ΣΥΝΕΧΗ ΚΛΑΣΜΑΤΑ ΚΑΙ Ο ΑΦΑΙΡΕΤΙΚΟΣ ΕΥΚΛΕΙΔΕΙΟΣ ΑΛΓΟΡΙΘΜΟΣ

ΑΓΓΕΛΙΝΑ Ε. ΒΙΔΑΛΗ

ΥΠΟΤΡΟΦΟΣ ΤΟΥ ΚΟΙΝΩΦΕΛΟΥΣ ΙΔΡΥΜΑΤΟΣ
ΑΛΕΞΑΝΔΡΟΣ Σ. ΩΝΑΣΗΣ

Επιβλέπων καθηγητής: ΓΙΑΝΝΗΣ Ν. ΜΟΣΧΟΒΑΚΗΣ

μΠλ∀

23 Σεπτεμβρίου, 2005

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον καθηγητή μου, **κ. Γιάννη Μοσχοβάκη** για όσα ανεκτίμητα έμαθα για τα μαθηματικά δουλεύοντας μαζί του, για τα αδιέξοδα και τα φωτεινά σημεία που είχαν οι δοκιμασίες στις οποίες με προέτρεψε και τώρα πια για την επιμονή του στην τελειοποίηση των διατυπώσεων, αλλά πάνω απ' όλα για το παράδειγμά του όταν προσεγγίζει με υπομονή και δυναμισμό νέα προβλήματα.

Ακόμη την καθηγήτρια **κ. Joan Rand Moschovakis** για μια εναλλακτική απόδειξη (με επαγωγή) που πρότεινε για το Λήμμα 3C.3 και τους καθηγητές **κ. Αντώνη Μελά** και **κ. Ευάγγελο Ράπτη** που μοιράστηκαν μαζί μου μερικά από τα προβλήματα που συνάντησα στη Θεωρία Αριθμών και πρότειναν λύσεις γι' αυτά.

Ακόμα νιώθω τυχερή που φοίτησα στο γόνιμο περιβάλλον του $\mu\prod\lambda\forall$, το οποίο διευθύνει «Λογικά» και άψογα ο καθηγητής **κ. Κώστας Δημητρακόπουλος**.

Κλείνοντας οφείλω να αναφέρω την ευγνωμοσύνη μου στο **Ίδρυμα Ωνάση**, για την τιμή που μου επεφύλλαξε, να υποστηρίξει οικονομικά την περάτωση των μεταπτυχιακών μου σπουδών και στους **γονείς μου** για την προτεραιότητα που έχουν δώσει στην μόρφωση.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ ΚΑΙ ΠΕΡΙΛΗΨΗ

Η θεωρία πολυπλοκότητας παραδοσιακά ενδιαφέρεται περισσότερο για άνω φράγματα στην πολυπλοκότητα ενός αλγορίθμου και μιλά λιγότερο για την ανάλυση της μέσης πολυπλοκότητας. Υπάρχουν βέβαια αλγόριθμοι με μεγάλα άνω φράγματα, αλλά πολύ πιο γρήγοροι στην πράξη από άλλους με μικρότερα. Έτσι είναι πολύ ενδιαφέρον να έχουμε την μέση πολυπλοκότητα ενός αλγορίθμου ή ακόμα καλύτερα και την ασυμπτωτική κατανομή της και να μπορούμε να την συγκρίνουμε με την πολυπλοκότητα του «χειρότερου παραδείγματος».

Ο Αλγόριθμος που θα αναλύσουμε γράφτηκε για πρώτη φορά στα στοιχεία του Ευκλείδη. Βρίσκει το μέγιστο κοινό διαιρέτη δύο αριθμών με μοναδικό εργαλείο την αφαίρεση, μια από τις δύο πιο απλούστερες και εύκολες στη υλοποίηση από έναν υπολογιστή πράξεις. Αν επιτρέψουμε μία ακόμη πράξη, τη διαίρεση τότε πολλά αφαιρετικά βήματα μπορούν να αντικατασταθούν από μία διαίρεση.

Ο Khintchin χρησιμοποιούσε τα συνεχή κλάσματα για να αντλήσει αποτελέσματα για τη θεωρία μέτρου. Ο Heilbronn ενδιαφέρθηκε για μια αριθμοθεωρητική ερώτηση που όπως γράφει στο [4] του έθεσε ο J. Gillis: «Ποιό είναι το μέσος μήκος μιας οικογένειας συνεχών κλασμάτων;». Μέσα στην απόδειξη αυτή του Heibronn βρέθηκε η ανάλυση της μέσης πολυπλοκότητας του Ευκλειδείου Αλγορίθμου και η ιδέα για το πώς θα μετρηθεί ο μέσος αριθμός βημάτων του Αφαιρετικού Ευκλειδείου Αλγορίθμου [6]. Η Vallé [12][2004] χρησιμοποιεί εντελώς διαφορετικές μεθόδους (Tauberian analysis) και βρίσκει μια ενιαία μέθοδο για την ασυμπτωτική ανάλυση πολλών αλγορίθμων που περιγράφονται όλοι με ανάλυση σε ειδικού κάθε φορά είδους συνεχή κλάσματα. Για μια ακόμα φορά στα μαθηματικά, ξεχασμένα αποτελέσματα αποκτούν νέα αξία υπό το πρίσμα νέων θεωριών και η οριακή περιοχή μεταξύ δύο κλάδων δίνει αυτά που ο καθένας ξεχωριστά αδυνατούν να δώσουν, ενώ μια μέθοδος που έδωσε πολλά σημαντικά αποτελέσματα, είναι σκόπιμο να αντικατασταθεί από μια νέα.

Η εργασία αυτή ξεκινά με μια εισαγωγή στα συνεχή κλάσματα. Στη συνέχεια γίνεται μια σύντομη επισκόπηση στις έννοιες της Θεωρίας Αριθμών που θα χρειαστούμε για το Κεφάλαιο 3. Τέλος στο Κεφάλαιο 3 γίνεται μια αναλυτική παρουσίαση του άρθρου [6], που ξεδιαλύνει πολλά σημεία που στην αρχική δημοσίευση ήταν δοσμένα πολύ περιληπτικά.

Α. Μια εισαγωγή στα συνεχή κλάσματα

Α.1. Πεπερασμένα συνεχή κλάσματα. Ένα **πεπερασμένο συνεχές κλάσμα** είναι μια έκφραση της μορφής

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \ddots + \cfrac{1}{x_N}}},$$

με μεταβλητές $x_1, x_2, \ldots, x_n$. Ένα συνεχές κλάσμα μπορεί να θεωρηθεί σαν στοιχείο του σώματος των ρητών συναρτήσεων $R(x_1, \ldots, x_n, \ldots)$ όπου R είναι ένας δακτύλιος με μονάδα.

Για μεγαλύτερη ευκολία θα χρησιμοποιήσουμε το συμβολισμό

$$/x_0, x_1, \ldots, x_N/ = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \ddots + \cfrac{1}{x_N}}}.$$

Οι μεταβλητές $x_0, x_1, \ldots, x_n$ μπορούν γενικά να πάρουν τιμές στο $\mathbb{R}, \mathbb{C}, \mathbb{Z}$ ή στο $\mathbb{N}$. Ωστόσο εμείς τις περισσότερες φορές θα τους δίνουμε τιμές που ανήκουν στο $\mathbb{N}$ ή στο $\mathbb{Z}$.

Ορισμος Α.1. Τα συνεχή κλάσματα μπορούν να να οριστούν αναδρομικά ως εξής:

$$/x_0/ = x_0,$$
$$/x_0, \ldots, x_{n+1}/ = x_0 + \frac{1}{/x_1, \ldots, x_{n+1}/}.$$

Κατ' αυτόν τον τρόπο:

$$/x_0, x_1/ = x_0 + \frac{1}{x_1} = \frac{x_0 x_1 + 1}{x_1}$$

$$/x_0, x_1, x_2/ = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2}} = \frac{x_0 x_1 x_2 + x_2 + x_0}{x_2 x_1}.$$

Ορισμος Α.2. Καλούμε τα $x_0, x_1, \cdots, x_n$ **μερικά πηλίκα** ή απλά πηλίκα του συνεχούς κλάσματος.

Ορισμος Α.3 (1Α.3). Για $m \leq N$ καλούμε το

$$r_m = /x_m, x_{m+1}, \cdots, x_N/ \tag{1}$$

το **m-οστό πλήρες πηλίκο** του συνεχούς κλάσματος $/x_0, x_1, \cdots, x_N/$.

Ορισμος Α.4. Ορίζουμε αναδρομικά τα πολυώνυμα $Q_n(x_1, x_2, \ldots, x_n)$ σε n μεταβλητές, για $n \geq 0$ ως εξής:

(2)

$$Q_n(x_1, x_2, \ldots, x_n) = \begin{cases} 1 & \text{αν } n = 0 \\ x_1 & \text{αν } n = 1 \\ x_1 Q_{n-1}(x_2, \ldots, x_n) + Q_{n-2}(x_3, \ldots, x_n) & \text{αν } n > 1 \end{cases}$$

Θεωρημα Α.5 (L. Euler,1A.5). *Το πολυώνυμο $Q_n(x_1, x_2, \ldots, x_n)$ είναι το άθροισμα όλων των όρων που μπορούν να κατασκευαστούν ξεκινώντας από το γινόμενο:*

$$1 \cdot x_1 \cdot x_2 \cdots x_n$$

και παραλείποντας 0 ή περισσότερα μη επικαλυπτόμενα ζευγάρια διαδοχικών μεταβλητών $x_j \cdot x_{j+1}$.

Κατ' αυτόν τον τρόπο παίρνουμε:

$$\begin{aligned} &Q_1(x_1) = x_1 \\ &Q_2(x_1, x_2) = x_1 x_2 + 1 \\ &Q_3(x_1, x_2, x_3) = x_1 x_2 x_3 + x_1 + x_3 \\ &Q_4(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4 + x_1 x_4 + x_3 x_4 + x_1 x_2 + 1. \end{aligned}$$

Ορισμος Α.6. Ορίζουμε την ακολουθία $(F_n)_{n \in \mathbb{N}}$ των αριθμών Fibonacci ως εξής:

$$F_0 = 0, \quad F_1 = 1$$
$$F_{n+2} = F_{n+1} + F_n, \text{ για } n \geq 0.$$

Θεωρημα Α.7. *Το πλήθος των όρων που αθροίζονται στο πολυώνυμο $Q_n(x_1, x_2, \ldots, x_n)$ ισούται με τον αριθμό Fibonacci F_{n+1}.*

Τα Q-πολυώνυμα εμφανίζουν την εξής συμμετρία:

$$Q_{n+1}(x_0, x_1, \ldots, x_n) = Q_{n+1}(x_n, \ldots, x_1, x_0).$$

Αυτό αποτελεί άμεση συνέπεια του Θεωρήματος Α.5: η συγκεκριμένη μετάθεση των μεταβλητών του Q-πολυωνύμου δεν επηρεάζει τα ζεύγη διαδοχικών όρων ενώ επιπλέον είναι και η μοναδική μετάθεση με αυτή την ιδιότητα. Συνεπώς για $n \geq 2$,

$$Q_n(x_1, x_2, \ldots, x_n) = x_n Q_{n-1}(x_1, \ldots, x_{n-1}) + Q_{n-2}(x_1, \ldots, x_{n-2}).$$

Η βασική ιδιότητα την οποία θα χρησιμοποιήσουμε επανειλημμένα στη συνέχεια είναι:

ΘΕΩΡΗΜΑ A.8 (1A.8).

$$/x_0, x_1, \ldots, x_n/ = \frac{Q_{n+1}(x_0, x_1, \ldots, x_n)}{Q_n(x_1, x_2, \ldots, x_n)}, \quad (n \leq N).$$

A.2. Από τα Q-πολυώνυμα στα συνεχή κλάσματα. Ωστόσο τις περισσότερες φορές δεν μας ενδιαφέρει η μελέτη ενός συνεχούς ως παράστασης με μεταβλητές $x_1, \ldots, x_n$, αλλά ως αναπαράσταση ενός πραγματικού (ή μιγαδικού) αριθμού. Τότε θα συμφωνήσουμε να συμβολίζουμε τα μερικά πηλίκα ως $a_1, \ldots, a_n$ ώστε να φαίνεται ότι πρόκειται για αριθμούς και όχι για μεταβλητές. Επίσης ορίζουμε τις ακολουθίες p_n, q_n ως εξής:

ΟΡΙΣΜΟΣ A.9 (1C.1). Για κάθε ακολουθία ακεραίων $a_0, a_1, \ldots, a_N$ και για κάθε n με $0 \leq n \leq N$ θέτουμε:

$$p_n = Q_{n+1}(a_0, a_1, \ldots, a_n)$$
$$q_n = Q_n(a_1, a_2, \ldots, a_n).$$

Τα $\dfrac{p_n}{q_n}$ καλούνται n-οστοί **κύριοι συγκλίνοντες αριθμοί** (principal convergents), ή απλά συγκλίνοντες του συνεχούς κλάσματος $/a_0, \ldots, a_N/$.

Είναι βολικό να ορίσουμε μερικούς ακόμη βοηθητικούς όρους:

$$p_{-2} = 0, \quad p_{-1} = 1, \quad q_{-2} = 1, \quad q_{-1} = 0, \quad q_0 = 1.$$

Από το Θεώρημα A.8:

$$/a_0, a_1, ..., a_n/ = \frac{p_n}{q_n}, \quad (n \leq N).$$

Είναι τώρα πολύ εύκολο να χρησιμοποιήσουμε τα γενικά αποτελέσματα για τα Q-πολυώνυμα ώστε να συνάγουμε αποτελέσματα για τις ακολουθίες p_n και q_n (βλέπε τον Ορισμό A.9) και το συνεχές κλάσμα $/a_1, \ldots, a_n/$. Αυτή είναι η προσέγγιση που ακολουθείται και στα [7] και [11] ενώ όλα τα άλλα βιβλία της βιβλιογραφίας δεν ορίζουν καθόλου τα Q-πολυώνυμα αλλά ξεκινούν ορίζοντας απευθείας τις ακολουθίες p_n και q_n. Ωστόσο η μελέτη των Q-πολυωνύμων δεν δίνει μόνο μια πληρέστερη γενική εικόνα, αλλά έχει ενδιαφέρον ακόμα και ανεξάρτητα από αυτό το συγκεκριμένο πλαίσιο αν μάλιστα σκεφτεί κανείς το Θεώρημα A.5 και τη στενή σχέση με τους αριθμούς Fibonacci.

ΘΕΩΡΗΜΑ A.10 (1C.2). *Για $n \geq 0$ και p_n, q_n όπως στον Ορισμό A.9,*

$$p_0 = a_0, \qquad p_n = a_n p_{n-1} + p_{n-2}, \tag{3}$$
$$q_0 = 1, \qquad q_n = a_n q_{n-1} + q_{n-2}, \tag{4}$$

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}, \tag{5}$$

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_{n-1}q_n}, \tag{6}$$

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n, \tag{7}$$

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_{n-2}q_n}. \tag{8}$$

Πορισμα Α.11. *Αν τα r_n είναι όπως στην σχέση (1), τότε για $2 \leq n \leq N$,*

$$/a_0, \dots, a_n/ = \frac{p_n}{q_n} = \frac{r_n p_{n-1} + p_{n-2}}{r_n q_{n-1} + q_{n-2}}.$$

Α.3. Απλά συνεχή κλάσματα.

Ορισμος Α.12. Ένα συνεχές κλάσμα $/a_0, a_1, \dots, a_N/$ είναι **απλό** αν τα $a_0, \dots, a_N$ είναι ακέραιοι και

$$a_0 \geq 0, a_1 > 0, \dots, a_n > 0.$$

Θα έχουμε πάντα αυτή την υπόθεση για το υπόλοιπο αυτού του Κεφαλαίου.

Θεωρημα Α.13. *Για $n > 2$, $q_n > q_{n-1}$, και για $n \geq 1$, $q_n \geq q_{n-1}$.*

Θεωρημα Α.14. *Για $n > 3$, $q_n > n$ και για $n \geq 1$, $q_n \geq n$.*

Θεωρημα Α.15. *Για $n \geq 0$, οι αριθμοί $Q_{n+1}(a_0, a_1, \dots, a_n)$ και $Q_n(a_1, a_2, \dots, a_n)$ είναι σχετικά πρώτοι.*

Χρησιμοποιώντας τον Ορισμό Α.9, αυτό απλά λέει ότι $(p_n, q_n) = 1$.

Το επόμενο θεώρημα αποδεικνύει ότι τα q_n μεγαλώνουν εκθετικά ως προς n. Για περισσότερα σχετικά με την ασυμπτωτική συμπεριφορά των q_n μπορεί κανείς να ανατρέξει στα [10].

Θεωρημα Α.16 ([5]). *Για όλα τα $n \geq 2$, $q_n \geq 2^{\frac{n-1}{2}}$.*

Θεωρημα Α.17. *Κάθε περιττός συγκλίνων είναι μεγαλύτερος από κάθε άρτιο.*

Παρατηρούμε ότι:

$$/a_0, a_1, ..., a_n, 1/ = /a_0, a_1, ..., a_n + 1/. \tag{9}$$

Θεωρημα Α.18 ([3],1D.10). *Αν δύο απλά συνεχή κλάσματα $/a_0, a_1, ..., a_N/$ και $/b_0, b_1, ..., b_M/$ έχουν την ίδια τιμή x και $a_N > 1$, $b_M > 1$ τότε έχουμε $M = N$ και τα συνεχή κλάσματα είναι ίδια, δηλ. αποτελούνται από την ίδια ακολουθία μερικών πηλίκων.*

Remark Α.19. Χρησιμοποιώντας την (9), βλέπουμε ότι το προηγούμενο Θεώρημα μοναδικότητας ισχύει επίσης και στην περίπτωση που έχουμε $a_N = 1, b_N = 1$.

A.4. Πόσο κοντά στο συνεχές κλάσμα είναι οι συγκλίνοτές; Όπως και πριν έχουμε $a_i > 0$ για $i \geq 0$, $x = /a_0, \dots, a_N/$ και $r_n = /a_n, \dots, a_N/$.

ΘΕΩΡΗΜΑ A.20. *Αν $N > 1, n > 0$, τότε οι διαφορές*

$$x - \frac{p_n}{q_n}, \qquad q_n x - p_n$$

φθίνουν σταθερά κατ' απόλυτη τιμή καθώς το n μεγαλώνει. Επιπλέον

$$q_n x - p_n = \frac{(-1)^n \delta_n}{q_{n+1}}, \tag{10}$$

όπου

$$0 < \delta_n < 1, \quad \textit{για} \quad 1 \leq n \leq N-2, \quad \delta_{N-1} = 1$$

και

$$\left|x - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{{q_n}^2} \tag{11}$$

για $n \leq N-1$. Και οι δύο ανισότητες είναι αυστηρές, εκτώς από την περίπτωση που $n = N-1$.

A.5. Άπειρα απλά συνεχή κλάσματα. Σε αυτή τη ενότητα θα ορίσουμε τα άπειρα συνεχή κλάσματα Τα αρχικά τμήματα των άπειρων συνεχών κλασμάτων είναι πεπερασμένα συνεχή κλάσματα. Θα ακολουθήσουμε σε βασικές γραμμές την παρουσίαση του [3]. Για περισσότερα σχετικά με τα ενδιάμεσα συνεχή κλάσματα μπορεί κανείς να ανατρέξει στα [5] και [11].

ΟΡΙΣΜΟΣ A.21. Έστω $a_0, a_1, a_2, \dots$ μια άπειρη ακολουθία ακεραίων με $a_1 > 0, a_2 > 0, \dots$. Τότε το $x_n = /a_0, a_1, \dots, a_n/$ είναι για κάθε n, ένα απλό συνεχές κλάσμα που αναπαριστά έναν ρητό αριθμό x_n. Αν ο x_n τείνει στο όριο x καθώς $n \to \infty$ τότε λέμε ότι το *άπειρο απλό συνεχές κλάσμα* $/a_0, a_1, a_2, \dots/$ *συγκλίνει στην τιμή* x και γράφουμε

$$x = /a_0, a_1, a_2, \dots/.$$

ΘΕΩΡΗΜΑ A.22. *Όλα τα άπειρα συνεχή κλάσματα συγκλίνουν.*

Συνεπώς, για κάθε n, οι n-οστοί συγκλίνοντες ενός άπειρου συνεχούς κλάσματος σχηματίζουν μια αυστηρά φθίνουσα ακολουθία η οποία συγκλίνει στο x. Για n περιττό, οι n-οστοί συγκλίνοντες του α σχηματίζουν μια αυστηρά φθίνουσα ακολουθία που συγκλίνει στο x. Άρα αν $x = /a_0, a_1, \dots/$ τότε:

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \dots < \frac{p_{2m}}{q_{2m}} < \dots < x < \dots < \frac{p_{2n+1}}{q_{2n+1}} < \dots < \frac{p_5}{q_5} < \frac{p_1}{q_1} \quad \textit{και}$$

$$\lim_{n \to \infty} \frac{p_{2n}}{q_{2n}} = \lim_{n \to \infty} \frac{p_{2n+1}}{q_{2n+1}}.$$

ΟΡΙΣΜΟΣ Α.23. Για κάθε θετικό ακέραιο r με $1 \leq r \leq a_{n+1}$ ονομάζουμε το κλάσμα

$$\frac{p_n r + p_{n-1}}{q_n r + q_{n-1}}$$

ενδιάμεσο κλάσμα.

ΘΕΩΡΗΜΑ Α.24. *Αν $x = /a_0, a_1, \ldots /$ τότε η ακολουθία*

$$\frac{p_{n-1}}{q_{n-1}}, \frac{p_n + p_{n-1}}{q_n + q_{n-1}}, \frac{2p_n + p_{n-1}}{2q_n + q_{n-1}}, \ldots, \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}$$

είναι μονότονη: αύξουσα για περιττό n και φθίνουσα για άρτιο n.

Α.6. Συνεχή κλάσματα και Ευκλείδιος Αλγόριθμος. Σε αυτή την ενότητα θα συμβολίζουμε το διατεταγμένο ζεύγος με πρώτο στοιχείο το x και δεύτερο το y με $\{x, y\}$.

ΘΕΩΡΗΜΑ Α.25 (Θεώρημα της Διαίρεσης για φυσικούς αριθμούς). *Εάν $x \geq y > 0$ και $x, y \in \mathbb{N}$, τότε υπάρχουν μοναδικοί αριθμοί $q \in \mathbb{N}$ και $\upsilon \in \mathbb{N}$ τέτοιοι ώστε*

$$x = yq + \upsilon \quad \text{και} \quad 0 \leq \upsilon < y.$$

Συμβολίζουμε το υπόλοιπο υ αυτής της διαίρεσης με $rem(x, y)$.

ΘΕΩΡΗΜΑ Α.26 (Θεώρημα της Διαίρεσης για πραγματικούς, με $q \in \mathbb{N}$). *Εάν $x \geq y > 0$ και $x, y \in \mathbb{R}$, τότε υπάρχουν μοναδικοί αριθμοί $q \in \mathbb{N}$ και $\upsilon \in \mathbb{R}$ τέτοιοι ώστε*

$$x = yq + \upsilon \quad \text{και} \quad 0 \leq \upsilon < y.$$

Επιπλέον,

$$q = \lfloor \frac{x}{y} \rfloor. \tag{12}$$

Συμβολίζουμε το υπόλοιπο υ αυτής της διαίρεσης με $rem(x, y)$.

ΟΡΙΣΜΟΣ Α.27. Έστω δύο φυσικοί αριθμοί x, y. Λέμε ότι ο y **διαιρεί** τον x και γράφουμε $y \mid x$, αν και μόνο αν $rem(x, y) = 0$, και συμβολίζουμε τον **μέγιστο κοινό διαιρέτη** δύο φυσικών αριθμών x, y με (x, y).

Αλγόριθμος ανάπτυξης σε συνεχές κλάσμα. Σε κάθε πραγματικό αριθμό x αντιστοιχούμε δύο πεπερασμένες ή άπειρες ακολουθίες ακεραίων $a_0, a_1, \ldots$ και $\xi_0, \xi_1, \ldots$ πραγματικών ως εξής:

1. Έστω $a_0 = \lfloor x \rfloor, \quad \xi_0 = x - a_0$.

2. Αν έχουν οριστεί τα $a_0, \ldots, a_n, \xi_0, \ldots, \xi_n$, και $\xi_n \neq 0$, τότε θέσε

$$a_{n+1} = \lfloor \frac{1}{\xi_n} \rfloor, \qquad \xi_{n+1} = \frac{1}{\xi_n} - a_{n+1}$$

3. Αν $\xi_n = 0$ τότε ο αλγόριθμος τερματίζει και αποδίδει τα $a_0, a_1, \ldots, a_n$ και τα $\xi_0, \ldots, \xi_n$.

REMARK A.28. Παρατηρείστε ότι ο αλγόριθμος επιστρέφει επιπλέον και τα πλήρη πηλίκα $r_n = /a_n, \ldots, a_N/$ του x, αφού για $\xi_m \neq 0$,

$$r_m = \frac{1}{\xi_m}.$$

Ας δούμε όμως τί ακριβώς κάνει ο αλγόριθμος. Όσο είναι $\xi_n \neq 0$, αυτός ο ορισμός εγγυάται ότι $0 \leq \xi_{n+1} < 1$ έτσι που ο $a_{n+1} = \lfloor \frac{1}{\xi_n} \rfloor$ είναι ένας θετικός ακέραιος αυστηρά μεγαλύτερος του 1.

Εάν $\xi_n = 0$ τότε οι ποσότητες a_{n+1} και ξ_{n+1} δεν ορίζονται και ο αλγόριθμος σταματάει, επιστρέφοντας την ακολουθία $a_0, a_1, \ldots, a_n$ οπότε το συνεχές κλάσμα που αντιστοιχεί στο x είναι το $/a_0, a_1, \ldots, a_n/$ και ο x είναι ρητός.

Μπορεί κανείς να έχει μια καλύτερη εικόνα για το πως λειτουργεί ο αλγόριθμος εάν γράψει τα τρία πρώτα βήματά του:

$$x = a_0 + \xi_0 = a_0 + \frac{1}{a_1 + \xi_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \xi_2}} = \ldots.$$

ΘΕΩΡΗΜΑ A.29 (1G.5). *Εάν $n \geq 0$, και $a_n, \xi_n > 0$ είναι η ακολουθία που αντιστοιχίζει στο x ο αλγόριθμος ανάπτυξης σε συνεχές κλάσμα, τότε*

$$x = /a_0, \ldots, a_n + \xi_n/.$$

ΘΕΩΡΗΜΑ A.30 (Ορθότητα Αλγόριθμου ανάπτυξης σε συνεχές κλάσμα). (1G.6) *Για την ακολουθία $a_0, a_1, \ldots, a_n$ που αντιστοιχίζει στο x ο αλγόριθμος ανάπτυξης σε συνεχές κλάσμα, έχουμε ότι:*

(a) Αν x ρητός τότε ο αλγόριθμος τερματίζει με $\xi_N = 0$ για κάποιο $N \geq 0$ και είναι $x = /a_0, \ldots, a_N/$, (με $a_N > 1$ εάν $N \neq 0$).

(b) Αν x άρρητος, τότε $\xi_n \neq 0$ για όλα τα n, οπότε ο αλγόριθμος δεν τερματίζει, και

$$x = \lim_{n\to\infty} /a_0, a_1, \ldots, a_n/.$$

Εάν κάνουμε εφαρμόσουμε τον αλγόριθμο ανάπτυξης σε συνεχές κλάσμα για κάποιους γνώριμους αριθμούς παίρνουμε:

$\frac{423}{720} = /1, 1, 2, 2, 1, 4/,$

$\pi = /3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, 1, 84, 2, 1, 1, 15, \ldots/,$

$e = /2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14, 1, 1, 16, 1, 1, \ldots/,$

$\phi = /1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, \ldots/,$

όπου $\phi = \dfrac{1+\sqrt{5}}{2}$.

Θεωρημα Α.31. *Κάθε ρητός αριθμός x μπορεί να αναπαρασταθεί με ένα πεπερασμένο συνεχές κλάσμα. Επιπλέον αυτή η αναπαράσταση είναι μοναδική εάν απαιτήσουμε να είναι $a_N > 1$.*

Proof. Από το θεώρημα Α.30 έχουμε μία πεπερασμένη αναπαράσταση του x με συνεχές κλάσμα. Από το Θεώρημα Α.18 έχουμε ότι αυτή είναι μοναδική. ⊣

Θα διατυπώσουμε τώρα τον Ευκλείδιο Αλγόριθμο και θα δούμε ότι ο αλγόριθμος ανάπτυξης του x σε συνεχές κλάσμα μπορεί να διατυπωθεί σαν μια ειδική περίπτωση του Ευκλειδείου Αλγορίθμου όταν αυτός εφαρμοστεί σε δύο αριθμούς $x, y \in \mathbb{R}$.

Ευκλείδειος Αλγόριθμος. Σε κάθε ζεύγος πραγματικών αριθμών $\{x, y\}$ με $x \geq y > 0$ αναθέτουμε δύο πεπερασμένες ή άπειρες ακολουθίες $a_1, a_2, a_3, \ldots$ και $\upsilon_{-1}, \upsilon_0, \upsilon_1, \upsilon_2, \ldots$ ως εξής:

1. Έστω $\upsilon_{-1} = x$, $\upsilon_0 = y$

2. Αν τα $\upsilon_{-1}, \ldots, \upsilon_i, a_1, \ldots, a_i$ έχουν ορισθεί και $\upsilon_i \neq 0$ τότε από το Θεώρημα της Διαίρεσης, πάρε υ_{i+1}, a_{i+1} τέτοια ώστε
$$\upsilon_{i-1} = \upsilon_i a_{i+1} + \upsilon_{i+1} \qquad 0 \leq \upsilon_{i+1} < \upsilon_i.$$
3. Αν $\upsilon_i = 0$ τότε ο αλγόριθμος τερματίζει και αποδίδει $\upsilon_{-1}, \upsilon_0, \ldots, \upsilon_{i-1}$ και $a_1, \ldots, a_i$.

Ο ευκλείδιος αλγόριθμος δουλεύει για το ζεύγος $\{x, y\}$ ώς εξής:
$$\begin{aligned}
x &= y\ a_1 + \upsilon_1 & 0 &< \upsilon_1 < y\\
y &= \upsilon_1 a_2 + \upsilon_2 & 0 &< \upsilon_2 < \upsilon_1\\
\upsilon_1 &= \upsilon_2 a_3 + \upsilon_3 & 0 &< \upsilon_3 < \upsilon_2\\
&\vdots & &\vdots\\
\upsilon_{n-3} &= \upsilon_{n-2} a_{n-1} + \upsilon_{n-1} & 0 &< \upsilon_{n-1} < \upsilon_{n-2}\\
\upsilon_{n-2} &= \upsilon_{n-1} a_n & \upsilon_n &= 0.
\end{aligned}$$
Αν x, y είναι θετικοί ακέραιοι, τότε ξέρουμε ότι ο αλγόριθμος τερματίζει αφού τα υπόλοιπα σχηματίζουν μια αυστηρά φθίνουσα ακολουθία θετικών ακεραίων, οπότε για κάποιο $n \in \mathbb{N}$ θα είναι $\upsilon_{n+1} = 0$. Αν ωστόσο τα x, y είναι πραγματικοί, μπορεί ο αλγόριθμος να μην τερματίζει, και τότε όλα τα υπόλοιπα είναι γνήσια μεγαλύτερα του 0.

Επιπλέον αν x, y είναι θετικοί ακέραιοι, τότε το τελευταίο θετικό υπόλοιπο υ_{i-1} ισούται με τον μέγιστο κοινό διαιρέτη των x και y. Αυτό μπορεί κανείς να το δει αν λάβει υπόψιν του την παρακάτω απλή παρατήρηση: αν
$$x = yq + \upsilon \quad \text{with} \quad 0 \leq \upsilon < y,$$

τότε τα ζευγάρια $\{x, y\}$ και $\{y, \upsilon\}$ έχουν ακριβώς τους ίδιους κοινούς διαιρέτες.

Θεωρημα A.32. *(a) Αν υλοποιήσουμε τον Ευκλείδειο Αλγόριθμο για το ζεύγος* $\{x, 1\}$ *τότε* $x = /a_1, \ldots, a_n, \ldots /$ *όπου* $a_0, \ldots, a_n, \ldots$ *είναι τα πηλίκα που εμφανίζονται στον Ευκλείδειο Αλγόριθμο.*

(b) Αν $x = \dfrac{h}{k}$ *με* $h \geq k$*, τα ίδια πηλίκα θα εμφανιστούν και αν υλοποιήσουμε τον Ευκλείδειο Αλγόριθμο για το ζεύγος* $\{h, k\}$.

Αξίζει να παρατηρήσει κανείς ότι ο λόγος για τον οποίο τα a_n καλούνται μερικά πηλίκα είναι ότι συμπίπτουν με τα πηλίκα τα οποία εμφανίζονται στον Ευκλείδειο Αλγόριθμο για το ζευγάρι $\{x, 1\}$.

Η αναπαράσταση που μας δίνει ο αλγόριθμος ανάπτυξης σε συνεχές κλάσμα μας δίνει τη δυνατότητα να αναπαριστούμε έναν πραγματικό αριθμό με τον βαθμό ακρίβειας, δηλαδή το μήκος συνεχούς κλάσματος, που θα επιλέξουμε. Η άλλη αναπαράσταση που χρησιμοποιούμε συνήθως για τους πραγματικούς αριθμούς είναι η δεκαδική. Στο Εδάφιο 1J θα αποδείξουμε ότι οι προσεγγίσεις με συνεχή κλάσματα έχουν την ιδιότητα να είναι **βέλτιστες προσεγγίσεις (best approximations)** των αριθμών, ιδιότητα η οποία έχει ιδιαίτερη σημασία για την θεωρητική έρευνα. Παρ' όλ' αυτά όμως αποδεικνύεται ότι είναι περίπλοκο το να κάνει κανείς πράξεις με συνεχή κλάσματα (βλέπε Hurwitz 1891).

B. Ανάλυση μέσης πολυπλοκότητας του Αφαιρετικού Ευκλειδείου αλγορίθμου

Σε αυτό το μέρος της διπλωματικής εργασίας θα επιθέσουμε την απόδειξη ενός ασυμπτωτικού τύπου για την μέση πολυπλοκότητα του αφαιρετικού Ευκλειδείου αλγορίθμου, το φημισμένο αποτέλεσμα των Yao-Knuth από την δημοσίευση [6].

B.1. Προκαταρκτικά. Τα αποτελέσματα που θα χρησιμοποιήσουμε και έχουν σχέση με συνεχή κλάσματα θα είναι πολύ λίγα, ωστόσο είναι σημαντικό να έχει κανείς μια γενικότερη εξοικείωση με τα συνεχή κλάσματα καθώς και τα Q-πολυώνυμα για να κατανοήσει τις αποδείξεις του πρώτου μέρους αυτού του κεφαλαίου.

Αφαιρετικός Ευκλείδιος αλγόριθμος. Δοθέντων δύο αριθμών, αντικαθιστούμε επανειλημμένα τον μεγαλύτερο από τους δύο με την διαφορά των δύο μέχρι και οι δύο αριθμοί να είναι ίσοι. Ο μέγιστος κοινός διαιρέτης των δύο αριθμών είναι η κοινή τιμή.

Για παράδειγμα:

$$\{18, 42\} \to \{18, 42-18=24\} \to \{18, 24-18=6\} \to \{18-6=12, 6\} \\ \to \{12-6=6, 6\}.$$

επομένως η απάντηση είναι 6, ενώ ο αριθμός των αφαιρετικών βημάτων είναι 4.

Ο αφαιρετικός Ευκλείδιος Αλγόριθμος μπορεί να διατυπωθεί πιο αυστηρά ως εξής:

1. Αν $u = 1$ ή $v = 1$ σταμάτα αποδίδοντας το 1 ως απάντηση.
2. Αν $u = v$, σταμάτα αποδίδοντας το u ως απάντηση.
3. Αν $u > v$ θέσε $u \leftarrow u - v$ και πήγαινε στο 1.
4. Αν $u < v$ θέσε $v \leftarrow v - u$ και πήγαινε στο 1.

Στο παράδειγμα μας ο Ευκλείδιος αλγόριθμος με χρήση διαίρεσης είναι:

$$42 = 18 \cdot 2 + 6$$
$$18 = 6 \cdot 3 + 0$$

η ανάλυση του $\frac{18}{42}$ σε συνεχές κλάσμα είναι:

$$\frac{18}{42} = 0 + \cfrac{1}{2 + \cfrac{1}{3}} = 0 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1}}} = /0, 2, 2, 1/$$

$$q_1 = 2, \quad q_2 = 2$$

Ο αριθμός των αφαιρετικών βημάτων είναι 2+2=4. Αυτό είναι λογικό: το να διαιρέσουμε δύο αριθμούς n, m τέτοιους ώστε $n = q \cdot m + r$, $0 \le r < n$ είναι το ίδιο με το να αφαιρούμε το m από το n, q φορές. (Θυμηθείτε ότι τα μερικά πηλίκα στον αλγόριθμο ανάπτυξης ενός αριθμού σε συνεχές κλάσμα δεν είναι άλλα από τα πηλίκα στον Ευκλείδιο Αλγόριθμο.)

Επομένως η διαίρεση $42 = 18 \cdot 2 + 6$ αντιστοιχεί στις εξής δύο αφαιρέσεις:

$$\{18, 42-18=24\} \to \{18, 24-18=6\},$$

ενώ η διαίρεση $18 = 6 \cdot 2 + 6$ αντιστοιχεί στις εξής δύο αφαιρέσεις:

$$\{18-6=12, 6\} \to \{12-6=6, 6\}.$$

Στο παράδειγμά μας οι δύο δυνατές αναλύσεις σε συνεχή κλάσματα είναι $/0, 2, 2, 1/$ και $/0, 2, 3/$. Ο λόγος για τον οποίο επιλέγουμε την ανάλυση $/0, 2, 2, 1/$ και δεν προσθέτουμε το τελευταίο 1 όταν μετράμε τα αφαιρετικά βήματα, είναι πως αν υλοποιήσουμε τον γνωστό Ευκλείδιο αλγόριθμο αντικαθιστώντας κάθε διαίρεση με τις αντίστοιχες αφαιρέσεις, αναγκαζόμαστε να κάνουμε ένα επιπλέον αφαιρετικό βήμα από ότι αν υλοποιούσαμε τον Αφαιρετικό Ευκλείδιο Αλγόριθμο για τον μέγιστο κοινό διαιρέτη. Στο παράδειγμά μας αυτό είναι το $\{6,6\} \to \{6,0\}$. (Ο αφαιρετικός αλγόριθμος τερματίζει όταν οι δύο αριθμοί του ζεύγους είναι ίσοι.)

Ορισμος B.1. Έστω $r = r(m,n)$ ο αριθμός των διαιρέσεων που πραγματοποιεί ο Ευκλείδιος Αλγόριθμος.

Θεωρημα B.2. *Για όλα τα* $n \geq m \geq 2$, $r(m,n) \leq 2\log m$. *Επομένως* $r(m,n) = O(\log n)$.

Ορισμος B.3. Έστω $S(n)$ ο μέσος αριθμός βημάτων για να υπολογίσουμε τον (m,n) με τον Αφαιρετικό Ευκλείδειο Αλγόριθμο, όταν το m κατανέμεται ομοιόμορφα στο διάστημα $1 \leq m \leq n$.

Το κύριο Θεώρημα που θα αποδείξουμε είναι:

Θεωρημα B.4 (Yao and Knuth).

$$S(n) = \frac{6}{\pi^2}(\ln n)^2 + O(\log n(\log\log n)^2)$$

Είναι φανερό ότι αυτή η απόδειξη είναι αποτέλεσμα μιας πολύ προσεκτικής ανάγνωσης και σε βάθος κατανόησης του δημοσιεύματος [4]. Ωστόσο ο Heilbronn προσπάθησε να απαντήσει μια αριθμοθεωρητική ερώτηση, η απόδειξη της οποίας τελικά φάνηκε ότι περιέχει την ανάλυση της μέσης πολυπλοκότητας του (διαιρετικού) Ευκλειδείου αλγορίθμου.

Έστω $\lfloor x \rfloor$ ο μεγαλύτερος ακέραιος που έχει την ιδιότητα να είναι μικρότερος ή ίσος του x.

Τότε $x \bmod y = x - y\lfloor \frac{x}{y} \rfloor$ είναι το υπόλοιπο της διαίρεσης του x με το y.

Αν $1 \leq m \leq n$, τότε από τον αλγόριθμο ανάπτυξης σε συνεχές κλάσμα υπάρχει μοναδική (εξαιτίας του 1 στο τέλος) πεπερασμένη ακολουθία ακεραίων τέτοια ώστε

$$\frac{m}{n} = /0, q_1, q_2, \ldots, q_r, 1/$$

Επιπλέον τα q_i είναι τα πηλίκα που εμφανίζονται στον Ευκλείδειο Αλγόριθμο (που χρησιμοποιεί διαίρεση). Έχουμε $1 \leq m \leq n$, επομένως $\frac{m}{n} \leq 1$ Ας υποθέσουμε ότι η εξίσωση της διαίρεσης για το ζεύγος $\{n,m\}$ είναι:

$$n = q_1 m + r_1, \quad 0 \leq r_1 < m$$

Αν $r_1 = 0$ τότε $\frac{m}{n} = \frac{m}{q_1 m} = \frac{1}{q_1}$.

Αλλιώς αν $r_1 \neq 0$ είναι

$$\frac{m}{n} = \frac{1}{\frac{n}{m}} = \frac{1}{\frac{mq_1 + r_1}{m}} = \frac{1}{q_1 + \frac{r_1}{m}}$$

όπου

$$q_1 = \lfloor \frac{n}{m} \rfloor, \qquad \frac{r_1}{m} = \frac{n \bmod m}{m} < 1.$$

Τώρα αφού $\frac{n \bmod m}{m} < 1$ μπορούμε να συνεχίσουμε τον αλγόριθμο αντικαθιστώντας το $\frac{m}{n}$ με $\frac{n \bmod m}{n}$.

Ο αριθμός των αφαιρέσεων για να υπολογίσουμε τον (m, n) είναι ακριβώς $q_1+q_2+\ldots+q_r$, επειδή αφαιρούμε τον μικρότερο ακέραιο m από τον μεγαλύτερο n «όσες φορές μπορούμε», δηλαδή $q_1 = \lfloor \frac{n}{m} \rfloor$ φορές, δηλαδή αφαιρούμε μέχρι το υπόλοιπο να είναι αυστηρά μικρότερο από τον μεγαλύτερο αριθμό. Τότε κοιτάμε πόσες φορές μπορούμε να αφαιρέσουμε το προηγούμενο υπόλοιπο από τον μικρότερο αριθμό. Έτσι βλέπουμε ότι ο Αφαιρετικός Ευκλείδειος κάνει ακριβώς τους ίδιους υπολογισμούς με τον Ευκλείδιο Αλγόριθμο, αν σε αυτόν υλοποιήσουμε τη διαίρεση με διαδοχικές αφαιρέσεις, έτσι ώστε *κάθε διαίρεση με πηλίκο q αντιστοιχεί σε q αφαιρέσεις του ίδιου αριθμού.* Εκτώς βέβαια από το τελευταίο βήμα, στο οποίο κάνουμε $q-1$ αφαιρέσεις, ώστε να καταλήξουμε σε δύο αριθμούς, που να είναι ίσοι μεταξύ τους (και με το μέγιστο κοινό διαιρέτη), αντί να καταλήξουμε με ένα 0 και το μέγιστο κοινό διαιρέτη.

Έτσι εάν θέσουμε

$$C(m, n) = q_1(m, n) + \ldots + q_{r(m,n)}(m, n)$$

τότε ο μέσος αριθμός βημάτων του Αφαιρετικού Ευκλειδείου αλγορίθμου θα είναι

$$S(n) = \frac{\sum_m C(m, n)}{n} = \frac{\sum_{m=1}^{n} \sum_{i=1}^{r(m,n)} q_i(m, n)}{n} \tag{13}$$

(το m είναι ομοιόμορφα κατανεμημένο στο $[1, n]$ και έτσι η πιθανότητα να πετύχουμε μια συγκεκριμένη τιμή του m είναι $\frac{1}{n}$.)

Στη συνέχεια θα ανάγουμε το πρόβλημα του υπολογισμού του αθροίσματος των πηλίκων q_i, στο πρόβλημα του υπολογισμού του πλήθους των λύσεων της εξίσωσης $xx' + yy' = n$ κάτω από συγκεκριμένες συνθήκες.

Ορισμος Β.5. Για $n \geq 1$, μια τετράδα $\{x, x', y, y'\}$ είναι μια **Η-αναπαράσταση του** n αν

$$n = xx' + yy', \quad (x, y) = 1$$

$$x > y > 0, \qquad x' \geq y' > 0.$$

Το όνομα Η-αναπαράσταση δόθηκε από τους Yao και Knuth προς τιμήν του Hans Heilbronn, μια και είναι μια ελαφρώς τροποποιημένη μορφή μιας αναπαράστασης που όρισε πρώτος ο Heilbronn στο δημοσίευμα [4].

ΘΕΩΡΗΜΑ B.6 (3A.7). *Υπάρχει μια 1-1 αντιστοιχία μεταξύ των H-αναπαραστάσεων του n και των διατεταγμένων ζευγών $\{m, j\}$ όπου*

$$0 < m < \frac{1}{2}n, \quad and \quad 1 \le j \le r(m,n).$$

Επιπλέον εάν η $\{x_j, x'_j, y_j, y'_j\}$ αντιστοιχεί στο ζεύγος $\{m, j\}$, και q_j είναι το $j+1$-οστό μερικό πηλίκο στο συνεχές κλάσμα

$$\frac{m}{n} = /0, q_1, q_2, \dots, q_j, \dots, q_r, 1/,$$

τότε

$$\frac{y_j}{x_j} = /0, q_j, \dots, q_1/ \qquad \frac{y'_j}{x'_j} = /0, q_{j+1}, \dots, q_r, 1/$$

και συνεπώς

$$\lfloor \frac{x_j}{y_j} \rfloor = q_j. \tag{14}$$

Ας σημειωθεί εδώ ότι η απόδειξη στο Θεώρημα B.6 που θα δώσουμε εδώ δεν είναι η ίδια με αυτή που παρουσιάζεται στη δημοσίευση των Yao και Knuth, αλλά είναι πολύ παρόμοια με την απόδειξη που έδωσε ο Heilbronn στο [4] και δίνει μια πολύ καλύτερη εποπτεία για το τί ακριβώς είναι μια H-αναπαράσταση. Οι αναδρομικές ιδιότητες των H-αναπαραστάσεων που αναδεικνύονται από την απόδειξη των Yao και Knuth παρουσιάζονται στο Παράρτημα.

ΠΟΡΙΣΜΑ B.7 (3A.8).

$$nS(n) = 2\sum \lfloor \frac{x}{y} \rfloor + 1 - (n \bmod 2)$$

όπου το άθροισμα είναι για όλες τις H-αναπαραστάσεις του n.

Συμβολίζουμε με

$$\sum{}' \lfloor \frac{x}{y} \rfloor$$

το άθροισμα για όλες τις H-αναπαραστάσεις του n με $x'y < \frac{1}{2}n$.

Τότε ισχύει

$$\sum \lfloor \frac{x}{y} \rfloor = \sum{}' \lfloor \frac{x}{y} \rfloor + O(n \log n). \tag{15}$$

B.2. Αναγωγή του προβλήματος. Το παρακάτω θεώρημα καθορίζει ποιές H-αναπαραστάσεις του n ικανοποιούν την $x'y < \frac{1}{2}n$, και συνεπώς μας δίνει έναν τρόπο να υπολογίσουμε το άθροισμα $\sum' \lfloor \frac{x}{y} \rfloor$.

ΘΕΩΡΗΜΑ B.8. *Αν $x', y > 0$ και $x'y < \frac{1}{2}n$, τότε υπάρχουν H-αναπαραστάσεις (x, x', y, y') του n αν και μόνον αν*

$$(y, n) = (y, x').$$

Και όταν αυτό ισχύει υπάρχουν ακριβώς $(y, n)\prod(1 - p^{-1})$ τέτοιες H-αναπαραστάσεις, όπου το γινόμενο είναι για όλους τους πρώτους p οι οποίοι διαιρούν τον (y, n) αλλά όχι το $\dfrac{y}{(y, n)}$.

ΟΡΙΣΜΟΣ B.9. Έστω

$$P(n) = \frac{\phi(n)}{n} = \prod_{p|n}\Big(1 - \frac{1}{p}\Big)$$

και έστω $P(n \setminus m)$ το παρόμοιο γινόμενο για όλους τους πρώτους που διαιρούν το n αλλά όχι το m, δηλαδή

$$P(n \setminus m) = \prod_{\substack{p|n \\ p\nmid m}}\Big(1 - \frac{1}{p}\Big).$$

ΘΕΩΡΗΜΑ B.10. *Για κάθε $n \geq 2$,*

$$\sum\lfloor\frac{x}{y}\rfloor = \sum_{m|n}\sum_{(j,m)=1} P(\frac{n}{m} \setminus j) \sum_{\substack{(k,j)=1 \\ 1\leq k<\frac{m^2}{2nj}}} \frac{m}{jk} + O(n\log n \cdot \log\log n), \tag{16}$$

όπου το άθροισμα στα αριστερά είναι για όλες τις H-αναπαραστάσεις (x, x', y, y') του n. Επομένως,

$$nS(n) = 2\sum_{m|n}\sum_{(j,m)=1} P(\frac{n}{m} \setminus j) \sum_{\substack{(k,j)=1 \\ 1\leq k<\frac{m^2}{2nj}}} \frac{m}{jk} + O(n\log n \cdot \log\log n). \tag{17}$$

B.3. Ασυμπτωτικοί τύποι. Σε αυτή τη ενότητα θα αποδείξουμε μερικούς ασυμπτωτικούς τύπους τους οποίους στη συνέχεια θα χρησιμοποιήσουμε για να προσεγγίσουμε το $S(n)$. Θα χρησιμοποιήσουμε πολλές θεμελιώδεις ιδέες και έννοιες της θεωρίας αριθμών.

ΛΗΜΜΑ B.11. *Αν p πρώτος αριθμός,*

$$\sum_{p|n}\frac{\log p}{p} = O(\log\log n).$$

ΛΗΜΜΑ B.12.

$$\sum_{d|n}\frac{\mu(d)}{d}\ln(\frac{1}{d}) = \sum_{p|n}\frac{\ln p}{p}P(n \setminus p) = O(\log\log n). \tag{18}$$

ΛΗΜΜΑ B.13.

$$\sum_{d|n} \frac{\ln d}{d} = O\big((\log\log n)^2\big). \tag{19}$$

ΛΗΜΜΑ B.14. *Για κάθε x και κάθε j,*

$$\sum_{\substack{(k,j)=1\\ k<x}} \frac{1}{k} = P(j)\ln x + O(\log\log j).$$

ΟΡΙΣΜΟΣ B.15. Ορίζουμε το $\mu_d(r)$ ως εξής:

$$\mu_d(r) = \begin{cases} \mu(r), & \text{if } (d,r)=1 \\ 0, & \text{αλλιώς.} \end{cases}$$

ΛΗΜΜΑ B.16.

$$\sum_{\substack{(j,m)=1\\ j<x}} \frac{P(j\setminus d)}{j} = P(m)\ln x \sum_{\substack{(r,m)=1\\ r<x}} \frac{\mu_d(r)}{r^2} + O(\log\log m)$$

(λείπει η απόδειξη, 20 Σεπτεμβρίου)

ΛΗΜΜΑ B.17.

$$\sum_{\substack{(j,m)=1\\ j<x}} \frac{P(j\setminus d)\ln j}{j} = \frac{1}{2}P(m)(\ln x)^2 \sum_{\substack{(r,m)=1\\ r<x}} \frac{\mu_d(r)}{r^2} + O(\log x\log\log m).$$

(λείπει η απόδειξη, 20 Σεπτεμβρίου)

B.4. Καταληκτικά βήματα. Από τον ορισμό του $P(n)$ είναι φανερό ότι:

$$P(a\setminus b)P(b) = P(ab) = P(b\setminus a)P(a)$$

Έστω $N = \dfrac{m^2}{2n}$. Από το Θεώρημα B.10, έχουμε ότι

$$\sum \lfloor \frac{x}{y} \rfloor = \sum_{m|n} m \sum_{\substack{(j,m)=1\\ j<N}} \frac{P(\frac{n}{m}\setminus j)}{j} \sum_{\substack{(k,j)=1\\ k<\frac{N}{j}}} \frac{1}{k} + O(n\log n\cdot\log\log n).$$

Χρησιμοποιόντας τα Λήμματα B.14, B.16 και B.17 και μετά από αρκετή δουλειά καταλήγουμε στο ότι

$$\sum \lfloor \frac{x}{y} \rfloor = \frac{1}{2}\sum_{m|n} mP(\frac{n}{m})P(m)(\ln n)^2 \sum_{r<N} \frac{\mu_n(r)}{r^2} + O(n\log n(\log\log n)^2).$$

Μπορούμε να επεκτείνουμε το άθροισμα ως προς r μέχρι το ∞, αφού από την (59) (ή από [3], Theorem 315), έχουμε

$$d(n) = \sum_{m|n} 1 = O(n^{\epsilon}) \quad \text{για κάθε } \epsilon \text{ θετικό}$$

και

$$\sum_{m|n} m \sum_{r\geq N} \frac{1}{r^2} = O(n^{\frac{1}{2}+\epsilon}).$$

Έτσι αφού χρησιμοποιόντας απλά επιχειρήματα του απειροστικού λογισμού $(\ln n)^2 \cdot n^{\frac{1}{2}+\epsilon} = O(n)$, έχουμε

$$\sum \lfloor \frac{x}{y} \rfloor = \frac{1}{2}\sum_{m|n} mP(\frac{n}{m})P(m)(\ln n)^2 \sum_{r\geq 1} \frac{\mu_n(r)}{r^2} + O(n\log n(\log\log n)^2). \tag{20}$$

Ο βασικός τύπος που θα χρειαζόμαστε είναι

$$\sum_{r\geq 1} \frac{\mu_n(r)}{r^2} = \prod_{p\nmid n}\Big(1-\frac{1}{p^2}\Big) = \frac{6}{\pi^2}\prod_{p|n}\Big(1-\frac{1}{p^2}\Big)^{-1}. \tag{21}$$

Βλέπει κανείς ότι εδώ είναι που εμφανίζεται η σταθερά $\frac{6}{\pi^2}$ η οποία ίσως ξενίζει τον αναγνώστη όταν διαβάζει για πρώτη φορά το Θεώρημα B.4.

Μένει απλά να υπολογίσουμε το άθροισμα

$$\sum_{m|n} mP(\frac{n}{m})P(m),$$

το οποίο όμως είναι μια πολλαπλασιαστική συνάρτηση του n πράγμα που σημαίνει ότι αρκεί να την υπολογίσουμε όταν $n = p^k$. Είναι

$$\begin{aligned}\sum_{m|p^k} mP(\frac{p^k}{m})P(m) &= \sum_{0\leq j\leq k} p^j \frac{\phi(p^{k-j})}{p^{k-j}}\frac{\phi(p^j)}{p^j} \\ &= \sum_{0<j<k} p^j\Big(1-\frac{1}{p}\Big)^2 + (p^0+p^k)\Big(1-\frac{1}{p}\Big) \\ &= p^k\Big(1-\frac{1}{p^2}\Big)\end{aligned}$$

Επομένως για $n = {p_1}^{k_1}\cdots {p_l}^{k_l}$, παίρνουμε

$$\begin{aligned}\sum_{m|n} mP(\frac{n}{m})P(m) &= {p_1}^{k_1}\cdots {p_l}^{k_l}\cdot\Big(1-\frac{1}{{p_1}^{2k_1}}\Big)\cdots\Big(1-\frac{1}{{p_l}^{2k_l}}\Big) \\ &= n\cdot\prod_{p|n}\Big(1-\frac{1}{p^2}\Big)\end{aligned}$$

η εξίσωση (20), με χρήση της (21) γίνεται:

$$\begin{aligned}\sum \lfloor \frac{x}{y} \rfloor &= \frac{1}{2}(\ln n)^2 \sum_{m|n} mP(\frac{n}{m})P(m) \cdot \frac{6}{\pi^2} \prod_{p|n} \Big(1 - \frac{1}{p^2}\Big)^{-1} \\ &\qquad + O(n \log n (\log\log n)^2) \\ &= \frac{1}{2}(\ln n)^2 n \cdot \prod_{p|n} \Big(1 - \frac{1}{p^2}\Big) \cdot \frac{6}{\pi^2} \prod_{p|n} \Big(1 - \frac{1}{p^2}\Big)^{-1} \\ &\qquad + O(n \log n (\log\log n)^2).\end{aligned}$$

Έτσι τελικά

$$\sum \lfloor \frac{x}{y} \rfloor = \frac{3}{\pi^2} n (\ln n)^2 + O(n \log n (\log\log n)^2).$$

Και χρησιμοποιόντας το Πόρισμα Β.7, παίρνουμε τελικά το Θεώρημα Β.4:

$$S(n) = \frac{6}{\pi^2}(\ln n)^2 + O(\log n (\log\log n)^2).$$

Παρατηρήσεις. Θα ήταν ιδιαίτερα ενδιαφέρον να αναπαράγουμε κάποιες ιδιαίτερα ενδιαφέρουσες παρατηρήσεις από το βιβλίο [1](δίνει ιδιαίτερα προσεγμένες, εκτενείς και πλήρεις αναφορές στα ερευνητικά αποτελέσματα που σχετίζονται με τις ενότητες που αναλύει) και το άρθρο [12].

Η μετρική θεωρία των συνεχών κλασμάτων θεμελιώθηκε με εργασίες των Gauss, Lévy, Khinchin, Kuzmin Wirsing and Babenko. Ωστόσο αυτά τα αποτελέσματα δεν μπορούν να βοηθήσουν στην ανάλυση του Ευκλειδείου Αλγορίθμου για θετικούς ακεραίους, του διακριτού αναλόγου του αλγορίθμου ανάπτυξης σε συνεχές κλάσμα, αφού οι ρητοί έχουν μέτρο μηδέν στους πραγματικούς αριθμούς. Οι πρώτοι που έδωσαν ανάλυση για τη μέση πολυπλοκότητα του (διαιρετικού) Ευκλειδείου Αλγορίθμου ήταν ο Heilbronn [4] και ο Dixon [1970, 1971] και οι δύο ανεξάρτητα. Ενώ ο Heilbronn χρησιμοποίησε συνδυαστικές μεθόδους, ο Dixon χρησιμοποίησε πιθανοτικές. Ακολούθησαν διάφορες βελτιώσεις του παράγοντα σφάλματος μεταξύ των άλλων και από τον Knuth. Πολύ αργότερα ο Hensley [1992] έδειξε ότι ο αριθμός των διαιρέσεων που πραγματοποιεί ο Ευκλείδιος Αλγόριθμος για όλα τα ζευγάρια (m, n) με $0 < m \leq n \leq x$ ακολουθεί ασυμπτωτικά την κανονική κατανομή, με μέση τιμή περίπου $12(\log 2)\pi^{-2} \log x$.

Ο Plankensteiner [1970] μέτρησε τον αριθμό των ζευγών (m, n) για τα οποία ο Ευκλείδειος Αλγόριθμος πραγματοποιεί ακριβώς k βήματα.

Μια αρκετά διαφορετική προσέγγιση η οποία μπορεί να δώσει αποτελέσματα που αφορούν πολλούς αλγορίθμους παρόμοιους με τον Ευκλείδειο, και η οποία μάλιστα εκτός από τη μέση τιμή της ασυμπτωτικής κατανομής, δίνει και τις ροπές τάξης k προτάθηκε από τη Vallé [12].

CHAPTER 1

AN INTRODUCTION TO CONTINUED FRACTIONS

In this chapter we will present the basic facts about continued fractions. The presentation is mostly influenced by [3] and [7], but also [5] mostly when it comes to good approximations. Another very helpful reference was [11], which offers an excellent overview of the theory of continued fractions, the only drawback being that everything is left as an exercise. As for the book [8] by S. Lang, it presents the really tight connection between continued fractions and diophantine approximation and has an outstanding presentation of the algebraic aspect of equivalent numbers.

1A. Finite continued fractions

A **finite continued fraction** is an expression of the form

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \ddots + \cfrac{1}{x_N}}},$$

in the variables $x_1, x_2, \dots, x_n$. We can formally understand a continued fraction as an element in the field of rational functions $R(x_1, \dots, x_n, \dots)$ where R is a ring with unity.

For convenience we will use the notation

$$/x_0, x_1, \dots, x_N/ = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \ddots + \cfrac{1}{x_N}}}.$$

In general the variables $x_0, x_1, \dots, x_n$ may be evaluated over $\mathbb{R}, \mathbb{C}, \mathbb{Z}$ or $\mathbb{N}$. In most cases we shall evaluate them over $\mathbb{N}$ or $\mathbb{Z}$.

DEFINITION 1A.1. Continued fractions can be defined inductively as follows:

$$/x_0/ = x_0,$$
$$/x_0, \dots, x_{n+1}/ = x_0 + \frac{1}{/x_1, \dots, x_{n+1}/}.$$

In this way we find that:

$$/x_0, x_1/ = x_0 + \frac{1}{x_1} = \frac{x_0 x_1 + 1}{x_1}$$

$$/x_0, x_1, x_2/ = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2}} = \frac{x_0 x_1 x_2 + x_2 + x_0}{x_2 x_1}.$$

DEFINITION 1A.2. We call $x_0, x_1, \cdots, x_n$ the **partial quotients** or just the quotients of the continued fraction.

DEFINITION 1A.3. For $m \leq N$ we call

$$r_m = /x_m, x_{m+1}, \cdots, x_N/ \tag{22}$$

the m**-th complete quotient** of the continued fraction $/x_0, x_1, \cdots, x_N/$.

We observe that:

$$/x_0, x_1, \dots, x_m, x_{m+1}/ = /x_0, x_1, \dots, x_m + \frac{1}{x_{m+1}}/. \tag{23}$$

DEFINITION 1A.4. We define the polynomials $Q_n(x_1, x_2, \dots, x_n)$ of n variables, for $n \geq 0$ by the following recursion:

(24)

$$Q_n(x_1, x_2, \dots, x_n) = \begin{cases} 1 & \text{if } n = 0 \\ x_1 & \text{if } n = 1 \\ x_1 Q_{n-1}(x_2, \dots, x_n) + Q_{n-2}(x_3, \dots, x_n) & \text{if } n > 1 \end{cases}$$

THEOREM 1A.5 (L. Euler). *The polynomial $Q_n(x_1, x_2, \dots, x_n)$ is the sum of all terms produced by starting with the product:*

$$1 \cdot x_1 \cdot x_2 \cdots x_n$$

and omitting zero or more nonoverlapping pairs of consecutive variables $x_j \cdot x_{j+1}$.

PROOF is by induction on n.

Basis: The result is trivial for $n = 0, 1$.

Induction Step: Assume the theorem holds for $k < n$, and notice that we have two kinds of terms produced by deleting zero or more nonoverlapping pairs from $1 \cdot x_1 \cdots x_n$: the ones that contain x_1 and the ones that don't.

To obtain the terms that contain x_1 we omit zero or more nonoverlapping pairs of consecutive variables from the product $1 \cdot x_2 \cdots x_n$. Using the induction hypothesis the sum of these terms is $x_1 Q_{n-1}(x_2, \ldots, x_n)$.

As for the terms that do not contain x_1, they also do not contain x_2 (the only way to omit x_1 is by omitting the pair $x_1 x_2$), so we obtain them by omitting zero or more nonoverlapping pairs of consecutive variables from the product $1 \cdot x_3 \cdots x_n$. Using the induction hypothesis the sum of these terms is $Q_{n-2}(x_3, \ldots, x_n)$, which completes the proof. ⊣

In this way we get:

$$
\begin{aligned}
&Q_1(x_1) = x_1 \\
&Q_2(x_1, x_2) = x_1 x_2 + 1 \\
&Q_3(x_1, x_2, x_3) = x_1 x_2 x_3 + x_1 + x_3 \\
&Q_4(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4 + x_1 x_4 + x_3 x_4 + x_1 x_2 + 1.
\end{aligned}
$$

Definition 1A.6. We define the sequence $(F_n)_{n \in \mathbb{N}}$ of the Fibonacci numbers as follows:

$$
\begin{aligned}
F_0 &= 0, \quad F_1 = 1 \\
F_{n+2} &= F_{n+1} + F_n, \ \text{ for } \ n \geq 0.
\end{aligned}
$$

Theorem 1A.7. *The number of summands appearing in the polynomial $Q_n(x_1, x_2, \ldots, x_n)$ is equal to the Fibonacci number F_{n+1}.*

Proof. This is obvious for $n = 0, 1$ and inductively, the number of summands that appears in $Q_n(x_1, x_2, \ldots, x_n)$ is

$$
\begin{aligned}
Q_n(1, 1, \ldots, 1) &= 1 \cdot Q_{n-1}(1, \ldots, 1) + Q_{n-2}(1, \ldots, 1) && \text{by (24)} \\
&= 1 \cdot F_n + F_{n-1} && \text{ind. hyp.} \\
&= F_{n+1}. && \text{Def. 1A.6}
\end{aligned}
$$

⊣

The Q-polynomials are symmetric in the sense that:

$$Q_{n+1}(x_0, x_1, \ldots, x_n) = Q_{n+1}(x_n, \ldots, x_1, x_0).$$

This is an immediate consequence of Theorem 1A.5: this specific permutation of the Q-polynomial variables leaves the pairs of successive terms unaffected and is moreover the only permutation with this very property. Consequently for $n \geq 2$,

$$Q_n(x_1, x_2, \ldots, x_n) = x_n Q_{n-1}(x_1, \ldots, x_{n-1}) + Q_{n-2}(x_1, \ldots, x_{n-2}).$$

The basic property we will use several times in all four chapters is:

Theorem 1A.8.

$$/x_0, x_1, \ldots, x_n/ = \frac{Q_{n+1}(x_0, x_1, \ldots, x_n)}{Q_n(x_1, x_2, \ldots, x_n)}, \quad (n \leq N).$$

PROOF. By induction on the number of variables n.
Basis:

$$/x_0, x_1/ = x_0 + \frac{1}{x_1} = \frac{x_0x_1+1}{x_1} = \frac{Q_2(x_0,x_1)}{Q_1(x_1)}.$$

Induction Step: Suppose that the hypothesis holds for n variables, so that:

$$/x_1, x_2 \dots, x_n/ = \frac{Q_n(x_1,\dots,x_n)}{Q_{n-1}(x_2,\dots,x_n)}.$$

Then

$$\begin{aligned}
/x_0, x_1, \dots, x_n/ &= x_0 + \frac{1}{/x_1, x_2 \dots, x_n/} \\
&= x_0 + \frac{1}{\dfrac{Q_n(x_1,\dots,x_n)}{Q_{n-1}(x_2,\dots,x_n)}} \\
&= \frac{x_0Q_n(x_1,\dots,x_n) + Q_{n-1}(x_2,\dots,x_n)}{Q_n(x_1,x_2,\dots,x_n)} \\
&= \frac{Q_{n+1}(x_0,x_1,\dots,x_n)}{Q_n(x_1,x_2,\dots,x_n)}.
\end{aligned}$$

⊣

1B. Fundamental properties of the Q-polynomials

In the first two proofs of the section we will use 2×2 matrices. The idea is that since we use induction of depth two, the properties of the Q-polynomials can be demonstrated clearer by use of 2×2 matrices. Many similar proofs use this technique. Of course the use of matrices is not necessary, it just gives more elegant proofs.

THEOREM 1B.1. *For $n \geq 1$,*

$$\begin{pmatrix} x_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} x_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} Q_{n+1}(x_0,\dots,x_n) & Q_n(x_0,\dots,x_{n-1}) \\ Q_n(x_1,\dots,x_n) & Q_{n-1}(x_1,\dots,x_{n-1}) \end{pmatrix}.$$

PROOF is by induction.
Basis. We compute:

$$\begin{pmatrix} x_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x_0x_1+1 & x_0 \\ x_1 & 1 \end{pmatrix} = \begin{pmatrix} Q_2(x_0,x_1) & Q_1(x_0) \\ Q_1(x_1) & Q_0 \end{pmatrix}.$$

Induction Step. Using the definition of the Q-polynomials and the inductive hypothesis, we have:

$$\begin{aligned}
&\begin{pmatrix} x_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} x_n & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x_{n+1} & 1 \\ 1 & 0 \end{pmatrix} \\
&= \begin{pmatrix} Q_{n+1}(x_0,\dots,x_n) & Q_n(x_0,\dots,x_{n-1}) \\ Q_n(x_1,\dots,x_n) & Q_{n-1}(x_1,\dots,x_{n-1}) \end{pmatrix}\begin{pmatrix} x_{n+1} & 1 \\ 1 & 0 \end{pmatrix} \\
&= \begin{pmatrix} x_{n+1}Q_{n+1}(x_0,\dots,x_n) + Q_n(x_0,\dots,x_{n-1}) & Q_n(x_1,\dots,x_n) \\ x_{n+1}Q_n(x_1,\dots,x_n) + Q_{n-1}(x_1,\dots,x_{n-1}) & Q_{n-1}(x_1,\dots,x_n) \end{pmatrix} \\
&= \begin{pmatrix} Q_{n+2}(x_0,\dots,x_{n+1}) & Q_{n+1}(x_0,\dots,x_n) \\ Q_{n+1}(x_1,\dots,x_{n+1}) & Q_n(x_1,\dots,x_n) \end{pmatrix}. \qquad \dashv
\end{aligned}$$

THEOREM 1B.2. *For* $n \geq 1$,

$$Q_n(x_0,\dots,x_{n-1})Q_n(x_1,\dots,x_n) - Q_{n+1}(x_0,\dots,x_n)Q_{n-1}(x_1,\dots,x_{n-1}) = (-1)^n.$$

PROOF. We just take the determinant of both sides of the first matrix equation of the previous theorem:

$$\begin{vmatrix} x_0 & 1 \\ 1 & 0 \end{vmatrix}\begin{vmatrix} x_1 & 1 \\ 1 & 0 \end{vmatrix}\cdots\begin{vmatrix} x_n & 1 \\ 1 & 0 \end{vmatrix} = \begin{vmatrix} Q_{n+1}(x_0,\dots,x_n) & Q_n(x_0,\dots,x_{n-1}) \\ Q_n(x_1,\dots,x_n) & Q_{n-1}(x_1,\dots,x_{n-1}) \end{vmatrix}$$

so we conclude that

$$\begin{aligned}
(-1)^{n+1} = Q_{n+1}(x_0,\dots,x_n)&Q_{n-1}(x_1,\dots,x_{n-1}) \\
&- Q_n(x_0,\dots,x_{n-1})Q_{n+1}(x_1,\dots,x_{n+1}),
\end{aligned}$$

from which we get the desired result by multiplying both sides by -1. $\dashv$

THEOREM 1B.3. *For* $n \geq 1$,

$$\begin{aligned}
Q_{n+2}(x_0,\dots,x_{n+1})&Q_{n-1}(x_1,\dots,x_{n-1}) \\
&- Q_n(x_0,\dots,x_{n-1})Q_{n+1}(x_1,\dots,x_{n+1}) = (-1)^{n+1}x_{n+1}.
\end{aligned}$$

PROOF. We compute directly from the inductive definition:

$$\begin{aligned}
&Q_{n+2}(x_0,\dots,x_{n+1})Q_{n-1}(x_1,\dots,x_{n-1}) \\
&\qquad - Q_n(x_0,\dots,x_{n-1})Q_{n+1}(x_1,\dots,x_{n+1}) \\
&= (x_{n+1}Q_{n+1}(x_0,\dots,x_n) + Q_n(x_0,\dots,x_n))Q_{n-1}(x_1,\dots,x_{n-1}) \\
&\quad - Q_n(x_0,\dots,x_{n-1})(x_{n+1}Q_n(x_1,\dots,x_n) + Q_{n-1}(x_1,\dots,x_{n-1})) \\
&= x_{n+1}[Q_{n+1}(x_0,\dots,x_n)Q_{n-1}(x_1,\dots,x_{n-1}) \\
&\qquad - Q_n(x_0,\dots,x_{n-1})Q_n(x_1,\dots,x_n)].
\end{aligned}$$

Now we can use Theorem 1B.2) to simplify the formula:

$$= x_{n+1}(-1) \cdot (-1)^n = (-1)^{n+1} x_{n+1}. \qquad \dashv$$

The following simple theorem is of great significance for the work in Chapter 3.

THEOREM 1B.4. *For* $k \geq 0$ *and* $l \geq 0$

$$Q_{k+l+2}(x_0, \dots, x_k, y_0, \dots, y_l)$$
$$= Q_{k+1}(x_0, \dots, x_k) Q_{l+1}(y_0, \dots, y_l) + Q_k(x_0, \dots, x_{k-1}) Q_l(y_1, \dots, y_l).$$

PROOF. Let us think of Euler's alternative definition of the Q-polynomials (see Theorem 1B.2). Then the Q-polynomial $Q_{k+l+2}(x_0, \dots, x_k, y_0, \dots, y_l)$ is obtained by adding up all possible terms produced by starting with the product

$$1 \cdot x_0 \cdots x_k \cdot y_0 \cdots y_l$$

and omitting zero or more nonoverlapping pairs of consecutive variables. The Q-polynomial $Q_{k+l+2}(x_0, \dots, x_k, y_0, \dots, y_l)$ has two kinds of terms:

1. The terms where the pair $x_k y_0$ is not omitted and the part of the Q-polynomial that contains these can be factored as

$$Q_{k+1}(x_0, \dots, x_k) Q_{l+1}(y_0, \dots, y_l)$$

2. The terms where the pair $x_k y_0$ is omitted and the part of the Q-polynomial that contains these can be factored as

$$Q_k(x_0, \dots, x_{k-1}) Q_l(y_1, \dots, y_l). \qquad \dashv$$

THEOREM 1B.5. *For* $2 \leq n \leq N$,

$$/x_0, x_1, \dots, x_N/$$
$$= \frac{/x_n, \dots, x_N/ \cdot Q_n(x_0, \dots, x_{n-1}) + Q_{n-1}(x_0, \dots, x_{n-2})}{/x_n, \dots, x_N/ \cdot Q_{n-1}(x_1, \dots, x_{n-1}) + Q_{n-2}(x_1, \dots, x_{n-2})}$$

PROOF. Using Theorem 1A.8 we compute:

$$/x_0, x_1, \dots, x_N/ = \frac{Q_{N+1}(x_0, x_1, \dots, x_N)}{Q_N(x_1, x_2, \dots, x_N)}$$

$$= \frac{Q_n(x_0, \dots, x_{n-1}) Q_{N-n+1}(x_n, \dots, x_N) + Q_{n-1}(x_0, \dots, x_{n-2}) Q_{N-n}(x_{n+1}, \dots, x_N)}{Q_{n-1}(x_1, \dots, x_{n-1}) Q_{N-n+1}(x_n, \dots, x_N) + Q_{n-2}(x_1, \dots, x_{n-2}) Q_{N-n}(x_{n+1}, \dots, x_N)}$$

(by Theorem 1B.4, with $k = n - 1$, $l = N - n$)

$$= \frac{\dfrac{Q_{N-n+1}(x_n, \dots, x_N)}{Q_{N-n}(x_{n+1}, \dots, x_N)} \cdot Q_n(x_0, \dots, x_{n-1}) + Q_{n-1}(x_0, \dots, x_{n-2})}{\dfrac{Q_{N-n+1}(x_n, \dots, x_N)}{Q_{N-n}(x_{n+1}, \dots, x_N)} \cdot Q_{n-1}(x_1, \dots, x_{n-1}) + Q_{n-2}(x_1, \dots, x_{n-2})}$$

$$= \frac{/x_n, \ldots, x_N/ \cdot Q_n(x_0, \ldots, x_{n-1}) + Q_{n-1}(x_0, \ldots, x_{n-2})}{/x_n, \ldots, x_N/ \cdot Q_{n-1}(x_1, \ldots, x_{n-1}) + Q_{n-2}(x_1, \ldots, x_{n-2})}$$

(by Theorem 1A.8.) ⊣

1C. From Q-polynomials to continued fractions

Most often we are not interested in studying a continued fraction as a formula in the variables $x_1, \ldots, x_n$, but rather as the representation of a real (or complex) number. Then we will agree to denote the partial quotients by $a_1, \ldots, a_n$ in order to indicate that we have to do with numbers instead of variables. We also define the sequences p_n, q_n as follows:

DEFINITION 1C.1. For every sequence of integeres $a_0, a_1, \ldots, a_N$ such that $0 \leq n \leq N$ let:

$$p_n = Q_{n+1}(a_0, a_1, \ldots, a_n)$$
$$q_n = Q_n(a_1, a_2, \ldots, a_n).$$

We call $\frac{p_n}{q_n}$ the n-th **principal convergent**, or just convergent of the continued fraction $/a_0, \ldots, a_N/$.

These are the convergents of the continued fraction. It is also convenient to define some additional terms:

$$p_{-2} = 0, \quad p_{-1} = 1, \quad q_{-2} = 1, \quad q_{-1} = 0, \quad q_0 = 1.$$

From Theorem 1A.8:

$$/a_0, a_1, ..., a_n/ = \frac{p_n}{q_n}, \quad (n \leq N).$$

It is now very easy to use the general results about Q-polynomials to get results about the sequences p_n and q_n (see Definition 1C.1) and the continued fraction $/a_1, \ldots, a_n/$. This approach is common with [7] and [11] while all other books in the references do not define the Q-polynomials but start from defining directly the sequences p_n and q_n. However studying the Q-polynomials gives us a better overall picture, not to mention that they themselves are really interesting mathematical objects thinking of Theorem 1A.5 and the relation to the Fibonacci numbers.

THEOREM 1C.2. *For $n \geq 0$, and p_n, q_n as in Definition 1C.1,*

$$p_0 = a_0, \qquad p_n = a_n p_{n-1} + p_{n-2}, \tag{25}$$
$$q_0 = 1, \qquad q_n = a_n q_{n-1} + q_{n-2}, \tag{26}$$

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}, \tag{27}$$

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_{n-1} q_n}, \tag{28}$$

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n, \tag{29}$$

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_{n-2} q_n}. \tag{30}$$

PROOF. One sees immediately that the preceding results about Q- polynomials guarantee that these three corollaries are true. In more detail, (25) and (26) follow from (24), while (27) and (28) follow from Theorem 1B.2. Finally (30) and (29) follow from Theorem 1B.3. The cases for $0 \le n \le 2$ are trivial to check. ⊣

COROLLARY 1C.3. *If the r_n's are defined by* (22), *then for* $2 \le n \le N$,

$$/a_0, \ldots, a_n/ = \frac{p_n}{q_n} = \frac{r_n p_{n-1} + p_{n-2}}{r_n q_{n-1} + q_{n-2}}.$$

PROOF. First, by Theorem 1A.8 and Definition 1C.1 we get

$$\frac{p_n}{q_n} = /a_0, \ldots, a_n/.$$

Then by Theorem 1B.5 and Definition 1C.1,

$$\frac{p_n}{q_n} = \frac{r_n p_{n-1} + p_{n-2}}{r_n q_{n-1} + q_{n-2}}.$$

⊣

THEOREM 1C.4. *For* $n \ge 1$,

$$\begin{aligned} /a_0, a_1, \ldots, a_n/ &= a_0 + \frac{1}{q_0 q_1} - \frac{1}{q_1 q_2} + \frac{1}{q_2 q_3} - \ldots + \frac{(-1)^{n-1}}{q_{n-1} q_n} \\ &= a_0 + \sum_{k=1}^{n} \frac{(-1)^{k-1}}{q_{k-1} q_k}. \end{aligned}$$

PROOF. By (28),

$$\begin{aligned} \sum_{k=1}^{n} \frac{(-1)^{k-1}}{q_{k-1} q_k} &= \sum_{k=1}^{n} \left(\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} \right) = \sum_{k=1}^{n} \frac{p_k}{q_k} - \sum_{k=1}^{n} \frac{p_{k-1}}{q_{k-1}} \\ &= \sum_{k=1}^{n} \frac{p_k}{q_k} - \sum_{k=0}^{n-1} \frac{p_k}{q_k} = \frac{p_n}{q_n} - \frac{p_0}{q_0}, \end{aligned}$$

so we have

$$a_0 + \sum_{k=1}^{n} \frac{(-1)^{k-1}}{q_{k-1} q_k} = \frac{p_0}{q_0} + \left(\frac{p_n}{q_n} - \frac{p_0}{q_0} \right) = \frac{p_n}{q_n} = /a_0, a_1, \ldots, a_n/.$$

⊣

1D. Simple continued fractions

DEFINITION 1D.1. A continued fraction $/a_0, a_1, \dots, a_N/$ is **simple** if $a_0, \dots, a_N$ are integers and

$$a_0 \geq 0, a_1 > 0, \dots, a_n > 0.$$

We will make this assumption for the rest of the remainder of this chapter.

THEOREM 1D.2. *For $n > 2$, $q_n > q_{n-1}$, and for $n \geq 1$, $q_n \geq q_{n-1}$.*

THEOREM 1D.3. *For $n > 3$, $q_n > n$ and for $n \geq 1$, $q_n \geq n$.*

PROOF is by induction on n:

$$q_0 = 1 \leq q_1 = a_1 < q_2 = a_1 a_2 + 1$$

$$q_1 = a_1 \geq 1, \quad q_2 = a_1 a_2 + 1 \geq 2$$

and for $n \geq 3$

$$q_n = a_n q_{n-1} + q_{n-2} > q_{n-1} + 1,$$

so that by the induction hypothesis $q_n > q_{n-1}$ and $q_n > n$. ⊣

THEOREM 1D.4. *For $n \geq 0$, $Q_{n+1}(a_0, a_1, \dots, a_n)$ and $Q_n(a_1, a_2, \dots, a_n)$ are relatively prime integers.*

In view of Definition 1C.1, this just says that $(p_n, q_n) = 1$.

PROOF. We use the notation of Definition 1C.1, $p_n = Q_{n+1}(a_0, \dots, a_n)$, $q_n = Q_n(a_1, \dots, a_n)$, so

$$(p_n, q_n) \mid p_n, \quad (p_n, q_n) \mid q_n,$$

by equation (27) we get that:

$$\begin{aligned}(p_n, q_n) \mid p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1} &\Rightarrow (p_n, q_n) \mid 1 \\ &\Rightarrow (p_n, q_n) = 1.\end{aligned}$$ ⊣

The following theorem shows that the q_n's grow exponentially in n. For more on the growth of the q_n's one can refer to [10].

THEOREM 1D.5 ([5]). *For all $n \geq 2$, $q_n \geq 2^{\frac{n-1}{2}}$.*

PROOF. For $n \geq 2$,

$$q_n = a_n q_{n-1} + q_{n-2} \geq q_{n-1} + q_{n-2} \geq 2q_{n-2}.$$

Successive application of the inequality yields

$$q_{2n} \geq 2^n q_0 = 2^n, \qquad q_{2n+1} \geq 2^n q_1 \geq 2^n,$$

which proves the theorem. ⊣

Thus the denominators of the convergents increase at least exponentially.

THEOREM 1D.6. *Every odd convergent is greater than any even convergent.*

PROOF. By (28),

$$\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{(-1)^{2n}}{q_{2n}q_{2n+1}} > 0.$$

So

$$\frac{p_{2n+1}}{q_{2n+1}} > \frac{p_{2n}}{q_{2n}}. \qquad \dashv$$

THEOREM 1D.7. *The n-th principal convergents, for even n, form a strictly increasing sequence and the n-th principal convergents, for odd n, form a strictly decreasing sequence, that is*

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots < \frac{p_{2m}}{q_{2m}} < \ldots$$
$$< \ldots < \frac{p_{2n+1}}{q_{2n+1}} < \ldots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

PROOF. By (30) we have that

$$\frac{p_{2n+2}}{q_{2n+2}} - \frac{p_{2n}}{q_{2n}} = \frac{(-1)^{2n+2}a_n}{q_{2n}q_{2n+2}} > 0, \quad \text{so} \quad \frac{p_{2n+2}}{q_{2n+2}} > \frac{p_{2n}}{q_{2n}}.$$

And similarly that

$$\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n-1}}{q_{2n-1}} < 0 \quad \text{so} \quad \frac{p_{2n+1}}{q_{2n+1}} < \frac{p_{2n-1}}{q_{2n-1}}. \qquad \dashv$$

We observe that:

(31) $$/a_0, a_1, ..., a_n, 1/ = /a_0, a_1, ..., a_n + 1/.$$

REMARK 1D.8. A number is representable by a simple continued fraction with an even number of convergents if and only if it is representable by one with an odd number of convergents.

It is often useful to choose one of the two alternative representations in order to simplify proofs and omit superfluous cases.

Recall how we defined the mth complete quotient r_m in Definition 1A.3.

THEOREM 1D.9. *For $n \leq N$, $a_n = \lfloor r_n \rfloor$, except that $a_{N-1} = \lfloor r_{N-1}, \rfloor - 1$ when the last partial quotient, $a_N = 1$.*

PROOF. If $N = 0$, then obviously $a_0 = r_0 = \lfloor r_0 \rfloor$. If $N > 0$, then

$$a_N = /a_N/ = r_N = \lfloor r_N \rfloor.$$

Now suppose $0 \leq n \leq N - 1$. We have

(32) $$r_n = a_n + \frac{1}{r_{n+1}}.$$

Case 1: If $n = N-1$ and $a_N = 1$ then

$$r_{N-1} = a_{N-1} + \frac{1}{a_N} = a_{N-1} + 1,$$

hence $a_{N-1} = \lfloor r_{N-1} \rfloor - 1$.

Case 2: Otherwise $r_{n+1} > 1$, because either $n = N-1$ and $a_N > 1$, so that

$$r_{n+1} = r_N = /a_N/ = a_N > 1,$$

or $n+1 < N$ and $r_{n+1} = a_{n+1} + \dfrac{1}{r_{n+2}} > 1$.

So by (32) we have that

$$a_n < r_n = a_n + \frac{1}{r_{n+1}} < a_n + 1,$$

which means that $a_n = \lfloor r_n \rfloor$. ⊣

Theorem 1D.10 ([3]). *If two simple continued fractions $/a_0, a_1, ..., a_N/$ and $/b_0, b_1, ..., b_M/$ have the same value x and $a_N > 1$, $b_M > 1$ then $M = N$ and the fractions are identical, i.e. they are formed by the same sequence of partial quotients.*

Proof. Suppose without loss of the generality that $N \le M$.

We will prove by induction on $n \le N$ that $a_n = b_n$, and then, by contradiction, that $N = M$.

For $n = 0$, we have $a_0 = \lfloor x \rfloor = b_0$ by Theorem 1D.9, as $a_N > 1$.

For $n = 1$,

$$a_0 + \frac{1}{(r_1)_a} = b_0 + \frac{1}{(r_1)_b}.$$

(Where $(r_n)_a$ is the n-th complete quotient of the continued fraction a.) And as

$$a_0 = b_0 = \lfloor x \rfloor, \quad \text{we have} \quad (r_1)_a = (r_1)_b,$$

Applying once more Theorem 1D.9 to $(r_1)_a$, $(r_1)_b$ we obtain $a_1 = b_1$.

Assume now that $n \ge 2$ and the result holds for $i \le n-1$. By Corollary 1C.3 we have,

$$\frac{(r_n)_a p_{n-1} + p_{n-2}}{(r_n)_a q_{n-1} + q_{n-2}} = x = \frac{(r_n)_b p_{n-1} + p_{n-2}}{(r_n)_b q_{n-1} + q_{n-2}},$$

and by cross multiplying we obtain

$$((r_n)_a - (r_n)_b)(p_{n-1}q_{n-2} - p_{n-2}q_{n-1}) = 0.$$

But $p_{n-1}q_{n-2} - p_{n-2}q_{n-1} = (-1)^n \neq 0$, by (27), and so $(r_n)_a = (r_n)_b$. It follows from Theorem 1D.9, that $a_n = b_n$. So for all $n \le N$, $a_n = b_n$.

If $M > N$, then

$$\frac{p_M}{q_M} = /a_0, \dots, a_N/ = /a_0, \dots, a_N, b_{N+1}, \dots, b_M/ = \frac{(r_{N+1})_b p_N + p_{N-1}}{(r_{N+1})_b q_N + q_{N-1}},$$

so $p_N q_{N-1} - p_{N-1} q_N = 0$ and by Corollary 1C.3 we have arrived at a contradiction. Hence $N = M$ and the fractions are identical. ⊣

REMARK 1D.11. Using (31), we can see that the preceding uniqueness Theorem also holds in the case when $a_N = 1, b_N = 1$.

1E. How close is a continued fraction to its convergents?

As before $a_i > 0$ for $i \geq 0$, $x = /a_0, \dots, a_N/$, $r_n = /a_n, \dots, a_N/$.

THEOREM 1E.1. *If* $1 \leq n \leq N-1$, *then*

$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n q'_{n-1}},$$

where q'_n *is defined by the following recursion:*

$$q'_1 = r_1$$

$$q'_n = r_n q_{n-1} + q_{n-2}, \quad \text{for} \quad 1 < n \leq N. \tag{33}$$

(Notice that in particular $q'_N = q_N$*.)*

PROOF. In the base case

$$x - \frac{p_0}{q_0} = x - a_0 = \frac{1}{r_1} = \frac{1}{q_0 r_1} = \frac{1}{q_0 q'_1}.$$

Suppose that $N > 1$ and $n > 0$. By (1C.3), for $1 \leq n \leq N-1$,

$$x = \frac{r_{n+1} p_n + p_{n-1}}{r_{n+1} q_n + q_{n-1}}.$$

Consequently

$$x - \frac{p_n}{q_n} = -\frac{p_n q_{n-1} - p_{n-1} q_n}{q_n (r_{n+1} q_n + q_{n-1})} = \frac{(-1)^n}{q_n (r_{n+1} q_n + q_{n-1})}.$$ ⊣

THEOREM 1E.2. *If* $N > 1, n > 0$, *then the differences*

$$x - \frac{p_n}{q_n}, \qquad q_n x - p_n$$

decrease steadily in absolute value as n *increases. Also*

$$q_n x - p_n = \frac{(-1)^n \delta_n}{q_{n+1}}, \tag{34}$$

where

$$0 < \delta_n < 1, \quad \text{for} \quad 1 \leq n \leq N-2, \quad \delta_{N-1} = 1$$

and

$$|x - \frac{p_n}{q_n}| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{q_n{}^2} \tag{35}$$

for $n \leq N-1$ *with strict inequality in both places except when* $n = N-1$.

Proof. Suppose $n \leq N-2$. As we saw in the proof of Theorem 1D.9 we have

$$a_{n+1} < r_{n+1} < a_{n+1} + 1, \tag{36}$$

while

$$a_{N-1} < r_{N-1} \leq a_{N-1} + 1,$$

where the equality holds when $a_N = 1$. Now using this we get the following two inequalities for $n \geq 1$:

$$q'_{n+1} = r_{n+1} q_n + q_{n+1} > a_{n+1} q_n + q_{n-1} \tag{37}$$

$$\begin{aligned} q'_{n+1} &= r_{n+1} q_n + q_{n+1} < (a_{n+1} + 1) q_n + q_{n-1} \\ &= (a_{n+1} q_n + q_{n-1}) + q_n = q_{n+1} + q_n \leq a_{n+2} q_{n+1} + q_n = q_{n+2} \end{aligned} \tag{38}$$

For the second inequality we have used that $r_{N-1} < a_{N-1} + 1$, which does not hold in the case $a_N = 1$, when we have the same with equality instead:

$$q'_{N-1} = (a_{N-1} + 1) q_{N-2} + q_{N-3} = q_{N-1} + q_{N-2} = q_N. \tag{39}$$

Moreover,

$$q_1 = a_1 < r_1 < a_1 + 1 \leq a_1 q_1 + q_0 = q_2.$$

From (37), (38) and Theorem 1E.1 it follows that

$$\frac{1}{q_{n+2}} < |p_n - q_n x| < \frac{1}{q_{n+1}}, \quad \text{for} \quad 1 \leq n \leq N-2, \tag{40}$$

while by (39) and $x = \frac{p_N}{q_N}$

$$|p_{N-1} - q_{N-1} x| = \frac{1}{q_N}, \quad \text{and} \quad p_N - q_N x = 0 \tag{41}$$

In either case (40) and (41) show that

$$|p_n - q_n x|, \qquad \Big|x - \frac{p_n}{q_n}\Big|.$$

decrease steadily as n increases, since q_n increases steadily. ⊣

1F. Infinite simple continued fractions

In this section we are going to define infinite simple continued fractions. These have finite continued fractions as their initial segments. We will essentially follow [3]. For more facts about intermediate fractions one can see [5] and [11].

Definition 1F.1. Suppose that $a_0, a_1, a_2, \ldots$ is an infinite sequence of integers with $a_1 > 0, a_2 > 0, \ldots$. Then $x_n = /a_0, a_1, \ldots, a_n/$ is for every n, a simple continued fraction representing a rational number x_n. If x_n tends to a limit x when $n \to \infty$ then we say that the *infinite simple continued fraction* $/a_0, a_1, a_2, \ldots/$ *converges to the value* x and we write

$$x = /a_0, a_1, a_2, \ldots/.$$

Theorem 1F.2. *All infinite simple continued fractions are convergent.*

Consequently, for even n*, the* n*-th principal convergents of an infinite continued fraction form a strictly increasing sequence converging to* x*. For odd* n*, the* n*-th principal convergents of* α *form a strictly decreasing sequence converging to* x*. That is if* $x = /a_0, a_1, \ldots/$ *then:*

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \ldots < \frac{p_{2m}}{q_{2m}} < \ldots < x < \ldots < \frac{p_{2n+1}}{q_{2n+1}} < \ldots < \frac{p_5}{q_5} < \frac{p_1}{q_1} \text{ and}$$

$$\lim_{n\to\infty} \frac{p_{2n}}{q_{2n}} = \lim_{n\to\infty} \frac{p_{2n+1}}{q_{2n+1}}.$$

One should notice this is a strengthening of Theorems 1D.7 and 1D.6.

Proof. We write

$$x_n = \frac{p_n}{q_n} = /a_0, a_1, \ldots, a_n/$$

and we call x_n the n-th convergent to $/a_0, a_1, a_2, \ldots/$. By Theorems 1D.7 and 1D.6 the even convergents form an increasing and the odd convergents a decreasing sequence and for all $n > 0$,

$$x_0 < x_2 < \ldots < x_{2n} < \ldots < x_1, \qquad x_0 < \cdots < x_{2n+1} < \ldots < x_3 < x_1.$$

That is the increasing sequence of even convergents is bounded above by x_1 and the decreasing sequence of odd convergents is bounded below by x_0. Hence the two series converge, say to the limits ξ_1, ξ_2 respectively. Then by Theorem 1D.6,

$$\lim_{n\to\infty} \frac{p_{2n}}{q_{2n}} = \xi_1 \le \xi_2 = \lim_{n\to\infty} \frac{p_{2n+1}}{q_{2n+1}}.$$

Finally by (28) and Theorem 1D.3 we have

$$\left|\frac{p_{2n}}{q_{2n}} - \frac{p_{2n-1}}{q_{2n-1}}\right| \le \frac{1}{q_{2n}q_{2n-1}} < \frac{1}{2n(2n-1)} \to 0,$$

and so $\xi_1 = \xi_2 = x$ and so the fraction $/a_0, a_1, a_2, .../$ converges to x. ⊣

DEFINITION 1F.3. For any positive integer r with $1 \leq r \leq a_{n+1}$ we call the fraction

$$\frac{p_n r + p_{n-1}}{q_n r + q_{n-1}}$$

an *intermediate fraction.*

DEFINITION 1F.4. The *mediant of two fractions* $\frac{a}{b}$ and $\frac{c}{d}$, with positive denominator, is the fraction

$$\frac{a+c}{b+d}.$$

LEMMA 1F.5. *The mediant of two fractions always lies between them in value.*

PROOF. Suppose without loss of generality, that $\frac{a}{b} \leq \frac{c}{d}$, in which case $bc - ad \geq 0$ and consequently

$$\frac{a+c}{b+d} - \frac{a}{b} = \frac{bc-ad}{b(b+d)} \geq 0$$

$$\frac{a+c}{b+d} - \frac{c}{d} = \frac{ad-bc}{b(b+d)} \leq 0.$$

⊣

THEOREM 1F.6. *If $x = /a_0, a_1, \dots/$ then the sequence*

$$\frac{p_{n-1}}{q_{n-1}}, \frac{p_n + p_{n-1}}{q_n + q_{n-1}}, \frac{2p_n + p_{n-1}}{2q_n + q_{n-1}}, \dots, \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}$$

is monotone: increasing for odd n and decreasing for even n.

PROOF. It is easy to verify that:

$$\frac{p_n(r+1) + p_{n-1}}{q_n(r+1) + q_{n-1}} - \frac{p_n r + p_{n-1}}{q_n r + q_{n-1}} = \frac{(-1)^{n+1}}{[q_n(r+1) + q_{n-1}][q_n r + q_{n-1}]}.$$

So for $r \geq 0$ we have that

$$\frac{p_{2n}(r+1) + p_{2n-1}}{q_{2n}(r+1) + q_{2n-1}} < \frac{p_{2n}r + p_{2n-1}}{q_{2n}r + q_{2n-1}}$$

$$\frac{p_{2n+1}(r+1) + p_{2n}}{q_{2n+1}(r+1) + q_{2n}} > \frac{p_{2n+1}r + p_{2n}}{q_{2n+1}r + q_{2n}}.$$

It follows that the sequence

$$\frac{p_{n-1}}{q_{n-1}}, \frac{p_n + p_{n-1}}{q_n + q_{n-1}}, \frac{2p_n + p_{n-1}}{2q_n + q_{n-1}}, \dots, \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}} \tag{42}$$

is monotone: increasing for odd n and decreasing for even n, (just as in the proof of Theorem 1D.7). Notice that the first and the last term of the sequence are both even- or both odd-order convergents.

The intervening terms (if there are any, that is, if $a_{n+1} > 1$), the intermediate fractions play an important role (though this role is not as important as the convergents' role).

Each of the intermediate fractions in the progression of (42) is the mediant of its preceding fraction and the fraction $\frac{p_n}{q_n}$.

Now the value x of the continued fraction lies between $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$, and the fractions $\frac{p_{n-1}}{q_{n-1}}$ and $\frac{p_{n+1}}{q_{n+1}}$, which are either both of odd or both of even order, lie on the same side of x and the fraction $\frac{p_n}{q_n}$ lies on the other side. In particular, the fractions $\frac{p_n + p_{n-1}}{q_n + q_{n-1}}$ and $\frac{p_n}{q_n}$ are always on opposite sides of x. So that the sequence

$$\frac{p_{n-1}}{q_{n-1}}, \frac{p_n + p_{n-1}}{q_n + q_{n-1}}, \frac{2p_n + p_{n-1}}{2q_n + q_{n-1}}, \dots, \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}$$

is monotone. ⊣

REMARK 1F.7. Notice that a_{n+1} is the largest positive integer r for which $\frac{p_{n-1}}{q_{n-1}}$ and $\frac{p_{n-1} + rp_n}{q_{n-1} + rq_n}$ are on the same side of x.

1G. Continued fractions and the Euclidean algorithm

In this section we will denote the ordered pair with first element x and second element y by $\{x, y\}$.

THEOREM 1G.1 (Division Theorem for natural numbers). *If $x \geq y > 0$ and $x, y \in \mathbb{N}$, then there exist unique numbers $q \in \mathbb{N}$ and $v \in \mathbb{N}$ such that*

$$x = yq + v \quad \textit{and} \quad 0 \leq v < y.$$

We denote the remainder v of this division by rem(x, y).

THEOREM 1G.2 (Division Theorem for reals, with $q \in \mathbb{N}$). *If $x \geq y > 0$ and $x, y \in \mathbb{R}$, then there exist unique numbers $q \in \mathbb{N}$ and $v \in \mathbb{R}$ such that*

$$x = yq + v \quad \textit{and} \quad 0 \leq v < y.$$

Moreover,

$$q = \lfloor \frac{x}{y} \rfloor. \tag{43}$$

We denote the remainder v of this division by $rem(x, y)$.

DEFINITION 1G.3. Let x, y be two natural numbers. We say that y **divides** x and we write $y \mid x$, if and only $rem(x, y) = 0$, and we denote the **greatest common divisor** of two natural numbers x, y by (x, y).

Continued fraction algorithm. To each real number x we assign two finite or infinite sequences $a_0, a_1, \ldots$ of integers and $\xi_0, \xi_1, \ldots$ of reals as follows:

1. Let $a_0 = \lfloor x \rfloor, \quad \xi_0 = x - a_0$.
2. If $a_0, \ldots, a_n, \xi_0, \ldots, \xi_n$ are defined, and $\xi_n \neq 0$, then let
$$a_{n+1} = \lfloor \frac{1}{\xi_n} \rfloor, \qquad \xi_{n+1} = \frac{1}{\xi_n} - a_{n+1}$$
3. If $\xi_n = 0$ then the algorithm terminates and returns $a_0, a_1, \ldots, a_n$ and $\xi_0, \ldots, \xi_n$.

REMARK 1G.4. Note that the algorithm also returns the complete quotients $r_n = /a_n, \ldots, a_N/$ of x, since for $\xi_m \neq 0$,
$$r_m = \frac{1}{\xi_m}.$$

Let us see what the algorithm does. While $\xi_n \neq 0$, this definition guarantees that $0 \leq \xi_{n+1} < 1$ so that $a_{n+1} = \lfloor \frac{1}{\xi_n} \rfloor$ is a positive integer strictly greater than 1.

If $\xi_n = 0$ then the quantities a_{n+1} and ξ_{n+1} are not defined and the algorithm stops, returning the sequence $a_0, a_1, \ldots, a_n$ so the continued fraction for x is $/a_0, a_1, \ldots, a_n/$ and x is a rational number.

The picture becomes clearer when we write down the first three steps of the algorithm:
$$x = a_0 + \xi_0 = a_0 + \frac{1}{a_1 + \xi_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \xi_2}} = \ldots.$$

THEOREM 1G.5. *For $n \geq 0$, and $a_n, \xi_n > 0$ assigned to x by the continued fraction algorithm,*
$$x = /a_0, \ldots, a_n + \xi_n/.$$

PROOF is by induction. For $n = 0$,
$$x = a_0 + \xi_0 = /a_0 + \xi_0/,$$
and if we suppose that
$$x = /a_0, \ldots, a_n + \xi_n/,$$

we get that. if $\xi_n \neq 0$,

$$\begin{aligned} x &= /a_0, \dots, a_n + \xi_n/ && \text{(ind. hyp.)} \\ &= /a_0, \dots, a_n, \frac{1}{\xi_n}/ && \text{(by (23))} \\ &= /a_0, \dots, a_n, a_{n+1} + \xi_{n+1}/ && \big(\xi_{n+1} := \frac{1}{\xi_n} - a_{n+1}\big). \end{aligned}$$

⊣

THEOREM 1G.6 (Correctness of the continued fraction algorithm). *For the sequence $a_0, a_1, \dots, a_n$ assigned to x by the continued fraction algorithm, we have that:*

(a) If x is rational then the algorithm terminates with $\xi_N = 0$ for some $N \geq 0$, and $x = /a_0, \dots, a_N/$, (with $a_N > 1$ if $N \neq 0$).

(b) If x is irrational, then $\xi_n \neq 0$ for all n, thus the algorithm does not terminate, and

$$x = \lim_{n\to\infty} /a_0, a_1, \dots, a_n/.$$

PROOF. (a) If the algorithm terminates and $\xi_n = 0$, then $N = n$ and $x = /a_0, \dots, a_N/$. As the continued fraction is finite it is also immediate that x is rational.

(b) Otherwise $\xi_n \neq 0$ for all $n \geq 0$ as $\dfrac{1}{\xi_n} = r_n$, by Theorem 1G.5 we have

$$\begin{aligned} |x - /a_0, a_1, \dots, a_n/| &= |/a_0, a_1, \dots, a_n + \frac{1}{r_n}/ - /a_0, a_1, \dots, a_n/| \\ &= |/a_0, a_1, \dots, a_n, r_n/ - /a_0, a_1, \dots, a_n/| \\ &\quad \text{(by (23))} \\ &= \Big| \frac{r_{n+1}p_n + p_{n-1}}{r_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} \Big| \\ &\quad \text{(by Corollary 1C.3)} \\ &= \Big| - \frac{p_n q_{n-1} - p_{n-1} q_n}{q_n(r_{n+1}q_n + q_{n-1})} \Big| \\ &= \Big| \frac{(-1)^n}{q_n(r_{n+1}q_n + q_{n-1})} \Big| \\ &= \Big| \frac{1}{q_n(r_{n+1}q_n + q_{n-1})} \Big|, \end{aligned}$$

and this gives

$$\lim_{n\to\infty} /a_0, a_1, \dots, a_n/ = x.$$

⊣

If we use the formulas the continued fraction algorithm above to compute the continued fractions of some familiar real numbers we get:

$$\frac{423}{720} = /1, 1, 2, 2, 1, 4/,$$
$$\pi = /3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, 1, 84, 2, 1, 1, 15, \dots/,$$
$$e = /2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14, 1, 1, 16, 1, 1, \dots/,$$
$$\phi = /1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, \dots/,$$

where $\phi = \dfrac{1+\sqrt{5}}{2}$.

THEOREM 1G.7. *Any rational number x can be represented as a finite continued fraction. Moreover this representation is unique if we demand that $a_N > 1$.*

PROOF. By Theorem 1G.6 we have a finite continued fraction representation of x. By Theorem 1D.10 we get the uniqueness. ⊣

We will now state the Euclidean algorithm and see the way the continued fraction algorithm can be stated as a special case of the Euclidean for $x, y \in \mathbb{R}$.

Euclidean algorithm. To each pair of real numbers $\{x, y\}$ such that $x \geq y > 0$ we assign two finite or infinite sequences $a_1, a_2, a_3, \dots$ and $\upsilon_{-1}, \upsilon_0, \upsilon_1, \upsilon_2, \dots$ as follows:

1. Let $\upsilon_{-1} = x$, $\upsilon_0 = y$

2. If $\upsilon_{-1}, \dots, \upsilon_i, a_1, \dots, a_i$ are defined and $\upsilon_i \neq 0$ then, by the division Theorem, choose υ_{i+1}, a_{i+1} such that
$$\upsilon_{i-1} = \upsilon_i a_{i+1} + \upsilon_{i+1} \qquad 0 \leq \upsilon_{i+1} < \upsilon_i.$$
3. If $\upsilon_i = 0$ then the algorithm terminates and returns $\upsilon_{-1}, \upsilon_0, \dots, \upsilon_{i-1}$ and $a_1, \dots, a_i$.

The Euclidean algorithm works for the pair $\{x, y\}$ as follows:

$$\begin{array}{rl}
x = y\ a_1 + \upsilon_1 & 0 < \upsilon_1 < y \\
y = \upsilon_1 a_2 + \upsilon_2 & 0 < \upsilon_2 < \upsilon_1 \\
\upsilon_1 = \upsilon_2 a_3 + \upsilon_3 & 0 < \upsilon_3 < \upsilon_2 \\
\vdots & \vdots \\
\upsilon_{n-3} = \upsilon_{n-2} a_{n-1} + \upsilon_{n-1} & 0 < \upsilon_{n-1} < \upsilon_{n-2} \\
\upsilon_{n-2} = \upsilon_{n-1} a_n & \upsilon_n = 0.
\end{array}$$

If x, y are positive integers, then we know that the algorithm terminates because the division remainders form a strictly decreasing sequence of positive integers, so for some $n \in \mathbb{N}$ it will be $\upsilon_{n+1} = 0$. If however x, y

are reals, it can be the case that the algorithm does not terminate, so all remainders are greater than zero.

Moreover if x, y are positive integers, we have that the last positive remainder v_{i-1} is equal to the greatest common divisor of x and y. This is based on the following simple observation: if

$$x = yq + v \quad \text{with} \quad 0 \leq v < y,$$

then the pairs $\{x, y\}$ and $\{y, v\}$ have exactly the same common divisors.

THEOREM 1G.8. *(a) If we execute the Euclidean algorithm for the pair* $\{x, 1\}$ *then* $x = /a_1, \dots, a_n, \dots /$ *where* $a_0, \dots, a_n, \dots$ *are the quotients in the Euclidean algorithm.*

(b) If $x = \dfrac{h}{k}$ *with* $h \geq k$*, it is equivalent to perform the Euclidean algorithm to the pair* $\{h, k\}$*.*

PROOF. (a) The division equation for the pair $\{x, 1\}$ is

$$\begin{array}{lll} x = 1 \cdot a_0 + v_1, & 0 \leq v_1 < 1 & (a_0 = \lfloor x \rfloor) \\ 1 = v_1 a_1 + v_2, & 0 \leq v_2 < v_1 & (a_1 = \lfloor \frac{1}{v_1} \rfloor) \\ v_1 = v_2 a_2 + v_3, & 0 \leq v_3 < v_2 & (a_2 = \lfloor \frac{v_1}{v_2} \rfloor) \\ \vdots & \vdots & \\ v_{n-1} = v_n a_n + v_{n+1}, & 0 \leq v_{n+1} < v_n & (a_n = \lfloor \frac{v_{n-1}}{v_n} \rfloor) \\ \vdots & \vdots & \end{array}$$

We can now construct the continued fraction for x:

$$x = 1 \cdot a_0 + v_1 = a_0 + \cfrac{1}{\cfrac{1}{v_1}} = a_0 + \cfrac{1}{\cfrac{v_1 a_1 + v_2}{v_1}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\cfrac{v_1}{v_2}}}$$

$$= \dots = a_0 + \cfrac{1}{a_2 + \cfrac{1}{\cfrac{v_1}{v_2}}} = a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{\cfrac{v_{n-1}}{v_n}}} = /a_0, a_1, \dots, a_n, \frac{v_{n-1}}{v_n}/.$$

By an easy induction on n, using that $a_{n+1} = \lfloor \dfrac{v_{n-1}}{v_n} \rfloor$, we can prove that

$$\xi_n = \frac{v_n}{v_{n-1}}.$$

So correctness follows from Theorem 1G.6.

(b) We observe that the quotients that appear in the Euclidean algorithm applied to the pair $\{h, k\}$ are the same as the quotients that appear in the Euclidean algorithm applied to the pair $\{x, 1\}$, because if we multiply each division equation that appears in the Euclidean algorithm for $\{x, 1\}$ we get exactly the divisions that appear in the Euclidean algorithm for $\{h, k\}$. ⊣

Notice the reason why the a_ns are called partial quotients: they coincide with quotients that appear in the Euclidean algorithm applied to the pair $\{x, 1\}$.

The representation determined by the continued fraction algorithm gives us the ability to represent a real number with the degree of accuracy we choose, according to the length of the continued fraction. The other system of representation, we use for real numbers, is that of decimal numbers or of systematic fractions (that is, fractions constructed according to some system of calculation). In chapter 1J we will show that the approximating values given by continued fractions have the property of being **best approximations** of the numbers, which is of great significance for theoretical investigations. However continued fractions turn out to be a very impractical representation for performing arithmetical operations (see Hurwitz 1891).

1H. Equivalent numbers

This definition of equivalence between numbers is closely and beautifully connected with the continued fraction algorithm because the operation in each step is such that we remain in the same equivalence class. The presentation here follows [3], [5], [8] and [10]. The latter two present also the algebraic point of view.

DEFINITION 1H.1. If ξ, η are two real numbers such that

$$\xi = \frac{a\eta + b}{c\eta + d}$$

where a, b, c, d are integers such that $ad - bc = \pm 1$, then ξ *is said to be equivalent to* η.

The relation we define this way is indeed an equivalence relation:

REFLEXIVE: $\xi = \dfrac{\xi + 0}{0\eta + 1}$.

SYMMETRIC: If ξ is equivalent to η then:

$$\xi = \frac{a\eta + b}{c\eta + d} \Rightarrow \xi c\eta + \xi d = a\eta + b \Rightarrow \xi c\eta - a\eta = b - \xi d \Rightarrow \eta = \frac{-d\xi + b}{c\xi - a}$$

and also $(-d)(-a) - bc = ad - bc = \pm 1$ and so η is equivalent to ξ.

Transitive: Suppose ξ is equivalent to η and η is equivalent to ζ. Then:

$$\xi = \frac{a\eta + b}{c\eta + d} \quad ad - bc = \pm 1$$
$$\eta = \frac{a'\zeta + b'}{c'\zeta + d'} a'd' - b'c' = \pm 1.$$

So substituting η in the first equation by it's expression in terms of ζ we get:

$$\xi = \frac{A\zeta + B}{C\zeta + D},$$

where

$$A = aa' + bc', \qquad B = ab' + bd', \qquad C = ca' + dc', \qquad D = cb' + dd'$$

$$AD - BC = (ad - bc)(a'd' - b'c') = \pm 1$$

Theorem 1H.2. *Any two rational numbers are equivalent.*

Proof. Every rational number can be expressed in the form $\frac{h}{k}$ where h, k are coprime integers. Then as $(h, k) = 1$ there exist natural numbers $h',\ k'$ such that:

$$hk' - h'k = 1$$

so

$$\frac{h}{k} = \frac{h' \cdot 0 + h}{k' \cdot 0 + k}.$$

We get that every rational is equivalent to 0, but also to any other rational, since our relation is transitive. ⊣

There is a correspondence between matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with determinant ± 1 and transformations $\dfrac{ax + b}{cx + d}$. In fact

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} ax + b \\ cx + d \end{pmatrix}.$$

The set of all such matrices (/transformations) with integral components is a group under matrix multiplication (/composition of transformations), for the product of two such matrices and the inverse of such a matrix again have determinant ± 1, so the product of any two elements of the group stays in the group.

If $\sigma \in G$ we define for any number x:

$$\sigma x = \frac{ax+b}{cx+d}.$$

Then if $\sigma, \tau \in G$ and I is the identity matrix,

$$\sigma(\tau x) = (\sigma\tau)x \quad \textit{and} \quad Ix = x.$$

Thus G operates on the set of numbers and two numbers ξ, η are equivalent if there exists $\sigma \in G$ such that $\sigma\xi = \eta$.

DEFINITION 1H.3. If $x = /a_0, a_1, \dots /$ is an infinite simple continued fraction with convergents p_n, q_n, we let

$$\sigma_{n-1} = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix}.$$

We call σ_{n-1} the $(n-1)$**-th continued fraction transformation of** x.

The determinant of the matrix is ± 1 because $p_{n-1}q_{n-2} - p_{n-2}q_{n-1} = (-1)^{n-2}$, by (27).

THEOREM 1H.4. *Let x be any irrational number with*

$$x = /a_0, a_1, \dots , a_{n-1}, r_n/,$$

where r_n is the n-th complete quotient of x, that is

$$r_n = /a_n, a_{n+1}, \dots /.$$

Then x is equivalent to r_n for $n \geq 1$.

PROOF. By Corollary 1C.3,

$$x = /a_0, a_1, ..., r_n/ = \frac{p_{n-1}r_n + p_{n-2}}{q_{n-1}r_n + q_{n-2}},$$

so that $x = \sigma_{n-1}r_n$. Thus x is equivalent to r_n for $n \geq 1$ and consequently all complete quotients of x are equivalent to each other. ⊣

Furthermore if we let

$$A_n = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix},$$

then $det(A_n) = -1$ and by induction on n using (25),

$$\sigma_n = A_0 A_1 \cdots A_n.$$

We see that this is a decomposition of the transformation σ_n, to each of the n steps of the equivalent continued fraction transformation.

Notice also the similarity of this decomposition to the one of Theorem 1B.1.

THEOREM 1H.5. *If*

$$x = \frac{P\zeta + R}{Q\zeta + S},$$

where $\zeta > 1$ *and* P, Q, R *and* S *are integers such that*

$$Q > S > 0, \quad PS - QR = \pm 1,$$

then there exists some $n \geq 0$ *such that*

$$\frac{R}{S} = \frac{p_{n-1}}{q_{n-1}}, \quad \frac{P}{Q} = \frac{p_n}{q_n}, \quad \textit{and} \quad \zeta = r_{n+1}.$$

In particular, $\frac{R}{S}$ *and* $\frac{P}{Q}$ *are successive convergents to the simple continued fraction with value* x.

PROOF. We develop P/Q in the continued fraction representation for rationals,

$$\frac{P}{Q} = \frac{p_n}{q_n} = /a_0, \ldots, a_n/. \tag{44}$$

As we have seen in Remark 1D.8 we can have n odd or even, as we please. So we choose n such that

$$PS - QR = (-1)^{n-1}. \tag{45}$$

The hypothesis $PS - QR = \pm 1$ implies that $(P, Q) = 1$ and $Q > 0$ and by (27) and Theorem 1D.4 it is also

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1},$$

$(p_n, q_n) = 1$ and $p_n > 0$. Hence $P = p_n, \quad Q = q_n$ and

$$p_n S - q_n R = PS - QR = (-1)^{n-1} = p_n q_{n-1} - p_{n-1} q_n,$$

so that

$$p_n(S - q_{n-1}) = q_n(R - p_{n-1}).$$

So $q_n \mid p_n(S - q_{n-1})$. But since $(p_n, q_n) = 1$ it must be that

$$q_n \mid (S - q_{n-1}).$$

But

$$q_n = Q > S > 0, \qquad q_n \geq q_{n-1} > 0,$$

and so

$$|S - q_{n-1}| < q_n.$$

It follows that q_n can't divide $(S - q_{n-1})$ unless it is zero. So

$$S = q_{n-1}, \quad R = p_{n-1}$$

and

$$x = \frac{p_n \zeta + p_{n-1}}{q_n \zeta + q_{n-1}}$$

which means that

$$x = /a_0, \dots, a_n, \zeta/.$$

Developing ζ as a simple continued fraction, $\zeta = /a_{n+1}, a_{n+2}, \dots/$ we come to the simple continued fraction representation of x,

$$x = /a_0, a_1, \dots, a_n, a_{n+1}, a_{n+2}, \dots/.$$

We have proved that,

$$\frac{R}{S} = \frac{p_{n-1}}{q_{n-1}} \qquad \frac{P}{Q} = \frac{p_n}{q_n}$$

and

$$\zeta = r_{n+1}. \qquad \dashv$$

THEOREM 1H.6. *Two irrational numbers ξ and η are equivalent if and only if for suitable $a_0, a_1, \dots, a_m, b_0, b_1, \dots, b_n$ and $c_0, c_1, \dots$ we have,*

(46) $$\xi = /a_0, a_1, \dots, a_m, c_0, c_1, \dots/ \quad \eta = /b_0, b_1, \dots, b_n, c_0, c_1, \dots/.$$

PROOF. Suppose ξ and η are as in (46) and let $\omega = /c_0, c_1, \dots/$. Then

$$\xi = /a_0, a_1, \dots, a_m, \omega/ = \frac{p_m \omega + p_{m-1}}{q_{m-1}\omega + q_{m-1}}$$

but also

$$p_m q_{m-1} - p_{m-1} q_m = \pm 1,$$

so ξ and ω are equivalent. Exactly the same argument shows that η and ω are equivalent, and so by transitivity ξ and η are equivalent. Conversely if ξ and η are two equivalent numbers, then

$$\eta = \frac{a\xi + b}{c\xi + d}, \qquad ad - bc = \pm 1.$$

We may suppose $c\xi + d > 0$, since otherwise we may replace the coefficients by their negatives. When we develop ξ by the continued fraction algorithm, we obtain for any k,

$$\xi = /a_0, a_1, \dots, a_k, a_{k+1}, \dots/ = /a_0, a_1, \dots, a_{k-1}, r_k/ = \frac{p_{k-1} r_k + p_{k-2}}{q_{k-1} r_k + q_{k-2}}.$$

Replacing ξ by this expression in η, we get

$$\eta = \frac{P\, r_k + R}{Q\, r_k + S},$$

where

$$P = ap_{k-1} + bp_{k-1}, \qquad R = ap_{k-2} + bp_{k-2}$$
$$Q = cp_{k-1} + dp_{k-1}, \qquad S = cp_{k-2} + dp_{k-2}$$

with

$$PS - QR = (ad - bc)(p_{k-1}q_{k-2} - p_{k-2}q_{k-1}) = \pm 1.$$

By (34) we can write

$$p_{k-1} = \xi q_{k-1} + \frac{\delta}{q_{k-1}}, \text{where } |\delta| < 1$$
$$p_{k-2} = \xi q_{k-2} + \frac{\delta'}{q_{k-2}}, \text{where } |\delta'| < 1.$$

Hence

$$Q = (c\xi + d)q_{k-1} + \frac{c\delta}{q_{k-1}}, \qquad S = (c\xi + d)q_{k-2} + \frac{c\delta'}{q_{k-2}}.$$

Now $c\xi + d > 0$, $q_{k-1} > q_{k-2} > 0$ and q_{k-1}, q_{k-2} tend to infinity, so that

$$Q > S > 0$$

for sufficiently large k. For such k

$$\eta = \frac{P\zeta + R}{Q\zeta + S},$$

where

$$PS - QR = \pm 1, \quad Q > S > 0, \quad \zeta = r_k > 1$$

and so by the previous theorem,

$$\eta = /b_0, b_1, \dots, b_l, \zeta/ = /b_0, b_1, \dots, b_l, a_k, a_{k+1}, \dots/$$

for some $b_0, b_1, \dots, b_l$. ⊣

1I. Periodic continued fractions

The proofs here follow [3] and [5] (there are only minor differences between the proofs in the two books).

DEFINITION 1I.1. A periodic continued fraction is an infinite continued fraction in which $a_l = a_{l+k}$ for a fixed positive k and all $l \geq L$. The sequence of partial quotients $a_L, a_{L+1}, \dots, a_{L+k-1}$ is called the period, and we write $/a_0, a_1, \dots/ = /a_0, a_1, \dots, \overline{a_L, \dots, a_{L+k}}/$ in analogy to the notation for decimal fractions.

THEOREM 1I.2. *A periodic continued fraction is a quadratic irrational, i.e. an irrational root of a quadratic equation with integral coefficients.*

Proof. Obviously the remainders of the periodic continued fraction satisfy the relationship:

$$r_{l+k} = r_l, \qquad l \geq L.$$

So we have

$$\alpha = \frac{p_{l-1}r_l + p_{l-2}}{q_{l-1}r_l + q_{l-2}} = \frac{p_{l+k-1}r_{l+k} + p_{l+k-2}}{q_{l+k-1}r_l + q_{l+k-2}} = \frac{p_{l+k-1}r_l + p_{l+k-2}}{q_{l+k-1}r_l + q_{l+k-2}}$$

so that

$$\frac{p_{l-1}r_l + p_{l-2}}{q_{l-1}r_l + q_{l-2}} = \frac{p_{l+k-1}r_l + p_{l+k-2}}{q_{l+k-1}r_l + q_{l+k-2}}.$$

As $p_{l-1}q_{l+k-1} - q_{l-1}p_{l+k-1} \neq 0$ (by Theorem 1D.6), the number r_l satisfies a quadratic equation with integer coefficients and consequently is an irrational number. But

$$\alpha = \frac{p_{l-1}r_l + p_{l-2}}{q_{l-1}r_l + q_{l-2}} \quad \text{so} \quad r_l = \frac{p_{l-2} - q_{l-2}\alpha}{q_{l-1}\alpha + q_{l-1}}$$

and if we substitute r_l in the previous quadratic equation, and clear of fractions, we get that α satisfies an equation

$$ax^2 + bx + c = 0. \tag{47}$$

And since α is irrational, $b^2 - 4ac \neq 0$. (If $b^2 - 4ac = 0$ then the double root of the equation would be $\frac{-b}{2a}$ so a rational number.) ⊣

The converse of the theorem is also true. The proof is a bit more difficult but also more interesting.

Theorem 1I.3. *The continued fraction which represents a quadratic irrational is periodic.*

Proof. Suppose α satisfies the quadratic equation with integer coefficients and $a > 0$

$$a\alpha^2 + b\alpha + c = 0. \tag{48}$$

Considering the continued fraction representation of α we can write

$$\alpha = \frac{p_{n-1}r_n + p_{n-2}}{q_{n-1}r_n + q_{n-2}}.$$

And if we substitute α in $a\alpha^2 + b\alpha + c = 0$ we obtain

$$A_n r_n^2 + B_n r_n + C_n = 0, \tag{49}$$

where

$$\begin{aligned}
A_n &= ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2,\\
B_n &= 2ap_{n-1}p_{n-2} + b(p_{n-1}q_{n-1} + p_{n-2}q_{n-1}) + 2cq_{n-1}q_{n-2},\\
C_n &= ap_{n-2}^2 + bp_{n-2}q_{n-2} + cq_{n-2}^2 = A_{n-1}.
\end{aligned}$$

If $A_n = ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2 = 0$, then the quadratic equation $a\alpha^2 + b\alpha + c = 0$ has a unique rational root namely $\dfrac{p_{n-1}}{q_{n-1}}$ but this is impossible as α is irrational. Hence $A_n \neq 0$ and

$$A_n y^2 + B_n y + C_n = 0$$

is an equation one of whose roots is r_n. It can be proved by induction on n that:

$${B_n}^2 - 4A_nC_n = (b^2 - 4ac)(p_{n-1}q_{n-2} - q_{n-1}p_{n-2})^2 = b^2 - 4ac.$$

That is, the discriminant of $A_ny^2 + B_ny + C_n = 0$ is the same as that of $ay^2 + by + c = 0$. Furthermore since

$$\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{{q_{n-1}}^2}$$

it follows that

$$p_{n-1} = \alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}} \qquad |\delta_{n-1}| < 1.$$

Therefore

$$\begin{aligned} A_n &= a\big(\alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}\big)^2 + b\big(\alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}\big)q_{n-1} + cq_{n-1}^2 \\ &= (a\alpha^2 + b\alpha + c)q_{n-1}^2 + 2a\alpha\delta_{n-1} + a\frac{\delta_{n-1}^2}{q_{n-1}} + b\delta_{n-1}. \end{aligned}$$

So we have

$$\begin{aligned} |A_n| &= \left|(a\alpha^2 + b\alpha + c)q_{n-1}^2 + 2a\alpha\delta_{n-1} + a\frac{\delta_{n-1}^2}{q_{n-1}} + b\delta_{n-1}\right| \\ &< 2|a\alpha| + |a| + |b|, \\ |C_n| &= |A_{n-1}| < 2|a\alpha| + |a| + |b|. \end{aligned}$$

Finally

$${B_n}^2 \leq 4A_nC_n + |b^2 - 4ac| < 4(2|a\alpha| + |a| + |b|)^2 + |b^2 - 4ac|.$$

Hence the coefficients of the quadratic equation $A_ny^2 + B_ny + C_n = 0$ are all bounded in absolute value (a, b, c are independent of n) and hence there are only a finite number of distinct values, as n varies. But in any case r_n can only take a finite number of distinct values, and therefore, for properly chosen l and k,

$$r_l = r_{l+k}$$

So the continued fraction representing α is periodic. ⊣

No proofs analogous to this are known for continued fractions representing algebraic irrational numbers of higher degrees. In general, all that is known concerning the approximation of algebraic numbers of higher degrees by rational fractions amounts to Liouville's Theorem and certain propositions strengthening it (see [5]).

1J. Convergents as best approximations

In this section we will follow [5]. In fact, in [5] there can be found many more facts, than the ones presented here and maybe this is the most interesting and well-written part of the book. Some of the facts are also covered in [3].

DEFINITION 1J.1. A fraction $\frac{a}{b}$, for $b > 0$ is called a **best approximation of the first kind** of a real number x if every other rational fraction with the same or smaller denominator differs from x by a greater amount, that is, if

$$0 < d \leq b, \quad \text{and} \quad \frac{a}{b} \neq \frac{c}{d}$$

imply that

$$\left|x - \frac{c}{d}\right| > \left|x - \frac{a}{b}\right|.$$

THEOREM 1J.2. *Every best approximation of the first kind is a convergent or an intermediate fraction of the continued fraction representing that number.*

PROOF. Suppose that $\frac{a}{b}$ is a best approximation of the first kind of the number x. Then, first of all, $\frac{a}{b} \geq a_0$ because if $\frac{a}{b} < a_0$ then the fraction $\frac{a_0}{1}$, (being distinct from $\frac{a}{b}$ and having a denominator that is no greater than b,) would lie closer to x than does $\frac{a}{b}$. Therefore $\frac{a}{b}$ would not be a best approximation of the first kind.

Also $\frac{a}{b} \leq a_0 + 1$, because supposing $\frac{a}{b} > a_0 + 1$, then

$$\frac{a}{b} - x = \left|x - \frac{a}{b}\right| > \left|x - \frac{a_0 + 1}{1}\right| = a_0 + 1 - x$$

($x = a_0 + \dfrac{1}{/a_1, \ldots /} \leq a_0 + 1$ as all a_is are integral).

But this contradicts $\frac{a}{b}$ being a best approximation of x of the first kind.

If $\frac{a}{b} = \frac{a_0}{1} = \frac{p_0}{q_0}$ then $\frac{a}{b}$ is a convergent, and if $\frac{a}{b} = \frac{a_0+1}{1} = \frac{p_0+p_{-1}}{q_0+q_{-1}}$, then $\frac{a}{b}$ is an intermediate fraction of x. Thus we can assume that

$$a_0 < \frac{a}{b} < a_0 + 1.$$

Suppose towards a contradiction that $\frac{a}{b}$ does not coincide with a convergent or intermediate fraction of the number x, then it must lie strictly between two consecutive such fractions. For instance for properly chosen k and r (with $k > 0,\ 0 \le r < a_{k+1}$ or $k = 0,\ 1 \le r < a_1$), it will lie between the fractions

$$\frac{p_k r + p_{k-1}}{q_k r + q_{k-1}}$$

and

$$\frac{p_k(r+1) + p_{k-1}}{q_k(r+1) + q_{k-1}}$$

so that

$$\begin{aligned}\left|\frac{a}{b} - \frac{p_k r + p_{k-1}}{q_k r + q_{k-1}}\right| &< \left|\frac{p_k(r+1) + p_{k-1}}{q_k(r+1) + q_{k-1}} - \frac{p_k r + p_{k-1}}{q_k r + q_{k-1}}\right| \\ &= \frac{1}{\big(q_k(r+1) + q_{k-1}\big)\big(q_k r + q_{k-1}\big)}\end{aligned}$$

On the other hand, it is obvious that

$$\left|\frac{a}{b} - \frac{p_k r + p_{k-1}}{q_k r + q_{k-1}}\right| = \frac{m}{b(q_k r + q_{k-1})}$$

where $m = |(q_k r + q_{k-1})a - (p_k r + p_{k-1})b| \ge 1$ as m is an integer that can't be zero because of our assumption. Consequently,

$$\frac{1}{b(q_k r + q_{k-1})} < \frac{1}{\big(q_k(r+1) + q_{k-1}\big)\big(q_k r + q_{k-1}\big)}$$

and hence,

$$q_k(r+1) + q_{k-1} < b.$$

Now the fraction

$$\frac{p_k(r+1) + p_{k-1}}{q_k(r+1) + q_{k-1}}$$

with denominator less than b is closer to the number x than is the fraction

$$\frac{p_k r + p_{k-1}}{q_k r + q_{k-1}}$$

(because, in general, from 1F.6, every intermediate fraction is closer to α than is the preceding one) and hence it is also closer than is the fraction $\frac{a}{b}$, which lies between the two previous expressions. This contradicts the assumption that $\frac{a}{b}$ is a best approximation of the first kind and the proof is complete. ⊣

DEFINITION 1J.3. A fraction $\frac{a}{b}$, for $b > 0$ is called a **best approximation of the second kind** of a real number x if

$$0 < d \leq b, \text{ and } \frac{a}{b} \neq \frac{c}{d}$$

imply that

$$|dx - c| > |bx - a|.$$

THEOREM 1J.4. *Every best approximation of the second kind is necessarily a best approximation of the first kind.*

PROOF. Indeed assuming towards a contradiction that $\frac{a}{b}$ is a best approximation of x of the first kind but not a best approximation of the second kind we have:

$$\left|x - \frac{c}{d}\right| \leq \left|x - \frac{a}{b}\right|$$

$$0 < d \leq b, \qquad \frac{a}{b} \neq \frac{c}{d}.$$

Then on multiplying the first of these inequalities by the third we obtain

$$|dx - c| \leq |bx - a|.$$

So $\frac{a}{b}$ is not a best approximation of the first kind and we arrive at a contradiction. ⊣

The converse is not true: a best approximation of the first kind can fail to be a best approximation of the second kind. For example the fraction $\frac{1}{3}$ is a best approximation of the first kind of the number $\frac{1}{5}$. (It can be easily verified that for all integers f: $\left|\frac{1}{5} - \frac{1}{3}\right| < \left|\frac{1}{5} - \frac{f}{2}\right|$ and $\left|\frac{1}{5} - \frac{1}{3}\right| < \left|\frac{1}{5} - \frac{f}{1}\right|$.)

However, it is not a best approximation of the second kind because:

$$|1 \cdot \frac{1}{5} - 0| < |3 \cdot \frac{1}{5} - 1| \quad \text{and} \quad 1 < 3.$$

THEOREM 1J.5. *Every best approximation of the second kind is a convergent.*

PROOF. Suppose that the fraction $\frac{a}{b}$ is a best approximation of the second kind of the number $x = /a_0, a_1, \ldots /$ whose convergents are $\frac{p_k}{q_k}$. If it were $\frac{a}{b} < a_0 = \frac{p_1}{q_0}$ then as $b \geq 1$ we would obtain

$$|1 \cdot x - a_0| < \left|x - \frac{a}{b}\right| \leq \left|bx - a\right|$$

That is $\frac{a}{b}$ would not be an approximation of the second kind. Thus,

$$\frac{a}{b} \geq a_0 = \frac{p_1}{q_0}.$$

Suppose towards a contradiction that the fraction $\frac{a}{b}$ does not coincide with one of the convergents, then one of the following two cases must occur:

Case 1: If $\frac{a}{b} > \frac{p_1}{q_1}$ then

$$\left|x - \frac{a}{b}\right| \geq \left|\frac{p_1}{q_1} - \frac{a}{b}\right| \geq \frac{1}{bq_1}$$

so that

$$|bx - a| > \frac{1}{q_1} = \frac{1}{a_1}.$$

On the other hand,

$$|1 \cdot x - a_0| \leq \frac{1}{a_1}$$

so that

$$|bx - a| > |a \cdot x - a_0|, \quad 1 \leq b,$$

which contradicts the assumption that $\frac{a}{b}$ is a best approximation of x of the second kind.

Case 2: Else if $\frac{a}{b}$ lies strictly between two convergents $\frac{p_{k-1}}{q_{k-1}}$ and $\frac{p_{k+1}}{q_{k+1}}$. So

$$\left|\frac{a}{b} - \frac{p_{k+1}}{q_{k+1}}\right| \geq \frac{1}{bq_{k+1}}$$

and

$$\left|\frac{a}{b} - \frac{p_{k+1}}{q_{k+1}}\right| < \left|\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}}\right| = \frac{1}{q_k q_{k+1}}$$

so that

(50) $$b > q_k.$$

On the other hand,

$$\left|x - \frac{a}{b}\right| \geq \left|\frac{p_{k+1}}{q_{k+1}} - \frac{a}{b}\right| \geq \frac{1}{bq_{k+1}}$$

and hence

$$|bx - a| \geq \frac{1}{q_{k+1}}$$

whereas

$$|q_k x - p_k| \leq \frac{1}{q_{k+1}}$$

so that

(51) $$|q_k x - p_k| \leq |bx - a|.$$

Inequalities (50), (51) show that $\frac{a}{b}$ is not a best approximation of the second kind. ⊣

THEOREM 1J.6. *Every convergent $\frac{p_n}{q_n}$ for $n \geq 1$ is a best approximation of the second kind.*

Remark: In the case of $x = a_0 + \frac{1}{2}$, the fraction $\frac{p_0}{q_0} = \frac{a_0}{1}$ is not a best approximation of the second kind because

$$1 \cdot x - (a_0 + 1) = 1 \cdot |1 \cdot x - a_0|.$$

For a proof of Theorem 1J.6 see [4].

CHAPTER 2

SOME NUMBER THEORY

We state some basic results from number theory, mainly concerning the behavior of some common arithmetical functions for large values of n, that we will use later. One could skip this chapter and refer to it whenever necessary. We will follow closely the presentation in [3] and [9].

Recall that for two functions f, g on the natural numbers,

$$f = O(g) \iff \text{for some } A > 0 \text{ and all } x, |f(x)| < Ag(x).$$

This is easily equivalent to assuming $|f(x)| < Ag(x)$ for all sufficiently large x.

THEOREM (**The Fundamental Theorem of Arithmetic**, [3]). *The* **standard form**

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad a_1 > 0, a_2 > 0, \dots, a_k > 0 \quad p_1 < p_2 < \dots < p_k$$

of n is unique, for $n \geq 2$.

2A. Sieve methods

THEOREM 2A.1 ([9]). *Let $A_1, \dots, A_r$ be subsets of a finite set A, let $B = A \setminus \bigcup_{i=1}^r A_i$, and let $f(x)$ be any complex valued function defined on A. For $j \leq r$ we put*

$$T_j = \sum_{x \in A} f(x) + \sum_{s=1}^{j} (-1)^s \sum_{\{i_1, \dots, i_s\} \subseteq \{1, \dots, r\}} \sum_{x \in A_{i_1} \cap \dots \cap A_{i_s}} f(x).$$

Then

$$\sum_{x \in B} f(x) = T_r.$$

PROOF. If g is a characteristic function of the set B, and f_i that of A_i, then for any $x \in A$ we have

$$g(x) = 1 + \sum_{s=1}^{r} (-1)^s \sum_{\{i_1,\dots,i_s\} \subset \{1,\dots,r\}} f_{i_1}(x) \cdots f_{i_s}(x). \tag{52}$$

Indeed, if $x \in B$, then both sides of (52) are equal to 1. If, on the other hand $x \notin B$, and x belongs to exactly m sets A_i, say to $A_{j_1}, \dots, A_{j_m}$, then the left hand side is equal to zero and the right is equal to

$$1 + \sum_{s=1}^{m} (-1)^s \sum_{\{i_1,\dots,i_s\} \subset \{j_1,\dots,j_m\}} 1 = 1 + \sum_{s=1}^{m} (-1)^s \binom{m}{s} = (1-1)^m = 0.$$

Multiplying both sides of (52) by $f(x)$ and summing over all $x \in A$, we obtain $T_r = \sum_{x \in B} f(x)$ (using the fact that $A \cap B = B$). ⊣

COROLLARY 2A.2 (**Inclusion exclusion principle**). *Let $A_1, \dots, A_r$ be subsets of a finite set A and $B = A \setminus \bigcup_{i=1}^{r} A_i$. We have*

$$|B| = |A| + \sum_{s=1}^{r} (-1)^s \sum_{\{i_1,\dots,i_s\} \subset \{1,\dots,r\}} |A_{i_1} \cap \ldots \cap A_{i_s}|.$$

PROOF is immediate applying Theorem 2A.1 with $f(x) = 1$. ⊣

2B. Modular Arithmetic

DEFINITION 2B.1. Let m be an integer. We say that two integers a and b are **congruent** modulo m if m divides $a - b$ and write $a \equiv b \bmod m$. That is

$$a \equiv b \bmod m \Leftrightarrow m \mid a - b.$$

DEFINITION 2B.2. A relation $\sim$ in a nonempty set A is called an equivalence relation in A if

1) $(\forall a \in A)[a \sim a]$
2) $a \sim b \Rightarrow b \sim a$
3) $[a \sim b \;\&\; b \sim c] \Rightarrow a \sim c$. For each $a \in A$ we define the equivalence class of a,

$$[a] = \{x \in A | x \sim a\}.$$

Clearly $a \sim b$ if and only if $[a] = [b]$.

It is easy to check that the relation $\sim$ defined by

$$a \sim b \Leftrightarrow a \equiv b \bmod m$$

is an equivalence relation.

Definition 2B.3. If $x \equiv a \bmod m$ then a is called a **residue** of x modulo m. If $0 \leq a \leq m-1$, then a is **the least non-negative residue** of x modulo m.

The equivalence class of $a \in \mathbb{Z}$ is

$$\begin{aligned}[a] &= \{x \in \mathbb{Z} | \, x \equiv a \bmod m\} \\ &= \{x \in \mathbb{Z} | \, m \mid x - a\} \\ &= \{x \in \mathbb{Z} | \, x - a = km, \text{ for some } k \in \mathbb{Z}\}.\end{aligned}$$

Definition 2B.4. We denote by $\mathbb{Z}_m$ the set of all equivalence classes defined by (2B.1). A **complete set of (incongruent) residues mod** m is any set X of natural numbers which contains exactly one member of each equivalence class $[a] \in \mathbb{Z}_m$, for example the set $\{0, 1, 2, \ldots, m-1\}$.

Theorem 2B.5. *Suppose that $(m, m') = 1$ and that a and a' run through a complete set of incongruent residues modulo m and m' respectively. Then $a'm + am'$ runs through a complete set of incongruent residues modulo mm'.*

Proof. There are m possible values for a and m' possible values for a'. So there are in total mm' possible values for $a'm + am'$. If two of these numbers were congruent then

$$a_1'm + a_1m' \equiv a_2'm + a_2m' \bmod mm'$$

which means that

$$mm' \mid (a_1' - a_2')m + (a_1 - a_2)m',$$

so

$$m \mid (a_1' - a_2')m + (a_1 - a_2)m' \quad \text{and} \quad m' \mid (a_1' - a_2')m + (a_1 - a_2)m'$$

and as $(m, m') = 1$ the latter yields

$$m \mid a_1 - a_2 \quad \text{and} \quad m' \mid a_1' - a_2',$$

or equivalently

$$a_1 \equiv a_2 \bmod m \quad \text{and} \quad a_1' \equiv a_2' \bmod m'$$

which is a contradiction.

Hence the mm' numbers are all incongruent and form a complete set of residues mod mm'. ⊣

Definition 2B.6. A function $f(m)$ is **multiplicative** if $(m, m') = 1$ implies that

$$f(mm') = f(m)f(m').$$

THEOREM 2B.7. *(a) If $f(m)$ and $h(m)$ are multiplicative functions of m, then so is $g(m) = f(m)h(m)$.*

(b) If $f(m)$ is a multiplicative function of m, then so is

$$g(m) = \sum_{d|m} f(d).$$

PROOF. (a) Take m, m' such that $(m, m') = 1$. Then

$$\begin{aligned} g(mm') = f(mm')h(mm') &= f(m)f(m') \cdot h(m)h(m') \\ &= f(m)h(m) \cdot f(m')h(m') = g(m)g(m'). \end{aligned}$$

(b) Take m, m' such that $(m, m') = 1$. If $d \mid m$, and $d' \mid m'$, then $(d, d') = 1$ and $c = dd'$ runs through all positive divisors of mm'. Hence

$$\begin{aligned} g(mm') = \sum_{c|mm'} f(c) &= \sum_{d|n, d'|n'} f(dd') \\ &= \sum_{d|m} f(d) \sum d' \mid m' f(d') = g(m)g(m'). \end{aligned}$$

⊣

DEFINITION 2B.8 (**Euler's function** $\phi(n)$). We denote by $\phi(n)$ the number of positive integers not greater than and coprime to n. That is the number of integers satisfying:

$$0 < m \leq n, \qquad (m, n) = 1.$$

THEOREM 2B.9. *Euler's function $\phi(n)$ is multiplicative.*

PROOF. Take m, m' such that $(m, m') = 1$. We want to show that $\phi(mm') = \phi(m)\phi(m')$. By Theorem 2B.5, $a'm + am'$ runs through a complete set of residues $\bmod mm'$ when a and a' run through complete sets $\bmod m$ and $\bmod m'$ respectively. So for finding the value of $\phi(mm')$ we just have to find the number of values of $a'm + am'$ which are prime to mm'. But

$$\begin{aligned} (a'm + am', mm') = 1 &\Leftrightarrow [(a'm + am', m) = 1 \ \& \ (a'm + am', m') = 1] \\ &\Leftrightarrow [(am', m) = 1 \ \& \ (a'm, m') = 1] \\ &\Leftrightarrow [(a, m) = 1 \ \& \ (a', m') = 1]. \end{aligned}$$

Therefore the $\phi(mm')$ numbers less than and prime to mm' are the least positive residues of the $\phi(m)\phi(m')$ values of $a'm + am'$ for which a is prime to m and a prime to m'. ⊣

Theorem 2B.9 gives us an easy way to compute the values of $\phi(m)$:

THEOREM 2B.10. *For all $m \geq 2$,*

$$\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

Proof. First of all, for p prime,

$$\phi(p^c) = p^c - p^{c-1} = p^c\Big(1 - \frac{1}{p}\Big),$$

because the positive numbers less than or equal to p^c that are *not* prime to p^c are the multiples of p that have the form ap, where $1 \le a \le p^{c-1}$, and there are p^{c-1} such numbers.

Now if $m = p_1^{a_1} \cdots p_s^{a_s}$ then using Theorem 2B.9 and this we get

$$\begin{aligned}\phi(m) &= \phi(p_1^{a_1}) \cdots \phi(p_s^{a_s}) \\ &= p_1^{a_1}\Big(1 - \frac{1}{p_1}\Big) \cdots p_s^{a_s}\Big(1 - \frac{1}{p_s}\Big) \\ &= m \prod_{p \mid m} \Big(1 - \frac{1}{p}\Big).\end{aligned}$$

⊣

2C. Dirichlet series

A real **Dirichlet series** is a series of the form

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \quad s \in \mathbb{R}.$$

The sum of the series $F(s)$ is called the **generating function** of a_n.

Theorem 2C.1 (Uniqueness Theorem ([3], §17.1)). *If* $\sum a_n n^{-s} = 0$ *for* $s > s_0$, *then* $a_n = 0$ *for all* n.

As a consequence if

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

for $s > s_1$, *then* $a_n = b_n$ *for all* n.

Multiplication of Dirichlet Series. We are given a finite set of Dirichlet Series

$$\sum \alpha_n n^{-s}, \sum \beta_n n^{-s}, \sum \gamma_n n^{-s}, \dots , \tag{53}$$

and we want to compute their **formal product**, that is we want to compute a series $\sum \chi_n n^{-s}$ such that

$$\chi_n = \sum_{uvw\cdots = n} \alpha_u \beta_u \gamma_w \cdots . \tag{54}$$

A way to understand the formal product is that we want to form all possible products with one factor selected from each series.

The cases we will most often encounter is the multiplication of two or three series.

Say we want to multiply $\sum \alpha_n n^{-s}$ and $\sum \beta_n n^{-s}$. If we denote their formal product by $\sum \xi_n n^{-s}$ then

$$\xi_n = \sum_{uv=n} \alpha_u \beta_v = \sum_{d|n} \alpha_d \beta_{\frac{n}{d}} = \sum_{d|n} \alpha_{\frac{n}{d}} \beta_d. \tag{55}$$

And if the two series are absolutely convergent, and their sums are $F(s)$ and $G(s)$, then we can write

$$\begin{aligned} F(s)G(s) &= \sum_u \alpha_u u^{-s} \sum_v \beta_v v^{-s} = \sum_{u,v} \alpha_u \beta_v (uv)^{-s} \\ &= \sum_n n^{-s} \sum_{uv=n} \alpha_u \beta_v = \sum_n \xi_n n^{-s}. \end{aligned}$$

Notice that we have just rearranged the terms of the product.

The definition of the formal product can be extended to an infinite set of series.

We will now have to take

$$\alpha_1 = \beta_1 = \gamma_1 = \ldots = 1$$

because we want the term $\alpha_u \beta_v \gamma_w \ldots$ in (54) to contain only a finite number of factors which are not 1 (every $n = \alpha_u \beta_v \gamma_w \ldots \in \mathbb{N}$ is finite), and if the series is absolutely convergent[1] we can define χ_n by (54).

Theorem 2C.2 ([3], Theorem 285). *If $f(1) = 1$ and $f(n)$ is multiplicative, then*

$$\sum f(n) n^{-s}$$

is the formal product of the series

$$1 + f(p)p^{-s} + f(p^2)p^{-2s} + \ldots + f(p^a)p^{-as} + \ldots.$$

Proof. We are now considering the case when the series (53) are

$$1 + f(p)p^{-s} + f(p^2)p^{-2s} + \ldots + f(p^a)p^{-as} + \ldots$$

where $p = 2, 3, 5, \ldots$ takes value over all primes. The Fundamental Theorem of Algebra guarantees that every n occurs only once as a product $uvw \cdots$ with a non-zero coefficient, and

$$\chi_n = f(p_1^{a_1}) f(p_2^{a_2}) \cdots = f(n)$$

for $n = p_1^{a_1} p_2^{a_2} \cdots$. ⊣

Corollary 2C.3. *The formal product of the series*

$$1 + p^{-s} + p^{-2s} + \ldots + p^{-as} + \ldots \quad \textit{is} \sum n^{-s}.$$

[1] We must assume *absolute* convergence because we have not specified the order in which the terms are to be taken.

Theorem 2C.4 ([3], Theorem 286). *If $f(1) = 1$ and $f(n)$ is multiplicative and*

$$\sum |f(n)| n^{-s}$$

is convergent, then

$$F(s) = \sum f(n) n^{-s} = \prod_p [1 + f(p)p^{-s} + f(p^2)p^{-2s} + \dots].$$

Proof. The terms of the series $\prod_{p \le P}[1 + f(p)p^{-s} + f(p^2)p^{-2s} + \dots]$ are all terms of the form

$$\begin{aligned}2^{-a_2 s}3^{-a_3 s}\cdots P^{-a_P s} f(2^{-a_2})f(3^{-a_3})\cdots f(P^{-a_P}) \\ = (2^{a_2}3^{a_3}\cdots P^{a_P})^{-s} f(2^{a_2}3^{a_3}\cdots P^{a_P}),\end{aligned}$$

where $a_2 \ge 0, a_3 \ge 0, \dots, a_p \ge 0$. Note that we have just used the multiplicative property of f. The Fundamental Theorem of Arithmetic guarantees that each of these terms appears only once. Letting $n = 2^{a_2}3^{a_3}\cdots P^{a_P}$ this yields

$$\prod_{p \le P}[1 + f(p)p^{-s} + f(p^2)p^{-2s} + \dots] = \sum_{n \in H_P} f(n) n^{-s}$$

where $H_P = \{n \in \mathbb{N} \mid p \mid n \Rightarrow p \le P, \text{for } p \text{ prime }\}$ is the set of all numbers, that do not have any prime factors greater than P.

As $\{n \in \mathbb{N} \mid n \le P\} \subset H_P$, we have

$$0 < \Big| \sum_{n=1}^{\infty} f(n) n^{-s} - \sum_{n \in H_P} f(n) n^{-s} \Big| \le \sum_{n \notin H_P} |f(n)| n^{-s} \le \sum_{P+1}^{\infty} |f(n)| n^{-s}.$$

But

$$\lim_{P \to \infty} \sum_{P+1}^{\infty} |f(n)| n^{-s} = 0,$$

and so

$$\begin{aligned}\sum_{n=1}^{\infty} f(n) n^{-s} &= \lim_{P \to \infty} \sum_{n \in H_P} f(n) n^{-s} \\ &= \lim_{P \to \infty} \prod_{p \le P}[1 + f(p)p^{-s} + f(p^2)p^{-2s} + \dots] \\ &= \prod_p [1 + f(p)p^{-s} + f(p^2)p^{-2s} + \dots].\end{aligned}$$

⊣

2D. Arithmetical functions and their order of growth

DEFINITION 2D.1 (**The Möbius function $\mu(n)$**). is defined as follows:
(i) $\mu(1) = 1$
(ii) $\mu(n) = 0$ if n has a square factor;
(iii) $\mu(p_1 p_2 \cdots p_k) = (-1)^k$ if all the primes $p_1, p_2, \dots, p_k$ are different.
One can see from the definition of $\mu(n)$ that it is multiplicative.

The Möbius functions combines well with the Principle of Inclusion and Exclusion, as in the following facts.

PROPOSITION 2D.2. *Let $D = \{p_1, \dots, p_n\}$ be a set of distinct prime numbers and let A be a given finite set of integers. Denote by S the number of elements of A which are not divisible by any of p_i's, and by S_d number of elements of A divisible by d. Then we have*

$$S = \sum_{d | p_1 \cdots p_n} \mu(d) S_d. \tag{56}$$

PROOF. We apply Corollary 2A.2, taking A_i to be the set of elements of A divisible by p_i. Then for $d = p_{i_1} \dots p_{i_s}$

$$S_d = S_{p_{i_1} \dots p_{i_s}} = |A_{i_1} \cap \dots \cap A_{i_s}|$$

and $\mu(p_{i_1} \dots p_{i_s}) = (-1)^s$, so that

$$T_n = \sum_{d | p_1 \dots p_n} \mu(d) S_d.$$

⊣

PROPOSITION 2D.3. *Suppose $f(k)$ is any complex-valued function.*
(a) Let $D = \{p_1, \dots, p_n\}$ be a set of distinct prime numbers and let A be a given finite set of integers. Then we have

$$\sum_{\substack{x \in A \\ (x, p_1 \cdots p_n) = 1}} f(x) = \sum_{d | p_1 \cdots p_n} \mu(d) \sum_{kd \in A} f(kd).$$

(b) For all j and x:

$$\sum_{\substack{(k,j)=1 \\ k < x}} f(k) = \sum_{d | j} \mu(d) \sum_{kd < x} f(kd).$$

PROOF. (a) We apply Theorem 2A.1, taking A_i to be the set of elements of A divisible by p_i. Then if $d = p_{i_1} \dots p_{i_s}$, and S_d is the set of all elements of A divisible by d, we have

$$S_d = S_{p_{i_1} \dots p_{i_s}} = A_{i_1} \cap \dots \cap A_{i_s} = \{h |\, h \in A, h = kd \text{ for some } k \in \mathbb{N}\}$$

and $\mu(p_{i_1}\dots p_{i_s}) = (-1)^s$, so that

$$T_n = \sum_{d|p_1\dots p_n} \mu(d) \sum_{kd\in A} f(kd).$$

(b) We apply (a) taking A to be the set of all positive integers less than x. Then the positive integers less than x that are coprime with j are coprime with all the prime factors, say $p_1, \dots, p_n$, of j. But if d has a square factor, then $\mu(d) = 0$, so if $p_1, \dots, p_n$ are the different prime factors of j, and we have,

$$\sum_{\substack{(k,j)=1\\ k<x}} f(k) = \sum_{d|p_1\dots p_n} \mu(d) \sum_{kd<x} f(kd) = \sum_{d|j} \mu(d) \sum_{kd<x} f(kd).$$ ⊣

By Proposition 2D.2, taking A to be the set of all numbers less than n and D the set of all prime divisors $p, p', \dots$ of n, we obtain

$$\phi(n) = n - \sum \frac{n}{p} + \sum \frac{n}{pp'} - \dots = n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{p|n} \Big(1 - \frac{1}{p}\Big), \tag{57}$$

which is a strengthened form of Theorem 2B.10.

THEOREM 2D.4.

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if} \quad n = 1 \\ 0 & \text{if} \quad n > 1 \end{cases}$$

PROOF. If $n = 1$ we have $\mu(n) = 1$.

Suppose now that $n > 1$, and the standard form (see the Fundamental Theorem of Arithmetic) of n is

$$n = p_1^{a_1} \cdots p_k^{a_k}, \text{ where } k \geq 1$$

then using only the definition of $\mu(d)$ we have

$$\begin{aligned}\sum_{d|n} \mu(d) &= 1 + \sum_{i} \mu(p_i) + \sum_{i,j} \mu(p_i p_j) + \dots \\ &= 1 - k + \binom{k}{2} - \binom{k}{3} + \dots = (1-1)^k = 0.\end{aligned}$$ ⊣

PROPOSITION 2D.5 (**The Möbious inversion formula**). *If*

$$g(n) = \sum_{d|n} f(d), \textit{ then } f(n) = \sum_{d|n} \mu(\frac{n}{d}) g(d) = \sum_{d|n} \mu(d) g(\frac{n}{d}).$$

PROOF. We have

$$\sum_{d|n} \mu(d) g\Big(\frac{n}{d}\Big) = \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} f(c) = \sum_{cd|n} \mu(d) f(c) = \sum_{c|n} f(c) \sum_{d|\frac{n}{c}} \mu(d).$$

But form Theorem 2D.4

$$\sum_{d|\frac{n}{c}} \mu(d) = \begin{cases} 1 & \text{if } \dfrac{n}{c} = 1 \Leftrightarrow n = c \\ 0 & \text{otherwise} \end{cases}$$

which yields

$$\sum_{c|n} f(c) \sum_{d|\frac{n}{c}} \mu(d) = f(n).$$

For further reference see [3], §16.4. ⊣

Definition 2D.6 (**The zeta function**). The zeta function is the simplest infinite Dirichlet series

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

It converges for $s > 1$. In particular (for a proof you can see [2])

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}. \tag{58}$$

Theorem 2D.7 (Theorem 280, [3]). *For $s > 1$ we have*

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}.$$

Proof. Since $p \geq 2$, for $s > 1$ we have

$$\frac{1}{1 - p^{-s}} = 1 + p^{-s} + p^{-2s} + \dots .$$

Now the terms of the series $\prod_{p \leq P}(1 + p^{-s} + p^{-2s} + \dots)$ are all terms of the form

$$2^{-a_2 s} 3^{-a_3 s} \cdots P^{-a_P s} = (2^{a_2} 3^{a_3} \cdots P^{a_P})^{-s},$$

where $a_2 \geq 0, a_3 \geq 0, \dots, a_p \geq 0$. The Fundamental Theorem of Arithmetic guarantees that each of these terms appears only once. Letting $n = 2^{a_2} 3^{a_3} \cdots P^{a_P}$ this yields

$$\prod_{p \leq P} \frac{1}{1 - p^{-s}} = \sum_{n \in H} n^{-s}$$

where $H_P = \{n \in \mathbb{N} \mid p \mid n \Rightarrow p \leq P, \text{for } p \text{ prime}\}$ is the set of all numbers, that do not have any prime factors greater than P.

As $\{n \in \mathbb{N} \mid n \leq P\} \subset H_P$, we have

$$0 < \sum_{n=1}^{\infty} n^{-s} - \sum_{n \in H_P} n^{-s} < \sum_{P+1}^{\infty} n^{-s}.$$

But

$$\lim_{P\to\infty}\sum_{P+1}^{\infty} n^{-s} = 0$$

and so by the Sandwich Theorem

$$\sum_{n=1}^{\infty} n^{-s} = \lim_{P\to\infty}\sum_{n\in H} n^{-s} = \lim_{P\to\infty}\prod_{p\leq P}\frac{1}{1-p^{-s}} = \prod_{p}\frac{1}{1-p^{-s}}. \qquad \dashv$$

THEOREM 2D.8 (Theorem 287 [3]). *We have*

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

PROOF.

$$\begin{aligned}
\frac{1}{\zeta(s)} &= \prod_p (1-p^{-s}) && \text{by Theorem 2D.7}\\
&= \prod_p [1+\mu(p)p^{-s}+\mu(p^2)p^{-2s}+\dots] && \mu(n) \text{ is multiplicative}\\
&= \sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} && \text{by Theorem 2C.4.}
\end{aligned} \qquad \dashv$$

The function $d(n)$ is the number of divisors of n, including 1 and n.

$$d(n) = \sum_{d|n} 1$$

by Theorem 315, p.260 of [3], for all ϵ:

$$d(n) = O(n^{\epsilon}). \tag{59}$$

The function $\sigma_k(n)$ is the sum of the k-th powers of the divisors of n. Thus

$$\sigma_k(n) = \sum_{d|n} d^k.$$

So

$$\sigma_0(n) = d(n)$$

and reversing the order of summation, (which is a very common trick,)

$$\sigma_{-1}(n) = \sum_{d|n}\frac{1}{d} = \sum_{d|n}\frac{d}{n} = \frac{1}{n}\sum_{d|n} d = \frac{1}{n}\sigma_1(n).$$

The order of $\sigma_1(n)$ is $O(n \ln\ln n)$. See Theorem 323, p.266 of [3]. Consequently it is

$$\sigma_{-1}(n) = O(\ln\ln n). \tag{60}$$

Now we are going to see two theorems that enable us to get very useful results about the order of growth of sums over the integers using integrals. Our presentation is based on [3] and [9]. In the latter book you can also find other similar results.

THEOREM 2D.9. *Suppose* $c_1, c_2, \dots$ *is a sequence of numbers, such that*

$$C(t) = \sum_{n \le t} c_n, \tag{61}$$

and $f(t)$ *is a function of* t. *Then*

$$\sum_{n \le x} c_n f(n) = \sum_{n \le x-1} C(n)\{f(n) - f(n+1)\} + C(x) f(\lfloor x \rfloor). \tag{62}$$

And if $c_j = 0$ *for* $j < n_1$ *and* $f'(t)$ *is continuous for* $t \ge n_1$, *we also have*

$$\sum_{n \le x} c_n f(n) = C(x) f(x) - \int_{n_1}^{x} C(t) f'(t) dt. \tag{63}$$

PROOF. Let $N = \lfloor x \rfloor$. From (61) we get

$$C(1) = c_1, C(2) = c_1 + c_2, \dots, c(N) = c_1 + \dots + c_n$$

so

$$c_1 = C(1), c_2 = C(2) - C(1), \dots, c_n = C(N) - C(N-1)$$

Substituting these expressions for $c_1, c_2, \dots, c_n$ we get that

$$\sum_{n \le x} c_n f(n) = C(1)f(1) + \{C(2) - C(1)\} f(2) + \dots + \{C(N) - C(N-1)\} f(N)$$
$$= C(1)\{f(1) - f(2)\} + \dots + C(N-1)\{f(N-1) - f(N)\} + C(N) f(N).$$

And as $C(N) = C(\lfloor x \rfloor) C(x)$ we have proved (62).

For the proof of the second part the main observation is that $C(t) = C(n)$ when $n \le t < n+1$, and so

$$C(n)\{f(n) - f(n+1)\} = -C(n) \int_n^{n+1} f'(t) dt$$
$$= -\int_n^{n+1} C(t) f'(t) dt.$$

Consequently

$$\begin{aligned}\sum_{n\le x} c_n f(n) &= C(x)f(\lfloor x\rfloor) - \sum_{n\le x-1}\int_n^{n+1} C(t)f'(t)dt\\ &= C(x)f(\lfloor x\rfloor) - \int_{n_1}^{\lfloor x\rfloor} C(t)f'(t)dt\\ &= C(x)f(\lfloor x\rfloor) - \int_{n_1}^{x} C(t)f'(t)dt + \int_{\lfloor x\rfloor}^{x} C(t)f'(t)dt\\ &= C(x)f(\lfloor x\rfloor) - \int_{n_1}^{x} C(t)f'(t)dt + C(x)\{f(x)-f(\lfloor x\rfloor)\}\\ &= C(x)f(x) - \int_{n_1}^{x} C(t)f'(t)dt.\end{aligned}$$

⊣

THEOREM 2D.10. *If a function decreases to zero and has a continuous derivative in the interval* $[1,\infty)$*, then for every* $x \ge 1$ *we have*

$$\sum_{n\le x} f(n) = (f(1)-C) + \int_1^\infty f(t)dt + O(f(t))$$

with $C = \int_1^x (\lfloor t\rfloor - t)f'(t)dt$.

PROOF. Taking $c_n = 1$ and $n_1 = 1$ we get $C(t) = \lfloor t\rfloor$ and so equation (63) gives

$$\sum_{n\le x} f(n) = \lfloor x\rfloor f(x) - \int_1^x \lfloor t\rfloor f'(t)dt \tag{64}$$

We can take $C = \int_1^x (\lfloor t\rfloor - t)f'(t)dt$ as the integral is convergent being majorized by $\int_1^\infty \big(-f'(t)\big)dt = f(1)$. So we can write

$$\begin{aligned}\int_1^x \lfloor t\rfloor f'(t)dt &= \int_1^x (\lfloor t\rfloor - t)f'(t)dt + \int_1^x tf'(t)dt\\ &= \int_1^\infty (\lfloor t\rfloor - t)f'(t)dt - \int_x^\infty (\lfloor t\rfloor - t)f'(t)dt\\ &\qquad\qquad + \Big([tf(t)]_1^x - \int_1^x f(t)dt\Big)\\ &= C - \int_x^\infty (\lfloor t\rfloor - t)f'(t)dt + xf(x) - f(1) - \int_1^x f(t)dt\\ &= C - O(\int_x^\infty -f'(t)dt) + xf(x) - f(1) - \int_1^x f(t)dt\\ &\quad (\text{as } 0 \le t - \lfloor t\rfloor < 1)\\ &= C + xf(x) - f(1) - \int_1^x f(t)dt - O(f(x)).\end{aligned}$$

Substituting now in (64) we get

$$\begin{aligned}\sum_{n\le x} f(n) &= (\lfloor x\rfloor - x)f(x) - C + f(1) + \int_1^x f(t)dt + O(f(x))\\ &= f(1) - C + \int_1^x f(t)dt + O(f(x))\end{aligned}$$

using again that $0 \le x - \lfloor x\rfloor < 1$. ⊣

COROLLARY 2D.11 ([3] Theorem 422).

$$\sum_{k\le n}\frac{1}{k} = \ln n + \gamma + O(\frac{1}{x}) = \ln n + O(1), \tag{65}$$

where

$$\gamma = 1 - \int_1^\infty \frac{(t-\lfloor t\rfloor)}{t^2}dt.$$

This is very basic asymptotic formula of which we will very frequently make use.

PROOF. We will use the previous Theorem (2D.10) applied to the function $f(t) = \dfrac{1}{t}$. (Of course $\lim_{t\to\infty} f(t) = 0$.)

$$\begin{aligned}\sum_{n\le x}\frac{1}{n} &= 1 - C + \int_1^x \frac{1}{t}dt + O\Big(\frac{1}{x}\Big)\\ &= \ln x + \gamma + O\Big(\frac{1}{x}\Big),\end{aligned}$$

where

$$\gamma = 1 - C = 1 - \int_1^\infty \frac{(t-\lfloor t\rfloor)}{t^2}dt.$$

⊣

COROLLARY 2D.12. *We have*

$$\sum_{n\le x}\frac{\ln n}{n} = \frac{1}{2}\ln^2 x + C_1 + O\Big(\frac{\log x}{x}\Big) \tag{66}$$

for some constant C_1.

PROOF. Just as before, we will use Theorem 2D.10 applied to the function $f(t) = \dfrac{\ln t}{t}$. (Of course $\lim_{t\to\infty} f(t) = 0$.)

$$\begin{aligned}\sum_{n\le x}\frac{\ln n}{n} &= 1 - C + \int_1^x \frac{\ln t}{t}dt + O\Big(\frac{\ln x}{x}\Big)\\ &= C_1 + \frac{1}{2}\ln^2 x + O\Big(\frac{\ln x}{x}\Big),\end{aligned}$$

where we have used that

$$\int_1^x \frac{\ln t}{t} dt = \frac{1}{2} \ln^2 t,$$

because

$$\int_1^x \frac{\ln t}{t} dt = \left[\ln^2 t\right]_1^x - \int_1^x \frac{\ln t}{t} dt. \qquad \dashv$$

LEMMA 2D.13.

$$\sum_{n \leq x} \frac{\ln n}{n^2} = O(1) \tag{67}$$

$$\sum_{n \leq x} \frac{(\ln n)^2}{n^2} = O(1) \tag{68}$$

PROOF. By de l' Hospital's we have

$$\lim_{r\to\infty} \frac{(\ln r)^2}{r^2} = \lim_{r\to\infty} \frac{\ln r}{r^2} = \lim_{r\to\infty} \frac{1}{2r^2} = 0$$

and since

$$\sum_{r=1}^{\infty} \frac{1}{r^2} < \infty,$$

we have that

$$\sum_{r=1}^{\infty} \frac{(\ln r)^2}{r^2} = O(1), \qquad \sum_{r=1}^{\infty} \frac{\ln r}{r^2} = O(1). \qquad \dashv$$

LEMMA 2D.14.

$$\sum_{r>x} \frac{1}{r^2} = O(\frac{1}{x}) \tag{69}$$

PROOF.

$$\sum_{r\geq x} \frac{1}{r^2} < \sum_{r\geq x} \frac{1}{r(r+1)} = \Big(\frac{1}{x} - \frac{1}{x+1}\Big) + \Big(\frac{1}{x+1} - \frac{1}{x+2}\Big) + \dots$$
$$= \frac{1}{x} + \lim_{k\to\infty} \frac{-1}{x+k} = O(\frac{1}{x}). \qquad \dashv$$

The rest of the chapter will be very useful for anyone who would like to read Heilbronn's paper [4]. (It was very interesting to see which ideas of [4] are reproduced in [6] and how they are extended.)

Lemma 2D.15.

$$\sum_{d=1}^{n}\frac{\mu(d)}{d^2}=\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}-\sum_{d>n}\frac{\mu(d)}{d^2} \tag{70}$$
$$=\frac{1}{\zeta(2)}-\sum_{d>n}\frac{\mu(d)}{d^2}=\frac{6}{\pi^2}+O(\frac{1}{n}).$$

Lemma 2D.16.

$$\sum_{m=1}^{n}\frac{\phi(m)}{m}=n\frac{6}{\pi^2}+O(\ln n) \tag{71}$$

Proof. The method of proof is very similar to that of [3], Theorem 330. We have:

$$\begin{aligned}
\sum_{m=1}^{n}\frac{\phi(m)}{m} &= \sum_{m=1}^{n}\sum_{d|m}\frac{\mu(d)}{d}=\sum_{dd'\le n}\frac{\mu(d)}{d}\\
&=\sum_{d=1}^{n}\frac{\mu(d)}{d}\sum_{d'=1}^{\lfloor\frac{n}{d}\rfloor}1=\sum_{d=1}^{n}\frac{\mu(d)}{d}\lfloor\frac{n}{d}\rfloor\\
&=\sum_{d=1}^{n}\frac{\mu(d)}{d}\Big(\frac{n}{d}+O(1)\Big)\\
&=n\sum_{d=1}^{n}\frac{\mu(d)}{d^2}+O(\sum_{d=1}^{n}\frac{\mu(d)}{d})\\
&=n\frac{6}{\pi^2}+nO(\frac{1}{n})+O(\sum_{d=1}^{n}\frac{1}{d}) \qquad \text{(by (70) and as } |\mu(d)|\le 1)\\
&=n\frac{6}{\pi^2}+nO(\frac{1}{n})+O(\ln n) \qquad \text{(by (65))}\\
&=n\frac{6}{\pi^2}+O(\ln n).
\end{aligned}$$

⊣

Lemma 2D.17.

$$\sum_{m=1}^{n}\frac{\phi(m)}{m^2}=\ln n\frac{6}{\pi^2}+O(1) \tag{72}$$

Proof. The proof is very similar to that of the previous lemma:
First of all

$$\sum_{d=1}^{n}\frac{\mu(d)}{d^2}=\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}-\sum_{d>n}\frac{\mu(d)}{d^2} \tag{73}$$
$$=\frac{6}{\pi^2}+O(\frac{1}{n})$$

$$
\begin{aligned}
\sum_{m=1}^{n} \frac{\phi(m)}{m^2} &= \sum_{m=1}^{n} \frac{1}{m} \sum_{d|m} \frac{\mu(d)}{d} = \sum_{dd' \leq n} \frac{\mu(d)}{d^2 d'} = \sum_{d=1}^{n} \frac{\mu(d)}{d^2} \sum_{d'=1}^{\lfloor \frac{n}{d} \rfloor} \frac{1}{d'} \\
&= \sum_{d=1}^{n} \frac{\mu(d)}{d^2} \Big(\ln \lfloor \frac{n}{d} \rfloor + O(1) \Big) \\
&= \sum_{d=1}^{n} \frac{\mu(d)}{d^2} \Big(\ln \frac{n}{d} + O(1) \Big) \\
&\qquad \text{(by the Mean Value Theorem)} \\
&= \ln n \sum_{d=1}^{n} \frac{\mu(d)}{d^2} - \sum_{d=1}^{n} \frac{\mu(d) \ln d}{d^2} + O(1) \sum_{d=1}^{n} \frac{\mu(d)}{d^2} \\
&= \frac{6}{\pi^2} \ln n + O(1) \qquad (\textit{by } (68))
\end{aligned}
$$

⊣

Note also the inequality:

$$
\frac{6}{\pi^2} = \frac{1}{\zeta(2)} < \frac{\phi(n)}{n} \sigma_{-1}(n) \leq 1, \tag{74}
$$

which holds because

$$
\frac{1}{\zeta(2)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} < \sum_{d|n} \frac{\mu(d)}{d} \sum_{d|n} \frac{1}{d} = \frac{\phi(n)}{n} \sigma_{-1}(n).
$$

CHAPTER 3

AVERAGE CASE ANALYSIS OF THE SUBTRACTIVE EUCLIDEAN ALGORITHM

In this (main) part of this paper, we will establish an asymptotic formula for the average complexity of the subtractive Euclidean algorithm, the celebrated Yao-Knuth result in [6].

3A. Preliminaries

In this Chapter we deal with *simple continued fractions whose first partial quotient is zero*, that is continued fractions of the form:

$$\cfrac{1}{x_1 + \cfrac{1}{x_2 + \ddots + \cfrac{1}{x_r}}} = /0, x_1, x_2, \dots, x_r/$$

Obviously any continued fraction in this class lies in the interval $[0, 1]$. This is a short of normalization, very useful when one wants to use probability theory, see for instance [6].

Now the basic observation is that

$$/0, x_1, x_2, \dots, x_r/ = \frac{1}{/x_1, x_2, \dots, x_r/}. \tag{75}$$

This gives us an easy way to modify the results of Chapter 1.

THEOREM 3A.1. *(analog of Theorem 1A.8)*

$$/0, x_0, x_1, \dots, x_n/ = \frac{Q_n(x_1, x_2, \dots, x_n)}{Q_{n+1}(x_0, x_1, \dots, x_n)}. \tag{76}$$

PROOF is easy, taking the reciprocal of the continued fraction in Theorem 1A.8. ⊣

If the partial quotients of the Q-polynomials in (76) are evaluated over $\mathbb{N} \setminus \{0\}$ they are relatively prime by Theorem 1D.4 and we will make very frequent use of this fact.

We will use very few results about continued fractions, but a very good general understanding of Q-polynomials and continued fractions is crucial for understanding the proofs in this chapter.

Subtractive Euclidean Algorithm. Here is Euclid's succinct description of the subtractive Euclidean algorithm: given two numbers, replace repeatedly the larger number by the difference of the two until both are equal; then their greatest common divisor is the common value.

For example:

$$\{18, 42\} \to \{18, 42 - 18 = 24\} \to \{18, 24 - 18 = 6\} \to \{18 - 6 = 12, 6\} \\ \to \{12 - 6 = 6, 6\}.$$

so the answer is 6. And the number of subtraction steps is 4.

More strictly the Subtractive Euclidean Algorithm can be formulated as follows:

1. If $u = 1$ or $v = 1$ terminate with 1 as the answer.
2. If $u = v$, terminate with u as the answer.
3. If $u > v$ set $u \leftarrow u - v$ and go to 1.
4. If $u < v$ set $v \leftarrow v - u$ and go to 1.

The Euclidean algorithm with use of division is:

$$42 = 18 \cdot 2 + 6$$
$$18 = 6 \cdot 3 + 0$$

the continued fraction representation of $\dfrac{18}{42}$ is:

$$\frac{18}{42} = 0 + \cfrac{1}{2 + \cfrac{1}{3}} = 0 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1}}} = /0, 2, 2, 1/$$

$$q_1 = 2, \quad q_2 = 2$$

The number of subtraction steps equals 2+2=4. This is reasonable: when we divide two numbers n, m such that $n = q \cdot m + r$ with $0 \leq r < n$ it is the same as subtracting m from n, q times. (Recall that the partial quotients in the continued fraction algorithm are exactly the quotients in the Euclidean algorithm.)

So the division $42 = 18 \cdot 2 + 6$ corresponds to the two subtractions:

$$\{18, 42 - 18 = 24\} \to \{18, 24 - 18 = 6\},$$

while the division $18 = 6 \cdot 2 + 6$ corresponds to the two subtractions:

$$\{18 - 6 = 12, 6\} \to \{12 - 6 = 6, 6\}.$$

In our example the two possible continued fraction representations are $/0, 2, 2, 1/$ and $/0, 2, 3/$. The reason we choose the representation $/0, 2, 2, 1/$ and do not count the final 1 when counting the subtraction steps, is that if we implement the division algorithm with subtractions we perform one more subtraction step than does the original subtractive algorithm for the gcd which in our example is $\{6, 6\} \to \{6, 0\}$. (The subtractive algorithm terminates when the two numbers of the pair are equal.)

Definition 3A.2. Let $r = r(m, n)$ denote the number of divisions by the Euclidean Algorithm.

Theorem 3A.3. *For all $n \geq m \geq 2$, $r(m, n) \leq 2 \log m$. Consequently $r(m, n) = O(\log n)$.*

Proof is by complete induction on m. We must consider three cases:

Case 1, $m \mid n$; now $r(n, m) = 1 \leq 2 \log m$, since $m \geq 2$ and so $\log m \geq 1$.

Case 2, $n = mq_1 + r_1$ with $0 < r_1 < m$, but $r_1 \mid m$; now $r(n, m) = 2$, and $2 \leq 2 \log m$, as above.

Case 3, $n = mq_1 + r_1$ and $m = r_1 q_2 + r_2$ with $0 < r_2 < r_1 < m$. Notice that the last, triple inequality implies that $m \geq 3$. If $r_2 = 1$, then only one more division is needed, so $r(n, m) = 3$, and (easily) $3 < 2 \log 3 \leq 2 \log m$. Suppose then that $r_2 \geq 2$, and consider the next division,

$$r_1 = r_2 q_3 + r_3 \qquad (q_3 \geq 1, 0 \leq r_3 < r_2).$$

Using the facts that $q_2 \geq 1$ and $r_2 < r_1$,

$$m = r_1 q_2 + r_2 \geq r_1 + r_2 > 2r_2,$$

which by the Induction Hypothesis for $r_2 \geq 2$ gives

$$\begin{aligned} r(n, m) = 2 + r(r_1, r_2) &\leq 2 + 2 \log r_2 \\ &\leq 2 + 2 \log(\frac{m}{2}) = 2\Big(1 + \log(\frac{m}{2}\Big) \leq 2 \log m, \end{aligned}$$

as required. ⊣

Definition 3A.4. Let $S(n)$ denote the average number of steps to compute (m, n) by the subtractive Euclidean Algorithm, when m is uniformly distributed in the range $1 \leq m \leq n$.

We will prove the following main theorem:

Theorem 3A.5 (Yao & Knuth).

$$S(n) = \frac{6}{\pi^2}(\ln n)^2 + O(\log n (\log \log n)^2)$$

It is obvious that this proof has been the result of a very careful reading and deep understanding of [4]. Heilbronn was in fact interested in a Number Theoretic question, that turned out to be essentially the question of the average case analysis of the Euclidean Algorithm (with division).

Let $\lfloor x \rfloor$ denote the largest integer less than or equal to x.

Then $x \bmod y = x - y\lfloor \frac{x}{y} \rfloor$ is the remainder of x after division by y.

If $1 \le m \le n$, then by the continued fraction algorithm there is a unique (because of the 1 at the end) finite sequence of integers such that

$$\frac{m}{n} = /0, q_1, q_2, \ldots, q_r, 1/$$

Moreover the q_i s are the quotients in the Euclidean algorithm that uses division. We have $1 \le m \le n$, hence $\frac{m}{n} \le 1$ Suppose the division equation for the pair $\{n, m\}$ is:

$$n = q_1 m + r_1, \quad 0 \le r_1 < m$$

If $r_1 = 0$ then $\frac{m}{n} = \frac{m}{q_1 m} = \frac{1}{q_1}$.

Else if $r_1 \neq 0$ it is

$$\frac{m}{n} = \frac{1}{\frac{n}{m}} = \frac{1}{\frac{mq_1 + r_1}{m}} = \frac{1}{q_1 + \frac{r_1}{m}}$$

where

$$q_1 = \lfloor \frac{n}{m} \rfloor, \qquad \frac{r_1}{m} = \frac{n \bmod m}{m} < 1.$$

Now since $\frac{n \bmod m}{m} < 1$ we can continue the algorithm substituting $\frac{m}{n}$ by $\frac{n \bmod m}{n}$.

The number of subtractions required to compute the gcd (m, n) is precisely $q_1 + q_2 + \ldots + q_r$, because we subtract the smaller integer m from the greater n "as many times as we can", that is $q_1 = \lfloor \frac{n}{m} \rfloor$ times, so we subtract until the remainder is strictly less than the greater number. Then we see how many times we can subtract the previous remainder from the smaller number. So we see that the subtractive algorithm does exactly the same computations as the Euclidean algorithm, when division is implemented by successive subtractions, so that *each division with quotient q corresponds to q subtractions of the same number.* Except for the last step, where we perform $q - 1$ in order to end up with two numbers, both equal to the greatest common divisor, rather than with a zero and the greatest common divisor.

So if we let

$$C(m,n) = q_1(m,n) + \ldots + q_{r(m,n)}(m,n)$$

then the average number of steps of the Subtractive Euclidean Algorithm will be

$$S(n) = \frac{\sum_m C(m,n)}{n} = \frac{\sum_{m=1}^{n} \sum_{i=1}^{r(m,n)} q_i(m,n)}{n} \tag{77}$$

(m is uniformly distributed in $[1,n]$ so the probability to hit some specific value of m is $\frac{1}{n}$.)

What we are going to do next is reduce the problem of computing the quotients q_i, to the problem of adding up all solutions of the equation $xx' + yy' = n$ under certain conditions.

Definition 3A.6. For $n \geq 1$, a quadruple $\{x, x', y, y'\}$ is an **H-representation of** n if

$$n = xx' + yy', \quad (x,y) = 1$$

$$x > y > 0, \qquad x' \geq y' > 0.$$

The name H-representation was given by Yao and Knuth to honor Hans Heilbronn, as it is a sharpened form of a representation first introduced by Heilbronn in [4].

Theorem 3A.7. *There is a* 1-1 *correspondence between H-representations of* n *and ordered pairs* $\{m, j\}$ *where*

$$0 < m < \frac{1}{2}n, \quad \textit{and} \quad 1 \leq j \leq r(m,n).$$

Furthermore if $\{x_j, x'_j, y_j, y'_j\}$ *corresponds to* $\{m, j\}$, *and* q_j *is the* $j+1$*-th partial quotient in the continued fraction*

$$\frac{m}{n} = /0, q_1, q_2, \ldots, q_j, \ldots, q_r, 1/,$$

then

$$\frac{y_j}{x_j} = /0, q_j, \ldots, q_1/ \qquad \frac{y'_j}{x'_j} = /0, q_{j+1}, \ldots, q_r, 1/$$

and consequently

$$\lfloor \frac{x_j}{y_j} \rfloor = q_j. \tag{78}$$

Note that the proof of Theorem 3A.7 that will be given here is not the one presented in the paper by Yao and Knuth but is very similar to the proof given by Heilbronn in [4] and gives a much better overview of what an H-representation actually does. The recursive properties of the

H-representations highlighted by the proof given by Yao and Knuth are presented in the Appendix.

Proof. Let $d = (m, n)$ be the gcd of m and n then we can develop $\frac{m}{n}$ in a unique way as a continued fraction ending with a 1:

$$\frac{m}{n} = /0, q_1, q_2, \ldots, q_r, 1/ = \frac{Q_r(q_2, \ldots, q_r, 1)}{Q_{r+1}(q_1, \ldots, q_r, 1)}$$

The Q-polynomials in this representation are relatively prime. (See Theorem 1D.4 and Theorem 3A.1.) So

$$m = d \cdot Q_r(q_2, \ldots, q_r, 1) \quad n = d \cdot Q_{r+1}(q_1, \ldots, q_r, 1)$$

we have supposed that $0 < \frac{m}{n} = \cfrac{1}{q_1 + \cfrac{1}{\cdots}} < \frac{1}{2}$, so it is

$$q_1 > 1. \tag{79}$$

Starting with a pair $\{m, j\}$ let it correspond to the H-representation

$$\{x_j, x'_j, y_j, y'_j\}$$

where

$$\begin{aligned} x_j &= Q_j(q_1, \ldots, q_j) & x'_j &= d \cdot Q_{r-j+1}(q_{j+1}, \ldots, q_r, 1) \\ y_j &= Q_{j-1}(q_1, \ldots, q_{j-1}) & y'_j &= d \cdot Q_{r-j}(q_{j+2}, \ldots, q_r, 1) \end{aligned}$$

then $\{x_j, x'_j, y_j, y'_j\}$ is an H-representation:

$$(x_j, y_j) = 1, \quad \text{by Theorem 1B.2}$$

Moreover by Theorem 1B.4,

$$x_j x'_j + y_j y'_j = d \cdot Q_r(q_1, \ldots, q_r, 1) = n$$

and as $1 \leq j \leq r$ one immediately sees that

$$x_j > y_j \geq y_1 = Q_0 = 1 > 0$$

$$x'_j \geq y'_j \geq x'_r = y'_r = d > 0$$

so that

$$\begin{aligned} x_j &> y_j > 0 \\ x'_j &\geq y'_j > 0. \end{aligned}$$

Notice that $x_1 = Q_1(q_1) = q_1 > y_1 = Q_0 = 1$ by (79) and that the only case when $x'_j = y'_j$ is for $j = r$, when $x'_r = y'_r = d$.

We also observe that

$$\frac{y_j}{x_j} = /0, q_j, \ldots, q_1/ \qquad \frac{y'_j}{x'_j} = /0, q_{j+1}, \ldots, q_r, 1/$$

Consequently as $/0, q_{j-1}, \dots, 1/ < 1$, we have

$$\frac{x_j}{y_j} = q_j + /0, q_{j-1}, \dots, 1/, \text{ hence } \lfloor \frac{x_j}{y_j} \rfloor = q_j.$$

The correspondence we have established is $1-1$, because supposing two different pairs $\{m, j\}$ and $\{m_1, j_1\}$ corresponded to the same H-representation $\{x, x', y, y'\}$, then if

$$(80) \quad \frac{m}{n} = /0, q_1, \dots, q_r/, \ q_r > 1 \quad \text{and} \quad \frac{m_1}{n} = /0, p_1, \dots, p_{r_1}/, \ p_{r_1} > 1$$

we would have $\frac{y}{x} = /0, q_j, \dots, q_1/$ and $\frac{y}{x} = /0, p_{j_1}, \dots, q_1/$, which by the uniqueness of a continued fraction representation ending with a 1, means that $j = j_1$ and $p_j = q_j, \dots, p_1 = q_1$. In the same way $\frac{y'}{x'} = /0, q_{j+1}, \dots, q_r, 1/$ and $\frac{y'}{x'} = /0, p_{j+1}, \dots, p_{r_1}, 1/$ implies that $r = r_1$ and $q_{j+1} = p_{j+1}, \dots, q_r = p_r$. But then by equation (80) we also have $m = m_1$.

Conversely given an H-representation $\{x, x', y, y'\}$ of n we can determine the unique $\{m, j\}$ it corresponds to as follows.

First let

$$d = (x', y')$$

Then develop $\frac{y}{x}$ and $\frac{x'}{y'}$ as continued fractions, with last partial quotient greater than 1 (for the uniqueness).

$$\frac{y}{x} = /0, a_j, \dots, a_1/ = \frac{Q_{j-1}(a_{j+1}, \dots, a_1)}{Q_j(a_j, \dots, a_1)}$$

$$\frac{y'}{x'} = /0, b_1, \dots, b_s/ = \frac{d \cdot Q_{s-1}(b_2, \dots, b_s)}{d \cdot Q_s(b_1, \dots, b_s)}$$

The numbers $a_j, \dots, a_1, b_1, \dots, b_s$ are uniquely determined by $\{x, x', y, y'\}$. The number that is represented by the continued fraction

$$/0, a_1, \dots, a_j, b_1, \dots, b_s/$$

has denominator n because

$$/0, a_1, \dots, a_j, b_1, \dots, b_s/ = \frac{Q_{j+s-1}(a_2, \dots, a_j, b_1, \dots, b_s)}{Q_{j+s}(a_1, \dots, a_j, b_1, \dots, b_s)}$$

Again by Theorem 1B.4,

$$
\begin{aligned}
d \cdot Q_{j+s}(a_1, \ldots, a_j, b_1, \ldots, b_s) \\
&= Q_j(a_1, \ldots, a_j)[d \cdot Q_s(b_1, \ldots, b_s)] \\
&\quad + Q_{j-1}(a_1, \ldots, a_{j-1})[d \cdot Q_{s-1}(b_2, \ldots, b_s)] \\
&= xx' + yy' = n
\end{aligned}
$$

So $/0, a_1, \ldots, a_j, b_1, \ldots, b_s/ = \dfrac{m}{n}$, for some number m, and as we have taken $a_1 > 1$, it is also $1 \leq m < \frac{1}{2}n$. That is starting with an H-representation $\{x, x', y, y'\}$ of n we have found the unique pair $\{m, j\}$ it corresponds to. ⊣

Corollary 3A.8.

$$nS(n) = 2\sum \lfloor \frac{x}{y} \rfloor + 1 - (n \bmod 2)$$

where the sum is over all H-representations of n.

Proof. By the previous lemma the sum $\sum \lfloor \frac{x}{y} \rfloor$ over all H-representations, equals the total number of subtractions to compute the greatest common divisor of m and n, (m, n) for $1 \leq m < \dfrac{1}{2}n$.

It is also the total number of subtractions to compute (m, n) for $\frac{1}{2}n < m < n$, since if we have some m with

$$1 \leq m < \frac{1}{2}n \quad \text{then} \quad \frac{1}{2}n < n - m < n$$

and the subtractive algorithm for the pair $\{m, n\}$ differs from the subtractive algorithm for the pair $\{n - m, n\}$ only at the first step, so they have the same number of steps:

$$
\begin{aligned}
\{m, n\} &\to \{n - m, m\} \to \ldots \to \{(m, n), (m, n)\} \\
\{n - m, n\} &\to \{n - m, m\} \to \ldots \to \{(n - m, n), (n - m, n)\}.
\end{aligned}
$$

Finally we add the cases:

Case 1. $m = n$ here the algorithm ends after 0 steps. (We add 0 to the formula.)

Case 2. $m = \dfrac{1}{2}n$ this case occurs only for n even and needs one step:

$$\{\frac{n}{2}, n\} \to \{\frac{n}{2}, \frac{n}{2}\}$$

Consequently for the two previous cases we add

$$1 - (n \bmod 2)$$

steps to the formula, as

$$1 - (n \bmod 2) = \begin{cases} 1 & \text{if } n \bmod 2 \equiv 0 \\ 0 & \text{otherwise.} \end{cases} \qquad \dashv$$

3B. Reduction of the problem

Let

$$\sum{}' \lfloor \frac{x}{y} \rfloor$$

denote the sum over all H-representations of n with $x'y < \frac{1}{2}n$.

For the excluded H-representations with

$$\frac{n}{x'y} \leq 2$$

we have

$$1 < \frac{x}{y} < \frac{x}{y} + \frac{y'}{x'} = \frac{n}{x'y} \leq 2$$

(we use the fact that $0 < y' \leq x'$ and that $0 < y < x$), so

$$1 < \frac{x}{y} < 2$$

which means that the excluded H-representations have

$$\lfloor \frac{x}{y} \rfloor = 1.$$

By (77) and Corollary 3A.8 we have

$$nS(n) = \sum_{m=1}^{n} \sum_{i=1}^{r(m,n)} q_i(m,n) = 2 \sum \lfloor \frac{x}{y} \rfloor + 1 - (n \bmod 2). \tag{81}$$

And as by Theorem 3A.3, $r = r(m,n) = O(\log n)$, we have

$$\sum_{m=1}^{n} \sum_{i=1}^{r(m,n)} 1 = n \cdot O(\log n),$$

so

$$\sum \lfloor \frac{x}{y} \rfloor = \sum{}' \lfloor \frac{x}{y} \rfloor + O(n \log n). \tag{82}$$

The following Theorem determines which H-representations of n satisfy $x'y < \dfrac{1}{2}n$, and consequently gives us a way to compute the sum $\sum{}' \lfloor \frac{x}{y} \rfloor$.

THEOREM 3B.1. *Given $x', y > 0$ and $x'y < \frac{1}{2}n$, there exist H-representations (x, x', y, y') of n if and only if*

$$(y, n) = (y, x').$$

And when this holds there are exactly $(y, n) \prod(1-p^{-1})$ such H-representations, where the product is over all primes p which divide (y, n) but not $\frac{y}{(y,n)}$.

PROOF. First let (x, x', y, y') be an H-representation of n then, as

$$n = xx' + yy' \text{ and } (x, y) = 1$$

we have

$$\left.\begin{array}{rl} (y,n) \mid yy' - n = xx' \overset{(x,y)=1}{\Rightarrow} & (y,n) \mid x' \\ \text{and of course} & (y,n) \mid y \end{array}\right\} \Rightarrow (y,n) \mid (x', y). \tag{83}$$

Moreover

$$\left.\begin{array}{r} (y,x') \mid yy' + xx' = n \\ (y,n) \mid y \end{array}\right\} \Rightarrow (x', y) \mid (y, n). \tag{84}$$

So by (83) and (84) we get

$$(y, x') = (y, n).$$

For the other direction let

$$d = (y, n) = (y, x').$$

Then there exist $a, b \in \mathbb{Z}$ such that

$$d = ax' + by.$$

We will show that if $x', y > 0$ and $x'y < \frac{1}{2}n$ then (x, x', y, y') is an H-representation.

Lemma A. *Suppose at least one of the numbers x, y', n is different than zero and that $d \mid n$ and let $d = (y, x')$.*

(a) The set of all solutions $\{x, y'\}$ to

$$n = x'x + yy' \tag{85}$$

is given by

$$\{x_q, y'_q\} = \Big\{\frac{an + qy}{d}, \frac{bn - qx'}{d}\Big\}, \quad \textit{for } q \in \mathbb{Z},$$

where $a, b \in \mathbb{Z}$ are such that $d = ax' + by$.

(b) For $k = 0, 1, 2, \dots, d-1$, exactly one value of q will give

$$k \cdot \frac{x'}{d} < y' = \frac{bn - qx'}{d} \leq (k+1) \cdot \frac{x'}{d}.$$

(c) Exactly d consecutive values of q will satisfy

$$0 < \frac{bn - qx'}{d} \leq x', \ \ i.e.\ y' \leq x'.$$

Proof. (a) Suppose we have a solution to (85), say $\{x_0, y_0'\}$, and take

$$\{x, y'\} = \{x_0 + q\frac{y}{d}, y_0' - q\frac{x'}{d}\}, \quad \text{where } q \in \mathbb{Z}. \tag{86}$$

We observe that for any $q \in \mathbb{Z}$, $\{x, y'\}$ satisfies the equation $x'x + yy' = n$.

We also have that all solutions to the equation $n = x'x + yy'$ are of the form (86). Because if we have two pairs $\{x, y'\}$ and $\{x_0, y_0'\}$, such that

$$n = x'x + yy'$$
$$n = x'x_0 + yy_0',$$

we get

$$x'(x - x_0) = y(y_0' - y'), \tag{87}$$

and as $d = (y, x')$,

$$\frac{x'}{d}(x - x_0) = \frac{y}{d}(y_0' - y').$$

Since $(\frac{x'}{d}, \frac{y}{d}) = 1$, we get that $\frac{x'}{d} \mid y_0' - y'$. Hence there exists a $q \in \mathbb{Z}$ such that $y_0' - y' = q\frac{x'}{d}$, which means that $y' = y_0' - q\frac{x'}{d}$. Then by (87) we also get $x = x_0 + q\frac{y}{d}$.

So starting with a single solution $\{x_0, y_0\}$ to (85) we can express every other solution $\{x, y'\}$ to $n = x'x + yy'$ as

$$\{x, y'\} = \{x_0 + q\frac{y}{d}, y_0 - q\frac{x'}{d}\}, \quad \text{for some } q \in \mathbb{Z}.$$

What remains is to find a solution $\{x_0, y_0'\}$ to (85). We have $d = ax' + by'$. Since $d \mid n$ we have

$$n = d\frac{n}{d} = \frac{an}{d}x' + \frac{bn}{d}y.$$

This means that $\{x_0, y_0'\} = \{\frac{an}{d}, \frac{bn}{d}\}$ is a solution to $n = x'x + yy'$.

(b) We want to see for how many values q we have

$$k \cdot \frac{x'}{d} < y_0 - q\frac{x'}{d} \leq (k+1) \cdot \frac{x'}{d},$$

but this is equivalent to

$$q \cdot \frac{x'}{d} < y_0 - k\frac{x'}{d} \text{ and } q\frac{x'}{d} \geq y_0 - (k+1) \cdot \frac{x'}{d}, \tag{88}$$

and as $x' > 0$, this is equivalent to

$$\frac{y_0 d}{x'} - k > q \geq \Big(\frac{y_0 d}{x'} - k\Big) - 1.$$

But exactly one value of $q \in \mathbb{Z}$ satisfies the preceding inequality. This means that there is a unique y_q with $k \cdot \frac{x'}{d} < y'_q \leq (k+1) \cdot \frac{x'}{d}$.

(c) We have that for $k = 0, 1, 2, \ldots, d-1$, exactly one value of q will be such that $k \cdot \frac{x'}{d} < y'_q \leq (k+1) \cdot \frac{x'}{d}$. Consequently, exactly d values of q will satisfy $0 < y'_q \leq d \cdot \frac{x'}{d}$. These values are consecutive and this can be seen as follows: subtracting 1 from (88), we obtain

$$\frac{y_0 d}{x'} - k - 1 > q - 1 \geq \Big(\frac{y_0 d}{x'} - k - 1\Big) - 1,$$

which is equivalent to

$$(k+1) \cdot \frac{x'}{d} < y_0 - (q+1)\frac{x'}{d} \leq (k+2) \cdot \frac{x'}{d},$$

so if a specific value of q gives a y'_q such that

$$k \cdot \frac{x'}{d} < y'_q \leq (k+1) \cdot \frac{x'}{d},$$

then

$$(k+1) \cdot \frac{x'}{d} < y'_{q-1} \leq (k+2) \cdot \frac{x'}{d}.$$

⊣ (Lemma A)

By Lemma A, exactly d consecutive values of q will satisfy $0 < y' \leq x'$. From the hypothesis we have $x'y < \frac{1}{2}n$, and this yields $\frac{n}{x'} > 2y$, so that we have

$$\frac{n}{x'} - y > y. \tag{89}$$

We have

$$\begin{aligned} x &= \frac{n - yy'}{x'} (\text{as } n = xx' + yy') \\ &\geq \frac{n}{x'} - y \quad (\text{because } \frac{y'}{x'} \leq 1) \\ &> y. \qquad (\text{by } (89)) \end{aligned}$$

So d of the solutions $\{x, y'\}$ to (85) satisfy $x > y > 0$ and $x' \geq y' > 0$. In order to count how many of these d solutions are H-representations, we have to count how many satisfy $(x, y) = 1$.

Lemma B. *If p is a prime divisor of $\frac{y}{d}$, then p does not divide $\frac{an}{d}$, hence p does not divide x.*

Proof. Since $(y, n) = d$, we have

$$(\frac{y}{d}, \frac{n}{d}) = 1,$$

hence if $p \mid \frac{y}{d}$, then $p \nmid \frac{n}{d}$.

Now supposing towards a contradiction that there exists p such that

$$p \mid \frac{y}{d} \quad \text{and} \quad p \mid a$$

we get that

$$p \mid a\frac{x'}{d} + b\frac{y}{d} = 1 \text{ which is a contradiction.}$$

(Note that $d = (y, x')$ yields that $\frac{x'}{d}$ is an integer.)

Now p is prime, $p \nmid a$ and $p \nmid \frac{n}{d}$, so $p \nmid a\frac{n}{d}$. Suppose towards a contradiction that $p \mid x$, then as by the hypothesis $p \mid x$ we would have that $p \mid x = \frac{an + qy}{d}$. So $p \nmid x$. ⊣ (Lemma B)

We have shown that $p \mid \frac{y}{d} \Rightarrow p \nmid x$ which is equivalent to:

$$p \mid x \Rightarrow p \nmid \frac{y}{d}. \tag{90}$$

Lemma C. *Let $p_1, \dots, p_s$ be the primes that divide d but not $\frac{y}{d}$. Then if q takes $p_1 \cdots p_s$, consecutive values the set of all*

$$x_q = \frac{an}{d} + q\frac{y}{d},$$

is a complete system of incongruent residues $\bmod (p_1 \cdots p_s)$*, and $\phi(p_1 \cdots p_s) = (p_1 - 1) \cdots (p_s - 1)$ of these values x_q will be relatively prime to $p_1 \cdots p_s$ and satisfy $(y, x_q) = 1$.*

Proof. Taking $p_1 \cdots p_s$ consecutive values of q, we have a complete system of incongruent residues $\bmod (p_1 \cdots p_s)$. By the hypothesis $p_1, \dots, p_s$ do not divide $\frac{y}{d}$, so $(\frac{y}{d}, p_1 \cdots p_s) = 1$. Then by [3], Theorem 56, we have that for these values of q, $x_q = \frac{an}{d} + q\frac{y}{d}$ is a complete system of incongruent residues $\bmod (p_1 \cdots p_s)$. Now $\phi(p_1 \cdots p_s) = (p_1 - 1) \cdots (p_s - 1)$ of these values x_q will be relatively prime to $p_1 \cdots p_s$ and will satisfy $(y, x_q) = 1$. Because if we assume towards a contradiction that

$$(y, x_q) \neq 1,$$

then there exists a prime p such that $p \mid x_q$ and $p \mid y$. Applying (90) we get that $p \nmid \frac{y}{d}$. But combining $p \nmid \frac{y}{d}$ and $p \mid y$ we realize that it must be $p \mid d$. Hence p is one of the primes that divide d but not $\frac{y}{d}$, that is $p \in \{p_1, \ldots, p_s\}$. But as $(x_q, p_1 \cdots p_s) = 1$, it is $(x_q, p) = 1$, which means that $p \nmid x_q$ and we have arrived at a contradiction. $\dashv$ (Lemma C)

So taking $p_1 \cdots p_s$ consecutive values of q we get $p_1 \cdots p_s$ values of x_q, and $(p_1 - 1) \cdots (p_s - 1)$ of these satisfy

$$(x_q, y) = 1.$$

But when q takes d consecutive values, we have exactly $\frac{d}{p_1 \cdots p_s}$ complete systems of incongruent residues $\bmod (p_1 \cdots p_s)$, like these in Lemma C. So in order to obtain the total number of solutions that satisfy $(x, y) = 1$ we just multiply $(p_1 - 1) \cdots (p_s - 1)$ by $\frac{d}{p_1 \cdots p_s}$. Consequently the total number of solutions that satisfy $(x, y) = 1$ is:

$$\frac{d(p_1 - 1) \cdots (p_s - 1)}{p_1 \cdots p_s} = d \prod_{\substack{p \mid d \\ p \nmid \frac{y}{d}}} (1 - \frac{1}{p})$$

$\dashv$

DEFINITION 3B.2. Let

$$P(n) = \frac{\phi(n)}{n} = \prod_{p \mid n} \Big(1 - \frac{1}{p}\Big)$$

and let $P(n \setminus m)$ denote the similar product over all primes that divide n but not m, that is

$$P(n \setminus m) = \prod_{\substack{p \mid n \\ p \nmid m}} \Big(1 - \frac{1}{p}\Big).$$

THEOREM 3B.3. *For each $n \geq 2$,*

$$\sum \lfloor \frac{x}{y} \rfloor = \sum_{m \mid n} \sum_{(j,m)=1} P(\frac{n}{m} \setminus j) \sum_{\substack{(k,j)=1 \\ 1 \leq k < \frac{m^2}{2nj}}} \frac{m}{jk} + O(n \log n \cdot \log \log n), \tag{91}$$

where the sum on the left is taken over all H-representations (x, x', y, y') of n. Hence by (81),

$$nS(n) = 2 \sum_{m \mid n} \sum_{(j,m)=1} P(\frac{n}{m} \setminus j) \sum_{\substack{(k,j)=1 \\ 1 \leq k < \frac{m^2}{2nj}}} \frac{m}{jk} + O(n \log n \cdot \log \log n). \tag{92}$$

PROOF. We will assume the "standard" notation (x, x', y, y') for H-representations in the computation which follows.

As $\frac{n}{x'y} = \frac{x}{y} + \frac{y'}{x'}$, by (82) and Theorem 3B.1 we have:

$$\sum \lfloor \frac{x}{y} \rfloor = \sum_{d|n} \sum_{\substack{(y,n)=d \\ 1 \le y < \frac{n}{2}}} \Big(d \cdot P(d \setminus (\frac{y}{d})) \sum_{\substack{(x',y)=d \\ 1 \le x' < \frac{n}{2y}}} \lfloor \frac{x}{y} \rfloor \Big) + O(n \log n)$$

$$= \sum_{d|n} \sum_{\substack{(y,n)=d \\ 1 \le y < \frac{n}{2}}} d \cdot P(d \setminus (\frac{y}{d})) \sum_{\substack{(x',y)=d \\ 1 \le x' < \frac{n}{2y}}} \Big(\frac{n}{x'y} - \frac{y'}{x'} + O(1) \Big)$$

$$+ O(n \log n).$$

But $\frac{y'}{x'} \le 1$, so

$$\sum \lfloor \frac{x}{y} \rfloor = \sum_{d|n} \sum_{\substack{(y,n)=d \\ 1 \le y < \frac{n}{2}}} d \cdot P(d \setminus (\frac{y}{d})) \sum_{\substack{(x',y)=d \\ 1 \le x' < \frac{n}{2y}}} \Big(\frac{n}{x'y} + O(1) \Big) + O(n \log n).$$

If we write $n = md, y = jd, x' = kd$, then

$(y, n) = d$ so $(jd, md) = d$ so $(j, m) = 1$

$(x', y) = d$ so $(kd, jd) = d$ so $(k, j) = 1$

$\frac{m^2}{2n} = \frac{m}{2d}$

$1 \le x'y < \frac{n}{2}$ so $1 \le kj < \frac{m}{2d} = \frac{m^2}{2n}$ and in particular, $j < \frac{m^2}{2n}$.

Replacing these in the formula above, we get, with some work:

$$\sum \lfloor \frac{x}{y} \rfloor = \sum_{m|n} \sum_{\substack{(j,m)=1 \\ j < \frac{m^2}{2n}}} \Big(\frac{n}{m} P(\frac{n}{m} \setminus j) \sum_{\substack{(k,j)=1 \\ 1 \le k < \frac{m^2}{2nj}}} \big(\frac{1}{\frac{n}{m}} \cdot \frac{m}{kj} + O(1) \big) \Big) + O(n \log n)$$

$$= \sum_{m|n} \sum_{\substack{(j,m)=1 \\ j < \frac{m^2}{2n}}} P(\frac{n}{m} \setminus j) \sum_{\substack{(k,j)=1 \\ 1 \le k < \frac{m^2}{2nj}}} \frac{m}{kj}$$

$$+ \sum_{m|n} \frac{n}{m} \sum_{\substack{(j,m)=1 \\ j < \frac{m^2}{2n}}} P(\frac{n}{m} \setminus j) \sum_{\substack{(k,j)=1 \\ 1 \le k < \frac{m^2}{2nj}}} O(1) + O(n \log n).$$

So it is enough to show that

$$\sum_{m|n} \frac{n}{m} \sum_{\substack{(j,m)=1 \\ j < \frac{m^2}{2n}}} P(\frac{n}{m} \setminus j) \sum_{\substack{(k,j)=1 \\ 1 \le k < \frac{m^2}{2nj}}} O(1) = O(n \log n \cdot \log \log n)$$

Indeed,

$$\begin{aligned}
\sum_{m|n}\frac{n}{m}\sum_{\substack{(j,m)=1\\ j<\frac{m^2}{2n}}}P(\frac{n}{m}\setminus j)\sum_{\substack{(k,j)=1\\ k<\frac{m^2}{2nj}}}1 &\leq \sum_{m|n}\frac{n}{m}\sum_{\substack{(j,m)=1\\ j<\frac{m^2}{2n}}}P(\frac{n}{m}\setminus j)\sum_{k<\frac{m^2}{2nj}}1\\
&\leq \sum_{m|n}\frac{n}{m}\sum_{\substack{(j,m)=1\\ j<\frac{m^2}{2n}}}P(\frac{n}{m}\setminus j)\frac{m^2}{2nj}\\
&= \sum_{m|n}\sum_{\substack{(j,m)=1\\ j<\frac{m^2}{2n}}}P(\frac{n}{m}\setminus j)\frac{m}{2j}\\
&\leq \sum_{m|n}\sum_{\substack{(j,m)=1\\ j<\frac{m^2}{2n}}}\frac{m}{2j} \qquad (\text{as } P(\frac{n}{m}\setminus j)\leq 1)\\
&= \sum_{m|n}\frac{m}{2}\sum_{\substack{(j,m)=1\\ j<\frac{m^2}{2n}}}\frac{1}{j}\\
&= \sum_{m|n}\frac{m}{2}\sum_{j<\frac{m^2}{2n}}\frac{1}{j}\\
&= O(\sum_{m|n}\frac{m}{2}\log\frac{m^2}{2n}) \qquad (\text{using } (65))\\
&= O(\log n\sum_{m|n}m) \qquad (\text{using } (93))\\
&= O(\log n\cdot n\log\log n) \qquad (\text{by } (60) \text{ (or [3], Theorem 323)}),
\end{aligned}$$

where

$$\text{(93)} \qquad \begin{aligned}
\ln\frac{m^2}{2n} &= \ln m^2 - \ln\frac{n}{2} = 2\ln m - \ln\frac{n}{2}\\
&= O(\log m) + O(\log n) \overset{m\leq n}{=} O(\log n). \qquad \dashv
\end{aligned}$$

3C. Asymptotic Formulas

In this section we will prove some basic asymptotic formulas, which we will then use to estimate $S(n)$. Many fundamental number theoretic methods are used.

LEMMA 3C.1. *For p prime,*

$$\sum_{p|n} \frac{\log p}{p} = O(\log\log n).$$

PROOF. Let n be divisible by k primes, so $2^k \leq n$ and so $k \leq \log n$. By the Prime Number Theorem ([3], Theorem 9) there exist constants c_1, c_2, such that the jth prime lies between $c_1 j \log j$ and $c_2 j \log j$. Then

$$c_1 j \log j \leq p_j \leq c_2 j \log j \leq c_2 j^2 \Rightarrow \log p_j \leq 2c_2 \log j$$

so

$$\begin{aligned} \sum_{p|n} \frac{\log p}{p} \leq \sum_{1\leq j\leq k} \frac{\log p_j}{p_j} &= O\Big(\sum_{1\leq j\leq k} \frac{\log j}{j\log j}\Big) \\ &= O\Big(\sum_{1\leq j\leq k} \frac{1}{j}\Big) = O(\log k) = O(\log\log n). \end{aligned}$$ ⊣

LEMMA 3C.2.

$$\sum_{d|n} \frac{\mu(d)}{d} \ln(\frac{1}{d}) = \sum_{p|n} \frac{\ln p}{p} P(n \setminus p) = O(\log\log n). \tag{94}$$

PROOF. Let $n = p_1^{a_1} \cdots p_k^{a_k}$, then for $i = 1, \ldots k$, $p_i \mid n$, so

$$\begin{aligned} P(n \setminus p_i) = \prod_{\substack{q|n \\ q\neq p_i}} \Big(1 - \frac{1}{q}\Big) &= \prod_{\substack{q|p_1\cdots p_k \\ q\neq p_i}} \Big(1 - \frac{1}{q}\Big) = \prod_{q|\frac{p_1\cdots p_k}{p_i}} \Big(1 - \frac{1}{q}\Big) \\ &= \frac{\phi(\frac{p_1\cdots p_k}{p_i})}{\frac{p_1\cdots p_k}{p_i}} = \sum_{d|\frac{p_1\cdots p_k}{p_i}} \frac{\mu(d)}{d} \quad \text{(by (57))}. \end{aligned} \tag{95}$$

Using this we can write

$$\begin{aligned} \sum_{d|n} \frac{\mu(d)}{d} \ln\Big(\frac{1}{d}\Big) &= -\sum_{d|n} \frac{\mu(d)}{d} \ln d \\ &= -\sum_{d|p_1\cdots p_k} \frac{\mu(d)}{d} \sum_{p_i|d} \ln p_i \\ &= -\sum_{p_i|n} \ln p_i \sum_{\substack{d|p_1\cdots p_k \\ p_i|d}} \frac{\mu(d)}{d} && \text{(take } h \text{ s.t. } d = h\cdot p_i) \\ &= \sum_{p_i|n} \frac{\ln p_i}{p_i} \sum_{h|\frac{p_1\cdots p_k}{p_i}} \frac{\mu(h)}{h} && \text{(as } \mu(d) = (-1)\cdot\mu(h)) \\ &= \sum_{p|n} \frac{\ln p}{p} P(n \setminus p) && \text{(by (95))} \\ &= O(\sum_{p|n} \frac{\ln p}{p}) && \text{(as } P(n\setminus p) < 1) \\ &= O(\log\log n) && \text{(by Lemma 3C.1).} \end{aligned}$$ ⊣

Now we are ready to find the asymptotic behavior of a sum very similar to that in Lemma 3C.1. Instead of summing over all prime divisors of n we now sum over all positive divisors of n. Notice also that the proof does not only use the result of Lemma 3C.1 but also extends the idea used in its proof.

LEMMA 3C.3.

$$\sum_{d|n} \frac{\ln d}{d} = O\big((\log\log n)^2\big). \tag{96}$$

PROOF. By standard infinite series arguments,

$$\sum_{j=1}^{\infty} \frac{j}{p^{j-1}} \leq \sum_{j=1}^{\infty} \frac{j}{2^{j-1}} < \infty$$

and so

$$1 + \frac{2}{p^1} + \ldots + \frac{j}{p^{j-1}} = O(1).$$

By (60), we have that

$$\sigma_{-1}(\frac{n}{p^j}) = O(\log\log \frac{n}{p^j}) = O(\log\log n),$$

and by Lemma 3C.1, we have that

$$\sum_{p|n} \frac{\ln p}{p} = O(\log\log n).$$

If p is a prime number that divides n and $j > 0$ is such that $p^j \mid n$ but $p^{j+1} \nmid n$, we write $p^j \,||\, n$.

We are now ready to prove our result: If $d = p_{i_1}^{j_{i_1}} \cdots p_{i_s}^{j_{i_s}}$, then

$$\ln d = \ln p_{i_1}^{j_{i_1}} + \cdots + \ln p_{i_s}^{j_{i_s}},$$

and so if we write all numerators of the sum

$$\sum_{d|n} \frac{\ln d}{d}$$

as sums of logarithms of powers of prime numbers, then we have the sum of fractions with numerator the logarithm of a power of a prime number, say p^k, and denominator a divisor of n, that is a multiple of p^k.

Example. Take $n = p_1 p_2^2$, then

$$\sum_{d|n} \frac{\ln d}{d} = \frac{\ln p_2}{p_2} + \frac{\ln p_1}{p_1} + \frac{\ln(p_1 p_2)}{p_1 p_2} + \frac{\ln p_2^2}{p_2^2} + \frac{\ln(p_1 p_2^2)}{p_1 p_2^2}$$

$$= \frac{\ln p_2}{p_2} + \frac{\ln p_1}{p_1} + \frac{\ln p_1 + \ln p_2}{p_1 p_2} + \frac{\ln p_2^2}{p_2^2} + \frac{\ln p_1 + \ln p_2^2}{p_1 p_2^2}$$
$$= \Big(\frac{\ln p_1}{p_1} + \frac{\ln p_1}{p_1 p_2} + \frac{\ln p_1}{p_1 p_2^2}\Big) + \Big(\frac{\ln p_2}{p_2} + \frac{\ln p_2}{p_1 p_2} + \frac{\ln p_2^2}{p_2^2} + \frac{\ln p_2^2}{p_1 p_2^2}\Big)$$
$$= \frac{\ln p_1}{p_1}\Big(1 + \frac{1}{p_2} + \frac{1}{p_2^2}\Big) + \frac{\ln p_2}{p_2}\Big(1 + \frac{1}{p_1}\Big) + \frac{\ln p_2^2}{p_2^2}\Big(1 + \frac{1}{p_1}\Big)$$
$$= \frac{\ln p_1}{p_1}\Big(1 + \frac{1}{p_2} + \frac{1}{p_2^2}\Big) + \Big(\frac{\ln p_2}{p_2} + \frac{\ln p_2^2}{p_2^2}\Big)\Big(1 + \frac{1}{p_1}\Big)$$

The most important step is to show that

$$\sum_{d|n} \frac{\ln d}{d} = \sum_{\substack{p^k | n,\, h | \frac{n}{p^k} \\ (h,p)=1}} \Big(\frac{\ln p^k}{p^k \cdot h}\Big).$$

We need three steps to show this. First, if $d \mid n$ and $d = p^k h$, then

$$\frac{\ln d}{d} = \frac{\ln p^k + \ln h}{h p^k}$$

so each of the terms $\frac{\ln p^k}{p^k h}$ occurs. Second each of these terms occurs exatly once, because $\frac{\ln p^k}{p^k h}$ can only be genearated from $\frac{\ln d}{d}$ with $d = p^k h$ because $(h,p) = 1$. Third is that, obviously, no other terms occur. The key fact for the computation that follows is that if $(h,p) = 1$ and $p^j \,||\, n$ then

$$h \mid \frac{n}{p^j} \Leftrightarrow h \mid \frac{n}{p^k}.$$

We have

$$\sum_{d|n} \frac{\ln d}{d} = \sum_{p^j \,||\, n} \sum_{k=1}^{j} \sum_{\substack{h | \frac{n}{p^k} \\ (h,p)=1}} \Big(\frac{\ln p^k}{p^k \cdot h}\Big)$$
$$= \sum_{p^j \,||\, n} \sum_{k=1}^{j} \Big(\frac{\ln p^k}{p^k}\Big) \sum_{h | \frac{n}{p^j}} \frac{1}{h}$$
$$= \sum_{p^j \,||\, n} \Big(\frac{\ln p}{p} + \frac{\ln p^2}{p^2} + \ldots + \frac{\ln p^j}{p^j}\Big) \sum_{d | \frac{n}{p^j}} \frac{1}{d}$$
$$= \sum_{p^j \,||\, n} \frac{\ln p}{p}\Big(1 + \frac{2}{p^1} + \ldots + \frac{j}{p^j}\Big)\sigma_{-1}(\frac{n}{p^j})$$
$$= O((\log\log n)^2). \qquad \dashv$$

LEMMA 3C.4. *For every x and every j,*

$$\sum_{\substack{(k,j)=1 \\ k<x}} \frac{1}{k} = P(j)\ln x + O(\log\log j).$$

PROOF. (Missing September 20, 2005.) ⊣

DEFINITION 3C.5. We define $\mu_d(r)$ as follows:

$$\mu_d(r) = \begin{cases} \mu(r), & \text{if } (d,r)=1 \\ 0, & \text{otherwise.} \end{cases}$$

LEMMA 3C.6.

$$\sum_{\substack{(j,m)=1 \\ j<x}} \frac{P(j \setminus d)}{j} = P(m)\ln x \sum_{\substack{(r,m)=1 \\ r<x}} \frac{\mu_d(r)}{r^2} + O(\log\log m)$$

PROOF. If $q_1, q_2, \ldots$ are all different prime factors of j *that do not divide* d, we obtain

$$\prod_{\substack{q|j \\ q\nmid d}} \Big(1 - \frac{1}{q}\Big) = 1 - \sum \frac{1}{q_1} + \sum \frac{1}{q_1 q_2} - \ldots,$$

by doing all multiplications on the left hand side of the equality. So by the Definitions 3C.5 and 3B.2, of $\mu_d(r)$ and $P(n \setminus m)$ respectively, we have

$$P(j \setminus d) = \prod_{\substack{q|j \\ q\nmid d}} \Big(1 - \frac{1}{q}\Big) = \sum_{\substack{r|j \\ (r,d)=1}} \frac{\mu(r)}{r} = \sum_{r|j} \frac{\mu_d(r)}{r},$$

so

$$P(j \setminus d) = \sum_{r|j} \frac{\mu_d(r)}{r}. \tag{97}$$

Now the sum is

$$\begin{aligned} \sum_{\substack{(j,m)=1 \\ j<x}} \frac{1}{j} \cdot P(j \setminus d) &= \sum_{\substack{(j,m)=1 \\ j<x}} \frac{1}{j} \sum_{r|j} \frac{\mu_d(r)}{r} \qquad \text{(by (97))} \\ &= \sum_{\substack{(r,m)=1 \\ r<x}} \frac{\mu_d(r)}{r} \sum_{\substack{(j,m)=1 \\ j<x/r}} \frac{1}{jr} \\ &= \sum_{\substack{(r,m)=1 \\ r<x}} \frac{\mu_d(r)}{r^2} \sum_{\substack{(j,m)=1 \\ j<x/r}} \frac{1}{j}, \end{aligned}$$

which by use of Lemma 3C.4 becomes,

$$= \sum_{\substack{(r,m)=1 \\ r<x}} \frac{\mu_d(r)}{r^2}\Big(P(m)\ln\frac{x}{r} + O(\log\log m)\Big) \qquad (\text{as } \sum_{r<x}\frac{1}{r^2} < \infty)$$

$$= P(m) \sum_{\substack{(r,m)=1 \\ r<x}} \frac{\mu_d(r)}{r^2}(\ln x - \ln r) + O(\log\log m)$$

$$= P(m) \sum_{\substack{(r,m)=1 \\ r<x}} \frac{\mu_d(r)}{r^2}\ln x + O(\sum_{\substack{(r,m)=1 \\ r<x}} \frac{\mu_d(r)}{r^2}\ln r) + O(\log\log m)$$

$$= P(m)\ln x \sum_{\substack{(r,m)=1 \\ r<x}} \frac{\mu_d(r)}{r^2} + O(\sum_{r<x}\frac{1}{r^2}\ln r) + O(\log\log m),$$

but $\sum_{r<x}\frac{\ln r}{r^2} = O(1)$, by (67), so we finally obtain,

$$\sum_{\substack{(j,m)=1 \\ j<x}} \frac{1}{j}\cdot P(j\setminus d) = P(m)\ln x \sum_{\substack{(r,m)=1 \\ r<x}} \frac{\mu_d(r)}{r^2} + O(\log\log m).$$

⊣

Lemma 3C.7.

$$\sum_{\substack{(j,m)=1 \\ j<x}} \frac{P(j\setminus d)\ln j}{j} = \frac{1}{2}P(m)(\ln x)^2 \sum_{\substack{(r,m)=1 \\ r<x}} \frac{\mu_d(r)}{r^2} + O(\log x\log\log m).$$

Proof. (Missing September 20, 2005.) ⊣

3D. Concluding Steps

From the definition of $P(n)$ it is obvious that:

$$P(a\setminus b)P(b) = P(ab) = P(b\setminus a)P(a)$$

Let $N = \frac{m^2}{2n}$. By Theorem 3B.3, we have that

$$\sum\lfloor\frac{x}{y}\rfloor = \sum_{m|n} m \sum_{\substack{(j,m)=1 \\ j<N}} \frac{P(\frac{n}{m}\setminus j)}{j} \sum_{\substack{(k,j)=1 \\ k<\frac{N}{j}}} \frac{1}{k} + O(n\log n\cdot\log\log n).$$

Using Lemma 3C.4, this yields

$$\sum\lfloor\frac{x}{y}\rfloor = \sum_{m|n} m \sum_{\substack{(j,m)=1 \\ j<N}} \frac{P(\frac{n}{m}\setminus j)}{j}(P(j)\ln(\frac{N}{j}) + O(\log\log j)),$$

$$+ O(n\log n\cdot\log\log n)$$

and as

$$\sum_{m|n} m \sum_{\substack{(j,m)=1\\ j<N}} \frac{P(\frac{n}{m} \setminus j)}{j} = O(\sum_{m|n} m \sum_{\substack{(j,m)=1\\ j<N}} \frac{1}{j}) = O(n\sigma_{-1}(n)\log n)$$

and

$$O(\log\log j) = O(\log\log N) = O(\log\log n)$$

We have

$$\begin{aligned}
\sum \lfloor \frac{x}{y} \rfloor &= \sum_{m|n} m \sum_{\substack{(j,m)=1\\ j<N}} \frac{P(\frac{n}{m})P(j \setminus \frac{n}{m})}{j} \ln(\frac{N}{j}) + O(n\sigma_{-1}(n)\log n \cdot \log\log n)\\
&= \sum_{m|n} mP(\frac{n}{m}) \sum_{\substack{(j,m)=1\\ j<N}} \frac{P(j \setminus \frac{n}{m})}{j} \ln(\frac{N}{j}) + O(n\sigma_{-1}(n)\log n \log\log n)\\
&= \sum_{m|n} mP(\frac{n}{m})\Big(\ln N \sum_{\substack{(j,m)=1\\ j<N}} \frac{P(j \setminus \frac{n}{m})}{j} - \sum_{\substack{(j,m)=1\\ j<N}} \frac{P(j \setminus \frac{n}{m})}{j} \ln j\Big) +\\
&+ O(n\sigma_{-1}(n)\log n \log\log n).
\end{aligned}$$

Here we can apply Lemmata 3C.6 and 3C.7

$$\begin{aligned}
&= \sum_{m|n} mP(\frac{n}{m})\Big(P(m)(\ln N)^2 \sum_{\substack{(r,m)=1\\ r<N}} \frac{\mu_{n/m}(r)}{r^2} - \frac{1}{2}P(m)(\ln N)^2 \sum_{\substack{(r,m)=1\\ r<N}} \frac{\mu_{n/m}(r)}{r^2}\\
&\quad +O(\log N \log\log m) + O(\log\log m)\Big) + O(n\sigma_{-1}(n)\log n \log\log n)\\
&= \frac{1}{2}\sum_{m|n} mP(\frac{n}{m})P(m)\Big(2(\ln N)^2 \sum_{\substack{(r,m)=1\\ r<N}} \frac{\mu_{n/m}(r)}{r^2} - (\ln N)^2 \sum_{\substack{(r,m)=1\\ r<N}} \frac{\mu_{n/m}(r)}{r^2}\Big) +\\
&\quad +O(\log n \log\log n)\sum_{m|n} mP(\frac{n}{m}) + O(n\sigma_{-1}(n)\log n \log\log n)\\
&= \frac{1}{2}\sum_{m|n} mP(\frac{n}{m})P(m)\Big((\ln N)^2 \sum_{\substack{(r,m)=1\\ r<N}} \frac{\mu_{n/m}(r)}{r^2}\Big) +\\
&\quad +O(\log n \log\log n \sum_{m|n} m) + O(n\sigma_{-1}(n)\log n \log\log n)\\
&= \sum_{m|n} mP(\frac{n}{m})\Big(\frac{1}{2}P(m)(\ln N)^2 \sum_{\substack{(r,m)=1\\ r<N}} \frac{\mu_{n/m}(r)}{r^2}\Big) + O(n\sigma_{-1}(n)\log n \log\log n)
\end{aligned}$$

Recall that $\mu_{\frac{n}{m}}(r) = (-1)^s$ if r is the product of $s \geq 0$ distinct primes none of which divide $\dfrac{n}{m}$, otherwise $\mu_{\frac{n}{m}}(r) = 0$. If p is prime, $p \mid r$ and $m \mid n$

and $(r,m)=1$ then we have that $p \mid n$ if and only if $p \mid \dfrac{n}{m}$. From this we deduce that $\mu_{\frac{n}{m}}(r)=\mu_n(r)$. We can write $\ln N$ as

$$\ln N = \ln\frac{m^2}{2n} = \ln(\frac{n}{2}\cdot\frac{m^2}{n^2}) = \ln\frac{n}{2} + \ln\left(\frac{m}{n}\right)^2 = \ln\frac{n}{2} + 2\ln\left(\frac{m}{n}\right)$$

So the formula becomes

$$= \frac{1}{2}\sum_{m|n} mP(\frac{n}{m})P(m)(\ln\frac{n}{2} + 2\ln\left(\frac{m}{n}\right))^2 \sum_{r<N}\frac{\mu_n(r)}{r^2} + O(n\log n(\log\log n)^2)$$

Note that we have removed the condition $(r,m)=1$. This is because if we have $(r,m)\neq 1$, then as $m \mid n$ we also have $(r,n)\neq 1$, so $\mu_n(r)=0$.

$$= \frac{1}{2}\sum_{m|n} mP(\frac{n}{m})P(m)\Big((\ln\frac{n}{2})^2 + 4(\ln 2\Big(\frac{m}{n}\Big))^2 + 4\ln\frac{n}{2}\ln\frac{m}{n}\Big)\sum_{r<N}\frac{\mu_n(r)}{r^2}$$
$$+O(n\log n(\log\log n)^2)$$
$$= \frac{1}{2}\sum_{m|n} mP(\frac{n}{m})P(m)(\ln\frac{n}{2})^2\sum_{r<N}\frac{\mu_n(r)}{r^2} + O(\ln n\sum_{m|n} m\ln\frac{n}{m}O(1))$$
$$+O(n\log n(\log\log n)^2)$$

because $\ln n > \ln\frac{n}{m} > 0$ (which follows from $n > \frac{n}{m} > 1$) and as $P(n)<1$ and $\dfrac{\mu_n(r)}{r^2} = O(1)$,

$$= \frac{1}{2}\sum_{m|n} mP(\frac{n}{m})P(m)(\ln n - \ln 2)^2\sum_{r<N}\frac{\mu_n(r)}{r^2} + O(\log n\sum_{m|n} m\ln\frac{m}{n})$$
$$+O(n\log n(\log\log n)^2).$$

Now by letting $d=\dfrac{n}{m}$ and using (96) we have:

$$\sum_{m|n} m\log\frac{n}{m} = n\sum_{d|n}\frac{\log d}{d} = O(n(\log\log n)^2),$$

and as

$$\ln n\sum_{m|n} mP(\frac{n}{m})P(m)\sum_{r<N}\frac{\mu_n(r)}{r^2} = O(\log n\cdot n\sigma_{-1}(n)),$$

we conclude that

$$\sum\lfloor\frac{x}{y}\rfloor = \frac{1}{2}\sum_{m|n} mP(\frac{n}{m})P(m)(\ln n)^2\sum_{r<N}\frac{\mu_n(r)}{r^2} + O(n\log n(\log\log n)^2).$$

We can extend the sum on r to ∞, since by (59) (or [3], Theorem 315), we have

$$d(n) = \sum_{m|n} 1 = O(n^{\epsilon}) \quad \text{for all positive } \epsilon$$

and

$$\begin{aligned}
\sum_{m|n} m \sum_{r \geq N} \frac{1}{r^2} &\leq \sum_{\substack{m|n \\ m \leq \sqrt{n}}} m \sum_{r \geq 1} \frac{1}{r^2} + \sum_{\substack{m|n \\ m > \sqrt{n}}} m \sum_{r \geq N} \frac{1}{r^2} \\
&= \sum_{\substack{m|n \\ m \leq \sqrt{n}}} m \sum_{r \geq 1} \frac{1}{r^2} + \sum_{\substack{m|n \\ m > \sqrt{n}}} m O(\frac{1}{N}) \qquad \text{(by (69))} \\
&= \sum_{\substack{m|n \\ m \leq \sqrt{n}}} m \sum_{r \geq 1} \frac{1}{r^2} + \sum_{\substack{m|n \\ m > \sqrt{n}}} m O(\frac{n}{m^2}) \qquad (N = \frac{m^2}{n}) \\
&= \sum_{\substack{m|n \\ m \leq \sqrt{n}}} m O(1) + \sum_{\substack{m|n \\ m > \sqrt{n}}} m O(1) \qquad (\text{as } m > \sqrt{n}) \\
&= O(\sqrt{n} \sum_{m|n} 1) + O(\sum_{\substack{m|n \\ m > \sqrt{n}}} m) \\
&= O(n^{\frac{1}{2}+\epsilon}) + O(n \sum_{\substack{m|n \\ m > \sqrt{n}}} \frac{1}{m}) \text{ (by (59) and reversing the sum)} \\
&= O(n^{\frac{1}{2}+\epsilon}) + O(\frac{n}{\sqrt{n}} \sum_{m|n} 1) \\
&= O(n^{\frac{1}{2}+\epsilon}) \qquad \text{(using (59) again).}
\end{aligned}$$

So, as by standard calculus arguments $(\ln n)^2 \cdot n^{\frac{1}{2}+\epsilon} = O(n)$, we have

$$\sum \lfloor \frac{x}{y} \rfloor = \frac{1}{2} \sum_{m|n} m P(\frac{n}{m}) P(m) (\ln n)^2 \sum_{r \geq 1} \frac{\mu_n(r)}{r^2} + O(n \log n (\log\log n)^2). \tag{98}$$

Now the basic formula we will need is

$$\sum_{r \geq 1} \frac{\mu_n(r)}{r^2} = \prod_{p \nmid n} \Big(1 - \frac{1}{p^2}\Big) = \frac{6}{\pi^2} \prod_{p|n} \Big(1 - \frac{1}{p^2}\Big)^{-1}. \tag{99}$$

This can be seen as follows,

$$\frac{1}{\zeta(2)} = \frac{6}{\pi^2} = \prod_p (1-p^{-2}) = \prod_{p\nmid n}(1-p^{-2})\prod_{p\mid n}(1-p^{-2}) \text{ (by Theorem 2D.7)}$$

$$= \prod_p (1+\mu_n(p)p^{-2}+\mu_n(p^2)p^{-4}+\dots)\prod_{p\mid n}(1-p^{-2})$$

$$= \sum_{r=1}^{\infty}\mu_n(r)r^{-2}\prod_{p\mid n}(1-p^{-2}) \qquad \text{(by Theorem 2D.8)}$$

see [3] §17.2, §17.4, §17.5

It remains to evaluate

$$\sum_{m\mid n} mP(\frac{n}{m})P(m),$$

but this is a multiplicative function. To see this take a, b such that $(a,b) = 1$. If $m_1 \mid a$, and $m_2 \mid b$, then $(m_1, m_2) = 1$ and m_1m_2 runs through all positive divisors of ab. Since $\phi(n)$ is multiplicative by Theorem 2B.9, we also have that $P(n) = \dfrac{\phi(n)}{n}$ is multiplicative, so as $(\dfrac{a}{m_1}, \dfrac{b}{m_2}) = 1$,

$$P(\frac{ab}{m_1m_2}) = P(\frac{a}{m_1})P(\frac{b}{m_2}).$$

So

$$\sum_{m\mid ab} mP(\frac{ab}{m})P(m) = \sum_{\substack{m_1\mid a\\ m_2\mid b}} m_1m_2P(\frac{ab}{m_1m_2})P(m_1m_2)$$

$$= \sum_{\substack{m_1\mid a\\ m_2\mid b}} m_1m_2P(\frac{a}{m_1})P(\frac{b}{m_2})P(m_1)P(m_2)$$

$$= \sum_{m_1\mid a} m_1P(\frac{a}{m_1})P(m_1)\sum_{m_2\mid b} m_2P(\frac{b}{m_2})P(m_2).$$

So it suffices to do the evaluation when $n = p^k$:

$$\sum_{m\mid p^k} mP(\frac{p^k}{m})P(m) = \sum_{0\le j\le k} p^j\,\frac{\phi(p^{k-j})}{p^{k-j}}\,\frac{\phi(p^j)}{p^j}$$

$$= \sum_{0<j<k} p^j\Big(1-\frac{1}{p}\Big)^2 + (p^0+p^k)\Big(1-\frac{1}{p}\Big)$$

$$= \sum_{0\le j\le k} p^j\Big(1-\frac{1}{p}\Big)^2 + (p^0+p^k)\Big(\Big(1-\frac{1}{p}\Big)-\Big(1-\frac{1}{p}\Big)^2\Big)$$

$$
\begin{aligned}
&= \Big(1-\frac{1}{p}\Big)^2 \sum_{j=0}^{k} p^j + (1+p^k)\Big(\Big(1-\frac{1}{p}\Big) - \Big(1-\frac{1}{p}\Big)^2\Big) \\
&= \Big(1-\frac{1}{p}\Big)\Big[\Big(1-\frac{1}{p}\Big)\frac{p^{k+1}-1}{p-1} + (1+p^k)\Big(1-\Big(1-\frac{1}{p}\Big)\Big)\Big] \\
&= \frac{p-1}{p}\Big[\frac{p-1}{p}\frac{p^{k+1}-1}{p-1} + \frac{1+p^k}{p}\Big] \\
&= \frac{p-1}{p}\Big[\frac{p^{k+1}+p^k}{p}\Big] = p^k\frac{p-1}{p}\frac{p+1}{p} = p^k\frac{p^2-1}{p} \\
&= p^k\Big(1-\frac{1}{p^2}\Big)
\end{aligned}
$$

So for $n = {p_1}^{k_1}\cdots {p_l}^{k_l}$, we get

$$
\begin{aligned}
\sum_{m|n} mP(\frac{n}{m})P(m) &= {p_1}^{k_1}\cdots {p_l}^{k_l}\cdot\Big(1-\frac{1}{{p_1}^{2k_1}}\Big)\cdots\Big(1-\frac{1}{{p_l}^{2k_l}}\Big) \\
&= n\cdot\prod_{p|n}\Big(1-\frac{1}{p^2}\Big)
\end{aligned}
$$

(98) becomes by use of (99):

$$
\begin{aligned}
\sum\lfloor\frac{x}{y}\rfloor &= \frac{1}{2}(\ln n)^2\sum_{m|n} mP(\frac{n}{m})P(m)\cdot\frac{6}{\pi^2}\prod_{p|n}\Big(1-\frac{1}{p^2}\Big)^{-1} \\
&\qquad + O(n\log n(\log\log n)^2) \\
&= \frac{1}{2}(\ln n)^2 n\cdot\prod_{p|n}\Big(1-\frac{1}{p^2}\Big)\cdot\frac{6}{\pi^2}\prod_{p|n}\Big(1-\frac{1}{p^2}\Big)^{-1} \\
&\qquad + O(n\log n(\log\log n)^2).
\end{aligned}
$$

So finally

$$\sum\lfloor\frac{x}{y}\rfloor = \frac{3}{\pi^2}n(\ln n)^2 + O(n\log n(\log\log n)^2).$$

And by means of Corollary 3A.8, we get Theorem 3A.5:

$$S(n) = \frac{6}{\pi^2}(\ln n)^2 + O(\log n(\log\log n)^2).$$

Remarks

It is very interesting to reproduce some remarks and further references from [1] and [10].

The metric theory of continued fractions has been established by studies of Gauss, Lévy, Khinchin, Kuzmin Wirsing and Babenko. However these results are not of much help with the discrete counterpart of the continued fraction algorithm, i.e. the Euclidean algorithm for positive integers, since rational inputs have measure zero. The standard Euclidean algorithm was first discussed independently by Heilbronn [4] and Dixon [1970, 1971]. While Heilbronn used combinatorial methods, Dixon used probability. Much later Hensley [1992] showed that the number of division steps done by the Euclidean algorithm over all pairs (m, n) with $0 < m \leq n \leq x$ is asymptotically normally distributed, with mean close to $12(\log 2)\pi^{-2} \log x$.

Plankensteiner [1970] counted the number of pairs (m, n) for which the Euclidean Algorithm takes k steps.

A quite different approach, that can deal with many euclidean-like algorithms and gives also, apart from the mean value, the moments of order k was proposed by Vallé [12].

APPENDIX: MORE ON H-REPRESENTATIONS

We have already defined what an H-representation is (recall Definition 3A.6) and we have used H-representations in Theorem 3A.7. Here we will investigate some further aspects of the notion of an H-representation.

If $0 < \dfrac{m}{n} < \dfrac{1}{2}$ and

$$\frac{m}{n} = /0, q_1, q_2, \ldots, q_r, 1/ = \frac{Q_r(q_2, \ldots, q_r, 1)}{Q_{r+1}(q_1, \ldots, q_r, 1)}$$

then by (79), we have $q_1 > 1$.

Let $d = (m, n)$. Using Theorem 1D.4 we obtain $n = d \cdot Q_{r+1}(q_1, \ldots, q_r, 1)$. On the other hand,

$$/0, 1, q_r, \ldots, q_2, q_1/ = \frac{Q_r(q_r, \ldots, q_2, q_1)}{Q_{r+1}(q_1, \ldots, q_r, 1)},$$

thus if we multiply both the numerator and denominator of the fraction with d, we have that

$$/0, 1, q_r, \ldots, q_2, q_1/ = \frac{m'}{n}$$

and from Theorem 1D.4, it follows that $(m, n) = (m', n) = d$.

As $0 < \dfrac{1}{/q_r, \ldots, q_2, q_1/} \leq 1$, we have $1 < /1, q_r, \ldots, q_2, q_1/ \leq 2$. The equality would hold if and only if $r = 1$, $q_r = 1$, that is if $\dfrac{m}{n} = /1, 1/ = \dfrac{1}{2}$, which is impossible from the hypothesis. Hence $\dfrac{1}{2} < \dfrac{m'}{n} < 1$.

In this way we establish a 1-1 correspondence $m \leftrightarrow m'$ between the natural numbers in the open intervals $(0, \frac{1}{2}n)$ and $(\frac{1}{2}n, n)$.

$$m = n \cdot /0, q_1, \ldots, q_r, 1/, \quad m' = n \cdot /0, 1, q_r, \ldots, q_1/, \quad q_1 > 1$$

H-representations can be described through two parallel recursions, the one going up and the other down.

$$\{m, r\} \leftrightarrow \{\frac{m'}{d}, d, \frac{n - m'}{d}, d\}.$$

and recursively, if

$$\{m, j\} \leftrightarrow \{x_j, x'_j, y_j, y'_j\}$$

then

$$\{m, j-1\} \leftrightarrow \{y_j, q_j x'_j + y'_j, x_j - q_j y_j, x'_j\}.$$

The basic remark is that we actually have two pairs

$$\begin{aligned} &\{x_j, y_j\} = \{y_{j-1} + q_j x_{j-1}, x_{j-1}\} \\ &\{x_1, y_1\} = \{q_1, 1\} \end{aligned}$$

and

$$\begin{aligned} &\{x'_{j-1}, y'_{j-1}\} = \{q_j x'_j + y'_j, x'_j\} \\ &\{x'_r, y'_r\} = \{d, d\} \end{aligned}$$

that can be constructed recursively independent of each other. The idea is to "entangle" two recursions -one going down and another going up- in one quadruple. In this way we split the "information" about the q_is occurring in the continued fraction representation of $\frac{m}{n}$ and $\frac{m'}{n}$ in two parts:

$$\begin{aligned} &\frac{y_j}{x_j} = /0, q_j, \dots, q_1/, \qquad q_1 > 1 \\ &\frac{y'_j}{x'_j} = /0, q_{j+1}, \dots, q_r, 1/. \end{aligned}$$

The construction of $\{x_j, y_j\}$ parallels the continued fraction process for $\frac{m'}{n}$ and the construction of $\{x'_j, y'_j\}$ parallels the continued fraction process for $\frac{m}{n}$.

If we write down the Euclidean algorithm for the pair $\{n, m\}$ and the Euclidean Algorithm for the pair $\{\frac{n}{d}, \frac{m'}{d}\}$ we have:

$$\begin{array}{ll}
n = q_1 \cdot m + r_1 & \frac{n}{d} = 1 \cdot \frac{m'}{d} + r'_1 \\
m = q_2 \cdot r_1 + r_2 & \frac{m'}{d} = q_r \cdot r'_1 + r'_2 \\
r_1 = q_3 \cdot r_2 + r_3 & r'_1 = q_{r-1} \cdot r'_2 + r'_3 \\
\vdots & \vdots \\
r_{r-3} = q_{r-1} \cdot r_{r-2} + d & r'_{r-3} = q_3 \cdot r'_{r-2} + r'_{r-1} \\
r_{r-2} = q_r \cdot d + d & r'_{r-2} = q_2 \cdot r'_{r-1} + d \\
d = 1 \cdot d + 0 & r'_{r-1} = q_1 \cdot d + 0
\end{array}$$

this gives a very practical algorithm that allows us to compute H-representations even by hand and bears great similarity to the algorithm Bezout introduced to express the gcd of two numbers as their linear combination.

$$n = q_1 \cdot m + r_1$$
$$n = q_1(q_2 \cdot r_1 + r_2) + r_1 = (q_1q_2 + 1) \cdot r_1 + (q_1)r_2$$
$$n = (q_1q_2 + 1) \cdot (q_3 \cdot r_2 + r_3) + (q_1)r_2 = (q_1q_2q_3 + q_3 + q_1) \cdot r_2 + (q_1q_2 + 1)r_3)$$
$$\vdots$$

$$\begin{array}{rc}
\{m, 1\} \leftrightarrow & \{q_1, m, r_1, 1\} = \{r'_{r-1}, m, r'_r, 1\} \\
\{m, 2\} \leftrightarrow & \{q_1q_2 + 1, r_1, q_1, r_2\} \\
\{m, 3\} \leftrightarrow & \{q_1q_2q_3 + q_1 + q_2, r_2, q_1q_2 + 1, r_3\} \\
\vdots & \\
\{m, r\} \leftrightarrow & \{\frac{m'}{d}, r_{r-1}, \frac{n - m'}{d}, r_r\} = \{\frac{m'}{d}, d, r'_1, d\}
\end{array}$$

Example. Take $n = 720$, $m = 153$ then

$$\frac{m}{n} = /0, 4, 1, 2, 2, 1, 1/$$

so $r = 5$ and

$$\frac{m'}{n} = /0, 1, 1, 2, 2, 1, 4/ = \frac{423}{720}$$

from which we get $m' = 423$, $d = (m, n) = (m', n) = 9$

The continued fraction process (Euclidean algorithm only the two last divisions differ slightly) for the pairs $\{n, m\}$, $\{n, m'\}$ and $\{\frac{n}{d}, \frac{m'}{d}\}$ is:

$720 = 4 \cdot 153 + 108$	$720 = 1 \cdot 423 + 297$	$80 = 1 \cdot 47 + 33$
$153 = 1 \cdot 108 + 45$	$423 = 1 \cdot 297 + 126$	$47 = 1 \cdot 33 + 14$
$108 = 2 \cdot 45 + 18$	$297 = 2 \cdot 126 + 45$	$33 = 2 \cdot 14 + 5$
$45 = 2 \cdot 18 + 9$	$126 = 2 \cdot 45 + 36$	$14 = 2 \cdot 5 + 4$
$18 = 1 \cdot 9 + 9$	$45 = 1 \cdot 36 + 9$	$5 = 1 \cdot 4 + 1$
$9 = 1 \cdot 9 + 0$	$36 = 4 \cdot 9 + 0$	$4 = 4 \cdot 1 + 0$

From this we obtain the H-representations:

$$720 = 4 \cdot 153 + 108$$
$$720 = 4 \cdot (1 \cdot 108 + 45) + 108 = 5 \cdot 108 + 4 \cdot 45$$
$$720 = 5 \cdot (2 \cdot 45 + 18) + 4 \cdot 45 = 14 \cdot 45 + 5 \cdot 18$$
$$720 = 14 \cdot (2 \cdot 18 + 9) + 5 \cdot 18 = 33 \cdot 18 + 14 \cdot 9$$
$$720 = 33 \cdot (1 \cdot 9 + 9) + 14 \cdot 9 = 47 \cdot 9 + 33 \cdot 9$$

$$\{m, 5\} \leftrightarrow \{47, 9, 33, 9\}$$
$$\{m, 4\} \leftrightarrow \{33, 18, 14, 9\}$$
$$\{m, 3\} \leftrightarrow \{14, 45, 5, 18\}$$
$$\{m, 2\} \leftrightarrow \{5, 108, 4, 45\}$$
$$\{m, 1\} \leftrightarrow \{4, 153, 1, 108\}$$

REFERENCES

[1] ERIC BACH and JEFFREY SHALLIT, **Algorithmic number theory**, MIT Press, Cambridge, MA, USA, 1996.

[2] LOUIS BRAND, **Advanced calculus**, 1962 ed., John Wiley and Sons, 1962.

[3] G.H. HARDY, **An introduction to the theory of numbers**, fifth ed., Oxford Science Publications, Oxford Press, 1979.

[4] HANS HEILBRONN, *On the average length of a class of finite continued fractions*, **Number theory and analysis** (Turán P., editor), Plennum Press, New York, 1969, pp. 87–96.

[5] A.Y. KHINCHIN, **Continued fractions**, Dover, 1997.

[6] A.C. YAO & D.E. KNUTH, *Analysis of the subtractive algorithm for greatest common divisors*, **Proc. Nat. Acad. Sci.**, vol. 72 (1979), pp. 4720–4722.

[7] DONALD E. KNUTH, **The art of computer programming**, Addison-Wesley Longman Publishing Co., Inc.Boston, MA, USA, 1997.

[8] SERGE LANG, **Introduction to Diophantine approximations**, second ed., Springer-Verlag, New York, 1995.

[9] W. NARKIEWICZ, **Number theory**, World Scientific, 1983.

[10] F. PHILIPPE, V. BRIGITTE, and V. ILAN, *Continued fractions from euclid to the present day*, 2000.

[11] JOE ROBERTS, **Elementary number theory; a problem-oriented approach**, the MIT Press, 1978.

[12] BRIGITTE VALLÉ, *Dynamical analysis of a class of euclidean algorithms*, **Theor. Comput. Sci.**, vol. 297 (2003), no. 1-3, pp. 447–486.