

1) Show that 2 is a primitive root modulo 11.

A number is a primitive root modulo a prime p if its multiplicative order modulo p is $\phi(p) = p-1$. Here p is 11, so we need to check that the order of 2 mod 11 is 10.

Let us compute successive powers of 2 mod 11:

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 5, 2^5 \equiv 10, 2^6 \equiv 9, 2^7 \equiv 7, 2^8 \equiv 3, 2^9 \equiv 6, 2^{10} \equiv 1 \pmod{11}$$

No smaller positive exponent gives 1 modulo 11 so the order of 2 is 10 $= \phi(11)$. Hence 2 is a primitive root modulo 11.

2) How many incongruent primitive roots does 14 have?

Soln: If primitive roots exist modulo n , their number equals $\phi(\phi(n))$. First compute $\phi(14)$. Since $14 = 2 \cdot 7$, $\phi(14) = \phi(2) \cdot \phi(7) = 1 \cdot 6 = 6$. Thus the primitive root if it exists, is $\phi(\phi(14)) = 2$.

(Primitive roots do exist where p is an odd prime number) so the formula applies.

The units modulo 14 are $\{1, 3, 5, 9, 11, 13\}$. An element is primitive if it has

order 6. Checking for 3: $3^1 \equiv 3, 3^2 \equiv 9, 3^3 \equiv 13, 3^4 \equiv 11, 3^5 \equiv 5, 3^6 \equiv 1 \pmod{14}$

So 3 has order 6. Its inverse 5 (since $3 \cdot 5 \equiv 1$) is the other root. So the two incongruent primitive roots modulo 14 are 3 and 5.