Ο Ευκλείδειος αλγόριθμος και μερικοί συγγενείς του

Γιάννης Μοσχοβάκης
ΕΚΠΑ και UCLA

Ημερίδα Μαθηματικών στην Εστία Επιστημών Πάτρας
Δευτέρα, 5 Ιουλίου 2010

Θέματα

(I) Η διδασκαλία της μαθηματικής μεθοδολογίας αυστηροί ορισμοί – αποδείξεις

(II) Η πληροφορική ως πηγή προβλημάτων στα «καθαρά» μαθηματικά

(III) Σχετικά αποτελέσματα από τη λογική

(1) Ο μέγιστος κοινός διαιρέτης μκδ(x, y)

(2) Εξισώσεις στην άλγεβρα και την αριθμητική

(3) Πρωτοβάθμια άλγεβρα: ο αλγόριθμος του Tarski

(4) Πρωτοβάθμια αριθμητική

(5) Ανεπίλυτα προβλήματα: πως δείχνουμε ότι υπάρχουν;

(6) Δισεπίλυτα προβλήματα: παραγοντοποίηση

Θέματα

(I) Η διδασκαλία της μαθηματικής μεθοδολογίας αυστηροί ορισμοί – αποδείξεις

(II) Η πληροφορική ως πηγή προβλημάτων στα «καθαρά» μαθηματικά

(III) Σχετικά αποτελέσματα από τη λογική

(1) Ο μέγιστος κοινός διαιρέτης μκδ(x, y)

(2) Εξισώσεις στην άλγεβρα και την αριθμητική

(3) Πρωτοβάθμια άλγεβρα: ο αλγόριθμος του Tarski

(4) Πρωτοβάθμια αριθμητική

(5) Ανεπίλυτα προβλήματα: πως δείχνουμε ότι υπάρχουν;

(6) Δισεπίλυτα προβλήματα: παραγοντοποίηση

Θέματα

(I) Η διδασκαλία της μαθηματικής μεθοδολογίας αυστηροί ορισμοί – αποδείξεις

(II) Η πληροφορική ως πηγή προβλημάτων στα «καθαρά» μαθηματικά

(III) Σχετικά αποτελέσματα από τη λογική

(1) Ο μέγιστος κοινός διαιρέτης μκδ(x, y)

(2) Εξισώσεις στην άλγεβρα και την αριθμητική

(3) Πρωτοβάθμια άλγεβρα: ο αλγόριθμος του Tarski

(4) Πρωτοβάθμια αριθμητική

(5) Ανεπίλυτα προβλήματα: πως δείχνουμε ότι υπάρχουν;

(6) Δισεπίλυτα προβλήματα: παραγοντοποίηση

Θέματα

(I) Η διδασκαλία της μαθηματικής μεθοδολογίας αυστηροί ορισμοί – αποδείξεις

(II) Η πληροφορική ως πηγή προβλημάτων στα «καθαρά» μαθηματικά

(III) Σχετικά αποτελέσματα από τη λογική

(1) Ο μέγιστος κοινός διαιρέτης μκδ(x, y)

(2) Εξισώσεις στην άλγεβρα και την αριθμητική

(3) Πρωτοβάθμια άλγεβρα: ο αλγόριθμος του Tarski

(4) Πρωτοβάθμια αριθμητική

(5) Ανεπίλυτα προβλήματα: πως δείχνουμε ότι υπάρχουν;

(6) Δισεπίλυτα προβλήματα: παραγοντοποίηση

Θέματα

(I) Η διδασκαλία της μαθηματικής μεθοδολογίας αυστηροί ορισμοί – αποδείξεις

(II) Η πληροφορική ως πηγή προβλημάτων στα «καθαρά» μαθηματικά

(III) Σχετικά αποτελέσματα από τη λογική

(1) Ο μέγιστος κοινός διαιρέτης μκδ(x, y)

(2) Εξισώσεις στην άλγεβρα και την αριθμητική

(3) Πρωτοβάθμια άλγεβρα: ο αλγόριθμος του Tarski

(4) Πρωτοβάθμια αριθμητική

(5) Ανεπίλυτα προβλήματα: πως δείχνουμε ότι υπάρχουν;

(6) Δισεπίλυτα προβλήματα: παραγοντοποίηση

(1) Ο μέγιστος κοινός διαιρέτης μκδ(x, y)

Θεώρημα Διαίρεσης

Για κάθε ζεύγος φυσικών αριθμών $x \geq y \geq 1$, υπάρχουν ακριβώς δύο φυσικοί αριθμοί **m** και **r**, τέτοιοι που

$$x = yq + r, \qquad 0 \leq r < y.$$

Θέτουμε:

$$q = \text{πηλ}(x, y) \quad \text{και} \quad r = \text{υπολ}(x, y)$$

$$y \mid x \iff \text{υπολ}(x, y) = 0 \qquad (\text{ο } x \text{ διαιρεί τον } y)$$

$$\boxed{\text{μκδ}(x, y) = \text{ο μέγιστος } k \text{ τέτοιος που } k \mid x \text{ και } k \mid y}$$

Πως υπολογίζουμε τον μκδ(231, 165) = ;

(1) Ο μέγιστος κοινός διαιρέτης $\mu\kappa\delta(x, y)$

Θεώρημα Διαίρεσης

Για κάθε ζεύγος φυσικών αριθμών $x \geq y \geq 1$, υπάρχουν ακριβώς δύο φυσικοί αριθμοί m και r, τέτοιοι που

$$x = yq + r, \qquad 0 \leq r < y.$$

Θέτουμε:

$$q = \pi\eta\lambda(x, y) \quad \text{και} \quad r = \upsilon\pi\circ\lambda(x, y)$$

$$y \mid x \iff \upsilon\pi\circ\lambda(x, y) = 0 \qquad (\text{ο } x \text{ διαιρεί τον } y)$$

$$\mu\kappa\delta(x, y) = \text{ο μέγιστος } k \text{ τέτοιος που } k \mid x \text{ και } k \mid y$$

Πως υπολογίζουμε τον $\mu\kappa\delta(231, 165) =$;

(1) Ο μέγιστος κοινός διαιρέτης $\mu\kappa\delta(x, y)$

Θεώρημα Διαίρεσης

Για κάθε ζεύγος φυσικών αριθμών $x \geq y \geq 1$, υπάρχουν ακριβώς δύο φυσικοί αριθμοί m και r, τέτοιοι που

$$x = yq + r, \qquad 0 \leq r < y.$$

Θέτουμε:

$$q = \pi\eta\lambda(x, y) \quad \text{και} \quad r = \upsilon\pi\circ\lambda(x, y)$$

$$y \mid x \iff \upsilon\pi\circ\lambda(x, y) = 0 \qquad (\text{ο } x \text{ διαιρεί τον } y)$$

$$\boxed{\mu\kappa\delta(x, y) = \text{ο μέγιστος } k \text{ τέτοιος που } k \mid x \text{ και } k \mid y}$$

Πως υπολογίζουμε τον $\mu\kappa\delta(231, 165) = ;$

(1) Ο μέγιστος κοινός διαιρέτης $\mu\kappa\delta(x, y)$

Θεώρημα Διαίρεσης

Για κάθε ζεύγος φυσικών αριθμών $x \geq y \geq 1$, υπάρχουν ακριβώς δύο φυσικοί αριθμοί m και r, τέτοιοι που

$$x = yq + r, \qquad 0 \leq r < y.$$

Θέτουμε:

$$q = \pi\eta\lambda(x, y) \quad \text{και} \quad r = \upsilon\pi\circ\lambda(x, y)$$
$$y \mid x \iff \upsilon\pi\circ\lambda(x, y) = 0 \qquad (\text{ο } x \text{ διαιρεί τον } y)$$

$$\boxed{\mu\kappa\delta(x, y) = \text{ο μέγιστος } k \text{ τέτοιος που } k \mid x \text{ και } k \mid y}$$

Πως υπολογίζουμε τον $\mu\kappa\delta(231, 165) =$;

Ο αλγόριθμος του Ευκλείδη $(x \geq y \geq 1)$

$$y \mid x \implies \mu\kappa\delta(x, y) = y$$

$$x = yq + r \;\; \& \;\; 0 < r < y \implies \mu\kappa\delta(x, y) = \mu\kappa\delta(y, r)$$

Για $x \geq y \geq 1$, έχουμε την αναδρομική εξίσωση για τον μκδ:

$$\mu\kappa\delta(x, y) = \text{αν } (\upsilon\pi\circ\lambda(x, y) = 0) \text{ τότε } y \text{ αλλιώς } \mu\kappa\delta(y, \upsilon\pi\circ\lambda(x, y)).$$

$$\begin{aligned} \mu\kappa\delta(231, 165) &= \\ &= \mu\kappa\delta(165, 66) \\ &= \mu\kappa\delta(66, 33) \\ &= 33. \end{aligned} \qquad \begin{aligned} 231 &= 165 \cdot 1 + 66 \\ 165 &= 66 \cdot 2 + 33 \\ 66 &= 33 \cdot 2 + 0 \end{aligned}$$

Ο αλγόριθμος του Ευκλείδη $(x \geq y \geq 1)$

$$\boxed{y \mid x \implies \mu\kappa\delta(x,y) = y}$$

$$x = yq + r \;\;\&\;\; 0 < r < y \implies \mu\kappa\delta(x,y) = \mu\kappa\delta(y,r)$$

Για $x \geq y \geq 1$, έχουμε την αναδρομική εξίσωση για τον μκδ:

$$\mu\kappa\delta(x,y) = \text{αν } (\upsilon\pi\circ\lambda(x,y) = 0) \text{ τότε } y \text{ αλλιώς } \mu\kappa\delta(y, \upsilon\pi\circ\lambda(x,y)).$$

$$\begin{aligned} \mu\kappa\delta(231,165) &= \\ &= \mu\kappa\delta(165,66) \\ &= \mu\kappa\delta(66,33) \\ &= 33. \end{aligned} \qquad \begin{aligned} 231 &= 165 \cdot 1 + 66 \\ 165 &= 66 \cdot 2 + 33 \\ 66 &= 33 \cdot 2 + 0 \end{aligned}$$

Ο αλγόριθμος του Ευκλείδη $(x \geq y \geq 1)$

$$\boxed{y \mid x \implies \mu\kappa\delta(x, y) = y}$$

$$\boxed{x = yq + r \ \ \& \ \ 0 < r < y \implies \mu\kappa\delta(x, y) = \mu\kappa\delta(y, r)}$$

Για $x \geq y \geq 1$, έχουμε την αναδρομική εξίσωση για τον μκδ:

$$\begin{aligned} \mu\kappa\delta(x, y) \ &= \ \text{αν } (\upsilon\pi\circ\lambda(x, y) = 0) \text{ τότε } y \\ &\quad\ \ \text{αλλιώς } \mu\kappa\delta(y, \upsilon\pi\circ\lambda(x, y)). \end{aligned}$$

$$\begin{aligned} \mu\kappa\delta(231, 165) \ &= \\ &= \mu\kappa\delta(165, 66) \\ &= \mu\kappa\delta(66, 33) \\ &= 33. \end{aligned} \qquad \begin{aligned} 231 \ &= \ 165 \cdot 1 + 66 \\ 165 \ &= \ 66 \cdot 2 + 33 \\ 66 \ &= \ 33 \cdot 2 + 0 \end{aligned}$$

Ο αλγόριθμος του Ευκλείδη $(x \geq y \geq 1)$

$$\boxed{y \mid x \implies \mu\kappa\delta(x,y) = y}$$

$$\boxed{x = yq + r \ \ \& \ \ 0 < r < y \implies \mu\kappa\delta(x,y) = \mu\kappa\delta(y,r)}$$

Για $x \geq y \geq 1$, έχουμε την αναδρομική εξίσωση για τον μκδ:

$$\begin{aligned} \mu\kappa\delta(x,y) \ &= \ \text{αν } (\upsilon\pi\circ\lambda(x,y) = 0) \text{ τότε } y \\ &\quad\ \ \text{αλλιώς } \mu\kappa\delta(y, \upsilon\pi\circ\lambda(x,y)). \end{aligned}$$

$$\begin{aligned} \mu\kappa\delta(231,165) \ &= \\ &= \mu\kappa\delta(165,66) \\ &= \mu\kappa\delta(66,33) \\ &= 33. \end{aligned} \qquad \begin{aligned} 231 \ &= \ 165 \cdot 1 + 66 \\ 165 \ &= \ 66 \cdot 2 + 33 \\ 66 \ &= \ 33 \cdot 2 + 0 \end{aligned}$$

Ο αλγόριθμος του Ευκλείδη $(x \geq y \geq 1)$

$$\boxed{y \mid x \implies \mu\kappa\delta(x,y) = y}$$

$$\boxed{x = yq + r \;\;\&\;\; 0 < r < y \implies \mu\kappa\delta(x,y) = \mu\kappa\delta(y,r)}$$

Για $x \geq y \geq 1$, έχουμε την αναδρομική εξίσωση για τον μκδ:

$$\begin{aligned} \mu\kappa\delta(x,y) \;\; = \;\; & \text{αν } (\upsilon\pi\circ\lambda(x,y) = 0) \text{ τότε } y \\ & \text{αλλιώς } \mu\kappa\delta(y, \upsilon\pi\circ\lambda(x,y)). \end{aligned}$$

$$\begin{aligned} \mu\kappa\delta(231,165) &= \\ &= \mu\kappa\delta(165,66) \\ &= \mu\kappa\delta(66,33) \\ &= 33. \end{aligned} \qquad \begin{aligned} 231 &= 165 \cdot 1 + 66 \\ 165 &= 66 \cdot 2 + 33 \\ 66 &= 33 \cdot 2 + 0 \end{aligned}$$

Η πολυπλοκότητα του Ευκλείδειου

$$\mathbf{c_\varepsilon(x,y)} \;=\; \text{ο αριθμός των διαιρέσεων που χρειάζονται για τον υπολογισμό του } \mu\kappa\delta\mathbf{(x,y)}$$

Αναδρομική εξίσωση για την πολυπλοκότητα του Ευκλείδειου:

$$\mathbf{c_\varepsilon(x,y)} \;=\; \begin{array}{l} \alpha\nu\ (\mathbf{y} \mid \mathbf{x})\ \tau\acute{o}\tau\varepsilon\ \mathbf{1} \\ \alpha\lambda\lambda\iota\acute{\omega}\varsigma\ \mathbf{1 + c_\varepsilon(y, \upsilon\pi o\lambda(x,y))} \end{array}$$

$$\begin{aligned} \mathbf{c_\varepsilon(231,165)} &= \mathbf{1 + c_\varepsilon(165,66)} \\ &= \mathbf{2 + c_\varepsilon(66,33)} \\ &= \mathbf{2 + 1 = 3} \end{aligned}$$

Η πολυπλοκότητα του Ευκλείδειου

$$\mathbf{c}_\varepsilon(\mathbf{x},\mathbf{y}) \;=\; \text{ο αριθμός των διαιρέσεων που χρειάζονται για τον υπολογισμό του μκδ}(\mathbf{x},\mathbf{y})$$

Αναδρομική εξίσωση για την πολυπλοκότητα του Ευκλείδειου:

$$\mathbf{c}_\varepsilon(\mathbf{x},\mathbf{y}) \;=\; \text{αν } (\mathbf{y} \mid \mathbf{x}) \text{ τότε } \mathbf{1} \quad \text{αλλιώς } \mathbf{1} + \mathbf{c}_\varepsilon(\mathbf{y}, \text{υπολ}(\mathbf{x},\mathbf{y}))$$

$$\begin{aligned} \mathbf{c}_\varepsilon(231,165) &= 1 + \mathbf{c}_\varepsilon(165,66) \\ &= 2 + \mathbf{c}_\varepsilon(66,33) \\ &= 2 + 1 = 3 \end{aligned}$$

Η πολυπλοκότητα του Ευκλείδειου

$$\mathbf{c}_\varepsilon(\mathbf{x},\mathbf{y}) \;=\; \text{ο αριθμός των διαιρέσεων που χρειάζονται για τον υπολογισμό του μκδ}(\mathbf{x},\mathbf{y})$$

Αναδρομική εξίσωση για την πολυπλοκότητα του Ευκλείδειου:

$$\mathbf{c}_\varepsilon(\mathbf{x},\mathbf{y}) \;=\; \text{αν } (\mathbf{y} \mid \mathbf{x}) \text{ τότε } \mathbf{1} \quad \text{αλλιώς } \mathbf{1} + \mathbf{c}_\varepsilon(\mathbf{y}, \text{υπολ}(\mathbf{x},\mathbf{y}))$$

$$\begin{aligned} \mathbf{c}_\varepsilon(\mathbf{231},\mathbf{165}) &= \mathbf{1} + \mathbf{c}_\varepsilon(\mathbf{165},\mathbf{66}) \\ &= \mathbf{2} + \mathbf{c}_\varepsilon(\mathbf{66},\mathbf{33}) \\ &= \mathbf{2} + \mathbf{1} = \mathbf{3} \end{aligned}$$

Άνω φράγμα πολυπλοκότητας

Θεώρημα

Για όλα τα $x \geq y \geq 2$, $c_\varepsilon(x, y) \leq 2 \log_2 y$.

Απόδειξη. Με (πλήρη) επαγωγή στο y. Χρειάζονται τρεις περιπτώσεις:

Περίπτωση 1, $y \mid x$.

Περίπτωση 2, $x = yq_1 + r_1$ με $0 < r_1 < y$ και $r_1 \mid y$.

Περίπτωση 3, $x = yq_1 + r_1$ και $y = r_1 q_2 + r_2$ με $0 < r_2 < r_1 < y$.

(Έπεται $y \geq 3$. Αν $r_2 = 1$, εύκολο. Αν $r_2 \geq 2$, κάνε άλλη μία διαίρεση)

Άνω φράγμα πολυπλοκότητας

Θεώρημα

Για όλα τα $\mathbf{x} \geq \mathbf{y} \geq \mathbf{2}$, $\mathbf{c_\varepsilon(x, y) \leq 2 \log_2 y}$.

Απόδειξη. Με (πλήρη) επαγωγή στο $\mathbf{y}$. Χρειάζονται τρεις περιπτώσεις:

Περίπτωση 1, $\mathbf{y \mid x}$.

Περίπτωση 2, $\mathbf{x = yq_1 + r_1}$ με $\mathbf{0 < r_1 < y}$ και $\mathbf{r_1 \mid y}$.

Περίπτωση 3, $\mathbf{x = yq_1 + r_1}$ και $\mathbf{y = r_1 q_2 + r_2}$ με $\mathbf{0 < r_2 < r_1 < y}$.

('Επεται $\mathbf{y \geq 3}$. Αν $\mathbf{r_2 = 1}$, εύκολο. Αν $\mathbf{r_2 \geq 2}$, κάνε άλλη μία διαίρεση)

Κάτω φράγμα – η ακολουθία Fibonacci

$$F_0 = 0, \quad F_1 = 1, \quad F_{k+2} = F_{k+1} + F_k$$

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

Θεώρημα

Αν $\varphi = \frac{1+\sqrt{5}}{2}$, τότε για κάθε $k \geq 1$, $\varphi^{k-2} \leq F_k \leq \varphi^{k-1}$

Θεώρημα

Για $k \geq 2$, $\mu\kappa\delta(F_{k+1}, F_k) = 1$ και

$$\frac{1}{\log_2(\varphi)} \log_2(F_k) \leq \boxed{c_\varepsilon(F_{k+1}, F_k) = k - 1} \leq 2 \log_2(F_k)$$

- Ο φ είναι η χρυσή τομή

Κάτω φράγμα – η ακολουθία Fibonacci

$$F_0 = 0, \quad F_1 = 1, \quad F_{k+2} = F_{k+1} + F_k$$
$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

Θεώρημα

Αν $\varphi = \frac{1+\sqrt{5}}{2}$, τότε για κάθε $k \geq 1$, $\varphi^{k-2} \leq F_k \leq \varphi^{k-1}$

Θεώρημα

Για $k \geq 2$, $\mu\kappa\delta(F_{k+1}, F_k) = 1$ και

$$\frac{1}{\log_2(\varphi)} \log_2(F_k) \leq \boxed{c_\varepsilon(F_{k+1}, F_k) = k - 1} \leq 2 \log_2(F_k)$$

- Ο φ είναι η χρυσή τομή

Κάτω φράγμα – η ακολουθία Fibonacci

$$F_0 = 0, \quad F_1 = 1, \quad F_{k+2} = F_{k+1} + F_k$$
$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

Θεώρημα

Αν $\varphi = \frac{1+\sqrt{5}}{2}$, τότε για κάθε $k \geq 1$, $\varphi^{k-2} \leq F_k \leq \varphi^{k-1}$

Θεώρημα

Για $k \geq 2$, $\mu\kappa\delta(F_{k+1}, F_k) = 1$ και

$$\frac{1}{\log_2(\varphi)} \log_2(F_k) \leq \boxed{c_\varepsilon(F_{k+1}, F_k) = k - 1} \leq 2 \log_2(F_k)$$

- Ο φ είναι η χρυσή τομή

Κάτω φράγμα – η ακολουθία Fibonacci

$$F_0 = 0, \quad F_1 = 1, \quad F_{k+2} = F_{k+1} + F_k$$
$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

Θεώρημα

Αν $\varphi = \frac{1+\sqrt{5}}{2}$, τότε για κάθε $k \geq 1$, $\varphi^{k-2} \leq F_k \leq \varphi^{k-1}$

Θεώρημα

Για $k \geq 2$, $\mu\kappa\delta(F_{k+1}, F_k) = 1$ και

$$\frac{1}{\log_2(\varphi)} \log_2(F_k) \leq \boxed{c_\varepsilon(F_{k+1}, F_k) = k - 1} \leq 2 \log_2(F_k)$$

- Ο φ είναι η χρυσή τομή

Ο δυαδικός αλγόριθμος του Stein για τον μκδ(x, y)

Αναδρομική εξίσωση:

$$\mu\kappa\delta(x,y) = \begin{cases} x & \text{αν } x = y \\ 2\mu\kappa\delta(x/2, y/2) & \text{αλλιώς, αν οι } x, y \text{ είναι άρτιοι} \\ \mu\kappa\delta(x/2, y) & \text{αλλιώς, αν ο } x \text{ άρτιος και ο } y \text{ περιττός} \\ \mu\kappa\delta(x, y/2) & \text{αλλιώς, αν ο } x \text{ περιττός και ο } y \text{ άρτιος} \\ \mu\kappa\delta(x-y, y) & \text{αλλιώς, αν } x > y, \\ \mu\kappa\delta(x, y-x) & \text{αλλιώς,} \end{cases}$$

- Με απλούστερες «δοσμένες» συναρτήσεις, επίσης λογαριθμικός

(2) Εξισώσεις στην άλγεβρα και την αριθμητική

Θεωρούμε εξισώσεις

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

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

$$p(x) := x^6 - x^5 - 3x^2 + 2x + 1 \qquad (d = 1, n = 6)$$
$$p(x_1, x_2, x_3) := x_1^3 x_2 - x_2 x_3 + 23 x_1 x_3^6 - 7 \qquad (d = 3, n = 7)$$

(1) Άλγεβρα: Υπάρχουν πραγματικές λύσεις της $(*)$; και ποιες;
Πραγματικοί αριθμοί: $0, -3, \frac{2}{11}, \sqrt{5}, \pi, \ldots$

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

Λέγεται: Πιο πρόβλημα είναι πιο δύσκολο;

(2) Εξισώσεις στην άλγεβρα και την αριθμητική

Θεωρούμε εξισώσεις

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

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

$$\mathbf{p(x)} = \mathbf{x^6 - x^5 - 3x^2 + 2x + 1} \qquad \mathbf{(d = 1, n = 6)}$$

$$\mathbf{p(x_1, x_2, x_3)} = \mathbf{x_1^5 x_2 - x_2 x_3 + 23 x_1 x_3^{16} - 7} \qquad \mathbf{(d = 3, n = 17)}$$

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

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

- Λογική: Ποιο πρόβλημα είναι πιο δύσκολο;

(2) Εξισώσεις στην άλγεβρα και την αριθμητική

Θεωρούμε εξισώσεις

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

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

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

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

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

- Λογική: Ποιο πρόβλημα είναι πιο δύσκολο;

(2) Εξισώσεις στην άλγεβρα και την αριθμητική

Θεωρούμε εξισώσεις

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

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

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

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

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

- Λογική: Ποιο πρόβλημα είναι πιο δύσκολο;

(2) Εξισώσεις στην άλγεβρα και την αριθμητική

Θεωρούμε εξισώσεις

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

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

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

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

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

- Λογική: Ποιο πρόβλημα είναι πιο δύσκολο;

(2) Εξισώσεις στην άλγεβρα και την αριθμητική

Θεωρούμε εξισώσεις

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

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

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

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

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

- Λογική: Ποιο πρόβλημα είναι πιο δύσκολο;

Αλγεβρικές εξισώσεις σε μια μεταβλητή ($\mathbf{d = 1}$)

Εξίσωση	Έχει λύση αν	Η λύση είναι
$ax + b = 0$ $(2x + 3 = 0)$	$a \neq 0$ (Ναι)	$x = -\frac{b}{a}$ $(x = -\frac{3}{2})$
$ax^2 + bx + c = 0$ $(x^2 + 3x + 1 = 0)$	$b^2 - 4ac \geq 0$ $(3^2 - 4 = 5 \geq 0, \text{Ναι})$	$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ $(x = \frac{-3 \pm \sqrt{5}}{2})$
$p(x) = 0$ $(x^6 - x^5 - 3x^2 + 2x + 1 = 0)$	αλγόριθμος του Sturm (1803-1855) 4 λύσεις	προσεγγιστικοί αλγόριθμοι $1, \approx 1,38879$ $\approx -0,3347, -1,2146$

Αλγεβρικές εξισώσεις σε μια μεταβλητή ($\mathbf{d = 1}$)

Εξίσωση	Έχει λύση αν	Η λύση είναι
$\mathbf{ax + b = 0}$ $\mathbf{(2x + 3 = 0)}$	$a \neq 0$ (Ναι)	$x = -\frac{b}{a}$ $(x = -\frac{3}{2})$
$ax^2 + bx + c = 0$ $(x^2 + 3x + 1 = 0)$	$b^2 - 4ac \geq 0$ $(3^2 - 4 = 5 \geq 0, \text{Ναι})$	$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ $(x = \frac{-3 \pm \sqrt{5}}{2})$
$p(x) = 0$ $(x^6 - x^5$ $- 3x^2 + 2x + 1 = 0)$	αλγόριθμος του Sturm (1803-1855) 4 λύσεις	προσεγγιστικοί αλγόριθμοι $1, \approx 1,38879$ $\approx -0,3347, -1,2146$

Αλγεβρικές εξισώσεις σε μια μεταβλητή ($\mathbf{d = 1}$)

Εξίσωση	Έχει λύση αν	Η λύση είναι
$\mathbf{ax + b = 0}$ $\mathbf{(2x + 3 = 0)}$	$\mathbf{a \neq 0}$ (Ναι)	$x = -\frac{b}{a}$ $(x = -\frac{3}{2})$
$ax^2 + bx + c = 0$ $(x^2 + 3x + 1 = 0)$	$b^2 - 4ac \geq 0$ $(3^2 - 4 = 5 \geq 0, \text{Ναι})$	$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ $(x = \frac{-3 \pm \sqrt{5}}{2})$
$p(x) = 0$ $(x^6 - x^5$ $- 3x^2 + 2x + 1 = 0)$	αλγόριθμος του Sturm (1803-1855) 4 λύσεις	προσεγγιστικοί αλγόριθμοι $1, \approx 1,38879$ $\approx -0,3347, -1,2146$

Αλγεβρικές εξισώσεις σε μια μεταβλητή ($\mathbf{d = 1}$)

Εξίσωση	Έχει λύση αν	Η λύση είναι
$\mathbf{ax + b = 0}$ $\mathbf{(2x + 3 = 0)}$	$\mathbf{a \neq 0}$ (Ναι)	$\mathbf{x = -\frac{b}{a}}$ $\mathbf{(x = -\frac{3}{2})}$
$ax^2 + bx + c = 0$ $(x^2 + 3x + 1 = 0)$	$b^2 - 4ac \geq 0$ $(3^2 - 4 = 5 \geq 0, \text{Ναι})$	$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ $(x = \frac{-3 \pm \sqrt{5}}{2})$
$p(x) = 0$ $(x^6 - x^5 - 3x^2 + 2x + 1 = 0)$	αλγόριθμος του Sturm (1803-1855) 4 λύσεις	προσεγγιστικοί αλγόριθμοι $1, \approx 1,38879$ $\approx -0,3347, -1,2146$

Αλγεβρικές εξισώσεις σε μια μεταβλητή ($\mathbf{d = 1}$)

Εξίσωση	Έχει λύση αν	Η λύση είναι
$\mathbf{ax + b = 0}$ $\mathbf{(2x + 3 = 0)}$	$\mathbf{a \neq 0}$ (Ναι)	$\mathbf{x = -\frac{b}{a}}$ $\mathbf{(x = -\frac{3}{2})}$
$\mathbf{ax^2 + bx + c = 0}$ $\mathbf{(x^2 + 3x + 1 = 0)}$	$\mathbf{b^2 - 4ac \geq 0}$ $(3^2 - 4 = 5 \geq 0$, Ναι)	$\mathbf{x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}}$ $(x = \frac{-3 \pm \sqrt{5}}{2})$
$\mathbf{p(x) = 0}$ $(x^6 - x^5$ $- 3x^2 + 2x + 1 = 0)$	αλγόριθμος του Sturm (1803-1855) 4 λύσεις	προσεγγιστικοί αλγόριθμοι $\mathbf{1, \approx 1,38879}$ $\mathbf{\approx -0,3347, -1,2146}$

Αλγεβρικές εξισώσεις σε μια μεταβλητή ($\mathbf{d = 1}$)

Εξίσωση	Έχει λύση αν	Η λύση είναι
$\mathbf{ax + b = 0}$ $\mathbf{(2x + 3 = 0)}$	$\mathbf{a \neq 0}$ (Ναι)	$\mathbf{x = -\frac{b}{a}}$ $\mathbf{(x = -\frac{3}{2})}$
$\mathbf{ax^2 + bx + c = 0}$ $\mathbf{(x^2 + 3x + 1 = 0)}$	$\mathbf{b^2 - 4ac \geq 0}$ $\mathbf{(3^2 - 4 = 5 \geq 0}$, Ναι$\mathbf{)}$	$\mathbf{x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}}$ $\mathbf{(x = \frac{-3 \pm \sqrt{5}}{2})}$
$\mathbf{p(x) = 0}$ $\mathbf{(x^6 - x^5 - 3x^2 + 2x + 1 = 0)}$	αλγόριθμος του Sturm (1803-1855) 4 λύσεις	προσεγγιστικοί αλγόριθμοι $\mathbf{1, \approx 1,38879}$ $\mathbf{\approx -0,3347, -1,2146}$

Αλγεβρικές εξισώσεις σε μια μεταβλητή ($\mathbf{d = 1}$)

Εξίσωση	Έχει λύση αν	Η λύση είναι
$\mathbf{ax + b = 0}$ $\mathbf{(2x + 3 = 0)}$	$\mathbf{a \neq 0}$ (Ναι)	$\mathbf{x = -\frac{b}{a}}$ $\mathbf{(x = -\frac{3}{2})}$
$\mathbf{ax^2 + bx + c = 0}$ $\mathbf{(x^2 + 3x + 1 = 0)}$	$\mathbf{b^2 - 4ac \geq 0}$ $\mathbf{(3^2 - 4 = 5 \geq 0}$, Ναι$\mathbf{)}$	$\mathbf{x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}}$ $\mathbf{(x = \frac{-3 \pm \sqrt{5}}{2})}$
$\mathbf{p(x) = 0}$ $\mathbf{(x^6 - x^5 - 3x^2 + 2x + 1 = 0)}$	αλγόριθμος του Sturm (1803-1855) 4 λύσεις	προσεγγιστικοί αλγόριθμοι $\mathbf{1, \approx 1,38879}$ $\mathbf{\approx -0,3347, -1,2146}$

Αλγεβρικές εξισώσεις σε μια μεταβλητή ($\mathbf{d = 1}$)

Εξίσωση	Έχει λύση αν	Η λύση είναι
$ax + b = 0$ $(2x + 3 = 0)$	$a \neq 0$ (Ναι)	$x = -\frac{b}{a}$ $(x = -\frac{3}{2})$
$ax^2 + bx + c = 0$ $(x^2 + 3x + 1 = 0)$	$b^2 - 4ac \geq 0$ $(3^2 - 4 = 5 \geq 0, \text{Ναι})$	$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ $(x = \frac{-3 \pm \sqrt{5}}{2})$
$p(x) = 0$ $(x^6 - x^5$ $- 3x^2 + 2x + 1 = 0)$	αλγόριθμος του Sturm (1803-1855) 4 λύσεις	προσεγγιστικοί αλγόριθμοι $1, \approx 1,38879$ $\approx -0,3347, -1,2146$

Αλγεβρικές εξισώσεις σε μια μεταβλητή ($\mathbf{d = 1}$)

Εξίσωση	Έχει λύση αν	Η λύση είναι
$\mathbf{ax + b = 0}$ $\mathbf{(2x + 3 = 0)}$	$\mathbf{a \neq 0}$ (Ναι)	$\mathbf{x = -\frac{b}{a}}$ $\mathbf{(x = -\frac{3}{2})}$
$\mathbf{ax^2 + bx + c = 0}$ $\mathbf{(x^2 + 3x + 1 = 0)}$	$\mathbf{b^2 - 4ac \geq 0}$ $\mathbf{(3^2 - 4 = 5 \geq 0}$, Ναι$\mathbf{)}$	$\mathbf{x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}}$ $\mathbf{(x = \frac{-3 \pm \sqrt{5}}{2})}$
$\mathbf{p(x) = 0}$ $\mathbf{(x^6 - x^5}$ $\mathbf{- 3x^2 + 2x + 1 = 0)}$	αλγόριθμος του Sturm (1803-1855) **4** λύσεις	προσεγγιστικοί αλγόριθμοι $\mathbf{1, \approx 1,38879}$ $\mathbf{\approx -0,3347, -1,2146}$

Αλγεβρικές εξισώσεις σε μια μεταβλητή ($\mathbf{d = 1}$)

Εξίσωση	Έχει λύση αν	Η λύση είναι
$\mathbf{ax + b = 0}$	$\mathbf{a \neq 0}$	$\mathbf{x = -\frac{b}{a}}$
$\mathbf{(2x + 3 = 0)}$	(Ναι)	$\mathbf{(x = -\frac{3}{2})}$
$\mathbf{ax^2 + bx + c = 0}$	$\mathbf{b^2 - 4ac \geq 0}$	$\mathbf{x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}}$
$\mathbf{(x^2 + 3x + 1 = 0)}$	$\mathbf{(3^2 - 4 = 5 \geq 0}$, Ναι)	$\mathbf{(x = \frac{-3 \pm \sqrt{5}}{2})}$
$\mathbf{p(x) = 0}$	αλγόριθμος του Sturm (1803-1855)	προσεγγιστικοί αλγόριθμοι
$\mathbf{(x^6 - x^5 - 3x^2 + 2x + 1 = 0)}$	**4** λύσεις	$\mathbf{1, \approx 1,38879}$ $\mathbf{\approx -0,3347, -1,2146}$

Θεώρημα διαίρεσης πολυωνύμων

Θεώρημα

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

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

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

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

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

Θεώρημα διαίρεσης πολυωνύμων

Θεώρημα

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

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

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

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

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

Ο αλγόριθμος του Sturm, για ρητό πολυώνυμο $\mathbf{p(x)}$

- Η ακολουθία Sturm του $\mathbf{p(x)}$:

$$\boxed{\mathbf{p_0(x)}} = \mathbf{p(x)}, \quad \boxed{\mathbf{p_1(x)}} = \mathbf{p'(x)} \quad (\text{η παράγωγος του } \mathbf{p(x)})$$

$$\mathbf{p_0(x)} = \mathbf{p_1(x)q_1(x)} - \boxed{\mathbf{p_2(x)}}$$

$$\mathbf{p_1(x)} = \mathbf{p_2(x)q_2(x)} - \boxed{\mathbf{p_3(x)}}$$

$$\vdots$$

$$\mathbf{p_r(x)} = \mathbf{p_{r+1}(x)q_{r+1}(x)}$$

- $\mathbf{w(a)}$ = ο αριθμός αλλαγών προσήμου στην ακολουθία

$$(\mathbf{p_0(a)}, \mathbf{p_1(a)}, \mathbf{p_2(a)}, \ldots, \mathbf{p_{r+1}(a)})$$

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

- Ο Ευκλείδιος σε πολυώνυμα, με μια «ρυτίδα»

Ο αλγόριθμος του Sturm, για ρητό πολυώνυμο $\mathbf{p(x)}$

- Η ακολουθία Sturm του $\mathbf{p(x)}$:

$$\boxed{p_0(x)} = p(x), \quad \boxed{p_1(x)} = p'(x) \quad (\text{η παράγωγος του } p(x))$$

$$p_0(x) = p_1(x)q_1(x) - \boxed{p_2(x)}$$

$$p_1(x) = p_2(x)q_2(x) - \boxed{p_3(x)}$$

$$\vdots$$

$$p_r(x) = p_{r+1}(x)q_{r+1}(x)$$

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

Αν $p(a)p(b) \neq 0$, *τότε το* $p(x)$ *έχει* $w(a) - w(b)$ *ρίζες στο* (a, b)

- Ο Ευκλείδιος σε πολυώνυμα, με μια «ρυτίδα»

Ο αλγόριθμος του Sturm, για ρητό πολυώνυμο $\mathbf{p(x)}$

- Η ακολουθία Sturm του $\mathbf{p(x)}$:

$$\boxed{p_0(x)} = p(x), \quad \boxed{p_1(x)} = p'(x) \quad (\text{η παράγωγος του } p(x))$$

$$p_0(x) = p_1(x)q_1(x) - \boxed{p_2(x)}$$

$$p_1(x) = p_2(x)q_2(x) - \boxed{p_3(x)}$$

$$\vdots$$

$$p_r(x) = p_{r+1}(x)q_{r+1}(x)$$

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

Αν $p(a)p(b) \neq 0$, *τότε το* $p(x)$ *έχει* $w(a) - w(b)$ *ρίζες στο* (a, b)

- Ο Ευκλείδιος σε πολυώνυμα, με μια «ρυτίδα»

Ο αλγόριθμος του Sturm, για ρητό πολυώνυμο $\mathbf{p(x)}$

- Η ακολουθία Sturm του $\mathbf{p(x)}$:

$$\boxed{p_0(x)} = p(x), \quad \boxed{p_1(x)} = p'(x) \quad (\text{η παράγωγος του } p(x))$$

$$p_0(x) = p_1(x)q_1(x) - p_2(x)$$

$$p_1(x) = p_2(x)q_2(x) - p_3(x)$$

$$\vdots$$

$$p_r(x) = p_{r+1}(x)q_{r+1}(x)$$

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

Αν $p(a)p(b) \neq 0$, *τότε το* $p(x)$ *έχει* $w(a) - w(b)$ *ρίζες στο* (a, b)

- Ο Ευκλείδιος σε πολυώνυμα, με μια «ρυτίδα»

Ο αλγόριθμος του Sturm, για ρητό πολυώνυμο $\mathbf{p(x)}$

- Η ακολουθία Sturm του $\mathbf{p(x)}$:

$$\boxed{p_0(x)} = p(x), \quad \boxed{p_1(x)} = p'(x) \quad (\text{η παράγωγος του } p(x))$$

$$p_0(x) = p_1(x)q_1(x) - \boxed{p_2(x)}$$

$$p_1(x) = p_2(x)q_2(x) - \boxed{p_3(x)}$$

$$\vdots$$

$$p_r(x) = p_{r+1}(x)q_{r+1}(x)$$

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

Αν $p(a)p(b) \neq 0$, *τότε το* $p(x)$ *έχει* $w(a) - w(b)$ *ρίζες στο* (a, b)

- Ο Ευκλείδιος σε πολυώνυμα, με μια «ρυτίδα»

Ο αλγόριθμος του Sturm, για ρητό πολυώνυμο $\mathbf{p(x)}$

- Η ακολουθία Sturm του $\mathbf{p(x)}$:

$$\boxed{p_0(x)} = p(x), \quad \boxed{p_1(x)} = p'(x) \quad (\text{η παράγωγος του } p(x))$$

$$p_0(x) = p_1(x)q_1(x) - \boxed{p_2(x)}$$

$$p_1(x) = p_2(x)q_2(x) - \boxed{p_3(x)}$$

$$\vdots$$

$$p_r(x) = p_{r+1}(x)q_{r+1}(x)$$

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

Αν $p(a)p(b) \neq 0$, *τότε το* $p(x)$ *έχει* $w(a) - w(b)$ *ρίζες στο* (a, b)

- Ο Ευκλείδιος σε πολυώνυμα, με μια «ρυτίδα»

Ο αλγόριθμος του Sturm, για ρητό πολυώνυμο $\mathbf{p(x)}$

- Η ακολουθία Sturm του $\mathbf{p(x)}$:

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

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

Αν $p(a)p(b) \neq 0$, *τότε το* $p(x)$ *έχει* $w(a) - w(b)$ *ρίζες στο* (a, b)

- Ο Ευκλείδιος σε πολυώνυμα, με μια «ρυτίδα»

Ο αλγόριθμος του Sturm, για ρητό πολυώνυμο $\mathbf{p(x)}$

- Η ακολουθία Sturm του $\mathbf{p(x)}$:

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

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

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

- Ο Ευκλείδιος σε πολυώνυμα, με μια «ρυτίδα»

Ο αλγόριθμος του Sturm, για ρητό πολυώνυμο $\mathbf{p(x)}$

- Η ακολουθία Sturm του $\mathbf{p(x)}$:

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

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

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

- Ο Ευκλείδιος σε πολυώνυμα, με μια «ρυτίδα»

Ο αλγόριθμος του Sturm, για ρητό πολυώνυμο $\mathbf{p(x)}$

- Η ακολουθία Sturm του $\mathbf{p(x)}$:

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

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

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

- Ο Ευκλείδιος σε πολυώνυμα, με μια «ρυτίδα»

(3) Πρωτοβάθμια άλγεβρα: 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 $\mathbf{p(x) = 0}$ έχει 5 (πραγματικές) λύσεις»
- «Υπάρχουν αριθμοί $\vec{x} = (x_1, x_2, \ldots, x_n)$ τέτοιοι που

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

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

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

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

(3) Πρωτοβάθμια άλγεβρα: 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 $\mathbf{p(x) = 0}$ έχει 5 (πραγματικές) λύσεις»
- «Υπάρχουν αριθμοί $\vec{x} = (x_1, x_2, \ldots, x_n)$ τέτοιοι που

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

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

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

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

(3) Πρωτοβάθμια άλγεβρα: 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 $\mathbf{p(x) = 0}$ 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 $\vec{x} = (x_1, x_2, \ldots, x_n)$,

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

(3) Πρωτοβάθμια άλγεβρα: 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 $\mathbf{p(x) = 0}$ έχει 5 (πραγματικές) λύσεις»
- «Υπάρχουν αριθμοί $\vec{\mathbf{x}} = (\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_n})$ τέτοιοι που

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

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

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

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

(3) Πρωτοβάθμια άλγεβρα: 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 $\mathbf{p(x) = 0}$ έχει 5 (πραγματικές) λύσεις»
- «Υπάρχουν αριθμοί $\vec{\mathbf{x}} = (\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_n})$ τέτοιοι που

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

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

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

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

Οι απλές (πρωτοβάθμιες) προτάσεις της άλγεβρας

είναι οι γραμματικά σωστές ακολουθίες από τα εξής 16 σύμβολα:

$0\ \ 1\ \ +\ \ -\ \ \cdot\ \ =\ \ <$ (αλγεβρικές πράξεις)

$\neg$ (όχι) $\ \&$ (και) $\ \vee$ (ή) (προτασιακοί τελεστές)

$\exists$ (υπάρχει) $\ \forall$ (για κάθε) (ποσοδείκτες)

$(\ )$ (σημεία στίξεως)

$\mathrm{x}\ |$ (μεταβλητές $\mathrm{x}|\ \ \mathrm{x}||\ \ \mathrm{x}|||\ \ \ldots$)

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

- Οι μεταβλητές ερμηνεύονται με πραγματικούς αριθμούς στο

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

Οι απλές (πρωτοβάθμιες) προτάσεις της άλγεβρας

είναι οι γραμματικά σωστές ακολουθίες από τα εξής 16 σύμβολα:

$\mathbf{0}$ $\mathbf{1}$ $+$ $-$ $\cdot$ $=$ $<$ (αλγεβρικές πράξεις)

$\neg$ (όχι) $\&$ (και) $\vee$ (ή) (προτασιακοί τελεστές)

$\exists$ (υπάρχει) $\forall$ (για κάθε) (ποσοδείκτες)

( ) (σημεία στίξεως)

x | (μεταβλητές x| x|| x||| ...)

- 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

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

Οι απλές (πρωτοβάθμιες) προτάσεις της άλγεβρας

είναι οι γραμματικά σωστές ακολουθίες από τα εξής 16 σύμβολα:

$\mathbf{0}$ $\mathbf{1}$ $+$ $-$ $\cdot$ $=$ $<$ (αλγεβρικές πράξεις)

$\neg$ (όχι) $\&$ (και) $\vee$ (ή) (προτασιακοί τελεστές)

$\exists$ (υπάρχει) $\forall$ (για κάθε) (ποσοδείκτες)

( ) (σημεία στίξεως)

x | (μεταβλητές x| x|| x||| ...)

- 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

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

Οι απλές (πρωτοβάθμιες) προτάσεις της άλγεβρας

είναι οι γραμματικά σωστές ακολουθίες από τα εξής 16 σύμβολα:

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

- 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

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

Οι απλές (πρωτοβάθμιες) προτάσεις της άλγεβρας

είναι οι γραμματικά σωστές ακολουθίες από τα εξής 16 σύμβολα:

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

- 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

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

Οι απλές (πρωτοβάθμιες) προτάσεις της άλγεβρας

είναι οι γραμματικά σωστές ακολουθίες από τα εξής 16 σύμβολα:

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

- 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

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

Οι απλές (πρωτοβάθμιες) προτάσεις της άλγεβρας

είναι οι γραμματικά σωστές ακολουθίες από τα εξής 16 σύμβολα:

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

- 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

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

Οι απλές (πρωτοβάθμιες) προτάσεις της άλγεβρας

είναι οι γραμματικά σωστές ακολουθίες από τα εξής 16 σύμβολα:

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

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

- Οι μεταβλητές ερμηνεύονται με πραγματικούς αριθμούς στο

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

Οι απλές (πρωτοβάθμιες) προτάσεις της άλγεβρας

είναι οι γραμματικά σωστές ακολουθίες από τα εξής 16 σύμβολα:

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

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

- Οι μεταβλητές ερμηνεύονται με πραγματικούς αριθμούς στο

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

Οι απλές (πρωτοβάθμιες) προτάσεις της άλγεβρας

είναι οι γραμματικά σωστές ακολουθίες από τα εξής 16 σύμβολα:

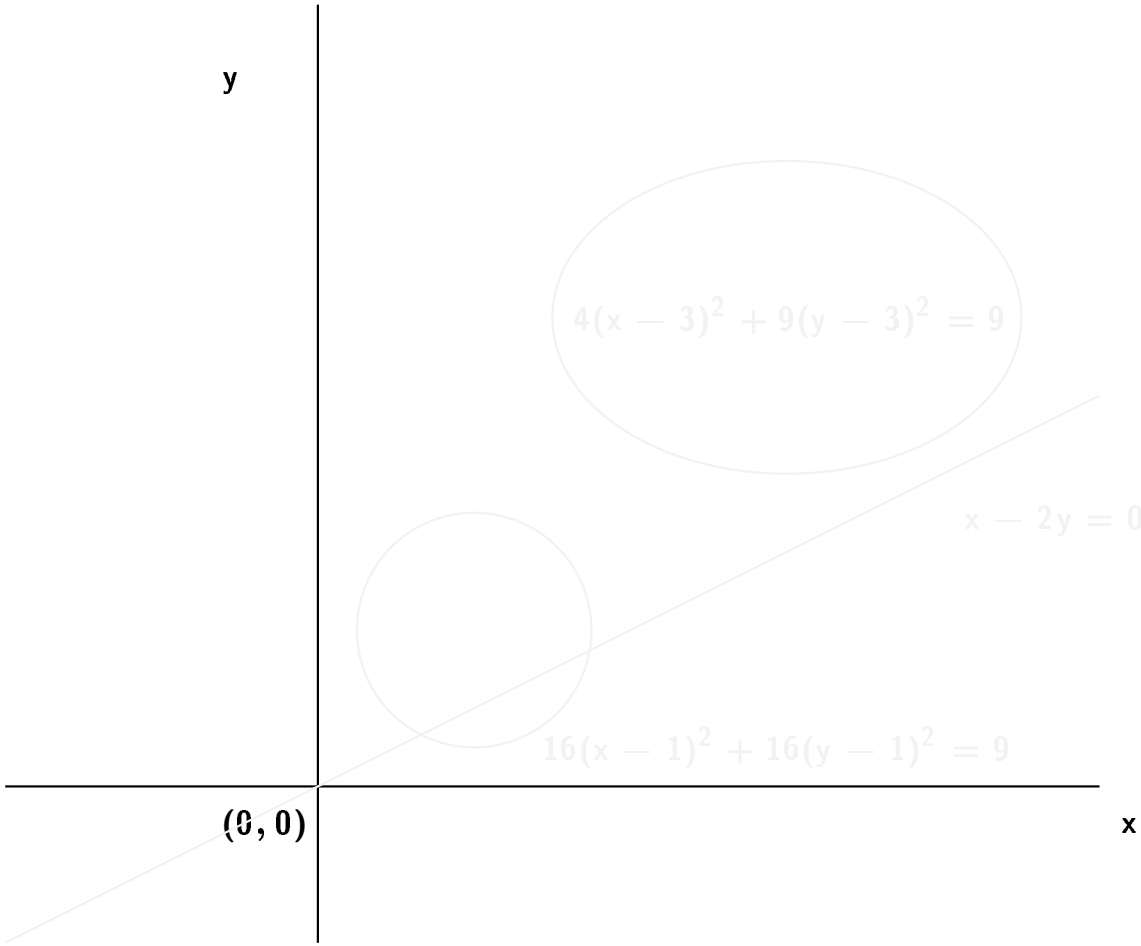
$\mathbf{0}\ \mathbf{1}\ +\ -\ \cdot\ =\ <$	(αλγεβρικές πράξεις)
$\neg$ (όχι) $\&$ (και) $\vee$ (ή)	(προτασιακοί τελεστές)
$\exists$ (υπάρχει) $\forall$ (για κάθε)	(ποσοδείκτες)
$(\ )$	(σημεία στίξεως)
$\mathbf{x}\ \vert$	(μεταβλητές $\mathbf{x}\vert\ \mathbf{x}\vert\vert\ \mathbf{x}\vert\vert\vert\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

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

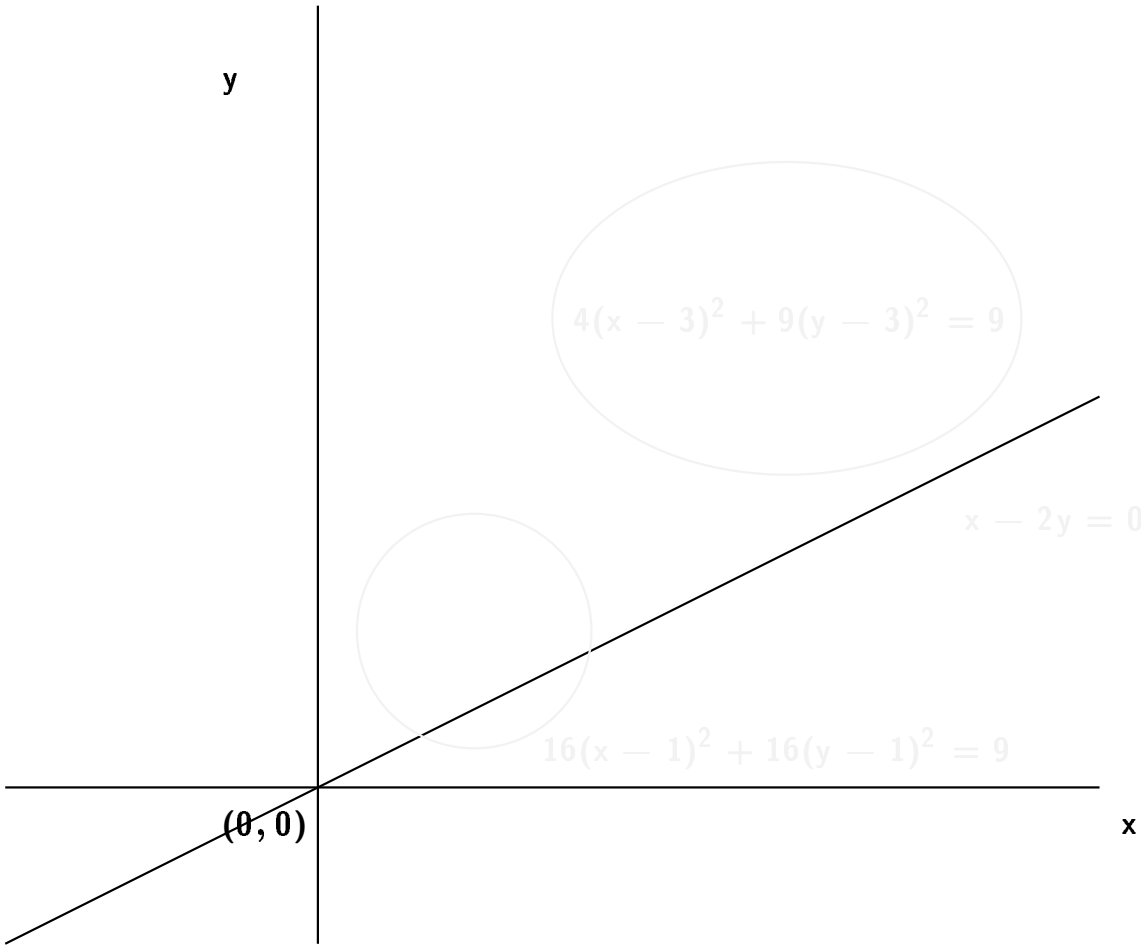
- Οι μεταβλητές ερμηνεύονται με πραγματικούς αριθμούς στο

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

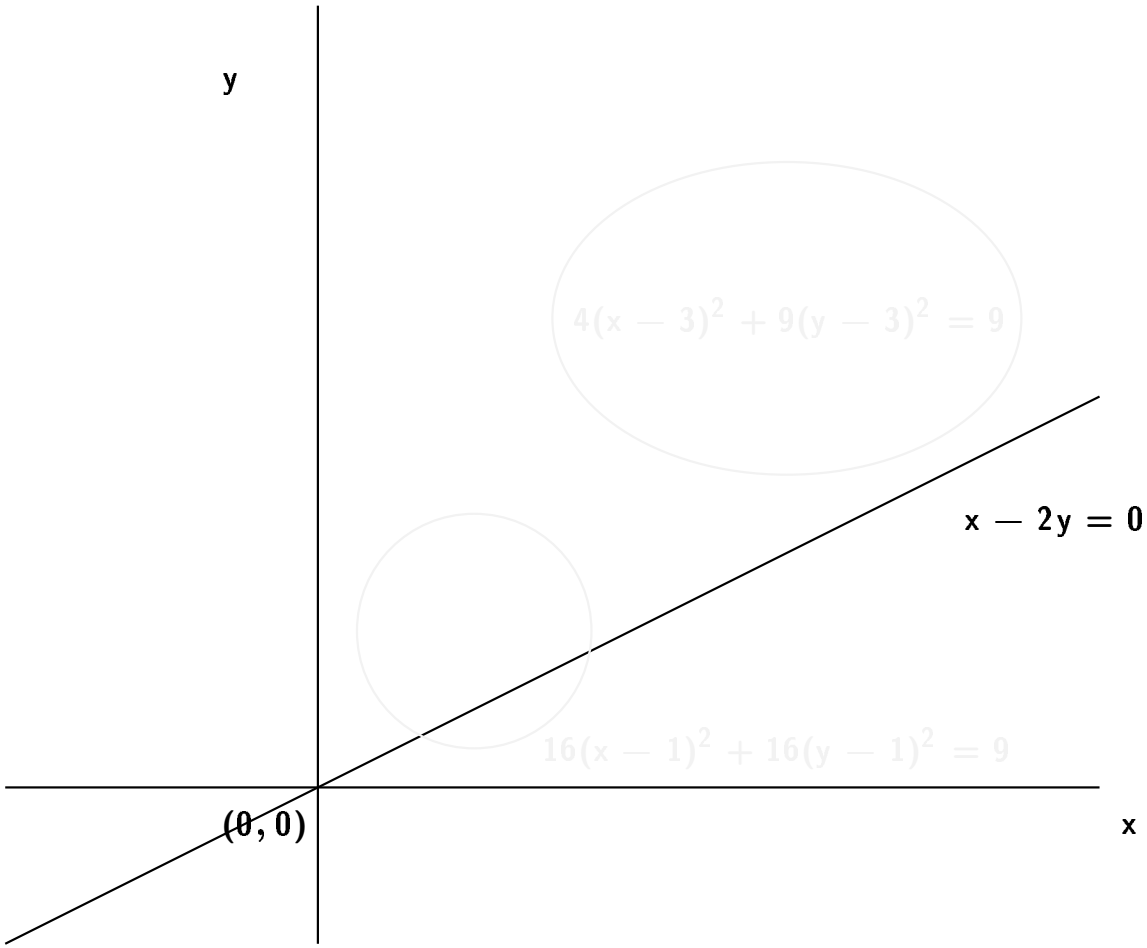
Αναλυτική γεωμετρία



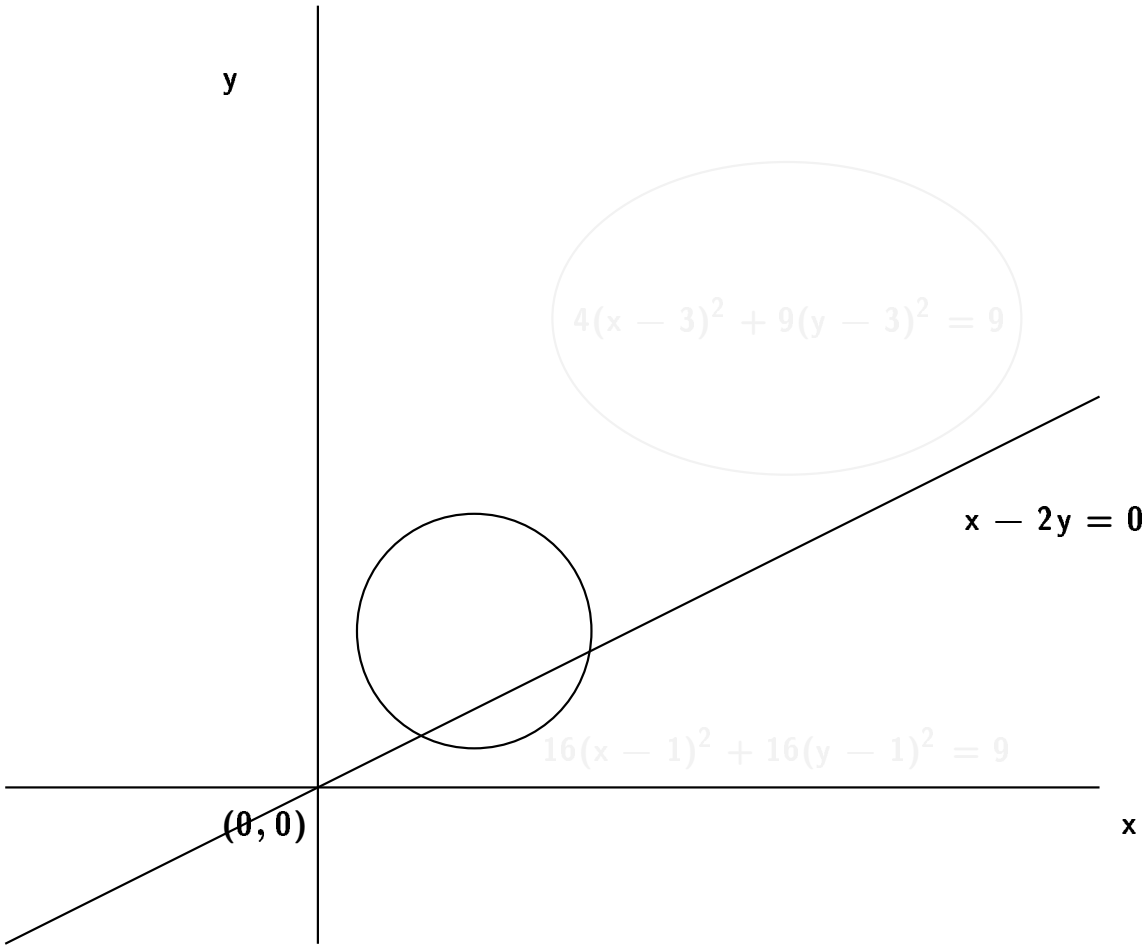
Αναλυτική γεωμετρία



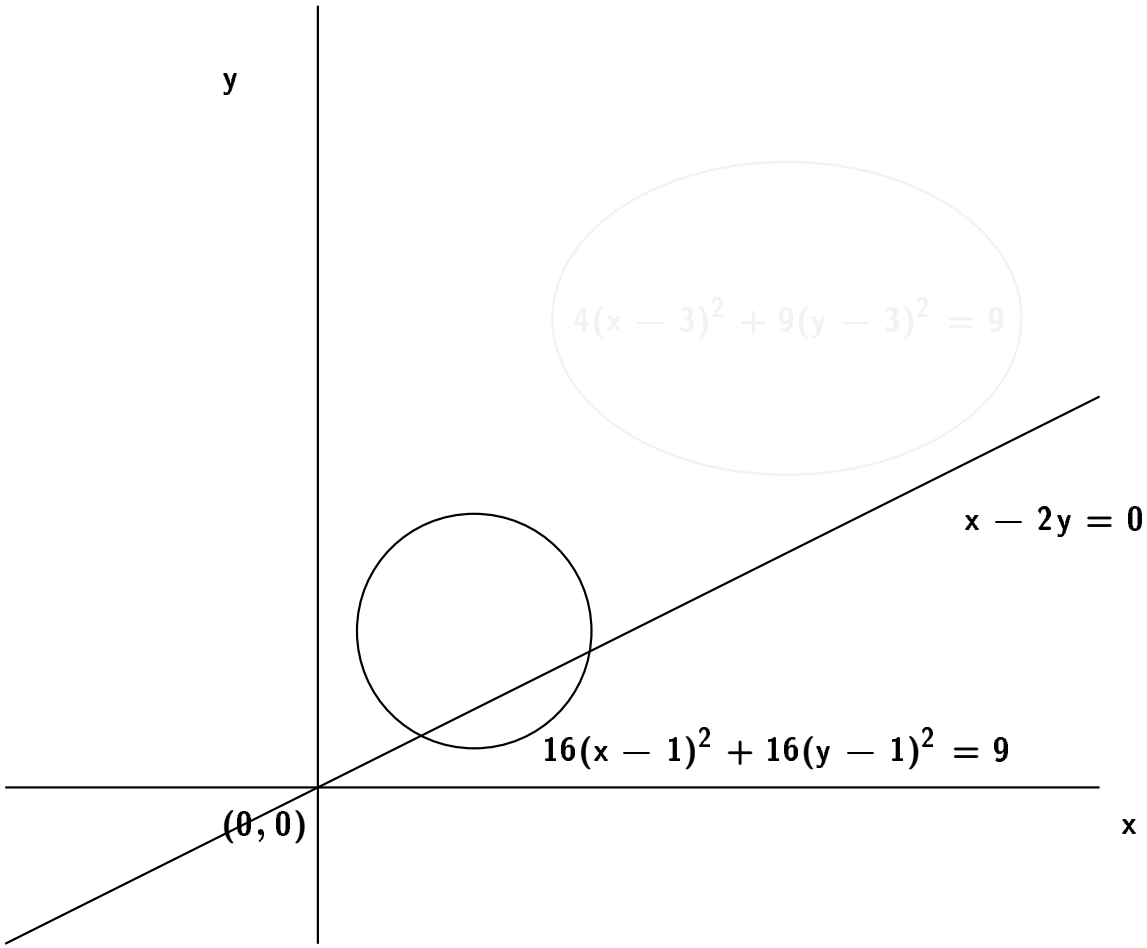
Αναλυτική γεωμετρία



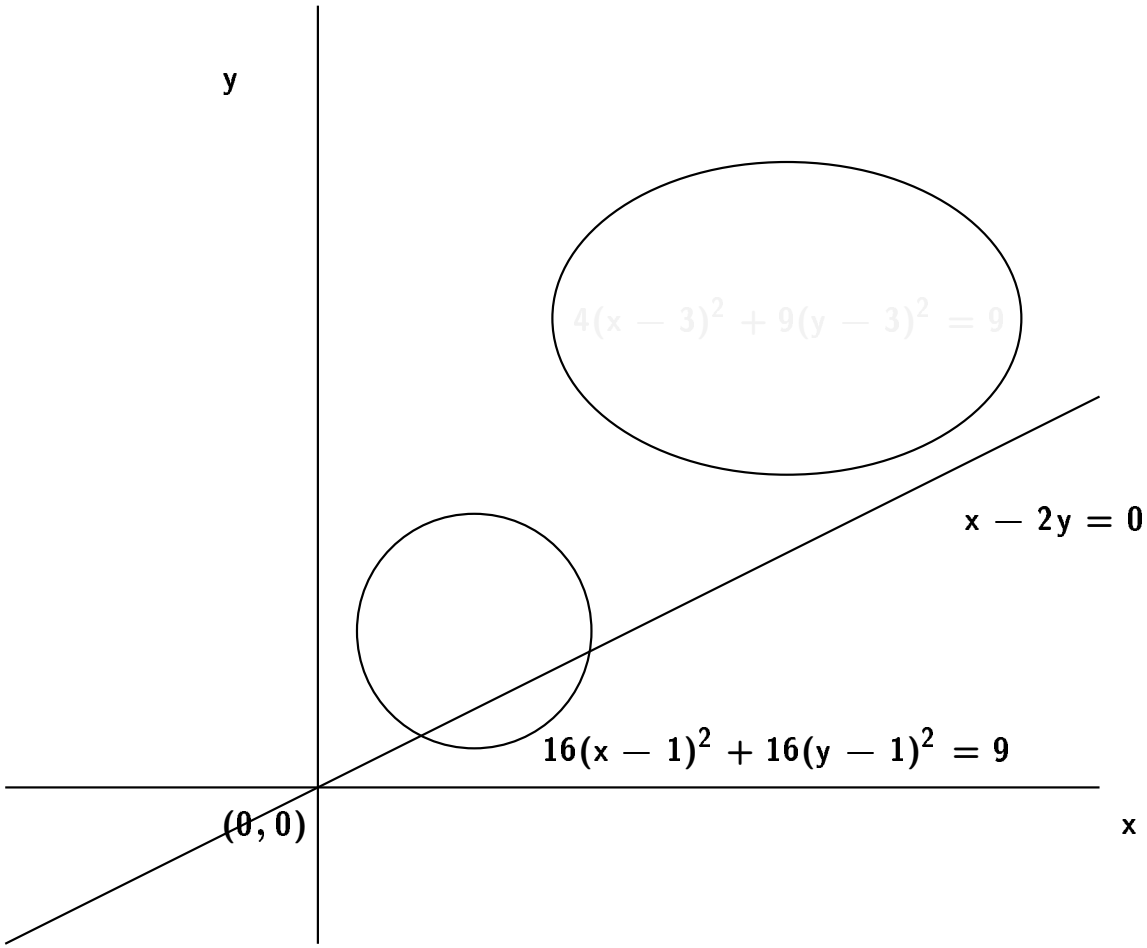
Αναλυτική γεωμετρία



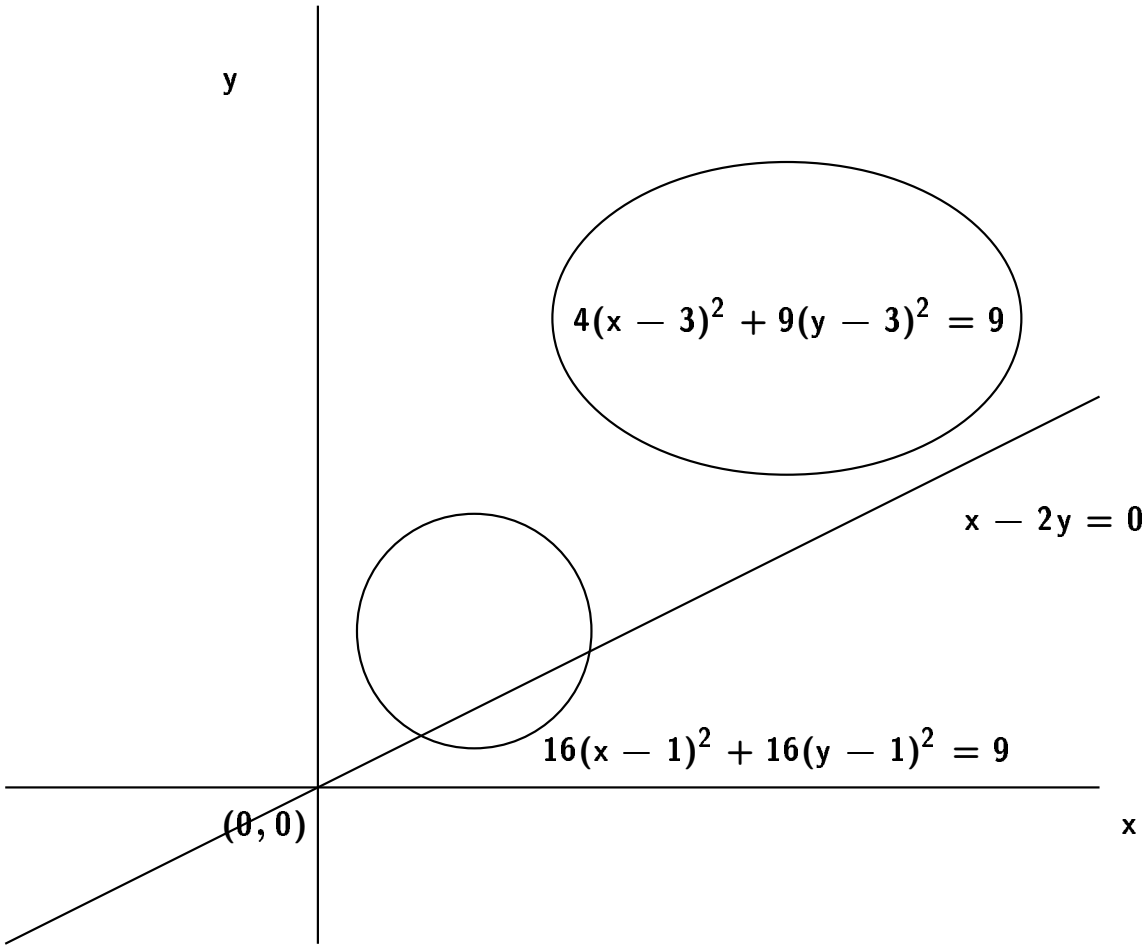
Αναλυτική γεωμετρία



Αναλυτική γεωμετρία



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

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

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

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

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

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

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

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

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

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

(4) Πρωτοβάθμια αριθμητική

Οι απλές (πρωτοβάθμιες) προτάσεις της αριθμητικής είναι οι γραμματικά σωστές ακολουθίες από τα 16 σύμβολα:

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

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 $x = -2$

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 $x = -2$

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 $x = -2$

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 $x = -2$

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 $x = -2$

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 $x = -2$

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 $\mathbf{x^n + y^n = z^n}$ δεν έχει ακέραιες, θετικές λύσεις για $\mathbf{n > 2}$

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

Η αριθμητική είναι πιο δύσκολη από την άλγεβρα!

Θεώρημα (Andrew Wiles, 1994)

Η εξίσωση $\mathbf{x^n + y^n = z^n}$ δεν έχει ακέραιες, θετικές λύσεις για $\mathbf{n > 2}$

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

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

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

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

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

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

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 $\mathbf{p(x_1, \ldots, x_n)}$ με ακέραιους συντελεστές η εξίσωση

$$\mathbf{p(x_1, \ldots, x_n) = 0}$$

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*»

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 $\mathbf{p(x_1, \ldots, x_n)}$ με ακέραιους συντελεστές η εξίσωση

$$\mathbf{p(x_1, \ldots, x_n) = 0}$$

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*»

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 $\mathbf{p(x_1, \ldots, x_n)}$ με ακέραιους συντελεστές η εξίσωση

$$\mathbf{p(x_1, \ldots, x_n) = 0}$$

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*»

(5) Ανεπίλυτα προβλήματα: πως δείχνουμε ότι υπάρχουν;

Το Αίτημα Church-Turing (1936)

Αν μια συνάρτηση $\mathbf{f}(\alpha)$ στις λέξεις από ένα πεπερασμένο αλφάβητο $\mathbf{\Sigma}$ υπολογίζεται από κάποιον αλγόριθμο, τότε η $\mathbf{f}(\alpha)$ 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 $\mathbf{f}(\alpha)$ 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»

(5) Ανεπίλυτα προβλήματα: πως δείχνουμε ότι υπάρχουν;

Το Αίτημα Church-Turing (1936)

Αν μια συνάρτηση $\mathbf{f}(\alpha)$ στις λέξεις από ένα πεπερασμένο αλφάβητο $\mathbf{\Sigma}$ υπολογίζεται από κάποιον αλγόριθμο, τότε η $\mathbf{f}(\alpha)$ 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 $\mathbf{f}(\alpha)$ 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»

(5) Ανεπίλυτα προβλήματα: πως δείχνουμε ότι υπάρχουν;

Το Αίτημα Church-Turing (1936)

Αν μια συνάρτηση $\mathbf{f}(\alpha)$ στις λέξεις από ένα πεπερασμένο αλφάβητο $\mathbf{\Sigma}$ υπολογίζεται από κάποιον αλγόριθμο, τότε η $\mathbf{f}(\alpha)$ 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 $\mathbf{f}(\alpha)$ 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»

(5) Ανεπίλυτα προβλήματα: πως δείχνουμε ότι υπάρχουν;

Το Αίτημα Church-Turing (1936)

Αν μια συνάρτηση $\mathbf{f}(\alpha)$ στις λέξεις από ένα πεπερασμένο αλφάβητο $\mathbf{\Sigma}$ υπολογίζεται από κάποιον αλγόριθμο, τότε η $\mathbf{f}(\alpha)$ 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 $\mathbf{f}(\alpha)$ 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»

(5) Ανεπίλυτα προβλήματα: πως δείχνουμε ότι υπάρχουν;

Το Αίτημα Church-Turing (1936)

Αν μια συνάρτηση $\mathbf{f}(\alpha)$ στις λέξεις από ένα πεπερασμένο αλφάβητο $\mathbf{\Sigma}$ υπολογίζεται από κάποιον αλγόριθμο, τότε η $\mathbf{f}(\alpha)$ 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 $\mathbf{f}(\alpha)$ 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»

(5) Ανεπίλυτα προβλήματα: πως δείχνουμε ότι υπάρχουν;

Το Αίτημα Church-Turing (1936)

Αν μια συνάρτηση $\mathbf{f}(\alpha)$ στις λέξεις από ένα πεπερασμένο αλφάβητο $\mathbf{\Sigma}$ υπολογίζεται από κάποιον αλγόριθμο, τότε η $\mathbf{f}(\alpha)$ 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 $\mathbf{f}(\alpha)$ 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»

(5) Ανεπίλυτα προβλήματα: πως δείχνουμε ότι υπάρχουν;

Το Αίτημα Church-Turing (1936)

Αν μια συνάρτηση $\mathbf{f}(\alpha)$ στις λέξεις από ένα πεπερασμένο αλφάβητο $\mathbf{\Sigma}$ υπολογίζεται από κάποιον αλγόριθμο, τότε η $\mathbf{f}(\alpha)$ 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 $\mathbf{f}(\alpha)$ 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»

(6) 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!

(6) Δισεπίλυτα προβλήματα: παραγοντοποίηση

- *Κάθε ακέραιος* $\mathbf{x} > \mathbf{1}$ *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!

(6) 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!

(6) Δισεπίλυτα προβλήματα: παραγοντοποίηση

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

$$20 = 2 \cdot 2 \cdot 5$$

$$1817 = 23 \cdot 79$$

$$60915799 = 7 \cdot 23 \cdot 71 \cdot 73 \cdot 73$$

$$9984204641 = 99961 \cdot 99881$$

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

(6) 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!

(6) Δισεπίλυτα προβλήματα: παραγοντοποίηση

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

$$20 = 2 \cdot 2 \cdot 5$$
$$1817 = 23 \cdot 79$$
$$60915799 = 7 \cdot 23 \cdot 71 \cdot 73 \cdot 73$$
$$9984204641 = 99961 \cdot 99881$$

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

(6) 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!

(6) 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!

(6) 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!

(6) 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!

(6) Δισεπίλυτα προβλήματα: παραγοντοποίηση

- *Κάθε ακέραιος* $\mathbf{x > 1}$ *είναι γινόμενο πρώτων αριθμών*

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

- 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

Υπολογιστική πολυπλοκότητα

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

αριθμός $= \mathbf{x}$	μήκος $= \mathbf{n}$
1817	**4**
60915799	**8**
9984204641	**10**

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

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

Υπολογιστική πολυπλοκότητα

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

αριθμός $= \mathbf{x}$	μήκος $= \mathbf{n}$
1817	**4**
60915799	**8**
9984204641	**10**

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

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

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 $n = 20, d = 12$ $\quad 20^{12} = 4.096.000.000.000.000$

$10^{20} = 100.000.000.000.000.000.000$

Θεώρημα: $P \neq NP$;

Κάθε αλγόριθμος που γνωρίζουμε για το SAT είναι

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 $n = 20, d = 12$ $\quad 20^{12} = 4.096.000.000.000.000$

$10^{20} = 100.000.000.000.000.000.000$

Εικασία $P \neq NP$:

Κάθε αλγόριθμος παραγοντοποίησης είναι εκθετικός

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 $n = 20, d = 12$ $\quad 20^{12} = 4.096.000.000.000.000$

$10^{20} = 100.000.000.000.000.000.000$

Εικασία $P \neq NP$:

Κάθε αλγόριθμος παραγοντοποίησης είναι εκθετικός

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 $n = 20, d = 12$ $\quad 20^{12} = 4.096.000.000.000.000$

$10^{20} = 100.000.000.000.000.000.000$

Εικασία $P \neq NP$:

Κάθε αλγόριθμος παραγοντοποίησης είναι εκθετικός

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 $n = 20, d = 12$ $20^{12} = 4.096.000.000.000.000$

$10^{20} = 100.000.000.000.000.000.000$

Εικασία $P \neq NP$:

Κάθε αλγόριθμος παραγοντοποίησης είναι εκθετικός

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 $n = 20, d = 12$ $\quad 20^{12} = 4.096.000.000.000.000$

$\quad 10^{20} = 100.000.000.000.000.000.000$

Εικασία $P \neq NP$:

Κάθε αλγόριθμος παραγοντοποίησης είναι εκθετικός

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 $n = 20, d = 12$ $\quad 20^{12} = 4.096.000.000.000.000$

$\quad 10^{20} = 100.000.000.000.000.000.000$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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