1. Using various choices for the bound, $B$, factor 71201983 with the Pollard $p$-1 method. How big does $B$ have to be in order for you to be successful? [2 marks]

2. Factor 88820773 using the Pollard Rho factoring algorithm with function, $f$, defined as $f(x) = x^2 + 1$. How many iterations are needed to factor this number? [2 marks]

3. The integer $p = 809$ is prime, and it can be verified that the element $\alpha = 89$ has order $n = 101$ in $\mathbb{Z}_{809}^*$. The element $\beta = 532$ is in the subgroup $\langle \alpha \rangle$. Let the sets $S_1$, $S_2$, and $S_3$ be defined as follows:

   $S_1 = \{x \in \mathbb{Z}_{809} : x \equiv 1 \pmod{3}\}$

   $S_2 = \{x \in \mathbb{Z}_{809} : x \equiv 0 \pmod{3}\}$

   $S_3 = \{x \in \mathbb{Z}_{809} : x \equiv 2 \pmod{3}\}$

   Using the Pollard Rho discrete logarithm algorithm, compute $\log_{\alpha}\beta$. [2.5 marks]

4. Why do factoring and discrete log have the same computational complexity? (Explain in your own words, given what you know about how the algorithms work.) [1.5 marks]