1020-11-96

Shuo Shen* (sshen@math.purdue.edu), 214-7 Halsey Dr., West Lafayette, IN 47906, and **Samuel S Wagstaff** (ssw@cerias.purdue.edu), computer science department, Purdue University, West Lafayette, IN 47906. *Elliptic Curves of Almost Prime Order.* Preliminary report.

Let E be an elliptic curve defined over finite field F_q, both k and q are odd primes. The elliptic curve $E(F_{q^k})$ is said to have almost prime order if the order of the quotient group $E(F_{q^k})/E(F_q)$ is prime. The probability that $E(F_{q^k})$ has almost prime order has been conjectured by Neal Koblitz and some other valuable related work was done by other researchers.

We give an asymptotic formula for the number of elliptic curves of almost prime order. The formula is proved based on Bateman-Horn's conjecture on the distribution of prime numbers. Our formula fits experimental data remarkably well. (Received August 19, 2006)