Έξι αποδείξεις της απειρίας των πρώτων αριθμών

Κεφάλαιο 1

Απολύτως φυσιολογικά, ξεκινάμε από την πιθανότατα παλαιότερη Απόδειξη του Βιβλίου, η οποία συνήθως αποδίδεται στον Ευκλείδη (*Στοιχεία* IX, 20). Δείχνει ότι η ακολουθία των πρώτων αριθμών δεν τερματίζεται.

■ **Η απόδειξη του Ευκλείδη.** Για κάθε πεπερασμένο σύνολο πρώτων αριθμών $\{p_1,\dots,p_r\}$, θεωρούμε τον φυσικό αριθμό $n = p_1p_2\cdots p_r + 1$. Αυτός ο n έχει κάποιον πρώτο διαιρέτη p. Όμως ο p δεν είναι κάποιος από τους p_i: αν συνέβαινε αυτό, ο p θα ήταν ταυτόχρονα διαιρέτης του n και του γινομένου $p_1p_2\cdots p_r$, συνεπώς θα ήταν διαιρέτης και της διαφοράς $n - p_1p_2\cdots p_r = 1$, το οποίο είναι αδύνατο. Άρα, ένα πεπερασμένο σύνολο $\{p_1,\dots,p_r\}$ δεν μπορεί να είναι η συλλογή *όλων* των πρώτων αριθμών. □

Πριν συνεχίσουμε, ας διευκρινίσουμε τον συμβολισμό που θα χρησιμοποιούμε. $\mathbb{N} = \{1,2,3,\dots\}$ είναι το σύνολο των φυσικών, $\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$ το σύνολο των ακεραίων, και $\mathbb{P} = \{2,3,5,7,\dots\}$ το σύνολο των πρώτων.

Στη συνέχεια, θα παρουσιάσουμε διάφορες άλλες αποδείξεις (μέσα από μια πολύ πιο πλούσια λίστα) που ελπίζουμε ότι θα απολαύσει ο αναγνώστης όσο και εμείς. Αν και αντιμετωπίζουν το ερώτημα από διαφορετικές οπτικές γωνίες, η ακόλουθη βασική ιδέα είναι κοινή σε όλες τους: Υπάρχουν οσοδήποτε μεγάλοι φυσικοί αριθμοί, και κάθε φυσικός αριθμός $n \geq 2$ έχει τουλάχιστον έναν πρώτο διαιρέτη. Από αυτά τα δύο δεδομένα από κοινού προκύπτει ότι το $\mathbb{P}$ είναι αναγκαστικά άπειρο σύνολο. Η επόμενη απόδειξη οφείλεται στον Christian Goldbach (από ένα γράμμα προς τον Leonhard Euler, 1730), η τρίτη απόδειξη είναι κατά τα φαινόμενα παρατήρηση πολλών, η τέταρτη δόθηκε από τον ίδιο τον Euler, η πέμπτη απόδειξη διατυπώθηκε από τον Harry Fürstenberg, ενώ η τελευταία απόδειξη οφείλεται στον Paul Erdős.

■ **Δεύτερη Απόδειξη.** Ξεκινάμε με κάποιες παρατηρήσεις για τους *αριθμούς Fermat* $F_n = 2^{2^n}+1$ για $n = 0,1,2,\dots$. Θα δείξουμε ότι οποιοιδήποτε δύο αριθμοί Fermat είναι σχετικώς πρώτοι (οπότε θα πρέπει να υπάρχουν άπειροι το πλήθος πρώτοι αριθμοί). Για τον σκοπό αυτό, επαληθεύουμε την αναδρομική σχέση

$$\prod_{k=0}^{n-1} F_k \;=\; F_n - 2 \qquad (n \geq 1),$$

απ' όπου έπεται άμεσα ο ισχυρισμός μας. Πράγματι, αν ο m είναι διαιρέτης, ας πούμε, του F_k και του F_n $(k < n)$, τότε ο m διαιρεί τον 2, άρα $m = 1$ ή 2. Όμως, η περίπτωση $m = 2$ απορρίπτεται, διότι όλοι οι αριθμοί Fermat είναι περιττοί.

$$\begin{aligned} F_0 &= 3\\ F_1 &= 5\\ F_2 &= 17\\ F_3 &= 257\\ F_4 &= 65537\\ F_5 &= 641\cdot 6700417 \end{aligned}$$

Οι πρώτοι έξι αριθμοί Fermat

Για να αποδείξουμε την αναδρομική σχέση εφαρμόζουμε επαγωγή ως προς n. Για $n = 1$ έχουμε $F_0 = 3$ και $F_1 - 2 = 3$. Επαγωγικά τώρα συμπεραίνουμε ότι

$$\begin{aligned} \prod_{k=0}^{n} F_k \;&=\; \Big(\prod_{k=0}^{n-1} F_k\Big) F_n \;=\; (F_n-2)F_n \;=\\ &= (2^{2^n}-1)(2^{2^n}+1) \;=\; 2^{2^{n+1}} - 1 \;=\; F_{n+1} - 2. \end{aligned}$$

□

■ **Τρίτη Απόδειξη.** Υποθέτουμε ότι το $\mathbb{P}$ είναι πεπερασμένο και ότι ο p είναι ο μέγιστος πρώτος. Θεωρούμε τον λεγόμενο *αριθμό Mersenne* $2^p - 1$ και θα αποδείξουμε ότι κάθε πρώτος παράγοντας q του $2^p - 1$ είναι μεγαλύτερος από τον p, απ' όπου προκύπτει αμέσως το ζητούμενο συμπέρασμα. Έστω q ένας πρώτος

Το θεώρημα του Lagrange

Αν G είναι μια πεπερασμένη (πολλαπλασιαστική) ομάδα και U είναι μια υποομάδα της, τότε ο $|U|$ διαιρεί τον $|G|$.

■ **Απόδειξη.** Θεωρούμε τη διμελή σχέση

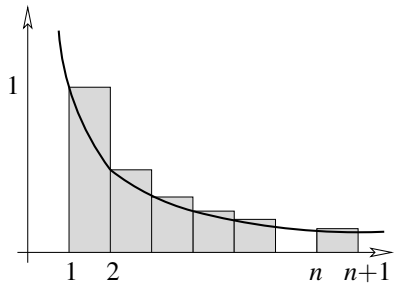
$$a \sim b :\iff ba^{-1} \in U.$$

Από τα αξιώματα της ομάδας προκύπτει ότι η $\sim$ είναι σχέση ισοδυναμίας. Η κλάση ισοδυναμίας που περιέχει ένα στοιχείο a είναι ακριβώς το σύμπλοκο

$$Ua = \{xa : x \in U\}.$$

Αφού προφανώς $|Ua| = |U|$, διαπιστώνουμε ότι η G διασπάται σε κλάσεις ισοδυναμίας, όλες πληθάριθμου $|U|$, άρα ο $|U|$ διαιρεί τον $|G|$. □

Στην ειδική περίπτωση όπου η U είναι κυκλική υποομάδα $\{a, a^2, \ldots, a^m\}$ συμπεραίνουμε ότι ο m (ο μικρότερος θετικός ακέραιος για τον οποίο $a^m = 1$, που λέγεται *τάξη* του a) διαιρεί το πλήθος των στοιχείων $|G|$ της ομάδας. Ειδικότερα, έχουμε ότι $a^{|G|} = 1$.



Σκαλοπάτια πάνω από τη συνάρτηση $f(t) = \frac{1}{t}$

που διαιρεί τον $2^p - 1$, οπότε έχουμε ότι $2^p \equiv 1 \pmod q$. Αφού ο p είναι πρώτος, αυτό σημαίνει ότι το στοιχείο 2 έχει τάξη p στην πολλαπλασιαστική ομάδα $\mathbb{Z}_q \backslash \{0\}$ του σώματος $\mathbb{Z}_q$. Αυτή η ομάδα έχει $q-1$ στοιχεία. Από το θεώρημα του Lagrange (βλ. πλαίσιο) γνωρίζουμε ότι η τάξη κάθε στοιχείου διαιρεί το πλήθος των στοιχείων της ομάδας, δηλαδή έχουμε ότι $p \,|\, q-1$, άρα και $p < q$. □

Ας δούμε στη συνέχεια μια απόδειξη που χρησιμοποιεί στοιχειώδη απειροστικό λογισμό.

■ **Τέταρτη Απόδειξη.** Έστω $\pi(x) := \#\{p \le x : p \in \mathbb{P}\}$ το πλήθος των πρώτων αριθμών οι οποίοι είναι μικρότεροι από ή ίσοι με τον πραγματικό αριθμό x. Αριθμούμε τους πρώτους $\mathbb{P} = \{p_1, p_2, p_3, \ldots\}$ κατά αύξουσα διάταξη. Θεωρούμε επίσης τον φυσικό λογάριθμο $\log x$, που ορίζεται από την $\log x = \int_1^x \frac{1}{t}\,dt$. Τώρα, συγκρίνουμε το εμβαδόν του χωρίου κάτω από το γράφημα της $f(t) = \frac{1}{t}$ με το αντίστοιχο εμβαδόν του χωρίου κάτω από μια μεγαλύτερη κλιμακωτή συνάρτηση. (Σχετικά με αυτή τη μέθοδο, βλ. επίσης το παράρτημα στη σελ. 12.) Για $n \le x < n+1$ έχουμε ότι

$$\begin{aligned} \log x &\le 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{n} \\ &\le \sum \frac{1}{m}, \text{ όπου το άθροισμα περιλαμβάνει όλους τους } m \in \mathbb{N} \text{ που έχουν μόνο πρώτους διαιρέτες } p \le x. \end{aligned}$$

Αφού κάθε τέτοιος m γράφεται *μονοσήμαντα* ως γινόμενο της μορφής $\prod_{p \le x} p^{k_p}$, βλέπουμε ότι το τελευταίο άθροισμα ισούται με

$$\prod_{\substack{p \in \mathbb{P} \\ p \le x}} \Big(\sum_{k \ge 0} \frac{1}{p^k} \Big).$$

Το εσωτερικό άθροισμα είναι γεωμετρική σειρά με λόγο $\frac{1}{p}$, και άρα

$$\log x \;\le\; \prod_{\substack{p \in \mathbb{P} \\ p \le x}} \frac{1}{1 - \frac{1}{p}} \;=\; \prod_{\substack{p \in \mathbb{P} \\ p \le x}} \frac{p}{p-1} \;=\; \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}.$$

Είναι όμως προφανές ότι $p_k \ge k+1$, άρα

$$\frac{p_k}{p_k - 1} \;=\; 1 + \frac{1}{p_k - 1} \;\le\; 1 + \frac{1}{k} \;=\; \frac{k+1}{k},$$

απ' όπου έπεται ότι

$$\log x \;\le\; \prod_{k=1}^{\pi(x)} \frac{k+1}{k} \;=\; \pi(x) + 1.$$

Όλοι γνωρίζουμε ότι η $\log x$ δεν είναι φραγμένη, άρα συμπεραίνουμε ότι ούτε η $\pi(x)$ είναι φραγμένη, και επομένως υπάρχουν άπειροι πρώτοι αριθμοί. □

■ **Πέμπτη Απόδειξη.** Μετά από την Ανάλυση σειρά έχει η Τοπολογία! Θεωρούμε την ακόλουθη περίεργη τοπολογία στο σύνολο $\mathbb{Z}$ των ακεραίων. Για $a, b \in \mathbb{Z}$, $b > 0$, θέτουμε

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

Καθένα από τα σύνολα $N_{a,b}$ είναι μια αμφίπλευρα άπειρη αριθμητική πρόοδος. Ονομάζουμε ένα σύνολο $O \subseteq \mathbb{Z}$ *ανοικτό* αν είτε το O είναι το κενό σύνολο είτε για κάθε $a \in O$ υπάρχει $b > 0$ τέτοιο ώστε $N_{a,b} \subseteq O$. Είναι φανερό ότι κάθε

ένωση ανοικτών συνόλων είναι πάλι ανοικτό σύνολο. Αν τα O_1, O_2 είναι ανοικτά, και για κάποιο $a \in O_1 \cap O_2$ έχουμε ότι $N_{a,b_1} \subseteq O_1$ και $N_{a,b_2} \subseteq O_2$, τότε $a \in N_{a,b_1 b_2} \subseteq O_1 \cap O_2$. Συμπεραίνουμε λοιπόν ότι κάθε πεπερασμένη τομή ανοικτών συνόλων είναι ανοικτό σύνολο. Άρα, αυτή η οικογένεια ανοικτών συνόλων επάγει πραγματικά μια τοπολογία στο $\mathbb{Z}$. Θα χρησιμοποιήσουμε δύο παρατηρήσεις:

(A) Κάθε μη κενό ανοικτό σύνολο είναι άπειρο.

(B) Επίσης, καθένα από τα σύνολα $N_{a,b}$ είναι κλειστό.

«Πετώντας επίπεδα βότσαλα, επ' άπειρον»

Η πρώτη παρατήρηση έπεται από τον ορισμό. Για τη δεύτερη, έχουμε ότι

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

πράγμα που δείχνει ότι το $N_{a,b}$ είναι συμπλήρωμα ενός ανοικτού συνόλου, άρα κλειστό.

Οι πρώτοι δεν έχουν εμφανιστεί στο κάδρο μέχρι στιγμής – εμφανίζονται όμως τώρα. Αφού κάθε ακέραιος $n \neq 1, -1$ έχει κάποιον πρώτο διαιρέτη p, και άρα περιέχεται στο $N_{0,p}$, συμπεραίνουμε ότι

$$\mathbb{Z} \setminus \{1, -1\} \;=\; \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

Τώρα, αν το $\mathbb{P}$ ήταν πεπερασμένο, τότε το σύνολο $\bigcup_{p\in\mathbb{P}} N_{0,p}$ θα ήταν πεπερασμένη ένωση κλειστών συνόλων (βάσει του (B)), δηλαδή κλειστό σύνολο. Θα είχαμε τότε ότι το $\{1, -1\}$ είναι ανοικτό σύνολο, κάτι που έρχεται σε αντίφαση με το (A). □

■ **Έκτη Απόδειξη.** Η τελευταία μας απόδειξη πηγαίνει ένα σημαντικό βήμα παραπέρα, αφού εξασφαλίζει όχι μόνο ότι υπάρχουν άπειροι πρώτοι αριθμοί, αλλά και ότι η σειρά $\sum_{p\in\mathbb{P}} \frac{1}{p}$ αποκλίνει. Η πρώτη απόδειξη αυτού του σημαντικού αποτελέσματος δόθηκε από τον Euler (και είναι καθ' εαυτή ενδιαφέρουσα), αλλά η απόδειξη που δίνουμε εδώ, η οποία είναι επινόηση του Erdős, είναι ιδιαίτερα γοητευτική.

Έστω $p_1, p_2, p_3, \ldots$ η ακολουθία των πρώτων αριθμών κατά αύξουσα διάταξη, και ας υποθέσουμε ότι η σειρά $\sum_{p\in\mathbb{P}} \frac{1}{p}$ συγκλίνει. Τότε, θα πρέπει να υπάρχει φυσικός αριθμός k τέτοιος ώστε $\sum_{i\geq k+1} \frac{1}{p_i} < \frac{1}{2}$. Στο υπόλοιπο της απόδειξης θα αποκαλούμε τους $p_1, \ldots, p_k$ *μικρούς* πρώτους, και τους $p_{k+1}, p_{k+2}, \ldots$ *μεγάλους* πρώτους. Για κάθε φυσικό αριθμό N έχουμε λοιπόν ότι

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

Έστω N_b το πλήθος των θετικών ακεραίων $n \leq N$ οι οποίοι διαιρούνται από τουλάχιστον έναν μεγάλο πρώτο, και N_s το πλήθος των θετικών ακεραίων $n \leq N$ οι οποίοι έχουν μόνο μικρούς πρώτους διαιρέτες. Θα δείξουμε ότι, για κατάλληλη επιλογή του N,

$$N_b + N_s \;<\; N,$$

απ' όπου προκύπτει η αντίφαση που ζητάμε διότι, από τον ορισμό, το άθροισμα $N_b + N_s$ θα έπρεπε να είναι ίσο με N.

Για να εκτιμήσουμε τον N_b παρατηρούμε ότι ο $\lfloor \frac{N}{p_i} \rfloor$ μετράει το πλήθος των θετικών ακεραίων $n \leq N$ που είναι πολλαπλάσια του p_i. Συνεπώς, από την (1) παίρνουμε ότι

$$N_b \;\leq\; \sum_{i\geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor \;<\; \frac{N}{2}. \tag{2}$$

Ας δούμε τώρα τον N_s. Γράφουμε κάθε $n \le N$ που έχει μόνο μικρούς πρώτους διαιρέτες στη μορφή $n = a_n b_n^2$, όπου a_n είναι το άνευ τετραγώνων μέρος του n. Κάθε a_n είναι λοιπόν το γινόμενο *διακεκριμένων* μικρών πρώτων, και συμπεραίνουμε ότι υπάρχουν ακριβώς 2^k διαφορετικά μέρη άνευ τετραγώνων. Επιπλέον, αφού $b_n \le \sqrt{n} \le \sqrt{N}$, βλέπουμε ότι υπάρχουν το πολύ $\sqrt{N}$ διαφορετικά μέρη που είναι τέλεια τετράγωνα, και επομένως

$$N_s \;\le\; 2^k\sqrt{N}.$$

Αφού η (2) ισχύει για *κάθε* N, απομένει να βρούμε έναν φυσικό αριθμό N με $2^k\sqrt{N} \le \frac{N}{2}$ ή ισοδύναμα $2^{k+1} \le \sqrt{N}$, και η συνθήκη αυτή ικανοποιείται από τον $N = 2^{2k+2}$. □

Παράρτημα: Άπειρες ακόμα αποδείξεις

Issai Schur

Η συλλογή των διαθέσιμων αποδείξεων για την απειρία των πρώτων περιέχει αρκετούς ακόμα παλιούς και νέους θησαυρούς, υπάρχει όμως μια απόδειξη πολύ πρόσφατης εσοδείας που είναι αρκετά διαφορετική και αξίζει ειδική μνεία. Η ιδέα είναι να βρούμε ακολουθίες S ακεραίων με την ιδιότητα ότι το σύνολο των πρώτων $\mathbb{P}_S$ που είναι διαιρέτες όρων της S είναι άπειρο. Κάθε τέτοια ακολουθία θα έδινε τη δική της απόδειξη για την απειρία των πρώτων. Οι αριθμοί Fermat F_n που μελετήσαμε στη δεύτερη απόδειξη σχηματίζουν μια τέτοια ακολουθία, ενώ οι δυνάμεις του 2 όχι. Πολύ περισσότερα παραδείγματα μας δίνει ένα θεώρημα του Issai Schur, ο οποίος το 1912 έδειξε ότι για κάθε μη σταθερό πολυώνυμο $p(x)$ με ακέραιους συντελεστές, το σύνολο όλων των μη μηδενικών τιμών $\{p(n) \neq 0 : n \in \mathbb{N}\}$ είναι μια τέτοια ακολουθία. Αν εφαρμόσουμε το αποτέλεσμα του Schur για το πολυώνυμο $p(x) = x$ παίρνουμε το θεώρημα του Ευκλείδη. Ένα άλλο παράδειγμα μας δίνει το πολυώνυμο $p(x) = x^2 + 1$: η ακολουθία των «τετραγώνων συν ένα» περιέχει άπειρους το πλήθος διαφορετικούς πρώτους παράγοντες.

Το επόμενο αποτέλεσμα, που οφείλεται στον Christian Elsholtz, είναι ένα πραγματικό διαμάντι: Γενικεύει το θεώρημα του Schur, η απόδειξή του χρησιμοποιεί ουσιαστικά μόνο έξυπνο μέτρημα, και κατά μία έννοια είναι βέλτιστο.

Έστω $S = (s_1, s_2, s_3, \dots)$ μια ακολουθία ακεραίων. Λέμε ότι

- η S είναι *σχεδόν 1-1* αν κάθε τιμή εμφανίζεται το πολύ c φορές για κάποια σταθερά c,
- η S έχει *υποεκθετική αυξητικότητα* αν $|s_n| \le 2^{2^{f(n)}}$ για κάθε n, όπου $f\colon \mathbb{N} \to \mathbb{R}_+$ είναι μια συνάρτηση τέτοια ώστε $\frac{f(n)}{\log_2 n} \to 0$.

Στη θέση του 2 θα μπορούσαμε να πάρουμε οποιαδήποτε βάση μεγαλύτερη από 1. Παραδείγματος χάριν, η $|s_n| \le e^{e^{f(n)}}$ οδηγεί στην ίδια κλάση ακολουθιών.

Θεώρημα. *Αν η ακολουθία $S = (s_1, s_2, s_3, \dots)$ είναι σχεδόν 1-1 και έχει υποεκθετική αυξητικότητα, τότε το σύνολο $\mathbb{P}_S$ των πρώτων αριθμών που διαιρούν κάποιο μέλος της S είναι άπειρο.*

■ **Απόδειξη.** Μπορούμε να υποθέσουμε ότι η ακολουθία $f(n)$ είναι μονότονα αύξουσα. Διαφορετικά, αντικαθιστούμε την $f(n)$ με την $F(n) = \max_{i \le n} f(i)$. Τότε μπορούμε εύκολα να επιβεβαιώσουμε ότι με αυτήν την $F(n)$ η ακολουθία S ικανοποιεί και πάλι τη συνθήκη της υποεκθετικής αυξητικότητας.

Υποθέτουμε, αντίθετα από το αποδεικτέο, ότι το σύνολο $\mathbb{P}_S = \{p_1, \dots, p_k\}$ είναι πεπερασμένο. Για $n \in \mathbb{N}$, θέτουμε

$$s_n = \varepsilon_n p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad \text{με } \varepsilon_n \in \{1, 0, -1\},\ \alpha_i \ge 0,$$

όπου οι $\alpha_i = \alpha_i(n)$ εξαρτώνται από το n. (Στην περίπτωση $s_n = 0$ μπορούμε να θέσουμε $\alpha_i = 0$ για κάθε i.) Τότε

$$2^{\alpha_1 + \cdots + \alpha_k} \le |s_n| \le 2^{2^{f(n)}} \quad \text{για } s_n \neq 0,$$

και συνεπώς, παίρνοντας λογαρίθμους με βάση 2 έχουμε ότι

$$0 \le \alpha_i \le \alpha_1 + \cdots + \alpha_k \le 2^{f(n)} \quad \text{για } 1 \le i \le k.$$

Έπεται ότι υπάρχουν το πολύ $2^{f(n)}+1$ διαφορετικές τιμές που μπορεί να πάρει καθένας από τους $\alpha_i = \alpha_i(n)$. Αφού η f είναι μονότονη, αυτό μας δίνει μια πρώτη εκτίμηση

$$\#\{\text{διακεκριμένοι } |s_n| \neq 0 \text{ για } n \le N\} \ \le \ (2^{f(N)}+1)^k \ \le \ 2^{(f(N)+1)k}.$$

Από την άλλη πλευρά, αφού η S είναι σχεδόν 1-1, μόνο c όροι της ακολουθίας μπορούν να είναι ίσοι με 0, και κάθε μη μηδενική απόλυτη τιμή μπορεί να εμφανιστεί το πολύ $2c$ φορές, οπότε προκύπτει το κάτω φράγμα

$$\#\{\text{διακεκριμένων } |s_n| \neq 0 \text{ για } n \le N\} \ \ge \ \frac{N-c}{2c}.$$

Συνδυάζοντας τα παραπάνω, βλέπουμε ότι

$$\frac{N-c}{2c} \ \le \ 2^{k(f(N)+1)}.$$

Παίρνοντας και πάλι λογαρίθμους με βάση 2 στα δύο μέλη, έχουμε ότι

$$\log_2(N-c) - \log_2(2c) \ \le \ k\,(f(N)+1) \quad \text{για κάθε } N.$$

Αυτό, όμως, δεν μπορεί να ισχύει όταν ο N είναι μεγάλος, διότι οι k και c είναι σταθερές, άρα ο λόγος $\frac{\log_2(N-c)}{\log_2 N}$ τείνει στο 1 καθώς το $N \to \infty$, ενώ ο λόγος $\frac{f(N)}{\log_2 N}$ τείνει στο 0. □

Μπορούμε να χαλαρώσουμε τις συνθήκες; Σίγουρα, καμία από αυτές δεν είναι περιττή.

Το ότι χρειαζόμαστε τη συνθήκη του «σχεδόν 1-1» γίνεται εμφανές αν θεωρήσουμε ακολουθίες S όπως οι $(2,2,2,\dots)$ και $(1,2,2,4,4,4,4,8,\dots)$, οι οποίες ικανοποιούν τη συνθήκη αυξητικότητας, όμως το $\mathbb{P}_S = \{2\}$ είναι πεπερασμένο.

Όσον αφορά τη συνθήκη υποεκθετικής αυξητικότητας, σημειώνουμε ότι δεν μπορούμε να την εξασθενίσουμε σε μια συνθήκη της μορφής $\frac{f(n)}{\log_2 n} \le \varepsilon$ για κάποιο σταθερό $\varepsilon > 0$. Για να το αντιληφθούμε αυτό, αναλύουμε την ακολουθία όλων των αριθμών της μορφής $p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ τους οποίους θεωρούμε σε αύξουσα διάταξη, όπου $p_1,\dots,p_k$ είναι δεδομένοι πρώτοι και ο k είναι μεγάλος. Αυτή η ακολουθία S αυξάνεται περίπου σαν την $2^{2^{f(n)}}$ με $\frac{f(n)}{\log_2 n} \approx \frac{1}{k}$, ενώ το $\mathbb{P}_S$ είναι πεπερασμένο εκ κατασκευής.

Βιβλιογραφία

[1] B. Artmann: *Euclid — The Creation of Mathematics,* Springer-Verlag, Νέα Υόρκη 1999.

[2] C. Elsholtz: *Prime divisors of thin sequences,* Amer. Math. Monthly **119** (2012), 331-333.

[3] P. Erdős: *Über die Reihe* $\sum \frac{1}{p}$*,* Mathematica, Zutphen B **7** (1938), 1-2.

[4] L. Euler: *Introductio in Analysin Infinitorum,* Tomus Primus, Lausanne 1748· Opera Omnia, Ser. 1, Vol. 8.

[5] H. Fürstenberg: *On the infinitude of primes,* Amer. Math. Monthly **62** (1955), 353.

[6] I. Schur: *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen,* Sitzungsberichte der Berliner Math. Gesellschaft **11** (1912), 40-50.

Το αίτημα του Bertrand

Κεφάλαιο 2

Έχουμε δει ότι η ακολουθία των πρώτων αριθμών $2,3,5,7,\ldots$ είναι άπειρη. Για να αντιληφθούμε ότι το μέγεθος των χασμάτων που υπάρχουν σε αυτή δεν είναι φραγμένο, θεωρούμε το γινόμενο $N := 2\cdot 3\cdot 5\cdots p$ όλων των πρώτων που είναι μικρότεροι από $k+2$, και παρατηρούμε ότι κανένας από τους k αριθμούς

$$N+2, N+3, N+4, \ldots, N+k, N+(k+1)$$

δεν είναι πρώτος, αφού για κάθε $2 \le i \le k+1$ γνωρίζουμε ότι ο i έχει έναν πρώτο παράγοντα που είναι μικρότερος από $k+2$, και αυτός ο παράγοντας διαιρεί επίσης τον N, άρα και τον $N+i$. Με αυτή τη συνταγή, βλέπουμε για παράδειγμα για $k=10$ ότι κανένας από τους δέκα διαδοχικούς αριθμούς

$$2312, 2313, 2314, \ldots, 2321$$

δεν είναι πρώτος.

Υπάρχουν όμως επίσης άνω φράγματα για τα χάσματα στην ακολουθία των πρώτων αριθμών. Ένα διάσημο φράγμα ορίζει ότι «το χάσμα μέχρι τον επόμενο πρώτο δεν μπορεί να είναι μεγαλύτερο από τον αριθμό από τον οποίο ξεκινάμε την αναζήτηση.» Αυτή η πρόταση είναι γνωστή ως το αίτημα του Bertrand, διότι διατυπώθηκε ως εικασία και επιβεβαιώθηκε εμπειρικά για $n < 3\,000\,000$ από τον Joseph Bertrand. Αποδείχθηκε για πρώτη φορά για όλους τους n από τον Pafnuty Chebyshev το 1850. Μια πολύ απλούστερη απόδειξη δόθηκε από τον ιδιοφυή Ινδό Ramanujan. Η Απόδειξη του Βιβλίου που θα παρουσιάσουμε οφείλεται στον Paul Erdős: περιλαμβάνεται στο πρώτο δημοσιευμένο άρθρο του Erdős, το οποίο εμφανίστηκε το 1932, όταν ο Erdős ήταν 19 ετών.

Joseph Bertrand

Το αίτημα του Bertrand
Για κάθε $n \ge 1$, υπάρχει κάποιος πρώτος p τέτοιος ώστε $n < p \le 2n$.

Beweis eines Satzes von Tschebyschef.

Von P. Erdős in Budapest.

Für den zuerst von Tschebyschef bewiesenen Satz, laut dessen es zwischen einer natürlichen Zahl und ihrer zweifachen stets wenigstens eine Primzahl gibt, liegen in der Literatur mehrere Beweise vor. Als einfachsten kann man ohne Zweifel den Beweis von Ramanujan[1]) bezeichnen. In seinem Werk *Vorlesungen über Zahlentheorie* (Leipzig, 1927), Band I, S. 66—68 gibt Herr Landau einen besonders einfachen Beweis für einen Satz über die Anzahl der Primzahlen unter einer gegebenen Grenze, aus welchem unmittelbar folgt, daß für ein geeignetes q zwischen einer natürlichen Zahl und ihrer q-fachen stets eine Primzahl liegt. Für die augenblicklichen Zwecken des Herrn Landau kommt es nicht auf die numerische Bestimmung der im Beweis auftretenden Konstanten an; man überzeugt sich aber durch eine numerische Verfolgung des Beweises leicht, daß q jedenfalls größer als 2 ausfällt.

In den folgenden Zeilen werde ich zeigen, daß man durch eine Verschärfung der dem Landauschen Beweis zugrunde liegenden Ideen zu einem Beweis des oben erwähnten Tschebyschefschen Satzes gelangen kann, der — wie mir scheint — an Einfachheit nicht hinter dem Ramanujanschen Beweis steht. Griechische Buchstaben sollen im Folgenden durchwegs positive, lateinische Buchstaben natürliche Zahlen bezeichnen; die Bezeichnung p ist für Primzahlen vorbehalten.

1. Der Binomialkoeffizient

$$\binom{2a}{a} = \frac{(2a)!}{(a!)^2}$$

[1]) Siehe Ramanujan, A Proof of Bertrand's Postulate. *Journal of the Indian Mathematical Society*, 11 (1919), S. 181—182 — *Collected Papers of* Srinivasa Ramanujan (Cambridge, 1927), S. 208—209.

■ **Απόδειξη.** Θα εκτιμήσουμε το μέγεθος του διωνυμικού συντελεστή $\binom{2n}{n}$ αρκετά προσεκτικά ώστε να συμπεράνουμε ότι αν δεν είχε κανέναν πρώτο παράγοντα στο διάστημα $n < p \le 2n$, τότε θα ήταν «πολύ μικρός». Το σκεπτικό που παρουσιάζουμε αποτελείται από πέντε βήματα.

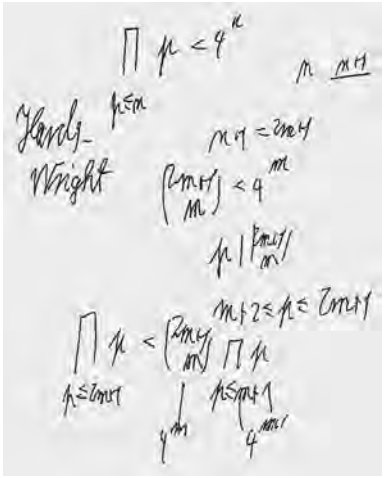
(1) Αρχικά αποδεικνύουμε το αίτημα του Bertrand για $n \le 511$. Για τον σκοπό αυτό δεν είναι απαραίτητο να ελέγξουμε 511 περιπτώσεις: αρκεί (αυτό είναι το «τέχνασμα του Landau») να ελέγξουμε ότι η

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 521$$

είναι μια πεπερασμένη ακολουθία πρώτων αριθμών, με την ιδιότητα ότι κάθε όρος της είναι μικρότερος από το διπλάσιο του προηγούμενου. Συνεπώς, κάθε διάστημα $\{y : n < y \le 2n\}$, με $n \le 511$, περιέχει κάποιον από αυτούς τους 11 πρώτους.

(2) Στη συνέχεια αποδεικνύουμε ότι

$$\prod_{p \le x} p \;\le\; 4^{x-1} \qquad \text{για κάθε πραγματικό } x \ge 2, \tag{1}$$



όπου ο συμβολισμός μας –εδώ και στη συνέχεια– σημαίνει ότι το γινόμενο εκτείνεται σε όλους τους *πρώτους* αριθμούς $p \le x$. Η απόδειξη που δίνουμε γι' αυτή τη σχέση χρησιμοποιεί επαγωγή ως προς το πλήθος αυτών των πρώτων. Δεν προέρχεται από το αρχικό άρθρο του Erdős, οφείλεται όμως κι αυτή στον Erdős (βλ. την εικόνα στο περιθώριο), και είναι πραγματικά μια Απόδειξη για το Βιβλίο. Κατ' αρχάς παρατηρούμε ότι αν q είναι ο μεγαλύτερος πρώτος που ικανοποιεί την $q \le x$, τότε

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

Αρκεί λοιπόν να ελέγξουμε την (1) για την περίπτωση που ο $x = q$ είναι πρώτος αριθμός. Για $q = 2$ παίρνουμε ότι «$2 \le 4$», οπότε προχωράμε θεωρώντας περιττούς πρώτους $q = 2m+1$. (Εδώ μπορούμε να υποθέσουμε, λόγω επαγωγής, ότι η (1) ισχύει για όλους τους ακεραίους x που ανήκουν στο σύνολο $\{2, 3, \ldots, 2m\}$.) Για $q = 2m+1$ χωρίζουμε το γινόμενο και υπολογίζουμε:

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

Όλα τα βήματα αυτού του «υπολογισμού της μιας γραμμής» έχουν απλή αιτιολόγηση. Πράγματι, η ανισότητα

$$\prod_{p\le m+1} p \;\le\; 4^m$$

ισχύει από την επαγωγική υπόθεση. Η ανισότητα

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

προκύπτει από την παρατήρηση ότι ο $\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$ είναι ακέραιος, και ότι οι πρώτοι που θεωρούμε είναι όλοι διαιρέτες του αριθμητή $(2m+1)!$, αλλά όχι του παρονομαστή $m!(m+1)!$. Τέλος, η ανισότητα

$$\binom{2m+1}{m} \;\le\; 2^{2m}$$

ισχύει διότι οι

$$\binom{2m+1}{m} \quad \text{και} \quad \binom{2m+1}{m+1}$$

είναι δύο (ίσοι!) προσθετέοι που εμφανίζονται στο

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

(3) Από το θεώρημα του Legendre (βλ. πλαίσιο) συμπεραίνουμε ότι ο $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ περιέχει τον πρώτο παράγοντα p ακριβώς

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

φορές. Σε αυτό το άθροισμα, κάθε προσθετέος είναι το πολύ ίσος με 1, διότι ικανοποιεί την

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

και είναι ακέραιος. Επιπλέον, οι προσθετέοι μηδενίζονται όταν $p^k > 2n$.

Το θεώρημα του Legendre

Ο αριθμός $n!$ περιέχει τον πρώτο παράγοντα p ακριβώς

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

φορές.

■ **Απόδειξη.** Ακριβώς $\lfloor \frac{n}{p} \rfloor$ από τους παράγοντες του γινομένου $n! = 1 \cdot 2 \cdot 3 \cdots n$ διαιρούνται με τον p, και αυτό μας δίνει $\lfloor \frac{n}{p} \rfloor$ p-παράγοντες. Κατόπιν, $\lfloor \frac{n}{p^2} \rfloor$ από τους παράγοντες του γινομένου $n!$ διαιρούνται με τον p^2, και αυτό μας δίνει τους επόμενους $\lfloor \frac{n}{p^2} \rfloor$ πρώτους παράγοντες p του $n!$, κ.λπ. □

Άρα, ο $\binom{2n}{n}$ περιέχει τον 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. Συνεπώς, η μεγαλύτερη δύναμη του p που διαιρεί τον $\binom{2n}{n}$ είναι το πολύ ίση με $2n$. Ειδικότερα, οι πρώτοι $p > \sqrt{2n}$ εμφανίζονται το πολύ μία φορά στην ανάλυση του $\binom{2n}{n}$.

Επιπλέον –και αυτό, σύμφωνα με τον Erdős, είναι το πιο σημαντικό στοιχείο της απόδειξής του– οι πρώτοι αριθμοί p που ικανοποιούν την $\frac{2}{3}n < p \leq n$ δεν διαιρούν τον $\binom{2n}{n}$ καθόλου! Πράγματι, αν $3p > 2n$ τότε έπεται (για $n \geq 3$, άρα και $p \geq 3$) ότι ο p και ο $2p$ είναι τα μόνα πολλαπλάσια του p που εμφανίζονται ως παράγοντες στον αριθμητή του $\frac{(2n)!}{n!n!}$, ενώ έχουμε δύο p-παράγοντες στον παρονομαστή.

Παραδείγματα όπως τα
$\binom{26}{13} = 2^3\cdot 5^2\cdot 7\cdot 17\cdot 19\cdot 23$
$\binom{28}{14} = 2^3\cdot 3^3\cdot 5^2\cdot 17\cdot 19\cdot 23$
$\binom{30}{15} = 2^4\cdot 3^2\cdot 5\cdot 17\cdot 19\cdot 23\cdot 29$
δείχνουν ότι «πολύ μικροί» πρώτοι παράγοντες $p < \sqrt{2n}$ μπορούν να εμφανίζονται υψωμένοι σε δυνάμεις στον $\binom{2n}{n}$, «μικροί» πρώτοι παράγοντες με $\sqrt{2n} < p \leq \frac{2}{3}n$ εμφανίζονται το πολύ μία φορά, ενώ παράγοντες στο διάστημα $\frac{2}{3}n < p \leq n$ δεν εμφανίζονται καθόλου.

(4) Είμαστε πλέον έτοιμοι να εκτιμήσουμε τον $\binom{2n}{n}$, αξιοποιώντας μια πρόταση του Raimund Seidel, η οποία βελτιώνει το αρχικό σκεπτικό του Erdős με κομψό τρόπο. Για $n \geq 3$, χρησιμοποιώντας μια εκτίμηση από τη σελίδα 14 για το κάτω φράγμα, παίρνουμε

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

Τώρα, υπάρχουν το πολύ $\sqrt{2n}$ πρώτοι στο πρώτο γινόμενο. Άρα, χρησιμοποιώντας την (1) για το δεύτερο γινόμενο και συμβολίζοντας με $P(n)$ το πλήθος των πρώτων που βρίσκονται μεταξύ του n και του $2n$ παίρνουμε ότι

$$\frac{4^n}{2n} \;<\; \left((2n)^{\sqrt{2n}}\right)\cdot\left(4^{\frac{2}{3}n}\right)\cdot(2n)^{P(n)},$$

δηλαδή,

$$4^{\frac{n}{3}} \;<\; (2n)^{\sqrt{2n}+1+P(n)}. \tag{2}$$

(5) Παίρνοντας τον λογάριθμο με βάση 2, γράφουμε την τελευταία ανισότητα στη μορφή

$$P(n) \;>\; \frac{2n}{3\log_2(2n)} - (\sqrt{2n}+1). \tag{3}$$

Μένει να επαληθεύσουμε ότι το δεξιό μέλος της (3) είναι θετικό αν ο n είναι αρκετά μεγάλος. Θα δείξουμε ότι αυτό ισχύει αν $n = 2^9 = 512$ (μάλιστα, ισχύει από τον $n = 468$ και πέρα). Γράφοντας $2n-1 = (\sqrt{2n}-1)(\sqrt{2n}+1)$ και απαλείφοντας τον παράγοντα $\sqrt{2n}+1$ βλέπουμε ότι αρκεί να δείξουμε ότι

$$\sqrt{2n}-1 \;>\; 3\log_2(2n) \qquad \text{για } n \geq 2^9. \tag{4}$$

Για $n = 2^9$, η (4) γίνεται $31 > 30$, και συγκρίνοντας τις παραγώγους $(\sqrt{x}-1)' = \frac{1}{2}\frac{1}{\sqrt{x}}$ και $(3\log_2 x)' = \frac{3}{\log 2}\frac{1}{x}$ βλέπουμε ότι η $\sqrt{x}-1$ αυξάνεται ταχύτερα από την $3\log_2 x$ για $x > (\frac{6}{\log 2})^2 \approx 75$, άρα σίγουρα και για $x \geq 2^{10} = 1024$. □

Από αυτού του είδους τις εκτιμήσεις μπορούμε να συμπεράνουμε ακόμα περισσότερα: Συγκρίνοντας τις παραγώγους των δύο μελών, παίρνουμε αντί της (4) την ισχυρότερη ανισότητα

$$\sqrt{2n}-1 \;\geq\; \frac{21}{4}\log_2(2n) \quad \text{για } \; n \geq 2^{11},$$

από την οποία με λίγες πράξεις και με χρήση της (3) έπεται ότι

$$P(n) \;\geq\; \frac{2}{7}\frac{n}{\log_2(2n)}.$$

Αυτή δεν είναι και τόσο κακή εκτίμηση: το «πραγματικό» πλήθος των πρώτων σε αυτό το διάστημα είναι περίπου ίσο με $n/\log n$. Αυτό προκύπτει από το «θεώρημα των πρώτων αριθμών», σύμφωνα με το οποίο το όριο

$$\lim_{n\to\infty} \frac{\#\{p \le n : p \text{ is prime}\}}{n/\log n}$$

υπάρχει, και είναι ίσο με 1. Αυτό το φημισμένο αποτέλεσμα αποδείχθηκε αρχικά από τον Hadamard και τον de la Vallée-Poussin το 1896. Οι Selberg και Erdős βρήκαν μια στοιχειώδη απόδειξη (χωρίς εργαλεία από τη μιγαδική ανάλυση, αλλά και πάλι μακροσκελή και πολύπλοκη) το 1948.

Όσον αφορά το ίδιο το θεώρημα των πρώτων αριθμών, φαίνεται ότι δεν έχει ακόμα ειπωθεί η τελευταία λέξη: για παράδειγμα, από μια απόδειξη της υπόθεσης του Riemann (βλ. σελ. 61), ενός από τα σημαντικότερα αναπάντητα ανοικτά ερωτήματα στα μαθηματικά, θα προέκυπτε μια ουσιαστική βελτίωση των εκτιμήσεων που δίνει το θεώρημα των πρώτων αριθμών. Αλλά και όσον αφορά το αίτημα του Bertrand θα περίμενε κανείς δραστική βελτίωση. Μάλιστα, ένα πολύ γνωστό ανοικτό πρόβλημα είναι το εξής:

> *Είναι σωστό ότι υπάρχει πάντα κάποιος πρώτος ανάμεσα στους n^2 και $(n+1)^2$;*

Για περισσότερες πληροφορίες βλ. [3, σελ. 19] και [4, σελ. 248, 257].

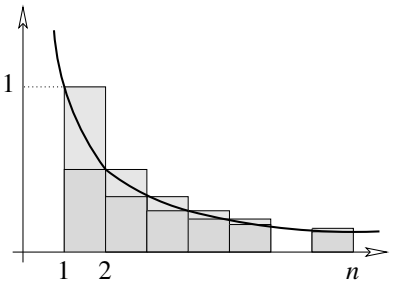
Παράρτημα: Κάποιες εκτιμήσεις

Εκτιμήσεις μέσω ολοκληρωμάτων

Υπάρχει μια πολύ απλή αλλά αποτελεσματική μέθοδος για να εκτιμήσουμε αθροίσματα με τη βοήθεια ολοκληρωμάτων (κάτι που έχουμε ήδη συναντήσει στη σελ. 4). Για να εκτιμήσουμε τους *αρμονικούς αριθμούς*

$$H_n \;=\; \sum_{k=1}^{n} \frac{1}{k}$$

σχεδιάζουμε το σχήμα στο περιθώριο, από το οποίο βλέπουμε ότι



$$H_n - 1 \;=\; \sum_{k=2}^{n} \frac{1}{k} \;<\; \int_1^n \frac{1}{t}\,dt \;=\; \log n$$

συγκρίνοντας το εμβαδόν του χωρίου κάτω από το γράφημα της $f(t) = \frac{1}{t}$ $(1 \le t \le n)$ με το άθροισμα των εμβαδών των έντονα σκιασμένων ορθογωνίων, και ότι

$$H_n - \frac{1}{n} \;=\; \sum_{k=1}^{n-1} \frac{1}{k} \;>\; \int_1^n \frac{1}{t}\,dt \;=\; \log n$$

συγκρίνοντας με το άθροισμα των εμβαδών των μεγάλων ορθογωνίων (στα οποία συμπεριλαμβάνουμε τα πιο αμυδρά σκιασμένα μέρη). Συνδυάζοντας τα παραπάνω, συμπεραίνουμε ότι

$$\log n + \frac{1}{n} \;<\; H_n \;<\; \log n \;+\; 1.$$

Ειδικότερα, έχουμε ότι $\lim_{n\to\infty} H_n \to \infty$, και ο ρυθμός αύξησης της H_n δίνεται από την $\lim_{n\to\infty} \frac{H_n}{\log n} = 1$. Υπάρχουν όμως πολύ καλύτερες γνωστές εκτιμήσεις (βλ. [2]), όπως

$$H_n \;=\; \log n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} + O\left(\frac{1}{n^6}\right),$$

όπου $\gamma \approx 0{,}5772$ είναι η «σταθερά του Euler».

Εδώ, με $O\left(\frac{1}{n^6}\right)$ συμβολίζουμε μια συνάρτηση $f(n)$ για την οποία ισχύει ότι $f(n) \le c\frac{1}{n^6}$ για κάποια σταθερά c.

Εκτιμήσεις για τα παραγοντικά – Ο τύπος του Stirling

Εφαρμόζοντας την ίδια μέθοδο για τον

$$\log(n!) \;=\; \log 2+\log 3+\cdots+\log n \;=\; \sum_{k=2}^{n}\log k$$

παίρνουμε

$$\log((n-1)!) \;<\; \int_1^n \log t\,dt \;<\; \log(n!),$$

όπου το ολοκλήρωμα υπολογίζεται εύκολα:

$$\int_1^n \log t\,dt \;=\; \Big[t\log t-t\Big]_1^n \;=\; n\log n-n+1.$$

Έτσι, έχουμε ένα κάτω φράγμα για τον $n!$

$$n! \;>\; e^{n\log n-n+1} \;=\; e\Big(\frac{n}{e}\Big)^n$$

και ταυτόχρονα ένα άνω φράγμα

$$n! \;=\; n\,(n-1)! \;<\; ne^{n\log n-n+1} \;=\; en\Big(\frac{n}{e}\Big)^n.$$

Χρειάζεται πιο λεπτομερής ανάλυση για να πάρουμε την ακριβή ασυμπτωτική συμπεριφορά του $n!$, η οποία δίνεται από τον *τύπο του Stirling*

$$n! \;\sim\; \sqrt{2\pi n}\Big(\frac{n}{e}\Big)^n.$$

Εδώ $f(n)\sim g(n)$ σημαίνει ότι $\lim\limits_{n\to\infty}\dfrac{f(n)}{g(n)}=1$.

Και πάλι, υπάρχουν ακόμα πιο ακριβείς εκτιμήσεις, όπως η

$$n! \;=\; \sqrt{2\pi n}\Big(\frac{n}{e}\Big)^n\left(1+\frac{1}{12n}+\frac{1}{288n^2}-\frac{139}{51840n^3}+O\left(\frac{1}{n^4}\right)\right).$$

Εκτιμήσεις για τους διωνυμικούς συντελεστές

Από το γεγονός ότι ο διωνυμικός συντελεστής $\binom{n}{k}$ ισούται με το πλήθος των k-υποσυνόλων ενός n-συνόλου, γνωρίζουμε ότι η ακολουθία $\binom{n}{0},\binom{n}{1},\ldots,\binom{n}{n}$ των διωνυμικών συντελεστών

- έχει άθροισμα $\sum\limits_{k=0}^{n}\binom{n}{k}=2^n$,
- είναι συμμετρική: $\binom{n}{k}=\binom{n}{n-k}$.

Από την ταυτότητα $\binom{n}{k}=\frac{n-k+1}{k}\binom{n}{k-1}$ προκύπτει εύκολα ότι για κάθε n οι διωνυμικοί συντελεστές $\binom{n}{k}$ σχηματίζουν μια ακολουθία που είναι συμμετρική και *μονότροπη*: είναι αύξουσα μέχρι το μέσον, οπότε οι μεσαίοι διωνυμικοί συντελεστές είναι οι μεγαλύτεροι στην ακολουθία:

$$1=\tbinom{n}{0}<\tbinom{n}{1}<\cdots<\tbinom{n}{\lfloor n/2\rfloor}=\tbinom{n}{\lceil n/2\rceil}>\cdots>\tbinom{n}{n-1}>\tbinom{n}{n}=1.$$

Σε αυτή τη σχέση, με $\lfloor x\rfloor$ (αντίστοιχα με $\lceil x\rceil$) συμβολίζουμε τον αριθμό x στρογγυλοποιημένο προς τα κάτω (αντίστοιχα προς τα πάνω) στον πλησιέστερο ακέραιο.

Χρησιμοποιώντας τους ασυμπτωτικούς τύπους για τα παραγοντικά τους οποίους αναφέραμε παραπάνω, μπορούμε να πάρουμε πολύ ακριβείς εκτιμήσεις για το μέγεθος των διωνυμικών συντελεστών. Σε αυτό το βιβλίο, όμως,

```
                1
              1   1
            1   2   1
          1   3   3   1
        1   4   6   4   1
      1   5   10  10  5   1
    1   6   15  20  15  6   1
  1   7   21  35  35  21  7   1
```

Τρίγωνο του Pascal

θα χρειαστούμε μόνο πολύ ασθενείς και απλές εκτιμήσεις, όπως η ακόλουθη: $\binom{n}{k} \leq 2^n$ για κάθε k, ενώ για $n \geq 2$ έχουμε ότι

$$\binom{n}{\lfloor n/2 \rfloor} \geq \frac{2^n}{n},$$

όπου η ισότητα ισχύει μόνο για $n = 2$. Ειδικότερα, για $n \geq 1$,

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

Αυτό ισχύει διότι ο $\binom{n}{\lfloor n/2 \rfloor}$, ένας από τους μεσαίους διωνυμικούς συντελεστές, είναι ο μεγαλύτερος όρος της ακολουθίας

$$\binom{n}{0} + \binom{n}{n}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1},$$

η οποία έχει άθροισμα 2^n, άρα έχει μέσο όρο ίσο με $\frac{2^n}{n}$.
Από την άλλη πλευρά, σημειώνουμε το άνω φράγμα

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \leq \frac{n^k}{k!} \leq \frac{n^k}{2^{k-1}},$$

για τους διωνυμικούς συντελεστές, που δίνει αρκετά καλή εκτίμηση για τους «μικρούς» διωνυμικούς συντελεστές στις ουρές της ακολουθίας, όταν ο n είναι μεγάλος (σε σχέση με τον k).

Βιβλιογραφία

[1] P. Erdős: *Beweis eines Satzes von Tschebyschef,* Acta Sci. Math. (Szeged) **5** (1930-32), 194-198.

[2] R. L. Graham, D. E. Knuth & O. Patashnik: *Concrete Mathematics. A Foundation for Computer Science,* Addison-Wesley, Ρέντινγκ MA 1989.

[3] G. H. Hardy & E. M. Wright: *An Introduction to the Theory of Numbers,* Πέμπτη έκδοση, Oxford University Press 1979.

[4] P. Ribenboim: *The New Book of Prime Number Records,* Springer-Verlag, Νέα Υόρκη 1989.

Οι διωνυμικοί συντελεστές δεν είναι (σχεδόν) ποτέ δυνάμεις

Κεφάλαιο 3

Υπάρχει ένας επίλογος στο αίτημα του Bertrand, ο οποίος οδηγεί σε ένα πολύ όμορφο αποτέλεσμα για τους διωνυμικούς συντελεστές. Το 1892, ο Sylvester ισχυροποίησε το αίτημα του Bertrand με τον ακόλουθο τρόπο:

> *Αν $n \geq 2k$, τουλάχιστον ένας από τους αριθμούς $n, n-1, \ldots, n-k+1$ έχει πρώτο διαιρέτη p μεγαλύτερο από k.*

Παρατηρήστε ότι για $n = 2k$ παίρνουμε ακριβώς το αίτημα του Bertrand. Το 1934 ο Erdős έδωσε μια σύντομη και στοιχειώδη απόδειξη του αποτελέσματος του Sylvester, η οποία ακολουθεί το πνεύμα της απόδειξής του για το αίτημα του Bertrand και αξίζει να συμπεριληφθεί στο Βιβλίο. Το θεώρημα του Sylvester διατυπώνεται ισοδύναμα ως εξής:

> *Ο διωνυμικός συντελεστής*
>
> $$\binom{n}{k} \;=\; \frac{n(n-1)\cdots(n-k+1)}{k!} \qquad (n \geq 2k)$$
>
> *έχει πάντα κάποιον πρώτο παράγοντα $p > k$.*

Έχοντας αυτή την παρατήρηση κατά νου, στρεφόμαστε σε ένα άλλο από τα διαμάντια του Erdős:

> *Πότε είναι ο $\binom{n}{k}$ ίσος με κάποια δύναμη m^ℓ;*

Η περίπτωση $k = \ell = 2$ μας οδηγεί σε ένα κλασικό θέμα. Πολλαπλασιάζοντας τον $\binom{n}{2} = m^2$ με 8 και αναδιατάσσοντας τους όρους καταλήγουμε στην $(2n-1)^2 - 2(2m)^2 = 1$, που είναι ειδική περίπτωση της *εξίσωσης του Pell*, $x^2 - 2y^2 = 1$. Από τη στοιχειώδη θεωρία αριθμών γνωρίζουμε ότι αυτή η εξίσωση έχει άπειρες το πλήθος θετικές λύσεις (x_k, y_k), οι οποίες προκύπτουν από την $x_k + y_k\sqrt{2} = (3+2\sqrt{2})^k$ για $k \geq 1$. Τα μικρότερα παραδείγματα είναι τα ζεύγη $(x_1, y_1) = (3,2)$, $(x_2, y_2) = (17,12)$, και $(x_3, y_3) = (99,70)$, απ' όπου βλέπουμε ότι $\binom{2}{2} = 1^2$, $\binom{9}{2} = 6^2$, και $\binom{50}{2} = 35^2$.
Για $k = 2$ και $\ell > 2$ δεν υπάρχουν άλλες λύσεις, και για $k = 3$ είναι γνωστό ότι η εξίσωση $\binom{n}{3} = m^\ell$ έχει μοναδική λύση, την $n = 50$, $m = 140$, $\ell = 2$ (βλ. το άρθρο του Győry [3]). Αυτό όμως είναι το τέλος της διαδρομής. Για $k \geq 4$ και οποιονδήποτε $\ell \geq 2$ δεν υπάρχουν λύσεις, και αυτό ακριβώς απέδειξε ο Erdős με ένα ιδιοφυές σκεπτικό.

Θεώρημα. *Η εξίσωση $\binom{n}{k} = m^\ell$ δεν έχει ακέραιες λύσεις με $\ell \geq 2$ και $4 \leq k \leq n-4$.*

■ **Απόδειξη.** Αρχικά παρατηρούμε ότι μπορούμε να υποθέσουμε ότι $n \geq 2k$, λόγω της $\binom{n}{k} = \binom{n}{n-k}$. Ας υποθέσουμε ότι το θεώρημα δεν ισχύει, δηλαδή ότι $\binom{n}{k} = m^\ell$. Η απόδειξη, με απαγωγή σε άτοπο, ακολουθεί τα εξής τέσσερα βήματα.

(1) Βάσει του θεωρήματος του Sylvester, υπάρχει πρώτος παράγοντας p του $\binom{n}{k}$ μεγαλύτερος από k, άρα ο p^ℓ διαιρεί τον $n(n-1)\cdots(n-k+1)$. Είναι εμφανές

ότι μόνο ένας από τους παράγοντες $n-i$ μπορεί να είναι πολλαπλάσιο οποιουδήποτε τέτοιου $p>k$, οπότε συμπεραίνουμε ότι $p^\ell \,|\, n-i$, και έπεται ότι

$$n \;\geq\; p^\ell \;>\; k^\ell \;\geq\; k^2.$$

(2) Θεωρούμε τυχόντα παράγοντα $n-j$ του αριθμητή και τον γράφουμε στη μορφή $n-j=a_j m_j^\ell$, όπου ο a_j δεν διαιρείται από καμία μη τετριμμένη ℓ-οστή δύναμη. Από το βήμα **(1)** βλέπουμε ότι ο a_j έχει μόνο πρώτους παράγοντες το πολύ ίσους με k. Στη συνέχεια θέλουμε να δείξουμε ότι $a_i \neq a_j$ για $i \neq j$. Ας υποθέσουμε ότι, αντιθέτως, $a_i = a_j$ για κάποιους $i<j$. Στην περίπτωση αυτή, έχουμε ότι $m_i \geq m_j+1$ και

$$\begin{aligned} k \;&>\; (n-i)-(n-j) \;=\; a_j(m_i^\ell - m_j^\ell) \;\geq\; a_j((m_j+1)^\ell - m_j^\ell) \\ &>\; a_j \ell m_j^{\ell-1} \;\geq\; \ell(a_j m_j^\ell)^{1/2} \;\geq\; \ell(n-k+1)^{1/2} \\ &\geq\; \ell(\tfrac{n}{2}+1)^{1/2} \;>\; n^{1/2}, \end{aligned}$$

το οποίο έρχεται σε αντίφαση με την ανισότητα $n>k^2$ από τα παραπάνω.

(3) Στη συνέχεια δείχνουμε ότι οι a_i είναι οι φυσικοί $1,2,\ldots,k$ με κάποια διάταξη. (Σύμφωνα με τον Erdős, αυτό το σημείο είναι η καρδιά της απόδειξης.) Δεδομένου πως ήδη γνωρίζουμε ότι είναι διακεκριμένοι, αρκεί να αποδείξουμε ότι

$$\text{ο} \quad a_0 a_1 \cdots a_{k-1} \quad \text{διαιρεί τον} \quad k!.$$

Θέτοντας $n-j=a_j m_j^\ell$ στην ισότητα $\binom{n}{k}=m^\ell$, παίρνουμε ότι

$$a_0 a_1 \cdots a_{k-1}(m_0 m_1 \cdots m_{k-1})^\ell \;=\; k! m^\ell.$$

Διαγράφοντας τους κοινούς παράγοντες των $m_0 \cdots m_{k-1}$ και m βλέπουμε ότι

$$a_0 a_1 \cdots a_{k-1} u^\ell \;=\; k! v^\ell$$

όπου $\text{μκδ}(u,v)=1$. Μένει να δείξουμε ότι $v=1$. Αν όχι, τότε ο v έχει κάποιον πρώτο διαιρέτη p. Αφού $\text{μκδ}(u,v)=1$, ο p πρέπει να είναι πρώτος διαιρέτης του $a_0 a_1 \cdots a_{k-1}$, άρα είναι μικρότερος ή ίσος του k. Από το θεώρημα του Legendre (βλ. σελ. 10) γνωρίζουμε ότι ο $k!$ διαιρείται από τον p υψωμένο στη δύναμη $\sum_{i\geq 1}\lfloor \frac{k}{p^i} \rfloor$. Στη συνέχεια θα κάνουμε μια εκτίμηση για τον εκθέτη του p στο γινόμενο $n(n-1)\cdots(n-k+1)$. Έστω i ένας θετικός ακέραιος, και έστω $b_1<b_2<\cdots<b_s$ εκείνοι από τους $n,n-1,\ldots,n-k+1$ που είναι πολλαπλάσια του p^i. Τότε $b_s=b_1+(s-1)p^i$, και άρα

$$(s-1)p^i \;=\; b_s - b_1 \;\leq\; n-(n-k+1) \;=\; k-1,$$

απ' όπου έπεται ότι

$$s \;\leq\; \left\lfloor \frac{k-1}{p^i} \right\rfloor + 1 \;\leq\; \left\lfloor \frac{k}{p^i} \right\rfloor + 1.$$

Άρα, για κάθε i το πλήθος των πολλαπλασίων του p^i μεταξύ των $n,\ldots,n-k+1$, άρα και μεταξύ των a_j, φράσσεται από την ποσότητα $\lfloor \frac{k}{p^i} \rfloor + 1$. Κατά συνέπεια, βλέπουμε ότι ο εκθέτης του p στο γινόμενο $a_0 a_1 \cdots a_{k-1}$ είναι το πολύ ίσος με

$$\sum_{i=1}^{\ell-1} \left(\left\lfloor \frac{k}{p^i} \right\rfloor + 1 \right)$$

ακολουθώντας τη συλλογιστική που χρησιμοποιήσαμε για την απόδειξη του θεωρήματος του Legendre στο Κεφάλαιο 2. Η μόνη διαφορά είναι ότι αυτή τη φορά η άθροιση σταματά στον $i=\ell-1$, διότι οι a_j δεν διαιρούνται από ℓ-οστές δυνάμεις.

Συνδυάζοντας τις δύο εκτιμήσεις, βλέπουμε ότι ο εκθέτης του p στον v^ℓ είναι το πολύ ίσος με

$$\sum_{i=1}^{\ell-1}\left(\left\lfloor\frac{k}{p^i}\right\rfloor+1\right)-\sum_{i\geq 1}\left\lfloor\frac{k}{p^i}\right\rfloor \;\leq\; \ell-1,$$

και καταλήγουμε σε αντίφαση όπως ήταν το ζητούμενο, διότι ο v^ℓ είναι ℓ-οστή δύναμη.

Αυτό είναι ήδη αρκετό για να ολοκληρωθεί η απόδειξη στην περίπτωση $\ell=2$. Πράγματι, αφού $k\geq 4$ κάποιος από τους a_i πρέπει να είναι ίσος με 4, αλλά κανένας από τους a_i δεν είναι τέλειο τετράγωνο. Υποθέτουμε λοιπόν στη συνέχεια ότι $\ell\geq 3$.

(4) Αφού $k\geq 4$, πρέπει να έχουμε $a_{i_1}=1$, $a_{i_2}=2$, $a_{i_3}=4$ για κάποιους i_1,i_2,i_3, δηλαδή,

$$n-i_1=m_1^\ell,\;\; n-i_2=2m_2^\ell,\;\; n-i_3=4m_3^\ell.$$

Ισχυριζόμαστε ότι $(n-i_2)^2\neq(n-i_1)(n-i_3)$. Αν όχι, θέτουμε $b=n-i_2$ και $n-i_1=b-x$, $n-i_3=b+y$, όπου $0<|x|,|y|<k$. Άρα,

$$b^2=(b-x)(b+y)\qquad\text{ή ισοδύναμα}\qquad (y-x)b=xy,$$

με την $x=y$ να αποκλείεται. Τώρα, από το βήμα **(1)** έχουμε ότι

$$|xy| \;=\; b|y-x| \;\geq\; b \;>\; n-k \;>\; (k-1)^2 \;\geq\; |xy|,$$

το οποίο είναι άτοπο.

Άρα έχουμε $m_2^2\neq m_1m_3$, όπου υποθέτουμε ότι $m_2^2>m_1m_3$ (η άλλη περίπτωση είναι ανάλογη), και προχωράμε στις τελευταίες μας διαδοχικές ανισότητες. Βρίσκουμε ότι

$$\begin{aligned}2(k-1)n &> n^2-(n-k+1)^2 > (n-i_2)^2-(n-i_1)(n-i_3)\\ &= 4[m_2^{2\ell}-(m_1m_3)^\ell] \geq 4[(m_1m_3+1)^\ell-(m_1m_3)^\ell]\\ &\geq 4\ell m_1^{\ell-1}m_3^{\ell-1}.\end{aligned}$$

Αφού $\ell\geq 3$ και $n>k^\ell\geq k^3>6k$, έπεται ότι

$$\begin{aligned}2(k-1)nm_1m_3 &> 4\ell m_1^\ell m_3^\ell = \ell(n-i_1)(n-i_3)\\ &> \ell(n-k+1)^2 > 3(n-\frac{n}{6})^2 > 2n^2.\end{aligned}$$

Δεδομένου ότι $m_i\leq n^{1/\ell}\leq n^{1/3}$ καταλήγουμε ότι

$$kn^{2/3}\;\geq\; km_1m_3\;>\;(k-1)m_1m_3\;>\;n,$$

ή, ισοδύναμα, ότι $k^3>n$. Με αυτή την αντίφαση η απόδειξη έχει ολοκληρωθεί. □

Βλέπουμε ότι η ανάλυση που έχουμε κάνει μέχρι τώρα συμφωνεί με την $\binom{50}{3}=140^2$, αφού

$$\begin{aligned}50 &= 2\cdot 5^2\\ 49 &= 1\cdot 7^2\\ 48 &= 3\cdot 4^2\end{aligned}$$

και $5\cdot 7\cdot 4=140$.

Βιβλιογραφία

[1] P. Erdős: *A theorem of Sylvester and Schur,* J. London Math. Soc. **9** (1934), 282-288.

[2] P. Erdős: *On a diophantine equation,* J. London Math. Soc. **26** (1951), 176-178.

[3] K. Győry: *On the diophantine equation* $\binom{n}{k}=x^l$, Acta Arithmetica **80** (1997), 289-295.

[4] J. J. Sylvester: *On arithmetical series,* Messenger of Math. **21** (1892), 1-19, 87-120· Collected Mathematical Papers Vol. 4, 1912, 687-731.

Αναπαριστώντας τους αριθμούς ως αθροίσματα δύο τετραγώνων

Κεφάλαιο 4

Ποιοι αριθμοί μπορούν να γραφτούν ως αθροίσματα δύο τετραγώνων;

Το ερώτημα αυτό είναι εξίσου παλιό με τη θεωρία αριθμών, και η απάντησή του είναι ένα κλασικό αποτέλεσμα αυτού του κλάδου των μαθηματικών. Το «δύσκολο» μέρος της απόδειξης είναι να επαληθεύσει κανείς ότι κάθε πρώτος αριθμός της μορφής $4m+1$ είναι άθροισμα δύο τετραγώνων. Ο G. H. Hardy γράφει ότι αυτό το *θεώρημα των δύο τετραγώνων* του Fermat «συγκαταλέγεται, απολύτως δικαιολογημένα, στα πλέον εκλεπτυσμένα της αριθμητικής». Ωστόσο, μία από τις παρακάτω Αποδείξεις μας για το Βιβλίο είναι αρκετά πρόσφατη.

Ας ξεκινήσουμε με κάποια σχόλια για «προθέρμανση». Αρχικά, θα πρέπει να διακρίνουμε ανάμεσα στον πρώτο $p=2$, τους πρώτους της μορφής $p=4m+1$, και τους πρώτους της μορφής $p=4m+3$. Κάθε πρώτος αριθμός ανήκει σε μία ακριβώς από αυτές τις τρεις κλάσεις. Σε αυτό το σημείο παρατηρούμε (χρησιμοποιώντας μια μέθοδο «τύπου Ευκλείδη») ότι υπάρχουν άπειροι πρώτοι της μορφής $4m+3$. Πράγματι, αν το πλήθος τους ήταν πεπερασμένο, τότε θα μπορούσαμε να θεωρήσουμε τον μεγαλύτερο πρώτο αυτής της μορφής. Έστω ότι είναι ο p_k. Θέτοντας

$$N_k \;:=\; 2^2\cdot 3\cdot 5\cdots p_k - 1$$

(όπου $p_1=2$, $p_2=3$, $p_3=5$, …είναι η ακολουθία όλων των πρώτων), βλέπουμε ότι ο N_k είναι ισότιμος με $3\,(\mathrm{mod}\,4)$, άρα θα πρέπει να έχει κάποιον πρώτο παράγοντα της μορφής $4m+3$, και αυτός ο πρώτος παράγοντας είναι μεγαλύτερος από p_k – το οποίο είναι άτοπο.

Το πρώτο μας λήμμα χαρακτηρίζει τους πρώτους για τους οποίους ο -1 είναι τετράγωνο στο σώμα $\mathbb{Z}_p$ (το οποίο περιγράφεται στο πλαίσιο της επόμενης σελίδας). Μας παρέχει επίσης έναν γρήγορο τρόπο για να αποδείξουμε ότι υπάρχουν άπειροι πρώτοι της μορφής $4m+1$.

Λήμμα 1. *Για κάθε πρώτο της μορφής $p=4m+1$ η εξίσωση $s^2\equiv -1\,(\mathrm{mod}\,p)$ έχει δύο λύσεις $s\in\{1,2,\ldots,p-1\}$, για $p=2$ υπάρχει μία τέτοια λύση, ενώ για πρώτους της μορφής $p=4m+3$ η εξίσωση δεν έχει λύση.*

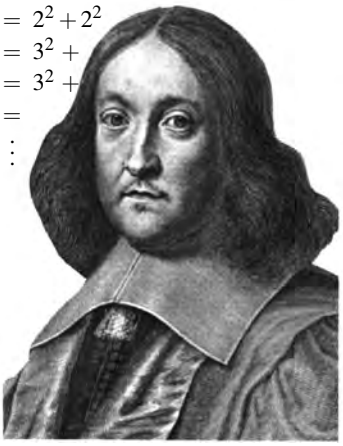
■ **Απόδειξη.** Για $p=2$ παίρνουμε $s=1$. Για περιττό p, ορίζουμε μια σχέση ισοδυναμίας στο $\{1,2,\ldots,p-1\}$ η οποία παράγεται μέσω της ταύτισης κάθε στοιχείου με το προσθετικό και με το πολλαπλασιαστικό αντίστροφό του στο $\mathbb{Z}_p$. Έτσι, οι «τυπικές» κλάσεις ισοδυναμίας θα περιέχουν τέσσερα στοιχεία

$$\{x,-x,\bar{x},-\bar{x}\}$$

αφού κάθε τέτοιο σύνολο 4 στοιχείων περιέχει και τα δύο αντίστροφα όλων των στοιχείων του. Υπάρχουν όμως μικρότερες κλάσεις ισοδυναμίας αν κάποιοι από τους τέσσερις αριθμούς συμπίπτουν:

- η σχέση $x\equiv -x$ είναι αδύνατη για περιττό p.
- η σχέση $x\equiv\bar{x}$ είναι ισοδύναμη με την $x^2\equiv 1$. Αυτή έχει δύο λύσεις, τις $x=1$ και $x=p-1$, οπότε προκύπτει η κλάση ισοδυναμίας $\{1,p-1\}$ μεγέθους 2.

$1 = 1^2+0^2$
$2 = 1^2+1^2$
$3 =$
$4 = 2^2+0^2$
$5 = 2^2+1^2$
$6 =$
$7 =$
$8 = 2^2+2^2$
$9 = 3^2+$
$10 = 3^2+$
$11 =$
$\vdots$



Pierre de Fermat

- η σχέση $x \equiv -\bar{x}$ είναι ισοδύναμη με την $x^2 \equiv -1$. Αυτή η εξίσωση μπορεί να μην έχει καμία λύση ή να έχει δύο διακεκριμένες λύσεις $x_0, p-x_0$: σε αυτή την περίπτωση η κλάση ισοδυναμίας είναι το σύνολο $\{x_0, p-x_0\}$.

Για $p = 11$ προκύπτει η διαμέριση $\{1,10\},\{2,9,6,5\},\{3,8,4,7\}$· για $p = 13$ η $\{1,12\},\{2,11,7,6\},\{3,10,9,4\}$, $\{5,8\}$: το ζεύγος $\{5,8\}$ δίνει τις δύο λύσεις της $s^2 \equiv -1 \bmod 13$.

Το σύνολο $\{1,2,\ldots,p-1\}$ έχει $p-1$ στοιχεία, και το έχουμε διαμερίσει σε τετράδες (κλάσεις ισοδυναμίας μεγέθους 4), συν ένα ή δύο ζεύγη (κλάσεις ισοδυναμίας μεγέθους 2). Για $p-1 = 4m+2$ βλέπουμε ότι υπάρχει μόνο το ζεύγος $\{1,p-1\}$, οι υπόλοιπες κλάσεις είναι τετράδες, και άρα η $s^2 \equiv -1 \pmod p$ δεν έχει λύση. Για $p-1 = 4m$ θα πρέπει να υπάρχει και το δεύτερο ζεύγος, και αυτό περιέχει τις δύο λύσεις της $s^2 \equiv -1$ που ψάχναμε. □

Σύμφωνα με το Λήμμα 1, κάθε περιττός πρώτος που διαιρεί έναν αριθμό M^2+1 θα πρέπει να είναι της μορφής $4m+1$. Έπεται ότι υπάρχουν άπειροι πρώτοι αυτής της μορφής: Διαφορετικά, θεωρούμε τον $(2\cdot 3\cdot 5\cdots q_k)^2+1$, όπου q_k είναι ο μεγαλύτερος τέτοιος πρώτος. Με σκεπτικό παρόμοιο με αυτό που χρησιμοποιήσαμε παραπάνω καταλήγουμε σε αντίφαση.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Πρόσθεση και πολλαπλασιασμός στο $\mathbb{Z}_5$

Πρωταρχικά σώματα

Αν ο p είναι πρώτος, τότε το σύνολο $\mathbb{Z}_p = \{0,1,\ldots,p-1\}$ με την πρόσθεση και τον πολλαπλασιασμό «modulo p» σχηματίζει ένα πεπερασμένο σώμα. Θα χρειαστούμε τις ακόλουθες απλές ιδιότητες:

- Για κάθε $x \in \mathbb{Z}_p$, $x \neq 0$, ο προσθετικός του αντίστροφος (τον οποίο συνήθως συμβολίζουμε με $-x$) είναι ο $p-x \in \{1,2,\ldots,p-1\}$. Αν $p > 2$, τότε οι x και $-x$ είναι διαφορετικά στοιχεία του $\mathbb{Z}_p$.
- Κάθε $x \in \mathbb{Z}_p\backslash\{0\}$ έχει μοναδικό πολλαπλασιαστικό αντίστροφο $\bar{x} \in \mathbb{Z}_p\backslash\{0\}$, με $x\bar{x} \equiv 1 \pmod p$.
  Από τον ορισμό των πρώτων έπεται ότι η απεικόνιση $\mathbb{Z}_p \to \mathbb{Z}_p$ με $z \mapsto xz$ είναι 1-1 για $x \neq 0$. Έτσι, στο πεπερασμένο σύνολο $\mathbb{Z}_p\backslash\{0\}$ θα πρέπει να είναι και επί, και άρα για κάθε x υπάρχει μοναδικό $\bar{x} \neq 0$ τέτοιο ώστε $x\bar{x} \equiv 1 \pmod p$.
- Τα τετράγωνα $0^2, 1^2, 2^2, \ldots, h^2$ ορίζουν διακεκριμένα στοιχεία του $\mathbb{Z}_p$, για $h = \lfloor \frac{p}{2} \rfloor$.
  Αυτό συμβαίνει διότι αν $x^2 \equiv y^2$, ή $(x+y)(x-y) \equiv 0$, τότε $x \equiv y$ ή $x \equiv -y$. Λέμε ότι τα $1 + \lfloor \frac{p}{2} \rfloor$ στοιχεία $0^2, 1^2, \ldots, h^2$ είναι τα *τετράγωνα* στο $\mathbb{Z}_p$.

Σε αυτό το σημείο, ας σημειώσουμε «εν παρόδω» ότι για *όλους* τους πρώτους υπάρχουν λύσεις της $x^2 + y^2 \equiv -1 \pmod p$. Πράγματι, υπάρχουν $\lfloor \frac{p}{2} \rfloor + 1$ διακεκριμένα τετράγωνα x^2 στο $\mathbb{Z}_p$, και υπάρχουν $\lfloor \frac{p}{2} \rfloor + 1$ διακεκριμένοι αριθμοί της μορφής $-(1+y^2)$. Αυτά τα δύο σύνολα αριθμών είναι πολύ μεγάλα για να είναι ξένα, αφού το $\mathbb{Z}_p$ έχει μόνο p στοιχεία, άρα θα πρέπει να υπάρχουν x και y τέτοιοι ώστε $x^2 \equiv -(1+y^2) \pmod p$.

Λήμμα 2. *Κανένας αριθμός $n = 4m+3$ δεν είναι άθροισμα δύο τετραγώνων.*

■ **Απόδειξη.** Το τετράγωνο οποιουδήποτε άρτιου αριθμού είναι $(2k)^2 = 4k^2 \equiv 0 \pmod 4$, ενώ για τα τετράγωνα των περιττών αριθμών έχουμε ότι $(2k+1)^2 = 4(k^2+k)+1 \equiv 1 \pmod 4$. Έπεται ότι κάθε άθροισμα δύο τετραγώνων είναι ισότιμο με $0, 1$ ή $2 \pmod 4$. □

Αυτό τεκμηριώνει επαρκώς για εμάς ότι οι πρώτοι $p = 4m+3$ είναι «κακοί». Προχωράμε επομένως με τις «καλές» ιδιότητες των πρώτων της μορφής $p = 4m+1$. Στην πορεία προς το κύριο θεώρημα που θα αποδείξουμε, το κρίσιμο βήμα είναι η επόμενη πρόταση.

Πρόταση. *Κάθε πρώτος της μορφής $p = 4m+1$ είναι άθροισμα δύο τετραγώνων, δηλαδή γράφεται ως $p = x^2+y^2$ για κάποιους φυσικούς αριθμούς $x, y \in \mathbb{N}$.*

Θα παρουσιάσουμε εδώ δύο αποδείξεις αυτού του αποτελέσματος – που είναι αμφότερες κομψές και αναπάντεχες. Η πρώτη απόδειξη περιλαμβάνει μια εντυπωσιακή εφαρμογή της «αρχής του περιστερώνα» (την οποία έχουμε ήδη χρησιμοποιήσει «εν παρόδω» πριν το Λήμμα 2 – βλ. Κεφάλαιο 28 για περισσότερες λεπτομέρειες), καθώς και μια έξυπνη κίνηση προς επιχειρήματα «modulo p» και πίσω. Η ιδέα οφείλεται στο Νορβηγό αριθμοθεωρητικό Axel Thue.

■ **Απόδειξη.** Θεωρούμε τα ζεύγη (x', y') ακεραίων με $0 \le x', y' \le \sqrt{p}$, δηλαδή $x', y' \in \{0, 1, \ldots, \lfloor\sqrt{p}\rfloor\}$. Υπάρχουν $(\lfloor\sqrt{p}\rfloor+1)^2$ τέτοια ζεύγη. Χρησιμοποιώντας την εκτίμηση $\lfloor x\rfloor + 1 > x$ για $x = \sqrt{p}$, βλέπουμε ότι υπάρχουν περισσότερα από p τέτοια ζεύγη ακεραίων. Έτσι, για κάθε $s \in \mathbb{Z}$, είναι αδύνατο όλες οι τιμές $x' - sy'$ που παράγονται από τα ζεύγη (x', y') να είναι διακεκριμένες modulo p. Δηλαδή, για κάθε s υπάρχουν δύο διαφορετικά ζεύγη

$$(x', y'),\ (x'', y'') \ \in\ \{0, 1, \ldots, \lfloor\sqrt{p}\rfloor\}^2$$

τέτοια ώστε $x' - sy' \equiv x'' - sy'' \pmod p$. Στη συνέχεια παίρνουμε διαφορές: Έχουμε ότι $x' - x'' \equiv s(y' - y'') \pmod p$. Συνεπώς, αν ορίσουμε $x := |x' - x''|$, $y := |y' - y''|$, βλέπουμε ότι

$$(x, y) \in \{0, 1, \ldots, \lfloor\sqrt{p}\rfloor\}^2 \quad \text{με} \quad x \equiv \pm sy \pmod p.$$

Γνωρίζουμε επίσης ότι οι x και y δεν μπορούν να είναι και οι δύο ίσοι με μηδέν, διότι τα ζεύγη (x', y') και (x'', y'') είναι διακεκριμένα.
Έστω τώρα s μια λύση της $s^2 \equiv -1 \pmod p$ (βάσει του Λήμματος 1, τέτοια λύση υπάρχει). Τότε, $x^2 \equiv s^2y^2 \equiv -y^2 \pmod p$, και έτσι έχουμε προσδιορίσει ότι

$$(x, y) \in \mathbb{Z}^2 \quad \text{με} \quad 0 < x^2 + y^2 < 2p \quad \text{και} \quad x^2 + y^2 \equiv 0 \pmod p.$$

Αλλά ο p είναι ο μόνος αριθμός ανάμεσα στους 0 και $2p$ ο οποίος διαιρείται με p. Συνεπώς $x^2 + y^2 = p$: έχουμε τελειώσει! □

Για την περίπτωση $p = 13$, $\lfloor\sqrt{p}\rfloor = 3$ θεωρούμε $x', y' \in \{0, 1, 2, 3\}$. Για $s = 5$, το άθροισμα $x' - sy' \pmod{13}$ παίρνει τις ακόλουθες τιμές:

x' \ y'	0	1	2	3
0	0	8	3	11
1	1	9	4	12
2	2	10	5	0
3	3	11	6	1

Η δεύτερη απόδειξη που θα δώσουμε για την πρόταση –η οποία είναι κι αυτή σαφώς Απόδειξη του Βιβλίου– ανακαλύφθηκε από τον Roger Heath-Brown το 1971 και εμφανίστηκε το 1984. (Μια συμπυκνωμένη «εκδοχή της μίας γραμμής» δόθηκε από τον Don Zagier.) Είναι τόσο στοιχειώδης που δεν χρειάζεται καν να χρησιμοποιήσουμε το Λήμμα 1.
Το σκεπτικό του Heath-Brown περιλαμβάνει τρεις γραμμικές ενελίξεις: μία μάλλον προφανή, μία κρυμμένη, και μία τετριμμένη η οποία δίνει το «τελικό χτύπημα». Η δεύτερη, αναπάντεχη, ενέλιξη αντιστοιχεί σε μια κρυμμένη δομή που υπάρχει στο σύνολο των ακέραιων λύσεων της εξίσωσης $4xy + z^2 = p$.

■ **Απόδειξη.** Μελετάμε το σύνολο

$$S \ := \ \{(x, y, z) \in \mathbb{Z}^3 : 4xy + z^2 = p, \quad x > 0, \quad y > 0\}.$$

Αυτό το σύνολο είναι πεπερασμένο. Πράγματι, αν $x \ge 1$ και $y \ge 1$ τότε $y \le \frac{p}{4}$ και $x \le \frac{p}{4}$. Συνεπώς, υπάρχουν μόνο πεπερασμένου πλήθους τιμές για τους x και y, και για δεδομένους x και y υπάρχουν το πολύ δύο τιμές για το z.

1. Η πρώτη γραμμική ενέλιξη ορίζεται από την

$$f : S \longrightarrow S, \quad (x, y, z) \longmapsto (y, x, -z),$$

δηλαδή, «εναλλάσσει τους x και y, και αλλάζει πρόσημο στον z». Είναι σαφές ότι απεικονίζει το S στον εαυτό του, και ότι είναι *ενέλιξη*: Αν εφαρμοστεί δύο φορές, μας δίνει την ταυτοτική απεικόνιση. Επίσης, η f δεν έχει σταθερά σημεία,

διότι αν είχαμε $z = 0$ θα παίρναμε $p = 4xy$, το οποίο είναι αδύνατο. Επιπλέον, η f απεικονίζει τις λύσεις που βρίσκονται στο

$$T \;:=\; \{(x,y,z) \in S : z > 0\}$$

στις λύσεις που βρίσκονται στο $S\backslash T$, για τις οποίες έχουμε ότι $z < 0$. Επίσης, η f αντιστρέφει τα πρόσημα του $x-y$ και του z, άρα απεικονίζει τις λύσεις που βρίσκονται στο

$$U \;:=\; \{(x,y,z) \in S : (x-y)+z > 0\}$$

στις λύσεις που βρίσκονται στο $S\backslash U$. Για να το τεκμηριώσουμε αυτό, θα πρέπει να επιβεβαιώσουμε ότι δεν υπάρχει λύση που να ικανοποιεί την $(x-y)+z = 0$, που όντως δεν υπάρχει διότι αυτό θα έδινε $p = 4xy+z^2 = 4xy+(x-y)^2 = (x+y)^2$.

Τι συμπέρασμα προκύπτει από τη μελέτη της f; Η βασική παρατήρηση είναι ότι αφού η f απεικονίζει τα σύνολα T και U στα συμπληρώματά τους, αντιμεταθέτει επίσης τα στοιχεία του $T\backslash U$ με εκείνα του $U\backslash T$. Δηλαδή, το πλήθος των λύσεων στο U οι οποίες δεν ανήκουν στο T είναι ίσο με το πλήθος των λύσεων στο T οι οποίες δεν ανήκουν στο U – *άρα, τα T και U έχουν το ίδιο πλήθος στοιχείων.*

2. Η δεύτερη ενέλιξη που μελετάμε είναι μια ενέλιξη στο σύνολο U:

$$g : U \longrightarrow U, \quad (x,y,z) \longmapsto (x-y+z, y, 2y-z).$$

Αρχικά ελέγχουμε ότι αυτή η απεικόνιση είναι πράγματι καλώς ορισμένη: Αν $(x,y,z) \in U$, τότε $x-y+z > 0, y > 0$ και $4(x-y+z)y+(2y-z)^2 = 4xy+z^2$, άρα $g(x,y,z) \in S$. Από την $(x-y+z)-y+(2y-z) = x > 0$ βλέπουμε ότι πράγματι $g(x,y,z) \in U$.

Επίσης, η g είναι ενέλιξη: το $g(x,y,z) = (x-y+z,y,2y-z)$ απεικονίζεται από την g στο $((x-y+z)-y+(2y-z), y, 2y-(2y-z)) = (x,y,z)$.

Τέλος, η g έχει ακριβώς ένα σταθερό σημείο: από την

$$(x,y,z) \;=\; g(x,y,z) \;=\; (x-y+z,y,2y-z)$$

έπεται ότι $y = z$, αλλά τότε $p = 4xy+y^2 = (4x+y)y$, που ισχύει μόνο όταν $y = z = 1$ και $x = \frac{p-1}{4}$.

Αν όμως η g είναι ενέλιξη στο U και έχει ακριβώς ένα σταθερό σημείο, τότε το *πλήθος των στοιχείων* του U *είναι περιττός αριθμός*.

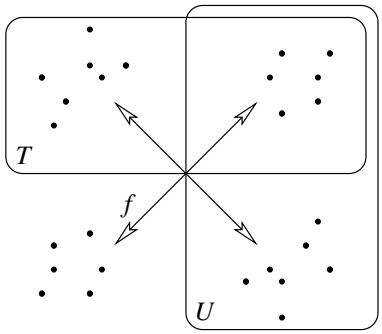
3. Η τρίτη, τετριμμένη, ενέλιξη που μελετάμε είναι η ενέλιξη στο T η οποία αντιμεταθέτει τους x και y:

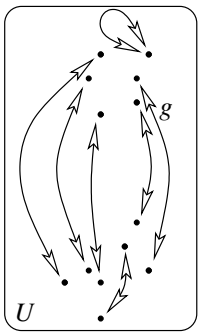
$$h : T \longrightarrow T, \quad (x,y,z) \longmapsto (y,x,z).$$

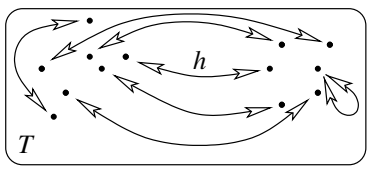
Αυτή η απεικόνιση είναι προφανώς καλώς ορισμένη, και είναι ενέλιξη. Συνδυάζουμε τώρα τα δεδομένα που έχουν προκύψει από τις δύο άλλες ενελίξεις: Το πλήθος των στοιχείων του T ισούται με το πλήθος των στοιχείων του U, που είναι περιττός αριθμός. Αν όμως h είναι μια ενέλιξη σε ένα πεπερασμένο σύνολο με περιττό πλήθος στοιχείων, τότε *έχει σταθερό σημείο*: Υπάρχει κάποιο σημείο $(x,y,z) \in T$ με $x = y$, δηλαδή, υπάρχει λύση της

$$p = 4x^2+z^2 = (2x)^2+z^2. \qquad \square$$

Ο Roger Heath-Brown συνέλαβε αυτή την απόδειξη το 1971, έχοντας μελετήσει μια επισκόπηση των άρθρων του Liouville που αφορούσαν ταυτότητες για συναρτήσεις ισοτιμίας. Η δεύτερη ενέλιξη μοιάζει μαγική, και παρουσιάστηκε χωρίς να δοθεί καμία εξήγηση για το πώς θα μπορούσε κάποιος να φτάσει σε αυτήν. Υπάρχει όμως μια γεωμετρική ερμηνεία, η οποία οπτικοποιεί και «εξηγεί» πολύ όμορφα την ενέλιξη, δίνοντας κατά κάποιον τρόπο μια «απόδειξη







Σε ένα πεπερασμένο σύνολο με περιττό πλήθος στοιχείων, κάθε ενέλιξη έχει τουλάχιστον ένα σταθερό σημείο.

χωρίς λόγια»: Θα τη συνοψίσουμε (για $p = 37$) σε ένα ολοσέλιδο σχήμα στην επόμενη σελίδα. Αυτή η εκδοχή της απόδειξης ανακαλύφθηκε, απ' ό,τι φαίνεται, από τον Alexander Spivak, έναν καθηγητή Δευτεροβάθμιας Εκπαίδευσης στη Μόσχα, ο οποίος την παρουσίασε το 2007 σε μια διάλεξη στον «Μαθηματικό Κύκλο» για μαθητές γυμνασίου και λυκείου στο Κρατικό Πανεπιστήμιο της Μόσχας.

■ **Απόδειξη.** Και πάλι, έστω ένας σταθερός πρώτος αριθμός $p = 4n+1$. Θεωρούμε το σύνολο των λύσεων

$$T = \{(x,y,z) \in \mathbb{N}^3 : 4xy + z^2 = p\}.$$

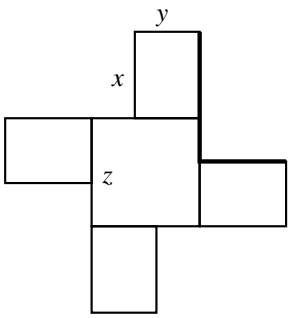
Από κάθε στοιχείο αυτού του συνόλου προκύπτει ένα *πτερυγωτό τετράγωνο*: Πρόκειται για το σχήμα που αποτελείται από ένα τετράγωνο και τέσσερα ορθογώνια στο επίπεδο και το οποίο παίρνουμε αν ξεκινήσουμε με ένα τετράγωνο με πλευρές μήκους z και επισυνάψουμε σε κάθε κορυφή ένα ορθογώνιο με μήκη πλευρών x και y κατά τρόπο συμμετρικό ως προς στροφές, έτσι ώστε η ακμή μήκους x να απομακρύνεται από το τετράγωνο, ενώ η ακμή μήκους y να κείται κατά μήκος της πλευράς του τετραγώνου.

Θεωρούμε δύο πτερυγωτά τετράγωνα «ίδια» αν είναι ομοιοθετικά. Ένας τρόπος για να επιτύχουμε μοναδικότητα, έτσι ώστε η αναπαράσταση του πτερυγωτού τετραγώνου να εξαρτάται μόνο από την καμπύλη του συνόρου του, είναι να απαιτήσουμε το σχήμα L που σχηματίζεται από τις δύο ακμές στην άνω δεξιά γωνία να έχει το ίδιο ύψος και πλάτος. Αν αυτή η συνθήκη δεν ικανοποιείται, τότε παίρνοντας ένα κατοπτρικό είδωλο (με ανάκλαση, π.χ., ως προς κατακόρυφο άξονα), μπορούμε να διορθώσουμε την κατάσταση. Έτσι, κάθε λύση στο T αντιστοιχεί σε ένα *μοναδικό* πτερυγωτό τετράγωνο που έχει εμβαδόν $4xy + z^2 = p$, και αυτή η αντιστοιχία είναι πράγματι αντιστρέψιμη: Από κάθε πτερυγωτό τετράγωνο μπορούμε να εκμαιεύσουμε μια λύση.

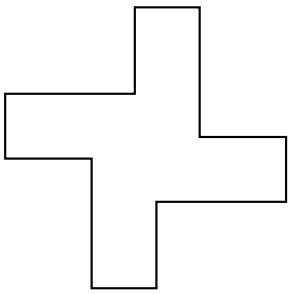
Παίρνοντας την ένωση του τετραγώνου και των τεσσάρων ορθογωνίων, για κάθε πτερυγωτό τετράγωνο παίρνουμε ένα μοναδικό, όπως θα το λέμε, *πτερυγωτό σχήμα*: Είναι ένα πολύγωνο με εμβαδόν p και τετραπλή συμμετρία, το οποίο έχει δώδεκα κορυφές: οκτώ κυρτές γωνίες με ορθή εσωτερική γωνία και τέσσερις μη κυρτές με ορθή εξωτερική γωνία. (Δεν μπορούμε να πάρουμε τετράγωνο σχήμα, διότι ο p είναι πρώτος, και άρα δεν μπορεί να είναι τετραγωνικός αριθμός.) Και πάλι θα θεωρούμε δύο πτερυγωτά σχήματα «ίδια» αν είναι ομοιοθετικά, οπότε μπορούμε να υποθέτουμε ότι το σχήμα L στην άνω δεξιά γωνία έχει ύψος τουλάχιστον όσο το πλάτος του.

Πλησιάζουμε πλέον στο καλύτερο σημείο: Για κάθε πτερυγωτό σχήμα παίρνουμε *είτε ένα είτε δύο* πτερυγωτά τετράγωνα, σχεδιάζοντας ταυτόχρονα, κατά τρόπο συμμετρικό ως προς στροφές, κατακόρυφες και οριζόντιες ευθείες προς το εσωτερικό ξεκινώντας από τις μη κυρτές γωνίες. Παίρνουμε *μία μόνο* λύση αν το σχήμα έχει τη συμμετρία ενός τετραγώνου, δηλαδή αν τα δύο μέλη των σχημάτων L έχουν το ίδιο μήκος. Αυτό συμβαίνει ακριβώς όταν $y = z$, αλλά τότε $p = 4xz + z^2 = (4x+z)z$. Υποθέτοντας ότι ο p είναι πρώτος, συμπεραίνουμε τότε ότι $z = 1$ και $x = n$. Με άλλα λόγια: Ακριβώς ένα πτερυγωτό σχήμα δίνει ένα μοναδικό πτερυγωτό τετράγωνο, ενώ τα υπόλοιπα πτερυγωτά σχήματα δίνουν από δύο πτερυγωτά τετράγωνα το καθένα. Συνεπώς, *το πλήθος $|T|$ των πτερυγωτών τετραγώνων είναι περιττό*.

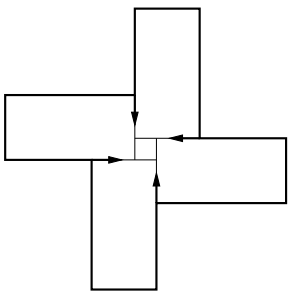
Όμως, τα πτερυγωτά τετράγωνα με μη τετραγωνικά ορθογώνια (με $x \neq y$) απαντούν σε ζεύγη, αφού μπορούμε πάντα να αναποδογυρίσουμε τα τέσσερα ορθογώνια πτερύγια από κατακόρυφο σε οριζόντιο προσανατολισμό (δηλαδή, να εναλλάξουμε τους x και y). Καθώς ο $|T|$ είναι περιττός, έπεται ότι το πλήθος των πτερυγωτών τετραγώνων που είναι τετράγωνα είναι περιττό, δηλαδή, το T



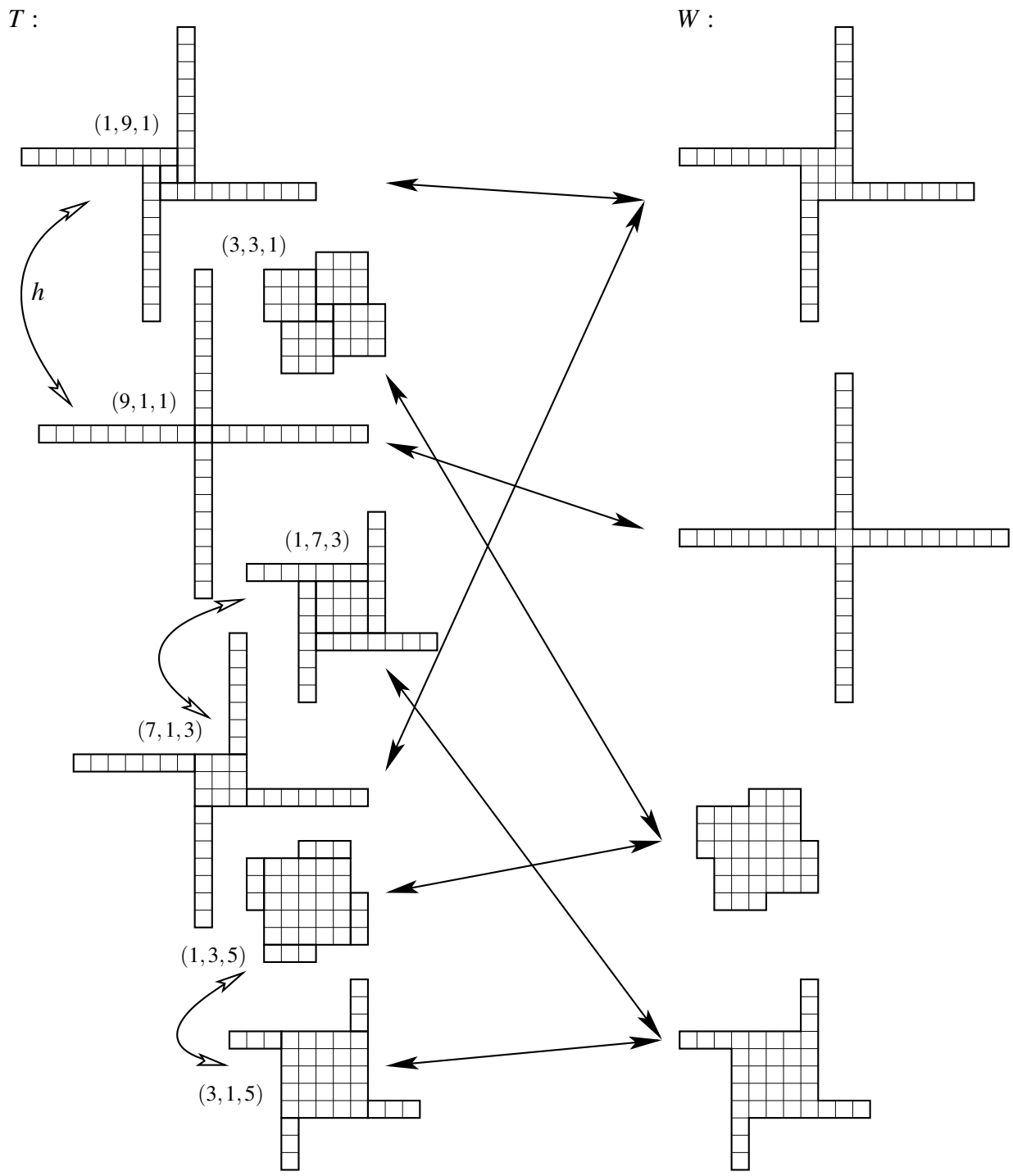
Το πτερυγωτό τετράγωνο που έχει εμβαδόν $4xy + z^2 = 73$ και αντιστοιχεί στο $(x,y,z) = (4,3,5)$, με το σχήμα L τονισμένο …



… και το αντίστοιχο πτερυγωτό σχήμα.



Το δεύτερο πτερυγωτό τετράγωνο προκύπτει από το παραπάνω πτερυγωτό σχήμα εμβαδού 73. Αναπαριστά τη λύση $(6,3,1)$.



Η απόδειξη του Spivak, για $n = 9$ και $p = 37$, όπου το σύνολο T των πτερυγωτών τετραγώνων έχει πληθάριθμο 7, ενώ το σύνολο W των πτερυγωτών σχημάτων έχει πληθάριθμο 4.

περιέχει περιττό πλήθος τριάδων (x, y, z) με $x = y$, και άρα περιέχει τουλάχιστον μία τέτοια τριάδα, και αυτή μας δίνει μια λύση της $(2x)^2 + z^2 = p$. □

Σε *κάθε* αναπαράσταση του $p = 4n + 1$ ως αθροίσματος δύο τετραγώνων, ένα από τα τετράγωνα είναι άρτιο, και το άλλο περιττό. Έτσι από την απόδειξη μέσω ενελίξεων προκύπτει και κάτι άλλο εκτός από το ότι ο p γράφεται

ως άθροισμα δύο τετραγώνων: Το πλήθος αυτών των αναπαραστάσεων στους θετικούς ακεραίους είναι *περιττό*. (Η αναπαράσταση είναι μάλιστα μοναδική, βλ. [3].) Σημειώνουμε επίσης ότι οι αποδείξεις που παρουσιάσαμε δεν είναι αποδοτικές: Προσπαθήστε να βρείτε τους x και y για έναν δεκαψήφιο πρώτο! Αποδοτικοί τρόποι για να βρεθούν τέτοιες αναπαραστάσεις εξετάζονται στα [1] και [8].

Το επόμενο θεώρημα απαντά πλήρως στο ερώτημα με το οποίο ξεκίνησε αυτό το κεφάλαιο.

Θεώρημα. *Ένας φυσικός αριθμός n μπορεί να αναπαρασταθεί ως άθροισμα δύο τετραγώνων αν και μόνο αν κάθε πρώτος παράγοντας της μορφής $p = 4m+3$ εμφανίζεται με άρτιο εκθέτη στο ανάπτυγμα του n σε γινόμενο πρώτων.*

■ **Απόδειξη.** Λέμε ότι ένας αριθμός n είναι *αναπαραστάσιμος* αν είναι άθροισμα δύο τετραγώνων, δηλαδή, αν $n = x^2 + y^2$ για κάποιους $x, y \in \mathbb{N}_0$. Το θεώρημα προκύπτει από τα ακόλουθα πέντε δεδομένα.

(1) Οι $1 = 1^2 + 0^2$ και $2 = 1^2 + 1^2$ είναι αναπαραστάσιμοι. Κάθε πρώτος της μορφής $p = 4m + 1$ είναι αναπαραστάσιμος.

(2) Το γινόμενο οποιωνδήποτε αναπαραστάσιμων αριθμών $n_1 = x_1^2 + y_1^2$ και $n_2 = x_2^2 + y_2^2$ είναι αναπαραστάσιμο: $n_1 n_2 = (x_1 x_2 + y_1 y_2)^2 + (x_1 y_2 - x_2 y_1)^2$.

(3) Αν ο n είναι αναπαραστάσιμος, $n = x^2 + y^2$, τότε και ο nz^2 είναι αναπαραστάσιμος, βάσει της $nz^2 = (xz)^2 + (yz)^2$.

Οι ισχυρισμοί (1), (2) και (3) μαζί δίνουν το σκέλος «αν» του θεωρήματος.

(4) Αν ο $p = 4m + 3$ είναι πρώτος και διαιρεί έναν αναπαραστάσιμο αριθμό $n = x^2 + y^2$, τότε ο p διαιρεί αμφότερους τους x και y, άρα ο p^2 διαιρεί τον n. Μάλιστα, αν είχαμε $x \not\equiv 0 \pmod p$, τότε θα μπορούσαμε να βρούμε $\bar{x}$ τέτοιον ώστε $x\bar{x} \equiv 1 \pmod p$, να πολλαπλασιάσουμε την εξίσωση $x^2 + y^2 \equiv 0$ με $\bar{x}^2$, και να καταλήξουμε έτσι στην $1 + y^2\bar{x}^2 = 1 + (\bar{x}y)^2 \equiv 0 \pmod p$, που σύμφωνα με το Λήμμα 1 είναι αδύνατο να ισχύει για $p = 4m + 3$.

(5) Αν ο n είναι αναπαραστάσιμος, και ο $p = 4m + 3$ διαιρεί τον n, τότε ο p^2 διαιρεί τον n, και ο n/p^2 είναι αναπαραστάσιμος. Αυτό έπεται από το (4), και ολοκληρώνει την απόδειξη. □

Κλείνουμε την ανάλυσή μας με δύο παρατηρήσεις:

- Αν a και b είναι δύο φυσικοί αριθμοί που είναι σχετικώς πρώτοι, τότε υπάρχουν άπειροι πρώτοι της μορφής $am + b$ $(m \in \mathbb{N})$ – αυτό είναι ένα φημισμένο (και δύσκολο) θεώρημα του Dirichlet. Ακριβέστερα, μπορεί κανείς να δείξει ότι το πλήθος των πρώτων $p \le x$ της μορφής $p = am + b$ περιγράφεται με μεγάλη ακρίβεια για μεγάλα x από τη συνάρτηση $\frac{1}{\varphi(a)} \frac{x}{\log x}$, όπου $\varphi(a)$ είναι το πλήθος των b με $1 \le b < a$ οι οποίοι είναι σχετικώς πρώτοι προς τον a. (Αυτό το αποτέλεσμα εκλεπτύνει σημαντικά το θεώρημα των πρώτων αριθμών, το οποίο εξετάσαμε στη σελ. 12.)
- Αυτό σημαίνει ότι οι πρώτοι για σταθερό a και μεταβλητό b εμφανίζονται με την ίδια ουσιαστικά συχνότητα. Εντούτοις, για παράδειγμα αν $a = 4$ μπορούμε να παρατηρήσουμε μια μάλλον ανεπαίσθητη, αλλά και πάλι παρατηρήσιμη και επίμονη τάση προς «περισσότερους» πρώτους της μορφής $4m + 3$. Η διαφορά ανάμεσα στις εμφανίσεις των πρώτων της μορφής $4m + 3$ και εκείνων της μορφής $4m + 1$ αλλάζει πρόσημο απείρως συχνά. Αν όμως θεωρήσουμε έναν μεγάλο τυχαίο x, τότε είναι πιθανότερο να υπάρχουν περισσότεροι πρώτοι $p \le x$ της μορφής $p = 4m + 3$ παρά της μορφής $p = 4m + 1$. Αυτό το φαινόμενο είναι γνωστό ως «μεροληψία Chebyshev» (βλ. Riesel [4] και Rubinstein και Sarnak [5].)

Βιβλιογραφία

[1] F. W. Clarke, W. N. Everitt, L. L. Littlejohn & S. J. R. Vorster: *H. J. S. Smith and the Fermat Two Squares Theorem,* Amer. Math. Monthly **106** (1999), 652-665.

[2] D. R. Heath-Brown: *Fermat's two squares theorem,* Invariant (1984), 2-5. σε μορφή LaTeX με παράρτημα ιστορικού περιεχομένου, Ιανουάριος 2008, στο eprints.maths.ox.ac.uk/677/1/invariant.pdf.

[3] I. Niven & H. S. Zuckerman: *An Introduction to the Theory of Numbers,* Πέμπτη έκδοση, Wiley, Νέα Υόρκη 1972.

[4] H. Riesel: *Prime Numbers and Computer Methods for Factorization,* Δεύτερη έκδοση, Progress in Mathematics **126**, Μπιρκχόυζερ, Βοστώνη MA 1994.

[5] M. Rubinstein & P. Sarnak: *Chebyshev's bias,* Experimental Mathematics **3** (1994), 173-197.

[6] A. Spivak: *Winged squares* [in Russian], Σημειώσεις διαλέξεων για τον μαθηματικό κύκλο στο Κρατικό Πανεπιστήμιο της Μόσχας, 15η διάλεξη 2007, mmmf.msu.ru/lect/spivak/summa_sq.pdf.

[7] A. Thue: *Et par antydninger til en taltheoretisk metode,* Kra. Vidensk. Selsk. Forh. **7** (1902), 57-75.

[8] S. Wagon: *Editor's corner: The Euclidean algorithm strikes again,* Amer. Math. Monthly **97** (1990), 125-129.

[9] D. Zagier: *A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares,* Amer. Math. Monthly **97** (1990), 144.