Math 316, 18.5 Primality Certificates

Name: ______________________________

Read and take notes on Section 18.5: Primality Certificates.

Reading Questions

1. Reread the first example in this section, which describes how to find a primality certificate for $N = 1\,000\,000\,033$.

   (a) Why do we have good reason to think this is a prime? More precisely, what is the probability that N is prime, given the test described at the beginning of the example?

   (b) Using trial division with small primes, we can write $N - 1$ as a product of small primes and another factor. In this example, "small" means less than or equal to 127. Write the resulting factorization of $N - 1$.

   (c) This allows us to write $N - 1 = K \cdot U$, where the prime factorization of K is known and, although the prime factorization of U is unknown, we do know that it has no prime factors less than a certain bound B. What are K, U, and B in this example?

   (d) To use the second version of the Lucas-Pocklington-Lehmer theorem, what do we need to verify about $B \cdot K$? (See the bulleted recap of the second version of the Lucas-Pocklington-Lehmer theorem, hereafter refered to as LPL v2, at the beginning of the section.) Verify that condition here.

   (e) For each prime q dividing K, we want to find b_q satisfying two criteria. What are the two criteria? (Again, see the bulleted recap of LPL v2.)

(f) List the primes q dividing K and the numbers b_q that are found to work in this example.

(g) The last bullet point in the recap of LPL v2 requires that we find a number b_0 satisfying two criteria. What are the two criteria?

(h) What number b_0 is found to work in this example?

(i) What is the data comprising the primality certificate for N in this example/

(j) Explain, in your own words, why providing the stated data is a primality certificate for N. (See the remark immediately following the statement of the primality certificate for this example.)

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