НАСТАВА МАТЕМАТИКЕ
LII, 4 (2007), 1–11

Др Шефкет Арсланагић и Валтер Јанус

ПОСТОЈИ БЕСКОНАЧНО МНОГО ПРОСТИХ БРОЈЕВА – ЕУКЛИДОВА ТЕОРЕМА

Увод

За поједине математичке исказе постоји „кроз дуги низ година“ велики број доказа – било је, у неку руку, „у тренду“ за поједине теореме изводити нове доказе.

Примјери тога су отприлике:

- *Питагорина теорема.*

Добар увид у окружење и разноврсност њених преко 300 доказа даје књижица [4] (такође вриједна препоруке и кад су у питању ученици). (Као куриозитет се тамо наводи да је каснији амерички предсједник James A. Garfield као посланик Конгреса 1876. године открио интересантан доказ Питагорине теореме, који је одштампан у часопису *New England Journal of Education.* Он је свој доказ пронашао док је за време рада Конгреса разбијајући досаду решавао математичке задатке!)

- *Неједнакост између геометријско-аритметичке средине.*

О овој основној чињеници из теорије тежинских средина, чији је први доказ дао MacLaurin у првој трећини 18. века, налазе се у књизи [5] 52 различита доказа.

- *Основно правило алгебре.*

И за њега је од првог Gauss-овог доказа из 1799. године – налази се у његовом докторату – осмишљено недогледно много даљих начина доказивања.

И теорема наведена у наслову, коју је у својим *Елементима* први формулисао и доказао Еуклид, спада у ову категорију. (Чак и данас се, поред свих ових резултата, у часописима објављују доста изненађујући нови докази.)

Какав је заправо интерес у томе да се једна одавно позната и елементарна чињеница стално изнова потврђује? Као што ћемо видјети код Еуклидове теореме, многи докази су резултат настављених размишљања, на примјер, о расподјели простих бројева. Нови доказ би онда био илустрација неке нове идеје или новог концепта једне тешке опште теорије. Код Еуклидове теорме се ту међутим придружују и културни и естетски мотиви, као што је Ribenboim [13, стр. 3] примјетио: „Навешћу неколико доказа ове теореме [...] од познатих, али и од заборављених математичара. Неки докази претпостављају занимљиве развитке;

други су једноставно паметни или необични“. Овакви мотиви су управо код елементарних резултата од великог значаја.

Најпослије, постоје и педагошки разлози, као што је Benjamin F. Finkel (у првом броју часописа *American Mathematical Monthlly*) написао: „Рјешавање проблема је један од најнижих облика математичког истраживања, ... ипак његова образовна вриједност не смије бити потцјењена. Ријеч је о степеницама којима се ум пење ка вишим пољима оригиналног истраживања и испитивања. Многи спавајући, неискоришћени умови потакнути су на дјеловање кроз савлађивање једног јединог проблема“.

У овом раду ће бити представљени неки од доказа ове теореме, коју је Immanuel Kant у својој *Критици чистог ума* назвао ремек-дјелом људског ума. Докази теку углавном индиректно, што значи да претпостављају да постоји само коначно много простих бројева, и из тога изводе контрадикцију.

Докази су већим дијелом „елементарни“ у смислу да је за њихово разумевање довољно познавање једноставних теорема о дјељивости, о редовима, односно о тополошким просторима. У којој мјери су посебно елегантни (у смислу који том појму даје Erdös, в. [1]), то препуштамо читаоцима на оцјену.

Велика помоћ код овог „путовања“ биле су нам на крају наведене књиге, чланци и интер-странице.

A) Првобитни доказ и неке његове варијације

Претпоставимо да су $p_1 = 2 < p_2 = 3 < \cdots < p_n$ сви прости бројеви.

(1) [Еуклид] Посматрајмо број $P_n = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Сваки прости дјелилац p броја P_n мора да буде различит од бројева $p_1, \ldots, p_n$. (Иначе би p морао да дијели број 1!) Тиме се добија да мора да постоји још један прости број.

Из овог доказа се индуктивно добија и једна (јако непрецизна) процјена n-тог простог броја: $p_n \leqslant 2^{(2^{n-1})}$.

(2) [Kummer] Код овог доказа се користи (мањи) број $Q_n = p_1 \cdot p_2 \cdot \ldots \cdot p_n - 1$ умјесто P_n.

(3) [Stieltjes] Замислимо производ $N_n = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ разложен на два фактора a и b, значи $N_n = a \cdot b$. Будући да ниједан прост број не дијели оба фактора, збир $a + b$ није дјељив ни са једним од постојећих простих бројева.

Еуклидов и Кумеров доказ сугеришу нека питања, до чијих је рјешења тренутно јако далеко. Дефинишимо сљедећа четири низа.

a) Нека је $a_1 = 2$. За $n \geqslant 1$ посматрајмо број $A_n = a_1 \cdot a_2 \cdot \ldots \cdot a_n + 1$ и означимо са a_{n+1}:

- **i)** најмањи, односно
- **ii)** највећи прости дјелилац броја A_n.

b) Полазећи од $b_1 = 3$ посматрајмо слична, али сада преко $B_n = b_1 \cdot b_2 \cdot \ldots \cdot b_n - 1$ изражена, два бесконачна низа простих бројева.

Вјероватно у оба случаја низови под **i)** садрже *све просте бројеве*. О низовима под **ii)** претпоставља се да у случају **a)** постоји *бесконачно много простих бројева* који се у њему *не јављају*, док су својства низа **b)** још увијек прилично непозната. (Али зна се да се у њему прости бројеви 7, 11, 13, 17, и 19 *не* појављују.)

B) Од релативно простих до простих бројева

Докази који ће сад услиједити темеље се на једноставној (у овом облику први пут од стране Hurwitz-a формулисаној) помоћној теореми.

Ако постоји бесконачан низ природних бројева, који су сви већи од 1 *и који су у паровима релативно прости, онда је скуп* $\mathcal{P}$ *свих простих бројева бесконачан.*

(Наиме, сваком природном броју додјељује се прости фактор одговарајућег члана низа.)

Обратите пажњу на то да се највећи заједнички делилац може одредити уз помоћ Еуклидовог алгоритма. Због тога познавање разлагања на просте факторе појединих чланова низа није потребно.

(1) [Goldbach] Фермаови бројеви $F_n = 2^{(2^n)} + 1$, $n \geqslant 0$, задовољавају услове помоћне теореме.

(Јер, потпуном индукцијом се лако докаже да вриједи $F_n = F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1} + 2$, $n \geqslant 1$. Због тога је за $0 \leqslant k < n$ број F_k један дјелилац броја $F_n - 2$. Ако би $d > 1$ био заједнички дјелилац бројева F_k и F_n, тада би d морало да дијели 2. Ово је, међутим, противрјечно, будући да су сви Фермаови бројеви непарни.)

(2) [Sylvester] Рекурзивно дефинисан низ $x_1 = 2$, $x_{n+1} = x_n^2 - x_n + 1$, $n \geqslant 1$, испуњава услове помоћне теореме.

(Јер се овдје потпуном индукцијом доказује да вриједи $x_{n+1} = x_1 \cdot x_2 \cdot \ldots \cdot x_n + 1$, $n \geqslant 1$.)

(3) Сада је блиско и питање да ли се идеје које се крију иза ова два доказа могу проширити. И заиста, вриједи сљедећа општија теорема.

За релативно просте природне бројеве a *и* b*, низ* $x_1 = a$*,* $x_{n+1} = x_1 \cdot x_2 \cdot \ldots \cdot x_n + b$*,* $n \geqslant 1$*, испуњава све услове помоћне теореме.*

(Доказ се може провести индуктивно и остаје читаоцу као задатак за вјежбање.)

Као још један начин уопштавања, могу се формирати и низови типа $x_1 \geqslant 2$, $x_{n+1} = x_n(x_n - 1)y_n + 1$, $n \geqslant 1$, који такође задовољавају услове помоћне теореме. (При томе је y_1, y_2, $\ldots$ прикладан низ природних бројева.) Примјер тога је $y_n = x_n$, односно рекурзија $x_{n+1} = x_n^2(x_n - 1) + 1$.

(4) [Schorn] За неки природан број $n \geqslant 2$ су два и два броја $n! \cdot i + 1$ и $n! \cdot j + 1$, $1 \leqslant i < j \leqslant n$, релативно проста.

(Јер, ако је $j = i + k$, $1 \leqslant k < n$, слиједи да је $n! \cdot j + 1 = (n! \cdot i + 1) + n! \cdot k$. Ово показује да (за свако n) мора постојати најмање n простих бројева.)

Значај *Фермаових простих бројева* (на питање да ли их има бесконачно много још није одговорено) за конструисање правилних многоуглова је познат још од Gauss-a. Испитивање да ли се неки конкретан број F_n може раставити на факторе, јесте проба за „супер-рачунаре“ (и од важности је за криптографију).

C) „Необични“ највећи заједнички дјелилац и бесконачно много простих бројева

Овај дио почињемо са два тврђења из теорије бројева која су и по себи интересантна. Нека су $a \geqslant 2$, $m, n \geqslant 1$ природни бројеви и нека је f_n n-ти *Фибоначијев број*. Највећи заједнички дјелилац бројева u и v означаваћемо са (u, v). Онда вриједи:

i) $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$ и

ii) $(f_m, f_n) = f_{(m,n)}$.

Оба тврђења се доказују помоћу Еуклидовог алгоритма. (Главне идеје су:

за **i)**: ако је $n = mq + r$ гдје је $q \geqslant 0$ и $0 \leqslant r < m$, вриједи да је $a^n - 1 = a^r(a^{mq} - 1) + (a^r - 1)$, из чега се добије да је $(a^m - 1, a^n - 1) = (a^n - 1, a^r - 1)$.

за **ii)**: сусједни Фибоначијеви бројеви су релативно прости и вриједи $f_{m+n} = f_{m-1}f_n + f_m f_{n+1}$, $m, n \geqslant 1$, из чега се добије $f_{(k+1)m} = f_{km-1}f_m + f_{km}f_{m+1}$ гдје је $m, k \geqslant 1$.)

(1) Узмимо да су $n-1$ бројева $p_2 = 3 < \cdots < p_n$ сви непарни прости бројеви. (При томе је $p_1 = 2$.) Онда су два и два од *Мерсенових бројева* $2^{p_1} - 1, \ldots, 2^{p_n} - 1$ релативно проста (узима се да је $a = 2$ у **i)**) и постоји најмање n непарних простих бројева (упореди помоћну теорему).

(2) Са бројевима $f_{p_1}, \ldots, f_{p_n}$ слично (помоћу **(ii)**) долазимо до противрјечности.

Значај *Мерсенових простих бројева* $M_p = 2^p - 1$ при карактеризацији парних савршених бројева је познат још од Euler-a. (Питање о бесконачности скупа таквих бројева је отворено.)

D) Бројеви са „довољно много“ простих фактора

Еуклидова теорема се може доказати и тако што се конструишу низови природних бројева чији чланови имају строго растући низ простих фактора.

(1) Низ $x_n = 2^{(2^n)} + 2^{(2^{n-1})} + 1$, $n \geqslant 1$, има претходно наведену особину. (Јер уз помоћ идентитета $a^4 + a^2 + 1 = (a^2 - a + 1)(a^2 + a + 1)$ слиједи за $a = 2^{(2^{n-1})}$: $x_{n+1} = (2^{(2^n)} - 2^{(2^{n-1})} + 1)x_n$, $n \geqslant 1$. Будући да су оба фактора већа од 1 и релативно проста, слиједи при $x_1 = 7$ да сваки члан низа x_n има барем n простих фактора.)

(2) Посматрајмо сада разлагање на просте факторе броја $n! = 1 \cdot 2 \cdot \ldots \cdot n$, $n \geqslant 2$, дакле $n! = \prod\limits_{p \leqslant n} p^{e_n(p)}$. (При томе се производ протеже на све просте

бројеве из интервала $[2, n]$.) Показујемо неједнакост $\prod_{p\leqslant n} {}^{p-1}\sqrt{p} > \dfrac{n}{e}$ и самим тиме бесконачност скупа $\mathcal{P}$ свих простих бројева.

Још од Legendre-a, позната је „компактна“ формула за одређивање експонената $e_n(p)$, и то $e_n(p) = \sum_{j\geqslant 1} \left\lfloor \dfrac{n}{p^j} \right\rfloor$. (При томе треба обратити пажњу на сљедеће: тачно $\lfloor n/p \rfloor$ фактора броја $n!$ су дјељиви са p, тачно $\lfloor n/p^2 \rfloor$ су још једном дјељиви са p, дакле са p^2, итд.) Због тога вриједи $e_n(p) \leqslant \sum_{j\geqslant 1} \dfrac{n}{p_j} = \dfrac{n}{p-1}$, из чега слиједи $\sqrt[n]{n!} \leqslant \prod_{p\leqslant n} {}^{p-1}\sqrt{p}$. Претпостављена неједнакост добија се из сљедеће процјене *Stirling*-овог типа: $\sqrt[n]{n!} > \dfrac{n}{e}$, односно у логаритмованом облику $\dfrac{1}{n}(\ln 2 + \cdots + \ln n) > \ln n - 1$.

(Будући да функција $y = \ln x$, $x > 0$, строго расте, вриједи, кад је $j = 2, \ldots, n$ да је $\ln j = (\ln j) \cdot 1 > \int_{j-1}^{j} \ln x\, dx$. Због тога је напокон

$$\ln 2 + \cdots + \ln n > \int_1^n \ln x\, dx = (x \ln x - x)|_1^n = n \ln n - n + 1 > n(\ln n - 1).)$$

(3) Нека је $f(x)$ неконстантни полином са цјелобројним коефицијентима. Тада из скупа $\{f(1), f(2), \ldots\}$ произлази бесконачно много простих фактора, односно простих бројева p, тако да је за одговарајући природни број N, вриједност полинома $f(N)$ дјељива са p.

Нека је $f(x) = a_n x^n + \cdots + a_1 x + a_0$, $n \geqslant 1$ и $a_n \neq 0$. Треба да буде $a_0 \neq 0$. (Тврђење за $a_0 = 0$ слиједи као код Еуклида – ставља се $N = p$.) Претпоставимо да скуп $\{f(1), f(2), \ldots\}$ садржи само коначно много простих дјелилаца $p_1, \ldots, p_r$ и посматрајмо бесконачни низ бројева $N_m = 2^m \cdot p_1 \cdot \ldots \cdot p_r \cdot a_0^2$, $m = 1, 2, \ldots$, за који вриједи (уз скраћеницу $q = 2^m \cdot p_1 \cdot \ldots \cdot p_r$) да је $f(N_m) = a_0(a_n a_0^{2n-1} q^n + \cdots + a_1 a_0 q + 1)$. Због тога што $|f(x)| \to \infty$ за $x \to \infty$, апсолутна вриједност заграде је за довољно велико m већа од 1, и према томе садржи барем један прости фактор, који мора бити различит од p_1 и p_r.

E) С оне стране еуклидског хоризонта

Горе наведене елементарне идеје јако брзо могу довести до тешких питања. Одговори су често дубоке теореме, из којих Еуклидова теорема произлази као једноставан закључак (због чега се само по себи разумије да више не можемо да говоримо о алтернативним доказима). При томе не можемо а да не поменемо сљедећа два резултата.

(1) [Dirichlet] Један интересантан посебан случај тачке **(3)** одељка **D)** чине линеарне функције $f(x) = dx + a$ ($a, d \in \mathbf{Z}$, $d \neq 0$), чије вриједности $f(1)$, $f(2)$, ... дају бесконачно много простих фактора. Овдје, додуше, вриједи један пуно значајнији резултат, а то је

Dirichlet-ова теорема. Нека је $a_n = dn + a$, $n = 0, 1, 2, \ldots$, строго растући (аритметички) низ цијелих бројева, при чему су бројеви a и d релативно

прости. Тада овај низ садржи бесконачно много простих чланова. (Тачније, вриједи чак и: свака класа остатака у $\mathbf{Z}_d^*$ садржи, грубо речено, „$\varphi(d)$-ти део свих простих бројева“.)

Доказаћемо сад, примјера ради, *два посебна случаја Дирихлеове теореме*, а то су:

(a) Постоји бесконачно много простих бројева облика $p = 3n + 2$.

Претпоставимо да постоји само коначно много таквих простих бројева, дакле $p_1 = 2, p_2 = 5, p_3 = 11, \ldots, p_N$. Тада је број $z = 3p_1 \cdot \ldots \cdot p_N - 1$ релативно прост са $p_1, \ldots, p_N$ и испуњава $z \equiv 2 \pmod 3$. z стога не може имати саме просте факторе q са $q \equiv 1 \pmod 3$! (Пошто n мора да буде непарно, доказали смо и да постоји бесконачно много простих бројева типа $p = 6m + 5$.)

(b) Далеко тежи је доказ да постоји и бесконачно много простих бројева облика $p = 6n + 1$. Њему се придодаје, сам по себи интересантан, исказ:

$(*)$ Сви прости фактори $p > 3$ тринома $x^2 + x + 1$, $x \in \mathbf{N}$, испуњавају $p \equiv 1 \pmod 6$.

(Јер, претпоставимо да је $p = 3m+2$ дјелилац од x^2+x+1. Сада, пак, p није дјелилац броја x и вриједи $(x-1)(x^2+x+1) \equiv 0 \pmod p$, што значи $x^3 \equiv 1 \pmod p$. Због тога се добије $x^{p-2} \equiv 1 \pmod p$, дакле $x^{p-1} \equiv x \pmod p$. Но, по „малој“ *Фермаовој теореми* је $x^{p-1} \equiv 1 \pmod p$. Због тога је $x \equiv 1 \pmod p$, из чега због $x^2 + x + 1 \equiv 3 \pmod p$ слиједи контрадикција $3 \equiv 0 \pmod p$. Стога мора да вриједи $p \equiv 1 \pmod 3$, дакле и $p \equiv 1 \pmod 6$.)

Опет претпостављамо да су $p_1 = 7, p_2 = 13, \ldots, p_N$ сви прости бројеви типа $p \equiv 1 \pmod 6$ и посматрамо сада број $z = w^2+w+1$, при чему је $w = p_1 \cdot \ldots \cdot p_N$. Из $w = 6k + 1$ се добије $z = 36k^2 + 18k + 3$, што значи $z \equiv 3 \pmod 9$. Због тога непарни број z није потпуни степен од 3, и z мора да садржи прости фактор $q > 3$, за којег због $(*)$ мора да буде испуњено $q \equiv 1 \pmod 6$. Али q је, у супротности са претпоставком, различит од свих $p_1, \ldots p_N$.

Даље примијећујемо да се исказ $(*)$ да уопштити на сљедећи начин: нека су p и q два проста броја, $p \neq q$. Ако је p дјелилац полинома $x^{q-1}+x^{q-2}+\cdots+x+1$, при чему $x \in \mathbf{N}$, онда вриједи $p \equiv 1 \pmod q$.

(Тако се може потврдити *бесконачно много других посебних случајева Дирихлеове теореме*, наиме да постоји бесконачно много простих бројева облика $p = qn + 1$, где је q дати прост број.)

За опште постављање проблема који са разних страна освјетљавају Дирихлеову теорему, желимо да укажемо на одговарајућу литературу, посебно на [13], главе 3, 4 и 6, и [15], главе III и IV. При томе се ради између осталог о питању полиномског „генерисања простих бројева“ (тј. да ли постоји полином с целобројним коефицијентима над скупом $\mathbf{N}$, односно $\mathbf{N}^n$, који као своје вриједности има бесконачно много, или чак све просте бројеве), и то:

(i) кроз полиноме $P(x)$ једне промјењиве и степена бар 2.

(Већ „безазлени“ полином $P(x) = x^2 + 1$ доводи до најтежих питања у вези са класама бројева $h(p)$ из квадратног поља $\mathbf{Q}(\sqrt{p})$, p прост.) До данас није

познат ниједан полином P за који скуп $P(\mathbf{N})$ садржи бесконачно много простих бројева, али се зна да се код неконстантних полинома међу бројевима $|P(n)|$, $n \in \mathbf{N}$, налази бесконачно много сложених.

(ii) кроз полиноме $P(x_1, \ldots, x_n)$ са коначно много промјењивих ($n \geqslant 2$). За такве полиноме су доказана многа дубока својства, од којих наводимо нека.

• Euler је показао да постоје одређени коефицијенти $d \in \mathbf{N}$ (он их је назвао „подобним“ бројевима [= numeri idonei]), за које вриједи: неки непарни број z је тачно онда прост када се може приказати у облику $z = x^2 + dy^2$ са $x, y \geqslant 0$ и НЗД$(x, dy) = 1$. (Данас је познато да постоји само коначно много таквих бројева.)

• Општије, вриједи чак: такозване примитивне квадратне форме $ax^2 + bxy + cy^2$ имају бесконачно много простих вриједности ако су a, b и c релативно прости.

• Када су апсолутне вриједности једног полинома $P \in \mathbf{C}[x_1, \ldots, x_n]$ над скупом $\mathbf{N}^n$ ($n \geqslant 1$) сами прости бројеви, онда је P константан.

• У вези са рјешењем *десетог Хилбертовог проблема*, чија је тема израчунљивост рјешења полиномских диофантских једначина, изведено је једно изненађујуће својство (Matijasevič, Putnam, Davis, Robinson):

Постоји полином $P(x_1, \ldots, x_n)$, такав да се *скуп његових позитивних вриједности* над скупом $\mathbf{N}^n$ *поклапа са скупом* $\mathcal{P}$ *свих простих бројева.* (Такви полиноми наведени су и експлицитно. При томе је за $n = 26$ степен полинома $d = 25$. Зна се такође да су величине бројева n и p „у директном односу“ једна према другој.)

(Осим тога је у овој области James 1982. године доказао завидну (мета-) теорему о теоријама $\mathbf{T}$ које се могу аксиоматизовати, а гласи: ако је неко тврђење P доказиво у $\mathbf{T}$, онда P изван $\mathbf{T}$ има „доказ“ који се састоји од 100 сабирања и множења целих бројева.)

Прије него што се посветимо даљим доказима Еуклидове теореме, треба споменути да је познати полином $P_{41}(x) = x^2 - x + 41$, који за $x = 0, 1, \ldots, 40$ даје саме просте бројеве, заједно са одговарајућим уопштењем $P_q(x) = x^2 - x + q$, повезан са једним интересантним проблемом факторизације: постоји тачно *девет* цијелих бројева d (тзв. *Hegner*-ових бројева), и то $d = 1, 2, 3, 7, 11, 19, 43, 67$ и 163, за које „цијели“ бројеви облика $a + b\sqrt{-d}$ дозвољавају јединствено растављање на просте факторе. (При томе су за $d = 1, 2$ бројеви a и b цијели, а у осталих седам случајева се за a и b морају дозвољавати и полуцијели бројеви – в. [6], стр. 251.) И управо за шест смислених цјелобројних вриједности $q = \frac{1+d}{4}$, наиме за $q = 2, 3, 5, 11, 17$ и 41, добију се, већ од Euler-а и Gauss-а претпостављени као једини могући полиноми $P_q(x)$.

(2) [Bertrand] Међу најтеже задатке теорије бројева убраја се проналажење „добрих“ функција $f\colon \mathbf{N} \to \mathbf{R}^+$ које гарантују да у интервалу $(n, n + f(n)]$ „увијек“ постоји један прост број (и то или за свако $n \geqslant 1$ или само за скоро свако $n \in \mathbf{N}$, тј. за свако $n \geqslant N_f$, при чему граница N_f зависи од f – при томе је додуше њено постојање осигурано, али у већини случајева није ефективно

израчунљиво). Сљедеће тврђење (за које је Erdös у узрасту од 19 година нашао посебно лијеп доказ, в. [1], глава 2) показује да је $f(n) = n$ једна таква функција.

Bertrand-ова теорема. За сваки природан број $n \geqslant 1$, постоји прост број међу бројевима $n+1$, $n+2$, ... , $2n$.

Из тога се изводи Еуклидова теорема, па слиједи: ако се умјесто n ставе редом 1, 2, 2^2, ... , 2^N, ... , тада је између свака два од ових бројева један прост број и скуп $\mathcal{P}$ је стога бесконачан. Осим тога се овако добија још увијек доста непрецизна процјена $p_n \leqslant 2^n$.

(Тренутно најбоље процјене n-тог простог броја дали су Rosser, Schoenfeld и Robin и оне гласе $n(\log n + \log\log n - \alpha) < p_n < n(\log n + \log\log n - \beta)$, при чему прва неједнакост вриједи са $\alpha = 1.0072629$ за свако $n \geqslant 2$, док друга вриједи за свако $n \geqslant 20$ кад је $\beta = 0.5$. На десној страни се може узети и $\beta = 0.9385$ када се ограничи да је $n \geqslant 7022$.)

У вези са напред помињаном функцијом f зна се, с једне стране, да је тренутно најбоља степена функција дата са $f(n) = n^{0.535+\varepsilon}$. (При томе је $\varepsilon > 0$ произвољно.) Она за скоро свако n даје интервале са траженим својством. С друге стране, може се показати и да постоји подскуп $M \subset \mathbf{N}$ густине 1, такав да чак сви интервали $[n, n + n^{1/6+\varepsilon}]$, $\varepsilon > 0$, за $n \in M$ садрже бар један прост број.

(Будући да су, за $N \geqslant 1$, сви узастопни бројеви $(N+1)!+2$, $(N+1)!+3$, ... , $(N+1)!+(N+1)$ сложени, непосредно се види да горе поменуте функције f морају бити неограничене.)

Претпоставља се и да између узастопних квадратних бројева леже увијек 2 проста броја, док између узастопних кубних леже четири.

Каткад интервали могу да буду и јако кратки, на пример, у случају *простих бројева близанаца* p и $p+2$, какви су 5 и 7 или 41 и 43. Још увијек се, додуше, не зна се да ли постоји бесконачно много таквих, али је Brun доказао запањујући резултат:

Збир $B = \sum_{(p,p+2)\in\mathcal{P}^2} \left(\frac{1}{p} + \frac{1}{p+2}\right)$, узет по свим простим паровима близанцима, конвергира (његова вредност B названа је *Бруновом константом*). Касније је компликованим методама аналитичке теорије бројева одређена и вриједност константе B. (Видјети о томе у [9], главе VII–IX, и [13], глава 4.)

F) Ојлеров доказ и једна његова варијација

Euler-у се приписује једноставан аналитички аргумент, који има значајне посљедице. Опет се претпоставља да постоји само n простих бројева p_1, ... , p_n.

(1) [Euler] Будући да сваки прост број p задовољава услов $1/p < 1$, бесконачни геометријски ред $1 + \frac{1}{p} + \frac{1}{p^2} + \cdots$ конвергира (и има збир $\frac{p}{p-1}$). Но тако слиједи

$$\left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots\right) \cdot \ldots \cdot \left(1 + \frac{1}{p_n} + \frac{1}{p_n^2} + \cdots\right) < \infty.$$

По основној теореми аритметике, сваки природни број z има јединствени приказ $z = p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$. Због тога се множењем добије да наведени производ n геометријских редова мора имати коначну вриједност $1 + \frac{1}{2} + \frac{1}{3} + \cdots$. (Ово, међутим, није могуће, јер хармонијски ред дивергира.)

(2) [Legendre] Сличан доказ се добије када се посматра n геометријских редова $1 + \frac{1}{p_j^2} + \frac{1}{p_j^4} + \cdots = \frac{p_j^2}{p_j^2 - 1}$ $(j = 1, 2, \ldots, n)$. Помоћу њих би се сада добило да сума $\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots$ има рационалну вриједност. (То је контрадикција, јер је $\zeta(2) = \pi^2/6$.)

G) Комбинаторни докази

Из претпоставке да постоји само коначно много простих бројева изводе се контрадикторне процјене величина теорије бројева. Посебно лијеп је сљедећи доказ који се користи *Ојлеровом φ-функцијом*, која за сваки природан број z рачуна број чланова скупа $\{1, 2, \ldots, z-1\}$ који су са z релативно прости. Опет се претпоставља да су $p_1 = 2$, $p_2 = 3$, … , p_r сви прости бројеви.

(1) За њихов производ $P = p_1 \cdot \ldots \cdot p_r$ би онда морало да вриједи $\varphi(P) = 1$, што је контрадикција са познатом формулом $\varphi(P) = (p_1 - 1) \cdot \ldots \cdot (p_r - 1) > 1$.

(2) Сваки природан број z се може написати у облику $z = z_1^2 \cdot k$, при чему је k број „слободан од квадрата“, тј. има представљање $k = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ са експонентима $e_j \in \{0, 1\}$ $(j = 1, \ldots, r)$. Но сада је $z_1 \leqslant \sqrt{z}$ и за k постоји највише 2^r могућности. Због тога за број z елемената скупа $\{1, 2, \ldots, z\}$ вриједи неједнакост $z \leqslant \sqrt{z} \cdot 2^r$, која је немогућа кад $z \to \infty$.

(Може се чак показати да удио α_n чланова скупа $\{1, 2, \ldots, n\}$ који су слободних од квадрата задовољава услов $\alpha_n \to 6/\pi^2 = 0.6079\ldots$ $(n \to \infty)$, тачније вриједи чак и $\alpha_n = \frac{6}{\pi^2} + o\Big(\frac{1}{\sqrt{n}}\Big)$, кад $n \to \infty$.)

(3) [Thue] Нека су $n, k \geqslant 1$ цијели бројеви за које треба да вриједи $(1+n)^k < 2^n$. Тада међу бројевима $1, 2, 3, \ldots, 2^n$ постоји бар $k+1$ прост.

Претпоставимо да постоји само r простих бројева, при чему је $r \leqslant k$. Сваки природан број z, $1 \leqslant z \leqslant 2^n$, има јединствено представљање $z = 2^{e_1} \cdot 3^{e_2} \cdot \ldots \cdot p_r^{e_r}$, при чему је $e_1 = n$ и $e_j = 0$ или је $0 \leqslant e_1 < n$, $0 \leqslant e_2 < n$, … , $0 \leqslant e_r < n$. Али из тога се добије за број свих посматраних бројева z, да би морало вриједити $2^n \leqslant 1 + n^r < (n+1)^r \leqslant (n+1)^k < 2^n$, што је контрадикција. (За $n = 2k^2$ слиједи због $1 + 2k^2 < 2^{2k}$, $k \geqslant 1$, да постоји најмање $k+1$ прост број мањи од $4^{(k^2)}$. Стога вриједи груба процјена $p_{k+1} < 4^{(k^2)}$.)

H) Fürstenberg-ов тополошки доказ

На скупу $\mathbf{Z}$ свих целих бројева се топологија може увјести на сљедећи начин.

За $a, b \in \mathbf{Z}$, $b > 0$, нека је $N_{a,b} = \{\, a + bn : n \in \mathbf{Z} \,\}$ (тј. $N_{a,b}$ је „обострано бесконачан“ аритметички низ). Скуп $O \subset \mathbf{Z}$ називамо отвореним када је или $O = \varnothing$ или када за свако $a \in O$ постоји $b > 0$, тако да вриједи $N_{a,b} \subset O$.

Из ове дефиниције се непосредно примјећује да је унија два отворена скупа O_1 и O_2 (па и коначно много њих) поново отворен скуп. Нека $a \in O_1 \cap O_2$. Тада постоји $b_1, b_2 > 0$ са $N_{a_1,b_1} \subset O_1$ и $N_{a_2,b_2} \subset O_2$. Слиједи да $a \in N_{a,b_1b_2} \subset O_1 \cap O_2$ и потребне карактеристике топологије су доказане.

Из њих слиједи да је:

(a) сваки непразни отворени скуп бесконачан;

(b) сваки скуп $N_{a,b}$ и затворен.

Само о **(b)** треба још мало размислити. Како је $N_{a,b} = \mathbf{Z} \setminus \bigcup_{k=1}^{b-1} N_{a+k,b}$ то је $N_{a,b}$ комплемент отвореног скупа.

Претпоставимо да је скуп $\mathcal{P}$ свих простих бројева коначан. Будући да сваки цијели број $z \neq \pm 1$ посједује један прости чинилац p, тј. садржан је у скупу $N_{0,p}$, слиједи да је $\mathbf{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathcal{P}} N_{0,p}$. Према **(b)** је због тога скуп $\mathbf{Z} \setminus \{-1, 1\}$ затворен. Онда је $\{-1, 1\}$ отворен скуп, што је у контрадикцији са **(a)**.

Закључак

На крају, вратимо се још једном теорији бројева.

У нади да смо овим прегледом једног малог дијела теорије простих бројева код читаоца пробудили интерес за познавањем тачних својстава „једноставних бројева“, примијетимо на крају да је Erdös на свој једноставан, али генијалан начин доказао бесконачност скупа $\mathcal{P}$, тако да се може извести још једна Euler-ова теорема, и то дивергенција реда $\sum_{p \in \mathcal{P}} \frac{1}{p}$. (В. [1], глава 1.)

Као завршетак желимо да понудимо сљедећи **задатак** (да, по у уводу цитираном ставу *Finkel*-а, читаоца позовемо да се „успне степеницама теорије бројева“): низ свих бројева облика $2^n - 3$, $n = 2, 3, \ldots$ садржи бесконачан подниз са члановима који су релативно прости у паровима. (В. такође [2], стр. 98–99.)

ЛИТЕРАТУРА

1. M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*, Springer-Verlag, Berlin-Heidelberg, 1998.
2. Š. Arslanagić, *Matematička indukcija*, Otisak, Sarajevo, 2001.
3. P. Basieux, *Die Top Ten der schönsten mathematischen Sätze*, Rowohlt Taschenbuch Verlag, Reinbeck bei Hamburg, 2000.
4. P. Baptist, *Pythagoras – und kein Ende?*, Ernst-Klett-Verlag, Leipzig-Stuttgart-Düsseldorf, 1997.
5. P. S. Bullen, D. S. Mitrinović and P. M. Vasić, *Means and Their Inequalities*, Reidel Publ., Dordrecht, 1988.
6. J. H. Conway and R.K. Guy, *Zahlenzauber*, Birkhäuser Verlag, Basel-Boston-Berlin, 1997.
7. А. Эвнин, *Девятнадцать доказательств теоремы Евклида*, Квант **32** (2001), 1, 35–38.

8. R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics*, Addison-Wesley Publ., Reading, Ma.-New York, 1989.
9. D. S. Mitrinović, J. Sándor and B. Crstici, *Handbook of Number Theory*, Kluwer Acad. Publ., Dordrecht-Boston-London, 1996.
10. L. J. Mordell, *Diophantine Equations*, Academic Press, London-New York, 1969.
11. I. Niven and H. S. Zuckermann, *Einführung in die Zahlentheorie*, Bd. I, Bibliograph. Inst., Mannheim-Wien-Zürich, 1976.
12. G. Pólya und G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, Bd. II, Springer-Verlag, Berlin-Heidelberg-New York, 1971.
13. P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York-Berlin-Heidelberg, 1971.
14. W. Schwarz, *Einführung in Methoden und Ergebnisse der Primzahlentheorie*, Bibliograph. Inst., Mannheim-Wien-Zürich, 1969.
15. E. Trost, *Primzahlen*, Birkhäuser Verlag, Basel-Stuttgart, 1968.
16. N. N. Worobjow, *Die Fibonnaccischen Zahlen*, Deutscher Verlag der Wissenschaften, Berlin, 1971.
17. E. W. Wiesstein, *CRC Concise Encyclopedia of Mathematics*, Chapman & Hall/CRC Boca Raton-London-New York-Washington D.C., 1999.
18. `http://www.mathworld.wolfram.com`
19. `http://www.utm.edu.research.primes`

Š. Arslanagić, Univerzitet u Sarajevu, Prirodno-matematički fakultet, Zmaja od Bosne 35, 71000 Sarajevo, Bosna i Hercegovina

E-mail: `asefket@pmf.unsa.ba`

W. Janous, Ursulinengymnasium, Fürstenweg 86, A-6010 Innsbruck, Österreich

E-mail: `walther.janous@tirol.com`

ОБАВЕШТЕЊА

СКУПШТИНА ДРУШТВА МАТЕМАТИЧАРА СРБИЈЕ

За време Републичког семинара о настави математике, у Нишу је 12.01.2008. године одржана редовна годишња **Скупштина Друштва математичара Србије**. На Скупштини је 88 делегата подружница и чланова Управног одбора усвојило извештаје о раду Друштва у претходној години које су поднели председник Друштва, Управни и Извршни одбор. За председника ДМС у наредном двогодишњем мандату поново је изабран

др Бранислав Поповић, доцент ПМФ у Крагујевцу.

Изабрани су и нови чланови Управног одбора Друштва из подружница које имају одговарајући број чланова.