MATH 152 Problem set 4 solutions

As usual, p, p_i, q and the like represent a prime number.

1.First we prove that 10 is a quadratic non-residue (mod p). We have

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

and none of the terms on the right side are zero because $p \geq 7$ by assumption. Let's compute each term:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1,$$

since $p \equiv 7 \pmod{40}$ implies $p \equiv 7 \pmod 8$. Also

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Here the first equality follows from quadratic reciprocity, the second from $p \equiv 7 \pmod{40}$ $\Rightarrow p \equiv 2 \pmod 5$. This shows that 10 is a quadradic non-residue (mod p).

Next we show that 10 is a primitive root (mod p), or equivalently, 10 has order $p-1$. By assumption $p - 1 = 2q$, so 10 has either order 2, q or $p-1$. But q cannot be the order of 10: since 10 is a nonresidue and q is odd 10^q is a nonresidue; in particular, $10^q \not\equiv 1 \pmod p$. Also, if 2 were the order of 10, i.e. $10^2 = 100 \equiv 1 \pmod p$, then $99 \equiv 3 \cdot 3 \cdot 11 \equiv 0 \pmod p$; this implies $p = 3$ or 11, but neither of them are 7 (mod 40), so this is impossible either. Therefore, the order of 10 (mod p) is $p-1$.

2. First suppose n is odd, and write $n = p_1 p_2 \dots p_k$ where p_i are odd primes. Our goal is to investigate for which primes p $(\frac{n}{p}) = 1$.

Case $p \equiv 1 \pmod 4$: By quadratic reciprocity, we have

$$\left(\frac{p_1 \dots p_k}{p}\right) = \left(\frac{p_1}{p}\right) \dots \left(\frac{p_k}{p}\right) = \left(\frac{p}{p_1}\right) \dots \left(\frac{p}{p_k}\right).$$

This value is 1 if and only if $(\frac{p}{p_i}) = -1$ for an even number of i's. And this holds if and only if for each $i = 1, \dots, k$ we have $p \equiv a_i \pmod{p_i}$, where a_i is never zero (mod p_i) and is a quadratic nonresidue (mod p_i) for an even number of i's. For each possible choice of a_i's, together with the relation $p \equiv 1 \pmod 4$, the Chinese remainder theorem gives the unique residue class mod $4p_1 \dots p_k = 4n$ to which p belongs.

Case $p \equiv 3 \pmod 4$: here the quadratic reciprocity gives

$$\left(\frac{p_1 \dots p_k}{p}\right) = \left(\frac{p_1}{p}\right) \dots \left(\frac{p_k}{p}\right) = (-1)^\beta \left(\frac{p}{p_1}\right) \dots \left(\frac{p}{p_k}\right)$$

(here β equals the number of p_i's that are 3 mod 4). This is 1 if and only if $(\frac{p}{p_i}) = -1$ for an even number of p_i's if β is even, and for an odd number of p_i's if β is odd. And this happens if and only if for each $i = 1, \dots, k$, $p \equiv b_i \pmod{p_i}$, where b_i is never zero (mod p_i) and is a quadratic nonresidue (mod p_i) for an even (in case β is even) or odd (in case β is odd) number of i's. Same as earlier, for each possible choice of b_i's, together with the relation $p \equiv 3 \pmod 4$, the Chinese remainder theorem determines the residue class mod $4n$ corresponding to p.

If n is even, so that $n = 2p_1 \dots p_k$ where p_i are odd primes, then we proceed the same as above (we also have to divide by the cases as to whether $p \equiv 1$ or $3 \pmod 4$), except that we will now have $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$ among the factors of $(\frac{n}{p})$. This gives an equivalence relation $p \equiv c_0 \pmod 8$ for some c_0, in addition to $p \equiv c_i \pmod{p_i}$ that we will obtain by the same method as above. Then the Chinese remainder theorem gives the corresponding residue class of p mod $8p_1 \dots p_k = 4n$.

3. (i) Pick a primitive element $g \pmod p$. By assumption g^{2d+1} has order $p-1$ for all $d = 0, 1, 2, \dots$. This means $(2d+1, p-1) = 1$ for all d, because if this does not hold for some d then g^{2d+1} will have order at most $(p-1)/(2d+1, p-1) < p-1$, a contradiction. Therefore $p-1$ is a power of 2.

(ii) Suppose $p = 2^k + 1$ is prime. We want to show that k has no odd factors. Recall the following factorization formula:

$$a^m + 1 = (a+1)(a^{m-1} - a^{m-2} + \dots - a + 1)$$

where m is an odd number. Now suppose k has an odd factor, i.e. $k = m2^n$ for an odd m. Then

$$2^k + 1 = (2^{2^n})^m + 1 = (2^{2^n} + 1)(\dots).$$

Comparing both sides makes it clear that the number in $(\dots)$ is strictly greater than 1. This shows that $2^k + 1$ is composite, a contradiction.

(iii) Pick a primitive element $g \pmod p$. Then for any $d = 0, 1, 2, \dots$, $g^{(2d+1)r} = 1$ implies $p - 1 \mid (2d+1)r$ But $p - 1 = 2^{2^n}$, so this means $p - 1 \mid r$. This shows that g^{2d+1} has order $p-1$, completing the proof.

4. Suppose $A^2 = 2$. Write $A = \sum_{i=0}^{\infty} a_i 7^i$, where a_i is between 0 and 6 inclusive. Note

that no matter what the a_i's are, we don't need to worry about A being divergent, because its Nth partial sum $\sum_{i=0}^{N} a_i 7^i$ is a Cauchy sequence in the p-adic norm.

We have $A^2 \equiv 2 \pmod 7 \Rightarrow a_0^2 \equiv 2 \pmod 7$. So we could say $a_0 = 3$. (Or we could also say $a_0 = 4$, which will give the "negative square root.")

We also have $A^2 \equiv 2 \pmod{49} \Rightarrow (a_0 + a_1 7)^2 \equiv 2 \pmod{49}$. Then $a_1 = 1$ is the only possibility (recall Exercise 3 from the previous problem set).

Similarly, $A^2 \equiv 2 \pmod{7^3 = 343} \Rightarrow (a_0 + a_1 7 + a_2 7^2)^2 \equiv 2 \pmod{343}$. $a_2 = 2$ is forced.

We can continue this process to obtain $a_3, a_4, \ldots$ and so on. In general, we will have $(\sum_{i=0}^{N} a_i 7^i)^2 \equiv 2 \pmod{7^{N+1}}$. This means that $|(\sum_{i=0}^{N} a_i 7^i)^2 - 2|_p \leq p^{-(N+1)}$, which approaches 0 as $N \to \infty$. So we see that this process will indeed give a square root of 2.

5. $D := \{x \in \mathbb{Q} : |x|_p < 1\}$ is a p-adic disc with radius 1 and center 0. Note that $x \in D \Leftrightarrow x = p^k m$, where $k \geq 1$ and $|m|_p = 1$.

A p-adic disc with radius 1 and center $p^\alpha n$, where $\alpha \geq 1$ and $|n|_p = 1$ is

$$D' = \{x \in \mathbb{Q} : |x - p^\alpha n|_p < 1\}.$$

And we have $x \in D' \Leftrightarrow x - p^\alpha n = p^k m$, where $k \geq 1$ and $|m|_p = 1$.

The question is asking us to show $D = D'$. This is clear because $x \in D \Leftrightarrow x = p^k m \Leftrightarrow x - p^\alpha n = p^k m - p^\alpha n = p^{\min(k,\alpha)} l \Leftrightarrow x \in D'$, where l here is whatever expression that makes the equality hold.

6. (a) $x^2 + 10x - 10 \equiv 0 \Leftrightarrow (x+5)^2 \equiv 35 \pmod p$. If 35 is a quadratic residue $\pmod p$, i.e. if $35 = g^{2k}$ for some primitive element g, then we have two distinct roots $x \equiv -5 \pm g^k \pmod p$.

In addition, if this equation has any solution other than $x \equiv -5$, it means 35 is a quadratic residue $\pmod p$. Therefore $n = 35$.

(b) Our goal is to find odd p's such that $(\frac{35}{p}) = 1$. First suppose $p \equiv 1 \pmod 4$. Then by quadratic reciprocity

$$\left(\frac{35}{p}\right) = \left(\frac{7}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{p}{7}\right)\left(\frac{p}{5}\right).$$

This equals 1 if and only if p is a quadratic residue mod 5 and 7, or p is a quadratic nonresidue mod 5 and 7. Therefore either $p \equiv 1, 4 \pmod 5$ and $p \equiv 1, 2, 4 \pmod 7$, or $p \equiv 2, 3 \pmod 5$ and $p \equiv 3, 5, 6 \pmod 7$.

On the other hand, if $p \equiv 3 \pmod 4$, then

$$\left(\frac{35}{p}\right) = \left(\frac{7}{p}\right)\left(\frac{5}{p}\right) = -\left(\frac{p}{7}\right)\left(\frac{p}{5}\right).$$

This equals 1 if and only if p is a residue mod 5 and nonresidue mod 7, or p is a nonresidue mod 5 and residue mod 7. Therefore either $p \equiv 1, 4 \pmod 5$ and $p \equiv 3, 5, 6 \pmod 7$, or $p \equiv 2, 3 \pmod 5$ and $p \equiv 1, 2, 4 \pmod 7$.