ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837

Διπλωματική Εργασία

Το αίτημα του Bertrand για τους αριθμούς Carmichael

Χαρίλαος Χόρτης

Τριμελής Επιτροπή:
Χρήστος Αθανασιάδης (Επιβλέπων)
Παντελεήμων Δοδός-Ντοντός
Διογένης-Ρωμανός Μαλικιώσης

Αθήνα, Δεκέμβριος 2023

Περίληψη

Στην παρούσα διπλωματική θα ασχοληθούμε με μία πρόσφατη δημοσίευση του Daniel Larsen, ο οποίος, ως μαθητής, κατάφερε να αποδείξει μία εικασία των Alford, Granville και Pomerance από το μακρινό 1994, περί της ύπαρξης αριθμού Carmichael μεταξύ καθενός επαρκώς μεγάλου φυσικού αριθμού και του διπλασίου του, κατ'αντιστοιχία με το κλασσικό θεώρημα που αφορά τους πρώτους αριθμούς.

Στο 1ο Κεφάλαιο θα παρουσιαστούν κάποια βασικά θεωρήματα της Στοιχειώδους Θεωρίας Αριθμών που αφορούν τους αριθμούς Carmichael και θα διατυπωθούν (ανευ αποδείξεως) κάποιες βασικές προτάσεις που θα μας χρειαστούν παρακάτω.

Στο 2ο Κεφάλαιο, ορίζοντας τις κατάλληλες ποσοτητες, ίσως κάπως αυθαίρετα με μια πρόχειρη ματιά, χρησιμοποιούμε μία ευρεία γκάμα τόσο αριθμοθεωρητικών όσο και συνδυαστικών λημμάτων ώστε να κατασκευάσουμε σύνολα ζευγών μη-συσταδοποιημένων πρώτων που θα παίξουν καταλυτικό ρόλο στην εύρεση των ζητούμενων αριθμών Carmichael.

Τέλος, στο 3ο Κεφάλαιο με την χρήση «ταπεινών εργαλείων» (ας μου επιτραπεί η έκφραση) από μαθήματα προπτυχιακού επιπέδου όπως ο Απειροστικός Λογισμός και η Θεωρία Πιθανοτήτων αποδεικνύεται ένα αρκετά τεχνικό αποτέλεσμα (Θεώρημα 6), το οποίο σε συνδυασμό με τη δουλειά του Κεφαλαίου 2 και με ένα ομολογουμένως περίτεχνο επιχείρημα, ολοκληρώνει την απόδειξη του κεντρικού θεωρήματος.

Abstract

The present thesis deals with a recent paper of Daniel Larsen (at the time of writing his paper a high school senior!) who managed to prove that between every sufficiently large natural number and its double there exists (at least) a Carmichael number, a conjecture prevalent in the Analytic Number Theory community since the early 90's due to a paper of Alford, Granville and Pomerance.

In Chapter 1, we present some basic theorems of Elementary Number Theory regarding Carmichael numbers and state (without proof) some propositions that are going to be useful in the rest of the chapters.

In Chapter 2, with seemingly little motivation, we define many notions that, with the help of combinatorial and number theoretic lemmas, become vital in constructing sets of pairs of "non-clustered" primes, the key-sets for finding the Carmichael numbers we look out for.

Finally, in Chapter 3, the ingenious use of elementary tools from Calculus and Probability Theory to prove a difficult technical theorem and some further neat observations and connections with the work done at Chapter 2, shall allow us to yield the desired result.

Ευχαριστίες

Ουφ, η αλήθεια είναι ότι είμαι λίγο συναισθηματικά φορτισμένος όσο γράφω αυτές τις σέρτικες αράδες. Και πως να μην είμαι άλλωστε, όταν ένας μεγάλος κύκλος, όπως αυτός της «εποπτευόμενης μάθησης», κάπου εδώ φτάνει στο τέλος του για να δώσει, με κάθε επισημότητα, την κυρίαρχη θέση του στην «αυτόβουλη μάθηση».

Προσπαθώντας να βάλω την σκέψη μου σε μία σειρά (λέμε τώρα...), μία στάση στο μακρινό παρελθόν φαντάζει ιδανική. Δάσκαλοι, καθηγητές, «καλοί» και «κακοί» συνέβαλαν με τα ερεθίσματά τους (ή μη), με τα κηρύγματά τους (ή μη) στην διαμόρφωση των ενδιαφερόντων και της προσωπικότητας μου σε κάποιον (αισθητό) βαθμό. Σαφώς μπορεί να αδικώ ορισμένους απ'αυτούς με την διάκριση που ετοιμάζομαι να κάνω, ωστόσο οφείλω ένα μεγάλο ευχαριστώ στους κ. Δημήτρη και κ. Νίκη, από την εποχή που δεν είχαμε επώνυμα, στους φυσικούς μου κ. Πάσχο, κ. Σαρρή και κ.Σκλαβενίτη, στους μαθηματικούς μου κ. Βασιλείου, κ.Βισκαδουράκη, κ. Ιωάννου, κ. Μαστρογιάννη (αν δεν κάνω λάθος) και κ. Λυκούδη, τους φιλολόγους κ. Γεωργαντή, κ. Ζαβραδινού και κ. Βαρθαλίτη και την κοινωνιολόγο μας κ. Τσακανίκα για διαφορετικούς λόγους τον καθένα, που δεν είναι της ώρας να αναλύσω.

Ως ενήλικος πλέον, μπαίνοντας στο μαθηματικό της Πάτρας, η προσαρμογή στο πιο αυστηρό και λιγότερο μεθοδολογικό τρόπο σκέψης των Μαθηματικών καθώς και σε ένα εντελώς διαφορετικό περιβάλλον απ'αυτό που είχα συνηθίσει τόσο σε θέμα προσώπων, όσο και από πλευράς υποχρεώσεων, ήταν σοκαριστική μα σχετικά άμεση και ομαλή. Παρά τις όποιες μας διαφωνίες, δεν μπορώ παρά να ευχαριστήσω τους κ. Τόγκα και κ. Ρουβέλα για τις εποικοδομητικές κουβέντες πέρι ανέμων και υδάτων (χρειάζονται και αυτές) και ιδιαιτέρως τον κ. Τζερμιά, που χάρη στις θαυμάσιες διαλέξεις του σε ένα αναρίθμητο πλήθος μαθημάτων καθώς και την αγάπη του για την θεωρία αριθμών, την οποία μεταδίδει με κάθε ευκαιρία, με ώθησε να εξερευνώ μαθηματικές ιδέες πέρα από τα στενά πλαίσια του μαθήματος, και την κ. Μαμωνά για την «ανοιχτή» (up for debate) προσέγγιση στα μαθήματά της και την δίψα της να προσφέρει άφθονο υλικό στους φοιτητές της.

Στο μεταπτυχιακό πρέπει να παραδεχθώ ότι τα πράγματα ήταν λίγο πιο απρόσωπα απ'ό,τι περίμενα. Θέλω πρωτίστως να ευχαριστήσω τους ανθρώπους της τριμελής επιτροπής, οι οποίοι με ενθάρρυναν να αναπτύξω το θέμα της διπλωματικής. Λίγη παραπάνω πίστωση δίνω στον κ. Αθανασιάδη (ή «Αθάνατο», όπως τον αποκαλώ εγώ) για τις εξαίρετες σημειώσεις του στο πεδίο της (άλγεβρο-)συνδυαστικής, που είναι ένας πραγματικός θησαυρός για κάθε ενδιαφερόμενο, και στον κύριο Μαλικιώση για την φιλική στάση που κράτησε εξαρχής στην υλοποίηση της εργασίας, παρότι δεν έχουμε συναντηθεί ποτέ δια ζώσης. Κατόπιν, με εξέπληξε ευχάριστα η λογική δομή και η συνεχής ροή των διαλέξεων που παρακολούθησα από τους κ. Εμμανουήλ και κ. Τσαπρούνη. Τους είμαι ευγνώμων για τη μαθησιακή εμπειρία. Σε πιο προσωπικό επίπεδο, ευχαριστώ τους κ. Συκιώτη και κ.

Τύρο για τις συμβουλές-παραινέσεις τους.

Μπορεί να τους αφιερώνω ένα μικρό κομμάτι στο χαρτί, κατέχουν ωστόσο ένα αντιστρόφως ανάλογο ποσοστό στην καρδιά μου. Οι φίλοι και οι παρέες με τις απόψεις, τις εμπειρίες, τις φιλοδοξίες, με τις ανησυχίες, τις ιδιαιτερότητες και τις κακουχίες αποτέλεσαν τον πυλώνα ώστε να ωριμάσω σαν άνθρωπος, σαν μαθηματικός και να γράφω με τις ώρες δακρύβρεχτα κειμενάκια σαν και αυτό που ξετυλίγεται μπροστά σας. Περικλή, Γιώργο Χ., Γιώργο Τ., Παντελή, Πέτρο, Κλεοπάτρα, Σταύρο, Κωνσταντίνα, Βασίλη, Νεφέλη, Λιάκο, είστε απίστευτοι! Ξεχωριστή μνεία στους Φίλιππο και Παναγιώτη για την υπομονή και την κατανοήση που έδειξαν στην γκρίνια, στην υστερία και στην απογοήτευση που μοιράστηκα μαζί τους τα δύο αυτά χρόνια του μεταπτυχιακού.

Για το τέλος, άφησα την φαμίλια. Καπετάνιε (φευ), νονέ, νονά, πατέρα (φευ), μητέρα, χωρίς την μακροχρόνια και απεριόριστη υποστήριξή σας, δε θα βρισκόμουν «εδώ» πέραν πάσης αμφιβολίας. Για εσάς και όσους με ξέρουν, είναι αυτονόητο, πιστεύω, ότι δε θα μπορούσα παρά να...

...αφιερώσω αυτή την διπλωματική στους γονείς μου.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Ξεκινάμε την περιήγησή μας δίνοντας ορισμούς, αναγκαίους για την κατανόηση του θέματος της εργασίας μας, και κάποιες συνοδευτικές προτάσεις πάνω στις οποίες στηρίζεται το θεώρημα που προσπαθούμε να αποδείξουμε.

1. Συμβολισμοί

Συμβάσεις: Κατα τα γνωστά, με $(a,b), [a,b]$ συμβολίζουμε τον μέγιστο κοινό διαιρέτη (ΜΚΔ) και το ελάχιστο κοινό πολλαπλάσιο (ΕΚΠ) των αριθμών a, b, αντίστοιχα. Επίσης, όταν γράφουμε $[\{a_1, ..., a_r\}]$ για θετικούς ακέραιους $a_1, ..., a_r$ εννοούμε το $[a_1, .., a_r]$.

Με $\mathbb{P}$ θα συμβολίζουμε από 'δω και πέρα το σύνολο των πρώτων αριθμών και η γραφή p ή p_i θα παραπέμπει αποκλειστικά σε κάποιον πρώτο αριθμό.

Με $\phi(m)$ συμβολίζουμε την τιμή της συνάρτησης του Euler σε κάποιο $m \in \mathbb{Z}_+$.

Με $\pi(x) = \sum_{p \leq x} 1$ την τιμή της συνάρτησης (καταμέτρησης) των πρώτων μέχρι ένα $x \in \mathbb{R}$, με $\pi(x; q, a) = \sum_{\substack{p \leq x \\ p \equiv a(\mod q)}} 1$ την τιμή της συνάρτησης (καταμέτρησης) των πρώτων της μορφής $a(\mod q)$ μέχρι ένα $x \in \mathbb{R}$ και με $E(x; q, a)$ το $E(x; q, a) = |\pi(x; q, a) - \frac{\pi(x)}{\phi(q)}|$.

Με $P^+(m)$ συμβολίζουμε τον μεγαλύτερο πρώτο που διαιρεί τον $m \in \mathbb{Z}$.

Με $|A|$ ή $\#A$ συμβολίσουμε το πλήθος των στοιχείων ενός συνόλου A.

Τέλος, έστω $f, g : [0, +\infty] \to \mathbb{R}$ δύο τελικά μη αρνητικές συναρτήσεις (δηλαδή από ένα x_0 και μετά παίρνουν μόνο μη αρνητικές τιμές).

Όποτε γράφουμε $f(x) = O(g(x))$ ή $g(x) = \Omega(f(x))$ θα εννοούμε ότι υπάρχουν $x_0, C > 0$ ώστε $f(x) \leq Cg(x)$ για κάθε $x \geq x_0$.

Αντίστοιχα, όποτε γράφουμε $f(x) = o(g(x))$ ή $g(x) = \omega(f(x))$ θα εννοούμε ότι για κάθε $C > 0$ υπάρχει $x_0 = x_0(C)$ ώστε $f(x) \leq Cg(x)$ για κάθε $x \geq x_0$.

2. Βασικές έννοιες και προτάσεις

Ορισμός (Ψευδοπρώτοι Fermat): Έστω ακέραιος $a > 1$. Αν ο σύνθετος αριθμός b είναι τέτοιος ώστε $a^{b-1} \equiv 1(\mod b)$, τότε λέμε ότι ο b είναι ψευδοπρώτος Fermat στη βάση a.

Π.χ. $9^3 \equiv 1(\mod 4)$, άρα το 4 είναι ψευδοπρώτος Fermat στη βάση 9.

Πρόταση 1 (Cipolla): Έστω p πρώτος τέτοιος ώστε $p \nmid a(a^2-1)$ και $n = \frac{a^{2p}-1}{a^2-1}$. Τότε ο n είναι ψευδοπρώτος Fermat στη βάση a. Κατα συνέπεια, σε κάθε βάση αντιστοιχούν άπειροι ψευδοπρώτοι Fermat.

Απόδειξη: Παρατηρούμε ότι $6 = 2 \cdot 3 \mid a(a^2-1)$ άρα $p \notin \{2,3\}$, δηλαδή $p > 3$ και περιττός.

Έπειτα $n = \dfrac{a^{2p}-1}{a^2-1} = \dfrac{a^p-1}{a-1} \cdot \dfrac{a^p+1}{a+1} = (1+a+...+a^{p-1})(1-a+a^2-...+a^{p-1})$

Άρα αν $n_1 = 1+a+...+a^{p-1}$ και $n_2 = 1-a+a^2-...+a^{p-1}$, τότε αφού p περιττός, n_1, n_2 περιττοί, ενώ από το μικρό θεώρημα του Fermat θα έχουμε:
$(a-1)(n_1-1) = (a-1)n_1 - (a-1) = a^p - 1 - (a-1) = a^p - a \equiv 0(\mod p)$
$(a+1)(n_2-1) = (a+1)n_2 - (a+1) = a^p + 1 - (a+1) = a^p - a \equiv 0(\mod p)$
και $p \nmid (a-1)(a+1)$, από υπόθεση,
οπότε από το Κινέζικο Θεώρημα Υπολοίπων $n_1, n_2 \equiv 1(\mod 2p) \Rightarrow n \equiv 1(\mod 2p)$ και συνεπώς $2p \mid n-1$.

Όμως $a^{2p} = (a^{2p}-1)+1 = (a^2-1)n+1 \equiv 1(\mod n)$, δηλαδή τελικά
$a^{n-1} \equiv (a^{2p})^{\frac{n-1}{2p}} \equiv 1(\mod n)$, όπως θέλαμε.

Για το 2ο σκέλος, μας αρκεί π.χ. ότι υπάρχουν άπειροι πρώτοι p τ.ω. $p > a(a^2-1)$, οπότε έχουμε το ζητούμενο. ■

Ορισμός (Αριθμοί Carmichael): Ένας σύνθετος αριθμός m ονομάζεται αριθμός Carmichael αν είναι ψευδοπρώτος Fermat σε κάθε βάση a για την οποία $(a,m) = 1$.

Παραδείγματα, αριθμών Carmichael υπάρχουν πάμπολλα, λ.χ. ήδη από το 1887 ο Τσέχος μαθηματικός Šimerka[5] είχε εντοπίσει τους 1105,1729(!),2465,2821,6601,8911. Η απόδειξη του παρακάτω θεωρήματος, η οποία θα πραγματοποιηθεί στο 3ο Κεφάλαιο, αποτελεί τον στόχο αυτής της εργασίας.

Θεώρημα 1 (Larsen[9]): Για κάθε $\epsilon > 0$ και $z = z(\epsilon)$ επαρκώς μεγάλο, θα υπάρχουν τουλάχιστον $\exp\Big(\frac{\log z}{(\log\log z)^{2+\epsilon}}\Big)$ αριθμοί Carmichael στο διάστημα $\big(z, z + \frac{z}{(\log z)^{\frac{1}{2+\epsilon}}}\big)$.

Μια χρήσιμη επισήμανση είναι ότι μπορούμε να θέσουμε το $\epsilon = \epsilon_0$ οσοδήποτε μικρό θέλουμε (αρκετά μικρότερο της μονάδας, ας πούμε) και αν αποδείξουμε το θεώρημα για αυτήν την τιμή, τότε αυτόματως θα ξέρουμε ότι ισχύει για κάθε ϵ τ.ω. $\epsilon \geq \epsilon_0$. Αυτή την πεπατημένη οδό θα ακολουθήσουμε στην συνέχεια, αλλά ας δούμε πρώτα κάποια πιο απτά αποτελέσματα.

Θεώρημα 2 (Korselt): Ο σύνθετος αριθμός m είναι αριθμός Carmichael ανν είναι ελεύθερος τετραγώνων και $p-1 \mid m-1$ για κάθε πρώτο p που διαιρεί τον m.

Απόδειξη:
($\Rightarrow$) Θα δείξουμε πρώτα ότι ο m είναι ελεύθερος τετραγώνων.

Προς άτοπο, έστω ότι $m = p^k m'$ όπου $(p^k, m') = 1$ και $k \geq 2$.

Από το Κινέζικο Θεώρημα Υπολοίπων το σύστημα
$x \equiv 1 + p(\mod p^k)$,
$x \equiv 1(\mod m')$
έχει μοναδική λύση $(\mod m)$ και επειδή $(x, p^k) = (x, m') = 1$ από την προπτυχιακή Θεωρία Αριθμών γνωρίζουμε ότι $(x, m) = (x, p^k \cdot m') = (x, p^k) \cdot (x, m') = 1$, όποτε μιας και ο m είναι αριθμός Carmichael $x^{m-1} \equiv 1(\mod m)$ και άρα
$x^{m-1} \equiv 1(\mod p^k) \Rightarrow (p+1)^{m-1} \equiv 1(\mod p^k) \Rightarrow (p+1)^{m-1} \equiv 1(\mod p^2) \Rightarrow 1 + (m-1)p \equiv 1(\mod p^2) \Rightarrow 1 - p \equiv 1(\mod p^2) \Rightarrow 0 \equiv p(\mod p^2)$, άτοπο. Συνεπώς $k = 1$.

Τώρα, πάλι από το προπτυχιακό μάθημα της Θεωρίας Αριθμών, γνωρίζουμε ότι κάθε πρώτος αριθμός έχει πρωταρχική ρίζα. Έστω r μία τέτοια πρωταρχική ρίζα ενός πρώτου p που διαιρεί τον m.

Εάν $(r, m) = 1$, τότε $r^{m-1} \equiv 1(\mod m) \Rightarrow r^{m-1} \equiv 1(\mod p)$, οπότε $p-1 \mid m-1$, όπως θέλαμε.

Εάν από την άλλη, $(r, m) = a > 1$ θεωρούμε το $r' = r + \frac{m}{a}$. Τότε $r' \equiv r(\mod p)$, δηλαδή r' πρωταρχική ρίζα, διότι $p \mid \frac{m}{a}$ και, καθώς $(\frac{m}{a}, a) = 1$ (m ελ. τετραγώνων),

$(r', m) = (r', \frac{m}{a}) \cdot (r', a) = (r, \frac{m}{a}) \cdot (\frac{m}{a}, a) = 1 \cdot 1 = 1,$
με την ισότητα $(r, \frac{m}{a}) = 1$ να ισχύει αφού $a = (r, m) = (r, a)(r, \frac{m}{a}) = a(r, \frac{m}{a})$

Μέσω του r' αναγόμαστε στην προηγούμενη περίπτωση και από την αυθαίρετη επιλογή του πρώτου p, έπεται το ζητούμενο.

($\Leftarrow$) Έστω $m = p_1 \cdots p_r$ όπου τα $p_i \neq p_j$ για $i \neq j$ και έστω αυθαίρετο a με $(a, m) = 1$.

Τότε $(a, p_i) = 1$ για κάθε i, οπότε από το μικρό Θεώρημα του Fermat
$a^{p_i - 1} \equiv 1(\mod p_i) \Rightarrow a^{m-1} \equiv 1(\mod p_i)$
(αφού, από υπόθεση, $p_i - 1 \mid m - 1$) για κάθε i, άρα από το Κινέζικο Θεώρημα Υπολοίπων
$a^{m-1} \equiv 1(\mod p_1 \cdots p_r) \equiv 1(\mod m)$, δηλαδή ο m είναι αριθμός Carmichael. ■

Πόρισμα 2.1 (Chernick): Αν ο k είναι φυσικός αριθμός τέτοιος ώστε οι αριθμοί $6k + 1, 12k + 1, 18k + 1$ να είναι όλοι πρώτοι, τότε ο $m = (6k + 1)(12k + 1)(18k + 1)$ είναι αριθμός Carmichael.

Απόδειξη: Ο ακέραιος m είναι σύνθετος και ελεύθερος τετραγώνων (προφανώς), οπότε πρέπει να δείξουμε ότι $6k, 12k, 18k \mid m-1$. Αρκεί να δείξουμε ότι το $36k = [6, 12, 18]k = [6k, 12k, 18k]$ είναι διαιρέτης του $m - 1$.

$m(\mod 4k) \equiv (6k+1)(12k+1)(18k+1)(\mod 4k) \equiv (2k+1)(1)(2k+1)(\mod 4k) \equiv (4k^2 + 4k + 1)(\mod 4k) \equiv 1(\mod 4k)$
συνεπώς $4k \mid m - 1$ ενώ

$m(\mod 9k) \equiv (6k + 1)(12k + 1)(18k + 1)(\mod 9k) \equiv (-3k + 1)(3k + 1)(1)$
$(\mod 9k) \equiv (1 - 9k^2)(\mod 9k) \equiv 1(\mod 9k)$
άρα $9k \mid m - 1$, οπότε από τη γνωστή Θεωρία Αριθμών

$36k = [4, 9]k = [4k, 9k] \mid m - 1$, απ'όπου έχουμε το ζητούμενο. ■

Πόρισμα 2.2: Ένας σύνθετος αριθμός m είναι αριθμός Carmichael ανν $a^m \equiv a(\mod m)$ για κάθε $a \in \mathbb{Z}$.

Απόδειξη: Η δεξια συνεπαγωγή είναι άμεση αν χρησιμοποιήσουμε την ισοδυναμία που μας δίνει το Θεώρημα 1.
Η αριστερή συνεπαγωγή είναι και αυτή άμεση, δουλεύοντας με κάποιο $a \in \mathbb{Z}$ τ.ω. $(a, m) = 1$ και τον ορισμό των αριθμών Carmichael.
Οι λεπτομέρειες αφήνονται στον αναγνώστη. ■

Ορισμός (Συνάρτηση Carmichael): Την συνάρτηση $\lambda : \mathbb{Z}_+ \to \mathbb{Z}_+$ τ.ω.
$\lambda(m) = \min\{k \in \mathbb{Z}_+ : \forall a(((a, m) = 1) \wedge (a^k \equiv 1(\mod m))\}$ την αποκαλούμε συνάρτηση Carmichael των θετικών ακεραίων

Συχνά επεκτείνουμε την χρήση της σε πεπερασμένες (αβελιανές) ομάδες, εννοώντας το εξής: Αν G μία πεπερασμένη (αβελιανή) ομάδα $\lambda(G) = \min\{k \in \mathbb{Z}_+ : \forall a((a \in G) \wedge (a^k = 1_G))\}$.
Με αυτήν την σύμβαση π.χ. $\lambda((\mathbb{Z}/m\mathbb{Z})^\times) = \lambda(m)$

Πρόταση 2: Έστω $m, k \in \mathbb{Z}_+$ τ.ω. $(m, k) = 1$. Τότε $\lambda(mk) = [\lambda(m), \lambda(k)]$. Συνεπώς, αν $m = p_1^{a_1} \cdots p_r^{a_r}$, με $p_i \neq p_j$ για $i \neq j$, τότε $\lambda(m) = [\lambda(p_1^{a_1}), ..., \lambda(p_r^{a_r})]$.

Απόδειξη: Δείχνουμε πρώτα ότι $[\lambda(m), \lambda(k)] \mid \lambda(mk)$ (1)

Έστω a τ.ω. $(a, m) = 1$. Τότε, από Κινέζικο Θεώρημα, το σύστημα
$x \equiv a(\mod m), x \equiv 1(\mod k)$
έχει μοναδική λύση $(\mod mk)$ και $(x, m) = (x, k) = 1 \Rightarrow (x, mk) = 1$ άρα, εξ'ορισμού, $x^{\lambda(mk)} \equiv 1(\mod mk)$, οπότε $x^{\lambda(mk)} \equiv 1(\mod m) \Rightarrow a^{\lambda(mk)} \equiv 1(\mod m)$.

Μιας και η επιλογή του a ήταν αυθαίρετη, δηλαδή μία τέτοια σχέση ισχύει για κάθε a τ.ω. $(a, m) = 1$, ένα επιχείρημα ευκλείδειας διαίρεσης, όπως αυτά που συναντάμε συχνα σε ένα προπτυχιακό μάθημα Άλγεβρας ή Θεωρίας Αριθμών, λόγω της ελαχιστότητας του $\lambda(m)$ μας δίνει $\lambda(m) \mid \lambda(mk)$.

Εργαζόμενοι ομοίως λ.χ. για $y \equiv 1(\mod m)$, $y \equiv b(\mod k)$ (όπου αυτή τη φορά $(b, k) = 1$) καταλήγουμε στο γεγονός ότι $\lambda(k) \mid \lambda(mk)$, οπότε η αρχική μας επιδίωξη πραγματοποιήθηκε.

Έστω τώρα c τ.ω. $(c, mk) = 1$. Τότε $(c, m) = (c, k) = 1$ και άρα
$c^{\lambda(m)} \equiv 1(\mod m)$, $c^{\lambda(k)} \equiv 1(\mod k)$
$\Rightarrow c^{[\lambda(m),\lambda(k)]} \equiv 1(\mod m)$, $c^{[\lambda(m),\lambda(k)]} \equiv 1(\mod k)$ και άρα $c^{[\lambda(m),\lambda(k)]} \equiv 1(\mod mk)$.
Από την αυθαιρεσία στην επιλογή του c και την ελαχιστότητα του $\lambda(mk)$, προκύπτει ότι $\lambda(mk) \mid [\lambda(m), \lambda(k)]$, οπότε μαζί με το (1), έχουμε την ποθητή ισότητα.

Για το 2ο σκέλος, χρησιμοποιούμε την εξής ιδιότητα του ΕΚΠ $[b_1, b_2, ..., b_k] = [b_1, [b_2, ..., b_k]]$ και κάνουμε επαγωγή στο πλήθος των (διαφορετικών) πρώτων παραγόντων του m.

Αν το m έχει 2 ή λιγότερους διαφορετικούς πρώτους παράγοντες, το αποτέλεσμα είναι άμεσο από το 1ο σκέλος.

Έστω ότι το έχουμε αποδείξει για κάθε k με $r - 1 \geq 2$ παράγοντες και m, όπως στην εκφώνηση.
Τότε $\lambda(m) = \lambda(p_1^{a_1} \cdots p_r^{a_r}) = \lambda(p_1^{a_1}(p_2^{a_2} \cdots p_r^{a_r})) = [\lambda(p_1^{a_1}), \lambda(p_2^{a_2} \cdots p_r^{a_r})] =$
$[\lambda(p_1^{a_1}), [\lambda(p_2^{a_2}), ..., \lambda(p_r^{a_r})]] = [\lambda(p_1^{a_1}), ..., \lambda(p_r^{a_r})]$ που είναι και το ζητούμενο, με την 3η ισότητα να ισχύει από το 1ο σκέλος, την 4η να αποτελεί το επαγωγικό βήμα και την 5η να είναι η ιδιότητα του ΕΚΠ που προαναφέραμε. ■

Πρόταση 3: (Θεώρημα Πρώτων Αριθμών): $\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$

Απόδειξη: Παραλείπεται. Αποδείξεις υπάρχουν σε παρα πολλά βιβλία-εργασίες Θεωρίας Αριθμών (βλ. [2], [4] ή για να ευλογούμε και τα γένια μας [16]) ή και άλλων συγγενών κλάδων (βλ. [3]). Οι περισσότεροι συγγραφείς παρουσιάζουν την απόδειξη με χρήση θεωρίας από την Μιγαδική Ανάλυση, ωστόσο υπάρχει μία «στοιχειώδης» απόδειξη που βασίζεται σε λιγότερο προηγμένα (αναλυτικά) μέσα και η οποία οφείλεται στους Erdös και Selberg (βλ.[11], και [15] για την φιλονικία τους). Επίσης βρίσκονται σε έξαρση τώρα τελευταία, οι αποδείξεις μέσω προσποιητής προσέγγισης (πχ [14]). ■

Απο δω και στο εξής θα αναφερόμαστε σε αυτό ως ΘΠΑ.

Πρόταση 4 (Siegel-Walfisz): Για $q \leq (\log x)^K, (a,q) = 1$,
$\pi(x;q,a) = \frac{\pi(x)}{\phi(q)} + O(\exp\Big(-c_1\sqrt{\log x}\Big))$, όπου $c_1 = c_1(K)$ κάποια θετική σταθερά.

Απόδειξη: Παραλείπεται. Βασίζεται στο εξής θεώρημα:
Για να μηδενίζεται μια L-σειρά Dirichlet $L(s,\chi)$ στο χωρίο
$\{s \in \mathbb{C} : 1 - \frac{c'}{\log q} < \mathrm{Re}(s) \leq 1\}$ θα πρέπει:
1. Ο χ να είναι πρωταρχικός πραγματικός χαρακτήρας και όχι ο κύριος.
2. Να υπάρχει μοναδικό σημείο μηδενισμού, το οποίο θα είναι πραγματικός αριθμός.
Έπειτα αποδεικνύουμε το θεώρημα του Siegel που μας διαβεβαιώνει ότι δεν υπάρχουν μηδενικά στην περιοχή $\{s \in \mathbb{C} : 1 - c_1(\epsilon)q^{-\epsilon} < \mathrm{Re}(s) \leq 1\}$ για κάθε $\epsilon > 0$,
απ' όπου έπεται η πρότασή μας (για περισσότερες πληροφορίες ανατρέξτε στα Κεφάλαια 20-22 του [6]). ■

Σχόλιο: Η σημασία της παραπάνω πρότασης έγκειται στο γεγονός ότι μπορείς να διαλέξεις ομοιόμορφα τη σταθερά C_1, που κρύβεται πίσω από τον συμβολισμό του μεγάλου όμικρον, για τα q της εκφώνησης. Αντιθέτως, οι συνήθεις μέθοδοι που αποδεικνύουν το Θεώρημα Πρώτων Αριθμών (και την επέκτασή του σε αριθμητικές προόδους) δεν είναι εφικτό να εξαλείψουν την εξάρτηση από το q για το C_1.

Πρόταση 5 (Bombieri-Vinogradov, ειδική περίπτωση): Υπάρχει θετική σταθερά J ώστε, για επαρκώς μεγάλα x, να υπάρχει ακέραιος $s_x \in [\sqrt{\log x}, e^{\sqrt{\log x}}]$ με

$$\sum_{\substack{q\leq x^{\frac{2}{5}} \\ s_x \nmid q}} \max_{2\leq t\leq x} \max_{(a,q)=1} \Big|\pi(t;q,a) - \frac{\pi(t)}{\phi(q)}\Big| \leq \frac{x}{e^{J\sqrt{\log x}}}$$

Απόδειξη: Ξεφεύγει αρκετά από τα πλαίσια αυτής της εργασίας, γι' αυτό και παραλείπεται. Η απόδειξη του «αυθεντικού» Bombieri-Vinogradov βρίσκεται στο [6], Κεφάλαιο 28. ■

Κεφάλαιο 2

Η κατασκευή των συνόλων $\mathbf{P}_n$

Συνεχίζουμε την περιπλάνηση μας, επικεντρωμένοι από τούδε και στο εξής στη δημοσίευση του Larsen. Θα κατασκευάσουμε «κατάλληλα» (προβιβάσιμα) σύνολα πολυωνύμων, έτσι ώστε το πλήθος των φυσικών αριθμών, σε καθέναν από τους οποίους ορισμένα (σε πλήθος, ενδεχομένως διαφορετικά για κάθε φυσικό) πολύωνυμα λαμβάνουν την τιμή κάποιου πρώτου, να είναι «αρκετά μεγάλο» (Θέωρημα 3).

Έπειτα με την βοήθεια ενός συνόλου «ξεχωριστών» πρώτων (**Q**) και διάφορες τροποποιήσεις στη μορφή των «κατάλληλων» συνόλων, για λόγους που θα γίνουν πιθανόν πιο ευκρινείς στο επόμενο κεφάλαιο, καταλήγουμε σε κάποια αρεστά σύνολα ζευγών πρώτων ($\mathbf{P}_n$), χάρη στα οποία θα χτιστούν οι αριθμοί Carmichael που ψάχνουμε.

1. Προβιβάσιμα σύνολα

Σε αυτό το σημείο θα είμαστε κάπως περιγραφικοί, μιας και η δουλειά που απαιτείται για την απόδειξη του Λήμματος 1, δε θα μας φανεί χρήσιμη σε κάποιο άλλο σημείο της εργασίας μας. Καταρχάς, ας δώσουμε έναν βασικό ορισμό.

Ορισμός (Πολλαπλασιαστικές Συναρτήσεις): Μία συνάρτηση $f : \mathbb{N} \to \mathbb{C}$ καλείται πολλαπλασιαστική αν

1. $f(1) = 1$

2. $f(mk) = f(m)f(k)$, όποτε $(m, k) = 1$.

Παραδείγματα πολλάπλασιαστικών συναρτήσεων αποτελούν η $s_a(m) = m^a$, η $\sigma_a(m) = \sum_{d|m} d^a$, η συνάρτηση ϕ του Euler και πολλές άλλες.

Ζωτικής σημασίας ρόλο στην μελέτη των πολλαπλασιαστικών συναρτήσεων, παίζει η συνάρτηση Möbius μ, η οποία ορίζεται ως εξής:

$$\mu(m) = \begin{cases} 1 \quad \text{για} \quad m = 1 \\ (-1)^r \quad \text{για} \quad m \quad \text{ελεύθερο τετραγώνων με r παράγοντες} \\ 0 \quad \text{σε κάθε άλλη περίπτωση} \end{cases}$$

Επίσης μπορούμε να ορίσουμε το γινόμενο Dirichlet δύο πολλαπλασιαστικών συναρτήσεων f, g ως:
$(f * g)(m) = \sum_{d|m} f(d)g(\frac{m}{d})$,
μέσω του οποίου βλέπουμε τις πολλαπλασιαστικές συναρτήσεις ως μία (αβελιανή) ομάδα εφοδιασμένη με πράξη ακριβώς το γινόμενο αυτό.
Κάπου εδώ αρχίζει να διαφαίνεται και η σημασία της συνάρτησης Möbius η οποία «προσφέρει» έναν κατάλληλο τύπο αντιστροφής για κάθε πολλαπλασιαστική συνάρτηση.

Πέραν αυτού όμως, η σημασία της εισαγωγής της συνάρτησης Möbius για εμάς έγκειται στην παρακάτω ταυτότητα, που μας «λύνει» συχνά τα χέρια σε υπολογισμούς:
$\sum_{d|m} \mu(d)f(d) = \prod_{p|m}(1 - f(p))$.
Η απλούστερη απόδειξη αυτής γίνεται με πολλαπλασιαστική αρχή, μιας και για κάθε p με $p \mid m$ κάθε διαιρέτης του m είτε θα διαιρείται (συντελεστής $\mu(p)f(p) = -f(p)$) είτε δε θα διαιρείται (συντελεστής 1) απ'τον p.

Πριν περάσουμε στην απόδειξη του Λήμματος 1, κάτι τελευταίο που πρέπει να τονιστεί είναι η μέθοδος της υπερβολής του Dirichlet ή μάλλον μία «ήπια» μορφή της, η οποία μας λέει ότι για πολλαπλασιαστικές συνάρτησεις f, g μπορούμε να κάνουμε το εξής:
$\sum_{m \le x} \sum_{d|m} f(d)g(\frac{m}{d}) = \sum_{d \le x} f(d) \sum_{m \le \frac{x}{d}} g(m)$

Λήμμα 1: $\sum_{k \le x} \frac{1}{\phi(k)} = O(\log x)$

Απόδειξη: Υποψιαζόμαστε, επειδή και τα μερικά αθροίσματα της αρμονική σειράς έχουν ένα παρεμφερές άνω φράγμα, ότι κάπως πρέπει να τα συνδέσουμε.

Παρατηρούμε αρχικά ότι $\phi(k) \ge \sqrt{\frac{k}{2}}$.

Αυτό προκύπτει άμεσα για $k = 1$. Για $a \in \mathbb{Z}$ τ.ω. $a \ge 2$ και για κάθε περιττό πρώτο p, έχουμε $\phi(p^a) = p^{a-1}(p-1) \ge p^{a-1} \ge p^{\frac{a}{2}}$, ενώ για $a = 1$, $\phi(3) = 2 \ge \sqrt{3}$ και $\phi(p) = p - 1 \ge 2\sqrt{p} - 2 > \sqrt{p}$ με την τελευταία ανίσωση να ισχύει για $p > 4 \Leftrightarrow p \ge 5$, δηλαδή τελικά $\phi(p^a) \ge \sqrt{p^a}$ για κάθε $a \in \mathbb{Z}_+$ και κάθε περιττό πρώτο.

Από την άλλη πλευρά, για κάθε $a \in \mathbb{Z}_+$ έχουμε: $\phi(2^a) = 2^{a-1} = \frac{2^a}{2} \geq \sqrt{\frac{2^a}{2}}$.
Συνεπώς για $k \geq 2 \Leftrightarrow k = \prod_{i=1}^{r} p_i^{a_r}$ όπου $p_i \neq p_j$ για $i \neq j$, $a_i \in \mathbb{Z}_+$, αν k περιττός, $2 \neq p_i$ για κάθε i και βρίσκουμε ότι $\phi(k) = \prod_{i=1}^{r} \phi(p_i^{a_i}) \geq \prod_{i=1}^{r} \sqrt{p_i^{a_i}} = \sqrt{\prod_{i=1}^{r} p_i^{a_r}} = \sqrt{k}$,
ενώ αν k άρτιος, κάποιο p_i θα είναι ίσο με 2, έστω το p_1, οπότε, όπως πριν,

$\phi(k) = \phi(2^{a_1}) \prod_{i=2}^{r} \phi(p_i^{a_i}) \geq \sqrt{\frac{2^{a_1}}{2}} \prod_{i=2}^{r} \sqrt{p_i^{a_i}} = \frac{1}{\sqrt{2}} \sqrt{2^{a_1} \prod_{i=2}^{r} p_i^{a_r}} = \sqrt{\frac{k}{2}}$,
η οποία, ως ασθενέστερη ανισότητα, προφανώς χαρακτηρίζει όλα τα k.

Έστω τώρα $g(k) = \frac{\mu(k)}{\phi(k)}$. Τότε η g είναι πολλαπλασιαστική, ώς γινόμενο πολλαπλασιαστικών συναρτήσεων, οπότε μπορούμε να εφαρμόσουμε σε αυτή την ταυτότητα με την συνάρτηση Möbius, δηλαδή θα βρούμε:

$$\sum_{d|k} \frac{\mu(d)^2}{\phi(d)} = \sum_{d|k} \mu(d) g(d) = \prod_{p|k} \left(1 - \frac{\mu(p)}{\phi(p)}\right) = \prod_{p|k} \left(1 + \frac{1}{p-1}\right) = \prod_{p|k} \frac{p}{p-1} =$$
$$\prod_{p|k} \frac{1}{1-\frac{1}{p}} = \frac{k}{k \prod_{p|k} (1-\frac{1}{p})} = \frac{k}{\phi(k)} \text{ και άρα}$$

$$\frac{1}{\phi(k)} = \sum_{d|k} \frac{1}{d} \frac{\mu(\frac{k}{d})^2}{\frac{k}{d}\phi(\frac{k}{d})}.$$

Συνεπώς, από την μέθοδο την οποία αναφέραμε πριν το λήμμα, θα έχουμε:

$$\sum_{k \leq x} \frac{1}{\phi(k)} = \sum_{d|k} \sum_{d|k} \frac{1}{d} \frac{\mu(\frac{k}{d})^2}{\frac{k}{d}\phi(\frac{k}{d})} = \sum_{d \leq x} \frac{1}{d} \sum_{k \leq \frac{x}{d}} \frac{\mu(k)^2}{k\phi(k)} \leq \sum_{d \leq x} \frac{1}{d} \sum_{k=1}^{\infty} \frac{\mu(k)^2}{k\phi(k)} \leq \sum_{d \leq x} \frac{1}{d} \sum_{k=1}^{\infty} \frac{\sqrt{2}}{k\sqrt{k}} =$$
$O(logx)$, όπως θέλαμε, με την πρώτη ανισότητα να ισχύει μιας και όλοι οι όροι του αθροίσματος είναι θετικοί. ■

Σχόλιο: Μιας και αναφέραμε την ανισότητα $\phi(k) \geq \sqrt{\frac{k}{2}}$, αξίζει να σημειώσουμε ότι ισχύει κάτι πολύ ισχυρότερο:

Για κάθε δ με $0 < \delta < 1$ η συνάρτηση: $\frac{\phi(k)}{k^{1-\delta}}$ τείνει στο άπειρο καθώς το k τείνει στο άπειρο.

Αυτό είναι το Θεώρημα 327 στην σελίδα 267 στο [8]. Μάλιστα, όπως έδειξε ο Ramanujan, η συνάρτηση αυτή δέχεται ελάχιστο όταν το k είναι πρωτοπαραγοντικό, αν ευσταθεί αυτός ο όρος (δηλαδή είναι κάποιο γινόμενο διαδοχικών πρώτων, με αρχικό πρώτο το 2).

Ορισμός (Προβιβάσιμα Σύνολα): Έστω $\{P_i(x) : 1 \leq i \leq m\}$ ένα σύνολο με m στο

πλήθος πρωτοβάθμια πολυώνυμα με ακέραιους συντελεστές και έστω $P(x)$ το γινόμενο τους. Αν δεν υπάρχει πρώτος p τ.ω. $\forall x \in \mathbb{Z}$ να έχουμε $p \mid P(x)$, τότε λέμε ότι το σύνολο αυτό είναι προβιβάσιμο (admissible).

Κάνουμε την σύμβαση η απροσδιόριστη από εδώ και πέρα να συμβολίζεται με κάποιο γράμμα που να παραπέμπει σε φυσικό, ακριβώς διότι μας ενδιαφέρουν μόνο οι τιμές των πολυωνύμων σε αυτούς.

Διατυπώνουμε τώρα την παρακάτω πρόταση, της οποίας η απόδειξη ξεφεύγει εντελώς από τις (τωρινές) δυνατότητες του γραφόντος:

Πρόταση 6 (Maynard[13]): α) Έστωσαν $\alpha > 0$, $0 < \theta < 1$, $\mathcal{A}$ ένα σύνολο ακεραίων, $\mathcal{P}$ ένα σύνολο πρώτων, $\mathcal{L} = \{L_1, .., L_m\}$ ένα προβιβάσιμο σύνολο και h, x ακέραιοι. Έστω επίσης ότι $L_i(k) = a_i k + b_i$ με $0 < a_i, b_i \leq x^\alpha$ για κάθε $1 \leq i \leq m$ και $m \leq (\log x)^\alpha$ καθώς και $1 \leq h \leq x^\alpha$.
Τότε υπάρχει σταθερά $c = c(\alpha, \theta)$, έτσι ώστε το ακόλουθο να ισχύει: Αν $m \geq c$ και η εξάδα $(\mathcal{A}, \mathcal{L}, \mathcal{P}, h, x, \theta)$ ικανοποιεί τις εξής 3 απαιτήσεις:

1. $\mathcal{A}$ είναι καλώς κατανεμημένο σε αριθμητικές προόδους, δηλαδή

$$\sum_{q \leq x^\theta} \max_a \left| \#\mathcal{A}(x; q, a) - \frac{\#\mathcal{A}(x)}{q} \right| = O\Big(\frac{\#\mathcal{A}(x)}{(\log x)^{100m^2}} \Big)$$

2. Οι πρώτοι στο $L(\mathcal{A}) \cap \mathcal{P}$ είναι καλώς κατανεμημένοι στις περισσότερες αριθμητικές προόδους, δηλαδή $\forall L \in \mathcal{L}$ θα έχουμε:

$$\sum_{\substack{q \leq x^\theta \\ (q,h)=1}} \max_{(L(a),q)=1} \left| \#\mathcal{P}_{L,\mathcal{A}}(x; q, a) - \frac{\#\mathcal{P}_{L,\mathcal{A}}(x)}{\phi_L(q)} \right| = O\Big(\frac{\#\mathcal{P}_{L,\mathcal{A}}(x)}{(\log x)^{100m^2}} \Big)$$

3. Το $\mathcal{A}$ δεν είναι υπερσυγκεντρωμένο σε καμία αριθμητική πρόοδο, δηλαδή για κάθε $q < x^\theta$

$\#\mathcal{A}(x; q, a) = O(\frac{\#\mathcal{A}(x)}{q})$

όπου $\mathcal{A}(x) = \{k \in \mathcal{A} : x \leq k \leq 2x\}$, $\mathcal{A}(x; q, a) = \{k \in \mathcal{A}(x) : k \equiv a(\mod q)\}$,
$L(\mathcal{A}) = \{L(m) : m \in \mathcal{A}\}$, $\phi_{L_i}(q) = \frac{\phi(a_i q)}{\phi(a_i)}$, $\mathcal{P}_{L,\mathcal{A}}(x) = \mathcal{P} \cap L(\mathcal{A}(x))$,
$\mathcal{P}_{L,\mathcal{A}}(x; q, a) = L(\mathcal{A}(x; q, a)) \cap \mathcal{P}$

και υπάρχει $\sigma > (\log m)^{-1}$ τέτοιο ώστε

$\frac{1}{m}\frac{\phi(h)}{h}\sum_{L\in\mathcal{L}}\frac{\phi(a_i)}{a_i}\#\mathcal{P}_{L,\mathcal{A}}(x)\geq\sigma\frac{\#\mathcal{A}(x)}{\log x}$, τότε

$\#\{k\in\mathcal{A}(x):\#(\{L_1(k),...,L_m(k)\}\cap\mathcal{P})\geq c^{-1}\sigma\log m\}=\Omega(\frac{\#\mathcal{A}(x)}{(\log x)^m\exp(cm)})$

β) Για κάθε $\mu\in\mathbb{N}$ και $\delta>0$, υπάρχει θετικός ακέραιος $K=K_\mu\leq\exp\{C'\mu\}$
(C' σταθερά) τ.ω. για $x>x_0(\delta,\mu)$ και $x^{\frac{7}{12}}\leq y\leq x$ και κάθε προβιβάσιμο σύνολο $\mathcal{L}=\{L_1,...,L_K\}$, όπου $L_i(k)=a_ik+b_i$ με $a_i=O((\log x)^{\frac{1}{\delta}})$ και $b_i=O(x)$, να έχουμε:

$\#\{x\leq k<x+y:\#\{i:P_i(k)\in\mathbb{P}\}\geq\mu\}=\Omega(\frac{y}{(\log x)^K})$.

Απόδειξη: Παραλείπεται. Το α) συνεπάγεται το β). ■

Θεώρημα 3: Για κάθε $\mu\in\mathbb{N}$ και $\delta>0$, υπάρχει θετικός ακέραιος $K=K_\mu$ τ.ω. για κάθε προβιβάσιμο σύνολο $\mathcal{W}=\{P_i(k):1\leq i\leq K\}=\{a_ix+b_i:1\leq i\leq K\}$, όπου $a_i>b_i>0$ για κάθε i, να ισχύει: $\#\{x\leq k<2x:\#\{i:P_i(k)\in\mathbb{P}\}\geq\mu\}\geq\frac{x}{(\log x)^K}$ για $x>x_0(\delta,\mu)$.

Μάλιστα η παραπάνω ανισότητα ισχύει για κάθε ζεύγος (x,d_+), το οποίο ικανοποιεί τις ακόλουθες ιδιότητες:
1. x επαρκώς μεγάλο σε σχέση με τα μ,δ
2. $d_+\geq a_i$ για κάθε i
3. $\log x\geq(\log d_+)^{2+\delta}$
4. Το s_{2xd_+} έχει πρώτο παράγοντα που δεν διαιρεί κανένα από τα a_i.

Σκίτσο Απόδειξης: Είναι πόρισμα της παραπάνω πρότασης για $\mathcal{L}=\mathcal{W}$, $\mathcal{P}=\mathbb{P}$, $\mathcal{A}=\mathbb{N}$, $\alpha=1$, $\theta=\frac{1}{3}$ και $\sigma=\frac{1}{6}$, με το h να είναι ο πρώτος παράγοντας του s_{2xd_+} που δεν διαιρεί κανένα εκ των a_i. Παρατηρήστε ότι σε σχέση με το φανερά γενικότερο β) της προηγούμενης πρότασης, διαλέγουμε συγκεκριμένο y ($y=x$), το οποίο μας επιτρέπει να πάρουμε το θ αρκετά μεγαλύτερο σε σχέση με το αντίστοιχο ($\theta<\frac{1}{30}$) με το οποίο δούλεψε ο Maynard, γι' αυτό και χρειάζεται να εργαστούμε αναλόγως. Επιπλέον, σε αντίθεση με το γενικότερο θεώρημα του Maynard, στο θεώρημα μας δεν υπάρχει σχέση εξάρτησης μεταξύ των K και x μόλις σταθεροποιήσουμε τα δ και μ, συνεπώς μπορούμε να υποθέτουμε πάντα ότι το x γίνεται εξαιρετικά μεγάλο, χωρίς να επηρεάζει αυτό την τιμή του K.

Να σημειώσουμε εδώ ότι αν έχουμε αποδείξει κάτι της μορφής

Ποσότητα που μας ενδιαφέρει $\geq c\frac{x}{(logx)^{K'}}$, για $c<1$ και $K'>0$, τότε μπορούμε να διαλέξουμε $K>K'$, έτσι ώστε

Ποσότητα που μας ενδιαφέρει $\geq\frac{x}{(logx)^K}$.

Το 2ο σκέλος προκύπτει από την αποδείξη της ανωτέρω πρότασης (είναι αποτέλεσμα της μεθόδου Goldston-Pintz-Yildirim για τον εντοπισμό πρώτων μέσω κατάλληλου κό-

σκινου).

Μετά από αυτήν την παρένθεση, ας μπούμε τώρα στο ψητό. Βλέπουμε ότι οι περιορισμοί που δίνονται στην αρχή για την εξάδα, ικανοποιούνται. Από τις υπόλοιπες τέσσερις «βαριές» απαιτήσεις, οι δύο εύκολα βγαίνουν αληθείς:

$$\sum_{q\le x^{\theta}} \max_{e} \big|\#\mathbb{N}(x;q,e) - \frac{\#\mathbb{N}(x)}{q}\big| \le \sum_{q\le x^{\theta}} 1 = x^{\theta} = O\Big(\frac{\#\mathbb{N}(x)}{(\log x)^{100m^2}}\Big)$$

$$\#\mathbb{N}(x;q,e) \le \lfloor \frac{x}{q} \rfloor + 1 = O\Big(\frac{\#\mathbb{N}(x)}{q}\Big).$$

Έστω για $1 \le i \le K$, ότι

$\rho_i(x;q,e) = \#\{a_i k + b_i \in \mathbb{P} : x \le k < 2x,\ k \equiv e(\mod q)\}$ και

$\rho_i(x) = \#\{a_i k + b_i \in \mathbb{P} : x \le k < 2x\}$.

Θα δείξουμε τις άλλες δύο απαιτήσεις:

1. $$\sum_{\substack{q\le x^{\frac{1}{3}}\\(q,h)=1}} \max_{(a_i e+b_i,q)=1} \big|\rho_i(x;q,e) - \rho_i(x)\frac{\phi(a_i)}{\phi(a_i q)}\big| = O\Big(\frac{\rho_i(x)}{(\log x)^{100m^2}}\Big).$$

2. $\dfrac{\phi(h)}{h}\dfrac{\phi(a_i)}{a_i}\rho_i(x) \ge \dfrac{x}{6\log x}$ (στην πραγματικότητα θα αρκούσε να δείξουμε ότι για τον μέσο όρο αυτών των K όρων, ισχύει αυτό το φράγμα),

Σταθεροποιούμε το i για το οποίο θα αποδείξουμε τις (1) και (2) και έστω

$$\Theta = \sum_{\substack{q\le x^{\frac{1}{3}}\\(q,h)=1}} \max_{(a_i e+b_i,q)=1} \big|\rho_i(x;q,e) - \rho_i(x)\frac{\phi(a_i)}{\phi(a_i q)}\big|.$$

Συμφωνούμε, παμψηφεί θέλω να πιστεύω, στην παράβλεψη των δείκτων για ευχέρεια στην δακτυλογράφηση.

Σε πρώτη φάση, ας προσπαθήσουμε να γράψουμε το $\rho(x;q,e)$ σε μια πιο «φιλική για τον χρήστη» μορφή. Αυτό μετράει το πλήθος των πρώτων της μορφής $a(e+mq)+b$ με $x \le e+mq < 2x \Leftrightarrow ax+b \le a(e+mq)+b < 2ax+b \Leftrightarrow ax < a(e+mq)+b < 2ax$ με την τελευταία ισοδυναμία να ισχύει διότι $0 < b < a$. Μα αυτό το πλήθος είναι ακριβώς το $\pi(2ax;aq,ae+b) - \pi(ax;aq,ae+b)$, δηλαδή

$\rho(x;q,e) = \pi(2ax;aq,ae+b) - \pi(ax;aq,ae+b)$,

και με την ίδια ακριβώς λογική:

$\rho(x) = \pi(2ax; a, b) - \pi(ax; a, b)$. Συνεπώς

$$\Theta = \sum_{\substack{q\le x^{\frac{1}{3}}\\(q,h)=1}} \max_{(ae+b,q)=1} \Big|\pi(2ax; aq, ae+b) - \pi(ax; aq, ae+b) - \frac{\phi(a)}{\phi(aq)}(\pi(2ax; a, b) -$$

$$\pi(ax; a, b))\Big| \le \sum_{\substack{q\le x^{\frac{1}{3}}\\(q,h)=1}} \max_{(f,aq)=1} \Big|\pi(2ax; aq, f) - \pi(ax; aq, f) - \frac{\phi(a)}{\phi(aq)}(\pi(2ax; a, b) - \pi(ax; a, b))\Big|,$$

με την τελευταία ανισότητα να ισχύει, διότι το μέγιστο αφορά κάποιο υπερσύνολο του αρχικού συνόλου, αφού $(ae + b, a) = (b, a) = 1$ από την προβιβασιμότητα του $\mathcal{W}$.

Από τριγωνική ανισότητα έχουμε:

$|\pi(ax; aq, f) - \frac{\phi(a)}{\phi(aq)}\pi(ax; a, b)| \le |\pi(ax; aq, f) - \frac{\pi(ax)}{\phi(aq)}| + \frac{\phi(a)}{\phi(aq)}|\pi(ax; a, b) - \frac{\pi(ax)}{\phi(a)}| =$
$E(ax; aq, f) + \frac{\phi(a)}{\phi(aq)}E(ax; a, b)$
και μία όμοια ανισότητα ισχύει αν στη θέση του ax βάλουμε το $2ax$, οπότε:

$$\Theta \le \sum_{\substack{q\le x^{\frac{1}{3}}\\(q,h)=1}} \max_{(f,aq)=1} \Big(E(2ax; aq, f) + E(ax; aq, f) + \frac{\phi(a)}{\phi(aq)}(E(2ax; a, b) + E(ax; a, b))\Big) \le$$

$$\sum_{\substack{q\le x^{\frac{1}{3}}\\(q,h)=1}} \max_{(f,aq)=1} \Big(E(2ax; aq, f) + E(ax; aq, f)\Big) + (E(2ax; a, b) + E(ax; a, b)) \sum_{\substack{q\le x^{\frac{1}{3}}\\(q,h)=1}} \frac{\phi(a)}{\phi(aq)} \le$$

$$\sum_{\substack{q\le ax^{\frac{1}{3}}\\(q,h)=1}} \max_{(f,q)=1} \Big(E(2ax; aq, f) + E(ax; aq, f)\Big) + (E(2ax; a, b) + E(ax; a, b)) \sum_{q\le x^{\frac{1}{3}}} \frac{1}{\phi(q)},$$

με την τελευταία ανισότητα να ισχύει διότι h, από υπόθεση, σχετικά πρώτο με το a (με τις υποθέσεις μας η άθροιση στα q συνεχίζει «ατάραχη», δοκιμάστε πχ $a = 4, h = 2, x = 1$ για να δείτε ότι η ανισότητα αποτυγχάνει σε διαφορετική περίπτωση) και $0 < \frac{\phi(a)}{\phi(aq)} \le \frac{1}{\phi(q)}$.

Παρατηρώντας ότι $(q, h) = 1 \Rightarrow h \nmid q \Rightarrow s_{2xd_+} \nmid q$, για z τ.ω. $x \le z \le 2x$ θα έχουμε:

$$E(az; a, b) \le \sum_{\substack{q\le ax^{\frac{1}{3}}\\(q,h)=1}} \max_{(e,q)=1} E(az; q, e) \le \sum_{\substack{q\le ax^{\frac{1}{3}}\\s_{2xd_+}\nmid q}} \max_{(e,q)=1} E(az; q, e) \le \sum_{\substack{q\le (2xd_+)^{\frac{2}{5}}\\s_{2xd_+}\nmid q}} \max_{(e,q)=1} E(az; q, e) \le$$

$$\sum_{\substack{q\le (2xd_+)^{\frac{2}{5}}\\s_{2xd_+}\nmid q}} \max_{2\le t\le 2xd_+} \max_{(e,q)=1} E(t; q, e) \le \frac{2xd_+}{e^{J\sqrt{\log(2xd_+)}}} \le \frac{2x}{e^{J\sqrt{\log x} - (\log x)^{\frac{1}{2+\delta}}}} = O\Big(\frac{x}{(\log x)^{100m^2+1}}\Big),$$

όπου η 1η ανισότητα ισχύει επειδή στο δεύτερο άθροισμα το q μπορεί να πάρει την τιμή a, την 2η την εξηγήσαμε παραπάνω, η 3η ισχύει για x επαρκώς μεγάλο και η 5η ισχύει από την πρόταση 5.

Σουλουπώνοντας την δουλειά μας, τελικά, με χρήση του Λήμματος 1, θα έχουμε:

$$\Theta \leq \sum_{\substack{q\leq ax^{\frac{1}{3}}\\(q,h)=1}} \max_{(f,q)=1} \Big(E(2ax;aq,f)+E(ax;aq,f)\Big)+(E(2ax;a,b)+E(ax;a,b)) \sum_{q\leq x^{\frac{1}{3}}} \frac{1}{\phi(q)} =$$

$$O\Big(\frac{x}{(\log x)^{100m^2+1}}\Big)+O\Big(\frac{x}{(\log x)^{100m^2+1}}\Big)+O\Big(\log x\Big(\frac{x}{(\log x)^{100m^2+1}}+\frac{x}{(\log x)^{100m^2+1}}\Big)\Big) =$$

$O\Big(\frac{x}{(\log x)^{100m^2}}\Big)$, και τελειώσαμε (επιτέλους) με την μία απαίτηση.

Για το 2, παρατηρούμε ότι:

$\rho(x) = \pi(2ax;a,b)-\pi(ax;a,b) = \frac{\pi(2ax)}{\phi(a)}-(\frac{\pi(2ax)}{\phi(a)}-\pi(2ax;a,b))-\frac{\pi(ax)}{\phi(a)}-(\pi(ax;a,b)-\frac{\pi(ax)}{\phi(a)}) \geq \frac{\pi(2ax)-\pi(ax)}{\phi(a)} - E(2ax;a,b) - E(ax;a,b) \geq \frac{ax}{2\phi(a)\log x} - O(\frac{x}{(\log x)^{100N^2+1}}) \geq \frac{ax}{3\phi(a)\log x}$, για πολύ μεγάλα x, όπου στην 2η ανισότητα χρησιμοποιήθηκε το ΘΠΑ.

Τέλος, αφού h πρώτος, $\phi(h) = h-1 \geq \frac{h}{2}$, οπότε συγκεντρωτικά:

$\frac{\phi(h)}{h}\frac{\phi(a)}{a}\rho(x) \geq \frac{x}{6\log x}$, δηλαδή οι 2 απαιτήσεις εδείχθησαν. ■

Σχόλιο: Σε μια εύλογη εσωτερική φιλοσοφική αναζήτηση, μπορεί κάποιος να αναρωτηθεί προς τι όλη αυτή η «μανία» με την προσέγγιση φαινομενικά περίπλοκων εκφράσεων της μορφής

$\frac{1}{\phi(q)} \sum_{\substack{m\leq x\\ m\equiv a(\mod q)}} f(m)$. Αυτά μπορούμε να φανταστούμε ότι αντιστοιχούν στο

$\frac{1}{\phi(q)} \sum_{\chi} \overline{\chi}(a) \sum_{\substack{m\leq x\\ m\equiv a(\mod q)}} \chi(m)f(m)$ και, κατα μία έννοια, «μετρούν» την απόκλιση της συνεισφοράς του κύριου χαρακτήρα σε σχέση με τους υπόλοιπους. Αυτή η απόκλιση (αποδεικνύεται ότι) σχετίζεται με το ότι αν η σειρά Dirichlet $\sum f(m)m^{-s}$ συγκλίνει στο $\{s\in\mathbb{C} : \mathrm{Re}(s) > a\}$ και εμφανίζει πόλο στο σύνορο, στην οποία περίπτωση η προσθήκη ένος μη-κύριου χαρακτήρα συχνά απαλείφει τον πόλο και η σειρά Dirichlet $\sum \chi(m)f(m)m^{-s}$ συγκλίνει στο $\{s\in\mathbb{C} : \mathrm{Re}(s) > a-\delta\}$ για κάποιο $\delta > 0$.

Το Θεώρημα 3 αποτελεί τον ακρογωνιαίο μας λίθο για τον εντοπισμό πρώτων σε προβιβάσιμα σύνολα. Για να το εφαρμόσουμε, ωστόσο, πρέπει πρώτα να βρούμε «κομψά» προβιβάσιμα σύνολα, δηλαδή, σύνολα τα οποία να ικανοποιούν τις προϋποθέσεις του Θεωρήματος και για τα οποία να μπορούμε να αδράξουμε λ.χ. παραπάνω ιδιότητες από την ίδια την δομή των a_i ή ακόμα-ακόμα και από την εκλογή του ίδιου του x που, σε τελευταία ανάλυση, καθορίζει το πλήθος των k που εξετάζουμε.

Παρακάτω οι προσπάθειες μας εντείνονται ώστε, σε πρώτη φάση, να βρεθεί ένα «καλό» και «μεγάλο» σύνολο πρώτων των οποίων τα (ελεύθερων τετραγώνων) πολλαπλάσια θα δημιουργήσουν αυτά τα «κομψά» προβιβάσιμα σύνολα και, σε δεύτερη φάση, θα «μετακινήσουμε» τα k (x) για λόγους (σημαίνουσας) ευκολίας.
Για την ώρα, έχουμε την εξής πρόταση:

Πρόταση 7 (Erdös[7]): Υπάρχουν σταθερές $E, \gamma > 0$ τ.ω.
$\#\{p \leq x : P^+(p-1) \leq x^{1-E}\} \geq \frac{\gamma x}{\log x}$ για επαρκώς μεγάλα x.

Σκίτσο Απόδειξης: Για την ακρίβεια, η εκδοχή που απέδειξε ο Erdös είναι η εξής:

Μπορούμε να βρούμε θετικό r τόσο μικρό ώστε
$\#\{p \leq (\log w)^{1+r} : P^+(p-1) \leq \log w\} \geq \dfrac{C_1(\log w)^{1+r}}{\log\log w}$ (για w επαρκώς μεγάλο).

Προς αυτό, έδειξε ότι *το πλήθος των πρώτων μικρότερων από* $(\log w)^{1+r}$ *οι οποίοι δεν βρίσκονται στο παραπάνω σύνολο είναι* $O(\frac{(\log w)^{1+r}}{(\log\log w)^2})$. Θυμηθείτε ότι από το ΘΠΑ γνωρίζουμε ότι το πλήθος των πρώτων $\leq (\log w)^{1+r}$ είναι σίγουρα μεγαλύτερο από $\frac{(\log w)^{1+r}}{2\log(\log w)^{1+r}} = \frac{(\log w)^{1+r}}{2(1+r)\log\log w}$.

Τώρα, γι'αυτό που είναι γραμμένο πλαγίως, ο Erdös είδε ότι για τους πρώτους αυτούς ισχύει ότι: $p-1 = qa,\ a \leq (\log w)^r$, όπου q πρώτος μεγαλύτερος από $\log w$.

Έπειτα χρησιμοποίησε το «αγνό» κόσκινο του Brun, για να αποδείξει ότι για σταθερό a το πλήθος των $p \leq s$ για τα οποία $\frac{p-1}{a}$ πρώτος είναι μικρότερο από

$C_2\dfrac{s}{a(\log\frac{s}{a})^2}\dfrac{\prod\limits_{p|a}(1-\frac{1}{p})}{\prod\limits_{\substack{p|a\\p>2}}(1-\frac{2}{p})}$, όπου C_2 θετική σταθερά,

οπότε αντικαθιστώντας όπου $s = (\log w)^{1+r}$ βρίσκουμε:

$$C_2\frac{(\log w)^{1+r}}{a(\log\frac{(\log w)^{1+r}}{a})^2}\frac{\prod\limits_{p|a}(1-\frac{1}{p})}{\prod\limits_{\substack{p|a\\p>2}}(1-\frac{2}{p})} \leq C_2\frac{(\log w)^{1+r}}{a(\log\log w)^2}\frac{\prod\limits_{p|a}(1-\frac{1}{p})}{\prod\limits_{\substack{p|a\\p>2}}(1-\frac{2}{p})} \leq$$

$$C_2\frac{(\log w)^{1+r}}{a(\log\log w)^2}\frac{\prod\limits_{p|a}(1-\frac{1}{p})(1+\frac{1}{p})}{\prod\limits_{\substack{p|a\\p>2}}(1-\frac{2}{p})(1+\frac{1}{p})} = C_2\frac{(\log w)^{1+r}}{a(\log\log w)^2}\frac{\prod\limits_{p|a}(1-\frac{1}{p^2})}{\prod\limits_{\substack{p|a\\p>2}}(1-\frac{1}{p}-\frac{2}{p^2})} \leq$$

$$C_2\frac{(\log w)^{1+r}}{a(\log\log w)^2}\frac{\prod\limits_{\substack{p|a\\p>2}}(1-\frac{1}{p})}{\prod\limits_{\substack{p|a\\p>2}}(1-\frac{1}{p}-\frac{2}{p^2})\prod\limits_{\substack{p|a\\p>2}}(1-\frac{1}{p})}=C_2\frac{(\log w)^{1+r}}{a(\log\log w)^2}\frac{1}{\prod\limits_{\substack{p|a\\p>2}}(1-\frac{2}{p(p-1)})\prod\limits_{\substack{p|a\\p>2}}(1-\frac{1}{p})}\leq$$

$$C_2\frac{(\log w)^{1+r}}{a(\log\log w)^2}\frac{1}{\prod\limits_{p>2}(1-\frac{2}{p(p-1)})\prod\limits_{\substack{p|a\\p>2}}(1-\frac{1}{p})}\leq C_3\frac{(\log w)^{1+r}}{(\log\log w)^2}\frac{1}{a\prod\limits_{\substack{p|a\\p>2}}(1-\frac{1}{p})}\leq$$

$$C_3\frac{(\log w)^{1+r}}{(\log\log w)^2}\frac{1}{a\prod\limits_{p|a}(1-\frac{1}{p})}=C_3\frac{(\log w)^{1+r}}{(\log\log w)^2}\frac{1}{\phi(a)}$$ (η ανισότητα από την οποία περνάμε από την σταθερά C_2 στην σταθερά C_3 είναι ορθή διότι η σειρά $\sum\limits_{p>2}\frac{2}{p(p-1)}$ συγκλίνει αρά και το αντίστοιχο απειρογινόμενο που αφαιρέθηκε συγκλίνει σε κάποιον μη μηδενικό πραγματικό αριθμό, από γνωστό κριτήριο), οπότε αθροίζοντας για όλα τα $a\leq(\log w)^r$, από το Λήμμα 1, έχουμε:

$$C_3\frac{(\log w)^{1+r}}{(\log\log w)^2}\sum_{i=1}^{(\log w)^r}\frac{1}{\phi(a)}\leq C_3\frac{(\log w)^{1+r}}{(\log\log w)^2}(C_4\log(\log w)^r)\leq C_5r\frac{(\log w)^{1+r}}{\log\log w}.$$

Οπότε, τελικά, το πλήθος των πρώτων που ψάχνουμε είναι τουλάχιστον $(\frac{(\log w)^{1+r}}{2(1+r)\log\log w})-(C_5r\frac{(\log w)^{1+r}}{\log\log w})=(\frac{1}{2(r+1)}-C_5r)\frac{(\log w)^{1+r}}{2\log\log w}$, το οποίο είναι πράγματι θετικό και της τάξης που θέλουμε για αρκετά μικρό r.

Αναγόμαστε τώρα στην διατύπωση της εκφώνησης θέτοντας $x^{\frac{1}{1+r}}=\log w$ απ'όπου προκύπτει ότι $1-E=\frac{1}{1+r}\Leftrightarrow E=\frac{r}{r+1}$. ■

Για το ιστορικό του θέματος, αξίζει να αναφερθεί ότι επικρατεί αρκετή ζέση στην κοινότητα για την εύρεση ενός ανώτατου φράγματος για τα E. Μια από τις εικασίες του Erdös είναι ότι το E παίρνει όλες τις τιμές στο διάστημα $(0,1)$. Προφανώς, αν δείξουμε ότι η πληθικότητα είναι αυτή που θέλουμε για κάποιο E_0, τότε σίγουρα για κάθε E τ.ω $E\leq E_0$ θα έχουμε την απαιτούμενη πληθικότητα. Σε μία αρκετά επιδραστική δημοσίευση, στην οποία μεταξύ άλλων απέδειξαν και την απειρία των αριθμών Carmichael (βλ. [1]), οι Alford, Granville και Pomerance έδειξαν ότι το σύνολο των E της Πρότασης 7 είναι ανοιχτό διάστημα χρησιμοποιώντας μία γενίκευση του θεωρήματος Siegel-Walfisz, το θεώρημα Brun-Titchmarsh.

Έπειτα από την παραπάνω ενδιαφέρουσα (για τον υποφαινόμενο, τουλάχιστον) εξιστόρηση, περνάμε τώρα στην απόδειξη της Πρότασης 8. Για S σύνολο θετικών ακεραίων συμβολίζουμε με $\mathbf{D}_S$ το $\{d:d\mid\prod\limits_{s\in S}s\}$ ενώ με rS συμβολίζουμε το $\{rs:s\in S\}$. Δίνουμε ξεχωριστή θέση στον παρακάτω ορισμό λόγω της ευρείας κλίμακας εφαρμογών στις οποίες εμφανίζεται.

Ορισμός (Λογαριθμική Διασπορά-Διάμετρος): Για ένα δοθέν (πεπερασμένο) σύνολο θετικών ακέραιων αριθμών S, η λογαριθμική διασπορά του είναι ο αριθμός
$\min_{\substack{s_1,s_2\in S\\ s_1\neq s_2}}\{|\log s_1-\log s_2|\}$, ενώ η λογαριθμική του διάμετρος είναι ο αριθμός
$\max_{s_1,s_2\in S}\{|\log s_1-\log s_2|\}$.

Από 'δω και πέρα, οποτεδήποτε βλέπουμε το σύμβολο $y=y(\epsilon)$ θα υποθέτουμε ότι είναι ένας αρκετά μεγάλος θετικός (φυσικός) αριθμός ο οποίος ικανοποιεί τα εκάστοτε ασυμπτωτικά καπρίτσια μας.

Έστω τώρα s_{2xd_+}, αυτός ο «αλλοπρόσαλος» μα πανταχούν παρών αριθμός που εμφανίζεται στο Θεώρημα 3 και την Πρόταση 5, για $x=\lceil e^{y^2+2\Delta}\rceil$, $d_+=(\prod_{\substack{\frac{y}{\log y}\leq p\leq y\\ P^+(p-1)\leq y^{1-E}}}p)^2$
και έστω p^* ο μεγαλύτερος πρώτος που τον διαιρεί (θα φανεί στη συνέχεια γιατί κάναμε αυτή την επιλογή). Ενδέχεται ο p^* να διαιρεί τον d_+ γι'αυτό και θεωρούμε τα:

$\boxed{\mathbf{Q}=\{\frac{y}{\log y}\leq p\leq y: P^+(p-1)\leq y^{1-E},\ p\neq p^*\}}$ και

$\boxed{L=\prod_{p\in\mathbf{Q}}p}$.

Αυτές οι δύο οντότητες θα συμβάλουν τα μέγιστα για την απόδειξη του Θεωρήματος 1, καθώς δίνουν μία αρκετά μεγάλη δεξαμενή πρώτων από την μία-άρα και κατ'επεκταση γινομένων πρώτων- όχι υπερβολικά μεγάλη ώστε να δημιουργεί προβλήματα, από την άλλη.

Μια εύλογη επισήμανση, σχετική με τα παραπάνω, είναι ότι:

$|\mathbf{Q}|\geq \#\{p\leq y: P^+(p-1)\leq y^{1-E}\}-\pi(\frac{y}{\log y})-1\geq \frac{\gamma y}{\log y}-\frac{2y}{\log y(\log y-\log\log y)}\geq \frac{\gamma y}{\log y}-\frac{4y}{(\log y)^2}\geq \frac{\eta y}{\log y}$,
όπου $\boxed{\gamma=2\eta}$ και η 2η ανισότητα αποτελεί συνδυασμό της Πρότασης 7 και του ΘΠΑ.

Λήμμα 2: Ισχύουν τα εξής

α) $\lim_{k\to\infty}\frac{2^{2k}}{\binom{2k}{k}}=\infty$

β)$\sum_{p\leq x}\frac{1}{p}=O(\log\log x)$ και $\sum_{p\leq x}\frac{1}{p}=\Omega(\log\log x)$

Απόδειξη: Από τον τύπο του Stirling έχουμε:

$\lim_{m\to\infty}\frac{\sqrt{2\pi m}(\frac{m}{e})^m}{m!}=1$, συνεπώς

$\lim_{k\to\infty}\frac{2^{2k}}{\binom{2k}{k}} = \lim_{k\to\infty}\frac{2^{2k}(k!)^2}{(2k)!} = \lim_{k\to\infty}\frac{2^{2k}(\sqrt{2\pi k}(\frac{k}{e})^k)^2}{\sqrt{4\pi k}(\frac{2k}{e})^{2k}} = \lim_{k\to\infty}\sqrt{k\pi} = \infty$, όπου χρησιμοποιήσαμε τις συνήθεις ιδιότητες των ορίων.

β) Πραγματικά το πιστεύω ότι αυτές οι αποδείξεις δίνονται για εμάς τους αργόσχολους που είμαστε τσακωμένοι με την θεωρία.

Για την μία κατεύθυνση έχουμε:
$\log x = \int_1^x \frac{1}{w}\mathrm{d}w \leq \sum_{m\leq x}\frac{1}{m} \leq \sum_{p\leq x}\sum_{i=1}^{\infty}\frac{1}{p^i} = \prod_{p\leq x}\frac{1}{1-\frac{1}{p}} \leq \prod_{p\leq x} e^{\frac{2}{p}} = \exp\left\{2\sum_{p\leq x}\frac{1}{p}\right\}$, όπου η πρώτη ανισότητα προκύπτει από την προσέγγιση Darboux του ολοκληρώματος με βήματα ακεραίους, η δεύτερη από το θεμελιώδες θεώρημα της Αριθμητικής, και η τρίτη από το ότι $e^{-2x} \leq 1-x$ για κάθε x με $x \in [0, \frac{1}{2}]$ (δείχνεται εύκολα με αναφορές σε ακρότατα κλπ).

Συνεπώς λογαριθμίζοντας και τα δύο μέλη και διαιρώντας δια 2 προκύπτει:

$$\frac{1}{2}\log\log x \leq \sum_{p\leq x}\frac{1}{p}.$$

Για την άλλη κατεύθυνση, παρατηρούμε ότι για θετικό ακέραιο k με $k > 4$ έχουμε:

$$(\sum_{p\leq x}\frac{1}{p})^k = \sum_{p_1,..,p_k\leq x}\frac{1}{p_1\cdots p_k}.$$

Προφανώς έχουμε: $p_1\cdots p_k \leq x^k$ και κάθε ακέραιος μικρότερος απο x^k μπορεί να γραφεί σαν γινόμενο αυτών των p_i με το πολύ $k!$ τρόπους (και μάλιστα μόνο οι ελεύθεροι τετραγώνω αριθμοί πιάνουν αυτό το άνω φράγμα). Συνεπώς

$$(\sum_{p\leq x}\frac{1}{p})^k \leq k!\sum_{m\leq x^k}\frac{1}{m} \leq k!(1+\int_1^{x^k}\frac{1}{w}\mathrm{d}w) = k!(1+k\log x) \leq k!2k\log x \leq k^k\log x$$

με την 2η ανισότητα να ισχύει πάλι από Darboux και την 4η επειδή $2k! \leq k^{k-1}$
$(2\cdot 2 < k,\ 3 \leq k, ..., k-1 \leq k,\ k \leq k$ είναι $k-1$ συγκρίσεις), οπότε θέτοντας $k = \lceil\log\log x\rceil$ και υψώνοντας εις την $\frac{1}{k}$ θα βρούμε:

$$\sum_{p\leq x}\frac{1}{p} \leq k(\log x)^{\frac{1}{k}} = \lceil\log\log x\rceil e^{\frac{\log\log x}{\lceil\log\log x\rceil}} \leq 2e\log\log x,$$
οπότε έχουμε το ζητούμενο! ■

Η επόμενη πρόταση θα χωρίσει (κάποια από) τα στοιχεία του $\mathbf{D_Q}$ σε κατάλληλα σύνολα τα οποία, όταν με το καλό (σύντομα) επικαλεστούμε το Θεώρημα 3, θα παίξουν τον ρόλο του $\{a_i\}$.

Πρόταση 8: Υπάρχει υποσύνολο του $\mathbf{D_Q}$ το οποίο μπορεί να διαμεριστεί σε $\frac{2^{|\mathbf{Q}|}}{2M}$ σύνολα στοιχείων, όπου M δύναμη του 2, καθένα εκ των οποίων έχει λογαριθμική διασπορά μεγαλύτερη του 1.

Απόδειξη: Καταρχάς, θα λέμε ότι το S έχει την ιδιότητα του μακρύ υποσυνόλου, αν κάθε υποσύνολο του $\mathbf{D}_S$ με τουλάχιστον $\frac{2^{|S|}}{2M}$ στοιχεία έχει λογαριθμική διάμετρο μεγαλύτερη του 1.

Έστω m ο μικρότερος ακέραιος για τον οποίο $\frac{2^{2m}}{\binom{2m}{m}} > 2M$ (τέτοιος υπάρχει από το Λήμμα 2). Μπορούμε να υποθέσουμε ότι το y είναι αυθαίρετα μεγάλο σε σχέση το m. Έστω $\mathbf{Q}_0$ ένα αυθαίρετο υποσύνολο του $\mathbf{Q}$ με $2m$ στοιχεία. Τότε κάθε υποσύνολο του $\mathbf{D}_{\mathbf{Q}_0}$ με τουλάχιστον $\frac{2^{|\mathbf{Q}_0|}}{2M} = \frac{2^{2m}}{2M}$ στοιχεία, περιέχει δύο στοιχεία έτσι ώστε το ένα απ'αυτά να έχει αυστηρά περισσότερους πρώτους παράγοντες από το άλλο.
Αυτό είναι έγκυρο, διότι τα στοιχεία με ακριβώς a παράγοντες είναι, από την δομή του $\mathbf{D}_{\mathbf{Q}_0}$, ακριβώς οι συνδυασμοί $\binom{2m}{a}$, για τους οποίους ξέρουμε από ένα προπτυχιακό μάθημα συνδυαστικής (ή Απειροστικού Λογισμού αν λάχει) ότι για κάθε a με $0 \leq a \leq 2m$ ισχύει:
$\binom{2m}{a} \leq \binom{2m}{m}$. Συνεπώς από την συνθήκη που έχουμε για το m προκύπτει άμεσα ο ισχυρισμός μας.
Όταν το y είναι αρκετά μεγάλο, το $\mathbf{Q}_0$ θα έχει την ιδιότητα του μακρύ υποσυνόλου, αφού αν $q_1, q_2 \in \mathbf{D}_{\mathbf{Q}_0}$, με q_1 να έχει περισσότερους παράγοντες από τον q_2, τότε $\frac{q_1}{q_2} > \frac{y}{\log y}\frac{1}{(\log y)^{2m-1}} > 1$ (ο λόγος δύο πρώτων στο $\mathbf{Q}_0$ ειναι τουλάχιστον $(\log y)^{-1}$).

Θα δείξουμε με επαγωγή ότι και το $\mathbf{Q}$ έχει την ιδιότητα του μακρύ υποσυνόλου.

Έστω λοιπόν, $\mathbf{Q}_1 = \mathbf{Q}_0 \cup \{p\}$, για κάποιο $p \in \mathbf{Q} \setminus \mathbf{Q}_0$ και $\mathbf{R}$ ένα υποσύνολο του $\mathbf{D}_{\mathbf{Q}_1}$ με τουλάχιστον $\frac{2^{|\mathbf{Q}_1|}}{2M}$ στοιχεία. Διασπάμε το $\mathbf{R}$ στα $\mathbf{R}_1 \cup (p\mathbf{R}_2)$ όπου $\mathbf{R}_1 = \mathbf{R} \cap \mathbf{D}_{\mathbf{Q}_0}$ και $\mathbf{R}_2 = (p^{-1}\mathbf{R}) \cap \mathbf{D}_{\mathbf{Q}_0}$. Τότε είτε το $\mathbf{R}_1$ είτε το $\mathbf{R}_2$ έχει τουλάχιστον $\frac{1}{2}\frac{2^{|\mathbf{Q}_1|}}{2M} = \frac{2^{|\mathbf{Q}_0|}}{2M}$ στοιχεία και είναι υποσύνολο του $\mathbf{D}_{\mathbf{Q_0}}$, άρα και αυτό θα έχει λογαριθμική διάμετρο άνω του 1 άρα και το $\mathbf{R}$. Αφού το $\mathbf{R}$ ήταν αυθαίρετο, τελικά και το $\mathbf{Q}_1$ έχει την ιδιότητα του μακρύ υποσυνόλου, οπότε προσθέτοντας, διαδοχικά, στοιχεία που δεν ανήκουν στο «τωρινό» σύνολό μας, θα καταλήξουμε στο ίδιο το $\mathbf{Q}$, δηλαδή, πράγματι, το $\mathbf{Q}$ έχει την ιδιότητα του μακρύ υποσυνόλου.

Έστω τώρα $\mathbf{D}_1$ το σύνολο που περιέχει τους μικρότερους $\frac{|\mathbf{D_Q}|}{2M}$ αριθμούς του $\mathbf{D_Q}$, $\mathbf{D}_2$ αυτό που περιέχει τους εναπομείναντες μικρότερους $\frac{|\mathbf{D_Q}|}{2M}$ αριθμούς του $\mathbf{D_Q}$,..., $\mathbf{D}_{2M}$ περιέχει τους εναπομείναντες μικρότερους $\frac{|\mathbf{D_Q}|}{2M}$ (που είναι και οι μεγαλύτεροι) αριθμούς του $\mathbf{D_Q}$. Ορίζουμε ως S_j το σύνολο που περιέχει το j-οστό στοιχείο των $\mathbf{D}_2, \mathbf{D}_4, ..., \mathbf{D}_{2M}$ (αφού είναι πεπερασμένα σύνολα μπορούμε να απαριθμήσουμε με κάποιον αυθαίρετο τρόπο τα στοιχεία τους). Αφού το $\mathbf{Q}$ έχει την ιδιότητα του μακρύ υποσυνόλου, τα $\mathbf{D}_3, \mathbf{D}_5, ..., \mathbf{D}_{2M-1}$

έχουν όλα λογαριθμική διάμετρο μεγαλύτερη του 1, και άρα τα S_j έχουν λογαριθμική διασπορά μεγαλύτερη του 1, καθότι αν d, d' δύο στοιχεία του S_j με $d > d'$, τότε, υπάρχει $\mathbf{D}_{2l+1}$, όπου $l \in \mathbb{Z}_+$, τ.ω. για κάθε $e_1, e_2 \in \mathbf{D}_{2l+1}$ να έχουμε $d > e_1 > e_2 > d'$ και άρα διαλέγοντας κατάλληλα e_1, e_2 θα έχουμε $\log d - \log d' = \log \frac{d}{d'} > \log \frac{e_1}{e_2} = \log e_1 - \log e_2 > 1$.
Εν κατακλείδι, τα S_j είναι $\frac{|\mathbf{D_Q}|}{2M}$ στο πλήθος, περιέχουν M στοιχεία και έχουν λογαριθμική διασπορά άνω του 1, άρα είναι τα σύνολα που θέλαμε. ■

Διατηρούμε προς ώρας τον συμβολισμό της Πρότασης 8 και μάλιστα τον εμπλουτίζουμε θέτοντας $S_j = \{d_{ij} : 1 \leq i \leq M\}$ για $1 \leq j \leq \frac{|\mathbf{D_Q}|}{2M}$.

Επειδή οι πρώτοι του $\mathbf{Q}$ είναι αρκετά μεγαλύτεροι από $M+1$ μπορούμε να ορίσουμε τα μη κενά σύνολα:

$C_{j,p} = \{c \in (\mathbb{Z}/p\mathbb{Z})^\times : (d_{ij}c + 1, p) = 1,\ \forall i\}$

για $p \in \mathbf{Q}$ και $1 \leq j \leq \frac{|\mathbf{D_Q}|}{2M}$, καθώς και το σύνολο

$C_j = \prod_{p \in \mathbf{Q}} C_{j,p}$ για $1 \leq j \leq \frac{|\mathbf{D_Q}|}{2M}$, το οποίο, από το Κινέζικο Θεώρημα Υπολοίπων, μπορούμε να το ταυτίσουμε με το $\mathbf{C}_j$ που είναι το σύνολο των ακεραίων $1 \leq c_j < L$ έτσι ώστε $c_j \equiv c_{j,p} (\mod p)$ για κάθε $p \in \mathbf{Q}$, όπου $c_{j,p} \in C_{j,p}$.

Παρατήρηση: $1 - \frac{|\mathbf{C}_j|}{L} \leq 1 - \prod_{p \in \mathbf{Q}} (1 - \frac{M+1}{p}) = 1 - \exp\left\{ -O(1) \sum_{p \in \mathbf{Q}} \frac{1}{p} \right\} =$

$1 - \exp\left\{ -O(1) \sum_{\frac{y}{\log y} \leq p \leq y} \frac{1}{p} \right\} = 1 - \exp\left\{ -O(1)(\sum_{p \leq y} \frac{1}{p} - \sum_{\frac{y}{\log y} \leq p} \frac{1}{p}) \right\} =$

$1 - \exp\Big\{ -O(1)(\log\log y - \log\log \frac{y}{\log y}) \Big\} = 1 - \exp\Big\{ -O(1)(\log \frac{\log y}{\log y - \log\log y}) \Big\} =$

$1 - \exp\left\{ -O(1)(\log \frac{1}{1 - \frac{\log\log y}{\log y}}) \right\} = 1 - \exp\{-o(1)\} = o(1),$

με την ανισότητα να ισχύει διότι για κάθε p οι τιμές του $c_{j,p}$ που πρέπει να αποφύγουμε είναι η μηδενική και το πολύ M ακόμα που αφορούν τον αντίθετο του πολλαπλασιαστικού αντιστρόφου καθενός εκ των d_{ij}, την 2η ισότητα να ισχύει από την Πρόταση 7 (και το ΘΠΑ), ενώ η 4η ισχύει από το Λήμμα 2.

Δειλά-δειλά τα προβιβάσιμα σύνολα επανέρχονται στο προσκήνιο.

Πρόταση 9: Για όλα τα $c_j \in \mathbf{C}_j$, το σύνολο $\{(d_{ij}L)k' + (d_{ij}c_j + 1) : 1 \leq i \leq M\}$ είναι προβιβάσιμο.

Απόδειξη: Έστω p πρώτος με $p \nmid L$. Τότε το L έχει πολλαπλασιαστικό αντίστροφο

$(\mod p)$, συνεπώς θέτοντας $k' \equiv -L^{-1}c_j(\mod p)$ θα έχουμε

$(d_{ij}L)k' + (d_{ij}c_j + 1) \equiv -d_{ij}c_j + d_{ij}c_j + 1 \equiv 1(\mod p)$ και άρα το p αποκλείεται να χαλά την προβιβασιμότητα του συνόλου.

Από την άλλη, αν $p \mid L$, τότε
$(d_{ij}L)k' + (d_{ij}c_j + 1) \equiv d_{ij}c_{j,p} + 1 \nmid (0 \mod p)$, από την κατασκευή του $\mathbf{C}_j$, οπότε και γι'αυτά τα p δεν υπάρχει θέμα, δηλαδή, πράγματι, το συνολό μας είναι προβιβάσιμο. ■

Σε αυτό το σημείο θα μπορούσε να αναρωτηθεί κάποιος γιατί δεν δουλεύουμε με κάποιο πιο απλό σύνολο όπως πχ το $\{d_{ij}k'+1 : 1 \leq i \leq M\}$. Η απάντηση είναι ότι σκεφτόμαστε «πονηρά» καθώς, το να γνωρίζουμε ότι οι πρώτοι που παίρνουμε απ'αυτό το προβιβάσιμο σύνολο είναι της μορφής $1(\mod kL)$ είναι μία πληροφορία που θα μας διευκολύνει στο εγγύς μέλλον, όταν με το καλό «αλιεύσουμε», με την αρωγή του Θεωρήματος 2, αριθμούς Carmichael που έχουν πρώτους παράγοντες αυτούς.

Ήρθε λοιπόν η ώρα για το Θεώρημα 3.
Για την σταθερά ϵ για την οποία θέλουμε να αποδείξουμε το θεώρημα (την οποία όπως τονίσαμε μπορούμε να την θεωρούμε ασύλληπτα μικρή) θέτουμε $\boxed{\Delta = \frac{\epsilon^2}{12}}$.

Γυρίζοντας πίσω στη διατύπωση του θεωρήματος αυτού θέτουμε $\boxed{\mu = 2}$, $\boxed{\delta = \Delta}$, τον K του θεωρήματος τον αντικαθιστούμε με το M, την ελάχιστη δύναμη του 2 που τον προσπερνά, τα προβιβάσιμα σύνολα μας θα είναι τα $\{(d_{ij}L)k' + (d_{ij}c_j + 1) : 1 \leq i \leq M\}$ για κάθε δείκτη j, ενώ για x διαλέγουμε $x = \boxed{Y = \lceil e^{y^{2+2\Delta}} \rceil}$ και $d_+ = (\prod_{\substack{\frac{y}{\log y} \leq p \leq y \\ P^+(p-1) \leq y^{1-E}}} p)^2$.

Παρατηρήστε ότι με αυτές τις επιλογές τα 2,4 (θυμηθείτε πως ορίσαμε το p^*) ικανοποιούνται για το ζεύγος (x, d_+) ενώ για την 3:

$e^{(\log d_+)^{2+\delta}} \leq e^{(\log(y^2L^2))^{2+\Delta}} \leq e^{(\log(y^2y^{\pi(y)}))^{2+\Delta}} \leq e^{(\log\left(y^2y^{\frac{2y}{\log y}}\right))^{2+\Delta}} \leq e^{(\log\left(y^{\frac{4y}{\log y}}\right))^{2+\Delta}} = e^{(4y)^{2+\Delta}} < e^{y^{2+2\Delta}} \leq x$, οπότε λογαριθμίζοντας προκύπτει και αυτή. Για την 1 όπως και για κάποιες πιθανές ενστάσεις του αναγνώστη για την «σταθερότητα» του x ας επαναλάβουμε, ελπίζοντας να μην γινόμαστε κουραστικοί, ότι το $K \equiv M$ έχει σταθεροποιηθεί μετά την εκλογή του μ, το x δεν εξαρτάται απ'αυτό (το K), και το ίδιο ισχύει και αντίστροφα, αφού οι τιμές του y επηρεάζουν μόνο τα προβιβάσιμα σύνολα (και όχι το μ).

Ορίζουμε (**A**, από το «αρχικό»):

$\mathbf{A}_j = \{X \leq k < 2X : (k, L) = 1$ και υπάρχουν $d, d' \in S_j$ τέτοια ώστε οι αριθμοί $dk + 1,\ d'k + 1$ να είναι πρώτοι$\}$,

$\mathbf{A} = \bigcup_{j=1}^{\frac{|\mathbf{D_Q}|}{2M}} \mathbf{A}_j \times \{j\}$ και (**T** από το «τελικό»)

$\mathbf{T}_j = \mathbf{A}_j \setminus \mathbf{B}_j,$

$\mathbf{T} = \bigcup_{j=1}^{\frac{|\mathbf{D_Q}|}{2M}} \mathbf{T}_j \times \{j\}.$

όπου $\boxed{X = YL}$ και τα $\mathbf{B}_j$ θα οριστούν ειρήσθω εν παρόδω (αφορούν την μη-συσταδοποίηση που θα δούμε στην επόμενη ενότητα).

Εφαρμόζοντας το Θεώρημα 3 για ένα σταθερο $c_j \in \mathbf{C}_j$ βρίσκουμε τουλάχιστον $\frac{Y}{(\log Y)^M}$ k' που να το ικανοποιούν και να είναι της μορφής
$Y \leq k' < 2Y \Rightarrow X \leq LY + c_j \leq Lk' + c_j < L(2Y-1) + L \leq 2X$, δηλαδή μπορούμε αυτά τα k' να τα βλέπουμε όπως τα k στα οποία αναφέρεται το $\mathbf{A}_j$ (από τον ορισμό των c_j έχουμε ότι $Lk' + c_j = k, L$ σχετικά πρώτοι). Αφού για κάθε επιλογή c_j παίρνουμε διαφορετικά k (σκεφτείτε τι συμβαίνει $\mod L$), τελικά, με χρήση και της παρατήρησης πριν την Πρόταση 9, θα έχουμε:

$|\mathbf{A}_j| \geq |\mathbf{C}_j| \frac{Y}{(\log Y)^M} = (1 - o(1)) \frac{X}{(\log Y)^M} \geq (1 - o(1)) \frac{X}{(\log X)^M}$ για κάθε δείκτη j.

2. Απόρριψη συσταδοποιημένων ζευγών

Διαισθητικά, θέλουμε να αποκλείσουμε κάποια από τα ζευγάρια που μόλις βρήκαμε, επειδή βρίσκονται πολύ κοντα σε δυνάμεις κάποιου $\alpha > 1$. Το Θεώρημα 4 θα μας δείξει πόσο μεγάλη είναι η «χασούρα» μας αν τα απωλέσουμε (θέλουμε να είναι ασυμπτωτικά μικρή σε σχέση με το πλήθος των ζευγαριών μας).

Στο πρακτικό κομμάτι, όπως το κατανοώ ο ίδιος τουλάχιστον, η ιδέα που οδήγησε στον παραπάνω αποκλεισμό σχετίζεται με τα προβλήματα που συναντά κανείς κατά την απόδειξη του Θεωρήματος 6, στο οποίο η λεγόμενη «συνθήκη μη-συσταδοποιήσης» κατέχει προεξέχουσα θέση.

Επίσης μπορείτε να σκέφτεστε, μιας και έτσι και αλλιώς κατα αυτόν τον τρόπο θα τα χρησιμοποιήσουμε, ότι τα V, W, m εξαρτώνται από το y (δεν είναι απλά «σταθερές», δείτε παρακάτω).

Ορισμός (Παραλληλία λιστών): Δύο λίστες $\{a_i : 1 \leq i \leq m\}$, $\{a'_i : 1 \leq i \leq m\}$ λέμε ότι ικανοποιούν την συνθήκη της παραλληλίας («είναι παράλληλες») αν υπάρχει $a > 1$ έτσι ώστε: $|a_i - a'_i - a| \leq \frac{1}{m}$ για κάθε i.

Ορισμός (Ομαλότητα λιστών): Μία λίστα λέμε ότι ικανοποιεί τη συνθήκη ομαλότητας αν ο αριθμός των i έτσι ώστε $|a_i - \zeta| \leq \frac{1}{m}$ είναι το πολύ 12 για κάθε ζ.

Θεώρημα 4: Έστω $C > 1$ πραγματικός αριθμός και $\{a_i : 1 \leq i \leq m\}, \{a'_i : 1 \leq i \leq m\}$ δύο λίστες πραγματικών αριθμών που βρίσκονται μεταξύ του 1 και του C οι οποίες ικανοποιούν την συνθήκη παραλληλίας. Έστω επίσης ότι η $\{a_i\}$ ικανοποιεί την συνθήκη ομαλότητας.

Τότε για κάθε $V, W > 0$ με $VW = O(m)$, το πλήθος των i για τα οποία υπάρχουν t όπου $|t| < W$ και μη μηδενικοί ακέραιοι s, s' ώστε

$|tc_i - s| \leq \frac{1}{V}$ & $|td_i - s'| \leq \frac{1}{V}$ είναι $O(\frac{C^3 W \log(CW) m}{V})$.

Απόδειξη: Για ακεραίους l, r, θεωρούμε το σύνολο $\mathbf{K}_{l,r}$ το οποίο περιέχει όλους τους δείκτες i για τους οποίους υπάρχει $|t| < W$, ώστε

$|ta_i - m| \leq \frac{1}{V}$ & $|ta'_i - r + l| \leq< \frac{1}{V}$, όπου $r, r - l$ και οι δύο μη μηδενικοί ακέραιοι. Σταθεροποιούμε τα l, r.

Αν i_1, i_2 είναι δύο δείκτες στους οποίους αντιστοιχούν t_1, t_2 με $\max\{|t_1|, |t_2|\} < W$, έτσι ώστε $|t_k a_{i_k} - r| \leq \frac{1}{V}$ & $|t_k a'_{i_k} - r + l| \leq \frac{1}{V}$ για $k \in \{1, 2\}$, τότε $|t_k(a_{i_k} - a'_{i_k}) - l| \leq \frac{2}{V}$.

Από υπόθεση, υπάρχει $a > 1$ τέτοιο ώστε $|a_i - a'_i - a| \leq \frac{1}{m}$ για κάθε i, συνεπώς:

$|t_k a - l| \leq |t_k(a_{i_k} - a'_{i_k}) - l| + |t_k||a_i - a'_i - a| \leq \frac{1}{V} + \frac{W}{m} = O(\frac{1}{V})$.

Επιπλέον, $|t_1 - t_2| \leq \frac{1}{a}|(t_1 a - l) - (t_2 a - l)| < |t_1 a - l| + |t_2 a - l| = O(\frac{1}{V})$ και

$|a_{i_1} - a_{i_2}| \leq |\frac{(t_1 a_{i_1} - r) - (t_2 a_{i_2} - r) + (t_2 - t_1) a_{i_2}}{|t_1|}| = O(\frac{1}{V|t_1|}) + O(\frac{1}{V|t_1|}) + O(\frac{a_{i_2}}{V|t_1|}) = O(\frac{a_{i_2}}{V|t_1|}) = O(\frac{a_{i_1} a_{i_2}}{V|r|}) = O(\frac{C^2}{V|r|})$, όπου χρησιμοποιήσαμε ότι $O(|t_1|) = \frac{|r|}{a_{i_1}}$.

Από την υπόθεση ομαλότητας της λίστας των a_i για κάθε $\rho \geq \frac{1}{m}$, ο αριθμός των i για τα οποία $|a_i - \zeta| \leq \rho$ είναι $O(\rho m)$ (δεν ξεκινάμε από το 0, επειδή ενδέχεται το ρ να είναι ασυμπτωτικά αρκετά μικρότερο του $\frac{1}{m}$ και να χάναμε κάποια i) για κάθε ζ.

Έστω λοιπόν $\rho = \frac{C^2}{V|r|}$. Αφού $|r| = O(a_{i_1}|t_1|) = O(CW)$, έπεται ότι $\frac{1}{m} < \frac{C}{m} = O(\frac{C}{VW}) = O(\frac{C^2}{V|r|}) = O(\rho)$.

Δηλαδή το $\mathbf{K}_{l,r}$ έχει $O(\frac{C^2 m}{V|r|})$ στοιχεία και άρα το $\mathbf{K} = \bigcup_{l,r} \mathbf{K}_{l,r}$ έχει

$$\mathbf{K} = \sum_{l=O(CW)} \sum_{\substack{r=O(CW) \\ r \neq 0}} |\mathbf{K}_{l,r}| = O(AW \sum_{\substack{r=O(CW) \\ r \neq 0}} \frac{1}{|r|} \frac{C^2 m}{V}) = O(CW \log(CW) \frac{C^2 m}{V}) =$$

$$O\Big(\frac{C^3 W \log(CW) m}{V}\Big)$$

που είναι και το ζητούμενο. ■

Μετά τους αρχικούς (δικαιολογημένους ;) ενδοιασμούς μου, πιστεύω ήρθε η ώρα να ορίσουμε το $\mathbf{B}_j$:

$\mathbf{B}_j = \{X \leq k < 2X :$ Υπάρχει t με $|t| < e^{\frac{\eta y}{(4+4\Delta)\log y}}$ και μη μηδενικοί ακέραιοι s, s' ώστε $|t\log(dk+1) - s| \leq \frac{1}{e^{\frac{\eta y}{(4+2\Delta)\log y}}}$ & $|t\log(d'k+1) - s'| \leq \frac{1}{e^{\frac{\eta y}{(4+2\Delta)\log y}}}$ όπου $d, d' \in S_j\}$

Πόρισμα 4.1: Οι προϋποθέσεις του Θεωρήματος 4 ικανοποιούνται για $C = 2\log X$, $m = X, a_i = \log(d(X+i-1)+1), a_i' = \log(d'(X+i-1)+1)$ για $1 \leq i \leq m$ και $V = e^{\frac{\eta y}{(4+2\Delta)\log y}}, W = e^{\frac{\eta y}{(4+4\Delta)\log y}}$, όπου $d > d'$ και $d, d' \in S_j$, για τυχόν j.

Συνεπώς, $|\mathbf{B}_j| = o(\frac{X}{(\log X)^M})$ για κάθε δείκτη j.

Απόδειξη: Αρχικά, παρατηρουμε ότι

$$a_i - a_i' = \log(d(X+i-1)+1) - \log(d'(X+i-1)+1) = \log\left(\frac{d(X+i-1)+1}{d'(X+i-1)+1}\right) = \log\left(\frac{d}{d'}\right) + O(\frac{1}{d'X}) = \log\frac{d}{d'} + O(\frac{1}{md'}),$$

οπότε θέτοντας $a = \log\frac{d}{d'}$, έχουμε $a > 1$ (εδώ είναι η μόνη στιγμή όπου χρησιμοποιούμε ουσιωδώς την Πρόταση 8) και $|a_i - a_i' - a| \leq \frac{1}{m}$ για κάθε i άρα οι $\{a_i\}$ και $\{a_i'\}$ είναι παράλληλες.

Έπειτα, ορίζοντας $b_i = a_{i+1} - a_i$ για $1 \leq i < n$, βρίσκουμε ότι η $\{b_i\}$ είναι φθίνουσα λίστα αριθμών για την οποία ισχύει $b_1 < 3b_{m-1}$, αφού (λόγω του γεγονότος ότι ο λογάριθμος είναι αύξουσα συνάρτηση):
$3b_{m-1} > b_1 \Leftrightarrow 3\Big(\log\Big(\frac{d(2m-1)+1}{d(2m-2)+1}\Big)\Big) > \log\Big(\frac{d(m+1)+1}{dm+1}\Big) \Leftrightarrow \Big(\frac{d(2m-1)+1}{d(2m-2)+1}\Big)^3 > \frac{d(m+1)+1}{dm+1}$ ενώ
$\Big(\frac{d(2m-1)+1}{d(2m-2)+1}\Big)^3 > \Big(\frac{d(2m-1)+1}{d(2m-2)+1}\Big)^2 = \Big(\frac{1}{2m-2+\frac{1}{d}}+1\Big)^2 \geq \frac{2}{2m-2+\frac{1}{d}} + 1 = \frac{1}{m-1+\frac{1}{2d}} + 1 > \frac{1}{m+\frac{1}{d}} + 1 = \frac{d(m+1)+1}{dm+1}.$

Επιπροσθέτως, η $\{a_i\}$ είναι αύξουσα με $a_m - a_1 > \frac{1}{2}$, καθότι για μεγάλα X (y), αυτή η διαφορά τείνει στο $\log 2$. Συνεπώς:

$\frac{1}{2m} < \frac{1}{2(m-1)} < \frac{a_m - a_1}{m-1} = \frac{\sum_{i=1}^{m-1} b_i}{m-1} < \frac{3\sum_{i=1}^{m-1} b_n}{m-1} = 3b_n$, οπότε $b_i \geq b_m > \frac{1}{6m}$ για κάθε δείκτη i. Αυτό δείχνει τη συνθήκη ομαλότητας για την $\{a_i\}$:

Εαν υπήρχε ζ τ.ω. για τουλάχιστον 13 i να είχαμε $|a_i - \zeta| < \frac{1}{2m}$, τότε τουλάχιστον 7 από τα a_i θα βρίσκονται είτε δεξιά είτε αριστερά του ζ στην πραγματική ευθεία, έστω ΧΒΓ δεξιά. Αν $i_1, ..., i_7$ οι δείκτες τους, με $i_1 < ... < i_7$, τότε αφού $\{a_i\}$ αύξουσα, $\frac{1}{m} \geq |a_{i_7} - \zeta| = a_{i_7} - \zeta = \sum_{j=1}^{6}(a_{i_{j+1}} - a_{i_j}) + a_1 - \zeta = \sum_{j=1}^{6} b_{i_j} + a_1 - \zeta > 6\frac{1}{6m} + a_1 + \zeta \geq \frac{1}{m}$, άτοπο.
Επίσης, προφανώς $VW = O(X)$.

Για το δεύτερο το μέρος, για ένα ζεύγος (d, d') ξέρουμε (το πολύ) από το θεώρημα 4 και την προηγούμενη εργασία, πόσα k χάνουμε, οπότε αφού τα ζεύγη είναι $\binom{M}{2}$ λόγω της πληθικότητας του S_j, το πολύ να χάσουμε $\binom{M}{2}$ επί το αρχικό πλήθος. Συνεπώς, λαμβάνοντας υπόψιν ότι $M = O(1)$, θα έχουμε:

$$|\mathbf{B}_j| = \binom{M}{2} O(\frac{mC^3 W \log(CW)}{V}) = O\Big(\frac{X(\log X)^3 \log X \log X}{V^{\frac{2\Delta}{4+4\Delta}}}\Big) =$$

$O\Big(\frac{X(\log X)^5}{V^{\frac{2\Delta}{4+4\Delta}}}\Big) = o\Big(\frac{X}{(\log X)^M}\Big)$, αφού $(\log X)^M = o(V)$ (λ.χ. το ένα έχει πολυωνυμική εξάρτηση ως προς το y, το άλλο εκθετική) και μόλις ολοκληρώσαμε την απόδειξη της πρότασης. ■

Από τα παραπάνω βρίσκουμε ότι $|\mathbf{T}_j| = |\mathbf{A}_j \setminus \mathbf{B}_j| \geq |\mathbf{A}_j| - |\mathbf{B}_j| = (1 - o(1))\frac{X}{(\log X)^M}$ και άρα:

$$|\mathbf{T}| = \sum_{j=1}^{\frac{|\mathbf{D_Q}|}{2M}} |\mathbf{T}_j| = (1 - o(1))\frac{X\frac{|\mathbf{D_Q}|}{2M}}{(\log X)^M}.$$

Αφού τα ζεύγη μας (k, j) είναι τόσα πολλά και οι επιλογές για το k είναι X, από την αρχή του περιστερώνα θα υπάρχει κάποιο k_0 με $X \leq k_0 < 2X$, στο οποίο να αντιστοιχούν τουλάχιστον $(1 - o(1))\frac{\frac{|\mathbf{D_Q}|}{2M}}{(\log X)^M}$ σε πλήθος j.

Τώρα, στο k_0, μπορεί να αντιστοιχούσαν πάνω από δύο πρώτοι σε κάποια j. Εξάλλου, το Θεώρημα 3 αναφέρεται σε τουλάχιστον 2 τέτοιες επιλογές. Αυτό σαφώς δε μας ενοχλεί, απλά διαλέγουμε αυθαίρετα δύο απ'αυτούς. Θέτουμε

$$\mathbf{P} = \{(p, p') : \text{ Υπάρχει } i \text{ τ.ω. } (k_0, i) \in \mathbf{T}, p = dk_0 + 1,\ p' = d'k_0 + 1,\ d, d' \in S_i, d < d'\}$$

και αριθμώντας τυχαία τα ζεύγη αυτά, και τους δείκτες των πρώτων αντιστοίχως, έστω

$$\boxed{\mathbf{P}_m = \{p_1, p_1', ..., p_m, p_m'\}}$$

$P_m = \prod_{p \in \mathbf{P}_m} p$ (με κατάχρηση συμβολισμού θα γράφουμε και $p \in \mathbf{P}$, εννοώντας ότι το p είναι συντεταγμένη ζεύγους που ανήκει στο $\mathbf{P}$).

Παρατηρήστε ότι: $|\mathbf{P}| = (1 - o(1))\frac{\frac{|\mathbf{D_Q}|}{2M}}{(\log X)^M} \geq (1 - (o(1))\frac{2^{\frac{\eta y}{\log y}}}{2M(\log X)^M} > e^{\frac{\eta y}{2\log y}}$ για αρκετά

μεγάλο y.

Με βάση την άνωθεν ασυμπτωτική προσέγγιση, για να αποδείξουμε το τελευταίο θεώρημα του κεφαλαίου, χρειάζεται να εισάγουμε τον εξής συμβολισμό:
$N_+ = \lfloor e^{\frac{\eta y}{2\log y}} \rfloor,\ \ N_- = \lceil \frac{1}{4} e^{\frac{\eta y}{2\log y}} \rceil$

$$\boxed{Z_+(y) = Y^{\frac{11}{12} e^{\frac{\eta y}{2\log y}}}, Z_-(y) = Y^{\frac{1}{3} e^{\frac{\eta y}{2\log y}}}}.$$

Θεώρημα 5: Έστω z κάποιος ακέραιος τ.ω. $z \in [Z_-(y), Z_+(y)]$. Τότε υπάρχει ακέραιος $n = n(z) \in [N_-, N_+]$ τ.ω. $|\log z - \frac{\log P_n}{2}| < \log X$

Απόδειξη: Παρατηρούμε ότι από ΘΠΑ

$L = \prod_{p \in \mathbf{Q}} p < y^{\frac{2y}{\log y}} = e^{2y} < \frac{Y^{\frac{1}{8}}}{\sqrt{2}}$ για μεγάλα y,
ενώ για κάθε $p \in \mathbf{P}$ έχουμε

$Y^{\frac{5}{4}} > 2XL > (2X-1)L + 1 \geq p = dk_0 + 1 > k_0 \geq X$, συνεπώς

$$P_{N_+} = \prod_{p \in \mathbf{P}_{N_+}} p > X^{|\mathbf{P}_{N_+}|} = X^{2\lfloor e^{\frac{\eta y}{2\log y}} \rfloor} > Y^{2\lfloor e^{\frac{\eta y}{2\log y}} \rfloor} > (Z_+(y))^2,$$

$$P_{N_-} = \prod_{p \in \mathbf{P}_{N_-}} p < (Y^{\frac{5}{4}})^{|\mathbf{P}_{N_-}|} = Y^{\frac{5}{2}\lceil \frac{1}{4} e^{\frac{\eta y}{2\log y}} \rceil} < (Z_-(y))^2,$$

$$\frac{\log P_{m+1} - \log P_m}{2} = \frac{\log\left(p_{m+1} p'_{m+1}\right)}{2} < \frac{\log(2XL)^2}{2} = \log(2XL) < 2\log X$$
για κάθε $m < N_+$. Οπότε σίγουρα τέτοιος n υπάρχει (το $2\log z$ θα βρίσκεται ανάμεσα στο $\log P_n$ και το $\log P_{n\pm 1}$). ■

Όπως είπαμε και στην αρχή του κεφαλαίου, αυτά τα σύνολα θα παίξουν καταλυτικό ρόλο για την απόδειξη του Θεωρήματος 1.

Μια άλλη χρήσιμη, όπως θα δούμε, ποσότητα είναι η

$$\boxed{b(z) = \log z - \frac{\log P_{n(z)}}{2} + \frac{1}{2e^{\frac{\eta y}{(4+6\Delta)\log y}}}}$$

Κεφάλαιο 3

Στην τελική ευθεία για την απόδειξη

Έπειτα από τις δυσκολίες που συναντήσαμε προσπαθώντας να βρούμε κατάλληλους και αρκετούς (κατα μία έννοια) πρώτους, η ένταση κλιμακώνεται για μια τελευταία φορά στην απόδειξη του Θεωρήματος 6.

Από την διατύπωση του ακόμα-ακόμα βλέπουμε αρκετές φαινομενικά αμετροεπείς προϋποθέσεις και περιορισμούς, οι οποίοι, εντούτοις, έχουν πολύ εύστοχα τοποθετηθεί εκεί από τον Larsen.

Μέσω της συνθήκης μη-συσταδοποίησης, και του κυρίαρχου ρόλου που επιτελεί αυτή στην απόδειξη, τεκμηριώνεται ως ένα βαθμό η προσπάθεια που έγινε στο Κεφάλαιο 2.

Στις συνέπειες του θεωρήματος, που αποτελούν ξεχωριστή ενότητα του Κεφαλαίου, αποσαφηνίζεται ρητά (Πόρισμα 6.1) η σύνδεση αυτή και πλέον, με κάποιες μαθηματικές «πινελιές», η απόδειξη του Θεωρήματος 1 καθίσταται δυνατή.

1. Ένα τεχνικό θεώρημα και η απόδειξή του

Ξεκινάμε υπενθυμίζοντας ορισμένα αποτελέσματα τα οποία θα επικαλεστούμε στην συνέχεια.

Λήμμα 3: Ισχύουν τα εξής:

α) $\cos x \geq 1 - \frac{x^2}{2}$ και $e^x \geq 1 + x$ για κάθε $x \in \mathbb{R}$

β) $\cos x \leq 1 - \frac{11}{24}x^2$ για $x \in [-1, 1]$, $\cos x \leq 1 - \frac{x^2}{4}$ για $x \in [-2, 2]$

γ) Έστω $a \in \mathbb{C}$ τ.ω. $|a| = 1$. Τότε $|\frac{1+a}{2}| = \sqrt{\frac{1+\mathrm{Re}(a)}{2}}$

δ) $\mathbf{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-t^2} \mathrm{d}t \leq e^{-x^2}$ και $\mathbf{erfc}(1) \leq \frac{16}{100}$

ε) $e^x \leq 1 + 2x$ για $x \in [0, 1]$

Απόδειξη: Δίνουμε απλά κάποιες υποδείξεις.

α),ε) Μελέτη παραγώγων-ακρότατων...

β) Κάνοντας ανάλογη δουλειά με το α) έχουμε ότι $\cos x \leq 1 - \frac{x^2}{2} + \frac{x^4}{24}$ για κάθε $x \in \mathbb{R}$ και επειδή $x \in [-1, 1]$ ($x \in [-2, 2]$, αντίστοιχα), θα έχουμε
$x^4 \leq x^2$ ($x^4 \leq 6x^2$, αντίστοιχα), οπότε...

γ) Υψώνουμε στο τετράγωνο...

δ) Στο διάστημα $[x, +\infty]$ η ολοκληρωτέα ποσότητα είναι μικρότερη ή ίση του e^{-x^2}. Το φράγμα στο σημείο 1 έγινε με χρήση σχετικών πινάκων. ■

Θεώρημα 6: Έστω $\{q_1, q_2, ..., q_N\}$ ένα σύνολο πρώτων που έχουν γινόμενο R και έστω q_0 ο μεγαλύτερος απ'αυτούς. Υποθέστε ότι $q_i^2 \geq q_0$ για κάθε i.
Έστω l κάποιος θετικός ακέραιος ο οποίος δεν διαιρείται από κάνενα q_i. Υποθέστε επίσης ότι $N > (\max(\log q_0, \lambda(l) \log(\phi(l))))^5$ και ότι για t με $\frac{2}{\lambda(l) \log q_0} < |t| < 4A \log U$ και w με $w \geq \frac{2\pi}{\lambda(l)}$, το πολύ οι μισοί από τους πρώτους q_i ικανοποιούν την σχέση:

$|t \log q_i - kw| < 8\sqrt{\frac{\log U}{N}}$ (συνθήκη μη-συσταδοποίησης)

για κάποιον ακέραιο k, όπου $U = (AN\phi(l) \log q_0)^2$, με το Α πραγματικό αριθμό μεγαλύτερο του 1 (θα μπορούσαν να παρθούν ανισότητες, αντί για ανισώσεις).

Τότε για επαρκώς μεγάλα N, το πλήθος των τιμών Π που διαιρούν το R και παράλληλα ικανοποιούν τις συνθήκες:

1. $\Pi \equiv 1(\mod l)$

2. $|\log \Pi - \frac{\log R}{2} - B| \leq \frac{1}{2A}$

είναι $2^{N - O(\sqrt{N} + \log U)}$ για κάθε $|B| \leq \frac{\sqrt{N} \log q_0}{36}$

Απόδειξη: Έστω $H = (\mathbb{Z}/l\mathbb{Z})^{\times}$, $h_i \equiv q_i(\mod l)$. Θα κατασκευάσουμε μια αλυσίδα εμφωλευμένων γνήσιων υποομάδων της $H = G_0$ ως εξής:
Το G_j θα είναι γνήσια υποομάδα του G_{j-1} τέτοια ώστε:

$\#\{i : h_i \in G_{j-1} \backslash G_j\} < \lambda(G_{j-1})^2 \log(\#\{i : h_i \in G_{j-1}\}|G_{j-1}|)$,
με τη διαδικασία να τερματίζει όταν καμία τέτοια (γνήσια) υποομάδα δεν υπάρχει.

Έστω G_k η τελευταία ομάδα της αλυσίδας που κατασκευάσαμε. Υποθέτουμε ότι $k \geq 1$ (δεν παίζει ρόλο, αν $k = 0$ απλά δε θα διαχωρίζαμε τους πρώτους, βλέπε παρακάτω).

Τότε επειδή $\frac{|G_{j-1}|}{|G_j|} \geq 2$ για $1 \leq j \leq k$ θα έχουμε:

$\phi(l) = |G_0| \geq \frac{|G_0|}{|G_k|} = \frac{|G_0|}{|G_1|} \cdots \frac{|G_{k-1}|}{|G_k|} \geq 2^k$ άρα $k \leq \log_2 \phi(l) = \frac{\log \phi(l)}{\log 2} < 2 \log \phi(l)$.

Επιπλέον, σε κάθε βήμα της διαδικασίας αφαιρούνται το πολύ $\lambda(G_0)^2 \log(N|G_0|) = \lambda(l)^2 \log(N\phi(l))$ από τα h_i. Οπότε, αν $m = \#\{i : h_i \in G_k\}$,

$N - m < (\lambda(l)^2 \log(N\phi(l))) \cdot (2 \log \phi(l)) < 2\lambda(l)^2 \log^2 \phi(l) \log N < 2N^{\frac{2}{5}} \log N < \frac{\sqrt{N}}{6}$, συνεπώς $m > \frac{5N}{6}$, οπότε όταν το N είναι αρκετά μεγάλο, το ίδιο ισχύει και για το m.

Έστω $p_1, ..., p_m$ οι πρώτοι των οποίων τα h_i ανήκουν στο G_k, με τον p_0 να είναι ο μεγαλύτερος απ'αυτούς, και $q_{a_1}, ..., q_{a_{N-m}}$ οι υπόλοιποι.

Έστω επίσης $B_k = B + \frac{\sum_{i=1}^{N-m} \log q_{a_i}}{2}$.

Τότε $|B_k| \leq |B| + \frac{\sum_{i=1}^{N-m} \log q_{a_i}}{2} \leq \frac{\sqrt{N} \log q_0}{36} + \frac{\sum_{i=1}^{N-m} \log q_0}{2} \leq \frac{\sqrt{N} \log q_0}{36} + \frac{\sqrt{N} \log q_0}{12} \leq \frac{\sqrt{N} \log q_0}{9} \leq \frac{2\sqrt{N} \log p_0}{9} = \frac{(\frac{8}{9}\sqrt{N}) \log p_0}{4} \leq \frac{\sqrt{m} \log p_0}{4}$.

Απο 'δω και πέρα θα γράφουμε το G_k ως G και θα χρησιμοποιήσουμε τον προσθετικό συμβολισμό για την πράξη που το διέπει.

Έστω $K = [B_k - \frac{1}{2A}, B_k + \frac{1}{2A}]$, $P = \prod_i p_i$, $r_i = \frac{\log p_i}{2}$, $r_0 = \frac{\log p_0}{2}$, g_i ο εκπρόσωπος του p_i στο G ($g_i \equiv p_i(\mod l)$), χ_0 ο τετριμμένος χαρακτήρας του G.

Ορίζουμε τώρα κάποιες βοηθητικές τυχαίες μεταβλητές.

Έστω D η τυχαία μεταβλητή υπεράνω του $\mathbb{R}$ έτσι ώστε $\mathcal{P}(D = \Pi) = \frac{1}{2^m}$ για κάθε Π διαιρέτη του P και X_i η τυχαία μεταβλητή υπεράνω του χώρου $G \times \mathbb{R}$ έτσι ώστε $\mathcal{P}(X_i = (g_i, r_i)) = \mathcal{P}(X_i = (0, -r_i)) = \frac{1}{2}$. Επιπροσθέτως με $I_B(S) := I_{\{S \in B\}}$ συμβολίζουμε την δείκτρια συνάρτηση του ενδεχομένου $\{S \in B\}$. Τότε για κάθε διαιρέτη Π του P έχουμε:

$$\sum_{i:p_i|\Pi} r_i + \sum_{i:p_i \nmid \Pi} -r_i = 2 \sum_{i:p_i|\Pi} r_i - \sum_{i:p_i|P} r_i = \log \Pi - \frac{\log P}{2} \tag{3.1}$$

$$\sum_{i:p_i|\Pi} g_i = 0 \Leftrightarrow \prod_{i:p_i|\Pi} p_i \equiv 1(\mod l) \Leftrightarrow \Pi \equiv (1 \mod l) \tag{3.2}$$

Άρα αν $Z = \{\Pi : \log \Pi - \frac{\log P}{2} \in K, \Pi \equiv (1 \mod l)\}$, τότε

$\frac{|Z|}{2^m} = \frac{|Z|}{|P|} = \mathcal{P}(D \in Z) = \mathbb{E}(I_{\{D\in Z\}}) = \mathbb{E}(I_Z(D)) = \mathbb{E}(I_{0\times K}(\sum_i X_i))$, όπου η τελευταία ισότητα ισχύει λόγω των (3.1) και (3.2).

Θέλουμε να δείξουμε ότι αυτή η μέση τιμή είναι θετική. Τώρα, επειδή αυτή η μέση τιμή είναι δύσκολο να προσεγγιστεί (πόσω μάλλον να υπολογιστεί), αλλάζουμε την δείκτρια συναρτησή μας σε κάποια αρεστή Γκαουσιανή ευελπιστώντας ότι η καλή συμπεριφορά αυτής στα $\pm\infty$ και οι υποθέσεις της εκφώνησης θα μας δώσουν αρκετή πληροφορία ώστε να υπάρξει η ζητούμενη (ασυμπτωτική) φραγή. Παρατηρούμε ότι η G είναι πεπερασμένη αβελιανή ομάδα ως υποομάδα πεπερασμένης αβελιανής (H), οπότε φρεσκάροντας τις γνώσεις μας στη Μη-Μεταθετική Άλγεβρα:

1. Όλες οι αναπαραστάσεις της είναι 1-διάστατες.

2.G ισόμορφη με την δυϊκή της $\hat{G} = \{\rho : G \to S^1 | \rho \text{ ομομορφισμός}\}$.

3. Οι χαρακτήρες της G είναι ακριβώς οι παραπάνω ομομορφισμοί καθώς το ίχνος ενός 1×1 πίνακα ταυτίζεται με το στοιχείο που υπάρχει στην (μοναδική) θέση $(1, 1)$ μέσω ισομορφισμού.

4.Από τις σχέσεις ορθογωνιότητας των χαρακτήρων, λαμβάνοντας υπόψιν ότι το πλήθος τους είναι $|G|$ και ότι $|C_G(0)| = |G|$, έχουμε:

$$\frac{1}{|G|}\sum_{\chi\in\hat{G}} \chi(g) = \begin{cases} |G|, g = 0 \\ 0\ , g \neq 0 \end{cases}$$

δηλαδή το άθροισμα είναι ίσο για κάθε g με την $I_0(g)$.

Έστω $F(x) = e^{-a^2(x-B_k)^2}$ όπου $a = 2A\sqrt{\log U}$.

Ο μετασχηματισμός Fourier της F είναι ο

$\hat{F}(t) = \int_{-\infty}^{+\infty} F(x)e^{-itx}\,\mathrm{d}x = \frac{\sqrt{\pi}}{a}e^{-\frac{t^2}{4a^2}-iB_kt}$, συνεπώς:

$$F(x) = \frac{1}{2\pi}\int_{-\infty}^{+\infty} \hat{F}(t)e^{itx}\mathrm{d}t = \frac{1}{2a\sqrt{\pi}}\int_{-\infty}^{+\infty} e^{-\frac{t^2}{4a^2}-iB_kt}e^{itx}\mathrm{d}t$$

Εκμεταλλευόμενοι τώρα την σχέση ορθογωνιότητας, ορίζουμε την συνάρτηση που αναζητούσαμε, όπως θα φανεί,

$$F^*(g, x) = \frac{1}{2a\sqrt{\pi}|G|}\sum_{\chi\in\hat{G}}\int_{-\infty}^{+\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\chi_t(g, x)\mathrm{d}t$$

όπου $\chi_t(g,x) = \chi(g)e^{itx}$.

Παρατηρήστε ότι, $F^*(e,x) = F(x)$ για $g = 0$, αλλιώς $F^*(g,x) = 0$.

Ας προσπαθήσουμε λοιπόν να προσεγγίσουμε την $\boxed{E_1 = \mathbb{E}(F^*(\sum_j X_j))}$.

Καταρχάς, $\mathbb{E}(\chi_t(X_j)) = \chi_t(0,-r_j)\mathcal{P}(X_j = (0,-r_j)) + \chi_t(g_j,r_j)\mathcal{P}(X_j = (g_j,r_j)) =$

$$\frac{e^{itr_j}\chi(g) + e^{-itr_j}}{2}$$

Έπειτα $2a\sqrt{\pi}|G|E_1 = 2a\sqrt{\pi}|G|\mathbb{E}\big(\frac{1}{2a\sqrt{\pi}|G|}\sum_{\chi\in\hat{G}_{-\infty}}\int^{+\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\chi_t(\sum_j X_j))\mathrm{d}t\big) =$

$$\mathbb{E}\big(\sum_{\chi\in\hat{G}_{-\infty}}\int^{+\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \chi_t(X_j))\mathrm{d}t\big) = \sum_{\chi\in\hat{G}_{-\infty}}\int^{+\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \big(\frac{e^{itr_j}\chi(g) + e^{-itr_j}}{2}\big)\mathrm{d}t =$$

$$\big|\sum_{\chi\in\hat{G}_{-\infty}}\int^{+\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \frac{e^{itr_j}\chi(g) + e^{-itr_j}}{2}\mathrm{d}t\big|$$

με την 2η ισότητα να ισχύει επειδή οι τυχαίες μεταβλητές X_j είναι ανεξάρτητες, η 3η επειδή το ολοκλήρωμά μας συγκλίνει κατά απόλυτη τιμή (οπότε και επιτρέπεται η εναλλαγή μέσης τιμής και ολοκληρώματος, το άθροισμα είναι έτσι και αλλιώς πεπερασμένο), ενώ η 4η επειδή η F^* είναι μη αρνητική (άρα και η E_1).

Στόχος μας είναι να δείξουμε ότι η κύρια συνεισφορά στην τιμή της τελευταίας έκφρασης προέρχεται από τον τετριμμένο χαρακτήρα, για μικρά t.

Έστω $t_1 = \frac{1}{r_0\sqrt{m}}, t_2 = \frac{3}{r_0\sqrt{m}}, t_3 = \frac{1}{\lambda(G)r_0}, t_4 = 4A\log U$.

Προφανώς $t_1 < t_2 < t_3 < t_4$, με την 2η ανίσωση λ.χ. να ισχύει αφού $m > \frac{5N}{6}$ και, από την κατασκευή του G, $m \geq \lambda(G)^2\log(m|G|)$.

Υποθέτουμε ότι $|G| > 1$ (άρα και $\lambda(G) > 1$) και διακρίνουμε περιπτώσεις (στο τέλος της απόδειξης θα σχολιάσουμε τι συμβαίνει αλλιώς):

1ον) Για τον τετριμμένο χαρακτήρα χ_0 έχουμε:

$$\big|\int_{-\infty}^{+\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \frac{e^{itr_j}\chi_0(g) + e^{-itr_j}}{2}\mathrm{d}t\big| = \big|\int_{-\infty}^{+\infty} e^{-\frac{t^2}{4a^2}-iB_k}\prod_j \frac{e^{itr_j} + e^{-itr_j}}{2}\mathrm{d}t\big| =$$

$$\Big|\int_{-\infty}^{+\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \cos(tr_j)\mathrm{d}t\Big| = \Big|\int_{0}^{+\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \cos(tr_j)\mathrm{d}t + \int_{-\infty}^{0} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \cos(tr_j)\mathrm{d}t\Big| =$$

$$\Big|\int_{0}^{+\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \cos(tr_j)\mathrm{d}t + \int_{0}^{+\infty} e^{-\frac{t^2}{4a^2}+iB_kt}\prod_j \cos(tr_j)\mathrm{d}t\Big| =$$

$$\Big|\int_{0}^{+\infty} e^{-\frac{t^2}{4a^2}}(e^{iB_kt}+e^{-iB_kt})\prod_j \cos(tr_j)\mathrm{d}t\Big| = 2\Big|\int_{0}^{+\infty} e^{-\frac{t^2}{4a^2}}\cos(B_kt)\prod_j \cos(tr_j)\mathrm{d}t\Big| =$$

$$2\Big|\int_{0}^{t_1} e^{-\frac{t^2}{4a^2}}\cos(B_kt)\prod_j \cos(tr_j)\mathrm{d}t + \int_{t_1}^{t_2} e^{-\frac{t^2}{4a^2}}\cos(B_kt)\prod_j \cos(tr_j)\mathrm{d}t +$$

$$\int_{t_2}^{t_3} e^{-\frac{t^2}{4a^2}}\cos(B_kt)\prod_j \cos(tr_j)\mathrm{d}t + \int_{t_3}^{t_4} e^{-\frac{t^2}{4a^2}}\cos(B_kt)\prod_j \cos(tr_j)\mathrm{d}t +$$

$$\int_{t_4}^{+\infty} e^{-\frac{t^2}{4a^2}}\cos(B_kt)\prod_j \cos(tr_j)\mathrm{d}t\Big| \geq 2\Big(\Big|\int_{0}^{t_1} e^{-\frac{t^2}{4a^2}}\cos(B_kt)\prod_j \cos(tr_j)\mathrm{d}t +$$

$$\int_{t_1}^{t_2} e^{-\frac{t^2}{4a^2}}\cos(B_kt)\prod_j \cos(tr_j)\mathrm{d}t\Big| - \int_{t_2}^{t_3}\prod_j |\cos(tr_j)|\mathrm{d}t - \int_{t_3}^{t_4}\prod_j |\cos(tr_j)|\mathrm{d}t - \int_{t_4}^{+\infty} e^{-\frac{t^2}{4a^2}}\mathrm{d}t\Big)$$

με την τελευταία ανισότητα να προκύπτει από την τριγωνική ανισότητα και τις σχέσεις $e^{-x^2} \leq 1, |\cos x| \leq 1$, ενώ οι εναλλαγές των άκρων επιτρέπονται λόγω της απόλυτης σύγκλισης του ολοκληρώματος.

Θέτοντας συνεπώς

$$I_1 = \int_{0}^{t_1} e^{-\frac{t^2}{4a^2}}\cos(B_kt)\prod_j \cos(tr_j)\mathrm{d}t,\ I_2 = \int_{t_1}^{t_2} e^{-\frac{t^2}{4a^2}}\cos(B_kt)\prod_j \cos(tr_j)\mathrm{d}t,$$

$$I_3 = \int_{t_2}^{t_3}\prod_j |\cos(tr_j)|\mathrm{d}t,\ I_4 = \int_{t_3}^{t_4}\prod_j |\cos(tr_j)|\mathrm{d}t,\ C = \int_{t_4}^{+\infty} e^{-\frac{t^2}{4a^2}}\mathrm{d}t$$

βλέπουμε ότι:

$$\Big|\int_{-\infty}^{+\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \frac{e^{itr_j}\chi_0(g)+e^{-itr_j}}{2}\mathrm{d}t\Big| \geq 2(|I_1+I_2| - I_3 - I_4 - C) \qquad (3.3)$$

2ον) Για κάθε μη τετριμμένο χαρακτήρα χ έχουμε:

$$|\int_{-\infty}^{\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \frac{e^{itr_j}\chi(g)+e^{-itr_j}}{2}\mathrm{d}t| \leq |\int_{-t_4}^{t_4} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \frac{e^{itr_j}\chi(g)+e^{-itr_j}}{2}\mathrm{d}t|+2C,$$

όπου C, όπως προηγουμένως. Όμως

$$|\int_{-t_4}^{t_4} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \frac{e^{itr_j}\chi(g)+e^{-itr_j}}{2}\mathrm{d}t| =$$

$$|\int_{0}^{t_4} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \frac{e^{itr_j}\chi(g)+e^{-itr_j}}{2}\,\mathrm{d}t + \int_{-t_4}^{0} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \frac{e^{itr_j}\chi(g)+e^{-itr_j}}{2}\,\mathrm{d}t\,| \leq$$

$$|\int_{0}^{t_4}\prod_j |\frac{e^{itr_j}\chi(g)+e^{-itr_j}}{2}|\mathrm{d}t + |\int_{-t_4}^{0}\prod_j |\frac{e^{itr_j}\chi(g)+e^{-itr_j}}{2}|\mathrm{d}t \leq$$

$$2\max_{s\in\{\pm1\}}\int_{0}^{t_4}\prod_j |\frac{e^{istr_j}\chi(g)+e^{-istr_j}}{2}|\mathrm{d}t =$$

$$2\max_{s\in\{\pm1\}}\Big(\int_{0}^{t_3}\prod_j |\frac{e^{istr_j}\chi(g)+e^{-istr_j}}{2}|\mathrm{d}t + \int_{t_3}^{t_4}\prod_j |\frac{e^{istr_j}\chi(g)+e^{-istr_j}}{2}|\mathrm{d}t\Big) \leq$$

$$2\big(\max_{s\in\{\pm1\}}\int_{0}^{t_3}\prod_j |\frac{e^{istr_j}\chi(g)+e^{-istr_j}}{2}|\mathrm{d}t + \max_{s\in\{\pm1\}}\int_{t_3}^{t_4}\prod_j |\frac{e^{istr_j}\chi(g)+e^{-istr_j}}{2}|\mathrm{d}t\big)$$

οπότε, θέτοντας

$$J_1^{\chi} = \max_{s\in\{\pm1\}}\int_{0}^{t_3}\prod_j |\frac{e^{istr_j}\chi(g)+e^{-istr_j}}{2}|\mathrm{d}t,\ J_2^{\chi} = \max_{s\in\{\pm1\}}\int_{t_3}^{t_4}\prod_j |\frac{e^{istr_j}\chi(g)+e^{-istr_j}}{2}|\mathrm{d}t,$$

τότε

$$|\int_{-\infty}^{\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \frac{e^{itr_j}\chi(g)+e^{-itr_j}}{2}\mathrm{d}t| \leq 2(J_1^{\chi}+J_2^{\chi}+C)$$

Τελικά συνδυάζοντας τις παραπάνω ανισότητες και παρατηρώντας ότι $I_4 = J_2^{\chi_0}$ (από την αρτιότητα του συνημιτόνου), θα βρούμε:

$$2a\sqrt{\pi}|G|E_1 = |\sum_{\chi\in\hat{G}_{-\infty}^{+\infty}}\int e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \frac{e^{itr_j}\chi(g)+e^{-itr_j}}{2}\mathrm{d}t| \geq$$

$$|\int_{-\infty}^{+\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \frac{e^{itr_j}\chi_0(g)+e^{-itr_j}}{2}\mathrm{d}t|-|\sum_{\substack{\chi\in\hat{G}\\ \chi\neq\chi_0}}\int_{-\infty}^{\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \frac{e^{itr_j}\chi(g)+e^{-itr_j}}{2}\mathrm{d}t| \geq$$

$$|\int_{-\infty}^{+\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \frac{e^{itr_j}\chi_0(g)+e^{-itr_j}}{2}\mathrm{d}t|-\sum_{\substack{\chi\in\hat{G}\\ \chi\neq\chi_0}}|\int_{-\infty}^{\infty} e^{-\frac{t^2}{4a^2}-iB_kt}\prod_j \frac{e^{itr_j}\chi(g)+e^{-itr_j}}{2}\mathrm{d}t| \geq$$

$$2(|I_1+I_2|-I_3-J_2^{\chi_0}-C)-\sum_{\substack{\chi\in\hat{G}\\ \chi\neq\chi_0}} 2(J_1^{\chi}+J_2^{\chi}+C)=$$

$$2\Big(|I_1+I_2|-I_3-\sum_{\substack{\chi\in\hat{G}\\ \chi\neq\chi_0}} J_1^{\chi}-\sum_{\chi\in\hat{G}}(J_2^{\chi}+C)\Big)$$

Ξεκινάμε τώρα να φράσσουμε καθέναν απ' αυτούς τους όρους. Όπως θα γίνει αντιληπτό, η (άνω) φραγή των όρων J_2^{χ} είναι αυτή που απαιτεί την συνθήκη μη-συσταδοποίησης.

Ας δούμε τι γίνεται με το I_1.

Έστω t τ.ω. $0 \leq t \leq t_1$. Αφού $A > 1$, τότε και $a > 1$. Συνεπώς, $e^{-\frac{t^2}{4a^2}} > \frac{99}{100}$ για μεγάλα m. Επιπλέον, $\cos(B_kt) \geq \cos\left(\frac{1}{2}\right) \geq \frac{5}{6}$ διότι $|B_kt| \leq \frac{\sqrt{m}\log p_0}{4r_0\sqrt{m}} = \frac{1}{2}$. Από το Λήμμα 3

$\cos(tr_i) \geq 1-\frac{t^2r_i^2}{2} \geq 1-\frac{1}{2m} \Rightarrow$

$\prod_{i=1}^{m}(\cos(tr_i)) \geq (1-\frac{1}{2m})^m > \frac{20}{33}$ για μεγάλα m.

$$I_1 = \int_0^{t_1} e^{-\frac{t^2}{4a^2}}\cos(B_kt)\prod_j \cos(tr_j)\mathrm{d}t > \int_0^{t_1}\frac{1}{2}\mathrm{d}t = \frac{1}{2r_0\sqrt{m}}$$

Από την άλλη, για $t_1 \leq t \leq t_2$, η ποσότητα $e^{-\frac{t^2}{4a^2}}\cos(B_kt)\prod_j \cos(tr_j)$ θα είναι θετική, καθώς $|B_kt| < \frac{\pi}{2}$ (το οποίο σίγουρα ισχύει για $|t| < \frac{\pi}{r_0\sqrt{m}}$) και $|tr_j| < \frac{\pi}{2}$ για κάθε i (το οποίο ισχύει για $|t| < \frac{\pi}{2r_0}$). Συνεπώς $I_2 > 0 \Rightarrow I_1 + I_2 > 0$.

Έστω τώρα $t_2 \leq t \leq t_3$. Τότε $|tr_i| \leq 1$ για κάθε i, συνεπώς από το Λήμμα 3 και επειδή το συνημίτονο φθίνει απολύτως στο $[0, \frac{\pi}{2}]$:

$$I_3 = \int_{t_2}^{t_3}\prod_{i=1}^{m}|\cos(tr_i)|\mathrm{d}t \leq \int_{t_2}^{t_3}\prod_{i=1}^{m}|\cos\frac{tr_0}{2}|\mathrm{d}t \leq \int_{t_2}^{t_3}(1-\frac{11}{24}\frac{t^2r_0^2}{4})^m\mathrm{d}t \leq$$

$$\int_{t_2}^{t_3}(1-\frac{t^2r_0^2}{9})^m\mathrm{d}t \leq \int_{t_2}^{t_3} e^{-\frac{mt^2r_0^2}{9}}\mathrm{d}t$$

Κάνοντας την αλλαγή μεταβλητών $u = \frac{\sqrt{m}tr_0}{3}$, θα βρούμε

$$I_3 \leq \frac{3}{r_0\sqrt{m}} \int_1^{\frac{\sqrt{m}}{3\lambda(G)}} e^{-u^2}\mathrm{d}u \leq \frac{3}{r_0\sqrt{m}} \int_1^{\infty} e^{-u^2}\mathrm{d}u \leq \frac{3\sqrt{\pi}}{2r_0\sqrt{m}} \cdot \mathbf{erfc}(1) \leq$$

$$\frac{3\sqrt{\pi}}{2r_0\sqrt{m}}\frac{16}{100} \leq \frac{44}{50}\frac{1}{2r_0\sqrt{m}}.$$

Ας περάσουμε τώρα στην φραγή των J_1^{χ}.

Έστω χ ένας μη τετριμμένος χαρακτήρας, s τ.ω. $s \in \{1,-1\}$, t τ.ω. $0, \leq t \leq t_3$. Παρατηρούμε, χρησιμοποιώντας το Λήμμα 3γ) ότι:

$$|\frac{\chi(g_j)+e^{-2istr_j}}{2}| = \sqrt{\frac{1+\mathrm{Re}\{(\chi(g)e^{2istr_j})\}}{2}} = \sqrt{\frac{1+\cos{(\frac{2\pi k_j}{\lambda(G)}+2str_j)}}{2}},$$

όπου $k_j < |\frac{\lambda(G)}{2}|$ είναι ο ακέραιος για τον οποίο $\chi(g_j) = e^{\frac{2\pi i k_j}{\lambda(G)}}$. Τέτοιος ακέραιος υπάρχει αφού η τάξη του στοιχείου g_j διαιρεί το $\lambda(G)$ και ο χ είναι ομομορφισμός.

Εάν $|k_j| \geq 1$, τότε μιάς και $|tr_j| \leq \frac{1}{\lambda(G)} < \frac{\pi}{3\lambda(G)}$, θα έχουμε:

$|\frac{2\pi k_j}{\lambda(G)}+2str_j| \geq |\frac{2\pi k_j}{\lambda(G)}| - |2str_j| \geq \frac{2\pi}{\lambda(G)} - \frac{2\pi}{3\lambda(G)} = \frac{4\pi}{3\lambda(G)} > \frac{4}{\lambda(G)}$ και

$|\frac{2\pi k_j}{\lambda(G)}+2str_j| \leq \pi + \frac{2}{\lambda(G)} \Rightarrow$

$|\pm 2\pi - (\frac{2\pi k_j}{\lambda(G)}+2str_j)| \geq 2\pi - (\pi+\frac{2}{\lambda(G)}) \geq \pi - \frac{2}{\lambda(G)} \geq \pi - 1 > 2 \geq \frac{4}{\lambda(G)}$

Συνεπώς ,για $|k_j| \geq 1$, η απόσταση μεταξύ του $\frac{2\pi k_j}{\lambda(G)}+2str_j$ και του κοντινότερου πολλαπλασίου του 2π είναι μεγαλύτερη από $\frac{4}{\lambda(G)}$. Λόγω του γεγονότος ότι το συνημίτονο φθίνει στο $[0,\pi]$ και από το Λήμμα 3, βρίσκουμε ότι:

$$|\frac{\chi(g_j)+e^{-2istr_j}}{2}| < \sqrt{\frac{1+\cos\frac{4}{\lambda(G)}}{2}} \leq \sqrt{\frac{1+1-\frac{4}{\lambda(G)^2}}{2}} = \sqrt{1-\frac{2}{\lambda(G)^2}} < 1-\frac{1}{\lambda(G)^2},$$

αν $|k_j| \geq 1$.

Τώρα, (κανονική) υποομάδα της G αποτελεί και ο πυρήνας ενός δοθέντος ομομορφισμού της. Αφού οι χαρακτήρες είναι ομομορφισμοί της, για κάθε μη τετριμμένο χαρακτήρα χ, $\ker\chi \subsetneq G$, οπότε από την κατασκευή του G, υπάρχουν τουλάχιστον $\lambda(G)^2\log(m|G|)$ τιμές του j τέτοιες ώστε $\chi(g_j) \neq 1$, δηλαδή $|k| \geq 1$. Συνεπώς επειδή ακόμα και όταν $k_j = 0$ ο αντίστοιχος όρος είναι το πολύ 1, τελικά:

$$J_1^\chi = \max_{s\{\in\pm 1\}} \int_0^{t_3} \prod_j |\frac{e^{istr_j}\chi(g) + e^{-istr_j}}{2}| \mathrm{d}t < \int_0^{t_3} (1 - \frac{1}{\lambda(G)^2})^{\lambda(G)^2 \log(m|G|)} \mathrm{d}t \leq \int_0^{t_3} e^{-\log(m|G|)} \mathrm{d}t =$$

$$\frac{e^{-\log(m|G|)}}{\lambda(G) r_0} = \frac{1}{m|G|\lambda(G) r_0} < \frac{1}{1000|G| r_0 \sqrt{m}} = \frac{1}{500|G|} \frac{1}{2r_0\sqrt{m}}$$

Έστω τώρα χ οποιοσδήποτε χαρακτήρας. Επειδή $G \leq H$, από τον ορισμό της συνάρτησης Carmichael, $\lambda(G) \leq \lambda(H) = \lambda(l)$. Η συνθήκη μη-συσταδοποίησης μας οδηγεί στο συμπέρασμα ότι για κάθε t με $\frac{2}{\lambda(G)\log p_0} = t_3 < |t| < t_4 = 4A \log U$, τουλάχιστον το 1/3 ($\frac{\frac{N}{2} - m}{m} > \frac{\frac{N}{2} - \frac{N}{6}}{m} > \frac{\frac{N}{3}}{N} = \frac{1}{3}$) των πιθανών τιμών του j είναι τέτοιες ώστε:

$|2tr_i - \frac{2\pi k}{\lambda(G)}| \geq 8\sqrt{\frac{\log U}{N}} > 7\sqrt{\frac{6}{5N}\log U} > 7\sqrt{\frac{\log U}{m}}$ για κάθε $k \in \mathbb{Z}$.

Αν u_s είναι οι ακέραιοι που ελαχιστοποιούν το $|2str_j - \frac{2\pi k}{\lambda(G)}|$ για $s \in \{-1, 1\}$, τότε $|2str_j - \frac{2\pi u_s}{\lambda(G)}| \leq \pi$ διοτί, αλλιώς, ο ακέραιος $k = u_s \pm \lambda(G)$ θα το ελαχιστοποιούσε περαιτέρω. Όμως, λόγω της 2π-περιοδικότητας του φθίνοντος στο $[0, \pi]$ συνημιτόνου, του Λήμματος 3 και των άνωθεν, θα βρούμε:

$\cos(2tr_j - \frac{2\pi k}{\lambda(G)}) \leq \max_{s\in\{\pm 1\}} \cos(2tr_j - \frac{2\pi u_s}{\lambda(G)}) < \cos(7\sqrt{\frac{\log U}{m}}) \leq 1 - \frac{49\log U}{4m} \leq 1 - \frac{12\log U}{m}$.
Οπότε και:

$$|\frac{\chi(g_j) + e^{-2istr_j}}{2}| = \sqrt{\frac{1 + \cos(\frac{2\pi k_j}{\lambda(G)} + 2str_j)}{2}} \leq \sqrt{1 - \frac{6\log U}{m}} \leq 1 - \frac{3\log U}{m}$$
όπου το k_j τ.ω. $\chi(g_j) = e^{\frac{2\pi k_j}{\lambda(G)}}$.

Με αυτά και με αυτά,

$$J_2^\chi = \max_{s\{\in\pm 1\}} \int_{t_3}^{t_4} \prod_j |\frac{e^{istr_j}\chi(g) + e^{-istr_j}}{2}| \mathrm{d}t \leq \int_{t_3}^{t_4} (1 - \frac{3\log U}{m})^{\frac{m}{3}} \mathrm{d}t \leq \int_{t_3}^{t_4} e^{-\log U} \mathrm{d}t \leq$$

$$t_4 e^{-\log U} = \frac{4A\log U}{U} = \frac{4A}{\sqrt{U}} \frac{\log U}{\sqrt{U}} \leq \frac{4}{N\phi(l)\log q_0} \leq \frac{1}{500|G|} \frac{1}{2r_0\sqrt{m}},$$
όπου για την προτελευταία ανισότητα χρησιμοποιήσαμε τον ορισμό του U και για την τελευταία ότι το N είναι όσο μεγάλο το επιθυμούμε.

Τέλος, για το J_3^χ, θέτοντας $u = \frac{t}{2a}$, θα έχουμε:

$$\int_{t_4}^{\infty} e^{\frac{-t^2}{4a^2}} \mathrm{d}t = 2a \int_{\frac{t_4}{2a}}^{\infty} e^{-u^2} \mathrm{d}u = a\sqrt{\pi}\,\mathbf{erfc}(\frac{t_4}{2a}) \leq a\sqrt{\pi} e^{-\frac{t_4^2}{4a^2}} = a\sqrt{\pi} e^{-\log U} = \frac{a\sqrt{\pi}}{U} =$$

$$\frac{2\sqrt{\pi}A}{\sqrt{U}}\sqrt{\frac{\log U}{U}} \leq \frac{2\sqrt{\pi}}{N\phi(l)\log q_0} \leq \frac{1}{500|G|}\frac{1}{2r_0\sqrt{m}}.$$

Καιρός να κάνουμε τον απολογισμό για τα φράγματα που υπολογίσαμε.

$$2a\sqrt{\pi}|G|E_1 \geq 2\Big(|I_1+I_2| - I_3 - \sum_{\substack{\chi\in\hat{G}\\ \chi\neq\chi_0}} J_1^{\chi} - \sum_{\chi\in\hat{G}}(J_2^{\chi}+C)\Big) \geq \frac{2}{r_0\sqrt{m}}\big(\frac{1}{2} - \frac{44}{50}\frac{1}{2} -$$
$$\frac{|G|}{500|G|}\frac{1}{2} - \frac{|G|}{500|G|}\frac{1}{2} - \frac{|G|}{500|G|}\frac{1}{2}\big) \geq \frac{6}{100}\frac{1}{r_0\sqrt{m}}, \text{ άρα}$$

$$E_1 \geq \frac{6}{100}\frac{1}{r_0\sqrt{m}}\frac{1}{2a\sqrt{\pi}|G|} = \frac{6}{100}\frac{1}{r_0\sqrt{m}}\frac{1}{4A\sqrt{\pi}|G|\sqrt{\log U}} \geq \frac{1}{125}\frac{1}{A|G|r_0\sqrt{m\log U}}.$$

Μια ακόμα παρατήρηση που μας διευκολύνει αρκετά είναι ότι:

$$\sup_{(g,x)}(F^* - I_{0\times K}) = \sup_{(0,x)}(F^* - I_{0\times K}) = \sup_{x}(F - I_K) = e^{-\frac{a^2}{(2A)^2}} = e^{-\log U} = \frac{1}{U} =$$
$$\frac{1}{AN\phi(l)\log q_0\sqrt{U}} \leq \frac{1}{4000}\frac{1}{A|G|r_0\sqrt{m\log U}}$$

Συγκεντρωτικά:

$$\mathbb{E}(I_{0\times K}(\sum_j X_j)) = \mathbb{E}(F^*(\sum_j X_j)) - \mathbb{E}(F^*(\sum_j X_j) - I_{0\times K}(\sum_j X_j)) \geq E_1 -$$
$$\sup_{(g,x)}(F^* - I_{0\times K}) \geq \frac{1}{125}\frac{1}{A|G|r_0\sqrt{m\log U}} - \frac{1}{4000}\frac{1}{A|G|r_0\sqrt{m\log U}} \geq \frac{1}{250}\frac{1}{A|G|r_0\sqrt{m\log U}}.$$

Συνεπώς:

$$|Z| = 2^m\mathbb{E}(I_{0\times K}(\sum_j X_j)) \geq \frac{2^m}{250A|G|r_0\sqrt{U}} > \frac{2^m}{U} = 2^{N-O(\sqrt{N}+\log U)}$$

δηλαδή υπάρχουν τουλάχιστον $2^{N-O(\sqrt{N})-\log U}$ τέτοια d ώστε $\Pi \equiv 1(\mod l)$ και $\log\Pi - \frac{\log P}{2} \in K \Leftrightarrow |\log\Pi - \frac{\log P}{2} - B_k| \leq \frac{1}{2A}$ και επειδή εξ' ορισμού του B_k, θα έχουμε: $|\log\Pi - \frac{\log P}{2} - B_k| = |\log\Pi - \frac{\log R}{2} - B|$, τελικά οι Π είναι αυτοί που ψάχναμε και άρα καταλήξαμε στο ζητούμενο. ■

Σχόλιο: Αν $|G| = 1$, τότε θα μας αρκούσε να ελέγξουμε μόνο την συγκομιδή από τον τετριμμένο (και μοναδικό) χαρακτήρα, στην οποία περίπτωση η σχέση (3.3) μαζί με την δουλειά που κάναμε για τους αντίστοιχους όρους, μας δίνει και πάλι το ζητούμενο.

2. Συνέπειες

Πόρισμα 6.1: Οι συνθήκες του Θεωρήματος 6 ικανοποιούνται για
$\{q_1, .., q_N\} = \mathbf{P}_{n(z)}$, $A = e^{\frac{\eta y}{(4+6\Delta)\log y}}$, $B \to b(z)$, $l = L$.

Απόδειξη: Από την στιγμή που το L είναι μικρό σε σχέση με το X (κρίνοντας από την εξάρτησή τους από το y) θα έχουμε $p_i^2 = (d_{p_i}k_0 + 1)^2 \geq X^2 \geq 2XL \geq p_0$, όπου το p_0 είναι ο μεγαλύτερος πρώτος στο $\mathbf{P}_{n(z)}$.

Επίσης $2n(z) > (\log p_0)^5$ αφού η εξάρτηση του ενός από το y είναι εκθετική, ενώ του άλλου πολυωνυμική.

Από την Πρόταση 2: $\lambda(L) = [\{\lambda(p) : p \in \mathbf{Q}\}] = [\{p-1 : p \in \mathbf{Q}\}]$.

Όμως από τον ορισμό του $\mathbf{Q}$, όλοι πρώτοι p που ανήκουν σε αυτό είναι τέτοιοι ώστε ο μέγιστος (και άρα όλοι) πρώτος διαιρέτης του $p-1$ να είναι μικρότερος του y^{1-V}. Αν με $v_q(p-1)$ συμβολίσουμε την μέγιστη δύναμη με την οποία ο πρώτος q διαιρεί τον $p-1$, θα έχουμε:

$$\lambda(L) = [\{p-1 : p \in \mathbf{Q}\}] = \prod_{\substack{q \leq y^{1-V} \\ q \in \mathbb{P}}} \max_{p \in \mathbf{Q}} q^{v_q(p-1)} \leq \prod_{\substack{q \leq y^{1-E} \\ q \in \mathbb{P}}} y = y^{\pi(y^{1-E})} < y^{\frac{2y^{1-E}}{(1-E)\log y}} = e^{\frac{2y^{1-E}}{1-E}}.$$

Επιπλέον, $\log \phi(L) < \log L < \log\left(y^{\frac{2y}{\log y}}\right) = 2y$, οπότε προκύπτει (λόγω της ύπαρξης E στον εκθέτη) ότι

$$2n(z) > (\lambda(L)\log\phi(L))^5 \Rightarrow 2n(z) > (\max(\log p_0, \lambda(L)\log\phi(L)))^5$$

Παράλληλα $|b(z)| \leq \log X + 1 \leq \frac{\sqrt{2n(z)}\log p_0}{36}$.

Ενθυμούμενοι τώρα πως κατασκευάσαμε το $\mathbf{P}$ (βλέπε Πόρισμα 4.1), τουλάχιστον οι μισοί από τους πρώτους $p \in \mathbf{P}_{n(z)}$ είναι τέτοιοι ώστε:

$$\min_{\substack{k \in \mathbb{Z} \\ k \neq 0}} (|t\log p - k|) \leq \frac{1}{e^{\frac{\eta y}{(4+2\Delta)\log y}}}$$

για κάθε συγκεκριμένο t τ.ω. $|t| \leq e^{\frac{\eta y}{(4+4\Delta)\log y}}$.

Συνεπώς, για όλα τα t τ.ω. $|t| \leq e^{\frac{\eta y}{(4+5\Delta)\log y}}$ και τα w με $|w| \geq \frac{2\pi}{\lambda(L)}$, το πολύ οι μισοί πρώτοι $p \in \mathbf{P}_{n(z)}$ είναι τέτοιοι ώστε:

$$|t\log p - kw| = |w| \cdot |w^{-1}t\log p - k| \leq \frac{|w|}{e^{\frac{\eta y}{(4+2\Delta)\log y}}} \leq \frac{1}{e^{\frac{\eta y}{(4+\Delta)\log y}}}.$$

(αφού $|w^{-1}t| \leq e^{\frac{\eta y}{(4+4\Delta)\log y}}$ για τα t που επιλέξαμε) για κάποιον μη μηδενικό ακέραιο k.

Επιπλέον, στην προσπάθεια να βάλουμε και το $k = 0$ στην «κουβέντα», αν $|t| \geq \frac{2}{\lambda(L)\log p_0}$,

παρατηρούμε ότι:

$|t \log p| \geq \frac{1}{\lambda(L)} \geq \frac{1}{e^{\frac{2y^{1-E}}{1-E}}} \geq \frac{1}{e^{\frac{\eta y}{(4+\Delta)\log y}}}$.

Οπότε για t τ.ω. $\frac{2}{\lambda(L)\log p_0} \leq |t| \leq e^{\frac{\eta y}{(4+5\Delta)\log y}}$ και w τ.ω. $|w| \geq \frac{2\pi}{\lambda(L)}$ το πολύ οι μισοί από τους πρώτους $p \in \mathbf{P}_{n(z)}$ είναι τέτοιοι ώστε:

$|t \log p - kw| \leq \frac{1}{e^{\frac{\eta y}{(4+\Delta)\log y}}}$ για κάποιον ακέραιο k.

Έστω τώρα $U = (2n(z)A\phi(L)\log p_0)^2$. Τότε $\log U \leq 4(\frac{\eta y}{\log y} + y + \log y) \leq 8y$ και άρα:

$8\sqrt{\frac{\log U}{2n(z)}} \leq \frac{32\sqrt{y}}{e^{\frac{\eta y}{4\log y}}} \leq \frac{1}{e^{\frac{\eta y}{(4+\Delta)\log y}}}$ καθώς και

$4A\log U \leq 32Ay \leq \frac{1}{e^{\frac{\eta y}{(4+5\Delta)\log y}}}$

Συνεπώς για κάθε t με $\frac{2}{\lambda(L)\log p_0} < |t| < 4A\log U$ και w τ.ω. $|w| \geq \frac{2\pi}{\lambda(L)}$ το πολύ οι μισοί πρώτοι $p \in \mathbf{P}_{n(z)}$ είναι τέτοιοι ώστε

$|t\log p - kw| < 8\sqrt{\frac{\log U}{2n(z)}}$ για κάποιον ακέραιο k, οπότε μόλις ολοκληρώσαμε την πολυπόθητη αντιστοιχία των δεδομένων μας με τις υποθέσεις του Θεώρηματος 6. ■

Έχουμε πλέον τα κατάλληλα πολεμοφόδια ώστε να δαμάσουμε το πρόβλημα που μας ταλανίζει από την αρχή αυτής της εργασίας.

Απόδειξη Θεωρήματος 1:
Ακολουθώντας τον συμβολισμό και την λογική του Πορίσματος 6.1, έστω Π ένας από τους διαιρέτες του $P_{n(z)} = \prod_{p \in \mathbf{P}_{n(z)}} p$, που μας εξασφαλίζει το Θεώρημα 6 ότι υπάρχουν (με κάποιες ωφέλιμες ιδιότητες). Τότε $\Pi \equiv 1(\mod L)$. Επιπλέον, καθένας από τους πρώτους παραγοντές του, από την κατασκευή του $\mathbf{P}_{n(z)}$, είναι ισότιμος με $1(\mod k_0)$, οπότε

$\Pi \equiv 1(\mod k_0) \Rightarrow$

$\Pi \equiv 1(\mod k_0 L)$ (αφού $(k_0, L) = 1$).

Επίσης, κάθε πρώτος παράγοντας του Π είναι της μορφής $dk_0 + 1$ για κάποιο $d \mid L$. Συνεπώς $p - 1 | \Pi - 1$ για κάθε p τ.ω. $p \mid \Pi$ και άρα, από το Θεώρημα 2, ο Π είναι αριθμός Carmichael.

Επιπροσθέτως, από το Θεώρημα 6, έχουμε ότι:

$|\log\Pi - \log z - \frac{1}{2A}| = |\log\Pi - \frac{\log P_{n(z)}}{2} - b(z)| \leq \frac{1}{2A}$, δηλαδή υπάρχουν τουλάχιστον:

$2^{2N_- - O(\sqrt{N_+} + \log U)} > e^{\frac{1}{3}e^{\frac{\eta y}{2\log y}}}$

αριθμοί Carmichael με λογάριθμο εντός του διαστήματος $(\log z, \log z + \frac{1}{A})$.

Επιθυμούμε τώρα να γράψουμε το κάτω φράγμα στο πλήθος των αριθμών Carmichael σε όρους του z και όχι του y.

Προς αυτό, παρατηρούμε ότι $z \leq \lceil e^{y^2+2\Delta} \rceil^{\frac{11}{12}} e^{\frac{\eta y}{2\log y}} \leq e^{\frac{\eta y}{(2-\frac{\epsilon}{2})\log y}}$, οπότε ανακαλώντας ότι $\Delta = \frac{\epsilon^2}{12}$

$(\log z)^{\frac{1}{2+\epsilon}} \leq \frac{1}{2}(\log z)^{\frac{2-\frac{\epsilon}{2}}{4+\frac{\epsilon}{2}}} \leq \frac{e^{\frac{\eta y}{(4+6\Delta)\log y}}}{2} = \frac{A}{2}$, αφού $\epsilon < 1$, z (y) αρκετά μεγάλο.

Συνεπώς, από το Λήμμα 3

$e^{\log z + \frac{1}{A}} \leq z(1+\frac{2}{A}) \leq z + \frac{z}{(\log z)^{\frac{1}{2+\epsilon}}}$.

Επίσης, $\log z \leq y^{2+2\Delta} e^{\frac{\eta y}{2\log y}}$ και $\log\log z \geq y^{1-\Delta}$, από την μορφή των $Z_{\pm}(y)$, ώστε λοιπόν

$\frac{\log z}{(\log\log z)^{2+\epsilon}} \leq \frac{y^{2+2\Delta} e^{\frac{\eta y}{2\log y}}}{y^{(1-\Delta)(2+\epsilon)}} = e^{\frac{\eta y}{2\log y}} y^{4\Delta-\epsilon+\epsilon\Delta} \leq e^{\frac{\eta y}{2\log y}} y^{12\Delta-\epsilon} \leq \frac{1}{3} e^{\frac{\eta y}{2\log y}}$,
για μεγάλα $y = y(\epsilon)$.

Άρα $e^{\frac{\log z}{(\log\log z)^{2+\epsilon}}} \leq e^{\frac{1}{3} e^{\frac{\eta y}{2\log y}}}$, οπότε υπάρχουν τουλάχιστον $e^{\frac{\log z}{(\log\log z)^{2+\epsilon}}}$ αριθμοί Carmichael στο διάστημα $\left(z, z + \frac{z}{(\log z)^{\frac{1}{2+\epsilon}}}\right)$ για κάθε z ακέραιο στο διάστημα $[Z_-(y), Z_+(y)]$ (επιλέγοντας κάθε φορά κατάλληλο $n = n(z)$, για να εφαρμόσουμε το Πόρισμα 6.1).

Τα διαστήματα αυτά όμως επικαλύπτονται για μεγάλα y (άρα δεν υπάρχουν κενά από z διαστήματα του $\mathbb{N}$, για μεγάλα z):

$Z_-(y+1) = \lceil e^{(y+1)^{2+2\Delta}} \rceil^{\frac{1}{3}} e^{\frac{\eta(y+1)}{2\log(y+1)}} \leq e^{\frac{101}{100}\frac{e}{3} y^{2+2\Delta} e^{\frac{\eta y}{2\log y}}} < e^{\frac{11}{12} y^{2+2\Delta} e^{\frac{\eta y}{2\log y}}} \leq Z_+(y)$, όπου για την πρώτη ανισότητα χρησιμοποιήσαμε ότι

$\lceil e^{(y+1)^{2+2\Delta}} \rceil \leq e^{\lceil (y+1)^{2+2\Delta} \rceil} \leq e^{ey^{2+2\Delta}}$, $e^{\frac{\eta(y+1)}{2\log(y+1)}} \leq \frac{101}{100} e^{\frac{\eta y}{2\log y}}$, για μεγάλα y.

Εν κατακλείδι, αυξάνοντας το y με βήμα 1, συμπεραίνουμε ότι για επαρκώς μεγάλα z, υπάρχουν τουλάχιστον $e^{\frac{\log z}{(\log\log z)^{2+\epsilon}}}$ αριθμοί Carmichael εντός του διάστηματος $\left(z, z + \frac{z}{(\log z)^{\frac{1}{2+\epsilon}}}\right)$, δηλαδή ο αρχικός μας στόχος επετεύχθη! ■ ■

Βιβλιογραφία

[1] William R Alford, Andrew Granville, and Carl Pomerance. There are infinitely many carmichael numbers. *Annals of Mathematics*, 139(3):703–722, 1994.

[2] Tom M Apostol. *Introduction to analytic number theory*. Springer Science & Business Media, 1998.

[3] Joseph Bak, Donald J Newman, and Donald J Newman. *Complex analysis*, volume 8. Springer, 2010.

[4] Paul T Bateman and Harold G Diamond. *Analytic number theory: an introductory course*, volume 1. World Scientific, 2004.

[5] Keith Conrad. Carmichael numbers and korselt's criterion. *Available at: carmichaelkorselt. pdf (Accessed 2 October 2023)*, 2016.

[6] Harold Davenport. *Multiplicative number theory*, volume 74. Springer Science & Business Media, 2013.

[7] Paul Erdos. On the normal number of prime factors of p-1 and some related problems concerning euler's ø-function. *The Quarterly Journal of Mathematics*, (1):205–213, 1935.

[8] Godfrey Harold Hardy and Edward Maitland Wright. *An introduction to the theory of numbers*. Oxford University Press, 2008.

[9] Daniel Larsen. Bertrand's postulate for carmichael numbers. *International Mathematics Research Notices*, 2023(15):13072–13098, 2023.

[10] Hendrik W Lenstra Jr and Carl Pomerance. Primality testing with gaussian periods. *Journal of the European Mathematical Society*, 21(4):1229–1269, 2019.

[11] Norman Levinson. A motivated account of an elementary proof of the prime number theorem. *The American Mathematical Monthly*, 76(3):225–245, 1969.

[12] math.stackexchange.com. https://math.stackexchange.com/.

[13] James Maynard. Dense clusters of primes in subsets. *Compositio Mathematica*, 152(7):1517–1554, 2016.

[14] Florian K Richter. A new elementary proof of the prime number theorem. *arXiv preprint arXiv:2002.03255*, 2020.

[15] Joel Spencer and Ronald Graham. The elementary proof of the prime number theorem. *The Mathematical Intelligencer*, 31(3), 2009.

[16] Πέτρος Καλαμβόκας. Αναλυτική απόδειξη του θεωρήματος των πρώτων αριθμών. Master's thesis, Εθνικό Καποδιστριακό Πανεπιστήμιο Αθηνών, 2012.