CONSTRUCTING A TEN BILLION FACTOR CARMICHAEL NUMBER

STEVEN HAYMAN AND ANDREW SHALLUE

Given a list $a_1, a_2, \ldots, a_n, b$ of elements of G, the subset product problem is to determine a subset of the a_i that product to the target b in G. The hardest problems are those for which n and $\log_2 |G|$ are roughly the same (we say these problems have density 1).

During the poster session at ANTS IX it was proposed that focusing on advances in algorithms that solve the subset-product problem would result in better algorithms for constructing large pseudoprimes such as Carmichael numbers. We here report a first advance in this program with the construction of a ten billion factor Carmichael number, a number with nearly three hundred billion decimal digits. Construction necessitated solving a subset product problem with n over ten billion and $\log_2 |G|$ close to 190.

The large density played a key role in the construction. The particular tool used was the Kuperberg idea detailed in [1]. Our algorithmic contribution was to sort for a_i that were already somewhat closer to the identity (using the same metric used in [2]), so that the Kuperberg idea could be applied to a subgroup of the original group G.

References

[1] Greg Kuperberg, *A subexponential-time quantum algorithm for the dihedral hidden subgroup problem*, SIAM J. Comput. **35** (2005), no. 1, 170–188 (electronic).

[2] Günter Löh and Wolfgang Niebuhr, *A new algorithm for constructing large Carmichael numbers*, Math. Comp. **65** (1996), no. 214, 823–836.