Homework 5, Math 4150

1. Exercise Set 4.1, #5. Find all incongruent solutions of each quadratic congruence below.

   (a) $x^2 \equiv 23 \pmod{77}$

   [Hint: Consider the congruences $x^2 \equiv 23 \pmod 7$ and $x^2 \equiv 23 \pmod{11}$ and use the Chinese Remainder Theorem].

   Solution. We have $x^2 \equiv 23 \pmod{11}$ and $x^2 \equiv 23 \pmod 7$ we can reduce both of them to,

   $$x^2 \equiv 2 \pmod 7$$
   $$x^2 \equiv 1 \pmod{11}$$

   For numbers equiv 1 modulo 11 we know these are 1 and $11 - 1$ so we have x is either $1, 11$. And modulo 7, we know there are either 0 or 2 solutions and listing out we get $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 2$. So 3 is a solution which means that $p - 3 = 4$ is the only other solution.

   Now using CRT we have $m_1 = 7, m_2 = 11$ and finding inverses to $11y_1 \equiv 1 \pmod 7$ and $7y_2 \equiv 1 \pmod{11}$. We have $11 \cdot 2 - 7 \cdot 3 = 1$ so the inverses are 2 and -3 which gives us,

   $$x = a \cdot 11 \cdot 2 + b \cdot 7 \cdot -3 \pmod{77}$$

   Now our various options are $a = 3, 4$ and $b = 1, -1$ plugging in we get,

   $$x = 45, 10, 67, 32 \pmod{77}$$

   (b) $x^2 \equiv 11 \pmod{39}$

   We can divide this into two congruencies $x^2 \equiv 11 \equiv 2 \pmod 3$ and $x^2 \equiv 11 \pmod{13}$. The first congruency we don't have a solution. So there isn't a solution to this problem.

   (c) $x^2 \equiv 46 \pmod{105}$

   We have $x^2 \equiv 46 \equiv 1 \pmod 5$, $x^2 \equiv 46 \equiv 4 \pmod 7$ and $x^2 \equiv 46 \equiv 1 \pmod 3$.

   We have $1, -1$ for the first one $2, 5$ for the second and $1, -1$ for the third. Now we have $M = 105$ so $m_1 = 35, m_2 = 21, m_3 = 15$. Our system of congruence ids $21y_1 \equiv a \pmod 5, 15y_2 \equiv b \pmod 7, 35y_3 \equiv c \pmod 3$ solutions to which are $1, 1, -1$. So our final solution would be,

   $$x \equiv a(21)(1) + b(15)(1) + c(35)(-1) \pmod{105}$$

   Plugging in all combinations we get,

   $$x \equiv 16, 86, 79, 44, 26, 89, 61, 19 \pmod{105}$$

Blank page:

2. Exercise Set 4.1, #6. Let p be an odd prime number. Prove that the $\frac{p-1}{2}$ quadratic residues modulo p are congruent to

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2,$$

modulo p.

Solution. $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ consist of $\frac{p-1}{2}$ unique square numbers so they are all quadratic residues. So it is enough to show that these residues are unique mod p. First assume that they are not unique so we have for some $a, b < \frac{p-1}{2}$ that $a^2 \equiv b^2 \pmod{p}$. So we have $p \mid a^2 - b^2$ or $p \mid (a+b)(a-b)$. This means that either $p \mid a+b$ or $p \mid a-b$. If its the latter then we have $a = b$ as $|a-b|$ can't exceed $p-1$ so it cannot be a multiple of p leaving only 0 as a choice. . If its the former then as $1 \leq a, b \leq \frac{p-1}{2}$ so $2 \leq a+b \leq p-1$ and p can't divide $p-1$. Hence we get $a = b$. So we show that in our set of $\frac{p-1}{2}$ squares of residues, all of them have to be distinct which means that all of the $\frac{p-1}{2}$ quadratic residues are congruent to the above list of squares.

3. Exercise Set 4.1, #7.
Note: In this question you are allowed to use the standard formulae for $\sum_{j=1}^{n} j^2$ and $\sum_{j=1}^{n} j^4$ without proof.

(a) Let p be a prime number with $p > 3$. Prove that the sum of the quadratic residues modulo p is divisible by p.

Solution. We have $\sum_j j^2 = \frac{n(n+1)(2n+1)}{6}$. We know the sum of the residues are $\sum_j^{\frac{p-1}{2}}$ so we have the sum as,

$$\frac{1}{6}\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)(p)$$

Now we know that this is an integer (as the formula returns an integer always). Now as p is a prime we know that 6 cannot divides p so that means that 6 divides either of the other two. So it's possible to write this as pk where $k = \frac{1}{6}\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)$ is an integer.

(b) Let p be a prime number with $p > 5$. Prove that the sum of the squares of the quadratic non-residues modulo p is divisible by p.

Solution. We know all the residues and non residues are $1, \ldots, p-1$. Out of this $1^2, \ldots, \frac{p-1}{2}^2$ are the quadratic residues. Now $\sum^{p-1} i^2$ is the sum of squares of all residues and non residues. And we need to subtract away the squares of residues. We know the residues themselves are $1^2 \ldots, \frac{(p-1)}{2}^2$, so squares of these would be $1^4, \ldots, \frac{p-1}{2}^4$. So first we have,

$$\sum_{i}^{p-1} i^2 = \frac{1}{6}(p-1)(p)(2p-1)$$

And we have,

$$\sum_{i}^{k} j^4 = (k)(k+1)(2k+1)(3k^2+3k-1)\frac{1}{30}$$
$$\sum_{i}^{\frac{p-1}{2}} j^4 = \frac{p-1}{2}\frac{p+1}{2}p...$$

We already see that p is a factor in this, so we have p divides both the sums which means p also divides $\sum_i^{p-1} i^2 - \sum_i^{\frac{p-1}{2}} j^4$ which is equivalent to the sum of squares of quadratic non-residues.

Blank page:

Blank page:

4. Exercise Set 4.2, #22. Let p be a prime number with $p \equiv 1 \pmod 4$. Prove that

$$\sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right) = 0.$$

Solution. We know from Eulers criterion that,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

Now $p \equiv 1 \pmod 4$ so we have $p = 4k + 1$ for some $k \in$ so we have $a^{\frac{p-1}{2}} = a^{2k} = (a^2)^k$. Now note that $1^2, \ldots, \frac{(p-1)}{2}^2$ gets us all the residues. And also note that given a residues a i.e. $x^2 \equiv a \pmod p$ then we have $x^4 \equiv a^2 \pmod p$ or $(x^2)^2 \equiv a^2 \pmod p$ or in other words the power of a residue is also a residue. Hence we have a^{2k} is also a residue for all $a \in [0, \frac{p-1}{2}]$. Now we need to show that these residues are unique.We have the following,

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) \equiv \sum_{a}^{(p-1)/2} a^{(p-1)/2} \equiv \sum_{a}^{\frac{p-1}{2}} a^{2k} \pmod p$$

Now note that given $a \neq b$ and $a, b < \frac{p-1}{2}$ we have a^{2k} and b^{2k} are distinct. So as we can write $a^{2k} = (a^k)^2$ it means that a^{2k} is a quadratic residue. Since we show that it has to be distinct we get that $\sum_a^{\frac{p-1}{2}} a^{2k}$ is just the sum of all the quadratic residues modulo p which as we showed above is equivalent to 0 modulo p. So we have $\sum_a^{(p-1)/2} \left(\frac{a}{p}\right) \equiv 0 \pmod p$. But $\left(\frac{a}{p}\right)$ can only be 1, -1. And we're summing $(p-1)/2$ of these, so they are bounded below by $\frac{-(p-1)}{2}$ and above by $\frac{p-1}{2}$. So the only possible value they can take such that they are equivalent to 0 modulo p is 0. Hence we complete the proof.

5. Exercise Set 4.2, #24.

(a) Let p be a prime number with $p \geq 7$. Prove that at least one of 2, 5, and 10 is a quadratic residue modulo p.

Solution.
We known that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Now assume 2 and 5 are not quadratic residues then we have $\left(\frac{2}{p}\right) = -1$ and $\left(\frac{5}{p}\right) = -1$. This give us $\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = -1 \cdot -1 = 1$. Hence if $2, 5$ are not residues then 10 must be a residue. Else one of $2, 5$ has to be residues. So we have shown that at least one of the three have to be residues.

(b) Could exactly two of 2, 5, and 10 be quadratic residues modulo p in part (a)? Why or why not?

No, exactly two cannot be residues modulo p. We have the following,

$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right)$$

If we have exactly two residues then exactly two of these terms are 1 and the other have to be -1. However, we see that if any two of the above are 1, then the other one has to be 1 as well. Hence we cannot have exactly two residues from the list.

(c) Let p be a prime number with $p \geq 7$. Prove that there at least two consecutive quadratic residues modulo p. [Hint: use part (a)].

Solution. We need residues such that $a^2 - b^2 = 1$ or that $(a+b)(a-b) = 1$. We need it such that $a + b = u$ and $a - b = \overline{u}$. So $2a = u + \overline{u}$ and $a = \frac{u+\overline{u}}{2}$ and $b = \frac{u-\overline{u}}{2}$ which would produce us two residues a^2 and b^2 such that $a^2 - b^2 = 1$. Now as one of $\{2, 5, 10\}$ are residues for a given p we can choose u such that u^2 is in this set. This prevent any trivial solutions (such as $0, 1$). Hence, we found a construction for two consequtive residues for primes greater than 7.

6. Exercise Set 4.2, # 26. Prove that there are infinitely many prime numbers expressible in the form $4n + 1$ where n is a positive integer.
[Hint: Assume, by way of contradiction, that there are only finitely many such prime numbers $p_1, \ldots, p_r$. Consider the positive integer $4p_1^2p_2^2 \cdots p_r^2 + 1$ and use Theorem 4.6].

Solution. Assume there are finitely many primes say $p_1, \ldots, p_r$. Now consider $N = 4p_1^2 \ldots p_r^2 + 1$. We see that $N \equiv 1 \pmod 4$. Now N is clearly in the form $4k + 1$ for some k. So any prime divisor of this must be of form $p \equiv 1 \pmod 4$. Now we have that $N = (2p_1 \ldots p_r)^2 + 1$. Let $2p_1 \ldots p_r = M$ so $M^2 \equiv -1 \pmod N$ and as p is a prime divisor of N we have $M^2 \equiv -1 \pmod p$ This means that -1 is a quadratic residue modulo p which means that $p \equiv 1 \pmod 4$. However, note that we cannot have $p \in \{p_1, \ldots, p_r\}$ as then we have $p \mid 4p_1^2 \ldots p_r^2 + 1$, but as p divides the first (if $p \in \{p_1, \ldots, p_r\}$) then we also have $p \mid 1$ which is not possible. Hence, this means we found a new prime divisor other than the finitely many ones we claimed which is of the form $4k + 1$ which is a contradiction that there are only finitely many $p_1, \ldots, p_r$. Hence, our assumption must be wrong and there are infinitely many primes of the form $4k + 1$.

7. Exercise Set 4.3, #34. Let p and q be odd prime numbers with $p = q + 4a$ for some $a \in \mathbb{Z}$. Prove that
$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Solution. First note that a is not necessarily a prime. So let us first factor it as follows,
$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)^t \left(\frac{p_1}{p}\right)^{k_1} \dots \left(\frac{p_n}{p}\right)^{k_n}$$

Now it is enough to show that $\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right)$ and for any p_k we have $\left(\frac{p_k}{p}\right) = \left(\frac{p_k}{q}\right)$.

For the first case i.e. 2 we have it's equal to $(-1)^{\frac{p^2-1}{8}}$. Now see that $(p^2-1)/8 = (q^2+16a^2+8aq-1)/8 = (q^2-1)/8 + (2a^2+aq)$ now if $t \geq 1$ this means that 2 is a factor of a and a is even meaning $2a^2+aq$ is even. So we get $(-1)^{(p^2-1)} = (-1)^{(q^2-1)/8}$ or,
$$\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right)$$

Now for the case for an arbitrary p_k. We see that $p \equiv q \pmod 4 a$ which means that for any $p_k \mid a$ we also have $p \equiv q \pmod p_k$. Now in addition as $p \equiv q \pmod 4$ we have,
$$\left(\frac{p_k}{p}\right)\left(\frac{p}{p_k}\right) = \left(\frac{p_k}{q}\right)\left(\frac{p_k}{a}\right)$$

As p, q will always share the same residue modulo 4. Now note that when looking at $\left(\frac{p}{a}\right)$ and $\left(\frac{q}{a}\right)$ we see that if p is a residue then as $p \equiv p - 4a \equiv q$ is also a residue and similarly if q is a residue then $q \equiv q + 4a \equiv p$ is also a residue. Hence either both are residues or both are non residues. In either case their value is the exactly same say k. So we have,
$$\left(\frac{p_k}{p}\right)k = \left(\frac{p_k}{q}\right)k$$

Or that $\left(\frac{p_k}{p}\right) = \left(\frac{p_k}{q}\right)$. Hence we get for any p_k that the legedre symbol is the same modulo p, q so their product must also all be the same or in other words we get,
$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$$

8. Exercise Set 4.3, #35. Let p be an odd prime number (with $p > 3$ in parts (b) and (c)). Prove the following statements.

   (a) $\left(\frac{-2}{p}\right) = 1$ if and only if $p \equiv 1, 3 \pmod 8$.

   Solution. We can write $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$. Now the product is equal to 1 if and only if either both are equal to 1 or both are equal to -1. For $\left(\frac{2}{p}\right) = 1$ we have $p \equiv 1, 7 \pmod 8$ and we have $\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1 \pmod 4$. So we have $4 \mid p-1$ and $8 \mid p-1$ or $8 \mid p-7$ to satisfy both we have $8 \mid p-1$ so $p \equiv 1 \pmod 8$.

   Now if both are equal to -1 we have $p \equiv 3 \pmod 4$ and either $p \equiv 3, 5 \pmod 8$. But $p \equiv 3 \pmod 4$ implies $p \equiv 3 \pmod 8$ so we have $p \equiv 3 \pmod 8$ as the only condition.

   So we have either $p \equiv 1, 3 \pmod 8$

   (b) $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$.

   Solution. We have $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 1 \pmod 4$ else we have $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = -1$ if and only if $p \equiv 3 \pmod 4$. Now in the first case we need $\left(\frac{p}{3}\right) = 1$. We know that p has to be a quadratic residue so we need $p \equiv 1 \pmod 3$. So we have both $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$. Using CRT we have $x \equiv 4{\cdot}1{\cdot}1 + 3{\cdot}{-1}{\cdot}1 \equiv 1 \pmod{1)2}$.

   Now in the second case we have $\left(\frac{p}{3}\right) = -1$. For this we need p to be a quadratic non-residue so we have $p \equiv 2 \pmod 3$ and $p \equiv 1 \pmod 4$. So this gives us $x \equiv 4 \cdot 1 \cdot 2 + 3 \cdot -1 \cdot 3 \equiv -1 \pmod{1)2}$

   Both the cases give us that $p \equiv \pm 1 \pmod{12}$

   (c) $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 6$.

   Solution.
   We can write $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1$
   Now this product to equal 1 we need both to be either 1 or both to be -1.

   Case 1: Both are 1. So we have $\left(\frac{-1}{p}\right) = 1$ which means that we have $p \equiv 1 \pmod 4$. And for $\left(\frac{3}{p}\right) = 1$ we see that we already have $p \equiv 1 \pmod 4$ which means that $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = 1$ so $\left(\frac{p}{3}\right) = 1$ which is true only if $p \equiv 1 \pmod 3$.

   Case 2: We have both as -1. For $\left(\frac{-1}{p}\right) = -1$ we need $p \equiv 3 \pmod 4$. Now this case implies that we have $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = -1$ so we have $\left(\frac{p}{3}\right) = 1$ or that $p \equiv 1 \pmod 3$.

Now note that in both cases we have $p \equiv 1 \pmod 3$ and cases modulo 4. But as p is an odd prime we know it can be either $1, 3$ modulo 4. SO the only condition we need to care about is $p \equiv 1 \pmod 3$. Now, modulo 6, a prime can be either 1 or 5. Between these two the first one implies 1 modulo 3. Hence we have $p \equiv 1 \pmod 6$.

Blank page: