Maciej Medyk – COT6427 – Secret Sharing Algorythms – Homework 01

Question 1 – Which one is a primitive root of 7? A. 3 || B. 5 || C. 2

3^1 (mod 7) = 3 (mod 7)	=	**3**	5^1 (mod 7) = 5 (mod 7)	=	**5**	2^1 (mod 7) = 2 (mod 7)	=	**2**
3^2 (mod 7) = 9 (mod 7)	=	**2**	5^2 (mod 7) = 25 (mod 7)	=	**4**	2^2 (mod 7) = 4 (mod 7)	=	**4**
3^3 (mod 7) = 27 (mod 7)	=	**6**	5^3 (mod 7) = 125 (mod 7)	=	**6**	2^3 (mod 7) = 8 (mod 7)	=	**1**
3^4 (mod 7) = 27 (mod 7)	=	**4**	5^4 (mod 7) = 625 (mod 7)	=	**2**	2^4 (mod 7) = 16 (mod 7)	=	**2**
3^5 (mod 7) = 243 (mod 7)	=	**5**	5^5 (mod 7) = 3125 (mod 7)	=	**3**	2^5 (mod 7) = 32 (mod 7)	=	**4**
3^6 (mod 7) = 729 (mod 7)	=	**1**	5^6 (mod 7) = 15625 (mod 7)	=	**1**	2^6 (mod 7) = 64 (mod 7)	=	**1**

Both **3 and 5 are primitive roots of 7** as each calculation gives unique result; however, 2 is not a primitive root of 7.

Question 2 – Find an inverse of "23" modulo "120". Also solve the following congruent equation 23x ≡ 3 (mod 120) for x. Use the Euclid's Algorithm and the Extended Euclid's Algorithm.

120 = **23** x 5 + **5**	**5** = 120 - 5 x **23**
23 = **5** x 4 + **3**	**3** = 23 - 4 x **5**
5 = **3** x 1 + **2**	**2** = 5 - 1 x **3**
3 = **2** x 1 + **1**	**1** = 3 - 1 x **2**
2 = **1** x 2 + 0	

1 = 3 – 1 x 2 = 1 x 3 – 1 x 2
1 = 1 x 3 – 1 x 2 = 3 – 1 x (5 – 1 x 3) = -1 x 5 + 2 x 3
1 = -1 x 5 + 2 x 3 = -1 x 5 + 2 x (23 – 4 x 5) = 2 x 23 – 9 x 5
1 = 2 x 23 – 9 x 5 = 2 x 23 – 9 x (120 – 5 x 23)
= **-9** x 120 + **47** x 23

47 is an inverse of 23 modulo 120 → (23 x 47) mod 120 = 1

23 x X ≡ 3 (mod 120)
47 x 23 x X ≡ 47 x 3 (mod 120)
1081 x X ≡ 141 (mod 120)
X ≡ 21 (mod 120)

Solutions are integers X such as X ≡ 21 (mod 120) which are **21, 141, 261, …** and **-99, -219, -339, ….**

Question 3 – Use the Fermat's little theorem to find: 3^{52} (mod 11) .

3^{52} (mod 11) = 3^{50+2} (mod 11) = $(3^{10})^5$ (mod 11) x 3^2 (mod 11) = 1^5 x 9 (mod 11) = **9**

Question 4 – What are the prime factorizations of “48” and “60”? Also, find GCD(48, 60) and LCM(48, 60).

To calculate GCD and LCM we need to find prime factorialization of 48 and 60.

48/**2**	=	24
24/**2**	=	12
12/**2**	=	6
6/**2**	=	3
3/**3**	=	1

60/**2**	=	30
30/**2**	=	15
15/**3**	=	5
5/**5**	=	1

GCD = $2^{\min(2,4)} \times 3^{\min(1,1)} \times 5^{\min(0,1)} = 2^2 \times 3^1 \times 5^0 = 4 \times 3 \times 1 =$ **12**
LCD = $2^{\max(2,4)} \times 3^{\max(1,1)} \times 5^{\max(0,1)} = 2^4 \times 3^1 \times 5^1 = 16 \times 3 \times 5 =$ **240**

Question 5 – What is the decimal expansion of $(1B6)_{16}$? What is the Hexadecimal expansion of “485”?

Decimal expansion of $(1B6)_{16}$ is (0=0, 1=1, 2=2, 3=3, 4=4, 5=5, 6=6, 7=7, 8=8, 9=9, A=10, B=11, C=12, D=13, E=14, F=15)

$1 \times 16^2 + 11 \times 16^1 + 6 \times 16^0 = 1 \times 256 + 11 \times 16 + 6 \times 1 = 256 + 176 + 6 =$ **438**

Hexadecimal expansion of 495 is

485 = 16 x 30 + 5 → 5
30 = 16 x 1 + 14 → E
1 = 16 x 0 + 1 → 1

Since 1 = 1 , 14 = E , 5 = 5 then 438 = **1E5**

Question 6 – What sequences of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (4_{xn}+1) \bmod 7$ with seed $x_0 = 3$?

$X_1 = 4 \times X_0 + 1 \bmod 7 = 4 \times 3 + 1 \bmod 7 = 13 \bmod 7 =$ **6**
$X_2 = 4 \times X_1 + 1 \bmod 7 = 4 \times 6 + 1 \bmod 7 = 25 \bmod 7 =$ **4**
$X_3 = 4 \times X_2 + 1 \bmod 7 = 4 \times 4 + 1 \bmod 7 = 17 \bmod 7 =$ **3**
$X_4 = 4 \times X_3 + 1 \bmod 7 = 4 \times 3 + 1 \bmod 7 = 13 \bmod 7 =$ **6** sequence starts to repeat

Therefore, expected sequence is 6, 4, 3, 6, 4, 3, 6, 4, 3, 6, 4, 3, ….

Question 7 – The validity of an ISBN can be evaluated as explained in the class. 1) If the first 9 digits are “987654321”, what is the check digit x_{10}? 2) Is “9753842601” (where x1=9 & x_{10}=1) a valid ISBN number?

If 987654321 are first 9 digits what is digit x_{10}?

$X_{10} = ((1 \times 9) + (2 \times 8) + (3 \times 7) + (4 \times 6) + (5 \times 5) + (6 \times 4) + (7 \times 3) + (8 \times 2) + (9 \times 1)) \pmod{11}$
$X_{10} = (9 + 16 + 21 + 24 + 25 + 24 + 21 + 16 + 9) \pmod{11}$
$X_{10} = 165 \pmod{11} \equiv 0 \pmod{11}$ → $\mathbf{X_{10} = 0}$ → 9876543210 is a valid ISBN

Is 9753842601 valid ISBN number?
$((1 \times 9) + (2 \times 7) + (3 \times 5) + (4 \times 3) + (5 \times 8) + (6 \times 4) + (7 \times 2) + (8 \times 6) + (9 \times 0) + (10 \times 1)) \pmod{11}$
$(9 + 14 + 15 + 12 + 40 + 24 + 14 + 48 + 0 + 10) \pmod{11}$
$186 \pmod{11} \equiv 10 \pmod{11}$ → **is not a valid ISBN**

Question 8 – Trace the Miller-Rabin probabilistic primality-test algorithm for a prime as well as a composite number. Provide details with respect to your tracing.

Using Miller-Rabin to test prime number of 41 and use security parameter t = 3.
n-1 = 41 -1 = 40

40/2 = 20
20/2 = 10
10/2 = 5
5/5 = 1

That means we have equation **n-1 = 2^3 x 5**

do outer_loop with index 1 and since (index <= t is true → 1 <= 3) then
    we choose a = 3
    y = a^5 (mod 41) = 3^5 (mod 41) = 243 (mod 41) = **38**
    since ((y != 1 is true → 38 != 1) and (y != n-1 is true → 38 != 40)) then set j = 1 and do inner_loop
        since ((j <= s is true → 1 <= 2) and (y != n-1 is true → 38 != 40)) then continue with inner_loop
            y = y^2 (mod 41) = 38^2 (mod 41) = 1444 (mod 41) = **9**
            j = j +1 = 2
        since ((j <= s is true→ 2 <= 2) and (y != n-1 is true → 9 != 40)) then continue with inner_loop
            y = y^2 (mod 41) = 9^2 (mod 41) = 81 (mod 41) = **40**
            j = j +1 = 3
        since ((j <= s is false → 3 > 2) and (y != n-1 is false→ 40 == 40)) then finish inner_loop
    since (y != n-1 is false → 40 == 40) continue
do outer_loop with index 2 and since (index <= t is true → 2 <= 3) then
    we choose a = 6
    y = a^5 (mod 41) = 6^5 (mod 41) = 7776 (mod 41) = **27**
    since ((y != 1 is true → 27 != 1) and (y != n-1 is true → 27 != 40)) then set j = 1 and do inner_loop
        since ((j <= s is true → 1 <= 2) and (y != n-1 is true → 27 != 40)) then continue with inner_loop
            y = y^2 (mod 41) = 27^2 (mod 41) = 729 (mod 41) = **32**
            j = j +1 = 2
        since ((j <= s is true→ 2 <= 2) and (y != n-1 is true → 32 != 40)) then continue with inner_loop
            y = y^2 (mod 41) = 32^2 (mod 41) = 1024 (mod 41) = **40**
            j = j +1 = 3
        since ((j <= s is false → 3 > 2) and (y != n-1 is false→ 40 == 40)) then finish inner_loop
    since (y != n-1 is false → 40 == 40) continue
do outer_loop with index 2 and since (index <= t is true → 3 <= 3) then
    we choose a = 28
    y = a^5 (mod 41) = 28^5 (mod 41) = 17210368 (mod 41) = **3**
    since ((y != 1 is true → 3 != 1) and (y != n-1 is true → 3 != 40)) then set j = 1 and do inner_loop
        since ((j <= s is true → 1 <= 2) and (y != n-1 is true → 3 != 40)) then continue with inner_loop
            y = y^2 (mod 41) = 3^2 (mod 41) = 9 (mod 41) = **9**
            j = j +1 = 2
        since ((j <= s is true→ 2 <= 2) and (y != n-1 is true → 9 != 40)) then continue with inner_loop
            y = y^2 (mod 41) = 9^2 (mod 41) = 81(mod 41) = **40**
            j = j +1 = 3
        since ((j <= s is false → 3 > 2) and (y != n-1 is false→ 40 == 40)) then finish inner_loop
    since (y != n-1 is false → 40 == 40) continue
do outer_loop with index 3 and since (index <= t is false → 4 > 3) then outer_loop ends
return prime

Using Miller-Rabin to test composite number of 49 and use security parameter 2.
n-1 = 49 -1 = 48

48/2 = 24
24/2 = 12
12/2 = 6
6/2 = 3
3/3 = 1

That means we have equation **$n-1 = 2^2 \times 3$**

do outer_loop with index 1 and since (index <= t is true → 1 <= 2) then
we choose a = 6
$y = a^5$ (mod 49) = 6^3 (mod 49) = 216 (mod 49) = **20**
since ((y != 1 is true → 20 != 1) and (y != n-1 is true → 20 != 40)) then set j = 1 and do inner_loop
since ((j <= s is true → 1 <= 3) and (y != n-1 is true → 20 != 24)) then continue with inner_loop
$y = y^2$ (mod 49) = 20^2 (mod 49) = 400 (mod 49) = **8**
j = j +1 = 2
since ((j <= s is true→ 2 <= 3) and (y != n-1 is true → 8 != 40)) then continue with inner_loop
$y = y^2$ (mod 49) = 8^2 (mod 49) = 64 (mod 49) = **15**
j = j +1 = 3
since ((j <= s is true → 3 <= 3) and (y != n-1 is true → 15 != 40)) then continue with inner_loop
$y = y^2$ (mod 49) = 15^2 (mod 49) = 225 (mod 49) = 29
j = j +1 = 4
since ((j <= s is false → 4 > 3) and (y != n-1 is true → 29 != 40)) then finish inner_loop
since (y != n-1 is true → 29 != 40) **return composite**