1018-14-176 **Peter Stevenhagen*** (psh@math.leidenuniv.nl), Department of Mathematics, University of California at San Diego, 9500 Gilman Dr, La Jolla, CA 92093-0112, and **Reinier Bröker**.

Constructing elliptic curves in almost polynomial time.

We present an algorithm that, on input of a positive integer N together with its prime factorization, constructs a finite field F and an elliptic curve E over F for which $E(F)$ has order N. Although it is unproved that this can be done for all N, a heuristic analysis shows that the algorithm has an expected run time that is polynomial in $2^{\omega(N)} \log N$, where $\omega(N)$ is the number of distinct prime factors of N. In the cryptographically relevant case where N is prime, an expected run time $O((\log N)^{4+\varepsilon})$ can be achieved. We illustrate the efficiency of the algorithm by constructing elliptic curves with point groups of order $N = 10^{2006}$ and $N =$nextprime$(10^{2006}) = 10^{2006} + 2247$. (Received March 06, 2006)