<u>Section 5 Lecture 32 – Primitive roots - Solutions</u>

Q1)

Note that 1 is never a primitive root as it just repeatedly gives 1, 1, …

(i)

$2^1 = 2 \pmod 3$
$2^2 = 1 \pmod 3$.

Hence this is a primitive root.

The only primitive root (mod 3) is 2

(ii)

$2^1 = 2 \pmod 5$
$2^2 = 4 \pmod 5$
$2^3 = 3 \pmod 5$
$2^4 = 1 \pmod 5$

Hence 2 is a primitive root.

$3^1 = 3 \pmod 5$
$3^2 = 4 \pmod 5$
$3^3 = 2 \pmod 5$
$3^4 = 1 \pmod 5$

Hence 3 is a primitive root

$4^1 = 4 \pmod 5$
$4^2 = 1 \pmod 5$
$4^3 = 4 \pmod 5$
$4^4 = 1 \pmod 5$

Hence 4 is not a primitive root.

The primitive roots (mod 5) are 2 and 3

(iii)

$2^1 = 2 \pmod{11}$, $2^2 = 4 \pmod{11}$, $2^3 = 8 \pmod{11}$, $2^4 = 5 \pmod{11}$, $2^5 = 10 \pmod{11}$, $2^6 = 9 \pmod{11}$, $2^7 = 7 \pmod{11}$, $2^8 = 3 \pmod{11}$, $2^9 = 6 \pmod{11}$, $2^{10} = 12 \pmod{11}$,
so primitive root

$3^1 = 3$ (mod 11), $3^2 = 9$ (mod 11), $3^3 = 5$ (mod 11), $3^4 = 4$ (mod 11), $3^5 = 1$ (mod 11), so will start to repeat and is not a primitive root

$4^1 = 4$ (mod 11), $4^2 = 5$ (mod 11), $4^3 = 9$ (mod 11), $4^4 = 3$ (mod 11), $4^5 = 1$ (mod 11), so will start to repeat and is not a primitive root

$5^1 = 5$ (mod 11), $5^2 = 3$ (mod 11), $5^3 = 4$ (mod 11), $5^4 = 9$ (mod 11), $5^5 = 1$ (mod 11), so will start to repeat and is not a primitive root

$6^1 = 6$ (mod 11), $6^2 = 3$ (mod 11), $6^3 = 7$ (mod 11), $6^4 = 9$ (mod 11), $6^5 = 10$ (mod 11), $6^6 = 5$ (mod 11), $6^7 = 8$ (mod 11), $6^8 = 4$ (mod 11), $6^9 = 2$ (mod 11), $6^{10} = 1$ (mod 11),
so primitive root

$7^1 = 7$ (mod 11), $7^2 = 5$ (mod 11), $7^3 = 2$ (mod 11), $7^4 = 3$ (mod 11), $7^5 = 10$ (mod 11), $7^6 = 4$ (mod 11), $7^7 = 6$ (mod 11), $7^8 = 9$ (mod 11), $7^9 = 8$ (mod 11), $7^{10} = 1$ (mod 11),
so primitive root

$8^1 = 8$ (mod 11), $8^2 = 9$ (mod 11), $8^3 = 6$ (mod 11), $8^4 = 4$ (mod 11), $8^5 = 10$ (mod 11), $8^6 = 3$ (mod 11), $8^7 = 2$ (mod 11), $8^8 = 5$ (mod 11), $8^9 = 7$ (mod 11), $8^{10} = 1$ (mod 11),
so primitive root

$9^1 = 9$ (mod 11), $9^2 = 4$ (mod 11), $9^3 = 3$ (mod 11), $9^4 = 5$ (mod 11), $9^5 = 1$ (mod 11), so will start to repeat and is not a primitive root

$10^1 = 10$ (mod 11), $10^2 = 1$ (mod 11), so will start to repeat and is not a primitive root

The primitive roots are 2, 6, 7, 8

Q2)

(i) $p = 3$

Product of primitive roots = 2 which is not 1 (mod 3) – this is the only exception

(ii) $p = 5$

Product of primitive roots = 2 x 3 = 6 = 1 (mod 5)

(iii) $p = 11$

Product of primitive roots = 2 x 6 x 7 x 8 = 672 = 1 (mod 11)