

Elementary Number Theory
Home work problem III, deadline October 6, 2006

For this problem it is recommended that you have at least made exercise 3.5.9. Let $m \in \mathbb{N}$. We shall be interested in the number of residue classes modulo m that satisfy $x^2 \equiv 1 \pmod{m}$. In other words, the number of integers x with $0 < x < m$ that satisfy $x^2 \equiv 1 \pmod{m}$. Call this number of solutions $q(m)$.

1. Make a table (manual or using a computer) of the values $q(m)$ for $m = 2, 3, \dots, 20$. Do you see any regularities in it?
2. From your table you may suspect that $q(p) = 2$ if p is an odd prime. What are the solutions in that case?
Prove that $q(p) = 2$ when p is an odd prime. (Hint: observe that $x^2 \equiv 1 \pmod{p}$ implies $p \mid x^2 - 1$ hence $p \mid (x - 1)(x + 1)$).
3. Again let p be an odd prime. Show that $q(p^k) = 2$ for every k .
4. Show that $q(2) = 1, q(4) = 2$ and $q(2^k) = 4$ for all $k > 2$.
5. Let $m, n \in \mathbb{N}$ and suppose that $\gcd(m, n) = 1$. Let $x_1, x_2 \in \mathbb{Z}$ be such that $x_1^2 \equiv 1 \pmod{m}$ and $x_2^2 \equiv 1 \pmod{n}$. According to the Chinese remainder theorem there exists an integer x_0 , unique modulo mn , such that $x_0 \equiv x_1 \pmod{m}$ and $x_0 \equiv x_2 \pmod{n}$.
 - (a) Show that $x_0^2 \equiv 1 \pmod{mn}$.
 - (b) Show that q is a multiplicative function.