

Μαθηματικά Πληροφορικής

4ο Μάθημα

Ηλίας Κουτσοπιάς

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Αθηνών
elias@di.uoa.gr

Νοέμβριος 2011

Γενικό πλάνο

Μορφές αποδείξεων

Αποδείξεις ύπαρξης

Αρχή του Περιστερώνα

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.
- ▶ **Αναδρομική επαγωγή.** Επαγωγή όχι στους φυσικούς αριθμούς αλλά σε μια δομή που ορίζεται αναδρομικά.

Μορφές αποδείξεων (συνέχεια)

- ▶ **Κατασκευαστική απόδειξη ύπαρξης.** Δείχνουμε την ύπαρξη ενός στοιχείου δίνοντας ένα αλγόριθμο που το παράγει. Στην ίδια κατηγορία ανήκει και η απόδειξη με αντιπαράδειγμα.
- ▶ **Μη κατασκευαστική απόδειξη ύπαρξης.** Τέτοιες αποδείξεις χρησιμοποιούν
 - ▶ την αρχή του περιστερώνα και τις γενικεύσεις του
 - ▶ κατάλληλη καταμέτρηση
 - ▶ 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 δυο κύβων;
- ▶ Ισοδύναμα, υπάρχουν δυο 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 δυο μεγάλες κατηγορίες:

- ▶ **Κατασκευαστικές αποδείξεις**, στις οποίες η απόδειξη είτε δίνει το στοιχείο που έχει την απαιτούμενη ιδιότητα είτε δίνει ένα αλγόριθμο που παράγει ένα τέτοιο στοιχείο.
 - ▶ Παράδειγμα: Υπάρχει ακέραιος που γράφεται με δυο τρόπους σαν άθροισμα δυο 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

Ναδειχτεί 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.

□

Μέγιστος κοινός διαιρέτης

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

Θεώρημα

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

ΠΑΡΑΔΕΙΓΜΑ

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

Αλγόριθμος του Ευκλείδη

Ο Αλγόριθμος του Ευκλείδη βρίσκει το μέγιστο κοινό διαιρέτη δυο αριθμών.

Αλγόριθμος του Ευκλείδη

```
1: function EUCLID( $a, b$ )           ▷ Υποθέτουμε ότι  $a > b$ 
2:   if  $b = 0$  then
3:     return  $a$                        ▷  $\gcd(a, 0) = a$ 
4:   else
5:      $\delta \leftarrow \text{EUCLID}(b, a \bmod b)$    ▷
      $\gcd(a, b) = \gcd(b, a \bmod a)$ 
6:     return  $\delta$ 
7:   end if
8: 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

```
1: function EUCLID( $a, b$ )           ▷ Υποθέτουμε ότι  $a > b$ 
2:   if  $b = 0$  then
3:     return ( $a, 1, 0$ )             ▷  $a \cdot 1 + b \cdot 0 = a$ 
4:   else
5:      $(\delta, x', y') \leftarrow \text{EUCLID}(b, a \bmod b)$    ▷
      $b \cdot x' + (a \bmod b) \cdot y' = \delta$ 
6:     return ( $\delta, y', x' - \lfloor \frac{a}{b} \rfloor y'$ )   ▷  $x = y', y = x' - \lfloor \frac{a}{b} \rfloor y'$ 
7:   end if
8: end function
```

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

Μη κατασκευαστική απόδειξη

- ▶ Θα δώσουμε τώρα μια μη κατασκευαστική απόδειξη μόνο για την περίπτωση $\delta = 1$. Από αυτή προκύπτει η γενική περίπτωση. Ουσιαστικά θα δείξουμε ότι υπάρχει y τέτοιο ώστε $by = 1 \pmod{a}$.
- ▶ Θεωρούμε τους αριθμούς $by - 1 \pmod{a}$ για $y = 1, \dots, a$.
- ▶ Όλοι αυτοί οι a αριθμοί είναι διαφορετικοί μεταξύ τους.
- ▶ Ανήκουν στο $\{0, \dots, a - 1\}$. Άρα κάποιος από αυτούς είναι ίσος με 0.
- ▶ Η απόδειξη είναι μη κατασκευαστική γιατί δεν μας δίνει τροπο να βρούμε το y , εκτός από το να δοκιμάσουμε όλες τις τιμές $1, \dots, a$.

Αρχή του Περιστερώνα

Πολλές μη κατασκευαστικές αποδείξεις ύπαρξης βασίζονται στο

Θεώρημα (Αρχή του Περιστερώνα)

Με οποιονδήποτε τρόπο να τοποθετήσουμε n περιστέρια σε $n - 1$ φωλιές, θα υπάρχει πάντα μια τουλάχιστον φωλιά με 2 τουλάχιστον περιστέρια.

ΠΑΡΑΔΕΙΓΜΑ

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

Αρχή του Περιστερώνα

Μερικές φορές χρησιμοποιούμε την πιο γενική μορφή:

Θεώρημα (Αρχή του Περιστερώνα)

Με οποιονδήποτε τρόπο να τοποθετήσουμε n περιστέρια σε m φωλιές, θα υπάρχει πάντα μια τουλάχιστον φωλιά με $\lceil n/m \rceil$ τουλάχιστον περιστέρια.

ΠΑΡΑΔΕΙΓΜΑ

Σε κάθε ομάδα 13 ατόμων θα υπάρχουν δυο 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 Περιστερώνα

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 $11\dots 100\dots 0$.

ΠΑΡΑΔΕΙΓΜΑ

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

Απόδειξη.

Ας θεωρήσουμε τους $n + 1$ αριθμούς $1, 11, 111, \dots, 11\dots 1$ και τα υπόλοιπα τους $\pmod n$.

Τα υπόλοιπα ανήκουν στο $\{0, \dots, n - 1\}$, άρα από την Αρχή του Περιστερώνα δυο 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 περισσότερα 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.

Θεώρημα

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

Μονότονες υποακολουθίες

- ▶ Έστω t_1, \dots, 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 $\phi_2 + 1 \leq \phi_4$.
- ▶ Άρα, τα ζεύγη (α_i, ϕ_i) είναι όλα διαφορετικά.
- ▶ Αν κάθε α_i και ϕ_i είναι το πολύ n , τότε υπάρχουν $n^2 + 1$ ζεύγη (α_i, ϕ_i) που παίρνουν τις n^2 τιμές $(1, 1), \dots, (n, n)$.
- ▶ Από την Αρχή του Περιστερώνα δυο από τα ζεύγη είναι ίδια, άτοπο.

Προσέγγιση αρρήτων με ρητούς

- ▶ ο αριθμός π μπορεί προσεγγιστεί σαν

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

- ▶ Υπάρχει καλύτερη προσέγγιση με άλλους παρονομαστές (όχι απαραίτητα δυνάμεις του 10);
- ▶ Ναι. $22/7 = 3.1428\dots$ ή ακόμα καλύτερα $355/113 = 3.141592\dots$
- ▶ 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 αρρήτου με ρητούς

Θεώρημα (Dirichlet)

Έστω θ ένας πραγματικός αριθμός. Τότε για οποιοδήποτε 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 $q = 0, 1, \dots, m$ και ας θεωρήσουμε το δεκαδικό μέρος τους $q\theta - \lfloor q\theta \rfloor$.
- ▶ Για παράδειγμα τα ακέραια πολλαπλάσια του $\sqrt{2}$ είναι $0, 1.41\dots, 2.82\dots, 4.24\dots$ κλπ και το δεκαδικό μέρος τους είναι $0, 0.41\dots, 0.82\dots, 0.24\dots$ κλπ.
- ▶ 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 $q = 0, 1, \dots, m$ υπάρχουν $m + 1$ τέτοιοι αριθμοί και όλοι βρίσκονται στο διάστημα $[0, 1)$.
- ▶ Αν θεωρήσουμε τους αριθμούς αυτούς ως περιστέρια και τα διαστήματα $[0, 1/m), [1/m, 2/m), \dots, [(m-1)/m, 1)$ ως φωλιές, μπορούμε να εφαρμόσουμε την Αρχή του Περιστερώνα.
- ▶ Κάποια φωλιά θα περιέχει δυο περιστέρια. Άρα υπάρχουν δυο 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 $p = p_2 - p_1$. Οι p και q είναι ακέραιοι στο διάστημα $1 \leq q \leq m$.

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

Κατασκευαστική προσέγγιση αρρήτου με ρητούς

Συνεχή κλάσματα

ΠΑΡΑΔΕΙΓΜΑ

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \dots}}} \quad \pi = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \dots}}}$$

Πρόταση

Τα συνεχή κλάσματα δίνουν την καλύτερη προσέγγιση αρρήτου από ρητούς όταν μας ενδιαφέρει να έχουμε μικρό αριθμητή και παρονομαστή.

Κατασκευαστική προσέγγιση αρρήτου με ρητούς

ΠΑΡΑΔΕΙΓΜΑ

$$\begin{aligned}\sqrt{2} &\approx 1 \\ &\approx 1 + \frac{1}{2} = \frac{3}{2} = 1.5 \\ &\approx 1 + \frac{1}{2 + \frac{1}{2}} = \frac{7}{5} = 1.4 \\ &\approx 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}} = \frac{17}{12} = 1.41667\end{aligned}$$

Προσέγγιση αρρήτων με κοινό παρονομαστή

Θέλουμε την κοινή προσέγγιση πολλών άρρητων αριθμών με ρητούς που να έχουν κοινό παρονομαστή ώστε να είναι εύκολη η πρόσθεση και η αφαίρεση τους. Για παράδειγμα, μια κοινή προσέγγιση του $\sqrt{2} = 1.414\dots$ και του $\sqrt{3} = 1.732\dots$ είναι $7/5 = 1.4$ και $9/5 = 1.8$, αντίστοιχα.

Θεώρημα

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

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

για κάθε $i = 1, \dots, n$.

Ο μόνος αλγόριθμος που έχουμε για να βρίσκει τέτοιους p_i και q , είναι να δοκιμάσουμε όλες τις m^n δυνατές τιμές του q .

Άλλα μη κατασκευαστικά θεωρήματα ύπαρξης

- ▶ Θεώρημα Brouwer. Fixed point theorem.
- ▶ Θεώρημα Nash στη Θεωρία Παιγνίων.
- ▶ Θεώρημα Arrow-Debreu στα Οικονομικά Μαθηματικά.