Homework 17, due October 16

(1) (Chapter 3, Exercise 26) Let $p \equiv 3 \pmod 4$ be a prime. Show that $x^2 \equiv -1 \pmod p$ has no solutions. (Hint: Suppose x exists. Raise both sides to the power $(p-1)/2$ and use Fermat's theorem.)

(2) Let n be a positive integer, and suppose there exist positive integers x, y with $x^2 \equiv y^2 \pmod n$ and $x \not\equiv \pm y \pmod n$.
   (a) Prove that n is composite. (What happens if n is prime?)
   (b) Show that $1 < \gcd(x+y, n) < n$. Thus, $\gcd(x+y, n)$ is a nontrivial factor of n.

(3) Let p be an odd prime, and let a, b be integers with $ab \not\equiv 0 \pmod p$.
   (a) If a and b are both squares mod p, show that ab is a square mod p.
   (b) If a and b are both non-squares mod p, show that ab is a square mod p.
   (c) If one of a or b is a square mod p, and the other is a non-square mod p, show that ab is a non-square mod p.