

Math 259 - Spring 2021
Pollard's $p - 1$ factorization algorithm

Instructions

- Each problem on this assignment is worth 5 points.
- This assignment is available until Friday May 14 at 11:59pm.
- You can submit a second attempt for this assignment if your first attempt is turned in by Sunday March 21 at 11:59pm.
- If you look up solutions or facts, don't forget to cite your sources and to rephrase everything in your own words.
- You will need to use a calculator or computer for this assignment.

Problem

1. Use Pollard's $p - 1$ method to factor $N = 1739$. Please show your work "as if" you were computing by hand; you can look at the worked out example for what you should show.
2. Use Pollard's $p - 1$ method to factor each of the following two numbers. For this problem you do not need to show all of your work, but do specify which value of a you used, which value of n worked, and which of the two primes you found was such that $p - 1$ was a product of small primes.
 - (a) $N = 220459$
 - (b) $N = 48356747$