# Μαθηματικά Πληροφορικής

2ο Μάθημα

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Αθηνών



## Είδη αποδείξεων

- Εξαντλητική μέθοδος ή μέθοδος επισκόπησης. Όταν το πρόβλημα έχει πεπερασμένο αριθμό περιπτώσεων, τις εξετάζουμε όλες.
- Μαθηματική επαγωγή. Έστω μια πρόταση $P(n)$ που ισχύει για $n = 1$. Αν η $P(n)$ συνεπάγεται την $P(n+1)$, τότε η πρόταση ισχύει για όλους τους φυσικούς.
- Δομική επαγωγή. Επαγωγή όχι στους φυσικούς αριθμούς αλλά σε μια δομή που ορίζεται επαγωγικά.



## Μορφές αποδείξεων (συνέχεια)

- Κατασκευαστική απόδειξη ύπαρξης. Δείχνουμε την ύπαρξη ενός στοιχείου δίνοντας έναν αλγόριθμο που το παράγει. Στην ίδια κατηγορία ανήκει και η απόδειξη με αντιπαράδειγμα.
- Μη κατασκευαστική απόδειξη ύπαρξης. Τέτοιες αποδείξεις χρησιμοποιούν μεταξύ άλλων
  - την αρχή του περιστερεώνα και τις γενικεύσεις του
  - την πιθανοτική μέθοδο που βασίζεται στο ότι ένα στοιχείο υπάρχει όταν έχει μη μηδενική πιθανότητα ύπαρξης.
  - τη διαγωνιοποίηση του Cantor.



## Εξαντλητική μέθοδος

- Αν η απόδειξη σπάει σε πεπερασμένο (και σχετικά μικρό) αριθμό περιπτώσεων μπορούμε να τις ελέγξουμε όλες.
- Με ισχυρούς υπολογιστές, η μέθοδος μπορεί να έχει κάποια χρησιμότητα.
- Τί σημαίνει «όλες οι περιπτώσεις»; Υπάρχουν εξαντλητικοί αλγόριθμοι που είναι καλύτεροι από άλλους.

## Το Πρόβλημα του Πορτιέρη

Το Προβλημα τοτ Πορτιερη
Σε μια μικρή πόλη $n$ άτομα πηγαίνουν σε ένα μπαρ. Για κάθε ζευγάρι ατόμων γνωρίζουμε αν θα τσακωθούν. Μπορούμε απαγορεύοντας την είσοδο σε $k \leq n$ άτομα να εγγυηθούμε ότι δεν θα ξεσπάσει καυγάς;

Γράφημα $G$ με σύνολο κορυφών $V$ και σύνολο ακμών $E$ είναι ένα ζεύγος $(V, E)$ όπου $E \subseteq \{\{u, v\} \mid u, v \in V\}$ δηλαδή μια ακμή είναι ένα μη διατεταγμένο ζεύγος κορυφών.

Εισοδος του Προβλήματος του Πορτιέρη: γράφημα $G = (V, E)$ με $n$ κορυφές, παράμετρος $k \leq n$. *Η ακμή $\{u, v\} \in E$ σημαίνει ότι οι $u$ και $v$ θα καυγαδίσουν.*
Ερωτημα: Μπορούμε να καλύψουμε όλες τις ακμές διαλέγοντας $k$ κορυφές του γραφήματος;

Αποδείξεις

## Το Πρόβλημα του Πορτιέρη

Εισοδος: ένα γράφημα $G = (V, E)$ με $n$ κορυφές, παράμετρος $k \leq n$.
Ερωτημα: Μπορούμε να καλύψουμε όλες τις ακμές διαλέγοντας $k$ κορυφές του γραφήματος;

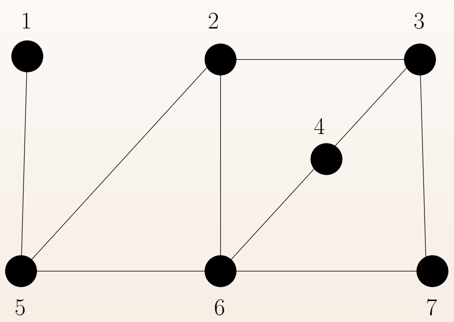
Ισοδύναμα: ρωτάμε αν το $G$ έχει κάλυμμα κορυφών μεγέθους το πολύ $k$.

Κάλυμμα κορυφών είναι ένα σύνολο $V' \subseteq V$ έτσι ώστε για κάθε ακμή $\{u, v\} \in E$ τουλάχιστον ένα από τα $u$, $v$ ανήκει στο $V'$.

Το Πρόβλημα του Πορτιέρη είναι γνωστό ως το Πρόβλημα της Εύρεσης Καλύμματος Κορυφών (Vertex Cover).

Αποδείξεις

## Παράδειγμα

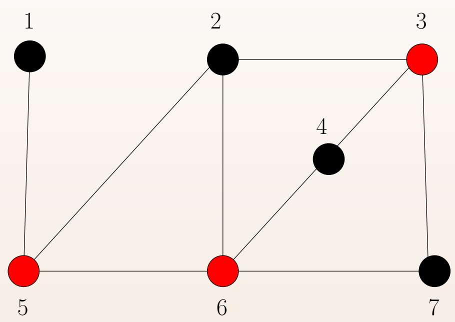



$n = 7$, $k = 3$.

Ο 1 τσακώνεται μόνο με τον 5.
Ο 5 με τους 1, 2 και 6.

Αποδείξεις

## Παράδειγμα




$n = 7$, $k = 3$.

Οι κορυφές $5, 6, 3$ καλύπτουν (αγγίζουν) όλες τις ακμές.
Για $k = 2$ δεν υπάρχει λύση.

## Πρώτος αλγόριθμος

Απαρίθμησε όλα τα δυνατά $k$-υποσύνολα των $n$ κορυφών και εξέτασε για το καθένα αν είναι κάλυμμα κορυφών.

♠ Συνολικά $\binom{n}{k}$ περιπτώσεις.

Αποδεικνύεται εύκολα ότι

$$(\frac{n}{k})^k \leq \binom{n}{k} \leq (\frac{en}{k})^k.$$

▷ Για $n = 1000,\ k = 10,\ \binom{1000}{10} \approx 2.63 \cdot 10^{23}$.

Αποδείξεις

## Δεύτερος αλγόριθμος

1. Κάθε κορυφή $v$ που τσακώνεται (συνδέεται με ακμή) με τουλάχιστον $k+1$ άλλους πρέπει να αποβληθεί (γιατί;). Σβήσε τη $v$ από το $G$ (μαζί με τις ακμές που προσπίπτουν στη $v$.)

2. Όσοι απομένουν τσακώνονται το πολύ με $k$. Διώχνοντας έναν, αποφεύγουμε το πολύ $k$ καυγάδες. Αν ο αριθμός των καυγάδων (ακμών) που απομένουν είναι πάνω από $k^2$ δεν υπάρχει λύση, ο αλγόριθμος τερματίζει.

3. Αφού το πολύ $k^2$ ακμές είναι ακάλυπτες, το πολύ $2k^2$ άτομα είναι υποψήφια για αποβολή. Δοκιμάζουμε όλες τις δυνατές περιπτώσεις, το πολύ $\binom{2k^2}{k}$.

▷ Για $k = 10,\ \binom{200}{10} \approx 2.24 \cdot 10^{16}$.

♠ Πετύχαμε πλήθος περιπτώσεων ανεξάρτητο του $n$.

Αποδείξεις

## Τρίτος (αναδρομικός) αλγόριθμος

```
function VC_Rec(G, k)

  if (E(G) ≠ ∅ and k = 0)
     return "failure"     // cannot cover the edges
  if (E(G) = ∅)
      return "success"   // all edges have been covered

  // E(G) ≠ ∅ and k > 0
  Pick  uv ∈ E(G) // One of u, v must be in the cover.
  if  (VC_Rec(G \ u, k − 1)= "success")
       return "success"
  else return VC_Rec(G \ v, k − 1)
```

▶ $E(G)$: σύνολο ακμών του γραφήματος $G$.
▶ $G \setminus v$: γράφημα που προκύπτει από το $G$ σβήνοντας την κορυφή $v$ (και όλες τις ακμές που προσπίπτουν στη $v$).

Αποδείξεις

## Πολυπλοκότητα του Αλγορίθμου VC_Rec

Η ρουτίνα $\text{VC\_Rec}(G,\ k)$ εκτελεί το πολύ δύο αναδρομικές κλήσεις, και σε κάθε μία η παράμετρος $k$ μειώνεται κατά 1.

Όταν το $k$ φτάσει στο 0, ο αλγόριθμος απλά ελέγχει αν υπάρχουν ακόμα ακμές και τερματίζει.

♠ Ο συνολικός αριθμός των αναδρομικών κλήσεων είναι το πολύ $2^k$.

Κάθε κλήση μπορεί να υλοποιηθεί σε γραμμικό χρόνο.

▷ Για $k = 10,\ 2^{10} = 1024$.

♢ Υπάρχει $o(2^k)$-αλγόριθμος; Μπορεί να δειχθεί ότι το Πρόβλημα του Καλύμματος Κορυφών είναι NP-complete.

## Όρια της εξαντλητικής μεθόδου

- Έστω πως απαριθμούμε $2^k$ περιπτώσεις.

• Ένα «σύγχρονο» λαπτοπ εκτελεί $\approx 2^{30}$ εντολές γλώσσας μηχανής/ δευτερόλεπτο.
∘ Ας υποθέσουμε, πολύ γενναιόδωρα, ότι σε ένα δευτερόλεπτο μπορούμε να απαριθμήσουμε και να ελέγξουμε $2^k$ περιπτώσεις για $k = 30$.
∘ Μία ώρα $= 3600 < 2^{12}$ δευτερόλεπτα, $\sim 2^{42}$ εντολές / ώρα.

♢ Ο ρυθμός αύξησης είναι τεράστιος. (Συνδυαστική Έκρηξη).
Για $k = 48$, θα χρειαζόμασταν 3 μέρες.

• Για $k = 100$, $2^{100} = 2^{30}2^{70}$,
άρα χρειαζόμαστε $2^{70}$ δευτερόλεπτα, δηλαδή $> 2^{58}$ ώρες.
∘ Ένας χρόνος έχει $8760 \approx 2^{13}$ ώρες.
∘ Άρα $\sim 2^{58-13} = 2^{45}$ χρόνια. Αυτό είναι παραπάνω από 30 τρισεκατομμύρια χρόνια...



## Μα, οι υπολογιστές δεν γίνονται ολοένα ταχύτεροι;

Ποτέ δεν θα γίνουν αρκετά γρήγοροι για να ελέγξουν $2^{100}$ περιπτώσεις σε λογικό χρόνο.

Αν η ταχύτητα διπλασιαστεί σε $2(2^{30}) = 2^{31}$ εντολές/δευτ., πηγαίνεις από το $k = 30$ στο $k + 1 = 31$. (Αγνοώντας το κόστος για προσπέλαση στη μνήμη και το δίσκο).

Και πρέπει να περιμένεις περίπου 18 μήνες (αν ισχύει ακόμα ο Νόμος του Moore!) για να συμβεί αυτό. Σε 18 χρόνια από σήμερα, ίσως μπορέσουμε να απαριθμήσουμε $2^{42+12} = 2^{54}$ περιπτώσεις σε μία ώρα.



## Μα, οι υπολογιστές δεν γίνονται ολοένα ταχύτεροι;

Οι νόμοι της φυσικής υποδεικνύουν ότι η ταχύτητα των ηλεκτρονικών υπολογιστών δεν θα αυξάνεται για πάντα. Ακόμα και με μαζικό παραλληλισμό, με τεράστιο speedup π.χ., $1000 \approx 2^{10}$, οι βελτιώσεις θα είναι ελάχιστες.

Για $k$ λίγο παραπάνω από $100$, δεν υπάρχει ελπίδα. $2^{250} \approx 10^{80}$ που είναι ο αριθμός των σωματιδίων στο σύμπαν εντός της εμβέλειας παρατήρησης μας.

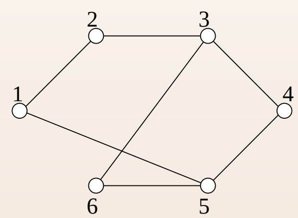
*Χρειάζονται καλύτεροι αλγόριθμοι...*



## Αριθμοί Ramsey

**Πρόταση 1**

*Σε κάθε ομάδα 6 ατόμων*
- *υπάρχουν 3 που γνωρίζονται ανά δυο*
- *ή υπάρχουν 3 που είναι άγνωστοι ανά δυο.*




**Απόδειξη.**

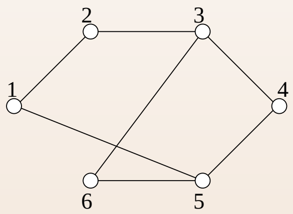
Δοκίμασε όλες τις περιπτώσεις. Πόσες είναι; □

## Αριθμοί Ramsey

**Πρόταση 2**

*Σε κάθε ομάδα 6 ατόμων*

- *υπάρχουν 3 που γνωρίζονται ανά δυο*
- *ή υπάρχουν 3 που είναι άγνωστοι ανά δυο.*




- Το παραπάνω δεν ισχύει για κάθε ομάδα 5 ατόμων. Αντιπαράδειγμα: Οι πέντε κάθονται σε ένα κυκλικό τραπέζι και ο καθένας γνωρίζει μόνο τους διπλανούς του.

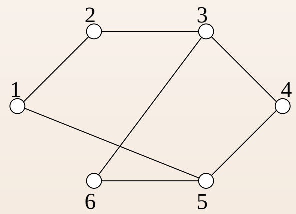


## Αριθμοί Ramsey

**Πρόταση 3**

*Σε κάθε ομάδα 6 ατόμων*

- *υπάρχουν 3 που γνωρίζονται ανά δυο*
- *ή υπάρχουν 3 που είναι άγνωστοι ανά δυο.*




- Το παραπάνω δεν ισχύει για κάθε ομάδα 5 ατόμων. Αντιπαράδειγμα: Οι πέντε κάθονται σε ένα κυκλικό τραπέζι και ο καθένας γνωρίζει μόνο τους διπλανούς του.

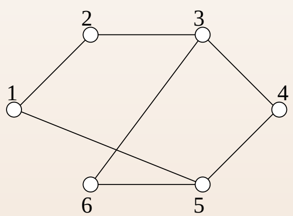


## Αριθμοί Ramsey

**Πρόταση 4**

*Σε κάθε ομάδα 6 ατόμων*

- *υπάρχουν 3 που γνωρίζονται ανά δυο*
- *ή υπάρχουν 3 που είναι άγνωστοι ανά δυο.*




- Το παραπάνω δεν ισχύει για ομάδες των 5 ατόμων. Αντιπαράδειγμα: Οι πέντε κάθονται σε ένα κυκλικό τραπέζι και ο καθένας γνωρίζει μόνο τους διπλανούς του.



## Αριθμοί Ramsey

Μπορούμε να γενικεύσουμε την πρόταση

**Θεώρημα 1**

*Σε καθε σύνολο 18 ατόμων υπάρχουν 4 που γνωρίζονται ανά δυο ή υπάρχουν 4 που είναι άγνωστοι ανά δυο.*

**Απόδειξη.**

Δοκίμασε όλες τις περιπτώσεις. Όμως τώρα οι περιπτώσεις είναι πάρα πολλές. □

## Αριθμοί Ramsey

**Θεώρημα 2**

*Σε κάθε σύνολο 49 ατόμων υπάρχουν 5 που γνωρίζονται ανά δυο ή υπάρχουν 5 που είναι άγνωστοι ανά δυο.*

**Απόδειξη.**

Η εξαντλητική μέθοδος δεν μπορεί να χρησιμοποιηθεί γιατί σήμερα είναι υπολογιστικά ανέφικτη. □



## Μαθηματική επαγωγή

Έστω $P(n)$ μια υπόθεση που αφορά τους φυσικούς αριθμούς. Για να αποδείξουμε την υπόθεση με επαγωγή

- Δείχνουμε ότι ισχύει για $n = 1$: $P(1)$
- Δείχνουμε για κάθε $n$: αν ισχύει για $n$ τότε θα ισχύει για $n + 1$:
$$P(n) \Rightarrow P(n+1)$$



## Παράδειγμα - $H_k$

- Ο αρμονικός αριθμός $H_k$ ορίζεται σαν
$$H_k = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k}$$
- Τι μεγέθους είναι ο $H_k$;



## Παράδειγμα - $H_k$

**Λήμμα 1**

*Να δειχτεί ότι για κάθε φυσικό $n$: $H_{2^n} \leq 1 + n$.*

**Απόδειξη.**

Βάση της επαγωγής: Για $n = 1$ έχουμε $H_{2^1} = H_2 = 3/2$ και $1 + n = 2$ και επομένως το λήμμα ισχύει: $3/2 \leq 2$.
Επαγωγική υπόθεση: Υποθέτουμε ότι το λήμμα ισχύει για κάποιο φυσικό αριθμό $n$: $H_{2^n} \leq 1 + n$.
Επαγωγικό βήμα: Θα δείξουμε ότι ισχύει για $n + 1$, δηλαδή ότι $H_{2^{n+1}} \leq 1 + (n + 1)$. □

## Παράδειγμα - $H_k$

**Απόδειξη (συνέχ.)**

Έχουμε

$$\begin{aligned} H_{2^{n+1}} &= 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{2^{n+1}} \\ &= (1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{2^n})+(\frac{1}{2^n+1}+\cdots+\frac{1}{2^{n+1}}) \\ &= H_{2^n}+(\frac{1}{2^n+1}+\cdots+\frac{1}{2^{n+1}}) \\ &\le (1+n)+(\frac{1}{2^n}+\cdots+\frac{1}{2^n}) \\ &= (1+n)+2^n\frac{1}{2^n} = (1+n)+1 = 1+(n+1). \end{aligned}$$

□



## Μαθηματική επαγωγή - γενικεύσεις

Κάποιες κοινές παραλλαγές της επαγωγής

- Η βάση δεν είναι πάντα για $n = 1$. Π.χ., για θεωρήματα της μορφής «Για κάθε φυσικό αριθμό $n \geq 4$: ...» η βάση είναι $n = 4$.
- Η επαγωγική υπόθεση είναι ότι η πρόταση ισχύει για **όλους** τους μικρότερους αριθμούς:

$$P(1), \ldots, P(n) \Rightarrow P(n+1)$$

Αυτή είναι η λεγόμενη Ισχυρή Επαγωγή.



## Οι αριθμοί Fibonacci

Οι αριθμοί Fibonacci ορίζονται ως εξής:

$$F_0 = 1, \quad F_1 = 1,$$

και για κάθε $n \geq 2$:

$$F_n = F_{n-1} + F_{n-2}.$$

**Λήμμα 2**

*Να δειχτεί ότι για κάθε ακέραιο $n \geq 0$,*

$$F_n \leq \phi^n,$$

*όπου $\phi = \frac{1+\sqrt{5}}{2} = 1.618\ldots$ είναι η χρυσή τομή.*

**Θεώρημα 3**

*Για κάθε θετικό ακέραιο $n$: $\frac{1}{2}\phi^n \leq F_n \leq \phi^n$.*



## Συνδυαστική ερμηνεία των αριθμών Fibonacci

Ορίζουμε $J_n$ ως τον αριθμό των τρόπων να γράψουμε το $n$ ως άθροισμα των στοιχείων ακολουθιών που αποτελούνται από $1$ και $2$. Π.χ., $J_4 = 5$ γιατί

$$1+1+1+1 = 1+1+2 = 1+2+1 = 2+1+1 = 2+2.$$

Ομοίως $J_1 = 1, J_2 = 2, J_3 = 3$ κοκ. Ορίζουμε $J_0 := 1$, και παίρνουμε (πώς;) για κάθε $n \geq 2$:

$$J_n = J_{n-1} + J_{n-2}$$

Άρα $J_n = F_n$, για κάθε $n$. *Ισοδύναμα*, $J_n$ είναι ο αριθμός των τρόπων να ανέβεις μια σκάλα με $n$ σκαλοπάτια αν κάθε φορά ανεβαίνεις ένα ή δύο σκαλιά ...

## Οι αριθμοί Fibonacci

**Θεώρημα 4**

*Να δειχτεί ότι για κάθε ακέραιους $n, m \geq 1$, οι αριθμοί Fibonacci ικανοποιούν τη σχέση*

$$F_{n+m} = F_n F_m + F_{n-1} F_{m-1}.$$

Το θεώρημα μας επιτρέπει να υπολογίσουμε έναν αριθμό Fibonacci χωρίς να υπολογίσουμε όλους τους προηγούμενους.

$$F_{2k+1} = F_{k+1}F_k + F_k F_{k-1} = (F_k + F_{k-1})F_k + F_k F_{k-1} = F_k^2 + 2F_k F_{k-}$$
$$F_{2k} = F_k F_k + F_{k-1}F_{k-1} = F_k^2 + F_{k-1}^2$$

Παράδειγμα:

$$F_{31} = F_{15}^2 + 2F_{15}F_{14}$$
$$F_{15} = F_7^2 + 2F_7 F_6$$
$$F_{14} = F_7^2 + F_6^2 \qquad F_7 = \ldots, F_6 = \ldots$$



## (Επαγωγικές) Αποδείξεις στη Στοιχειώδη Αριθμοθεωρία

**Ορισμός 1**

Ένας θετικός ακέραιος $p > 1$, καλείται πρώτος αν δεν μπορεί να γραφτεί ως γινόμενο δύο ακεραίων $a$, $b$ με $1 < a, b < p$.

**Θεώρημα 5**

*Κάθε θετικός ακέραιος $n \geq 2$ μπορεί να γραφτεί ως γινόμενο πρώτων αριθμών.*

**Απόδειξη:** με ισχυρή επαγωγή στο $n$.
Αν $p$ πρώτος θεωρούμε ότι το $p$ είναι γινόμενο με έναν όρο.



## Απόδειξη του Θεωρήματος 5

Αν $p$ πρώτος θεωρούμε ότι το $p$ είναι γινόμενο με έναν όρο.

ΒΑΣΗ. $n = 2$. ισχύει.

ΕΠΑΓΩΓΙΚΗ ΥΠΟΘΕΣΗ. Έστω ισχύει για $2 \leq k < n$.

ΕΠΑΓΩΓΙΚΟ ΒΗΜΑ. Θα δείξουμε για $n \geq 3$. Αν $n$ πρώτος, τελειώσαμε. Ειδάλλως, $n = ab$, $1 < a, b < n$. Από την ΕΥ και ο $a$ και ο $b$ γράφονται ως γινόμενο πρώτων αριθμών.



## Μέγιστος Κοινός Διαιρέτης

Για $a, b \in \mathbb{Z}$, λέμε ότι ο $a$ διαιρεί τον $b$ (συμβολίζεται με $a \mid b$), αν υπάρχει $k \in \mathbb{Z}$, τέτοιο ώστε $b = ka$.

**Ορισμός 2**

Για $a, b \in \mathbb{Z}$, ο μέγιστος κοινός διαιρέτης των $a$ και $b$ (συμβολίζεται με $\gcd(a, b)$), ορίζεται ως ο μεγαλύτερος ακέραιος $d$ τ.ω. $d \mid a$ και $d \mid b$.

Εξ ορισμού, όλοι οι ακέραιοι διαιρούν το $0$. Άρα $\gcd(0, b) = b$. Ορίζουμε $\gcd(0, 0) := 0$.

## Αλγόριθμος για τον Μέγιστο Κοινό Διαιρέτη

$$\gcd(a,b) = \begin{cases} a & \text{αν } b = 0 \\ \gcd(b, a \bmod b) & \text{αν } b > 0. \end{cases}$$

### Αλγόριθμος του Ευκλείδη

**function** $\textsc{Euclid}(a,b)$ ▷ Υποθέτουμε ότι $a \geq b$
  **if** $b = 0$ **then**
    **return** $a$ ▷ $gcd(a,0) = a$
  **else**
    $\delta \leftarrow \textsc{Euclid}(b, a \bmod b)$ ▷ $gcd(a,b) = gcd(b, a \bmod b)$
    **return** $\delta$
  **end if**
**end function**



## Ορθότητα του Αλγορίθμου του Ευκλείδη

Θα αποδείξουμε με τη σειρά τις εξής προτάσεις.

### Λήμμα 3 (Bézout)

*Έστω $a, b \in \mathbb{Z}$, όχι και οι δύο μηδέν. Τότε* $\gcd(a,b) = \min\{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}$.

### Λήμμα 4

*Αν $d \mid a$ και $d \mid b$, τότε $d \mid \gcd(a,b)$.*

### Θεώρημα 6

*Για ακέραιους $a \geq 0$ και $b > 0$, $\gcd(a,b) = \gcd(b, a \bmod b)$.*



## Απόδειξη του Λήμματος 3

Έστω $S = \{ax + by \geq 0 \mid x, y \in \mathbb{Z}\}$ και $s$ το ελάχιστο θετικό $(> 0)$ στοιχείο του $S$.

$\exists\, x_s, y_s \in \mathbb{Z}$, τ. ώ. $s = ax_s + by_s$. Θέτουμε $q = \lfloor a/s \rfloor$.

$a \bmod s = a - qs = a(1 - qx_s) + b(-qy_s)$. Άρα $a \bmod s \in S$. Επίσης $0 \leq a \bmod s < s$. Συνεπώς $a \bmod s = 0$, οπότε $s \mid a$.

Ομοίως αποδεικνύεται ότι $s \mid b$. Άρα $s \leq \gcd(a,b)$.

Επιπλέον $\gcd(a,b) \mid s \xRightarrow{s>0} \gcd(a,b) \leq s$. Τελικά $s = \gcd(a,b)$. □



## Απόδειξη του Θεωρήματος 6

Προφανώς $\gcd(a,b) \mid b$.

Θέτουμε $q = \lfloor a/b \rfloor$. Τότε $a \bmod b = a - qb$. Άρα $\gcd(a,b) \mid a \bmod b$.

$$\left.\begin{array}{l} \gcd(a,b) \mid b \\ \gcd(a,b) \mid a \bmod b \end{array}\right\} \xRightarrow{\text{Λήμμα 4}} \gcd(a,b) \mid \gcd(b, a \bmod b).$$

Παρόμοια (πώς;) αποδεικνύεται ότι $\gcd(b, a \bmod b) \mid \gcd(a,b)$. Άρα επειδή και οι δύο ποσότητες είναι θετικές:

$$\gcd(a,b) = \gcd(b, a \bmod b).$$

□

## Πολυπλοκότητα του Αλγορίθμου του Ευκλείδη

- Πόσα βήματα κάνει ο αλγόριθμος για να υπολογίσει τον μέγιστο κοινό διαιρέτη δυο αριθμών; Εξαρτάται από τους αριθμούς. Θέλουμε μια εκτίμηση για τη χειρότερη περίπτωση.
- Το Θεώρημα του Lamé (δεν θα το αποδείξουμε) λέει ότι ο αριθμός των διαιρέσεων, ή ισοδύναμα οι φορές που υπολογίζουμε το $a \bmod b$, είναι λιγότερες από $k-1$ όταν $a > b \geq 1$ και $b < F_k$.
- Εδώ θα δείξουμε ένα πιο απλό αποτέλεσμα.



## Πολυπλοκότητα του Αλγορίθμου του Ευκλείδη

Παρατηρούμε ότι ο αριθμός των διαιρέσεων ισούται με τον αριθμό $r$ των αναδρομικών κλήσεων που εκτελεί ο αλγόριθμος. Συνεπώς ο αριθμός βημάτων του αλγορίθμου είναι $O(r)$.

**Θεώρημα 7**

*Για κάθε θετικούς ακέραιους $a, b$ με $a \geq 2$ και $a \geq b$, ο αριθμός των διαιρέσεων του αλγόριθμου του Ευκλείδη δεν ξεπερνά το* $2\lfloor \log a \rfloor$.

**Απόδειξη**: Με ισχυρή επαγωγή στο $a$.



## Απόδειξη του Θεωρήματος 7

ΒΑΣΗ. $a = 2$, άρα $b \in \{1, 2\}$.
$\textsc{Euclid}(2,1) = \textsc{Euclid}(1,0) = 1$.
$\textsc{Euclid}(2,2) = \textsc{Euclid}(2,0) = 2$.
Μία άρα $\leq 2\lfloor \log 2 \rfloor = 2$ διαιρέσεις.

ΕΠ. ΥΠΟΘΕΣΗ. $\forall 2 \leq k < a$, $\textsc{Euclid}(k, b)$ εκτελεί το πολύ $2\lfloor \log k \rfloor$ διαιρέσεις.

ΕΠ. ΒΗΜΑ. $\mathrm{dc}(a,b) :=$ αριθμός διαιρέσεων του $\textsc{Euclid}(a,b)$.
$\mathrm{dc}(a,b) \leq 2 + \mathrm{dc}(a \bmod b, b \bmod (a \bmod b)) \leq$
$2 + 2\lfloor \log(a \bmod b) \rfloor \leq 2 + 2(\lfloor \log a \rfloor - 1) = 2\lfloor \log a \rfloor$. □

*Ισχυρισμός*: Για $a \geq b$, $a \bmod b < a/2$.
Άρα $\log(a \bmod b) \leq \log a - 1$.



## Θεμελιώδες Θεώρημα της Αριθμοθεωρίας

**Λήμμα 5**

*Αν $a \mid bc$ και $\gcd(a,b) = 1$, τότε $a \mid c$.*

**Λήμμα 6**

*Αν $p$ πρώτος και $p \mid bc$, τότε $p \mid b$ ή $p \mid c$.*

**Λήμμα 7**

*Αν $p$ πρώτος και $p \mid a_1 a_2 \ldots a_n$, τότε ο $p$ διαιρεί κάποιο $a_i$.*

**Θεώρημα 8**

*Κάθε θετικός ακέραιος $n \geq 2$ μπορεί να γραφτεί με μοναδικό τρόπο ως γινόμενο πρώτων αριθμών:*

$$n = p_1 \cdot p_2 \ldots p_j, \ (p_1 \leq p_2 \leq \ldots \leq p_j).$$

## Απόδειξη του Λήμματος 5

**Λήμμα 5**

Αν $a \mid bc$ και $\gcd(a,b)=1$, τότε $a \mid c$.

Από το Λήμμα 3 (Bézout),

$$\begin{aligned}\forall k \in \mathbb{Z}_{>0},\ \gcd(ka,kb) &\overset{\text{Bézout}}{=} \\ \min\{s>0 \mid s = kax + kby \quad \text{με } x,y \in \mathbb{Z}\} &= \\ k \cdot \min\{s>0 \mid s = ax+by \quad \text{με } x,y\in\mathbb{Z}\} &\overset{\text{Bézout}}{=} \\ k \gcd(a,b).\end{aligned}$$

Πάλι από το Λήμμα 3, $a \mid \gcd(ca,cb)$.

Όμως $\gcd(ca,cb) = c\cdot\gcd(a,b) = c\cdot 1 = c$. □



## Απόδειξη του Θεωρήματος 8

Από το Θεώρημα 5, κάθε ακέραιος $\geq 2$ μπορεί να γραφτεί ως γινόμενο πρώτων. Έστω πως υπάρχουν ακέραιοι με δύο διαφορετικές παραγοντοποιήσεις. Διαλέγουμε τον ελάχιστο τέτοιο αριθμό $n$. Ορίζουμε για $m\in\mathbb{N}$, $[m] := \{1,\ldots,m\}$.

$n = p_1p_2\ldots p_j = q_1q_2\ldots q_k$, όπου $p_i$, $i\in[j]$, και $q_i$, $i\in[k]$, πρώτοι αριθμοί.

Αφού $p_1 \mid n \Rightarrow p_1 \mid q_1q_2\ldots q_k$. Από το Λήμμα 7, για κάποιο $i\in[k]$, $p_1 \mid q_i$. Επειδή και οι δύο είναι πρώτοι, $p_1 = q_i$.

$n/p_1 = p_2\ldots p_j = q_1\ldots q_{i-1}q_{i+1}\ldots q_k < n$. Υποχρεωτικά κάποιο $p_l$, $l\in[j]\setminus\{1\}$, διαφέρει από κάποιο $q_t$, $t\in[k]\setminus\{i\}$. Βρήκαμε αριθμό μικρότερο του $n$ με δύο διαφορετικές παραγοντοποιήσεις, άτοπο. □



## Ισχυροποίηση της πρότασης

Κάποιες φορές για να αποδείξουμε μια πρόταση με μαθηματική επαγωγή, παραδόξως μας συμφέρει να την ισχυροποιήσουμε. Παράδειγμα:

**Πρόταση 5**

$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2.$

**Απόδειξη.**

Ας χρησιμοποιήσουμε επαγωγή και ας υποθέσουμε ότι η πρόταση ισχύει για κάποιο $n$. Προσθέτουμε και στα δυο μέλη το $\frac{1}{(n+1)^2}$. Αλλά, τώρα το δεξί μέλος είναι $2+\frac{1}{(n+1)^2}$ που δεν είναι μικρότερο του 2. Η προσέγγιση αυτή αποτυγχάνει.
Είναι εύκολο όμως να δείξουμε την πιο ισχυρή πρόταση

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}.$$

□



## Ισχυροποίηση της πρότασης

ΕΠΑΓΩΓΙΚΗ ΥΠΟΘΕΣΗ. $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$.

ΕΠΑΓΩΓΙΚΟ ΒΗΜΑ.

$$\begin{aligned}1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} + \frac{1}{(n+1)^2} &\leq \\ 2 - \frac{1}{n} + \frac{1}{(n+1)^2} &= \\ 2 - \frac{(n+1)^2}{n(n+1)^2} + \frac{n}{n(n+1)^2} &= \\ 2 - \frac{(n+1)^2 - n}{n(n+1)^2}.\end{aligned}$$

Όμως $\frac{(n+1)^2-n}{n(n+1)^2} \geq \frac{1}{n+1}$. Άρα

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} + \frac{1}{(n+1)^2} \leq 2 - \frac{1}{n+1}.$$

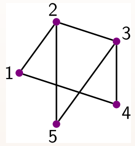
□

## Θεωρία Ramsey

Frank P. Ramsey (1903-1930)



## Γραφήματα



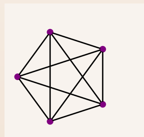

Γράφημα $G$ με σύνολο κορυφών $V$ και σύνολο ακμών $E$ είναι ένα ζεύγος $(V, E)$ όπου

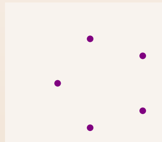
$$E \subseteq \{\{u, v\} \mid u, v \in V\}$$

δηλαδή μια ακμή είναι ένα μη διατεταγμένο ζεύγος κορυφών.

**Ορισμός 3 (Πλήρες / Κενό)**

$G = (V, E)$ καλείται πλήρες (κλίκα) αν $E = \{\{u, v\} \mid u, v \in V\}$.
Αν $E = \varnothing$ το $G$ καλείται κενό και το $V$ ανεξάρτητο σύνολο.







## Θεωρία Ramsey

**Θεώρημα 9 (Ramsey)**

*Για κάθε φυσικό $k$, υπάρχει φυσικός $R(k)$ τέτοιος ώστε κάθε γράφημα με $R(k)$ ή περισσότερες κορυφές περιέχει ένα πλήρες υπογράφημα με $k$ κορυφές ή ένα κενό υπογράφημα με $k$ κορυφές.*

Η πρόταση για κάποιο $k$ δεν φαίνεται να συνεπάγεται την πρόταση για κάποιο $k + 1$.
Αν όμως γενικεύσουμε / ισχυροποιήσουμε το θεώρημα, τότε μπορούμε να το αποδείξουμε με επαγωγή.

**Θεώρημα 10 (Ramsey)**

*Για κάθε θετικούς ακέραιους $k, m \geq 2$ υπάρχει φυσικός $R(k, m)$ τέτοιος ώστε κάθε γράφημα με $R(k, m)$ ή περισσότερες κορυφές περιέχει ένα πλήρες υπογράφημα με $k$ κορυφές ή ένα κενό υπογράφημα με $m$ κορυφές.*



## Απόδειξη Θεωρήματος Ramsey

**Θεώρημα 11 (Ramsey)**

*Για κάθε θετικούς ακέραιους $k, m \geq 2$ υπάρχει φυσικός $R(k, m)$ τέτοιος ώστε κάθε γράφημα με $R(k, m)$ ή περισσότερες κορυφές περιέχει $k$-κλίκα ή $m$-ανεξάρτητο σύνολο.*

Η επαγωγική απόδειξη απαιτεί λίγη προσοχή στις αρχικές συνθήκες.

**Πρόταση 6**

*Για κάθε θετικούς ακέραιους $k, m \geq 2$, $R(k, 2) = k$ και $R(2, m) = m$.*

Θα αποδείξουμε το Θεώρημα του Ramsey με ισχυρή επαγωγή στο άθροισμα $k + m$.
ΒΑΣΗ: Για $k + m = 4$, ισχύει από την Πρόταση. Ομοίως και για $k + m = 5$, αφού τότε ο ένας από τους $k, m$ ισούται με 2.

## Απόδειξη Θεωρήματος Ramsey (σκελετός)

ΒΑΣΗ: Για $k+m=4$ και $k+m=5$, ισχύει από την Πρόταση.

ΕΠΑΓΩΓΙΚΗ ΥΠΟΘΕΣΗ: Ισχύει για $k, m \geq 2$ με $k+m \geq 5$.

ΕΠΑΓΩΓΙΚΟ ΒΗΜΑ: Θα δείξουμε για αριθμούς $k, m \geq 2$ με $k+m \geq 6$. (Άρα χβτγ $k, m \geq 3$).
Η επαγωγική υπόθεση διασφαλίζει την ύπαρξη των $R(k-1, m)$ και $R(k, m-1)$ (αφού $k+m-1 \geq 5$, και $k-1, m-1 \geq 2$).

Θα δείξουμε ότι υπάρχει το $R(k, m)$ και μάλιστα

$$R(k, m) \leq R(k-1, m) + R(k, m-1).$$

Αν $G=(V, E)$ και $S \subseteq V$, ορίζουμε $G[S]$ ως το υπογράφημα του $G$ που ενάγεται από το $S$, δηλ. περιέχει μόνο τις ακμές του $E$ με άκρα στο $S$.



## Απόδειξη Θεωρήματος Ramsey

Έστω γράφημα $G=(V, E)$ με $n := R(k-1, m) + R(k, m-1)$ κορυφές. Διάλεξε $v \in V$. Το $V \setminus \{v\}$ διαμερίζεται σε $A$ και $B$, τους γείτονες και τους μη γείτονες του $v$.

Περίπτωση 1. Αν $|A| \geq R(k-1, m)$ από ΕΥ το $G[A]$ περιέχει $(k-1)$-κλίκα ή $m$-ανεξάρτητο σύνολο. Άρα το $G$ περιέχει $k$-κλίκα ή $m$-ανεξάρτητο σύνολο.

Περίπτωση 2. Αν $|B| \geq R(k, m-1)$ από ΕΥ το $G[B]$ περιέχει $k$-κλίκα ή $(m-1)$-ανεξάρτητο σύνολο. Άρα το $G$ περιέχει $k$-κλίκα ή $m$-ανεξάρτητο σύνολο.



## Απόδειξη Θεωρήματος Ramsey

Δεν υπάρχει άλλη περίπτωση! Αν δεν είμαστε στις Περ. 1 ή 2:

$$\left.\begin{array}{l} |A| < R(k-1, m) \\ |B| < R(k, m-1) \end{array}\right\} \Rightarrow \left.\begin{array}{l} |A| \leq R(k-1, m) - 1 \\ |B| \leq R(k, m-1) - 1 \end{array}\right\} \Rightarrow$$

$$|A| + |B| \leq R(k-1, m) + R(k, m-1) - 2 = n - 2.$$

Άρα $|V| = |A| + |B| + 1 \leq n - 1$, άτοπο.

Επομένως οποιοδήποτε γράφημα με $n$ κορυφές περιέχει $k$-κλίκα ή $m$-ανεξάρτητο σύνολο.



## Ένα άνω φράγμα

Αποδείξαμε την αναδρομική σχέση:

$$\begin{array}{ll} R(k, m) \leq R(k-1, m) + R(k, m-1) & k, m \geq 3 \\ R(k, 2) = k & k \geq 2 \\ R(2, m) = m & m \geq 2 \end{array}$$

Χρησιμοποιώντας απλές ιδιότητες των δυωνυμικών συντελεστών μπορούμε να αποδείξουμε επαγωγικά (πώς;) ότι για $k, m \geq 2$

$$R(k, m) \leq \binom{m+k-2}{k-1}. \tag{1}$$

**Άσκηση.** Μέσω της (1) δείξτε ότι $R(k, k) < 4^k$.