18.781
PROBLEM SET 5

JOHN WANG

1. Problem 1

Problem 1.1. *Solve* $x^2 \equiv 21 \pmod{41}$ *using Tonelli's algorithm.*

Solution First, we check if $a^{(p-1)/2} = a^{20} \equiv 1 \pmod{p}$. We use repeated square to obatin the sequence $21^2 \equiv 32 \pmod{41}$, $21^4 \equiv 18 \pmod{41}$, $21^8 \equiv 37 \pmod{41}$, $21^{16} \equiv 16 \pmod{41}$. Therefore, we see that $21^{20} = 21^{16}21^4 = (18)(16) \equiv 1 \pmod{41}$. Therefore, we see that 21 is a quadratic residue modulo 41, and we continue the algorithm.

We write $p - 1 = 40 = (8)(5) = 2^3 5$. From this, we see that $t = 5$ and $s = 3$. Now, we pick a quadratic non-residue modulo 41. We find obtain a list of quadratic residues modulo 41 and pick a number, $n = 11$, which is not a part of that list. Now, we let $c = n^t = 11^5 \equiv 3 \pmod{41}$. We see that $c^{-1} = 3$ so that $r = a^t = 21^5 \equiv 9 \pmod{41}$. In the first loop, we find that $d = r^{2^{s-i-1}} = 9^{2^{3-1-1}} = 9^2 = 81 \equiv -1 \pmod{41}$. Therefore, we continue the algorithm and set $b = bc = 3$ and $r = rc^2 = (9)(3^2) \equiv -1 \pmod{41}$ and $c = c^2 = 9$. Now in the second loop, we find $d = (-1)^{2^{3-2-1}} = 1$ so that we stop the algorithm. We set $b = (3)(9) = 27$ and we return $a^{(t+1)/2}b$. This comes out to $21^{6/2}27 = 21^3 27 \equiv 29 \pmod{41}$. To get the other solution, we take $-21 \equiv 12 \pmod{41}$.

Thus, our two solutions are $x = 12, 29 \pmod{41}$. □

2. Problem 2

Problem 2.1. *Let p be a prime congruent to 2 modulo 3, and let $(a, p) = 1$. Show that the congruence $x^3 \equiv a \pmod{p}$ has the unique solution $x \equiv a^{(2p-1)/3} \pmod{p}$.*

Solution First we shall show existence. By Fermat's Little Theorem, we know that $a^{p-1} \equiv 1 \pmod{p}$ and $a^p \equiv a \pmod{p}$ if $(a, p) = 1$. Thus, we know that $a^{p-1}a^p \equiv a \pmod{p}$ by multiplying these two congruences together. This shows that $a^{2p-1} \equiv a \pmod{p}$. Now, if $3|2p-1$, then it is clear that $a^{((2p-1)/3)^3} \equiv a \pmod{p}$. However, since $p \equiv 2 \pmod{3}$, we know that $2p \equiv 1 \pmod{3}$ which is equivalent to saying that $3|2p - 1$. This shows that $x = a^{(2p-1)/3} \pmod{p}$ is a solution to the congruence $x^3 \equiv a \pmod{p}$.

To show uniqueness, we assume there exist two solutions x_1 and x_2 to the congruence. Then we know that $x_1^3 \equiv x_2^3 \equiv a \pmod{p}$. Thus, since $x_1^3 \equiv x_2^3 \pmod{p}$, and we know that x_2^{-1} exists because p is a prime, we can rewrite the expression to $(x_1x_2^{-1})^3 \equiv 1 \pmod{p}$. Now let us set $a = x_1x_2^{-1}$. We know that $a^3 \equiv 1 \pmod{p}$ and also that $a^{p-1} \equiv 1 \pmod{p}$ from Fermat's Little Theorem. This means that the order of a must divide 3 and $p - 1$. However, since p is a prime, we know that $p - 1$ is even. The only number that divides 3 and $p - 1$ is thus 1. Therefore, we know that $a^1 \equiv 1 \pmod{p}$. This implies that $x_1x_2^{-1} \equiv 1 \pmod{p}$, which can be rewritten as $x_1 \equiv x_2 \pmod{p}$. This shows uniqueness. □

3. Problem 3

Problem 3.1. *Let $f(x) = ax^2 + bx + c$ and let $D = b^2 - 4ac$ be the discriminant of this quadratic polynomial. Let p be an odd prime, such that $p \nmid a$. Show that if $p|D$ then $f(x) \equiv 0 \pmod{p}$ has exactly one solution. If $p \nmid D$ the $f(x) \equiv 0 \pmod{p}$ has either 0 or 2 solutions and if x_0 is a solution, then $f'(x_0) \not\equiv 0 \pmod{p}$.*

Solution Divididing the congruence by a yields the congruence $x^2 + (b/a)x + c/a \equiv 0 \pmod{p}$. This can be done because p is a prime. Next, we complete the square, to get the congruence $x^2 + (b/a)x + (b^2/4a^2) - (b^2/4a^2) + c/a \equiv 0 \pmod{p}$ which can be simplified to:

$$ax^2 + bx + c \equiv 0 \pmod{p} \tag{3.1}$$

$$\left(x + \frac{b}{2a}\right)^2 \equiv \frac{b^2}{4a^2} - \frac{c}{a} \pmod{p} \tag{3.2}$$

$$\left((2a)\left(x + \frac{b}{2a}\right)\right)^2 \equiv b^2 - 4ac \pmod{p} \tag{3.3}$$

Now, if $p|D$, then we know that $p|b^2 - 4ac$ by definition, which also implies that $p|((2a)(x + (b/2a)))^2$. Since $p \nmid a$, we know that $p \nmid a^2$, and also that $p \nmid 4$ if $p > 2$. Therefore, we find that $p|(x + b/2a)^2$, so that we must have:

$$\left(x + \frac{b}{2a}\right)^2 \equiv 0 \pmod{p} \tag{3.4}$$

We see that $x = -b(2a)^{-1} \pmod{p}$ is the only unique solution which solves the congruence. Since p is a prime, we know the inverse of $2a$ exists and is unique. Therefore, the case where $p|D$ has exactly one solution.

Now if $p \nmid D$, then we must solve $((2a)(x+b/2a))^2 \equiv b^2 - 4ac \pmod{p}$. Let us say that x_1 is a solution to this congruence. Then we must have $-(x_1 + b/2a) = x_2 + b/2a$ also satisfying the congruence. This implies that $x_2 = -x_1 - b/a$ will also satisfy the congruence. Thus, in the case of $p \nmid D$, we have either two solutions or zero solutions if x_1 is not a solution.

Now, we must show that if x_0 is a solution, then $f'(x_0) \not\equiv 0 \pmod{p}$. First, we rewrite the congruence $f(x) \equiv 0 \pmod{p}$ into:

$$(2ax_0 + b)^2 \equiv b^2 - 4ac \pmod{p} \tag{3.5}$$

We know that $f'(x_0) \equiv 2ax_0 + b \pmod{p}$. Thus, if $p \nmid D$, then we know that $(2ax_0 + b)^2 \not\equiv 0 \pmod{p}$ so that clearly $f'(x) \not\equiv 0 \pmod{p}$. Now if $p|D$, we know that the square root of $(2ax_0 + b)^2 \not\equiv 0 \pmod{p}$, so that $f'(x_0) = 2ax_0 + b \not\equiv 0 \pmod{p}$. This completes the proof. □

Problem 3.2. *Show that if p is an odd prime, e a natural number, and $(a,p) = 1$, then $x^2 \equiv a \pmod{p^e}$ has exactly $1 + \left(\frac{a}{p}\right)$ solutions.*

Solution First we will show that if $(a,p) = 1$, then $x^2 \equiv a \pmod{p}$ has exactly $1 + \left(\frac{a}{p}\right)$ solutions. Note that there are a maximum of 2 solutions by the previous problem. Also note thet the determinant is $D = (-4)(-a) = 4a$. First, if $p|4a$, then we know that $\left(\frac{a}{p}\right) = 0$ by definition. Moreover, from the previous problem, we know that if $p|D$, there will be exactly 1 solution, so $1 + \left(\frac{a}{p}\right)$ correctly gives the number of solutions in this case.

Now, if $p \nmid 4a$, then $p \nmid D$ so there are either 0 or 2 solutions by the previous problem's results. Thus, we have $\left(\frac{a}{p}\right) = \pm 1$. If $\left(\frac{a}{p}\right) = 1$, then there is at least one solution, so there must be two solutions to $x^2 \equiv a \pmod{p}$. This means that $1 + \left(\frac{a}{p}\right) = 2$ gives the correct number of solutions. If $\left(\frac{a}{p}\right) = -1$, then there are no solutions to $x^2 \equiv a \pmod{p}$, and $1 + \left(\frac{a}{p}\right) = 0$ also gives the correct number of solutions.

Now, since we have shown that $1 + \left(\frac{a}{p}\right)$ is the number of solutions to $x^2 \equiv a \pmod{p}$, we can use Hansel's lemma to lift the solutions to $x^2 \equiv a \pmod{p^e}$. Since we know that $f'(x_0) \not\equiv 0 \pmod{p}$ for each solution x_0 to $f(x_0) \equiv 0 \pmod{p}$, the conditions for Hansel's lemma are satisfied. Since Hansel's lemma shows that there is a unique $t \pmod{p}$ such that $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$, we know there are exactly $1 + \left(\frac{a}{p}\right)$ solutions to the equation $f(x) \equiv 0 \pmod{p^e}$. This completes the proof. □

4. Problem 4

Which of the following congruences have solutions, and how many? To complete this problem, we use the following two lemmas proven in class:

Lemma 4.1. *Suppose that $m = 1, 2, 4, p^\alpha, 2p^\alpha$ where p is an odd prime. If $(a,m) = 1$ then the congreuence $x^n \equiv a \pmod{m}$ has $(n, \phi(m))$ solutions or no solutions according as $a^{\phi(m)/(n,\phi(m))}, 1 \pmod{m}$.*

Lemma 4.2. *Let $f(x)$ be a fixed polynomial with integral coefficients and for any positive integer m, let $N(m)$ denote the number of solutions of the congruence$f(x) \equiv 0 \pmod{m}$. If $m = m_1 m_2$ iwhere $(m_1, m_2) = 1$, then $N(m) = N(m_1)N(m_2)$. If $m = \prod p^\alpha$ is the canonical factorization of m, then $N(m) = \prod N(p^\alpha)$.*

These two lemmas will allow us to the determine the number of solutions the following congruences:

Problem 4.1. $x^2 \equiv -2 \pmod{118}$

Solution First, we note that $118 = 2 \cdot 59$, where both 2 and 59 are primes. Because we know this, we can now apply lemma 4.1 to determine the number of solutions to $x^2 \equiv -2 \pmod{59}$ and $x^2 \equiv -2 \pmod{2}$. We know that $\phi(59) = 58$ because it is a prime. Moreover, $\phi(59)/(2, \phi(59)) = 29$ and we see that $(-2)^{29} \equiv 1 \pmod{58}$. This means there are 2 solutions to the congruence $x^2 \equiv -2 \pmod{59}$. Next, we see from inspection that $x = 0$ is the only solution to $x^2 \equiv -2 \pmod{2}$. The total number of solution of $x^2 \equiv -2 \pmod{118}$ is therefore $2 \cdot 1 = 2$. □

Problem 4.2. $x^2 \equiv -1 \pmod{244}$.

Solution We note that $244 = 4 \cdot 61$. We now want to determine the number of solutions to $x^2 \equiv -1 \pmod 4$ and $x^2 \equiv -1 \pmod{61}$. However, we see that $x^2 \equiv -1 \pmod 4$ has no solutions because $x = 0, 1, 2, 3$ do not work. This means there are no solutions to $x^2 \equiv -1 \pmod 4$, and thus that there are no solutions to $x^2 \equiv -1 \pmod{244}$. $\square$

Problem 4.3. $x^2 \equiv -1 \pmod{365}$.

Solution We see that $365 = 5 \cdot 73$. Thus, we need to determine the number of solutions of $x^2 \equiv -1 \pmod 5$ and $x^2 \equiv -1 \pmod{73}$. First, we note that the number of solutions to $x^2 \equiv -1 \pmod 5$ is given by $1 + \left(\frac{4}{5}\right)$ due to a lemma from class, which can be rewritten $1 + \left(\frac{2^2}{5}\right) = 2$. Next, we note that $\left(\frac{-1}{73}\right) = 1$ because $73 \equiv 1 \pmod 4$ so that $x^2 = -1 \pmod{73}$ has $1 + \left(\frac{-1}{73}\right) = 2$ solutions. Thus, we see that $x^2 \equiv -1 \pmod{365}$ has $2 \cdot 2 = 4$ solutions. $\square$

Problem 4.4. $x^2 \equiv 7 \pmod{227}$.

Solution We note that 227 is a prime number, so the number of solutions of the congruence is $1 + \left(\frac{7}{227}\right)$. This means, we simply need to evaluate $\left(\frac{7}{227}\right) = \left(\frac{227}{7}\right)$ using quadratic reciprocity because $227 \equiv 3 \pmod 4$. and $7 \equiv 3 \pmod 4$. This simplifies to $\left(\frac{227}{7}\right) = \left(\frac{3}{7}\right) = \left(\frac{7}{3}\right)$, again by quadratic reciprocity. Since $\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1$, we have shown that $x^2 \equiv 7 \pmod{227}$ has 2 solutions. $\square$

Problem 4.5. $x^2 \equiv 267 \pmod{789}$.

Solution We see that the prime factorization of 789 is $789 = 3 \cdot 263$. Thus, we need to check the number of solutions to $x^2 \equiv 267 \pmod 3$ and $x^2 \equiv 267 \pmod{263}$. These congruences simplify to $x^2 \equiv 0 \pmod 3$ and $x^2 \equiv 14 \pmod{263}$ respectively. Clearly, $x^2 \equiv 0 \pmod 3$ has 2 solutions because $\left(\frac{0}{3}\right) = 1$. However, we know that $\phi(263)/(2, \phi(263)) = 262/2 = 131$ and that $14^{131} \equiv -1 \pmod{263}$. This means that $x^2 \equiv 14 \pmod{263}$ has no solutions. This implies that $x^2 \equiv 267 \pmod{789}$ also has no solutions. $\square$

5. Problem 5

Problem 5.1. *Show that for all primes p, the congruence $x^8 \equiv 16 \pmod p$ has a solution.*

Solution First, we note that if $p = 2$, we can choose $x \equiv 0 \pmod 2$, which will solve the congruence. Thus, we can prove the statement for odd primes p. We know from a theorem in class that if p is a prime and $(a, p) = 1$, then $x^n \equiv a \pmod p$ has $(n, p-1)$ solutions if and only if $a^{(p-1)/(n,p-1)} \equiv 1 \pmod p$. First, we know that $(16, p) = 1$ for all primes p. Thus, we only have to evaluate $16^{(p-1)/(n,p-1)} \pmod p$. We see that $(8, p-1)$ can only take on values $2, 4, 8$ since p is an odd prime, so $p - 1$ is even.

If $(8, p-1) = 2$, then we see that $16^{(p-1)/2} = 8^{p-1} \equiv 1 \pmod p$ by Fermat's Little Theorem. If $(8, p-1) = 4$, then $16^{(p-1)/4} = 2^{(p-1)} \equiv 1 \pmod p$ also by Fermat. If $(8, p-1) = 8$, then $16^{(p-1)/8} = 2^{(p-1)/2}$. Using the definition of quadratic residues, we see that $2^{(p-1)/2} = \left(\frac{2}{p}\right)$. Since $(8, p-1) = 8$ implies that $p-1 \equiv 0 \pmod 8$, we see that $\left(\frac{2}{p}\right) = 1$ by a lemma proven in class. This completes the proof. $\square$

6. Problem 6

Problem 6.1. *Prove that there are infinitely many primes of the form $8k + 7$.*

Solution Suppose the contrary. Then there exists a finite set of primes $p_1, p_2, \ldots, p_m$ which are the only primes satisfying $p \equiv 7 \pmod 8$. Now let us construct the number $N = (4p_1p_2 \ldots p_m)^2 - 2$. Note that N is even so it must have a prime factor since it is greater than 2. Let us find an odd prime factor q. Then by construction, we know that 2 is a quadratic residue modulo q. However, we see that $\left(\frac{2}{q}\right) = 1$ implies that $q = \pm 1 \pmod 8$ by a lemma shown in class. If we assume that none of the prime factors of N have the form $8k + 7$, then they must all be of the form $8k + 1$. However, this implies that $N = (8k + 1)(8k + 1) = 64k^2 + 16k + 1 = 8(8k^2 + 2k) + 1 = 8k' + 1$, which is a contradiction since $N = 8k + 6$. This means that some prime factor of N is congruent to $7 \pmod 8$. However, this means that q is not in the list $p_1, p_2, \ldots, p_m$ because $q | N$ but $p_i \nmid N$. This is a contradiction, and thus, there must be infinitely many primes of the form $8k + 7$. $\square$

7. Problem 7

Problem 7.1. *Determine by congruence conditions the set of primes p such that $\left(\frac{10}{p}\right) = 1$.*

Solution First, the properties of the Jacobi symbol allow us to factor $\left(\frac{10}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{2}{p}\right)$. By a lemma from class, we know the following:

$$\left(\frac{2}{p}\right) = \begin{cases} -1 & \text{if } p \equiv \pm 3 \pmod 8 \\ 1 & \text{if } p \equiv \pm 1 \pmod 8 \end{cases} \tag{7.1}$$

In order to evaluate $\left(\frac{5}{p}\right)$, we note that $5 \equiv 1 \pmod 4$ which means we can use quadratic reciprocity to find that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. We know that half of the reduced residue system modulo 5 will be quadratic residues. First, we know that $\left(\frac{-1}{5}\right) = 1$ by a lemma shown in class and trivially that $\left(\frac{1}{5}\right) = 1$. We know that $\left(\frac{2}{5}\right) = -1$ because $5 \equiv -3 \pmod 8$. Finally, we know that $\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$. Therefore, we find:

$$\left(\frac{p}{5}\right) = \begin{cases} -1 & \text{if } p \equiv \pm 2 \pmod 5 \\ 1 & \text{if } p \equiv \pm 1 \pmod 5 \end{cases} \tag{7.2}$$

Using the Chinese Remainder Theorem, we can then solve for all p such that $\left(\frac{5}{p}\right)\left(\frac{2}{p}\right) = 1$. This occurs if $p \equiv \pm 1 \pmod 8, p \equiv \pm 1 \pmod 5$ or when $p \equiv \pm 3 \pmod 8, p \equiv \pm 2 \pmod 5$. The Chinese Remainder Theorem says there is a unique solution to each of the systems of congruences modulo 40. The system $p \equiv 1 \pmod 8, p \equiv 1 \pmod 5$ has a solution $p \equiv -9 \pmod{40}$. The system $p \equiv 1 \pmod 8, p \equiv -1 \pmod 5$ gives the solution $-1 \pmod{40}$. Continuing in this manner, we find the following characterization of all primes p such that $\left(\frac{10}{p}\right) = 1$:

$$p = \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40} \tag{7.3}$$

□

8. Problem 8

Problem 8.1. *Determine, by congruence conditions, the set of primes p such that -3 is a quadratic residue mod p.*

Solution We need to determine the primes p such that $\left(\frac{-3}{p}\right) = 1$. We use the properties of Legendre symbols to symplify this expression:

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \tag{8.1}$$

$$= \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)c \tag{8.2}$$

Where c is a constant depending on p. From the lemma proven in class, we know the following:

$$\left(\frac{-1}{p}\right) = \begin{cases} -1 & \text{if } p \equiv 3 \pmod 4 \\ 1 & \text{if } p \equiv 1 \pmod 4 \end{cases} \tag{8.3}$$

From quadratic reciprocity, we know that c is given by:

$$c = \begin{cases} -1 & \text{if } p \equiv 3 \pmod 4 \\ 1 & \text{if } p \equiv 1 \pmod 4 \end{cases} \tag{8.4}$$

Thus, if $p \equiv 3 \pmod 4$, then $\left(\frac{-1}{p}\right) = -1$ and $c = -1$, so that $\left(\frac{-1}{p}\right)c = 1$. If $p \equiv 1 \pmod 4$, we see that $\left(\frac{-1}{p}\right)c = (1)(1) = 1$. This, we see that $\left(\frac{-1}{p}\right)c = 1$ in all cases. Therefore, we can further simplify out expression to:

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) \tag{8.5}$$

Since $\left(\frac{p}{3}\right)$ simplifies to $\left(\frac{k}{3}\right)$ where $k \equiv p \pmod 3$, we see that we can break expression down to evaluate $\left(\frac{0}{3}\right)$, $\left(\frac{1}{3}\right)$, and $\left(\frac{2}{3}\right)$. Since $\left(\frac{0}{3}\right) = 0$, we ignore it. We see that $\left(\frac{1}{3}\right) = 1$ and $\left(\frac{2}{3}\right) = \left(\frac{-1}{3}\right) = -1$ by the lemma proven in class. Therefore, we have:

$$\left(\frac{-3}{p}\right) = \begin{cases} -1 & \text{if } p \equiv -1 \pmod 3 \\ 1 & \text{if } p \equiv 1 \pmod 3 \end{cases} \tag{8.6}$$

□

Problem 8.2. *Prove that there are infinitely many primes of the form of each of the forms $3k+1$ and $3k-1$.*

Solution Suppose by contradiction, that there exists a finite set $S = \{k_1, k_2, \ldots, k_n\}$ for which $3k_i + 1$ and $3k_i - 1$ are both primes for any $i \in \{1, 2, \ldots, n\}$. Let k_n be the largest k_n possible where $3k_n + 1$ and $3k_n - 1$ are both prime. Let $P = \{p_1, p_2, \ldots, p_m\}$ be the set consisting of all primes of the form $3k+1$ less than or equal to $3k_n + 1$ and $Q = \{q_1, q_2, \ldots, q_r\}$ be the set consist of all primes of the form $3k-1$ less than or equal to $3k_n + 1$. Now, we shall construct the number $N = (q_1 q_2 \ldots q_r p_1 p_2 \ldots p_m)^2 + 3$. Since we know that $q_i \equiv -1 \pmod 3$, we know that $q_i^2 \equiv 1 \pmod 3$. We also know that $p_i \equiv 1 \pmod 3$ so that $p_i^2 \equiv 1 \pmod 3$. This means that $(q_1 q_2 \ldots q_r p_1 p_2 \ldots p_m)^2 \equiv 1 \pmod 3$, implying that $N \equiv 1 \pmod 3$. This also implies that $N - 2 = (q_1 q_2 \ldots q_r p_1 p_2 \ldots p_m)^2 + 1 \equiv -1 \pmod 3$.

However, we see that N must be prime. This is because any prime s which divides N would have the following congruence: $(q_1 q_2 \ldots q_r p_1 p_2 \ldots p_m)^2 \equiv -3 \pmod s$. By the previous problem, we see that $s \equiv 1 \pmod 3$. However, since $p_1, p_2, \ldots, p_m$ consist of all the primes of this form, none of them can possibly divide $(q_1 q_2 \ldots q_r p_1 p_2 \ldots p_m)^2 + 1$. Therefore, we see that N does not have any prime factors, and is thus a prime.

Moreover, we see that $N - 2$ must be prime. This is because there does not exist any prime s for which $s | (q_1 q_2 \ldots q_r p_1 p_2 \ldots p_m)^2 + 1$, since this is equivalent to $(q_1 q_2 \ldots q_r p_1 p_2 \ldots p_m)^2 \equiv -1 \pmod s$. This follows because the only primes s for which this congruence is solvable are primes of the form $4k+1$. Since the union $P \cup Q$ consists of all primes less than $3k_n + 1$, s cannot belong to the set $P \cup Q$ which implies that s cannot be a prime. Since $N - 2$ does not have any prime factors, it must be a prime.

We have therefore found a new pair N and $N-2$ which have the forms $3k+1$ and $3k-1$ which are prime, and which do not belong to the lists P and Q respectively. This is a contradiction. □

9. Problem 9

Problem 9.1. *Let p be an odd prime, and let $(k, p) = 1$. Show that the number of solutions (x, y) to $y^2 \equiv x^2 + k \pmod p$ is exactly $p - 1$.*

Solution We know that the congruence $y^2 \equiv x^2 + k \pmod p$ can be rewritten as $y^2 - x^2 \equiv k \pmod p$. Factoring out the left hand side, we obtain $(y - x)(y + x) \equiv k \pmod p$. Now we can set new variables $z = x + y$ and $w = x - y$ so that we obtain the congruence $zw \equiv k \pmod p$. Thus, there exists a bijection between the solutions of the congruence $y^2 \equiv x^2 + k \pmod p$ and the congruence $zw \equiv k \pmod p$.

Now, let us fix z and find the number of solutions w to $zw \equiv k \pmod p$ is simply $gcd(z, p)$ if $gcd(z, p) | k$ and 0 otherwise. Notice that if $z \neq p$, then $gcd(z, p) = 1$ because p is a prime. Moreover, it is clear that $1 | k$. However, if $z = p$, then $gcd(z, p) = p \nmid k$. This implies that when $z = p$, there are no solutions. This means that the total number of solutions is $\sum_{z=1}^{p-1} gcd(z, p)$ since we must exclude $gcd(p, p)$ from the solutions. Since $gcd(z, p) = 1$ for $x \in \{1, 2, \ldots, p-1\}$, we see that this sum is equal to $p - 1$. Thus, the congruence has $p - 1$ solutions. □

Problem 9.2. *Show that $\sum_{x=1}^{p} \left(\frac{x^2+k}{p}\right) = -1$.*

Solution We know that the number of solutions to the congruence $y^2 \equiv x^2 + k \pmod p$ given a fixed x is $1 + \left(\frac{x^2+k}{p}\right)$ by a lemma shown in class. Thus, the total number of solutions to $y^2 \equiv x^2 + k \pmod p$ is given by the expression:

$$\sum_{x=1}^{p} 1 + \left(\frac{x^2+k}{p}\right) = p + \sum_{x=1}^{p} \left(\frac{x^2+k}{p}\right) \tag{9.1}$$

However, we know from the previous problem that the number of solutions to the congruence is $p - 1$. This implies that $\sum_{x=1}^{p} \left(\frac{x^2+k}{p}\right) = -1$. □

Problem 9.3. *Now let $(ab, p) = 1$, show that the number of solutions to the congruence $ax^2 + by^2 \equiv 1 \pmod p$ is $p - \left(\frac{-ab}{p}\right)$.*

Solution We know that $ax^2 + by^2 \equiv 1 \pmod p$ can be rewritten as $by^2 \equiv 1 - ax^2 \pmod p$. Moreover, since p is a prime, we know that b^{-1} exists, so we can write $y^2 \equiv b^{-1}(1 - ax^2) \pmod p$. From a lemma proven in class, we know that the number of solutions to this congruence, holding x fixed, is simply $1 + \left(\frac{b^{-1}(1-ax^2)}{p}\right)$. Thus, the total number of solutions to the congruence is the sum of this expression, ranging over all possible

x values. This can be written:

$$\sum_{x=1}^{p} 1+\left(\frac{b^{-1}(1-ax^2)}{p}\right) = p+\sum_{x=1}^{p}\left(\frac{b^{-1}}{p}\right)\left(\frac{1-ax^2}{p}\right) \tag{9.2}$$

$$= p+\sum_{x=1}^{p}\left(\frac{b}{p}\right)\left(\frac{1-ax^2}{p}\right) \tag{9.3}$$

$$= p+\sum_{x=1}^{p}\left(\frac{b-bax^2}{p}\right) \tag{9.4}$$

$$= p+\sum_{x=1}^{p}\left(\frac{-ab}{p}\right)\left(\frac{x^2-a^{-1}}{p}\right) \tag{9.5}$$

$$= p+(-1)\left(\frac{-ab}{p}\right) \tag{9.6}$$

Which is what we wanted to prove. Note that the second step from above comes about because $\left(\frac{b}{p}\right)^{-1} = \left(\frac{b}{p}\right)$. We also know that a^{-1} exists because p is a prime. The final step uses the result from the previous problem that $\sum_{x=1}^{p}\left(\frac{x^2+k}{p}\right) = -1$, where in this case $k=-a^{-1}$. $\square$

10. Problem 10

Problem 10.1. *Write a gp program to calculate the number of quadratic residues R and quadratic non-residues N in the set $\{1,2,\dots,(p-1)/2\}$ for any given odd prime p. Tabulate the results for the first 100 odd primes. What do you observe?*

Solution The program to tabulate the number of quadratic residues and non residues in the set $\{1,2,\dots,(p-1)/2\}$ for the first 100 odd primes is given below:

```
printQR(p)=
{
    QR = 0;
    QNR = 0;
    for(a=1, (p-1)/2,
        if(kronecker(a,p) == 1, QR++);
        if(kronecker(a,p) == -1, QNR++);
    );
    print("Prime " p " R: " QR " N: " QNR);
}

{
    plist = primes(101);
    for(i=2, 101,
         printQR(plist[i])
    );

}
```

We observe that when $p \equiv 1 \pmod 4$, the number of quadratic residues and non-residues is the same. When $p \equiv 3 \pmod 4$, there are more quadratic residues than non-residues in the set. $\square$