C Foley
(attempt 2)

# Initial Test

**Instructor: Mehrdad Nojoumian**
**COT 6427: Secret Sharing Protocols**

**(1)** Which one is a primitive root of 7?

Definition: a primitive root modulo a prime **p** is an integer **r** in $Z_p$ such that every nonzero element of $Z_p$ is a power of **r**.

a) 3

b) 5

c) 2

47

**(2)** Find an inverse of "23" modulo "120". Subsequently, Solve the congruent equation $23x \equiv 3 \pmod{120}$ for "x". (Hint: Use Euclid's Algorithm & Extended Euclid's Algorithm) 21

Definition: an integer **ā** such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an inverse of **a** modulo **m**.

9

**(3)** Use the Fermat's little theorem to find: $3^{52} \pmod{11}$

Theorem: $a^{p-1} \equiv 1 \pmod{p}$

9

**(4)** What are the prime factorizations of "48" and "60"?

$48 = 2^3 \times 3$ $60 = 2^4 \times 3 \times 5$

**(5)** Find GCD(48, 60) and LCM(48, 60).

**(6)** What is the decimal expansion of $(1B6)_{16}$ ? What is the Hexadecimal expansion of "485"?

$1B6_{16} = 438_{10}$ $485_{10} = 1D5_{16}$

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

0 6 4 3

$23x \equiv 1 \pmod{120}$

$120 = 23 \times 5 + 5$

$23 = 5 \times 4 + 3$

$5 = 3 \times 1 + 2$

$3 = 2 \times 1 + 1$

$2 = 1 \times 2 + 0$

$1 = 3 - 2 \times 1$

$= 3 - [5 - 3 \times 1] \times 1 = -1 \times 5 + 2 \times 3$

$= -1 \times 5 + 2(23 - 4 \times 5) = -9 \times 5 + 2 \times 23$

$= -9(120 - 23 \times 5) + 2 \times 23$

$= -9 \times 120 + 45 \times 23 + 2 \times 23$

$= -9 \times 120 + 47 \times 23$

---

$23x \equiv 3 \pmod{120}$

$47 \times 23x \equiv 47 \times 3 \pmod{120}$

$x \equiv 141 \pmod{120}$

$x \equiv 21$

---

$3^{52} \pmod{11}$

$3^{10} \equiv 1 \pmod{11}$

$52 = 5 \times 10 + 2$

$3^{52} = (3^{5 \times 10})(3^2) \pmod{11}$

$= 9 \pmod{11}$

$= 9$