ASSIGNMENT 4 - NUMBER THEORY, WINTER 2009

Submit by Monday, February 9, 16:00 (use the designated mailbox in Burnside Hall, 10^{th} floor).

Solve the following questions:

(14) Find a generator for the cyclic groups $(\mathbb{Z}/27\mathbb{Z})^*$ and $(\mathbb{Z}/125\mathbb{Z})^*$.

(15) Prove that every Carmichael number has at least 3 prime factors.

(16) Suppose that $t+1, 2t+1$ and $3t+1$ are primes.
   (a) Prove that for $t > 2$ this implies that $6|t$.
   (b) Prove that $(t+1)(2t+1)(3t+1)$ is a Carmichael number.
   (c) Find the first 2 Carmichael numbers of this shape (more, if you have access to suitable software).

(17) Let p be an odd prime. Prove that there are precisely $(p-1)/2$ squares in $(\mathbb{Z}/p\mathbb{Z})^\times$ and that they form a subgroup. Note that we therefore have $(p+1)/2$ squares in $\mathbb{Z}/p\mathbb{Z}$.

Prove that for every congruence class a mod p the equation

$$x^2 + y^2 = a,$$

has a solution.

(18) Prove that if $(n-1)! \equiv -1 \pmod{n}$ then n is prime. (This is a pretty, but totally useless, primality test.)

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

F. Prove that for every $n \geq 3$ we have

$$(\mathbb{Z}/2^n\mathbb{Z})^* \cong A \times B,$$

where A is a group of order 2 and B is a cyclic group of order 2^{n-2}. (Thus, $(\mathbb{Z}/2^n\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}$, but not in an obvious way.) Hint: consider the elements $-1, 5$ of $(\mathbb{Z}/2^n\mathbb{Z})^*$.

G. Let $p > 2$. Prove that the numerator of the rational number

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

is divisible by p.