# Θεωρία Αριθμών με Εφαρμογές στην Κρυπτογραφία

Ευαγγελόπουλος Δημήτρης

Φεβρουάριος 2013

# ΠΡΟΛΟΓΟΣ

Η Θεωρία Αριθμών είναι ο κλάδος των Μαθηματικών που ασχολείται με τις ιδιότητες των ακέραιων αριθμών, καθώς και με τα προβλήματα που προκύπτουν από τη μελέτη αυτή. Ο σκοπός αυτής της διπλωματικής εργασίας είναι μια συνοπτική μελέτη της Θεωρίας Αριθμών, κυρίως μέσω της κατανομής των πρώτων, με εφαρμογές στην Κρυπτογραφία.

Ξεκινώντας το πρώτο κεφάλαιο περιέχει τη Βασική Θεωρία Αριθμών και συγκεκριμένα: το Θεμελιώδες Θεώρημα της Αριθμητικής, τον Αλγόριθμο της Διαίρεσης, τη Θεωρία Ισοτιμιών και κάποιες βασικές αριθμητικές συναρτήσεις.

Στη συνέχεια το δεύτερο κεφάλαιο αναφέρεται στην απειρία των πρώτων. Ξεκινά με το θεώρημα του Ευκλείδη για την ύπαρξη άπειρων πρώτων αριθμών. Ακολουθούν το θεώρημα του Dirichlet, το Αίτημα του Bertrand και άλλες δύο παράγραφοι για τους δίδυμους πρώτους και την Εικασία του Goldbach.

Έπειτα γίνεται μια εισαγωγή στην Αναλυτική Θεωρία Αριθμών. Αναφέρεται το Θεώρημα των Πρώτων Αριθμών και δίνεται μια σκιαγράφηση της στοιχειώδους απόδειξής του από τους Erdos και Selberg. Ακόμα παρουσιάζονται αρκετές ισοδύναμες μορφές του Θεωρήματος των Πρώτων Αριθμών.

Τέλος, στην Κρυπτογραφία μελετάμε θεμελιώδεις μεθόδους και βασικούς αλγορίθμους σχετικά με την Πιστοποίηση Πρώτων Αριθμών (αλγόριθμοι Fermat, Miller-Rabin και Solovay-Strassen) και την Παραγοντοποίηση Ακεραίων σε Πρώτους Παράγοντες (αλγόριθμοι του Dixon και p-1 του Pollard).

# ΠΕΡΙΕΧΟΜΕΝΑ

**1. Βασική Θεωρία Αριθμών**
*1.1* Οι Αρχές της Καλής Διάταξης και της Μαθηματικής Επαγωγής.....7
*1.2* Διαιρετότητα.....10
*1.3* Το Θεμελιώδες Θεώρημα της Αριθμητικής.....18
*1.4* Ισοδυναμίες.....21
*1.5* Οι Συναρτήσεις $\pi(x)$ και $\Lambda(n)$.....25
**2. Η Απειρία των Πρώτων**
*2.1* Πόσοι Πρώτοι Υπάρχουν;.....27
*2.2* Το Θεώρημα του Dirichlet.....37
*2.3* Το Αίτημα του Bertrand.....41
*2.4* Δίδυμοι Πρώτοι.....46
*2.5* Η Εικασία του Goldbach.....49
**3. Η Κατανομή των Πρώτων**
*3.1* Εισαγωγή.....51
*3.2* Η Προσέγγιση του Chebyshev.....55
*3.3* Οι Συναρτήσεις $\psi(x)$ και $\theta(x)$ του Chebyshev.....63
*3.4* Ισοδύναμες Μορφές του Θεωρήματος των Πρώτων Αριθμών.....65
*3.5* Σκιαγράφηση της Στοιχειώδους Απόδειξης.....72
**4. Εφαρμογές στην Κρυπτογραφία**
*4.1* Εισαγωγή.....75
*4.2* Πιστοποίηση Πρώτου.....76
*4.3* Αλγόριθμοι Πιστοποίησης Πρώτου.....79
*4.4* Παραγοντοποίση σε Πρώτους Παράγοντες.....89

**Βιβλιογραφία** 99

# Chapter 1

# ΒΑΣΙΚΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

## 1.1 ΟΙ ΑΡΧΕΣ ΤΗΣ ΚΑΛΗΣ ΔΙΑΤΑΞΗΣ ΚΑΙ ΤΗΣ ΜΑΘΗΜΑΤΙΚΗΣ ΕΠΑΓΩΓΗΣ

Το πιο σημαντικό υποσύνολο ακεραίων είναι οι φυσικοί αριθμοί, δηλαδή οι αριθμοί

$$\{1, 2, 3, \ldots\}.$$

Σε αυτή την παράγραφο θα αναφέρουμε δύο σημαντικές ιδιότητες αυτών των αριθμών: την αρχή της καλής διάταξης και την αρχή της μαθηματικής επαγωγής. Κάθε μία από τις παραπάνω μπορεί να αποδειχθεί αρκεί να αληθεύει η άλλη. Η αρχή της καλής διάταξης είναι η απλούστερη από τις δύο και είναι η εξής:

***Αρχή Καλής Διάταξης***
Εάν $A$ είναι ένα μη κενό σύνολο φυσικών αριθμών, τότε το $A$ έχει ένα ακριβώς ελάχιστο στοιχείο.

**Παράδειγμα**
Θα αποδείξουμε την αρχή καλής διάταξης για σύνολο $S \subset \mathbb{N}_0$, με $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

**Απόδειξη**
Θα δείξουμε ότι το $S$ έχει ελάχιστο στοιχείο. Διακρίνουμε δύο περιπτώσεις:
i)Αν το μηδέν ανήκει στο $S$, τότε είναι μικρότερο από καθε φυσικό αριθμό που ανήκει στο $S$, επομένως έχουμε ελάχιστο στοιχείο.
ii)Αν το μηδέν δεν ανήκει στο $S$, τότε το $S$ περιέχει μόνο φυσικούς αριθμούς

και από την αρχή καλής διάταξης, θα περιέχει ελάχιστο στοιχείο.
Και στις δύο περιπτώσεις το $S$ έχει ελάχιστο στοιχείο. ■

***Αρχή της Μαθηματικής Επαγωγής***
Εάν το $S$ είναι ένα σύνολο από φυσικούς, με τις εξής ιδιότητες:
•$1 \in S$
•αν $n \in S$ τότε $n+1 \in S$
τότε όλοι οι ακέραιοι $\geq 1$ ανήκουν στο $S$.

Υπάρχουν, βέβαια, εναλλακτικές διατυπώσεις αυτής της αρχής. Για παράδειγμα, στην πρώτη ιδιότητα ο αριθμός $1$ μπορεί να αντικατασταθεί από οποιονδήποτε φυσικό $k$, αν στο συμπέρασμα γίνει η ίδια αντικατάσταση. Επίσης η δεύτερη ιδιότητα μπορεί να αντικατασταθεί από την παρακάτω:
"αν $1, 2, 3, \ldots, n \in S$ τότε $n+1 \in S$ (ισχυρή επαγωγή)."

**Παράδειγμα**
Θα δείξουμε ότι το $1$ είναι ο μικρότερος φυσικός.

**Απόδειξη**
*1ος Τρόπος(Χρήση Μαθηματικής Επαγωγής)*
Έστω $S$ το σύνολο όλων των φυσικών που είναι μεγαλύτεροι ή ίσοι του $1$.
Έχουμε:
i)$1 \in S$
ii)Αν $k \in S$ τότε $k+1 > k \geq 1$ οπότε

$$k+1 \in S.$$

Άρα από επαγωγή το $S$ είναι το σύνολο όλων των φυσικών αριθμών και το $1$ είναι το ελάχιστο στοιχείο.

*2ος Τρόπος(Χρήση Καλής Διάταξης)*
Από αρχή καλής διάταξης το $S$ θα έχει ελάχιστο στοιχείο, έστω $s$ αυτό. Υποθέτουμε ότι $s < 1$ και έχουμε:

$$0 < s < 1 \implies 0 < s^2 < s.$$

Τότε όμως το $s$ δεν είναι το ελάχιστο στοιχείο. Καταλήξαμε σε άτοπο. Επομένως το $1$ είναι ο μικρότερος φυσικός. ■

**Παρατήρηση**
Όπως αναφέραμε και προηγουμένως η αρχή της καλής διάταξης και της μαθηματικής επαγωγής είναι ισοδύναμες. Για την απόδειξη αυτού του ισχυρισμού ο αναγνώστης παραπέμπεται στο [16].

## 1.2 ΔΙΑΙΡΕΤΟΤΗΤΑ

***Ορισμός***
Θεωρούμε τους ακέραιους $a, b$. Αν υπάρχει ακέραιος $m$ τέτοιος ώστε

$$b = ma$$

λέμε ότι ο $a$ διαιρεί τον $b$ και ότι ο $b$ είναι πολλαπλάσιο του $a$.
Συμβολίζουμε $a|b$. Αν ο $a$ δεν διαιρεί το $b$ συμβολίζουμε $a \nmid b$.
Αν ο $b > 1$ είναι ένας ακέραιος του οποίου οι μόνοι παράγοντες είναι οι $\pm 1, \pm b$ τότε ο $b$ ονομάζεται *πρώτος*. Σε κάθε άλλη περίπτωση ο $b > 1$ ονομάζεται *σύνθετος*.

***Θεώρημα***
Η διαιρετότητα έχει τις ακόλουθες ιδιότητες:
i)$a|a$
ii)$a|b$ και $b|c$ τότε $a|c$
iii)$a|b$ και $a|c$ τότε $a|(mb + nc)$ για κάθε $m, n \in \mathbb{Z}$
iv)$a|b$ και $b|a$ τότε $a = \pm b$
v)$a|b$ και $a > 0, b > 0$ τότε $a < b$
vi)$a|b$ τότε $ac|bc$, για $c \in \mathbb{Z}$, $c \neq 0$
vii)$a|0$, $\forall a \in \mathbb{Z}$ και $0|a$ μόνο εάν $a = 0$
viii)$a|b$ και $c|d$ τότε $ac|bd$.

Οι αποδείξεις είναι αρκετά απλές και για αυτό παραλείπονται, αλλά όλες βασίζονται στον ορισμό της διαιρετότητας, δηλαδή

$$a|b \Longrightarrow b = ma \ , \ m \in \mathbb{Z}$$

Θα αναφέρουμε σαν παράδειγμα τις αποδείξεις των (i) και (ii). Για τις υπόλοιπες ο αναγνώστης παραπέμπεται σε οποιοδήποτε εισαγωγικό βιβλίο στη θεωρία αριθμών.

***Απόδειξη***
ii)Αν $a|b$ και $b|c$ τότε υπάρχουν $m, n \in \mathbb{Z}$ τέτοιοι ώστε $b = ma$ και $c = nb$.
Όποτε

$$c = nma$$

και αφού $nm \in \mathbb{Z}$ έχουμε ότι $a|c$.
iii)Αφού $a|b$ και $a|c$ τότε υπάρχουν ακέραιοι $x, y$ τέτοιοι ώστε $b = ax$ και

$c = ay$. Οπότε

$$mb + nc = max + nay = a(mx + ny)$$

και επειδή ο $mx + ny$ είναι ακέραιος

$$a|(mb + nc). \qquad \blacksquare$$

Το παραπάνω αναφέρει ότι αν ο $a$ είναι ένας κοινός διαιρέτης των $b, c$ τότε ο $a$ διαιρεί κάθε γραμμικό συνδυασμό των $b$ και $c$.

Υπάρχουν όμως και περιπτώσεις όπου $a \nmid b$. Σε αυτές τις περιπτώσεις έχουμε το παρακάτω ισχυρό εργαλείο.

***Θεώρημα(Αλγόριθμος της Διαίρεσης)***
Έστω $a, b$ ακέραιοι με $b \neq 0$. Τότε υπάρχουν μοναδικοί ακέραιοι $q$ και $r$, $0 \leq r < |b|$ τέτοιοι ώστε

$$a = bq + r.$$

Οι αριθμοί $q$ και $r$ ονομάζονται πηλίκο και υπόλοιπο αντίστοιχα.

***Απόδειξη***
Έστω $S$ το σύνολο όλων των ακέραιων της μορφής $a + kb \ , \ k \in \mathbb{Z}$ δηλαδή

$$S = \{\ldots, a - 2b, a - b, a, a + b, a + 2b, \ldots\}$$

Παρατηρούμε ότι ο ακέραιος

$$a + (|a| + 1)|b|$$

είναι μη αρνητικός και ανήκει στο $S$. Από την αρχή καλής διάταξης το $S$ περιέχει ένα ελάχιστο μη αρνητικό ακέραιο, έστω $r$ αυτός. Τότε ο αριθμός $r - a$ είναι από κατασκευής πολλαπλάσιο του $b$ και επομένως

$$a = bq + r.$$

Υποθέτουμε με απαγωγή σε άτοπο ότι $r \geq |b|$. Τότε ο ακέραιος $r - |b|$ θα είναι ένας μη αρνητικός ακέραιος που ανήκει στο $S$, μικρότερος του $r$, το οποίο είναι αδύνατο.

Άρα $0 \leq r < |b|$.
Για να δείξουμε τη μοναδικότητα των $q, r$ υποθέτουμε ότι υπάρχουν $q_1, r_1 \in \mathbb{Z}$ τέτοια ώστε

$$a = bq_1 + r_1 \ , \ 0 \leq r < |b|.$$

Τότε

$$b(q_1 - q) = r - r_1 \Longrightarrow b|(r - r_1).$$

Όμως από ιδιότητες διαιρετότητας αν $r \neq r_1$ τότε

$$|r - r_1| \geq |b|.$$

Αλλά αυτό είναι αδύνατο μιας και $-b < r - r_1 < b$.
Άρα $r = r_1$ και επειδή $b(q_1 - q) = r - r_1 = 0$ και $b \neq 0$ θα είναι $q = q_1$.
Επομένως οι $q, r$ υπάρχουν και είναι μοναδικοί. ■

**Παρατήρηση**
Ο αλγόριθμος της διαίρεσης συχνά χρησιμοποιείται για να διαχωρίσουμε τους ακέραιους σε κλάσεις. Για παράδειγμα, αν $a = 2q + 1$ λέμε ότι ο $a$ είναι περιττός, ενώ αν $a = 2q+0$ λέμε ότι ο $a$ είναι άρτιος. Παρόμοιες κατηγοριοποιήσεις μπορούν να γίνουν με βάση τη διαίρεση ενός αριθμού με το $3, 4, \ldots$.

***Ορισμός(Μέγιστος Κοινός Διαιρέτης)***
Έστω $a, b \in \mathbb{Z}$, όχι και οι δύο μηδέν. Ο μεγαλύτερος θετικός ακέραιος που διαιρεί και τον $a$ και τον $b$ ονομάζεται *μέγιστος κοινός διαιρέτης* των $a, b$. Συμβολίζεται ως $\gcd(a, b)$.

**Παράδειγμα**

$$\gcd(3, 9) = 3 \ , \ \gcd(-7, 21) = 7 \ , \ \gcd(0, -5) = 5$$

***Ορισμός***
Αν $\gcd(a, b) = 1$ τότε λέμε ότι οι αριθμοί $a, b$ είναι *πρώτοι προς αλλήλους* (ή *πρώτοι μεταξύ τους*).

***Θεώρημα***
Για τους μη μηδενικούς ακέραιους $a, b$ ο $\gcd(a, b)$ υπάρχει, είναι μοναδικός και

μπορεί να χαρακτηριστεί ως ο μικρότερος γραμμικός συνδυασμός των $a, b$.

***Απόδειξη***
Δοθέντων $a, b \in \mathbb{Z}$, $a, b \neq 0$ θεωρούμε το σύνολο:

$$S = \{ax + by > 0 : x, y \in \mathbb{Z}\}$$

Το S είναι μη κενό μιας και για $x = a$, $y = b$ είναι $a^2 + b^2 > 0$. Άρα το $S$ έχει ελάχιστο στοιχείο, έστω $d$ αυτό. Θα δείξουμε ότι το $d$ είναι ο gcd$(a, b)$.
Πρώτα θα δείξουμε ότι ο $d$ είναι κοινός διαιρέτης των $a, b$. Γνωρίζουμε ότι $d = ax + by$ και ο $d$ είναι ο μικρότερος τέτοιος γραμμικός συνδυασμός. Από τον αλγόριθμο της διαίρεσης του $a$ με το $d$ είναι

$$a = qd + r \ , \ \ 0 \leq r < d.$$

Έστω ότι $r \neq 0$. Τότε

$$r = a - qd = a - q(ax + by) = (1 - qx)a - qyb > 0.$$

Έτσι ο $r$ είναι θετικός γραμμικός συνδυασμός των $a, b$, οπότε $r \in S$. Επίσης $r < d$. Επομένως καταλήγουμε σε άτοπο, αφού το $d$ είναι το ελάχιστο στοιχείο του $S$.
Άρα $r = 0$ και $a = qd$, δηλαδή

$$d|a.$$

Εφαρμόζοντας τον αλγόριθμο της διαίρεσης του $b$ με το $d$ καταλήγουμε εντελώς ανάλογα στο ότι

$$d|b.$$

Οπότε ο $d$ είναι κοινός διαιρέτης των $a, b$.
Έστω $d_1$ ένας άλλος κοινός διαιρέτης των $a, b$. Από ιδιότητες διαιρετότητας ο $d_1$ διαιρεί οποιονδήποτε γραμμικό συνδυασμό των $a, b$. Επομένως

$$d_1|d.$$

Άρα ο $d$ είναι ο gcd$(a, b)$.
Για τη μοναδικότητα έχουμε: Έστω $d_1$ ένας άλλος gcd$(a, b)$. Τότε $d_1 > 0$ και $d_1$ κοινός διαιρέτης των $a, b$. Έχουμε:
i)$d_1|d$ αφού $d =$ gcd$(a, b)$
ii)$d|d_1$ αφού $d_1 =$ gcd$(a, b)$.

Άρα από ιδιότητες διαιρετότητας $d = \pm d_1$ και επειδή είναι και οι δύο θετικοί είναι

$$d = d_1. \qquad \blacksquare$$

**Παρατήρηση**
Αν οι $a, b$ είναι πρώτοι μεταξύ τους, τότε $\gcd(a, b) = 1$ όπως είδαμε και στον ορισμό. Συμπεραίνουμε λοιπόν ότι οι αριθμοί $a, b$ είναι πρώτοι μεταξύ τους αν και μόνο αν το $1$ μπορεί να εκφραστεί ως γραμμικός συνδυασμός των $a, b$.

***Πρόταση***
Αν $d = \gcd(a, b)$, οι ακέραιοι

$$\frac{a}{d} \ , \ \frac{b}{d}$$

είναι πρώτοι μεταξύ τους.

***Απόδειξη***
Από το προηγούμενο θεώρημα $d = ma + nb$, $m, n \in \mathbb{Z}$. Οπότε

$$1 = \frac{ma}{d} + \frac{nb}{d} = m\frac{a}{d} + n\frac{b}{d}.$$

Προφανώς η μονάδα είναι ο μικρότερος γραμμικός συνδυασμός των $\frac{a}{d}, \frac{b}{d}$. Άρα

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

που σημαίνει ότι οι $\frac{a}{d}, \frac{b}{d}$ είναι πρώτοι μεταξύ τους.

***Λήμμα***
Για κάθε $c \in \mathbb{Z}$ ισχύει ότι

$$\gcd(a, b) = \gcd(a, b + ac).$$

***Απόδειξη***
Έστω ότι $\gcd(a, b) = d$ και $\gcd(a, b + ac) = d_1$. Ο $d$ είναι ο ελάχιστος θετικός γραμμικός συνδυασμός των $a, b$. Γράφουμε

$$d = ax + by.$$

Ακόμα ο $d_1$ είναι γραμμικός συνδυασμός των $a, b + ac$, επομένως

$$d_1 = ar + (b + ac)s = a(cs + r) + bs.$$

Άρα ο $d_1$ είναι επίσης γραμμικός συνδυασμός των $a, b$, οπότε

$$d_1 \geq d.$$

Από την άλλη, $d_1|a$ και $d_1|b + ac$, δηλαδή $d_1|b$. Οπότε $d_1|d$, δηλαδή

$$d_1 \leq d.$$

Τελικά $d_1 = d$, που σημαίνει ότι

$$\gcd(a, b) = \gcd(a, b + ac). \qquad \blacksquare$$

***Λήμμα του Ευκλείδη***
Αν $a|bc$ και $\gcd(a, b) = 1$, τότε

$$a|c.$$

***Απόδειξη***
Αφού $\gcd(a, b) = 1$ μπορούμε να γράψουμε $1 = ax + by$. Άρα

$$c = acx + bcy.$$

Όμως $a|acx$ και $a|bcy$ οπότε

$$a|c. \qquad \blacksquare$$

**Ο Αλγόριθμος του Ευκλείδη**

Με τον αλγόριθμο του Ευκλείδη είμαστε ικανοί όχι μόνο να βρούμε τον μέγιστο κοινό διαιρέτη δύο αριθμών αλλά να τον γράψουμε και σαν γραμμικό συνδυασμό αυτών.

***Θεώρημα(Ευκλείδιος Αλγόριθμος)***

Έστω οι ακέραιοι $a, b$ με $a > 0$. Μετά από τις διαδοχικές διαιρέσεις:

$$\begin{aligned} b &= q_1 a + r_1 \ , \ 0 < r_1 < a \\ a &= q_2 r_1 + r_2 \ , \ 0 < r_2 < r_1 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \ , \ 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

το τελευταίο μη μηδενικό υπόλοιπο $r_n$ είναι ο $\gcd(a, b)$. Ακόμα, ο $r_n$ μπορεί να γραφεί σαν γραμμικός συνδυασμός των $a, b$, ακολουθώντας την αντίστροφη διαδικασία και κάνοντας διαδοχικές αντικαταστάσεις.

***Απόδειξη***

Κάνοντας διαδοχικές διαιρέσεις όπως διατυπώνονται στο θεώρημα, κάθε υπόλοιπο $r_i$ είναι μικρότερο από το προηγούμενο, αλλά παραμένει θετικό. Έτσι η ακολουθία των $r_i$ θα τελειώνει με ένα μηδενικό υπόλοιπο. Άρα υπάρχει τελευταίο μηδενικό υπόλοιπο $r_n$. Θα δείξουμε ότι αυτό είναι και ο $\gcd(a, b)$:
Από προηγούμενο λήμμα είναι

$$\gcd(a, b) = \gcd(a, b - q_1 a) = \gcd(a, r_1) = \gcd(r_1, a - q_2 r_1) = \gcd(r_1, r_2).$$

Συνεχίζοντας την ίδια διαδικασία καταλήγουμε ότι

$$\gcd(a, b) = \gcd(r_{n-1}, r_n) = r_n$$

μιας και $r_n | r_{n-1}$. Οπότε

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

Για να εκφράσουμε το $r_n$ ως γραμμικό συνδυασμό των $a, b$ έχουμε:

$$r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) = (1 + q_n q_{n-1}) r_{n-2} - q_n r_{n-3} = \dots$$

Συνεχίζοντας με διαδοχικές αντικαταστάσεις θα έχουμε:

$$r_n = ax + by. \qquad \blacksquare$$

Ακολουθεί ένα παράδειγμα για να γίνει κατανοητό πόσο απλός και εύχρηστος είναι ο αλγόριθμος του Ευκλείδη.

**Παράδειγμα**
Για το $\gcd(232, 136)$ έχουμε:

$$232 = 1 \cdot 136 + 96$$

$$136 = 1 \cdot 96 + 40$$

$$96 = 2 \cdot 40 + 16$$

$$40 = 2 \cdot 16 + 8$$

$$16 = 2 \cdot 8 + 0$$

Άρα

$$\gcd(232, 136) = 8.$$

Ακόμα

$$8 = 40 - 2 \cdot 16 = 40 - 2(96 - 2 \cdot 40) = 5 \cdot 40 - 2 \cdot 96 = 5(136 - 96) - 2 \cdot 96 =$$

$$= 5 \cdot 136 - 7 \cdot 96 = 5 \cdot 136 - 7(232 - 136) = 12 \cdot 136 - 7 \cdot 232.$$

Επομένως

$$\gcd(232, 136) = 8 = 12 \cdot 136 - 7 \cdot 232.$$

## 1.3 ΤΟ ΘΕΜΕΛΙΩΔΕΣ ΘΕΩΡΗΜΑ ΤΗΣ ΑΡΙΘΜΗΤΙΚΗΣ

Το Θεμελιώδες Θεώρημα της Αριθμητικής (ΘΘΑ) αποτελεί ένα από τα πιο σημαντικά αριθμοθεωρητικά αποτελέσματα. Αναφέρει ότι κάθε ακέραιος μπορεί να αναπαρασταθεί ως γινόμενο πρώτων κατά μοναδικό τρόπο. Στον επόμενο πίνακα παρουσιάζεται αυτή η ιδιότητα για τους δέκα πρώτους ακέραιους:

| $n$ | **Παραγοντοποίηση** |
|---|---|
| 1 | 1 |
| 2 | 2 |
| 3 | 3 |
| 4 | 2·2 |
| 5 | 5 |
| 6 | 2·3 |
| 7 | 7 |
| 8 | 2·2·2 |
| 9 | 3·3 |
| 10 | 2·5 |

Όπως βλέπουμε από τον παραπάνω πίνακα κάθε αριθμός μέχρι το δέκα έχει ακριβώς μια πρώτη παραγοντοποίηση. Θα αποδείξουμε το θεώρημα για κάθε $n \in \mathbb{N}$.

***Θεμελιώδες Θεώρημα Αριθμητικής***
Για κάθε $n > 1$ υπάρχουν πρώτοι $p_1 \leq p_2 \leq \ldots \leq p_r$ τέτοιοι ώστε

$$n = p_1 p_2 \ldots p_r$$

και η παραγοντοποίηση είναι μοναδική.

***Απόδειξη***
Πρώτα θα δείξουμε με επαγωγή στο $n$ ότι κάθε ακέραιος έχει τουλάχιστον μια πρώτη παραγοντοποίηση. Μια τέτοια παραγοντοποίηση ισχύει για κάθε $n \leq 10$. Υποθέτουμε ότι κάθε ακέραιος $m$, $1 \leq m \leq k$, έχει μια πρώτη παραγοντοποίηση. Ο αριθμός $k+1$ είναι είτε πρώτος είτε σύνθετος.

Αν είναι πρώτος τότε η παραγοντοποίησή του είναι ο ίδιος ο αριθμός.
Αν είναι σύνθετος τότε θα έχουμε:

$$k+1 = ab$$

με $1 < a < k+1$ και $1 < b < k+1$.
Αφού $1 < a \leq k$ και $1 < b \leq k$ από επαγωγική υπόθεση οι $a, b$ έχουν μια πρώτη παραγοντοποίηση έστω:

$$a = p_1 p_2 \dots p_s \ , \ \ b = p'_1 p'_2 \dots p'_t.$$

Οπότε

$$k+1 = p_1 p_2 \dots p_s p'_1 p'_2 \dots p'_t.$$

Έτσι ο $k+1$ έχει τους παραπάνω πρώτους παράγοντες. Οπότε επαγωγικά κάθε ακέραιος έχει μια πρώτη παραγοντοποίηση.
Τώρα θα δείξουμε ότι αυτή η παραγοντοποίηση είναι μοναδική. Θα χρησιμοποιήσουμε πάλι επαγωγή στο $n$. Από τον πίνακα παρατηρούμε ότι η παραγοντοποίηση για κάθε $n \leq 10$ είναι μοναδική. Υποθέτουμε για κάθε ακέραιο $m$, $1 < m \leq k$, ότι μπορεί να αναπαρασταθεί κατά μοναδικό τρόπο ως γινόμενο πρώτων. Εξετάζουμε τον $k+1$ και υποθέτουμε με απαγωγή σε άτοπο, ότι έχει δύο πρώτες παραγοντοποιήσεις:

$$k+1 = p_1 p_2 \dots p_u = p'_1 p'_2 \dots p'_v$$

με $p_1 \leq p_2 \leq \dots \leq p_u$ και $p'_1 \leq p'_2 \leq \dots \leq p'_v$. Τότε $p'_1 | k+1$ δηλαδή $p'_1 | p_1 p_2 \dots p_u$. Οπότε $p'_1 | p_i$, για κάποιο $i$. Όμως αφού $p'_1, p_i$ πρώτοι θα είναι

$$p'_1 = p_i.$$

Ακολουθώντας την ίδια διαδικασία έχουμε

$$p_1 = p'_j$$

και επειδή $p_1 = p'_i \geq p'_1$ και $p'_1 = p_i \geq p_1$ τότε

$$p_1 = p'_1.$$

Τότε όμως ο $\frac{k+1}{p_1}$ είναι ακέραιος μικρότερος του $k$ και

$$p_2 p_3 \dots p_u = \frac{k+1}{p_1} = p'_2 p'_3 \dots p'_v.$$

Από την επαγωγική υπόθεση είναι

$$u = v \ , \ \ p_2 = p'_2, p_3 = p'_3, \ldots, p_u = p'_u.$$

Άρα η πρώτη παραγοντοποίηση είναι μοναδική για κάθε $n \geq 1$. ■

**Παρατήρηση**
Στην παραγοντοποίηση ενός ακέραιου $n$ ένας συγκεκριμένος πρώτος $p$ ενδέχεται να εμφανίζεται περισσότερες από μία φορές. Αν οι διαφορετικοί πρώτοι παράγοντες του $n$ είναι οι $p_1, p_2, \ldots, p_r$ και κάθε $p_i$ εμφανίζεται σαν παράγοντας $a_i$ φορές τότε γράφουμε

$$n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r} = \prod_{i=1}^{r} p_i^{a_i}.$$

# 1.4 ΙΣΟΔΥΝΑΜΙΕΣ

Θα κάνουμε μια αναφορά σε ένα σημαντικό κλάδο της Θεωρίας Αριθμών, τη θεωρία Ισοδυναμιών (ή Ισοτιμιών). Η θεωρία Ισοδυναμιών εισήχθη από τον Gauss και βοήθησε πολύ στην αντιμετώπιση προβλημάτων σχετικών με τη διαιρετότητα των ακεραίων. Θα μελετήσουμε κάποια βασικά στοιχεία παρακάτω.

***Ορισμός***
Θεωρούμε τους ακέραιους $a, b, m$ με $m > 0$. Θα λέμε ότι ο $a$ είναι *ισοδύναμος με το* $b$ *modulo* $m$ και συμβολίζουμε

$$a \equiv b(\text{mod}m)$$

αν ο $m$ διαιρεί τη διαφορά $a - b$, δηλαδή

$$m|(a - b).$$

Ειδικότερα:

$$a \equiv 0(\text{mod}m) \iff m|a$$

$$a \equiv b(\text{mod}m) \iff (a - b) \equiv 0(\text{mod}m).$$

Αν $m \nmid (a - b)$ τότε λέμε ότι οι $a, b$ είναι *μη ισοδύναμοι* mod$m$. Συμβολίζουμε

$$a - b \not\equiv 0(\text{mod}m).$$

**Παραδείγματα**
1)$17 \equiv 12(\text{mod}5)$, $100 \equiv -40(\text{mod}20)$, $11 \equiv -1(\text{mod}12)$, $8 \equiv 2(\text{mod}2)$.
2)Ο $n$ είναι άρτιος αν και μόνο αν $n \equiv 0(\text{mod}2)$.
3)Ο $n$ είναι περιττός αν και μόνο αν $n \equiv 1(\text{mod}2)$.
4)Αν $a \equiv b(\text{mod}m)$ και $c|m$, $c > 0$, τότε $a \equiv b(\text{mod}c)$.

***Θεώρημα***
Η ισοτιμία $\equiv$ είναι σχέση ισοδυναμίας, δηλαδή έχουμε:
i)$a \equiv a(\text{mod}m)$
ii)Αν $a \equiv b(\text{mod}m)$ τότε $b \equiv a(\text{mod}m)$
iii)Αν $a \equiv b(\text{mod}m)$ και $b \equiv c(\text{mod}m)$ τότε $a \equiv c(\text{mod}m)$.

***Απόδειξη***
i)$a \equiv a(\text{mod}m) \iff m|(a-a) \iff m|0$
που ισχύει από ιδιότητες διαιρετότητας.
ii)$a \equiv b(\text{mod}m) \iff m|(a-b) \iff m|(b-a) \iff b \equiv a(\text{mod}m)$.
iii)$a \equiv b(\text{mod}m) \iff m|(a-b)$ και $b \equiv c(\text{mod}m) \iff m|(b-c)$ τότε

$$m|(a-b)+(b-c) \iff m|(a-c) \iff a \equiv c(\text{mod}m). \qquad \blacksquare$$

***Θεώρημα***
Αν $a \equiv b(\text{mod}m)$ και $c \equiv d(\text{mod}m)$ τότε:
i)$ax+cy \equiv bx+dy(\text{mod}m)$ , $\forall x, y \in \mathbb{Z}$
ii)$ac \equiv bd(\text{mod}m)$.

***Απόδειξη***
i)Αφού $m|(a-b)$ και $m|(c-d)$ έχουμε:

$$m\Big|[x(a-b)+y(c-d)] \iff m\Big|[(ax+cy)-(bx+dy)] \iff ax+cy \equiv bx+dy(\text{ mod } m)$$

ii)Από (i) για $x=c$, $y=-b$ έχουμε

$$ac-bd = c(a-b)+b(c-d) \equiv 0(\text{mod}m)$$

οπότε

$$ac \equiv bd(\text{mod}m). \qquad \blacksquare$$

**Παρατήρηση**
Θέτοντας $c=a$ και $d=b$ στο (ii) του παραπάνω θεωρήματος και χρησιμοποιώντας επαγωγή έχουμε:

$$a^n \equiv b^n(\text{mod}m) \ , \ n \geq 1.$$

**Παραδείγματα**
1)Είναι $19 \equiv 11(\text{mod}4)$ (α) και $6 \equiv 2(\text{mod}4)$ (β). Έχουμε:

$$25 \equiv 13(\text{mod}4)$$

$$13 \equiv 9(\text{mod}4)$$
$$114 \equiv 22(\text{mod}4)$$

αθροίζοντας, αφαιρώντας και πολλαπλασιάζοντας τις (α),(β) αντίστοιχα.

2)*Κριτήριο διαιρετότητας δια 9.*
Ένας ακέραιος $n > 0$ είναι διαιρετός δια 9 αν και μόνο αν το άθροισμα των ψηφίων του διαιρείται με το 9. Έχουμε

$$n = a_0 + 10a_1 + 10^2a_2 + \ldots + 10^k a_k$$

όπου $a_0, a_1, \ldots, a_k$ είναι τα ψηφία του $n$.
Από το προηγούμενο θεώρημα έχουμε modulo 9:

$$10 \equiv 1, 10^2 \equiv 1, \ldots, 10^k \equiv 1(\text{mod}9).$$

Άρα

$$n \equiv a_0 + a_1 + a_2 + \ldots + a_k(\text{mod}9). \qquad \blacksquare$$

Τα επόμενα θεωρήματα αναφέρουν μερικές ακόμα σημαντικές ιδιότητες των ισοτιμιών.

***Θεώρημα***
Αν $c > 0$, τότε

$$a \equiv b(\text{mod}m) \iff ac \equiv bc(\text{mod}cm).$$

***Απόδειξη***
Έχουμε

$$a \equiv b(\text{mod}m) \iff m|(a-b) \iff cm|c(a-b) \iff ac \equiv bc(\text{mod}cm). \ \blacksquare$$

***Θεώρημα (Νόμος Διαγραφής)***
Αν $ac \equiv bc(\text{mod}m)$ και $d = \text{gcd}(m, c)$ τότε

$$a \equiv b\Big(\text{ mod } \frac{m}{d}\Big).$$

***Απόδειξη***
Αφού $ac \equiv bc(\text{mod}m)$ έχουμε

$$m|c(a-b)$$

και επειδή $d = \text{gcd}(m, c)$ θα είναι

$$\frac{m}{d}\Big|\frac{c}{d}(a-b).$$

Όμως $\text{gcd}\,(\frac{m}{d}, \frac{c}{d}) = 1$ άρα

$$\frac{m}{d}\Big|(a-b) \iff a \equiv b(\text{mod}\frac{m}{d}). \qquad \blacksquare$$

**Παρατήρηση**
Ο νόμος της διαγραφής μας λέει ότι ένας κοινός παράγοντας $c$ μπορεί να απαλοιφεί από μια ισοτιμία αρκεί να διαιρέσουμε και το modulo με τον $d = \text{gcd}(c, m)$. Συγκεκριμένα, αν ένας κοινός παράγοντας και το modulo είναι πρώτοι μεταξύ τους τότε μπορεί ο κοινός παράγοντας να διαγραφεί από την ισοτιμία.

## 1.5 ΟΙ ΣΥΝΑΡΤΗΣΕΙΣ $\pi(x)$ ΚΑΙ $\Lambda(n)$

Σε αυτή την παράγραφο θα αναφερθούμε σε κάποιες συναρτήσεις, τις οποίες θα χρησιμοποιήσουμε εκτενώς στη συνέχεια. Η πρώτη είναι ίσως η πιο σημαντική για αυτή την εργασία και ορίζεται ως εξής:

***Ορισμός***
Η συνάρτηση $\pi(x)$ εκφράζει το πλήθος των πρώτων που δεν υπερβαίνουν τον πραγματικό αριθμό $x$. Μπορούμε να την εκφράσουμε ως

$$\pi(x) = \sum_{p \leq x} 1.$$

Παρατηρούμε ότι ο παραπάνω τύπος δεν είναι αρκετός ώστε να προσδιορίσει τις τιμές της $\pi(x)$. Τέτοιος τύπος δεν υπάρχει, αφού δεν γνωρίζουμε την κατανομή των πρώτων.
Στο κεφάλαιο 3 θα χρησιμοποιήσουμε αρκετά τη συνάρτηση $\pi(x)$ και θα αναφερθούμε στο θεώρημα των πρώτων αριθμών. Η μελέτη της συνάρτησης $\pi(x)$ περιέχει άλλη μια συνάρτηση, η οποία μετρά όχι μόνο τους πρώτους, αλλά και τις δυνάμεις αυτών. Ακολουθεί ο ορισμός αυτής, που ονομάζεται συνάρτηση von Mangoldt.

***Ορισμός***
Η συνάρτηση $\Lambda\colon \mathbb{N} \to \mathbb{C}$ ορίζεται για κάθε $n \in \mathbb{N}$ ως εξής:

$$\Lambda(n) = \begin{cases} \ln p & \text{, αν } n = p^r \text{ με } p \text{ πρώτο και } r \in \mathbb{N} \\ 0 & \text{, σε κάθε άλλη περίπτωση.} \end{cases}$$

***Θεώρημα***
Για κάθε $n \in \mathbb{N}$ έχουμε

$$\sum_{m|n} \Lambda(m) = \ln n.$$

***Απόδειξη***
Η παραπάνω σχέση είναι προφανής για $n = 1$.
Για την περίπτωση που $n \geq 2$ έχουμε:
Υποθέτουμε ότι

$$n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$$

είναι η πρώτη παραγοντοποίηση του $n$. Τότε οι μόνες μη μηδενικές συνεισφορές στο άθροισμα $\sum_{m|n} \Lambda(m)$ προέρχονται από τους φυσικούς αριθμούς $m$ που είναι της μορφής

$$m = p_j^{b_j} \ , \qquad j = 1, 2, \ldots, r \ , \ 1 \leq b_j \leq a_j.$$

Επομένως είναι

$$\sum_{m|n} \Lambda(m) = \sum_{j=1}^{r} \sum_{b_j=1}^{a_j} \ln p_j = \sum_{j=1}^{r} \ln p_j^{a_j} = \ln \left(p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}\right) = \ln n. \qquad \blacksquare$$

# Chapter 2

# Η ΑΠΕΙΡΙΑ ΤΩΝ ΠΡΩΤΩΝ

## 2.1 ΠΟΣΟΙ ΠΡΩΤΟΙ ΥΠΑΡΧΟΥΝ;

Δύο πολύ σημαντικές ιδιότητες της ακολουθίας των πρώτων είναι ότι υπάρχουν πάρα πολλοί από αυτούς, αλλά η πυκνότητά τους είναι σχετικά μικρή. Η απάντηση στην ερώτηση "πόσοι πρώτοι υπάρχουν;" δίνεται από το εξής θεμελιώδες θεώρημα:

***Θεώρημα***
Υπάρχουν άπειροι πρώτοι αριθμοί.

Στην πραγματικότητα, υπάρχουν άπειροι σε κάθε αριθμητική πρόοδο. Ο παραπάνω ισχυρισμός αποδείχτηκε από τον Dirichlet. Θα επανέλθουμε σε αυτό αργότερα. Πρώτα θα δώσουμε μερικές αποδείξεις του θεμελιώδους θεωρήματός μας. Κάποιες από αυτές τις αποδείξεις οφείλονται σε διάσημους μαθηματικούς, ενώ άλλες σε κάποιους "ξεχασμένους". Κάποιες χρησιμοποιούν στοιχειώδεις μεθόδους, άλλες ανάλυση και άλλες προέρχονται από τελείως διαφορετικούς κλάδους. Υπάρχουν ακόμα περισσότερες αποδείξεις της απειρίας των πρώτων(...αλλά σίγουρα δεν είναι άπειρες!). Ξεκινώντας θα αναφέρουμε την πιο διάσημη και παλαιότερη, την απόδειξη του Ευκλείδη:

***Απόδειξη(Ευκλείδης)***
Χρησιμοποιούμε τη μέθοδο της απαγωγής σε άτοπο. Υποθέτουμε λοιπόν ότι οι πρώτοι είναι πεπερασμένοι και ότι είναι κατά αύξουσα σειρά ακριβώς οι

$$p_1, p_2, \ldots, p_r.$$

Θεωρούμε τον αριθμό $N$ που ορίζεται ως εξής:

$$N = p_1 p_2 \dots p_r + 1$$

Ο $N$ είναι είτε πρώτος είτε σύνθετος.
Αν είναι πρωτος τότε $N > p_r$, όπου $p_r$ ο μεγαλύτερος πρώτος, το οποίο είναι άτοπο.
Αν είναι σύνθετος τότε από το θεμελιώδες θεώρημα της αριθμητικής θα έχει ένα πρώτο διαιρέτη έστω $p$. Όμως ο $p$ δεν είναι κανένας από τους $p_i \ , \ i = 1, 2, \dots, r$. Αν ήταν θα διαιρούσε και τον αριθμό $N$ αλλά και το γινόμενο $p_1 p_2 \dots p_r$, επομένως θα διαιρούσε και τη διαφορά τους:

$$N - p_1 p_2 \dots p_r = 1,$$

το οποίο είναι άτοπο. Έτσι το πεπερασμένο σύνολο $\{p_1, p_2, \dots, p_r\}$ δεν μπορεί να αναπαριστά όλους τους πρώτους. ■

Η απόδειξη του Ευκλείδη γοητεύει με την απλότητά της. Άλλη μια αντίστοιχη απόδειξη είναι αυτή του ολλανδού μαθηματικού Thomas Joannes Stieltjes που διετύπωσε το 1890.

***Απόδειξη(Stieltjes)***
Υποθέτουμε ότι $p_1, p_2, \dots, p_r$ είναι όλοι οι πρώτοι. Θέτουμε

$$N = p_1 p_2 \dots p_r$$

και έστω ότι $N = mn$ είναι μια παραγοντοποίηση του $N$, όπου $m, n \geq 1$. Κάθε ένας από τους $p_i$, διαιρεί ακριβώς έναν από τους αριθμούς $m, n$. Αν κάποιος διαιρούσε και τους δύο, έστω $p_k$ αυτός, τότε θα έπρεπε να ισχύει ότι $p_k^2 | N$, το οποίο είναι αδύνατο. Τότε όμως ο $m + n$ δεν διαιρείται από κανέναν από τους $p_i$, $i = 1, 2, \dots, r$, το οποίο όμως είναι άτοπο από το θεμελιώδες θεώρημα της αριθμητικής μιας και $m + n \geq 2$. ■

Η απόδειξη του Stieltjes κινήθηκε στο ίδιο μοτίβο με αυτή του Ευκλείδη. Από την άλλη μεριά ο Goldbach χρησιμοποίσε μια πολύ απλή και έξυπνη ιδέα:

***Ισχυρισμός***
Για να αποδείξουμε την απειρία των πρώτων είναι αρκετό να βρούμε μια άπειρη ακολουθία φυσικών αριθμών $\{a_k\}_{k \in \mathbb{N}}$ με $a_k > 1$, οι οποίοι είναι πρώτοι μεταξύ τους.

***Απόδειξη***
Έστω $q_i$, $i = 1, 2, \ldots$ πρώτοι με $q_1|a_1, q_2|a_2, \ldots$. Αφού οι αριθμοί $a_1, a_2, \ldots$ είναι πρώτοι μεταξύ τους δεν μπορούν να έχουν κοινό διαιρέτη. Οπότε

$$q_1 \neq q_2 \neq q_3 \neq \ldots$$

και έτσι προκύπτουν άπειροι το πλήθος πρώτοι αριθμοί. ■

Την παρακάτω απόδειξη την έγραψε ο Goldbach σε ένα γράμμα προς τον Euler το 1730. Χρησιμοποιεί τους αριθμούς Fermat και λέγεται ότι είναι η μόνη γραπτή απόδειξη του Goldbach:

***Απόδειξη(Goldbach)***
Σύμφωνα με τον προηγούμενο ισχυρισμό αρκεί να δείξουμε το εξής:

"Οι αριθμοί Fermat $F_n = 2^{2^n} + 1, n \geq 0$, είναι πρώτοι μεταξύ τους."

Για να το δείξουμε αυτό αρκεί να επαληθεύσουμε την αναδρομική σχέση:

$$\prod_{k=1}^{n-1} F_k = F_n - 2 \qquad , \qquad n \geq 1.$$

Πράγματι, αν $m$ είναι ένας διαιρέτης κάποιου $F_k$ και του $F_n$ $(k < n)$ τότε ο $m$ θα διαιρεί και το 2(αφού $2 = F_n - \prod_{k=1}^{n-1} F_k$).Επομένως $m = 1$ ή $m = 2$. Όμως ο $m$ δεν μπορεί να είναι 2 γιατί όλοι οι αριθμοί Fermat είναι περιττοί.
Τώρα για να αποδείξουμε την αναδρομή θα κάνουμε επαγωγή στο $n$:
Για $n = 1$ έχουμε $F_0 = 3$ και $F_1 - 2 = 3$. Επαγωγικά:

$$\prod_{k=0}^{n} F_k = (\prod_{k=0}^{n-1} F_k) \cdot F_n = (F_n - 2)F_n = (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2$$

Συνοψίζοντας, οι αριθμοί Fermat είναι πρώτοι μεταξύ τους, επομένως οι πρώτοι είναι άπειροι το πλήθος. ■

**Παρατηρήσεις**
•Βασιζόμενοι στην ιδέα της παραπάνω απόδειξης αξίζει να αναρωτηθούμε πώς μπορούμε να δημιουργήσουμε άπειρες ακολουθίες αριθμών που είναι πρώτοι μεταξύ τους. Το 1947 ο Bellman παρουσίασε μια μέθοδο δημιουργίας τέτοιων ακολουθιών. Η ιδέα είναι η εξής:

Έστω $f(x)$ ένα πολυώνυμο με ακέραιους συντελεστές. Έστω επίσης $f_1(x) = f(x)$ και ορίζουμε επαγωγικά

$$f_{n+1}(x) = f(f_n(x)) \qquad , \qquad n \geq 1.$$

Υποθέτουμε ότι $f(0) \neq 0$ και $f_n(0) = f(0)$, για κάθε $n \geq 2$.
Αν $n \neq 0$ και $\gcd(n, f(0)) = 1$ τότε $\gcd(f(n), f(0)) = 1$. Υπό αυτές τις συνθήκες, αν $\gcd(n, f(0)) = 1$ τότε οι ακέραιοι $n, f_1(n), f_2(n), \ldots$ είναι πρώτοι μεταξύ τους.
•Οι πέντε αρχικοί αριθμοί Fermat είναι οι $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$. Παρατηρούμε ότι και οι πέντε είναι πρώτοι. Ο $F_5$ ήδη έχει 10 ψηφία και γενικά η ακολουθία αυξάνει πολύ γρήγορα. Όμως $F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$ δηλαδή ο $F_5$ είναι σύνθετος. Ένα σημαντικό πρόβλημα αποτελεί το αν ο $F_n$ είναι πρώτος ή σύνθετος. Συγκεκριμένα αποτελεί ανοικτό πρόβλημα, όπως και τα ερωτήματα:
◦"Υπάρχουν άπειροι το πλήθος Fermat πρώτοι;"(Eisenstein 1844)
◦"Υπάρχουν άπειροι το πλήθος Fermat σύνθετοι;"

Ακολουθεί μια απόδειξη διαφορετική από τις προηγούμενες, η οποία κάνει χρήση ακέραιων πολυωνύμων. Έστω $\mathbb{Z}[x]$ το σύνολο των πολυωνύμων με ακέραιους συντελεστές και έστω $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

***Λήμμα***
Για κάθε μη σταθερό πολυώνυμο $f(x) \in \mathbb{Z}[x]$, το σύνολο των πρώτων διαιρετών των ακεραίων $\{f(k) : k \in \mathbb{N}_0\}$ είναι άπειρο. Επομένως και το συνολικό πλήθος των πρώτων είναι άπειρο.

***Απόδειξη***
Θεωρούμε πολυώνυμο

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m \quad , \quad f(x) \in \mathbb{Z}[x]$$

και υποθέτουμε ότι για το σύνολο $\{f(k) : k \in \mathbb{N}_0\}$, το πλήθος των πρώτων που διαιρούν κάποιο $f(k)$ είναι πεπερασμένο. Έστω $P = \{p_1, p_2, \ldots, p_n\}$ το σύνολο των προαναφερθέντων πρώτων και έστω $D = p_1 p_2 \ldots p_n$.
Χωρίς βλάβη της γενικότητας, θεωρούμε ότι $a_0 \neq 0$. Επιλέγουμε $t \in \mathbb{Z}$ τέτοιο ώστε $p_i^t \nmid f(0) = a_0$ , $i = 1, 2, \ldots, n$. Από το θεμελιώδες θεώρημα της αριθμητικής και επειδή οι $p_i$ είναι όλοι οι πρώτοι αριθμοί θα είναι $a_0 = p_{k_1}^{b_1} p_{k_2}^{b_2} \ldots p_{k_m}^{b_m}$, όπου $p_{k_1}, p_{k_2}, \ldots, p_{k_m}$ είναι αναδιάταξη των $\{p_1, p_2, \ldots, p_n\}$,

$m \leq n$ και $b_1, b_2, \ldots, b_m \leq t$. Άρα

$$a_0 | D^t = p_1^t p_2^t \ldots p_n^t.$$

Τότε υπάρχει $b \in \mathbb{Z}$ τέτοιο ώστε $D^t = a_0 b$. Για $k > 1$ έχουμε:

$$f(kD^{2t}) = \sum_{j=1}^{m} a_j k^j D^{2tj} + a_0 = a_0 \Big( \sum_{j=1}^{m} a_j k^j b^{2j} a_0^{2j-1} + 1 \Big) = M.$$

Επιλέγοντας $k$ αρκετά μεγάλο, ο ακέραιος $M$ θα έχει ένα πρώτο διαιρέτη $p > a_0 b$. Τότε όμως $p > D^t = p_1^t p_2^t \ldots p_n^t$, δηλαδή $p > p_i \ \ , \ \ i = 1, 2, \ldots, n$ και $p | f(kD^{2t})$. Επομένως $p \notin P$ το οποίο μας οδηγεί σε άτοπο. ■

Κλείνουμε την ενότητα των στοιχειωδών αποδείξεων με μια απόδειξη που οφείλεται στον Euler. Ο Euler έδειξε ότι υπάρχουν άπειροι πρώτοι επειδή μια συγκεκριμένη έκφραση που σχηματίζεται από όλους τους πρώτους τείνει στο άπειρο.

***Απόδειξη(Euler)***
Έστω με απαγωγή σε άτοπο ότι $p_1, p_2, \ldots, p_n$ είναι όλοι οι πρώτοι.Αφού $\frac{1}{p_i} < 1 \ \ , \ \ i = 1, 2, \ldots, n$ έχουμε:

$$\sum_{k=0}^{\infty} \frac{1}{p_1^k} = \frac{1}{1 - \frac{1}{p_1}}$$

$$\sum_{k=0}^{\infty} \frac{1}{p_2^k} = \frac{1}{1 - \frac{1}{p_2}}$$

$$\vdots$$

$$\sum_{k=0}^{\infty} \frac{1}{p_n^k} = \frac{1}{1 - \frac{1}{p_n}}$$

και πολλαπλασιάζοντας τις $n$ εξισώσεις κατά μέλη έχουμε:

$$\prod_{i=1}^{n} \Big( \sum_{k=0}^{\infty} \frac{1}{p_i^k} \Big) = \prod_{i=1}^{n} \frac{1}{1 - \frac{1}{p_i}}$$

Το αριστερό μέλος της ισότητας είναι το άθροισμα των αντιστρόφων όλων των φυσικών αριθμών, με κάθε ένα να τον μετράμε μια φορά. Αυτός ο ισχυρισμός

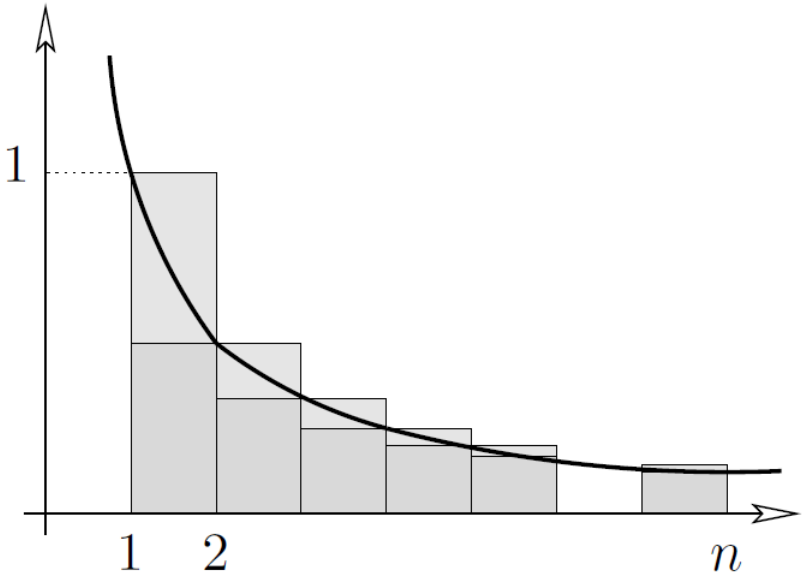
προκύπτει από το θεμελιώδες θεώρημα της αριθμητικής σύμφωνα με το οποίο κάθε φυσικός αριθμός γράφεται ως γινόμενο πρώτων παραγόντων κατά μοναδικό τρόπο. Επομένως:

$$\prod_{i=1}^{n}\Big(\sum_{k=0}^{\infty}\frac{1}{p_i^k}\Big)=\sum_{n=1}^{\infty}\frac{1}{n}$$

και είναι γνωστό ότι η σειρά $\sum_{n=1}^{\infty}\frac{1}{n}$ αποκλίνει. Αντίθετα το δεξί μέλος είναι προφανώς πεπερασμένο, οπότε καταλήγουμε σε άτοπο. ■

Στη συνέχεια θα χρησιμοποιήσουμε αναλυτικές μεθόδους για την απόδειξη του βασικού μας θεωρήματος.

***Απόδειξη***
Έστω $\pi(x)$ η συνάρτηση που έχει ήδη οριστεί, η οποία μετρά τον αριθμό των πρώτων που είναι μικρότεροι ή ίσοι με τον πραγματικό αριθμό $x$. Τοποθετούμε τους πρώτους $p_1, p_2, p_3, \ldots$ σε αύξουσα σειρά και θεωρούμε τη συνάρτηση $\ln x$, η οποία ορίζεται ως $\ln x = \int_1^x \frac{1}{t}\,dt$. Θα συγκρίνουμε το εμβαδόν του χωρίου ανάμεσα στη γραφική παράσταση της $f(t)=\frac{1}{t}$ και του οριζόντιου άξονα με μια συνάρτηση σκαλοπάτι.



Για $n \leq x < n+1$ έχουμε:

$$\ln x \leq 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n-1} + \frac{1}{n} \leq \sum \frac{1}{m},$$

όπου το άθροισμα εκτείνεται σε όλα τα $m \in \mathbb{N}$, που έχουν μόνο πρώτους διαιρέτες $p \leq x$. Επειδή κάθε τέτοιο $m$ μπορεί να γραφεί κατά μοναδικό τρόπο ως γινόμενο της μορφής $\prod_{p \leq x} p^{k_p}$, βλέπουμε ότι το παραπάνω άθροισμα ισούται με

$$\prod_{p \leq x} \Big( \sum_{k \geq 0} \frac{1}{p^k} \Big).$$

Αυτό ισχύει γιατί

$$\prod_{p \leq x} \Big( \sum_{k \geq 0} \frac{1}{p^k} \Big) = (\frac{1}{2} + \frac{1}{2^2} + \ldots) \cdot (\frac{1}{3} + \frac{1}{3^2} + \ldots) \cdot \ldots \cdot (\frac{1}{p_r} + \frac{1}{p_r^2} + \ldots)$$

και αν αναπτύξουμε τα γινόμενα προκύπτουν όλοι οι αντίστροφοι των φυσικών $m$ γραμμένοι σε γινόμενο πρώτων παραγόντων.
Επίσης είναι γνωστό ότι $\sum_{k \geq 0} \frac{1}{p^k} = \frac{1}{1 - \frac{1}{p}}$, αφού $\frac{1}{p} < 1$.Επομένως έχουμε:

$$\ln x \leq \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}} = \prod_{p \leq x} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}.$$

Όμως γνωρίζουμε ότι $p_k \geq k+1$ και έτσι:

$$\frac{p_k}{p_k - 1} = \frac{p_k - 1 + 1}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leq 1 + \frac{1}{k} = \frac{k+1}{k}.$$

Άρα

$$\ln x \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1.$$

Αλλά η συνάρτηση $\ln x$ δεν είναι φραγμένη, οπότε και η $\pi(x)$ θα είνα μη φραγμένη, το οποίο σημαίνει ότι υπάρχουν άπειροι πρώτοι. ■

Συνεχίζουμε αποδεικνύοντας πως οι πρώτοι αριθμοί όχι μόνο είναι άπειροι, αλλά και η σειρά $\sum_p \frac{1}{p}$ αποκλίνει. Αυτή η απόδειξη επινοήθηκε από τον διάσημο μαθηματικό Paul Erdős.

***Απόδειξη(Erdős)***
Έστω $p_1, p_2, p_3, \ldots$ η ακολουθία των πρώτων σε αύξουσα σειρά. Θα ονομάσουμε τους $p_1, p_2, \ldots, p_k$ "μικρούς" πρώτους και τους $p_{k+1}, p_{k+2}, \ldots$ μεγάλους πρώτους. Υποθέτουμε με απαγωγή σε άτοπο ότι η σειρά $\sum_p \frac{1}{p}$ συγκλίνει.Τότε υπάρχει φυσικός αριθμός $k$ τέτοιος ώστε

$$\sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2}.$$

Επίσης για τυχαίο φυσικό αριθμό $N$ έχουμε:

$$\sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}.$$

Θέτουμε $N_b$ το πλήθος των φυσικών $n \leq N$, οι οποίοι διαιρούνται από τουλάχιστον ένα μεγάλο πρώτο και $N_s$ το πλήθος των φυσικών $n \leq N$, οι οποίοι έχουν μόνο μικρούς πρώτους διαιρέτες.
Θα αποδείξουμε ότι για συγκεκριμένο $N$ έχουμε:

$$N_b + N_s < N,$$

το οποίο θα είναι άτοπο, αφού εξ ορισμού είναι $N_b + N_s = N$.
Για να υπολογίσουμε το $N_b$ παρατηρούμε ότι το $\left\lfloor \frac{N}{p_i} \right\rfloor$ μετρά τους φυσικούς $n \leq N$ οι οποίοι είναι πολλαπλάσια του $p_i$. Έτσι συνδυάζοντας αυτή τη σχέση με την $\sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}$ έχουμε:

$$N_b \leq \sum_{i \geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor < \frac{N}{2} \qquad (1)$$

Για το $N_s$ εργαζόμαστε ως εξής:
Παρατηρούμε ότι για κάθε φυσικό αριθμό $n$ έχουμε:

$$n = p_1^{2a_1} p_2^{2a_2} \ldots p_k^{2a_k} q_1^{2b_1+1} q_2^{2b_2+1} \ldots q_l^{2b_l+1} = (p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} q_1^{b_1} q_2^{b_2} \ldots q_l^{b_l})^2 q_1 q_2 \ldots q_l$$

όπου $p_i, q_i$ πρώτοι.
Έτσι $n = a^2 b$ με τον $b$ ελεύθερο τετραγώνου. Οπότε κάθε $n \leq N$ που έχει μόνο μικρούς παράγοντες, το γράφουμε στη μορφή $n = a_n^2 b_n$, με τον $b_n$ ελεύθερο τετραγώνου. Τότε όμως όλοι οι $b_n$ θα είναι γινόμενο διαφορετικών μικρών

πρώτων και θα είναι $b_n = 2^{e_1}3^{e_2}\dots p_k^{e_k}$ με $e_i = 0$ ή 1. Έτσι υπάρχουν το πολύ $2^k$ επιλογές για το $b_n$. Ακόμα, επειδή $a_n \leq \sqrt{n} \leq \sqrt{N}$ συμπεραίνουμε ότι υπάρχουν το πολύ $\sqrt{N}$ επιλογές για το $a_n$. Άρα

$$N_s \leq 2^k\sqrt{N}.$$

Όμως αφού η $(1)$ ισχύει για κάθε $n \in \mathbb{N}$ αρκεί να βρούμε $N$ τέτοιο ώστε

$$2^k\sqrt{N} \leq \frac{N}{2} \Longrightarrow 2^{k+1} \leq \sqrt{N}.$$

Επιλέγοντας το $N = 2^{2k+2}$ προκύπτει ότι

$$N_b < \frac{N}{2} \quad \text{και} \quad N_s \leq \frac{N}{2}$$

δηλαδή $N_b + N_s < N$, το οποίο είναι άτοπο.
Όμως υποθέσαμε ότι η $\sum_p \frac{1}{p}$ συγκλίνει, επομένως οι πρώτοι είναι άπειροι και επιπλέον το άπειρο άθροισμα των αντιστρόφων τους αποκλίνει. ■

Κλείνοντας το κεφάλαιο για την απειρία των πρώτων αξίζει να σημειώσουμε πως υπάρχουν και άλλες αποδείξεις, στις οποίες χρησιμοποιούνται έννοιες από τελείως "απρόσμενους" κλάδους των μαθηματικών, όπως η τοπολογία και η θεωρία κωδίκων. Θα καταγράψουμε την τοπολογική απόδειξη.

***Απόδειξη(τοπολογική)***
Κατασκευάζουμε μια τοπολογία στο $\mathbb{Z}$ ως εξής:
Για $a, b \in \mathbb{Z}$ με $b > 0$ ορίζουμε

$$N_{a,b} = \{a + nb \ : \ n \in \mathbb{Z}\}.$$

Το σύνολο $O \subset \mathbb{Z}$ καλείται ανοικτό αν $O = \varnothing$ ή αν για κάθε $x \in O$, υπάρχει $b > 0$ τέτοιο ώστε $N_{x,b} \subset O$. Τότε είναι προφανές ότι αυθαίρετες ενώσεις παραμένουν ανοικτό σύνολο. Για να δείξουμε ότι πεπερασμένες τομές είναι ανοικτό, θεωρούμε $m$ θετικό ακέραιο και όποτε τα σύνολα $O_1, O_2, \dots, O_m$ είναι ανοικτά με $y \in O_1 \cap O_2 \cap \dots \cap O_m$ και $N_{a,b_i} \subset O_i$, τότε θέτουμε $b = \text{lcm}^*(b_1, b_2, \dots, b_m)$ έτσι ώστε $y \in N_{a,b} \subset O_1 \cap O_2 \cap \dots \cap O_m$. Επομένως έχουμε ορίσει μια τοπολογία στο $\mathbb{Z}$.

Ακολουθούν δύο ιδιότητες αυτής της τοπολογίας:

1)Κάθε μη-κενό ανοικτό σύνολο είναι άπειρο.
2)Κάθε σύνολο $N_{a,b}$ είναι κλειστό.

Η πρώτη ιδιότητα προέρχεται από τον ορισμό που δώσαμε για τα ανοικτά. Η δεύτερη από το γεγονός ότι

$$N_{a,b} = \mathbb{Z} \backslash \bigcup_{i=1}^{b-1} N_{a+i,b}$$

μιας και το σύνολο $N_{a,b}$ είναι το συμπλήρωμα ενός ανοικτού συνόλου. Άρα είναι κλειστό.

Όμως γνωρίζουμε ότι κάθε $n \in \mathbb{Z}$ με $n \neq 1, 0, -1$ έχει τουλάχιστον ένα πρώτο διαιρέτη $p$. Έτσι κάθε $n$ θα περιέχεται στο σύνολο

$$\mathbb{Z} \backslash \{-1, 1\} = \bigcup_{p \text{ πρώτος}} N_{0,p} \, .$$

Αν το πλήθος των πρώτων ήταν πεπερασμένο, τότε το $\bigcup_p N_{0,p}$ θα ήταν πεπερασμένη ένωση και θα έπρεπε να είναι κλειστό από την ιδιότητα (2). Όμως το συμπλήρωμα ενός κλειστού συνόλου είναι ανοικτό, οπότε το σύνολο $\{-1, 1\}$ θα ήταν ανοικτό και άπειρο από την ιδιότητα (1). Επομένως καταλήξαμε σε άτοπο που σημαίνει ότι το πλήθος των πρώτων είναι άπειρο. ■

∗lcm=least common multiple( ελάχιστο κοινό πολλαπλάσιο)

Για τον αναγνώστη που ενδιαφέρεται προτείνεται η μελέτη της απόδειξης μέσω της θεωρίας κωδίκων. Μπορεί να τη βρει στο [6], παράγραφος 3.1.6, σελ. 83-84.

## 2.2 ΤΟ ΘΕΩΡΗΜΑ ΤΟΥ DIRICHLET

Το σύνολο των περιττών αριθμών περιέχει άπειρους πρώτους. Επομένως μοιάζει λογικό να αναρωτηθούμε πότε άλλες παρόμοιες ακολουθίες έχουν την ίδια ιδιότητα. Θα εξετάσουμε τις ακολουθίες της μορφής

$$\{an + b\}.$$

Αν οι $a, b$ είχαν ένα κοινό διαιρέτη $d$, κάθε ένας όρος της ακολουθίας θα διαιρούνταν από το $d$ και έτσι θα μπορούσαμε να έχουμε το πολύ ένα πρώτο στην $\{an + b\}$, (για $n = 0$).
Έτσι μια αναγκαία συνθήκη για την ύπαρξη άπειρων πρώτων στις ακολουθίες που εξετάζουμε είναι η $\gcd(a, b) = 1$. Ο Dirichlet απέδειξε ότι η παραπάνω συνθήκη είναι και ικανή, δηλαδή ότι αν $\gcd(a, b) = 1$ με $a, b \in \mathbb{N}$, τότε υπάρχουν άπειροι πρώτοι στην αριθμητική πρόοδο $\{an + b\}$.
Αυτό το αποτέλεσμα μπορεί να μη μοιάζει τόσο σημαντικό σε κάποιον, ειδικότερα μετά το σύνολο των αποδείξεων της απειρίας των πρώτων που αναφέραμε. Παρ' όλα αυτά, λαμβάνοντας υπ' όψιν ότι σύμφωνα με το Prime Number Theorem (κεφάλαιο 3) η πυκνότητα των πρώτων γίνεται όλο και πιο μικρή όσο οι αριθμοί μεγαλώνουν, το θεώρημα του Dirichlet μοιάζει πολύ σημαντικό.

Παρακάτω θα εξετάσουμε διάφορες περιπτώσεις του θεωρήματος του Dirichlet. Η απόδειξή του θα μπορούσε κάλλιστα να είναι το θέμα κάποιας άλλης διπλωματικής εργασίας. Αν κάποιος αναγνώστης ενδιαφέρεται μπορεί να ρίξει μια ματιά στο [3] κεφάλαιο 7.

***Θεώρημα***
Υπάρχουν άπειροι πρώτοι της μορφής $3n + 2$.

***Απόδειξη***
Υποθέτουμε ότι $p_1, p_2, \ldots, p_k$ είναι όλοι οι πρώτοι που είναι ισοϋπόλοιποι $2 \bmod 3$ και έστω

$$x = p_1 p_2 \ldots p_k.$$

Αν $x \equiv 1 \bmod 3$ τότε

$$x + 1 \equiv 2 \bmod 3$$

και θα υπάρχει πρώτος $p_i \equiv 2 \bmod 3$, που θα διαιρεί τον $x + 1$. Όμως

$$p_i | x = p_1 p_2 \ldots p_k \ \ \& \ \ p_i | x + 1,$$

οπότε σύμφωνα με το συλλογισμό στην απόδειξη του Ευκλείδη καταλήγουμε σε άτοπο.
Αν $x \equiv 2 \bmod 3$ τότε

$$x + 3 \equiv 2 \bmod 3$$

και όπως προηγουμένως θα υπάρχει πρώτος $p_i \equiv 2 \bmod 3$ που διαιρεί τον $x + 3$. Όμως πάλι

$$p_i | x \ \ \& \ \ p_i | x + 3$$

το οποίο είναι άτοπο αφού $p_i \neq 3$.
Από τις δύο παραπάνω περιπτώσεις που κατέληξαν σε άτοπο συμπεραίνουμε ότι υπάρχουν άπειροι πρώτοι της μορφής $3n + 2$. ■

***Θεώρημα***
Υπάρχουν άπειροι πρώτοι της μορφής $4n - 1$.

***Απόδειξη***
Με απαγωγή σε άτοπο υποθέτουμε ότι υπάρχουν πεπερασμένοι πρώτοι αυτής της μορφής. Θεωρούμε $p$ τον μεγαλύτερο και θέτουμε

$$N = 2^2 \cdot 3 \cdot 5 \cdot \ldots \cdot p - 1.$$

Το γινόμενο $3 \cdot 5 \cdot \ldots \cdot p$ περιέχει ως παράγοντες όλους τους περιττούς πρώτους. Επειδή το $N$ είναι της μορφής $4n-1$ δεν μπορεί να είναι πρώτος αφού $N > p$. Επίσης κανένας πρώτος $\leq p$ δεν διαιρεί το $N$. Έτσι όλοι οι πρώτοι παράγοντες του $N$ πρέπει να είναι μεγαλύτεροι του $p$. Όμως δεν γίνεται όλοι οι διαιρέτες του $N$ να είναι της μορφής $4n + 1$ γιατί το γινόμενο τέτοιων αριθμών είναι και αυτό της ίδιας μορφής. Επομένως τουλάχιστον ένας πρώτος παράγοντας του $N$ θα είναι της μορφής $4n-1$ μιας και οι $4n+2$ και $4n$ είναι άρτιοι. Οπότε καταλήξαμε σε άτοπο και η υπόθεσή μας για την ύπαρξη πεπερασμένων πρώτων της μορφής $4n - 1$ είναι εσφαλμένη. ■

***Θεώρημα***
Υπάρχουν άπειροι πρώτοι της μορφής $6n + 5$.

***Απόδειξη***
Εργαζόμαστε όπως προηγουμένως με $p$ το μεγαλύτερο πρώτο της μορφής $6n + 5$. Θεωρούμε τον αριθμό

$$N = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p - 1.$$

Παρατηρούμε ότι κάθε πρώτος, εκτός των $2, 3$, είναι της μορφής $6n + 1$ και $6n + 5$. Επίσης το γινόμενο δύο αριθμών της μορφής $6n + 1$ είναι και αυτό της ίδιας μορφής.Όμως

$$N \equiv -1 \bmod 6 \equiv 5 \bmod 6.$$

Οπότε τουλάχιστον ένας πρώτος παράγοντας του $N$ θα είναι της μορφής $6n+5$ (αφού οι $6n$, $6n + 2$, $6n + 4$ είναι άρτιοι).
Επομένως υπάρχει πρώτος $6n + 5 > p$ το οποίο είναι άτοπο. Άρα οι πρώτοι της μορφής $6n + 5$ είναι άπειροι. ■

Θα δείξουμε και την απειρία των πρώτων της μορφής $8n + 5$. Πρώτα θα αναφέρουμε χωρίς απόδειξη ένα σημαντικό θεώρημα:

***Θεώρημα***
Αν οι αριθμοί $a, b$ δεν έχουν κοινούς διαιρέτες, τότε κάθε περιττός πρώτος διαιρέτης του $a^2 + b^2$ είναι της μορφής $4n + 1$.

**Παρατήρηση**
Άμεσο αποτέλεσμα του παραπάνω θεωρήματος είναι ότι υπάρχουν άπειροι πρώτοι της μορφής $4n + 1$.

***Θεώρημα***
Υπάρχουν άπειροι πρώτοι της μορφής $8n + 5$.

***Απόδειξη***
Θεωρούμε τον αριθμό

$$q = 3^2 \cdot 5^2 \cdot 7^2 \cdot \ldots \cdot p^2 + 2^2.$$

Ο $q$ είναι το άθροισμα δύο τετραγώνων, τα οποία δεν έχουν κοινούς διαιρέτες. Επίσης το τετράγωνο ενός περιττού αριθμού $2m + 1$ είναι:

$$(2m + 1)^2 = 4m^2 + 4m + 1 = 4m(m + 1) + 1.$$

Οπότε ο περιττός $3^2 \cdot 5^2 \cdot 7^2 \cdot \ldots \cdot p^2$ είναι της μορφής $8n + 1$ (αφού το γινόμενο των διαδοχικών $m, m + 1$ είναι άρτιος).
Άρα ο $q$ είναι της μορφής $8n+5$. Ακολουθώντας την ίδια διαδικασία μπορούμε να κατασκευάσουμε άπειρους πρώτους της μορφής $8n + 5$. ■

Τέλος ακολουθεί χωρίς απόδειξη το θεώρημα του Dirichlet:

***Θεώρημα Dirichlet***
Αν $a > 0$ και $\gcd(a, b) = 1$ τότε υπάρχουν άπειροι πρώτοι στην αριθμητική πρόοδο

$$an + b \ , \ \ n = 0, 1, 2, \dots \ .$$

## 2.3 ΤΟ ΑΙΤΗΜΑ ΤΟΥ BERTRAND

Έχουμε δει ότι η ακολουθία των πρώτων αριθμών είναι άπειρη. Παρ΄ όλα αυτά γνωρίζουμε ότι τα κενά μεταξύ των πρώτων είναι πολύ μεγάλα. Στην πραγματικότητα μπορούμε να βρούμε όσους συνεχόμενους σύνθετους επιθυμούμε. Παρατηρούμε ότι για τους αριθμούς:

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$$

ισχύει ότι:

$$2\Big|\Big[(n+1)!+2\Big], 3\Big|\Big[(n+1)!+3\Big], \ldots, (n+1)\Big|\Big[(n+1)!+(n+1)\Big].$$

Επομένως έχουμε $n$ διαδοχικούς σύνθετους.Για παράδειγμα, για $n=5$ έχουμε:

$$2|722,\ \ 3|723,\ \ 4|724,\ \ 5|725,\ \ 6|726.$$

Υπάρχουν όμως και ανώτατα όρια για τα κενά στην ακολουθία των πρώτων. Ένα τέτοιο όριο, γνωστό και ως Αίτημα του Bertrand, αναφέρει ότι:
"Το κενό μέχρι τον επόμενο πρώτο δεν μπορεί να είναι μεγαλύτερο από τον αριθμό που ξεκινήσαμε την αναζήτησή μας."
Ο Joseph Bertrand είκασε και επαλήθευσε εμπειρικά για $n < 3,000,000$ αυτόν τον ισχυρισμό. Η πρώτη απόδειξη οφείλεται στον Pafnuty Chebyshev το 1850. Παρακάτω θα δώσουμε την απόδειξη του Αιτήματος του Bertrand όπως την διατύπωσε ο Paul Erdős σε ηλικία 19 ετών.

***Αίτημα του Bertrand***
Για κάθε $n \geq 1$, υπάρχει κάποιος πρώτος $p$ τέτοιος ώστε

$$n < p \leq 2n.$$

***Απόδειξη***
Θα υπολογίσουμε το μέγεθος των δυωνυμικών συντελεστών $\binom{2n}{n}$ με σκοπό να δούμε ότι αν δεν είχαν κανένα πρώτο παράγοντα $p$ με $n < p \leq 2n$, τότε θα ήταν πολύ μικροί.
Θα δουλέψουμε σε πέντε στάδια:
1)Πρώτα ελέγχουμε το αίτημα για $n < 4000$. Φυσικά δεν θα χρειαστεί να ελέγξουμε και τις 4000 περιπτώσεις. Αρκεί να παρατηρήσουμε ότι η:

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$$

είναι η ακολουθία των πρώτων, όπου κάθε ένας είναι μικρότερος από τον διπλάσιο του προηγούμενού του. Έτσι κάθε σύνολο $\{y : n < y \leq 2n\}$ με $n \leq 4000$, περιέχει έναν από αυτούς τους 14 πρώτους.
2)Τώρα θα δείξουμε ότι

$$\prod_{p \leq x} p \leq 4^{x-1} \ , \ \ x \geq 2. \ (1)$$

Θα χρησιμοποιήσουμε επαγωγή στο πλήθος των πρώτων. Πρώτα παρατηρούμε ότι αν $q$ ο μεγαλύτερος πρώτος με $q \leq x$ τότε:

$$\prod_{p \leq x} p = \prod_{p \leq q} p \ \text{ και } \ 4^{q-1} \leq 4^{x-1}.$$

Έτσι αρκεί να δείξουμε την $(1)$ για $x = q$, όπου $q$ πρώτος.
Για $q = 2$ έχουμε $2 \leq 4$ που ισχύει. Θα ελέγξουμε τους περιττούς πρώτους $q = 2m + 1$. Έστω η επαγωγική υπόθεση ότι ισχύει για όλους τους ακέραιους $x \leq 2m$.
Για $q = 2m + 1$ έχουμε:

$$\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p \cdot \prod_{m+1 < p \leq 2m+1} p \leq 4^m \cdot \binom{2m+1}{m} \leq 4^m \cdot 2^{2m} = 4^{2m}$$

όπου

$$\prod_{m+1 < p \leq 2m+1} p \leq \binom{2m+1}{m}$$

προκύπτει από το ότι ο

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$$

είναι ακέραιος, στον οποίο οι πρώτοι που περιέχονται στο γινόμενο είναι παράγοντες του αριθμητή $(2m+1)!$, αλλά όχι του παρονομαστή $m!(m+1)!$. Άρα

$$\prod_{m+1 < p \leq 2m+1} p \Big| \binom{2m+1}{m},$$

οπότε προκύπτει η ανισότητα.
Επίσης είναι

$$\binom{2m+1}{m} \leq 2^{2m}$$

μιας και

$$\binom{2m+1}{m} = \binom{2m+1}{m+1} \text{ και } \sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1}.$$

3)Θα χρειαστούμε το θεώρημα του Legendre. Έχουμε:

***Θεώρημα Legendre***
Ο αριθμός $n!$ περιέχει τον πρώτο παράγοντα $p$ ακριβώς

$$\sum_{k\geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$$

φορές.

***Απόδειξη***
Από τον $p$ διαιρούνται ακριβώς $\lfloor \frac{n}{p} \rfloor$ παράγοντες του $n!$.
Από τον $p^2$ διαιρούνται ακριβώς $\lfloor \frac{n}{p^2} \rfloor$ παράγοντες του $n!$.

$$\vdots$$

Οπότε προσθέτοντας τα παραπάνω ακέραια μέρη βρίσκουμε το ζητούμενο. ■

Άρα από το θεώρημα Legendre ο αριθμός

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

περιέχει τον πρώτο παράγοντα $p$ ακριβώς

$$\sum_{k\geq 1} \left( \left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor \right)$$

φορές. Κάθε προσθετέος είναι το πολύ 1 αφού ισχύει:

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor < \frac{2n}{p^k} - 2\left(\frac{n}{p^k} - 1\right) = 2$$

και είναι ακέραιος.
Επίσης οι προσθετέοι για τους οποίους $p^k > 2n$ μηδενίζονται. Επομένως ο $\binom{2n}{n}$ περιέχει το $p$ ακριβώς

$$\sum_{k\geq 1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right) \leq \max\{r:\ \ p^r \leq 2n\}$$

φορές. Άρα η μεγαλύτερη δύναμη του $p$ που διαιρεί τον $\binom{2n}{n}$ δεν μπορεί να ξεπερνά το $2n$.
Στην πραγματικότητα, οι πρώτοι $p > \sqrt{2n}$ εμφανίζονται το πολύ μία φορά στο $\binom{2n}{n}$. Ακόμα, οι πρώτοι $p$ με $\frac{2}{3}n < p \leq n$ δεν διαιρούν το $\binom{2n}{n}$. Πράγματι, το ότι $3p > 2n$ συνεπάγεται ότι οι αριθμοί $p$ και $2p$ είναι τα μόνα πολλαπλάσια του $p$ που είναι παράγοντες του αριθμητή του $\binom{2n}{n} = \frac{(2n)!}{n!n!}$. Ο παρονομαστής έχει δύο φορές παράγοντα τον $p$.
4)Τώρα μπορούμε να υπολογίσουμε το $\binom{2n}{n}$.
Για $n \geq 3$ γνωρίζουμε ότι $\binom{2n}{n} \geq \frac{4^n}{2n}$ οπότε έχουμε:

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

και επειδή δεν υπάρχουν περισσότεροι απο $\sqrt{2n}$ πρώτοι $p$ με $p \leq \sqrt{2n}$ έχουμε:

$$4^n \leq (2n)^{1+\sqrt{2n}} \cdot \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \cdot \prod_{n<p\leq 2n} p\ ,\ \ n \geq 3\ \ (2)$$

5)Υποθέτουμε ότι δεν υπάρχει πρώτος $p$ με $n < p \leq 2n$. Έτσι το δεύτερο γινόμενο στο δεξί μέλος της $(2)$ θα ισούται με τη μονάδα. Από $(1), (2)$ έχουμε:

$$4^n \leq (2n)^{1+\sqrt{2n}} \cdot 4^{\frac{2}{3}n}$$

δηλαδή

$$4^{\frac{1}{3}n} \leq (2n)^{1+\sqrt{2n}} \qquad (3).$$

Η $(3)$ όμως δεν είναι σωστή για $n$ αρκετά μεγάλο. Πράγματι, είναι γνωστό ότι $a + 1 < 2^a$, για $a \geq 2$, οπότε:

$$2n = \left(\sqrt[6]{2n}\right)^6 < \left(\left\lfloor\sqrt[6]{2n}\right\rfloor + 1\right)^6 < 2^{6\lfloor\sqrt[6]{2n}\rfloor} \leq 2^{6\sqrt[6]{2n}} \qquad (4).$$

Τότε για $n \geq 50$ (δηλαδή $18 < 2\sqrt{2n}$) από $(3), (4)$ είναι:

$$2^{2n} \leq (2n)^{3\left(1+\sqrt{2n}\right)} < 2^{\sqrt[6]{2n}\left(18+18\sqrt{2n}\right)} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{2/3}}.$$

Άρα

$$(2n)^{1/3} < 20$$

το οποίο συνεπάγεται ότι $n < 4000$ και καταλήξαμε σε άτοπο. ■

**Άσκηση 1**
Έστω $p_n$ ο νιοστός πρώτος. Να δείξετε ότι $p_n < 2^n$ για $n \geq 2$.

**Λύση**
Θα εργαστούμε επαγωγικά στο $n$.
Για $n = 2$ έχουμε $p_2 = 3 < 2^2$.
Έστω ότι ισχύει για $n = k$, δηλαδή $p_k < 2^k$. Θα δείξουμε ότι $p_{k+1} < 2^{k+1}$.
Από το αίτημα του Bertrand υπάρχει πρώτος ανάμεσα στους $p_k$ και $2p_k$, οπότε $p_{k+1} < 2p_k$. Όμως από επαγωγική υπόθεση $p_k < 2^k$, άρα

$$p_{k+1} < 2p_k < 2 \cdot 2^k = 2^{k+1}.$$

Άρα $p_n < 2^n$ για $n \geq 2$.

**Άσκηση 2**
Χρησιμοποιώντας το Αίτημα του Bertrand θα δείξουμε ότι αν $m \geq 2$ και $m! = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$, τότε $a_i = 1$ για τουλάχιστον μια τιμή του $i$.

**Λύση**
Για $m = 2$ το παραπάνω προφανώς ισχύει.
Για $m > 2$ θέτουμε $m = 2k$ ή $m = 2k + 1$, αν ο $m$ είναι άρτιος ή περιττός αντίστοιχα. Αν ο $p$ είναι πρώτος μεταξύ των $k$ και $2k$ τότε $2p > m$. Επομένως ο εκθέτης του $p$ στην παραγοντοποίηση του $m!$ θα είναι ακριβώς 1.

## 2.4 ΔΙΔΥΜΟΙ ΠΡΩΤΟΙ

Αν οι αριθμοί $p$ και $p+2$ είναι πρώτοι, τότε ονομάζονται δίδυμοι πρώτοι. Τα μικρότερα ζεύγη δίδυμων πρώτων είναι τα

$$\{3,5\} \ , \ \{5,7\} \ , \ \{11,13\} \ , \ \{17,19\}.$$

Δεν είναι γνωστό αν υπάρχουν άπειρα τέτοια ζεύγη, αλλά αν ελέγξουμε τη λίστα με τους πρώτους θα οδηγηθούμε στην εξής εικασία:

***Εικασία***
Υπάρχουν άπειρα ζεύγη δίδυμων πρώτων.

Πολλοί μαθηματικοί έχουν ασχοληθεί με την παραπάνω εικασία. Το 1919 ο Brun απέδειξε το εξής:

***Θεώρημα Brun***
Έστω $S$ το σύνολο των δίδυμων πρώτων. Τότε το άθροισμα

$$\sum_{p\in S}\Big(\frac{1}{p}+\frac{1}{p+2}\Big)$$

συγκλίνει.

**Παρατηρήσεις**
•Αν το σύνολο $S$ είναι πεπερασμένο, τότε το άθροισμα σίγουρα συγκλίνει. Το θεώρημα του Brun εκφράζει τη σπανιότητα των δίδυμων πρώτων, ακόμα και αν είναι άπειροι.
•Το άθροισμα

$$B=\Big(\frac{1}{3}+\frac{1}{5}\Big)+\Big(\frac{1}{5}+\frac{1}{7}\Big)+\Big(\frac{1}{11}+\frac{1}{13}\Big)+\ldots+\Big(\frac{1}{p}+\frac{1}{p+2}\Big)+\ldots$$

καλείται σταθερά του Brun. Η σταθερά του Brun έχει υπολογιστεί από διάφορους μαθηματικούς(Shanks και Wrench(1974), Brent(1976), Nicely(1995)) και ισχύει ότι:

$$B=1.902160577783278\ldots.$$

•Υπάρχει μεγάλος ανταγωνισμός για την εύρεση του μεγαλύτερου γνωστού ζεύγους δίδυμων πρώτων. Το 2000 οι Wassing, Jarai, Indlekofer ανακάλυψαν το μεγαλύτερο ζεύγος $\{p,p+2\}$, με

$$p=2409110779845\cdot 2^{60000}-1.$$

•Άλλη μια εικασία υποστηρίζει ότι υπάρχουν άπειρες τριάδες πρώτων της μορφής

$$p \ , \ p+2 \ , \ p+6.$$

***Θεώρημα***
Υπάρχει μια $1-1$ αντιστοιχία μεταξύ δίδυμων πρώτων και των φυσικών $n$ για τους οποίους ο $n^2-1$ έχει ακριβώς τέσσερις διαιρέτες.

***Απόδειξη***
Έστω οι δίδυμοι πρώτοι $p = x-1$ και $q = p+2 = x+1$.
Τότε

$$x^2 - 1 = p \cdot q$$

και προφανώς οι $1, p, q, p \cdot q$ είναι οι μόνοι διαιρέτες του $p \cdot q = x^2 - 1$.
Αντίστροφα, ο αριθμός $x^2 - 1$ έχει από υπόθεση ακριβώς τέσσερις διαιρέτες και οι

$$1, x-1, x+1, x^2-1$$

είναι διαιρέτες του και όλοι διαφορετικοί. Άρα είναι οι μόνοι διαιρέτες του $x^2-1$. Ακόμα, ο $x-1$ δεν μπορεί να έχει κανένα διαρέτη εκτός από τον εαυτό του και τη μονάδα, γιατί αν είχε θα ήταν και διαιρέτης του $x^2-1$. Άρα ο $x-1$ είναι πρώτος. Επίσης, ο $x+1$ είναι πρώτος γιατί οι μόνοι του διαιρέτες είναι οι $1, x+1$. Θα μπορούσε να είναι και ο $x-1$ διαιρέτης του αλλά αν

$$(x-1)\Big|(x+1) \Longrightarrow x = 3.$$

Οπότε οι $x-1, x+1$ είναι δίδυμοι πρώτοι. ■

***Θεώρημα***
Το $5$ είναι ο μόνος πρώτος που εμφανίζεται σε δύο ζεύγη δίδυμων πρώτων.

***Απόδειξη***
Έστω ότι υπάρχει πρώτος $p \neq 5$, ο οποίος εμφανίζεται σε δύο ζεύγη δίδυμων πρώτων. Τότε

$$p-2 \ , \ p \ , \ p+2$$

είναι όλοι πρώτοι. Προφανώς είναι και οι τρεις περιττοί. Εξετάζουμε τις περιπτώσεις:
i)αν $p \equiv 0 \bmod 3$, τότε $p = 3k$, άρα δεν είναι πρώτος.

ii)αν $p \equiv 1 \bmod 3$, τότε $p+2 \equiv 0 \bmod 3$, δηλαδή $p+2 = 3k$, άρα ο $p+2$ δεν είναι πρώτος.
iii)αν $p \equiv 2 \bmod 3$, τότε $p-2 \equiv p+1 \equiv 0 \bmod 3$, δηλαδή $p-2 = 3k$ το οποίο είναι άτοπο αφού θα είναι $p = 5$.
Οπότε το $5$ είναι ο μόνος πρώτος που εμφανίζεται σε δύο ζεύγη δίδυμων πρώτων $\{3,5\}, \{5,7\}$. ■

Τέλος, ο Leopold Kronecker διατύπωσε αλλά δεν απέδειξε ότι κάθε άρτιος αριθμός μπορεί να γραφεί με άπειρους τρόπους ως η διαφορά δύο πρώτων, το οποίο δείχνει την ύπαρξη άπειρων δίδυμων πρώτων.
Ακολουθεί άλλη μια εικασία, ίσως η διασημότερη όλων των εποχών.

## 2.5 Η ΕΙΚΑΣΙΑ ΤΟΥ GOLDBACH

Σε ένα γράμμα του προς τον Euler το 1742 ο Christian Goldbach διατύπωσε ότι κάθε άρτιος αριθμός μεγαλύτερος του 2 είναι το άθροισμα δύο πρώτων. Αυτός ο ισχυρισμός είναι γνωστός ως η "εικασία του Goldbach" και έχει μελετηθεί εκτενώς τους περασμένους τρεις αιώνες. Ο διάσημος άγγλος μαθηματικός G.H. Hardy περιέγραψε την εικασία του Goldbach ως ένα από τα δυσκολότερα ανοιχτά προβλήματα των μαθηματικών.

***Εικασία του Goldbach***
Κάθε άρτιος αριθμός μεγαλύτερος του 2 είναι το άθροισμα δύο πρώτων.

Ο Goldbach επίσης είκασε ότι κάθε περιττός αριθμός μεγαλύτερος του 7 ισούται με το άθροισμα τριών περιττών πρώτων. Παρότι ο ισχυρισμός αυτός παραμένει ανοιχτό πρόβλημα, ο Vinogradov απέδειξε το 1937 ότι όλοι οι αρκετά μεγάλοι περιττοί αριθμοί γράφονται σαν άθροισμα τριών περιττών πρώτων.
Ακολουθούν δύο προτάσεις σχετικές με την εικασία του Goldbach:

***Πρόταση***
Η εικασία του Goldbach συνεπάγεται ότι κάθε περιττός μεγαλύτερος του 7 γράφεται ως άθροισμα τριών περιττών πρώτων.

***Απόδειξη***
Έστω $n$ ένας περιττός αριθμός μεγαλύτερος του 7. Τότε ο $n-3$ είναι άρτιος και μεγαλύτερος του 4. Τότε από την εικασία του Goldbach ο $n-3$ γράφεται ως άθροισμα δύο πρώτων $p$ και $q$. Επιπλέον οι $p$, $q$ είναι περιττοί, αφού μόνο το 4 είναι το άθροισμα δύο άρτιων πρώτων. Οπότε

$$n = 3 + p + q$$

δηλαδή ο $n$ γράφεται ως άθροισμα τριών περιττών πρώτων. ■

***Πρόταση***
Η εικασία του Goldbach είναι ισοδύναμη με το ακόλουθο:
"Κάθε φυσικός $n > 5$ είναι το άθροισμα τριών πρώτων."

***Απόδειξη***
Ας υποθέσουμε ότι η εικασία του Goldbach αληθεύει.
•Αν ο $n > 5$ είναι άρτιος τότε ο $n - 2 \geq 4$ είναι άρτιος. Οπότε ο $n-2$ είναι το

άθροισμα $p+q$ δύο πρώτων. Επομένως ο

$$n = 2 + p + q$$

είναι το άθροισμα τριών πρώτων.
•Αν ο $n > 5$ είναι περιττός τότε ο $n - 3 \geq 4$ είναι άρτιος. Οπότε ο $n - 3$ γράφεται ως $p + q$ με $p, q$ πρώτους. Άρα ο

$$n = 3 + p + q$$

είναι το άθροισμα τριών πρώτων.
Αντίστροφα, υποθέτουμε ότι κάθε φυσικός $n \geq 5$ είναι το άθροισμα τριών πρώτων.
Έστω $n \geq 4$ άρτιος. Τότε ο $n + 2$ είναι το άθροισμα τριών πρώτων. Όμως αφού ο $n + 2$ είναι άρτιος, τουλάχιστον ένας από τους τρεις πρώτους θα είναι το 2. Έτσι

$$n + 2 = p + q + 2$$

για κάποια $p, q$. Επομένως:

$$n = p + q$$

δηλαδή ο $n$ γράφεται ως άθροισμα δύο πρώτων. ■

# Chapter 3

# Η ΚΑΤΑΝΟΜΗ ΤΩΝ ΠΡΩΤΩΝ

## 3.1 ΕΙΣΑΓΩΓΗ

Όπως είδαμε στο πρώτο κεφάλαιο η συνάρτηση $\pi(x)$ μετρά το πλήθος των πρώτων μέχρι τον αριθμό $x$. Επίσης, αφού οι πρώτοι είναι άπειροι ισχύει ότι

$$\pi(x) \to \infty$$

καθώς $x \to \infty$.
Πώς κατανέμονται όμως στον άξονα των πραγματικών αριθμών; Ποια είναι η συμπεριφορά της $\pi(x)$ ως συνάρτηση του $x$; Αυτές οι ερωτήσεις αποτέλεσαν έναυσμα για βαθειά μελέτη για πολλούς μαθηματικούς. Το 1792 και το 1798 ο Gauss και ο Legendre διατύπωσαν την εικασία ότι η $\pi(x)$ είναι ασυμπτωτικά ίση με την $\frac{x}{\ln x}$, δηλαδή

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

Ο Gauss κοιτώντας τη λίστα των πρώτων μέχρι το 3,000,000 παρατήρησε ότι η συνάρτηση των πρώτων αριθμών συνδέεται στενά με τη συνάρτηση $Li(x)$, η οποία δίνεται από τον τύπο:

$$Li(x) = \int_2^x \frac{1}{\ln t}\, dt.$$

Ακόμα απέδειξε ότι

$$\pi(x) \sim Li(x).$$

Αν στο παραπάνω ολοκλήρωμα εφαρμόσουμε παραγοντική ολοκλήρωση παρατηρούμε ότι καθώς $x \to \infty$ η $Li(x)$ είναι ασυμπτωτικά ίση με την $\frac{x}{\ln x}$.

Σύμφωνα με τα παραπάνω ο Gauss διατύπωσε το εξής:

***Θεώρημα Πρώτων Αριθμών (Prime Number Theorem)***
Αν $\pi(x)$ είναι η συνάρτηση των πρώτων αριθμών, τότε

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

Ο Legendre κοιτώντας και αυτός τη λίστα των πρώτων είκασε ότι

$$\pi(x) \sim \frac{x}{\ln x - 1.08366}.$$

Χρειάστηκε να περάσουν περίπου 100 χρόνια για να γίνει η εικασία του Gauss θεώρημα. Το 1896 ο Hadamard και ο de la Vallée Poussin, ανεξάρτητα, απέδειξαν αυτό που είναι πλέον γνωστό ως Θεώρημα των Πρώτων Αριθμών. Οι πρώτες αυτές αποδείξεις ήταν αναλυτικές μιας και χρησιμοποιούσαν μιγαδική ανάλυση. Αργότερα, το 1949, ο Erdős και ο Selberg απέδειξαν το Θεώρημα των Πρώτων Αριθμών χρησιμοποιώντας στοιχειώδεις μεθόδους. Στο τέλος του κεφαλαίου θα παρουσιάσουμε μια σκιαγράφηση αυτής της απόδειξης.

Η πρώτη σοβαρή απόπειρα για την απόδειξη του σπουδαίου θεωρήματος είχε γίνει από τον Chebyshev το 1848. Παρότι δεν τα κατάφερε έδωσε δύο σημαντικά εργαλεία. Απέδειξε ότι υπάρχουν σταθερές $A_1, A_2$ με $0.922 < A_1 < 1$ και $1 < A_2 < 1.105$ τέτοιες ώστε:

$$A_1 < \frac{\pi(x)\ln x}{x} < A_2.$$

Ακόμα απέδειξε ότι αν το $\frac{\pi(x)\ln x}{x}$ έχει όριο αυτό θα πρέπει να είναι το $1$.
Το 1882 ο Sylvester βελτίωσε τις σταθερές του Chebyshev σε $A_1 = 0.95695$ και $A_2 = 1.04423$.

Ο Riemann ήταν άλλος ένας διάσημος μαθηματικός που προσπάθησε να δώσει απόδειξη του θεωρήματος. Στήριξε τις μελέτες του στη συνάρτηση ζήτα (zeta function) που εισήγαγε. Αν και δεν ολοκλήρωσε την απόδειξη, οι ιδιότητες της συνάρτησης ζήτα που διατύπωσε ήταν το εφαλτήριο για να τα καταφέρουν οι Hadamard και de la Vallée Poussin.

Ένα άλλο σημαντικό ερώτημα σχετικό με την κατανομή των πρώτων είναι το

ποιος είναι ο νιοστός πρώτος $p_n$. Την απάντηση δίνει το ακόλουθο θεώρημα.

***Θεώρημα***
Ο νιοστός πρώτος $p_n$ δίνεται ασυμπτωτικά από τη σχέση

$$p_n \sim n \ln n.$$

***Απόδειξη***
Από το Θεώρημα των Πρώτων Αριθμών έχουμε ότι

$$\pi(x) \sim \frac{x}{\ln x}.$$

Έστω $y = \frac{x}{\ln x}$. Τότε

$$\ln y = \ln x - \ln(\ln x).$$

Ασυμπτωτικά όμως το $\ln(\ln x)$ είναι μικρό σε σχέση με το $\ln x$, οπότε

$$\ln y \sim \ln x.$$

Από την αρχική σχέση

$$x = y \ln x \sim y \ln y.$$

Άρα η αντίστροφη συνάρτηση της $\frac{x}{\ln x}$ ασυμπτωτικά είναι η $x \ln x$. Επομένως από το Θεώρημα των Πρώτων Αριθμών η αντίστροφη της $\pi(x)$ θα είναι ασυμπτωτικά η $x \ln x$. Όμως

$$\pi(p_n) = n \Longrightarrow \pi^{-1}(n) = p_n.$$

Άρα

$$p_n \sim n \ln n. \qquad \blacksquare$$

Τέλος, παραθέτουμε ένα πίνακα που περιέχει τις $\pi(x), Li(x), \frac{x}{\ln x}$:

| $x$ | $\pi(x)$ | $\pi(x)/(x/\ln x)$ | $Li(x)-\pi(x)$ | $x/\pi(x)$ |
|---|---|---|---|---|
| 10 | 4 | 0.921 | 2.2 | 2.500 |
| $10^2$ | 25 | 1.151 | 5.1 | 4.000 |
| $10^3$ | 168 | 1.161 | 10 | 5.952 |
| $10^4$ | 1,229 | 1.132 | 17 | 8.137 |
| $10^5$ | 9,592 | 1.104 | 38 | 10.425 |
| $10^6$ | 78,498 | 1.084 | 130 | 12.740 |
| $10^7$ | 664,579 | 1.071 | 339 | 15.047 |
| $10^8$ | 5,761,455 | 1.061 | 754 | 17.357 |
| $10^9$ | 50,847,534 | 1.054 | 1,701 | 19.667 |
| $10^{10}$ | 455,052,511 | 1.048 | 3,104 | 21.975 |
| $10^{11}$ | 4,118,054,813 | 1.043 | 11,588 | 24.283 |
| $10^{12}$ | 37,607,912,018 | 1.039 | 38,263 | 26.590 |
| $10^{13}$ | 346,065,536,839 | 1.034 | 108,971 | 28.896 |
| $10^{14}$ | 3,204,941,750,802 | 1.033 | 314,890 | 31.202 |
| $10^{15}$ | 29,844,570,422,669 | 1.031 | 1,052,619 | 33.507 |
| $10^{16}$ | 279,238,341,033,925 | 1.029 | 3,214,632 | 35.812 |
| $10^{17}$ | 2,623,557,157,654,233 | 1.027 | 7,956,589 | 38.116 |
| $10^{18}$ | 24,739,954,287,740,860 | 1.025 | 21,949,555 | 40.420 |
| $10^{19}$ | 234,057,667,276,344,607 | 1.024 | 99,877,775 | 42.725 |
| $10^{20}$ | 2,220,819,602,560,918,840 | 1.023 | 222,744,644 | 45.028 |
| $10^{21}$ | 21,127,269,486,018,731,928 | 1.022 | 597,394,254 | 47.332 |
| $10^{22}$ | 201,467,286,689,315,906,290 | 1.021 | 1,932,355,208 | 49.636 |
| $10^{23}$ | 1,925,320,391,606,803,968,923 | 1.020 | 7,250,186,216 | 51.939 |

**Παρατήρηση**

Όπως βλέπουμε από την προτελευταία στήλη η $Li(x)$ παρουσιάζεται σαν "υπερεκτίμηση" της $\pi(x)$. Όμως το 1914 ο Littlewood απέδειξε ότι η διαφορά $Li(x)-\pi(x)$ αλλάζει πρόσημο άπειρες φορές.

## 3.2 Η ΠΡΟΣΕΓΓΙΣΗ ΤΟΥ CHEBYSHEV

Όπως αναφέραμε προηγουμένως ο Chebyshev έκανε μεγάλες προσπάθειες για την απόδειξη του Θεωρήματος των Πρώτων Αριθμών. Αν και δεν ολοκλήρωσε την απόδειξη, έδωσε μια καλή προσέγγιση για τη συνάρτηση των πρώτων αριθμών.

***Θεώρημα(Chebyshev)***
Υπάρχουν θετικές σταθερές $A_1, A_2$ τέτοιες ώστε

$$A_1 \frac{x}{\ln x} < \pi(x) < A_2 \frac{x}{\ln x}.$$

**Σημείωση**
Η απόδειξη του θεωρήματος του Chebyshev θα βασιστεί σε κάποια λήμματα που αναφέρονται παρακάτω. Τα λήμματα θα διατυπωθούν χωρίς απόδειξη μιας και οι αποδείξεις αυτές είναι πέρα από το σκοπό αυτής της εργασίας.

Ξεκινώντας, θα μελετήσουμε το μέγεθος των $n!$ και $\binom{2n}{n}$.

***Λήμμα(Τύπος του Stirling)***
Για $n \in \mathbb{N}$ ισχύει η παρακάτω προσέγγιση

$$n! \sim n^n e^{-n} \sqrt{2\pi n}.$$

Όμως μπορούμε να έχουμε μια απλούστερη προσέγγιση. Αφού το $\frac{n^n}{n!}$ είναι όρος του αναπτύγματος του $e^n$, θα είναι $e^n > \frac{n^n}{n!}$ και έχουμε:

***Λήμμα 1***
Για $n \in \mathbb{N}$ έχουμε

$$n^n e^{-n} < n! < n^n.$$

***Λήμμα 2***
Για $n \in \mathbb{N}$ έχουμε

$$\frac{4^n}{2n} < \binom{2n}{n} < 4^n.$$

Για την απόδειξη του παραπάνω για την αριστερή ανισότητα εργαζόμαστε επαγωγικά. Για τη δεξιά παρατηρούμε ότι

$$(1+1)^{2n} = 1 + \binom{2n}{1} + \ldots + \binom{2n}{n} + \ldots + 1.$$

Επίσης ο $\binom{2n+1}{n}$ είναι ένας από τους δύο ίσους όρους του αναπτύγματος $(1+1)^{2n+1}$. Οπότε έχουμε

***Λήμμα 3***
Για $n \in \mathbb{N}$ έχουμε

$$\binom{2n+1}{n} < 4^n.$$

Τώρα θα δούμε πως τα $n!$ και $\binom{2n}{n}$ παραγοντοποιούνται ως γινόμενα πρώτων. Υποθέτουμε ότι $e_p(n)$ είναι οι εκθέτες των πρώτων παραγόντων του $n!$. Δηλαδή

$$n! = \prod_p p^{e_p(n)}.$$

Όπως ήδη αναφέραμε στο Αίτημα του Bertrand:

***Λήμμα(Legendre)***
Για τα $e_p(n)$ που ορίσαμε και για $n \in \mathbb{N}$ έχουμε

$$e_p(n) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$$

Η απόδειξη του προηγούμενου λήμματος αναφέρεται στο δεύτερο κεφάλαιο.

Για την αναπαράσταση του $\binom{2n}{n}$ ως γινόμενου πρώτων θέτουμε $E_p(n)$ τους εκθέτες του $p$ στο $\binom{2n}{n}$. Δηλαδή

$$\binom{2n}{n} = \prod_p p^{E_p(n)}.$$

Έχουμε ότι:

$$E_p(n) = e_p(2n) - 2e_p(n) = \sum_i \left( \left\lfloor \frac{2n}{p_i} \right\rfloor - \left\lfloor 2\frac{n}{p^i} \right\rfloor \right).$$

Από την παραπάνω σχέση παρατηρούμε ότι κάθε όρος του αθροίσματος θα είναι 0 ή 1 και το πλήθος των όρων δεν ξεπερνά τον εκθέτη της μεγαλύτερης δύναμης του $p$, η οποία δεν ξεπερνά το $2n$. Έτσι ισχύουν τα εξής:

***Λήμμα 4***
Για $n \in \mathbb{N}$ έχουμε

$$E_p(n) \leq \log_p(2n).$$

***Λήμμα 5***
Η συνεισφορά του $p$ στο $\binom{2n}{n}$ δεν ξεπερνά το $2n$.

***Λήμμα 6***
Κάθε πρώτος $p$ με $n < p < 2n$ εμφανίζεται ακριβώς μια φορά στο $\binom{2n}{n}$.

***Λήμμα 7***
Κανένας πρώτος $p$ με $\frac{2n}{3} < p < n$ δεν είναι διαιρέτης του $\binom{2n}{n}$.

***Λήμμα 8***
Κανένας πρώτος $p > \sqrt{2n}$ δεν εμφανίζεται περισσότερες από μια φορές στο $\binom{2n}{n}$.

Από τα παραπάνω προκύπτει το εξής σημαντικό θεώρημα

***Θεώρημα***
Για $n \in \mathbb{N}$ και $p$ πρώτο έχουμε

$$\prod_{p \leq n} p < 4^n.$$

***Απόδειξη***
Με επαγωγή στο $n$. Υποθέτουμε ότι η σχέση ισχύει για φυσικούς μικρότερους του $n$ και εξετάζουμε τις περιπτώσεις $n = 2m$ και $n = 2m + 1$.

Αν $n = 2m$ τότε

$$\prod_{p\leq 2m} p = \prod_{p\leq 2m-1} p < 4^{2m-1}$$

από επαγωγική υπόθεση.
Αν $n = 2m+1$ τότε

$$\prod_{p\leq 2m+1} p = \Big(\prod_{p\leq m+1} p\Big)\Big(\prod_{m+1<p<2m+1} p\Big) < 4^{m+1}\binom{2m+1}{m} \leq 4^{m+1}4^m = 4^{2m+1}$$

οπότε

$$\prod_{p\leq n} p < 4^n. \qquad \blacksquare$$

Ως συνέπεια του προηγούμενου θεωρήματος έχουμε το ακόλουθο.

***Θεώρημα***
Για $n \in \mathbb{N}$ και $A_2$ θετική σταθερά έχουμε

$$\pi(n) < A_2\frac{n}{\ln n}.$$

***Απόδειξη***
Είναι

$$4^n > \prod_{p\leq n} p > \prod_{\sqrt{n}\leq p\leq n} p < \sqrt{n}^{\pi(n)-\pi(\sqrt{n})}.$$

Παίρνοντας λογαρίθμους έχουμε:

$$n\ln 4 > \Big(\pi(n) - \pi(\sqrt{n})\Big)\frac{\ln n}{2} \Longrightarrow \pi(n) - \pi(\sqrt{n}) < \frac{n2\ln 4}{\ln n} \Longrightarrow$$

$$\pi(n) < (2\ln 4)\frac{n}{\ln n} + \sqrt{n} < A_2\frac{n}{\ln n}. \qquad \blacksquare$$

***Θεώρημα***
Για $n \in \mathbb{N}$ και $A_1$ θετική σταθερά έχουμε

$$\pi(n) > A_1\frac{n}{\ln n}.$$

***Απόδειξη***
Από προηγούμενα λήμματα έχουμε:

$$(2n)^{\pi(2n)} > \binom{2n}{n} > \frac{4^n}{2n}.$$

Παίρνοντας λογαρίθμους έχουμε τη σχέση:

$$\Big(\pi(n)+1\Big)\ln(2n) > \ln(2^{2n}) = 2n\ln 2.$$

Επομένως για άρτιο $m$:

$$\pi(m)+1 > \frac{m}{\ln m}\ln 2 \Longrightarrow \pi(m) > A_1\frac{m}{\ln m}. \qquad \blacksquare$$

Ως συμπέρασμα της προσέγγισης του Chebyshev ακολουθεί η επόμενη πρόταση

***Πρόταση***

$$\frac{\pi(x)}{x} \to 0$$

καθώς $x \to 0$.

***Απόδειξη***
Από το προηγούμενο θεώρημα έχουμε

$$0 < \pi(x) \le A_2\frac{x}{\ln x} \Longrightarrow 0 < \frac{\pi(x)}{x} \le A_2\frac{1}{\ln x}.$$

Όμως $\frac{A_2}{\ln x} \to 0$ καθώς $x \to \infty$, επομένως

$$\frac{\pi(x)}{x} \to 0$$

καθώς $x \to 0$. $\blacksquare$

**Παρατήρηση**
Από τη σκοπιά των Πιθανοτήτων βλέπουμε ότι η πιθανότητα να επιλέξουμε ένα πρώτο μικρότερο ή ίσο από τον $x$ δίνεται από τον τύπο $\frac{\pi(x)}{x}$. Για μεγάλα $x$ αυτό το πηλίκο είναι προσεγγιστικά ίσο με $\frac{1}{\ln x}$. Για παράδειγμα για τον

αριθμό $e^{1000}$ η πιθανότητα να επιλέξουμε τυχαία ένα πρώτο μικρότερο ή ίσο από αυτόν είναι $0.001$. Αυτό μας δείχνει ότι οι πρώτοι, αν και σπάνιοι, είναι σχετικά "πυκνοί" στους ακεραίους.

Άλλο ένα συμπέρασμα της προσέγγισης του Chebyshev είναι το ακόλουθο θεώρημα

***Θεώρημα***
Υπάρχουν θετικές σταθερές $B_1, B_2$ τέτοιες ώστε

$$B_1 n \ln n \leq p_n \leq B_2 n \ln n$$

όπου $p_n$ ο νιοστός πρώτος.

***Απόδειξη***
Προφανώς $\pi(p_n) = n$ και από το θεώρημα του Chebyshev είναι

$$\pi(p_n) \leq A_2 \frac{p_n}{\ln p_n}$$

για $n \geq 2$. Δηλαδή

$$\frac{1}{A_2} n \ln p_n \leq p_n$$

και επειδή $p_n > n$ τότε

$$\frac{1}{A_2} n \ln n < \frac{1}{A_2} n \ln p_n \leq p_n$$

για $n \geq 2$. Επομένως

$$B_1 n \ln n \leq p_n$$

για $n \geq 2$ και $B_1 = \frac{1}{A_2}$.
Αντίστοιχα, έχουμε

$$n = \pi(p_n) \geq A_1 \frac{p_n}{\ln p_n}.$$

Παρατηρούμε ότι $\frac{\ln p_n}{\sqrt{p_n}} \to 0$ καθώς $n \to \infty$. Έτσι υπάρχει $k \in \mathbb{N}$ τέτοιο ώστε

$$\frac{\ln p_n}{\sqrt{p_n}} < A_1$$

για $n > k$. Άρα

$$n \frac{\ln p_n}{p_n} \geq A_1 > \frac{\ln p_n}{\sqrt{p_n}} \ , \ n > k.$$

Οπότε $n > \sqrt{p_n}$ δηλαδή $p_n < 2\ln n$ για $n > k$. Ορίζουμε

$$B_2 = \max\left\{\frac{2}{A_1}, \frac{p_2}{2\ln 2}, \frac{p_3}{3\ln 3}, \ldots, \frac{p_{k-1}}{(k-1)\ln(k-1)}\right\}.$$

Τότε

$$p_n \leq B_2 n \ln n$$

για $n \geq 2$. ■

***Πρόταση***
Η σειρά

$$\sum_p \frac{1}{p}$$

αποκλίνει.

***Απόδειξη***
Για $n \geq 2$ έχουμε

$$p_n \geq B_1 n \ln n \Longrightarrow \frac{1}{p_n} \leq \frac{1}{B_1 n \ln n}$$

από το προηγούμενο θεώρημα. Όμως, είναι γνωστό ότι η σειρά

$$\sum_{n=1}^{\infty} \frac{1}{n \ln n}$$

αποκλίνει. Άρα θα αποκλίνει και η

$$\sum_p \frac{1}{p}.$$ ■

Αν και οι πρώτοι είναι άπειροι το πλήθος και η σειρά $\sum_p \frac{1}{p}$ αποκλίνει, το κάνει πολύ αργά. Στην επόμενη πρόταση θα δούμε ότι μπορούμε να φράξουμε τη σειρά των αντιστρόφων των πρώτων.

***Πρόταση***
Υπάρχει σταθερά $k$ τέτοια ώστε

$$\sum_{2<p\leq x} \frac{1}{p} < k \ln(lnx) \ , \ x > 3.$$

***Απόδειξη***
Από το προηγούμενο θεώρημα έχουμε

$$p_n \geq B_1 n \ln n.$$

Οπότε

$$\sum_{2<p\leq x} \frac{1}{p} = \sum_{n=2}^{\pi(x)} \frac{1}{p_n} < \sum_{n=2}^{\lfloor x \rfloor} \frac{1}{B_1 n \ln n} < \frac{1}{B_1} \sum_{n=2}^{\lfloor x \rfloor} \frac{1}{n \ln n}.$$

Παρατηρούμε ότι

$$\frac{1}{n \ln n} = \int_{n-1}^{n} \frac{dt}{n \ln n} \leq \int_{n-1}^{n} \frac{dt}{t \ln t}$$

για $t \in \mathbb{R}$. Επομένως

$$\sum_{2<p\leq x} \frac{1}{p} < \frac{1}{B_1} \sum_{n=2}^{\lfloor x \rfloor} \frac{1}{n \ln n} \leq \frac{1}{2B_1 \ln 2} + \frac{1}{B_1} \sum_{n=3}^{\lfloor x \rfloor} \int_{n-1}^{n} \frac{dt}{t \ln t} \leq$$

$$\frac{1}{2B_1 \ln 2} + \frac{1}{B_1} \int_{2}^{x} \frac{dt}{t \ln t} = \frac{1}{2B_1 \ln 2} + \frac{1}{B_1} \ln(\ln x) - \frac{1}{B_1} \ln(\ln 2) =$$

$$\frac{1}{B_1} \ln(\ln x) + C < k \ln(\ln x)$$

για $k$ αρκετά μεγάλο. ■

## 3.3 ΟΙ ΣΥΝΑΡΤΗΣΕΙΣ $\psi(x)$ ΚΑΙ $\theta(x)$ ΤΟΥ CHEBYSHEV

Σε αυτή την παράγραφο θα ορίσουμε τις συναρτήσεις $\psi(x)$ και $\theta(x)$ του Chebyshev. Ακόμα θα δούμε κάποιες ισοδύναμες μορφές του Θεωρήματος των Πρώτων Αριθμών που προκύπτουν μέσω αυτών των συναρτήσεων.

***Ορισμός***
Για $x > 0$ ορίζουμε τη συνάρτηση $\psi\colon \mathbb{R} \to \mathbb{R}$ του Chebyshev με τον τύπο

$$\psi(x) = \sum_{n \leq x} \Lambda(n).$$

Εξ ορισμού $\Lambda(n) = 0$ εκτός αν ο $n$ είναι δύναμη πρώτου. Έτσι μπορούμε να γράψουμε τη συνάρτηση $\psi$ ως εξής

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{m \in \mathbb{N}} \sum_{p^m \leq x} \Lambda(p^m) = \sum_{m \in \mathbb{N}} \sum_{p \leq x^{1/m}} \ln p.$$

Τώρα αν $x^{1/m} < 2$ τότε το άθροισμα πάνω στα $p$ δεν έχει νόημα. Δηλαδή

$$x^{1/m} < 2 \Longrightarrow \frac{1}{m} \ln x < \ln 2 \Longrightarrow m > \frac{\ln x}{\ln 2} = \log_2 x.$$

Επομένως

$$\psi(x) = \sum_{m \leq log_2 x} \sum_{p \leq x^{1/m}} \ln p.$$

***Ορισμός***
Για $x > 0$ ορίζουμε τη συνάρτηση $\theta\colon \mathbb{R} \to \mathbb{R}$ του Chebyshev με τον τύπο

$$\theta(x) = \sum_{p \leq x} \ln p$$

όπου $p$ πρώτος.

Τότε η $\psi(x)$ μπορεί να γραφεί ως

$$\psi(x) = \sum_{m \leq \log_2 x} \theta(x^{1/m}).$$

Ακολουθεί ένα θεώρημα που συσχετίζει τις $\psi$, $\theta$:

***Θεώρημα***
Για $x > 0$ ισχύει ότι

$$0 \leq \frac{\psi(x)}{x} - \frac{\theta(x)}{x} \leq \frac{(\ln x)^2}{2\sqrt{x}\ln 2}.$$

***Απόδειξη***
Αφού $\psi(x) = \sum_{m \leq \log_2 x} \theta(x^{1/m})$ έχουμε

$$0 \leq \psi(x) - \theta(x) = \sum_{2 \leq m \leq \log_2 x} \theta(x^{1/m}).$$

Επίσης από τον ορισμό της $\theta(x)$ έχουμε

$$\theta(x) = \sum_{p \leq x} \ln p \leq \sum_{p \leq x} \ln x \leq x \ln x.$$

Επομένως

$$0 \leq \psi(x) - \theta(x) \leq \sum_{2 \leq m \leq \log_2 x} x^{1/m} \ln(x^{1/m}) \leq \log_2 x \cdot \sqrt{x} \cdot \ln \sqrt{x} =$$

$$\frac{\ln x}{\ln 2} \cdot \frac{\sqrt{x}}{2} \cdot \ln x = \frac{\sqrt{x}(\ln x)^2}{2 \ln 2}$$

Άρα

$$0 \leq \frac{\psi(x)}{x} - \frac{\theta(x)}{x} \leq \frac{(\ln x)^2}{2\sqrt{x}\ln 2}.$$ ■

**Σημείωση**
Από την παραπάνω ανισότητα έχουμε ότι

$$\lim_{x \to \infty} \left( \frac{\psi(x)}{x} - \frac{\theta(x)}{x} \right) = 0$$

δηλαδή αν μια εκ των $\frac{\psi(x)}{x}$ ή $\frac{\theta(x)}{x}$ έχει όριο τότε θα έχει και η άλλη το ίδιο.

## 3.4 ΙΣΟΔΥΝΑΜΕΣ ΜΟΡΦΕΣ ΤΟΥ ΘΕΩΡΗΜΑΤΟΣ ΤΩΝ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ

Ξεκινώντας θα αναφέρουμε ένα πολύ σημαντικό θεώρημα που αφορά τις αριθμητικές συναρτήσεις, την ταυτότητα του Abel.

***Θεώρημα***
Για κάθε αριθμητική συνάρτηση $a(n)$ θεωρούμε

$$A(x) = \sum_{n \leq x} a(x)$$

με $A(x) = 0$ για $x < 1$. Υποθέτουμε ότι η συνάρτηση $f(x)$ έχει συνεχή παράγωγο στο διάστημα $[y, x]$. Τότε ισχύει

$$\sum_{y<n\leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

***Απόδειξη***
Θέτουμε $k = \lfloor x \rfloor$ και $m = \lfloor y \rfloor$. Τότε θα είναι $A(x) = A(k)$ και $A(y) = A(m)$. Έχουμε

$$\sum_{y<n\leq x} a(n)f(n) = \sum_{n=m+1}^{k} a(n)f(n) = \sum_{n=m+1}^{k} \Big[A(n) - A(n-1)\Big]f(n) =$$

$$\sum_{n=m+1}^{k} A(n)f(n) - \sum_{n=m}^{k-1} A(n)f(n+1) =$$

$$\sum_{n=m+1}^{k-1} \Big\{A(n)\Big[f(n) - f(n+1)\Big]\Big\} + A(k)f(k) - A(m)f(m+1) =$$

$$- \sum_{n=m+1}^{k-1} \Big\{A(n)\int_n^{n+1} f'(t)dt\Big\} + A(k)f(k) - A(m)f(m+1) =$$

$$- \sum_{n=m+1}^{k-1} \int_n^{n+1} A(t)f'(t)dt + A(k)f(k) - A(m)f(m+1) =$$

$$-\int_{m+1}^{k} A(t)f'(t)dt + A(x)f(x) - \int_{k}^{x} A(t)f'(t)dt - \int_{y}^{m+1} A(t)f'(t)dt =$$

$$A(x)f(x) - A(y)f(y) - \int_{y}^{x} A(t)f'(t)dt. \qquad \blacksquare$$

**Παρατήρηση**
Αφού $A(t) = 0$ για $t < 1$ η ταυτότητα του Abel για $y < 1$ θα έχει τη μορφή

$$\sum_{n \le x} a(n)f(n) = A(x)f(x) - \int_{1}^{x} A(t)f'(t)dt.$$

Η παραπάνω ταυτότητα αναφέρθηκε με σκοπό να μπορέσουμε να βρούμε μια σχέση μεταξύ της $\theta(x)$ και $\pi(x)$. Έτσι ακολουθεί το εξής θεώρημα:

***Θεώρημα***
Για $x \ge 2$ έχουμε

$$\theta(x) = \pi(x)\ln x - \int_{2}^{x} \frac{\pi(t)}{t}dt \qquad (1)$$

και

$$\pi(x) = \frac{\theta(x)}{\ln x} + \int_{2}^{x} \frac{\theta(t)}{t(\ln t)^2} \qquad (2)$$

***Απόδειξη***
Θέτουμε $a(n)$ την ακόλουθη συνάρτηση

$$a(n) = \begin{cases} 1 & \text{, αν ο } n \text{ είναι πρώτος} \\ 0 & \text{, αν ο } n \text{ είναι σύνθετος} \end{cases}$$

Από τους ορισμούς των $\pi(x), \theta(x)$ έχουμε

$$\pi(x) = \sum_{p \le x} 1 = \sum_{1 < a \le x} a(n)$$

και

$$\theta(x) = \sum_{p \leq x} \ln p = \sum_{1 < n \leq x} a(n) \ln n.$$

Επιλέγουμε $f(x) = \ln x$, η οποία έχει συνεχή παράγωγο στο διάστημα $[1, x]$. Από ταυτότητα του Abel έχουμε:

$$\theta(x) = \sum_{1 < n \leq x} a(n) \ln n = \pi(x) \ln x - \int_1^x \frac{\pi(t)}{t} dt.$$

Επειδή $\pi(t) = 0$ για $t < 2$ έχουμε:

$$\theta(x) = \pi(x) \ln x - \int_2^x \frac{\pi(t)}{t} dt.$$

η οποία είναι η πρώτη σχέση του θεωρήματος.

Για τη δεύτερη σχέση θέτουμε

$$b(n) = a(n) \ln n$$

και έχουμε

$$\pi(x) = \sum_{3/2 < n \leq x} b(n) \frac{1}{\ln n}$$

και

$$\theta(x) = \sum_{n \leq x} b(n).$$

Επιλέγουμε $f(x) = \frac{1}{\ln x}$ και για $y = \frac{3}{2}$ έχουμε από την ταυτότητα του Abel:

$$\pi(x) = \sum_{3/2 < n \leq x} b(n) \frac{1}{\ln n} = \frac{\theta(x)}{\ln x} - \frac{\theta(3/2)}{\ln(3/2)} + \int_{3/2}^x \frac{\theta(t)}{t(\ln t)^2} dt$$

και επειδή $\theta(t) = 0$ για $t < 2$ είναι:

$$\pi(x) = \frac{\theta(x)}{\ln x} + \int_2^x \frac{\theta(t)}{t(\ln t)^2}. \qquad \blacksquare$$

Αφού αποδείξαμε τις δύο παραπάνω σχέσεις μπορούμε πλέον να διατυπώσουμε

κάποιες ισοδύναμες μορφές του Θεωρήματος των Πρώτων Αριθμών.

***Θεώρημα***
Οι επόμενες προτάσεις είναι ισοδύναμες

$i)$ $\lim\limits_{x\to\infty} \dfrac{\pi(x)}{\frac{x}{\ln x}} = 1$

$ii)$ $\lim\limits_{x\to\infty} \dfrac{\theta(x)}{x} = 1$

$iii)$ $\lim\limits_{x\to\infty} \dfrac{\psi(x)}{x} = 1$

***Απόδειξη***
Από το προηγούμενο θεώρημα έχουμε

$$\frac{\theta(x)}{x} = \frac{\pi(x)\ln x}{x} - \frac{1}{x}\int_2^x \frac{\pi(t)}{t}dt$$

και

$$\frac{\pi(x)\ln x}{x} = \frac{\theta(x)}{x} + \frac{\ln x}{x}\int_2^x \frac{\theta(t)}{t\ln^2 t}dt.$$

Για να δείξουμε ότι η (i) συνεπάγεται τη (ii) αρκεί να δείξουμε ότι

$$\lim_{x\to\infty}\frac{1}{x}\int_2^x \frac{\pi(t)}{t}dt = 0.$$

Όμως από την (i) έχουμε ότι

$$\frac{\pi(t)}{t} = O\Big(\frac{1}{\ln t}\Big) \ , \ \ t \geq 2.$$

Οπότε

$$\frac{1}{x}\int_2^x \frac{\pi(t)}{t}dt = O\Big(\frac{1}{x}\int_2^x \frac{dt}{\ln t}\Big) = O\Big(\frac{1}{x}Li(x)\Big).$$

Έχουμε λοιπόν:

$$\int_2^x \frac{1}{\ln t}dt = \int_2^{\sqrt{x}} \frac{1}{\ln t}dt + \int_{\sqrt{x}}^x \frac{1}{\ln t}dt \leq \frac{\sqrt{x}}{\ln 2} + \frac{x-\sqrt{x}}{\ln\sqrt{x}}.$$

Επομένως

$$\frac{1}{x}Li(x) \to 0$$

καθώς $x \to \infty$. Άρα (i)$\Longrightarrow$(ii), δηλαδή

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1 \Longrightarrow \lim_{x\to\infty} \frac{\theta(x)}{x} = 1.$$

Για να δείξουμε ότι η (ii) συνεπάγεται την (i) αρκεί να δείξουμε ότι

$$\lim_{x\to\infty} \frac{\ln x}{x} \int_2^x \frac{\theta(t)}{t \ln^2 t} dt = 0.$$

Από (ii) έχουμε ότι

$$\theta(t) = O(t).$$

Επομένως

$$\frac{\ln x}{x} \int_2^x \frac{\theta(t)}{t \ln^2 t} dt = O\Big(\frac{\ln x}{x} \int_2^x \frac{1}{\ln^2 t} dt\Big).$$

Έχουμε δηλαδή

$$\int_2^x \frac{1}{\ln^2 t} dt = \int_2^{\sqrt{x}} \frac{1}{\ln^2 t} dt + \int_{\sqrt{x}}^x \frac{1}{\ln^2 t} dt \leq \frac{\sqrt{x}}{\ln^2 2} + \frac{x - \sqrt{x}}{\ln^2 \sqrt{x}}$$

οπότε

$$\frac{\ln x}{x} \int_2^x \frac{1}{\ln^2 t} dt \to 0$$

καθώς $x \to \infty$. Άρα (ii)$\Longrightarrow$(iii), οπότε η (i) και η (ii) είναι ισοδύναμες.
Επίσης από το θεώρημα στη σελίδα 58 προκύπτει ότι οι (ii) και (iii) είναι ισοδύναμες. ■

Αποδείξαμε, λοιπόν, τις ισοδύναμες σχέσεις που περιλαμβάνουν τις συναρτήσεις $\pi(x), \theta(x), \psi(x)$. Στο επόμενο θεώρημα θα δείξουμε την ισοδυναμία σχέσεων που περιλαμβάνουν την συνάρτηση $\pi(x)$ και τον νιοστό πρώτο $p_n$.

***Θεώρημα***

Έστω $p_n$ ο νιοστός πρώτος. Οι ακόλουθες πρότασεις είναι ισοδύναμες

1) $\lim\limits_{x\to\infty} \dfrac{\pi(x)\ln x}{x} = 1$

2) $\lim\limits_{x\to\infty} \dfrac{\pi(x)\ln(\pi(x))}{x} = 1$

3) $\lim\limits_{n\to\infty} \dfrac{p_n}{n\ln n} = 1$

***Απόδειξη***

Υποθέτουμε ότι η (1) ισχύει. Παίρνοντας λογάριθμους στο όριο έχουμε

$$\lim_{x\to\infty}\left[\ln\Big(\frac{\pi(x)\ln x}{x}\Big)\right] = 0 \Longrightarrow$$

$$\lim_{x\to\infty}\Big[\ln(\pi(x)) + \ln(\ln x) - \ln x\Big] = 0 \Longrightarrow$$

$$\lim_{x\to\infty}\left[\ln x\Big(\frac{\ln(\pi(x))}{\ln x} + \frac{\ln(\ln x)}{\ln x} - 1\Big)\right] = 0.$$

Όμως γνωρίζουμε ότι $\ln x \to \infty$ καθώς $x \to \infty$. Οπότε

$$\lim_{x\to\infty}\Big(\frac{\ln(\pi(x))}{\ln x} + \frac{\ln(\ln x)}{\ln x} - 1\Big) = 0.$$

Άρα

$$\lim_{x\to\infty}\frac{\ln(\pi(x))}{\ln x} = 1. \qquad (a)$$

Από (1) και (a) προκύπτει ότι

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

που σημαίνει ότι (1)$\Longrightarrow$(2).

Υποθέτουμε ότι ισχύει η (2). Παίρνοντας λογάριθμους στο όριο έχουμε

$$\lim_{x\to\infty}\left[\ln\Big(\frac{\pi(x)\ln(\pi(x))}{x}\Big)\right] = 0 \Longrightarrow$$

$$\lim_{x\to\infty}\Big(\ln(\pi(x))+\ln(\ln\pi(x))-\ln x\Big)=0\Longrightarrow$$

$$\lim_{x\to\infty}\left[\ln\pi(x)\Big(1+\frac{\ln(\ln\pi(x))}{\ln\pi(x)}-\frac{\ln x}{\ln\pi(x)}\Big)\right]=0.$$

Όμως είναι $\ln\pi(x)\to\infty$ καθώς $x\to\infty$, οπότε έχουμε

$$\lim_{x\to\infty}\Big(1+\frac{\ln(\ln\pi(x))}{\ln\pi(x)}-\frac{\ln x}{\ln\pi(x)}\Big)=0\Longrightarrow$$

$$\lim_{x\to\infty}\frac{\ln x}{\ln\pi(x)}=1. \qquad (b)$$

Από (2) και (b) είναι

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

δηλαδή (2)$\Longrightarrow$(1).
Τώρα υποθέτουμε πάλι ότι ισχύει η (2). Για $x=p_n$ είναι $\pi(x)=n$ άρα $\pi(x)\ln\pi(x)=n\ln n$. Έτσι

$$\lim_{n\to\infty}\frac{n\ln n}{p_n}=1,$$

το οποίο δείχνει ότι (2)$\Longrightarrow$(3).
Τέλος, υποθέτουμε ότι ισχύει η (3). Για δοσμένο $x$ ορίζουμε το $n$ από την ανισότητα

$$p_n\le x<p_{n+1}.$$

Έτσι $n=\pi(x)$ και έχουμε

$$\frac{p_n}{n\ln n}\le\frac{x}{n\ln n}<\frac{p_{n+1}}{n\ln n}=\frac{p_{n+1}}{(n+1)\ln(n+1)}\cdot\frac{(n+1)\ln(n+1)}{n\ln n}.$$

Άρα

$$\lim_{n\to\infty}\frac{x}{n\ln n}=1,$$

δηλαδή

$$\lim_{x\to\infty}\frac{x}{\pi(x)\ln\pi(x)}=1. \qquad \blacksquare$$

## 3.5 ΣΚΙΑΓΡΑΦΗΣΗ ΤΗΣ ΣΤΟΙΧΕΙΩΔΟΥΣ ΑΠΟΔΕΙΞΗΣ

Όπως έχουμε ήδη αναφέρει, ο Chebyshev προσπαθώντας να αποδείξει το Θεώρημα των Πρώτων Αριθμών χρησιμοποίησε στοιχειώδεις μεθόδους. Άλλωστε μοιάζει λογικό η απόδειξη ενός θεωρήματος για τους πρώτους να χρησιμοποιεί μεθόδους τις αριθμητικής. Παρ' όλα αυτά δεν κατάφερε να ολοκληρώσει την απόδειξη. Μερικά χρόνια αργότερα ο Riemann προσέγγισε διαφορετικά το πρόβλημα χρησιμοποιώντας μιγαδική ανάλυση. Με τις βάσεις που έθεσε μερικές δεκαετίες αργότερα οι Hadamard και de la Vallée Poussin κατάφεραν τελικά να ολοκληρώσουν την απόδειξη. Αν και το μεγάλο αυτό πρόβλημα είχε λυθεί, μέσα από τη λύση του προέκυψε ένα άλλο:
"Υπάρχει απόδειξη του Θεωρήματος των Πρώτων Αριθμών που χρησιμοποιεί μόνο στοιχειώδεις μεθόδους;"
Οι πρώτες απόψεις αμφέβαλαν για την ύπαρξη αυτή. Στήριζαν αυτές τις αμφιβολίες στην πεποίθηση ότι η μιγαδική ανάλυση είναι βαθύτερη από την πραγματική. Από την άλλη μεριά, πίστευαν ότι αν υπήρχε τέτοια απόδειξη θα ανοίγονταν καινούριοι δρόμοι στη Θεωρία Αριθμών.
Ο διάσημος Άγγλος μαθηματικός G.H. Hardy αναφέρει σε μια διάλεξή του το 1921 (το κείμενο προέρχεται από το [11]):
G.H. Hardy:
*No elementary proof of the prime number theorem is known and one may ask whether it is reasonable to expect one. Now we know that the problem is roughly equivalent to a theorem about an analytic function, the theorem that Riemann's zeta function has no roots on a certain line. A proof of such a theorem,not fundamentally dependent upon the ideas of the theory of functions seems to me to be extraordinarily unlikely. It is rash to assert that a mathematical theorem cannot be proved in a particular way; but one thing seems quite clear. We have certain views about the logic of the theory; we think that some theorems, as we say "lie deep" and others nearer to the surface. If anyone produces an elementary proof of the prime number theorem, he will show that these views are wrong, that the subject does not hang together in the way we have supposed, and that it is time for the books to be cast aside and for the theory to be rewritten.*
Αυτό, όμως, που συνέβη ήταν εντυπωσιακό. Ο Selberg και μετά ο Erdős και το 1948 και οι δύο μαζί κατάφεραν να αποδείξουν με στοιχειώδη μαθηματικά το Θεώρημα των Πρώτων Αριθμων, βασιζόμενοι στις μεθόδους του Chebyshev. Αυτές οι αποδείξεις στηρίχθηκαν σε ασυμπτωτικές σχέσεις της συνάρτησης von Mangoldt. Αυτές οι σχέσεις ονομάζονται πλέον τύποι Selberg. Σε αυτή την παράγραφο θα αναφέρουμε χωρίς απόδειξη τους τύπους Selberg και θα

οδηγηθούμε μέσα από αυτές στην απόδειξη του Θεωρήματος των Πρώτων Αριθμών. Για την πλήρη απόδειξη ο αναγνώστης μπορεί να μελετήσει τα [18],[7].

***Θεώρημα (Τύπος του Selberg)***
Για $x \geq 1$ ισχύει ότι

$$\psi(x)\ln x + \sum_{n\leq x}\Lambda(n)\psi\Big(\frac{x}{n}\Big) = 2x\ln x + O(x).$$

Χρησιμοποιώντας την παραπάνω σχέση θα δείξουμε τα βήματα που χρειάζονται για την απόδειξη του θεωρήματος.

Πρώτα, κάνοντας χρήση της συνάρτησης

$$\sigma(x) = e^{-x}\psi(e^x) - 1$$

ο τύπος του Selberg συνεπάγεται μια ολοκληρωτική ανισότητα της μορφής

$$|\sigma(x)|x^2 \leq 2\int_0^x\int_0^y |\sigma(u)|dudy + O(x). \qquad (1)$$

Το Θεώρημα των Πρώτων Αριθμών ισοδυναμεί με το να δείξουμε ότι

$$\sigma(x) \to 0$$

καθώς $x \to \infty$. Επομένως, αν θέσουμε

$$c = \limsup_{x\to\infty} |\sigma(x)|$$

αρκεί να δείξουμε ότι $c = 0$. Αυτό αποδεικνύεται αν υποθέσουμε ότι $c > 0$ και καταλήγουμε σε άτοπο εργαζόμενοι ως εξής:
Από τον ορισμό του $c$ έχουμε

$$|\sigma(x)| \leq c + g(x), \qquad (2)$$

όπου $g(x) \to 0$ καθώς $x \to \infty$. Αν είναι $c > 0$ από (1),(2) έχουμε την παρακάτω ανισότητα

$$|\sigma(x)| \leq c' + h(x), \qquad (3)$$

με $0 < c' < c$ και $h(x) \to 0$ καθώς $x \to \infty$.
Ξεκινώντας από τις (1),(2) για να καταλήξουμε στην τελευταία ανισότητα αυτό αποτελεί το μεγαλύτερο μέρος της απόδειξης. Τέλος, αν στην (3) θέσουμε $x \to \infty$ έχουμε ότι $c \leq c'$, το οποίο μας οδηγεί σε άτοπο και έτσι ολοκληρώνεται η απόδειξη.

Για την απόδειξη του τύπου του Selberg ο αναγνώστης παραπέμπεται στο [3].

# Chapter 4

# ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ

## 4.1 ΕΙΣΑΓΩΓΗ

Κρυπτογραφία είναι η επιστήμη που ασχολείται με την κωδικοποίηση και αποκωδικοποίηση μυστικών μηνυμάτων. Κάποιες από τις πιο ισχυρές και ασφαλείς μεθόδους κωδικοποίησης βασίζονται στη θεωρία αριθμών και ειδικότερα στους πρώτους αριθμούς. Σε αυτό το κεφάλαιο θα εξετάσουμε δύο σημαντικές έννοιες, την πιστοποίηση πρώτου και την παραγοντοποίηση σε πρώτους παράγοντες. Πιστοποίηση πρώτου είναι οποιαδήποτε διαδικασία απαντά στο ερώτημα αν ένας φυσικός αριθμός είναι πρώτος ή όχι. Έχει αποκτήσει τεράστιο ενδιαφέρον λόγω της στενής της σχέσης με την κρυπτογραφία και ειδικά την κρυπτογραφία δημοσίου κλειδιού. Όπως φαίνεται από το όνομά του, το σύστημα με δημόσιο κλειδί έχει κρυπτογραφικό κλειδί που είναι όχι μόνο γνωστό αλλά και δημοσιευμένο σε κάποιο βιβλίο ανάλογο του τηλεφωνικού καταλόγου. Το δημόσιο κλειδί, χοντρικά, μπορούμε να το σκεφτόμαστε σαν το κλειδί μιας καταπακτής (καταπακτή σημαίνει ότι εύκολα μπαίνεις αλλά βγαίνεις μόνο αν έχεις τα κατάλληλα μέσα) δια μέσου της οποίας τα μηνύματα εξαφανίζονται.

## 4.2 ΠΙΣΤΟΠΟΙΗΣΗ ΠΡΩΤΟΥ

Με μια πρώτη ματιά, το πρόβλημα της πιστοποίησης πρώτου μοιάζει προφανές. Αν ο $n$ δεν είναι πρώτος, θα έχει ένα διαιρέτη $m$ με $1 < m < n$. Επομένως αρκεί να ελέγξουμε όλους τους ακέραιους $2, 3, \ldots, \frac{n}{2}$ για να δούμε αν κάποιος από αυτούς διαιρεί τον $n$. Αν υπάρχει τέτοιος διαιρέτης, τότε ο $n$ είναι σύνθετος. Αν όχι, τότε ο $n$ είναι πρώτος. Αρκεί να ελέγξουμε μέχρι το $\frac{n}{2}$ γιατί αν ο $n$ έχει διαιρέτη $m < n$, τότε θα έχει και διαιρέτη $m \leq \frac{n}{2}$.
Ο παραπάνω αλγόριθμος μπορεί να βελτιωθεί. Παρατηρούμε ότι αν $n = m \cdot k$, τότε ένας εκ των $m, k$ πρέπει να είναι $\leq \sqrt{n}$. Επομένως, αρκεί να ελέγξουμε τους ακέραιους από το $2$ έως το $\sqrt{n}$, αντί για το $\frac{n}{2}$. Επιπλέον, αν ο $n$ έχει ένα διαιρέτη $m$ με $1 < m \leq \sqrt{n}$ τότε θα έχει και ένα πρώτο διαιρέτη $p$ με $1 < p \leq \sqrt{n}$. Άρα αρκεί να ελέγξουμε μόνο τους πρώτους που είναι $\leq \sqrt{n}$. Μετά τις παραπάνω παρατηρήσεις προκύπτει το εξής:

***Γενικός Αλγόριθμος Πιστοποίησης Πρώτου***
Για δοθέν $n > 0$ ελέγχουμε όλους τους πρώτους $p$ με $p \leq \sqrt{n}$. Ο $n$ είναι πρώτος αν και μόνο αν κανένας από τους $p$ δεν διαιρεί τον $n$.

**Παράδειγμα**
Ο $79$ είναι πρώτος;

Παρατηρούμε ότι $8 < \sqrt{79} < 9$, οπότε πρέπει να ελέγξουμε όλους τους πρώτους $\leq 8$, δηλαδή τους $2, 3, 5, 7$. Κανένας από αυτούς δεν διαιρεί το $79$, άρα το $79$ είναι πρώτος.

***Το Κόσκινο του Ερατοσθένη***
Κόσκινο στη Θεωρία Αριθμών είναι μια μέθοδος ή διαδικασία κατά την οποία βρίσκεις αριθμούς με συγκεκριμένες ιδιότητες, διαπερνώντας όλους τους φυσικούς αριθμούς μέχρι ένα άνω όριο. Όσοι δεν ικανοποιούν αυτή την ιδιότητα διαγράφονται. Στο τέλος της διαδικασίας θα έχουν μείνει μόνο οι φυσικοί με την επιθυμητή ιδιότητα.
Το κόσκινο του Ερατοσθένη είναι μια μέθοδος εύρεσης όλων των πρώτων μικρότερων ή ίσων ενός συγκεκριμένου αριθμού $x$. Η μέθοδος είναι η ακόλουθη: Για δοθέν $x > 0$ καταγράφουμε όλους τους πρώτους που είναι $\leq x$. Ξεκινώντας με το $2$, που είναι πρώτος, διαγράφουμε όλα τα πολλαπλάσια του $2$ στη λίστα. Ο επόμενος μη διεγραμμένος αριθμός στη λίστα, δηλαδή το $3$, είναι πρώτος.

Διαγράφουμε όλα τα πολλαπλάσια του $3$. Ο επόμενος μη διεγραμμένος αριθμός στη λίστα, δηλαδή το $5$, είναι πρώτος. Συνεχίζουμε με τον ίδιο τρόπο. Όπως εξηγήσαμε προηγουμένως η διαγραφή σταματά όταν φτάσουμε σε αριθμούς $> \sqrt{x}$. Όσοι αριθμοί δεν έχουν διαγραφεί είναι πρώτοι.

**Παράδειγμα**
Ποιοι είναι οι πρώτοι μέχρι το $100$;

Θα εφαρμόσουμε το Κόσκινο του Ερατοσθένη για αριθμούς $\leq 100$. Ξεκινώντας κάθε γύρο διαγραφών θα συνεχίζουμε τη διαδικασία όσο οι αριθμοί είναι $\leq \sqrt{100} = 10$.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
| 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
| 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 60 |
| 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 |
| 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |

Έτσι προκύπτει η λίστα

$$\{2, 3, 5, 7, \ldots, 83, 89, 97\}$$

που αποτελείται από τους 25 πρώτους που είναι μικρότεροι του $100$.

**Παρατηρήσεις**
1)Με κατάλληλη τροποποίηση το Κόσκινο του Ερατοσθένη μπορεί να δώσει όλους τους φυσικούς που είναι πρώτοι προς το $m$ και μικρότεροι ή ίσοι του $x$.

Η διαδικασία είναι η παρακάτω:
Έστω $m, x$ και $p_1, p_2, \ldots, p_k$ οι πρώτοι παράγοντες του $m$ σε αύξουσα σειρά. Καταγράφουμε όλους τους φυσικούς $\leq x$. Ξεκινάμε με το $p_1$ (αντί του 2) και διαγράφουμε όλα τα πολλαπλάσιά του. Συνεχίζουμε με το $p_2$, το $p_3$, έως το $p_k$. Οι μη διεγραμμένοι αριθμοί είναι ακριβώς αυτοί που είναι πρώτοι προς το $m$ και $\leq x$. Αν κάποιο $p_i > x$, αγνοούμε αυτό και όλους τους μεγαλύτερους πρώτους.
2)Θέλουμε να εξετάσουμε αν ένας αριθμός $n$ με 200 ψηφία είναι πρώτος ή όχι. Αν προσπαθήσουμε με δοκιμαστικές διαιρέσεις με όλους τους πρώτους μέχρι το $\sqrt{n}$ (Γενικός Αλγόριθμος Πιστοποίησης Πρώτου και Κόσκινο Ερατοσθένη) πρέπει να εξετάσουμε $\sim 4 \cdot 10^{97}$ πρώτους τους μικρότερους του $10^{100} \sim \sqrt{n}$. Αν ο υπολογιστής εξετάζει $10^9$ πρώτους ανά δευτερόλεπτο θα χρειαστούμε περίπου $10^{81}$ χρόνια!

## 4.3 ΑΛΓΟΡΙΘΜΟΙ ΠΙΣΤΟΠΟΙΗΣΗΣ ΠΡΩΤΟΥ

Όπως είδαμε στις προηγούμενες παραγράφους είναι θεωρητικά πολύ απλό να ελέγξουμε αν ένας ακέραιος είναι πρώτος, είτε με το γενικό αλγόριθμο είτε με το κόσκινο του Ερατοσθένη. Το πρόβλημα όμως, όπως είδαμε στην προηγούμενη παρατήρηση, είναι ότι για μεγάλα $n$ οι μέθοδοι αυτές είναι υπολογιστικά αδύνατες. Επομένως για αυτούς τους αριθμούς πρέπει να χρησιμοποιήσουμε άλλες μεθόδους.
Αλγόριθμος πιστοποίησης πρώτου είναι ένας αλγόριθμος με είσοδο έναν ακέραιο $n$ και έξοδο εάν είναι πρώτος ή σύνθετος. Υπάρχουν δύο κατηγορίες τέτοιων αλγορίθμων. Οι ντετερμινιστικοί και οι πιθανοτικοί αλγόριθμοι. Οι ντετερμινιστικοί στην έξοδό τους αποφαίνονται με βεβαιότητα αν ο $n$ είναι πρώτος ή σύνθετος. Για παράδειγμα ο γενικός αλγόριθμος και το κόσκινο του Ερατοσθένη είναι ντετερμινιστικοί αλγόριθμοι. Οι πιθανοτικοί στην έξοδό τους αποφαίνονται αν ο $n$ δεν είναι πρώτος ή αν πιθανώς είναι πρώτος. Επομένως ένας πιθανοτικός αλγόριθμος ενδέχεται να δώσει σαν πιθανό πρώτο κάποιο σύνθετο. Αυτοί οι σύνθετοι ονομάζονται ψευδοπρώτοι. Αντίθετα, αν ο αλγόριθμος αποφανθεί ότι ο $n$ είναι σύνθετος τότε σίγουρα είναι σύνθετος.
Ένα λογικό ερώτημα θα ήταν το εξής:
"Αφού οι ντετερμινιστικοί αλγόριθμοι αποφαίνονται με βεβαιότητα αν ένας αριθμός είναι πρώτος ή όχι, τότε γιατί υπάρχουν οι πιθανοτικοί που μπορεί να πέσουν έξω;"
Η απάντηση είναι απλή. Προτιμούμε τους πιθανοτικούς αλγόριθμους όταν θέλουμε εξοικονόμηση χρόνου, μιας και είναι πιο γρήγοροι από τους ντετερμινιστικούς.

***ΠΙΘΑΝΟΤΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ***
Στην κρυπτογραφία, το να γνωρίζουμε αν ένας ακέραιος είναι πιθανόν πρώτος με μεγάλη πιθανότητα είναι πολλές φορές εξίσου χρήσιμο με το να γνωρίζουμε αν είναι σίγουρα πρώτος. Παρακάτω, λοιπόν, θα εξετάσουμε κάποιους πιθανοτικούς αλγόριθμους πιστοποίησης πρώτου, ή πιο σωστά πιστοποίησης σύνθετου, μιας και αποφαίνονται με βεβαιότητα μόνο αν ο αριθμός είναι σύνθετος.

***Ο Αλγόριθμος του Fermat***
Αρχικά θα διατυπώσουμε το ακόλουθο θεώρημα:

***Μικρό Θεώρημα του Fermat***
Αν ο $p$ είναι πρώτος, με $p \nmid a$, τότε

$$a^{p-1} \equiv 1 \bmod p,$$

το οποίο αποτελεί ειδική περίπτωση του εξής:

***Θεώρημα Euler***
Αν $\gcd(a, n) = 1$ τότε

$$a^{\phi(n)} \equiv 1 \bmod n.$$

Επομένως, παρατηρούμε ότι αν υπάρχει ακέραιος $a$ με

$$a^{p-1} \not\equiv 1 \bmod p,$$

τότε ο $p$ δεν είναι πρώτος. Ενώ αν

$$a^{p-1} \equiv 1 \bmod p,$$

τότε ο $p$ είναι πιθανός πρώτος. Αν η τελευταία σχέση ισχύει για διάφορα $a$, τότε η πιθανότητα ο $p$ να είναι πρώτος συνεχώς αυξάνεται. Σύμφωνα με τα παραπάνω, έχουμε τον ακόλουθο αλγόριθμο πιστοποίησης πρώτου:

**Αλγόριθμος Fermat**
Σαν είσοδο έχουμε έναν ακέραιο $n$.
•*Βήμα 1ο:* Επιλέγουμε έναν ακέραιο $a$ με $2 < a < n - 2$.
•*Βήμα 2ο:* Υπολογίζουμε το $a^{n-1} \bmod n$.
•*Βήμα 3ο:* Αν η παραπάνω ποσότητα είναι διαφορετική του $1 \bmod n$ τότε ο $n$ είναι σύνθετος, ενώ αν είναι $1 \bmod n$ τότε ο $n$ πιθανώς είναι πρώτος.

**Παράδειγμα**
Εφαρμόζουμε τον αλγόριθμο Fermat για τον $n = 11387$:
Για $a = 2$ πρέπει να υπολογίσουμε το $2^{11386} \bmod 11387$. Παρατηρούμε ότι

$$2^{13} \equiv 8192 \equiv -3195 \bmod 11387 \Longrightarrow$$

$$2^{26} \equiv 10208025 \equiv 5273 \bmod 11387 \Longrightarrow$$

$$\vdots$$

$$2^{11388} \equiv 8642 \bmod 11387 \Longrightarrow$$
$$2^{11387} \equiv 4321 \bmod 11387.$$

Όμως αν $a^{n-1} \equiv 1 \bmod n$ θα ήταν

$$a^n \equiv a \bmod n$$

και $4321 \not\equiv 2 \bmod 11387$. Άρα ο $11387$ δεν είναι πρώτος. Συγκεκριμένα $11387 = 59 \cdot 193$.

Το 1891 ο Lucas βασίστηκε στον αλγόριθμο του Fermat και έδωσε μια επέκτασή του, η οποία τον έκανε ντετερμινιστικό:

***Θεώρημα Lucas***
Έστω ένας ακέραιος $n > 1$. Αν για κάθε πρώτο διαιρέτη $p$ του $n-1$ υπάρχει ακέραιος $a$ τέτοιος ώστε:
i)$a^{n-1} \equiv 1 \bmod n$ και
ii)$a^{\frac{n-1}{p}} \not\equiv 1 \bmod n$
τότε ο $n$ είναι πρώτος.

***ΨΕΥΔΟΠΡΩΤΟΙ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗ ΠΡΩΤΟΥ***
Όπως ήδη παρατηρήσαμε ο αλγόριθμος του Fermat αποφαίνεται με βεβαιότητα μόνο αν ο αριθμός είναι σύνθετος. Υπάρχουν όμως και περιπτώσεις στις οποίες χαρακτηρίζει πιθανούς πρώτους κάποιους σύνθετους. Για αυτούς τους αριθμούς έχουμε τον παρακάτω ορισμό:

***Ορισμός***
Έστω $n$ ένας σύνθετος ακέραιος. Ο $n$ λέγεται *ψευδοπρώτος ως προς τη βάση* $b$ αν για $b > 1$, $\gcd(n, b) = 1$ είναι $b^{n-1} \equiv 1 \bmod n$.

**Παράδειγμα**
Για $n = 341$ και $b = 2$ έχουμε:

$$2^{341-1} \equiv 1 \bmod 341$$

αλλά

$$341 = 11 \cdot 31.$$

Άρα ο $341$ είναι ψευδοπρώτος ως προς τη βάση 2. Οι 5 μικρότεροι ψευδοπρώτοι ως προς τη βάση 2 είναι οι αριθμοί $341, 561, 645, 1105$ και $1387$.

***Θεώρημα***
Για κάθε βάση $b > 1$, υπάρχουν άπειροι το πλήθος ψευδοπρώτοι ως προς τη βάση $b$.

***Απόδειξη***
Έστω $b > 1$. Θα δείξουμε ότι αν ο $p$ είναι περιττός πρώτος και $p \nmid b^2 - 1$ τότε ο ακέραιος

$$n = \frac{b^{2p} - 1}{b^2 - 1}$$

είναι ψευδοπρώτος ως προς τη βάση $b$. Προφανώς ο $n$ είναι σύνθετος αφού

$$n = \frac{b^p - 1}{b - 1} \cdot \frac{b^p + 1}{b + 1}.$$

Από το θεώρημα του Fermat έχουμε

$$b^p \equiv b \bmod p \Longrightarrow b^{2p} \equiv b^2 \bmod p. \qquad (1)$$

Επίσης

$$n - 1 = \frac{b^{2p} - b^2}{b^2 - 1}. \qquad (2)$$

Από (1),(2) και επειδή $p \nmid b^2 - 1$ έχουμε ότι

$$p | n - 1.$$

Όμως

$$n - 1 = b^{2p-2} + b^{2p-4} + \ldots + b^2.$$

Επομένως ο $n - 1$ είναι άθροισμα άρτιων το πλήθος προσθετέων , οι οποίοι είναι όλοι είτε άρτιοι είτε περιττοί. Άρα ο $n-1$ είναι άρτιος σε κάθε περίπτωση. Οπότε

$$2p | n - 1$$

και τότε

$$b^{2p} - 1 | b^{n-1} - 1.$$

Όμως

$$b^{2p} - 1 \equiv 0 \bmod n \Rightarrow b^{n-1} - 1 \equiv 0 \bmod n \Rightarrow b^{n-1} \equiv 1 \bmod n$$

οπότε ο $n$ είναι ψευδοπρώτος ως προς τη βάση b. ■

Οι πιθανοτικοί αλγόριθμοι για να αυξήσουν την πιθανότητα να είναι ένας αριθμός πρώτος δοκιμάζουν περισσότερες από μια βάσεις. Υπάρχουν όμως και αριθμοί, οι οποίοι είναι ψευδοπρώτοι ως προς κάθε βάση:

***Ορισμός***
Έστω $n$ ένας σύνθετος ακέραιος. Ο $n$ ονομάζεται *αριθμός Carmichael* αν είναι ψευδοπρώτος ως προς κάθε βάση $b$, με $b > 1$ και $\gcd(n, b) = 1$.

Οι αριθμοί Carmichael είναι πολύ σπάνιοι. Στους πρώτους 25,000,000,000 ακέραιους υπάρχουν μόνο 2,163. Παρ' όλα αυτά έχει αποδειχθεί από τους Alford, Granville και Pomerance ότι υπάρχουν άπειροι το πλήθος αριθμοί Carmichael.
Πριν αναφέρουμε τους δύο βασικούς πιθανοτικούς αλγόριθμους, θα χρειαστούμε και τους εξής ορισμούς:

***Ορισμός***
Για κάθε ακέραιο $a$ και περιττό πρώτο $p$ το *σύμβολο Legendre* ορίζεται ως εξής:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{αν } a \equiv 0 \bmod p \\ +1 & \text{αν } a \not\equiv 0 \bmod p \text{ και υπάρχει } x \in \mathbb{Z}\text{: } a \equiv x^2 \bmod p \\ -1 & \text{αν δεν υπάρχει τέτοιο } x \end{cases}$$

***Ορισμός***
Αν $n$ είναι ένας θετικός, περιττός ακέραιος με

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

με $p_i$ πρώτους, και $a$ ένας θετικός ακέραιος τότε το *σύμβολο Jacobi* ορίζεται ως

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \dots \left(\frac{a}{p_k}\right)^{e_k}$$

με $\left(\frac{a}{p_i}\right)$ , $i = 1, 2, \dots, k$ το σύμβολο Legendre.

***Ορισμός***
Ένας σύνθετος, περιττός ακέραιος $n$ λέγεται *Euler ψευδοπρώτος ως προς τη*

*βάση* $b$ αν

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \bmod n,$$

όπου $(\frac{b}{n})$ το σύμβολο Jacobi.

***Ορισμός***
Έστω $n$ ένας σύνθετος ακέραιος με $n-1 = 2^s t$, με $t$ περιττό και $s$ τη μέγιστη δύναμη του 2 τέτοια ώστε $2^s | n-1$. Για $b > 1$, $\gcd(n, b) = 1$ ο $n$ λέγεται *ισχυρός ψευδοπρώτος ως προς τη βάση* $b$ αν είτε
i)$b^t \equiv 1 \bmod n$ ή
ii)υπάρχει $r$, $0 \leq r < s$ τέτοιο ώστε $b^{2^r t} \equiv -1 \bmod n$.

Αφού ολοκληρώσαμε τους παραπάνω ορισμούς είμαστε σε θέση να παρουσιάσουμε τους ακόλουθους αλγόριθμους πιστοποίησης πρώτου:

**Αλγόριθμος Solovay-Strassen**
Σαν είσοδο έχουμε ένα περιττό ακέραιο $n$.
•*Βήμα 1ο:* Επιλέγουμε τυχαία $k$ ακέραιους $b_1, b_2, \ldots, b_k$ με $1 < b_i < n$.
•*Βήμα 2ο:* Για κάθε $1 < i < k$ υπολογίζουμε το $\gcd(b_i, n)$.
Αν $\gcd(b_i, n) > 1$ τότε ο $n$ είναι σύνθετος και σταματά η διαδικασία.
•*Βήμα 3ο:* Για κάθε $1 < i < k$ υπολογίζουμε το $A = b_i^{\frac{n-1}{2}} \bmod n$ και
$B = (\frac{b_i}{n}) \bmod n$.
Αν $A \neq B$ τότε ο $n$ είναι σύνθετος και σταματά η διαδικασία.
•*Βήμα 4ο:* Αν ικανοποιούνται τα (2),(3) ο $n$ είναι πιθανός πρώτος με πιθανότητα μεγαλύτερη του $1 - \frac{1}{2^k}$.

**Παρατήρηση**
Οι Solovay-Strassen προηγουμένως είχαν αποδείξει ότι:
"Ο $n$ μπορεί να είναι Euler ψευδοπρώτος για το πολύ τις μισές βάσεις $b$ με $1 < b < n$ και $\gcd(b, n) = 1$."
Όμως η περίπτωση ένας αριθμός να είναι Euler ψευδοπρώτος ως προς τη βάση $b$ είναι η ίδια με την περίπτωση να τρέξουμε τον αλγόριθμο και να μας δώσει σαν πιθανό πρώτο ένα σύνθετο. Άρα η πιθανότητα λανθασμένης εκτίμησης από τον αλγόριθμο είναι μικρότερη από $1/2$. Όμως τον αλγόριθμο τον "τρέξαμε"

για $k$ τυχαίους ακέραιους, επομένως η πιθανότητα ο $n$ να είναι πρώτος είναι

$$1 - \left(\frac{1}{2}\right)^k.$$

Τέλος, θα αναφέρουμε τον αλγόριθμο των Miller-Rabin, ο οποίος είναι και ο πιο αποδοτικός από τους προαναφερθέντες. Η ιδέα πάνω στην οποία βασίστηκαν είναι απλή και στηρίζεται στον ορισμό των ισχυρών ψευδοπρώτων:
Αν ο $n$ είναι πρώτος τότε ο $n-1$ είναι άρτιος, οπότε γράφεται στη μορφή $n-1 = 2^s t$, όπως στον ορισμό των ισχυρών ψευδοπρώτων. Όμως ο $n$ είναι πρώτος, άρα από το θεώρημα του Fermat έχουμε ότι

$$b^{n-1} \equiv 1 \bmod n.$$

Αν υπολογίσουμε τις τετραγωνικές ρίζες της ισοτιμίας θα έχουμε τις εξής περιπτώσεις:

$$b^{n-1} \equiv 1 \bmod n \Longrightarrow \begin{cases} b^{2^r t} \equiv -1 \bmod n \\ \text{ή} \\ b^t \equiv 1 \bmod n \end{cases}$$

με $0 \leq r < s$. Αν μέσα από την αλγοριθμική διαδικασία προκύψει ότι καμία από τις δύο ισοτιμίες δεν αληθεύει τότε ο αριθμός $n$ είναι σύνθετος.

**Αλγόριθμος Miller-Rabin**
Σαν είσοδο έχουμε ένα περιττό ακέραιο $n > 1$.
•*Βήμα 1ο:* Βρίσκουμε το $n-1$ και το γράφουμε στη μορφή $n-1 = 2^s t$ με $t$ περιττό.
•*Βήμα 2ο:* Επιλέγουμε ένα τυχαίο φυσικό $b$, με $1 < b < n$.
•*Βήμα 3ο:* Υπολογίζουμε το $m_1 \equiv b^t \bmod n$.
Αν $m_1 \equiv \pm 1 \bmod n$ τότε ο $n$ είναι πιθανός πρώτος και σταματάμε τη διαδικασία.
Αλλιώς υπολογίζουμε το $m_2 \equiv m_1^2 \bmod n$.
Αν $m_2 \equiv 1 \bmod n$ τότε ο $n$ είναι σύνθετος.
Αλλιώς αν $m_2 \equiv -1 \bmod n$ τότε ο $n$ είναι πιθανός πρώτος και σταματάμε τη διαδικασία.
Αλλιώς υπολογίζουμε το $m_3 \equiv m_2^2 \bmod n$.
Αν $m_3 \equiv 1 \bmod n$ τότε ο $n$ είναι σύνθετος.
Αλλιώς αν $m_3 \equiv -1 \bmod n$ τότε ο $n$ είναι πιθανός πρώτος.
Συνεχίζουμε τα ίδια βήματα του αλγορίθμου έως ότου να οδηγηθούμε σε πιθανό

πρώτο ή να φτάσουμε στο $m_t$.

**Παράδειγμα**
Για $n = 561$ έχουμε:
$n - 1 = 560 = 16 \cdot 35 = 2^4 \cdot 35$ οπότε $s = 4, t = 35$.
Έστω $b = 2$, τότε:

$$m_1 \equiv 2^{35} \equiv 263 \bmod 561$$

$$m_2 \equiv 263^2 \equiv 166 \bmod 561$$

$$m_3 \equiv 166^2 \equiv 67 \bmod 561$$

$$m_4 \equiv 67^2 \equiv 1 \bmod 561$$

Άρα ο $n = 561$ είναι σύνθετος. Πράγματι,

$$561 = 3 \cdot 11 \cdot 17.$$

***ΝΤΕΤΕΡΜΙΝΙΣΤΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ***

Έχουμε ήδη αναφέρει τρεις ντετερμινιστικούς αλγόριθμους, τον γενικό αλγόριθμο πιστοποίησης πρώτου, το κόσκινο του Ερατοσθένη και το θεώρημα Lucas. Στη συνέχεια θα αναφέρουμε το βασικό εκπρόσωπο αυτής της ομάδας αλγορίθμων. Το μεγάλο πρόβλημα των ντετερμινιστικών αλγορίθμων είναι ότι είναι πολύ αργοί. Μέχρι το 2003 ήταν ανοιχτό πρόβλημα το αν υπάρχει ντετερμινιστικός αλγόριθμος, ο οποίος δουλεύει σε πολυωνυμικό χρόνο.
Το 2003, ο M. Agrawal μαζί με δύο φοιτητές του, τους N. Kayal και N. Saxena, κατασκεύασαν έναν αλγόριθμο, πλέον γνωστό ως αλγόριθμο AKS, ο οποίος είναι ντετερμινιστικός και ανήκει στο P. Βασίζεται πάνω σε επεκτάσεις του μικρού θεωρήματος του Fermat.

***Θεώρημα***

Έστω $n$ ένας φυσικός αριθμός και $s \leq n$. Υποθέτουμε, επίσης, ότι $q, r$ είναι πρώτοι και ικανοποιούν τα εξής

$$q|r-1, \;\; n^{\frac{r-1}{q}} \not\equiv 0 \text{ ή } 1 \bmod r \text{ και}$$

$$\binom{q+s-1}{s} \geq n^{2\lfloor\sqrt{r}\rfloor}.$$

Αν για κάθε $a$ με $1 \leq a < s$ ισχύουν:

$$\gcd(a,n) = 1 \text{ και}$$

$$(x-a)^n \equiv x^n - a\Big( \bmod \gcd(x^r-1, n)\Big)$$

τότε ο $n$ είναι δύναμη πρώτου.

Η απόδειξη καθώς και η περαιτέρω μελέτη του αλγόριθμου AKS είναι πέρα από τα όρια αυτής της εργασίας. Ο αναγνώστης που ενδιαφέρεται μπορεί να μελετήσει την εργασία των Agrawal,Kayal και Saxena με τίτλο "Primes is in P".

**Αλγόριθμος AKS**

Σαν είσοδο έχουμε ένα ακέραιο $n > 1$.
•*Βήμα 1ο:* Αν $n = a^b$ με $a > 0$ και $b > 1$ τότε ο $n$ είναι σύνθετος.
•*Βήμα 2ο:* Επιλέγουμε $q, r, s$ που ικανοποιούν τις υποθέσεις του θεωρήματος AKS.
•*Βήμα 3ο:* Για $a = 1, 2, \ldots, s-1$ έχουμε:
Αν $a|n$ τότε ο $n$ είναι σύνθετος.

Αν $(x-a)^n \not\equiv x^n - a \Big( \text{ mod } \gcd(x^r-1, n) \Big)$ τότε πάλι ο $n$ είναι σύνθετος.
•*Βήμα 4ο:* Ο $n$ είναι πρώτος.

## 4.4 ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΣΕ ΠΡΩΤΟΥΣ ΠΑΡΑΓΟΝΤΕΣ

Κλείνοντας το κεφάλαιο αυτό θα αναφερθούμε σε κάποιες σύγχρονες μεθόδους παραγοντοποίησης. Με τον γενικό αλγόριθμο που ορίσαμε μπορούμε μέσω διαδοχικών διαιρέσεων να παραγοντοποιήσουμε οποιονδήποτε αριθμό. Παρ' όλα αυτά η διαδικασία αυτή καθίσταται πρακτικά αδύνατη όταν την επιχειρήσουμε σε "πολύ μεγάλους" αριθμούς. Ένα ακόμη μειονέκτημα του γενικού αλγόριθμου είναι ότι ταυτόχρονα απαντά σε δύο ερωτήματα:
"Είναι ο $n$ πρώτος;" και
"Ποια η παραγοντοποίησή του σε πρώτους παράγοντες;"
Ενώ με βάση τους αλγόριθμους πιστοποίησης (Miller-Rabin, Solovay-Strassen κλπ) γνωρίζουμε από πριν αν ο αριθμός που θέλουμε να παραγοντοποιήσουμε είναι σύνθετος. Ξεκινώντας την παρουσίαση διάφορων αλγορίθμων παραγοντοποίησης, πρώτος, όπως και στην πιστοποίηση πρώτου, είναι αυτός του Fermat, ο οποίος αποτελεί και βάση για άλλους ακόμη ταχύτερους.

***Ο Αλγόριθμος του Fermat***
Η ιδέα της μεθόδου είναι απλή και είναι η εξής. Έστω ότι θέλουμε να παραγοντοποιήσουμε τον αριθμό $n$. Αν καταφέρουμε να βρούμε ακέραιους $x, y$ τέτοιους ώστε

$$n = x^2 - y^2$$

τότε

$$n = (x - y)(x + y).$$

Επομένως, καταφέραμε να "σπάσουμε" τον $n$ σε δύο παράγοντες.

**Παρατήρηση**
Αν υποθέσουμε ότι ο $n$ είναι περιττός, τότε κάθε αναπαράστασή του σαν γινόμενο δύο ακεραίων μπορεί να γραφτεί στην παραπάνω μορφή.
Πράγματι, αν $n = a \cdot b$ θέτουμε

$$x = \frac{a+b}{2} \text{ και } y = \frac{a-b}{2}.$$

Οι $x, y$ είναι ακέραιοι, αφού $a, b$ περιττοί μιας και $n$ περιττός. Έχουμε

$$x^2 - y^2 = \frac{a^2 + 2ab + b^2 - a^2 + 2ab - b^2}{4} = a \cdot b = n.$$

Οπότε

$$n = x^2 - y^2 = (x - y)(x + y).$$

Για να βρούμε τους ακέραιους $x, y$ εργαζόμαστε ως εξής:
Υπολογίζουμε τους ακέραιους $x^2 - n$, με $x > \lfloor \sqrt{n} \rfloor$, έως ότου προκύψει τέλειο τετράγωνο ακεραίου. Δηλαδή

$$x^2 - n = y^2 \Longrightarrow n = x^2 - y^2 = (x - y)(x + y).$$

Ο αλγόριθμος είναι ο παρακάτω

**Αλγόριθμος Fermat**
Σαν είσοδο έχουμε ένα περιττό ακέραιο $n$.
•*Βήμα 1ο:* Θέτουμε $x = \lfloor \sqrt{n} \rfloor + 1$ και $y2 = x^2 - n$.
•*Βήμα 2ο:* Όσο ο $y2$ δεν είναι τέλειο τετράγωνο αυξάνουμε το $x$ κατά 1 και θέτουμε $y2 = x^2 - n$.
•*Βήμα 3ο:* Θέτουμε $y2 = y^2$.
•*Βήμα 4ο:* Επιστρέφουμε $n = (x - y)(x + y)$.

**Παράδειγμα**
Για $n = 5959$ είναι

$$\lfloor \sqrt{5959} \rfloor + 1 = 78.$$

Έχουμε:

| | | | |
|---|---|---|---|
| $x$ : | 78 | 79 | 80 |
| $y2$ : | 125 | 282 | 441 |

Όμως $441 = 21^2$ επομένως

$$n = 5959 = 80^2 - 21^2 = (80 - 21)(80 + 21) = 59 \cdot 101.$$

**Παρατήρηση**
Όπως προκύπτει από τα παραπάνω ο αλγόριθμος του Fermat είναι ιδιαίτερα απλός, αλλά δεν είναι εξίσου αποδοτικός. Σε κάποιες περιπτώσεις μπορεί να χρειαστεί περισσότερο χρόνο και από τον γενικό αλγόριθμο.

### *Ο Αλγόριθμος του Dixon*

***Ορισμός***
*Βάση παραγοντοποίησης* $B$ καλείται το σύνολο των διακεκριμένων πρώτων

$$\{-1, p_1, \ldots, p_k\},$$

όπου $-1 = n - 1 \bmod n$. Ο ακέραιος $n$ καλείται *B-λείος* αν γράφεται σαν γινόμενο στοιχείων του $B$. Ο ακέραιος $b$ λέγεται *B-προσαρμοσμένος ως προς τον φυσικό* $n$ αν ο ακέραιος $c$, με

$$-\frac{n}{2} \leq c \leq \frac{n}{2} \text{ και } b^2 \equiv c \bmod n$$

είναι $B$-λείος.

**Παράδειγμα**
Έστω η βάση

$$B = \{-1, 2, 3, 5\}$$

και οι αριθμοί $1800$ και $40$. Παρατηρούμε ότι

$$1800 = 2^3 \cdot 3^2 \cdot 5^2 \text{ και } 40 = 2^3 \cdot 5$$

επομένως είναι $B$-λείοι.
Επίσης

$$59^2 \equiv 40 \bmod 1147 \text{ και } -\frac{1147}{2} \leq 40 \leq \frac{1147}{2}.$$

Άρα ο $b = 59$ είναι $B$-προσαρμοσμένος ως προς τον 1147.

***Θεώρημα (Βασικό Κριτήριο Παραγοντοποίησης)***
Έστω ο φυσικός $n$ και έστω ότι υπάρχουν φυσικοί $x, y$ με

$$x^2 \equiv y^2 \bmod n$$

αλλά

$$x \not\equiv \pm y \bmod n.$$

Τότε ο $n$ είναι σύνθετος και ο $d = \gcd(x-y, n)$ δίνει μη τετριμμένο παράγοντα του $n$.

***Απόδειξη***
Αν $d = n$ τότε $x \equiv y \bmod n$ το οποίο δεν ισχύει από υπόθεση.
Αν $d = 1$ και από την ιδιότητα

$$a|bc \text{ και } \gcd(a, b) = 1 \Rightarrow a|c$$

έχουμε

$$n|x^2 - y^2 = (x - y)(x + y) \text{ και } \gcd(n, x - y) = 1 \Rightarrow n|x + y$$

δηλαδή

$$x \equiv -y \bmod n$$

που είνα άτοπο από υπόθεση. Άρα $d \neq 1, n$ και ο $d$ είναι μη τετριμμένος παράγοντας του σύνθετου $n$.

**Παράδειγμα**
Είναι

$$12^2 \equiv 2^2 \bmod 35 \text{ και } 12 \not\equiv \pm 2 \bmod 35.$$

Άρα ο $35$ είναι σύνθετος και ο $\gcd(12-2, 35) = 5$ είναι μη τετριμμένος παράγοντάς του.

Η βασική ιδέα του αλγόριθμου του Dixon είναι ότι παίρνουμε μια βάση που αποτελείται από μικρούς πρώτους και φτιάχνουμε τετράγωνα που να γράφονται σαν γινόμενα στοιχείων της βάσης. Έτσι κατασκευάζουμε ένα πίνακα του οποίου η κάθε γραμμή αποτελείται από τους εκθέτες των πρώτων αριθμών της βάσης κάθε τέτοιου τετραγώνου. Αν πάρουμε περισσότερα τέτοια τετράγωνα από τα στοιχεία της βάσης, ο πίνακας που θα προκύψει θα έχει $\bmod 2$ γραμμικές εξαρτήσεις μεταξύ των γραμμών. Οι γραμμικά εξαρτημένες γραμμές δίνουν $x^2 \equiv y^2 \bmod n$. Αν $x \not\equiv \pm y \bmod n$ τότε από το βασικό κριτήριο παραγοντοποίησης έχουμε μη τετριμμένο παράγοντα του $n$.

**Παράδειγμα**
Θα παραγοντοποιήσουμε τον $n = 849239$. Έχουμε

$$\sqrt{849239} = 921, 5 \ldots .$$

Για $t = 922, 923, \ldots$ υπολογίζουμε τον μικρότερο θετικό της κλάσης $t^2 \bmod n$:

$$922^2 \equiv 5 \cdot 13^2 \bmod n$$

$$\vdots$$

$$933^2 \equiv 2 \cdot 5^4 \cdot 17 \bmod n$$

$$\vdots$$

$$937^2 \equiv 2 \cdot 5 \cdot 13^2 \cdot 17 \bmod n$$

Παρατηρούμε ότι οι ενδιάμεσοι αριθμοί δίνουν μεγάλους πρώτους παράγοντες και εδώ έχουμε επιλέξει $B = \{-1, 2, 3, 5, 7, 11, 13, 17\}$.
Πολλαπλασιάζοντας τις 3 ισοδυναμίες κατά μέλη έχουμε

$$922^2 \cdot 933^2 \cdot 937^2 \equiv 2^2 \cdot 5^6 \cdot 13^4 \cdot 17^2 \bmod n.$$

Επομένως για $x = 922 \cdot 933 \cdot 937$ και $y = 2 \cdot 5^3 \cdot 13^2 \cdot 17$ είναι

$$x^2 \equiv y^2 \bmod n \quad \text{και} \quad x \not\equiv \pm y \bmod n.$$

Άρα υπολογίζοντας τον $\gcd(x-y, n) = 691$ έχουμε ένα γνήσιο παράγοντα του $n$.

Σύμφωνα με τα παραπάνω έχουμε:

**Αλγόριθμος Dixon**
Σαν είσοδο έχουμε ένα φυσικό $n$ προς παραγοντοποίηση.
•*Βήμα 1ο:* Επιλέγουμε φυσικό $y$ και κατασκευάζουμε βάση $B$ των πρώτων παραγόντων $p_1, p_2, \ldots, p_{\pi(y)}$ του $n$ με $p_i \leq y$, $i = 1, 2, \ldots, \pi(y)$.

•*Βήμα 2ο:* Αν $p_i \nmid n$ για όλα τα $i$, βρίσκουμε ακέραιους $b_i$, με $1 \leq b_i \leq n$ και $i = 1, 2, \ldots, \pi(y) + 2$, $B$-προσαρμοσμένους ως προς τον $n$.

•*Βήμα 3ο:* Αν $b_i^2 = (-1)^{a_{i0}} p_1^{a_{i1}} \ldots p_{\pi(y)}^{a_{i\pi(y)}} \bmod n$ τότε αντιστοιχούμε στο $b_i$ το διάνυσμα $u_i$ των εκθετών mod2: $u_i = (u_{i0}, u_{i1}, \ldots u_{i\pi(y)})$
($u_{ij} = 0$ αν $a_{ij}$ άρτιος, $u_{ij} = 1$ αν $a_{ij}$ περιττός)

•*Βήμα 4ο:* Υπολογίζουμε το υποσύνολο $I$ του $\{1, 2, \ldots, \pi(y) + 2\}$ με $\sum_{i \in I} u_i = 0$.

•*Βήμα 5ο:* Υπολογίζουμε τα γινομένα $b = \prod_{i\in I} b_i$, $c = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_{\pi(y)}^{\gamma_{\pi(y)}}$ όπου $2\gamma_j = \sum_{i\in I} a_{ij}$.
ΠΡΟΣΟΧΗ: Πρέπει κάθε πρώτος της βάσης $B$ να χρησιμοποιείται άρτιο πλήθος φορών.

•*Βήμα 6ο:* Αν $b \not\equiv \pm c \bmod n$ υπολογίζουμε τον $\gcd(b+c, n)$, ο οποίος αποτελεί μη τετριμμένο παράγοντα του $n$. Αν $b \equiv \pm c \bmod n$ υπολογίζουμε άλλο $I \subset \{1, 2, \dots, \pi(y)+2\}$ ή άλλο $y$ και επαναλαμβάνουμε τη διαδικασία.

**Σημείωση**
Για την εύρεση ακέραιων $b_i$ δοκιμάζουμε ακέραιους της μορφής $\lfloor\sqrt{kn}\rfloor + j$, $j = 0, 1, \dots, k = 1, 2, \dots$. Ο μικρότερος ακέραιος που είναι τετράγωνο τέτοιων $b_i$ είναι αρκετά μικρός, επομένως υπάρχουν αυξημένες πιθανότητες να είναι $B$-προσαρμοσμένος ως προς το $n$.

**Παράδειγμα**
Θα παραγοντοποιήσουμε τον αριθμό $n = 93623$.
1) Έστω η βάση $B = \{-1, 2, 3, 5, 7, 11, 13\}$. Αφού $|B| = 7$ πρέπει να βρούμε 8 $B$-προσαρμοσμένους ακέραιους ως προς τον 93623.
2) Κανένας πρώτος της βάσης $B$ δεν διαιρεί τον $n$. Για $\lfloor\sqrt{kn}\rfloor + j$, $k, j = 1, 2, \dots, 9$. Έχουμε:

$$\sqrt{n} = 305.9\dots \qquad b_1 : 306^2 = 93636 \equiv 13 \bmod n$$

$$\sqrt{2n} = 432.7\dots \qquad b_2 : 433^2 = 187489 \equiv 243 \equiv 3^5 \bmod n$$

$$\sqrt{3n} = 529.9\dots \qquad b_3 : 531^2 = 281961 \equiv 1092 \equiv 2^2 \cdot 3 \cdot 7 \cdot 13 \bmod n$$

και $\qquad b_4 : 537^2 = 288369 \equiv 7500 \equiv 2^2 \cdot 3 \cdot 5^4 \bmod n$

$$\sqrt{4n} = 611.9\dots \qquad b_5 : 612^2 = 374544 \equiv 52 \equiv 2^2 \cdot 13 \bmod n$$

$$\sqrt{5n} = 684.1\dots \qquad \text{δεν υπάρχει τέτοιο } b_i$$

$$\sqrt{6n} = 749.4\dots \qquad b_6 : 809^2 = 654481 \equiv -880 \equiv -2^4 \cdot 5 \cdot 11 \bmod n$$

$$\sqrt{7n} = 809.5\dots \qquad b_7 : 866^2 = 749956 \equiv 972 \equiv 2^2 \cdot 3 \cdot 5 \bmod n$$

$$\sqrt{8n} = 865.4\dots \qquad b_8 : 918^2 = 842724 \equiv 117 \equiv 3^2 \cdot 13 \bmod n.$$

3) Οπότε προκύπτουν 8 διανύσματα του $\mathbb{Z}_2^7$:

$$u_1 = (0\ 0\ 0\ 0\ 0\ 0\ 1) \qquad u_5 = (0\ 0\ 0\ 0\ 0\ 0\ 1)$$
$$u_2 = (0\ 0\ 1\ 0\ 0\ 0\ 0) \qquad u_6 = (1\ 0\ 0\ 1\ 0\ 1\ 0)$$
$$u_3 = (0\ 0\ 1\ 0\ 1\ 0\ 1) \qquad u_7 = (0\ 0\ 1\ 0\ 0\ 0\ 0)$$
$$u_4 = (0\ 0\ 1\ 0\ 0\ 0\ 0) \qquad u_8 = (0\ 0\ 0\ 0\ 0\ 0\ 1)$$

Σημείωση: Σε όσους αριθμούς έχουμε άρτιο εκθέτη η αντίστοιχη τιμή τους προκύπτει μηδέν.
4) Επομένως προκύπτει το γραμμικό ομογενές σύστημα:

$$x_1\bar{u}_1 + x_2\bar{u}_2 + \ldots + x_8\bar{u}_8 \equiv 0 \bmod 2.$$

Δηλαδή

$$\left.\begin{aligned} x_6 &= 0 \\ x_2 + x_3 + x_4 + x_7 &= 0 \\ x_3 &= 0 \\ x_1 + x_3 + x_5 + x_8 &= 0 \end{aligned}\right\} \bmod 2.$$

Μια λύση του συστήματος είναι

$$x_1 = x_5 = 1$$
$$x_2 = x_3 = x_4 = x_6 = x_7 = x_8 = 0$$

Άρα

$$I = \{x_1, x_5\}.$$

Τότε:
5)

$$b = \prod_{i \in I} b_i = b_1 b_5 = 187272$$

$$c^2 = 13 \cdot 2^2 \cdot 13 \Rightarrow c^2 = 13^2 \cdot 2^2 \Rightarrow c = 26.$$

6) Όμως

$$187272 \equiv 26 \bmod n$$

άρα δεν μπορούμε να βρούμε μη τετριμμένο παράγοντα του $n$.
4) Βρίσκουμε άλλη λύση

$$I' = \{x_1, x_4\}$$

5)

$$b = 433 \cdot 537 = 232521$$

$$c^2 = 3^5 \cdot 2^2 \cdot 3 \cdot 5^4 = \left(2 \cdot 3^3 \cdot 5^2\right)^2 \Rightarrow c = 1350$$

6)

$$232521 \equiv 45275 \bmod n \Rightarrow b \not\equiv \pm c \bmod n.$$

Άρα ο $\gcd(b + c, n) = 373$, όπως προκύπτει από τον αλγόριθμο του Ευκλείδη, είναι μη τετριμμένος παράγοντας του $n$ και συγκεκριμένα

$$93623 = 373 \cdot 521.$$

***Ο Αλγόριθμος p-1 του Pollard***

Η μέθοδος $p-1$ προτάθηκε το 1974 από τον John Pollard και δουλεύει ικανοποιητικά για την παραγοντοποίηση ακεραίων με παράγοντες που έχουν μια συγκεκριμένη ιδιότητα. Η ιδιότητα αυτή αφορά τους σύνθετους $n$ που έχουν πρώτο παράγοντα $p$ τέτοιο ώστε ο $p - 1$ να έχει μόνο μικρούς παράγοντες. Τότε μπορούμε να υπολογίσουμε ένα πολλαπλάσιο του $p - 1$ (χωρίς προφανώς να γνωρίζουμε τον $p - 1$ ή τον $p$) σαν γινόμενο δυνάμεων μικρών πρώτων.
Παρατηρούμε λοιπόν, ότι ο αλγόριθμος $p-1$ του Pollard όπως και ο αλγόριθμος του Dixon βασίζονται σε ένα προκαθορισμένο σύνολο $B$ που αποτελείται από μικρούς πρώτους. Παρουσιάζουμε τον αλγόριθμο:

**Αλγόριθμος p-1 του Pollard**
Σαν είσοδο έχουμε έναν αριθμό $n$ προς παραγοντοποίηση και ένα σύνολο $B$.
•*Βήμα 1ο:* Υπολογίζουμε το

$$k = \prod_{q \le B, q \text{ πρώτος}} q^{\lfloor \log_q B \rfloor}$$

π.χ. Για $B = 13$: $\quad k = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
ΠΡΟΣΟΧΗ: $2^3 = 3 < 13$ και $2^4 = 16 > 13$ άρα $\log_2 13 = 3$.

•*Βήμα 2ο:* Επιλέγουμε ακέραιο $a$, με $1 < a < n$, και υπολογίζουμε τον $\gcd(a, n) = d$.

•*Βήμα 3ο:* Αν $d > 1$ (συνήθως $d = 1$ αφού $a = 2$ και $n$ περιττός), τότε ο $d$ είναι

μη τετριμμένος παράγοντας του $n$.
Αν $d = 1$ υπολογίζουμε τον $\gcd(a^k - 1, n) = d_1$.

•*Βήμα 4ο:* Αν $1 < d_1 < n$ ο $d_1$ είναι μη τετριμμένος παράγοντας του $n$.
Αν $d_1 = 1$ ή $d_1 = n$ επιλέγουμε άλλο $B$ και επαναλαμβάνουμε τη διαδικασία.

Αν λοιπόν ο $n$ έχει την ιδιότητα που αναφέραμε προηγουμένως και $p$ ένας πρώτος παράγοντάς του, θα είναι

$$p - 1 = 2^a \cdot 3^b \cdot 5^c \cdot 7^d \dots$$

όπου κάθε παράγοντας του $p - 1$ θα ανήκει στο $B$. Άρα ο $k$ θα είναι από κατασκευή πολλαπλάσιο του $p - 1$, δηλαδή

$$k = \lambda(p - 1).$$

Τότε όμως για κάθε $a$, με $1 < a < n$ και $\gcd(a, p) = 1$, έχουμε από το μικρό θεώρημα του Fermat

$$a^k = a^{\lambda(p-1)} = (a^{p-1})^\lambda \equiv 1 \bmod p \Rightarrow a^k - 1 \equiv 0 \bmod p \Rightarrow p | a^k - 1.$$

Επομένως αν $d \neq n$ και $1 < d < n$, ο $d$ είναι μη τετριμμένος παράγοντας του $n$.

**Παράδειγμα**
Θα παραγοντοποιήσουμε τον $n = 1241143$. Θεωρούμε τη βάση

$$B = \{-1, 2, 3, 5, 7, 11, 13\}.$$

Τότε

$$k = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 32760$$

Επιλέγουμε τυχαία $a = 2$. Τότε $\gcd(2, 1241143) = 1$, επομένως υπολογίζουμε τον $2^k - 1 = 2^{32760} - 1$.
Είναι $\gcd(2^{32760} - 1, 1241143) = 547$ και $1 < 547 < 1241143$.
Άρα ο $547$ είναι μη τετριμμένος παράγοντας του $1241143$ και πιο συγκεκριμένα

$$1241143 = 547 \cdot 2269.$$

Αφού οι $547, 2269$ είναι πρώτοι έχουμε την παραγοντοποίηση που ζητάμε.

# ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] A. Adler and J.E. Coury, *The Theory of Numbers*, Jones and Bartlett Publishers, Boston, London, 1995.

[2] M. Aigner and G.M. Ziegler, *Proofs from the BOOK*, Springer-Verlag, New York, 1999.

[3] T. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1994.

[4] P. Bateman and H. Diamond, *Analytic Number Theory*, World Scientific Publishing, New Jersey, London, 2004.

[5] G. Everest and T. Ward, *An Introduction to Number Theory*, Springer-Verlag, New York, 2005

[6] B. Fine and G. Rosenberger, *Number Theory: An Introduction via the Distribution of Primes*, Birkhäuser, Boston, Basel, Berlin, 2007.

[7] G.H. Hardy and E.W. Wright, *An Introduction to the Theory of Numbers*, 5th edition, Clarendon Press, Oxford, 1979.

[8] A.E. Ingham, *The Distribution of Prime Numbers*, Stechert-Hafner, New York, London, 1964.

[9] Χ. Κουκουβίνος και Α. Παπαϊωάννου, *Κρυπτογραφία*, Εκδόσεις Ε.Μ.Π., Αθήνα, 2005.

[10] L. Moser, *An Introduction to the Theory of Numbers*, The Trillia Group, West Lafayette, 2004.

[11] M. Nathanson, *Elementary Methods in Number Theory*, Springer-Verlag, NewYork,

2000.

[12] Α. Παπαϊωάννου και Μ. Ρασσιάς, *Εισαγωγή στη Θεωρία Αριθμών*, Εκδόσεις Συμεών, Αθήνα, 2010.

[13] M. Rassias, *Problem-Solving and Selected Topics in Number Theory*, Springer, New York, London, 2010.

[14] P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York, 1996.

[15] D. Shanks, *Solved and Unsolved Problems in Number Theory*, Chelsea Publishing Company, New York, 1978.

[16] J. Shockley, *Intoduction to Number Theory*, Holt, Rinehart and Winston, New York, Chicago, London, 1967.

[17] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge University Press, Cambridge, 1995.

[18] G. Tenenbaum and M. Mendes France, *Les Nombres Premiers*, Presses Universitaires de France, Paris, 1997.