Test 2 Solutions

Michael Middlezong

15 July 2024

Problem 1

The main idea behind this solution is that after completing the square, we are left with an expression we have dealt with before.

Completing the square, we get

$$\sum_{k=0}^{p-1}\left(\frac{ak^2+bk+c}{p}\right)=\sum_{k=0}^{p-1}\left(\frac{a(k+\frac{b}{2a})^2-\frac{b^2-4ac}{4a}}{p}\right).$$

Since $\frac{b}{2a}$ is a constant, the expression $k+\frac{b}{2a}$ runs through all residues mod p. Therefore, we can perform the substitution $k'=k+\frac{b}{2a}$ to get

$$\sum_{k'=0}^{p-1}\left(\frac{ak'^2-\frac{b^2-4ac}{4a}}{p}\right).$$

Now, suppose $p\mid b^2-4ac$. Then, since $p\nmid 4a$ (assuming p is an odd prime),

$$\frac{b^2-4ac}{4a}\equiv 0 \pmod{p}.$$

In this case, our expression simplifies to

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

Next, consider the case where $p\nmid b^2-4ac$. Then, writing $C=-\frac{b^2-4ac}{4a}$, we are looking for

$$\sum_{k'=0}^{p-1}\left(\frac{ak'^2+C}{p}\right).$$

If $\left(\frac{a}{p}\right)=1$, then for m satisfying $m^2\equiv a \pmod{p}$,

$$\sum_{k'=0}^{p-1}\left(\frac{ak'^2+C}{p}\right)=\sum_{k'=0}^{p-1}\left(\frac{(mk')^2+C}{p}\right)=-1=-\left(\frac{a}{p}\right).$$

Otherwise, the expression ak'^2 is always a quadratic nonresidue, and more specifically, it loops through all the quadratic nonresidues twice and equals zero once.

Let d be any nonzero quadratic residue. From the previous part, we have

$$\sum_{k'=0}^{p-1}\left(\frac{dk'^2+C}{p}\right)=-1.$$

Also, the expression dk'^2 loops through all the nonzero quadratic residues twice and equals zero once. Together, ak'^2 and dk'^2 loop through all residues twice. Since adding a fixed offset C makes no difference, the expression

$$\sum_{k'=0}^{p-1}\left(\frac{ak'^2+C}{p}\right)+\sum_{k'=0}^{p-1}\left(\frac{dk'^2+C}{p}\right)$$

is then twice the sum of the Legendre symbol for all residues, which we know to be 0. This means

$$\sum_{k'=0}^{p-1}\left(\frac{ak'^2+C}{p}\right)=-\sum_{k'=0}^{p-1}\left(\frac{dk'^2+C}{p}\right)=-(-1)=-\left(\frac{a}{p}\right).$$

Therefore, if $p\nmid b^2-4ac$, we have

$$\sum_{k=0}^{p-1}\left(\frac{ak^2+bk+c}{p}\right)=-\left(\frac{a}{p}\right)$$

and thus the proof is complete.

Problem 2

Problem 3

Problem 4

First, we show that if $p \equiv -1 \pmod 8$, then 2 is a quadratic residue mod p. Using Gauss' lemma, it suffices to count the number of residues among

$$2, 4, 6, \ldots, p-1$$

that are in the interval $[\frac{p+1}{2}, p-1]$.

Since $p \equiv -1 \pmod 8$, the endpoints of that interval are both even. Thus, we are looking to count the numbers

$$\frac{p+1}{2}, \frac{p+1}{2} + 2, \ldots, \frac{p+1}{2} + \frac{p-3}{2} = p - 1.$$

There are $s = \frac{p-3}{4} + 1$ of them, and s is even because $p - 3 \equiv 4 \pmod 8$. Hence, Gauss' lemma yields $\left(\frac{2}{p}\right) = (-1)^s = 1$.

For the sake of contradiction, let $p \mid 2^n + 1$ satisfy $p \equiv -1 \pmod 8$. Since 2 is a quadratic residue mod p, there exists m such that $m^2 \equiv 2 \pmod p$. Furthermore,

$$2^n \equiv -1 \implies m^{2n} \equiv -1 \implies m^{4n} \equiv 1 \pmod p.$$

If we let $d = \operatorname{ord}_p(m)$, the above congruences imply $d \mid \gcd(4n, p-1)$ and $d \nmid 2n$.

Since $p - 1 \equiv -2 \pmod 8$, the first condition implies $\nu_2(d) < 2$. Therefore, $d \mid 4n \implies d \mid 2n$, giving us a contradiction. Thus, $2^n + 1$ does not have any prime divisors of the form $8k - 1$.

Problem 5

Problem 6

When m is odd, $2^m - 1 \equiv 3 \pmod 4$ and $2^m - 1 \equiv 1 \pmod 3$, so by CRT,

$$2^m - 1 \equiv 7 \pmod{12}.$$

Consider a prime p dividing $2^m - 1$. Since $p > 3$, the possible residues of p mod 12 are

$$p \equiv 1, 5, 7, 11 \pmod{12}.$$

We claim that there must exist a prime $p \equiv 5 \pmod{12}$ or $p \equiv 7 \pmod{12}$ dividing $2^m - 1$. This is because otherwise, all primes dividing $2^m - 1$ would be congruent to 1 or $11 \equiv -1$ mod 12, and their product could not be 7 mod 12.

For the sake of contradiction, assume $2^m - 1 \mid 3^n - 1$. Then,

$$3^n \equiv 1 \pmod p.$$

We claim that 3 is not a quadratic residue mod p. If $p \equiv 5 \pmod{12}$, then quadratic reciprocity gives us

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

On the other hand, if $p \equiv 7 \pmod{12}$, then quadratic reciprocity gives us

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

In either case, 3 is not a quadratic residue mod p.

Then, let g be a primitive root mod p, and let d be the order of 3 mod p. We can write $3 \equiv g^k \pmod p$ where k is odd. Thus,

$$3^d \equiv 1 \implies g^{dk} \equiv 1 \pmod p.$$

Since $p - 1$ is the order of g mod p, we have $p - 1 \mid dk \implies 2 \mid dk$. We know k is odd, so d must be even. We then know $d \mid n$, but n is odd, so this is a contradiction. This concludes the proof.

Problem 7

Problem 8

Problem 9