QUESTION

For each pair (a, p) below, use Euler's criterion to decide whether or not the equation $x^2 \equiv a \bmod p$ has any solutions:-

(i) (2,5) (ii) (3,13) (iii) (7,31).

ANSWER

(i) We need to calculate $a^{\frac{(p-2)}{2}} \bmod p$, i.e. $2^2 \bmod 5$. Now $2^2 \equiv -1 \bmod 5$, so $x^2 \equiv 2 \bmod 5$ has no solutions.

(ii) $a^{\frac{(p-1)}{2}} \equiv 3^6 \equiv (-4)^3 \equiv -4.3 \equiv -12 \equiv 1 \bmod 13$, and so the equation $x^2 \equiv 3 \bmod 13$ has two solutions. (For interest, they are $\pm 4 \bmod 13$.)

(iii) $a^{\frac{(p-1)}{2}} \equiv 7^{15} \bmod 31$. Now $7^2 \equiv 49 \equiv -13 \bmod 31$, so $7^3 \equiv -91 \equiv 2 \bmod 31$. Thus $7^{15} \equiv 2^5 \equiv 32 \equiv 1 \bmod 31$. Thus the equation $x^2 \equiv 7 \bmod 31$ has two solutions. (Actually, $\pm 10 \bmod 31$.)