QUESTION

Let U_n denote the group of units modulo n.

(i) Explain the following terms: (a) $g \in U_n$ is a primitive root and (b) $g \in U_n$ is a quadratic non-residue.

(ii) Suppose that $p = 2^m + 1$ is a prime for some $m > 0$. Show rhat $g \in U_p$ is a quadratic non-residue if and only if it is a primitive root.

(iii) Using quadratic reciprocity, or otherwise, show that

$$3^{\frac{(p-1)}{2}} \equiv -1(\text{modulo } p).$$

(iv) If n is an integer of the form $n = 2^{2^m} + 1$ such that $3^{\frac{(n-1)}{2}} \equiv -1$ (modulo n) show that n is a prime. (Hint: In the proof of (iv) you may assume (see question 8(viii)) without proof that $\phi(n) \leq n - \sqrt{n}$ if p is a composite integer.)

ANSWER

(i) If U_n is a cyclic group then any generator, $g \in U_n$ is called a primitive root modulo n. A quadratic non-residue, $g \in U_n$, is any element for which the equation $g = h^2$ has no solution $f \in U_n$.

(ii) If $p = 2^{2^m} + 1$ is a prime then U_p is cyclic of order $p - 1 = 2^{2^m}$. Choose a generator, $g \in U_p$. Then g^j is a generator if and only if $\gcd(j, 2^{2^m}) = 1$ is odd, which is equivalent to j being odd. On the other hand $g^j = h^2 = g^{2s}$ has a solution if and only if j is even. Hence g^j is a quadratic non-residue if and only if j is odd.

(iii) If the order of 3 in U_p is equal to 2^α then $3^{2^{\alpha-1}} = -1$, since $3^{2^{\alpha-1}}$ is not congruent to 1 (modulo p) but its square is. Hence the given congruence is equivalent, by part (ii), to 3 being a quadratic non-residue modulo p. In terms of Legendre symbols

$$\left(\frac{3}{P}\right) = -1$$

if and only if

$$3^{\frac{(p-1)}{2}} \equiv -1 \text{ (modulo } p).$$

By Quadratis Reciprocity

$$\left(\frac{3}{P}\right)\left(\frac{p}{3}\right) = (-1)^{(s-1)(p-1)/4} = 1$$

However $p \equiv (-1)^{2^m} + 1 \equiv 2$ (modulo 3) and

$$\left(\frac{2}{3}\right) = -1,$$

as required.

(iv) If $3^{\frac{(n-1)}{2}} \equiv -1$ (modulo n) then the order of 3 in U_n is at least $n-1$. However, $g^{\phi(n)} \equiv 1$ for all $g \in U_n$. Hence if n is composite the Hint yields

$$n - 1 \leq \phi(n) \leq n - \sqrt{n}$$

which is impossible. Hence n must be prime.