Perspective on Quantum Computers-I

وحید کریمی پور
دانشگاه صنعتی شریف

The Physics of Quantum Information

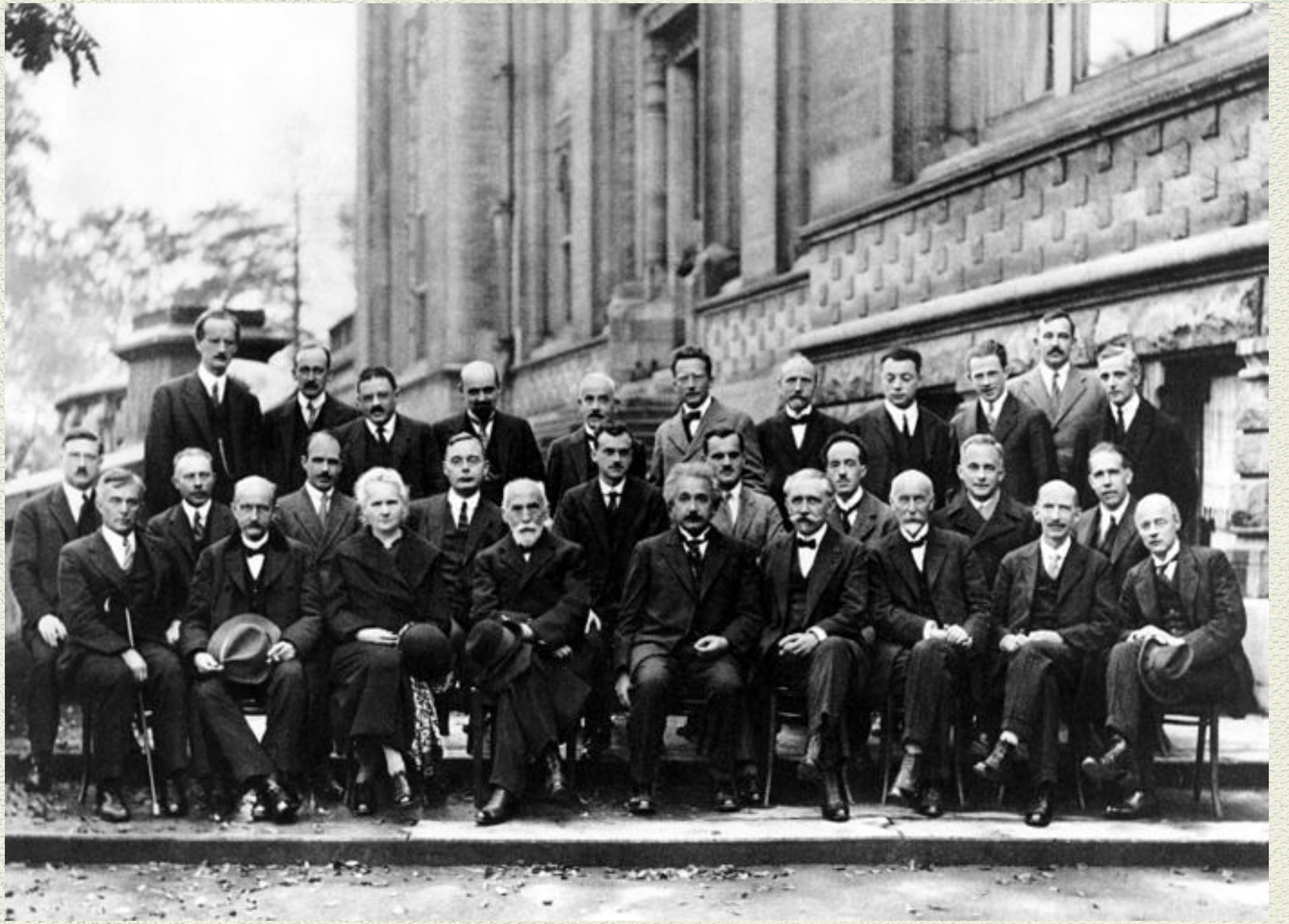
John Preskill

Institute for Quantum Information and Matter, California Institute of Technology
AWS Center for Quantum Computing
Pasadena, California 91125, USA

Rapid ongoing progress in quantum information science makes this an apt time for a Solvay Conference focused on The Physics of Quantum Information. Here I review four intertwined themes encompassed by this topic: Quantum computer science, quantum hardware, quantum matter, and quantum gravity. Though the time scale for broad practical impact of quantum computation is still uncertain, in the near future we can expect noteworthy progress toward scalable fault-tolerant quantum computing, and discoveries enabled by programmable quantum simulators. In the longer term, controlling highly complex quantum matter will open the door to profound scientific advances and powerful new technologies.

Overview talk at the 28th Solvay Conference on Physics
"The Physics of Quantum Information"
Brussels, 19-21 May 2022

1- Introduction



Solvay Conference on the Physics of Quantum Information.

Solvay conferences on physics [edit]

No	Year	Title	Translation	Chair
1	1911	La théorie du rayonnement et les quanta	The theory of radiation and quanta	Hendrik Lorentz (Leiden)
2	1913	La structure de la matière	The structure of matter	
3	1921	Atomes et électrons	Atoms and electrons	
4	1924	Conductibilité électrique des métaux et problèmes connexes	Electric conductivity of metals and related problems	
5	1927	Electrons et photons	Electrons and photons	
6	1930	Le magnétisme	Magnetism	Paul Langevin (Paris)
7	1933	Structure et propriétés des noyaux atomiques	Structure & properties of the atomic nucleus	
8	1948	Les particules élémentaires	Elementary particles	Lawrence Bragg (Cambridge)
9	1951	L'état solide	The solid state	
10	1954	Les électrons dans les métaux	Electrons in metals	
11	1958	La structure et l'évolution de l'univers	The structure and evolution of the universe	
12	1961	La théorie quantique des champs	Quantum field theory	
13	1964	The Structure and Evolution of Galaxies		J. Robert Oppenheimer (Princeton)
14	1967	Fundamental Problems in Elementary Particle Physics		Christian Møller (Copenhagen)
15	1970	Symmetry Properties of Nuclei		Edoardo Amaldi (Rome)
16	1973	Astrophysics and Gravitation		
17	1978	Order and Fluctuations in Equilibrium and Nonequilibrium Statistical Mechanics		Léon Van Hove (CERN)
18	1982	Higher Energy Physics		
19	1987	Surface Science		F. W. de Wette (Austin)
20	1991	Quantum Optics		Paul Mandel (Brussels)
21	1998	Dynamical Systems and Irreversibility		Ioannis Antoniou[9] (Brussels)
22	2001	The Physics of Communication		
23	2005	The Quantum Structure of Space and Time		David Gross (Santa Barbara)
24	2008	Quantum Theory of Condensed Matter		Bertrand Halperin (Harvard)
25	2011	The Theory of the Quantum World		David Gross
26	2014	Astrophysics and Cosmology		Roger Blandford (Stanford)
27	2017	The Physics of Living Matter: Space, Time and Information in Biology		Boris Shraiman (Santa Barbara)
28	2022	The Physics of Quantum Information		David Gross (Santa Barbara) Peter Zoller (Innsbruck U.)

2- Algorithms and Computation

یک نمونه از آلگوریتم

اقلیدس: قرن چهارم قبل از میلاد
اسکندریه

پیدا کردن مقسوم علیه مشترک دو عدد

$$gcd\ (32,18)$$

$$32 = 18 \times 1 + 14$$

$$18 = 14 \times 1 + 4$$

$$14 = 4 \times 3 + 2$$

$$4 = \boxed{2} \times 2 + 0$$

$gcd\ (40,16)$

$$40 = 16 \times 2 + 8$$

$$16 = \boxed{8} \times 2 + 0$$

$gcd\ (51,21)$

$$51 = 21 \times 2 + 9$$

$$21 = 9 \times 2 + 3$$

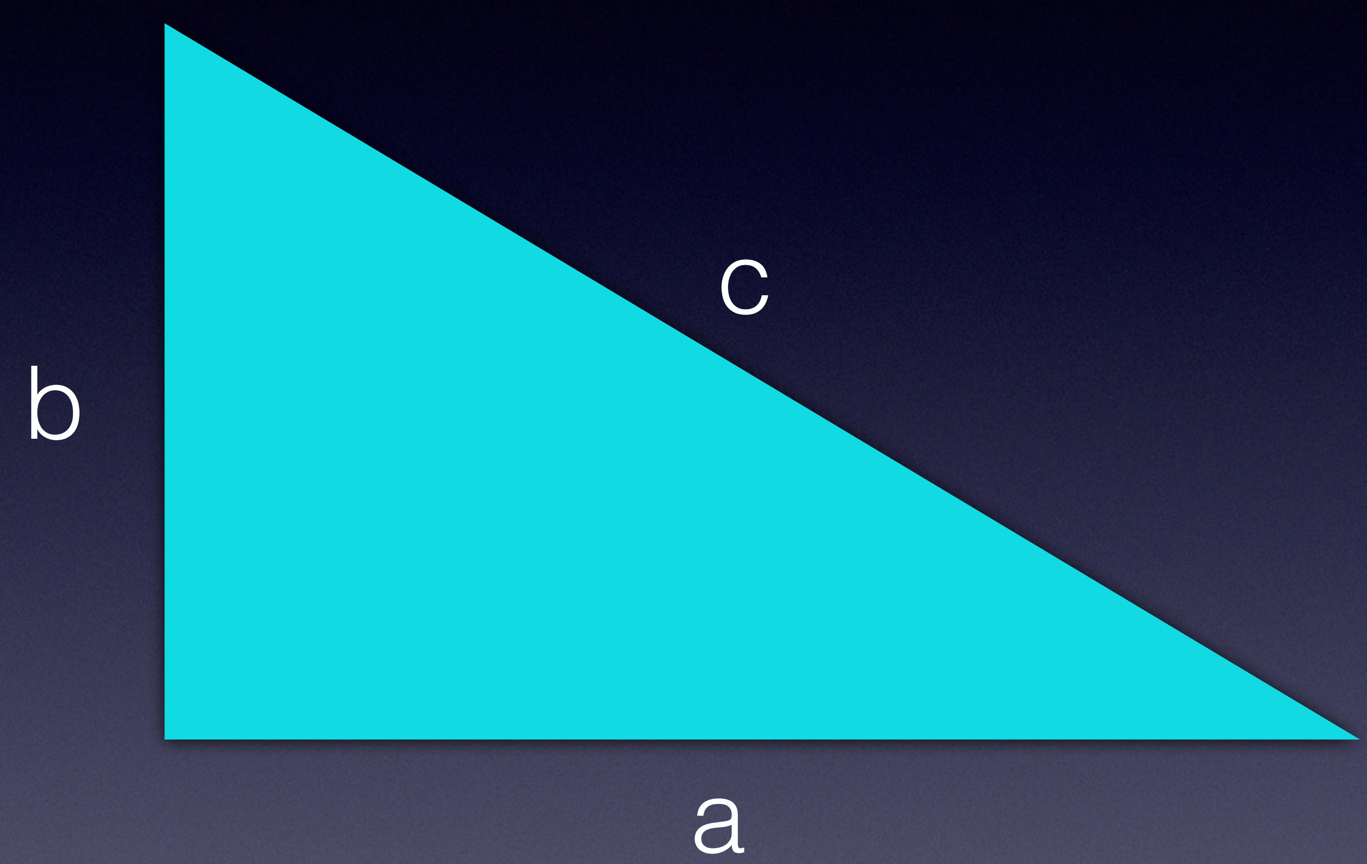
$$9 = \boxed{3} \times 3 + 0$$

درس اول:

کامپیوترها می توانند آلگوریتم ها را با سرعت باورنکردنی اجرا کنند.

اگر حل مسئله ای یک آلگوریتم داشته باشد، کامپیوتر به سرعت می تواند آن را حل کند.

سوال: آیا کامپیوتر می تواند قضیه ها را هم ثابت کند؟



اعداد فیثاغورثی

$$3^2 + 4^2 = 5^2$$

$$a^2 + b^2 = c^2$$

$$5^2 + 12^2 = 13^2$$

قضیه فرما:

$$a^n + b^n = c^n$$

Pierre de Fermat

3. 2. poris. Esto prius productum 32. posterius 272. Ponatur summa numerorum 1 N. Igitur $\frac{272}{1N}$ est summa quadratorum, & quia ex summa numerorum in interuallum eorundem $\frac{1}{o}$ fit interuallum quadratorum, quo rursus ducto in numerorum interuallum fit 32. erit $\frac{32}{1N}$ quadratus interualli numerorum, 7. 2. poris. qui si auferatur à duplo summæ quadratorum, nimirum à $\frac{544}{1N}$ residuum $\frac{512}{1N}$ æquatur quadrato summæ numerorum 1 Q. & omnia ducendo in 1 N. fiunt 512 æquales 1 C. & fit 1 N 8. summa numerorum, & 34. summa quadratorum, & 2. interuallum eorundem. Vnde facilè reperiuntur numeri 3. & 5. Hinc fit Canon.

Aufer prius productum à duplo posterioris, residuum est cubus summæ numerorum, per quam si diuidas prius productum, fit quadratus interualli numerorum.

QVAESTIO VIGESIMA QVARTA.

Inuenire duos numeros vt productum ex summa numerorum in interuallum quadratorum, & productum ex summa quadratorum in interuallum numerorum, datos conficiant numeros. Oportet autem duplum posterioris producti multatum priore producto, relinquere cubum, ita vt per eius latus diuidendo prius productum, oriatur quadratus.

Esto prius productum 128. posterius 68. Ponatur interuallum numerorum 1 N. ergo summa quadratorum erit $\frac{68}{1N}$ & ob causam in precedente allatam $\frac{128}{1N}$ erit quadratus summæ numerorum. Itaque 7. 2. poris. si à duplo summæ quadratorum quod est $\frac{136}{1N}$ auferatur quadratus summæ numerorum nimirum $\frac{128}{1N}$ residuum $\frac{8}{1N}$ est quadratus interualli numerorum. Quare $\frac{8}{1N}$ æquatur 1 Q. & omnia in 1 N. fiunt 8. æquales 1 C. est ergo 1 N 2. interuallum numerorum, & summa quadratorum 34. & quadratus summæ numerorum 64. vnde licet variis modis quæstionem soluere, & inuenire quæsitos numeros 3. & 5. Hinc fit Canon.

Aufer prius productum à duplo posterioris, residuum est cubus interualli numerorum, itaque per eius latus diuidendo prius productum, oritur quadratus summæ numerorum.

QVÆSTIO XXXIV.

ΕΥΡΕΙΝ δύο ἀριθμοὺς πρὸς ἀλλήλους λόγον ἔχοντας δεδομένον ὅπως καὶ ἡ σύνθεσις τῶν ἀπ' αὐτῶν τετραγώνων πρὸς συναμφότερον λόγον ἔχῃ δεδομένον. ἐπιτετάχθω δὴ τὸν μείζονα τοῦ ἐλάσσονος εἶναι τριπλασίονα, τὴν δὲ σύνθεσιν τῶν ἀπ' αὐτῶν τετραγώνων συναμφοτέρου εἶναι πενταπλασίονα. τετάχθω ὁ ἐλάσσων ςου ἑνός. ὁ ἄρα μείζων ἔσται ςς γ. λοιπόν ἐστι τὸ σύνθεμα, τῶν ἀπ' αὐτῶν τετραγώνων συναμφοτέρου εἶναι πενταπλασίονα. ἀλλὰ τὸ σύνθεμα, τῶν ἀπ' αὐτῶν τετραγώνων ποιεῖ δυνάμεις ι. τὸ δὲ αὐτῶν σύνθεμα ςς δ. ὥστε δυνάμεις ι πενταπλασίονές εἰσιν ςς δ. ἀριθμοὶ ἄρα κ ἴσοι δυνάμεσι ι. καὶ γίνεται ὁ ἀριθμὸς μο β. ἔσται ὁ μὲν ἐλάσσων μο β ὁ δὲ μείζων μο ς. καὶ ποιοῦσι τὰ τῆς προτάσεως.

Inuenire duos numeros, datam inter se rationem habentes, vt & summa quadratorum ab ipsis, ad summam ipsorum datam habeat rationem. Imperatum sit maiorem minoris esse triplum; summam autem quadratorum, summæ numerorum esse quincuplam. Ponatur minor 1 N. Maior igitur erit 3 N. Superest vt summa quadratorum ab ipsis, summæ vtriusque sit quincupla. Cæterùm summa quadratorum ab ipsis ortorum fit 10 Q. summa verò ipsorum est 4 N. vnde constat 10 Q. quincuplos esse ad 4 N. Quamobrem 20 N. æquantur 10 Q. & fit 1 N. 2. Est igitur minor 2. maior 6. & quæstioni satisfaciunt.

IN QVÆSTIONEM XXXIV.

CIRCA hanc quæstionem & octo sequentes nulla est difficultas, nec ampliori indigent explicatione. Canones etiam pro qualibet formari nullo negotio possunt, quod tibi relinquo pe ragendum.

QVÆSTIO XXXV.

ΕΥΡΕΙΝ δύο ἀριθμοὺς ἐν λόγῳ τῷ δοθέντι ὅπως ἡ σύνθεσις τῶν ἀπ' αὐτῶν

Invenire duos numeros in data ratione, vt summa quadratorum ab

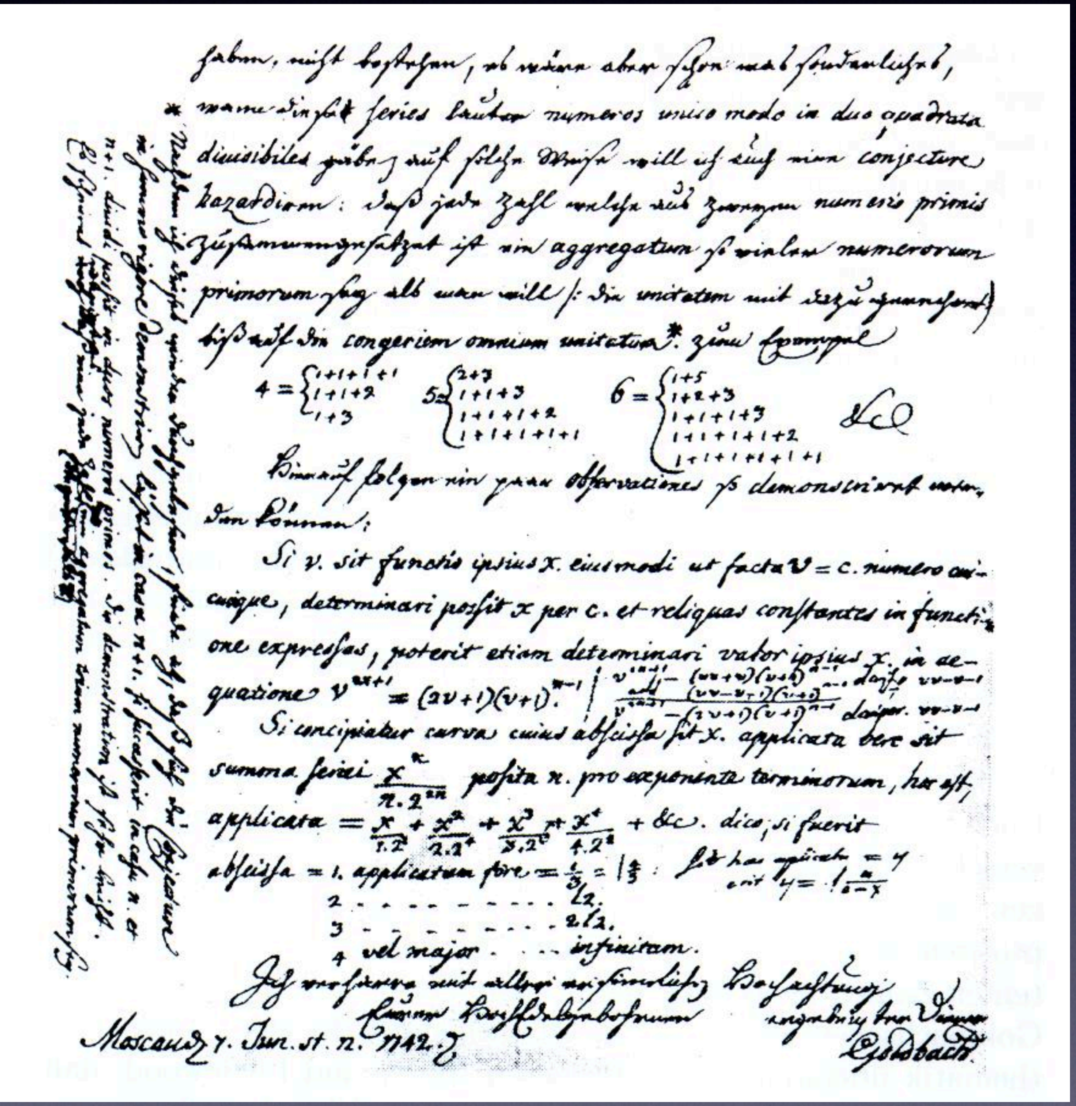
حدس گلدباخ:

هر عدد زوج را می توان به صورت مجموع دو عدد اول نوشت.

کریستین گلدباخ

20=13+7 24=13+11 46=5+41

لئونارد اویلر



Si v. sit functio ipsius x. eiusmodi ut facta v = c. numero cuicunque, determinari possit x per c. et reliquas constantes in functione expressas, poterit etiam determinari valor ipsius x. in aequatione

Si concipiatur curva cuius abscissa sit x. applicata vero sit summa seriei $\frac{x^n}{n.2^{2n}}$ posita n. pro exponente terminorum, hoc est, applicata $= \frac{x}{1.2} + \frac{x^2}{2.2^4} + \frac{x^3}{3.2^6} + \frac{x^4}{4.2^8} + \&c.$ dico, si fuerit abscissa = 1. applicatam fore = ...

2 . . . . l2.

3 . . . . 2l2.

4 vel major . . . . infinitam.

Moscau d. 7. Jun. st. n. 1742.

Goldbach.

نامه گلدباخ به اویلر: ۷ ژوئن ۱۷۲۴

1938	100,000
2020	8,875,694,145,621,773,516,800,000,000,000

تا کنون حدس گلدباخ نه ثابت شده است
و نه مثال نقضی برای آن پیدا شده.

حدس اویلر:

معادله $x^4 + y^4 + z^4 = w^4$ هیچ جواب صحیحی ندارد.

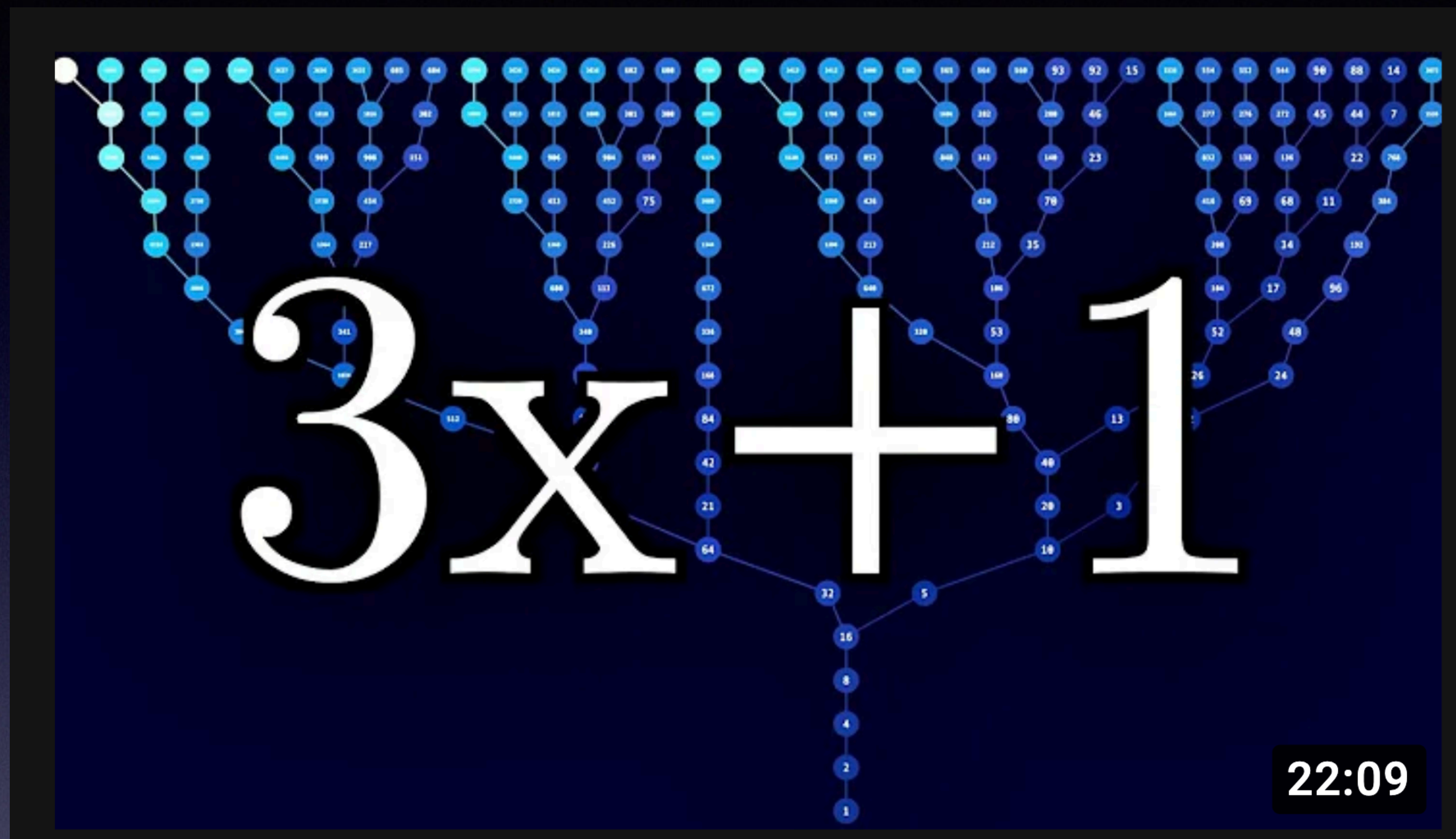
Leonard Euler (1707-1783)

ابطال حدس اویلر: $x^4 + y^4 + z^4 = w^4$

Naom Elkies (1988)

$$(2,682,440)^4 + (15,365,639)^4 + (18,796,760)^4 = (20,615,673)^4$$

Collatz Conjecture



x {
فرد $3x + 1$
زوج $\frac{x}{2}$

3 → 10 → 5 → 16 → 8 → 4 → 2 → 1

7 → 22 → 11 → 34 → 17 → 52 → 26 → 13

40 → 20 → 10 → 5 ………… → 1

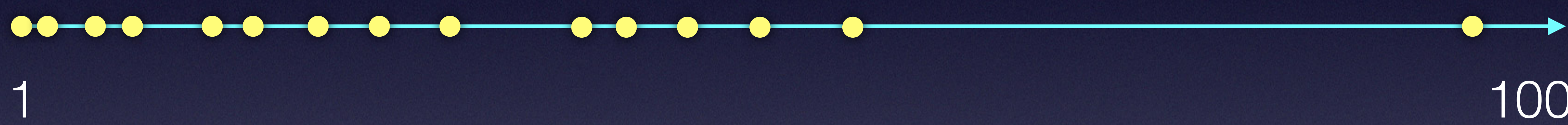
$$2^{68} \approx 3 \times 10^{20}$$

تا کنون حدس کولاتز نه ثابت شده است
و نه مثال نقضی برای آن پیدا شده.

توزیع اعداد اول

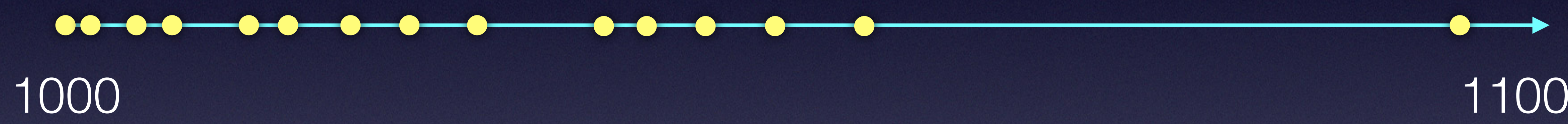
کارل فردریک گاووس

$$n(x) \sim \frac{1}{\ln(x)}$$

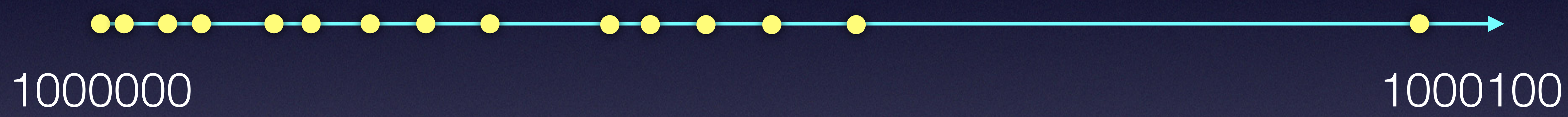


$$\frac{100}{ln(100)} \approx 21$$

در این فاصله ۱۴ تا عدد اول وجود دارد



در این فاصله ۷ تا عدد اول وجود دارد



$$N[x] \sim \int_2^x dx \frac{1}{\log(x)}$$

n	Number of Primes less than n	$\int_2^x \frac{dx}{\log x}$
1000	168	178
10000	1229	1246
50000	5133	5167
100000	9592	9630
500000	41538	41606
1000000	78498	78628
2000000	148933	149055
5000000	348513	348638
10000000	664579	664918
20000000	1270607	1270905
90000000	5216954	5217810
100000000	5761455	5762209
1000000000	50847534	50849235
10000000000	455052511	455055614

n	Number of Primes less than n		$\int_2^n \frac{dx}{\log x}$
1000	168	<	178
10000	1229		1246
50000	5133		5167
100000	9592		9630
500000	41538		41606
1000000	78498		78628
2000000	148933	<	149055
5000000	348513		348638
10000000	664579		664918
20000000	1270607		1270905
90000000	5216954		5217810
100000000	5761455		5762209
1000000000	50847534		50849235
10000000000	455052511	<	455055614

ابطال حدس گاووس

Stanley Skewes
1955

n= $10^{10^{10000000000000000000000000000000000}}$

ابطال حدس گاووس

$$10^{10^{10000000000000000000000000000000000000}}$$

$$10^{10000000000000000000000000000000000000}$$ تعداد ارقام این عدد؟

درس دوم: با تست کردن مثال ها، هر چقدر هم که آن مثال ها متعدد باشند
نمی توان قضیه ای را ثابت کرد.

سوال: آیا می توان قضایای ریاضی رابا کامپیوتر ثابت کرد؟

دیوید هیلبرت

تعاریف و اصول موضوعه →

صورت قضیه →

→ 1

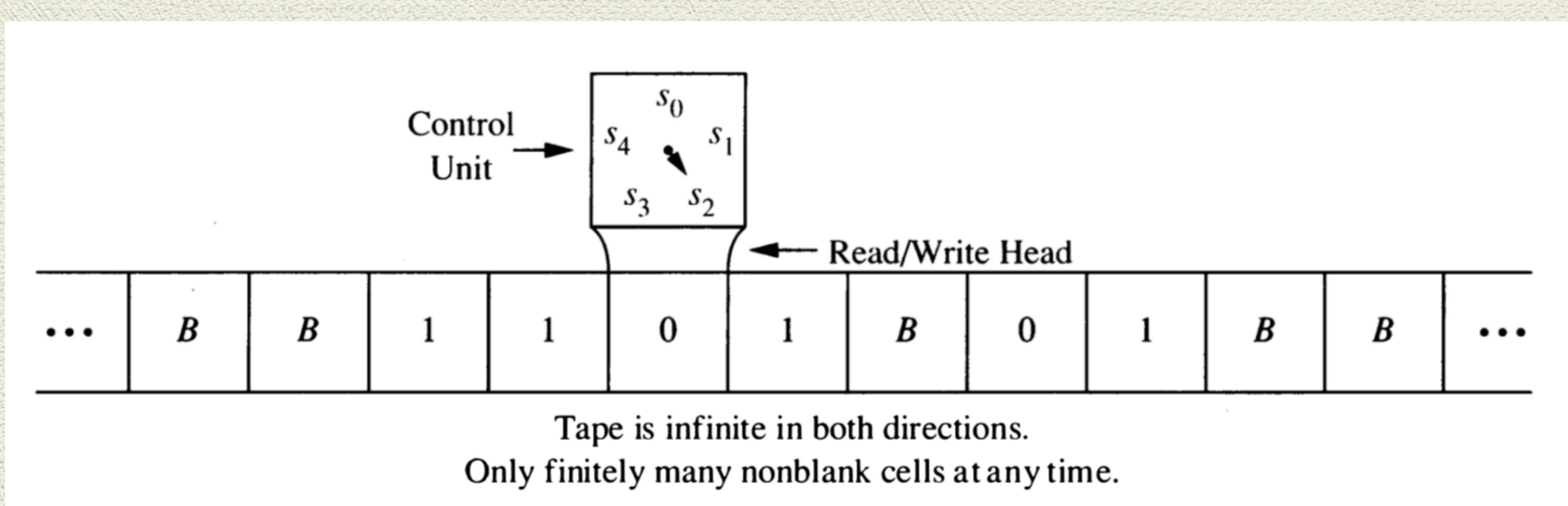
→ 0

پاسخ: خیر، نمی توان.

Alan Turing
(1912-54)

Modeling Computation

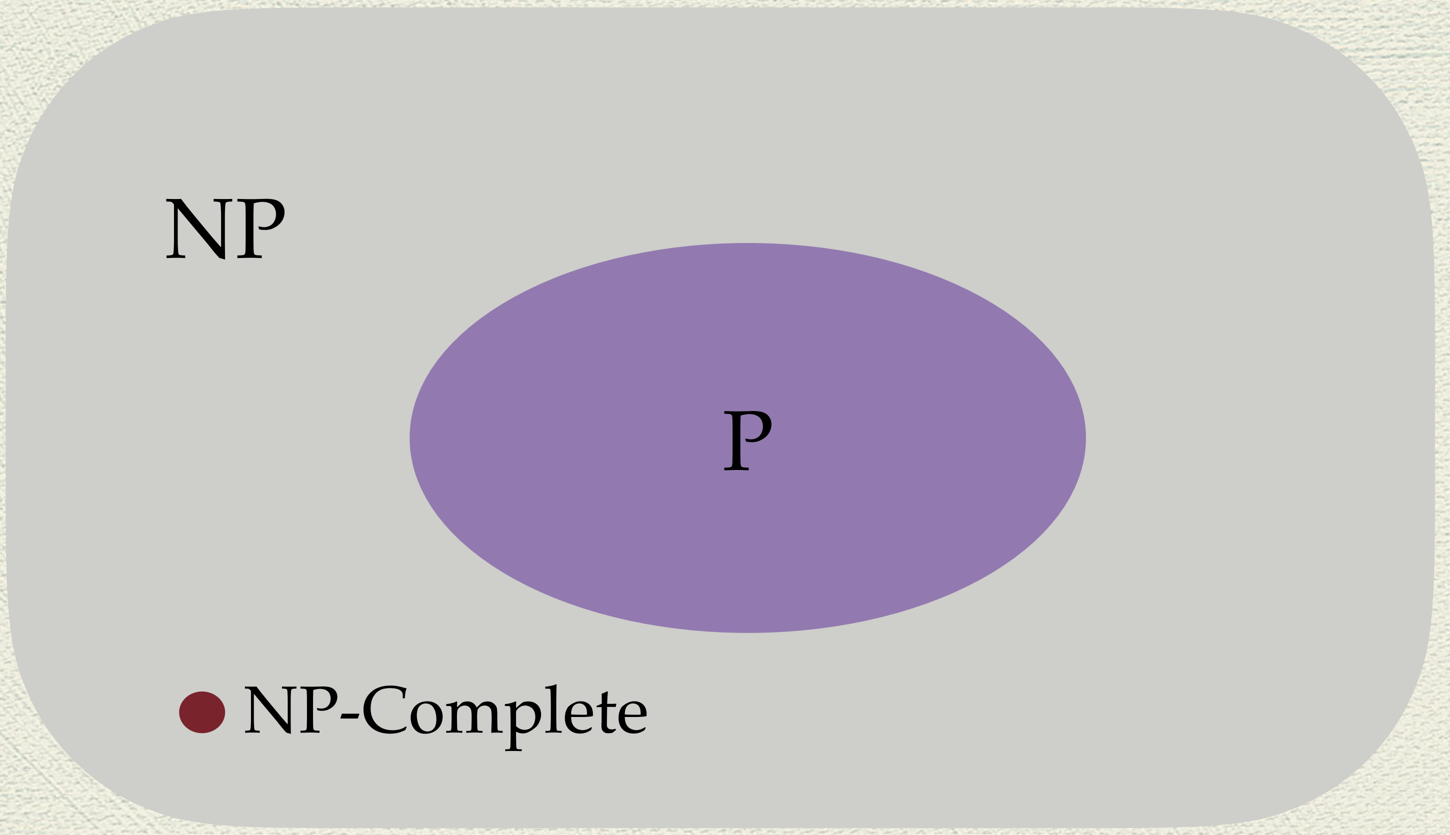
What kind of problems are in principle solvable in the physical world?



- Church-Turing Thesis (1930s)

Computational Complexity (1970's)

What kind of problems are "efficiently" solvable in the physical world?



A Survey of Quantum Complexity Theory

Umesh V. Vazirani

Quantum Computation	Last semester
Quantum Information	This semester
Quantum Error Correction	This semester