Θεωρια Αριθμων

Θεωρητικα Θεματα

Ακαδημαϊκο Ετος

2016 - 2017

Τμημα Β′

Διδασκων: Α. Μπελληγιάννης

Ιστοσελιδα Μαθηματος:
http://users.uoi.gr/abeligia/NumberTheory/NT2016/NT2016.html

19 Οκτωβρίου 2016

— Το παρόν κείμενο αποτελεί ένα σύνολο **πρόχειρων** *σημειώσεων, κυρίως επί Θεωρητικών Θεμάτων, για τις ανάγκες του μαθήματος*
Θεωρία Αριθμών, Χειμερινό Εξάμηνο Ακαδημαϊκού Έτους 2016 - 2017,
και τελεί υπο **συνεχή επεξεργασία**.

Περιεχόμενα

Μέρος 1. Διαιρετότητα Ακεραίων

1. Αρχή Καλής Διάταξης και Μαθηματική Επαγωγή

Στην Θεωρία Αριθμών μεγάλο ρόλο στην ανάπτυξη της θεωρίας αλλά και σε αποδεικτικές μεθόδους διαδραματίζουν διάφορες αρχές αξιωματικού χαρακτήρα. Οι σημαντικότερες από αυτές τις αρχές είναι οι εξής:

(ΑΚΔ) Αρχη Καλης Διαταξης: Κάθε μη κενό υποσύνολο του συνόλου $\mathbb{N}$ έχει ελάχιστο στοιχείο.

(ΑΜΕ) Αρχη Μαθηματικης Επαγωγης: Έστω S ένα υποσύνολο του συνόλου $\mathbb{N}$ για το οποίο ισχύουν τα εξής:
(α) $1 \in S$.
(β) $\forall k \in \mathbb{N}$: $k \in S \implies k+1 \in S$.
Τότε: $S = \mathbb{N}$.

(ΑΜΕ)$_1$ Αρχη Μαθηματικης Επαγωγης$_1$: Έστω $P(n)$ μια πρόταση η οποία εξαρτάται από τον φυσικό αριθμό $n \in \mathbb{N}$, για την οποία ισχύουν τα εξής:
(α) Η πρόταση $P(1)$ είναι αληθής.
(β) $\forall k \in \mathbb{N}$: η πρόταση $P(k)$ είναι αληθής $\implies$ η πρόταση $P(k+1)$ είναι αληθής.
Τότε: η πρόταση $P(n)$ είναι αληθής, $\forall n \in \mathbb{N}$.

(ΑΜ) Αρχη Μεγιστου: Κάθε μη κενό άνω φραγμένο υποσύνολο του συνόλου $\mathbb{N}$ έχει μέγιστο στοιχείο.

Υπενθυμίζουμε ότι αν S είναι ένα σύνολο, τότε ένα **ελάχιστο στοιχείο** του συνόλου S είναι ένα στοιχείο $s_0 \in S$ για το οποίο ισχύει ότι: $s_0 \leq s$, $\forall s \in S$. Προφανώς αν s_0, s_1 είναι ελάχιστα στοιχεία του συνόλου S, τότε επειδή ισχύει ότι $s_0 \leq s_1$ (επειδή το s_0 είναι ελάχιστο στοιχείο του S και $s_1 \in S$) και $s_1 \leq s_0$ (επειδή το s_1 είναι ελάχιστο στοιχείο του S και $s_0 \in S$), έπεται ότι $s_0 = s_1$. Άρα ένα ελάχιστο στοιχείο ενός συνόλου S, αν υπάρχει, είναι μοναδικό και συμβολίζεται συνήθως με: $\min S$.

Έστω $S \subseteq \mathbb{N}$ ένα υποσύνολο του $\mathbb{N}$. Ένα **άνω φράγμα** για το S είναι ένας φυσικός αριθμός $m \in \mathbb{N}$ για τον οποίο ισχύει ότι: $s \leq m$, $\forall s \in S$. Το υποσύνολο $S \subseteq \mathbb{N}$ καλείται **άνω φραγμένο** αν υπάρχει ένα άνω φράγμα για το S.

Θα δείξουμε ότι οι παραπάνω αρχές είναι μεταξύ τους ισοδύναμες.

Θεώρημα 1.1. *Οι ακόλουθες αρχές είναι ισοδύναμες:*

1. *(ΑΚΔ): Κάθε μη κενό υποσύνολο του συνόλου $\mathbb{N}$ έχει ελάχιστο στοιχείο.*
2. *(ΑΜΕ): Έστω S ένα υποσύνολο του συνόλου $\mathbb{N}$ για το οποίο ισχύουν τα εξής:*
   (α) $1 \in S$.
   (β) $\forall k \in \mathbb{N}$: $k \in S \implies k+1 \in S$.
   Τότε: $S = \mathbb{N}$.
3. *(ΑΜΕ)$_1$: Έστω $P(n)$ μια πρόταση η οποία εξαρτάται από τον φυσικό αριθμό $n \in \mathbb{N}$, για την οποία ισχύουν τα εξής:*
   (α) *Η πρόταση $P(1)$ είναι αληθής.*
   (β) $\forall k \in \mathbb{N}$: *η πρόταση $P(k)$ είναι αληθής $\implies$ η πρόταση $P(k+1)$ είναι αληθής.*
   Τότε: η πρόταση $P(n)$ είναι αληθής, $\forall n \in \mathbb{N}$.
4. *(ΑΜ): Κάθε μη κενό άνω φραγμένο υποσύνολο του συνόλου $\mathbb{N}$ έχει μέγιστο στοιχείο.*

Απόδειξη. • (ΑΚΔ) $\implies$ (ΑΜΕ) Υποθέτουμε ότι ισχύει η Αρχή Καλής Διάταξης, και έστω S ένα υποσύνολο του $\mathbb{N}$ έτσι ώστε $1 \in S$, και $k \in S \implies k+1 \in S$.

Υποθέτουμε ότι $S \neq \mathbb{N}$. Τότε το σύνολο $\mathbb{N} \setminus S$ είναι μη-κενό. Επόμενως από την αρχή καλής διάταξης έπεται ότι το $\mathbb{N} \setminus S$ έχει ελάχιστο στοιχείο:

$$\ell = \min(\mathbb{N} \setminus S), \quad \text{δηλαδή} \quad \ell \in \mathbb{N} \setminus S \quad \text{και} \quad \ell \leq x, \ \ \forall x \in \mathbb{N} \setminus S$$

Αν $\ell = 1$, τότε $1 \in \mathbb{N} \setminus S$ το οποίο είναι άτοπο διότι από την υπόθεση έχουμε $1 \in S$. Άρα $\ell > 1$ και επομένως $1 \leq \ell - 1 < \ell$.

Τότε το στοιχείο $\ell - 1$ θα ανήκει στο S διότι διαφορετικά $\ell - 1 \in \mathbb{N} \setminus S$ κάτι το οποίο είναι άτοπο διότι $\ell - 1 < \ell$ και το ℓ είναι το ελάχιστο στοιχείο του $\mathbb{N} \setminus S$. Απο την ιδιότητα (β) του συνόλου S θα έχουμε τότε: $1 \in S$, και $\ell - 1 \in S \implies \ell \in S$. Αυτό όμως είναι άτοπο διότι εκ' κατασκευής $\ell \in \mathbb{N} \setminus S$, δηλαδή $\ell \notin S$.

Στο άτοπο καταλήξαμε υποθέτοντας ότι $S \neq \mathbb{N}$. Επομένως θα έχουμε $S = \mathbb{N}$, και άρα ισχύει η πρώτη εκδοχή (ΑΜΕ) της Αρχής Μαθηματικής Επαγωγής.

- (ΑΜΕ) $\implies$ (ΑΜΕ)$_1$ Υποθέτουμε ότι ισχύει η πρώτη εκδοχή (ΑΜΕ) της Αρχής Μαθηματικής Επαγωγής και έστω η πρόταση $P(n)$, $n \in \mathbb{N}$, για την οποία ικανοποιούνται οι συνθήκες του μέρους **3**.. Θεωρούμε το ακόλουθο σύνολο

$$S = \big\{ n \in \mathbb{N} \mid \text{η πρόταση } \ P(n) \ \text{ είναι αληθής} \big\}$$

Προφανώς τότε για το υποσύνολο S ικανοποιούνται οι συνθήκες (α) και (β) του μέρους **2**.. Επομένως θα έχουμε ότι $S = \mathbb{N}$, το οποίο σημαίνει ότι η πρόταση $P(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$. Άρα ισχύει η δεύτερη εκδοχή (ΑΜΕ)$_1$ της Αρχής Μαθηματικής Επαγωγής.

- (ΑΜΕ)$_1$ $\implies$ (ΑΚΔ) Υποθέτουμε ότι ισχύει η δεύτερη εκδοχή (ΑΜΕ)$_1$ της Αρχής Μαθηματικής Επαγωγής και έστω $S \subseteq \mathbb{N}$ ένα μη-κενό υποσύνολο του $\mathbb{N}$.

Υποθέτουμε ότι το S δεν έχει ελάχιστο στοιχείο. Για κάθε $n \in \mathbb{N}$, θεωρούμε την πρόταση

$$P(n): \ \text{για κάθε} \ \ k \in \mathbb{N} \ \ \text{έτσι ώστε} \ \ 1 \leq k \leq n, \ \ \text{ισχύει ότι:} \ \ k \notin S$$

Η πρόταση $P(1)$, δηλαδή ο ισχυρισμός ότι $1 \notin S$, είναι αληθής. Πράγματι, αν $1 \in S$ τότε προφανώς το 1 είναι ελάχιστο στοιχείο του S κάτι το οποίο είναι άτοπο διότι το S δεν έχει ελάχιστο στοιχείο.

Υποθέτουμε ότι η πρόταση $P(n)$ είναι αληθής, δηλαδή κανένας από τους αριθμούς $1, 2, \cdots, n$ δεν ανήκει στο S. Αν το $n+1$ ανήκει στο S, τότε επειδή $k \notin S$, όπου $1 \leq k \leq n$, έπεται άμεσα ότι το $n+1$ είναι ελάχιστο στοιχείο του S κάτι το οποίο είναι άτοπο διότι το S δεν έχει ελάχιστο στοιχείο. Άρα θα έχουμε ότι $n+1 \notin S$. Αυτό όμως σημαίνει ότι η πρόταση $P(n+1)$ είναι αληθής.

Από την δεύτερη εκδοχή της Αρχής Μαθηματικής Επαγωγής, έπεται τότε ότι η πρόταση $P(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$, και επομένως $\forall n \in \mathbb{N}$, $1 \leq k \leq n \implies k \notin S$. Με άλλα λόγια $\forall n \in \mathbb{N}$, $n \notin S$. Αυτό όμως, επεισδή $S \subseteq \mathbb{N}$, σημαίνει ότι $S = \emptyset$ κάτι το οποίο είναι άτοπο από την αρχική μας υπόθεση.

Στο άτοπο καταλήξαμε υποθέτοντας ότι το μη-κενό υποσύνολο S του $\mathbb{N}$ δεν έχει ελάχιστο στοιχείο. Άρα το S έχει ελάχιστο στοιχείο και επομένως ισχύει η Αρχή Καλής Διάταξης.

– Έτσι έχουμε δείξει ότι οι τρεις πρώτες αρχές (ΑΚΔ), (ΑΜΕ), (ΑΜΕ)$_1$ είναι ισοδύναμες. Ολοκληρώνουμε την απόδειξη δείχνοντας ότι: (ΑΚΔ) $\implies$ (ΑΜ) $\implies$ (ΑΜΕ)$_1$.

- (ΑΚΔ) $\implies$ (ΑΜ) Υποθέτουμε ότι ισχύει η Αρχή Καλής Διάταξης, και έστω $T \subseteq \mathbb{N}$ ένα μη-κενό και άνω φραγμένο υποσύνολο του $\mathbb{N}$. Έστω $b \in \mathbb{N}$ ένα άνω φράγμα του T, δηλαδή:

$$b \in \mathbb{N} \ \ \text{και} \ \ \ t \leq b, \ \ \forall t \in T$$

Ορίζουμε ένα νέο σύνολο, το σύνολο όλων των άνω φραγμάτων του T στο $\mathbb{N}$:

$$S = \big\{ s \in \mathbb{N} \mid t < s, \ \ \forall t \in T \big\}$$

Το σύνολο S είναι μη κενό διότι $\forall t \in T: \ t \leq b < b+1$, και άρα $b+1 \in S$.

Από την Αρχή Καλής Διάταξης, έπεται ότι το σύνολο S έχει ελάχιστο στοιχείο, έστω ότι αυτό είναι το s_0:

$$s_0 = \min S, \quad \text{δηλαδή} \;\; s_0 \in S \;\; \text{και} \;\; s_0 \leq s, \;\; \forall s \in S$$

Από το ορισμό του συνόλου S, έπεται ότι υπάρχει ένα στοιχείο $t_0 \in T$ έτσι ώστε: $s_0 - 1 \leq t_0$. Πράγματι, αν $s_0 - 1 > t$, $\forall t \in T$, τότε θα είχαμε ότι $s_0 - 1 \in S$ κάτι το οποίο είναι άτοπο διότι $s_0 - 1 < s_0$ και το s_0 είναι ένα ελάχιστο στοιχείο του S.

Άρα πράγματι υπάρχει ένα στοιχείο $t_0 \in T$ έτσι ώστε: $s_0 - 1 \leq t_0$. Επειδή όμως έχουμε και $t_0 < s_0$, έπεται ότι θα έχουμε $s_0 - 1 = t_0 \in T$. Ισχυριζόμαστε ότι:

$$t_0 = \max T, \quad \text{δηλαδή το} \;\; t_0 \;\; \text{είναι μέγιστο στοιχείο του} \;\; T$$

Πράγματι, το t_0 ανήκει εκ' κατασκευής στο T και επιπλέον επειδή από τον ορισμό του συνόλου S έχουμε $t < s_0$, $\forall t \in T$, έπεται ότι $t \leq s_0 - 1 = t_0$, $\forall t \in T$. Δηλαδή $t_0 = \max T$.

- (AM) $\Longrightarrow$ (AME)$_1$ Υποθέτουμε ότι ισχύει η Αρχή Μεγίστου και έστω $P(n)$ μια πρόταση η οποία εξαρτάται από το $n \in \mathbb{N}$, για την οποία ισχύει ότι η $P(1)$ είναι αληθής, και για κάθε φυσικό αριθμό n: $P(n)$ είναι αληθής $\implies$ $P(n+1)$ είναι αληθής.

Έστω ότι υπάρχει $m \in \mathbb{N}$ έτσι ώστε η πρόταση $P(m)$ δεν είναι αληθής. Ορίζουμε τότε ένα σύνολο T ως εξής:

$$T = \big\{ t \in \mathbb{N} \mid \text{η πρόταση } P(n) \text{ είναι αληθής } \forall n \in \mathbb{N} : \; 1 \leq n \leq t \big\}$$

Επειδή η πρόταση $P(1)$ είναι αληθής, έπεται ότι $1 \in T$ και άρα $T \neq \emptyset$. Επιπρόσθετα ο φυσικός αριθμός m είναι προφανώς ένα άνω φράγμα για το σύνολο T. Πράγματι αν $k \in \mathbb{N}$ και $m \leq k$, τότε $k \notin T$, διότι διαφορετικά αν $k \in T$, τότε θα είχαμε ότι η $P(m)$ είναι αληθής κάτι το οποίο δεν ισχύει.

Έτσι το T είναι ένα μη-κενό και άνω φραγμένο υποσύνολο του $\mathbb{N}$. Επομένως από την Αρχή Μεγίστου, το σύνολο T έχει ένα μέγιστο στοιχείο, έστω ότι αυτό είναι το t_0:

$$t_0 = \max T, \;\; \text{δηλαδή} \;\; t_0 \in T \;\; \text{και} \;\; t \leq t_0, \; \forall t \in T$$

Από τον ορισμό του συνόλου T θα έχουμε ότι η πρόταση $P(t_0)$ είναι αληθής. Τότε από την υπόθεση θα έχουμε και ότι η πρόταση $P(t_0 + 1)$ είναι αληθής. Αυτό όμως σημαίνει ότι η πρόταση $P(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$ έτσι ώστε: $1 \leq n \leq t_0 + 1$, και επομένως ο αριθμός $t_0 + 1$ ανήκει στο σύνολο T. Αυτό όμως είναι άτοπο διότι $t_0 < t_0 + 1$ και το t_0 είναι μέγιστο στοιχείο τπυ T.

Στο άτοπο καταλήξαμε υποθέτοντας ότι υπάρχει $m \in \mathbb{N}$ έτσι ώστε η πρόταση $P(m)$ δεν είναι αληθής. Άρα η πρόταση $P(n)$ είναι αληθής, $\forall n \in \mathbb{N}$, και επομένως ισχύει η δεύτερη εκδοχή (AME)$_1$ της Αρχής Μαθηματικής Επαγωγής. ■

Παρατήρηση 1.2. Είδαμε στο Θεώρημα 1.1 ότι οι αρχές (AME) και (AME)$_1$ είναι ισοδύναμες, δείχνοντας πρώτα άμεσα ότι (AME) $\Longrightarrow$ (AME)$_1$ και κατόπιν δείχνοντας με έμμεσο τρόπο ότι (AME)$_1$ $\Longrightarrow$ (AME).

Εδώ δείχνουμε άμεσα ότι (AME)$_1$ $\Longrightarrow$ (AME).

Έστω ότι ισχύει η (AME)$_1$, και υποθέτουμε ότι $S \subseteq \mathbb{N}$ είναι ένα υποσύνολο του $\mathbb{N}$ για το οποίο γνωρίζουμε ότι $1 \in S$ και ότι η συνθήκη $n \in S$ συνεπάγεται τη συνθήκη $n + 1 \in S$. Θα δείξουμε ότι $S = \mathbb{N}$, χρησιμοποιώντας την υπόθεση ότι ισχύει η (AME)$_1$. Θεωρούμε την Πρόταση[1]

$$\forall n \in \mathbb{N} : \quad P(n) : \;\; \text{οι αριθμοί } 1, 2, \cdots, n \;\; \text{ανήκουν στο σύνολο } S$$

[1] Θέτοντας, $\forall n \in \mathbb{N}$:

$$\mathbb{N}_n = \{1, 2, \cdots, n\}$$

η Πρόταση $P(n)$ μπορεί να γραφεί ως εξής:

$$P(n) : \quad \mathbb{N}_n \subseteq S$$

Επειδή $1 \in S$, έπεται ότι η Πρόταση $P(1)$ είναι αληθής. Υποθέτουμε $n > 1$ και ότι η πρόταση $P(n)$ είναι αληθής, δηλαδή οι αριθμοί $1, 2, \cdots, n \in S$. Επειδή από την υπόθεσή μας $n \in S \Longrightarrow n+1 \in S$, έπεται ότι οι αριθμοί $1, 2, \cdots, n, n+1 \in S$. Αυτό σημαίνει ότι η Πρόταση $P(n+1)$ είναι αληθής. Από την $(\text{ΑΜΕ})_1$ έπεται ότι η η Πρόταση $P(n)$ είναι αληθής, $\forall n \in \mathbb{N}$. Με άλλα λόγια για κάθε φυσικό αριθμό n, οι αριθμοί $1, 2,' \cdots, n$ ανήκουν στο S. Αυτό σημαίνει ότι $\mathbb{N} \subseteq S$ και επομένως, επειδή $S \subseteq \mathbb{N}$, θα έχουμε τελικά $S = \mathbb{N}$. Έτσι δείξαμε ότι ισχύει η (ΑΜΕ).

Η Αρχή Μαθηματικής Επαγωγής έχει πολλές εκδοχές, και στο Θεώρημα 1.1 είδαμε δύο από αυτές. Πολύ χρησιμες στις εφαρμογές είναι και οι ακόλουθες εκδοχές της Αρχής Μαθηματικής Επαγωγής:

$(\text{ΑΜΕ})_2$ Αρχη Μαθηματικης Επαγωγης$_2$: Έστω $P(n)$ μια πρόταση η οποία εξαρτάται από τον φυσικό αριθμό $n \in \mathbb{N}$, για την οποία ισχύουν τα εξής:
- (α) Η πρόταση $P(1)$ είναι αληθής.
- (β) $\forall m \in \mathbb{N}$, όπου $2 \leq m < n$: η πρόταση $P(m)$ είναι αληθής $\Longrightarrow$ η πρόταση $P(n)$ είναι αληθής.

Τότε: η πρόταση $P(n)$ είναι αληθής, $\forall n \in \mathbb{N}$.

$(\text{ΑΜΕ})_3$ Αρχη Μαθηματικης Επαγωγης$_3$: Έστω $n_0 \in \mathbb{N}$ και $P(n)$ μια πρόταση η οποία εξαρτάται από τον φυσικό αριθμό $n \in \mathbb{N}$, $\forall n \geq n_0$, για την οποία ισχύουν τα εξής:
- (α) Η πρόταση $P(n_0)$ είναι αληθής.
- (β) $\forall n \in \mathbb{N}$, όπου $n > n_0$: η πρόταση $P(n)$ είναι αληθής $\Longrightarrow$ η πρόταση $P(n+1)$ είναι αληθής.

Τότε: η πρόταση $P(n)$ είναι αληθής, $\forall n \geq n_0$.

$(\text{ΑΜΕ})_4$ Αρχη Μαθηματικης Επαγωγης$_4$: Έστω $n_0 \in \mathbb{N}$ και $P(n)$ μια πρόταση η οποία εξαρτάται από τον φυσικό αριθμό $n \in \mathbb{N}$, $\forall n \geq n_0$, για την οποία ισχύουν τα εξής:
- (α) Η πρόταση $P(n_0)$ είναι αληθής.
- (β) $\forall m \in \mathbb{N}$, όπου $n_0 \leq m < n$: η πρόταση $P(m)$ είναι αληθής $\Longrightarrow$ η πρόταση $P(n)$ είναι αληθής.

Τότε: η πρόταση $P(n)$ είναι αληθής, $\forall n \geq n_0$.

Οι εκδοχές $(\text{ΑΜΕ})_1$, $(\text{ΑΜΕ})_3$ της Αρχής Μαθηματικής Επαγωγής είναι γνωστές ως Αρχές της **απλής** Μαθηματικής Επαγωγής και οι εκδοχές $(\text{ΑΜΕ})_2$, $(\text{ΑΜΕ})_4$ της Αρχής Μαθηματικής Επαγωγής είναι γνωστές ως Αρχές της **ισχυρής** Μαθηματικής Επαγωγής.

Άσκηση 1.3. Γνωρίζοντας ότι ισχύει η Αρχή Καλής Διάταξης, ή ισοδύναμα μια από τις αρχές (ΑΜΕ) ή $(\text{ΑΜΕ})_1$, να αποδειχθεί ότι ισχύουν και οι εκδοχές $(\text{ΑΜΕ})_k$, όπου $k = 2, 3, 4$.

– Από τώρα και στο εξής στο μάθημα και στη συνέχεια των σημειώσεων, θα υποθέτουμε ότι ισχύει η Αρχή Καλής Διάταξης (ΑΚΔ), και επομένως θα ισχύει η Αρχή Μεγίστου (ΑΜ) καθώς και όλες οι εκδοχές της Αρχής Μαθηματικής Επαγωγής (ΑΜΕ), $(\text{ΑΜΕ})_1$, $(\text{ΑΜΕ})_2$, $(\text{ΑΜΕ})_3$, $(\text{ΑΜΕ})_4$.

2. Η m-αδική αναπαράσταση ενός φυσικού αριθμού

Σκοπός της παρούσης ενότητας είναι η απόδειξη του Θεωρήματος 2.2 που δίνει, δοθέντων ακεραίων $n \geq 1$ και $m \geq 2$, την m-αδική αναπαράσταση του n.

Χρειαζόμαστε το ακόλουθο λήμμα.

Λήμμα 2.1. *Έστω m, n θετικοί ακέραιοι με $m \geq 2$. Τότε υπάρχει μοναδικός μη αρνητικός ακέραιος k ώστε $m^k \leq n < m^{k+1}$.*

Απόδειξη. Πρώτα δείχνουμε με μαθηματική επαγωγή ότι

$$m^s \geq 1 + s \tag{2.1}$$

για κάθε ακέραιο $s \geq 1$. Πράγματι, για $s = 1$ ισχύει αφού $m \geq 2$. Υποθέτουμε ότι για κάποιο $s \geq 1$ ισχύει $m^s \geq 1 + s$. Τότε

$$m^{s+1} = m \cdot m^s \geq m(1 + s) = (1 + s) + (m - 1)(1 + s) \geq (1 + s) + 1 = 1 + (s + 1)$$

Επομένως απο την Αρχή Μαθηματικής Επαγωγής η ανισότητα (2.1) ισχύει για κάθε $s \geq 1$. Σαν συνέπεια της ανισότητας $m^n > n$.

Ορίζουμε $S = \{s \in \mathbb{N} : m^s > n\}$. Αφού όπως δείξαμε $n \in S$, το S είναι μη κενό σύνολο φυσικών αριθμών. Άρα από την αρχή του ελαχίστου έχει ελάχιστο στοιχείο s_0 το οποίο γράφεται στην μορφή $s_0 = k + 1$ για κάποιον μη αρνητικό ακέραιο k. Τότε, $k \notin S$ άρα $m^k \leq n$ και $k + 1 \in S$ άρα $n < m^{k+1}$.

Θα δείξουμε τώρα την μοναδικότητα του k. Υποθέτουμε

$$m^k \leq n < m^{k+1} \qquad \text{και} \qquad m^l \leq n < m^{l+1}$$

για ακέραιους k, l και θα δείξουμε ότι $k = l$. Εστω ότι δεν ισχύει, και έχουμε $k < l$. Άρα $k + 1 \leq l$, συνεπώς

$$n < m^{k+1} \leq m^l \leq n$$

που είναι αντίφαση. ■

Στο ακόλουθο Θεώρημα η έκφραση (2.2) λέγεται m-αδική αναπαράσταση του n και οι ακέραιοι a_i είναι τα ψηφία του n με βάση τον m.

Θεώρημα 2.2. *Έστω m ένας ακέραιος με $m \geq 2$. Κάθε ακέραιος $n \geq 1$ αναπαρίσταται κατά μοναδικό τρόπο στη μορφή*

$$n = a_0 + a_1 m + a_2 m^2 + \ldots + a_k m^k, \tag{2.2}$$

όπου k είναι ο (μοναδικός) μη αρνητικός ακέραιος για τον οποίο $m^k \leq n < m^{k+1}$ και οι $a_0, a_1, \ldots, a_k$ είναι ακέραιοι που ικανοποιούν τις $1 \leq a_k \leq m - 1$ και $0 \leq a_i \leq m - 1$ για κάθε $i = 0, 1, \ldots, k - 1$.

Απόδειξη. Πρώτα δείχνουμε την ύπαρξη των k και $a_0 \ldots, a_k$. Για $k \geq 0$ συμβολίζουμε με $P(k)$ την εξής πρόταση: κάθε φυσικός n με $m^k \leq n < m^{k+1}$ έχει m-αδική αναπαράσταση. Θα αποδείξουμε ότι η $P(k)$ ισχύει για κάθε $k \geq 0$ με τη μέθοδο της μαθηματικής επαγωγής.

Πρώτα δείχνουμε την $P(0)$. Έστω $1 \leq n < m$. Θέτουμε $a_0 = n$. Τότε η a_0 είναι μια m-αδική αναπαράσταση του n.

Έστω $k \geq 1$ και ας υποθέσουμε ότι ισχύουν οι προτάσεις $P(0), P(1), \ldots, P(k - 1)$. Θα δείξουμε ότι ισχύει η $P(k)$. Έστω $m^k \leq n < m^{k+1}$. Από την ταυτότητα της διαίρεσης του n με m^k, υπάρχουν a_k και r με $0 \leq r < m^k$ έτσι ώστε

$$n = a_k m^k + r. \tag{2.3}$$

Τότε,

$$0 < m^k - r \leq n - r = a_k m^k \leq n < m^{k+1}.$$

Διαιρώντας αυτή την ανισότητα με m^k παίρνουμε $0 < a_k < m$. Αφού οι m και a_k είναι ακέραιοι, βλέπουμε ότι

$$1 \leq a_k \leq m - 1.$$

Αν $r = 0$, τότε η $n = a_k m^k$ είναι μια m-αδική αναπαράσταση του n. Αν $r \geq 1$ τότε από το Λήμμα 2.1 έχουμε $m^l \leq n < m^{l+1}$ για κάποιον μη αρνητικό ακέραιο l. Αφού $r < m^k$ ισχύει $l < k$. Από την επαγωγική υπόθεση η $P(l)$ ισχύει, άρα ο r έχει μια m-αδική αναπαράσταση της μορφής

$$r = a_0 + a_1 m + \cdots + a_{k-1} m^{k-1},$$

όπου $0 \leq a_i \leq m - 1$ για κάθε $i = 0, 1, \ldots, k - 1$. Τότε ο n αναπαρίσταται στη μορφή

$$n = a_0 + a_1 m + \cdots + a_{k-1} m^{k-1} + a_k m^k.$$

Από το Λήμμα 2.1 κάθε φυσικός αριθμός n ανήκει σε κάποιο διάστημα της μορφής $[m^k, m^{k+1})$, άρα προκύπτει ότι κάθε θετικός ακέραιος έχει m-αδική γραφή.

Τώρα θα δείξουμε την μοναδικότητα της m-αδικής γραφής. Υποθέτουμε ότι δεν ισχύει και θα καταλήξουμε σε αντίφαση. Έστω n ο ελάχιστος θετικός ακέραιος για τον οποιό η m-αδική γραφή δεν είναι μοναδική και

$$n = b_0 + b_1 m + \cdots + b_s m^s \tag{2.4}$$

μια άλλη διαφορετική από την (2.2) m-αδική αναπαράσταση του n, όπου $0 \leq b_j \leq m - 1$ για κάθε $j = 0, 1, \ldots, s$ και $b_s \geq 1$. Αν $s \geq k + 1$, τότε

$$n < m^{k+1} \leq b_s m^s \leq n,$$

το οποίο δεν μπορεί να συμβαίνει. Άρα $k \leq s$. Με ανάλογο επιχείρημα δείχνουμε $s \leq k$. Άρα, $k = s$. Αν $a_k < b_k$, τότε

$$\begin{aligned} n &= a_0 + a_1 m + \cdots + a_{k-1} m^{k-1} + a_k m^k \\ &\leq (m-1) + (m-1)m + \cdots + (m-1)m^{k-1} + a_k m^k \\ &= (m^k - 1) + a_k m^k \\ &< (a_k + 1)m^k \ \leq \ b_k m^k \leq \ n, \end{aligned}$$

το οποίο είναι αδύνατο. Άρα, $b_k \leq a_k$. Με ανάλογο επιχείρημα δείχνουμε ότι $a_k \leq b_k$, άρα $a_k = b_k$. Τότε

$$\begin{aligned} n - a_k m^k &= a_0 + a_1 m + a_2 m^2 + \cdots + a_{k-1} m^{k-1} \\ &= b_0 + b_1 m + b_2 m^2 + \cdots + b_{k-1} m^{k-1} \end{aligned}$$

Αφού $n - a_k m^k < n$ και ο n έχει επιλεγεί σαν ο ελάχιστος θετικός ακέραιος που δεν έχει μοναδική m-αδική γραφή έχουμε $a_i = b_i$ για κάθε $i = 0, 1, \ldots, k - 1$. Αυτό όμως είναι αντίφαση, γιατί υποθέσαμε ότι οι m-αδικές αναπαραστασεις (2.4) και (2.2) του n είναι διαφορετικές μεταξύ τους. ■

Παράδειγμα 2.3. (1) *2-αδική αναπαράσταση του* 100:

Έχουμε

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 16, \quad 2^5 = 32, \quad 2^6 = 64, \quad 2^7 > 100.$$

Επομένως

$$100 = 2^6 + 36 = 2^6 + 2^5 + 4 = 2^6 + 2^5 + 2^2.$$

Σαν συνέπεια τα 2-δικά ψηφία του 100 είναι $(1, 1, 0, 0, 1, 0, 0)$.

(2) 3-*αδική αναπαράσταση του* 100:

Έχουμε

$$3^1 = 3, \quad 3^2 = 9, \quad 3^3 = 27, \quad 3^4 = 81, \quad 3^5 > 100.$$

Επομένως

$$100 = 3^4 + 19 = 3^4 + 2 \cdot 3^2 + 1 = 3^4 + 2 \cdot 3^2 + 3^0.$$

Σαν συνέπεια τα 3-δικά ψηφία του 100 είναι $(1, 0, 2, 0, 1)$. $\surd$

Στην επόμενη ενότητα θα μας απασχολήσουν κριτήρια διαιρετότητας ακέραιων αριθμών και σ' αυτό το πλαίσιο θα χρησιμοποιήσουμε την δεκαδική παράσταση ενός ακέραιου αριθμού.

3. **Το Λήμμα του Ευκλείδη**

Στην παρούσα ενότητα θα δούμε μια ενδιαφέρουσα απόδειξη του Λήμματος του Ευκλείδη.

Θεώρημα 3.1 (Λήμμα του Ευκλείδη). *Έστω $a, b \in \mathbb{Z}$ και p ενας πρώτος αριθμός. Τότε:*

$$p \mid ab \quad \Longrightarrow \quad p \mid a \quad \text{ή} \quad p \mid b$$

Απόδειξη. Προφανώς το συμπέρασμα ισχύει αν $a = 0$ ή $b = 0$. Επομένως μπορούμε να υποθέσουμε ότι $a \neq 0 \neq b$.

Επειδή για έναν ακέραιο x ισχύει: $p \mid x$ αν και μόνον αν $p \mid |x|$, μπορούμε να υποθέσουμε ότι $a, b \in \mathbb{N}$.

Θεωρούμε το σύνολο των θετικών ακεραίων x των οποίων το πολλαπλάσιο με τον a διαιρείται από τον πρώτο p:

$$X = \{x \in \mathbb{N} \mid p \mid ax\}$$

Επειδή από την υπόθεση $p \mid ab$, έπεται ότι $b \in X$ και άρα το σύνολο X είναι ένα μη-κενό υποσύνολο του $\mathbb{N}$.

Από την Αρχή Καλής Διάταξης, έπεται ότι το X έχει ελάχιστο στοιχείο, έστω θ:

$$\theta := \min X, \quad \text{δηλαδή:} \quad p \mid a\theta \quad \text{και} \quad x \in \mathbb{N} \ \ \& \ \ p \mid ax \quad \Longrightarrow \quad \theta \leq x$$

Θα δείξουμε ότι $\forall x \in X\colon\ \theta \mid x$. Πράγματι από την Ευκλείδεια Διαίρεση του x με το θ, θα έχουμε:

$$x = \theta q + r, \qquad 0 \leq r < \theta$$

Τότε $ax = a\theta q + ar$. Επειδή $x \in X$, θα έχουμε $p \mid ax$. Επειδή $\theta \in X$, θα έχουμε $p \mid a\theta$ και επομένως $p \mid a\theta q$. Τότε:

$$p \mid ax \quad \& \quad p \mid a\theta q \qquad \Longrightarrow \qquad p \mid ax - a\theta q = ar$$

Αν $r \neq 0$, τότε επειδή $p \mid ar$, θα έχουμε $r \in X$ και επομένως $\theta \leq r$ το οποίο είναι άτοπο διότι $r < \theta$. Άρα $r = 0$ και επομένως $x = \theta q$ και άρα $\theta \mid x$, $\forall x \in X$.

Ιδιαίτερα $\theta \mid p$ διότι $p \in X$. Επειδή ο p είναι πρώτος, έπεται ότι είτε $\theta = 1$ ή $\theta = p$. Αν $\theta = 1$, τότε επειδή $p \mid a\theta$, θα έχουμε $p \mid a$. Αν $p = \theta$, τότε επειδή $\theta \mid x$, $\forall x \in X$ και $b \in X$, έπεται ότι $p \mid b$. ■

Ως άμεση συνέπεια έχουμε το ακόλουθο πόρισμα το οποίο είναι επίσης γνωστό ως Λήμμα του Ευκλείδη.

Πόρισμα 3.2. *Έστω p ένας πρώτος αριθμός και $a, b \in \mathbb{Z}$. Τότε:*

$$p \mid ab \quad \& \quad (p, a) = 1 \qquad \Longrightarrow \qquad p \mid b$$

4. **Κριτήρια Διαιρετότητας**

Έστω $a > 1$ ένας φυσικός αριθμός και έστω η παράσταση του

$$a = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0, \qquad a_m \neq 0 \quad \text{και} \quad 0 \leq a_i \leq 9, \;\; 0 \leq i \leq m$$

στο δεκαδικό σύστημα. Θέτοντας

$$a^* = a_m 10^{m-1} + a_{m-1}10^{m-2} + \cdots + a_2 10 + a_1$$

έχουμε τα ακόλουθα κριτήρια διαιρετότητας:

Θεώρημα 4.1. *Αν* $a = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$ *είναι όπως παραπάνω, τότε:*

1.
$$2 \mid a \iff 2 \mid a_0$$

2.
$$3 \mid a \iff 3 \mid a_0 + a_1 + \cdots + a_m$$

3.
$$4 \mid a \iff 4 \mid a_1 10 + a_0$$

4.
$$5 \mid a \iff 5 \mid a_0$$

5.
$$6 \mid a \iff 2 \mid a_0 \;\; \& \;\; 3 \mid a_0 + a_1 + \cdots + a_m$$

6.
$$7 \mid a \iff 7 \mid a^* - 2a_0$$

7.
$$8 \mid a \iff 8 \mid a_2 10^2 + a_1 10 + a_0$$

8.
$$9 \mid a \iff 9 \mid a_0 + a_1 + \cdots + a_m$$

9.
$$10 \mid a \iff a_0 = 0$$

10.
$$11 \mid a \iff 11 \mid a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^m a_m$$

11.
$$13 \mid a \iff 13 \mid 9a_0 - a^*$$

12.
$$25 \mid a \iff 25 \mid a_1 10 + a_0$$

Απόδειξη. **1.** Επειδή $2 \mid 10^k$, $\forall k \geq 1$, έπεται ότι

$$2 \mid a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10$$

και επομένως:

$$2 \mid a \iff 2 \mid a - (a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10) \iff 2 \mid a_0$$

2. Επειδή $10^k = (9+1)^k = \sum_{i=0}^{k} \binom{k}{i} 9^i = 9x_k + 1$, όπου $x_k = \sum_{i=1}^{k} \binom{k}{i} 9^{i-1}$. Επομένως:

$$\begin{aligned} a &= a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0 \\ &= a_m(9x_m+1) + a_{m-1}(9x_{m-1}+1) + \cdots + a_1(9x_1+1) + a_0 \\ &= 9A + (a_m + a_{m-1} + \cdots + a_1 + a_0), \qquad \text{όπου} \qquad A = a_m x_m + a_{m-1}x_{m-1} + \cdots a_1 x_1 \end{aligned}$$

Επομένως, επειδή $3 \mid 9A$, θα έχουμε:

$$3 \mid a \iff 3 \mid a_m + a_{m-1} + \cdots + a_1 + a_0$$

3. Επειδή $100 = 4 \cdot 25$, έπεται ότι $4 \mid 10^2$ και άρα $4 \mid 10^k$, $\forall k \geq 2$. Επομένως $4 \mid a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_2 10^2$. Θέτοντας $A = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_2 10^2$, θα έχουμε $a = A + a_1 10 + a_0$, και επειδή $4 \mid A$, θα έχουμε:

$$4 \mid a \iff 4 \mid a - A \iff 4 \mid a_1 10 + a_0$$

4. Επειδή $5 \mid 10^k$, $\forall k \geq 1$, έπεται ότι

$$5 \mid a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10$$

και επομένως:

$$5 \mid a \iff 5 \mid a - (a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10) \iff 5 \mid a_0$$

5. Αν $6 \mid a$, τότε προφανώς $2 \mid a$ και $3 \mid a$, και από τα **1.** και **2.** θα έχουμε ότι $2 \mid a_0$ και $3 \mid a_m + a_{m-1} + \cdots + a_1 + a_0$. Αντίστροφα αν $2 \mid a_0$ και $3 \mid a_m + a_{m-1} + \cdots + a_1 + a_0$, τότε $2 \mid a$ και $3 \mid a$ και άρα $a = 2\kappa = 3\lambda$. Προφανώς τότε ο αριθμός λ είναι άρτιος και επομένως $\lambda = 2\mu$. Τότε $a = 6\mu$ και άρα $6 \mid a$.

6. Βλέπε την Πρόταση 4.2 παρακάτω.

7. Η απόδειξη είναι παρόμοια με την απόδειξη του κριτηρίου διαιρετότητας με το 4. Επειδή $1000 = 8 \cdot 25$, έπεται ότι $8 \mid 10^k$, $\forall k \geq 3$. Επομένως $4 \mid a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_3 10^3$. Θέτοντας $A = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_3 10^3$, θα έχουμε $a = A + a_2 10^3 + a_1 10 + a_0$, και επειδή $4 \mid A$, θα έχουμε:

$$8 \mid a \iff 8 \mid a - A \iff 4 \mid a_2 10^3 + a_1 10 + a_0$$

8. Η απόδειξη είναι παρόμοια με την απόδειξη του κριτηρίου διαιρετότητας με το 3. Στο **2**. δείξαμε ότι $a = 9A + (a_m + a_{m-1} + \cdots + a_1 + a_0)$, όπου $A = a_m x_m + a_{m-1}x_{m-1} + \cdots a_1 x_1$. Έτσι, επιειδή $9 \mid 9A$, έπεται ότι θα έχουμε:

$$9 \mid a \iff 9 \mid a_m + a_{m-1} + \cdots + a_1 + a_0$$

9. Η απόδειξη είναι άμεση.

10. Για την απόδειξη, βλέπε την Πρόταση 4.3 παρακάτω.

11. Για την απόδειξη, βλέπε την Πρόταση 4.4 παρακάτω.

12. Η απόδειξη είναι παρόμοια με την απόδειξη των κριτηρίων διαιρετότητας με το 4ή το 8 χρησιμοποιώντας ότι, επειδή $100 = 4 \cdot 25$, έχουμε $25 \mid 10^k$, $\forall k \geq 2$. ■

Οι ακόλουθες τρεις προτασεις είναι αφιερωμένες στην απόδειξη των κριτηρίων διαιρετότητας με τυς αριθμούς 7, 11, και 13.

Πρόταση 4.2. *Έστω $a > 1$ ένας φυσικός αριθμός και έστω η παράσταση του*

$$a = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0, \qquad a_m \neq 0 \quad \textit{και} \quad 0 \leq a_i \leq 9, \;\; 0 \leq i \leq m$$

στο δεκαδικό σύστημα. Τότε:

$$7 \mid a \iff 7 \mid a^* - 2a_0$$

όπου:

$$a^* = a_m 10^{m-1} + a_{m-1}10^{m-2} + \cdots + a_2 10 + a_1$$

Απόδειξη. Παρατηρούμε ότι

$$a = 10 \cdot a^* + a_0$$

• Υποθέτουμε πρώτα ότι $7 \mid a^* - 2a_0$. Τότε $a^* - 2a_0 = 7k$, για κάποιον θετικό ακέραιο k και επομένως

$$10 \cdot a^* - 20a_0 = 710k \implies 10 \cdot a^* + a_0 - 21a_0 = 7(10k) \implies a = 7(10k) + 21a_0 \implies$$

$$\implies a = 7(10k + 3a_0) \implies 7 \mid a$$

• Υποθέτουμε ότι $7 \mid a$. Τότε $a = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0 = 7b$, για κάποιον θετικό ακέραιο b, και επομένως:

$$10(a_m 10^{m-1} + a_{m-1}10^{m-2} + \cdots + a_2 10 + a_1) + a_0 = 7b \implies 10a^* = 7b - a_0 \implies$$

$$\implies 10a^* = 7b + 20a_0 - 21a_0 \implies 10a^* - 20a_0 = 7(b - 3a_0) \implies 10(a^* - 2a_0) = 7(b - 3a_0)$$

Επειδή ο 7 είναι πρώτος και, όπως προκύπτει από την παραπάνω σχέση, $7 \mid 10(a^* - 2a_0)$, και επειδή $7 \nmid 10$, από το Λήμμα του Ευκλείδη θα έχουμε $7 \mid a^* - 2a_0$. ■

Πρόταση 4.3. **1.** *Για κάθε περιττό φυσικό αριθμό n ισχύει:*

$$11 \mid 10^n + 1$$

2. *Για κάθε άρτιο φυσικό αριθμό n:*

$$11 \mid 10^n - 1$$

3. *Έστω $a > 1$ ένας φυσικός αριθμός και έστω η παράσταση του*

$$a = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0, \qquad a_m \neq 0 \quad \textit{και} \quad 0 \leq a_i \leq 9, \;\; 0 \leq i \leq m$$

στο δεκαδικό σύστημα. Τότε:

$$11 \mid a \iff 11 \mid a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^m a_m$$

Απόδειξη. **1.** Γράφουμε $n = 2k + 1$ όπου $k \geq 0$. Έχουμε $10^n + 1 = 10^{2k+1} + 1$. Θα χρησιμοποιήσουμε την Αρχή Μαθηματικής Επαγωγής. Ορίζουμε $P(k)$ να είναι η Πρόταση

$$11 \mid 10^{2k+1} + 1$$

Έχουμε ότι η $P(0)$ ισχύει, γιατί το 11 διαιρεί το 11. Υποθέτουμε ότι $k \geq 0$ και ότι η $P(k)$ ισχύει, δηλαδή ότι το 11 διαιρεί το $10^{2k+1} + 1$. Θα δείξουμε την $P(k+1)$, δηλαδή ότι το 11 διαιρεί το $10^{(2(k+1)+1)} + 1 = 10^{2k+3} + 1$. Πράγματι, έχουμε

$$10^{2k+3} + 1 = 100 \cdot 10^{2k+1} + 1 = (99 + 1) \cdot 10^{2k+1} + 1 = 11 \cdot (9 \cdot 10^{2k+1}) + (10^{2k+1} + 1)$$

Χρησιμοποιώντας ότι το 11 διαιρεί το $10^{2k+1} + 1$ έχουμε ότι το 11 διαιρεί $10^{2k+3} + 1$. Άρα η $P(k+1)$ ισχύει. Επομένως σύμφωνα με την Αρχή Μαθηματικής Επαγωγής αυτό που θέλουμε να δείξουμε ισχύει για κάθε $k \geq 0$.

2. Γράφουμε $n = 2k$ όπου $k \geq 1$. Έχουμε $10^n - 1 = 10^{2k} - 1$. Θα χρησιμοποιήσουμε την Αρχή Μαθηματικής Επαγωγής. Ορίζουμε $Q(k)$ την Πρόταση

$$11 \mid 10^{2k} - 1$$

Έχουμε ότι η $Q(1)$ ισχύει, γιατί το 11 διαιρεί το $10^2 - 1 = 99$. Υποθέτουμε ότι $k \geq 1$ και ότι η $Q(k)$ ισχύει, δηλαδή ότι το 11 διαιρεί το $10^{2k} - 1$. Θα δείξουμε την $Q(k+1)$, δηλαδή ότι το 11 διαιρεί το $10^{2(k+1)} - 1 = 10^{2k+2} - 1$. Πράγματι, έχουμε

$$10^{2k+2} - 1 = 100 \cdot 10^{2k} - 1 = (99+1) \cdot 10^{2k} - 1 = 11 \cdot (9 \cdot 10^{2k}) + (10^{2k} - 1)$$

Χρησιμοποιώντας ότι το 11 διαιρεί το $10^{2k} - 1$ έχουμε ότι το 11 διαιρεί $10^{2k+2} - 1$. Συνεπώς η $Q(k+1)$ ισχύει. Άρα σύμφωνα με την Αρχή Μαθηματικής Επαγωγής αυτό που θέλουμε να δείξουμε ισχύει για κάθε $k \geq 1$.

3. Θέτουμε

$$A = a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^m a_m$$

Έχουμε

$$\begin{aligned} a &= a_0 + a_1 \cdot 10 + a_1 - a_1 + a_2 \cdot 10^2 + a_2 - a_2 + \cdots\cdots + a_m \cdot 10^m + a_m - a_m \\ &= A + a_1(10+1) + a_2(10^2 - 1) + a_3(10^3 + 1) + \cdots + a_m(10^m - (-1)^{m+1})) \end{aligned}$$

Χρησιμοποιώντας τα μέρη **1**. και **2**. έχουμε ότι ο 11 διαιρεί τον

$$a_1(10+1) + a_2(10^2 - 1) + a_3(10^3 + 1) + \cdots + a_m(10^m - (-1)^m))$$

Επομένως ο 11 διαιρεί τον a αν και μόνο αν διαιρεί τον A. ■

Πρόταση 4.4. *Έστω $a > 1$ ένας φυσικός αριθμός και έστω η παράσταση του*

$$a = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0, \qquad a_m \neq 0 \quad \textit{και} \quad 0 \leq a_i \leq 9, \;\; 0 \leq i \leq m$$

στο δεκαδικό σύστημα. Τότε:

$$13 \mid a \iff 13 \mid a^* - 9a_0$$

όπου:

$$a^* = a_m 10^{m-1} + a_{m-1} 10^{m-2} + \cdots + a_2 10 + a_1$$

Απόδειξη. Όπως και στην Πρόταση 4.2, παρατηρούμε ότι: Παρατηρούμε ότι

$$a = 10 \cdot a^* + a_0$$

- Υποθέτουμε πρώτα ότι $13 \mid a^* - 9a_0$. Τότε $a^* - 9a_0 = 13k$, για κάποιον θετικό ακέραιο k και επομένως

$$10 \cdot a^* - 90a_0 = 1310k \implies 10 \cdot a^* + a_0 - 91a_0 = 13(10k) \implies a = 13(10k) + 91a_0 \implies$$

$$\implies a = 13(10k + 7a_0) \implies 13 \mid a$$

- Υποθέτουμε ότι $13 \mid a$. Τότε $a = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0 = 13b$, για κάποιον θετικό ακέραιο b, και επομένως:

$$10(a_m 10^{m-1} + a_{m-1} 10^{m-2} + \cdots + a_2 10 + a_1) + a_0 = 13b \implies 10a^* = 13b - a_0 \implies$$

$$\implies 10a^* = 13b + 90a_0 - 91a_0 \implies 10a^* - 90a_0 = 13(b - 7a_0) \implies 10(a^* - 9a_0) = 13(b - 3a_0)$$

Επειδή ο 13 είναι πρώτος και, όπως προκύπτει από την παραπάνω σχέση, $13 \mid 10(a^* - 9a_0)$, και επειδή $13 \nmid 10$, από το Λήμμα του Ευκλείδη θα έχουμε $13 \mid a^* - 9a_0$. ■

Σημειώνουμε ότι ισχύει ένα γενικότερο κριτήριο διαιρετότητας. Για να το διατυπώσουμε και να το αποδείξουμε, πρώτα χρειαζόμαστε το ακόλουθο απλό Λήμμα.

Λήμμα 4.5. *Έστω $m > 1$ ένας θετικός ακέραιος και υποθέτουμε ότι $(10, m) = 1$. Τότε υπάρχει $b \in \mathbb{N}$ έτσι ώστε: $m \mid 10b - 1$. Αν b' είναι ένας άλλος ακέραιος έτσι ώστε $m \mid 10b' - 1$, τότε $b' = b - mr$, για κάποιον ακέραιο r.*

Απόδειξη. Επειδή $(10, m) = 1$, έπεται ότι υπάρχουν ακέραιοι x, b έτσι ώστε $xm + 10b = 1$. Τότε $10b - 1 = (-x)m$ και επομένως $m \mid 10b - 1$.

Έστω b και b' δύο ακέραιοι έτσι ώστε $m \mid 10b - 1$ και $vm \mid 10b' - 1$. Τότε $10b - 1 = km$ και $10b' - 1 = lm$, και επομένως $10(b' - b) = (l - k)m$. Δηλαδή $m \mid 10(b' - b)$ και επειδή $(m, 10) = 1$, θα έχουμε $m \mid b' - b$ και άρα $b' - b = rm$για κάπιον ακέραιο r. Έτσι τελικά $b' = b + rm$. ■

Θεώρημα 4.6. *[K. Conrad] Έστω $a > 1$ ένας φυσικός αριθμός και*

$$a = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0, \qquad a_m \neq 0 \quad \text{και} \quad 0 \leq a_i \leq 9, \;\; 0 \leq i \leq m$$

η παράσταση του στο δεκαδικό σύστημα. Έστω επίσης $k > 1$ ένας θετικός ακέραιος έτσι ώστε $(10, k) = 1$, και έστω $b \in \mathbb{N}$ ένας αριθμός για τον οποίο ισχύει $k \mid 10b - 1$, βλέπε Λήμμα 4.5. Τότε:

$$k \mid a \iff k \mid a^* + ba_0$$

όπου:

$$a^* = a_m 10^{m-1} + a_{m-1}10^{m-2} + \cdots + a_2 10 + a_1$$

Απόδειξη. Όπως και στην Πρόταση 4.2, παρατηρούμε ότι:

$$a = 10 \cdot a^* + a_0$$

Επειδή $k \mid 10b - 1$, έπεται ότι

$$10b - 1 = kr \quad \text{για κάποιον ακέραιο} \quad r \quad \text{και άρα} \quad 10ba_0 - a_0 = kra_0$$

- Υποθέτουμε πρώτα ότι $k \mid a^* + ba_0$. Τότε $a^* + ba_0 = ks$, για κάποιον θετικό ακέραιο s και επομένως

$$10 \cdot a^* + 10ba_0 = k10s \implies 10 \cdot a^* = k(10s) - 10ba_0 \implies 10a^* = k(10s) - (rk + 1)a_0 \implies$$
$$\implies 10a^* = k(10s) - rka_0 - a_0 \implies a = 10a^* + a_0 = k(10s - ra_0) \implies k \mid a$$

- Υποθέτουμε ότι $k \mid a$. Τότε $a = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0 = ks$, για κάποιον θετικό ακέραιο s, και επομένως:

$$10(a_m 10^{m-1} + a_{m-1}10^{m-2} + \cdots + a_2 10 + a_1) + a_0 = ks \implies 10a^* = ks - a_0 \implies$$
$$\implies 10a^* = ks + kra_0 - 10ba_0 \implies 10a^* + 10ba_0 = k(s + ra_0) \implies 10(a^* + ba_0) = k(s + ra_0)$$

Όπως προκύπτει από την παραπάνω σχέση, θα έχουμε $k \mid 10(a^* + ba_0)$ και άρα επειδή $(k, 10) = 1$, από το Λήμμα του Ευκλείδη θα έχουμε $k \mid a^* + ba_0$. ■

Παράδειγμα 4.7. Διατηρώντας τους συμβολισμούς του Θεωρήματος 4.1, θα έχουμε:

(1) Ο 7 διαιρεί τον αριθμό $a = 826 = 8 \cdot 10^2 + 2 \cdot 10 + 6$ διότι $a^* = 8 \cdot 10 + 2 = 82$ και $2a_0 = 2 \cdot 6 = 12$. Έτσι

$$a^* - 2a_0 = 82 - 12 = 70 \implies 7 \mid a^* - 2a_0 \implies 7 \mid a = 826$$

Πράγματι: $826 = 7 \cdot 118$.

(2) Ο 11 διαιρεί τον αριθμό $a = 8703585473$, γιατί ο 11 διαιρεί τον

$$a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^m a_m = 3 - 7 + 4 - 5 + 8 - 5 + 3 - 0 + 7 - 8 = 0$$

Πράγματι: $8703585473 = 11 \cdot 791235043$.

(3) Ο 13 διαιρεί τον αριθμό $a = 50661 = 5\cdot 10^4+6\cdot 10^2+6\cdot 10+1$ διότι $a^* = 5\cdot 10^2+6\cdot 10+6 = 5066$ και $9a_0 = 9\cdot 1 = 9$. Έτσι

$$a^* - 9a_0 = 5066 - 9 = 5057 \quad \text{και} \quad 13 \mid 5057, \quad \text{διότι} \quad 5057 = 13\cdot 389, \quad \Longrightarrow \quad 13 \mid 50661$$

Πράγματι: $50661 = 13\cdot 3897$. $\surd$

Παρατήρηση 4.8. Ο παρακάτω πίνακας δίνει τιμές για τον ακέραιο αριθμό b έτσι ώστε, βλέπε Λήμμα 4.5:

$$k \mid 10b - 1$$

k	b
3	1
7	-2
9	1
11	-1
13	4
17	-5
19	2
21	-2
23	7
27	-8
29	3
31	-3
33	10
37	-11
39	4
41	-4
43	13
47	-14
49	5

Θέτοντας, στο Θεώρημα 4.6, $k = 3, 7, 9, \cdots$ και b να είναι η αντίστοιχη τιμή από τον παραπάνω πίνακα, αποκτούμε κριτήρια διαιρετότητας για τους αριθμούς $k = 3, 7, 9, \cdots$. $\surd$

Παράδειγμα 4.9. Έτσι για παράδειγμα εφαρμόζοντας το Θεώρημα 4.6 για $k = 19$, $k = 29$ και $k = 37$, αποκτούμε τα ακόλουθα κριτήρια διαιρετότητας με τα 19, 29 και 37:

Έστω $a > 1$ ένας φυσικός αριθμός και

$$a = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0, \qquad a_m \neq 0 \quad \text{και} \quad 0 \leq a_i \leq 9, \;\; 0 \leq i \leq m$$

η παράσταση του στο δεκαδικό σύστημα. Έστω επίσης:

$$a^* = a_m 10^{m-1} + a_{m-1}10^{m-2} + \cdots + a_2 10 + a_1$$

- <u>Κριτηριο διαιρετοτητας με το 19:</u> *Ισχύει ότι:*

$$19 \mid a \quad \Longleftrightarrow \quad 19 \mid a^* + 2a_0$$

- Κριτηριο διαιρετοτητας με το 29: *Ισχύει ότι:*
$$29 \mid a \iff 29 \mid a^* + 3a_0$$
- Κριτηριο διαιρετοτητας με το 37: *Ισχύει ότι:*
$$37 \mid a \iff 37 \mid a^* - 11a_0 \quad \surd$$

Παράδειγμα 4.10. Εξετάζουμε την διαιρετότητα του αριθμού 101156 με τον αριθμό 19.
Θα έχουμε
$$a = 101156 = 1 \cdot 10^5 + 0 \cdot 10^4 + 1 \cdot 10^3 + 1 \cdot 10^2 + 5 \cdot 10 + 6 \quad \& \quad a_0 = 6$$
$$a^* = 101156 = 1 \cdot 10^4 + 0 \cdot 10^3 + 1 \cdot 10^2 + 1 \cdot 10 + 5 = 10115$$
Άρα
$$a^* + 2a_0 = 10115 + 2 \cdot 6 = 10115 + 12 = 10127$$
Επειδή $10127 = 19 \cdot 533$, έπεται ότι:
$$19 \mid 10127 \quad \Longrightarrow \quad 19 \mid 101156 \quad \surd$$

5. **Η Εικασία του Bertrand και η Κατανομή των Πρώτων Αριθμών**

Σκοπός της παρούσης ενότητας είναι η απόδειξη ενός σημαντικού αποτελέσματος στην Θεωρία Αριθμών το οποίο είναι γνωστό ως Εικασία του Bertrand (Bertrand Conjecture ή Bertrand Postulate). Θα δούμε επίσης κάποιες ενδιαφέρουσες συνέπειες στην κατανομή των πρώτων αριθμών.

5.1. **Η Εικασία του Bertrand.** Η ακόλουθη Εικασία του Bertrand (Bertrand Conjecture ή Bertrand Postulate) μας δίνει ένα μέτρο της πυκνότητας των πρώτων αριθμών στο σύνολο όλων των φυσικών αριθμών.

Θεώρημα 5.1. *(*Εικασια του Bertrand*) Για κάθε φυσικό αριθμό $n \neq 1$, υπάρχει πρώτος p έτσι ώστε:*

$$n \ < \ p \ < \ 2n \tag{5.1}$$

Σχόλιο 5.2. Ο ισχυρισμός της εικασίας του Bertrand επαληθεύεται εύκολα για μικρές τιμές του n:

$$\begin{array}{lcll} p & = & 3 & \text{αν} \quad n = 2 \\ p & = & 5 & \text{αν} \quad n = 3 \\ p & = & 7 & \text{αν} \quad 4 \leq n \leq 6 \\ p & = & 13 & \text{αν} \quad 7 \leq n \leq 12 \\ p & = & 23 & \text{αν} \quad 13 \leq n \leq 22 \\ p & = & 43 & \text{αν} \quad 23 \leq n \leq 42 \\ p & = & 83 & \text{αν} \quad 43 \leq n \leq 82 \\ p & = & 131 & \text{αν} \quad 83 \leq n \leq 127 \end{array}$$

Σχόλιο 5.3. Τον ισχυρισμό ότι για κάθε φυσικό αριθμό $n \neq 1$, υπάρχει πρώτος p έτσι ώστε $n \ < \ p \ < \ 2n$, διατύπωσε το 1845 ο Γάλλος Μαθηματικός Joseph Bertrand (1822-1900), ο οποίος επαλήθευσε το ισχυρισμό για φυσικούς αριθμούς $\leq 3.000.000$.

Ο ισχυρισμός αποδείχθηκε για κάθε φυσικό αριθμό από τον Ρώσο Μαθηματικό P.L. Chebyshev (1821-1894) το 1850, με χρήση μεθόδων της Ανάλυσης. Αργότερα δώθηκαν απλούστερες αποδείξεις, για παράδειγμα από τους Erdös και Ramanujan, καθώς και βελτιωμένες εκδοχές της εικασίας του Bertrand.

Εδώ θα παρουσιάσουμε μια παραλλαγή της απόδειξης του Erdös, στην πρώτη εργασία που δημοσίευσε το 1931.

Για την απόδειξη του Θεωρήματος 4.1, η οποία δεν είναι εύκολη, θα χρειασθούμε κάποια προκαταρκτικά βοηθητικά αποτελέσματα, τα οποία έχουν ενδιαφέρον και από μόνα τους.

Λήμμα 5.4. *Έστω $n \geq 2$ ένας φυσικός αριθμός. Έστω $p_1, p_2, \cdots, p_k$ όλοι οι πρώτοι αριθμοί οι οποίοι είναι μικρότεροι ή ίσοι του n. Τότε:*

$$\prod_{i=1}^{k} p_i = p_1 \cdot p_2 \cdot \cdots \cdot p_k \ \leq \ 4^n \tag{5.2}$$

Απόδειξη. Παρατηρούμε ότι: για $n = 2$ έχουμε $k = 1$ και $p_1 = 2 < 4^2 = 4$.

Για $n = 3$, έχουμε $k = 2$ και $p_1 = 2$ και $p_2 = 3$. Τότε $p_1 p_2 = 2 \cdot 3 = 6 < 4^3 = 48$.

Επομένως η ζητούμενη σχέση (4.2) αληθεύει, όταν $n = 2, 3$.

Η απόδειξη για κάθε $n > 3$ θα γίνει πρώτα στην περίπτωση κατά την οποία ο αριθμός n είναι περιττός και ακολούθως στην περίπτωση κατά την οποία ο n είναι άρτιος.

Υποθέτουμε ότι ο αριθμός n είναι περιττός. Θα δείξουμε το ζητούμενο με χρήση Αρχής Μαθηματικής Επαγωγής.

- Όπως είδαμε παραπάνω, για $n = 3$ η ζητούμενη σχέση ισχύει.
- ΕΠΑΓΩΓΙΚΗ ΥΠΟΘΕΣΗ: Υποθέτουμε ότι για n περιττό και $n > 3$ ισχύει:

$$\prod_{j=1}^{k} p_i = p_1 \cdot p_2 \cdot \cdots \cdot p_j \ \leq \ 4^n, \qquad \forall\, j: \ \text{περιττός} \ \ \text{και} \ \ 3 < j < n$$

Θα δείξουμε πρώτα ότι ισχύει η ζητούμενη σχέση για την περίπτωση n περιττός.

Επειδή ο n είναι περιττός έπεται ότι θα είναι της μορφής $n = 2\lambda + 1$ για κάποιον φυσικό αριθμό λ. Τότε

$$\frac{n+1}{2} = \frac{2(\lambda+1)}{2} = \lambda + 1 \quad \text{και} \quad \frac{n-1}{2} = \frac{2\lambda}{2} = \lambda$$

Επομένως αν ο λ είναι άρτιος, τότε ο αριθμός $\frac{n+1}{2}$ είναι περιττός, και αν ο λ είναι περιττός, τότε ο αριθμός $\frac{n-1}{2}$ είναι περιττός. Θεωρούμε τον φυσικό αριθμό

$$k = \frac{n \pm 1}{2}$$

όπου διαλέγουμε το πρόσημο έτσι ώστε ο αριθμός k να είναι περιττός. Τότε προφανώς $k \geq 3$ και ο αριθμός $n - k \geq 1$ είναι άρτιος ως διαφορά περιττών.

Έστω p ένας πρώτος αριθμός έτσι ώστε $k < p \leq n$. Τότε ο p είναι περιττός διότι $p > k > 3$.

- ΙΣΧΥΡΙΣΜΟΣ:

$$p \mid n! \quad \text{και} \quad p \nmid k! \quad \text{και} \quad p \nmid (n-k)!$$

Πραγματικά, επειδή $p \leq n$, έπεται προφανώς ότι $p \mid n!$. Επίσης αν $p \mid k!$, τότε επειδή ο αριθμός p είναι πρώτος, θα έχουμε $p \mid a$ όπου $a \leq k$. Αυτό όμως είναι άτοπο διότι $k < p$. Έτσι πράγματι $p \nmid k!$. Παρόμοια βλέπουμε ότι $p \nmid (n-k)!$, διότι αν $p \mid (n-k)!$, τότε όπως και προηγούμενως θα έχουμε $p \mid a$ για κάποιο a με $1 \leq a \leq n-k$. Ιδιαίτερα $p \leq n-k$ και μάλιστα $p \leq n-k-1$, διότι αν $p = n-k$ τότε έπεται ότι ο p είναι άρτιος το οποίο είναι άτοπο. Έτσι $k < p \leq n-k-1$ και επομένως $n \geq 2k+1$. Αυτό είναι άτοπο όπως βλέπουμε εύκολα από την επιλογή του k, δηλαδή $k = \frac{n \pm 1}{2}$. Επομένως $p \nmid (n-k)!$.

- ΙΣΧΥΡΙΣΜΟΣ:

$$p \mid \binom{n}{k}$$

Πραγματικά από την Ευκλείδεια Διαίρεση θα έχουμε:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = pm + r, \qquad 0 \leq r < p$$

Τότε επειδή $p \mid n!$, θα έχουμε

$$n! = p\big(mk!(n-k)!\big) + k!(n-k)!r \implies n! - p\big(mk!(n-k)!\big) = k!(n-k)!r \implies$$

$$\implies p \mid k!(n-k)!r$$

και επειδή ο p είναι πρώτος και $p \nmid k!$ και $p \nmid (n-k)!$ θα έχουμε $p \mid r$ και αυτό είναι δυνατόν μόνο αν $r = 0$ διότι $r < p$. Άρα δείξαμε ότι

$$p \mid \binom{n}{k}, \quad \forall p \in \mathbb{P} \quad \& \quad k < p \leq n$$

Τότε όμως θα έχουμε και:

$$\prod_{k<p\leq n} p \mid \binom{n}{k} \quad \text{και επομένως} \quad \prod_{k<p\leq n} p \leq \binom{n}{k}$$

Επειδή

$$\binom{n}{k} = \binom{n}{n-k}$$

και οι παραπάνω διωνυμικοί συντελεστές εμφανίζονται στο διωνυμικό ανάπτυγμα

$$(1+1)^n = 2 \cdot 2^{n-1}$$

θα έχουμε προφανώς ότι

$$\prod_{k<p\leq n} p \leq 2^{n-1}$$

Χρησιμοποιώντας την Επαγωγικη Υποθεση, θα έχουμε:

$$\prod_{p\leq n} p = \prod_{p\leq k} p \prod_{k<p\leq n} p < 4^k 2^{n-1} = 2^{n+2k-1} \leq 2^{2n} = 4^n$$

Επομένως σύμφωνα με την Αρχή Μαθηματικής Επαγωγής η σχέση (4.2) ισχύει για κάθε n περιττό.

Μένει να δείξουμε την σχέση (4.2) για την περίπτωση κατά την οποία n είναι άρτιος. Σ΄ αυτή την περίπτωση ο πρώτος p δεν μπορεί να είναι ίσος με n και τότε επειδή ο $n-1$ είναι περιττός, από την παραπάνω ανάλυση θα έχουμε:

$$\prod_{p\leq n} p = \prod_{p\leq n-1} p < 4^{n-1} < 4^n$$

Επομένως δείξαμε ότι η σχέση (4.2) ισχύει για κάθε φυσικό αριθμό n. ■

Λήμμα 5.5. *Έστω $n \geq 3$ ένας φυσικός αριθμός, και έστω p ένας πρώτος αριθμός έτσι ώστε:*

$$\frac{2n}{3} < p \leq n$$

Τότε:

$$p \nmid \binom{2n}{n}$$

Απόδειξη. Επειδή $3p > 2n$, έπεται ότι οι αριθμοί p και $2p$ είναι τα μοναδικά ακέραια πολλαπλάσια του p τα οποία εμφανίζονται ως παράγοντες του $(2n)!$. Επομένως p^2 είναι η μεγαλύτερη δύναμη του p η οποία διαιρεί τον αριθμό $(2n)!$.

Παρόμοια επειδή $2p > n$, έπεται ότι p είναι η μεγαλύτερη δύναμη του p η οποία διαιρεί τον αριθμό $n!$ και άρα p^2 είναι η μεγαλύτερη δύναμη του p η οποία διαιρεί τον αριθμό $n!n!$.

Συνδυάζοντας τις παραπάνω παρατηρήσεις έπεται ότι

$$p \nmid \binom{2n}{n} = \frac{(2n)!}{n!n!}$$

■

Προχωρούμε τώρα στην απόδειξη τους Θεωρήματος 5.1.

Απόδειξη Θεωρήματος 5.1: Από το Σχόλιο 5.2 έπεται ότι το ζητούμενο ισχύει για κάθε φυσικό αριθμό $n \leq 127$.

Υποθέτουμε ότι $n \geq 128$, και έστω ότι δεν υπάρχει πρώτος αριθμός p έτσι ώστε: $n < p < 2n$.

Έστω

$$\binom{2n}{n} = \prod_{p \leq 2n} p^r$$

η πρωτογενής ανάλυση του αριθμού $\binom{2n}{n}$. Τότε:

(1) Επειδή, από την υπόθεσή μας, δεν υπάρχει κανένας πρώτος μεταξύ των n και $2n$, έπεται ότι η πρωτογενής ανάλυση του $\binom{2n}{n}$ θα είναι της μορφής:

$$\binom{2n}{n} = \prod_{p \leq n} p^r$$

(2) Αν p είναι ένας πρώτος στην παραπάνω πρωτογενή ανάλυση, και ισχύει $\frac{2n}{3} < p \leq n$, τότε από το Λήμμα 4.5, έπεται ότι θα έχουμε $p \nmid \binom{2n}{n}$. Τότε η πρωτογενής ανάλυση του $\binom{2n}{n}$ θα είναι της μορφής

$$\binom{2n}{n} = \prod_{p \leq \sqrt{2n}} p^r \cdot \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^r$$

(3) Επειδή όμως αν p είναι ένας πρώτος, όπου $\sqrt{2n} < p \leq \frac{2n}{3}$, έπεται ότι ο p είναι η μεγαλύτερη δύναμη του p η οποία διαιρεί τον $\binom{2n}{n}$. Επομένως για την πρωτογενή ανάλυση του $\binom{2n}{n}$ θα έχουμε

$$\binom{2n}{n} = \prod_{p \leq \sqrt{2n}} p^r \cdot \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^r \leq \prod_{p \leq \sqrt{2n}} 2n \cdot \prod_{p \leq \frac{2n}{3}} p$$

(4) Επειδή ο αριθμός των πρώτων $p \leq \sqrt{2n}$ είναι μικρότερος από τον αριθμό των περιττών $\leq \sqrt{2n}$, έπεται ότι θα έχουμε ότι αυτός ο αριθμός θα είναι μικρότερος από $\frac{\sqrt{2n}}{2} - 1 = \sqrt{\frac{n}{2}} - 1$. Επομένως θα έχουμε:

$$\prod_{p \leq \sqrt{2n}} 2n \leq (2n)^{\sqrt{\frac{n}{2}} - 1}$$

(5) Από το Λήμμα 4.4, έπεται ότι

$$\prod_{p \leq \frac{2n}{3}} p < 4^{\frac{2n}{3}}$$

(6) Συνδυάζοντας τις σχέσεις (3), (4), και (5), θα έχουμε:

$$\binom{2n}{n} < (2n)^{\sqrt{\frac{n}{2}} - 1} 4^{\frac{2n}{3}}$$

(7) Επειδή ο αριθμός $\binom{2n}{n}$ είναι ο μεγαλύτερος από τους $2n+1$ όρους στο διωνυμικό ανάπτυγμα $(1+1)^{2n}$, έπεται ότι

$$(2n+1)\binom{2n}{n} > (2n)\binom{2n}{n} > 2^{2n}$$

και άρα

$$\frac{2^{2n}}{2n} \;<\; \binom{2n}{n} \;<\; (2n)^{\sqrt{\frac{n}{2}}-1}\, 4^{\frac{2n}{3}}$$

και η τελευταία σχέση δίνει την σχέση

$$2^{\frac{2n}{3}} \;<\; (2n)^{\sqrt{\frac{n}{2}}}$$

(8) Παίρνοντας λογαρίθμους στην τελευταία σχέση και διαιρώντας με $\frac{\sqrt{2n}}{6}$, θα έχουμε:

$$\sqrt{8n}\log 2 - 2\log(2n) \;<\; 0$$

(9) Παραγωγίζοντας την συνάρτηση $f(x) = \sqrt{8x}\log 2 - 2\log(2x)$, θα έχουμε:

$$f'(n) = \frac{\sqrt{2n}\log 2 - 3}{n}$$

Επειδή $f(128) = 8\log 2 > 0$ και επειδή $f'(n) > 0$, $\forall n \geq 128$, έπεται ότι η συνάρτηση $f(n)$ είναι αύξουσα και επομένως θετική για $n \geq 128$:

$$f(n) = \sqrt{8n}\log 2 - 2\log(2n) > 0$$

(10) Οι σχέσεις στο (8) και (10) μας οδηγούν σε αντίφαση.

Επομένως η υπόθεση ότι $n \geq 128$, και δεν υπάρχει πρώτος αριθμός p έτσι ώστε: $n < p < 2n$, μας οδήγησε σε άτοπο. Άρα υπάρχει παντα ένας πρώτος αριθμός p έτσι ώστε: $n < p < 2n$, $\forall n \geq 1$. □

Υπενθυμίζουμε ότι, όπως έχουμε δείξει στο μάθημα, βλέπε (λυμένη) Άσκηση 11 του Φυλλαδίου Ασκήσεων **1**, ο n-οστός πρώτος αριθμός είναι μικρότερος ή ίσος από τον αριθμό $2^{2^{n-1}}$:

$$p_n \;\leq\; 2^{2^{n-1}}$$

Το ακόλουθο σημαντικό Θεώρημα είναι άμεση συνέπεια του Θεωρήματος 5.1, δίνει ένα πολύ καλύτερο φράγμα.

Θεώρημα 5.6. *Έστω $\mathbb{P} = \{p_1, p_2, \cdots, p_n, \cdots\}$ το σύνολο όλων των πρώτων αριθμών, εφοδιασμένο με την φυσική του διάταξη: $p_1 = 2, p_2 = 3, \cdots$, και $p_k < p_m$ όταν $k < m$. Τότε, $\forall n \in \mathbb{N}$:*

$$p_n \;\leq\; 2^n$$

Απόδειξη. Από το Θεώρημα 5.1 έπεται ότι, $\forall k \geq 2$:

$$\text{υπάρχει ένας πρώτος } \; p \; \text{ έτσι ώστε}: \quad 2^{k-1} < p < 2^k$$

Επομένως υπάρχουν το πολύ $k-1$ πρώτοι αριθμοί, χωρίς να λαμβάνουμε υπ' όψιν τον πρώτος 2, οι οποίοι είναι $\leq 2^k$. Επομένως υπάρχουν το πολύ k πρώτοι αριθμοί οι οποίοι είναι $\leq 2^k$. Δηλαδή:

$$p_n \;\leq\; 2^n$$

■

Επειδή προφανώς $p_n \neq 2^n$, όταν $n \neq 1$, από το Θεώρημα 5.6, έχουμε ότι:

$$p_n \;\leq\; 2^n - 1, \quad \forall n > 1$$

Για να φανεί πόσο καλύτερο είναι το φράγμα $p_n \leq 2^n$ του Θεωρήματος 5.6 από το φράγμα $p_n \leq 2^{2^{n-1}}$ το οποίο έχουμε αποδείξει στην τάξη, διαλέγουμε $n = 7$. Τότε $p_7 = 17$, δηλαδή ο 17 είναι ο 7ος πρώτος αριθμός. Επίσης το φράγμα του Θεωρήματος 5.6 είναι $x = 2^7 = 128$. Από την άλλη πλευρά το δεύτερο φράγμα είναι $2^{2^{7-1}} = 2^{2^6} = 2^{64} = 2^{7\cdot 9+1} = 2\cdot(2^7)^9 = 2x^9 = 2\cdot(128)^9$.

5.2. **Η Κατανομή των πρώτων αριθμών.** Υπενθυμίζουμε ότι η συνάρτηση η οποία μετράει το πλήθος των πρώτων αριθμών οι οποίοι είναι μικρότεροι από δοθέντα πραγματικό αριθμό ορίζεται ως εξής[2]:

$$\pi : \mathbb{R} \longrightarrow \mathbb{R}, \qquad \pi(x) = \left|\left\{p \in \mathbb{N} \mid p : \text{ πρώτος } \& \ p \leq x\right\}\right|$$

Το ακόλουθο σπουδαίο Θεώρημα των Πρώτων Αριθμών αναλύει την ασυμπτωτική συμπεριφορά της συνάρτησης $\pi(x)$.

Θεώρημα 5.7. *(*Θεωρημα των Πρωτων Αριθμων*)*

$$\lim_{x\to\infty}\pi(x)\frac{\log x}{x} = 1$$

Σχόλιο 5.8. (1) Από το Θεώρημα των Πρώτων Αριθμών έπεται ότι το κλάσμα $\frac{\pi(x)}{\frac{x}{\log x}}$ προσεγγίζει την τιμή 1 όταν ο πραγματικός αριθμός x τείνει στο άπειρο, δηλαδή όταν μεγαλώνει απεριόριστα. Με άλλα λόγια οι συναρτήσεις $\pi(x)$ και $\frac{x}{\log x}$ είναι ασυμπτωτικά ίσες, δηλαδή παίρνουν ίδιες τιμές για μεγάλη τιμή της μεταβλητής x. Αυτό το συμβολίζουμε με: $\pi(x) \sim \frac{x}{\log x}$, όταν $x \to \infty$.

(2) Από το Θεώρημα των Πρώτων Αριθμών προκύπτει ότι αν n είναι ένας αρκετά μεγάλος φυσικός αριθμός, και διαλέξουμε τυχαία έναν αριθμό από το 1 μέχρι το n, τότε η πιθανότητα αυτός ο αριθμός να είναι πρώτος είναι ασυμπτωτικά $\frac{1}{\log n}$, δηλαδή προσεγγιστικά όταν ο αριθμός n είναι μεγάλος αυτή η πιθανότητα είναι περίπου $\frac{1}{\log n}$.

Για παράδειγμα θα έχουμε ότι η πιθανότητα ενός αριθμού $1 \leq x \leq n$ να είναι πρώτος, αν $n = 10, 10^2, 10^3, 10^6, 10^9, 10^{12}, 10^{15}$, είναι (όλες οι παρακάτω τιμές είναι προσεγγιστικές):

(α΄) Αν $n = 10$, τότε $\log 10 = 2.30$ και άρα:

$$\frac{1}{\log n} = \frac{1}{2.30} = \mathbf{0.434}$$

(β΄) Αν $n = 100 = 10^2$, τότε $\log 100 = 4.30$ και άρα:

$$\frac{1}{\log n} = \frac{1}{4.60} = \mathbf{0.217}$$

(γ΄) Αν $n = 1000 = 10^3$, τότε $\log 100 = 6.90$ και άρα:

$$\frac{1}{\log n} = \frac{1}{4.60} = \mathbf{0.144}$$

(δ΄) Αν $n = 1000000 = 10^6$, τότε $\log 1000000 = 13.81$ και άρα:

$$\frac{1}{\log n} = \frac{1}{4.60} = \mathbf{0.072}$$

(ε΄) Αν $n = 1000000000 = 10^9$, τότε $\log 1000000000 = 20.70$ και άρα:

$$\frac{1}{\log n} = \frac{1}{20.70} = \mathbf{0.048}$$

(ϛ΄) Αν $n = 1000000000000 = 10^{12}$, τότε $\log 1000000000000 = 27.63$ και άρα:

$$\frac{1}{\log n} = \frac{1}{27.63} = \mathbf{0.036}$$

[2]Αν X είναι ένα σύνολο, τότε συμβολίζουμε με $|X|$ το πλήθος των στοιχείων του συνόλου S.

(ζ) Αν $n = 1000000000000000 = 10^{15}$, τότε $\log 1000000000000000 = 34.53$ και άρα:

$$\frac{1}{\log n} = \frac{1}{34.53.70} = \mathbf{0.028}$$

(3) Άτυπα θα λέγαμε ότι αν μπορούσαμε να διαλέξουμε τυχαία έναν φυσικό αριθμό από το σύνολο $\mathbb{N}$ όλων των φυσικών αριθμών, τότε η πιθανότητα αυτός ο αριθμός να είναι πρώτος είναι προσεγγιστικά 0. Αυτό το συμπέρασμα μπορεί να διατυπωθεί ακριβέστερα ως εξής. Έστω ότι, για έναν πραγματικό αριθμό x, ο φυσικός αριθμός $[x]$ συμβολίζει τον μεγαλύτερο ακέραιο ο οποίος είναι $\leq x$. Τότε αποδεικνύεται ότι η πιθανότητα ένας φυσικός αριθμός να είναι πρώτος υπάρχει και είναι ίση με:

$$\mathsf{lim}_{x\to\infty}\frac{\pi(x)}{[x]} = 0$$

Σχόλιο 5.9. Το Θεώρημα των Πρώτων Αριθμών θεωρείται από τα σπουδαιότερα αποτελέσματα της Θεωρίας Αριθμών. Η απόδειξη του είναι αρκετά δύσκολη και ξεφεύγει από τα πλαίσια του μαθήματος. Το Θεώρημα αποδείχθηκε ανεξάρτητα, από τον Jaque Hadamard και τον Charles Jean de Vallée-Poussin το 1896 με αναλυτικές μεθόδους.

Το 1948, επίσης ανεξάρτητα, οι Μαθηματικοί Selberg και Erdös απέδειξαν το Θεώρημα των Πρώτων Αριθμών με στοιχειώδεις μεθόδους.

Σχόλιο 5.10. Αν όπως πριν, p_n συμβολίζει τον n-οστο πρώτο αριθμό, τότε από το Θεώρημα των Πρώτων Αριθμών προκύπτει ότι:

$$p_n \sim n\log n$$

όπου $\log n$ συμβολίζει τον φυσικό λογάριθμο του n.

Μια άμεση συνέπεια του Θεωρήματος των Πρώτων Αριθμών είναι το ακόλουθο Πόρισμα το οποίο γενικεύει την εικασία του Bertrand:

Πόρισμα 5.11.

$$\forall\,\epsilon > 0,\quad \exists\, m = m(\epsilon) > 0:\ \ \forall n > m(\epsilon):\quad \exists\, p:\ \textit{πρώτος έτσι ώστε:}\ \ n < p < (1+\epsilon)n$$

Επιστρέφοντας στην Εικασία του Bertrand, αποδεικνύουμε την ακόλουθη ενδιαφέρουσα εφαρμογή της:

Θεώρημα 5.12 (L. Greenfield and S. Greenfield (1998))**.** *Αν n είναι ένας φυσικός αριθμός, τότε το σύνολο των $2n$ αριθμών $\mathcal{N} = \{1, 2, \cdots, 2n\}$ μπορεί να διαμερισθεί σε n το πλήθος ζευγάρια αριθμών*

$$\{a_1, b_1\},\ \ \{a_2, b_2\},\ \cdots,\ \ \{a_n, b_n\}$$

έτσι ώστε ο αριθμός $a_i + b_i$ να είναι πρώτος, $1 \leq i \leq n$.

Απόδειξη. Η απόδειξη θα γίνει με χρήση Αρχής Μαθηματικής Επαγωγής.

(1) Για $n = 1$, το αποτέλεσμα είναι προφανές, διότι τότε $\mathcal{N} = \{1, 2\}$ και ο αριθμός $1 + 2 = 3$ είναι πρώτος.

(2) Για $n > 1$, υποθέτουμε ο ισχυρισμός είναι αληθής για κάθε σύνολο $\{1, 2, \cdots, 2m\}$ με $m < n$.

(3) Για την γενική περίπτωση, και σύμφωνα με το Θεώρημα 5.1 (Εικασία του Bertrand), υπάρχει ένας πρώτος αριθμός p έτσι ώστε $2n < p \leq 4n$. Επειδή προφανώς ο αριθμός $4n$ δεν είναι πρώτος, έπεται ότι μπορούμε να γράψουμε $p = 2n + m$, όπου $1 \leq m < 2k$, και $k \leq n$.

Θεωρούμε τότε τα ζευγάρια

$$(2n, m),\ (2n-1, m+1),\ \cdots,\ (n+\lceil k\rceil, n+\lfloor k\rfloor)$$

όπου για έναν πραγματικό αριθμό x:

(α') $\lfloor x\rfloor = \max\{m \in \mathbb{Z} \mid m \leq x\}$ συμβολίζει τον μεγαλύτερο ακέραιο $\leq x$.

(β') $\lceil x\rceil = \min\{n \in \mathbb{Z} \mid n \geq x\}$ συμβολίζει τον μικρότερο ακέραιο $\geq x$.

Επειδή προφανώς ο αριθμός m δεν μπορεί να είναι άρτιος, έπεται ότι ο m είναι περιττός και άρα ο αριθμός $m-1$ είναι άρτιος και άρα της μορφής $m-1 = 2r$, όπου $r < n$. Τότε τα παραπάνω ζεύγη αποδεικνύουν τον ισχυρισμό για το σύνολο $\{m, m+1, \cdots, 2n\}$. Επειδή ο ισχυρισμός για το σύνολο $\{1, 2, \cdots, m-1\}$ προκύπτει από την Επαγωγική Υπόθεση, έπεται ότι ο ισχυρισμός ισχύει και για το n.

Επομένως ο ισχυρισμός είναι αληθής για κάθε $n \geq 1$. ■

Το ακόλουθο Θεώρημα του Erdös γενικεύει την εικασία του Bertrand:

Θεώρημα 5.13 (Erdös). *Για κάθε φυσικό αριθμό k, υπάρχει ένας φυσικός αριθμός N έτσι ώστε για κάθε $n > N$, υπάρχουν τουλάχιστον k το πλήθος πρώτοι αριθμοί p έτσι ώστε: $n < p < 2n$.*

Αναφέρουμε χωρίς απόδειξη τα ακόλουθα αποτελέσματα τα οποία προκύπτουν από την Εικασία του Bertrand:

Θεώρημα 5.14. *Υπάρχουν σταθερές $C, c > 0$ έτσι ώστε, $\forall x \in \mathbb{R}$:*

$$c\frac{\log x}{x} \ \leq\ \pi(x)\ \leq\ C\frac{\log x}{x}$$

Θεώρημα 5.15. *Κάθε φυσικός αριθμός $n > 6$ μπορεί να γραφεί ως άθροισμα διακεκριμμένων πρώτων αριθμών.*

Τέλος το ακόλουθο είναι ένα ενδιαφέρον πρόβλημα για το οποίο δεν είναι γνωστή η απάντηση:

Ανοιχτό Πρόβλημα: (Εικασια του Legendre). Είναι αληθές ότι για κάθε φυσικό αριθμό $n > 1$ υπάρχει πάντα ένας πρώτος αριθμός p έτσι ώστε:

$$n^2\ <\ p\ <\ (n+1)^2\ ;$$

6. **Ο Αλγόριθμος του Ευκλείδη και το Θεώρημα του Lamé**

Έστω a, b δύο φυσικοί αριθμοί. Τότε όπως γνωρίζουμε, ο μέγιστος κοινός διαιρέτης (a, b) των αριθμών a και b προκύπτει ως το τελευταίο μη-μηδενικό υπόλοιπο στις διαδοχικές διαιρέσεις στον Αλγόριθμο του Ευκλείδη. Επομένως υπάρχει αλγοριθμικός τρόπος εύρεσης του μέγιστου κοινού διαιρέτη δύο αριθμών.

Επομένως για προφανείς λόγους έχει μεγάλη σημασία να γνωρίζουμε πόσες διαιρέσεις χρειαζόμαστε για τον υπολογισμό του μέγιστου κοινού διαιρέτη με χρήση του Αλγόριθμου του Ευκλείδη.

Ο Γάλλος Μαθηματικός Gabriel Lamé το 1845 απέδειξε ότι ο αριθμός των διαιρέσεων οι οποίες απαιτούνται στην εφαρμογή του Αλγόριθμου του Ευκλείδη για τον υπολογισμό του μέγιστου κοινού διαιρέτη δύο αριθμών είναι το πολύ πέντε φορές το πλήθος των δεκαδικών ψηφίων του μικρότερου από τους δύο αριθμούς.

Σκοπός μας στην παρούσα παράγραφο είναι να δώσουμε μια απόδειξη του Θεωρήματος του Lamé. Η απόδειξη χρησιμοποιεί, με αναπάντεχο τρόπο, ιδιότητες της ακολουθίας Fibonacci.

Θεώρημα 6.1 (Θεωρημα του Lamé (1845))**.** *Έστω $a, b \in \mathbb{N}$ δύο φυσικοί αριθμοί. Τότε για τον αριθμό n των διαιρέσεων οι οποίες απαιτούνται για τον υπολογισμό του μέγιστου κοινού διαιρέτη (a, b) των αριθμών a, b με χρήση του Αλγόριθμου του Ευκλείδη, ισχύει ότι:*

$$n \leq 5 \cdot \big(\textit{πλήθος δεκαδικών ψηφίων του αριθμού } \min\{a, b\}\big)$$

Απόδειξη. Αν $a = b$, τότε προφανώς $(a, b) = a = b$. Υποθέτουμε ότι $a \neq b$ και χωρίς βλάβη της γενικότητας, έστω $a > b$.

– **Βήμα 1**: Θέτουμε $r_0 = a$ και $r_1 = b$. Από τον Ευκλείδειο Αλγόριθμο τότε θα έχουμε τις ακόλουθες σχέσεις:

$$\begin{array}{rcll} r_0 & = & r_1 q_1 + r_2 & \text{όπου} \quad 0 \leq r_2 < r_1 \\ r_1 & = & r_2 q_2 + r_3 & \text{όπου} \quad 0 \leq r_3 < r_2 \\ r_0 & = & r_1 q_1 + r_2 & \text{όπου} \quad 0 \leq r_4 < r_3 \\ & \vdots & & \vdots \quad \vdots \\ r_{n-2} & = & r_{n-1} q_{n-1} + r_n & \text{όπου} \quad 0 \leq r_n < r_{n-1} \\ r_{n-1} & = & r_n q_n & \end{array} \tag{6.1}$$

όπου έχουμε υποθέσει ότι:

$$0 \neq r_i, \quad i = 2, 3, \cdots, n \quad \& \quad r_{n+1} = 0$$

Τότε γνωρίζουμε ότι:

$$(a, b) = r_n$$

και το πλήθος των διαιρέσεων οι οποίες απαιτούνται στην εκτέλεση του Αλγόριθμου του Ευκλείδη για τον παραπάνω υπολογισμό είναι ακριβώς n.

– **Βήμα 2**: Υπενθυμίζουμε ότι η ακολουθία Fibonacci $\{F_n\}_{n \geq 1}$ ορίζεται ως εξής:

$$F_1 = 1, \ F_2 = 1, \ F_3 = 2, \quad \& \quad F_{n+1} = F_n + F_{n-1}, \quad \forall n \geq 2$$

- Ισχυρισμός: $b = r_1 \geq F_{n+1}$.

Η απόδειξη θα γίνει με χρήση Αρχής Μαθηματικής Επαγωγής:

(1) Το τελευταίο μη-μηδενικό υπόλοιπο r_n είναι ένας φυσικός αριθμός και άρα $r_n \geq 1 = F_2$. Άρα:

$$r_n \geq F_2$$

(2) Επειδή $r_{n-1} = r_n q_n$, και επειδή $r_n < r_{n-1}$, έπεται ότι $q_n \neq 1$. Επομένως $q_n \geq 2$, και τότε $r_{n-1} = r_n q_n \geq 2r_n \geq 2 = F_3$. Άρα:

$$r_{n-1} \ \geq \ F_3$$

(3) Επαγωγικη Υποθεση: Υποθέτουμε ότι:

$$r_{n-k+1} \ \geq \ F_{k+1}, \qquad \text{για κάθε} \quad k \in \mathbb{N} \quad \text{έτσι ώστε}: \quad 1 \leq k < n$$

Ιδιάιτερα θα έχουμε:

$$r_2 \ \geq \ F_n \qquad \& \qquad r_3 \ \geq \ F_{n-1}$$

(4) Για $k = n$, από τις σχέσεις (3.1) θα έχουμε: $r_1 = r_2 q_2 + r_3$. Επειδή ο αριθμός q_2 είναι φυσικός, θα έχουμε $q_2 \geq 1$ και επομένως $r_1 \geq r_2 + r_3$. Τότε με χρήση της Επαγωγικής Υπόθεσης, θα έχουμε:

$$r_1 \geq r_2 + r_3 \geq F_n + F_{n-1} = F_{n+1}$$

Επομένως έχουμε δείξει το Ισχυρισμό:

$$b \ \geq \ F_{n+1}$$

και επομένως έχουμε δείξει ότι:

- *αν n είναι ο αριθμός των διαιρέσεων οι οποίες απαιτούνται στην εκτέλεση του Αλγόριθμου του Ευκλείδη για τον υπολογισμό του μέγιστου κοινού διαιρέτη (a, b), όπου $a > b$, τότε αναγκαστικά ο μικρότερος αριθμός b δεν μπορεί να είναι μικρότερος από τον $(n+1)$-οστό αριθμό της ακολουθίας Fibonacci.*

– **Βήμα 3**: Θα δείξουμε πρώτα τον ακόλουθο ισχυρισμό.

- Ισχυρισμός:

$$F_n \ \geq \ \phi^{n-2}, \quad \forall n \geq 3, \qquad \text{όπου} \quad \phi = \frac{1+\sqrt{5}}{2}$$

Υπενθυμίζουμε ότι ο αριθμός ϕ είναι ρίζα της εξίσωσης $x^2 - x - 1 = 0$ και άρα

$$\phi^2 = \phi + 1$$

(1) Για $n = 3$, έχουμε: $F_3 = 2$ και $\phi^{3-2} = \phi = \frac{1+\sqrt{5}}{2} = 1.6180...$, και άρα προφανώς θα έχουμε

$$F_3 \ > \ \phi^{3-2}$$

(2) Επαγωγικη Υποθεση: Υποθέτουμε ότι $N > 3$ και υποθέτουμε ότι:

$$F_k \ > \ \phi^{k-2}, \qquad \forall k: \quad 3 < k < n$$

(3) Για $k = n$, με χρήση της Επαγωγικής Υπόθεσης, θα έχουμε:

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ &> \phi^{n-1-2} + \phi^{n-2-2} \\ &= \phi^{n-3} + \phi^{n-4} \\ &= \phi^{n-4}\big(\phi + 1\big) \\ &= \phi^{n-4}\phi^2 \\ &= \phi^{n-2} \end{aligned}$$

Επομένως θα έχουμε:

$$b \ \geq \ F_{n+1} \ > \ \phi^{n-1}$$

– **Βήμα 4**: Θα έχουμε διαδοχικά:

(1) Παίρνοντας λογάριθμους με βάση 10 στην παραπάνω σχέση, θα έχουμε:
$$\log_{10} b \ > \ (n-1) \cdot \log_{10} \phi$$
(2) Βλέπουμε εύκολα ότι:
$$\log_{10} \phi \ > \ \frac{1}{5}$$
(3) Επομένως θα έχουμε: $\log_{10} b \ > \ \frac{1}{5}(n-1)$ και άρα:
$$n - 1 \ < \ 5 \log_{10} b$$
(4) Έστω k το πλήθος των δεκαδικών ψηφίων του b στην δεκαδική παράσταση του. Τότε προφανώς $b \ < \ 10^k$ και άρα:
$$\log_{10} b \ < \ k$$
(5) Συνδυάζοντας τις δύο τελευταίες σχέσεις, θα έχουμε:
$$n - 1 \ < \ 5k$$
και επειδή ο k είναι ακέραιος, θα έχουμε:
$$n \ < \ 5k$$
■

Σχόλιο 6.2. Το Θεώρημα του Lamé δείχνει ότι ο αλγόριθμος του Ευκλείδη για την εύρεση του μέγιστου κοινού διαιρέτη είναι αρκετά ταχύς και αποτελεσματικός, διότι μας βρίσκει τον μέγιστο κοινό διαιρέτη δύο αριθμών σε πολυωνυμικό χρόνο.

Σχόλιο 6.3. Υπάρχουν άπειρα ζεύγη αριθμών για τα οποία ο αλγόριθμος του Ευκλείδη για την εύρεση του μέγιστου κοινού διαιρέτη τους απαιτεί ακριβώς n βήματα.

Πράγματι, αν F_{n+1}, F_{n+2} είναι δύο διαδοχικοί όροι της ακολουθίας Fibonacci, $\forall n \geq 1$, τότε
$$(F_{n+1}, F_{n+2}) = 1$$
και όπως έχουμε δεί στο μάθημα για την εύρεση του μέγιστου κοινού διαιρέτη $(F_{n+1}, F_{n+2}) = 1$ απιτούνται ακριβώς n βήματα:
$$\begin{aligned} F_{n+2} &= F_{n+1} \cdot 1 + F_n \\ F_{n+1} &= F_n \cdot 1 + F_{n-1} \\ &\vdots \\ F_4 &= F_3 \cdot 1 + F_2 \\ F_3 &= F_2 \cdot 2 \end{aligned}$$
Άρα $(F_{n+1}, F_{n+2}) = F_2 = 1$, και όπως βλέπουμε στην εκτέλεση του αλγορίθμου απαιτούνται ακριβώς n βήματα.

Μέρος 2. Αριθμητικές Συναρτήσεις

Μέρος 3. Ισοτιμίες

Μέρος 4. Πρωταρχικές Ρίζες

Μέρος 5. Τετραγωνικά Υπόλοιπα

Μέρος 6. Βιβλιογραφία