Μαθηματικά Πληροφορικής

1ο Μάθημα

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Αθηνών

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 δίνονται 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 χρυσή τομή

Η χρυσή τομή είναι ο αριθμός $\phi = \frac{1+\sqrt{5}}{2} = 1.618\ldots$. Ισχύει $\phi^2 = \phi + 1$. Ας πολλαπλασιάσουμε το ϕ και το ϕ^2 με τους φυσικούς αριθμους.

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

Η χρυσή τομή

- 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 χρυσή τομή

- Ας δοκιμάσουμε να καταρρίψουμε την υπόθεση με 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.
- Αν 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 τα υποσύνολα A_n και B_n να είναι τα στοιχεία των A και B που δεν ξεπερνούν το n.
- Πόσα στοιχεία έχει το A_n; Όσοι είναι οι φυσικοί k για τους οποίους 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

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

- Ισχύει ότι $A_n \cap B_n = \varnothing$. (Γιατί;) Άρα η αρχική υπόθεση ισχύει αν και μόνο αν $|A_n| + |B_n| = n$, 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 δύο οποιοιδήποτε θετικοί 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 $n = \lfloor k\mu \rfloor$.

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 δύο οποιοιδήποτε θετικοί 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 $n = \lfloor k\mu \rfloor$.

Γενίκευση

Η προηγούμενη διατύπωση περιείχε μία περιττή λέξη:

Θεώρημα

Έστω δυο θετικοί 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 αριθμούς της μορφής $n^2 + n + 41$ για $n = 0, 1, 2, \ldots$:

$$41, 43, 47, 53, 61, \ldots.$$

- 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 $n = 0, 1, 2, \ldots, 39$, άλλα για $n = 40$ βλέπουμε ότι το $40^2 + 40 + 41 = 40 \cdot (40 + 1) + 41$ διαιρείται από το 41.

Υπόθεση - Κατάρριψη

Για την κατάρριψη μιας υπόθεσης, αρκεί ένα αντιπαράδειγμα.

Υπόθεση: Για κάθε φυσικούς αριθμούς n, k,

$$\lfloor \frac{n+k}{2} \rfloor = \lfloor \frac{n}{2} \rfloor + \lfloor \frac{k}{2} \rfloor.$$

Εικασίες

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

Το Θεώρημα του Φερμά

- Το Θεώρημα του Fermat είναι ίσως η πιο γνωστή πρώην 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. $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $100 = 53 + 47$.
- Η εικασία δεν έχει αποδειχτεί ούτε καταρριφθεί.
- Έχει επιβεβαιωθεί με τη βοήθεια υπολογιστή για όλους τους αριθμούς μέχρι το 10^{17}.

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 αυτή 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 υπολογιστική βοήθεια.

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 οποιονδήποτε 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:

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

- Για $s > 1$ 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 s που ικανοποιούν $\zeta(s) = 0$, είναι μιγαδικοί αριθμοί με πραγματικό μέρος ίσο με $1/2$.
- Η εικασία προτάθηκε από τον Riemann το 1859 και δεν έχει ακόμα αποδειχτεί ούτε καταρριφθεί. Έχει επαληθευτεί υπολογιστικά για τις πρώτες 1.5×10^9 ρίζες.

Η εικασία του Riemann

- Η εικασία του Riemann σχετίζεται άμεσα με την πυκνότητα των πρώτων αριθμών.
- Πόσοι πρώτοι αριθμοί είναι μικρότεροι από 1000; (168) 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 το πολύ κατά $\sqrt{n}\ln n$.

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.
- Πιο απλά: υπάρχουν προβλήματα για τα οποία είναι σημαντικά 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,

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

  και θέλουμε να βρούμε αν υπάρχουν τιμές των μεταβλητών που κάνουν την πρόταση αληθή.
- Αν κάποιος μας υποδείξει κατάλληλες τιμές μπορούμε εύκολα να επιβεβαιώσουμε αν οι τιμές αυτές έχουν την επιθυμητή ιδιότητα.
- 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.

P vs. NP

Ας περιοριστούμε σε υπολογιστικά προβλήματα απόφασης, στα οποία η απάντηση είναι «ΝΑΙ» ή «ΌΧΙ».

Η κλάση P περιλαμβάνει τα προβλήματα απόφασης στα οποία η απάντηση μπορεί να βρεθεί αποδοτικά, δηλ. σε χρόνο πολυωνυμικό ως προς το μέγεθος n της εισόδου.

Η κλάση NP περιλαμβάνει τα προβλήματα απόφασης στα οποία εάν μας δοθεί μαζί με την είσοδο, μια υπόδειξη με μέγεθος πολυωνυμικό στο n, τότε μπορούμε να βρούμε την απάντηση σε πολυωνυμικό χρόνο.

Πρόταση

SATISFIABILITY $\in$ NP.

Προφανώς P $\subseteq$ NP. Το μεγάλο ερώτημα είναι αν P $\neq$ NP.

Planar 3-Coloring

- Δίνεται χάρτης. Μπορεί να χρωματιστεί με τρία χρώματα ώστε γειτονικές χώρες να έχουν διαφορετικά χρώματα;
- Γνωρίζουμε από το Θεώρημα των Τεσσάρων Χρώματων, πως τέσσερα χρώματα είναι πάντα αρκετά.

Πρόταση

Planar 3-Coloring $\in$ NP.

Θεώρημα

Εάν βρεθεί πολυωνυμικός αλγόριθμος για το Satisfiability *ή το* Planar 3-Coloring, *τότε* P = NP.

Χιλιάδες προβλήματα είναι «ισοδύναμα» με το Satisfiability και το Planar 3-Coloring. Αν βρούμε πολυωνυμικό αλγόριθμο για ένα από αυτά, τότε P=NP!! Όλα αυτά τα προβλήματα χαρακτηρίζονται ως NP-πλήρη.

Εφαρμογές;

- Αν και τέτοια θέματα φαίνονται να μην έχουν εφαρμογές, πολλές φορές η ανάπτυξη της τεχνολογίας μεταφέρει τέτοια 'θεωρητικά' θέματα στο πεδίο των εφαρμογών.
- Η εικασία του Riemann σχετίζεται με την επίδοση κρυπτογραφικών αλγορίθμων.
- Εάν καταρριφθεί η εικασία P$\neq$NP, αλλάζει δραματικά η έννοια του δύσβατου (intractable) υπολογιστικού προβλήματος. Καλό για πολλές εφαρμογές, κακό για πολλές άλλες, όπως π.χ., τις κρυπτογραφικές.