M328K: Homework 7

Katherine Ho

October 30, 2024

1. Determine whether the following quadratic congruences are solvable:

   (a) $x^2 \equiv 219 \pmod{419}$

   Proof. The quadratic congruence is solvable if

$$\left(\frac{219}{419}\right) = 1$$

$$\left(\frac{219}{419}\right) = \left(\frac{3 \cdot 73}{419}\right) = \left(\frac{3}{419}\right)\left(\frac{73}{419}\right)$$

Since $3 \equiv 3 \pmod 4$ and $419 \equiv 3 \pmod 4$,

$$\left(\frac{3}{419}\right) = -\left(\frac{419}{3}\right) = -\left(\frac{2}{3}\right)$$

$$\implies 3 \equiv 3 \pmod 8 \to \left(\frac{2}{3}\right) = -1$$

$$= -(-1) = 1$$

Since $73 \not\equiv 3 \pmod 4$,

$$\left(\frac{73}{419}\right) = \left(\frac{419}{73}\right) = \left(\frac{54}{73}\right) = \left(\frac{3}{73}\right)\left(\frac{18}{73}\right)$$

$$= \left(\frac{3}{73}\right)\left(\frac{3}{73}\right)\left(\frac{3}{73}\right)\left(\frac{2}{73}\right)$$

$$\implies \left(\frac{3}{73}\right) = \left(\frac{73}{3}\right) = \left(\frac{1}{3}\right) = 1$$

$$\implies \left(\frac{2}{73}\right) = \left(\frac{73}{2}\right) = \left(\frac{1}{2}\right) = 1$$

$$= 1$$

$$\left(\frac{219}{419}\right) = (1)(1) = 1$$

The quadratic congruence is solvable. □

(b) $3x^2 + 6x + 5 \equiv 0 \pmod{89}$

Proof. First, we can use algebra to modify the left expression.

$$\begin{aligned} 3x^2 + 6x + 5 &\equiv 0 \pmod{89} \\ 3(x^2 + 2x + 1) + 2 &\equiv 0 \pmod{89} \\ 3(x+1)^2 &\equiv -2 \pmod{89} \\ 90(x+1)^2 &\equiv -60 \pmod{89} \\ (x+1)^2 &\equiv 29 \pmod{89} \end{aligned}$$

The congruence is solvable if $\left(\frac{29}{89}\right) = 1$.

$$\begin{aligned} \left(\frac{29}{89}\right) &= \left(\frac{89}{29}\right) = \left(\frac{2}{29}\right) \\ &\implies 29 \equiv 5 \pmod{8} \to \left(\frac{2}{29}\right) = -1 \\ &= -1 \end{aligned}$$

The congruence is not solvable. □

(c) $2x^2 + 5x - 9 \equiv 9 \pmod{101}$

Proof. First, we can use algebra to modify the left expression.

$$\begin{aligned} 2x^2 + 5x - 18 &\equiv 0 \pmod{101} \\ 16x^2 + 40x - 144 &\equiv 0 \pmod{101} \\ 16x^2 + 40x + 25 - 25 - 144 &\equiv 0 \pmod{101} \\ (4x+5)^2 &\equiv 169 \pmod{101} \\ (4x+5)^2 &\equiv 68 \pmod{101} \end{aligned}$$

The congruence is solvable if $\left(\frac{68}{101}\right) = 1$.

$$\begin{aligned} \left(\frac{68}{101}\right) &= \left(\frac{4}{101}\right)\left(\frac{17}{101}\right) \\ \left(\frac{4}{101}\right) &= \left(\frac{2^2}{101}\right) = \left(\frac{1}{101}\right) = 1 \\ \left(\frac{17}{101}\right) &= \left(\frac{101}{17}\right) = \left(\frac{16}{17}\right) = \left(\frac{2^4}{17}\right) = \left(\frac{1}{17}\right) = 1 \\ \left(\frac{68}{101}\right) &= (1)(1) = 1 \end{aligned}$$

The congruence is solvable. □

2. Let g be a primitive root of an odd prime p. Show that the quadratic residues and quadratic nonresidues of p are (modulo p) precisely the even powers and odd powers of g, respectively. In particular, p has the same number $(p-1)/2$ of quadratic residues and quadratic nonresidues.

Proof. We say that a is a quadratic residue of p if the congruence $x^2 \equiv a \pmod{p}$ has a solution. Let $x = g^n$, ie. power of g.
Then, the quadratic residues are of the form

$$(g^n)^2 = g^{2n}$$

We can see that the quadratic residues are the even powers of g. And so the non residues must be the odd powers of g.

□

3. Let p be an odd prime and let M be the product of the quadratic residues of p that belong to $\{1, 2, \ldots, p-1\}$. Show that M is congruent modulo p to 1 or -1 according to whether $p \equiv 3 \pmod{4}$ or $p \equiv 1 \pmod{4}$. (Hint: Use a primitive root of p.)

Proof. Every quadratic residue is of the form k^2 for $k \in \{1, \ldots, \frac{p-1}{2}\}$. The product of quadratic residues M is

$$M = \prod_{k=1}^{\frac{p-1}{2}} k^2$$

Since $k^2 \equiv (-1) \cdot k \cdot (p-k) \pmod{p}$, we have

$$\prod_{k=1}^{\frac{p-1}{2}} k^2 = (-1)^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} k \cdot \prod_{k=1}^{\frac{p-1}{2}} (p-k) = (-1)^{\frac{p-1}{2}} \cdot (p-1)! \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$

Now consider the following.

$$(-1)^{\frac{p+1}{2}} = \begin{cases} 1 & \text{if } \frac{p+1}{2} \text{ is even} \\ -1 & \text{if } \frac{p+1}{2} \text{ is odd} \end{cases}$$

$\frac{p+1}{2}$ is even for $p \equiv 3 \pmod{4}$ and $\frac{p+1}{2}$ is odd for $p \equiv 1 \pmod{4}$. So,

$$(-1)^{\frac{p+1}{2}} = \begin{cases} 1 & \text{if } p \equiv 3 \pmod{4} \\ -1 & \text{if } p \equiv 1 \pmod{4} \end{cases}$$

Thus M is congruent modulo p to 1 or -1 according to whether $p \equiv 3 \pmod{4}$ or $p \equiv 1 \pmod{4}$.

□

4. Show that $(5/p) = 1$ if and only if $p \equiv 1, 9, 11, \text{ or } 19 \pmod{20}$.

Proof. $\left(\frac{5}{p}\right) = 1$ if 5 is a quadratic residue $\pmod{p}$. So there must be an integer x where $x^2 \equiv 5 \pmod{p}$.

By the law of quadratic reciprocity,

$$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{\frac{(5-1)(p-1)}{4}} = (-1)^{\frac{4(p-1)}{4}} = (-1)^{p-1}$$

Since p is an odd prime, then $p-1$ is even and $(-1)^{p-1}=1$. So, we get

$$\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)=1$$

Since we know this, we can determine when p is a quadratic residue modulo 5, ie.

$$x^2 \equiv p \pmod 5$$

The possible values are $x=0,1,2,3,4,5$. Then the quadratic residues are $0,1,4$. So p is a quadratic residue for $p\equiv 1$ or $p\equiv 4 \pmod 5$. We exclude $p\equiv 0 \pmod 5$ since p is an odd prime. So, $\left(\frac{p}{5}\right)=1$ iff $p\equiv 1$ or $p\equiv 4 \pmod 5$.

- If $p\equiv 1 \pmod 5$, the possible values modulo 20 are $p\equiv 1,6,11,16 \pmod{20}$. Excluding non-odd numbers, we get $p\equiv 1,11 \pmod{20}$.
- If $p\equiv 4 \pmod 5$, the possible values modulo 20 are $p\equiv 4,9,14,19 \pmod{20}$. Excluding non-odd numbers, we get $p\equiv 9,19 \pmod{20}$.

Thus $\left(\frac{5}{p}\right)=1$ iff $p\equiv 1,9,11$, or $19 \pmod{20}$.

□

5. Prove that 7 is a primitive root of any prime of the form $p=2^{4n}+1$ for $n\geq 1$.

Proof. Let $p=2^{4n}+1$ be a prime. So we have $p-1=2^{4n}$. Let k be the order of $7 \pmod p$. Then $7^k\equiv 1 \pmod p$. Since k is the order, it must divide $p-1$. Therefore, k must be of the form 2^m for where $0\leq m\leq 4n$.
Suppose $k<2^{4n}$. Then k must divide $2^{4n}-1$. Therefore, $7^{2^{4n-1}}\equiv 1 \pmod p$. Then square both sides and we get $7^{2^{4n}}\equiv 1 \pmod p$ Since $p=2^{4n}+1$, we can use the fact that $a^{p-1}\equiv 1 \pmod p$:

$$7^{2^{4n}}\equiv 7^{p-1}\equiv 1 \pmod p$$

This implies that 7 is a quadratic residue $\pmod p$. However by the quadratic reciprocity law, 7 is not a quadratic residue $\pmod p$. This is a contradiction, so $k<2^{4n}$ is false. So, $k=2^{4n}=p-1$. Thus 7 is a primitive root of p where p is a prime of the form $p=2^{4n}+1$. □