Homework 11, solutions

Solution to Problem 7. $p > 3$ is a prime. Let g be a primitive root modulo p. Then $1, g^2, g^4, \ldots, g^{p-3}$ are the quadratic residues modulo p and $g, g^3, \ldots, g^{p-2}$ are the quadratic non-residues modulo p.

a) Let S be the sum of all the quadratic residues modulo p. Thus

$$S \equiv 1 + g^2 + \ldots g^{p-3} = 1 + g^2 + (g^2)^2 + \ldots + (g^2)^{(p-3)/2} \pmod{p} .$$

Multiplying by $g^2 - 1$ we get

$$(g^2-1)S \equiv (g^2-1)(1+g^2+(g^2)^2+\ldots+(g^2)^{(p-3)/2}) = (g^2)^{1+\frac{p-3}{2}}-1 = g^{p-1}-1 \equiv 0 \pmod{p} .$$

Since $p > 3$, we have $g^2 - 1 \not\equiv 0 \pmod{p}$, and hence $S \equiv 0 \pmod{p}$.

Second method. The quadratic residues modulo p are exactly the numbers $1^2, 2^2, \ldots, ((p-1)/2)^2$. Thus

$$S \equiv 1^2 + 2^2 + \ldots + ((p-1)/2)^2 \pmod{p} .$$

Recall now that $1^2 + 2^2 + \ldots + n^2 = n(n+1)(2n+1)/6$. Thus

$$S \equiv \frac{1}{6}\frac{p-1}{2}(\frac{p-1}{2}+1)(2\frac{p-1}{2}+1)) = (p-1)(p+1)p/24 \equiv 0 \pmod{p}$$

(we us the fact that p is relatively prime to 24).

b) Let T be the sum of squares of all quadratic non-residues. Then

$$T \equiv g^2 + (g^3)^2 + \ldots (g^{p-2})^2 = g^2(1 + g^4 + (g^4)^2 + \ldots + (g^4)^{(p-3)/2}) \pmod{p} .$$

Multiplying by $g^4 - 1$, we get

$$(g^4-1)T \equiv g^2(g^4-1)(1+g^4+(g^4)^2+\ldots+(g^4)^{(p-3)/2}) = g^2((g^4)^{(p-1)/2}-1) = g^2((g^2)^{p-1}-1) \equiv 0 \pmod{p} .$$

Since $p > 5$, we have $g^4 - 1 \not\equiv 0 \pmod{p}$, hence $T \equiv 0 \pmod{p}$.

Second method. Let $t = (p-1)/2$ and let $s_1, \ldots, s_t$ be the quadratic non-sesidues modulo p. Then, for any a, the numbers $a^2s_1, a^2s_2, \ldots, a^2s_t$ are also the quadratic non-residues modulo p (these numbers are pairwise incongruent modulo p, they are non-squares modulo p and we have t of them, so we get all the quadratic non-residues modulo p). It follows that

$$T \equiv s_1^2 + \ldots + s_t^2 \equiv (a^2 s_1)^2 + \ldots + (a^2 s_t)^2 \equiv a^4 T \pmod{p} .$$

Thus p divides $(a^4 - 1)T$. Taking $a = 2$ we get $p|15T$. Since $p > 5$, we have $\gcd(15, p) = 1$, so $p|T$.

Solution to Problem 8. Let g be a primitive root modulo p. Then $1, g^2, g^4, \ldots, g^{p-3}$ are the quadratic residues modulo p. Let P be the product of all quadratic residues modulo p. Thus

$$P \equiv 1 \cdot g^2 \cdot \ldots \cdot g^{p-3} = g^{0+2+4+\ldots+(p-3)} = g^{2(1+2+\ldots+(p-3)/2)} = g^{(p-3)(p-1)/4} \pmod{p} .$$

Recall now that $g^{(p-1)/2} \equiv -1 \pmod{p}$. It follows that

$$P \equiv (-1)^{(p-3)/2} = (-1)^{(p+1)/2} \pmod{p} .$$

Consequently, $P \equiv 1 \pmod{p}$ if and only if $p \equiv 3 \pmod{4}$.

Second method. The quadratic residues modulo p are exactly the numbers $1^2, 2^2, \ldots, ((p-1)/2)^2$. Thus

$$P \equiv \left[(\frac{p-1}{2})! \right]^2 .$$

In homework 6 (problem 47a) from chapter 2 in the book) we proved that

$$\left[(\frac{p-1}{2})! \right]^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

so the result follows.

Solution to problem 10. a) Multiplying both sides by 4 we get

$$4x^2 + 4x \equiv 12 \equiv -1 \pmod{13} , \text{ i.e. } (2x+1)^2 \equiv 0 \pmod{13} .$$

It follows that $2x + 1 \equiv 0 \pmod{13}$, i.e. $x \equiv 6 \pmod{13}$.

b) We have $d = 4 + 48 = 52 \equiv 1 \pmod{17}$, so $d = 1^2$ is a square modulo 17. Completing to squares we get $(6x + 2)^2 \equiv 1 \pmod{17}$, so $6x + 2 \equiv 1 \pmod{17}$ or $6x + 2 \equiv -1 \pmod{17}$. The first congruence yields $x \equiv 14 \pmod{17}$, the second $x \equiv 8 \pmod{17}$.

c) We have $d = 9 + 4 = 13 \pmod{19}$. Now

$$\left(\frac{13}{19}\right) = \left(\frac{19}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = (-1)\cdot\left(\frac{13}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Thus d is not a square modulo 19 and therefore the congruence has no solutions.

d) We have $d = 1 + 40 = 41 \equiv -5 \pmod{23}$. Now

$$\left(\frac{-5}{23}\right) = \left(\frac{-1}{23}\right)\left(\frac{5}{23}\right) = (-1)\cdot\left(\frac{23}{5}\right) = -\left(\frac{3}{5}\right) = -\left(\frac{5}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1.$$

Thus d is a square modulo 23 and therefore the congruence has solutions.

We have $41 \equiv 18 \equiv 2\cdot 9 \equiv 25\cdot 9 = 15^2 \pmod{23}$. Now our congruence

$$2x^2 + x - 5 \equiv 0 \pmod{23}$$

is equivalent to

$$16x^2 + 8x + 1 - 41 \equiv (4x+1)^2 - 15^2 \equiv 0 \pmod{23} .$$

Thus either $4x+1 \equiv 15 \pmod{23}$ or $4x+1 \equiv -15 \pmod{23}$. The first case yields $x \equiv 15 \pmod{23}$, the second case yields $x \equiv -4 \equiv 19 \pmod{23}$.

Solution to problem 22. Note that

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

as we have $(p-1)/2$ quadratic recidues and $(p-1)/2$ quadratic non-recidues so the sum has $(p-1)/2$ terms equal to 1 and $(p-1)/2$ terms equal to -1. We can write the above sum as

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

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

When $p \equiv 1 \pmod{4}$, we have $\left(\frac{-1}{p}\right) = 1$ and therefore

$$0 = 2\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right), \text{ i.e. } \sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right) = 0.$$

Solution to problem 24. Note that

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

Since the Legendre symbols are ± 1, this is the same as

$$\left(\frac{2}{p}\right)\left(\frac{5}{p}\right)\left(\frac{10}{p}\right)=1.$$

It follows that either exactly one or all three of the Legendre symbols must be 1. This proves part a) and shows that the answer to part b) is "no".

c) Note that 1,4,9 are sqaures, hence quadratic residues modulo p. It follows from a) that either $1, 2$, or $4, 5$, or $9, 10$ are consecutive quadratic residues modulo p.

Solution to problem 27. Suppose p is a prime such that $p \equiv 3 \pmod 4$ and $q = 2p + 1$ is also a prime. If $p = 3$ then clearly $2^p - 1 = 7$ is a Mersenne prime. Conversely, suppose that $2^p - 1$ is a prime. Note that $2p \equiv 6 \pmod 8$, so $q = 2p + 1 \equiv 7 \pmod 8$. It follows from the quadratic reciprocity that $(\frac{2}{q}) = 1$. Thus $2^p = 2^{(q-1)/2} \equiv 1 \pmod q$. In other words, q divides $2^p - 1$. Since $2^p - 1$ is a prime, we have $q = 2^p - 1$. In other words, $2p + 1 = 2^p - 1$. This means that $p = 2^{p-1} - 1$. As the left hand side is a prime, we have $p - 1$ is a prime which can happen only if $p = 3$.

Remark. It is not hard to prove that $2^x > 2x + 2$ for $x > 3$.

Solution to problem 33. Note that 107 is a prime number. We have

$$\left(\frac{71}{107}\right)=-\left(\frac{107}{71}\right)=-\left(\frac{36}{71}\right)=-\left(\frac{6^2}{71}\right)=-1.$$

Thus 71 is not a quadratic residue modulo 107, hence there is no integer n such that $n^2 - 71$ is divisible by 107.

Solution to problem 34. Since $p \equiv q \pmod 4$, p and q are either both $\equiv 1 \pmod 4$ or both $\equiv 3 \pmod 4$. Note that

$$\left(\frac{a}{q}\right)=\left(\frac{4a}{q}\right)=\left(\frac{4a+q}{q}\right)=\left(\frac{p}{q}\right).$$

Similarly,

$$\left(\frac{a}{p}\right)=\left(\frac{4a}{p}\right)=\left(\frac{4a-p}{p}\right)=\left(\frac{-q}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{q}{p}\right).$$

Using quadratic reciprocity, we have

$$\left(\frac{a}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right) = (-1)^{(p-1)(q+1)/4}\left(\frac{a}{q}\right).$$

It is eqsy to see that $(-1)^{(p-1)(q+1)/4} = 1$ when p and q are either both $\equiv 1 \pmod 4$ or both $\equiv 3 \pmod 4$. Thus indeed

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$