Math 445 Homework 6 SOlutions

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....)

From (*), clearing denomenators, we have that $nb^2d^2 = a^2d^2 + c^2b^2 = (ad)^2 + (bc)^2$ is a sum of two squares. So for every prime p with $p \equiv 3 \pmod 4$, $p^k || nb^2d^2 = n(bd)^2$ with k even. But since $(bd)^2$ is a perfect square, $p^m || (bd)^2$ has m even. So $p^{k-m} || n$ has $k - m$ even. Consequently, every prime p with $p \equiv 3 \pmod 4$ which appears in the prime factorization of n has even exponent. Therefore, by our main result from class, n can be expressed as a sum of two squares.

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

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

$(12, 17-1) = (12, 16) = (4\cdot 3, 4\cdot 4) = 4\cdot(3, 4) = 4$, so we need to determine if, mod 17, $16^{\frac{17-1}{4}} = 16^4 \equiv 1$. But $16 \equiv -1$, so $16^4 \equiv (-1)^4 = 1$, as desired. Therefore, $x^{12} \equiv 16 \pmod{17}$ has $(12, 16) = 4$ solutions.

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

$(48, 17-1) = (48, 16) = 16$, so we need to determine if, mod 17, $9^{\frac{17-1}{16}} = 9^1 = 9 \equiv 1$. But it isn't; it is $9 \not\equiv 1$. So $x^{48} \equiv 9 \pmod{17}$ has no solutions.

(c) $x^{20} \equiv 13 \pmod{17}$

$(20, 17-1) = (20, 16) = 4\cdot(5, 4) = 4$, so we need to determine if, mod 17, $13^{\frac{17-1}{4}} = 13^4 \equiv 1$. But, mod 17, $13^2 = 169 \equiv -1$, so $13^4 \equiv (-1)^2 = 1$, as desired. So $x^{20} \equiv 13 \pmod{17}$ has $(20, 16) = 4$ solutions.

(d) $x^{11} \equiv 9 \pmod{17}$

$(11, 17-1) = (11, 16) = 1$ (since $1 = 3\cdot 11 - 2\cdot 16$), so we need to determine if, mod 17, $9^{\frac{17-1}{1}} = 9^{16} \equiv 1$. But since (9,17)=1 (since $2\cdot 9 - 1\cdot 17 = 1$), $9^{16} \equiv 1 \pmod{17}$ by Fermat's Little Theorem. So $x^{11} \equiv 9 \pmod{17}$ has 1 solution.

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.

On the other hand, show (by example) that if $p \equiv 1 \pmod 4$ this result need <u>not</u> be true.

Since $p \equiv 3 \pmod 4$, $p-1 \equiv 2 \pmod 4$, so $p-1 = 4k+2 = 2(2k+1)$ for some k. Then $(4, p-1) = (2 \cdot 2, 2(2k+1)) = 2(2, 2k+1) = 2$. By our result from class, $x^4 \equiv a$ (mod p) has a solution $\Leftrightarrow a^{\frac{p-1}{(4,p-1)}} = a^{\frac{p-1}{2}} \equiv 1 \pmod p$. But since $2|p-1$, $(2, p-1) = 2$, and so by the same result, $x^2 \equiv a \pmod p$ has a solution $\Leftrightarrow a^{\frac{p-1}{(2,p-1)}} = a^{\frac{p-1}{2}} \equiv 1$ (mod p).

So $x^4 \equiv a \pmod p$ has a solution $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p \Leftrightarrow x^2 \equiv a \pmod p$ has a solution, as desired.

On the other hand, for $p = 17$ and $a = 2$, $a^4 = 16 \equiv -1 \pmod{17}$, and so $a^8 \equiv (-1)^2 = 1 \pmod{17}$. So $a^{\frac{p-1}{(4,p-1}} \not\equiv 1 \pmod{17}$, so $x^4 \equiv 2 \pmod{17}$ has no solution; but $a^{\frac{p-1}{(2,p-1}} \equiv 1 \pmod{17}$, so $x^2 \equiv 2 \pmod{17}$ has a solution.

24. [NZM, p.106, # 2.8.13] Show that, for a prime p, the numbers $1^k, 2^k, \ldots (p-1)^k$ are all <u>distinct</u> mod $p \Leftrightarrow (k, p-1) = 1$.

This result is immediate for $p = 2$; there is only one element, 1^k, to look at, but $p - 1 = 1$, so $(k, p-1) = 1$ for all k.

For $p > 2$ prime, if the a^k are all distinct mod p, then the function

$$F : \{1, \ldots, p-1\} \to \{1, \ldots, p-1\} \text{ given by } F(x) = x^k \pmod p$$

is one-to-one. (The range is right, since $(x, p) = 1$ implies $(x^k, p) = 1$ (i.e., if $p|x^k$ then $p|x$).) But then by the pigeonhole principle, F is also onto. So for any a with $(a, p-1) = 1$, the equation $x^k \equiv a \pmod p$ has a solution. Since the k-th powers are all unique, it has exactly one solution. So by our result giving the count of solutions to such equations, since, if $x^k \equiv a \pmod p$ has a solution, it has precisely $(k, p-1)$ solutions, we must have $(k, p-1) = 1$.

On the other hand, if two of the powers are equal, mod p, we have $a^k \equiv b^k \pmod p$ for a and b distinct mod p; setting $c = a^k$, we then have two solutions, mod p, to $x^k \equiv c$ (mod p). Since the number of solutions to this equation, of positive, is $(k, p-1)$, we must therefore have $(k, p-1) \geq 2$, and therefore $(k, p-1) > 1$. So if $(k, p-1) = 1$, then all of the a^k must be distinct, mod p.