Quantum physics offers new way to factor numbers

November 28 2016, by Lisa Zyga

Credit: CC0 Public Domain

(Phys.org)—Any number can, in theory, be written as the product of prime numbers. For small numbers, this is easy (for example, the prime factors of 12 are 2, 2, and 3), but for large numbers, prime factorization becomes extremely difficult—so difficult that many of today's cryptography algorithms rely on the complexity of the prime factorization of numbers with hundreds of digits to keep private

information secure.

However, no one is exactly sure of just how difficult it is to decompose very large numbers into their prime factors. This question, called the factorization problem, is one of the biggest unsolved problems in computer science, despite the use of advanced mathematical and computer science strategies in attempts to solve it.

Now in a new study published in *Physical Review Letters*, researchers Jose Luis Rosales and Vicente Martin at the Technical University of Madrid have taken a different approach to the problem.

The researchers have shown that the arithmetic used in factoring numbers into their prime factors can be translated into the physics of a device—a "quantum simulator"—that physically mimics the arithmetic rather than trying to directly calculate a solution like a computer does.

Although the researchers have not yet built a quantum simulator, they show that the prime factors of large numbers would correspond to the energy values of the simulator. Measuring the energy values would then give the solutions to a given factoring problem, suggesting that factoring large numbers into primes may not be as difficult as currently thought.

"The work opens a new avenue to factor numbers, but we do not yet know about its power," Rosales told *Phys.org*. "It is very striking to find a completely new way to factor that comes directly from quantum physics. It does not demonstrate that factoring numbers is easy, but finding new ways to factor certainly does not add to the strength of algorithms based on its assumed complexity."

For now, the researchers do not know the technical complexity of building such a device, or whether it would even be possible to factor very large numbers.

"We have shown that a quantum simulator able to factor numbers exists and, in principle, it could be built," Martin said. "Whether the simulator is feasible with current technology in a way that it can factor numbers of the same size as the ones used in cryptography remains to be seen, but the avenue is now open. The prospect of building such a device before a quantum computer is built is something to be pondered seriously."

Toward a quantum number theory

Besides the potential for practical applications, the results are also interesting on a more fundamental level.

"In our opinion, the contributions of the paper have two sides: in pure mathematics and in applied cryptography," Rosales said.

One of the most mathematically interesting aspects of the new work is that it involves redefining the factorization problem by introducing a new arithmetic function that could then be mapped onto the physics of the quantum simulator and correspond to the energy values. In a sense, the researchers are rewriting the math problem in terms of physics.

"The manuscript tries to bridge number theory with quantum physics," Rosales said, noting that researchers have been trying to do this for several decades. "Nowadays with the development of quantum information and computation and the discovery of Shor's algorithm, the connection seems more intriguing and important than ever."

In the long-term, this type of investigation could ultimately lead to a quantum number theory—a theory of numbers that is based on physical quantum systems.

"To develop a quantum number theory, what we need is a quantum system (at least a theoretical one) to able to reproduce the prime

numbers," Martin said. "In the paper, our take was to try to obtain a system able to factorize a number into its primes. The method is 'analogue' in the sense that it is not like Shor's algorithm, which is programmable in a quantum computer following the gate model. Instead, it is the measurement of a carefully set quantum system that provides the answer.

"To carry out this program, we need to first devise an arithmetic formulation of the factorization problem that is amenable to be quantized. We have to find an arithmetic function, eventually related to a Hamiltonian, and set up the quantum-mechanical problem such that its solution corresponds to the solution of the factorization problem. In the work we succeeded in carrying out these ideas. We found the correct arithmetic function, defined the factorization set to bind the Hamiltonian and obtained the solution of the quantum-mechanical problem. To the best of our knowledge, this has not been achieved before, although ours was not the first attempt.

"As it is always done in physics, to validate the results, we have to prove its predictive capabilities, so we did predictions with them: obtained a factorization algorithm that is completely new, with no similitude to any other factorization algorithm that we know of, and thoroughly checked the statistics of the solution against the prime number theorem.

"The results left us really astounded. To demonstrate this, in the paper we show how the spectrum reproduces the prime counting function and is almost identical to the Riemann's. This is obtained as a direct consequence of the quantum mechanical theory and has no counterpart in number theory. Carrying this to the extreme, this could be even considered the physics underlying the Riemann hypothesis [one of the most important open problems in number theory] in the sense that the Hamiltonian is naturally bounded, without any further assumptions."

The researchers explain that, in this paper, they just hinted that the results have deeper mathematical implications, and they plan to further investigate these possibilities in the future. They are also looking into what it would take to build a quantum simulator.

"We have ongoing research in the theory of building a simulator," Rosales said. "The first impression is encouraging, although nothing is decided yet."

More information: Jose Luis Rosales and Vicente Martin. "Quantum Simulation of the Factorization Problem." *Physical Review Letters*. DOI: 10.1103/PhysRevLett.117.200502 , Also at arXiv:1601.04896 [quant-ph]