

**Outline notes for PS07**  
**Math 126**

**Definitions.** (Ch. 16) binary expansion, Carmichael number.

**Problem outlines.**

16.1, 16.3, 16.5, 17.1, 17.3(a,c), 17.5(a,b).

**16.5.** Compute  $2^{9990} \pmod{9991}$  by successive squaring, and use answer to determine if 9991 is prime. (See: Fermat's Little Theorem and pp. 109–110.)

**17.3(a).** *Assume:*  $b, k, m \in \mathbb{Z}$ ,  $\gcd(b, m) = 1$ ,  $\gcd(k, \varphi(m)) = 1$ .

*Conclude:* There exists exactly one  $x \pmod{m}$  such that  $x^k \equiv b \pmod{m}$ .

**17.5.** (a) Apply methods of chapter to find  $x$  such that  $x^2 \equiv 23 \pmod{1279}$ . Identify point where methods fail.

(b) Generalize (a) to problem of finding  $x$  such that  $x^2 \equiv b \pmod{p}$ , where  $p$  is odd. Identify point where methods fail in general.