Μαθηματικά Πληροφορικής

4ο Μάθημα

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Αθηνών

Μορφές αποδείξεων

Υπάρχουν πολλά είδη αποδείξεων. Εδώ θα δούμε τα πιο κοινά:

- Εξαντλητική μέθοδος ή μέθοδος επισκόπησης. Όταν το πρόβλημα έχει πεπερασμένο αριθμό περιπτώσεων, τις εξετάζουμε όλες.
- Μαθηματική επαγωγή. Έστω μια πρόταση $P(n)$ που ισχύει για $n = 1$. Αν η $P(n)$ συνεπάγεται την $P(n+1)$, τότε η πρόταση ισχύει για όλους τους φυσικούς.
- Δομική επαγωγή. Επαγωγή όχι στους φυσικούς αριθμούς αλλά σε μια δομή που ορίζεται επαγωγικά.

Μορφές αποδείξεων (συνέχεια)

- Κατασκευαστική απόδειξη ύπαρξης. Δείχνουμε την ύπαρξη ενός στοιχείου δίνοντας ένα αλγόριθμο που το παράγει. Στην ιδία κατηγορία ανήκει και η απόδειξη με αντιπαράδειγμα.
- Μη κατασκευαστική απόδειξη ύπαρξης. Τέτοιες αποδείξεις χρησιμοποιούν
  - την αρχή του περιστερεώνα και τις γενικεύσεις του
  - την πιθανοτική μέθοδο που βασίζεται στο ότι ένα στοιχείο υπάρχει όταν έχει μη μηδενική πιθανότητα ύπαρξης.
  - την διαγωνιοποίηση του Cantor.

Παράδειγμα: Άθροισμα κύβων

- Υπάρχει φυσικός ακέραιος που μπορεί να γραφεί με δύο διαφορετικούς τρόπους σαν άθροισμα δύο κύβων;
- Ισοδύναμα, υπάρχουν δύο διαφορετικά ζεύγη φυσικών αριθμών $\{a_1, b_1\}$ και $\{a_2, b_2\}$ με $a_1^3 + b_1^3 = a_2^3 + b_2^3$;
- Ο 1729 μπορεί να γραφεί σαν $1^3 + 12^3$ και σαν $9^3 + 10^3$.

Κατασκευαστικές ή Όχι;

Γενικά οι αποδείξεις ύπαρξης χωρίζονται σε δύο μεγάλες κατηγορίες:

- Κατασκευαστικές αποδείξεις, στις οποίες η απόδειξη είτε δίνει το στοιχείο που έχει την απαιτούμενη ιδιότητα είτε έναν αλγόριθμο που παράγει ένα τέτοιο στοιχείο.
  - Παράδειγμα: Υπάρχει ακέραιος που γράφεται με δύο τρόπους σαν άθροισμα δύο κύβων. Η απόδειξη $1729 = 1^3 + 12^3 = 9^3 + 10^3$ είναι κατασκευαστική.
- Μη κατασκευαστικές αποδείξεις, στις οποίες δείχνουμε ότι το στοιχείο υπάρχει, αλλά ούτε το στοιχείο δίνεται ούτε αλγόριθμος που να το παράγει.

Παράδειγμα μη Κατασκευαστικής Απόδειξης

ΠΑΡΑΔΕΙΓΜΑ

Να δειχτεί ότι υπάρχουν άρρητοι x και y τέτοιοι ώστε ο x^y είναι ρητός.

Απόδειξη.

- Είτε οι $x_1 = \sqrt{2}$, $y_1 = \sqrt{2}$ έχουν την ιδιότητα είτε οι $x_2 = \sqrt{2}^{\sqrt{2}}$, $y_2 = \sqrt{2}$ την έχουν.
- Γιατί; $x_1^{y_1} = x_2$ και $x_2^{y_2} = 2$. Αν x_2 είναι ρητός τότε το πρώτο ζευγάρι έχει την ιδιότητα, διαφορετικά το δεύτερο ζευγάρι την έχει.
- Η απόδειξη είναι μη κατασκευαστική γιατί δεν μας λέει ποια x και y έχουν την ιδιότητα.

$\square$

Μέγιστος κοινός διαιρέτης

- Ο διαχωρισμός σε κατασκευαστικές ή μη αποδείξεις δεν είναι αυστηρός.
- Θα δούμε ένα παράδειγμα δύο αποδείξεων του ιδίου θεωρήματος, μια κατασκευαστική και μια μη κατασκευαστική.

Θεώρημα

Έστω a και b δύο ακέραιοι με μέγιστο κοινό διαιρέτη δ. Τότε υπάρχουν ακέραιοι x και y τέτοιοι ώστε $ax + by = \delta$.

ΠΑΡΑΔΕΙΓΜΑ

$a = 13 \qquad b = 16 \qquad \gcd(a, b) = 1 \qquad x = 5 \qquad y = -4$

Αλγόριθμος του Ευκλείδη

Ο Αλγόριθμος του Ευκλείδη βρίσκει τον μέγιστο κοινό διαιρέτη δύο αριθμών.

Αλγόριθμος του Ευκλείδη

```
function EUCLID(a, b)                 ▷ Υποθέτουμε ότι a > b
    if b = 0 then
        return a                      ▷ gcd(a, 0) = a
    else
        δ ← EUCLID(b, a mod b)        ▷ gcd(a, b) = gcd(b, a mod b)
        return δ
    end if
end function
```

$$\gcd(a, b) = \begin{cases} a & \text{αν } b = 0 \\ \gcd(b, a \bmod b) & \text{αν } b > 0. \end{cases}$$

Γενικευμένος Αλγόριθμος του Ευκλείδη

Με μικρές αλλαγές ο αλγόριθμος επιστρέφει κατάλληλα x και y.

Γενικευμένος Αλγόριθμος του Ευκλείδη

function Euclid(a, b) ▷ Υποθέτουμε ότι $a > b$
  if $b = 0$ **then**
    return $(a, 1, 0)$ ▷ $a \cdot 1 + b \cdot 0 = a$
  else
    $(\delta, x', y') \leftarrow$ Euclid$(b, a \bmod b)$ ▷ $b \cdot x' + (a \bmod b) \cdot y' = \delta$
    return $(\delta, y', x' - \lfloor \frac{a}{b} \rfloor y')$ ▷ $x = y'$, $y = x' - \lfloor \frac{a}{b} \rfloor y'$
  end if
end function

$$\begin{aligned} \delta &= bx' + (a \bmod b)y' = bx' + (a - b\lfloor \frac{a}{b} \rfloor)y' \\ &= ay' + b(x' - \lfloor a/b \rfloor y'). \end{aligned}$$

Μη κατασκευαστική απόδειξη

Δόθηκε στην τάξη όταν παρουσιάσαμε τον αλγόριθμο του Ευκλείδη. Για την ακρίβεια δείξαμε την παρακάτω ισχυρότερη πρόταση, γνωστή ως Λήμμα του Bézout:

$$\text{Αν } a^2 + b^2 > 0, \quad \gcd(a, b) = \min_{\delta > 0}\{\delta = ax + by \mid x, y \in \mathbb{Z}\}.$$

Πιθανοτική Μέθοδος

Μη κατασκευαστική μέθοδος απόδειξης. Για να αποδείξουμε την ύπαρξη ενός αντικειμένου με μια ιδιότητα P:

1. Ορίζουμε μια κατανομή πιθανότητας στα αντικείμενα που μας ενδιαφέρουν.
2. Διαλέγουμε με βάση την κατανομή ένα αντικείμενο και δείχνουμε ότι έχει την ιδιότητα P με θετική πιθανότητα. Ας είναι μικρή, αρκεί να είναι > 0.

Αν κανένα αντικείμενο δεν είχε την ιδιότητα, τότε η πιθανότητα να διαλέξουμε κάποιο που την έχει θα ήταν μηδέν.

★ Το συμπέρασμα ότι υπάρχει αντικείμενο με την ιδιότητα είναι ντετερμινιστικό, χωρίς περιθώριο λάθους. Οι πιθανότητες παίζουν ρόλο μόνο σαν *εργαλείο* στην απόδειξη.

Πιθανοτική Μέθοδος

Μη κατασκευαστική μέθοδος απόδειξης. Για να αποδείξουμε την ύπαρξη ενός αντικειμένου με μια ιδιότητα P:

1. Ορίζουμε μια κατανομή πιθανότητας στα αντικείμενα που μας ενδιαφέρουν.
2. Διαλέγουμε με βάση την κατανομή ένα αντικείμενο και δείχνουμε ότι έχει την ιδιότητα P με θετική πιθανότητα. Ας είναι μικρή, αρκεί να είναι > 0.

Αν κανένα αντικείμενο δεν είχε την ιδιότητα, τότε η πιθανότητα να διαλέξουμε κάποιο που την έχει θα ήταν μηδέν.

★ **Παράδειγμα:** Γίνεται λαχειοφόρος αγορά με έπαθλο ένα ταξίδι. Αν αποδείξουμε ότι η πιθανότητα να κερδίσει κάποιος το ταξίδι είναι μη μηδενική, έχουμε αποδείξει ότι υπάρχει λαχνός που κερδίζει.

Πιθανοτική Μέθοδος

Πρώτο παράδειγμα εφαρμογής
της Πιθανοτικής Μεθόδου

Διχρωματικά Σύνολα

Δίνεται σύνολο V και E σύνολο n-υποσυνόλων του V, $n \geq 2$. Μπορούμε να χρωματίσουμε τα στοιχεία του V με δύο χρώματα ώστε όλα τα στοιχεία του E να είναι διχρωματικά;

Διαισθητικά, όσο μεγαλώνει το $|E|$, τόσο πιο δύσκολο.

- Ορίζουμε $m(n) :=$ ελάχιστο μέγεθος μιας εισόδου E που να μην είναι 2-χρωματίσιμη.
  - $m(n)$: *ελάχιστος* αριθμός έ. ώ. $\exists$ E με $|E| \geq m(n)$, έτσι ώστε για κάθε χρωματισμό του V, υπάρχει μονοχρωματικό σύνολο στο E.
  - $m(n)$: *μέγιστος* αριθμός έ. ώ. $\forall E$, με $|E| < m(n)$ υπάρχει χρωματισμός του V τ. ώ. κάθε σύνολο στο E να είναι διχρωματικό.

Προφανώς (;) $m(n) \geq 3$. Καλύτερο κάτω φράγμα;

Διχρωματικά Σύνολα

Θεώρημα

Αν $|E| < 2^{n-1}$, υπάρχει πάντα χρωματισμός του V με δύο χρώματα ώστε όλα τα σύνολα στο E να είναι διχρωματικά.

Σε κάθε στοιχείο του V ανάθεσε ένα από τα δύο χρώματα με πιθανότητα $1/2$. Για $e \in E$, όρισε το γεγονός A_e : *«το e μονοχρωματικό»*.

$$P(A_e) = 2/2^n = 2^{1-n}.$$

$$P(\bigcup_{e \in E} A_e) \leq \sum_{e \in E} P(A_e) < (2^{n-1}) 2^{1-n} = 1.$$

Ο τυχαίος χρωματισμός κάνει όλα τα σύνολα διχρωματικά με πιθανότητα

$$1 - P(\bigcup_{e \in E} A_e) > 0.$$

Διχρωματικά Σύνολα

◇ Στο Θεώρημα 2 δείξαμε ότι $m(n) \geq 2^{n-1}$.

◇ Μπορεί να αποδειχθεί (όχι εύκολα) ότι

$$m(n) < (1 + o(1)) \frac{e \ln 2}{4} n^2 2^n.$$

◇ **Άσκηση.** Δείξτε ότι $m(n) \leq \binom{2n-1}{n}$.

Πιθανοτική Μέθοδος

Δεύτερο παράδειγμα εφαρμογής
της Πιθανοτικής Μεθόδου

Πιθανοτική Μέθοδος

Αν $G = (V, E)$, γράφημα και $S \subseteq V$, το γράφημα που ενάγεται από το S ορίζεται ως

$$G[S] = (S, E') \text{ όπου } E' = \{uv \in E \mid u \in S \text{ και } v \in S\}.$$

$R(t)$: ελάχιστο $n \in \mathbb{N}$ έ. ώ. κάθε γράφημα G με n κορυφές περιέχει ως εναγόμενο υπογράφημα μια t-κλίκα ή ένα t-ανεξάρτητο σύνολο.

Γνωρίζουμε ότι $R(t) < 4^t$.

♡ Θα δείξουμε μέσω της πιθανοτικής μεθόδου ότι $R(t) > 2^{t/2}$.

Κάτω φράγμα στο $R(t)$

Θεώρημα (Erdős 1947)

Αν $\binom{n}{t} 2^{1-\binom{t}{2}} < 1$, τότε $R(t) > n$.

$G = (V, E)$, $|V| = n$. Κάθε μία από τις $\binom{n}{2}$ ακμές τοποθετείται ανεξάρτητα με πιθανότητα $1/2$.

$S \subseteq V$, $|S| = t$.
Γεγονός A_s: «$G[S]$ είναι t-κλίκα ή t-ανεξάρτητο σύνολο».

$$P[A_s] = 2^{-\binom{t}{2}} + 2^{-\binom{t}{2}} = 2 \cdot 2^{-\binom{t}{2}}.$$

$$P[\bigcup_S A_s] \leq \sum_S P[A_s] = \binom{n}{t} 2^{1-\binom{t}{2}} < 1 \implies P[\bigcap \overline{A_s}] > 0.$$

Όμως $P[\bigcap \overline{A_s}] > 0 \Leftrightarrow R(t) > n$.

Κάτω φράγμα στο $R(t)$

Για ποιες τιμές του n ισχύει η υπόθεση του θεωρήματος;

$$\binom{n}{t} 2^{1-\binom{t}{2}} = \binom{n}{t} \frac{2^{1+t/2}}{2^{t^2/2}} < \frac{n^t}{t!} \frac{2^{1+t/2}}{2^{t^2/2}}.$$

Για $t \geq 3$ και $n \leq \lfloor 2^{t/2} \rfloor$ παίρνουμε

$$\frac{n^t}{t!} \frac{2^{1+t/2}}{2^{t^2/2}} < 1.$$

Άρα $R(t) > 2^{t/2}$ για $t \geq 3$.

Αρχή του Περιστερεώνα

Πολλές μη κατασκευαστικές αποδείξεις ύπαρξης βασίζονται στο

Θεώρημα (Αρχή του Περιστερεώνα)

Αν τοποθετήσουμε n περιστέρια σε $n-1$ φωλιές, θα υπάρχει μία τουλάχιστον φωλιά με 2 τουλάχιστον περιστέρια.

ΠΑΡΑΔΕΙΓΜΑ

Αν έχουμε $n+1$ φυσικούς αριθμούς που ανήκουν στο διάστημα $1,\ldots,n$, τότε δύο τουλάχιστον από τους αριθμούς είναι ίσοι. Εδώ τα «περιστέρια» είναι οι αριθμοί και οι «φωλιές» οι αριθμοί $1,\ldots,n$.

Μορφές αποδείξεων | Αποδείξεις ύπαρξης | Αρχή του Περιστερεώνα

Αρχή του Περιστερεώνα

Πολλές μη κατασκευαστικές αποδείξεις ύπαρξης βασίζονται στο

Θεώρημα (Αρχή του Περιστερεώνα)

Αν τοποθετήσουμε n περιστέρια σε $n-1$ φωλιές, θα υπάρχει μία φωλιά με 2 τουλάχιστον περιστέρια.

ΠΑΡΑΔΕΙΓΜΑ

Αν έχουμε $n+1$ φυσικούς αριθμούς που ανήκουν στο διάστημα $1,\ldots,n$, τότε δύο τουλάχιστον από τους αριθμούς είναι ίσοι. Εδώ τα «περιστέρια» είναι οι αριθμοί και οι «φωλιές» οι αριθμοί $1,\ldots,n$.

Αρχή του Περιστερεώνα

Μερικές φορές χρησιμοποιούμε την πιο γενική μορφή:

Θεώρημα (Αρχή του Περιστερεώνα)

Αν τοποθετήσουμε n περιστέρια σε m φωλιές, θα υπάρχει μία τουλάχιστον φωλιά με τουλάχιστον $\lceil n/m \rceil$ περιστέρια.

ΠΑΡΑΔΕΙΓΜΑ

Σε κάθε ομάδα 13 ατόμων θα υπάρχουν δύο που γεννήθηκαν τον ίδιο μήνα.

ΠΑΡΑΔΕΙΓΜΑ

Σε κάθε ομάδα 100 ατόμων θα υπάρχουν τουλάχιστον 9 $(= \lceil 100/12 \rceil)$ που γεννήθηκαν τον ίδιο μήνα.

Μορφές αποδείξεων | Αποδείξεις ύπαρξης | Αρχή του Περιστερεώνα

Αρχή του Περιστερεώνα

Μερικές φορές χρησιμοποιούμε την πιο γενική μορφή:

Θεώρημα (Αρχή του Περιστερεώνα)

Αν τοποθετήσουμε n περιστέρια σε m φωλιές, θα υπάρχει μία φωλιά με τουλάχιστον $\lceil n/m \rceil$ περιστέρια.

ΠΑΡΑΔΕΙΓΜΑ

Σε κάθε ομάδα 13 ατόμων θα υπάρχουν δύο που γεννήθηκαν τον ίδιο μήνα.

ΠΑΡΑΔΕΙΓΜΑ

Σε κάθε ομάδα 100 ατόμων θα υπάρχουν τουλάχιστον 9 $(= \lceil 100/12 \rceil)$ που γεννήθηκαν τον ίδιο μήνα.

Εφαρμογές της Αρχής του Περιστερεώνα

Πρόταση

Κάθε φυσικός αριθμός n έχει ένα ακέραιο πολλαπλάσιο που η δεκαδική του παράσταση αποτελείται από μια σειρά από 1 ακολουθούμενη από μια σειρά από 0, είναι δηλαδή της μορφής $11\ldots100\ldots0$.

ΠΑΡΑΔΕΙΓΜΑ

Για $n = 12$ υπάρχει πολλαπλάσιο αυτής της μορφής: $11100 = 12 \cdot 925$.

Απόδειξη.

Ας θεωρήσουμε τους $n+1$ αριθμούς 1, 11, 111, $\ldots$, $11\ldots1$ και τα υπόλοιπα τους $\mod n$.
Τα υπόλοιπα ανήκουν στο $\{0,\ldots,n-1\}$, άρα από την Αρχή του Περιστερεώνα δύο από τους αριθμούς έχουν το ίδιο υπόλοιπο. Η διαφορά τους είναι πολλαπλάσιο του n. $\square$

Μονότονες υποακολουθίες

- Έστω μια ακολουθία αριθμών, π.χ. 6,2,4,3,7,5.
- Κάθε ακολουθία που προκύπτει όταν αγνοήσουμε μηδέν ή περισσότερους όρους της ακολουθίας λέγεται υποακολουθία. Παράδειγμα: 6,4,3,5.
- Μια ακολουθία λέγεται *μονότονη* αν είναι είτε αύξουσα είτε φθίνουσα. Για παράδειγμα, η 6,4,3 είναι μονότονη, η 6,4,7 δεν είναι μονότονη. Η 6,6,6,6 είναι μονότονη.

Θεώρημα

Κάθε ακολουθία πραγματικών αριθμών με n^2+1 στοιχεία περιέχει μια μονότονη υποακολουθία με $n+1$ στοιχεία.

Μονότονες υποακολουθίες

- Έστω $t_1,\ldots,t_{n^2+1}$ μια ακολουθία. Παράδειγμα: 5,3,4,1,2.
- Ορίζουμε ως α_i να είναι το μήκος της μακρύτερης αύξουσας υποακολουθίας με τελευταίο στοιχείο το t_i. Παράδειγμα: $\alpha_2 = 1$, $\alpha_3 = 2$.
- Ορίζουμε ως ϕ_i να είναι το μήκος της μακρύτερης φθίνουσας υποακολουθίας με τελευταίο στοιχείο το t_i. Παράδειγμα: $\phi_2 = 2$, $\phi_4 = 3$.
- Αν $t_i \leq t_j$ για $i < j$, τότε $\alpha_i + 1 \leq \alpha_j$. Παράδειγμα: $3 < 4$, άρα $\alpha_2 + 1 \leq \alpha_3$.
- Αν $t_i \geq t_j$ για $i < j$, τότε $\phi_i + 1 \leq \phi_j$. Παράδειγμα: $3 > 1$, άρα $\phi_2 + 1 \leq \phi_4$.
- Αρα, τα ζεύγη (α_i, ϕ_i) είναι όλα διαφορετικά.
- Αν κάθε α_i και ϕ_i είναι το πολύ n, τότε τα n^2+1 ζεύγη (α_i, ϕ_i) παίρνουν τις n^2 τιμές $(1,1)$, $\ldots$, (n,n).
- Από την Αρχή του Περιστερεώνα δύο από τα ζεύγη είναι ίδια, άτοπο.

Προσέγγιση αρρήτων με ρητούς

- ο αριθμός π μπορεί προσεγγιστεί σαν

$$\frac{3}{1}, \quad \frac{31}{10}, \quad \frac{314}{100}, \quad \frac{3141}{1000}, \ldots$$

- Υπάρχει καλύτερη προσέγγιση με άλλους παρονομαστές (όχι απαραίτητα δυνάμεις του 10);
- Ναι. $22/7 = 3.1428\ldots$ ή ακόμα καλύτερα $355/113 = 3.141592\ldots$
- Έστω θ ένας άρρητος αριθμός και m ένας φυσικός αριθμός· πόσο καλά μπορούμε να προσεγγίσουμε τον θ με κλάσματα των οποίων ο παρονομαστής είναι το πολύ m;

Προσέγγιση του π με ρητούς, $m = 10$

q	closest $\frac{p}{q}$	$\lvert \pi - \frac{p}{q} \rvert$
1	$\frac{3}{1}$	$0.14159\ldots$
2	$\frac{6}{2} = 3$	n/a
3	$\frac{9}{3} = 3$	n/a
4	$\frac{13}{4} = 3.25$	$0.10840\ldots$
5	$\frac{16}{5} = 3.2$	$0.05840\ldots$
6	$\frac{19}{6} = 3.1666\ldots$	$0.02507\ldots$
7	$\frac{22}{7} = 3.1428\ldots$	$0.00126\ldots$
8	$\frac{25}{8} = 3.125$	$0.01659\ldots$
9	$\frac{28}{9} = 3.1111\ldots$	$0.03048\ldots$
10	$\frac{31}{10} = 3.1$	$0.04159\ldots$

Πηγή: https://www.math.uci.edu/~ndonalds/math180b/1contfrac.pdf

Προσέγγιση άρρητου με ρητούς

Θεώρημα (Dirichlet)

Έστω θ άρρητος. Τότε για οποιονδήποτε φυσικό m, υπάρχουν ακέραιοι p και q, με $1 \leq q \leq m$, τέτοιοι ώστε

$$|\theta - \frac{p}{q}| < \frac{1}{mq}.$$

Απόδειξη.

- Ας πάρουμε τα ακέραια πολλαπλάσια $q\theta$, για $q = 0, 1, \ldots, m$ και ας θεωρήσουμε το δεκαδικό μέρος τους $q\theta - \lfloor q\theta \rfloor$.
- Για παράδειγμα τα ακέραια πολλαπλάσια του $\sqrt{2}$ είναι 0, $1.41\ldots$, $2.82\ldots$, $4.24\ldots$ κλπ και το δεκαδικό μέρος τους είναι 0, $0.41\ldots$, $0.82\ldots$, $0.24\ldots$ κλπ.

□

Προσέγγιση άρρητου με ρητούς

Θεώρημα (Dirichlet)

Έστω θ άρρητος. Τότε για οποιονδήποτε φυσικό m, υπάρχουν ακέραιοι p και q, με $1 \leq q \leq m$, τέτοιοι ώστε

$$|\theta - \frac{p}{q}| < \frac{1}{mq}.$$

Απόδειξη.

- Ας πάρουμε τα ακέραια πολλαπλάσια $q\theta$, για $q = 0, 1, \ldots, m$ και ας θεωρήσουμε το δεκαδικό μέρος τους $q\theta - \lfloor q\theta \rfloor$.
- Οι αριθμοί αυτοί είναι της μορφής $q\theta - p$, όπου q και $p = \lfloor q\theta \rfloor$ είναι ακέραιοι.

□

Προσέγγιση αρρήτου με ρητούς

Συνέχεια.

- Για $q = 0, 1, \ldots, m$ υπάρχουν $m + 1$ τέτοιοι αριθμοί και όλοι βρίσκονται στο διάστημα $[0, 1)$.
- Αν θεωρήσουμε τους αριθμούς αυτούς ως περιστέρια και τα διαστήματα $[0, 1/m)$, $[1/m, 2/m)$, $\ldots$, $[(m-1)/m, 1)$ ως φωλιές, μπορούμε να εφαρμόσουμε την Αρχή του Περιστερεώνα.
- Κάποια φωλιά θα περιέχει δύο περιστέρια. Άρα υπάρχουν δύο αριθμοί $q_1\theta - p_1$ και $q_2\theta - p_2$ που διαφέρουν λιγότερο από $1/m$, δηλαδή $|(q_2 - q_1)\theta - (p_2 - p_1)| < 1/m$.
- Ας θέσουμε $q = q_2 - q_1$ και $p = p_2 - p_1$. Έχουμε ότι $1 \leq q \leq m$.

$$|q\theta - p| < 1/m \Rightarrow |\theta - \frac{p}{q}| < \frac{1}{mq}.$$

Σχόλια στο Θ. του Dirichlet

Θεώρημα (Dirichlet)

Έστω θ άρρητος. Τότε για οποιονδήποτε φυσικό m, υπάρχουν ακέραιοι p και q, με $1 \le q \le m$, τέτοιοι ώστε

$$|\theta - \frac{p}{q}| < \frac{1}{mq}.$$

Παρατηρήστε ότι $1 \le q \le m \Rightarrow \left[\frac{1}{mq} \le 1/m \text{ και } \frac{1}{mq} \le 1/q^2\right]$.

Τουλάχιστον δύο τρόποι να ερμηνεύσουμε το θεώρημα:

1. Δοθέντος m, υπάρχει ρητή προσέγγιση του θ με απόκλιση μικρότερη από $1/m$ και παρονομαστή το πολύ m.
2. Υπάρχει ρητή προσέγγιση p/q του θ με απόκλιση μικρότερη από $1/q^2$.

Πόσοι ρητοί με τη δεύτερη ιδιότητα υπάρχουν; Το επόμενο πόρισμα μας λέει: άπειροι.

Πόρισμα του Θ. του Dirichlet

Πόρισμα

Έστω θ άρρητος. Υπάρχουν άπειροι ρητοί p/q, τέτοιοι ώστε

$$|\theta - \frac{p}{q}| < \frac{1}{q^2}. \qquad (1)$$

Απόδειξη.

Έστω ότι μόνο οι ρητοί $\frac{p_1}{q_1}, \ldots, \frac{p_k}{q_k}$ ικανοποιούν την (1).
Αν $\delta = \min_{1\le i\le k} |\theta - \frac{p_i}{q_i}|$, τότε $\delta > 0$. Έστω $M \in \mathbb{Z}_{>0}$ τ. ώ. $1/M < \delta$. Από το Θ. Dirichlet υπάρχει p/r, $1 \le r \le M$, τ. ώ.

$$|\theta - \frac{p}{r}| < \frac{1}{Mr} \begin{cases} <\delta & \text{γιατί } r \ge 1 \\ \le 1/r^2 & \text{γιατί } M \ge r. \end{cases}$$

Άρα $\frac{p}{r} \notin \{\frac{p_1}{q_1}, \ldots, \frac{p_k}{q_k}\}$, άτοπο. □

Πόρισμα του Θ. του Dirichlet

Πόρισμα

Έστω θ ένας άρρητος αριθμός. Υπάρχουν άπειροι ρητοί p/q, τέτοιοι ώστε

$$|\theta - \frac{p}{q}| < \frac{1}{q^2}.$$

Αν αντικαταστήσουμε το $1/q^2$ με $1/q^a$, $a > 2$, αποδεικνύεται (δύσκολα!) ότι ο αριθμός των λύσεων μπορεί να είναι πεπερασμένος.

Θεώρημα του Roth: Για κάθε $a > 2$, αν ο θ είναι άρρητος αλγεβρικός αριθμός υπάρχουν πεπερασμένα ζευγάρια σχετικά πρώτων αριθμών p, q έτσι ώστε

$$|\theta - \frac{p}{q}| < \frac{1}{q^a}.$$

Προσέγγιση αρρήτων με κοινό παρονομαστή

Η προσέγγιση πολλών άρρητων αριθμών με ρητούς που έχουν κοινό παρονομαστή διευκολύνει την πρόσθεση και την αφαίρεση τους. Π.χ., μια κοινή προσέγγιση του $\sqrt{2} = 1.414\ldots$ και του $\sqrt{3} = 1.732\ldots$ είναι $7/5 = 1.4$ και $9/5 = 1.8$, αντίστοιχα.

Θεώρημα

Έστω $\theta_1, \ldots, \theta_n$ άρρητοι αριθμοί. Τότε για οποιοδήποτε θετικό ακέραιο m, υπάρχουν ακέραιοι $p_1, \ldots, p_n$ και q, με $1 \le q \le m^n$, τέτοιοι ώστε

$$|\theta_i - \frac{p_i}{q}| < \frac{1}{mq}$$

για κάθε $i = 1, \ldots, n$.

Μονοχρωματικό ορθογώνιο

Θεώρημα

Αν χρωματίσουμε κάθε σημείο του επιπέδου με ακέραιες συντεταγμένες κόκκινο ή μπλε, θα υπάρχει πάντα ορθογώνιο του οποίου οι κορυφές έχουν το ίδιο χρώμα.

Απόδειξη.

Θεωρούμε τις τομές των ευθειών $y = 0, 1, 2$ με τις ευθείες $x = i$, $i = 1, 2, \ldots, 9$. Σε κάθε ευθεία $x = i$ υπάρχουν 3 χρωματισμένα σημεία. Οι διαφορετικοί χρωματισμοί τους είναι $2^3 = 8$, άρα από την ΑτΠ δύο από τις 9 κάθετες ευθείες $x = j$ και $x = k$, $j \neq k$, έχουν τον ίδιο χρωματισμό (δηλ. το χρώμα του (j, y) είναι ίδιο με του (k, y) για $y = 0, 1, 2$.)

Πάλι από την ΑτΠ, δύο από τα σημεία $(j, 0), (j, 1), (j, 2)$ πρέπει να έχουν το ίδιο χρώμα, έστω τα $(j, y_1), (j, y_2)$. Το ορθογώνιο με κορυφές $(j, y_1), (j, y_2), (k, y_1), (k, y_2)$ είναι μονοχρωματικό. □

Άλλα μη κατασκευαστικά θεωρήματα ύπαρξης

- Θεώρημα Robertson-Seymour για ύπαρξη αλγορίθμου ο οποίος αποφασίζει αν ένα γράφημα G ανήκει σε μια κλειστή ως προς ελάσσονα οικογένεια γραφημάτων.
- Θεώρημα Brouwer. Fixed point theorem.
- Θεώρημα Nash στη Θεωρία Παιγνίων.

Θεωρήματα Brouwer

Ορισμός

Δίνεται συνάρτηση $f : K \to K$. Το $x_0 \in K$ καλείται σταθερό σημείο (fixed point) της f αν $f(x_0) = x_0$.

Θεώρημα

Κάθε συνεχής συνάρτηση $f : [a, b] \to [a, b]$ έχει σταθερό σημείο.

Γενικότερα:

Θεώρημα

Κάθε συνεχής συνάρτηση $f : K \to K$ όπου το K κλειστό, φραγμένο και κυρτό έχει σταθερό σημείο.

Παράδειγμα: το K κλειστός δίσκος στον Ευκλείδειο χώρο.