Math 180B, problem set for May 31

(1) Alice and Bob are using the Diffie-Hellman key exchange protocol to establish a shared secret. They agree to use the modulus 59, and the primitive root 2 (mod 59). Alice’s secret exponent is 10, Bob’s secret exponent is 7.
   (a) What does Alice send to Bob?
   (b) What does Bob send to Alice?
   (c) What is the shared secret?

(2) Using the baby-step/giant-step method, find $x$ such that $2^x \equiv 43 \pmod{53}$.

(3) Using the baby-step/giant-step method, find $x$ such that $2^x \equiv 43 \pmod{101}$.

(4) Using the Pollard rho method, find $x$ such that $2^x \equiv 3 \pmod{47}$.

(5) Suppose you are using the Pollard rho method to find $x$ such that $g^x \equiv a \pmod{p}$. Suppose that in the sequence $X_0, X_1, X_2, \cdots$ that you compute, the first repetition happens when you find that $X_{932} = X_{765}$. How many steps will it take to complete the algorithm? I.e., what is the smallest value of $k$ for which $X_{2k} = X_k$?

If you want to try some more serious calculations, replace problems (1)-(4) above with the following:

(1) Alice and Bob are using the Diffie-Hellman key exchange protocol to establish a shared secret. They agree to use the modulus $p = 123456789123456823$, and the primitive root $3 \pmod{p}$. Alice’s secret exponent is 103768812158231052, Bob’s secret exponent is 59041580926275362.
   (a) What does Alice send to Bob?
   (b) What does Bob send to Alice?
   (c) What is the shared secret?

(2) Using the baby-step/giant-step method, find $x$ such that $2^x \equiv 3 \pmod{123456803}$.

(3) Using the baby-step/giant-step method, find $x$ such that $2^x \equiv 5 \pmod{123456803}$.

(4) Using the Pollard rho method, find $x$ such that $2^x \equiv 3 \pmod{123456803}$.