1023-68-810 **Andrew Shallue*** (shallue@math.wisc.edu), University of Wisconsin-Madison, Mathematics Department, 480 Lincoln Dr, Madison, WI 53706-1388. *A Faster Algorithm for Random Dense Subset Sums.*

In the Random Modular Subset Sum (RMSS) problem we are given a modulus m, a target t, and elements $a_1, \ldots, a_n \in Z/mZ$ generated uniformly at random. We are asked to find $x_i \in \{0, 1\}$ such that $\sum_{i=1}^{n} a_i x_i = t \bmod m$. A dense RMSS problem is one for which $m = 2^{cn}$ with $c < 1$. For the case of $m = 2^{cn/2}$ with $c < 1$, we present an algorithm that runs using time and space $O(n^2 \log m \cdot m^{1/2})$, and succeeds with probability at least $1 - 2^{-\frac{(1-c)n}{16}}$. For example, if $m = 2^{n/4}$ it runs in time $O(2^{n/8+3\log n})$ which is the fastest algorithm known for this case. (Received September 21, 2006)