Problem Set 5

Due on Thursday, November 16, 2006.

Problem 22: Primitive Roots

Write a computer program to find pairs (p, g), where p is an odd prime and g is a primitive root of p. The program should take as input a number $n_0 < 2^{256}$ and find the smallest odd prime p_0 such that $p_0 \geq n_0$. It should then find the smallest number $u \geq 2$ such that $p = up_0 + 1$ is prime. Finally, it should find the smallest number $g \geq 2$ such that g is a primitive root of p.

Your program should print out n_0, p_0, u, p, and g. It should also print out a "proof" using the Lucas test that g is a primitive root of p. That is, for each prime divisor q of $p-1$, it should compute and print q, $(p-1)/q$, and $g^{(p-1)/q} \bmod p$, demonstrating that the latter is not equal to 1.

Your program should be written in C, C++, or Java and should use one of the big number libraries discussed in Section 37 of Lecture Notes 7 (if using C or C++) or using the appropriate Java class libraries (if using Java). You may use any of the provided functions in solving this problem. In particular, you do not need to implement your own primality testing function or modular exponentiation function if the versions provided by the package are adequate for this problem.