香港大學數學系主辦公開講座

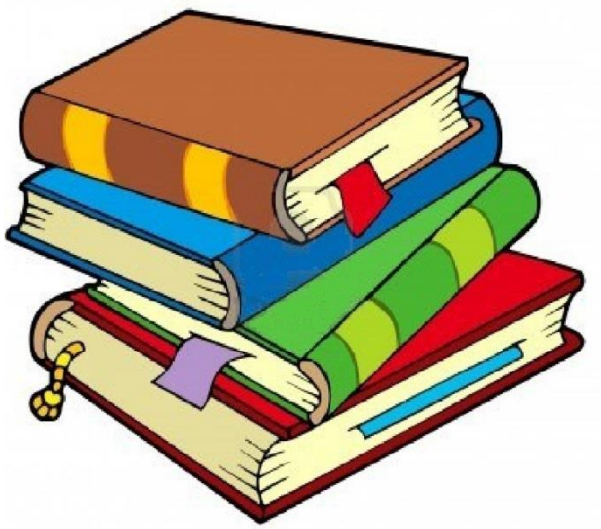
閒談 質數

——一些猜想和故事

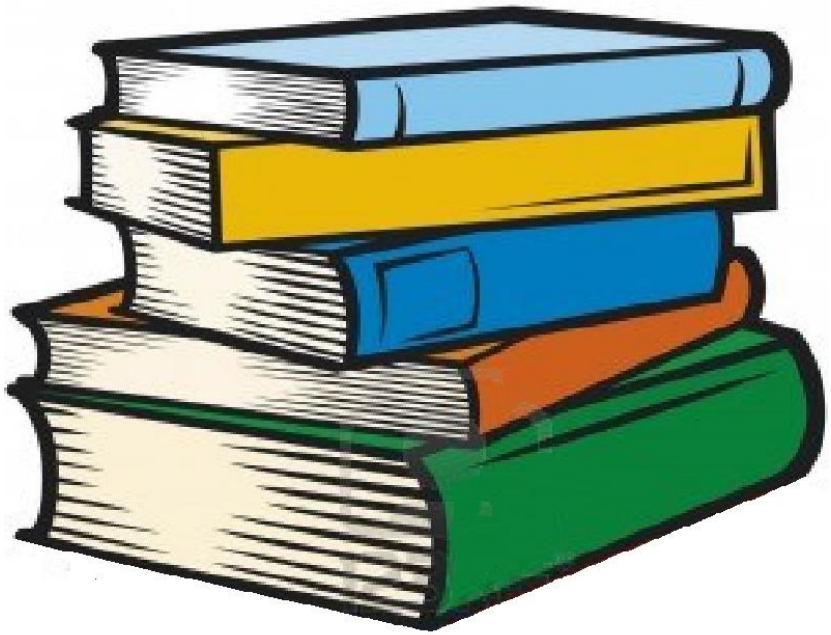
劉旭金博士

2014年2月15日

導引



四本故事書



五個未來的經典結果

《數學女孩》(数学ガール)

作家:結城浩 (程式設計師)

內容簡介: 喜歡數學、不擅長與人交流的男主角在升上高中後， 以為會跟國中時期一樣孤單。但竟然遇到了同樣對數學有興趣的兩位女孩米爾迦、蒂蒂

《數學女孩》蒂蒂篇

插圖來自《数学ガール》漫画(結城浩/茉崎ミュキ)

《數學女孩》蒂蒂篇


嗯，5和7都是質數沒錯——但是5和7都只是質數的一個例子。「舉例」和「定義」並不一樣！
啊，好的。質數就是……『祇有1和自己本身能整除自己的數』，這是數學老師叫我們一定要記起來的定義。
妳認爲這個定義正確嗎？
啊，1不是質數。老師好像也是這樣教的，不過……

《數學女孩》蒂蒂篇

Euclid (歐幾里得)

Euclid (325-265 BC)

Elements Book I - XIII

- 生於公元前325-265，古希臘數學家，被稱為「幾何之父」
- 著作 Elements《幾何原本》包含許多幾何知識，並樹立了一套系統方法，成為歐洲數學的基礎
- 《幾何原本》共有13卷，第七卷及第九卷中有討論質數

Euclid 的兩大貢獻(一)

《幾何原本》第七卷

Fundamental Theorem of Arithmetic (算術基本定理)

質因子分解:

每個大於 1 的自然數均可寫為質數的積

唯一性:

這些質因子按大小排列之後，寫法僅有一種方式

例如: $12 = 2^2 \cdot 3$,

$12 = 1 \cdot 2^2 \cdot 3$,

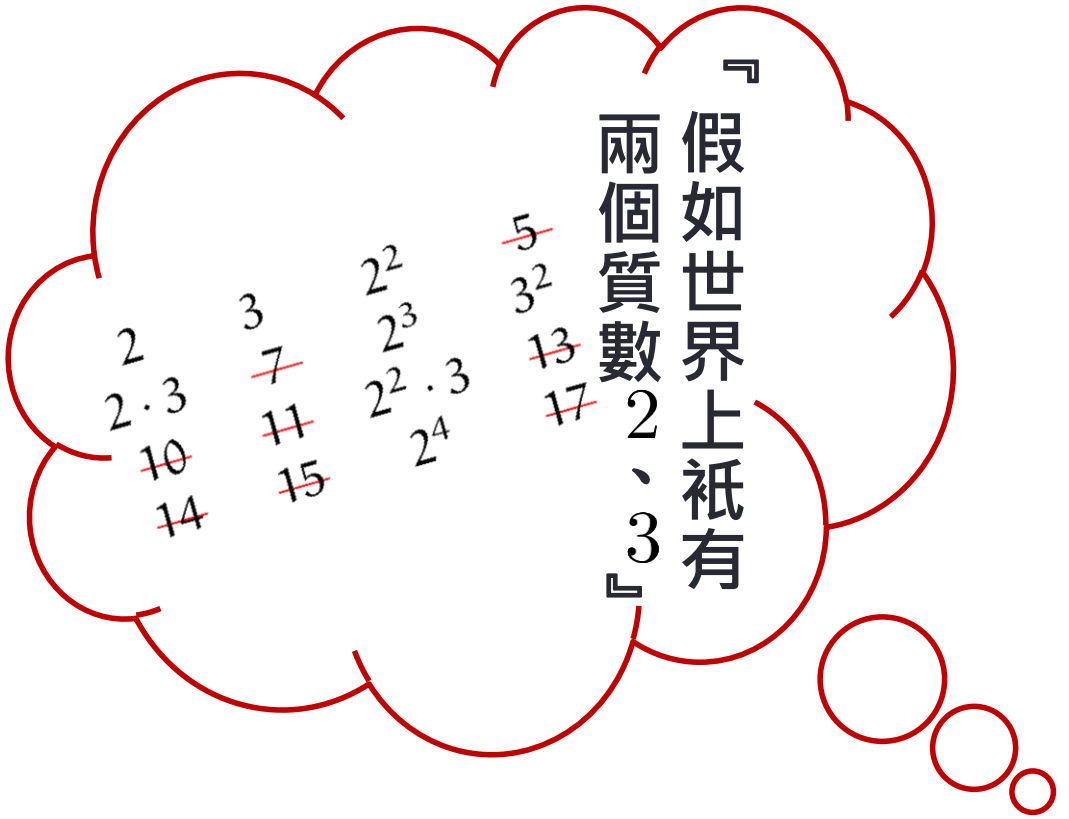
$12 = 1 \cdot 1 \cdot 2^2 \cdot 3$

$2014 = 2 \cdot 19 \cdot 53$

Euclid 的兩大貢獻(二)

《幾何原本》第九卷

Theorem: 質數有無窮多個



Euclid 的兩大貢獻(二)

《幾何原本》第九卷

Theorem: 質數有無窮多個

證明：假設只是有限多個質數 $p_1, p_2, \cdots, p_n$

考慮

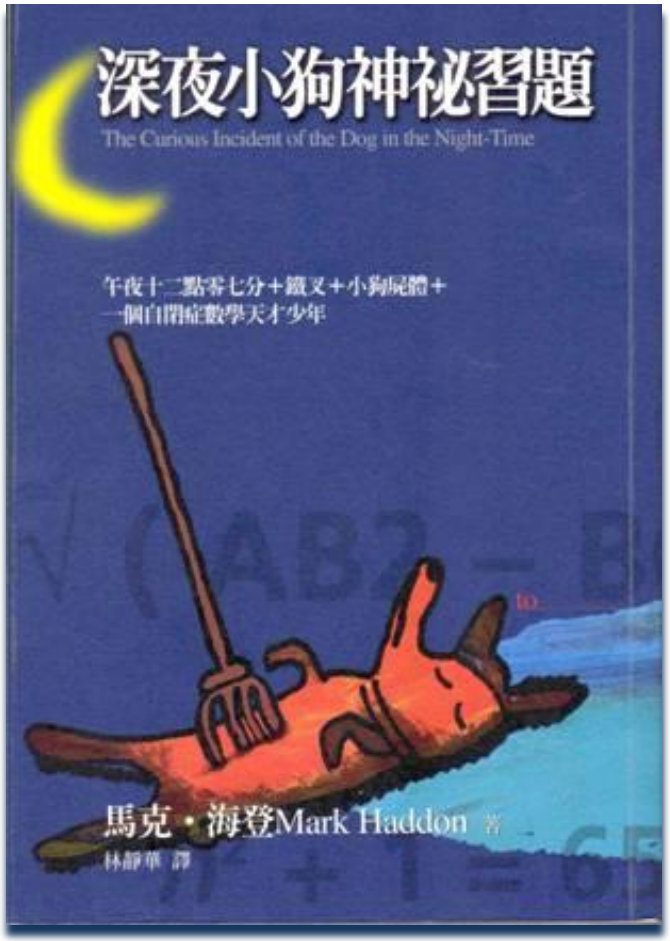
$$N = p_1 p_2 \cdots p_n + 1$$

$p_1, p_2, \cdots, p_n$ 中沒有一個質數能整除 N

但 N 可寫為 $p_1, p_2, \cdots, p_n$ 的積

出現矛盾

《深夜小狗神秘習題》
(The Curious Incident of the Dog in the Night-Time)



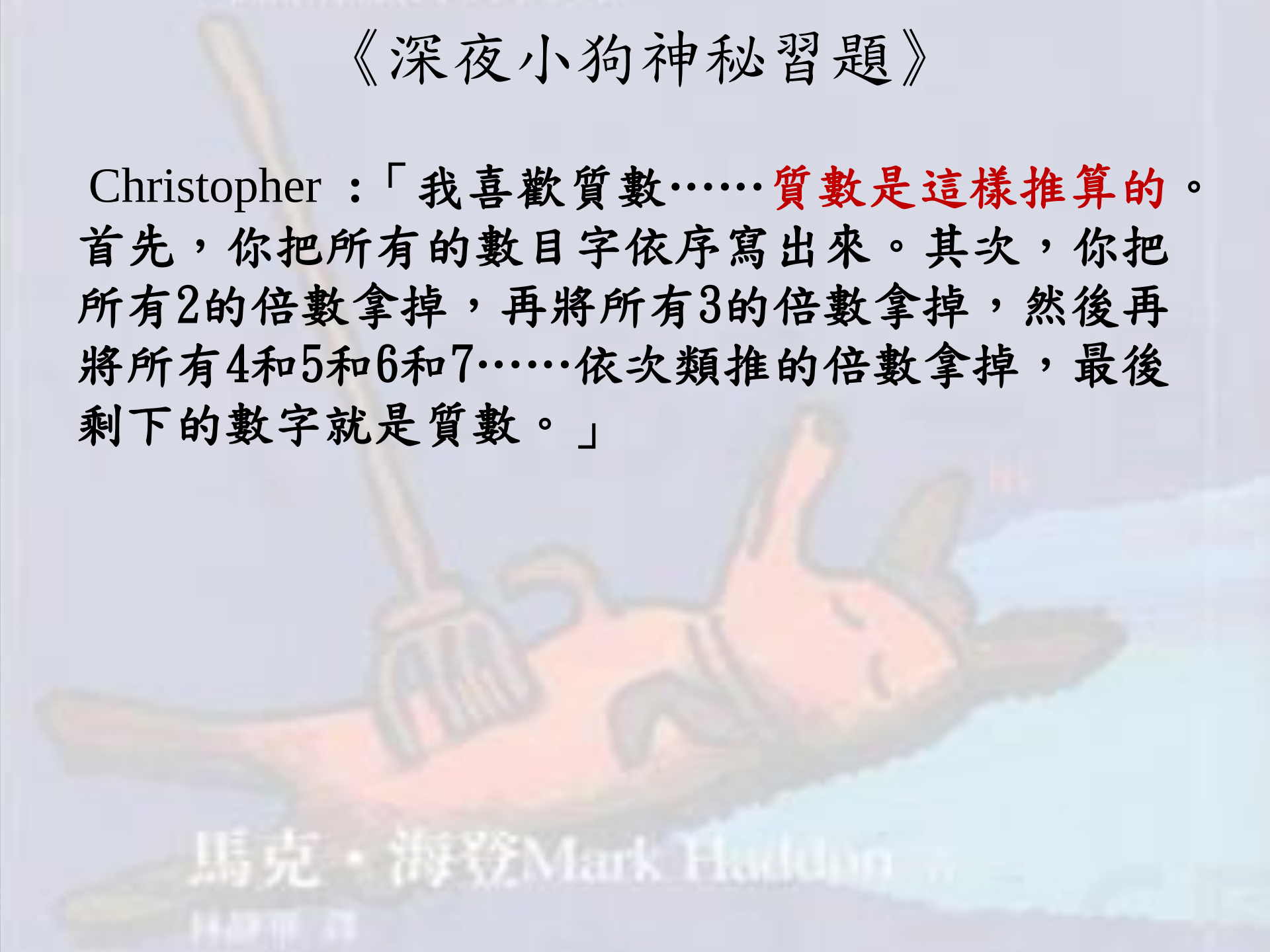
作者: Mark Haddon (英國)

- 2003年「惠布瑞特年度最佳好書獎」
- 2004年聖誕節登上暢銷排行榜冠軍（這是七年來《哈利波特》首次位居第二名）

內容簡介: 某個深夜裡，十五歲患有自閉症的數學天才Christopher發現隔壁鄰居家的小狗被鐵叉刺死。Christopher決定自己來當偵探, 調查兇手、真相……

《深夜小狗神秘習題》

Christopher：「我喜歡質數……質數是這樣推算的。首先，你把所有的數目字依序寫出來。其次，你把所有2的倍數拿掉，再將所有3的倍數拿掉，然後再將所有4和5和6和7……依次類推的倍數拿掉，最後剩下的數字就是質數。」



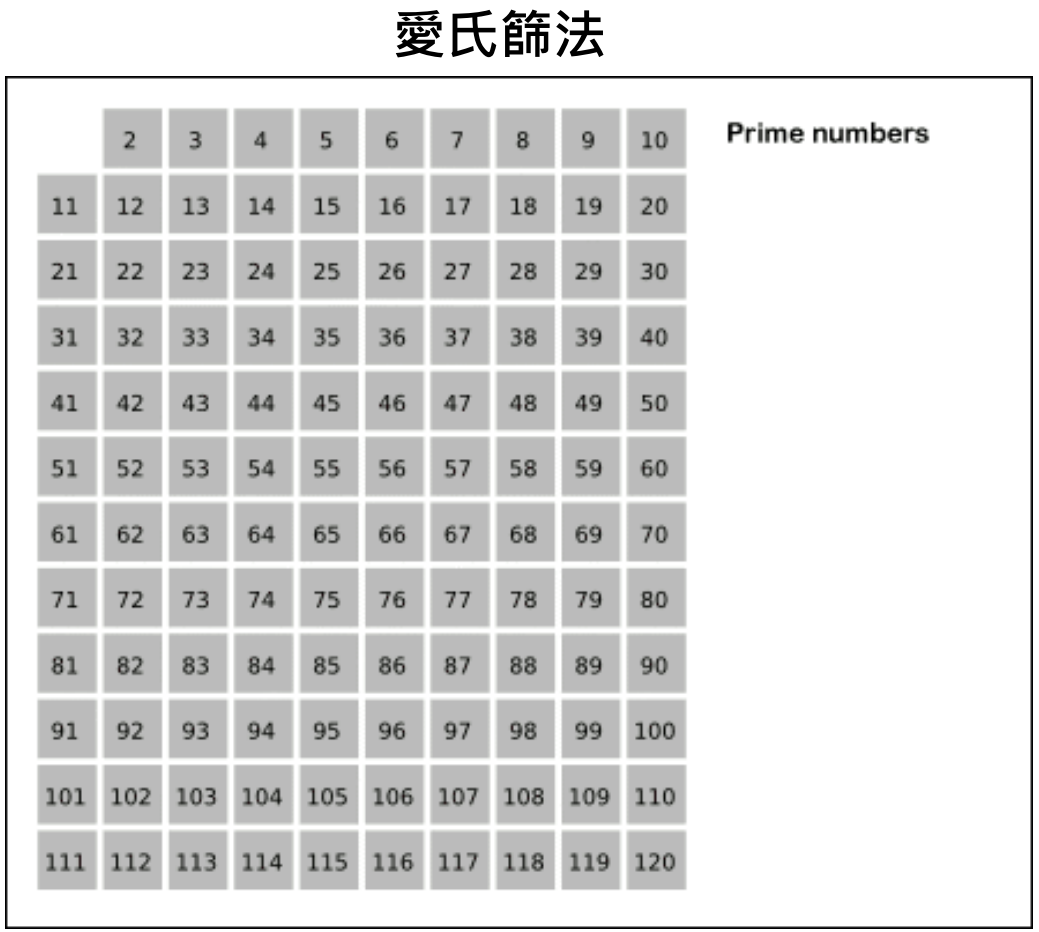
愛氏篩 (Sieve of Eratosthenes)

- 公元前250年，由古希臘數學家Eratosthenes提出
- 尋找 2至 n 之間的質數的步驟:

(a) 取出序列中的第一個數字

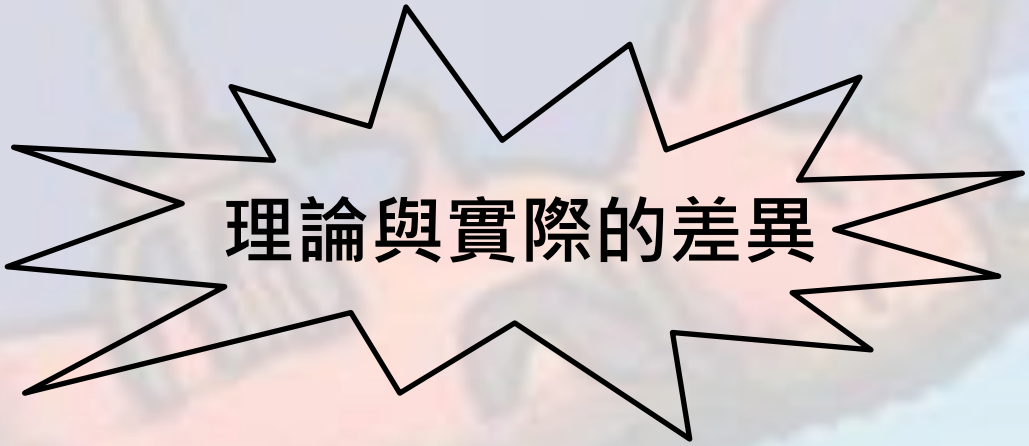
(b) 刪去該數字的倍數

(c) 對剩下的數列重覆步驟 (a)



《深夜小狗神秘習題》

Christopher：「**推算質數的方法很簡單**，但是沒有人能想出一個簡單的方程式來告訴你一個非常大的數目字是不是質數，或者它的下一個數目字是不是質數。如果一個數字真的很大很大，**說不定連計算機也要花好幾百年的時間才能算出它是不是質數**」



Gauss (高斯) 的先見之明

Gauss (1777-1855)

- 生於1777-1855，德國數學家
- 歷史上最重要數學家之一，被譽為「數學王子」

Mathematics is the Queen of Science. Number Theory is the Queen of Mathematics.

- Gauss 提出「鑒別一個自然數是質數還是合成數是一個重要的問題」
- 「如何能有效率地測試是否質數？」
- 何謂有效率？

測試法與效率

- 計算機科學中，以時間複雜度 (Time Complexity) 量度算法的效率
- Time Complexity 是輸入值長度ℓ的函數
- 若函數是多項式，這算法就定義為有效率

例子：

測試法	Time Complexity	有效率
X	ℓ^6	✓
Y	ℓ^{2014}	✓
Z	10^{ℓ}	✗

質數測試法的效率問題

- 用愛氏篩測試數字是否質數:

  ℓ = “數字的數位”

  （例如:數字 20140215 的 $\ell = 8$ ）

  Time Complexity : 10^{ℓ} (Proof skipped)

  所以，愛氏篩質數測試法不是有效率

- Gauss 以後的150年，計算機科學家(及數學家)一直尋找有效率的質數測試法，即測試法的 Time Complexity 是 ℓ 的多項式，但一直沒成功

- 2002年，三位印度的計算機科學家成功突破

AKS質數測試法

- 2002年，Agrawal-Kayal-Saxena 找到有效率的測試法

Agrawal (1966-)

Kayal
(Microsoft Researcher)

Saxena
(Professor)

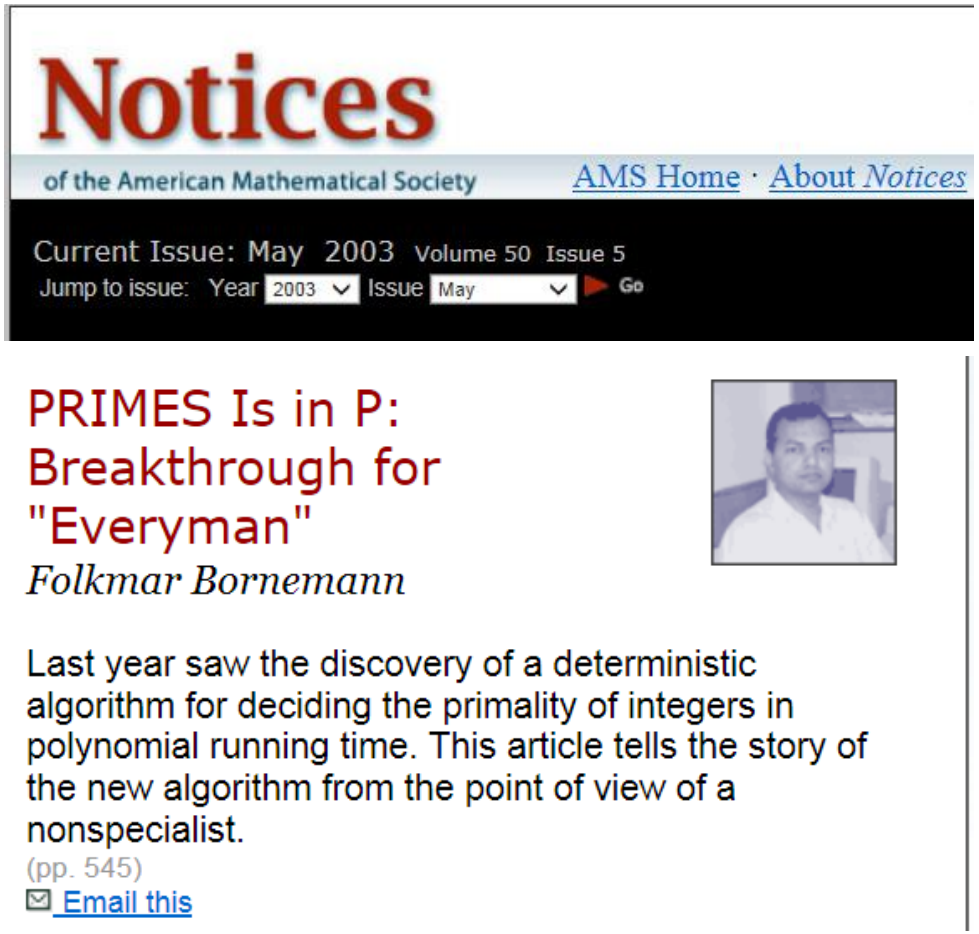
AKS質數測試法

Input: integer $n > 1$.

1. If $(n = a^b$ for $a \in \mathcal{N}$ and $b > 1)$, output COMPOSITE.
2. Find the smallest r such that $o_r(n) > \log^2 n$.
3. If $1 < (a, n) < n$ for some $a \leq r$, output COMPOSITE.
4. If $n \leq r$, output PRIME.[1]
5. For $a = 1$ to $\lfloor \sqrt{\phi(r)} \log n \rfloor$ do
   if $((X + a)^n \neq X^n + a \pmod{X^r - 1, n})$, output COMPOSITE;
6. Output PRIME.

AKS質數測試法

- AKS質數測試法的Time Complexity: ℓ^8
- 獲得了許多獎項



美國數學學會 (2003)

大質數與電子前鋒基金會(EFF)

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

HOME | ABOUT | OUR WORK | DEEPLINKS BLOG | PRESS ROOM

EFF Cooperating Computing Awards
Rules
News
Frequently Asked Questions
Prime Number Resources and Information
Press Release Announcing Awards
1,000,000 decimal digits prize
10,000,000 decimal digits prize

EFF Cooperative Computing Awards 計算獎項

Thinking about claiming this award? You MUST read this entire page first!

The Electronic Frontier Foundation (EFF), the first civil liberties group dedicated to protecting the health and growth of the Internet, is sponsoring cooperative computing awards, with over half a million dollars in prize money, to encourage ordinary Internet users to contribute to solving huge scientific problems.

Through the EFF Cooperative Computing Awards, EFF will confer prizes of:

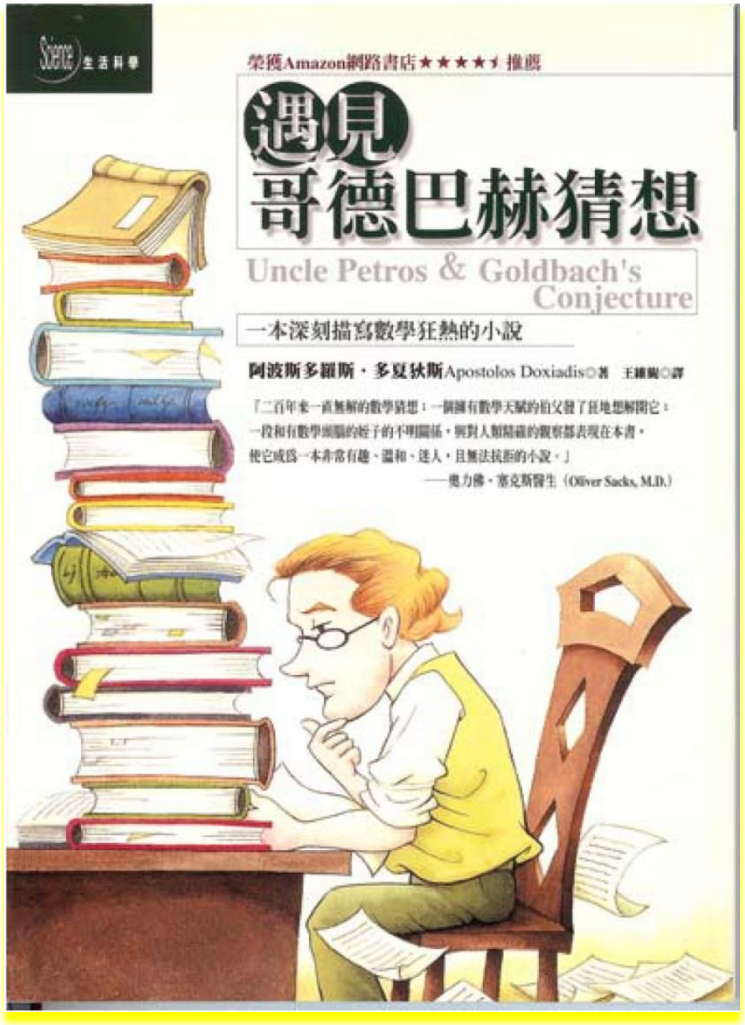
- **$50,000** to the first individual or group who discovers **a prime number with at least 1,000,000 decimal digits** (awarded Apr. 6, 2000) 5萬美元，至少一百萬個位
- **$100,000** to the first individual or group who discovers **a prime number with at least 10,000,000 decimal digits** (awarded Oct. 22, 2009) 10萬美元，至少有一千萬個位
- **$150,000** to the first individual or group who discovers **a prime number with at least 100,000,000 decimal digits**
- **$250,000** to the first individual or group who discovers **a prime number with at least 1,000,000,000 decimal digits**

Largest known prime

rank	prime	digits	who	when
1	$2^{57885161}-1$	17425170	G13	2013
2	$2^{43112609}-1$	12978189	G10	2008
3	$2^{42643801}-1$	12837064	G12	2009
4	$2^{37156667}-1$	11185272	G11	2008
5	$2^{32582657}-1$	9808358	G9	2006
6	$2^{30402457}-1$	9152052	G9	2005
7	$2^{25964951}-1$	7816230	G8	2005
8	$2^{24036583}-1$	7235733	G7	2004
9	$2^{20996011}-1$	6320430	G6	2003
10	$2^{13466917}-1$	4053946	G5	2001

- 15萬美元，至少有1億個位
- 25萬美元，至少有10億個位

《遇見哥德巴赫猜想》
(Uncle Petros & Goldbach's Conjecture)



作家:Apostolos Doxidis (希臘)

數學天才Petros 窮其一生，試圖證明哥德巴赫猜想。故事敘述 Petros 的際遇，以及在數學學術圈中的價值觀。……

哥德巴赫猜想 (Goldbach Conjecture) 的由來

Goldbach (哥德巴赫)

- 生於1690-1764，德國數學家

Euler (歐拉)

- 生於1707-1783， 瑞士數學家
- 歷史上最重要數學家之一

Euler (1707-1783)

在1742年，Goldbach 與 Euler通信，Goldbach 提出以下猜想，現稱哥德巴赫猜想。

哥德巴赫猜想(Goldbach Conjecture)

- Weak Goldbach Conjecture
  任一大於5的奇數，都可表示成三個質數之和

  $$\text{奇數} = p_1 + p_2 + p_3$$

- Strong Goldbach Conjecture
  任一大於2的偶數, 都可表示成兩個質數之和

  $$\text{偶數} = p + p'$$

例子:

$$\begin{aligned}
7 &= 2+2+3 \\
9 &= 3+3+3 \\
11 &= 3+3+5 \\
13 &= 3+5+5 \\
&\vdots \\
2013 &= 3+997+1013
\end{aligned}$$

$$\begin{aligned}
4 &= 2+2 \\
6 &= 3+3 \\
8 &= 3+5 \\
10 &= 5+5 \\
&\vdots \\
2014 &= 983+1031
\end{aligned}$$

Diophantus’問題簡介

- 原於公元三世紀的 Diophantus

線性方程組

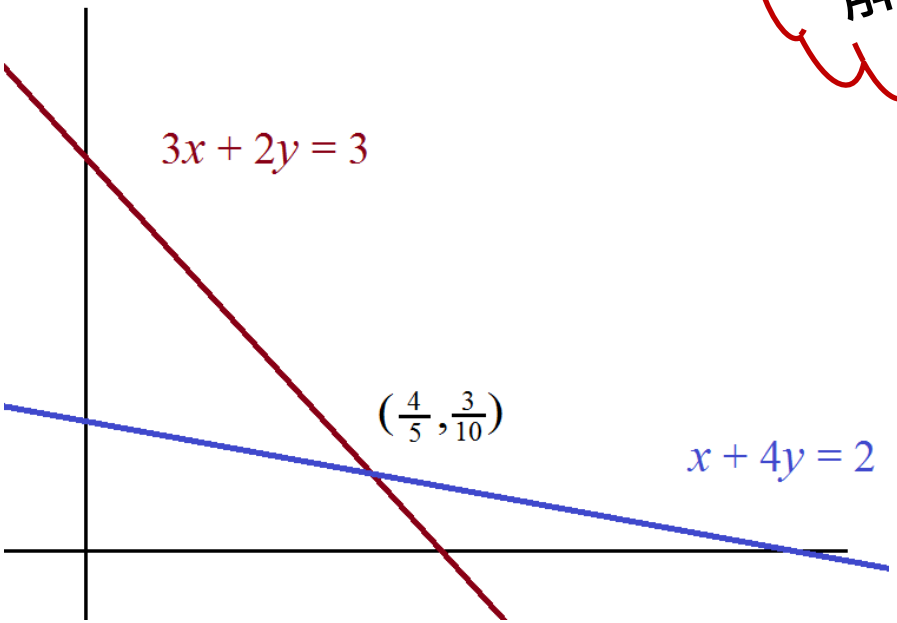
$$\begin{cases} 3x+2y = 3 \\ x+4y = 2 \end{cases}$$

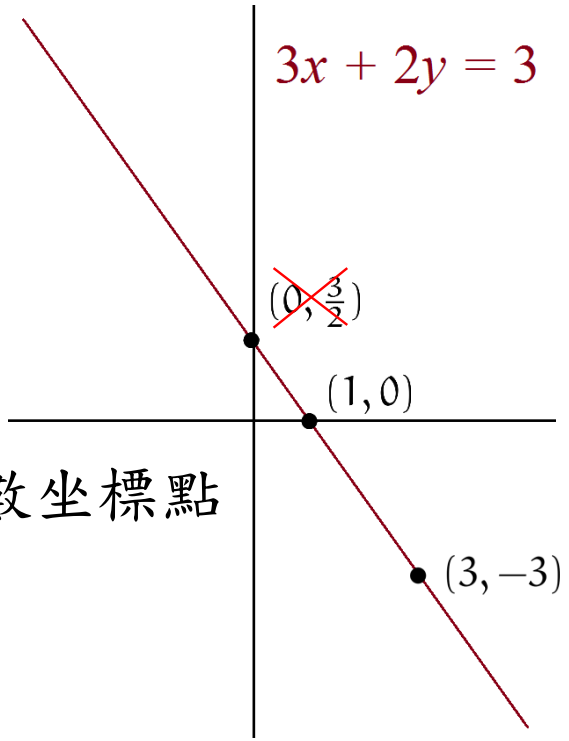
只求整數解

二元一次不定方程

$$3x+2y=3$$

$(0,\frac{3}{2})$, $(1,0)$, $(3,-3)$, $\cdots$





整數坐標點

Diophantus’問題

- Diophantus’問題是指求方程或方程組的整數解
  (Solve equations in integers)

例子:

求以下方程/方程組的整數解

(a) $x + y + z = 15$

(b) $\begin{cases} x + y + z = 2 \\ x + 2y + 3z = 15 \end{cases}$

(c) $x^2 - 10y^2 = 9$

(d) $x^2 + y^2 = z^2$

Goldbach's 問題

Diophantus' Problem: 求方程或方程組的整數解
(solve in integers)

Goldbach's Problem: 求方程或方程組的質數解
(solve in primes)

Strong Goldbach Conjecture: 對於每個大於2的雙數n，
$x+y=n$ 有質數解

Weak Goldbach Conjecture: 對於每個大於5的單數n，
$x+y+z=n$ 有質數解

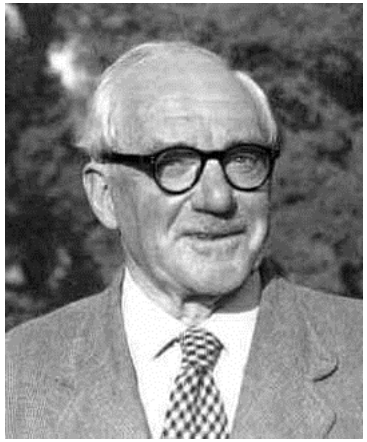
Goldbach Conjecture 只是一個特殊的 Goldbach's Problem

Weak Goldbach Conjecture 的進展過程

- 20 世紀初，英國數學家 Hardy and Littlewood 發明了圓法來處理這個 Goldbach problem

對單數 $n \le 10^{6846169}$
$n = p_1 + p_2 + p_3$??

Hardy (1877-1947)



Littlewood (1885-1977)

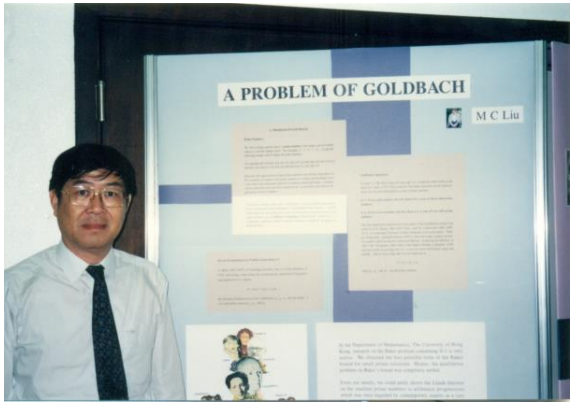
- 1937年，前蘇聯數學家 I.M. Vinogradov 建基於圓法證明了:

任一大於 $10^{6846169}$ 的奇數，都可以表示成三個質數之和

Vinogradov (1891-1983)

Weak Goldbach Conjecture 的進展過程

- 2002年，廖明哲教授(HKU)與王天澤將 $10^{6846169}$ 縮小至 10^{1347}



廖明哲

王天澤(1963-)

Weak Goldbach Conjecture 的進展過程

- 2013年 Helfgott (CNRS) 宣布完全證明 Weak Goldbach Conjecture.

Helfgott (1977-)

January/February 2014

其他 Goldbach's Problem

- 線性方程組的質數解

  1990年，廖明哲教授與曾啟文教授證明了:

  當 m, n 滿足一些基本條件，以下
  的方程組有質數解

$$\begin{cases} x + y + z + u + v = m \\ x + 2y + 3z + 4u + 5v = n \end{cases}$$

- 華羅庚於1938年證明: 當 N 滿足一些條件，

$$x^2 + y^2 + z^2 + u^2 + v^2 = N$$

  有質數解 (i.e. N 可寫成5個質數平方之和)

《博士熱愛的算式》
(博士の愛した数式)

作家:小川洋子

- 2004年，第一屆書本大獎及第五十五屆讀賣文學獎
- 改編成電影於2006年公映

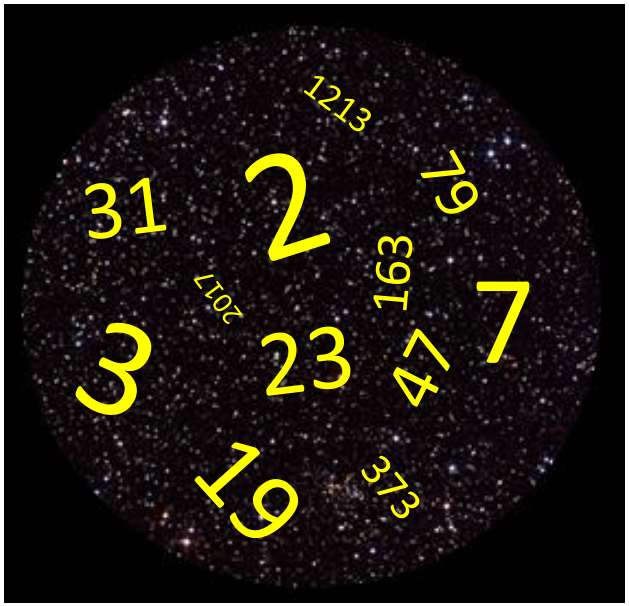
內容簡介: 數學博士在車禍後，對於所有發生的事只能維持80分鐘的記憶。他的嫂子聘請了管家杏子照顧他。雖然每一天博士都忘記杏子，但數學輕輕地連繫著她和博士之間的相處……

管家杏子:

「在這個世界上，質數是博士的最愛。

我認為質數的魅力在於**無法說明出現的秩序**。…… 無法根據一定的規則預測質數的出現。這種惱人的反覆無常，使追求完美的博士完全拜倒在它的石榴裙下。」

質數的宏觀規律



- 設 $\pi(x)$ = 少於 x 的質數數量

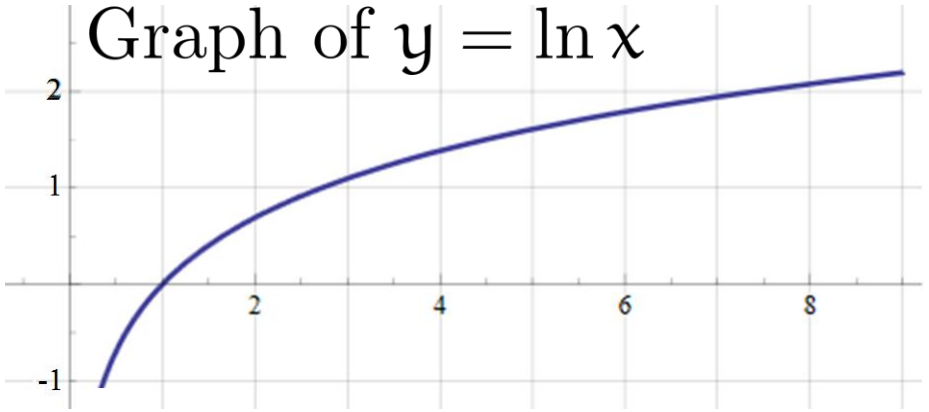
  e.g. $\pi(10) = 4, \pi(15) = 6$

- 18世紀末，法國數學家Legendre及德國數學家Gauss分別地發現

  $\pi(x)$ 與 $\dfrac{x}{\ln x}$ 愈來愈近

Legendre
(1752-1833)

Gauss
(1777-1855)



$\pi(x) \sim \frac{x}{\ln x}$ 的數據支持

x	$\pi(x)$=少於 x 的質數數量	$x/\ln x$	$\frac{\pi(x) - x/\ln x}{x/\ln x}$
10^2	25	21.71	0.151
10^3	168	144.7	0.161
10^4	1,229	1,085	0.132
10^5	9,592	8,685	0.104
10^6	78,498	72,382	0.084
10^7	664,579	620,420	0.071
10^8	5,761,455	5,428,681	0.061
10^9	50,847,534	48,254,942	0.054
10^{10}	455,052,511	434,294,481	0.048
10^{11}	4,118,054,813	3,948,131,653	0.043
10^{12}	37,607,912,018	36,191,206,825	0.039
10^{13}	346,065,536,839	334,072,678,387	0.034
10^{14}	3,204,941,750,802	3,102,103,442,166	0.033
10^{15}	29,844,570,422,669	28,952,965,460,216	0.031
10^{16}	279,238,341,033,925	271,434,051,189,532	0.029

相對誤差
Relative error

質數的分佈

- 對 $x > 0$，定義 $\pi(x)$為質數計數函數

Prime Number Theorem (質數分佈定理)：$\pi(x) \sim \frac{x}{\ln x}$

A Puzzle

	質數的孤獨	Introduction to Number Theory
第一頁	無頁號	無頁號
第二頁	0002	2
第三頁	0003	3
最後一頁	1787	572

問題: 為什麼「質數的孤獨」較薄?

Ans: 它的頁號全是質數

$$\frac{1787}{\ln 1787} \approx 238.6\,, \quad \pi(1787) = 276$$

質數的微觀規律(一)

質數表 (1-175)

2	3	5	7	11	13	17	19
23	29	31	37	41	43	47	53
59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131
137	139	149	151	157	163	167	173

觀察:找到等差數列 (Arithmetic Progression)

- 三項: 3, 5, 7
- 四項: 5, 11, 17, 23
- 五項: 5, 11, 17, 23, 29
- 六項: 7, 37, 67, 97, 127, 157

$a, a+d, a+2d, \cdots, a+(k-1)d$
(k terms, common difference = d)
e.g. 2, 6, 10, 14,
(四項, 等差 = 4)

尋找質數等差數列

- **Theorem.** If $p, p+d, p+2d, \cdots, p+(k-1)d$ are all primes and Q = the product of all primes $< k$, then Q divides d.

(i.e. d 是Q的倍數)

$$\begin{bmatrix} k = \text{number of terms} \\ d = \text{common difference} \end{bmatrix}$$

e.g. 5, 11, 17, 23, 29 $\quad (d = 6,\ k = 5,\ Q = 2 \times 3 = 6)$

257, 269, 281, 293 $\quad (d = 12,\ k = 4,\ Q = 2 \times 3 = 6)$

- 不容易尋找多項的質數等差數列

e.g. 如果 $p, p+d, p+2d, \cdots, p+13d$ 是質數等差數列，

那麼 $d \geq 30030$ (因為 $Q = 2 \cdot 3 \cdots 11 \cdot 13 = 30030$)

[$k\uparrow \Rightarrow Q\uparrow \Rightarrow d\uparrow$, 愈難尋找]

尋找質數等差數列

- 目前紀錄: 26 項

$$\mathrm{p},\ \mathrm{p}+\mathrm{d},\ \mathrm{p}+2\mathrm{d},\cdots,\ \mathrm{p}+25\mathrm{d} \text{ are all primes, where}$$

$$\mathrm{p} = 43142746595714191,\ \mathrm{d} = 23681770 \times 223092870.$$

Largest known primes in AP [edit]

For prime *q*, *q*# denotes the primorial 2·3·5·7·...·*q*.

As of April 2010, the longest known AP-*k* is an AP-26, found on April 12, 2010 by Benoãt Perichon on a PlayStation 3 with software by Jaroslaw Wroblewski and Geoff Reynolds, ported to the PlayStation 3 by Bryan Little, in a distributed PrimeGrid project:[2]

> 43142746595714191 + 23681770·23#·*n*, for *n* = 0 to 25. (23# = 223092870) (sequence A204189 in OEIS)

By the time the first AP-26 was found the search was divided into 131,436,182 segments by PrimeGrid[3] and processed by 32/64bit CPUs, Nvidia CUDA GPUs, and Cell microprocessors around the world.

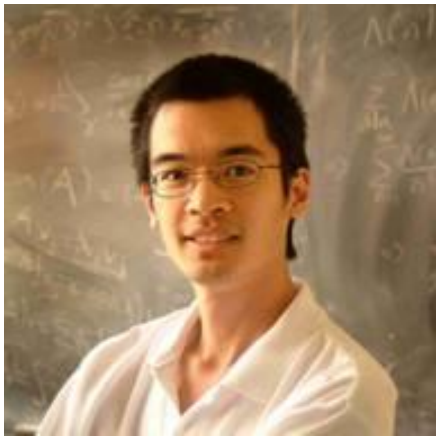
質數中的等差數列

Green-Tao Theorem (格林–陶定理), 2004

質數序列中包含有任意長的等差數列

(For every $k = 1,2,3,4,\ldots$, one can find arithmetic progressions of k terms in primes.)

Ben Green (1977-)
Professor, University of Oxford



Terence Tao (1975-)
Professor, UCLA
2006 Fields Medalist

質數的微觀規律(二)

質數表 (1-175)

2	3	5	7	11	13	17	19
23	29	31	37	41	43	47	53
59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131
137	139	149	151	157	163	167	173

觀察:孿生質數 (Twin Primes) “相距2的質數對”

e.g. $(3,5)$, $(11,13)$, $(29,31)$, $(41,43)$

孿生質數猜想 (Twin Prime Conjecture)

存在無限對孿生質數

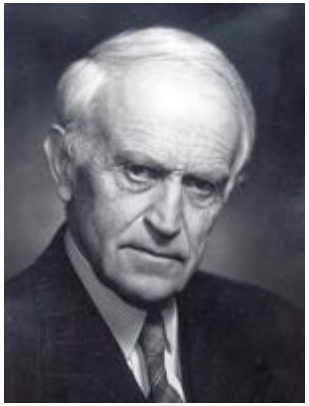
孿生質數: $y - x = 2$ 的質數解

- Twin Prime Problem: 對所有自然數 n,
  $y - x = 2,\ x > n$ 都有一對質數解
- Strong Goldbach Problem: 對所有自然數 $n \geq 2$,
  $y + x = 2n$ 都有一對質數解

觀察:

1) 它們是同類型
2) 如果是求整數解，它們都非常容易解答
   e.g. $x = n, y = n$ 是 $y + x = 2n$ 的一對整數解
3) 質數解: x, y 是質數(1個質因子數量)
   整數解: x, y 是整數(沒限制質因子數量)

孿生質數猜想:二十世紀的方向與成果



Brun (1885-1978)

1915年，挪威數學家 Brun 提出的研究方向:

定立上限 a, b

	整數解		質數解
• x, y 的質因子個數	不限	x:不超過 a	1個
		y:不超過 b	1個
• 難度	非常容易	可處理	困難

若上限成功降至1 (i.e. $a = 1, b = 1$), 即成功解決了 Strong Goldbach Conjecture 及 Twin prime conjecture

孿生質數猜想：二十世紀的方向與成果

Year	Mathematician	(a,b)
1915	V. Brun	(9,9)
1924	H. Rademacher	(7,7)
1932	T. Estermann	(6,6)
1940	A. Buchstab	(4,4)
1956	Y. Wang (王元)	(3,4)
1957	A. Vinogradov	(3,3)
1957	Y. Wang (王元)	(2,3)
1962 1963	C.D. Pan (潘承洞) M. Barban	(1,4) (1,4)
1965	E. Bombieri A. Vinogradov	(1,3) (1,3)
1966 1973	J.R. Chen (陳景潤)	(1,2)

目標：$a = 1,\ b = 1$

- 開啟了中國數學家在 Strong Goldbach 及 Twin Prime 命題研究上的先河
- 著名的**陳氏定理**

- 所有足夠大的偶數$2n$都可表示成 $2n = x + y$，而當中 x是質數，y的質因子個數不超過 2　1+2 定理　2-1 定理
- $y - x = 2$ 有無限對解，y的質因子個數不超過 2，x是質數 (i.e.有無限個質數 p而$p + 2$ 的質因子個數不超過 2.)

發表“1+2”定理證明的曲折

科学网 新闻 论坛 博客 招生招聘 论文 科研网址 实名举报 科学时报社 | 电子杂志订阅 | English | RSS | 直播

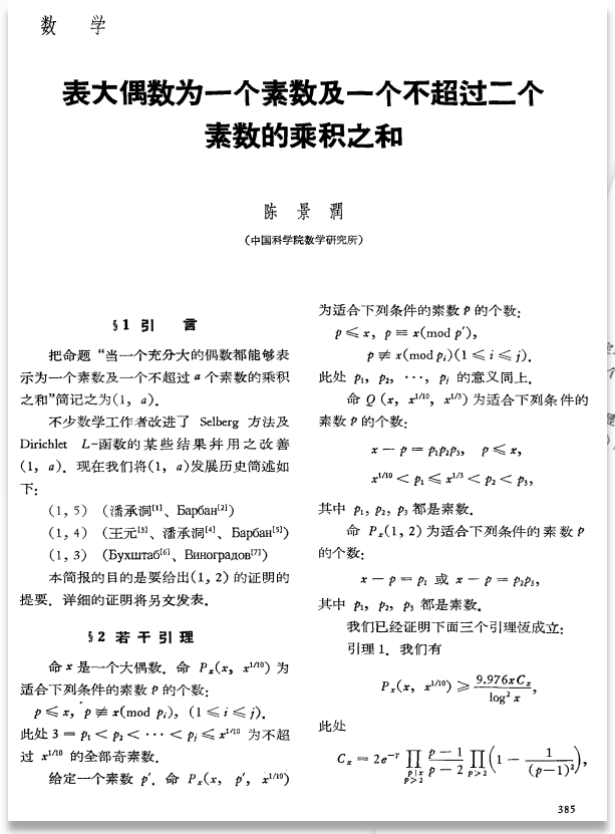
新 闻 NEWS

科学网首页>新闻中心>正文 生命科学 医药健康 基础科学 工程技术 信息科学 资源环境 前沿交叉 政策管理

作者：王丹红 来源：科学时报 发布时间：2009-2-3 2:33:38 小字号 中字号 大字号

王元院士：陈景润是如何做数学的

- 1966年陳景潤証明“1+2”的論文以簡報形式發表於《科學記錄》上
- “文革”開始了，《科學記錄》不能再發表學術文章
- 1972年，陳景潤將“1+2”証明全文投到《中國科學》



数 学

表大偶数为一个素数及一个不超过二个素数的乘积之和

陈 景 润

(中国科学院数学研究所)

§1 引 言

把命题“当一个充分大的偶数都能够表示为一个素数及一个不超过 a 个素数的乘积之和”简记之为$(1, a)$.

不少数学工作者改进了 Selberg 方法及 Dirichlet L-函数的某些结果并用之改善$(1, a)$. 现在我们将$(1, a)$发展历史简述如下:

$(1, 5)$ (潘承洞[1]、Барбан[2])

$(1, 4)$ (王元[3]、潘承洞[4]、Барбан[5])

$(1, 3)$ (Бухштаб[6]、Виноградов[7])

本简报的目的是要给出$(1, 2)$的证明的提要. 详细的证明将另文发表.

§2 若 干 引 理

命 x 是一个大偶数. 命 $P_x(x, x^{1/10})$ 为适合下列条件的素数 p 的个数:

$p \leqslant x$, $p \equiv x \pmod{p_i}$, $(1 \leqslant i \leqslant j)$.

此处 $3 = p_1 < p_2 < \cdots < p_j \leqslant x^{1/10}$ 为不超过 $x^{1/10}$ 的全部奇素数.

给定一个素数 p'. 命 $P_x(x, p', x^{1/10})$ 为适合下列条件的素数 p 的个数:

$p \leqslant x$, $p \equiv x \pmod{p'}$,

$p \not\equiv x \pmod{p_i} (1 \leqslant i \leqslant j)$.

此处 $p_1, p_2, \cdots, p_j$ 的意义同上.

命 $Q(x, x^{1/10}, x^{1/3})$ 为适合下列条件的素数 p 的个数:

$$x - p = p_1 p_2 p_3, \quad p \leqslant x,$$

$$x^{1/10} < p_1 \leqslant x^{1/3} < p_2 < p_3,$$

其中 p_1, p_2, p_3 都是素数.

命 $P_x(1, 2)$ 为适合下列条件的素数 p 的个数:

$$x - p = p_1 \text{ 或 } x - p = p_1 p_2,$$

其中 p_1, p_2, p_3 都是素数.

我们已经证明下面三个引理成立:

引理 1. 我们有

$$P_x(x, x^{1/10}) \geqslant \frac{9.976 x C_x}{\log^2 x},$$

此处

$$C_x = 2e^{-\gamma} \prod_{\substack{p|x \\ p>2}} \frac{p-1}{p-2} \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right),$$

385

386

發表“1+2”定理證明的曲折

- 《中國科學》找了王元為審稿人

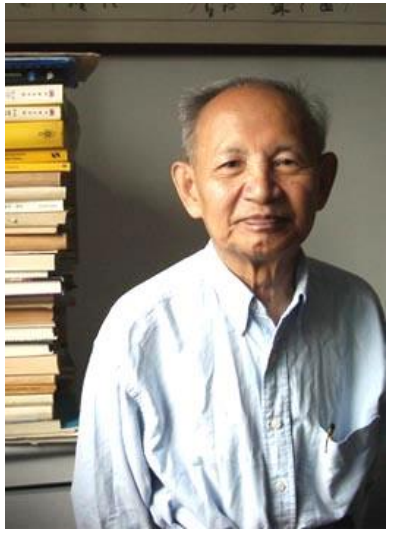
  王元憶述：「那時搞純理論研究被看成搞封建主義、資本主義……」

  「如果支持‘1+2’發表，輕則受到批判，戴上‘復辟封資修’、‘反攻倒算’等的帽子，重則後果難測」

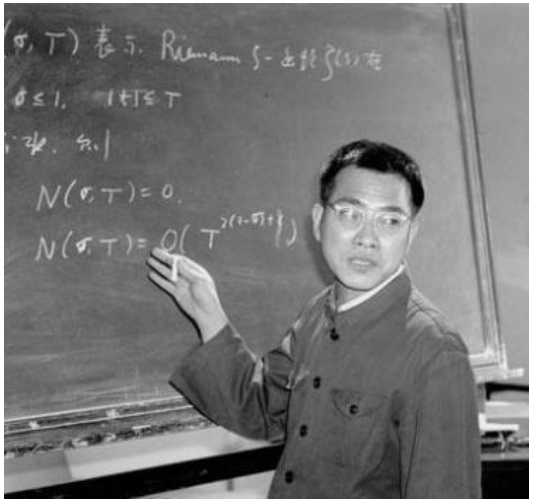
  「不支持呢，讓這樣為中華民族爭光的數學成果埋沒掉，良心上過不去」

  「經過反復思考，我決定支持‘1+2’盡快發表」

- 1973年，陳景潤“1+2”的詳細証明終於發表在《中國科學》上



王元 (1931-)



陳景潤 (1933-1996)

孿生質數：隔兩分鐘的巴士

- 質數分佈定理：平均 $p_{next} - p \approx \ln p$

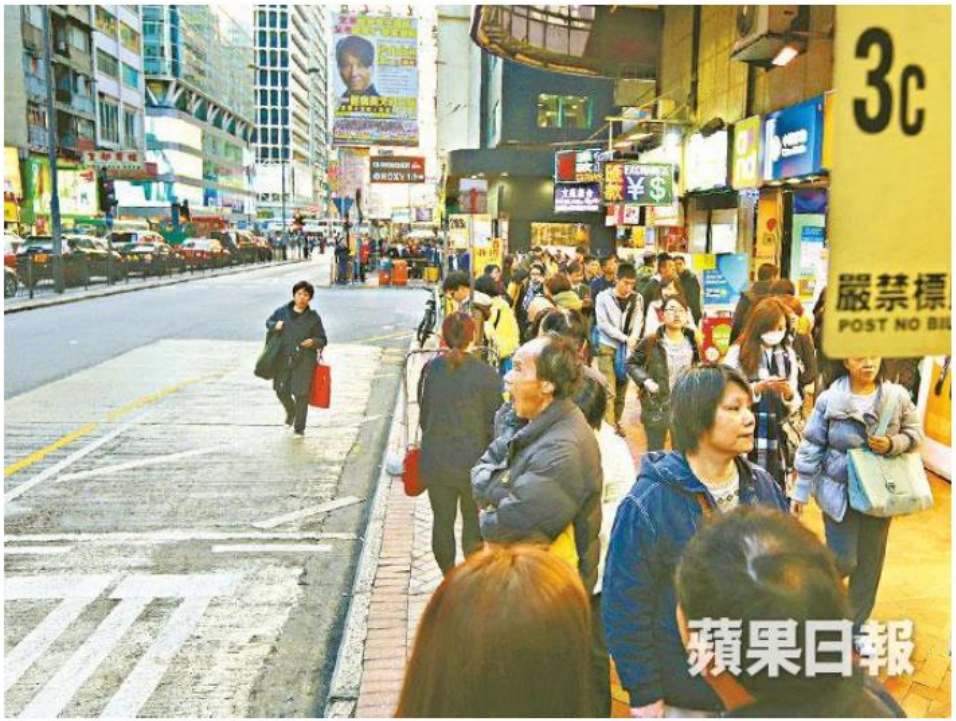
- 孿生質數猜想：
  有無限對 p, p_{next}
  滿足 $p_{next} - p = 2$.

- 20 世紀，數學家找到無限對 p, p_{next} 有以下情況：
  $p_{next} - p$ 少於平均值 $\ln p$

2014年01月24日 「一係冇車　一係嚟三班車」運署縱容巴士脫班

「一係冇車　一係嚟三班車」
運署縱容巴士脫班

97,502



■在非繁忙時段，旺角彌敦道巴士站等車的乘客仍大排長龍，難見巴士埋站。 易仰民 攝

孿生質數猜想:廿一世紀初的突破

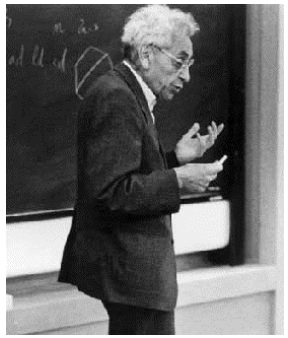
- 20世紀的成果:有無限對 p, p_{next} 滿足

  1940 年，Erdös :

  $$p_{next} - p \leq (1-\delta)\ln p \qquad (0 < \delta < 1)$$

  2000年前最好的結果:

  $$p_{next} - p \leq 0.25 \ln p$$



Erdös (1913-1996)

- 2003年， Goldston & Yildirim 公佈突破，但其後發現錯誤

Goldston (1954-)

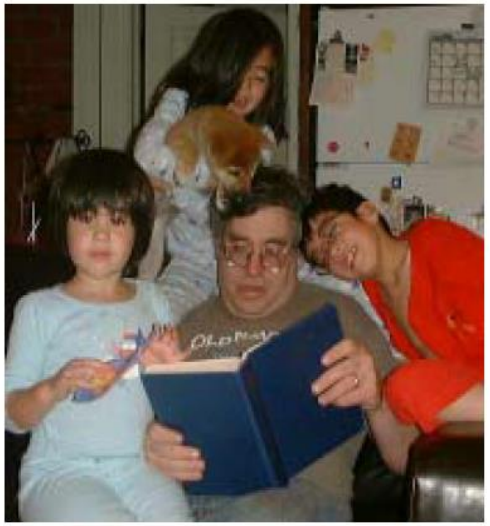
Yildirim (1961-)

Goldston 的突破、失敗、成功

Spring 2004

My 30 Minutes of Fame

By Dan Goldston



I've only had 3 or 4 really good mathematical ideas in the last twenty years, so when the latest one occurred after more than a decade I felt both elated and lucky. The idea was both simple and obvious, and was entirely convincing. What I didn't know then that I know now is that the idea was wrong - mathematically false as formulated, confused in its intent, and ultimately futile even when repaired. But before I knew these things I had received the small-time fame that is accorded people who achieve something in a respectable field of little interest to the general public, and the even smaller-time fame of mistaken fame. 15 minutes of fame and 15 minutes of negative fame. But fame unlike merit is a non-negative additive functions, hence the title of this article.

- 2005年， Goldston-Pintz-Yildirim 三人合力完成突破

Pintz (1950-)

孿生質數猜想:2005年的成果與展望

- 質數分佈定理: 平均 $p_{next} - p \approx \ln p$

- **有無限對 p, p_{next} 滿足**

$p_{next} - p \le (1-\delta)(\ln p)^1$ (Erdös, 1940)

$p_{next} - p \le 0.25(\ln p)^1$ (2000 前)

$p_{next} - p \le (\ln p)^{0.501}$ (Goldston-Pintz-Yildirim, 2005)

$\vdots$ $\vdots$

$p_{next} - p \le \text{constant}$ **中期目標？**

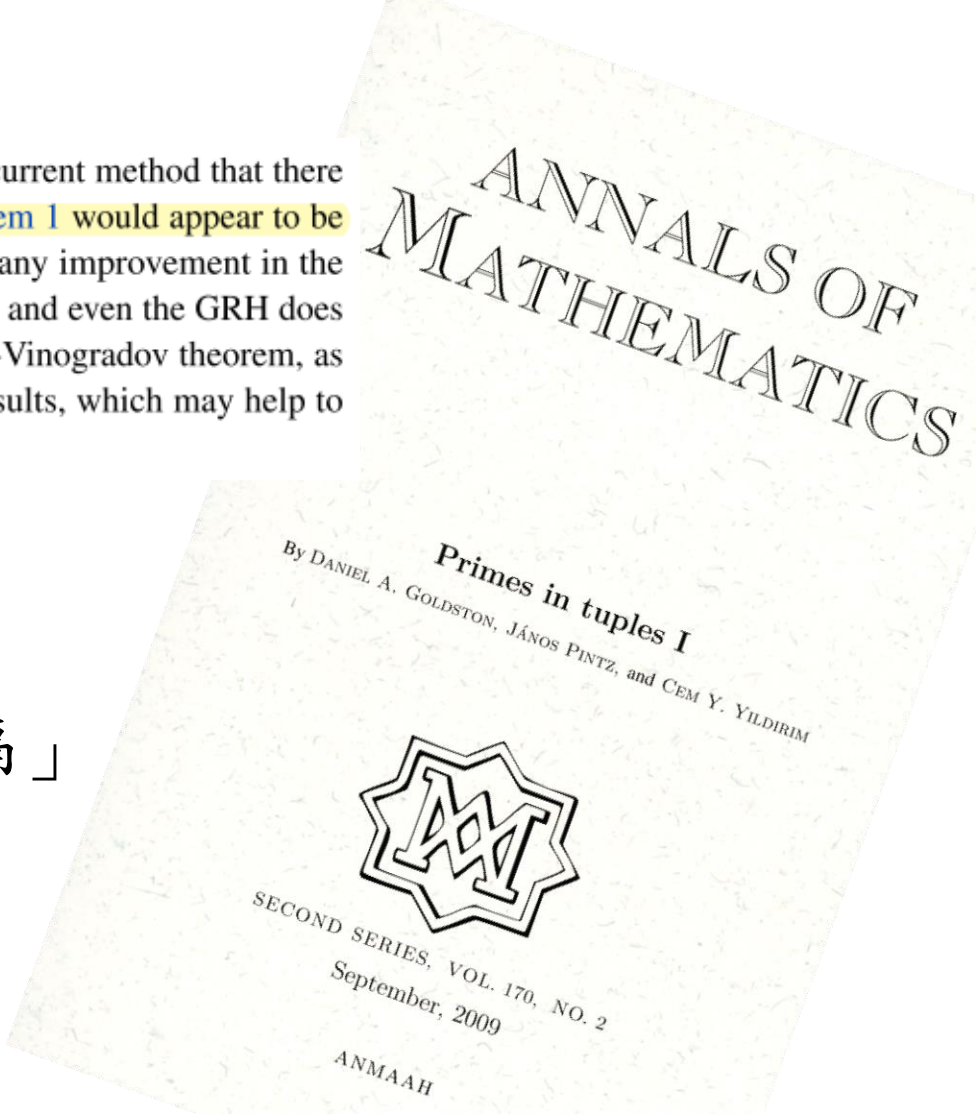
$\vdots$ $\vdots$

$p_{next} - p = 2$ (Twin Prime Conjecture)

Goldston-Pintz-Yildirim 說是一線之差

在2005年的文章中，Goldston-Pintz-Yildirim 寫道:

Question 1. Can it be proved unconditionally by the current method that there are, infinitely often, bounded gaps between primes? Theorem 1 would appear to be within a hair's breadth of obtaining this result. However, any improvement in the level of distribution ϑ beyond $1/2$ probably lies very deep, and even the GRH does not help. Still, there are stronger versions of the Bombieri-Vinogradov theorem, as found in [3], and the circle of ideas used to prove these results, which may help to obtain this result.



「從 $p_{next} - p \leq (\ln p)^{0.501}$

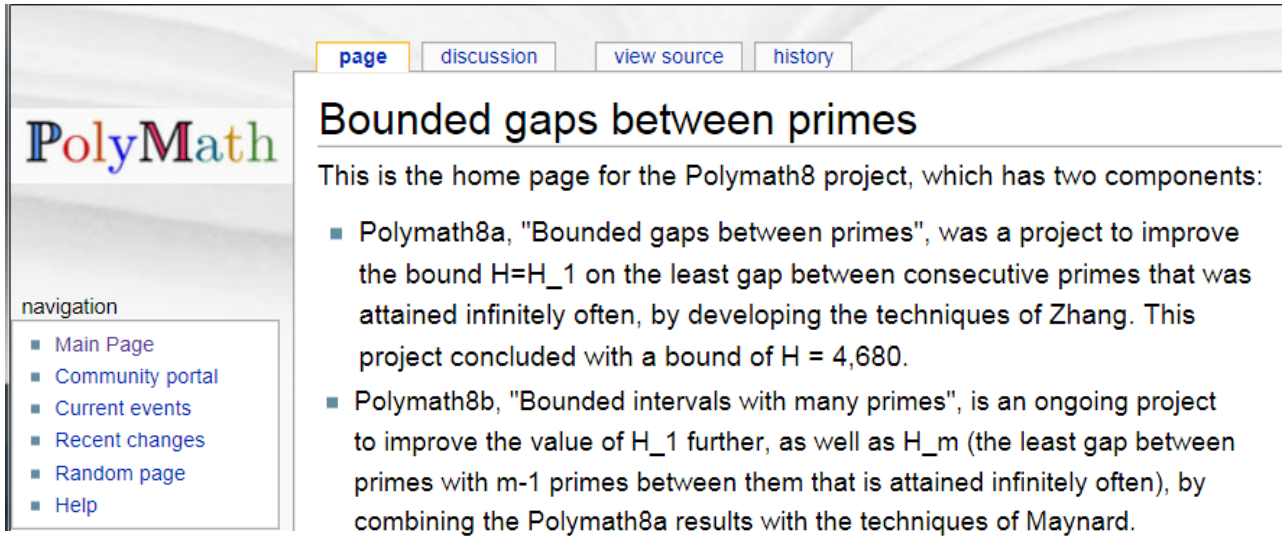
到 $p_{next} - p \leq \text{constant}$

可能只是一根頭髮絲之隔」

孿生質數猜想：2013年的突破

有無限對 p, p_{next}

2005	$p_{next} - p \leq (\ln p)^{0.501}$	Goldston-Pintz-Yildirim
May, 13	$p_{next} - p \leq 70,000,000$	Y. Zhang (張益唐)
Aug, 13	$p_{next} - p \leq 4,680$	Polymath8a (Tao et al.)



Maynard
(博士後研究員)

Dec, 13	$p_{next} - p \leq 270$		Polymath8b (Maynard et al.)
??	$p_{next} - p = 2$	Twin Prime Conjecture	??

張益唐的故事:半生磨劍，一舉揚名天下知

Y. Zhang (1955 -)

- 1978年，進入北京大學攻讀數學
- 1982年，修讀碩士，師從潘承彪
- 1985年，入讀 Purdue University (普渡大學)，導師為莫宗堅
- 1991年，取得 Purdue University 數學博士學位
- 1999年，擔任 University of New Hampshire (新罕布什爾大學) 的講師

REFERENCES:

1. AMS Blogs
2. AMS Notices (May 2003)
3. Annals of Mathematics
4. CASE PRESS, 國立台灣大學
5. Discover Magazine
6. Quanta Magazine
7. The Math Department Newsletter, San Jose State University
8. 中国科学
9. 科学记录
10. 數學女孩
    数学ガール漫画(結城浩/茅崎ミュキ)
11. 深夜小狗神秘習題
12. 遇見哥德巴赫猜想
13. 博士熱愛的算式
14. 數學傳播
15. 蘋果日報（2014年01月24日）
16. 科学时报（2009年2月3日）

Websites:

1. EFF (https://www.eff.org/)
2. Front for the arXiv (http://front.math.ucdavis.edu/math.NT)
3. GIMPS (http://www.mersenne.org/)
4. Google Images
5. Hausdorff center for mathematics (http://www.math.uni-bonn.de/~saxena/)
6. Microsoft Research (http://research.microsoft.com/en-us/people/neeraka)
7. PolyMath (http://michaelnielsen.org/polymath1/)
8. Wikipedia
9. Wikiquote
10. 久久漫画 (http: //99manga.com/)
11. 科学网 (http: //news.sciencenet.cn/htmlnews//2009/2/215836.html)

Youtube:

1. 台大科學教育發展中心
2. 美国之音中文网
3. iCNTV 人物官方频道

Thank you

THE END