Math 445 Homework 4

Due Monday, September 30

15. (NZM, Problem 2.8.8) Determine how many solutions (mod 17) each of the following congruence equations has:

    (a) $x^{12} \equiv 16 \pmod{17}$ (b) $x^{48} \equiv 9 \pmod{17}$

    (a) $x^{20} \equiv 13 \pmod{17}$ (b) $x^{11} \equiv 9 \pmod{17}$

16. If p is a prime, and $p \equiv 3 \pmod{4}$, show that the congruence equation $x^4 \equiv a \pmod{p}$ has a solution $\Leftrightarrow$ $x^2 \equiv a \pmod{p}$ does.

17. (NZM, Problem 2.8.23) Show that if p is prime and $ord_p(a) = 3$, then $a^2 + a + 1 \equiv 0 \pmod{p}$. Use this to show that (for the same a) $ord_p(a + 1) = 6$.

18. (NZM, Problem 2.8.16, sort of) [If you need some big relatively prime numbers in a hurry....] Show that for m, n, a positive integers, $a \geq 2$, that $(a^m - 1, a^n + 1)|2$ if m is odd. (They are therefore relatively prime if a is even, and half of each is, if a is odd.)

    One approach: Setting $d = (a^m - 1, a^n + 1)$, show that $ord_d(a)$ is odd, and therefore $a^n \equiv 1 \pmod{d}$, so $d \leq 2$.

19. (NZM, Problem 2.8.18) Show that if a, b are both primitive roots of 1 modulo the **odd** prime p, then ab is *not* a primitive root of 1 modulo p.

    Hint: there is a specific, smaller, number k for which we can guarantee $(ab)^k \equiv 1 \pmod{p}$ ...