Assignment 2, due January 20

Problem 1

Prove that there are infinitely many primes of the form $6q+5$ for some integer q.

Problem 2

Prove that if $a = qb + r$, where a, b, q, r are integers, show that

$$\gcd(2^a - 1, 2^b - 1) = \gcd(2^b - 1, 2^r - 1).$$

Problem 3

Show that if $a|b$ then $(2^a - 1)|(2^b - 1)$.

Problem 4

Using the two previous exercises and Euclid Algorithm, show that

$$\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1.$$

Derive that two Mersenne numbers are coprime.

Problem 5

For which primes p the number $2p^2 + 1$ is also prime?
Hint: Consider the remainder of division of $2p^2 + 1$ by 3.