QUESTION

Find the orders of the following elements:-

(i) 2 mod 7 (ii) 3 mod 14 (iii) 5 mod 17.

ANSWER

Note that if $\gcd(a, n) = 1$, then the order of a mod n is a divisor of $\phi(n)$.

(i) $\phi(7) = 6$, so $o(2)$ is 1,2,3 or 6. $o(2) \neq 1$ as only 1 has order 1, and $o(2) \neq 2$ as only -1 has order 2. (This is because 7 is prime, so th only roots of $x^2 \equiv 1$ mod 7 are ± 1) If we calculate 2^3 mod 7 we find $2^3 \equiv 8 \equiv 1$ mod 7, so the order of 2 mod 7 is 3.

(ii) $\phi(14) = 14\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{7}\right) = 6$ so the order is 1,2,3 or 6. Again, only 1 has order 1, so we may eliminate 1, but the argument we used too eliminate 2 worked for primes only, so we must check 2 directly. $3^2 \equiv 9 \not\equiv 1$ mod 14. so the order is not 2. Also $3^3 \equiv 27 \equiv -1 \not\equiv 1$ mod 14, so the order is not 3. Thus the order must be 6.

(iii) $\phi(17) = 16$, so the order is 1,2,4,8 or 16. As 17 is a prime, we can eliminate 1 and 2 as in part (i). Now $5^4 \equiv 25^2 \equiv 8^2 \equiv 64 \equiv 13$ mod 17, so the order is not 4. Also $5^8 \equiv 13^2 \equiv (-4)^2 \equiv 16$ mod 17, so the order is not 8. Thus the order is 16.