

# 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.
- ▶ Let us choose  $a > 1$  such that  $p$  does not divide  $a$ . Often we will choose  $a = 2$  for convenience.
- ▶ By Fermat's Little Theorem  $a^{p-1} \equiv 1 \pmod{p}$ .
- ▶ Let  $m = \text{lcm}(1, 2, 3, \dots, B)$ . Since  $p - 1$  is  $B$ -power smooth,  $p - 1 \mid m \implies p \mid \gcd(a^m - 1, N) > 1$ .
- ▶ If  $\gcd(a^m - 1, N) < N$ , then  $\gcd(a^m - 1, N)$  is a nontrivial factor of  $N$ .

# Factoring Magic!

- ▶ An example of integer factorization using Pollard's  $p-1$  method.
- ▶ Let  $N = 5917$  and let  $B = 5$ .  $m = \text{lcm}(1, 2, 3, 4, 5) = 60$ .
- ▶ Let  $2^{60} - 1 = 3416 \pmod{5917}$ , and  $\text{gcd}(2^{60} - 1, 5917) = \text{gcd}(3416, 5917) = 61$ .
- ▶ 61 is a factor of 5917!
- ▶ But if  $p - 1$  and  $q - 1$  (where  $pq = N$ ) are not  $B$ -power smooth, Pollard  $p-1$  does not work :(
- ▶ The issue is that  $\mathbb{Z}/p\mathbb{Z}$  has order  $p-1$ .

# Group Law for Elliptic Curves



# Lenstra's Elliptic Curve Factorization

