Μαθηματικά Πληροφορικής

1ο Μάθημα

Ηλίας Κουτσουπιάς

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

2 Νοεμβρίου 2011

Γενικό πλάνο

Σχετικά με το μάθημα

- Το μάθημα πραγματεύεται θέματα μαθηματικών που είναι χρήσιμα στην πληροφορική και τις τηλεπικοινωνίες
- Μέσα από εφαρμογές θα προσπαθήσουμε να μάθουμε τεχνικές που είναι χρήσιμες στην ανάλυση και σχεδίαση πληροφορικών συστημάτων.

Σχετικά με το μάθημα

- Σελίδα του μαθήματος: `http://theory.di.uoa.gr/classes/Math4CS-11f`
- Απαιτήσεις:
  - Ασκήσεις (30%)
  - Τελικό διαγώνισμα (80%)
  - Απαιτείται τουλάχιστον 4 και στις ασκήσεις και στο τελικό διαγώνισμα.
- Αντιγραφή, ακόμα και στις ασκήσεις, συνεπάγεται μηδενισμό στην τάξη για το τρέχον ακαδημαϊκό έτος - για όλες τις εξεταστικές περιόδους.
- Τις ασκήσεις πρέπει να προσπαθείτε να τις κάνετε μόνοι σας. Επιτρέπεται και ενθαρρύνεται να τις συζητήσετε με άλλους, όχι όμως να αντιγράψετε τις λύσεις. Τις λύσεις πρέπει να τις βρείτε και να τις γράψετε μόνοι σας.

Σχετικά με το μάθημα

Τα δωρεάν συγγράμματα είναι

- Kenneth H. Rosen. Διακριτά μαθηματικά και εφαρμογές τους. Εκδόσεις Τζιόλα, 2008
- Βουτσαδάκης Γιώργος, Κυρούσης Λευτέρης, Μπούρας Χρήστος, Σπυράκης Παύλος. Διακριτά μαθηματικά και εφαρμογές τους. Εκδόσεις Gutenberg, 2008

Υπάρχουν επίσης πολύ καλά εγχειρίδια στην Αγγλική γλώσσα που καλύπτουν μεγάλο μέρος της ύλης του μαθήματος, όπως τα:

- Kenneth H. Rosen. Discrete Mathematics and its Applications.
- Lazlo Lovasz, Jozsef Pelikan, Katalin Vesztergombi. Discrete Mathematics.
- Eric Lehman and Tom Leighton. Mathematics for Computer Science. Μπορείτε να το βρείτε online.

Υποθέσεις - Θεωρήματα

- Στα μαθηματικά και στις άλλες επιστήμες κάνουμε συχνά υποθέσεις. Όταν δείξουμε ότι μια υπόθεση είναι αληθής, τότε την ονομάζουμε θεώρημα ή πρόταση.
- Τα μαθηματικά που διδασκόμαστε στο σχολείο και στο Πανεπιστήμιο, αποτελούνται συνήθως από ορισμούς, θεωρήματα και αποδείξεις που μας 'σερβίρονται' έτοιμες.
- Η πιο ενδιαφέρουσα πλευρά των μαθηματικών είναι όταν εξερευνούμε τα σύνορα της γνώσης. Εκεί πρέπει να κάνουμε υποθέσεις και μετά να τις αποδείξουμε ή να τις καταρρίψουμε.
- Υπόθεση $\longleftrightarrow$ Απόδειξη $\longleftrightarrow$ Θεώρημα

Υποθέσεις - Εικασίες

- Πολλές φορές, όταν δεν μπορούμε να αποδείξουμε μια υπόθεση, την αναθεωρούμε.
- Άλλες φορές, όταν καταφέρνουμε να αποδείξουμε μια υπόθεση, η ίδια η απόδειξη μας βοηθάει να γενικεύσουμε την πρόταση.

Η μαγεία της χρυσής τομής

Ας παίξουμε λίγο με τη χρυσή τομή, τον αριθμό $\phi = \frac{1+\sqrt{5}}{2} = 1.618\ldots$, για τον όποιο ισχύει $\phi^2 = \phi + 1$. Ας πολλαπλασιάσουμε το ϕ και το ϕ^2 τους φυσικούς αριθμους.

$1 \cdot \phi = 1.618\ldots$	$1 \cdot \phi^2 = 2.618$
$2 \cdot \phi = 3.236\ldots$	$2 \cdot \phi^2 = 5.236$
$3 \cdot \phi = 4.854\ldots$	$3 \cdot \phi^2 = 7.854$
$4 \cdot \phi = 6.472\ldots$	$4 \cdot \phi^2 = 10.472$
$5 \cdot \phi = 8.090\ldots$	$5 \cdot \phi^2 = 13.090$
$6 \cdot \phi = 9.708\ldots$	$6 \cdot \phi^2 = 15.708$

Η μαγεία της χρυσής τομής

- Παρατηρείστε πως στα ακέραια μέρη των γινομένων φαίνεται ότι εμφανίζονται όλοι οι φυσικοί αριθμοί $1, 2, 3, \ldots$.
- Είναι όμως αλήθεια; Για να απαντήσουμε πρέπει πρώτα να διατυπώσουμε με σαφήνεια την υπόθεση και μετά να προσπαθήσουμε να την αποδείξουμε ή καταρρίψουμε.
- *Υπόθεση: Για κάθε φυσικό αριθμό n, υπάρχει ακριβώς ένας φυσικός αριθμός k τέτοιος ώστε $n = \lfloor k\phi \rfloor$ ή $n = \lfloor k\phi^2 \rfloor$.*

Η μαγεία της χρυσής τομής

- Ας δοκιμάσουμε να καταρρίψουμε την υπόθεση. Έχουμε ευτυχώς το κατάλληλο εργαλείο, τον υπολογιστή. Ας πάρουμε ένα μεγάλο 'τυχαίο' n, π.χ. $n = 1000$, και ας δοκιμάσουμε τα k που είναι κοντά στα n/ϕ και n/ϕ^2. Βρίσκουμε ότι η υπόθεση ισχύει για αυτό το n.
- Αφού έχουμε πειστεί αρκετά για την αλήθεια της υπόθεσης ας προσπαθήσουμε να την αποδείξουμε.

Απόδειξη

- Ορίζουμε τα σύνολα $A = \{\lfloor k\phi \rfloor : k = 1, 2, \ldots\}$ και $B = \{\lfloor k\phi^2 \rfloor : k = 1, 2, \ldots\}$.
- Για κάθε φυσικό n ορίζουμε το υποσύνολο A_n και B_n να είναι τα στοιχεία των A και B που δεν ξεπερνούν το n.
- Πόσα στοιχεία έχει το A_n; Όσα είναι οι φυσικοί k για τα όποιους ισχύει

$$\lfloor k\phi \rfloor \leq n \Leftrightarrow k\phi < n+1 \Leftrightarrow k < \frac{n+1}{\phi} \Leftrightarrow k \leq \left\lfloor \frac{n+1}{\phi} \right\rfloor.$$

Δηλαδή, ο αριθμός των στοιχείων του σύνολου A_n είναι $|A_n| = \left\lfloor \frac{n+1}{\phi} \right\rfloor$. Με τον ίδιο τρόπο βρίσκουμε $|B_n| = \left\lfloor \frac{n+1}{\phi^2} \right\rfloor$.

Απόδειξη

- Ο αριθμός λοιπόν των στοιχείων και του A_n και του B_n είναι

$$\left\lfloor \frac{n+1}{\phi} \right\rfloor + \left\lfloor \frac{n+1}{\phi^2} \right\rfloor.$$

- Με λίγη σκέψη καταλήγουμε ότι η αρχική υπόθεση ισχύει αν και μόνο αν αυτός ο αριθμός είναι ίσος με n, δηλαδή:

$$\left\lfloor \frac{n+1}{\phi} \right\rfloor + \left\lfloor \frac{n+1}{\phi^2} \right\rfloor = n.$$

Απόδειξη

- Παρατηρούμε ότι το ϕ έχει την ιδιότητα
$$\frac{n+1}{\phi} + \frac{n+1}{\phi^2} = n+1.$$
- Οι δυο αριθμοί $\frac{n+1}{\phi}$ και $\frac{n+1}{\phi^2}$ έχουν άθροισμα $n+1$ και δεν είναι ακέραιοι. Άρα τα ακέραια μέρη τους έχουν άθροισμα n.

Γενίκευση

- Ποια ιδιότητα του ϕ και του ϕ^2 χρησιμοποιήσαμε στην παραπάνω απόδειξη;
- Μόνο ότι
$$\frac{1}{\phi} + \frac{1}{\phi^2} = 1$$
και ότι είναι άρρητοι.
- Η ίδια λοιπόν απόδειξη μπορεί να χρησιμοποιηθεί για να δείξουμε το πιο γενικό θεώρημα:

- **Θεώρημα**

  Έστω δυο οποιοιδήποτε άρρητοι λ και μ που ικανοποιούν $\frac{1}{\lambda} + \frac{1}{\mu} = 1$. Για κάθε φυσικό αριθμό n, υπάρχει ακριβώς ένας φυσικός αριθμός k τέτοιος ώστε $n = \lfloor k\lambda \rfloor$ ή $n = \lfloor k\mu \rfloor$.

Υπόθεση - Κατάρριψη

- Ας παρατηρήσουμε τους αριθμους της μορφής $n^2 - n + 41$ για $n = 1, 2, \ldots$:
$$41, 43, 47, 53, 61, \ldots.$$
- Όλοι αυτοί οι αριθμοί είναι πρώτοι.
- *Υπόθεση: Για κάθε φυσικό αριθμό n, ο αριθμός $n^2 - n + 41$ είναι πρώτος.*
- Δοκιμάζοντας πολλές τιμές για το n διαπιστώνουμε ότι η υπόθεση δεν ισχύει. Ισχύει για $n = 1, 2, \ldots, 40$, άλλα για $n = 41$ βλέπουμε ότι το $41^2 - 41 + 41$ διαιρείται προφανώς από το 41.

Εικασίες

- Μια υπόθεση που δεν μπορούμε να την καταρρίψουμε ή να την αποδείξουμε την αποκαλούμε εικασία.
- Οι εικασίες είναι η κινητήρια δύναμη των μαθηματικών. Προσπαθώντας να αποδείξουμε εικασίες αναγκαζόμαστε να αναλυψουμε νέες θεωρίες και τεχνικές.

Το Θεώρημα του Φερμά

- Το Θεώρημα του Fermat είναι ίσως η πιο γνώστη εικασία: Η εξίσωση $x^n + y^n = z^n$ δεν έχει λύση για μη μηδενικούς ακέραιους x, y, και z και για ακέραιο $n > 2$.
- Προτάθηκε από τον Pierre Fermat τον 17ο αιώνα και αποδείχτηκε από τον Andrew Wiles το 1995.

Η εικασία του Goldbach

- Το 1742 ο Christian Goldbach διατύπωσε την εξής υπόθεση: Κάθε άρτιος αριθμός μεγαλύτερος του 2 μπορεί να γραφτεί σαν άθροισμα 2 πρώτων αριθμών. Π.χ. $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$.
- Η εικασία δεν έχει αποδειχτεί ούτε καταρριφθεί.
- 'Εχει επιβεβαιωθεί με τη βοήθεια υπολογιστή για όλα τους αριθμους μέχρι 10^{14}.
- Προτείνω θερμά το όμορφο μυθιστόρημα του Απόστολου Δοξιάδη 'Ο θείος Πέτρος και η εικασία του Γκόλντμπαχ'.

Το Θεώρημα των 4 χρωμάτων

- Κάθε χάρτης μπορεί να χρωματιστεί με τέσσερα χρώματα έτσι ώστε γειτονικές χώρες να έχουν διαφορετικά χρώματα.
- Η υπόθεση αυτή προτάθηκε πριν από 130 χρόνια
- Αποδείχτηκε τελικά το 1976 από τους Kenneth Appel και Wolfgang Haken. Η απόδειξη βασίζεται στον έλεγχο 1936 περιπτώσεων και η κάθε περίπτωση απαιτεί τον έλεγχο πολλών λογικών συνδυασμών. Μόνο με τη βοήθεια υπολογιστή μπορούν να ελεγχθούν όλες οι περιπτώσεις.
- Παραμένει ανοικτό αν υπάρχει σύντομη απόδειξη, που δεν απαιτεί τεράστια υπολογιστική ικανότητα.

Η εικασία του $3x + 1$

- Πάρε ένα φυσικό αριθμό x. Αν είναι άρτιος διαίρεσε τον με το 2, αλλιώς υπολόγισε το $3x + 1$. Επανέλαβε με το αποτέλεσμα μέχρι να προκύψει το 1.
- $7 \to 22 \to 11 \to 34 \to 17 \to 52 \to 26 \to 13 \to 40 \to 20 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$
- Εικασία: Αν ξεκινήσουμε από οποιοδήποτε φυσικό αριθμό x θα φτάσουμε πάντα στο 1.
- Προτάθηκε από διάφορους, γι αυτό και λέγεται επίσης το πρόβλημα του Collatz, το πρόβλημα του Ulam, ο αλγόριθμος του Hasse, κλπ.
- Παραμένει ανοικτό.

Η εικασία του Riemann

- Η συνάρτηση ζ του Riemann ορίζεται ως εξής:

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \dots$$

- Για $x > 1$ το άθροισμα συγκλίνει. Η συνάρτηση μπορεί να επεκταθεί και στους μιγαδικούς αριθμούς.
- Η εικασία του Riemann λέει ότι οι μόνες μη τετριμμένες ρίζες της ζ συνάρτησης, δηλαδή οι τιμές του x που ικανοποιούν $\zeta(x) = 0$, είναι μιγαδικοί αριθμοί με πραγματικό μέρος ίσο με $1/2$.
- Η εικασία προτάθηκε από τον Riemann πριν από 150 χρόνια περίπου και δεν έχει ακόμα αποδειχτεί ούτε καταρριφθεί.

Η εικασία του Riemann

- Η εικασία του Riemann σχετίζεται άμεσα με την πυκνότητα των πρώτων αριθμών.
- Πόσοι πρώτοι αριθμοί είναι μικρότεροι από 1000; Από n; Ας ορίσουμε αυτόν τον αριθμό ως $\pi(n)$. Πόσο μεγάλο είναι το $\pi(n)$;
- Έχει αποδειχτεί ότι το $\pi(n)$ είναι περίπου $n/\ln n$.
- Πόσο κοντά στο $n/\ln n$ είναι; Η εικασία του Riemann είναι ισοδύναμη με την πρόταση ότι το $\pi(n)$ και το $n/\ln n$ διαφέρουν κατά το πολύ $\sqrt{n}\ln n$.

P=NP

- Η πιο σημαντική εικασία στην πληροφορική και μια από τις σημαντικότερες εικασίες γενικότερα είναι η εικασία P≠NP.
- Η εικασία λέει ότι υπάρχουν προβλήματα που λύνονται από μη ντετερμινιστικές μηχανές Turing σε πολυωνυμικό χρόνο αλλά απαιτούν περισσότερο από πολυωνυμικό χρόνο σε ντετερμινιστικές μηχανές.
- Με πιο απλά λόγια, η εικασία λέει ότι υπάρχουν προβλήματα για τα οποία είναι αρκετά πιο δύσκολο να βρούμε τη λύση τους από το να επιβεβαιώσουμε την ορθότητά της.

SATISFIABILITY

- Το πρόβλημα της ικανοποιησιμότητας απλών λογικών προτάσεων είναι γνωστό σαν SATISFIABILITY. Σ' αυτό το αλγοριθμικό πρόβλημα, δίνεται μια λογική πρόταση, για παράδειγμα,

$$(x_1 \vee x_2 \vee x_3) \wedge (\overline{x}_1 \vee x_2 \vee \overline{x}_3) \wedge (x_1 \vee \overline{x}_2 \vee \overline{x}_3) \wedge (\overline{x}_1 \vee x_2 \vee x_3) \wedge (\overline{x}_1 \vee \overline{x}_2 \vee x_3),$$

  και θέλουμε να βρούμε αν υπάρχουν τιμές των μεταβλητών που κάνουν την πρόταση αληθή.
- Προφανώς, αν κάποιος μας υποδείξει κατάλληλες τιμές μπορούμε εύκολα να επιβεβαιώσουμε αν οι τιμές αυτές έχουν την επιθυμητή ιδιότητα. Αλλά χωρίς κάποια τέτοια υπόδειξη, πόσο δύσκολο είναι να ελέγξουμε αν υπάρχουν τέτοιες τιμές;
- Η εικασία P=NP λέει ότι χωρίς υπόδειξη, το πρόβλημα είναι δύσκολο, και πιο συγκεκριμένα, ότι δεν μπορεί να λυθεί πάντα σε χρόνο πολυωνυμικό ως προς το μήκος της πρότασης.

Εφαρμογές;

- Αν και τέτοια θέματα φαίνονται να μην έχουν εφαρμογές, πολλές φορές η ανάπτυξη της τεχνολογίας μεταφέρει τέτοια 'θεωρητικά' θέματα στο πεδίο των εφαρμογών.
- Για παράδειγμα, η εικασία του Riemann έχει άμεση σχέση με την κρυπτογραφία.