

Συνεχή κλάσματα & Αφαιρετικός Ευκλείδειος αλγόριθμος

Αγγελίνα Βιδάλη
επιβλέπων καθηγητής: Γιάννης Μοσχοβάκης

μΠ λV

5 Ιουλίου, 2006

Δομή διπλωματικής εργασίας

1ο κεφ. Εισαγωγή στα συνεχή κλάσματα

2ο κεφ. Λίγη Θεωρία Αριθμών

3ο κεφ. Μέση πολυπλοκότητα Αφαιρετικού Ευκλείδειου Αλγόριθμου:

Πρόβλημα:

Έστω n σταθερό. (Και όσο χρειάζεται μεγάλο)

$$1 \leq m \leq n$$

$S(n) = E$ (Πόσες αφαιρέσεις κάνει ο αλγόριθμος
για να βρει τον μ.κ.δ(n, m);)

Θεώρημα (Yao & Knuth 1979)

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

Συνεχή κλάσματα

Συνεχή κλάσματα και \mathbb{Q} -πολυώνυμα

Άπειρα συνεχή κλάσματα

Συνεχή κλάσματα και Ευκλείδειος Αλγόριθμος

Αφαιρετικός Ευκλείδειος αλγόριθμος

Ανάλυση μέσου αριθμού βημάτων

H-αναπαραστάσεις

Πεπερασμένα συνεχή κλάσματα

πεπερασμένο συνεχές κλάσμα στις μεταβλητές x_1, x_2, \dots, x_n :

$$x_0 + \frac{1}{x_1 + \frac{1}{x_2 + \dots + \frac{1}{x_N}}}$$

συμβολισμός: $/x_0, x_1, \dots, x_N/$

Π.χ.

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

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

Q-πολυώνυμα

Ορισμός

Για $n \geq 0$:

$$Q_0 = 1$$

$$Q_1(x_1) = x_1$$

$$Q_n(x_1, x_2, \dots, x_n) = x_1 Q_{n-1}(x_2, \dots, x_n) + Q_{n-2}(x_3, \dots, x_n)$$

Q-πολυώνυμα

Ορισμός

Για $n \geq 0$:

$$Q_0 = 1$$

$$Q_1(x_1) = x_1$$

$$Q_n(x_1, x_2, \dots, x_n) = x_1 Q_{n-1}(x_2, \dots, x_n) + Q_{n-2}(x_3, \dots, x_n)$$

Κατ' αυτόν τον τρόπο παίρνουμε:

$$Q_1(x_1) = x_1$$

$$Q_2(x_1, x_2) = x_1 x_2 + 1$$

$$Q_3(x_1, x_2, x_3) = x_1 x_2 x_3 + x_1 + x_3$$

$$Q_4(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4 + x_1 x_4 + x_3 x_4 + x_1 x_2 + 1.$$

Θεώρημα (L. Euler)

Το πολυώνυμο $Q_n(x_1, x_2, \dots, x_n)$ 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 $x_j \cdot x_{j+1}$.

$$1 \cdot x_1 \cdot x_2 \cdot x_3 \cdot x_4$$

$$Q_4(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4 + x_3 x_4 + x_1 x_4 + x_1 x_2 + 1.$$

Θεώρημα (L. Euler)

Το πολυώνυμο $Q_n(x_1, x_2, \dots, x_n)$ 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 $x_j \cdot x_{j+1}$.

$$1 \cdot x_1 \cdot x_2 \cdot x_3 \cdot x_4$$

$$Q_4(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4 + x_3 x_4 + x_1 x_4 + x_1 x_2 + 1.$$

Θεώρημα (L. Euler)

Το πολυώνυμο $Q_n(x_1, x_2, \dots, x_n)$ 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 $x_j \cdot x_{j+1}$.

$$1 \cdot x_1 \cdot x_2 \cdot x_3 \cdot x_4$$

$$Q_4(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4 + x_3 x_4 + x_1 x_4 + x_1 x_2 + 1.$$

Θεώρημα (L. Euler)

Το πολυώνυμο $Q_n(x_1, x_2, \dots, x_n)$ 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 $x_j \cdot x_{j+1}$.

$$1 \cdot x_1 \cdot x_2 \cdot x_3 \cdot x_4$$

$$Q_4(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4 + x_3 x_4 + x_1 x_4 + x_1 x_2 + 1.$$

Θεώρημα (L. Euler)

Το πολυώνυμο $Q_n(x_1, x_2, \dots, x_n)$ 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 $x_j \cdot x_{j+1}$.

$$1 \cdot x_1 \cdot x_2 \cdot x_3 \cdot x_4$$

$$Q_4(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4 + x_3 x_4 + x_1 x_4 + x_1 x_2 + 1.$$

Q-πολυώνυμα και συνεχή κλάσματα

Θεώρημα

Έχουμε

$$/x_0, x_1, \dots, x_n/ = \frac{Q_{n+1}(x_0, x_1, \dots, x_n)}{Q_n(x_1, x_2, \dots, x_n)},$$

ενώ επιπλέον

$$\mu.κ.δ(Q_{n+1}(x_0, x_1, \dots, x_n), Q_n(x_1, x_2, \dots, x_n)) = 1.$$

Άπειρα συνεχή κλάσματα

Ορισμός

Το $/a_0, a_1, \dots, a_n/$ είναι **απλό** αν $a_0 \geq 0, a_1 > 0, a_2 > 0, \dots$
 $a_0, a_1, a_2, \dots \in \mathbb{N}$

Ορισμός

Έστω a_0, a_1, a_2, \dots μια άπειρη ακολουθία ακεραίων με
 $a_0 \geq 0, a_1 > 0, a_2 > 0, \dots$. Θέτουμε $x_n = /a_0, a_1, \dots, a_n/$. Αν

$$\lim_{n \rightarrow \infty} x_n = x$$

τότε λέμε ότι το άπειρο απλό συνεχές κλάσμα $/a_0, a_1, a_2, \dots/$
συγκλίνει στην τιμή x και γράφουμε $x = /a_0, a_1, a_2, \dots/$.

Θεώρημα

Όλα τα άπειρα απλά συνεχή κλάσματα συγκλίνουν.

Αλγόριθμος ανάπτυξης σε συνεχές κλάσμα

Σε κάθε πραγματικό αριθμό x αντιστοιχούμε δύο ακολουθίες $a_0, a_1, \dots \in \mathbb{N}$ και $\xi_0, \xi_1, \dots \in \mathbb{R}$ ως εξής:

1. Έστω $a_0 = \lfloor x \rfloor$, $\xi_0 = x - a_0$.
2. Αν έχουν οριστεί τα $a_0, \dots, a_n, \xi_0, \dots, \xi_n$, και $\xi_n \neq 0$, τότε θέσει

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

3. Αν $\xi_n = 0$ τότε ο αλγόριθμος τερματίζει και επιστρέφει τα a_0, a_1, \dots, a_n και τα ξ_0, \dots, ξ_n .

έτσι

$$\begin{aligned} x &= a_0 + \xi_0 = a_0 + \frac{1}{a_1 + \xi_1} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \xi_2}} = \dots \\ &= [a_0, \dots, a_n + \xi_n]. \end{aligned}$$

Θεώρημα (Ορθότητα Αλγόριθμου ανάπτυξης σε συνεχές κλάσμα)

- (α) Αν x ρητός τότε ο αλγόριθμος **τερματίζει** με $\xi_N = 0$ για κάποιο $N \geq 0$ και είναι $x = /a_0, \dots, a_N/$.
- (β) Αν x άρρητος, τότε $\xi_n \neq 0$ για όλα τα n , οπότε ο αλγόριθμος **δεν τερματίζει**, και

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

Θεώρημα (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 $v \in \mathbb{N}$ τέτοιοι ώστε

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

Θεώρημα (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 $v \in \mathbb{N}$ τέτοιοι ώστε

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

Θεώρημα (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 $v \in \mathbb{R}$ τέτοιοι ώστε

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

Επιπλέον,

$$q = \left\lfloor \frac{x}{y} \right\rfloor.$$

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, \dots και $v_{-1}, v_0, v_1, v_2, \dots$ ως εξής:

1. Έστω $v_{-1} = x, v_0 = y$
2. Αν τα $v_{-1}, \dots, v_i, a_1, \dots, a_i$ έχουν ορισθεί και $v_i \neq 0$ τότε από το Θεώρημα της Διαίρεσης, πάρε v_{i+1}, a_{i+1} τέτοια ώστε

$$v_{i-1} = v_i a_{i+1} + v_{i+1} \quad 0 \leq v_{i+1} < v_i.$$

3. Αν $v_i = 0$ τότε ο αλγόριθμος τερματίζει και επιστρέφει $v_{-1}, v_0, \dots, v_{i-1}$ και a_1, \dots, a_i .

Ο ευκλείδειος αλγόριθμος δουλεύει για το ζεύγος $\{x, y\}$ ως εξής:

$$x = ya_1 + v_1 \qquad 0 < v_1 < y$$

$$y = v_1 a_2 + v_2 \qquad 0 < v_2 < v_1$$

$$v_1 = v_2 a_3 + v_3 \qquad 0 < v_3 < v_2$$

\vdots

\vdots

$$v_{n-3} = v_{n-2} a_{n-1} + v_{n-1} \qquad 0 < v_{n-1} < v_{n-2}$$

$$v_{n-2} = v_{n-1} a_n \qquad v_n = 0.$$

Αντιστοιχία Ευκλείδειου με αλγ. ανάπτυξης σε συν. κλάσμα

Θεώρημα

(a) Αν υλοποιήσουμε τον Ευκλείδειο Αλγόριθμο, για το ζεύγος $\{x, 1\}$ και a_0, \dots, a_n, \dots : τα πηλίκα που εμφανίζονται τότε $x = /a_1, \dots, a_n, \dots/$.

(b) Αν $x = \frac{h}{k} \in \mathbb{Q}$, $h \geq k$, τότε αν υλοποιήσουμε τον Ευκλείδειο Αλγόριθμο για το ζεύγος $\{h, k\}$. παίρνοντας πάλι τα πηλίκα a_0, \dots, a_n, \dots έχουμε:
 $x = /a_1, \dots, a_n, \dots/$

$$\frac{h}{k} = \frac{a_1 k + v_1}{k} = a_1 + \frac{1}{\frac{k}{v_1}} = a_1 + \frac{1}{\frac{v_1 a_2 + v_2}{v_1}} = a_1 + \frac{1}{a_2 + \frac{1}{\frac{v_1}{v_2}}}$$

Τα συνεχή κλάσματα ως μορφή αναπαράστασης αριθμών

Μερικά αναπτύγματα γνώριμων αριθμών:

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

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

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

$$\phi = /1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, \dots /,$$

$$\text{όπου } \phi = \frac{1 + \sqrt{5}}{2}.$$

Τα συνεχή κλάσματα είναι μια **μορφή αναπαράστασης** των πραγματικών αριθμών. Άλλες αναπαραστάσεις:

- ▶ δεκαδικοί αριθμοί
- ▶ δυαδικοί αριθμοί
- ▶ ανάλυση σε πρώτους παράγοντες (μόνο στο \mathbb{N})

Συνεχή κλάσματα

Συνεχή κλάσματα και \mathbb{Q} -πολυώνυμα

Άπειρα συνεχή κλάσματα

Συνεχή κλάσματα και Ευκλείδειος Αλγόριθμος

Αφαιρετικός Ευκλείδειος αλγόριθμος

Ανάλυση μέσου αριθμού βημάτων

H-αναπαραστάσεις

Αφαιρετικός Ευκλείδειος αλγόριθμος

”ανθυφαιρουμένου αεί του ελάσσονος από του μείζονος”

{18, 42}

1. Αν $u = 1$ ή $v = 1$ τότε $\mu.κ.δ(u, v) = 1$.
2. Αν $u = v$, τότε $\mu.κ.δ(u, v) = u$.
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.

Αφαιρετικός Ευκλείδειος αλγόριθμος

”ανθυφαιρουμένου αεί του ελάσσονος από του μείζονος”

$$\{18, 42\} \rightarrow \{18, 42 - 18 = 24\}$$

1. Αν $u = 1$ ή $v = 1$ τότε $\mu.κ.δ(u, v) = 1$.
2. Αν $u = v$, τότε $\mu.κ.δ(u, v) = u$.
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.

Αφαιρετικός Ευκλείδειος αλγόριθμος

”ανθυφαιρουμένου αεί του ελάσσονος από του μείζονος”

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

1. Αν $u = 1$ ή $v = 1$ τότε $\mu.κ.δ(u, v) = 1$.
2. Αν $u = v$, τότε $\mu.κ.δ(u, v) = u$.
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.

Αφαιρετικός Ευκλείδειος αλγόριθμος

”ανθυφαιρουμένου αεί του ελάσσονος από του μείζονος”

$$\begin{aligned}\{18, 42\} &\rightarrow \{18, 42 - 18 = 24\} \rightarrow \{18, 24 - 18 = 6\} \\ &\rightarrow \{18 - 6 = 12, 6\}\end{aligned}$$

1. Αν $u = 1$ ή $v = 1$ τότε $\mu.κ.δ(u, v) = 1$.
2. Αν $u = v$, τότε $\mu.κ.δ(u, v) = u$.
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.

Αφαιρετικός Ευκλείδειος αλγόριθμος

”ανθυφαιρουμένου αεί του ελάσσονος από του μείζονος”

$$\begin{aligned}\{18, 42\} &\rightarrow \{18, 42 - 18 = 24\} \rightarrow \{18, 24 - 18 = 6\} \\ &\rightarrow \{18 - 6 = 12, 6\} \rightarrow \{12 - 6 = 6, 6\}.\end{aligned}$$

1. Αν $u = 1$ ή $v = 1$ τότε $\mu.κ.δ(u, v) = 1$.
2. Αν $u = v$, τότε $\mu.κ.δ(u, v) = u$.
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.

Ευκλείδιος αλγόριθμος (με διαίρεση):

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

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

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

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

Υλοποίηση διαίρεσης με διαδοχικές αφαιρέσεις:

Αριθμός αφαιρετικών βημάτων: $2+3=5$.

Ευκλείδιος αλγόριθμος (με διαίρεση):

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

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

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

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

Υλοποίηση διαίρεσης με διαδοχικές αφαιρέσεις:

Αριθμός αφαιρετικών βημάτων: $2+3=5$.

-Είναι ο Αφαιρετικός Ευκλείδιος.

Αν $1 \leq m \leq n$, τότε

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

Για $1 \leq i < r$,

τα q_i είναι τα πηλίκα των διαιρέσεων του Ευκλειδείου

Αλγορίθμου:

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

$$m = r_1 q_2 + r_3, \quad 0 < r_2 < r_1$$

...

βημάτων Αφαιρετικού Ευκλειδείου = $q_1 + q_2 + \dots + q_r$.

Μέσος αριθμός βημάτων Αφαιρετικού Ευκλείδειου

Ορισμός

$S(n)$: ο μέσος αριθμός βημάτων για να υπολογίσουμε τον μ.κ.δ(m, n) με τον Αφαιρετικό Ευκλείδειο Αλγόριθμο, όταν το m κατανέμεται ομοιόμορφα στο διάστημα $1 \leq m \leq n$.

Θεώρημα (Yao & Knuth)

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

Μέσος αριθμός βημάτων:

Ευκλειδείου (με διαίρεση)

[Heilbronn 1969]

$$\frac{12 \ln 2}{\pi^2} \ln n + O(n^{-\frac{1}{6}+\epsilon})$$

(worst case complexity: $O(\ln m)$ για διαδοχικούς Fibonacci)

Αφαιρετικού Ευκλειδείου

[Yao&Knuth 1979]

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

(worst case complexity: $O(n)$ για το ζεύγος $\{n, 1\}$)

Πως εμφανίζεται η σταθερά $\frac{6}{\pi^2}$;

$$\frac{1}{\zeta(2)} = \frac{6}{\pi^2}$$

Στο "μέτρημα" εμφανίζεται το γινόμενο:

$$\begin{aligned}\prod_p \left(1 - \frac{1}{p^2}\right) &= \frac{1}{\zeta(2)} \\ &= \left(\sum_{n=1}^{\infty} \frac{1}{n^2}\right)^{-1} \\ &= \end{aligned}$$

Πως εμφανίζεται η σταθερά $\frac{6}{\pi^2}$;

$$\frac{1}{\zeta(2)} = \frac{6}{\pi^2}$$

Στο "μέτρημα" εμφανίζεται το γινόμενο:

$$\begin{aligned}\prod_p \left(1 - \frac{1}{p^2}\right) &= \frac{1}{\zeta(2)} \\ &= \left(\sum_{n=1}^{\infty} \frac{1}{n^2}\right)^{-1} \\ &= \frac{6}{\pi^2}.\end{aligned}$$

Έστω n σταθερό, θέλουμε να υπολογίσουμε το άθροισμα:

$$S(n) = \frac{\sum_{m=1}^n (\# \text{ βημάτων όταν έχω το ζεύγος } \{m, n\})}{n}$$
$$= \frac{\sum_{m=1}^n (q_1^{(m)} + \dots + q_r^{(m)})}{n}$$

όπου

$$\frac{m}{n} = /0, q_1^{(m)}, q_2^{(m)}, \dots, q_r^{(m)}, 1/.$$

Έστω n σταθερό, θέλουμε να υπολογίσουμε το άθροισμα:

$$S(n) = \frac{\sum_{m=1}^n (\# \text{ βημάτων όταν έχω το ζεύγος } \{m, n\})}{n}$$
$$= \frac{\sum_{m=1}^n (q_1^{(m)} + \dots + q_r^{(m)})}{n}$$

όπου

$$\frac{m}{n} = /0, q_1^{(m)}, q_2^{(m)}, \dots, q_r^{(m)}, 1/.$$

Ιδέα:

Θα κάνουμε αναγωγή του προβλήματος σε ένα άλλο:

στο μέτρημα των ακεραίων λύσεων μίας εξίσωσης ως προς n .

Δομή άρθρου (ομοιότητα με τη δομή του άρθρου του Heilbronn)

- ▶ 1ο μέρος

- ▶ παρατήρηση ότι
$$S(n) = \frac{\sum_{m=1}^n (q_1^{(m)} + \dots + q_r^{(m)})}{n}$$

- ▶ 2ο μέρος (Αριθμοθεωρία)

Δομή άρθρου (ομοιότητα με τη δομή του άρθρου του Heilbronn)

► 1ο μέρος

► παρατήρηση ότι $S(n) = \frac{\sum_{m=1}^n (q_1^{(m)} + \dots + q_{r(m)}^{(m)})}{n}$

► Αναγωγή: αρκεί να μετρήσουμε τις H-αναπαράστασεις $\{x, x', y, y'\}$ του n , αφού

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

► 2ο μέρος (Αριθμοθεωρία)

Δομή άρθρου (ομοιότητα με τη δομή του άρθρου του Heilbronn)

► 1ο μέρος

- παρατήρηση ότι $S(n) = \frac{\sum_{m=1}^n (q_1^{(m)} + \dots + q_r^{(m)})}{n}$
- Αναγωγή: αρκεί να μετρήσουμε τις H-αναπαραστάσεις $\{x, x', y, y'\}$ του n , αφού

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

- μέτρημα των H-αναπαραστάσεων

► 2ο μέρος (Αριθμοθεωρία)

Δομή άρθρου (ομοιότητα με τη δομή του άρθρου του Heilbronn)

► 1ο μέρος

- παρατήρηση ότι $S(n) = \frac{\sum_{m=1}^n (q_1^{(m)} + \dots + q_r^{(m)})}{n}$
- Αναγωγή: αρκεί να μετρήσουμε τις Η-αναπαραστάσεις $\{x, x', y, y'\}$ του n , αφού

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

- μέτρημα των Η-αναπαραστάσεων

- $\sum \left\lfloor \frac{x}{y} \right\rfloor =$

$$\sum_{d|n} \sum_{\substack{(y,n)=d \\ 1 \leq y < \frac{n}{2}}} \left(\# \text{Η-αναπαρ.} \cdot \sum_{\substack{(x',y)=d \\ 1 \leq x' < \frac{n}{2y}}} \left\lfloor \frac{x}{y} \right\rfloor \right) + O(n \log n)$$

► 2ο μέρος (Αριθμοθεωρία)

Δομή άρθρου (ομοιότητα με τη δομή του άρθρου του Heilbronn)

► 1ο μέρος

- παρατήρηση ότι $S(n) = \frac{\sum_{m=1}^n (q_1^{(m)} + \dots + q_r^{(m)})}{n}$
- Αναγωγή: αρκεί να μετρήσουμε τις Η-αναπαραστάσεις $\{x, x', y, y'\}$ του n , αφού

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

- μέτρημα των Η-αναπαραστάσεων

- $\sum \left\lfloor \frac{x}{y} \right\rfloor =$

$$\sum_{d|n} \sum_{\substack{(y,n)=d \\ 1 \leq y < \frac{n}{2}}} \left(\# \text{Η-αναπαρ.} \cdot \sum_{\substack{(x',y)=d \\ 1 \leq x' < \frac{n}{2y}}} \left\lfloor \frac{x}{y} \right\rfloor \right) + O(n \log n)$$

► 2ο μέρος (Αριθμοθεωρία)

- **Ασυμπτωτικοί τύποι**

Δομή άρθρου (ομοιότητα με τη δομή του άρθρου του Heilbronn)

▶ 1ο μέρος

- ▶ παρατήρηση ότι $S(n) = \frac{\sum_{m=1}^n (q_1^{(m)} + \dots + q_r^{(m)})}{n}$
- ▶ Αναγωγή: αρκεί να μετρήσουμε τις Η-αναπαράστασεις $\{x, x', y, y'\}$ του n , αφού

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

- ▶ μέτρημα των Η-αναπαράστασεων
- ▶ $\sum \left\lfloor \frac{x}{y} \right\rfloor = \sum_{d|n} \sum_{\substack{(y,n)=d \\ 1 \leq y < \frac{n}{2}}} \left(\# \text{Η-αναπαρ.} \cdot \sum_{\substack{(x',y)=d \\ 1 \leq x' < \frac{n}{2y}}} \left\lfloor \frac{x}{y} \right\rfloor \right) + O(n \log n)$
- ▶ 2ο μέρος (Αριθμοθεωρία)
 - ▶ Ασυμπτωτικοί τύποι
 - ▶ Σύνθεση ασυμπτωτικών τύπων για υπολογισμό του $\sum \left\lfloor \frac{x}{y} \right\rfloor$

Δομή άρθρου (ομοιότητα με τη δομή του άρθρου του Heilbronn)

► 1ο μέρος

- παρατήρηση ότι $S(n) = \frac{\sum_{m=1}^n (q_1^{(m)} + \dots + q_r^{(m)})}{n}$
- Αναγωγή: αρκεί να μετρήσουμε τις Η-αναπαράστασεις $\{x, x', y, y'\}$ του n , αφού

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

- μέτρημα των Η-αναπαράστασεων
- $\sum \left\lfloor \frac{x}{y} \right\rfloor = \sum_{d|n} \sum_{\substack{(y,n)=d \\ 1 \leq y < \frac{n}{2}}} (\# \text{Η-αναπαρ.} \cdot \sum_{\substack{(x',y)=d \\ 1 \leq x' < \frac{n}{2y}}} \left\lfloor \frac{x}{y} \right\rfloor) + O(n \log n)$

► 2ο μέρος (Αριθμοθεωρία)

- Ασυμπτωτικοί τύποι
- Σύνθεση ασυμπτωτικών τύπων για υπολογισμό του $\sum \left\lfloor \frac{x}{y} \right\rfloor$
- $S(n) = \frac{6}{\pi^2} (\ln n)^2 + O(\log n (\log \log n)^2)$

H- αναπαράσταση

Ορισμός

Για $n \geq 1$, μια τετράδα $\{x, x', y, y'\}$ είναι μια **H-αναπαράσταση του n** αν

$$\begin{aligned}n &= xx' + yy', & (x, y) &= 1 \\x &> y > 0, & x' &\geq y' > 0.\end{aligned}$$

1-1 αντιστοιχία: $\{m, j\} \leftrightarrow$ H-αναπαράσταση

Αν

$$\frac{m}{n} = /0, q_1^{(m)}, q_2^{(m)}, \dots, q_j^{(m)}, q_{j+1}^{(m)}, \dots, q_r^{(m)}, 1/,$$

τότε η H-αναπαράσταση $\{x_j, x'_j, y_j, y'_j\}$ που αντιστοιχεί στο $q_j^{(m)}$ έχει την ιδιότητα

$$\frac{y_j}{x_j} = /0, q_j^{(m)}, \dots, q_1^{(m)} / \quad \frac{y'_j}{x'_j} = /0, q_{j+1}^{(m)}, \dots, q_r^{(m)}, 1/$$

1-1 αντιστοιχία: $\{m, j\} \leftrightarrow$ H-αναπαράσταση

Αν

$$\frac{m}{n} = /0, q_1^{(m)}, q_2^{(m)}, \dots, q_j^{(m)}, q_{j+1}^{(m)}, \dots, q_r^{(m)}, 1/,$$

τότε η H-αναπαράσταση $\{x_j, x'_j, y_j, y'_j\}$ που αντιστοιχεί στο $q_j^{(m)}$ έχει την ιδιότητα

$$\frac{y_j}{x_j} = /0, q_j^{(m)}, \dots, q_1^{(m)} / \quad \frac{y'_j}{x'_j} = /0, q_{j+1}^{(m)}, \dots, q_r^{(m)}, 1/$$

και

$$\lfloor \frac{x_j}{y_j} \rfloor = q_j^{(m)}.$$

Αν $m \in (0, \frac{n}{2})$ τότε η αντιστοιχία είναι 1 – 1.

Λήμμα

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

όπου το άθροισμα είναι για όλες τις Η-αναπαράστασεις του n .

Ιδέα απόδειξης:

Από την 1-1 αντιστοιχία έχουμε:

$$\sum_{1 < m < \frac{n}{2}} (q_1^{(m)} + \dots + q_r^{(m)}) = \sum \left\lfloor \frac{x}{y} \right\rfloor$$

Λήμμα

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

όπου το άθροισμα είναι για όλες τις Η-αναπαράστασεις του n .

Ιδέα απόδειξης:

Από την 1-1 αντιστοιχία έχουμε:

$$\sum_{1 < m < \frac{n}{2}} (q_1^{(m)} + \dots + q_r^{(m)}) = \sum \lfloor \frac{x}{y} \rfloor$$

Συμμετρία: αν $m \in (\frac{n}{2}, n)$ τότε $n - m \in (1, \frac{n}{2})$ και

#βημάτων για input $\{m, n\} = \#βημάτων$ για input $\{n - m, n\}$
γιατί το 1ο βήμα του αλγορίθμου είναι:

$$\begin{aligned} \{m, n\} &\rightarrow \{n - m, m\} \rightarrow \dots \\ \{n - m, n\} &\rightarrow \{n - m, m\} \rightarrow \dots \end{aligned}$$

Το άθροισμα που πρέπει να υπολογίσουμε μετά την αναγωγή είναι:

$$\sum \left\lfloor \frac{x}{y} \right\rfloor = \sum_{d|n} \sum_{\substack{(y,n)=d \\ 1 \leq y < \frac{n}{2}}} \left(d \cdot \prod_{\substack{p|d \\ p \nmid \frac{y}{d}}} \left(1 - \frac{1}{p} \right) \sum_{\substack{(x',y)=d \\ 1 \leq x' < \frac{n}{2y}}} \left\lfloor \frac{x}{y} \right\rfloor \right) + O(n \log n)$$

.....

και μετά από πολλές πράξεις παίρνουμε ότι

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

ΤΕΛΟΣ