Selected Passages from Correspondence with Friends 7 no. 1 (2019), 1–2. ISSN 2054–7145

SEARCHING FOR A NEEDLE IN A HAYSTACK, WHICH, IN ITS TURN, IS LOCKED IN A BIG BLACK BOX

ALEXANDRE BOROVIK AND ŞÜKRÜ YALÇİNKAYA

Researchers at the Universities of Manchester and Istanbul have solved an important problem of computational algebra, first posed in 1999, which was viewed by mathematicians around the world as absolutely impenetrable.

Assume you do all calculations in modular arithmetic modulo very large prime p (a standard setup in cryptography).

You are given matrices X and Y. You can multiply and invert these matrices on a computer; can you find a matrix U expressed in terms of X and Y and such that U^p, that is, U multiplied with itself p times is the identity matrix, while U itself is not the identity matrix?

It is a "needle in a haystack" problem. The catch is that the number of possible expressions is astronomical, and the problem was thought to be intractable. However the researchers found a practical algorithm for its solution and tested it for primes like $p = 115756986668303657898962467957$.

Some computational processes in algebra and cryptography (say, in "cloud computing") could be seen as black boxes, that is, devices which carry out computations with inputs and outputs represented in encrypted form, as strings of 0s and 1s. Even if the matrices are crunched inside of a black box and we are given strings – not matrices – for X and Y, our algorithm still finds a string representing U.

Multiplication of powers of U imitates addition in modular arithmetic, and this gives access to arithmetic hidden in the black box; this is critically important for symbolic computational algebra – to the degree that a solution to the problems was assumed, in many papers, as being provided by a make-believe "SL_2 Oracle". The researchers solved the problem without the help of fictitious oracles; this will find many applications. The findings also suggest that certain cryptosystems based on matrices are unlikely to be more secure than those based on plain modular arithmetic.

2010 *Mathematics Subject Classification* ????.

Publicity announcement of the paper A. Borovik and Ş. Yalçınkaya *Adjoint representations of black box groups* $\mathrm{PSL}_2(\mathbb{F}_q)$, J. Algebra 506 (2018) 540–591. In Abstract, The University of Manchester , 2018.

Notes

- Modular arithmetic with respect to modulo n, where n is natural number, deals with numbers $0, 1, 2, \ldots, n-1$ and "curtailed" operations of addition and multiplication: the sum $a+b$ (correspondingly, the product ab) of two numbers a and b is replaced by its remainder upon division by n; these operation are written as $a+b \bmod n$ and $ab \bmod n$. For example, if $n=7$, $3+5=1 \bmod 7$, because $3+7=8$, but after division by 7 gives remainder 1: $8=7+1$. Similarly $4\times 6 \bmod 7=3$, because $4\times 6=24$, which gives remainder 3 after division by 7: $24=3\times 7+3$. Modular arithmetic modulo large prime numbers is a cornerstone of modern cryptography.
- Matrices, as we use them in our paper, are square tables, filled with numbers; they are operated ("multiplied") according to certain algebraic rules universally accepted throughout all mathematics, with result always being a square table of the same size. These algebraic rules could be equally applied to ordinary numbers, or to so-called complex numbers, or, as in our case, to modular arithmetic.
- The identity matrix is filled with zeroes, with the exception of positions on the diagonal which goes from the left upper corner to the right bottom corner, which a filled with numbers 1. In matrix multiplication, identity matrices play the same role as the number 1 in arithmetic.
- The Observable Universe contains around 10^{80} electrons. Our haystack is much bigger: the number of different matrices which can be produced in our example with

  $$p = 115756986668303657898962467957$$

  is about 10^{87}. The probability to hit the desired matrix U at random is about 1 in 10^{58}; for comparison the number of elementary particles in the Sun is 10^{57}.

Click here to read the full article.

Partners

- Istanbul University, Turkey

Footnotes

The researchers' work was partially supported by the Marie Curie FP7 Initial Training Network MALOA (PITN-GA-2008-MALOA no. 238381) and by CoDiMa (CCP in the area of Computational Discrete Mathematics; EPSRC grant EP/M022641/1), and by The Dame Kathleen Ollerenshaw Trust. In the project, they were using the GAP software package by The GAP Group, GAP–Groups, Algorithms, and Programming, Version 4.8.4; 2016 (http://www.gap-system.org).

School of Mathematics, University of Manchester, UK; alexandre ≫ at ≪ borovik.net

Department of Mathematics, İstanbul University, Turkey; sukru.yalcinkaya ≫ at ≪ istanbul.edu.tr