Math 445 Homework 5

Due Wednesday, October 6

21. Show that if an integer n can be expressed as the sum of the squares of two *rational* numbers
$$n = (\frac{a}{b})^2 + (\frac{c}{d})^2 \ ,$$
then n can be expressed as the sum of the squares of two *integers*.

    (Hint: Not directly! Show that n has the correct prime factorization....)

22. [NZM, p. 106, # 2.8.8] Determine how many solutions (mod 17) each of the following congruence equations has:

    (a) $x^{12} \equiv 16 \pmod{17}$ (b) $x^{48} \equiv 9 \pmod{17}$
    (c) $x^{20} \equiv 13 \pmod{17}$ (d) $x^{11} \equiv 9 \pmod{17}$

23. 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.

24. [NZM, p.107, # 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 $(ab)^k \equiv 1 \pmod p$ ...)

25. [NZM, p.106, # 2.8.2] Find a primitive root modulo 23.