MAT 373 Homework 14

Justyce Countryman

May 6, 2024

Problem 1: Let p be an odd prime and let a, b be integers such that $p \nmid ab$. Prove that the congruence $(x^2 - a)(x^2 - b)(x^2 - ab) \equiv 0 \pmod{p}$ always has a solution for some integer x.

Proof. Suppose p is an odd prime and let a, b be integers such that $p \nmid ab$. We need to consider all possible combinations of a, b being quadratic residuals (mod p) or non-quadratic residuals (mod p).

Case 1: a and b are quadratic residuals (mod p):

This tells us that $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ have solutions for some integer x, indicating that $p|(x^2 - a)$ and $p|(x^2 - b)$ are possible. Since p is a prime, and it divides at least one of $(x^2 - a)$, $(x^2 - b)$, or $(x^2 - ab)$ for some integer x, then the congruence $(x^2 - a)(x^2 - b)(x^2 - ab) \equiv 0 \pmod{p}$ will have a solution for some integer x.

Case 2: Either a or b is a quadratic residual (mod p) and the other is a non-quadratic residual (mod p):

In this case, either $p|(x^2 - a)$ or $p|(x^2 - b)$ for some integer x, but not both. This again allows the congruence $(x^2 - a)(x^2 - b)(x^2 - ab) \equiv 0 \pmod{p}$ to have a solution for some integer x.

Case 3: Both a and b are non-quadratic residuals (mod p):

This case requires the knowledge that since $p \nmid ab$, then $p \nmid a$ and $p \nmid b$. Because of this, we can use Legendre symbols to say that $(\frac{a}{p}) = (\frac{b}{p}) = -1$. More importantly, we can say:

$(\frac{ab}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p}) = (-1)(-1) = 1.$

This means ab is a quadratic residual (mod p) and $p|(x^2 - ab)$ for some integer x. Once again, the congruence $(x^2 - a)(x^2 - b)(x^2 - ab) \equiv 0 \pmod{p}$ holds the fact that there is a solution for some integer x.

Therefore, since all possible cases of a and b are considered and they all ended with $(x^2 - a)(x^2 - b)(x^2 - ab) \equiv 0 \pmod{p}$ having a solution for some integer x, this congruence will always have a solution for some integer x.

□

Problem 2: If p is an odd prime, prove that $(\frac{1}{p}) + (\frac{2}{p}) + ... + (\frac{p-1}{p}) = 0$

Proof. Suppose p is an odd prime. This tells us that there are exactly $\frac{p-1}{2}$ quadratic residues (mod p) and $\frac{p-1}{2}$ non-quadratic residues (mod p). In other words, an equal number of both. We can use this information to mention that there are an equal number of Legendre symbols of the forms $(\frac{a_1}{p})$, where a_1 is a quadratic residue (mod p), and $(\frac{a_2}{p})$, where a_2 is a non-quadratic residue (mod p).

We know that the Legendre symbol $(\frac{a}{p})$ for some integer a in which $a \nmid p$ is either 1 if a is a quadratic residue (mod p) or -1 if a is a non-quadratic residue (mod p). Therefore, all of the Legendre symbols will have their numeric values cancelled out, thus indicating that $(\frac{1}{p}) + (\frac{2}{p}) + ... + (\frac{p-1}{p}) = 0$.

□

Problem 3: Let p be an odd prime and let q be the smallest positive quadratic nonresidual of p. Prove that q is a prime.

Proof. Suppose p is an odd prime and q is the smallest positive quadratic nonresidual of p. For the sake of contradiction, let's suppose q is not a prime. This would indicate that q does not have exactly 2 positive divisors. Also, $q \neq 1$ because 1 is always a quadratic residual (mod p) for all p. As a result, we know that q has more than 2 positive divisors. From this, we can have $q = ab$ for some positive integers a, b, where $1 < a, b < q$.

Since we know q is a quadratic nonresidual of p, we have:

$(\frac{q}{p}) = (\frac{ab}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p}) = -1.$

This tells us that one of $(\frac{a}{p})$ or $(\frac{b}{p})$ is 1 and the other is -1, indicating that a or b is a positive quadratic nonresidual (mod p). However, this leads to a contradiction because we know that both a and b are less than q, so this would make q not the smallest positive quadratic nonresidual (mod p) as previously assumed. Thus, q must be prime.

□

Problem 4a: Evaluate $(\frac{51}{53})$

$(\frac{51}{53}) = (\frac{-2}{53}) = (\frac{-1}{53}) \cdot (\frac{2}{53}) = (-1)^{\frac{53-1}{2}} \cdot (-1)^{\frac{53^2-1}{8}} = (-1)^{26} \cdot (-1)^{351} = -1$

Note: This also tells us that $x^2 \equiv 51 \pmod{53}$ has no solution.

Problem 4b: Evaluate $(\frac{8}{101})$

$(\frac{8}{101}) = (\frac{2^2}{101}) \cdot (\frac{2}{101}) = (\frac{2}{101}) = (-1)^{\frac{101^2-1}{8}} = (-1)^{1275} = -1.$

Note: This also tells us that $x^2 \equiv 8 \pmod{101}$ has no solution.

Problem 4c: Evaluate $(\frac{19}{53})$ (Hint: Use LQR)

Since 19 and 53 are primes and not both 19 and 53 are congruent to 3 (mod 4), so by LQR, we have:
$(\frac{19}{53}) = (\frac{53}{19}) = (\frac{-4}{19}) = (\frac{-1}{19}) \cdot (\frac{2^2}{19}) = (\frac{-1}{19}) = (-1)^{\frac{19-1}{2}} = (-1)^9 = -1$

Note: This also tells us that $x^2 \equiv 19 \pmod{53}$ has no solution.