IYBSSD2022

International Year
of Basic Sciences
for Sustainable Development

2022 – Международна година
на фундаменталните науки
за устойчиво развитие

Може ли чистата математика да бъде полезна?

Веселин Дренски
Институт по математика и информатика
Българска академия на науките
drensky@math.bas.bg

Често задаван въпрос:

Трябва ли ни математиката, след като има компютри, които могат да сметнат всичко и интернет, където може да се научи всичко?

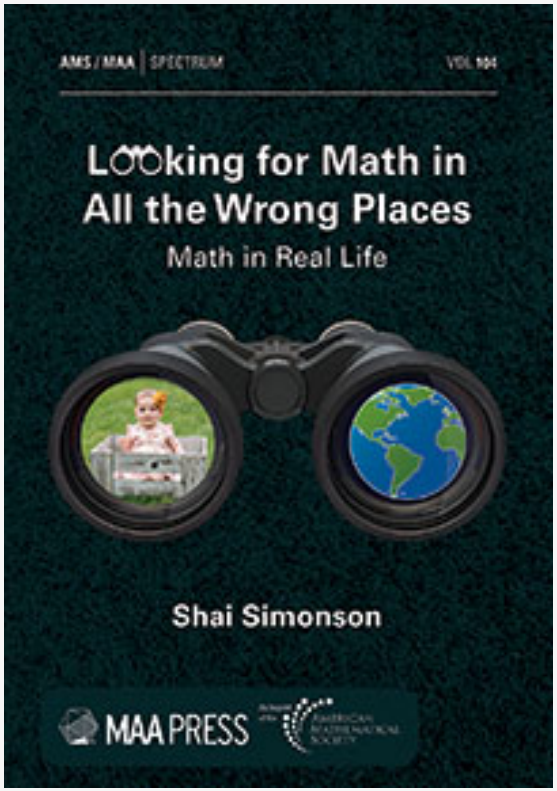
Една забавна история като отговор

Моят дипломант Пламен Коев защити дипломна работа за приложенията на компютрите за решаване на проблеми от абстрактната алгебра. По-късно той защити дисертация в Бъркли за приложение на линейната алгебра за създаване на компютърни алгоритми за решаване на практически задачи.
Търсачките в Интернет използват математически методи за нареждане по важност на възможните отговори. Понякога се налага да се наредят стотици хиляди отговора. В Бъркли Пламен Коев установи, че когато в Google се търси "Plamen" на първо място се появява името на волейболиста Пламен Константинов. Той така организира данните за себе си в Интернет, че при търсенето с "Plamen" на първо място се появяваше той.

Като постдокторант в MIT Пламен Коев организира международна група от "чисти математици" от България, Канада, САЩ и Хонг Конг, която създаде алгоритми за бързо пресмятане на симетрични полиноми. (Спомнете си формулите на Виет за квадратното уравнение и техния аналог за уравнения от по-висока степен!) Оказва се, че такива пресмятания са необходими за решаването на множество приложни задачи, вариращи от геномика, безжични комуникации, разпознаване на цели (как да различим нашите танкове или самолети от вражеските) и др.
Днес Пламен Коев е професор в Щатския университет в Сан Хосе, Калифорния и продължава да поддържа връзки с България. Той е научен ръководител на Стивън Спасов от Софийската математическа гимназия "Паисий Хилендарски", който на Европейския конкурс за млади учени (European Contest for Young Scientists – EUCYS) за 2022 г. спечели наградата на ЦЕРН. Освен това Стивън беше удостоен с Грамота за Дебютен пробив в областта на компютърните технологии в конкурса на президентската инициатива Награда "Джон Атанасов" за 2022 г.

През тази година се появи една завладяваща читателя книга с провокативно заглавие:

“Търсене на математика на всички грешни места”



В нея авторът прилага математически методи в различни случаи, които възникват в ежедневието, за да докаже твърдението, че математиката е буквално навсякъде.

Достатъчно е да погледнем съдържанието на книгата, за да се убедим, че математиката е наистина навсякъде.

- Introduction
- Summer Carnivals
- Games
- Holidays
- Magic
- Locks
- Limits
- Wine and Averages
- Music
- Parabolas, Caternaries, and Kites
- A Day in the Woods
- Viral Puzzles
- Happy Birthday
- COVID-19
- Estimations
- High-Tech Interviews
- Sports

Преди 10 дни проф. Владя Борисова, председател на Патентно ведомство, даде интервю:

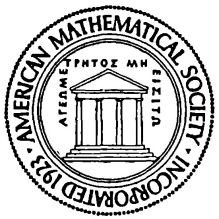

Живеем сред изобретения, без да го осъзнаваме

Ако перефразираме заглавието на интервюто, ще се окаже, че *“Живеем сред математика, без да го осъзнаваме.”*
В същото интервю се казва, че *“в световен мащаб най-значимите изобретения са в медицината и изкуствения интелект.”* Трудно можем да си представим много от сериозните изследвания по изкуствен интелект без използването на сериозна математика.

През вековете отношението към математиката е било твърде различно.

Сред интелектуалния елит на древна Гърция математиката е била поставена в култ.

На входа на Академията на Платон има надпис
"Никой, който не знае геометрия, не трябва да влиза тук."
Ще отбележим, че от 1923 г. печатът на Американското математическо дружество (основано през 1888 г.) показва гръцки храм заедно с този надпис.



Inscription over the door of
Plato's Academy:
ἀγεωμέτρητος μηδεὶς εἰσίτω μοῦ τὴν στέγην

В периода 529 – 534 година от новата ера по заповед на император Юстиниан I се създава Corpus Iuris Civilis (Свод на гражданското право) – основополагаща колекция от трудове в областта на юриспруденцията. Глава 18, §2 на Книга 9 е озаглавена *"De maleficis et mathematicis et ceteris similibus"* (*За злосторниците и математиците и други подобни на тях*). В първия абзац се казва, че е по-лошо да умъртвиш човек с отрова, отколкото да го убиеш с меч. Това е малко шокиращ намек за геометрията, защото вторият абзац гласи *"Artem geometriae discere atque exerceri publice intersit. Ars autem mathematica damnabilis interdicta est."*
Първото изречение означава: *"Изучаването и практикуването на изкуството на геометрията представлява публичен интерес."*
Преводът на второто изречение е *"Но прокълнатото изкуство математика е забранено."* **Единственото успокоение е, че по това време "изкуството математика" означава "астрология".**

От 1902 г. текстът *Artem geometriae discere atque exerceri publice interest* стои на печата на Немския математически съюз (основан през 1890 г.).

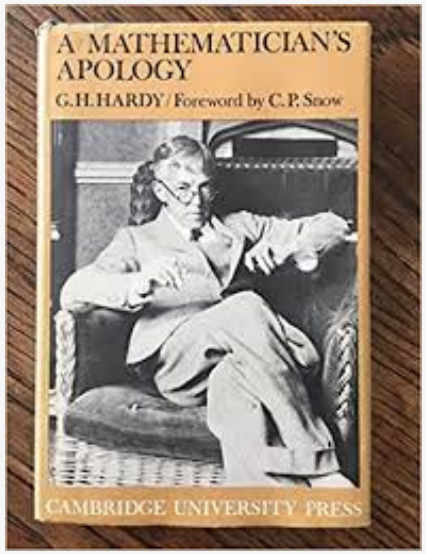
Има области на чистата математика, които са очевидно полезни

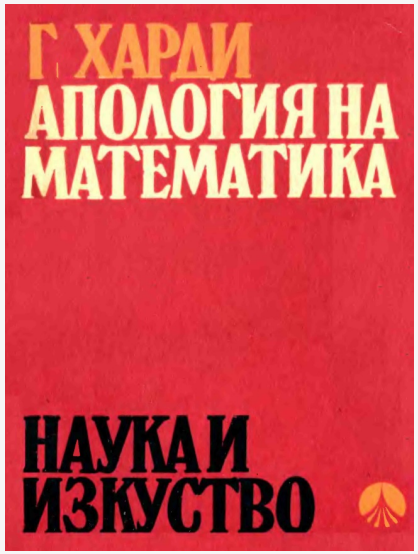
- **Геометрията в Древния Египет.** Всяка година Нил се разлива различно. Това е водило до промяна на земите на земеделците – реката поглъщала част от земите на едни и давала нови земи на други. За пресмятането на площите, свързано със събирането на данъци са били необходими знания по планиметрия. Мащабните строежи на пирамидите изискват знания по стереометрия.
- **Диференциални уравнения.** Диференциалните уравнения имат забележителното свойство да предсказват поведението на света около нас. Те се използват в множество от дисциплини, започвайки от биология, икономика, физика, химия, инженерни науки и техните приложения в практиката. Решенията на някои от уравненията могат да се намерят в явен вид, чрез просто интегриране, но някои изискват използването на значително по-сложна математика.

Отново към въпроса: Може ли чистата математика да бъде полезна?

Една от най-добрите книги, написана от математик, е написана през 1940 г. от Годфри Харолд Харди – един от най-великите математици на всички времена.

Godfrey Harold Hardy, *A Mathematician's Apology*
Превод на български от 1971 г.: *Апология на математика*





В своята книга Харди пише:
“Изучаването на математика е, ако и безполезно, все пак съвършено безвредно и невинно занимание.
Полезна ли е математиката, *директно* полезна, като например химията или физиологията?
Едва ли мога да направя нещо по-добро от това да се върна към гърците. Ще формулирам и докажа две от знаменитите теореми на гръцката математика.”

Първият пример е евклидовото доказателство за съществуването на безбройно много прости числа.
Простите числа

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$$

са числа, които не могат да се разложат на по-малки множители.

Вторият ми пример е питагоровото доказателство на "ирационалността" на $\sqrt{2}$.

Изобщо няма никакво съмнение в "сериозността" и на двете теореми. Ето защо толкова повече заслужава да отбележим, че никоя от тези теореми няма и най-малко практическо значение.

Математика и музика в Древна Елада

Школата на Питагор свързва директно музиката и математиката. Питагор смятал, че не чувството е водещо при предаването и разбирането на музиката. Тя, като божествено изкуство, трябва да се приеме от разума и според математическата хармония, подчинена на числата. Той пръв определил, че височината на музикалната нота е обратнопропорционална на дължината на струната, която я произвежда, и че интервалите между хармоничните звукови честоти образуват прости цифрови съотношения.

Октавата (например от “До” до “До”) се състои от 12 полутона, като честотата на най-горния тон е два пъти по-голяма от тази на най-долния. При *равномерната гама* отношението между честотите на два съседни полутона е едно и също, т.е. честотата на всеки полутон е $\sqrt[12]{2}$ пъти по-голяма от тази на предишния. В *Питагореево умерената гама* честотата на нотата се изчислява като тази на седмия полутон над дадения се умножава с 3/2 и се дели на 2, за да се смъкнем с една октава по-надолу и да намерим *умерената пета* на нотата.

Тъй като уравнението $2^x = 3^y$ няма решение в естествени числа се оказва, че в Питагореево умерената гама нотите “Ми бемол” и “Ре диез” са с различна честота, въпреки, че отговарят на един и същи черен клавиш на пианото.

“Ми бемол”=313.24 Hz и “Ре диез” = 309.03 Hz, което е разлика от почти четвърт тон.

Един от стандартите в съвременната музика фиксира, че нотата “Ла” е с честота 440 Hz. От 1936 г. американската радиостанция WWV, която предава информация за точно време, на всеки час излъчва сигнал с честота 440 Hz с цел да помага на оркестрите да настройват своите инструменти. Същото прави и радиостанцията WWVH.

Отново Харди

Аз бих могъл да цитирам колкото искате тънки теореми от теорията на числата, чийто смисъл всеки би могъл да разбере. Тук спада например така наречената "основна теорема на аритметиката", която гласи, че всяко цяло число може да се разложи по *един единствен начин* на произведение от прости числа.

Така например $666 = 2 \cdot 3 \cdot 3 \cdot 37$ или $13 \cdot 89 \neq 17 \cdot 73$.

Историята показва, че Харди не е бил прав в следното свое твърдение

Има едно утешително заключение, което е лесно за един истински математик. Истинската математика няма нищо общо с войната. Засега никой не е открил някакво военно приложение на теорията на числата или на теорията на относителността и изглежда неправдоподобно някой да направи това в течение на много години.

Няма математически клон, колкото и абстрактен да е,
който някой ден да не бъде приложен
към явленията от реалния свят.
Николай Иванович Лобачевски

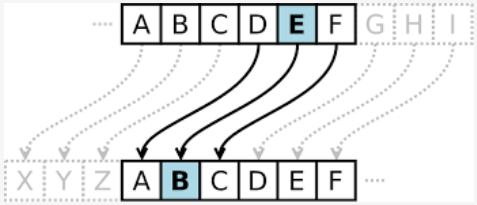
Теорията на числата изиграва съществена роля в успешното разбиване на шифрите, ползвани от германските военноморски сили.
Навярно за широката нематематическа публика Алън Тюринг, един от най-известните логици на XX век, е известен преди всичко като човекът, изиграл ключова роля в разбиването на шифрите. Той създава няколко метода за криптоанализ и прави подобрения на използваната за целта изчислителна електромеханична машина "Бомба", което прави възможно дешифрирането на кодовете на "Енигма".

В цялата история на цивилизацията защитата на информацията е заемала важно място

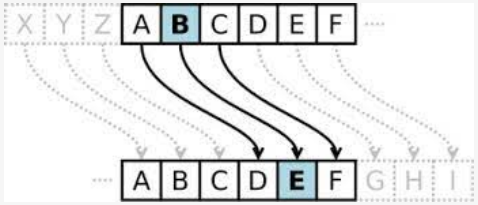
В Древния Египет са обръсвали главата на роб, татуирали са съобщението върху главата му и са чакали косата да порасне. Тогава робът е отивал при получателите на съобщението, които отново са обръсвали главата на роба и са прочитали съобщението.
Същият принцип, че *врагът не знае, че има съобщение*, е залегнал при водните знаци, които съдържат потвърждение на истинността на обектите (банкноти, произведения на изкуството и др.). Оказва се, че и тук се появява чиста математика (например дискретни преобразования на Фурие).

Шифрите – врагът вижда съобщението, но не може да го прочете

Още Гай Юлий Цезар е използвал шифър, за да контактува със своите пълководци. В неговия шифър буквите се изместват с фиксирано число, а при дешифрирането се изместват със същото число в другата посока.



Шифриране



Дешифриране

Криптография със симетричен ключ

Ако знаем алгоритъма, с който се шифрира с шифъра на Цезар, можем със същия алгоритъм да дешифрираме съобщението. Такива шифри се създават и са обект на изучаване с *криптографията със симетричен ключ*.

Започвайки от най-старото използване на криптографията с нестандартни йероглифи, намерени на стената на гробница от Средното царство на Древния Египет около 1900 BC до края на 70-те години на XX век, всички системи за криптиране са използвали алгоритми със симетричен ключ.

Криптография с публичен ключ

Основната разлика между криптографията със симетричен ключ и *асиметричната криптография*, или *криптографията с публичен ключ*, е в това, че последната се базира на брилянтната идея, че ключът за криптиране не е секретен (и много често свободно достъпен) и само ключът за декриптиране е секретен. Това позволява използването на канали за предаване на информация, които не са сигурни.

За целта се използват математически задачи, за които е лесно да се провери дали някакво число е решение, но е трудно да се намерят всички решения.

Разлагане на числата в произведение на прости множители

Оказва се, че основната теорема на аритметиката е пример на такава задача. Много е лесно, като се използва алгоритъмът за деление, изучаван в началното училище, да се провери дали едно число се дели на друго. Но е много по-трудно да се разложи едно число в произведение на прости множители.

Числа на Ферма

В няколко свои писма между 1630 и 1640 г. Пиер Ферма изказва хипотезата, че всички числа от вида

$$F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, \ldots,$$

са прости. Такива числа днес се наричат *числа на Ферма*. Хипотезата на Ферма е вярна за първите 5 числа

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65\ 537.$$

През 1732 г. Леонард Ойлер доказва, че F_5 се дели на 641. Това лесно може да се провери, но ако не знаем този факт, е много трудно да намерим разлагането

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4\ 294\ 967\ 297 = 641 \times 6\ 700\ 417$$

и да докажем, че и двете числа 641 и 6 700 417 са прости.

Същото е вярно и за

$$F_6 = 2^{64} + 1 = 18\ 446\ 744\ 073\ 709\ 551\ 617$$

$$= 274\ 177 \times 67\ 280\ 421\ 310\ 721.$$

Досега не е известно нито едно просто число на Ферма F_n за $n > 4$. Съществува хипотеза, че всички прости числа на Ферма са за $n \leq 4$. Към 24 ноември 2021 г. са намерени прости делители на 360 числа на Ферма, най-голямото от които е за $n = 18\ 233\ 954$.

През 1978 г. Ривест, Шамир и Адлеман от MIT публикуват статия, в която предлагат алгоритъм с публичен ключ, известен днес като RSA-алгоритъм.
Много по-късно става известно, че Джеймс Елис, работещ за британските секретни служби още през 1969 г. е стигнал до идеята за подобен публичен ключ. Но на Елис не са му стигнали знания по теория на числата, за да разработи действаща система за криптиране. По-късно друг сътрудник, Клифорд Кокс, който е завършил математика, разработва работеща версия. Но това остава в тайна до 1997 г.

Идея за RSA-алгоритъма

Избираме две секретни прости числа p и q и обявяваме публично тяхното произведение $n = pq$. Нека $\lambda(n)$ е най-малкото общо кратно на $p-1$ и $q-1$. От *Малката теорема на Ферма* следва, че ако a е естествено число $< n$, което не се дели на p и q, то $a^{\lambda(n)+1}$ дава остатък a при деление на n. Избираме естествено число e, което е взаимно просто с $\lambda(n)$ и намираме число d, за което de дава остатък 1 при деление на n. Числото e е публично известнио, а d секретно.

Публичният ключ се състои от *модула* n и *публичната* (или *криптираща*) *експонента* e.
Персоналният ключ се състои от числата p, q и от *личната* (или *декриптираща*) *експонента* d, които трябва да се държат секретни.

Криптиране на съобщението

Алис дава своя публичен ключ (n и e) на Боб и държи в тайна своя личен ключ d. Боб иска да изпрати съобщение на Алис. Той използва стандартна процедура, за да превърне съобщението в число a по-малко от n. Тогава той пресмята a^e, намира остатъка c от делението на a^e на n и изпраща c на Алис.

Декриптиране на съобщението

Алис пресмята c^d, дели го с частно и остатък на n. Оказва се, че остатъкът е равен на числото на Боб a. След това със стандартна процедура превръща числото a в оригиналното съобщението на Боб.

Колко трудно е да се пробие криптирането с RSA-алгоритъма?

През март 1991 г. Лабораторията, създадена за RSA-алгоритъма публикува списък от произведения на две прости числа, които се записват с от 100 до 617 цифри в десетична бройна система. Обявена е награда, която достига до US$200 000 за разлагане на прости множители на някое от тези числа. (Такива награди са платени в размер до $20 000.) Плащането на такива награди е преустановено официално през 2007 г., но и до днес хората продължават да търсят разлагания.

Към февруари 2020 г. най-малките 23 от всичките 54 изброени числа са разложени на прости множители.

Най-малкото число от списъка е разложено за няколко дни от Арйен Ленстра:

RSA-100 = 152260502792253336053561837813263742971806811496
13806886579084945801229632589528976540003506920061 39;

RSA-100 = 379752279369436739228088727554456278545655366381 99
× 400946909509208810306837352927614683892148997240 61.

RSA-250 има 250 десетични цифри и през февруари 2020 г. е разложено от Фабрис Будо, Пиерик Годри, Аврора Гилевич, Надя Хенингер, Еманuел Томе и Паул Цимерман. Колективът използва компютри, работещи едновременно на много места по света. Времето за пресмятане се равнява приблизително на 2 700 години, ако се използва Intel Xeon Gold 6130 CPU с честота 2.1GHz:

RSA-250 = 21403246502407449612644230728393335630086147151447550177977549208814180234471401366433455190958046796109928518724709145876873962619215573630474547705208051190564931066876915900197594056934574522305893259766974716817380693648946998715784949759374979371

= 64135289477071580278790190170577389084825014742943447208116859632024532344630238623598752668347708737661925585694639798853367

×33372027594978156556226010605355114227940760344767554666784520987023841729210037080257448673296881877565718986258036932062711

Вместо заключение

Преди повече от 100 години мексиканският поет Амадо Нерво написа детското стихотворение за малкото хартиено корабче:

El barquito de papel
Amado Nervo

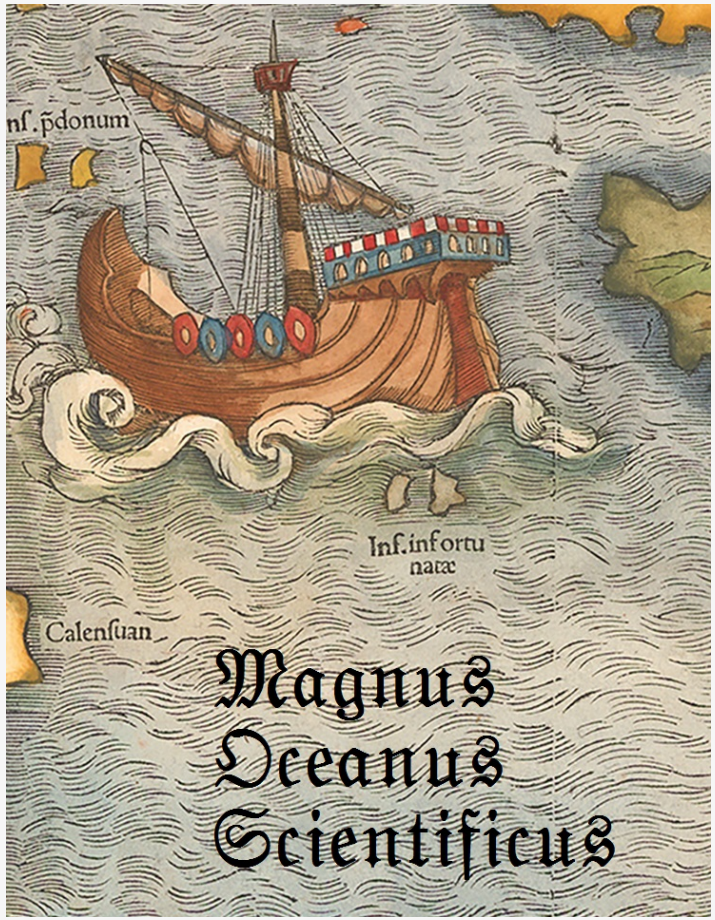
Con la mitad de un periódico
hice un barco de papel,
en la fuente de mi casa
le hice navegar muy bien.
Mi hermana con su abanico
sopla, y sopla sobre él.
¡Buen viaje, muy buen viaje,
barquichuelo de papel!

The small paper ship
Amado Nervo

With the half of a newspaper
I made a paper ship,
that in the fountain of my house
is sailing very well.
My sister blows and blows
on it with her fan.
Have a good trip! Have a very good trip,
small paper ship!

За съжаление, има учени, които правят своите малки хартиени корабчета, плуват с тях в коритото на чешмата на двора на техния университет или институт и твърдят, че плуват във Великия научен океан.

Да работим така, че да посрещнем Международната година на фундаменталните науки за устойчиво развитие във Великия научен океан, а не с малкото хартиено корабче в коритото на чешмата на двора!



Попътен вятър и щастливо плаване!