Problem 1

Consider the following computational problem: Given $N, a, b, x, y$, where $N \geq 1$ is prime, $a, b, x, y$ are integers between 1 and $N - 1$, compute $a^xb^y \pmod{N}$.

1. Describe an algorithm that takes at most $4k + C$ multiplications, where $k = \log N$ and $C$ is a positive constant.

2. Design an algorithm that uses at most $2k + C'$ multiplications, for some constant $C'$.

Problem 2

A common form of Fermat’s Little Theorem is: $a^p = a \pmod{p}$, for any prime $p$ and integer $a$. Prove this by induction on $a$. (Hint: prove that $(a + b)^p = a^p + b^p$ modulo $p$).

Problem 3

At some point, long ago, people seeking prime numbers had hoped that many integers of the form $2^n - 1$ (so-called Mersenne numbers) would be prime. It’s true for $n = 2, 3$ but not $n = 4$. Prove that if $n > 2$ is not a prime number then $2^n - 1$ is not a prime either.

Problem 4

Consider the Fibonacci numbers: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$, for $n > 1$. Show how to compute $F_n$ using only $O(\log n)$ additions and multiplications. (Hint: express the recurrence as a two-by-two matrix.)