Mathematica might be helpful for this assignment, but I think you should be able to do all or most of it in Excel.

1. Without using Mathematica or Alpha or other aids, in each case, use the information about $\phi(n)$ to factor $n$.
   (a) $n = 8549$, $\phi(n) = 8364$.
   (b) $n = 15931$, $\phi(n) = 15664$. (Calculating $\gcd(n, \phi(n))$ is useful.)
   (c) $n = 221911$, $\phi(n) = 214968$. (Calculating $\gcd(n, \phi(n))$ is useful.)

2. A theoretical comparison of Pollard’s two methods: In class, I stated that on average, a number $n$ will have largest prime divisor $\approx n^{63}$. This means that the second largest prime divisor should be around $(n^{37})^{63} \approx n^{23}$. The difficulty in factoring a number is often measured by its second largest prime divisor: once this prime is found, the last divisor can be found by just one more division. Typically, one expects Pollard’s rho method to find a prime divisor $p$ of $n$ in roughly $\sqrt{p}$ steps. For the $p - 1$ method, one finds $p$ in $k$ steps when $p - 1$ is a divisor of $k!$. Assuming that $n$ and $p - 1$ are “average” numbers,
   (a) On average, how big does $k$ have to be for $p - 1$ to be a divisor of $k!$?
   (b) Based on part (a) and the discussion above, which of Pollard’s methods is better on average?

3. Factor each of the numbers below using (i) Fermat’s method, (ii) Pollard’s rho method, (iii) Pollard’s $p - 1$ method.
   (a) $n = 1189$
   (b) $n = 1927$
   (c) $n = 17, 819$
   (d) $n = 36, 287$

4. Factor $n = 48, 227$ using both Pollard’s rho method and the $p - 1$ method.

5. Consider the number $n = 13, 019 = 47 \times 227$.
   (a) How many steps does Fermat’s method take to factor $n$?
   (b) How many steps does Fermat’s method take to factor $3n$?
   (c) How many steps does Fermat’s method take to factor $3 \cdot 3 \cdot 5 \cdot 7n$?

6. For extra credit: In class, I said I don’t know how to factor $n$ if $n = pqr$, a product of three distinct primes.
   (a) Show how knowing $\phi(n) = (p - 1)(q - 1)(r - 1)$ tells you how to factor $n$.
   (b) Extend to $n$ as a product of $k$ distinct primes.