# Ανεπίλυτα και δυσεπίλυτα προβλήματα στα μαθηματικά: λογική, πληροφορική και mastercard

Γιάννης Ν. Μοσχοβάκης
UCLA και ΕΚΠΑ

Ηράκλειο, 19 Μαΐου, 2008

# Περίληψη

- Υπάρχουν ανεπίλυτα προβλήματα; (Μαθηματική Λογική)
  - Στα μαθηματικά
  - Αυστηρά διατυπωμένα
  - Με απόδειξη ότι δεν έχουν λύση
- Υπάρχουν δισεπίλυτα προβλήματα; (Πληροφορική)
  (χωρίς λύση που να μπορεί πρακτικά να υπολογιστεί)
  - Στα μαθηματικά
  - Αυστηρά διατυπωμένα
  - Με απόδειξη της δυσκολίας υπολογισμού της λύσης
- Και έχουν όλα αυτά κάποια σχέση με την καθημερινότητα;
  (Πιστωτικές κάρτες)

(Βασικά, και στις τρεις ερωτήσεις) Ναι!

# Παραδείγματα από την άλγεβρα – εξισώσεις

| Εξίσωση | Έχει λύση αν | Η λύση είναι |
|---|---|---|
| $ax + b = 0$<br>$(2x + 3 = 0)$ | $a \neq 0$<br>(Ναι) | $x = -\frac{b}{a}$<br>$(x = -\frac{3}{2})$ |
| $ax^2 + bx + c = 0$<br>$(x^2 + 3x + 1 = 0)$ | $b^2 - 4ac \geq 0$<br>$(3^2 - 4 = 5 \geq 0,$ Ναι$)$ | $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$<br>$(x = \frac{-3 \pm \sqrt{5}}{2})$ |
| $p(x) = 0$<br>$(x^6 - x^5$<br>$- 3x^2 + 2x + 1 = 0)$ | αλγόριθμος του Sturm (1803-1855)<br>4 λύσεις | προσεγγιστικοί αλγόριθμοι<br>$1, \approx 1,38879$<br>$\approx -0,334734, -1,21465$ |

# Ο αλγόριθμος του Tarski

**Θεώρημα** (Tarski, 1930)

*Υπάρχει αλγόριθμος που αποφασίζει αν η τυχαία απλή (πρωτοβάθμια) πρόταση της άλγεβρας αληθεύει*

Παραδείγματα απλών προτάσεων της άλγεβρας:

- «Η εξίσωση $p(x) = 0$ έχει 5 (πραγματικές) λύσεις»
- «Υπάρχουν αριθμοί $\vec{x} = (x_1, x_2, \ldots, x_n)$ τέτοιοι που

$$p(\vec{x}) = 0 \text{ και } q(\vec{x}) \geq 0 \text{ και } r(\vec{x}) \geq 0\text{»}$$

όπου $p(\vec{x}) = p(x_1, \ldots, x_n)$ πολυώνυμο, π.χ., $\boxed{x_1^5 x_2 - x_2 x_3 + 23 x_1 x_3^{16}}$

- «Για όλους τους $\vec{x} = (x_1, x_2, \ldots, x_n)$,

$$p(\vec{x}) = 0 \text{ ή } \Big( q(\vec{x}) > 0 \text{ και υπάρχει } y \text{ τέτοιος που } r(y, \vec{x}) = 0 \Big)\text{»}$$

# Οι απλές (πρωτοβάθμιες) προτάσεις της άλγεβρας

είναι οι γραμματικά σωστές ακολουθίες από τα εξής 16 σύμβολα:

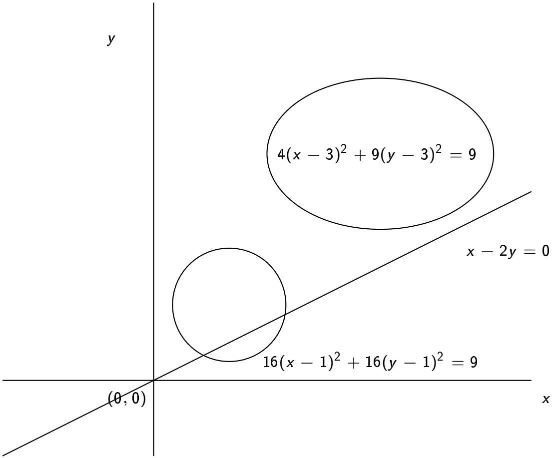
| | |
|---|---|
| $0 \quad 1 \quad + \quad - \quad \cdot \quad = \quad <$ | (αλγεβρικές πράξεις) |
| $\neg$ (όχι) & (και) $\vee$ (ή) | (προτασιακοί τελεστές) |
| $\exists$ (υπάρχει) $\forall$ (για κάθε) | (ποσοδείκτες) |
| ( ) | (σημεία στίξεως) |
| $x \quad \vert$ | (μεταβλητές $x\vert \quad x\vert\vert \quad x\vert\vert\vert \quad \ldots$) |

- Για κάθε αριθμό υπάρχει ένας μεγαλύτερος (Ελληνικά)
- $(\forall x)(\exists y)[x < y]$ («μαθηματικά-Ελληνικά»)
- $(\forall x|)(\exists x||)(x| < x||)$ (τυπική απλή πρόταση)

- Οι μεταβλητές ερμηνεύονται με πραγματικούς αριθμούς στο

$$\mathbb{R} = \{1, -3, \frac{2}{3}, \sqrt{5}, \pi, \ldots\}$$

# Αναλυτική γεωμετρία



# Η γεωμετρία του Ευκλείδη

Η χρήση Καρτεσιανών συντεταγμένων μεταφράζει τα προβλήματα της Ευκλείδειας Γεωμετρίας σε προβλήματα της άλγεβρας που εκφράζονται από απλές (πρωτοβάθμιες) προτάσεις, άρα

**Πόρισμα** (Tarski, 1930)

*Η Γεωμετρία του Ευκλείδη είναι αποκρίσιμη,*

δηλαδή *υπάρχει αλγόριθμος που αποφασίζει αν η τυχαία πρόταση της Γεωμετρίας του Ευκλείδη αληθεύει ή όχι*

- Ο κύκλος του Απολλώνιου
- Η γραμμή των τριών σημείων και ο κύκλος των 9 σημείων του Euler
- ...
- Υπάρχουν πολύ σημαντικές εφαρμογές στα γραφικά

# Οι απλές (πρωτοβάθμιες) προτάσεις της αριθμητικής

είναι οι γραμματικά σωστές ακολουθίες από τα 16 σύμβολα:

| | |
|---|---|
| $0 \quad 1 \quad + \quad - \quad \cdot \quad = \quad <$ | (αριθμητικές σύμβολα) |
| $\neg$ (όχι) & (και) $\vee$ (ή) | (προτασιακοί τελεστές) |
| $\exists$ (υπάρχει) $\forall$ (για κάθε) | (ποσοδείκτες) |
| ( ) | (σημεία στίξεως) |
| $x \quad \vert$ | (μεταβλητές $x\vert \quad x\vert\vert \quad x\vert\vert\vert \quad \ldots$) |

ακριβώς όπως και για την άλγεβρα, $\boxed{\text{αλλά}}$

- Οι μεταβλητές ερμηνεύονται στο σύνολο των ακέραιων αριθμών

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$$

# Άλγεβρα και αριθμητική

- «Υπάρχει λύση της εξίσωσης $2x + 3 = 0$»

  Αληθεύει στην άλγεβρα ($x = -\frac{3}{2}$)

  Δεν αληθεύει στην αριθμητική

- «Υπάρχει λύση της $x^4 + 2x^3 + x^2 + 5x + 6$»

  2 λύσεις στην άλγεβρα (με τον Sturm, ή και πιο εύκολα)

  Οι ακέραιες λύσεις πρέπει να διαιρούν τον 6, οπότε δοκιμάζουμε τους αριθμούς $0, \pm 1, \pm 2, \pm 3, \pm 6$ και βρίσκουμε ότι η μόνη ακέραιη λύση είναι η $x = -2$

# Η αριθμητική είναι πιο δύσκολη από την άλγεβρα!

**Θεώρημα** (Andrew Wiles, 1994)

*Η εξίσωση* $x^n + y^n = z^n$ *δεν έχει ακέραιες, θετικές λύσεις για* $n > 2$

Η εικασία έγινε από τον Fermat το 1640, που πίστευε ότι την είχε αποδείξει (μόνο που «δε χώραγε η απόδειξη» στο περιθώριο του σημειωματάριού του!) και γι' αυτό είναι γνωστή ως Το τελευταίο θεώρημα του Fermat, αλλά σωστή απόδειξη δεν δόθηκε πριν από το 1994

# Πρώτοι αριθμοί

Ο $x > 1$ είναι πρώτος αν διαιρείται μόνο από τον 1 και τον $x$

$$\text{Πρώτοι: } 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$$

- Υπάρχουν 1229 πρώτοι αριθμοί $< 10000$
- Υπάρχουν άπειροι το πλήθος πρώτοι αριθμοί (Ευκλείδης)

Ο $x$ είναι δίδυμος πρώτος αν είναι πρώτος και ο $x + 2$ είναι επίσης πρώτος

$$\text{Δίδυμοι πρώτοι: } 3, 5, 11, 17, 29, 41, 59, 71, 101, 107, \ldots$$

- Υπάρχουν 205 δίδυμοι πρώτοι αριθμοί $< 10000$
- Υπάρχουν άπειροι το πλήθος δίδυμοι πρώτοι αριθμοί; Άγνωστο

# Αριθμητικές αλήθειες

**Θεώρημα** (Turing, Church, 1936)

*Δεν υπάρχει αλγόριθμος που να αποφασίζει αν η τυχαία απλή πρόταση της αριθμητικής αληθεύει*, με άλλα λόγια,

Το πρόβλημα της αριθμητικής αλήθειας είναι ανεπίλυτο

**Θεώρημα** (Matiyasevich 1970, $\Leftarrow$ Davis, Putnam, Robinson)

*Δεν υπάρχει αλγόριθμος που να αποφασίζει αν για τυχαίο πολυώνυμο* $p(x_1, \ldots, x_n)$ *με ακέραιους συντελεστές η εξίσωση*

$$p(x_1, \ldots, x_n) = 0$$

*έχει ακέραιες λύσεις*, με άλλα λόγια,

Το 10ο πρόβλημα του Hilbert είναι ανεπίλυτο

Hilbert 1900: 23 προβλήματα «*που θα απασχολήσουν τους μαθηματικούς στον 20ο αιώνα*»

## Πως μπορούμε να αποδείξουμε ότι ένα πρόβλημα είναι απόλυτα ανεπίλυτο;

### Το Αίτημα Church-Turing (1936)

*Αν μια συνάρτηση $f(\alpha)$ στις λέξεις από ένα πεπερασμένο αλφάβητο $\Sigma$ υπολογίζεται από κάποιον αλγόριθμο, τότε η $f(\alpha)$ υπολογίζεται από κάποιο πρόγραμμα σε έναν υπολογιστή με άπειρα μεγάλο σκληρό δίσκο*

- Το απαιτούμενο πρόγραμμα μπορεί να εκφραστεί σε οποιαδήποτε από τις συνήθεις γλώσσες (Pascal, C, Java, ...)
- «Άπειρος» σημαίνει «απεριόριστος»: ο υπολογισμός κάθε συγκεκριμένης τιμής $f(\alpha)$ είναι πεπερασμένος

- Οι αυστηρές αποδείξεις των θεωρημάτων αναποκρισιμότητας γίνονται με τη μαθηματική και λογική ανάλυση των υπολογισμών που μπορεί να κάνει μια μηχανή
- Χρησιμοποιούνται βασικοί μέθοδοι του Kurt Gödel

CT: «Ο πρώτος φυσικός νόμος των μαθηματικών»

# Δισεπίλυτα προβλήματα: παραγοντοποίηση

- *Κάθε ακέραιος* $x > 1$ *είναι γινόμενο πρώτων αριθμών*

$$\begin{aligned} 20 &= 2 \cdot 2 \cdot 5 \\ 1817 &= 23 \cdot 79 \\ 60915799 &= 7 \cdot 23 \cdot 71 \cdot 73 \cdot 73 \\ 9984204641 &= 99961 \cdot 99881 \end{aligned}$$

- Ο πολλαπλασιασμός είναι εύκολος,
  αλλά η παραγοντοποίηση είναι δύσκολη!

# Υπολογιστική πολυπλοκότητα

Το μήκος $n$ ενός θετικού ακεραίου $x$ είναι ο αριθμός των ψηφίων του (στο δεκαδικό σύστημα)

| αριθμός $= x$ | μήκος $= n$ |
|---|---|
| 1817 | 4 |
| 60915799 | 8 |
| 9984204641 | 10 |

$$\text{μήκος του } x = n \iff 10^{n-1} \leq x < 10^n$$

- Η πολυπλοκότητα ενός αλγόριθμου είναι ο αριθμός (ατομικών) πράξεων που κάνει η μηχανή για να υπολογίσει την τιμή $f(x)$ όταν το μήκος του $x$ είναι $n$

# Πολυωνυμικοί και εκθετικοί αλγόριθμοι

| Πράξη με $x, y$, με μήκος $\leq n$ | Πολυπλοκότητα | |
|---|---|---|
| $x+y, x-y$ | $\sim Cn$ | (πολυωνυμικός) |
| $x \cdot y$ | $\sim Cn^2$ | (πολυωνυμικός) |
| παραγοντοποίηση | $\sim C10^n$ | (εκθετικός) |

- Πολυωνυμικός αλγόριθμος : πολυπλοκότητα $\sim Cn^d$
- Εκθετικός αλγόριθμος : πολυπλοκότητα $\sim C10^n$

για $n = 20, d = 12$

$$
\begin{aligned}
20^{12} &= 4.096.000.000.000.000 \\
10^{20} &= 100.000.000.000.000.000.000
\end{aligned}
$$

Εικασία $P \neq NP$:

Κάθε αλγόριθμος παραγοντοποίησης είναι εκθετικός

# Το κρυπτογραφικό σύστημα RSA
(Ron Rivest, Adi Shamir, και Leonard Adleman, 1978)

- Η κωδικοποίηση βασίζεται σε δυο (μεγάλους) πρώτους αριθμούς, $p$ και $q$ και έναν αριθμό $E < pq$.
  Το γινόμενο $n = pq$ και ο αριθμός $E$ κοινοποιούνται
- Για κάθε κείμενο $T < pq$, η κωδικοποίηση του $T$ είναι ένας αριθμός $C < E$, που επίσης κοινοποιείται
- Ο δέκτης της πληροφορίας (π.χ., η τράπεζα) γνωρίζει έναν μυστικό αριθμό $D$, με τον οποίο μπορεί εύκολα να αποκωδικοποιήσει την πληροφορία και να διαβάσει το $T$
- Εικασία RSA: *Δεν υπάρχει αλγόριθμος που να υπολογίζει το $T$ από τα $E, n, C$ χωρίς να παραγοντοποιήσει τον αριθμό $n$*

Η ασφάλεια της μεθόδου στηρίζεται στις εικασίες $P \neq NP$ και RSA