ ρίζα modulo $2p^\alpha$.

Πράγματι, οἱ $\phi(p^\alpha)$ καὶ $\phi(2p^\alpha)$ εἶναι μεταξύ τους ἴσοι (ἔχομε $\phi(2p^\alpha) = \phi(2)\phi(p^\alpha) = \phi(p^\alpha)$)· ἂς συμβολίσομε μὲ c τὴν κοινή τους τιμή. Ἐπιπλέον, εἶναι εὔκολο νὰ δεῖ κανεὶς ὅτι οἱ ἰσοτιμίες $g_0^r \equiv 1 (\bmod p^\alpha)$ καὶ $g_0^r \equiv 1 (\bmod 2p^\alpha)$ εἶναι δυνατὸν νὰ ἰσχύουν μόνο συγχρόνως* (ἂ $g_0^r - 1$ διαιρεῖται ἀπὸ τὸ 2). Ἀλλά, καθὼς ὁ g_0 εἶχαι ἀρχικὴ ρίζα $\bmod p^\alpha$ καὶ ἡ πρώτη ἰσοτιμία ἀληθεύει γιὰ $r=c$ καὶ ὄχι γιὰ $r<c$, ἕπεται ὅτι ὁ g_0 εἶναι ἀρχικὴ ρίζα $\bmod 2p^\alpha$.

§3. Εὕρεση τῶν ἀρχικῶν ριζῶν modulo p^α καὶ $2p^\alpha$.

Οἱ ἀρχικὲς ρίζες modulo p^α καὶ $2p^\alpha$, ὅπου p περιττὸς πρῶτος καὶ $\alpha \geq 1$, μποροῦν νὰ εὑρεθοῦν μὲ χρήση τοῦ παρακάτω γενικοῦ θεωρήματος.

Ἔστω $c = \phi(m)$ καὶ $q_1, \ldots, q_k$ οἱ διαφορετικοὶ πρῶτοι διαιρέτες τοῦ c. Γιὰ νὰ εἶναι ὁ ἀκέραιος πρῶτος πρὸς τὸν c ἀριθμὸς g ἀρχικὴ ρίζα $\bmod m$, πρέπει καὶ ἀρκεῖ ὁ g νὰ μὴν ἱκανοποιεῖ καμιὰ ἀπὸ τὶς παρακάτω ἰσοτιμίες

$$g^{\frac{c}{q_1}} \equiv 1 (\bmod m),\ g^{\frac{c}{q_2}} \equiv 1 (\bmod m),\ \ldots,\ g^{\frac{c}{q_k}} \equiv 1 (\bmod m). \quad (1)$$

Πράγματι, ἂν ὁ g εἶναι ἀρχικὴ ρίζα τότε ἡ τάξη της εἶναι c καὶ, συνεπῶς, καμιὰ ἀπὸ τὶς ἰσοτιμίες (1) δὲν εἶναι δυνατὸν νὰ ἰσχύει. Ἀντιστρόφως, ἂς ὑποθέσομε ὅτι ὁ g δὲν ἱκανοποιεῖ καμιὰ ἰσοτιμία ἀπὸ τὶς (1). Ἂν ἡ τάξη δ τοῦ g ἦταν μικρότερη ἀπὸ c, τότε, παριστάνοντας μὲ q ἕναν ἀπὸ τοὺς πρώτους διαιρέτες τοῦ $\frac{c}{\delta}$, θὰ εἴχαμε $\frac{c}{\delta} = qu$, $\frac{c}{q} = \delta u$, $g^{\frac{c}{q}} \equiv 1 (\bmod p)$, τὸ ὁποῖο ἀντιφάσκει πρὸς τὴν ὑπόθεσή μας. Ἕπεται ὅτι $\delta = c$ καὶ ὁ g εἶναι ἀρχικὴ ρίζα.

---

* Συμφ. τ. Μετ. Δηλαδὴ ἡ πρώτη ἰσχύει ἂν καὶ μόνο ἂν ἰσχύει ἡ δεύτερη.

Παράδειγμα 1. Έστω $m=41$. Έχομε $\varphi(41)=40=2^3\cdot 5$, $40/5=8$, $40/2=20$. Κατά συνέπεια, μιά νά είναι ό μή διαιρετός άπ' τά 41 άριθμός g άρχική ρίζα $\bmod 41$, πρέπει καί άρκεί ό g νά μήν ίκανοποιεί καμιά ίσοτιμία

$$g^8\equiv 1 \pmod{41}, \quad g^{20}\equiv 1 \pmod{41}. \qquad (2)$$

Άλλά έλέγχοντας τούς άριθμούς $2,3,4,\ldots$ βρίσκομε (modulo 41)

$$2^8\equiv 10, \quad 3^8\equiv 1, \quad 4^8\equiv 18, \quad 5^8\equiv 18, \quad 6^8\equiv 10$$
$$2^{20}\equiv 1, \quad 4^{20}\equiv 1, \quad 5^{20}\equiv 1, \quad 6^{20}\equiv 40.$$

Άπ' αύτές βλέπομε ότι οί άριθμοί $2,3,4,5$ δέν είναι άρχικές ρίζες $\bmod 41$, άφού καθένας άπ' αύτούς ίκανοποιεί μία τουλάχιστον άπ' τίς ίσοτιμίες (2). Ό άριθμός 6 είναι άρχική ρίζα άφού δέν ίκανοποιεί καμιά άπ' τίς ίσοτιμίες (2).

Παράδειγμα 2. Έστω $m=1681=41^2$. Μιά άρχική ρίζα κι έδώ θά μπορούσε νά βρεθεί χρησιμοποιώντας τό γενικό θεώρημα. Όμως τή βρίσκομε άπλούστερα έφαρμόζοντας τό θεώρημα ε, §2. Γνωρίζοντας ήδη (παράδειγμα 1), ότι τό 6 είναι άρχική ρίζα $\bmod 41$, βρίσκομε

$$6^{40}=1+41(3+41l),$$

$$(6+41t)^{40}=1+41(3+41l-6^{39}t+41T)=1+41u.$$

Προκειμένου τό u νά μή διαιρείται άπ' τό 41, άρκεί νά πάρομε $t=0$. Γι' αύτό, ώς άρχική ρίζα modulo 1681 μπορούμε νά πάρομε τόν άριθμό $6+41\cdot 0=6$.

Παράδειγμα 3. Έστω $m=3362=2\cdot 1681$. Άρχική ρίζα, καί έδώ, θά μπορούσε νά βρεθεί χρησιμοποιώντας τό γενικό θεώρημα. Όμως τή βρίσκομε άπλούστερα έφαρμόζοντας τό θεώρημα ζ, §2. Γνωρίζοντας ήδη (παράδειγμα 2), ότι τό 6 είναι άρχική ρίζα $\bmod 1681$, ώς άρχική ρίζα $\bmod 3362$ μπορούμε νά πάρομε τόν περιττό άπ' τούς άριθμούς $6, 6+1681$, δηλ. τόν άριθμό 1687.

§4. Δείκτες modulo p^α και $2p^\alpha$.

a. Έστω p περιττός πρώτος, $\alpha \geqslant 1$. Σε έναν απ' τους αριθμούς p^α, $2p^\alpha$. $c = \varphi(m)$, g αρχική ρίζα $\bmod m$.

b. Αν δ διατρέχει τα ελάχιστα μη αρνητικά υπόλοιπα $\delta = 0, 1, \ldots, c-1$ modulo c, τότε ο g^δ διατρέχει ένα περιορισμένο σύστημα υπολοίπων $\bmod m$.

Πράγματι, ο g^δ διατρέχει c αριθμούς πρώτους προς τον m και, λόγω του **b**, §1, ανισοτίμους $\bmod m$.

c. Για αριθμούς a πρώτους προς τον m εισάγομε την έννοια του δείκτη, η οποία είναι ανάλογη με την έννοια του λογαρίθμου· εδώ η αρχική ρίζα παίζει ρόλο ανάλογο με το ρόλο της βάσης των λογαρίθμων.

Αν

$$a \equiv g^\gamma \pmod m$$

(υποθέτομε $\gamma \geqslant 0$), τότε γ ονομάζεται δείκτης του αριθμού a modulo m ως προς βάση g και παριστάνεται συμβολικά $\gamma = \operatorname{ind} a$ (ακριβέστερα, $\gamma = \operatorname{ind}_g a$).

Λόγω του **b**, κάθε a πρώτος προς τον m έχει κάποιο μοναδικό δείκτη γ' ανάμεσα απ' τους αριθμούς της ακολουθίας

$$\gamma = 0, 1, \ldots, c-1.$$

Γνωρίζοντας τον γ' μπορούμε να βρούμε και όλους τους δείκτες του αριθμού a· σύμφωνα με το c, §1 αυτοί θα είναι όλοι οι μη αρνητικοί αριθμοί της κλάσης

$$\gamma \equiv \gamma' \pmod c.$$

Έπεται αμέσως απ' τον ορισμό του δείκτη, που δόθηκε, ότι οι αριθμοί με τον ίδιο δείκτη γ σχηματίζουν μιαν κλάση αριθμών modulo m.

d. Έχομε

$$\operatorname{ind} ab \ldots l \equiv \operatorname{ind} a + \operatorname{ind} b + \ldots + \operatorname{ind} l \pmod c$$

και, ειδικώτερα,

$$\operatorname{ind} a^n \equiv n \operatorname{ind} a \pmod c.$$

Πράγματι,

$a \equiv g^{inda} \pmod m$, $b \equiv g^{indb} \pmod m$, ..., $l \equiv g^{indl} \pmod m$,

ἀπ' ὅπου, πολλαπλασιάζοντας κατὰ μέλη βρίσκομε

$$ab\ldots l \equiv g^{inda+indb+\ldots+indl} \pmod m.$$

Συνεπῶς, ὁ ἀριθμὸς $inda+indb+\ldots+indl$ εἶναι ἕνας ἀπὸ τοὺς δείκτ τοῦ γινομένου $ab\ldots l$.

Λόγῳ τῆς πρακτικῆς χρήσης τῶν δεικτῶν, γιὰ κάθε πρῶτο μέτρο (modulo) p (ἐννοεῖται, ὄχι πολὺ μεγάλο) ἔχουν κατασκευασθεῖ πίνακες δεικτῶν. Εἶναι δύο πίνακες· ὁ ἕνας γιὰ τὴν εὕρεση τοῦ δείκτη δοθέντος ἀριθμοῦ, ὁ ἄλλος γιὰ τὴν εὕρεση τοῦ ἀριθμοῦ ἀπὸ τὸ δείκτη. Οἱ πίνακες περιέχουν τὰ ἐλάχιστα μὴ ἀρνητικὰ ὑπόλοιπα τῶν ἀριθμῶν (περιορισμένο σύστημα) καὶ τοὺς ἐλαχίστους δείκτες τους (πλῆρες σύστημα) modula p καὶ $c = \phi(p) = p-1$, ἀντιστοίχως.

Παράδειγμα. Κατασκευάζομε τὸν ἀναφερθέντα πίνακα γιὰ τὸ μέτρο $p=41$. Παραπάνω ἀποδείχθηκε (παράδειγμα 1, §3) ὅτι ἡ $g=6$ εἶναι ἀρχικὴ ρίζα mod 41· τὴν παίρνομε ὡς βάση γιὰ τοὺς δείκτες. Βρίσκομε (οἱ ἰσότιμες θεωροῦνται mod 41):

$6^0 \equiv 1$	$6^8 \equiv 10$	$6^{16} \equiv 18$	$6^{24} \equiv 16$	$6^{32} \equiv 37$
$6^1 \equiv 6$	$6^9 \equiv 19$	$6^{17} \equiv 26$	$6^{25} \equiv 14$	$6^{33} \equiv 17$
$6^2 \equiv 36$	$6^{10} \equiv 32$	$6^{18} \equiv 33$	$6^{26} \equiv 2$	$6^{34} \equiv 20$
$6^3 \equiv 11$	$6^{11} \equiv 28$	$6^{19} \equiv 34$	$6^{27} \equiv 12$	$6^{35} \equiv 38$
$6^4 \equiv 25$	$6^{12} \equiv 4$	$6^{20} \equiv 40$	$6^{28} \equiv 31$	$6^{36} \equiv 23$
$6^5 \equiv 27$	$6^{13} \equiv 24$	$6^{21} \equiv 35$	$6^{29} \equiv 22$	$6^{37} \equiv 15$
$6^6 \equiv 39$	$6^{14} \equiv 21$	$6^{22} \equiv 5$	$6^{30} \equiv 9$	$6^{38} \equiv 8$
$6^7 \equiv 29$	$6^{15} \equiv 3$	$6^{23} \equiv 30$	$6^{31} \equiv 13$	$6^{39} \equiv 7$

ὁπότε οἱ ἀναφερθέντες πίνακες θὰ εἶναι:

$p=41$, $p-1=2^3.5$, $g=6$

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Ἐδῶ ὁ ἀριθμὸς τῆς γραμμῆς δείχνει τὸ ψηφίο τῶν δεκάδων καὶ ὁ ἀριθμὸς τῆς στήλης τὸ ψηφίο τῶν μονάδων τοῦ ἀριθμοῦ (ἀντιστ. τοῦ δείκτη). Στὴν τομὴ τῆς ἐν λόγῳ γραμμῆς καὶ στήλης τοποθετεῖται ὁ ἀντίστοιχος δείκτης (ἀντιστ. ἀριθμός).

Γιὰ παράδειγμα, βρίσκομε τὸν $\mathrm{ind}\,25$ ἀπ' τὸν πρῶτο πίνακα στὴν τομὴ τῆς γραμμῆς ὑπ. ἀριθμ. 2 καὶ τῆς στήλης ὑπ. ἀριθμ. 5, δηλ. $\mathrm{ind}\,25=4$. Ὁ ἀριθμὸς τοῦ ὁποίου ὁ δείκτης εἶναι 33 βρίσκεται ἀπ' τὸ δεύτερο πίνακα, στὴν τομὴ τῆς γραμμῆς ὑπ' ἀριθμ. 3 καὶ τῆς στήλης ὑπ' ἀριθμ. 3, δηλ. $33=\mathrm{ind}\,17$.

§5. Συνέπειες τῆς προηγούμενης θεωρίας.

α. Ἔστω p περιττός πρῶτος, $\nu \geq 1$, m ἕνας ἀπ' τοὺς ἀριθμοὺς p^ν, $2p^\nu$ καὶ, τέλος, $c = \varphi(m)$.

b. Ἔστω $(n,c) = d$. τότε:

1. Ἡ ἰσοτιμία

$$x^n \equiv a \pmod m \,, \quad (a,m)=1 \qquad (1)$$

εἶναι ἐπιλύσιμη (δηλαδὴ καὶ ὁ a εἶναι n-δύναμο ὑπόλοιπο $\bmod m$) τότε καὶ μόνο τότε, ὅταν ὁ $\mathrm{ind}\, a$ εἶναι πολλαπλάσιο τοῦ d.

Σὲ περίπτωση ἐπιλυσιμότητας ἡ ἰσοτιμία ἔχει d λύσεις.

2. Σ' ἕνα περιορισμένο σύστημα ὑπολοίπων $\bmod m$ ὁ ἀριθμὸς τῶν n-δύναμων ὑπολοίπων εἶναι c/d.

Πράγματι, ἡ ἰσοτιμία (1) ἰσοδυναμεῖ μὲ τὴν

$$n \,\mathrm{ind}\, x \equiv \mathrm{ind}\, a \pmod c, \qquad (2)$$

ἡ ὁποία εἶναι ἐπιλύσιμη τότε καὶ μόνο τότε ὅταν ὁ $\mathrm{ind}\, a$ εἶναι πολλαπλάσιο τοῦ d. (cf. §2, Κεφ. IV).

Σὲ περίπτωση ἐπιλυσιμότητας τῆς ἰσοτιμίας (2) βρίσκομε d ἀνισοτίμες $\bmod c$ τιμὲς γιὰ τὸν $\mathrm{ind}\, x$· σ' αὐτὲς ἀντιστοιχοῦν d ἀνισοτίμες $\bmod m$ τιμὲς γιὰ τὸν x.

Ἄρα, ἀληθεύει ὁ ἰσχυρισμὸς 1.

Μεταξὺ τῶν ἀριθμῶν $0, 1, \ldots, c-1$, οἱ ὁποῖοι εἶναι οἱ ἐλάχιστοι δείκτες ἑνὸς περιορισμένου συστήματος ὑπολοίπων $\bmod m$, ὑπάρχουν c/d πολλάσια τοῦ d. Γι' αὐτὸ ἀληθεύει ὁ ἰσχυρισμὸς 2.

Παράδειγμα 1. Γιὰ τὴν ἰσοτιμία

$$x^8 \equiv 23 \pmod{41} \qquad (3)$$

ἔχομε $(8,40)=8$, ὅπου $\mathrm{ind}\, 23 = 36$ δὲν διαιρεῖται ἀπ' τὸ 8. Ἄρα ἡ ἰσοτιμία (3) δὲν εἶναι ἐπιλύσιμη.

Παράδειγμα 2. Γιὰ τὴν ἰσοτιμία

$$x^{12} \equiv 37 \pmod{41} \qquad (4)$$

ἔχομε $(12,40)=4$, ὅπου $\mathrm{ind}\, 37 = 32$ διαιρεῖται ἀπ' τὸ 4. Ἄρα ἡ ἰσοτιμία (4) εἶναι ἐπιλύσιμη καὶ ἐπίσης αὐτὴ ἔχει 4 λύσεις. Τὶς ἐν λόγῳ λύσεις βρίσκομε ὡς ἑξῆς: Ἡ ἰσοτιμία (4) εἶναι ἰσοδύναμη μὲ τὶς

$12\,ind x \equiv 32 \pmod{40}$, $ind x \equiv 6 \pmod{10}$.

Ἄρα γιά τόν $ind x$ βρίσκομε 4 ἀνισοϋπόλοιπες $mod\,40$ τιμές :

$ind x = 6, 16, 26, 36$,

πού ἀντιστοιχίζομε μέ τίς ὁποῖες βρίσκομε τίς 4 λύσεις τῆς ἰσοτιμίας (4),

$x \equiv 39, 18, 2, 23 \pmod{41}$.

Παράδειγμα 3. Οἱ ἀριθμοί

$$1, 4, 10, 16, 18, 23, 25, 31, 37, 40, \tag{5}$$

οἱ δείκτες τῶν ὁποίων εἶναι πολλαπλάσια τοῦ 4, ἀποτελοῦν ὅλα τά διτετραγωνικά ὑπόλοιπα (ἤ, ὅπερ τό αὐτό, ὅλα τά n-δύναμα ὑπόλοιπα γιά ὁποιοδήποτε $n = 4, 12, 28, \ldots$ μέ $(n, 40) = 4$), πού ὑπάρχουν μεταξύ τῶν ἐλαχίστων θετικῶν ὑπολοίπων $mod\,41$. Τό πλῆθος τῶν ἀριθμῶν τῆς λίστας (5) εἶναι $10 = 40/4$.

c. Στενά συναρτημένο μέ τό **b.1** εἶναι τό ἑξῆς:

Ὁ ἀριθμός a εἶναι n-δύναμο ὑπόλοιπο $mod\,m$ τότε καί μόνο τότε ὅταν

$$a^{\frac{c}{d}} \equiv 1 \pmod{m}. \tag{6}$$

Πράγματι, ἡ συνθήκη $ind\,a \equiv 0 \pmod{d}$ ἰσοδυναμεῖ μέ τήν $\frac{c}{d}\, ind\,a \equiv 0 \pmod{c}$. Ἡ τελευταία ὅμως ἰσοδυναμεῖ μέ τήν (6).

Παράδειγμα. Ἀπ' τό θεώρημα τῆς §3 τό ἀδύνατον τῆς ἰσοτιμίας $g^{c/q} \equiv 1 \pmod{m}$ ἰσοδυναμεῖ μέ τό ὅτι ὁ g εἶναι q-δύναμο ἀνισοϋπόλοιπο $mod\,m$. Εἰδικώτερα, τό ἀδύνατον τῆς ἰσοτιμίας $g^{c/2} \equiv 1 \pmod{m}$ ἰσοδυναμεῖ μέ τή συνθήκη νά εἶναι ὁ g τετραγωνικό ἀνισοϋπόλοιπο $mod\,m$ (πρβλ. **b**, §2, Κεφ. V).

d. 1. Ἡ τάξη δ τοῦ a $mod\,m$ ὁρίζεται ἀπ' τήν ἰσότητα $(ind\,a, c) = c/\delta$ · εἰδικώτερα, τό ν' ἀνήκει ὁ a στό σύνολο τῶν ἀρχικῶν ριζῶν $mod\,m$ ἰσοδυναμεῖ μέ τήν ἰσότητα $(ind\,a, c) = 1$.

2. Σ' ἕνα περιωρισμένο σύστημα ὑπολοίπων $mod\,m$ τό πλῆθος τῶν ἀριθμῶν μέ τάξη δ εἶναι $\varphi(\delta)$ · εἰδικώτερα, τό πλῆθος τῶν ἀρχικῶν ριζῶν εἶναι $\varphi(c)$.

Πράγματι, ὁ δ εἶναι ὁ ἐλάχιστος διαιρέτης τοῦ c, πού διακρίνει τήν $a^{\delta} \equiv 1 \pmod{m}$. Αὐτή ἡ συνθήκη ἰσοδυναμεῖ μέ τήν

$$\delta\, ind\,a \equiv 0 \pmod{c},$$

ἢ $ind\, a \equiv 0 \pmod{\frac{c}{\delta}}$.

Ἔστω, ὁ δ εἶναι ὁ ἐλάχιστος διαιρέτης τοῦ c γιά τόν ὁποῖο ὁ c/δ διαιρεῖ τόν $ind\, a$, ἀπ' ὅπου ὁ c/δ εἶναι ὁ μέγιστος διαιρέτης τοῦ c, ὁ ὁποῖος διαιρεῖ τόν $ind\, a$, δηλ. $c/\delta = (ind\, a, c)$. Ἄρα ἀληθεύει ὁ ἰσχυρισμός 1.

Μεταξύ τῶν ἀριθμῶν $0, 1, \ldots, c-1$, οἱ ὁποῖοι εἶναι οἱ ἐλάχιστοι δείκτες ἑνός περιορισμένου συστήματος ὑπολοίπων $mod\, m$, τά πολλαπλάσια τοῦ c/δ εἶναι οἱ ἀριθμοί τῆς μορφῆς $\frac{c}{\delta} y$, ὅπου $y = 0, 1, \ldots, \delta-1$.

Ἡ συνθήκη $\left(\frac{c}{\delta} y, c\right) = \frac{c}{\delta}$ ἰσοδυναμεῖ μέ τή συνθήκη $(y, \delta) = 1$.

ἡ τελευταία ἱκανοποιεῖται ἀπό $\phi(\delta)$ τιμές y. Ἄρα ἀληθεύει ὁ ἰσχυρισμός 2.

Παράδειγμα 1. Σ' ἕνα περιορισμένο σύστημα ὑπολοίπων $mod\, 41$, οἱ ἀριθμοί τάξης 10 εἶναι οἱ ἀριθμοί a πού ἐπαληθεύουν τή συνθήκη $(ind\, a, 40) = \frac{40}{10} = 4$, δηλ. οἱ ἀριθμοί 4, 23, 25, 31. Τό πλῆθος αὐτῶν τῶν ἀριθμῶν εἶναι $4 = \phi(10)$.

Παράδειγμα 2. Σ' ἕνα περιορισμένο σύστημα ὑπολοίπων $mod\, 41$, οἱ ἀρχικές ρίζες εἶναι οἱ ἀριθμοί a, πού ἱκανοποιοῦν τή συνθήκη $(ind\, a, 40) = 1$, δηλ. οἱ ἀριθμοί
6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.
Τό πλῆθος αὐτῶν τῶν ἀρχικῶν ριζῶν εἶναι $16 = \phi(40)$.

(Μετάφραση τῶν §§ 1-5, κεφ. VI τοῦ βιβλίου του I.M. Βινογκράντοφ "Στοιχεῖα Θεωρίας Ἀριθμῶν" (8η Ρωσική ἔκδοση, 1981), ἀπ' τόν Ν. Τζανάκη).