Homework due Friday, November 15, 11:59pm

Recall that a *primitive root* modulo n is a generator of $\mathbb{Z}_n^\times$.

(1) Show that $\mathbb{Z}_3[i] = \{a + bi : a, b \in \mathbb{Z}_3,\ i^2 = -1\}$ is a finite field. Find a generator for the cyclic group $\mathbb{Z}_3[i]^\times$.
(2) Show that 2 is not a primitive root modulo the prime 179424673.
(3) Find the total number of primitive roots for each modulus.
  (a) 25
  (b) 41
  (c) 54
  (d) 1296
(4) Show that the product of all primitive roots modulo p is congruent to $(-1)^{\phi(p-1)}$ modulo p.
(5) Let p be prime. Use the existence of primitive roots modulo p to give another proof of Wilson's theorem.
(6) Suppose $p \equiv 1 \pmod 4$. Show that if a is a primitive root modulo p, then so is $-a$.

Additional problems, not to be turned in:

(1) A *Fermat prime* is a prime of the form $2^n + 1$.
  (a) Find the first four Fermat primes.
  (b) Let $p > 3$ be a Fermat prime. Show that $\left(\frac{3}{p}\right) = -1$.
  (c) Show that 3 is a primitive root mod p.