Solutions to Homework 8

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

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

(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 not divisible by p, the numbers $a^2 s_1, a^2 s_2, \ldots, a^2 s_t$ 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 $(p+1)/2$ is even, i.e. $p \equiv 3 \pmod{4}$.

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. If we want to solve the congruence

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

where p is an odd prime and $p \nmid a$, we consider the equivalent congruence (multiplying both sides by $4a$, which is invertible modulo p):

$$4a^2x^2 + 4abx + 4ac = (2ax)^2 + 2(2ax)b + b^2 - b^2 + 4ac = (2ax+b)^2 - (b^2 - 4ac) \equiv 0 \pmod{p}$$

i.e.

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p} .$$

Let $d = b^2 - 4ac$. If d is a quadratic non-residue modulo p then the congruence has no solutions. If d is a quadratic residue modulo p then $u^2 \equiv d \pmod{p}$ for some u and therefore

$$2ax + b \equiv u \pmod{p} \text{ or } 2ax + b \equiv -u \pmod{p}$$

and each of these two linear congruences has a unique solution, so our original congruence has exactly two solutions. Finally, if $d \equiv 0 \pmod{p}$ then $2ax + b \equiv 0 \pmod{p}$, and this congruence has unique solution.

a) We are solving the congruence $x^2 + x - 3 \equiv 0 \pmod{13}$. Thus $a = 1, b = 1, c = -3$, $d = b^2 - 4ac = 13$. Since $d \equiv 0 \pmod{13}$, we have $2ax + b = 2x + 1 \equiv 0 \pmod{13}$, which has unique solution $x \equiv 6 \pmod{13}$.

b) We are solving the congruence $3x^2 + 2x - 4 \equiv 0 \pmod{17}$. Thus $d = 4 + 48 = 52 \equiv 1 \pmod{17}$. Since $d \equiv 1^2 \pmod{17}$ is a qudratic residue modulo 17, we have two solutions:

$$6x + 2 \equiv 1 \pmod{17} \text{ or } 6x + 2 \equiv -1 \pmod{17} .$$

The first congruence yields $x \equiv 14 \pmod{17}$, the second $x \equiv 8 \pmod{17}$.

c) We are solving the congruence $x^2 + 3x - 1 \equiv 0 \pmod{19}$. 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 are solving the congruence $2x^2 + x - 5 \equiv 0 \pmod{23}$. 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 quadratic residue modulo 23 and therefore the congruence has two solutions. We need to solve first the congruence $u^2 \equiv 41 \pmod{23}$. We have $41 \equiv 18 \equiv 2\cdot 9 \equiv 25\cdot 9 = 15^2 \pmod{23}$, so $u = 15$. 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 28 d, e. Follow the method discussed in the solution to problem 37. If you do not want to use the Jacobi symbol, factor the numbers appearing in your computation into primes. For example, to compute $\left(\frac{2817}{4177}\right)$ using properties of the Jacobi symbol:

$$\left(\frac{2817}{4177}\right) = \left(\frac{4177}{2817}\right) = \left(\frac{1360}{2817}\right) = \left(\frac{2^4}{2817}\right)\left(\frac{85}{2817}\right) = \left(\frac{85}{2817}\right) = \left(\frac{2817}{85}\right) =$$

$$\left(\frac{33 \cdot 85 + 12}{85}\right) = \left(\frac{12}{85}\right) = \left(\frac{2^2}{85}\right)\left(\frac{3}{85}\right) = \left(\frac{85}{3}\right) = \left(\frac{28 \cdot 3 + 1}{3}\right) = 1.$$

(we used the facts that $4177 \equiv 1 \pmod 4$, $85 \equiv 1 \pmod 4$).

To avoid using the Jacobi symbol, one would need to factor 2817 first, or use the following trick: $2817 \equiv -1360 \pmod{4177}$ so

$$\left(\frac{2817}{4177}\right) = \left(\frac{-1360}{4177}\right) = \left(\frac{-1}{4177}\right)\left(\frac{2^4}{4177}\right)\left(\frac{5}{4177}\right)\left(\frac{17}{4177}\right)$$

and then compute the Legendre symbols

$$\left(\frac{5}{4177}\right) = \left(\frac{4177}{5}\right) = \left(\frac{2}{5}\right) = -1$$

and

$$\left(\frac{17}{4177}\right) = \left(\frac{4177}{17}\right) = \left(\frac{245 \cdot 17 + 12}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{2^2}{17}\right)\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

We leave the computation of $\left(\frac{-107}{211}\right)$ to the reader (the answer is -1).

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

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

Solution to problem 37. a) We will use Jacobi's quadratic reciptocity:

1. If m and n are distinct odd numbers then
   $\left(\frac{n}{m}\right) = \begin{cases} -\left(\frac{m}{n}\right) & \text{if } m \equiv 3 \equiv n \pmod 4 \text{ ;} \\ \left(\frac{m}{n}\right) & \text{if at least one of } m, n \text{ is } \equiv 1 \pmod 4 \text{ .} \end{cases}$
   Equivalently, if m, n are relatively prime, then $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$.

2. $\left(\frac{2}{m}\right) = \begin{cases} 1 & \text{if } m \equiv 1, 7 \pmod 8 \text{ ;} \\ -1 & \text{if } m \equiv 3, 5 \pmod 8 \text{ .} \end{cases}$
   Equivalently, $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.

3. $\left(\frac{-1}{m}\right) = \begin{cases} 1 & \text{if } m \equiv 1 \pmod 4 \text{ ;} \\ -1 & \text{if } m \equiv 3 \pmod 4 \text{ .} \end{cases}$
   Equivalently, $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$.

To compute $\left(\frac{-79}{105}\right)$ note that $105 = 79 + 26$

Since $105 \equiv 1 \pmod 4$, we have $\left(\frac{-1}{105}\right) = 1$ and

$$\left(\frac{-79}{105}\right) = \left(\frac{-1}{105}\right)\left(\frac{79}{105}\right) = \left(\frac{105}{79}\right) = \left(\frac{26}{79}\right) = \left(\frac{2}{79}\right)\left(\frac{13}{79}\right).$$

Now $79 = 6 \cdot 13 + 1$, $79 \equiv 7 \pmod 8$ and $13 \equiv 1 \pmod 4$ so $\left(\frac{2}{79}\right) = 1$ and

$$\left(\frac{13}{79}\right) = \left(\frac{79}{13}\right) = \left(\frac{1}{13}\right) = 1.$$

Putting these together, we get $\left(\frac{-79}{105}\right) = 1$.

Alternatively, we factor $105 = 3 \cdot 5 \cdot 7$ and use the definition of the Jacobi symbol:

$$\left(\frac{-79}{105}\right) = \left(\frac{-79}{3}\right)\left(\frac{-79}{5}\right)\left(\frac{-79}{7}\right).$$

Since $-79 = (-27) \cdot 3 + 2 = (-16) \cdot 5 + 1 = (-12) \cdot 7 + 5$, we get

$$\left(\frac{-79}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

$$\left(\frac{-79}{5}\right) = \left(\frac{1}{5}\right) = 1,$$

$$\left(\frac{-79}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Thus $\left(\frac{-79}{105}\right) = (-1) \cdot 1 \cdot (-1) = 1$.

To compute $\left(\frac{87}{133}\right)$ and $\left(\frac{91}{129}\right)$ follow one of the above approaches (for the second approach, $133 = 7 \cdot 19$, $129 = 3 \cdot 43$). You should get $\left(\frac{87}{133}\right) = -1$ and $\left(\frac{91}{129}\right) = -1$.

b) If a is a quadratic residue modulo n and m is a divisor of n then a is a quadratic residue modulo m. Thus, if $n = p_1 \dots p_k$ is a product of odd primes then $\left(\frac{a}{p_i}\right) = 1$ for all i and therefore $\left(\frac{a}{n}\right) = 1$.

The converse if usually false. For example, if $n = p^2$ and p is an odd prime then $\left(\frac{a}{n}\right) = 1$ for every a not divisible by p. Howver, if a is a quadratic non-residue modulo p then it is also a quadratic non-residue modulo p^2. For example, $\left(\frac{2}{9}\right) = 1$ but 2 is a quadratic non-residue modulo 9.