ASSIGNMENT 5 - NUMBER THEORY, WINTER 2009

Submit by Wednesday, February 18, 16:00.

Solve 4 of the following questions:

(19) For which integers $n \in \{3, 4, 5\}$ can we solve the equation

$$y^2 + y + 6n = 0 \pmod{101}?$$

(20) *Germain primes* are primes q of the form $q = 2p + 1$, where p is prime. For example,

$$5, 7, 11, 23, 47, \dots$$

are Germain primes. (Sophie Germain showed in 1823 that if $q = 2p + 1$ is a Germain prime then the Fermat equation $x^p + y^p = z^p$ has no solutions such that x, y and z are all indivisible by p - an important step towards establishing Fermat's theorem for such exponents. For more on this fascinating person see http://www.agnesscott.edu/Lriddle/WOMEN/germain.htm) It is unknown if there are infinitely many Germain primes, but it is conjectured to be true.

Prove that if $p \equiv 3 \pmod 4$ and $q = 2p + 1$ is prime then $2^p \equiv 1 \pmod q$. Conclude that $2^{251} - 1$ is not a prime. (This is an example of a Mersenne number; we'll study these numbers soon.)

(21) Prove that if $p \equiv 1 \pmod 4$ and $q = 2p + 1$ is prime then 2 is a primitive root modulo q.

(22) By modifying Euclid's argument, prove that there are infinitely many primes $p \equiv 3 \pmod 4$.

(23) Show that the gaps between consecutive primes can be arbitrary large.

(24) Consider primes of the form $x^2 + 1, x^2 - 1, x^3 + 1, x^3 - 1, x^2 - y^2, x^2 + y^2, x^3 - y^3$. In which cases can you prove that there are only finitely many primes of that shape? In which cases would you conjecture that there are infinitely many primes of that shape?

The honors students need to submit also 1 of the following problems.

(H). Find for which Germain primes q the residue class of 5 is a primite root modulo p.

(I). A natural number n is called *perfect* if

$$2n = \sum_{d|n} d,$$

that is, n is the sum of its proper divisors (those not equal to n). The perfect numbers up to 10^4 are

$$6, 28, 496, 8128.$$

For example: $6 = 1 + 2 + 3, 28 = 1 + 2 + 4 + 7 + 14$.

Prove the following: *Let n be an even number. Then n is perfect if and only if $n = 2^{p-1}(2^p - 1)$ and $2^p - 1$ is a Mersenne prime.*

Hint: For the hard direction, write $n = 2^k m$, m odd. Show that $\sigma(m) = 2^{k+1}c$ for some c and $m = (2^{k+1} - 1)c$. Proceed to show that $c = 1$.

It is not known if there are odd perfect numbers or not. It is known that the smallest odd perfect number, if it exists, is greater than 10^{300}.