Prime Numbers and Quantum Computers

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)


15 = 3 \times 5

UCSB 2012
RSA-129 =
1143816257578888676692357799761466120102182967212423
6256256184293570693524573389783059712356395870505898
9075147599290026879543541
= 
3490529510847650949147849619903898133417764638493387
843990820577 ×
3276913299326670954996198819083446141317764296799294
2539798288533

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

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

Quantum computer

\[ |x\rangle = |x_{n-1}, \ldots, x_0\rangle = |x_{n-1}\rangle \otimes \ldots \otimes |x_0\rangle \]
The Prime State

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

\[ \pi\left(2^n\right) \] is the prime counting function
Ex. $n=3$

$$|P(3)\rangle = \frac{1}{\sqrt{4}} (|2\rangle + |3\rangle + |5\rangle + |7\rangle)$$
Prime counting function

\[ \pi(x) : \text{number of primes } p \text{ less than or equal to } x \]

\[ \pi(100) = 25 \]


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)

$$\lim_{x \to \infty} \frac{\pi(x)}{Li(x)} = 1, \quad Li(x) = \int_2^x \frac{dt}{\log t} \approx \frac{x}{\log x} + \frac{x}{(\log x)^2} + \ldots$$
<table>
<thead>
<tr>
<th>$x$</th>
<th>$\pi(x)$</th>
<th>$\pi(x) - x / \ln x$</th>
<th>$li(x) - \pi(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^1$</td>
<td>4</td>
<td>-0.3</td>
<td>2.2</td>
</tr>
<tr>
<td>$10^2$</td>
<td>25</td>
<td>3.3</td>
<td>5.1</td>
</tr>
<tr>
<td>$10^3$</td>
<td>168</td>
<td>23</td>
<td>10</td>
</tr>
<tr>
<td>$10^4$</td>
<td>1,229</td>
<td>143</td>
<td>17</td>
</tr>
<tr>
<td>$10^5$</td>
<td>9,592</td>
<td>906</td>
<td>38</td>
</tr>
<tr>
<td>$10^6$</td>
<td>78,498</td>
<td>6,116</td>
<td>130</td>
</tr>
<tr>
<td>$10^7$</td>
<td>664,579</td>
<td>44,158</td>
<td>339</td>
</tr>
<tr>
<td>$10^8$</td>
<td>5,761,455</td>
<td>332,774</td>
<td>754</td>
</tr>
<tr>
<td>$10^9$</td>
<td>50,847,534</td>
<td>2,592,592</td>
<td>1,701</td>
</tr>
<tr>
<td>$10^{10}$</td>
<td>455,052,511</td>
<td>20,758,029</td>
<td>3,104</td>
</tr>
<tr>
<td>$10^{11}$</td>
<td>4,118,054,813</td>
<td>169,923,159</td>
<td>11,588</td>
</tr>
<tr>
<td>$10^{12}$</td>
<td>37,607,912,018</td>
<td>1,416,705,193</td>
<td>38,263</td>
</tr>
<tr>
<td>$10^{13}$</td>
<td>346,065,536,839</td>
<td>11,992,858,452</td>
<td>108,971</td>
</tr>
<tr>
<td>$10^{14}$</td>
<td>3,204,941,750,802</td>
<td>102,838,308,636</td>
<td>314,890</td>
</tr>
<tr>
<td>$10^{15}$</td>
<td>29,844,570,422,669</td>
<td>891,604,962,452</td>
<td>1,052,619</td>
</tr>
<tr>
<td>$10^{16}$</td>
<td>279,238,341,033,925</td>
<td>7,804,289,844,393</td>
<td>3,214,632</td>
</tr>
<tr>
<td>$10^{17}$</td>
<td>2,623,557,157,654,233</td>
<td>68,883,734,693,281</td>
<td>7,956,589</td>
</tr>
<tr>
<td>$10^{18}$</td>
<td>24,739,954,287,740,860</td>
<td>612,483,070,893,536</td>
<td>21,949,555</td>
</tr>
<tr>
<td>$10^{19}$</td>
<td>234,057,667,276,344,607</td>
<td>5,481,624,169,369,960</td>
<td>99,877,775</td>
</tr>
<tr>
<td>$10^{20}$</td>
<td>2,220,819,602,560,918,840</td>
<td>49,347,193,044,659,701</td>
<td>222,744,644</td>
</tr>
<tr>
<td>$10^{21}$</td>
<td>21,127,269,486,018,731,928</td>
<td>446,579,871,578,168,707</td>
<td>597,394,254</td>
</tr>
<tr>
<td>$10^{22}$</td>
<td>201,467,286,689,315,906,290</td>
<td>4,060,704,006,019,620,994</td>
<td>1,932,355,208</td>
</tr>
<tr>
<td>$10^{23}$</td>
<td>1,925,320,391,606,803,968,923</td>
<td>37,083,513,766,578,631,309</td>
<td>7,250,186,216</td>
</tr>
<tr>
<td>$10^{24}$</td>
<td>18,435,599,767,349,200,867,866</td>
<td>339,996,354,713,708,049,069</td>
<td>17,146,907,278</td>
</tr>
<tr>
<td>$10^{25}$</td>
<td>176,846,309,399,143,769,411,680</td>
<td>3,128,516,637,843,038,351,228</td>
<td>55,160,980,939</td>
</tr>
<tr>
<td>$10^{26}$</td>
<td>1,699,246,750,872,437,141,327,603</td>
<td>28,883,358,936,853,188,823,261</td>
<td>155,891,678,121</td>
</tr>
<tr>
<td>$10^{27}$</td>
<td>16,352,460,426,841,680,446,427,399</td>
<td>267,479,615,610,131,274,163,365</td>
<td>508,666,658,006</td>
</tr>
</tbody>
</table>
The fluctuations of $\pi(x)$ around $Li(x)$ are expected 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

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

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

Efficient construction
Grover construction of the Prime state

\[ |\psi_0\rangle = \sum_{x < 2^n} |x\rangle = \sum_{p \in \text{primes}} |p\rangle + \sum_{c \in \text{composites}} |c\rangle \]

\[ M \]

\[ N \]

**Oracle**

\[ U_{\text{oracle}} |x\rangle = \mp |x\rangle, \quad x: \text{prime/composite} \]

**# Calls to Oracle**

\[ R(n) \leq cte \sqrt{n} \]
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:

- Green smiley face: then \( x \) is composite with certainty \( a \): strong witness

Test:

- Red sad face: 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)

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

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

$$T \sim x^2 \quad S \sim \log x$$
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

(JL Latorre, GS, 2015)

Density matrix of the Prime state

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

\[ S_n = -Tr_A \left( \rho_n \log \rho_n \right) \]
A random density matrix has

\[ S_n \approx (n/2) - 1/2 \quad \text{(Don Page)} \]

The Prime state is not random
Prime correlations (Hardy-Littlewood)

Entanglement encode correlations between primes

\[ \rho = e^{-H_E} \]

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


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

Thanks for your attention