MODEL ANSWERS TO THE EIGHTH HOMEWORK

5.1.1.

p/q	3	5	7	11	13	17	19	23
3	0	-1	1	-1	1	-1	1	-1
5	-1	0	-1	1	-1	-1	1	-1
7	-1	-1	0	1	-1	-1	-1	1
11	1	1	-1	0	-1	-1	-1	1
13	1	-1	-1	-1	0	1	-1	1
17	-1	-1	-1	-1	1	0	1	-1
19	-1	1	1	1	-1	1	0	1
23	1	-1	-1	-1	1	-1	-1	0

Looking at the table,

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

when the pair p, q is one of

$$3,5;\ 3,13;\ 3,17;\ 5,7;\ 5,11;\ 5,13;\ 5,17; 5,19;\ 5,23;\ 7,13;$$
$$7,17;\ 11,13;\ 11,17;\ 13,17;\ 13,19;\ 13,23; 17,19;\ 17,23.$$

The rule is given by quadratic reciprocity; we have equality unless both p and q are congruent to 3 modulo 4.

5.1.2. If the equation

$$x^2 \equiv a \mod p$$

has a solution then

$$a^{(p-1)/2} \equiv 1 \mod p.$$

If $p \equiv 3 \mod 4$ then there is an integer k such that $p = 4k+3$. In this case

$$\frac{p+1}{4} = k+1 \qquad \text{and} \qquad \frac{p-1}{2} = 2k+1.$$

Let

$$b = a^{k+1}.$$

We check that b is a solution of the equation

$$x^2 \equiv a \mod p.$$

We have

$$\begin{aligned} b^2 &= (a^{k+1})^2 \\ &= a^{2k+2} \\ &= a^{2k+1}a \\ &\equiv a \mod p. \end{aligned}$$

Thus b is a solution of the equation

$$x^2 \equiv a \mod p.$$

It follows that $\pm b$ are both of the solutions to the equation

$$x^2 \equiv a \mod p.$$

5.1.3. We first factor

$$\begin{aligned} 2272 &= 2 \cdot 1136 \\ &= 2^2 \cdot 568 \\ &= 2^3 \cdot 284 \\ &= 2^4 \cdot 142 \\ &= 2^5 \cdot 71. \end{aligned}$$

As $8|2272$ we have to check that 37 modulo 8 is congruent to one.

$$\begin{aligned} 37 &= 32 + 5 \\ &\equiv 5 \mod 8. \end{aligned}$$

Thus 37 is not a quadratic residue of 2272.

5.1.5. Let $a \in \mathbb{Z}$. Knowledge of the last n digits of a is equivalent to determining the residue class of a modulo 10^n. So we want to know the number of solutions of

$$x^2 = b \mod 10^n.$$

By the Chinese remainder theorem, we have to count the number of solutions to

$$x^2 \equiv b \mod 5^n \qquad \text{and} \qquad x^2 \equiv b \mod 2^n.$$

As we are assuming there is a solution, the number of solutions to the first equation is always two. The number of solutions to the second equation is always one if $n = 1$, and always 2 if $n = 2$. If $n \geq 3$ then the number of solutions is always 4.

Thus there are 2, 4 or 8 possibilities for the last n digits, according as $n = 1$, $n = 2$ or $n \geq 3$.

5.1.6. We want to solve the equation

$$x^2 = x \mod 10^3 \qquad \text{that is} \qquad x^2 - x = 0 \mod 10^3.$$

By the Chinese remainder theorem, we have to solve the equations

$$x^2 - x = 0 \mod 5^3 \qquad \text{and} \qquad x^2 = x \mod 2^3.$$

We first solve the equations

$$x^2 - x = 0 \mod 5 \qquad \text{and} \qquad x^2 - x = 0 \mod 2.$$

Both equations have solutions $x = 0$ and $x = 1$.
Let $f(x) = x^2 - x$. Then $f'(x) = 2x - 1$. It easy to see that all four solutions have non-zero derivative and so all solutions are non-singular. So we can lift all of these solutions to four solutions modulo 125 and modulo 8.
Now $x = 0$ and $x = 1$ are always solutions, modulo any prime. So the four solutions modulo 125 and 8 are still 0 and 1. By the Chinese remainder theorem there are four solutions, one for every possible choice of 0 and 1. Again, two of them are clear, 0 and 1 are two solutions. But they don't have four digits.
So we just have to solve

$$x = 0 \mod 125x \qquad\qquad 1 \mod 8$$

and

$$x = 1 \mod 125x \qquad\qquad 0 \mod 8.$$

To solve the first equation we need to find z_1 so that

$$125z_1 \equiv 1 \mod 8.$$

This reduces to

$$5z_1 \equiv 1 \mod 8.$$

This has solution $z_1 = 5$. This gives

$$x = 5 \cdot 125 = 625.$$

To solve the first equation we need to find z_2 so that

$$8z_2 = 1 \mod 125.$$

This has solution $z_2 = 47$. This gives

$$x = 47 \cdot 8 = 376.$$

5.2.1. By Gauss's Lemma we need to count the number μ of elements of

$$\{ -2k \mid 1 \leq k \leq \frac{p-1}{2} \}$$

which are equivalent modulo p to a number in the interval $(-p/2, 0)$. Now the numbers $-2k$ lie in the interval $(-p, 0)$. Therefore we just need to count the number of integers $-2k$ in the interval $(-p/2, 0)$. Now $-2k > -p/2$ if and only if $k < p/4$. Thus

$$\mu = \llcorner p/4 \lrcorner.$$

We consider p modulo 8. We have

$$\mu = \begin{cases} 2k & \text{if } p = 8k+1 \text{ or } 8k+3 \\ 2k+1 & \text{if } p = 8k+5 \text{ of } 8k+7. \end{cases}$$

It follows that μ is even if and only if $p \equiv 1 \mod 8$ or $p \equiv 3 \mod 8$ and so $(-1)^\mu$ is 1 if and only if $p \equiv 1 \mod 8$ or $p \equiv 3 \mod 8$. Therefore -2 is a quadratic residue if and only if $p \equiv 1 \mod 8$ or $p \equiv 3 \mod 8$. On the other hand,

$$\begin{aligned} \left(\frac{-2}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) \\ &= (-1)^{(p-1)/2}(-1)^{(p^2-1)/8}. \end{aligned}$$

We again consider what happens modulo 8. If $p = 8k+1$ or $8k+5$ then the first factor is positive. If $p = 8k+1$ or $8k+7$ the second factor is positive. Thus the product is both if $p \equiv 1 \mod 8$ or $p \equiv 8k+3 \mod 8$.

5.2.3. We have

$$\begin{aligned} \left(\frac{-a}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) \\ &= (-1)^{(p-1)/2}\left(\frac{a}{p}\right). \end{aligned}$$

On the other hand,

$$(-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p = 4k+1 \\ -1 & \text{if } p = 4k+3. \end{cases}$$

Thus if $p \equiv 1 \mod 4$ then a is quadratic residue if and only if $-a$ is a quadratic residue and $p \equiv 3 \mod 4$ then exactly one of a and $-a$ is a quadratic residue.

5.2.6. Let t be the order of -4 modulo q. Then t divides $q-1$ and we want to show that $t = q-1$. Now

$$q - 1 = 2p.$$

As p is prime and t divides $2p$ it follows that either $t = 1$ or $t = 2$ or $t = p$ or $t = 2p$. As p is odd it follows that $p > 2$ and so $q \geq 7$. Thus

$-4 \neq 1 = \mod q$ and so $t \neq 1$.

$$(-4)^2 = 16.$$

If this is equivalent to 1 modulo q then $q|15$ so that $q = 3$ or 5, which we have seen is not true. Thus $t \neq 2$. Suppose that $t = p$. Then

$$\begin{aligned}\left(\frac{-4}{q}\right) &= (-4)^{(q-1)/2} \\ &= (-4)^p \\ &= 1.\end{aligned}$$

But

$$\begin{aligned}\left(\frac{-4}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{4}{q}\right) \\ &= (-1)^{(q-1)/2}\left(\frac{2^2}{q}\right) \\ &= (-1)^p \\ &= -1,\end{aligned}$$

as p is odd, a contradiction.
Thus $t = 2p = q - 1$ and -4 is a primitive root.
5.2.8. First note that as p and m are coprime, the numbers

$$m \qquad 2m, \qquad 3m \qquad \dots \qquad (p-2)m \qquad \text{and} \qquad (p-1)m$$

are a complete residue system. Thus

$$\begin{aligned}\sum_{a=1}^{p}\left(\frac{ma}{p}\right) &= \sum_{a=1}^{p-1}\left(\frac{ma}{p}\right) \\ &= \sum_{a=1}^{p-1}\left(\frac{a}{p}\right).\end{aligned}$$

Suppose that $p = 2k + 1$. Then $p - 1 = 2k$ and precisely k of the numbers from 1 to $p - 1$ are quadratic residues and k of the numbers from 1 to $p - 1$ are not quadratic residues.
It follows that

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