QUESTION

Suppose p is an odd prime, and that $q = 4p + 1$ is also a prime. Show that $\left(\frac{2}{q}\right) = -1$, and hence prove that 2 is a primitive root mod q.

ANSWER

As p is odd, $p = 2t+1$ for some $t \in Z$. Thus $q = 4p+1 = 8t+4+1 = 8t+5$, so that $q \equiv 5 \bmod 8$. Thus $\left(\frac{2}{q}\right) = -1$ by th. 7.3. Hence, by Euler's criterion (th.6.5), $2^{\frac{(q-1)}{2}} \equiv -1 \bmod q$, i.e. $2^{2p} \equiv -1 \bmod q$. Now q is prime, so $\phi(q) = q - 1 = 4p$. Hence the possible orders of 2 mod q are the divisors of $4p$, viz. $1, 2, 4, p, 2p$ and $4p$. If the order of 2 were $1, 2, p$ or $2p$, then $262p$ would be $\equiv 1 \bmod q$. But we've seen $2^{2p} \equiv -1 \not\equiv 1 \bmod q$ (as q is odd), so the order can only be 4 or $4p$. The order is not 4 as $2^4 = 16$, and this would be $\equiv 1 \bmod q$ only if q were a divisor of 15, i.e. 3 or 5. But $q = 4p+1 \geq 4.3+1$ (as q is odd, so ≥ 3), so q cannot be 3 or 5. Thus the order of 2 mod q is none of $1, 2, 4, p, 2p$ and so it must be $4p (= \phi(q))$, so 2 is a primitive root mod q, as required.