Συνεχή κλάσματα & Αφαιρετικός Ευκλείδειος αλγόριθμος

Αγγελίνα Βιδάλη
επιβλέπων καθηγητής: Γιάννης Μοσχοβάκης

$\mu\prod\lambda\forall$

13 Ιουνίου, 2009

Δομή διπλωματικής εργασίας

1ο κεφ. Εισαγωγή στα συνεχή κλάσματα

2ο κεφ. Λίγη Θεωρία Αριθμών

3ο κεφ. Μέση πολυπλοκότητα Αφαιρετικού Ευκλειδείου 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)

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

Πεπερασμένα συνεχή κλάσματα

πεπερασμένο συνεχές κλάσμα στις μεταβλητές $x_1, x_2, \ldots, x_n$:

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

συμβολισμός: $/x_0, x_1, \ldots, x_N/$

Π.χ.

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

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

Q-πολυώνυμα

Ορισμός

Για $n \geq 0$:

$$\begin{aligned} Q_0 &= 1 \\ Q_1(x_1) &= x_1 \\ Q_n(x_1, x_2, \ldots, x_n) &= x_1 Q_{n-1}(x_2, \ldots, x_n) + Q_{n-2}(x_3, \ldots, x_n) \end{aligned}$$

Q-πολυώνυμα

Ορισμός

Για $n \geq 0$:

$$\begin{aligned} Q_0 &= 1 \\ Q_1(x_1) &= x_1 \\ Q_n(x_1, x_2, \dots, x_n) &= x_1 Q_{n-1}(x_2, \dots, x_n) + Q_{n-2}(x_3, \dots, x_n) \end{aligned}$$

Κατ' αυτόν τον τρόπο παίρνουμε:

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

Θεώρημα (L. Euler)

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 $x_j \cdot x_{j+1}$.

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

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

Θεώρημα (L. Euler)

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

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

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

Θεώρημα (L. Euler)

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

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

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

Θεώρημα (L. Euler)

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

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

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

Θεώρημα (L. Euler)

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

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

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

Q-πολυώνυμα και συνεχή κλάσματα

Θεώρημα

Έχουμε

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

ενώ επιπλέον

$$\mu.\kappa.\delta(Q_{n+1}(x_0, x_1, \ldots, x_n), Q_n(x_1, x_2, \ldots, x_n)) = 1.$$

Άπειρα συνεχή κλάσματα

Ορισμός

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

Ορισμός

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

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

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

Θεώρημα

Όλα τα άπειρα απλά συνεχή κλάσματα συγκλίνουν.

Αλγόριθμος ανάπτυξης σε συνεχές κλάσμα

Σε κάθε πραγματικό αριθμό x αντιστοιχούμε δύο ακολουθίες $a_0, a_1, \ldots \in \mathbb{N}$ και $\xi_0, \xi_1, \ldots \in \mathbb{R}$ 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 επιστρέφει τα $a_0, a_1, \ldots, a_n$ και τα $\xi_0, \ldots, \xi_n$.

έτσι

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

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

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 $x = /a_0, \ldots, a_N/$.

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

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

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 $\upsilon \in \mathbb{N}$ τέτοιοι ώστε

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

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 $\upsilon \in \mathbb{N}$ τέτοιοι ώστε

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

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 $\upsilon \in \mathbb{R}$ τέτοιοι ώστε

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

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 $a_1, a_2, a_3, \ldots$ και $v_{-1}, v_0, v_1, v_2, \ldots$ ως εξής:

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

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

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

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

$$
\begin{aligned}
x &= ya_1 + \upsilon_1 & 0 &< \upsilon_1 < y \\
y &= \upsilon_1 a_2 + \upsilon_2 & 0 &< \upsilon_2 < \upsilon_1 \\
\upsilon_1 &= \upsilon_2 a_3 + \upsilon_3 & 0 &< \upsilon_3 < \upsilon_2 \\
&\vdots & &\vdots \\
\upsilon_{n-3} &= \upsilon_{n-2} a_{n-1} + \upsilon_{n-1} & 0 &< \upsilon_{n-1} < \upsilon_{n-2} \\
\upsilon_{n-2} &= \upsilon_{n-1} a_n & \upsilon_n &= 0.
\end{aligned}
$$

Αντιστοιχία Ευκλειδείου με αλγ. ανάπτυξης σε συν. κλάσμα

Θεώρημα

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

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

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

Τα συνεχή κλάσματα ως μορφή αναπαράστασης αριθμών

Μερικά αναπτύγματα γνώριμων αριθμών:

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

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

όπου $\phi = \dfrac{1+\sqrt{5}}{2}$.

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

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

Αφαιρετικός Ευκλείδειος αλγόριθμος

"ανθυφαιρουμένου αεί του ελάσσονος από του μείζονος"

$\{18, 42\}$

1. Αν $u = 1$ ή $v = 1$ τότε $\mu.\varkappa.\delta(u, v) = 1$.
2. Αν $u = v$, τότε $\mu.\varkappa.\delta(u, v) = u$.
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 $\mu.\varkappa.\delta(u, v) = 1$.
2. Αν $u = v$, τότε $\mu.\varkappa.\delta(u, v) = u$.
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 $\mu.\varkappa.\delta(u, v) = 1$.
2. Αν $u = v$, τότε $\mu.\varkappa.\delta(u, v) = u$.
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"

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

1. Αν $u = 1$ ή $v = 1$ τότε $\mu.\varkappa.\delta(u, v) = 1$.
2. Αν $u = v$, τότε $\mu.\varkappa.\delta(u, v) = u$.
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"

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

1. Αν $u = 1$ ή $v = 1$ τότε $\mu.\varkappa.\delta(u, v) = 1$.
2. Αν $u = v$, τότε $\mu.\varkappa.\delta(u, v) = u$.
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):

$$\begin{aligned} 42 &= 18 \cdot \color{red}{2} + 6 \\ 18 &= 6 \cdot \color{red}{3} + 0 \end{aligned}$$

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

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

Υλοποιήση διαίρεσης με διαδοχικές αφαιρέσεις:

Αριθμός αφαιρετικών βημάτων: $\color{red}{2+3}=5$.

Ευκλείδιος αλγόριθμος (με διαίρεση):

$$\begin{aligned} 42 &= 18 \cdot 2 + 6 \\ 18 &= 6 \cdot 3 + 0 \end{aligned}$$

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

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

Υλοποιήση διαίρεσης με διαδοχικές αφαιρέσεις:
Αριθμός αφαιρετικών βημάτων: $2+3=5$.

-Είναι ο Αφαιρετικός Ευκλείδιος.

Αν $1 \leq m \leq n$, τότε

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

Για $1 \leq i < r$,
τα q_i είναι τα πηλίκα των διαιρέσεων του Ευκλειδείου Αλγορίθμου:

$$\begin{aligned} n &= m\, q_1 + r_1, \quad 0 < r_1 < m \\ m &= r_1\, q_2 + r_3, \quad 0 < r_2 < r_1 \\ &\ldots \end{aligned}$$

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

Μέσος αριθμός βημάτων Αφαιρετικού Ευκλειδείου

Ορισμός

$S(n)$: ο μέσος αριθμός βημάτων για να υπολογίσουμε τον $\mu.\varkappa.\delta(m, n)$ 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:

$$S(n) = \frac{\sum_{m=1}^{n} \left(\#\ \text{βημάτων όταν έχω το ζεύγος } \{m, n\}\right)}{n}$$
$$= \frac{\sum_{m=1}^{n} \left(q_1^{(m)} + \ldots + q_{r(m)}^{(m)}\right)}{n}$$

όπου

$$\frac{m}{n} = /0, q_1^{(m)}, q_2^{(m)}, \ldots, q_{r(m)}^{(m)}, 1/.$$

Έστω n σταθερό, θέλουμε να υπολογίσουμε το άθροισμα:

$$S(n) = \frac{\sum_{m=1}^{n} \left(\text{\# βημάτων όταν έχω το ζεύγος } \{m,n\}\right)}{n}$$
$$= \frac{\sum_{m=1}^{n} \left(q_1^{(m)} + \ldots + q_{r(m)}^{(m)}\right)}{n}$$

όπου

$$\frac{m}{n} = /0, q_1^{(m)}, q_2^{(m)}, \ldots, q_{r(m)}^{(m)}, 1/.$$

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 $S(n) = \frac{\sum_{m=1}^{n} \left(q_1^{(m)} + \ldots + q_{r(m)}^{(m)} \right)}{n}$
- 2ο μέρος (Αριθμοθεωρία)

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

- 1ο μέρος
  - παρατήρηση ότι $S(n) = \dfrac{\sum_{m=1}^{n} \left(q_1^{(m)} + \ldots + q_{r(m)}^{(m)}\right)}{n}$
  - Αναγωγή: αρκεί να μετρήσουμε τις H-αναπαραστάσεις $\{x, x', y, y'\}$ του n, αφού

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

- 2ο μέρος (Αριθμοθεωρία)

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

- 1ο μέρος
  - παρατήρηση ότι $S(n) = \dfrac{\sum_{m=1}^{n} \left(q_1^{(m)} + \ldots + q_{r(m)}^{(m)} \right)}{n}$
  - Αναγωγή: αρκεί να μετρήσουμε τις H-αναπαραστάσεις $\{x, x', y, y'\}$ του n, αφού

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

  - μέτρημα των H-αναπαραστάσεων

- 2ο μέρος (Αριθμοθεωρία)

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

- 1ο μέρος
  - παρατήρηση ότι $S(n) = \dfrac{\sum_{m=1}^{n} \left(q_1^{(m)} + \ldots + q_{r(m)}^{(m)} \right)}{n}$
  - Αναγωγή: αρκεί να μετρήσουμε τις H-αναπαραστάσεις $\{x, x', y, y'\}$ του n, αφού

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

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

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

- 1ο μέρος
  - παρατήρηση ότι $S(n) = \dfrac{\sum_{m=1}^{n}\left(q_1^{(m)} + \ldots + q_{r(m)}^{(m)}\right)}{n}$
  - Αναγωγή: αρκεί να μετρήσουμε τις H-αναπαραστάσεις $\{x, x', y, y'\}$ του n, αφού
    $$nS(n) = 2\sum \lfloor \frac{x}{y} \rfloor + 1 - (n \bmod 2)$$
  - μέτρημα των H-αναπαραστάσεων
  - $\sum \lfloor \frac{x}{y} \rfloor =$
    $\sum_{d|n} \sum_{\substack{(y,n)=d \\ 1 \le y < \frac{n}{2}}} \left(\#\text{H-αναπαρ.} \cdot \sum_{\substack{(x',y)=d \\ 1 \le x' < \frac{n}{2y}}} \lfloor \frac{x}{y} \rfloor \right) + O(n \log n)$
- 2ο μέρος (Αριθμοθεωρία)
  - Ασυμπτωτικοί τύποι

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

- 1ο μέρος
  - παρατήρηση ότι $S(n) = \dfrac{\sum_{m=1}^{n} \left(q_1^{(m)} + \ldots + q_{r(m)}^{(m)}\right)}{n}$
  - Αναγωγή: αρκεί να μετρήσουμε τις H-αναπαραστάσεις $\{x, x', y, y'\}$ του n, αφού

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

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

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

- 1ο μέρος
  - παρατήρηση ότι $S(n) = \dfrac{\sum_{m=1}^{n} \left(q_1^{(m)} + \ldots + q_{r(m)}^{(m)}\right)}{n}$
  - Αναγωγή: αρκεί να μετρήσουμε τις H-αναπαραστάσεις $\{x, x', y, y'\}$ του n, αφού

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

  - μέτρημα των H-αναπαραστάσεων
  - $\sum \lfloor \frac{x}{y} \rfloor =$ $\sum_{d|n} \sum_{\substack{(y,n)=d \\ 1 \le y < \frac{n}{2}}} \left(\#\text{H-αναπαρ.} \cdot \sum_{\substack{(x',y)=d \\ 1 \le x' < \frac{n}{2y}}} \lfloor \frac{x}{y} \rfloor\right) + O(n \log n)$
- 2ο μέρος (Αριθμοθεωρία)
  - Ασυμπτωτικοί τύποι
  - Σύνθεση ασυμπτωτικών τύπων για υπολογισμό του $\sum \lfloor \dfrac{x}{y} \rfloor$
  - $S(n) = \dfrac{6}{\pi^2} (\ln n)^2 + O(\log n (\log \log n)^2)$

H- αναπαράσταση

Ορισμός

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

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

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

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

Αν

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

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

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

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

Αν

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

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

$$\frac{y_j}{x_j} = /0, q_j^{(m)}, \ldots, q_1^{(m)}/ \qquad \frac{y_j'}{x_j'} = /0, q_{j+1}^{(m)}, \ldots, q_r^{(m)}, 1/$$

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

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

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

Ιδέα απόδειξης:

Από την 1-1 αντιστοιχία έχουμε:

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

Λήμμα

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

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

Ιδέα απόδειξης:

Από την 1-1 αντιστοιχία έχουμε:

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

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:

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

Το άθροισμα που πρέπει να υπολογίσουμε μετά την αναγωγή είναι:

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

....

και μετά από πολλές πράξεις παίρνουμε ότι

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

ΤΕΛΟΣ