998-11-98 **Daniel J. Bernstein*** (conf6594@box.cr.yp.to). *How to find smooth parts of integers.*

You're given a set P of primes and a sequence S of integers. Which of the integers in S are P-smooth? What is the largest P-smooth divisor of each integer? What are all the factors from P of each integer? These questions occur in many applications: computing discrete logarithms, for example, and proving primality. I previously pointed out an algorithm that answers all three questions in time $b(\log b)^{3+o(1)}$, where b is the total number of bits in P and S. Franke, Kleinjung, Morain, and Wirth, in a recent paper on ECPP, pointed out an algorithm variant that answers only the first two questions but that typically takes time only $b(\log b)^{2+o(1)}$. In this talk I will present an algorithm that always answers the first two questions in time $b(\log b)^{2+o(1)}$. (Received February 14, 2004)