1125-11-965
Ted Chinburg* (ted@math.upenn.edu), Dept. of Math, U. Penn., 209 S. 33rd Street, Philadelphia, PA 19104, Brett Hemenway, Dept. of Computer Science, 3330 Walnut St., University of Pennsylvania, Philadelphia, PA 19104, Nadia Heninger, Department of Computer Science, 3330 Walnut St., University of Pennsylvania, Philadelphia, PA 19104, and Zachary Scherr, Buckmell University, Department of Mathematics, 380 Olin Science Building, Lewisburg, PA 17837. Capacity theory and Coppersmith's algorithm for integral points. Preliminary report.

In 1996, Coppersmith described polynomial time algorithms for finding (i) small solutions to one variable polynomial congruences, and (ii) small integral solutions to polynomial equations in two variables. I will describe how capacity theory can be used to quantify how far one can extend Coppermith's method of treating problem (ii). This has applications to finding an unknown divisor d of a given large integer N given a sufficiently close approximation to d. (Received September 13, 2016)