Name: ______________________________

Read and take notes on 18.2, Pollard's $p - 1$ Method. **Note**: The change of base formula for logarithms is $\ln(x)/\ln(a) = \log_a(x)$. This fact is useful for understanding how the examples follow the given algorithm.

Reading Questions

1. Make sure you understand the meanings of the following terms: B-smooth, smoothness bound.
2. **Note.** For a set $\{p_1, \ldots, p_t\}$ of primes (usually consecutive primes, starting with 2), for a number to be $\{p_1, \ldots, p_t\}$-smooth means that all its prime factors lie in the set $\{p_1, \ldots, p_t\}$. If $\{p_1, \ldots, p_t\}$ is the set of primes less than or equal to a bound B, than being B-smooth is equivalent to being $\{p_1, \ldots, p_t\}$-smooth.
3. (a) In what cases does Pollard's $p - 1$ method work well?

   (b) Why is this method is important, despite the fact that it only works in certain special cases?
4. Fix $B = 10$. Give three examples of numbers that are B-smooth and one example of a number that is *not* B-smooth.
5. Consider $n = 1581$. Fix $B = 3$.

   (a) First we choose random b in $1 < b < n$. Choose $b = 1000$. Then compute $g = \gcd(b, n)$. What is g? Explain why we must continue with the algorithm.

(b) The primes less than or equal to B are $p_1 = 2$ and $p_2 = 3$. For $p_1 = 2$:

i. Compute $\ell = \text{floor}(\ln(n)/\ln(p_1))$.

ii. Compute $r = p_1^{\ell} \,\%n$.

iii. Replace b by $b^r \,\%n$.

iv. Compute $g = \gcd(b - 1, n)$.

(c) Explain why we may stop the algorithm at this point.

(d) If we had found $g = 1$ in the previous part, what would we have needed to do?

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