МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2016
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2016
Proceedings of the Forty Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Pleven, April 6–10, 2016

КЛАСИЧЕСКИ ЗАДАЧИ ОТ ТЕОРИЯТА НА ЧИСЛАТА И СЪВРЕМЕННИ МЕТОДИ И ПОСТИЖЕНИЯ, СВЪРЗАНИ С ТЯХ

Дойчин И. Толев

Настоящата статия е посветена на последните достижения свързани с някои класически задачи в теорията на числата — проблемите на Голдбах, хипотезата за простите числа близнаци, както и задачата за откриване на големи разлики между съседни прости числа.

През 1742 г., в кореспоненция между Голдбах и Ойлер, са били формулирани две знаменити хипотези, по-късно станали известни като *Бинарна и Тернарна хипотези на Голдбах.* Те гласят съответно:

Хипотеза 1. *Всяко четно число по-голямо от* 2 *се представя като сума на две прости числа.*

Всяко нечетно число по-голямо от 5 *се представя като сума на три прости числа.*

Лесно се вижда, че ако е вярна бинарната хипотеза, то вярна е и тернарната. Наистина, ако имаме нечетно число $N \geq 5$, то числото $N-3$ е четно и $N-3 \geq 2$. Тогава, ако е вярна бинарната хипотеза, ще съществуват прости числа p_1 и p_2 такива, че $N-3 = p_1+p_2$, откъдето следва, че $N = p_1+p_2+3$ е сума на три прости числа.

Към настоящия момент тернарната хипотеза е напълно доказана. Ще споменем накратко основните стъпки, направени в това направление. През 1923 г. Харди и Литлууд [12], с помощта на разработения от тях *кръгов метод*, установяват, че ако се допусне верността на *Разширената хипотеза на Риман*, то съществува асимптотична формула за броя на решенията на уравнението

$$N = p_1 + p_2 + p_3, \tag{1}$$

в прости числа p_1, p_2, p_3, откъдето следва, че всяко достатъчно голямо нечетно число се представя като сума на три прости числа. През 1937 г. И. М. Виноградов [2] намира метод за оценяване на експоненциални суми, в които сумационната променлива пробягва прости числа. Той показва, че ако се използва този метод, става възможно в разсъжденията на Харди и Литлууд да бъде отстранена зависимостта от Разширената хипотеза на Риман и е достатъчно да се използват значително по-слаби (но вече доказани) резултати относно разпределението на простите числа в аритметични прогресии. По такъв начин Виноградов доказва съществуването на ефективно изчислима константа N_0 такава, че всяко нечетно число $N \geq N_0$ може да се представи във вида (1).

Първият явен израз за N_0 (а именно $N_0 = e^{e^{e^{41.96}}}$, където e е неперовото число) е намерен през 1939 г. от Бороздкин. Впоследствие тази стойност е намалявана многократно и до неотдавна най-силният резултат в това направление принадлежеше на Лиу и Ванг [16], които през 2002 г. установяват, че допустима стойност е $N_0 = 2 \cdot 10^{1346}$. Макар и значително по-малка от предишните, константата на Лиу и Ванг все още не е достатъчно малка, за да може представимостта на нечетните числа по-малки от нея да бъде проверена посредством компютър.

Финалната стъпка по отношение на доказването на тернарната хипотеза е извършена през 2013 г. от Хелфгот в работите [13], [14], [15]. Той използва нови и прецизни аналитични методи и с тяхна помощ установява, че ако $N_0 = 10^{27}$, то всяко нечетно $N \geq N_0$ се представя във вида (1). Това решава тернарния проблем на Голдбах, защото проверката на представимостта на нечетните $N < 10^{27}$ вече може да се извърши с помощта на компютър. И така, валидна е следната

Теорема 2. *Всяко нечетно число по-голямо от 5 се представя като сума на три прости числа.*

Бинарната хипотеза в настоящия момент не е доказана, но са установени голям брой резултати, които в един или друг аспект са приближения към нея. Ще цитираме първо известната теорема на Чен [5], доказана през 1973 г. и която гласи

Теорема 3 (Чен)**.** *Съществува ефективно изчислима константа N_1 такава, че всяко четно число $N \geq N_1$ се представя като сума на просто число и на число притежаващо най-много два прости множителя.*

Неотдавна Ямада [24] установи, че горната теорема е вярна при $N_1 = e^{e^{36}}$.

Друг подход към изследването на бинарната хипотеза представлява оценката на величината $E(X)$, която при зададено $X > 2$ се определя като броя на четните числа, ненадминаващи X, които не могат да се представят като сума на две прости числа. Очевидно бинарната хипотеза на Голдбах е еквивалентна на твърдението

$$E(X) = 0 \qquad \text{при} \qquad X > 2,$$

което, както отбелязахме, в настоящия момент не е доказано. От друга страна, ясно е, че $E(X)$ не надхвърля броя на четните числа, ненадминаващи X, т.е. в сила е тривиалната оценка

$$E(X) \leq [X/2]. \tag{2}$$

Голям интерес представлява намирането на нетривиални оценки отгоре за $E(X)$, т.е. оценки по-силни от тази в (2). Работата в това направление е започната още през 1937 г., непосредствено след появата на статията на И. М. Виноградов [2]. Независимо един от друг Чудаков [3], Ван дер Корпут [6] и Естерман [8] използват неговия метод и доказват, че за произволно голяма константа $A > 0$ може да се намери $X_0(A)$ такова, че

$$E(X) \leq \frac{X}{(\ln X)^A} \qquad \text{при} \qquad X > X_0(A).$$

През 1975 г. Монтгомери и Вон [20] установяват по-силен резултат, а именно, че съществува константа $\delta < 1$ такава, че при достатъчно големи X е изпълнено

$$E(X) \leq X^{\delta}. \tag{3}$$

Впоследствие са публикувани редица статии, в които се доказва неравенство от вида (3) с конкретни стойности на δ. Най-силният резултат от този вид принадлежи на Лу [17], който през 2010 г. доказва неравенството (3) при достатъчно големи X и при $\delta = 0.879$.

Друга известна хипотеза от теорията на простите числа е свързана с така наречените прости числа близнаци. Такива са всяка двойка прости числа, разликата на които е равна на 2, например двойките 3 и 5, 11 и 13, 17 и 19, 41 и 43, както и още много други. Най-големите прости числа от такъв вид, известни до този момент, са

$$65516468355 \cdot 2^{333333} \pm 1,$$

като всяко от тях притежава 100355 цифри в десетичното си представяне[1]. Още в древността е възникнала следната

Хипотеза 4. *Съществуват безбройно много двойки от прости числа близнаци.*

Тази хипотеза в настоящия момент не е доказана и, наред с бинарната хипотеза на Голдбах, се счита за един от най-трудните проблеми в теорията на числата. През 1973 г. Чен в статията [5] доказва също следната

Теорема 5 (Чен)**.** *Съществуват безбройно много прости числа p такива, че числото $p+2$ притежава в каноничното си разлагане най-много два прости множителя.*

Ще обърнем по-сериозно внимание и на един друг подход за изследване на задачата за близнаците. Очевидно, ако p_n означава n-тото просто число, то Хипотеза 4 е еквивалентна на твърдението, че съществуват безбройно много n, за които

$$p_{n+1} - p_n = 2.$$

Във връзка с това, още през двадесетте години на миналия век редица математици са се опитвали да установят, че за безбройно много n разликата $p_{n+1} - p_n$ е „малка“. Да отбележим, че от асимптотичния закон за разпределение на простите числа може да се направи заключението, че очакваната средна стойност на тази разлика е $\ln p_n$. Затова можем да считаме, въпросната разлика за малка, ако тя не надминава $c \ln p_n$ за някаква положителна константа $c < 1$.

В продължение на повече от 80 години с тази задача се занимават редица математици, като Харди, Литлууд, Ердьош, Селберг, Бомбиери, Хаксли, Мотохаши и много други, но едва през 2009 г. Голдстон, Пинц и Ялдарим [11] доказват следната

Теорема 6 (Голдстон, Пинц, Ялдарим)**.** *За произволна константа $c \in (0,1)$ съществуват безбройно много n такива, че $p_{n+1} - p_n < c \ln p_n$.*

В работата [11] Голдстон, Пинц и Ялдарим получават също условно доказателство на много по-силен резултат. За да го формулираме, ще дадем дефиниция на понятието *ниво на разпределение на редицата от простите числа*.

Нека $\pi(x, q, l)$ е броят на простите числа $p \le x$, за които $p \equiv l \pmod q$. Предполага се, че ако $(q, l) = 1$ то $\pi(x, q, l)$ е приближено равно на $\dfrac{1}{\varphi(q)} \displaystyle\int_2^x \frac{dt}{\ln t}$, където

[1] По-подробна информация може да се намери на следната интернет страница: http://primes.utm.edu/primes/page.php?id=89650

$\varphi(q)$ е функцията на Ойлер. Според известната теорема на Зигел, това наистина е така, при условие, че $q \le (\ln x)^c$ за някоя константа $c > 0$. Ако обаче q зависи от x и расте като степенна функция с нарастването на x, поведението на $\pi(x, q, l)$ не е известно (освен ако не допускаме верността на някои недоказани хипотези, като например Разширената хипотеза на Риман).

Да вземем грешката, която се допуска при замяна на $\pi(x, q, l)$ с предполагаемата приближена стойност, т.е.

$$\Delta(x, q, l) = \pi(x, q, l) - \frac{1}{\varphi(q)} \int_2^x \frac{dt}{\ln t},$$

както и максималната стойност на модула на горната величина за всевъзможните l взаимно прости с q, т.е.

$$\Delta^*(x, q) = \max_{(l,q)=1} |\, \Delta(x, q, l)| \,.$$

При $x \ge 2$ и $\theta \in (0, 1)$ разглеждаме сумата

$$\Sigma(x; \theta) = \sum_{q \le x^\theta} \Delta^*(x, q). \tag{4}$$

Лесно се проверява, че за достатъчно големи x имаме $\Sigma(x; \theta) \le x(\ln x)^2$, но тази оценка е безполезна. Оказва се, обаче, че за някои стойности на θ сумата $\Sigma(x; \theta)$ може да се оцени значително по-точно и този факт играе основна роля при решаването на много задачи от теорията на числата.

Казваме, че числото $\theta \in (0, 1)$ е ниво на разпределение на редицата на простите числа, ако за всяка константа $A > 0$ и за достатъчно големи x е изпълнено

$$\Sigma(x; \theta) \le \frac{x}{(\ln x)^A}. \tag{5}$$

Очевидно, ако θ е ниво на разпределение на редицата на простите числа, то всяко число $\theta' \in (0, \theta)$ също е ниво на разпределение. През 1965 г. Бомбиери [4] и независимо А. Виноградов [1] доказват следната

Теорема 7 (Бомбиери, А. Виноградов)**.** *Всяко $\theta \in \left(0, \frac{1}{2}\right)$ е ниво на разпределение на редицата на простите числа.*

Това е една от най-важните теореми в теорията на простите числа и има голям брой приложения. В частност, варианти на тази теорема се използват при доказателствата на гореспоменатите теореми на Чен (Теорема 3 и Теорема 5).

Не е известно дали твърдението на Теорема 7 е изпълнено и за някои $\theta \in \left[\frac{1}{2}, 1\right)$. Предполага се, че е вярна следната хипотеза на Елиот и Халберстам [7]

Хипотеза 8. *Всяко $\theta \in (0, 1)$ е ниво на разпределение на редицата на простите числа.*

Това твърдение към настоящия момент не е доказано.

Да се върнем към въпроса за разликите между съседните прости числа. През 2009 г. Голдстон, Пинц и Ялдарим в работата [11] доказват също следната

Теорема 9 (Голдстон, Пинц, Ялдарим). *Да допуснем, че някое* $\theta \in \left(\frac{1}{2}, 1\right)$ *е ниво на разпределение на редицата от простите числа. Тогава съществува* $C = C(\theta) > 0$ *такова, че за безбройно много* n *е изпълнено*

$$p_{n+1} - p_n \le C. \tag{6}$$

Голдстон, Пинц и Ялдарим намират явен вид на величината $C(\theta)$ и показват, например, че при $\theta \ge 0.971$ може да се вземе $C(\theta) = 16$. В доказателството на тази теорема се прилага специфичен метод на решетото, който е близък до решетото на Селберг. Използва се също информация за разпределението на простите числа в аритметични прогресии, но се оказва, че теоремата на Бомбиери и Виноградов (Теорема 7) за тази цел не е достатъчно силна. Поради това се налага да се предположи верността на неин усилен вариант, какъвто и до днес не е доказан, така че резултатът от Теорема 9 е само условен.

Решаващият пробив за задачата за съществуването на безбройно много двойки прости числа в ограничени интервали е направен от Джанг [25], който през 2013 г. намира безусловно доказателство на следната

Теорема 10 (Джанг). *Съществуват безбройно много* n *такива, че*

$$p_{n+1} - p_n < 7 \cdot 10^7.$$

В доказателството на тази теорема се използва метод на решетото, подобен на този в работата на Голдстон, Пинц и Ялдарим. Основната идея на Джанг е, че информацията за разпределението на простите числа в аритметични прогресии се използва не като се прилага оценката (5) за сумата (4), а като се разглежда друга сума $\Sigma^*(x, \theta)$, която е подобна на сумата (4), но е по-сложна. (За да избегнем навлизането в технически подробности, няма да даваме формула за тази сума, а на интересуващия се читател препоръчваме статията [25]). Джанг прилага така наречения дисперсионен метод на Линник и свежда оценяването на сумата $\Sigma^*(x, \theta)$ до оценяването на експоненциални суми на няколко променливи, а оценките за тях получава със средствата на алгебричната геометрия. Така Джанг показва, че за някое $\theta \in \left(\frac{1}{2}, 1\right)$ и при произволно $A > 0$ е изпълнено $\Sigma^*(x, \theta) \le \frac{x}{(\ln x)^A}$. Последната оценка може да се използва в доказателството като заместител на оценката (5), за която и до днес не е известно дали е вярна когато $\theta \in \left(\frac{1}{2}, 1\right)$.

След публикуването на статията на Джанг със задачата за заменяне на константата $7 \cdot 10^7$ с по-малка се заемат редица математици и след няколко месеца е публикувана колективната работа (под псевдонима Polymath) [21], в която константата е намалена до 4680. През месец ноември 2013 г. съществен напредък в това направление правят Дж. Мейнард [18] и (независимо) Т. Тао (публикувано в неговия блог[2]). Техният метод позволява да бъде получен резултат от типа на Теорема 10, с много по-малка константа, но също и по значително по-лесен начин — без да се прибягва до оценяването на експоненциални суми чрез методите на алгебричната геометрия. И така, те доказват следната

[2]Виж страницата `http://terrytao.wordpress.com/`

Теорема 11 (Мейнард, Тао). *Съществуват безбройно много n такива, че*

$$p_{n+1} - p_n < 600.$$

Основната идея в доказателството на Теорема 11 е прилагането на нов вид решето, което, в известен смисъл, представлява многомерен вариант на решетото на Голдстон, Пинц и Ялдарим. Методът до голяма степен е елементарен и единственият по-дълбок резултат от аналитичната теория на числата, който се използва, е теоремата на Бомбиери-Виноградов (Теорема 7).

Доказателството на Мейнард и Тао е интересно и с това, че за да се получи подобен резултат не е необходимо да се използва теоремата на Бомбиери и Виноградов в пълната ѝ сила. Достатъчно е да се знае, че някакво фиксирано, макар и много малко $\theta > 0$ е ниво на разпределение на редицата от простите числа, а резултати от такъв тип са били известни още през петдесетте години на миналия век. (Все пак, да отбележим, че при по-голяма стойност на θ се получава по-малка числена стойност на константата C, стояща в дясната страна на неравенството (6)).

Друга важна особеност на метода на Майнард–Тао е, че с негова помощ може да се докаже не само съществуването на безбройно много двойки прости числа в интервали с ограничена дължина, но даже, при произволно $m \in \mathbb{N}$, съществуването на безбройно много m-орки от прости числа в такива интервали. С методите от работите на Голдстон, Пинц, Ялдарим и Джанг това не може да бъде направено. В сила е следната теорема

Теорема 12 (Мейнард, Тао). *Нека е дадено произволно $m \in \mathbb{N}$. Съществува константа $C > 0$ такава, че за безбройно много $n \in \mathbb{N}$ имаме*

$$p_{n+m} - p_n < Cm^3 e^{4m}.$$

След публикуването на работата на Мейнард, както и появата на доказателството на Тао в неговия блог, са получени и по-точни резултати. Групата от математици, работещи под псевдонима Polymath, публикува статията [22], в която са изложени най-силните резултати, които могат да бъдат получени чрез съчетаване и оптимално използване на методите на Голдстон, Пинц, Ялдарим, Джанг, Мейнард и Тао. Ще цитираме два резултата от тази статия. Първият от тях е получен през 2014 г. и представлява по-силен вариант на Теорема 11. В сила е следната

Теорема 13 (Polymath). *Съществуват безбройно много $n \in \mathbb{N}$ такива, че*

$$p_{n+1} - p_n \leq 246.$$

Друг резултат от [22] представлява усилване на Теорема 12, а именно:

Теорема 14 (Polymath). *Нека е дадено произволно $m \in \mathbb{N}$. Съществува константа $C > 0$ такава, че за безбройно много $n \in \mathbb{N}$ имаме*

$$p_{n+m} - p_n < C\, m\, e^{\left(4 - \frac{52}{283}\right)m}.$$

В статията [22] е показано, че при допускане верността на хипотезата на Елиот и Халберстам (Хипотеза 8), както и някои нейни обобщения, са изпълнени и по-силни твърдения, но на този въпрос няма да се спираме, а на интересуващия се читател препоръчваме да погледне в цитираната статия.

Интересна задача, свързана с разпределението на разликите между съседните прости числа, е да се изследва дали те могат да бъдат „големи". Първо да отбележим, че за произволно естествено число k съществуват стойности на n, за които

$$p_{n+1} - p_n \geq k. \tag{7}$$

Наистина

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

представляват k на брой последователни естествени числа, като всички те са съставни (първото от тях се дели на 2, второто — на 3, и т.н., последното — на $k+1$). Следователно, ако p_n е най-голямото просто число, за което $p_n < (k+1)! + 2$, изпълнено е (7).

Както отбелязахме по-горе в статията, средната стойност на разликата между две съседни прости числа $p_{n+1} - p_n$ е $\ln p_n$, така че необичайно голяма можем да считаме разлика, която надхвърля $C \ln p_n$ за някакво $C > 1$. Интересът към откриването на големи разлики се е породил още в началото на миналия век През 1938 г. Ранкин [23] подобрява предишни резултати на Ердьош и доказва следната

Теорема 15 (Ранкин)**.** *Съществува константа $C > 0$ такава, че за безбройно много n е изпълнено*

$$p_{n+1} - p_n \geq C \frac{(\ln p_n)\,(\ln\ln p_n)\,(\ln\ln\ln\ln p_n)}{(\ln\ln\ln p_n)^2}. \tag{8}$$

През следващите повече от 70 години подобренията на резултата на Ранкин са свързани единствено с увеличаването на константата C.

Едва през 2014 г. Грийн, Конягин, Тао, Форд [9], както и (независимо от тях) Мейнард [19] доказват, че в израза от дясната страна на (8) вместо константата C може да се постави функция на n, клоняща към безкрайност. Малко по-късно тези петима математици обединяват усилията си и през 2015 г. публикуват работата [10], в която доказват следната

Теорема 16 (Грийн, Конягин, Тао, Форд, Мейнард)**.** *Съществува константа $C > 0$ такава, че за безбройно много n е изпълнено*

$$p_{n+1} - p_n \geq C \frac{(\ln p_n)\,(\ln\ln p_n)\,(\ln\ln\ln\ln p_n)}{(\ln\ln\ln p_n)}. \tag{9}$$

Виждаме че изразът в дясната страна на (9) нараства по-бързо от този в (8), но се отличава от него само с множител $\ln\ln\ln p_n$. Както споделя Тао в неговия блог, подобрения на оценката от Теорема 16 могат да бъдат постигнати само чрез използването на съществено нови идеи и, според него, това ще е много трудно.

Надяваме се, прогрес по решаването на тази, а и на другите задачи, споменати в настоящата статия, да бъде постигнат в не чак толкова далечно бъдеще.

ЛИТЕРАТУРА

[1] А. И. Виноградов. О плотностной гипотезе для L-рядов Дирихле. *Известия АН СССР, сер. матем.*, **29** (1965), 903–934.

[2] И. М. Виноградов. Представление нечетного числа суммой трех простых чисел. *ДАН СССР*, **15**, (1937), 6–7.

[3] Н. Г. Чудаков. О плотности совокупности четных чисел, непредставимых как сумма двух нечетных простых. *Изв. АН СССР. Сер. матем.*, **2**, № 1 (1938), 25–40.

[4] E. Bombieri. On the large sieve. *Mathematika*, **12** (1965), 201–225.

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

[6] J. G. van der Corput. Sur l'hypothèse de Goldbach. *Proc. Akad. Wet. Amsterdam*, **41** (1938), 76–80.

[7] P. D. T. A. Elliott, H. Halberstam. A conjecture in prime number theory. In: Symposia Mathematica, vol. **IV** (INDAM, Rome, 1968/69), 59—72. Academic Press, London, 1970.

[8] T. Estermann. On Goldbach's problem: Proof that almost all even positive integers are sums of two primes. *Proc. London Math. Soc.*, **44**, No 2 (1938), 307–314.

[9] K. Ford, B. Green, S. Konyagin, T. Tao. Large gaps between consecutive prime numbers. arXiv:1408.4505v2 [math.NT].

[10] K. Ford, B. Green, S. Konyagin, J. Maynard, T. Tao. Long gaps between primes. arXiv:1412.5029v2 [math.NT].

[11] D. Goldston, J. Pintz, C. Yildirim. Primes in tuples I. *Ann. of Math. (2)*, **170** (2009), 819–862.

[12] G. H. Hardy, J. E. Littlewood. Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes. *Acta Math.*, **44** (1923), 1–70.

[13] H. A. Helfgott. Major arcs for Goldbach's problem. arXiv:1305.2897v2 [math.NT].

[14] H. A. Helfgott. Minor arcs for Goldbach's problem. arXiv:1205.5252v3 [math.NT].

[15] H. A. Helfgott. The ternary Goldbach conjecture is true. arXiv:1312.7748 [math.NT].

[16] M.-Ch. Liu, T. Wang. On the Vinogradov bound in the three primes Goldbach conjecture. *Acta Arith.*, **105**, No 2, (2002), 133–175.

[17] W. C. Lu. Exceptional set of Goldbach number. *J. Number Theory*, **130**, (2010), 2359–2392.

[18] J. Maynard. Small gaps between primes. *Ann. of Math.*, **181**, No 1 (2015), 383–413.

[19] J. Maynard. Large gaps between primes. arXiv:1408.5110v1 [math.NT].

[20] H. L. Montgomery, R. C. Vaughan. The exceptional set in Goldbach's problem. *Acta Arith.*, **27** (1975), 353–370.

[21] D. H. J. Polymath. New equidistribution estimates of Zhang type, and bounded gaps between primes. arXiv:1402.0811v3 [math.NT].

[22] D. H. J. Polymath. Variants of the Selberg sieve, and bounded intervals containing many primes. *Research in the Mathematical Sciences*, **1**, (2014), article 12.

[23] R. A. Rankin. The difference between consecutive prime numbers. *J. London Math. Soc.* **13** (1938), 242–247.

[24] T. Yamada. Explicit Chen's theorem. arXiv:1511.03409 [math.NT].

[25] Y. Zhang. Bounded gaps between primes. *Ann. of Math.*, **179**, No 2 (2014), 1121–1174.

Дойчин Толев
Факултет по Математика и Информатика
СУ „Св. Климент Охридски“
бул. Дж. Баучер, № 5
1164 София
e-mail: dtolev@fmi.uni-sofia.bg

CLASSICAL PROBLEMS IN NUMBER THEORY AND MODERN METHODS AND ACHIEVEMENTS RELATED TO THEM

Doychin Tolev

The present paper is devoted to the latest achievements in the study of several classical problems in number theory – Goldbach's conjectures, prime twins conjecture and the problem about the large differences between consecutive prime numbers.