EE2302 Foundations of Information Engineering Semester A, 2022/23

Solutions to Test 2

1. Note that $495 = 3^2 \times 5 \times 11$.
   Therefore, $\phi(495) = \phi(3^2) \times \phi(5) \times \phi(11) = 3 \times (3 - 1) \times 4 \times 10 = 240$.

2. Simplifying the equation, we obtain $16x \equiv -5 \equiv 38 \pmod{43}$.
   Next, we apply extended Euclidean algorithm.

43	16		
1	0	43	a
0	1	16	b
1	-2	11	$c = a - 2b$
-1	3	5	$d = b - c$
3	-8	1	$e = c - 2d$

   Therefore, $16^{-1} \equiv -8 \equiv 35 \pmod{43}$
   $x \equiv (35)(38) \equiv 40 \pmod{43}$.

3.
   a) $f \circ g = f\big(g(x)\big) = 3(4x + 7) \pmod{13} = 12x + 8 \pmod{13}$.

   b) Let $y = 4x + 7 \pmod{13}$.
      Then $x = 4^{-1}(y - 7) = 10(y + 6) = 10y + 8 \pmod{13}$
      Hence, $g^{-1}(y) = 10y + 8 \pmod{13}$.

4. Substitute each possible value to the equation and check whether the equation holds. It is straightforward to check that $x = 0, 1, 3$, or 4.

5. By Fermat's Little Theorem, $x^6 \equiv 1 \pmod{7}$.
   Therefore, the given equation can be simplified as $(x^6)^{337} \times x^2 \equiv x^2 \equiv 4 \pmod{7}$.
   Trying all values from 0 to 6, we obtain x =2 or 5.

6. Use the following table:

a_i	m_i	M_i	α_i
2	3	20	$20^{-1} \equiv 2^{-1} \equiv 2 \pmod 3$
1	4	15	$15^{-1} \equiv 3^{-1} \equiv 3 \pmod 4$
3	5	12	$12^{-1} \equiv 2^{-1} \equiv 3 \pmod 5$

$$\begin{aligned} x &= 2(20)(2) + 1(15)(3) + 3(12)(3) \pmod{60} \\ &= 233 \pmod{60} \\ &= 53 \end{aligned}$$

7.

a) $a = -1$.

b) Let the number be x and write it as $a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$.
Then $x \equiv a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0 \pmod{11}$
$\equiv a_n(-1)^n + a_{n-1}(-1)^{n-1} + \cdots + a_1(-1) + a_0 \pmod{11}$
Hence, the rule is to check whether the alternating sum

$$a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n$$

is divisible by 11.

8. $50\,x + 30\,y = 1490$.

50	30		
1	0	50	a
0	1	30	b
1	-1	20	$c = a - b$
-1	2	10	$d = b - c = -a + 2b$

$50(-1) + 30(2) = 10$
Multiplying both sides by 149, we obtain $50(-149) + 30(298) = 1490$.
The general solution is given by

$x = -149 + 3t.$
$y = 298 - 5t.$

Since x, y must be non-negative, we obtain $50 \le t \le 59$, so there are 10 combinations.

9.

a) Since $N = 37 \times 47$, which implies

$$\phi(N) = (p-1)(q-1) = 36 \times 46 = 1656.$$

and $25d \equiv 1 \pmod{1656}$.

1656	25		
1	0	1656	a
0	1	25	b
1	-66	6	$c = a - 66b$
-4	265	1	$d = b - 4c$

Hence, $d \equiv 265 \pmod{1656}$.

b) The ciphertext is given by $c = 314^{25} \pmod{N} = 314^{25} \pmod{1739}$.

$$314^2 \bmod 1739 = 1212\ mod\ 1739$$

$$314^4 \bmod 1739 = 1228 \bmod 1739$$

$$314^8 \bmod 1739 = 271 \bmod 1739$$

$$314^{16} \bmod 1739 = 403 \bmod 1739$$

$$314^{25} \pmod{1739} = 314^{16+8+1} \bmod 899 = 403 \times 271 \times 314 \bmod 1739$$

$$= 1541\ mod\ 1739$$

Hence, $c = 1541$.