Неке далекосежне хипотезе теорије бројева

Као што реч „хипотеза“ каже сама по себи, за тврђења која ћемо овде изнети под том класификацијом није до дана данашњег установљено да ли су тачна или нису (другим речима, њихов доказ немамо, али није нити ико пронашао ни контрапример, и обе могућности остају у оптицају до даљњег). Међутим, из одређених разлога ова тврђења (уз многа друга, јакако) мотивишу научнике да се њима подробније баве, уз наду да ће њихов статус једном коначно бити расветљен (живи били, па видели, мада су солидне шансе да нећемо, бар за оне који не верују у загробни живот).

1 *abc*-хипотеза

Хипотезу познату под називом *abc-хипотеза* поставили су француски математичар Joseph Oesterlé и британски математичар David Masser 1988, односно 1985. године. Пре него што је овде формулишемо, увешћемо неколико неопходних појмова.

Дефиниција 1.1. • Производ различитих простих бројева који деле задат природан број n називамо *радикал природног броја* n, и означавамо са $\mathrm{rad}(n)$; другим речима,

$$\mathrm{rad}(n) = \prod_{\substack{p \mid n \\ p \text{ је прост}}} p.$$

• За тројку узајамно простих природних бројева (a, b, c) кажемо да је *abc-тројка* акко важи $a + b = c$ и $\mathrm{rad}(abc) < c$.

Пример. • Тројка $(1, 8, 9)$ је *abc*-тројка. Заиста, важи $1 + 8 = 9$, и $\mathrm{rad}(1 \cdot 8 \cdot 9) = \mathrm{rad}(72) = \mathrm{rad}(2^3 \cdot 3^2) = 2 \cdot 3 = 6 < 9$.

• Показаћемо да важи и општије: тројка $(1, 9^n - 1, 9^n)$ је *abc*-тројка за ма који природан број n. Очигледно важи $1 + (9^n - 1) = 9^n$, па преостаје још проверити други услов. Приметимо, производ $1 \cdot (9^n - 1) \cdot 9^n$ можемо записати и као $8 \cdot 9^n \cdot \frac{9^n - 1}{8}$ (последњи чинилац је природан број због $9^n - 1 \equiv 1^n - 1 = 0 \pmod 8$, тј. $8 \mid 9^n - 1$). Дакле, због бројева 8 и 9^n, радикал овог производа садржи просте чиниоце 2 и 3 (сваки тачно по једном, по дефиницији радикала), као и све просте чиниоце који се појављују у броју $\frac{9^n - 1}{8}$, а њихов производ може бити највише баш $\frac{9^n - 1}{8}$. Све заједно:

$$\mathrm{rad}(1 \cdot (9^n - 1) \cdot 9^n) = \mathrm{rad}\left(8 \cdot 9^n \cdot \frac{9^n - 1}{8}\right) \leqslant 2 \cdot 3 \cdot \frac{9^n - 1}{8} = \frac{3}{4}(9^n - 1) < 9^n.$$

За тројку узајамно простих природних бројева (a, b, c) за које важи $a + b = c$ уведимо још ознаку

$$q(a, b, c) = \log_{\mathrm{rad}(abc)} c.$$

Приметимо, посматрана тројка је *abc*-тројка ако и само за ту тројку функција q има вредност већу од 1.

Сада смо спремни да формулишемо хипотезу. Прво ћемо навести тзв. „слабу“ верзију хипотезе.

Хипотеза 1.2 (*abc*-хипотеза, слаба верзија)**.** *Постоји константа C таква да за све тројке узајамно простих природних бројева (a, b, c) за које важи $a + b = c$ имамо $q(a, b, c) < C$.*

Напоменимо, највећа до сада позната вредност функције q износи приближно 1.62991, и достиже се за тројку

$$(2, 3^{10} \cdot 109, 23^5), \text{ тј. } (2, 6\,436\,341, 6\,436\,343).$$

Ову „рекордну“ тројку је пронашао Eric Reyssat још 1987. год., и од тада није надмашена наведена вредност функције q! С обзиром на овакав развој догађаја, природно је поставити и верзију хипотезе са експлицираном вредношћу константе C.

Хипотеза 1.3 (*abc*-хипотеза, слаба верзија, експлицитна)**.** *За све тројке узајамно простих природних бројева (a, b, c) за које важи $a + b = c$ имамо $q(a, b, c) < 2$.*

Сад ћемо формулисати и тзв. „јаку“ верзију хипотезе. Навешћемо три формулације за које није тешко видети да су међусобно еквивалентне.

Хипотеза 1.4 (*abc*-хипотеза, јака верзија)**.**

- *За сваки позитиван реалан број ε постоји само коначно много тројки узајамно простих природних бројева (a, b, c) за које важи $a + b = c$ и $c > \mathrm{rad}(abc)^{1+\varepsilon}$.*
- *За сваки позитиван реалан број ε постоји константа K_ε таква да, за све тројке узајамно простих природних бројева (a, b, c) за које важи $a + b = c$, имамо $c < K_\varepsilon \cdot \mathrm{rad}(abc)^{1+\varepsilon}$.*
- *За сваки позитиван реалан број ε постоји само коначно много тројки узајамно простих природних бројева (a, b, c) за које важи $a + b = c$ и $q(a, b, c) > 1 + \varepsilon$.*

На основу свега до сада реченог, вероватно није сасвим јасно зашто би *abc*-хипотеза уопште била занимљива људима који се баве теоријом бројева (или било коме генерално). Међутим, као што ћемо одмах видети, испоставља се да, колико год она апстрактно и (можда) неприродно деловала, читав низ разних (врло тешких) тврђења из теорије бројева, која на први поглед (па и на други, трећи...) немају никакве везе са *abc*-хипотезом, заправо се могу извести као њене последице.

Последица 1.5. *Претпоставимо да важи хипотеза 1.4. Тада једначина*

$$x^n + y^n = z^n$$

у скупу природних бројева има само коначан број решења за која важи $n > 3$ и НЗД$(x, y, z) = 1$ (приметимо, решења која нису овог облика не доносе ништа суштински ново, јер ако је (dx, dy, dz) решење за неко n, онда је и (x, y, z) решење за то n). Штавише, уколико важи хипотеза 1.3, тада горња једначина нема ниједно решење у скупу природних бројева за $n > 5$.

Доказ. Претпоставимо најпре да важи хипотеза 1.4. Претпоставимо да је (x, y, z) једна тројка за коју важи НЗД$(x, y, z) = 1$ и која испуњава постављену једначину за неко n, $n > 3$. С обзиром на $x^n + y^n = z^n$, дефинисана је функција $q(x^n, y^n, z^n)$, па можемо извести следећи рачун:

$$q(x^n, y^n, z^n) = \log_{\mathrm{rad}(x^n y^n z^n)} z^n = \log_{\mathrm{rad}(xyz)} z^n = n \log_{\mathrm{rad}(xyz)} z$$
$$\geqslant n \log_{xyz} z > n \log_{z^3} z = \frac{n}{3} \log_z z = \frac{n}{3} \geqslant \frac{4}{3}$$

(објашњење за неке кораке: при почетку смо користили $\mathrm{rad}(x^n y^n z^n) = \mathrm{rad}(xyz)$, што је очигледно по дефиницији радикала; неједнакост на почетку другог реда следи из неједнакости $\mathrm{rad}(xyz) \leqslant xyz$, имајући у виду да се знак мења ако неједнакост примењујемо у основи логаритма, а слично важи и за наредну неједнакост, због $x, y < z$; неједнакост на крају следи из претпоставке $n > 3$). На основу хипотезе 1.4 за $\varepsilon = \frac{1}{3}$ (најпогоднија је овде трећа верзија) следи да оваквих тројки (x^n, y^n, z^n) може бити само коначно много, а онда то важи и за тројке (x, y, z), што је и требало доказати.

Докажимо сада и други део поставке, уколико претпоставимо хипотезу 1.3 и $n > 5$. Тада на исти начин као горе добијамо $q(x^n, y^n, z^n) > \frac{n}{3} \geqslant 2$, што је управо у супротности са хипотезом 1.3. □

Ово на упечатљив начин демонстрира снагу *abc*-хипотезе, будући да из формулације 1.3 у свега неколико редова добијамо велику Фермаову теорему као последицу, а знамо да чувени Вајлсов доказ велике Фермаове теореме (једини досад познат доказ) запрема више од 100 страница текста и користи изразито дубоку „машинерију“. (Притом, претпостављени услов $n > 5$ не квари много слику, јер је велика Фермаова теорема за $n = 5$ свакако доказана чак 1825. године, а за $n = 3$ и $n = 4$ још и раније, у 18. и 17. веку, респективно.)

Међутим, можда ово и даље није довољно убедљив показатељ значаја *abc*-хипотезе, јер за велику Фермаову теорему ипак већ знамо да је тачна, па можда може бити упитно од каквог је значаја њено алтернативно извођење преко *abc*-хипотезе. У наставку наводимо, илустрације ради, неколико одабраних отворених проблема за које се може показати (што овде не чинимо) да су последица *abc*-хипотезе. Као што се може приметити, на основу саме формулације ових проблема (а и многих других које овде не наводимо) заиста је практично недокучиво у каквој су они вези са *abc*-хипотезом, а ипак се испоставља да јесу.

Последица 1.6. *Кажемо да је природан број* квадратно засићен *акко се сваки прост чинилац у његовој факторизацији јавља са експонентом бар* 2. *Хипотеза 1.4 имплицира да постоји бесконачно много тројки узастопних природних бројева који су сви квадратно засићени.*

Последица 1.7. *Прости бројеви p за које важи $p^2 \mid 2^{p-1} - 1$ називају се* Виферихови (Wieferich) прости бројеви. *Хипотеза 1.4 имплицира да постоји бесконачно много простих бројева који нису Виферихови.*

Напомена. Чини се да су Виферихови прости бројеви врло ретки: до данас су позната свега два, 1093 и 3511, и то су и једини постојећи мањи од $6.7 \cdot 10^{15}$. Ипак, постоје одређени разлози (повезани са униформном

дистрибуцијом корена јединице у модуларној мултипликативној групи целих бројева) због којих се претпоставља да Виферихових простих бројева заправо има бесконачно много, но ово је тренутно отворен проблем. Међутим, такође није познато ни да ли постоји бесконачно много простих бројева који *нису* Виферихови (тј. теоријски је могуће и да, без обзира на њихову привидну реткост, *сви* прости бројеви од неке тачке па надаље буду Виферихови!); горња последица решава ово питање под *abc*-хипотезом. (Приметимо још, тривијално, да бар једна од те две групације заиста мора бити бесконачна.)

Последица 1.8. *Хипотеза 1.4 имплицира да постоји само много четворки природних бројева* (x, y, p, q)*,* $x, y, q > 1$*,* $p > 2$*, за које важи*

$$\frac{x^p - 1}{x - 1} = y^q.$$

Напомена. Приметимо, уколико израз са леве стране запишемо у систему са базом x, добијамо број $\underbrace{11\ldots11}_{p \text{ пута}}{}_{(x)}$. Дакле, тврђење из горње последице се може и преформулисати: постоји само коначно много потпуних степена који се у некој бази записују искључиво помоћу цифре 1 (наравно, под претпоставком *abc*-хипотезе; без ње је ово тврђење отворен проблем, с тим што се зна да јесте тачно уколико уместо потпуних степена тражимо само потпуне квадрате).

2 Шинцелова хипотеза H

Пољски математичар Andrzej Schinzel поставио је 1958. године хипотезу која се данас у његову част назива *Шинцелова хипотеза H* (где слово H у називу потиче одатле што ју је сам Шинцел тако означио у раду у ком ју је поставио). Дајемо одмах формулацију.

Хипотеза 2.1 (Шинцелова хипотеза H)**.** *Нека су* $f_1(x), f_2(x), \ldots, f_k(x)$ *несводљиви полиноми са позитивним водећим коефицијентима чије су вредности целобројне за ма који целобројан аргумент. Означимо*

$$Q(x) = \prod_{i=1}^{k} f_i(x).$$

Претпоставимо да не постоји прост број p *такав да* $p \mid Q(x)$ *за сваки цео број* x*. Тада постоји бесконачно много целих бројева* m *таквих да су све вредности* $f_1(m), f_2(m), \ldots, f_k(m)$ *прости бројеви.*

Пример. Посматрајмо полиноме $f_1(x) = x$ и $f_2(x) = x + 1$. За њих важи $Q(x) = x(x + 1)$. Међутим, приметимо да је израз $x(x + 1)$ паран за сваки цео број x; другим речима, имамо $2 \mid Q(x)$ за све целе x, па за прост број p из формулације хипотезе можемо узети $p = 2$. Према томе, овај пар полинома *не* испуњава претпоставке Шинцелове хипотезе H (јер је претпоставка да такав прост број *не* постоји), па на овај пар не можемо применити хипотезу.

Погледајмо сада на примеру и како се хипотеза успешно може применити. Ова хипотеза за последице има читав низ тврђења у којима се наводи постојање простих бројева одређеног облика (а која су без ове хипотезе отворени проблеми, по правилу врло тешки), а има и неке последице у чијој се формулацији не види одмах веза с простим бројевима. За илустрацију, показаћемо како се из ове хипотезе може врло брзо извести постојање бесконачног броја парова простих близанаца (о којима је било речи раније). За још неке примере погледати скорашње писмене испите (конкретно, не само задатке где се помиње Шинцелова хипотеза H, него и оне где се помиње Диксонова хипотеза, будући да је она, као што ћемо ускоро видети, специјалан случај Шинцелове).

Последица 2.2. *Уколико претпоставимо да важи Шинцелова хипотеза* H*, тада постоји бесконачно много парова простих близанаца.*

Доказ. Посматрајмо полиноме $f_1(x) = x$ и $f_2(x) = x + 2$. Тврдимо да они испуњавају услове хипотезе. Заиста, они су очито несводљиви, имају позитивне водеће коефицијенте, и имају целобројне вредности за целобројне аргументе (ово последње је тривијално испуњено јер су им коефицијенти из $\mathbb{Z}$). Покажимо још и испуњеност услова који се тиче полинома Q.

Имамо $Q(x) = x(x+2)$. Претпоставимо супротно: за неки прост број p важи $p \mid x(x+2)$ за сваки цео број x. Приметимо, за $x = -1$ имамо $Q(-1) = -1$, а ово није дељиво ниједним простим бројем; дакле, такав прост број p не може постојати. (Ако се неко не досети да убаци вредност $x = -1$, ово није једини пут ка решењу. Можемо убацити и нпр. $x = 1$, за шта добијамо $Q(1) = 3$, што значи да је једини прост број p који „има шансе да ради“ број 3, сви остали отпадају због $x = 1$; с друге стране, за број 3 имамо $3 \nmid Q(2) = 8$, па отпада и могућност $p = 3$ због $x = 2$, те не преостаје ниједна могућност за p. Ово су само неки примери могућег закључивања, слична идеја се може реализовати на много начина.)

Према томе, испуњени су сви услови, па можемо применити Шинцелову хипотезу H. Хипотеза нам даје да постоји бесконачно много целих бројева m таквих да су $f_1(m)$ и $f_2(m)$ истовремено прости бројеви, тј. да су m и $m + 2$ истовремено прости бројеви, а ово управо значи да постоји бесконачно много парова простих близанаца. □

Напомена. Приметимо још, услов из формулације хипотезе „чије су вредности целобројне за ма који целобројан аргумент“ јасно испуњавају сви полиноми са целобројним коефицијентима (што је био случај у претходној последици, а и у пракси су посматрани полиноми најчешће управо такви), међутим има и полинома чији коефицијенти нису целобројни а који ипак испуњавају овај услов. На пример, такав је полином $\frac{x^2}{2} + \frac{x}{2}$ (те, дакле, и он може бити међу полиномима на које желимо да применимо Шинцелову хипотезу H).

2.1 Диксонова хипотеза

Један специјалан случај Шинцелове хипотезе H, а који је већ сам за себе прилично моћан, формулисао је 1904. године амерички математичар Leonard Eugene Dickson, па се у његову част назива *Диксонова хипотеза*. Формулација је готово идентична Шинцеловој, уз додатно ограничење да су сви полиноми $f_1, f_2, \ldots, f_k$ линеарни (у овом случају, наравно, није потребно посебно захтевати да посматрани полиноми морају бити несводљиви, будући да је то за линеарне полиноме аутоматски задовољено).

Приметимо, за последицу 2.2 нам није била неопходна „пуна снага“ Шинцелове хипотезе H, већ се иста последица могла извести (на идентичан начин) и само уз претпоставку Диксонове хипотезе.

Доказ Диксонове хипотезе (а тиме и Шинцелове, поготово) тренутно делује далеко изван домета садашњих алата теорије бројева. Но, поменимо ипак да постоји и један доказан случај Диксонове хипотезе, а то је случај $k = 1$. Тада се Диксонова хипотеза тачно своди на (раније виђену) Дирихлеову теорему о простим бројевима у аритметичким прогресијама. Заиста, уколико имамо само један линеаран полином, рецимо $f(x) = ax + b$, тада важи $Q(x) = f(x) = ax + b$, и услов да не постоји прост број p такав да $p \mid ax + b$ за све целе x управо је еквивалентан са НЗД$(a, b) = 1$ (што је био услов код Дирихлеове теореме).