Butlletí de la Societat Catalana de Matemàtiques
Vol. 2, núm. 21, 2006. Pàg. 229–245

Progressions aritmètiques de nombres primers*

Martin Klazar

Resum L'any 2004 Ben Green i Terence Tao van anunciar la demostració d'un resultat fonamental conjecturat per Lagrange fa prop de dos-cents anys: els nombres primers contenen progressions aritmètiques arbitràriament llargues. Aquest article conté el context històric d'aquest resultat en les investigacions sobre els nombres primers i pretén descriure de manera entenedora les idees generals d'aquesta demostració.

Paraules clau: nombres primers, progressions aritmètiques.

Classificació MSC2000: 11.

1 Introducció

Els nombres primers contenen progressions aritmètiques arbitràriament llargues. Aquest és el títol del *preprint* [23] publicat el 8 d'abril de 2004 al servidor ArXiv [56], que descriu exactament el resultat principal:

1 Teorema (Green-Tao [23]) *Els nombres primers contenen una seqüència aritmètica de longitud k per a cada nombre natural k.*

Dit d'una altra manera, per a cada nombre natural k existeix una quantitat k de nombres primers $p_1 < p_2 < \cdots < p_k$ de manera que, $p_2 - p_1 = p_3 - p_2 = \cdots = p_k - p_{k-1}$. Per exemple, les progressions aritmètiques

$$5, 11, 17, 23, 29$$

* Aquesta és la traducció de Kepa Uharte i Oriol Serra de l'article «Prvoèísla obsahují libovolnì dlouhé aritmetické posloupnosti » [25], que va aparèixer a la revista de la Societat Matemàtica Txeca, *Pokroky Matematiky, Fyziky a Astronomie*. Els editors del Butlletí agraeixen a l'autor i a la revista el permís per publicar-ne aquesta traducció.

o

$$199, 409, 619, 829, 1.039, 1.249, 1.459, 1.669, 1.879, 2.089$$

són formades per nombres primers.

Els autors, Ben Green[1] i Terence Tao,[2] van obrir una gran escletxa a la teoria dels nombres primers i a tota la teoria de nombres. El resultat de Green i Tao va despertar immediatament una gran atenció i un gran interès. Amb aquest resultat els dos autors s'han incorporat sens dubte a la sala de la glòria de la teoria de nombres al costat de matemàtics com Dirichlet, Riemann, Vinogradov, Erdős i d'altres.

L'objectiu d'aquest article és integrar el seu resultat en un context històric (secció 3) i apropar especialment al lector els mètodes que van fer servir Green i Tao per demostrar el seu teorema sobre els nombres primers (secció 2). Com que l'article original [23] té gairebé cinquanta pàgines, en aquest article podem donar només una panorama general que es pot prendre com una guia per a l'article original. Tanmateix, donarem les formulacions exactes dels resultats tal com apareixen a [23].

La prova del teorema 1 és efectiva en el sentit que dóna una funció explícita $f\colon \mathbb{N} \to \mathbb{N}$, de manera que, per a cada k, el conjunt $\{1, 2, \ldots, f(k)\}$ dels primers $f(k)$ nombres naturals conté una progressió aritmètica de longitud k composta de nombres primers. Tao [51] indica que es pot prendre la funció

$$f(k) = 2^{2^{2^{2^{2^{2^{100k}}}}}} .$$

Amb una modificació de la prova del teorema 1, Green i Tao van aconseguir una versió més forta del resultat.

2 TEOREMA *Sigui A un subconjunt del conjunt de nombres primers amb densitat relativa superior positiva, és a dir,*

$$\limsup_{N\to\infty} \pi(N)^{-1} |A \cap ([1, N]| = c > 0 ,$$

on $\pi(N)$ denota el nombre de primers a $[1, N]$. Aleshores A conté progressions aritmètiques de llargada k per a cada enter positiu k.

Se sap que per al conjunt $Q_1 = \{p \in \mathbb{P} : \ p = 4n + 1\}$ de nombres primers el valor de la constant c al teorema 2 és $c = \frac{1}{2}$. D'altra banda, cada $p \in Q_1$ és una suma de dos quadrats ($p = a^2 + b^2$ per a dos nombres naturals a, b; vegeu la secció 3). El teorema 2 prova de manera ben curiosa el fet, fins ara desconegut, que existeixen progressions aritmètiques arbitràriament llargues creades per sumes de dos quadrats. Per exemple, $37 = 1^2 + 6^2$, $61 = 5^2 + 6^2$, $85 = 9^2 + 2^2$, $109 = 10^2 + 3^2$ és una progressió d'aquestes de llargària 4.

1 Ben Green va obtenir el seu doctorat a la Universitat de Cambridge sota la direcció de Tim Gowers i als seus vint-i-set anys és *professor* en aquesta Universitat.

2 Terence Tao va obtenir el seu doctorat a Princeton als vint-i-un anys i tres anys més tard va ser nomenat *full professor* a la Universitat de Califòrnia a Los Angeles; va obtenir la Medalla Fields en la darrera edició de l'ICM que es va fer a Madrid l'agost de 2006.

2 La prova del teorema dels nombres primers de Green i Tao

Denotem els nombres naturals $\{1,2,3,\dots\}$ amb $\mathbb{N}$, i el conjunt $\{1,2,\dots,N\}$, per $N \in \mathbb{N}$, amb $[N]$. Els símbols $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$ denoten els conjunts de nombres enters, racionals, reals i complexos respectivament. Si A és un conjunt finit, denotem per $|A|$ el nombre d'elements de A (altrament $|\cdot|$ denota el valor absolut). Per *progressió aritmètica* de longitud k a $\mathbb{N}$ s'entén el conjunt dels k nombres $\{x, x+r, x+2r, \dots, x+(k-1)r\}$ per alguns naturals x i r. Denotem amb $\mathbb{Z}_N$ l'anell dels enters mòdul N i representem els seus elements amb els nombres $\{0,1,\dots,N-1\}$.

Donada una funció real $f\colon A \to \mathbb{R}$ on A és un conjunt finit, denotem per $\mathbb{E}(f)$ el *valor mitjà* de f en A,

$$\mathbb{E}(f) = \mathbb{E}(\{f(x)\colon x \in A\}) = \frac{1}{|A|}\sum_{a\in A} f(a)\,.$$

La funció no negativa $\nu\colon \mathbb{Z}_N \to \mathbb{R}$ és una *mesura* si

$$\mathbb{E}(\nu) = 1 + o(1)\,.$$

El símbol $o(1)$ (respectivament $O(1)$) indicarà sempre una funció real $e(N)$ de la variable N, de manera que, per a $N \to \infty$, tenim $e(N) \to 0$ (respectivament, la funció $|e(N)|$ està fitada). Quan aquesta funció depèn d'altres paràmetres, generalment són indicats com a subíndex, per exemple $o_k(1)$. El símbol $O(F)$, on F és una funció de N, és l'abreviació de $O(1)F$, i de manera anàloga per a $o(F)$. El paràmetre $k \geq 3$ denotarà sempre (llevat quan parlem de k-pseudoaleatorietat) la longitud de la progressió aritmètica. Una de les característiques del punt de vista de Green i Tao consisteix a treballar sempre en un context *finit* i, per raons de simplicitat, considerar $\mathbb{Z}_N$ en lloc d'intervals de naturals $[0,N]$. Més encara, suposen sempre que N és un nombre primer prou gran, de manera que els elements de $\mathbb{Z}_N$ siguin invertibles.

L'eina clau de la prova del teorema 1 és el teorema de Szemerédi[3] [47]:

3 Teorema (Szemerédi) *Per a cada $d > 0$ real i cada $k \geq 3$ natural existeix un nombre natural $N_0 = N_0(d,k)$, de manera que per a $N \geq N_0$ qualsevol conjunt $X \subset [N]$ que verifiqui $|X| \geq dN$ conté una progressió aritmètica de longitud k.*

El teorema de Szemerédi es pot reformular de manera equivalent de la manera següent:

4 Teorema (Szemerédi) *Siguin $0 < \delta < 1$ un nombre real i $k \geq 3$ un enter. Sigui $f\colon Z_N \to \mathbb{R}$, que satisfà $0 \leq f(x) \leq 1$ per a cada $x \in \mathbb{Z}_N$ i $\mathbb{E}(f) \geq \delta$.*

3 Endre Szemerédi és un dels més cèlebres matemàtics hongaresos actuals, membre de l'Acadèmia Hongaresa de Ciències. Una de les eines que va fer servir per provar el seu teorema sobre progressions aritmètiques, l'anomenat «lema de regularitat», és avui un resultat citat en àrees tan diverses com l'anàlisi harmònica, la teoria ergòdica, la teoria de nombres o la combinatòria.

Aleshores, per a cada N prou gran, es satisfà

$$\mathbb{E}\Big(\prod_{i=0}^{k-1} f(x+ir) \mid x,r \in \mathbb{Z}_n\Big) \geq c - o_{\delta,k}(1), \tag{1}$$

on $c = c(k,\delta) > 0$ és una constant positiva que depèn només de δ i de k.

En aquest teorema l'equació (1) dóna una mesura del valor de f sobre progressions aritmètiques que proporciona immediatament el resultat del teorema 3. És aquesta versió la que van fer servir Green i Tao per provar el seu teorema. La prova està organitzada en dues etapes.

1. **El teorema relatiu de Szemerédi.** Del teorema 4 Green i Tao en deriva el que anomenen *teorema relatiu de Szemerédi*, que diu el que segueix (la formulació exacta i la definició de conjunt pseudoaleatori les donarem més endavant): *per a cada $\delta > 0$ i $k \geq 3$ existeix $N_1 = N_1(\delta,k)$ tal que, per a $N \geq N_1$ i cada conjunt k-pseudoaleatori $\widetilde{X} \subset \mathbb{Z}_N$, qualsevol subconjunt $X \subset \widetilde{X}$ que compleix $|X| \geq \delta|\widetilde{X}|$ conté una progressió aritmètica de longitud k*. Dit d'una altra manera, subconjunts densos d'una certa classe de conjunts (no necessàriament de tots els nombres naturals) tenen també la propietat de contenir progressions aritmètiques arbitràriament llargues.
2. **Realització dels nombres primers com un conjunt dens d'un conjunt pseudoaleatori.** Denotem $P = P_N \subset \mathbb{Z}_N$ el conjunt de tots els nombres primers menors que N. Green i Tao van trobar la manera d'utilitzar el pas 1 per als nombres primers. Van demostrar que per a cada $k \geq 3$ i N prou gran existeixen un conjunt k-pseudoaleatori $\widetilde{P} \subset \mathbb{Z}_n$ i una constant $\delta = \delta(k) > 0$, de manera que $\widetilde{P} \supset P$ i $|P| \geq \delta|\widetilde{P}|$.

Les dues etapes juntes permeten concloure que el conjunt de nombres primers conté progressions aritmètiques arbitràriament llargues. Vegem-ho més detalladament.

2.1 El teorema relatiu de Szemerédi

Ara formulem la generalització del teorema de Szemerédi, que és el nucli de tota la prova. Es distingeix només del teorema 4 per la incorporació de la *mesura k-pseudoaleatòria ν*, la definició de la qual donarem després de l'enunciat del teorema.

5 Teorema (teorema relatiu de Szemerédi) *Siguin $0 < \delta < 1$ un nombre real i $k \geq 3$ un enter. Siguin $\nu\colon Z_N \to \mathbb{R}^+$ una mesura k-pseudoaleatòria i $f\colon \mathbb{Z}_N \to \mathbb{R}$ una funció tal que $0 \leq f(x) \leq \nu(x)$ per a cada $x \in \mathbb{Z}_N$ i $\mathbb{E}(f) \geq \delta$. Aleshores, per a cada N prou gran es satisfà*

$$\mathbb{E}\Big(\prod_{i=0}^{k-1} f(x+ir) \mid x,r \in \mathbb{Z}_N\Big) \geq c - o_{\delta,k}(1), \tag{2}$$

on $c = c(k,\delta) > 0$ és una constant positiva que depèn només de δ i de k.

La constant c és la mateixa en ambdós teoremes i la conclusió del teorema principal es deriva una altra vegada de l'equació (2).

Què s'entén per k-pseudoaleatorietat? Aquesta noció és essencial en tota la demostració. Intuïtivament, un conjunt pseudoaleatori comparteix les propietats probabilístiques d'un conjunt purament aleatori. La definició necessària, però, es descriu en termes tècnicament molt més precisos.

6 DEFINICIÓ (k-PSEUDOALEATORIETAT) *La mesura $\nu\colon \mathbb{Z}_N \to \mathbb{R}^+$ és k-pseudoaleatòria si compleix les dues condicions següents:*

1. Condició de formes lineals. *Siguin $\psi_i(x) = \sum_{j=1}^{t} L_{ij}x_j + b_i$, $i \in [m]$, m formes lineals amb t variables, on $b_i \in \mathbb{Z}_N$, $m \leq k2^{k-1}$, $t \leq 3k-4$ i L_{ij} són nombres racionals, els numeradors i els denominadors dels quals estan fitats en valor absolut per k; interpretem L_{ij} de manera natural com a elements de $\mathbb{Z}_N$ (ja que N és un nombre primer prou gran en relació amb k). Suposem que la matriu (L_{ij}) no té files nules i que cap fila no és múltiple racional d'una altra fila. Llavors (per a cada elecció de funcions ψ_i) es satisfà:*
$$\mathbb{E}\Big(\prod_{i=1}^{m} \nu(\psi_i(x)) \mid x \in \mathbb{Z}_N^t\Big) = 1 + o_k(1)\,.$$
2. Condició de correlació. *Per a cada nombre natural m, $m \leq 2^{k-1}$, existeix una funció pes $\tau = \tau_m\colon \mathbb{Z}_N \to \mathbb{R}^+$, tots els moments de la qual estan fitats (és a dir, $\mathbb{E}(\tau^q) = O_{k,q}(1)$ per a cada $q \in \mathbb{N}$) i, per a cada m-ples de nombres (no necessàriament diferents) $h_1, \ldots, h_m \in \mathbb{Z}_N$, es satisfà:*
$$\mathbb{E}\Big(\prod_{i=1}^{m} \nu(x+h_i) \mid x \in \mathbb{Z}_N\Big) \leq \sum_{1\leq i<j\leq m} \tau(h_i - h_j)\,.$$

Adonem-nos que la definició de mesura és un cas especial de la condició de funcions lineals quan $m = 1$. A més, en la condició de correlació, tenim m funcions lineals $x + h_i$, de manera que a la matriu corresponent hi ha una sola fila amb $L_{11} = L_{21} = \cdots = L_{m1} = 1$.

2.1.1 Estructura de la prova del teorema relatiu de Szemerédi. La prova del teorema 5 fa servir tres resultats: el teorema 4 i les proposicions 7 i 8 que hi ha enunciades més endavant. Green i Tao parteixen del teorema 4, del qual no donen demostració; hi ha diverses proves d'aquest teorema: la prova original d'E. Szemerédi [47] és de naturalesa combinatòria; Furstenberg [14], [15] en va donar una fent servir teoria ergòdica i T. Gowers en va donar encara una altra recentment que involucra anàlisi de Fourier [20]; també se'n poden trobar proves a [49] i [50]. No fa gaire, i de manera independent, V. Rödl[4] i els seus estudiants (B. Nagle, M. Schacht, J. Skokan), d'una banda, i T. Gowers,[5] de l'altra,

4 Vojtech Rödl (1949) és un matemàtic txec que treballa a la Universitat Emory d'Atlanta, (EUA).

5 Timothy Gowers (1963) és professor a la Universitat de Cambridge; l'any 1998 li va ser lliurada la medalla Fields.

van trobar una nova prova combinatòria d'una generalització del teorema de Szemerédi.

Vegem els altres dos resultats que condueixen a la prova del teorema 5.

Donats $\omega \in Q_d = \{0,1\}^d$ i $h \in \mathbb{Z}_n^d$, denotem per $\omega \cdot h = \omega_1 h_1 + \cdots + \omega_d h_d$. Fixat $d \in \mathbb{N}$, per a cada funció $f\colon \mathbb{Z}_N \to \mathbb{R}$ definim l'anomenada *norma uniforme U^d de Gowers* (denominació implantada per Green i Tao) com a

$$\|f\|_{U^d} = \mathbb{E}\Big(\prod_{\omega \in Q_d} f(x + \omega \cdot h) \mid x \in \mathbb{Z}_n, h \in \mathbb{Z}_n^d \Big)^{1/2^d}.$$

No és difícil veure que aquest valor mitjà és sempre positiu, de manera que es pot aixecar a $1/2^d$ i la definició és correcta. Per exemple, $\|f\|_{U^1} = (\mathbb{E}(f)^2)^{1/2} = |\mathbb{E}(f)|$; així, doncs, $\|\cdot\|_{U^1}$ només és una seminorma (pot ser anul·lada per una funció no nul·la f). Es pot provar en canvi que $\|\cdot\|_{U^d}$ és una norma per a tot $d \geq 2$.

7 Proposició (teorema de Von Neumann generalitzat) *Sigui $\nu\colon \mathbb{Z}_N \to \mathbb{R}^+$ una mesura k-pseudoaleatòria. Siguin $f_0, f_1, \ldots, f_{k-1}\colon \mathbb{Z}_N \to \mathbb{R}$ funcions que satisfan $|f_i(x)| \leq 1 + \nu(x)$ per a cada $x \in \mathbb{Z}_N$ i cada $i = 0, \ldots, k-1$. Aleshores,*

$$\mathbb{E}\Big(\prod_{i=0}^{k-1} f_i(x + ir) \mid x, r \in \mathbb{Z}_N \Big) \leq O(\min_{0 \leq i \leq k-1} \|f_i\|_{U^{k-1}}) + o(1). \tag{3}$$

En aquesta proposició, l'equació (3) relaciona l'expressió a la dreta de (2) amb les normes uniformes de Gowers.

Una família $\mathcal{B}$ de subconjunts de $\mathbb{Z}_N$ és una *σ-àlgebra* si és tancada respecte de les operacions d'intersecció, unió i complementació i conté el conjunt buit i $\mathbb{Z}_N$. Per *àtom* de $\mathcal{B}$ entenem un conjunt mínim no buit a $\mathcal{B}$. Els àtoms constitueixen una partició de $\mathbb{Z}_N$. El valor mitjà de la funció $f\colon \mathbb{Z}_N \to \mathbb{R}$ *condicionat* a la σ-àlgebra $\mathcal{B}$ és la funció $\mathbb{E}(f \mid \mathcal{B})\colon \mathbb{Z}_N \to \mathbb{R}$ definida com a

$$\mathbb{E}(f \mid \mathcal{B})(x) = \frac{1}{|A(x)|} \sum_{y \in A(x)} f(y),$$

on $A(x)$ és l'àtom que conté x. Observem que aquesta funció és constant a cada àtom.

8 Proposició (generalització del teorema de Koopman - Von Neumann)

*Siguin $0 < \varepsilon < 1$, $\nu\colon \mathbb{Z}_N \to \mathbb{R}^+$ una mesura k-pseudoaleatòria i $f\colon \mathbb{Z}_N \to \mathbb{R}$ una funció que satisfà $0 \leq f(x) \leq \nu(x)$ per a cada $x \in \mathbb{Z}_N$. Per a N prou gran existeix una σ-*àlgebra *$\mathcal{B}$ a $\mathbb{Z}_N$ i un conjunt $\Omega \in \mathcal{B}$ tals que*

1. $\sum_{x \in \Omega} \nu(x) = o_\varepsilon(N)$;
2. $\mathbb{E}(\nu - 1 \mid \mathcal{B})(x) = o_\varepsilon(1)$ *uniformement en x a $\mathbb{Z}_N \backslash \Omega$;*

3. $\|g - \mathbb{E}(g \mid \mathcal{B})\|_{U^{k-1}} \leq \varepsilon^{1/2^k}$*, on* g *és igual a* f *en* $\mathbb{Z}_N \backslash \Omega$ *i és* 0 *a* Ω*.*

L'objectiu d'aquesta proposició és obtenir una descomposició d'una funció arbitrària en una part *uniforme* i una altra d'*antiuniforme* (llevat d'un petit error).

La prova de la proposició 7 ocupa unes quatre pàgines i fa servir la desigualtat de Cauchy-Schwarz i la k-pseudoaleatoritat de ν. La prova de la proposició 8 ocupa unes dotze pàgines i hi apareix per exemple el teorema clàssic de Weierstrass sobre l'aproximació de funcions per polinomis.

2.1.2 La prova del teorema 5. Amb l'ajuda dels tres resultats esmentats, la prova ja és fàcil (mitja pàgina) i la indiquem breument. Siguin δ, k, ν i f com en el teorema 5, i $\varepsilon > 0$ arbitrari però fixat. La proposició 8 ens proporciona aleshores una σ-àlgebra $\mathcal{B}$ i el conjunt $\Omega \in \mathcal{B}$. Posem $f = g + h$, on $g = f - \mathbb{E}(f \mid \mathcal{B})$ i $h = \mathbb{E}(f \mid \mathcal{B})$. El valor mitjà

$$S = \mathbb{E}\Big(\prod_{i=0}^{k-1} f(x + ir) \mid x, r \in \mathbb{Z}_N \Big)$$

del teorema 5 l'expressem, gràcies a la linealitat de $\mathbb{E}$, com a:

$$\begin{aligned} S &= \mathbb{E}\Big(\prod_{i=0}^{k-1} h(x + ir) \mid x, r \in \mathbb{Z}_N \Big) + \sum \mathbb{E}\Big(\prod_{i=0}^{k-1} (g \circ h)(x + ir) \mid x, r \in \mathbb{Z}_N \Big) \\ &= M + E, \end{aligned}$$

on la suma E conté tots els $2^k - 1$ sumands en els quals, en el producte, apareix la funció g almenys en un factor. Podem prescindir del conjunt excepcional Ω, d'acord amb la proposició 8. A banda d'aquest, d'acord amb la proposició 8 el valor mitjà condicionat $\mathbb{E}(\nu \mid \mathcal{B})$ es comporta més o menys com la constant 1 i, per tant, la versió del teorema 4 de Szemerédi ens dóna $M \geq c(k, \delta) - o_{k,\delta,\varepsilon}(1)$. Cadascun dels $2^k - 1$ sumands de la suma E és petit gràcies a la proposició 8 i la proposició 7, així que

$$E = O(\varepsilon^{1/2^k}) + o(1)\,.$$

Tot plegat, arribem a

$$S \geq c(k, \delta) - O_k(\varepsilon^{1/2^k}) - o_{k,\delta,\varepsilon}(1)\,.$$

Com que $\varepsilon > 0$ es pot escollir arbitràriament, la fita inferior de $\mathbb{E}(\cdot)$ al teorema 4 queda provada.

2.2 Els nombres primers com a subconjunt dens d'un conjunt pseudoaleatori

Un cop provat el teorema relatiu de Szemerédi, el segon pas consisteix a provar que els nombres primers es poden descriure com un subconjunt dens d'algun conjunt pseudoaleatori.

La funció de *Von Mangoldt* $\Lambda\colon \mathbb{N} \to \mathbb{R}$ es defineix com a

$$\Lambda(n) = \begin{cases} \log p, & \text{si } n = p^m \\ 0, & \text{altrament.} \end{cases}$$

Recordem que la funció de Möbius $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ es defineix $\mu(n) = (-1)^r$, si n és un producte de r nombres primers diferents, i $\mu(n) = 0$ altrament (però $\mu(1) = 1$). Val la identitat

$$\Lambda(n) = \sum_{d|n} \mu(d) \log(n/d),$$

que és la fórmula d'inversió de Möbius de la identitat $\log n = \sum_{d|n} \Lambda(d)$, que es dedueix de la definició de Λ. La funció d'*Euler* $\varphi\colon \mathbb{N} \to \mathbb{N}$ donada per la fórmula $\varphi(n) = n(1 - 1/p_1) \cdots (1 - 1/p_r)$, on p_i són els nombres primers que divideixen n, dóna la quantitat de nombres $m \in \mathbb{N}, m \le n$, relativament primers amb n. El símbol p denotarà sempre un nombre primer.

Del *teorema dels nombres primers* (la quantitat de nombres primers menors que x és asimptòticament $x/log x$) es dedueix que $\mathbb{E}(\Lambda(n) \mid n \in \mathbb{Z}_N) = 1 + o(1)$. Si existissin una mesura k-pseudoaleatòria ν i una constant $c = c(k) > 0$, de manera que

$$\nu(n) \ge c\Lambda(n) \tag{4}$$

per a cada $n \in \mathbb{Z}_N$, el teorema 5 implicaria immediatament el teorema de Green-Tao (ja que $\mathbb{E}(c\Lambda) = c + o(1) \ge \delta > 0$ per a un N gran, i nombres de la forma $n = p^r$ amb $r \ge 2$ es poden ometre). Una mesura ν així, però, no existeix. Per a $q \in \mathbb{N}$, la mesura ν està repartida més o menys equitativament entre q classes mòdul q, mentre que Λ està concentrada en les $\varphi(q)$ classes dels nombres relativament primers amb q. Com que $\liminf \varphi(q)/q = 0$, per a un N gran, la desigualtat (4) no es pot obtenir. L'estratègia senzilla de trobar la mesura k-pseudoaleatòria ν que satisfaci (4), doncs, no funciona.

2.2.1 La funció de Von Mangoldt modificada Green i Tao van evitar aquest problema amb l'anomenat *truc-W*. Sigui $w = w(N)$ una funció de creixement lent (n'hi ha prou, per exemple, amb $w = \log\log\log N$) i sigui

$$W = W(N) = \prod_{p \le w} p.$$

La funció Λ de Von Mangoldt *modificada* es defineix per la relació:

$$\widetilde{\Lambda}(n) = \begin{cases} \frac{\varphi(W)}{W} \log(Wn + 1) & \text{si } Wn + 1 \text{ és primer,} \\ 0 & \text{altrament.} \end{cases}$$

Adonem-nos que, si n segueix una progressió aritmètica, també ho fa $Wn + 1$. La funció Λ modificada així ja es pot fitar superiorment per una mesura k-pseudoaleatòria.

9 PROPOSICIÓ *Sigui* $\varepsilon_k = \frac{1}{2^{k(k+4)!}}$ *i* N *un nombre primer prou gran. Aleshores existeix una mesura* k*-pseudoaleatòria* $\nu\colon \mathbb{Z}_N \to \mathbb{R}^+$*, de manera que*

$$\nu(n) \geq \frac{1}{k2^{k+5}}\widetilde{\Lambda}(n)$$

val per a cada n *de l'interval* $\varepsilon_k N \leq n \leq 2\varepsilon_k N$*.*

Del teorema 5 i la proposició 9, el teorema Green-Tao ja es dedueix de manera senzilla. Al lector potser se li acudiran dos problemes tècnics:

1. La progressió aritmètica ha de ser a $\mathbb{N}$ i no a $\mathbb{Z}_N$.
   Això es resol si limitam n a l'interval $[\varepsilon_k N, 2\varepsilon_k N]$.
2. No volem progressions aritmètiques degenerades del tipus $x + ir$, $0 \leq i \leq k-1$ amb $r = 0$.
   En $\mathbb{E}(\cdot)$ al teorema 5, però, aquestes progressions hi contribueixen només en $O(\log^k N/N) = o(1)$ i no tenen cap influència.

Com es defineix la mesura ν de la proposició 9?

10 DEFINICIÓ *La funció abreujada de Von Mangoldt* $\Lambda_R(n)$*, on* $R > 0$ *és un paràmetre, és definida per la relació:*

$$\Lambda_R(n) = \sum_{d|n, d\leq R} \mu(d)\log(R/d) = \sum_{d|n} \mu(d)\log_+(R/d),$$

on $\log_+ x = \max(0, \log x)$*.*

Goldston i Yildirim[6] [17, 18, 19] van investigar la funció Λ_R en relació amb les estimacions dels intervals entre nombres primers consecutius.

11 DEFINICIÓ *Siguin* $R = N^{k^{-1}2^{-k-4}}$ *i* ε_k *definit com a la Proposició 9. Definim la funció* $\nu\colon \mathbb{Z}_N \to \mathbb{R}^+$ *amb la fórmula*

$$\nu(n) = \begin{cases} \frac{\varphi(W)}{W} \cdot \frac{1}{\log R} \cdot \Lambda_R(Wn+1)^2 & \text{per a } n \in [\varepsilon_k N, 2\varepsilon_k N], \\ 1 & \text{altrament.} \end{cases}$$

Green i Tao van provar que la funció ν definida així té la propietat característica de la proposició 9 (lema 8.4 a [23]), que és una mesura (lema 8.7 a [23]) i que és k-pseudoaleatòria (proposicions 8.8 i 8.10 a [23]).

Amb això hem acabat la visió general de la prova del teorema 1. Ara descriurem com Green i Tao van provar la k-pseudoaleatorietat de ν.

Com ells mateixos exposen, els procediments habituals basats en mètodes de sedàs (*sieve theory*), que van esforçar-se a aplicar, es van mostrar insuficients.

6 Daniel Goldston (1954) és professor a la Universitat Estatal de San José de Califòrnia, als Estats Units. Yalçin Yildirim (1961) treballa a la Universitat Bogaziçi d'Istanbul, a Turquia.

Després A. Granville els va aconsellar que intentessin utilitzar un nou mètode per estimacions de la funció Λ_R amb ajuda de la integració complexa, que D. Goldston i C. Yildirim van desenvolupar mentre investigaven la grandària de l'espai entre nombres primers consecutius. Green i Tao van trobar que el mètode Goldston-Yildirim funciona amb exactitud per assolir una expressió asimptòtica pels productes de quadrats de la funció Λ_R, que són necessaris per a la prova de la k-pseudoaleatorietat de ν.

2.2.2 La prova de la k-pseudoaleatorietat de ν amb el mètode Goldston i Yildirim.

12 Proposició (Goldston i Yildirim) *Considerem m funcions lineals $\psi_i(x) = \sum_{j=1}^{t} L_{ij}x_j + b_i$, $i \in [m]$, amb t variables, on L_{ij} i b_i són nombres complexos que compleixen $|L_{ij}| \le \frac{1}{2}w(N)^{1/2}$, la matriu (L_{ij}) no té files nul·les i cap fila no és un múltiple d'una altra. Sigui $B = I_1 \times \cdots \times I_t$, on $I_i \subset \mathbb{R}$ són t intervals, cadascun d'una llargària almenys R^{10m}. Llavors, per a una funció de creixement prou lent $w(N)$, es satisfà*

$$\mathbb{E}\Big(\prod_{i=1}^{m}\Lambda_R(W\psi_i(x)+1)^2 \mid x \in B \cap \mathbb{Z}^t\Big) = (1+o_{m,t}(1))\Big(\frac{W\log R}{\varphi(W)}\Big)^m.$$

La condició de les formes lineals per a ν (com també la propietat $\mathbb{E}(\nu) = 1 + o(1)$) s'aconsegueix amb l'aplicació de la proposició 12. En la prova de la proposició 12 el valor mitjà presentat més amunt s'expressa (llevat d'un petit error) amb l'ajuda de les integrals (des d'ara $i = \sqrt{-1}$)

$$\frac{1}{(2\pi i)^m}\int_{\Gamma_1}\cdots\int_{\Gamma_1} F(z,u)\prod_{j=1}^{m}\frac{R^{z_j+u_j}}{z_j^2u_j^2}\,dz_j\,du_j$$
$$= \frac{1}{(2\pi i)^m}\int_{\Gamma_1}\cdots\int_{\Gamma_1}\Big(\sum_{d,e\in\mathbb{N}^m}\prod_{j=1}^{m}\frac{\mu(d_j)\mu(e_j)}{d_j^{z_j}e_j^{u_j}}\prod_{p}M_{d,e}(p)\Big)\prod_{j=1}^{m}\frac{R^{z_j+u_j}}{z_j^2u_j^2}\,dz_j\,du_j,$$

on integrem $2m$ vegades en el pla complex sobre el camí $\Gamma_1 = \{\frac{1}{\log R}+i\tau\colon \tau\in\mathbb{R}\}$, $z = (z_1,\dots,z_m)$ i $u = (u_1,\dots,u_m)$ són $2m$ variables complexes, les components de $d = (d_1,\dots,d_m)$ i $e = (e_1,\dots,e_m)$ són nombres naturals i

$$M_{d,e}(p) = \frac{1}{p^t}\cdot|\{x\in\mathbb{Z}_p^t\colon\ \forall j\in[m]\ p|d_je_j \Rightarrow W\psi_j(x)+1=0\}|.$$

En aquesta igualtat es fan servir la definició de la funció Λ_R, l'intercanvi de l'ordre entre el sumatori i les integrals, i la representació integral de la funció $\log_+$ (que surt a la definició Λ_R):

$$\log_+ x = \frac{1}{2\pi i}\int_\Gamma \frac{x^z}{z^2}\,dz$$

per a cada $x > 0$ real i cada camí $\Gamma = \{\alpha + i\tau\colon \tau\in\mathbb{R}\}$, $\alpha > 0$.

Per a cada real $\sigma > 0$ denotem per $D_\sigma^m = \{(z,u) \in \mathbb{C}^{2m} \colon -\sigma < \mathrm{Re}(z_j), \mathrm{Re}(u_j) < 100,\ j \in [m]\}$. Donada una funció $G = G(z,u)$ amb $2m$ variables, holomorfa a la regió D, denotem per $V_l(G,D)$ el suprem $\sup_{z,u\in D} |\partial G(z,u)|$ quan ∂G recorre la fila l. La funció $F(z,u)$, que apareix en la integral múltiple de la proposició 12, fent servir els productes d'Euler per als nombres primers, es factoritza com a $F = G_1G_2G_3$, amb

$$G_3(z,u) = \prod_{j=1}^m \prod_p \frac{(1-p^{-1-z_j})(1-p^{-1-u_j})}{1-p^{-1-z_j-u_j}} = \prod_{j=1}^m \frac{\zeta(1+z_j+u_j)}{\zeta(1+z_j)\zeta(1+u_j)},$$

on $\zeta(s) = \prod_p (1-p^{-s})^{-1} = \sum_{n\geq 1} n^{-s}$ és la clàssica funció de Riemann. Així, G_3 és holomorfa per a $\mathrm{Re}(z_j), \mathrm{Re}(u_j) > 0$. Les funcions G_1 i G_2 són donades amb productes d'Euler més complicats, però resulta que també són funcions holomorfes una mica a l'esquerra de 0, és a dir, a $D = D_{1/6m}^m$, i compleixen $G_1(0,0) = 1 + o_m(1)$, $G_2(0,0) = (W/\varphi(W))^m$, $V_m(G_1,D) \leq O_m(1)$ i $V_m(G_2,D) \leq w(N)^{O_m(w(N))}$ (lema 9.3 a [23]). Green i Tao van calcular la integral múltiple de la proposició 12, que dóna $\mathbb{E}(\cdot)$, amb ajuda del lema següent, que també atribueixen a Goldstone i Yildrim [19].

13 LEMA *Sigui $G(z,u)$ una funció de $2m$ variables complexes que depenen del paràmetre real $N > 0$, holomorfa en $D = D_\sigma^m$ per algun $\sigma > 0$ i que satisfà l'estimació $V_m(G,D) = \exp(O_{m,\sigma}(\log^{1/3} R))$.*[7] *Llavors*

$$\begin{aligned} &\frac{1}{(2\pi i)^m} \int_{\Gamma_1} \cdots \int_{\Gamma_1} G(z,u) \prod_{j=1}^m \frac{\zeta(1+z_j+u_j)}{\zeta(1+z_j)\zeta(1+u_j)} \frac{R^{z_j+u_j}}{z_j^2 u_j^2}\, dz_j\, du_j \\ = \quad & G(0,0)\log^m R + \sum_{j=1}^m O_{m,\sigma}(V_j(G,D)\log^{m-j} R) + O_{m,\sigma}(\mathrm{e}^{-\delta\sqrt{\log R}}) \end{aligned}$$

per algun $\delta = \delta(m) > 0$.

Després l'expressió asimptòtica buscada es dedueix de l'aplicació del lema 13 a $G = G_1G_2$ i $\sigma = 1/6m$: com que $R = N^{k^{-1}2^{-k-4}}$ i $w(N)$ és de creixement prou lent, la hipòtesis del lema 13 sobre $V_m(G,D)$ es satisfà, i $G(0,0)\log^m R$ és d'un ordre més gran que la resta d'elements. La prova del lema 13 es fa per inducció sobre m i ocupa en l'apèndix del *preprint* [23] unes quatre pàgines. Fa servir residus, la deformació del camí d'integració i l'absència de zeros de la funció $\zeta(s)$ que apareix al denominador de l'integrand.[8]

3 Breu història de la investigació dels nombres primers

La gent es dedica als nombres primers ja des de l'antiguitat i el descobriment de les seves propietats és una de les branques més boniques i importants de la

7 $R = R(N)$ és funció de N. El lema es fa servir amb R com a la definició 11.

8 El setembre de 2004 Tao a [52] va donar una prova simplificada de la proposició 12, que ja no necessita les propietats de la funció $\zeta(s)$.

matemàtica. La importància pràctica dels nombres primers per a la criptografia i la transmissió d'informació, però, va ser descoberta no fa gaire, a la dècada dels setanta del segle XX. Introduïm algunes de les fites més rellevants en la història de les investigacions sobre els nombres primers. El teorema de Green-Tao sens dubte n'és una.

- Euclides al segle IV a. C. va incloure als seus *Elements* la prova que el conjunt de nombres primers no és finit ([2]).
- El 1640 Pierre de Fermat (1601–1665) va enunciar: si p és un nombre primer, llavors p divideix $n^p - n$ per a cada nombre natural n. Aquest teorema, conegut com el petit teorema de Fermat, el va demostrar Euler l'any 1736 ([10, 37]).
- Leonhardt Euler (1707–1783) també va demostrar una altra afirmació de Fermat que tot nombre primer de la forma $4n + 1$ és una suma de dos quadrats ([10]). A més, va establir la identitat $\prod_p (1 - p^{-s})^{-1} = \sum_{n\geq 1} n^{-s}$, que és vàlida per a $s > 1$, fins i tot per a $Re(s) > 1$, i va provar que la sèrie $\sum_{p\in\mathbb{P}} p^{-1}$ és divergent.
- L'any 1794 Carl Friedrich Gauss (1777–1855) va demostrar que, per a cada nombre primer p de la forma $2^{2^n} + 1$, es pot construir un polígon regular de p costats amb regle i compàs ([26, 27, 46]). L'any 1796 va trobar la prova de la llei de reciprocitat quadràtica i, potser encara abans, va deduir empíricament el teorema dels nombres primers: $\pi(x) \sim x/\log x$, o bé més exactament $\pi(x) \sim \mathrm{li}(x) = \int_2^x (dt/\log t)$ ([16]). (El símbol $\pi(x)$ tradicionalment es fa servir per denotar la quantitat de nombres primers més petits o iguals que x).
- Peter Dirichlet (1805–1859) va demostrar l'any 1837 que, per a cada dos nombres relativament primers $a, m \in \mathbb{N}$, la progressió aritmètica $\{a + im : i = 0, 1, 2, \dots\}$ conté infinits nombres primers ([8, 34, 43, 53]).
- Pafnuty Lvovich Txebixev (1824–1894) va assolir l'any 1852 una forma feble del teorema dels nombres primers: per a $x \geq 2$ i dues constants positives c_1, c_2 es satisfà $c_1 x/\log x < \pi(x) < c_2 x/\log x$ ([16, 34, 53]).
- Bernhard Riemann (1826–1866) va publicar l'any 1859 el treball revolucionari *Uber die Anzahl der Primzahlen unter einer gegebenen Grösse* [40], en el qual va esbossar el mètode de prova del teorema dels nombres primers basat en l'anàlisi complexa i on es formula la famosa hipòtesi de Riemann, un dels problemes matemàtics oberts més intrigants de l'actualitat: si $\zeta(s) = 0$ i $\mathrm{Re}(s) > 0$, llavors $\mathrm{Re}(s) = 1/2$ ([40, 9]).
- Jacques Hadamard (1865–1963) i Charles de la Vallée Poussin (1866–1962) l'any 1896 van donar independentment, fent servir mètodes d'anàlisi complexa, la primera prova del teorema del nombre primer ([9, 16, 53, 55]).
- Viggo Brun (1882–1978), poc després de la I Guerra Mundial, va crear amb treballs innovadors una nova disciplina de la teoria de nombres basada en

mètodes de sedàs. Va aconseguir demostrar, per exemple, que existeixen infinites parelles de nombres de la forma $n, n+2$ tals que tots dos tenen, pel cap alt 9 factors primers (comptats amb multiplicitat) i que la suma dels inversos dels primers bessons convergeix ([3, 22]).

- Lev Genrikhovich Šnirelman (1905–1938) va publicar l'any 1930 el teorema segons el qual hi ha una constant absoluta c tal que cada nombre natural $n \geq 2$ és la suma, a tot estirar, de c nombres primers ([48, 45, 33]).
- Ivan Matveevich Vinogradov (1891–1983) va demostrar l'any 1937 que tot nombre senar prou gran és la suma de tres nombres primers ([54, 21, 33]).
- Paul Erdős (1913–1996) i Atle Selberg (1917) van trobar l'any 1949 la prova elemental del teorema del nombre primer, és a dir, sense fer servir l'anàlisi complexa ([11, 42, 29, 34, 35]).
- Jin-run Chen (1933–1996) l'any 1966 va demostrar que existeix una quantitat infinita de nombres primers p, de manera que $p+2$ també és o bé un nombre primer o bé una suma de dos nombres primers ([4, 5, 33]).
- Yuri Matiasevitx (1947) va resoldre l'any 1970 el desè problema de Hilbert: va provar que la resolubilitat en els enters d'equacions polinòmiques a coeficients enters és un problema algorísmicament irresoluble. De la seva solució se'n dedueix que existeix un polinomi a coeficients enters $P(x_1, \ldots, x_r)$, de manera que el conjunt $\mathbb{N} \cap P(\mathbb{N}^r)$ és precisament un conjunt de nombres primers ([30, 31, 7], [32]).
- Vaughan R. Pratt (1944) va demostrar l'any 1975 que la propietat de ser un nombre primer pertany, en la teoria de la complexitat algorísmica, a la classe de problemes anomenada NP ([38, 6, 36]).
- Michael O. Rabin (1931) va donar l'any 1976 un algorisme probabilístic per decidir en temps polinomial si un nombre donat és primer ([39, 6, 28, 36]).
- Ron Rivest (1947), Adi Shamir (1952) i Len Adleman (1945) van publicar l'any 1977 un sistema criptogràfic amb una clau pública, anomenat després *sistema RSA* segons les seves inicials, basat en la dificultat de la factorització dels nombres en nombres primers ([6, 36, 41]).
- Peter Shor (1959) va donar l'any 1994 un algorisme quàntic que permet obtenir en temps polinomial la factorització de nombres naturals en nombres primers ([44, 6]).
- John Friedlander (1941) i Henryk Iwaniec (1947) van demostrar l'any 1998 que existeix una quantitat infinita de nombres primers de la forma $x^2 + y^4$, $x, y \in \mathbb{N}$ ([12] a [13]).
- Roger Heath-Brown (1952) va demostrar l'any 2001 que existeix una quantitat infinita de nombres primers de la forma $x^3 + 2y^3$, $x, y \in \mathbb{N}$ ([24]).
- Manindra Agrawal (1966), Neeraj Kayal (1979) i Nitin Saxena (1981) l'any 2002 van trobar conjuntament el primer test de primalitat determinista que s'executa en temps polinomial ([1]).

Referències

[1] Agrawal, M.; Kayal, N.; Saxena, N. «PRIMES is in P». *Ann. of Math.*, (2), 160 (2004), 2, 781–793.

[2] Bečvářová, M. *Eukleidovy Základy: Jejich vydání a překlady*. Praga: Prometheus, 2002.

[3] Brun, V. «Le crible d'Eratosthène et le théorème de Goldbach». *C. R. Acad. Sci.* [París], 168 (1919), 544–546.

[4] Chen, J. «On the representation of a large even integer as the sum of a prime and the product of at most two primes». *Kexue Tongbao*, 17 (1966), 385–386.

[5] Chen, J. «On the representation of a large even integer as the sum of a prime and the product of at most two primes». *Sci. Sinica*, 16 (1973), 157–176.

[6] Crandall, R.; Pomerance, C. *Prime numbers. A computational perspective*. Nova York: Springer-Verlag, 2001.

[7] Davis, M. «Hilbert's tenth problem is unsolvable». *Amer. Math. Monthly*, 80 (1973), 233–269.

[8] Dirichlet, P. G. L. «Beweis des Satzes, daß jede unbegrenzte aritmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält». *Abh. Akad. Berlin* (1837), 45–71.

[9] Edwards, H. M. *Riemann's zeta function*. Nova York, Londres: Academic Press, 1974.

[10] Edwards, H. M. *Fermat's last theorem: A genetic introduction to algebraic number theory*. Nova York: Springer-Verlag, 1977.

[11] Erdős, P. «On a new method in elementary number theory which leads to an elementary proof of the prime number theorem». *Proc. Nat. Acad. Sci.* [EUA], 35 (1949), 374–384.

[12] Friedlander, J.; Iwaniec, H. «Asymptotic sieve for primes». *Ann. of Math.*, (2), 148 (1998), 1041–1065.

[13] Friedlander, J.; Iwaniec, H. «The polynomial X^2+Y^4 captures its primes». *Ann. of Math.*, (2), 148 (1998), 945–1040.

[14] Furstenberg, H. «Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions». *J. Analyse Math.*, 31 (1977), 204–256.

[15] Furstenberg, H.; Katznelson, Y.; Ornstein, D. «The ergodic theoretical proof of Szemerédi's theorem». *Bull. Amer. Math. Soc.*, 7 (1982), 527–552.

[16] Goldstein L. J. «A history of the prime number theorem». *Amer. Math. Monthly*, 80 (1973), 599–615.

[17] GOLDSTON, D.; YILDIRIM, C. Y. «Higher correlations of divisor sums related to primes, I: Triple correlations». [Integers], 3 (2003), 66 p.

[18] GOLDSTON, D.; YILDIRIM, C. Y. *Higher correlations of divisor sums related to primes, III: k-correlations.* arXiv:math.NT/0209102, 32 p.

[19] GOLDSTON, D.; YILDIRIM, C. Y. *Small gaps between primes.* [Preprint]

[20] GOWERS, W. T. «A new proof of Szemerédi's theorem». *Geom. Funct. Anal.*, 11, 3 (2001), 465–588.

[21] GOWERS, W. T. *Vinogradov's three-primes theorem.* 17 p. http://www.dpmms.cam.ac.uk/~wtg10/

[22] GREAVES, G. *Sieves in number theory*. Berlín: Springer-Verlag, 2001.

[23] GREEN, B.; TAO, T. *The primes contain arbitrarily long arithmetic progressions.* arXiv:math.NT/0404188 (versió 1: 8 abril 2004; darrera actualització versió 5: 9 febrer 2006).

[24] HEATH-BROWN, D. R. «Primes represented by $x^3 + 2y^3$». *Acta Math.*, 186 (2001), 1–84.

[25] KLAZAR, M. «Prvoèísla obsahují libovolnì dlouhé aritmetické posloupnosti». *Pokroky Matematiky, Fyziky a Astronomie*, 49, 3 (2004), 177–188.

[26] KŘÍŽEK, M. *Od Fermatových prvoèísel ke geometrii.* A: ŠOLCOVÁ, A.; KŘÍSEK, M.; MINK, G. [ed.] Matematik Pierre de Fermat. *Cahiers du CEFRES č.* 28, 131–161. Praga, CEFRES, 2002.

[27] KŘÍSEK, M.; LUCA, F.; SOMER, L. *17 lectures on Fermat numbers: From number theory to geometry*. Nova York: Springer-Verlag, 2001.

[28] KUČERA, L. *Kombinatorické algoritmy*. Praga: SNTL, 1983.

[29] LEVINSON, N. «A motivated account of an elementary proof of the prime number theorem». *Amer. Math. Monthly*, 76 (1969), 225–245.

[30] MATIJASEVIČ, J. V. «Diofantovost' perečislimych množestv». *Dokl. Akad. Nauk SSSR*, 191 (1970), 279–282.

[31] MATIJASEVIČ, J. V. «Diofantovo predstavlenie množestv prostych čisel». *Dokl. Akad. Nauk SSSR*, 196 (1971), 770–773.

[32] MATIJASEVIČ, JU. V. *Hilbert's tenth problem.* Cambridge, MA: MIT Press, 1993.

[33] NATHANSON, M. B. *Additive number theory: The classical bases.* Nova York: Springer-Verlag, 1996.

[34] NATHANSON, M. B. *Elementary methods in number theory*. Nova York: Springer-Verlag, 2000.

[35] NOVÁK, B. «O elementárním dukazu prvočíselné věty ». *Časopis pro Pěstování Matematiky*, 100 (1975), 71–84.

[36] PAPADIMITRIOU, CH. H. *Computational complexity*. Reading, MA: Addison-Wesley, 1994.

[37] Porubský, Š. «Fermat a teorie čísel.» A: Šolcová, A.; Kříšek, M.; Mink, G. [ed.] Matematik Pierre de Fermat. *Cahiers du CEFRES č.* 28, 49–86. Praga, CEFRES, 2002.

[38] Pratt, V. R. «Every prime has a succinct certificate». *SIAM J. Comput.*, 4 (1975), 214–220.

[39] Rabin, M. O. «Probabilistic algorithms». A: Traub, J. F. [ed.] *Algorithms and complexity*, 21–39 [Nova York: Academic Press], 1976.

[40] Riemann, B. «Über die Anzahl der Primzahlen unter einer gegebenen Grösse». *Monatsberichte der Berliner Akademie*, 1859, 671–680.

[41] Rivest, R.; Shamir, A.; Adleman, L. «A method for obtaining digital signatures and public-key cryptosystems». *Comm. ACM*, 21 (1978), 120–126.

[42] Selberg, A. «An elementary proof of the prime-number theorem» *Ann. of Math.*, (2), 50 (1949), 305–313.

[43] Serre, J.-P. *A course in arithmetics*. Nova York: Springer-Verlag, 1973.

[44] Shor, P. «Algorithms for quantum computation: discrete logarithms and factoring». A: *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*. Los Alamitos, CA: IEEE Comput. Soc. Press, 1994, 124–134.

[45] Schnirelmann, L. «Über additive Eigenschaften von Zahlen». *Mat. Annalen*, 107 (1933), 649–690.

[46] Stillwell, J. *Elements of algebra: Geometry, numbers, equations*. Nova York: Springer-Verlag, 1994.

[47] Szemerédi, E. «On sets of integers containing no k elements in arithmetic progression». *Acta Arith.*, 27 (1975), 199–245.

[48] Šnirel'man, L. G. «Ob additivnych svojstvach čisel». *Izvestija Donskogo Politechničeskogo Instituta v Novočerkasske*, 14 (1930), 3–28.

[49] Tao, T. *A quantitative ergodic theory proof of Szemerédi's theorem.* arXiv:math.CO/0405251, 51 p.

[50] Tao, T. *A quantitative ergodic theory proof of Szemerédi's theorem (abridged)*, 20 p. http://www.math.ucla.edu/~tao/preprints/

[51] Tao, T. *A bound for progressions of length k in the primes*, 4 p. http://www.math.ucla.edu/~tao/preprints/

[52] Tao, T. *A remark on Goldston-Yildirim correlation estimates*, 8 p. http://www.math.ucla.edu/~tao/preprints/

[53] Tenenbaum, G. *Introduction to analytic and probabilistic number theory*. Cambridge, Regne Unit: Cambridge University Press, 1995.

[54] Vinogradov, I. M. «Predstavlenie nečotnogo čisla summoj trjoch prostych čisel». *Dokl. Akad. Nauk SSSR*, 15 (1937), 291–294.

[55] Zagier, D. «Newman's short proof of the prime number theorem». *Amer. Math. Monthly*, 104 (1997), 705–708.

[56] http://www.arxiv.org/

Martin Klazar
KAM, Katedra Aplikované Matematiky
Univerzita Karlova v Praze
Malostranské námestí, 25
118 00 Praha 1
klazar@kam.mff.cuni.cz