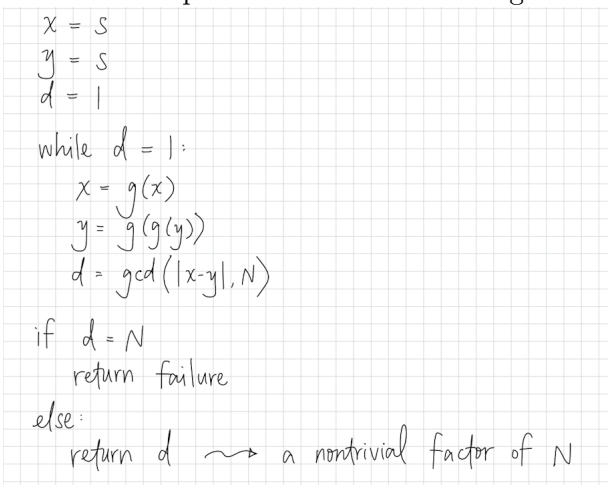
Dartmouth College Department of Mathematics
Math 148 Introduction to Public Key Cryptography and Elliptic Curves
Spring 2025

Problem Set # 4 (due by Canvas upload by the end of Friday 16 May)

Problems:

1. Recall the "Optimized" Pollard Rho Algorithm shown below:



Prove that the algorithm will in fact exit the while loop and terminate.

2. (HPS 3.33). Use a quadratic sieve to factor 493 using prime powers up to $B = 11$ on values from $F(23)$ to $F(38)$. Record the sieving process in whatever way makes the most sense to you (see the sieving diagrams from HPS).

3. (HPS 1.34) Let p be an odd prime number and let b be an integer with $p \nmid b$. Prove that b has two square roots modulo p or b has no square roots modulo p.

4. Suppose that $t = \alpha_p$ is a solution to the congruence

$$t^2 \cong N \mod p^e.$$

Prove that each number in the sequence $\{F(\alpha_p + kp^e)\}_{k\in\mathbb{N}}$ is divisible by p where $F(x) = x^2 - N$, $e \in \mathbb{N}$. Explain why this is important in the context of the quadratic sieve algorithm.