

AI 数学的突破进展 Breakthrough in AI Math

AI 推翻埃尔德什 #205 问题 AI disproves Erdős Problem #205

鸣鹤散人

星海智慧 Starry Wisdom Foundation

21 JAN 2026

POCY 13 CHNM 12

Version 13.12.03

Licensed under CC BY 4.0

1. 埃尔德什 #205 问题的背景 Background for Erdős Problem #205
2. 埃尔德什的 $2^k + p$ 反例 Erdős' Counter-Examples to $2^k + p$
3. 埃尔德什 #205 问题 Erdős Problem #205
4. AI 的反例构造 AI's Counter-Example Construction

所需知识 Knowledge Needed

领域：数论
Area: Number Theory

程度：中学 +
Level: High School +

尽量浅显易懂！我也是那种看公式需要翻译为人话的哈哈
In easy terms! I also need translator for messy formulas :-)

明星：GPT 5.2 思考版（线下）+ 亚里士多德
Stars: GPT 5.2 thinking (offline) + Harmonic Aristotle

哥德巴赫猜想 Goldbach's Conjecture

- 哥德巴赫猜想是在 1742 年由哥德巴赫在与欧拉的通信中首次提出 The Goldbach's conjecture was first mentioned in 1742 in a letter written to Euler by Goldbach
- 基本表述为任意大于 2 的偶数可以表达为两个素数 (质数) 之和 The basic form is that any even number greater than 2 can be represented by the sum of two primes
- 2013 年 Helfgott 解决了弱哥德巴赫即任意大于 1 的奇数可表达为不超过三个素数之和 In 2013 Helfgott proved the weaker version that any odd number greater than 1 is a sum of no more than 3 primes.

$2^k + p$ 问题 $2^k + p$ Problem

- 哥德巴赫猜想可以理解为用两份全体素数集合相加去覆盖偶数集合，这种集合相加是指从集合中分别挑选数字相加。可记为 $\{2, 3, 5, 7, 11, 13, \dots\} + \{2, 3, 5, 7, 11, 13, \dots\} \sim \{2, 4, 6, 8, 10, \dots\}$?
Goldbach's conjecture can be understood as two copies of the set of all primes, added together to cover the set of even numbers.
This addition of sets means picking numbers from each set to add
- 如果把其中一个素数集合替换成 2 的幂的集合能否覆盖奇数? $\{1, 2, 4, 8, 16, 32, \dots\} + \{2, 3, 5, 7, 11, 13, \dots\} \sim \{1, 3, 5, 7, 9, \dots\}$?
Replacing one of the prime set with the set of powers of 2, can it cover the set of all odd numbers?

$2^k + p$ 问题 $2^k + p$ Problem

- 也就是说，给定奇数 n , $n - 2^k$ 里是否有素数? This is to ask, given odd number n , are there primes in $n - 2^k$?
- 素数的问题往往可以用概率探索去评估 Oftentimes questions regarding primes can use "heuristics" to estimate
- 我们假设 $n - 2^k$ 是素数这件事对于不同的 k 来说是独立事件 Now we assume that $n - 2^k$ being prime are independent events for different k
- 由素数定理 n 以下的数中素数的密度约为 $1/\log n$, 那么奇数中的素数密度为 $2/\log n$
From prime number theorem among numbers under n the density of prime is $1/\log n$. So density of prime in odd numbers is $2/\log n$

素数定理 Prime Number Theorem

- 据记载高斯在 1793 年 16 岁时已提出猜想 n 附近素数的密度为 $1/\log n$
In 1793 at age of 16 Gauss is said to have already conjectured the density of prime near n is $1/\log n$
- 这一猜想经黎曼等几代数学家研究终于在 1896 年由阿达马和普桑完成证明，后称为素数定理 This conjecture was studied by generations of mathematicians such as Riemann and finally proved in 1896 by Hardmard and Poussin. It's then referred to as the prime number theorem
- 但素数表现出的随机性并未因素数定理而明晰，反而愈加神秘
But the random character of prime becomes more mysterious

$2^k + p$ 问题 $2^k + p$ Problem

- $n - 2^k$ 为素数看作关于 k 的独立事件即伯努利试验 Then these independent primality events can be viewed as Bernoulli trials
- 这里试验一直失败的概率为 $(1 - 2/\log n)^k, k = 1, 2, 3, \dots$ is the probability of consecutive failures
- 因为 $2^k < n$, 我们可以一直试验 k 到 $k \approx \log_2 n$ is the upper limit that we can perform the trial k up to as $2^k < n$
- $(1 - 2/\log n)^{\log_2 n}$ 的极限, 也就是无法表达的数的密度, 大于 0
The density of unrepresentable numbers is then the limit of $(1 - 2/\log n)^{\log_2 n}$, which is greater than 0
- **Exercise** 试说明这一极限为何大于 0, 或者解出该极限 Try explain why this limit is greater than 0, or solve this limit

中国剩余定理 Chinese Remainder Theorem

- 中国剩余定理出自《孙子算经》，著作年代有争议，应成书于 1500-2500 年前，不排除最初由《孙子兵法》的作者孙武传世的可能性 The Chinese remainder theorem originated from "The Mathematical Classic of Sun Zi", one of the oldest math books of ancient China. Although controversial it cannot be ruled out it was from the same Sun Zi who wrote the famous "Art of the War"
- 《孙子算经》：有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二。问物几何？ From "The Mathematical Classic of Sun Zi": We don't know the numbers of certain objects, counting by 3 then 2 are left, counting by 5 then 3 are left, counting by 7 then 2 are left. How many objects are there?

中国剩余定理 Chinese Remainder Theorem

- 明朝数学家程大位在《算法统宗》中将解法编成易于上口的《孙子歌诀》：
三人同行七十稀， 五树梅花廿一支，
七子团圆正半月， 除百零五便得知。
- 中国剩余定理从概率的观点可以理解为互素的除数上的除法相对独立 From probabilistic point of view the Chinese remainder theorem can be understood as the division by relative prime numbers are independent.
- Exercise** 试解开孙子的物不知数（《射鵰英雄传》黄蓉通关瑛姑最后一题） Try solve the Chinese remainder problem of Sun Zi.

中国剩余定理 Chinese Remainder Theorem

- 我们只考虑两个同余式的解法，更多的可以递归 We consider solving two congruence equations, more equations can then be solved recursively
- $n \equiv r_1 \pmod{d_1}$, $n \equiv r_2 \pmod{d_2}$
- 这里除数为 d_1, d_2 互素 Here d_1, d_2 are relatively prime
- $nd_2 \equiv r_1 d_2 \pmod{d_1 d_2}$, $nd_1 \equiv r_2 d_1 \pmod{d_2 d_1}$
- 正反运用辗转相除法可得整数 a_1, a_2 满足 $a_1 d_1 + a_2 d_2 = 1$
Apply Euclidean algorithm forward and reverse we can obtain integers a_1, a_2 satisfying $a_1 d_1 + a_2 d_2 = 1$
- $nd_2 a_2 \equiv r_1 d_2 a_2 \pmod{d_1 d_2}$, $nd_1 a_1 \equiv r_2 d_1 a_1 \pmod{d_2 d_1}$
- $n \equiv r_1 a_2 d_2 + r_2 a_1 d_1 \pmod{d_1 d_2}$

费马小定理 Fermat's Little Theorem

- 费马于 1640 年在给朋友的信中提到证明了此定理，说很想把证明一起写给他但又担心会使信过长（是不是有点熟悉的样子）。 In 1640 Fermat mentioned this theorem in a letter to his friend. He said he wanted to send the proof in the letter too but was afraid of making the letter too long (sounds familiar isn't it)
- 费马小定理可以表述为 2 的幂的序列除以奇素数 p 的余数序列循环且周期可以整除 $p - 1$ 。 Fermat's Little Theorem can be stated this way: dividing the sequence of powers of 2 by prime $p > 2$, the remainders are periodic with the period dividing $p - 1$
- $p = 3 : \{1, 2, 4, 8, 16, 32, \dots\} \equiv \{1, 2, 1, 2, 1, 2, \dots\} \pmod{3}$
- $p = 5 : \{1, 2, 4, 8, 16, 32, \dots\} \equiv \{1, 2, 4, 3, 1, 2, 4, 3, \dots\} \pmod{5}$

埃尔德什的 $2^k + p$ 反例 Erdős' Counter-Examples to $2^k + p$

- 我们虽然用概率探索法说明了 $2^k + p$ 反例密度大于 0，但这并不算做证明仍然只算猜测 Even though we illustrated the positive density of counter examples for $2^k + p$, but heuristics do not constitute proofs, only educated guesses
- 1950 年埃尔德什巧妙的以同余类覆盖全体自然数 $k = \{1, 2, 3, \dots\}$ ，从而找到密度大于零的一组反例 In 1950 Erdős found a sequence of counter-examples with positive density using congruence classes to cover all natural numbers $k = \{1, 2, 3, \dots\}$

$$2^{24} - 1 = 16777215 = 3^2 \times 5 \times 7 \times 13 \times 17 \times 241$$

除以 周期 2 的幂序列的余数

Mod Period Remainders of $\{2^k, k = 0, 1, 2, 3, 4, 5, \dots\}$

3	2	$\{1, 2, 1, 2, 1, 2, 1, \dots\}$
5	4	$\{1, 2, 4, 3, 1, 2, 4, 3, 1, \dots\}$
7	3	$\{1, 2, 4, 1, 2, 4, 1, \dots\}$
13	12	$\{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1, \dots\}$
17	8	$\{1, 2, 4, 8, 16, 15, 13, 9, 1, \dots\}$
241	24	$\{1, 2, 4, 8, 16, 32, 64, 128, 15, 30, 60, 120, 240, 239, 237, 233, 225, 209, 177, 113, 226, 211, 181, 121, 1, \dots\}$

Table: 2 的幂的同余类 $2^k \pmod p$ congruence classes

以周期为模组建同余覆盖 Cover by Congruence Class of Periods

2^k 的同余类	k 的同余类	被覆盖的除以 24 的同余类
2^k congruence	k congruence	Congruence classes mod 24 covered
1 mod 3	0 mod 2	{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22}
2 mod 5	1 mod 4	{1, 5, 9, 13, 17, 21}
1 mod 7	0 mod 3	{0, 3, 6, 9, 12, 15, 18, 21}
11 mod 13	7 mod 12	{7, 19}
8 mod 17	3 mod 8	{3, 11, 19}
121 mod 241	23 mod 24	{23}

Table: 覆盖除以 24 的所有 24 个同余类 Covering of all congruence classes of mod 24

埃尔德什的同余覆盖 Erdős' Covering by Congruence Classes

- 当我们挑选关于 k 的同余类去覆盖全体自然数时，就得到相对应的关于 2^k 的同余类如上表第一列。Once we selected congruence classes about k to cover all natural numbers, we also obtain the corresponding congruence classes about 2^k , as listed in the first column of the above table
- 于是运用中国剩余定理可从六个关于 2^k 的同余类解出
 $n \equiv 2036812 \pmod{(2^{24} - 1)/3 = 5592405}$
Above solution is then obtained applying the Chinese remainder theorem to the 6 congruence classes about 2^k
- Exercise** 试说明为什么这样的 n 构成了 $2^k + p$ 的反例 Try explain why such n constitutes counter-examples of $2^k + p$

埃尔德什 #205 问题 Erdős Problem #205

- 既然 $2^k + p$ 问题中素数不够用来覆盖，那么减弱成比素数更密的集合呢？比如像哥德巴赫猜想研究中考虑的半素数，即两个素数的乘积？埃尔德什提出的弱版直接弱化到密度约为一半左右，而根据素数定理素数的密度为零 Since prime is not enough for $2^k + p$ problem, what about denser sets, say the semiprimes used in the study of Goldbach's conjecture? The version Erdős proposed directly weakens to a set of $\sim 1/2$ density, note the density of primes is 0 according to prime number theorem
- 埃尔德什提出的覆盖自然数方案为 $2^k + m, \Omega(m) < \log \log m$
Above is Erdős' proposed covering for natural numbers

哈代-拉马努金定理 $\Omega(m)$, $\omega(m)$, Hardy-Ramanujan Theorem

- $\Omega(m), \omega(m)$ 分别代表计入重复的素因子个数和不计重复的素因子个数 $\Omega(m), \omega(m)$ represent number of prime factors, counting duplicity and not counting duplicity, respectively
- $m = 12 = 2^2 \times 3, \omega(12) = 2, \Omega(12) = 2 + 1 = 3$
- $m = 72 = 2^3 \times 3^2, \omega(72) = 2, \Omega(72) = 3 + 2 = 5$
- 1917 年哈代和拉马努金证明了满足以下的 $\{m\}$ 集合密度为 1:
$$|\omega(m) - \log \log m| < (\log \log m)^{1/2+\epsilon}$$

In 1917 Hardy and Ramanujan proved the set $\{m\}$ satisfying the above inequality has a density of 1
- 这一结果同样适用于 $\Omega(m)$ Same applies to $\Omega(m)$

埃尔德什 #205 问题 Erdős Problem #205

- 2025 年 10 月 16 日 Wouter van Doorn 率先在埃尔德什问题论坛上贴出概率辨析的结果质疑 #205 猜想为假 On October 16, 2025 Wouter van Doorn first posted heuristic arguing the falsehood of #205 conjecture
- 对于每个 k , $\Omega(n - 2^k) < \log \log(n - 2^k)$ 的概率为 $1/2$
- k 可以取值到 $\log_2 n$, 那么伯努利试验连续失败的概率为 $(1/2)^{\log_2 n} = 1/n$
Since k can go up to $\log_2 n$, the probability of consecutive failures of Bernoulli trials is $(1/2)^{\log_2 n} = 1/n$
- 由调和级数的发散可知当有无限多个反例 By the divergence of harmonic series infinitely many counter-examples should exist

AI 的反例构造简化版 AI's Counter-Example Simplified

- 我这里对 AI 的证明作了一些简化 Here I make some simplification to AI's disproof
- E 为任意自然数，构造一套有 $E+2$ 个同余方程的方程组 We construct $E+2$ congruence equations
- $\{p_1, p_2, \dots, p_E\} = \{5, 7, 11, 13, 17, 19, \dots\}$
- $n \equiv 0 \pmod{2^E}$
- $n \equiv 0 \pmod{3}$
- $n \equiv 2^{k-1} \pmod{p_k^E}, k = 1, 2, 3, \dots, E$
- 运用中国剩余定理解出 $m < M = 2^E \times 3 \times 5^E \times 7^E \times \dots \times p_E^E$ is solved via Chinese remainder theorem

AI 的反例构造简化版 AI's Counter-Example Simplified

- 素数定理的一个等价的素数阶乘形式为

$$\log(2 \times 3 \times 5 \times \dots \times p) \sim p$$

Above is the equivalent primorial form of the prime number theorem

- 运用素数定理可得到

$$\log M \sim E^2 \log E$$

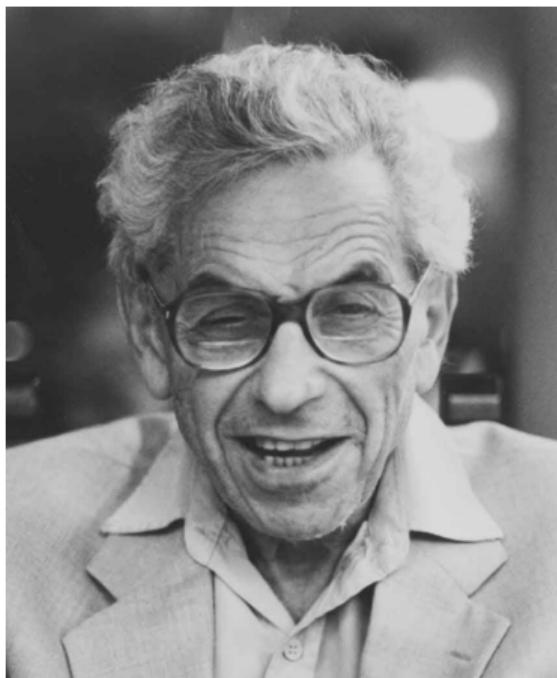
Above can be derived from prime number theorem

- $\log \log M \sim 2 \log E$

- $E \sim \sqrt{2 \log M / \log \log M} \gg \log \log m$

保罗·埃尔德什 Paul Erdős (1913-1996) Q & A

Source: Rutgers University (<https://sites.math.rutgers.edu/~sg1108/People/Math/Erdos>)



参考资料 References

- 埃尔德什问题论坛关于埃尔德什 #205 问题的讨论
Discussion of Erdős Problem #205 on Erdős Problem forum
- Pat Sothanaphan 对 AI 推翻 #205 猜想的解读笔记
Pat Sothanaphan's note translating AI's disproval in lean
- Leeham 2026 年 1 月 11 日发布贴
Leeham's annoucement posts on January 11, 2026