**СТАТИЈАТА ПРВ ПАТ Е ОБЈАВЕНА ВО СПИСАНИЕТО ТАНГЕНТА ВО 1995/96 ГОДИНА**

# ПРОСТИ БРОЈЕВИ

др Ратко Тошић, Природно-математички факултет, Нови Сад

> I know numbers are beautiful. If you don't see why, someone can't tell you. If they aren't beautiful, nothing is.
>
> Paul Erdös

## Увод

У основи математике лежи аритметика – теорија природних бројева. У теорији бројева има много дубоких и лепих теорема, а такође и мноштво тешких и до сада нерешених проблема који стотинама година одолевају настојањима највећих математичара. Многи делови савремене математике настали су као резултат решавања и уопштавања проблема из теорије бројева. Карл Фридрих Гаус (1777–1855), који је учинио многа важна открића у математици, рекао је: "Математика је краљица наука, теорија бројева је краљица математике."

Бројеви су фасцинирали људе од најранијих почетака цивилизације. Питагора је открио да музичка хармонија зависи од односа целих бројева и закључио је да је све у природи број. Према Плутарху, Ксенократ је израчунао да је број слогова који се могу формирати од слова грчке азбуке једнак 1002000000000. То је први забележен покушај решавања неког тешког комбинаторног проблема који се односи на бројеве. У једном проблему који је поставио Архимед (проблем о биковима) као решење појављује се број који се у децималној нотацији (која није била позната Архимеду) записује помоћу 206545 цифара. Да би се наштампао тај број потребна је читава књижица од 50 страница. Леополд Кронекер (1823–1891) рекао је да је бог створио целе бројеве а све остало је дело човека. Управо на примеру теорије бројева најбоље се потврђује мисао да добра математика никад не застарева. Док Аристотелова физика са данашње тачке гледишта изгледа примитивна и рудиментарна, Архимедова и Еуклидова математика још увек блиста пуним сјајем.

Ниједна грана математике није толико омиљена код аматера као теорија бројева. У исто време, ниједна грана математике није постављала толико замки и проузроковала толико неуспеха и код највећих математичара. Од почетка рачунарске ере, програмери тестирају своје способности, квалитет својих програма и моћ рачунара решавајући проблеме из теорије бројева и откривајући разне куриозитете у тој области.

Заинтересовани читалац може да се позабави решавањем задатака датих на крају овог чланка. Решења задатака објавићемо у неком од наредних бројева часописа.

# Неки основни појмови

У скупу целих бројева, један од основних појмова је *дељивост*.

Нека су $a$ и $b$ цели бројеви. Ако постоји цео број $m$ такав да је $b = ma$, онда кажемо да је $a$ *делитељ* или *фактор* броја $b$ а да је $b$ *садржалац* или *умножак* броја $a$. То записујемо са $a|b$. На пример, $5|15$, $7|28$, $5|0$.

Ако је $a|b$, очигледно је и $a|(-b)$, $(-a)|b$ и $(-a)|(-b)$. Зато се, при разматрању дељивости, најчешће ограничавамо на ненегативне целе бројеве, при чему се једино број 0 не појављује као делитељ.

Кажемо да је $a$ *прави делитељ* од $b$, ако је $a|b$ и $a \neq b$.

Позитиван цео број $p$ већи од 1 је *прост* ако су му једини позитивни делитељи бројеви 1 и $p$. За позитиван цео број који није прост, кажемо да је *сложен*. Сваки сложен број $n$, дакле, има делитељ различит од 1 и $n$.

Нека су $a$ и $b$ ненегативни цели бројеви од којих је бар један већи од нуле. За број $k$ кажемо да је *заједнички делитељ* бројева $a$ и $b$ ако је $k|a$ и $k|b$. Највећи позитиван цео број који је делитељ и од $a$ и од $b$, назива се *највећи заједнички делитељ* бројева $a$ и $b$. Означавамо га са $NZD(a,b)$.

На пример, $NZD(4,20) = 4$, $NZD(0,5) = 5$, $NZD(30,80) = 10$, $NZD(8,15) = 1$.

Постоји врло једноставан алгоритам за одређивање највећег заједничког делитеља два броја. Алгоритам потиче од старогрчког математичара Еуклида, који је живео око 300. године пре нове ере. По њему је и добио назив *Еуклидов алгоритам*. О томе алгоритму детаљније ће бити речи другом приликом.

За два цела броја $a$ и $b$, при чему је бар један различит од нуле, рећи ћемо да су *узајамно прости* ако је $NZD(a,b) = 1$. На пример, бројеви 14 и 25 су узајамно прости, као и бројеви 8 и 15.

Нека су $a_1, a_2, \ldots, a_n$ ненегативни цели бројеви, при чему је бар један различит од нуле. За највећи позитиван број $d$, који је делитељ свих тих бројева, кажемо да је њихов *највећи заједнички делитељ*. Означавамо га са $NZD(a_1, a_2, \ldots, a_n)$. Нека су $a_1, a_2, \ldots, a_n$ цели бројеви, при чему је бар један различит од нуле. Ако је $NZD(a_i, a_j) = 1$, за $1 \leq i < j \leq n$, кажемо да су бројеви $a_1, a_2, \ldots, a_n$ *по паровима узајамно прости*. Ако је $NZD(a_1, a_2, \ldots, a_n) = 1$, онда су бројеви $a_1, a_2, \ldots, a_n$ *узајамно прости*. На пример, бројеви 6, 10 и 15 су узајамно прости али нису по паровима узајамно прости. То важи и за бројеве 6, 15 и 35. Бројеви 18, 25 и 77 су по паровима узајамно прости.

За цео број $k$ кажемо да је *заједнички садржалац* целих бројева $a$ и $b$ ако је $a|k$ и $b|k$. Најмањи позитиван цео број $m$ који је заједнички садржалац бројева $a$ и $b$ је *најмањи заједнички садржалац* тих бројева. Обележавамо га са $NZS(a,b)$. Јасно је да је

$$NZS(a,b) = NZS(-a,b) = NZS(a,-b) = NZS(-a,b).$$

Најмањи заједнички садржалац више бројева дефинише се као најмањи позитиван цео број који је садржалац сваког од њих.

Једно од најважнијих тврђења у теорији бројева је *основна теорема аритметике* која тврди да се сваки цео број већи од 1 може представити као производ простих бројева и то на један једини начин до на поредак фактора. Другим речима, сваки цео број већи од 1 може се на јединствен начин представити у облику

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

где су $p_i$ прости бројеви и $\alpha_i > 0$, за $i = 1, 2, \ldots, k$; $p_1 < p_2 < \cdots < p_k$. За такво представљање кажемо да је *канонски облик* броја $n$. Из практичних разлога, међутим, ми узимамо да је $\alpha_i \geq 0$, јер онда било који прост број може формално да фигурише у канонском представљању неког броја.

## Ератостеново сито

Као што смо видели, сви природни бројеви се могу разврстати у три класе: просте, сложене и број 1, који није ни прост ни сложен. Прости бројеви се могу окарактерисати и као бројеви који имају тачно два делитеља.

Проблем добијања потпуне листе простих бројева мањих од датог броја $n$, заокупљао је пажњу математичара вековима. Један поступак за утврђивање простоте датог броја и налажење свих простих бројева мањих од датог броја $n$, дао је старогрчки математичар Ератостен. Пре него што опишемо његов алгоритам, доказаћемо следеће тврђење.

**ТЕОРЕМА 3** *Позитиван цео број $n$ је сложен ако и само ако има прост фактор $p$, такав да је $p \leq \sqrt{n}$.*

**ДОКАЗ** Ако $n$ има прост фактор $p \leq \sqrt{n}$, онда је $n$, очигледно, сложен број.

Обрнуто, ако је $p$ најмањи прост фактор сложеног броја $n$, тада је $n = pm$, за неки цео број $m$ и при томе је $m \geq p$. Следи да је $p \leq \sqrt{n}$. □

Горње тврђење може се формулисати и на следећи начин:

*Позитиван цео број $n > 1$ је прост ако и само ако не садржи прост фактор $p \leq \sqrt{n}$.*

На овоме критеријуму се и заснива Ератостенов алгоритам, познат и под називом *Ератостеново сито*, по Ератостену из Кирене, који га је први применио у 3. веку пре нове ере.

Ератостенов алгоритам, мало модификован, састоји се у следећем:

1. *Исписати у низ све природне бројеве од 2 до $n$.*

2. *Уочити у низу први број који није ни подвучен ни прецртан и подвући га а затим прецртати све његове умношке у низу.*

3. *Ако су сви бројеви низа означени (подвучени или прецртани), поступак је завршен; у противном, применити корак 2.*

По завршетку рада, добијамо све просте бројеве не веће од $n$. То су подвучени бројеви.

Ако нам је циљ само да утврдимо да ли је број $n$ прост или сложен, горњи алгоритам треба мало модификовати. Теорема 1 нам у том случају казује да се процес завршава или кад је прецртан број $n$ (у ком случају је $n$ сложен број), или кад за први следећи број $p$ који треба подвући важи $p^2 > n$ (у ком случају је $n$ прост број).

Ератостен из Кирене (око 276 – 194. године пре нове ере) школовао се у Александрији и Атини. Руководио је александријском библиотеком. Био је у врло пријатељским односима са Архимедом. Поред математике, бавио се астрономијом, филологијом, филозофијом, географијом, музиком. Поставио је основе математичке географије; први је нашао метод за мерење дужине лука меридијана. Пронашао је прибор за конструктивно решење проблема удвостручења коцке (мезолабиј). Ератостеново сито описано је у 13. глави прве књиге "Увод у аритметику" Никомаха из Герасе (1. век наше ере). Поступак се разликује од горе изложеног само у томе што се одмах полази од низа непарних бројева.

## Бесконачност скупа простих бројева

Поменимо још и безуспешне покушаје многих математичара да се нађе општа формула за просте бројеве, тј. функција $f(n)$ чије би вредности, за све целобројне вредности од $n$, биле прости бројеви. На пример, функција $f(n) = n^2 - 79n + 1601$ даје просте бројеве за $0 \leq n \leq 79$, али "отказује" за $n = 80$, јер је $f(80) = 80^2 - 79 \cdot 80 + 1601 = 1681 = 41^2$ сложен број. Читалац који воли да ради са рачунаром, лако ће проверити ово тврђење.

У вези са "ловом" на формуле које дају просте бројеве, свакако је интересантно поменути Фермаову погрешну хипотезу. Он је изучавао бројеве облика $f_n = 2^{2^n} + 1$, где је $n$ произвољан цео ненегативан број. Такви бројеви су по њему добили име *Фермаови бројеви*. За првих 5 вредности од $n$, он је добио редом бројеве $f_0 = 3, \quad f_1 = 5, \quad f_2 = 17, \quad f_3 = 257, \quad f_4 = 65537$ и провером утврдио да су сви они прости. Ферма је изрекао хипотезу да је и за сваки природан број $n \geq 5$, број $f_n$ прост. Међутим, Ојлер је показао да је број $f_5$ производ два проста броја:

$$f_5 = 4294967297 = 641 \cdot 6700417.$$

Са данашње тачке гледишта изгледа чудно да за математичаре у 17. и 18. веку није било лако да утврде да ли је неки десетоцифрени број прост. Лако је поделити 4294967297 са 641 или било којим другим целим бројем; међутим, како је $65536^2 < 4294967297 < 65537^2$, следи да би за проверу простоте броја $f_5$, по критеријуму из Теореме 1, било потребно испитати дељивост броја $f_5$ са свим простим бројевима мањим од 65537. У време кад нису постојале довољно ефикасне рачунске машине, па чак ни довољно велике таблице простих бројева, то је био прилично мукотрпан посао. Треба рећи да се и ми данас налазимо пред сличним тешкоћама кад треба да тестирамо на простоту неки 200–цифрени

број, или кад треба да извршимо његову факторизацију, без обзира на чињеницу да располажемо неупоредиво моћнијим средствима за рачунање. Брза факторизација великих бројева нема само теоријски значај него налази и практичну примену, на пример, у криптоанализи. Што се самих Фермаових бројева тиче, без обзира да ли су прости или сложени, показало се да имају низ врло интересантних својстава. Следећа теорема односи се на једно такво својство.

**ТЕОРЕМА 4** *Свака два различита Фермаова броја су узајамно прости.*

**ДОКАЗ** У доказу ћемо користити специјалан случај ($a = 2$, $b = 1$) идентитета познатог из средњошколске математике:

$$a^n - b^n = (a + b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots - b^{n-1}),$$

који важи за сваки позитиван паран број $n$.

Нека су $f_n$ и $f_{n+k}$, $k > 0$, два различита Фермаова броја. Претпоставимо да је $m$ цео позитиван број, такав да је $m|f_n$ и $m|f_{n+k}$. Нека је $x = 2^{2^n}$. Тада је

$$\frac{f_{n+k} - 2}{f_n} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k-1} - x^{2^k-2} + \cdots - 1,$$

па је $f_n|(f_{n+k} - 2)$. Следи да је $m|(f_{n+k} - 2)$. Како је и $m|f_{n+k}$, то је $m|2$. Међутим, Фермаови бројеви су непарни, па је $m = 1$, одакле следи тврђење. □

Пјер Ферма (Pierre de Fermat, 1601–1665), француски математичар. По образовању је био правник и зарађивао је за живот бавећи се адвокатуром. Математиком се бавио из љубави, као "аматер". Један је од оснивача теорије вероватноће. Неколико теорема из теорије бројева носе његово име. Један од проблема који је поставио (Фермаова велика теорема) остао је нерешен преко 300 година (све до прошле године) али су покушаји његовог решавања од стране многих великих математичара имали за резултат многа значајна открића у математици.

Питање простоте Фермаових бројева појављује се и у вези са проблемом конструкције правилних многоуглова помоћу шестара и лењира. Гаус је доказао следеће тврђење:

**ГАУСОВА ТЕОРЕМА** *Правилан многоугао са $n$ страница може се конструисати шестаром и лењиром ако и само ако је $n$ природан број облика $n = 2^s p_1 p_2 \dots p_k$, где је $s$ ненегативан цео број а $p_1$, $p_2$, $\dots$, $p_k$ различити Фермаови прости бројеви или је $n = 2^s$, где је $s$ цео број већи од 1.*

Ово Гаусово откриће утицало је на то да се повећа интерес за изучавање Фермаових бројева. Међутим, све до данас није пронађен ни један прост Фермаов број већи од $f_4$.

Карл Фридрих Гаус (Karl Friedrich Gauss, 1777–1855), немачки математичар кога су савременици називали "краљем математичара" (princeps mathematicorum). Његов математички таленат испољио се у раном детињству. Гаус је, сећајући се свог детињства, говорио у шали: "Научио сам да рачунам пре него да говорим." Родио се у Брауншвајгу. Више образовање стекао је на Универзитету у Гетингену, где је затим провео 50 година. Био је директор опсерваторије у Гетингену а на универзитету је предавао математику и астрономију. Као деветнаестогодишњи студент направио је значајно откриће: дао је дефинитиван одговор на питање за које $n$ је могуће конструисати шестаром и лењиром правилан $n$–угао. Специјално, решавањем једначине $x^{17} - 1 = 0$, доказао је могућност конструкције правилног 17–угла. Гаус је доказао основну теорему алгебре о постојању решења алгебарске једначине $n$–тог степена. У свом делу "Аритметичка истраживања" (Disquisitiones Arithmeticae) поставио је темеље савремене теорије бројева. Бавио се и астрономијом, теоријом магнетизма и оптиком.

Лако се проверава да међу првих 20 природних бројева има осам простих док их међу првих 20 троцифрених бројева (од 100 до 119) има само пет. Природно се поставља питање: да ли су почев од неког природног броја сви природни бројеви сложени, тј. да ли је број простих бројева коначан? Одговор на то питање дао је Еуклид. Следећа теорема, заједно са доказом, укључена је у његову књигу "Елементи". Ми ћемо овде изложити два доказа Еуклидове теореме. Први је оригинални Еуклидов, други је дао мађарски математичар Ђерђ Поја (G. Pólya, 1887–1985).

**ТЕОРЕМА 5** *Број простих бројева је бесконачан.*

**ДОКАЗ 1** Претпоставимо да је број простих бројева коначан и нека су $p_1, p_2, \ldots, p_n$ сви прости бројеви, при чему је $p_n$ највећи од њих. Посматрајмо број

$$q = p_1 p_2 \cdots p_n + 1.$$

Број $q$ није дељив ни са једним од простих бројева $p_1, p_2, \ldots, p_n$, јер при дељењу са сваким од њих даје остатак 1. Како је $q > 1$, следи да је $q$ прост број већи од $p_n$ или је сложен број који има прост фактор већи од $p_n$. У оба случаја долазимо у контрадикцију са претпоставком да је $p_n$ највећи прост број. Дакле, број простих бројева не може бити коначан. □

**ДОКАЗ 2** Из Теореме 2 следи да је сваки од Фермаових бројева дељив неким непарним простим бројем који није делитељ ниједног другог Фермаовог броја. Зато из претпоставке да је број простих бројева коначан, следи да је и број Фермаових бројева коначан, што је контрадикција. Дакле, број простих бројева је бесконачан. □

Сваки прост број већи од 2 је непаран, а сваки непаран број је или облика $4k-1$ или облика $4k+1$, за неки ненегативан цео број $k$. Следи да бар у једној од ове две класе има бесконачно много простих бројева. Уствари, може се доказати да свака од те две класе садржи бесконачно много простих бројева. Доказ те чињенице за просте бројеве облика $4k - 1$ је једноставан (видети задатак 2),

уз коришћење аргумената сличних оним у Еуклидовом доказу Теореме 5; то, међутим, није случај кад се ради о класи бројева облика $4k+1$.

Општији проблем је следећи: Нека су $a$ и $m$ узајамно прости природни бројеви. Да ли има бесконачно много простих бројева облика $a+km$, где је $k$ природан број? Наводимо без доказа познато тврђење које даје одговор на то питање.

**ДИРИХЛЕОВА ТЕОРЕМА** *Нека су $a$ и $m$ узајамно прости природни бројеви. Тада аритметичка прогресија*

$$\{a,\ a+m,\ a+2m,\ a+3m,\ \ldots\}$$

*садржи бесконачно много простих бројева.*

Петер Густав Лежен Дирихле (P. G. L Dirichlet, 1805–1859), немачки математичар, рођен у Дирену. Од 1822. до 1827. године радио је као домаћи учитељ у Паризу. Био је доцент у Вроцлаву, затим професор Универзитета у Берлину а после смрти Гауса, у Гетингену. Постигао је дубоке и фундаменталне резултате у теорији бројева. Значајни су, такође, његови радови у механици и математичкој физици, посебно теорији потенцијала. Његова предавања имала су огроман утицај на Г. Римана, Ф. Ајзенштајна, Л. Кронекера, Р. Дедекинда и друге познате математичаре.

Голдбах је 1742. године изрекао хипотезу да се сваки паран број већи од 2 може представити у облику збира два проста броја а да се сваки непаран број већи од 7 може представити као збир три непарна проста броја. И. М. Виноградов (1891– 1983) је 1937. године аналитичким методама доказао тачност тога тврђења за довољно велике непарне бројеве, тј. за све непарне бројеве веће од неког великог броја $N_0$.

У теорији бројева има много нерешених проблема који се односе на просте бројеве а који су врло једноставни по формулацији. Не зна се, на пример, да ли између свака два узастопна потпуна квадрата $n^2$ и $(n+1)^2$ постоји прост број. Исто тако, не знамо да ли има бесконачно много простих бројева облика $(2n)^2+1$. Кронекер (L. Kronecker, 1823–1891) је претпоставио, али то никад није доказано, да се сваки позитиван паран број може представити као разлика два проста броја на бесконачно много начина. Ако би то било тачно онда би се потврдила и хипотеза да има бесконачно много парова *простих бројева близанаца*, тј. парова простих бројева који се разликују за 2. На пример, прости бројеви близанци су 3 и 5, 5 и 7, 11 и 13, 101 и 103, 1000000000061 и 1000000000063.

## Мерсенови бројеви

Следећа теорема даје један потребан али не и довољан услов да би број облика $2^n-1$ био прост. У доказу теореме користићемо специјалан случај ($a=2^r$, $b=1$) познатог идентитета, који важи за сваки природан број $n$:

$$a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\cdots+b^{n-1}).$$

**ТЕОРЕМА 6** *Ако је $n$ природан број и $2^n - 1$ прост, онда је и $n$ прост број.*

**ДОКАЗ** Доказаћемо еквивалентно тврђење, тј. да је $2^n - 1$ сложен број, ако је $n$ сложен број. Нека је $n = rs, \quad r > 1, s > 1$. Тада је

$$\begin{aligned} 2^n - 1 &= 2^{rs} - 1 \\ &= (2^r)^s - 1 \\ &= (2^r - 1)((2^r)^{s-1} + (2^r)^{s-2} + \cdots + 1). \quad \square \end{aligned}$$

У следећој табели могу се уочити неке чињенице у вези са степенима броја 2 од $2^2$ до $2^9$ (4 до 512).

| $n$ | $2^n$ | $2^n - 1$ | | | $2^n + 1$ | | |
|---|---|---|---|---|---|---|---|
| 2 | 4 | 3 | | прост | 5 | | прост |
| 3 | 8 | 7 | | прост | 9 | = | $3 \cdot 3$ |
| 4 | 16 | 15 | = | $3 \cdot 5$ | 17 | | прост |
| 5 | 32 | 31 | | прост | 33 | = | $3 \cdot 11$ |
| 6 | 64 | 63 | = | $3^2 \cdot 7$ | 65 | = | $5 \cdot 13$ |
| 7 | 128 | 127 | | прост | 129 | = | $3 \cdot 43$ |
| 8 | 256 | 255 | = | $3 \cdot 5 \cdot 17$ | 257 | | прост |
| 9 | 512 | 511 | = | $3 \cdot 7^2$ | 513 | = | $3^3 \cdot 19$ |

Примећујемо, на пример, да су оба суседа броја $2^6 = 64$ (63 и 65) сложени бројеви. То исто важи за број $2^9 = 512$. С друге стране, после пара простих бројева 3 и 5, у таблици не налазимо више ниједан пример да су и $2^n - 1$ и $2^n + 1$ прости бројеви. То није случајно. Наиме, од три узастопна броја $2^n - 1$, $2^n$ и $2^n + 1$, један мора бити дељив са 3, а то не може бити број $2^n$. Следеће тврђење, заједно са Теоремом 6, битно сужава област вредности од $n$ за које су $2^n - 1$ или $2^n + 1$ прости бројеви.

**ТЕОРЕМА 7** *Ако природан број $n > 1$ није степен броја 2, онда је $2^n + 1$ сложен број.*

**ДОКАЗ** У доказу користимо познати идентитет:

$$a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots + b^{n-1}),$$

који важи за сваки позитиван непаран број $n$.

Претпоставимо да $n$ није степен двојке. Следи да се $n$ може написати у облику $n = rs$, где је $r$ непаран број већи од 1. У случају кад је $n$ непаран прост број, тврђење следи на основу горњег идентитета, за $a = 2$, $b = 1$, тј. у том случају је $3|(2^n + 1)$. Дакле, преостаје да размотримо случај кад су и $r$ и $s$ већи од 1. Узмимо да је $a = 2^s$. Тада је $2^n = a^r$, па је $2^n + 1 = a^r + 1$. На основу истог идентитета, налазимо да је $a + 1$ прави делитељ од $2^n + 1$. $\square$

На основу доказаног тврђења, закључујемо да број облика $2^s + 1$ може бити прост само ако је он Фермаов број.

Утврђивање простоте (сложености) бројева облика $2^n \pm 1$ је проблем којим су се бавили многи математичари. Ландри (Landry) је 1869. године нашао факторизацију броја $2^{58}+1$ и прокоментарисао то овим речима: "Ниједна од многобројних факторизација бројева облика $2^n \pm 1$ није нам задала више муке нити одузела више времена. Број $2^{58}+1$ дељив је са 5 и када извршимо дељење тим фактором добија се број од 17 цифара који има два деветоцифрена проста фактора. Ако бисмо загубили овај резултат, не бисмо имали стрпљења и храбрости да поновимо сва израчунавања и могуће је да би прошле многе године пре него што би неко поново нашао факторизацију овог броја. Само десетак година касније Орифеј (Aurifeuille) је приметио да је

$$2^{58}+1 = (2^{29}-2^{15}+1)(2^{29}+2^{15}+1).$$

Тај резултат се лако уопштава:

$$2^{4n+2}+1 = (2^{2n+1}-2^{n+1}+1)(2^{2n+1}+2^{n+1}+1).$$

Према Теореми 6, број облика $2^n-1$ не може бити прост ако $n$ није прост. Зато се користи следећа нотација. Пишемо $M_p = 2^p-1$, где се подразумева да је $p$ прост број. Бројеви $M_p$ називају се *Мерсенови бројеви* по француском математичару из 17. века који их је изучавао у вези са савршеним бројевима. Мерсенови прости бројеви, као и прости бројеви облика $2^n+1$ су од посебног значаја. Разлози за то су, делом историјски а делом се заснивају на чињеници да такви прости бројеви налазе примену у другим областима математике.

Марен Мерсен (Marin Mersenne, 1588–1648) био је математичар, физичар, филозоф, теоретичар музике и теолог. Био је пријатељ Р. Декарта, са којим је заједно похађао језуитски колеџ. На својим путовањима у Италију и Холандију упознао се са Кавањеријем, Паскалом, Фермаом и Хајгенсом, с којима је водио интензивну преписку. Био је централна личност једне од најзначајнијих научних група у Француској на почетку 17. века. Године 1644, у предговору његове књиге "Физичко–математичка размишљања" (Cogita Physico–Mathematica) дао је оригиналне доказе неких Фермаових тврђења о простим и савршеним бројевима.

Мерсен је тврдио да су 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 и 257 једини прости бројеви, не већи од 257, за које је број $2^p-1$ прост. Међутим, ова листа садржи грешке, које су откривене много времена после смрти М. Мерсена. Наиме, два броја за која је Мерсен тврдио да су прости, уствари су сложени, а испуштена су три проста броја. Первушин (1827–1900) је, 1883. године, доказао да је $M_{61}$ прост. За бројеве $M_{89}$ и $M_{107}$ је, такође, утврђено да су прости. С друге стране, за бројеве $M_{67}$ и $M_{257}$ показано је да су сложени.

Највећи познати прости бројеви су Мерсенови бројеви. Наиме, за бројеве облика $2^n-1$ постоје специјалне методе које, уз помоћ рачунара, омогућавају да се утврди њихова евентуална простота, лакше него у случају осталих бројева. Фирма CRAY RESEARCH користи генерисање простих бројева као ултимативни тест рачунара које пројектује, јер та изузетно интензивна нумеричка

операција брзо указује на разне проблеме у дизајнирању и конструкцији суперрачунара. Највећи број за који, према нама доступним подацима, сада поуздано знамо да је прост је број $2^{859433} - 1$. Провера је извршена у лабораторијама компаније CRAY RESEARCH у Минесоти (САД), прошле године, уз коришћење суперрачунара најновије генерације CRAY C90

Данас су позната укупно 33 Мерсенова броја. Потпуна листа простих бројева $p$ за које су познати Мерсенови бројеви (према нама расположивим подацима) је: 2, 3, 5, 7, 13, 17, 19, 31, 69, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433.

## Дистрибуција простих бројева

Једна од најлепших теорема у математици је *теорема о простим бројевима* која са великом тачношћу даје одговор на питање колико има простих бројева не већих од датог природног броја $n$.

Обележимо са $\pi(n)$ број простих бројева не већих од $n$. На пример, $\pi(5) = 3$, $\pi(15) = 6$. Теорема о простим бројевима тврди да се за велике вредности од $n$ функција $\pi(n)$ понаша као функција $\frac{n}{\ln n}$, (при чему је са $\ln n$ означен логаритам за базу $e = 2,718281828\ldots$). Ово тврђење се обично записује у облику

$$\pi(n) \sim \frac{n}{\ln n}.$$

Кажемо да је $\pi(n)$ асимптотски једнако са $\frac{n}{\ln n}$.

Гаус је ово тврђење изнео као хипотезу 1840 године. Теорему су независно доказали 1896 године Вале–Пусен (La Vallee Poussin, 1866–1962) и Адамар (J. S. Hadamard, 1865–1963). Касније су, 1946 године, Ердеш (P. Erdös, 1913) и Селберг (A. Selberg, 1907) дали елементаран, али не и лак доказ теореме. Теорема уствари тврди да ма како био мали реалан број $\varepsilon > 0$, може се наћи довољно велики природан број $n_0$ (који зависи од $\varepsilon$), такав да је за сваки природан број $n > n_0$,

$$1 - \varepsilon < \frac{\pi(n)}{\frac{n}{\ln n}} < 1 + \varepsilon.$$

Пре Вале–Пусена и Адамара, Чебишев (1821–1894) је доказао неке значајне особине функције $\pi(n)$. Он је, 1850 године, доказао да је за сваки природан број $n > 1$,

$$\frac{7}{8} \cdot \frac{n}{\ln n} \leq \pi(n) \leq \frac{9}{8} \cdot \frac{n}{\ln n}.$$

Ова оцена је слабија од оне коју даје теорема о простим бројевима, али има ту добру страну да важи за сваки природан број већи од 1.

Следећа табела илуструје вредност теореме о простим бројевима.

| $n$ | $\pi(n)$ | $\frac{n}{\ln n}$ | $\pi(n)\frac{\ln n}{n}$ |
|---|---|---|---|
| 1000 | 168 | 145 | 1.159 |
| 10000 | 1229 | 1086 | 1.132 |
| 100000 | 9592 | 8686 | 1.104 |
| 1000000 | 78498 | 72382 | 1.084 |
| 10000000 | 664579 | 620421 | 1.071 |
| 100000000 | 5761455 | 5428681 | 1.061 |

## З А Д А Ц И

**1.** Доказати да је сваки прост број већи од 3 облика $6n-1$ или $6n+1$.

**2.** Доказати да постоји бесконачно много простих бројева облика $4k-1$, где је $k$ позитиван цео број.

**3.** Доказати да не постоји највећи прост број облика $3k+2$, где је $k$ позитиван цео број.

**4.** Наћи низ од 1995 узастопних природних бројева, међу којима нема простих.

**5.** Доказати да се непаран број облика $6n+1$, где је $n$ природан број, не може представити као разлика два проста броја.

**6.** Наћи све просте бројеве $p$, такве да је $p+1$

(а) потпун квадрат;

(б) потпун куб.

**7.** Доказати да се сваки непаран прост број може на тачно један начин представити као разлика квадрата два природна броја.

**8.** Наћи све природне бројеве $n$, такве да су $n, n+10$ и $n+14$ прости бројеви.

**9.** Наћи све тројке простих бројева које образују аритметичку прогресију са разликом 2.

**10.** Нека је $N$ производ свих простих бројева не већих од $n$, за $n>2$. Доказати да је $N>n$.

**11.** Нека је $p_n$ $n$–ти прост број. Доказати да је $p_n>2n$, за $n>4$.

**12.** Доказати да између бројева $n$ и $n!$ постоји бар један прост број, за $n>2$.

**13.** Користећи претходни задатак дати још један доказ да има бесконачно много простих бројева.

**14.** Прост број $n$ записан у бинарном систему има све цифре јединице. Доказати да је онда и број његових цифара прост број.

**15.** Доказати да Фермаови бројеви задовољавају рекурентну релацију

$$f_{n+1} = f_0 f_1 f_2 \cdots f_n + 2.$$

**16.** Користећи претходни задатак доказати да су свака два различита Фермаова броја узајамно прости.

**17.** Доказати да за $n > 5$, сваки број облика $2^{2^n} - 1$ има прост фактор већи од 1000000.

**18.** Доказати да за сваки природан број $n$, број $2^{2^n} - 1$ има бар $n$ различитих простих фактора.

**19.** (а) Колико има непарних природних бројева $n$ мањих од 1000000000, таквих да се правилан $n$–угао може конструисати шестаром и лењиром?

(б) Колико има природних бројева $n$ мањих од 1000 таквих да се правилан $n$–угао може конструисати шестаром и лењиром?

**20.** Да ли постоји скуп $S$ од 1995 природних бројева који има следеће две особине:

(а) Сваки збир два или више бројева из скупа $S$ је сложен број;

(б) Свака два броја из $S$ су узајамно прости?

**21.** Нека је $f(x) = x^2 - x + 1$. Доказати да су, за сваки природан број $m > 1$, бројеви

$$m, \quad f(m), \quad f(f(m)), \ldots$$

по паровима узајамно прости.

**22.** Користећи претходни задатак, доказати да има бесконачно много простих бројева.

**23.** (а) Одредити сва решења једначине $\pi(n) = \frac{n}{2}$ у скупу природних бројева.

(б) Наћи најмањи природан број $n > 1$ за који је $\pi(n) < \frac{n}{3}$.

**24.** Одредити све природне бројеве $n$ за које је

(а) $$\frac{\pi(n-1)}{n-1} < \frac{\pi(n)}{n};$$

(б) $$\frac{\pi(n-1)}{n-1} > \frac{\pi(n)}{n}.$$

**25.** Нека је

$$a_1, a_2, \ldots, a_k$$

ограничен низ такав да је

$$1 < a_1 < a_2 < \cdots < a_k \leq n,$$

при чему ниједан члан није делитељ производа осталих.

Показати да је $k \leq \pi(n)$.

**26.** Дат је низ

$$a_1 = 3,\ a_2 = 3 + 2k,\ a_3 = 3 + 4k,\ a_4 = 3 + 6k, \ldots$$

где је $k$ природан број. Доказати да у том низу не постоје три узастопна члана који су сви прости бројеви.

## ОДГОВОРИ, УПАТСТВА И РЕШЕНИЈА НА ЗАДАЧИТЕ

**1.** Следи на основу чињенице да су бројеви облика $6n$, $6n+2$ и $6n+4$ дељиви са 2, док су бројеви облика $6n+3$ дељиви са 3.

**2.** Претпоставимо да има само коначно много простих бројева облика $4k-1$. Нека су $p_1$, $p_2, \ldots,$ $p_m$ сви такви бројеви. Посматрајмо број

$$q = 4p_1p_2 \cdots p_m - 1.$$

Приметимо да је производ бројева облика $4k+1$, увек број истог таквог облика. Зато број $q$ има бар један прост фактор $p$ облика $4k-1$. Број $p$ је различит од свих бројева $p_i$, $i = 1, 2, \ldots, m$, зато што ниједан од тих бројева није делитељ од $q$. Дошли смо до контрадикције са претпоставком да су $p_1, p_2, \ldots, p_m$ једини прости бројеви облика $4k-1$. Следи да таквих бројева има бесконачно много.

**3.** Приметимо да је производ бројева облика $3k+1$ увек број истог таквог облика. Претпоставимо да постоји највећи прост број облика $3k+2$, тј. да има коначно много таквих бројева. Нека су $p_1$, $p_2, \ldots,$ $p_m$ сви такви бројеви. Посматрајмо број

$$q = 3p_1p_2 \cdots p_m + 2.$$

Број $q$ има бар један прост фактор $p$ облика $3k+2$, који, међутим, мора бити различит од свих простих бројева $p_i$, $i = 1, 2, \ldots, m$, што је контрадикција.

**4.** У низу од $n-1$ узастопних бројева

$$n!+2,\ n!+3,\ldots,\ n!+n,$$

сви бројеви су сложени (први је дељив са 2, други са 3, ..., последњи са $n$).

**5.** Претпоставимо да је $6n+1=p-q$, где су $p$ и $q$ прости бројеви. Ако је $q=2$, онда је $p=6n+3$, што је немогуће. Ако је $q=2k+1$, онда је $p=6n+2k+2$, што је, такође, немогуће.

**6.** (а) Нека је $p$ прост број, такав да је $p+1=x^2$, за неки природан број $x$. Тада је $p=x^2-1=(x-1)(x+1)$. Следи да је $x-1=1$, тј. $p=3$.

(б) Ако је за неки прост број $p$, $p=x^3-1=(x-1)(x^2+x+1)$, онда је $x-1=1$, тј. $p=7$.

**7.** Сваки непаран број може се на јединствен начин представити као разлика квадрата два узастопна природна броја :

$$2k+1=(k+1)^2-k^2.$$

Нека је $p$ непаран прост број такав да је $p=x^2-y^2$, где су $x$ и $y$ природни бројеви. Тада је $p=(x-y)(x+y)$, па је $x-y=1$, тј. $x=y+1$, одакле следи тврђење.

**8.** Очигледно, 2 није такав број. Природан број $n>2$ може се написати у облику $n=3q+r$, где је $0\leq r\leq 2$. За $r=2$, број $n+10$ је сложен; за $r=1$, сложен је број $n+14$. За $r=0$, једини прост број облика $3q$ је 3 а у том случају су прости и бројеви $3+10=13$ и $3+14=17$.

**9.** Посматрајмо бројеве $p$, $p+2$ и $p+4$, где је $p$ прост број. Ако је $p$ облика $3q+1$, онда је $3|(p+2)$. Ако је $p$ облика $3q+2$ онда је $p|(p+4)$. Преостаје само могућност да је $p=3$, у ком случају се добија решење: 3, 5, 7.

**10.** Нека је $p$ највећи прост број који није већи од $n$. Број $N-1=2\cdot 3\cdot 5\cdots p-1$ садржи само просте факторе веће од $n$. Следи да је $N-1>n$; тим пре је $N=2\cdot 3\cdot 5\cdots p>n$.

**11.** Тврђење важи за $n=5$: $p_5=11>10$. Ако је $p_n>2n$, онда је $p_{n+1}\geq p_n+2>2n+2=2(n+1)$.

**12.** Нека је $p$ прост фактор броја $n!-1$. Очигледно је $n<p\leq n!-1<n!$.

**13.** Следи на основу тога што, према претходном задатку, између свака два узастопна члана бесконачног низа

$$3, \quad 3!, \quad (3!)!, \quad ((3!)!)!, \ldots$$

постоји бар један прост број.

**14.** Број $2^p - 1$ у бинарном систему записује као низ од $p$ јединица. Сада тврђење следи на основу Теореме 6.

**15.** Користити математичку индукцију, узимајући у обзир да је $f_n = 2^{2^n} + 1$ и $f_{n+1} - 2 = 2^{2^{n+1}} - 1 = (2^{2^n} - 1)(2^{2^n} + 1)$.

**16.** Нека је $d|f_n$ и $d|f_{n+k}$, за неке природне бројеве $n$ и $k$. Како је $f_{n+k} = f_0 f_1 \cdots f_n \cdots f_{n+k-1} + 2$, то је $d|2$. Због непарности Фермаових бројева, следи да је $d = 1$.

**17.** Према задатку 15, $2^{2^n} - 1 = f_n - 2 = f_0 f_1 \cdots f_{n-1}$, па је број $2^{2^n} - 1$ дељив са сваким Фермаовим бројем $f_i$, за $0 \leq i \leq n-1$. Међутим, Фермаов број $f_5$ садржи прост фактор 6700417, одакле следи тврђење.

**18.** Број $2^{2^n} - 1$ је производ $n$ различитих Фермаових бројева, који су по паровима узајамно прости, одакле следи тврђење.

**19.** (а) 29; (б) 50.

**20.** Да. Такав је скуп $S = \{k \cdot 1995! + 1 \mid k = 1, 2, \ldots, 1995\}$. Збир $r$ бројева из тога скупа дељив је са $r$.

**21.** Како је $f(1) = f(0) = 1$, то је слободни члан $P_n(0)$ полинома $P_n(x) = \underbrace{f(f(\cdots(f}_{n}(x))\cdots))$ једнак 1. Следи да је, за сваки природан број $m$, остатак при дељењу $P_n(m)$ са $m$ једнак 1. Узимајући $m' = P_k(m)$ уместо $m$, добијамо да су $P_{n+k}(m)$ и $m' = P_k(m)$ узајамно прости бројеви.

**22.** Следи на основу чињенице да у бесконачном низу

$$m, \quad f(m), \quad f(f(m)), \ldots$$

сваки члан садржи прост фактор који није фактор ниједног другог члана низа.

**23.** (а) $n \in \{2, 4, 6, 8\}$; (б) $n = 28$.

**24.** (а) $n$ прост број; (б) $n$ сложен број.

**25.** Канонски облик сваког члана $a_i$ садржи бар један прост фактор $p_i$ са експонентом ($\geq 0$) већим него што је експонент од $p_i$ у канонском разлагању производа осталих чланова низа. То значи да се $p_i$ појављује у броју $a_i$ са експонентом већим него у било ком другом члану низа. Назовимо $p_i$ "представником" броја $a_i$. Како сваки прост број може бити представник највише једног члана низа, следи да је $k \leq \pi(n)$.

**26.** Ако је $k = 3t$ за неки природан број $t$, онда тврђење важи јер су у том случају сви чланови низа дељиви са 3. Нека је $k \neq 3t$. Ако тврђење не важи, онда су за неки $n > 1$, бројеви

$$a_n = a > 3,\ a_{n+1} = a + 2k,\ a_{n+2} = a + 4k$$

три проста броја. Како је $a$ прост број, то је $3|(a+1)$ или $3|(a+2)$. У првом случају, за $k = 3t+1$, следи $3|((a+1)+(6t+3))$, тј. $3|(a+2k)$. У другом случају, за $k = 3t+1$, следи $3|((a+2)+6t)$, тј. $3|(a+2k)$, а за $k = 3t+2$, добијамо $3|((a+2)+(12t+6))$, тј. $3|(a+4k)$. Како је $a_n$ прост број и $n > 1$, следи да бар један од бројева $a_{n+1}$, $a_{n+2}$ није прост. За $n = 1$ могу сва три броја $a_1$, $a_2$, $a_3$ бити прости. На пример, за $k = 2$ је $a_1 = 3$, $a_2 = 7$, $a_3 = 11$.)