QUESTION

Explain why 2^{p-3} is a root of $4x \equiv 1 \bmod p$, for any odd prime p. Hence find the smallest positive residue of $2^{16} \bmod 19$.

ANSWER

If p is odd, then $\gcd(2, p) = 1$ so by Fermat's Little Theorem (th.4.2), $2^{p-1} \equiv 1 \bmod p$. Thus $2^2.2^{p-1} \equiv 1 \bmod p$, that is $4.2^{p-3} \equiv 1 \bmod p$. Thus 2^{p-3} is a solution of the congruence $4x \equiv 1 \bmod p$.

Now we know, by cor.3.6, that this congruence has a unique solution mod p. Thus if we discover that $x = a$ is a solution, we'll know that $2^{p-3} \equiv a \bmod p$. For our case, $p = 19$, so we solve $4x \equiv 1 \bmod 19$. We have $4x \equiv 1 \equiv 20 \bmod 19$, so on division by 9, $x \equiv 5 \bmod 19$. (Other methods of solution are available-you may, for example, have multiplied the congruence through by 5.)

Thus $2^{p-3} = 2^1 6 \equiv 5 \bmod 19$.