Εξισώσεις στην άλγεβρα και στην αριθμητική

Γιάννης Ν. Μοσχοβάκης
UCLA και ΕΚΠΑ

Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
26 Μαΐου, 2008

Περίληψη

Θεωρούμε εξισώσεις

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

όπου το $p(x_1, \ldots, x_d)$ είναι πολυώνυμο με ακέραιους συντελεστές σε $\boxed{d \text{ μεταβλητές}}$ και με $\boxed{\text{βαθμό } n}$, π.χ.,

$$\begin{aligned} p(x) &= x^6 - x^5 - 3x^2 + 2x + 1 \qquad (d = 1, n = 6) \\ p(x_1, x_2, x_3) &= x_1^5 x_2 - x_2 x_3 + 23 x_1 x_3^{16} - 7 \quad (d = 3, n = 17) \end{aligned}$$

(1) Άλγεβρα: Υπάρχουν πραγματικές λύσεις της (*), και ποιες;
Πραγματικοί αριθμοί: $0, -3, \frac{2}{3}, \sqrt{5}, \pi, \ldots$

(2) Αριθμητική: Υπάρχουν ακέραιες λύσεις της (*), και ποιες;
Ακέραιοι: $\ldots, -2, -1, 0, 1, 2, \ldots$

- $\boxed{\text{Λογική: Ποιο πρόβλημα είναι πιο δύσκολο;}}$

Αλγεβρικές εξισώσεις σε μια μεταβλητή ($d = 1$)

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

Διαίρεση ρητών πολυωνύμων

Θεώρημα

Για τυχαία πολυώνυμα με ρητούς συντελεστές $f(x), g(x)$ *αν* $\beta\alpha\theta(f(x)) \geq \beta\alpha\theta(g(x))$, *τότε υπάρχουν μοναδικά πολυώνυμα* $q(x), r(x)$ *τέτοια που*

$$\boxed{f(x) = g(x)q(x) + r(x) \text{ όπου } r(x) = 0 \text{ ή } \beta\alpha\theta(r(x)) < \beta\alpha\theta(g(x))}$$

Με $r^*(x) = -r(x)$, η εξίσωση της διαίρεσης παίρνει τη μορφή

$$\boxed{f(x) = g(x)q(x) - r^*(x)}$$

όπου πάλι $r^*(x) = 0$ ή $\beta\alpha\theta(r^*(x)) < \beta\alpha\theta(g(x))$

Ο αλγόριθμος του Sturm, για ρητό πολυώνυμο $p(x)$

- Η ακολουθία Sturm του $p(x)$:

$$\begin{aligned}
\boxed{p_0(x)} &= p(x), \quad \boxed{p_1(x)} = p'(x) \quad (\text{η παράγωγος του } p(x)) \\
p_0(x) &= p_1(x)q_1(x) - \boxed{p_2(x)} \\
p_1(x) &= p_2(x)q_2(x) - \boxed{p_3(x)} \\
&\vdots \\
p_r(x) &= p_{r+1}(x)q_{r+1}(x)
\end{aligned}$$

- $w(\alpha) =$ ο αριθμός αλλαγών προσήμου στην ακολουθία $(p_0(\alpha), p_1(\alpha), p_2(\alpha), \ldots, p_{r+1}(\alpha))$

$$\boxed{\text{Αν } p(a)p(b) \neq 0, \text{ τότε το } p(x) \text{ έχει } w(a) - w(b) \text{ ρίζες στο } (a, b)}$$

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

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

όπου $p(\vec{x}) = p(x_1, \ldots, x_n), q(\vec{x}), r(\vec{x})$ πολυώνυμα,

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

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

Οι απλές (πρωτοβάθμιες) προτάσεις της άλγεβρας

είναι οι γραμματικά σωστές ακολουθίες από τα εξής 16 σύμβολα:

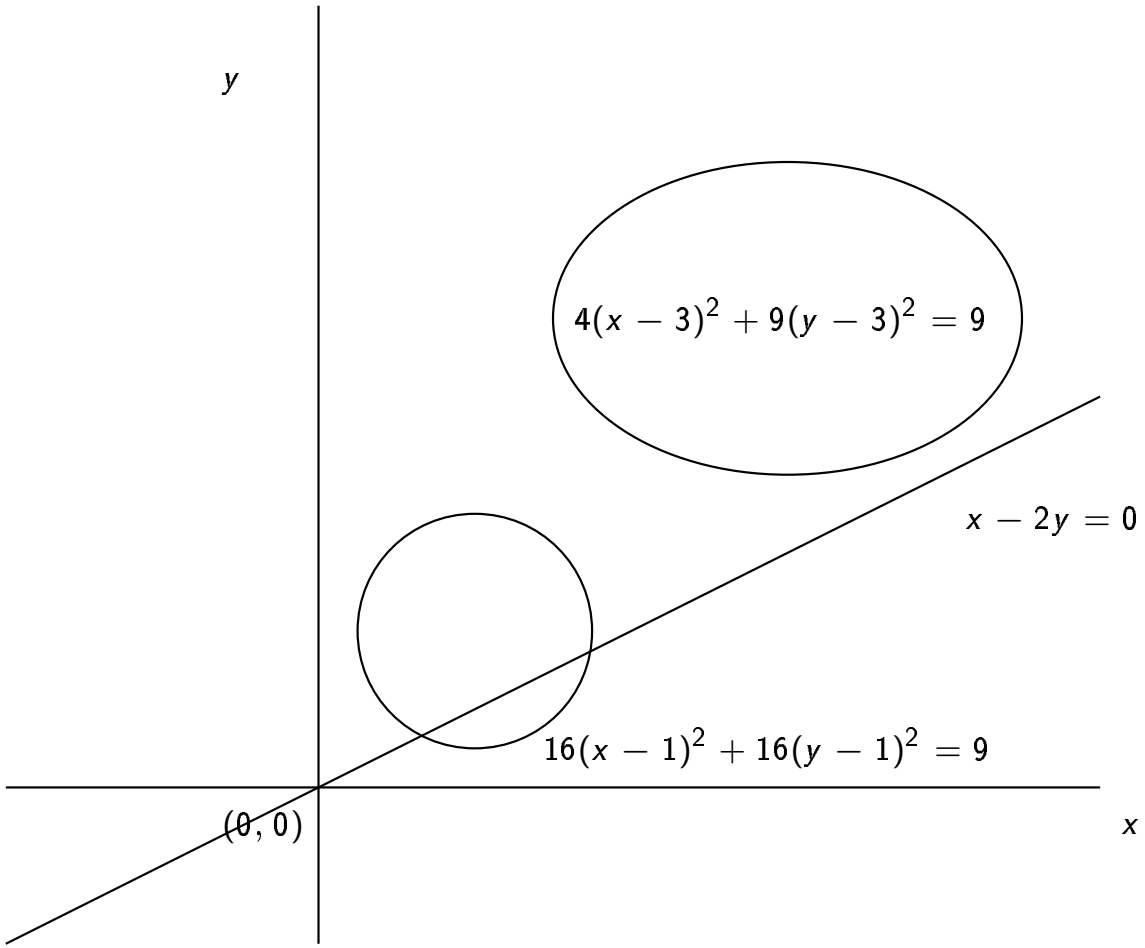
$0 \quad 1 \quad + \quad - \quad \cdot \quad = \quad <$	(αλγεβρικές πράξεις)
$\neg$ (όχι) $\quad \&$ (και) $\quad \vee$ (ή)	(προτασιακοί τελεστές)
$\exists$ (υπάρχει) $\quad \forall$ (για κάθε)	(ποσοδείκτες)
$(\quad)$	(σημεία στίξεως)
$x \quad \vert$	(μεταβλητές $x\vert \quad x\vert\vert \quad x\vert\vert\vert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

- Για κάθε αριθμό υπάρχει ένας μεγαλύτερος (Ελληνικά)
- $(\forall x)(\exists y)[x < y]$ («μαθηματικά-Ελληνικά»)
- $(\forall x\vert)(\exists x\vert\vert)(x\vert < x\vert\vert)$ (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 απλά προβλήματα της Ευκλείδειας Γεωμετρίας σε προβλήματα της άλγεβρας που εκφράζονται από απλές (πρωτοβάθμιες) προτάσεις, άρα:

Πόρισμα (Tarski, 1930)

Η (απλή) Γεωμετρία του Ευκλείδη είναι αποκρίσιμη,

δηλαδή *υπάρχει αλγόριθμος που αποφασίζει αν η τυχαία, απλή 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

Γεωμετρία: διαισθητικά απλές προτάσεις όχι πάντα απλές

- Απλή: Κάθε γωνία τριχοτομείται

  Όχι απλή: Κάθε γωνία τριχοτομείται με κανόνα και διαβήτη

- Απλή: Κάθε κύβος διπλασιάζεται

  Όχι απλή: Κάθε κύβος διπλασιάζεται με κανόνα και διαβήτη

- Όχι απλή: Ο κύκλος με ακτίνα 1 τετραγωνίζεται

  (Επειδή ο π δεν είναι αλγεβρικός αριθμός)

Οι απλές (πρωτοβάθμιες) προτάσεις της γεωμετρίας είναι αυτές που εκφράζονται στην πρωτοβάθμια γλώσσα της άλγεβρας με τη χρήση Καρτεσιανών συντεταγμένων

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) $\quad \&$ (και) $\quad \vee$ (ή)	(προτασιακοί τελεστές)
$\exists$ (υπάρχει) $\quad \forall$ (για κάθε)	(ποσοδείκτες)
$(\quad)$	(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, 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 $x^4 + 2x^3 + x^2 + 5x + 6 = 0$»

  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

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

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 Σ 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»