Math 445 Homework 5 Solutions

Due Wednesday, October 6

21. If an integer n can be expressed as the sum of the squares of two *rational* numbers

$$(*) \qquad n = (\frac{a}{b})^2 + (\frac{c}{d})^2 ,$$

then n can be expressed as the sum of the squares of two *integers*.

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. How many solutions (mod 17) each of the following congruence equations have?

(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 $p \equiv 3 \pmod 4$, then the congruence equation $x^4 \equiv a \pmod p$ has a solution $\Leftrightarrow$ $x^2 \equiv a \pmod p$ does.

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, $x^4 \equiv a \pmod p$ 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 $\Leftrightarrow a^{\frac{p-1}{(2,p-1)}} = a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

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.

24. 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.

Since p is odd, $p-1$ is even. Since a and b are primitive roots, $\text{ord}_p(a) = p-1 = \text{ord}_p(b)$. So, mod p, $a^{p-1} \equiv 1 \equiv b^{p-1}$, but $a^{\frac{p-1}{2}} \not\equiv 1 \not\equiv b^{\frac{p-1}{2}}$. By the Miller-Rabin test, the latter two equations imply that $a^{\frac{p-1}{2}} \equiv -1 \equiv b^{\frac{p-1}{2}}$. Consequently, $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (-1)(-1) = 1$, so $\text{ord}_p(ab) | \dfrac{p-1}{2} < p-1$, so ab is not a primitive root mod p .

25. Find a primitive root modulo 23.

Following our argument from class, since $23-1 = 22 = 2 \cdot 11$, we will find an a with $a^{22/11} = a^2 \not\equiv 1 \pmod{23}$ and b with $b^{22/2} = b^{11} \not\equiv 1 \pmod{23}$. Then $c = ab$ will be a primitive root. But $a = 2$ works; $2^2 = 4 \not\equiv 1$. And since 11 is odd, $b = 22 \equiv -1$ works; $22^{11} \equiv (-1)^{11} = -1 \not\equiv 1 \pmod{23}$. So, from our argument in class, $c = 2 \cdot 22 = 44 \equiv 21$ is a primitive root, mod 23.

Note: There are, in fact, $\Phi(\Phi(23)) = \Phi(22) = \Phi(2 \cdot 11) = (2-1)(11-1) = 10$ pimitive roots mod 23. They can be found by raising the one found here, 21, to all of the exponents relatively prime to 22. (Via Maple, they are: $21, 21^3 = 15, 21^5 = 14, 21^7 = 10, 21^9 = 17, 21^{13} = 19, 21^{15} = 7, 21^{17} = 5, 21^{19} = 20, 21^{21} = 11$. So, in consecutive order, they are 5,7,10,11,14,15,17,19,20,21 .)