QUESTION

Use Gauss' Lemma to decide for each of the following pairs (a, p) whether or not a is a square mod p.

(i) (5,23) (ii) (10,17) (iii) (10,13).

ANSWER

(i) Here S consists of the first $\frac{(23-1)}{2} = 11$ multiples of 5, viz. $S = \{5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55$
Reducing these to their least positive residues mod 23 gives the set $s' = \{5, 10, \underline{15}, \underline{20}, 2, 7, \underline{12}, \underline{17}, \underline{22}, 4, 9\}$. We have underlined those exceeding $\frac{23}{2}$, and we note that there are 5 of them. Thus $n = 5, (-1)^5 = -1$, so $\left(\frac{5}{23}\right) = -1$ and 5 is non-square mod 23.

(ii) Here $\frac{(P-1)}{2} = \frac{16}{2} = 8$, so we want the first 8 multiples of 10. Thus $S = \{10, 20, 30, 40, 50, 60, 70, 80\}$. Reducing to least positive residues mod 17 gives $S' = \{\underline{10}, 3, \underline{13}, 6, \underline{16}, 9, 2, \underline{12}\}$ and the ones exceeding $\frac{17}{2}$ have been underlined. Again there are 5 of them, so $n = 5, (-1)^5 = -1$ and $\left(\frac{10}{17}\right) = -1$. Thus 10 is a non-square mod 17.

(iii) Here $\frac{(p-1)}{2} = \frac{12}{2} = 6$, so $S = \{10, 20, 30, 40, 50, 60\}$. Reducing mod 13, $S' = \{\underline{10}, \underline{7}, 4, 1, \underline{11}, \underline{8}\}$, where the entries bigger then $\frac{13}{2}$ are underlined. Thus $n = 4, (-1)^4 = 1$, and $\left(\frac{10}{13}\right) = 1$. Thus 10 is a square mod 13. (In fact it is 6^2.)