МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2012
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2012
Proceedings of the Forty First Spring Conference
of the Union of Bulgarian Mathematicians
Borovetz, April 9–12, 2012

РАЗПРЕДЕЛЕНИЕ НА ПРОСТИТЕ ЧИСЛА И НЯКОИ ПРИЛОЖЕНИЯ*

Петър Попиванов

В този доклад, предназначен за по-широка аудитория, се предлагат няколко класически и по-нови резултати от теорията на простите числа. Направен е кратък обзор върху разпределението на простите числа сред естествените $\mathbb{N}$ и се дискутират също така почти простите числа от ред 2. Полиномите с целочислени коефициенти се разглеждат във връзка с техните функционални стойности върху $\mathbb{N}$: прости или съставни числа. Най-сетне се конструират функции от експоненциален вид, изобразяващи $\mathbb{N}$ в множеството на простите числа.

1. Целта на нашето изложение е да запознае един сравнително по-широк кръг от колеги математици, и по-специално учители по математика, с някои класически, а и по-нови резултати от теорията на простите числа. Основания: простите числа са своеобразните „тухли“, изграждащи теорията на числата. Нещо повече, обогатяването на познанията в такива направления е особено полезно, защото разширява кръгозора ни както със сериозни твърдения, така и с привлекателни примери (често пъти ефектни миниатюри) печели за каузата на математиката по-голяма аудитория и разбира се, ученическата. А това е много нужно в наши дни и точно в тази посока концентрирах усилията си.

Предлаганият текст резюмира някои от най-важните и интересни въпроси, свързани с разпределението на простите числа сред естествените $\mathbb{N} = \{1, 2, 3, \dots\}$. Напомняме, че едно число $p \in \mathbb{N}$ се нарича просто, ако се дели само на 1 и на себе си. Означаваме с $P \subset \mathbb{N}$ множеството на простите числа $\{2(= p_1), 3(= p_2), 5(= p_3), 7(= p_4), 11(= p_5), 13(= p_6), \dots\}$. Още от Евклид се знае, че те са безбройно много.

Понеже всяко естествено число се разлага на произведение от прости множители, то в този смисъл простите числа представляват „тухлите“ на $\mathbb{N}$, на целите числа $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ и на рационалните числа $\mathbb{Q}$. За да направим изложението по-кратко, още сега даваме

Дефиниция 1. *Числото $n \in \mathbb{N}$ се нарича почти просто от ред $k \geq 2$, ако може да се представи като произведение на най-много k прости множителя. Значи всяко просто число е почти просто, но обратното не е вярно. С P_k означаваме множеството на почти простите числа от ред k.*

---

* **2000 Mathematics Subject Classification:** 11A41, 11B25, 11N13, 11B34, 11M26.

Ключови думи: просто число, полупространство, разпределение на простите числа, Риманова дзета функция.

2. За да формулираме закона за разпределение на простите числа, ще напомним някои свойства на знаменитата дзета-функция на Риман [12], [17]. В реалния случай тя е въведена от Ойлер през 1737 г., а в комплексния случай е изследвана от Риман около 1859-1860 г. И така, нека $s = \tau + it$. Тогава $\zeta(s) = \sum_{1}^{\infty} \frac{1}{n^s}$, $\tau > 1$.

При $\tau \leq 1$ тя се дефинира с аналитично продължение и се оказва, че е мероморфна функция в $\mathbb{C}$ с единствен прост полюс при $\tau = 1$, имащ резидуум 1. Риман открива връзка между $\zeta(s)$ и разпределението на нулите ѝ в ивицата $0 \leq \tau \leq 1$ с разпределението на простите числа. По-долу са изброени някои свойства на $\zeta(s)$:

а) $\zeta(s) \neq 0$ при $\tau > 1$;

б) $\zeta(1 + it) \neq 0$ при $t \neq 0$ (доказано от Адамар и Вале́-Пусен, 1896 г.);

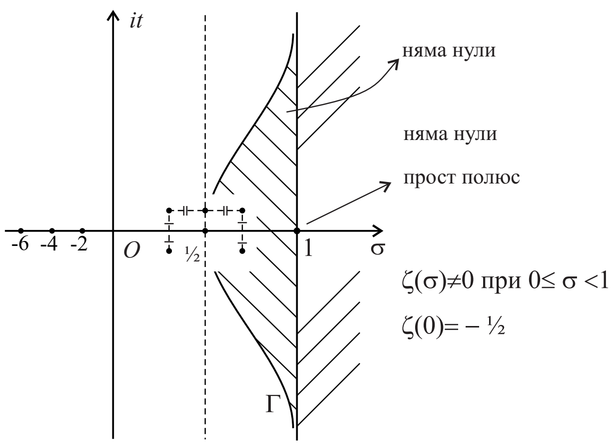
в) Единствените нули на $\zeta(s)$ при $\tau < 0$ са -2, -4, $-6, \ldots$;

г) В ивицата $0 \leq \tau \leq 1$ нулите на $\zeta(s)$ са симетрични относно правата $\tau = \frac{1}{2}$ и реалната ос;

д) $\zeta(s)$ притежава безбройно много нули върху правата $\tau = \frac{1}{2}$ (Харди, 1914 г.);

е) Съществуват такива константи $1 \gg A > 0$, $\alpha \geq 1$, щото $\zeta(s) \neq 0$ в областта, заключена между кривата $\Gamma : \tau = 1 - \frac{A}{\ln^{\alpha}(|t| + 2)}$ и правата $\tau = 1$ (доказано от Вале-Пусен, 1896 г.).

Очевидно Γ има вертикална асимптота $\tau = 1$ (вж. Фиг. 1).



Въз основа на своите изследвания върху $\zeta(s)$, Риман изказва следната хипотеза:

(R) Всички нули на $\zeta(s)$ в ивицата $0 \leq \tau \leq 1$ лежат върху правата $\tau = \frac{1}{2}$.

Досега тя не е нито доказана, нито опровергана.

Като следствие от хипотезата (R) се доказва следният забележителен резултат.

Означаваме с $\Pi(x) = \#\{p \in P, p \leq x\}$, т.е. $\Pi(x)$ е броят на простите числа, ненадминаващи x; $\forall x : \Pi(x) \in \mathbb{N} \cup \{0\}$.

Ясно е, че $\Pi(x)$ е стъпаловидна функция със скокове от 1 за всяко $x = p_n$, $\Pi(x) \to \infty$ при $x \to \infty$.

Основен резултат за разпределението на простите числа, **ако е вярно (R),** се дава от:

$$\Pi(x) = \operatorname{li} x + O(\sqrt{x}\log x), \quad x \to \infty. \tag{1}$$

Нещо повече, ако (1) е изпълнено, то е вярно (R). Следователно (R) и (1) са еквивалентни.

Напомняме, че интегралният логаритъм

$$\operatorname{li} x = \int_2^x \frac{dt}{\log t} = \frac{x}{\log x} + \cdots + (r-1)!\frac{x}{\log^r x} + O\left(\frac{x}{\log^{r+1} x}\right),$$

$x \to \infty$ и $r \in \mathbb{N}$ е кое да е, но остатъкът O зависи от r.

Наблюдението, че $\Pi(x) \sim \operatorname{li} x$ дължим на Гаус и то още в младежките му години. Льожандр предлага формулата $\Pi(x) \sim \dfrac{x}{\log x}$ (приблизително през 1808 г.).

Да предположим сега, че може да се докаже следният **отслабен** вариант на хипотезата на Риман:

$$\zeta(s) \neq 0 \ \text{ при } \ 1 \geq \sigma \geq \theta, \ \theta > \frac{1}{2}. \tag{R1}$$

Тогава ще бъде вярна (и еквивалентна на (R1)) асимптотичната формула:

$$\Pi(x) = \operatorname{li} x + O(x^\theta \log x), \quad x \to \infty. \tag{2}$$

Напълно естествено възниква въпросът:

Каква асимптотика е **доказана строго** за $\Pi(x)$ и каква е оценката за остатъка?

Изключително голям принос в това отношение има Чебишов, който в периода 1848-1850 г. създаде сериозен апарат за изследване на поведението на $\Pi(x)$ (вж. [2], [3]). Чак през 1896 г. едновременно Адамар и Вале-Пусен доказаха следната теорема:

Теорема 1. $\lim\limits_{x\to\infty} \Pi(x) : \dfrac{x}{\log x} = 1.$

И двете доказателства са сложни, защото използват комплициран апарат от комплексния анализ (вж. [4]). През 1980 г. Д. Нюман предложи скица на ново, кратко и достъпно доказателство в [14], която беше опростена от Д. Цагир в [15].

Доказателството на Теорема 1 почива на свойство б) на ζ функцията. Най-добрата оценка за остатъка в асимптотичната формула до началото на 80-те години на миналия век беше:

$$\Pi(x) = \operatorname{li} x + O\left(xe^{-b\log^{3/5} x \log^{-1/5} \log x}\right), \quad x \to \infty,$$

където $b = \text{const} > 0$.

3. Някои допълнения и уточнения. Да означим с R остатъка: $R(x) = \Pi(x) - \operatorname{li} x$. В строго определен смисъл резултатът от (1) е неподобряем, защото е доказано, че съществуват редици $X \to \infty$, $Y \to \infty$ със свойствата: $R(X) < -\sqrt{X}\dfrac{\log\log\log X}{\log\log X}$ и $R(Y) > \sqrt{Y}\dfrac{\log\log\log Y}{\log\log Y}$. От друга страна съгласно (1): $R(X) = O(\sqrt{X}\log X)$ и т.н.

Следствия от Теорема 1:

Следствие 1. *Нека $x = p_n \Rightarrow \Pi(x) = n$. Тогава* $\lim\limits_{n\to\infty} n\dfrac{\log p_n}{p_n} = 1 \Rightarrow \lim\limits_{n\to\infty}(\log n + \log\log p_n - \log p_n) = 0 \Rightarrow \lim\limits_{n\to\infty}\left(-1 + \dfrac{\log\log p_n}{\log p_n} + \dfrac{\log n}{\log p_n}\right) = 0 \Rightarrow \lim\limits_{n\to\infty} \dfrac{\log n}{\log p_n} = 1 \Rightarrow$

$p_n \sim n\log n$, $n \to \infty$, *защото* $\lim \dfrac{n\log p_n}{p_n} = 1$.

Следствие 2. $\lim\limits_{n} \dfrac{p_{n+1}}{p_n} = 1$.

Така намерихме асимптотичното поведение на n-тото просто число p_n. Оттук незабавно следва, че $\sum\limits_n \dfrac{1}{p_n} \sim \sum\limits_n \dfrac{1}{n\log n} \sim \displaystyle\int_2^\infty \dfrac{dx}{x\log x}$ съгласно критерия на Коши и следователно

$$\sum \frac{1}{p_n} = \infty. \tag{3}$$

Допълнение. Дж. Б. Росер доказа през 1939 г., че $p_n > n\log n$, $\forall n \geq 1$. Нещо повече, при $17 \leq x \leq e^{100}$ и $x \geq e^{200}$: $\dfrac{x}{\log x} < \Pi(x) < \dfrac{x}{\log x - 2}$.

Друга удобна формула за работа при $x \geq 55$ е:

$$\frac{x}{\log x + 2} < \Pi(x) < \frac{x}{\log x - 4}.$$

Нарочно привеждаме тези формули (макар и приближени), защото в тях **явно** е указано за какви стойности на x са валидни. Асимптотичните формули са верни за „достатъчно големи x“, но често пъти е деликатен въпросът за какви **конкретни** x са приложими.

Ето и един по-нов резултат на Росер и Шонфелд (1962):

$$\forall n \geq 67, n \in \mathbb{N}: \quad \frac{n}{\log n - \frac{1}{2}} < \Pi(n) < \frac{n}{\log n - \frac{3}{2}}.$$

4. Ще отделим известно място на постулата на Бертран от 1845 г., доказан наскоро след това от Чебишов (1852).

Хипотеза (Бертран). *Нека числото $x > 1$. Тогава в интервала $(x, 2x)$ се съдържа поне едно просто число.*

Чебишов доказа този резултат и дори го обобщи при достатъчно големи $x > x_0$ в интервала $(x, \delta x)$, където $\delta > \dfrac{6}{5}$.

Асимптотичната формула от Теорема 1 ни позволява да установим с лекота следното твърдение.

Предложение 1. *Нека $\varepsilon > 0$ е фиксирано. Тогава съществува такова x_0, щото при $x \geq x_0$ в интервала $(x, (1+\varepsilon)x)$ се съдържа поне едно просто число.*

Доказателството е елементарно, защото $\Pi(x) \sim \dfrac{x}{\log x}$, $x \to \infty$, $\Pi((1+\varepsilon)x) \sim \dfrac{x(1+\varepsilon)}{\log x + \log(1+\varepsilon)}$, $x \to \infty$, и значи $\lim\limits_{x\to\infty} \dfrac{\Pi((1+\varepsilon)x)}{\Pi(x)} = 1 + \varepsilon > 1$. И така при $x \geq x_0$: $\Pi((1+\varepsilon)x) > \Pi(x)$, а $\Pi((1+\varepsilon)x) - \Pi(x)$ ни дава броя на простите числа в интервала $(x, (1+\varepsilon)x)$.

5. Друг интересен въпрос от теорията на простите числа е оценката на разликата на две последователни прости числа $d_n = p_{n+1} - p_n$, където $2 = p_1 < p_2 < \cdots < p_n < \cdots \to \infty$. По-специално, интересуваме се от оценки от вида

$$0 < p_{n+1} - p_n \leq K p_n^\delta, \quad 1 > \delta = \text{const} > 0, \quad K = \text{const} > 0. \tag{4}$$

Чудаков и Ингам [9] доказаха през 30-те години на 20 век, че (4) е вярно при $\delta = \dfrac{48}{77} + \varepsilon (\forall \varepsilon > 0)$ (т.е. $\delta > 0,6223$), $\delta = \dfrac{38}{61} + \varepsilon$ (т.е. $\delta > 0,6229$), $\delta = \dfrac{5}{8} = 0,625$ а Хъксли установи през 70-те години, че $\delta = \dfrac{7}{12} + \varepsilon$ (т.е. $\delta > 0,5883$). Очакванията са, че по този начин ще се достигне до $\delta = \dfrac{1}{2}$ в (4).

Условен резултат 1. Ако е вярно (R), то $d_n \ll \sqrt{p_n} \log p_n$.

Хипотеза 2. $d_n \ll \log^2 p_n$ или дори $d_n \ll \log p_n$. В подкрепа на Хипотеза 2 са два резултата от началото на 40-те години на 20 век на Ердьош [3]:

а) съществуват безбройно много прости p'_k, за които $p'_{k+1} - p'_k < c \log p'_k$, $0 < c < 1$.

б) за безбройно много прости числа p''_k е вярна оценката

$$p''_{k+1} - p''_k > b \log p''_k \frac{\log\log p''_k . \log\log\log\log p''_k}{(\log\log\log p''_k)^2}, \quad b = \mathrm{const} > 0.$$

Ще напомним, че две последователни прости числа p_k, p_{k+1} се наричат близнаци, ако $p_{k+1} - p_k = 2$. Значи, близнаци са $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$,... Интересен и открит от дълги години е въпросът:

Крайно или безкрайно е множеството на близнаците–прости числа?

През 1919 г. норвежкият математик Брун доказа в [5], че (сумата) редът от реципрочните стойности на близнаците, е сходящ, т.е.

$$\frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \cdots < \infty. \tag{5}$$

Сумата (5) е пресметната с точност до много десетични знаци. Разбира се, от сходимостта на (5) не следва, че редът има безбройно много ненулеви членове. Той може да бъде и крайна сума, ако близнаците са краен брой.

Ето едно сравнение между три реда, което говори в известен смисъл за „гъстотата“ в разпределението на техните членове.

Хармоничният ред $\sum_n \dfrac{1}{n}$ е разходящ. Зачертаваме всички негови членове, чиито знаменатели са съставни числа. Така стигаме до реда (3), който е пак разходящ. След като в (3) оставим само реципрочните стойности на близнаците, стигаме до (5). Значи близнаците са много по-малко (по-редки в разпределението си).

До известна степен (макар и не напълно) резултатите в този абзац се допълват от следната теорема на Чен от 1975 г. (вж. [10]).

Теорема 2 (Chen J. R., 1933–1996)**.** *Съществува достатъчно голямо число x_0, така че щом $x > x_0 \Rightarrow [x, x + \sqrt{x}] \cap P_2 \neq \emptyset$.*

С други думи, в интервала $[x, x + \sqrt{x}]$ се съдържа поне едно почти просто число от ред 2. Тези числа са или прости, или произведение от 2 прости множителя, но за метода на доказателство са неразличими. Известна е хипотезата, че при $x > x_0$: $[x, x + 2\sqrt{x}] \cap P \neq \emptyset$.

Забележка. Можем да тълкуваме (4) така. В интервала $[p_n, p_n + K p_n^\delta]$ се съдържа следващото просто число p_{n+1}.

Резултатът на Чен може да се подобри, а именно: при $x \geq x_0$: $\left[x, x + x^{0,4717}\right] \cap P_2 \neq \emptyset$ ([10]).

6. Пристъпваме към постановката и кратък обзор върху хипотезата на Голдбах. Членът на Петербургската академия на науките Голдбах в писмо до Ойлер през 1742 г. изказва предположението, че всяко естествено число, по-голямо или равно на 6, може да се представи като сума от 3 прости. Ойлер му отговаря, че за да се реши проблемът, достатъчно е да се докаже, че всяко четно число е сума от 2 прости. Така стигаме до хипотезата на Голдбах:

(G) Всяко четно число, по-голямо от 2, е сума от 2 прости числа.

Твърдението (G) е еквивалентно на:

(G_1) Всяко четно естествено $n > 4$ е сума от 3 прости числа.

Доказателството на (G_1) е съвсем просто.

а) Нека $n > 1$. Тогава съгласно (G) $2n = p + q$, $p, q \in P$. Значи $2(n+1) = 2 + p + q$, т.е. (G_1) е изпълнено.

б) Обратно, нека $n > 2$ и е валидно (G_1). Следователно $2n = p + q + r$, $p, q, r \in P$. Поне едно от трите числа трябва да бъде четно, защото сумата от 3 нечетни числа е нечетно. Понеже 2 е единственото просто четно число, то нека $r = 2$. Тогава $2(n-1) = p + q$, $2(n-1) > 2$ и значи е налице (G).

Бележка 1. От хипотезата (G) следва, че всяко нечетно число $n > 7$ е сума от три нечетни прости. Наистина, нека естественото нечетно $n > 7 \Rightarrow 4 < n - 3$ и $n - 3$ е четно. Съгласно (G): $n - 3 = p_1 + p_2$, където $p_{1,2} \in P$. Ако допуснем, че p_1 и p_2 са прости и четни, то $p_1 = p_2 = 2$ и значи $n = 5$. Ако p_1 е нечетно, а p_2 четно, то $p_2 = 2 \Rightarrow n = 5 + p_1$ и значи n се оказва четно. Остава само p_1, p_2 да бъдат нечетни, $n = 3 + p_1 + p_2$ и т.н.

Хипотезата (G) не е доказана и досега (2012 г.). Ще формулирам главните постижения, очертаващи прогреса при изследване на (G).

Теорема 3 (Виноградов, 1937, вж. [11])**.** *Съществува такава константа $a > 1$, щото всяко нечетно $n > a$ може да се представи като сума от 3 различни нечетни прости числа.*

През 1956 г. руският математик К. Бороздкин намери оценка отгоре за a, а именно: $a \le e^{e^{16{,}038}} < 3^{3^{15}}$. Понеже a е много голямо, едва ли можем да се надяваме, че по компютърен път може да се докаже теоремата на Виноградов за нечетните n: $17 < n \le a$. Естествено е да се запитаме дали резултатът на Виноградов е оптимален, т.е. кога и дали може нечетното n да се представи като сума от по-малко от 3 прости числа.

Пример [8]**.** Разглеждаме редицата от нечетни съставни числа $n_k = (14k+3)^2 > 280$, $k \in \mathbb{N}$. Тогава n_k не може да се представи във вида $n_k = p_{1k} + p_{2k}$; $p_{1k}, p_{2k} \in P$. Ако допуснем противното, веднага заключаваме, че поне едното от двете числа p_{1k}, p_{2k} трябва да бъде четно. Нека за определеност $p_{1k} = 2 \Rightarrow p_{2k} > 140 \Rightarrow$ простото число $p_{2k} = n_k - 2$ се дели на 7 – абсурд!

През 1973 г. Чен [6] (вж. също [10]) установи следния интересен резултат.

Теорема 4 (Чен)**.** *Всяко достатъчно голямо четно число n е сума от просто и полупросто число от ред* 2.

Следователно $2n = p_1 + p_2$, $p_{1,2} \in P$ или $2n = p_1 + p_2 p_3$, където $p_3 \in P$.

Това е безспорно стъпка напред в доказването на (G). Отново методът на доказателството „не различава“ P и P_2.

7. Още преди 350 години Ферма е поставил проблема да се построи нетривиална функция $f : \mathbb{R} \to \mathbb{R}$, която да изобразява $\mathbb{N} \to P$.

Очевидно е следното предложение.

Предложение 2. *Всеки полином с целочислени коефициенти*

$$f(x) = a_o x^n + a_1 x^{n-1} + \cdots + a_n \tag{6}$$

и да речем $a_0 > 0$, за безбройно много стойности на $x \in \mathbb{N}$ приема значения $f(x) \notin P$, т.е. съставни числа.

Американският математик Р. Бук доказа през 1946 г., че не съществува рационална функция на x, която за всички стойности $x \in \mathbb{N}$ да приема стойности само прости числа, с изключение на тривиалната функция (константа).

Ще приведа примера с тричлена на Ойлер $f(x) = x^2 - x + 41$, който за $x = 0, 1, \ldots, 40$ приема стойности прости числа, но $f(41)$, е съставно. Вече знаем, че съществува редица от естествени числа $\{n_k\} \nearrow +\infty$, за която $f(n_k) \notin P$.

$(*)$ Възниква въпросът: Съществува ли $\{m_k\} \nearrow +\infty$, $m_k \in \mathbb{N}$, за която $f(m_k) \in P$?

Същият въпрос се поставя и за съвсем простия полином $g(x) = x^2 + 1$.

За съжаление и досега (2012 г.) горните въпроси нямат отговор.

Единственото, което се знае за проблема $(*)$, е в случая на линеен полином, т.е. $n = 1$.

Теорема 5 (Дирихле – 1837, [4])**.** *Да разгледаме аритметичната прогресия $an+b$, където $a, b \in \mathbb{N}$ и a, b са взаимно прости. Тогава за безбройно много стойности на $n \in \mathbb{N}$ членовете на прогресията са прости числа.*

По отношение на проблема $(*)$ полският математик Х. Иваниец доказа в [7] през 1978 г., че за безбройно много стойности на $n_k \in \mathbb{N}$ числата от вида $n_k^2 + 1 \in P_2$, т.е. са полупрости от ред 2.

За пълнота ще приведа още един резултат на руския математик Б. М. Бредихин от 1963 г. Той доказа, че съществуват безбройно много прости числа, представими във вида $x^2 + y^2 + 1$ за подходящи $x, y \in \mathbb{N}$. Тук обаче полиномът е на 2 променливи.

Не мога да се въздържа да не формулирам един знаменит резултат на Грийн-Тао от 2004 г. (уточнен и обобщен през 2006 г.). Тао е Фийлдсов медалист за 2006 г.

Теорема 6 (Грийн-Тао, вж. [16])**.** *За всяко естествено число n съществуват, и то безбройно много, n-членни аритметични прогресии, чиито членове са прости числа.*

Нарочно ще приведа няколко примера, защото намирането им при големи n е трудно.

Пример:

$n = 1 : \quad \div 1$

$n = 2 : \quad \div 1, 2$

$n = 3 : \quad \div 3, 7, 11$

$n = 4 : \quad \div 251, 257, 263, 269$

$n = 5 : \quad \div 5, 11, 17, 23, 29$

$n=6: \quad \div 7, 37, 67, 97, 127, 157$

$n=7: \quad \div 7, 157, 307, 457, 607, 757, 907$

През 2004 г. беше намерена следната прогресия с 23 елемента прости числа:

$n=23: \quad \div 56211383760397 + k.44546738095860; \quad k=0,1,\dots,22.$

Очевидно полиномът (6) с целочислени коефициенти взаимно прости числа трябва да бъде неразложим над пръстена $\mathbb{Z}$, за да приема върху $\mathbb{N}$ безбройно много стойности от P. Това необходимо условие не е достатъчно, защото $h(x)=x^2+x+4$ е неразложим над $\mathbb{Z}$ и полето $\mathbb{Q}$ ($h(x)$ има комплексни корени, а линейните полиноми над $\mathbb{Q}$ – само корени от $\mathbb{Q}$). От друга страна $x^2+x+4=x(x+1)+4 \geq 6$ при $x \in \mathbb{N}$ и следователно стойностите на h са четни. Буняковски изказа през 1857 г. хипотезата, че за безбройно много стойности $x \in \mathbb{N}$, $\dfrac{1}{2}h(x)$ е просто число, но засега това не е нито доказано, нито опровергано.

Ще приключа това изложение с малко обобщение на един резултат на американския математик Милс от 1946 г. [13].

Предложение 3. *Нека простите числа* p_n *удовлетворяват оценката*

$$p_{n+1}-p_n < KP_n^{\delta}, \tag{7}$$

където $1>\delta>\dfrac{1}{2}$ *и константата* $K>\dfrac{1}{2}$. *Означаваме с* β *кое да е число* $\beta > \dfrac{1}{1-\delta} > 2$. *Тогава, съществува константа* $A(\beta)>1$ *и такава, че* $\left[A^{\beta^n}\right] \in P$, $\forall n \in \mathbb{N}$.

Както е прието, с $[x] \in \mathbb{Z}$ означаваме цялата част на $x \in \mathbb{R}$, т.е. $x-1<[x]\leq x$.

Този резултат преформулираме така. Функцията от експоненциален тип $\left[A^{\beta^n}\right]$ приема за всяко n прости стойности и очевидно $n \to \infty \Rightarrow \left[A^{\beta^n}\right] \to \infty$. Не се твърди, че функцията приема *всички* прости стойности. Както споменахме по-горе, сред полиномите и рационалните функции такава функция не съществува. Затова се обърнахме към експоненциалната. За съжаление $[x]$ има скокове в целочислените точки, но инак е частично постоянна (стъпаловидна). В точка **5** подробно дискутирахме кога е валидна оценката (7).

8. Ще спомена само едно приложение на простите числа в геометрията. Още в юношеска възраст Гаус доказа, че правилен n-ъгълник е построим с пергел и линийка точно когато $n=2^k p_1 \dots p_m$, където $k \geq 0$, $k \in \mathbb{Z}$, а $p_1,\dots,p_m$ са различни помежду си прости числа от вида $p_i = 2^{2^s}+1$, $s \geq 0$, $s \in \mathbb{Z}$. Преди столетия Ферма беше изказал предположението, че всички числа от вида $2^{2^s}+1$, $s \geq 0$, $s \in \mathbb{Z}$ (така наречените числа на Ферма) са прости. Това е така при $s=0,1,2,3,4$. Ойлер установи, че при $s=5$ числото на Ферма е съставно, защото се дели на 641. Остава и досега открита хипотезата, че за безбройно много стойности на $s \in \mathbb{N}$ числата на Ферма са прости.

С това приключвам своето изложение.

ЛИТЕРАТУРА

[1] Математическая энциклопедия, т. 1 – т. 5. Советская энциклопедия, Москва, 1977–1985.

[2] Ш. Михелович. Теория чисел, Издание второе. Высшая школа, Москва, 1967.

[3] А. Бухштаб. Теория чисел. Учпедгиз, Москва, 1960.
[4] K. Chandrasekharan. Introduction to analytic number theory. Springer-Verlag, Berlin-New York, 1968.
[5] V. Brun. La série $\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\cdots$ où les dénominateurs sont "nombres jumeaux" est convergante ou finie. *Bull. Sci. Math.*, **43** (1919), 100–104 et 124–128.
[6] J. R. Chen. On the representation of a large even number as the sum of prime and the product of at most two primes (Parts I and II). *Sc. Sinica*, **16** (1973), 151–176 and **21** (1978), 421–430.
[7] H. Iwaniec. Almost primes represented by quadratic polynomial. *Invent. Math.*, **47** (1978), 171–188.
[8] W. Sierpinski. Elementary theory of numbers. Ed. Polish Scientific publishers and North Holland, Warsaw, 1987.
[9] A. Ingham. On the difference between consecutive primes. *Quart. J. Math. Oxford Ser.*, **8** (1937), 255–266.
[10] P. Chengtong, W. Yuan, J. R. Chen. A brief outline of his life and works. *Acta Math. Sinica, New Series*, **12** (1996), 225–233.
[11] И. Виноградов. Метод тригонометрических сумм в теории чисел. Москва, 1971.
[12] F. Olver. Introduction to asymptotics and special functions. Academic Press, NY and London, 1974.
[13] W. Mills. A prime-representing function. *Bull. of the AMS*, **53** (1947), 604.
[14] D. Newman. Simple analytic proof of the prime number theorem. *Amer. Math. Monthly*, **87** (1980), 693–696.
[15] D. Zagier. Newman's short proof of the prime number theorem. *Amer. Math. Monthly*, **104** (1997), 705–708.
[16] B. Green, T. Tao. The primes contain arbitrarily long arithmetic progressions. Annals of Math., **167** (2008), 481–547.
[17] Е. Титчмарш. Теория дзета функции Римана. М., Ил., 1953.

Петър Попиванов
Институт по математика и информатика
Българска академия на науките
ул. Акад. Г. Бончев, бл. 8
1113 София, България
e-mail: popivano@math.bas.bg

DISTRIBUTION OF PRIMES AND SEVERAL APPLICATIONS

Petar Popivanov

This talk deals with several classical and more modern results from the theory of primes and is devoted to a larger audience. A short survey is given and almost primes of order two are discussed too. Polynomials with integer coefficients are considered from the point of view of their composite and prime functional values. Exponential type functions mapping $\mathbb{N}$ into the set of primes are also constructed.