QUESTION

For which of the following moduli does a primitive root exist? In the cases where one does exist, find one.

(i) 11 (ii) 30 (iii) 18 (iv) 27 (v) 4 (vi) 33.

ANSWER

By th.6.3, a primitive root mod n exists$\Leftrightarrow$ n is a power of an odd prime, twice a power of an odd prime, 2 or 4. Thus primitive roots exist for (i), (iii), (iv) and (v), but not for (ii) or (vi).

For a primitive root mod 11, we need an element of order 10. The possible orders for a mod 11 are 1,2,5 or 10, so we need to pick $a \not\equiv \pm 1$ mod 11 such that $a^5 \not\equiv 1$ mod 11. By trial and error, $a = 2$ is a suitable choice.

For a primitive root mod 18, we need, by the argument of th.6.3, to find an odd element a such that a is a primitive root mod 9. Now $\phi(9) = 6$, so we wish to find a, odd, such that $o(a)$ mod 9 is not equal to any of 1,2 and 3. By trial and error, 5 is a suitable choice.

For a primitive root mod 27, th.6.2 shows that we need only pick a primitive root mod 9. By the above, 5 is a suitable choice. (2 would also do here.)

Finally, for a primitive root mod 4, as $\phi(4) = 2$ we need only pick a residue prime 5to 4 and different from 1. 3 is the only possible candidate.