Elliptic Curves

Jake Fisher and Davis Lister

May 1, 2018

Pollard's p-1 Factoization

- Let B be a positive integer. The prime factorization of an integer $n = \prod p_i^{e_i}$. If $\forall i \ p_i^{e_i} \leq B$, n is B-power smooth.
- We wish to find a nontrivial factor of a large positive integer N using the Pollard p-1 method.
- Let us choose a positive integer B. Suppose that there is a prime factor p of N such that $p - 1$ is B-power smooth.

Group Law for Elliptic Curves

-

Lenstra's Elliptic Curve Factorization

-