

MAT 421 Number Theory

Takehome Exam 3

Note: Read the test instructions in my email carefully and thoroughly before you begin your exam. Failure to follow the instructions could result in point reductions or no point on individual problems.

1. (20pts) Use the repeated squaring method to compute the least residue of 2^{340} modulo 341.
2. (10 pts) Use the Fermat's little theorem to show that 91 is not a prime.
3. (10 pts) Use the Lucas-Lehmer test to determine if $M_{11} = 2^{11} - 1$ is a prime.
4. (20 pts) Factor 91 by the Monte Carlo Method with $f(x) = x^2 - 1$ and $x_0 = 2$. For each k step, compare x_k only with x_j for which $j = 2^h - 1$ where k is an $(h + 1)$ -bit integer.
5. (10 pts) Use Fermat factorization to factor 809009.
6. (10 pts) Use generalized Fermat factorization to factor 17018759.
7. (20 pts) Use Pépin's test to show that $F_4 = 2^{16} + 1$ is a prime.