Name: _____

Read and take notes on the introduction to Chapter 18, Factorization Attacks, and Section 18.1, Pollard's Rho Method. **Note**: The function $f(x)$ given in the algorithm should include a reduction modulo n, as is made clear by the examples at the end of the section.

Reading Questions

1. Describe two advantages and two disadvantages of Pollard's rho method.

2. How does one initialize the algorithm for Pollard's rho method, i.e. what are x, $f(x)$, and y at the beginning of the algorithm? (See note above.)

3. Consider $n = 209$.

   (a) Use Fermat's Test (with base $b = 2$) to show that n is composite.

   (b) Apply one cycle of the algorithm of Pollard's rho method to n: compute $x - y$ and use the Euclidean algorithm to find g. Have you found a proper factor of n? Has the algorithm failed? If not, repeat the algorithm to find a proper factor of n.

4. Consider $n = 4031$.

   (a) Use Fermat's Test (base $b = 2$) to show that n is composite.

   (b) About how many cycles of the algorithm to we expect to need to find a factor of $n = 4031$?

   (c) Apply Pollard's rho method to $n = 4031$ to find a factor. (You may use *Mathematica* or some other tool to compute gcds.) How many cycles does it actually take to find a factor?

5. What struck you in this reading? What is still unclear? What remaining questions do you have?