Homework due Friday, November 1, 11:59pm

(1) An integer is *squareful* if it is divisible by p^2 for some p. Show that there exists a sequence of 17 consecutive squareful numbers. For example, 48,49,50 is a sequence of 3 squareful numbers. Hint: Use the Chinese Remainder Theorem.

(2) Let p be an odd prime. Show that

$$1^2 3^2 5^2 7^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

(3) Prove that if p is prime and $d \mid p-1$, then $x^d - 1 = 0$ has d solutions over $\mathbb{Z}_p$.

(4) Show that there are infinitely many primes congruent to 1 (mod 4). Hint: Suppose we had a finite list $p_1, \ldots, p_m$, and consider the integer

$$(2p_1 \cdots p_m)^2 + 1.$$

(5) Show that a positive integer n can be written as the sum of two squares if

$$n = 2^t p_1^{d_1} \cdots p_r^{d_2} q_1^{e_1} \cdots q_s^{e_s},$$

where the p_i are distinct primes congruent to 1 modulo 4, the q_i are distinct primes congruent to 3 modulo 4, the d_i and e_i are positive integers, and the e_i are all even. Hint: use the Diophantus-Brahmagupta identity

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

Optional: Prove the converse.

(6) Find a simple criterion to determine when -2 is a quadratic residue modulo p, where p is an odd prime. (E.g. in terms of the congruence class of p modulo m for a certain m.)