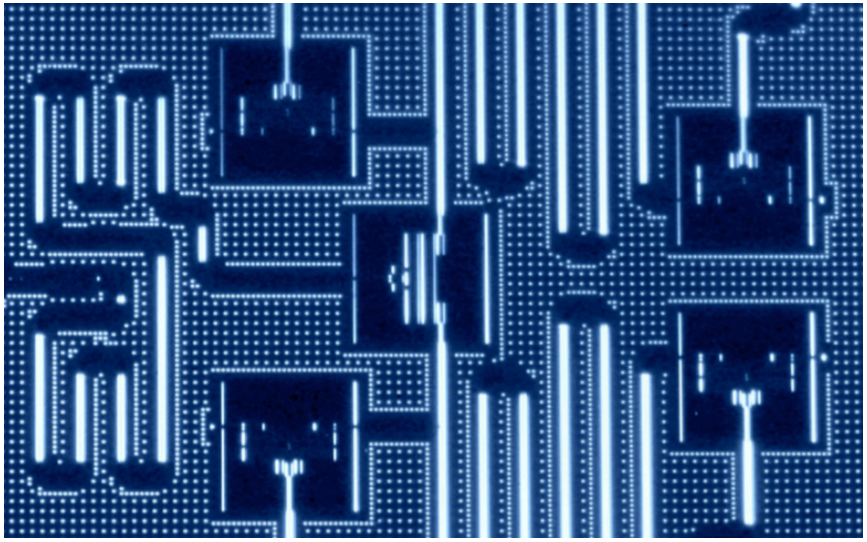
Prime Numbers
and
Quantum Computers



1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Germán Sierra
Instituto de Física Teórica CSIC-UAM, Madrid

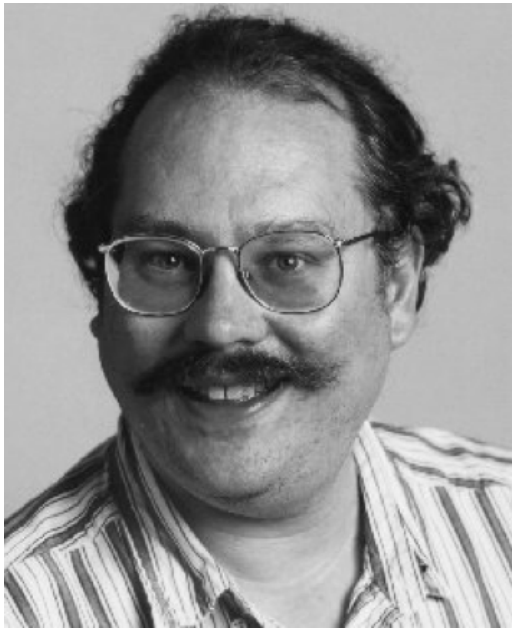
Workshop on Quantum Computing for High Energy Physics

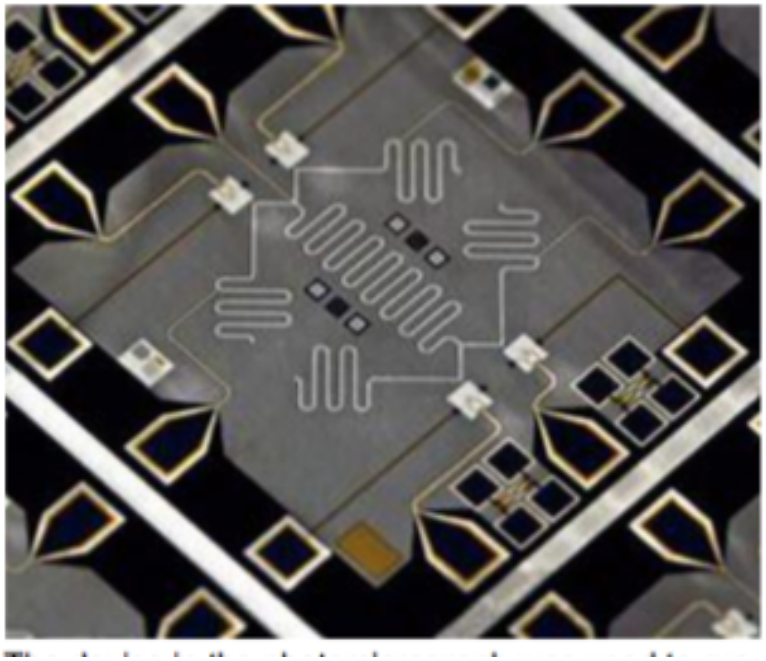
CERN, Geneva, 5-6 Nov 2018

Title:Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer

Authors:Peter W. Shor (AT&T Research)

arXiv:quant-ph/9508027





15 = 3 x 5

UCSB 2012

RSA-129 =

114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

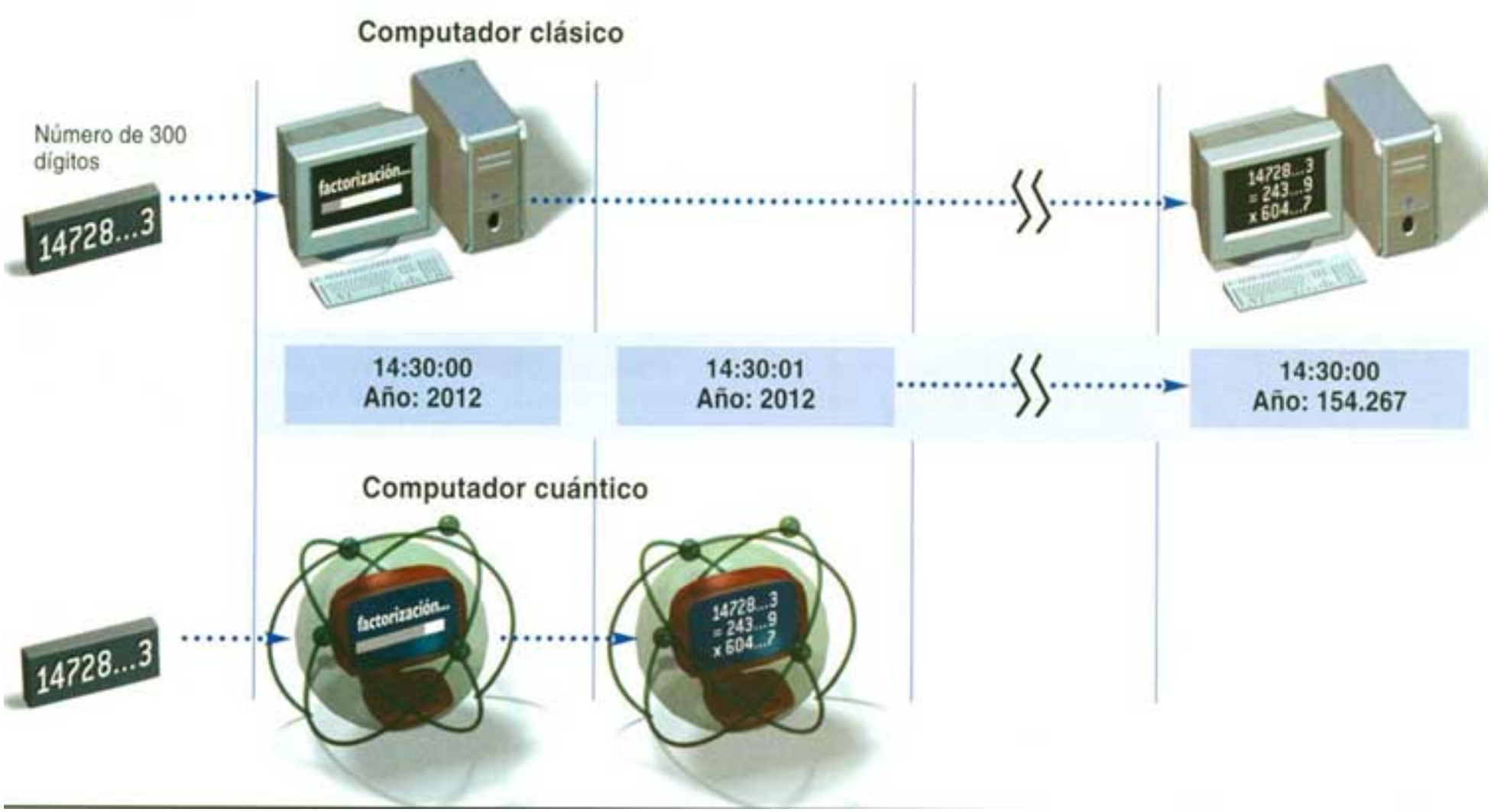
=

3490529510847650949147849619903898133417764638493387843990820577 ×

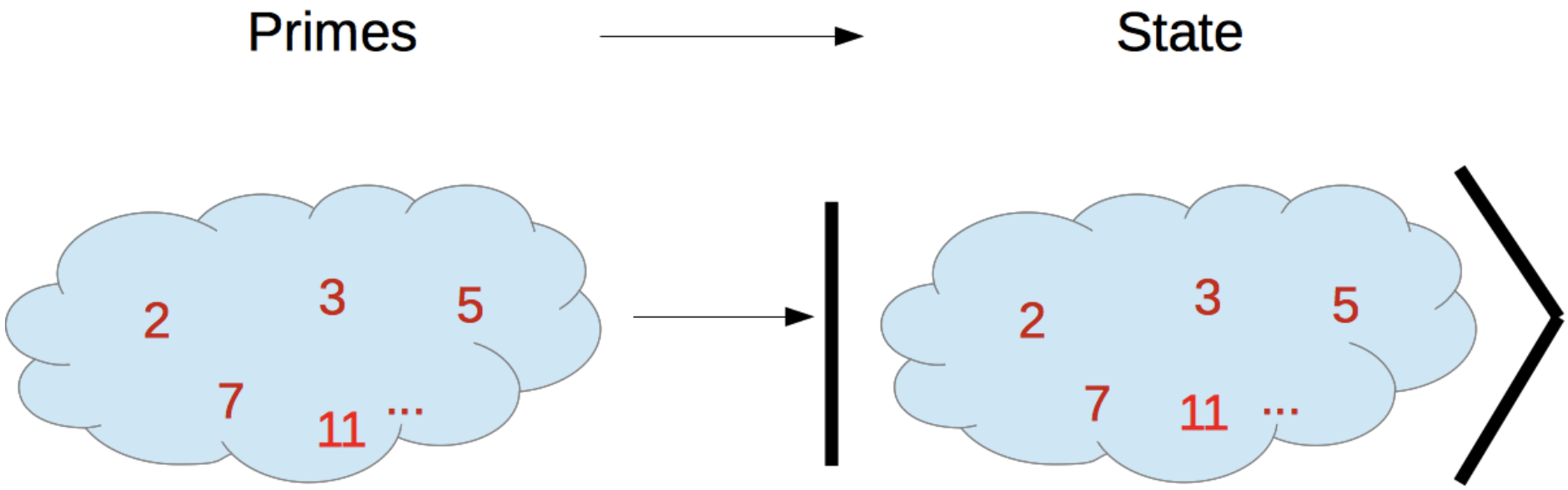
3276913299326670954996198819083446141317764296799294253979828853 3

Factorized in 1994 using 1.600 computers connected in internet

Quantum promise



Prime numbers go quantum



Quantum Computation and prime numbers
(JI Latorre, GS, 2013)

Classical computer

n bits $x = x_0 2^0 + x_1 2^1 + \ldots x_{n-1} 2^{n-1}, \quad x_i = 0,1, \quad x = 0,1,\ldots 2^n - 1$

Quantum computer

n qubits $|x\rangle = |x_{n-1},\ldots,x_0\rangle = |x_{n-1}\rangle \otimes \ldots \otimes |x_0\rangle$

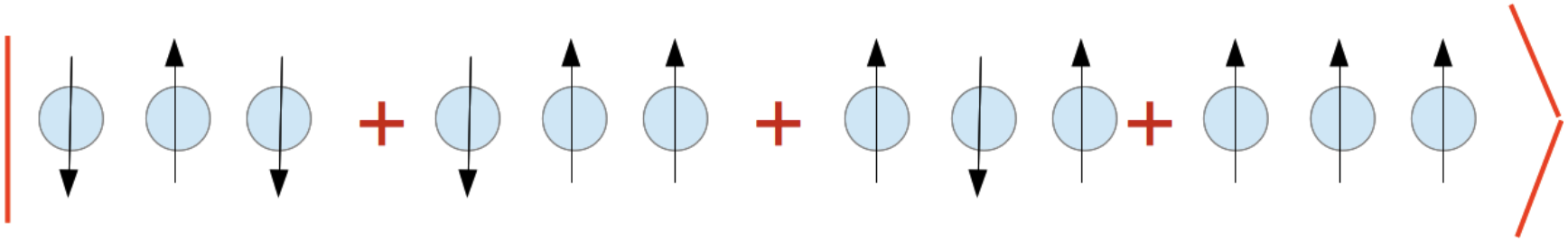
The Prime State

$$|P(n)\rangle = \frac{1}{\sqrt{\pi(2^n)}} \sum_{p<2^n \in Primes} |p\rangle$$

$\pi(2^n)$ is the prime counting function

Ex. n=3

$$|P(3)\rangle = \frac{1}{\sqrt{4}}\left(|2\rangle + |3\rangle + |5\rangle + |7\rangle\right)$$



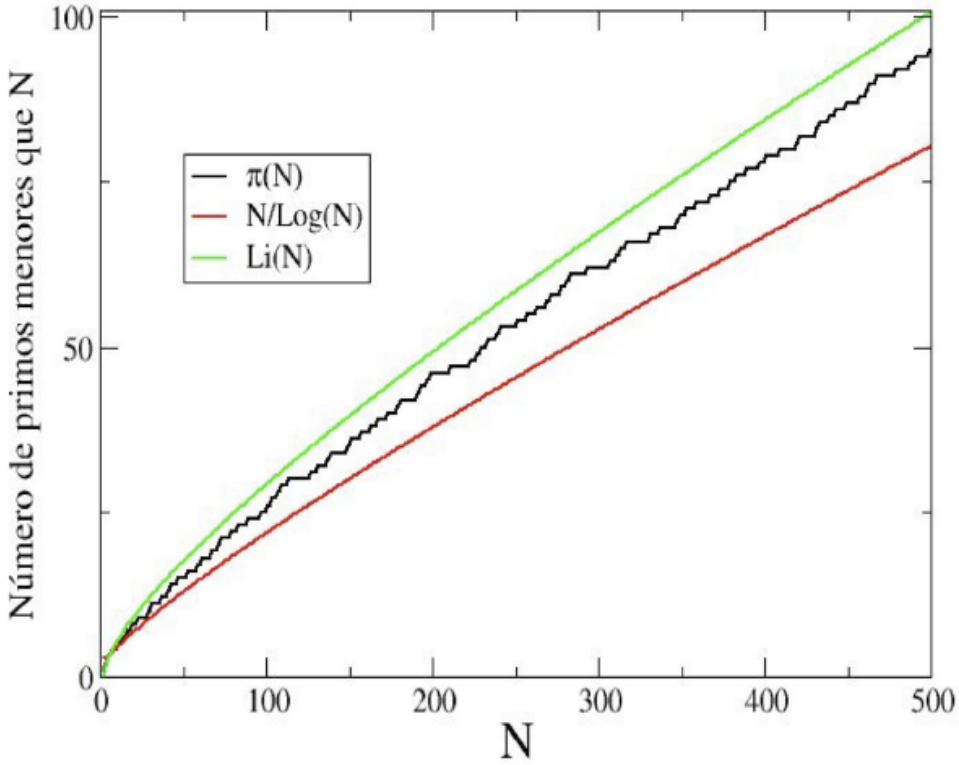
Prime counting function

$\pi(x)$: number of primes p less than or equal to x

$$\pi(100) = 25$$

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

Asymptotic behaviour: Gauss law



$$\pi(x) \approx Li(x) \approx \frac{x}{\ln x}$$

$$x \to \infty$$

Average behaviour or “mean field”

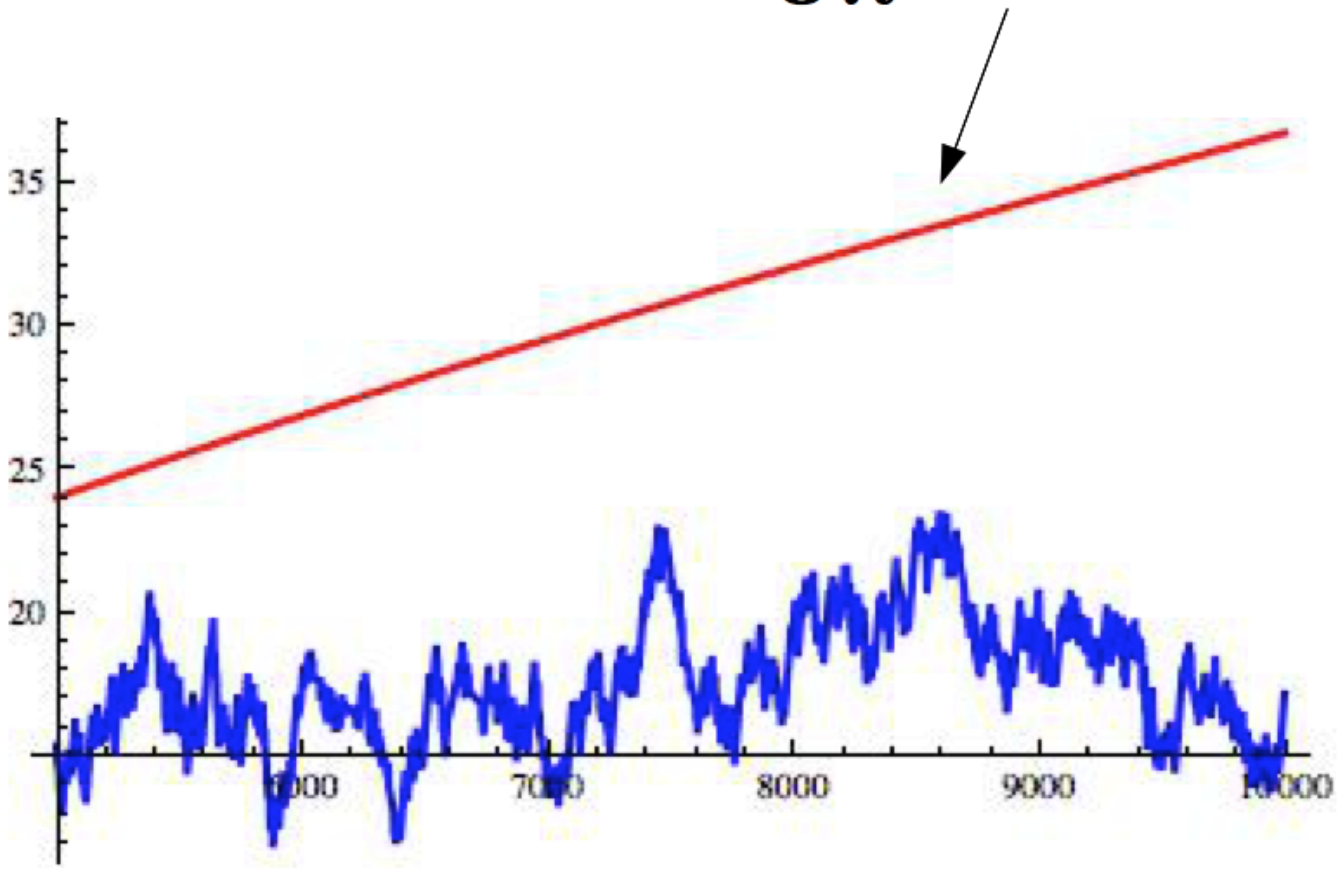
Prime Number Theorem (1896)

$$\lim_{x\to\infty}\frac{\pi(x)}{Li(x)}=1, \qquad Li(x)=\int_2^x\frac{dt}{\log t}\approx\frac{x}{\log x}+\frac{x}{(\log x)^2}+\dots$$

x	π(x)	π(x) − x / ln x	li(x) − π(x)
10	4	−0.3	2.2
10^2	25	3.3	5.1
10^3	168	23	10
10^4	1,229	143	17
10^5	9,592	906	38
10^6	78,498	6,116	130
10^7	664,579	44,158	339
10^8	5,761,455	332,774	754
10^9	50,847,534	2,592,592	1,701
10^{10}	455,052,511	20,758,029	3,104
10^{11}	4,118,054,813	169,923,159	11,588
10^{12}	37,607,912,018	1,416,705,193	38,263
10^{13}	346,065,536,839	11,992,858,452	108,971
10^{14}	3,204,941,750,802	102,838,308,636	314,890
10^{15}	29,844,570,422,669	891,604,962,452	1,052,619
10^{16}	279,238,341,033,925	7,804,289,844,393	3,214,632
10^{17}	2,623,557,157,654,233	68,883,734,693,281	7,956,589
10^{18}	24,739,954,287,740,860	612,483,070,893,536	21,949,555
10^{19}	234,057,667,276,344,607	5,481,624,169,369,960	99,877,775
10^{20}	2,220,819,602,560,918,840	49,347,193,044,659,701	222,744,644
10^{21}	21,127,269,486,018,731,928	446,579,871,578,168,707	597,394,254
10^{22}	201,467,286,689,315,906,290	4,060,704,006,019,620,994	1,932,355,208
10^{23}	1,925,320,391,606,803,968,923	37,083,513,766,578,631,309	7,250,186,216
10^{24}	18,435,599,767,349,200,867,866	339,996,354,713,708,049,069	17,146,907,278
10^{25}	176,846,309,399,143,769,411,680	3,128,516,637,843,038,351,228	55,160,980,939
10^{26}	1,699,246,750,872,437,141,327,603	28,883,358,936,853,188,823,261	155,891,678,121
10^{27}	16,352,460,426,841,680,446,427,399	267,479,615,610,131,274,163,365	508,666,658,006

The fluctuations of $\pi(x)$ around $Li(x)$ are expect to be bounded by

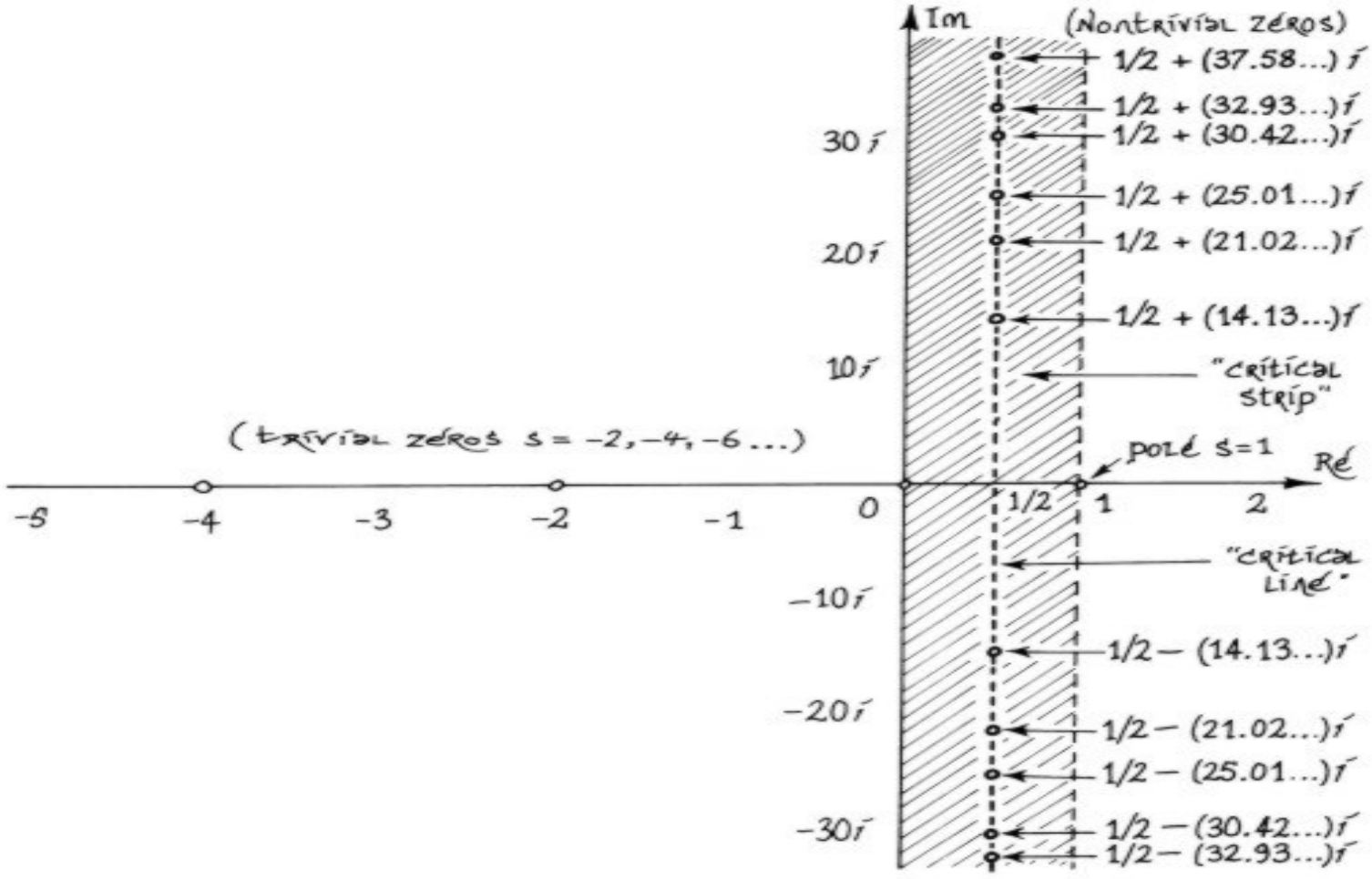
$$|Li(x)-\pi(x)|<\frac{1}{8\pi}\sqrt{x}\log x$$



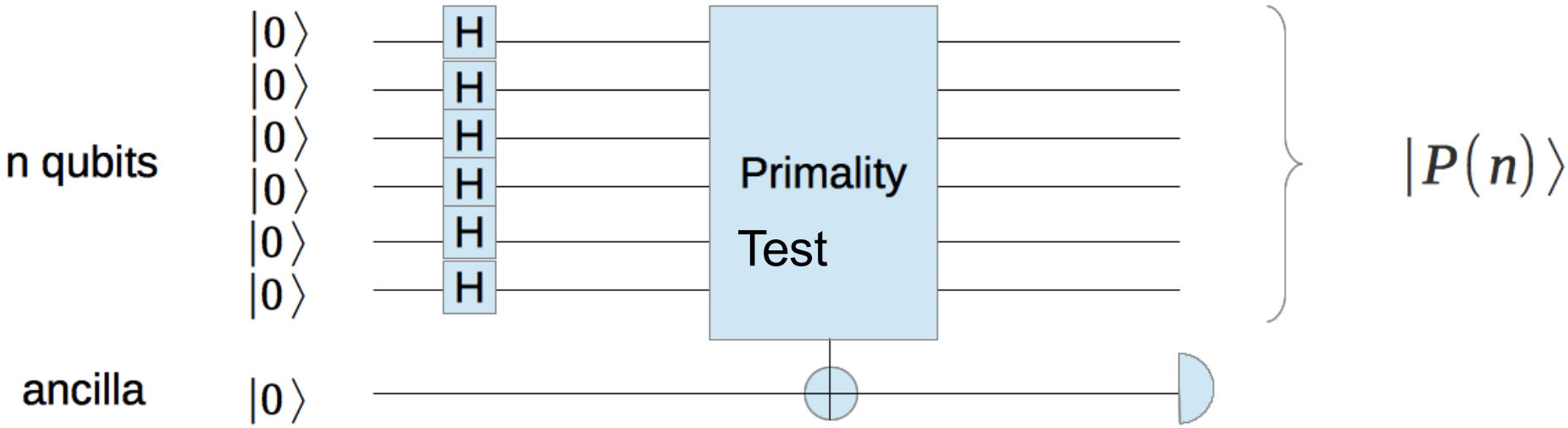
This statement is equivalent to the Riemann hypothesis (RH)

The Riemann Hypothesis

Non trivial zeros of the zeta function $\zeta(s)$ have real part equal to 1/2



First construction of the Prime state



$$U_{primality}\sum_x |x\rangle|0\rangle = |P(n)\rangle|0\rangle + \sum_{c\in composite} |c\rangle|1\rangle$$

$$Prob(|P(n)\rangle) = \frac{\pi(2^n)}{2^n} \approx \frac{1}{n\log 2}$$

Efficient construction

PNT

Grover construction of the Prime state

$$|\psi_0\rangle = \sum_{x<2^n} |x\rangle = \underbrace{\overbrace{\sum_{p\in primes} |p\rangle}^{M} + \sum_{c\in composites} |c\rangle}_{N}$$

ORACLE $\quad U_{oracle}|x\rangle = \mp|x\rangle,\ x: prime/composite$

CALLS TO ORACLE $\quad R(n) \le cte\sqrt{n}$

Problem: given x determine if it is prime or not

Miller-Rabin primality test:

Choose a in the range $1 < a < x$ (witness)

Run a test that involves a, x

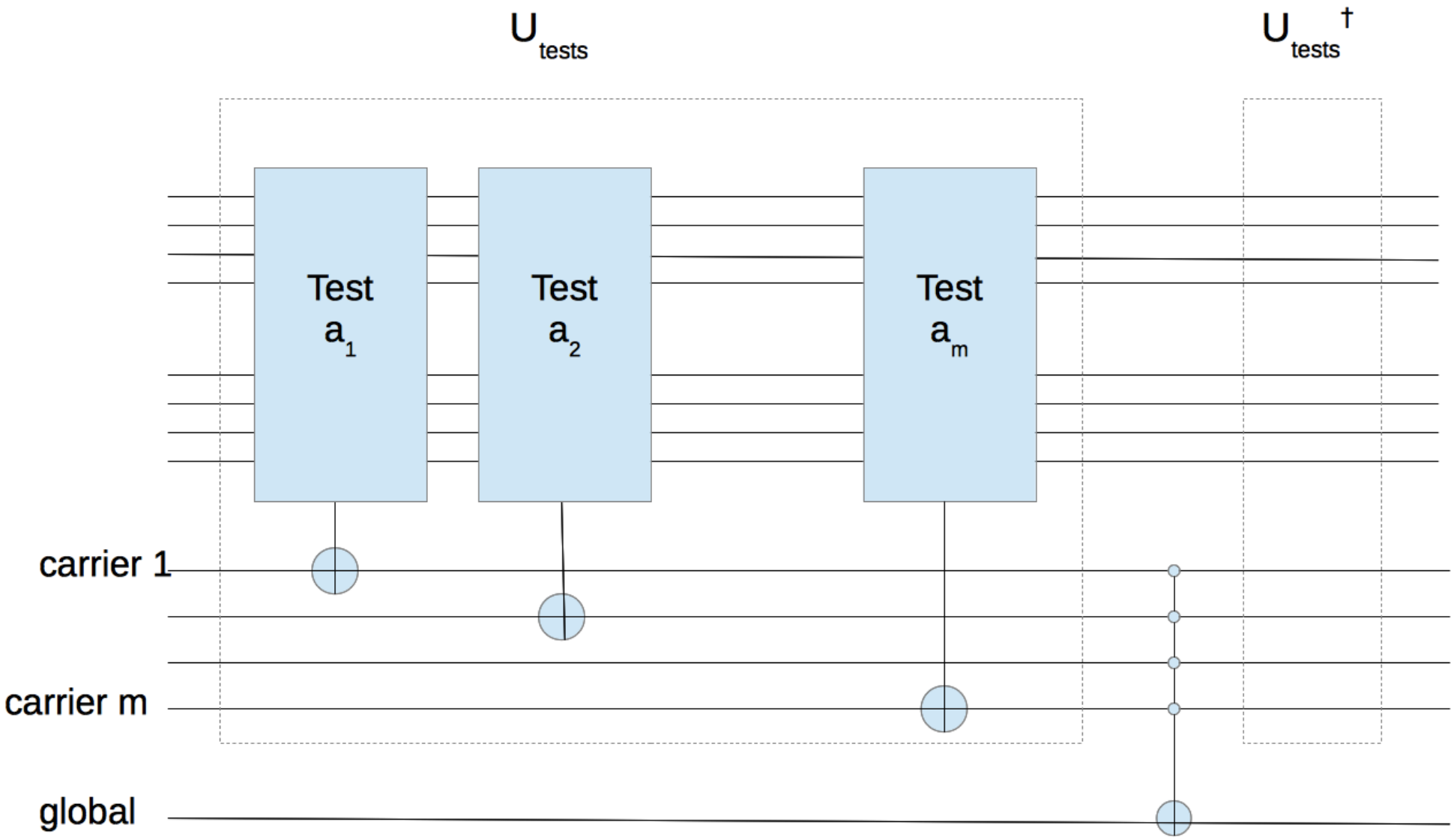
Test  then x is composite with certainty a: strong witness

Test  then
1) x is prime with high probability
2) x is composite a: strong lier

Solution: use several witnesses

For $x < 3 \times 10^{14}$, $a = 2,3,5,7,11,13,17$

With k witnesses the error is 2^{-2k}

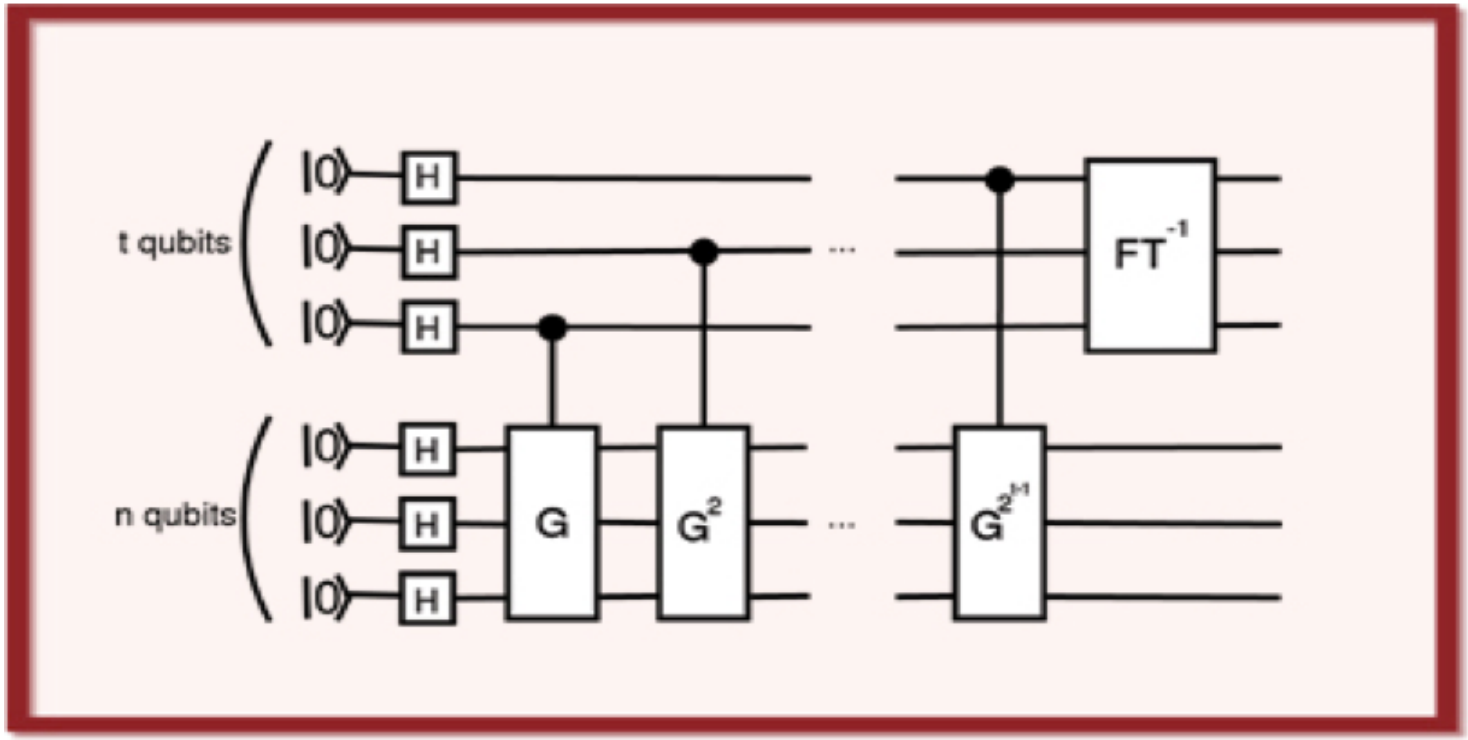


Structure of the quantum primality oracle

Quantum Counting of Prime numbers

quantum primality oracle + quantum counting algorithm

Brassard, Hoyer, Tapp (1998)



Counts the number of solutions to the oracle

Bounded error in quantum counting

$$\left|\pi_{QM}(x) - \pi(x)\right| \leq \frac{2\pi}{c} \frac{x^{1/2}}{\log^{1/2} x}$$

Riemann Hypothesis

$$\left|Li(x) - \pi(x)\right| < \frac{1}{8\pi} \sqrt{x} \log x$$

Error of quantum counting < fluctuations under the RH

A quantum computer could falsify the RH, but not prove it !!

Quantum speed up

Classical versus quantum computation of $\pi(x)$

Best classical algorithm by Lagarias-Miller-Odlyzko (1987)

time $T \sim x^{\frac{1}{2}}$ space $S \sim x^{\frac{1}{4}}$

A Quantum Computer could calculate the size of fluctuations more efficiently than a classical computer

$T \sim x^{\frac{1}{2}}$ $S \sim \log x$

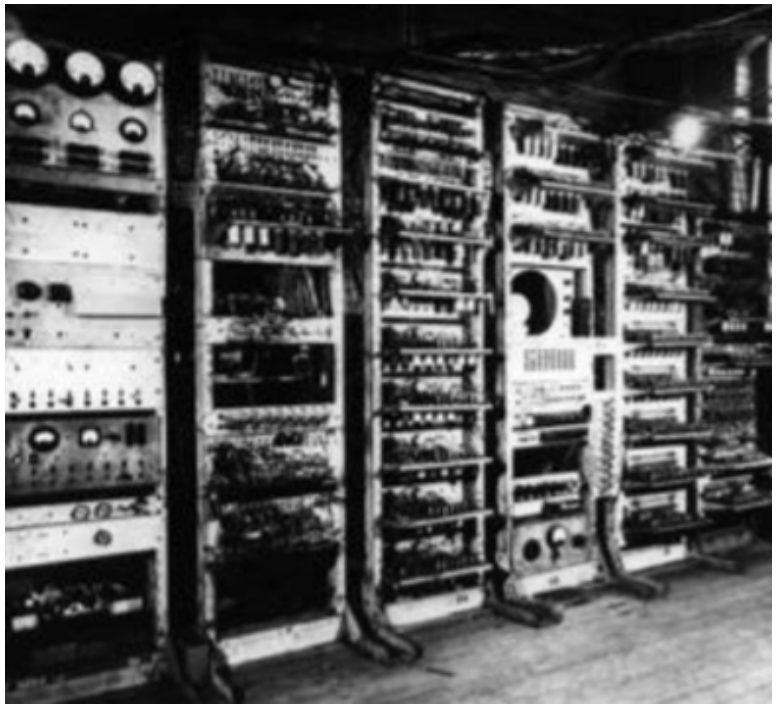
Turing, computers and number theory

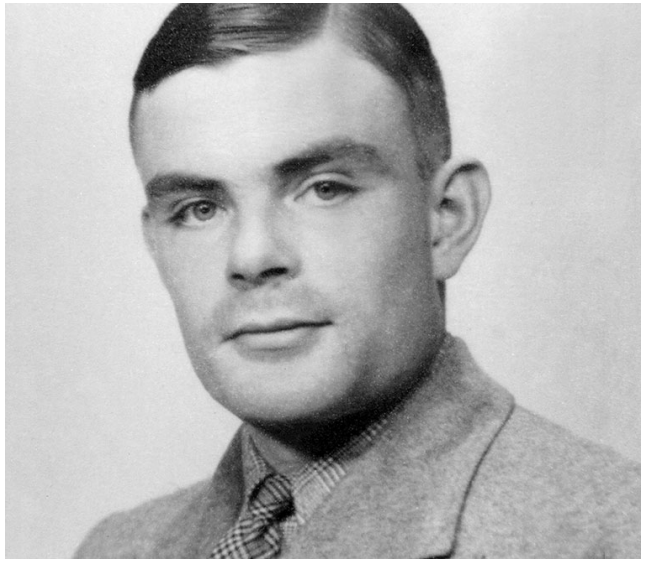
Turing did not believe in the Riemann hypothesis and wanted to disprove it.

In 1950 he used the electronic computer at the Manchester university

to find the first 1104 Riemann zeros who all lie on the critical line.

Then the machine broke down.

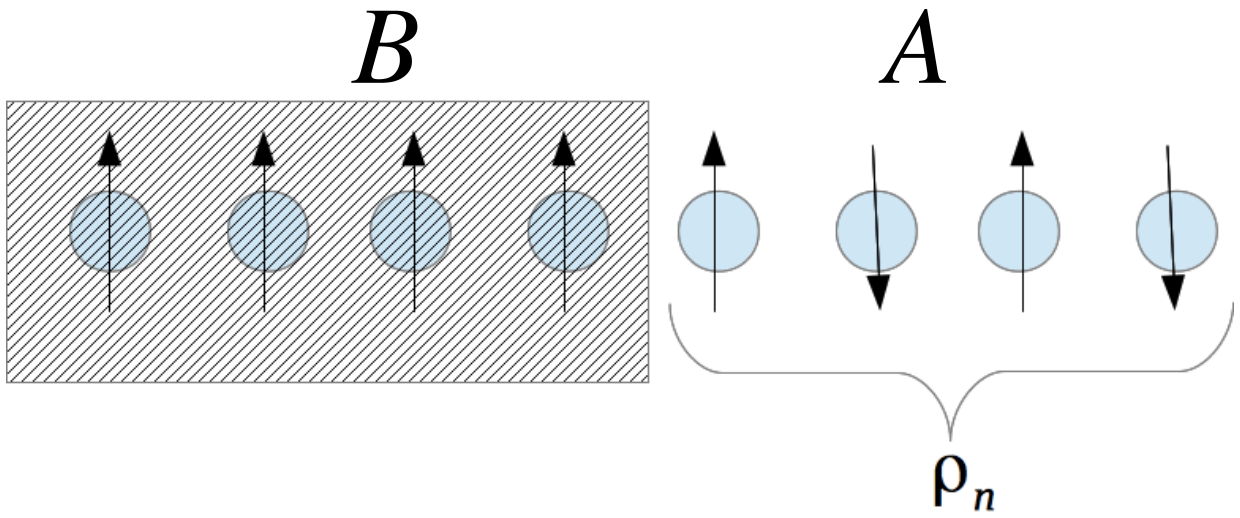




Entanglement entropy of the Prime state

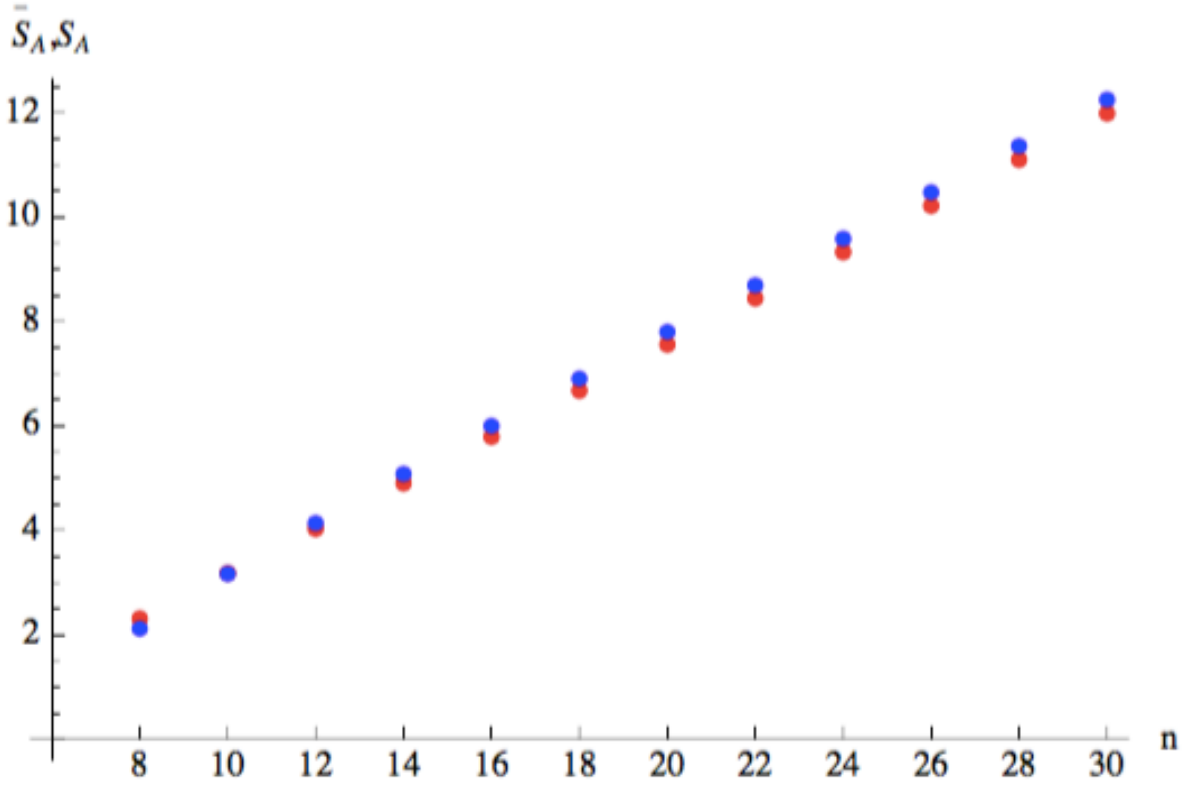
(JI Latorre, GS, 2015)

Density matrix of the Prime state



$$\rho_n = -Tr_B \left| P(n) \right\rangle \left\langle P(n) \right|$$

$$S_n = -Tr_A \left(\rho_n \log \rho_n \right)$$



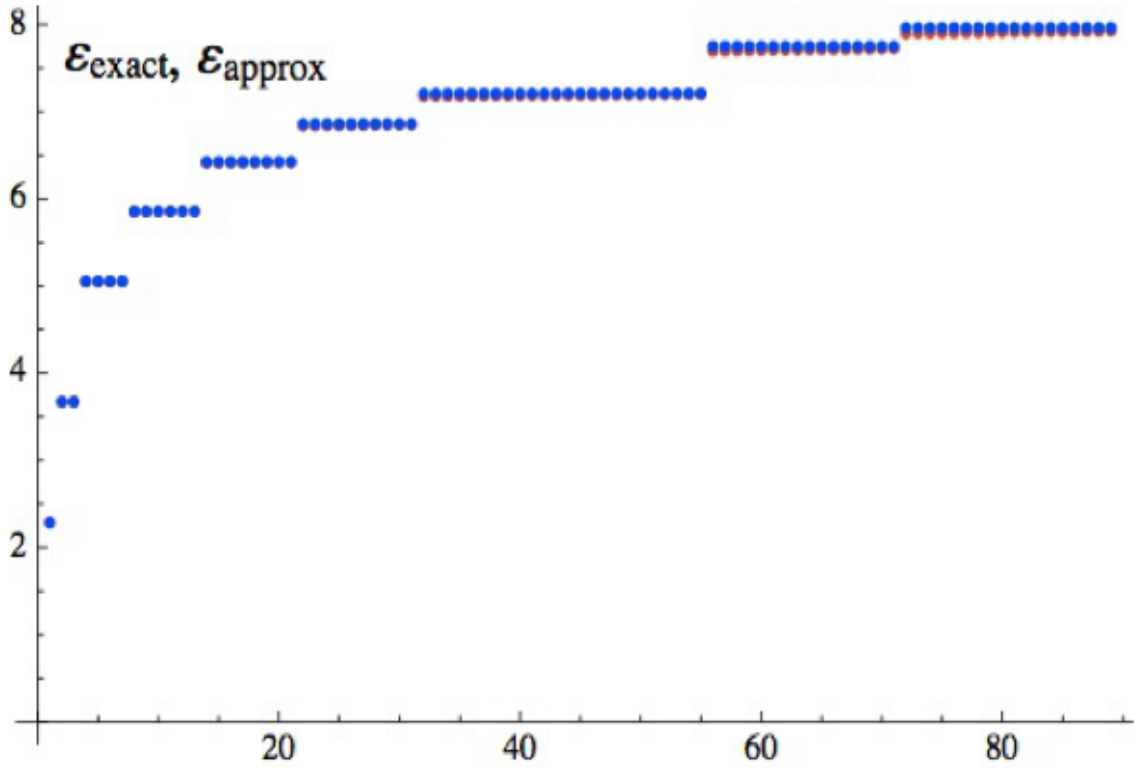
Volumen law entropy $S_n \approx 0.885\,(n/2) + cte$

A random density matrix has $S_n \approx (n/2) - 1/2$ (Don Page)

The Prime state is not random

Entanglement Spectrum of the Density Matrix

$$\rho = e^{-H_E}$$



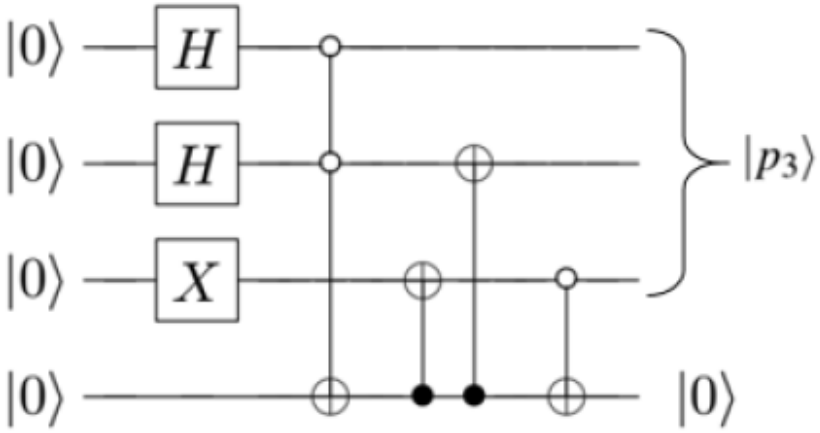
$$\rho_n \approx 1 + \frac{C}{n \log 2}$$

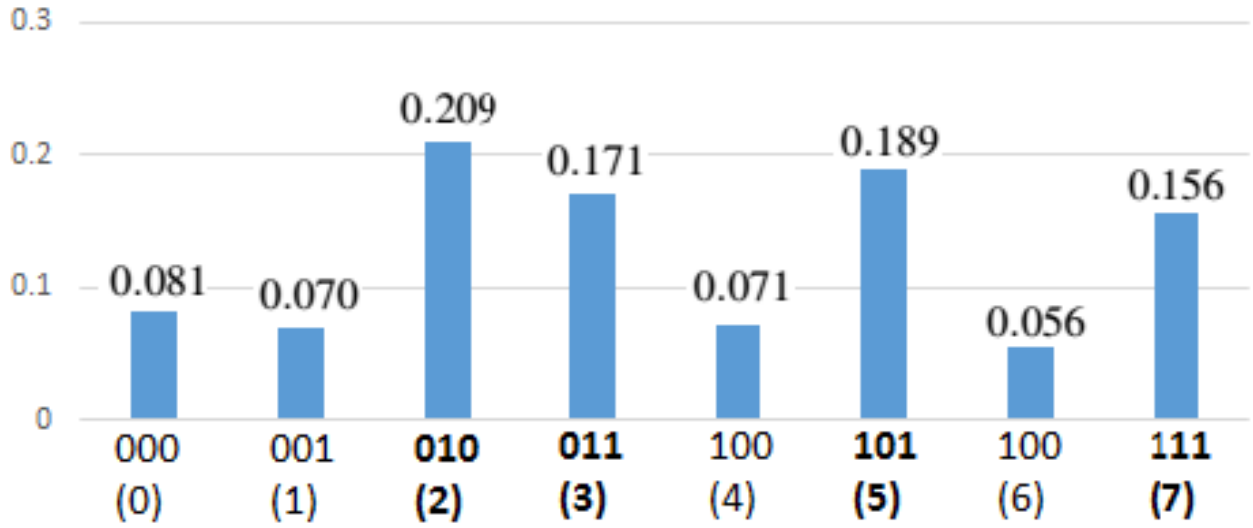
→ Prime correlations (Hardy-Littlewood)

Entanglement encode correlations between primes

IBM quantum computer and the Prime state

(Diego García-Martín, GS, 2018)





Conclusions

- Use quantum computers to study fundamental quantities in number theory:

Counting by measuring

- Number theory provides interesting highly entangled states to test quantum computers:

Quantum Arithmetics

Work done in collaboration with J.I. Latorre and D. García-Martín

"Quantum Computation of prime number functions",
J.I. Latorre and G.S., Quan. Info. Comm. 2014.

"There is entanglement in the primes",
J.I. Latorre and G.S., Quan. Info. Comm. 2015.

"Five experimental Tests on the 5-Qubit IBM Quantum Computer",
D. García-Martín and G.S., J. Applied Maths and Phys. 2018

Thanks for your attention