

1. 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 $\approx (n^{.37})^{.63} \approx n^{.23}$. The difficulty of factoring a number is often measured by its **second largest prime divisor**: once this is found, the last divisor is just a division away. Typically one expects Pollard's rho-method to find the 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 n and $p-1$ are "average",
 - a. How big does k have to be on average for $p-1$ to be a divisor of $k!$?
 - b. Based on the above, which of Pollard's methods is better on average?
2. Factor each of the following numbers using Fermat's method, Pollard's rho-method and Pollard's $p-1$ method.
 - a. 1189
 - b. 1927
 - c. 17819
 - d. 36287
3. Factor 48227 using both Pollard's rho-method and the $p-1$ method.