Tutorial 8

Q2

1. $(x + 3) \bmod 7 = 2$
   $\implies x \bmod 7 = (2 - 3) \bmod 7 = -1 \bmod 7 = 6$
   $\implies x = 6 + 7i, \; i \in \mathbb{Z}$
   $\implies x \in \{..., -8, -1, 6, 13, ...\}$
   x can have many values.

2. $5y \bmod 11 = 3$
   $\implies (5 \bmod 11 \times y \bmod 11) \bmod 11 = 3$
   $\implies y \bmod 11 = (3 \times 5^{-1} \bmod 11) \bmod 11$
   $5^{-1} \bmod 11 = 9$
   $\implies y \bmod 11 = (3 \times 9) \bmod 11 = 5$
   $\implies y = 5 + 11i, \; i \in \mathbb{Z}$
   $\implies x \in \{..., -17, -6, 5, 16, 27, ...\}$
   y can have many values.

Q3

$3^x \bmod 7, \; x \in \{1, 2, 3, 4, 5, 6\}$

3^1	3^2	3^3	3^4	3^5	3^6
3	2	6	4	5	1

Since the answers of $3^x \bmod 7$ have never repeated, 3 is a primitive root of 7.

Q4

$p = 11, \; q = 3, \; M = 6, \; e = 7$

ii)

$n = p \times q = 11 \times 3 = 33$
$R = 2, \; R^{-1} \bmod 33 = 2^{-1} \bmod 33 = 17$

iii)

$d = e^{-1} \bmod \phi(n)$
$= 7^{-1} \bmod (\phi(11) \times \phi(3))$
$= 7^{-1} \bmod 20 = 3$

$M' = MR^e \bmod n$
$S' = M'^d = M^d R^{e \times d} \bmod n = M^d R \bmod n$
$= 6^3 \times 2 \bmod 33 = 3$

Verification:
$S = S' R^{-1} \bmod n = 3 \times 17 \bmod 33 = 18$
$S = M^d \bmod n \implies M = S^e \bmod n = 18^7 \bmod 33 = 6$