Name: _____

Read and take notes on 18.3, Pocklington-Lehmer Criterion. Focus on Proth's Corollary, Fermat numbers, Pepin's Test, and Euler's lemma for speeding up the search for factors.

Reading Questions

1. Make sure you are familiar with the following: Proth's Corollary, Fermat numbers, Pepin's Test, Euler's speed-up Lemma, Mersenne numbers, the Lucas-Lehmer test.
2. (a) In what cases is the Pocklington-Lehmer criterion especially useful?

   (b) In what cases is it most often applied?

   (c) How else can the technique be used, besides being used to prove primality?

3. Let $N = 5$.

   (a) Write N in the form $N = u2^n + 1$, where $u < 2^n$ and u is odd.

   (b) Find b such that $b^{(N-1)/2} = -1 \bmod N$.

   (c) What does Proth's Corollary allow you to conclude about N?

4. Use Pepin's Test to show that the third Fermat number, $F_3 = 257$, is prime.

5. What lemma (due to Euler) allows us to speed up the search for prime factors of Fermat numbers by a factor of 128? State the lemma here.

6. Take a look at the following recent article. (The link is live in the pdf file.) What is the largest known prime number?

   http://www.nytimes.com/2016/01/22/science/new-biggest-prime-number-mersenne-primes.html?_r=0

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