Number Theory Homework V

RDB

July 11, 2022

This is our last homework! Homework is the most important part of our class. I hope that these assignments have been enlightening and fun.

Exercise 1 How many mutually incongruent solutions do each of the following quadratic congruence equations have?

(a) $x^2 = 3 \pmod{11}$

(b) $x^2 + 2x + 1 = 0 \pmod{5}$

(c) $x^2 - x + 2 = 0 \pmod{7}$

Solution 1

(a) (3 points) The quadratic residues of 11 are $\{1, 4, 9, 5, 3\}$, giving $5^2 \equiv 3 \pmod{11}$. This means that $-5 \equiv 6 \pmod{11}$ is another solution, so there are two solutions.

By the way, note that

$$\begin{aligned}(x-5)(x-6) &= x^2 - 11x + 30 \\ &\equiv x^2 - 3 \pmod{11},\end{aligned}$$

even though these two polynomials are not literally equal.

(b) (3 points) This quadratic factors, giving $(x+1)^2 \equiv 0 \pmod{5}$. If we let $y = x + 1$, this becomes $y^2 \equiv 0 \pmod{5}$, which has the unique solution $y = 0$. Therefore $x = -1 \equiv 4 \pmod{5}$ is the unique solution.

(c) (4 points) This quadratic does not factor, but we can write

$$x^2 - x + 2 = (x - 1/2)^2 - \frac{1}{4} + 2.$$

If we multiply by 4, then we obtain

$$4(x^2 - x + 2) = (2x - 1)^2 + 7.$$

Since $\gcd(4, 11) = 7$, our equation is equivalent to

$$(2x - 1)^2 + 7 \equiv 0 \pmod{7},$$

or

$$(2x - 1)^2 \equiv 0 \pmod{7}.$$

This has a unique solution, namely the x such that $2x \equiv 1 \pmod{7}$, which is $x = 4$.

Exercise 2 Prove or provide a counterexample to the following statement: If n is composite, then $\gcd(n, \phi(n)) > 1$.

Solution 2
(10 points) The smallest counterexample is $n = 15$, since $\phi(15) = 8$ and $\gcd(15, 8) = 1$.

Numbers n such that $\gcd(n, \phi(n)) = 1$ are called *cyclic*. It turns out that n is cyclic iff it is the product of distinct primes $p_1 p_2 \cdots p_r$ where no p_i divides any $p_j - 1$. For example, $n = 2 \cdot 3$ is *not* cyclic, because 2 divides $3 - 1$, but $n = 3 \cdot 5$ *is*, because 3 does not divide $5 - 1$ and 5 does not divide $3 - 1$.

Exercise 3 Using the law of quadratic residues, determine the value of $\left(\frac{5}{p}\right)$ for an odd prime $p \neq 5$. [Hint: Your answer will probably be of the form, "if $p \equiv X \pmod{Y}$, then $\ldots$, otherwise, $\ldots$"]

Solution 3
(10 points) Note that $5 \equiv 1 \pmod{4}$, so quadratic reciprocity states that

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$$

for any odd prime $p \neq 5$. The quadratic residues of 5 are 1 and 4, so

$$\left(\frac{5}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1, 4 \pmod{5} \\ -1, & \text{if } p \equiv 2, 3 \pmod{5} \\ 0, & \text{if } p \equiv 0 \pmod{5} \end{cases}$$

Exercise 4

(a) Is 11 a quadratic residue mod 863?

(b) Is 3 a quadratic residue mod 1223?

(c) Is 5 a quadratic resiude mod 11027?

Solution 4

(a) (3 points) Since $11 \equiv 863 \equiv 3 \pmod 4$, quadratic reciprocity states that

$$\left(\frac{11}{863}\right) = -\left(\frac{863}{11}\right).$$

Since $863 \equiv 5 \pmod{11}$,

$$\left(\frac{863}{11}\right) = \left(\frac{5}{11}\right),$$

and 5 is a quadratic residue mod 11. It follows that 11 is *not* a quadratic residue mod 863.

(b) (3 points) Since $3 \equiv 1223 \equiv 3 \pmod 4$, quadratic reciprocity states that

$$\begin{aligned}\left(\frac{3}{1223}\right) &= -\left(\frac{1223}{3}\right)\\ &= -\left(\frac{2}{3}\right)\\ &= 1.\end{aligned}$$

Therefore 3 is a quadratic residue mod 1223.

(c) (4 points) Since $5 \equiv 1 \pmod 4$, quadratic reciprocity states that

$$\begin{aligned}\left(\frac{5}{11027}\right) &= \left(\frac{11027}{5}\right)\\ &= \left(\frac{2}{5}\right)\\ &= -1.\end{aligned}$$

Therefore 5 is not a quadratic residue mod 11027.

Exercise 5

(**a**) How many quadratic residues of 11 are in the interval $[1, 11/2)$?

(**b**) How many quadratic residues of 13 are in the interval $[1, 13/2)$?

(**c**) How many quadratic residues of 27 are in the interval $[1, 27/2)$?

(**d**) Suppose that $p = 4k+1$ is prime. Show that x is a quadratic residue of p iff $p-x$ is. What does this imply about the number of quadratic residues in the interval $[1, p/2)$?

Solution 5

(**a**) There are 5: $1, 3, 4, 5$

(**b**) There are 3: $1, 3, 4$

(**c**) There are 6 (or 7): $1, 4, 7, 9, 10, 13$ (possibly including 0)

(**d**) Correction: This should have read $p - x$, not $x - p$.