Τεστ ελέγχου πρώτων με χρήση αθροισμάτων Gauss και Jacobi

Αλέξανδρος Γ. Συγκελάκης - Εμμανουήλ Γ. Τσακνάκης *

1 Αυγούστου 2006

1 Περιγραφή του Αλγορίθμου

Περίληψη

Έστω ότι έχουμε ένα μεγάλο περιττό αριθμό n που θέλουμε να ελέγξουμε αν είναι πρώτος. Μία συνήθης μέθοδος είναι να υπολογίσουμε, για παράδειγμα, το $2^{n-1} \pmod n$. Αν το αποτέλεσμα δεν είναι $1 \pmod n$, ο n είναι σύνθετος, αν το αποτέλεσμα είναι $1 \pmod n$, ο n μπορεί και να είναι πρώτος. Ένα πιο ισχυρό «ψευδοτέστ» είναι να ελέγξουμε αν ισχύει η ισοτιμία $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n$[1] για ποικιλία αριθμών a. Ωστόσο, κανένα από αυτά τα τεστ δε μας εξασφαλίζει ότι ο n είναι πρώτος.

Σε αυτό το κεφάλαιο, θα αναφερθούμε σε μία μέθοδο των Adleman-Pomerance-Rumely[1], συμπληρωμένη από τους Cohen-Lenstra[4] , η οποία χρησιμοποιεί πληροφορίες αντλούμενες από αυτά τα τεστ, για να παράγει μια πολύ μικρή λίστα πιθανών διαιρετών του n. Είναι τότε εύκολο να ελέγξουμε αν αυτοί είναι διαιρέτες του n και να αποδείξουμε αν ο n είναι πρώτος ή σύνθετος.

Το «ψευδοτέστ» που χρησιμοποιήθηκε εδώ, εμπεριέχεται στο Λήμμα 1.5 και είναι το $(a+b)^n \equiv a^n + b^n \pmod n$ εαν ο n είναι πρώτος. Μπορούμε να δούμε ότι το Θεώρημα 1.1 δίνει ένα τρόπο παραγοντοποίησης ενός σύνθετου αριθμού n δίνοντας μία λίστα πιθανών διαιρετών του παρόλο που αυτό είναι απίθανο, καθώς τέτοια n αποτυγχάνουν σε τουλάχιστον ένα από τα γνωστά «ψευδοτέστ» και έτσι δεν ικανοποιούν τις υποθέσεις του Θεωρήματος.

Διάφορες εκδόσεις του αλγορίθμου αυτού έχουν αποδείξει για μερικούς αριθμούς μήκους 200 ψηφίων ότι είναι πρώτοι, σε μερικά λεπτά.

Ο αλγόριθμος που παρουσιάζουμε, βασίζεται στο βιβλίο του L. Washington[8]

Έστω E ένα πεπερασμένο σύνολο περιττών πρώτων αριθμών. Στην πράξη κάθε πρώτος του E πρέπει να είναι μικρός. Ας θεωρήσουμε επίσης ότι $n^{p-1} \not\equiv 1 \pmod{p^2}, \forall p \in E$ και διαλέγουμε εκθέτες $a_p \geq 1$ θέτοντας

*Τμήμα Μαθηματικών, Πανεπιστήμιο Κρήτης

[1]Το $\left(\frac{a}{n}\right)$ συμβολίζει το σύμβολο Jacobi

$$t = 2 \cdot \prod_{p \in E} p^{a_p}$$

Έστω

$$s = \prod_{q-1|t} q^{\upsilon_q(t)+1},$$

όπου το q διατρέχει πρώτους αριθμούς.

Στην πράξη το t επιλέγεται έτσι ώστε $s > \sqrt{n}$. Εαν τυχαίνει $s >> \sqrt{n}$, τότε επιτρέπεται να αφαιρέσουμε μερικούς πρώτους q από το s, διατηρώντας όμως τη συνθήκη $s > \sqrt{n}$. Θεωρούμε επίσης ότι $(n, st) = 1$ καθώς διαφορετικά, η εξέταση του n για το αν είναι πρώτος ή όχι θα ήταν εύκολη.

Η παραπάνω επιλογή των s και t δίνει ότι (Λήμμα 2.1 [2])

$$n^t \equiv 1 \pmod{s} \tag{1.1}$$

□

Παράδειγμα 1.1 *Ας πάρουμε $n = 493$ και $E = \{3, 5\}$. Καταρχήν $493^2 \equiv 4 \not\equiv 1 \pmod{9}$ και $493^4 \equiv 24 \not\equiv 1 \pmod{25}$. Φτιάχνουμε τον αριθμό $t = 2 \cdot 3 \cdot 5 = 30$, του οποίου οι διαιρέτες είναι μέσα στο σύνολο $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$. Οι πρώτοι αριθμοί του συνόλου $A + 1 = \{2, 3, 4, 6, 7, 11, 16, 31\}$ που διαιρούν το t, είναι οι $\{2, 3, 7, 11, 31\}$. Έτσι λοιπόν, το s όπως το ορίσαμε παραπάνω, είναι $s = 2^2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 = 85932$ και σίγουρα $s > \sqrt{(n)}$. Ελέγχουμε ότι $(n, st) = 1$ και μένει τώρα να ελέγξουμε ότι πράγματι $493^{30} \equiv 1 \pmod{85932}$.*

Επείδη $s >> \sqrt{n}$, αν πάρουμε $E = \{3\}$ (αφαιρούμε δηλαδή το 5), τότε $t' = 2 \cdot 3 = 6$, του οποίου οι διαιρέτες είναι μέσα στο σύνολο $A' = \{1, 2, 3, 6\}$. Οι πρώτοι αριθμοί του συνόλου $A' + 1 = \{2, 3, 4, 7\}$ είναι οι $\{2, 3, 7\}$ και έτσι το καινούριο s', είναι το $s' = 2^2 \cdot 3^2 \cdot 7 = 252$ και $s' > \sqrt{n}$ και έτσι έχουμε λιγότερες πράξεις στη συνέχεια του αλγορίθμου για το αν ο αριθμός n είναι ή όχι πρώτος.

□

Ο τελικός μας στόχος, είναι να δείξουμε το θεώρημα 1.1, το οποίο αποτελεί και τον αλγόριθμο με τον οποίο θα εξετάσουμε εαν ένας αριθμός είναι ή όχι πρώτος. Πρώτα όμως χρειαζόμαστε μερικά βασικά αποτελέσματα τα οποία και θα αποδείξουμε αναλυτικά.

Καταρχήν το ότι $n^{p-1} \not\equiv 1 \pmod{p^2}$ $\big($ενώ $n^{p-1} \equiv 1 \pmod{p}$ (Θ. Fermat) $\big)$, δίνει ότι το n^{p-1} είναι γεννήτορας της ομάδας $(1 + p\mathbb{Z}_p)/(1 + p^{1+a_p}\mathbb{Z}_p)$, καθώς κάθε αριθμός ισότιμος με $1 \pmod{p}$ αλλά όχι $\mod p^2$, είναι γεννήτορας της παραπάνω ομάδας (Λήμμα 2.2).

Συνεπώς για κάθε ακέραιο r με $(r, p) = 1$, μπορούμε να γράψουμε

$$r^{p-1} \equiv (n^{p-1})^{l_p(r)} \pmod{p^{1+a_p}}$$

[2] Η απόδειξη αυτής της σχέσης, καθώς και υπολοίπων σχέσεων που η απόδειξή τους δεν σχετίζεται με την απόδειξη της ορθότητας του αλγορίθμου που θα παραθέσουμε στο τέλος, παρατίθεται αναλυτικά στο παράρτημα, στο τέλος της παρούσης εργασίας.

για κάποιο ακέραιο $l_p(r)$ ο οποίος ορίζεται μοναδικά $\mod p^{a_p}$.

Παρατήρηση: Ο πρώτος αριθμός 2, προκαλεί κάποιες τεχνικές δυσκολίες, γι' αυτό το λόγο επιλέγουμε $4 \not| t$. Τα επόμενα όμως δύο Λήμματα, θα μας επιτρέψουν, να ορίσουμε κατάλληλο $l_2(r)$ για $r|n$.

Λήμμα 1.1 *Αν υποθέσουμε ότι υπάρχει ακέραιος c, με*

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

Τότε

$$\upsilon_2(r-1) \geq \upsilon_2(n-1), \forall r \text{ με } r|n,$$

όπου $\upsilon_2(k)$, είναι το πλήθος των 2 στην πρωτογενή ανάλυση του k. (Ονομάζεται και $2-part$ του k).

Απόδειξη:

Ας είναι x_r η τάξη του $c \pmod{r}$ δηλαδή ο ελάχιστος φυσικός τέτοιος ώστε $c^{x_r} \equiv 1 \pmod{r}$, και ας είναι

$$n-1 = 2^{\lambda} \cdot \mu, \mu \text{ περιττός}, \lambda \geq 1$$

Αφού $c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ άρα $c^{\frac{n-1}{2}} \equiv -1 \pmod{r}$, συνεπώς $c^{\frac{n-1}{2}} \not\equiv 1 \pmod{r}$ δηλαδή $c^{2^{\lambda-1}\cdot\mu} \not\equiv 1 \pmod{r}$.

Καθώς όμως $c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, άρα υψώνοντας στο τετράγωνο έχουμε $c^{n-1} \equiv 1 \pmod{n}$ και είναι η πρώτη φορά που συμβαίνει αυτό με τα 2-άρια που έχει το $n-1$ στην ανάλυσή του. Άρα σίγουρα το $2-part$ του $n-1$ πρέπει να είναι ίσο με το $2-part$ του x_r και συμβολικά

$$\upsilon_2(n-1) = \upsilon_2(x_r) \tag{1.2}$$

Όταν το r είναι πρώτος, έχουμε $c^{r-1} \equiv 1 \pmod{r}$, απ' όπου $x_r|r-1$, δηλαδή

$$\upsilon_2(x_r) \leq \upsilon_2(r-1) \tag{1.3}$$

Συνδιάζοντας τις (1.2), (1.3) παίρνουμε το ζητούμενο για όλους τους πρώτους διαιρέτες του n, άρα και για όλους τους διαιρέτες του.

□

Παρατήρηση: Στην πράξη, δεν είναι δύσκολο να βρούμε ένα τέτοιο c, διότι εαν ο n είναι πρώτος, οι μισοί από τους ακεραίους c από το 1 εως το $n-1$ ικανοποιούν την υπόθεση του Λήμματος 1.1. Θα θεωρήσουμε λοιπόν ότι ένα τέτοιο c υπάρχει.

Λήμμα 1.2 *Για κάθε αριθμό r με $r|n$, μπορούμε να γράψουμε*

$$r \equiv n^{l_2(r)} \pmod{2^{k+1}},$$

όπου $k = \upsilon_2(n-1)$ και το $l_2(r)$ είναι υπολογισμένο $\mod 2$.

Απόδειξη:

Από το Λήμμα 1.1 αφού $\upsilon_2(r-1) \geq \upsilon_2(n-1)$, άρα υπάρχουν περιττοί αριθμοί λ, μ τέτοιοι ώστε $r-1 = 2^m\lambda, n-1 = 2^k\mu$ και $m \geq k$. Αφού $r|n$, υπάρχει ακέραιος k_1 τέτοιος ώστε $n = k_1 r$. Άρα $n-1 = k_1 r - r + r - 1 = r(k_1-1) + r - 1$ απ' όπου

$$2^k\mu = r(k_1 - 1) + 2^m\lambda \tag{1.4}$$

Διακρίνουμε τις περιπτώσεις

- Αν $m = k$, τότε διαιρώντας την 1.4 με 2^k παίρνουμε $\mu = \dfrac{r(k_1-1)}{2^k} + \lambda$. Άρα $\dfrac{r(k_1-1)}{2^k} \in \mathbb{Z}$ και αφού μ, λ περιττοί, είναι άρτιος. Άρα $r(k_1 - 1) \equiv 0 \pmod{2^{k+1}}$ απ' όπου $\underbrace{rk_1}_{n} - r \equiv 0 \pmod{2^{k+1}}$ και τελικά $r \equiv n \pmod{2^{k+1}}$.
- Εαν $m > k$, τότε $m - k \geq 1$ και διαιρώντας και πάλι με 2^k την 1.4 παίρνουμε $\mu = \dfrac{r(k_1-1)}{2^k} + 2^{m-k}\lambda$. Όμως μ περιττός και $2^{m-k}\lambda$ άρτιος συνεπώς $\dfrac{r(k_1-1)}{2^k} \in \mathbb{Z}$ και μάλιστα είναι περιττός. Άρα $\dfrac{r(k_1-1)}{2^k} = 1 + 2\xi$ για κάποιο $\xi \in \mathbb{Z}$. Συνεπώς $r(k_1-1) = 2^k + 2^{k+1}\xi$ απ' όπου $\underbrace{rk_1}_{n=2^k\mu-1} - r = 2^k + 2^{k+1}\xi$ δηλαδή $r \equiv 2^k\mu + 1 + 2^k \pmod{2^{k+1}}$ και τελικά $r \equiv 2^k(\mu+1) + 1 \equiv 1 \pmod{2^{k+1}}$ διότι ο $\mu + 1$ είναι άρτιος.

Σε κάθε περίπτωση λοιπόν $r \equiv n^{l_2(r)} \pmod{2^{k+1}}$, όπου $k = \upsilon_2(n-1)$ και το $l_2(r)$ είναι υπολογισμένο $\mod 2$.

□

Συνοψίζοντας έχουμε:

Για κάθε ακέραιο $r|n$, διαλέγουμε έναν ακέραιο $l(r)$ τέτοιο ώστε $l(r) \equiv l_p(r) \pmod{p^{a_p}}, \forall p \in E$, και $l(r) \equiv l_2(r) \pmod 2$, στην περίπτωση που ο πρώτος είναι το 2.

Τότε, $r^{p-1} \equiv n^{(p-1)l(r)} \pmod{p^{1+a_p}}, \forall p \in E$ και όμοια $r \equiv n^{l(r)} \pmod{2^{\overbrace{\upsilon_2(n-1)}^{k}+1}}$ στην περίπτωση που ο πρώτος είναι το 2.

Σκοπός της εργασίας είναι να δείξουμε ότι οι πιθανοί διαιρέτες r του n, είναι της μορφής $r \equiv n^l \pmod s$ με $1 \leq l < t$ (λόγω της σχέσης 1.1). Σε αυτό θα μας βοηθήσουν οι χαρακτήρες Dirichlet, καθώς επίσης και τα αθροίσματα Jacobi για να δείξουμε τις Προτάσεις 1 και 2, που θα μας βοηθήσουν στην επίτευξη του τελικού μας στόχου που είναι η απόδειξη του Θεωρήματος 1.1.

Ας είναι q ένας πρώτος διαιρέτης του s. Για κάθε πρώτο $p|q-1$, παίρνουμε ένα χαρακτήρα Dirichlet $\chi_{q,p}$ με οδηγό q και τάξη p^k, όπου $k = \upsilon_p(q-1)$. Επειδή $q-1|t$ άρα $\upsilon_p(q-1) \leq \upsilon_p(t) = a_p$ συνεπώς $k \leq a_p$.

Παρατήρηση: Το σύνολο αυτών των χαρακτήρων $\chi_{q,p}$, καθώς το p διατρέχει τους πρώτους διαιρέτες του $q-1$, παράγει την ομάδα των χαρακτήρων Dirichlet $\bmod q$ (Λήμμα 2.4).

Θα πάρουμε αρχικά την περίπτωση περιττού p. Διαλέγουμε ακεραίους a και b τέτοιους ώστε $ab(a+b) \not\equiv 0 \pmod p$ και $(a+b)^p \not\equiv a^p + b^p \pmod{p^2}$ (αυτό είναι πάντοτε εφικτό).

Έστω

$$\mathcal{J} = \mathcal{J}(\chi_{q,p}^a, \chi_{q,p}^b) = -\sum_{y=0}^{q-1} \chi_{q,p}^a(y), \chi_{q,p}^b(1-y),$$

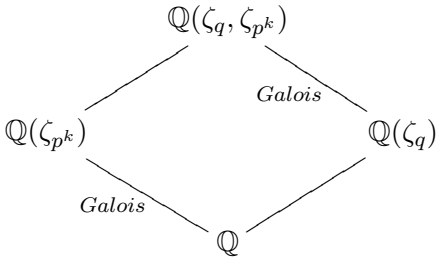
άθροισμα Jacobi και έστω η ομάδα Galois $G = Gal(\mathbb{Q}(\zeta_{p^k})/\mathbb{Q})$, όπου ζ_{p^k} μία p^k-ρίζα της μονάδος.

Θεωρούμε

$$\alpha := \sum_{\substack{x=1 \\ p \not| x}}^{p^k-1} \left[\frac{nx}{p^k}\right] \sigma_x^{-1} \ \in \mathbb{Z}[G],$$

όπου $\mathbb{Z}[G]$ είναι ο δακτύλιος της ομάδας G, $[y]$ το ακέραιο μέρος του πραγματικού αριθμού y και $\sigma_x : \zeta_{p^k} \mapsto \zeta_{p^k}^x$, ο αυτομορφισμός ο οποίος δρα στις p^k-ρίζες της μονάδος, στέλνοντάς τις ζ_{p^k} στις $\zeta_{p^k}^x$.

Παρατήρηση: Μπορούμε να επεκτείνουμε τον ορισμό της σ_x στην ομάδα $Gal(\mathbb{Q}(\zeta_{p^k}, \zeta_q)/\mathbb{Q}(\zeta_q))$ η οποία δρα ταυτοτικά στις q-ρίζες της μονάδος, και όπως παραπάνω στις p^k ρίζες της μονάδος (Θεώρημα της μεταφοράς, Λήμμα 2.4). Σχηματικά



Λήμμα 1.3 *Έστω $ab(a+b) \not\equiv 0 \pmod p$ και ας πάρουμε*

$$\beta := \sum_{\substack{x=1 \\ p \not| x}}^{p^k-1} \left(\left[\frac{(a+b)x}{p^k}\right] - \left[\frac{ax}{p^k}\right] - \left[\frac{bx}{p^k}\right] \right) \sigma_x^{-1}$$

Τότε,

$$(n - \sigma_n)\beta = (\sigma_a + \sigma_b - \sigma_{a+b})\alpha$$

Απόδειξη:

Ας θεωρήσουμε

$$\theta := \frac{1}{p^k} \sum_{\substack{x=1 \\ p \nmid x}}^{p^k-1} x\sigma_x^{-1} \overset{\star}{=} \sum_{\substack{x=1 \\ p \nmid x}}^{p^k-1} \left\{ \frac{x}{p^k} \right\} \sigma_x^{-1},$$

το στοιχείο Stickelberger, όπου $\{y\}$ παριστάνει το δεκαδικό μέρος του y. Η ισότητα $\star$ ισχύει διότι $\frac{x}{p^k} = \left[\frac{x}{p^k} \right] + \left\{ \frac{x}{p^k} \right\}$ και $\left[\frac{x}{p^k} \right] = 0, \ \forall \ x = 1, \ldots, p^k$ με $p \nmid x$.

Για κάθε αριθμό m με $(m, p) = 1$ έχουμε

$$(m - \sigma_m)\theta \overset{\text{Λήμμα2.5}(c)}{=} \sum_{\substack{x=1 \\ p \nmid x}}^{p^k-1} \left(m\left\{ \frac{x}{p^k} \right\} - \left\{ \frac{mx}{p^k} \right\} \right) \sigma_x^{-1} = \sum_{\substack{x=1 \\ p \nmid x}}^{p^k-1} \left[\frac{mx}{p^k} \right] \sigma_x^{-1} \ {}^{3} \quad (1.5)$$

Συνεπώς, καθώς $(n, p) = 1$ (διότι $(n, t) = 1$) έχουμε $(n - \sigma_n)\theta = \alpha$ και $(\sigma_a + \sigma_b - \sigma_{a+b})\theta = ((a + b - \sigma_{a+b}) - (a - \sigma_a) - (b - \sigma_b))\theta = \beta$ (Λόγω της υπόθεσης στην αρχή και της σχέσης 1.5).

Πολλαπλασιάζοντας με $(n - \sigma_n)$ παίρνουμε

$$(n - \sigma_n)\beta = (\sigma_a + \sigma_b - \sigma_{a+b}) \underbrace{(n - \sigma_n)\theta}_{\alpha} = (\sigma_a + \sigma_b - \sigma_{a+b})\alpha$$

και αποδείχθηκε αυτό που θέλαμε.

□

Λήμμα 1.4 *Εαν* $(a + b)^p \not\equiv a^p + b^p \pmod{p^2}$ *και* $ab(a + b) \not\equiv 0 \pmod{p}$, *τότε*

$$\sum_{\substack{x=1 \\ p \nmid x}}^{p^k-1} \left(\left[\frac{(a+b)x}{p^k} \right] - \left[\frac{ax}{p^k} \right] - \left[\frac{bx}{p^k} \right] \right) x^{-1} \not\equiv 0 \pmod{p}$$

Απόδειξη:

Εαν $x \equiv y \pmod{p^k}$ τότε $x^p \equiv y^p \pmod{p^{k+1}}$ (Λήμμα 2.6).

Συνεπώς υπάρχει ένας καλώς ορισμένος ομομορφισμός δακτυλίων (Λήμμα 2.7)

$$\begin{array}{rcl} \varphi : \mathbb{Z}[G] & \to & \mathbb{Z}/p^{k+1}\mathbb{Z} \\ \displaystyle\sum_{\substack{x=1 \\ p \nmid x}}^{p^k-1} c_x\sigma_x & \mapsto & \displaystyle\sum_{\substack{x=1 \\ p \nmid x}}^{p^k-1} c_x x^p \pmod{p^{k+1}} \end{array}$$

[3] Είναι πολύ εύκολο να δείξουμε ότι $\sigma_x^{-1} = \sigma_{x^{-1}}$ και από εδώ και στο εξής θα το χρησιμοποιούμε όπως είναι βολικότερο.

Όμως $(\sigma_a+\sigma_b-\sigma_{a+b})(p^k\theta)=p^k\beta$ και εφαρμόζοντας τον ομομορφισμό φ και στα δύο μέλη παίρνουμε

$$\varphi\big((\sigma_a+\sigma_b-\sigma_{a+b})(p^k\theta)\big)\equiv\varphi\big(p^k\beta\big)\pmod{p^{k+1}} \tag{1.6}$$

Όμως

$$\begin{aligned}\varphi\big((\sigma_a+\sigma_b-\sigma_{a+b})(p^k\theta)\big) &= \varphi(\sigma_a+\sigma_b-\sigma_{a+b})\varphi(p^k\theta)=\big(a^p+b^p-(a+b)^p\big)\not{p^k}\frac{1}{\not{p^k}}\sum_{\substack{x=1\\ p\not| x}}^{p^k-1}x\varphi(\sigma_{x^{-1}})\\ &= \big(a^p+b^p-(a+b)^p\big)\sum_{\substack{x=1\\ p\not| x}}^{p^k-1}x^{1-p}\end{aligned}$$

και

$$\begin{aligned}\varphi(p^k\beta) &= p^k\sum_{\substack{x=1\\ p\not| x}}^{p^k-1}\left(\left[\frac{(a+b)x}{p^k}\right]-\left[\frac{ax}{p^k}\right]-\left[\frac{bx}{p^k}\right]\right)\varphi(\sigma_x^{-1})\\ &= \underbrace{p^k\sum_{\substack{x=1\\ p\not| x}}^{p^k-1}\left(\left[\frac{(a+b)x}{p^k}\right]-\left[\frac{ax}{p^k}\right]-\left[\frac{bx}{p^k}\right]\right)x^{-p}}_{B}\\ &\overset{\star}{\equiv} p^k\sum_{\substack{x=1\\ p\not| x}}^{p^k-1}\left(\left[\frac{(a+b)x}{p^k}\right]-\left[\frac{ax}{p^k}\right]-\left[\frac{bx}{p^k}\right]\right)x^{-1}\pmod{p^{k+1}}\end{aligned}$$

και η ισότητα $(\star)$ ισχύει διότι $x^p\equiv x\pmod p$ απ' όπου $x^{-p}\equiv x^{-1}\pmod p$ και πολλαπλασιάζοντας και τα δύο μέλη της τελευταίας με B έχουμε την ζητούμενη ισοτιμία (Ας σημειωθεί ότι το x έχει επιλεγεί έτσι ώστε $p\not| x$ για να υπάρχει ο $x^{-1}\mod p$).

Άρα τελικά

$$\big(a^p+b^p-(a+b)^p\big)\sum_{\substack{x=1\\ p\not| x}}^{p^k-1}x^{1-p}\equiv p^k\sum_{\substack{x=1\\ p\not| x}}^{p^k-1}\left(\left[\frac{(a+b)x}{p^k}\right]-\left[\frac{ax}{p^k}\right]-\left[\frac{bx}{p^k}\right]\right)x^{-1}\pmod{p^{k+1}} \tag{1.7}$$

Όμως το x^{p-1}, άρα και το x^{1-p} διατρέχει όλα τα $y\mod p^k$ καθώς $y\equiv 1\pmod p$ και κάθε τιμή του y την παίρνει $p-1$ φορές (Λήμμα 2.8)

Επίσης όλα τα $y\mod p^k$ δηλαδή τα $0,1,2,\ldots,p^k-1$ τα οποία είναι $\equiv 1\pmod p$ είναι σε πλήθος p^{k-1} [είναι σε πλήθος όσα και εκείνα που είναι $\equiv 0\pmod p$ (εκείνα που δεν είναι πρώτα προς τον πρώτο p, είναι σε πλήθος $p^k-\varphi(p^k)=p^{k-1}$)].

Συνεπώς

$$\sum_{\substack{x=1\\ p\not| x}}^{p^k-1} x^{1-p} \equiv (p-1) \sum_{j=0}^{p^{k-1}-1} (1+jp) \equiv -p^{k-1} \pmod{p^k}$$

άρα αφού εξ' υποθέσεως $p^2 \not| \ a^p + b^p - (a+b)^p$ και $p^{k-1} | \sum_{\substack{x=1\\ p\not| x}}^{p^k-1} x^{1-p}$ άρα $p^{k+1} \not| \left(a^p + b^p - (a+b)^p\right) \sum_{\substack{x=1\\ p\not| x}}^{p^k-1} x^{1-p}$, και τελικά το αριστερό μέλος της 1.7 δεν διαιρείται από το p^{k+1} συνεπώς το ίδιο συμβαίνει και για το δεξί το οποίο όμως είναι διαιρετό από το p^k. Αναγκαστικά λοιπόν

$$p \not| \sum_{\substack{x=1\\ p\not| x}}^{p^k-1} \left(\left[\frac{(a+b)x}{p^k} \right] - \left[\frac{ax}{p^k} \right] - \left[\frac{bx}{p^k} \right] \right) x^{-1}$$

□

Ας θεωρήσουμε τώρα το άθροισμα Gauss που ορίζεται να είναι το

$$g(\chi_{q,p}) := -\sum_{y=1}^{q-1} \chi_{q,p}(y) \zeta_q^y \in \mathbb{Z}[\zeta_{p^k}, \zeta_q]$$

Επεκτείνουμε όπως πριν, τον ορισμό της σ_x, έτσι ώστε $\sigma_x(\zeta_q) = \zeta_q$, δηλαδή η σ αφήνει αναλλοίωτες τις q–ρίζες της μονάδος.

Τότε λόγω της ιδιότητας $\mathcal{J}(\chi_1, \chi_2) = \dfrac{g(\chi_1) g(\chi_2)}{g(\chi_1 \chi_2)}$ $(\chi_1 \chi_2 \neq 1)$ έχουμε

$$\begin{aligned}
\mathcal{J}^\alpha &= \frac{g(\chi_{q,p}^a)^\alpha g(\chi_{q,p}^b)^\alpha}{g(\chi_{q,p}^{a+b})^\alpha} \quad (\text{Ισχύει } \ g(\chi_{q,p}^r) = g(\chi_{q,p})^{\sigma_r}) \\
&= \frac{g(\chi_{q,p})^{\sigma_a \alpha} g(\chi_{q,p})^{\sigma_b \alpha}}{g(\chi_{q,p})^{\sigma_{a+b}\alpha}} = g(\chi_{q,p})^{(\sigma_a + \sigma_b - \sigma_{a+b})\alpha} \\
&\overset{\text{Λήμμα } 1.3}{=} g(\chi_{q,p})^{(n-\sigma_n)\beta}
\end{aligned}$$

Λήμμα 1.5 *Έστω r τυχαίος πρώτος με $(r, pq) = 1$. Τότε*

$$g(\chi_{q,p})^{r-\sigma_r} \equiv \chi_{q,p}(r)^{-r} \quad \left(\mathrm{mod}\ r\mathbb{Z}\left[\frac{1}{q}, \zeta_q, \zeta_{p^k}\right] \right)$$

Απόδειξη:

Έχουμε $g(\chi_{q,p})^r = (-1)^r \left(\sum_{y=1}^{q-1} \chi_{q,p}(y) \zeta_q^y \right)^r \equiv -\sum_{y=1}^{q-1} \chi_{q,p}^r(y) \zeta_q^{yr} \pmod{r}$

Θέτω y' το yr. Τότε καθώς το ζ_q^{yr} είναι μία άλλη (εν γένει) q-ρίζα της μονάδος έστω ζ_q', άρα και πάλι το y' θα παίρνει τις τιμές από 1 εως $q-1$. Οπότε η παραπάνω σχέση γράφεται

$$-\sum_{y'=1}^{q-1}\chi_{q,p}^r\Big(\frac{y'}{r}\Big)\zeta_q^{y'} = -\chi_{q,p}(r)^{-r}\sum_{y=1}^{q-1}\chi_{q,p}^r(y)\zeta_q^y \equiv \chi_{q,p}(r)^{-r}g(\chi_{q,p})^{\sigma_r} \pmod r$$

□

Τώρα έχουμε τα απαραίτητα εφόδια για να αποδείξουμε την πρώτη ισχυρή πρόταση

Πρόταση 1 *Έστω p περιττός πρώτος και έστω $\mathcal{J}$ το άθροισμα Jacobi όπως ορίστηκε παραπάνω (μαζί με τα a, b που επιλέξαμε). Εαν το $\mathcal{J}^\alpha$ δεν είναι ισότιμο με μία p^k-ρίζα της μονάδος $\bmod n\mathbb{Z}[\zeta_{p^k}]$, τότε ο n είναι σύνθετος. Εαν $\mathcal{J}^\alpha \equiv \zeta \pmod n$ με $\zeta^{p^k}=1$, τότε*

$$\chi_{q,p}(r) = \chi_{q,p}(n)^{l(r)},\ \ \forall\ r \text{ με } r|n.$$

Απόδειξη:

Από το Λήμμα 1.5, εαν ο n είναι πρώτος, τότε $\mathcal{J}^\alpha = g(\chi_{q,p})^{(n-\sigma_n)\beta} \overset{\text{Λήμμα 1.5}}{\equiv} \chi_{q,p}(r)^{-n\beta} \pmod n$.

Συνεπώς το $\mathcal{J}^\alpha$ είναι ισότιμο $\bmod n$ με μία p^k ρίζα της μονάδος. Αυτό αποδεικνύει το πρώτο μέρος της πρότασης.

Ας θεωρήσουμε τώρα ότι ο n δεν είναι (ακόμη) γνωστό εαν είναι πρώτος ή όχι, αλλά ότι $\mathcal{J}^\alpha \equiv \zeta \pmod n$ με $\zeta^{p^k}=1$.

Ας πάρουμε $u = g(\chi_{q,p})^\beta$. Τότε η $\mathcal{J}^\alpha = g(\chi_{q,p})^{(n-\sigma_n)\beta}$ γίνεται $u^{n-\sigma_n} = \mathcal{J}^\alpha \equiv \zeta \pmod n$, και δουλεύουμε στον δακτύλιο $r\mathbb{Z}\Big[\frac{1}{q}, \zeta_q, \zeta_{p^k}\Big]$.

Για $i \geq 1$ έχουμε

$$u^{n^i-\sigma_n^i} = u^{(n-\sigma_n)(n^{i-1}+\cdots+\sigma_n^{i-1})} \equiv \zeta^{n^{i-1}+\cdots+\sigma_n^{i-1}} = \zeta^{in^{i-1}} \pmod n \qquad (1.8)$$

διότι $\zeta^{n^{i-k}\cdot\sigma_n^{k-1}} = \sigma_n^{k-1}\Big(\zeta^{n^{i-k}}\Big) = \zeta^{n^{i-k}\cdot n^{k-1}} = \zeta^{n^{i-1}}\ \ \forall\ k=1,\ldots,i$

Θέτουμε στην 1.8 όπου $i=(p-1)p^k$ και έτσι έχουμε

$$u^{n^{(p-1)p^k}-\sigma_n^{(p-1)p^k}} \equiv \zeta^{(p-1)p^k n^{(p-1)p^k-1}} \equiv 1 \pmod n \qquad (1.9)$$

Όμως $u^{\sigma_n^{(p-1)p^k}} = \Big(g\big(\chi_{q,p}(r)\big)^\beta\Big)^{\sigma_n^{(p-1)p^k}} = g\Big(\chi_{q,p}^{n^{(p-1)p^k}}(r)\Big)^\beta$

και

$\chi_{q,p}^{n^{(p-1)p^k}}(r) = \chi_{q,p}(r)$ διότι $n^{\varphi(p^{k+1})} \equiv 1 \pmod{p^{k+1}} \equiv 1 \pmod{p^k}$ απ' όπου $n^{(p-1)p^k} \equiv 1 \pmod{p^k}$ άρα $n^{(p-1)p^k} = 1 + p^k\lambda$, για κάποιο $\lambda \in \mathbb{Z}$ και τελικά $\chi_{q,p}^{n^{(p-1)p^k}}(r) = \chi_{q,p}^{1+p^k\lambda}(r) = \chi_{q,p}(r)\Big(\chi_{q,p}^{p^k}(r)\Big)^\lambda = \chi_{q,p}(r)$, διότι ο $\chi_{q,p}$ έχει τάξη p^k.

Άρα αντικαθιστώντας τις παραπάνω στην (1.9), έχουμε

$$u^{n^{(p-1)p^k}-1} \equiv 1 \pmod{n} \tag{1.10}$$

Ας είναι τώρα r ένας πρώτος διαιρέτης του n. Το Λήμμα 1.5 δίνει ότι
$u^{r^i-\sigma_r^i} = u^{(r-\sigma_r)(r^{i-1}+\cdots+\sigma_r^{i-1})} \equiv \chi_{q,p}(r)^{-r(r^{i-1}+\cdots+\sigma_r^{i-1})\beta} \equiv \chi_{q,p}^{-ir^i\beta}(r) \pmod{r}$
Θέτωντας $i = p-1$ παίρνουμε

$$u^{r^{p-1}-\sigma_r^{p-1}} \equiv \chi_{q,p}(r)^{-(p-1)r^{p-1}\beta} \pmod{r} \tag{1.11}$$

Απ' το Λήμμα 1.4, το β δρα στις p^k-ρίζες της μονάδος μέσω ενός ακεραίου που δεν διαιρείται από το p διότι εξ' ορισμού (Παράγραφος 2.1 του Παραρτήματος) ο εκθέτης του ζ_{p^k} όταν το β δράσει πάνω του, θα είναι ακριβώς εκείνη η παράσταση του Λήμματος 1.4, που δεν είναι διαιρετή από το p.

Συνεπώς (Λήμμα 2.9) υπάρχει p^k-ρίζα της μονάδος η τέτοια ώστε

$$\zeta = \eta^{-n\beta}$$

Ας πάρουμε $l = l(r)$ άρα $r^{p-1} \equiv n^{(p-1)l} \pmod{p^{k+1}}$ και $\sigma_r^{p-1} = \sigma_n^{(p-1)l}$ διότι στις μεν q-ρίζες της μονάδος ισχύει $\sigma_r^{p-1}(\zeta_q) = \zeta_q = \sigma_n^{(p-1)l}(\zeta_q)$ και στις δε p^k-ρίζες της μονάδος $\sigma_r^{p-1}(\zeta_{p^k}) = \zeta_{p^k}^{r^{p-1}} \overset{\star}{=} \zeta_{p^k}^{n^{(p-1)l}} = \sigma_n^{(p-1)l}(\zeta_{p^k})$ και η ισότητα $(\star)$ ισχύει διότι εφόσον $r^{p-1} \equiv n^{(p-1)l} \pmod{p^{k+1}}$ άρα $r^{p-1} \equiv n^{(p-1)l} \pmod{p^k}$ συνεπώς $\zeta_{p^k}^{r^{p-1}} = \zeta_{p^k}^{n^{(p-1)l}+p^k\lambda} = \zeta_{p^k}^{n^{(p-1)l}}$ για κάποιο $\lambda \in \mathbb{Z}$.

Άρα

$$u^{n^{(p-1)l}-r^{p-1}} = u^{n^{(p-1)l}-\sigma_n^{(p-1)l}+\sigma_r^{p-1}-r^{p-1}} = u^{n^{(p-1)l}-\sigma_n^{(p-1)l}} \cdot u^{\sigma_r^{p-1}-r^{p-1}} \tag{1.12}$$

Όμως η 1.8 για $i = (p-1)l$ δίνει
$u^{n^{(p-1)l}-\sigma_n^{(p-1)l}} \equiv \zeta^{(p-1)ln^{(p-1)l-1}} = \eta^{-\beta(p-1)ln^{(p-1)l}} \pmod{n}$ άρα και $\mod r$
Επίσης από 1.11 $u^{\sigma_r^{p-1}-r^{p-1}} \equiv \chi_{q,p}(r)^{(p-1)r^{p-1}\beta} \pmod{r}$, συνεπώς η 1.12 γίνεται

$$u^{n^{(p-1)l}-r^{p-1}} \equiv \eta^{-\beta(p-1)ln^{(p-1)l}} \cdot \chi_{q,p}(r)^{(p-1)r^{p-1}\beta} \equiv \left(\frac{\chi_{q,p}(r)}{\eta^l}\right)^{(p-1)r^{p-1}\beta} \pmod{r}$$

Καθώς $n^{p-1} \not\equiv 1 \pmod{p^2}$ προκύπτει ότι $z := \dfrac{n^{(p-1)p^k}-1}{p^{k+1}} \not\equiv 0 \pmod{p}$ διότι
$n^{(p-1)p^k}-1 = (n^{p-1}-1)\underbrace{(n^{(p-1)(p^k-1)} + n^{(p-1)(p^k-2)} + \cdots + n^{2(p-1)} + n^{p-1} + 1)}_{\substack{p^k \text{ όροι, και κάθε ένας είναι } \equiv 1 \pmod{p} \text{ λόγω της } n^{p-1}\equiv 1 \pmod{p}}} \equiv$
$0 \pmod{p^{k+1}}$ άρα τελικά $p^{k+1} || n^{(p-1)p^k} - 1$.

Καθώς $n^{(p-1)l} - r^{p-1} \equiv 0 \pmod{p^{k+1}}$ έχουμε

$$z \cdot \left(n^{(p-1)l} - r^{p-1}\right) = \frac{n^{(p-1)p^k}-1}{p^{k+1}} \cdot \left(n^{(p-1)l} - r^{p-1}\right) \equiv 0 \pmod{n^{(p-1)p^k}-1}$$

Άρα $n^{(p-1)p^k}-1 | z(n^{(p-1)l}-r^{p-1})$. Δηλαδή υπάρχει w τ.ω.

$$z(n^{(p-1)l}-r^{p-1}) = w\cdot(n^{(p-1)p^k}-1)$$

Τότε $\left(\frac{\chi_{q,p}(r)}{\eta^l}\right)^{z(p-1)r^{p-1}\beta} \equiv u^{z\left(n^{(p-1)l}-r^{p-1}\right)} = u^{w(n^{(p-1)p^k}-1)} \overset{(1.10)}{\equiv} 1^w \equiv 1 \pmod r$.

Δηλαδή

$$\left(\frac{\chi_{q,p}(r)}{\eta^l}\right)^{z(p-1)r^{p-1}\beta} \equiv 1 \pmod r$$

.

Αλλά $p \not| z(p-1)r^{p-1}$ (διότι κανένας από τους 3 όρους δεν είναι διαιρετός από p) και ο β από το Λήμμα 1.4, δρα στο $\frac{\chi_{q,p}(r)}{\eta^l}$ (που είναι σίγουρα p^k ρίζα της μονάδος ˙ ίσως και p^d ρίζα της μονάδος με $d<k$) μέσω ενός ακεραίου που δεν διαιρείται από το p.

Αφού λοιπόν $\frac{\chi_{q,p}(r)}{\eta^l}$ είναι p–οστής δύναμης ρίζα του 1 και ο εκθέτης μετά την δράση του β, δεν διαιρείται από το p, έπεται ότι $\frac{\chi_{q,p}(r)}{\eta^l} \equiv 1 \pmod r$.

Από Λήμμα 2.10 οι ρίζες της μονάδας είναι διακριτές $\bmod r$. Άρα

$$\frac{\chi_{q,p}(r)}{\eta^l} = 1 \text{ απ' όπου } \chi_{q,p}(r) = \eta^l$$

Δηλαδή $\chi_{q,p}(r) = \eta^{l(r)}$ για κάθε πρώτο διαιρέτη r του n (το η είναι ανεξάρτητο του r).Εφόσον $l(r_1\cdot r_2) \equiv l(r_1)+l(r_2) \pmod{p^k}$ έχουμε ότι $\chi_{q,p}(r) = \eta^{l(r)}$ για όλους τους διαιρέτες r του n.

Για $r=n$ και παίρνοντας $l=1$, έχουμε $\chi_{q,p}(n) = \eta^{l(n)} = \eta^1 = \eta$,άρα $\chi_{q,p}(r) = \chi_{q,p}(n)^{l(r)}$ για κάθε $r|n$.Εδώ ολοκληρώνεται η απόδειξη της Πρότασης 1.

□

Θεωρούμε τώρα την περίπτωση $p=2$. Έστω $\chi_{q,2}$ είναι ο τετραγωνικός χαρακτήρας $\bmod q$. Από την ιδιότητα $g(\chi_{q,p})g(\overline{\chi_{q,p}}) = \chi_{q,p}(-1)q$ έχουμε $g(\chi_{q,2})^2 = \chi_{q,2}(-1)q$, δηλαδή $g(\chi_{q,2})^{n-1} = (\pm q)^{(n-1)/2}$.

Πρόταση 2 *Αν $q^{(n-1)/2} \not\equiv \pm 1 \pmod n$, τότε ο n είναι σύνθετος. Αν $q^{(n-1)/2} \equiv \pm 1 \pmod n$, τότε*

$$\chi_{q,2}(r) = \chi_{q,2}(n)^{l(r)}$$

Απόδειξη:

Έστω ότι ο n είναι πρώτος. Τότε $q^{n-1} \equiv 1 \pmod n$, δηλαδή $q^{(n-1)/2} \equiv \pm 1 \pmod n$.

Εστω τώρα ότι δεν ξέρουμε αν ο n είναι πρώτος. Είναι $g(\chi_{q,2})^{r-1} \equiv \chi_{q,2}^{-r} = \chi_{q,2}(r) \pmod r$, με r περιττό πρώτο (Λήμμα 2.11).

Επίσης $g(\chi_{q,2})^{n-1} = (\pm q)^{(n-1)/2} \equiv \eta \pmod n$,με $\eta = \pm 1$.

Έστω r ένας περιττός πρώτος διαιρέτης του n και $l = l(r)$.

Έχουμε

$$g(\chi_{q,2})^{n^l-1} = g(\chi_{q,2})^{(n-1)(n^{l-1}+\cdots+1)} \equiv \eta^{n^{l-1}+\cdots+1} \equiv \eta^l \pmod n$$

Έπεται λοιπόν ότι

$$g(\chi_{q,2})^{n^l-r} \equiv g(\chi_{q,2})^{n^l-1} g(\chi_{q,2})^{1-r} \equiv \frac{\eta^l}{\chi_{q,2}(r)} \pmod r$$

.

Έστω $k = u_2(n-1)$, τότε $2(n-1) = 2^{k+1}z$, με z περιττό.

Αφού $r^{p-1} \equiv n^{(p-1)l} \pmod{p^{k+1}}$ άρα για $p = 2$ παίρνουμε $n^l - r \equiv 0 \pmod{2^{k+1}}$ και $g(\chi_{q,2})^{2(n-1)} \equiv \eta^2 \equiv 1 \pmod n$, θα έχουμε

$$\left(\frac{\eta^l}{\chi_{q,2}(r)}\right)^z \equiv g(\chi_{q,2})^{(n^l-r)z} \equiv g(\chi_{q,2})^{2^{k+1}wz} \equiv g(\chi_{q,2})^{2(n-1)w} \equiv 1 \pmod r$$

Αφού ο z είναι περιττός και $\dfrac{\eta^l}{\chi_{q,2}(r)} = \pm 1$ συνεπάγεται ότι $\chi_{q,2}(r) = \eta^{l(r)}$ για κάθε πρώτο διαιρέτη r του n. Αφού $l(r_1 r_2) \equiv l(r_1) + l(r_2) \pmod{2^k}$, έχουμε $\chi_{q,2}(r) = \eta^{l(r)}$ για όλους τους διαιρέτες του n. Για $r = n$ έχουμε $\chi_{q,2}(n) = \eta^{l(n)} = \eta^1 = \eta$ δηλαδή $\chi_{q,2}(r) = \chi_{q,2}(n)^{l(r)}$ για όλα τα $r|n$.

Θεώρημα 1.1 *Έστω n, s και t όπως ορίστηκαν παραπάνω.Υποθέτουμε ότι:*

1. $q^{\frac{n-1}{2}} \equiv \pm 1 \pmod n$ *για όλα τα* $q \mid s$.
2. $\mathcal{J}(\chi_{q,p}^a, \chi_{q,p}^b)^\alpha \equiv \zeta \pmod n$ *με* $\zeta^{p^k} = 1$ *για όλους τους πρώτους* $q|s$ *και όλους τους περιττούς πρώτους* $p|q-1$ *(όπου* $k = u_p(q-1)$*, τα* α *και* a, b *όπως έχουν οριστεί παραπάνω.*
3. *Υπάρχει* $c \in \mathbb{Z}$ *με* $c^{\frac{n-1}{2}} \equiv -1 \pmod n$.

Τότε κάθε διαιρέτης r του n ικανοποιεί την

$$r \equiv n^i \pmod s$$

με $0 \le i < t$. *Αν μία εκ΄των* $(1), (2)$ *και* (3) *δεν ισχύει, τότε ο* n *είναι σύνθετος.*

Απόδειξη :

Έστω $p \mid n$ και $q \mid s$. Από τις προτάσεις 1 και 2 έχουμε ότι $\chi_{q,p}(r) = \chi_{q,p}(n)^{l(r)}$ για όλα τα $p|q-1$. Αφού αυτοί οι χαρακτήρες γεννάνε την ομάδα των χαρακτήρων Dirichlet $\bmod q$, έπεται ότι

$$\chi(r) = \chi(n)^{l(r)}$$

για όλους τους χαρακτήρες Dirichlet $\bmod q$. Δηλαδή $\chi(r) = \chi(n^{l(r)})$ και αφού έχουμε οδηγό q, συνεπάγεται ότι

$$r \equiv n^{l(r)} \pmod{q} \tag{1.13}$$

Αν q είναι περιττός και $q^2 \mid s$ έπεται ότι $q \in E$ και q^{1+a_q} είναι η μεγαλύτερη δύναμη του q που διαιρεί το s. Επίσης

$$r^{q-1} \equiv (n^{q-1})^{l(r)} \pmod{q^{1+a_q}} \tag{1.14}$$

από τον ορισμό του $l(r)$. Θεωρούμε τον ισομορφισμό (Λήμμα 2.12)

$$(\mathbb{Z}/q^{1+a_q}\mathbb{Z})^\times \cong (\mathbb{Z}/q\mathbb{Z})^\times \oplus \big((1+q\mathbb{Z}_q)/(1+q^{1+a_q}\mathbb{Z}_q)\big)$$

που στέλνει το x στο (x, x^{q-1}). Αφού τα r και $n^{l(r)}$ έχουν την ίδια εικόνα (από τις 1.13 και 1.14) θα πρέπει

$$r \equiv n^{l(r)} \pmod{q^{1+a_q}} \tag{1.15}$$

Για $q = 2$, από τον ορισμό του s έχουμε ότι το 4, αλλά οχι το 8, διαιρεί το s. Άρα

$$r \equiv n^{l(r)} \pmod{4} \tag{1.16}$$

Από τις 1.15 και 1.16 έχουμε ότι $r \equiv n^{l(r)} \pmod{s}$. Αφού $n^t \equiv 1 \pmod{s}$ έχουμε $r \equiv n^i \pmod{s}$, $0 \le i < t$.

□

Παράδειγμα 1.2 *Έστω $n = 48611$. Παίρνουμε $E = \{3\}$ και τότε $t = 6$. Ελέγχουμε αν $n^{p-1} \not\equiv 1 \pmod{p^2}$ και πράγματι $48611^2 \not\equiv 1 \pmod 9$. Έχουμε $s = 2^2 3^2 7 = 252$. Είναι $252 > \sqrt{48611} \simeq 220,48$ και $2^{24305} \equiv -1$, $3^{24305} \equiv 1$, $7^{24305} \equiv 1 \pmod{48611}$. Άρα η συνθήκη (1) ικανοποιείται καθώς επίσης και η (3) για $c = 2$.*

Μένει να ελέγξουμε την συνθήκη (2).

Έχουμε $p = 3$ και επιλέγουμε $q = 7$. Ας είναι ζ μια πρωταρχική $3-$ρίζα της μονάδος. Ένας χαρακτήρας $\chi = \chi_{7,3}$, με οδηγό 7 και τάξη 3, μπορεί να βρεθεί επιλέγοντας μια πρωταρχική ρίζα τάξης 3 $\pmod 7$ και θέτοντας $\chi(3) = \zeta$. Τότε έχουμε $\chi(y) = 1$ για $y = \pm 1$,$\chi(y) = \zeta$ για $y = \pm 3$ και $\chi(y) = \zeta^2$ για $y = \pm 2$.

Έστω $a = b = 1$. Τότε $J(\chi,\chi) = -\sum_{k=1}^{6} \chi(k)\chi(1-k) = -(\chi(1)\chi(0) + \chi(2)\chi(-1)+\chi(3)\chi(-2)+\chi(-3)\chi(-3)+\chi(-2)\chi(3)+\chi(-1)\chi(2)) = -3\zeta^2-2 = (3\zeta+3)-2 = 3\zeta+1$

Έχουμε $\alpha = \left[\frac{n}{3}\right]\sigma_1^{-1} + \left[\frac{2n}{3}\right]\sigma_2^{-1} = 16203 + 32407\sigma_2$ διότι $2^{-1} \equiv 2 \pmod 3$

Τότε

$$\mathcal{J}^\alpha = (1+3\zeta)^{16203} \cdot (1+3\zeta^2)^{32407}$$

$$(1+3\zeta)^{16203} = 46636 + 31749\zeta \pmod{48611}$$ [4]

$$(1+3\zeta^2)^{32407} = 21206 + 30341\zeta \pmod{48611}$$

Δηλαδή $\mathcal{J}^\alpha \equiv \zeta^2 \pmod{48611}$

Άρα η συνθήκη (2) *ισχύει.*

Από το θεώρημα 1.1 έχουμε ότι $r \equiv n^i \pmod{s}$ *για κάθε* $r|s$ *όπου* $0 \leq i < 6$.

Αφού $n \equiv 227 \pmod{s}$ *οι πιθανοί διαιρέτες του* 48611 *είναι οι*

$$r = 1, 227, 121, 251, 25, 131 \pmod{252}$$

Αν ο 48611 *είναι σύνθετος θα πρέπει να έχει ένα παράγοντα* $r \leq \sqrt{48611} \simeq 220,48$. *Οι μόνοι πιθανοί διαιρέτες είναι οι* $121, 25$ *και* 131. *Αφού κανένας από αυτούς δεν είναι διαιρέτης του* 48611, *ο* 48611 *είναι πρώτος.*

□

Παρατήρηση: Εαν $3 \leq p < 6 \cdot 10^9$ και $p \neq 1093, 3511$, τότε μπορούμε να εκλέξουμε $a = b = 1$. Κοίταξε [3]

[4] Για την εύρεση της δύναμης αυτής $\pmod{48611}$, ένας εύκολος τρόπος, είναι χρησιμοποιώντας τους διαδοχικούς τετραγωνισμούς και γράφοντας σε δυαδική μορφή τον εκθέτη $16203 = (11111101001011)_2$.

2 Παράρτημα

2.1 Δακτύλιος Ομάδας

Έστω G μία πεπερασμένη ομάδα. Ο δακτύλιος ομάδας $\mathbb{Z}[G]$ είναι το σύνολο των απεικονίσεων (όχι αναγκαστικά ομομορφισμών) απ' το G στο $\mathbb{Z}$ εφοδιασμένο με τις επόμενες δύο πράξεις

- Εαν $f_1, f_2 \in \mathbb{Z}[G]$, ορίζουμε

$$\big(f_1 + f_2\big)(\sigma) = f_1(\sigma) + f_2(\sigma), \forall\ \sigma \in G$$

- Ο πολλαπλασιασμός είναι λίγο πιο τεχνικός και ορίζεται ως εξής

$$f_1 \cdot f_2 = \sum_{\tau \in G} f_1(\tau) f_2(\tau^{-1}\sigma)$$

Οι παραπάνω δύο πράξεις δομούν το $\mathbb{Z}[G]$ σε δακτύλιο. Έτσι δικαιολογείται και το όνομα «δακτύλιος ομάδας».

Το τυπικό στοιχείο $f \in \mathbb{Z}[G]$, γράφεται στη μορφή

$$f = \sum_{\sigma \in G} f(\sigma)\sigma \ \text{ ή } \ f = \sum_{\sigma \in G} n_\sigma \sigma$$

Το ενδιαφέρον μας στρέφεται τώρα στην περίπτωση όπου $G = Gal(K/\mathbb{Q})$ [5] για ένα αριθμητικό σώμα K (π.χ. το κυκλοτομικό σώμα $\mathbb{Q}(\zeta_n)$, το οποίο είναι επέκταση Galois πάνω απ' το $\mathbb{Q}$ και πιο συγκεκριμένα στην περίπτωση που το K είναι ένα κυκλοτομικό σώμα).

Εξ' ορισμού η G δρα στο K. Μπορούμε να επεκτείνουμε την δράση της G με ένα φυσικό τρόπο σε δράση του $\mathbb{Z}[G]$ ως ακολούθως

Εαν $f \in \mathbb{Z}[G]$ και $x \in K$, τότε θέτουμε

$$x^f = f(x) = \prod_{\sigma \in G} \sigma(x)^{n_\sigma}$$

Είναι εύκολο να επαληθεύσουμε τις παρακάτω ιδιότητες $\big(x, x_1, x_2 \in K$ και $f, f_1, f_2 \in \mathbb{Z}[G]\big)$

(i) $x^{f_1+f_2} = x^{f_1}x^{f_2}$

(ii) $x^{f_1 f_2} = (x^{f_1})^{f_2} = (x^{f_2})^{f_1}$

(iii) $(x_1 + x_2)^f = x_1^f + x_2^f$

(iv) $(x_1 x_2)^f = x_1^f x_2^f$

[5] Εαν $K = \mathbb{Q}(\zeta_n)$ με ζ_n μία πρωταρχική n-ρίζα της μονάδος, τότε η επέκταση $K/\mathbb{Q}$ είναι επέκταση Galois με αντίστοιχη αβελιανή ομάδα Galois που δίνεται από την $G = Gal(K/\mathbb{Q}) = \big\{\sigma_a, (a,n) = 1 \ \text{ όπου } \ \sigma_a(\zeta_n) = \zeta_n^a\big\}$. Ο βαθμός της επέκτασης $K/\mathbb{Q}$ είναι $\varphi(n)$, όπου φ είναι η συνάρτηση του Euler.

2.2 Απαραίτητα Λήμματα

Λήμμα 2.1 *Η επιλογή των* s, t *δίνει* $n^t \equiv 1 \pmod{s}$

Απόδειξη:

Από το θεώρημα του Euler, καθώς $(n, q) = 1$ (λόγω της $(n, s) = 1$ και της $q|s$), έχουμε ότι

$$n^{\phi(q^{\upsilon_q(t)+1})} \equiv 1 \pmod{q^{\upsilon_q(t)+1}}, \text{ δηλαδή}$$

$$n^{q^{\upsilon_q(t)}(q-1)} \equiv 1 \pmod{q^{\upsilon_q(t)+1}} \tag{2.1}$$

Όμως $q - 1|t$ και $q^{\upsilon_q(t)}|t$ απ' όπου $q^{\upsilon_q(t)}(q-1)|t$, άρα $t = q^{\upsilon_q(t)}(q-1) \cdot t'$, για κάποιο $t' \in \mathbb{Z}$. Υψώνοντας λοιπόν την σχέση 2.1 στην δύναμη t' παίρνουμε $n^t \equiv 1 \pmod{q^{\upsilon_q(t)+1}}$.

Η τελευταία σχέση όμως, ισχύει για κάθε πρώτο q με $q - 1|t$, και καθώς όλοι αυτοί είναι διακεκριμένοι, παίρνουμε

$$n^t \equiv 1 \pmod{\prod_{q-1|t} q^{\upsilon_q(t)+1}}$$

απ' όπου έχουμε το ζητούμενο.

□

Λήμμα 2.2 *Κάθε αριθμός ισότιμος με* $1 \pmod{p}$ *αλλά όχι* $\bmod p^2$ *είναι γεννήτορας της ομάδας* $(1 + p\mathbb{Z}_p)/(1 + p^{1+a_p}\mathbb{Z}_p)$, *με* $a_p \geq 1$.

Απόδειξη:

Ας είναι $\beta \equiv 1 \pmod{p}$ και $\beta \not\equiv 1 \pmod{p^2}$

Αφού

$$1 + p\mathbb{Z}_p = \left\{1 + a_1 p + a_2 p^2 + \cdots / a_i \in \{0, 1, \ldots, p-1\}\right\}$$

και

$$1 + p^{1+a_p}\mathbb{Z}_p = \left\{1 + b_1 p^{1+a_p} + b_2 p^{2+a_p} + \cdots / b_i \in \{0, 1, \ldots, p-1\}\right\}$$

άρα

$$(1+p\mathbb{Z}_p)/(1+p^{1+a_p}\mathbb{Z}_p) = \left\{1 + c_1 p + c_2 p^2 + \cdots + c_{a_p} p^{a_p} / c_i \in \{0, 1, \ldots, p-1\}\right\}$$

η οποία έχει p^{a_p} στοιχεία (διότι τα $c_i \in \{0, 1, \ldots, p-1\}$ άρα κάθε ένα c_i έχει p επιλογές) άρα και η τάξη της είναι p^{a_p}.

Ας υποθέσουμε τώρα ότι υπάρχει κάποιο στοιχείο r, με $1 \leq r < p^{a_p}$ τέτοιο ώστε $\beta^r \equiv 1 \pmod{p^{1+a_p}}$ $(a_p \geq 1)$. Παίρνουμε το r να είναι το ελάχιστο δυνατό για το οποίο ισχύει η παραπάνω. Άρα το r είναι η τάξη του στοιχείου. Τότε αφού $r|p^{a_p}$, άρα $r = p^k$, με $0 \leq k < a_p$.

Διακρίνουμε τις περιπτώσεις

- Εαν $k = 0$, τότε $\beta \equiv 1 \pmod{p^{1+a_p}}$, αδύνατο λόγω της $\beta \not\equiv 1 \pmod{p^2}$ και του ότι $a_p \geq 1$.

- Εαν $k \geq 1$, τότε $\beta^{p^k} \equiv 1 \pmod{p^{1+a_p}} \equiv 1 \pmod{p^{2+k}}$ (διότι $2+k \leq 1+a_p$ όταν $k < a_p$). Όμως η μορφή του β που ανήκει στην παραπάνω ομάδα είναι

$$\beta = 1 + c_1 p + c_2 p^2 + \cdots + c_{a_p} p^{a_p}, \;\; c_i \in \{0, 1, \ldots, p-1\}$$

και τότε

$$\beta^{p^k} = \left(1 + c_1 p + c_2 p^2 + \cdots + c_{a_p} p^{a_p}\right)^{p^k} \equiv 1 + c_1 p^{k+1} \pmod{p^{2+k}}$$

διότι όλοι οι όροι πλην του δεύτερου όρου συνδιασμένου με τις μονάδες, περιέχουν πολλαπλάσιο του p^{k+2} και εξαφανίζονται. Άρα πρέπει $c_1 p^{k+1} \equiv 0 \pmod{p^{2+k}}$ δηλαδή $c_1 \equiv 0 \pmod{p}$ που είναι αδύνατο καθώς εαν είχαμε $c_1 \equiv 0 \pmod{p}$ τότε $\beta \equiv 1 \pmod{p^2}$, αδύνατο λόγω της υπόθεσης.

□

Λήμμα 2.3 *Ας είναι* $q - 1 = \prod_{i=1}^{m} p_i^{k_i}$ *και* $\chi_{i,j}$ *ο* j*-χαρακτήρας με οδηγό* q *και τάξη* $p_i^{k_i}$*. Τότε, το σύνολο αυτών των χαρακτήρων* $\chi_{i,j}$*, καθώς το* p_i *διατρέχει τους πρώτους διαιρέτες του* $q-1$*, παράγει την ομάδα των χαρακτήρων Dirichlet* $\bmod q$.

Απόδειξη:

Παίρνουμε

$$\chi_{i,j} : (\mathbb{Z}/q\mathbb{Z})^\times \to \mu_{p_i^{k_i}}, \;\; \forall i = 1, \ldots, m$$

όπου $\mu_{p_i^{k_i}}$ είναι το σύνολο των $p_i^{k_i}$ ριζών της μονάδος (που αποτελεί πολλαπλασιαστική ομάδα) και ο οποίος έχει οδηγό q και τάξη $p_i^{k_i}$.

Τότε ορίζουμε

$$\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mu_{q-1}$$

με $\chi = \chi_{1,j_1}\chi_{2,j_2}\ldots\chi_{m,j_m}$ κατά τον γνωστό τρόπο κατασκευής του, τον χαρακτήρα με οδηγό q και τάξη $\prod_{i=1}^{m} p_i^{k_i} = q - 1$.

Με τον τρόπο αυτό κατασκευάζουμε όλη την ομάδα των χαρακτήρων Dirichlet $\bmod q$. (Εξ' ορισμού, δεν ξεχνούμε ότι οι χαρακτήρες Dirichlet $\bmod q$ έχουν τάξη $q-1$. Οι χαρακτήρες $\chi_{i,j}$ που ορίσαμε παραπάνω, έχουν μεν οδηγό q αλλά η τάξη τους είναι $p_i^{k_i}$ άρα δεν αποτελούν όλους τους χαρακτήρες $\bmod q$ (Εκτός εαν το q είναι δύναμη πρώτου)).

□

Παράδειγμα 2.1 *Ας πάρουμε την περίπτωση* $q = 7$ *Τότε* $q - 1 = 6 = 2 \cdot 3$

Θέτουμε λοιπόν $p_1 = 2$ *με* $k_1 = 1$, *και* $p_2 = 3$ *με* $k_2 = 1$.

Οι χαρακτήρες $\chi_{1,j}$ *με οδηγό* 7 *και τάξη* 2, *είναι οι*

	1	2	3	4	5	6
$\chi_{1,1}$	1	1	1	1	1	1
$\chi_{1,2}$	1	1	-1	1	-1	-1

Το $\chi_{1,j}(3)$ *είναι γεννήτορας του* $\mathbb{Z}_7^\times$, *αρκεί λοιπόν να ορίσουμε το* $\chi_{1,j}(3)$ *για να βρούμε όλους τους χαρακτήρες. Παίρνουτας* $\chi_{1,j}(3) = \pm 1$, *έχουμε όλους τους δυνατούς χαρακτήρες*

$$\chi_{1,j} : \mathbb{Z}/7\mathbb{Z} \to \mu_2$$

Οι χαρακτήρες $\chi_{2,j}$ *με οδηγό* 7 *και τάξη* 3, *είναι οι*

	1	2	3	4	5	6
$\chi_{2,1}$	1	1	1	1	1	1
$\chi_{2,2}$	1	ω^2	ω	ω	ω^2	1
$\chi_{2,3}$	1	ω	ω^2	ω^2	ω	1

όπου $\omega = e^{2\pi i/3}$. *Οι τιμές* $\chi_{2,j}(3) = 1, \omega, \omega^2$ *αρκούν για να υπολογίσουμε τους χαρακτήρες*

$$\chi_{2,j} : \mathbb{Z}/7\mathbb{Z} \to \mu_3$$

Οι παραπάνω χαρακτήρες παράγουν όλους τους χαρακτήρες $\mod 7$. *Παράγουν δηλαδή τους χαρακτήρες*

	1	2	3	4	5	6
χ_1	1	1	1	1	1	1
χ_2	1	ω^2	ω	ω	ω^2	1
χ_3	1	ω	ω^2	ω^2	ω	1
χ_4	1	1	-1	1	-1	-1
χ_5	1	ω^2	$-\omega$	ω	$-\omega^2$	-1
χ_6	1	ω	$-\omega^2$	ω^2	$-\omega$	-1

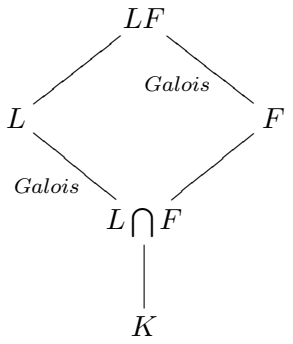
Πράγματι, παίρνουτας τον χαρακτήρα $\gamma := \chi_{1,j_1}\chi_{2,j_2}$ *για* $j_1 = 1, 2$ *και* $j_2 = 1, 2, 3$, *παίρνουμε την ομάδα των χαρακτήρων* $\mod 7$.

□

Λήμμα 2.4 *Ας είναι* K, F, L *σώματα. Εαν η* L/K *είναι πεπερασμένη επέκταση Galois και η* F/K *είναι επέκταση σωμάτων, τότε η* LF/F *είναι επέκταση Galois και*

$$Gal(LF/F) \cong Gal(L/L \bigcap F)$$

Σχηματικά



Απόδειξη :

Η επέκταση LF/F είναι Galois. Πράγματι, αφού L/K είναι Galois, άρα το L είναι σώμα ανάλυσης ενός συνόλου διαχωρισίμων πολυωνύμων $S \subseteq K[X]$. Επομένως και το LF είναι σώμα ανάλυσης του ίδιου $S \subseteq F[X]$. Επίσης εαν $f(x) \in K[X]$ διαχωρίσιμο, τότε έπεται ότι $f(x) \in F[X]$, επίσης διαχωρίσιμο. Άρα η LF/F είναι επέκταση Galois.

Θεωρούμε τώρα την απεικόνιση

$$\begin{aligned} \varphi : Gal(LF/F) &\rightarrow Gal(L/K) \\ \sigma &\mapsto \sigma|_L \end{aligned}$$

Αφού η L/K είναι κανονική επέκταση, άρα $\sigma|_L \in Gal(L/K)$, δηλαδή η φ είναι καλά ορισμένη και επίσης ομομορφισμός ομάδων.

$\ker\varphi = \{\sigma \in Gal(LF/F) |\ \ \sigma|_L = id_L\}$ Επομένως εαν $\sigma \in \ker\varphi$, τότε $\sigma|_F = id_F$ και $\sigma|_L = id_L$ απ' όπου το σώμα των σταθερών στοιχείων του $\ker\varphi$, περιέχει το σώμα F και το σώμα L. Επομένως, θα περιέχει και το LF, δηλαδή $\sigma = id_{LF}$ άρα η φ είναι 1–1.

Όμως ισχύει $Im\varphi \leq Gal(L/K)$ και συνεπώς από το θεμελιώδες θεώρημα της θεωρίας Galois, έχουμε ότι $Im\varphi = Gal(L/E)$, όπου $K \leq E \leq L$ και E το σώμα των σταθερών στοιχείων της $Im\varphi$.

Αρκεί να αποδείξουμε τώρα ότι $E = F \bigcap L$. Έστω λοιπόν $a \in F \bigcap L$. Τότε το a παραμένει σταθερό $\forall\ \sigma|_L, \sigma \in Gal(LF/F)$ $\big(a \in F$ και $\sigma \in Gal(LF/F)$ δίνουν $\sigma(a) = a$ και $\sigma|_L(a) = a\big)$. Άρα λοιπόν $a \in E$ και έτσι $F \bigcap L \leq E$.

Εαν τώρα $a \in E$ τότε $a \in L$ και $\sigma|_L(a) = a$, $\forall\ \sigma \in Gal(LF/F)$ πράγμα που σημαίνει ότι $\sigma(a) = a$, $\forall\ \sigma \in Gal(LF/F)$ δηλαδή $a \in F$ απ' όπου $a \in F \bigcap L$ και τελικά ότι $E \leq F \bigcap L$. Συνεπώς πράγματι $E = F \bigcap L$.

Άρα

$$Gal(LF/F)/\underbrace{\ker\varphi}_{id} \cong Im\varphi = Gal(L/L\bigcap F).$$

□

Λήμμα 2.5 *Ας είναι $[y], \{y\}$ το ακέραιο και το δεκαδικό μέρος του πραγματικού αριθμού y αντίστοιχα. Τότε ισχύουν τα παρακάτω:*

(a) $\displaystyle\sum_{\substack{x=1\\ p\not| x}}^{p^k-1} \frac{x}{p^k} = \frac{p^k - p^{k-1}}{2}$

(b) (Gauss) Εαν $\mu, \nu \in \mathbb{N}$ *με* $(\mu, \nu) = 1$, *τότε*

$$\sum_{\kappa=1}^{\nu-1} \left[\frac{\kappa\mu}{\nu}\right] = \sum_{\lambda=1}^{\mu-1} \left[\frac{\lambda\nu}{\mu}\right] = \frac{(\mu-1)(\nu-1)}{2}$$

(c) $\displaystyle\sum_{\substack{x=1\\ p\not| x}}^{p^k-1} \left\{\frac{mx}{p^k}\right\} = \frac{p^k - p^{k-1}}{2} = \sigma_m \sum_{\substack{x=1\\ p\not| x}}^{p^k-1} \left\{\frac{x}{p^k}\right\}$, *με* $(m, p) = 1$.

Απόδειξη :

(a) $\displaystyle\sum_{\substack{x=1\\ p\not| x}}^{p^k-1} \frac{x}{p^k} = \sum_{x=1}^{p^k-1} \frac{x}{p^k} - \sum_{\substack{x=1\\ p| x}}^{p^k-1} \frac{x}{p^k}$

Όμως $\displaystyle\sum_{x=1}^{p^k-1} \frac{x}{p^k} = \frac{1+2+\cdots+p^k-1}{p^k} = \frac{p^k(p^k-1)}{2p^k} = \frac{p^k-1}{2}$
και απ' την άλλη,

$$\sum_{\substack{x=1\\ p| x}}^{p^k-1} \frac{x}{p^k} = \frac{p}{p^k}+\frac{2p}{p^k}+\cdots+\frac{(p-1)p}{p^k}+\frac{p^2}{p^k}+\frac{p^2+p}{p^k}+\cdots+\frac{3p^2}{p^k}+\cdots+\frac{p^k-p}{p^k} =$$
$$\sum_{x=1}^{p^{k-1}-1} \frac{x}{p^{k-1}} = \frac{p^{k-1}-1}{2}$$

προσθέτωντας λοιπόν τις δύο τελευταίες παίρνουμε το ζητούμενο.

(b) Χρησιμοποιώντας ένα σύστημα καρτεσιανών συντεταγμένων xOy, θεωρούμε τα σημεία $A(\nu, 0), B(\nu, \mu), \Gamma(0, \mu)$. Στο εσωτερικό του ορθογωνίου ΟΑΒΓ βρίσκονται τα σημεία με συντεταγμένες (κ, λ) όπου $\kappa = 1, \ldots, \mu - 1,\ \lambda = 1, \ldots, \nu - 1$. Το πλήθος των σημείων αυτών είναι $(\mu-1)(\nu-1)$. Όμως πάνω στη διαγώνιο ΟΒ δεν ανήκει κανένα από τα σημεία αυτά, αφού τότε οι συντεταγμένες θα ικανοποιούν τη σχέση $\kappa \cdot \mu = \lambda \cdot \nu$, πράγμα αδύνατο αφού $(\mu, \nu) = 1$. Τα σημεία (κ, λ) που βρίσκονται κάτω από τη διαγώνιο (με το κ δοσμένο), ικανοποιούν την ανισότητα $\dfrac{\lambda}{\kappa} < \dfrac{\mu}{\nu}$ απ' όπου $\lambda < \dfrac{\mu\kappa}{\nu}$. Επομένως $\lambda \in \left\{1, 2, \ldots, \left[\dfrac{\mu\kappa}{\nu}\right]\right\}$ δηλαδή το λ παίρνει $\left[\dfrac{\mu\kappa}{\nu}\right]$ τιμές. Το συνολικό πλήθος σημείων είναι $\displaystyle\sum_{\kappa=1}^{\nu-1} \left[\frac{\mu\kappa}{\nu}\right]$. Επίσης, αφού κάτω από τη διαγώνιο βρίσκονται τα μισά από τα σημεία (κ, λ) του εσωτερικού δηλαδή $\dfrac{(\mu-1)(\nu-1)}{2}$ θα έχουμε τελικά το ζητούμενο.

(c)

$$\sum_{\substack{x=1\\ p\nmid x}}^{p^k-1}\left\{\frac{mx}{p^k}\right\}=\sum_{\substack{x=1\\ p\nmid x}}^{p^k-1}\left(\frac{mx}{p^k}-\left[\frac{mx}{p^k}\right]\right)=m\sum_{\substack{x=1\\ p\nmid x}}^{p^k-1}\frac{x}{p^k}-\sum_{\substack{x=1\\ p\nmid x}}^{p^k-1}\left[\frac{mx}{p^k}\right] \quad (2.2)$$

Όμως

$$\begin{aligned}\sum_{\substack{x=1\\ p\nmid x}}^{p^k-1}\left[\frac{mx}{p^k}\right] &= \sum_{x=1}^{p^k-1}\left[\frac{mx}{p^k}\right]-\sum_{\substack{x=1\\ p|x}}^{p^k-1}\left[\frac{mx}{p^k}\right]=\sum_{x=1}^{p^k-1}\left[\frac{mx}{p^k}\right]-\sum_{x=1}^{p^{k-1}-1}\left[\frac{mx}{p^{k-1}}\right]\\ &\overset{Gauss}{=} \frac{(m-1)(p^k-1)}{2}-\frac{(m-1)(p^{k-1}-1)}{2}\\ &= m\cdot\frac{p^k-p^{k-1}}{2}-\frac{p^k-p^{k-1}}{2} \quad (2.3)\end{aligned}$$

Από τις 2.2, 2.3 και με τη βοήθεια του Λήμματος 2.5 (a) έχουμε

$$\sum_{\substack{x=1\\ p\nmid x}}^{p^k-1}\left\{\frac{mx}{p^k}\right\}=m\cdot\frac{p^k-p^{k-1}}{2}-\left(m\cdot\frac{p^k-p^{k-1}}{2}-\frac{p^k-p^{k-1}}{2}\right)=\frac{p^k-p^{k-1}}{2}$$

Απ'την άλλη λόγω του ότι ο σ_m πειράζει μόνο τις m-ρίζες της μονάδος και αφήνει αναλλοίωτη οποιαδήποτε άλλη ποσότητα, έχουμε ότι

$$\sigma_m\sum_{\substack{x=1\\ p\nmid x}}^{p^k-1}\left\{\frac{x}{p^k}\right\}=\sum_{\substack{x=1\\ p\nmid x}}^{p^k-1}\left\{\frac{x}{p^k}\right\}=\sum_{\substack{x=1\\ p\nmid x}}^{p^k-1}\frac{x}{p^k}\overset{\text{Λήμμα2.5}(a)}{=}\frac{p^k-p^{k-1}}{2}$$

□

Λήμμα 2.6 *Εαν* $x\equiv y\pmod{p^k}$ *τότε* $x^p\equiv y^p\pmod{p^{k+1}}$

Απόδειξη:

Καταρχήν

$$x^p-y^p=(x-y)\underbrace{(x^{p-1}+x^{p-2}y+\cdots+xy^{p-2}+y^{p-1})}_{A}$$

Αρκεί λοιπόν να δείξουμε ότι $p|A$ και διακρίνουμε τις εξής περιπτώσεις

- Εαν $p|x$ τότε $p|y$ άρα $p|A$ και συνεπώς $x^p-y^p\equiv 0\pmod{p^{k+1}}$
- Εαν $p\nmid x$ τότε $p\nmid y$ άρα $(p,x)=(p,y)=1$ και από το θεώρημα του Fermat έχουμε ότι $x^{p-1}\equiv 1\pmod p$ και $y^{p-1}\equiv 1\pmod p$. Συνεπώς για κάθε παράγοντα $x^{p-k}\cdot y^{k-1}$ της παράστασης A ισχύει

$$x^{p-k}\cdot y^{k-1}\equiv y^{p-k}\cdot y^{k-1}=y^{p-1}\equiv 1\pmod p$$

άρα η παράσταση A διαιρείται από το p. □

Λήμμα 2.7 *Η παρακάτω απεικόνιση*

$$\begin{array}{rcl} \varphi : \mathbb{Z}[G] & \to & \mathbb{Z}/p^{k+1}\mathbb{Z} \\ \displaystyle\sum_{\substack{x=1 \\ p\not| x}}^{p^k-1} c_x\sigma_x & \mapsto & \displaystyle\sum_{\substack{x=1 \\ p\not| x}}^{p^k-1} c_x x^p \pmod{p^{k+1}} \end{array}$$

είναι καλώς ορισμένος ομομορφισμός δακτυλίων.

Απόδειξη:

Θα δείξουμε ότι η παραπάνω απεικόνιση είναι καλώς ορισμένη ενώ για το ότι είναι ομομορφισμός δακτυλίων είναι απλή εφαρμογή του ορισμού και παραλείπεται.

Έστω λοιπόν $\sigma_x, \sigma_y \in \mathbb{Z}[G]$. Τότε εαν $\sigma_x = \sigma_y$ τότε $\sigma_x(\zeta) = \sigma_y(\zeta),\ \forall\ \zeta\ p^k$-ρίζα της μονάδος, άρα και για τις πρωταρχικές ρίζες της μονάδος. Έστω ζ_{p^k} μία πρωταρχική p^k-ρίζα της μονάδος. Τότε $\sigma_x(\zeta_{p^k}) = \sigma_y(\zeta_{p^k})$ απ' όπου $\zeta_{p^k}^x = \zeta_{p^k}^y$ εξ' ορισμού.

Χωρίς βλάβη της γενικότητας ας υποθέσουμε ότι $x \neq y$ και μάλιστα $x > y$. Άρα η παραπάνω σχέση γράφεται $\zeta_{p^k}^{x-y} = 1$ απ' όπου $x - y | p^k$ διότι το ζ_{p^k} είναι πρωταρχική p^k ρίζα της μονάδος. Άρα $x \equiv y \pmod{p^k}$ απ' όπου $x^p \equiv y^p \pmod{p^k}$ δηλαδή $\varphi(\sigma_x) = \varphi(\sigma_y)$.

□

Λήμμα 2.8 (i) *Ας υποθέσουμε ότι η πολυωνυμική ισοτιμία*

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

όπου p πρώτος και r φυσικός ≥ 2, έχει μία λύση $b \pmod{p^{r-1}}$. Τότε εαν $f'(b) \not\equiv 0 \pmod{p}$, υπάρχει μοναδική λύση της $f(x) \equiv 0 \pmod{p^r}$ που αντιστοιχεί στη $b \pmod{p^{r-1}}$, η $a \equiv tp^{r-1} + b \pmod{p^r}$, όπου t είναι ένας ακέραιος που επαληθεύει την γραμμική ισοτιμία $f'(b)t \equiv (-f(b)/p^{r-1}) \pmod{p}$.

(ii) *Έστω p πρώτος με $p \not| x$. Τότε το x^{p-1} διατρέχει όλα τα $y \mod p^k$ καθώς $y \equiv 1 \pmod{p}$ και κάθε τιμή του y την παίρνει $p-1$ φορές.*

Απόδειξη:

(i) Έστω $a \pmod{p^r}$ μία λύση της $f(x) \equiv 0 \pmod{p^r}$, που αντιστοιχεί στη $b \pmod{p^{r-1}}$. Τότε $a \equiv b \pmod{p^{r-1}}$. Επομένως $a = tp^{r-1} + b$, όπου $t \in \mathbb{Z}$. Τότε

$$\begin{array}{rcl} f(a) & = & f(tp^{r-1} + b) = a_0(tp^{r-1} + b)^n + \cdots + a_{n-1}(tp^{r-1} + b) + a_n \\ & = & a_0\left[\displaystyle\sum_{k=0}^{n} \binom{n}{k} b^k (tp^{r-1})^{n-k}\right] + \cdots + a_{n-1}(tp^{r-1} + b) + a_n \end{array}$$

Από το παραπάνω ανάπτυγμα παίρνουμε

$$f(a) = f(b) + f'(b)tp^{r-1} + Mp^{2r-2}$$

όπου $M \in \mathbb{Z}$. Καθώς $f(b) \equiv 0 \pmod{p^{r-1}}$, υπάρχει $s \in \mathbb{Z}$ έτσι, ώστε $f(b) = sp^{r-1}$. Επίσης, επειδή $r \geq 2$, έχουμε $2r - 2 \geq r$. Επομένως

$$f(a) \equiv (s + tf'(b))p^{r-1} \pmod{p^r}$$

Συνεπώς

$$f(a) \equiv 0 \pmod{p^r} \Leftrightarrow s + tf'(b) \equiv 0 \pmod{p}$$

Αφού $f'(b) \not\equiv 0 \pmod{p}$, άρα $(p, f'(b)) = 1$ και επομένως η γραμμική ισοτιμία

$$tf'(b) \equiv -s \pmod{p}$$

έχει μοναδική λύση $t \pmod{p}$. Άρα ο ακέραιος $a = tp^{r-1} + b$ επαληθεύει την ισοτιμία $f(x) \equiv 0 \pmod{p^r}$. Έστω $t' \in \mathbb{Z}$, με $t \equiv t' \pmod{p}$. Τότε ο $a' = t'p^{r-1} + b$ επαληθεύει επίσης την ισοτιμία $f(x) \equiv 0 \pmod{p^r}$. Επειδή $p|t - t'$, έχουμε $p^r|a - a'$ και επομένως $a \equiv a' \pmod{p^r}$. Επομένως, η κλάση του $a \pmod{p^r}$ είναι η μοναδική λύση της $f(x) \equiv 0 \pmod{p^r}$ που είναι η αντίστοιχη της $b \pmod{p^{r-1}}$.

(ii) Το x^{p-1} διατρέχει τα $y \mod p^k$ με $y \equiv x^{p-1} \equiv 1 \mod p$. Αρκεί η $x^{p-1} \equiv y \pmod{p^k}$ να έχει $p - 1$ λύσεις. Θα δουλέψουμε με τη μέθοδο της μαθηματικής επαγωγής πάνω στο k.

- Για $k = 1$: Η $x^{p-1} \equiv y \equiv 1 \pmod{p}$ έχει πράγματι $p - 1$ ρίζες.
- Έστω λοιπόν $k \geq 2$ και ας υποθέσουμε ότι η $x^{p-1} \equiv y \pmod{p^{k-1}}$ έχει $p - 1$ ρίζες, τότε και η $x^{p-1} \equiv y \pmod{p^k}$ έχει $p - 1$ ρίζες. Ας είναι λοιπόν $b \mod p^{k-1}$ ρίζα της $x^{p-1} \equiv y \pmod{p^{k-1}}$. Συνεπώς $b^{p-1} \equiv y \pmod{p^{k-1}}$ και $p \nmid y$ άρα $b \not\equiv 0 \pmod{p^{k-1}}$. Εαν πάρω $f(x) = x^{p-1} - y$ τότε η τυπική παράγωγος στο b είναι $f'(b) = (p - 1)b^{p-2} \not\equiv 0 \pmod{p}$ διότι $p \nmid p - 1$ και $p \nmid b$ αφού εξ' υποθέσεως $p \nmid x$.
  Συνεπώς αφού $b \not\equiv 0 \pmod{p^{k-1}}$ και $f'(b) \not\equiv 0 \pmod{p}$, άρα υπάρχει μοναδική λύση της $x^{p-1} \equiv y \pmod{p^k}$ που αντιστοιχεί στην $b \mod p^{k-1}$, και η δοθείσα ισοτιμία έχει ακριβώς $p - 1$ λύσεις.

□

Λήμμα 2.9 *Ας είναι μ_{p^k} η ομάδα των p^k-ριζών της μονάδος με p πρώτο και $\zeta \in \mu_{p^k}$. Τότε εαν $(n, p) = 1$ και β όπως ορίστηκε στο Λήμμα 1.3,*

(i) *Εαν $\zeta^{-n\beta} = 1$ τότε $\zeta = 1$*

(ii) *Η απεικόνιση*

$$\begin{array}{rcl} \phi : \mu_{p^k} & \to & \mu_{p^k} \\ \zeta & \mapsto & \zeta^{-n\beta} \end{array}$$

είναι αυτομορφισμός

Απόδειξη:

(i) Εαν $\zeta^{-n\beta} = 1$ και $\zeta \neq 1$ τότε πρέπει

$$p | n \cdot \left(\sum_{\substack{x=1 \\ p \not| x}}^{p^k-1} \left(\left[\frac{(a+b)x}{p^k} \right] - \left[\frac{ax}{p^k} \right] - \left[\frac{bx}{p^k} \right] \right) x^{-1} \right)$$

κάτι το οποίο δεν ισχύει λόγω της $(n, p) = 1$ και του Λήμματος 1.4. Άρα $\zeta = 1$.

(ii) Αρκεί να δείξουμε ότι ο ϕ είναι μορφισμός και 1–1.

- **Μορφισμός:** Ας είναι $\zeta_1, \zeta_2 \in \mu_{p^k}$. Τότε $\phi(\zeta_1 \cdot \zeta_2) = \left(\zeta_1 \cdot \zeta_2\right)^{-n\beta} = \zeta_1^{-n\beta}\zeta_2^{-n\beta} = \phi(\zeta_1)\phi(\zeta_2)$.
- **1–1:** Ας είναι $\zeta_1, \zeta_2 \in \mu_{p^k}$ με $\phi(\zeta_1) = \phi(\zeta_2)$. Τότε $\zeta_1^{-n\beta} = \zeta_2^{-n\beta}$ απ' όπου $\left(\frac{\zeta_1}{\zeta_2}\right)^{-n\beta} = 1$ και έτσι από το (i) έχουμε $\frac{\zeta_1}{\zeta_2} = 1$ απ' όπου $\zeta_1 = \zeta_2$.

Παρατήρηση: Αφού η παραπάνω απεικόνιση είναι και επί, άρα

$$\forall\ \zeta \in \mu_{p^k},\ \ \exists\ \eta \in \mu_{p^k}\ \text{ τέτοιο ώστε }\ \phi(\eta) = \zeta,$$

δηλαδή

$$\zeta = \eta^{-n\beta}$$

□

Λήμμα 2.10 *Έστω ζ πρωταρχική n-ρίζα της μονάδος και ας υποθέσουμε ότι $p \not| n$ και $\mathcal{P}$ ένα πρώτο ιδεώδες του $\mathbb{Q}(\zeta)$, πάνω από το p. Τότε*

(i) *ισχύει $n \in \mathcal{P} \bigcap \mathbb{Z} = p\mathbb{Z}$*

(ii) *οι n-ρίζες της μονάδος είναι διακεκριμένες* $\mod \mathcal{P}$.

Απόδειξη:

(i) Καταρχήν το ότι $p\mathbb{Z} \subseteq \mathcal{P} \bigcap \mathbb{Z}$ είναι προφανές. Θα δείξουμε τώρα ότι εαν το R_1 είναι τυχαίο ιδεώδες του $R := \mathbb{Q}(\zeta)$, τότε το $R_1 \bigcap \mathbb{Z}$ είναι ιδεώδες του $\mathbb{Z}$. Πράγματι εαν $k \in R_1 \bigcap \mathbb{Z}$ και $\lambda \in \mathbb{Z}$, τότε $(k \in R_1 \bigwedge \lambda \in \mathbb{Z}$ δηλαδή $\lambda \in R,$ αφού $\mathbb{Z} \subseteq R) \bigwedge (k \in \mathbb{Z} \bigwedge \lambda \in \mathbb{Z})$ απ' όπου $k\lambda \in R_1$ (αφού R_1 ιδεώδες του R) και $k\lambda \in \mathbb{Z}$ και τελικά $k\lambda \in R_1 \bigcap \mathbb{Z}$. Εφαρμόζοντας λοιπόν το παραπάνω, έχουμε ότι το $\mathcal{P} \bigcap \mathbb{Z}$ είναι ιδεώδες του $\mathbb{Z}$. Άρα $\mathcal{P} \bigcap \mathbb{Z} \subseteq \mathbb{Z}$. Θα δείξουμε ότι $\mathcal{P} \bigcap \mathbb{Z} \neq \mathbb{Z}$.

Εαν $\mathcal{P} \bigcap \mathbb{Z} = \mathbb{Z}$, τότε θα ήταν $\mathbb{Z} \subseteq \mathcal{P}$ δηλαδή $\mathbb{Z}R \subseteq \mathcal{P}R$ απ' όπου $R \subseteq \mathcal{P}R$ (αφού $\mathbb{Z}R = R$). Όμως το $\mathcal{P}$ είναι ιδεώδες του R, δηλαδή $\mathcal{P}R = \mathcal{P}$ απ' όπου $R \subseteq \mathcal{P}$ και επειδή $\mathcal{P} \subseteq R$ έχουμε $\mathcal{P} = R$, άτοπο αφού $\mathcal{P}$ πρώτο ιδεώδες του R.

Επίσης το $p\mathbb{Z}$ είναι maximal ιδεώδες. Έστω A ιδεώδες του $\mathbb{Z}$ (με $A \neq \mathbb{Z}$) τέτοιο ώστε $p\mathbb{Z} \subseteq A \subset \mathbb{Z}$. Αρκεί να δείξουμε ότι $A = p\mathbb{Z}$. Όπως γνωρίζουμε τα ιδεώδη A του $\mathbb{Z}$ είναι της μορφής $A = n\mathbb{Z}, n \in \mathbb{N}, n \neq 1$ (αφού $A \neq \mathbb{Z}$). Έχουμε όμως $p \in p\mathbb{Z} \subset A$ άρα $p = n \cdot m, m \in \mathbb{Z}$ και αφού $n \neq 1$ πρέπει $n = p$ δηλαδή $A = p\mathbb{Z}$.

Τελικά λοιπόν, έχουμε ότι $p\mathbb{Z} \subseteq \mathcal{P} \bigcap \mathbb{Z} \subset \mathbb{Z}$ και αφού το $p\mathbb{Z}$ είναι maximal ιδεώδες, είναι $p\mathbb{Z} = \mathcal{P} \bigcap \mathbb{Z}$.

(ii) Όπως είναι γνωστό για $X = 1$ στην ταυτότητα $X^{n-1} + \cdots + X + 1 = \prod_{j=1}^{n-1}(X - \zeta^j)$, παίρνουμε

$$n = \prod_{j=1}^{n-1}(1 - \zeta^j).$$

Ας υποθέσουμε λοιπόν ότι ζ^i, ζ^j με $j > i$, δύο διαφορετικές n–ρίζες της μονάδος με $\zeta^i \equiv \zeta^j \pmod{\mathcal{P}}$. Τότε ισοδύναμα $\zeta^i - \zeta^j \in \mathcal{P}$ δηλαδή $\zeta^i(1 - \zeta^{j-i}) \in \mathcal{P}$

Όμως εαν $\zeta^i \in \mathcal{P}$, τότε καθώς $\zeta^{-i} \in \mathbb{Z}[\zeta]$, έχουμε $\mathcal{P} \ni \zeta^i\zeta^{-i} = 1$ συνεπώς για κάθε $\alpha \in \mathbb{Z}[\zeta]$, αφού $1 \in \mathcal{P}$ άρα $\alpha = \alpha \cdot 1 \in \mathcal{P}$, απ' όπου $\mathbb{Z}[\zeta] \subseteq \mathcal{P}$. Όμως απ' την άλλη $\mathcal{P} \subseteq \mathbb{Z}[\zeta]$ άρα $\mathcal{P} = \mathbb{Z}[\zeta]$,άτοπο αφού το $\mathcal{P}$ είναι πρώτο ιδεώδες.

Άρα $1 - \zeta^{j-i} \in \mathcal{P}$ συνεπώς $n = \prod_{j=1}^{n-1}(1 - \zeta^j) \in \mathcal{P}$ άρα τελικά $n \in \mathcal{P}$.

Όμως $n \in \mathbb{Z}$ άρα $n \in \mathcal{P} \bigcap \mathbb{Z} = p\mathbb{Z}$ απ' όπου τελικά $p|n$, άτοπο.

□

Λήμμα 2.11 *Έστω r περιττός πρώτος. Τότε ισχύει*

$$g(\chi_{q,2}(r))^{r-1} \equiv \chi_{q,2}(r)^{-r} \pmod{r}$$

Απόδειξη:

Από το Λήμμα 1.5 έχουμε $g(\chi_{q,2})^r \equiv \chi_{q,2}(r)^{-r} \cdot g(\chi_{q,2})^{\sigma_r} \pmod r$. Αρκεί λοιπόν, να δείξουμε ότι $g(\chi_{q,2})^{\sigma_r} = g(\chi_{q,2})$

Όμως

$$g(\chi_{q,2})^{\sigma_r} = -\sigma_r\Big(\sum_{y=1}^{q-1}\chi_{q,2}(y)\zeta_q^y\Big) = -\sum_{y=1}^{q-1}\sigma_r\big(\chi_{q,2}(y)\big)\zeta_q^y = -\sum_{y=1}^{q-1}\chi_{q,2}^r(y)\zeta_q^y =$$

$g(\chi_{q,2}^r) = g(\chi_{q,2})$, διότι r περιττός πρώτος.

□

Λήμμα 2.12 *Η απεικόνιση*

$$\begin{aligned}\phi : (\mathbb{Z}/q^{1+a_q}\mathbb{Z})^\times &\to (\mathbb{Z}/q\mathbb{Z})^\times \oplus \big((1+q\mathbb{Z}_q)/(1+q^{1+a_q}\mathbb{Z}_q)\big)\\ x &\mapsto (x, x^{q-1})\end{aligned}$$

είναι ισομορφισμός.

Απόδειξη:

Το ότι είναι μορφισμός είναι απλή εφαρμογή του ορισμού. Από την άλλη το πλήθος των στοιχείων του $(\mathbb{Z}/q^{1+a_p}\mathbb{Z})^\times$ είναι $\varphi(q^{1+a_q}) = q^{a_q}(q-1)$ και το πλήθος των στοιχείων του $(\mathbb{Z}/q\mathbb{Z})^\times \oplus \big((1+q\mathbb{Z}_q)/(1+q^{1+a_q}\mathbb{Z})\big)$ είναι $(q-1)q^{a_q}$. Θα δείξουμε ότι ο ϕ είναι και 1-1. Ας πάρουμε $\varphi(x) = \varphi(y)$ απ' όπου $(x, x^{q-1}) = (y, y^{q-1})$ και έτσι

$$\begin{aligned}x &\equiv y \pmod q\\ x^{q-1} &\equiv y^{q-1} \pmod{q^{1+a_q}}\end{aligned}$$

Όμως $x^{q-1} - y^{q-1} \equiv 0 \pmod{q^{1+a_q}}$ άρα $q^{1+a_q} | (x-y)(x^{q-2} + \cdots y^{q-2})$ $(q \geq 2)$.

Όμως $q \not| (x^{q-2} + \cdots y^{q-2})$ $\Big($διότι εαν $q|(x^{q-2} + \cdots y^{q-2})$ τότε $x^{q-2} + \cdots y^{q-2} \equiv 0 \pmod q \overset{x\equiv y \pmod q}{\Longrightarrow} x^{q-2} + \cdots x^{q-2} \equiv 0 \pmod q$ οπότε $(q-2)x^{q-2} \equiv 0 \pmod q$ άρα $q|q-2$ (άτοπο) ή $q|x^{q-2}$ (άτοπο διότι $x \in (\mathbb{Z}/q^{1+a_q}\mathbb{Z})^\times\Big)$.

Άρα λοιπόν $q^{1+a_q} | x - y$ απ' όπου $x \equiv y \pmod{q^{1+a_q}}$ δηλαδή η φ είναι 1-1.

Άρα λοιπόν είναι και επί λόγω της ισοπληθικότητας των παραπάνω συνόλων.

□

Βιβλιογραφία

Ξενόγλωσση

[1] Adleman, L., Pomerance C. and Rumely, R.: On distinguishing prime numbers from composite numbers, Annals of Math. 117 (1983) 173–206.

[2] Baker A.J., An Introduction to p-Adic Numbers and p-Adic Analysis, Online Notes, 2005.

[3] Cohen, H.: A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics 138, Springer-Verlag, Berlin 1993.

[4] Cohen H. - Lenstra H. W. Jr., Primality Testing and Jacobi Sums, Mathematics of Computation, Vol. 42, No. 165. (Jan., 1984), p. 297–330.

[5] Koblitz N., P-Adic Numbers, P-Adic Analysis, Zeta-Functions Second Edition, Graduate Texts in Mathematics 58, Springer-Verlag, 1984.

[6] Morandi P., Field and Galois Theory, Graduate Texts in Mathematics 167, Springer-Verlag, 1996.

[7] Schoof R., Four primality testing algorithms, to appear in "Surveys in algorithmic number theory" Cambridge University Press, 2004.

[8] Washington, L.: Introduction to cyclotomic fields 2nd edition, Graduate Texts in Math. 83, Springer-Verlag, New York 1997.

Ελληνόγλωσση

[1] Αντωνιάδης Ι., Σημειώσεις μαθήματος «Άλγεβρα ΙΙ», Χειμ. Εξάμηνο 2005-2006.

[2] Λάκκης Κ., Άλγεβρα, Θεσσαλονίκη 1980.

Ιστοσελίδες

[1] http://www.wikipedia.org

[2] http://planetmath.org