Introduction to Number Theory
5. exercise set, solutions

1. Quadratic residues mod 19 can be found by calculating $1^2, 2^2, ..., 18^2 \pmod{19}$. One gets that the complete set of quadratic residues is $\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$.

By Euler's criterion $(a/p) \equiv a^{(p-1)/2} \pmod p$. We check which values of $a \in \{1, 2, ..., 18\}$ satisfy $a^9 \equiv 1 \pmod{19}$ and which satisfy $a^9 \equiv -1 \pmod{19}$. Those satisfying $a^9 \equiv 1$ (mod 19) are quadratic residues. This gives the same answer.

2. We know that $\left(\frac{0}{p}\right) = 0$. Furthermore we also know that there are equally many quadratic residues and non-residues (mod p) among $\{1, 2, ..., p-1\}$. As $\left(\frac{j}{p}\right) = 1$ if j is a quadratic residue and -1 if j is a non-residue we have

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

as desired. $\square$

3. (i) As a is a primitive root (mod p) we have $\left(\frac{a}{p}\right) \neq 0$ and that $a^{(p-1)/2} \not\equiv 1 \pmod p$. As by Euler's criterion we have $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$ it follows that we have $\left(\frac{a}{p}\right) = -1$. Now it follows from the multiplicativity of Legendre symbol that

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

It follows immediately that there is an equal number of quadratic residues and non-residues as $(-1)^j = 1$ if and only if j is even. $\square$

(ii) As a is a primitive root (mod p) we have that $\{1, 2, ..., p-1\} = \{a, a^2, ..., a^{p-1}\}$ in some order. Now there are equally many even and odd numbers among $\{1, 2, ..., p-1\}$ so the claim follows from part (i). $\square$

4. Note that $920 = 2^3 \cdot 5 \cdot 23$. The congruence $x^2 \equiv 761 \pmod 5$ has a solution $x = 1$ and the congruence $x^2 \equiv 761 \pmod{23}$ has a solution $x = 5$. Furthermore $761 \equiv 1 \pmod 8$ and $8|920$. Therefore the congruence $x^2 \equiv 1 \pmod{761}$ has a solution by Theorem 4.3.(i). Now the part (ii) of Theorem 4.3. tells that the number of solutions is $2^{2+2} = 16$.

5. By using the multiplicativity of the Legendre symbol, the quadratic residue law and Theorem 4.9. we have

$$\left(\frac{52}{97}\right) = \left(\frac{2}{97}\right)^2 \left(\frac{13}{97}\right) = \left(\frac{13}{97}\right) = \left(\frac{97}{13}\right) = \left(\frac{2}{13}\right) = -1$$

and

$$\left(\frac{240}{773}\right) = \left(\frac{16}{773}\right)\left(\frac{15}{773}\right) = \left(\frac{2}{773}\right)^4 \left(\frac{5}{773}\right)\left(\frac{3}{773}\right) = \left(\frac{773}{5}\right)\left(\frac{773}{3}\right) = \left(\frac{3}{5}\right)\left(\frac{2}{3}\right) = -\left(\frac{5}{3}\right) = -\left(\frac{2}{3}\right) = 1.$$

6. There was a mistake in the problem statement. It should have read $(7/p)$ instead of $(5/p)$. We have $(7/7) = 0$ so assume that $p > 7$. We have two cases to consider.

1) Assume that $p \equiv 1 \pmod 4$. The quadratic residue law gives

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

It is easy to check that quadratic residues mod 7 are $1, 2$ and 4. Now one can use the Chinese remainder theorem to solve the systems of congruences

$$\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 1 \pmod 7 \end{cases} \quad \begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 2 \pmod 7 \end{cases} \quad \begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 4 \pmod 7 \end{cases}$$

to see that in this case $(7/p) = 1$ if and only if $p \equiv 1, 9$ or $-3 \pmod{28}$. Similarly one sees that non-residues in this case are $-11, 5$ and 13.

2) Assume that $p \equiv 3 \pmod 4$. Then the quadratic residue law gives

$$\left(\frac{7}{p}\right)\left(\frac{p}{7}\right) = -1$$

so

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

Now we can see by using similar analysis as in case 1) that $(7/p) = -1$ if and only if $p \equiv -5, -13$ or $11 \pmod{28}$.

Therefore

$$\left(\frac{7}{p}\right) = \begin{cases} 1 \text{ if } p \equiv \pm 1, \pm 3, \pm 9 \pmod{28} \\ -1 \text{ if } p \equiv \pm 5, \pm 11, \pm 13 \pmod{28} \end{cases}$$

7. We have $(5/5) = 0$. Assume $p > 5$. By the quadratic residue law we have

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

Thus

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

But quadratic residues mod 5 are 1 and 4. Thus

$$\left(\frac{5}{p}\right) = \begin{cases} 1 \text{ if } p \equiv \pm 1 \pmod 5 \\ -1 \text{ if } p \equiv \pm 2 \pmod 5 \end{cases}$$

8*. Call the sum of the third powers of quadratic residues mod p by X_p. It is straightforward to check that $X_3 \equiv 1 \pmod 3$, $X_5 \equiv 0 \pmod 5$ and $X_7 \equiv 3 \pmod 7$. Assume that $p > 7$. Let a be a primitive root $\pmod p$. By problem 3. quadratic residues correspond to even powers of a. Thus we have

$$X_p \equiv \sum_{\ell=1}^{\frac{p-1}{2}} \left(a^{2\ell}\right)^3 \equiv \sum_{\ell=1}^{\frac{p-1}{2}} a^{6\ell} \pmod p.$$

But now

$$\begin{aligned}(a^6-1)X_p &\equiv (a^6-1)\sum_{\ell=1}^{\frac{p-1}{2}} a^{6\ell} \\ &\equiv a^{3(p+1)} - a^6 \\ &\equiv a^6\left(a^{3p-3}-1\right) \\ &\equiv 0 \pmod{p},\end{aligned}$$

where the last step follows from Fermat's little theorem. As $p > 7$ and a is a primitive root $\pmod{p}$ it follows that $a^6 \not\equiv 1 \pmod{p}$ so $X_p \equiv 0 \pmod{p}$. Therefore the answer is

$$X_p\ (\mathrm{mod} p) = \begin{cases} 1 \text{ if } p = 3 \\ 0 \text{ if } p = 5 \\ 3 \text{ if } p = 7 \\ 0 \text{ if } p > 7 \end{cases}$$

.